# データ収集間隔を5分と1時間とした時のWi-Fi情報を活用した個人認証手法における認証精度への影響

小林 良輔[1,2]　山口 利恵[2]

**概要**：近年，行動情報を活用した個人認証手法に関する多くの研究がなされている．IoT 技術の発達により，人の周辺機器に搭載されているセンサー等から，行動情報を容易に収集可能となったことがその原因の一つと考えられる，特に，スマートフォンは行動情報を収集するための IoT デバイスとして使用されることが多い．最近では大多数の人が自分専用のスマートフォンを所持しており，これらの機器は行動情報を収集することで，所有者の行動をトラッキングすることができる．ただし，人の行動をトラッキングすることは，スマートフォンのバッテリー消費やプライバシー問題に影響を与える．これらの問題は，情報収集の間隔が短いほどより深刻になることが容易に考えられる．そこで本論文では，行動認証技術の一つである Wi-Fi 情報を活用した個人認証手法において，データ収集間隔を 5 分と 1 時間の 2 つのケースに設定した場合における認証精度の影響を調査した．本実験では，16,027 人から各自のスマートフォンを用いて Wi-Fi の情報を収集し，その中からランダムに 100 人のデータを選択して利用した．その結果，2 つのケースにおいて認証精度への影響は軽微であることがわかった．

# Effects of Tracking Interval on Accuracy of Personal Authentication Using Wi-Fi Information Captured by Smartphone

RYOSUKE KOBAYASHI[1,2]　RIE Shigetomi YAMAGUCHI[2]

## 1. はじめに

近年，行動情報を活用した個人認証 (行動認証) 手法に関する多くの研究がなされている．行動認証は，人の行動情報から得られる個人ごとの特徴を活用した認証手法である．最近では IoT (Internet of Things) 技術の発展により行動情報を容易に収集できるようになった．行動認証で利用するデータは IoT デバイスによって自動的に収集することが可能で，人々はデータが収集されていることに意識する必要はない．したがって，パスワードベースなどの従来の認証手法とは異なり，利用者は認証のために意識的にデータを入力する必要はない．IoT デバイスを活用した行動認証手法は，従来の認証手法と比較して，利用者にとってより便利な手法であることが期待されている．

上で述べた通り，スマートフォンは行動情報の収集に役立てることができる．人の行動情報を収集するためにはセンサーが必要であり，スマートフォンには GPS，電波，加速度などのさまざまなセンサーが搭載されている．我々は行動認証手法における研究において，さまざまな IoT デバイスの中からスマートフォンに注目することにした．その理由の 1 つは，現在ほとんどの人が自身のスマートフォンを所持し利用していることだ．*Statista* の調査によると，スマートフォンは多くの国で 70 %を以上普及しているとのことだ [1]．もう 1 つの理由は，スマートフォンユーザーはほとんどの場合，自身のデバイスを携帯しているということである．スマートフォンは間違いなく人々の生活に欠かせないものになっている．この 2 つの理由から，多くの人が常に携帯しているスマートフォンが，人間の行動を観察するための最も適切なデバイスであると判断し，スマートフォンを行動認証研究における実験に利用することとした．

人の行動情報を個人認証に活用するには，スマートフォンのセンサーで所持者の行動をトラッキングする必要がある．つまり，スマートフォンのセンサーを一定の間隔で起

[1] 三菱電機インフォメーションシステムズ株式会社
[2] 東京大学大学院情報理工学系研究科

動し，その時点でのセンサー情報を収集する必要がある．起動の回数が多いほど，つまりデータ収集間隔が短いほど，行動追跡の精度が向上することになる．ただしデータ収集間隔を短くすることは，以下の 2 つの問題を表面化させることになる．1 つ目はスマートフォンのバッテリー消費量の増加である．普段から所持しているスマートフォンは行動認証のためだけに使用されるものではなく，認証以外のサービスに利用されていることが主なのは明らかである．認証機能がバッテリーの大部分を使用したとすると，本来使用するためのサービスにバッテリー充てることができず，それは行動認証に期待されている便利さとは程遠いものとなるであろう．2 つ目はプライバシーの問題である．頻繁な行動追跡は，ユーザーが監視されていると感じるため，ユーザーに不快感を与える可能性がある．これらの問題があるため，スマートフォンセンサーを活用した認証手法では，より長いデータ収集間隔が推奨されるべきであると我々は考える．

本誌で参照する行動情報に関する既存の研究では，5 分ごとに情報が収集され実験が行われた [2]．データ収集間隔が行動認証の精度に及ぼす影響を調べるために，本論文では 2 つの実験を行った．1 つは既存研究と同様にデータ収集間隔を 5 分に設定し，もう 1 つの実験では収集間隔を 1 時間に設定した．実験では，人の行動を表す情報として既存研究と同様，Wi-Fi 情報を利用した．この 2 つの実験の結果を比較することにより，データ収集間隔の長さが認証精度に与える影響を調査した．

本論文は次のように構成されている．2 章では，スマートフォンを活用した行動認証手法に関するいくつかの既存の研究を紹介する．3 章では，Wi-Fi 情報を利用した認証技術について説明する．4 章では，本実験におけるデータセット，実験シナリオ，および実験の結果について説明する．5 章では，実験結果からの行動認証の精度に対するデータ収集間隔の影響について説明する．6 章では，本論文における結論と今後の課題について記述する．

## 2. 関連研究

本章では行動情報を活用した個人認証手法に関する既存の研究をいくつか紹介する．個人認証に活用される行動には次に述べる 2 つのタイプがあると考えられる．第一のタイプは特定の動作を活用したものである．この動作を活用する認証手法では，ユーザーはタッチスクリーンジェスチャー [3] や歩容 [4] など，認証時に意識的な動作をとる必要がある．つまり，従来のパスワード認証や生体認証と同様，ユーザーは認証を求められると自ら認証情報を入力する必要があるのである．第二のタイプは，頻繁な繰り返しによって獲得される無意識の行動パターンである生活習慣を活用する認証手法である．生活習慣を記録したデータを意味するライフログを利用した認証方法の例として，リスクベース認証 [5] がある．クエリの入力を意識せずにユーザーを認証する方法は，一般に *Implicit Authentication* [6] と呼ばれている．我々のターゲットは後者のタイプの行動情報を活用した認証手法であり，前者はこの論文では言及しない．

位置情報は人の生活習慣を理解しやすくするライフログの一種である．行動認証に関する研究では，位置情報を活用したものが多い．Mahbub ら [7] は，位置情報から得られる移動履歴を活用した個人認証手法に隠れマルコフモデルを採用することを提案している．また，Sieranoja ら [8] は，ガウス混合モデル-ユニバーサルバックグラウンドモデルによってモデル化された，GPS から得られる短期間の位置情報の変化データを使用した．これら 2 つの研究では，彼らの実験にオープンデータを使用している．データが収集された間隔は彼らの論文に正確に記載されてはいないが，データからそれはほんの数秒であったと推測することができる．Fridman ら [9] は，オープンデータではなく 200 人の被験者の行動データを実験のために収集し，実験に使用している．彼らは位置情報だけでなく，テキスト，アプリ利用履歴，ウェブサイトの閲覧情報も収集し，個人認証手法に活用されている．4 つのモダリティは，各被験者のスマートフォンまたはタブレットにインストールされた追跡アプリケーションによって 1 秒間隔で収集された．これらの既存の研究によって示されるように，行動情報を利用する従来の認証方法では，人の行動の追跡間隔は非常に短かったことがわかる．

人間の生活習慣を表すいくつかの種類の行動情報では，センサーによる定期的なトラッキングをせずに収集できるものもある．たとえば，スマートフォンアプリの利用情報は利用者がアプリを利用した場合にのみ情報が収集され，この情報の中には所有者の特徴が含まれていると考えられる．つまり，情報を収集するためにスマートフォンのセンサーを起動する必要はない．この種類の行動情報を利用する個人認証手法を提案した研究も存在する．Ashibani ら [10] は，個人認証にスマートフォンアプリケーションの利用情報を活用した．彼らは，Android アプリを使用して，ネットワークの使用状況とネットワークアクセス時間の長さに基づいて，アプリケーションへのアクセス情報を取得している．また，アプリケーションへのアクセス情報ではなく，アプリケーションの利用内容を利用した認証方法に関する研究も存在する．Sultana ら [11] は Twitter に投稿されたコンテンツを使用した個人認証手法を提案している．

## 3. 認証手法

本章では，Wi-Fi 情報を活用した認証手法について説明する．本論文では，この手法を単に Wi-Fi 認証と呼ぶこととする．スマートフォンに搭載されているの Wi-Fi センサーは，周囲に設置されているの Wi-Fi アクセスポイント

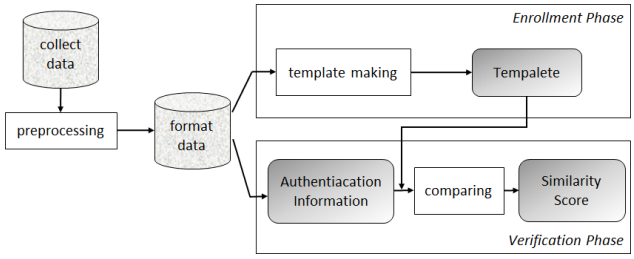


**図 1** Overview of Wi-Fi Authentication Method

を検索し，そのアクセスポイントの情報を取得する．アクセスポイントはスマートフォンに接続されているものだけでなく接続されていないものについても取得対象となる．センサーによってキャプチャされる情報には，Service Set ID (SSID)，Basic Service Set ID (BSSID)，およびキャプチャの時間が含まれる．Wi-Fi 認証手法ではこれらの情報のうち，キャプチャされたアクセスポイントの BSSID と時間を使用する．本論文では BSSID の情報を単にアドレスと呼ぶこととする．

### 3.1 手法概要

図 1 は Wi-Fi 認証手法の概要を示したものである．Wi-Fi 認証手法は，Wi-Fi 情報から得られる日常生活の個人の特徴を活用したものだ．人の行動というものは通常，生活習慣に応じて毎日同じように繰り返される．ただし，この日常の行動パターンが常に同じであるとは限らない．例えば，電車遅延などでいつもとは違う時間の電車に乗ったり，初めての場所に行くといったことである．このように人間の行動には変動があり，本論文ではこの変動をゆらぎと呼ぶ．日常の行動パターンの繰り返しを利用して個人認証を行うためには，このゆらぎを吸収するような処理が必要となってくる．

一般に，認証システムは 2 つのフェーズで構成されるものだ．1 つ目は登録フェーズであり，2 つ目は検証フェーズである．本論文で扱う Wi-Fi 認証手法も 2 つのフェーズで構成されている．登録フェーズは，テンプレートを作成するために行われ，検証フェーズより前に実施される必要がある．テンプレートとは，Wi-Fi 情報を分析して得られたユーザーに関する生活習慣の特徴が含まれている情報である．検証フェーズでは，認証情報を前のフェーズで作成したテンプレートと比較することにより，ユーザーが正当であるかどうかを確認するために行われる．Wi-Fi 認証手法では，認証情報とテンプレートの比較結果から類似度スコアを計算し，スコアが特定のしきい値よりも高い場合，ユーザーが正当であると判断する．

### 3.2 データ処理

図 1 には Wi-Fi 情報を活用した認証手法において実施される 3 つのデータ処理が記載されている．本節ではこれらの処理について説明する．

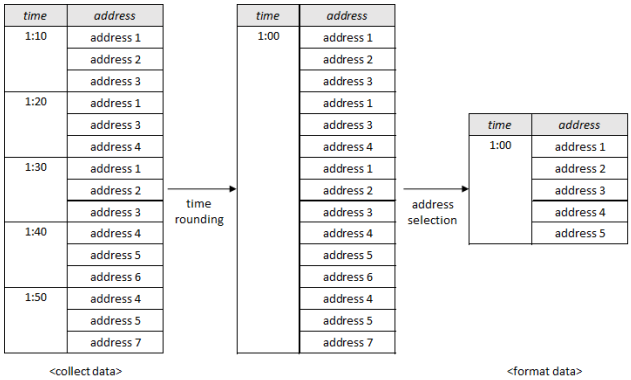


**図 2** Example of Preprocessing

#### 3.2.1 Preprocessing

*preprocessing* とは，スマートフォンのセンサーで収集したデータを，人の行動のゆらぎを吸収するためのフォーマットデータに変換するプロセスである．Wi-Fi 情報には，時間のゆらぎとアドレスのゆらぎといった 2 種類のゆらぎが表される．ここでは 2 種類のゆらぎそれぞれについて，ゆらぎとは何かをを説明し，そのゆらぎを吸収するための処理について説明する．

人は自身の生活習慣において，ほぼ同じ時間にほぼ同じ行動を取ることが多い．たとえば，通勤や通学のために毎朝同じ電車に乗ることが想定される．ある日電車が遅れたとすると，同じ電車に乗ったとしても目的地に到着するのはいつもと少し違う時間になることになる．その結果，自身のスマートフォンセンサーは異なる時間に同じアドレスをキャプチャすることになる．この事象は時間のゆらぎとして表される．時間のゆらぎを吸収するには，ある時間に取得されたデータと，その時間から一定の期間内に取得されたデータとを同じであると見なす必要がある．これを満たすために，センサーがデータをキャプチャする時間を時間単位で丸めることとする．これは，時間の分単位を削除することを意味するものである．

普段の生活パターンと同じ行動をとっていても，時にはモバイルアクセスポイントを持っている誰かとすれ違う可能性もある．このときスマートフォンセンサーは，通常はキャプチャしないアクセスポイントのアドレスを取得することになる．この事象はアドレスのゆらぎとして表されることになる．アドレスのゆらぎを吸収するためには，スマートフォンユーザーの行動を特徴付けるアドレスを抽出し，それらの特徴を持たないアドレスを破棄する必要がある．これを満たすために，1 時間で最もキャプチャされた 5 つのアドレスを選択し，その 5 つのアドレスをユーザーの行動を特徴づけるものだと定義する．

*preprocessing* の例を図 2 に示す．図の左側は収集し

たデータ例を示しており，センサーが 1:10 に 3 つのアドレス (address1, address2, address3) をキャプチャしたことを表している．収集データにたいして時間丸めとアドレス選択を処理することにより，フォーマットデータを得ることができる．図の右側に示されているフォーマットデータは，センサーが 1:00 に 5 つのアドレス (address1,address2,address3,address4,address5) をキャプチャしたことを表している．$A_{d,t}$ をある日 $d$ とある時間 $t$ $(0 \leq t \leq 23)$ のフォーマットデータのアドレスのセットとして定義すると，図 2 のフォーマットデータは以下のように表現することができる．

$$A_{d,1} = \{\text{address 1, address 2, address 3, address 4, address 5}\}.$$

#### 3.2.2 Template Making

この処理は，スマートフォンユーザーの特徴を備えたテンプレートを作成するためのものである．テンプレートにユーザーの特徴を持たせるためには，ある程度の長さの Wi-Fi 情報が必要となってくる．なぜなら，人の行動は毎日わずかに異なり，1 日の情報だけでは十分に特徴を表すことができないからである．この期間を登録期間と呼び，本論文では登録期間として 30 日間を設定した．

$a$ をあるアドレスとして， $c(A_{d,t}, a)$ を以下の通り定義する．

$$c(A_{d,t}, a) = \begin{cases} 1 & \texttt{if } \ a \in A_{d,t} \\ 0 & \texttt{otherwise} \end{cases}$$

このとき，テンプレート $T_t(a)$ を以下の通り定義する．

$$T_t(a) = \frac{\Sigma_d \ c(A_{d,t}, a)}{W}$$

$$where \begin{cases} W & = \Sigma_a \ \Sigma_d \ c(A_{d,t}, a) \\ d & \in \text{登録期間} \end{cases}$$

#### 3.2.3 Comparing

この処理は，認証情報とテンプレートとを比較することによって類似度スコアを計算するためのものである．認証システムは，ユーザーの特徴を持つテンプレートと認証情報がどれだけ類似しているかを計算することにより，ユーザーが正当であるかどうかを検証することができる．認証情報は，毎日繰り返される習慣を利用しているもので，1 日のデータで構成されている．つまり，ある日 $d$ の認証情報は，$A_{d,t}$ $(where\ 0 \leq t \leq 23)$ として表すことができる．

ある日 $d$ において検証を実施し類似度スコアを算出したとして，その類似度スコアを $S_d$ とすると，$S_d$ は以下の通り定義される．

$$S_d = \frac{\Sigma_t \ \Sigma_a \ T_t(a)}{24}$$

$$where\ a \in A_{d,t}.$$

類似度スコア $S_d$ があるしきい値より高い時に，認証システムはそのユーザーを正当だと判定する．

## 4. 実験

### 4.1 データセット

東京大学大学大学院情報理工学系研究科ソーシャル ICT 研究センター (SICT) は，2017 年 1 月 11 日から 4 月 26 日まで，ライフスタイル認証に関する研究データを収集するために，MITHRA プロジェクトという大規模な実証実験を実施した [12] ．実験参加者はインターネット等で募集され，総参加者数は 57,046 名であった．すべての参加者は，MITHRA プロジェクトに参加する前にデータを提供することに同意し，実験期間中の自身が決めたタイミングで参加を開始した．また，参加者はいつでも実験を中断することもできた．MITHRA プロジェクトは，同情報理工学系研究科の倫理審査委員会によって約半年間に渡り審査が行われ，同委員会の承認を得たうえで実施された．

参加者の一部は，この実証実験のために東京大学が開発した MITHRA アプリケーションを自身のスマートフォンにインストールした．このアプリケーションはバックグラウンドで 5 分ごとに起動され，アプリケーションがインストールされているデバイスに関する情報とデバイス周辺の情報を収集する仕組みであった．収集された情報には，場所，Wi-Fi の SSID と BSSID，IP アドレス，OS バージョン，およびデバイスモデル名，が含まれている．本実験では MITHRA アプリケーションによって収集されたデータを使用した．

MITHRA アプリケーションをインストールした参加者は，実証実験参加者のうちの 16,027 人であった．本実験では参加者の中から以下の条件を満たす 100 人のユーザーをランダムに選び，そのデータを使用した．

- Android 端末利用者.
- 60 日以上の実験参加者.

実験は最大 3 か月以上に渡り実施されたが，本実験ではそのうち 60 日間のデータのみを使用した．データの最初の 30 日間は登録フェーズ用で，最後の 30 日間は検証フェーズ用に使用した．

### 4.2 実験シナリオ

本研究では，2 つの実験を実施した．1 つはデータ収集間隔を 5 分に設定したものであり，もう 1 つは間隔を 1 時間に設定したものである．これら 2 つの実験には同じデータセットを利用した．MITHRA アプリケーションは 4.1 節で説明したように 5 分ごとに実行されるため，Wi-Fi 情報のデータ収集間隔も 5 分となっている．そのため，2 つ目の実験では 1 時間ごとに最初のデータを残し，前処理で他のデータを削除することにより，1 時間ごとに Wi-Fi 情報が収集されたとシミュレートすることにより実施した．

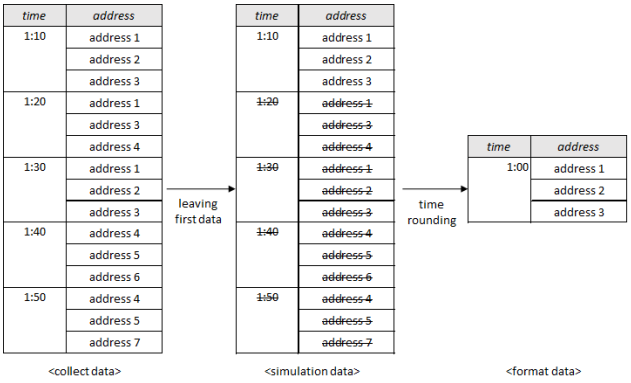


**図 3** Example of Simulation to Collect Data Hourly

図 3 は，1 時間ごとにデータを収集するシミュレーションの例を示している．図の中央は，1 時間のうち最初にキャプチャされたデータが残り，その他のデータは削除されていることを表している．この例の場合，すべてのアドレスが 1 回だけキャプチャされるようにシミュレートされているため，*preprocessing* で 1 時間に最もキャプチャされた 5 つのアドレスを選択する必要はなく，

$$A_{d,1} = \{\text{address 1, address 2, address 3}\}.$$

と表すことができる．図 2 と図 3 のフォーマットデータを比べると，その違いを確認することができる．

### 4.3 実験結果

本実験は，TAR (True Acceptance Rate : 本人受入率) と FAR (False Acceptance Rate : 他人受入率) を用いて評価を行った．TAR と FAR は次のように定義される．

$$TAR = \frac{(Number\ of\ Acceptance)}{(Number\ of\ Personal\ Test)}$$

$$FAR = \frac{(Number\ of\ Acceptance)}{(Number\ of\ Others\ Test)}$$

ここで $PersonalTest$ とは，あるユーザーのテンプレートと同じユーザーの認証情報を比較するテストを意味する．また $OthersTest$ とは，あるユーザーのテンプレートと別のユーザーの認証情報を比較するテストを意味する．この実験では，60 日間のデータのうち後半 30 日間のデータを認証情報として用いて，$PersonalTest$ と $OthersTest$ の両方を実施した．また本実験での別のユーザーとは，自分以外の 99 人のユーザーすべてを意味し，$OthersTest$ の認証情報は，99 人のユーザーのデータから作成された．$PersonalTest$ は 30 回 (30 日分のデータを使用) 実施され，$OthersTest$ は合計 2,970 回実施された (99 人 × 30 日)．

図 4 と図 5 は実験結果を示したグラフである．図 4 は，しきい値を 0 から 1 に変化させた時の，データ収集間隔が 5 分と 1 時間の 100 ユーザーの平均 TAR を示したものだ．この図からしきい値が高くなるにつれ，TAR は低くなっていくことがわかる．5 分間隔の方が TAR は少し高くなっているが，この図の 2 つの結果に大きな差はないことがわかる．実際，しきい値が 0.26 の時に 2 つの差は最大となり，約 0.1 である．図 5 は，しきい値を 0 から 0.2 に変化させたときの，データ収集間隔が 5 分と 1 時間の 100 ユーザーの平均 FAR を示している．この図から，どちらの場合も FAR の値が非常に低いことがわかる．

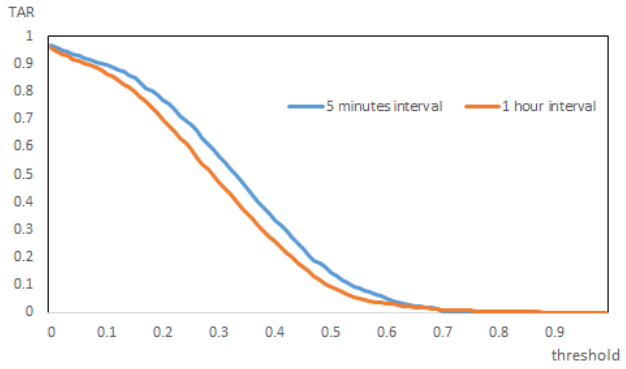


**図 4** Average TAR of 100 Users

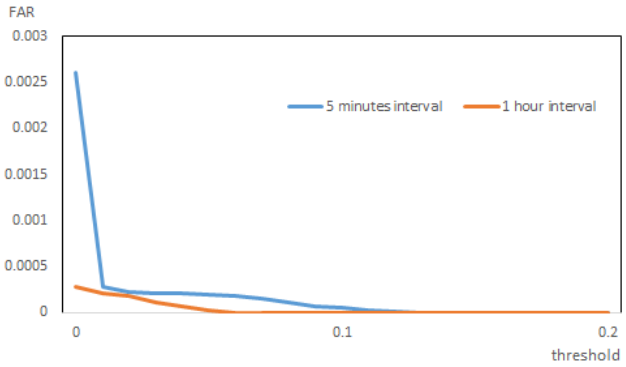


**図 5** Average FAR of 100 Users

## 5. 考察

FRR（False Rejection Rate，FRR = 1-TAR）および FAR は，認証手法を評価するためによく使用される指標である．2 つの指標があるしきい値で同じ値をとる場合，その値は EER (Equal Error Rate) として認証手法の精度と見なされることも多い．ただし，本研究で対象とした Wi-Fi 認証手法では，FAR は 4 章での結果から FRR よりもはるかに低くなることがわかる．すなわち，これらの 2 つの値が同じ値をとるしきい値を設定することはできない．そこで，TAR のみを考慮した認証精度について本章で考察する．

図 4 は，100 ユーザーの平均 TAR を示したものであるので，ユーザーごとの 2 つの結果の違いを確認することはできない．そこでここでは，しきい値を 0.26 に設定した際の，5 分間隔と 1 時間間隔の違いを確認する．図 6 は，5 分間隔の TAR から各ユーザーの 1 時間間隔の TAR を引い

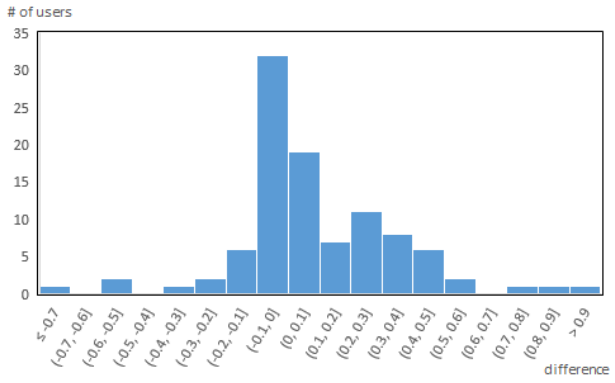


**図 6** Histogram of Differences of Two TARs

た差異のヒストグラムを示したものである．また表 1 は，差異に関する統計値を示したものである．

**表 1** Statistics of Differences of Two TARs

| Max | Min | Mean | Median | Mode | $\sigma$ |
|---|---|---|---|---|---|
| 0.933 | -0.733 | 0.098 | 0.033 | 0.000 | 0.254 |

表から，差の最大値は平均よりもはるかに高く，最小値は平均よりもはるかに低いことがわかる．平均値は 0 に近く，データ収集間隔の違いは Wi-Fi 認証方式の認証精度に影響を与えていないことがわかる．また，この図は平均から逸脱しているユーザーが少ないことも示している．表から中央値と最頻値は同じ範囲に入っていることもわかる．これらの結果から，データ収集間隔を 5 分から 1 時間に変更しても，ほとんどのユーザーの Wi-Fi 認証の精度に大きな影響はないと結論付けることができる．

## 6. おわりに

本稿では，スマートフォンセンサーを用いた認証方法で人間の行動を追跡する必要性について説明し，追跡間隔が短いと問題があることを指摘した．この問題を解決するために，既存研究で提案された間隔を 5 分から 1 時間に変更し，Wi-Fi 認証方式での認証精度への影響を調査した．その結果，データ収集間隔の長さは精度にほとんど影響を与えないことが判明した．

最後に，将来の課題について言及する．本論文では 5 分と 1 時間の違いのみを検討したが，ここで設定されたデータ収集間隔の長さが認証方法に最適であるということは言えない．今後は，実験に基づいて最適な間隔を検証していく必要がある．また，なりすましに対する脆弱性の変化を調べる必要や，データ収集間隔がバッテリー消費にどの程度影響するかを評価する必要がある．

## 参考文献

[1] Statista: Smartphone ownership rate by country 2018, https://www.statista.com/statistics/539395/smartphone-penetration-worldwide-by-country/.

[2] 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). IEEE, 2015. pp. 463–469.

[3] T. Feng, Z. Liu, K. A. Kwon, W. Shi, B. Carbunar, Y. Jiang and N. Nguyen, “Continuous Mobile Authentication using Touchscreen Gestures.” IEEE Conference on Technologies for Homeland Security (HST), pp.451–456, 13-15 Nov. 2012.

[4] Thanh Trung Ngo, Yasushi Makihara, Hajime Nagahara, Yasuhiro Mukaigawa and Yasushi Yagi, “The largest inertial sensor-based gait database and performance evaluation of gait-based personal authentication.” Pattern Recognization 47, pp.228–237, 2014.

[5] WIEFLING Stephan, IACONO Luigi Lo, DÜRMUTH Markus. “Is this really you? An empirical study on risk-based authentication applied in the wild.” In: IFIP International Conference on ICT Systems Security and Privacy Protection. Springer, Cham, 2019. p. 134-148.

[6] S. Elaine, N. Yuan, J. Markus and C. Richard, “Implicit authentication through learning user behavior.” International Conference on Information Security. Springer, 2010, pp.99–113,

[7] U. Mahbub and R. Chellappa, “PATH: Person authentication using trace histories.” 2016 IEEE 7th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON). IEEE, 2016, pp.1–8.

[8] S. Sieranoja, T. Kinnunen and P. Franti, “GPS trajectory biometrics: From where you were to how you move.” Joint IAPR International Workshops on Statistical Techniques in Pattern Recognition (SPR) and Structural and Syntactic Pattern Recognition (SSPR). Springer, 2016, pp.450–460.

[9] 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 11.2. IEEE, 2016, pp.513–521.

[10] Y. Ashibani and Q. H. Mahmoud, “A behavior profiling model for user authentication in IoT networks based on app usage patterns.” IECON 2018-44th Annual Conference of the IEEE Industrial Electronics Society. IEEE, 2018, pp.2841–2846.

[11] M. Sultana, P. P. Paul and M. L. Gavrilova, “User recognition from social behavior in computer-mediated social context.” IEEE Transactions on Human-Machine Systems 47.3. IEEE, 2017, pp.356–367.

[12] R. Kobayashi, H. Susuki, N. Saji and R. S. Yamaguchi “Lifestyle authentication and MITHRA project.” 2018 10th International Conference on Communication Systems & Networks (COMSNETS). IEEE, 2018. pp. 464–467.