平日休日の行動パターンの違いに着目した認証手法

大河 澪耶[1]　小林 良輔[1]　山口 利恵[1]

概要：近年のスマートフォンの普及により，個人認証の重要性は増してきている．その個人認証の種類として，知識情報，所持情報，生体情報を用いた認証の 3 つの従来手法が存在する中で近年，スマートフォンやウェアラブルデバイスに蓄積されている人の行動情報を用いた行動認証や，複数の行動情報を利用するライフスタイル認証が注目を集めている．ユーザの行動パターンを利用した行動認証においては，テンプレートに複数のライフスタイルの情報が混ざりこんでしまい，認証精度が低下してしまう．そのため複数のテンプレートを準備することが求められる．生体情報を用いた認証や意識的な行動の情報を用いた認証の研究においては複数のテンプレートが用いられている．一方，ユーザの行動パターンを表す認証要素の一つである Wi-Fi 情報を用いた認証の研究ではそのような研究は行われていない．本論文では，スマートフォンから収集された Wi-Fi 情報から平日と休日の 2 つのテンプレートを作成し認証を行うことで，テンプレートに複数のライフスタイルが混ざってしまい認証精度が低下してしまう問題を解決する最初の一歩の手法を提案する．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た．そして平日のデータを用いた認証の TAR の平均値が 0.926，休日のデータを用いた認証の TAR の平均値が 0.939 という結果を得た．結果をユーザ個別に見ていくと精度が改善したケースもある一方，そうではないケースも存在した．

A Behavioral Authentication Method Utilizing Tendency of the Days of the Week

REIYA OKAWA[1]　RYOSUKE KOBAYASHI[1]　RIE SHIGETOMI YAMAGUCHI[1]

1. はじめに

1.1 背景・目的

近年，スマートフォンの普及が進んでおり，日本においてはその普及率が 3 分の 2 を超えている [1]．スマートフォンの普及により，EC サイトなどの多くのオンラインサービスが利用されることとなった．このようなオンラインサービスにおいては，個人認証が必須となってくる．なぜなら，正当なユーザを正しく認証し，不正なユーザによるアクセスを正当なユーザから守らないと，甚大な被害が発生する可能性があるためである．

個人認証の種類として，ID とパスワードなどの知識情報を用いた認証 [2]，デジタル証明書など所持情報を用いた認証 [3]，虹彩や顔，指紋などの生体情報を用いた認証 [4] の 3 つの従来手法が存在する [5]．その中で近年，スマートフォンやウェアラブルデバイスに蓄積されている人の行動情報を用いた行動認証や，複数の行動情報を利用するライフスタイル認証 [6] が注目を集めている．

行動認証のメリットとしては，認証時にユーザに対して明示的な行動を求める必要がないことが挙げられる．なぜならユーザのデバイスが自動的にデータを収集するためである．また，すでに述べたようにスマートフォン等の普及などにより，人の行動情報が以前と比較して容易に取得し，それを用いた実験が行いやすくなったことも挙げられる．

行動認証の認証要素としては，歩容 [7] やスマートフォンのタッチ操作の情報 [8], [9]，キーストロークの情報 [10] や Wi-Fi 情報 [11] などが挙げられる．本論文ではこのうち，Wi-Fi 情報を用いた行動認証の研究に注目した．

ところで，人の行動情報を考えると，人は複数のライフスタイルを持っていることは容易に想像がつく．例えば 1 週間の中で大学のオンライン授業を家で受講する日もあれば休日に買い物に行くこともあるだろう．あるいは一時的

[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

な旅行でライフスタイルが変化することもあれば，1 週間の中で活動的な日とおとなしく家にいる日の両方があることもあるだろう．

一方，認証システムを考える際には 2 種類のデータを利用することとなる．まずテンプレートは事前にユーザの特徴を反映した情報を蓄積したものである．次に認証情報は，実際に認証する際にユーザの情報を収集したものである．この 2 種類のデータを比較することで認証スコアを算出する．

このように人は複数のライフスタイルを持っていることと認証システムのことの両方を考慮すると，テンプレートには複数のライフスタイルの情報が混ざりこんでしまい，認証精度が低下してしまうことがわかる．そのため複数のテンプレートを準備することが求められる．

生体情報を用いた認証やユーザの意識的な行動の情報を用いた認証の研究においては複数のテンプレートが用いられている．一方，Wi-Fi 情報を用いた認証の研究ではそのような研究は行われていない．

本論文では，スマートフォンから収集された Wi-Fi 情報から平日と休日の 2 つのテンプレートを作成し認証を行うことで，テンプレートに複数のライフスタイルが混ざってしまい認証精度が低下してしまう問題を解決する最初の一歩の手法を提案する．

1.2 本論文の構成

本論文の構成を以下に示す．2 章では Wi-Fi 情報を用いた認証の研究と複数のテンプレートを用いた認証の既存研究を示す．3 章ではスマートフォンから収集された Wi-Fi 情報から平日と休日の 2 つのテンプレートを作成し認証を行う手法について説明する．データセットや実験手順の説明，実験結果については 4 章で述べる．5 章では実験結果について，ユーザ全体と個別のそれぞれの観点から考察を行っていく．最後に結論と今後の展望を 6 章で述べる．

2. 関連研究

2.1 Wi-Fi データを用いた認証

Wi-Fi 情報を用いた研究としてまず Neal ら [12] らによるものがある．彼らはアプリケーション，Bluetooth，Wi-Fi の 3 種類のデータそれぞれ個別と全てを利用した計 4 種類の実験を行ったが，ここでは Wi-Fi 情報のみを用いた実験について説明する．ユーザごとに最も多く収集された Wi-Fi アドレス 10 個を要素とする 10 次元のベクトルを作成する．テンプレートと認証情報をこのような手法で作成すると次に比較を行い認証スコアを算出する．認証スコアは，テンプレートと認証情報それぞれのベクトルでアドレスが一致した割合を元に計算される．19 ヶ月間のデータを用いて，1 日のデータからテンプレートを，その次の日のデータから認証情報を作成しすでに述べた手法でスコアを算出，実験を行った結果，Neal らは 92.7%の平均精度を達成した．

Li ら [13] や Acien ら [14] によっても Wi-Fi 情報を用いた認証の研究が行われた．彼らは Neal らの Wi-Fi アドレスを利用した研究の手法に加えて時間帯という考えも利用した．Li らは認証情報（3 秒間のデータから作成される）と 3 種類のテンプレート（認証情報と同時間帯，1 個前の時間帯，1 個後の時間帯）をそれぞれ比較し，最も認証スコアが高いものを最終的なスコアとする手法を提案した．テンプレートの中で Wi-Fi アドレスが認証情報と一致するものを求め，それらの頻度の平方の和を計算することで認証スコアは求めることができる．ここで頻度とは，Wi-Fi アドレスがある時間帯で何日収集されたかを表す数字である．同時間帯だけでなくその前後の時間帯のテンプレートとも認証情報を比較しているのは時間のゆらぎを吸収するためである．加速度センサーの情報も合わせて 23 人のデータを利用して実験を行った結果，Li らは 9.19%の EER を達成した．一方 Acien らは，認証スコアの計算手法としては Li らと同様のものを採用した．しかしテンプレートとして認証情報と同時間帯のみのものを使用し，認証情報は以前にユーザがデバイスのロックを解除してから認証時までの情報を元に作成することとした．彼らは最大計 7 種類の情報（48 人のデータからなる）を利用して認証実験を行ったが，その中で Wi-Fi と加速度センサーの情報を利用した認証においては 29.2%の EER を達成した．

また，小林ら [11] は，テンプレートと認証情報を比較し，同じ Wi-Fi アドレスかつ同じ時間帯である行列の要素の数の割合を認証スコアとした認証実験を行った (図 1)．テンプレートは 30 日間のデータから作成され，一定時間での丸め，アドレスの選定，データ取得頻度の濃淡の追加，2 値化というデータ処理がなされる．一方認証情報は 1 日のデータから作成され，一定時間での丸めというデータ処理がなされる．このようなデータ処理を行うことで，テンプレートと認証情報それぞれが，行が {0h〜1h,1h〜2h,···,23h〜24h}，列が Wi-Fi アドレスである行列で表される（行列の要素の値は 0 か 1 となっている）．この行列を足し算し，要素の値が 1 か 2 のある中で 2 である割合を認証スコアとした．なお，行列の加算後の列である Wi-Fi アドレスはテンプレートの Wi-Fi アドレスとしている．そしてテンプレートは 30 日間のデータから，認証情報は 1 日のデータと 1 時間のデータの 2 種類から作成した．100 人のユーザのデータを用いて実験を行ったところ，TAR の平均が 93.2%（1 日のデータを元に認証情報を作成した場合）となった．

2.2 複数のテンプレートを用いた認証

Uludag ら [15] や Roy ら [16] は指紋情報を用いた研究を行った．彼らはセンサや環境状況，生体情報そのものの変化であったり，得られるデータサイズの小ささといった原

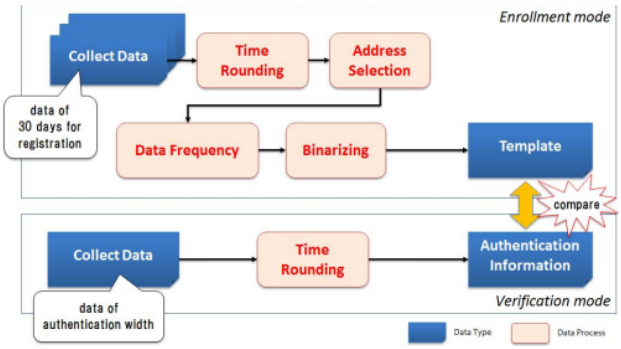

図 1 小林らによる Wi-Fi 情報のデータを処理する流れ [11]

因から複数のテンプレートを作成し，認証実験を行った．

Maiorana ら [10] は，スマートフォンのキー操作に着目した．あるキーが押されている時間や次のキーが押されるまでの時間などをユーザごとに複数回計測し，Uludag ら [15] で示された階層型クラスタリングの手法等を用いて複数テンプレートの作成を行った．

Kumar ら [9] は，スマートフォンの画面上のスワイプ動作の情報を用いた認証の研究を行った．スマートフォンのスワイプ動作を考えると，片手だけで画面全体をカバーすることができないことや，ユーザが使用するアプリケーションによってスワイプ動作に違いがあることがわかる．そこで彼らはタッチポイントの座標を用いて，スワイプ動作を画面の左半分で行われたものと右半分で行われたものに分割し，2 つのテンプレートをユーザごとに作成した．単一のテンプレートを用いた認証と結果を比較したところ，精度が向上した．

3. 提案手法

提案手法は，スマートフォンから収集された Wi-Fi 情報から平日と休日の 2 つのテンプレートをユーザごとに作成し認証を行うものである．ここでいう休日とは土日祝のことを指しており，ユーザごとにその活動の種類から平日と休日を定義しているわけでない．テンプレートは 1 ヶ月のデータから作成され，認証情報は 1 日分のデータから作成される (図 2)．各ユーザの平日と休日それぞれのテンプレートおよび認証情報の作成方法は Wi-Fi 情報を用いた既存研究を主に参考にした．

(1) テンプレート

- 一定時間での丸め
  既存研究 [11] と同じである．
- アドレスの選定
  既存研究 [17] と同じである．
- データ取得頻度の濃淡の追加
  既存研究 [11] と同じである．
- 2 値化
  既存研究 [11] と同じである．

(2) 認証情報

- 一定時間での丸め
  既存研究 [11] と同じである．

このようにして各ユーザの平日と休日それぞれのテンプレートおよび認証情報を作成した後は，比較を行い認証スコアを算出する．比較は平日同士，休日同士のデータを比較した．すなわち平日のテンプレートと比較するのは平日の認証情報であり，休日のテンプレートと比較するのは休日の認証情報ということである．認証スコアである一致率や閾値は既存研究 [11] と同様に算出した．

4. 実験

4.1 データセット

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実験を行った．過去 2 回に渡って実証実験を行ってきたが，今回使用するデータが収集された実証実験では，行動情報の収集と認証結果の通知を行う「MITHRA アプリ」と，スマートフォンの歩数管理アプリの「aruku &」とを連携させるものであった．本論文では MITHRA アプリが収集したデータのうち，Wi-Fi 情報に関するものを選択し利用した．Wi-Fi 情報は，理想的な場合で 5 分間隔で収集される．

今回使用するデータが収集された実証実験は 2021 年の 2 月 1 日から 2021 年 3 月 31 日の 2 ヶ月間行われ，計 3,088 人のユーザが参加した．実際に利用したデータはユーザ ID，時刻，Wi-Fi の BSSID である．そして実験期間全ての日（59 日間）の Wi-Fi 情報が存在するユーザが 205 人であった．本論文ではここから 100 人のデータをランダムに抽出し実験を行った．

4.2 実験手順

まず，テンプレートは各ユーザで平日休日それぞれで 2 月のデータを元に作成した．認証情報は各ユーザで平日休日それぞれで 3 月のデータを元に作成した．テンプレートおよび認証情報の作成手法は 3 章で示した通りである．

次にテンプレートと認証情報の比較について説明する．比較の方法は 2 つある．

- 本人認証
  あるユーザのテンプレートと，同じユーザの認証情報を比較する．
- 他人認証
  あるユーザのテンプレートと、別のユーザの認証情報を比較する．

比較の様子を図 3 に示す．

そして今回の実験ではユーザ 1 人あたり次の回数の比較

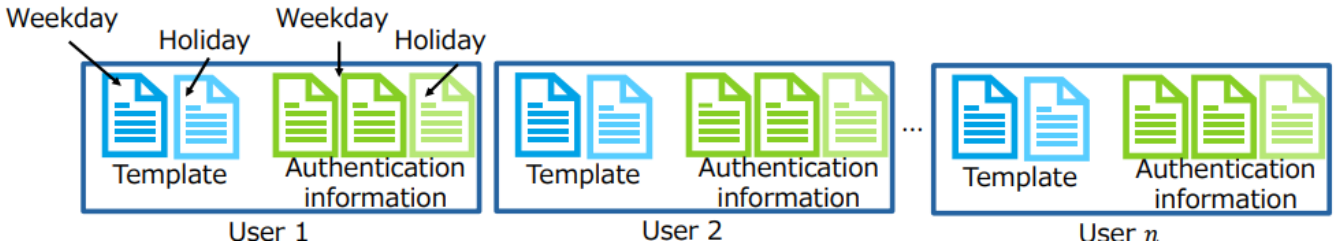

図 2 ユーザごとのテンプレートと認証情報

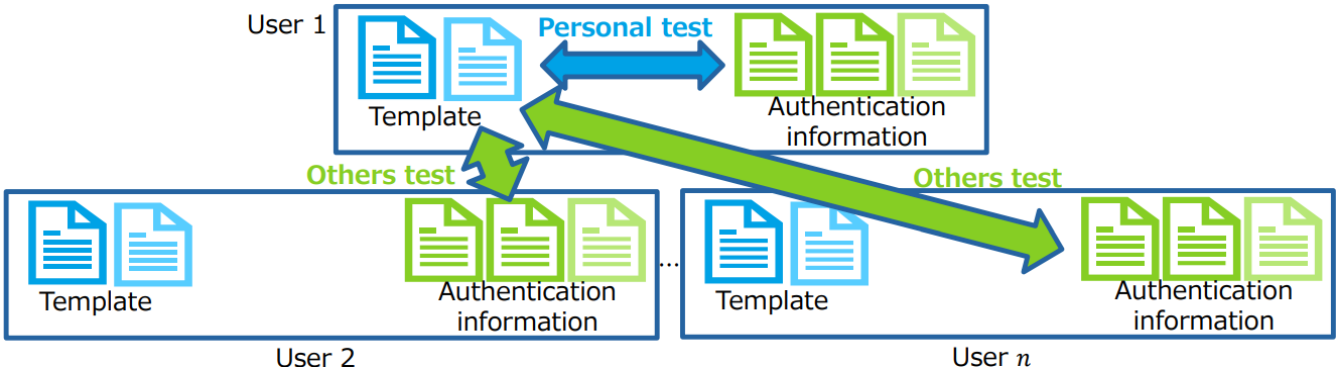

図 3 本人認証と他人認証

を行った．

- 本人認証（平日）：23 回（3 月の平日が 23 日あるため）
- 本人認証（休日）：8 回（3 月の休日が 8 日あるため）
- 他人認証（平日）：2,277 回（99 ×23 日）
- 他人認証（休日）：792 回（99 ×8 日）

また，閾値は 0.01 に設定し，これよりも認証スコアが高ければ認証成功，そうでなければ認証失敗とした．

最後に評価指標について説明する．本論文では本人受入率 (TAR) と他人受入率 (FAR) の 2 つで実験の評価を行った．定義は次の通りである．

- 本人受入率 (TAR)：認証成功回数 / 本人認証試行回数
- 他人受入率 (FAR)：認証成功回数 / 他人認証試行回数

4.3 実験結果

平日のデータを利用した実験の結果を図 4 に，休日のデータを利用した実験の結果を図 5 に示す．図では各ユーザの TAR と FAR を，TAR の昇順に並べている．FAR は TAR と比較してその値がはるかに小さいため，図中で識別することは難しい． また，各 TAR ごとのユーザの分布を，図 6（平日のデータを利用した実験）と図 7（休日のデータを利用した実験）に示す．多くのユーザの TAR は 1 に近いが，一部のユーザの TAR は極端に小さいことがわかる．

5. 考察

5.1 ユーザ全体

提案手法の有効性を確かめるために，データを平日と休日の 2 つに分割しない手法で本論文と同様の実験を行った．そして評価指標の平均値を，本論文の実験結果と比較したのが図 8 である．FAR の平均値はどれもほぼ 0 に近い．一方 TAR の平均値については，データを平日と休日の 2 つに分割しない手法が 0.950，平日のデータを利用した結果が 0.926，休日のデータを利用した結果が 0.939 となっており，この結果を見るとデータを分割しない方が精度が良いことになる．

5.2 ユーザ個別

5.2.1 評価指標の値がデータを分割する前と比較して改善したのかどうか

前節の結果を踏まえ，ユーザごとに個別に評価指標の値が改善したのかどうかを調査することにした．具体的には TAR と FAR それぞれにおいて，データを分割する前と比較して平日および休日の評価指標が改善したのかどうかを調べた．各ユーザの評価指標の値の変化を次に示す 4 つに分類した．

グループ A　平日と休日の評価指標のうち，片方は改善しもう片方は改悪した場合

グループ B　平日と休日ともに評価指標の値が変化しなかった場合

グループ C　上記以外の場合で，平日と休日の少なくとも一方の評価指標が改善した場合

グループ D　上記以外の場合で，平日と休日の少なくとも一方の評価指標が改悪した場合

上記 4 つの分類と平日休日それぞれで評価指標の値が改

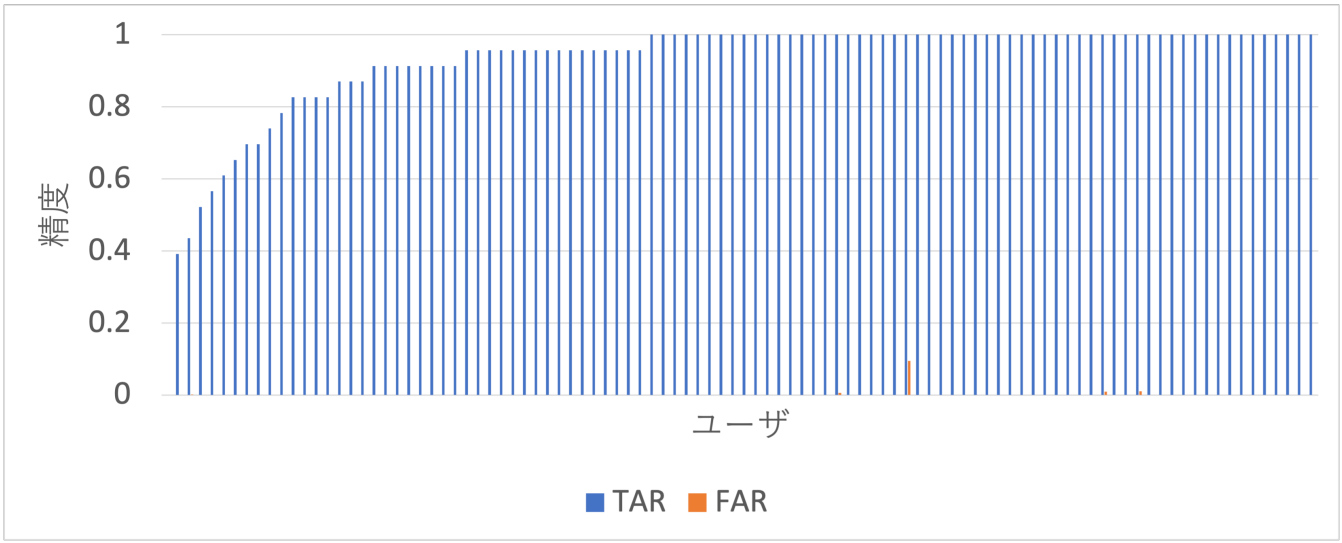

図 4 平日のデータを用いたユーザごとの実験結果

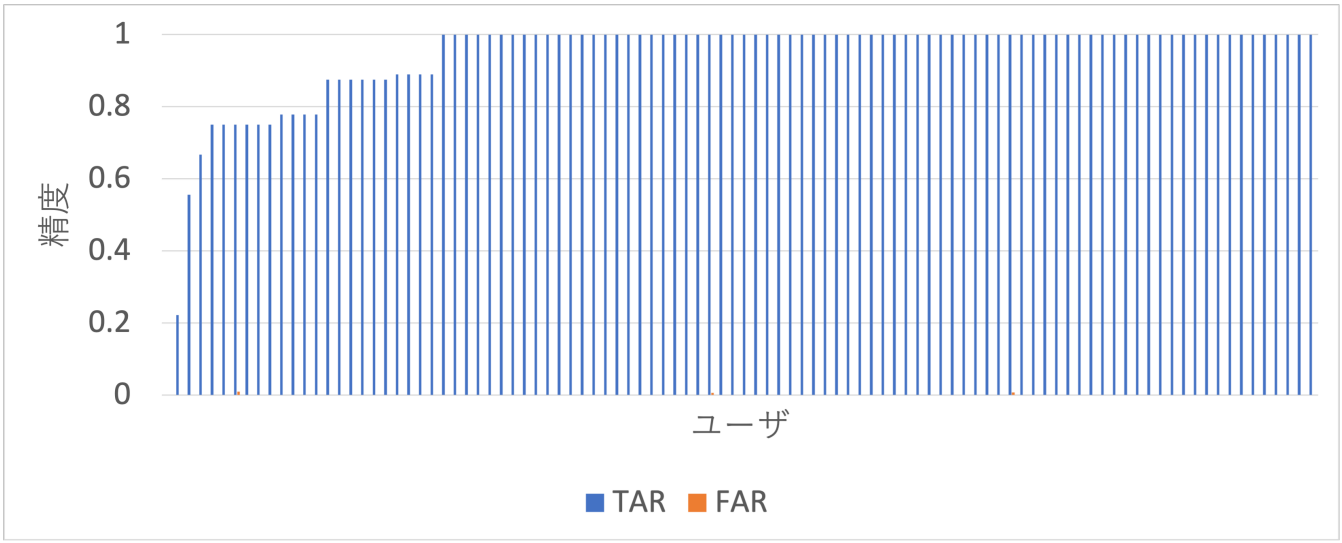

図 5 休日のデータを用いたユーザごとの実験結果

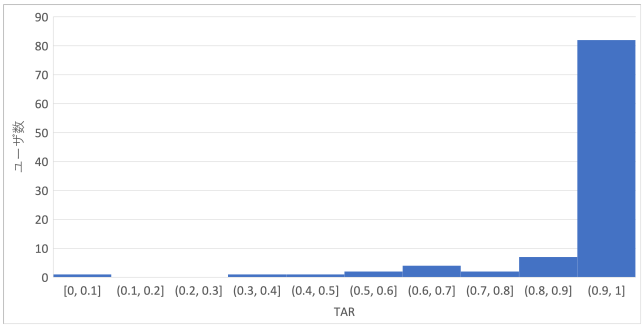

図 6 各 TAR ごとのユーザの分布（平日のデータを利用した実験）

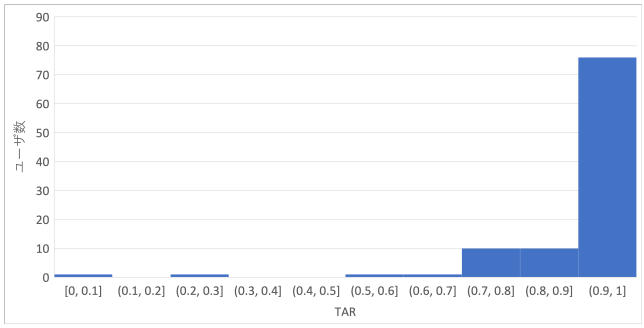

図 7 各 TAR ごとのユーザの分布（休日のデータを利用した実験）

善したかどうかとの関係性は表 1 に示す通りである．そして分類結果は図 9 に示す通りになった．図からわかるように，何人かのユーザの評価指標の値が改善した一方，平日休日共に改悪したユーザも存在する．また，データを分割しない場合から平日のデータを利用した場合の TAR の変化量をユーザ個別で昇順にして見たものが図 10 であり，データを分割しない場合から休日のデータを利用した場合の TAR の変化量をユーザ個別で昇順にして見たものが図 11 である．このような結果から，平日と休日の評価指標が共に改悪したユーザのデータは平日と休日に分割しない方が良いかもしれないことがわかる．例えばこれらのユーザは新型コロナウイルス蔓延の影響で 1 週間ほぼずっ

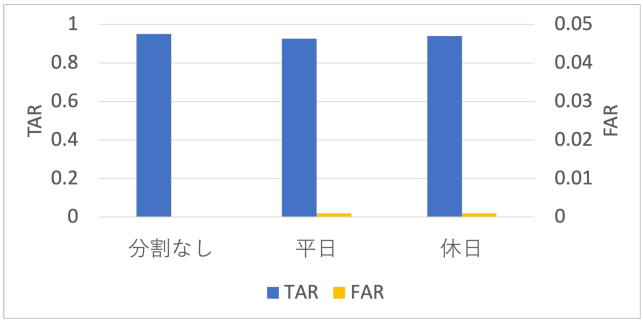

図 8　評価指標の平均値の比較結果

表 1　評価指標が改善したかどうかの分類の定義

		平日		
		改善	変化なし	改悪
休日	改善	C	C	A
	変化なし	C	B	D
	改悪	A	D	D

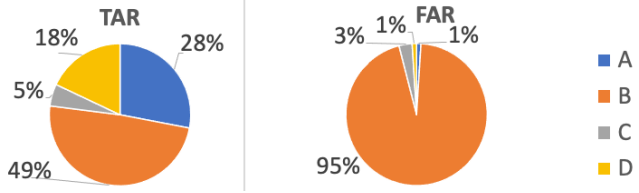

図 9　評価指標が改善したかどうかの分類結果

と家にいたなどが原因として考えられる（本実験で用いたデータが一部地域で，新型コロナウイルス蔓延拡大防止から発令された緊急事態宣言の期間に収集されたものである）．あるいは，これらのユーザの土日が休日でないとすればデータ分割の方法を変更する必要がある．さらにあるいは，1 週間の中で 3 つ以上のライフスタイルのパターンが存在するユーザである可能性もあり，その場合はそれに応じてより多くの数のデータ分割を正しく行う必要があると思われる．

5.2.2　比較結果を表す行列の要素の割合

また，今回の論文の手法では既存研究に倣って，テンプレートと認証情報はそれぞれ行列で表した．（その要素は 0 または 1 である．）それぞれの要素には，1 日の中で 1 時間単位で Wi-Fi アドレスを収集すれば 1 を，収集しなければ 0 を設定する．テンプレートについては 2 月それぞれの日の行列を加算し 2 値化することで比較結果に対応する行列の要素が 0 または 1 であるテンプレートと認証情報が作成される．2 章で述べたように，この 2 つのデータに対応する行列を加算し，要素が 2 である割合を認証スコアとするのである．すなわち要素が 2 であることは，テンプレートと認証情報で Wi-Fi アドレスおよび時間帯が一致したことを意味している．そのため比較結果の行列の中で 2 の要素の割合が高いと，テンプレートがユーザの特徴をより正確に捉えていると言える．

そこでユーザごとに比較結果の行列の中で 0, 1, 2 の要素がそれぞれどの程度存在するのかを調査した．平日のデータを利用した場合の結果が図 12 であり，休日のデータを利用した場合の結果が図 13 である．各ユーザの 3 種類の要素それぞれの割合は複数の比較結果の行列の平均値である．（各ユーザの比較結果の行列は，認証情報が作成される 3 月の日数分存在する．）またユーザの並び順は，図 10 や図 11 と同様に，データを分割しない場合から平日（休日）のデータを利用した場合の TAR の変化量が昇順になるように並び替えている．図 10〜図 13 からわかるように 2 の割合が大きいユーザの TAR 変化量は 0 に近く，TAR 変化量が 0 に近いユーザの TAR はデータを分割する前から元々高い．以上のことから元々テンプレートがユーザの特徴をよく表しているユーザの TAR は，データを平日と休日に分割したとしても大きく下がることはないことがわかる．

6.　結論・今後の展望

本論文では，行動認証の認証システムにおいて，テンプレートの中で複数のライフスタイルのデータが混ざってしまうことで認証精度が低下する問題があることを挙げた．またその解決案として複数のテンプレート作成があり，生体情報を用いた認証やユーザの意識的な行動の情報を用いた認証の研究ではそのような複数テンプレートの作成が行われていることを説明した．一方，ユーザの行動パターンを表す認証要素の一つである Wi-Fi 情報を利用した認証の研究においては，複数のテンプレート作成が行われていないことも述べた．

こうした背景を元に本論文では，スマートフォンから収集された Wi-Fi 情報から平日と休日の 2 つのテンプレートを作成し認証を行うことで，テンプレートに複数のライフスタイルが混ざってしまい認証精度が低下してしまう問題を解決する最初の一歩の手法を提案した．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，平日のデータを用いた認証の TAR の平均値が 0.926，休日のデータを用いた認証の TAR の平均値が 0.939 という結果を得た．結果をユーザ個別に見ていくと精度が改善したケースもある一方，そうではないケースも存在した．

今後の課題として，まずユーザごとに複数のライフスタイルを持っているため，ユーザごとに最適なテンプレートの分割を自動で行うことが挙げられる．ユーザによっては複数テンプレートを作成する必要がないこともある一方，同じデータ分割の数でもユーザごとに違う分け方をする必要があり，そうすることでより認証精度の向上に貢献できると考えられる．さらに，複数テンプレートを作成した後，認証を継続していくことを考えると，複数のテンプレートの更新という課題も見えてくる．この 2 つの課題に対して対処することで，より認証精度の高い継続して利用できる

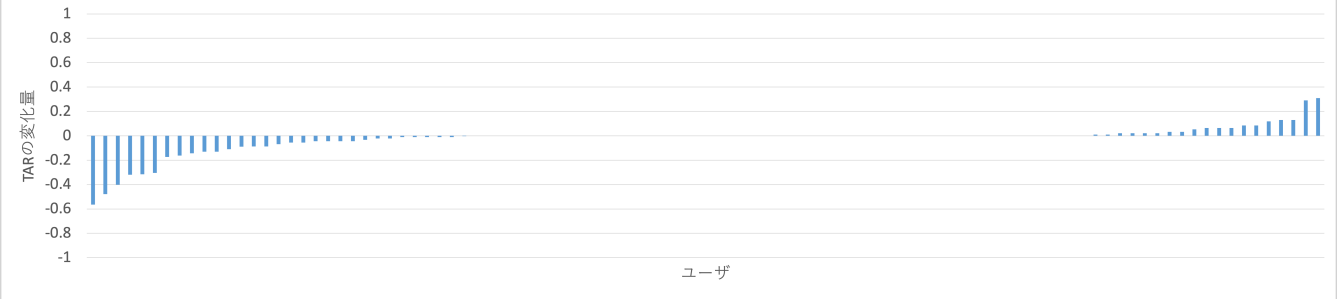

図 10 各ユーザの評価指標の改善度合い（平日のデータ）

図 11 各ユーザの評価指標の改善度合い（休日のデータ）

行動認証システムが実現できると考えられる．

参考文献

[1] 総務省：令和 3 年版情報通信白書（PDF 版），総務省（オンライン），入手先 ⟨https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r03/pdf/01honpen.pdf⟩（参照 2022-05-10）.

[2] Sprager, S. and Juric, M. B.: Inertial Sensor-Based Gait Recognition: A Review, *Sensors*, Vol. 15, No. 9, pp. 22089–22127 (2015).

[3] Ramadan, M., Du, G., and C. Xu, F. L.：A Survey of Public Key Infrastructure-Based Security for Mobile Communication Systems, *Symmetry*, Vol. 8, No. 9, p. 85 (2016).

[4] Aravinth, J. and Valarmathy, S.: Multi classifier-based score level fusion of multimodal biometric recognition and its application to remote biometrics authentication, *The Imaging Science Journal*, Vol. 64, No. 1, pp. 1–14 (2016).

[5] Delac, K. and Grgic, M.: A survey of biometric recognition methods, *46th International SyrnPoSium Electronics in Marine*, pp. 184–193 (2004).

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

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

[8] Feng, T., Liu, Z., Kwon, K., Shi, W. L., Carbunar, B., Jiang, Y. and Nguyen, N.: Continuous mobile authentication using touchscreen gestures, *2012 IEEE Conference on Technologies for Homeland Security (HST)*, pp. 451–455 (2012).

[9] Kumar, R., Phoha, V. V. and Serwadda, A.: Continuous authentication of smartphone users by fusing typing, swiping, and phone movement patterns, *2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, pp. 1–8 (2016).

[10] Maiorana, E., Campisi, P., González-Carballo, N. and Neri, A.: Keystroke dynamics authentication for mobile phones, *2011 ACM Symposium on applied computing (SAC)*, pp. 21–26 (2011).

[11] Kobayashi, R. and Yamaguchi, R. S.: Behavioral Authentication Method Utilizing Wi-Fi History Information Captured by IoT Device, *2017 International Workshop on Secure Internet of Things (SIoT)*, pp. 20–29 (2017).

[12] Neal, T. J., Woodard, D. L. and Striegel, A. D.: Mobile Device Application, Bluetooth, and Wi-Fi Usage Data as Behavioral Biometric Traits, *2015 IEEE 7th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, pp. 1–6 (2015).

[13] Li, G. and Bours, P.: Studying WiFi and Accelerometer Data Based Authentication Method on Mobile Phones (ICBEA), *2018 2nd International Conference on biometric engineering and applications*, pp. 18–23 (2018).

[14] Acien, A., Morales, A., Vera-Rodriguez, R., Fierrez, J. and Tolosana, R.: MultiLock: Mobile Active Authentication Based on Multiple Biometric and Behavioral Patterns, *1st International Workshop on Multimodal Understanding and Learning for Embodied Applications (MULEA)*, pp. 53–59 (2019).

[15] Uludaga, U., Rossb, A. and Jain, A.: Biometric template selection and update: a case study in fingerprints, *Pattern recognition*, Vol. 37, No. 7, pp. 1533–1542 (2004).

[16] Roy, A., Memon, N. and Ross, A.: MasterPrint: Exploring the Vulnerability of Partial Fingerprint-Based Authentication Systems, *IEEE Transactions on Information Forensics and Security*, Vol. 12, No. 9, pp. 2013–2025 (2017).

[17] 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.

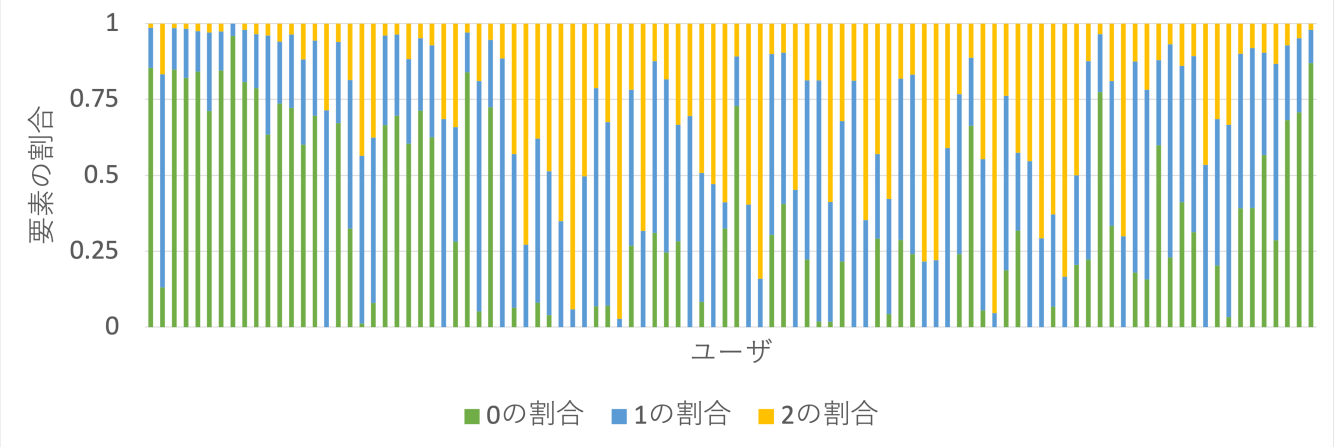

図 12 各ユーザの比較結果に対応する行列の中での各要素の割合（平日のデータ）

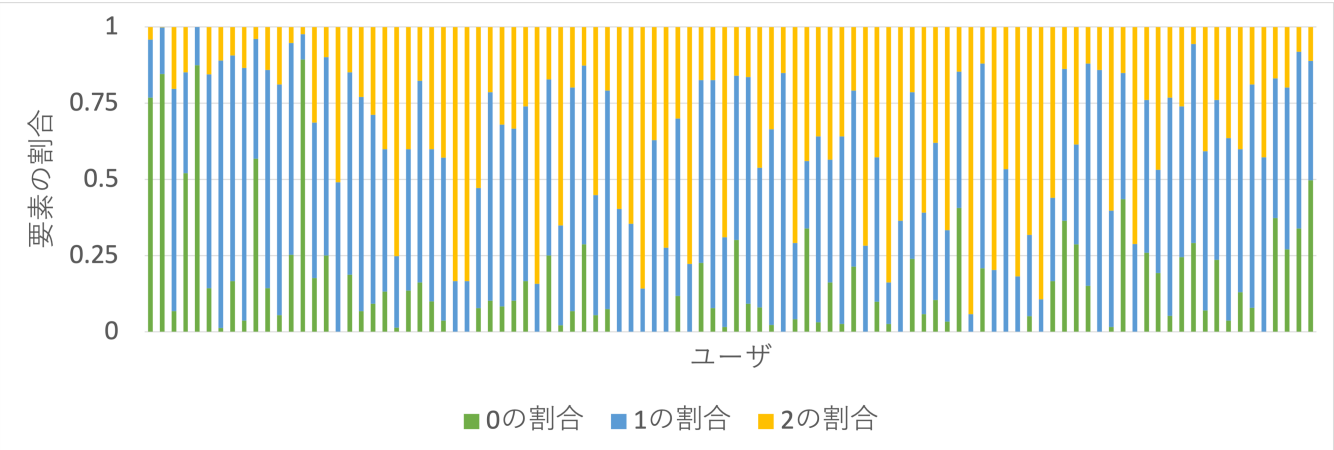

図 13 各ユーザの比較結果に対応する行列の中での各要素の割合（休日のデータ）

463–469 (2015).