

移動・Wi-Fi履歴情報から見る個人ごとの生活習慣類似性評価

小林 良輔¹ 山口 利恵²

Evaluation of Personal Lifestyle Habits Similarity Using Location and Wi-Fi History Information

RYOSUKE KOBAYASHI¹ RIE Shigetomi YAMAGUCHI²

1. はじめに

モバイル端末は爆発的な普及を見せており、商業や軍事・医療など特定の分野にとどまらず、スマートフォンやタブレットなどは一般的な個人も利用するようになっている。さらに近年ではこれらのモバイル端末はインターネットに接続する通信機能が搭載されており、IoT (Internet of Things) 時代と呼ばれている。一般ユーザーはモバイル端末を通して非対面ながら、SNS 等を利用したユーザー同士のコミュニケーションやECサイトを利用した買い物などが可能となる。このようにスマートフォンなどのモバイル端末は我々の日々の生活に欠かせないものとなってきている。

モバイル端末を利用する上で必要となってくるのが、個人認証技術である。ユーザーはインターネットを通してモバイル端末から様々なサービスを利用できるようになった。一方でユーザーは非対面でサービスを利用しているため、サービスプロバイダーはサービスを利用しているユーザーが正当なユーザーであることを確認する必要がある。サービス利用者が正当ユーザーではなく悪意を持った者になりすましていた場合、正当なユーザーが例えばクレジット不正利用などの被害を被ったり、サービスプロバイダーもシステム攻撃などの被害を被る可能性がでてくる。そのためモバイル端末の利用など、現在では個人認証技術は非常に重要な仕組みであると考えられている。

個人認証技術の一つとしてパスワードを利用した認証手法があり、現在もっとも多く利用されている認証手法である。しかしながら多くのサービスで個人認証技術が必要と

されるため、ユーザーは利用するサービスの数だけパスワードを管理しなければならない。多くのパスワードを管理することはユーザーに多大な負担がかかるが、サービスの数はさらに増えていっており、ユーザーは自分のパスワードを管理できない状況となっている。Yahoo! JAPANでは1日あたり15,000件程度もパスワード忘れによるパスワード再設定の依頼があり [1]、ユーザーはパスワードを記憶できていない。パスワードといったユーザーの記憶に頼る認証手法の代わりに、指紋などといった生体情報を活用する認証手法も利用されている。生体認証手法はユーザーの記憶に頼る必要がなく、また何も所持する必要がないためユーザー負担が少ない認証手法として期待されている。しかしながら生体認証手法は、生体情報がプライバシー情報でオンラインで利用されることの抵抗や、不変であることから万一漏洩してしまった場合になりすましを防ぐことが困難であるといった課題も指摘されている。

こういった現在利用されている個人認証手法の課題を解決するために、近年では人の行動情報を活用した認証手法が提案されている。特に、歩行 [2] や腕振り [3] といった単純な行動ではなく、生活習慣における行動情報を活用したライフスタイル認証 [4] が期待されている。近年のモバイル端末には様々な種類のセンサーが搭載されており、端末を所持するユーザーの行動は自動的に収集することが可能である。

本研究ではスマートフォンが収集する位置とWi-Fiの履歴情報を活用して、人の日々の生活における行動習慣の類似性を評価することを目的とし、今後の個人認証への適用への助けとなることを目指す。

1.1 論文の構成

本論文の構成は次のようになっている。2章では行動情

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

² 東京大学大学院情報理工学系研究科

報を活用した認証手法に関する関連研究について紹介する。3章では、本研究で利用した位置情報・Wi-Fi情報、および人の行動の特徴について説明する。4章では位置情報とWi-Fi情報を活用した生活パターンの類似性算出手法について提示する。5章では、本研究で行った実験及びその結果について説明し、結果から得られる知見に対して考察する。6章では、本研究で算出する類似性を個人認証に適用することを見据え、攻撃モデルを想定し、攻撃に対する耐性について検証を行う。最後に7章では本論文の結論の今後の課題について記述する。

2. 関連研究

人の生活習慣における行動情報を活用した個人認証に関する研究は、近年いくつか見ることができている。本研究でも活用した、スマートフォンで収集することのできる位置情報 [5] や Wi-Fi 情報 [6] を用いた認証手法などが提案されている。スマートフォンで収集できる情報以外でも、ウェアラブル端末の加速度センサーで収集される運動情報 [7] や、SNS (Social Networking Service) への投稿内容 [8] を活用した個人認証手法なども提案されている。これらの行動情報を活用した認証手法は、人は常に同じ行動をとるとは限らないという理由により、生体認証など既存に利用されている技術と比較すると、認証精度が低い傾向にある。

この問題を解決するために、単に1つの要素で認証を行うのではなく、複数の行動情報を組み合わせる手法も提案されている [9][10]。生体認証などでも複数の要素を組み合わせる手法は提案されており、大きく3つのタイプ、結果組み合わせ手法、スコア組み合わせ手法、特徴量組み合わせ手法が提案されている。しかしながら行動情報を活用した認証手法では、組み合わせ手法として、結果組み合わせ手法のみが利用されており、スコア組み合わせ手法や特徴量組み合わせ手法は既存研究では利用されていない。そこで本研究では行動情報を活用した認証手法でスコアの組み合わせ手法を採用することができるように、位置情報とWi-Fi情報を利用して行動習慣の類似性の数値化を行う。

3. 準備

本研究で実施した生活習慣の類似性評価について述べるに前もって、本章では本研究で利用した位置情報・Wi-Fi情報、および人の行動の特徴について説明する。

3.1 位置情報とWi-Fi情報

本節では位置情報とWi-Fi情報について、およびこれらの表記方法について説明する。

3.1.1 位置情報

ユーザー u がある時刻 t にある場所 l に滞在していると想定する。 u にとっては t が決まると l も一意に決定される。この l を位置情報といい、 $L_u(t) = l$ と表す。

3.1.2 Wi-Fi履歴情報

ユーザー u がある時刻 t に、 u の周辺に無線LANアクセスポイント w が設置されていることを想定する。この無線LANアクセスポイントの情報のことを本論分ではWi-Fi情報という。一般的に u の周辺に設置されている無線LANアクセスポイントの数は1つとは限らない。ある時刻 t に u の周辺に無線LANアクセスポイント w_1, w_2, \dots が設置されているとすると、Wi-Fi情報は $W_u(t) = \mathbf{w} = \{w_1, w_2, \dots\}$ と表される。スマートフォン等の電波センサーが取得するWi-Fi情報には、無線LANアクセスポイントのSSID (Service Set Identifier) やBSSID (Basic Service Set Identifier)、電波強度などが含まれているが、本研究ではそのうちBSSIDのみを利用する。そのため本紙ではWi-Fi情報というと単に無線LANアクセスポイントのBSSIDを指すものとする。

3.2 人の行動の特徴

大橋 [11] によると人の生活行動は1日単位での周期性のあるリズム行動である。人は一般的に日中の活動と夜間の睡眠の2層を基本とする活動形態をとっており、その行動はパターン化されたものとなる。本研究の試みはこの1日単位でパターン化された行動を、位置情報とWi-Fi情報を利用して評価することにある。

このように人の行動はパターン化されるものであるが、しかしながら毎日同じ時間に同じ行動をするということではない。人の行動にはゆらぎがあり、日々パターン化された似た行動をとっていたとしても、時間のずれなどが起きているのである。そのため生活行動の情報をパターン化するためには、このゆらぎを吸収するための処理が必要となる。ゆらぎ吸収処理については4章にて説明する。

4. 類似性評価手法

日々の行動情報の類似性を評価する方法として、その人の本人らしさを表した情報であるテンプレートを作成し、テンプレートと日々の情報を比較することで類似性を算出する。本章では位置情報とWi-Fi情報を活用した類似性評価手法について説明する。

4.1 ゆらぎ吸収処理

3.2節で述べた通り、人の行動にはゆらぎがふくまれており、毎日まったく同じ行動をとるとは限らない。ゆらぎを含んだ情報で日々の行動の類似性を評価しても、その類似性にずれが生じる恐れがある。そのため類似性評価をするためには、センサー等で収集された行動情報に対してゆらぎを吸収するような処理を行う必要がある。類似性評価手法を説明する前に、本節ではこのゆらぎ吸収処理について記述する。

本研究で活用する情報は位置情報、Wi-Fi情報、および

それらの情報を収集した時間情報である。行動のゆらぎを吸収するための処理もこの3種類の情報に対して行い、以下で説明する。

- 時間情報のゆらぎ

例えば出勤のために毎日同じ電車に乗るケースを想定する。同じ電車に乗ったとしても電車が遅延すると乗る時間は同じになるとは限らない。これが時間のゆらぎである。このようなゆらぎを受け入れるためには、多少時間がずれている情報でも同じ情報だとみなす必要がある。本研究では1時間ごとに位置情報とWi-Fi情報を丸める処理を施すことによって時間のゆらぎ吸収を試みる。すなわち $t = (d, time)$ (d : 日, $time$: 時以下) として, d を固定, n 時 $\leq time < (n+1)$ 時 ($n = 0, 1, \dots, 23$) において, $L_u(d, time)$ および $W_u(d, time)$ を一定とする。

- 位置情報のゆらぎ

時間情報と同様, 位置情報についても同じ生活パターンで行動していたとしてもゆらぎが存在する。すなわち同じ時間にまったく同じ位置にいるとは限らず, ずれた位置に滞在する可能性が高いと考えられる。この位置情報のゆらぎを受け入れるためには, 滞在位置が多少ずれていたとしても同じ情報だとみなせばよいこととなる。本研究では位置情報のゆらぎを無視するために, 位置を表現する道具としてメッシュコードを採用する。メッシュとは, 緯度経度に基づいて地域をほぼ同じ大きさの網目に分割したものであり [13], このメッシュを識別するためのコードをメッシュコードと呼ぶ。メッシュにはその大きさにより種類が分けられているが, 本研究では一辺が約 1km の基準地域メッシュを採用した。ある時間 n 時 $\leq time < (n+1)$ 時において, 最も長い時間滞在したメッシュを l としたとき, $L_u(d, time) = l$ (n 時 $\leq time < (n+1)$ 時) とする。

- Wi-Fi 情報のゆらぎ

スマートフォンセンサーが収集する Wi-Fi 情報の中には, たまたま街中ですれ違った人が持っていたモバイル無線 LAN アクセスポイントのアドレスなども含まれている。このような情報は, 別の日に再度まったく同じ行動をとったとしても, 収集されるとは限らない。つまり同じ生活パターンの中でも収集される Wi-Fi 情報にはずれが出てくるのである。これが Wi-Fi 情報のゆらぎである。このゆらぎを吸収するために, 本研究では検出回数の少ない Wi-Fi 情報は切り捨て, 検出回数が多い順に最大 5 つの Wi-Fi 情報のみを選定する。すなわち, ある時間 n 時 $\leq time < (n+1)$ 時において, 検出回数の多い 5 つの Wi-Fi 情報が w_1, w_2, \dots, w_5 としたとき, $W_u(d, time) = \{w_1, w_2, \dots, w_5\}$ (n 時 $\leq time < (n+1)$ 時) とする。

INPUT:DB 行動情報

d : テンプレート作成期間

$L_u(d, h)$: u の d 日 h 時における位置情報

$W_u(d, h)$: u の d 日 h 時における Wi-Fi 情報

OUTPUT: $T_u^{location}(h), T_u^{wifi}(h)$ テンプレート

```
(1)  $T_u^{location}(h) = \{\}, T_u^{wifi}(h) = \{\}$ 
(2)  $c_{location} = 0, c_{wifi} = 0$ 
(3) for  $d$  in  $d$ 
(4) if  $L_u(d, h)$  in  $T_u^{location}(h)$  then
(5)    $T_u^{location}(h)[L_u(d, h)] += 1$ 
(6) else
(7)    $T_u^{location}(h)[L_u(d, h)] = 1$ 
(8)  $c_{location} += 1$ 
(9) for  $w$  in  $W_u(d, h)$ 
(10) if  $w$  in  $T_u^{wifi}(h)$  then
(11)    $T_u^{wifi}(h)[w] += 1$ 
(12) else
(13)    $T_u^{wifi}(h)[w] = 1$ 
(14)  $c_{wifi} += 1$ 
(15) for  $t_{location}$  in  $T_u^{location}(h)$ 
(16)  $T_u^{location}(h)[t_{location}] = T_u^{location}(h)[t_{location}] / c_{location}$ 
(17) for  $t_{wifi}$  in  $T_u^{wifi}(h)$ 
(18)  $T_u^{wifi}(h)[t_{wifi}] = T_u^{wifi}(h)[t_{wifi}] / c_{wifi}$ 
(19) return  $T_u^{location}(h), T_u^{wifi}(h)$ 
```

図 1 テンプレート作成アルゴリズム

以上のゆらぎ吸収処理により, 位置情報および Wi-Fi 情報は以下のように表現できる。

$$L_u(d, h) = l_{d,h}$$

$$W_u(d, h) = w_{d,h}, |w_{d,h}| \leq 5$$

$$h = 0, 1, 2, \dots, 23$$

4.2 テンプレート

テンプレートはその人の本人らしさを表した情報であり, テンプレート作成期間に収集された行動情報を元にあらかじめ作成する。テンプレートも行動情報から作成されるものであるから, 前節で説明したゆらぎ吸収処理を施す必要がある。また, テンプレート作成期間の行動から, とりうる行動に対して重みを付与する必要もある。例えば毎朝同じ時間に出勤するとしても, 会社に出勤するケースや取引先に直接出勤するケースなどが考えられる。週に一度取引先に直接出勤し残りは会社に出勤するすると, この 2 つのケースを同じ確度で考えると本人らしさを表した情報とはならない。そこで取りうる行動に対して重みを付与するのである。すなわちユーザー u のテンプレート $T_u^{location}(h), T_u^{wifi}(h)$ は図 1 のアルゴリズムで得ることができる。

INPUT:DB 行動情報

- $L_u(d, h)$: u の d 日 h 時における位置情報
- $W_u(d, h)$: u の d 日 h 時における Wi-Fi 情報
- $T_u^{location}(h)$: u の h 時における位置テンプレート
- $T_u^{wifi}(h)$: u の h 時における Wi-Fi テンプレート

OUTPUT : $S_u^{location}(d, h)$, $S_u^{wifi}(d, h)$ 類似性

- (1) $S_u^{location}(d, h) = 0$, $S_u^{wifi}(d, h) = 0$
- (2) if $L_u(d, h)$ in $T_u^{location}(h)$ then
- (3) $S_u^{location}(d, h) = T_u^{location}(h)[L_u(d, h)]$
- (4) for w in $W_u(d, h)$
- (5) if w in $T_u^{wifi}(h)$ then
- (6) $S_u^{wifi}(d, h) += T_u^{wifi}(h)[w]$
- (7) return $S_u^{location}(d, h)$, $S_u^{wifi}(d, h)$

図 2 類似性算出アルゴリズム

4.3 類似性スコア算出

4.1 節で説明したゆらぎ吸収処理を施した行動情報と、4.2 節で作成されるテンプレートを比較することでその行動情報の類似性の値を算出する。この算出された値を本論文では類似性スコアと呼ぶこととする。ユーザー u の d 日 h 時における類似性スコアを $S_u^{location}(d, h)$, $S_u^{wifi}(d, h)$ とすると、この値は図 2 のアルゴリズムで算出される。このようにして算出される類似性スコアは式の通り 1 時間ごとの値であり、ゆらぎ吸収処理で行動情報を 1 時間ごとに丸めた結果である。

5. 実験

本研究では 4 章で説明した手法に従って実験を行った。本章では本実験で利用したデータセットの説明および、実験結果について記述する。

5.1 データセット

本実験では、東京大学大学院情報理工学系研究科ソーシャル ICT 研究センター次世代個人認証講座が 2017 年 1 月～4 月に実施した大規模実証実験 MITHRA プロジェクト [12] で収集したデータを利用した。MITHRA プロジェクトでは合計で約 57,000 人のデータを収集し、その中で位置情報と Wi-Fi 情報は 16,027 人から収集された。このデータから以下の条件を満たす実験協力者をランダムに 100 人選定し、本実験のデータとして利用した。

- Android 利用者
- 60 日以上プロジェクトに参加

選定された 100 人のデータのうち、最初の 60 日間のデータを本実験で利用した。60 日間のうち最初の 30 日間をテ

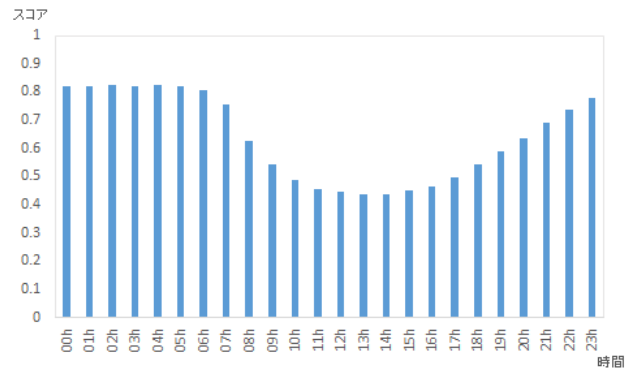


図 3 1 時間ごとの類似性スコア (位置)

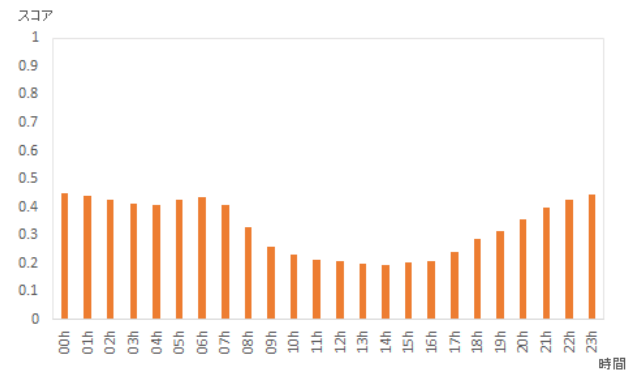


図 4 1 時間ごとの類似性スコア (Wi-Fi)

ンプレート作成期間、残りの 30 日間をテンプレートと比較するテスト期間のデータとして設定した。

5.2 実験結果

本実験では後半 30 日間をテスト期間として実験を行い、以下の評価を行った。本節では実験結果および結果からの考察について説明する。

5.2.1 1 時間ごとの類似性

図 3 と 4 は、1 時間ごとの類似性スコアを表している。スコアはテスト期間 30 日および全 100 人の平均値を表している。位置、Wi-Fi とも昼間はスコアが低く、夜間はスコアが高くなっている。これは 3.2 節で記述した通り、一般的に人は昼間に活動し、夜間に睡眠をとることが理由と考えられる。睡眠は自宅とすることが通常でパターンが変化することは少ない一方で、活動には会社、取引先に行くなど複数のパターンがあることがある。そのため昼間のスコアの方が低くなっていると考えられる。表 1 は時間によ

表 1 1 時間ごとの類似性スコア

| | 最大値 (時間) | 最小値 (時間) |
|-------|-------------|-------------|
| 位置 | 0.824 (03h) | 0.437 (14h) |
| Wi-Fi | 0.448 (00h) | 0.193 (14h) |

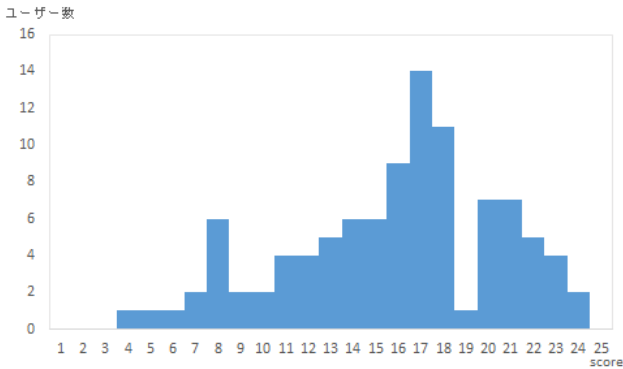


図 5 1日ごとの類似性スコア (位置)

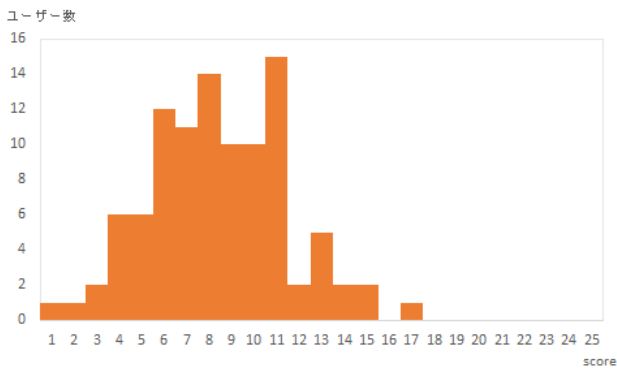


図 6 1日ごとの類似性スコア (Wi-Fi)

る最大値, 最小値, およびその値をとる時間を表している. この表から人は 14 時頃に最も活動していると考えることができる.

5.2.2 1日ごとの類似性

本研究は日々の生活パターンの類似性を位置情報と Wi-Fi 情報を利用して評価することが目的である. そのため 1 時間ごとに算出した類似性スコアを 1 日分 (24 時間分) 加えた値について評価を行った. 図 5, 6 はテスト期間 30 日間の結果の平均値とユーザー数のヒストグラムを表したものである. 位置と Wi-Fi の結果を比較すると, 全体的に位置の方がスコアが大きいことがわかる. また表 2 は位置と Wi-Fi それぞれの最大値, 平均値, 最小値, および他人の行動情報と比較した時の類似性スコアの最大値である. 他人の行動情報と比較して類似性スコアを算出することにより, ある人の生活パターンが他人と異なっているかどうかを確認することができる. 表 2 を見ると, 位置については他人と比較した最大値が本人どうしの最小値よりも低い結果となっており, 生活パターンが他人と異なっていることが表現されている. 一方で Wi-Fi は他人と比較した最大値の方が大きい結果となっている. これは Wi-Fi 情報 (BSSID) は一般に端末固有の情報であるが, 一部の端末では同じ ID が設定されているものも存在する. そのため異なる生活パターンでも, Wi-Fi では同じ情報として表現されていると考えられる.

表 2 1日ごとの類似性スコア

| | 最大値 | 平均値 | 最小値 | 最大値 (他人) |
|-------|------|------|------|----------|
| 位置 | 23.6 | 15.3 | 3.42 | 1.75 |
| Wi-Fi | 16.3 | 7.90 | 0.60 | 2.34 |

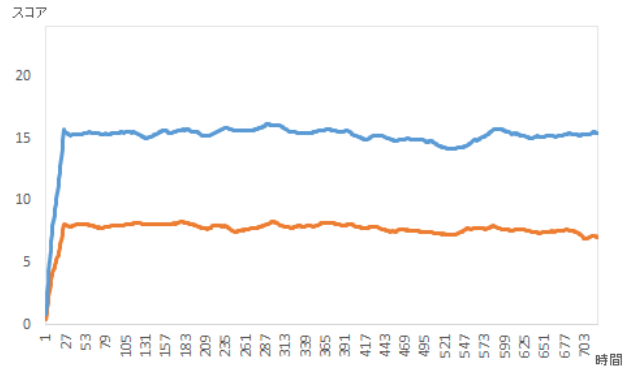


図 7 24 時間の類似性スコアの変化

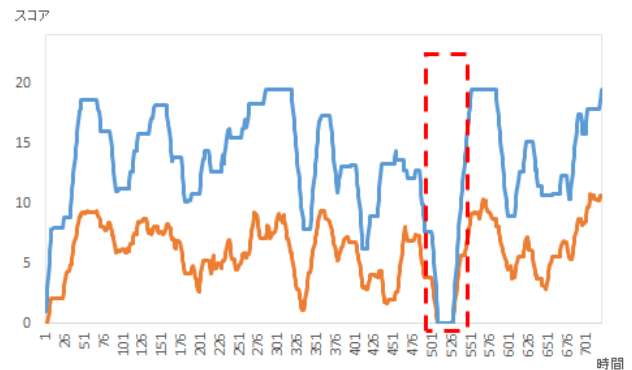


図 8 あるユーザーの 24 時間の類似性スコアの変化

5.2.3 直近 24 時間の類似性スコアの変化

5.2.2 節では 1 日ごとの 24 時間分のスコアについて見たが, 本節では 24 時間分のスコアの, 時間ごとの変化について検証する. 図 7 は 100 ユーザーの平均値を表したものであり, 上の線が位置を, 下の線が Wi-Fi を表している. どちらも最初の 24 時間はスコアが上昇していくが, その後は大きな変化がないことがわかる. これは平均的には人の生活パターンは大きく変わらないということを指し示していると考えられる. 図 8 はあるユーザーのスコアの変化である. 図 7 のように平均的にはスコアに大きな変化がなくても, ユーザーごとに見ると変化していることが見てとれる. 点線枠内のようにスコアが極端に低くなるころでは, 旅行などのように通常の生活パターンではない行動をしたと予想することができる.

6. 個人認証への適用

本研究で算出された類似性スコアは, 1 章で述べた通り

個人認証への適用を目指すものである。位置情報や Wi-Fi 情報から抽出することができる生活パターンから本人の類似性を見出すことが可能なことは 5 章で述べた通りであるが、個人認証に活用する上では攻撃に対する耐性についても考察しておく必要がある。本章では普段使用しているスマートフォンが他人に盗まれ、その他人が通常の行動を続けたケースを想定して直近 24 時間分の類似性スコアがどのように変化していくかを検証する。

6.1 検証データセット

検証には 5.1 節と同じデータを利用する。このデータのうち、異なる 2 人がテスト期間中に同じ場所 (メッシュ) に滞在したケースは 170 ケース存在し、全ケースについて検証を行った。

6.2 検証方法

ユーザー u_1, u_2 が同じ場所 l に滞在するケースを考える。 u_2 が l に滞在した時間のスコアは u_1 が l に滞在した時間から直近 24 時間の u_1 のテンプレートと u_1 の行動情報とを比較して算出したスコアとする。それ以降は 1 時間ごとに u_1 のテンプレートと u_2 の行動情報とを比較して算出したスコアを加え、24 時間前のスコアを減算して直近 24 時間分のスコアとする。

6.3 検証結果

図 9, 10 は全 170 ケースの平均値を表した検証結果である。横軸の時間が 0 の時に u_2 が l に滞在したことを意味しており、その後はスコアが減少していく様子を見ることができる。グラフ内の縦棒はスコアが表 2 の最小値となる時間を示しており、吹き出しはその時間を過ぎた最小の時間と、その際のスコアを表している。縦棒の位置のスコアを閾値と設定として個人認証に適用すると、平均的には本人は正しく本人と認められる。また本攻撃モデルを考えた時は、スマートフォンを盗まれた後、位置情報で 15 時間後、Wi-Fi 情報で 19 時間後に盗まれたことに気づくことができる。

7. おわりに

本論文では人の生活パターンの類似性を、スマートフォンで収集した位置情報と Wi-Fi 情報を利用して数値化して評価を行った。その結果、ともに類似性を表現できる情報であることを検証した。また本論文で実施した類似性算出手法では、Wi-Fi 情報よりも位置情報の方が高くなること



図 9 攻撃モデルの類似性スコアの変化 (位置)



図 10 攻撃モデルの類似性スコアの変化 (Wi-Fi)

が確認できた。算出された類似性スコアが個人認証に適用されることを踏まえ、スマートフォンが盗まれたケースを想定し、類似性スコアが減少していく様子の検証も行った。

今後は本実験で算出した類似性スコアを組み合わせることにより個人認証への適用を目指し、またさらに、スコアの組み合わせだけでなくそれぞれのデータの特徴量を組み合わせることによりよい認証手法の構築を目指す。

参考文献

- [1] マイナビニュース: Yahoo! JAPAN、パスワード入力が不要のログイン方法を導入, 入手先 <http://news.mynavi.jp/news/2017/04/20/220/> (参照 2017-04-20).
- [2] Mohammad O. Derawi, Claudia Nickel, Patrick Bours, Christoph Busch: Unobtrusive User-Authentication on Mobile Phones using Biometric Gait Recognition, 2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2010 IEEE, pp.306-311
- [3] 松尾 賢治, 奥村 文教, 橋本 真幸, 小池 淳, 久保田 彰, 羽鳥 好律: 腕の振りに基づく生体認証とテンプレート更新による経時変化の抑制, 電子情報通信学会論文誌 B, Vol.J91-B No.6, pp.695-705 (2008).
- [4] Ryosuke Kobayashi, Hiroya Susuki, Nobuyuki Saji, Rie Shigetomi Yamaguchi: Lifestyle authentication and MITHRA project, 10th International Conference on Communication Systems & Networks (COMSNETS), pp. 464-467 (2018).
- [5] Yujin Tang, Nakazato Hidenori, and Yoshiyori Urano:

- User authentication on smart phones using a data mining method, Information Society (i-Society), 2010 International Conference on. IEEE, 2010.
- [6] Ryosuke Kobayashi and Rie Shigetomi Yamaguchi: One hour term authentication for Wi-Fi information captured by smartphone sensors, Information Theory and Its Applications (ISITA), 2016 International Symposium on. IEEE, 2016.
 - [7] Susuki Hiroya and Rie Shigetomi Yamaguchi: Cost-Effective Modeling for Authentication and Its Application to Activity Tracker, International Workshop on Information Security Applications. Springer, Cham, 2015.
 - [8] Madeena Sultana, Padma Polash Paul and Marina L. Gavrilova: User Recognition From Social Behavior in Computer-Mediated Social Context, IEEE Transactions on Human-Machine Systems 47.3 (2017): 356-367.
 - [9] Lex Fridman, Steven Weber, Rachel Greenstadt, Moshe Kam: Active Authentication on Mobile Devices via Stylometry, Application Usage, Web Browsing, and GPS Location, IEEE Systems Journal, arXiv:1503.08479v1 [cs.CR] 29 Mar 2015
 - [10] A. Fridman, A. Stolerman, S. Acharya, P. Brennan, P. Juola, R. Greenstadt, M. Kam: Multi-modal decision fusion for continuous authentication, Computers and Electrical Engineering, p. Accepted, 2014
 - [11] 大橋 久美子: 看護における「生活リズム」: 概念分析, 聖路加看護学会誌, Vol.14 No.2, August 2010.
 - [12] 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, pp.223-230 (2017).
 - [13] 総務省: 地域メッシュ統計の特質・変革, 入手先 (<http://www.stat.go.jp/data/mesh/pdf/gaiyo1.pdf>) (参照 2017-08-28).