Computer Security Symposium 2022
24 - 27 October 2022

スマートフォンで収集した位置，Wi-Fi情報，およびそれらの相関を活用した個人認証手法のなりすまし耐性

小林 良輔[1,2,a)]　山口 利恵[2]

概要：近年，人の行動情報を活用した個人認証手法について多く研究がなされている．人の行動情報はその個人の特性を表すことが知られており，顔や指紋と同様，個人認証に活用される．特に人の滞在場所や移動履歴を表す位置情報は，個人の特性を強く表し，行動認証の中では高い精度で認証することが可能である．一方で位置情報は他人が容易に推測できる情報であり，その推測した情報を用いてなりすましに活用される恐れがある．そこで本研究ではスマートフォンが収集する位置情報に加え，Wi-Fi 情報および位置と Wi-Fi の相関情報を個人認証手法に活用することで，なりすまし耐性を向上させること目指す．

キーワード：行動認証, ライフスタイル認証, スマートフォン, 相関認証

Resistance to Spoofing of User Authentication Methods Using Location and Wi-Fi Information Collected by Smartphones and Their Correlation

Ryosuke Kobayashi[1,2,a)]　Rie Shigetomi Yamaguchi[2]

Abstract: There are a lot of studies on user authentication methods utilizing human behavior. Since it is believed that human behavior expresses his/her characteristic, the information is applied for user authentication techniques such as fingerprints or face. In particular, location information, which represents a person's location and movement history, strongly expresses personal characteristics and can be used for highly accurate authentication in behavioral authentication. On the other hand, location information can be easily guessed by others, and the guessed information can be used for spoofing. Therefore, in addition to location information collected by smartphones, this research aims to improve the resistance to impersonation by utilizing Wi-Fi information and the correlation between location and Wi-Fi information in user authentication methods.

Keywords: behavioral authentication, lifestyle authentication, smartphone, correlation authentication

1. はじめに

従来の個人認証手法は所持情報，知識情報，生体情報を活用して実現されており，これらの情報は認証の 3 要素と呼ばれている [1]．その中で近年では行動情報を活用した認証手法，行動認証が提案されており，行動認証は第 4 の認証手法と呼ばれることもある [2]．行動認証が持つ特徴のうち，他の 3 つの認証手法と比較したときに最も異なる一つはユーザーが意識せずに情報を入力し認証されるという点である．IoT (Internet of Things) 技術の発展により，人の行動情報は容易にかつ自動的に収集できるようになった．例えば今や多くの人が持つスマートフォンには多数のセンサーが搭載されており，スマートフォンを持ち歩いているだけで所有者の行動情報を自動的に収集することが可能だ．このように収集される行動情報を活用することで，

[1] 三菱電機インフォメーションシステムズ株式会社
MITSUBISHI ELECTRIC INFORMATION SYSTEMS CORPORATION
[2] 東京大学
The University of Tokyo
[a)] kobayashi@yamagula.ic.i.u-toyo.ac.jp

ユーザーが意識しない個人認証手法を実現することができる．

ユーザーが意識せずに認証されることによる利点が 2 つ挙げられる．ひとつはユーザーの負担が増えない多要素認証の実現である．近年の様々なサービスでは多要素認証を要求されることが多い．複数の要素を用いて認証する多要素認証では，ひとつの要素を用いる場合と比較して高い安全性が期待される．ひとつの要素ではその認証情報を盗まれてしまうと容易になりすましが可能となるが，多要素を利用をするとひとつの認証情報を盗まれてもなりすまされる可能性は低いからである．一方で認証要素を増やすことは，認証情報を複数回入力する必要があるため一般的にユーザーの負担を増加させることとなる．しかし行動認証であればユーザーは意識的に認証情報を入力する必要がないため，多要素認証に組み込むことでユーザーへの負担を変化させずに安全性を高めることができるというわけだ．もうひとつの利点は継続的認証 [3] に活用できるということだ．継続的認証とは，サービスログイン時の認証だけでなく，サービス利用中も継続的に認証する手法である．モバイル端末が増加するにつれ，現在ではサービス利用中の端末を他人に盗まれる可能性も増加している．ログイン時の認証のみではサービス利用中に利用者が替わることをシステムは検知できないが，継続的認証を実現することで検知することができるということだ．しかしながらサービス利用中に何度も認証情報の入力を要求されると，利用者の負担は非常に大きくなるだろう．行動認証を活用することで，利用者の負担を増加させない継続的認証を実現できるわけだ．

行動情報が個人認証に活用されるということは，この情報は顔や指紋といった生体情報と同様にその人の特徴を表した情報であると言える．特に位置情報はその特性が強く，認証に活用した時に行動認証の中では高い精度を得ることができる [4]．位置情報はスマートフォンなどのに搭載されている GPS を用いることで収集することができ，その履歴情報を分析することでその人の自宅や勤務先を推定することが可能となる [5]．これらの分析結果が人の特徴を強く表すということである．

位置情報は人の特徴を強く表す情報である一方で，他人に読み取られやすい情報でもあるといえる．位置情報は指紋や顔と同様に物理的に表面に出ている情報であり，他人に知られたり推測されたりする情報である．例えば目の前に存在している人のその時間位置情報は当然知ることができる．またある人の勤務している会社の情報がわかれば，日中はそのオフィスに滞在しているだろうと推測することも可能である．このように位置情報は他人に読み取られやすく，個人認証に活用するとなると認証情報を推測されやすいということになる．すなわち，位置情報を活用した認証手法は，他人によるなりすましが容易に行われる恐れがあるということだ．

位置情報を活用した認証手法で，なりすましの恐れを低減させるために，Wi-Fi 情報との相関関係を利用した既存研究 [6] がある．Wi-Fi 情報も位置情報と同様，スマートフォンのセンサーで自動的に収集できる情報であり，位置情報と組み合わせて利用することは容易である．この手法では位置情報のみを推測されたとしても，Wi-Fi 情報は容易には推測されないという仮定の下でなりすましの耐性を上げる手法である．一方で認証精度の観点では，位置情報のみを活用した認証手法の方が精度が高いという問題もある．そこで本論文では，なりすましの耐性を高めたまま認証精度も低減させないため，位置情報を活用した認証手法，Wi-Fi 情報を活用した認証手法，位置情報と Wi-Fi 情報の相関関係を利用した認証手法それぞれを組み合わせた手法を提案する．

1.1 本書の構成

本書の構成は以下の通りである．2 章では本研究における提案手法について説明する．3 章では本研究における実験について，使用したデータセット，実験シナリオ，および実験の結果について記述する．最後に 4 章では本書のまとめとして結論し，今後の課題について説明する．

2. 提案手法

本研究における提案手法の概要を図 1 に記す．本手法ではスマートフォンから収集される位置情報と Wi-Fi 情報を活用する．位置情報からは，位置情報を活用した認証手法を利用しスコアを算出し，Wi-Fi 情報からは Wi-Fi 情報を活用した認証手法を利用しスコアを算出する．また位置情報と Wi-Fi 情報から，これらの相関関係を活用した認証手法を利用しスコアを算出する．これら 3 種類のスコアを組み合わせて最終的なスコアを算出し，認証判定を行う．本章では，これら 3 種類のスコア算出方法と，スコアの組み合わせ方式について説明する．

2.1 位置・Wi-Fi 情報を活用した認証手法

位置情報を活用した認証手法におけるスコア算出と，Wi-Fi 情報を活用した認証手法におけるスコア算出手法については，小林らの手法 [7] を用いる．本節ではその手法について説明する．

2.1.1 位置情報と Wi-Fi 情報の記法

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．

また，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

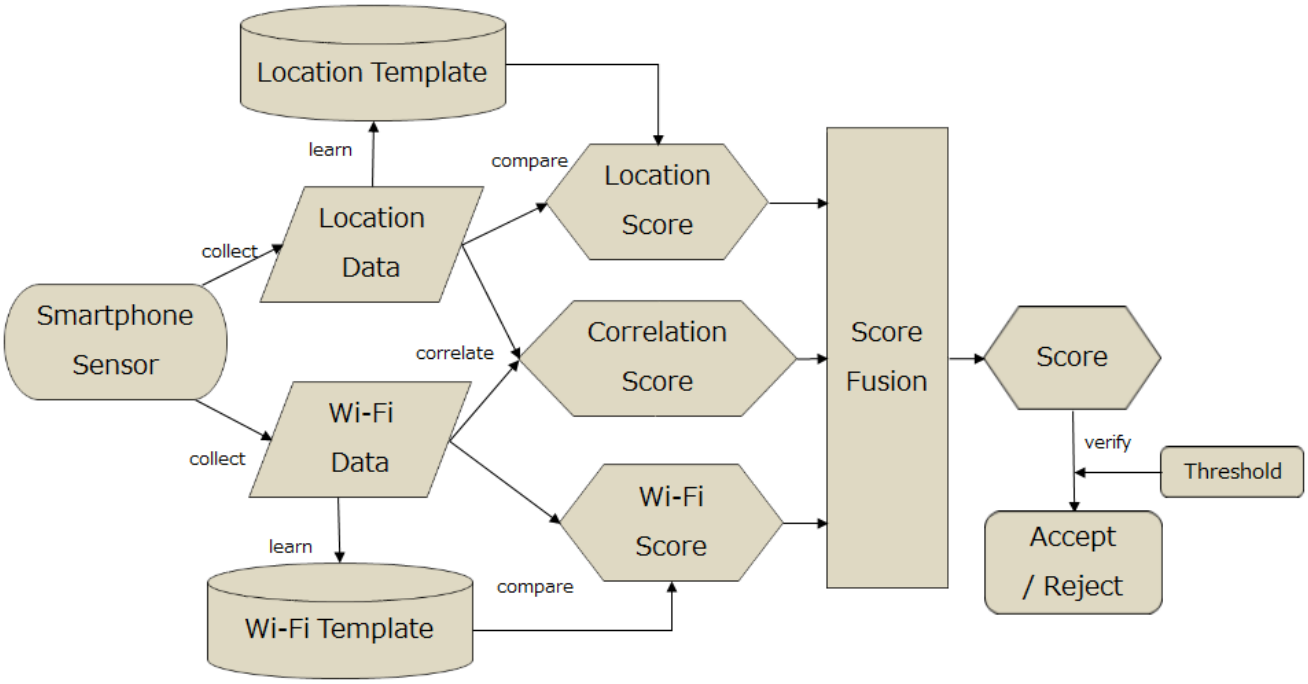


図 1: 位置, Wi-Fi, 相関を活用した行動認証手法概要

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 $w_1, w_2, \cdots$ が設置されているとすると，Wi-Fi 情報は $W_u(t) = \boldsymbol{w} = \{w_1, w_2, \cdots\}$ 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 Indentifier)，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．

2.1.2 前処理

大橋 [8] 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．ただし人は周期的に生活行動をするといっても，毎日同じ時間に同じ行動をするということではなく，同じ行動をとるにしてもいつもと時間がずれたり，またその日だけの行動をとるということもある．このようなずれを行動のゆらぎといい，行動情報を認証に活用するためにはこの行動のゆらぎを吸収する処理を行わなければならない．本節ではゆらぎを吸収するための位置情報，Wi-Fi 情報における前処理について説明する．ゆらぎ吸収処理には時間のゆらぎ，位置のゆらぎ，Wi-Fi のゆらぎの 3 つがあり以下それぞれについて説明する．

- 時間のゆらぎ
  これが時間のゆらぎである．時間のゆらぎを吸収するためには，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 $(n = 0, 1, \cdots, 23)$ において，$L_u(d, time)$ および $W_u(d, time)$ を一定とする..
- 位置のゆらぎ
  位置情報のゆらぎを吸収するためには，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 quadkey[9] を採用し，位置情報を地点ではなくある程度の広さを持つエリアとして考慮する．位置のゆらぎを吸収するために，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エリアを l としたとき，$L_u(d, time) = l$ (n 時 $\leq time < (n+1)$ 時) と表現することとする．
- Wi-Fi のゆらぎ
  Wi-Fi 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 $w_1, w_2, \cdots, w_5$ としたとき，$W_u(d, time) = \{ w_1, w_2, \cdots, w_5\}$ (n 時 $\leq time < (n+1)$ 時) とする．

2.1.3 テンプレート

一般的な (従来の) 認証手法は主に登録フェーズと検証フェーズからなる．登録フェーズでは人の本人らしさを表した情報を事前に登録する．この情報のことを一般的にテンプレートと呼ぶ．検証フェーズでは事前に登録されたテンプレートと認証情報を比較することで，認証判定を行う．本節では登録フェーズに登録されるテンプレートにお

INPUT:DB 行動情報
　$\boldsymbol{d}$: 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 $\boldsymbol{d}$
(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 2: テンプレート作成アルゴリズム

ける，その作成アルゴリズムについて記述する．

ユーザー u の位置，および Wi-Fi のテンプレートをそれぞれ $T_u^{location}(h),\ T_u^{wifi}(h)$ としたとき，これらの情報は図 2 で得ることができる．

2.1.4　スコア算出

認証時の行動情報と前節で作成されるテンプレートを比較することで，認証におけるスコアを算出することができる．本節ではそのスコア算出方式について記述する．

ユーザー u の d 日 h 時におけるスコアを $S_u^{location}(d,h),\ S_u^{wifi}(d,h)$ とすると，この値は図 3 のアルゴリズムで算出される．

2.2　位置と Wi-Fi の相関関係を活用した認証手法

位置と Wi-Fi の相関関係を活用した認証手法におけるスコア算出手法については，Miyazawa らの手法 [6] を用いる．本節ではその手法について説明する．

Miyazawa らの手法における位置と Wi-Fi の相関とは，位置情報における変化と Wi-Fi 情報における変化のことである．つまりスマートフォンの位置が変化していると，周辺の Wi-Fi 機器も変化しているという仮定の元に，その関係を定量的にスコアで表し認証に活用している．

2.2.1　位置と Wi-Fi の変化

ユーザー u がある時刻 t_1 から別の時刻 $t_2 (t_1 < t_2)$ の間

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 : $S_u^{location}(d,h),\ S_u^{wifi}(d,h)$ スコア
(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 3: スコア算出アルゴリズム

に移動した距離を，

$$d = |L_u(t_2) - L_u(t_1)|$$

と表す．このとき，移動速度 v は，

$$v = \frac{d}{t_2 - t_1}$$

と表すことができる．本手法では人が歩行している時を対象としており，$5 \leq v[m/min] \leq 300$ のデータを対象としている．

またある時刻 t におけるユーザー u の周辺に設置されたアクセスポイントの数を $|W_u(t)|$ とし，その中で特に u が所持するスマートフォンに接続されたアクセスポイントを c_bssid_t とすると，時刻 t_1 から t_2 における Wi-Fi の変化は，

$$\frac{|W_u(t_2) \cap W_u(t_1)|}{|W_u(t_1)|}$$

の値と，$c\_bssid_{t_1}$ と $c\_bssid_{t_2}$ の差異によって表される．

2.2.2　スコア算出

前節で設定した位置情報の変化と Wi-Fi 情報の変化から，共に変化している場合は高いスコアを，一方のみが変化している場合は低いスコアを本手法では与えている．すなわちある時刻 t におけるスコア $s_u(t)$ を以下の通り定義する．ここで T は設定された閾値である．

$$s_u(t) = \begin{cases} 1 & if\ \frac{|W_u(t_2) \cap W_u(t_1)|}{|W_u(t_1)|} < T \\ 1 & if\ c\_bssid_t \neq c\_bssid_{t'} \\ -1 & if\ c\_bssid_t = c\_bssid_{t'}\ (\neq \phi) \\ 0 & otherwise \end{cases}$$

この値を利用し，ある日 d におけるスコア $S_u^{corr}(d)$ を，

$$S_u^{corr}(d) = \frac{\Sigma_{t \in d} s_u(t)}{|t|}$$

と定義する．

2.3 組み合わせ方式

本研究ではこれまでに算出した 3 種類のスコアの平均値を取ることで最終的なスコアとした．なお，$0 \leq S_u^{location}(d),\ S_u^{wifi}(d) \leq 1$ であるのに対し，$-1 \leq S_u^{corr}(d) \leq 1$ であるため，相関関係のスコアについては正規化を行なってから平均値をとった．すなわち最終的なスコアを $S_u(d)$ とすると，

$$S_u(d) = \frac{S_u^{location}(d) + S_u^{wifi}(d) + \frac{S_u^{corr}(d)+1}{2}}{3}$$

と表される．

3. 実験

本章では本研究で実施した実験について説明する．

3.1 データセット

本実験では，東京大学が 2021 年に実施した実証実験 [10] で得られたデータセットを使用した．この実証実験は東京大学情報理工学研究科倫理審査委員会の審査のもとで実施されている．実証実験の概要については以下の通りである．なお，詳細については [10] を参照されたい．

- 実施時期
  2021 年 2 月 1 日〜3 月 31 日
- 参加者数
  3088 人
- 収集データ
  位置情報，Wi-Fi 情報

このデータセットの中から本実験では，Android 利用者かつ 50 日以上データが収集された 85 人のデータを使用した．

3.2 実験シナリオ

本研究では位置情報を他人に推定されたケースを想定した行動認証のなりすまし耐性を検証することを目的としている．その上で以下の実験を実施した．

- 単要素での認証実験
  位置情報，Wi-Fi 情報，相関関係それぞれひとつの要素のみを活用した認証手法において，認証精度の検証を行う．
- 組み合わせの認証実験
  位置情報，Wi-Fi 情報，相関関係の 3 つの認証手法から 2 つを組み合わせる認証，および 3 つすべてを組み合わせる認証を実施して認証精度の検証を行う．なお組み合わせ方式は 2.3 節に記載の通り平均スコアを算出して行う．

本節ではこれらの実験シナリオについて詳細を説明する．

3.2.1 単要素での認証実験

位置情報と Wi-Fi 情報を活用した認証手法の実験では，テンプレート作成期間を設定する必要がある．そこで本実験では，d 日における認証実験のテンプレート作成期間を 1〜(d-1) 日までとした ($2 \leq d \leq$ (実験参加日数))．例えば 60 日間のデータを収集したユーザーの場合，2 日目のデータに対する認証実験については 1 日目のデータのみでテンプレートを作成し，60 日目のデータに対する認証実験については 1〜59 日目の 59 日間のデータでテンプレートを作成した．

また本実験は位置情報が推定されたケースにおけるなりすまし耐性を評価することが目的だが，位置情報を活用した認証手法においては位置情報を推定されるとそのまま認証情報となるため本実験では位置推定を適用せず，また Wi-Fi 情報を活用した認証手法においても位置情報を推定されることに対する影響がないため，こちらも本実験では適用しない．位置推定を適用するのは相関関係を活用した認証手法のみとなる．すなわち他人からのなりすましにおける実験は，推定された位置情報と自分の Wi-Fi 情報で行うこととする．この元で，本人の認証情報における認証可否と他人の認証情報における認証可否とを算出する実験を行った．

3.2.2 組み合わせの認証実験

組み合わせについては 2 種類のスコアの組み合わせを 3 通り，および 3 種類のスコアの組み合わせを 1 通りの計 4 通りの実験を実施した．それぞれのスコアについては単要素での認証実験で算出されたものを使用した．

3.3 評価指標

本実験での評価指標には FRR(False Rejection Rate: 本人拒否率) と FAR(False Acceptance Rate: 他人受入率) を使用した．本実験では FRR は本人の認証情報で手法の精度を評価する指標であり，FAR は他人からのなりすまし耐性を評価する指標である．FRR が低いほど認証精度が高い手法であるといえ，また FAR が低いほど位置情報を推定された場合のなりすまし耐性が高い手法だということができる．

ある閾値 k のもとで，2 章で算出したスコア S が $S \geq k$ を満たすときに認証成功，$S \leq k$ の時に認証失敗とすると，FRR,FAR は以下で定義される．

$$FRR = \frac{\text{(認証失敗回数)}}{\text{(本人認証情報での認証試行回数)}}$$

$$FAR = \frac{\text{(認証成功回数)}}{\text{(他人認証情報での認証試行回数)}}$$

上の定義により k を変化させることで FRR,FAR も変化していくが，$FRR = FAR$ となる値を EER (Equal Error Rate) と呼び，この値も評価指標として使用する．単になりすまし耐性を強化する，すなわち FAR を小さくするだ

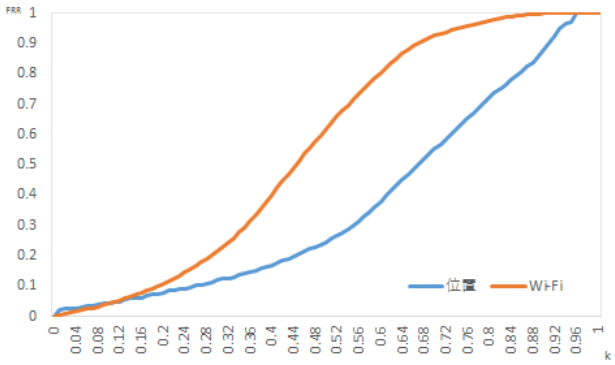


図 4: 位置, Wi-Fi 認証の閾値 k と FRR

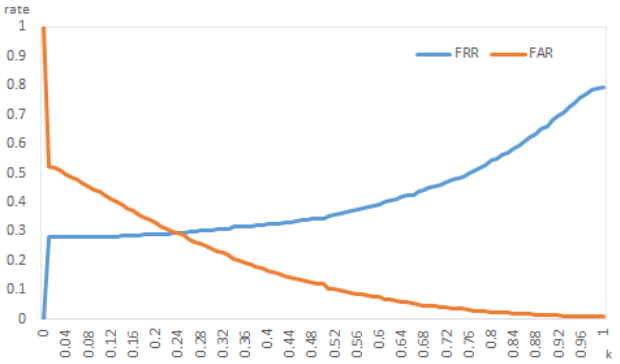


図 5: 相関認証の閾値 k と FRR,FAR

けであれば k を大きくすればよいが，そうすると FRR が大きくなり認証手法としてユーザービリティの低い方式となってしまう．そのトレードオフの関係を評価するために EER を指標として使用する．

3.4 実験結果

本節では実験結果について記述する．

3.4.1 単要素での認証実験結果

図 4 は，位置情報を活用した認証手法と Wi-Fi 情報を活用した認証手法における実験結果である．横軸は閾値 k であり，k を変化させた時の FRR を表した図である．前節で述べた通りこれらの実験については他人からの位置推定を想定した実験は実施していない．そのため結果として FRR のみを表している．$k = 0.1$ あたりまでは Wi-Fi を活用した認証手法の方が FRR が小さいが，それ以降は位置を活用した認証手法の方が FRR が小さいことがわかる．また図 5 は相関関係を活用した認証手法における実験結果である．図 4 と同様，横軸は閾値 k であり，k を変化させた時の FRR,FAR を表している．$k = 0.24$ で $FRR = FAR$ となり，$EER = 0.29$ を得ることができる．なお，$k = 0.24$ のとき，位置認証では $FRR = 0.09$, Wi-Fi 認証では $FRR = 0.14$ である．

3.4.2 組み合わせの認証実験結果

図 6 は，位置情報，Wi-Fi 情報，相関関係を組み合わせた認証手法における実験結果である．左側から順に，位置と Wi-Fi(gw)，位置と相関 (gc)，Wi-Fi と相関 (wc)，位置と Wi-Fi と相関 (gwc) それぞれの k を変化させた時の FRR,FAR を示している．それぞれの EER とそのときの k の値を整理したのが表 1 である．

表 1: 組み合わせ認証の EER

	k	EER
(a) gw	0.42	0.214
(b) gc	0.47	0.298
(c) wc	0.22	0.146
(d) gwc	0.37	0.175

3.5 考察

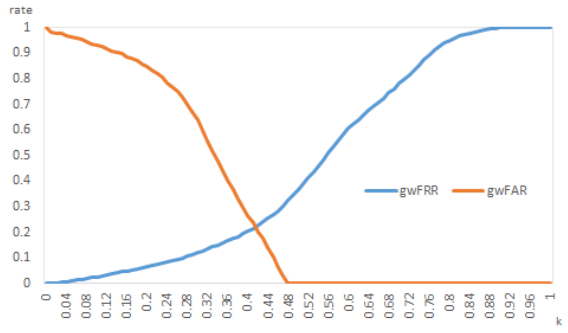
本節では実験結果から得られる知見について考察する．位置を推定されたケースのなりすまし耐性を評価する実験結果は図 5 と図 6（および表 1）である．それぞれの EER を見ると，Wi-Fi 情報と相関関係の組み合わせの結果が最も低く，この方式が最もなりすましに耐性があるように見える．これは，本研究の前提が位置情報が推定されていることにあり，そのため位置情報を活用せず Wi-Fi 情報を活用している方式が耐性が強いと考えることができる．Wi-Fi 情報が推定されるという仮定を置けば，Wi-Fi 情報を活用せずに位置情報を活用する方式（(gc)）の EER が最も低くなると推測される．

4. おわりに

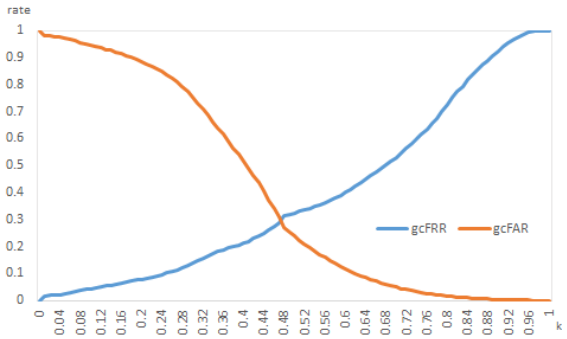
近年，行動情報を活用した認証手法について多くの研究がなされている．様々な行動情報の中で，位置情報は特に本人らしさを強く表す特性を持ち，活用した認証手法は高い認証精度を得ることができる．一方で位置情報は他人からも推定されやすく，位置情報を活用した認証手法ではなりすましされる恐れもある．そこで本研究では位置情報が推定されたケースを想定し，他の認証手法と組み合わせることでなりすまし耐性を強化する実験を行った．本章では本研究で得られた結論と今後の課題について述べる．

4.1 結論

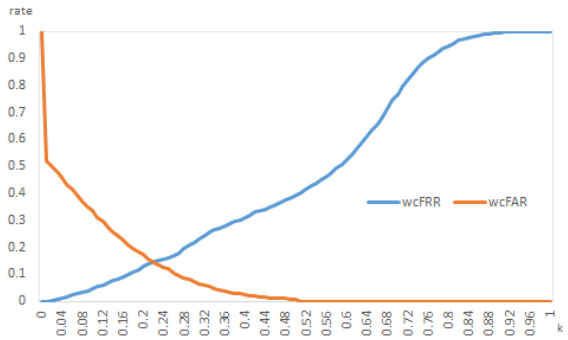
位置情報が推定されたケースに対応するため，位置情報と Wi-Fi 情報の相関関係を活用した認証手法に関する既存研究が存在する．一方でこの相関認証は位置認証や Wi-Fi 認証と比較すると精度が高くないという課題もある．そこで本研究では位置，Wi-Fi，相関それぞれを活用した認証手法を組み合わせることで，認証精度となりすまし耐性を向上させる手法を検証した．その結果，Wi-Fi と相関を組み合わせた手法が最も良い結果を得ることができた．これは本研究の前提が位置情報が推定されたケースを想定した



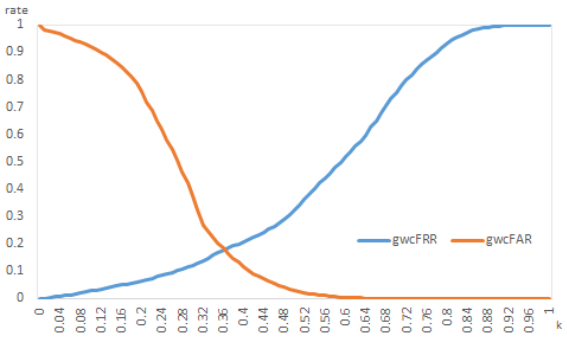
(a) 位置と Wi-Fi



(b) 位置と相関



(c) Wi-Fi と相関



(d) 位置と Wi-Fi と相関

図 6: 組み合わせ認証の閾値 k と FRR,FAR

ものであり，位置認証を組み合わせないことが良い結果につながったと考えられる．

4.2 今後の課題

本研究では位置情報すべてが推定されたと想定して実験を行った．しかしながら実際には一日中すべての時間の位置情報が推定可能とは限らず，自宅や勤務先が知られていたとしても一日のうちの一部が推定されるだけであろう．そこで今後は，一部の位置情報が推定されたケースを想定して，どのような手法が適しているかを検証することが課題となる．また今回は位置情報のみを推定可能としたが，一部の Wi-Fi 情報も推定可能となるケースも考えられる．位置，Wi-Fi ともに一部の情報が推定されたと想定して，検証していくことも今後の課題である．

本研究では認証手法の組み合わせとして，単純にスコアの平均値をとる方式を採用した．この組み合わせ方式も，それぞれ適切な重みを付与するなどよりよい手法もあると想定できる．そういった組み合わせ手法を検討することも今後の課題となる．

参考文献

[1] 独立行政法人情報処理推進機構: オンライン本人認証方式の実態調査報告書，入手先 ⟨https://www.ipa.go.jp/files/000040778.pdf⟩ (参照 2022-08-22).

[2] Rie Shigetomi Yamaguchi, Toshiyuki Nakata, and Ryosuke Kobayashi: *Redefine and Organize, 4th Authentication Factor, Behavior.* International Journal of Networking and Computing, 10-2 (pp.189-199). 2020.

[3] Issa Traore: *Continuous Authentication Using Biometrics: Data, Models, and Metrics.* Igi Global, 2011.

[4] Lex Fridman, Steven Weber, Rachel Greenstadt and Moshe Kam: *Active Authentication on Mobile Devices via Stylometry, Application Usage, Web Browsing, and GPS Location.* IEEE Systems Journal, Volume: 11, Issue: 2, June 2017. pp.513-521.

[5] 佐治信之，小林良輔，鈴木宏哉 and 山口利恵：MITHRA データセットの再構成とライフスタイルの可視化. マルチメディア, 分散協調とモバイルシンポジウム 2018 論文集 (2018): pp.1566-1573.

[6] Akira Miyazawa, Tran Phuong Thao, and Rie Shigetomi Yamaguchi: *Multi-factor Behavioral Authentication Using Correlations Enhanced by Neural Network-based Score Fusion.* 2022 IEEE 19th Annual Consumer Communications & Networking Conference (CCNC). IEEE, 2022.

[7] 小林良輔 and 山口利恵：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. マルチメディア, 分散協調とモバイルシンポジウム 2018 論文集 (2018): pp.1559-1565.

[8] 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.

[9] Microsoft: Bing Map Tile System, 入手先 ⟨https://docs.microsoft.com/en-us/bingmaps/articles/bing-maps-tile-system⟩ (参

照 2022-08-22).
[10] 重田信夫, 冨田清次, 小林良輔, 佐治信之 and 山口利恵：ライフスタイル認証・解析 実証実験 2021 レポート. マルチメディア, 分散協調とモバイルシンポジウム 2022 論文集 (2022): pp.301-309.