ライフスタイル認証・解析　実証実験 2019 ステップ 1 のまとめ

重田 信夫[1,*] 小林 良輔[1] 佐治 信之[2] 山口 利恵[1]

概要：現在，多く利用されている個人認証手法の一つとして ID/パスワードがあるが，この利用にはユーザーの負担も大きい．この解決のため，人の行動習慣を個人の特徴と捉えて認証要素の一つとする“ライフスタイル認証・解析”を提案している．ここでは，個人のスマートフォン等から得られる様々な行動データを用い，リテラシーに頼らない個人認証や個人向けの行動支援，個人向けサービス提供などの実現を目指して研究と実験を進めている．
2017 年には 5 万人規模の実験を実施し，GPS，Wi-Fi，アプリの閲覧履歴，活動量など，多様かつ大量の行動データの取得に成功した．さらに 2019 年 1 月～4 月に実証実験 2019(ステップ 1)として本人性の評価である認証値を可視化する実験を行った．この内容は，普段の行動データから得られる標準的なパターンと，現在の行動パターンとを比較し認証値として数値化するものである．本稿ではここで得た結果をまとめる．特に，スマートフォン種別による収集データ量の影響，各種アルゴリズムの違いによる認証値の比較についての考察を含む．

キーワード：ライフスタイル認証，行動認証，個人認証，実証実験，スマートフォン

Summary Report of Experiment 2019 Step 1 on Lifestyle Authentication and Analysis

Nobuo Shigeta[1,*] Ryosuke Kobayashi[1] Nobuyuki Saji[2] Rie Shigetomi Yamaguchi[1]

Abstract: In recent years, ID / password is one of the widely used personal authentication methods, but the use of this method is troublesome. In order to solve this problem, we have been promoting research and experiments by proposing “lifestyle authentication and analysis” that considers human behavior habits as individual characteristics and uses it as an authentication factor. In 2017, we conducted experiments with 50,000 people and succeeded in acquiring various and large amounts of behavioral data. In addition, in January to April 2019, an experiment was conducted to visualize the authentication results of the individual as a demonstration experiment 2019 (step 1). In this experiment, we compared the template obtained from ordinary behavior data with the current behavior pattern and quantified it as a certified value.
This paper summarizes the results obtained here.

Keywords: Lifestyle Authentication, Behavior authentication, User Authentication, Demonstration experiment, Smartphone

1. はじめに

1.1 背景

近年，スマートフォンの急速な普及とともにインターネットを通してさまざまなオンラインサービスが発展し社会的な利便性向上に寄与している．これらのサービスを利用するにあたって必要となる“自分が正当なユーザーであること”を示すために，個人認証技術に対する注目が高まってきている．

1.2 従来の認証とライフスタイル認証

本人認証は，登録フェーズで本人確認を行い，本人情報を登録する．認証フェーズでは，登録時の本人情報と認証時に提供される情報とが一致しているかどうかを見ることで，本人性の認証を行っている[1].

これまで個人認証手法としては，“知識・所持・身体的特徴”といった 3 要素を活用するものが多い [2].
我々は，この 3 つに加えて“第 4 の認証”として行動履歴を用いて多要素認証を行う“ライフスタイル認証・解析”の技術を提唱している[3]（図 1 参照）.

これは人々のライフスタイルや行動様式が持つ習慣性や多様性に着目し，生活行動のセンシングデータを活用した個人認証技術であり，ユーザーに特別な負荷をかけさせない前提でライフスタイルの情報を活用するものである．この認証要素は効率重視のこれまでの考え方とは異なり，高い利便性から人の生活に寄り添ったインフラ技術として広まることが期待される.

2017 年の実証実験(これを実証実験 2017 と呼ぶ) においては，具体的な行動情報として位置情報（GPS 等），電波情報（Wi-Fi，Bluetooth），活動量（歩数等），アプリ使用情

1 東京大学 大学院情報理工学系研究科
Graduate School of Information Science and Technology, The University of Tokyo
2 株式会社コードノミー，株式会社インフォコーパス
Codenomy Inc., Infocorpus Inc.

* shigeta@yamagula.ic.i.u-tokyo.ac.jp

図 1　ライフスタイル認証の概念

図 2　実証実験のマイルストーン

報などスマートフォンやウェアラブル端末で収集が可能なデータを収集し分析した[4].

これに続く 2019 年の実証実験（その 1）では，上記を発展させ，被験者の行動データをリアルタイムに解析し，実際の認証活用シーンを想定して，認証値の結果を被験者の端末にフィードバックすることを実現した.

1.3　本論文の構成

本論文の構成は以下のとおり.

第 2 章では，既存研究として 2017 年に実施した実証実験について述べる．第 3 章では，実証実験 2019(その 1) の概要について述べる．目的と概要，実施手段，認証アルゴリズムについて説明する．第 4 章では，実験で得られた知見や課題について述べる．得られたデータは特徴を捉えやすくするため可視化した．これを用いて被験者の実際の行動との整合性や妥当性を確認した．認証値として蓄積したデータは，情報の量と質，端末機種による違い，行動との関連性等について考察する．第 5 章では，今後の実サービス連動を想定した実験に向けた課題を示す．第 6 章では，本論文の結論をまとめと今後の方向性を記述する.

2.　実証実験 2017 について

2017 年 1 月から約 3 ヶ月半の期間で実施した MITHRA (Multi-factor Identification / auThentication ReseArch) プロジェクトの実証実験においては，スマートフォンの各種センサーを用いて，位置情報や Wi-Fi 電波情報，アプリの利用履歴情報を収集するためのスマートフォンアプリ（MITHRA アプリと呼ぶ）を使い，各種情報を収集・分析を進めてきた[5][6].

この実験では，5 万人を超える被験者から大量の行動データを収集し，行動解析のための基礎的な研究に活用した．得られた主な成果を下記に示す[7][8][9][10].

- データの可視化[11]

位置情報（例：自宅，職場等の推定），各種の習慣的行動特性（例：日曜～土曜のパターンを把握），位置情報と運動量データの関連性を可視化した.

- 認証アルゴリズムの開発[12]

位置情報（例：GPS 等），無線環境（例：Wi-Fi，Bluetooth 等）を利用して行動データを収集・分析・評価した.

3.　実証実験 2019（その 1）について

実証実験 2019 は，ライフスタイル認証・行動解析の社会実装を目指し，具体的な技術確立を目標とするものである．実証実験のマイルストーンを図 2 に示す.

その第一段階(その 1)では，スマートフォンから収集した行動情報を収集・分析し，認証値を判定し，その結果をタイムリーに被験者端末に表示することを確認する．これは引き続き実施するサービス連動実験の前提となる基盤技術である.

実験では，各種の認証アルゴリズムをシステムに実装し，行動と認証値の関係を確認する．特に被験者の行動が適切に反映されるだけでなく，特別な行動の場合も認証値に違和感なく反映されることを確認する．得られた課題はアルゴリズムの改良や今後のサービス連動に向けた研究に活用する．[13]

3.1　実験の概要

実証実験の実施内容を示す.

目的： データ収集，認証システムおよびデータ表示の相互連携を確認する．具体的には，多様な端末（ iOS, Android ）で得られた行動データを収集・分析・蓄積し行動パターンをテンプレートとして確定する．被験者の現在の行動データをテンプレートと照合し認証値を得てリアルタイムに提供する．認証値の変化を可視化し行動特性を把握する上でのノウハウや課題を蓄積する.

期間：

- iOS 系： 2019 年 1 月 11 日～2019 年 4 月 15 日
- Android 系： 2019 年 1 月 29 日～2019 年 4 月 15 日

被験者：本研究を実施した社会連携講座の関係者 30 名.

使用端末： iOS 系と Android 系の各 15 台（計 30 台）.

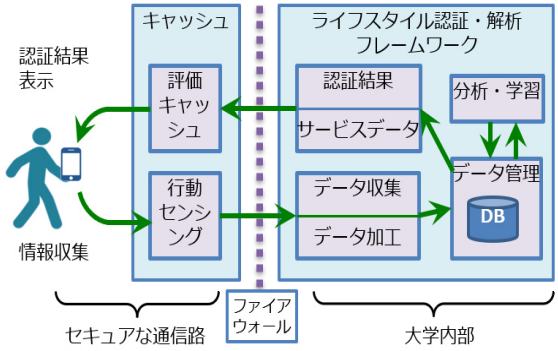

図 3　実験システムの構成

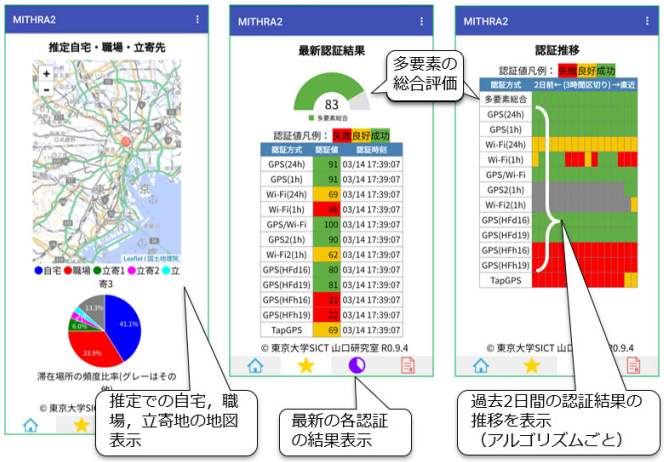

図 4　MITHRA2 アプリケーションの画面例

3.2 実施手段

3.2.1 システム概要

構築したシステム構成を図 3 に示す．

東京大学内にライフスタイル認証・解析フレームワークを搭載したサーバーを設置した．ここには被験者のスマートフォンから定期的に収集されるデータをデータベースに蓄積する．収集したデータからテンプレートを作成するために分析学習エンジンを設置した．認証評価は，搭載された複数のアルゴリズムによって処理され，現在値と変化履歴を含めて被験者のスマートフォンに表示される．

3.2.2 収集するデータの種類

行動データとしてスマートフォンで収集する情報は実証実験 2017 の経験も踏まえて以下とした．

- GPS 情報： 緯度・経度・位置精度
- Wi-Fi 情報： 補足した BSSID（限定あり）
- Bluetooth 情報： 補足した BD ADDR（限定あり）
- 端末状態：バッテリー残量（%）
- アクティビティ情報： 歩数に相当する

3.2.3 スマートフォンアプリケーション

Android および iOS のスマートフォンで動作するアプリケーションを開発した．主な機能は，搭載されたセンサーの測定データを周期的に収集し大学内サーバーに送信する機能，サーバーで処理された認証値等の結果を表示する機能を用意した．なお，実験のため各種アルゴリズムの認証値の比較が可能なように，結果を対比して参照できる画面設計とした．画面例を図 4 に示す．

画面例左の地図表示は．被験者自身の行動パターンを認識してもらうことと実験への参加に役立つものである．画面中央の認証値は，どのような行動をしていた場合のものか，被験者に直感的に知らせて確認する必要があり，分かり易くするために認証値が高い方から，緑・黄・赤の 3 色表示とした．

3.3 認証アルゴリズム

3.3.1 アルゴリズムの種類

認証アルゴリズムは表 1 のとおり，11 種類を使用した．（#6 と#7 は実験途中で追加したものである）

認証要素として，位置情報（GPS 等）と Wi-Fi 情報（BSSID のリスト等）を使用するかにより大別される．テンプレートと照合するデータの対比時間幅により，24 時間か 1 時間かにより分類される．またテンプレートの作り方や観測値との類似度の判定方法によりさらにバリエーションがある．これらは実証実験 2017 のデータ解析の研究成果を活用したものである．

表 1　使用したアルゴリズム

#	認証方式	認証要素	データ収集期間
1	GPS (24h)	位置情報	24 時間
2	GPS (1h)	位置情報	1 時間
3	Wi-Fi (24h)	Wi-Fi 情報	24 時間
4	Wi-Fi (1h)	Wi-Fi 情報	1 時間
5	GPS／Wi-Fi	位置と Wi-Fi 情報	最新値
6	GPS2 (1h)直近	位置情報	直近の 1 時間
7	Wi-Fi2 (1h)直近	Wi-Fi 情報	直近の 1 時間
8	GPS(HFd16)	位置情報	24 時間
9	GPS(HFd19)	位置情報	24 時間
10	GPS(HFh16)	位置情報	1 時間
11	GPS(HFh19)	位置情報	1 時間
	多要素総合	上記の組合せ	

3.3.2 テンプレートと認証判定

認証アルゴリズムの一例として，表 1 の#2「GPS (1h)」

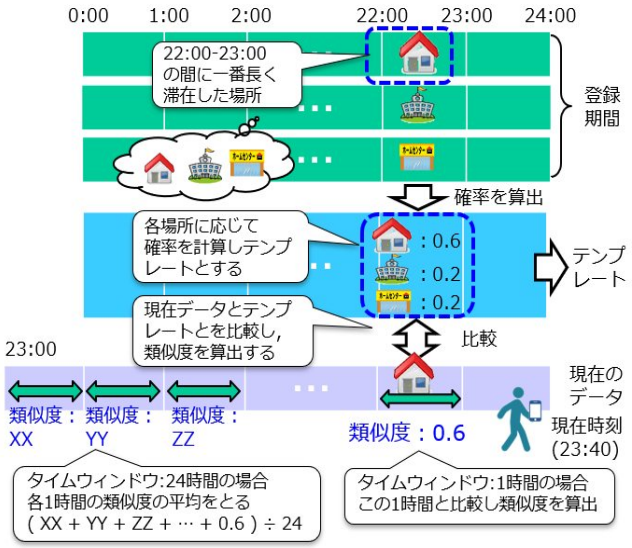

図 5　テンプレート作成と比較による判定

（これは GPS のタイムウィンドウ 1 時間の情報を使用するもの）の動作を説明する．

図 5 に示すように，被験者の位置情報を 1 時間単位（図では 22 時～23 時）で最も多く滞在した場所を求める．この日は自宅に居たとする．別の日は同じ時間帯に職場に居て，また別の日は別の立寄り先に居たとする．テンプレートの登録期間でこれらの存在確率を決定しテンプレートとする．存在する比率に応じて，例では自宅 : 0.6，職場 : 0.2，立寄り先 : 0.2 とした．なおこのアルゴリズムの場合は，テンプレートは 30 日間に亘って自動更新して固めたものである．

認証判定を行う場合，このテンプレートと現在のデータを比較する．現在時刻が 23:40 だとすると，その前の 1 時間（22 時～23 時）の位置が自宅であれば，認証値（つまりテンプレートとの類似度）は 0.6 となる．

また 24 時間での判定を行う場合は，図 5 の左側にあるように過去 24 時間のテンプレートの平均をとって認証値とする．

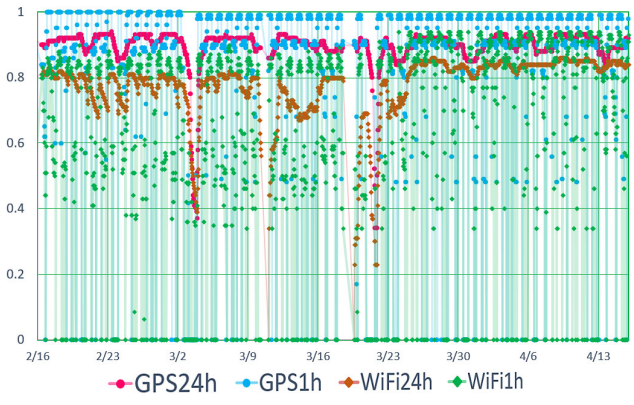

図 6　認証値データの例

4.　実験の成果

4.1　結果の概要

結果として得られる認証値は，実験で収集する行動データを，各アルゴリズムに応じて計算して得られる認証値を時系列的に記録したものである．横軸は時間軸，縦軸は認証値（0≦認証値≦1）である．

図 6 は，ある被験者の全実験期間の認証値を示している．アルゴリズムは 4 種類(GPS24h, GPS1h, WiFi24h, WiFi1h)のみ示す．色は認証アルゴリズムの違いである．

1 時間ベースの認証値は，1 時間単位でテンプレートとの類似度を評価するため，1 時間単位で所在が変わると変動する．認証値が下がる場合は被験者の行動が通常とは異なる場合と想定される．位置情報はメッシュ区画（900m×900m）単位で評価するため，オフィス内や自宅内での移動は変動とはなりにくいと想定される．

Wi-Fi の電波についても住宅内やオフィス内等の限定エリアで使用されることが多く，部屋間やフロア間の移動程度でもデータ（BSSID のリスト）の変動が認識されるため，認証値としての変化の頻度が高いことが推定される．

一方 24 時間単位の認証値は，1 時間ごとの類似度の移動平均をとるため（図 5），個々の行動変化の影響は受けにくく 1 日以上の旅行等の行動変化時に変動する．この性質から 24 時間単位の認証値は時間や場所のゆらぎの影響を受けにくく，人物の特定には向いていると考えられる．

4.2　端末種別ごとの特徴

実験に使用した端末は大別して，iOS 系と Android 系のスマートフォンに分けられる．それぞれ特徴的なデータ収集の特性がある．

・iOS 系スマートフォン

アプリケーションは一定の時間間隔で動作することが制限されており，情報の収集タイミングが一律ではない．例えば，位置情報は位置変化が検出された場合等に通知される．このため位置情報を得たい場合，タイムリーな結果が得られないこともある．また同一場所で留まっている場合などは，必要に応じて位置データの補間等の工夫が必要となる場合がある．

また，Wi-Fi 情報として，実際に端末が Wi-Fi 接続した場合のみ，その BSSID 情報が収集されるため，得られる情報の密度が低いことが見受けられた．

・Android 系スマートフォン

アプリケーションは，一定時間間隔（実験では 5 分間隔）での情報収集が可能であるため，細かな動きにそった情報が得られた．情報が多いことにより，時系列変化の詳しい状況が読み取れ，行動変化がいつから起こったのか等がよ

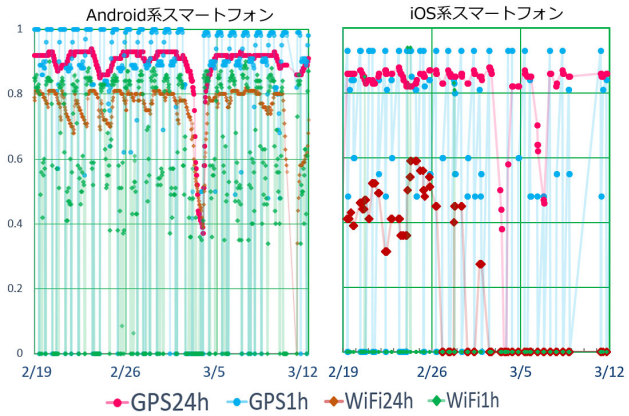

図 7　端末機種によるデータの差

り明確に判断できる．

図 7 は同一の被験者が，iOS 系と Android 系の両方の端末を持ち歩いた場合の，同一期間のデータの比較を示す．

両者を比べると，変動の傾向はほぼ一致しているが情報の密度が Android の方が高いことがわかる．3 月 2 日～3 日の認証率低下は，休暇を利用した旅行の影響が伺える．また Wi-Fi24h の認証値の差（iOS 系が低く出ていること）は，情報量の違いがテンプレートの精度に影響を与えた可能性もある．

4.3　認証値の即応性について

認証値によって何らかのサービス提供を想定した場合，被験者がいつもと異なる行動をした場合，他人の可能性があるため，「直ちに認証値が下がるべきだ」という意見が被験者から得られた．

一方，人間の行動は必ず揺らぎがあり，同一行動をしているつもりでも時間のずれ，位置のずれなどが生じるものである．このため正しい本人であるのに拘わらず，認証値が下がってしまい目指している利用者の利便性・満足性の獲得には逆行する可能性もある．

このような背景から，認証値の判定には 1 時間単位の評価と 24 時間単位の評価を設けて実験した．1 時間単位の評価では，いつもと違う行動をした場合，直ちに認証値が下げたい場合に有効である．被験者からは，非日常行動の認証値への反応を直ちに反映する，つまり即応性を求める要望も得られた．この点に応えるために直近の 1 時間のデータを活用する方式も実験途中でアルゴリズムに加えた．

24 時間単位の評価は，行動の揺らぎを吸収し，24 時間の生活パターン（自宅と職場のサイクル）をベースとして行動を区別するため，他人との確実な識別に有効性がある．

具体例では，　のように 1 時間ベースの認証値が短時間で変動するのに対して，24 時間ベースの認証値は，比較的安定した推移を示している．

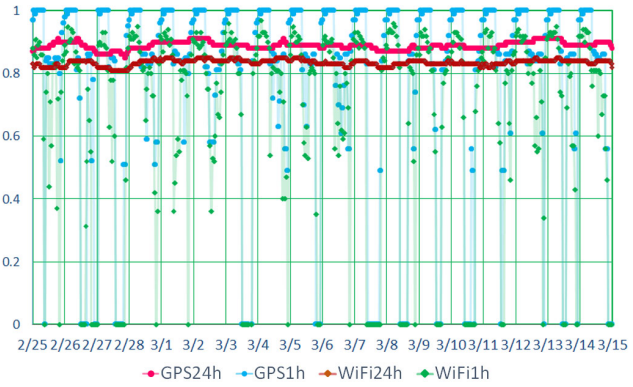

図 8　24 時間／1 時間の認証値変化

これらの両方の特徴を活かした評価方法については研究途上である．例えば認証値の利用目的つまり提供するサービスの特性に応じた認証値を返答することや，または各認証アルゴリズムの組合せ方で工夫ができないか等については今後の課題である．

4.4　端末所有者のローテーション

被験者 A の持つ端末を別の被験者 B に手渡した場合の認証値の変化を見た．被験者の行動パターンを学習したテンプレートは，先の被験者 A の行動に基づいて作成されている．後から端末を使用する被験者 B は他人であり，認証値が低く（できればゼロに）なることが望まれる．実験では生活環境の関連性が低いと想定される職場が異なる人同士の場合，生活環境の関連性が高いと想定される同一職場の人にローテーションした場合を想定して実験した．

認証値の変化は次のとおりである．

(1)　職場が異なる人にローテーションした場合

・iOS 系スマートフォン

位置情報をベースとした認証値（24 時間，1 時間とも）は確実に低下した．特に GPS24 の変化は変動が顕著であり，ローテーションから 24 時間以内に別の被験者に渡ったこ

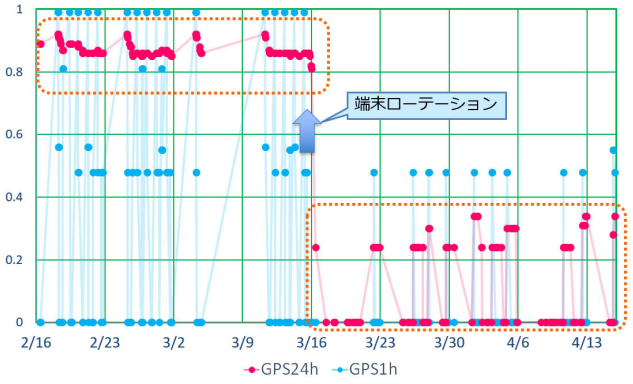

図 9　社間ローテーション（iOS 系）

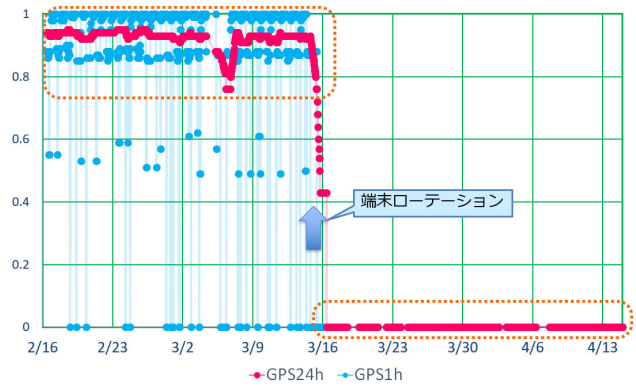

図 10　社間ローテーション（Android 系）

とが認識できる状況であった．　図 9 に iOS 系の場合の例を示す．

・Android 系スマートフォン

同様に，ローテーション後は顕著に認証値低下がみられたが，Android の場合はほぼゼロになる結果が得られた．この理由は情報量の多さから揺らぎによると考えられる誤差が低減されること，またテンプレート自身の精度が高いことが推定される．図 10 に Android 系の場合の例を示す．

(2)　同一の職場の人にローテーションした場合

平日昼間時間帯は，ほぼ同一の環境（同一オフィス，同一 Wi-Fi エリア）にいることも推定されるため，昼間時間帯での個人の識別はやや困難となる傾向がみられる．

・iOS 系スマートフォン

ローテーション後の認証値は低下傾向にあるが、一部の時間帯でみると変化は小さく、識別が困難なことも見受けられる。この点は同一の職場の影響を大きく受けていることが推定される．図 11 に iOS 系の場合の例を示す．

・Android 系スマートフォン

図 12 は Android 端末の同一職場内ローテーションの場合であるが，位置情報が 5 分ごとにとらえられ変化が詳し

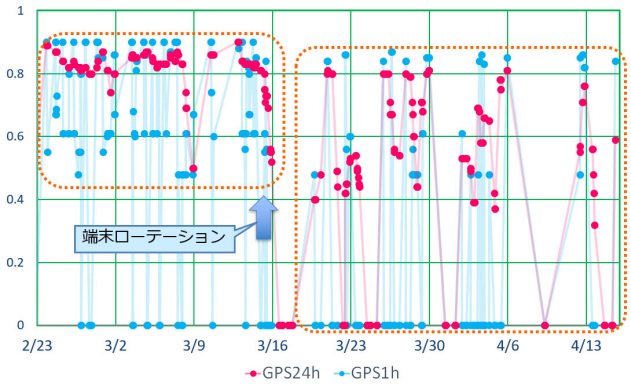

図 11　社内ローテーション（iOS 系）

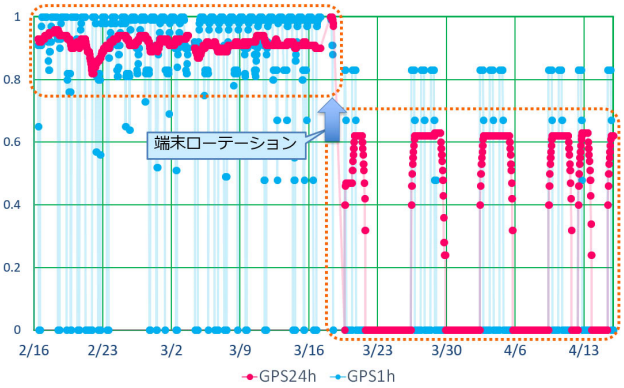

図 12　社内ローテーション（Android 系）

く得られている．ローテーションによる認証値の低下は明確で分かりやすいものとなった．

なお，ローテーション後の被験者の勤務パターン（週 3 日等）が判断できるなど行動特性を知るための興味深い状況も把握できた．図 12 に Android 系の場合の例を示す．

4.5　Wi-Fi 情報の活用

Wi-Fi はその電波の飛ぶ範囲が比較的狭いため，被験者の場所で受信可能な Wi-Fi のリストは被験者の行動を知るうえで重要な情報となる．特に室内環境においては位置情報としての GPS 受信が難しいことから，Wi-Fi の有効性が想定される．

ただし iOS の場合，実際に Wi-Fi 接続したアドレスのみを収集できる．このため付近の Wi-Fi のリストを把握できる Android の場合の情報量が勝り，より詳細な行動データが得られる．なお，位置情報 GPS 系のデータと Wi-Fi データには高い類似性がみられる．（図 13 参照）

Android 端末の場合，位置情報の代わりに Wi-Fi を使用することも可能とみられる．位置情報の収集が困難な室内や，GPS をオフにした場合には有効とみられる．

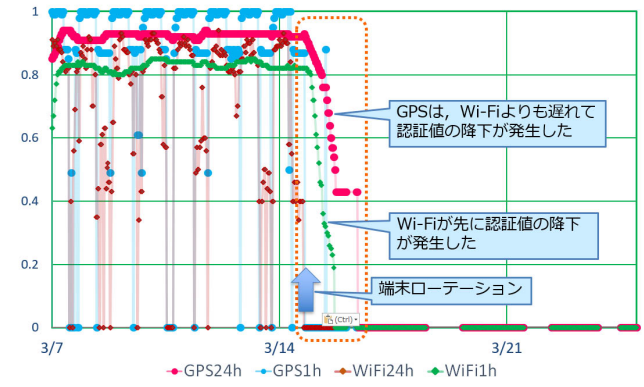

図 13　Wi-Fi ベースの認証値との関係性（1）

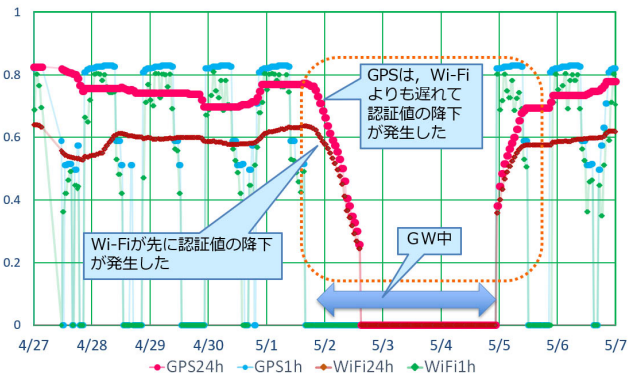

図 14　Wi-Fi ベースの認証値との関係性（2）

なお図 14 は，GW 前後の行動変化がとらえられているもので，環境変化に対する感度についても同等であることが分かった．

4.6　テンプレート作成段階の挙動

実験ではテンプレート作成に 30 日間をあてているが，実際にはより短期間にテンプレートが安定する（つまり認証値が安定する）場合もある．認証値の変化にその安定化に向けた期間が読み取れる情報がある．図 15 は，テンプレートの更新を行いつつ認証値を計測している段階のもので，この被験者の場合は，GPS1h 認証値として実験参加から約 2 週間で認証値が安定化していることが推定できる．テンプレート作成期間は，得られたデータから判定することも可能とみられる．

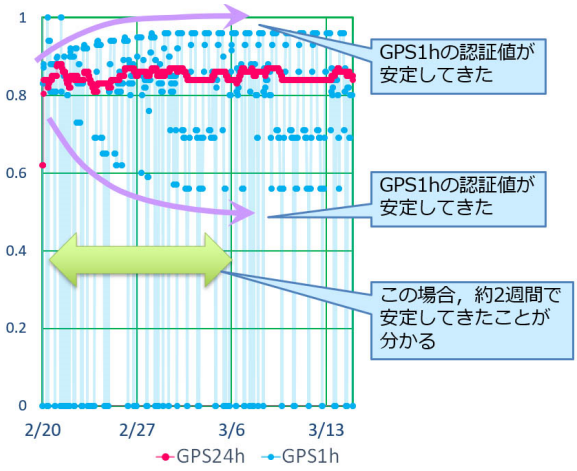

図 15　認証値の安定化にかかる期間

5.　今後の課題

5.1　認証値の組合せ

今回，各種アルゴリズムで得られた認証値にはばらつきも多い．これらの認証値を組合せた複合認証値（multi と呼ぶ）の導入を検討してきた．基本的には重要視する項目を重視した加重平均を得ようとし，実験では試行錯誤を行った．まだ改善途上である．

課題となるのは，行動データとして扱うべき要素は何か，認証値を利用するサービスに求められる認証精度，即応性が必要かどうか，スマートフォンから得られるデータにバリエーションがある場合の扱い方等であった．今後の研究に向けてこれらの知見を活かしていく．

5.2　端末計測データの違い

本来の実験内容とは別だが，実証実験を展開していくうえで問題となるのは，スマートフォンの機種依存性を克服することが必要である．具体的には

- Android 系のバージョンや機種への依存性
- iOS 系の仕様上の制約
- ばらつきの大きい GPS の受信感度や精度の克服

などが挙げられる．今後の実験に向けてはこれらを課題に対応していくことも必要である．

6.　まとめ

本稿ではライフスタイル認証・解析の評価に向けた実証実験 2019(その 1) の結果報告を行った．ライフスタイル認証の基礎データを収集するスマートフォンと，データを蓄積・分析するフレームワークとの連動を確認し，各種の認証アルゴリズムを実装した．

認証値を時系列で収集することにより，その時間的変化や，環境的変化を捉えることが出来た．特徴的な挙動についても理解を進めてきた．

データだけでなく被験者から得た多くの意見を踏まえて今後の実サービスとの連動を目指す．

謝辞

本実験に参加いただいた関係各位に感謝の意を表します．本論文の研究は，次世代個人認証・行動解析技術社会連携講座の各社（三菱 UFJ ニコス，凸版印刷，三菱電機インフォメーションシステムズ，日立製作所）による．

参考文献

[1] 山口利恵，鈴木宏哉，小林良輔：認証精度の違う多要素・段階認証，コンピュータセキュリティシンポジウム 2015 論文集 pp. 795 － 802, (2015)

[2] X. Huang, Y. Xiang, A. Chonka, J. Zhou and R. H.Deng, ”A Generic Framework for Three-Factor Authentication: Preserving Security and Privacy in Distributed Systems,” in IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 8, pp. 1390-1397, Aug.(2011).

[3] 小林良輔，疋田敏朗，鈴木宏哉，山口利恵：行動センシングログを元にしたライフスタイル認証の提案，コンピュータセキュリティシンポジウム 2016 論文集，Vol.2016，No.2，pp.1284-1290 (2016).

[4] 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，協調とモバイルシンポジウム 2017，pp.223-230,No.1H-2 (2017).

[5] 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-，暗号と情報セキュリティシンポジウム 2017，No.4D2-1(2017).

[6] 鈴木宏哉，山口利恵：倫理審査，同意取得，アプリ審査の壁を越えて…ライフスタイル認証実証実験の履歴収集に関して，コンピュータセキュリティシンポジウム 2017 論文集 (2017).

[7] 鈴木宏哉，小林良輔，山口利恵：ライフスタイル認証モデルの提案とその評価に向けた実証実験，日本ソフトウェア科学会第 34 回大会，pp.27-32, [一般 11-3-L](2017).

[8] 小林良輔，佐治信之，山口利恵：ライフスタイル認証の活用事例とその検証：低リスクシナリオ，コンピュータセキュリティシンポジウム 2017 論文集(2017).

[9] 疋田敏朗，小林良輔，鈴木宏哉，山口利恵：MITHRA プロジェクトの移動履歴データの解析，マルチメディア，分散協調とモバイルシンポジウム 2017 論文集，Vol.2017,pp.231-238 (2017).

[10] 小林良輔，山口利恵：MITHRA データセットで Wi-Fi 個人認証その 1，マルチメディア，分散，協調とモバイルシンポジウム 2017 論文集，Vol.2017，pp.239-244 (2017)

[11] 佐治信之，小林良輔，鈴木宏哉，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)

[12] 藤尾正和，高橋健太，鈴木宏哉，小林良輔，山口利恵：携帯端末の移動履歴を用いた本人認証，暗号と情報セキュリティシンポジウム 2018.

[13] 重田信夫，小林良輔，佐治信之，藤尾正和，高橋健太，山口利恵：ライフスタイル認証・解析 実証実験 2019(その 1) 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 2019 論文集(2019)