

ライフスタイル認証・解析 実証実験 2019(その1) レポート

重田 信夫¹ 小林 良輔¹ 佐治 信之² 藤尾 正和³ 高橋 健太³ 山口 利恵¹

概要：“ライフスタイル認証・解析”は個人の行動パターンに基づく情報で認証する技術であり、さまざまな行動支援や、個人向けサービス提供などの実現を目指すものとして提案している。2017年1月～4月には、5万人規模の実証実験2017を実施し、GPS、Wi-Fi、アプリの閲覧履歴、活動量など、多様かつ大量のデータ取得に成功し、解析技術の向上に貢献した。この実験の成果を受け、行動データを元に認証アルゴリズムを開発・実装し、今後の個人向けサービスと連携させることを目指し、2019年1月～4月にライフスタイル認証・解析の実証実験2019を実施した。ここではスマートフォンにより収集した位置情報、Wi-Fi情報を中心に認証結果をタイムリーに評価し本人にフィードバックすることや、スマートフォン所有者が代わった場合の影響等を検証した。本稿では、本実験の概要とその到達点について報告する。

Experiment 2019 Report on Lifestyle Authentication and Analysis

NOBUO SHIGETA¹ RYOSUKE KOBAYASHI¹ NOBUYUKI SAJI² MASAKAZU FUJIO³
KENTA TAKAHASHI³ RIE Shigetomi YAMAGUCHI¹

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。また、スマートフォンから収集される大量の個人データも、オンライン上だけでなく、様々な実社会での活動支援サービスに活用されている。例えばECサイトでのショッピング時、ビッグデータに基づいたターゲティング広告やレコメンデーション、また実店舗で進みつつあるキャッシュレス決済の利用拡大など社会構造の変革につながる動きがみられる。[1][2]

ここでこれらのサービスを利用するにあたって、共通に必要な“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

認証とは、登録時に本人確認を行い、認証情報を登録する。認証時には、登録時の情報と認証時の情報が一致しているかどうかを見ることで、認証を行っている。[3]

これまで個人認証手法としてIDとパスワードが主流であった。これに加え、指紋や顔認証といった生体認証の仕組みも広く使われるようになった。(図1の上部参照)

これらの認証方式は、従来型の“知識・所持・身体的特徴”といった3要素を活用するものである。[4]

これらの活用にあたっては、例えば情報の漏洩に伴うなりすましの問題や、パスワードの適切な管理や利用の都度入力を求められるといったユーザビリティの低下、また身体的特徴データには漏洩した際などに変更が困難等の課題が知られている。

我々は、上記3要素に加えて“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。[5]

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、ユーザーに負荷をかけさせないライフスタイルの情報を活用する。ただし個人の活動には当然、揺らぎが存在することと、また必ずしも日々同じ行動

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.

³ 株式会社日立製作所 研究開発グループ
Hitachi, Ltd. Research & Development Group



図 1 従来の認証 3 要素と第 4 の認証

をとるとは限らないことから、長い時間の行動を捉える必要がある。ユーザーの利便性を考慮しつつ、用途によっては他の要素と組合わせた多要素認証を含めて提案してきた。(図 1 の下部参照)

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。今後、人のライフパターンを活用した様々な快適なサービスが社会実装されることにより、安全な社会の実現や、生活に余裕を感じられる心豊かな潤いを楽しむ社会づくりを目指す。

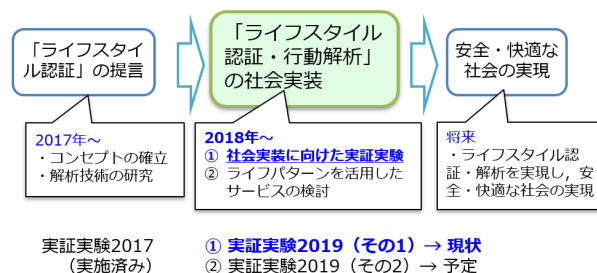
2017 年の実証実験 (これを実証実験 2017 と呼ぶ) においては、具体的な行動情報として位置情報 (GPS 等)、電波情報 (Wi-Fi, Bluetooth)、活動量 (歩数等)、アプリ使用情報などスマートフォンやウェアラブル端末で収集が可能なデータを収集し分析した。[6]

2019 年、先の情報収集に重点があった実証実験 2017 の結果を受けて、行動データから実際の認証活用シーンを想定して、行動データの解析結果を被験者に提供した。この実験の位置づけは、図 2 に示す通り、行動情報を認証と連携し社会実装を図る段階の、最初のステップとして実施した。

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 2017 を紹介する。第 3 章では、の実証実験 2019(その 1) について述べる。目的と概要、実施手段、実験の運用、認証アルゴリズムについて説明する。第 4 章では、実験の成果を述べる。情報の蓄積、被験者ヒアリング、端末ローテーションの結果を説明する。第 5 章では、今後の実験に向けた課題について述べる。第 6 章では、本論文の結論をまとめ、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 [7][8]。

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。今後の実用化および社会実装を進めるうえで、行動の特徴を捉えるデータの、それぞれの特性に応じた解析のためのフレームワークを明らかにした。

2.1 実験の目的と概要

実証実験の実施内容を示す。

- 目的：行動認証に係わるデータ収集
- 期間：2017 年 1 月 11 日～4 月 26 日
- 被験者：57,046 人 (一般募集)
- 手段：スマートフォン、ウェアラブル端末から収集
- 収集データ
 - － 環境データ (端末情報, 位置情報, Wi-Fi, Bluetooth 等)
 - － アプリ利用データ
 - － 活動量データ

2.2 主な成果

実験から得られた主な成果を下記に示す [9][10][11][12]。

- データの可視化 [13]
 - － 位置情報 (例：自宅、職場等の推定) の変化
 - － 周期的行動特性 (例：日曜～土曜のパターンを可視化)
 - － 位置情報と運動量データの関連性可視化
- 認証に向けた分析アルゴリズムの開発 [14]
 - － 位置情報ベース (例：時間ごとの存在確率を評価)
 - － 環境情報ベース (例：近傍にある Wi-Fi, Bluetooth の類似性を評価)

3. 実証実験 2019（その 1）について

実証実験 2019 は、スマートフォンから収集した行動情報を周期的に収集・分析し、認証判定を行い、その結果を被験者端末に表示することを実現した。システム全体の構成や実装に向けた課題の抽出を目指す。

3.1 実験の目的と概要

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。
 - － 多様な端末（iOS, Android）での運用を確認する。
 - － 端末所有者の変更による影響度を評価する。
- 期間：
 - － iOS：1月11日～4月15日
 - － Android：1月29日～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に限定した。
- 使用端末：表 1 に示す合計 30 台。

3.2 実施手段

3.2.1 システム概要

システム構成図を図 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。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。

被験者のスマートフォンと東京大学のサーバーとの間は https によるセキュアな通信路で結ばれ、学内のサーバーは厳重なセキュリティ管理のもと運用した。

3.2.2 端末アプリケーション

ライフスタイル認証・解析の実験に必要な行動情報を収集するためのスマートフォン向けのアプリケーションを開発した。これを“MITHRA2 アプリ”と呼ぶ。2017 年の実

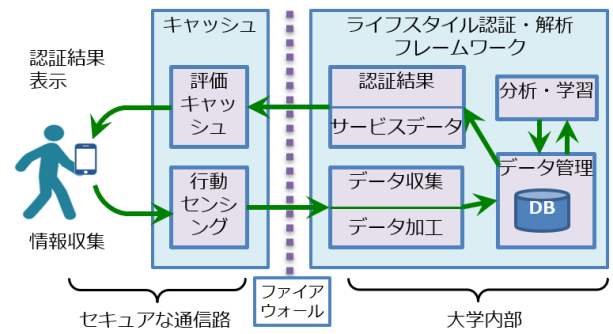


図 3 システム構成

証実験の際に使用したアプリケーションは、1日1回の情報収集であったが、今回は収集したデータを逐次サーバーに送信する方式で、タイムリーな行動情報を得て認証値をフィードバックすることができる方式とした。

主な仕様を示す。

- 収集するデータの種類
以下の項目を収集した。
 - － GPS 情報：緯度・経度・高度・精度
 - － Wi-Fi 情報：補足した BSSID のリスト
 - － Bluetooth 情報：補足した BD_ADDR のリスト
 - － バッテリー情報：残量 (%)
 - － アクティビティ情報：歩数に相当
- データ送信機能
Android および iOS のスマートフォンで動作し、搭載されたセンサーの測定データを周期的に収集し、東京大学内サーバーに送信（暗号通信）する。
情報の収集間隔は、Android の場合は 5 分間隔とした。iOS の場合は OS 仕様の制約から、アプリ起動時や位置変化を OS が感知した場合にのみ送信されることとなる。このため、iOS 版と Android 版では収集できる情報量が異なることとなった。この違いにより認証結果や認証精度にどのように影響するかも検証できる。
- データ表示機能
スマートフォン画面を図 6 に示す。具体的には以下の通り。

- － 位置表示（図 6 の (A)）

ライフスタイルを特徴づける存在率が高い場所（地図をメッシュ化した位置情報）の順位に基づき、自宅や職場、立寄り場所を推定し、表示する。

- － 認証値表示（図 6 の (B)）

現在の認証値（0～1 の値、テンプレートとの類似性、距離等）を知らせることで、被験者の今の行動がどの程度本人らしいかを視覚表示した。画面には認証アルゴリズムごとの値を表示し、認証値が高いものから、緑・黄・赤の 3 色表示とした。

さらに各アルゴリズムを組合せ、多要素総合の評価も加え、上部の半円グラフで表示した。

表 1 実証実験に使用したスマートフォン

No	端末	OS	台数／属性
1	iPhone6	iOS 12.2	10 台、被験者に貸与 ローテーションあり
2	iPone 各種	iOS 10.x 以上	5 台、個人所有物
3	Android 各種	Android 6～9	10 台、被験者に貸与 ローテーションあり
4	Android 各種	Android 6～9	5 台、個人所有物

－ 認証履歴表示 （図 6 の (C)）

過去 48 時間分の認証履歴を 3 時間単位の時間幅で表示することとした。これにより被験者は 2 日分の行動と認証値との関連性を認識し、結果を実感することができる。

－ 規約やチャット機能 （図 6 の (D)）

被験者相互間の情報交換やログ収集の機能を加えた。

3.3 実験の運用

実証実験の運用にあたり、次の点を考慮した。

- 多種の端末準備

使用する Android 端末メーカは 6 社、また Android の OS バージョンも 6～9 まで幅がある。これは次のステップで想定される規模の大きい実験への展開を考慮したことによる。

- テンプレート学習期間

各被験者のテンプレートを固定化するため、実験開始から約 1 カ月を学習期間（自動更新する期間）とした。ただしこの時間は、アルゴリズムや被験者の行動によるので一概には決定できない。

- データのモニタリング

被験者は特別なアプリ操作は不要であるがサーバー管理者側から各端末のデータアップロード状況をチェックし、異常があれば早めに対応できる運用とした。

- 端末の所有者変更

被験者は同一の職場の人も複数いるため行動パターンが近い可能性もある。このため、実験の途中で同一社内、および別の社との端末交換ローテーションを実施した。これは所有者が替わった場合に正しく変化を識別できることを確認するためである。

3.4 認証アルゴリズム

3.4.1 種類

認証アルゴリズムは表 2 のとおり、11 種類を使用した。認証要素として、位置情報を使用するか Wi-Fi 情報を使用するか、データ参照時間が 24 時間か 1 時間かにより大別される。またテンプレートの作り方や類似度の判定方法により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。

3.4.2 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、#2（GPS (1h) : GPS の 1 時間情報を使用するもの）の動作を説明する。図 4 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）の位置情報から、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,

表 2 実験で使用した認証アルゴリズム

No	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	位置情報 / Wi-Fi 情報	瞬時
6	GPS2 (1h) 追加	位置情報	1 時間 (直近)
7	Wi-Fi2 (1h) 追加	Wi-Fi 情報	1 時間 (直近)
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	

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、テンプレートは 30 日間に亘って自動更新しテンプレートを固めた。

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。（図 5 参照）

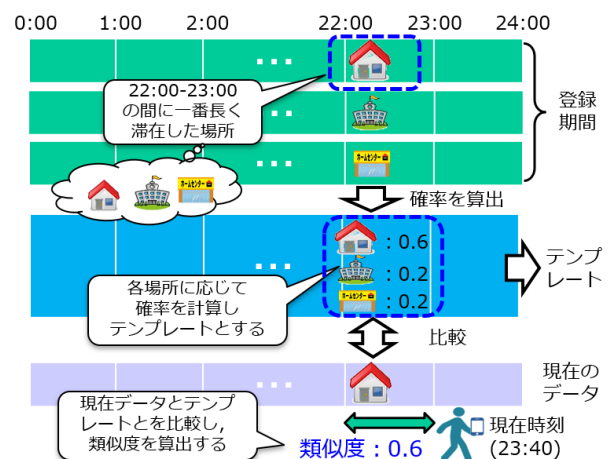


図 4 テンプレート作成と評価判定

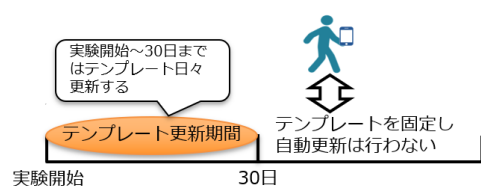


図 5 テンプレートの更新期間

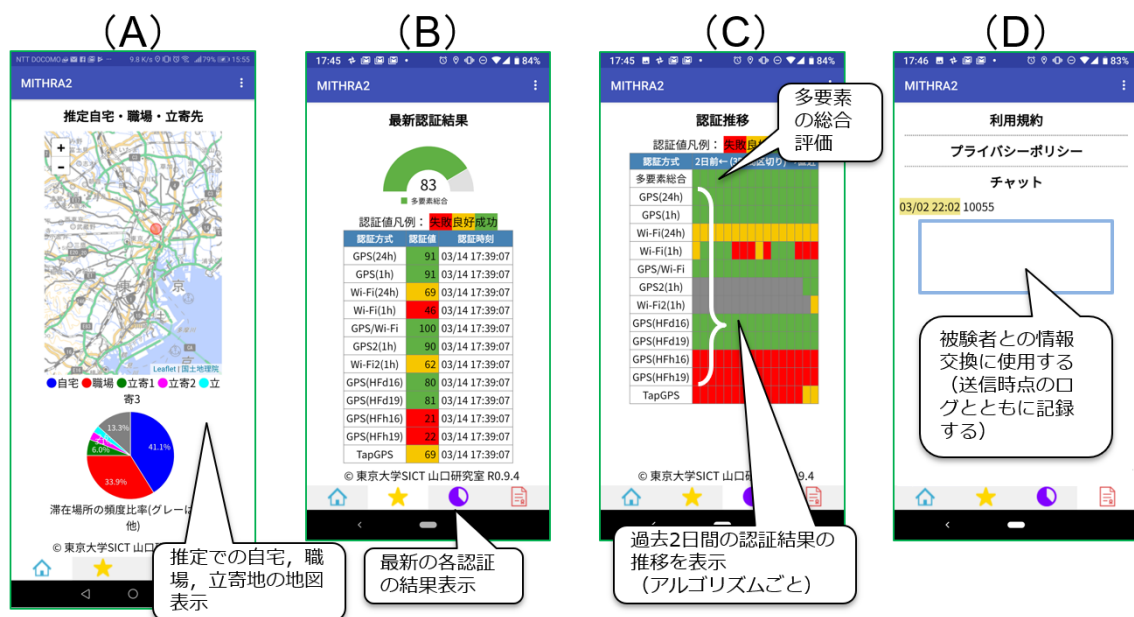


図 6 MITHRA2 アプリの画面

4. 実験の成果

4.1 情報の蓄積

今回実験に使用した iOS および Android スマートフォンの各 15 台ずつから有効なデータが収集された。データの欠落は、端末の設定に起因するもの、電源切れ、通信環境不良等の部分にみられた。これらも含めライフスタイルデータが蓄積された。

ある端末で収集された情報の量的変化の一例を図 7 に示す。GPS の状態や、Wi-Fi や Bluetooth でキャッチした BSSID の捕捉数等、また電池残量も示されている。このグラフにより運用の状況を把握できた。

認証値の状況については図 8 にある被験者の 10 日間の認証変動を示す。ここでは認証アルゴリズムとして、GPS(24h)、GPS(1h)、Wi-Fi(24h) の 3 種の認証値のみを示す。GPS(24h) は安定した認証値が得られるが、短時間の行動変化は把握できないとみえる。一方、GPS(1h) では短時間での場所変化をキャッチすることができる。また Wi-Fi についてはさらに短時間変化が大きいことが捉えられた。

なお、青色破線で囲った土日のデータでは、GPS(24h) も低下がみられた。テンプレートが平日の行動を中心に固定化したことが想定される。

4.2 被験者ヒアリング

被験者の意見をヒアリングしたところ、行動の変化が認証値に即座に反映されることを期待する意見が伺えた。

行動の変化から認証結果の変化への応答性を高めることは、今後の社会実装時に大切であろう。同時に誤認証の可能性も持つと考えられる。これらの意見は認証アルゴリズム

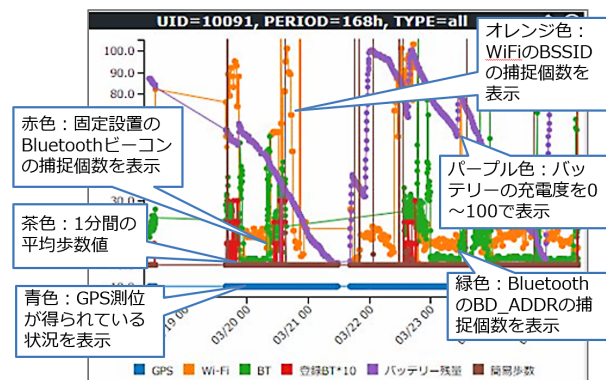


図 7 収集した情報量

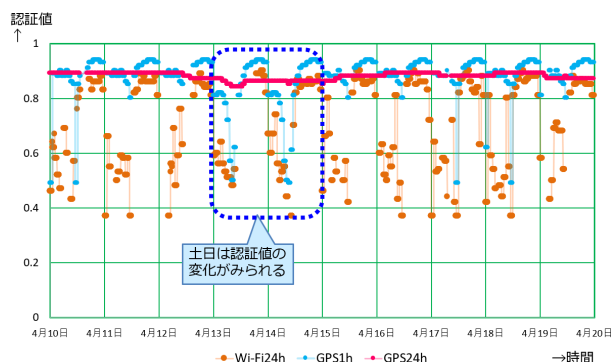


図 8 ある被験者の 10 日間の推移

ムの今後の改善に活かすこととする。

4.3 端末ローテーション

端末所有者の変更を行った場合の認証値の変化を図 9 と図 10 に示す。

図 9 のグラフは、所属会社の異なる 2 人の間で端末をローテーションした場合の認証値の変化を示す。GPS(1h)

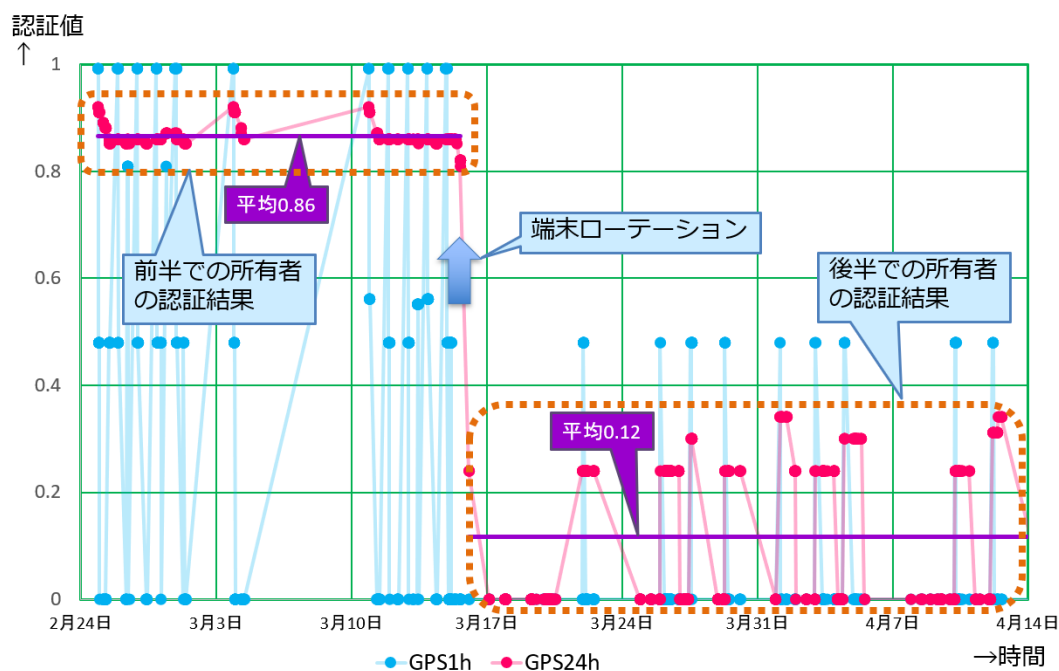


図 9 端末ローテーションの影響 (社間交換)

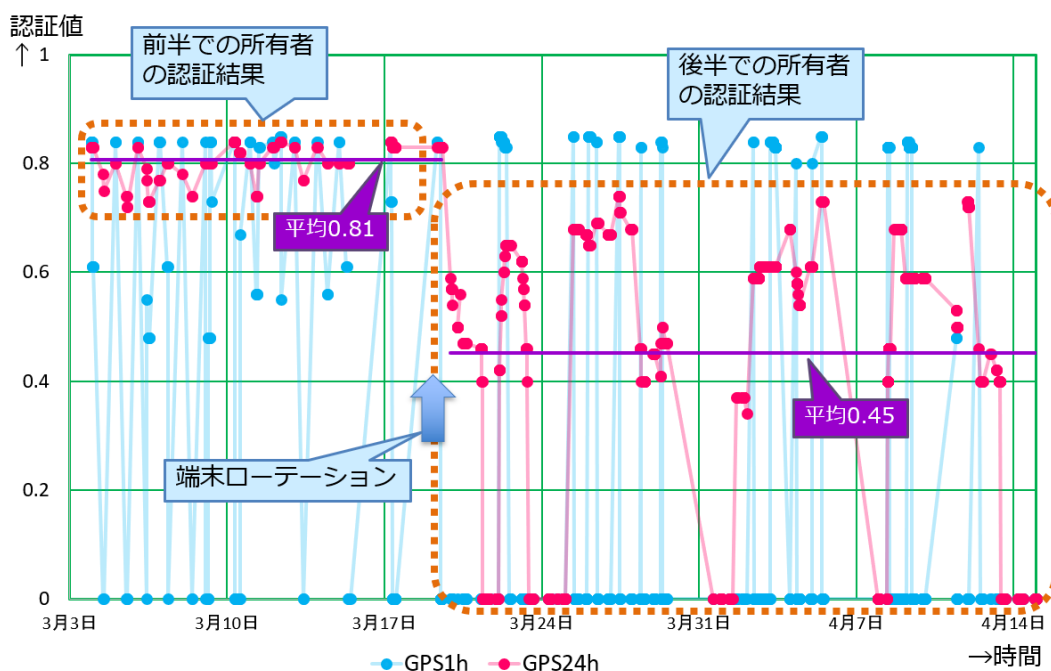


図 10 端末ローテーションの影響 (社内交換)

の値は短時間での変動が大きいので、平均的で安定した値を示す GPS(24h) が示す認証値を比較する。端末ローテーション前（テンプレート作成した人）とローテーション後（本端末のテンプレートとは無関係な人）との間で比較すると、ローテーション前の平均=0.86 がローテーション後の平均=0.12 に低下している。このことから端末の所持者が変わったことが把握できる。

図 10 のグラフは、所属会社が同じ 2 人の間で端末をローテーションした場合の認証値の変化を示す。この場合は、

ローテーション前 0.81 がローテーション後 0.45 に低下している。図 9 の場合と比べ落ち幅が小さいことが分かる。この現象の詳細な分析は今後の研究であるが、同一社や同一組織の場合、業務時間帯での生活圏に重なりが多いと推定され、このことが認証値の落差が小さい理由と想定される。

なお、1 時間単位の位置情報に基づく GPS(1h) については、人の行動変化を敏感に捉えており、この特性を活かして多要素要因として組合せる活用が望まれる。

5. 今後の課題

5.1 端末動作に関する課題

今回の実証実験では、多種類の端末での情報収集を確認するため、貸与版の Android 端末 10 台はすべて機種が異なるスマートフォンを準備した。OS バージョン、メーカーの違いによるトラブルも多発した。

情報収集の障害となった事例を具体的に述べる。経験で得られたノウハウは今後の実験に活用する。

- Android 端末の設定の課題
 - － APN の自動設定問題
 - － SIM ロック解除端末における SIM 限定問題
- Android 端末のアプリ起動設定の課題
 - － 電源の省エネ設定の解除
 - － スリープ時の動作の設定
 - － アプリケーション自動起動への許可
 - － アプリケーション使用時間の制限解除
- iOS 端末のタイマー起動に関する仕様制約

5.2 認証値に関する課題

認証値の分析、被験者からのヒアリングにより幾つかの要望や課題が指摘された。主なものを示す。

- 行動の変化が認証値に反映されるまでに時間を要するタイムラグの課題
- 各認証アルゴリズムの組合せ(多要素)に工夫が必要
- iOS と Android との認証結果の差が生じること

これらは今後の改善につなげる。アルゴリズムの差による部分については被験者にも信頼をもって利用されるための対策が求められる。

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。認証値の時間的変化や、端末所持者を変えた際の影響など、各種の成果と課題を得て、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。

商標等について

本文中で使用した商標等は下記のとおりです。

Android は Google LLC の商標です。

iPhone は Apple inc. の登録商標です。

iOS は Cisco の米国およびその他の国における商標または登録商標です。

参考文献

- [1] 平成 29 年度 我が国におけるデータ駆動型社会に係る基盤整備(電子商取引に関する市場調査), 経済産業省ホームページ <https://www.meti.go.jp/press/2018/04/20180425001/20180425001-2.pdf>
- [2] 平成 28 年版消費者白書、消費者庁ホームページ <https://www.caa.go.jp/policies/policy/consumer-research/white-paper/2016/>
- [3] 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)
- [4] 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).
- [5] 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).
- [6] 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).
- [7] 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).
- [8] 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).
- [9] 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, 日本ソフトウェア学会 第 34 回大会, pp.27-32, [一般 11-3-L](2017).
- [10] 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).
- [11] 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).
- [12] 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)
- [13] 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)
- [14] 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,