

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

鈴木 宏哉¹ 山口 利恵¹

概要: 近年, 実験倫理に対する配慮に注目が集まっており, 特に被験者実験については注意深く実施する事が求められている. 一方で実験実施に関わるセキュリティ, プライバシ保護について詳細に研究報告される事は少なく, この知見を共有する事は研究分野全体の発展に寄与するものとする. そこで本稿では, 著者らが2017年1月から3ヶ月半をかけ実施した5万人規模のライフスタイル認証実証実験における倫理的配慮, 技術的対応について詳細に記す. 本実験ではスマートフォンやウェアラブル端末を用い, 位置情報など個人のプライバシーに結びつくデータを収集した. そのデータ管理や倫理審査, 被験者同意の取得, アプリ審査などについて実事例を紹介する.

キーワード: ライフスタイル認証, 被験者実験, プライバシ保護, 倫理審査

Ethical and Technical Considerations in Lifestyle Authentication Experiment

HIROYA SUSUKI¹ RIE SHIGETOMI YAMAGUCHI¹

Abstract: In recent years ethical consideration is one of the most important things in research field. Researchers are required to manage human subjects experiments carefully. However, there are not many detailed examples of security and privacy considerations related to experiment implementation. In this paper, we describe in detail the ethical considerations and technical countermeasures in the lifestyle authentication experiment that is over a period of three and a half months since January 2017. We collected the location and Wi-Fi network data from smartphone in the experiment.

Keywords: Lifestyle Authentication, Human Subjects Experiment, Privacy Protection, Ethics Review

1. はじめに

1.1 背景

近年, 情報科学の分野では, 情報通信技術の進展, スマートフォン等のモバイルデバイスの普及などによって, 様々な情報を収集する事が可能となってきた. これは社会全体でも高い関心を寄せられており, いわゆるビッグデータと呼ばれるこの多種多様で膨大なデータを収集分析する事で, 新しいサービスや産業が生まれる事が期待されている. 一方で, 収集されるデータには個人情報や個人のプライバシー

に繋がるデータも含まれており, 情報収集者, 情報利用者の慎重な取り扱いが求められている. データの適切な取り扱いの必要性は, 個人情報保護法においても「個人情報の保護に関する基本方針」の中で「1 (1) 個人情報をめぐる状況」に記されており, 社会全般の議論として注目されている [1].

このような情報の取り扱いに対する社会的関心の高まりに応じ, 研究分野においても法令遵守と適切な研究実施が求められている. 他の分野と比べ我々セキュリティ研究者は, サイバー・フィジカル両面で人に関わる研究を多数行っており, 人のプライバシーに繋がる情報を利用して研究する機会も多くなっている. このような人に関わる研究に

¹ 東京大学
The University of Tokyo

において、被験者実験はその評価を行うために不可欠なものである。例えば、金岡のまとめによると 2012 年から 2016 年の SOUPS において 2015 年を除き 9 割以上の論文で被験者実験が行われている [2]。被験者実験では研究者が個人情報や個人のプライバシーに繋がる情報を直接取り扱う機会も多く、特に注意深く実施する必要がある。しかし、多数の被験者実験が行われているにも関わらず、ガイドラインなどは十分に整備されておらず、各研究者がそれぞれの知見や経験、所属組織内のルールなどに基づいて実施しているのが現状である。更に、実験実施に関わるセキュリティ、プライバシー保護について研究論文で詳細に報告される事は少なく、参考となる事例も少ない。そのため、実験実施者の配慮の不足からトラブルになる事例も出ている。

そこで本稿では、著者らが 2017 年 1 月から 3 ヶ月半をかけ実施した 5 万人規模のライフスタイル認証実証実験における倫理的配慮、技術的対応について詳細に記す事でその知見を共有する。国内において同様の規模で個人認証に関わるデータ収集実験を行なった事例はなく、この知見を共有する事は研究分野全体の発展に寄与するものと考え、本実験ではスマートフォンと活動量計を用い、位置情報やアプリの利用履歴、活動量など個人のプライバシーに結びつくデータを収集した。そのデータ管理や倫理審査、被験者同意の取得、アプリ審査などについて実事例を紹介する。

1.2 既存研究と法制度

人を対象とした研究を行う代表的な分野として医療分野があり、古くから被験者に対する配慮に重きが置かれてきた。医学系研究の倫理指針の前文には次のような記載がある [3]。「人を対象とする医学系研究は、研究対象者の身体及び精神又は社会に対して大きな影響を与える場合もあり、様々な倫理的、法的又は社会的問題を招く可能性がある。研究対象者の福利は、科学的及び社会的な成果よりも優先されなければならない。また、人間の尊厳及び人権が守られなければならない。」一方、情報科学の分野はそもそも医療と比べ歴史も浅く、技術的にもユーザインターフェースの研究など被験者への影響が小さい研究に留まっていた。しかし、近年の技術の急速な進展により、人に関わる様々な情報が電子化され収集されるようになった事で、利用者の身体及び精神、そして社会に大きな影響を与え得るようになっていく。そのような社会的背景の中で、EU においては GDPR(General Data Protection Regulation)[4]、日本では個人情報保護法 [5] の検討などで、電子データにおける個人情報とプライバシー保護について議論されてきた。

社会では法制度の整備が進んでいる一方、研究分野では統一的なガイドラインの制定などは進んでいない。情報処理学会の「情報システムと社会環境研究会」が情報システムの評価ガイドラインを出しているが、研究倫理や法令遵守についての言及があるのみである [6][7]。人を扱った実

表 1 実証実験全体の実験参加者数 (重複を含む)

データ種別	収集方法	実験参加者
MITHRA アプリデータ	MITHRA アプリ	16,027
漫画閲覧履歴	マンガワン	7,584
電子チラシ履歴	Shufoo!	33,338
活動量履歴	活動量計 HJA-750C	97
合計		57,046

験を行う上での留意点をまとめたものとして Schechter の論文がある [8]。実験方法を注意深く説明する事、倫理的配慮の説明、倫理審査の承認の有無を明らかにする事などが挙げられている。近年では研究者自身による倫理的配慮だけでなく、Schechter も言及している各研究組織による倫理審査で承認されているかどうか、公正な指針として重要視されるようになっていく。SOUPS2017(Thirteenth Symposium on Usable Privacy and Security) では、全 26 件の発表論文中、19 件で倫理審査の承認に関し言及されている [9]。SOUPS のようなユーザブルセキュリティに関するシンポジウムでは特に関心が高い事が分かる。Nature に掲載された Althoff らが行った実験は、世界 111 カ国 717,527 人の匿名ユーザから 6800 万日分の活動量データを収集した非常に大規模な実験である。この論文にはスタンフォード大学機関審査委員会のガイドラインに従って実施された事が記されている [10]。しかし、Althoff らはガイドラインに従った事は記載しているが、実際に被験者への配慮としてどのような事を行なったのか、データ収集のための詳細な手続きは明記していない。他の論文でも、論文紙面の制約などもあり、多くは倫理審査を受けたという事のみが記載されるに留まっている。社会的な背景もあり分野全体で適切な研究実施が求められている一方、十分な情報が無いの現状である。著者らが行なったライフスタイル認証実証実験において倫理審査の承認を受けるために実施した具体的な対応を共有する事で、議論が行われ、今後の実験実施の参考になる事を望む。

2. ライフスタイル認証実証実験

2 章では、著者らが実施したライフスタイル認証の実証実験の概要について説明する。

2.1 実験概要

著者らは MITHRA(Multi-factor Identification / authentication ReseArch) プロジェクトと名付けた研究プロジェクトにおいて、新たな個人認証技術としてライフスタイル認証を提案し、その評価を行っている [11]。ライフスタイル認証は個人の行動パターンの特徴を利用する事で、特別な操作をする事なく認証が可能な手法である。ライフスタイル認証の有効性を評価するために、大規模な多要素データの収集を目的として実施したのがライフスタイル認証実証実験である [12]。2017 年 1 月 11 日 (水) から 2017

表 2 MITHRA アプリで収集するデータ。○は MITHRA アプリが収集するデータ、△は○の MITHRA アプリと組み合わせてデータを収集。電子チラシ履歴のみ MITHRA アプリデータを提供しない実験参加者がいる

データ項目	収集項目	収集アプリ	データ収集端末	データ収集間隔	備考
端末情報	○	MITHRA アプリ	スマートフォン	5 分間隔 / 移動トリガー	Android / iOS*
IP アドレス	○	MITHRA アプリ	スマートフォン	5 分間隔 / 移動トリガー	*iOS 版は前回測位からの
Wi-Fi	○	MITHRA アプリ	スマートフォン	5 分間隔 / 移動トリガー	大きな移動をトリガー
位置情報	○	MITHRA アプリ	スマートフォン	5 分間隔 / 移動トリガー	としてデータ収集を実行
漫画閲覧履歴	△	マンガワンアプリ	スマートフォン	利用毎	アプリ連携
電子チラシ履歴	△	Shufoo!アプリ	スマートフォン	利用毎	アプリ連携
活動量履歴	△	オムロンアプリ	活動量計	10 秒間隔	活動量計を配布

年 4 月 26 日 (水) までの約 3 ヶ月半の期間でのべ 5 万 7 千人の被験者からデータを収集した (表 1)。実験実施方法、得られたデータの概略 [13]、またそのデータを用いた研究については移動履歴データの特徴 [14]、WiFi 認証 [15] の各論文を参照頂きたい。

2.2 収集データ

表 2 は、収集したデータの種別、データ収集間隔などを記載したものである。実証実験では、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 情報など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) を作成した。その実装については 5 章で詳しく述べる。実験参加者は、Android または iOS 用の MITHRA アプリを自身のスマートフォンにインストールし、普段通りの生活を行う。また、表 2 の通り、MITHRA アプリで収集するスマートフォンデータ以外に漫画閲覧履歴、電子チラシ履歴、活動量計データの 3 種のデータを収集した。漫画閲覧履歴、電子チラシ履歴のデータ収集実験に参加する場合は、各社のアプリ (Shufoo! [16]、マンガワン [17]) をインストールし、普段通りに利用する。Shufoo! は凸版印刷株式会社が提供し、2017 年 8 月時点でユニークユーザ数 860 万人/月、掲載店舗数 10 万 4,000 店、ページビュー数 3 億 PV/月の電子チラシサービスである。マンガワンは株式会社小学館が提供し、2017 年 6 月時点でアプリのダウンロード数が 1,100 万を超える漫画閲覧サービスである。活動量計実験については、MITHRA アプリのインストールに加え、配布する活動量計 (オムロンヘルスケア社製 HJA-750C) を身に付けて実験に参加する。

2.3 実験終了までの流れ

実験実施にあたり、まず研究計画を元に 2016 年 4 月から倫理審査を受け、審査結果の指摘事項を元に、実験計画とアプリ実装の修正を繰り返し、2016 年 9 月に最初の承認を得た (4 章)。その後も、被験者数を増やすために抽選による謝礼手続きを追加したり、活動量計実験でアンケートの実施を追加するなどした際には、変更の申請を行い倫理審査を受けた (5 章)。並行してアプリ実装とアプリ審査

を行い、審査結果に応じた実装変更を行なった。当初、実験開始は Android と iOS 共に 2017 年 1 月 11 日を予定していたが、iOS のアプリ審査が遅れたため、1 月 26 日の開始となった。プレスリリースなどを利用した被験者募集も 1 月 11 日以前を予定していたが、1 月 19 日とした (6 章)。結果的に、実験終了日を 3 月 31 日から 4 月 26 日に延長する事に繋がった。実験開始後はアップロードされるデータの管理、デモンストレーションの実施を行い、4 月 26 日の実験終了後は個人情報を取り除くデータの後処理 (5.4 節) と被験者への謝礼の配布を実施した (6.2 節)。

3. 倫理審査

3.1 東京大学の倫理審査

著者らの所属する東京大学情報理工学系研究科では、次のような「ヒトを対象とする研究」を行う場合、部局が実施する倫理審査の承認を得る必要がある。

- 人を対象とする医学系研究
 - 機器を開発し、人に使用する研究
 - 個人情報の取扱い等、倫理的配慮が必要な研究
- 本実験は「個人情報の取扱い等、倫理的配慮が必要な研究」に該当し、倫理審査の承認の元に実施している。倫理審査では主に下記の項目を文書にて説明した。
- 研究課題 (キーワード、研究従事者)
 - 研究の概要 (目的、方法、実施期間、対象及び収集等、実験参加者の実体験)
 - 研究を実施する施設とその役割 (本学、学外)
 - 研究における倫理的配慮 (インフォームド・コンセント、個人情報保護、資料等の取扱)
 - 安全の確保

また、被験者への説明文書、同意書、同意撤回書についても倫理審査により確認がなされる。通常は紙の書類を用いて説明を行い、その同意を得た旨の署名を同意書に記載頂き実験への参加同意となる。今回の実験では当初より 5 万人規模の大規模実験を予定しており、全被験者から書面の同意を得る事は困難であったため、電子的な説明と同意取得を行なった。詳細は 4 章で述べる。

通常、被験者への説明文書の項目としては、下記のように

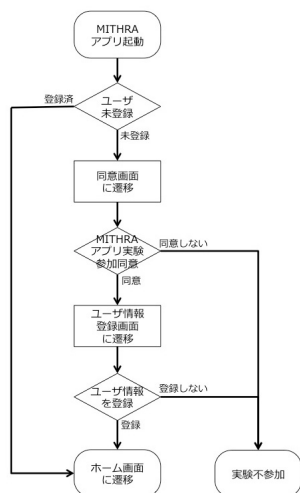


図 1 同意・ユーザ情報登録の流れ



図 2 左図: MITHRA アプリ同意画面 (一部), 右図: ユーザ情報登録画面

な項目があり、それぞれの項目に同意したかのチェックボックスを備えた同意書を用いて同意を得る。今回は活動量計を用いた実験に参加する被験者のみ、MITHRA アプリ上での同意に加え、追加で書面の同意を取得した。同時に、その同意を撤回するための同意撤回書を配布した。

- (1) 研究の概要
- (2) 研究協力の任意性と撤回の自由
- (3) 個人情報の保護
- (4) 研究成果の発表
- (5) 研究参加者にもたらされる利益及び不利益
- (6) 研究終了後の資料等の取扱方針
- (7) 費用負担
- (8) 連絡先

4. 個人情報と同意取得, ユーザ登録

本実験では個人情報保護法に従いデータ取得にあたり全ての実験参加者から本人の同意を得た。

4.1 実験参加に関する同意と辞退

図 1 は、MITHRA アプリインストール後の実験同意とユーザ登録の流れを示したフロー図である。アプリのインストール後、起動時に図 2(左図) のような同意画面が表示される。

MITHRA アプリの同意画面の文言は次の 3 項目からなり、各項目ごとにチェックボックスを設け、3つのチェックボックス全てにチェックを入れた上で「同意ボタン」を押す事で実験参加の「同意」となる。これは個人情報保護法のガイドライン 2-12「本人の同意」にある【本人の同意を得ている事例】の事例 4)「本人による同意する旨の確認欄へのチェック」に相当する [18]。

実験の目的と取得するデータ

このアプリでは、利用者の同一性を確認する、新たな個人認証方式を生み出すための研究のため、以下のデータを東京大学に送信します。

- ・Wi-Fi などの電波センサーのデータ
- ・GPS などの位置情報
- ・IP アドレス、MAC アドレスなどの端末情報

実験期間と公表方法

実験期間は 2017 年 1 月から 3 月までの 3 ヶ月間です。実験期間後のデータは利用しません。みなさまから取得したデータは集計され、統計や解析結果として公表されます。

参加の中止

この実験への参加を中止するためにはアプリの [参加中止] メニューを選択して下さい。この場合、実験終了後のポイントは貰えません。

同意文の作成にあたっては、他のアプリケーションでよく用いられる単一の長い同意文に対して一つの同意ボタンのみの UI ではなく、簡潔に表現した 3つのチェック項目に分け、また画面遷移をさせずに単一のページにまとめるなど、被験者が読み飛ばさないための配慮を行なった。各項目の詳細情報はプライバシーポリシーに記載し、アプリ内と MITHRA プロジェクトのホームページに掲載した [19]。また、実験期間の途中で参加を辞める場合は設定画面から実験参加の中止を行う事で辞退可能とし、辞退者のデータは削除した。MITHRA アプリの実験参加登録者の内、辞退者は 924 名であった。実験の終了日を実験期間中に 2017/3/31 から 2017/4/26 に延長した事で、同意文の「実験期間」とプライバシーポリシーの「取得の予定期間」

表 3 同意の取得方法

データ種別	同意取得方法	同意取得元
MITHRA アプリ	MITHRA アプリの同意画面	東京大学
漫画閲覧履歴	マンガワンアプリ内ページ	小学館
電子チラシ履歴	Shufoo!アプリ内ページ	凸版印刷
活動量計データ	手書き同意書	東京大学

を変更した。なお、同意文書、プライバシーポリシーの作成ではひかり総合法律事務所の板倉陽一郎弁護士にご協力頂いた。

MITHRA アプリ以外のデータ提供についても、表 3 で示した方法でマンガワン、Shufoo!、活動量計実験のそれぞれで実験参加者の同意を取った上で実施している。

4.2 ユーザ登録

図 1 のフローに示した通り、実験参加の同意手順に引き続き、図 2(右図) のようなユーザ登録画面が表示される。実験参加の同意、ユーザ登録の両方が終了しなければアプリのホーム画面に遷移せず、MITHRA アプリはデータを収集しない。

ユーザ登録では表 4 のようにメールアドレスを任意、それ以外を必須項目として、文字入力と項目選択により入力させた。メールアドレス以外については登録内容の確認処理は行なっておらず、被験者の自己申告を登録データとして記録した。メールアドレスの取り扱いについては、5 章で詳しく述べる。性別については、近年のジェンダー議論を考慮し「その他」の項目を設けた。

実験実施後に登録データから確認できた実験設計の問題点として、各選択項目の先頭「男性」「10 代」「北海道」を選ぶ被験者がいた事が挙げられる。DICOMO2017 の報告 [13] では具体的な数値を示していなかったが、本稿でユーザ登録情報、収集データの位置情報、平成 28 年度の人口推計 [20] を用いて比較を行った結果を示す (図 3)。地域の「その他」は 7 件のみだったため割愛する。全体で 16,027 名の被験者が人口比率に比例して全国から参加していた場合、各地域の被験者数の割合は人口推計と一致する。しかし、図 3 の通り「北海道」では 5% も多い事が分かる。ただし、これは偶然、北海道在住の被験者が多かっただけの可能性もある。そこで、収集したデータの位置情報を用いて、その被験者の滞在時間が最も長い都道府県をその被験者の所在地として推定を行った。推定値は 4.5% と人口推定の値に近く、この結果は実際と異なる情報を入力した被験者の存在を示している。各地域の申告値と推定値を比較すると、「北海道」「東北」「九州」が推定値より多くなっている。そのうち「東北」「九州」は 0.4%、0.6% と「北海道」の 5% に比べ小さく、実態との不一致は大部分が「北海道」として入力されている事が分かる。実態に合わない入力を最も多く行っているのが「関東」の被験者で、3.4% も少ない。

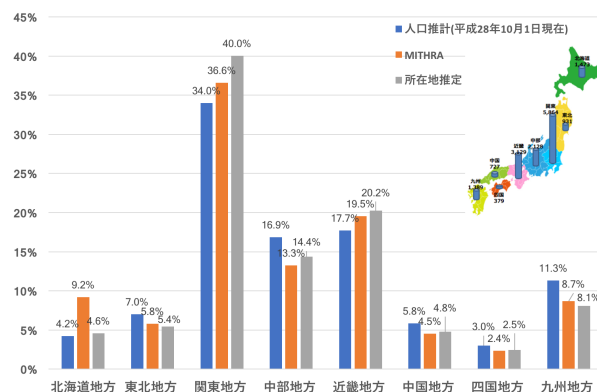


図 3 被験者の居住地域の割合：ユーザ登録による自己申告と所在地推定結果、政府による平成 28 年の人口推定との比較

5. アプリ開発とアプリ審査

5 章では、アプリの実装とアプリストアでの配布のためのアプリ審査、データ管理について説明する。なお、サーバ管理については TIS 株式会社、アプリ作成についてはフェンリル株式会社に委託した。2 社とも本学と共同研究契約を結んでいる。

5.1 アプリ開発

フェンリルによる UI 開発では、青を基調にデザインする事で実験参加者の安心感をもたらすという配慮がなされている [21]。通常、大学などの研究機関による実装ではコストや時間の観点で UI 設計にまで配慮する事が難しく、実証実験成功の一因と考える。トップ画面では、被験者個人の総移動距離と実験参加者全体の総移動距離を表示するように、実験参加者が主体的に参加できるような配慮を行なった。被験者のプライバシーに配慮して実装した機能として、データ収集をオフにする機能がある。データ収集を望まない場合、任意でオフにする事が可能である。被験者が再開の設定を忘れてデータ収集が停止したままになる事が無いように、経過時間を選択式にし一定時間後に再開する実装とした。

5.2 アプリ審査

今回の実証実験では、広く一般の被験者に実験に参加頂くため、Android と iOS の両アプリを作成し、アプリストアでダウンロードできるようにした。公式のアプリストアでダウンロードを可能とするためには、各 OS のアプリ審査で承認を得る必要がある。Android は Google Play デベロッパーポリシーセンター?、iOS は App Store 審査ガイドライン [22] に従って審査が行われる。

ここでは特に Apple の審査に関して述べる。主にパフォーマンスとプライバシーの 2 点に関して指摘を受け、実装の変更を行なった。本実験の目的は履歴情報が認証に有効かどうかを評価するためのデータ収集である。そ

表 4 ユーザ登録画面での入力項目、必須入力項目は○、任意入力項目は△

項目	任意	入力項目・選択肢	備考
ユーザ名	○	文字列 (字種・文字数制限あり、ニックネーム、被験者間での重複可)	アプリ上の表示にのみ利用
メールアドレス	△	文字列 (字種・文字数制限あり)	機種変更、謝礼の連絡に利用
性別	○	男性/女性/その他	性別、年代、お住いの地域は
年代	○	10代 / 20代 / 30代 / 40代 / 50代 / 60代以上	プルダウンメニューにより各項目の
お住いの地域	○	北海道 / 東北 / 関東 / 中部 / 近畿 / 中国 / 四国 / 九州 / その他	左の項目から順に表示される

のため、定期的なデータ収集を行いたいと考えていたが、バックグラウンド処理により定期的な起動はバッテリー消費への影響が大きいという指摘を受けた。Android 版はタイマー起動により定期的にデータを収集するが、iOS 版は Apple のポリシーによりタイマー起動が許可されず、Significant-Change Location Service と呼ばれる前回の測位から大きく位置が変動した場合にコールバックが呼ばれる API の使用を勧められた。そのため、大きな移動や基地局の切り替わりが無いとデータ収集されない実装となっている。結果的に、iOS 版では同じ場所から動かない場合、一度記録された後はデータが記録されないという動作をする。

メールアドレスの入力については、機種変更時のデータ連携、実験終了後の連絡手段として当初、必須項目として実装を行なった。しかし、Apple の個人情報取得の制限により、アプリの機能を実現するためにはメールアドレスが必須では無いという判断があり、任意入力項目に変更した。結果、入力アドレスの確認が不要となったが、一方で誤入力による登録ミスを防ぐためにはメールアドレスの導通を確認する必要がある。そのため、仮登録メールを送付し、登録 URL をクリックする手順に、24 時間の時間制限を超えた場合、自動でメールアドレス欄を空欄にし、メールアドレス未登録のユーザと同じように扱う実装変更を行なった。

位置情報の取得に関しても、その位置情報を何らかの形でアプリの機能に利用しない場合は取得不可と指摘された。データ収集を行う場合、それがユーザに還元されない当初の実装ではアプリ提供者のみの利益となっているとみなされるためである。全実験参加者の総移動距離を算出し協調参加型の機能をトップ画面に実装したり、位置情報を用いたデモ機能を実装するなどユーザ還元の仕組みを加えて、位置情報の取得を可能とした。

アプリ審査では本実験の社会的意義について述べたが、最終的に Apple のユーザ利点を重視する審査方針に従って、個人情報の収集やパフォーマンスに影響のある動作を制限する実装に変更した。

5.3 データ収集とアップロード

予備実験によりデータの収集間隔とアップロード間隔を決定した。データ収集という実験の目的のみを考えると、

データ収集間隔は短い程望ましい。一方で、GPS の位置情報や周辺の Wi-Fi 情報を収集するセンサーを動かし続ける事は、バッテリーの電力消費、計算リソースの消費、ストレージ容量の消費などスマートフォンのリソース消費の拡大に繋がる。リソース消費の大きいアプリはユーザから好まれず、アプリ削除、すなわち実験からの辞退に繋がるため、適切な間隔の決定には十分な配慮を行なった。Android では 5 分に一回、iOS では大きな移動や基地局の切り替わりをトリガーとしてデータ収集を行う実装とした。当初、iOS も 5 分に一回のデータ収集を行う実装としていたが、Apple の実装ポリシーによりトリガーベースの実装となった。詳細は 5.2 節で述べる。Wi-Fi も同様に iOS の制約がある。iOS では、スマートフォン周辺の Wi-Fi アクセスポイント情報へのアクセス権はアプリに与えられておらず、接続されているアクセスポイント情報が取得できるのみである。これは Apple の方針として、アプリの権限を限定する事によりセキュリティを担保しているためである。

また、データのアップロード間隔についてもデータ収集のたびに逐次アップロードする方法や、定期的にアップロードする方法、実験期間終了後に一括アップロードする方法を検討した。スマートフォン内のストレージ容量と通信容量、通信時の電力消費、またスマートフォンの故障によるデータ消失の危険性も加味し、一日一回のアップロードとした。

5.4 外部アプリ、活動量計との連携、匿名化

今回の実験では表 2 の通り、Shufoo! とマンガワンの二つの商用アプリの利用履歴も収集した。各アプリの利用履歴は 2 社が管理するサーバに蓄積されており、それぞれのデータは実験期間終了後に東大側に提供頂く方法を取った。実験参加の同意についても同様で、各アプリ上で参加募集のページを作成頂き、それぞれに同意を取得した (表 3)。各アプリの募集ページのリンクを経由して MITHRA アプリをインストールした被験者の仮 ID を用いて、データの連結を行なった。活動量計の実験ではアンケート収集のため個別に書面の実験同意を取得した。MITHRA アプリの登録時に実験用メールアドレスを登録頂き、メールアドレスと活動量計の ID を対応付ける事でデータの連結を行なった。

収集したデータは最終的に、メールアドレスとメールア

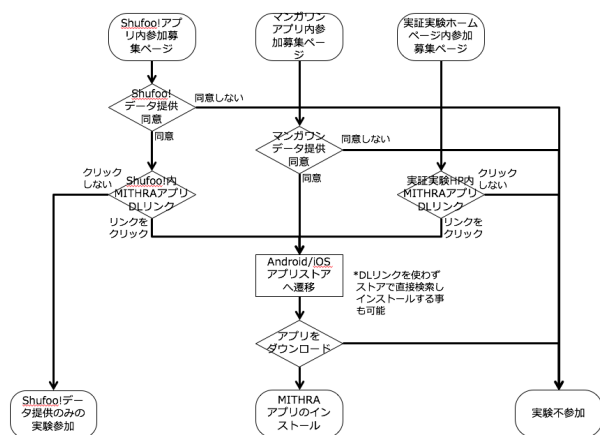


図 4 実証実験への参加の流れ



図 5 アプリ内での実証実験参加募集画面 (例: マンガワン)

ドレス未登録の被験者データを一意に識別するために用いたアプリの UUID を切り離し、別の ID を与える事で匿名化した上で解析に用いている。

6. 被験者募集と謝礼

6 章では、5 万人規模の被験者募集をどのように行なったのか募集方法と謝礼について述べる。

6.1 参加者募集と実験参加方法

図 4 は、実験参加者の募集と実験参加の流れを示した図である。今回の実験参加の募集には大きく 2 種類あり、連携アプリ経由の募集と、それ以外に分けられる。前者は、マンガワンと Shufoo! の各アプリのユーザー向けにアプリ内の告知を使い募集したもので、MITHRA アプリ単独の実験ではなく、連携アプリのデータ収集も含んだ多要素データセットを作成するためのものである。後者は、その他の募集チャネルを利用している。

- MITHRA アプリ

東京大学山口研究室ホームページ、東京大学内ポスター掲示、懸賞サイト等を利用した募集、デモンストレーション実施に合わせた募集など

- マンガワンアプリ内での募集

マンガワンの利用者向けに、MITHRA アプリデータとマンガ閲覧履歴の両方を提供頂く実験参加者を募集

- Shufoo!アプリ内での募集

Shufoo!の利用者向けに電子チラシアプリの利用履歴データを提供頂く実験参加者を募集。マンガワンとは異なり、Shufoo!データのみの提供でも実験参加が可能

図 5 は、実験参加者募集の例としてマンガワンアプリの募集ページを示している。各募集チャネルからの実験参加者数は、表 1 のようになった。

Shufoo!データのみの実験参加者を除き、図 4 の流れは最終的に、MITHRA アプリをダウンロードするため Android または iOS のアプリストアに遷移する。

6.2 実験参加者への謝礼

謝礼には、MITHRA 実験の謝礼に加え、Shufoo!、マンガワン、活動量計実験のそれぞれで謝礼がある。MITHRA 実験の謝礼は景品抽選への参加権で、Shufoo!、マンガワンは各アプリで利用可能なポイントが付与され、活動量計実験についてはモバイルバッテリーを謝礼とした。MITHRA 実験とマンガワンは 27 日以上の実験参加 (当初 30 日以上としていたが、データ収集サーバの障害による停止期間を考慮し変更) を要件とし、Shufoo!と活動量計は実験参加を要件とした [23]。本実験では不必要な個人情報を取得しないように、ユーザ登録では詳細な住所や氏名の入力をさせていない。一方で、日本全国からの実験参加者に謝礼を提供する必要がある、その実施に次のような工夫をした。

MITHRA 実験の謝礼配布の連絡にはメールを用い、本学からは当選した旨と賞品受け取りのための委託業者への連絡方法のみを知らせた。抽選の当選者は委託業者が用意した Web サーバのフォームを用いて必要な情報を知らせ、業者より配送を受けるという方法を取り、これにより東大側に該当被験者の住所・氏名・連絡先情報が渡らないようにした。Shufoo!、マンガワンのポイント付与も各社が実施しており、東大と各社の間では該当被験者の仮 ID のみがやりとりされ、謝礼の配布に関して東大が個人情報を取り扱っていない。活動量計実験については機縁法により被験者募集を行っており、謝礼は実験実施者より配布を行う事で、自宅住所などの個人情報は得ていない。

7. おわりに

近年、実験倫理に対する配慮に注目が集まっており、特に被験者実験については注意深く実施する事が求められている。本稿では、著者らが 2017 年 1 月から 3 ヶ月半をかけ実施した 5 万人規模のライフスタイル認証実証実験にお

ける倫理的配慮, 技術的対応について詳細に記した. 国内において同様の規模で個人認証に関わるデータ収集実験を行なった事例はなく, 実験実施に関わるセキュリティ, プライバシー保護について記した本稿の知見が今後の研究実施の参考となれば幸いである.

謝辞 本論文の研究は, 次世代個人認証技術講座 (三菱UFJ ニコス寄付講座) による.

参考文献

- [1] 個人情報保護委員会: 個人情報の保護に関する基本方針 (参照 2017-8-22), https://www.ppc.go.jp/files/pdf/290530_personal_basicpolicy.pdf (2017).
- [2] 金岡晃: Usable Security & Privacy 研究でのクラウドソーシング利用の現状 (参照 2017-8-22), <https://www.slideshare.net/akirakanaoka/usable-security-privacy> (2017).
- [3] 厚生労働省: 人を対象とする医学系研究に関する倫理指針 (参照 2017-8-22), <http://www.mhlw.go.jp/stf/seisakunitsuite/bunya/hokabunya/kenkyujigyou/i-kenkyu/index.html> (2017).
- [4] Union, E.: General Data Protection Regulation (参照 2017-8-25), http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf (2017).
- [5] 個人情報保護委員会: 個人情報保護法について (参照 2017-8-22), <https://www.ppc.go.jp/personalinfo/> (2017).
- [6] 情報処理学会情報システムと社会環境研究会: 情報システムの有効性評価量的評価のガイドライン 第 1.1 版 (参照 2017-8-22), <http://ipsj-is.jp/works/情報システムの有効性評価手法分科会/量的評価ガイドライン/> (2012).
- [7] 情報処理学会情報システムと社会環境研究会: 情報システムの有効性評価質的評価のガイドライン 第 1.00 版 (参照 2017-8-22), <http://ipsj-is.jp/works/情報システムの有効性評価手法分科会/質的評価ガイドライン/> (2013).
- [8] Schechter, S.: Common Pitfalls in Writing about Security and Privacy Human Subjects Experiments, and How to Avoid Them, Technical report (2013).
- [9] SOUPS: SOUPS2017(Thirteenth Symposium on Usable Privacy and Security) (参照 2017-8-22) (2017).
- [10] Althoff, T., Hicks, J. L., King, A. C., Delp, S. L., Leskovec, J. et al.: Large-scale physical activity data reveal worldwide activity inequality, *Nature*, Vol. 547, No. 7663, p. nature23018 (2017).
- [11] 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).
- [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証実験-MITHRA プロジェクト-, SCIS2017 暗号と情報セキュリティシンポジウム, No. 4D2-1 (2017).
- [13] 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 (DICOMO2017) シンポジウム, No. 1H-2 (2017).
- [14] 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 (DICOMO2017) シンポジウム, No. 1H-3 (2017).
- [15] 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 (DICOMO2017) シンポジウム, No. 1H-4 (2017).
- [16] 凸版印刷株式会社: Shufoo! (参照 2017-8-22), <http://www.shufoo.net/biz/index.html> (2017).
- [17] 株式会社小学館: マンガワン (参照 2017-8-22), <http://manga-one.com> (2017).
- [18] 個人情報保護委員会: 個人情報の保護に関する法律についてのガイドライン (通則編) (参照 2017-8-22), <https://www.ppc.go.jp/files/pdf/guidelines01.pdf> (2017).
- [19] 東京大学ソーシャル ICT 研究センター: ライフスタイル認証実証実験プライバシーポリシー (参照 2017-8-22), http://www.yamagula.ic.i.u-tokyo.ac.jp/mithra/home/privacy_policy.html (2017).
- [20] 総務省統計局: 都道府県別人口 1. 人口の動向 (参照 2017-8-22), <http://www.stat.go.jp/data/jinsui/2016np/pdf/gaiyou3.pdf> (2017).
- [21] フェンリル株式会社: フェンリル、東京大学の「ライフスタイル認証」実証実験に参画 (参照 2017-8-22), <https://www.fenrir-inc.com/jp/news/2017/03/08/lifestyle/> (2017).
- [22] Apple: App Store 審査ガイドライン (参照 2017-8-22), <https://developer.apple.com/app-store/review/guidelines/jp/> (2017).
- [23] 東京大学ソーシャル ICT 研究センター: MITHRA プロジェクト (参照 2017-8-22), <http://www.yamagula.ic.i.u-tokyo.ac.jp/mithra/announce.html> (2017).