MITHRAデータセットでWi-Fi個人認証その1

小林 良輔[1]　山口 利恵[1]

概要：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技術講座では，ライフスタイル認証に関する大規模実証実験 (MITHRA プロジェクト) を 2017 年 1 月〜4 月に実施した．本研究では，この大規模実証実験で収集されたデータセットを，既に提案されている Wi-Fi 情報を利用した個人認証手法に適用し，その結果を検証した．

Wi-Fi User Authentication Using MITHRA Dataset Part I

Ryosuke Kobayashi[1]　Rie Shigetomi Yamaguchi[1]

1. はじめに

近年，スマートフォンやタブレット端末の普及により，ますます EC サイト等のオンラインサービスが利用されるようになっている．オンラインサービスを利用するためには個人認証を必要とするケースがあり，その多くではパスワード認証が使われている．しかしながら，オンラインサービス利用の増加と，利用にパスワードを必要とすることから，サービス利用者にとっては多くのパスワードを記憶しておかなければならないという負担を強いられることとなる．多くのパスワードを記憶できないユーザーは，異なるサービスで同じパスワードを設定することもあるが，このようなパスワード設定はパスワードリスト攻撃など不正ログインの標的となる恐れがある．このように個人認証を多く求められる現代社会では，パスワードを利用した認証手法は利用者にとって安全性やユーザビリティの観点で有用とは言えなくなってきている．

ワンタイムパスワードや乱数表を用いた認証手法など，パスワードの認証以外の個人認証手法もこれまで提案され利用されてはいるが，広く普及するところまでには至っていない．これらの認証手法が普及しないのは，サービス提供者側はに認証方式を変更することで利用者が負担に感じ，利用者がサービスから離れていくことを恐れていることが原因の一つである．最近では生体情報を活用した認証手法も使われてきてはいるが，生体情報を読み取るためのセンサーが必要であったり，写真から指紋情報を読み取るなどの攻撃手法が存在するなどの問題点が指摘されている．様々な認証手法が提案されてはいるが，社会はいまだに安全性やユーザビリティの高い認証手法を必要としている．

こういった中でライフスタイル認証という新たな認証手法が着目されている．ライフスタイル認証では人の生活リズムにおける行動パターンから個人の特徴を抽出し，個人認証に活用している．IoT(Internet of Things) 時代と呼ばれる現在では，容易に人の生活行動情報を採取し，デジタルデータとして記録することができる．ユーザーが普段から携帯しているスマートフォンやウェアラブル端末は多数のセンサーが搭載されており，周辺の電波情報やユーザー自身の運動情報などが採取されている．このような情報を活用した個人認証手法が既存研究として提案されている．

しかしながら既存研究では，十分な被験者数で実験・評価が行われていない．ライフスタイル認証で利用する行動情報はプライバシーに関する情報であり，研究に利用できる十分なデータが存在しなかったためである．そこで我々はこの問題を解決するために，大規模データ収集を目的とした実証実験（MITHRA プロジェクト）を行った．本研究では既存研究で提案された認証手法を，実証実験で収集したデータを用いて評価することを目的とする．特に認証手法としては，スマートフォンで取得する Wi-Fi 情報を活用する認証手法を対象とした．

[1] 東京大学大学院情報理工学系研究科

1.1 論文の構成

本論文は以下の通りに構成されている．2 章ではライフスタイル認証の概要について説明する．特に本実験で利用した Wi-Fi 情報を利用した認証手法については，詳細を説明する．3 章では，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技術講座で行われた大規模実証実験について説明する．4 章では，本研究で行った実験及びその結果について説明する．5 章では，実験結果についての考察や，本実験で利用した Wi-Fi 情報と，位置情報の関係について考察する．6 章では本論文の結論の今後の課題について記述する．

2. ライフスタイル認証

本章では近年提案された，ライフスタイル認証という新しい個人認証手法について概要を説明する．ライフスタイル認証とは，人間の行動パターンから得られる個人特性を利用した個人認証手法である [1]．人間の行動パターンはライフログと呼ばれる電子データを解析することで得られることができる．ライフログとは人間の生活履歴を電子データとして記録したものである．IoT 時代と呼ばれる昨今では身近な様々な機器にセンサーが搭載されており，人間の行動が自動的に記録されている．例えばスマートフォンには GPS や電波センサー，加速度センサーなどが搭載されており，スマートフォンを携帯しているだけでそのユーザーのライフログが自動的に収集・記録される．

このようにして得ることのできる人間の行動パターンには，個人性があり認証に活用できると考えられている．

2.1 Wi-Fi 情報を利用した個人認証

本節では Wi-Fi 情報を利用した個人認証手法に関する既存研究の紹介，スマートフォンが取得する Wi-Fi 情報の特徴，および個人認証手法の概要について説明する．

2.1.1 Wi-Fi 認証に関する既存研究

Wi-Fi 情報を利用した個人認証に関する既存研究に [2][3][4][5] などがある．[2] ではスマートフォンが取得する，スマートフォン端末周辺の無線 LAN アクセスポイントの履歴情報を活用した個人認証手法を提案している．この手法では 30 日分のデータを利用して個人ごとのテンプレートを作成し，1 日 (24 時間) 分のデータを認証情報としてテンプレートと比較をしている．

また [3] では 1 時間分のデータを認証情報としてテンプレートと比較している．1 時間での認証は 24 時間での認証と比べると精度が悪くなる結果となっている．ただし 1 時間での認証は昼間と夜間で精度に大きな差があり，ユーザーによっては夜間では 100% 認証に成功しているケースもある．

[5] でも 1 時間分のデータを認証情報とした実験を行っているが，[3] と比べて実験被験者数が増加している．[3] では実験被験者を 17 人で実施しているが，[5] では 47 人で実験を行っている．被験者数が増えても精度はほとんど変わっておらず，Wi-Fi 情報を利用した個人認証手法の有用であることを述べている．

無線 LAN アクセスポイントの履歴情報以外に，電波強度も活用した認証手法が [4] で提案されている．電波強度を活用することで，仕事や研究で普段同じ部屋にいる人同士でも認証精度を上げることができるとしている．また 1 時間の認証は 24 時間の認証と比べて精度が悪くなるが，[4] では平日・休日のパラメータを追加することで，条件によっては 1 時間での認証も可能であると述べている．

2.1.2 Wi-Fi 情報の特徴

2.1.1 節で述べた通り，既存研究ではスマートフォンが取得した無線 LAN アクセスポイントの履歴情報を個人認証に活用している．本節ではスマートフォンが取得する Wi-Fi 情報の特徴について説明する．

ライフスタイル認証は人間の生活における行動パターンを活用した認証手法である．Wi-Fi 情報を活用した認証手法もライフスタイル認証の一要素として考えられ，同様に行動パターンを活用している．この人間の生活における行動パターンは日々似てはいるが，まったく同じというわけではない．人間の行動にはゆらぎが存在するのである．

スマートフォンが取得する Wi-Fi の情報には，人間の行動のゆらぎが二つの面で表現される．一つ目は Wi-Fi 情報を取得する時間のゆらぎである．人は毎日同じような行動をしていても，時間がずれるということがある．この時間のずれは Wi-Fi 情報を取得する時間に表れることとなる．

二つ目は同じ Wi-Fi 情報を取得する頻度のゆらぎである．人の行動にはよく行うものもあれば，たまにしか行わない行動もある．よく行う行動時に取得する Wi-Fi 情報は取得頻度が高く，たまにしか行わない行動は取得頻度が低いというように，行動のゆらぎは Wi-Fi 情報の取得頻度に表れることとなる．

このように人間の行動にはゆらぎが存在するため，行動パターンを活用する個人認証手法はこのゆらぎを吸収するものでなければならない．特に Wi-Fi 情報を利用した個人認証手法においては，時間のゆらぎと取得頻度のゆらぎを吸収する必要がある．

2.1.3 Wi-Fi 認証手法概要

Wi-Fi 情報を利用した個人認証手法の概要を図 1 に示す．以下，この内容について説明する．

Wi-Fi 情報を利用した個人認証手法には登録モードと検証モードの二つのモードからなる．二つのモードの流れとしては，登録モードではテンプレートが作成され，検証モードでは入力された認証情報とテンプレートの比較が行われ，認証の合否を判定する，といったものである．

登録モードで作成されるテンプレートは 30 日間のデータを元に作成される．2.1.2 節で述べたように，Wi-Fi 情報

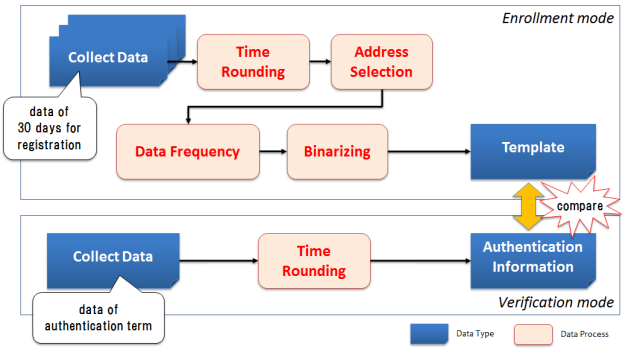

図 1　Wi-Fi 認証手法データ処理

を利用した個人認証手法は時間のゆらぎと取得頻度のゆらぎを吸収する必要があり，そのためにテンプレートは 30 日間のデータからゆらぎ吸収のための処理が施されて作成される．時間のゆらぎ吸収のためには時間丸めの処理が行われ，取得頻度のゆらぎ吸収のためにはアドレス選定・濃淡付与処理が行われる．ゆらぎ吸収のための処理が行われた後，認証情報との比較を行うために，二値化処理が行われる．

検証モードではテンプレートと比較するための認証情報が作成される．認証情報は [2] では 24 時間のデータを元に作成することが提案されているが，[3] などでは 1 時間のデータから作成することも提案されている．既存研究の実験結果では 24 時間のデータを元に作成した認証情報がより高い精度を出しており，本論文での実験では 24 時間のデータを元に認証情報を作成する．このように作成された認証情報をテンプレートと比較し，一致率を算出する．一致率があらかじめ定められたセキュリティパラメータ k より大きい場合には認証成功と判断する．

3. MITHRA プロジェクト

本章では，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技術講座で行われた大規模実証実験について説明する．なお，本論文では概要の説明にとどめる．詳細については [6] を参照されたい．

この大規模実証実験は MITHRA プロジェクトとよばれ，ライフスタイル認証の研究に関わる様々な大規模データ収集を目的として，2017 年 1 月 11 日〜4 月 26 日に実施された．Web サイト等で実験協力者の募集が行われ，全体で延べ人数，約 5 万 7 千人が実験に参加した．図 2 は実験協力者募集の様子である．(https://www.yamagula.ic.i.u-tokyo.ac.jp/mithra/announce.html)

データ収集はいくつかの手段によって行われたが，そのうちの一つは，同講座が用意した MITHRA アプリというスマートフォンアプリによって行われた．希望者は自分が所有しているスマートフォンに MITHRA アプリをインストールし，実験参加に同意，ユーザー情報を登録することで実験に参加することができ，MITHRA アプリをインストールしたスマートフォンを常時携帯することで，ユーザーの行動情報がサーバにアップロードされた．MITHRA アプリがアップロードするデータはスマートフォンに搭載されているセンサー類が取得するものであり，GPS が取得する位置情報，Wi-Fi センサーが取得する Wi-Fi 情報が含まれている．本研究ではこのうちの Wi-Fi 情報を利用している．

MITHRA アプリをインストールして大規模実験に協力したユーザーは 16,027 人であり，そのうち Android ユーザーは 1,391 人であった．本論文で実施した実験では Android 端末にインストールされた MITHRA アプリが収集したデータを活用した．

4. 実験

本章では MITHRA プロジェクトで収集したデータを用いて Wi-Fi 個人認証手法を検証した実験について説明する．なお認証手法については，2.1 節で紹介した手法を用いた．

4.1 データセット

本節では実験で利用したデータセットについて説明する．

4.1.1 データ収集仕様

本実験で用いたデータは Android 版の MITHRA アプリで収集されたデータである．Android 版 MITHRA アプリは 5 分ごとにデータを収集し，1 日に一度サーバへ収集したデータをアップロードする．収集する Wi-Fi に関するデータには，Wi-Fi ルータの SSID (Service Set Identifier)，BSSID (Basic Service Set Identifier)，受信した電波強度，および受信した日時が含まれている．この中で実験に利用したのは BSSID と受信した日時である．

4.1.2 データ選定

Android 版 MITHRA アプリで収集されたデータから以下の方法で実験に利用するデータを選定した．

- 対象ユーザー
  まず Android 版 MITHRA アプリをインストールしたユーザー 1,391 人のうち，30 日以上実験に参加した 772 人を選定した．その中からさらにランダムで 100 人を選定し，本実験の対象ユーザーとした．
- 対象日実験対象としたユーザー 100 人は，MITHRA プロジェクト参加期間がそれぞれ異なるため，それぞれの参加期間のうち最初の 30 日に収集されたデータを本実験での利用対象とした．

4.2 実装

本実験では 30 日間のデータを対象としたが，その 30 日

図 2　大規模実証実験募集

間のデータを用いてテンプレートの作成を行った．また 30 日間のそれぞれの 1 日分のデータを認証情報としてテンプレートの比較を行った．セキュリティパラメータには $k = 0.01$ を設定した．

4.3　実験結果

本実験では本人受入率 (TAR) と他人受入率 (FAR) について評価を行った．本実験における TAR および FAR の定義は以下の通りである．

- 本人受入率：認証成功回数 / 本人認証試行回数
- 他人受入率：認証成功回数 / 他人認証試行回数

また一人あたりの本人認証試行回数および他人認証試行回数は以下の通りである．

- 本人認証試行回数：本人 (1 人) × 日数 (30 日) = 30 回
- 他人認証試行回数：他人 (99 人) × 日数 (30 日) = 2970 回

本実験の結果は表 1 と図 3 の通りである．表 1 ではユーザー 100 人に対する本人受入率と他人受入率それぞれの，最大値，平均値，最小値を表している．図 3 ではユーザーごとの本人受入率と他人受入率を表している．これらを見ると，大多数のユーザーにとって精度の高い結果となったことがわかる．他人受入率も非常に低いことから，Wi-Fi の情報は個人の特徴を強く表し，また他人と異なっているということがわかる．

表 1　実験結果

	最大値	平均値	最小値
本人受入率	1.000	0.932	0.033
他人受入率	0.043	0.001	0

また，図 4 は本人受入率のヒストグラムである．この図からも大多数のユーザーにとって精度の高い結果となったことがわかる．実際に 100 人中 87 人のユーザーの本人受入率が 0.9 以上となった．

一方で少数のユーザーは本人受入率が非常に低い値となる結果となった．特に 1 人のユーザーは本人受入率が 0.033 と，ほとんど本人認証試行に失敗している．この通り，Wi-Fi を利用した個人認証手法は，高い精度を出す一方で，一部のユーザーにとっては適用できないということがわかる．

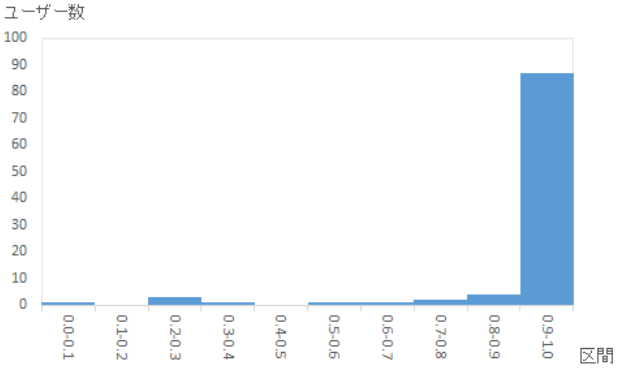

図 4　TAR のヒストグラム

5.　考察

本章では本実験結果の考察を，既存研究での実験結果と比較しながら行う．

5.1　既存研究との比較

既存研究 [2] での実験結果は表 2 と図 5 の通りである．この値は本実験と同様，セキュリティパラメータを $k = 0.01$ と設定した時の結果である．

表 2　既存研究の実験結果

	最大値	平均値	最小値
本人受入率	1.000	0.901	0.088
他人受入率	0.182	0.075	0

本人受入率を見ると，既存研究よりも本実験の方が精度が高くなっていることがわかる．実験対象ユーザー数が 17 人から 100 人と増えても高い精度を確保することができており，実験で適用した個人認証手法が特定のユーザー群にのみ有用というわけではなく一般に利用できるという

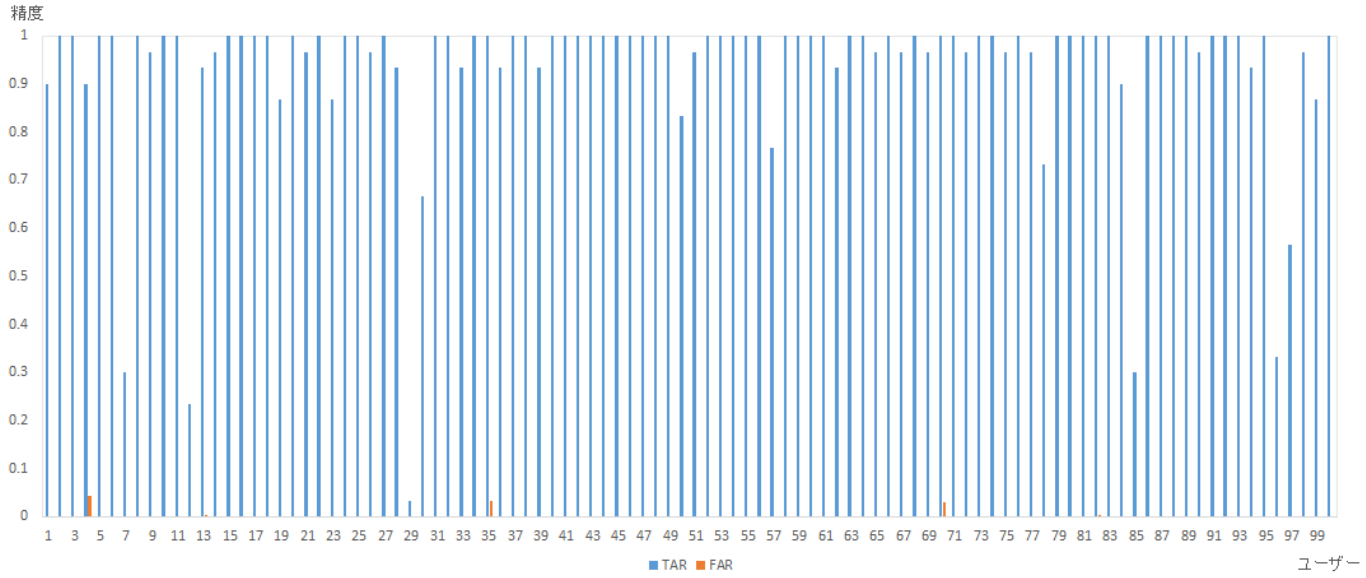

図 3 ユーザーごとの TAR と FAR

ことがわかる．ここで一般に利用できるというのはすべてのユーザーにとってこの認証手法が有用という意味ではない．最小値を見ると本実験の結果も既存実験の結果も非常に低く，Wi-Fi 認証手法が適さないユーザーがいることがわかる．

また他人受入率を見ても既存研究の結果の方が値が高く，本実験での結果の方が精度が高くなっていることがわかる．既存研究で他人受入率が高くなったのは，既存研究での実験被験者の多くが東京大学の学生や職員であることから，行動パターンが似通っていたことが原因と考えられる．本実験では実験対象者を一般に募集したため，行動パターンが似ている人が少なく，他人受入率が低くなったと考えられる．

5.2 Wi-Fi 認証の適用アプリケーション

図 6 は本実験におけるセキュリティパラメータ k を変化させたときの本人拒否率 (FRR=1-TAR) と他人受入率を表している．一般的に k を増加させていくと FRR は増加し，FAR は減少していくので，FRR=FAR となる値を ERR (Equal Erroe Rate) として認証精度の指標とすることが多い．しかしながら本実験では図 6 で見れるように，k を小さくしても FAR が非常に低いため FRR=FAR となる k が存在しない．この結果から Wi-Fi 情報を利用した個人認証手法は，低い FAR が求められるようなアプリケーションに利用できると考えられる．

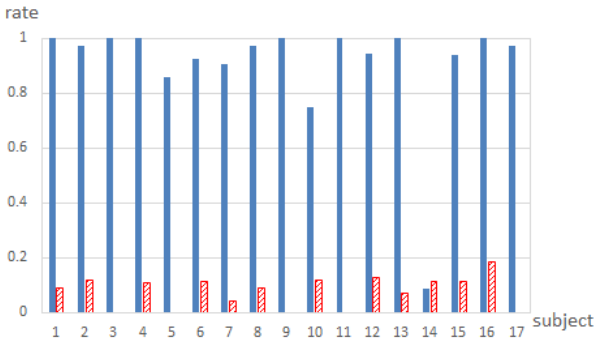

図 5 既存研究におけるユーザーごとの TAR と FAR

6. おわりに

本論文では既に提案されているスマートフォンが取得する Wi-Fi 情報を利用した個人認証手法に，MITHRA プロジェクトで収集したデータの中から 100 人分のデータを選定し適用させた．その結果，既存研究より精度の高い結果となり，提案されている個人認証手法の有用性が確認できた．

MITHRA プロジェクトでは Wi-Fi 情報にかぎらず位置情報等も収集している．今後は Wi-Fi 情報に加えて位置情

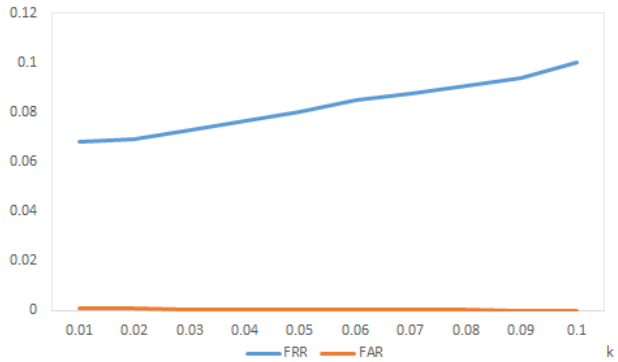

図 6 閾値を変化させたときの FRR と FAR

報などの他の情報とも組み合わせて個人認証実験を行い，精度を上げていくことが課題である．

参考文献

[1] 小林良輔，山口利恵: ライフスタイル認証におけるゆらぎ吸収を目的としたテンプレート更新手法の提案，コンピュータセキュリティシンポジウム 2016 論文集,2016(2), pp.1291-1298 (2016).

[2] RYOSUKE KOBAYASHI, RIE Shigetomi YAMAGUCHI: A Behavior Authentication Method Using Wi-Fi BSSIDs around Smartphone Carried by a User, Computing and Networking (CANDAR), 2015 Third International Symposium on. IEEE, 2015.

[3] 小林良輔，山口利恵: Wi-Fi 履歴情報を活用した複合認証における個人認証手法，コンピュータセキュリティシンポジウム 2015 論文集 2015.3 (2015): pp.889-896.

[4] 平岩啓，満保雅浩: 無線 LAN 情報の認証への応用の検討，電子情報通信学会論文誌 D 99.10 (2016): 1034-1044.

[5] RYOSUKE KOBAYASHI, 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.

[6] 鈴木 宏哉, 小林 良輔, 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 1H-3 (2017).