「マルチメディア，分散，協調とモバイル
(DICOMO2021) シンポジウム」 令和3年6月-7月

ライフスタイル認証の攻撃耐性に関する実験報告

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．
2019 年 1 月～4 月に行った実証実験 2019（その 1）においては他人からの攻撃モデル（スマートフォンが他人に窃取され，本人に成りすまし使用を継続する想定）を設定し行動データを収集した．有効なデータが収集できたスマートフォン 15 台のデータをもとに，端末種別・認証アルゴリズム・攻撃者の属性（元の所有者と行動パターン類似性の大小）などの諸条件で分けて認証値データの分析を行った．この結果，攻撃後の認証値が低下する状況と攻撃が検出されるまでの時間を計測した．本論文ではここで得られた結果をまとめた．これらをライフスタイル認証の今後の研究と社会実装に役立てる．

Experimental Report on Attack Resistance of Lifestyle Authentication

NOBUO SHIGETA[1] RYOSUKE KOBAYSAHI[1] NOBUYUKI SAJI[2]
RIE Shigetomi YAMAGUCHI[1]

1. はじめに

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進展している．これらのサービスを利用するにあたって，本人性を確認する個人認証技術の必要性が高まっている．

現在もっとも多く利用されている認証手法の一つとして ID/パスワードの利用，生体認証の利用等があるが，ユーザーの負担や利便性の課題も指摘される．この解決のため，人の生活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”を提案してきた．（図 1 参照）[1][2]

MITHRA (Multi-factor Identification / authentication ReseArch) プロジェクトでは，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て，リテラシーに頼らない個人認証や個人毎の行動支援，個人向けサービス提供などの実現を目指してきた．

2017 年の 1～4 月には，5 万人規模の実証実験を実施し，2019 年 6 月～8 月にライフスタイル認証・解析の実証実験（商品販売・決済モデル)を実施した．これまでの実験では認証精度の向上や，実サービスへの適応性（実際の決済システムとの連携）を評価してきた．

一方，実験では被験者がスマートフォンにより行動データを収集しサーバで解析する方式をとっており，スマートフォンの盗難や他人との貸し借りといった事象に対してライフスタイル認証の耐性の確認も進めてきた．

本論文では，被験者が持つスマートフォンを実験途中で他の被験者から攻撃（窃取）された状態（自分のスマートフォンが他人に使われる状況）をつくりだし，その前後で収集される行動データや認証値にどの様な変化が見られるかについて分析したのでこれを報告する．

図 1 第 4 の認証要素としての「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.

2. 関連研究

既存研究として 2017 年に実施した実証実験 2017，および実証実験 2019（その 1） について述べる[3][4][5][6][7].

2.1 実証実験 2017

2.1.1 概要

MITHRA プロジェクトにおいて，2017 年 1 月から約 3 ヶ月半の期間，実証実験 2017 を実施した．スマートフォンの各種センサー等を用いて，位置情報や Wi-Fi 電波情報，アプリの利用履歴情報と言った行動データの収集と蓄積を目的とした．このためにスマートフォンアプリ（MITHRA アプリと呼ぶ）を開発し，得られた各種情報の分析を進めてきた.

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.

後続の社会実装を進めるうえで，行動の特徴を捉えるデータ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.

実験概要および諸元について表 1 に示す.

2.1.2 主な成果

実験から得られた主な成果を下記に示す[8][9][10][11].

- 認証に向けた分析アルゴリズムの開発
  - 位置情報ベース（例：時間ごとの存在位置を評価）
  - 環境情報ベース（例 : Wi-Fi，Bluetooth の類似性を評価）
- データの可視化
  - 位置情報（例：推定自宅，推定職場等）の変化
  - 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

表 1 実証実験 2017 の概要

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	・端末情報 ・行動データ（位置情報，活動量データ） ・環境データ（Wi-Fi，Bluetooth 等） ・アプリ利用データ

2.2 実証実験 2019（その 1）

2.2.1 概要

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．[12]

目的は, 行動データの安定的に収集し, 認証システム（サーバ側）およびデータ表示（端末アプリケーション）の相互連携を確認すること，多様な端末（ iOS 端末，Android 端末 ）での運用を確認すること，被験者の行動データを的確に収集することである.

特に，実験途中でスマートフォンの所持者を変更し，攻撃（盗難／窃取）状況を想定したデータ収集も行った.

実験概要および諸元について表 2 に示す.

表 2 実証実験 2019（その 1）の概要

期間	・iOS： 2019 年 1 月 11 日～4 月 15 日 ・Android： 2019 年 1 月 29 日～4 月 15 日
被験者	30 人（本研究を実施した社会連携講座の関係者に限定した）
手段	スマートフォン（30 台）から収集 （iOS、Android、各 15 台）
収集データ	・端末情報（バッテリー残量（%）） ・行動データ（位置情報：緯度・経度・精度，アクティビティ情報： 歩数に相当） ・環境データ（Wi-Fi 情報：補足した BSSID，Bluetooth 情報： 補足した BD_ADDR）

2.2.2 認証アルゴリズム

認証アルゴリズムは位置情報（GPS 等）に基づくもの，環境情報（Wi-Fi, Bluetooth 等）に基づくものなど 11 種類の要素を使用した[13].

2.2.3 主な成果

使用したスマートフォンの 30 台から有効な行動データが収集された．最新の認証結果を得るための，行動データの随時送信や，サーバと端末アプリの連携動作（認証結果の端末への表示）も確認できた．また各種の認証アルゴリズムを評価し，位置情報や Wi-Fi 情報の有効性について確認できた.

3. 攻撃耐性に関する実証実験

3.1 目的と概要

3.1.1 実験の目的

実験で収集する行動データ（位置情報，Wi-Fi 情報等）の変化を分析し，攻撃（スマートフォンを窃取した別人が本人になりすましを行う想定）に対する耐性（検出の実現性，検出にかかる時間等）を確認する.

3.1.2 実施時期と被験者

本実験は 2019 年の 1 月～4 月に実施した実証実験 2019（その 1）のデータを用い，攻撃を実施した端末のデータを抽出し，攻撃耐性の観点から分析した．この実証実験では被験者全 30 名のうち 20 名（端末 20 台）が攻撃耐性の確認実験に参加した．継続的に有効なデータが得られたのは最終的に 15 台であった.

3.2 認証値について

3.2.1 アルゴリズム

攻撃実験モデルでは2つの認証要素とアルゴリズムを使用して認証値を判断した．

- GPS24h: 位置情報に基づき，現在の位置情報と標準的な行動パターン（テンプレート）とを比較し 24 時間のタイムウィンドウで類似性を判定するアルゴリズム．
- Wi-Fi24h: Wi-Fi の基地局の情報（BSSID）に基づき，現在の受信エリアの Wi-Fi 情報と標準的な行動パターン（テンプレート）とを比較し 24 時間のタイムウィンドウで判定するアルゴリズム．ただし攻撃耐性の評価においては，接続していない周辺 Wi-Fi の情報リストも収集できる Android 端末のデータのみ活用した．

3.2.2 行動の学習（テンプレートの作成）

被験者の通常の行動パターンを学習しテンプレートを作成する．これには経験的に実験開始後 3 週間以上の学習期間が必要と分かっている．今回の実験でも 3 週間以上（平均 30 日以上）の学習期間をとり，信頼できるテンプレートを作成した．

3.2.3 具体的なテンプレートの作成方法

GPS24h（GPS データによるタイムウィンドウ 24 時間の場合）を説明する．（図 2 参照）

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．この例では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．

Wi-Fi24h の場合も GPS の場合と同様に，時間帯別の Wi-Fi 基地局の情報（BSSID）を記録し，確率を求めたものがテンプレートとなる．

3.2.4 現在の認証値の決定方法

認証値の判定を行う場合，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，タイムウィンドウ 1 時間の場合認証値（つまりテンプレートとの類似度）は 0.6 となる．

GPS24h では，図 2 の左側にあるように過去 24 時間分のテンプレートの類似度の移動平均をとって認証値を決定する．

Wi-Fi24h の場合も同様に，1 時間のタイムウィンドウでの類似度を算出し，この 24 時間の移動平均をとり 24 時間のタイムウィンドウの認証値を得る．

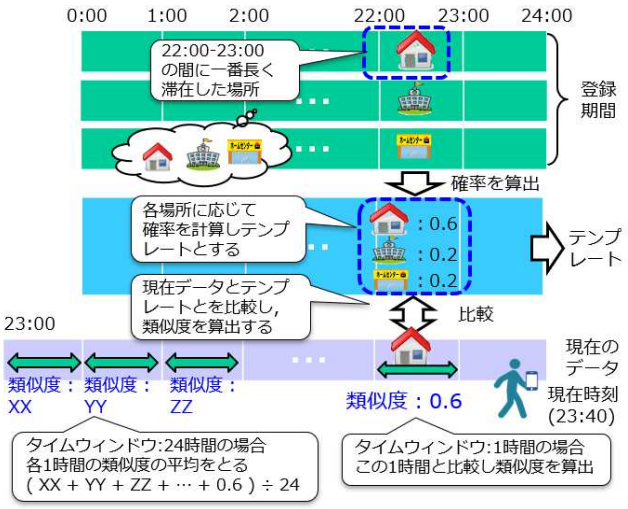

図 2 テンプレート作成と認証値の決定

3.3 端末機種の違いによる収集データの違い

実験に使用したスマートフォンには，Android 端末と iOS 端末を使用した．

OS の機能の差によりデータ計測アプリには次に示す機能差が生じる．データの内容や密度が異なるため，端末機種の違いを考慮してデータ収集を行った．

- Android 端末の場合：5 分に一回，周期的に位置情報（GPS 等）や Wi-Fi データなどのセンサデータを計測する．また Wi-Fi 基地局に接続していない状況でも近辺で観測された基地局情報（BSSID のリスト）を収集することが可能である．

- iOS 端末の場合：仕様上，定期的な（上記の 5 分間隔での）データ収集ができない．このため位置情報などの変化があった時をトリガとしてデータ収集する．このためデータ収集タイミングがコントロールできず，情報密度がばらついたデータとなる．また Wi-Fi 情報については近辺の基地局情報は収集できず、実際に接続した基地局情報だけを収集できる．このため Wi-Fi から得られる情報が Android 端末に比べ大幅に少ないものとなる．

これらの違いが生じるため、データは分析の際，機種の差を区別して取り扱う必要がある．

3.4 攻撃モデル

想定する攻撃モデルは，「端末の盗難／窃取」である．本来の端末所持者によるテンプレートの学習期間が終了した以降，端末が正常動作することを確認したのち，そのまま攻撃者（他人）が同一端末を窃取し使用を継続する状況を作り出す．つまり攻撃者が本来の端末所持者になりすますことの可能性，言い換えるとなりすましが失敗することの確認を行う．

図 3 2 つの攻撃モデル（攻撃者の違い）

前提として被験者（本来の端末所有者と，攻撃後にこの端末を所有する攻撃者）はいずれも社会人（月～金の昼間時間帯に職場にて就業している）ものとする．

攻撃者の種類により次の 2 つの攻撃モデルを設けた．（図 3 参照）

- 自社内攻撃モデル： 生活圏が近い人物による窃取が行われるモデル（同一社の社員，または同一オフィスに勤務する社員が端末を窃取し使用を続けるモデル）
- 他社からの攻撃モデル： 生活圏が異なる人物による窃取（所在地が異なる会社の社員が端末を窃取し使用を続けるモデル）

この設定では，自社内攻撃モデルの方が両者の生活圏が近いことから認証値（本人との類似度）が高まる機会が多く，本人と攻撃者の認証値による識別の難易度が高いと想定できる．

3.5 攻撃の検出

端末が元の所有者と異なる他人に使用された場合，ライフスタイルが異なるため，当然認証値は低下する．この認証値低下がどの様に表れるか，つまり本人だと認証されなくなる状況がどの様に表れるかを分析する．

検証項目としては，以下を評価する．

- 攻撃前後の認証値の変化の程度
- 攻撃後，認証値が一定以下に低下するまでの時間

3.6 実験で設定した攻撃事例

攻撃事例は，端末機種／攻撃モデル／使用した認証アルゴリズムの違いを考慮し表 3 に示す組合せで実施した．

iOS 端末（10 台）と Android 端末（10 台）を各事例（A～D）に各 5 台を準備したが，実験終了後に有効なデータが確認できた端末台数は表 3 のとおりであった．

表 3 使用端末と攻撃/認証方法

事例	機種 OS バージョン	攻撃 モデル	認証値アルゴリズム	有効 台数
A	iPhone 6	他社から	GPS24h	4
B	(iOS 12.2)	自社内		5
C	Android	他社から	GPS24h,	2
D	6.0 ～ 7.1.1	自社内	Wi-Fi24h	4

3.6.1 攻撃（盗難／窃取）の実現方法

端末は被験者間で指定した日時に一斉に交換する方法とした．なお，被験者の都合で一部の端末は一斉交換日時の前後に交換されたものもある．この場合の交換日時は他のデータからの推定値を用いた．

3.6.2 攻撃後の端末の挙動による補正

一部の端末の受け渡し時，稼働停止（電源 OFF）したと見られる事象があった．盗難の検出時間を評価する場合，停止時間を確認可能な Android 端末の場合では停止時間を無視する時間補正を行った．これは Android 端末では，通常稼働時は 5 分間隔でデータ収集するため，端末が停止した（電源断等）の停止時間をほぼ把握できるため．

一方，iOS 端末の場合，不定期にデータ収集（位置の移動を伴う場合等）がなされることから，端末の停止を完全には把握できない．このため補正は行わないこととした．

3.6.3 具体的な攻撃の検出方法

以下の 2 つの方法で評価する．

- 攻撃前後での認証値の平均値を比較

今回の攻撃モデルの被験者（社会人）は比較的規則的な行動パターンを示しており，行動の揺らぎがあっても定常的な認証値を維持する傾向が見られる．攻撃発生時刻が既知である場合，攻撃前後における前半期間の全体の平均認証値と後半期間の全体の平均認証値を比較する．

- 攻撃発生の検出に要する時間を評価

攻撃開始後，認証値が最初に 0.5 以下（本人である確率が 0.5 以下，つまり本人でない可能性の方が高くなる状態）となるまでの時間を計測する．

3.6.4 使用した認証値アルゴリズム

- iOS 端末

位置情報ベースの情報を，24 時間のタイムウィンドウで評価する方式のアルゴリズム（GPS24h）のみを使用．

- Android 端末

GPS24h に加えて，Wi-Fi 環境の情報を，24 時間のタイムウィンドウで評価する方式のアルゴリズム（Wi-Fi24h）を使用．

4. 実験結果

4.1 攻撃による認証値（平均値）低下

GPS24h を使用した場合，攻撃発生による前後の認証値の変化の事例を示す．

4.1.1 iOS 端末／他社から攻撃の場合（事例 A サンプル）

iOS 端末で他社から攻撃された場合，認証値は攻撃前の平均値 0.87 に対して，攻撃後の平均値は 0.13 に低下した．この時間的変化を図 4 に示す．攻撃後，明らかに他人が使用していることが推察される．

4.1.2 iOS 端末／自社内攻撃の場合（事例 B サンプル）

iOS 端末で自社内から攻撃された場合，認証値は攻撃前の平均値 0.78 に対して，攻撃後の平均値は 0.44 に低下した．この時間的変化を図 5 に示す．

攻撃後においても攻撃者が自社内の場合，特に昼間時間帯において位置情報の類似性が高いため，認証値の低下が小さくなり攻撃が確認しづらい傾向がある．

4.1.3 Android 端末／他社から攻撃の場合（事例 C サンプル）

Android 端末で他社から攻撃された場合，認証値は攻撃前の平均値 0.92 に対して，攻撃後の平均値は 0.01 に大きく低下した．この時間的変化を図 6 に示す．

このケースの場合，攻撃者との位置情報の類似性がほぼ無いことにより，ほぼゼロになったと考えられる．

4.1.4 Android 端末／自社内攻撃の場合（事例 D サンプル）

Android 端末で自社内から攻撃された場合，認証値は攻撃前の平均値 0.85 に対して，攻撃後の平均値は 0.29 に低下した．この時間的変化を図 7 に示す．

このケースの場合も攻撃者が同一社内で位置情報の類似性が高く，認証値の低下が小さくなったと考えられる．

4.1.5 攻撃による認証値（平均値）低下のまとめ

15 台の端末で実施した認証値低下の状況を図 8・図 9・図 10 に示す．全体として，他社から攻撃モデルの場合は認証値が大きく低下することが分かる．自社内攻撃の場合，認証値の低下が十分でなく，攻撃検出が明確でない状況がある．実用的に攻撃検出として利用するには，認証値の判定のためのしきい値（この実験では 0.5 とした）を適切に決めることが重要と見られる．

また iOS 端末と Android 端末との比較では，Android 端末が収集する位置情報データの量が多く，より正確な判定につながっていると推察される．

GPS24h と Wi-Fi24h との比較では，Wi-Fi を使った認証値の変化がより敏感に表れることが分かった．

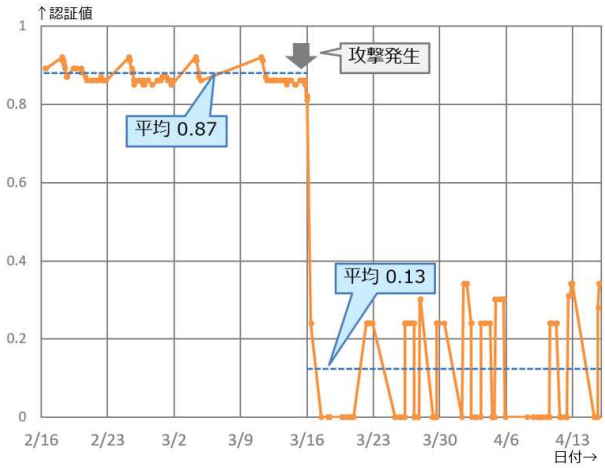

図 4 認証値低下（GPS24h,iOS,他社から攻撃）

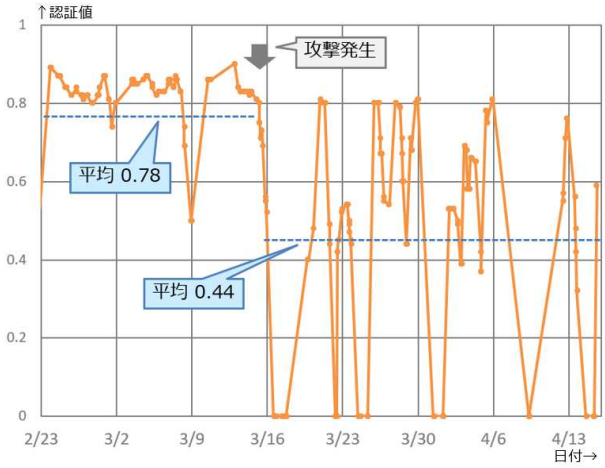

図 5 認証値低下（GPS24h,iOS,自社内攻撃）

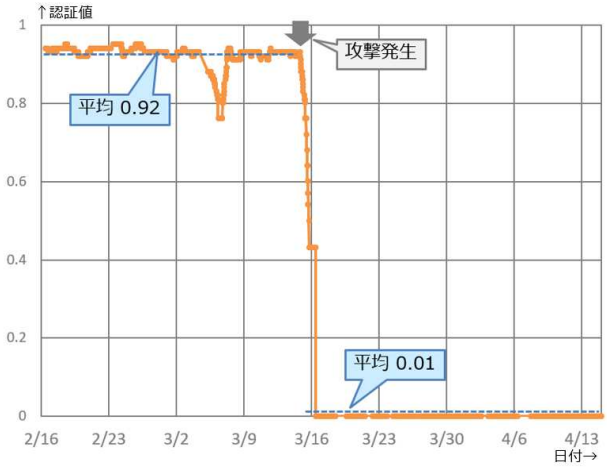

図 6 認証値低下（GPS24h,Android,他社から攻撃）

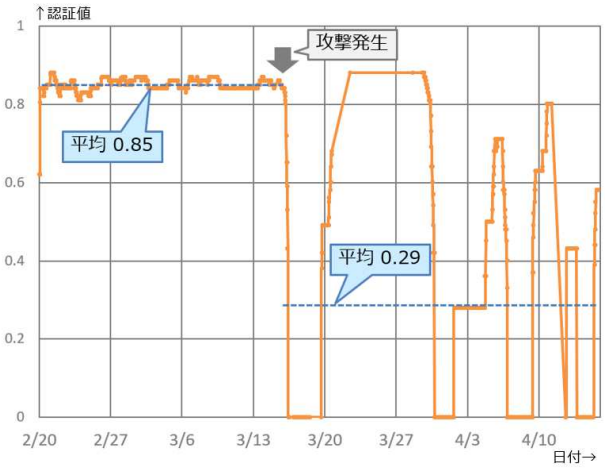

図 7 認証値低下（GPS24h,Android,自社内攻撃）

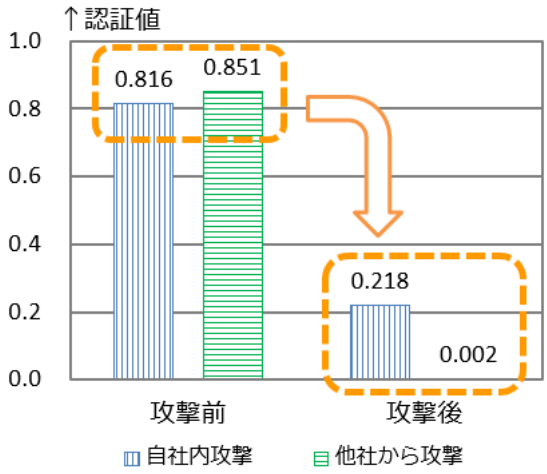

図 10 認証値低下の平均値（Android,Wi-Fi24h）

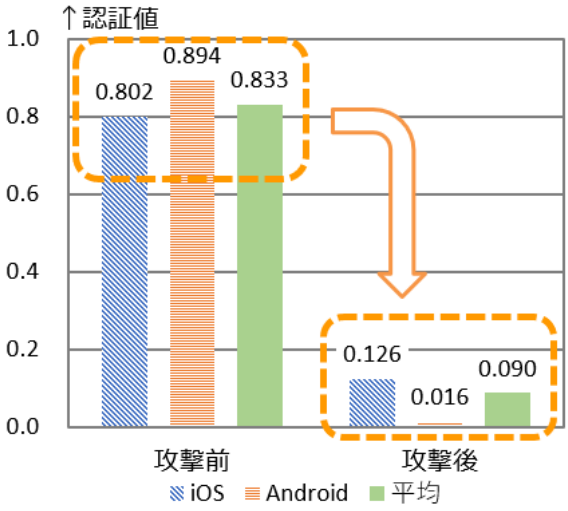

図 8 認証値低下の平均値（GPS24h,他社から攻撃）

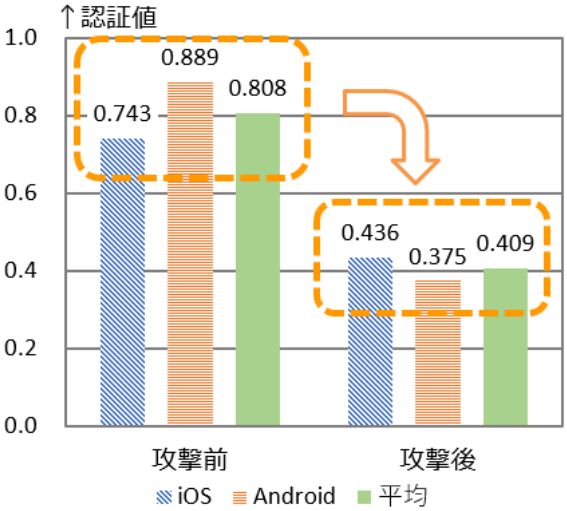

図 9 認証値低下の平均値（GPS24h,自社内攻撃）

4.2 攻撃の検出にかかる時間

攻撃発生から認証値の低下が発生するが，しきい値として 0.5 以下に低下するまでの時間を計測した．ただし端末が停止していた（電源が切られていた）時間を除く補正を行った．

下記に述べる事例 A～D は，4.1 で認証値低下の例を挙げたサンプルと同一の被験者である．

4.2.1 iOS 端末／他社攻撃の場合（事例 A サンプル）

GPS24h において認証値の低下は時間とともに低下する．認証値が 0.5 以下となるまでの時間は，このケースの場合，22 時間 54 分を要した．この時間的変化を図 11 に示す．

4.2.2 iOS 端末／自社内攻撃の場合（事例 B サンプル）

GPS24h において自社内攻撃の場合，認証値は前例よりも緩やかに低下した．認証値が 0.5 以下となるまでの時間は，このケースの場合，26 時間 46 分を要した．この時間的変化を図 12 に示す．

4.2.3 Android 端末／他社から攻撃の場合（事例 C サンプル）

Android 端末においては，Wi-Fi の環境情報がより多く得られることにより，GPS24h に加えて Wi-Fi24h についても攻撃検出の時間を計測した．認証値が 0.5 以下となるまでの時間は，このケースの場合，GPS24h の場合 22 時間 59 分，Wi-Fi24h の場合 11 時間 58 分を要した．

GPS24h の認証値低下よりも Wi-Fi24h の認証値低下が早いこととなった．この変化を図 13 に示す．

4.2.4 Android 端末／自社内攻撃の場合（事例 D）

このケースも同様に GPS24h と Wi-Fi24h の両方において攻撃検出の時間を計測した．認証値が 0.5 以下となるまで

の時間は，GPS24h の場合 21 時間 16 分，Wi-Fi24h の場合 12 時間 15 分を要した．このケースでも GPS24h の認証値低下よりも Wi-Fi24h の認証値低下が早いこととなった．この変化を図 14 に示す．

4.2.5 攻撃の検出にかかる時間のまとめ

15 台の端末で実施した攻撃検出時間の平均値を図 15 に示す．全体的に，自社内攻撃の検出時間が大きくなっている．このことは自社内からの攻撃が本人行動との類似性が高いことと一致する．GPS24h においは，Android 端末が iOS 端末よりも検出時間が短い．Android 端末の位置データの量が多く，より的確に行動を把握できることが分かった．Android 端末の Wi-Fi 情報の利用は，さらに検出時間を短くすることが分かった．

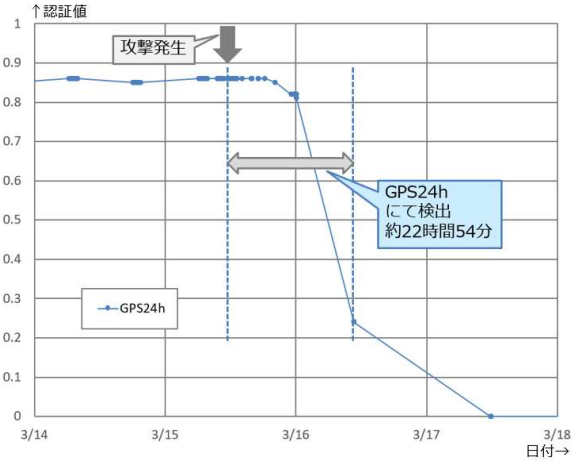

図 11 検出時間（GPS24h,iOS,他社から攻撃）

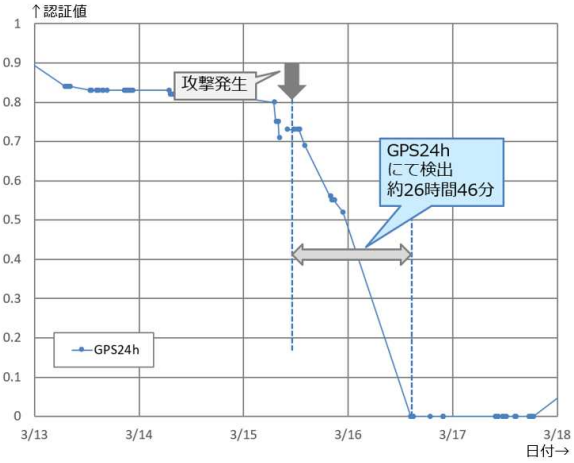

図 12 検出時間（GPS24h,iOS,自社内攻撃）

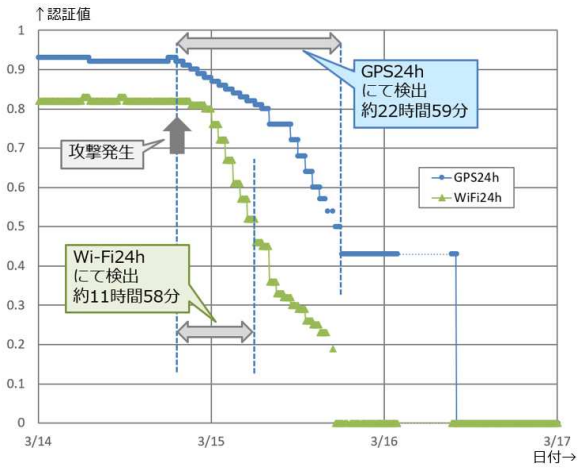

図 13 検出時間（GPS24h/WiFi24h,Android,他社から攻撃）

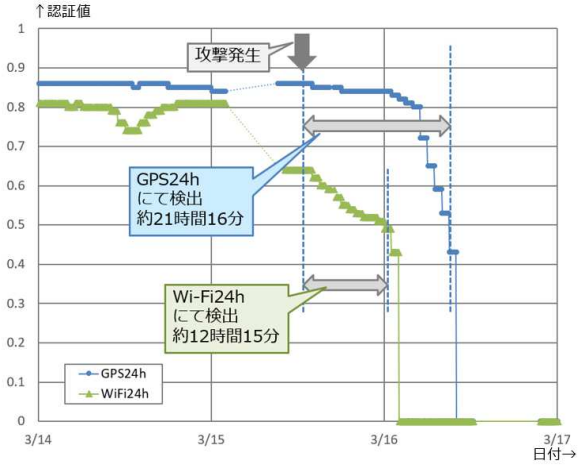

図 14 検出時間（GPS24h/WiFi24h,Android,自社内攻撃）

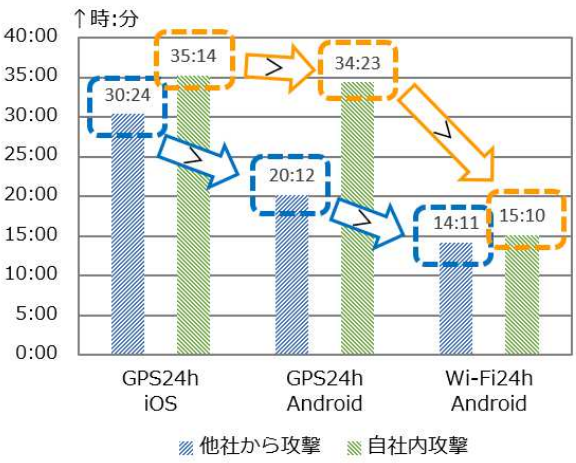

図 15 検出時間の平均値

5. 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） のデータを用いて端末への攻撃（盗難／窃取）を想定したモデルの分析を行った.

実験では各種の認証アルゴリズムを実装したが，攻撃評価には GPS24h と Wi-Fi24h の 2 種類を使用した.

認証値を時系列で収集／評価することにより，その時間的変化から攻撃モデルでの特徴を明らかにした.

いずれの事例でも攻撃事象を正しく認識できることが確認できた. また検出までの時間についても 24 時間のタイムウィンドウを使用した場合は妥当と考えられる.

ライフスタイル認証は，今回使用した認証要素（位置情報，Wi-Fi 情報）以外の多要素を組合せて認証を実現するものである．今回明らかになった認証要素とアルゴリズムの特徴や攻撃への耐性について，今後の実用化に向けた研究に役立てる方針である.

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] 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).

[3] 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).

[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-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).

[5] 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).

[6] 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).

[7] 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).

[8] 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).

[9] 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).

[10] 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, pp.1566-1573 (2018).

[11] 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.

[12] 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，pp.928-934 (2019).

[13] 重田信夫，小林良輔，佐治信之，山口利恵：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，コンピュータセキュリティシンポジウム 2019 論文集，pp.9-16 (2019).