Vol.2015-CSEC-71 No.6
2015/12/4

無線LAN情報の認証への応用

平岩 啓[1,a)]　満保 雅浩[2]

概要：近年ライフログへの注目が集まり，その市場規模が拡大している．一方，公衆無線 LAN の増加とともに生活のほとんどの場において無線 LAN 通信が利用できる環境が整いつつある．無線 LAN から得られる情報を蓄積したライフログには個人の識別につながる特徴が存在すると考えられるため，本論文では，無線 LAN から得られた情報を個人認証に応用することを検討する．具体的にはスマートフォン端末上で，電波強度を含む無線 LAN 情報を取得し，リスクベース認証や複合認証での個人認証の可能性を検討する．無線 LAN 情報は携帯端末により自動的に取得することが可能であるため，本論文のユーザビリティの高い個人認証を実現することが期待できる．

キーワード：無線 LAN，Wi-Fi，認証，ライフログ，リスクベース認証

Application of the Wireless LAN Information to User Authentication.

Satoshi HIRAIWA[1,a)]　Masahiro MANBO[2]

Abstract: In recent years attention to the life log collection and its market have been growing. At the same time, wireless LAN communication is available in most places with the increase of the public wireless LAN. In this paper, we examine whether identification of the individual features are possible from the information obtained from the wireless LAN and show that the wireless LAN information is useful for user authentication in the framework of the risk-based authentication.

Keywords: wireless LAN, Wi-Fi, authentication, life log, Risk-based authentication

1. はじめに

無線 LAN を介したインターネットへの接続を可能する公衆無線 LAN が街中に増加しており，NTT docomo は 2015 年 2 月時点で全国 121,900 エリアに 152,100 個ものアクセスポイントを設置し基本無料の Wi-Fi サービスを行っている [1]．同様に，自宅や職場，学校，ショッピングセンターなど生活するほとんどの場においても無線 LAN アクセスポイントが設置され無線 LAN 通信が利用できる環境になりつつある．このように Wi-Fi 通信可能エリアが拡大してる無線 LAN 情報をライフログとして利用して，無線 LAN 信号から現在地を測位するサービスも提供されている [2]．

個人認証とは本人しか持ち得ない属性を元にその属性を確認し本人であることを証明することであり，代表的な方式として予め設定した ID とパスワードを正しく答えられるかで本人か否かの識別を行う知識認証方式 (パスワード方式) がある．この方式はシステム導入のコストが低く多くの場所で利用されている一方で，問題点もある．1 つに ID とパスワードの設定，管理がユーザーの負担となることだ．ユーザーは予め ID とパスワードを設定し管理する．その際にパスワードを推測されることや漏洩することへの対策として複雑な文字列を設定し記憶する必要があり，ユーザビリティを下げる原因となっている．パスワードの管理を必要としない生体認証においても導入コストや認証精度などの問題が多く残されている．

[1] 金沢大学大学院自然科学研究科
Graduate School of Natural Science and Technology, Kanazawa University
[2] 金沢大学理工研究域
Institute of Science and Engineering, Kanazawa University
[a)] sh654874@stu.kanazawa-u.ac.jp

これらの問題に対して注目されるのが，複合認証である．複合認証では，複数の認証作業を行い初めてユーザーの認証がされる．特徴として，認証精度が高くない認証を複数組み合せることで高い認証精度を実現できる．また，リスクベース認証とは認証におけるリスクに応じて，追加の (複数の) 認証を要求する方式である．複合認証により，パスワードのセキュリティが低い場合でも追加の認証作業により，正しく認証が可能になる．

本論文では，無線 LAN 情報を個人認証に利用することを検討する [3]．無線 LAN は多くの場所で提供されており，スマートフォンでのデータ取得が容易である．無線 LAN 情報は普段の生活において自動で取得できるため，パスワードのように設定管理する必要がなくなることが期待される．

本論文中の無線 LAN 情報とは Wi-Fi 規格通信を提供するアクセスポイント（以後 AP と呼ぶ）から発信されるビーコン信号のことであり，実際にユーザーがデータ通信で利用する AP に限らず周囲に点在する全ての AP の情報を用いる．具体的には，スマートフォン端末に実装した実験用アプリケーション（以後アプリと呼ぶ）により AP の SSID と BSSID 及びビーコン信号の電波強度を時系列とともに記録する．この記録データをライフログとみなし，個人の特徴となるデータを抽出し個人識別に用いる．無線 LAN 情報は行動に基づき得られるが，行動は普遍ではないために，高い本人一致率を達成することは難しいと予想される．そのためリスクベース認証や複合認証の一部として利用する．なお，ライフログとは生活の中で得られる多種多様な情報を記録したデータ，あるいはその記録する技術のことである．

また，本論文では，3.1 節の関連研究 [6] とユーザーの個人識別精度の比較を行い，提案手法の優位性を示すとともに，Wi-Fi データの取り扱いについて検討する．

2. 関連研究と提案手法への着想

2.1 関連研究

船越ら [4] はスマートフォンの GPS 機能によって得られた位置情報をライフログとして扱い，そのライフログよりユーザーの行動特性を分析し本人認証を行っている．[4] ではユーザーの行動特性を抽出し，適切な値をパラメータに設定することで本人認証が可能であると示している．[4] ではライフログに GPS による位置情報を用いており，GPS による位置の測位は屋内やビル群において誤差が大きく正確さに欠ける問題がある．

また，小林ら [5][6] は無線 LAN 情報を用いた研究のひとつに“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”を提案している．[6] では，Wi-Fi により得られた AP の BSSID と時刻のデータに対して p-タイル法を用いてユーザーの特徴を抽出し，得られたデータからユーザーの認証を行っている．具体的には，以下の目的と順序で処理を行い，行動特性を抽出している．

アドレスの選定
: たまたま取得された（取得頻度の低い）AP の情報は，個人を特徴付ける量とはならないと予想し，より個人の特徴を得るために，たまたま取得された AP の情報を排除する．

データ取得頻度の濃淡
: 3.3 節で後述する丸め込みを行ったデータに対して，データの取得頻度に応じて濃淡をつける．個人を特徴付けるであろう AP の情報は濃く，そうでない情報は淡くなる．

p-タイル法による 2 値化
: データ取得頻度の濃淡をもとに，p-タイル法（画像処理における 2 値化手法）を用いて 2 値化する．

以上のアルゴリズムをもとにした認証実験により，本人受け入れ率と他人受け入れ率に大きな差があることから目的とする複合認証に利用可能であると示している．しかし無線 LAN 情報を取得する状況に対する追加の議論がされていない．

2.2 提案手法の着想

無線 LAN 情報を用いた位置の測定は GPS の苦手とする屋内やビル群でも精度良く測定可能である [2][7].

認証を行う複数のユーザーが同じ空間に存在するとき，同じ AP の信号を受信していることが考えられる．その状況のもとユーザーの識別を時刻と BSSID のみに頼る場合，複数ユーザーをライフログで識別することは難しい．しかし信号強度をユーザーの識別に導入することで，より細かくユーザーの識別が可能になり誤って他人を受け入れてしまうことを避けることができると考える．ここで信号強度とは，AP から発信される電波信号の強度を表しており，単位は dBm である．一般的に AP の近辺では信号強度が強く，AP からの距離の 2 乗に反比例して信号強度は弱くなる．空間における信号の伝搬については [8] を参照されたい．

ユーザーの行動情報には多くのゆらぎが含まれ十分に特徴を得るのは行動を多くの場合に場合分けする必要がある．特に平日と休日では行動パターンにも大きな違いがあると考え，認証時におけるタイミングが平日か休日かで認証に用いるデータを分けることで行動情報を的確に捉えることができる．

3. 提案手法

ユーザーは曜日や時間に依存した規則的な行動パターン持ち，それに従い行動していることが多い [9]．行動パターンはユーザーによって異なっており，ユーザー独自の固有性を抽出することが出来れば，認証を行うユーザーの実際

の行動がその固有性と整合するかをみることにより本人であるか否かの判断をすることができる．ユーザーの固有の情報となる行動パターンを行動特性といい，ライフログから行動特性を抽出したデータのことを学習データとする．一方で，認証したいユーザーのライフログのことをテストデータとする．

3.1 提案手法の特徴

本論文では，ユーザーの行動を捉えるために無線 LAN 情報をライフログとして用いる．無線 LAN 情報は生活する全ての空間においても取得することが可能であり，さらにユーザーの行動そのものがパスワードとなることから改めて推測や漏洩を意識してパスワードを設定管理する必要がない．また，信号強度も用いてユーザーの識別を行う．信号強度はユーザーと AP の距離を示す指標として扱い，同じ BSSID を取得する場合でも信号強度の差異から，より細かにユーザーの識別が可能になり誤って他人を認証してしまうことを避けられると考える．具体的には，ある二人が同じ AP からの信号を受信したときに，受信した信号強度に違いがあれば 2 者間には距離が存在すると考える．さらに信号強度から AP までの距離を知ることが可能であり，AP が複数個設置されている空間では，複数の信号強度から位置の特定が可能になる．

またライフログからユーザーの行動特性の抽出には，複数の日のうちで，同じ時間帯にしきい値以上の回数で記録される無線 LAN 情報を学習データとして抽出する手法を採用する．これは，ユーザーの行動パターンに合わせて取得される無線 LAN 情報は，その規則性のために異なる日の同じ時刻に何度も同じ無線 LAN 情報が記録されるはずであと考えたためである．[9] では人は曜日や日時に依存した行動パターンを持ち，それに従い行動していることが多いと述べている．本論文では，特に平日と休日では行動パターンにも大きな違いがあると考える．このためにライフログを平日と休日に分けて個人の識別に用いる．ユーザーの識別は学習データとテストデータを比較検証することで行う．具体的には，行動特性を表す学習データに対して，テストデータがどれだけ一致する BSSID を持ち，信号強度が大きく異なっていないかを比較してユーザーが同一か否かを判断する．

3.2 行動特性の抽出

ユーザーは曜日や日時に依存した規則的な行動パターンを持っていることが知られている．しかしユーザーは常にまったく同じ行動をとるものではなく，行動の始まりや終わりの時間にはばらつきがある．また行動パターンに含まれていないイレギュラーな行動をとることもあり，そのユーザーの行動情報にはゆらぎが存在する．以後，行動パターンの時間のばらつきのことを“時間のゆらぎ”，行動パターンからは予測できないイレギュラーな行動を“行動のゆらぎ”と呼ぶ．具体的な例を示す，あるユーザーの出社時間は 8:00 から 8:30 の間のいずれかであり日によってばらつきがあることを“時間のゆらぎ”，急な出張があり普段行くことのない地方で活動することを“行動のゆらぎ”という．

学習データとテストデータの生成にあたって，より的確な行動特性を抽出するためにも，以下の処理をライフログに対して行いゆらぎの吸収や排除を行う必要がある．

- 時間のゆらぎの丸め込み
- 行動のゆらぎの排除

ここで，認証をしたいユーザーの 1 時間から 24 時間までの一定時間のライフログに対して丸め込み処理をしたデータをテストデータ，ユーザーのライフログに対して丸め込み処理とゆらぎ排除処理の両方を行ったデータがそのユーザーの学習データとなる．

3.3 丸め込み

Algorithm1 の丸め込みの概要は，時刻 hh 時 mm 分を hh:mm と表現するとき，時刻 hh:00 から時刻 hh+1:00 までの 1 時間に記録された LifeLog を NewLifeLog へと格納していく，ただし重複する BSSID アドレスの格納を許さず，重複する BSSID を持つ信号の強度は平均値をとる．この処理によりユーザーの行動に時間の幅を持たせ，10 分間隔の厳密な行動を記録するのではなく，おおよその時間帯での行動を新たにライフログとして記録される．時間のゆらぎをまとめることが出来る．

行動には数分から 1 時間程度の時間のゆらぎがあると考えて，1 時間の内に取得したデータに対して丸め込み処理を行う．

Algorithm 1 丸め込み

```
LifeLog , NewLifeLog , x , signal , i
while recording time of Lifelog is same hour do
  x ⇐ address of LifeLog[i]
  if x ∈ NewLifeLog then
    no processing.
  else
    signal ⇐ the average of signal of x
    NewLifeLog ⇐ x , signal
  end if
  i++
end while
return NewLifeLog
```

3.4 ゆらぎの排除と行動特性の抽出

ユーザーの行動パターンに合わせて取得される無線 LAN 情報は，その規則性のために同じ時刻のタイミングで何度もライフログに記録されるはずである．そのためにユーザーの行動特性を最も表しているのはライフログ中で同じ

時間帯に高い頻度で記録されるデータである．行動特性を抽出するときに，ライフログからあるしきい値以上の記録回数をもつデータをサンプリングすることで正確な行動特性の抽出と同時に行動のゆらぎを取り除くことができる．

Algorithm2 のゆらぎの排除の概要は，丸め込み処理を行ったライフログに対して，日付関係なく同じ時刻帯 hour に記録された BSSID の記録回数をカウントする．しきい値を設定し，カウントがしきい値より大きければ，その BSSID を Learn へ格納する．丸め込み処理同様に信号の強度は平均値をとる．この処理によってユーザーの行動特性を色濃く表すデータのみ Learn へと出力される．ここで得られる Leran が学習データとなり，またしきい値のことを“ゆらぎのしきい値”と呼ぶ．Algorithm2 内では，しきい値を k とする．ゆらぎのしきい値をライフログの取得期間の 30 %，50 %，70 %に設定することで 1 人のユーザーに対し 3 通りの学習データを作成する．

Algorithm 2 ゆらぎの排除（行動特性の抽出）

```
NewLifeLog, Learn, x, y, signal
for each hour of the day do
  i ⇐ 0
  while LifeLog[i] do
    x ⇐ address of NewLifeLog[i]
    y ⇐ time of NewLifeLog[i]
    if y = hour then
      Cnt(x) ⇐ the number of x in y
      if Cnt(x) = k then
        signal ⇐ the average of signal of x
        Leran ⇐ address, signal
      end if
    end if
    i++
  end while
end for
return Learn
```

3.5 一致率の計算

学習データとテストデータとを比較検証した評価結果として学習データとテストデータの類似のようすを示す一致率を新たに考える．一致率に対してセキュリティパラメータを定義し，一致率がセキュリティパラメータ以上であれば認証成功，未満であれば認証失敗となる．一致率は学習データとテストデータの一致するデータの割合を表し，Algorithm3 一致率の計算で求める．

互いにデータを有している時間帯を i とし，i の総数を N とする．時間帯 i での一致データ件数を M_i とする．テストデータが同時間帯 i の学習データと同じ BSSID の AP を有し，且つその信号強度が学習データの信号強度に対して設定した値 (dBm) の範囲内であれば M_i をカウントする．また時間帯 i での学習データ件数を S_i とする．そして全ての時間帯において M_i と S_i をカウントしていき一致率 C[%] を求める．

$$C = \sum_{i}^{N} (M_i/S_i)/N * 100$$

Algorithm 3 一致率の計算

```
Learn , Test , i , j , k , t1 , t2
while Learn[] and Test[] are exist do
  t1 ⇐ time of Learn[i]
  t2 ⇐ time of Test[j]
  if t2 > t1 then
    while t2 > t1 do
      i++, t1 ⇐ time of Learn[i]
    end while
  else if t2 < t1 then
    while t2 < t1 do
      j++, t2 ⇐ time of Test[j]
    end while
  else
    while time of Learn[i] = t1 do
      y ⇐ address of Test[j]
      k ⇐ j
      while time of Test[k] = t2 do
        x ⇐ address of Learn[i]
        if x = y And signal of x ≈ signal of y then
          M++
        end if
        k++
      end while
      k = j , i++ , S++
    end while
    N++ , C+= M/S
  end if
end while
C = 100 * C/N
return C
```

4. 評価実験

提案手法をもとに評価実験を行った．評価実験では，ユーザーの識別能力について以下違いに基づき評価する．

(1) 信号強度取り扱いの違いの識別への有用性
(2) 平日休日での識別結果の違い
(3) 異なるテストデータ長での識別
(4) 文献 [6] の手法による識別結果の違い

無線 LAN 情報のライフログ取得には，大学生に協力をしてもらった．被験者が普段使用し持ち歩くスマートフォンにアプリをインストールし，普段と同じ生活のライフログを取得する．この実験に用いるライフログデータは以下に示す．

- 被験者人数 : 5 人
- ライフログ取得期間 : 約 2 ヶ月

アプリはデータ取得を 10 分間隔で行い，取得されたデータは実験用に設置した web サーバーへと送られデータベースに保存される．アプリが何も取得できなかった場合は SSID,BSSID を null として記録し扱う．取得されるデータ

量にはユーザーの環境によって差異があるが特に考慮しない．またスマートフォン端末の性能，通信環境によってはデータ取得が出来なかったり，サーバーへデータ送信中にパケットが落ちてしまうケースもあったが，これらは実用上も起こりうるため，データ欠損したままのデータを用いた．

4.1 信号強度の取り扱いの違いによる個人認証

被験者 5 名の内 4 名は大学の同一研究室に所属する学生である．そのため平日の日中帯は同じ場所に停留しており，その時間帯の行動パターンがほぼ同じであることから，その間に取得される無線 LAN 情報が類似していることが考えられる．そこで 4 名の被験者が同時刻に同じ室内で行動していた際に取得されるライフログから個人識別を行うことで，提案する信号強度を用いた個人識別手法が有効であるかを検証した．

実験環境は以下に示す．

- 被験者人数：4 人
- 日数と時間：9 日間 14-16 時

それぞれに学習データを作成する．また同じ行動を行っている（同じ場所にいる）データのみを選択して評価実験を行うので，行動にゆらぎはないと考え，4.4 節で述べたゆらぎを取り除くためのしきい値は 1 とする．テストデータは同じく上記の 9 日間のライフログを用い，テストデータ長は 14-16 時の 3 時間とする．学習データとテストデータの信号強度の誤差がどれだけの数値範囲（dBm）内であるかをデータの一致の信号条件として加える．信号強度を考慮しない場合（信号条件なし）の一致度を算出した後に，信号条件を変えながら一致度の算出を行った．信号条件の値は大きければ大きいほど誤差を許し小さければ小さいほど誤差を認めない．信号強度の条件 7 通り設定し，これを変えながら本人識別を 252 回，他人識別を 756 回行った．

4.2 行動特性による個人認証

被験者のライフログに平日と休日というパラメータを付加し，それぞれの学習データとテストデータとから個人の識別を行うことで提案する手法の評価を行う．各パラメータ毎のライフログ取得期間の内，直近 3 割のデータをテストデータ，それ以外を学習データとした．本実験では，行動のゆらぎのしきい値に 0.3,0.5,0.7 を設定して学習データを抽出する．テストデータ長は 24 時間と 1 時間の 2 通りについて行い，テストデータ長を 24 時間としたときは，信号条件を“± 5dBm”として行った．テストデータ長が 1 時間の評価実験では，全ての時刻においてテストデータと学習データの比較を行うために，しきい値は 0.3 とした．また，信号条件がないときと信号条件“± 5dBm”の 2 通りで行った．

以上の条件のもと，テストデータ長を 24 時間としたときで

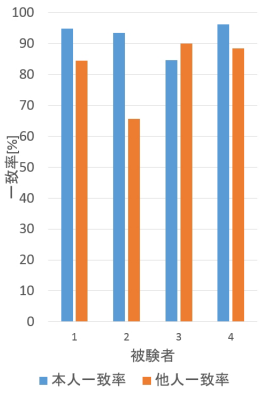

図 1 信号条件なし
Fig. 1 signal terms : no

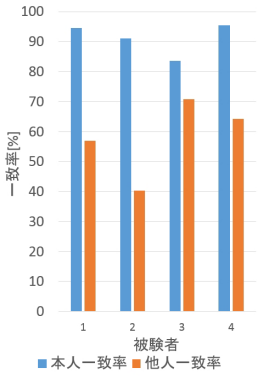

図 2 信号条件 10dBm
Fig. 2 signal terms : 10dBm

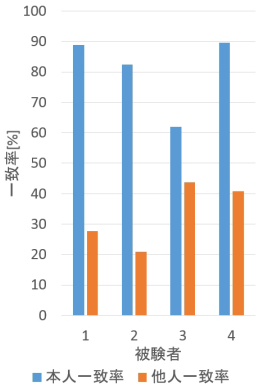

図 3 信号条件 5dBm
Fig. 3 signal terms : 5dBm

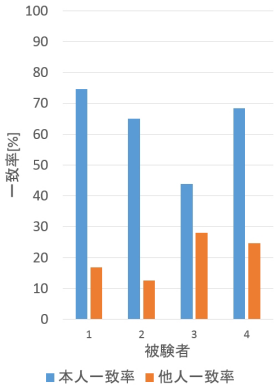

図 4 信号条件 3dBm
Fig. 4 signal terms : 3dBm

本人識別を 246 回，他人識別を 984 回行った．テストデータ長が 1 時間としたときでは，本人識別を 3,936 回，他人識別を 15,744 回行った．

4.3 関連研究との比較実験

提案手法と文献 [6] で提案される p-タイル法を用いての手法との比較実験を行う．比較実験では，5.2 節と同じライフログを用いて，異なる 2 つのテストデータ長（24 時間と 1 時間）で個人識別を行う．また，比較のために提案手法では，平日休日の区分けを行なわずに，信号強度の考慮をしたものと信号強度を考慮していないものの 2 通り行う．行動のゆらぎのしきい値には 0.3 を設定して学習データを抽出する．識別結果から以下の項目について比較する．

(1) 行動特性の抽出，一致率計算アルゴリズムの違いによる識別結果
(2) 信号強度や平日休日の有無による識別結果

p-タイル法，提案手法のそれぞれで本人識別を 2050 回，他人識別を 8200 回行った．

5. 実験結果と考察

5.1 信号強度による個人認証

信号条件を取り扱う場合による一致度の結果は図 1,2,3,4 の通りになった．より信号条件を厳しく設定した場合の結

果についてはページ数の都合上，割愛するが，これらと同様の傾向がみられた．

● 信号強度取り扱いの違いの識別への有用性

図 1 では，本人一致率，他人一致率ともに高い数値を示した．特に，被験者 3 の結果に注目すると本人よりも他人の方が一致率が高い結果となっている．このことから，AP の BSSID のみではユーザーの識別は困難であるとわかる．図 2,3,4 では図 1 に比べ，本人一致率と他人一致率のどちらも低下した．しかし，信号条件を厳しくした場合でも本人一致率は，他人一致率よりも常に高く，40 %以上の一致率を保っている．他人一致率は信号条件により大きく一致率を下げる結果となった．以上から，同じ AP の無線 LAN 情報を受信している場合においても，信号強度に着目することでユーザーの識別が可能である．

また同じ AP からの信号でありながら，取得する信号強度に差が得られたのは，ユーザーと AP の距離が異なっていることだけが要因ではないと考える．ユーザーの細かな行動によっても信号強度が影響していると考えられる．例として，携帯端末に多く触れる，ポケットや鞄など信号を遮蔽するものに携帯端末を収める，など信号強度を変化させる要因は複数ある．そういった細かな行動もライフログのひとつであり，ユーザーの識別に必要な要因であると推測する．

5.2 行動特性による個人認証

24 時間の行動特性による認証結果は，平日が図 5,7,9，休日が図 6,8,10 の通りになった．

1 時間の行動特性による認証結果は，平日が図 11，休日が図 12 の通りになった．折れ線グラフが信号条件“±5dBm”の結果で，棒グラフが信号強度を含めない場合の結果である．

● 異なるテストデータ長での識別

テストデータ長を 24 時間としたとき，本人一致率はほとんどの組み合わせで高い結果を示した．また図 10 では本人一致率が 90 %にまで達している．一方で，他人一致率は最も高い場合で図 10 の 7 %であり，他人一致率は低い結果となった．しきい値が大きくなるにつれて，他人一致率が下がる傾向があった．一致率はしきい値によって変化し，図 10 で本人一致率がとても小さい値になる場合があったものの，ほとんどの本人一致率は 50 %を超える結果となった．しきい値を的確に設定することが出来ればユーザーの識別が可能である．

また，テストデータ長が 1 時間のとき，信号条件のあるなしに関わらず，本人一致率はどの時間においても高い結果を示すことが分かる．他人受入率も低い値に収まっている．特徴として，図 11 では，夜から朝にかけての他人一致率は低く，平日の夕方頃では本人一致率が低下し他人一致率が 10 %にまで上がる結果となった．図 12 では，時間

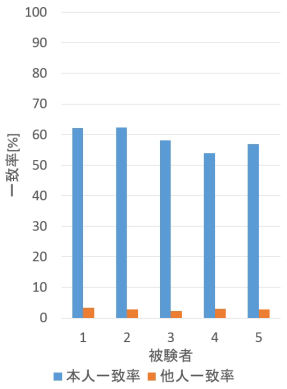

図 5 平日 24h しきい値 0.3
Fig. 5 weekday, threshold 0.3

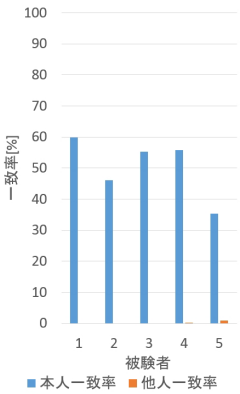

図 6 休日 24h しきい値 0.3
Fig. 6 holiday, threshold 0.3

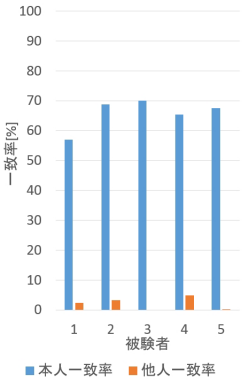

図 7 平日 24h しきい値 0.5
Fig. 7 weekday, threshold 0.5

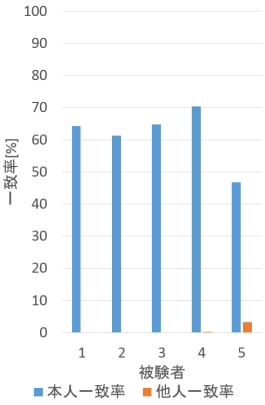

図 8 休日 24h しきい値 0.5
Fig. 8 holiday, threshold 0.5

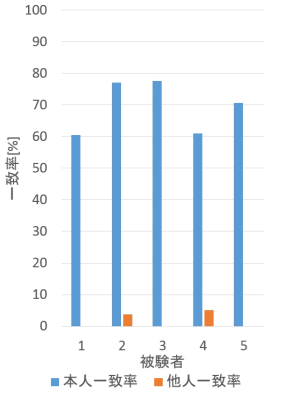

図 9 平日 24h しきい値 0.7
Fig. 9 weekday, threshold 0.7

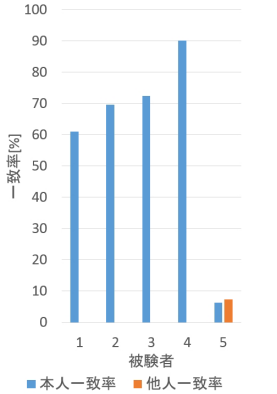

図 10 休日 24h しきい値 0.7
Fig. 10 holiday, threshold 07

による一致率の変動はあるが他人一致率は常に低い．1 時間という短いテストデータ長でも，ユーザーの識別が可能である．

二つのテストデータ長での識別結果には，本人一致率には差がない結果となった．認証に必要なテストデータ長は短いほうが有用であると考えられる．しかし，図 11 のように他人一致率が高い時間帯もあることから，テストデータ長の使い分けや，短いほど偶然に一致することがもありえるため，適正なテストデータ長を検討する必要がある．

しきい値により一致率が変化する原因を考察する．しき

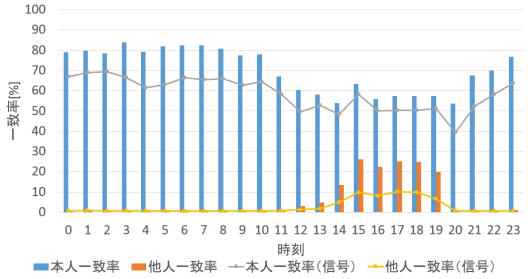

図 11 平日テストデータ長 1 h
Fig. 11 weekday : test data length is 1hour

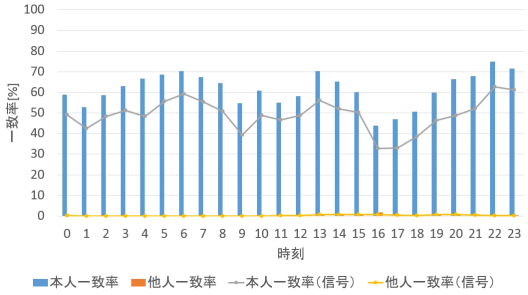

図 12 休日テストデータ長 1h
Fig. 12 holiday : test data length is 1hour

い値が小さければ，学習データには行動のゆらぎが多く含まれる．このゆらぎに他人の行動情報が含まれたために他人一致率が得られたと考えられる．一方で，行動にゆらぎが多く行動のパターンが明確でないユーザーは，しきい値が大きいと確かな学習データが得られずに本人一致率を低下させる原因になる．

- **信号強度取り扱いの違いの識別への有用性**

図 11,12 から信号強度のあるなしによる識別の違いが見て取れる．図 11 では，信号強度を考慮することによって他人一致率が 26 %まであった時刻も 10 %未満まで抑えることができている．また本人一致率も同時に低下している．これは信号条件によりユーザーのわずかな行動の違いにも反応してしまったためだと考えられる．しかし，本人一致率は，他人一致率に比べ高い数値を持つので十分に有効である．

- **平日休日での識別結果の違い**

平日と休日との結果を比較する．今回の解析は，平日と休日でライフログを分けた場合でのみ行っている．平日では他人一致率がわずかながら見られるが，休日においては他人一致率は有効な値を示さなかった．このことから他人一致率を下げる方法として，平日や休日などの日時を考慮することは有効であると考えられる．

5.3 比較実験による検証

p-タイル法を用いた認証結果は，テストデータ長を 24 時間としたときは図 13，1 時間としたときは図 15 の通りになった．提案手法での認証結果は，テストデータ長を 24 時間としたときは図 14，1 時間としたときは図 16 の通り

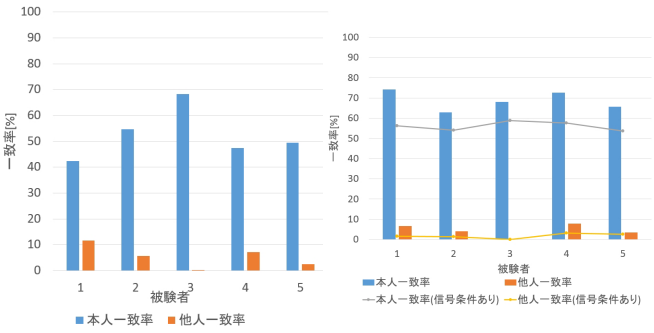

図 13 p-タイル法:24h
Fig. 13 p-tile method: test data 24hour

図 14 提案手法:24h
Fig. 14 proposed method: test data 24hour

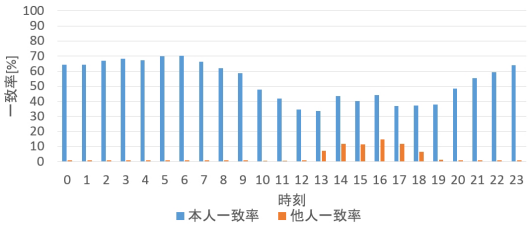

図 15 p-タイル法:1h
Fig. 15 p-tile method: test data 1hour

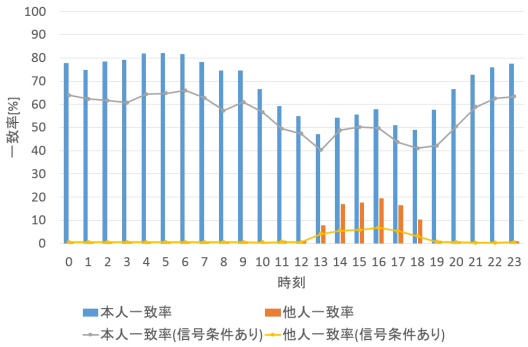

図 16 提案手法:1h
Fig. 16 proposed method: test data 1hour

になった．折れ線グラフが信号条件“± 5dBm”の結果で，棒グラフが信号強度を含めない場合の結果である．

- **アルゴリズムの違いによる結果**

信号強度を考慮しない場合の結果について考察する．図 15,16 ともに一致率には似た傾向が見られる．しかし，p-タイル法での本人一致率は，提案手法の図 14,16 に比べて低く，他人一致率との開きがない．一方で，提案手法の図 16 では，p-タイル法の図 15 に比べてわずかに夕方における他人一致率が高いという結果となった．このことから，信号強度を考慮しない場合の提案するアルゴリズムは，高い本人一致率を得ることができ，文献 [6] の手法は，他人一致率を低く抑えることができる．2 つの長所をもとに，アルゴリズムを組み合せることが今後の課題である．

また，行動特性の抽出をする際に，提案手法では，丸め込みを行った後のデータに対して行動のゆらぎの排除を行っている．一方の [6] では，アドレスの選定（行動のゆらぎの排除に類似した処理）を行ってから丸め込みをして

いる．先にアドレスの選定をすることで，ユーザーが停留している地点の AP の情報しか選定できていない可能性がある．ユーザーが停留していなくとも，日々の買い物など行動特性を表す AP は存在すると考えられ，このことが本人一致率を低下させている原因と考えられる．

● 取り扱う情報による違い

信号強度を含めた結果について考察する．提案手法の図 16 と p-タイル法の図 15 から，本人一致率はとも近い結果となったが，特徴として，図 15 の方が 0 時から 9 時までの間は平均して 3.8 %高く，それ以降の時間では，提案手法の方が平均して 5.8 %高い結果となった．また他人一致率は提案手法の方が低い結果となった．提案手法は，図 5,11 で示すように，信号条件により他人一致率を低く抑えている．また，平日と休日の分け方は，図 11,12 より，ユーザーの識別が可能といえるので，有用であると考えられる．

5.4 攻撃への耐性

考えられる攻撃手法への耐性を考察する．ここではデータの通信路上での盗聴などの攻撃には考察しない．

● 成りすまし

提案する手法はユーザーの行動情報で認証を行うため，成りすまし相手と同じ行動をすることで成りすましされることが考えられる．しかし認証に必要なテストデータ長が長い場合，その間成りすまし相手と同じ行動をすることことは難しいと言える．またテストデータ長に関わらず，信号強度を考慮することで同じ空間に居るだけでは成りすましの成功は低いと考えられる．

端末が盗難や紛失の被害にあった際には，2 次的に成りすましの被害にあう可能性がある．被害にあった直後ではなりすましを防ぐのは難しい．しかし時間の経過に従い，端末によって新たなライフログが記録されていく．6.2 節に示したように，1 時間のテストデータ長であっても個人を識別可能であり，他人が使用していることを検出できると期待される．

●AP の変更

ユーザー本人が管理する AP だけではなく，第 3 者が管理する AP の情報も取得しており，得られるライフログには，ユーザーに依存しないデータも含まれる．例えば，ユーザーの行動特性を強く表していた AP が移動撤去させられた場合には，異なる認証結果が得られることも考えられる．この対策として，重み付き認証方式が挙げられる．ユーザーが管理する AP には高い重みを与え，重みが高ければ高いほど，より本人らしいと判断する．この方式の導入は今後の課題である．

6. むすび

本論文ではユーザーの周りに存在する Wi-Fi 環境をもとに，無線 LAN 情報をライフログとして取得し，その蓄積されたデータから個人認証を行う手法を提案した．そして提案した手法をもとに，実際に無線 LAN 情報を取得した後に，これら蓄積された無線 LAN 情報から行動特性を抽出し，ユーザーの識別実験を行った．信号強度取り扱いの違いの識別への有用性や異なるテストデータ長での識別，平日休日での識別結果の違いについて評価を行い，各ユーザーに適したしきい値や信号条件を設定することでユーザー識別が可能であることを示した．しかし，本人一致率は平均 60 %ほどであり，行動情報は普遍でないため，無線 LAN 情報のみで個人認証を行うのではなく，複合認証やリスクベース認証への応用が期待される．また文献 [5][6] との比較実験を行い，アルゴリズムの有用性を示した．更に，信号強度と平日休日の情報に着目することで，同じ空間にいるユーザーであっても，ユーザー識別が可能であることを示した．今後の課題は，行動特性の抽出方法や一致度の算出方法をより良いものにすること，無線 LAN 情報が環境に依存する問題を解決することである．

参考文献

[1] NTT docomo：サービスエリア, https://www.nttdocomo.co.jp/service/data/docomo_wifi/area/index.html.
[2] Koozyt：*Palace Engine*, http://www.placeengine.com/.
[3] 平岩啓：無線 *LAN* 情報を用いた個人識別, 金沢大学, 平成 26 年度, 学士学位論文, 2015 年 2 月.
[4] 船越琢矢，満保雅浩，安永憲司：位置情報の認証システムへの応用, The 31th Symposium on Cryptography and Infomation Security, 1B1-4, 2014.
[5] 小林良輔，山口利恵：*A Behavior Authentication Method Using Wi-Fi BSSIDs around Smartphone Carried by a User*, 2nd International Workshop on Information and Communication Security, 2015.
[6] 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, Computer Security Symposium 2015, 3D1-2, 2015.
[7] Mikey Cambel.: *Apple tech uses Wi-Fi access points for indoor navigation, 3D potitionig*, http://appleinsider.com/articles/14/04/15/apple-tech-uses-wi-fi-access-points-for-indoor-navigation-3d-positioning.
[8] 安達三郎：電磁波工学，コロナ社, pp167-168, 2004 年 10 月初版第 17 刷発行
[9] 神崎優子，清水明宏：ライフログサービスに適した位置情報分析手法の研究, 高知工科大学, 平成 21 年度, フロンティアプロジェクト, 学士学位論文, 2010.