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

小林 良輔† 山口 利恵‡

† 東京大学
113-8656 東京都文京区 本郷 7-3-1
kobayashi.ryousuke@sict.i.u-tokyo.ac.jp

‡ 東京大学
113-8656 東京都文京区 本郷 7-3-1
yamaguchi.rie@i.u-tokyo.ac.jp

あらまし 近年，リスクベース認証など行動情報を活用した認証方式が注目されている．IP アドレスなどの履歴情報から個人認証を行う方式はユーザー側にとって利便性が高く，今後の普及が期待されている．本論文ではスマートフォンのセンサーが取得する Wi-Fi の情報に着目し，Wi-Fi 情報を活用した認証方式を検討した．近年では個人がスマートフォンを携帯し，スマートフォンのセンサーが取得する Wi-Fi 情報は個人を特徴づける量になっていると考えられる．一方で人の行動は常に同じではないので，一つの行動情報では精度の高い個人認証を行えない. そのため，Wi-Fi 情報を複合認証の一要素として活用できるかについて検証を行った．

An Authentication Component for Cognitive Authentication Using Wi-Fi Information

RYOSUKE KOBAYASHI† RIE Shigetomi YAMAGUCHI‡

†The University of Tokyo
7-3-1, Hongo, Bunkyo, Tokyo, 113-8656, JAPAN
kobayashi.ryousuke@sict.i.u-tokyo.ac.jp

‡The University of Tokyo
7-3-1, Hongo, Bunkyo, Tokyo, 113-8656, JAPAN
yamaguchi.rie@i.u-tokyo.ac.jp

Abstract In recent years, an authentication method is taken notice of using humans' behavior such as risk-based authentication. It is highly convenient for users to authenticate using history information of IP address. We consider a new authentication method using Wi-Fi information a smartphone sensor catching. Today most of people carry around their smartphones all the time, and Wi-Fi information the sensors catching is possible to characterize the users' behavior. In this paper, we examined that Wi-Fi information can be an authentication component for cognitive authentication.

1 はじめに

近年, スマートフォンが急速的に普及しており, 多くの国で普及率が 50%を超える値 [1] となっている．スマートフォンが普及したことにより, 我々の生活利便性は一層向上した. 例えばスマートフォンを利用しての EC サイトの利用である．企業側もスマートフォン専用の EC サイトを用意したり, また独自のアプリケーションをユーザーに提供することなどで, ますますスマートフォンを利用した EC サイトの活用利便性が向上してきている．

スマートフォンによるECサイトの利用が増加してきている一方で,ECサイトを利用する上で必要となる認証の方法についてはまったく変化していない. 我々はECサイトの画面上にユーザーIDとパスワードを入力して, 初めて購入することができる.(もちろんあらかじめユーザーIDとパスワードは登録しておく必要がある.) このユーザーIDとパスワードで認証する方式には2つの問題点がある. 1つ目は成りすましの問題である. ユーザーIDとパスワードが他者に漏洩したり, もしくは推測されたりした場合は容易になりすますことが可能である [2]. 2つ目はユーザビリティの問題である. ユーザーIDとパスワードを使った認証方式では, セキュリティを向上させるためにあらかじめ登録をしておく必要があることや認証時にユーザーが複雑な文字列を入力をする必要がある. 一方でスマートフォン端末を利用するユーザーが増加しており, これらのユーザーは複雑な文字列の入力がより困難となっている. この2つの問題を解決する認証技術として, 複数の行動履歴で認証を行う複合認証が注目されている. リスクベース認証などの行動履歴認証では, ユーザーが意識的に情報を入力する必要がないためユーザビリティが良いといった利点がある. 一方で, 一般的にユーザビリティの良い認証方式は認識率が低いといった欠点もある.

この欠点を補う手段として複合認証がある. 一要素の行動履歴認証では認識率が低くとも, 認証要素を複数にすることで認識率を上げることが可能となる. また複合認証では, 我々は行動履歴での複合認証を実現させるために, 認証要素を探し出さなければならない. 複合認証を実現させるために必要となる認証要素は完璧に個人を特徴づけるデータである必要はない. 複数の要素を組み合わせて個人と特定できればよいからである.

認証要素となりうる行動履歴を探すにあたり, 我々はスマートフォンが持つセンサー情報に着目した. スマートフォンが普及したことにより, スマートフォンが持つセンサー情報を容易に取得できるようになった. スマートフォンが持つセンサー情報はユーザーが意識することなく自動的に取得できるものであるため, センサー情報を利用した認証方式はユーザビリティが良いと推測される. このセンサー情報の中で我々は特に,Wi-Fiの情報に着目した. 本論文の目的はスマートフォンのセンサーが取得するWi-Fiの情報が, 認証要素となりうるかを検証することにある. 次章以降ではWi-Fiの情報を利用した認証方式を提案し, 実際にスマートフォンセンサーで取得したデータで提案した認証方式で個人認証が可能なことを示す.

2 従来の行動認証研究

2.1 スマートフォンを利用した従来の認証研究

スマートフォンを利用した認証手法の研究はこれまでにも行われている. スマートフォンのカメラを利用した手法 [3] や, フリック操作を利用した手法 [4], 加速度センサーを利用した手法 [5] などがある. しかしこれらの手法はユーザビリティの点で問題がある. カメラを利用した手法では, 認証時にスマートフォン端末を取り出してカメラでイメージを写さなければならず, フリック操作を利用した手法では, あらかじめフリック操作の情報を登録しておく必要がある. また加速度センサーを利用した手法では, スマートフォン端末の位置が重要であり, スマートフォン端末を衣服のポケットなど常に一定の位置に配置しておかなければならないといった問題がある.

2.2 Wi-Fi情報を認証に利用した先行研究

Wi-Fi情報を認証に利用した先行研究に [6] がある. 本論文の以降については先行研究 [6] を単純に先行研究と記載する. この先行研究と本論文の差異は以下2点である.

- 認証情報を構成するWi-Fiアクセスポイントのアドレス
  先行研究ではテンプレートを作成するために, センサーが取得したアドレスの中から

個人性の強いアドレスの選定を行っており, この処理を認証情報に対しても行っている. しかしこのアドレス選定処理は過去 30 日間の履歴データをもとに行っており, 端末の盗難があった場合は, 盗難者の個人性ではなく本来の端末ユーザの個人性が強いアドレスが選定される. そのためアドレス選定処理を認証情報に対しても行うのは適当ではないと考え, 本研究では認証情報に対してアドレス選定処理は行っていない.

- 認証情報に必要とするデータの時間
  先行研究では認証情報を作成するために直近 24 時間のデータを必要としている. この認証方式ではスマートフォン端末が盗難された場合, 盗難される前の本人のデータが端末に残っているため容易に成りすますことが可能となる. このなりすましを避けるために, 本研究では直近 24 時間のデータに加え, 直近 1 時間のデータも使用し認証を行っている.

3 本論文で提案する認証手法

本論文では先行研究に対して追加の手法について提案・実験を行っている. 本章では追加手法についての説明を行う. なお, 先行論文で定義された表記については本論文でも使用する.

3.1 認証情報を構成するアドレス

本論文では 2.2 節に記載した通り, 認証情報を構成するアドレスについてアドレス選定処理を行っていない. それに伴い, テンプレート T と認証情報 N の比較手法について変更している. 本節ではその比較手法について説明する.

テンプレート T と認証情報 N,T と N の比較結果 R について, 先行研究では以下の関係があった.

$$List(R) = List(T) \cup List(N) \qquad (1)$$

本研究では $List(N)$ はセンサーがキャッチしたアドレス全体の集合であり,$List(T)$ の要素数は平均して $List(N)$ の 0.73% [6] である. そのため (1) 式の関係だと比較結果 R のアドレスには重要度の低いアドレスが多く含まれることとなる. 重要なアドレスはテンプレート T を構成するアドレスであるため, 本研究では以下の通りとする.

$$List(R) = List(T)$$

また, 比較結果 R の $Value$ については図 1 の通り, 一致率 P については次の通りに定義する.

$$P = \frac{CNT(R(T,N),2)}{CNT(R(T,N),1) + CNT(R(T,N),2)}$$

$time \in \{0\text{h},1\text{h},\cdots,23\text{h}\}$, $address \in List(T)$
としたとき,
for $address$ in $List(T)$
  if $address$ in $List(N)$
    for $time$ in $\{0h, 1h, \cdots, 23h\}$
      if $Value(T, time, address) == Value(N, time, address) == 0$
        $Value(R, time, address) = 0$
      elseif $Value(T, time, address) == Value(N, time, address) == 1$
        $Value(R, time, address) = 2$
      elseif $Value(T, time, address) != Value(N, time, address)$
        $Value(R, time, address) = 1$
  else
    for $time$ in $\{0h, 1h, \cdots, 23h\}$
      if $Value(T, time, address) == 0$
        $Value(R, time, address) = 0$
      elseif $Value(T, time, address) == 1$
        $Value(R, time, address) = 1$

図 1: $Value$ の決定アルゴリズム

3.2 24 時間認証と 1 時間認証

2.2 節に記載した通り, 先行研究では直近 24 時間のデータをもって認証を行っている. 24 時間のデータで認証を行う手法は本研究と先行研究で前節以外に差異はないが, 本研究では新たに 1 時間のデータをもって認証を行う手法について提案する.

3.2.1 認証情報の作成

先行研究で提案された直近 24 時間のデータをもとに作成した認証情報は, 行が 1 時間ごとの情報で列がアドレス情報の行列となっている.

行ごとに分割すると 1 時間ごとの情報が 24 個組み合わさった情報となっている．この 24 個の情報の中で一番直近の 1 時間の情報を 1 時間認証の認証情報とする．

3.2.2 テンプレートの作成

テンプレートも 24 時間認証の認証情報と同様に, 行が 1 時間ごとの情報で列がアドレス情報の行列となっている．1 時間認証を行う際に使用するテンプレートは,24 時間認証で使用するテンプレートから比較対象の認証情報の時間に該当する情報を抜き出したものとする．例えば認証情報が 0 時の情報であるならば, テンプレートも 0 時の情報を抜き出して使用する．

3.2.3 比較

比較手法については 3.1 節と同じである．

4 実験

我々は 3 章で提案した追加手法について実験を行った．本章では実験の内容とその結果について説明する．なお, 実験データについては先行研究と同じものを使用した．

4.1 データについて

4.1.1 採取方法

被験者に常時スマートフォンを携帯させ, スマートフォンのセンサーで Wi-Fi の情報を採取した．採取したデータには Wi-Fi の BSSID とそのデータをキャッチした時間が含まれている．

4.1.2 採取条件

以下の条件でデータ採取を行った．

- 被験者人数:17 人
- データ採取期間:30 日以上
  データ採取期間については被保険者によって差異があり, 採取したすべてのデータを実験に利用した．

データの採取は 5 分ごとに行っており, 採取したデータはスマートフォン端末に保存した．

4.2 実装

4.2.1 実装

本実験のために Python3.4 を使用して実装を行った．また採取したデータは MySQL Ver14.14 を利用して作成した DB にて管理した．

実験のために実装したアルゴリズムを以下に示す．

- アドレスの選定
  先行研究と同じである．
- テンプレートの作成
  先行研究と同じである．
- 比較
  図 2 のアルゴリズムで実装を行った．

INPUT:T テンプレート,N 認証情報
OUTPUT:P 一致率

1. $R := T$
2. $Value$ の決定は図 1 の通り
3. $countT := CNT(R, 2)$
4. $countF := CNT(R, 1)$
5. $countN := CNT(R, 0)$
6. $P := countT/(countT + countF)$
7. return P

図 2: 比較のアルゴリズム

4.2.2 テンプレートの作成

先行研究と同様に, 本実験では実験期間で採取したすべてのデータをもとにテンプレートの

作成を行った．データを採取した期間は 4.1.2 項で記載した通りである．

4.2.3　認証時の情報の作成

24 時間認証について先行研究と同様に，本実験では実験期間のある 1 日のデータをもとに認証時の情報の作成を行った．1 時間認証については実験期間内の時間単位のある 1 時間をもとに認証時情報の作成を行った．

4.2.4　閾値の決定

実験では複数の閾値 k を与え，本人受入率と他人受入率の変化を確認した．

4.3　平均試行回数

本実験の試行回数は以下のとおりである．

- 本人認証：36 回
- 他人認証：573 回

4.4　実験結果

本実験では閾値 k を 0.01,0.1,0.5 と 3 パターン設定して本人受入率，他人受入率を確認した．本人受入率，他人受入率については以下の通り定義する．

- 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

4.4.1　24 時間認証

24 時間認証の結果については図 3 の通りとなった．なお，図 3 の値は被験者 17 人の平均値である．

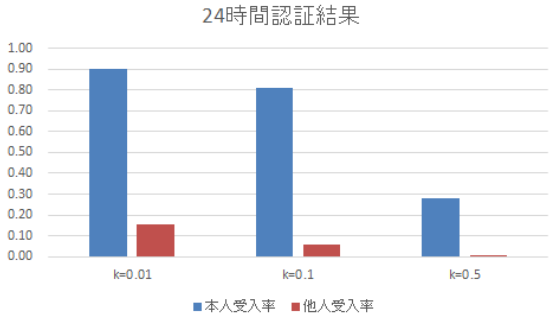

図 3: 24 時間認証結果

4.4.2　1 時間認証

1 時間認証の結果については図 4 の通りとなった．なお，図 4 の値は被験者 17 人の平均値である．

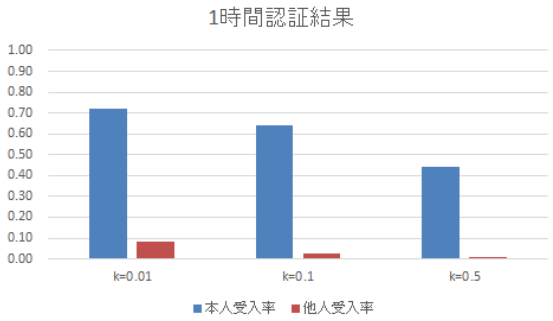

図 4: 1 時間認証結果

また時間ごとの認証結果は図 5〜図 7 の通りとなった．

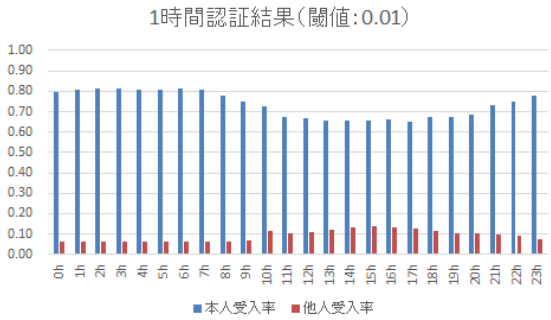

図 5: 1 時間認証の時間ごとの結果 (k=0.01)

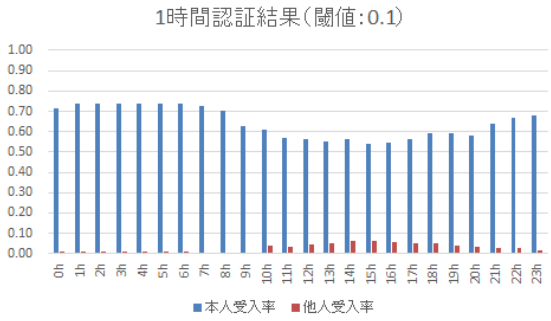

図 6: 1 時間認証の時間ごとの結果 (k=0.1)

5 考察

5.1 24 時間認証と 1 時間認証の差異

24 時間認証と 1 時間認証の結果を比較すると $k = 0.01$ や $k = 0.1$ では 24 時間認証の方が認証精度が高いことがわかる. 一方 $k = 0.5$ の場合は 1 時間認証の方が認証精度が高くなっている. これは,1 時間認証では一致率が高いケースと低いケースではっきり分かれており,24 時間認証では一致率が全体的になだらかであると想像される. 人の行動にはゆらぎがあり,1 時間単位で見ると固有の行動をとるケースととらないケースがはっきりしており,24 時間単位で見るとある程度固有の行動をとるというように捉えることができる.

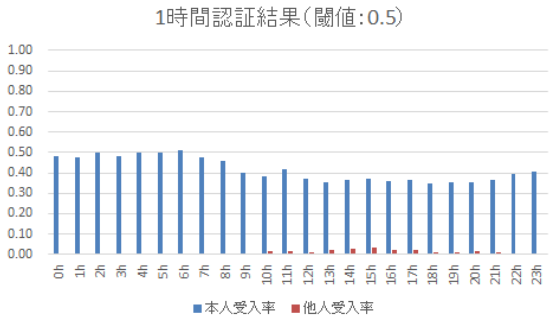

図 7: 1 時間認証の時間ごとの結果 (k=0.5)

5.2 1 時間認証の時間ごとの結果

1 時間認証の時間ごとの結果を見ると, 夜間の時間帯は認証精度が高く, 日中は認証精度が低くなっていることがわかる. 一般的に人は夜間には自宅にいることが多く, スマートフォンセンサーがキャッチする Wi-Fi 情報はある程度一定である考えられる. 一方で日中は職場や学校にいることが多いと考えられるが, 出張に出かけたりや休日は別の行動をとったりなど, 夜間と比較すると一定の行動をとらず, センサーがキャッチする Wi-Fi 情報も夜間と比較すると多岐にわたる. そのため日中と比較すると夜間の時間帯の方が認証精度が高くなったと考えられる. 前節の通り 1 時間単位では固有の行動をとるケースととらないケースがはっきりしていると考えられるが, 本節の結果もあわせて考えると, 人は夜間には固有の行動をとり, 日中は比較的異なる行動をとるということがわかる.

他人受入率については夜間より日中の時間帯の方が大きくなっている. これは実験を行った被験者が東京大学関係者であり, 日中に複数被保険者が同じ Wi-Fi 情報をキャッチすることがあったためと考えられる.

5.3 認証要素としての利用可否

5.3.1 実験結果からの検討

4.4 節での結果から,Wi-Fi の情報が認証要素となりうるかを判断する.

24 時間認証,1 時間認証ともに閾値が 0.01 など低い値では非常に高い本人受入率となっており, 実験者の中には本人受入率が 1.0 となるケースもあった. 本論文の目的としている個人認証に利用できる認証要素とは, 複合認証の一要素として利用できるかということであるから, 完全に本人と他人を区別できる必要はなく, 本人と他人とを区別できる程度に受入率に差があればよい. 結果として本人受入率と他人受入率の値は全体的に大きく差があり,Wi-Fi の情報は個人認証に利用できると判断できる. 閾値についても値を低く設定することで本人受入率が高く, 逆に値を高く設定することで他人受入率が低くなるという結果となった. 以上の実験結果から Wi-Fi の情報は認証要素となりうると判断できる.

5.3.2 認証手法の採用

本研究では 24 時間認証と 1 時間認証の 2 つについて提案・実験を行った. 結果として閾値の値で差はあるものの 24 時間認証の方が高い認証精度となった. しかしながら 1 時間認証には 2.2 に記載した通り, 端末盗難時のなりすましを比較的防ぐことができるというメリットもある. 1 時間認証は夜間帯に認証精度が高くなることを考えると, 夜間帯は 1 時間認証を採用し, 日中は 24 時間認証を採用するといった組み合わせ方式がよいと考えられる.

6 おわりに

本論文ではスマートフォンが持つセンサー情報の中で Wi-Fi 情報に着目した先行研究に加え, 以下の追加の提案・実験を行った.

- 認証情報を構成するアドレスの不要処理を削除
- 24 時間認証と 1 時間認証の比較

特に 24 時間認証と 1 時間認証の比較を行うことで, 単純にどちらかの認証手法を採用するのではなく, 組み合わせることによって認証精度とセキュリティの両面を確保できることがわかった.

スマートフォンセンサーが取得する Wi-Fi 情報で認証を行う方式は, ユーザーが意識してあらかじめ情報を登録する必要がなく, また認証時も情報を入力する必要がない. そのため従来の行動履歴認証と比べ非常にユーザビリティが良く, 大きな利点だと考えられる. スマートフォンやタブレット端末が急速的に普及してきている昨今では, これまで以上にユーザビリティが求められると考えられるため, 本認証方式は今後大いに期待されるであろう.

今後の課題は,Wi-Fi の情報を実際に認証要素として運用していくために, よりよい方式を検討していくことである. 例えば本論文ではスマートフォン端末の盗難について多少検討を行ったが, その他のなりすまし手法や, そのなりすましについて防ぐ手法などを検討していきたい.

参考文献

[1] OnDeviceResearch: Global smartphone penetration 2014, https://ondeviceresearch.com/blog/global-smartphone-penetration-2014 (参照日：2015-05-15).

[2] 大谷 和也, 柿崎 淑郎, 佐々木 良一: 情報漏えいリスクを低減するアカウント管理手法, 情報処理学会研究報告 Vol.2015-IS-131 No.1

[3] Kam Yuen Cheng,Ajay Kumar: Contactless Finger Knucle Identification using Smartphones, 2012 International Conference of the Biometrics Special Interest Group

[4] 山田 健一郎, 納富 一宏, 斎藤 恵一: スマートフォン操作時における行動的特徴量を利用した個人識別手法, バイオメディカル・ファジィ・システム学会誌 Vol.16, No.1, pp.41-48 (2014)

[5] Thanh Trung Ngo,Yasushi Makihara,Hajime Nagahara,Yasuhiro Mukaigawa,Yasushi Yagi: The largest inertial sensor-based gait database and performance evaluation of gait-based personal authentication, Pattern Recognization 47 (2014),pp.228-237

[6] 小林 良輔, 山口 利恵: p-タイル法を用いたスマホセンサーによる個人認証手法, マルチメディア, 分散, 協調とモバイル (DICOMO2015) シンポジウム pp.295-302

[7] 田村 秀行: コンピュータ画像処理入門, 総研出版, p.67, 1985