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

小林 良輔[1]　疋田 敏朗[1]　鈴木 宏哉[1]　山口 利恵[1]

概要：近年，様々のモノがインターネットにつながり，自動的に多種多様なデータが取得される IoT 時代となっている．取得される膨大な量のデータはビッグデータと呼ばれ，特に人々の行動を記録したライフログが有名である．これらのセンシングデータを解析することで，人々のライフスタイルを知ることが可能となる．センシングデータが示すライフスタイル情報から，その人の特徴を把握することが可能であり，現在でも EC サイトのリコメンデーションなどに利用されている．本論文では人々のライフスタイルや行動様式が持つ習慣性や多様性に着目し，生活行動のセンシングデータを活用した新しい個人認証技術である，「ライフスタイル認証」を提案する．

キーワード：ライフスタイル認証，IoT，ビッグデータ

Title : A Proposal of Lifestyle Authentication Based on the Behavior Sensing Log

Ryosuke Kobayashi[1]　Toshiro Hikita[1]　Hiroya Susuki[1]　Rie Shigetomi Yamaguchi[1]

Abstract: The IoT era has been coming when a variety of things are connecting to the Internet and a variety of data are automatically collected via the Internet. The enormous amount of data is called Big Data, such as life-log that is recorded data of human behavior. It is possible to know the human lifestyle by analyzing the sensing data, and we can obtain the human's characteristics from the lifestyle information acquired from the sensing data. In this paper, we propose "Lifestyle Authentication" which is a new personal authentication method utilizing the human lifestyle and its attributes.

Keywords: lifestyle authentication, IoT, BigData

1. はじめに

1.1 背景

近年，ネットワークインフラの発達やセンサーの小型化などの要因により，様々なモノがインターネットに接続されて自動的にデータが取得される IoT(Internet of Things) 時代となっている．取得されるデータは IoT 時代以前と比較すると，より精密であり多種多様であり，またリアルタイム性を帯びたものである．そのためこれらのデータ量は膨大となり，膨大となったデータはビッグデータと呼ばれている．ビッグデータとは「事業に役立つ知見を導出するためのデータ」[1] と定義されているように，ビッグデータを新たなサービスや研究に活用されることが期待されている．特に，昨今急激な進化を見せている人工知能 (AI) の分野でもビッグデータは十分に活用されている．人工知能の多大な学習のためにビッグデータが使われているのである．また一方で，ビッグデータをリアルタイムに処理し，活用するために人工知能が使われているといった面もある．

このように IoT 時代の現在，多種多様なデータがリアルタイムで自動的に取得され，活用されることが期待されている．我々はこのデータを個人認証に利用した，「ライフスタイル認証」を本論文で提案する．

1.2 現状の個人認証技術の問題点

現在，個人認証技術は web サイトへのログインなど様々なケースで利用されている．そのケースの多くではパス

[1] 東京大学
The University of Tokyo

ワード認証や，指紋などの生体認証が使われている．しかしこれらの既存手法については攻撃手法 [2][3] が知られているのが現状である．この問題を解決するための 1 つの手段として，1 つの要素で認証を行うのではなく複数の要素で認証する多要素認証がある．複数の要素で個人認証を行うことで，1 つの要素が攻撃を受けたとしても，全体としてはセキュリティを破られないといった手法である．一方で，一般的には複数の要素で認証を行う手法は，利用者のユーザビリティが低下する傾向にある．複数の要素で認証するためには，利用者が複数の認証情報を入力する必要があるからである．

そこで我々は，ユーザビリティが低下するといった問題を解決する手法として，「ライフスタイル認証」を提案する．ライフスタイル認証で利用者のユーザビリティを下げず，また多要素認証を実現することが可能となる．

2. ライフスタイル認証とは

本章ではライフスタイル認証について概念を説明し，ライフスタイル認証におけるライフスタイルの定義や属性，またライフスタイルの認証手法以外への活用例について説明する．

2.1 ライフスタイル認証の概念

現在利用されている個人認証手法は，認証時に何らかの動作を必要とするものである．パスワード認証であれば認証時にパスワードを入力する必要があるし，指紋認証であれば認証時に指をセンサーにかざす必要がある．それに対し，認証時に明示的な動作を必要としない認証手法をライフスタイル認証と呼ぶ．人は，普段の生活での行動の中で，意識せずとも同じ行動を繰り返すことがある．例えば毎朝同じ時間の電車に乗ったり，お昼に同じ店で昼食をとったり，夜に自宅に帰る，といった行動である．すなわちライフスタイル認証とは，通常の生活の中での行動パターン情報を利用した認証手法のことである．

2.2 ライフスタイル

ライフスタイル認証を認証時に明示的な動作を必要としない認証手法としたとき，ライフスタイルとは人が普段から意識せずに行っている行動のことをいう．特に，日々の生活での行動パターンや生活リズムなど習慣化された行動である．習慣化された行動にはさまざまは属性を持ち，認証要素となりうる助けとなている．次節にてその属性について具体的に説明する．

2.3 ライフスタイルの属性

大橋 [4] によると，生活リズムは 3 つの属性を持つ．本節ではその属性について説明し，ライフスタイルが認証に利用できることを説明する．

以下で 3 つの属性について説明する．

- 日中の活動と夜間の睡眠の 2 層を基本とする一日の活動形態
  人の行動は一般的に，昼間と夜間で異なるのが通常である．昼間の覚醒している時間帯に，外で仕事をしたり，学校に行ったりし，夜間の休息の時間帯には自宅で過ごし，睡眠に入る．
- 一日周期のリズム現象
  人の生活行動はパターン化されたリズム現象であり，その周期は一日単位である．その生活パターンは一日ごとに繰り返されるものということである．
- 生活リズムの多様性
  人々の生活パターンは，人によって異なる個別性を持ち，また同じ人の生活パターンでも時とともに変化していく可変性も持つ．

上記の属性で特に着目すべきは，その周期性である．個人認証では，あらかじめ登録されたデータと入力データが一致している，もしくは似通っているかの照合を行っている．つまり認証を行うための要素は，繰り返し同じ，もしくは似た情報を入力できる必要があるのである．ライフスタイルはその周期性によりこの条件を満たすことが可能となる．

その他にも個別性を持つことも，ライフスタイルを個人認証に利用するために必要な要因となる．単純に周期性を持ち，繰り返しデータを入力できるとしても，そのデータが他者と同じであれば容易に他人へのなりすましが可能となる．生体情報が個人認証に利用されているのは，その情報が他人と異なり個別性を持っているからである．ライフスタイルも生体と同じように個別性を持つことが，認証に利用できる要因となっているのである．

2.4 ライフスタイル情報の活用例

本節ではライフスタイルの情報を活用している例として，犯罪者プロファイリングについて説明する．犯罪プロファイリングとは「犯罪現場から得られた資料及び被害者に関する情報等から，犯人の性別，年齢層，生活スタイル，心理学的特徴，犯罪前歴の有無，居住地域等，犯罪捜査に役立つ情報を推定すること」と定義された [5]，犯罪情報分析の一手法である．

犯罪プロファイリングという手法を利用することで，連続的に発生した事件が同一犯によるものかどうかを判断したり，また連続事件の発生地点から犯人の居住地を推定することが可能である．これは例えば，被疑者は発生地点でタバコを吸う，などといった特徴量を解析することで可能となっている．

このように人の行動パターンは現在でも活用されている．しかしながらこれまでは，行動情報が容易に使える形にはなっておらず，上の例では犯罪現場を捜査をすること

で得られるものであった．現在では様々なモノにセンサーが搭載されており，行動情報がセンシングログとして容易に取得され，活用できるようになっている．センシングログが容易に使えるようになり，ライフスタイル情報の活用の幅が広がってきている．

3. センシングログ

ここでは，ライフスタイル認証で活用するセンシング・ライフログとは何かを述べ，そのセンシングログの取得方法や，それらの情報を活用したサービスについて述べる．

3.1 センシング・ライフログとは

センシング・ライフログとは，モノ（マシン）や個人から取得された履歴情報を指し，個人やマシンに密接に関係する人々やマシンの行動を表した履歴情報である．

これらの情報は，取得できた範囲や取得方法によって特徴が異なり，近年のスマートフォンには，位置センサー，温度・湿度センサー，加速度センサーなど様々なセンサーが取り付けられ，また，サーバサイドもビッグデータ時代と呼ばれるように簡単に情報を収集できる枠組みが整ってきたことから，センシング・ライフログの活用が可能となってきた．

これらの情報は，情報そのものの関係性や分析を行うことで，付加的な情報を得ることが出来るようになり，基本的な属性と呼ばれるような名前や住所といった情報に加えて，個人の行動に関することの取得も可能である．例えば，買い物の購買履歴を活用することで，趣味趣向が見えたり，加速度センサーを活用することで，人がどのくらい運動したのかなどの活動量への変換も可能となる．

近年は，この変換手法の工夫が活発に研究されており，特に人工知能の発展という観点では，機械学習を用いた自動的な特徴の発見の研究の応用によって，新たな利用履歴分析が可能となってきた．

3.2 取得の容易さ

前節で述べたようなセンシング・ライフログは，従来のPC からの取得に加え，スマートフォン，ウェアラブル端末など，ユーザーが持つ複数の情報機器によって取得される．このような情報に加え，スマートシティなどの普及に伴い，ユーザーの周りにある様々なセンサーの情報も活用が可能となってきたいる．ユーザーの周りには，１００個以上のデバイスが存在し，それらの情報が有機的に繋がってきた．

同時に，これらの情報を独立のものとして扱う事に加え，それぞれの情報の関係性から別の特徴を見いだすようなことも行われており，単なるログだけにとどまらないような活用方法も検討されている．

3.3 センシングログを活用したサービス

センシング・ライフログの活用事例として，購買のリコメンドサービスや天気予報などが行われてきている．また，サービス手提供者側にとっては，顧客情報を活用することが出来るため，販売促進や顧客サポートにも活用されてきた．これらによって，ユーザーのサービスに対する全体の利便性が高まることにつながっており，特にマーケティング活動において実績が報告されている [6]．

これらの情報は，目の前のサービスだけの利用にとどまらず，全く新たな価値として利用されることも多い．ユーザーとしては，センシング・ライフログの活用は，ユーザー自身とって何らかのサービスの結果としての明確な利点があるために提出してきたものであったが，最近はユーザーが気づかないところでの情報の活用が進んでいるという状況もある．

4. ライフスタイル認証の具体例

ライフスタイル認証は，3 章で述べたとおり，人々やマシンの行動を表した履歴情報である様々なセンシングログによって実現が可能となる．

この章では，センシングログとして検討可能な事例を示し，ライフスタイル認証として利用できる要素として考えられる様々な特徴について述べる．各ライフログと認証として必要な本人らしさをどのように出していくのかについて説明する．

4.1 位置情報

ライフスタイル認証における位置情報の活用法は，ユーザーの今いる位置の情報を活用して本人らしさを出すことにある (図 1)．近年のスマートフォンや PC 端末にはデフォルトで位置情報を取得する GPS 機能が附属しており，従来の衛星を活用した位置情報の取得だけでなく，WiFi や携帯電話の基地局の情報との組み合わせを活用した位置情報の取得も容易にできるようになっており，より簡易的に情報を手に入れることが出来る．

位置情報を活用した本人らしさとは，例えば，普段夜に 20 時に帰宅する人が遅くまで外にいる場合には異常と判断することが可能，というように，普段の生活パターンが現れやすい情報である，ということがある．こういった考え方は，既にリスクベース認証においては実用化されており，海外からのアクセスや普段と違うデバイスからのアクセスなどがあった場合には，エラーメッセージが登録してあるメールアドレスにメールが送付されるなどの対策がとられている．

こういった位置情報を活用した認証は複数の研究が行われており，[7][8][9] において検討がなされており，位置情報はライフスタイル認証において実用化に最も近い要素の一つということができる．

一方で，デバイスからの偽造が比較的容易である情報であるので，ユーザビリティが高い手段の一つではあるが，安全性評価については別途の検討が必要である．

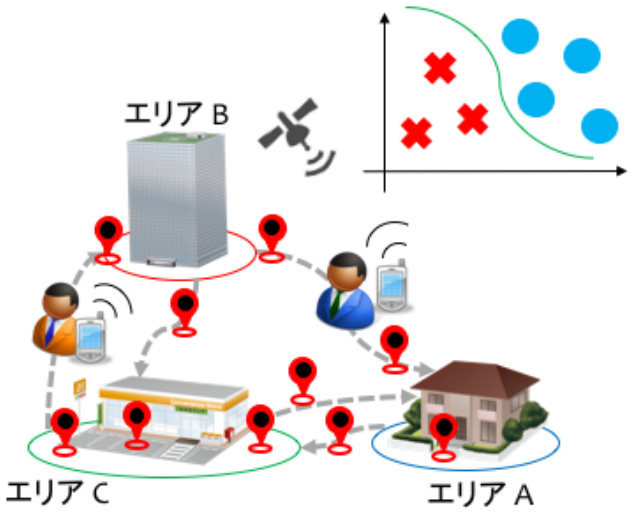

図 1　位置情報を利用した一日の行動習慣の特定

4.2　Wi-Fi

Wi-Fi 情報とは無線 LAN アクセスポイントの端末情報を意味する．近年のスマートフォンは，自動的に近辺に設定されているアクセスポイントを探し出し，その端末情報を取得するような仕組みとなっている．ライフスタイル認証における Wi-Fi 認証では，スマートフォンが取得する端末の BSSID とその取得時間を利用している [10][11]．

無線 LAN アクセスポイントは駅や職場など毎日行くような公共の場所や，自宅などに設置されており，Wi-Fi 情報の履歴を追うことで行動パターンが把握できる．

このように Wi-Fi 情報は 4.1 と互換性が高く，同様に実現性の高い要素といえる．また，GPS が屋内では精度が低下するのと比べ，無線 LAN アクセスポイントは建物に設定されていることが多く，屋内で精度が低下しないことが Wi-Fi 認証の利点である．

一方で，モバイル Wi-Fi ルータの所持者と偶然すれ違ったりすると，スマートフォンはその本人らしさから離れるノイズ情報をキャッチし，認証精度を下げる要因となる．Wi-Fi 認証の精度を保つためには，このようなノイズをうまく除去することが課題となる．

4.3　運動履歴

運動履歴とは，最近普及しているスマートウォッチやウェアラブル端末等から取得できる活動量（歩数計）を指す．

毎日の生活パターンが一定の人については，ある日の活動が始まった時間，つまり，通勤や通学が始まった時間の習慣性や毎日運動を行うことなどが特徴として現れる (図 2)．本人らしさは，毎日の運動パターンであるが，通常毎日運動をする人が突然運動をしないことや，本来活動をしていない時間に活動している情報などから本人か本人ではないかを測定する．

こういった運動履歴を表した認証については，[12][13] において検討が行われている．

今後は，相関性についての検討を行うことで，4.1 との相関性を表すことでより精度の高い認証を行うことが可能となるであろう．

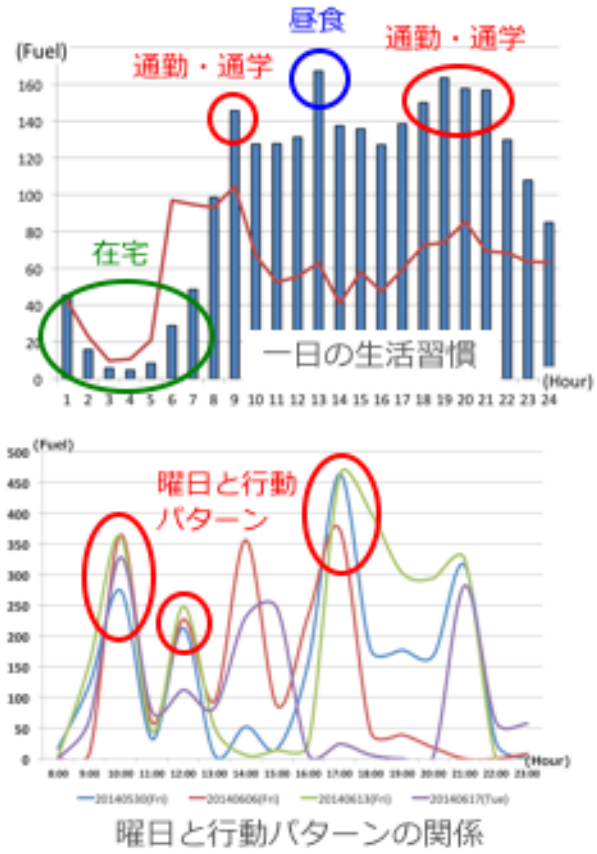

図 2　あるユーザーの運動履歴に見る行動パターン

4.4　アプリ履歴

スマートフォンでは様々なアプリケーションを利用することができる．アプリ履歴とはスマートフォン上のアプリケーションを利用した履歴情報のことである．

特定のアプリケーションでは，ユーザーによって利用時間や内容など利用パターンが一定のものがあり，その情報から個人性を抽出することが可能となる．[14] では，マンガ閲覧アプリケーションの閲覧時間に着目して，利用パ

ターンを抽出している (図 3).

図 3　あるユーザーのマンガ閲覧アプリケーション利用時間

5.　ライフスタイル認証の性質

ライフスタイル認証は，従来の認証手法と異なった様々な特徴から生じる性質を持っている．特にユーザーに負担をかけさせないことに重点があるので，ユーザーをサービス提供者，検証者の意図するような動きをさせることはコンセプトとして難しい．

様々なユーザーの生活パターンからユーザーごとにある特徴を何らからの手段で読み取らなければならない．ここでは，様々な要素に関して，共通する性質について述べる．

5.1　従来の認証とライフスタイル認証の違い

[15] に書かれているとおり，認証とは，登録時に本人確認を行い，認証情報を登録する．認証時には，登録時の情報と認証時の情報が一致しているかどうかを見ることで，認証を行っている．この節では，従来の認証とライフスタイル認証の違いについて述べる．

5.1.1　長時間の認証情報の活用

ライフスタイル認証は，ユーザーに負荷をかけさせない分，従来の認証のように，ある瞬間の情報を元にして認証情報を生成することとは異なり，ある程度長い時間の情報を活用して認証を行うことが多い．

その理由は，ユーザーの日々の行動情報を認証要素としているため，どうしてもユーザーの情報に揺らぎが生じてしまう事が上げられる．

一方で，こういった長い時間の行動情報の活用は，要素によっては，なりすましなどを瞬時に難しい可能性がある．ユーザーの利便性を十分に考慮に入れ，システムの全体設計を行わなければならない．

5.1.2　リスクベース認証との比較

リスクベース認証は，不正検知技術から発展してきた技術である．不正検知の多くは，サービス提供者持つ履歴データを解析し，通常との相違点を見つけることで不正者の追跡を行っている．従来は，システム全体の履歴データを活用し，不正者を追跡してきたが，近年は各個人ごとにおいても通常の履歴情報との比較を行うことで不正者を追跡することが可能となってきた．

これらの情報は，登録時の情報に重点をおいている従来の認証とは異なり，サービスを提供の過程で収集した情報を活用している．

本稿で述べているライフスタイル認証は，このリスクベース認証に近いものであるが，リスクベース認証では活用が検討されてこなかった履歴情報に関しても検討に含めており，より広い概念を提案している．一方で，利用している基礎的な数理モデル等は似ている．

5.2　特徴

ここでは，ライフスタイル認証において生じる特徴を述べる．

5.2.1　認証情報の Window 幅

5.1.1 節で述べた通り，利用する認証情報は，長いものとなる．そのため，認証要素ごとに認証に利用する情報の時間的な長さや量には統一的な分量はなく，ケースバイケースで，認証の精度とのバランスを見ながら決定される．また，要素だけでなく，その日のパターンによって特徴のとりやすさが変わるため，同一要素，同一人物であったとしても，毎日同じとは限らないような要素が求められている．

このように認証情報の長さにばらつきがあるため，そのばらつきを利用したような攻撃も考えられる．

5.2.2　データの信憑性

従来の認証要素のように，サービス提供者側に常に情報が集約されるとは限らない．

ユーザーが持つ端末にも複数の種類があり，スマートフォンだけでなく，同時に活用している PC，ウェアラブル端末，スマートウォッチなど，様々な端末の情報が利用可能である．

また，サービス提供者側が持つ情報も認証に活用することが可能である．アプリの履歴情報や防犯カメラ等の情報も利用可能である (図 4).

このように，統一的な規格があったとしても，様々なセキュリティポリシーによって管理されている情報は，どうしてもデータの信憑性が異なってしまう．これらが認証精度に影響が出ることを考慮すべきである．

5.2.3　認証精度のばらつき

前節で述べたことに加え，人間の行動パターンを元にした認証であるため，揺らぎが生じる．この揺らぎの結果，毎回違う認証精度が生じてしまうのはやむを得ない．それぞれの要素は，認証精度がまちまちとなったり，ユーザーの突発的な動き，例えば，旅行や特別なイベントなどでも

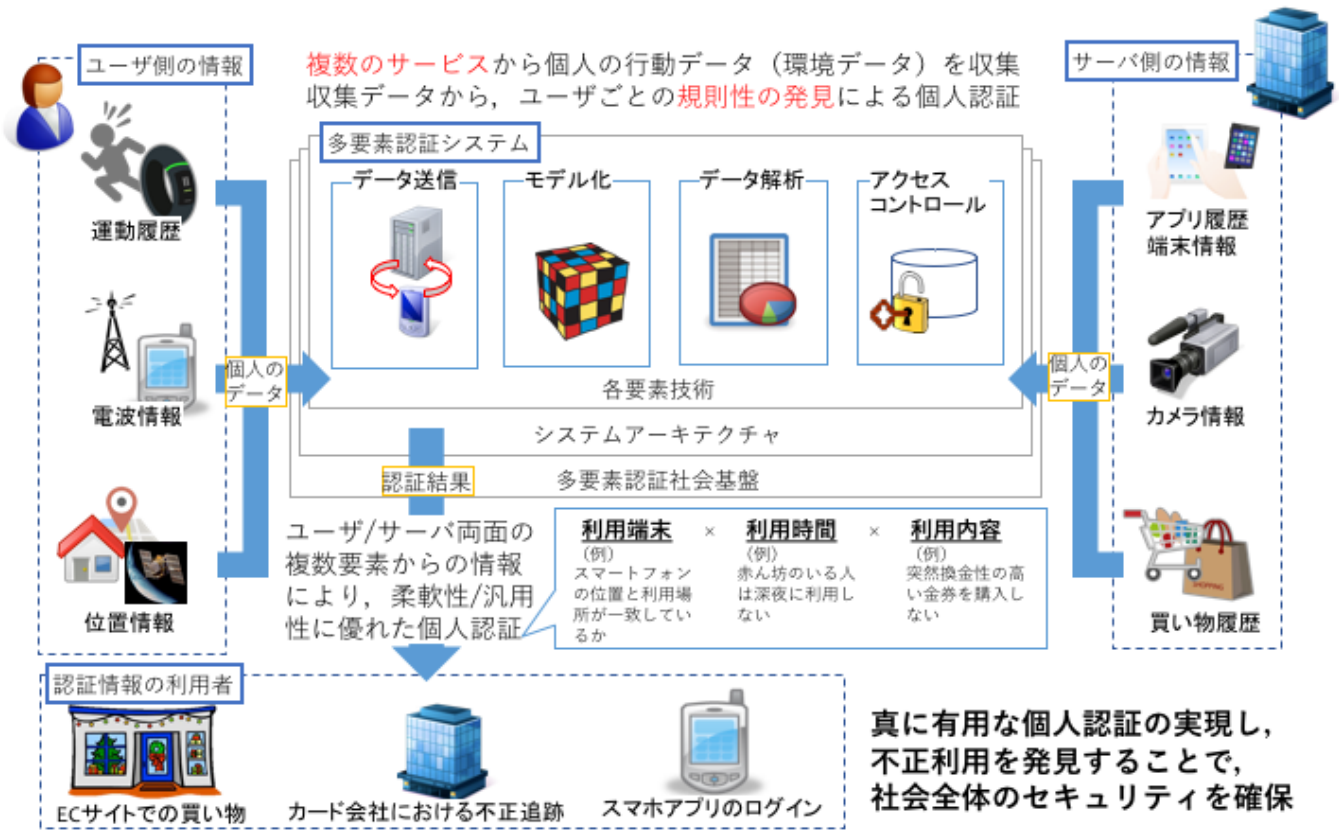

図 4　ライフスタイル認証システム

本人らしさが変わってしまう．

このような精度が違ったとしても全体でシステムの安全性を吸収するような仕組みが必要である．

5.3　問題点

本節ではライフスタイル認証の問題点について述べる．

5.3.1　プライバシー問題

ライフスタイル認証で利用する情報は，ユーザーの詳細な行動を示したプライバシー情報である．位置情報からはユーザーの自宅推定を可能としたり [16]，アプリ利用履歴からユーザーの嗜好性を見ることができる．ライフスタイル認証では新たにデータを収集するものではなく，既に収集されているデータを活用するものであるが，このデータを認証システムに活用する際にはユーザーの同意を取ることが必須となる．

5.3.2　従来認証手法の必要性

ライフスタイル認証は従来の認証手法の問題を解決する 1 つの手段として提案された．しかしながら，ライフスタイルが変化した場合の認証精度の低下や，認証情報の Window 幅の長さから一定期間は認証不可であることから，ライフスタイル認証それだけで認証システムを実現することはできない．ライフスタイル認証で認証が通らないケースの代替手段が必要となってくるのである．代替手段としては，パスワード認証や生体認証など，従来の認証手法が考えられる．

6.　おわりに

近年の社会は IoT 時代と呼ばれ，多種多様なデータがリアルタイムに収集される時代となっている．本論文ではこのデータを個人認証手法に活用した，「ライフスタイル認証」を提案した．

今後の課題として，ライフスタイル認証として利用できる要素見つけることと，多要素認証を実現するための各要素を組み合わせる手法を検討することである．

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] 総務省，「情報通信白書平成 24 年度版」（平成 24 年），http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h24/pdf/24honpen.pdf

[2] Matt Weir, Sudhir Aggarwal, Breno de Medeiros and Bill Glodek, *Password Cracking Using Probabilistic Context-Free Grammars*, 30th IEEE Symposium on Security and Privacy, pp.391-405, 17-20 May, 2009.

[3] Tsutomu Matsumoto, Hiroyuki Matsumoto, Koji Ya-

mada and Satoshi Hoshino, *Impact of artificial "gummy" fingers on fingerprint systems*, Proc. SPIE 4677, Optical Security and Counterfeit Deterrence Techniques IV, 275, April 18, 2002.

[4] 大橋久美子：看護における「生活リズム」：概念分析，聖路加看護学会誌 Vol.14 No.2 August 2010.

[5] 渡邉和美，高村茂，桐生正幸：犯罪者プロファイリング入門，北大路書房 (2006).

[6] 株式会社野村総合研究所 (総務省パーソナルデータの利用・流通に関する研究会提出資料)，：ビッグデータ時代のパーソナルデータ（ライフログ）の利用・流通に関するビジネスについて，http://www.soumu.go.jp/main_content/000190689.pdf (2016.8.12 閲覧)

[7] 石井智也，鈴木宏哉，山口利恵，中山英樹，山西健司：個人認証を見据えた位置情報による識別に関する解析，コンピュータセキュリティシンポジウム 2015, pp. 1035-1042, (2015)

[8] 船越琢矢，満保雅浩：位置情報のユーザ識別への活用，電子情報通信学会技術研究報告. SITE, 技術と社会・倫理, vol.114, pp. 71-76, (2014)

[9] Lex Fridman, Steven Weber, Rachel Greenstadt and Moshe Kam: *Active Authentication on Mobile Devices via Stylometry, Application Usage, Web Browsing, and GPS Location*, IEEE Systems Journal, Cryptography and Security, 2015.

[10] RYOSUKE KOBAYASHI and RIE Shigetomi YAMAGUCHI: *A Behavior Authentication Method Using Wi-Fi BSSIDs around Smartphone Carried by a User*, 2015 Third International Symposium on Computing and Networking (CANDAR), pp. 463-469, (2015).

[11] RYOSUKE KOBAYASHI and RIE Shigetomi YAMAGUCHI: *One Hour Term Authentication for Wi-Fi Information Captured by Smartphone Sensors*, ISITA2016, (to appear).

[12] Hiroya SUSUKI and Rie Shigetomi YAMAGUCHI: *User Authentication Trial by Behavior Data of Wearable Device*, IWSEC 2014: 9th International Workshop on Security, 2014.

[13] Hiroya SUSUKI and Rie Shigetomi YAMAGUCHI: *Cost-Effective Modeling for Authentication and its application to Activity Tracker*, WISA2015: The 16th International Workshop on Information Security Applications, 2015.

[14] 小林良輔，山口利恵：マンガアプリの閲覧作品と閲覧時間を利用した個人認証手法，マルチメディア、分散、協調とモバイル (DICOMO2016) シンポジウム, (2016)

[15] 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 (CSS2015)

[16] 堀口良太，長岡亨，畑成年：GPS 携帯電話による大規模パーソンプローブ調査のためのトリップ情報抽出手法に関する研究，土木計画学研究 講演集 (2006)