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

鈴木 宏哉　小林 良輔　山口 利恵

近年，スマートフォンの普及に伴い，様々なオンラインサービスの利用が増加している．サービス利用における重要な基盤として個人認証技術があり，多くのサービスで利用されている．一方で，サービスプロバイダがユーザ利便性だけを追求し簡易な認証を利用した結果，安全性が低下し不正アクセスを受けるという事例も多々報告されている．著者らは利便性と安全性の両方に配慮した認証手法としてライフスタイル認証を提案している．ライフスタイル認証は個人の行動履歴に含まれる個人性を用いて認証を行う手法であり，ユーザに認証のための特別な動作を要求しない認証手法である．本稿では，そのモデルと，ライフスタイル認証の有効性を評価するために 2017 年 1 月より 5 万人規模の被験者を集め実施した実証実験について報告する．

In recent years, smartphones became widespread and online services is increasing. User authentication technology is the basis of the services. However, the security of user authentication technology is not sufficient. We proposed lifestyle authentication as an authentication method considering both security and usability. Lifestyle authentication is a method of authenticating using individuality included in user behavior history. It does not require the user to perform a special action for authentication. In this paper, we describe the model of lifestyle authentication and an experiment for data collection.

1　はじめに

近年，スマートフォンの普及に伴い，オンラインサービスの利用が増加している．サービス利用における重要な基盤として個人認証技術があり，Web サイトへのログインなど様々な場面で利用されている．その多くでパスワード認証や，指紋などの生体認証が使われている．一方で，サービスプロバイダがユーザ利便性だけを追求し簡易な認証を利用した結果，不正アクセスを受けたという事例も多々報告されている．この問題を解決するための 1 つの手段として，単一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．複数の認証要素を用いる事で，ある認証要素の安全性が低下しても全体の安全性が担保できるという特徴がある．しかし，同時に認証要素の増加は利用者のユーザビリティの低下を招くという側面もある．これは認証要素の数だけ利用者が認証情報を入力する必要があるためである．

そこで，著者らは利便性と安全性の両方に配慮した認証手法としてライフスタイル認証を提案している [8] [15]．ライフスタイル認証は個人の行動履歴に含まれる本人らしさを用いて認証を行い，認証のための特別な動作をユーザに要求せずに多要素認証を実現する手法である．本稿では，リスクベース認証との比較によりそのモデルと，ライフスタイル認証の有効性を評価するために 2017 年 1 月より約 3ヶ月半で延べ 57,046 人規模の被験者を集め実施した実証実験について報告する．

2　既存研究とライフスタイル認証

個人認証手法には様々な技術があり，利用用途に合わせて単独または組み合わせて利用されている．2 章では，オンラインサービスで利用されている代表的な

---

* Lifestyle Authentication Model and Experiment for Data Collection

Hiroya Susuki, Rosuke Kobayashi, Rie Shigetomi Yamaguchi, 東京大学, The University of Tokyo.

認証手法の一つであるリスクベース認証の適用例を元に既存の認証技術について述べる．

2.1 特徴による認証手法の分類

個人認証には，知識，所持，生体の認証の 3 要素と呼ばれる認証要素の種別ごとの分類以外に，各認証要素の用い方や性質によって名付けられている区分がある．なお，各用語は定義の統一がなされておらず，用語の利用者によって解釈に幅があり曖昧性がある．

多要素認証 (Multi-Factor Authentication)

多要素認証は複数の認証要素を組み合わせるものである．一般的な事例としては，IC カードと PIN 認証を利用した銀行 ATM などがある．ビジネス用途では RSA の SecurID などのように，ハードウェアトークンやソフトウェアトークンを利用したワンタイムパスワード (OTM) の普及も進んでいる [6]．

暗黙認証 (Implicit Authentication)

通常，認証はユーザの明示的な動作によって実行される．パスワード認証であればパスワードの入力，指紋認証であれば指紋を読み取り機でスキャンする，IC カード認証であれば，IC カードを読み取り機にかざす，といった操作である．一方，暗黙認証は認証のための明示的な動作を必要としない [4] [2] [3]．代表的な例として顔認証がある．通路に設置されたカメラで撮影した顔画像から認証を行い，扉の施錠を解除したりする事ができる．なお，スマートフォンの顔認証のようにユーザが端末を顔に向ける操作などを必要とする場合は暗黙認証には含まない．

継続認証 (Continuous Authentication)

通常，個人認証では利用の度に認証を必要とするが，頻繁に利用するサービスのために毎回認証操作をする事は利便性の低下に繋がる．近年ではブラウザに ID・パスワードを記憶する機能や，パスワード管理ソフトなども登場し，ユーザがパスワードを記憶する必要が無い仕組みも存在している．しかし，これらの仕組みは他人にブラウザを利用されたり，管理ソフトのマスターパスワードの漏洩などの問題がある．そこで，認証は毎回行いつつ認証操作を簡略化する仕組みとして研究されているのが，継続認証である．Xu らはスマートフォンのタッチ操作を認証要素に用いる事で継続認証をする研究を行なっている [7]．継続認証にタッチ操作を用いる事で暗黙認証となっており，認証のための動作を必要としていない．継続認証では暗黙認証と組み合わされる事が多く，継続認証に暗黙認証が含意される事もある．

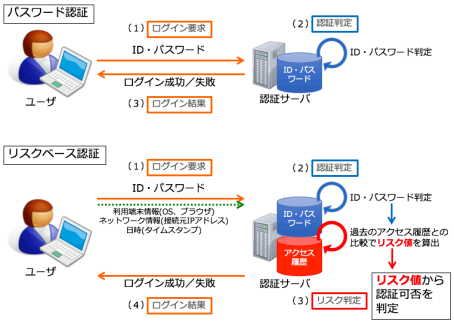

図 1　パスワード認証とリスクベース認証の比較

リスクベース認証 (Risk-based Authentication)

リスクベース認証は認証要求のリスクの度合いを用いる認証手法である．リスクとは，なりすましなどで本人ではない他人がログインしようとしている可能性であり，それを数値化したものがリスク値である．単にルールベースにより特定のパターンの場合は高リスクと判定するような実装から，確率値を求めるような実装も存在する．リスクが高い場合に，単純に認証失敗とする実装もあれば，追加の認証を要求する実装もある．

2.2 リスクベース認証の実用例

2.2 節では前節で示したリスクベース認証の具体例を用い，どのように安全性と利便性の両立を図っているかを示す．

図 1 は，パスワード認証とリスクベース認証を比較した図である．リスクベース認証の例は，パスワード認証にリスクベース認証を組み合わせた例である．通常，パスワード認証は入力された ID とパスワードが登録されているデータと一致するかを確認し，認証判定を行う．図 1 の例では，リスクベース認証はこの ID とパスワードが入力される際に得られる副次的な情報を認証情報として利用している．利用端末情報

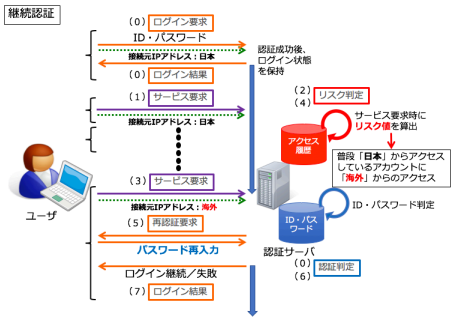

図 2　継続認証とリスクベース認証の組み合わせ例

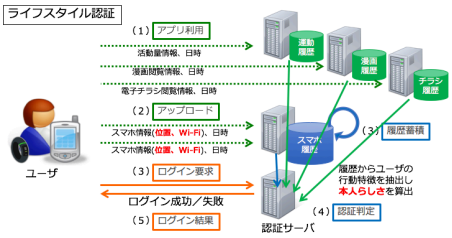

図 3　ライフスタイル認証

(OS，ブラウザ) やネットワーク情報 (接続元 IP アドレス)，日時 (タイムスタンプ) を用いて，過去のアクセス履歴から普段のユーザ環境と一致するかや，ログイン時間帯などの普段のユーザの振る舞いと一致するかを元にリスク判定を行う．これはユーザ自身が明示的に提示している情報ではなく，暗黙的な情報であり，暗黙認証を行なっていると言える．更に接続元 IP アドレスが海外であったり，特定の要注意国からのアクセスであったりといった周辺知識もリスク判定に加味される．リスクが高かった場合，追加認証を行う実装も多い．例えば，大分銀行では「秘密の質問」による追加認証を行なっている [16]．

図 2 は，継続認証とリスクベース認証の組み合わせ例である．この例では，ユーザのアクセス元 IP アドレスを暗黙認証の情報として用い，アクセス元 IP アドレスから判定されるリスク値が低ければ認証を継続する事できる．ユーザは毎回ログイン認証を行う必要が無く，例えば出張などで普段のアクセス元と異なる海外からログインする場合はリスクが高くなり追加認証が必要となる．これは前節で説明した全ての認証技術を適用した事例である．このようにリスクベース認証では，履歴情報を認証要素に用いる事で利便性と安全性の両立を図っている．一方で，利用可能な情報が主となる認証要素に付帯する情報を用いており，収集可能な情報に限りがあるという問題もある．

2.3　ライフスタイル認証

ライフスタイル認証ではリスクベース認証の考え方を発展させ，ユーザの行動履歴から認証を行う手法である [12]．人は普段の生活中で意識せずとも同じ行動を繰り返している．例えば，毎朝同じ時間の電車に乗り，お昼に行きつけの同じ店で昼食をとり，夜に自宅に帰る，といった行動パターンである．従来はこのような行動履歴のデータの収集は困難であったが，スマートフォンなどのモバイル端末の普及により，ユーザの位置情報などを常時収集する事が可能となっている．更に，スマートフォンにインストールされているアプリケーションの利用履歴も行動パターンの解析に有用である．これらの情報から認証を行うのがライフスタイル認証である．ライフスタイル認証は，図 3 の例のようにより多くの認証情報を組み合わせる事ができ，要求される安全性に応じて認証要素の組み合わせを変える事ができるという特徴を持つ．

3　ライフスタイル認証

ライフスタイル認証には多種の認証要素が用いられる．3 章では，図 3 で示したライフスタイル認証の各要素の具体例を挙げる．なお，現在着手している要素はあくまで一例であり，ライフスタイル認証の要件を満たすと考えられる認証要素は多数存在する．

3.1　位置情報

近年のスマートフォンやモバイル端末には GPS 機能が附属しており，端末の位置情報を知る事ができる．加えて，GPS 衛星を活用した位置情報の取得だけでなく，携帯電話の基地局情報や Wi-Fi のアクセスポイントを組み合わせる事で，衛星が見えない場所においても位置情報の取得ができるようになっている．更に，屋内位置推定の研究も行われており，今後は常時位置推定が可能になると考えられる．位置情報

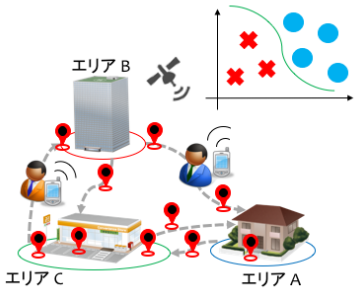

図 4　位置情報を利用した認証

を活用した認証については，既に多くの研究が行われている [13] [14] [1].

3.2　Wi-Fi 情報

Wi-Fi 情報とは無線 LAN アクセスポイントの電波情報を意味する．スマートフォンは端末周辺のアクセスポイントを自動的に探し出し，その電波情報を取得する仕組みを持つ．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．Wi-Fi 認証では，アクセスポイントの BSSID とその取得時間を利用している [5].

3.3　運動履歴

運動履歴とは，古くは歩数計などで記録していた生活の中の活動に伴う運動強度 (活動量) を数値化し，記録したものである (図 5)．活動量は近年普及が進むスマートウォッチやウェアラブル端末等から取得でき，毎日の運動パターンなどから本人らしさが得られる [18].

3.4　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．アプリ履歴とはそのアプリケーションを利用した履歴情報のことである．アプリケーションの中には，ユーザ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．既存研究 [10] 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，

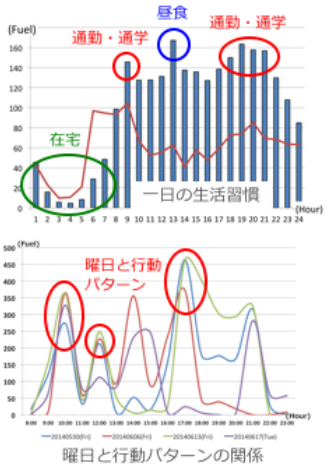

図 5　あるユーザーの運動履歴に見る行動パターン

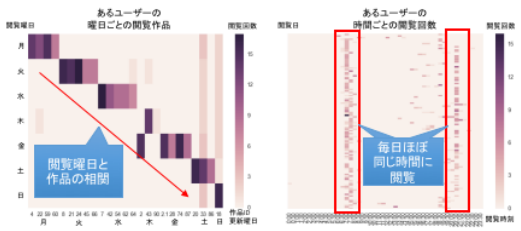

図 6　あるユーザーのマンガ閲覧アプリケーション利用時間

利用パターンを抽出している (図 6).

4　ライフスタイル認証実証実験

4 章では，ライフスタイル認証実証実験について説明する．

4.1　実証実験目的

従来の個人認証の研究では，個別の認証要素に関する研究が主であり，多要素認証の研究は比較的少ない．また，多要素認証の実験を行っていても数十人から数百人規模の実験がほとんどであり，大規模な多人数のデータを集めた事例は少ない．本実験では既存の事例にはない 5 万人規模のデータを収集する事が目的である [19]．なお，実験にあたり東京大学の倫理審査の承認を得て実施した．

表 1　実証実験全体の実験参加者数 (重複を含む)

データ種別	収集方法	参加者
MITHRA データ	MITHRA アプリ	16,027
漫画閲覧履歴	マンガワン	7,584
電子チラシ履歴	Shufoo!	33,338
活動量計データ	活動量計	97
合計		57,046

図 7　左図: **MITHRA** アプリ同意画面 (一部)，右図: ユーザ情報登録画面

4.2　データ収集

実験は，2017 年 1 月 11 日 (水) から 2017 年 4 月 26 日 (水) までの約 3ヶ月半で実施した [20]．実証実験全体の参加者数については，表 1 のようになった．なお，表の参加者数には重複する参加者を含む．

収集データは表 1 に示す通り，MITHRA アプリで収集するスマートフォンデータ以外に漫画閲覧履歴，電子チラシ履歴，活動量計データの 3 種がある．

実証実験では，スマートフォンの各種センサーを用いて位置情報や Wi-Fi 情報などを収集するためのスマートフォンアプリ（MITHRA アプリと呼ぶ）を作成した．漫画閲覧履歴，電子チラシ履歴のデータ収集実験に参加する場合は，各社のアプリ (Shufoo! [17]，マンガワン [9]) をインストールする．活動量計実験については，MITHRA アプリのインストールに加え，配布する活動量計 (オムロンヘルスケア社製 HJA-750C) を身に付けて実験に参加する．

アプリのインストール後，起動時に図 7(左図) のような同意画面が表示される．同意の手順に引き続き，図 7(右図) のようなユーザ登録画面が表示される．同意とユーザ登録の両方が終了後，データ収集を開始する．なお，マンガワン，Shufoo!，活動量計実験はそれぞれに実験参加者の同意を取り実施した．

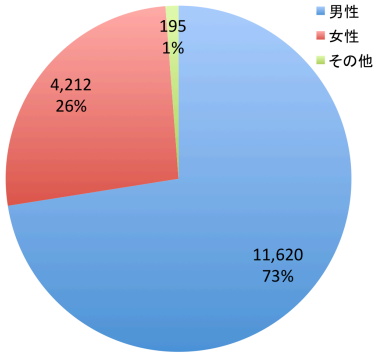

図 8　登録者の性別内訳

5　実証実験の収集データ

5 章では，実証実験の収集データについて述べる．

5.1　MITHRA アプリ実験の総参加者数

実験期間中に MITHRA アプリの実験には 17,216 件の登録があり，うち 924 件が「辞退」，機種変更などで登録が「無効」になった件数が 265 件となった．残る有効参加者数が 16,027 件となっている．

5.2　ユーザ登録情報

本実験ではユーザ属性を分析するために MITHRA アプリの初期登録画面でユーザ登録情報の入力を求めた．ユーザ属性「性別」「年代」「居住地域」の登録は，選択肢による自己申告制としたため，全員が事実を入力しているとは限らない．そのため，入力を忌避する実験参加者によって，選択肢の先頭項目「性別: 男性」「年代: 10 代」「居住地域: 北海道地方」が選択されている可能性を考慮する必要がある．

5.3　MITHRA アプリ収集データ項目

表 2 は，本実験で収集するデータの種別，データ収集間隔などを記載している．表 3 は，表 2 の MITHRA

表 2　MITHAR アプリで収集するデータ．○は MITHRA アプリが収集するデータ，△は全被験者が対象ではなく別途収集するデータ，電子チラシ履歴のみ MITHRA データを提供しない実験参加者がいる

データ 項目	収集 項目	収集 アプリ	データ 収集端末	データ 収集間隔	備考 備考
端末情報	○	MITHRA	スマートフォン	5 分間隔／トリガー	Android ／ iOS*
IP アドレス	○	MITHRA	スマートフォン	5 分間隔／トリガー	(*iOS 版は前回測位から
Wi-Fi	○	MITHRA	スマートフォン	5 分間隔／トリガー	の移動や基地局の変化を
位置情報	○	MITHRA	スマートフォン	5 分間隔／トリガー	トリガーとして収集)
漫画閲覧履歴	△	マンガワン	スマートフォン	利用毎	アプリ連携
電子チラシ履歴	△	Shufoo!	スマートフォン	利用毎	アプリ連携
活動量	△	ー	活動量計	10 秒間隔	活動量計を配布

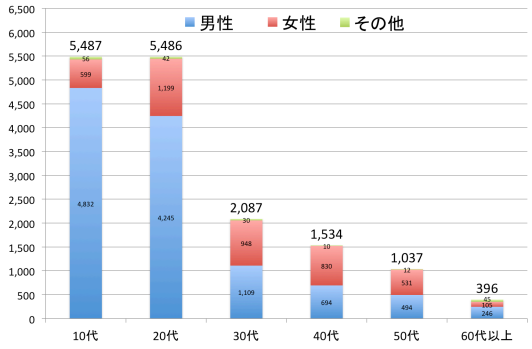

図 9　登録者の年代性別内訳

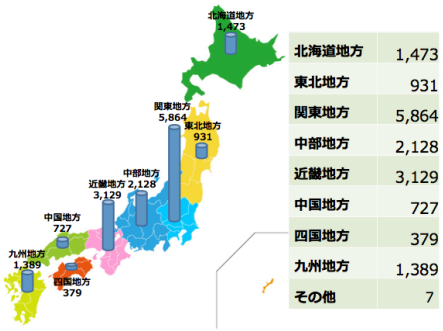

図 10　登録者の居住地域内訳

アプリが収集するデータ項目の詳細を一覧にしたものである．端末情報，IP アドレス，位置情報とはスマートフォン自身から得られるその端末の情報である．Wi-Fi とは，スマートフォン自身が接続しているアクセスポイント，または端末周辺のアクセスポイントの SSID，BSSID の情報の事である．

表 3　MITHAR データセットに含まれるデータ項目

大項目	小項目
記録日時	年月日時分
ユーザ情報	アプリのユニーク ID， メールアドレス (任意入力)
端末情報	端末型番， OS，OS バージョン
Wi-Fi 情報	割り当て IP アドレス， 接続先 BSSID，周辺 AP の SSID / BSSID / 信号強度
位置情報	緯度，経度，データソース， 衛星数，精度

MITHRA アプリは Android 版と iOS 版の両方を提供したが，両者には違いが存在する．スマートフォン OS の違いによる最も大きな差は，データ収集間隔にある．Android 版はタイマー起動により定期的にデータを収集するが，iOS 版は Apple のポリシーによりタイマー起動が許されず，Significant-Change Location Service と呼ばれる前回の測位から大きく位置が変動した場合にコールバックが呼ばれる API をトリガーとした．そのため iOS 版では大きな移動や基地局の切り替わりが無いとデータ収集されない実装となっている．

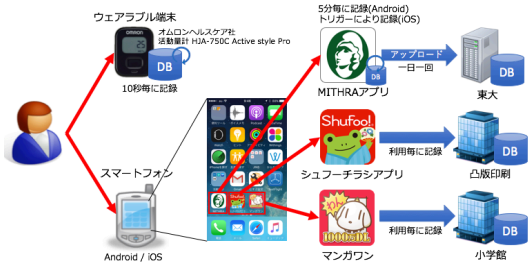

図 11　データ収集とアップロード

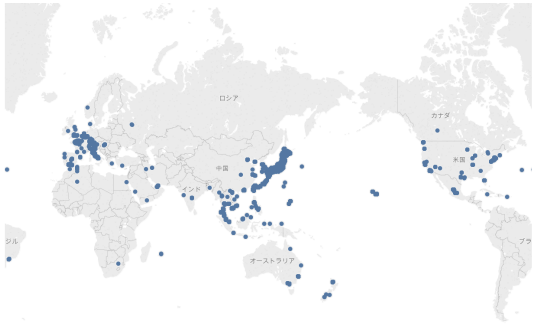

図 12　全実験参加者の移動先を世界地図にプロット

5.4　アップロードデータ数

1 日分を 1 件としてデータをアップロードする (図 11)．アップロード総数は 247,569 件であった．参加者 16,027 名のうち，実際に 1 件以上のデータをアップロードした実験参加者は 7,629 名であった．残りの約 8,500 名は実験参加に同意したもののアップロード前に辞退またはアンインストールした参加者である．

5.5　位置情報データ

3/31 時点までのアップロードデータから抽出した位置情報データの総件数は 23,444,482 件であった．図 12 は収集した位置情報データを世界地図にプロットしたものである．実験期間中に国外に移動した実験参加者の移動履歴が確認できる．

5.6　Wi-Fi データ

3/31 時点までのデータについて収集した Wi-Fi データの総件数は 121,112,775 件であった．1 件のデータには「SSID，BSSID，信号強度」が 1 セット含まれる．例えば，ある場所に 3 台のアクセスポイント (AP) があり，各 1 種類の信号を発している場合，1 回の記録時点でのデータ件数は 3 件となる．

5.7　漫画閲覧履歴データ

2015 年 9 月に実施した前回実験時は 49,261 人から 2015/8/24 から 2015/12/17 の閲覧データを収集した [10] [11]．今回の実験ではマンガワンデータのみではなく，漫画閲覧履歴データと MITHRA データの両方の提供に同意した被験者 7,584 名からデータを収集した．

5.8　電子チラシ履歴データ

Shufoo!の電子チラシの閲覧履歴データについては，閲覧履歴データの提供に同意した実験参加者が 33,338 名である．このうち MITHRA データの提供にも同意した被験者数は 2,596 名であった．なお，漫画閲覧履歴と電子チラシ履歴の両方の実験に参加した実験参加者が 2 名含まれていた．

5.9　活動量計データ

活動量計実験の結果についてはこれからの解析となるため，本稿では詳細を述べない．今回の実験では，オムロンヘルスケア社製の活動量計 HJA-750C を 97 名の実験参加者に配布し，データ収集を行った．HJA-750C は医療機関向けの活動量計であり，10 秒間隔で活動量 (METS) を記録することができる．既存研究として，Nike 社の活動量計 FuelBand を用いた個人認証の研究があるが，1 分単位の活動量を用いたものである [18]．

6　まとめ

本稿では著者らが提案するライフスタイル認証のモデルを既存のリスクベース認証との比較により示した．更に，ライフスタイル認証の有効性を評価するために実施したデータ収集実験について示した．ライフスタイル認証とは，スマートフォンを始めとするセンサーの増加による収集可能になった多量のユーザ行動の履歴データを利用し，認証を行う手法である．今回の実験ではスマートフォンにより収集できるデー

タ，漫画閲覧履歴，電子チラシ履歴，活動量を用いたが，ライフスタイル認証の認証要素はこれに限るものではない．今回収集した 5 万人規模のデータを解析し，各認証要素の有効性を評価すると共に新たな認証要素となり得る履歴データの特徴を見つける事でより多くの認証要素を見出す必要がある．

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] Fridman, L., Weber, S., Greenstadt, R., and Kam, M.: Active authentication on mobile devices via stylometry, application usage, web browsing, and GPS location, (2015).

[2] Hayashi, E., Das, S., Amini, S., Hong, J., and Oakley, I.: Casa: context-aware scalable authentication, *Proceedings of the Ninth Symposium on Usable Privacy and Security*, ACM, 2013, pp. 3.

[3] Jakobsson, M., Shi, E., Golle, P., and Chow, R.: Implicit authentication for mobile devices, *Proceedings of the 4th USENIX conference on Hot topics in security*, USENIX Association, 2009, pp. 9–9.

[4] Khan, H. and Hengartner, U.: Towards application-centric implicit authentication on smartphones, *Proceedings of the 15th Workshop on Mobile Computing Systems and Applications*, ACM, 2014, pp. 10.

[5] Kobayashi, R. and Yamaguchi, R. S.: A Behavior Authentication Method Using Wi-Fi BSSIDs around Smartphone Carried by a User, *2015 Third International Symposium on Computing and Networking (CANDAR)*, IEEE, 2015, pp. 463–469.

[6] RSA: RSA SecurID(参照 2017-9-4), https://www.rsa.com/ja-jp/products-services/identity-access-management/securid, 2017.

[7] Xu, H., Zhou, Y., and Lyu, M. R.: Towards Continuous and Passive Authentication via Touch Biometrics: An Experimental Study on Smartphones, *Symposium On Usable Privacy and Security, SOUPS*, Vol. 14, 2014, pp. 187–198.

[8] キーマンズネット: 何もしないで本人認証できる?ライフスタイル認証 (参照 2016-12-7), http://www.keyman.or.jp/at/30009164/.

[9] 株式会社小学館: マンガワン (参照 2017-8-22), http://manga-one.com, 2017.

[10] 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).

[11] 小林良輔, 山口利恵: マンガアプリにおける閲覧ならびにその他の利用履歴情報を活用した個人認証手法の提案, *SCIS2017* 暗号と情報セキュリティシンポジウム, No. 4D2-3(2017).

[12] 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(2016), pp. 1284–1290.

[13] 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* 論文集, Vol. 2015, No. 3(2015), pp. 1035–1042.

[14] 船越琢矢, 満保雅浩: 位置情報のユーザ識別への活用 (情報セキュリティ, ライフログ活用技術, ライフインテリジェンス, オフィス情報システム, 一般), 電子情報通信学会技術研究報告. *SITE,* 技術と社会・倫理, Vol. 114, No. 320(2014), pp. 71–76.

[15] 大豆生田崇志: スマホの利用履歴がＩＤ・パスワードに東大など「ライフスタイル認証」の実験開始, Vol. 2016 年 7 月 7 日号, 日経 BP 社, 2016, pp. 012.

[16] 大分銀行: 追加認証（リスクベース認証）(参照 2017-9-4), https://www.oitabank.co.jp/deposit-services/web/internetbanking/auth.html, 2017.

[17] 凸版印刷株式会社: Shufoo! (参照 2017-8-22), http://www.shufoo.net/biz/index.html, 2017.

[18] 鈴木宏哉, 山口利恵: ウェアラブルデバイスを活用した個人の行動によるユーザ認証の検討, *SCIS2015* 暗号と情報セキュリティシンポジウム, (2015), pp. 4C2–4.

[19] 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-, *SCIS2017* 暗号と情報セキュリティシンポジウム, No. 4D2-1(2017).

[20] 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 *(DICOMO2017)* シンポジウム, No. 1H-2(2017).