個人認証における認証要素の時間的特性に関する考察

鈴木 宏哉[1,a)]　山口 利恵[1,b)]

概要：近年，モバイル端末の普及とオンラインサービスの増加により，ユーザ行動の履歴情報を常時記録できるようになってきた．これらの行動履歴情報はレコメンデーションなど様々なサービスで活用されており，個人認証の分野においても行動認証としてリスクベース認証などに利用され始めている．一方で，ユーザ行動はユーザを取り巻く環境の変化に応じて変動するため，履歴情報を用いる行動認証では認証情報の時間的性質を考慮する必要がある．本稿では，個人認証における時間的性質について考察し，履歴情報を用いた行動認証と既存の個人認証手法との違いを整理する事で，認証要素を選択するための指針の一つを提供する．

キーワード：行動認証，経時変化，テンプレート更新，モデル化

An Analysis of Time Characteristics of the User Authentication

Hiroya Susuki[1,a)]　Rie Shigetomi Yamaguchi[1,b)]

Abstract: The spreading mobile devices and increasing online services, it becomes that much easier to record user's behavioral data. The behavioral data is utilized effectively for various purposes such as recommendation services. In the authentication field, the behavioral authentication also utilizes the data. However, user behavior is changed by the environmental changes over time. Therefore, behavioral authentication needs to consider time characteristics of the authentication factors. In this paper, we organized the characteristics and discussed difference of authentication factors.

Keywords: Behavioral Authentication, Temporal Changes, Template Update, Modeling

1. はじめに

近年，モバイル端末の普及とオンラインサービスの増加により，モバイル端末上のセンサーや端末上で利用しているサービルのログを用いて，ユーザの移動履歴や購買，運動履歴など様々な行動履歴情報を常時記録できるようになってきた．行動履歴情報には，ユーザ個人の生活習慣や趣味嗜好が含まれており，レコメンデーションなど様々なサービスで活用されている．個人認証の分野においても，この履歴情報を利用し，行動的特徴を用いた個人認証（以後，行動認証と記す）の研究がなされている [1][2]．行動認証が実際に利用されている事例の一つとしてリスクベース認証がある．リスクベース認証には，ユーザ自身が明示的な認証の操作を行う必要がないという利点がある．例えば，Google はアクセス元 IP アドレスの履歴などを用いたリスクベース認証を行っている [3]．Google は，利用者の過去のアクセスにおける IP アドレスや利用している端末，ブラウザなどの利用端末情報を履歴として用い，不審な認証要求に対して警告を行ったり，追加の認証を求める仕組みを提供している．その他の事例としては，オンラインバンキングやクレジットカードによる購買において，購買時の時間帯や金額，送金，購入先が過去の履歴と異なる疑わしい行動の場合に操作を停止するようなリスクベース認証がある．この時，行動認証はユーザが明示的に認証の操作を行う必要がない点が特徴の一つであり，利便性の高い認証手法と言える．一方で，行動認証はユーザの行動履歴を

[1] 東京大学
The University of Tokyo, 7-3-1 Hongo, Bunkyo-ku, Tokyo 113–8656, Japan
[a)] susuki.hiroya@sict.i.u-tokyo.ac.jp
[b)] yamaguchi.rie@i.u-tokyo.ac.jp

元に認証するため，直近のユーザの行動や過去の一定期間のユーザの行動が認証の精度にも影響を与えてしまう．更に，ユーザ行動はユーザ自身やその周辺環境の変化によって変動するため，履歴情報を用いた行動認証では認証情報の時間的性質を考慮する必要がある．

本稿では，認証情報の時間的性質を考慮した認証のモデル化と，行動認証と従来の認証要素との違いについて検討，整理を行った．なお，本稿では，時間経過による情報処理機器の性能向上に伴う危殆化などについては検討しない．

本論文の構成は次のようになっている．2 章では，行動認証に関する関連研究について紹介する．3 章では，本稿で用いる用語と認証のモデルについて説明する．4 章で既存の様々なサービスで用いられる認証手法を元に時間的特性について考察を行い，5 章で結論を述べる．

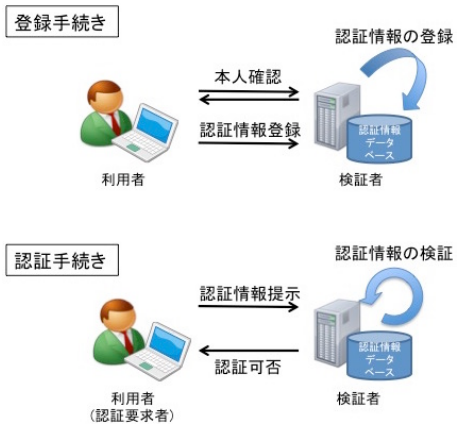

図 1　認証の手続き (登録・認証)
Fig. 1　The procedure of registration and authentication

2. 関連研究

2 章では，行動認証とテンプレート更新に関する関連研究について紹介する．

2.1 行動認証

近年，研究が進んでいる認証手法として，行動的特徴を用いた認証 (以後，行動認証と記す) がある．行動認証は従来，生体認証の一種に分類されてきたが，本稿では行動認証を認証の 3 要素と同様の分類項目として扱う．

行動認証には，歩容認証 [4] や署名 [5]，キーストローク [6] を用いた研究があり，歩行や署名，キーボードのタイピングなどの人間の動作や行動に含まれる個人性を用いて認証を行う手法である．実サービスでの利用が進む行動認証手法としては，リスクベース認証がある．リスクベース認証は，ユーザのアクセス履歴など過去の行動履歴などを元に不正のリスクを評価するもので，利用者自身が明示的な操作を行う必要の無い暗黙的な認証要素が用いられている．代表的な事例として，利用者の過去のアクセスにおける IP アドレスや利用している端末，ブラウザなどの利用端末情報を用いた Google のリスクベース認証がある [3]．また，スマートフォンや活動量計などのモバイルデバイスの普及により，従来は収集できなかった行動的特徴が収集できるようになっており，位置情報を用いた認証や，Wi-Fi のアクセスポイント情報を用いた認証 [7]，活動量計を用いた認証など [8] が提案されている．

行動認証には，他の認証要素と異なる特徴として時間的性質がある．利用者本人の過去の履歴情報から作成された情報と入力データの比較により認証を行うという点と，認証時に入力されるデータが時系列の連続値である点の二つの特徴がある．行動認証は近年研究が進んでいる認証手法ではあるが，特徴的な時間的な性質が十分に考慮されておらず，他の認証要素と比較して特徴的な性質を整理する事で認証要素を選択する際の判断材料になり得る．

2.2 認証の 3 要素とテンプレート更新

認証手法は，各認証要素の特徴の違いから大きく，知識認証 (Something You Know)，所持認証 (Something You Have)，生体認証 (Something You are) の 3 つに分類されており，「認証の 3 要素」と呼ばれている [9]．多要素認証では特徴の異なる認証要素を組み合わせる事が推奨されており，認証要素の特徴を整理する上でこの認証の 3 要素の違いを考慮する事は重要である．一方で，認証の 3 要素にまたがって比較した研究は無く，生体認証の各認証要素の比較 [10] のように 3 要素の中での評価を行った研究が主となっている．各認証要素の相関について検討した研究は無く，特に本稿で着目している認証要素の時間的性質の違いについては検討されてこなかった．

生体認証は，人間の身体という経年変化があるものから認証情報を取得するため，特に時間的な性質を考慮する必要がある．通常，生体認証に用いられる認証要素は成長や老化の影響を受けにくい特徴を用いているが，経年変化の考慮は必要であり，特に長期的に利用する認証システムや成長による変化の大きい子供が利用する場合は認証精度への影響を考える必要がある．顔認証 [11]，指紋認証 [12] など各認証要素毎にテンプレート更新の研究がなされており，経時的な変化の抑制を考慮した研究なども提案されている [13]．一般に認証の 3 要素のうち，知識認証と所持認証では経年変化が考慮されていないが，生体認証は人間の身体という経年変化があるものから認証情報を取得するため，考慮する必要がある．

実際には，知識認証や所持認証においても経年変化は起こり得る．知識認証では，例えば属性認証のように本人の住所を訪ねるような認証方式の場合，時間変化で引っ越しをした場合は属性が変化してしまう．同様に，所持認証においても，所持している IC カードの経年劣化などについては認証モデルとしては考慮されていない．

表 1 認証に関する用語と定義
Table 1 Terms and difinitions about authentication

用語	定義
認証情報	認証要求者が主張する利用者自身である事を立証するための情報
識別情報	認証システム内で利用者を一意に区別するための識別子
特徴情報	認証情報に変換処理を施して得られる特徴量
認証要求者	認証の対象となる当事者
利用者	認証システムを利用し，認証を行う当事者
検証者	利用者の認証情報を検証する当事者
経路	利用者が入力した認証情報を伝送する道筋
入力装置	認証情報を入力するための装置

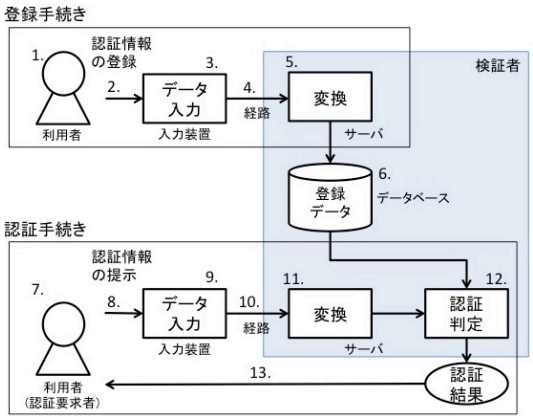

図 2 認証手続きの構成要素と手順のモデル
Fig. 2 Authentication Model

2.3 多要素認証

一般的な多要素認証の事例としては，PIN 認証と IC カードを利用した銀行 ATM が代表的なものである．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) の普及が進んでいる [14]．Google のリスクベース認証も多要素認証の一種と考える事ができ，アクセス元の IP アドレスなどでリスク判定を行った上で，追加認証としてパスワード認証などを行っている．

認証要素の組み合わせには多くのパターンがあるが，既存の研究やサービスは固定された組み合わせのみを検討しており，認証要素の柔軟な組み合わせは検討されていない．今後，多要素認証の普及が進む事で，求められるセキュリティレベルや利便性などサービスに応じた認証要素の組み合わせが必要となる．先行研究で，認証要素の切り替えにより安全性を担保する多要素認証システムの確率モデルの提案がなされているが [15]，提案モデルでは認証要素の独立性を仮定しており，各認証要素の性質まではモデル化されていない．今後，認証要素を確率的に扱うためにも，各認証要素の違いについて考慮し，統一的に扱えるモデルを検討する必要がある．本稿では，その前段階として各認証要素における時間的性質について検討を行った．

3. 用語の定義と認証のモデル

3 章では，本稿で用いる用語と認証のモデルについて説明する．本稿で用いる用語の定義と認証のモデルについては，先行研究で定義したものを元にした [16].

3.1 用語の定義

表 1 は，本稿で用いる用語の定義である．NIST の Electronic Authentication Guideline (NIST SP 800-63-2) [17]，及び，情報処理推進機構の「オンライン本人認証方式の実態調査報告書」[18]，日本国政府の「オンライン手続におけるリスク評価及び電子署名・認証ガイドライン」[19] などを参考とした．

「認証」とは，「認証要求者」が提示する「認証情報」と，事前に「登録」されている「利用者」の認証情報の同一性を検証する事により，認証要求者が主張する利用者である事の信用を確立する手順である．図 1 は，認証における「登録」と「認証」の手続きの概略を示している．本稿では，図 1 の登録手続きにおける本人確認手続きについては検討せず，正しく行われているものとする．

利用者は，事前に自身を識別可能な認証情報を登録し，認証システムのサービスを受ける．検証者は，サービス事業者などの認証を実施する主体であり，登録された認証情報を管理する．認証情報は，認証要求者が主張する利用者自身である事を立証するための情報である．認証情報には，他人と容易に識別できる容易識別性と，なりすましを防ぐための機密性の両方が求められる．更に，スマートフォンのロック解除のように頻繁に認証を行うシステムの場合，利用者にとって使い易い認証情報である事も重要である．他人が知り得ない秘匿された情報であれば，認証情報は必ずしも利用者を一意に識別可能な情報である必要はない．例えば，同一のパスワードを異なる利用者が用いていても認証を行う事は可能である．

また，本稿における認証情報には識別情報も含む．識別情報とは，認証システムが各利用者を一意に区別するために利用する ID であり，システムに指定された ID を利用する場合と，利用者自身が任意にシステム内で重複しない ID を決定する場合などがある．近年では，この識別情報としてメールアドレスを利用するシステムが増えている．これはメールアドレスの一意性を利用して，システム内で一意な識別情報として利用できるためである．1 対 1 認証の場合，識別情報とその識別情報と紐付けて登録されている利用者の認証情報を照合する事で認証を行う．1 対 n 認証の場合，識別情報は必要とせず，提示された認証情報に一定の閾値以上で適合する利用者がいれば，その利用者として認証を行う．

「特徴情報」とは，入力された認証情報から利用者を識

別可能な特徴的な情報を抽出したものである．図 2 の手順 5. と 11. に相当する処理の結果得られる情報が「特徴情報」である．例えば，指紋認証では指紋の凹凸情報を画像としてそのまま比較するのではなく，マニューシャと呼ばれる指紋の特徴点を取り出して比較している．本稿では，パスワード認証においてハッシュ関数で得られたパスワードのハッシュも特徴情報と考える．

利用者は入力装置を用いて認証情報を入力する．入力装置には，PC やスマートフォンなどの機器に加えて，各種センサや読み取り機が含まれる．本稿では，PC のマウス，キーボード，スマートフォンのタッチパネル，携帯電話のキーについては専用センサ，専用入力装置には含まない．専用の入力装置とは，IC カードリーダや生体認証の読み取り機，GPS センサなどを指す．

3.2 認証のモデル

本稿では認証のモデルとして図 2 の手順と構成要素を想定している．

図 2 における手順 2. と 8. の，1 回の認証試行に用いる認証情報を X とした時，特徴情報 F は特徴抽出関数 $Extract$ を用いて，

$$F = Extract(X)$$

と表せる．特徴情報 $F = \{f_1, f_2, \ldots, f_m\}$ は m 個の特徴量の集合である．また，入力される認証情報 X は $X = \{x_1, x_2, \ldots, x_n\}$ と表す．x 間の順序には意味があるものとする．例えば，あるパスワード認証システムにおいて，認証情報 X_1 として「P@ssw0rd」という文字列が入力された時，X_1 は表 2 のように表される．この時，各文字の時間的な入力間隔は考慮されていないが，入力順序は有意である．一方，加速度センサーを用いた歩容認証では，3 軸の加速度センサーを用いてミリ秒間隔で収集したデータを用い認証を行う．Gafurov らは 1 秒間に 16 サンプル収集し，一定距離を歩行した結果で認証を行っており [20]，この手法を例にとると，各 x 間のインターバルは 1/16 秒となる．行動認証は人間の動作や行動から個人性を求める手法であり，入力される認証情報に時間的な連続性がある．本稿では，入力順序を統一的に扱うために x_1 から x_n まで時間的な連続性があると考える．また，インターバルは次のように表す．

$$\Delta x = |t_{x_n} - t_{x_{n-1}}|$$

パスワードのように入力途中の時間を考慮しないが順序に意味がある場合は $\Delta x \to 0$ と考える．Δx の値は必ずしも一定ではなく，認証要素によっては区間によってばらつきがあるものもある．

図 2 における手順 12. の認証判定では，認証判定関数 $Match(F)$ により，登録済みの情報と比較され，本人かどうかの判定結果を返す．

表 2 認証情報のパスワード認証の例
Table 2 Authentication Information Example: Password Authentication

認証情報	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8
X_1	P	@	s	s	w	0	r	d

$$Result = Match(F)$$

$$Result = \begin{cases} Accept & \text{認証成功} \\ Reject & \text{認証失敗} \end{cases}$$

認証情報を更新する場合は，登録データの更新関数 $Update(F)$ により，入力された特徴量 F を用いて登録済みの認証情報を更新する．

3.3 本人拒否率と他人受入率

本稿で提案するモデルと本人拒否率と他人受入率の関係について整理する．

認証情報 X から特徴抽出関数 $Extract$ を用いて求められる F によって，本人拒否率 (FRR) と他人受入率 (FAR) が決まる．識別情報 u のある利用者の F_u が，過去の本人の特徴量 F'_u との類似度が高ければ本人拒否率は低くなる．利用者 u 以外 a が入力する X_a から求められた F_a が F_u と類似する他人が多い程，他人受入率は高くなる．一般に，X のエントロピーが小さい程，他人と類似しやすくなるため，X の情報量は多い方が良いと考えられる．

パスワード認証では入力する文字の種類を大文字，小文字，英数字や記号とする事で，英語小文字だけより，x 毎，すなわち一文字毎のエントロピーを大きくし，更に，入力するパスワードの文字数を増やす事で $X = \{x_1, x_2, \ldots, x_n\}$ の n を増やして認証に有効なエントロピーを得ている．

行動認証の場合，認証情報の X は，各 x の情報の粒度に依存する．例えば，歩容認証において X を 1 歩分の歩行時の 3 軸加速度センサーの情報とした場合，加速度センサーのサンプリング間隔が 1 ミリ秒間隔であれば，x_1 は足を動かし始めてから 1 ミリ秒間の XYZ 軸の加速度 3 値のみとなる．先行研究の活動量計を用いた行動認証では，市販の活動量計が用いられており，サンプリング間隔が 1 分間隔となっている [8]．1 分間の歩数やカロリーなどの活動量では，1 分間に何歩歩いたかの情報しか得られず，x_1 だけで本人性を見つける事は困難である．このように人間の行動といった連続性のある情報を認証情報として用いる場合，n には十分な長さが必要となる．

4. 考察

4 章では，既存の認証要素や様々なサービスを元に時間的特性について整理する．

表 3 は，我々が先行研究で各認証要素の特徴について評価したものを改訂したものである [16]．各種特徴と認証要素の関係性を安全性・利便性の観点で整理しており，「×」

はその特徴が安全性や利便性を低下する要因を示し，「○」は安全性や利便性に影響が無い，もしくは「×」と比較して影響が少ない事を示す．「△」は軽微な影響があるなど，限定的な事を示す．

4.1 認証情報のゆらぎとノイズ

認証情報のゆらぎとノイズについて考察する．本稿では，ゆらぎはノイズの一種と考える．認証要素には，表 3 の「入力のゆらぎ」で評価を行っているように入力時にノイズが加わるものがある．

虹彩認証を例とすると，図 2 における手順 2. と 8. の利用者の入力操作を要因とするノイズと，手順 3. と 9. の入力装置を要因とするノイズがある．利用者が入力する際の瞳の位置や角度による入力値のゆらぎや，太陽光などの外部環境による影響，画像処理性能の問題で発生する入力値のゆらぎがある．パスワード認証を例とすると，利用者自身の忘却により異なるパスワードを入力してしまったり，誤タイプにより異なる文字を入力するといったノイズが考えられる．

認証情報 X に含まれるノイズは，認証判定で本人拒否を起こす要因となる．ノイズに対しては，3 章で定義した特徴抽出関数 $Extract$ により，特徴量 F に変換する事で除去する事も期待されるが，逆にノイズが伝搬する事も考えられる．ノイズを nz と置き，ノイズが含まれない認証情報が X とすると，ノイズを含む認証情報 X' が入力された結果，特徴量は F' となる．

$$X' = X + nz$$

$$F' = Extract(X')$$

ノイズが含まれなかった場合の特徴量を F とした時，ノイズ nz の大きさに依らず $|F - F'|$ が小さければ，ノイズに対して頑健な $Extract$ と言える．

行動認証においては，認証情報の時間的な連続性に着目した特徴量が用いられる．例えば，活動量計を用いた行動認証では，1 分間隔で収集される活動量データの変化量を特徴量として用いており [8]，通常よりゆっくり歩いた場合は同じ歩行動作をしていても異なる人間として判定されてしまう可能性がある．既存の歩容認証の研究の多くは，障害物がない特定の場所や廊下などで歩行する事を前提としている．実社会での利用を考えると，直線を自然な速度で歩ける場所や長さは限られており，ノイズとなる情報が増えると想定される．このノイズに対しては，直線での歩行を行っている情報を多く取得するために認証情報 X の n を増やす，すなわち，長く歩行する事で有効な情報を取り出すという事が考えられる．

これは，表 3 における履歴長の議論にも関連する．認証情報の長さは，認証精度を向上させるという観点では長い方が良いが，一方で，認証システムの利便性を下げてしまうという問題もある．

4.2 認証情報の変化

認証情報の変化と時間の関係に関して考察する．3 章で定義した通り，「認証とは，認証要求者が提示する認証情報と，事前に登録されている利用者の認証情報の同一性を検証する事により，認証要求者が主張する利用者である事の信用を確立する手順」である．

4.2.1 なりすまし

パスワード認証のような従来の認証手法では認証情報が変化しない事を前提としていた．このような一意な認証情報を用いる認証手法は，認証情報が全く同じである事が仮定されているため，パスワードを盗み見られたような場合になりすましが問題となる．一方で，行動認証は行動の情報から本人の特徴を抽出するため，攻撃者が外部から観察していてもなりすましは容易ではない．例えば，署名認証の場合，記入し終わった文字を攻撃者が複写する事はできても，記入途中の筆の動きを再現する事は困難である．これは，時間的な連続性を認証情報に用いる行動認証の利点と言える．

4.2.2 テンプレート更新

行動認証や生体認証は認証情報が変化するため，認証情報を更新する必要がある．この時，認証情報の変化として変化には時間的な長短がある．

短期変動　時間単位や日単位での変化．前後の時間で急激な変化

中長期的変動　月単位や年単位での緩やかな変化

例えば，生体認証においては，加齢による長期的な経年変化と，怪我や病気による身体の変化や事故などによる身体の欠損による急激な変化がある．ただし，身体の欠損については，欠損の前後で時間的な連続性が失われるため，テンプレート更新を一度行うか，該当する認証要素を登録をし直す事で利用可能である．

行動認証は生体認証に比べ，ゆらぎが大きく，認証要素を利用者が意図的に変更する事もできる．人間の行動は時間と共に変化するため，生体認証以上に時間変化を考慮する必要がある．

例えば，行動認証において認証情報の変化が起こる顕著な例として，位置情報を用いた認証における「引っ越し」と「出張」という二つの状況がある．「引っ越し」の場合は，自宅の場所が変わるため，通勤経路が変わり，過去の

---

*1 専用の入力装置を必要とするかどうか
*2 利用者の操作や入力装置の性能，周辺環境の影響により認証精度が変わるかどうか
*3 認証情報を隠す事ができるか
*4 認証情報を変更できるかどうか
*5 同一または類似の認証情報を持つ他の利用者が存在するか
*6 経年変化と表記しているが，時間変化全般を指す
*7 一定期間の認証情報を必要とするかどうか

表 3 認証要素の特徴
Table 3 The other features of authentication factors

種別		入力装置		認証情報						社会的受容性
詳細		専用機材の有無 *1	入力のゆらぎ *2	秘匿不能性 *3	変更可能性 *4	類似性 *5	経年変化 *6	履歴長 *7	忘却紛失	プライバシー
知識	パスワード	○	○	○	○	○	○	○	×	○
	PIN	○	○	○	○	○	○	○	×	○
	パターンロック	○	○	○	○	○	○	○	×	○
	秘密の質問	○	○	○	○	○	○	○	×	△
	属性情報	○	○	○	△	○	△	○	△	○
	画像	○	○	○	○	○	○	○	×	○
生体	指紋	×	×	×	×	△	×	○	○	△
	網膜	×	×	△	×	△	×	○	○	△
	虹彩	×	×	△	×	△	×	○	○	△
	静脈	×	×	△	×	△	×	○	○	△
	顔	×	×	×	△	△	×	○	○	△
	声紋	×	×	△	×	△	×	△	○	△
	DNA	×	×	×	×	△	×	○	○	×
行動	歩容	×	×	△	△	○	×	△	○	○
	署名	×	×	×	△	△	×	△	○	○
	キーストローク	×	×	×	△	△	×	△	○	○
	ジェスチャー	×	×	×	△	△	×	△	○	○
	活動量	×	×	△	△	△	×	×	○	○
	位置情報	×	×	△	△	×	×	×	○	×
	行動履歴	○	×	△	△	△	×	×	○	△
	利用端末情報	○	○	×	○	×	△	×	○	○
所持	利用端末	×	○	△	○	△	○	○	×	○
	IC カード	×	○	○	○	○	△	○	×	○
	乱数表	×	○	○	○	○	○	○	×	○
	暗号鍵	×	○	○	○	○	○	○	×	○
	OTP	△	○	○	○	○	○	○	×	○
	SMS/Mail	×	○	○	○	○	○	○	×	○

位置情報の履歴と大きく異なってしまう．そのため，位置情報だけを用いた行動認証では，通勤通学先が特異な場所でない限り，他人として本人拒否される可能性が高い．この時，過去一週間の位置情報と比較して本人かどうかを判定する手法だった場合，引っ越し先で 4 日過ごし，過去の履歴情報が新しい住所が過半数を占めるまで，位置情報を用いた行動認証が利用できない．この時，テンプレート更新に相当する認証情報の更新または再度登録を行う事で，通常通り利用する事ができる．「出張」も数日間ホテルに滞在し，出張先の職場に通う事から「引っ越し」と同様に通勤経路が変わり，過去の位置情報の履歴と大きく異なってしまう．ただし，出張はあくまで数日間の移動のため，出張から戻った後は自宅から通う従来の通勤経路に戻る．この時，過去一週間の位置情報と比較する認証手法の場合，出張先では認証されず，一方で帰宅後は出張先の位置情報が履歴として用いられるため，帰宅後の認証も本人拒否率が高くなってしまうという問題がある．これは認証判定関数 $Match(F)$ が参照する過去の履歴情報をどのように利用するかに依存する問題ではあるが，常時テンプレート更新を行う認証システムでは考慮すべき問題である．

表 3 の「履歴長」の観点で，長い履歴を必要とする認証手法は，同様の問題点がある事を考慮する必要がある．

4.3 プライバシー

行動認証とプライバシーの関係について考察する．

行動認証は人間が普段，無意識に行っている行動から情報を抽出するため，情報を収集されているという不快感は低いと考えられる．一方，行動認証は，人間の行動の時系列の変化を特徴として用いるため，利用者の行動を追跡し続ける事で利用可能なシステムと言える．常時監視されているという印象を持つ事で，不快感を感じる利用者もいると考えられる．

特に，プライバシーに配慮する上で，考慮すべき認証要素としては位置情報がある．自宅や職場を知られる事は大きなプライバシー上の問題を抱える事となる．実際に Hayashi らが行った位置情報を用いた多要素認証の実験か

らは，被験者 36 名が一日に滞在する場所と時間の内訳として，平均で 38.9%が自宅，18.7%が学校職場となり，上位 2 カ所で 6 割近い時間を過ごしているという結果が得られている [2]．Wi-Fi のアクセスポイント情報を位置に相当する情報として用いた行動認証の手法も提案されている [21]．

このように人間の一日の行動が，位置情報の観点で 4 割が自宅，2 割が学校職場という特徴的な場所で過ごしているという事実は，連続した行動の情報を用いる行動認証では容易に本人の行動を追跡できるという事も表している．

5. おわりに

近年，普及が進む行動認証において従来の認証要素との違いとして，時間的な性質がある．本研究では，認証のモデルを定義し，行動認証と既存の認証要素との違いについて評価を行い，整理を行った．今回整理した行動認証の特徴を考慮する事で，適切な認証要素の選択を行う事ができる．今後の課題としては，時間的性質と安全性，利便性の関係性についても整理を行う必要がある．

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] 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 2014)*, pp. 187–198 (2014).

[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, p. 3 (2013).

[3] Google: 前回のアカウントアクティビティ，Google（オンライン），入手先 ⟨https://support.google.com/mail/answer/45938?hl=ja⟩（参照 2016-02-28）.

[4] Iwama, H., Okumura, M., Makihara, Y. and Yagi, Y.: The OU-ISIR gait database comprising the large population dataset and performance evaluation of gait recognition, *Information Forensics and Security, IEEE Transactions on*, Vol. 7, No. 5, pp. 1511–1521 (2012).

[5] Schimke, S., Vielhauer, C. and Dittmann, J.: Using adapted levenshtein distance for on-line signature authentication, *Pattern Recognition, 2004. ICPR 2004. Proceedings of the 17th International Conference on*, Vol. 2, IEEE, pp. 931–934 (2004).

[6] Bergadano, F., Gunetti, D. and Picardi, C.: User authentication through keystroke dynamics, *ACM Transactions on Information and System Security (TISSEC)*, Vol. 5, No. 4, pp. 367–397 (2002).

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

[8] Susuki, H. and Yamaguchi, R. S.: Cost-Effective Modeling for Authentication and Its Application to Activity Tracker, *Information Security Applications*, Springer, pp. 373–385 (2015).

[9] 板倉征男，外川政夫：ネット社会と本人認証–原理から応用まで–，電子情報通信学会 (2010).

[10] 瀬戸洋一：バイオメトリックセキュリティ認証技術の動向と展望，情報処理，Vol. 47, No. 6, pp. 571–576 (2005).

[11] Rattani, A., Marcialis, G. L. and Roli, F.: Biometric template update using the graph mincut algorithm: A case study in face verification, *Biometrics Symposium, 2008. BSYM'08*, IEEE, pp. 23–28 (2008).

[12] Uludag, U., Ross, A. and Jain, A.: Biometric template selection and update: a case study in fingerprints, *Pattern Recognition*, Vol. 37, No. 7, pp. 1533–1542 (2004).

[13] 松尾賢治，奥村文教，橋本真幸， 小池淳，久保田彰，羽鳥好律：腕の振りに基づく生体認証とテンプレート更新による経時変化の抑制，電子情報通信学会論文誌 B, Vol. 91, No. 6, pp. 695–705 (2008).

[14] RSA: RSA SecurID, RSA (online), available from ⟨https://www.rsa.com/ja-jp/products-services/identity-access-management/securid⟩ (accessed 2016-04-19).

[15] Susuki, H., Yamaguchi, R. S. and Sakamoto, S.: Multi-Factor Authentication Updating System Evaluation Dynamically for Service Continuity, *The 2nd International Conference on Information Systems Security and Privacy* (2016).

[16] 鈴木宏哉，山口利恵：個人認証における認証要素の特性と多要素認証への適用に関する考察，情報処理学会研究報告インターネットと運用技術 (IOT)， Vol. 2016, No. 13, pp. 1–8 (2016).

[17] Burr, W. E., Dodson, D. F., Newton, E. M., Perlner, R. A., Polk, W. T., Gupta, S. and Nabbus, E. A.: NIST Special Publication 800–63–2 Electronic Authentication Guideline, National Institute of Standards and Technology (online), available from ⟨http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf⟩ (accessed 2016-04-07).

[18] 情報処理推進機構：オンライン本人認証方式の実態調査報告書，情報処理推進機構（オンライン），入手先 ⟨https://www.ipa.go.jp/security/fy26/reports/ninsho/⟩（参照 2016-04-15）.

[19] 電子政府ガイドライン作成検討会：オンライン手続におけるリスク評価及び電子署名・認証ガイドライン，内閣高度情報通信ネットワーク社会推進戦略本部（オンライン），入手先 ⟨https://www.kantei.go.jp/jp/singi/it2/guide/⟩（参照 2016-04-12）.

[20] Gafurov, D., Helkala, K. and Søndrol, T.: Biometric gait authentication using accelerometer sensor, *Journal of computers*, Vol. 1, No. 7, pp. 51–59 (2006).

[21] Albayram, Y., Kentros, S., Jiang, R. and Bamis, A.: A method for improving mobile authentication using human spatio-temporal behavior, *Computers and Communications (ISCC), 2013 IEEE Symposium on*, IEEE, pp. 000305–000311 (2013).