認証精度の違う多要素・段階認証

山口 利恵 †　　鈴木 宏哉 †　　小林 良輔 †

東京大学大学院 情報理工学系研究科 ソーシャル ICT 研究センター
113-8656 東京都文京区本郷 7-3-1
yamaguchi.rie@i.u-tokyo.ac.jp, susuki.hiroya@sict.i.u-tokyo.ac.jp,
kobayashi.ryousuke@sict.i.u-tokyo.ac.jp

あらまし 現状，多要素認証というと，０と１を結果とするような要素を多段階に組み合わせたものが多い．一方，リスクベース認証と呼ばれるような行動を元にした認証要素も増えているところ，０か１の出力とならないような認証要素においても個人認証の手助けになる場合も考えられる．特に，IoT 社会といわれるなか，様々なセンサーデバイスが普及する中，行動に関する要素が社会に受け入れられる可能性は高い．このような認証の手助けとなるような要素についての認証における有効性について検討する．

Multi-Factor/Stage Authentication with Different Accuracy

Rie Shigetomi YAMAGUCHI†　　Hiroya SUSUKI†　　Ryosuke KOBAYASHI†

†Social ICT Research Center
Graduate School of Information Science and Technology
The University of Tokyo
7-3-1 Hongo, Bunkyo-ku, Tokyo 113–8656, JAPAN
yamaguchi.rie@i.u-tokyo.ac.jp, susuki.hiroya@sict.i.u-tokyo.ac.jp,
kobayashi.ryousuke@sict.i.u-tokyo.ac.jp[1ex]

Abstract The output of recent solution called multi-factor or multi-stage authentication is the logic of “AND” or “OR” to input combination of binary results such as 0 or 1. The output of risk-based authentication, which is one way of multi-factor authentication and has become more popular, is difficult to combine of binary results. The way is necessary to combine that the result is not binary results. Because most people have got smartphones, which have got a lot of kinds of Sensor device, that called IoT society, active authentication is possible to become more popular. We discuss about effectiveness of active authentication.

1　はじめに

インターネット上には，様々な種類のサービスが存在しており，その中でも本人を特定した上で行うようなサービス，例えば，ソーシャル･ネットワーキング･サービス（英: social networking service，SNS）や Web メールサービス等のようなサービスもいろいろと普及している．このようなサービスにおける認証の方式としては，ID とパスワードが一番利用がなされている．

この結果，様々な問題も起きている．この問題の解決のために，様々な認証手法が既に提案されてきているが，安全性だけでなく，コストや利便性が大きく横たわっている．しかし，このようなオンラインにおける個人認証の問題点は，セキュリティの研究に携わるものであれば，

特に目新しい問題ではなく，10 年以上の間，広く問題点として指摘されてきた．にもかかわらず，新たな方式は生まれてきておらず，逆に攻撃方法は日々進化する現状にあって，抜本的な解決には至っていない．

このような状況を解決する手段として，不正検知技術が発展してきている．この不正検知技術は，サービス全体において，「普段と違う動き」を発見し，不正者を追跡することによって，不正を検知しようとしている．これは，ユーザの行動履歴を核として本人を追跡しようとしていることにほかならない．このような手法は，ユーザが気がつかないなかで，認証を行っているため，ユーザの負担に対する抵抗感が少ない．

このようなユーザの「行動」も認証要素の一つとなり得る．このような要素は，本人データの揺らぎも大きく単体では認証要素とはなりえない．この問題を解決するためには，各要素の適切な組み合わせが必要である．同時に，ある特定の一つの手法が社会に席巻するのではなく，様々な認証手法をシステムの変化や社会情勢の変化に対応しながら，組み合わせができるような評価手法が必要といえる．

本稿では，「行動」という認証要素の可能性とともに，その要素を活かすための多要素認証の必要性について述べる．

1.1 構成

本論文は下記のように構成する．2 章において認証の現状とその問題点を指摘する．2 章で述べた問題点を解決する一つの手段として，「行動認証」という概念について，3 章で述べる．この「行動認証」という概念は，従来の個人認証においていわれてきたほどの認証精度がないため，統一した認証の安全性評価と組み合わせ手法が必要ということについて，4 章で述べ，5 章においてそれでも解決しづらい現状について議論する．6 章においてまとめる．

2 現状の認証

この章では，現状利用されている個人認証という技術について説明する．

2.1 認証とは

「認証」という言葉は，意味が広い．時には，複数の属性情報を組み合わせてある特定の人物を探し出す「識別」をすることで認証をした，と示すこともある．

ここでは，認証は，登録をおこなった人物とあるトランザクションを依頼してきた人物が同一人物であるかどうかを確認する行為とする．登録時に既に別人になりすまして依頼を行ってきた場合には，それを見つけることはできない．登録時に，相手に本人であるかやサービスを受ける資格があるかどうかについては，別の手段で確認されるべきことで，ここでの論点とはしない．

2.2 認証の 3 要素

オンラインにおける個人認証は，3 要素として，それぞれ，表 1 であげられているとおり，利点と欠点があるといわれている．

セキュリティの観点から上記の要素を組み合わせることも推奨されている．しかし，ここで提案されている技術が広く社会に受け入れられていない現状もまたある．

2.3 知識に頼る現状とその問題点

2.2 節で述べたような様々な技術が提案され，実用化され，また，10 年以上にわたり，その問題点が多々指摘されているにもかかわらず，ほとんどのサイトで ID とパスワードを利用している．その理由について考察する．

2.3.1 ID とパスワードだけに頼る現状

シマンテックの調査 [1] によると，企業 Web サイトの管理者に向け「現在，御社サイトでどのような認証を実施していますか？」という問

表 1: 認証の 3 要素における比較

	具体例	長所	短所
知識 知っていること	・PIN ・パスワード	・コストがかからない	・忘却・盗難 ・推測
所持 持っていること	・ハードウェア （IC カード，乱数表） ・ソフトウェア	・忘却しない ・セキュリティ強度が向上	・所持品の配布 ・所持品を読み取る等の装置が必要 ・盗難・紛失
身体的特徴 ユーザ本人の特徴	・バイオメトリクス	・忘却や紛失の心配が無い	・心理的な抵抗 （プライバシー） ・読み取る装置が必要 ・改変が困難

いに対し，77 %のサイトが ID とパスワードを活用していると答えている．この結果は，複数回答であったため，ID とパスワードだけが利用されている，とはまでは言えないが，次に使われている認証のワンタイムパスワードが 24.7 %という現状から考えると，ID とパスワードだけを活用しているサイトが非常に多いということができる．また，同じ調査において，ネットユーザに対し,「決済サービスのパスワードはそれぞれ別々に設定していますか？」という問いに対し，1 種類と答えた人が全体の 15 %，2 ー 3 種類と答えた人が全体の 47 %であった．つまり，62 %の人は 1 - 3 種類の ID とパスワードしか利用していないという現状がある．この結果，パスワードリスト攻撃という問題など，様々なセキュリティ問題を引き起こしている [3].

2.3.2 問題があったとしても利用されてしまう現実

こういった問題を解決するため，ID とパスワードだけでなく，複数回の ID とパスワードの入力を求めることや，SMS（携帯電話のショートメッセージサービス）を活用したようなワンタイムパスワードといった追加の認証を加えたような仕組みも存在する．同様に乱数表等の活用も提案されている．このような仕組みは，2 段階認証とも呼ばれており，一部のサービスにおいて実際に利用されているものの，広い分野での普及は進んでいない．

また，IPA の調査によると，新たな認証手段を利用しない理由として，コストに対する意識に加え，他の手段は利用率の低下に繋がるという懸念があるということである．この懸念は，2013 年のインターネットコムの調査によっても指摘されている．2 段階認証をしているサービスを離脱した人の理由として,「2 段階認証が面倒（手間）だったから」という理由を選んだ人が 82 %に上っている．つまり，2 段階認証を活用したシステムはユーザにとって利用が煩雑となることを理由として活用がされていないのである [4].

このような現状から，サービス事業者はユーザへの負担を考え新たな方式にはうつりにくい.

3 行動認証とは

2 章で述べたような現状を打破するためにはどのようにしたらよいのであろうか.

3.1 ユーザの求めている認証と現状

2.3.2 節で述べたとおり，サービス事業者は，二段階認証や他の手法への導入に対して，コスト以上にユーザの負担があるため利用しない，という声が大きい．iPhone での生体認証，不正検知やリスクベース認証などの普及から考えると，ユーザが明示的な動きをすることなく，

認証の要素として利用できるような手法がより多く今後導入されると考えられる．

特に，IoT 社会と言われ社会にセンサーが多々導入される昨今，ユーザの明示的な動きなくユーザの周辺にある情報，つまりデータが簡単に取得できるようになってきた．また，ビッグデータ解析時代と呼ばれるように，機械学習を中心とした様々な手法が提案されておきており，より簡単にデータ解析が行うことができるようになってきた．このような状況を鑑み，データ解析を中心とした検討ができるようになってきている．

3.2 現状の多様な行動認証

行動に関する認証は，新しいものではなく，既に一部で導入されている．ここでは，リスクベース認証，生体認証の一部について述べる．

3.2.1 リスクベース認証

リスクベース認証は，不正検知という観点から進んできた認証である．

不正検知においては，全体の履歴データを解析し，通常とは違う履歴データが生じた場合には，不正者であると判断している．従来は，そのシステム全体の履歴データからいつもとの違いを発見し，不正者を追跡してきた．このような技術が応用され，各個人ごとについても従来の動きと違うようなことが起きた場合には，本人以外では，と，判断し，不正者として検出している．例えば，既に銀行やネットサービスで利用されているリスクベース認証は，普段，東京の IP からサーバへアクセスしている人が大阪の IP からサーバへアクセスした際に，不正者の可能性があるとして検出している．これらの手法は，既に実用化されており，IP の位置情報以外のどのような要素を活用しているかについては，各社が公開していないため予想であるが，端末やブラウザの情報を利用しているようである．

また，検出後，追加の認証を求めていることが多い．

3.2.2 生体認証と評されてきた行動に関する認証

従来，生体認証とされてきた認証手法の一部も行動に関する認証であるといえる．例えば，署名の仕方を利用してるような手書き文字に関する認証や，歩容認証の一部も行動認証といえる．

3.3 今後増えていくであろう認証要素

既に様々な手法があるが，今後，下記のような手法も活用されていくであろう．

3.3.1 IoT 社会と多様性

PC だけでなくスマートフォン，タブレット等の同一ユーザの複数端末の活用や，ウェラブル端末等，ユーザは一つの端末で認証を行うという社会ではなくなっている．スマートグリッド，スマートシティの普及に伴い．今後ユーザは身の回りに 100 個以上のデバイスを持つであろうといわれている．このようなデバイスで取得したデータは，常に認証に利用できる．

ユーザは身の回りに様々なデバイスを利用して取得したセンサーデータを活用した認証が可能となる．たとえば，既にある利用端末情報や生体情報だけでなく，過去の買い物履歴やスマートフォンの持つセンサー情報もその要素の一つとなるであろう．

3.3.2 スマートフォンの持つセンサー要素を用いた認証

スマートフォンには，様々なセンサーがついており，それらのセンサーを利用し，認証を行うことを提案されている．位置情報 [6]，Wifi[7]，運動履歴 [8] など，色々なケースが考えられる．

3.4 行動認証の性質と問題点

既に実用化されているリスクベース認証をとってみても，IP 等の行動に関する認証だけでは，認証精度は低い．認証精度を上げるため，追加の認証を要求している．このように，行動

に関する認証要素は，その要素単体での利用は難しい．

3.4.1 既存インフラの活用

3.3.1 節で述べたような現状から考えるに，行動認証は，認証用の新たなハードウェアやインフラを用意するのではなく，既にあるようなデバイスや方式を活用することで認証が可能となるケースが増えるだろう．

スマートフォンが既に持つようなセンサーを活用して認証を行うことで，ユーザに対して新たなデバイス等の利用方法を説明しなかったとしても，利用を可能とできる．

3.4.2 行動認証の性質と問題点

行動によって得られた情報を認証に活用するために，性質を整理する．

- データの収集間隔がそれぞれ違う：従来の認証手法のように，認証を要求する時間だけの情報で認証をするとは限らない．位置情報や運動履歴のように，認証時点だけでなく，丸一日の情報を活用して認証を利用しているとは限らない．
- 認証精度がかわる：行動は，人間が行うものであるため，揺らぎが生じる．

このように，既存デバイスやインフラを活用することで，ユーザの明示的な動作等がなかったとしても，サービス事業者が設定することによって，負担なく利用が可能となる．一方，それぞれの認証精度が違うという問題がある．

認証要素が増えるに従い，行動履歴情報を活用した認証は普及するであろうと思われる．しかしながら，それぞれの要素は，認証精度がまちまちであり，また，ユーザも統一的な動きをしているわけではないので，データそのものも「揺らぎ」のようなことが起こるであろうと考えられる．この揺らぎを解消する方法が必要である．

4 多段階・多要素認証

ここまで述べてきた揺らぎ等を解決するためには，認証結果として,「尤もらしさ」や「点数付け」を返す緩やかな認証が必要となる [5]．ここでは，このような手法の現状と必要な要件について述べる．

4.1 現状の多段階認証

多段階認証は，従来の認証よりも安全であると一般的に考えられているため，様々な場での利用が進んでいる．

4.1.1 ハードウェアの利用

単純な ID とパスワードだけでなく，SMS（携帯電話のショートメッセージサービス）を活用したようなワンタイムパスワードの利用や暗号を利用し専用ソフトウェアやハードウェアを活用した仕組みが存在する．このような仕組みは，２段階認証と呼ばれており，一部のサービスにおいて実際に利用されているが，コストやユーザへの説明の困難さなどを理由として，抜本的な解決となっているかというとそうではない．

4.1.2 生体認証との組み合わせ

生体情報のセキュリティ強度が安定していないとされる中，FIDO や ApplePay のようなスマートフォンなどに生体センサーが埋め込まれ決済などに利用されるようなケースが増えてきた．こういった特殊なセンサーを利用した認証は，従来，一社の独自開発でそれぞれの会社のサービスにおいて活用されていることが多かった．しかし，最近では，同じ枠組みで数社にわたって利用されるサービスがうまれつつあり，特に決済の分野においては，広く利用されることが多くなった．

この理由として，生体情報を手元の端末やカードにおいて管理することで，よりプライバシーへの抵抗感を減らし利用されつつある．このような，ユーザが手元にもつ端末に対して，起動（アクチベード）には，生体情報のような

より本人を特定しやすいような情報を提示し，端末内に持つカギ情報や端末情報と暗号技術を組み合わせてサービスへの権利を提示するようなことが増えて行くであろう．

4.1.3　リスクベース認証

3.2.1 節でのべたとおり，リスクベースも一つの要素でやっているわけではなく，複数の要素を組み合わせている．一つの要素だけでは，本人を認証できないため，色々なケースを組み合わせている．

4.2　多段階認証の問題点

多要素・段階認証は，安全性が上がったのであろうか．現状では，安全性が向上に関する評価について，既にある機械学習の手法を適用可能な可能性もあるが，数学的になされているかというとそうともいえない．

現状では，経験的・定性的に，安全であるとしている．つまり，少なくとも ID とパスワードとの組み合わせよりも安全と感じる，ということで普及がなされている．

4.2.1　0，1 の組み合わせ

前章で紹介した技術は，二段階や多要素であっても，「○」か「×」，つまり，0 と 1 の組み合わせであった．たとえば，例えば，生体認証の利用をしたとしても，要素それぞれの閾値が設定され，その閾値を突破したかどうかで認証を決めてきた．

4.2.2　環境変化への対応と認証バラエティ

また，安全性や周辺環境は，常に変化し続けるものであり，導入当時の設定がいつまでも適切とは限らない．

パスワードリスト攻撃や，指紋認証におけるグミ指の発見など，セキュリティに関する状況は，常に変化し続ける．同じようなセキュリティ基準での対応では対応しきれない．

また，同じサービスだとしても，同じセキュリティ基準が適切とは限らない．お茶とダイヤモンドの購入が同じセキュリティ要素によって判断されることは，ダイヤモンドと同じ基準をお茶には過剰すぎることとなり，サービス内の認証閾値の多様性も求められている．

同時に，数年前にスマートフォンの普及が予想できなかったように，ユーザ端末も変化する者であり，端末の多様性に対応する必要性がある．

多様な認証要素に対してどのような統一的な認証要素が必要なのだろうか．

4.3　複数の認証要素における統一評価の必要性

安全性を確立するためには，各要素の認証精度を統一した尺度で評価しなければ，安全性があがらない．つまり，各要素を統一で評価する必要性がある．

4.3.1　多要素・多段階の要件

行動が，はやればはやるほどゆるやかな認証要素が増えていくので，一つの要素では認証ができない．また，導入同時は安全だったとしても，セキュリティホールの発見などにより，突然精度が下がる必要性がある．

そこで，下記の要件を吸収した方式の提案が必要である．

- 要素ごとの精度の吸収 (常に，0，1 とは限らない)
- 要素の柔軟な入れ替えを可能 (特定一つの要素によるセキュリティホールの排除)
- サービスに応じた強度の変化
- 個人ごとの要素選択の自由
- 使い勝手の良い認証要素の発見
- 既存インフラの活用

4.4 組み合わせ評価手法

それぞれの要素ごとの統一された尺度をもった精度をもとに，次に，全体のセキュリティ強度の評価手法が必要である．ここに関しても，機械学習等で既に提案されている精度の評価手法を適用可能であろう．

5 議論

ここでは，図 1 で表したような状況になった場合に，現状の分析と行動認証が導入された後の問題点について述べる．

5.1 ID とパスワードに代わるような手法が必要なのか

2 章で述べたとおり，ID とパスワードが広く使われているが，それを利用しない手法も多々提案されている．しかし，ある特定の一つの技術が社会に普及していない．リスクベース認証の普及という状況を鑑みるに，不正検知やリスクベースといったユーザの明示的な動きを利用しないような認証の手助けとなる技術が普及しつつある．

つまり，ID とパスワードにとって変わるような手法の提案が社会として求められるのではなく，ID とパスワードを共存して利用していく手法を考えなければならないのであろう．

5.2 行動認証とプライバシー

行動認証が流行れば流行るほど，ユーザが意識せずに認証が終わることが増えていく．つまり，ユーザの動きによって，ユーザが気づくことなく認証が終わるようになるので，ユーザは自分が気づかないままに履歴を集められることがある．また，ユーザが気づかないままに属性の変更等が容易となるようなことも考えられる．

サービス事業者にとってのメリットは大きいが，ユーザにとってのプライバシーについては別途の検討が必要である．こういった認証を利用するためには，事前によく説明をしておく方法について検討しなければならない．

特に，ユーザの同意の取り方については，事前によく検討しなければならない．

6 まとめと今後の課題

従来，ID とパスワードにかわるような何か画期的な認証手法を探求してきた．今後は，認証の瞬間は一瞬だとしても，長い時間のデータを活用して認証を行う手法が主流となるだろう．つまり，生活そのもので本人性を出すことで認証として成り立たせることとなる．また，従来の 1 箇所の高い壁をつくることでセキュリティを担保してきたような仕組みから，攻撃者にとって小さい壁をたくさんつくることで，一つ一つの壁は低いとしても全体としてセキュリティを担保するような枠組みがより多く利用されるに違いない．

一方で，行動認証のような本人の明示的な動きなく認証するような仕組みは，技術的に可能となる時が近いとしても，ユーザの意図しないような動きをする可能性もあることから，プライバシー等，技術以外での乗り越えるべき項目は多々存在する．この項目の解決のために十分な議論が必須である．

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] シマンテック「個人・企業のパスワード管理」に関する意識調査：https://www.jp.websecurity.symantec.com/welcome/pdf/password_mafnagement_survey.pdf（2015 年 5 月 1 日閲覧）

[2] IPA「オンライン本人認証方式の実態調査」：https://www.ipa.go.jp/security/fy26/reports/ninsho/（2015 年 8 月 24 日閲覧）

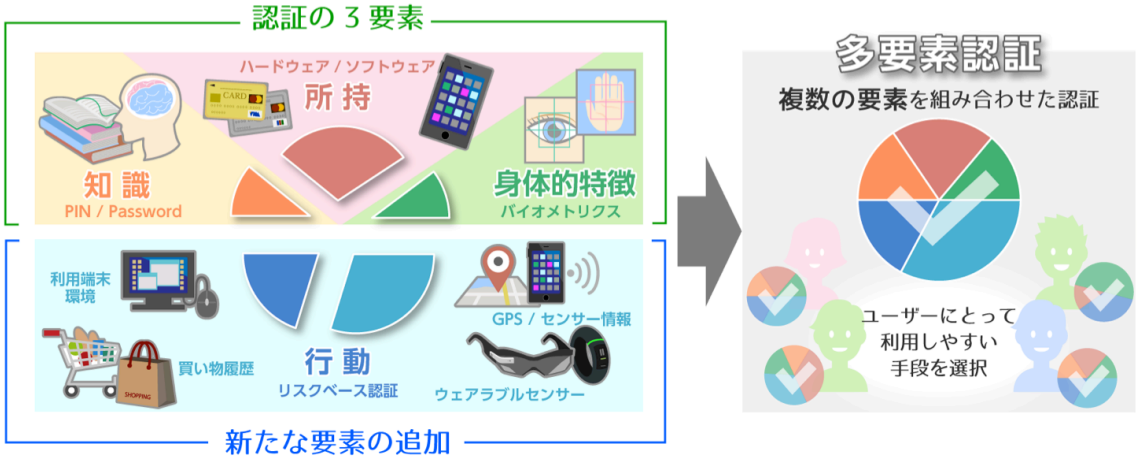

図 1: 行動認証と多要素認証

[3] IPA「プレス発表　パスワードリスト攻撃による不正ログイン防止に向けた呼びかけ」: https://www.ipa.go.jp/about/press/20140917.html（2015 年 8 月 24 日閲覧）

[4] インターネットコム「「二段階認証」 に関する調査」: 2013

[5] 山口利恵, 鈴木宏哉, 坂本静生　「スマートフォンを事例とする多要素認証確率の提案」: SCIS2015 暗号と情報セキュリティシンポジウム, 4C2-5, 2015.

[6] 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」: CSS2015 コンピュータとセキュリティシンポジウム, 2015.

[7] 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」: DICOMO2015，マルチメディア、分散、協調とモバイルシンポジウム，2015.

[8] 鈴木宏哉，山口利恵「ウェ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.