Vol.2021-SPT-41 No.17
2021/3/1

ウェアラブル端末を用いた覗き見耐性を持つジェスチャー認証手法の提案と評価

嘉藤 鴻介* 渡辺 一樹* 油田 健太郎†
岡崎 直宣† 朴 美娘*

あらまし 近年，スマートフォンやタブレットなどの携帯端末が普及しており，その中に個人情報が多く含まれている．現在それにアクセスするために PIN，パターンロックや指紋認証などの個人認証が用いられているが，それらは覗き見攻撃や盗難によって個人情報が漏洩する可能性がある．そこで本研究では，ユーザが常時身に付けており，盗難の可能性が低いスマートウォッチ上でスマートフォンの認証を行うことができる認証方式の提案を目指す．それにあたって，ユーザ画面をタッチすることなく認証を行えるジェスチャーを用いた方式に着目した．現在まで，画面に表示されている特徴的なジェスチャーアイコンが 9 種類のみなので，覗き見耐性の評価実験を行った際に，ジェスチャーとそれに対応する画面上のアイコンを攻撃者が偶然発見し，登録位置が漏洩してしまうという課題があった．そこで本論文では，ジェスチャー認証方式の覗き見耐性を向上するために，認証登録時にダミー番号を追加し，認証時に表示されたアイコンとは異なるジェスチャーを行って認証する方式を提案する．実験として，ユーザビリティを確認する実験を行った結果，平均認証時間が 10.9 秒，認証成功率は 73.3%となり，長期的な慣れの実験を行ったところ，平均認証時間が 8.8 秒まで減少し，認証成功率が 93%まで向上した．またダミー番号を 2 つ以上追加した覗き見実験によって，全ての認証情報は漏洩しない結果となった．

キーワード：個人認証，スマートウォッチ，ジェスチャー

Proposal and Evaluation of Gesture Authentication Method with -Peep Resistance- Smart watches

Kousuke Kato* Kazuki Watanabe* Kentaro Aburada†
Naonobu Okazaki† Mirang Park*

Abstract: In recent years, mobile terminals such as smartphones and tablets have become widespread, and many personal information is contained in them. Currently, personal authentication such as PIN, pattern lock and fingerprint authentication is used to access it, but personal information may be leaked by peeping attacks and theft. Therefore, in this research, we aim to propose an authentication method that users can always wear and authenticate smartphones on smart watches that are less likely to be stolen. In doing so, we focused on a method that uses gestures that allow authentication without touching the user screen. Until now, since there are only nine types of characteristic gesture icons displayed on the screen, we conducted an evaluation experiment of attacker accidentally discovered the gesture and the corresponding icon on the screen, and the registered position was leaked. Therefore, in this paper, in order to improve the peep resistance of the gesture authentication method, we propose a method of authenticating by adding a dummy number at the time of authentication registration and performing a gesture different from the icon displayed at the time of authentication. As an experiment, as a result of conducting an experiment to confirm usability, the average authentication time was 10.9 seconds and the authentication success rate was 73.3%. After a long-term familiarity experiment, the average authentication time decreased to 8.8 seconds. The authentication success rate improved to 93%. In addition, a peep experiment in which two or more dummy numbers were added resulted in no leakage of all authentication information.

Keywords: Personal Authentication, Smart watches, Gesture

1. はじめに

近年，スマートフォンやタブレットなどの携帯端末が普及しており，それらの機器にはユーザのスケジュールやメールなどの個人情報が含まれ，アクセスするためには個人認証が用いられている．例えば，PIN コードやパターンロック，指紋認証や顔認証などの生体認証が用いられているが，PIN コードやパターンロックは画面のタッチによって認証情報が直接入力されるため，第三者の覗き見攻撃と盗難によって個人情報が漏洩する可能性がある．また生体認証であれば，指紋の再現や顔をマスクで再現し，認証を突破できることが報告されている[1].

一方で，それらの携帯端末と連携するウェアラブル端末が多く登場してきており，携帯端末との連携が進んでいる．その数は年々増加してきており，2022 年までに世界で 4 億 5300 万台まで増加すると予測されている[2]．スマートウォッチもスマートフォンと同様に個人情報が多く含まれているため，それにアクセスするために個人認証が用いられており，スマートフォンと同様に覗き見攻撃に脆弱な PIN やパターンロックが用いられている．

* 神奈川工科大学, Kanagawa Institute of Technology
† 宮崎大学, University of Miyazaki

以上，スマートフォンとスマートウォッチそれぞれのデバイスにアクセスするために各デバイス上で個人認証を行うことはユーザにとって負担がかかり，覗き見攻撃にも脆弱であることが考えられる．よって，ペアリングが完了した一つのデバイスで個人認証が行うことができる，一元的な認証方法が必要である．

現在では，スマートフォンのロックを解除した際に自動的にスマートウォッチのロックが解除される機能[3]や，スマートフォンがスマートウォッチの Bluetooth の範囲内に存在することで，自動的にスマートフォンのロックが解除される機能[4]が存在する．しかし，スマートフォンに対する覗き見攻撃や盗難によって個人情報が漏洩する可能性ある．

そこで本研究では，盗難による個人情報の漏洩の可能性が携帯端末より低いスマートウォッチ上で，スマートフォンの個人認証を行うことができる認証方式の提案を目的とする．それによって携帯端末の個人情報の漏洩を防ぐことができると考えられる．

これまで，携帯端末における個人認証方式が研究されている [5, 6, 7]．しかし，そのほとんどがタッチスクリーンを用いた手法であり，それらをスマートウォッチでの個人認証へと応用すると，スマートウォッチの小型スクリーン上でボタンやアイコンなどのタッチが難しくなり，ユーザビリティが低下してしまうことが考えられる．

近年では，スマートウォッチ向けの認証方式も研究されている [8, 9, 10]．しかし，覗き見攻撃の耐性がないことや，小型スクリーンのタッチの困難さを考慮した覗き見耐性の向上を行っていることが原因で認証時間が長くなり，ユーザビリティが低下する問題がある．

そこで，我々はジェスチャーを用いた認証方式に着目した．スマートウォッチでジェスチャーを行うことで画面をタッチすることなく認証ができ，覗き見耐性を向上させる際に画面の大きさを考慮する必要がないため，ユーザビリティの低下を防ぐことができる．

ジェスチャーを用いた認証方式として，携帯端末でジェスチャーを行う方式 [11] やスマートフォンを取り出す動作による方式が提案されている [12]．しかし，他人受け入れ率と覗き見耐性のバランスに問題があったり，圧力センサなどの多くのスマートウォッチに搭載されていない機器を用いたりする必要がある．また，スマートウォッチを身に付けている手でスマートフォンを持ち，その手で持ち上げる動作をすることでスマートフォンのロック解除を行う手法やその手首を捻るジェスチャーを行うことでスマートフォンの解除を行う認証手法が提案されている [13, 14]．しかし，スマートウォッチを身につける腕と携帯端末を持つ手を同じにする必要があることや，タブレットなどの大きな携帯端末を持った状態でのジェスチャーはユーザに負担がかかる．さらに，ユーザが登録場所上のジェスチャーアイコンと同じジェスチャーを行う認証方式 [15]が提案されている．ジェスチャーを認証に用いることにより，画面をタッチすることなく認証可能なため利便性が向上し，ジェスチャーアイコンを毎回ランダムに表示させることで，覗き見耐性があると考えられている．しかし，覗き見耐性の評価実験により，覗き見耐性を十分に持つとは言えない問題がある．

そこで本論文では，ジェスチャー認証方式[15]の覗き見耐性を向上するために，認証登録時にダミー番号を追加し，表示されたアイコンとは異なるジェスチャーを用いた認証方式を提案する．認証中にダミージェスチャーを行うことで，覗き見耐性が向上すると考えられる．

以降，2 章で関連研究の紹介を行い，3 章で覗き見耐性を持つジェスチャーを用いた提案方式について述べる．また，4 章でユーザビリティと覗き見耐性の確認実験を行い，最後に 5 章でまとめとする．

2. 関連研究

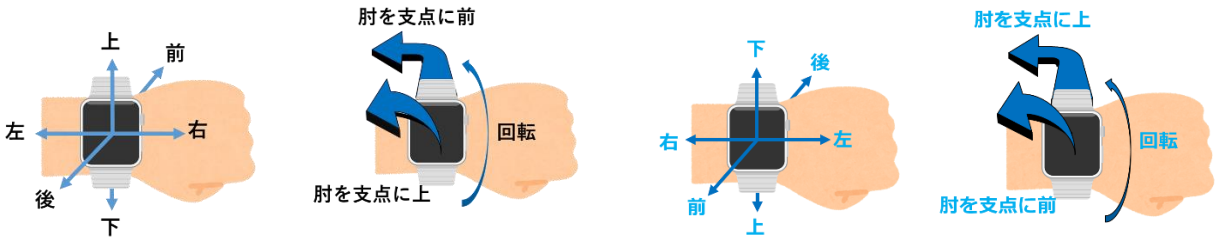
2.1 スマートフォン向けの認証方式

これまで，スマートフォンやタブレットなどの携帯端末向けの認証方式として，画面に表示された 4×4 のアイコン上の，登録アイコンと異なるアイコンをタッチすることで認証を行う方式[5]や，金庫のダイヤルをモチーフにし，PIN を入力するためにインディケータを振動機能でユーザに知らせる方式[6]，認証ごとにパターンロックが変化する方式[7]などが提案されている．

上記の方式は，携帯端末のタッチスクリーンをタッチすることで認証を行っている．そのため，それらをスマートウォッチへ応用すれば，小型スクリーン上のタッチの困難性からユーザビリティが低下する問題がある．また，覗き見耐性を向上させるために認証時間が長くなるなど，ユーザへの負担が増加している．

2.2 スマートウォッチ向けの認証方式

スマートウォッチにおける個人認証方式として，小型スクリーン上のタッチの困難性を解消した方式[8]が提案されている．この方式では，4 つのボタン中の 1 つのボタンをタッチまたは 2 つのボタンを同時にタッチすることによって PIN と同様に一桁で 10 通りの組み合わせを実現している．専用の GUI なしでも利用可能なため，画面が非表示状態でも使用出来る点が特徴的な方式なのだが，覗き攻撃に脆弱である点は PIN と同様である．



(a) 通常時　　(b) ダミー番号登録時

図 1: 提案方式におけるジェスチャーの種類

そこで以前我々は，ボタンのタッチのしやすさを考慮しつつ，覗き見耐性の向上を目的とした認証方式として，3×3 のアイコンを画面に表示し，登録アイコンとは異なるアイコンをシフトルールと呼ばれる規則に基づいてタッチする方式を提案した[9]．結果として覗き見耐性は向上したが，認証時間が長くなり，ユーザビリティの課題が考えられる．

一方で，タッチスクリーンを用いずにスマートウォッチの側面にあるつまみ(竜頭)の回転によって PIN を入力する方式も提案されている[10]．ここでは，PIN と比べ覗き見耐性が格段に向上しているが，前述した方式と同様に認証時間が長くなる課題がある．

2.3 ジェスチャーを用いた認証方式

これまで，携帯端末向けのジェスチャーを用いた認証方式が提案されている[11, 12]．文献[11]では，携帯端末で一筆書きまたは単一動作を行うことで認証される方式を提案している．ここでは，個人を判別するために加速度センサと角速度センサを用いている．しかし，一筆書きの場合，覗き見耐性と他人受け入れ率(FAR：False Acceptance Rate)の両方が高くなり，単一動作であれば FAR と覗き見耐性の両方が低下する．

また，携帯端末を取り出す動作で認証を行う方式[12]では，加速度センサと圧力センサから取得できるデータから個人を判定している．しかし，スマートウォッチ上で認証を行うことを考慮すると，現在普及している多くのスマートウォッチには圧力センサが搭載されていないため，実現が困難である．

そこで，スマートウォッチとスマートフォンの両方で同時にジェスチャーを行い，個人の判定を行う認証方式が提案されている[13,14]. Shrirang らはスマートウォッチを身につけた腕にスマートフォンを持ち，持ち上げる動作をすることで認証を行う方式している[13]．認証方法としては，2 つの端末の加速度データと角速度データを取得し，それらを個人の判定に用いている．各被験者に対して認証を行った実験では，FAR と FRR(False Rejection Rate)が 1.7%と約 1.0%となっており，覗き見の実験では FAR が 2.9%という結果になっている．

しかし，上記 2 つの方式の問題点として，スマートウォッチとスマートフォンのジェスチャーを行う腕と手を同一にする必要がある点が挙げられる．また，タブレットなどのスマートフォンより大きい携帯端末で上記 2 つの認証方式を使用する際，それを持ちジェスチャーを行うこともユーザに負担がかかると考えられる．

前述した認証方式[13,14]の問題を解消するために，スマートウォッチの画面上に 3×3 のアイコンがランダムに表示され，ユーザが登録位置上のアイコンが示すジェスチャーを行うことで位置を指定する認証方式[15]が提案されている．スマートウォッチのジェスチャーのみで認証を行うことで，画面をタッチする操作がなく利便性が向上し，ジェスチャーアイコンを毎回ランダムに表示させることで，覗き見耐性があると考えられていたが，覗き見耐性の評価実験により，覗き見耐性を十分に持つとは言えないことが課題として挙げられている．

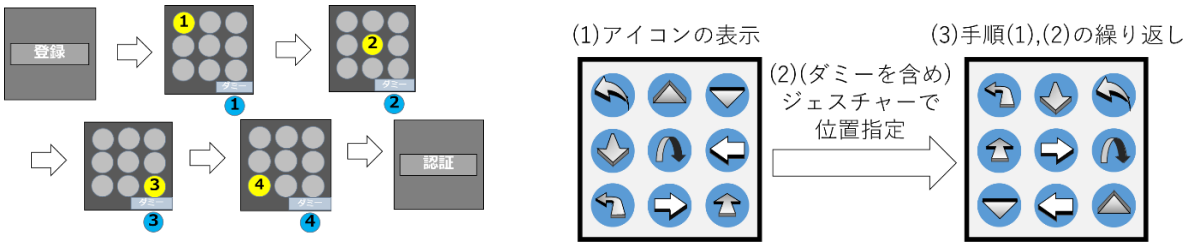
3. 提案方式

本研究では，2.3 節で述べたジェスチャーを用いた認証方式[15]での覗き見耐性を向上するため，この方式を改良する認証方式を提案する．具体的には，認証登録時にダミーを追加し，認証時に表示されたアイコンとは異なるジェスチャーを行って認証する方式である．

この方式では，携帯端末を操作せずにスマートウォッチの操作のみで認証を行うことができ，認証ごとにジェスチャーの種類が変化するため，覗き見攻撃に対する耐性を持つと考えられる．

3.1 基本コンセプト

ここでは，ジェスチャーを用いた認証方式[15]と同様に，認証時にスマートウォッチの加速度データと角速度データからジェスチャーの判定を行うことで認証情報を入力する．ジェスチャーは図 1 (a)のように動かし，以下の 9 種類を採用している．



(a) 登録手順　　(b) 認証手順

図 2: 提案方式の登録・認証手順

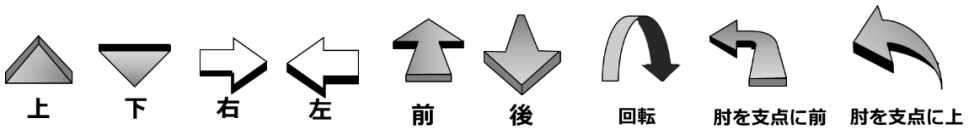


図 3: ジェスチャーとアイコンの対応

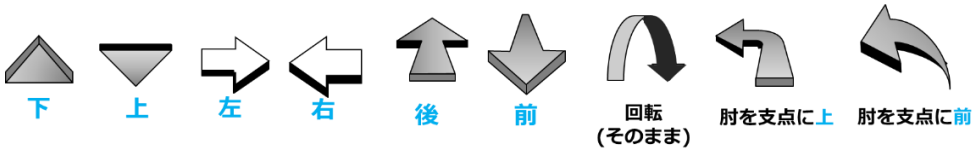


図 4: ジェスチャーとアイコンの対応(ダミー番号登録時

- 上, 下, 右, 左, 前, 後
- 回転, 肘を支点に前, 肘を支点に上

またダミーが登録された場合には, 図 1 (b)の様にジェスチャーとアイコンの対応が上下左右前後, または肘を支点に前・上が異なるジェスチャーになる. ただし, ジェスチャーとアイコンの都合上, 「回転」のジェスチャーとアイコンは通常通りの仕様となる.

これらのジェスチャーを採用した理由としては, 多くのスマートウォッチに搭載されている加速度センサと角速度センサによってジェスチャーが明確に区別できるためである. よって, 認証情報は 3×3 のマトリクス上の複数位置とその順番とし, ユーザは図 2 (a)のように登録し, 以下の手順で位置を登録する.

[登録手順]

(1) 画面上の「登録」ボタンを押すと, 3×3 のアイコンが表示される.
(2) ユーザは登録したい場所を 4 つの画面にそれぞれ一つずつタッチする.
(3) ダミー番号を追加したい場合は,「ダミー」ボタンを押して登録する.
(4) 全て登録して「認証」ボタンを押す.

手順(2)において, 本提案方式が偶然に認証される確率(以後, 偶然認証率と呼ぶ)については, N桁を登録した場合, $1/9^N$となる. PIN 方式と同等以上の偶然認証率$1/10{,}000$以下を実現するためには, $N \geq 5$ である必要がある. 今回は関連研究[15]と同様にユーザビリティを考慮し, $N \geq 4$ とする.

認証時には, 3×3 のマトリクス上の登録位置をジェスチャーによって指定する. 認証は図 2 (b)のように行い, 以下の手順で行う.

[認証手順]

(1) 画面に 3×3 のアイコンが表示される. このとき, 9 種類のジェスチャーに対応したアイコンがランダムに過不足なく表示される.
(2) ユーザは登録位置上のアイコンに相当するジェスチャーを行うことで位置を指定する. ただし, ダミー番号を登録した場所では, 表示されたアイコンと異なるジェスチャーを行う.
(3) 手順(1)と(2)を 4 回繰り返す.

手順(1)において, アイコンをランダムに表示することでジェスチャーのみを覗き見されても認証情報が漏洩しないようになる. 手順(2)において, ジェスチャーとアイコンの対応を図 3 のように定めたが, ダミー番号を登録した場合のジェスチャーとアイコンの対応は図 4 のようになる.

4. 実装

3 章の提案方式の実装を行う. 開発環境として, Android Studio 上で Java 言語を用いてプログラムの開発を行い,

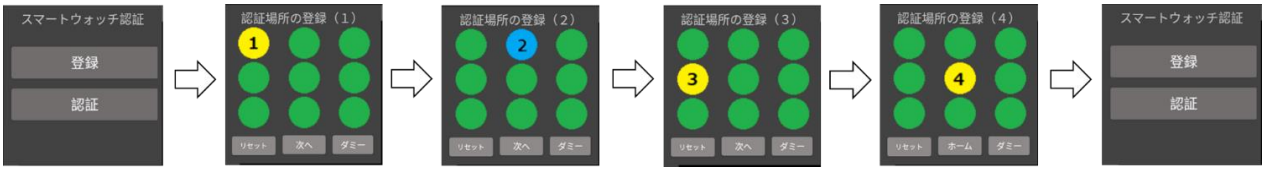


図 5: 登録画面

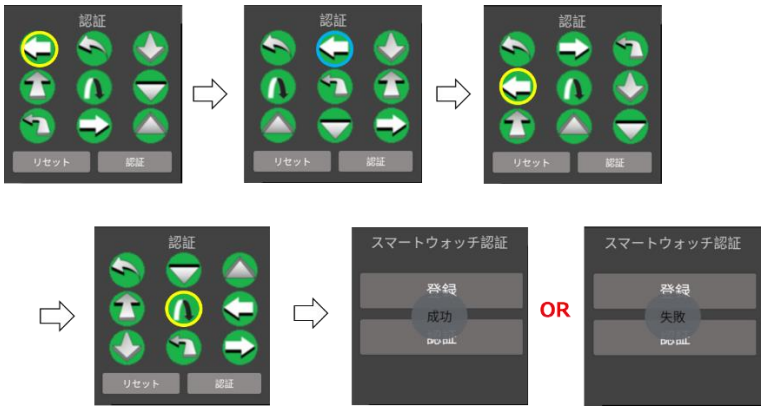


図 6: 認証画面

それを Sony Smart Watch 3 に実装する．実装した登録画面と認証画面は図 5，図 6 のようにしている．

登録画面では，ホーム画面で登録ボタンと認証ボタンが用意されており，登録ボタンを押すと登録場所の画面へ移行する．同じ登録場所でも認証可能であることを示すために，画面は 4 つに分割して表示されている．アイコンをタッチすると，タッチされた番号が黄色に変化して，1～4 の番号が順番に表示される．ダミーボタンをタッチすると，番号が青色に変化して登録される．

認証画面では，ユーザは登録位置上のアイコンに相当するジェスチャーを行うことでその位置を指定できる．例えば上段の左上，上段真ん中，中段の左，中段の真ん中の順で認証情報を登録した場合，登録手順で 1 番目に登録した場所に表示されている左のジェスチャーを行う．スマートウォッチがジェスチャーを認識すると振動し，ジェスチャーアイコンが再びランダムに表示される．同様に 2 番目に登録した場所に表示されている左のジェスチャーだが，ここはダミーとして登録した場所なので，この場合は左ではなく右のジェスチャーを行う．以降は通常通り 3 番目の左，4 番目の回転となる．登録した場所上のジェスチャーアイコンとジェスチャーが全て一致した場合は認証成功，一つでも一致しない場合は認証失敗となり，画面に表示される．また，ジェスチャーの失敗を考慮し，認証を最初から開始するためのリセットボタンと，認証判定を行う認証ボタンをアイコンの下に配置する．

5. 評価実験と考察

4 章で実装を行った Sony Smart Watch 3 を用いて，提案方式の性能を評価するためにユーザビリティ，慣れによる使用感の変化，覗き見耐性の確認実験を行う．

5.1 ユーザビリティの確認実験

提案方式の使いやすさを評価するため，ユーザビリティの確認実験を行う．提案方式はジェスチャーを用いて認証を行うが，実際の認証情報は離散的なマトリックスの位置となる．そのため，この実験では FAR と FRR を求めず，認証時間と認証成功率を求めることに加えて，被験者にアンケートに答えてもらうことで評価を行う．被験者は神奈川工科大学生 10 名であり，以下の手順で実験を行う．

(1) 被験者に提案方式の説明を行い，ジェスチャーの練習を行ってもらう．
(2) 被験者は認証情報の登録を行う．このとき登録する場所を 4 つとして，最低 1 つ以上はダミー番号を追加してもらう．
(3) 被験者は成功・失敗に関わらず認証を 5 回行う．
(4) 被験者はアンケートに答える．

手順(4)のアンケートについて，被験者は以下の 5 つの項目を 1～5 の 5 段階で答えてもらう．

- 理解度：理解しやすかったか
- 使用感：使いやすかったか

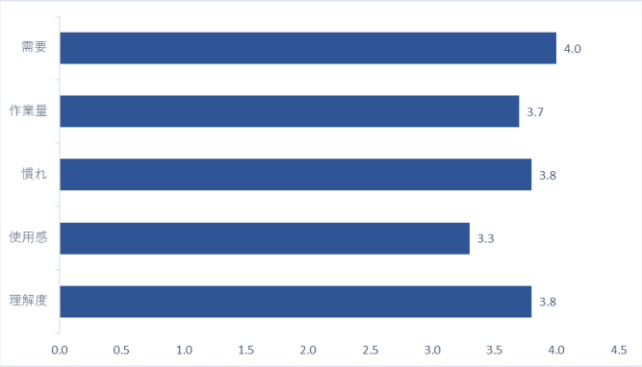


図 7: アンケート結果

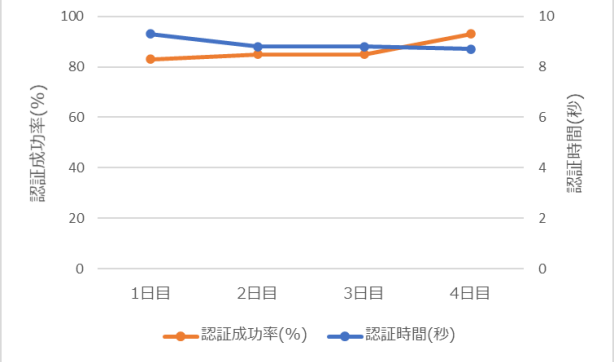


図 8: 認証時間と認証成功率の変化

- 慣れ：慣れれば使いやすいと思うか
- 作業量：認証の作業量が多いと感じたか
- 需要：また使いたいと思うか

実験の結果として，平均認証時間が 10.9 秒，認証成功率は 73.3%となった．また，アンケート結果を図 7 に示す．使用感の項目のみが 3.5 を下回り，それ以外は 3.5 以上となった．このような結果となった理由として，被験者がジェスチャーを間違えてしまったとき，リセットボタンをタッチして 1 つ目のジェスチャーからやり直すことがあったことと，ダミージェスチャーに未だ慣れていないため，認証時間が長くなってしまったことが原因であると考えられる．

5.2 慣れによるユーザビリティの変化の調査

前節の実験結果から，ユーザが日常的に認証を行うことを考慮し，慣れによるユーザビリティの変化を確認する実験を行う．具体的には，二週間で認証時間と成功率の変化を調査する．被験者は前節でユーザビリティの実験を行った被験者の内 8 名であり，以下の手順で実験を行う．

(1) 被験者は認証情報を登録する．このとき登録する場所を 4 つとし，十分な覗き見耐性を持つことを考慮して，最低 2 つ以上はダミー番号を追加してもらう．
(2) 被験者は成功・失敗に関わらず認証を 5 回行う．
(3) 手順(2)を 2 週間で 4 日間行う．

図 8 に日数ごとの平均認証時間と認証成功率を示す．結果として，4 日目には平均認証時間が 9.4 秒から 8.8 秒へ 0.6 秒減少し，認証成功率は 83%から 93%と 10%向上した．よって，日を追うごとにユーザビリティが向上することが確認できる．

5.3 覗き見耐性の確認実験

提案方式における覗き見耐性の確認実験を行う．被験者は神奈川工科大学生 10 名であり，以下の手順で実験を行った．

(1) 二人一組の班を作り，ユーザと覗き見者の役割を決める．
(2) ユーザはスマートウォッチを左腕に付けて，認証情報を登録する．登録時には，十分な覗き見耐性を考慮し，最低ダミー番号を 2 つ以上追加してもらう．
(3) ユーザは成功・失敗に関わらず認証を 5 回行う．このとき，覗き見者はユーザの認証を覗き見し，認証情報を特定する．なお，覗き見中はメモを取ってよいこととする．
(4) ユーザと覗き見者の役割を交代し，再び手順(2)と(3)を行う．

手順(3)において，ユーザが成功・失敗に関わらず認証を 5 回行うと定めた理由は，ユーザがジェスチャーを正確に行うことができずに誤判定された場合でも，覗き見者はジェスチャーの予測が可能であると考えたからである．

実験結果として，覗き見回数と漏洩桁数に対応する漏洩率を表 1 に示す．漏洩率が多ければ多いほど緑色が濃くなるように着色している．4 桁のうち一桁も漏洩していないなら「×」，一桁漏洩しているなら「1」，二桁なら「2」，三桁なら「3」，四桁全て漏洩していたなら「4」と表記している．結果として，1 回目から 5 回目の覗き見攻撃で全ての登録位置を見破る実験者はいなかった．しかし，被験者によって全く漏洩しなかったり，三桁まで漏洩されたりと，漏洩率に偏りが見られることが多かった．その原因として，ダミージェスチャーの中で唯一「回転」のジェスチャーは通常時と同様なため，覗き見者がそこを見抜いて推測し，見破ることができたためであると考えられる．

表 1: 覗き見実験結果

被験者	覗き見回数				
	1回目	2回目	3回目	4回目	5回目
A	×	×	×	×	×
B	×	1	1	1	1
C	×	×	1	1	3
D	1	1	1	1	2
E	×	×	×	1	1
F	×	×	×	×	×
G	1	1	1	2	2
H	1	1	1	1	1
I	2	2	2	2	3
J	1	1	2	2	2

表 2: 関連研究と提案方式の比較

	偶然認証確率	認証時間 （慣れの実験）	認証成功率 （慣れの実験）	FAR	FRR	覗き見成功率
PIC[8]	1/10,000	1.2秒	92.1%	ー	ー	100%
シフトルールを用いた方式[9]	1/5,9049	13.8秒	89.4%	ー	ー	0%
竜頭を用いた認証方式[10]	1/10,000	16.9秒	84%	ー	ー	10%
持ち上げ動作による認証方式[13]	ー	ー	ー	1.7%	約1.0%	2.9%
TwistIn[14]	ー	2.3秒	ー	0.6%	0%	5.0%
ジェスチャーを用いた認証方式[15]	1/6,561	14.0秒 (7.6秒)	76.9% (91.4%)	ー	ー	10%
提案方式	1/6,561	10.9秒 (8.8秒)	73.3% (93%)	ー	ー	0%

5.4 考察

提案手法と関連方式のユーザビリティと覗き見耐性の比較を行う．比較対象はスマートウォッチにおける認証方式[8, 9, 10]，スマートウォッチとスマートフォンにおいて同時にジェスチャーを行う認証方式[14, 15]である．これらを比較した表を表 2 に示す．

提案方式の偶然認証率については，PIN と同等以上の 1/10,000以下を達していないため，ジェスチャーを行う認証方式[15]と同様に，他の関連研究より高くなっている．

認証時間については，提案方式は PIC[8]より長く，シフトルールを用いた方式[9]，ジェスチャーを用いた方式[15]よりも短いが，慣れによる認証時間の比較では，関連方式[15]よりも時間が長くなる．

また，認証成功率はすべての関連研究と比べて低い結果となっているが，5.2 節の実験結果からジェスチャーの慣れによって 93%まで向上し，PIC[8]やジェスチャーを用いた方式[15]と同程度の認証成功率となっている．

覗き見成功率について，PIC[8]は画面のタッチ操作がそのまま認証情報となることから覗き見耐性がないと考えられるので，100%と記述した．提案方式については，シフトルールを用いた方式[9]と同様に，十分な覗き見耐性を持っていると考えられる．

6. おわりに

本論文では，スマートウォッチでスマートフォンやタブレットなどの携帯端末を，アンロックすることを考慮した個人認証方式として提案されていたジェスチャー認証方式[15]の覗き見耐性を向上するために，認証登録時にダミー番号を追加し，表示されたアイコンとは異なるジェスチャーを用いた認証を提案した．

また，ユーザビリティ，慣れによるジェスチャーの使用感と覗き見耐性の確認実験を行った結果，平均認証時間が 10.9 秒，認証成功率が 73.3%となり，日を追うごとに認証時間と認証成功率が向上し，それぞれ 8.8 秒, 93.3%まで向上した．また，ダミー番号を二つ以上追加した覗き見攻撃によって 4 桁全ての認証情報が漏洩することはなかった．

今後の課題を以下に示す．

- ユーザビリティの向上

本論文の提案方式では，ジェスチャー認証方式[15]と同様に，ジェスチャーを複数回行う必要があるため，他の関連研究の認証方式より認証時間が長くなってしまうことが考えられる．そこで，認証時間を短くする工夫を行うことによって，ユーザビリティを向上させる必要がある．

- ジェスチャーの改良

評価実験時に被験者の意見を聞き，「肘を支点に上」「肘を支点に前」のジェスチャーが失敗しやすく，もう少しジェスチャーを行いやすくできないかという声が多く挙がった．また，ダミー時の「回転」ジェスチャーは従来のジェスチャーと変わりはないという課題がある．そのため，新たに認証しやすいジェスチャーの検討と，ダミー時の「回転」ジェスチャーに代わるジェスチャーについて考える必要がある．

参考文献

[1] Bkav 's new mask beats Face ID in "twin way": Severity level raised, do not use Face ID in business transactions, 入手先 <https://www.bkav.com/en/top-news/-/viewcontent/65202/bkav-s-new-mask-beats-faceid-in-twin-way-severity-level-raised-donot-use-face-id-in-business-transactions>, 2020-12-29 参照.

[2] Gartner: Gartner Says Worldwide Wearable Device Sales to Grow 26 Percent in 2019, 入手先<https://www.gartner.com/en/newsroom/press-releases/2018-11-29-gartner-says-worldwide-wearable-device-sales-to-grow->2020-12-29 参照.

[3] Apple Watch のロックを解除する，入手先 <https://support.apple.com/jajp/guide/watch/apd0e1e73b6f/watchos>, 2020-12-29 参照.

[4] Smart lock, 入手先 <https://support.google.com/android/answer/9075927>, 2020-12-29 参照.

[5] 喜多 義弘, 岡崎 直宣, 西村 広光, 鳥居 秀幸, 岡本 剛, 朴 美娘"覗き見耐性を持つユーザ認証システムの実装と評価, " 電子情報通信学会論文誌, vol. J97-D, no. 12, pp. 1770-1784, 2014.

[6] 石塚 正也，高田 哲司, "CCC：携帯端末での暗証 番号認証における振動機能を応用した覗き見攻撃対 策手法，" 情報処理学会論文誌, vol. 56, no. 9, pp. 1877-1888, 2015.

[7] 田中 基偉, 稲葉 宏幸, "利便性を考慮した覗き見に耐性を有する改良型背景パターンスライド認証方式の提案，" 情報処理学会論文誌. Vol. 58, no. 9, pp.1513-1522, 2017.

[8] Ian O., Jun H. H., Hunsung C., Geumhwan C., Rasel I. and Hyoungshick K., "The Personal Identification Chord: A Four ButtonAuthentication System for Smartwatches," Proc. of the 2018 on Asia Conference on Computer and Communications Security, pp. 75-87, 2018.

[9] 長友 誠, 渡辺 一樹, 油田 健太郎, 岡崎 直宣， 朴 美娘, "覗き見耐性を持つ小型タッチスクリー ン端末における個人認証方式の提案," 2019 Symposium on Cryptography and Information SEcurity(SCIS2019), 3E4-2, pp. 1-7, 2019.

[10] 稲村 勝樹，市村 安佑，"スマートウォッチの竜頭 型コントローラを用いた暗証番号入力方法,"情報処 理学会研究報告，vol. 2019-IOT-44, no. 38, pp. 1-6, 2019.

[11] 濱野雅史，新井 イスマイル，"加速度センサ・ジャイ ロセンサを併用したスマートフォンの利用認証手法の提案," 情報処理学会研究報告，vol. 2014-MBL-70, no. 17, pp. 1-8, 2014.

[12] 出田 怜，村尾 和哉，寺田 努，磯 俊樹，稲村 浩，塚 本 誠彦，"携帯電話の取り出し動作に基づく画面ロッ ク解除手法のなりすまし耐性の評価,"情報処理学会 研究報告，vol. 2017-UBI-55, no. 4, pp. 1-8, 2017.

[13] Shrirang M., Reza R., Ronald P. and David K., "Continuous Smartphone Authentication using Wristbands," Workshop on Usable Security(USEC), 12 pages, 2019.

[14] Ho-Man C. L., Chi-Wang F., Pheng-Ann H., "TwistIn: Tangible Authentication of Smart Devices via Motion Co-analysis with a Smartwatch," Proc. of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, vol. 2, no. 2, 24 pages, 2018.

[15] 長友誠, 小関朋奈, 渡辺一樹, 池田健太郎, 岡崎直宜, 朴美娘 "スマートウォッチにおけるジェスチャを用いた個人認証方式の提案と評価, " 2020 Symposium on Cryptography and Information Security(SCIS 2020), IE2-1, 電子情通信報学会, 2020.