情報処理学会論文誌 Vol.63 No.4 1082–1093 (Apr. 2022)

推薦論文

録画による覗き見攻撃に安全な個人認証のユーザインタフェース改良による実用性向上

江原 知志[1,a)] 高田 哲司[1,b)]

受付日 2021年5月2日, 採録日 2022年1月11日

概要：覗き見攻撃は携帯端末での個人認証において現実的に起こりうる脅威の1つである．この脅威に対する対策手法として，携帯端末の振動機能を利用した個人認証手法が複数提案されている．しかしそれらの手法には認証に時間がかかるという実用面の課題がある．そこで本研究では，振動機能を利用した既存手法の1つに対し，ユーザインタフェース改良を図ることによって，覗き見攻撃に対する安全性を維持しながら既存手法より認証時間を短縮することを試みた．1つは入力操作に必要な情報の取得時間を短縮させるものであり，もう1つは直感的な入力操作方法の導入である．この提案に基づく認証システムをAndroidアプリケーションとして実装し，実験参加者による評価実験を行った．実験結果から，改良対象となったシステムとの比較で認証時間を平均6秒短縮することに成功した．また安全性についても想定脅威に対して同等程度の安全性が維持されることが確認された．さらに，振動を利用した他の既存認証手法とも比較議論を行い，提案手法が先行研究の手法よりも操作負担が低く，安全性を危殆化させうる問題点が少ない手法であることを示した．

キーワード：覗き見攻撃，録画攻撃，個人認証，ユーザインタフェース，振動，入力方法

Better Usability of Camera-recording Based Shoulder Surfing Resilient User Authentication by Redesigning User Interface

Satoshi Ehara[1,a)] Tetsuji Takada[1,b)]

Received: May 2, 2021, Accepted: January 11, 2022

Abstract: Shoulder surfing attack is one of threats in a user authentication. As a countermeasure against this threat, vibration applied user authentication schemes have been proposed. However, a survey of previous studies revealed that this type of schemes have an issue of long operation time. We, then, took one of the previous studies and attempted to reduce the operation time by improving its user interface. We updated the UI of the original scheme as follows: (1) we reduced the number of cursor move to less than half for conveying the input position, and (2) we introduce a more intuitive dial operation method than button operation. We implemented a prototype system as Android application and conducted evaluation experiments with participants. As a result, we succeeded to reduce the operation time compared to the original scheme while keeping security against camera-based shoulder surfing attack. Moreover, we found a security issue in the original scheme through the experiment and our scheme is less affected by the issue. We also discuss about both usability and security in vibration applied user authentication schemes and showed that our scheme has fewer security and usability issues than the schemes in previous studies.

Keywords: shoulder surfing, recording attack, user authentication, user interface, vibration, input operation

1. はじめに

パスワードや暗証番号等の記憶に基づく個人認証における脅威の1つに覗き見攻撃がある．覗き見攻撃とは，攻撃者が正規ユーザの認証行為を覗き見ることで入力された秘密情報（例：暗証番号，パスワード）を不正に取得する攻撃である．この攻撃は実行に際して技術的なスキルを必要としないため，誰でも攻撃者になりうる．また様々なシー

[1] 電気通信大学
The University of Electro-Communications, Chofu, Tokyo 182–8585, Japan
[a)] hrstsh@mail.uec.jp
[b)] zetaka@computer.org

本論文の内容は2020年10月のコンピュータセキュリティシンポジウム2020（CSS2020）で報告され，同プログラム委員長により情報処理学会論文誌ジャーナルへの掲載が推薦された論文である．

ンで計算機や携帯端末を利用するようになり，個人認証を覗き見される機会も増えている．このような状況から，本脅威は身近に存在する脅威であり，そのリスクは無視できないものだと考える．

このような現状を背景に，覗き見攻撃の対策手法について様々な研究が報告されている．これらの提案は，大きく分けて 2 つの脅威モデルのどちらかを想定している．

- 認証行為を人間が覗き見することを想定
- 認証行為をビデオカメラで録画することを想定

以降本論文では前者を「人による覗き見攻撃」，後者を「録画攻撃」と呼ぶ．これらの脅威モデルの違いは，認証行為の捕捉・記録能力にある．「人による覗き見攻撃」は，人間が認証行為を見てその状況を記憶するため，捕捉できる情報が一部に限られる可能性がある．また時間経過とともに忘却によって捕捉した情報が欠損する可能性もある．これに対して「録画攻撃」は，視覚的に捕捉可能な情報はすべて記録でき，忘却による情報欠損も生じないと仮定する．さらに録画攻撃は認証行為が録画データとして記録に残るため，事後の処理能力も拡大する．たとえば，録画データを繰り返し再生したり，なんらかの情報処理を適用したりすることで秘密情報を特定することも可能になる．Shukla ら [14] や Guixin ら [4] は，指先と携帯端末の位置を追跡することで，携帯端末の画面内容が映っていない録画データから入力値の推測が可能であることを示した．したがって，「人による覗き見攻撃」よりも「録画攻撃」の方が攻撃者に有利な状況を示した脅威モデルとなっている．

そこで本研究では，記憶に基づく個人認証を対象として，録画攻撃に対して安全性を提供しうる手法の調査を行った．調査の結果，既存の対策手法は認証を行うのにかかる時間（認証時間）が通常の暗証番号認証よりも長くなっていることに注目した．対象脅威に対する安全性を改善するため，認証時間が長くなることはやむを得ない面もある．しかし，認証時間の長さが個人認証そのものを利用しない理由になりうるという事実がある．Harbach ら [5] は，携帯電話で画面ロックを使用しないユーザの主な要因が認証時間が長いことであることを明らかにした．したがって，認証時間の長さは個人認証における実用性の評価軸として無視できないといえる．

そこで本研究では，録画攻撃を脅威モデルとした個人認証には認証時間が長く，実用上の問題が残されていることを明らかにし，その改善策として先行研究の 1 つである個人認証手法 “Circle Chameleon Cursor”（CCC）[8] のユーザインタフェースを改良することで録画攻撃への安全性を確保しつつ，認証時間の短縮を試みた．その結果，有望な結果を得ることができたのでここに報告する．

以降，本論文では 2 章で録画攻撃に耐性のある既存の個人認証手法の調査結果と，本研究で提案する個人認証手法の改良元である CCC の説明，およびこの手法を改良元とした理由について述べる．3 章で CCC の問題点と CCC を改良した本研究での提案手法の説明を行う．4 章で CCC と提案手法を比較するために行った評価実験とその結果を示し，5 章で実験結果に対する考察と今後の課題を述べる．

2. 関連研究

本章では記憶に基づく個人認証の中で，録画攻撃に対して安全性を提供しうる手法の先行研究について調査し，各手法を 3 つのカテゴリに分類する．そのうえでカテゴリごとに実用上の問題点を議論する．また，本研究で提案する個人認証手法の改良元である CCC [8] の手法説明と，この手法を改良元として選択した理由について述べる．

2.1 録画攻撃対策の先行研究

調査した録画攻撃対策の個人認証手法を**表 1** に示す．表内の “AD（Additional Device）” 列は認証を行う装置以外に追加の装置が必要であるかを示しており，“AT（Authentication Time）” 列は各認証手法における認証時間を示している．認証時間値の注釈 *1，*2 は，*1 が中央値，*2 が平均値であることを示している．表 1 内のいずれの手法も，チャレンジ&レスポンス認証方式をとっている．これは認証システムからユーザへワンタイム情報（チャレンジ）を伝達し，ユーザはその情報を利用して自身の秘密情報を入力する（レスポンス）という認証方式である．チャレンジは認証システムがランダムに決定し，レスポンスはチャレンジに依存するため，入力のたびにレスポンスが変化する．そのため，チャレンジを攻撃者が視覚的に捕捉困難な方法を用いてユーザへ伝達することで録画攻撃への対策となっている．我々は，このチャレンジの伝達方法について「振動，音声，その他」の 3 カテゴリに分類した．「振動，音声」

表 1 録画攻撃対策の関連研究の比較

Table 1 Comparison of prior works on countermeasures against camera-recording attack to PIN authentication.

認証手法	秘密情報種別	カテゴリ	AD	AT（s）
SSSL [13]	PIN（5 桁）	音声	必要	8^{*2}
Spinlock（音声）[2]	PIN（4 桁）	音声	必要	10.81^{*2}
近藤ら [9]	PIN（4 桁）	音声	必要	11.73^{*2}
PhoneLock（音声）[1]	PIN（4 桁）	音声	必要	12.2^{*1}
VDA [6]	PIN（4 桁）	振動	-	8.44^{*2}
Spinlock（振動）[2]	PIN（4 桁）	振動	-	13.86^{*2}
TictocPIN [11]	PIN（4 桁）	振動	-	15.31^{*2}
M-VDLS [3]	PIN（4 桁）	振動	-	18.88^{*2}
PVRotate [7]	PIN（4 桁）	振動	-	21.2^{*2}
VibraInput [10]	PIN（4 桁）	振動	-	23.8^{*2}
PhoneLock（振動）[1]	PIN（4 桁）	振動	-	28.2^{*1}
CCC [8]	PIN（4 桁）	振動	-	36.41^{*2}
GlassUnlock [15]	PIN（4 桁）	その他	必要	4.8^{*2}
3DPIN [12]	PIN（4 桁）	その他	必要	12.9^{*2}

は振動や音声を用いてシステムからユーザへチャレンジを伝達する手法である．「その他」は振動や音声以外の方法をチャレンジ伝達に用いる手法である．GlassUnlock [15] はスマートグラスにチャレンジを表示することでユーザのみがチャレンジを取得できる手法である．3DPIN [12] は，3D 表示に対応した視差バリア方式のディスプレイを用いてチャレンジを伝達するため，画面正面にいるユーザのみがチャレンジを取得可能な手法となっている．

3 つのカテゴリを比較すると，同じ秘密情報種別でも認証時間に差があることが分かる．「音声」と「その他」のカテゴリの認証手法は，PIN（4 桁）の秘密情報において 4.8 秒から 12.9 秒の認証時間となっている．一方，「振動」カテゴリに該当する認証手法においては，VDA [6] を除いたすべての認証手法が 13 秒以上の時間を要している．このため「振動」カテゴリの認証手法は，他の 2 カテゴリに属する認証手法よりも認証時間が長いという特徴があるといえる．一方で「振動」カテゴリの認証手法は，他カテゴリの手法との比較で利用シーンに関する制約が少ないといえる．「音声」や「その他」のカテゴリの認証手法では認証時にイヤホンやスマートグラス等の追加装置が必要となるが，「振動」カテゴリの認証手法では携帯端末に実装されている振動機能を利用できるため追加装置を必要としないからである．したがって，「音声」や「その他」のカテゴリの認証手法には，利用シーンが制限されるという点が，「振動」カテゴリの認証手法では認証時間が長いという点が課題としてあげられる．そのため，これらの問題点を改善することで実用性を向上させることが可能であると考える．しかし，利用シーンの制限は追加装置を必要とする限り発生し，これを改善することは，別のチャレンジ伝達方法を使用することに等しいと考える．一方，認証時間の短縮は同じ「振動」カテゴリの認証手法でもチャレンジ伝達の仕方や入力方法を工夫することで実現できる可能性があると考えた．よって本研究ではこのアプローチに基づく改善を試みた．

「振動」カテゴリの認証手法改善において我々は CCC [8] に着目し，その改良を試みた．表 1 からも分かるとおり，CCC は「振動」カテゴリの認証手法において最も認証時間が長い手法であるが，それは以下に述べる 2 つの要因によるものだと考えられ，かつそれらの要因には改良の余地があると考えたからである．1 つ目は，実験に用いたプロトタイプシステムの実装方法である．CCC は Web アプリケーションとして実装されていたが，この実装方法では表示速度や反応速度に遅延が発生する問題があったことが文献 [8] で指摘されている．よって認証時間を評価するうえで適切な実装であったとはいいがたい．したがって，これをネイティブアプリケーションとして実装することで改善される可能性があると考えた．2 つ目は，チャレンジ伝達に必要となる時間が長いことである．詳細は 3.1 節で議論するが，CCC におけるチャレンジ伝達方法はシンプルである一方で，チャレンジ取得に必要となる時間が長いことが文献 [8] でも指摘されている．よって，CCC 手法を踏襲しつつそのチャレンジ伝達方法を改良できれば，ユーザの操作に依存しない形で認証時間を短縮できる可能性があると考えた．したがって，上記 2 つの理由から本研究では CCC を改良元として認証時間短縮を試みた．

2.2 CCC（Circle Chameleon Cursor）

本節では，提案手法の改良元となった先行研究である “Circle Chameleon Cursor”（CCC）[8] について説明する．CCC は，入力行為をビデオで録画されてもその録画データから入力値を特定することを困難にした暗証番号認証手法である．CCC は金庫等における「ダイヤル式数値入力」をベースとし，以下の 2 つのアイデアを組み合わせることで録画攻撃に対する安全性を実現している．

(1) 入力位置のランダム化と隠蔽：通常のダイヤル入力における数値の入力位置は，1 つで「固定位置」である．したがって，入力位置が仮に視認できない状況であっても，正規ユーザと同じ操作を行えば金庫を開けることが可能であり，入力位置が視認できるのと実質的に同じ状況だといえる．そこで CCC では，入力位置をシステムがランダムに変更することとした．これにより，4 桁の数字を入力するのに最大で 4 つの入力位置を使用することになる．また入力位置をランダム化してもそれが視認可能であれば覗き見攻撃に対して脆弱となる．よってシステムからユーザに入力位置を伝達する方法として振動を利用し，入力位置を視認困難にした．

(2) 間接的入力操作：通常のダイヤル入力では，利用者がダイヤルつまみを直接つまんで回転させ，入力位置に入力したい数字を移動させる．しかし，この操作方法ではダイヤルつまみの操作時に入力したい数字を指で指し示してしまうリスクがある．そこで CCC では，ダイヤルつまみの回転操作をボタンを通じて間接的に行うようにした．

これらの工夫により，入力位置をユーザに伝達する際の「振動」情報が攻撃者に漏洩しないかぎり，認証行為をカメラで録画しても入力値の特定は困難となっている．

次に CCC における入力方法について説明する．認証を開始すると**図 1** 左に示す画面が表示される．画面は縦方向に 3 つの部分から構成されており，それぞれ「入力状況表示部」「入力ダイヤル部」「操作 UI 表示部」と呼ぶ．画面中央の「入力ダイヤル部」には入力ダイヤルがあるが，これは既存の入力ダイヤルと同様に数値を入力するためのインタフェースである役割の他に，システムが決定した入力位置をユーザに伝達する役割も担っている．数値入力は以下に述べる 2 手順で行う．

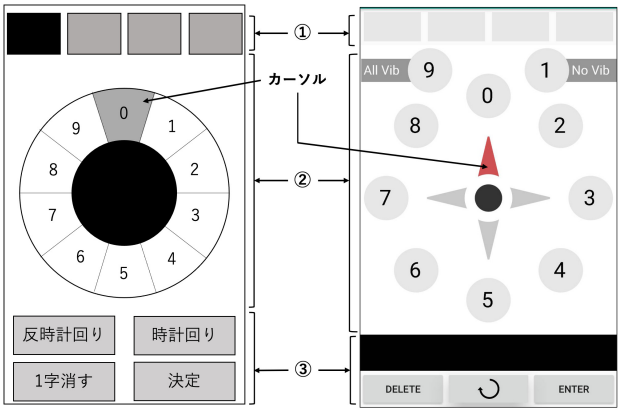

図 1 CCC（左）と VDPin（右）のインタフェース
Fig. 1 PIN input interfaces: CCC (left) and VDPin (right).

CCC 入力手順 1 入力位置の取得：図 1 左の画面が表示されると，入力ダイヤル内にカーソルが表示される．このカーソルは図 1 左の画面中にある入力ダイヤル内の数字 “0” の位置を開始位置として入力ダイヤル内の 10 個の数字ラベルを時計回りに 1 周する．その移動中，システムがランダムに決定した数値ラベルの位置にカーソルが到達したときにのみ振動が 1 回発生する．したがって，入力ダイヤルに存在する 10 個の数値ラベルのうち，振動が発生したときにカーソルが存在していた数値ラベルの場所が入力位置となる．このようにカーソル表示という視覚情報と振動情報の組合せにより，システムからユーザへ入力位置を伝達する．

CCC 入力手順 2 数字の入力：入力ダイヤルを回転させ，入力したい数字を入力位置へ移動させる．入力ダイヤルの回転は図 1 左内の操作 UI 表示部にある「時計回り・反時計回り」ボタンを用いる．移動が完了したら，同じく操作 UI 表示部にある「決定」ボタンを押下して入力を確定する．

この 2 手順によって 1 つの数字が入力される．したがって，この手順を必要回数分（4 桁暗証番号であれば 4 回）繰り返すことで暗証番号を入力する．

3. 録画攻撃に安全な個人認証手法 VDPin

本章では改良元である CCC の問題点を整理し，次にその問題点に対する改善アイデアと，そのアイデアに基づいて提案する VDPin について説明する．

3.1 CCC の問題点

CCC の認証時間を長くしていると考えられる要因について述べる．2.2 節で述べたとおり，CCC には 2 手順の操作が存在するが，その各手順において以下に述べる問題があると我々は考えた．

CCC 問題点 1 CCC 入力手順 1 では，入力位置を取得するのにカーソルが入力ダイヤル内を 1 周移動するのを待つ必要がある．この待機時間が認証時間を長くしているといえる．CCC におけるカーソル移動間隔は 300 ms であり，カーソルが 1 周するのに 3 秒待機する必要がある．4 桁暗証番号認証の場合，これが 4 回必要となるので合計で 12 秒の時間が入力位置取得のために必要となっている．

CCC 問題点 2 CCC 入力手順 2 では，ユーザの操作が攻撃者に入力値を伝えてしまうリスクを避けるため，入力ダイヤルの回転操作をボタンで行っていた．しかし，入力ダイヤルの移動量が多いとボタンを複数回押下する必要があり，現実のダイヤルとは違って直感的な操作とはいいがたく，操作時間を長くしている可能性があると考えた．また直感的な操作でないがゆえに操作ミスが発生し，それを修正するためにさらにボタンを押す必要が生じることから，操作時間を長くしている可能性もあると考えた．

3.2 問題改善のアイデア

前節で述べた 2 つの問題点に対する 2 つの改善方法について述べる．

1 つ目は，入力位置取得にかかる時間を短縮することである．ここで我々は，CCC の操作方法をベースにしつつ，カーソルの移動回数を削減することを考えた．入力位置の伝達ではカーソル移動のために「移動回数 × 移動間隔」分の時間がかかる．このうち移動間隔を小さくすることは困難であることが石塚ら [8] の調査で明らかになっている．カーソル移動を高速化すると，振動情報とカーソル位置による視覚情報にズレが発生し，入力位置を正しく判別することが困難になるからである．したがって，カーソルの移動回数を減らすべきであると考えた．

2 つ目は，入力ダイヤルの回転操作を現状よりも直感的に操作できるようにすることである．そこで我々は，入力ダイヤルを直接操作させないということは維持しつつ，現状よりも直感的に操作可能な別の方法を取り入れることにより操作時間の短縮を試みる．

3.3 改良版システム：VDPin

これまでの議論をもとに，我々は録画による覗き見攻撃にも安全な暗証番号認証のための新たなユーザインタフェース Vibration Direction PIN（VDPin）を考案した．VDPin には前節のアイデアに基づき以下の 2 つの仕組みを導入した．

- 入力位置の通知方法を改良した．認証時間短縮のためにはカーソルの移動回数を減らす必要がある．そこで我々は振動回数を 1 通りでなく複数通りに変更することとした．CCC では「移動回数は 10 回，そのうち振動が発生する回数は 1 回」であったのに対し，VDPin ではそれらを「移動回数は 4 回，そのうち振動が発生

する回数は 0，1，2，4 回のいずれか」に変更した．

- 「タッチバー」と呼ぶ新たな操作方法を導入した．タッチバーとは，特定領域内で画面にふれたまま指を動かすと，その移動距離に応じた操作を可能にする仕組みであり，スクロールバーと同等の操作を可能にするものである．この方法を入力ダイヤルの操作に適用することで，間接的な操作でありつつもボタンより直感的なダイヤル操作を可能にした．

図 1 右は VDPin における入力画面である．画面構成は基本的に CCC と同じであるが，「入力ダイヤル部」と「操作 UI 表示部」に変更が加えられている．

入力ダイヤル部の変更は 2 点ある．1 つは入力ダイヤルの中央部に入力位置伝達用のカーソル表示領域が追加された．上下左右を示す 4 つの三角形が用意され，その三角形群をカーソルが時計回りに移動する．CCC では数字表示とカーソル表示領域が入力ダイヤルで共通化されていたが，VDPin では独立する形とした．もう 1 つは，数値ラベルのレイアウトが変更されたことである．VDPin では 8 個の数字ラベルによる正円形表示（図 1 右の “1” と “9” を除く 8 つの数字）と，その上部に 2 個の数字ラベル（図 1 右の “1” と “9”）が表示されるレイアウトとした．ただし，数値ラベルの配置位置が変更されただけであり，10 個の数字ラベルは概念的に 1 つの円環として接続されている．そのため従来どおりダイヤル操作で数字の位置を移動させることが可能である（**図 2** 参照）．数値ラベルの配置位置の変更は，後述する VDPin の「入力位置の取得」において CCC からの変更に対応した結果である．また，これらの数字ラベルの位置のどれか 1 つが入力位置になることは CCC と同様である．

操作 UI 表示部の変更は「タッチバー」の追加である．図 1 右の操作 UI 表示部にある黒塗りの四角形部分がタッチバーである．この領域を指で触ったまま指を左右に移動させると入力ダイヤルが回転する．これにより，入力したい数字を入力位置に移動させる．

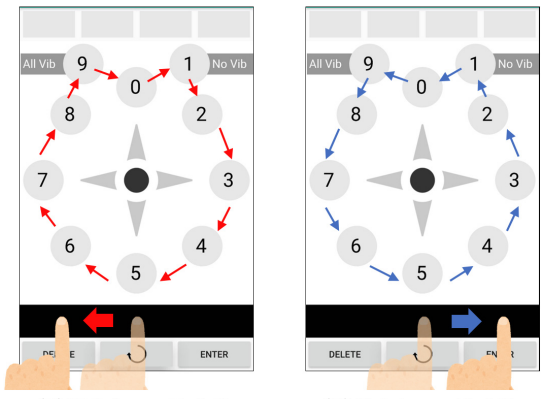

図 2 タッチバーの操作と数字の移動の仕方の対応
Fig. 2 How to operate a numeric dial using the touch bar.

次に入力方法について説明する．VDPin による入力方法は基本的に CCC と同じである．「入力位置の取得」と「数字の入力」の 2 手順で 1 つの数字を入力する．

まず「入力位置の取得」について説明する．VDPin では「移動回数は 4 回，そのうち振動が発生する回数は 0，1，2，4 回のいずれか」と述べた．カーソルは，入力ダイヤル内中央の 4 つの三角形を上向き三角形を開始位置として時計回りに移動するため，移動回数は 4 回である．この移動時に振動が発生するが，その振動回数は 1 回のみから 0，1，2，4 回のどれかとなった．この 4 つの三角形が指し示す向きと振動回数の組合せにより，数字ラベル 10 カ所のどれか 1 つが入力位置になる．その仕組みについて振動回数別に説明する．

- **振動 1 回**：カーソルが 4 回移動する中で 1 回だけ振動が発生したとする．この場合振動が発生したときにカーソルが存在していた三角形が指す向きにある数字ラベルの位置が入力位置となる．たとえば，下向き三角形の場所にカーソルがあるときにだけ振動が発生した場合，入力位置は図 1 右における数字ラベル “5” の位置が入力位置となる．つまり振動 1 回の場合，入力位置は図 1 右における “0，3，5，7” のいずれかとなる．
- **振動 2 回**：振動 2 回の場合，隣り合う 2 つの三角形にカーソルが存在するときに 1 回ずつ振動が発生する．つまりカーソルが 1 周する間に（上右，右下，下左，上左）のどれかの組合せで振動が発生する．これは 2 つの三角形が指し示す向きをベクトル合成した向きに存在する数値ラベルの位置が入力位置になることを示すためである．たとえば，上向きと左向きの 2 つの三角形にカーソルが存在したときに振動が発生した場合，図 1 右で数字ラベル “8” の位置が入力位置となる．つまり振動 2 回の場合，入力位置は図 1 右における “2，4，6，8” のいずれかとなる．
- **振動 4 回**：カーソルが 1 周移動する際，すべての三角形にカーソルが存在するタイミングで振動が 1 回ずつ発生することを意味する．この場合，入力位置は図 1 右における数値ラベル “9” の位置となる．
- **振動 0 回**：カーソルが 1 周移動する間に 1 度も振動が発生しないことを意味する．この場合，入力位置は図 1 右における数値ラベル “1” の位置となる．

いいかえると，正円上にある 8 カ所の数字ラベルを振動回数 1 回と 2 回のケースで指し示し，振動したときにカーソルが存在した三角形の向きが入力位置を視覚的に指し示すようになっている．また残りの 2 カ所については，振動 0 回と 4 回を適用したという仕組みになっている．

これにより，カーソルの移動間隔が CCC と同様であっても，移動回数は 10 回から 4 回になるため，入力位置の取得にかかる時間は短縮され，トータルとして認証時間の

短縮が見込める仕組みになっている．

次に「数字の入力」について説明する．VDPin では CCC における「時計回り・反時計回りボタン」が「タッチバー」に置き換わっている．図 2 はタッチバー上での指の移動方向と入力ダイヤルの回転方向の対応を示している．図 2 (A) はタッチバー上で指を左へ動かした場合の入力ダイヤルの様子を示している．この場合，入力ダイヤルは時計回りに回転する．同様に図 2 (B) はタッチバー上で指を右へ動かした場合であり，入力ダイヤルは反時計回りに回転する．入力ダイヤルの回転量はタッチバー上の指の移動距離に対応しており，タッチバーを端から端まで動かすと入力ダイヤルが 1 周回転するように設定している．タッチバーで入力する数字を入力位置へ移動した後，「ENTER ボタン」を押下して入力を確定する．

4. 評価実験

VDPin による効果を検証するために評価実験を行った．実験は VDPin の認証時間を明らかにするための操作性評価実験と，録画攻撃に対する安全性を検証するための安全性評価実験の 2 つを実施した．VDPin と CCC を比較するために，VDPin と CCC をそれぞれ Android のネイティブアプリケーションとして実装し，実験に使用した．

4.1 操作性評価実験

本実験は，3.3 節で述べた改善提案が認証時間や認証成功率にどのような影響を与えたかを検証することを目的として行った．VDPin の CCC からの改善は (i) 入力位置の通知方法，(ii) タッチバーの導入である．この 2 つの改善が認証時間や認証成功率に与える影響を調査するため，CCC および VDPin の条件に加えて，図 1 において「操作 UI 表示部」が CCC と VDPin で入れ替わった 2 条件を設けた．したがって実験は以下の 4 条件で実施した．

- C_{btn}：CCC
- C_{tbr}：CCC（ただし，操作方法はタッチバー）
- V_{btn}：VDPin（ただし，操作方法はボタン）
- V_{tbr}：VDPin

11 人の参加者が実験に参加した．全員が 20 代男性で大学生，大学院生または大学を卒業した社会人であり，スマートフォンの利用者であった．実験に使用した Android 端末は Samsung Galaxy S6（5 人），ASUS ZenFone 5（1 人），Google Nexus 5X（5 人）であった．

実験は以下の手順で実施した．

(1) 実験の手順説明：参加者には覗き見攻撃対策の 2 つの認証手法を操作する実験であることを伝えた．
(2) 暗証番号の登録：システムでランダムに生成した 4 桁数字を暗証番号として割り当てた．
(3) 操作説明・操作練習：4 条件の認証システムについて操作方法を説明し，認証成功するまで練習させた．

表 2 各条件の認証時間・認証成功率の結果
Table 2 Authentication time (AT) and authentication success rate (SR) in four conditions by CCC and VDPin.

条件	AT（s）			SR
	（平均値）	（中央値）	（最小値）	
C_{btn}	22.70	19.70	17.39	85.45%
C_{tbr}	22.05	21.56	18.11	89.09%
V_{btn}	15.94	15.14	12.33	94.55%
V_{tbr}	16.07	15.51	11.47	96.36%

(4) 評価実施：各実験条件ごとに各参加者に認証操作を 5 回ずつ行わせた．4 条件の実施順序は参加者ごとにランダム順とし，学習効果による影響に配慮した．
(5) アンケート：参加者の人口統計情報および使用したシステムに対する主観的な印象として「ストレス度合い」と「操作に必要とする集中力」についてアンケートを実施した．

各条件ごとの認証時間と認証成功率の結果を**表 2** に示す．表内の AT は認証時間，SR は認証成功率を表す．VDPin における CCC からの 2 つの改善それぞれが認証時間に与えた影響を調べるために，各条件の平均認証時間についてすべてのペアの組合せでウィルコクソンの符号付き順位和検定を行った（ボンフェローニ補正後の有意水準 $\alpha = 0.0083$）．その結果，C_{btn} と C_{tbr}，V_{btn} と V_{tbr} では有意差は得られなかった（それぞれ，$p = 0.9658$，$p = 0.8311$）．一方それ以外のすべてのペアで有意差が得られた（該当するすべてのペア条件において，$p < 0.001$）．また，認証成功率についてもウィルコクソンの符号付き順位和検定を行ったところ，すべてのペア間で有意差は得られなかった．

実験手順 (5) のアンケートでは「入力位置の取得」と「数字の入力」について実験参加者の主観的印象をアンケートで調査した．**表 3** にアンケートでの質問内容と回答結果を示す．設問 1，2 は CCC と VDPin のどちらが入力位置の取得に必要とされる集中力やストレス度合いが大きいかを調査した．設問 3 から設問 6 は CCC と VDPin それぞれにおいて 2 種類の入力方法のどちらが集中力を必要とし，ストレスを感じるかを調査した．各設問に対する回答は「どちらかの条件」またはどちらも同等の負担であるという意味の「両方同じ」の 3 択から選択させた．

4.2 安全性評価実験

本研究で実装した CCC と VDPin に対して録画攻撃を行い，録画攻撃に対する安全性を評価した．本実験では，操作性評価実験で用いた 4 つの条件に対して攻撃実験を行った．以下に実験手順について述べる．

(1) 攻撃用映像の準備：録画攻撃の対象となるユーザの認証行為を録画した．
(2) 入力値の推測：参加者に録画データから入力値の推測を行わせた．

表 3 アンケートの設問と結果
Table 3 Post-experiment survey: Questions and its responses.

	質問内容	CCC	VDPin	両方同じ
設問 1	入力位置を認識するためによりストレスを感じたのはどちらか	9 人	1 人	1 人
設問 2	入力位置を認識するためにより集中力を必要としたのはどちらか	8 人	2 人	1 人
	質問内容	C_{btn}	C_{tbr}	両方同じ
設問 3	C_{btn} と C_{tbr} においてよりストレスを感じたのはどちらか	7 人	4 人	0 人
設問 4	C_{btn} と C_{tbr} においてより集中力を必要としたのはどちらか	5 人	4 人	2 人
	質問内容	V_{btn}	V_{tbr}	両方同じ
設問 5	V_{btn} と V_{tbr} においてよりストレスを感じたのはどちらか	6 人	4 人	1 人
設問 6	V_{btn} と V_{tbr} においてより集中力を必要としたのはどちらか	4 人	5 人	2 人

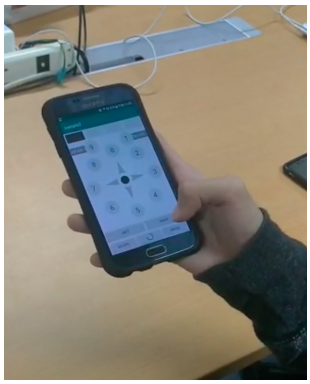

図 3 安全性評価実験に使用した録画データ
Fig. 3 An example of the recorded data used in the attack experiment.

まず攻撃用映像の準備として，被害者役の参加者に前述の 4 条件で 1 回ずつ認証操作を行わせ，その様子を録画した．入力する暗証番号は各条件ごとに乱数を用いて無作為に決定した．録画は ASUS ZenFone5（動画の解像度：1,920 × 1,080 pixel）を使用し，被害者役が利用する携帯端末から約 60 cm の距離から録画を行った．ZenFone5 は誰でも入手可能なスマートフォンであり，携帯端末から約 60 cm の距離ではカメラが被害者の視界に入らないため，現実世界で実行可能な条件であると考えられる．また，この距離は石塚ら [8] の録画攻撃実験において採用された距離である．撮影した映像のスクリーンショットを**図 3** に示す．

次に，攻撃者役の参加者に入力値の推測を行わせた．用意した録画データを Web ページ上で閲覧可能にし，攻撃者役の参加者には各動画を最低 3 回視聴したうえで推測を行うよう指示した．推測した入力値とどのような方法を用いて推測を行ったかを Google フォームを利用して回答させた．推測は 5 回までとし，推測値を回答するたびにその値が正解かどうかを参加者にフィードバックした．本実験において，動画再生に関する操作および時間制約はいっさい設けなかった．何回でも動画を閲覧することができ，一時停止やスロー再生等も自由に行える状況で実験を実施した．また紙や鉛筆の使用も禁止しなかった．

表 4 各条件の特定成功桁数ごとの推測数
Table 4 Relationship between the number of identified digits and the number of successful cases in four authentication systems.

条件	0 桁	1 桁	2 桁	3 桁	4 桁	合計推測数
C_{btn}	4	8	6	2	0	20
C_{tbr}	14	2	0	0	1	17
V_{btn}	7	8	5	0	0	20
V_{tbr}	17	3	0	0	0	20

4 人の参加者が攻撃者役として，1 人の参加者が被害者役として実験に参加した．攻撃者役の参加者全員が著者と同じ研究室に所属する 20 代の学生であり，操作性評価実験にも参加していた．このため，CCC と VDPin のどちらの認証手法についても十分理解していた．被害者役の参加者は操作性評価実験の参加者の中から，攻撃者役の 4 人以外でなおかつセキュリティを専門として学んでいない人を選んだ．これは平均的なユーザによる認証行為を想定したためである．

攻撃実験の結果を**表 4** に示す．表内の各列に示されている「桁数」は，攻撃者が回答した 4 桁数字のうち入力値特定に成功した桁数を表しており，4 桁の列は「暗証番号 4 桁を完全に特定した」ことを意味する．実験結果をまとめると以下のとおりである．

- C_{tbr}（CCC・タッチバー方式）において 1 名の参加者が暗証番号 4 桁の特定に成功した．
- 3 桁の特定に至った回答は C_{btn}（CCC・ボタン方式）条件において 2 件発生した．
- VDPin においては 3 桁以上の特定に至る回答はなかった（V_{btn}，V_{tbr} 条件）．

なお C_{tbr} 条件において合計推測数が 17 回になっている理由は，1 人の参加者が 2 回目の推測で暗証番号を完全に特定したためである．C_{tbr} 条件で暗証番号の特定に成功した理由は，被攻撃者役が認証時に行っていた動作にある．この動作については 5 章で述べる．

5. 考察

本章では，VDPin の安全性と利便性について (1) CCC と (2) 先行研究との比較議論を行う．これらの議論により，

VDPin が既存手法よりも望ましい安全性と利便性を兼ね備えた手法であることを示す．

5.1 CCC との比較

5.1.1 録画攻撃への安全性と認証時間の比較について

4.1 節および 4.2 節の評価結果から，以下の 2 点が明らかとなった．

(a) 録画攻撃への安全性：CCC と VDPin は録画攻撃に対して同等程度の安全性を持つ

(b) 認証時間：VDPin は CCC よりも認証時間が短い

項目 (a) は表 4 に示されている結果より，暗証番号を 4 桁すべて特定できた攻撃者数，暗証番号のうち 2 桁または 3 桁の値を特定できた攻撃数において VDPin は CCC と同等か少ない結果となっていることが根拠である．項目 (b) については，表 2 の結果から操作時間が平均で 6 秒程度短縮されており，統計的にも有意差があることが明らかになっている．これが根拠となっている．

これらの結果から，本研究の目的である「CCC と同等の安全性を確保しつつ，認証時間を短縮する暗証番号入力手法」は実現できたと考える．

5.1.2 利便性について

VDPin は CCC との比較で操作時間を短縮した．これにより 2 章で述べた実用性向上を実現したが，それは利用者になんらかの負担を課すことで実現されたものではないか，という懸念が残っている．この懸念について，3 つの指標を用いて CCC と VDPin の利便性について比較議論を行う．

1 つ目の指標は認証成功率である．表 2 において CCC と VDPin の認証成功率を確認すると，2 手法の認証成功率に有意差はなかったものの，VDPin の方が認証成功率は高い結果となっている（表 2 内 SR 列参照）．したがって，VDPin は CCC と比較して認証成功率を低下させるような操作負担が追加されているという指摘はあたらないと考える．

2 つ目の指標は入力位置の通知方法による影響である．VDPin には振動回数が 0，1，2，4 回の 4 パターンが存在するため，振動による入力位置の取得が困難になった可能性がある．その場合，ユーザは「入力位置の再通知ボタン」を押して入力位置取得処理をやり直す必要がある．したがって，入力位置の取得に関する負担増加はこの再通知回数で検証可能といえる．評価実験から，CCC と VDPin それぞれにおいて 10 回の認証試行を行う中で再通知処理を行った平均実施回数は，CCC で 2.36 回，VDPin で 0.91 回となった．また，表 3 の設問 1，2 の結果を見ると，入力位置の取得に関するストレスや集中力度合いの負担も VDPin の方が大きいと回答した参加者は少数である．これらの結果から，入力位置の通知方法の変更により入力位置の取得が困難化したという懸念もあたらないと考える．

最後の指標はダイヤル操作による影響である．VDPin ではタッチバーによる操作方法を新たに導入した．この操作法は認証時間短縮を意図して実装したものだが，副作用として操作負担を増加させている懸念がある．これについて，表 3 の設問 3 から設問 6 の結果を見ると，ストレスや集中力度合いの負担については参加者間でも意見が分かれていることが分かる．つまり一部の実験参加者にとってはタッチバーの導入が操作負担を増加させたと受け止められている．これについて，参加者の 1 人からは「タッチバーはダイヤルを素早く移動できるように感じるが，指のスライド量の加減が難しい」という意見が得られている．タッチバーのインタフェースは，単なる黒塗り領域で示されており，指をどの程度動かせばダイヤルがどの程度回転するのかが把握しにくいといえる．今回の評価実験では，ボタン操作とタッチバー操作で認証時間・認証成功率ともに有意な差は見られなかったが，タッチバーの操作性が改善されれば，認証時間も変化する可能性がある．タッチバーの操作性改善は，今後の課題である．

5.1.3 安全性について

VDPin として導入された改良点は (a) 入力位置通知方法と (b) タッチバーによるダイヤル操作であり，どちらもユーザインタフェースの改良である．これらの改良は認証時間短縮を意図して導入したものであるが，結果的に安全性改善にも貢献している可能性がある．それは，「ユーザによる望ましくない動作」の抑制である．CCC も VDPin も入力位置を通知するためカーソルが既定回数移動するが，いずれも「カーソルが 1 周移動し終わるまで，次の操作を始めてはならない」という暗黙のルールがある．移動完了前にユーザがなんらかの操作を始めてしまうと，「操作開始前までのカーソル移動範囲において入力位置が確定した」ということを攻撃者に知らせてしまうことになるからである．4.2 節の攻撃実験で，1 名の攻撃者が C_{tbr} 条件で暗証番号を 4 桁すべて特定できた原因はこれである．この懸念に対し，VDPin はカーソル移動回数が 4 回であり，振動回数が複数パターン存在するため，最低でもカーソルが 3 つ目の位置に移動するまでは入力位置が確定しない仕組みになっている．したがって，懸念されるような望ましくない動作をユーザが行いにくい仕組みになっているといえる．

5.2 先行研究との比較

VDPin は CCC をベースにユーザインタフェースを改良することで認証時間短縮を実現した．しかし表 1 に目を向けると，振動を用いた覗き見攻撃対策の認証手法には VDPin よりも認証時間が短い手法が 3 つ存在する（TictocPIN，Spinlock，VDA）．本節ではこれらの手法に残されている問題点について言及し，VDPin との比較を行う．

まずはじめに TictocPIN [11] について議論する．この手法は，認証画面に表示される視覚情報とシステム側からユーザに通知される振動情報をチャレンジとし，回答とな

る「色」を導出して回答する手法である．つまり暗証番号を色に変換して回答するのだが，回答候補である色は最大で 4 色であるため，数字を 1 つ入力するために振動パターンの認識と色による回答を 2 回行う必要がある．つまり暗証番号 4 桁を入力するのに 8 回の回答操作が必要であることから，操作負担の問題があるといえる．

次に TictocPIN の安全性に関して述べる．この手法は認証画面の設計により 1 度覗き見攻撃を行うと入力値が 10 種類から 5 種類に絞り込むことができる．したがって 4 桁暗証番号の場合，1 回覗き見攻撃を行うことで，秘密情報の候補数を 625 通り（$= 5^4$）にまで絞り込むことが可能である．また CCC と同様に，ユーザの望ましくない動作により入力値の絞り込みが可能になる懸念がある．振動パターンの通知が完了する前にユーザがなんらかの操作を始めてしまうと，その操作を始める前までのタイミングで回答となる色が確定したことを攻撃者に伝えてしまうことになるからである．

次に Spinlock について議論する．Spinlock の入力操作は次の 3 ステップで行われる．

(Step 1) 画面に表示されている円の円周上を指でなぞる．
(Step 2) なぞり操作の間，一定の制約のもとランダムな間隔で振動が発生する．
(Step 3) その振動の発生回数をユーザが数え上げ，入力したい値と振動回数が同じになったら指を離すことで入力値が確定する．

つまり，入力操作中に発生した振動回数が入力値となる手法である．この手法では，ユーザが振動発生回数を数える必要があること，そしてその回数が入力したい値と同じになったかを判定する必要がある．この 2 つの処理をユーザが脳内で処理する必要がある点で操作負担があるといえる．なお，この入力操作が受け入れ可能なものとはいいがたいことが評価実験におけるリセット率から示されている．リセット率とは入力操作をやり直した割合を示しており，4 桁暗証番号におけるリセット率は 62.3%であった．つまり実験で実施された認証試行のうち半数以上は入力操作のやり直しが必要であったことを示しており，その操作負担は軽視できる程度ではないと考える．

次に Spinlock の安全性について議論する．Spinlock は，入力操作方法がユーザの暗証番号選択に悪影響を与える懸念がある．この手法における入力操作は入力値と相関があるといえる．画面をなぞっている間に発生する振動回数が入力値になるため，入力値が大きい場合はなぞる距離が長くなり，小さい場合はなぞる距離が短くなるからである．振動の発生間隔をランダムにすることで入力値の特定は困難化しているものの，操作状況から推測による入力値の絞り込みは可能である．特に入力値が小さい場合はなぞる距離が短くなることから，その推測精度が高くなることも指摘されている．一方，利用者目線で考えると，操作負担の軽減を狙って小さな値の数字を優先的に選択して暗証番号を作成する懸念がある．そうすることにより，入力時になぞる距離を短くすることができるからである．しかし前述のとおり，このような暗証番号の選択は覗き見攻撃による入力値の推測可能性を高めることになり，結果的に覗き見攻撃に対する安全性を危殆化させる．このように入力操作に由来する安全性の懸念がある．

最後に VDA について議論する．VDA の入力操作は次の 2 ステップで行う．

(Step 1) 3 行 3 列の行列形式に表示された 1 から 9 の数字のうちランダムな 1 つをチャレンジ情報として取得する．
(Step 2) 取得した数字と入力したい値を「加算」し，その値の mod 10 を入力する．

ここで Step1 の処理について詳細を説明する．VDA ではカーソルの表示と振動パターンによってチャレンジをユーザに伝達する．カーソルは，行列内の「行」を覆う形で表示され，行列内の一番上の行から一番下の行まで順に指し示す．カーソルがどこかの行を示しているときに特定の振動パターンが発生する．この振動発生時のカーソルの表示位置がチャレンジとなる値が存在する「行」を，発生する振動のパターンが「列」を示している．この「行」と「列」の 2 情報によりユーザは行列内の特定の数値をチャレンジとして取得できる仕組みである．操作負担としては，システムからランダムな数値を取得したうえでユーザの脳内で加算と mod 10 の計算を行う必要がある．このように，ユーザの脳内でなんらかの処理を行わせ回答値を決定する手法は “mental operation” と呼ばれ，視聴覚情報として観察することは不可能なため覗き見攻撃対策としては効果的である．しかし，安全確保のための処理をユーザに負わせており，操作負担であるといえる．またユーザの教育レベルによっては利用可能性に制約がある手法ともいえる．

次に VDA の安全性について議論する．認証画面の設計から，加算に用いられる数値は 1 から 9 までの 9 種類となっている．したがって，1 回覗き見を行うと，10 種類の値のうち 1 つだけは暗証番号の値でないことが確定する．“0” を加算するという可能性がないため，「ユーザの回答値=暗証番号の値」は起こりえないからである．したがって，同一ユーザの認証行為を繰り返し覗き見することができれば，いずれ暗証番号を特定できることになる．また，VDA もユーザによる望ましくない動作により入力値の絞り込みが可能になる懸念がある．VDA ではカーソルが 3 カ所を移動する際，どこか 1 カ所でのみ振動パターンが発生する．ここで 3 カ所の移動が完了する前にユーザがなんらかの動作を行った場合，振動が発生した場所を攻撃者に特定される可能性がある．それは結果的に入力値を 3 つに絞り込めることにつながる．このことから覗き見攻撃についても一定のリスクが存在するといえる．さらに，操作負

担を軽減するため，ユーザによる暗証番号の選択が以下のように偏る懸念がある．

- “0” を暗証番号に多用する懸念
- 小さな値の数字（1, 2 等）だけで暗証番号を作成する懸念

これらの値を暗証番号に選択する可能性が高い理由は，回答時に必要となる計算を簡単化するためである．暗証番号の値が “0” の場合，加算および mod 10 の計算が不要になり，システム側が通知する数字をそのまま回答として選択するだけになる．また小さな数字を使う理由も同じである．たとえば，暗証番号の値が “1” だとすればシステムが通知する値が何であれ，加算処理が簡単になることは理解できるだろう．このように入力操作がユーザの暗証番号選択に悪影響を与え，結果として覗き見攻撃以外の他の攻撃方法に対する安全性が危殆化する懸念がある．

これまでの議論をまとめると，TictocPIN，Spinlock，VDA の 3 手法は VDPin よりも認証時間は短い一方で利便性または安全性について以下のような問題があることが明らかになった．

S1：操作負担の増加（Mental operation を含む）
S2：1 回の覗き見攻撃による入力値絞り込みの可能性
S3：複数回の覗き見攻撃による入力値絞り込みの可能性
S4：ユーザの望ましくない行為による入力値絞り込みの可能性
S5：入力操作に起因するユーザの暗証番号選択への悪影響

ここまでの議論から，TictocPIN・Spinlock・VDA・VDPin の 4 手法と上記の 5 つの問題点との関係を**表 5** に示す．なお，表 5 において VDA の S2，S3 が括弧書きになっている理由は，VDA ではチャレンジの数字として 10 種類目を伝達する方法（たとえば，VDPin のように「1 度も振動しない」等）を追加した場合，この問題点に該当しなくなるからである．

VDPin はこれら 5 つの問題のうち，S4 を除く 4 つの問題は該当しないという特徴を持つ．「ダイヤル操作」以外に操作負担はなく，回答入力のためになんらかの計算や振動発生回数の数え上げ，そして数字以外の別の回答値を導出するといった処理を行わないと回答値が得られないということはない．また認証画面と入力操作から入力値の特定または絞り込みを可能にする情報の漏洩はなく，覗き見攻撃によって総あたり攻撃に必要な攻撃回数を減少させる要素もない．また入力位置もシステムによってランダムに決定されるため，繰り返し覗き見を行っても，入力値が絞り込まれる可能性もない．また入力操作は暗証番号の値と独立していることから，提案するユーザインタフェースが暗証番号の選択に悪影響を及ぼす懸念もない．

表 5 録画攻撃対策手法の問題点比較
Table 5 Comparison of the remained issues in the VDPin and prior works.

認証手法	S1	S2	S3	S4	S5
TictocPIN	○	○		○	
Spinlock	○	○	○		○
VDA	○	(○)	(○)	○	○
VDPin				○	

一方，S4 は TictocPIN や VDA に存在している懸念だが，VDPin についても同様の懸念はある．このリスクが最大限効果を発揮した場合，1 回の覗き見攻撃で VDA は入力値が 3 つに絞り込まれ，TictocPIN は入力値が特定される可能性がある．これに対して VDPin は，振動パターンに複数のバリエーションがあるため，カーソルが 3 つ目の位置に移動するまで入力位置は確定しない．したがってカーソルが 3 つ目の位置に移動するまで，ユーザが望ましくない動作を行う可能性は少なく，そういった行為を抑制できると考える．またカーソルが 3 つ目の位置にあるときにユーザが望ましくない動作を行ったとしても，入力位置の候補は 4 つ[*1]あり，他の手法よりも絞り込みにより残る候補数は多い手法となっている．したがってこのリスクによる安全性への懸念は TictocPIN や VDA よりも小さい手法だといえる．

5.3 今後の課題

今後の課題はシステム改良と評価実験の再実施である．その目的は 3 つある．

1 つ目は，提案手法に関する普遍的な評価結果を得るためである．本論文で報告している実験は，いずれも 20 代男性という特定の属性を持つ参加者のみで実施している．したがって，その実験結果は提案手法の可能性を示したにすぎないといえる．操作性については，多様な属性を持つ実験参加者を募集したうえで，あらためて評価を行うべきであると考えている．安全性についても同様であり，被害者役の人数を増やすとともに，特定被害者に対する複数回の覗き見攻撃という脅威についても攻撃実験を行い，提案手法の安全性を再検証する必要があると考えている．

2 つ目は，システム改良による操作性・安全性への影響に関する再評価である．5.1.2 項で述べたとおり，タッチバーには改良の余地がある．スクロールバーと同等のインタフェースにする，タッチバーの視覚的表示を「黒塗り四角形」から別のものに改良し指の移動量とダイヤル回転量の関係を理解しやすくする等の改良を行い，その改良による操作性と安全性への影響についてあらためて評価を実施する．

最後は，先行研究と提案手法に関するユーザの操作負担

[*1] (1) カーソル “上·右” で振動 → 図 1 右の入力位置 “2”．(2) “右” のみで振動 → 入力位置 “3”．(3) “右・下” で振動 → 入力位置 “4”．(4) “上・右・下” で振動 → 入力位置 “9”（入力位置 “9” は 4 方向すべてで振動する場合だが，“上・右・下” で振動した時点で 4 方向すべてで振動するパターンであることが確定するため）．

の比較検証である．これは 5.2 節で述べた 5 つの問題点のうち「S1：操作負担の増加」に関する検証を意味する．この評価はセキュリティとユーザビリティを議論するうえで重要だと考える．その理由は，録画攻撃に対する安全性と短い認証時間や高い認証成功率を実現することが示されたとしても，それがユーザに対して大きな操作負担を強いた結果であるならば，ユーザにとって真に望ましい対策手法とはいいがたいと考えるからである．特に覗き見攻撃対策の個人認証手法は，視覚情報から暗証番号を特定困難にするため，ユーザに Mental operation を操作の一部として課す手法が少なくないことは前節で述べたとおりである．ユーザに要求される操作負担について実験参加者の協力のもと評価を行い，録画攻撃に対する安全性評価・認証時間や認証成功率といった定量的評価に加え，それらだけでは明らかにならないユーザの操作負担評価の 3 軸で比較考察を行うことで覗き見攻撃対策手法としての評価を試みる．

6. おわりに

個人認証における覗き見攻撃は，今も現実の脅威として存在する問題である．特に録画機器による覗き見攻撃は，今後大きな脅威になると考え本論文における想定脅威とした．この問題に対し，実用性の観点で先行研究を調査した．本論文では「利用シーンの制約が小さいこと」と「個人認証にかかる時間が短いこと」の 2 点を実用性の評価軸とした．調査の結果，利用シーンの制約が小さい「振動」を用いた手法に着目したが，この手法には認証時間が長いという問題が残されていた．

そこで本研究では，振動を用いた先行研究の 1 つである “CCC [8]” のユーザインタフェースを改良することで認証時間の短縮を可能にする録画攻撃対策手法 “VDPin” を提案した．VDPin では認証時間を短縮するため，入力位置を取得するための処理を変更し，また入力用ダイヤルの操作方法としてタッチバーと呼ぶ操作方法を導入した．

VDPin ならびに CCC を Android アプリケーションとして実装し，操作性と録画攻撃に対する安全性について，評価実験を実施した．その結果，改良前の手法である CCC と比較し，録画攻撃に対する安全性を維持しつつも，約 6 秒の認証時間短縮を実現した．また振動を用いた覗き見攻撃対策の個人認証について考えられる問題点を整理し，先行研究と VDPin についてそれらの問題点を比較議論することで，VDPin が一番問題点の少ない手法であることを明らかにした．

参考文献

[1] Bianchi, A., Oakley, I., Kostakos, V. and Kwon, D.S.: The phone lock: Audio and haptic shoulder-surfing resistant PIN entry methods for mobile devices, *Proc. 5th International Conference on Tangible, Embedded, and Embodied Interaction* (*TEI '11*), pp.197–200, Association for Computing Machinery (2010).

[2] Bianchi, A., Oakley, I., Kwon, D.-S.: Spinlock: A Single-Cue Haptic and Audio PIN Input Technique for Authentication, *Proc. 6th International Conference on Haptic and Audio Interaction Design* (*HAID '11*), pp.81–90 (2011).

[3] Chakraborty, N., Anand, S.V., Randhawa, G.S. and Mondal, S.: On Designing Leakage-Resilient Vibration Based Authentication Techniques, *2016 IEEE Trustcom/BigDataSE/ISPA*, pp.1875–1881 (2016),

[4] Guixin, Y., Tang, Z., Fang, D., Chen, X., Kim, K.I., Taylor, B. and Wang, Z.: Cracking Android Pattern Lock in Five Attempts, *NDSS* (2017).

[5] Harbach, M., De Luca, A. and Egelman, S.: The Anatomy of Smartphone Unlocking: A Field Study of Android Lock Screens, *Proc. 2016 CHI Conference on Human Factors in Computing Systems* (*CHI '16*), pp.4806–4817, ACM (2016).

[6] Higashiyama, Y., Yanai, N., Okamura, S. and Fujiwara, T.: Revisiting Authentication with Shoulder-Surfing Resistance for Smartphones, *2015 3rd International Symposium on Computing and Networking* (*CANDAR*), pp.89–95, DOI: 10.1109/CANDAR.2015.107 (2015).

[7] Hirakawa, Y., Hirose, F. and Sasano, I.: PVRotate: An Improved Vibration-Based User Authentication Method, *International Journal of Future Computer and Communication*, Vol.8, No.2, pp.50–54 (2019).

[8] 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).

[9] 近藤 潤，平野 学，神谷直希：音声入力と相対値入力による覗き見に強い認証方式の提案，FIT2011（第 10 回情報科学技術フォーラム）論文誌，Vol.4, pp.33–38 (2011).

[10] Kuribara, T., Shizuki, B. and Tanaka, J.: Vibrainput: Two-step PIN entry system based on vibration and visual information, *CHI '14 Extended Abstracts on Human Factors in Computing Systems* (*CHI EA '14*), pp.2473–2478 (2014).

[11] Kwon, T. and Hong, J.: Analysis and Improvement of a PIN-Entry Method Resilient to Shoulder-Surfing and Recording Attacks, *IEEE Trans. Information Forensics and Security*, Vol.10, No.2, pp.278–292, DOI: 10.1109/TIFS.2014.2374352 (2015).

[12] Lee, M.-K., Kim, J.B. and Franklin, M.K.: Enhancing the Security of Personal Identification Numbers with Three-Dimensional Displays, *Mobile Information Systems 2016* (2016).

[13] Perkovic, T., Cagalj, M. and Rakic, N.: SSSL: Shoulder Surfing Safe Login, *SoftCOM 2009 – 17th International Conference on Software, Telecommunications & Computer Networks*, pp.270–275 (2009).

[14] Shukla, D., Kumar, R., Serwadda, A. and Phoha, V.V.: Beware, Your Hands Reveal Your Secrets!, *Proc. 2014 ACM SIGSAC Conference on Computer and Communications Security* (*CCS '14*), pp.904–917, ACM (2014).

[15] Winkler, C., Gugenheimer, J., De Luca, A., Haas, G., Speidel, P., Dobbelstein, D. and Rukzio, E.: Glass Unlock: Enhancing Security of Smartphone Unlocking through Leveraging a Private Near-eye Display, *Proc. 33rd Annual ACM Conference on Human Factors in Computing Systems* (*CHI '15*), pp.1407–1410 (2015).

推薦文

本論文は提案する認識方式，先行研究の調査，提案方式

の改良点等，丁寧に構成されている．ラボテストの実験で評価しているが，その内容には信頼性がある．以上より，論文誌への掲載に値する論文として推薦する．

（コンピュータセキュリティシンポジウム 2020
プログラム委員長　森 達哉）

江原 知志

1997 年生．2020 年電気通信大学情報理工学域卒業．2022 年 1 月現在，電気通信大学大学院情報理工学研究科在学中．在学中は個人認証の覗き見攻撃対策の研究に従事．ユーザブルセキュリティに関心がある．

高田 哲司 （正会員）

2000 年電気通信大学大学院情報システム学研究科情報システム運用学専攻博士後期課程修了．博士（工学）．2003 年ソニーコンピュータサイエンス研究所研究員．2005 年独立行政法人産業技術総合研究所情報技術研究部門研究員．2010 年電気通信大学大学院情報理工学研究科准教授．現在に至る．ユーザブルセキュリティ，個人認証，情報視覚化に興味を持つ．IEEE-CS 会員．