情報処理学会論文誌 Vol.56 No.9 1877–1888 (Sep. 2015)

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

石塚 正也[1] 高田 哲司[1,a)]

受付日 2014年12月4日, 採録日 2015年6月5日

概要：携帯端末で個人認証を行う利用者にとって覗き見攻撃は現実的な脅威の 1 つである．この脅威に対する既存の対策方法は，入力操作や画面を隠すというほかにいくつかの提案がなされているが，それらの提案手法には入力手法の複雑化や学習負荷，秘密情報の増加にともなう記憶負担の増大，専用デバイスが別途必要などの問題がある．これに対して本論文では，現時点において入手可能なスマートフォンで暗証番号認証を行うことを想定し，スマートフォンの振動機能を応用することで覗き見攻撃への安全性を向上させうる暗証番号入力手法 CCC（Circle Chameleon Cursor）を考案した．振動機能の利用により，CCC は視覚的情報による秘密情報の特定を困難にしつつ，認証操作時における認証端末と利用者間での秘密情報共有を可能にする．またその共有秘密を既存のダイヤルによる暗証番号入力操作に応用することにより，最小限の学習負担と記憶負担増加量ならびに別途専用デバイスは不要という利点を持つ入力手法となっている．このアイデアを基に Android スマートフォンアプリとしてプロトタイプを実装し，被験者による攻撃実験を実施した．その結果，3 つの利用状況において認証操作を録画した動画記録から入力値を正しく特定できた被験者は 0 人という結果を得た．

キーワード：覗き見攻撃，録画攻撃，ショルダサーフィン，携帯端末，個人認証，振動，インタフェースデザイン，操作負荷

CCC: Repeated Observaton Attack Resilient PIN Authentication System Using Vibration

Masaya Ishizuka[1] Tetsuji Takada[1,a)]

Received: December 4, 2014, Accepted: June 5, 2015

Abstract: In this paper, we proposed simple yet secure Personal Idenfication Number (PIN) authentication scheme against observation attack for mobile devices. An observation attack (also known as a shoulder surfing attack) is an actual threat for mobile phone users. Some research works propose secure schemes against this sort of attack. However, these schemes have remained issues such as a complex input method, memory load increase for an additional secret and required a dedicated device. Our scheme, named Circle Chameleon Cursor, focuses on improving the issues of a PIN input scheme for a smart phone. The features of the proposed scheme as follows: 1) We use two secrets and the second secret is shared using a simple vibration signal between a mobile phone and a user. It makes hard to retrieve an input value even if an attack has some movie records about both a screen and a user operation. 2) CCC does not increase a memory load of a secret when a user does not use a PIN authentication. And 3) CCC does not require an additional dedicated device. We implemented a prototype system on an Android smart phone and conducted an observation attack experiment using some movie records of an authentication operation of the system. The result was that no one succeeded to identify an input value correctly.

Keywords: shoulder surfing attack, camera recording attack, social hacking, mobile device, user authentication, PIN, vibration, interface design, operation load

1. はじめに

覗き見攻撃は個人認証における現実的脅威の 1 つであ

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

る．銀行 ATM やゴルフ場ロッカにおいて暗証番号が覗き見され，それにより発生する金銭被害はよく知られている犯罪事例である [1]．

しかしこの脅威は，次に述べる 2 つの技術的変化によりさらに拡大すると想定される．

(1) 個人認証を行う場面の多様化
携帯電話の普及により様々なサービスを携帯電話を通じて利用するようになった．それにともない個人認証も携帯電話を通じて行うことになる．しかし携帯電話は利用者が常時携帯し，必要に応じて使用するため利用場面が多様化する．その場面には，満員電車の中など安全に個人認証を行うには適切とはいいがたい場所もありうる．これは結果として覗き見攻撃に遭遇する可能性を高めることになる．

(2) 動画撮影機器の小型化と普及
動画撮影機器は小型化が進み，今やペンやネクタイピンに装備することやレターケースなどに隠すことも可能である [2]．また最近の携帯電話やウェアラブルデバイスにも動画撮影機能が搭載されており，自分の知らぬところで周囲の端末利用者が動画撮影をしていることもあるだろう．一方，防犯目的のため街中に監視カメラの設置も進んでおり，様々な場所や方法で動画撮影が行われる社会になりつつある．したがって自分が撮影されていることに気づかぬまま個人認証を行ってしまう状況も十分に起こりうるといえる．

これらの想定から，覗き見攻撃は悪意ある第三者が故意に認証操作を覗き見て秘密情報を窃取し，悪用するだけでなく，悪意がないまま個人認証シーンが撮影され，その録画記録を見た第三者が入力値を特定してしまい，結果として悪用してしまうという可能性も十分起こりうる状況になりつつある．

したがって携帯端末で行う個人認証は覗き見攻撃に対して安全性が確保されるべきである．しかしながら携帯端末で現在利用可能な個人認証 3 手法（暗証番号，パスワード，パターンロック）はどれも秘密情報を直接入力するため，覗き見攻撃に対する安全性は確保されていない．よって本研究では，携帯端末での暗証番号認証を想定し，覗き見攻撃への安全性を向上させうる個人認証手法を提案する．

以降，本論文では 2 章で既存研究と想定脅威について述べ，3 章で提案システム CCC の基本アイデアとプロトタイプシステムについて説明する．4 章では被験者による提案手法の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や今後の課題について述べ，6 章でまとめを述べる．

2. 関連研究と想定脅威

本章では個人認証における覗き見攻撃を対象とした既存研究を紹介する．それと同時に既存手法に残されている問題点を整理し，本論文で想定する脅威モデルを明確化する．

2.1 覗き見攻撃対策に関する関連研究

EyePIN [3] は視線入力装置を利用し，視線によるジェスチャとして数字を描くことで秘密情報を入力する方法である．問題点は視線入力装置が必要となる点と，目の動きが録画できれば入力値が特定されうる点である．

VibraPass [4] は，秘密情報入力時に偽回答を混入させることで覗き見攻撃に対する安全性を向上させる手法である．銀行 ATM での利用を想定し，暗証番号入力前に利用者の携帯端末と銀行 ATM をペアリングする．暗証番号入力を開始するとランダムに決定される桁の入力時に携帯端末が振動する．携帯端末が振動した際，利用者は意図的に暗証番号ではない数字を入力する．この仕組みにより入力値が認証試行ごとに変化するため，覗き見攻撃への安全性が向上する手法である．問題点は認証機器とは別のペアリング用端末を必要とし，またペアリング処理も必要となる．また偽回答は「正解以外」を回答とするため正解となる確率が高くなる．したがって偽回答なしの場合と同一程度の理論的安全性を確保するためには秘密情報を増やす必要があり，記憶負担が増えることになる．

Back-of-Device Shapes（BoDS）[5] は，Android のパターンロックと同様にストロークを秘密情報として入力する認証手法である．特徴的な点は，スマートフォンの背面側に備えられた入力装置で事前に決定しておいたストローク形状を入力する点である．問題点は 2 点ある．1 つは背面からはいうに及ばず，端末前面から入力行為を録画されたとしても秘密情報が特定される懸念があることであり，もう 1 つは 2014 年 11 月現在，端末背面側でのストロークの入力操作が可能な携帯端末は限られるため，提案手法のメリットを享受できる利用者は限定される点にある．

喜多らの方式 [6] は，6×6 のマスの中からパスワードとなる英数字を探し，振動機能で入力する文字を変化させる方式である．問題点は，カメラ録画攻撃により認証行為複数回分の記録が窃取されると秘密情報が特定される可能性がある点と，記憶負担が増える点，そして記憶情報と画面提示情報から正解選択肢を導出する処理が必要となる点である．

Undercover [7] は，認証画面に表示された画像群から正解となる画像を認識するとともに，トラックボールの回転方向または振動を感知し，それらの情報を組み合わせて得られる正解回答ボタンを押すことで回答入力を行う認証手法である．問題点は，認証に必要な情報提示のためにトラックボールが必要となる点と，正解回答を得るために視覚情報と触知情報を組み合わせ最終的な回答を導出する処理が必要となる点である．

fakePointer [8] は，既定の暗証番号とランダムに生成された値を組み合わせて入力値を確定させる認証手法である．問題点は，ランダムに生成される第 2 の秘密情報を利用者と認証システム間で共有するために別の安全な通信路

が必要となる点である．

Phone Lock [9] は，各入力マスに割り当てられている数値を，視覚情報でなく振動パターンで伝達することで覗き見攻撃に対する安全性を向上させる手法である．問題点は，振動パターンと数値の対応表を利用者が記憶する必要があり，記憶負担が増える点である．またどの数値がどのマスに割り当てられているかが不明なため，触知により回答マスを探索する操作も必要となる．

Spinlock [10] は，携帯端末から発せられる振動情報の感知回数を暗証番号の数字として入力する認証手法である．問題点は，入力操作のあいだ振動信号を何回感知したかを利用者が数える必要がある点と，認証行為を多数回攻撃者に録画された場合，入力値が特定される懸念がある点である．また Bianchi らは文献 [11] で不可視なパスワード認証における設計指針について議論を行っている．

このほかに画像を応用した個人認証における覗き見攻撃対策も提案されている [12], [13]．これらの手法は，認証時に提示する画像を不鮮明化する処理を施すことで覗き見攻撃に対する安全性向上を提案している．

なお個人認証ではないが機密情報を第三者に漏洩させずに入力する方法として桜井らの手法 [14] がある．この手法はダイヤル操作を模して間接的に情報入力する方法となっている．問題点は，1 文字あたりの入力操作が増えることと，入力操作を多数回攻撃者に録画された場合，入力値が特定される可能性がある点である．また入力文字 1 つあたりの回答回数を増やすことによって覗き見攻撃への安全性を向上させる方法としては Roth らの研究 [15] もあるが，この手法も録画記録による攻撃に対して安全ではないという問題がある．

2.2 想定する脅威モデル

前節で覗き見攻撃に対する関連研究を紹介した．本節ではこれらの既存研究を総括し，残されている問題点と本研究で改善を目指すべき脅威モデルを明確にする．**表 1** は，前節で紹介された既存研究の比較である．比較基準は以下の 4 点である．

(1) 認証端末のほかに別途装置が必要か？
(2) 認証場面 1 回分の録画記録があっても入力値の特定が困難か？
(3) 認証場面複数回分の録画記録があっても入力値の特定が困難か？
(4) 記憶負担が増加しないか？

なお上記項目における「認証場面」とは，認証端末の画面表示と利用者による入力操作の双方を含む視覚的情報と定義する．記憶負担の増加とは，暗証番号認証であれば暗証番号以外に記憶すべき情報があるかで判断する．

この比較結果から，既存研究には 3 つの問題点が残されているといえる．

- 複数回分の録画記録による覗き見攻撃に対する安全性が確保できない．
- 認証端末のほかに別装置が必要．
- 記憶負担の増加．

これに対し，1 章での議論から技術の進歩や機器の普及を考えると，以下のようなストーリで特定ユーザの認証行為が複数回録画される可能性は考えられる．

Case 1：いつも同じ場所で認証操作を行っていたが，そこに監視カメラがあることに気づいていなかった．
Case 2：同僚のそばでいつも認証操作を行っていたが，その同僚のメガネに録画機能があった．

認証操作の録画記録が 1 つの場合と複数の場合における脅威は大きく異なる．理由は，録画データ数が増えるに従い秘密情報の正解候補が絞り込まれ，最終的にある数の録画データが得られれば秘密情報が一意に特定可能になることがあるからである．これは Intersection 攻撃とも呼ばれている．また携帯端末のほかに別途装置が必要になるということは，個人認証における安全性改善手法の普及を妨げることになる．携帯端末利用者にとって，個人認証は安全にオンラインサービスや端末を利用するためのコストであり，利用者における本来の利用目的ではない．したがって別途装置が必要な認証手法を携帯端末の利用者が受け入れる可能性は低いと考える．記憶負担の増大についても同様だといえる．

したがって本論文における想定脅威モデルは「認証端末の画面情報と入力操作がカメラにより録画され，かつ同一利用者による複数回分の認証操作にかかわる録画記録が攻撃者に窃取された」という状況を想定する．この状況においても利用者が入力した秘密情報の特定を困難にする手法の実現を目指す．またこの安全性要件の実現において，提案手法の普及を阻害する要因を可能な限り排除するため，認証端末以外の装置を必要とせず，また必要最小限の記憶負担増加にすることも目標とする．

表 1 認証システムの比較表
Table 1 Remained issues in proposed systems.

方式	別装置	一回録画	多数回録画	記憶負担
EyePIN	必要	×	×	
BoDS	必要*1	×	×	
VibraPass	必要*2	○	×	増加
喜多ら		○	×	増加
Spinlock		○	×	
fakePointer	必要	○	○	増加
Undercover	必要	○	○	
Phone Lock		○	○	増加

*1 現在背面でストローク入力可能な端末は限定されるため．
*2 ATM とペアリングする携帯端末が必要なため．

3. CCC: Circle Chameleon Cursor

3.1 基本コンセプト

2.2 節で述べた脅威モデルに対する安全性向上策について，金庫の暗証番号入力つまみを例にして説明する．金庫の入力つまみは，つまみの上方に入力値を指し示すための箇所（以後カーソルと述べる）が 1 つだけ存在する（図 1）．したがってダイヤル操作を覗き見し，カーソルで指し示す数字を見ていれば暗証番号は誰でも特定可能である．

そこで CCC では以下の 2 つの工夫により，ダイヤル操作による入力値の特定を困難にする．

1) カーソルの位置をランダムに決定．
2) カーソルを視覚的に表示しない．

図 2 がその概念図である．図 2 ではダイヤル内のすべての数字にカーソルがあるが，この中のうちどれか 1 つだけが正しいカーソルとなる．このカーソル位置は数値入力のたびに認証システムによりランダムに決定される．また図中では説明のためカーソルが視認可能だが，実際には非表示とする．これにより第三者にダイヤル操作を覗き見されてもどの位置がカーソルなのかが分からず暗証番号の特定は困難になる．

一方，正規利用者もカーソル位置が不明なため暗証番号の入力ができない．したがって認証システムは利用者とカーソル位置を共有する必要がある．その一方法として，暗証番号入力用のカーソル位置を暗証番号と一緒に秘密情報として記憶しておく方法が考えられるが，これは 2 つの点で問題がある．1 つは暗証番号のほかに “カーソル位置” 情報を記憶する必要があるため記憶負担が増える点である．もう 1 つは Replay 攻撃が可能になるという点である．カーソル位置を記憶可能にするということは，カーソル位置を固定するということになる．すると正規利用者が行うダイヤル操作はつねに同一操作になり，暗証番号の特定には至らないものの，攻撃者が同じダイヤル操作を行えば認証を通過することが可能となってしまう．

そこで CCC では事前にカーソル位置を決定し記憶するのではなく，認証時にカーソル位置をシステムが決定し，認証利用者に通知する．その通知方法として認証画面と入力操作を録画されても，第三者によるカーソル位置の特定を困難にするため振動機能を利用する．この方法により以下の 3 つの利点が得られることになる．

(1) 記憶負担が増えない．
(2) 録画による覗き見攻撃にも安全．
(3) 別装置が不要[*3]．

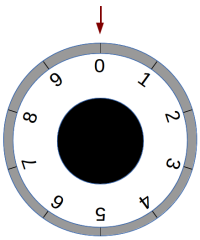

図 1 通常の金庫ダイヤル
Fig. 1 Conventional number input dial.

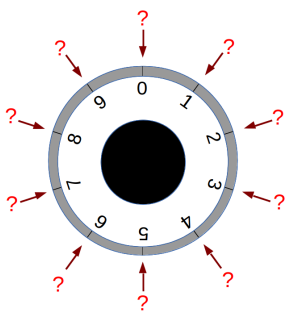

図 2 提案方式のイメージ
Fig. 2 A novel number input dial concept in our proposal.

3.2 プロトタイプと認証方法

前節のアイデアを基にした 4 桁暗証番号による CCC のプロトタイプを実装した．本節では本プロトタイプシステムの実装と操作方法について説明する．図 3 はプロトタイプシステムのユーザインタフェース画面である．インタフェース画面は大きく 3 つの部分から構成される．画面上部から，入力状況のインジケータ，暗証番号入力用つまみ，入力操作用のボタン群である．また暗証番号入力用つまみには，番号入力用カーソル位置を利用者に伝達するために使用するインジケータが用意されている．暗証番号入力つまみの数字の “5” の位置が黒く塗りつぶされているが，これがインジケータである．

次に入力方法について説明する．以降では数字 1 つの入力にかかわる説明である．実際には，暗証番号の桁数回この入力操作を繰り返す．入力操作は以下の 2 手順からなる．

手順 1：カーソル位置の認識

認証を開始すると図 4 のようにインジケータが暗証番号入力用つまみ内で回転する．インジケータがつまみ上の特

図 3 認証画面の全体像
Fig. 3 A screen snapshot of CCC's user interface.

[*3] 既存のスマートフォンでも利用可能．

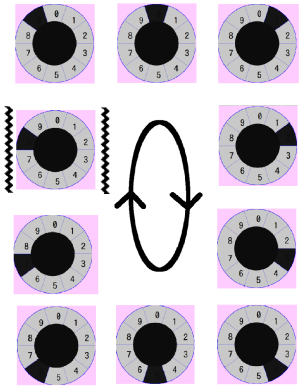

図 4 認証中の画面の推移
Fig. 4 Indicator rotation and vibration for sharing a number input position.

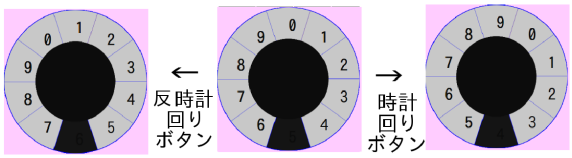

図 5 表示されている数字の移動方法
Fig. 5 Rotating dial operation by buttons.

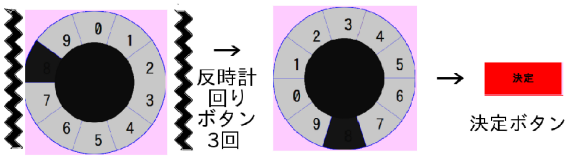

図 6 “1” の入力方法
Fig. 6 An input scheme of the number “1”.

定の数字マスに到達すると端末が振動する．つまりインジケータがつまみを 1 周すると，どこかの数字マスで必ず振動する．その数字マスが番号入力用カーソル位置となる．なお，カーソル位置は CCC がランダムに決定する．振動形態はパルス状の単振動信号である．

手順 2：数字入力

手順 1 で取得した入力用カーソルを使って暗証番号を入力する．入力用カーソル位置に入力したい数字が表示されるように，暗証番号入力用つまみを回転させる（**図 5**）．つまみの回転には画面下部の “時計回り” または “反時計回り” ボタンを使用する（図 3）．入力用つまみを直接触って回転させる操作を許容せずボタン操作にした理由は，被験者がつまみ操作時に指で暗証番号を指し示してしまう懸念があるためである．

入力つまみの回転操作によりカーソル位置に入力したい数字を移動させたら画面下部の “決定” ボタンを押下する．これにより入力値が確定する．入力値が確定したら入力状況インジケータの表示が更新される．

図 6 は入力方法の一例を示したものである．図中左の画面はインジケータが “8” キーの位置に来たときに端末が振動したことを示している．つまり，このキーの位置が番号入力用カーソル位置ということである．ここで利用者が次に入力したい番号が “1” だとする．この場合，現在 “8” キーがある位置に “1” キーを移動させる必要がある．そのために “反時計回り” ボタンを 3 回押下し，“1” キーが希望する位置になるようつまみを回転させる．この状態で “決定” ボタンを押す．これにより “1” がシステムに入力される．

上記の操作を繰り返し，必要桁数分の数値が入力されたら検証処理が行われる．入力された数値と既定の暗証番号が同一であれば認証成功となる．検証処理が終了すると認証結果画面が表示され，その画面内には認証成否と認証時間が提示される．

入力のやり直し：

暗証番号の入力途中で入力ミスに気付いた場合，入力値の破棄と再入力が可能である．画面左下にある “一字消す” ボタンを押下すると，すでに入力された数値のうち最後に入力された数値が破棄され，入力状況インジケータの表示も更新される．その後は前述の手順 1 に戻って入力操作をやり直すことができる．

表 2 数字キーの操作と操作ボタンラベルの関係
Table 2 Button labels for number rotation in two key layouts.

円形つまみ（Cpad）	テンキー配列（Npad）
時計回り	右シフト
反時計回り	左シフト

3.3 キー配置の影響について

3.2 節で説明したプロトタイプは金庫のつまみを模したユーザインタフェースであった．暗証番号の入力インタフェースとして代表的なものにはダイヤル形状のほかにテンキー配列もある．そこで提案手法におけるユーザインタフェースの見た目上の差による影響を検証するため，テンキー配列によるプロトタイプも実装した．

円形つまみによるユーザインタフェースとの差は 2 点ある．1 つは数字キーの配置をテンキー配列にしている点である．もう 1 つは，つまみの回転ボタンを時計回り/反時計回りのかわりに右シフト/左シフトとした点である．テンキー配列における数字キーの移動は原理的にダイヤル状のときと同様である．つまり数字キーはその数値の順に円環状に接続されていると仮定し，それをボタン操作で回転させることで希望するキー位置に希望する数値を移動可能にする．その際，見た目上はキー配置が円形ではないため，操作用ボタンの文字ラベルを右シフト，左シフトに変更した．ダイヤル状 UI との対応表は**表 2** のとおりである．

これらのボタンラベルは行単位で数字キーを見た際，各ボタンを押下することで数字キーがどう移動するかを基にしている．数字キーは値の順に円環になっていると仮定しているため，**図 7** の状態で右シフトボタンを押下すると

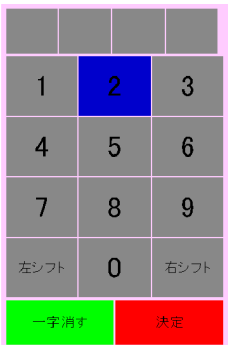

図 7 テンキー配列によるユーザインタフェース画面
Fig. 7 CCC's user interface in the numeric keypad layout.

"0" キーは "1" キーの場所に，"1" キーは "2" キーの場所に移動する．図 7 の状態で左シフトボタンを押下すると "0" キーは "9" キーの場所に移動することになる．なお以降では，ダイヤル状プロトタイプシステムを Cpad，テンキー配列によるプロトタイプシステムを Npad と呼ぶことにする．

4. 評価実験

提案手法の安全性と利便性について被験者による評価実験を行った．本章では評価実験の内容とその結果について述べる．

4.1 利用可能性に関する評価実験

CCC における操作法が利用者に過度の負担を課する手法でないことと，入力インタフェースの形状や振動による携帯端末から利用者へのカーソル位置伝達に関するシステムの設定条件について最適な値を探るため被験者による評価を行った．

実験で使用するシステムは 3.2 節で述べたプロトタイプシステムであり，HTML+JavaScript で実装したプロトタイプシステムを Apache Cordova により Android アプリケーション化したものを使用した．実験に使用したハードウェアは京セラ製 Android スマートフォン KYY04 で，画面サイズは 4.0 インチ，筐体サイズは 125 × 64 × 10.8 mm，端末重量は 140 g である．暗証番号入力インタフェースはダイヤル状インタフェース（Cpad）とテンキー配列型インタフェース（Npad）の 2 種類を用い，ユーザインタフェースの形状差による影響の有無に関する検証も行った．

4.1.1 実験手順

実験手順は以下のとおりである．

(1) システムの説明と操作練習
提案する認証システムについての説明を行い，練習目的のため各々のインタフェースで 2 回ずつ合計 4 回ほど認証操作を実施させた．

(2) 暗証番号決定
4 桁の暗証番号を被験者に自由に決定させた．

表 3 被験者の構成情報
Table 3 Demographic information of subjects.

	20 代	30 代	40 代	50 代
男性	9	1	0	1
女性	3	0	0	1
スマートフォンユーザ	10	1	0	1

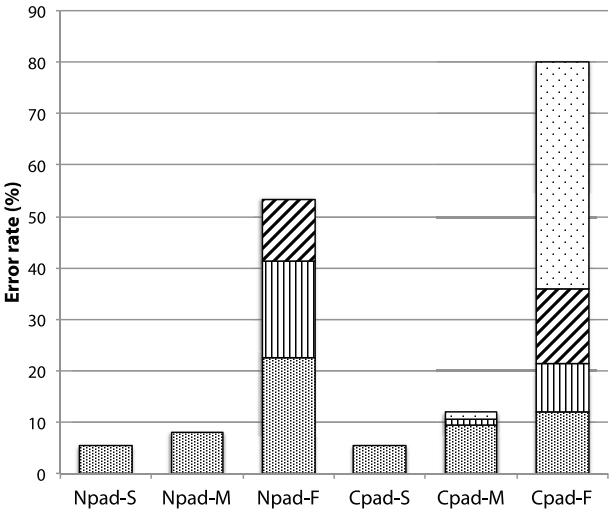

図 8 認証エラー率
Fig. 8 Error rates of CCC in six UI conditions.

(3) 認証操作実験
各被験者に対して，6 条件でそれぞれ 5 回ずつ，合計 30 回の認証操作を実施させた．6 条件とは，2 種類のユーザインタフェース形状と 3 条件のカーソル位置伝達用インジケータの移動速度によるものである．インジケータの移動速度は高速なものから順に 150 ms（Fast），300 ms（Medium），450 ms（Slow）を用意した．これらの時間値は，インジケータの移動間隔時間を示したものである．本実験では，これら 6 条件において最も入力エラーが少なく，かつ操作時間が短くなる条件を実験により明らかにする．本実験では，入力値（4 桁数値），認証結果（成功/失敗），認証時間を測定した．なお 6 条件による認証操作の実施順序は，学習効果による偏りが発生しないように配慮して実施した．

(4) 事後アンケート調査
提案手法に対する被験者の主観的負荷を，NASA-TLX（NASA Task Load Index）テストを用いて測定した．

被験者は 15 名で年齢性別に関する情報は**表 3** のとおりである．なお 15 名中 12 名はスマートフォン利用者であり，被験者全員が高等教育を受けているか，修了している人であった．

4.1.2 実験結果

図 8 と**表 4** に認証エラーに関する実験結果を示す．

図 8 の横軸ラベルは（ユーザインタフェース形状）-（インジケータ速度）の組合せとなっている．インジケータ速度は 150 ms を F（Fast），300 ms を M（Medium），450 ms

表 4 認証エラー回数
Table 4 The number of error times in six conditions.

	Npad-S	Npad-M	Npad-F	Cpad-S	Cpad-M	Cpad-F
# of errors	4	6	40	4	9	60
# of 4 digits error	0	0	0	0	1	33
# of 3 digits error	0	0	9	0	0	11
# of 2 digits error	0	0	14	0	1	7
# of 1 digit error	4	6	17	4	7	9

表 5 認証時間
Table 5 Average, S.D., median, and minimum operation time of CCC.

	Npad-S	Npad-M	Npad-F	Cpad-S	Cpad-M	Cpad-F
平均値（s）	45.33	37.74	41.57	42.43	36.41	41.46
標準偏差（s）	18.06	11.21	8.62	16.67	14.88	12.61
中央値（s）	38.77	34.66	40.27	37.92	31.77	40.49
最小値（s）	24.95	22.02	28.72	25.71	22.33	21.63

を S（Slow）として 1 文字で示している．なお表 4 も同様である．縦軸はエラー発生率を示している．各棒グラフ中の模様は認証エラー時の誤入力桁数を割合として示したもので，Cpad-F の棒グラフの模様を例に説明すると上から順に誤入力桁数が 4 桁，3 桁，2 桁，1 桁の割合を示している．図 8 から，入力インタフェースの形状によらずインジケータ速度が Fast の場合はエラー率が 50%を超える結果となった．この結果からインジケータ移動速度が 150 ms（Fast）の条件は実用的でないといえる．

表 4 では，各条件における認証エラーの発生回数を示している．またこの表では認証エラー発生時に入力を誤った桁数（誤入力桁数）に関する結果も示している．たとえば，暗証番号が “1124” であるのに入力値が “1225” であった場合，2 桁目と 4 桁目が誤入力になっているので，誤入力桁数は 2 となる．この結果から，インジケータ速度が Fast 以外の場合，ほとんどの入力ミスは 1 桁であることが分かる．またインジケータの速度が同一の場合，Cpad のエラー回数は Npad の回数を下回らず，インジケータ速度が M，F になるとその差が 1.5 倍となった[*4]．またインジケータ速度が Fast の場合には誤入力桁数が分散する結果となっているが Npad の場合は誤入力桁数が少ない方に分布しているのに対し，Cpad の場合は誤入力桁数が多い方にエラー回数が多く分布する結果となった．

次に認証時間の結果を**表 5** および**図 9** に示す．

表 5 は各条件における認証成功時の認証時間を抽出し，算出した平均値，標準偏差，中央値および最小操作時間である．また図 9 は各条件における，平均値と標準偏差を示した棒グラフである．

図 9 から，どちらのインタフェース形状においてもインジケータ速度が Medium（300 ms）の場合に平均認証時間が最小となった．また認証時間はいずれの条件においても

[*4] Npad-M : Cpad-M = 6 回 : 9 回，Npad-F : Cpad-F = 40 回 : 60 回．

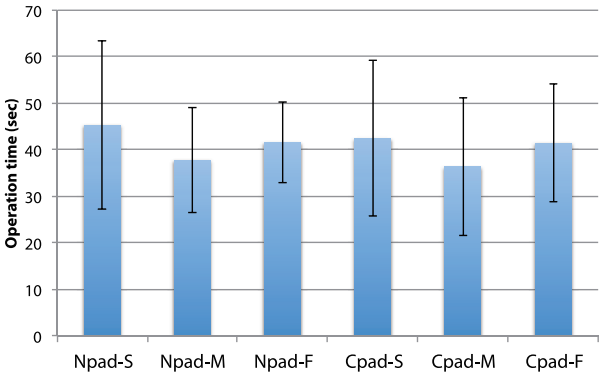

図 9 各条件における認証時間の平均値と標準偏差
Fig. 9 Average and S.D. of operation time in CCC.

最小値で 20 秒を超える結果となり，また中央値は平均値を下回る結果となった．なおインジケータ速度が Fast の場合に認証時間が短縮されず，Medium 条件よりも長くなった理由は入力用カーソル位置の取得に時間がかかるようになったためである．

4.1.3 負荷評価

図 10 に NASA-TLX テストにおける主観的負荷評価の結果を示す．図 10 のグラフは各評価項目における評価結果の平均値と標準偏差を示しており，縦軸の値が小さいほど被験者が感じた負荷が少ないという意味である．評価結果から，一般的な傾向としてインジケータ移動速度が Fast のときよりも Slow，Medium の方が被験者が感じる負担が少ないという結果となった．またこの傾向はユーザインタフェースの形状に依存しないことも分かった．ただしフラストレーションの評価だけはこの傾向と異なり，Medium よりも Slow の方が高いフラストレーションを感じるという結果となった．

4.2 覗き見攻撃に対する安全性評価実験

想定脅威モデルに対する CCC の安全性を評価するため，認証行為を録画した動画を用いて被験者による覗き見攻撃実験を実施した．

4.2.1 実験手順

まず始めに認証行為の録画データを作成した．録画環境として以下の 3 つの状況を選択した．

1) 著者所属の大学研究室内
2) ファーストフード店内
3) 通勤電車内

これらの状況を選択した理由は以下の 2 つからである．

- 認証利用者の背後または周囲に第三者が来る可能性が高い．
- 周囲に一定の環境音が存在する．

CCC は，秘密情報の一部である入力用カーソル位置が第三者に漏洩しないという前提で成立する手法であり，その伝達方法として振動を利用している．しかし振動は副次

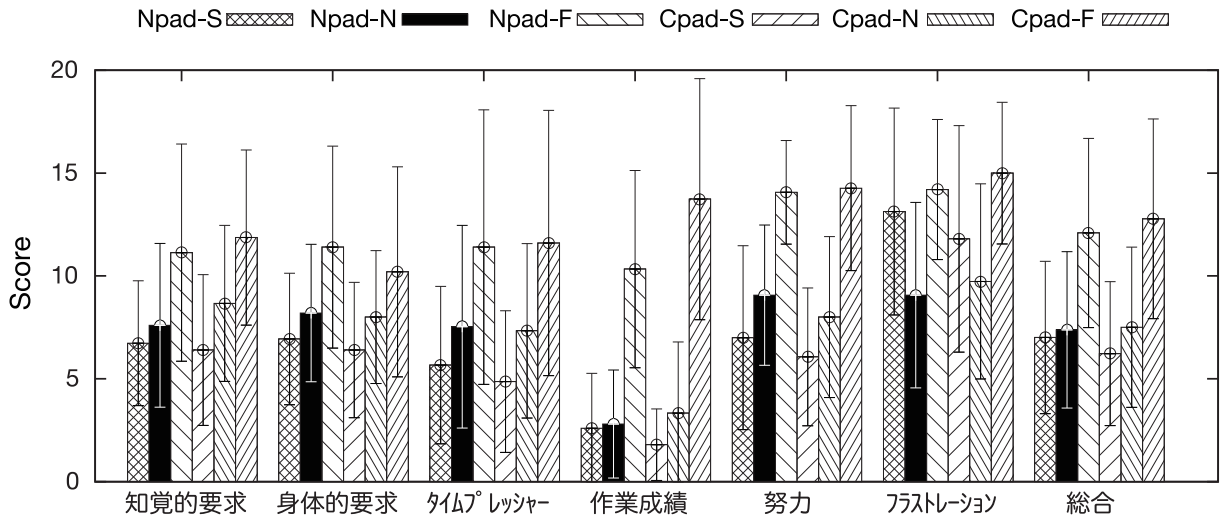

図 10 NASA-TLX による負荷評価結果
Fig. 10 Subjective task load evaluation in CCC.

的に振動音を発生させる．したがってカメラによる録画により振動の有無が音として検出可能になる懸念がある．そこで現実的に攻撃されうる環境での環境音をまじえた状況で認証行為を録画し，そこから入力値が特定可能かを検証するために上記の 3 状況を録画環境として選択した．

録画条件は次のとおりである．撮影機器は民生用デジタルカメラである OLYMPUS TG-320 を用いた．認証に利用した携帯端末は 4.1 節で実験に使用した端末と同一端末である．動画撮影は，認証操作に使用した端末から 60 cm 離れた場所にカメラを設置し，携帯端末の画面と入力操作の双方を撮影した．なお携帯端末と録画撮影カメラとの間の距離は既存研究 [9] における実験条件にならった．システム側の条件としてはインジケータ移動速度を Medium (300 ms) とし，ユーザインタフェース形状は Cpad と Npad の双方で撮影を行った．つまり 3 つの録画環境 × 2 種のユーザインタフェース形状から撮影条件は 6 条件となり，それぞれの条件において 1 回ずつ認証操作の動画撮影を行った．動画撮影は端末操作 1 名と撮影者 1 名の計 2 名で実施した．端末操作は被験者の 1 名に依頼し，撮影は著者の 1 名が行った．なお撮影時に使用した暗証番号はすべての撮影条件で同一値とした．この撮影条件は，撮影場所とユーザインタフェースこそ異なるものの「同一利用者の複数回の認証行為を撮影した」ことと同意である．

実験方法について述べる．実験では次に述べるような状況を想定した．

「とある攻撃者が特定ターゲットの個人認証操作を複数回録画（盗撮）した．しかし暗証番号の特定に難航したため，撮影した動画を Web 上に共有し，複数人で協力して暗証番号を特定しようと試みた」

この状況は，撮影した認証行為の動画データを攻撃者が自由に事後解析する状況を想定している．したがって著者らは，1 つの指示を除いていっさいの制約を被験者に課さなかった．提供された動画は Web ブラウザを通じて繰り返し閲覧可能であり，複数の動画を並置して閲覧することも可能である．また被験者は，動画から知りえた情報をメモすることから，動画をダウンロードし計算機で解析処理することも含めて，好きな方法で解析可能な状況とした．唯一の指示は安易に暗証番号特定を断念しないよう「各認証動画を最低でも 3 回は見るように」と指示したのみである．なお本実験では，以下の 3 点を回答するよう被験者に依頼した．

i) 特定（推測）した暗証番号（4 桁数値 1 つ）
ii) 特定（推測）結果に対する自信の有無（2 択）
iii) 特定（推測）の根拠（自由記述）

被験者は 15 名で，全員が高等教育を受けているか修了した被験者であった．また 9 名がスマートフォンユーザであった．被験者の構成情報は**表 6** のとおりである．なお被験者には本実験実施前に CCC の認証操作について十分な説明を行った．

表 6 被験者の構成情報
Table 6 Demographic information of subjects.

	20 代	30 代	40 代	50 代
男性	10	1	0	0
女性	2	0	0	2
スマートフォンユーザ	7	1	0	1

4.2.2 実験結果

15 名の被験者のうち，暗証番号を正しく特定できた被験者は 0 名であった．また全回答を精査した結果，以下の結果が明らかになった．

- 2 桁以上正解している回答はなかった．
- 1 桁正解で，かつその回答内容に “自信あり” とした回答はなかった．

動画からの暗証番号特定方法だが，認証操作における手

の動き始めのタイミングや，手に伝わっている振動を動画から推測しようと試みたという回答があった．また動画を音声処理して振動発生タイミングを検出しようとした被験者が 1 名いたが，今回の動画データでは成功しなかったという回答を得た．これらの結果から，今回の実験で用いた撮影機材と撮影条件のもとで撮影された複数の動画記録を用いて事後解析を制約なしで許容しても暗証番号の特定は困難という結果が示された．

5. 考察

5.1 利用可能性について

4.1 節の実験結果から以下の 2 つの結論が導き出せたと考える．

1 つはインジケータ速度についてである．今回 3 つの速度値を設定して比較実験をした結果，300 ms（Medium）が最も望ましいインジケータ速度であると結論付ける．150 ms（Fast）は，認証エラー率が 50%を超えることから現実的ではない．450 ms（Slow）は認証エラー率だけ見ると Medium 速度よりも良い結果であるが，認証時間に注目すると Medium 速度よりも認証時間が長くなるという問題がある．また NASA-TLX の結果から利用者が感じるフラストレーションも高くなっている．Slow 条件の場合にフラストレーションが高くなる理由は，インジケータ速度が遅すぎてインジケータの回転待ち時間が長くなり「もう少し回転速度が速くても処理できる」として利用者が不快に感じたためである．これらの議論から今回の 3 条件においては Medium 条件がインジケータ回転速度として最も望ましいといえる．なお 4.2 節の攻撃実験で CCC の撮影条件としてインジケータ速度を Medium 一択にした理由は，この実験結果をふまえたものである．

もう 1 つはユーザインタフェース形状についてである．2 種類のユーザインタフェース形状による評価実験を行ってきたが，主観的負荷と認証時間について大きな差は見られなかった．また認証エラー率も Slow および Medium 条件において実験結果に差は見いだせなかった．これらの結果からユーザインタフェース形状について優劣を決定可能なデータは得られなかった．ただしインジケータ速度が Fast の際の認証エラーに注目すると，Npad のエラーは誤入力桁数の少ないエラーが多く発生しているのに対し，Cpad のエラーは半数以上が全桁誤入力というエラーとなっている．これはインジケータ速度が速くなるとともに，ユーザインタフェース形状による影響が表出する可能性を示唆しており，その検証は今後の課題である．

上記の考察から最良の条件を [Npad & Medium] と仮定すると，認証成功率は 90%超で，平均認証時間は 37.7 秒となる．この結果から認証時間を短縮する必要性はあるものの，提案手法の利用可能性において疑問が残る手法ではないといえる．

5.2 覗き見攻撃に対する安全性について

4.2 節の実験結果から，15 名の被験者による攻撃実験で暗証番号を完全に特定できた被験者は 0 名であった．また部分的に回答が正解していたものの，その回答に自信があると回答した被験者も 0 名であった．これらの結果からランダムに決定される振動発生タイミングを特定する以外に入力値の推定または特定を可能にしうる脆弱性の存在可能性は低いと考える．したがって，今回の実験条件において，認証操作と画面表示をカメラで録画され，その動画が複数セッション分攻撃者に窃取され，それらを時間をかけて事後解析したとしても，入力値の特定を困難なままにするという目的は達成されたと考える．

ただし，本提案手法はいかなる条件下においても安全性を担保しうる手法ではない．認証行為の動画記録から振動発生タイミングが抽出可能かどうかが問題であり，それは「周囲の環境音」「端末の振動音」「撮影機材の性能」の 3 要因に影響を受ける．撮影機材の性能は今後向上することに疑いの余地はなく，周囲の環境音も利用者側で制御できる範囲は限定的である．提案手法の安全性はこれらの要因に依存することは利用者も留意する必要がある．またこの点に関する改善案については 5.5 節で述べる．

5.3 既存の対策システムとの比較

2 章で紹介した既存の覗き見攻撃対策システムから，認証操作を複数セッション分動画撮影されても安全性を確保しうるとした 3 システム：fakePointer，Undercover，Phone Lock について提案手法と比較した結果を**表 7** に示す．なお，CCC は Npad-M の条件，Phone Lock は，CCC と同等の条件と考えうる振動による 10 種類の信号を用いて 4 回入力を行う “Haptic 4PIN-10 cue” 条件を，そして Undercover は提示画像に画像処理を適用しない Original Picture による実験結果の値を記載している．また各認証手法と条件における秘密情報の情報量と回答回数を**表 8** に示す．fakePointer，Phone Lock，CCC の 3 手法は，4 回の入力回数で 10,000 通りの秘密情報をとりうる．したがって，情報量としては 13.3 bit 相当となる．一方，Undercover は文献 [7] より 7 回の入力回数で 20,480 通りの秘密情報をとりうる．このことから秘密情報の情報量としては 14.3 bit

表 7 既存手法との認証エラーおよび認証時間の比較
Table 7 Comparison of error rate and operation time between CCC and other systems.

	認証時間		エラー率（%）
	平均値（s）	中央値（s）	
fakePointer	17.35	-	5.6
Undercover	-	32.0	26.3
Phone Lock	-	28.2	10.4
CCC（Npad-M）	37.7	34.7	8.0

表 8 実験条件の比較
Table 8 Secret information and the number of input operation of CCC and other systems.

	秘密情報量（bit）	回答入力回数
fakePointer	13.3	4
Undercover	14.3	7
Phone Lock	13.3	4
CCC（Npad-M）	13.3	4

表 9 システム要件および認証操作に必要な負担の比較
Table 9 Requirements and operation loads comparison between CCC and related systems.

	別装置	振動信号種類数	追加記憶（永続）	追加記憶（一時）	脳内処理
fakePointer	要	-	-	要	要
Undercover	要	5	-	-	要
Phone Lock	不要	10	要	-	要
CCC（Npad-M）	不要	1	-	-	-

相当となる．

fakePointer と CCC を比較すると，認証時間とエラー率の双方において fakePointer の方が良好な結果となっている．しかし，fakePointer は秘密情報入力に必要となるチャレンジ情報を認証操作を行う前に事前に取得し記憶する手法であるため，表 7 に記載の認証時間に入力用チャレンジ取得のための操作時間が含まれない．したがって認証時間については同一条件による比較とはいえず，優劣の判断はできないと考える．

Undercover，Phone Lock と CCC との比較では認証エラー率では CCC の方が良好な結果となる一方で，認証時間は他の 2 手法と比較して CCC の方が劣る結果となった．ただし，Phone Lock の認証時間の中央値は 28.2 (s)，Undercover の認証時間も 20 (s) を下回ることはなかったのに対して，CCC の最小認証時間は 22.0 (s) なので認証操作に慣れるに従い，その差は縮まる可能性はあると考えている．また認証時間の短縮については次節でも議論する．

表 9 は，認証手法のシステム要件ならびに認証操作に必要となる各種負担について比較を行った表である．この表からいえることは，CCC は既存の 3 手法よりも認証利用時に利用者に課される負担が低いという点である．

別装置についてだが，fakePointer は認証端末とは別に通信機器が必要となるため携帯端末単体での個人認証システムとしては実装が容易とはいい難い．Undercover はトラックボールまたは 5 種類の振動信号が伝達できるデバイスが必要となる．Undercover の実装では，別装置を利用するかわりに既存の携帯端末の振動機能を応用する方法も考えられる．しかしそのためには複数の振動信号を組み合わせて 1 つの値を伝達する手法で 5 種類の値を伝達することになると思慮する．すると振動信号の組合せパターンとそれが意味する値の関連付けを別途記憶する必要が生じることになる．Phone Lock に永続記憶の負担があるのは同様の理由からである．Phone Lock の利用者は，振動信号と各振動信号に対応する数値との関連付けを記憶保持する必要がある．一方 fakePointer における一次的な記憶負担の増加は，事前に入力用チャレンジ情報を取得し，認証操作が完了するまでそれを記憶保持しなければならないためである．

また fakePointer や Undercover は，入力時にのみ必要となる入力用チャレンジ情報と認証操作画面で提供される視覚情報を組み合わせて回答を決定する必要があるが，これは利用者が脳内で行う必要がある．Undercover ではこの処理のことを “Mental reassembly” と呼んでいるが，本論文ではこのように認証操作のために利用者が脳内で行う処理のことを「脳内処理」と定義する．脳内処理の一例について紹介する．Undercover における Mental reassembly とは事前に記憶している秘密画像，認証操作機器に記載されている正解番号算出表，そして入力操作時にトラックボールから得られる回転情報の 3 つの入力情報をもとに利用者が脳内で正解回答となる番号を導き出す処理である．fakePointer の場合は，事前に記憶している暗証番号と認証操作開始前に取得し記憶した入力ポインタ指示用記号列を組み合わせ，利用者が脳内で正解入力に必要なダイヤル回転量を求める必要がある．Phone Lock の場合は，事前に記憶している暗証番号のほかに，各数字と振動パターンの対応表も記憶しておく必要がある．認証操作時には振動パターンを端末から取得し，記憶している対応表を用いて該当する振動パターンが示す数字を取得，そしてその数字が自分の入力したい数字かどうかを判定するという処理を利用者が脳内で処理する必要がある．この脳内処理は覗き見攻撃対策のために利用者に課される負担の 1 つであるといえる．

これらの要件および負担に対して CCC はいっさい必要がない手法となっている．CCC では認証を行う携帯端末以外の別装置は必要とせず，携帯端末内の振動機能を利用する．ただし利用する振動信号は 1 種類であり，振動信号自体に意味を持たせていない．また CCC の操作は振動発生時のインジケータの位置のみを記憶し，その位置に入力したい数値を移動させる操作である．したがって上述したような脳内処理は不要である．記憶負担も認証操作時に入力用カーソルの位置をその場で記憶するだけであり，暗証番号以外の情報を永続的ならびに数分単位で一時的にも記憶する必要がない．また提案手法の操作法は，金庫におけるダイヤル操作と同じメタファであり，覗き見攻撃対策のために複雑かつ経験のない操作方法を新たに習得する必要もない．これは既存の提案手法にはない CCC ならではの利点であると考える．

5.4 今後の課題

5.4.1 操作性改善について

認証エラーの低減ならびに認証時間の短縮に向けた今後の課題について2点述べる．

1つめの課題は提案システムの実装法を再検討することである．提案手法において認証エラーを誘発している原因は2つある．1つは入力用カーソル位置の伝達処理であり，もう1つは数字入力つまみの回転処理である．入力用カーソル位置の伝達は前述のとおり視覚情報と振動情報を組み合わせて行っている．しかし現在の実装では，この視覚情報と振動情報の同期には限界があり，インジケータの回転速度が速くなるにつれて視覚情報と振動発生タイミングとの間に“微妙なずれ”が認識されるようになる．これが結果として入力用カーソル位置の認識を誤らせる結果を招き，認証エラーを発生させていると考える．数字入力つまみの回転処理における問題は，回転ボタンを連打した際に，押下回数どおりに入力が受付けられず，つまみが意図したとおりに回転しないまま決定ボタンを押してしまう事象がしばしば発生していた．これも誤入力を招き，認証エラーを発生させていた．

これらの問題の原因はプロトタイプシステムの実装にあると考える．今回はWeb技術（HTML+JavaScript）を用いて実装したが，この実装環境ではパフォーマンス上の問題が出やすいことが分かっている．現在の実装環境で実装方法を見直すことと別の実装方法による再実装の双方を今後検討する予定である．

もう1つの課題は，カーソル位置認識にかかわる別の操作法を検討することである．認証時間の短縮は覗き見攻撃対策の実用化に向けて必要不可欠である．提案手法では，認証時間の多くは入力用カーソル位置の認識に費やされている．よってこの認識時間を短縮できれば認証時間の短縮につながる．そこで現手法とは別の方法による入力用カーソル位置の取得を検討，評価する必要があると考えている．インジケータを回転させつつ振動の発生を待つかわりにPhone Lock [9]や東山らの提案手法 [16]のように利用者が能動的に入力用カーソル位置を探索する方法は有力な代替案であると考えている．これも今後の課題である．

5.5 安全性に関する今後の課題

本研究で実施した攻撃実験において暗証番号を特定した被験者はいなかったが，安全性を確実にするために以下の2点について言及する．

1つは攻撃者による入力値特定を支援してしまうような利用者操作を抑止するユーザインタフェースの検討である．正規利用者が振動により入力用カーソル位置を認知すると，即座に数字入力用つまみの回転操作を始めようとする．これは利用者にとっては自然な振舞いだが，攻撃者にとっては入力用カーソル位置特定の大きなヒントになる．理由は，ユーザがつまみ回転操作を始める直前のインジケータの位置が入力用カーソル位置であると推測できてしまうからである．この対策として，プロトタイプシステムではインジケータが1周回転し終わるまでつまみ回転用ボタンを押下不能にしている．しかし，これだけでは十分な対策とはいいがたい．今後検討を進めていく必要がある．

もう1つは振動検知の困難化である．提案手法は利用者が携帯端末を把持し，その状態で振動を認識することにより秘密情報の一部を取得する．端末を把持していない攻撃者はその振動情報を得ることができないため，入力値の特定が困難になるという前提のうえに安全性が確保されている．今回の攻撃実験では，想定した実験条件のもとで動画撮影をした結果，動画記録から振動情報を抽出することはできなかった．しかし，攻撃ならびに環境/機材などの条件が変われば振動情報が窃取される可能性はある．そういった懸念のある状況下でも，振動情報の窃取を困難にする方法について検討を進める必要がある．振動によって発生する振動音については，認証操作時に雑音としてホワイトノイズを端末から発生させる対策を検討している．また携帯端末を机の上などに置いてしまうことで振動タイミングが漏洩する懸念については端末を把持するよう認証操作時の携帯端末の姿勢に関わる制約を設けることも考えている．

6. おわりに

本論文では，携帯端末での暗証番号認証における覗き見攻撃を想定し，その対策となりうる個人認証手法“CCC”を提案した．CCCは金庫のダイヤルメタファをもとに，数字を指し示すカーソルの位置をランダム化するとともに視覚的に視認不能にすることで覗き見攻撃による入力値特定を困難にした．また正規利用者と認証端末との間で入力用カーソル位置を共有するために振動機能を利用している．これによりカメラ録画による覗き見攻撃が行われ，攻撃者に複数セッション分の動画記録が窃取されたとしても，入力値の特定を困難にしている．

この提案手法をAndroidアプリケーションとして実装し，利用可能性と覗き見攻撃に対する安全性の評価実験を行った．その結果，最も好ましい条件で平均認証時間が37.7 (s)，認証エラー率は8.0%という結果を得た．また安全性に関する実験においては，想定条件下で撮影された複数動画を事後解析させたとしても暗証番号の抽出が困難であることが確認された．また提案手法は既存の覗き見攻撃対策手法と比較しても利用者に課される負担が少ない手法であることも明らかにした．

謝辞 被験者実験に協力いただいたすべての方々へ，ここに御礼申し上げます．また本研究はJSPS科研費26540055の助成を受けたものです．

参考文献

[1] 株式会社みずほ銀行：みずほ銀行：5. キャッシュカードの盗難・偽造の手口について，入手先 ⟨http://www.mizuhobank.co.jp/crime/cashcard/cc_05.html⟩（参照 2014-11-23）.

[2] 株式会社セブン銀行：ATM 利用時のスキミングにご注意ください，入手先 ⟨http://www.sevenbank.co.jp/support/info_skimming.html⟩（参照 2014-11-23）.

[3] De Luca, A., Weiss, R. and Drewes, H.: Evaluation of eye-gaze interaction methods for security enhanced PIN-entry, *Proc. 19th OZCHI '07*, pp.199–202 (2007).

[4] De Luca, A., von Zezschwitz, E. and Hußmann, H.: VibraPass: Secure authentication based on shared lies, *Proc. CHI '09*, pp.913–916 (2009).

[5] De Luca, A., von Zezschwitz, E., Nguyen, N.D.H., Maurer, M.E., Rubegni, E., Scipioni, M.P. and Langheinrich, M.: Back-of-device authentication on smartphones, *Proc. CHI '13*, pp.2389–2398 (2013).

[6] 喜多義弘，朝貝洸紀，菅井文郎，朴 美娘，岡崎直宣：バイブレートパターンを用いた覗き見耐性を持つパスワード認証方式の提案と実装，暗号と情報セキュリティシンポジウム（SCIS2013）(2013).

[7] Sasamoto, H., Christin, N. and Hayashi, E.: Undercover: Authentication usable in front of prying eyes, *Proc. CHI '08*, pp.183–192 (2008).

[8] 高田哲司：fakePointer：映像記録による覗き見攻撃にも安全な認証手法，情報処理学会論文誌，Vol.49, No.9, pp.3051–3061 (2008).

[9] 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. TEI '11*, pp.197–200 (2011).

[10] Bianchi, A., Oakley, I. and Kwon, D.S.: Spinlock: A Single-Cue Haptic and Audio PIN Input Technique for Authentication, *Proc. HAID 2011*, pp.81–90 (2011).

[11] Bianchi, A., Oakley, I. and Kwon, D.S.: Open Sesame: Design Guidelines for Invisible Passwords, *IEEE Computer*, Vol.45, No.4, pp.58–65 (2012).

[12] 原田篤史，漁田武雄，水野忠則，西垣正勝：画像記憶のスキーマを利用したユーザ認証システム，情報処理学会論文誌，Vol.46, No.8, pp.1997–2013 (2005).

[13] Hayashi, E., Dhamija, R., Christin, N. and Perrig, A.: Use Your Illusion: Secure authentication usable anywhere, *Proc. SOUPS '08*, pp.35–45 (2008).

[14] 桜井鐘治，後沢 忍：機密情報入力方式の検討，情報処理学会研究報告，2010-CSEC-43, pp.1–6 (2010).

[15] Roth, V., Richter, K. and Freidlinger, R.: A PIN-entry Method Resilient Against Shoulder Surfing, *Proc. 11th ACM CCS '04*, pp.236–245 (2004).

[16] 東山侑真，岡村真吾，矢内直人，藤原 融：タッチパネル端末の特性を利用した覗き見攻撃耐性をもつ個人認証手法，コンピュータセキュリティシンポジウム 2014（CSS 2014）(2014).

石塚 正也

2012 年電気通信大学電気通信学部情報通信工学科卒業．2014 年同大学大学院情報理工学研究科総合情報学専攻修士課程修了．在学中はモバイルシステムの個人認証にかかる研究に従事．ソーシャルエンジニアリング，ネットワークセキュリティにも関心がある．

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 年産業技術総合研究所情報技術部門研究員．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．個人認証，ユーザブルセキュリティ，情報視覚化に興味を持つ．IEEE/CS 会員．