Vol.2016-DPS-166 No.22
Vol.2016-CSEC-72 No.22
2016/3/4

メンタルタスクと視線遮断動作を併用したユーザ認証の覗き見対策の提案

遠藤将[†1]　村松弘明[†2]　藤田真浩[†3]　西垣正勝[†3]

概要：携帯端末におけるユーザ認証の脅威として覗き見攻撃が考えられる．覗き見攻撃に対しては認証方式のチャレンジ&レスポンス化が基本対策となるが，既存手法の多くは，ユーザに過大なメンタルタスク（記憶負荷や所要時間など）または専用デバイスの所持を要求する方式となっており，利便性の低下が大きいという問題がある．そこで本研究では，覗き見攻撃者からの視線を遮断するためのフィジカルタスクを併用した覗き見攻撃対策を提案する．ユーザにフィジカルタスクを要求することによって，軽度のメンタルタスクだけで覗き見耐性が維持されることが期待できる．また，ユーザがこのフィジカルタスクを違和感なく適切に行えるようなユーザ認証インタフェースの検討を行う．提案方式が利便性の低下を抑え，かつ覗き見攻撃に対して安全な認証方式であることを検証する．

キーワード：ユーザ認証，覗き見攻撃，ユーザインタフェース

A Shoulder-Surfing Resistant User Authentication by Using Mental Task and Anti-Peeping Motion

MASASHI ENDO[†1]　HIROAKI MURAMATSU[†2]
MASAHIRO FUJITA[†3]　MASAKATSU NISHIGAKI[†3]

Abstract: Shoulder-surfing is one of big threats to user authentication for mobile devices. A typical method of resisting shoulder-surfing is challenge-response. However, almost all conventional methods require excessive amount of mental task (e.g., memory or time consumed) and/or possession of the device only for user authentication of users. These methods have a problem of reducing the usability. In this paper, we propose the method that combines use of physical task (anti-peeping motion) and mental task. To require physical task of the user, it is expected to maintain resistance to shoulder-surfing with a much easier mental task. Moreover, we improve user authentication interface so that users carry out physical task without feeling uncomfortable. We evaluate that our method prevents shoulder surfing and reduction of usability.

Keywords: user authentication, shoulder-surfing, user interface

1. はじめに

近年，スマートフォンが急速に普及しており，携帯端末上でプライバシ情報や機密情報を扱う場面が増加している．プライバシ情報および機密情報保護のため，携帯端末にはPIN（Personal Identification Number）やパターンロックなどのユーザ認証技術が導入されている．しかし，これらの認証手法においては，認証行為を覗き見することでPINやパターンロックなどの秘密情報を不正に取得することが可能である．このような攻撃は覗き見攻撃と呼ばれ，ユーザ認証における脅威の一つとして知られている．

覗き見攻撃を対策するためには，認証情報をワンタイム化することが肝要である．認証情報をワンタイム化する手法としては，認証方式をチャレンジ&レスポンス形式にすることが有効である．しかし，現在までに提案されているチャレンジ&レスポンス方式では，ユーザに過大なメンタルタスク（探索負荷が大きい[1]，時間がかかる[2]，記憶負荷が高い[3][4]）や専用デバイスの所持[5]を求めているものがほとんどであり，利便性の大きな低下へと直結していた．

本研究では，メンタルタスクと攻撃者からの視線を遮断するための動作（フィジカルタスク）を併用した覗き見対策を提案する．覗き見対策の一部として，ユーザへフィジカルタスクを要求することによって，ユーザへ要求するメンタルタスクを軽度とすることが可能となる．これにより，覗き見攻撃耐性を備えたユーザ認証方式が，利便性の低下を抑えた形で実現される．さらに，フィジカルタスクを組み込むにあたり，ユーザがその動作を「自然」かつ「適切」に行えるようなインタフェースについても検討する．

本論文の構成は以下のとおりである．2 章で覗き見対策における既存研究とその課題を述べる．3 章で提案方式について説明した後，4 章で提案方式に対する基礎実験の報告をする．5 章では提案方式の安全性および利便性に関する考察を行い，6 章でまとめと今後の課題を述べる．

†1 静岡大学情報学部
Faculty of Informatics, Shizuoka University
†2 静岡大学大学院総合科学技術研究科
Graduate School of Integrated Science and Technology, Shizuoka University
†3 静岡大学創造科学技術大学院
Graduate School of Science and Technology, Shizuoka University

ⓒ2016 Information Processing Society of Japan

Vol.2016-DPS-166 No.22
Vol.2016-CSEC-72 No.22
2016/3/4

図 1 fakePointer

2. 既存研究とその課題

2.1 チャレンジ&レスポンス方式を利用した覗き見対策

覗き見攻撃を対策するためには，認証情報をワンタイム化することが肝要である．認証情報をワンタイム化する手法としては，認証方式をチャレンジ&レスポンス形式にすることが有効である．チャレンジ&レスポンス形式の認証方式の一般的な手順は以下のとおりである．認証システムには，あらかじめユーザが秘密情報を登録してあるものとする．

【手順】

① 認証システムは，チャレンジを被認証者（ユーザ）へ提示する．
② ユーザは，自身の有している秘密情報とチャレンジからレスポンス（認証システムへ入力する情報）を計算する．
③ ユーザは，②で計算したレスポンスをシステムへ入力する．
④ システムは，登録されている秘密情報と①で提示したチャレンジから（入力されるであろう）レスポンスを計算する．この値と③で入力された値が一致していた場合，被認証者を正規ユーザとして認証する．

チャレンジ&レスポンスの本来の目的は，通信路を盗聴する攻撃者に対し，通信路に流れるチャレンジとレスポンスから秘密情報を逆計算することを防ぐことにある．これを達成するには，②における計算に暗号演算（典型的にはハッシュ値の計算）が必要となる．しかし，人間は暗号演算のような複雑な計算を行うことはできない．このため，画像認証におけるチャレンジ&レスポンスでは，チャレンジまたはレスポンスを覗き見攻撃者から隠す方法が採られる．

2.2 fakePointer

fakePointer は，安全な環境（覗き見が不可能な通信路）下を用いてユーザのみにチャレンジを渡す方式である[4]．認証手順を以下に示す．認証システムには，あらかじめユーザが 4 桁の PIN（各桁は 0～9 のうちいずれかの整数）を登録しているものとする．

【手順】

① ユーザは前もって，人目に晒されない安全な環境下でチャレンジとなる選択シンボル情報を取得しておく．選択シンボル情報は四つの記号のいずれかであり，システムが認証毎にランダムに決定する．
② 覗き見攻撃の危険性がある環境下で認証をする際，ユーザは自身の秘密情報となる PIN と①で取得しておいた選択シンボル情報を利用して，次のようにレスポンスの入力を行う．
③ 図 1 のように認証画面が表示される．ユーザは左右ボタンによって記号上の数字を左右にシフトさせ，1 桁目の PIN と 1 つ目の選択シンボル情報を重ね合わせて決定ボタンを押す．
④ ③を 4 回繰り返すことで 4 桁の PIN の入力を行う．

fakePointer は，カメラなどの録画装置を用いた複数回の覗き見攻撃に対しても安全な認証方式となっている．しかし，認証毎に，事前に安全な環境上でチャレンジ（選択シンボル情報）を取得しておかなければならず，チャレンジをレスポンスの入力まで記憶し続けておかなければならない．これは，ユーザにとって大きな負荷となり得る．

2.3 Undercover

Undercover は，別装置を用いてユーザのみにチャレンジを渡す方式である[5]．認証手順を以下に示す．認証システムには，あらかじめユーザが 6 桁の PIN（各桁は 1～5 のうちいずれかの整数）を登録しているものとする．

【手順】

① 図 2 のような装置に取り付けられたトラックボールをユーザが手で覆うと，トラックボールが回転する．この回転方向（上，下，左，右，回転せずにバイブレーションが鳴るの 5 パターン）がチャレンジとなる．回転方向はシステムが入力毎にランダムに決定する．
② トラックボールの回転方向に応じて，「各入力ボタンに対する数字の割り当て」が異なる（図 3）．ユーザは，①で取得した回転方向から，自身の 1 桁目の PIN が割り振られたボタンを特定する．
③ ユーザが②のボタンを押すことで 1 桁目の PIN が入力される．
④ ①～③を 6 回繰り返すことで，6 桁の PIN の入力をおこなう．

Undercover も，カメラなどの録画装置を用いた複数回の覗き見攻撃に対しても安全な認証方式となっている．しかし，認証を行う端末以外にトラックボールを所持しなければならない．

ⓒ2016 Information Processing Society of Japan

Vol.2016-DPS-166 No.22
Vol.2016-CSEC-72 No.22
2016/3/4

図 2 Undercover

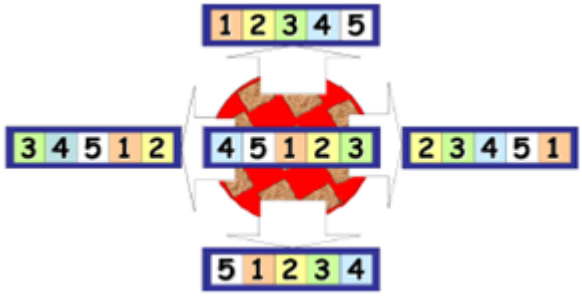

図 3 回転方向によるチャレンジの取得

2.4 CCC

CCC は，スマートフォンのバイブレーション機能を用いてユーザのみにチャレンジを渡す方式である[6]．認証手順を以下に示す．認証システムには，あらかじめユーザが 4 桁の PIN（各桁は 0～9 のうちいずれかの整数）を登録しているものとする．

【手順】

① 図 4 のように認証画面が表示される．認証が始まるとインジケータが図 5 のように 1 周回る．その最中にどこかで端末が振動する．振動時にインジケータが指していたマスが，チャレンジとなる「入力用マス」である．入力用マスはシステムが毎回にランダムに決定する．

② 「暗証番号入力用つまみ」全体を回転させて，①で取得した入力用マスの上に PIN の 1 桁目が描かれたマスを重ね合わせて決定ボタンを押すことでレスポンスを入力する．

③ ①～②を 4 回繰り返すことで PIN の入力をおこなう．

CCC も，カメラなどの録画装置を用いた複数回の覗き見攻撃に対して安全な認証方式となっている．ただし，バイブレーションの音が漏れないことが大前提である．静かな環境などでは，バイブレーションの音が攻撃者に漏れてしまう可能性が少なくない．インジケータが一周するのを待たなくてはならないため，チャレンジの取得に時間がかかるという点も問題である．

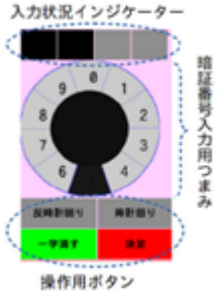

図 4 CCC 認証画面

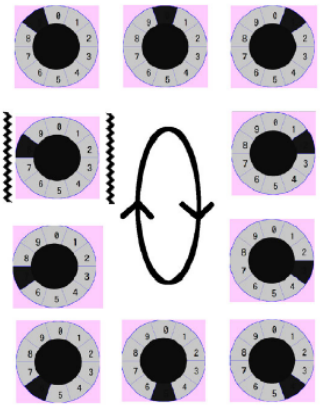

図 5 インジケータの回転

3. 提案方式

3.1 攻撃者モデル

本稿では文献[7]で示されている覗き見攻撃者モデルを想定して議論を進める．

【攻撃者モデル】

1. 攻撃者は 1 人である．
2. 攻撃者は一方向から覗き見（目視による覗き見，または，カメラによる録画）を行う．
3. 攻撃者は認証行為を複数回覗き見することができる．覗き見の都度，覗き見の方向を変更できる．

3.2 フィジカルタスクとメンタルタスクを併用した覗き見対策

本稿では，攻撃者からの視線を遮断するための動作（フィジカルタスク）とメンタルタスクを併用した覗き見対策を提案する．覗き見対策の一部として，ユーザへフィジカルタスクを要求することによって，ユーザへ要求するメンタルタスクを軽度とすることが可能である．すなわち，覗き見対策の導入に伴う利便性の低下を限定的にすることが期待される．

フィジカルタスクには種々の方法が考えられるが，本稿では，その一例として，「端末を傾ける」というタスクを採用する．具体的には，端末をある方向に傾けた状態でユーザにチャレンジを送った後，その方向と正反対の方向に端末を傾けてレスポンスを入力する．認証手順を以下に示す．認証システムには，あらかじめユーザが 4 桁の PIN（各桁は 1~9 のうちいずれかの整数）を登録しているものとする．

【手順】

① 画面に 1~9 の数字が表示されている．ユーザが携帯端末をある方向に 90 度傾けると数字の配置が変わる．数字の配置は認証毎にシステムがランダムに割り振る．これがチャレンジとなる．

② ユーザは，「登録している PIN が元々配置されていた位置」に新たに配置された数字を記憶する．

③ ユーザは，携帯端末を元の向きに戻す．画面の数字の配置も①の状態に戻る．

ⓒ2016 Information Processing Society of Japan

Vol.2016-DPS-166 No.22
Vol.2016-CSEC-72 No.22
2016/3/4

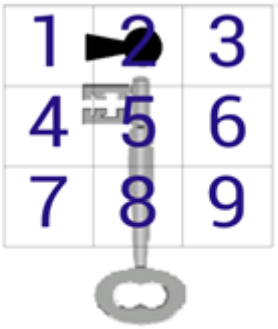

図 6-a 初期画面

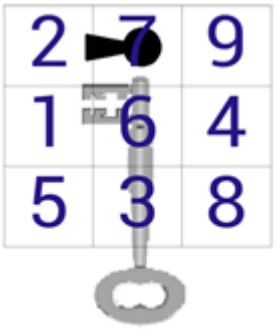

図 6-b チャレンジ取得画面

図 6-c レスポンス入力画面

図 6 提案方式

④ ユーザは，携帯端末を①と正反対の方向に 90 度傾け（これによって携帯端末の画面は，②の向きとは 180 度反対の向きに傾けられた状態となる）て，②で記憶した 4 桁の数字の位置をレスポンスとして入力する．

本方式であれば，携帯端末の②の画面と④の画面を 2 方向から覗き見をしない限り，攻撃者は正規ユーザの PIN を入手することができない．すなわち，3.1 節に示した攻撃者モデル対して安全な方式となっている．

本方式において，ユーザが行うメンタルタスクは，「PIN の位置に表示される数字を覚え，端末を逆方向に傾けて入力するまでその数字を記憶する」だけであるため，その負荷は比較的小さいものであると期待される．なお，2 章に示した既存方式においては，PIN の 1 桁ごとにチャレンジを取得しているのに対し，提案方式では 1 回のチャレンジの取得によって 4 桁の PIN のレスポンスを解答する方式であることに注意されたい．

3.3 フィジカルタスクへの実世界のメタファのマッピング

提案方式では，覗き見対策の一部としてフィジカルタスクを利用している．このフィジカルタスクに，実世界のメタファをマッピングすることで，フィジカルタスクをユーザに「自然」かつ「適切」に行わせることができるようになると期待される．

例えば 3.2 節で示した認証方式においては，「端末を傾ける」というフィジカルタスクをユーザに求めている．このタスクにマッピング可能な実世界のメタファには種々の方法が考えられるが，本稿では，その一例として「鍵を開錠する」という動作をマッピングする．具体的な認証手順（右利きのユーザの例）を以下に示す．

【手順】

① 画面に 1~9 の数字と鍵の画像が表示される（図 6-a）．ユーザは，携帯端末を鍵に見立てて左手で図 7-a のように持つ．

② ユーザは，自分の目の前に鍵穴の付いたドアがあると想定し，その鍵穴に自分が持っている鍵（携帯端末）を挿すような要領で携帯端末を持つ（図 7-b）．この時点で，携帯端末は図 6-b のような画面に変わる．図 6-b の数字の配置は認証毎にシステムがランダムに割り振る．これがチャレンジとなる．

③ ユーザは，「登録している 4 桁の PIN が元々配置されていた位置」に新たに配置された数字を記憶する．例えば PIN が「1234」だった場合，①の状態の画面（図 6-a）における「1234」）の数字の位置には，②の状態の画面（図 6-b）で「2791」が表示されるので，ユーザは「2791」を記憶する．

④ ユーザは，左親指を画面に添える．これによって，画面に表示された鍵は，鍵穴に挿入された画像に変わる．それと同時に，鍵は挿入されたままで数字の配置は①の状態に戻る．ユーザは，鍵を回して開錠する要領で，携帯端末を右に 180 度回転する．この状態（図 7-c）になった時点で，携帯端末の画面は図 6-c のように変わる．

⑤ ユーザは，③で記憶した 4 桁の数字をレスポンスとして入力する．

開錠のメタファを導入することによって，ユーザは「ある方向に端末を傾けてチャレンジを取得し，正反対の方向に端末を傾けてレスポンスを入力する」というフィジカルタスクを，自然にかつ適切に行うことが可能となることが期待される．すなわち，(i) このようなフィジカルタスクが要求されることに対し，ユーザが納得を示し易くなる，(ii) ユーザのフィジカルタスクが望ましくない形に逸脱すること[1]が発生しにくくなる，などの効果が助長される．

1. 例えばユーザが，3.3 節の手順②を図 8-a のような体勢で行い，手順⑤を図 8-b のような体勢で行った場合，手順②と手順⑤の両方の画面がユーザの正面にいる攻撃者に覗き見られてしまう．物理的なドアの開錠をユーザにイメージさせることによって，ユーザの意識の中に「鍵穴は動かない」という制約が自然に生じる．

ⓒ2016 Information Processing Society of Japan

図 7-a　初期状態

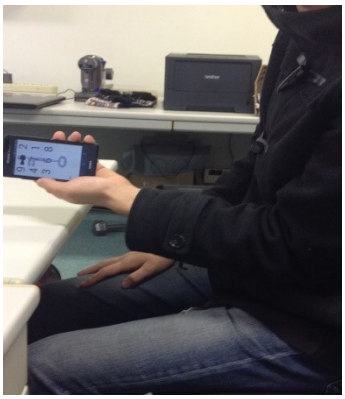

図 7-b　チャレンジ取得動作

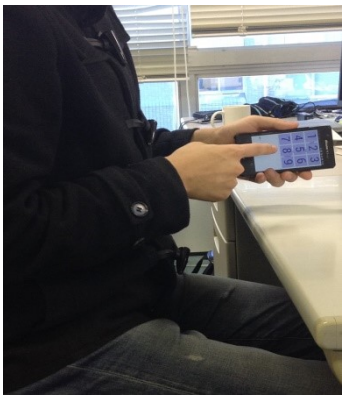

図 7-c　レスポンス入力動作

図 7　認証動作の流れ

図 8-a　チャレンジ取得動作

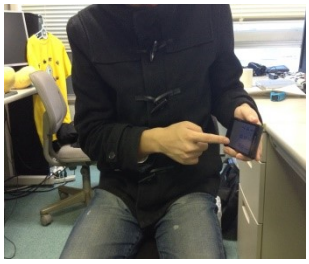

図 8-b　レスポンス入力動作

図 8　不適切な動作

4. 基礎実験

4.1 実験目的

提案方式の利便性, 安全性を, 既存方式である fakePointer, Undercover, CCC の 3 方式と比較することにより調査する. また,「鍵を開錠する」というメタファをフィジカルタスクにマッピングすることにより得られる効果を調査するために, 図 6 のように画面に鍵の画像が表示される方式（鍵あり方式）に対するユーザの印象と図 6 の画面から鍵の画像を削除した方式（鍵無し方式）に対するユーザの印象を比較する.

4.2 実験方法

情報系，工学系の大学生 6 名を，鍵あり方式のグループ 3 名と鍵無し方式のグループ 3 名に分け実験を行う．被験者には，認証方式に慣れてもらうため無制限で練習を行ってもらった後，10 回の認証試行における認証成功率と所要時間の計測を行う．また，提案方式と既存方式の比較，および，鍵あり方式と鍵無し方式の比較を行うため，実験後に質問紙によるアンケートを行う．アンケートは次の 2 項目である．質問 1 では，fakePointer，Undercover，CCC の 3 方式を被験者に説明した上でアンケートに答えてもらっている．また，質問 1 において既存方式の方が優れていると答えた被験者には，その理由を尋ねることとした．質問 2 では，鍵あり方式のグループには鍵無し方式を，鍵無し方式のグループには鍵あり方式を説明した上で，アンケートに答えてもらっている.

質問1.　fakePointer，CCC，Undercover の認証方式を理解した上で，実験で行った認証方式も合わせた 4 方式を比較しながら，安全性と利便性の両方の面でそれぞれの認証方式がどれだけ許容できるかを「許容できる・少し許容できる・どちらとも言えない・少し許容できない・許容できない」から一つ選んでください.

質問2.　鍵ありの方式と鍵なしの方式のどちらが良いと思うかを「鍵ありがとても良いと思う・鍵ありが良いと思う・どちらでもない・鍵なしが良いと思う・鍵なしがとても良いと思う」から一つ選んでください.

4.3 実験システム

提案方式の基礎実験を行うため，実験システムの実装を行った．実験用携帯端末のサイズと質量は次のとおりである．サイズ：約 131mm×約 67mm×約 10.5mm，重量：約 141g．携帯端末の傾きを検出し，チャレンジ取得画面（3.3 節の手順②の画面）とレスポンス入力画面（3.3 節の手順⑤の画面）への切り替えを行うために，端末に搭載されている加速度センサと方位センサを利用した.

チャレンジ取得画面に切り替わる条件は，（右利きユーザの場合）左手に持った携帯端末を左に 90 度傾けることである．また，ユーザが左親指を画面に添える動作（3.3 節の手順④）を画面のタップによって捉え，チャレンジ取得時の携帯端末の向きを記録しておく．レスポンス入力画面に切り替わる条件は，携帯端末をチャレンジ取得画面から 180 度反対に傾けることである．人間の動作は正確ではないため，それぞれの角度に対して，約±20 度の誤差は許容した.

4.4 実験結果

実験の結果を表 1 に示す．平均所要時間は 10.69 秒，認証成功率は平均 93.3%であった.

アンケートの質問 1 に対する結果を表 2 に示す．その内

ⓒ2016 Information Processing Society of Japan

表 1 実験結果

グループ	被験者No.	平均所要時間[s]	認証成功率
鍵ありグループ	1	7.30	9/10
	2	12.05	9/10
	3	6.91	9/10
鍵なしグループ	4	17.66	9/10
	5	9.87	10/10
	6	10.34	10/10
	全体平均	10.69	93.3% (56/60)

訳は以下のとおりである．

- 提案方式 :「許容できる」1 名，「少し許容できる」3 名，「どちらとも言えない」0 名，「少し許容できない」2 名，「許容できない」0 名．
- fakePointer :「許容できる」1 名，「少し許容できる」3 名，「どちらとも言えない」2 名，「少し許容できない」0 名，「許容できない」0 名．
- Undercover :「許容できる」0 名，「少し許容できる」0 名，「どちらとも言えない」0 名，「少し許容できない」3 名，「許容できない」3 名．
- CCC :「許容できる」0 名，「少し許容できる」3 名，「どちらとも言えない」1 名，「少し許容できない」1 名，「許容できない」1 名．

被験者の中で提案方式よりも既存方式のほうが許容できると述べていた被験者は 3 名となった．その理由として，3 名の被験者は「安全性の観点から fakePointer のほうがよい」という意見が得られた．

アンケートの質問 2 に対する結果を表 3 に示す．被験者の回答は次のとおりである．「鍵ありがとても良いと思う」1 名，「鍵ありが良いと思う」4 名，「どちらでもない」1 名，「鍵なしが良いと思う」0 名，「鍵なしがとても良いと思う」0 名．

5. 考察

5.1 所要時間および認証成功率

表 4 に提案方式と既存方式の所要時間および認証成功率の比較を示す（既存方式のデータはそれぞれの文献からの転載）．提案方式の認証成功率は，fakePointer や CCC と同様に 90%を超える高い精度となっていることがわかる．平均所要時間については，提案方式は 3 つの既存方式と比べて大幅に短い時間で認証を行えていることが確認された．認証にかかる時間はユーザの利便性に大きな影響を与えると考えられるので，提案方式は所要時間の面で高い利便性を有しているといえる．

5.2 提案方式に対するユーザの心象

表 2 より，提案方式と既存方式に対するユーザの許容度は，fakePointer ，提案方式，CCC，Undercover の順に高い結果であった．fakePointer が提案方式を若干上回った理由は，被験者が利便性よりも安全性を優先していることに起因していた．ただし，提案方式よりも fakePointer のほうが許容できると回答した 3 名の被験者のうち 1 名からは「日常的に利用するのであれば，提案方式のほうが良い」という旨のコメントも得られている．今回の実験では，被験者には提案方式のみを実施してもらい，既存方式については紙面による説明に留めている．今後，他方式についても実装し，被験者に実際に fakePointer のメンタルタスクを体験してもらったうえで比較を行いたい．

なお，提案方式よりも fakePointer のほうが許容できると回答した 3 名の被験者のうち別の 1 名から,「チャレンジ取得画面を覗き見ることができる位置にいる攻撃者は，レスポンス入力画面を見なくても，指の動きからどこを押しているのかを推測することができるので，提案方式は安全性を確保できていないのではないか」というコメントがあった．このため，提案方式の改良として，小さい指の動きで入力ができるような入力インタフェースの導入を検討している．

5.3 フィジカルタスクのメタファによるユーザの心象の変化

表 3 より，鍵の開錠のメタファによって，携帯端末を傾ける動作に対する被験者の印象が向上する結果が得られていることが確認された．とは言え，通常，覗き見対策の導入が利便性を阻害することは必然である．このため，被認証者の心象を更に向上させるための工夫については，今後も検討を続けていく必要がある．

6. まとめと今後の課題

本稿では，メンタルタスクと視線遮断動作（フィジカルタスク）を併用したユーザ認証の覗き見対策の提案を行った．実験結果より，提案方式が，既存方式と比較して認証成功率を高く保ちつつ，所要時間の短い認証方式となっていることが確認できた．しかし，提案方式は，攻撃者のモデルを「一方向からの覗き見」に限定しており，安全性を幾分妥協したうえで利便性を向上させるアプローチとなっている．今後は，提案方式の利便性を保ちつつ，安全性を更に高めることができないか検討していきたい．

ⓒ2016 Information Processing Society of Japan

表 2 実験アンケート結果

被験者No.	提案方式	fakePointer	Undercover	CCC
1	少し許容できない	どちらとも言えない	許容できない	許容できない
2	少し許容できる	少し許容できる	許容できない	少し許容できない
3	許容できる	少し許容できる	許容できない	少し許容できる
4	少し許容できない	どちらとも言えない	少し許容できない	少し許容できる
5	少し許容できる	少し許容できる	少し許容できない	どちらとも言えない
6	少し許容できる	許容できる	少し許容できない	少し許容できる

表 3 鍵あり・鍵なしの比較

被験者No.	鍵あり・鍵なしについて
1	鍵ありが良いと思う
2	鍵ありが良いと思う
3	鍵ありが良いと思う
4	鍵ありが良いと思う
5	どちらでもない
6	鍵ありがとても良いと思う

表 4 既存方式との比較

	平均所要時間(s)	認証成功率
提案方式	10.69	93.3%
fakePointer	17.35	94.4%
Undercover	45	73.7%
CCC	34.34	91%

今回の実験結果より，物理的な既存動作のメタファを「認証操作におけるフィジカルタスク」に与えることは，ユーザに対して当該フィジカルタスクの実行を自然にかつ適切に促す効果があることが分かった．認証方式に対するユーザの理解促進や利便性向上を目的とした認証インタフェースについて，より深く検討を行なっていく予定である．

参考文献

[1] L.Sobrado, and J.-C.Birget, “Graphical passwords”, The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, Vol.4, 2002.
[2] V. Roth, K. Fischer, and R. Freidinger, “A PIN entry method resilient against shoulder surfing”, In Proceedings of ACM CSS’04, pp.236-245, 2004.
[3] 徐強, 西垣正勝, “ニーモニックに基づくワンタイムパスワード型画像認証の実現可能性に関する検討”, 情報処理学会研究報告 Vol.2006-CSEC-32, pp.317-322, 2006.
[4] 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.
[5] H. Sasamoto, N. Christin, and E. Hayashi, “Undercover: authentication usable in front of prying eyes”, Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI 2008, pp. 183-192, 2008.
[6] 石塚正也, 高田哲司, “CCC:振動機能を応用した携帯端末での個人認証における覗き見攻撃対策手法の提案”, インタラクション 2014(インタラクティブ発表), 2014.
[7] A. De Luca, M. Harbach, E. von Zezschwitz, M.E. Maurer, B.E. Slawik, H. Hussmann, and M. Smith, “Now You See Me, Now You Don’t – Protecting Smartphone Authentication from Shoulder Surfers”, CHI 2014, pp. 2937-2946, 2014.

ⓒ2016 Information Processing Society of Japan