Vol.2018-DPS-174 No.14
Vol.2018-CSEC-80 No.14
2018/3/5

利便性と安全性に配慮した チャレンジ・レスポンス分離型ユーザ認証の提案

遠藤将[†1]　松野宏昭[†1]　村松弘明[†1]　藤田真浩[†2]　西垣正勝[†2]

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存在する．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であり，既存手法の多くでは，チャレンジを覗き見攻撃者から隠すことで安全性を確保するという方法が採られている．しかし，本来チャレンジ&レスポンス型の認証方式ではチャレンジまたはレスポンスのどちらかを隠すことができれば複数回の覗き見攻撃に対して安全性を確保することができる．そこで本研究では，携帯端末の画面からチャレンジを受け渡し，背面カメラを用いてレスポンスの入力をさせることで，チャレンジとレスポンスを同時に盗聴することを防止可能とする覗き見対策手法を提案する．また，背面カメラという操作部が目視できない入力インタフェースにおいて正確な入力を可能とし，覗き見攻撃者には秘密情報に関する情報を一切漏らさないようなフィードバックの与え方について検討する．

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

1. はじめに

スマートフォンの急速な普及に伴い，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，パスワードや PIN（Personal Identification Number），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パスワードや PIN，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．現在までに提案されているチャレンジ&レスポンス型の認証では，チャレンジを覗き見攻撃者の盗聴から隠くしながらユーザに受け渡すことによって安全性を確保するという方法が主に採られている．しかし，本来チャレンジ&レスポンス型の認証では，チャレンジとレスポンスの両方を同時に盗聴されなければ複数回の覗き見攻撃に対して安全性を確保することができる．また，既存のチャレンジ&レスポンス型の認証では，覗き見攻撃者からチャレンジを隠すために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]）を求める方式や専用デバイスの所持を求める方式[5]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，チャレンジの取得とレスポンスの入力を別のインタフェースで行うことで，チャレンジを覗き見可能な攻撃者からはレスポンスを覗き見できず，レスポンスを覗き見可能な攻撃者からはチャレンジを覗き見できないチャレンジ・レスポンス分離型の認証方式を提案する．これは携帯端末の画面にチャレンジを表示し，携帯端末の背面からレスポンスを入力することで実現される．携帯端末の背面からの入力は，現在普及している多くの携帯端末に内蔵されている背面カメラを用いることで実現する．このため，提案方式は専用のセンサやデバイスの追加を必要としない方式となっている．ここで，携帯端末の背面から入力を行うという，ユーザが操作部を目視できない入力インタフェースにおいては、ユーザにとって正確な入力を行うことは比較的難しくなり，利便性の低下につながることが想定される．そこで，ユーザ自身がどのような操作を行っているのかという操作感をユーザに与えつつ，覗き見攻撃者に対しては秘密情報に関する情報を一切与えないようなフィードバックの提示方法について検討する．

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，背面入力インタフェースにおける関連研究について述べる．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 静岡大学大学院総合科学技術研究科
Graduate School of Integrated Science and Technology, Shizuoka University
†2 静岡大学創造科学技術大学院
Graduate School of Science and Technology, Shizuoka University

Vol.2018-DPS-174 No.14
Vol.2018-CSEC-80 No.14
2018/3/5

図 1　fakePointer
Figure 1　fakePointer.

2. 関連研究

2.1 チャレンジ&レスポンス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，チャレンジ&レスポンス型の認証方式にすることが有効である．チャレンジ&レスポンス型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．そこで，毎回のチャレンジに対するレスポンスを人間に計算させるタイプのユーザ認証では，複数回の覗き見攻撃に耐性を持たせるために，主にチャレンジを覗き見攻撃者から隠す方法が採られている．

2.1.1 fakePointer

fakePointer は，安全な環境（覗き見が不可能な通信路）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 4 つの記号で構成され，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，③④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，事前に安全な環境下でチャレンジ（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．

2.1.2 バイブレーション方式

Higashiyama らによって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認証方式（以下、本稿では「バイブレーション方式」と呼称する）が提案されている[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「矢印（8 方向の矢印と矢印無しの 9 つの記号)」と「タップの強さ（強・弱)」の組み合わせで構成された秘密情報 4 組を登録しているものとする．

【手順】

① 1 回短く振動「・」，2 回短く振動「‥」，1 回長く振動「－」の 3 種類のバイブレーションパターンがある．図 2 のように 3×3 のパネルが表示され，左列の 3 枚のパネルに「・」，中央列の 3 枚のパネルに「‥」，右列の 3 枚のパネルに「－」がそれぞれ割り当てられている．

② 認証開始時には 1 行目の「・」「‥」「－」のパネルが青く表示されている．青く表示された 3 枚のパネル（カーソル領域）は認証が開始されると一行ずつ下へ 3 行目まで移動していく．その際，どこかの行で一度バイブレーションが振動する．

③ カーソル領域がどの位置にあるときに，どのバイブレーションパターンで振動するかをシステムが入力毎にランダムに決定する．バイブレーションが振動したときのカーソル領域の位置と振動パターンにより

Vol.2018-DPS-174 No.14
Vol.2018-CSEC-80 No.14
2018/3/5

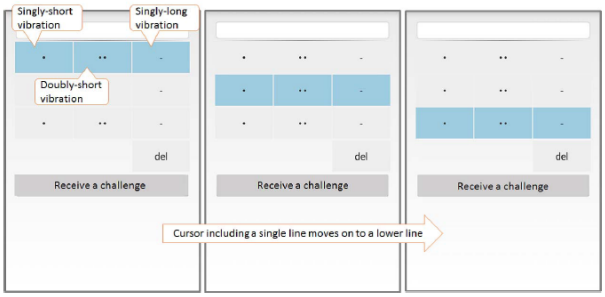

図 2　バイブレーションパターンとカーソル領域移動を用いたチャレンジの取得

Figure 2　Challenge acquisition by vibration pattern and cursor's movement.

一意に特定されたパネルがチャレンジとなる．

④　チャレンジパネルを中心として，1 組目の秘密情報の「矢印」方向にあるパネルを，1 組目の秘密情報の「タップの強さ」でタップする．

⑤　2〜4 組目の秘密情報に対しても②~④の操作を繰り返すことで 4 つの秘密情報の入力を行う．

バイブレーション方式は，バイブレーションの振動音が漏洩しない限り安全な方式となっているが，静かな場面や攻撃者がバイブレーションの振動音を盗聴可能な近さにいる場合，秘密情報が漏洩することになる．また，強弱タップという微細動作を利用する方式は，人間の目視による覗き見攻撃に対しては有効であるが，カメラなどの撮像デバイスによる録画攻撃においては，タップしてから離すまでの時間やタップした指の色変化などを観察することでタップの強弱の判別がついてしまうという問題が存在する．

2.1.3 Undercover

Undercover は，専用デバイス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 5 枚のパス画像を登録しているものとする．

【手順】

①　図 3 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という 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 4）．ユーザは，①で取得した回転方向から，各入力ボタンに割り当てられた数字を求める．

③　ディスプレイに 5 枚の画像が一列に表示される．一番右の画像は「パス画像なし」を意味する．その他の 4 枚にパス画像が存在する場合，パス画像の位置に該当する番号が割り当てられた入力ボタンを押すことでレスポンスの入力を行う．パス画像が存在しない場合，5 番が割り当てられた入力ボタンを押すことで，パス画像なしが選択される．

④　以上を 7 試行（うち 5 試行がパス画像あり，2 試行がパス画像なし）行うことで認証情報の入力が完了する．

図 3　Undercover

Figure 3　Undercover.

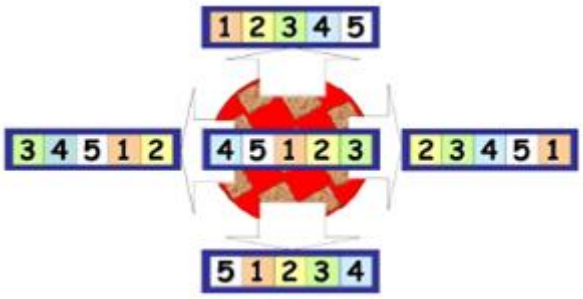

図 4　回転方向によるチャレンジの取得

Figure 4　Challenge acquisition by sensing rotational direction.

Undercover 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，認証を行う端末以外にトラックボールとボタンが設置された機器を所持していなければならない．

2.2 端末背面からの入力インタフェース

2.2.1 LensGesture

LensGesture は，内蔵カメラを入力デバイスとして用いる方式である[7]．LensGesture では操作方法として，Static LensGesture と Dynamic LensGesture という二つの手法が提案されている．

Static LensGesture とは，カメラレンズ全体を覆われている状態，部分的に覆われている状態（左，右，下）の 4 状態によって入力操作を行う手法である．4 状態を識別するために，カメラから取得した映像をリアルタイムで解析し，輝度によってカメラレンズ全体が覆われているかどうかの判定を行い，照度によってカメラレンズが部分的に覆われているかどうかの判定を行っている．

Dynamic LensGesture とは，指がカメラレンズを左右，上

Vol.2018-DPS-174 No.14
Vol.2018-CSEC-80 No.14
2018/3/5

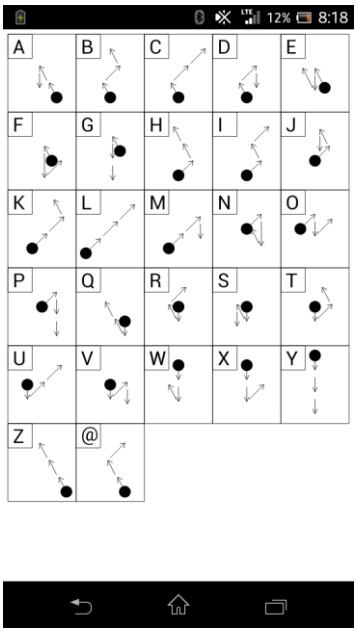

図 5　提案方式の認証画面

Figure 5　Authentication screen of proposed method.

下へ通過する動作によって入力操作を行う手法である．4 動作を識別するために，カメラから取得した映像をリアルタイムで解析し，前後のフレームを比較することで指がどの方向からどの方向へ動かされているかの判定を行っている．

2.2.2 XSide

XSide は，端末背面に設置したタッチパネルを入力デバイスとして用いる方式である[8]．XSide では，認証情報を端末背面のタッチパネルと表面のタッチパネルに分割して入力することで、認証操作の覗き見耐性を確保している．しかし，チャレンジ&レスポンス型の認証方式が採用されていないため複数回の覗き見攻撃に対して脆弱である，現在普及している多くの携帯端末の背面にはタッチパネルが設置されていない，片手での操作が難しい，といった問題が存在する．

3.　提案方式

3.1　攻撃者モデル

本稿では XSide で示されている覗き見攻撃者モデルを想定したうえで，攻撃者が複数回に渡る覗き見攻撃を実行可能であるとして議論を進める．

【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，カメラなどの撮像デバイスによる録画）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．

図 6　カメラを覆った際のフィードバック

Figure 6　Feedback for covering the camera.

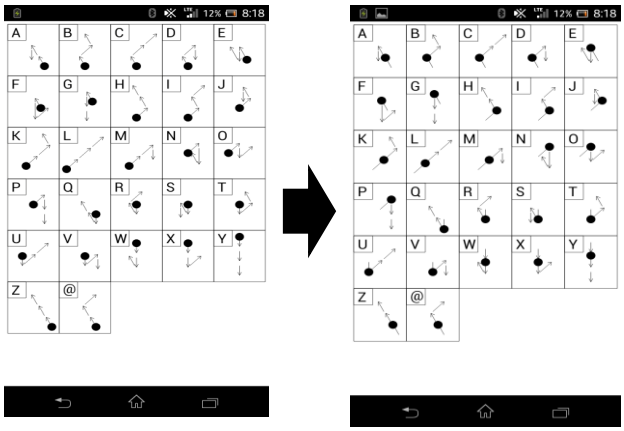

図 7　指の動きに対するボール移動

Figure 7　Feedback for finger movement.

3.2　認証手順

チャレンジを提示するインタフェースとレスポンスを入力するインタフェースを分離することで，安全性（覗き見攻撃者がチャレンジとレスポンスを同時に盗聴することを防ぐ）と利便性（正規ユーザに過大なメンタルタスクを課さない）に配慮したユーザ認証方式を提案する．携帯端末の画面にチャレンジを提示し，チャレンジと秘密情報からレスポンスを求め，求めたレスポンスを端末の背面に設置された内蔵カメラを用いて入力するという方法を採る．現在普及している携帯端末には背面に内蔵カメラが設置されていることが一般的であるため，提案方式は多くの携帯端末に適用可能であると考えられる．

提案方式の認証手順を以下に示す．ユーザは、あらかじめ 27 種類の文字（アルファベット A~Z と記号@）の中から 3 文字を選択し、これを秘密情報として認証システムに登録しているものとする．

【手順】

① 携帯端末のディスプレイ画面に 27 種類の文字（アルファベット A~Z と記号@）が付記された 27 枚のパネルが表示される．各パネルには，システムが毎回ランダムに 3 つの「操作方向」を割り当てる．この操作方向の割り当てがチャレンジとなる．3 つの操作方向は、「ボール」を始点とした 3 本の「矢印」として画面に表示される（図 5）．

② それぞれの「操作方向」は、{左上，右上，下} の 3 種類のいずれかとなる．ユーザは，携帯端末の背面に

設置された内蔵カメラ全体を指で覆った後，秘密情報の 1 文字目の文字に割り当てられた 1 つ目の操作方向（矢印）へ指を動かす．このとき，指はカメラの範囲から完全に抜けないように止める．指の動きに連動して，ボールが矢印の上を移動する．このとき，他の文字および記号に割り当てられたボールも同様に各矢印の上を移動するが，ユーザは自身の文字または記号に割り当てられたボールの動きのみを視線で追うことで正規のフィードバックのみを受け取ることができる．

③ ユーザは，携帯端末の背面に設置された内蔵カメラ全体をもう一度指で覆った後，秘密情報の 1 文字目の文字に割り当てられた 2 つ目の操作方向（矢印）へ指を動かす．指の動きに連動して，ボールが矢印の上を移動する．

④ ユーザは，携帯端末の背面に設置された内蔵カメラ全体を更にもう一度指で覆った後，秘密情報の 1 文字目の文字に割り当てられた 3 つ目の操作方向（矢印）へ指を動かす．指の動きに連動して，ボールが矢印の上を移動する．②～④の操作によって 1 文字目の秘密情報に対するレスポンスを入力する．

⑤ ②～④を秘密情報の文字数だけ繰り返す．

提案方式では，携帯端末の背面方向から覗き見を行う攻撃者に対しては，既存方式のチャレンジ&レスポンス方式と同様にチャレンジを隠した覗き見対策となっているが，さらに、携帯端末の画面方向から覗き見を行う攻撃者に対しても，レスポンスの入力を隠した覗き見対策となっていることに注意されたい．つまり，提案方式においては，携帯端末の画面方向と背面方向という 2 方向から同時に覗き見をされない限り，攻撃者は正規ユーザの秘密情報を盗聴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に対して安全な方式となっている．

提案方式においては，秘密情報と対応する 3 つの操作を確認することでレスポンスの導出が可能であり，過大なメンタルタスクを必要とせずに認証を実行できることが期待される．なお，提案方式は現状，左上，右上，下という 3 状態のみしか判別できていない．そのため，Roth らの認証方式[2]と同様の手法を採り，3 択の操作を繰り返すことでレスポンスを入力するという方法を採っている．

3.3 フィードバック

「携帯端末の背面からの入力」という入力インタフェースのおいては，ユーザは操作部を目視できないため、レスポンスを正確に入力することが難しくなることが想定される．そこで，ユーザ自身がどのような操作を行っているかという操作感をユーザに与えつつ，攻撃者に対しては入力内容に関する情報を一切与えないようなフィードバックの提示方法を検討する必要がある．

前者（ユーザ自身がどのような操作を行っているかという操作感をユーザに与える）に対しては、提案方式では，「①ボール操作が可能になったこと」と「②ボール操作が行われたこと」に関するフィードバックをユーザに返すこととした。①については、カメラ全体を指で覆うという操作に対して,「ボールの色が変化する」というアニメーションをフィードバックとして用いるようにした．具体的には，カメラを覆っていないときには，ボールが黒色で表示される．そして，カメラを覆った状態が一定時間以上維持されると，ボールが赤色に変化する（図 6）．②については，カメラを覆った指を左上，右上，下のいずれかに動かすという操作に対して,「ボールが矢印を辿って移動する」というアニメーションをフィードバックとして用いるようにした．後者（攻撃者に対しては入力内容に関する情報を一切与えない）に対しては，提案方式では，正規のフィードバックの提示と同時に，ダミーとなるフィードバックを提示することとした．認証画面中のすべての文字のパネルにボールと矢印が表示され、それぞれのボールは、すべて同じタイミングで色が変わったり、移動したりする。これにより、表示ディスプレイを見ながら背面カメラを操作しているユーザには正規のフィードバックを特定できるが，表示ディスプレイあるいは背面カメラの一方しか覗き見ができない攻撃者には正規のフィードバックが得らないようにできる（図 7）．

4. 基礎実験

4.1 実験目的

提案方式の利便性，安全性を既存のチャレンジ&レスポンス方式である fakePointer，バイブレーション方式，Undercover の 3 方式と比較することにより調査する．

4.2 実験方法

被験者として情報系の大学生 9 名に対して実験を行う．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い，被験者が自身で慣れたと判断した段階で，9 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を行うために，実験後に質問紙によるアンケートを実施する．アンケートの内容は以下の通りである．既存の 3 方式について紙面による説明をした上でアンケートに回答してもらう．

- fakePointer，バイブレーション方式，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．

4.3 実験システム

提案方式の評価実験を行うため，実験システムのプロトタイプを実装した．実験用携帯端末の仕様は次の通りであ

Vol.2018-DPS-174 No.14
Vol.2018-CSEC-80 No.14
2018/3/5

表 1　実験結果

Table 1　Result of the experiment.

被験者	認証成功率	平均所要時間[s]
1	8/9	8.03
2	9/9	10.46
3	7/9	9.15
4	9/9	9.88
5	9/9	10.37
6	9/9	9.10
7	9/9	6.85
8	8/9	9.16
9	8/9	11.62
全体平均	93.8%(76/81)	9.40

表 2　実験アンケート結果

Table 2　Questionnaire result.

被験者	提案方式	fakePointer	バイブレーション方式	Undercover
1	許容できる	少し許容できない	許容できる	許容できない
2	少し許容できる	どちらとも言えない	少し許容できる	許容できない
3	少し許容できる	少し許容できない	どちらとも言えない	どちらとも言えない
4	少し許容できる	少し許容できない	少し許容できる	少し許容できない
5	少し許容できる	許容できない	少し許容できる	少し許容できない
6	許容できる	どちらとも言えない	許容できる	許容できない
7	許容できる	少し許容できない	少し許容できる	少し許容できない
8	許容できる	少し許容できない	少し許容できる	許容できない
9	許容できる	少し許容できない	少し許容できる	許容できない

る．サイズ：約 140mm（高さ）×約 70mm（幅）×約 10mm（厚さ），重量：約 150g．カメラを覆っているかの判定，および指を動かした方向の判定には，カメラからリアルタイムで得られる画像データを処理した上で指の色情報と輝度情報を用いて判定を行っている．ただし，今回の実験では，指と色情報や輝度情報が近いことによる誤判定や暗い状況において指の色情報や輝度情報が取得できなくなることによる誤判定の可能性を考慮し，背景に誤判定の要因になる可能性があるものが入らないように配慮した上で，明るい部屋で実験を実施する．

4.4 実験結果

実験によって得られた認証成功率と所要時間を表 1 に示す．認証成功率は平均 93.8%、所要時間は平均 9.40 秒であった．アンケートの結果を表 2 に示す．その内訳は以下の通りである．

- 提案方式：「許容できる」5 名，「少し許容できる」4 名，「どちらとも言えない」0 名，「少し許容できない」0 名，「許容できない」0 名．
- fakePointer：「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」2 名，「少し許容できない」6 名，「許容できない」1 名．
- バイブレーション方式：「許容できる」2 名，「少し許容できる」6 名，「どちらとも言えない」1 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」1 名，「少し許容できない」3 名，「許容できない」5 名．

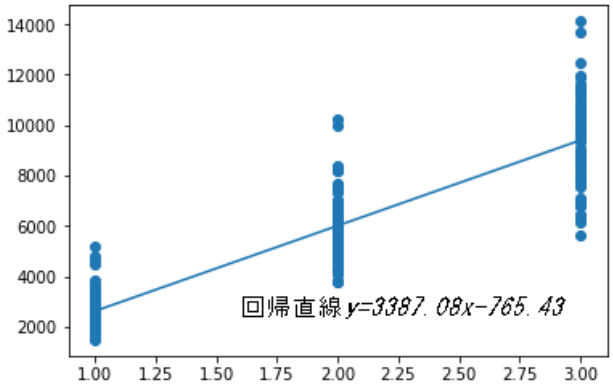

図 8　文字数を説明変数，所要時間を目的変数としたときの回帰直線（縦軸：所要時間[ms]，横軸：文字数）

Figure 8　Regression line (Explanation variable: the number of strings, Objective variable: the time required[ms]).

アンケート結果をスコア化（「許容できない」を 1 点とし，「許容できる」を 5 点とする）したときの各認証方式の平均スコアは大きい順に提案方式が 4.6 点，バイブレーション方式が 4.1 点，fakePointer が 2.1 点，Undercover が 1.6 点となった．また，アンケートにおいて，全被験者が提案方式を既存方式と同等以上に許容できると回答していることが分かる．

5. 考察

5.1 所要時間および認証成功率

平均所要時間を比較するにあたって，ランダム攻撃の成功確率を考慮する必要がある．各認証方式に対するランダム攻撃の成功確率を表に示す．ここで，ランダム攻撃の成功確率は，パスワード 1 文字あたりの入力候補数を M，パスワードの文字数を N とすると，$(1/M)^N$ と表すことができる．例えば，入力文字数を少なくすれば認証にかかる所要時間も短縮可能であるが，同時にランダム攻撃に対する耐性は低減してしまう．そこで，提案方式の 1 文字目から 3 文字目までの各文字を入力するまでにかかった時間から，文字数を説明変数と所要時間を目的変数としたときの回帰式を求め，さらに既存方式におけるランダム攻撃の成功率が，提案方式において何文字で実現されるかを求めることによって，ランダム攻撃に対して同等の安全性を確保した場合の認証所要時間を算出する．この算出された所要時間を用いて比較を行うものとする．

図 8 に線形単回帰分析によって得られた回帰直線を示す（縦軸：認証所要時間[ms]，横軸：文字数）．分析の結果，回帰直線の方程式は $y=3387.08x-765.43$ となることが分かった．また，既存方式によって実現されているランダム攻撃の成功確率が提案方式で実現される桁数は $log_{27}M^N$ によって算出される．この算出された桁数を回帰直線の方程式

表 3　既存方式との比較

Table 3　Comparison with conventional methods.

	ランダム攻撃の成功確率	所要時間[s]	認証成功率
提案方式	(1/10)^4	8.70	93.8%
	(1/18)^4	11.12	
	$(1/{}_7C_2)*(1/4)^5$	9.49	
fakePointer	(1/10)^4	17.35	94.4%
バイブレーション方式	(1/18)^4	7.98	97%
Undercover	$(1/{}_7C_2)*(1/4)^5$	45	73.7%

に代入することで，提案方式において既存方式と同等のランダム攻撃の成功確率を実現するためにかかる所要時間が分かる．

以上より，表 3 に提案方式と既存方式のランダム攻撃の成功確率，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）．ただし，提案方式の所要時間には，各既存方式と同等のランダム攻撃に対する成功確率を実現するためにかかる所要時間を記述している．

提案方式の所要時間について，fakePointer，Undercover と比較すると，ランダム攻撃の成功確率を同等にした際の所要時間が大幅に短縮されているが，バイブレーション方式と比較すると，3 秒程度多く時間がかかることが分かる．本稿における実験では，ユーザに認証の練習回数を委ねたため，被験者間で所要時間にある程度の差が見られた．提案方式は，「背面カメラを用いての入力」という一般的に普及していない入力インタフェースであるため，操作の習得に時間がかかる可能性があり，認証システムの導入フェーズと普段の利用を想定したフェーズを明確に分離した上でユーザ実験を行う必要がある．また，被験者内でも所要時間に差が見られた．提案方式においては、指を動かす速度が速すぎた場合は，背面カメラの撮像範囲から一瞬で指が抜けてしまい、入力のやり直しとなる。これが原因でだと考えられる．対策としては，指の動かす速度をユーザにガイドするように認証画面を改善することが考えられる．

提案方式の認証成功率は，fakePointer やバイブレーション方式と同様に 90%を超える高い認証精度となっていることがわかる．

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，提案方式，バイブレーション方式，fakePointer，Undercover の順に高い結果であった．この結果から，利便性と安全性の両方の面を考慮した場合には，提案方式が最も許容できる方式であることが分かる．しかし，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，被験者に実際に操作してもらった上で比較をしてもらう必要がある．

6. まとめと今後の課題

本稿では，安全性と利便性に配慮したチャレンジ・レスポンス分離型ユーザ認証の提案を行った．実験結果より，提案方式が高い認証成功率を保ちつつ，所要時間の比較的短い認証方式となっていることが確認できた．しかし，実験の設定やユーザインタフェースに改良点が見つかった．この点については, より深く検討を行っていく予定である．

また，提案方式の安全性については，覗き見攻撃に関する実証実験が未実施である．本稿では，画面に表示されたチャレンジと背面に設置された内蔵カメラからのレスポンス入力を同時に盗取できないという前提をおいて議論を進めてきた．しかし実際には，画面と指の動きの両方を盗取できる角度が存在することが考えられる．今後は，覗き見攻撃に対する評価実験を行うとともに，より覗き見攻撃に対して安全な認証方式の検討を行っていきたい．

アンケートからは、利便性と安全性の両方の面を考慮した場合，提案方式が最も許容できる方式であるという結果が得られた．これについては，既存方式を実装した上で，実証実験を通じた比較を行い、結果の信頼度を高めていく．

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] Yuma Higashiyama, Naoto Yanai, Shingo Okamura, Toru Fujiwara, “Revisiting Authentication with Shoulder-Surfing Resistance for Smartphones,” Proceedings of the Third International Symposium on Computing and Networking (CANDAR’15), pp.89-95, 2015.
[7] X. Xiao, T. Han, J. Wang, “LensGesture: augmenting mobile interactions with back-of-device finger gestures”, ICMI 2013, pp.287-294, 2013.
[8] 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.