覗き見耐性を持つマウス操作と数字盤を組み合わせた個人認証方式の提案と評価

坂本 憲理[†1]　長友 誠[†1]　岡崎 直宣[†2]　朴 美娘[†1]

概要：現在，オフィスやネットカフェなどの公共の場において個人認証が多く行われている．その認証方式としてキーボードを用いたパスワード認証が一般的だが，覗き見や録画による認証情報の漏洩が起こりうる．一方，その代替として生体認証が普及している．たとえば指紋認証の場合，指紋センサーが必要であるが，共有 PC ではそれが搭載されていない．そこで本研究では，覗き見耐性を持ち，かつ公共の場において共有 PC でも使用可能な認証方式を提案する．具体的には，マウスを用いて画面上に表示された数字盤内のセルを操作することで認証を行う．マウスを机の下などで隠しながら認証操作を行うことで，覗き見や録画に対する耐性を持つと考えられる．また，提案方式を実装し，アンケートによるユーザビリティ評価と慣れによる認証時間の変化，および覗き見耐性の確認について実験を行った．その結果，認証時間は約 10 秒となり，覗き見によりすべての認証情報が漏洩することはなかった．

キーワード：個人認証，覗き見耐性，マウス

Proposal and Evaluation of Personal Authentication Method Combining Mouse Operation and Number Plate with Shoulder Surfing Resistance

Kensuke Sakamoto[†1]　Makoto Nagatomo[†1]　Naonobu Okazaki[†2]　Mirang Park[†1]

Abstract: Currently, personal authentication has been used in various places such as in an office and cyber cafe. Password authentication using keyboard is one of general methods, but the leakage of authentication information is easy to happen by shoulder surfing or recording. On the other hand, biometric authentication is an alternative. For example, in the case of fingerprint authentication, a fingerprint sensor is necessary, but shared PCs do not equip it. In this paper, we propose an authentication method that has shoulder surfing resistance, can be used with shared PCs and in various places. Specifically, authentication can be done by operating a mouse on the cell of the number plate displayed on the screen. This method is considered to have the resistance of shoulder surfing or recording by hiding the mouse operation under the desk. We also implement the proposed method, and conduct the experiment on usability evaluation by questionnaire in order to confirm shoulder-surfing resistance and reduction of authentication time by repeating. As a result, average authentication time was about 10 seconds and there were no cases of leakage of all authentication information by shoulder surfing.

Keywords: Personal authentication, Shoulder surfing resistance, Mouse

1. はじめに

近年，パスワード認証に替わる認証方式として生体認証が普及し始めている．生体認証には指紋や虹彩などの身体的特徴を用いた認証と署名や歩行などの行動的特徴を用いた認証がある．身体的特徴を用いた認証の場合，認証情報を記憶しなくてもよい利点があるが，専用のセンサーが必要である．また認証情報が漏洩した場合，再登録が難しいという欠点もある．行動的特徴を用いた認証の場合も認証情報を記憶せずに使える利点があるが，認証精度がユーザによって変化してしまう問題がある．また，認証情報として署名を用いる場合，ディスプレイに軌跡が表示されることで，覗き見への耐性が失われる．

一方，オフィスやネットカフェなどの人の出入りが多いところでは，認証中の動作を覗かれることで認証情報が漏洩してしまう問題がある．例えば，銀行の ATM の入力操作を覗かれることでキャッシュカードの暗証番号が漏洩した事例がある[1]．また，店舗内にかかわらず一般家庭にも IP カメラが普及している．これらのうち，覗き見可能な IP カメラのライブ映像を掲載している Web サイトが存在する[2]．そのため，第三者によりカメラを通して覗き見され，認証情報の漏洩が懸念される．これはユーザが認証操作を隠すことで認証情報の漏洩を防ぐことはできるが，一般的にオフィスや公共の場での PC で使われているパスワード認証では，キーボードが使われており認証操作を隠すことは難しい．

現在，覗き見耐性を持つ個人認証方式に関する研究が活

†1 神奈川工科大学
Kanagawa Institute of Technology
†2 宮崎大学
University of Miyazaki

© 2018 Information Processing Society of Japan

発に行われている．例えばタブレットやスマートフォンなどのモバイル端末向けでは，シフト規則や振動機能などを用いた認証方式が提案されている[3],[4],[5]．また，マウス操作を用いた方式[6],[7],[8],[9]では，ソフトウェアキーボードを使う際の覗き見耐性を高めるため複数のダミーカーソルを表示している．しかし，覗き見への対策やユーザビリティの考慮などの課題がある．

そこで以前我々は公共の場において共有 PC で使用可能な，マウス操作を用いた個人認証方式[10]を提案したが，認証成功率が約 60%と低く，ユーザビリティが確保されていない．本論文ではこれを改良し，マウス操作と数字盤を組み合わせた認証方式を提案する．また提案方式を実装し，ユーザビリティ評価・慣れによる認証時間の変化・覗き見耐性の有無の 3 つについて調査する．

以下，2.で関連研究の紹介，3.で提案方式の説明，4.で提案方式の実装を述べる．5.で実験と評価を行い，最後の 6.でまとめと今後の課題について述べる．

2. 関連研究

2.1 覗き見耐性を持つ認証方式

タブレットやスマートフォンなどモバイル端末向けの覗き見耐性を持つ認証方式が研究されている[3],[4],[5]．STDS 認証[3]では，暗証番号やパスワードの代わりにアイコンを用いて認証を行う．シフト規則を使い，本物のアイコンをタップするのではなくあらかじめ決めておいた規則に従いシフト先のアイコンをタップする．覗き見攻撃によりタップしたアイコンが漏洩した場合でも，それは本物のパスワードではないため，覗き見耐性を有している．しかし，ユーザはアイコンの他にシフト規則も覚えておく必要があるため，記憶負荷がかかる．

Puzzle authentication[4]は，4×4 のマトリクスに配置されたセルをスライド操作で入れ替える認証方式である．ユーザは，セルの位置とそこに配置するパスワードとして数字または色を登録する．パスワードとして登録していない数字または色を使うことで間接的にパスワードを入力でき，覗き見耐性を有している．しかし，間接的なスライド操作ができるまで，一定の慣れが必要である．

CCC[5]は，スマートフォンの振動機能とダイヤル操作を用いて 4 桁の暗証番号を入力する認証方式である．認証時に番号を入力するカーソル位置はシステムが決定する．インジケータがダイヤルのつまみ上で回転し，特定のマスに到達するとスマートフォンが振動する．振動した時のインジケータの示すマスが暗証番号を入力するカーソル位置であり，ユーザは暗証番号をカーソルの位置にあわせるように操作し，認証を行う．振動した瞬間を攻撃者が特定するのは困難であり，入力カーソル位置が漏洩しないため，覗き見耐性を有している．しかし，認証はインジケータが 1 周してから操作が可能になるため，平均認証時間が 37.7 秒掛かっている．また，通常の PC で使用する際は振動機能を持つデバイスが必要となる．

PC 向けの認証としてワンタイムパスワードの 1 つであるマトリクス認証がある．マトリクスのセルに数字を配置し，認証を行うごとにランダムで数字が表示される．ユーザはあらかじめ使用するセルの位置とその順番をイメージとして覚えておき，認証時にはキーボードでそのセルの数字を入力する．この時，第三者により入力した数字が盗まれても，認証する毎に異なる数字が配置されるため，覗き見耐性を有する．

この例として，SECUREMATRIX[6]が挙げられる．数字が表示された 4×4 のマトリクス表を 4 つ使用し，ワンタイムパスワードを生成する．認証情報を登録する際，同じ位置を複数使うことができるため，パスワード長が 8 桁でも組み合わせ数は約 280 兆 (64^8)通りである．しかし認証中のキーボード入力とディスプレイに表示されているマトリクスを同時に録画されていた場合，パスワードである登録位置が漏洩する可能性がある．

以上のような問題点を解決するため，我々はマウスを用いた認証方式に着目した．

2.2 マウス操作を用いた認証方式

CursorCamouflage[7],[8]は，ディスプレイに表示されたソフトウェアキーボードを使用し，英数字を入力する認証方式である．認証時には，画面上にリアルカーソルと同じ形状をしたダミーカーソルが複数表示される．リアルカーソルが動くとダミーカーソルも同時にランダムの方向で動くため，覗き見されていた場合でも，どのキーをクリックしたか識別できないようになっており，一定の覗き見耐性を有している．しかし，攻撃者がマウスの動きとカーソルの動きを同時に見ることでリアルカーソルを発見し，認証情報が漏洩する可能性がある．

文献[9]も，CursorCamouflage と同様にソフトウェアキーボードを使用し，複数のダミーカーソルを表示する認証方式である．カーソルに色をつけることによってリアルカーソルを見失わないよう工夫している．しかし，攻撃者もカーソルを追跡しやすくなり，認証情報が漏洩する可能性がある．また実験として，16 個のカーソルを表示し，パスワードが辞書的なものであった場合，攻撃成功率が 15%と高い．

3. 提案方式

3.1 基本コンセプト

この節では，マウス操作を用いた覗き見耐性を持つ認証方式[10]の基本コンセプトについて説明する．入力インターフェースとして 3 ボタンマウス(**図 1**)を使用し，出力インターフェースはディスプレイ上に表示される $N \times N$ のマトリクス(**図 2**)を使用する．なお，マウスは左クリック，右ク

© 2018 Information Processing Society of Japan

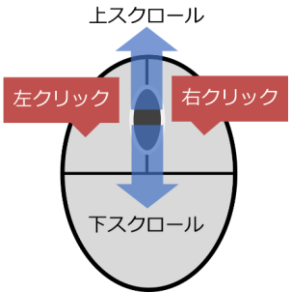

図 1. 入力インターフェース

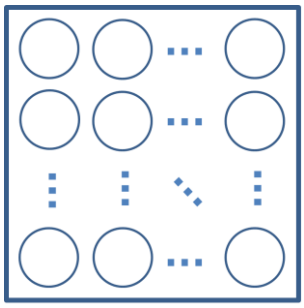
図 2. 出力インターフェース

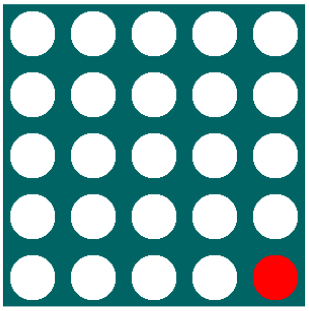
図 3. パターン方式

リック，上スクロール，下スクロール，ホイールクリックができるマウスとする．

認証情報は，マトリクス上の複数セルの位置とその順番である．ユーザはマウス操作で認証情報を登録する．また認証時は，あらかじめ登録した位置をマウス操作で決定する．登録フェーズと認証フェーズは以下のとおりである．

登録フェーズ：

(1) $N \times N$ のマトリクスが表示される．初期位置はランダムで表示される．
(2) 初期位置から登録したい位置までマウス操作のクリックとスクロールで移動する．この時，現在位置の移動の様子がディスプレイに反映される．
(3) 移動後，ホイールクリックで登録する．
(4) 手順(1)~(3)を登録する桁数に応じて繰り返す．

手順(2)のマウス操作において，左クリックは左移動，右クリックは右移動，上スクロールは上移動，下スクロールは下移動にそれぞれ対応する．

認証フェーズ：

(1) 登録時と同じ大きさの $N \times N$ のマトリクスが表示され，初期位置がランダムで表示される．
(2) 初期位置からマウス操作で登録した位置まで移動する．この時，現在位置の移動の様子がディスプレイに反映されることはない．そのためユーザは現在位置を常時把握する必要がある．
(3) 移動後，ホイールクリックで決定する．
(4) 手順(1)~(3)を登録した桁数に応じて繰り返す．
(5) 手順(1)~(4)により決定した位置とその順番が登録位置とその順番に一致した場合，認証成功となる．

この方式の利点は，マウスを机の下などに隠し，覗き見耐性を高めることができる点である．攻撃者はマウスのクリックやスクロールの操作音から登録位置を推測する必要がある．しかし，操作音だけでは移動方向を特定できないため，登録位置を推測できない．

3.2 パターン方式

以前我々は 3.1 節で述べた基本コンセプトに基づいた，パターン方式[10]を提案した．**図 3** にパターン方式の認証画面を示す．1 回の認証で偶然に認証が成功する確率を 1/10,000 以下にすることを目標とし，マトリクスのサイズは 5×5 に設定するとともに，ユーザが登録する認証情報の桁数を 3 桁にしている．

初期位置はランダムに決定され，赤色で塗りつぶされる．ユーザはマウス操作で現在位置を登録した位置まで移動させ決定する．この時，初期位置が登録した位置に近ければ覗き見により登録位置が漏洩する可能性が高くなるため，最低 3 回移動しなければ決定ができないようにした．以下，登録フェーズと認証フェーズを説明する．

登録フェーズ：

(1) 5×5 のマトリクスが表示される．初期位置はランダムで決定され，赤色で塗りつぶされる．
(2) 初期位置からマウス操作で登録したい位置まで移動する．この時，移動するごとに赤色で塗りつぶされるセルを更新する．
(3) 移動後，ホイールクリックで現在位置を登録する．
(4) 手順(1)~(3)を 3 回繰り返す．

認証フェーズ：

(1) 5×5 のマトリクスが表示される．初期位置はランダムで決定され，赤色で塗りつぶされる．
(2) ユーザは事前に登録した位置へ現在位置をマウス操作で移動する．なお，覗き見耐性を高めるため現在位置は表示されない．
(3) 移動後，ホイールクリックで現在位置を決定する．
(4) 手順(1)~(3)を 3 回繰り返す．
(5) 手順(1)~(4)により決定した 3 つの位置が登録位置と一致した場合，認証成功となる．

この方式を実装し，ユーザビリティ評価を行った．そのアンケート結果により，使いやすさとニーズに関する項目が低く被験者全員にとって使いやすい方式とはならなかった．以下アンケート結果を踏まえ，低評価となった理由について述べる．

● 登録フェーズの手間

被験者が認証情報を登録する際，位置を決定するためにクリックやスクロールを複数回行うのは手間だと感じた被験者が複数名いた．

© 2018 Information Processing Society of Japan

● 現在位置の不可視

覗き見耐性を高めるため認証中は現在位置が表示されないため，ユーザは現在位置を常時把握しておく必要がある．しかしユーザがマウス操作を正しく行えなかったことで，ユーザが把握している現在位置と実際の現在位置がずれ，正しく認証できない被験者が複数名いた．

そこで，パターン方式をより使いやすくするため，まず登録フェーズでの操作を再検討した．マウス操作で初期位置から登録したい位置まで移動することなく，マトリクス上のセルを直接指定することで登録できるようにし，ユーザの使用負荷を低減する．

また，現在位置の見える化を検討した．認証中に現在位置が表示されることで，ユーザは現在位置を把握できるが，攻撃者も把握できてしまう．また攻撃者がホイールクリック音によって，認証情報を推測できる可能性がある．そのためマウスを操作しているユーザだけが現在位置を把握できるように工夫を施す必要がある．

これらの課題を解消するために我々は，マウス操作と数字盤を組み合わせた方式（以下，数字盤方式という）を提案する．

3.3 数字盤方式

この方式では位置とその順番に加え，1 つの数字が認証情報となる．数字盤には，マトリクスのサイズに応じた数字をセル上に配置する．配置する数字は重複しないように最小は 1，最大はマトリクスのセル数とする．例えば 5×5 のマトリクスを使用した場合，配置する数字は 1~25 となる(**図 4**) ．また，表示されるすべての数字の桁数を揃える．例えば最大の数字が 25 である場合，1~9 までの数は 10 の位に 0 を表示し，“01~09”のように表示する．これは，数字の表示桁数によって数字の追いやすさが変化しないようにするためである．

ユーザが認証を行う際，登録された数字で示した現在位置をマウス操作で登録位置まで移動させ決定する．すべての数字は，クリックまたはスクロールした方向に移動する．また，この数字盤は上下左右が繋がっているトーラス構造を持つ．例えば右クリックした場合は右端の列の数字が左端に移動し，上スクロールした場合は上端の行の数字が下端に移動する(図 4).

次に数字盤方式における決定時の操作について述べる．マウス操作で数字を登録位置まで移動した後，左または右クリックとホイールクリックを同時に行う．この時，数字はクリックした方向に移動する．このような操作を取り入れた理由は，攻撃者がユーザのマウス音によって決定した位置を識別できないようにするためである．攻撃者に決定したタイミングおよび画面に表示されている数字の配置が同時に把握されると，認証情報が漏洩してしまう．そこで決定時に動きをつけることで，数字を動かす操作と決定の操作との識別ができなくなると考えられる．また同理由により，1 桁入力する度に初期位置の変更はしない．

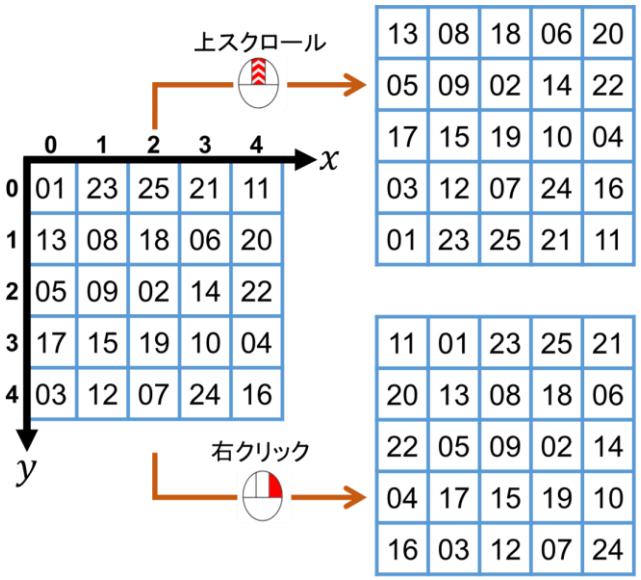

図 4. 数字盤方式と動き方

登録フェーズと認証フェーズは以下のとおりである．

登録フェーズ：

(1) $N \times N$ のマトリクスが表示される．

(2) マトリクス上の登録したい位置を桁数分クリックする．

(3) マトリクスのセル数に対応する数字が一覧で表示され，登録したい数字をクリックする．

認証フェーズ：

(1) 登録時と同じ大きさの $N \times N$ のマトリクスの各セルに数字が配置された数字盤が表示される．

(2) ユーザは登録した数字を見つける．

(3) マウス操作で手順(2)の数字を登録した位置に移動する．この時，ユーザがマウス操作をするごとにすべての数字が同じ方向に移動する．

(4) 移動後，左または右クリックとホイールクリックを同時に行い，現在位置を決定する．

(5) 手順(3),(4)を登録した桁数に応じて繰り返す．

(6) 最後の登録位置が漏洩しないようにするため複数回，マウス操作で数字を移動させる．

(7) 手順(1)~(6)により決定した位置とその順番が登録位置とその順番に一致した場合，認証成功となる．

4. 提案方式の実装

本研究では，3.3 節で提案した数字盤方式を Windows10 の統合開発環境 Eclipse 上で Java 言語を用いて開発を行った．

提案方式を実装する際，マトリクスの大きさと認証情報の桁数を決める必要がある．パターン方式のユーザビリティ評価では，マトリクスのサイズは 5×5，桁数は 3 桁で丁

© 2018 Information Processing Society of Japan

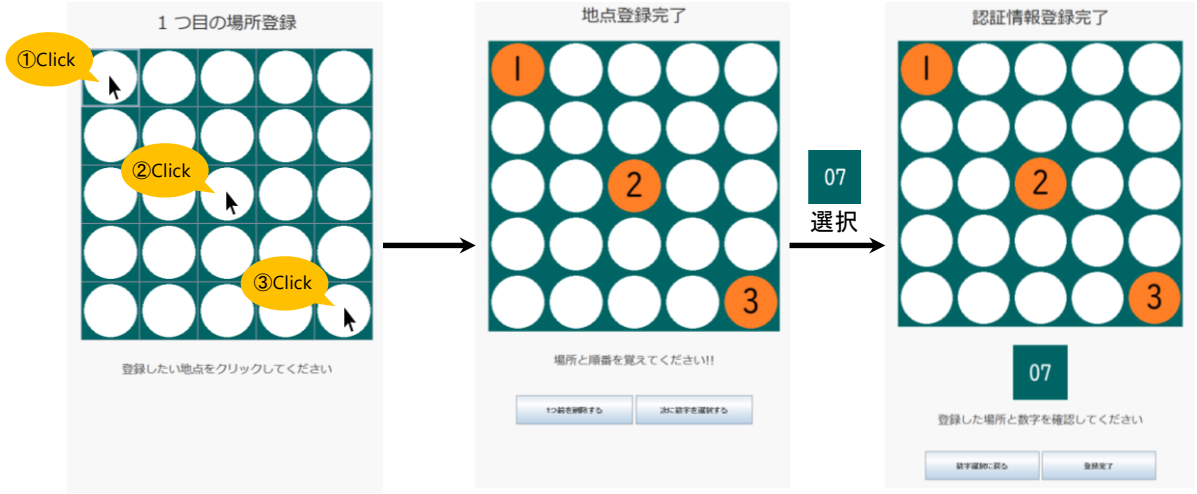

図 5. 登録手順

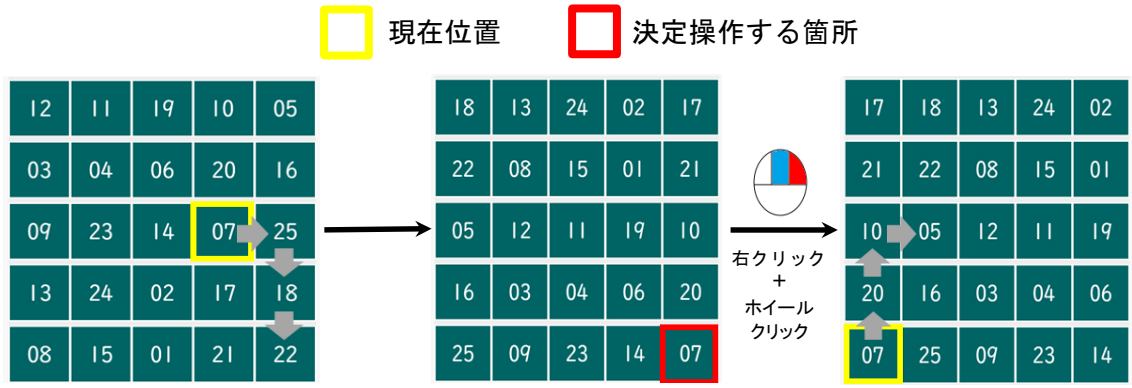

図 6. 認証フェーズの例

度よいとの結果だった．また，パターン方式と数字盤式で比較実験を行うため，数字盤方式のマトリクスサイズも 5×5 にし，認証情報の桁数は 3 桁にした．よって数字盤方式の認証情報の組み合わせ数は$25 \times {}_{25}P_3 = 345{,}000$通りである．以下で登録手順と認証フェーズの例を 1 つずつ挙げる．

登録手順を**図 5** に示す．ユーザが認証情報として座標((0,0)，(2,2)，(4,4))をこの順番にし，数字は“07”で登録を行うと想定する．マトリクス内のセルはすべてボタンになっている．ユーザは 1 桁目に登録したい(0,0)の位置にカーソルを移動し，ボタンをクリックする．クリック後，(0,0)の位置に 1 が表示される．同様に，2 桁目および 3 桁目の位置を登録する．位置の登録が終わった後，01~25 の数字が記載されているボタンの一覧が表示される．ユーザはここで“07”のボタンをクリックする．最後に登録したい位置と順番，そして数字に誤りがないか確認し，登録完了となる．

次に，ユーザは登録した((0,0),(2,2),(4,4))を数字の“07”を用いて認証を行う．まず，01~25 の数字がランダムに配置された 5×5 のマトリクスが表示され，ユーザは登録した数字の“07”の位置を探す．マウスの操作で数字を 1 桁目に登録した(0,0)に移動する．ホイールボタンを押しながら左または右クリックし，1 桁目として決定する．次に 2 桁目の(2,2)に移動し，現在位置を決定する． 2 桁目を決定する時，ホイールクリックしながら右クリックしていた場合，現在位置は(3,2)になる．3 桁目からの認証操作を**図 6** に示す．右クリックを 1 回，下スクロールを 2 回行い，3 桁目に登録した(4,4)まで移動する．この場合，右クリックしながら決定操作を行っているため現在位置は(0,4)になる．ここで 3 桁目の位置を隠すため，マウスを複数回移動する．ここでは上スクロールを 2 回，右クリックを 1 回行う．その後，指定した位置と登録した位置が一致し，認証成功となる．

5. 実験と考察

4 章で実装したアプリケーションを使用し，本研究では，ユーザビリティ評価，慣れによる認証時間の変化の確認，覗き見耐性の有無の確認，の 3 つの実験を行った．すべての実験において机の上に置いた 15.6 インチのノートパソコンを使用する．また，マウスはクリック音が明瞭に聞こえる Microsoft Mobile Mouse3500 を使用する．なお，被験者が認証を行う際には椅子に座り，マウスを机の下に隠しながら操作を行う．

© 2018 Information Processing Society of Japan

5.1 ユーザビリティ評価

この実験では，ユーザビリティ評価を行うため以前我々が提案したパターン方式[10]を再現し，本研究で提案した数字盤方式との比較実験を行う．被験者は大学生 40 名である．計測する項目を以下に述べる．

● 認証にかかった時間

被験者が認証を行う時間を計測する．認証時間が長すぎる場合は操作が複雑であり，使いやすいものとは言えない．

● 認証成功率

被験者全体の認証試行回数のうち正しく認証できた回数の割合を算出する．値が高いほど使いやすいと評価できる．

また，被験者にこれらの認証方式の使いやすさを評価してもらうため，アンケートの 5 項目を 5 段階で回答してもらう．なお，ユーザビリティ評価の比較を行うため，パターン方式と数字盤方式どちらも以下の同じ設問に回答してもらう．

● 認証方式の理解度

実験説明やチュートリアルを通して認証するための操作について理解できたか評価する．

● 使い勝手

認証情報の登録操作や認証操作の使いやすさを評価する．

● 慣れによる使いやすさ

繰り返し認証を行うことで認証操作に慣れ，使いやすくなるか評価する．

● 安全性

後ろから覗かれた場合でも自分の認証情報が漏洩せず，安心して使えるか評価する．

● ニーズ

この認証を再び使いたいか評価する．

また，数字盤方式のみ登録位置の偏りを調べた．数字盤では正方形のマトリクスを用いている．そのため登録情報が覚えやすい中央または四つ角に集中しないか確認する．

5.1.1 実験手順

最初に，マウスを用いた認証方式について説明し，研究目的や基本的なコンセプトの理解を深めてもらう.その後，パターン方式について以下の手順で実験を行う．

(1) 認証情報および操作方法について説明する．
(2) 被験者は認証操作に慣れてもらうためチュートリアルを行う．
(3) 被験者は認証情報を登録する．
(4) 被験者は 5 回の認証を行う．
(5) 被験者はアンケートに回答する．

同様の手順で数字盤方式についても実験を行う．

5.1.2 実験結果

図 7 にそれぞれの方式で認証にかかった回数ごとの平均認証成功時間を示す．数字盤方式のみ 1 回目の認証時間が 30.7 秒と時間が掛かっているが，2 回目以降ではパターン方式とほとんど同じ時間であることが分かる．5 回目ではどちらの方式でも約 15 秒になり，方式による認証時間の差は見られなかった．しかし，数字盤方式において，ユーザは認証開始時に登録数字を見つける必要があるが，パターン方式と認証時間の差がなかった．そのため，パターン方式より数字盤方式の方がマウス操作を簡単に行えると思われる．

また, 認証成功率については, パターン方式の平均が 66%であったが，数字盤方式では 87%となり約 20%向上した．パターン方式では現在位置が表示されないが，数字盤方式では数字を見ることで現在位置を常時把握できるため，認証成功率が向上したと思われる．

図 8 にアンケート結果を示す．すべての項目においてパターン方式より数字盤方式の点数が高い結果となった．特に使い勝手とニーズの項目が向上した．また，後ろから覗かれた場合でも，ユーザのみ現在位置を識別できる工夫を施しているため, 安全性の項目が低下することは無かった．

図 9 に数字盤方式での各登録位置の使用回数を示す．登録された回数が多い位置ほど背景色を濃くしている．今回は正方形のマトリクスを用いたため，覚えやすい四つ角と中心の位置が頻繁に登録されている．今後は，登録位置に偏りを生じさせないようにするため正方形ではない形をしたアウトプットインターフェースを考える必要がある．

5.2 慣れによる認証時間の変化

5.1 節のユーザビリティ評価で認証時間を計測した結果, 回数を重ねるごとに時間が短縮していることが分かった．そこで，日数を増やし繰り返し認証を行うことで操作に慣れたときの，認証時間の変化を確認する実験を行う．実験は日常的に認証を行うことを想定した頻度で行う．具体的には，1 週間に 3 日認証を行い，1 日に 5 回の認証を行うことにした．また，マウスの使用頻度によって認証時間が変化することが考えられるため，その確認も行う．被験者は提案方式をよく理解しているユーザビリティ評価の実験に参加した被験者のうち 33 名で行う．実験を行うごとに，認証時間と判定結果を記録する．実験手順は以下のとおりである．

(1) 初回のみ認証情報の登録を行う．2 回目以降はここで登録した認証情報を使ってもらい, 途中から認証情報の変更は行わない. 被験者が認証情報を忘れた場合は開示を行う．
(2) 1 日に認証操作を 5 回行う．
(3) 手順(2)の内容を週に 3 日で 2 週間行い，合計 6 日間の実験を行う．

図 10 に，日付ごとに被験者全員の平均認証成功時間を算出した結果を示す．具体的には，最初に各被験者の日別平均認証成功時間を計算し，その結果を用いて被験者全員の日別ごとの平均を計算した．また，同時に標準偏差も計算した．

© 2018 Information Processing Society of Japan

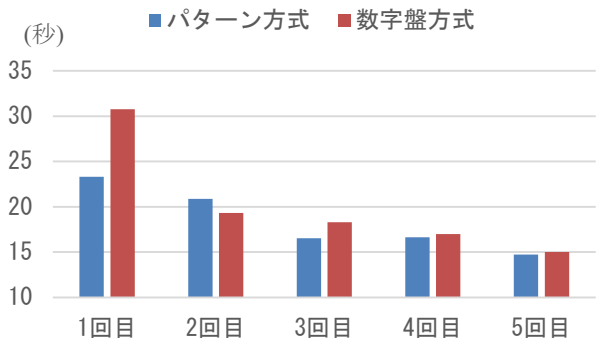

図 7. 認証時間

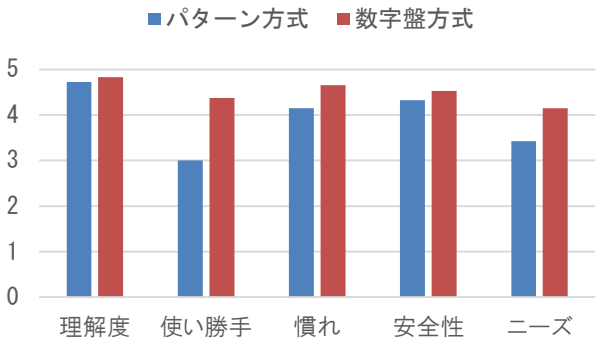

図 8. アンケート結果

13	5	4	1	8
5	4	2	5	4
6	1	8	3	4
1	6	3	2	2
10	3	2	5	13

図 9. 各位置の使用回数

初日の認証平均時間は約 18 秒であり，標準偏差は 6.3 秒であった．また被験者によって認証時間に大きなばらつきが生じた．これはマウスの操作に慣れている人と慣れていない人で認証時間に差が生じたためである．しかし，6 日目になると認証平均時間は約 10 秒となり，標準偏差は 2.6 秒となった．よって，平均時間が短くなるとともに，ばらつきも少なくなった．そのためマウスの使用頻度にかかわらず，認証回数を重ねることによって認証時間が短くなることが分かった．

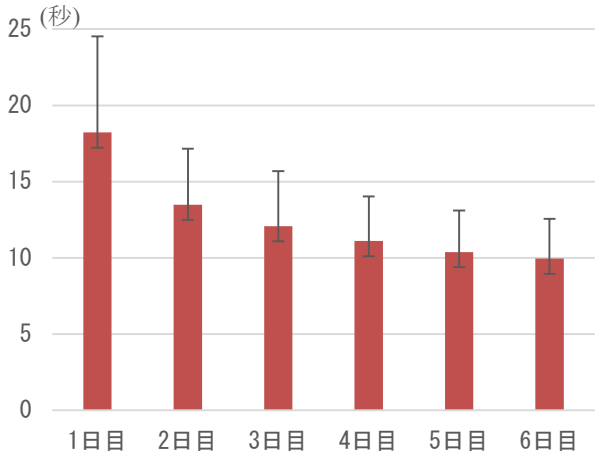

図 10. 慣れによる認証時間と標準偏差の変化

5.3 覗き見耐性の実験

この実験では提案した数字盤方式における覗き見耐性の有無を確認する．**図 11** のように覗き見を行う人は，認証を行う人の背後に立ち，認証画面を覗き見ると同時にマウスのクリック音を聞き，認証情報を推測する．実験は認証画面がよく見え，かつマウスのクリック音が明瞭に聞こえる理想的な状況で行う．被験者は提案方式をよく理解しているユーザビリティ評価の実験に参加した被験者のうち 15 名で行う．今回は，登録した数字が漏洩しなかったケースと数字のみ漏洩したケースを想定した 2 種類の覗き見実験を行う．後者の実験を行う理由は，ユーザが登録した数字を誕生日などの記念日に設定している場合，SNS を通して攻撃者に数字が漏洩する可能性があるためである．

5.3.1 実験手順

(1) 5 人の班を作る．班の中から親を 1 人決める．
(2) 親が 3 桁の認証情報と数字を 1 つ登録する．その他の被験者は登録の様子を見ない．
(3) 親は認証を 10 回成功するまで行う．この時，同じ班の他の被験者は親の後ろから覗き見を行う．
(4) 手順(2),(3)を班の全員が親を終えるまで行う．

数字の漏洩を想定した実験を行う際は，手順(2)の後に親は同じ班の他の被験者に登録した数字を伝える．

5.3.2 実験結果

表 1 に数字が漏洩しなかったケースおよび漏洩したケースの 2 つの実験における各桁数の特定率を示す．特定率は以下の式で算出する．

$$\text{特定率}(\%) = \frac{\text{特定できた人数}}{\text{総試行回数}} \quad (1)$$

ここで特定できた人数とは，位置と順番，あるいは数字が正確に推測できた人のことである．そのため，位置を 1 つに絞れなかった場合は，推測できなかったとみなす．総試行回数は，覗き見を行った人の合計人数であり，今回は 1 回の認証で 4 人が覗き見し，5 回入れ替わる実験を 3 組

© 2018 Information Processing Society of Japan

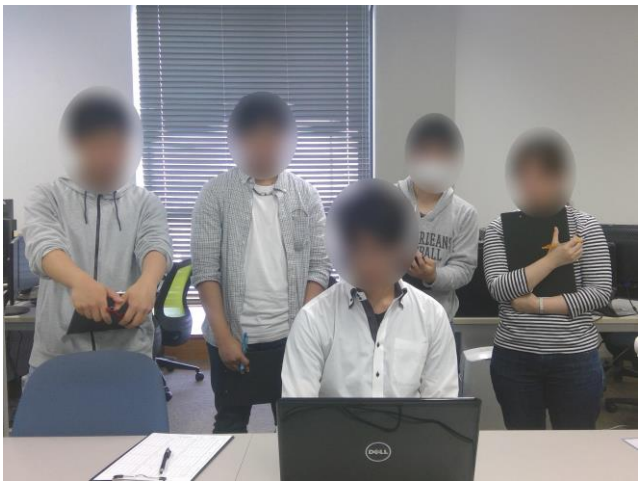

図 11. 覗き見実験の様子

表 1. 10 回覗き見された場合の特定率

	1 桁	2 桁	3 桁	数字
数字の漏洩なし	11.7%	1.7%	0.0%	5.0%
数字の漏洩あり	15.0%	8.3%	6.7%	-

行ったため，$4 \times 5 \times 3 = 60$(回)となる．

数字が漏洩していないケースを想定した実験では，3 桁すべて特定できた人はいなかった．そのため今回提案した数字盤方式は，現在位置が表示されるにもかかわらず，覗き見耐性を有していることが分かった．特定できた被験者は，登録位置が偏りやすい四つ角に着目し，同じ数が頻繁に表示されることから認証情報を推測できたと答えている．

数字が漏洩したケースを想定した実験ではどの桁においても，数字が漏洩しなかったケースに比べて特定率がやや高かった．数字が分かることで現在位置を識別でき，認証を行う毎に同じ位置を通ることで認証情報が推測されたと考えられる．しかしユーザが操作に慣れていた場合は数字の移動が速くなり，覗き見している人が数字を追えなくなることから数字が漏洩した場合でも，一定の覗き見耐性を有していることが分かった．いずれの実験結果においても公共の場で認証を行う場合，攻撃者がマウスのクリック音が聞こえたり，認証動作を 10 回連続して覗いたりするとは考えづらい．そのため，提案した認証方式は覗き見に対する耐性を有していると言える．

6. まとめ

本論文では，公共の場において共有 PC で使用可能なマウス操作と数字盤を組み合わせた個人認証方式を提案した．また提案方式を実装し，ユーザビリティ評価，慣れによる認証時間の変化，そして覗き見耐性の有無について調査を行い考察した．その結果，提案方式の認証成功率は 87%となり，使いやすいことが分かった．認証時間は初回のみ 30 秒要していたが，回数を重ねるごとに操作に慣れ，最終的には平均認証時間が約 10 秒となった．また，事前に数字が漏洩しなかったケースを想定した覗き見実験では，すべての認証情報が漏洩することが無かった．ゆえに提案方式では覗き見耐性を有していることが分かった．今後の課題を以下に述べる．

- 録画耐性の評価

本論文では覗き見耐性のみ評価を行ったが，録画耐性の評価は行っていない．例えば，認証画面を複数回録画することで認証情報が漏洩するかどうかの実験を行う．

- ユーザビリティの改善

数字盤方式では認証開始後，自身の現在位置を見つけるため数字を探さなければならず，認証に時間が掛かる．そこで，数字ではなく記号を使うことにより現在位置を見つけやすくなる可能性がある．

- トラックパッドへの応用

公共の場で自分のノートパソコンを用いて認証を行う際，そもそもマウスを使わないケースがある．マウスの代替としてあらかじめ搭載されているトラックパッドで操作する場合は，操作方法を改良する必要がある．

参考文献

[1] “ATM コーナー・店舗内での犯罪にご注意ください”. http://www.smbc.co.jp/security/attention/index3.html,(参照 2018-08-06).

[2] “Insecam World biggest online cameras directory”. http://www.insecam.org/,(参照 2018-08-06).

[3] 喜多義弘，岡崎直宣，西村広光，鳥井秀幸，岡本剛，朴美娘, “覗き見耐性をも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.

[4] Yoshihiro Kita, Kentaro Aburada, Mirang Park, and Naonobu Okazaki, “Proposal of a puzzle authentication method with shoulder-surfing attack resistance and high-usability,” IEICE ComEX, vol. 4, pp. 95-98, 2015.

[5] 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.

[6] “W ワンタイム 2 要素認証 SECUREMATRIX”. https://www.cseltd.co.jp/product/smx,(参照 2018-08-06).

[7] Keita Watanabe, Fumito Higuchi, Masahiko Inami, and Takeo Igarashi, “CursorCamouflage: Multiple Dummy Cursors as A Defense against Shoulder Surfing,” In SIGGRAPH Asia 2012 Emerging Technologies (SA ‘12), 2012.

[8] 渡邊恵太，樋口文人，稲見昌彦，五十嵐健夫, “複数ダミーカーソル中における自己自身のカーソル特定,” 情報処理学会インタラクション 2013, pp. 25-31, 2013.

[9] Alexander De Luca, Emanuel von Zezschwitz, Laurent Pichler, Heinrich Hussmann, “Using Fake Cursors to Secure On-Screen Password Entry,” CHI2013, pp. 2399-2402, 2013.

[10] Makoto Nagatomo, Yoshihiro Kita, Kentaro Aburada, Naonobu Okazaki, and Mirang Park, “Implementation and user testing of personal authentication having shoulder surfing resistance with mouse operations,” IEICE ComEX, vol. 7, no. 3, pp. 77-82, 2018.

© 2018 Information Processing Society of Japan