Vol.2017-CSEC-78 No.29
Vol.2017-SPT-24 No.29
2017/7/14

覗き見耐性を持つマウス操作を用いた個人認証方式の提案

長友誠[†1]　朴美娘[†1]　岡崎直宣[†2]

概要：現在の個人認証方式として，キーボード入力によるパスワード認証が主に使われる．キーボードによる認証はいくつか問題がある．例えば，覗き見による情報漏洩や，文字数の増加に従って記憶負荷が大きくなることが挙げられる．また，パスワード認証の代わりとして使われる生体認証は，記憶負荷がない利点があるが，生体情報が漏洩すれば，その情報は再登録不可になる欠点がある．本論文では，マウス操作を用いた覗き見と録画耐性を持つ認証方式について検討する．マウスは机の下などで操作可能なので，従来のキーボードによる操作より覗き見や録画耐性を持つと考えられる．ユーザがパスワードとして任意の場所を指定し，それを机の下などでマウスの操作を使い，移動することによって場所を記憶する方式を提案する．また，提案方式を実装し，実験を行うと共にアンケートを実施し，ユーザビリティの評価を行う．

キーワード：マウス認証，覗き見，録画攻撃

Personal Authentication Method Having Shoulder Surfing Resistance by Mouse Operation

MAKOTO NAGATOMO[†1]　MIRANG PARK[†1]　NAONOBU OKAZAKI[†2]

Abstract: As current personal authentication, password authentication by keyboard is mainly used. Authentication by keyboard have some problems of compromise by peep and memory burden by increase of number of characters. In addition, biometric authentication, used as substitute for password authentication, that a user can be authenticated by bodily or behavioral feature have advantage of no memory burden, but have disadvantage that it is impossible to reregister the features when compromise occur. In this paper, we consider authentication methods having shoulder surfing resistance by mouse operation. It is considered that mouse operations have more shoulder surfing resistance than keyboard ones because the user can easily hide the mouse under the desk, handkerchief, and so on than keyboard during authentication. We propose methods that a user can select some positions on matrix using mouse operations. We implement the proposed methods, and perform an experiment and evaluate the proposed method.

Keywords: Mouse Authentication, Shoulder Surfing, Recording Attack

1. はじめに

キーボードによるパスワード認証は，E-mail のパスワードやコンピュータのロックなどで主に使われている．パスワード認証には，文字数の増加と共に記憶負荷が大きくなる問題点がある．例えば，誕生日などのユーザに関する情報がパスワードとして設定されると安全性が低くなる．逆に，意味の無い文字列を設定すればユーザの記憶負荷が大きくなる．そのため，記憶負荷が小さくなる認証としてグラフィカルなパスワードに関する研究が行われている [1, 8, 9]．また，キーボードによるによる認証には録画や覗き見による情報漏洩の危険性がある [3].

そこで，パスワード認証に代わる認証として，身体的特徴や行動的特徴を用いた生体認証が利用されている．身体的特徴による認証には，指紋や光彩による認証があり，行動的特徴を用いた認証には，署名や歩行による認証がある．生体認証の利点として，記憶負荷が無いことやなりすましができない利点があるが，一方で，認証情報が漏えいすれば再登録が不可になることや，行動的特徴による認証では個人で認証精度に差が現れる欠点がある．

また，行動的特徴の生体認証の 1 つとしてマウスによる署名がある [4, 6, 10]．この認証にはいくつか問題点があり，署名に時間がかかることや，録画や覗き見に対する耐性を持っていない問題点がある．録画や覗き見に関しては，署名中に画面の応答を常に受け取りながら認証を行う必要があり，それらを防ぐことは難しい．

そこで，本研究では，覗き見耐性を持つマウス操作を用いた認証方式の提案を行う．この提案方式では，ユーザがマウスを使う事を考え，ホテルなどの公共のパソコンや，職場のパソコン，マウスを付けたノートパソコンで個人認証を行う．

以下，2 章で関連研究の紹介，3 章で提案方式の基本デザインの紹介を行った後，4 章で 3 つの方式を提案し，5 章で提案方式の実験と評価を行う．最後に 6 章で結論と今後の課題を述べる．

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

Vol.2017-CSEC-78 No.29
Vol.2017-SPT-24 No.29
2017/7/14

2. 関連研究

この章では，関連する方式として，提案方式とインタフェースが似ている方式，覗き見耐性を有する方式を紹介する．

2.1 SECUREMATRIX

SECUREMATRIX [2]はマトリックスと数字を使った認証方式である．水平方向に並べられた，4 つの 4×4 のマトリックス中の，順序を踏まえた，指定されたセルの場所が認証情報として登録される．各セルにはランダムに 0 から 9 の数字が表示されており，ユーザは登録したセルの場所の数字をキーボードで打つことにより認証を行う．この方式は，マトリックスの場所を認証情報とする点で，本論文で紹介する提案方式と類似している．

この認証方式の利点は，ユーザが認証情報を場所のイメージとして持つことができるので，ユーザの記憶負荷が少なくなる点があるが，キーボートと画面の録画に弱い欠点がある．

2.2 STDS

STDS (Secret Tap with Double Shift) [11, 12]はアイコンとシフト機能を使ったスマートフォンにおける認証方式である. 認証情報は, ユーザが指定した複数のアイコンである．

認証の際には，ユーザは 4×4 の 16 個のアイコン群を提示され，登録したアイコンから，指定したシフト規則に従って別アイコンをタップする事で認証を行う．

このシフト規則を用いれば，覗き見や録画に対する耐性が高まるが，録画攻撃に対しては，2 回の録画で認証情報が特定される．

2.3 CCC

CCC (Circle Chameleon Cursor) [5]は，スマートフォンにおける，振動を使った覗き見耐性を持つ認証方式である．インタフェースとして，金庫のダイヤルのようなものを用い，ダイヤルを回して数字を指定することによって認証を行う．認証中はダイヤル上のカーソルが回り続け，ランダムに決められた場所へカーソルが来るとスマートフォンが振動する．ユーザは，ダイヤルを回すことで，振動した場所に登録した数字を移動し，認証を行う．

この方式は，振動機能を用いているので覗き見耐性を持つ利点があるが, [5]の実験では認証時間が 34.34 秒であり，4 桁の入力時間であることを考えると長い．

3. 提案方式の基本設計

この章では，覗き見耐性を持つマウスを用いた認証方式を提案する．ここで使用する入力インタフェースは，以下の機能を持つマウスを想定する（図 3.1）．

- 右クリック，左クリック，ホイールクリック
- 上ホイール回転，下ホイール回転
- 上移動，下移動，左移動，右移動

出力インタフェースは N×N のマトリックスとする (図 3.2)．

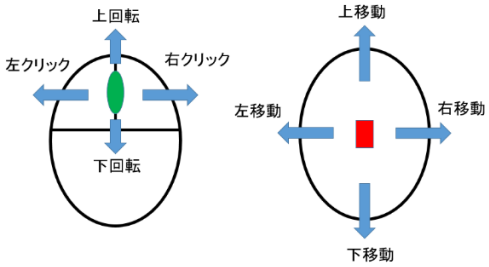


図 3.1 入力インタフェース

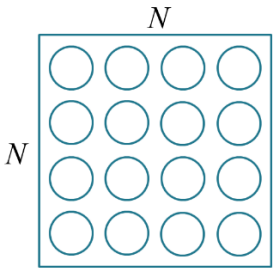


図 3.2 出力インタフェース

次に提案方式の認証手順を以下に示す．

登録段階：

N×N のマトリックスが 1 つ表示される．各セルが持つ情報はそれぞれ異なる．次にマウスクリック，ホイールクリック，ホイール回転，マウス移動を使い，マトリックス上のセルを 1 つ指定する．その後，そのマトリックスは消去される．直後に，N×N のマトリックスが表示され，再びマウス操作を用いてマトリックス上のセルを 1 つ選択する．これを任意の回数繰り返す．このとき，マウス操作に対する応答がマトリックス上に反映され，ユーザは自分が行った操作を確かめながら登録を行うことができる．認証情報としては，指定したセルの情報とその順番が登録される．

認証段階：

登録段階で最初に表示されたものと同じ大きさを持つマトリックスが表示される．ここでも各セルは異なる情報を持つ．次に登録段階と同様に，マウスクリック，ホイールクリック，ホイール回転，マウス移動を使い，登録した情報と同じ情報を持つセルを指定する．そのマトリックスが消去された後，再びマトリックスが表示され，マウス操作を用いてマトリックス上のセルを指定する．これを登録段階で繰り返した回数分繰り返す．ここでは，覗き見に対する耐性を持たせるために，ユーザが行ったマウス操作に対しての応答を画面に表示しない．

この認証方式の利点は，ユーザがマウスを置く場所に自由度があることである．例えば，ユーザは簡単にマウスを机の下に隠しながら認証を行え，覗き見耐性を付けることが出来る．

ここで，この方式がどれくらいの強さを持つかを調べるために，N×N のマトリックスについて，ランダムにパスワードを打ち，1 回で偶然に認証が成功する確率(偶然認証確率)がどのくらいあるのかを考察する．N×N のマトリックス

Vol.2017-CSEC-78 No.29
Vol.2017-SPT-24 No.29
2017/7/14

を用いて m 回登録を行ったとすると，その組み合わせは N^{2m} である．よって，偶然認証確率は $1/N^{2m}$ である．例えば，N=5, m=3 である場合，偶然認証確率は 1/15,625 となる．どのくらいのパスワード強度を持たせたいかをユーザビリティを考慮しながら N と m の値を決める必要がある．

4. 実装・開発

本研究では，上記の基本設計に基づき，3 つの方式を開発した．プログラムは，Windows10 の統合開発環境 Eclipse 上で Java 言語を用いて開発を行った．以下でそれらの方式を紹介する．

4.1 パターン

この方式は，1 つの 5×5 のマトリックス上の場所をマウスクリックとホイールを用いて指定していく方式である．場所だけでなく，登録順番も認証情報に含まれる．以下に認証の詳細な流れを述べる．

登録段階：

1 つの 5×5 のマトリックスが画面に表示される．ユーザはマウス操作を用い，ランダムに決定されたセルからマウス操作を用いてセル間の移動を行い，マトリックス上の任意の場所を指定する．現在選択しているセルは赤色で塗りつぶされる．マウス操作とその効果は以下の通りである(認証段階でも操作と効果の対応は同じ).

- 右クリック：1 つ右のセルへ移動
- 左クリック：1 つ左のセルへ移動
- ホイール上回転：1 つ上のセルへ移動
- ホイール下回転：1 つ下のセルへ移動

加えて，ホイールクリックにより現在選択しているセルの場所を保存することができる．

その後，再びランダムに決定されたセルから任意の場所を指定する操作を行い，ホイールクリックで場所を保存する．これを任意の回数行うことにより，複数の 5×5 のマトリックスの位置とその順番を保存していく．

登録ボタンを押せば保存した場所と順番が認証情報としてまとめて登録される．

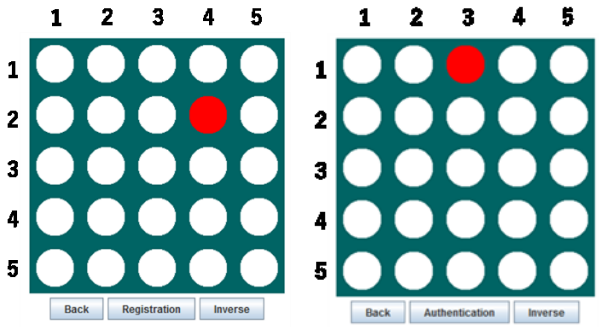
認証段階：

ランダムに決められた初期位置を持つ 5×5 のマトリックスが表示される．次に，マウス操作でセル間の移動を行い，マトリックスの場所の保存を行う．この段階では，登録段階と違い，現在位置のセルに関する情報は画面に表示されない．

ここで，例を 1 つ上げる（図 4.1）．ユーザは，(1, 1)と(5, 1)を登録したいとする．

登録段階：

図 4.1 (a)のマトリックスが表示される．最初にユーザは，左クリックを 3 回，ホイール上回転を 1 回，ホイールクリックを行うことにより，(1, 4)を保存する．次にそのマトリックスは消去され，ランダムに決められた初期位置を持つ 5×5 のマトリックスが再び表示される．マウス操作を用いて (5, 1)を保存し，最後に登録ボタンをクリックすれば，保存した(1, 1)と(5, 1)とその順番が認証情報として登録される．



(a)登録画面　　(b) 認証画面

図 4.1 パターン認証

認証段階：

図 4.1 (b)のマトリックスが表示される．ユーザは，左クリック 2 回とホイールクリックにより，(1, 1)を保存し，再び初期位置がランダムの 5×5 のマトリックスが表示され，マウス操作で(5, 1)を保存する．最後に，認証ボタンを押せば，登録した座標と保存した座標とその順番が一致し，認証が成功する．

4.2 数字と色

この方式では，ユーザが指定した数字と色の組み合わせとその順番が認証情報となる．この方式を提案した理由は，場所より色を覚えやすい人がいると考えたからである．ここでは色が赤，青，緑，黄色で，数字が 1 から 9 とし，その組み合わせが 6×6 のマトリックスのセル上に表示され，初期位置のセルから，登録したい情報を持つセルに移動し，指定することにより，登録や認証を行う(マウスの操作とその効果は前述した「パターン」と同じ)．この方式でも認証情報を登録する順番は認証情報に入る．この方式の詳細な流れを以下に紹介する．ユーザは(4, 黄色)，(8, 緑)を登録したいとする（図 4.2）．

登録段階：

図 4.2 (a)の 6×6 のマトリックスが表示される．各セルはランダムに色が塗られており，その上にランダムに数字が表示される．ただし，色と数字の組み合わせは重複することが無い．最初に，ユーザは上ホイール回転を 1 回行って座標(2, 1)に移動し，ホイールクリックで(4, 黄色)を保存する．次に再びランダムに数字と色の組み合わせが配置された 6×6 のマトリックスが表示され，ランダムに決められた初期位置からマウス操作で(8, 緑)のセルに移動し，ホイールクリックを押し，(8, 緑)を保存する．最後に，登録ボタンを押して認証情報の登録が完了する．この登録段階では，現在選択しているセルは黒の円で囲われ，現在位置を確認できる．

Vol.2017-CSEC-78 No.29
Vol.2017-SPT-24 No.29
2017/7/14

(a)登録画面　　(b) 認証画面

図 4.2. 数字と色による認証

認証段階：

図 4.2 (b)の数字と色がランダムに決められたマトリックスが表示される．最初にユーザは左クリックを 4 回，上ホイール回転を 1 回とホイールクリックを行い，(4, 黄色)を保存する．次にそのマトリックスは消去され，再びランダムに数字と色と初期位置が決められた 6×6 のマトリックスが表示され，マウス操作で(8, 緑)のセルに移動し，ホイールクリックを押すことにより(8, 緑)が保存される．最後に認証ボタンを押せば，登録した情報と合致しているので認証が成功する．

4.3 組み合わせ

この方式では，認証情報は前述した「パターン」と同じで，マトリックスの位置が認証情報として保存される．ただし，位置の指定方法を，マウスクリック，ホイール回転，ホイールクリックとマウス移動の組み合わせ操作を行うことにより，直接マトリックス上の位置を指定する．その組み合わせの数には限りがあるので，今回はマトリックスの大きさを 4×4 に固定する．セルを指定する際は，それぞれの操作に対応する画像を持つセルの操作を行い，指定する．その操作と画像の対応を図 4.3 に示す．

以下で 1 つの例を用い，認証の流れを紹介する（図 4.4）．ユーザは座標(4, 1)と(4, 4)を登録したいとする．

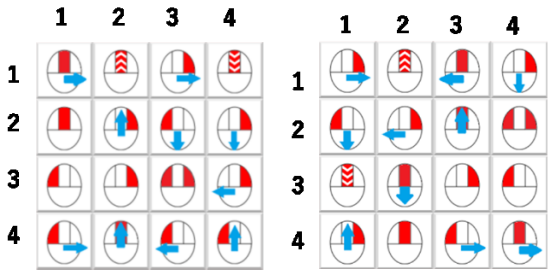
登録段階：

1 つの 4×4 のマトリックスが画面に表示される．各セルには前述したマウスの操作の組み合わせを示した画像がランダムに選出され，表示される（図 4.4 (a)）．最初に，ユーザはホイール下回転を行い，(4, 1)を保存する．再びランダムに画像が表示された 4×4 のマトリックスが表示され，座標(4, 4)に表示されている画像に対応する操作を行い，保存を行う．最後に登録ボタンを押せば登録が完了する．

認証段階：

登録段階と同じように 1 個の 4×4 のマトリックスが表示される．ここでも，セルの画像がランダムに選出される（図 4.4 (b)）．最初に，ユーザはマウス右ボタンを押しながらマウスを下に動かして(4, 1)の保存を行う．次に再び画像がランダムに選ばれた 4×4 のマトリックスが表示され，座標(4, 4)に割り当てられた画像の操作を行い，(4, 4)の保存を行う．

図 4.3. マウス操作の組み合わせ



(a)登録画面　　(b) 認証画面

図 4.4. 組み合わせ認証

最後に認証ボタンを押せば登録した座標と，この段階で保存した座標とその順番が一致し，認証が成功する．

5. 評価

この章では，既存方式と提案方式の比較と，提案方式の 1 つであるパターンについてユーザビリティを測る実験を行い，評価する．

5.1 既存方式との比較

4 章で紹介した 3 つの提案方式について，パスワードの強度は，米国国立標準技術研究所のガイドライン[7]によって定められた，2^{-14} 程度の強度を目指す．パスワードの長さを決めるために，攻撃者がランダムに 1 回パスワードを選択した際に偶然に認証が成功する確率を計算した(偶然認証確率)．表 1 と 2 は 4 章で紹介した「パターン」と「組み合わせ」に対応する 5×5，4×4 のマトリックスと，「数字と色」についての偶然認証確率を示し，表中の赤文字は確率 2^{-14} 程度以下の確率を示している．これらの表より，提案方式の各パスワードの長さを以下のように設定する．

パターン：3 つ以上
数字と色：3 つ以上
組み合わせ：4 つ以上

これを基にし，提案方式とキーボードによる認証，SECUREMATRIX，STDS，CCC をパスワードの組み合わせの数，覗き見耐性，認証情報について以下の条件を仮定して比較，考察をする．その結果を表 3 に示す．

Vol.2017-CSEC-78 No.29
Vol.2017-SPT-24 No.29
2017/7/14

表 1　4×4 と 5×5 のマトリックスの偶然認証確率

偶然認証率	4×4	5×5
2 箇所	1/256	1/625
3 箇所	1/4,096	1/15,625
4 箇所	1/65,536	1/456,161

表 2　数と組み合わせの偶然認証確率

	偶然認証確率
2 つの組み合わせ	1/1,296
3 つの組み合わせ	1/46,656

キーボードによる認証：
パスワードに使える文字は‘a’-‘z’, ‘A’-‘Z’, ‘0’-‘9’の 62 種類，桁数は 8 桁以上．認証の際にキーボードを隠すことはしない．

SECUREMATRIX：
マトリックスの数は 4 つ，桁数は 8 桁以上．認証の時にキーボードを隠さない．

CCC：
桁数は 4(PIN と同様).

STDS：
認証情報は 4 つのアイコンと 2 つのシフト規則.

パターン，数字と色，組み合わせ：
上記で述べた桁数．認証の際，マウスを机の下など他の人が見えない場所に隠す．

キーボードによる認証，SECUREMATRIX と比べると，提案方式は組み合わせ数が少ないが，マウスを机の下などに隠すことができるため, 覗き見耐性を持つと考えられる．

STDS と比べると，提案方式は組み合わせ数が少ないが認証情報をイメージとして覚えることができ，記憶負荷が少ないと考えられる．

CCC と比べると，提案方式は組み合わせの数が多い．しかし, CCC の認証情報は PIN と同様で 4 桁の数字であるため，認証情報を覚えやすい．

5.2　提案方式のユーザビリティの実験と評価

5.2.1 実験

今回の実験では, 提案した 3 つの方式の中で「パターン」のみに絞り，ユーザビリティの評価を行うために実験を行った．被験者は神奈川工科大学に所属する学生 20 名である．実験の流れを以下に述べる．

実験のはじめとして，実験の説明を被験者に行う．その後にユーザ登録をしてもらい，操作に慣れてもらうためチュートリアルを行う．このチュートリアルは，被験者全員の操作性のレベルを揃える目的がある．チュートリアルの中身は図 5.1 に示すとおりで，段階が上がるごとに操作の難易度が上がる．

表 3　提案方式と従来方式の比較

	従来方式				提案方式		
	キーボードによる認証	SECUREMATRIX	STDS	CCC	Pattern	数字と色	組み合わせ
組み合わせの数	62^8 以上	64^8 以上	65,536	10,000	15,625 以上	46,656 以上	65,536 以上
覗き見耐性	×	×	○	○	○	○	○
認証情報	文字列	場所	アイコンとシフト	数字 (PIN と同様)	場所	数字と色の組み合わせ	場所

次に，ユーザは 1 つの 5×5 のマトリックスの任意の場所を 1 つ指定し，このマトリックスが消えた後に再び新たに現れた 5×5 のマトリックスの任意の場所を 1 つ決める．これを更に 1 回行い，合計で 3 つの，5×5 のマトリックスの場所を登録する(図 5.2)（セルの移動方法は「パターン」と同じ）．その後に，認証を実際に行う(図 5.3). 登録または認証の際には，初期位置はランダムで表示され，覗き見耐性を持たせるために，最低 3 回は移動を行わないと場所の保存ができない．最後に，被験者には認証が 3 回成功するまで認証を繰り返し，アンケートを行う．

今回はユーザビリティのみを測る実験であるため，マウスは机の上に置いたままで実験を行った．今後覗き見耐性の実験をする際には，マウスを机の下に隠すなどして認証を行う予定である．

この実験で測る項目は以下の通りである．

● チュートリアルにかかった時間
認証の受け入れやすさを測るため．この時間が短いほどこの認証への理解が早い．

● 認証の際にかかった時間
認証の煩わしさを測るため．操作性が良くてもこの時間が長ければユーザにとって不便である．

● 認証成功確率(認証成功回数/認証試行回数)
操作性を測るため．これが大きければ結果的に認証にかかる時間も確率的に減る．今回の実験では，認証成功回数は 3 で，認証試行回数は 3＋認証が失敗した回数で計算する．

アンケートに関する主項目は以下の通りである．各項目を 1～5 の 5 段階で評価してもらい，ユーザビリティの評価を行う(5 が最高評価で 1 が最低評価とする).

● 認証方法の理解度
チュートリアル内容の改善のため．例えチュートリアルにかかった時間が短くても，チュートリアルの内容が十分でなければこの項目は低くなる．

● 使いやすさ
例え認証成功率が高くても，操作に煩わしさが生じれば使いやすい認証とは言えないため．

● 慣れによる使いやすさの向上
今後，慣れによる認証成功率などの向上を調べる必要があるかどうかを判断するため．

Vol.2017-CSEC-78 No.29
Vol.2017-SPT-24 No.29
2017/7/14

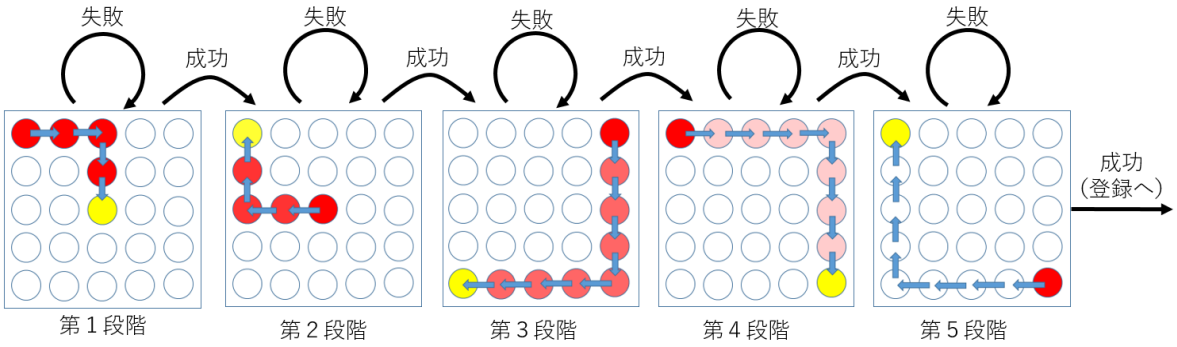


図 5.1　チュートリアル

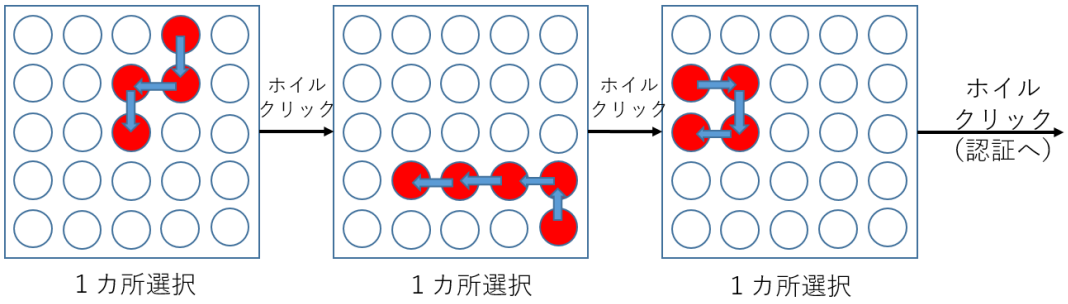


図 5.2 登録実験の例

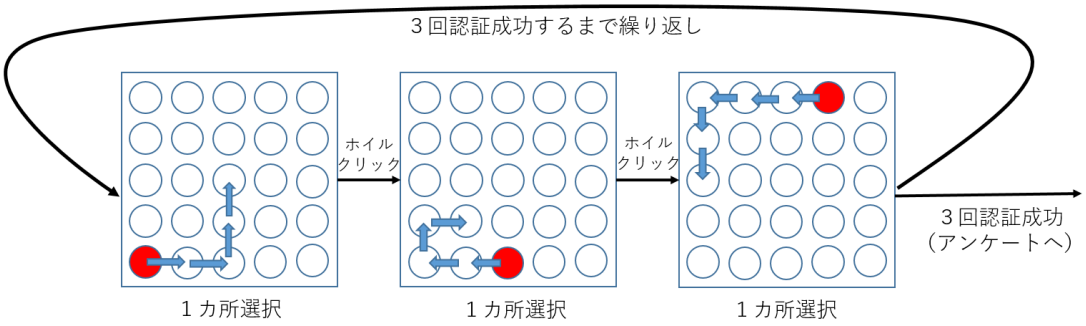


図 5.3　認証実験の例

● 覗き見に対する安全性

今後，覗き見耐性を調べる実験を行うつもりだが，その実験を行う前に提案を修正する必要があるか調べるため．この項目が低ければ安全性を持つ工夫をする必要がある．

● ニーズ (この認証をまた使いたいと思えるか)

印象による認証の受け入れを測るため．この項目が高ければこの方式を実用した際の普及率が高いと考えられる．

上記の 5 項目に付随して，以下の項目をアンケートに追加する．

● 何カ所がちょうど良いか(理想桁数)

ユーザが覚えることができる桁数をあらかじめ知っておくことによって，ある程度のパスワードの強度を得るために，マトリックスの大きさを決めることができる．

● 改善点はあるか

5.2.2 入力時間による評価と考察

図 5.4 にチュートリアルの各段階においてにかかった時間の平均を示す．チュートリアルは段階が上がるごとに難易度が上がるが，認証の際と同じシチュエーションである第 5 段階では時間が多くかかっている．また，チュートリアル全体にかかった時間の平均は 40.7 秒であった．よって，この方式の操作に慣れる時間は多く必要ない．

図 5.5 に 1 回目，2 回目，3 回目の認証が成功した際の入力時間の平均を示す．認証時間とは，ユーザが最初に入力をした時からパスワード 3 つ目の入力が終わるまでの時間を表す．図に示す通り，認証回数が多くなるごとに認証時間は短縮されている．3 回目の認証の平均時間は約 15 秒で，今回は 3 つのパスワードを入力する必要があるため，1 パスワードを入力するのに約 5 秒かかっている計算になる．これは PIN 方式などと比べると遅い．しかし，回数が多くなるに従って認証時間は減少しているので，今後は認証成功回数を増やす実験を行い，認証時間の収束を調べる必要がある．

Vol.2017-CSEC-78 No.29
Vol.2017-SPT-24 No.29
2017/7/14

5.2.3 認証成功率による評価と考察

図 5.6 に各被験者の認証成功率を 25%ずつ区切ったヒストグラムを表す．この実験での認証成功率は，各被験者に対して，3 / 3 回認証が成功するまでに認証を試みた回数，で計算される．25%～50%が一番多い．各被験者の認証成功率の平均を計算すると 63%であった．よって，認証の難易度は高いと考えられる．しかし，今回は時間の都合上 3 回認証が成功するまでしか実験を行っていないため，実際は回数を重ねると更に認証成功率が上がると予想できる．今後は，実際に成功率の収束を実験する必要がある．

5.2.4 アンケートによる評価と考察

図 5.7 に主 5 項目の平均とユーザがちょうどよいと思った桁数(理想桁数)の平均を示す．操作自体は単純で直感的であるため理解度の評価が高い．

覗き見耐性に対する評価は，認証の際に画面に操作に対応する応答が表示されないため，高い．今後は覗き見の実験を行い，本当に覗き見耐性を有しているかを調べる必要がある．

使いやすさの評価については低評価であるが，慣れによる使いやすさは 4 以上であるため，操作性は問題ない．また，ニーズに関しては，平均が 3.4 であるため，使いやすさとニーズを考慮した改善が必要である．

理想桁数に関しては，3 と 2 以外の回答がなく，平均が 2.55 であるため，2 桁または 3 桁が妥当な桁数になる．今後は，認証回数を重ねた場合，理想桁数がどのように収束するかを調べる実験を行う必要がある．

改善点はあるかという質問に対しては，ホイール上下操作が難しい，年齢が高い人も使えるようにすると良い，現在位置が分からなくなった時の対処法があればよいなどの回答をもらった．今後このような改善点を考慮しつつ，提案の修正を行う．

6. おわりに

本研究では，マウスボタンとセンサを使った個人認証方式の提案を行った．提案方式では，認証中のマウス操作に対する応答を画面に表示することなく認証ができるので，覗き見耐性と録画耐性を持つと考えられる．今後の課題を以下に述べる．

- 今回実験しなかった残り 2 つの提案方式のユーザビリティの評価
- 覗き見耐性実験と評価

班を作り，その中で親を決め，親が認証している間は他の班の人が覗き見を行い，パスワードが特定できるか検証する．これを班全員が親を終えるまで行う．

- 慣れによる認証時間と認証成功確率の収束値の検証

同じ被験者に対して 1 週間毎などの認証間隔を決め認証をしてもらい，認証時間と成功確率がどのように変化するかを検証する．

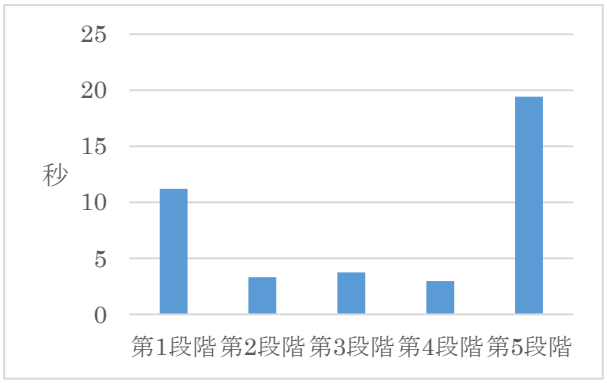


図 5.4 平均チュートリアル時間

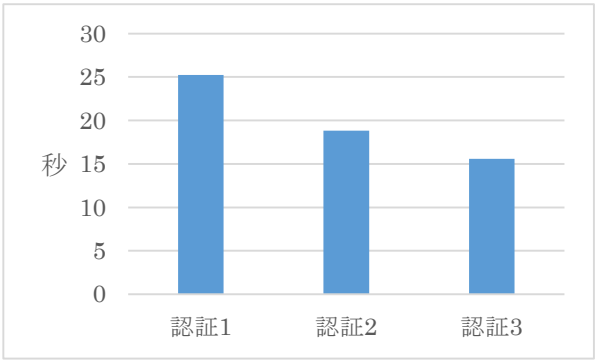


図 5.5 平均認証時間

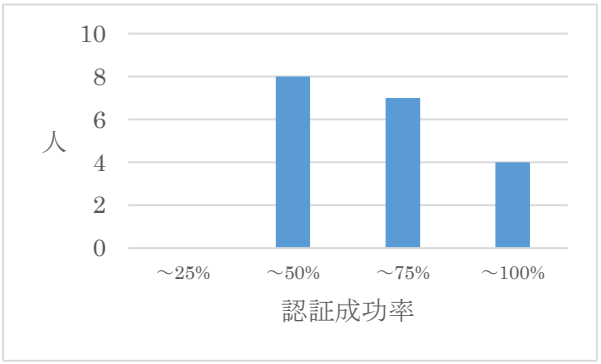


図 5.6 認証成功率のヒストグラム

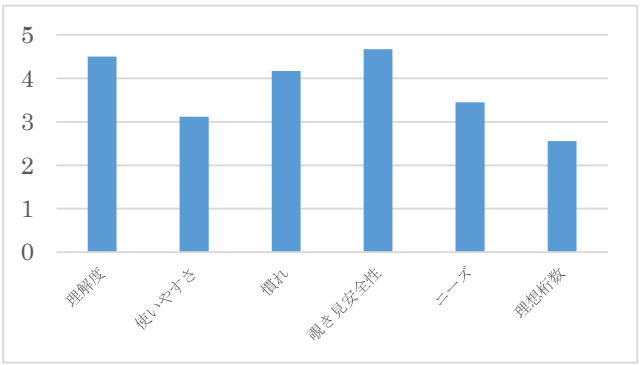


図 5.7 アンケートの評価平均

● 理想桁数の変動に関する実験

同じ被験者に 1 週間ごとに違うパスワードで認証をしてもらう．そのときのユーザの理想桁数の変動を調べることによって，実用的なものに仕上げる際に，認証の回数が上がると今までのパスワードに付随して桁数を増やすことを勧める，などの実装が見込める．そうすることで，認証を使えば使うほどセキュリティが向上していくシステムを作ることができる．

● 関連方式とのユーザビリティの比較

提案方式と関連方式の認証を行い，認証時間や認証成功確率，アンケートの評価を比較する．

参考文献

[1] Claude Castelluccia, Markus Durmuth, Maximilian Golla, Fatma Deniz.. Towards Implicit Visual Memory-Based Authentication, The Network and Distributed System Security Symposium (NDSS). 2017.

[2] “CSE: SECUREMATRIX”. https://www.cseltd.co.jp/product/smx/, (参照 2017-06-5).

[3] Davide Balzarotti, Marco Cova, Giovanni Vigna.. ClearShot: Eavesdropping on Keyboard Input from Video. Proceedings of the 2008 IEEE Symposium on Security and Privacy, 2008, pp. 170-183.

[4] Hansheng Leia, Srinivas Palla, Venu Govindarajua.. Mouse Based Signature Verification for Secure Internet Transactions, Applications of Neural Networks and Machine Learning in Image Processing IX. 2005.

[5] 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, 情報処理学会インタラクション 2014, 2014, pp. 501-503.

[6] Nan Zheng, Aaron Paloski, Haining Wang.: An Efficient User Verification System via Mouse Movements. Proceedings of the 18th ACM conference on Computer and communications security, 2011, pp. 99-110.

[7] NIST special publication 800-63-1 electronic authentication guideline, National Institute of Standards and Technology, 2011.

[8] Nur Haryani Zakaria, David Griffiths, Sacha Brostoff, Jeff Yan.. Shoulder Surfing Defence for Recall-based Graphical Passwords. Symposium on Usable Privacy and Security (SOUPS), 2011, pp.1-12.

[9] Robert Biddle, Sonia Chiasson, P.C. van Oorschot.. Graphical Passwords: Learning from the First Twelve Years. ACM Computing Surveys (CSUR), 2012, pp.1-25.

[10] Ross A, J. Everitt, Peter W. McOwan.. Java-Based Internet Biometric Authentication System. IEEE Transactions on Pattern Analysis and Machine Intelligence vol.25, issue.9, 2003, pp. 1166–1172.

[11] Yoshihiro Kita, Fumio Sugai, Mirang Park.. Proposal and its Evaluation of a Shoulder-Surfing Attack Resistant Authentication Method, Secret Tap with Double Shift. International Journal of Cyber-Security and Digital Forensics (IJCSDF), 2013, vol. 2, no.1, pp. 48-55.

[12] 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, 2014, vol. J97-D, no.12, pp.1770-1784.