タッチスクリーンを利用した覗き見耐性を持つパズル型認証方式の提案

増田 裕仁[1]　喜多 義弘[1]　朴 美娘[1]　岡崎 直宣[2]

概要：近年，スマートフォンなどのモバイル端末の普及率は上がり続けており，それにより個人情報の情報漏洩などが懸念されている．個人情報の漏洩を防ぐために現在の個人認証では，PIN 方式やパスワード方式，パターン方式などが使われている．しかし，これらの認証では，覗き見により認証情報が盗まれ，個人情報が漏洩する可能性がある．そこで，本研究では，覗き見による情報漏洩を防ぐために，従来のパスワード方式による認証に位置とパズルの要素を組み込み，パスワードを指定した位置に揃えるといった認証を提案する．また，提案方式の評価実験を行い，覗き見耐性の評価と考察を行った．その結果，提案方式では認証時に覗き見を行われた場合でも，第三者に認証情報となる位置とパスワードが特定されないことが分かった．このことから，提案方式は覗き見耐性を十分に有していると考えられる．

A Puzzle Authentication Method with Shoulder Surfing Attack Resistance using Touch-Screen

Yuji Masuda[1]　Yoshihiro Kita[1]　Mirang Park[1]　Naonobu Okazaki[2]

1. はじめに

近年，スマートフォンやタブレットなどのモバイル端末が広く普及している．これらの端末は，以前の携帯電話に比べ機能や性能が上がり，電話，メールだけでなく，データ通信，アプリ，動画視聴などパソコンに近い形で使用できるようになってきている．

従って，従来の PC と同様に，モバイル端末の内部の情報が外部に流出されないように，現在，スマートフォンやタブレットにおけるロック機能には，パスワード認証，PIN 認証，パターン認証などが主に使われている．

しかし，これらの認証を公共の場で使用するときには第三者に覗き見をされ，入力した認証情報が盗まれるショルダーハッキング攻撃を受ける問題がある．

このような問題を解決するために，複数回の覗き見耐性を有するパスワード認証[1]や，覗き見・盗撮に耐性を持つパスワード認証[2]，映像記録による覗き見攻撃にも安全な認証手法[3]という研究がある．

しかし，これらの研究では，偶然による認証確率が高くなる，複数回録画された場合回数が増えるごとにパスワードが絞られてしまう，認証者への記憶負担が大きくなってユーザビリティが下がってしまうなどの問題がある．

そこで，本研究では，覗き見による認証情報の流出を防ぐと共にユーザビリティを向上させることを目的とする．そこで，従来のパスワード認証方式にパズルの要素を付加して，認証者だけが知る認証位置を指定することにより，覗き見によるパスワードの流出を防ぐ方式を提案する．また，提案方式を Android 端末に実装し，覗き見耐性および録画耐性の評価を行う．また，ユーザビリティに対する評価を行うためにアンケートを実施する．

その結果，認証時の録画攻撃による回数が増えるほど，位置とパスワードが特定されてしまう可能性があることや認証にかかる時間が長くなるなどの問題があるが，覗き見により認証情報を盗まれる可能性が低いことがわかった．これにより，本研究で提案する方式は覗き見攻撃により認証情報が盗まれることを防ぐことができることが期待される．

†1 神奈川工科大学
Kanagawa Institute of Technology, Atsugi, Kanagawa 243-0292,Japan
†2 宮崎大学
University of Miyazaki, Miyazaki 889-2192,Japan

2. 従来の認証方式

2.1 パスワード認証方式

現在，認証方式において最も汎用的に使われている方式がパスワード認証方式である．パスワード認証方式では，まず，ユーザーが半角英数字，記号を含む文字列をシステム側に登録する．認証時にはユーザーが登録しておいた文字列を入力し，システム側に登録されているものと一致すれば認証が成功になる．パスワードに関しては半角英数字，記号を含む 8 桁以上が推奨されている．また，定期的に変更することも推奨されている．

しかし，パスワードに記号なども含む場合，ユーザーが覚えられないためパスワードを短くしたり，名前や生年月日など覚えやすいものにしてしまう場合がある．そうすると，総当たり攻撃や辞書攻撃によりパスワードを他人に知られてしまう可能性があるため，辞書に掲載されている単語の組み合わせや，数字のみといった組み合わせは避けるべきとしている．

パスワード認証方式の利点としては，ユーザーは認証時に登録したパスワードを入力するだけでよいという点や，システム導入のコストが低いことが挙げられる．欠点としては，パスワードを忘れてしまうことや，覗き見攻撃によりパスワードを他人に知られてしまう問題などがある．

2.2 PIN 方式

PIN(Personal Identification Number)方式というのは，個人識別番号のことであり，0～9 の数字を使用し，その中から 4 桁から 12 桁のパスワードを設定して認証を行う方式であ

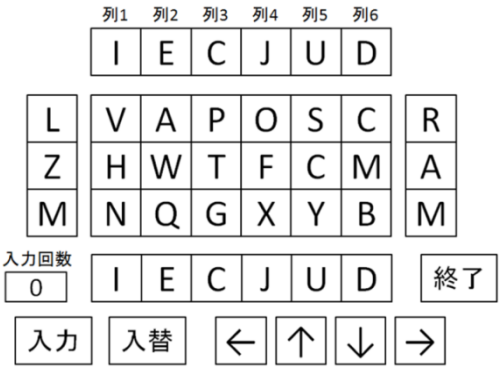

図 2.1 覗き見・盗撮に耐性を持つパスワード認証

る．この方式の利点としては，使用している文字列が数字のみであるため，ユーザーが覚えやすいところである．しかし，パスワード方式と同様，覗き見や録画耐性がなく，さらには総当たり攻撃にも弱いため，パスワードを盗まれる可能性が高くなる問題がある．

2.3 パターン方式

パターン認証方式は，Android 端末に標準で搭載されている認証方式として，9 つの点からユーザーが決めたルートに沿って線を描いて認証を行う方式である．ただし，各点を通れる回数は 1 度だけであり，4 つ以上の点を通る必要ある．

この方式の問題点としては，ユーザーは，設定した通りに線をなぞればよいのでユーザビリティは高いが，複雑なパターンになり過ぎるとパターンを忘れてしまう恐れがある．さらには，第三者に簡単なパターンを覗き見されてしまうと，すぐに認証情報が漏洩してしまうという問題がある．

2.4 複数回の覗き見耐性を有するパスワード認証方式 (FCTG)[1]

この方式は, Faked Cognitive Trapdoor Game(FCTG)と呼ばれるものとして，0 から 9 の数字の中から 8 桁の数字が左右 4 桁ずつ配置される．ユーザーは設定したパスワードが含まれる方向を判別し，含まれている方向が右ならば右のボタン，左ならば左のボタンを押し，左右どちらにも含まれていなければ偽入力を行う．

この認証方式は，複数回の覗き見耐性を有しているが，入力情報が「左」,「右」のみであるため，1 回ごとの偶然認証成功確率が 1/2 であり，偶然による認証成功確率が高くなってしまうという問題がある．

2.5 覗き見・盗撮に耐性を持つパスワード認証[2]

図 2.1 に示すようにこの方式は，ユーザーが予め 4 桁の英文字パスワードとパスワードの指定列を登録しておき，認証画面では画面内から登録した英文字を探し出し，その文字を指定した列に移動する．この入力をパスワードの桁数分繰り返し，すべてのパスワードが指定列にあれば認証が成功する．

この認証方式では，攻撃者が認証画面を覗いたとしても，ユーザーの指定列が分からない限り，1 桁につき最大で 18 通りのパスワード候補が得られるだけである．よって，パスワード桁数が 4 桁の場合パスワードの総数が 18 の 4 乗になるため，覗き見耐性を持つ．

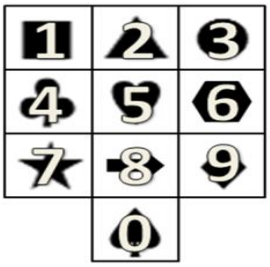
図 2.2 fakePointer 認証の画面

しかし，複数回，カメラなどで録画された場合，回数が増えるごとにパスワードを絞り込むことができてしまうという問題がある．

2.6 fakePointer:映像記録による覗き見攻撃にも安全な認証手法[3]

この方式では, 認証者は認証前に回答選択情報を取得し，回答選択情報に含まれている記号を覚える．その後，上位層に表示されている数字キーの配置をキー操作により変更し，認証者は回答選択情報の上に暗証番号が重なるように配置を変更し，決定キーを押す．例えば図 2.2 で回答選択情報が三角の記号で，この状態で決定キーを押した場合，入力された数字は 2 になる．

この認証方式では，回答選択情報が漏洩した場合でも，認証行為に関する映像記録が攻撃者にわたらない限り安全性に影響はなく，認証行為複数回分の映像記録が漏洩した場合でも，パスワードを特定することができない．

しかし，この認証方式では，認証選択情報とパスワードの両方を認証者は覚えなくてはならないため，認証者への記憶負担が大きいという問題がある．

3. 提案方式

3.1 目的と設計方針

本研究では，覗き見による情報漏洩を防ぐために，位置とパズルの要素を加えた認証方式を提案する．提案方式は，次の設計方針に基づくものとする．

- 覗き見耐性

  複数回の覗き見をされても認証情報が盗み取られないことを目標とする．

- 録画耐性

  ここでの録画耐性というのは，ビデオカメラなどによる動画ではなく，カメラなどによる静止画対策を考える．

  2 回以上の録画耐性を有するように設計を行うと，ユーザーが記憶する位置とパスワードの桁数が増え，ユーザビリティが悪くなってしまうため，今回は 1 回の録画攻撃に耐性を持つことを目標とする．

- 偶然認証耐性

  2.2 節で説明した PIN 方式の 4 桁に相当する，偶然認証の確率 1/10000 の強度を目標とする．

- ユーザビリティ

  ユーザーに入力の記憶負荷がかからない認証方式を目指す．

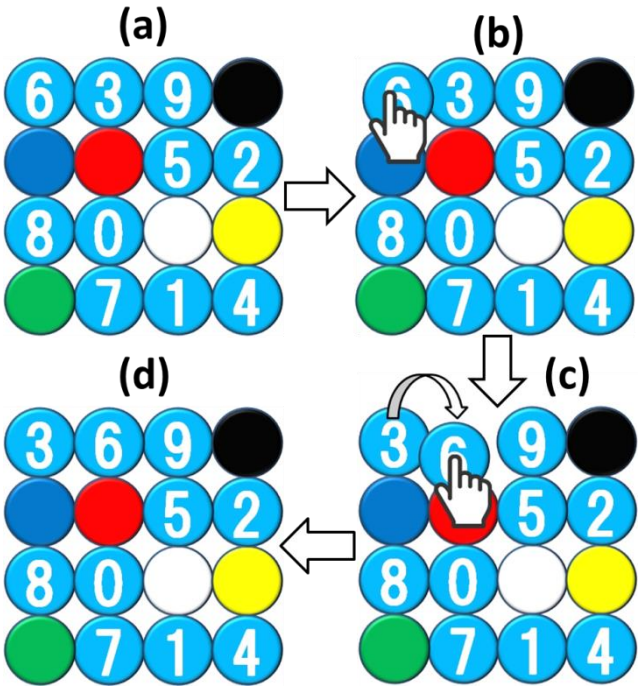

図 3.1 本提案方式のマスの動作

3.2 覗き見耐性を持つパズル型認証方式の提案

提案方式では，認証画面が 0 から 9 の数字と赤，青，緑，黄，黒，白のマスを 4×4 の四角形に配置し，認証画面に表示されているマスのいずれか 1 つをタッチし，そのまま上下左右又は斜めへ自由にスライドさせて認証を行う．最初に，ユーザーは認証のための位置とパスワードを登録する．認証開始時に 0 から 9 の数字と赤，青，緑，黄，黒，白のマスがランダムに表示されるので，ユーザーは登録したパスワードの位置を確認する．その後，認証画面に表示されているマスを 1 つ選択し，そのマスをタッチした後にスライドをさせて，上下左右斜めの数字と入れ替えながら，登録した位置とパスワードを合わせる．

例として，数字のマスおよび色のマスの動かし方を図 3.1 にて説明する．(a)のような画面で(b)は画面上の数字の 6 を押した時の画面である．マスを 1 秒ほど押したままにすると，押しているマスが半透明になり，固定されていたマスから少し浮かび上がり，そのマスをドラッグで動かすことができる．この状態から 6 を右のマスに移動させると(c)に元々6 の隣にあった 3 の数字と入れ替えることができる．この動きは上下左右斜めに数字または色のマスが存在していれば，どの方向でも可能である．さらに，画面上から指を離さない限り，他のマスへ動かし何度でも隣のマスと(d)のように入れ替えることができる．そして，この地点で指を離すと，6 と 3 のマスが入れ替わった状態になる．

この認証方式では，位置とパスワードを認証情報として登録する．位置については，図 3.2 のようにユーザーが任意の 4 ヶ所を登録することができる．赤い丸で囲まれている位置が，ユーザーが登録した位置である．

位置は必ず 4 ヶ所を登録しなければならないため，同じ場所を複数登録することはできない．

位置については，16 ヶ所の中からユーザーが任意で 4 ヶ所選ぶことから，位置登録のパターンの総数は ${}_{16}C_4$=1820 通りになる．

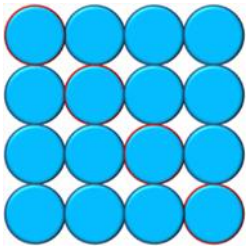

図 3.2 位置登録例の画面

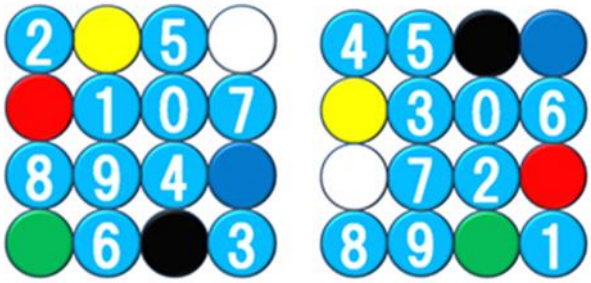

図 3.3 認証成功画面

パスワード登録に関しては，登録した位置にパスワードを合わせるため，パスワードは位置の数と同じく 4 個使用する．パスワードは登録した位置ごとに移動するのではなく，登録した位置にパスワードが含まれていれば，認証成功としている．一例を挙げると，パスワードを「1234」，位置を図 3.2 のように登録を行ったとする．その場合，最終的な配置が図 3.3 のようにパスワードの順番が違う場合でも認証成功になる．

パスワードについては，位置と同じく 16 個の中からユーザーが任意で 4 個選ぶため，パスワード登録パターンの総数は ${}_{16}C_4$=1820 通りになる．もし，この認証方式で位置を固定したまま登録するパスワードを 8 個とすると，認証を同時に 2 画面で行うことになる．その場合，登録するパスワードパターンの総数は ${}_{16}C_8 \times {}_{16}C_4$ =12870 × 1820=23423400 通りになる．

4. 実装

今回の提案方式を実現させるために， 実装には Java 言語を用いて，開発ソフトは Eclipse を使用した．デバッグに使用した端末は AndroidOS 4.1.2 である．図 4.1 に認証画面から位置の設定画面，パスワードの設定画面を示す．

図 4.1(a)の「並べ替える」ボタンを押すと，数字と色のマスの配置をランダムに置き換えることができる．これは，最初に現れたランダム配置が自分の設定した位置と離れた位置にある場合や，移動が困難であると判断した場合に使用される．

図 4.1(b)に位置の設定画面を示す．位置を登録する場合は，ユーザーは登録したい位置のマスをタップする．「戻る」ボタンを押すと，認証画面に戻る．

図 4.1(c)に位置選択時の画面を示す．登録するパスワードのマスが 4 つの場合，登録する位置も 4 か所になる．タップを行ったマスは枠が赤くなり，登録位置の 1 カ所として登録される．4 カ所を押すと位置が 4 か所登録され，パスワード設定画面へ移行する．

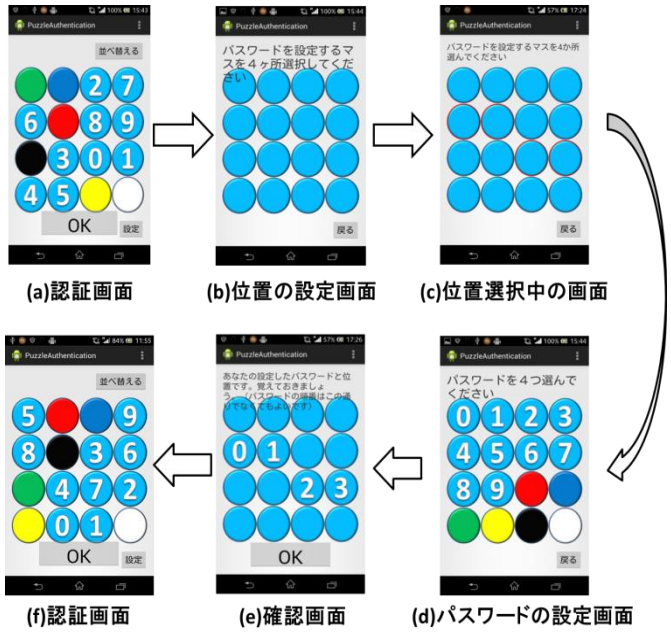

図 4.1 認証画面設定

図 4.1(d)にパスワードの設定画面を示す．パスワードを登録する場合は，位置と同様にユーザーは選択したいパスワードのマスをタップする．「戻る」ボタンを押すと，位置選択画面に戻る．登録するパスワードが 4 つの場合，ユーザーは 4 つの数字，または色のマスを選択する．4 つのパスワードを選択し終えると，パスワードのマスが 4 つ登録される．その後，図 4.1(e)の確認画面が表示され，OK ボタンを押すと認証画面へ移行する．

図 4.2 に認証成功画面と失敗画面を示す．認証に成功した場合は「認証成功」と表示され，認証が成功になる．認証に失敗した場合は「認証失敗」と表示され，認証が失敗になる．

5. 評価

5.1 覗き見耐性に対する評価

認証方式の覗き見耐性を評価するために評価実験を行った．実験では，神奈川工科大学情報学部の学生 15 人を被験者として行った．

実験方法としては，認証者 1 人，覗き見をする人 14 人に分かれて実験を行う．

次に，認証者は位置とパスワードの登録を行った後，覗き見をする人は認証者の認証画面が見える位置に立ち，覗き見を行う．認証者は認証を 5 回行い，その間に覗き見をする人は位置とパスワードを特定することができるかの検証を行った．

実験の結果，位置とパスワードを全て特定できた人は 1 人もいなかった．これにより，認証方式は第三者による覗き見に十分な耐性を有していると言える．

5.2 録画耐性に対する評価

まず，1 回の録画攻撃をされた場合を想定する．その場合，最初に考えられる問題は，位置とパスワードを固定しているため，認証成功時の数字と色を，次回の認証で同じように再現を行うことで認証が通ってしまうという問題が考えられる．ただし，この方法だと前回の認証を再現するのに長い時間がかかるため，対策としては，認証に時間制限を設けることが有効である．

図 4.2 認証成功と失敗画面

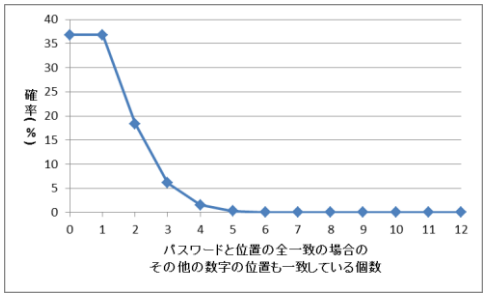

図 5.1 パスワードと位置の全一致の場合のその他の数字の一致数による確率の変化図

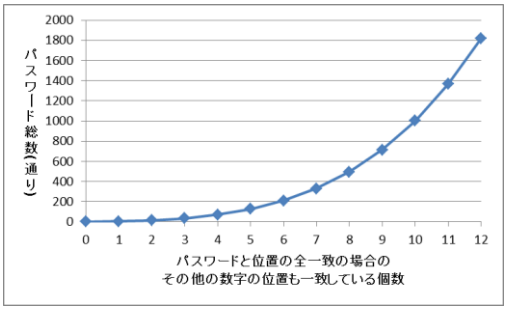

図 5.2 パスワードと位置の全一致の場合とその他の数字の一致数によるパスワード総数の変化図

他には，マスを何度でも動かす方式ではなく，一筆書きの要領で動かすように変更，すなわち動かせるマスを毎回の認証で 1 個のみにすることがもう一つの有効な手段として考えられる．

次に，録画攻撃を 2 回行われた場合を想定する．この認証方式では，録画攻撃に対する対策として，パスワードを揃える位置は固定であるが，その位置におけるパスワードの順番は一致しなくてもよいとしている．しかし，この方式でも，低確率で 2 回の録画を行っただけで位置とパスワードの両方を特定される可能性がある．そのパターンとしては，ユーザーが意識せずに認証を行い，2 回の認証ともに全てのパスワードと位置が一致している場合である．4 個のパスワードの順番が 2 回とも一致する確率は 1/4!，よって1/24となり，約 4.17%になる．しかし，他の数字も複数一致していた場合，特定することは困難になるため，僅かではあるが，この確率よりはもう少し低くなる．2 回の録画における，パスワードと位置の全一致の場合のその他

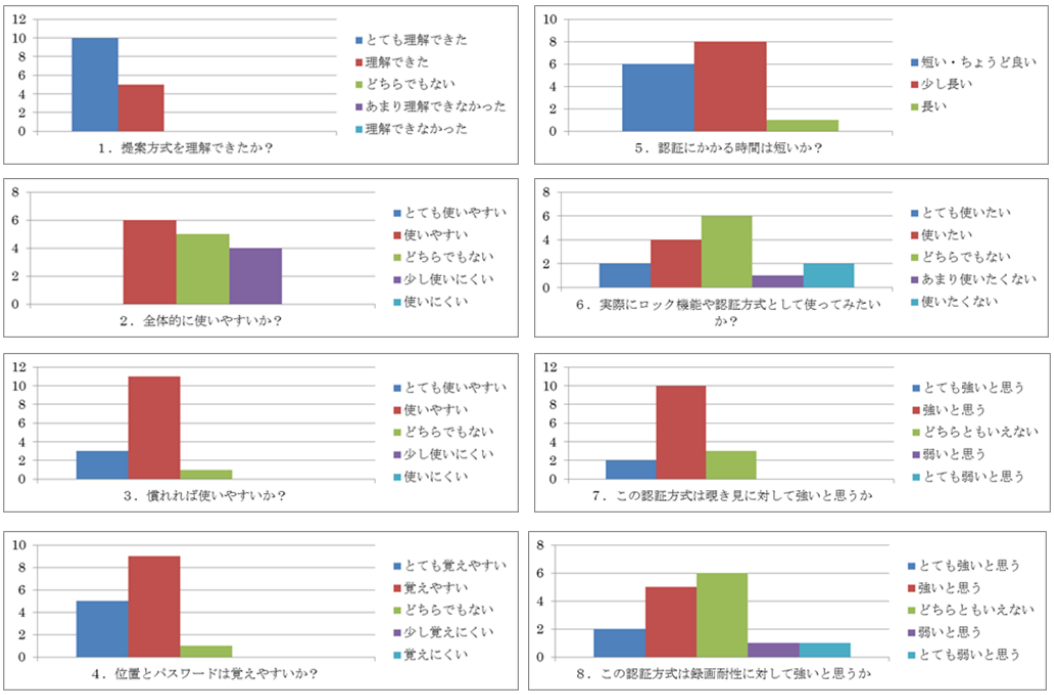

図 5.3　アンケート結果

の登録した位置とパスワード以外の他の数字が一致する確率を図 5.1，一致した個数によるそれぞれのパスワード総数を図 5.2 に示す．

2 回の録画攻撃を行われ，2 回の認証ともに全てのパスワードと位置が一致していた場合でも，図 5.1，図 5.2 から他の数字も 5 個以上一致していればパスワード総数は 100 通り以上となり特定は困難になるため，特定される確率は 0.16%ほど下がる．

よって，2 回認証で位置とパスワードが等しく，かつ他の数字の一致が 4 個以下の確率は約 4%となった．

5.3 ユーザビリティに対する評価

提案の認証方式を評価するために，神奈川工科大学情報学部生 15 名にアンケートを実施した．アンケートの質問項目は次のような 8 問になる．ここで，(5)の質問については 3 段階，その他の質問は 5 段階の評価を行った．

各質問に対するそれぞれの評価を図 5.3 に結果を示す．

(1)　提案方式を理解できたか
本研究の認証方式は全ての人が理解できたと答えた．本研究の実験では，学生が大多数であったため，学生には理解しやすい認証だということが考えられる．

(2)　全体的に使いやすいか
アンケートでは，使い易いという意見はあったが，どちらでもない，少し使いにくいという意見も同程度見受けられた．原因としては，ユーザーインターフェースの問題が考えられる．
現在の操作方法としては，移動するマスを一度長押しする必要があるが，触れた瞬間に動かせるように改良をする必要がある．

(3)　慣れれば使いやすいか
慣れれば使いやすいという意見が多かった．逆に言えば慣れていないと使いにくいということが考えられるので，初めて使う人にもすぐに使いこなすための提案がさらに必要である．

(4)　位置とパスワードは覚えやすいか
覚えやすいという意見が多かったため，記憶するものがパスワードと位置の両方であった場合でも，ユーザーにはさほど支障はないということがわかった．

(5)　認証にかかる時間は短いか
認証時間は長いという意見の方が多かった．この結果から，ユーザビリティを考慮した認証としては致命的な問題であると感じたため，さらなる改善が必要である．

(6)　実際にロック機能や認証方式として使ってみたいか
全体的に使いたいという意見がやや多かったが，どちらでもない，使いたいという意見も見受けられた．そのため，もっとユーザーが使いたいと思わせるような使いやすさを追求する必要がある．

(7)　この認証方式は覗き見に対して強いと思うか
実験で，パスワードと位置を一人も特定することができなかったように，アンケートでも強いという意見が多かった．しかし，今後もさらに覗き見耐性を向上させる方法を考えることで提案認証をよりよいものにすべきである．

(8)　この認証方式は録画耐性に対して強いと思うか
アンケートでは，強いという意見が多かった．しかし，実際には 2 回の録画により，パスワードと位置が特定される可能性は約 4%あり，3 回以上になるとさらに高くなること

が考えられる．そのため，複数回の録画に対する対策を講じる必要がある．

6. 考察

実験の結果では，誰一人として位置とパスワードを特定することができなかったが，今回の実験における認証者は，ある程度慣れている人であり，慣れていない人が認証を行った場合についての覗き見耐性も考える必要がある．よって，今回の実験では，慣れている人が認証を行った場合は覗き見耐性を十分に有していると考えられる．

録画を 2 回行われた場合，約 4%の確率で位置とパスワードを特定されるということが分かったが，3 回以上行われた場合，さらに特定される可能性が高くなることが想定される．

そのため，複数の録画攻撃により認証情報を盗まれるのを防ぐために，対策を講じる必要である．

今回の提案方式では，16 個の中からユーザーが任意で 4 個をパスワードとして選ぶ方式であるため，パスワード登録パターンの総数は$_{16}C_4$=1820 通りとなり，偶然認証率 1/1820 となった．PIN 方式の 4 桁に相当する偶然認証の確率 1/10000 の強度は達成できなかったため，今後は偶然認証の確率を上げるような仕組みをさらに考える必要がある．

5.3 節のアンケート結果から，位置とパスワードの覚えやすさについては評価が良かったものの，使い易さや，認証時間についてはあまり良い評価は得られなかった．

そのため，実装の細かな部分の改良や，すぐに認証者が慣れるような仕組みを新たに考える必要がある．

7. おわりに

本研究では，覗き見による情報漏洩を防ぐために，従来のパスワード方式とパズルの要素を組み合わせて，指定した位置にパスワードを揃えることによって，覗き見をされても認証情報が盗まれないパズル型認証方式を提案した．この方式としては，パスワードではないマスをドラッグした場合でも，パスワードを揃えることができるというものがあり，さらに，覗き見をされていると思った場合には，パスワードを登録している位置とは関係ない部分を動かすことによりさらに覗き見の対策を行うことができる．そして，この認証方式は実験結果から覗き見により認証情報を盗まれる可能性が低いことがわかった．これにより，提案方式は覗き見攻撃により認証情報が盗まれることを防ぐことができる．

今後の課題を以下に述べる．

- 複数回の録画攻撃に対する対策

認証時の録画攻撃による回数が増えるほど，位置とパスワードが特定されてしまう可能性が高くなるため，録画への対策を講じる必要がある．

- 認証にかかる時間

アンケートを行った学生の半数以上が，認証にかかる時間が長いという意見であった．そのため，斜め移動を実装し認証時間を減らすという方法が考えられる．しかし，斜め移動を実装することにより認証画面の再現が簡単にできてしまうという問題がある．

参考文献

[1] 北林良太，稲葉宏幸，“複数回の覗き見に耐性を有するパスワード認証方式の提案”, 電子情報通信学会技術研究報告，ICSS，情報通信システムセキュリティ，Vol.109, No.115，pp.21-26，電子情報通信学会，(2009).

[2] 藤田和秀,平川豊,“覗き見・盗撮に耐性を持つパスワード認証方式の検討”電子情報通信学会　pp.61-66 (2008).

[3] 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，情報処理学会，(2008).

[4] 喜多義弘,菅井文朗,朴美娘,岡崎直宣,“モバイル端末における覗き見耐性をもつ認証方式の提案と実装,” pp.413-420，コンピュータセキュリティシンポジウム，(2012).

[5] 原田篤史,漁田武雄,水の忠則,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, pp1997-2013，情報処理学会，(2005).

[6] 和斉薫,菅井文朗,喜多義弘,朴美娘,岡崎直宣,“アイコンとフリック入力を用いた覗き見耐性を持つ認証方式の検討”，情報処理学会研究報告 IPSJ SIG Technical Report, pp.1-6, (2012).

[7] 菅井文郎,池田匡視,岡崎直宣,朴美娘,“アイコンとタッチパネル液晶を用いた覗き見耐性を持つ認証方式についての検討”，情報処理学会研究報告 IPSJ SIG Technical Report,pp.1-6(2012).