情報処理学会論文誌 Vol.58 No.9 1513–1522 (Sep. 2017)

利便性を考慮した覗き見に耐性を有する改良型背景パターンスライド認証方式の提案

田中 基偉[1,a)] 稲葉 宏幸[2,b)]

受付日 2016年11月24日, 採録日 2017年6月6日

概要：オンラインバンキング等の Web サービスにおいて，暗証番号やパスワードを用いた個人認証方式が多く利用されている．しかし，これらの認証方式は，入力の覗き見や通信路の盗聴によりパスワード情報が流出する危険性がある．覗き見に耐性を有する既存の方式として，文字の背景に色の配列を表示し，利用者が上下左右にスライドさせることで認証を行う方式が提案されている．著者らはその方式を改良することで安全性を向上させた背景パターンスライド認証方式を提案しているが，操作方法はさらに複雑になっており，利便性についての問題が指摘されていた．本論文では背景パターンスライド認証方式に対して，同等の安全性を保ちつつ，その利便性を改良した認証方式を提案する．さらに覗き見に対する安全性や総当たり攻撃に対する安全性を評価し，利便性について評価実験を行うことで，提案手法の性能評価を行う．

キーワード：パスワード認証，覗き見，総当たり攻撃，利便性，カラーユニバーサルデザイン

Proposal of Improved Background Pattern Slide Authentication against Shoulder Surfing in Consideration of Convenience

Motoi Tanaka[1,a)] Hiroyuki Inaba[2,b)]

Received: November 24, 2016, Accepted: June 6, 2017

Abstract: A personal authentication system using PIN or password is widely used in Web services such as online banking. However these authentication system has a weakness of password leakage by shoulder surfing in inputs or eavesdropping. As an existing system against shoulder surfing, it is known that the authentication method in which users slide background color array displayed behind characters. Although the authors have proposed the improved version of the background pattern slide authentication in safeness, its operation procedure seems more complicated. In this report, we proposed a new method to improve usability while maintaining equivalent security. Furthermore, we evaluate the safety against shoulder surfing and brute force attacks and evaluate the performance of the proposed method by conducting evaluation experiments on convenience.

Keywords: password authentication, shoulder surfing, brute force attacks, convenience, color universal design

1. はじめに

近年，様々な情報機器の普及により，時間や場所を問わずに誰もが簡単に様々なサービスを利用することができるようになった．それにより，利用者が本人であることを確認する個人認証技術が重要になってきている．最も一般的に利用されている個人認証方式にパスワード認証方式がある．パスワード認証方式は，導入時のコストが安価であることや，認証時に特別な所有物を必要としない等の利点があり，一般的に広く利用されている．また，入力するパスワードに使用する文字種や桁数を増加させることにより安全性を容易に高めることが可能である．しかし，利用者がパスワードを忘れてしまうことや，安易なパスワードを設

[1] 京都工芸繊維大学大学院工芸科学研究科情報工学専攻
Department of Information Science, Graduate School of Science and Technology, Kyoto Institute of Technology, Kyoto 606–8585, Japan
[2] 京都工芸繊維大学情報工学・人間科学系
Faculty of Information and Human Sciences, Kyoto Institute of Technology, Kyoto 606–8585, Japan
[a)] tanaka12@sec.is.kit.ac.jp
[b)] inaba@kit.ac.jp

定することにより第三者に推測されてしまう危険性が指摘されている [1]．また，考えられるすべてのパスワードを試す「総当たり攻撃」や，パスワードの入力動作を覗き見することによりパスワードを解読する「覗き見攻撃」，通信路の「盗聴」の危険性があげられる [2]．パスワード情報を不正に取得された場合，不正アクセスや個人情報の漏洩，なりすましの危険性がある．そのため，覗き見等によるパスワード情報の漏洩を防ぐためにパスワードそのものを入力しない方式が研究されている [3], [4], [5], [6], [7]．一方，画像をパスワードにする認証方式も提案されている [8], [9]．

文献 [3] では，ランダムに並んだ文字から，バイブレートのパターンによって，目的の文字から上下左右にずらした文字を入力することで，本来のパスワードを分からなくする方式である．バイブレートは覗き見している人には分からないため覗き見に耐性を持つ．しかし，この方式ではバイブレートパターンを数種類記憶し，判別する必要があり，利用者の負担が大きい．

文献 [4] で提案されている Fake Pointer は，記号を背景としたパネル上に数字が表示されており，数字を選択シンボル情報に合わせることで入力する方式である．この方式は複数回の覗き見にも耐性を持つ．しかし，選択シンボル情報は，認証の前に人の目に晒されない場所に移動し確認しなければならず，そのための携帯端末等の機器が必要になるといった問題がある．

文献 [5], [6] の CTG および FCTG 方式は入力した文字の背景の色を使って入力するため，攻撃者には利用者が選んだ色の情報しか分からず，覗き見に耐性を有している．また，特別な機器を必要とせず，利用者の記憶するべき情報はパスワードのみである．しかし，覗き見に対する耐性を有する一方で，総当たり攻撃には弱いという欠点を持っている．

文献 [7] で提案されている背景配列の移動量を用いた方式は，背景の色を移動させ，パスワードの背景色を順に揃える認証方式である．攻撃者には利用者がどの色を選択したのかも分からないため，文献 [5] と比較して高い覗き見に対する耐性を持つ．

さらに著者らによって文献 [7] をもとに，1 文字ごとに入力に使用する色を指示する系列配列と，本来必要でない偽の入力を挟み込む偽入力とを導入することで，総当たり攻撃にもある程度の耐性を有し，覗き見にも耐性を有する方式である背景パターンスライド認証方式が提案されている [10]．しかし，操作方法はさらに複雑になっており，元となった方式である CTG 方式や，背景配列の移動量を用いた方式に比べて，利便性に劣るという問題が残されていた [11]．

文献 [8] は画像を用いた認証方式であり，秘密情報であるパス画像とその他の不正解用のおとり画像を使用している．認証は複数の画像の中からパス画像を選択すればよい．この方式はおとり画像の数を変更することで総当たり攻撃に対する安全性を柔軟に変更可能であり，さらに利便性も考慮されている．しかし，覗き見に対する安全性は考えられていない．

文献 [9] で提案されている SWIPASS も，画像を利用する認証方式であるが，選択時にスワイプ操作を利用している点に特徴がある．スワイプ方向も秘密情報となっているため，覗き見にもある程度の耐性を持つ．この方式は総当たり攻撃に対する安全性を有し，利便性の面も優れているが，覗き見に対する安全性では背景パターンスライド認証方式 [10] の方が優れていると考えられる．

そこで本論文では，背景パターンスライド認証方式を改良し，同等の安全性を保ちつつ，利便性を向上させる認証方式を提案する．さらに，その認証方式について，覗き見に対する安全性や総当たり攻撃による安全性を評価するとともに，評価実験を行うことで，提案手法の利便性に関する性能を明らかにする．

2. 覗き見に耐性を有する認証方式

2.1 CTG 方式

攻撃者が認証の一連の動作を覗き見ても，認証をパスするための必要な情報を得られないようにする手法として，CTG（Cognitive Trapdoor Game）方式が提案されている [5]．**図 1** にその認証画面を示す．CTG 方式は，パスワード入力時に，システム側がテンキーの背景色を白と黒の 2 色にランダムにかつ均等に塗り分けを行う．利用者はパスワードの先頭桁から順に，入力したい数字が白と黒のどちらに含まれているのかを判断し二者択一で回答する．一度回答するたびに背景色はランダムに再配置され，この操作をパスワードの最後の桁まで繰り返すことで認証を行う．この手法では，覗き見に対する安全性は高いが，総当たり攻撃に非常に弱いという問題がある．

CTG 方式の安全性を考えるため，文字の種類数を A，パスワード長を λ，背景の種類数を b とする．このとき，攻撃者がランダムに入力を行って認証に成功する確率 P は

$$P = \frac{1}{b^{\lambda}} \tag{1}$$

となる．たとえば $b = 2$，$\lambda = 4$ の場合では，$P = \frac{1}{16}$ になり，総当たり攻撃には非常に弱いことが分かる．

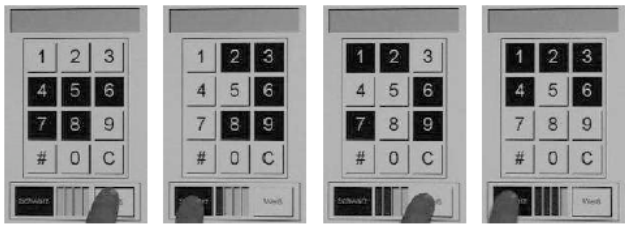

図 1 CTG 方式における入力の様子（文献 [5] より引用）
Fig. 1 Input scene in CTG method (quoted from Ref. [5]).

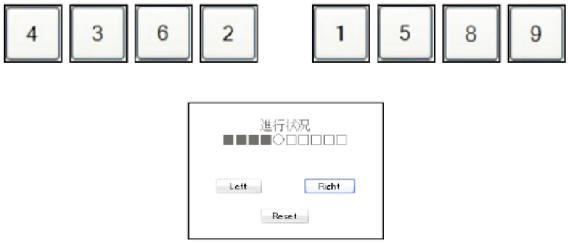

図 2 FCTG 方式における入力画面（文献 [6] より引用）
Fig. 2 Screen image of FCTG method (quoted from Ref. [6]).

また，複数回の覗き見に対する安全性は，$b = 2$ の場合では，1 回覗き見されるごとに各桁のパスワードの候補数が半分になるため，覗き見回数を K とし K 回覗き見された後のパスワード候補数を S_K とすると

$$S_K = \left(\frac{A}{2^K}\right)^{\lambda} \tag{2}$$

である．したがって，$A = 10$，$\lambda = 4$ の場合には 4 回の覗き見でパスワードをほぼ特定可能であることが分かる．そのため，複数回の覗き見に対しては耐性を有さないことが分かる．

2.2 FCTG 方式

CTG 方式を改良し，入力中に正しいパスワード入力（真入力と呼ぶ）に関係のない，偽の入力（偽入力と呼ぶ）を挟み込むことにより覗き見耐性を向上させる方式として FCTG（Faked Cognitive Trapdoor Game）方式が提案されている [6]．**図 2** にその入力画面を示す．具体的な入力形式は CTG 方式と同様であり，入力したい値が含まれている方を二者択一で回答する．CTG ではテンキーを白と黒に塗り分けていたが，FCTG 方式では各数字を左右に振り分けて表示し，入力者は左右どちらかの二者択一で回答する．入力画面にはパスワードに用いる文字の種類のうちすべての文字が表示されているわけではなく，一部が表示されていない状態になっている．入力したい文字が左右どちらにも表示されていなければ，その入力を偽入力として左右どちらを選択してもよい．FCTG 方式では，入力を覗き見したとしても，各桁の入力が真入力か偽入力かどうかは容易に判別できない．しかし，偽入力箇所で非表示であった数字が次の真入力箇所で入力する数字の候補になるために，攻撃者にパスワード候補のヒントを与えてしまい，実際表示されている数字の個数よりも候補が少なくなってしまうことがある．

2.3 背景配列の移動量を用いた認証方式

背景に異なる色や図形の配列（背景配列）を表示し，その背景配列を上下左右に動かすことで認証を行う方式が提案されている [7]．**図 3** にその認証画面を示す．背景の種類数は 2 つ以上で，かつ種類ごとに同数が使用される．また背景の並びは入力ごとに変更される．この認証では，パスワードの各文字について順に，背景をすべて同じ種類の背景に合わせることができていれば認証成功となる．使用する背景の種類は，利用者がパスワードの最初の文字の背景を合わせる際に任意に選択してよい．したがって，使用する背景の種類はあらかじめ覚えておく必要がなく，認証のたびに変えることができる．

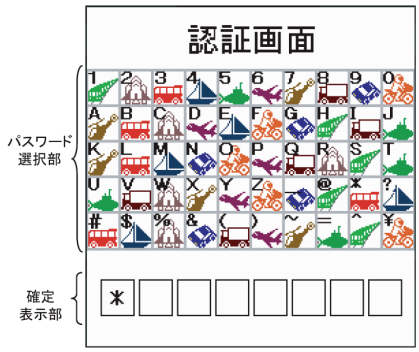

図 3 背景配列の移動量を用いた認証方式の認証画面（文献 [7] より引用）
Fig. 3 Authentication method based on vector of background matrix (quoted from Ref. [7]).

総当たり攻撃に対する安全性を示す．パスワード 1 文字目の背景色は任意に選択できるため，1 文字目の入力は認証成功率に影響しない．したがって，攻撃者がランダムに入力を行って認証に成功する確率 P は，パスワード長 λ，背景の種類数 b を用いて

$$P = \frac{1}{b^{\lambda-1}} \tag{3}$$

と表現できる．

また，複数回の覗き見に対する安全性も導出されており，K 回覗き見された後のパスワード候補数を S_K とすると，背景配列のサイズ N_b を用いて，

$$S_K = \left(b\left(\frac{N_b}{b}\right)^{\lambda} - 1\right) \times \left(\left(\frac{b^2(b-1)+N_b^2}{bN_b^2}\right)^{\lambda-1}\right)^{K-1} + 1 \tag{4}$$

となる．この式より，1 回覗き見された後のパスワード候補数を S_1 とすると，

$$S_1 = b \times \left(\frac{N_b}{b}\right)^{\lambda} \tag{5}$$

となる．この手法では，認証に使用する背景の種類を利用者が記憶する必要がなく，毎回任意に選択できるというメリットがある．

2.4 背景パターンスライド認証方式

2.3 節の認証方式に，系列配列と偽入力という手法を導入することで覗き見に対する安全性を高める方式が著者らに

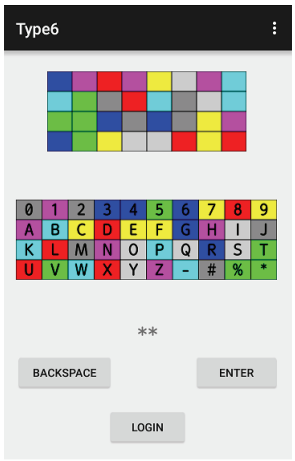

図 4 背景パターンスライド認証方式の認証画面（文献 [10] より引用）

Fig. 4 Screen image of background pattern slide authentication (quoted from Ref. [10]).

よって提案されている [10]．その認証画面を図 4 に示す．

2.4.1 系列配列を用いた方式

利用者が入力に使用する色をパスワードの文字ごとに毎回異なったものにし，それをどのような順番で使用するかをシステム側が指示する方式である．2.3 節の背景配列の移動量を用いた認証方式では，利用者は認証のたびに，認証に用いる色（認証色）を決定し，その色をパスワードの各文字について，背景を移動させて揃えていた．それに対しこの方式では，背景配列の他に背景色だけが表示された配列（系列配列と呼ぶ）を表示し，利用者はこの系列配列から任意に 1 マス選択する．そして，その選択したマスに表示されている背景色を認証色として用いて，背景配列を移動させ入力を行う．1 文字の入力を行うと，システム側は背景配列と系列配列の両方をランダムに塗り替える．利用者は塗り替えられた後も選択したマスと同じマスに表示されている色だけに着目し，新しく表示された色を認証色として用いて入力を行う．利用者により入力されたパスワードの文字の背景色の並びが，系列配列のいずれかのマスの色の並びと一致していれば認証成功となる．

この方式の総当たり攻撃に対する安全性を示す．系列配列にすべての背景色が必ず 1 つは表示されているという条件の下では，2.3 節の方式から確率は変化しない．したがって，攻撃者がランダムに入力を行って認証に成功する確率は，式 (3) と同様である．

1 回の覗き見に対する安全性を示す．系列配列の各マスに対して色の組合せを考えるため，1 回覗き見された後のパスワード候補数を S_1 とすると，背景配列のサイズ N_b，系列配列のサイズ N_s を用いて

$$S_1 = N_s \times \left(\frac{N_b}{b}\right)^{\lambda} \tag{6}$$

と表現できる．式 (5) と比較すると，系列配列のサイズ N_s が背景の色の種類数 b よりも大きければ，覗き見後のパスワード候補数は増加することが分かる．

2.4.2 偽入力を用いた方式

本来のパスワードに必要のない偽の入力（偽入力と呼ぶ）を挟み込むことで，覗き見の際のパスワード候補を増加させ，覗き見耐性を向上させる方式である．利用者はパスワードを登録する際に，偽入力のタイミングを共有するための 1 つの色（偽入力判別色と呼ぶ）をあらかじめ決定しておく．背景配列がランダムに塗り替えられた際に，偽入力判別色が次に入力したいパスワードの文字の背景として表示されていた場合，その入力を偽入力とする．偽入力時には利用者は，背景を任意に動かして入力するものとする．偽入力箇所以外の，利用者により入力されたパスワードの文字の背景色がすべて一致していれば認証成功となる．

総当たり攻撃に対する安全性は，偽入力の数 f の値にかかわらず，確率は変化しない．したがって，攻撃者がランダムに入力を行って認証に成功する確率は，式 (3) と同様である．

1 回の覗き見に対する安全性を示す．$\lambda + f$ 回の入力の中から，どの入力が偽入力（パスワードの推測に必要のない入力）なのかを考えるため，1 回覗き見された後のパスワード候補数は，

$$S_1 = \binom{\lambda + f}{f} \times b \times \left(\frac{N_b}{b}\right)^{\lambda} \tag{7}$$

と表現できる．ここで $\binom{n}{k}$ は二項係数 ${}_nC_k$ である．したがって，偽入力数 f を多くすることにより覗き見後のパスワード候補数を増加させることができる．

2.5 系列配列・偽入力の両方を用いた方式

系列配列・偽入力の両方を用いた場合の 1 回の覗き見に対する安全性は，式 (6)，(7) より，

$$S_1 = \binom{\lambda + f}{f} \times N_s \times \left(\frac{N_b}{b}\right)^{\lambda} \tag{8}$$

となり，式 (5) に比較して，覗き見に対する安全性が向上していることが分かる．

この方式では，パスワード長は利用者が自由に設定でき，利用者の記憶にかかる負担は，パスワードと偽入力判別色 1 種のみである．しかし，操作方法はやや複雑であるため，利便性に問題がある可能性がある．

2 章で述べた各認証方式に対する利便性の評価と比較は文献 [11] で行われており，背景パターンスライド認証方式の利便性についての問題が指摘されている．具体的な問題点を以下に示す．

(1) 文字種が 40 種類と多いため，背景配列の中から入力したい文字を探すのに時間がかかる．
(2) 系列配列において，中央部のマスよりも隅のマスが選ばれる傾向があり，推測が容易になってしまう．

(3) 偽入力であることがうまく伝わらず，エラーの原因となりやすい．

以上の問題点を改善する改良手法を次章で提案する．

3. 提案手法

2.4 節で述べた背景パターンスライド認証方式を改良することで，利便性を向上させた認証方式を提案する．提案手法の認証画面を図 5 に示す．最上段に入力に使用する色を指示する系列配列が表示されており，その下に実際に文字の背景に色を合わせる背景配列がある．背景配列上で上下左右にフリックすることで，その方向に背景の色全体を移動させることができる．また，背景は巡回的に移動するようになっている．その下の確定表示部では，現在入力が確定された文字数を “∗” で表示している．最下段には，3 つのボタンが配置されており，BACKSPACE ボタンで 1 文字削除，ENTER ボタンで 1 文字確定，LOGIN ボタンで認証を行う．

3.1 文字配列に対しての改良

1 つ目の改良点は，背景配列の文字の並べ方の変更である．実装した方式では，4 × 10 マスの背景配列に，数字，英字，記号の順に並んでいる．改良点として，一般的な qwerty 配列に変更することが考えられる．ふだん qwerty 配列に慣れている人にとっては，目的の文字を探すことが容易になり，時間短縮が期待できる．

3.2 系列配列に対しての改良

2 つ目の改良点は，系列配列の並べ方の変更である．図 4 の背景パターンスライド認証方式では，4 × 8 マスの系列配列が並んでいるが，この並びでは中央部分のマスを選択した場合に，選択したマスが分かりにくいため，結果として隅のマスしか選ばれないという問題があった．改良点として，系列配列の大きさにより，系列配列を 4〜6 マス程度のブロックに分割する．今回実装したパラメータにおいては系列配列が 32 マスであるため，ブロックサイズを同一にするためと，画面上の配置に偏りがでないようにするため，系列配列を 4 マスずつのブロックに 8 分割するのが望ましい．これにより，選択したマスを識別しやすくなることが期待できる．

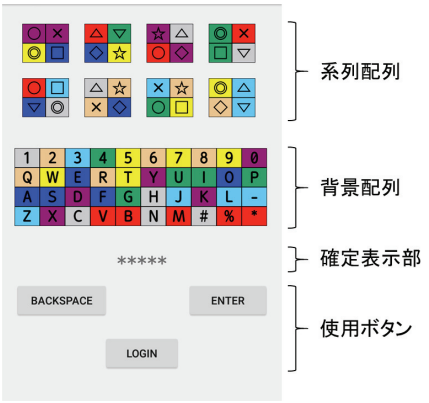

図 5 提案手法の認証画面
Fig. 5 Screen image of the proposed method.

3.3 偽入力に対しての改良

背景パターンスライド認証方式では，色を指示するのは系列配列で，偽入力を指示するのは背景配列上であったため，パスワード文字を 1 文字入力するごとに，上部の系列配列と下部の背景配列との間で視線を移動させる必要があり，偽入力の確認忘れや，見誤りによるエラーが起こっていた．そこで 3 つ目の改良点として，偽入力のタイミングを伝える方法を変更し，系列配列上で偽入力を指示できる方法を提案する．具体的には，系列配列上に何種類かの記号を種類ごとに同数表示する．その記号により偽入力であるかどうかを判断する．

認証方法は，利用者は事前に偽入力であることを共有するための記号（偽入力判別記号と呼ぶ）を 1 種類設定しておく．認証開始時には，系列配列から任意に 1 マス選択する．選択した系列配列のマスの記号が，偽入力判別記号であれば，その入力を偽入力とする．偽入力時には利用者は，背景を任意に動かして入力するものとする．選択したマスの記号が偽入力判別記号でなければ，パスワード文字の背景色を選択したマスの色に合わせる．1 文字入力するたびに系列配列，背景配列の色と系列配列上の記号がランダムに再配置される．2 文字目以降の入力も同様に行う．偽入力箇所以外の，利用者により入力されたパスワードの文字の背景色の並びが，系列配列のいずれかのマスの並びと一致していれば認証成功となる．なお，どの記号が偽入力判別記号であっても偽入力回数が変化しないようにするため，系列配列上の各マスの記号の表示回数を均一にする必要がある．この認証手順を以下に示す．ここで，パスワード長を λ，偽入力数を f とする．

Step0 事前にパスワード（W_1〜W_λ）と偽入力判別記号 1 種を登録する．

Step1 $i = 1$ とする．利用者は系列配列から任意に 1 マス選択し，記憶する（以下，認証マスと呼ぶ）．

Step2 システムは系列配列・背景配列の色をランダムに配置し，系列配列の記号もランダムに配置する．
Step1 で選択した認証マスの現在の記号が，
偽入力判別記号と異なるならば Step3 へ
偽入力判別記号と一致するならば Step4 へ

Step3 パスワード文字 W_i に，Step1 で選択した認証マスの現在の色を合わせる．Step5 へ

Step4 偽入力なので任意に背景を動かす．Step5 へ

Step5 ENTER ボタンを押し，背景色と文字の対応関係を確定させる．

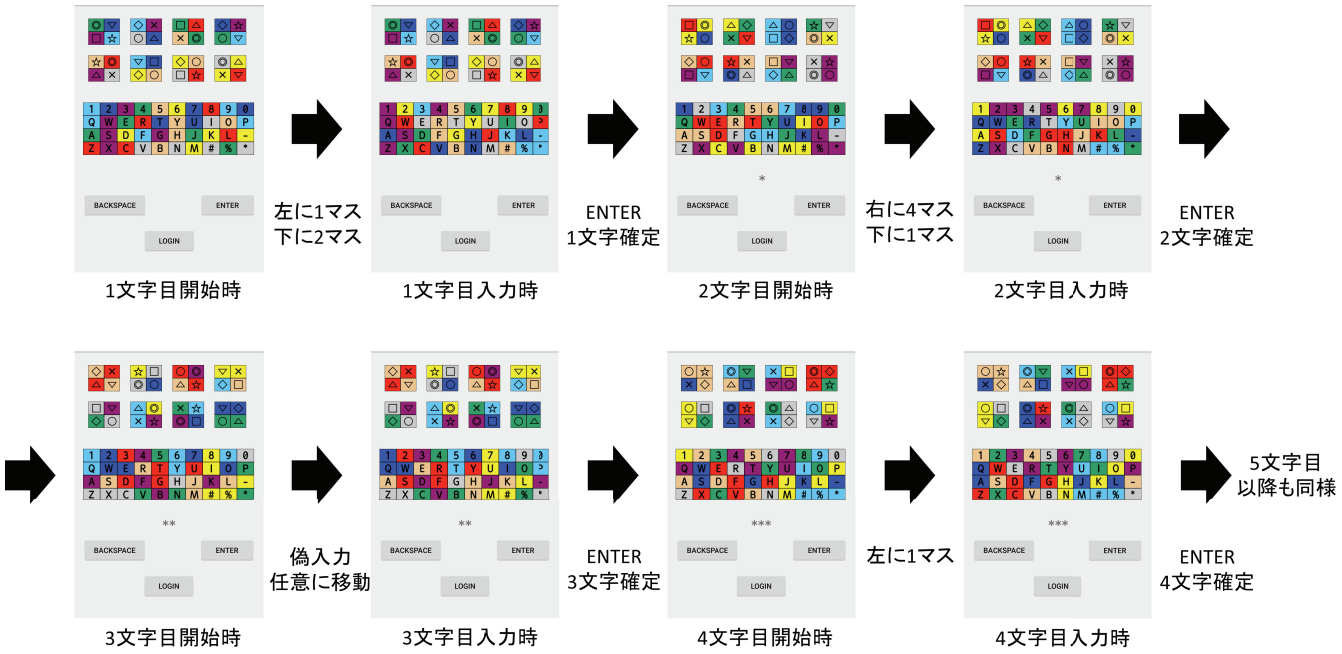

図 6 認証の流れ

Fig. 6 Flow in authentication.

Step6 $i = i + 1$ とする．

$i > \lambda + f$ ならば Step7 へ

$i \leq \lambda + f$ ならば Step2 へ

Step7 パスワードのすべての文字と f 回の偽入力に対して入力を行ったので，LOGIN ボタンで認証を行う．

Step8 システムは，偽入力箇所以外のパスワードの文字の背景色の並びが，系列配列のいずれかのマスの並びと一致していれば認証成功とする．

3.4 動作例

具体的な動作例による画面の遷移を図 6 に示す．利用者は事前にパスワードとして “ABCDEFG”，偽入力判別記号として “◎” を登録しているものとする．

入力を始める前に，系列配列から認証に用いるマス（認証マス）を選択する．ここでは，左から 4 マス目，上から 3 マス目の位置（初期状態ではブルー，“□”）を選択したとする．認証マスの記号は “□” で偽入力判別記号ではないので，この入力は真入力である．したがって，パスワード 1 文字目 “A” の背景色を認証マスの色であるブルーに合わせる．ENTER ボタンで 1 文字目の入力が確定し，系列配列・背景配列・記号がランダムに再配置される．認証マスはベージュ，“×” であるので真入力である．したがって，2 文字目 “B” も同様に入力を行う．3 文字目 “C” において，認証マスはイエロー，“◎” であるので，これは偽入力である．偽入力時には任意に移動させ，ENTER ボタンで確定させる．4 文字目では先ほど入力できなかった “C” を入力する．認証マスはレッド，“☆” であるので真入力である．したがって，“C” の背景色をレッドに合わせる．同様に “D”，“E”，“F”，“G” についても入力を行い，LOGIN ボタンで認証を行う．

4. 提案手法の安全性評価

提案手法の安全性を評価する．以下では，総当たり攻撃に対する安全性 P と，パスワードの候補数 S を情報量 I (bit) で表すために，

$$I_P = -\log_2(P) \tag{9}$$

$$I_S = -\log_2\left(\frac{1}{S}\right) \tag{10}$$

と定義している．また，攻撃者は認証アルゴリズム，パスワードの桁数，偽入力の回数を知っているという条件で評価を行う．

4.1 総当たり攻撃耐性

総当たり攻撃に対する安全性を示す．系列配列にすべての背景色が必ず 1 つは表示されているため，1 文字目の入力に対し，2 文字目以降が一致すればよい．また偽入力について，偽入力時には任意の入力をすればよいため，総当たり攻撃の認証成功率には影響しない．したがって，攻撃者がランダムに入力を行って認証に成功する確率 P は，パスワード長を λ，背景の色の数を b とすると，

$$P = \frac{1}{b^{\lambda-1}} \tag{11}$$

となり，2.4 節の改良前から変化していないことが分かる．

4.2 覗き見攻撃耐性

1 回の覗き見に対する安全性を示す．偽入力の判別のために使用する記号の種類数を r とすると，攻撃者は r 種類

表 1 パラメータの設定例および総当たり攻撃と覗き見に対する安全性
Table 1 Example of parameter settings and its safety.

背景配列の大きさ N_b	背景の色の数 b	系列配列の大きさ N_s	記号の種類数 r	パスワード長 λ	総当たり攻撃耐性 I_P (bit)	覗き見耐性 I_S (bit)
40	5	30	10	9	18.58	35.23
40	8	32	8	7	18.00	24.25
40	10	30	10	9	26.58	26.23
44	11	33	11	10	31.13	28.50
48	8	32	8	7	18.00	26.09
48	12	36	9	8	25.09	24.34

の記号から，偽入力判別記号 1 つを推測するので，提案手法の 1 回の覗き見に対する安全性 S_1 は，系列配列の大きさを N_s，背景配列の大きさを N_b とすると，

$$S_1 = r \times N_s \times \left(\frac{N_b}{b}\right)^{\lambda} \tag{12}$$

となる．たとえば，$r = 8$, $N_s = 32$, $N_b = 40$, $b = 8$, $\lambda = 7$, $f = 1$ のとき，1 回覗き見された後のパスワードの候補数 S_1 を情報量 I_S (bit) で表すと，$I_S = 24.25$ (bit) となる．また，同じパラメータを有する既存手法として，2.3 節の背景配列の移動量を用いた方式 [7] では $I_S = 19.25$ (bit)，2.4 節の背景パターンスライド認証方式 [10] では $I_S = 24.25$ (bit) となる．このように，提案手法は同程度のパラメータで比較すると，背景配列の移動量を用いた認証方式よりも覗き見に対する耐性が高く，かつ，背景パターンスライド認証方式と同等の覗き見に対する耐性を持つことが分かる．

4.3 パラメータの選択

提案手法における各パラメータの選択について考える．背景配列の大きさ N_b は，使用できる文字の数に等しく，一般に数字，英字，記号を使うことが想定される．記号を増やすことも可能であるが，文字を探す時間が増えることや画面のサイズを考慮する必要がある．また，qwerty 配列により配置することを考えると，N_b はキーの数である 40〜48 程度が望ましい．

背景の色の数 b は，背景配列に各色を同数表示するために，N_b を割り切れる数である必要がある．また，式 (11), (12) より，総当たり攻撃耐性と覗き見耐性は背景の色の数によってトレードオフの関係になっている．そのため，最低限の総当たり攻撃耐性を有しながら，できるだけ覗き見耐性を高く設定することになる．一般に，総当たり攻撃耐性について，4 桁の PIN コードが持つ総当たり攻撃耐性である $P = 10^{-4}$ を最低基準（$I_P \geq 13.29$ (bit)）とすることが多い．

系列配列の大きさ N_s は，背景配列と同様に，各色を同数表示するために，背景の色の数で割り切れる必要がある．また，N_s は大きければ大きいほど安全性は高まるが利便性は低くなる．

偽入力の判別のために使用する記号の種類数 r は，系列配列に各記号を同数表示するために，N_s を割り切れる数である必要がある．また，r は大きければ大きいほど安全性は高まる．しかし，1 回の認証において，系列配列の各マスに対して，すべての記号が同数表示されなければならないため，パスワードの長さにも影響する．パスワードの長さ λ は，偽入力数を f とすると，

$$\lambda = f \times r - f \tag{13}$$

となるため，パスワード長は限られてしまう．一般に，同じパスワード長において，偽入力数を増やすよりも記号の種類数を増やしたほうが安全性，利便性ともに良いので，以下では偽入力数 $f = 1$ としている．一般的にパスワード長は 8〜16 文字程度であるため，r はそれに合わせて設定することになる．

以上の考察に基づいて，パスワード長 λ が 8 文字前後の場合の各パラメータの設定例と，各設定値における総当たり攻撃耐性と 1 回の覗き見に対する耐性を**表 1** に示す．

5. 提案手法の利便性評価

5.1 実験概要

提案手法の利便性についての評価を行うために，2.4 節で述べた改良前の既存手法と 3 章で述べた提案手法を Android 端末に実装し，評価実験を行った．実験の被験者は 20 歳から 23 歳の学生男女 14 人（男性 9 人，女性 5 人）である．また，被験者はふだんからスマートフォンを利用し，タッチ式インタフェースを使い慣れている．実験に使用した端末は，AndroidOS 5.1 で，画面サイズは 5.0 インチである．実験姿勢や端末の持ち方には特に制限を設けなかった．パスワードとして使用できる文字種（背景配列の大きさ N_b）は数字，英大文字，記号 4 種の合計 40 種である．また，背景の色の数 b は 8 色，系列配列の大きさ N_s は 32 マス，使用できる記号の種類数 r は 8 種，パスワード長 λ は 7，偽入力数 f は 1 回とした．なお，実験ではすべての被験者について共通のパスワード “AK65%TZ” を用いた．パスワードの慣れによる影響がでないよう，被験者ごとに 2 つの方式の実験順を変更した．

評価項目としたのは，操作時間，エラー回数，主観評価

の 3 項目である．操作時間は，1 回の認証にかかる所要時間とし，エラー回数は，認証に成功するまでの認証に失敗した回数とした．また，操作時間とエラー回数は 1 人あたり 3 回の認証の平均をとっている．主観評価は，認証実験後にアンケートを行い，理解のしやすさ，入力のしやすさ，操作の慣れやすさ，安心のしやすさ，需要の程度の 5 項目について各々 5 段階で評価してもらった．

5.2 実験結果

既存手法と提案手法の，平均操作時間と標準偏差，平均エラー回数と標準偏差を**表 2** に示す．平均操作時間は，提案手法では約 4 秒短くなっている．平均操作時間に対して，t 検定（自由度：13，有意水準 5%）を行ったところ，$T = 2.304$ となり，有意な差が確認された．また，平均エラー回数では，既存手法では 1 回あたりのエラー回数が 0.31 回であるのに対し，提案手法では 0.12 回と減っている．平均エラー回数においても同様に t 検定（自由度：13，有意水準 5%）を行ったところ，$T = 2.280$ となり，平均エラー回数においても有意な差が確認された．したがって，操作時間，エラー回数においては提案手法のほうが優れているといえる．

次に，主観評価アンケートの結果について述べる．各項目は，5 段階評価で 1 が最も悪く，5 が最も良い評価である．**表 3** に各項目の平均点と括弧内にその標準偏差を示す．安心のしやすさの項目では提案手法はわずかに平均点が低くなっているが，これは記号を使うことによって偽入力位置のヒントになると感じたことによると考えられる．しかし，理解のしやすさ，入力のしやすさ，操作の慣れやすさ，需要の程度の各項目で，提案手法の平均点が高くなっていることから，主観評価でも提案手法のほうが良い評価を得ていると結論できる．

系列配列の認証マスの使用率について，文献 [11] で，隅のマスばかり選ばれるという問題点が報告されていた．5.1 節で述べた実験における，改良前の既存手法の使用率を**図 7** に，提案手法における使用率を**図 8** に示す．系列配列が分割されていない既存手法では，4 隅のマスの使用率が 80%程度あり，推測が容易である．それに対し，系列配列を分割した提案手法では，4 隅のマスの使用率が 50%程度に下がっており，改善が認められる．しかし，依然として使用されるマスに偏りがあるため，利用者自身により意識的に隅のマスを選ばないようにすることや，認証のたびに違うマスを選ぶことが必要だと考える．

表 2 平均操作時間と平均エラー回数
Table 2 Average operation time and number of errors.

	既存手法	提案手法
平均操作時間 (s)	41.82	37.45
標準偏差 (s)	10.18	8.99
平均エラー回数（回）	0.31	0.12
標準偏差（回）	0.19	0.20

表 3 主観評価結果
Table 3 Subjective assessment.

評価項目（1 悪い…良い 5）	既存手法	提案手法
理解のしやすさ	2.43(0.90)	3.36(1.04)
入力のしやすさ	2.71(0.96)	3.36(0.72)
操作の慣れやすさ	3.21(0.67)	3.57(0.90)
安心のしやすさ	4.71(0.45)	4.50(0.50)
需要の程度	2.57(0.98)	3.21(0.94)

5.3 考察

提案手法は，既存手法より平均操作時間が短くなったとはいえ，スマートフォンのロック解除等に日常的に利用するには長いと考えられる．しかし，認証実験で使用したパスワードは著者らが用意したものであるため，文字を探す際に手間を要することもあり，ふだん使っている慣れたパスワードではより認証時間が短くなると推測できる．

1 章で述べた画像認証方式との比較を行う．文献 [8] の方式は，総当たり攻撃耐性を柔軟に変更可能で，4 枚の画像を順番付きで選択するのにかかる時間は 30 秒未満と利便性も高い．しかし，覗き見に対する安全性は考えられておらず，提案手法の方が安全性は高い．覗き見にも耐性を持つ SWIPASS [9] では，選択（スワイプ）する画像が 3 枚と少ないこともあり，認証時間は 8 秒程度である．しかし，覗き見に対する安全性が比較的低いという欠点があるため，同一条件での比較は難しい．

以上のことより，提案手法は求められる安全性は高いが利用頻度がそれほど多くない状況，たとえばオンラインバンキング等の重要なサービスの認証では十分に実用的であ

31	0	0	0	0	2.4	2.4	14
0	2.4	0	0	0	2.4	2.4	2.4
0	0	0	2.4	0	0	0	0
21	0	0	0	2.4	0	2.4	12

図 7 既存手法の使用率（%）
Fig. 7 Usage rate of sequence array for existing method.

24	0	0	2.4	0	2.4	0	4.8
4.8	2.4	0	2.4	0	0	2.4	0
4.8	2.4	2.4	7.1	2.4	2.4	0	4.8
19	0	2.4	0	0	0	2.4	4.8

図 8 提案手法の使用率（%）
Fig. 8 Usage rate of sequence array for proposed method.

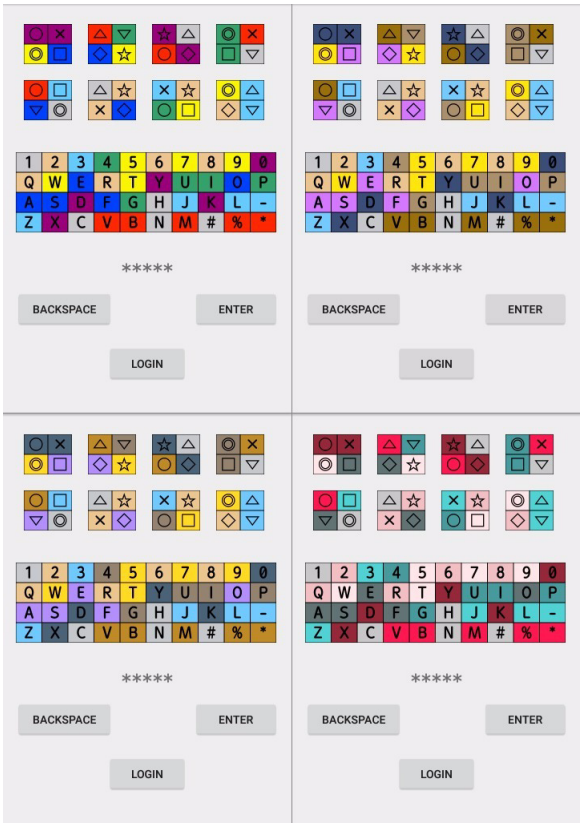

図 9 色覚タイプによる見え方のシミュレート
Fig. 9 Simulation of appearance for each color vision type.

ると考える．

6. 認証に使用する色について

提案方式では認証時に各色を識別できることが前提になっている．そのため，いわゆる色弱（色覚異常）等で色の識別が難しい場合には認証が困難になる可能性がある．その対策方法として，たとえば，文献 [12] で述べられている，色覚の多様性に配慮したカラーユニバーサルデザイン推奨配色セット等を用いる方法が考えられる．また，文献 [7] と同様に絵記号やハッチング等を併用する方法も考えられる．

5.1 節で実装した提案方式では，カラーユニバーサルデザイン推奨配色セット [12] を参考に色を決定している．提案方式の各色覚タイプによる見え方を，色のシミュレータ [13] を用いてシミュレートした結果を**図 9** に示す．図 9 は左上が C 型（一般色覚），右上が P 型色覚（Protanope），左下が D 型色覚（Deuteranope），右下が T 型色覚（Trianope）による見え方である．この結果より，使用する色が 8 色の場合には，どの色覚タイプにおいても各色を識別することが可能になっている．

7. おわりに

本論文では，系列配列と偽入力を導入することにより，覗き見や盗聴への耐性を強化した背景パターンスライド認証方式とその改良方式について述べ，その性能を評価した．改良型背景パターンスライド認証方式では，安全性を大きく低下させることなく，利便性を向上できることを明らかにした．改良手法の具体的な改良点の 1 つ目は，文字の並びを一般的な qwerty 配列に変更し，目的の文字を探す時間の短縮をはかることである．2 つ目は，系列配列を分割することで，選択したマスを識別しやすくし，エラー回数の減少と安全性の向上を可能にした．3 つ目は，偽入力の指示方法を，系列配列上に表示される記号を使用して偽入力のタイミングを指示する方法に変更することで，エラー回数を減少させることができた．改良手法は，総当たり攻撃，覗き見攻撃耐性ともに低下することなく高い安全性を有していることを示した．また，利便性の評価を行うために，改良前の既存手法と提案手法で評価実験を行った．その結果，操作時間，エラー回数，主観評価のすべての項目で利便性の評価が高くなることを明らかにした．提案手法は認証時に色の識別が必要であるが，カラーユニバーサルデザインに基づく配色を用いることにより，色覚異常を有していても利用が可能である．本提案手法によって，個人情報や金融情報等，重要な情報を取扱うインターネットサービスにおいて安全な個人認証方式の提供が期待できる．

今回の実験において実験被験者数は 14 人と少ないため，その実験精度は十分に高いとはいえない．提案手法を実用に供する場合には，より人数を増やして実験を行い，さらに精度を高める必要はあるだろう．また，求められる安全性に応じてパスワードの桁数を減らすことや，操作方法の見直し等，さらなる改良を加えることで，より短い認証時間で認証できる手法の実現を目指したい．

参考文献

[1] 総務省：安心してインターネットを使うために：安全なパスワード管理（オンライン），入手先 ⟨http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/staff/01.html⟩（参照 2016-11-09）．
[2] IPA 独立行政法人情報処理推進機構：オンライン本人認証方式の実態調査報告書（オンライン），入手先 ⟨https://www.ipa.go.jp/files/000040778.pdf⟩（参照 2016-11-16）．
[3] 喜多義弘，朝貝洸紀，菅井文郎，朴 美娘，岡崎直宣：バイブレートパターンを用いた覗き見耐性を持つパスワード認証方式の提案と実装，暗号と情報セキュリティシンポジウム（SCIS2013），2D4-3, pp.1–7 (2013)．
[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] Roth, V., Richter, K. and Freidinger, R.: A PIN-entry method resilient against shoulder surfing, *Proc. 11th ACM Conference on Computer and Communication Security*, pp.236–245 (2004)．
[6] 北林良太，稲葉宏幸：複数回ののぞき見に耐性を有するパスワード認証方式の提案，電子情報通信学会研究報告，Vol.109, No.115, pp.21–26 (2009)．
[7] 櫻井鐘治，撫中達司：背景配列の移動量を用いた個人認証方式ののぞき見に対する安全性評価，情報処理学会論文誌，Vol.49, No.9, pp.3038–3050 (2008)．

[8] 高田哲司，森 康洋：1 つの秘密情報で複数の安全性を提供しうる個人認証，*Computer Security Symposium*, pp.842–849 (2016).
[9] Kosugi, M., Suzuki, T., Uchida, O. and Kikuchi, H.: SWIPASS: Image-Based User Authentication for Touch Screen Devices, *Journal of Information Processing*, Vol.24, No.2, pp.227–236 (2016).
[10] 杉本洋介，稲葉宏幸：背景色と偽入力を用いた覗き見耐性を持つパスワード認証方式の提案，*Computer Security Symposium*, pp.1029–1033 (2014).
[11] 田中基偉，稲葉宏幸：覗き見耐性を有する背景パターンスライド認証方式の実装と利便性評価，電子情報通信学会研究報告，Vol.116, No.130, pp.29–32 (2016).
[12] NPO 法人カラーユニバーサルデザイン機構：カラーユニバーサルデザイン推奨配色セット（オンライン），入手先 ⟨http://www2.cudo.jp/wp/?p=2204⟩（参照 2016-11-08）.
[13] Asada, K.: Chromatic Vision Simulator - Web Edition - 1.11 (online), available from ⟨http://asada.tukusi.ne.jp/webCVS/⟩ (accessed 2016-11-16).

田中 基偉

2016 年京都工芸繊維大学工芸科学部情報工学課程卒業．現在，同大学大学院博士前期課程情報工学専攻．主に情報セキュリティに関する研究に従事．

稲葉 宏幸 （正会員）

1987 年大阪大学工学部通信工学科卒業．1989 年同大学大学院工学研究科通信工学専攻修士課程修了．1992 年京都工芸繊維大学大学院工芸科学研究科博士後期課程修了．工博．同年京都工芸繊維大学大学院工芸科学研究科助手．2000 年同助教授，2010 年同教授，現在に至る．主に情報理論，符号理論，情報セキュリティの研究に従事．著書『情報セキュリティの基礎』（共著）等．電子情報通信学会，IEEE 各会員．