情報処理学会論文誌　Vol. 49　No. 9　3038–3050 (Sep. 2008)

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

桜井鐘治[†1]　撫中達司[†1]

本論文では，パスワードによるチャレンジレスポンス型の個人認証方式として，文字の背後に異なる色や図形の配列（背景配列）を表示した認証画面に対して，利用者がパスワードを基に方向キーを使って背景配列を移動させた量を用いて認証を行う方式において，複数のパスワードを用いることで，のぞき見に対する安全性を高めた認証方式を提案する．提案の方式は，パスワード文字候補を複数のグループに分けてその中の 1 つを直接選択する従来の個人認証方式と比べて，のぞき見に対する安全性が高いことを示す．

Resistance Evaluation of User Authentication Method Using Matrix against Shoulder Surfing

Shoji Sakurai[†1] and Tatsuji Munaka[†1]

This paper proposes a user authentication method of challenge-response type with plural passwords. The authentication method displays an array of colors or figures behind characters. Users move the background array with direction keys, and prove that they know their passwords by making a response as using this amount of the movement. We show that our method's resistance against shoulder surfing attack is improved by using plural shorter passwords, and present that our method is better in the resistance than a conventional user authentication method to choose the one of the groups of the password character candidates directly.

†1 三菱電機株式会社
Mitsubishi Electric Corporation

1. はじめに

認証操作をのぞき見られることにより暗証番号やパスワードなどの認証情報を不正に取得され，被害者の口座から預金を不正に引き出される被害が発生し，大きな社会問題となっている．この被害を防ぐためにワンタイムパスワード生成装置や IC カードなどの物理トークンを利用した認証方式が提案されている．しかし，このような物理トークンを導入した場合には，利用者の物理トークンが正規のトークンであることは認証できるが，この物理トークンを使用している者が正規の利用者であるかは認証できない．このため，さらに PIN（Personal Identification Number）やパスワードなどの正規の利用者のみが記憶している秘密情報を入力することによる，利用者の認証が必要である．しかしながら，利用者が秘密情報を入力する操作については，依然としてのぞき見に対しての十分な対策がとられていない．秘密情報の入力をのぞき見た後に物理トークンを不正に入手する計画的な犯行に対しては，物理トークンだけでは十分な対策とはなっていない．

この問題を解決するために，特別なハードウェアを用いずに，利用者の記憶する PIN やパスワードなどの秘密情報を基に利用者を認証し，のぞき見に対する安全性を高めた認証方式がこれまでにも提案されている[1)–5)]．文献 1) では，利用者は暗証番号と別に隠しウィンドウとして乱数列内の位置（桁の番号）を記憶しておき，認証画面に表示される乱数列のうちで隠しウィンドウの位置の数値は暗証番号に置き換え，その他の数値は適当な数値に置き換えることで，のぞき見に対する安全性を高めている．この認証方式については，のぞき見に対する安全性の評価式も導出されているが，利用者にとっては，暗証番号のほかに，隠しウィンドウを憶える必要があり，さらに認証操作では，隠しウィンドウに該当する数値の置き換えに加えて，該当しない数値は適当に乱数を選ぶ必要があるため，利用者に与える負担が高く操作性において課題があった．一方，文献 2) では，パスワードに利用できる文字の配列を表示し，さらに各文字の下に，文字を認証のたびに異なるグループに分けるための数字を表示し，利用者は記憶するパスワードの各文字についてこのグループ分けの数字を順に入力することで認証を行う方式を提案している．この方式では，利用者にとっては，憶える情報はパスワードのみであるが，パスワードを使った一連の認証操作の途中でパスワードとは別の数字の入力が必要であり，依然として操作性において課題があった．これに対して，文献 3) では，乱数を使って認証画面のパスワード文字の背景を決定し，さらに背景を選択するためのボタンを認証画面に設けることで，パスワードとは別の数字の入力をなくし，利用者に与える負担を軽減している．この認証方式については，のぞき見が繰り

返された場合の安全性の評価式も導出されているが，のぞき見された後のパスワードの候補数はパスワードの 1 文字ごとに算出される．このため，のぞき見に対する安全性を高めるためにパスワードを長くしても，のぞき見を行う者に推定されるパスワードの候補数は 1 文字ごとの候補数を長さの分だけかけ合わせた数にしかならない．文献 4) では，文献 3) の方式の背景を白と黒の 2 つだけにし，暗証番号の 1 桁について背景が白か黒かの選択を複数回繰り返すことで認証を行う．さらに，のぞき見を行う者に推定されるパスワードの候補数が一定数以下にならないように選択回数を制限する方式が提案されているが，のぞき見の回数は 1 回としており，のぞき見が繰り返された場合の安全性については評価されていない．文献 5) の方式は，パスワードに利用できる文字をグループに分けて，その中の 1 つのグループを選択することで認証を行うことは文献 2)，3) と同じである．この方式では，1 つのグループ内の文字にだけ下線が引かれており，文字に下線が引かれているグループはシフトキーを押すごとに変わるようになっている．利用者がパスワードの文字に下線を引くように操作することで認証を行う．これにより，文献 3) と同じようにパスワードとは別の数字の入力をなくし，利用者に与える負担を軽減しているが，のぞき見に対する安全性の評価は被験者を使った実験でしか行われていない．

一方，人間の画像認識能力の高さに着目し，画像をパスワードにする認証方式[6)–8)] がこれまでにも提案されてきたが，これらの認証方式では毎回の認証時にパスワード画像がディスプレイ上に表示されるため，のぞき見に対して脆弱であることが報告されている[9)]．この問題に対して，文献 10) では，パスワード画像にモザイク画を用いることで，のぞき見を行う者に何が選択されているかを推定することを困難にする方式も提案されているが，のぞき見に対する安全性の評価は被験者を使った実験でしか行われていない．

本論文では，認証操作に対するのぞき見の問題に対して，特別なハードウェアを用いずにのぞき見に対する安全性を高めた個人認証方式として，背景配列の移動量を用いた認証方式[11)]（以降，単に移動量認証方式とする）を基に，複数のパスワードを用いることでのぞき見に対しての安全性を高めた認証方式（以降では，単に提案方式とする）を提案する．さらに，この提案方式の安全性を評価するための式の導出を行い，この式を使って従来の方式との比較を行う．また，操作性についても考察を行う．

2. 実行環境と認証方法

2.1 認証の実行環境

本論文では，認証を実行する環境として**図 1** に示す環境を想定する．利用者は，端末を使ってサービス提供者が提供する何らかのサービスを利用する者である．サービス提供者は，利用者へ何らかのサービスを提供する者あるいは装置で，サービスを提供する際には正規の利用者であることを確認するために個人認証を行う．攻撃者は，利用者の認証操作をのぞき見ることにより，利用者のパスワードを取得し，利用者になりすましてサービスを不正に利用することを試みる者である．端末は，利用者へ情報を表示するディスプレイと利用者からのキー入力を受付ける入力デバイスを備えた装置である．

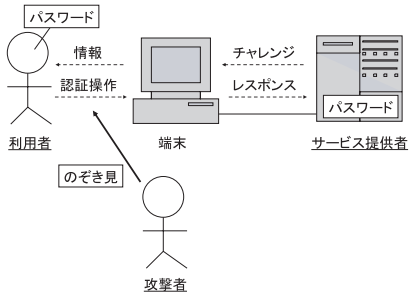

図 1　認証の実行環境
Fig. 1　An environment for authentication.

利用者とサービス提供者の間では，あらかじめ 1 つ以上のパスワードを共有しており，端末を介してチャレンジ・レスポンスによる個人認証を行う．サービス提供者からのチャレンジを基にして端末に表示される情報に対して，利用者がパスワードを基にした認証操作を行うことにより，端末でレスポンスが生成されてサービス提供者へ送り返される．サービス提供者側では，送り出したチャレンジに対して利用者と共有しているパスワードを用いて独自にレスポンスを求め，これを利用者側の端末から受け取ったレスポンスと比較することにより正規の利用者かを判定する．サービス提供者は，具体的には，ネットワークを介して端末に接続されたリモートホストであったり，端末に挿入された IC カードであったりする．

2.2 移動量認証方式

2.2.1 認証画面の構成と動作

提案方式の基となる移動量認証方式について説明する．**図 2** に認証画面を示す．認証画面は，上段のパスワード選択部と，下段の確定表示部から構成される．

パスワード選択部は，文字配列と背景配列から構成され，パスワードの選択に使用される．文字配列は，文字の二次元配列である．文字配列の要素は，パスワードに使用できる文

図 2　背景配列の移動量を用いた個人認証方式の認証画面
Fig. 2　Authentication method based on vector of background matrix.

字からなる．背景配列は，文字の背景の二次元配列である．背景配列の要素は，文字配列を表示する際に個々の文字の背景として使用される図形や色からなる．図 2 では，背景配列の要素に図形を用いている．1 つの背景配列には同じ背景が少なくとも 2 つ以上含まれ，背景配列の並びはサービス提供者からのチャレンジに基づいて決定される．確定表示部は，何文字のパスワードを決定したかを枠の中に “*”で表示する．

認証画面に対しての操作は，端末の上下左右の方向キーと入力キーおよびクリアキーの合計 6 つを使って行う．端末の上下左右の 4 つの方向キーのいずれかを押下すると，文字配列はそのままで，背景配列の要素だけが押下されたキーの方向に移動する．**図 3** に，方向キーによる背景配列の移動についての概念的なイメージを示す．図 3 では，背景配列の要素に色を用いている．背景には表示されている背景配列のパターンが繰り返して使用される．このため，たとえば下方向キーを押下して背景配列を下方向に移動すると，背景配列の最下段の要素が最上段に移動する．入力キーを押下すると，背景配列のそれまでの上下方向と左右方向の移動量を確定し，確定表示部の枠に “*”が 1 つ追加される．また，このとき同時に背景配列がランダムに移動する．この移動分は，端末の内部で入力キーの押下後に右方向（または左方向）と下方向（または上方向）のキーが移動した分だけ押下されたものとして移動量に追加される．クリアキーを押下すると，確定が 1 つクリアされ，確定表示部に表示されている “*”が 1 つ削除される．所定の回数だけ確定された後に，それまでに確定された上下方向と左右方向の移動量の配列がチャレンジに対するレスポンス値として端末からサービス提供者へ送られる．

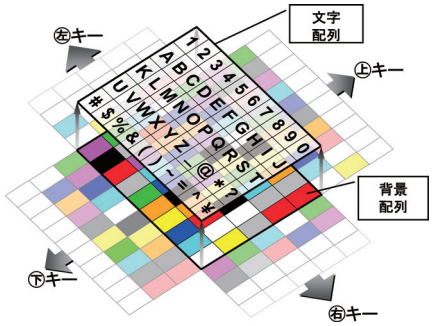

図 3　方向キーによる背景配列の移動
Fig. 3　Shift of background matrix by direction keys.

2.2.2　認証方法（認証フェーズ）

利用者は，上記の認証画面を使って認証操作を行う．利用者は，方向キーと入力キーを操作して，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せることで，サービス提供者に対して自身がパスワードを記憶している正規の利用者であることを示す．認証操作で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背景配列の中から任意に選択してよい．このため，使用する背景の種類は，あらかじめ決めておいたものではなく，認証のたびに変えることができる．利用者は，まずパスワードの 1 文字目で背景の種類を選び，2 文字目以降の文字の背景を 1 文字目で選んだ背景と同じ種類のものに合わせる．このため，パスワードの長さは 2 以上必要である．サービス提供者側では，認証を開始する際に，各要素を乱数により決定した背景配列を生成し，これをチャレンジとして端末へ送る．チャレンジに対するレスポンスを受け取った際に，チャレンジとレスポンスと登録済みパスワードとを基に，パスワードのすべての文字について同じ種類の背景が選択されているかをチェックすることで利用者の認証を判定する．

移動量認証方式による認証操作の例を，**図 4** に示す．この例では，パスワードとして “S2#JM@UD”があらかじめ登録されているものとする．このパスワードは，「週に 2 回はジムで運動」というパスフレーズの “回”を “#”に，“で”を “@”にそれぞれ置き換え，残りの部分をローマ字にして “Syuu ni 2# ha JiMu @ UnDou”と表記した中の大文字，数字，“#”および “@”だけを並べて作ったものである．図 4 の例では，パスワードの 3 文字目までの認証操作を示している．図 4 (a) は認証を開始した際に最初に表示された画面である．ここで，利用者はパスワードの背景としてバスを選択したものとする．まず，図 4 (a) に対

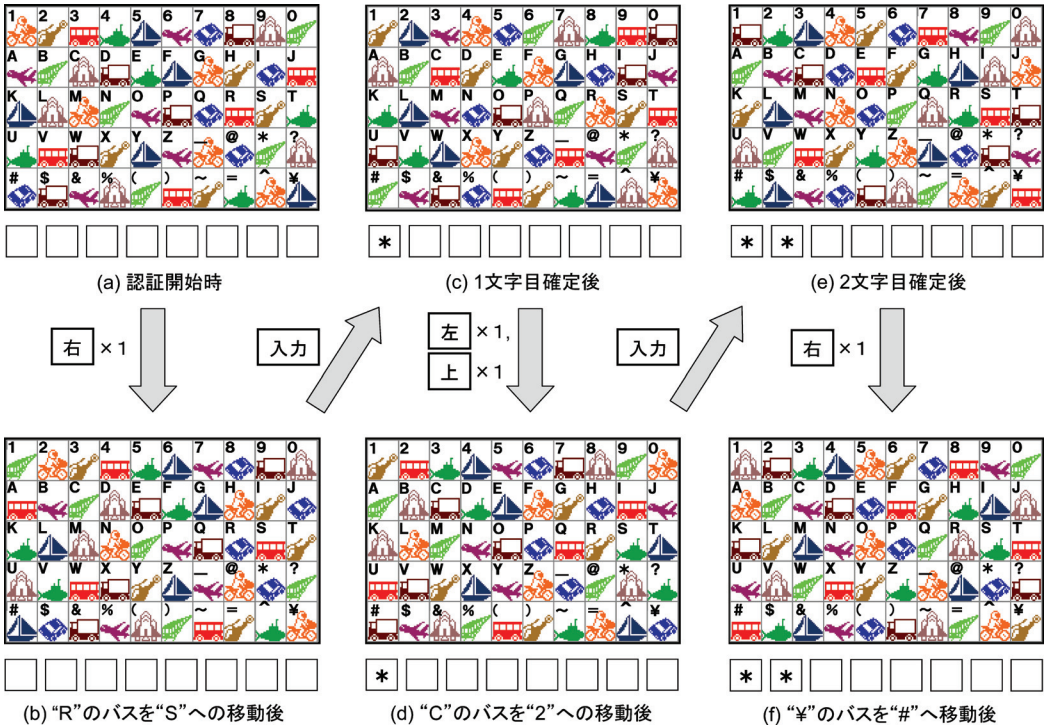

図 4　移動量認証方式による認証操作の例
Fig. 4　An example of operation with authentication method based on vector of background matrix.

し右方向キーを 1 回押下して “R”の背景のバスを 1 文字目のパスワード “S”の後へ移動させ（図 4 (b)），入力キーを押下して 1 文字目の背景を確定する．ここでは，“R”の背景のバスを使ったが，別の場所のバスを使ってもよい．入力キーを押下した後には背景配列は上下左右にランダムに移動する（図 4 (c)）．次に，認証画面図 4 (c) に対し左方向キーと上方向キーをそれぞれ 1 回押下して “C”の背景のバスを 2 文字目のパスワード “2”の後へ移動させ（図 4 (d)），入力キーを押下して 2 文字目の背景を確定する．入力キーを押下した後には背景配列は上下左右にランダムに移動する（図 4 (e)）．さらに，認証画面図 4 (e) に対し右方向キーを 1 回押下して “¥”の背景のバスを 3 文字目のパスワード “#”の後へ移動させ（図 4 (f)），入力キーを押下して 3 文字目の背景を確定する．以降同様に，パスワードの最後の文字まで，背景をバスに合わせて確定する操作を繰り返す．

2.2.3　パスワードの登録方法（登録フェーズ）

移動量認証方式では，サービス提供者側で認証を判定する際に平文のパスワードを使用する．このため，登録フェーズで端末からパスワードの登録更新を行う際には，利用者はパスワードをキーから直接入力する必要がある．さらに，携帯電話など 1 つのキーに複数の文字が割り付けられている端末を使用する場合には，どの文字が入力されているかを確認するために文字の画面への表示が必要である．したがって，端末からパスワードの登録更新を行う登録フェーズは，キー入力や画面を第三者に盗み見られない安全な場所で行うことが必要である．

2.3 提案方式

本論文では，のぞき見に対する安全性を高めるために，この移動量認証方式を基にして複数のパスワードを用いるように拡張した認証方式を提案する．利用者は登録フェーズであらかじめ複数のパスワードを登録しておき，認証を行う認証フェーズでは最初のパスワードから順にすべてのパスワードについて，パスワードの最初の文字で背景の種類を選び，残りの文字の背景を最初の文字で選んだ背景と同じものに合わせる操作を繰り返すことで認証を行う．利用者はすべてのパスワードについて登録している順番で認証操作を繰り返す．このとき，使用する背景の種類は，パスワードごとに異なるものを使用することができる．サービス提供者側では，登録済みのすべてのパスワードについて，各パスワードのすべての文字の背景に同じ種類が選択されているかをチェックすることで利用者の認証を判定する．たとえば，パスフレーズとして「9 時から会社．6 時に退社.」を使い，“から”を “〜”へ，“に”を “@”へ置き換えて残りをローマ字にして，“9 ji〜KaiSya．6 ji @ TaiSya.”としたものから，大文字，数字，特殊文字だけを抜き出して 2 つのパスワード “9〜KS”と “6@TS”として登録されているものとする．

認証フェーズでは，利用者はまず最初のパスワード “9〜KS”の背景をすべてバスに合せて，次に 2 つ目のパスワード “6@TS”の背景は “電車”に合わせるといった具合に認証操作を行う．このとき，各パスワードごとの背景が同じであればよいので，たとえば最初のパスワードの背景が電車で，2 つ目のパスワードの背景をバスとしてもよいし，最初のパスワードの背景が船で 2 つ目のパスワードの背景をトラックとしてもよい．サービス提供者側では，“9〜KS”の背景に同じ種類が選択されており，さらに “6@TS”の背景に同じ種類が選択されている場合のみ認証を成功とする．

提案方式の登録フェーズは，パスワードを複数登録する点以外は，移動量認証方式と同じである．

3. パスワードの推定に対する安全性評価式

3.1 パスワードの候補数

文字配列における文字の配列の行数を m，列数を n，背景の種類の数を b（b は 2 以上の整数で，m か n の約数）とすると，パスワードに利用できる文字の数は，$m \cdot n$ となる．攻撃者が 1 回も認証操作をのぞき見ていない状態でのパスワードの候補数は，パスワードの長さを λ（$\lambda \geq 2$）とすると，$(m \cdot n)^{\lambda}$ となり，この中に 1 つだけ本当のパスワードが含まれる．

以降では，このパスワード候補数に基づき，オンラインシステムや IC カードなどの試行回数が制限されたシステムに適用することを前提として，この条件下で行える攻撃に対しての安全性を評価する式を導出する．このため，ここではすべてのパスワード候補を総当たりで試す brute-force 攻撃はできないものとする．

3.2 移動量認証方式の安全性評価式

3.2.1 偶然に認証に成功する確率

移動量認証方式に対して攻撃者が適当に操作した際に認証が偶然に成功するのは，最初の文字の背景を確定した際の背景の種類と，2 文字目から λ 文字目までの背景を確定した際の背景の種類が同じになる場合である．最初の文字の背景の種類は b 種類の中のどれでもよいため，攻撃者が適当に操作した際に偶然に認証が成功する確率は，$1/b^{\lambda-1}$ となる．

3.2.2 認証を 1 回のぞき見た後のパスワード候補数

移動量認証方式の安全性を評価するために，認証操作を攻撃者がのぞき見たときに推定するパスワードの候補数を導出する．以降では，利用者は認証が必ず成功するように操作するものと仮定する．攻撃者が k 回の認証操作をのぞき見た後のパスワード候補数を $Npw(m, n, b, \lambda, k)$ とし，まず，攻撃者が 1 回の認証操作を見た後のパスワード候補数 $Npw(m, n, b, \lambda, 1)$ を求める．各背景は種類に関係なく均等に背景配列に登場するものとし，その登場数を c とすると，c は $m \cdot n/b$ で表される．パスワード文字は，1 回の認証を実施した際に背景が同じ種類であった b 個のグループに分けられる．各グループにはそれぞれ c 個の文字が含まれる．このため，パスワード候補数 $Npw(m, n, b, \lambda, 1)$ は，以下の式で表される．

$$Npw(m, n, b, \lambda, 1) = b \cdot c^{\lambda} = b \cdot \left(\frac{m \cdot n}{b}\right)^{\lambda} \tag{1}$$

3.2.3 認証を k 回のぞき見た後のパスワード候補数

次に，攻撃者が k 回の認証操作をのぞき見た後のパスワード候補数 $Npw(m, n, b, \lambda, k)$ を求める．移動量認証方式でパスワードの候補が 2 回目以降の認証を実行した際にも，候補として残るには，2 回目以降の認証でもパスワード候補の最初の文字の背景の種類と 2 文字目から λ 文字目までの残りの $\lambda - 1$ 個の文字の背景の種類が同じである必要がある．

移動量認証方式の認証画面には種類が同じ背景が複数カ所に登場するため，2 文字目以降のパスワードの背景を確定する際には，最初の文字の背景と 2 文字以降の文字の背景とに，背景配列内のまったく同一の背景が使用される場合と，種類は同じであるが背景配列内の別の背景が使用される場合とがある．この違いにより，パスワードの候補数 Npw は変化する．

この変化の原因を**図 5** に示す例を使って説明する．ここで，パスワードは “AB”の 2 文

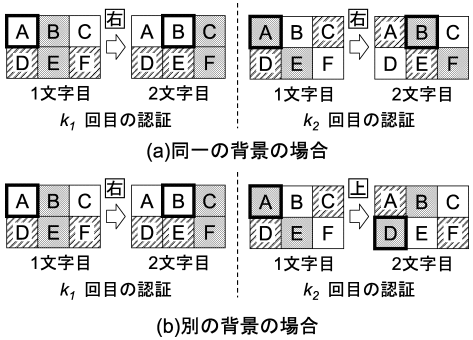

図 5　使用する背景によるパスワード候補数の変化
Fig. 5　A change of password candidates based on a background.

字とする．図 5 (a) では，k_1 回目の認証で 1 文字目の “A” の背景を白で確定し，2 文字目の “B” もこの同一の背景で確定している．次に，k_2 回目の認証で 1 文字目の “A” の背景を灰色で確定し，2 文字目の “B” もこの同一の背景で確定している．これら 2 回の認証をのぞき見た場合には，{AB，BC，CA，DE，EF，FD} がパスワード候補となる．一方，図 5 (b) では，k_1 回目の認証で 1 文字目の “A” の背景を白で確定し，2 文字目の “B” もこの同一の背景を使って確定し，さらに，k_2 回目の認証で 1 文字目の “A” の背景を灰色で確定するところまでは図 5 (a) と同じであるが，2 文字目の “B” は別の灰色の背景を使って確定している．これら 2 回の認証をのぞき見た場合には，{AB，BC，CA，FE} のみがパスワード候補となる．

このように，パスワードの最初の文字の背景と 2 文字以降の文字の背景に背景配列内のまったく同一の背景が使用される場合には，2 文字の相対的な位置関係がパスワードと同じものもそれぞれ同一の背景となる．図 5 (a) の例では，“AB” と同じ “BC”，“DE”，“EF” の背景もそれぞれ同一の背景となる．

一方，種類は同じであるが背景配列内の別の背景が使用される場合には，パスワードと同じ種類の背景でパスワード候補の 2 文字の背景が同じになる場合と，パスワードと異なる種類の背景でパスワード候補の 2 文字の背景が同じになる場合とがあり，パスワード以外のパスワード候補が同じ種類の背景になる確率 $P_0(m,n,b)$ は，以下の式で表される．

$$\begin{aligned} P_0(m,n,b) &= \frac{c-1}{mn-1}\cdot\frac{c-1}{mn-1}+\frac{mn-c}{mn-1}\cdot\frac{c}{mn-1} \\ &= \frac{1}{b}\cdot\frac{mn(mn-2)}{(mn-1)^2}+\frac{1}{(mn-1)^2} \end{aligned} \tag{2}$$

ここで，$mn \gg 1$ の場合には，$P_0(m,n,b) \simeq 1/b$ となる（以降では，$P_0 = 1/b$ とする）．

各認証回でパスワード内のある 2 文字に背景配列内の同一の背景が使用される確率は $1/c$，種類は同じであるが別の背景を使用される確率は $(c-1)/c$ である．1 回目の認証でパスワード内のある 2 文字に同一の背景が使用された場合に，さらに 2 回目の認証でもパスワード内のこの 2 文字に同一の背景が使用される確率は $1/c$，2 回目の認証でパスワード内のこの 2 文字に種類は同じであるが別の背景が使用される確率は $(c-1)/c$ である．これより，パスワード候補内のある 2 文字について，背景の種類が同じになる確率 $P_1(m,n,b)$ は，以下の式で表される．

$$\begin{aligned} P_1(m,n,b) &= \frac{1}{c}\left(\frac{1}{c}\cdot 1+\frac{c-1}{c}P_0\right)+\frac{c-1}{c}P_0 \\ &= \frac{b+c^2-1}{b\cdot c^2} \\ &= \frac{b^2(b-1)+m^2n^2}{bm^2n^2} \end{aligned} \tag{3}$$

パスワードの長さは λ であるので，パスワード候補の背景の種類がすべて同じになるためには，最初の文字の背景の種類と 2 文字目から λ 文字目までの $\lambda-1$ 個の文字の背景の種類が同じになることが必要である．したがって，λ 個の文字の背景の種類が同じになる確率 $P(m,n,b)$ は，以下の式で表される．

$$\begin{aligned} P(m,n,b) &= P_1(m,n,b)^{\lambda-1} \\ &= \left(\frac{b^2(b-1)+m^2n^2}{bm^2n^2}\right)^{\lambda-1} \end{aligned} \tag{4}$$

パスワード候補には利用者のパスワードが必ず 1 つ含まれることから，$Npw(m,n,b,\lambda,k)$ は，式 (1) の $Npw(m,n,b,\lambda,1)$ から本当のパスワード分の 1 を引いた値に，式 (4) の $P(m,n,b)$ を $k-1$ 乗したものをかけて，さらに本当のパスワード分の 1 を加えた値となり，以下の式で表される．

$$
\begin{aligned}
Npw(m,n,b,\lambda,k) &= (Npw(m,n,b,\lambda,1)-1)\cdot P(m,n,b)^{k-1}+1 \\
&= \left(b\left(\frac{m\cdot n}{b}\right)^{\lambda}-1\right) \\
&\quad\cdot\left(\left(\frac{b^2(b-1)+m^2n^2}{bm^2n^2}\right)^{\lambda-1}\right)^{k-1}+1 \qquad (5)
\end{aligned}
$$

式 (5) において，$(b^2(b-1)+m^2\cdot n^2)/(b\cdot m^2\cdot n^2)$ の値は，b が 2 以上の整数で m か n の約数であることから，1 より小さい値となる．さらに，λ が 2 以上であることより，攻撃者が認証操作をのぞき見た回数が k が増加するにつれて，パスワードの候補数は 1 に近づいていく．つまり，攻撃者にとっては本当のパスワードだけに候補を絞り込んでいけることが分かる．

ここで，$k-1$ のべき乗を行っている値が 1 より小さい値を $\lambda-1$ 乗したものであることから，λ を小さな値にすることで，のぞき見の回数 k の増加に対するパスワード候補数 $Npw(m,n,b,\lambda,k)$ の減少を緩やかにすることができることが分かる．

3.3　提案方式の安全性評価式

3.3.1　偶然に認証に成功する確率

提案方式に対して攻撃者が適当に操作した際に認証が偶然に成功するのは，各パスワードの最初の文字を確定した際の背景の種類と，各パスワードの 2 文字目以降の背景を確定した際の背景が同じになる場合である．登録したパスワードが d 個で，長さの合計が λ の場合を考えると，適当に背景を決めることができる各パスワードの先頭の d 個の文字に対して，残りの $\lambda-d$ 個の文字の背景の種類が各パスワードの先頭の文字の背景の種類と一致する必要がある．このため，攻撃者が適当に操作した際に認証が成功する確率は，$1/b^{\lambda-d}$ となる．これより，パスワードの合計の長さが同じ場合で考えると，登録パスワードの個数が多い場合の方が登録パスワードの個数が少ない場合よりも偶然に認証に成功する確率は高くなる．

3.3.2　認証を k 回のぞき見た後のパスワード候補数

提案方式について，攻撃者が k 回の認証をのぞき見た後のパスワード候補数を求める．利用者が d 個のパスワードを登録したとした場合に，攻撃者が想定するパスワードの長さを並べたものを $\{\lambda_1,\cdots,\lambda_i,\cdots,\lambda_d\}$ とし，その集合を S とすると，

$$
S=\left\{\{\lambda_1,\cdots,\lambda_i,\cdots,\lambda_d\}\mid 2\le\lambda_i,\lambda=\sum_{i=1}^{d}\lambda_i,1\le d\le\left\lfloor\frac{\lambda}{2}\right\rfloor\right\} \qquad (6)
$$

となる．ここで $\lfloor a\rfloor$ は，a 以下の最大の整数を表す．

長さ λ_i のパスワードの候補数は式 (5) より，以下の式で表される．

$$
\begin{aligned}
Npw(m,n,b,\lambda_i,k) &= \left(b\cdot\left(\frac{m\cdot n}{b}\right)^{\lambda_i}-1\right) \\
&\quad\cdot\left(\left(\frac{b^2(b-1)+m^2n^2}{bm^2n^2}\right)^{\lambda_i-1}\right)^{k-1}+1 \qquad (7)
\end{aligned}
$$

ここで，攻撃者が推定するパスワード候補の総数を $NdpwHigh(m,n,b,\lambda,k)$ とすると，この値は，登録したパスワードの個数を d とした際にとりうる集合 S の要素についての $Npw(m,n,b,\lambda_i,k)$ の総積を，集合 S ととりうるパスワードの個数 d について総和した値であり，以下の式で表される．

$$
NdpwHigh(m,n,b,\lambda,k)=\sum_{d=1}^{\lfloor\frac{\lambda}{2}\rfloor}\sum_{S}\prod_{i=1}^{d}Npw(m,n,b,\lambda_i,k) \qquad (8)
$$

式 (8) の $NdpwHigh(m,n,b,\lambda,k)$ では，1 つの長いパスワード候補と，これを単に複数に分割したものも候補として数えている．しかしながら，攻撃者が提案方式においてパスワード候補を試す場合には，これらの候補を 1 回の認証操作で試すことができる．

たとえば，長さ $\lambda=4$ のパスワードのパスワード候補の集合が $\{\{ABCD\},\{abcd\}\}$ の 2 つである場合に，長さ $\lambda=2$ のパスワードまでを含めて攻撃者が想定するパスワードの候補の集合は，$\{\{ABCD\},\{abcd\},\{AB,CD\},\{AB,cd\},\{ab,CD\},\{ab,cd\}\}$ となる．この中で，$\{ABCD\}$ と $\{AB,CD\}$ は，途中で背景の種類を切り替えることなく 1 回の認証で試すことができる．同様に，$\{abcd\}$ と $\{ab,cd\}$ も 1 回の認証操作で試すことができる．この 1 回の認証操作で試すことができる重複分を除外するには，偶数番目のパスワードの長さ λ_i については 1 だけ $Npw(m,n,b,\lambda_i,k)$ から引いた値を使用すればよい．これによって，先の例では，$\{AB,CD\}$ と $\{ab,cd\}$ がパスワードの候補から除外される．

この重複分を除外したあとの攻撃者にとっての実質的なパスワード候補の数を $Ndpw(m,n,b,\lambda,k)$ とすると，この値は以下の式で表される．

$$
Ndpw(m,n,b,\lambda,k)=\sum_{d=1}^{\lfloor\frac{\lambda}{2}\rfloor}\sum_{S}\prod_{i=1}^{d}(Npw(m,n,b,\lambda_i,k)-q) \qquad (9)
$$

ここで，q は $i+1$ を 2 で割った余りを表す．

4. 従来方式との比較

4.1 安　全　性

提案方式と移動量認証方式および従来の認証方式との比較を，これまで導出した式を使って行う．比較の対象とする従来方式には，文献 3) において安全性が評価されている認証方式を用いる．この認証方式の認証画面は，図 2 に示した提案方式の認証画面とほぼ同じであるが，背景を選択するため，画面の下部にさらに背景の種類数だけのボタンが 1 行追加されている．利用者はこのボタンを使ってパスワードの文字の背景を最初の文字から順に各文字ごと直接選択することで認証操作を行う．このため，認証操作では複数の文字から構成されるグループを攻撃者にも分かる方法で直接指定することになる．

この従来方式に対して攻撃者が適当に操作した際に認証が成功するのは，選択したボタンがパスワード文字の背景に一致する場合であり，この確率は，$1/b^{\lambda}$ となる．

従来方式において認証操作を k 回のぞき見た後のパスワード候補数 $E|Sk|$ を求める式についても文献 3) の中で導出されている．この式に，認証を 1 回ものぞき見ていないときのパスワード文字の候補数 $m \cdot n$ と，認証を 1 回のぞき見た後のパスワード文字の候補数 $(m \cdot n/b)$，パスワード数 λ をあてはめると，$E|Sk|$ は次の式で表される．

$$E|Sk| = \left(\left(\frac{\frac{m \cdot n}{b} - 1}{m \cdot n - 1} \right)^{k} (m \cdot n - 1) + 1 \right)^{\lambda} \tag{10}$$

本論文では，安全性の比較を，これまでに求めたのぞき見後のパスワード候補数，式 (5)，式 (9)，式 (10) を用いて行う．

文献 3) においては，パスワードの候補数以外にも，安全性を評価する値として，攻撃者が認証を試みた際にチャレンジを基にして表示される認証画面に対して，それまでにのぞき見た認証操作を基に認証されやすいレスポンスを推定して返す場合の認証に成功する確率を求めている．従来方式では，文字グループの選択はパスワードの各文字ごとに独立であり，与えられた認証画面において認証されやすいレスポンスを推定することは，最も多くのパスワード候補を含むグループを選択するだけであり，攻撃者にとっては簡単な判断である．

一方，提案方式および移動量認証方式では，背景配列を移動させることができる．したがって，認証されやすいレスポンスを推定して返すためには，とりうるすべての文字ととりうる背景（種類ではなく背景配列の個々の要素）と，さらに推定されるパスワードの長さとのすべての組合せの場合の数を考え，すべての場合における認証に成功する確率を計算し，

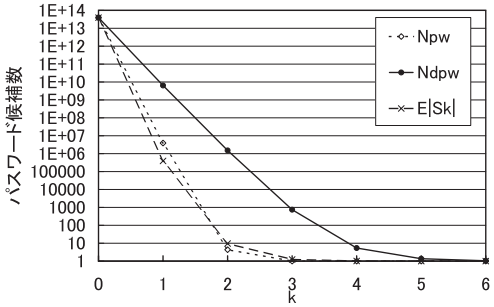

図 6　認証を k 回のぞき見た場合のパスワードの候補数（$m = 5$，$n = 10$，$b = 10$，$\lambda = 8$）
Fig. 6　Number of password candidates after k times of shoulder surfing $(m = 5, n = 10, b = 10, \lambda = 8)$.

この中で最も確率が大きくなる組合せを選ぶことが必要である．実際にこの計算を行うことは非常に困難である．このため，本論文では，認証されやすいレスポンスを返す場合に認証に成功する確率の導出は行わない．

パスワードの候補数の例として，図 2 の場合（各パラメータは，$m = 5$，$n = 10$，$b = 10$，$\lambda = 8$）について，式 (5)，式 (9)，式 (10) を用いて求めた結果を**図 6** に示す．図 6 より，移動量認証方式（Npw）でも，のぞき見の回数が 1 回の場合には，従来方式（$E|Sk|$）よりもパスワード候補数が多く残っていることが分かる．さらに，提案方式（$Ndpw$）では，のぞき見の回数が増加してもパスワード候補数が従来方式や移動量認証方式よりも多く残っている．この結果は，パラメータを変えても同じ傾向であり，提案方式によりのぞき見に対する安全性を向上させることができたと考える．

4.2 パスワードの長さとパスワード候補数

次にパスワードの合計の長さ λ を変えた場合のパスワード候補数とその増加率の変化を**表 1** に示す．表 1 より，移動量認証方式（Npw）では，パスワードを長くすると候補数が減ることが分かる．このことは，3.2.3 項の後半の部分において考察した内容と一致する．また，表 1 より，従来方式（$E|Sk|$）は，文字が長くなるのにともない候補数が一定の割合で増加していることが分かる．これは，従来方式のパスワード候補数がパスワードの各文字の候補数を長さの分だけかけ合わせた値であることにより説明できる．これに対して，提案方式（$Ndpw$）は，パスワードを長くした場合に，パスワードの長さが長くなっているにもかかわらずパスワードの候補数が減少している部分がある．たとえば，のぞき見回数 k が

表 1　パスワードの合計長を長くした際の候補数の増加率（$m = 5$，$n = 10$，$b = 10$）
Table 1　Increase rates of the number of candidates when total length of passwords is lengthend ($m = 5, n = 10, b = 10$).

k	認証方式	パスワード文字数												候補数増加率
		6 文字		7 文字		8 文字		9 文字		10 文字		11 文字		
2	$E\|Sk\|$	5.4	→	7.2										32.7%
				7.2	→	9.5								32.7%
						9.5	→	12.7						32.7%
								12.7	→	16.8				32.7%
										16.8	→	22.3		32.7%
	Npw	8.2	→	5.9										−28.1%
				5.9	→	4.3								−26.6%
						4.3	→	3.2						−24.7%
								3.2	→	2.5				−22.3%
										2.5	→	2.0		−19.5%
	$Ndpw$	$4.2 * 10^4$	→	$8.6 * 10^4$										102%
				$8.6 * 10^4$	→	$1.5 * 10^6$								1,647%
						$1.5 * 10^6$	→	$3.0 * 10^6$						99.4%
								$3.0 * 10^6$	→	$5.4 * 10^7$				1,711%
										$5.4 * 10^7$	→	$1.7 * 10^8$		222%
3	$E\|Sk\|$	1.17	→	1.20										2.7%
				1.20	→	1.23								2.7%
						1.23	→	1.26						2.7%
								1.26	→	1.30				2.7%
										1.30	→	1.33		2.7%
	Npw	1	→	1										0.0%
				1	→	1								0.0%
						1	→	1						0.0%
								1	→	1				0.0%
										1	→	1		0.0%
	$Ndpw$	151	→	93										−38.4%
				93	→	743								697%
						743	→	507						−31.7%
								507	→	4,065				700%
										4,065	→	4,002		−1.6%

3 回の場合で，パスワードが 6 文字から 7 文字に変化した際に候補数が 151 から 93 に減少している．このことは，複数のパスワードの個々の長さを考慮すると容易に理解できる．たとえば，パスワードの文字数の合計が 6 文字の場合に，できるだけ多くパスワードを登録しようとすると，2 文字のパスワードが 3 つになるが，これが 7 文字の場合には，パスワードを登録できる数は 3 つのままで，2 文字のパスワードが 2 つと 3 文字のパスワードが 1 つとなる．のぞき見の回数が増えるにつれて，3 文字のパスワードの方が 2 文字のパスワードに比べて，候補数が少なくなるため，この逆転現象が発生する．ここで見方を変えて，偶数文字から偶数文字へ増加分，奇数文字から奇数文字への増加分を調べると，k が 3 の場合にも，6 文字から 8 文字で 391%，7 文字から 9 文字で 444%，8 文字から 10 文字で 546%，9 文字から 11 文字で 688%，何れも候補数が増加していることが分かる．このこと

は，2 文字増えた場合には，登録できるパスワードの個数が必ず 1 つ増えるため，攻撃者が推定すべきパスワード長の組合せ数が増え，結果として全体の候補数が増加する．

ここで，このパスワード候補数の増加は，利用者がパスワードごとに種類の異なる背景を使用することを条件としており，種類の異なる背景を使用することを利用者に強制しない場合には，利用者はすべてのパスワードに同じ種類の背景を用いてしまうこともできる．このことを攻撃者が知りうる場合には，攻撃者はまず，利用者がすべてのパスワードに同じ種類の背景を用いて認証を行ったものとしてパスワード候補を推定し，この候補から試すことが予想される．このときのパスワード候補は，移動量認証方式として推定したものに一致する．このように，実際に利用者がすべてのパスワードに同じ種類の背景を用いて認証を行っていた場合には，提案方式をサービス提供者側で採用していても攻撃者が不正に認証に成功する確率は移動量認証方式と同じになってしまう．このことを防ぐために，提案方式では，利用者がパスワードごとに種類の異なる背景を使用することを必須にする必要があり，このためにサービス提供者側ではパスワードごとに種類の異なる背景を使用していない認証については，これをチェックして認証を失敗とすることが必要である．

したがって，提案方式では，利用者は 1 つの長いパスワードを憶えるのではなく，いくつかの短いパスワードを憶えて順に使うことが必要になる．利用者が 1 つのパスワードを分けて使うとした場合には，パスワードを憶えるのに加えて，さらに切れ目がどこであるかを憶えておく必要が生じ，この数が多くなるとこれを利用者が記憶する負担が大きくなる．

一方，パスフレーズによりパスワードを記憶する場合には，同じ長さのパスワードを憶えるとの比べて，憶える実際の情報量は増えるにもかかわらず，憶えるための利用者の心理的な負担がほぼ同じであることが実験を通して報告されている[12)]．パスフレーズの場合には，1 つのパスフレーズ内の意味のある一まとまりからパスワードを 1 つ作り，次の一まとまりから次のパスワードを作るようにしたり，意味の関連する複数パスフレーズの各フレーズから個々のパスワードを作るようにしたりすることで，切れ目を憶えるための負荷を新たに生じさせることなく複数のパスワードを憶えることができるものと考えられる．

また，文献 12) では，パスワードよりもパスフレーズの方がクラッキングが困難であったとの実験結果も報告されている．ただし，パスフレーズの場合も，パスワードに辞書上の単語をそのまま使わないように注意が必要であるのと同じように，パスフレーズに映画や劇の有名な台詞をそのまま使うと容易に推測される恐れがあるため，あくまでも他人に知られていない個人的なフレーズを使うように注意が必要であることが指摘されている[13)]．

このように，提案方式は，1 つの長いパスワードを憶えて分けて使うのではなく，パスフレーズを憶えていくつかの短いパスワードとして使うことで，のぞき見に対してパスワード候補を多く残し，安全性を高めるのに有効であるといえる．

しかし一方で，攻撃者が適当に操作した際に認証が成功する確率は，従来方式の $1/b^{\lambda}$ に対し，移動量認証方式は $1/b^{\lambda-1}$，提案方式は $1/b^{\lambda-d}$ であり，従来方式，移動量認証方式，提案方式の順に，さらに提案方式で登録パスワードの数が増えるにつれ，b 倍で大きくなる．このように，提案方式では，のぞき見に対する安全性が向上する半面，攻撃者による適当な操作に対する安全性が低下するトレードオフが存在する．

4.3　ATM への適用

次に，冒頭で取り上げた ATM への適用について考察する．現状の ATM では，PIN には 4 桁の数字が使用されており，攻撃者が適当に操作した際に認証が成功する確率は $1/10^4$ である．ATM では試行回数が制限されているため brute-force 攻撃はここではないものとする．

パスワードに使用できる文字を数字の 10 文字のみとし，背景配列を 2 行 5 列とすると，b は 10 の約数の 2 または 5 となる．まず，移動量認証方式を適用した場合を考えると，適当な操作で認証が成功する確率を現状と同じ $1/10^4$ 以下とするために必要なパスワードの長さ λ は，$b=2$ の場合で，$2^{\lambda-1}=2^{14}$（$=16384$）より，最低でも 15 文字，$b=5$ の場合で，$5^{\lambda-1}=5^6$（$=15625$）より，最低でも 7 文字となる．さらに，提案方式を適用した場合を考えると，のぞき見に対してのパスワード候補数が最も多く残るようにすべての登録パスワードを 2 文字とした場合にも，適当な操作で認証が成功する確率を現状と同じ $1/10^4$ 以下とするために必要なパスワードの合計の長さは，これを λ' とすると，$b=2$ の場合で，$2^{\lambda'/2}=2^{14}$ より，最低でも 28 文字，$b=5$ の場合で，$5^{\lambda'/2}=5^6$ より，最低でも 12 文字となる．

また，パスワードに使用できる文字を図 2 の認証画面にあるように英数字と特殊文字の 50 文字とし，背景配列を 10 行 5 列すると，b は 50 の約数の 2，5，10 または 25 となる．移動量認証方式で認証が成功する確率を現状と同じ $1/10^4$ 以下とするために必要なパスワードの長さ λ は，$b=2$ および $b=5$ の場合についてはパスワードが数字のみの場合と同じく，最低でもそれぞれ 15 文字と 7 文字となる．また，$b=10$ の場合で，$10^{\lambda-1}=10^4$（$=10000$）より，最低でも 5 文字，$b=25$ の場合で，$25^{\lambda-1}=25^3$（$=15625$）より，最低でも 4 文字となる．さらに，提案方式で，のぞき見に対してのパスワード候補数が最も多く残るようにすべての登録パスワードを 2 文字とした場合にも，適当な操作で認証が成功する確率を現状と同じ $1/10^4$ 以下とするために必要なパスワードの合計の長さ λ' は，$b=2$ および

$b = 5$ の場合についはパスワードが数字のみの場合と同じく，最低でもそれぞれ 28 文字と 12 文字となる．また，$b = 10$ の場合で，$10^{\lambda'/2} = 10^4$ より，最低でも 8 文字，$b = 25$ の場合で，$25^{\lambda'/2} = 25^3$ より，最低でも 6 文字となる．

実際には，合計の長さが 28 文字や 12 文字といったパスワードは，利用者が記憶することを考えると適用は難しいと考えられる．このため，提案方式を ATM に適用する際には，パスワードは数字だけでなく，英字および特殊文字も使用することが必要である．また，パスワードに英数字および特殊文字を使用するようにした際にも，25 種類の背景を使った場合には，これらの区別がつきにくいことと，背景配列から種類が同じ背景をさがすための利用者の負担が大きくなることが予想されるため実用的ではない．このため，ATM に提案方式を適用する際には，たとえば図 2 にあるように英数字と特殊文字含む 50 文字で背景が 10 種類の認証画面を使用し，パスワードの合計の長さが 8 文字以上とすることで，適当な操作で認証が成功する確率が現状と同じ $1/10^4$ を維持し，さらにのぞき見に対する安全性を高めたシステムが提供できる．

4.4 操　作　性

次に，提案方式の操作性について考察する．

まず，モバイル機器の文字入力の操作性に関する指標の 1 つとされている入力文字あたりのキー操作回数（KSPC）[14] について考える．ここでは，**図 7** を使って提案方式でパスワード 1 文字の背景を確定するのに必要なキー操作回数を求める．図 7 では，$m = 5$，$n = 10$ としている．また，利用者は最もキー操作回数が少なくなるように操作を行うこととする．

図 7 (a) は，黒塗りで示したパスワード文字の位置にちょうど目的の背景がある場合で，この場合のキー操作は入力キーの押下だけであり，キー操作回数は 1 回である．図 7 (b) は，パスワード文字に隣接した上下左右 4 つの位置のいずれかに目的の背景がある場合で，この場合には，上下左右のいずれかのキーを 1 回押下してパスワードの位置に目的の背景を移動させた後に入力キーを押下する．したがって，キー操作回数は 2 回となる．同様に，図 7 (c) から図 7 (g) は，必要なキー操作回数がそれぞれ 3 回，4 回，5 回，6 回，7 回である背景の位置を示している．背景配列は 5 行であるため，利用者は上方向または下方向のキーを 3 回以上押下することはない．また，背景の種類の数 b を 10 とした場合，各背景は種類が同じものが 5 つ存在するが，図 7 (g) に示すようにキー操作が 8 回となる位置は 2 つしかなく，5 つすべてがこの位置になることはない．このため，キー操作回数は最大でも 7 回となる．

次に，キー操作回数が h 回となる場合を考える．キー操作回数が h 回になる確率を $P_{KPC}(h)$ とし，さらにキー操作回数が h 回以上になる確率を $P'_{KPC}(h)$ とすると，$P_{kspc}(h)$ は以下の式で表される．

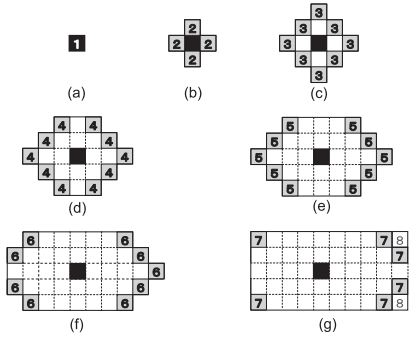

図 7　背景を確定するのに必要なキー操作回数（$m = 5$，$n = 10$）
Fig. 7　Keystrokes per Character to decide background ($m = 5, n = 10$).

$$P_{kspc}(h) = P'_{kspc}(h) - P'_{kspc}(h+1) \tag{11}$$

なお，キー操作は必ず 1 回以上になるため $P'_{kspc}(1)$ は 1 である．また，キー操作回数の最大値は 7 であるため，$P'_{kspc}(8)$ は 0 である．

ここで，提案方式の KSPC を E_{kspc} とすると，E_{kspc} は以下の式で表される．

$$E_{kspc} = \sum_{i=1}^{7} i \cdot P_{kspc}(i) \tag{12}$$

式 (12) は，式 (11) より，以下の式で表される．

$$E_{kspc} = \sum_{i=1}^{7} i \cdot (P'_{kspc}(i) - P'_{kspc}(i+1)) \tag{13}$$

さらに，式 (13) の総和を展開すると，

$$\begin{aligned} E_{kspc} = {} & P'_{kspc}(1) + P'_{kspc}(2) + P'_{kspc}(3) \\ & + P'_{kspc}(4) + P'_{kspc}(5) + P'_{kspc}(6) \\ & + P'_{kspc}(7) - 7 \cdot P'_{kspc}(8) \end{aligned} \tag{14}$$

となる．

$P'_{kspc}(h)$ は，キー操作回数が $h-1$ 回以下となる位置に目的の背景が 1 つも含まれていない確率に等しい．たとえば，$P'_{kspc}(3)$ は，キー操作回数が 2 回以下となる位置（図 7 (b)

に示した 5 つの位置）に目的の背景が 1 つもない確率に等しく，以下のように求められる．

$$P'_{KPC}(3) = \frac{45}{50} \cdot \frac{44}{49} \cdot \frac{43}{48} \cdot \frac{42}{47} \cdot \frac{41}{46} = \frac{45!}{40!} \cdot \frac{45!}{50!}$$

同様に，

$P'_{kspc}(2) = (45!/44!) \cdot (49!/50!)$
$P'_{kspc}(4) = (45!/32!) \cdot (37!/50!)$
$P'_{kspc}(5) = (45!/22!) \cdot (27!/50!)$
$P'_{kspc}(6) = (45!/12!) \cdot (17!/50!)$
$P'_{kspc}(7) = (45!/3!) \cdot (8!/50!)$

となる．また，$P'_{kspc}(1) = 1$，$P'_{kspc}(8) = 0$ であることより，これらを式 (14) に代入して E_{kspc} を求めると，2.7234 回となる．

KSPC は，移動量認証方式でも提案方式でも同じである．一方，文献 3) の従来方式では，パスワードの背景と一致するボタンを押下することで背景を選択するため，KSPC は 1 である．このほか，文献 14) には，携帯電話で広く利用されている，1 つのキーに割り付けられた複数の文字からキーの押下回数で入力文字を決定する “マルチタップ方式”について，入力文字にアルファベットとスペースの 27 文字からなる英語のコーパスを使用した場合の KSPC が求められており，2.0342 となっている．入力文字がパスワードのようにランダムなものでないことや，さらに入力文字の種類数が異なることから単純な比較はできないが，マルチタップ方式の入力文字の種類数は 27 と提案方式の入力文字の種類数 50 に比べて少ないことから，入力文字の種類数が同じであれば，提案方式はマルチタップ方式により直接パスワードを入力する方式と同程度のキー操作回数になるものと予想される．

次に，認証で使用するキーの数と操作性について考える．提案方式では，認証操作を端末の上下左右の方向キーと入力キーおよびクリアキーの合計 6 つのキーだけを使って行う．さらに，利用者が入力を間違えない場合に限ると，4 つの方向キーと入力キーの 5 つのキーのみを使用する “Five-key Text Entry”と呼ばれるテキスト入力方式となる．この入力方式は，利用者が手元のキーを確認せずに操作を行うことができる方式とされている[15]．また，キーの数が 10 個より少ない場合には，多少の練習で手元のキーを確認しなくても入力ができるようになることも実験により確認されている[16]．これらより，クリアキーを含めた場合でも，提案方式は利用者が手元のキーを確認せずに操作を行うことができる方式であると考えることができる．

最後に，提案方式で複数の背景から目的の背景を選択することについて考える．人間とコンピュータの相互作用（HCI）のモデルを使って複数の文字列リストから 1 つの文字列の場所を選択する行為にかかる時間は，候補の数を n，k を 200 ms/bit とすると，$k \cdot \log_2(n+1)$ となり，n が 10 の場合に 692 ms となることが算出されている[14]．提案方式では，背景のパスワードを 1 文字処理するごとに複数の背景から目的の背景を選択することが必要となる．ただし，提案方式では，目的の背景がパスワードの位置に近くにある場合や遠くにしかない場合などがあり，背景の種類の数を 10 とした場合にも，利用者が 10 個の候補から選んでいるかどうかは正確には分からない．また，提案方式では，目的とする背景をパスワードごとに変えることも必要である．このため，目的の背景を選ぶ行為が操作性に与える影響については定量的な評価も含めて今後の課題とする．

5. おわりに

本論文では，パスワード文字の背景配列の移動量を用いて認証を行うチャレンジ・レスポンス型の個人認証方式で複数のパスワードを用いる方式を提案し，提案方式の安全性を評価するために，提案方式についての解析を行い，攻撃者が認証操作をのぞき見た場合のパスワード候補数についての導出を行った．この結果から，複数のパスワードを用いる提案方式により，のぞき見に対する安全性をより高めることができることを示した．また，提案方式ののぞき見に対する安全性が，パスワード文字候補のグループの 1 つを直接選択する従来の個人認証方式と比べて高いことを示した．

参考文献

1) Matsumoto, T. and Imai, H.: Human Identification Through Insecure Channel, *EUROCRYPT '91*, LNCS-547, pp.409–421, Springer-Verlag (1991).
2) 井島裕昭，松本　勉：操作性の良い質問応答型個人認証方式，1994 年暗号と情報セキュリティシンポジウム講演会論文集，SCIS94–13C (1994).
3) 古原和邦，今井秀樹：均等写像を用いた質問応答型直接個人認証方式の覗き見攻撃に対する安全性について，電子情報通信学会論文誌 A，Vol.J79-A, No.8, pp.1352–1359 (1994).
4) Roth, V., Richter, K. and Freidinger, R.: A PIN-entry method resilient against shoulder surfing, *Proc. CCS '04*, pp.236–245, ACM Press (2004).
5) Tan, D.S., Keyani, P. and Czerwinski, M.: Spy-resistant keyboard: More secure password entry on public touch screen displays, *Proc. OZCHI '05*, Computer-Human Interaction Special Interest Group (CHISIG) of Australia, pp.1–10 (2005).
6) Dhamija, R. and Perrig, A.: Dejà Vu: A User Study Using Images for Authentica-

tion, *Proc. 9th USENIX Security Symposium* (2000).
7) Wiedenbeck, S., Waters, J., Sobrado, L. and Birget, J.-C.: Design and evaluation of a shoulder-surfing resistant graphical password scheme, *Proc. AVI '06*, pp.177–184, ACM Press (2006).
8) 高田哲司，小池英樹：あわせ絵：画像登録と利用通知を用いた正候補選択方式による画像認証方式の強化法，情報処理学会論文誌，Vol.44, No.8, pp.2002–2012 (2003).
9) Tari, F., Ozok, A.A. and Holden, S.H.: A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords, *Proc. SOUPS '06*, pp.56–66, ACM Press (2006).
10) 原田篤史，漁田武雄，水野忠則，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, pp.1997–2013 (2005).
11) 桜井鐘治，吉田真利子，撫中達司：モバイル個人認証の提案と評価，コンピュータセキュリティシンポジウム 2004（CSS2004），pp.625–630 (2004).
12) Yan, J., Blackwell, A., Anderson, R. and Grant, A.: The Memorability and Security of Passwords – Some Empirical Results, Technical Report No. 500, Computer Laboratory, University of Cambridge (2000).
13) Schneier, B.: *Applied cryptography (2nd ed.): Protocols, algorithms, and source code in C*, John Wiley & Sons, Inc., New York, NY, USA (1995).
14) MacKenzie, I.S.: KSPC (Keystrokes per Character) as a Characteristic of Text Entry Techniques, *Proc. Mobile HCI '02*, LNCS-2411, Berlin, pp.405–416, Springer-Verlag (2002).
15) MacKenzie, I.S. and Soukoreff, R.W.: Text Entry for Mobile Computing: Models and Methods, Theory and Practice, *Human–Computer Interaction*, Lawrence Erlbaum Associates, pp.147–198 (2002).
16) Ingmarsson, M., Dinka, D. and Zhai, S.: TNT: A numeric keypad based text input method, *Proc. CHI'04*, pp.639–646 (2004).

(平成 19 年 11 月 30 日受付)
(平成 20 年 6 月 3 日採録)

桜井　鐘治（正会員）

1989 年九州大学工学部電子工学科卒業．同年三菱電機（株）入社．以来，OS/ネットワークの開発に従事．現在，情報技術総合研究所において，ネットワーク，セキュリティ，金融システムに関する研究・開発に従事．ACM，IEEE-CS 各会員．

撫中　達司（正会員）

1986 年東京電機大学大学院理工学研究科数理学科修士課程修了．同年三菱電機（株）入社．以来，OS/ネットワークの開発に従事．現在，同社情報技術総合研究所において，ITS ネットワーク，モバイルネットワーク，センサネットワーク，ネットワークセキュリティに関する研究に従事．2007 年より東海大学専門職大学院組込み技術研究科非常勤講師．2005 年電気通信普及財団テレコムシステム技術賞（奨励賞）受賞．博士（工学）．電子情報通信学会，IEEE 各会員．