情報処理学会論文誌 Vol.59 No.1 179–188 (Jan. 2018)

改良型パターンロック覗き見耐性向上手法の提案と評価

稲村 勝樹[1,a)] 新林 直樹[1]

受付日 2017年4月11日, 採録日 2017年10月3日

概要：近年，スマートフォンやタブレット端末など，タッチパネルを有する携帯端末が普及し，時や場所を選ばずに様々な情報を利活用できるようになった．このような端末では，端末を利用する際にタッチパネルの入力を利用したユーザ認証を行うことで情報漏洩を防いでおり，なかでも Android 端末ではパターンロックと呼ばれる方式が採用されている．しかし，この方式では覗き見攻撃により簡単にパスパターンを記憶されてしまうといった問題がある．この問題に対し，東川らによってランダムに表示された数字列を一時的に記憶した後に入力することによって，パターンロックの覗き見耐性の向上を図る方式が提案されている．この方式において，記憶の増加や入力の複雑化によるユーザの利便性の低下といった課題がある．本稿では，入力パスパターンの方法を変更することで利便性の改善を図り，かつ覗き見耐性をさらに向上させる改良方式を提案し，その実装評価について述べる．これにより既存の携帯端末でパターンロックより安全なユーザ認証が実現できることを示す．

キーワード：スマートフォン，タブレット端末，タッチパネル，ユーザ認証，パターンロック，覗き見攻撃

Proposal and Evaluation of Improved Pattern Lock against Shoulder Surfing

Masaki Inamura[1,a)] Naoki Arabayashi[1]

Received: April 11, 2017, Accepted: October 3, 2017

Abstract: Recently, mobile terminals with touch-panel, e.g., smart-phones or tablets, have become widespread, and so users can use/access many types of information regardless of time and place. These terminals prevent leakage of information with user authentication using input on touch-panel, especially using pattern lock over Android. However, this authentication method has a problem of leakage of pass-pattern easily with shoulder surfing. Against this problem, Higashikawa et al. proposed a pattern lock method against shoulder surfing with memorizing a random digit string temporarily and entering it. However, the above method has a problem of deterioration in convenience for a user because of increasing user's memory and complication of input pattern. In this paper, we propose a improved method with modification in the input pass-pattern because of improving convenience and more protection against shoulder surfing. Furthermore, we show evaluation of usability and safety in our method. By using our proposal, safer user authentication method than pattern lock can be realized on existing mobile terminals.

Keywords: smart-phone, tablet, touch-panel, user authentication, pattern lock, shoulder surfing

1. はじめに

近年，スマートフォンやタブレット端末といった携帯端末の利用が広がっている．このような携帯端末は企業や大学などで活用される機会が増えるにつれ出荷台数も増加し，2016 年度には携帯端末の出荷台数が 4,533 万台に達すると予想されている [1]．

一方，携帯端末が普及するにともない，時や場所を選ばずに企業の秘匿情報や学内のプライバシ情報といった重要かつ機密な情報を携帯端末に保存しておく，あるいはこれらの情報にインターネットを経由してアクセスする機会が

[1] 東京電機大学理工学部
School of Science and Engineering, Tokyo Denki University, Hatoyama-machi, Hiki-gun, Saitama 350–0394, Japan
[a)] minamura@rd.dendai.ac.jp

増えている．このような状況において，携帯端末の紛失や盗難が発生すると，第三者にこれらの情報が漏洩してしまう可能性が生じる．それを防ぐために，携帯端末の不正利用対策が必要となる．

この不正利用の対策として一般的に搭載されている機能として，多くの携帯端末には利用を許可されていない第三者による操作を防ぐための画面ロック機能があり，このロックを解除するためにはログイン操作によるユーザ認証を行うようになっている．ここで一般的に利用されている認証方式としては，指紋認証 [2], [3] などの生体認証，英数字を用いたパスワード認証，画像認証 [4]，数字を用いた個人識別番号（PIN: Personal Identification Number）などのほか，Android が搭載されている端末ではパターンロックが採用されている．このパターンロックについては，オンライン時あるいはオフライン時に他人の監視下ではない状況における安全性の考察が行われている [5], [6]．しかし，屋外など不特定多数の他人がいる環境でログイン操作が行われることもあり，パターンロックによる認証方式では携帯端末を持つユーザの後方からユーザの操作を盗み見する覗き見攻撃（ショルダーサーフィン，またはショルダーハッキング）が懸念される．

この覗き見攻撃への対策について，スマートフォンが普及する以前から，いくつかの方式が検討されている [7], [8], [9], [10], [11], [12], [13], [14] が，その中でも東川らによってスマートフォンのパターンロックに特化した覗き見耐性のある認証方式が提案されている [15]．この方式には，パスパターンに対応する数字を認証時に毎回変更し，入力画面でその数字に合わせて画面をなぞっていくといった特徴がある．これにより認証時に入力パスパターンが毎回異なるため，認証情報をそのまま入力していた従来の方式に対して覗き見耐性が高くなる．しかし，東川らの方式を含めて，これまでの覗き見耐性を持つ認証方式では入力の複雑さなどにより利便性の低下が懸念される．

そこで本稿では，東川らの方式を改良し，覗き見耐性を維持しつつ，利便性の低下を抑えた認証方式を提案する．改良点は

- パスパターンに対応して記憶する数字の規則を変更，
- 入力画面での入力規則の追加，

の 2 点であり，これにより利便性の低下を抑えている．

本稿では，2 章で既存の関連認証方式とその課題について説明した後，3 章で本稿の提案方式のベースである東川らの方式の概要を説明し，4 章では改良した提案方式について述べる．5 章で東川らの方式との比較評価実験について述べ，6 章でまとめとする．

2. 関連認証方式

2.1 パターンロック以外の方式

パターンロック以外で採用されている古典的かつ一般的な認証方式として，パスワードによる認証があげられる．これは，ユーザ自身が自由に文字列を決定して携帯端末に登録し，認証時にはその登録した文字列を入力することで個人を識別する方式である．本来はパーソナルコンピュータなどある程度の大きさを持ったキーボードを用いることを想定した認証方式であり，スマートフォンのようなキーボードが搭載されていない端末では，画面にキーボードを表示して指で画面に接触しながら入力するなどの方式が必要となる．この場合，もしキーボードの配置が変わらないのであれば，指の動きは毎回固定されるため，入力文字数が多くても複数回の覗き見で攻撃が成功する可能性が高い（パスワード認証はパスワード入力時に周囲に人がいないことを前提とした方式であり，本来は文字数に関係なく覗き見をさせてはならない [16]）．これを防ぐには，後述する本稿の提案方式と同様に，入力パターンを変えるため画面に表示したキーボードの配置を変更する必要があるが，これはキーボードの文字種が多いため入力の利便性が著しく低下する．このような理由から，携帯端末におけるログイン操作時において，一般的なパスワードによる認証方式はほとんど採用されていない．

近年になって採用されている認証方式としては，指紋による生体認証があげられる [2], [3]．これは個人によって指紋特徴が異なることを利用し，センサに指を接触させて指紋を読み取り，個人の特定を行う方式である．最近ではセンサが小型化され，この指紋認証機能が搭載された携帯端末が出荷されている．一方で，指紋認証に対する攻撃手法は以前から研究されており，人工物を用いた指紋の偽造 [17]，写真で撮影した指の画像から指紋を特定する攻撃 [18] などが知られている．3 メートル離れたところからの撮影でも指紋を特定できており，指紋を撮影する機会は携帯端末利用時以外にも多く存在することから，覗き見耐性が高いとはいえない．また，人間の指を交換することは不可能であるため，1 度漏洩した指紋の情報は再利用することができない．指紋認証に用いられる指の数には制限があり，パターンロックやパスワードのように情報漏洩時の認証情報を更新することが容易でないといった課題も残されている．また，指紋認証用のセンサを搭載する必要があるが，このセンサの導入コストは低価格帯のスマートフォンなどには無視できず，タッチパネルだけで成立するパターンロックやパスワードと異なり，すべての携帯端末に指紋認証機能が搭載されているわけではない．したがって，タッチパネルのみで成立する認証機能を指紋認証にすべて置き換えることは難しいと考えられる．

指紋認証以外の生体認証としては，顔認証や虹彩認証を搭載した携帯端末の例があげられる [19], [20]．しかし，顔認証に対する攻撃手法 [21] や虹彩認証に対する攻撃手法 [22], [23], [24] が知られているほか，それぞれの認証方式においても認証情報の更新，導入コストといった指紋認

証と同様の課題をかかえている．

2.2 パターンロックの改良方式

2.2.1 fakePointer

fakePointer [12] は，入力画面における 0 から 9 までの数字と背景画像との組合せで，1 桁の値を入力する認証方式である．長期記憶している秘密情報は 4 桁の PIN であり，上記の入力を 4 桁分行う．背景画像は認証ごとにランダムに生成される使い捨てパスワードであり，認証開始前にユーザと安全に共有されるため，覗き見耐性のある認証といえる．しかし，認証を開始する前に，安全な通信路を用いてユーザと背景画像を共有しなければならないため，安全な通信路の設計が必要となる．また，認証サーバとの通信を前提とした認証方式であるため，携帯端末単体での画面ロック機能として採用しにくいといった課題がある．

2.2.2 STDS 方式

STDS（Secret Tap with Double Shift）方式 [13] では，秘密情報として利用者が覚えやすいアイコンとタップ位置のシフト情報を登録しておく．認証画面には 1 桁の入力につき 16 個のアイコンが表示される．パスアイコンをそのまま入力するのではなく，シフト情報に基づいてシフト後のアイコンを選択し，その該当するアイコンを入力する．しかし，画像の入力画面を覗き見されることで，シフト情報が漏洩するといった課題がある．その対策として，認証ごとにシフト情報をユーザが任意に決定できる機能がある．この対策により覗き見耐性を向上させることができるが，シフト情報をそのつど変更しなければならず，ユーザへの負担が大きい．

2.2.3 CCC 方式

CCC（Circle Chameleon Cursor）方式 [14] は，金庫の暗証番号入力用つまみを模したユーザインタフェースを持つ認証方式である．ランダムに変わる入力値を指し示すための位置を，振動を利用して認証ごとにユーザと共有する．受け取ったカーソルの位置に暗証番号のダイヤルを合わせることで入力を行う．入力位置を振動によってユーザのみに伝え，暗証番号ダイヤルを用いて間接的に入力しているので，録画攻撃を含めて覗き見耐性があるといえる．しかし，環境音のない静かな場所では振動の情報が露呈してしまい，入力情報が漏洩してしまう可能性がある．また，1 桁ずつ 4 回この共有を行わなければならないため，認証に時間を要する．

3. 東川らの認証方式

2.1 節で説明したパスワードや生体認証を用いた認証方式，および 2.2 節で説明したパターンロックの改良方式には，いずれも覗き見耐性を持たせるにあたってユーザの利便性が低下するという課題がある．それに対し東川らは，既存の携帯端末で採用されているパターンロックの入力方法をそのまま踏襲することでユーザの入力方式への理解や操作を容易にし利便性の低下を抑えつつ，入力時のパターンを規則に従って毎回変更することで覗き見耐性を持たせる認証方式を提案している [15]．この方式は主にパスパターン登録，数字の記憶，ログイン認証の 3 フェーズから構成される．この 3 章では，本稿の提案方式のベースとなる東川らの認証方式について説明する．

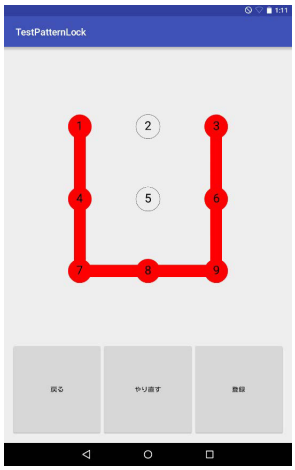

図 1 登録するパスパターン例
Fig. 1 Example of pass-pattern in the registration.

登録されるパスパターンと，数字の記憶との関係について説明する．一般的なパターンロック方式や東川らの認証方式でも採用されているパスパターンの登録方法は，ユーザが画面上に表示される 3 × 3 の計 9 個の点のうち，重複を許していくつかの点（通過点）を結んでいくものである．**図 1** の場合，左上の点から下に 3 個の通過点を通り，そこから右にさらに 2 個の通過点を結び，最後に右上の点まで 2 個の通過点を上に結び，計 8 個の通過点とその通過の仕方でパスパターンが構成されている（なお，図 1 では登録時にも各点に番号が振られているが，実装実験用のソフトウェアの画面設計の都合によるもので，この登録時にはこの番号は関係ないものとする）．数字の記憶を行うときには，この登録したパスパターンの通過点に従って，画面上に表示された番号を記憶していく．このとき，最初の画面では登録したパスパターンの最初の通過点から 3 個目の通過点まで計 3 個の通過点に位置している番号を，その通過した順番で記憶する．記憶したら次の画面に遷移し，登録したパスパターンの 4 個目の通過点から 6 個目の通過点まで計 3 個の通過点に位置している番号を，その通過した順番で記憶する．このように，登録パスパターンの通過点を 3 個ずつに区切りながら，その通過した順番で番号を記憶することを，通過点の最後の位置まで繰り返す．なお，登録したパスパターンの通過点が 3 の倍数でない場合は，その最後の記憶用の画面において最後の通過点までの位置の番号（1 個，または 2 個）を記憶し終了とする．

パスパターン登録，数字の記憶，ログイン認証の手順に

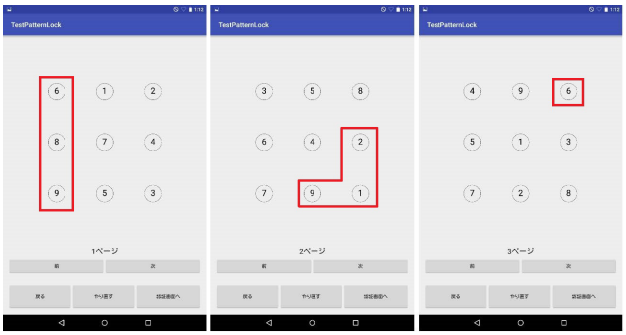

図 2 東川らの認証方式におけるチャレンジ画面（左より画面 1，2，3）

Fig. 2 Challenge screen in the method by Higashikawa and Manbo (screen 1, 2, 3 from the left).

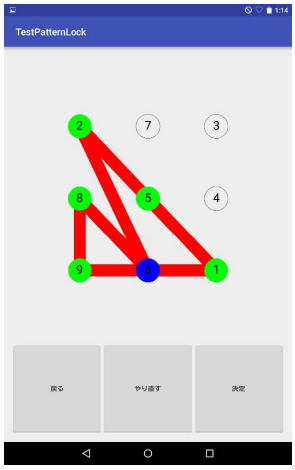

図 3 東川らの認証方式における入力画面と入力例

Fig. 3 Input screen and example of input pattern in the method by Higashikawa and Manbo.

ついて，図 1，**図 2**，**図 3** の例を用いて説明する．ログイン認証は以下の手順で行われる．

(1) 認証の基本となるパスパターンを決定し，端末に登録する．図 1 で示した例では，8 個の通過点とその通過の仕方が登録される．

(2) ログイン認証時は，まず 1 から 9 の数字がランダム配置された画面（これを『チャレンジ画面』とする）の 1 ページ目が表示されるので，登録したパスパターンの 1 個目から 3 個目まで計 3 個の通過点と同じ位置にある数字を，その通過した順番で記憶する（図 2 画面 1 赤枠箇所）．

(3) チャレンジ画面の 2 ページ目が表示されるので，登録したパスパターンの 4 個目から 6 個目まで計 3 個の通過点と同じ位置にある数字を，その通過した順番で記憶する（図 2 画面 2 赤枠箇所）．

(4) チャレンジ画面の 3 ページ目が表示されるので，登録したパスパターンの 7 個目および最後の計 2 個の通過点と同じ位置にある数字を，その通過した順番で記憶する（図 2 画面 3 赤枠箇所）．

(5) 手順 (2) から手順 (4) を記憶できるまで繰り返し，記憶できたら入力画面へ移る（図 2 によって記憶された数字の順番は “6899126” となる）．

(6) 図 3 ような 1 から 9 までの数字がランダムに配置された点が画面に表示されるので，手順 (5) で記憶した数字の順番になぞる．ただし，同じ数字が連続した場合は 1 個の数字と見なす．また，次の数字になぞる途中に数字の点がある場合，その数字をなぞってもよいこととする．手順 (5) の場合，記憶された数字のうち “9” が並んでいるので，なぞっていく数字の順番は “689126” となる．これを図 3 と照らし合わせると，“9” から “1” になぞる途中に “6” が，“1” から “2” になぞる途中に “5” があるので，実際のなぞる順番は “68961526” となる．

これによりログイン認証時に入力でなぞる指の軌跡が毎回変更されるため，覗き見耐性を持つことになる．ただし，図 3 にも示されるように，入力時の軌跡が複雑になり，誤入力の可能性が高まるなどの利便性の低下が懸念される．

4. 提案方式

4.1 改良点

本研究において，3 章の最後で述べた課題に対応するため東川らの方式を改良し，覗き見耐性を維持しつつ，利便性の低下を抑えた認証方式を提案する．その改良点について説明する．

1 点目は，パスパターンに基づく数字の記憶の規則変更である．東川らの認証方式では，登録したパスパターンに従い，通過点を先頭から 3 個ずつに区切り，各ページにおいてその通過点の位置に該当する箇所に表示されている数字を記憶する方式となっている．また，記憶する数字が連続した場合は，1 個の数字と見なすことになっている．この方式では，万が一記憶用のチャレンジ画面，および入力画面と指のなぞり方を覗き見により全部記憶されてしまった場合，入力画面の数字とチャンレンジ画面の数字を照らし合わせることで，パスパターンの軌跡を解読されてしまう可能性が残されている．それに対し提案方式では，各ページにおいて記憶する 3 個ずつの通過点のうち最初の位置（全体では $3n-2$ 番目の通過点の位置，n は自然数）に注目する．その位置の数字が奇数だった場合は，そのページの 1 個目と 2 個目を記憶して 3 個目は記憶しない，偶数だった場合は，2 個目と 3 個目を記憶して 1 個目は記憶しないといった規則に変更した．この変更により，仮に入力画面とチャレンジ画面を記憶されたとしても，登録されたパスパターンが解析されにくくなる．たとえばチャレンジ画面の 1 画面の例を**図 4** に示して説明する．この 1 画面において記憶する（あるいは入力画面で入力する）数字が “74” の順だとする．この場合，新たな数字の記憶の規則に基づく実際のパスパターンの候補としては，

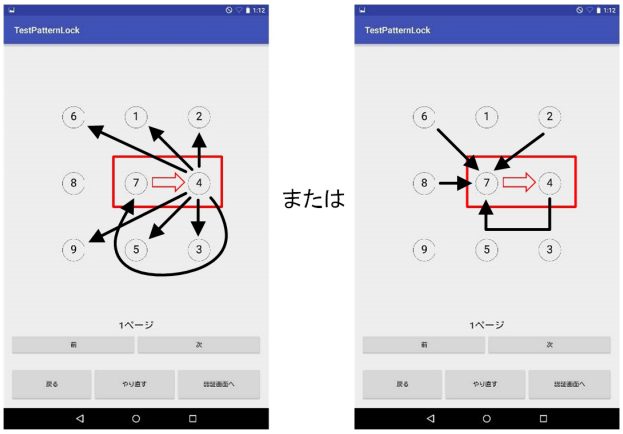

図 4 パスパターンの候補
Fig. 4 Prospect of pass-patter.

(1) “74” がこの画面における 1 個目，2 個目とするもの（図 4 の左側）．この場合，“741”，“742”，“743”，“745”，“746”，“747”，“749” がパスパターンの候補となる，
(2) “74” がこの画面における 2 個目，3 個目とするもの（図 4 の右側）．この場合，“274”，“474”，“674”，“874” がパスパターンの候補となる，

の計 11 種類が考えられる．記憶の数字を減らすには，同じように 1 個目で奇数・偶数の判断の後に 1 個目と 2 個目，1 個目と 3 個目を選択させる方法も考えられるが，この場合は 1 個目の情報が分かってしまう可能性が高く，2 個の数字の順序が確定され，提案方式よりも候補の数が減少する．したがって，提案方式のように 1 個目と 2 個目，2 個目と 3 個目を選択させる方法が良いと考えられる．図 4 で示したチャレンジ画面以外の場合，あるいは実際の入力画面の数字の配置によっては，このパターンの候補には変動があり，特に記憶する 1 個目の数字が偶数なら図 4 の左側に相当するパターンは該当しないが，それでも複数のパターンの候補がある．このことから，チャレンジ画面と入力画面を対応させたとしても，1 回の認証だけでは登録されているパターンを一意に特定することはできない．なお，記憶する 1 個目が偶数の場合は実際のパターンにおけるこの画面時の順番の 2 個目になるため，候補の数に偏りが出る場合がある．これを解消するには，記憶する数字に関する規則を複雑化する必要があるが，この場合はユーザが操作手順を理解するのが難しくなり，負担が大きくなることが懸念される．パターンの候補数を増やし特定されにくくすることとユーザの操作に対する負担をなるべく増やさないようにすることのバランスを考え，上記の方式を採用する．また，記憶する数字が連続した場合は，東川らの認証方式と同様とする．これについては，**図 5** に示すとともに，4.2 節の手順 (2) から手順 (4) で具体的に説明する．

2 点目は，入力画面での入力規則の追加である．東川らの認証方式では，チャレンジ画面で記憶した数字列をそのまま入力していた．その中で，端の点から他の点を通過せずに逆端の点をなぞる場合がある．**図 6** の例では，“8” から “9” へのなぞり方が該当する．この場合，その途中にある点と点の間（図 6 における “7” と “5” の間）を通過する際に，あやまって “7” か “5” を通過したと判定され，認証が失敗する可能性がある．その場合，改めて入力画面を提示して認証をやり直すことになるが，これは覗き見の機会を増やすことにつながり，パターンが解読されやすくなる．そこで提案方式では，図 6 の中央の点を必ず通過する入力規則を追加した．図 6 の場合，“8” から “9” へなぞるには “5” を通過することとする．これにより，あやまって点を通過する可能性が減少し，認証失敗の可能性が減少することで，覗き見の機会を減少させることができると考えられる．

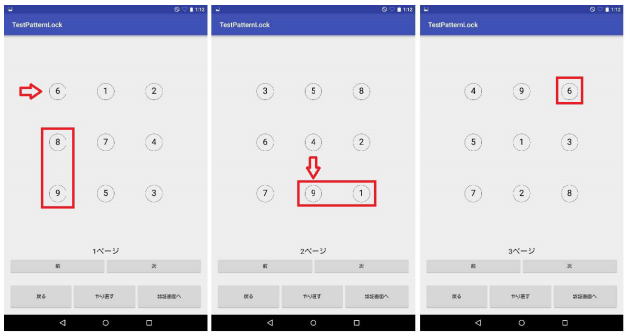

図 5 提案方式におけるチャレンジ画面（左より画面 1，2，3）
Fig. 5 Challenge screen in our proposal (screen 1, 2, 3 from the left).

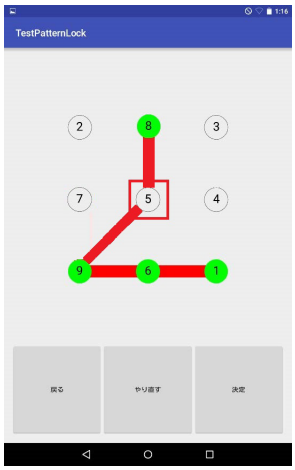

図 6 提案方式における入力画面と入力例
Fig. 6 Input screen and example of input pattern in our proposal.

4.2 認証手順

改良を行った認証方式の手順を以下に示す．

(1) 図 1 で示した例のように認証の基本となるパスパターンを決定し，端末に登録する．
(2) ログイン認証時は，まず 1 から 9 の数字がランダム配置された画面（これを『チャレンジ画面』とする）の 1

ページ目が表示される．このとき，この画面におけるパスパターンの通過点 1 個目の位置の数字に注目し，奇数ならば 1 個目と 2 個目，偶数ならば 2 個目と 3 個目と同じ位置にある数字を記憶する．図 5 画面 1 の場合，1 個目（矢印の位置）が偶数なので，2 個目と 3 個目を記憶する（図 5 画面 1 赤枠箇所）．

(3) チャレンジ画面の 2 ページ目が表示される．このとき，パスパターンの通過点 4 個目の位置の数字に注目し，奇数ならば 4 個目と 5 個目，偶数ならば 5 個目と 6 個目と同じ位置にある数字を記憶する．図 5 画面 2 の場合，4 個目（矢印の位置）が奇数なので，4 個目と 5 個目を記憶する（図 5 画面 2 赤枠箇所）．

(4) チャレンジ画面の 3 ページ目が表示される．パスパターンの通過点 7 個目の位置の数字に注目し，奇数ならば 7 個目と 8 個目，偶数ならば 8 個目と 9 個目と同じ位置にある数字を記憶する．図 5 画面 3 の場合，残りの通過点が 2 個以内であるため，そのままの数字を記憶する（図 5 画面 3 赤枠箇所）．

(5) 手順 (2) から手順 (4) を記憶できるまで繰り返し，記憶できたら入力画面へ移る（図 5 によって記憶された数字の順番は “8916” となる）．

(6) 図 6 ような 1 から 9 までの数字がランダムに配置された画面が表示される．

(7) 手順 (2)，(3)，(4) で記憶した数字を順番になぞる．ただし，東川らの方式のルールに加え，端から他の点を通らず逆端の点をなぞるルートが存在するときは中央の点をなぞることとする（図 6 の場合，“8” から “9” へなぞる途中で，赤枠で囲った中央の “5” をなぞるようにする）．実際のなぞる順番は “859616” となる．

5. 比較評価実験と結果の考察

5.1 実験条件

3 章および 4 章のそれぞれの方式について，以下の仕様の端末に実装し，比較評価実験を行った．

ハードウェア：ASUS 製タブレット端末 Nexus7

OS：Android5.1.1

本実験において，両方式におけるチャレンジ画面，および入力画面の数字の配置については JAVA 言語の乱数生成を用いてランダムに発生させた．なお，この場合で複数の認証を行ったとき，提案方式では登録されたパターンのある通過点に該当する箇所の数字をまったく使用せず，入力画面を完全に記憶されてもパターンと一致させることができない通過点が存在する可能性がありうるが，本実験において後述の 5.4 節で行った最大の覗き見回数である 5 回まで試行したうちに，そのような状態が発生したケースは認められなかった．

また，5 章では便宜上，東川らの方式を改良前，提案方式を改良後と表現する．

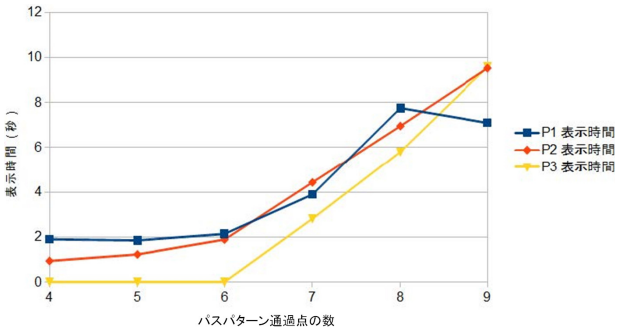

図 7 改良前におけるチャレンジ画面の平均表示時間

Fig. 7 Average display time in challenge screen before improvement.

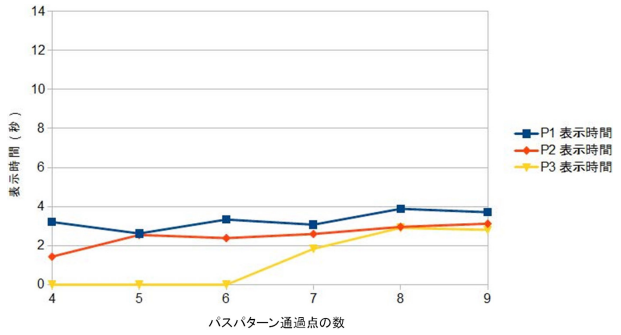

図 8 改良後におけるチャレンジ画面の平均表示時間

Fig. 8 Average display time in challenge screen after improvement.

5.2 平均表示時間

チャレンジ画面やパスパターン入力画面の表示時間が短いほど，覗き見攻撃は行われにくい．また，表示時間が短いということは認証におけるユーザの操作時間が短いということを意味し，ユーザへの負担がより少ないともいえる．したがって，できる限り表示時間が短い方が望ましいと考えられる．そこで被験者 8 名（全員が 20 代）による操作実験を行い，その平均表示時間を比較する．

図 7 に改良前におけるチャレンジ画面の各ページの平均表示時間，**図 8** に改良後におけるチャレンジ画面の各ページの平均表示時間を示す．図 7 から改良前においては，パスパターンの通過点の数が多くなるほど，各ページの表示時間が長くなることが分かる．一方，図 8 から改良後においては，パスパターンの通過点の数が多くなっても，各ページの表示時間は改良前以下，かつほぼ一定時間に収まっていることが分かる．このことから，ユーザへの記憶に関する負担が改良後で改善されていると推測される．さらに，パスパターンの通過点の数が多くなっても表示時間が増えないということは，改良後は通過点の数を増やしても攻撃者が覗き見できる時間が増えないということでもあり，通過点の数を増やすことでいっそうパターンの特定が難しくなることが期待できる．

次に，**図 9** に改良前・改良後における入力画面の平均表示時間を示す．この図から，改良前と比較して改良後は

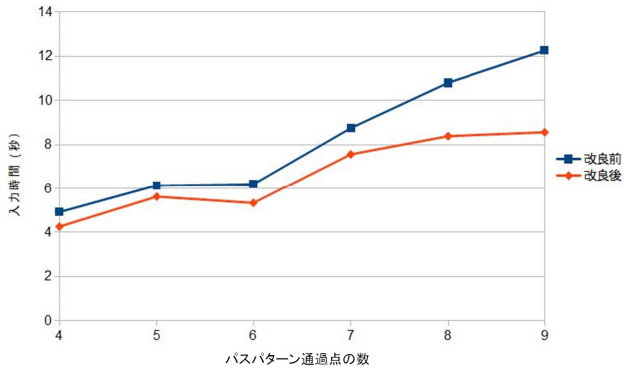

図 9 改良前・改良後における入力画面の平均表示時間
Fig. 9 Average display time in input screen before/after improvement.

表示時間が短くなっていることが分かる．このことから，入力時間が短くなることでユーザへの負担が改善されていると同時に，攻撃者に与える覗き見の時間が減少することで，より安全性が向上していると考えられる．

5.3 平均認証成功率

認証失敗が多い場合，入力操作が難しいことが考えられ，1 回の入力操作自体におけるユーザへの負担が大きいと考えられる．さらに，その操作の失敗時には認証の操作を繰り返し行う必要が生じ，よりユーザへの負担が増す．したがって，できる限り認証成功率が高くなることが望ましいと考えられる．そこで 5.2 節と同様に被験者 8 名（全員が 20 代）による操作実験を行い，その平均認証成功率を比較する．

図 10 に改良前・改良後における平均認証成功率を示す．改良前ではパスパターンの通過点の数が増加すると認証成功率が徐々に減少し，9 個では約 55%まで低下している．それに対して改良後では，通過点の数にかかわらず認証成功率は 80%以上を維持している．安全性を考慮するとパスパターンの通過点の数は多いほどよく，その場合において改良後ではユーザの入力失敗回数の削減が期待できる．また，認証の成功率が高いということは再度認証を行う必要性が低く，攻撃者に再度覗き見の機会を与える可能性が低いことにもなり，安全性の向上も期待できる．

5.4 覗き見耐性

実際に改良前に対して改良後の覗き見耐性がどれだけ向上しているかを比較するために，通過点の数が 4 個から 9 個のそれぞれのパスパターンにおいて，被験者がパスパターンを特定するまでに必要とした覗き見回数を計測した．

被験者は 4 名（全員が 20 代）でそれぞれ A，B，C，D とし，以下の条件で実験を行った．

- 覗き見できる回数の上限を 5 回とする．
- 認証失敗時は，認証の再操作時に覗き見していたとしても上記の回数に含めない．

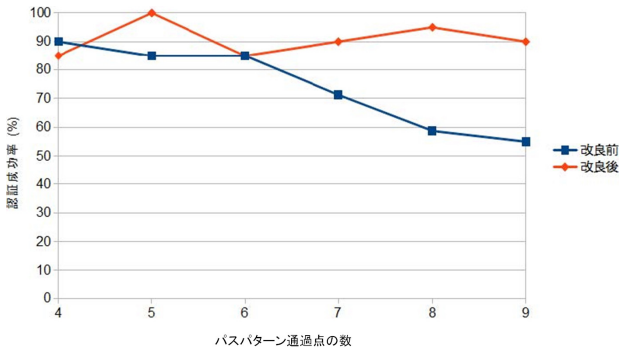

図 10 改良前・改良後における平均認証成功率
Fig. 10 Average success rate of authentication before/after improvement.

表 1 改良前の覗き見攻撃結果（被験者 A）
Table 1 Result of shoulder surfing before improvement (subject A).

通過点の数	攻撃結果	覗き見回数	特定された通過点の数
4	失敗	5	3
5	失敗	5	2
6	失敗	5	3
7	成功	4	7
8	成功	4	8
9	成功	5	9

表 2 改良前の覗き見攻撃結果（被験者 B）
Table 2 Result of shoulder surfing before improvement (subject B).

通過点の数	攻撃結果	覗き見回数	特定された通過点の数
4	失敗	5	3
5	失敗	5	3
6	失敗	5	1
7	成功	5	7
8	成功	5	8
9	失敗	5	7

- 認証していない状態ではメモをとることができる．
- それぞれの操作手順を理解しており，操作を行える．

なお，覗き見できる回数の上限については，後述の結果にあるとおり被験者 C を除き改良前において通過点の数が多いときには覗き見の回数が 5 回で攻撃が成功している場合があること，通常の携帯端末の使用条件において他人が覗き見できる状態でユーザが連続して認証を行う回数が 5 回を超えることは考えにくいことから，5 回と設定した．

はじめに，**表 1**，**表 2**，**表 3**，**表 4** に改良前におけるそれぞれの被験者の攻撃実験結果を示す．

この 4 名の中では被験者 D の攻撃成功数が多く，被験者 A や B も成功している箇所があることが示されている．また，通常ならパスパターンの通過点の数が増えれば全通過点の特定が難しくなると予想されるところが，被験者 A，D の結果から必ずしも通過点の数が増えても覗き見が

表 3 改良前の覗き見攻撃結果（被験者 C）
Table 3 Result of shoulder surfing before improvement (subject C).

通過点の数	攻撃結果	覗き見回数	特定された通過点の数
4	失敗	5	0
5	失敗	5	3
6	失敗	5	1
7	失敗	5	0
8	失敗	5	1
9	失敗	5	1

表 4 改良前の覗き見攻撃結果（被験者 D）
Table 4 Result of shoulder surfing before improvement (subject D).

通過点の数	攻撃結果	覗き見回数	特定された通過点の数
4	成功	4	4
5	失敗	5	4
6	成功	2	6
7	成功	5	7
8	成功	4	8
9	成功	3	9

表 5 改良後の覗き見攻撃結果（被験者 A）
Table 5 Result of shoulder surfing after improvement (subject A).

通過点の数	攻撃結果	覗き見回数	特定された通過点の数
4	失敗	5	2
5	失敗	5	2
6	失敗	5	2
7	失敗	5	0
8	失敗	5	5
9	失敗	5	6

表 6 改良後の覗き見攻撃結果（被験者 B）
Table 6 Result of shoulder surfing after improvement (subject B).

通過点の数	攻撃結果	覗き見回数	特定された通過点の数
4	失敗	5	2
5	失敗	5	1
6	失敗	5	0
7	失敗	5	2
8	失敗	5	0
9	失敗	5	2

表 7 改良後の覗き見攻撃結果（被験者 C）
Table 7 Result of shoulder surfing after improvement (subject C).

通過点の数	攻撃結果	覗き見回数	特定された通過点の数
4	失敗	5	1
5	失敗	5	1
6	失敗	5	0
7	失敗	5	0
8	失敗	5	0
9	失敗	5	0

表 8 改良後の覗き見攻撃結果（被験者 D）
Table 8 Result of shoulder surfing after improvement (subject D).

通過点の数	攻撃結果	覗き見回数	特定された通過点の数
4	失敗	5	2
5	成功	5	5
6	成功	3	6
7	失敗	5	4
8	成功	5	8
9	失敗	5	0

難しくなっていないことが示されている．これは，5.2 節，5.3 節でも示したとおり，通過点の数が増えると表示時間も長くなり覗き見できる時間が増えること，認証失敗の回数が増えることで実際に覗き見できる回数が多くなることから，攻撃の成功確率が増えたものと考えられる．また攻撃が失敗した場合でも，ある程度の通過点の数は特定できている場合が多く，さらに数回覗き見ができた場合は容易にパスパターンを特定できるものと考えられる．

次に，**表 5**，**表 6**，**表 7**，**表 8** に改良後におけるそれぞれの被験者の攻撃実験結果を示す．

改良後では，被験者 D を除き，いずれの通過点の数においても攻撃が失敗していることが示されている．また，被験者 D も，改良前では表 4 で示すとおり攻撃が成功できるパターンにおける通過点の数の種類が 6 種類中 5 種類だったのに対し，改良後では表 8 で示すとおり攻撃が成功できるパターンにおける通過点の数の種類が 6 種類中 3 種類に減少している．このことから，改良前よりも改良後の方が覗き見耐性が向上していると考えられる．また，被験者 D において，通過点の数が最も多い 9 個では攻撃が失敗していることが示されている．これについて，4.1 節で説明した改良点をふまえて考察する．1 点目の記憶の規則について，規則を複雑化することなく，かつそのチャレンジ画面から推測できるパターンの候補を複数にすることで，ユーザには記憶しやすく，攻撃者にはパターンを推測されにくくすることを目的としている．5.2 節の結果で示されているとおり，実際にチャレンジ画面の表示時間が一定であることから，記憶に関するユーザへの負担が改良前よりも軽減され，また覗き見攻撃の結果からパターンの推測がされにくいといった効果も得られていると考えられる．2 点目の入力規則について，通過時の誤入力が起きそうな箇所では中央の点を必ず通過することにより，誤入力を減らすことを目的としている．5.2 節，5.3 節の結果で示されているとおり，通過点の数が増えても表示時間はほとんど変わらず覗き見できる時間が増加していないこと，認証失敗の回数が通過点の数に依存せず一定で実際に覗き見できる回数がほとんど増加していないことから，改良前よりも誤操作

の回数が減少していると考えられる．このことが，覗き見攻撃の結果の改善につながっていると考えられる．

以上の結果から，改良後は改良前よりも覗き見耐性が向上していると考えられる．

5.5 部分情報によるパターンロック解除の可能性

通過点のうち，攻撃者が $3n$ 番目だけが分からない状態，すなわち $3n-2$ 番目と $3n-1$ 番目の通過点がすべて知られた場合において，もしすべてのチャレンジ画面における $3n-2$ 番目の数字が奇数だった場合は攻撃者が知っている $3n-2$ 番目と $3n-1$ 番目の通過点の情報だけでロックを外すことができる．この $3n-2$ 番目と $3n-1$ 番目の通過点がすべて知られたときのすべてのチャレンジ画面における $3n-2$ 番目の数字が奇数になる条件付き確率は $\left(\frac{5}{8}\right)^k$（$k$ はチャレンジ画面の数）となる．したがって，上記のような特殊条件において，改良後は改良前よりもセキュリティが低下する．

ただし，上記の条件のときに必ずしも改良前が安全であるとはいえない．それは，

- ある点から次の点に移動できる場合の数を考えたとき，自分自身と点対称の位置の点には移動できないので，ある点が真ん中の場合は次の点は 8 個，それ以外では次の点は 7 個の候補がある，
- 1 個前の点からある点に移動してくる場合も同様に，ある点が真ん中の場合は 1 個前の点は 8 個，それ以外では 1 個前の点は 7 個の候補がある，
- $3n$ 番目だけが分からない場合でも，その前後の点は知っているので，上記の候補の中から絞り込みが可能，
- （追加）経験的に実際の人間における指のなぞり方から，さらに確率的に通過点の候補が絞り込める，

といった理由により，$3n$ 番目の点の候補が限定されてくるからである．したがって，その候補になるパターンの絞り込みにより少ない回数でパターンロックを外すことができる可能性がある．あるいは，ユーザが次の認証を行ったときに，$3n$ 番目の点の候補だけに絞って覗き見により記憶することで，パターンの特定が容易になる．

なお，今回の実験結果において，上記のような特殊な点のみが発生して解読できるケースを確認できていない．今後，この条件が起こりうる可能性を検討する必要がある．

6. おわりに

本稿では，覗き見耐性を持つパターンロックについて，利便性を向上させるための改良方式を提案した．記憶する数字の個数を減らすための規則，および入力画面での誤操作が少なくなるような規則を導入することで，ユーザの認証における負担の増加を抑えながら覗き見耐性を向上させることを目指した．この提案方式について，実際に利便性と覗き見耐性が両立できていることを確認するために，改良前の方式である東川らの認証方式と合わせてタブレット端末に実装し比較評価実験を行った．その結果，提案方式はユーザに与える記憶に関する負担や入力の複雑さが改善され，改良前と比較して利便性が向上していることを示した．さらに，覗き見耐性の改善により安全性の向上が期待できることを示した．

今後は，より詳細に負担や安全性の評価を行うと同時に，今回の実験では簡単な固定パスパターンを利用しているため，より複雑なパスパターンでの検証を行う．また，被験者とパスパターンによっては提案方式でも覗き見攻撃が成功している場合もあるため，さらなる覗き見耐性向上について検討する．一方で，今回行った実験では覗き見耐性に関する検証を行う目的のため，操作の理解が早い 20 代を被験者とした．しかし，提案方式は少なくとも一般的なパスパターンよりも操作手順は複雑になるためユーザの学習が必要であり，携帯端末の操作に慣れていない（たとえば高齢者層の）ユーザに対して利便性が低下している可能性が考えられる．その点を検証するために，その操作手順の学習に必要となる時間などの評価を行う．いずれの場合も，通常のパスパターンや一般的な携帯端末の既存認証方法である PIN との比較も行う．

参考文献

[1] 独立行政法人情報処理推進機構：情報セキュリティ白書 2014 (2014).

[2] Igaki, S., Eguchi, S., Yamagishi, F., Ikeda, H. and Inagaki, T.: Real-time fingerprint sensor using a hologram, *Applied Optics*, Vol.31, No.11, pp.1794–1802, OSA (1992).

[3] Bahuguna, R.D. and Corboline, T.: Prism fingerprint sensor that uses a holographic optical element, *Applied Optics*, Vol.35, No.26, pp.5242–5245, OSA (1996).

[4] Suo, X., Zhu, Y. and Owen, G.S.: Graphical Passwords: A Survey, *Proc. Annual Computer Security Application Conference* (*ACSAC 2005*), pp.463–472, IEEE press (2005).

[5] Bellovin, S.M. and Merritt, M.: Encrypted Key Exchange: Password-based Protocols Secure against Dictionary Attacks, *Proc. IEEE Computer Society Symposium on Research in Security and Privacy* (*S&P '92*), pp.72–84, IEEE press (1992).

[6] 石黒 司，福島和英，清本晋作，三宅 優：モバイル端末のロック解除向けパターン認証の安全性評価，情報処理学会研究報告，コンピュータセキュリティ（CSEC），Vol.2012-CSEC-58, No.41, pp.1–6 (2012).

[7] Matsumoto T.: Human Identification Through Insecure Channel, *Proc. Advances in Cryptology* (*EUROCRYPT '91*), LNCS 547, pp.409–421, Springer (1991).

[8] Matsumoto, T.: Human-Computer Cryptography: An Attempt, *J. Computer Security*, Vol.6, No.3, pp.129–150, IOS Press (1998).

[9] 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のぞき見攻撃に対するさまざまな安全特性について，電子情報通信学会論文誌，Vol.J79-A, No.8, pp.1352–1359 (1998).

[10] Roth, V., Richter, K. and Freidinger, R.: A PIN-entry

Method Resilient against Shoulder Surfing, *Proc. ACM Conference on Computer and Communications Security* (*CCS 2004*), pp.236–245, ACM (2004).
[11] Tan, D.S., Keyani, P. and Czerwinsky, M.: Spy-resistant Keyboard: More Secure Password Entry on Public Touch Screen Displays, *Proc. Australia Conference on Computer-Human Interaction* (*OZCHI 2005*), pp.1–10, ACM (2005).
[12] 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).
[13] 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 (2014).
[14] 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，pp.501–503 (2014).
[15] 東川 創，満保雅浩：パターンロックの覗き見耐性向上手法について，暗号と情報セキュリティシンポジウム（SCIS 2015），2C1-4 (2015).
[16] 国民のための情報セキュリティサイト：ソーシャルエンジニアリング対策，総務省（オンライン），入手先 ⟨http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/staff/12.html⟩（参照 2017-10-10）.
[17] Matsumoto, T.: Gummy and Conductive Silicone Rubber Fingers, *Proc. Advances in Cryptology* (*ASIACRYPT 2002*), LNCS 2501, pp.574–576, Springer (2002).
[18] 産経ニュース：「ピースサインは危険!!」3 メートル離れて撮影でも読み取り可能，産経新聞（オンライン），入手先 ⟨http://www.sankei.com/affairs/news/170109/afr1701090002-n1.html⟩（参照 2017-10-10）.
[19] 富士通：arrows NX F-02H，入手先 ⟨http://www.fmworld.net/product/phone/f-02h/⟩（参照 2017-10-10）.
[20] サムソン：Galaxy S8/S8+，入手先 ⟨http://www.galaxymobile.jp/galaxy-s8/⟩（参照 2017-10-10）.
[21] Carman, A.: The Galaxy S8's facial scanner can, unsurprisingly, be tricked with a photo, *The Verge*, available from ⟨https://www.theverge.com/2017/3/31/15136226/samsung-galaxy-s8-face-scan-security⟩ (accessed 2017-10-10).
[22] 松本 勉：虹彩照合技術の脆弱性評価（その 1），電子情報通信学会研究報告，ユビキタスネットワーク社会におけるバイオメトリクスセキュリティ研究会第 1 回研究発表会予稿集，pp.53–59 (2003).
[23] 松本 勉：虹彩照合技術の脆弱性評価（その 2），コンピュータセキュリティシンポジウム（CSS 2003），pp.187–192 (2003).
[24] 松本 勉：虹彩照合技術の脆弱性評価（その 3），暗号と情報セキュリティシンポジウム（SCIS 2004），pp701–706 (2004).

稲村 勝樹 （正会員）

1972 年生．1998 年東京工業大学工学部有機材料工学科卒業．2000 年北陸先端科学技術大学院大学情報科学研究科博士前期課程修了．同年第二電電（株）（現 KDDI（株））入社，（株）京セラ DDI 未来通信研究所（退職時（株）KDDI 研究所，現（株）KDDI 総合研究所）配属．2014 年東京理科大学大学院工学研究科博士後期課程修了．同年東京電機大学理工学部理工学科情報システムデザイン学系助教，現在に至る．暗号・電子署名アルゴリズム，情報セキュリティ，サイバーテロ対策の研究に従事．電子情報通信学会，INSTICC 各会員．博士（工学）．

新林 直樹

1993 年生．2016 年東京電機大学理工学部理工学科情報システムデザイン学系卒業．同年（株）ラック入社，現在に至る．