モバイル端末に適したアイコンを用いた個人認証方式の録画攻撃耐性とユーザビリティに関する考察

和斉 薫 † 菅井 文郎 † 喜多 義弘 ‡ 久保田 真一郎 † 朴 美娘 ‡
岡崎 直宣 †

† 宮崎大学
889-1602 宮崎県宮崎市学園木花台西 1-1
tf1376014@student.miyazaki-u.ac.jp

‡ 神奈川工科大学
243-0292 神奈川県厚木市下萩野 1030

あらまし モバイル端末内の情報の漏洩を防ぐために，画面ロックとその解除認証方式が広く使用されている．しかし，混雑した場所で安心して利用できる覗き見耐性と高いユーザビリティを兼ね備えた認証方式は実現されていないのが現状である．アイコン画像とそれを選択するタップ入力を用いたモバイル端末向けの認証方式である SecretTap 方式は覗き見耐性と高いユーザビリティを有しているが，アイコンを選択する回数を増やすことで確率的誤認証に対する耐性を向上させるが，入力回数が多くなるためユーザビリティが低下する問題があった．また，複数回の録画攻撃に対する耐性を備えていない問題があった．本稿では，入力方法の工夫などによりこれらの問題を改善する方式である「SecretFlick 方式」「SecretVibe 方式」を提案し，覗き見耐性，ユーザビリティに関する評価を行った．

A Study for Shoulder-surfing Resistance and Usability of Icon-based User Authentication Method for Mobile Terminals.

Kaoru Wasai † Fumio Sugai † Yoshihiro Kita ‡ Shin-ichiro Kubota †
Mirang Park ‡ Naonobu Okazaki †

†University of Miyazaki
1-1 Gakuen-kibanadai-nisi, Miyazaki, Miyazaki 889-1602, JAPAN
tf1376014@student.miyazaki-u.ac.jp

‡Kanagawa Institute of Technology
1030 Shimo-hagino, Atugi, Kanagawa 243-0292, JAPAN

Abstract Some authentication methods to unlock the screen-lock on mobile terminals are widely used. However, there are few methods suitable for mobile terminals that have both shoulder-surfing resistant and high usability. The Secret-Tap method uses icon and tap-input and has high shoulder-surfing resistant and well usability. However, there is a problem that a lot of inputs are required in order to reduce the probability for breaking the authentication. It also has vulnerability to multi-time recording attacks. In this paper, we propose a method to improve these problems by introducing a new input method.

1　はじめに

近年，スマートフォンやタブレット等のモバイル端末が広く普及してきている．多くのモバイル端末の中には個人情報等の重要な情報が格納されており，これらの情報漏えいを防ぐため，画面の操作ロック及びPIN(Personal Identification Number) やAndroid Password Pattern [1] 等の個人認証方式を利用した画面ロック解除の認証が広く利用されている．しかし，既存の多くの認証方式では，人などに覗き見られることに耐性がなく，人の目にさらされた環境において認証を行うと，第三者に認証情報が露呈する可能性が高い．さらに，多くのモバイル端末はキーボードを搭載しておらず，タッチパネル液晶といくつかのボタンのみが標準の入力デバイスとして搭載されている．そのため，モバイル端末において既存の認証方式を用いると，入力方法の違いのためユーザビリティが低下する場合がある．そこで，高いユーザビリティと覗き見攻撃に対する耐性の両方を同時に備えたモバイル端末向けの認証方式が必要である．

Secret Tap 方式 [2] は，画面上のアイコンをタップ入力するだけの簡単な操作で高いユーザビリティを有し，覗き見耐性を強化した認証方式である．しかし，この方式には2つの問題が存在する．1つは，画像選択回数を増加させ，確率的誤認証に対する耐性を向上させる対策をとるが，この方法では認証のための入力回数が多くなるため，ユーザビリティが低下する問題である．もう1つは，覗き見耐性と1回の録画攻撃耐性は実現しているが、複数回の録画攻撃耐性は実現していない問題である．そのため，複数回の認証動作をカメラなどで録画され，解析されてしまうと認証情報が容易に露呈してしまう．そこで本研究では，2つの問題を改善する拡張方式を提案する．前者の問題に対し，Secret Tap 方式の入力方法であるタップ入力にフリック入力を追加した認証方式 Secret Flick 方式を提案する．この方式は，1回の入力において偶然に認証を突破される確率（確率的誤認証率）を低くし，十分安全な強度にするために必要な入力回数を少なくすることでユーザビリティの向上を目指す．2つ目の問題に対し，Secret Tap 方式にモバイル端末のバイブレーション機能を用いることで複数回の録画攻撃耐性を実現する SecretVibe 方式を提案する．この2つの提案手法に関して評価，考察を行う．

2　研究背景

2.1　モバイル端末における画面ロックおよび画面ロック解除認証

現在，デスクトップ端末，モバイル端末を問わず画面ロックを利用したセキュリティが広く普及している．画面ロックは，端末を操作できる状態からユーザが任意に，または，あらかじめ設定した時間内にマウスやキーボードなどの入力がなかった場合などに，端末の操作をできない状態にする機能である．この画面ロックを解除するためには，設定しているパスワードや暗証番号などを用いた個人認証が必要となる．画面ロックは，デスクトップ端末では席を外している間に，モバイル端末では紛失，盗難の際に，端末内の情報の盗難，改ざんを防ぐ目的がある．かばんの中やポケットの中に身に着けている状態でも画面ロックを行う．このため，メール，電話などモバイル端末の機能を使用する毎に画面ロックを解除する必要があり，モバイル端末はデスクトップ端末と比較して画面ロックの解除認証の頻度が非常に多くなってしまう．そこで，画面ロックの解除認証においてモバイル端末はデスクトップ端末よりもユーザビリティを配慮する必要がある．

2.2　覗き見攻撃

覗き見攻撃とは，攻撃者が人の記憶を用いてユーザの認証操作を覗き見ることで認証情報を不正に取得する攻撃方法である．この攻撃を防ぐ簡単な対策としては，ユーザが第三者に認証操作を見られないように注意することが考えられる．しかし，混雑した電車やエレベータの中などでは人の目を避けることが難しい場面も多い．覗き見攻撃に耐性を持たせるには，人間には記憶力と処理能力に限界があることを利用し，ある程度認証方式を複雑し，すべてを記憶することを困難にすることで耐性を持たせることが可能になる．しかし，認証方式を複雑にするこ

とでユーザビリティが低下してしまうおそれがある．

2.3 録画攻撃

録画攻撃とは，カメラなどの録画機器を用い，ユーザの認証画面，認証操作をすべてまたは一部を録画し，コンピュータを用いて解析する攻撃方法である．そのため，覗き見攻撃とは違い，記憶能力と処理能力の限界がない．したがって，録画攻撃耐性を持たせるには，覗き見攻撃に対する耐性を持たせることより複雑な認証方式が必要になり，頻繁に認証を行う画面ロック解除において，ユーザビリティを著しく損ねる．

3 関連研究

本章では認証方式の関連研究を述べる．

3.1 画像パスワード認証方式

この認証方式は，表示される画像からあらかじめ認証情報として設定したパスワード画像を選択するという簡単な操作で認証を行うため，高いユーザビリティを有している．また，人間は既知の画像の認識に長けていることから画像パスワード認証は認証情報の記憶が容易であるとされている [3]．既存の画像パスワード認証方式には，人間の顔の画像を用いる Passfaces [4] や画像にエピソード記憶を利用する事でユーザの記憶負荷を軽減する story [5] がある．しかし，これらの方式は，覗き見攻撃に対する耐性（覗き見耐性），録画攻撃に対する耐性（録画攻撃耐性）が低いため，第三者に認証操作を覗き見られると認証情報が簡単に露呈してしまう．また，覗き見耐性をもつ既存の認証方式には，fakePointer [6] や CDS [7]，背景配列の移動量を用いた認証方式 [8] がある．しかし，これらの既存の認証方式は，覗き見攻撃に対する安全性に重点を置いているため，ユーザビリティが低く，モバイル端末の画面ロック解除の認証に使用するには不向きである．

3.2 Secret Tap 方式 [2]

Secret Tap 方式は，アイコンを用いた覗き見耐性を持つ，タッチパネル液晶向けのチャレンジレスポンス型の認証方式である．事前に設定した認証情報（登録アイコンとシフト量）をもとに入力方法を工夫することで覗き見耐性と 1 回の録画攻撃耐性を実現させている．認証画面には，4 × 4 マスに 16 個のアイコンが表示され，その内の 1 つが事前に認証情報として設定されている登録アイコンであり，残りのアイコンはダミーのアイコンである．認証画面に表示される 16 個のアイコンを 2 × 2 マスの 4 つのグループに分割し，それぞれを第 1 象限から第 4 象限としている．登録アイコンが表示された象限を基準に，反時計回りにシフト量分シフトした象限内のいずれかのアイコンをタップすることで認証を行う．この認証操作をあらかじめ決めた入力回数繰り返し行い，すべての認証において正解した場合に認証成功となる．この認証方式は，2 × 2 マスのグループに分け，グループを入力することにより，どのアイコンが設定された登録アイコンであるかを隠蔽することが可能である．さらに，シフト量を設定する事で，どの象限グループが正解となっているかを隠蔽することを可能にしている．いる．

しかし，Secret Tap 方式には以下の 2 つの問題が存在する．

(1) 入力回数問題
米国国立標準技術研究所の「電子認証に関するガイドライン」[9] によると，パスワード及び暗証番号に必要な強度は $2^{14}(1/16384)$ とされており，この強度を本研究の目標の強度とする．Secret Tap 方式では，1 回の入力においての入力パターンが 4 通りであるため，入力 1 回における確率的誤認証率は 1/4 である．入力回数を n 回とすると確率的誤認証率は $1/4^n$ となり，目標の強度にするためには，7 回の入力回数が必要になる．これは，10 進数 PIN4 桁や Android password patturn と比較しても入力回数が多くユーザビリティが低い．さらに，入力回数を増やした場合，登録アイコンの数が入力回数よりも少ないと，同じ登録アイコンが複数回出現してしまうため，覗き見耐性の低下も懸念される．

(2) 複数回録画攻撃耐性問題

Secret Tap 方式は，一連の認証において毎回同じシフト量を用いるため，攻撃者はシフト量を 0 から 3 までそれぞれ仮定して解析することが可能である．このシフト量に基づき，1 回目の一連の認証操作の録画記録から，1 回の入力につき，入力された象限内の 4 個のアイコンを登録アイコンの候補として考える．2 回目の認証操作の録画記録からも同様に，シフト量毎に登録アイコンの候補を絞り込むことができる．シフト量の仮定毎に 1 回目と 2 回目のアイコンの候補を比較し，合致した登録アイコンの候補の数が多いシフト量の仮定が真のシフト量であり，合致したアイコンが登録アイコンではないかと推測することができる．このことから，Secret Tap 方式は 2 回以上の録画攻撃耐性を十分に実現していないことが分かる．

4 提案手法

本研究では Secret Tap 方式に新たな機能を追加することで入力回数問題を解決する Secret Flick 方式，複数録画耐性問題を解決する Secret Vibe 方式を提案する．

まず，Secret Tap 方式の確率的誤認証率を目標の強度にするとユーザビリティが低下する原因は，入力 1 回の確率的誤認証に対する耐性が低く，入力回数を増やす必要があるためである．そこで，従来のタップ入力にフリック入力を追加することで入力バリエーションを増やし，入力回数を少なくすることでユーザビリティの向上を目指す．この方式を Secret Flick 方式と呼ぶ．

次に，Secret Tap 方式が複数回の録画攻撃耐性を実現できていない原因は，一連の認証でシフト量が変わらないことで攻撃者がシフト量を仮定できてしまうことにある．そこで，Secret Tap 方式にユーザにしか伝わらない情報であるバイブレーションを導入し，認証中の毎回の入力時に認証情報を変化させ，複数回の録画攻撃耐性を実現する認証方式を提案する．この方式を Secret Vibe 方式と呼ぶ．

4.1 SecretFlick 方式

Secret Flick 方式を考案するにあたり目標を以下のように定めた．

(1) 覗き見攻撃に対する耐性

同じ人に何回認証動作を見られても認証情報が露呈することはない十分な強度を持つこと．

(2) 録画攻撃に対する耐性

1 回の録画攻撃に対して耐性を持つこと．複数回の録画攻撃に耐性を持たせるとダミーにしなければならない情報量が増えてしまい，認証手続きが複雑になる．そのため，モバイル端末では，頻繁に行う画面ロック解除認証において，ユーザビリティを著しく損ねてしまいユーザに受けいれられなくなってしまう．そこで，既存手法と同程度の 1 回の録画攻撃に対する耐性を持つことを目標とする．

(3) 確率的誤認証に対する耐性

米国国立標準技術研究所の「電子認証に関するガイドライン」[9] による，パスワード及び暗証番号に必要な強度 $2^{14}(1/16384)$ を目指す．なお，本提案手法において，毎回ランダムでアイコンが表示されるため，10 進数 PIN4 桁による認証方式に対して行われる brute-force 攻撃を行うことができない．

(4) ユーザビリティ

覗き見耐性を持つモバイル端末向け認証方式として，ユーザに受け入れられるユーザビリティを持つことを目標とし，以下の項目を考慮した．

- ユーザに負担がかからない入力回数を 4 回程度と仮定し，4 回程度の入力で十分な強度を実現すること．
- モバイル端末で使用されることを前提とし，片手で認証が行えること．
- スマートフォンの液晶の大きさ，約 4 インチの大きさの液晶でもストレス無く認証が行えること．

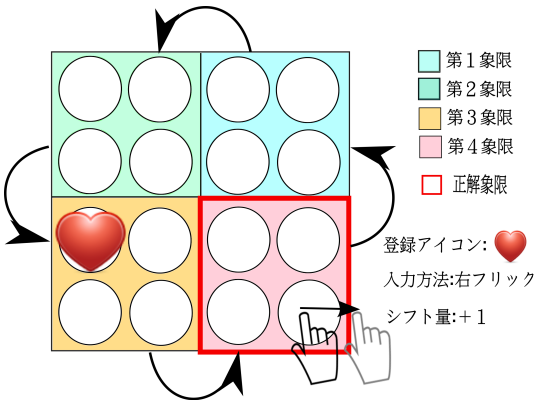

図 1: Secret Flick 方式の認証画面

事前に認証情報となる複数の登録アイコン，シフト量，登録アイコンごとの入力方法（上下左右方向のフリック入力かタップ入力のいずれか）を設定しておく．図 1 に Secret Flick 方式の認証画面を示す．ここで，登録アイコンが表示されている象限から設定したシフト量分だけ反時計回りにシフトした象限を正解象限とする．Secret Flick 方式では，表示されているそれぞれの登録アイコンに設定した入力方法，タップ入力またはフリック入力を正解象限内のいずれかのアイコンに対して行う．この操作を規定の入力回数繰り返し，すべて正確に入力できた場合，認証成功となる．図 1 で認証例を説明する．シフト量を+1，表示されている登録アイコンはフリック入力の右方向が設定されている．登録アイコンは第 3 象限に表示されており，シフト量が+1 であるから第 3 象限から反時計回りに 1 つシフトした第 4 象限が正解象限になる．ユーザはこの正解象限内のいずれかのアイコンにおいて，表示された登録アイコンに対応付けた入力方法である右向きのフリック入力を行うことで 1 回の入力が完了する．入力方法をタップ入力のみからタップ入力と 4 方向のフリック入力を追加することで 5 倍の入力バリエーションにすることができる．そのため，入力 1 回の確率的誤認証率を Secret Tap 方式の 1/4 から 1/20 まで下げることが可能である．したがって，提案手法は，目標の強度である $2^{14}(1/16384)$ にするために必要な入力回数を Secret Tap 方式の 7 回から 4 回まで少なくすることが可能である．

4.2 拡張 SecretFlick 方式

Secret Flick 方式には，新たな認証情報として登録アイコンごとに対応付けた入力方法を追加しているため，ユーザの記憶負荷が上がる問題がある．そこで，この方式の記憶負荷を軽減する拡張 Secret Flick 方式を提案する．この改良方式は，ユーザが事前に設定する認証情報であるシフト量を事前に設定せず，認証の初回で入力する象限をもとにシフト量を決定し，2 回目以降は初回の入力で決めたシフト量をもとに Secret Flick 方式による認証を繰り返し行う．ユーザはシフト量の存在のみを記憶しておき，具体的なシフト量を記憶しておく必要がないため，記憶負荷が軽減される．具体的には，認証の初回に入力した象限を正解象限とし，登録アイコンのある象限から正解象限までシフトしている量を認証に必要なシフト量として，2 回目以降の認証を行う．ただし，正解象限を選択する際には，表示されている登録アイコンにあらかじめ対応付けている操作（フリック入力の 4 方向またはタップ入力）により入力しなければならず，異なった操作により入力すると認証失敗となる．

4.3 Secret Vibe 方式

Secret Vibe 方式を考案するにあたり目標を以下のように定めた．

(1) 覗き見攻撃に対する耐性
　同じ人に何回認証動作を見られても認証情報が露呈することはない強度を持つこと．

(2) 録画攻撃に対する耐性
　複数回の録画攻撃に対して十分な耐性を持つこと．

(3) 　ユーザビリティ
　複数回の録画攻撃耐性を持つ認証方式として，ユーザに受け入れられるユーザビリティを持つこと．

Secret Vibe 方式は，事前に認証情報となる複数の登録アイコンとシフト量，振動パターンに対応付けたシフト量の変化値を設定する．

認証画面は，Secret Flick 方式と同様図 1 が表示される．認証画面が表示されると，同時に

無振動を含む 4 種類の振動パターンのうちランダムに選ばれた 1 種類が振動する．このとき，ユーザは振動パターンを感じ取り，事前に認証情報として設定したシフト量と振動パターンに基づくシフト量を足した値が真のシフト量となる．この真のシフト量を用いて，正解象限内のアイコンをタップ入力することで認証を行う．この操作を規定の入力回数繰り返し，すべて正確に入力できた場合，認証成功となる．

5　実装と評価

5.1　実装

各提案手法は Android 上で動作するアプリケーションとして実装した．実装環境は，プログラミング言語 Java を用い，統合開発環境 Eclipse と Android SDK を用いた．実装したアプリケーションの各提案手法の認証画面を図 2 に示す．Secret Flick 方式では，シフト量に基づいた正解象限のアイコンをタップ入力またはフリック入力する．設定した入力回数入力を行うと認証の成否の判定と認証完了までの時間がダイアログで表示される．

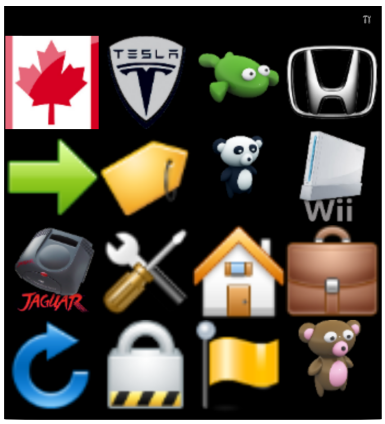

図 2: 提案手法の認証画面

5.2　確率的誤認証に対する耐性に関する評価

Secret Flick 方式と拡張 Secret Flick 方式，Secret Tap 方式，一般的に使用される 10 進数 PIN4 桁の確率的誤認証率を表 1 に示す．SecretVibe 方式の確率的誤認証率は，SecretTap と同じ強度である．同表において，目標の強度 $2^{14}(1/16384)$ に相当する強度を実現するときの入力回数を太字で示している．確率的誤認証率は，入力が n 回の場合，Secret Tap 方式は $1/4^n$，Secret Flick 方式は $1/20^n$，拡張 Secret Flick 方式は $1/\left(5 \times 20^{n-1}\right)$ となる．Secret Tap 方式では，入力回数が 7 回の場合に 1/16384 となり，目標の強度に相当する．しかし，7 回の入力回数は，ユーザビリティの観点から実用的とは言えない．Secret Flick 方式では，入力回数が 4 回の場合 1/160000 となり，目標の強度を大きく上回る．拡張 Secret Flick 方式は，認証の最初の入力においてどの象限の入力も許すため Secret Flick 方式と比較し，確率的誤認証率が上がるが，入力回数は 4 回で目標の強度に到達する．

表 1: 既存手法と提案手法の確率的誤認証率の比較

	3 回	4 回	5 回
Secret Tap	1/64	1/256	1/1024
Secret Flick	1/8000	**1/160000**	1/3200000
拡張 Secret Flick	1/2000	**1/40000**	1/800000
10 進数 PIN	1/1000	1/10000	**1/100000**
	6 回	7 回	n 回
Secret Tap	1/4096	**1/16384**	$1/4^n$
Secret Flick	1/16400000	1/128000000	$1/20^n$
拡張 Secret Flick	1/16000000	1/320000000	$1/(5 \times 20^n)$
10 進数 PIN	$1/10^6$	$1/10^7$	$1/10^n$

5.3　覗き見耐性に関する評価

提案手法が実際に覗き見耐性を実現しているかを調べる目的で，実装したアプリケーションを用いて評価実験を行った．被験者は，宮崎大学工学部情報システム工学科に所属する学生 16 人で行った．評価実験では，まず，各手法の概要と覗き見耐性および録画攻撃耐性についてを十分説明した後，実際に被験者にアプリケーションの操作及び認証を行ってもらった．その後，被験者の目の前で提案手法をそれぞれ 10 回ゆっくり行い，認証情報である登録アイコン，シフト量，登録アイコンに対応付けた入力方法を推測してもらった．この評価実験を各提案手法それぞれ認証情報を変更して 2 回ずつ繰り返し行った．本実験では，認証情報である登録アイコン，シフト量，登録アイコンに対応付けた入力方法のすべてが正解した場合に覗き見攻撃が成功し

たものとした．また，ユーザビリティの観点から評価実験は入力回数を 4 回，登録アイコンの数を 4 個に設定した．なお，事前に被験者に教えていない．

評価実験の結果，すべての提案手法について，被験者は認証情報を正しく推定することができず，十分な覗き見耐性を有していることが確認できた．しかし，Secret Flick 方式，拡張 Secret Flick 方式においては，登録アイコンは推定されなかったが，フリック入力，タップ入力といった入力操作を推定されてしまった．

5.4 複数回の録画攻撃耐性に関する考察

Secret Vibe 方式では，タップ入力する毎にバイブレーション機能の振動パターンによりランダムにシフト量を変化させる．こうすることにより，複数回録画攻撃耐性問題の原因である一連の認証で固定のシフト量となることを防ぐことができる．バイブレーションの振動はカメラで録画することができず，音もカメラには録音されない程度の音であり，振動パターンは，カメラの録画には記録されないと考えられ，ユーザのみに真のシフト量が伝えられる．そのため，シフト量を仮定し，タップ入力毎に，認証情報となるアイコンの候補を仮定すると複数回の録画攻撃ではアイコンを特定することはできない．このことから，Secret Vibe 方式は，Secret Tap 方式と比べ，複数回の録画攻撃耐性に対する耐性が向上していると考えられる．

5.5 ユーザビリティに関するアンケート結果と考察

提案手法がユーザに受け入れられるユーザビリティを有しているかを評価する目的でアンケート調査を行った．被験者は 5.3 節の評価実験と同じである．Secret Tap 方式と提案手法の説明を行い，実際にアプリケーションを使用してもらい，評価実験を行った後でアンケートに答えてもらった．それぞれの手法について SD(Semantic Differential) 法を用い主観的な印象度，認証方式において許容できる入力回数を答えてもらった．また，確率的誤認証率に関して，被験者が回答した許容回数における強度は安心と思うかを回答してもらった．SD 法を用いて取得した各項目の印象語と得点の対応関係を表 2 に示す．SD 法の得点は，高いほど肯定的であり，低いほど否定的な評価となる．SD 法によるアンケート結果を表 3 に示す．同表において，数値は得点の平均値であり，括弧内の値は被験者が回答した得点の標準偏差である．

アンケートの結果，Secret Flick 方式と拡張 Secret Flick 方式は,「確率的誤認証の安心さ」の項目で Secret Tap 方式を大きく上回った．被験者の入力の許容回数は，どの認証方式でも約 4 回であり，Secret Flick 方式と拡張 Secret Flick 方式はこの入力回数において確率的誤認証率は十分な強度をもつ．そのため，Secret Flick 方式，拡張 Secret Flick 方式は，実現可能なユーザビリティで安全性を確保できている．

表 2: 各手法の印象に関する測定項目と得点

測定項目	印象語と得点
理解のしやすさ	難しい 1 点 ← → 5 点 容易
使いやすさ	使いにくい 1 点 ← → 5 点 使いやすい
覚えやすさ	覚えにくい 1 点 ← → 5 点 覚えやすい
覗き見耐性があることで安心と感じたか	安心でない 1 点 ← → 5 点 安心
確率的誤認証について安心と感じたか	安心でない 1 点 ← → 5 点 安心
使いたいと思うか	使いたくない 1 点 ← → 5 点 使いたい

表 3: SD 法による各認証方式の印象度の結果

	理解のしやすさ	使いやすさ	覚えやすさ	(覗き見耐性) 安心さ	(確率的誤認証) 安心さ	使いたいと思うか	許容回数
Secret Tap	4.6(0.4)	4.6(0.5)	4.6(0.9)	4.2(0.7)	3.1(1.2)	4.2(1.2)	4.8(0.9)
Secret Flick	4.3(1.0)	3.9(1.0)	3.1(0.9)	4.6(0.5)	4.6(0.9)	4.0(0.9)	4.0(0.7)
拡張 Secret Flick	4.4(0.7)	4.3(0.8)	3.5(0.7)	4.7(0.5)	4.7(0.4)	4.1(0.8)	4.4(0.9)
Secret Vibe 方式	4.2(0.4)	3.3(0.5)	3.4(0.9)	4.7(0.4)	3.2(0.8)	3.7(0.9)	4,2(1.0)

しかし，Secret Flick 方式と Secret Vibe 方式は,「使い易さ」,「覚えやすさ」の項目で Secret Tap 方式よりも低くなっている．これは，Secret Flick 方式と Secret Vibe 方式が従来方式に新たな認証操作と認証情報を追加したためと考えられる．また，Secret Vibe 方式は，被験者が振動パターンを設定できない状態のため，これらの項目が既存方式よりも低下したのではないかと考える．拡張 Secret Flick 方式は，Secret Flick 方式よりも「覚えやすさ」の項目が高く，記憶

負荷の軽減を実現していると考えられる.「覗き見攻撃に対しての安心さ」の項目について，Secret Vibe 方式は Secret Tap 方式と比較し高くなっている.「理解のしやすさ」,「覗き見攻撃に対しての安心さ」の項目について，各提案手法は Secret Tap 方式と同程度あり，Secret Tap 方式の良さを維持していると考える.

また，入力回数を 10 進数 PIN4 桁相当になるように設定した場合，Secret Tap 方式よりも Secret Flick 方式の方が使い易いと 16 人中 13 人が回答した．この結果から，Secret Flick 方式は記憶負荷が増加するが，入力回数を減らすことでユーザビリティが向上しているといえる.

6 まとめ

本論文では，従来の認証方式の 2 つの問題点をそれぞれ解決する 2 つの提案手法を提案した．1 つは，覗き見耐性を持つ従来の認証方式の安全性を確保しつつ，入力回数を減らすことでユーザビリティを考慮した Secret Flick 方式であり，もう 1 つは，従来の認証方式に新たな機能を追加し，2 回以上の録画攻撃耐性を実現した Secret Vibe 方式である．それぞれの提案手法を Android に実装し，それを用いて評価実験，アンケート調査を行った．Secret Flick 方式に関して，評価実験により，実現可能な入力回数において安全性を確保していることがわかった．さらに，Secret Flick 方式の記憶負荷を軽減する拡張 Secret Flick 方式を考案した．この方式は，認証情報を減らすことで記憶負荷を軽減することが分かった．Secret Vibe 方式に関して，従来の認証方式と比較し認証情報が増えるため，ユーザビリティが低下する．しかし，従来の認証方式よりも安心と感じる被験者が多く，複数回の録画攻撃耐性をもつ認証方式として実用的なユーザビリティを備えていることが分かった.

今後は，複数回の録画攻撃耐性を備え，偶然に認証を突破される安全性も考慮した高いユーザビリティを有する認証方式の考案をしていきたい.

参考文献

[1] Google，Android-open source project，http://sourve.android.com/

[2] 菅井文郎，油田健太郎，山場久昭，朴美娘，岡崎直宣，“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の提案”，マルチメディア，分散，協調とモバイル (DICOMO2012) シンポジウム，pp.2402-2409(2012).

[3] L.Sobrad，J.Birget，J.C，Graphical passwords. The Rutgers Scholar，4,(Sept. 2002).http://RutgersScholar.rutgers.edu/volume04/sobrbirg/sobrbirg.htm.

[4] Brostoff,S., Sasse,M.A.,“ Are Passfaces more usable than passwords? A Field Trial Investigation”，People and ComputersXIV-Usability or Else，Proc.of HCI2000，Springer，2000，pp.405-424.

[5] D.Davis,F.Monrose,and M.K.Reiter,“ On user choice in graphical password schemes”.in Proceedings of the 13th Usenix Security Symposium San Diego，CA，2004.

[6] 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(Sep.2008).

[7] H.Gao，Z.Ren，X.Liu，U.Aickelin，“ A new graphical password scheme resistant to shoulder-surfing”,Proceedings - 2010 International Conference on Cyberworlds, CW 2010, pp.192-199

[8] 桜井鐘治, 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).

[9] NIST Special Publication 800-63 Version 1.0.2 Electronic Authentication Guideline, National Institute of Standards and Technology，(2006)，(訳)SP800-63 電子認証に関するガイドライン，独立行政法人情報処理推進機構，(2007).