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耐性とユーザビリティに関する検討

和斉 薫[1] 菅井 文郎[1] 喜多 義弘[2] 朴 美娘[2] 岡崎 直宣[3]

概要：モバイル端末内の情報の漏えいを防ぐため，画面ロック及び画面ロック解除認証が広く利用されているが，覗き見攻撃に対する耐性と高いユーザビリティを同時に実現している認証方式は実用化されていない．以前提案された Secret Tap 方式は，アイコンと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．この方式は高い覗き見攻撃に対するを備えているが，2 つの問題が存在する．1 つ目は，偶然に認証を突破される確率を十分な強度にするためには，一連の認証において，入力回数を多くする必要があり，ユーザビリティが低下する問題である．2 つ目は，複数回の録画攻撃に対する耐性が実現できていない問題である．本研究では，入力方法のバリエーションを増やして，偶然に認証を突破される確率を下げることにより，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方法と，バイブレーション機能によりユーザにしか伝わらない認証情報を用いることで複数回の録画攻撃に対する耐性を実現する方法の 2 つのアプローチから，Secret Tap 方式の 2 つの問題をそれぞれ改善する 2 つの拡張方式を提案する．

An Examination of Usability and Shoulder-surfing Resistance about Icon-based User Authentication Method for Mobile Terminals.

Kaoru Wasai[1] Fumio Sugai[1] Yosihiro Kita[2] Mirang Park[2] Naonobu Okazaki[3]

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，損害につながる情報の流出を防ぐため，画面の操作ロック及び PIN(Personal Identification Number) 等の個人認証方式を利用した画面ロック解除の認証が必要になる．しかし，既存の多くの認証方式では，人の目にさらされた環境で画面ロック解除の認証を行うと，第三者に認証情報が露呈する可能性が高く問題がある．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，モバイル端末を対象とした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認証方式が必要である．

高いユーザビリティを備える認証方式に画像パスワード認証方式がある．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 [1]．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 [2] 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 [3] 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 [4] や CDS [5]，背景配列の移動

[1] 宮崎大学大学院工学研究科
Uniersity of Miyazaki
[2] 神奈川工科大学
Kanagawa Institute of Technology
[3] 宮崎大学工学部
Uniersity of Miyazaki

量を用いた認証方式 [6] がある．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考えられているため，ユーザビリティが低い．そのため，モバイル端末には不向きである．

Secret Tap 方式 [7] 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，覗き見耐性を備えた認証方式である．しかし，この方式には 2 つの問題が存在する．1 つは，偶然に認証を突破される確率を十分低くするためには，一連の認証におけるタップ入力の回数を多くする必要があり，入力回数を多くすると，ユーザビリティが低下してしまう問題である．もう 1 つは，覗き見耐性と 1 回の録画耐性は実現しているが、複数回の録画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 つの問題をそれぞれ改善する 2 つの拡張方式を提案する．1 つ目の問題に対し，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 方式にバイブレーション機能を用いて拡張した認証方式 Secret Vibe 方式を提案する．この方式は，バイブレーション機能を用いて振動パターンを導入することで，認証中の認証情報の変化量をユーザのみに伝えることが可能になる．この機能を利用し，複数回の録画耐性の実現を目指す．さらに，2 つの提案手法に関して評価，考察を行う．

2. 考慮すべき項目

2.1 画面ロック

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．そのため，攻撃者に認証操作を見られても認証情報が露呈することがない覗き見耐性を持つ認証方式が必要である．人は記憶力，処理能力において限界がある．そのため，ある程度認証方式を複雑にすると攻撃者は認証操作をすべて記憶することが困難になり，覗き見耐性を持たせることができる．

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記録し，コンピュータで解析する攻撃方法である．そのため，記憶能力と処理能力の限界がない．したがって，録画耐性を持たせることは，覗き見耐性を持たせることよりもより複雑な認証方式が必要になる．さらに，複数回の録画耐性を持たせる場合，単に認証方式を複雑にするだけではなく，録画された情報から認証情報が特定されないように，冗長な情報により隠蔽することが必要になる．そのため，認証操作が複雑になり，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 Android Password Pattern [8]

Android Password Pattern は，Google が開発し Android OS で標準の画面ロック解除の認証方式として採用されている．この方式は，事前に認証情報となる 4 節点以上のパターンを登録し，認証画面で登録したパターンを指でなぞることで認証を行う．画面に表示された節点をなぞるだけで認証を行うことが可能であるため，高いユーザビリティを持つ認証方式である．しかし，認証操作を覗き見られたり，録画されてしまうと簡単に認証情報が露呈してしまう．また，タッチパネル特有の画面になぞった跡が残り，認証情報が露呈する問題点もある．

3.2 Convex Hull Click Scheme(CHC)[9]

CHC は，チャレンジ・レスポンス型の画像パスワード認証方式である．事前にユーザは複数のパスアイコンを登録する．認証画面には複数のパスアイコンを含むアイコンがランダムに配置され，表示される複数のパスアイコンで形作られる凸包形内のアイコンを選択することで認証を行う．この方式は，直接パスアイコンを選択せずに認証を行

うことにより覗き見耐性を実現している．しかし，モバイル端末のような小さい画面の場合，表示されるアイコンの数が少なくなる．ゆえに，表示される凸包形内のアイコンの数が少なくなるため，攻撃者にパスアイコンの推測を容易にしてしまう．また，認証中ユーザは，毎回複数のパスアイコンを探す必要があり，ユーザビリティが低下してしまう．よって，この方式は高いユーザビリティが必要であるモバイル端末には不向きである．

3.3 Secret Tap 方式 [7]

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．事前にユーザは複数のアイコン（登録アイコン）を認証情報として登録する．認証時に表示される複数のアイコンの中から登録アイコンを手掛かりにタップ入力を行うことで認証を行う．この方式は，認証操作が簡単であり，高いユーザビリティを有している．

この方式の認証画面を図 1 に示す．事前に認証情報として，登録アイコン，シフト量を設定する．認証画面には 4 × 4 マスにアイコンがランダムで表示される．表示される 16 個のアイコンの内，必ず 1 個は登録アイコンを含み，残りのアイコンはダミーのアイコンである．認証画面を 2 × 2 ずつ 4 つに分け，それぞれを第 1 象限から第 4 象限とし，象限内の任意のアイコンをタップ入力する．いずれかのアイコンをタップ入力すると，再び別の複数のアイコンがランダムで表示される．この操作を事前に設定された入力回数繰り返し，すべて正しいアイコンを選択していた場合，認証成功となる．

この方式では，認証方式に覗き見耐性を持たせる工夫として，シフト量という値を定めている．シフト量とは，認証時に登録アイコンが表示されている象限から，反時計回りにどれだけシフトした象限内のアイコンをタップ入力して認証を行うかを決める値である．

図 1 はシフト量+1，登録アイコンは第 3 象限に表示されている．この場合，ユーザは登録アイコンが表示されている象限から反時計回りに 1 つシフトした第 4 象限のいずれかのアイコンをタップ入力する．シフト量を認証情報として設定することにより，どの象限に登録アイコンが表示されているかを隠蔽することが可能となり，覗き見耐性を向上させている．さらに，設定した登録アイコンが表示されている象限を入力する事を回避することで，登録アイコンの直接タップ入力を防ぐことが可能である．また，この方式では登録アイコンの出現確率を一連の認証操作を通して均一になるようにしている．これは，認証中に同じ登録アイコンが何度も出現することにより攻撃者に推測されやすくなることを防ぐ目的がある．入力回数よりも登録アイコンの数が多い場合，十分な数のアイコンを用意する事ができれば，1 回の録画耐性について十分な強度を確保することが可能である．

しかし，Secret Tap 方式には 2 つの問題が存在する．

1 つは，偶然に認証を突破される確率を十分安全な値にすると，多くの入力回数が必要になり，ユーザビリティが低下してしまう問題である．1 回の入力においての入力パターンは 4 通りであるため，攻撃者により偶然に認証を突破される確率は 1/4 である．10 進数の PIN 数字 4 桁相当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，覗き見耐性が下がることが考えられる．

もう 1 つは，1 回の録画耐性を持つが，複数回の録画耐性を持たない問題である．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 回以上の録画耐性を十分に実現していないことが分かる．

この方式には 2 つのトレードオフが存在する．1 つは，覗き見攻撃に対する耐性とユーザビリティの間のトレードオフである（トレードオフ 1）．覗き見耐性，録画耐性を持たせるには，認証情報が露呈しないように認証方式を複雑にする必要がある．そのため，認証方式のユーザビリティが低下してしまう．逆に，高いユーザビリティを持たせた認証方式は認証操作が簡単になってしまうため，攻撃者は認証情報の推測が容易になり，覗き見耐性が低下してしまう．

もう 1 つは，録画耐性と 1 回の入力における偶然に認証を突破される確率の間のトレードオフである（トレードオフ 2）．Secret Tap 方式では，表示されるアイコンの数は 16 個であり，これを 4 つの象限のグループに分けている．録画耐性はユーザの 1 回の入力において攻撃者に推測される登録アイコンの候補の数が多いほど高くなる．したがって，録画耐性はグループ内のアイコンの数に依存し，録画耐性を上げるためには，グループ内のアイコンの数を増やす必要がある．しかし，グループ内のアイコンを増やすとグループの数が減ってしまう．また，偶然に認証を突破される確率を低くするには，入力パターンの総当たり数を増やす必要がある．したがって，偶然に認証を突破される確

率は，グループの数に依存し，低くするためには，グループの数を増やす必要がある．しかし，グループの数を増やすとグループ内のアイコンの数が減ってしまう．

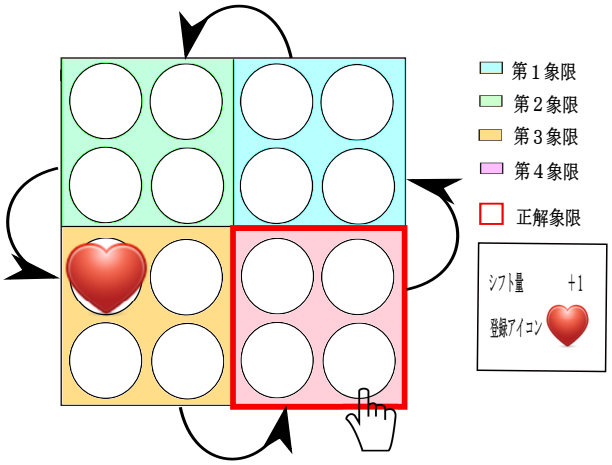

図 1 Secret Tap 方式の認証画面 [7]
Fig. 1 Authentication screen of Secret Tap [7].

4. 提案手法

既存手法には覗き見耐性を持つ認証方式が存在するが，モバイル端末を対象とし，高いユーザビリティを有した認証方式は少ない．Secret Tap 方式は，画面のアイコンをタップするという簡単な操作で高いユーザビリティを有し，覗き見耐性をも持つ認証方式を実現している．さらに，モバイル端末の小さい画面でも使用可能である．しかし，この方式は前述した 2 つの問題がある．

本研究では，2 つの問題を改善する 2 つの拡張方式を提案する．Secret Tap 方式に新たな機能を追加することで 2 つの問題に対しそれぞれ認証方式を提案する．

まず，1 つ目の問題である Secret Tap 方式の偶然に認証を突破される確率を 10 進数 PIN4 桁に同等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 回の偶然に認証を突破される確率が高く，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が増やし，入力 1 回の偶然に認証を突破される確率を低くする．このことにより，10 進数 4 桁 PIN の強度にするための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 Secret Flick 方式を提案する．

2 つ目の問題である Secret Tap 方式が 2 回以上の録画耐性を実現できていない原因は一連の認証において認証情報が変わらず，攻撃者は認証情報を仮定できてしまうためと考える．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ることで，複数回の録画耐性を実現する認証方式 Secret Vibe 方式を提案する．

4.1 Secret Flick 方式

Secret Flick 方式を考案するにあたり設計方針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
1 回の録画攻撃に対して耐性を持つこと．

(3) 偶然に認証に成功する確率
10 進数の PIN4 桁に相当する強度を持つこと．これは，現在広く普及している ATM において 10 進数の PIN4 桁が利用されていることを考慮した．なお，brute-force 攻撃に対しては認証の試行回数に制限を設けるなどの方式を併用することで対策が可能なためここでは特に考慮しない．

(4) ユーザビリティ
覗き見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．提案手法において，ユーザに負担がかからないと想定する入力回数を PIN4 桁の入力回数である 4 回程度と仮定する．この入力回数で十分な認証強度を実現することを目標とした．また，モバイル端末は操作を片手で行うことが多く，認証は両手よりも片手で行えた方がユーザビリティが向上すると考え，認証動作を片手だけで行えることを目標とした．提案方式はアイコンを用いるが，スマートフォンの約 4.0 インチの大きさのタッチパネル液晶でも快適に認証を行えることを目標とした．

事前に認証情報となる複数の登録アイコン，シフト量，登録アイコンごとに入力方法を設定しておく．Secret Flick 方式の認証画面を図 2 に示す．ここで，登録アイコンが表示されている事象から設定したシフト量分だけ反時計回りにシフトした事象を正解事象と呼ぶ．Secret Flick 方式では，表示されている登録アイコンに設定した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．この操作を設定した入力回数繰り返し，すべて正確に入力できた場合に認証成功となる．図 2 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．同図の例の場合，登録アイコンが第 3 象限にあり，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，登録アイコンに設定した右向きのフリック入力をすることで 1 回の正確な入力が完了する．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も許すことで入力バリエーションを 5 倍に増やすことができる．このように，入力のバリエーションを増やすことにより，1 回の入力の偶然に認証を突破される確率を

Secret Tap 方式の 1/4 から 1/20 まで下げることが可能である．さらに，10 進数 PIN4 桁以上の強度にする場合，必要となる入力回数を 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．

3.3 節で述べたトレードオフ 2 に関して，Secret Tap 方式において偶然に認証を突破される確率を下げるには，入力ができるグループ（象限）を増やす必要がある．これは，1 回の入力での選択肢を増やすためである．しかし，表示されるアイコンの数が固定であるのでグループの数を増やすとグループ内のアイコンの数が減少する．そのため，1 回の入力で攻撃者に推測されてしまう登録アイコンの候補の数が少なくなってしまい，攻撃者に登録アイコンの特定がされやすくなる．Secret Flick 方式では，入力のバリエーションを増やすことで偶然に認証を突破される確率を下げている．そのため、グループ内のアイコンの数やグループの数に影響がない．したがって，Secret Flick 方式はトレードオフ 2 に悪い影響は与えない．

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，認証の最初の入力でシフト量を設定する．記憶する認証情報を減らすことでユーザの記憶負荷の軽減を図る．この方式では，認証の最初に入力したアイコンの象限が登録アイコンが表示されている象限からどの程度シフトしているかでシフト量を定める．ここで，アイコンへの入力方法は，表示されている登録アイコンに対応づけている入力方法で行う．その後，そのシフト量で入力回数繰り返し認証を行う．認証例を図 2 で説明する．同図の例は，登録アイコンが第 4 象限に表示されており，この登録アイコンの入力方法は右方向のフリックに設定されている．また，シフト量は事前に設定されていない．認証の最初の入力でどの象限内のアイコンを入力するかでこの後の一連の認証のシフト量が変わる．また，設定されている右フリックで入力しなければ認証は失敗となる．第 1 象限を入力した場合，第 4 象限から 1 つシフトした象限であるため，この一連の認証の間シフト量は+1 となる．同様に第 2 象限はシフト量＋ 2，第 3 象限はシフト量+3，第 4 象限はシフト量+0 となる．

この方式は認証の最初の入力においてどの象限でも入力を許すため初回の偶然に認証を突破される確率が Secret Flick 方式の 1/20 から 1/5 に上がってしまう．しかし，目標の PIN 数字 4 桁相当の強度を得るためには Secret Flick 方式と同じ回数である 4 回で十分である．

4.2 Secret Vibe 方式

Secret Vibe 方式を考案するにあたり設計方針を以下の

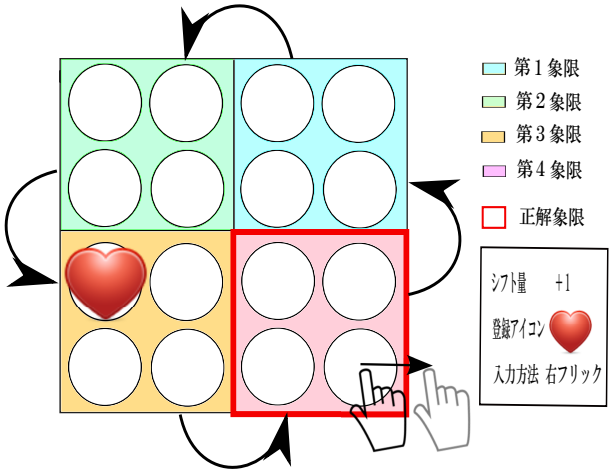

図 2 Secret Flick 方式の認証画面
Fig. 2 Schematic diagram of the authentication screen of Secret Flick.

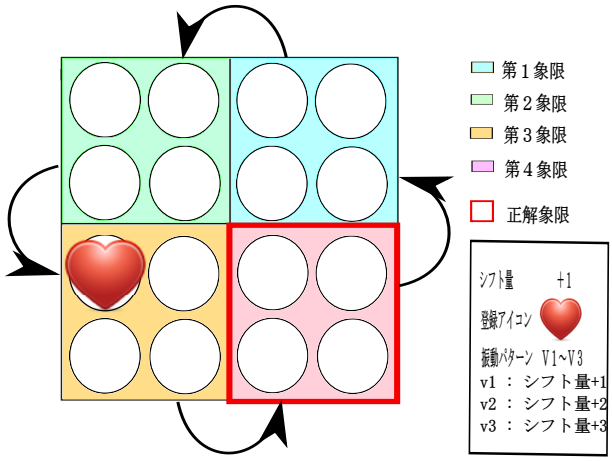

図 3 Secret Vibe 方式の認証画面
Fig. 3 Authentication screen of Secret Vibe.

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．

(4) ユーザビリティ
複数回の録画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．

事前に認証情報として複数の登録アイコン，シフト量，バイブレーションの振動パターンごとに対応付けたシフト量の変化値を設定しておく．Secret Vibe 方式の認証画面を図 3 に示す．この認証画面が表示され，タップ操作を受け付けている状態の時，無振動を含む 4 種類の振動パターンの内ランダムに選ばれた 1 種類が振動する．ユーザは振動パターンを感じ取り，その振動パターンに対応するシフト量の変化値（+0 から+3）を記憶する．ユーザは正解象限から振動パターンに対応するシフト量の変化値だけ反時

計回りにシフトした象限内のいずれかのアイコンをタップ入力をする．この操作を設定した入力回数繰り返し，すべて正確に入力できた場合に認証成功となる．図 3 で Secret Vibe 方式の認証例を説明する．シフト量が+1，登録アイコンは第 3 象限に表示されているので正解象限は第 4 象限となる．ユーザがこの時振動パターン V1 を感じ取った場合，V1 に対応づけられた変化値は+1 であるので正解象限から反時計回りに 1 つシフトした第 1 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．バイブレーションでの振動は，ビデオカメラにも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での記録は不可能と考えられる．そのため，シフト量を仮定し，入力毎に登録アイコンの候補を仮定する攻撃方法では登録アイコンを特定できない．

5. 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 4 に示す．この認証画面において Secret Vibe 方式ではバイブレーション機能により無振動を含む振動パターンが振動し続け，振動パターンをもとに振動しシフト量を変化させてタップ入力する．Secret Flick 方式では，この画面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がダイアログに表示される．このダイアログには実際に認証にかかった時間も表示されるように実装した．

アプリケーションに実装した各提案手法の認証画面を図 5 に示す．同図上の表示されるリストのアイコンをタップすると認証情報となる登録アイコンとして設定される．登録アイコンとして設定されたアイコンは 1 のエリアにアイコン一覧として表示される．2 のエリアでは，認証の入力回数が設定でき，3 のエリアでシフト量の値を設定を行う．4 のエリアで Secret Flick 方式と Secret Tap 方式の切り替えを行う．登録アイコンごとの入力方法はエリア 2 に表示されているアイコンをロングタップすることで入力方法の一覧が表示され，選択することで設定することができる．5 のエリアでは Secret Vibe と Secret Tap 方式の切り替えを行うことができる．OK ボタンを選択することで認証情報の設定が完了する．

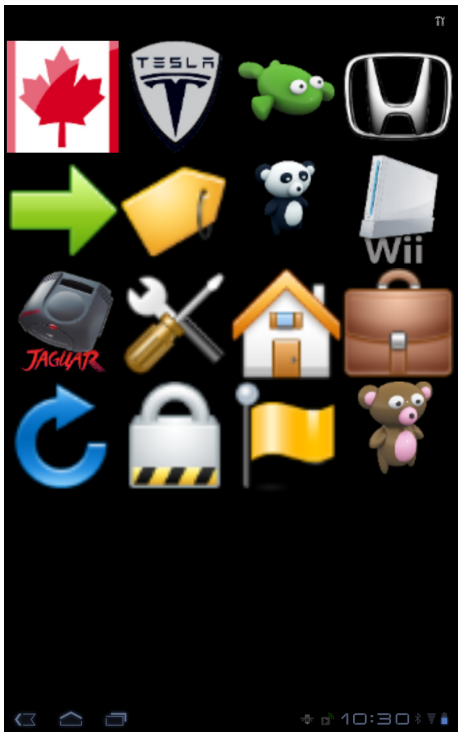

図 4 提案手法の認証画面
Fig. 4 Authentication screen of Proposal method.

図 5 提案手法の登録アイコンの設定画面
Fig. 5 Password icon setting screen of Proposal method.

6. 評価および考察

6.1 偶然に認証を突破される確率

Secret Flick 方式と拡張 Secret Flick 方式，Secret Tap 方式，10 進数 PIN4 桁の偶然に認証を突破される確率を表 1 に示す．同表において，10 進数 4 桁の PIN に相当する強度を各提案手法で実現するときの入力回数を太字で示している．提案手法である Secret Vibe 方式は，1 回の入力においての入力パターンは 4 通りであるため，Secret Tap 方式と同じ値である．偶然に認証を突破される確率は，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 $1/(5 \times 20^{n-1})$ 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，4 桁の 10 進数 PIN に相当する強度を超える．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．また，Secret Flick 方式は，入力回数が 3 回の場合 1/8000 となり，10 進数 PIN に相当する強度に満たないが近い値になる．これは，ユーザがセキュリティの観点から許容できるならば，10 進数 PIN4 桁の入力回数よりも 1 回少なく認証を行うことが可能である．入力回数が 4 回の場合 1/160000 となり，4 桁の 10 進数 PIN と同じ入力回数で 4 桁の 10 進数 PIN に相当する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，偶然に認証を突破される確率は上がるが入力回数は 4 回で目標の強度に相当する．

表 1 既存手法と提案手法の偶然認証に成功する確率の比較
Table 1 Comparison of proposed methods and existing methods for the probability of success by accident.

	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**	$1/10^5$
	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	$1/10^6$	$1/10^7$	$1/10^n$

6.2 覗き見耐性

Secret Flick 方式，拡張 Secret Flick 方式，Secret Vibe 方式が実際に覗き見耐性を実現しているかを評価するために評価実験を行った．評価実験では，各提案手法を Android 上に実装したアプリケーションを用いた．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 10 人である．評価実験では，まず，2 つの提案手法の要点を十分説明し，その後，実際に被験者に Android に実装した各提案手法を操作してもらった．被験者に 2 つの提案手法を十分理解してもらった上で，被験者の目の前で 10 回の認証をゆっくり行い，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し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．覗き見攻撃は，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成功とした．また，ユーザビリティの観点から評価実験のパラメータは入力回数が 4 回，登録アイコンの数が 4 個に設定した．なお，実験に用いたパラメータは被験者には事前に教えていない．

評価実験の結果，Secret Flick 方式，拡張 Secret Flick 方式，Secret Vibe 方式について，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，入力方法がどのアイコンに対応付けられているかは推定できていないが，被験者にどんな入力方法が設定されているかが推定されてしまっていた．さらに，Secret Vibe 方式では，機器によってはバイブレーションの音が大きいものも存在し，振動パターンが推定されてしまう場合がある．

6.3 複数回の録画耐性

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によりランダムにシフト量を変化させる．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攻撃方法ではアイコンを特定することはできない．このことから，提案手法は Secret Tap 方式と比べ，複数回の録画耐性に対する耐性が向上していると考えられる．

6.4 ユーザビリティ

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を行った．被験者は上記と同じである．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う形式で行った．提案手法についてと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 (桁数) を答えてもらった．偶然に認証を突破される確率に関しての項目は，被験者が回答した許容回数における確率において安心かどうかを答えてもらった．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．同表の偶然認証とは偶然に認証を突破される確率を示す．また，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 と図 6 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．

アンケート結果より，Secret Flick 方式と拡張 Secret Flick 方式は，許容回数における「偶然認証の安心さ」の項目で Secret Tap 方式を大きく上回った．また，被験者の入力の許容回数は，どの認証方式でも約 4 回であった．Secret Flick 方式と拡張 Secret Flick 方式はこの入力回数において偶然に認証を突破される確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

Table 2　Measurment items and scores on the impression of each method.

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
偶然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

Table 3　Results of the questionnaire using semantic differential method.

	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	(偶然認証) 安心さ	使いたいと思うか	許容回数
Secret Tap	4.7(0.4)	4.7(0.5)	4.2(0.9)	4.5(0.8)	3.0(1.2)	4.4(0.7)	4.5(0.9)
Secret Flick	4.6(0.9)	4.1(0.8)	3.1(0.9)	4.7(0.5)	4.4(0.9)	4.1(1.1)	3.6(0.4)
拡張 Secret Flick	4.7(0.5)	4.5(0.7)	3.5(0.7)	4.7(0.5)	4.8(0.4)	4.4(0.7)	4.1(0.9)
Secret Vibe 方式	4.7(0.4)	4.5(0.5)	3.8(0.9)	4.8(0.4)	3.3(0.8)	4.2(0.8)	4.1(1.0)

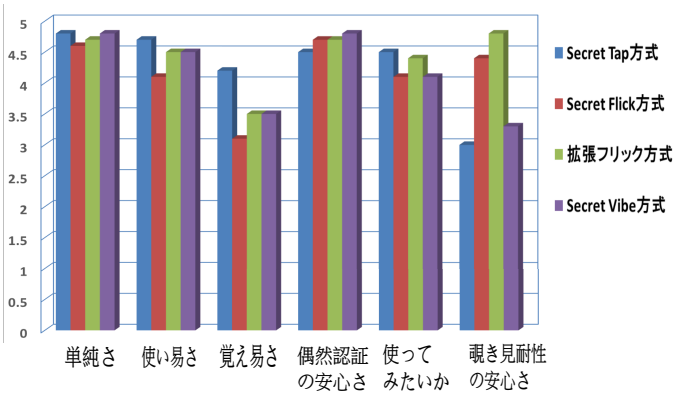

図 6　SD 法を用いたアンケートの結果

Fig. 6　Result of questionnaire using semantic differential method.

S 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．拡張 Secret Flick 方式は，Secret Flick 方式よりも「覚えやすさ」の項目の値が高く，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．「単純さ」,「覗き見の安心さ」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 10 人中 8 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．

7.　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アンケート被験者が多く，複数回の録画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] L.Sobrad, J.Birget, J.C, Graphical passwords. The Rutgers Scholar, 4,(Sept. 2002).http://RutgersScholar.rutgers.edu/volume04/sobrbirg/sobrbirg.htm.

[2] 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.

[3] 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.

[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(Sep.2008).

[5] 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

[6] 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).

[7] 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).

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

[9] S.Wiedenbeck, J.Waters, L.Sobrado, and J.Birget, “Design and Evaluation of a Shoulder-Surfing Resistant Graphical Password Scheme”, in International Working Conference on Advanced Visual Interfaces 2006, pp177-184(2006).