Vol.2014-MBL-73 No.23
Vol.2014-ITS-59 No.23
2014/11/21

安全性強度を柔軟に設定できるモバイル端末向け個人認証方式の一検討

和斉 薫[1]　宗 裕文[1]　山場 久昭[1]　久保田 真一郎[1]　朴 美娘[2]　岡崎 直宣[1,a)]

概要：近年，スマートフォン等のモバイル端末の普及に伴い，そこに格納される情報の漏洩をどう防止するのかが重要な課題になってきている．現在，画面ロックとその解除認証が使用されているが，録画攻撃耐性や覗き見耐性を備えつつ，高いユーザビリティも実現している認証方式はない．一般に，安全性とユーザビリティの間にはトレードオフの関係があり，双方を単一の認証方式で同時に満足させることは困難である．この問題を解決するアプローチとして，モバイル端末を使用する環境やそこに格納されている情報の重要度に応じて，認証方式に要求されるセキュリティ要件が変化することに着目し，ユーザビリティを重視すべき場面では高いユーザビリティを持つ認証方式に，安全性を重視すべき場面では高いセキュリティを実現できる認証方式に，場面に応じた認証方式を切り換えるという対応策が考えられる．本稿では，以前に我々が提案した認証方式である Secret Tap 方式及びそのいくつかの拡張方式を組み合わせることにより，異なるセキュリティ要件が求められる複数の局面に適用可能な統合的認証方式を提案する．また，ここで採用した局面ごとの認証方式について，その対応する場面に求められるセキュリティ要件とユーザビリティを満たしていることを，Java で実装した実験システムを利用した実験とその被験者へのアンケートにより確認する．

1. はじめに

近年，個人が所有するモバイル端末を業務で使用する BYOD(Bring Your Own Device) の普及が進んでいることもあり [1]，モバイル端末の中に個人情報だけでなく，業務上秘密にしなければならない重要な情報が格納されたり，端末を通じてこのような情報にアクセスできるようになりつつあり，これらの情報の漏洩を防ぐことが強く求められるようになってきている．そのためモバイル端末では，通常，その操作を始める前に個人認証を行わなければならないように設定する．

モバイル端末は，パソコンなどに比べ場所を選ばずに使用できるのが利点であるが，そのためにそのロック画面の解除認証が，人の目や録画機器に晒された環境で行われることが多い．その際に，他者が覗き見によってパスワードなどの認証情報を容易に得てしまうこと（以下，覗き見攻撃）や，ビデオカメラなどの録画機器により認証操作を録画されてしまい，その動画像の解析から認証情報を得られてしまうこと（以下，録画攻撃）にさらされ易い．しかし，現在使用されている多くの個人認証方式は，これらの攻撃によるパスワードの剽窃への対策が不十分である．

その一方で，モバイル端末の個人認証方式には，解除認証の手間がかからないこと（以下，ユーザビリティ）への配慮も重要である．

ここで，覗き見耐性と録画攻撃耐性を含む安全性とユーザビリティの間には，トレードオフの関係がある．認証操作を複雑にすると覗き見攻撃への耐性は強くなるが，ユーザビリティは低くなってしまう．

そのどちらを優先するべきであるのかはモバイル端末を使用する環境や端末に格納されている情報の重要度に応じて異なる．例えば，モバイル端末に企業の業務情報が格納されていたり，録画攻撃が行われることが懸念される混雑した建物内で解除認証を行う場合は，認証情報が露呈しないような高いセキュリティが要求され，ユーザビリティが低くなることは諦めなければならない．逆に，自室に 1 人しかいない状況で解除認証を行う場面では，覗き見攻撃や録画攻撃が起こる可能性が低く，ユーザビリティが高いことを優先することができる．

そこで，本研究では，以前に我々が提案した認証方式である Secret Tap 方式 [2] とそのいくつかの拡張方式 [3]〜[5] を組み合わせることにより，異なるセキュリティ要件が求められる複数の場面に適用可能な統合的認証方式を提案す

[1] 宮崎大学
University of Miyazaki
[2] 神奈川工科大学
Kanagawa Institute of Technology
[a)] oka@cs.miyazaki-u.ac.jp

る．まず，求められるセキュリティ要件の厳しさと望ましいユーザビリティの程度により，種々の場面に応じて求められるセキュリティレベルを整理した．その上で，それぞれのセキュリティレベルに対して適切な認証方式を Secret Tap 方式といくつかの拡張方式から選定した．この統合的認証方式の下では，いずれの認証方式が選択されていても，同一の認証情報（具体的には，各ユーザが認証のために選択したアイコンの組）が利用できる．すなわちユーザは，各認証方式毎に異なる認証操作を同一の認証情報を用いて行うことができ，その実現にはタッチパネル液晶などモバイル端末の機能が活用されている．

以下，本論文では，2 章で研究の背景と関連研究について述べ，3 章で提案手法の仕組みと認証方法について説明する．4 章で提案手法についてセキュリティとユーザビリティの評価および考察を行い，5 章で本論文をまとめる．

2. 研究背景

本節では，まずモバイル端末での個人認証の特徴として，画面ロック解除操作が頻繁に行われること，その操作が他者の目に触れ易い場所で行われうること，その操作を行うにあたりタッチパネル液晶等の技術が活用されていることを述べる．次に，モバイル端末での覗き見攻撃に対する耐性，録画攻撃に対する耐性について，既存研究の紹介とともに説明する．

2.1 モバイル端末での個人認証

現在の多くのモバイル端末には，端末を紛失したり，盗難にあった場合などに，端末内の情報の漏洩や改竄を防ぐために，画面をロックし操作できなくなる機能が搭載されている．これは，予め設定した時間内にマウスやキーボードなどからの入力がなかった場合，または，ユーザが明示的に指示した場合に，端末の操作が可能な状態から操作が不可能な状態にし，再び操作できる様にするためには，パスワードや Personal Identification Number(PIN) などの個人認証を必要とするものである．

モバイル端末の個人認証方式の特徴の一つとして，タッチパネル液晶を利用したものが多いことが挙げられる．タッチパネル液晶を活用した個人認証方式として代表的なものに，Android Password Pattern(以下，APP)[6] がある．APP は，格子状に並んだ節点に対し，認証情報として 4 節点以上を結ぶパターンを予め決めておき，それを指でなぞることで認証を行う．Google が開発し，Android 端末の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．

また，デスクトップ型 PC や銀行の ATM が比較的閉じた空間で使用されるのに対して，モバイル端末は場所を選ばずに使用できるため，ロック解除のための認証操作が他者の目に触れ易いという特徴も挙げられる．デスクトップ型 PC が使用される場所は，ユーザ本人しかいない個室であったり，複数の人間がいるオフィスであっても，自分の背後に他者がいないことを確認した上で認証操作を行うことは，比較的容易である．それに対し，モバイル端末は，まわりに他者が多数いる状況下で，送信されてきたメールやかかってきた電話に即時に対応しようとすれば，覗き見されないような状況を直ちに確保することは容易ではない．APP は，ユーザビリティが高い反面，覗き見攻撃に対する耐性が低く，認証操作を覗き見られると，容易に認証情報（選ばれていた節点とその順序）が漏洩してしまう．

2.2 覗き見による認証情報奪取攻撃

ここでは，覗き見による認証情報奪取攻撃を次の 2 つに分類する．

2.2.1 （目視による）覗き見攻撃

覗き見攻撃とは，ユーザが個人認証を行っているところを他者が覗き見し，その結果として，パスワードなどの認証情報を得てしまうことである．

覗き見攻撃を防ぐための最も簡単な対策は，認証操作を行っているところを他者に見られないようにすることである．しかし，混雑した電車やエレベータの中などで，人の目を避けることが難しい場面も多い．したがって，覗き見攻撃を防ぐためには，認証方式に覗き見攻撃に対する耐性を持たせることが不可欠と言える．

認証方式に覗き見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する．ある程度認証方式を複雑にするとすべての認証情報，認証操作を記憶することが困難になり，その結果，覗き見耐性が実現できるわけである．ただし，認証操作を複雑にしてしまうため，ユーザビリティがある程度低下してしまうことは避けられない．

2.2.2 録画攻撃

録画攻撃は，ビデオカメラなどの録画機器を用いて認証画面と認証操作のすべてまたは一部を記録し，コンピュータを用いて解析する．そのため，実質的に記憶能力と処理能力の限界がなく，認証方式に録画攻撃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難しい．また，この攻撃への耐性を実現するのは，単に認証方式を複雑にするだけでは困難であり，録画された情報から認証情報が特定されないように，冗長な情報により認証情報を隠蔽することが必要になる．そのため，録画攻撃への耐性を持たせようとすると，認証操作がより複雑にせざるをえず，それゆえ，ユーザビリティを低下させてしまう．

2.3 関連研究

キーボードによる文字入力が不得手なモバイル端末において有効なユーザ認証の方向性の一つに，画像を用いて認証を行うものがある．これは，人間の記憶の特徴の 1 つとして，本人にとって意味のある写真や絵などの画像記憶は，

単語や文などの言語記憶と比較して，その記憶容量も大きく，かつ持続時間も長いということを利用しようというものである．[7]

画像を用いた認証方式は，この記憶の特徴を活かすことで認証情報の記憶を容易にしている [8]．また，この種の認証方式の認証操作は，表示される画像やアイコン群の中から事前に認証情報として設定したパス画像を選択するだけで良いため，高いユーザビリティを確保している．具体的な認証方式には，人間の顔の画像を用いる Passfaces [9] や，画像に加え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 [10] がある．しかし，これらの認証方式は，認証を行う際にパス画像を直接指で選択するため，覗き見耐性および録画攻撃耐性が低く，他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．

目視による覗き見耐性を持つ認証方式には，様々な方式がある [11]〜[18]．しかし，これらの認証方式は，比較的大きい画面の PC や ATM での使用を想定しており，モバイル端末で使用しようとすると，画面の大きさや入力方法の違いなどによりユーザビリティが低下してしまうことが懸念される．

録画攻撃耐性を備えた認証方式の 1 つに fakePointer [11] がある．この認証方式は，PIN と背景にあるマークの組み合わせによって認証を行う．永続記憶による固定パスワードとしての PIN とランダムに生成される使い捨てパスワードとしてのマークを併用することで，どちらかの情報が漏洩しても認証情報を特定することを困難にしている．しかし，この認証方式は，認証を行う前に使い捨ての認証情報である背景のマークを事前にモバイル端末を用いて取得する手間が発生する．また，背景のマークを取得しているところを覗き見されると，認証情報の一部を奪われてしまうことになるため，そうならないように配慮することも必要となる．

3. 提案手法

本研究では，モバイル端末を対象として，覗き見攻撃へ耐性を持った認証方式を提案する．ただし既に述べた様に，認証操作のユーザビリティを高く保ちつつ，覗き見攻撃への耐性を実現するのは困難である．そこで本研究では，いくつかの認証方式を組み合わせることにより，それを達成する．

ここで，覗き見攻撃への耐性を持つとは，それぞれ覗き見攻撃により取得した情報では認証情報を特定できないことと定義する．また「(ある認証方式に) n 回の録画攻撃耐性がある」とは，同一モバイル端末の認証操作の録画データが n 回分ある時に，認証情報の候補となるパスアイコンとシフト量の組み合わせの数が，当該の認証方式の確率的誤認証による突破確率の逆数までしか絞り込めないことと定義する．

SecretTap は，十分なユーザビリティを保ったまま，覗き見耐性と 1 回の録画攻撃耐性を備える．しかし，複数回の録画攻撃への耐性は十分ではない．また，入力をランダムに選んだ時に，偶然に認証されてしまう確率が高いという弱点も持つ．以下，本論文では，「認証情報がわからなくとも，入力をランダムに選んだ時に，確率的に誤って認証してしまうこと」を「確率的誤認証」と呼ぶ．

以上を踏まえ，筆者らは，いくつかの改良方式の提案を行っている．しかしながら，その代償として，ユーザビリティの低下，確率的誤認証への耐性が向上した分，他の攻撃への耐性が悪化するなどの副作用が生じてしまっている．

そこで，求められるセキュリティ要件の厳しさにより，種々の場面に応じて求められるセキュリティレベルを整理した．その上で，それぞれのセキュリティレベルに対して適切な認証方式を Secret Tap 方式といくつかの拡張方式から選定した．それらを組み合わせることにより統合的認証方式を構成することとした．

以下では，まず，Secret Tap 方式およびその拡張方式群の概要と，本研究で導入したセキュリティレベルを説明する．その上で，それぞれのレベルに対して適切な認証方式を Secret Tap 方式とその拡張方式の中から選定し，それらを組み合わせた統合的認証方式を提案する．

3.1 Secret Tap 方式 [2]

SecretTap 方式 [2] は，著者らが，タッチパネル液晶を備えたデバイス向けに提案した，チャレンジ・レスポンス型の認証方式である．覗き見耐性を持たせるとともに，認証操作にアイコンを採用したことによりユーザビリティを高めていることがその特徴である．

この認証方式では，利用者が覚えやすいであろうアイコンを予め多数用意しておき，ユーザは事前にその中から n 個を認証情報として選び，登録しておく．これらの登録されたアイコンを，パスアイコンと呼ぶ．認証時には，図 1 に示すような 4 × 4 マスの認証画面が m 面表示されるが，16 個のアイコンの中にパスアイコンが毎回 1 つだけ含まれる．パスアイコン以外のアイコンはダミーアイコンと呼ぶ．ダミーアイコンは，当該のユーザがパスアイコンとして選択しなかったものの中からランダムに選択される．ユーザは，基本的には，表示されているアイコンの中からロック解除のためのアイコン（解除アイコン）を選択してタップする．そして，m 面すべてで解除アイコンを選択できれば，認証成功とみなす．

この方式の特徴は，シフト量と呼ぶ値を導入することにより，パスアイコンでないアイコンを解除アイコンとして指定できる点である．パスアイコンではないアイコンをタップ入力することにより，認証操作を見られても認証情報は取得されない．具体的には，まず，認証画面を 2 × 2 マス毎の第 1 象限から第 4 象限のグループに分ける．その

Vol.2014-MBL-73 No.23
Vol.2014-ITS-59 No.23
2014/11/21

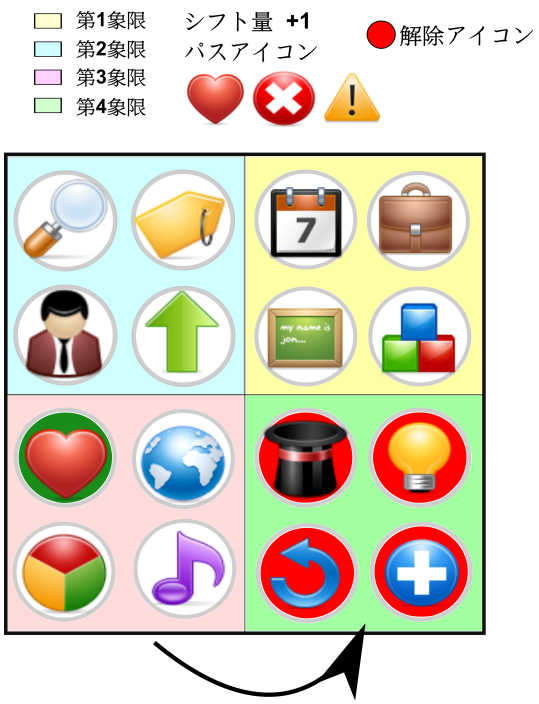

図 1　各認証方式で用いられる認証画面
Fig. 1　Authentication screen of Proposal method.

上で，パス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ずれた象限内の 4 つのアイコン全てを解除アイコンとする．4 つのアイコンのいずれかをタップすれば正解である．

[2] では，実証実験の結果から，SecretTap が覗き見耐性を備えることが示されている．また，この方式は，1 回の録画攻撃耐性を実現している．

ただし，Secret Tap 方式が次の 2 つの弱点を持つことも同時にわかっている．

まず，確率的誤認証がおこり易い．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」[19] では，パスワード及び暗証番号に必要な強度を 2^{-14} としている．（確率的に誤まって認証が成功してしまう確率が $\frac{1}{2^{14}}$ 以下であること．）Secret Tap 方式は，タップする位置を 4 つの象限から選ぶため，1/4 の確率で正解の象限が選ばれてしまう．よって，入力回数を 4 回にした場合，1/256 の確率で認証が成功してしまう．これは，4 桁の PIN の確率的誤認証の確率 1/10000 と比べても遥かに大きい．入力回数を増やせば確率的誤認証に対する耐性を高くすることができるが，逆にユーザビリティは低くなってしまう．

次に，複数回の録画攻撃に対する耐性は十分ではない．複数回分の認証動画があれば，そこからパスアイコンの候補を絞り込むことができてしまう．

筆者らは，この 2 つの弱点に対処する改良手法を提案している．

3.2　確率的誤認証に対する耐性を高めた認証方式

筆者らは，少ない入力回数でも確率的誤認証に対する耐性を高くする目的で，以下 2 つの認証方式，SecretFlick 方式 [5] と SecretTap with Double Shift（以下，STDS）方式 [3] を提案している．これらの方式は，SecretTap 方式を拡張したものであり，SecretTap 方式持つ複数回の覗き見耐性と 1 回の録画攻撃耐性は継承しつつ，入力 1 回の確率的誤認証に対する耐性を高めている．

3.2.1　SecretFlick 方式

SecretTap 方式では，アイコンを選択する際の，画面への触れ方は問われなかった．SecretFlick 方式 [5] は，真上から触れるだけのタップ入力なのか，上下左右に指を払う操作であるフリック入力なのかを区別する．事前に，各パスアイコンに対してアクション（上，下，左，右それぞれの方向へのフリック入力，または，タップ入力のいずれか）を割り当てておき，認証時には，解除アイコンに割り当てられたアクションでその解除アイコンを選択した場合に正解とする．これにより，1 回の入力が持つ意味を増やすことができ，確率的誤認証に対する耐性を高くすることに成功している．具体的には，1 回の入力の選択肢が Secret Tap 方式の 4 通りから 20 通りに増え，入力 1 回の確率的誤認証率は，1/20 となる．

ただし，Secret Tap 方式に比べ，複数回の録画攻撃に対する耐性は低くなる．各回の入力画面に表示されていたアイコンと，その時のアクションとを，複数回の認証動画で比較することにより，パスアイコンが特定し易くなってしまうからである．

3.2.2　STDS 方式

STDS [3] は，SecretTap 方式の象限間のシフト量に加え，新たに象限内でのシフト量を認証情報として用いる．Secret Tap では，パスアイコンを含む象限から反時計回りにシフト量分ずらした象限内のアイコンはすべて解除アイコンであるが，この方式では，解除アイコンを 1 つに限定する．すなわち，象限内のシフト量が 0 の時に，パスアイコンが象限内で左上に位置していれば，シフト量分ずらした象限内の左上のアイコンのみが解除アイコンとなる．すなわち，表示されたアイコン群の中からランダムに 1 つのアイコンを選んだとき，それが解除アイコンである確率は Secret Tap 方式の 1/4 に対して 1/16 となり，確率的誤認証に対する耐性を高めることができる．

その一方で，STDS は Secret Tap 方式に比べ，録画攻撃に対する耐性が低くなる．Secret Tap 方式では，仮にシフト量がわかったとしても，タップされた象限の位置から，パスアイコンを 4 つにまでしか絞り込めないが，STDS の場合，二つのシフト量がともに知られてしまうと，タップされた指の位置から，直ちにパスアイコンが特定されてしまう．1 回の認証つき，入力回数を n 回と設定した場合，Secret Tap 方式では，1 回の認証動画から，パスアイコン

の組の候補の数を 4^{n+1} にまで絞り込むことができる．これに対し，STDS では，入力回数によらず，4^{1+1} にまで絞り込むことができてしまう．

3.3 複数回の録画攻撃耐性を目指した認証方式

複数回の録画攻撃に対して耐性をもつことを目指した SecretTap 方式の拡張方式を以下に示す．これらの認証方式の特徴は，携帯端末が持つバイブレーション機能を活用することにより，ユーザに対して，動画に記録されない形で，認証に必要な情報を伝達していることである．

3.3.1 Secret Vibe 方式

Secret Vibe 方式 [5] は，モバイル端末が持つバイブレーション機能を活用することによって，複数回の録画攻撃耐性を目指した Secret Tap の拡張方式である．

Secret Tap 方式では，シフト量を固定しているため，複数回分の録画データを比較すると，パスアイコンやシフト量などの認証情報が特定されやすくなる．そこで Secret Vibe 方式では，毎回異なるシフト量を使用することにより，録画攻撃のもとであっても，認証情報の剽窃を困難とするよう工夫している．

ユーザは，自分が予め選んでおいたシフト量に対し，モバイル端末がランダムに選んだシフト量を加えた値を実際のシフト量として，Secret Tap 方式と同様の認証操作を行う．端末が選択したシフト量をユーザに伝える手段としては，バイブレーション機能を活用する．振動パターンを感じ取れるのはユーザだけであり，録画データには振動パターンは記録されることは無いので，認証情報の特定は複数回の録画攻撃の下でもより困難になる．

3.3.2 Fake Mode 方式

Fake Mode は，認証時にモバイル端末でバイブレーションが起動した場合に解除アイコンとは異なるアイコンを故意に入力し，攻撃者の混乱を誘う認証方式である．Secret Tap に Fake Mode [4] を組み合わせることにより，録画攻撃耐性や覗き見耐性を向上させることができる．

ただし，解除アイコンをタップすべきか否かの選択を，バイブレーションの有無に応じて正しく行わなければならないため，その分ユーザの注意力を要するという意味で，ユーザビリティはやや低下してしまう．

3.4 セキュリティフェーズ

本研究では，求められるセキュリティ要件に応じて，すなわち，覗き見攻撃や録画攻撃への耐性がどの程度必要とされるかにより，セキュリティレベルを分類する．ただし今回は，複数回の録画攻撃耐性が考慮する必要があるか否かにより，二段階に分けることとした．これは，複数回の録画攻撃耐性が要求されない環境であれば，Secret Tap 方式で対応できるからである．また，Secret Tap 方式のユーザビリティが十分高いことから，覗き見攻撃を考慮しなくとも良いような環境でも，ユーザは Secret Tap 方式を不満なく使用できると考えられたからである．

これら 2 つの段階は，具体的には，次の二つの状況を想定していると考えることができる．

状況 I:勤務先のオフィスビルなどで監視カメラが設置されており，そこで認証操作を繰り返し行うような環境

このような環境では, 複数回の録画攻撃に晒されることを想定する必要がある．また，しばしば，このような環境で用いられるモバイル端末には，業務上の特に秘匿すべき情報が格納されていることからも，高いセキュリティが求められる．

状況 II:上記以外の日常生活全般の環境

このような環境では，監視カメラが存在しないか，存在しても，それらの管理者が別個であり，撮影された動画像の情報が集約されることが無いと期待されることを想定する．

また，Secret Tap 方式は確率的誤認証に弱いことから，別の方式を採用すべき次のような状況を想定する．

状況 III:モバイル端末が他者の手に渡っている環境

このような環境では，紛失や盗難などにより，モバイル端末が他者の手に渡り，偶然に認証を突破することが想定される．そのため，確率的誤認証に対する耐性について高める必要がある．

本研究では，これら 3 つの環境それぞれに対応した 3 つのセキュリティ要件（A1,A2,B）を導入した．以下では，これら 3 つのセキュリティ要件について，想定する環境がいずれであるのか，満たすべきセキュリティ上の耐性，および，ユーザビリティをどの程度確保すべきであるのかについて，説明する（表 1）．

(1)LEVEL A1

このセキュリティレベルは，状況 II のような環境を想定する．必要なセキュリティ要件は，複数回の覗き見耐性と 1 回の録画攻撃耐性をもつことである．

(2)LEVEL A2

このセキュリティレベルは，状況 I のような環境を想定する．必要なセキュリティ要件は，複数回の録画攻撃耐性と複数回の覗き見耐性を持つことである．

(3)LEVEL B

このセキュリティレベルは，状況 III のような環境に想定する．必要なセキュリティ要件は，確率的誤認証に対する耐性が高いことである．ここで，確率的誤認証に対する耐性の目標の強度に関して，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」[19] によるパスワード及び暗証番号に必要な強度 2^{-14} を目指す．

3.4.1 各認証方式の確率的誤認証に対する耐性比較

表は，各認証方式の入力回数が 4 回の時の確率的誤認証に対する耐性をエントロピーで示している．現在使用されている認証方式の目安として同表に PIN が 4 桁の場合の

表 1　セキュリティレベルにおける認証方式の分類
Table 1　Classification of authentication method in security level.

セキュリティレベル	セキュリティ要件	ユーザビリティ	認証方式
LEVEL A1	1 回の録画攻撃耐性 複数回の覗き見耐性	高いユーザビリティ	Secret Tap SecretTap+FakeMode
LEVEL A2	複数回の録画攻撃耐性 複数回の覗き見耐性	ユーザビリティが高いことは問わない	Secret Vibe
LEVEL B	1 回の録画攻撃耐性 複数回の覗き見耐性 確率的誤認証に対する耐性が目標の強度	ユーザの許容回数で目標の強度	Secret Flick，STDS

表 2　各認証方式の入力回数 4 回におけるエントロピーの比較
Table 2　Comparison of proposed methods and existing methods for the entropy.

認証方式	エントロピー (bit)
4 桁 PIN	13.29
Secret Tap(LEVEL1)	8.0
Secret Flick(LEVEL2)	**17.29**
STDS(LEVEL2)	**16.0**
Secret Vibe(LEVEL3)	8.0

エントロピーをも示す．

表 2 より，Secret Flick と STDS は，目標以上のエントロピーをもつことが確認できる．したがって，Secret Flick および STDS は，LEVEL B に対応する認証方式に必要なセキュリティ要件の 1 つである確率的誤認証に対する高い耐性を満たす．

一方，Secret Tap および Secret Vibe はこの目標の強度を達しておらず，LEVEL B に対応する認証方式のセキュリティ要件を満たさない．

3.4.2　攻撃者が同一ユーザの認証操作及び認証操作の複数回の録画データを持つ場合（複数回の録画攻撃耐性）

2 つのアイコンが同じ画面に出現した場合，そのうちの少なくとも一方はパスアイコンではない．これを利用することにより，録画データが十分に多くあれば，パスアイコンの特定も可能となる．しかしながら，たとえパスアイコンが特定されても，シフト量と，シフト量の変化値と振動パターンの対応付けを推測することはできないため，認証情報の候補となるパスアイコンとシフト量の組み合わせの数がその認証方式の確率的誤認証率までしか攻撃者によって推測されない．したがって，Secret Vibe 方式は，LEVEL A2 のセキュリティ要件である複数回の録画攻撃耐性を満たす．

3.5　統合的認証方式

モバイル端末における認証方式に必要である高いユーザビリティを持たせるために，タッチパネル液晶とアイコンを用いた認証方式，Secret Tap [2] とそのいくつかの拡張方式 [3]〜[5] を組み合わせることにより，前述した異なるセキュリティ要件に求められる複数の場面に適用可能な統合的認証方式を提案する．これらの認証方式では，いずれも共通の認証情報（自分が選択した数個のパスアイコンとシフト量）と認証画面を用いる．認証情報であるパスアイコンの数は，ユーザにより変更することができるが，[3] の予備実験により，ユーザが記憶することができるアイコン数の上限は 4，5 個であることがわかっている．そこで，本論文では，すべての認証方式においてパスアイコン数を 4 個に設定したとして議論を行う．

各セキュリティレベルが想定している場面および各セキュリティレベルに対し，どの認証方式が適当であるかを表 1 に示す．今回提案する方式では，このセキュリティレベルに応じて，対応した認証方式にユーザが切り替えるものとする．また，モバイル端末の操作が，設定された時間行われなかった場合は，ユーザがモバイル端末を紛失したとものと見なし，LEVEL B に対応する認証方式へ自動的に移行を行う．

なお，本方式を採用するにあたり，以下を前提とする．

(1) ユーザは，認証操作を行う環境や格納される情報などの条件から必要なセキュリティレベルを判断することができる．
(2) 認証方式に使用される認証情報の設定は，覗き見攻撃や録画攻撃の脅威に晒される可能性が低い場所において行われ，その時点で攻撃者に認証情報が知られることはない．

モバイル端末の盗難や紛失の危険性を考慮すると，常に LEVEL B に適した認証方式を使用しなければならない，しかしそれでは，本来，LEVEL A1 に適した認証方式で十分な場合でも，ユーザビリティの低い手法を採用することになってしまう．そこで，一定時間モバイル端末の操作がなかった場合に，ユーザがモバイル端末を紛失した，あるいは，盗難にあったとみなし，自動的に LEVEL B に対応した認証方式に移行するという方法をとる．LEVEL B に自動移行するまでの時間は，ユーザが選択できるものとする．

表 3　各回の評価実験の環境と評価対象の認証方式
Table 3　Evaluation experiment of the environment and evaluation of authentication method.

評価実験の種類	被験者の人数	被験者の情報	被験者の年齢（最年少から最年長）	対象の認証方式
A	7 人	宮崎大学の学生	21 歳から 25 歳	PIN，APP，SecretTap
B	21 人	神奈川工科大学の学生	20 歳から 26 歳	PIN，APP，SecretTap，STDS
C	68 人	学生以外の一般の方	9 歳から 65 歳	PIN，APP，STDS
D	16 人	宮崎大学の学生	18 歳から 30 歳	SecretTap，SecretFlick，SecretVibe

表 4　各認証方式の印象に関する測定項目と得点
Table 4　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
使いたいと思うか	使いたくない 1 点 ← → 5 点 使いたい

4. 評価および考察

統合的認証方式に採用した各認証方式が，その対応するセキュリティレベルに適したセキュリティ要件を満たし，また十分なユーザビリティを持つことを確認するために，評価およびアンケート調査を行った．本節ではその結果を示す．

4.1 覗き見攻撃耐性に関する評価実験

4.1.1 実装

まず，各認証方式を Android 上で動作するアプリケーションとして実装した．実装はプログラミング言語 Java で行い，統合開発環境 Eclipse と Android SDK を用いた．それぞれの認証方式に従い，必要な認証情報を登録した上で認証操作を行うと，認証の成否の判定結果，および，認証完了までに要した時間が表示される．

4.1.2 目的と方法

評価実験は複数回に分けて実施し，各回で対象とした認証方式は表 3 に示すように，それぞれ異なるものである．評価実験では，被験者が攻撃者の役を担当した．すなわち，4.1.1 で実装したアプリケーションをインストールしたタブレットを実際に担当者が操作して認証するところを見てもらい，認証情報であるパスアイコンとシフト量を推測してもらうという形で行った．被験者がすべてのパスアイコンおよびシフト量を正しく答えられた場合，覗き見攻撃が成功とした．なお，複数回の覗き見攻撃が行われることを想定し，被験者の目の前で各認証方式を 10 回ずつゆっくり認証操作を行った．

実験に先立ち，被験者には各認証方式の概要と覗き見耐性及び録画攻撃耐性について十分に説明を行い，さらに，認証方式を覚えてもらうために実際にアプリケーションの操作も体験してもらって，それらを正しく理解できたことの確認を行った．また，被験者には認証方式において使用される全種類のアイコンが記載された紙を渡し，その紙が手元にある状態で実験を行った．

4.1.3 実験結果

PIN と APP に対する覗き見攻撃実験（評価実験 A，B）では，被験者全員が認証情報を正しく答えることができ，攻撃を成功させることができた．この結果から，現在広く使用されているこの 2 つの認証方式は，覗き見耐性が低いことが再確認できた．

一方，SecretTap（評価実験 A，B），STDS（評価実験 B，C），Secret Flick と Secret Vibe（評価実験 E）に対する覗き見攻撃実験では，どの被験者も認証情報を推測することができなかった．この結果から，これら全ての認証方式が，複数回の覗き見耐性を持っていることが確認できた．

また，評価実験 B では，パスアイコン数を 4，入力回数が 7 回と設定した場合の SecretTap についても，同時に評価実験も行っている．この実験では，2 名の被験者が，1 個以上のパスアイコンの特定に成功した．この結果から，入力回数をパスアイコン数より多く設定してしまうと，覗き見耐性が低下することが示された．

4.2 ユーザビリティに関する評価

各セキュリティレベルに対応する認証方式が，必要とされるユーザビリティを満足するか否かを評価するため，4.1 節の覗き見攻撃耐性に関する評価実験を終えた後で，アンケート調査を実施した．

アンケートでは，(1) 被験者に各認証方式毎の許容できる入力回数と，(2) 主観的な印象度を答えてもらった．印象度の回答には，5 段階の Semantic Differential(SD) 法を用いた．

表 5　SD 法を用いた評価実験 A のアンケート結果
Table 5　Questionnaire results of the evaluation experiment A using semantic differential method.

	理解のしやすさ	使いやすさ	慣れた後の使いやすさ	安心さ	使いたいと思うか
Secret Tap	4.0	4.0	4.4	4.9	4.4
PIN	4.9	4.9	5.0	2.4	3.3
APP	4.7	4.7	4.9	2.1	3.6

表 6　SD 法を用いた評価実験 B のアンケート結果
Table 6　Questionnaire results of the evaluation experiment B using semantic differential method.

	理解のしやすさ	使いやすさ	慣れた後の使いやすさ	安心さ	使いたいと思うか	許容できる入力回数
Secret Tap	4.5	3.6	3.9	4.5	4.5	3.9
STDS	3.9	2.5	3.1	4.7	3.1	3.9

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 4 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 5〜7 に示す．

4.2.1　Secret Tap

ここでは，Secret Tap のユーザビリティをユーザがどのように評価したのか，既存の手法，具体的には PIN や APP と比較する（表 5）．

被験者は，「使いたいと思うか」と「安心と感じたか」については，Secret Tap 方式を，「理解のしやすさ」，「使いやすさ」，「慣れた後使いやすいと思うか」については，PIN および APP に高い得点を付けている．

以上の結果から，PIN と APP は使い易いが，覗き見耐性を持つ SecretTap の方が安全性が高いため，多少ユーザビリティを犠牲にしてでも PIN や APP よりも Secret Tap 方式の方を使用したいと感じたと判断できる．

ユーザが使いたいと言っているということは，ユーザビリティは既存手法には劣るものの，許容範囲であると判断できる．

4.2.2　Secret Flick と STDS

評価実験 B のアンケート結果で SecretTap と STDS のユーザビリティを（表 6），評価実験 D のアンケート結果で SecretTap と SecretFlick のユーザビリティを（表 7），それぞれ比較する．

アンケート結果の「安心と感じたか」の項目についてどちらの認証方式も SecretTap より高い結果であった．これは，確率的誤認証に対する耐性が向上したことにより，多くの被験者が安心に感じたためだと考えられる．

また，被験者が許容する平均入力回数については，SecretFlick，STDS ともに 3.9 回という結果になった．被験者が許容する平均入力回数において Secret Flick と STDS は，目標以上の強度をもつため，ユーザが許容できるユーザビリティを持つといえる．

一方，「理解のしやすさ」「使い易さ」「慣れた後に使いやすいか」の項目で STDS，SecretFlick ともに SecretTap を下回った．これは，確率的誤認証に対する耐性を上げるために，認証操作を複雑にしたことや認証情報を増やしたことが原因だと考えられる．

4.2.3　Secret Vibe

LEVEL A2 では，セキュリティ要件を満たせば，ユーザビリティは高いことを求めないものとした．したがって，Secret Vibe はセキュリティ要件を満たしているため，LEVEL A2 に適した認証方式だということが言える．Secret Vibe がどの程度のユーザビリティを持つのかを示すための参考として，評価実験 D のアンケート結果を表 7 に示す．

5.　まとめ

本論文では，モバイル端末で認証を行う場面に応じてセキュリティ要件が変化することに着目し，セキュリティ要件に応じた認証方式に切り替えることができる認証方式を提案した．提案手法では，認証方式を切り替えることで，ユーザビリティと録画攻撃耐性のトレードオフのバランスを柔軟に変化させることが可能である．また，各認証方式を Android 上に実装し，それを用いて覗き見耐性に関する評価実験およびアンケート調査を行った．この結果から，各認証方式が各場面で必要とされるセキュリティ要件およびユーザビリティの程度を満足していることを示した．今後は，LEVELB に対応する認証方式に移行する時間の長さや認証方式を切り替える操作方法に対する改善策を模索するとともに，統合的認証方式のユーザビリティに関する評価実験を実施する予定である．

表 7 SD 法を用いた評価実験 D のアンケート結果

Table 7 Questionnaire results of the evaluation experiment D using semantic differential method.

	理解のしやすさ	使いやすさ	覚えやすさ	安心さ	使いたいと思うか	許容できる入力回数
Secret Tap	4.6	4.6	4.2	4.2	4.2	5.0
Secret Flick	4.3	3.9	3.1	4.6	4.0	3.9
Secret Vibe	4.2	3.3	3.3	4.6	3.7	4.1

参考文献

[1] Cisco : *BYOD* 世界各国の動き-従業員が引き起こすイノベーションを生かす (online), 入手先 <http://www.cisco.com/web/JP/ibsg/howwethink/pdf/BYOD Horizons-Global.pdf>(参照 2014-10-26)

[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] 喜多義弘, 菅井文郎, 朴美娘, 岡崎直宣: モバイル端末における覗き見耐性を持つ認証方式の提案と実装, コンピュータセキュリティシンポジウム (CSS2012), 2D2-1, pp.1-8(2012).

[4] 喜多義弘, 菅井文郎, 朴美娘, 岡崎直宣, 西村広光, 鳥井秀幸, 岡本剛: STDS 認証方式における録画解析による攻撃への耐性に関する一検討, 第 12 回情報科学技術フォーラム (FIT2013), RL-002, pp.1-8(2013).

[5] 和斉薫，菅井文郎，喜多義弘，久保田真一郎，朴美娘，岡崎直宣: 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，コンピュータセキュリティシンポジウム (CSS2013)，3D1-3, pp.700-707(2013).

[6] Google: Android – open source project, http://source.android.com/

[7] 一般財団法人日本情報経済社会推進協会 (JIPDEC)，: 画像活用型本人認証システム・製品ユーザ向け説明ガイド，一般財団法人日本情報経済社会推進協会 (JIPDEC)(online)，入手先<http://www.jipdec.or.jp/dupc/project/ImageAuthentication/UGuide_ImageAuthentication.pdf>(参照 2014-10-26).

[8] Sobrad, L., Birget，J.C.:Graphical passwords, The Rutgers Scholar(online), available from <http://rutgersscholar.rutgers.edu/volume04/sobrbirg/sobrbirg.htm>(accessed 2014-10-26).

[9] Brostoff, S., Sasse, M.A.: Are Passfaces more usable than passwords? A Field Trial Investigation，In Proceedings of Human Computer Interaction, pp.405-424(2000).

[10] Davis, D., Monrose, F.and Reiter, M.K.: On user choice in graphical password schemes, in Proceedings of the 13th Usenix Security Symposium San Diego(2004).

[11] 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).

[12] 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).

[13] 北林良太, 稲葉宏幸: 複数回の覗き見に耐性を有するパスワード認証方式の提案, 電子情報通信学会技術研究報告, ICSS, 情報通信システムセキュリティ, Vol.109, No.115, pp.21-26(2009).

[14] 山本匠，漁田武雄，西垣正勝：不鮮明化画像を利用した暗示・応答型画像認証方式の提案，情報処理学会論文誌, Vol.50, No.9, pp.2062-2076(2009).

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

[16] Gao, H., Ren, Z.,Liu, X., Aickelin, U.: A new graphical password scheme resistant to shoulder-surfing, Proceedings - 2010 International Conference on Cyberworlds, pp.192-199(2010).

[17] Wazir, Z.K., Mohammed, Y.A., Yang, X.: A Graphical Password Based System for Small Mobile Devices, International Journal of Computer Science Issue, Vol.8, Issue 5, No.2, pp.145-154(2011).

[18] Arash, H.L., Omar, B.Z., Samaneh, F., Rosli, S.: Shoulder Surfing Attack in Graphical Password Authentication, International Journal of Computer Science and Information Security, Vol.6, No.2, pp145-154(2009).

[19] 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).