論　文

覗き見耐性をもつユーザ認証システムの実装と評価*

喜多　義弘† 岡崎　直宣†† 西村　広光† 鳥井　秀幸†
岡本　剛† 朴　美娘†

Implementation and Evaluation of Shoulder-Surfing Attack Resistant Users*

Yoshihiro KITA†, Naonobu OKAZAKI††, Hiromitsu NISHIMURA†, Hideyuki TORII†, Takeshi OKAMOTO†, and Mirang PARK†

あらまし　情報漏洩防止のために画面ロックが多くのモバイル端末に搭載され，その解除認証に暗証番号やパターンなどの認証方式が利用されている．しかし，既存の認証方式では，覗き見や録画に対する耐性がなく，認証情報が他人にばれてしまう危険性がある．そこで本研究では，モバイル端末内の情報が漏洩するのを防ぐために，覗き見耐性をもつユーザ認証システムを実装する．具体的には，端末のユーザのみが知り得る認証情報の間接的な入力法則を採用し，覗き見に対する耐性を有する．また，グラフィカルなアイコンのタップ入力により，高いユーザビリティを目指す．

キーワード　覗き見攻撃，画像認証，Android アプリケーション，モバイル端末

1. まえがき

近年，スマートフォンなどのモバイル端末が急速に普及し，BYOD（Bring Your Own Device）によるビジネス体系が確立され，多くの人が個人情報や社内情報が入ったモバイル端末をもち歩くようになった [1]．そのため，モバイル端末の置き忘れや紛失などの場合に，他人にモバイル端末を操作されて内部の情報が漏れないように，多くのモバイル端末には画面ロックの機能が備わっている．画面ロックとは，端末起動時や無操作時，または，ユーザの任意によって端末の操作ができない状態にする機能であり，画面ロックの状態から再び端末の操作ができる状態にするためには，本人認証が必要になる．画面ロックに利用されている既存の認証方式には，暗証番号（Personal Identification Number: PIN），Android Password Pattern（以下，Android PP），顔認証などがある．しかし，PIN や Android PP には覗き見耐性がないため，他人から認証動作を覗き見られた際，容易に認証情報が漏洩する [2]．顔認証は覗き見耐性を有しているが，利用するには専用のカメラを搭載している必要があるため，端末によっては利用できないことがある．また，生体認証特有の本人拒否率及び他人受入率を考慮せねばならず，実用化における利便性や安全性に課題がある [3]．

一方，監視カメラの普及やカメラ本体の小型化が進むことにより，モバイル端末のユーザが気づかない間に認証動作を録画されることが増えると予想されている [4]．実際に銀行の ATM で認証動作の盗撮による情報漏洩 [5] が発生しており，録画された認証動作を解析されることにより，認証情報が漏れ，悪用されることが懸念される．

認証時における覗き見の問題に対して，様々な研究が行われている [6]～[14]．しかし，録画による覗き見への対策やモバイル端末上での利用を想定したユーザビリティの考慮などの課題がある．

そこで本研究では，モバイル端末の覗き見による画面ロックの認証情報漏洩を防止するために，覗き見耐性をもつユーザ認証システムを実装する．具体的には，我々が以前提案した，覗き見耐性をもつ STDS（Secret Tap with Double Shift）認証方式 [15] を，ユーザ認証システムに導入する．STDS 認証方式は，ユーザのみが知り得る認証情報の間接的な入力法則を有し，覗き見に対する耐性を有する．更に，STDS 認証方式と

† 神奈川工科大学，厚木市
Kanagawa Institute of Technology, Atsugi-shi, 243–0292 Japan
†† 宮崎大学，宮崎市
University of Miyazaki, Miyazaki-shi, 889–2192 Japan
* 本論文はシステム開発論文である．

併せて録画への対策を講じ，時間や場所を問わずに利用できるユーザビリティと実用性を目指す．

以降本論文では，**2.** で覗き見耐性をもつ認証方式について述べ，既存の認証方式の問題点を挙げる．**3.** では認証方式として導入する STDS 認証方式について述べ，**4.** では STDS 認証方式を導入したユーザ認証システムを実装する．**5.** では提案システムの有用性について考察する．

2. 覗き見耐性をもつ認証方式

覗き見による攻撃方法は，大きく二つに分けることができる．一つは「他人が認証動作を直接覗き見る攻撃」（以下，覗き見攻撃）であり，もう一つは「監視カメラなどの録画機器によって認証動作を記録し解析する攻撃」（以下，録画攻撃）である．一般に，認証動作を完全に記録できる録画攻撃の方が，覗き見攻撃よりも耐性をもたせることが難しい．

覗き見耐性をもつ認証方式とは，認証動作を他人に見られていても認証情報が露呈しない認証方式である．覗き見耐性をもたない認証方式では，認証情報を盗まれないようにするために，常に周りの目を気にして認証しなければならない．また，他人に見られるだけでなく，監視カメラなどの録画機器に認証動作を録画され，認証情報が露呈する危険性もある．そのため，覗き見耐性をもたせるためには，何度も見られても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．

以下では，覗き見耐性をもつ既存の認証方式とその問題点について述べる．

2.1 覗き見耐性をもつ PIN 認証方式

覗き見への耐性を有するため，PIN の入力を工夫した認証方式がある．

認証方式 [6] は，0 から 9 までの番号を画面の左右に 4 桁ずつ配置し，あらかじめ定めた PIN が含まれている 4 桁の番号を右か左かで答える方式である．覗き見への対策として，PIN が含まれていない場合の偽入力を備えており，PIN が特定されにくいように工夫されている．しかし，認証の入力は「PIN が含まれているのは右か左か」の二つの入力しかないため，1 回の入力における認証成功の確率は $\frac{1}{2}$ であり，任意の入力によって偶然に認証が成功してしまうこと（以下，確率的誤認証）に対する耐性は低いという問題がある．

SECUREMATRIX [7] は，認証ごとに異なるマトリクス表をユーザに提示し，ユーザはあらかじめ登録したマトリクス表上の場所にある数字を PIN として入力する認証方式である．認証ごとに異なるマトリクス表により，PIN をワンタイムパスワードとして利用できるため，覗き見攻撃により PIN を取得されても安全である．また，マトリクス表上には同じ番号が複数存在しているため，ユーザが秘密情報としてあらかじめ登録したマトリクス表上の PIN 取得の場所を絞り込むことは難しい．しかし，複数回の覗き見攻撃や録画攻撃を受け，PIN やマトリクス表を複数取得された場合，秘密情報である PIN 取得の場所を特定される可能性がある．

2.2 覗き見耐性をもつグラフィカル認証方式

覗き見耐性をもちつつ，認証情報をグラフィカルにすることによって，ユーザビリティを向上した認証方式がある．

認証方式 [8] は，ユーザが秘密情報として複数選択したアイコンを頂点とし，それらを結び囲んだ多角形内に含まれるアイコンを，認証情報のアイコンとする．認証情報となるアイコンは，秘密情報のアイコンの位置によって毎回異なるため，認証動作を覗き見られても認証情報が漏洩することはない．しかし，これらの認証方式は，録画攻撃により秘密情報のアイコンがある程度絞り込まれてしまう可能性があるため，録画攻撃への対策を検討する必要がある．

認証方式 [9] は，画面上に指でパターンを描く認証方式であり，画面を分割したエリア上に描いたパターンが含まれるか否かを認証情報にしている．入力に時間差をつけたり，偽のパターンを組み合わせて描いたりと，認証入力を惑わすことによって覗き見耐性を有しているが，画面上に残る指跡から認証情報を割り出すことが可能であるため，覗き見耐性は十分ではない．

2.3 録画攻撃への耐性を有する認証方式

背景配列の移動量を用いた個人認証方式 [10] 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，入力を工夫し覗き見耐性をもたせた認証方式である．文字の背景に異なる色や図形の配列（背景配列）を表示し，パスワードの背景が同一になるように背景を移動させ，認証を行う．パスワードを直接入力はせず，また，背景配列の中には同一の背景がいくつもあるため，パスワードの候補を絞られにくい．しかし，パスワード 1 文字ごとに背景を移動させるため，認証入力に時間を要し，画面ロックの認証方式には不向きである．

fakePointer [11] は，PIN と背景のマークとの組合

せによって認証を行う認証方式である．PIN は永続記録による固定パスワードであり，マークは常にランダムに生成される使い捨てパスワードを利用している．その 2 種類の認証情報によって，どちらかの情報が漏洩しても認証情報の特定が困難である．この認証方式は，認証を行う前に使い捨てパスワードである背景のマークを取得する必要があり，それを取得する際には覗かれないように人目を気にする必要がある．

振動機能を応用した個人認証方式 [12] は，金庫などで使用されるダイヤル式ロックをもとにしており，認証のたびにランダムに変わるダイヤルの番号入力位置を振動によって通知し，その入力位置に暗証番号どおりに数字を合わせて認証を行う．暗証番号を間接的に入力し，かつ，入力位置を振動によって端末のユーザのみに通知するため，認証動作を録画されても暗証番号は露呈されない．しかし，この認証方式は認証入力位置を確認するために振動を感じ取る必要があるため，暗証番号を入力するまでに時間を要し，画面ロックの認証方式には不向きである．

2.4 付属装置を利用した認証方式

監視カメラなどの死角に認証用の付属装置を設置し，その装置を介して認証を行う認証方式がある．この認証方式は，肩越しの視線や監視カメラから認証入力を隠すことより，覗き見耐性を得ている．例として，認証台上のトラックボールを手で覆い，そのボールの転がし方で認証を行う Undercover 認証方式 [13] や，モバイル端末の背面にタッチセンサーを取り付け，そのタッチパターンによって認証を行う認証方式 [14] がある．これらの認証方式は，端末に専用の装置を取り付ける必要があるため，導入にコストがかかるなどの問題がある．

3. STDS 認証方式の導入

本研究では，覗き見耐性をもつユーザ認証システムの認証方式として，STDS（Secret Tap with Double Shift）認証方式を導入する．STDS 認証方式は，我々が以前に提案した認証方式 [15] であり，暗証番号やパスワードの代わりにアイコンを用いたチャレンジレスポンス型の方式である．認証情報は，パスワードの代わりとなるアイコン（以降，パスアイコン）と，端末間との共通鍵である移動法則（以降，シフト）の 2 種類の情報を用いる．シフトの詳細は **3.2** で説明する．認証時，端末はパスアイコンを 1 個含む一定長のアイコン列（以降，チャレンジアイコン）をチャレンジとしてユーザに提示し，ユーザはアイコン列内のパスアイコンからシフトに従い，アイコン列内を移動した先のアイコン（以降，レスポンスアイコン）をレスポンスとして選択する．

アイコンを含むグラフィカルなパスワードには，そのパスワードの特徴や共通点をユーザ独自の観点で決めやすいため，登録したユーザは覚えやすく，攻撃者は覚えにくいという性質がある [16]．その性質は覗き見耐性への補強に繋がると考え，暗証番号などテキストベースのパスワードの代わりにアイコンを用いて認証を行う．

また本研究では，覗き見耐性をもつユーザ認証システムの実装に当り，以下の項目を目標とする．

- 覗き見攻撃への耐性

攻撃者は覗き見により，レスポンスアイコンの個数や種類について特定が可能であり，覗き見攻撃は録画攻撃よりも発生頻度が高いと考えられる．そのため複数回の覗き見により，レスポンスアイコンが露呈しても，パスアイコンが特定されない強度を目指す．

- 録画攻撃への耐性

録画機器によって認証画面を記録されることにより，レスポンスアイコンだけでなくチャレンジアイコンも特定されることが考えられる．そこで，録画攻撃によりチャレンジアイコンが露呈しても，パスアイコンが特定されない強度を目指す．

- 確率的誤認証への耐性

任意の入力により偶然に誤認証が起こらないように，米国国立標準技術研究所の「電子的認証に関するガイドライン」[17] 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．

- ユーザビリティ

ユーザの受け入れやすさを考慮し，既存の認証手法と同程度の認証入力時間を目指す．

以下では，STDS 認証方式の認証プロトコル，シフトによるレスポンスアイコンの決定方法，及び録画攻撃対策のための追加機能について述べる．

3.1 認証プロトコル

STDS 認証方式は，ユーザが認証情報を登録する登録フェーズと，ユーザの認証を行う認証フェーズからなる．以下では，本プロトコルで用いる定義と記法，及び，各フェーズのプロトコルについて述べる．

3.1.1 定義と記法

本プロトコルで用いる記号及び機能について，以下を定義する．

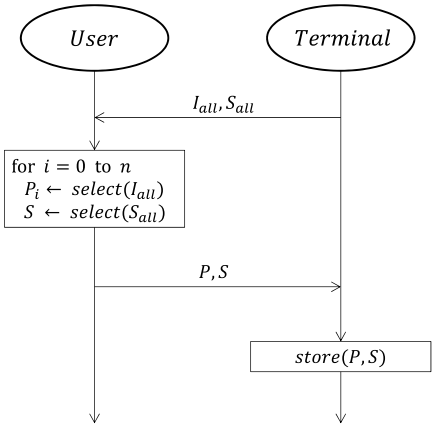

図 1　登録フェーズ
Fig. 1　The registration phase.

- 記号
  - $User$: ユーザ
  - $Terminal$: ユーザが所有する端末
  - S_{all}: 選択可能な全てのシフト移動量
  - I_{all}: 選択可能な全てのアイコン列
  - S: ユーザが選択したシフト移動量
  - n: パスアイコン数
  - $P ::= P_0, P_1, ..., P_{n-1}$

パスアイコン $P_0, P_1, ..., P_{n-1}$ を含むアイコン列 P

  - m: チャレンジアイコンの最大アイコン列長
  - $C ::= C_0, C_1, ..., C_{m-1}$

チャレンジアイコン $C_0, C_1, ..., C_{m-1}$ を含むアイコン列 C

  - R_u: ユーザが導出したレスポンスアイコン
  - R_t: 端末が導出したレスポンスアイコン
  - $A \rightarrow B$: A から B へ送信する．
  - $A \leftarrow B$: A へ B を代入する．
- 機能

以下の機能において，$array$ は任意の数列（アイコン列）とする．

  - $select(array)$

$array$ から要素を選択する．

  - $store(array)$

$array$ を端末に保存する．

  - $random(array)$

$array$ からランダムに要素を返す．

  - $shuffle(array)$

$array$ の要素をランダムに並べ換える．

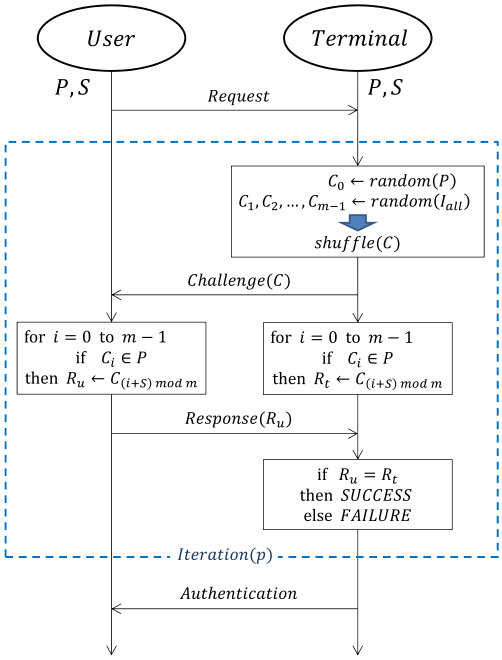

図 2　認証フェーズ
Fig. 2　The authentication phase.

3.1.2　登録フェーズ

図 1 に，登録フェーズを示し，以下で説明する．

（1）　$Terminal \rightarrow User : I_{all}, S_{all}$

端末はユーザに対し，選択可能な全てのアイコン列 I_{all}，及び，選択可能な全てのシフト移動量 S_{all} を送信する．

（2）　$User : P_i \leftarrow select(I_{all})$ （for $i = 0$ to n）

ユーザは I_{all} からパスアイコンを n 個選択し，パスアイコンのアイコン列 P へ代入する．

（3）　$User : S \leftarrow select(S_{all})$

ユーザは S_{all} から移動量を選択し，シフト移動量 S へ代入する．

（4）　$User \rightarrow Terminal : P, S$

ユーザは端末に P 及び S を送信する．

（5）　$Terminal : store(P, S)$

端末は P 及び S を保存する．

登録フェーズを完了したとき，ユーザ及び端末間において，パスアイコン列 P とシフト移動量 S を共有した状態になる．

3.1.3　認証フェーズ

図 2 に，認証フェーズを示し，以下で説明する．

（1）　$User \rightarrow Terminal : Request$

ユーザは端末に認証リクエスト（端末の起動）を送信する．

（2） $Terminal : C_0 \leftarrow random(P),$
$C_1, C_2, ..., C_{m-1} \leftarrow random(I_{all})$

端末は，アイコン C_0 にランダムに選択したパスアイコンを，C_0 以外の要素にランダムに選択したアイコンを代入し，チャレンジアイコンのアイコン列 C を作成する．このとき，C に含まれるパスアイコンは 1 個とし，アイコンの重複はしない．

（3） $Terminal : shuffle(C)$

端末は，C の要素をランダムに並べ換える．

（4） $Terminal \rightarrow User : Challenge(C)$

端末はユーザに対し，チャレンジとして C を送信する．

（5） $User$: if $C_i \in P$ then $R_u \leftarrow C_{(i+S) \bmod m}$
(for $i = 0$ to $m-1$)

ユーザは，C に含まれるパスアイコンから S の分だけ C 内を移動した先のアイコンを導出し，そのアイコンをユーザのレスポンスアイコン R_u とする．

（6） $Terminal$:
if $C_i \in P$ then $R_t \leftarrow C_{(i+S) \bmod m}$
(for $i = 0$ to $m-1$)

端末も (5) と同様に，C に含まれるパスアイコンから S の分だけ C 内を移動した先のアイコンを導出し，そのアイコンを端末のレスポンスアイコン R_t とする．

（7） $User \rightarrow Terminal : Response(R_u)$

ユーザは端末に対し，レスポンスとして R_u を送信する．

（8） $Terminal$: if $R_u = R_t$
then $SUCCESS$ else $FAILURE$

端末は，R_u と R_t を比較し，一致していれば $SUCCESS$ とし，そうでなければ $FAILURE$ とする．

（9） $Iteration(p)$

(2)〜(8) を p 回繰り返す．

（10） $Terminal \rightarrow User : Authentication$

端末はユーザに対し，認証結果を送信する．全てのパスアイコンにおいて $SUCCESS$ であれば認証成功とし，1 個でも $FAILURE$ があれば認証失敗とする．

3.2 シフトによるレスポンスアイコンの決定方法

STDS 認証方式では，覗き見耐性を得るために，シフトによってレスポンスアイコンを決定する．認証時，画面上に表示している 4 × 4 のアイコン群を，2 × 2 の 4 個組のアイコン群に分ける．それぞれのアイコン群を第 1〜第 4 グループとし，パスアイコンを含むグループからグループ間またはグループ内を移動し，その移動先にあるアイコンをレスポンスアイコンとする．シフトの対象がグループ間の場合をグループ間シフト，グループ内の場合をグループ内シフトとする．**3.1** で定義した，ユーザが選択したシフト量 S は，グループ間シフト及びグループ内シフトの総移動量であり，$S = 4 \times S_{inter} + S_{inner}$ で求められる．ここで S_{inter} はグループ間シフトの値，S_{inner} はグループ内シフトの値をそれぞれ表す．

図 3 に，グループ間シフトによる移動例を示す．この例では，第 1 グループの右上のアイコンがパスアイコンである．このときパスアイコンも含め，各グループの右上のアイコンがレスポンスアイコンの候補にな

図 3　グループ間シフトによる移動例
Fig. 3　Example of the shift function inter groups.

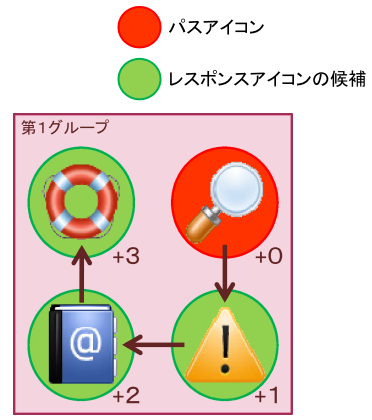

図 4　グループ内シフトによる移動例
Fig. 4　Example of the shift function inner groups.

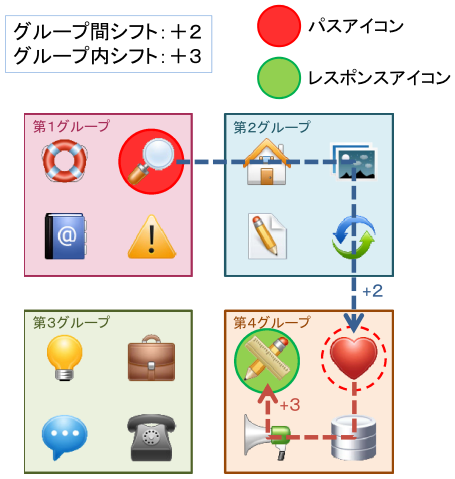

図 5　両シフトの併用による移動例
Fig. 5　Example of using the two shift functions.

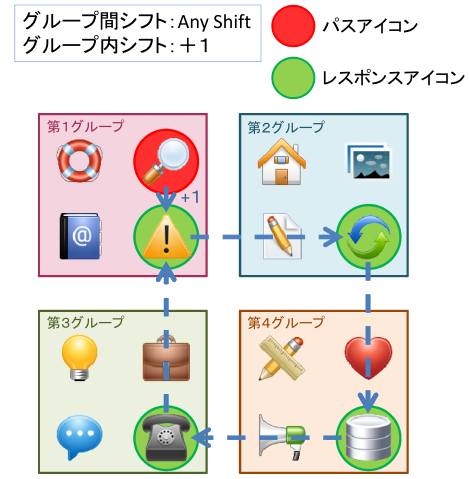

図 6　グループ間シフトに Any Shift を導入した際の移動例
Fig. 6　Example of the shift function inter groups is ‘Any Shift’.

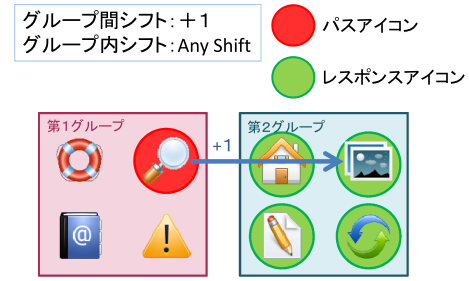

図 7　グループ内シフトに Any Shift を導入した際の移動例
Fig. 7　Example of the shift function inner groups is ‘Any Shift’.

る．シフトの値には+0～+3 を割り当てることができ，その値の分だけ時計回りにグループ間を跨ぎ，移動先のアイコンがレスポンスアイコンになる．

図 4 に，グループ内シフトによる移動例を示す．この例では，第 1 グループ内を対象とし，右上のアイコンがパスアイコンである．パスアイコンを含め，グループ内の全てのアイコンがレスポンスアイコンの候補になる．グループ間シフトと同様，シフトの値は+0～+3 を割り当てることができ，その値の分だけ時計回りにグループ内のアイコン間を移動し，移動先のアイコンがレスポンスアイコンになる．

図 5 に，グループ間シフト及びグループ内シフトの併用による移動例を示す．この例では，グループ間シフトの値は+2，グループ内シフトの値は+3 であり，パスアイコンは第 1 グループの右上のアイコンである．まず，グループ間シフトにより時計回りで 2 グループ先の第 4 グループに移動する．次に，グループ内シフトにより第 4 グループ内の右上のアイコンから時計回りに 3 アイコン移動し，移動先の左上のアイコンがレスポンスアイコンになる．

グループ間シフトとグループ内シフトを併用することにより，画面上の 16 個のアイコン全てがレスポンスアイコンの候補になり得るため，認証動作を覗かれたとしても，認証情報であるパスアイコンを特定することは困難である．

3.3　録画攻撃対策のための追加機能

3.3.1　Any Shift 機能

録画攻撃への対策を施すために，Any Shift 機能を追加する．Any Shift 機能とは，グループ間シフトまたはグループ内シフトの値を固定せず，認証入力の際にユーザが任意にシフト値を決定できる機能 [15] である．

図 6 に，グループ間シフトに Any Shift を導入した際の移動例を示す．パスアイコンの位置を第 1 グループの右上のアイコンとし，グループ間シフトは Any Shift，グループ内シフトは+1 とする．このとき，レスポンスアイコンは各グループの右下のアイコンになり，ユーザはこれら 4 個のアイコンから任意に 1 個を選択し，タップする．

図 7 に，グループ内シフトに Any Shift を導入した際の移動例を示す．図 6 と同様にパスアイコンの位置を第 1 グループの右上のアイコンとし，グループ間シ

フトは+1，グループ内シフトは Any Shift とする．このとき，レスポンスアイコンは第 2 グループ内の全てのアイコンになり，ユーザはグループ内のアイコンから任意に 1 個を選択し，タップする．

Any Shift を導入することにより，ユーザは認証画面が変わるたびに任意のシフトでタップが可能であるため，認証動作を録画されても，シフトやアイコンを絞り込むことが容易ではない．

3.3.2 フェイクモード

Any Shift 機能を導入する際，もう片方のシフトの値は固定されたままであるため，シフト値を特定されてしまう可能性がある．そこで録画対策への更なる対策として，フェイクモードを追加する．

フェイクモードは，認証入力の際，アプリケーションが合図を発したとき，レスポンスアイコンとは異なるアイコンをわざとタップすることにより，攻撃者の混乱を誘う機能である．フェイクモードで認証を行うことにより，認証動作を録画されても，シフト値が異なるアイコンをタップするため，パスアイコンを特定することは容易ではない．更に Any Shift 機能も併用することにより，録画攻撃への強固な対策になると考えられる．

4. ユーザ認証システムの実装

4.1 アプリケーションの実装

Android OS を搭載したモバイル端末を対象とし，ユーザ設定アプリケーションは Android アプリケーション，認証アプリケーションは常駐型の Java アプリケーションとして実装する．

図 8 に，ユーザ認証システムの構造を示す．ユーザ認証システムは，ユーザ設定アプリケーションと認証アプリケーションの二つのアプリケーションからなる．

ユーザ設定アプリケーションは，**3.1.2** の登録フェーズに当り，メイン画面と認証情報設定画面をユーザに提示する．メイン画面では画面ロックの有効化または無効化を，認証情報設定画面では認証情報をユーザが任意に登録する．そして，画面ロックの有効または無効，及び認証情報はモバイル端末内の記憶装置へ書き込む．

認証アプリケーションは，**3.1.3** の認証フェーズに当り，端末画面起動受理部と認証入力画面からなる．端末画面起動受理部では，認証画面の起動を行う．Android 端末から画面起動通知を受理した際，まずモバイル端末内の記憶装置から画面ロックの有効または

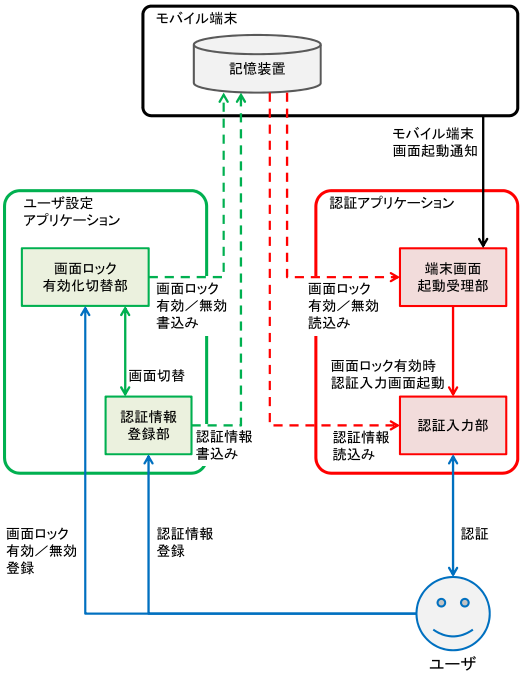

図 8 覗き見耐性をもつユーザ認証システムの構造
Fig. 8 A structure of the user authentication system resists shoulder-surfing attack.

無効の値を読み取る．そして，画面ロックが有効であれば，認証入力画面を起動し，ユーザに提示する．認証入力画面を起動する際，認証情報を記憶装置から読み取る．ユーザは，認証入力画面を通じて認証を行い，画面ロックを解除する．認証アプリケーションは，端末の画面起動通知を受理するため，端末上に常駐する必要がある．

図 9 に，ユーザ設定アプリケーションのメイン画面を示す．アプリケーション起動時はメイン画面を提示する．ユーザは画面下部のボタンを使って操作する．LOCK（UNLOCK）ボタンは，画面ロックの有効／無効を切り替える．SETTING ボタンは，認証情報登録画面に切り替わり，認証情報を登録する．EXIT ボタンは，アプリケーションを終了する．

図 10 は，認証情報登録のパスアイコン登録画面を示す．パスアイコン登録画面では，アイコン群の中から任意のアイコンをタップすることにより，パスアイコンの候補を 4〜6 個挙げることができる．アイコン群には，パスアイコンを最大の 6 個に設定しても認証時のチャレンジアイコンが重複しないように，$16 \times 6 = 96$ 個のアイコンが含まれている．画面上に

図 9　メイン画面
Fig. 9　Main display of Secret Tap.

図 10　パスアイコン登録画面
Fig. 10　Pass icon registration display.

図 11　シフト値登録画面
Fig. 11　Shift values registration display.

表示しきれていないアイコンは，アイコン群を上下にスライドすることによって表示することができる．画面下部の CLEAR ボタンによりパスアイコンの全取消し，BACK ボタンによりパスアイコンの単数取消しを行うことができる．そして登録画面を終了する際は，CANCEL ボタンによりパスアイコンを登録（更新）せずに終了，OK ボタンによりパスアイコンを登録して終了することができる．また，パスアイコンが 3 個以下の場合は OK ボタンを押しても登録することができない．

図 11 は，シフト値登録画面を示す．シフト値登録画面では，グループ間シフトまたはグループ内シフトで任意のシフトを選択することができる．シフトを選択すると，右下の格子図にパスアイコンとレスポンスアイコンとの位置を提示し，シフトによるレスポンスアイコンの移動先をユーザが直観的に理解しやすいようにしている．また，シフトの向きは，時計回りと反時計回りのどちらかを選択できる．

図 12 は，認証時の認証画面を示す．画面内には，16 個のアイコンが 4 × 4 の格子状に並んでおり，ユーザはパスアイコンとシフトからレスポンスアイコンを導

図 12　認証画面
Fig. 12　Authentication display of Secret Tap.

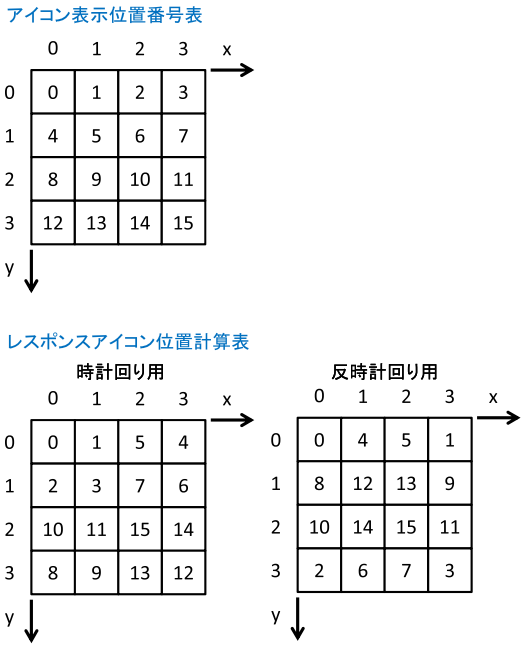

図 13　アイコン表示位置 ID 表及びシフト値計算表
Fig. 13　Tables of identification number of icons and shift calcuration.

き出しタップする．タップするごとにアイコン群はパスアイコンとともに総入れ替えをし，ランダムに並ぶ．全てのパスアイコン分のレスポンスアイコンをタップした後に認証判定に移行し，全て正解のレスポンスアイコンであれば画面ロックを解除し，1 個でも不正解であればユーザに対し再度タップを促す．タップによる入力は，再入力も含め計 3 回まで可能であり，それを超えた場合は端末を再起動するまでタップ入力を受け付けない．

4. 2　STDS 認証方式の実装

ユーザ認証システムに覗き見耐性をもたせるために，STDS 認証方式を実装する．認証入力の際，パスアイコンの表示位置は認証のたびに異なるため，そのたびにレスポンスアイコンの位置を決定する必要がある．まずパスアイコンを含むグループとグループ内の位置を逐一把握し，グループ間シフト及びグループ内シフトをそれぞれ考慮しながらレスポンスアイコンの位置を計算する．しかし，その計算量が多くなると，レスポンスアイコンの正否判定やパスアイコンの表示に遅れが生じ，認証入力に支障が出るため，複雑なシフト移動処理を軽減することが必要である．そこで，レスポンスアイコン位置計算表を作成し，あらかじめシフト値別のレスポンスアイコンを決定する手法を提案する．

図 13 に，アイコン表示位置番号表及びレスポンスアイコン位置計算表を示す．表内には 0 から 15 までの番号があり，横軸を x 軸，縦軸を y 軸，第 1 グループの左上のアイコンを $(x, y) = (0, 0)$ とした座標軸を設ける．レスポンスアイコン位置計算表には，第 1 グループの左上のアイコン（番号 0）を基準とし，x 軸方向にはグループ内シフトの移動先アイコンの番号を，y 軸方向にはグループ間シフトの移動先アイコンの番号を，シフトの向きに従って順番に入れる．

以下に，パスアイコンの位置を起点としてレスポンスアイコンの位置を求める手順を示す．

（1）　アイコン表示位置番号表に従い，パスアイコンの位置の座標 (x_p, y_p) を導き出す．

（2）　座標 (x_p, y_p) を以下の剰余式に代入し，レスポンスアイコンの座標 (x_t, y_t) を求める．

$$x_t = (x_p + S_{inner}) mod 4,$$
$$y_t = (y_p + S_{inter}) mod 4$$

（3）　シフトの向きに合うレスポンスアイコン位置

計算表を用い，表中の座標 (x_t, y_t) の番号 N を導き出す．

（4） アイコン表示位置番号表において，番号 N の位置がレスポンスアイコンの位置になる．

例として，パスアイコンが第 1 グループの右上，グループ間シフトの値が+2，グループ内シフトの値が+3，シフトの向きが時計回りである場合のレスポンスアイコンを求める．まず，パスアイコンの座標はアイコン表示位置番号表により，番号 1 の $(x_p, y_p) = (1, 0)$ になる．座標 $(1, 0)$ と各シフト値を剰余式に代入し，$(x_t, y_t) = (0, 2)$ になる．時計回り用のレスポンスアイコン位置計算表の座標 $(0, 2)$ により，番号は 10 となり，アイコン表示位置番号表での 10 の位置（第 4 グループの左上）がレスポンスアイコンになる．

4.3 フェイクモードの実装

録画攻撃への対策として，フェイクモードを実装する．合図には，バイブレート機能を用いる．その理由として，覗き見や録画されている場合でも，攻撃者に気づかれることなく，ユーザに合図として伝えることができるためである．ユーザが振動を感知しやすく，かつ，振動音が周りに聞こえないようにするために，振動時間は 0.5 秒とする．

合図があった際の認証判定は，通常時の認証判定を反転することによって行う．つまり，通常レスポンスアイコンであるアイコンは不正解になり，それ以外の 15 個のアイコンが正解になる．フェイクモード時の認証強度を保つため，1 回の認証におけるアイコンのタップ数は「パスアイコン数＋偽の入力数」とする．

5. ユーザ認証システムの評価及び考察

覗き見耐性をもつユーザ認証方式の有用性を確認するため，3. 節で挙げた各目標について，以下に述べる．

5.1 覗き見攻撃への耐性の評価

覗き見攻撃への耐性を評価するために，覗き見攻撃の実験を行った．被験者は，神奈川工科大学情報学部の学生 118 名を対象とし，以下に，実験実施要項を示す．

- 実験手順は以下のとおりである．

（1） 5〜6 人の班を作成する．

（2） 班内で親を 1 人決める．

（3） 親はあらかじめ認証情報を登録する．

（4） 班員は親を囲み，親は認証入力を行う．

（5） 班員は親の認証動作を覗き見て，認証情報を特定する．

（6） 認証成功回数が 10 回になるまで，親は認証入力を繰り返す．

- 実験を行う前に，各認証方法についてレクチャーを合計 20 分間行う．
- 以下の認証方式を，それぞれ親を交代しながら行う．
  - PIN
  - Android PP
  - 覗き見耐性をもつユーザ認証方式
    - Any Shift なし，フェイクモードなし
    - Any Shift あり，フェイクモードなし
    - Any Shift なし，フェイクモードあり
- 認証情報を途中で変更する場合，変更した時点から認証成功回数を数え直す．
- 認証情報の特定の可否による賞罰は与えない．

以上の実験の結果，PIN 及び Android PP については，全員が親の認証情報を特定することができた．しかし，STDS 認証方式については，Any Shift 及びフェイクモード関係なく，誰一人として認証情報を特定できなかった．

これにより，STDS 認証方式は覗き見耐性を有している．

5.2 録画攻撃への耐性の考察

本論文では，STDS 認証方式における録画攻撃の耐性を考察するために，パスアイコン特定率（以下，SP 率）を定義する．SP 率とは，攻撃によって特定されたパスアイコン候補群に占める正解のパスアイコンの割合であり，以下の式によって求める．

$$\text{SP 率 (\%)} = \frac{\text{正解のパスアイコン数}}{\text{パスアイコン候補数}} \times 100$$

SP 率が高いほど，パスアイコンが特定され，攻撃者に認証を解かれやすくなることを示す．以下では，STDS 認証方式の各機能における，1 回目及び 2 回目の録画攻撃への耐性について，SP 率を用いて考察をする．

5.2.1 1 回目の録画攻撃への耐性

1 回目の録画攻撃への耐性について，STDS 認証方式の各機能の有無別に場合分けをし，それぞれ考察する．また，ここでのパスアイコン数は 4 個を想定する．

- Any Shift 及びフェイクモードを用いない場合

録画攻撃によって露呈する情報は，各チャレンジアイコン及びレスポンスアイコンである．シフト移動量は固定であるため，レスポンスアイコンをもとにチャレンジアイコンをシフト別に分けることができる．シフトはグループ間シフトとグループ内シフトでそれぞ

れ 4 パターンずつあるため，シフト別に分けたアイコン列は $4 \times 4 = 16$ 組できる．この中には，パスアイコンのアイコン列が含まれるため，この 16 組のアイコン列をパスアイコン候補としたとき，SP 率は以下のようになる．

$$\text{SP 率} = \frac{1}{16} \times 100 = 6.25\% \quad (1)$$

シフト別にアイコンを分ける手法は，パスアイコンを導くための効率的な解析手法の一つであり，攻撃者が行う攻撃方法であると考えられる．この解析手法を以下では「シフト分別法」とし，各機能での解析手法として用いる．

- Any Shift のみを用いる場合

Any Shift には，グループ間シフトが Any Shift の場合と，グループ内シフトが Any Shift の場合の二つがある．攻撃者は，ユーザがどちらの場合を用いているか分からないため，両方とも考える必要がある．前者の場合，グループ間シフトは 1 個のレスポンスアイコンにつき 4 パターン考えられ，レスポンスアイコンごとに異なる．レスポンスアイコンはパスアイコンと同数であるため，グループ間シフトの組合せは $4^4 = 256$ 組である．後者の場合も，前者と同様にグループ内シフトの組合せは 256 組である．

シフト分別法により，Any Shift ともう一方の固定したシフト別に分けたとき，シフト別のアイコン列は $256 \times 4 + 256 \times 4 = 2,048$ 組でき，この中にパスアイコンのアイコン列も含まれる．このときの SP 率は以下のようになる．

$$\text{SP 率} = \frac{1}{2,048} \times 100 = 0.04\% \quad (2)$$

式 (1) 及び式 (2) より，Any Shift のみを用いた場合は，Any Shift 及びフェイクモードを用いない場合よりも SP 率が低い．そのため，Any Shift により録画攻撃への耐性が向上したことが考えられる．

- フェイクモードのみを用いた場合

フェイクモードにおいて，偽の入力回数は 2 回としたとき，入力回数はパスアイコン数と偽の入力回数により 6 回となる．攻撃者は，この入力回から正解の入力回を導出する必要がある．このときの入力回の組合せは ${}_6C_4 = 15$ 通りあり，この中に正解の入力回が含まれる．このときの SP 率は，式 (1) と入力回の組合せにより，以下のようになる．

$$\text{SP 率} = (\frac{1}{16} \times \frac{1}{15}) \times 100 = 0.41\% \quad (3)$$

式 (1) 及び式 (3) より，フェイクモードのみ用いた場合は，Any Shift 及びフェイクモードを用いない場合よりも SP 率が低い．そのため，フェイクモードにより録画攻撃への耐性が向上したことが考えられる．また式 (2) より，Any Shift の方がフェイクモードよりも SP 率が低いため，録画攻撃への耐性は Any Shift の方が向上することが考えられる．

- Any Shift とフェイクモードを併用する場合

式 (2) とフェイクモードの入力回の組合せにより，SP 率は以下のようになる．

$$\text{SP 率} = (\frac{1}{2,048} \times \frac{1}{15}) \times 100 = 0.003\% \quad (4)$$

式 (2)〜式 (4) により，Any Shift とフェイクモードを併用する場合が最も SP 率が低い．これにより，Any Shift とフェイクモードを併用することにより，それぞれ単独で用いるよりも録画攻撃への耐性が向上することが考えられる．

5. 2. 2 2 回目の録画攻撃への耐性

2 回目の録画攻撃の場合，露呈する情報は 1 回目と同じであるが，レスポンスアイコンは異なる．そのため，シフト分別法によりチャレンジアイコンをシフト別に分けた 16 組のアイコン列は 1 回目のものと異なる．しかし，パスアイコンのアイコン列は 1 回目と 2 回目とも同じアイコンが含まれるため，パスアイコンが露呈することになる．パスアイコン以外の 15 組のアイコン列で，1 回目と 2 回目が同じである確率は $(1/15)^4 \times 15 = 1/3,375$ である．このことから，2 回目の録画攻撃によりパスアイコンが特定され，またシフト別に分けていることから，シフトの移動量も同時に特定されると考えられる．

Any Shift を用いた場合も同様に，シフト分別法により 1 回目と 2 回目のシフト別に分けたアイコン列を比較することにより，パスアイコンが露呈する．

フェイクモードを用いた場合も，シフト分別法により 1 回目と 2 回目のパスアイコンを含むアイコン列が特定されるが，それらのアイコン列には偽の入力回で入力したアイコンが含まれている．しかし，それらのアイコンは 1 回目と 2 回目とで異なるため，結果として同じアイコンであるパスアイコンが露呈する．

これらにより，STDS 認証方式において録画攻撃対策の機能を用いたとしても，2 回以上の録画攻撃によって認証情報が露呈してしまうことが考えられる．

5. 3 確率的誤認証への耐性評価

確率的誤認証に対する認証方式の強度は，以下の情

報量の計算によって求められる．

$$\text{情報量 } H = -\sum_i P_i \log_2 P_i$$

米国国立標準技術研究所 [17] が定めている，パスワード及び暗証番号に必要な強度は 2^{-14} である．これは，考え得るパスワード及び暗証番号の総パターン数が 2^{14} 通り以上必要であることを示している．この強度を式 (1) の P_i に代入すると，

$$\begin{aligned} H &= -\sum_{i=1}^{2^{14}} 2^{-14} \log_2 2^{-14} \\ &= \log_2 2^{14} \\ &= 14 \end{aligned} \tag{5}$$

となり，情報量 14bit 以上が強度の目標になる．

提案手法は，認証画面に 16 個のアイコンがあり，Any Shift 機能を用いない場合，レスポンスアイコンは 1 個である．そのため，提案手法の情報量は，パスアイコン数を n 個とした場合，式 (1) に代入し，以下のとおりになる．

$$\begin{aligned} H &= -\sum_{i=1}^{16^n} 16^{-n} \log_2 16^{-n} \\ &= \log_2 2^{4n} \\ &= 4n \end{aligned} \tag{6}$$

式 (5) 及び式 (6) より，目標の強度を上回るには，パスアイコン数が 4 個以上である必要がある．また，Any Shift 機能を用いた場合，レスポンスアイコンは一画面に 4 個であるため，そのときの情報量は，パスアイコン数を n 個とした場合，式 (1) に代入し，以下のとおりになる．

$$\begin{aligned} H &= -\sum_{i=1}^{4^n} 4^{-n} \log_2 4^{-n} \\ &= \log_2 2^{2n} \\ &= 2n \end{aligned} \tag{7}$$

式 (5) 及び式 (7) より，Any Shift 機能を用いた場合，目標の強度を上回るには，パスアイコン数が 7 個以上である必要がある．

認証入力の際，ユーザはパスアイコンを覚えておく必要があるため，必要なパスアイコン数が増えることは大きな負担になる．そのため，確率的誤認証に対して十分な耐性を得るには，ユーザビリティの低下を考慮する必要がある．

フェイクモードを用いた場合は，用いない場合と比べて情報量に大きな差はないため，必要なパスアイコン数に変わりはない．しかし，認証動作の一連において，偽の入力がある分だけ入力回数が増えるため，ユーザビリティの低下に繋がる．

5.4 ユーザビリティ評価

5.4.1 認証入力時間計測による評価

STDS 認証方式の慣れによる正確性や使いやすさの変化を評価するために，認証入力時間を計測した．神奈川工科大学の学生 6 人を被験者として，PIN 認証方式，STDS 認証方式の Any Shift なし，Any Shift あり，及びフェイクモードのそれぞれで連続 10 回ずつの認証入力を行った．パスアイコン及びシフトの移動量は被験者の任意とし，端末起動から画面ロック解除までの時間を計測する．途中で入力ミスにより認証失敗になっても続行し，ロック解除後に入力ミス数を自己申告してもらった．そして，これら一連の実験を開始 1 週間後，2 週間後，及び 3 週間後にもそれぞれ行い，慣れによる入力時間の変化を計測した．また，それぞれの機能の慣れを正確に計測するため，フェイクモードは単独の機能として用いており，Any Shift との併用は行っていない．

図 14 に，各方式の認証失敗回数を示す．グラフは 10 回の認証入力中に認証失敗した回数の 6 人の合計値である．図より，どの方式も第 2 週の失敗回数が最も低いことから，慣れによって入力の正確性が向上したと考えられる．しかし，第 1 週目は第 0 週目よりも失敗回数が多いことから，第 1 週目までは慣れが不十分であり，正確性が向上するためには 2 週間以上の使用が必要であると考えられる．

また，既存手法である PIN 認証方式において，各週の失敗回数が第 0 週目よりも多い．失敗した理由を実験後の被験者に対して伺った結果，被験者の慣れから起こる集中力低下や認証時間の短縮への焦燥感など，心理的な影響が考えられた．これは STDS 認証方式においても起こっていると考えられる．

図 15 に，各方式の認証入力時間を示す．グラフは各回の学生 6 人の平均時間であり，途中の入力ミスによって認証失敗をした回は含まない．図より，各週で時間が短縮していることが確認でき，第 0 週と第 3 週とを比較すると，Any Shift あり及びフェイクモードは 2 秒程度，その他は 1 秒程度短縮している．このこ

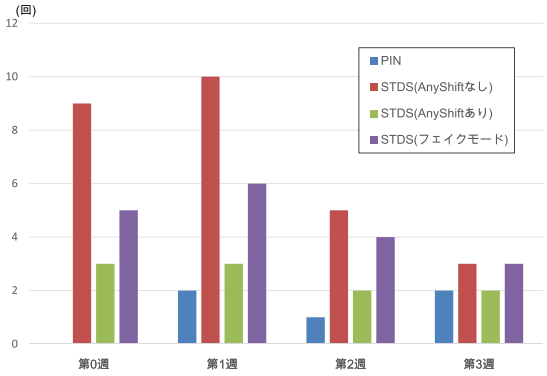

図 14　各方式における認証失敗回数
Fig. 14　Numbers of failed authentication in each method.

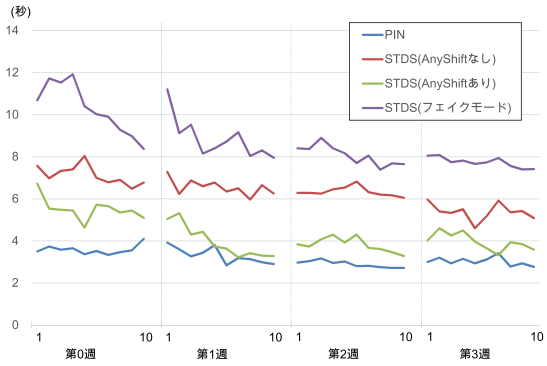

図 15　各方式における認証入力時間
Fig. 15　Input time of authentication in each method.

とから，慣れによって入力時間が短縮したことが考えられる．特にどのグラフも第 1 週目での 1 回目と 10 回目との時間差が大きく，第 2 週目と第 3 週目では大きな変化が見られないことから，慣れによる使いやすさの変化は正確性より早く現れやすく，2 週間程度で慣れが完了すると考えられる．

Any Shift ありの入力時間は従来の PIN 認証方式と比較して 0.5 秒程度の差であるため，実用的な時間内で認証入力できることが考えられる．一方フェイクモードは，第 2 週目で PIN 認証方式と比較しても 5 秒程度の差がある．この差が生じた理由として，フェイクモードは偽の入力を含むため他の方式より入力回数が多く，端末の振動を感知する必要があるため入力が慎重になりがちであることが挙げられる．

5. 4. 2　アンケート調査による評価

STDS 認証方式についてユーザへの受け入れやすさを評価するため，**5. 1** での実験で被験者になった学生

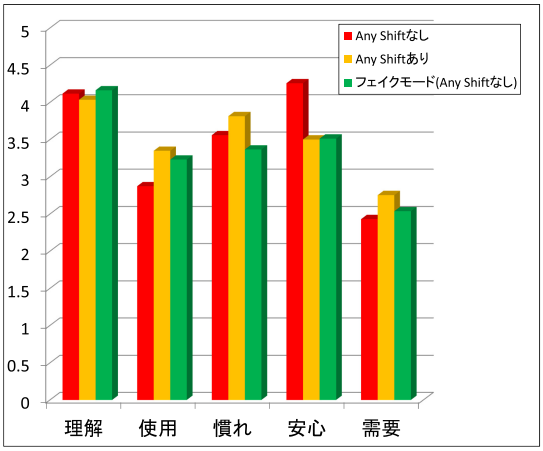

図 16　ユーザビリティに関するアンケート結果
Fig. 16　The results of usability.

にアンケート調査を実施し，86 名から有効な回答を得た．

アンケートは，提案手法の Any Shift 機能及びフェイクモードの有無別における以下の項目について，5 段階（最高値 5〜最低値 1）で評価する．

- 理解

機能や操作は理解しやすいか

- 使用

使いやすいか

- 慣れ

慣れれば使いやすいか

- 安心

覗き見に対して安心か

- 需要

普段の生活で使いたいか

図 16 に，アンケート結果を示す．棒グラフの値は平均値である．

理解については，いずれも高い評価（4 以上）を得た．このことから，シフトの動き方や操作は理解しやすいと考えられる．

使用及び慣れについては，いずれも評価値 3 以上であり．Any Shift ありが最も高かった．この理由として，Any Shift によりシフトを計算する手間が減少することによって，操作性が向上したことが考えられる．

安心については，いずれも評価値 3 以上を得たが，Any Shift なしが最も高かった．また，Any Shift 及びフェイクモードを利用した被験者の感想で以下が挙がった．

- Any Shift

– 「1 画面の正解確率が 1/16 から 1/4 になると不安だ.」

– 「解きやすくなったが攻撃者も解きやすそう.」

- フェイクモード

– 「振動音が周りに聞こえる.」

– 「歩きながらや周りが騒々しいときは振動が分からない.」

これらの感想から，異なった操作感や攻撃者が有利になることへの懸念が被験者の安心感に影響していることが，Any Shift やフェイクモードの評価値が低い理由であると考えられる．

需要に関しては，いずれの方式も評価値 3 以下になった．需要が低い理由として，STDS 方式は画面ごとにシフトの計算が必要であり，認証入力に手間がかかることから，安全性よりもユーザビリティを優先していることが考えられる．

以上により，ユーザビリティに関して一定の評価を得ることができたが，需要を高めるための改善が必要である．

6. むすび

本論文では，モバイル端末内の情報が漏洩するのを防ぐために，覗き見耐性をもつユーザ認証システムを提案し，Android アプリケーションとして実装した．認証方式に，覗き見耐性を有する STDS 認証方式を採用し，録画攻撃への更なる耐性を有すべく，フェイクモードの導入も行った．本システムにより，覗き見攻撃及び 1 回の録画攻撃への耐性を有し，その有用性及びユーザビリティについて実験を通して確認した．これらにより，本システムをモバイル端末に用いることによって，覗き見攻撃及び録画攻撃による情報漏洩を防ぐことができる．

今後の課題を以下に述べる．

- 確率的誤認証への対策

Any Shift 機能を用いる際，確率的誤認証への対策案としてパスアイコン数を増やすことを提案したが，ユーザビリティの低下を招く原因になるため，最善策ではない．ユーザビリティを考慮した確率的誤認証への対策を講じる必要がある．

- 複数回の録画攻撃への耐性強化

現在のフェイクモードは，2 回以上の録画攻撃に対して無効になることから，改良を行う必要がある．具体的には，偽の入力回はパスアイコンを含まないなどのパスアイコンの重複を避ける対策や，端末の振動を利用した合図の改良が考えられる．

- セキュリティとユーザビリティとの両立を考慮した拡張

覗き見耐性を高めるために，1 回の認証画面に提示するアイコン数を増やすことによって，考え得るパスアイコンの組合せ数を増やすことは有用である．そのため，現在の 4×4 の認証画面から，9×9 など配置するアイコン数の増加や，増加を考慮したシフトの変更も考えられる．しかし，大規模化や複雑化はユーザビリティの低下に繋がるため，セキュリティとユーザビリティとの両立を考慮した拡張が求められる．

文　献

[1] “スマートフォン＆タブレットの業務利用に関するセキュリティガイドライン,” 日本スマートフォンセキュリティフォーラム（JSSEC），2012.

[2] S. Xiaoyuan, “A design and analysis of graphical password,” Computer Science Theses, Georgia State University, 2006.

[3] “生体認証導入・運用のためのガイドライン,” 独立行政法人情報処理推進機構，2007.

[4] A.H. Lashkari, S. Farmand, O.B. Zakaria, and R. Saleh, “Shoulder surfing attack in graphical password authentication,” Int. J. Computer Science and Information Security, vol.6, no.2, pp.145–154, 2009.

[5] 冨高　彩，“ATM 盗撮と建物物侵入罪・偽計業務妨害罪の成否,” 上智法学論集，vol.54,pp.135–149, 2011.

[6] 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,” 信学技報，vol.109，no.115，pp.21–26, 2009.

[7] SECUREMATRIX，株式会社シー・エス・イー，https://www.cseltd.co.jp/smx/ 参照 Jan.9, 2014.

[8] W.Z. Khan, M.Y. Aalsalem, and Y. Xiang, “A graphical password based system for small mobile devices,” Int. J. Computer Science Issue, vol.8, Issue 5, no.2, pp.145–154, 2011.

[9] N.H. Zakaria, D. Griffiths, S. Brostoff, and J. Yan, “Shoulder surfing defense for recall-based graphical passwords,” Proc. 7th Symposium on Usable Privacy and Security (SOUPS’11), pp.1–12, 2011.

[10] 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,” 情処学論，vol.49,no.9,pp.3038–3050, 2008.

[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方式,” 情処学論，vol.49,No.9,pp.3051–3061, 2008.

[12] 石塚正也，高田哲司，“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,” Computer Security Symposium 2013, pp.708–715, 2013.

[13] H. Sasamoto, N. Christin, and E. Hayashi, “Undercover: Authentication usable in front of prying eyes,” Proc. SIGCHI Conference on Human Factors in Com-

puting Systems (CHI'08), pp.183–192, 2008.
[14] A.D. Luca, E. von. Zezshcwitz, N.D.H. Ngyuen, M.-E. Maurer, E. Rubegni, M.P. Scipioni, and M. Langheinrich, "Back-of-Device Authentication on Smartphones," Proc. SIGCHI Conference on Human Factors in Computing Systems (CHI'13), pp.2389–2398, 2013.
[15] Y. Kita, F. Sugai, M. Park, and N. Okazaki, "Proposal and its evaluation of a shoulder-surfing attack resistant authentication method: Secret tap with double shift," Int. J. Cyber Security and Digital Forensics (IJCSDF), vol.2, no.1, pp.48–55, The Security of Digital Information and Wireless Communications (SDIWC), 2014.
[16] R. Biddle, S. Chiasson, and P.C.V. Oorschot, "Graphical passwords: Learning from the first twelve years," J. ACM Computing Surveys (CSUR), vol.44, Issue.4, no.4, pp.1–25, 2012.
[17] "NIST special publication 800-63-1 electronic authentication guideline," National Institute of Standards and Technology, 2011.

（平成 26 年 1 月 30 日受付，6 月 17 日再受付）

喜多　義弘

2004 宮崎大学工学部情報システム工学科卒．2010 同大大学院工学研究科システム工学専攻博士後期課程単位取得満期退学．2012 神奈川工科大学セキュリティ研究センター特別研究員．博士（工学）．ネットワークセキュリティ，認証等の研究に従事．情報処理学会会員．

岡崎　直宣　（正員）

1986 東北大学工学部通信工学科卒．1991 同大学大学院工学研究科電気及び通信工学専攻博士後期課程修了．同年，三菱電機株式会社入社．2002 宮崎大学工学部助教授．2007 同大学准教授を経て 2011 同教授．博士（工学）．通信プロトコル設計，ネットワーク管理，ネットワークセキュリティ，モバイルネットワーク等の研究に従事．情報処理学会，電気学会，IEEE 各会員．

西村　広光　（正員）

1995 信州大学情報工学科卒．1997 同大学大学院工学系研究科修士課程修了．2000 同大学大学院工学系研究科博士課程修了．同年，神奈川工科大学助手．2005 同大学専任講師，現在に至る．博士（工学）．画像処理，パターン認識，ヒューマンインタフェースの研究に従事．情報処理学会，ヒューマンインタフェース学会，画像電子学会，学生相談学会各会員．

鳥井　秀幸　（正員）

1995 筑波大学第三学群工学システム学類卒．2000 同大学院工学研究科知能機能工学専攻修了．同年，神奈川工科大学情報ネットワーク工学科助手，講師を経て，2008 同大学情報ネットワーク・コミュニケーション学科准教授，現在に至る．博士（工学）．系列設計及び移動体通信に関わる研究に従事．IEEE 会員．

岡本　剛　（正員）

2002 豊橋技術科学大学大学院工学研究科博士後期課程修了．同年，神奈川工科大学助手．2005 同大学講師，2010 同大学准教授となり，現在に至る．博士（工学）．コンピュータウイルスの検出や，侵入検出などコンピュータセキュリティの研究に従事．

朴　美娘　（正員）

1983 漢陽大学工学部電子工学科卒．同年，同大学工学部助手．1993 東北大学大学院工学研究科情報工学専攻博士後期課程修了．同年，同大学電気通信研究所助手．1994 三菱電機株式会社入社．2010 神奈川工科大学情報学部教授．博士（工学）．ネットワークセキュリティ，暗号プロトコル設計，認証等の研究に従事．情報処理学会，日本セキュリティ・マネジメント学会各会員．