様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　２９　年　　５　月　２９　日現在

機関番号：　３２７１４
研究種目：　基盤研究(C)（一般）
研究期間：　2014～2016
課題番号：　２６３３０１６４

研究課題名（和文）覗き見耐性とユーザビリティを有するモバイル端末向けユーザ認証方式

研究課題名（英文）User Authentication Method with Shoulder-surfing Resistance and High-usability for Mobile Terminal

研究代表者

岡崎　美蘭（Okazaki, Miran）

神奈川工科大学・情報学部・教授

研究者番号：００５４５１５５

交付決定額（研究期間全体）：（直接経費）　　2,900,000円

研究成果の概要（和文）：　モバイル端末を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．本研究では，覗き見耐性とユーザビリティを有するユーザ認証方式について検討した．そこで，「シフト」という独自の移動法則を用いてアイコンをタップするSTDS認証方式，従来のパスワード認証にパズルの要素を組み込み，パスワードを指定した位置に備えるパズル認証方式を提案した．さらに，ユーザが認証時に画面を見ないでポケットや鞄の中で画面をタップすることによって本人を確認できるリズム認証を提案した．また，各方式の実装を行い，覗き見耐性，ユーザビリティに関する評価を行った．

研究成果の概要（英文）：The existing mobile terminal authentication schemes not have the resistance of shoulder-surfing attack. We studied user authentication method with peeping resistance and usability. The user authentication method with peeping resistance is a problem of increasing the user's memory burden due to complication of the input method. Also, it is a problem that authentication information is extracted by record analysis by a video recording device such as a camera.
In this paper, we proposed and implemented several user authentication schemes with peeping tolerance and high usability. We proposed the STDS authentication method to tap the icon using our own movement rule "shift" and puzzle authentication method to prepare for password specified position. In addition, we suggested rhythm authentication that allows users to confirm their identity by tapping the screen in a pocket or bag. We implemented each method on Android terminal and evaluated about peeping resistance and usability.

研究分野：　情報セキュリティ

キーワード：　ユーザ認証　録画攻撃対策　アクセス制御

１．研究開始当初の背景

スマートフォンやタブレットなど，従来のモバイル PC よりもモビリティ性能が高く，多機能な端末などの登場により，画面処理や入力方法など，汎用的なコンピュータと同等な操作環境をモバイル端末上で実現することが可能となり，今後はこのような端末を用いたモバイルクラウドサービスが急速に伸びていくことが予想される．

モバイルクラウドサービスの導入は，設備投資コストの軽減のみならず，データ管理の容易さや必要に応じた柔軟なシステム構築ができる利便性をもたらす．すなわち，スマートフォンやタブレットなどの高機能端末の業務への導入(BYOD:Bring Your Own Device)により，営業活動や業務の効率化はもちろん，大規模な災害や事故発生時の事業継続計画(BCP:Business Continuty Plan)が実現可能になる．一方，スマートフォンなどのモバイル端末からクラウドサービスを利用する際には，情報漏えいなど様々なセキュリティ上の脅威が常に存在する．例えば，ユーザが PC やタブレットなど多様な端末経由で保存したデータをクラウド上で集約できることは，クラウド利用による大きなメリットとなる．しかし，スマートフォンやタブレットは PC に比べると紛失・盗難の危険性が高く，ボットウィルス感染などにより他者の支配下に置かれると，簡単にクラウドへのアクセス認証が突破され，他者によるクラウドへの不正アクセスやなりすましを可能にする端末として悪用される可能性が大きい．現在多くのモバイル端末には，PIN(Personal Identification Number) やパスワード，パターンなどを利用した画面ロックの解除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，覗き見耐性が実現されておらず，人の目にさらされた環境で画面ロックの解除認証を行うと他人に認証情報がばれてしまう可能性がある．そこで，モバイル端末の個人認証における覗き見の問題に対する様々な研究が国内外で行われている．しかし，これらの覗き見耐性を持つユーザ認証方式には，入力方法の複雑化によるユーザの記憶負担の増加や，カメラなどの録画機器による記録解析からの認証情報の抽出に対する対策などの課題が残されている．特に，録画機器による覗き見耐性を強化するためには，端末の裏側にセンサー等の外部装置を付けたり，ユーザ認証動作を複雑にする必要があり，ユーザが覚える認証情報を増やすことによりユーザビリティが大きく下がるという問題点がある．

２．研究の目的

本研究では，スマートフォンやタブレットなど，従来のモバイル PC よりもモビリティ性能が高く，多機能な端末を用いたモバイルクラウドサービスを利用する際のアクセス制御基盤技術の確立を目的とする．特に，モバイルクラウドサービスを利用するユーザが常に持ち歩くことができるモバイル端末側での情報漏えい対策に対応した，覗き見耐性を持つ個人認証方式の確立を目的とする．ここでの覗き見耐性というのは，人間の目と記憶による攻撃だけではなく，ビデオカメラなどの録画機器による記録解析からの攻撃に対しても耐性をもつことを目指す．さらに，本研究ではモバイル端末の画面上のアイコンをタップして操作するという扱いやすい入力方式によって高いユーザビリティを有し，年代・職種などを問わずに使いやすい方式の実用化を目指す．

３．研究の方法

(1)「録画攻撃への耐性を持つモバイル端末認証方式の提案」に取り組む．

覗き見による攻撃方法は大きく２つに分けることができる．１つは「他人が認証動作を直接覗き見る攻撃-覗き見攻撃」であり，もう１つは「ビデオカメラなどの録画機器によって記録し解析する攻撃-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持たせることがはるかに難しく，ユーザビリティも低下してしまう．そこでまず，覗き見攻撃だけでなく，録画攻撃への耐性も持つモバイル端末認証方式の提案に取り組む．

(2)「提案方式の実装とユーザビリティの検証実験」

画面ロックを搭載した Android OS 向けの端末に提案した認証方式を実装する．そして，５０名程度の被験者を対象として，比較的長期間端末を利用してもらった上で，認証方式に習熟した状態での様々な観点からのユーザビリティの評価や，高い精度での録画攻撃に対する評価実験を行う．また，アンケート調査により，使いやすさ，慣れやすさ，安心感などの効果について評価を行う．また，認証動作を実際に録画し，既存の解析手法を用いて録画映像から認証情報を解析する実験を行う．そして，解析後に絞られた認証情報のパターン数が暗証番号４桁と同等の強度を有するかどうかを評価する．

４．研究成果

(1) STDS 認証方式の提案と実装

本研究では，モバイル端末の仮面ロック解除パスワードとして，格子状に配置したアイコン群からパスワードアイコンを登録し，認証時には登録したパスワードアイコンと異なるアイコンをタップすることで，覗き見攻撃だけでなく，録画攻撃への耐性も持つことを目的とした認証方式を提案し実装した．

例えば，数多くのアイコンからランダムに 16 個選択し，4×4 の格子状に配置する．次に，4×4 のアイコン群を 2×2 の 4 個組(象限)のアイコン群に分ける．この中にはユーザが認証情報として予め登録したアイコン

図 1　STDS シフトの使用方法

(登録アイコン)も含んでいる．認証の入力には，認証の鍵として表示したアイコン(認証アイコン)をタップすることにより行う．
STDS 方式では，登録アイコンを含む象限から，「シフト」と呼ぶ独自の移動法則を用いて象限間または象限内を移動し，その移動先にあるアイコンを認証アイコンとする．シフトの対象が象限間の場合を象限間シフト，象限内の場合を象限内シフトとする（図 1)．
さらに，STDS 認証方式に録画攻撃への耐性を持たせるために，2 つの機能を導入した．1 つは Any Shift という，シフト値を固定せず，認証時にユーザが移動量を任意選択できる機能である．もう 1 つは Fake Mode という，認証時にシフト値での移動に関係のないアイコンを，ユーザが任意選択する機能である．これにより，認証動作を録画されても，攻撃者がシフト値を特定できないようにする．
また，提案手法が覗き見攻撃および録画攻撃への耐性を有しているかを評価するために，Android 端末上にアプリケーションとして実装し，50 人の被験者を対象に覗き見耐性の評価実験を行った．その結果，従来の PIN および Android Password Pattern は全員が認証情報を見破ったが，提案方式は全員とも認証情報を見破ることができなかった．これにより，提案方式は覗き見攻撃に耐性を有していることが言える．また，録画攻撃耐性の評価のため，Any Shift と Fake Mode を使用する場合の評価を行った．そこで，認証画面と認証動作の両方を録画されても特定されにくいが，複数の認証動作を録画された場合は，登録アイコンを特定されやすくなることが分かった．

(2) パズル型認証方式の提案と実装
本研究では，覗き見による認証情報の流出を防ぐと共にユーザビリティを向上させるため，従来のパスワード認証方式にパズルの要素を付加した．提案方式では，認証画面に 0 から 9 の数字と赤，青，緑，黄，黒，白のマスを 4×4 の四角形に配置し，認証画面に表示されているマスのいずれか 1 つをタッチし，そのまま上下左右又は斜めへ自由にスライドさせて認証を行う（図２）．
ここで，ユーザがパスワードとして登録するものは 4×4 の四角形上での位置と 4 個のマスである．認証開始時に 0 から 9 の数字と赤，青，緑，黄，黒，白のマスがランダムに表示されるので，ユーザは登録したパスワードの位置を確認する．その後，認証画面に表示されているマスを 1 つ選択し，そのマスをタッチした後にスライドをさせて，上下左右斜めの数字と入れ替えながら，登録した位置とパスワードを合わせる．
提案方式を Android 端末に実装し，覗き見耐性および録画耐性の評価を行った．また，ユーザビリティに対する評価を行うためにアンケートを実施した．その結果，従来の STDS 方式より認証時間も短くなり，使いやすいという意見があった．

図２　パズル認証画面

(3) 機械学習を利用したリズム認証方式の提案と評価
リズム認証とは，ユーザが楽曲などに合わせてキーボード入力や画面タップをし，連続した入力データの時間差を認証情報として用いる認証方法であり，ユーザの行動的特徴を活かしたバイオメトリクス認証の 1 つである．ユーザは自身のイメージした曲のメロディに合わせてキーボード入力や画面タップし，キー入力時間やタップ時間などの特徴量を認証情報としている．認証情報の入力は，入力装置を操作することにより，入力することができるので，とても容易に認証を行うことができる．また，認証を行う際に，手で隠す，鞄やポケットの中で認証を行うことにより，覗き見，録画耐性を得ることも可能である．
本研究では，ユーザが入力したタップ動作からユーザを識別できる特徴量（指の識別，指間の距離，指圧など）を定義し，機械学習の一つである自己組織化マップ（SOM）を利

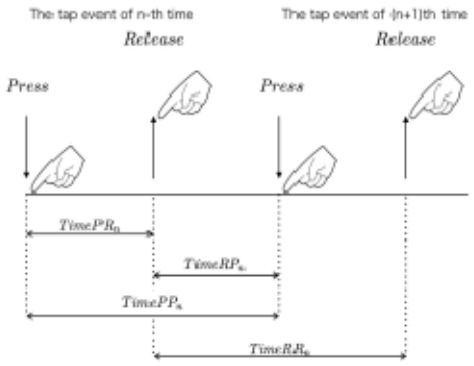

図３　タップのイベント時間

用して，認証を行った．認証情報の登録では，ユーザが端末上でタップした認証情報がサーバへ送信され，サーバで SOM を作成する．サーバは作成した SOM 情報を端末へ送信することで登録が完了する．サーバで SOM を作成する理由として 2 つ挙げられる．まず，SOM 作成の膨大な処理への対応である．SOM は数千～数万のノードによって構成されて，各ノードにつき探索および学習を数万回行うため，処理が膨大である．その処理をモバイル端末上で行うには負荷が大きく，端末の動作が不安定になることが考えられるため，処理能力が高いサーバで SOM を作成する．次に，端末間での認証情報の共有によるユーザの負荷軽減がある．複数台の端末を有するユーザが各端末上で本人認証を行う際，ユーザ本人の既存 SOM を端末へ送信して認証情報を共有することにより，各端末で認証情報の新規登録や変更を行う必要がなく，普段通りに認証を行うことができる．これによりユーザは，新たに認証情報を覚えたり，複数の認証情報を管理したりする必要がない．

認証時のユーザは，端末上をタップしてリズムを入力し，その入力情報と SOM とを照合することで認証の成否を判断する．このように認証操作が画面をタップするだけなので，利便性が高く記憶負荷が小さいと考えられる．

また，提案方式の有用性を評価するために，被験者 20 名を対象にモバイル端末のタッチスクリーン上で童謡「猫踏んじゃった」の冒頭 4 小節をタップしてもらって認証精度を求めたが，良い結果が得られなかった．理由としては，SOM 作成にサーバが必要となる問題，利用者が少ないタップ数でリズム認証を行った場合は，得られる特徴量が減り，識別率が低下すること考えられる．

そこで，リズム認証方式の実用化に向け，端末内だけで認証が行えるようになるシステムを検討した．そこで，計算処理が高速で，特徴量の重要度が計算できる RandomForest を利用して，被験者 24 名の方に，童謡「猫踏んじゃった」の冒頭 4 小節の 19 タップを 20 回入力してもらって，評価を行った．その結果，RandomForest の算出結果を元に，使用する特徴量を選択することにより識別率を上げることに成功し，特徴量を選択する有用性を確認した．

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計６件）
① Y. Kita, M. Park, and N. Okazaki ″Proposal of an Authentication Method using Two Types of Machine Learning and Mouse Operation Trajectory,″ The First International Symposium on BioComplexity 2016 (ISAROB, 2016), pp.346-349, 2016/1.
② Y. Kita, M. Park, and N. Okazaki ″Proposal of Rhythm Authentication Method using Users Classification by Self-Organizing Map,″ International Conference on Network-Based Information Systems(NBiS2015), pp665-668, 2015.
③Y. Kita, K. Aburada, M. Park, and N. Okazaki, ″Proposal of a Puzzle Authentication Method with Shoulder-surfing Attack Resistance and High-usability,″ IEICE ComEX, Vol.4, No.3, pp.95-98, 2015.
④喜多 義弘, 岡崎 直宣, 朴 美娘, "覗き見耐性を持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 D, Vol.J97-D, No.12, pp.1770-1784, 2014.

〔学会発表〕（計１２件）
①堀 孝浩, 喜多 義弘, 朴 美娘, 岡崎 直宣, ″Random Forest による実用化に向けたリズム認証の実験評価,″ 2017 Symposium on Cryptography and Information Security(SCIS2017), 1B2-1, 2017.01
②堀 孝浩, 喜多 義弘, 豊田 健太郎, 朴 美娘, 岡崎 直宣, ″テンポ感を特徴量に取り入れたリズム認証の評価,″ 情報処理学会第 78 回全国大会, 1W-3, 20160310
③日隈光基, 喜多義弘,朴美娘, 岡崎直宣 “パズル型認証方式の録画攻撃耐性の一検討”, IPSJ 火の国シンポジウム 2016, 20160302
④増田 裕仁, 喜多 義弘, 朴 美娘, 岡崎 直宣, ″タッチスクリーンを利用した覗き見耐性を持つパズル型認証方式の提案,″ 情報処理学会マルチメディア，分散，協調とモバイルシンポジウム（DICOMO2014）論文集, pp.1005-1010, July 2014.
⑤喜多 義弘, 神里 麗葉, 朴 美娘, 岡崎 直宣, ″自己組織化マップを利用したリズム認証方式とその認証精度に関する考察,″ 情報処理学会マルチメディア，分散，協調とモバイルシンポジウム（DICOMO2014）論文集, pp.1011-1018, July 2014.
⑥喜多 義弘, 朴 美娘, 岡崎 直宣：パズル

型認証方式の録画攻撃耐性に関する考察，バイオメトリクス（BioX）研究報告，2014.06

〔図書〕（計　　件）

〔産業財産権〕

○出願状況（計３件）

名称：個人認証用プログラム
発明者：岡崎　美蘭、　岡崎　直宣
権利者：同上
種類：特許
番号：特願 2015-183574
出願年月日：2015/9/17
国内外の別：国内

名称：個人認証装置及びプログラム
発明者：岡崎　美蘭、　岡崎　直宣
権利者：同上
種類：特許
番号：特願 2015-165962
出願年月日：2015/8/25
国内外の別：国内

名称：個人認証装置及びプログラム
発明者：岡崎　美蘭、　飯岡　勇人
権利者：同上
種類：特許
番号：2014-046134
出願年月日：2014/3/10
国内外の別：国内

○取得状況（計　　件）

名称：
発明者：
権利者：
種類：
番号：
取得年月日：
国内外の別：

〔その他〕
ホームページ等
http://okalab-kait.jp/

６．研究組織
(1)研究代表者
岡崎 美蘭（朴 美娘）(OKAZAKI, Miran)
神奈川工科大学・情報学部・教授
研究者番号：００５４５１５５

(2)研究分担者
岡崎 直宣 (OKAZAKI, Naonobu)
宮崎大学・工学部・教授
研究者番号：９０３４７０４７

(3)連携研究者

(4)研究協力者
喜多 義弘 (Kita Yoshihiro)