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　３０　年　　６　月　１１　日現在

機関番号：　１２６１２
研究種目：　挑戦的萌芽研究
研究期間：　2014～2017
課題番号：　２６５４００５５

研究課題名（和文）利用状況に応じた携帯端末向け個人認証の研究

研究課題名（英文）Research on user authentication systems for mobile terminals that could counter the threats depending on usage situations

研究代表者

高田　哲司（Takada, Tetsuji）

電気通信大学・大学院情報理工学研究科・准教授

研究者番号：７０４１５７０１

交付決定額（研究期間全体）：（直接経費）　　2,800,000円

研究成果の概要（和文）：携帯端末は様々な状況下で利用されるため，想定される脅威も様々である．よって，そのセキュリティ機能である個人認証も状況や脅威に応じて柔軟であるべきである．
本研究では，この目的に資する個人認証の実現に取り組み，以下の成果をあげた．
1）ユーザの秘密情報を変更せずに，提供しうる安全性を柔軟に変更可能な画像認証 2）ライフログデータを想定し「特定の規則」を用いて秘密情報を定義する時限式パスワードによる個人認証 3）振動や圧力入力の応用により，第三者に認証行為を覗き見されたとしても入力した秘密情報の窃取が困難な個人認証手法 4）ユーザ自身により個人認証の利用可能性を制御する枠組みの提案

研究成果の概要（英文）：Since a mobile terminal is always carried and used in various situations, assumed threats in a use of the mobile terminal are also changed depending on the context. Therefore, a user authentication in mobile terminals, as a basic security function of them, should be flexible according to the situations and threats.
In this research, We worked on developing user authentication systems that could contribute to the above goal. The research results are as follows.
1) Image-based user authentication system that can flexibly configure a providable security level without changing a user credential, 2) a user authentication method with a time-limited password that is defined using a "time-period based rule" for life-log based data, 3) credential input schemes that could make it hard to steal a credential data by a shoulder surfing attack by using vibration information and pressure input, 4) Proposal a scheme of an availability control of a user authentication by users themselves.

研究分野：　Usable Security, User authentication

キーワード：　User authentication　Usable security　Mobile system　Shoulder surfing attack

１．研究開始当初の背景

スマートフォンに代表される携帯端末は，利用者が機器を占有利用する利用形態が一般的である．それにともない，利用者の電子メール，メッセージサービスや通話の履歴，各種サービスの利用権限や電子現金など，利用者の個人情報や機微情報を保持する機器となっている．したがって，携帯端末のセキュリティ対策は必要不可欠であり，なかでも個人認証（=端末ロック）は最も基本的なセキュリティ対策である．

しかし，携帯端末における個人認証には以下の２つの問題がある．

a) 個人認証の利用形態が all or nothing の２つしかない．つまり個人認証を「常に利用する」か「全く利用しない」かのどちらかの利用形態しか認めていない．

b) パスワードや暗証番号など既存の個人認証手法を携帯端末に適用しているだけで，携帯端末での利用状況における脅威を考慮していない．

携帯端末は，常時携帯されるため様々な場面で利用される．その様々な利用状況において，常に１つの個人認証手法でセキュリティを担保することには「ムダ」があると考えることができる．ここでいう「ムダ」とは，必要以上の安全性を担保しうる個人認証の利用をユーザに強いている，という意味である．利用状況によっては，想定される脅威レベルが低くなることが想定される．例えば，自宅で携帯端末を利用する場合は，外出先で利用する場合と比較してその脅威レベルは低くなると考えられる．このような場合，その脅威に対抗できる個人認証手法も簡易なもので良いということになる．このような状況がありうるにもかかわらず，現在は既存の個人認証手法を画一的に適用している．これは過度の負担を携帯端末ユーザに強いていることになる．この問題ゆえにユーザは個人認証を敬遠し，「個人認証(=端末ロック)は利用しない」という望ましくない状況を生んでいると言える．したがって，利用状況に応じた脅威を数値化し，その脅威に応じて必要な安全性を担保しうる個人認証手法を携帯端末ユーザに提示することが望ましいと考えた．

携帯端末で個人認証を行う上で取り上げるべき別の問題に「覗き見」がある．正規利用者の個人認証行為を第三者が「覗き見」し，入力した暗証番号やパスワードを窃取する．その後，窃取した暗証番号やパスワードを用いて正規利用者になりすまし，悪事を行うという問題である．前述の通り，携帯端末が保持または蓄積している情報は重要な情報が多く，携帯端末を第三者に悪用された場合，それによって発生しうる被害・損害が大きくなることは想像に難くない．それゆえ，本脅威に対する対策の確立は携帯端末における個人認証において重要な課題である．

したがって，これらの問題に対応しうる新たな個人認証を携帯端末向けに実現する必要がある．

２．研究の目的

上記の問題をふまえ，本研究では「利用状況に応じた携帯端末のための個人認証」を研究目的とし，以下の３つの研究課題を設定した．

i) 携帯端末の利用状況に応じて適切な認証手法を複数の認証手法から選択/提供しうる situation-aware な個人認証基盤の実現

ii) パスワードや暗証番号など「特定の情報」を 秘密情報（credential）にするかわりに，「特定の規則」を秘密とする life-log を応用した個人認証の実現

iii) 悪意ある第三者によって認証行為を「覗き見」されることにより個人認証の「秘密情報」が窃取され，悪用されることを困難にする手法の実現．

1.「研究開始当初の背景」の章で記述した２つの問題のうち問題 a）に対応する課題が上記の課題 i）であり，問題 b)に対応するのが課題 ii, iii）となっている．

３．研究の方法

課題 i）この課題では，具体的に２つの仕組みを実現する必要がある．１つは状況認識により利用状況を推定し，その状況における脅威を数値化する仕組みであり，もう１つは数値化された脅威に応じて適切な個人認証手法を提示する仕組みである．前者はスマートフォンに搭載されている各種センサー情報を用いてユーザが個人認証を実施するシーンの状況を収集し，それらを複数の状況に集約する．これにより作成された各利用状況における想定脅威をユーザ評価に基づき数値化する．後者の仕組みは，ユーザに提供しうる個人認証手法を複数用意し，それらに対してそれぞれの手法が担保しうる安全性を数値化（X_i）して付与しておく．一方，前者の仕組みによって利用状況にて想定される脅威に対抗するために必要となる数値（Y）と各認証手法が提供しうる安全性の指標の数値群（X_i）を比較し，Y を超える X_i のうち最小の値を持つ個人認証手法をユーザに提示する．これにより，利用状況における脅威に対して安

全性を担保するのに必要十分な個人認証手法を利用状況に応じてユーザに提供することが可能となる．

課題 ii）個人認証における秘密情報（Credential）を「特定の値」から「特定の規則」にする．このアイデアは life-log に代表される「情報流」の存在を想定している．具体的には携帯端末に蓄積される移動履歴，Suica による購買履歴，そして Twitter をはじめとする SNS への投稿情報などである．これら情報流に存在するデータの一部をユーザが決定する「規則」によって切り取り，それを個人認証の「秘密情報」として利用する．この方法により「知識ベースの時限式パスワードによる個人認証」を実現することが可能になると考えた．時限式とは，いわゆるワンタイムパスワードと同様のものを意図しているが，その利用可能時間と定義方法が異なる．ワンタイムパスワードは，長くても数分程度しか生成されたパスワードを利用することができず，またその利用可能時間は個人認証システムが規定している．これに対し，提案する時限式パスワードは，情報源の更新頻度とユーザが決定する「規則」の定義によって，秘密情報の利用可能時間が決定される．定義次第では既存のワンタイムパスワードより利用時間を長くしつつ，それでも時間経過とともにパスワードが自動的に更新される秘密情報を使用する個人認証手法となる．これにより，覗き見されたとしてもそのパスワードを悪用可能な時間は制限され，覗き見の脅威に対する対策になりうると考えた．これは計算機ではなく，常時携帯して利用される携帯電話ならの特徴を応用した手法でもある．

課題 iii）個人認証に対する「覗き見」の脅威に対抗するための手法を考案する．個人認証システムは，「利用者，秘密情報，入力手法」の三位一体であると我々は捉え．本研究ではこの中の「入力手法」に着目した．覗き見による秘密情報の窃取が成立する理由は，視覚的表示に依存した入力方法に原因があると考えたからである．またもう１つの目標として，既存の個人認証にも適用可能な手法であることを目標とした．既存の覗き見対策手法は，残念ながら既存の個人認証手法とは異なる入力手法として実装されており，既存の個人認証を改良するという観点で望ましいとは言いがたいからである．

４．研究成果

課題 i）本課題については，当初の課題設定に対する直接的な研究成果を導き出すことができなかった．最大の問題は，現在のスマートフォンに搭載されているセンサー情報で個人認証の利用状況に関する状況推定に資するデータが得られないという点にある．試行錯誤したものの，時空間情報だけがその目的に資するが，それは既存の研究でも模索されており，新しい知見を生み出すには至らなかった．しかし「利用状況に応じて適切な個人認証を提示する」という目的について議論・考察をした結果，その目的に合致しうる別の成果を生み出すことができた．その成果とは以下の２つである．

I） 秘密情報を変更せずに個人認証が提供する安全性を柔軟に変更可能な画像認証

再認式と呼ばれる画像認証が提案されている．この手法では，１０枚の画像群の中から秘密情報として事前に決定した画像１枚を選択する．この操作を複数回繰り返し，全ての回答が正解であれば正規利用者として認証する手法である．この画像認証では，認証画面に秘密情報ではない画像も表示する．これを”おとり画像”と呼ぶが，このおとり画像の枚数を増やすことにより，理論的な安全性を変更することができる．つまり”１０枚から１枚を選択する”から”１００枚から１枚を選択する”とすることでランダムに選択した回答が正解である確率は１０分の１となり安全性を向上させることが可能になる．しかし，回答選択肢が増えるとユーザの操作負担，すなわち正解画像を探索するデータ数が増えるため，認証時間が長くなるという問題が生じる．そこで本研究では，認証画面の画像群における正解画像の配置を工夫することにより，その負担軽減を可能にする手法を提案した．それは画像群をグリッド表示した場合に，グリッド内の小部分領域内に全ての正解画像を配置する方法である．これにより正規利用者が正解画像を探索する領域を縮小することが可能になり，結果として認証時間の短縮につなげられると考えた．

本研究ではこのアイデアに基づき，１００枚の画像から４枚の正解画像を選択する再認式画像認証のプロトタイプを実装した．プロトタイプでは４列×２５行の画像グリッドを生成し，正解画像はそのグリッド内の任意の５行内に配置する方法とした．この手法を，正解画像をグリッド領域内全領域の任意の場所に配置する手法と比較する評価実験を行なった．被験者は，２０歳男性９名である．その結果，認証成功率はどちらも１００％となり両手法の間で差が生じなかったが，認証時間は限定領域に集中配置した場合が平均で１４．６秒だっ

たのに対し，グリッド全領域にランダムに配置した場合は２８．０秒とおよそ倍の時間がかかる結果となった．また両システムに対する正解画像の探索負荷に対する主観的評価も，集中配置が３．５６だったのに対し，全領域へのランダム配置は６．３３という結果となった（７段階評価：数値が大きいほど負担が大きいことを示す）．

当然だが，今回の評価実験で用いた２つの手法では，提供しうる安全性が異なる．ただし重要な点は，おとり画像の枚数を変更するだけで，正規利用者が記憶保持する秘密状況にはまったく影響を与えずに提供しうる安全性を変更できるという点である．なぜならば，利用状況に応じて提供する個人認証手法が増えた場合，結果的にユーザは複数の秘密情報を記憶保持しなければならなくなり，それはユーザに負担を強いることになるからである．また，安全性強化のためにおとり画像を増やすことは１つの方法として考えつくが，画像枚数が増えた場合に，ユーザの正解画像探索負担を軽減しうる手法を考案したという点も重要だと考える．安全性強化のためにユーザに負担を強いることは簡単だが，それにより個人認証を使わないということになっては意味がない．本提案は，利用状況に応じた個人認証の１手法として有益な知見を示したと考える．

II) 利用者の自己制御により第三者による個人認証をつうじた”なりすまし”を困難にするシステム．

利用状況に応じてシステムが判断し，必要十分な個人認証を提供する基盤を実現するのが目的であったが，これとは真逆の方法について検討を行い，提案したシステムが”authentication shutter”である．このアイデアは「個人認証をユーザが自分で制御する」というものである．現状の個人認証が，なぜ”なりすまし”に悪用されるのか？を検討した結果，個人認証システムが誰でも常時利用可能だからである，という着眼点に至った．これに対し，あるユーザアカウントでの個人認証は，ある条件を満たした場合でしか行うことができない，という仕組みが実現できれば，第三者による悪用を困難化し，かつアカウント悪用の事実を正規利用者が知らないままになるということを防ぐことが可能になると考えた．これは物理世界における「車庫のシャッター」と同様である．車庫のオーナーは，車庫に車を入れるときにシャッターを自分で開けて車を入れ，そしてシャッターを閉める．外出時には，シャッターを開けて車を車庫から出し，そのあと車庫のシャッターを閉める．これにより，第三者がオーナに無断でその車庫に車をとめることを防いでいる．これと同じ仕組みを個人認証に導入すれば，オンライン攻撃を困難化することが原理的に可能となる．

このアイデアについて，概念整理を行うとともに，プロトタイプシステムの設計を示して，その実現可能性について議論した．これも携帯電話を常時携帯しているということが重要になっている．

課題 ii）本課題に対し，Twitter を life-log データとみなし，時間帯を用いた規則に基づく秘密情報を想定した個人認証を実現した．今回，個人認証の秘密情報を規定する規則としては”時間帯”（time-slot）を用いた．その理由は life-log に基づくデータの多くは属性情報として時刻情報を持つからである．時間帯の決定方法としては Span と Period の２種類を提案した．

Span は現在時刻を基準として過去の一定期間を規則とするものである．例としては「今日より 30 日前から 25 日前まで」という具合である．一方，Period は時間に関する周期情報を規則とするものである．例としては「先週火曜日の１９時台」という具合である．この規則定義と対象となる life-log データの生成状況によっては，該当するデータが複数になることもありうる．この場合，個人認証の秘密情報は複数の正解が存在することになるが，そのうちの１つを個人認証における正解回答とした．この秘密情報を用い，11 個の選択肢の中から正解となる Tweet を回答することで個人認証を行うシステムを携帯端末向けアプリケーションとして実装した．

このアプリケーションを用いて被験者実験を行なった．その結果，認証成功率は Span で４０～７０％，Period で１０～３５％となった．また秘密情報設定直後であっても認証成功率が５０％に届かないという結果になった．一方，認証時間も，Span で１０～６５秒，Period で１０～９０秒となり，利用可能性に疑問が残る結果となった．これらの利用可能性に関する問題は，規則から秘密情報を導出する処理に原因がある．規則自体はユーザが記憶しているとしても，その規則から現時点で何が正しい秘密情報なのかを導出する必要がある．これもユーザの記憶に依存しているのだが，Tweet からその生成日付・曜日・時刻を思い出すのは困難だということが今回の結果を招いたと言える．Tweet を対象とした規則ベースの個人認証についてはこの点をふまえ，改良方法を模索する必要がある．また Twitter のデータに限定せず，他の情報流データに対する規則ベースの個人認証についても引き続き検討を行う．

課題 iii）本課題に対しては，２つの研究成果をあげた。

１つは Circle Chameleon Cursor(CCC)と呼ぶシステムである。暗証番号による個人認証を対象とし、覗き見に対する安全性を担保する方法として「視覚情報+振動情報」を利用し，認証システムからユーザへ秘密情報の入力に必要な情報を伝達する仕組みを採用した．「暗証番号でドアを開閉する金庫」を例に説明する。金庫の“数値入力ダイヤル”は、暗証番号を入力する”位置”がダイヤルの上方に固定されており，視覚的にも認識可能である．これは正規利用者も覗き見をする攻撃者も同じ条件であり、これこそが覗き見攻撃を成立させている原因である．そこで本研究では、この数値入力位置を視覚情報だけで提示せず、視覚と振動の組み合わせでユーザに提示する．振動情報の利用により，視覚だけでは捉えられない情報が加わることになる．これにより，覗き見をしても回答入力に必要な情報が得られないため，結果として覗き見攻撃を困難にする．

CCC のもう１つの特徴は,カメラ等で個人認証の入力操作シーン（操作+画面表示）を録画したとしても、入力値の特定を困難にしている点である．先行研究の多くは、人間による覗き見には安全であるが，カメラで個人認証行為を録画された場合には、入力値を特定されてしまう．それは，視覚情報に依拠した回答入力手法だからである．カメラで録画された場合，画面の表示内容と操作内容が１００％記録され，かつあとで何度でも再生できることになる．したがって，入力方法を複雑にしてもカメラ録画による覗き見の場合，それは無意味となる．また認証行為の録画回数が 2〜3 回程度であれば、一定の安全性を担保できる手法も提案されているが、無限回の録画でも入力値の特定が困難な手法は少ない．本手法は、数値を入力する位置を数値入力のたびに CCC 側がランダムに数値入力位置を決定するため，振動情報が攻撃者に漏洩しない限り，カメラで認証行為を多数回録画したとしても、入力値の特定が困難な個人認証手法となっている．

なお４桁の暗証番号を想定し，被験者による CCC の評価実験を行った結果，以下の結果を得た．

- 操作ミスは約１０％ほど発生した．その原因の多くは数値入力位置の誤認識であった
- 入力操作時間は、４０秒前後であった．視覚＋振動情報による入力位置の取得に慣れていないことが要因であった．
- 攻撃実験の結果、４桁暗証番号のうち２桁以上特定できた被験者はいなかった．また１桁の特定に成功した被験者のうち，自信を持ってそれを特定したという被験者は１人もいなかった．

これらの結果から，安全性についての懸念はないものの，利用可能性については改善の余地がある．この課題を改善するための仕組みを考案・実現するのは今後の課題である．

もう１つのシステムは、携帯端末の圧力センサーを利用した個人認証手法である。圧力入力も視覚情報として捉えることが難しい．それゆえに覗き見に対する対抗策となりうる．単に携帯端末を加圧しているか否かであれば指の状況を観察することで視覚的に判定することは可能である．これに対して本研究では，複数の値（多値）の入力を想定した入力手法が可能であれば，視覚情報からの特定は困難となり覗き見対策になりうると考えた．ここで多値の入力値として４，６，８，１０段階の４種を想定し、現状の圧力値を視覚的にフィードバックした状態でユーザがどの程度，多値の離散値を入力可能か検証を試みた．その結果、４値であれば７８％，１０値でも５４％の成功率になることを被験者５名による被験者実験で明らかにした．この結果を，我々は好意的に捉えており，覗き見対策に活用可能な入力手法であるとして考えている．しかし、それと同時に入力値の決定方法に課題が残されていることも明らかになった．このため、本研究期間内で個人認証手法に本入力手法を適用したプロトタイプを実装し、評価を行うまでには至らなかった．これについては今後の課題である．

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　２　件）

（１）森康洋，高田哲司：”秘密情報を変更せずに提供しうる安全性を柔軟に変更可能な再認式画像認証の提案”, 情報処理学会論文誌, Vol.57, No.12, pp.2641-2653, 査読有, 2016.

（２）石塚正也，高田哲司：”CCC: 携帯端末での暗証番号認証における振動機能を応用した覗き見攻撃対策手法”, 情報処理学会論文誌, Vol.56, No.9, pp.1877-1888, 査読有, 2015.

〔学会発表〕（計　１０　件）

（１） Tetsuji Takada, “Authentication Shutter: Alternative Countermeasure against Password Reuse Attack by Availability Control”, 12th Int’l Workshop on Frontiers in Availability, Reliability and

Security (FARES 2017), 査読有, August 2017.

（２）荻野貴大, 高田哲司: “携帯端末における画面押し込み圧力を用いた多値離散値入力の可能性検証”, インタラクション 2017, March 2017.

（３）高田哲司, 森康洋: “１つの秘密情報で複数の安全性を提供しうる個人認証”, コンピュータセキュリティシンポジウム 2016 (CSS 2016), October 2016.

（４）荻野貴大: “圧力を利用した個人認証の提案”, コンピュータセキュリティシンポジウム 2016 (CSS 2016), October 2016.

（５）森康洋, 高田哲司: “回答候補画像の追加と正解画像の集中配置による再認式画像認証の安全性向上と操作負担抑制”, コンピュータセキュリティシンポジウム 2015 (CSS 2015), October 2015.

（６）Tetsuji Takada, Masaya Ishizuka, “Chameleon Dial: Repeated Camera-recording Attack Resilient PIN input scheme”, ACM Int'l Joint Conf. on Pervasive and Ubiquitous Computing (UbiComp 2015), 査読有, September 2015.

（７）森康洋, 高田哲司: “スクロールとスライド操作による携帯端末向け個人認証”, インタラクション 2015, March 2015.

（８）高浪悟, 高田哲司: “個人認証のパーソナライズ化を目指した規則ベース個人認証の提案”, コンピュータセキュリティシンポジウム 2014 (CSS 2014), October 2014.

（９）森康洋, 高田哲司: “選択と並べ替えによる個人認証の提案”, コンピュータセキュリティシンポジウム (CSS 2014), October 2014.

（１０）高田哲司: “Authentication Shutter: 個人認証における攻撃を遮断可能にする対策の提案”, コンピュータセキュリティシンポジウム 2014 (CSS 2014), October 2014.

〔その他〕
ホームページ等
http://www.az.inf.uec.ac.jp/

６．研究組織
(1)研究代表者
高田　哲司（TAKADA Tetsuji）
電気通信大学・大学院情報理工学研究科・准教授
研究者番号：70415701