情報処理学会論文誌 Vol. 49 No. 9 3051–3061 (Sep. 2008)

fakePointer：映像記録による覗き見攻撃にも安全な認証手法

高 田 哲 司[†1]

本論文では，ビデオ撮影による覗き見攻撃に対しても安全性を確保可能にする認証手法 “fakePointer” について述べる．これまでの覗き見攻撃はその実行主体が人間であった．しかし近年ではビデオカメラにより認証行為を撮影し，その映像記録から秘密情報を解析し，収集する手法が用いられる傾向にあり，その手法による事件も実際に発生している．しかし，そうした脅威に対して有効な技術的対策手法は数少なく，またそれらの手法の多くは，現状の脅威に対して部分的な安全性のみを提供するにとどまるか，安全性は向上するものの，ユーザによる実行可能性が低い手法であったりする．そこで本論文では，現状の脅威を基に覗き見攻撃において想定すべき脅威を整理し，その脅威に対しても安全性を確保しうる手法として fakePointer を提案した．fakePointer は，認証行為の映像記録があったとしてもユーザの入力値を特定困難にする入力インタフェースと，認証のたびにランダムに生成される回答選択情報を利用した回答入力方法のランダム化により，現状で想定される覗き見攻撃の脅威に対しても一定の安全性を確保しうる認証手法となっている．

fakePointer: A User Authentication Scheme that Makes Peeping Attack with a Video Camera Hard

Tetsuji Takada[†1]

I propose a novel user authentication scheme called “fakePointer”. The system makes peeping attack with a video camera hard on a user authentication. A peeping attack is one of threats for a user authentication. An attack looks into a target authentication activity from a behind and thieves secret information of the target. In these days, moreover, a method of the attack has changed to recording an authentication activity as a movie by a video camera. It also changed supposed threats of the attack. In this paper, I reconsider about threats of the peeping attack in a latest attack method and make clear a necessary requirement for building a secure authentication. One of the requirement is that it is hard for an attacker to identify user input from a video record of victim’s authentication activity. The other is that input method of secret must be randomized in each authentication action. I realize a user authentication scheme as a fakePointer that meets with above requirements.

1. はじめに

認証にはいくつかの攻撃手法が存在するが，その 1 つに「覗き見攻撃[⋆1]」がある．この攻撃は，正規ユーザの認証行為を覗き見ることで暗証番号やパスワード（以降，秘密情報と総称する）を不正に取得する攻撃手法である．近年この攻撃は，その実行主体が人間からビデオカメラを使った手法に変わりつつある．つまりビデオカメラを使用して，認証画面と操作盤を撮影し，後でその映像記録から秘密情報を解析/取得する方法である．この手法を利用した事件は現実にも発生しており，日本でもいくつかの銀行 ATM で事件になっている[1)–4)]．

この攻撃手法に対する根本的な対策は，第三者に覗き見られることのない環境で認証を行うことであり，認証を行う “場所” が兼ね備えるべき条件であるといえる．しかしこの実現は現実的に困難であると考える．また近年のモバイル/ユビキタス環境の普及にともない，その状況は今後ますます望ましくない方向へ進んでいくと推測される．生活空間の様々なところにカメラが設置され，意図せず認証行為を撮影されたり，サービスの性格上，第三者のいる中で認証をしなければならない場面も起こりうると考えられるからである．したがって，認証行為を「覗き見困難にする」対策も必要だが，それとあわせて「覗き見られても一定の安全性を確保可能」にする対策も必要であるといえる．

そこで本論文では，覗き見攻撃に対する安全性を確保しうる認証手法 “fakePointer” を提案する．fakePointer は，攻撃者がビデオカメラを用いて認証行為を録画するという脅威を想定し，その条件下でも攻撃者による秘密情報の特定を困難にする認証手法である．ユーザは認証時に使い捨ての “回答選択情報” を取得し，その情報を用いて自身の秘密情報を入力する．認証画面は 2 層構造の表示になっており，ビデオで認証行為を撮影してもユーザが入力した回答値が特定困難な仕組みとなっている．また回答選択情報は認証のたびにランダムに生成されるため，その認証行為で使用した回答選択情報を取得しない限り，攻撃者は同一ユーザの認証行為の映像記録を複数取得したとしても秘密情報の特定は困難な仕組みとなっている．

†1 産業技術総合研究所
National Institute of Advanced Industrial Science and Technology
⋆1 Shoulder Surfing/Shoulder Hacking/Observation Attack/Peeping Attack とも呼ばれる．

以降本論文では，2 章で覗き見攻撃における現状の脅威を再考し，想定すべき脅威を明確にする．3 章では覗き見攻撃対策に関する関連研究について述べ，4 章では，fakePointer の仕組みと認証方法について説明する．最後に 5 章では，fakePointer の安全性と利便性に関する考察を行う．

2. 覗き見攻撃による脅威

覗き見攻撃とは，第三者が認証行為を覗き見ることで対象ユーザの秘密情報を奪取する攻撃手法である．従来は人間がこの攻撃を行っていたが，最近では人間が行うかわりにビデオカメラで認証行為を撮影する手法が用いられるようになり，現実にその手法による事件も発生している[1)–4)]．この攻撃方法の変化は，覗き見攻撃による脅威の想定が大きく変わることを意味する．従来までの覗き見攻撃は攻撃主体が人間であるため，記憶力と処理能力に限界があるという前提で対策を検討していた．しかしビデオ撮影による攻撃方法の出現により，それらの限界がなくなることになる．つまり認証行為が映像記録化されるため記憶能力の限界がなくなるとともに，映像記録を基に事後にあらゆる可能性を配慮した解析が可能となるため処理能力の限界もなくなることになる．

またさらに悪いことに，認証行為を撮影するカメラが攻撃者に設置されてから，その設置に気がついて撤去するまでの期間によっては，攻撃者は同一ユーザの認証記録を複数個取得するという状況も発生しうる．したがって覗き見攻撃への対策は，今後以下の 2 点を脅威として想定すべきであると考える．

(1)　攻撃者は認証時の画面表示と操作に関する映像記録を持っている．
(2)　攻撃者は同一ユーザの認証行為に関する映像記録を複数個持っている．

これらの想定脅威は，まれに発生するケースでもなく，また最悪のケースを想定したものでもない．むしろ，モバイル/ユビキタス環境の普及にともない，今後は日常的に発生しうる脅威と考える．ユビキタス環境実現のためや監視目的のために設置されたカメラが，悪意の有無を問わず，認証行為を撮影してしまう可能性は否定できない．またモバイル/ユビキタス環境の普及により，第三者の目がある環境下で認証せざるをえない状況も増加する可能性もある．それゆえ，この脅威に対する対策は急務である．

3. 既存の対策手法

覗き見攻撃に対する既存の対策手法ならびに関連研究について述べる．第三者による認証行為の覗き見を困難にする手法は数多く提案されている[5)–10)]．この中には，覗き見攻撃対策が目的ではないため，認証画面は隠蔽するが認証操作は覗き見られるという手法も含まれている．この種の対策は覗き見攻撃に対する基本的な対策としてその有用性は認めるが，覗き見攻撃の可能性を完全に排除することにはならず，またその適用が困難な状況もあることが問題として残る．なお本論文では，覗き見られることを想定脅威としているため，この種の対策手法は議論の対象外とする．

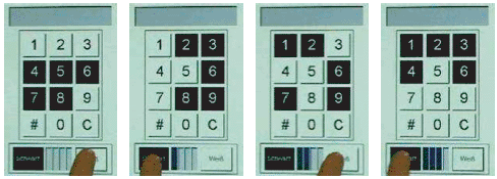

図 1　Roth らによる暗証番号入力例
Fig. 1　PIN Entry Method proposed by Roth, et al.

覗き見られることを前提とした認証手法の提案もいくつか存在する．しかし，それらは人間による覗き見攻撃を想定した対策であるため，ビデオ撮影による覗き見攻撃の脅威に対して安全性を確保できないのが問題である．その具体例について述べる．

Spy-Resistant Keyboard[11)] は，公共空間に設置された大型ディスプレイでの認証を想定したソフトウェアキーボードである．各キーにはアルファベットの大文字 ‘A’，小文字 ‘a’，数字 1 というように 3 つのシンボルが割り当てられており，ユーザはまずはじめに，それらのうちのどのシンボルを入力するかをシフトキーで指定する．次に画面下部にあるキー指示用のシンボルを，入力するシンボルのあるキーまで Drag することで希望の文字を入力する．キー指示用シンボルの Drag を開始すると，キー上に表示されていたシンボル情報が消去される仕組みとなっており，攻撃者が覗き見していても入力値の特定が困難な仕組みとなっている．しかし，この対策手法がビデオ撮影による覗き見攻撃に脆弱であることは明らかであり，またその認証操作が複雑であるという問題もある．

Roth らの論文[12)] で提案されている暗証番号入力手法（**図 1**）も同様の問題をかかえている．図 1 は，提案手法において数字の “3” を入力する例を示している．この手法では，ユーザは入力したい数字の背景色を回答することで数値を入力する．この例では，“白，黒，白，黒” と 4 回背景色を回答することで数字の “3” を入力する．すなわち 4 桁の数字を入力するには背景色を 16 回回答する必要がある．なお Roth らは，本手法の応用事例としてビデオ撮影による覗き見攻撃を想定した対策手法も提案している．それは 4 回の背景色回答で

特定される数字を 1 つから複数にする方法である．しかしそれは，ビデオ撮影による覗き見攻撃への安全性を向上させる一方で，Brute-force 攻撃に対する安全性を低下させるという問題がある．なお論文 14)–16) で提案されている手法は，この手法と類似した手法である．

論文 13)–17) で提案されている認証手法は，認証行為をビデオ撮影しても秘密情報が即座に特定されない手法として提案されている．一例として論文 13) の手法について説明する．この論文で提案されている手法は，視覚情報による質問応答型の認証手法であり，複数の実装例が提案されているが，ここでは路線図を用いた手法について紹介する．路線図上の各駅には番号が割り当てられており，その番号は駅ごとにユニークではなく，各値は複数の駅に割り当てられている．認証時には，システムによって生成された路線図がユーザに提示される．ユーザは秘密情報として複数の駅を事前に定義しておき，認証時には秘密情報となっている駅に割り当てられた数値を回答として答えるという仕組みである．各数値は複数の駅に割り当てられているため，回答値から秘密情報である駅を特定することは困難となっている．

しかしこの手法は，想定脅威の 2 つめである「攻撃者は同一ユーザの認証行為に関する映像記録を複数持ちうる」という問題に対しては脆弱なままである．つまり，認証行為 1 回分の映像記録だけでは秘密情報の推定は困難だが，その映像記録数が増えるに従い，秘密情報が特定される可能性が高くなるという問題である[14),18)]．

なお画像認証でもこの問題に対する対策は重要であり[19)]，画像認証ならではの対策手法がいくつか提案されている[20),21)]．しかし，これらの手法も前章で述べた想定脅威に対して安全であるとはいえない．

4. fakePointer：覗き見攻撃に対抗しうる認証手法

本論文では，2 章で述べた脅威に対して安全性を確保可能にする認証手法 “fakePointer” を提案する．なお以降の議論では，以下の 2 つの事項を仮定したうえで話を進める．

(1)　4 桁数字による暗証番号認証を対象とする．

(2)　想定する脅威の発生箇所は現実世界のみとする．

つまり覗き見攻撃に対して脆弱な認証手法の 1 つである暗証番号認証を例にとるとともに，現実世界で起きる覗き見攻撃を対象とし，通信路上で発生する覗き見攻撃ともいえる盗聴は対象外とする．

4.1 基本コンセプト

fakePointer の基本コンセプトを金庫のダイヤルを例に説明する．**図 2** はいわゆる金庫の

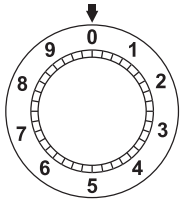

図 2　金庫のつまみ
Fig. 2　A dial of a safety box.

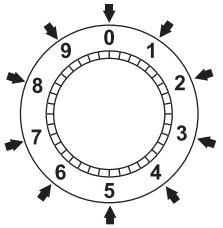

図 3　おとりの回答指示矢印付き金庫のつまみ
Fig. 3　A dial of a safety box with fake indicators.

暗証番号入力用ダイヤルである．これが覗き見攻撃に脆弱である理由は明白である．暗証番号を指し示す矢印が 1 つしかなく，覗き見すればユーザが入力した数字が一目瞭然だからである．そこで暗証番号を指し示す矢印を複数用意し，すべての回答選択肢がつねに選択された状況にする（**図 3**）．正規ユーザは，これらの矢印のうち，どの矢印を暗証番号の指示に使用するかを事前に決定し，記憶しておく．これにより入力値を視覚的に特定することを困難にする．しかし，これでも 2 章で述べた想定脅威のうち，2 つめの脅威に対して脆弱なままである．回答に使用する矢印が 1 つで，それが認証回数によらず固定であるならば，映像記録から 10 個の暗証番号候補が割り出せてしまう．また複数の矢印を組み合わせて暗証番号を入力したとしても，それは問題の解決にはならない．なぜならば，それは暗証番号の特定を困難にはするものの，依然として Replay 攻撃は可能なためである．

またさらに，つまみ側の数字の並びが数字入力のたびにランダムに変更されたとしても，回答用矢印が複数回の認証にわたって固定ならば暗証番号は割り出せてしまう．なぜなら，奪取した複数の映像記録のそれぞれから，各矢印で入力された暗証番号を抽出し，それらの中から出現頻度の高い入力値を特定すればそれが秘密情報となるからである．

つまりこの問題は，回答指示用の矢印が認証回数によらず固定であることに起因したものであるといえる．そこで fakePointer では，認証のたびに毎回変更される複数個の矢印で 4 桁の暗証番号を入力する方法を採用する．つまり，4 桁数字を最大で 4 つの矢印を使用して入力することになる．また暗証番号指示用の矢印は固定ではなく毎回ランダムに決定される．これにより，攻撃者が多数の認証記録映像を奪取したとしても，それらからの秘密情報特定を困難にする．

つまり，2 章で想定された脅威に対して対抗しうる手法に必要とされる要件は次の 2 つであるといえる．

- ユーザの入力値が視覚的に特定不能な秘密情報入力インタフェース．
- 秘密情報入力方法が認証のたびにランダムに変化する入力手法．

4.2 認証手順

前節での議論に基づき，ビデオ撮影による覗き見攻撃対策に必要な要件を満たす実装として fakePointer を考案した．fakePointer では，既存の認証で使用している秘密情報に加えて “回答選択情報” と呼ぶ使い捨てのパスワードを導入し，それを秘密情報の入力に利用することで前節で述べた 2 つの要件を満たす秘密情報入力手法を実現している．

fakePointer における認証手順を**図 4** に示す．この図 4 中の Start 時点において，ユーザはすでに暗証番号を記憶しているものとする．fakePointer では，認証前に “回答選択情報” を取得しなければならない．回答選択情報とは，秘密情報を入力するのに必要不可欠な情報であり，この存在が既存の認証手法とは大きく異なる点である．

図 5 は回答選択情報の一例であり，4 種類の図形で構成されている．ただし回答選択情報に使用される情報の種類数は，認証時の回答選択肢の数と同数またはそれ以上の種類が必要となる．つまり暗証番号認証の場合，回答選択情報に使用する図形は最低でも 10 種類必要となる．図 5 の例は，その 10 種類の図形の中からランダムに選択された 4 つの図形である．

なお回答選択情報とその取得に必要とされる要件を以下にあげる．

- 回答選択情報の取得は，第三者に見られないような環境で実施．
- 回答選択情報はいつでも取得（設定）可能．
- 回答選択情報はいつでも更新可能．
- 回答選択情報の取得に際し，事前の認証は不要．
- 1 度設定された回答選択情報の再閲覧は不能．
- 認証終了と同時に回答選択情報は無効化される．

つまり回答選択情報は秘密情報の一部であり，かつそれは記憶することを前提とする．上記の要件を満たすような回答選択情報の取得方法として例を 2 つあげる．

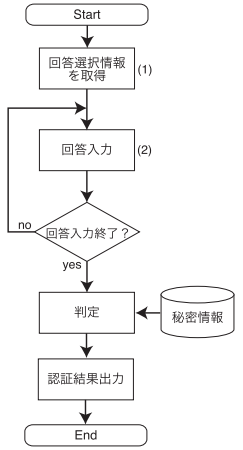

図 4　fakePointer における認証手順
Fig. 4　An authentication process overview of the fakePointer.

図 5　回答選択情報の例
Fig. 5　A sample of answer selection information.

1 つは，ネットワークにアクセス可能な携帯端末を利用した手法である．ユーザは必要に応じて該当端末から認証システムにアクセスし，回答選択情報を取得する方法であり，認証サーバとユーザ間で回答選択情報を共有することになる．

もう 1 つは，表示機能つき IC カードによる方法である．これはユーザとクライアント機器，すなわち IC カードとの間で回答選択情報を共有する手法である．ユーザは IC カードより回答選択情報を取得し，それを記憶にとどめる．その IC カードを持って銀行に行き，ATM で認証を行って現金を引き出す手法である．

これらの手法の共通点は，携帯可能な端末を利用している点である．ここでいう携帯端末とは，一般的なカバンに収納が可能であり可搬であること，そして端末画面の向きを自由に変更可能という特徴を持つことを想定している．ユーザは好きなときに好きな場所で回答選

図 6　fakePointer の認証画面例
Fig. 6　A screen snapshot of the fakePointer.

択情報の取得が可能なので，このような端末であれば，カバンの中やコートの内側に端末を隠して操作したり，埋め込み機器のない壁によりかかった状況で端末を操作したりするなどにより，第三者に見られない状況で回答選択情報を取得することは十分可能であると考える．またこれらの端末は，上記の要件にもあるとおり，1 度設定された回答情報が再閲覧できないという条件を満たす実装が必要となる．

図 6 は，fakePointer の認証画面例である．fakePointer の認証画面は 2 層の表示画面が重なった画面構成となっている．上位層には既存の暗証番号認証と同様，数字キーが表示される．下位層には回答選択情報を含む図形群が表示され，そのそれぞれが各数字キーの背景画像となる．金庫ダイヤルの例にあてはめて考えると，上位層が数字盤であり，下位層が入力値指示のための矢印群となる．なお認証画面下部には，何桁までの暗証番号が入力済みかを示す表示が用意される．

4.3 回答方法

fakePointer における秘密情報入力方法について説明する．ユーザは，認証前に事前に回答選択情報を取得し，記憶しておく．ここでは回答選択情報が図 5 であると仮定する．認証を開始すると，図 6 のような画面がユーザに提示される．この画面表示のうち，上位層に表示される数字キーの配置はキー操作により変更可能となっている（**図 7**）．この機能を利用し，ユーザは 1 つめの回答選択記号の上に暗証番号の 1 桁目が重なるよう数字キーの配置を変更し，決定キーを押す．これで暗証番号の 1 桁目が入力されたことになる．具体例で説明する．暗証番号 1 桁目の入力において，その認証試行における回答選択情報が図 5 であると仮定し，認証画面が図 6 の状態でユーザが決定キーを押した場合，入力された数字

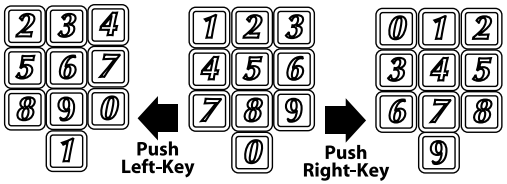

図 7　ユーザ操作による数字配置の制御
Fig. 7　A user can change a layout of number keys.

は “9” と解釈される．なぜならば，1 つめの回答選択記号は “スペード” であり，決定キーが押された際にスペードが背景画像となっている数値は図 6 より “9” だからである．なお秘密情報が入力されるたびに，認証画面の上位層の表示はテンキー配列にリセットされる．

以降，すべての暗証番号入力が完了するまでこの手順を繰り返す．入力完了後，入力された値と既定の秘密情報を比較し，同一値であれば認証成功となる．

ここであらためて fakePointer についてその要点を整理する．fakePointer は永続記憶による固定パスワードとランダムに生成される使い捨てパスワードを利用した認証であり，その 2 種類の秘密情報を利用したユニークな入力方法を採用することでビデオ撮影による覗き見攻撃に対しても一定の安全性を確保しうる手法を実現している．その秘密情報入力方法には，2 つの特徴がある．1 つは，固定パスワードを使い捨てパスワードを利用して入力指示する入力手法である．これにより，正規ユーザは認証のたびに同一の固定パスワードを入力しながらも，攻撃者から見た秘密情報の入力行為は，認証のたびに異なるパスワードの入力を行っているように見せることを可能にしている．もう 1 つは，回答選択情報と同種類の情報をおとりとして利用し，認証時にユーザに提示されるすべての回答選択肢がつねに選択されているように見える入力インタフェースを利用した点である．これらの特徴により，認証行為の映像記録が攻撃者に複数個奪取されたとしても，秘密情報の特定が困難な手法となっている．

5. 考　　察

本章では fakePointer の安全性と利便性について考察するとともに，関連手法との比較について述べる．

5.1 安全性

fakePointer の覗き見攻撃に対する安全性について 3 つのケースをあげて考察する．

1 つめのケースは，回答選択情報が漏洩した場合である．fakePointer では回答選択情報が攻撃者に知られたとしても，その回答選択情報を使用した認証行為の映像記録がない限り安全である．回答選択情報は秘密情報と無関係な情報であるため，その取得が秘密情報の特定を可能または容易にする要素はない．よって回答選択情報のみが攻撃者に漏洩したとしても，その認証行為に関する映像記録が攻撃者に渡らない限り安全性に影響はない．

2 つめのケースは，認証行為 1 回分の映像記録が漏洩した場合である．認証行為 1 回分の映像記録，すなわち認証時の画面と操作に関する映像記録が攻撃者に渡ったとしても，fakePointer はその安全性を維持可能である．fakePointer では，攻撃者が認証行為の映像記録を奪取したとしても，その認証で使用された回答選択情報を知りえない限り，どの数字が暗証番号として入力されたかを特定するのは困難な仕組みとなっているからである．

最後のケースは，認証行為複数回分の映像記録が漏洩した場合である．fakePointer では，この場合にもその安全性を維持可能である．fakePointer は，ランダムに生成される回答選択情報を認証のたびにユーザに取得させ，それを用いて回答入力を行う．そのため，複数の映像記録を基に統計解析を行っても，秘密情報の特定を可能にするような情報は得られないからである．

したがって fakePointer は，2 章で述べた想定脅威に対して安全性を確保可能である．また fakePointer は，覗き見攻撃に対する安全性を確保する一方で，他の攻撃方法に対する安全性が低下するといった副作用もない．fakePointer の Brute-force 攻撃に対する安全性は，既存の 4 桁数字による暗証番号認証と同様であり，ランダムに入力した 4 桁数字が暗証番号と一致する確率は 1/10,000 である．

5.2 利　便　性

fakePointer における利便性について 3 点ほど述べる．1 つめは認証操作が容易な点である．これは 2 つの特徴からなる．1 つめの特徴は認証操作に使用するキーの数が少ない点である．fakePointer の認証操作に必要なキーは，数字キーの配置変更のための左右キーと，入力値確定のためのスペースキーの 3 種類だけである．これはキー操作のためにキーボードに目を配る必要性を減らし，画面に集中して認証操作が可能になる．またキー操作の代替としてマウスやタッチパネルによる操作でも入力可能という利点を生む．またキー操作の映像記録が秘密情報の特定を容易にはしないという利点もある．

もう 1 つの特徴は，既存の手法と比較して操作が直観的だという点である．fakePointer では，認証行為がビデオ撮影されることが想定脅威であるため，既存の対策手法[11),12),17),21)]のように，秘密情報の入力を複雑化することで安全性を確保することができない．したがって，ランダムに生成される使い捨てパスワードの導入と，視覚的に入力値が特定困難なインタフェースを用いることで安全性を確保した．よって fakePointer では，認証操作に複雑さを追求する必要はなく，回答選択記号と暗証番号の数値を重ねるという単純な操作で認証可能とした．これは認証操作において，なんらかの計算行為を強要したり，秘密情報の入力以外にも偽証用の入力が必要といった手間を増大させることもなく，直観的な操作方法であると考える．

2 つめは，覗き見攻撃対策のために必要となる記憶負担の増加が必要最低限になるように配慮されている点である．既存の対策手法の多くは，ユーザに対する記憶負担が多少なりとも増大する手法であり[15),17)]，それは fakePointer も例外ではない．fakePointer の場合は，回答選択情報の記憶がユーザに課せられる新たな記憶負担となる．しかし fakePointer では，回答選択情報が使い捨てという特徴を持つため，ユーザは認証前にそれを取得してから認証が完了するまでの間だけ記憶保持すればよく，その記憶負担の増加は一時的である．したがって覗き見対策に必要な秘密情報を永続的に記憶しなければならない他の手法よりも記憶負担は低いと考えられ，また認証時以外の記憶負担は，従来の認証方法における記憶負担と同等となる．

なお桜井らの論文[15)]では，記憶負担を減らす方法として，証明者は 1 桁目の暗証番号を画面中の好きな色で選択し，以降はその色で暗証番号を選択することにより，暗証番号を選択するための色情報を記憶しなくてもよいという手法を提案している．しかしこの手法は，記憶負担を軽減する一方で安全性を低下させることになり，望ましい記憶負担軽減法とはいえない．

3 つめは，ハードウェアトークンなど専用機器の所有が必須条件ではない点である．fakePointer のユーザは，認証前に回答選択情報を取得し，それを検証側と証明側で共有する必要がある．しかし，認証における基本的な安全性は永続記憶している秘密情報に依存しているため，回答選択情報の共有に関して時間的制約はない．よって fakePointer では，認証システム側に回答選択情報を「発行」する仕組みを用意し，ユーザはそれを利用して必要なときに回答選択情報を取得するという実現方法も可能となっている．したがって，ユーザの利便性を低下させかねない専用機器の所有を不要にすることも可能である．

5.3 既存の対策手法との比較

fakePointer は，既存の認証手法を基にビデオ撮影による覗き見攻撃への安全性を付与することを目指した手法である．それゆえ fakePointer は次の特性を備えている．1 つは，秘密情報は既存の認証手法のものをそのまま流用しており，それは永続記憶を想定している．

もう 1 つは，回答選択情報が使い捨てである点である．それは認証前にユーザと認証システムとの間で共有する必要があるが，RSA SecurID [23] のように時刻に応じて厳密に同期した情報を使用する必要はない．つまり回答選択情報の取得と認証行為を時間的に分離することが可能となる．これは 2 つの利点を生むといえる．1 つは回答選択情報の記憶維持期間はユーザが選択可能になる点である．4.2 節で述べた要件さえ満たされていれば，ユーザは認証前の都合の良いときに回答選択情報を取得すればよい．したがって，回答選択情報の記憶負担を大きいと感じる人は認証直前に取得し，少ないと感じる人は事前に回答選択情報を取得するという対応が可能となる．つまり fakePointer は，その利用に回答選択情報の記憶が必要不可欠ではあるが，それはなんらかの規則に基づき強制される行為というよりも，記憶可能な範囲で実施する対策ということができる．

もう 1 つの利点は，回答選択情報を忘れてしまったとしても，それが認証不能という致命的な状況を招かないという点である．回答選択情報は秘密情報の一部であるが，それはあくまで覗き見攻撃対策のための情報であり，認証そのものに関する秘密情報ではない．したがって，仮にユーザが回答選択情報を忘却したとしても，次の 2 つの方法により認証不能になることを回避できる．1 つは，覗き見攻撃の脅威がない場面で従来どおりの認証方法により認証を行う方法であり，もう 1 つは，新たに回答選択情報を取得し，それを用いて fakePointer で認証を行う方法である．したがって既存の対策手法とは異なり，覗き見攻撃対策で必要となる情報の記憶に失敗しても，永続記憶による秘密情報さえ維持できていれば継続して認証は可能である．この特徴は，新たな認証手法に対するユーザの心理的負担を軽減しうる特徴であると考える．

これまでの議論をまとめると，fakePointer は既存の対策手法にはない以下の特徴を持つ手法であるといえる．

- ビデオ撮影による覗き見攻撃に対する安全性を確保．
- 覗き見対策に必要となる情報の記憶必須期間をユーザが柔軟に選択可能．
- 覗き見攻撃対策への対応不備が認証不能につながらない．
- 専用機器の所持は必須要件ではない．

また 2 つの関連手法を例にあげ，既存の対策手法との差異について説明する．

1 つめは徐らの提案している手法[18] である．この手法では覗き見対策として画像認証による One-Time Password を用いている．この手法では，RSA SecurID [23] のように専用機器から発生するランダムな数字を使用するかわりに，画像パスワードを記憶することとしている．認証のたびに秘密情報であるパスワード画像を変更するとともに，その記憶補完のため，設定した画像に基づいた Story を作成し，設定したパスワード画像とあわせて記憶することで，毎回変更される画像パスワードの記憶を可能にするという手法である．

この手法には 4 つの問題点があると考える．

1) 徐らの手法では，認証に成功した後，その場でパスワード画像を更新するとしているが，それが現状の認証環境へ適用可能かという点で疑問が残る．
2) 前述の 1) の運用条件のもとで，彼らが安全性確保の条件としている「連続した 2 回の認証行為をビデオ撮影されない限り安全」という条件が成立するのかという点に疑問が残る．少なくとも，銀行 ATM に隠しカメラが設置され，その存在に一定期間気づかなかったとした場合，上記条件の成立は困難であると考える．
3) Story づけによる記憶補完を行うため，認証のたびに秘密情報である画像を更新してもその記憶は可能であると述べているが，それが一般ユーザの多くが実行可能かという点でまだ疑問が残る．徐らの論文の評価実験の結果にもあるように，一部のユーザはその記憶補完に失敗しており，またその実行可能性は認証頻度にも依存する懸念があることも指摘されている．また Story づけによる記憶補完がうまく機能しないという実験結果[22] もあり，その手法の実行可能性についてはまだ議論の余地があると考える．
4) 徐らの手法では，認証のたびに更新した画像パスワードとそれに関する Story を作成し，記憶する必要がある．しかし，実際の運用ではこれらのほかに「シークレットプレイス」と呼ばれる秘密情報更新に使用するための情報も記憶する必要がある．またこれらのうちの 1 つでも忘却した場合，それは認証不能となる．これらを総合的に考えると，記憶可能性に関する主張について疑問が残るとともに，記憶に失敗した場合は致命的な結果になることから，その実行可能性にも疑問が残る．

これに対し fakePointer では，1)，2) に関する懸念はない．また記憶に関しても，回答選択情報を限定された期間だけ記憶すれば fakePointer による対策が実施可能であり，また仮に回答選択情報を忘れたとしても，それが認証不能にはつながらないため，提案手法と比較してその記憶負担は低く，実行可能性も高い手法であると考える．

2 つめは RSA SecurID [23] である．この手法は，暗証番号（知識）と One-Time Password（所有物）の組合せによる 2 要素認証として知られており，記憶情報と専用機器により発行される情報の双方を利用した認証として fakePointer と同様の認証システムであるといえる．

この認証手法について，実世界でのビデオ撮影による覗き見攻撃を想定すると，次のような差がある．RSA SecurID では，認証操作が数値の直接入力であるため，認証行為のビデ

オ撮影によって暗証番号は特定される．また暗証番号が特定された場合，なりすましに必要なのはランダムに発行される数値だけとなり，問題は所有物に対する脅威となる．しかし認証トークンにはアクセス制御がなく，それを手にしたり，覗き見したりすることができればなりすましに成功する可能性がある．したがって RSA SecurID のユーザは，認証トークンの扱いに常時注意を払うべきということになり，それは利用者に少なからぬ負担を強いることになる．

これに対して fakePointer では，認証行為のビデオ撮影から暗証番号が特定されることがなく，また回答選択情報は記憶にとどめ，設定済みの回答選択情報の再閲覧は不能となっていることから，一定のアクセス制御が実現されているといえ，ユーザが 1 度設定した回答選択情報の漏洩に注意を払う必要はない．

ただし fakePointer と RSA SecurID はその目的に大きな差があり，認証システムとしての比較には議論の余地があることに注意されたい．RSA SecurID は，認証における安全性を総合的に向上させるため，既存の認証手法とは異なる新たな認証手法を提案したものであり，一方 fakePointer は，既存の認証手法における特定脅威への安全性を強化する手法を提案したものだからである．

5.4　今後の課題

fakePointer における今後の課題について述べる．

第 1 の課題は被験者による評価実験である．本論文の内容は認証手法の提案にとどまっているが，この提案手法が多くのユーザにとって実行可能なものであり，かつ設計どおりの安全性を実現していることを検証する必要がある．

なお本論文の提案手法とは若干異なるのだが，本手法の基となった認証手法に対して実施した評価実験の結果を参考までに掲載する．この評価実験は，論文 24) で提案した認証手法に対しそのプロトタイプを実装して行った被験者実験である．被験者は 6 人で，全員が 20 代男性の大学院生である．実験手順は，まずはじめに認証方法について説明を行い，その後プロトタイプシステムを使用して 3 回ほど認証を手順確認のために行わせた．そしてその後に評価実験としてプロトタイプによる認証を 3 回実施させた．認証手順は，まず被験者に回答選択情報を提示して記憶させ，「記憶した」と被験者が回答したら，その後すぐに認証行為を実施した．またこの実験では，被験者による認証行為を大型ディスプレイに表示し，実験をしていない他の被験者がその認証行為を見られるようにした．これにより人間による覗き見攻撃が実際に行える環境とした．

実験結果から，18 回（= 6 人 × 3 回）の試行のうち認証に失敗したのは 1 回だけであった．またその認証時間は最短が 9.84 秒，最長が 29.75 秒で平均は 17.35 秒となった[⋆1]．また実験をしていない被験者による覗き見攻撃実験は 1 度も成功しなかった．したがってこの実験結果における FRR はおよそ 5.6%（= 1/18），人間による覗き見攻撃に関する FAR は 0%となる．ただしこれらの実験結果は本論文で提案している手法とは若干異なり，本論文の提案手法は論文 24) の内容を改良したものである．したがって同様の実験を提案手法で実施し，その改善効果を実際に検証する必要がある．

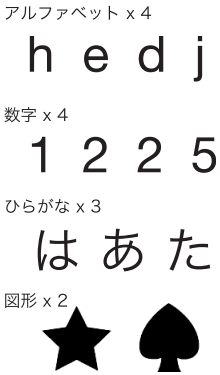

図 8　回答選択情報の一例
Fig. 8　Variation of answer selection symbols.

次の課題は，回答選択情報の記憶可能性に関する問題である．fakePointer では，認証のたびに回答選択情報を記憶する必要がある．その記憶負担が可能な範囲で小さくなるよう配慮されてはいるが，その記憶が曖昧では回答入力できないため，回答選択情報はユーザにとって記憶しやすい情報であることが望ましい．そこでここでは，この問題に対して 3 つの改善案を提案する．

1 つめの案は，回答選択情報にユーザの好きな情報を使用する方法である．回答選択情報は，必要な種類の情報さえ用意可能ならば，図形以外でも運用可能である．**図 8** にあるように数字，平仮名，アルファベットや写真なども利用可能である．このように利用者にとって記憶が容易だと感じられる情報を使用することで記憶負担の軽減が可能になると考える．

2 つめの案は回答選択情報の記号数を削減する方法である．回答選択情報は，原則として

⋆1 この認証時間の結果は認証失敗の事例も含んでいる．

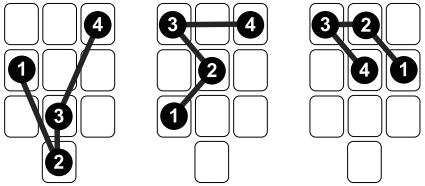

図 9　位置と順序による回答選択情報提示例
Fig. 9　An another answer selection symbol specified with positions and their order.

秘密情報の文字数と同一数としているが，図 8 のひらがなや図形の例のように，これらが同一数でなくても fakePointer による認証は可能である．秘密情報と回答選択情報の記号数が異なる場合は，回答選択情報を記号集合として扱い，集合内のいずれかの記号で秘密情報を選択するものとする．ただし，認証画面に複数の回答選択用記号が同時に表示されると Brute-force 攻撃に対する安全性が低下する．この問題を回避するため，認証画面中に表示される回答選択情報は複数ある回答選択情報のうちの 1 つだけとし，他の記号は回答選択情報に含まれない記号とする．

3 つめの案は，回答選択位置そのものを回答選択情報として提示する方法である．回答選択情報の役割は，秘密情報を指し示す “位置” をユーザに教示しているといえる．したがって，回答選択情報を**図 9** のような形式とし，各桁の回答位置を直接指示することも可能である．つまり，回答選択情報を記号で与えるかわりに，回答を指し示す位置と順序を直接図としてユーザに配布するのである．なおこの回答位置とその順序は認証のたびにランダムに変更される．図 9 は回答選択位置を示す回答選択情報の例である．図 9 左の回答選択情報を例に説明すると，1 桁目の暗証番号を左列中段の位置で回答し，2 桁目を中央最下段の位置で回答する，というように，以降，同様の手順で秘密情報を入力することを意味する．

もしこの回答選択情報による運用が可能ならば，認証画面は 2 層表示の必要がなく，既存の銀行 ATM と同様の画面のまま操作方法を変更することで fakePointer による認証が可能となる．これはユーザインタフェースの差異に起因するユーザの違和感を軽減しうるとともに，操作面においても入力のたびに認証画面を読み取り，入力値を指示する位置を探索する作業が不要となるため，秘密情報入力における作業負担軽減にも寄与すると考える．

最後の課題は，回答選択情報と認証行為の映像記録がともに奪取されないという条件を妥当化する手法の提案である．fakePointer の覗き見攻撃に対する安全性は，認証行為の映像記録とその認証で使用された回答選択情報の双方が攻撃者に奪取されない限り保たれる．しかしこれは，回答選択情報の取得を第三者に見られない環境で行うという前提のもとに成立するものであり，ユーザの行動に依存している．携帯端末の利用によってその条件を満たすことは可能であることは前述した．しかし，認証により高い安全性を求める場合には，ユーザの行動になんらかの規定を設け，ユーザが誤って不適切な行為を行わないようにする配慮も必要であると考える．そこでそのような要望を想定し，以下の 2 つの方法を提案する．

1 つは時間差取得である．これは回答選択情報を取得してから認証行為を行うまでの間に一定間隔以上の時間経過を必須とする方法である．つまり銀行でお金を引き出したい場合，回答選択情報を取得してから既定の時間以上経過しないと銀行 ATM で正しく秘密情報を入力しても認証に成功せず，結果としてお金を引き出せないという方法である．いい換えると，取得した回答選択情報は既定の時間を経過しない限り，回答選択情報として有効化されないということである．

もう 1 つは位置差取得である．これは回答選択情報を取得した場所と認証実施場所との間が一定の距離以上離れていることを条件とする方法である．例としては，オフィスを出る前に回答選択情報を取得し，昼食時に銀行 ATM に寄って認証を行い，お金を引き出すという利用法である．なおこの手法は，自然と時間差取得にもなる．この手法では，位置差によっては利便性を大きく害する可能性があるが，不特定多数のユーザを想定する場合，距離差を大きくとることは現実的に困難であり，また認証に求める安全性にも依存するが，距離差を大きくすればするほど好ましいという性格のものではなく，むしろ認証実施場所のそばで回答選択情報を取得することを防ぐという意味であることに注意されたい．したがって，たとえば銀行店舗内の ATM とは離れた場所に，回答選択情報発行機を設置する方法も求める安全性によっては妥当な実現例であると考える．ATM を使用するユーザは，まず発行機で回答選択情報を取得し，そのうえで発行機とは離れた場所にある ATM の列に並び，認証を行う．これにより双方の映像記録が奪取され，かつ回答選択情報の記録と認証行為の映像記録の整合性をとることを困難にする．

このように時間差または位置差を利用して，攻撃者が回答選択情報と認証行為の映像記録の組を奪取しにくい環境を構築することが必要である．また視覚情報に依存しない回答選択情報の発行方法などを検討していく必要もあると考えており，これは今後の課題である．

6. おわりに

本論文では，認証における脅威の 1 つである「覗き見攻撃」に対する対策として，“fakePointer” を提案した．またその認証手法の安全性と利便性について考察を行った．

本論文では，覗き見攻撃による現実の脅威としてビデオカメラにより認証画面と操作方法の双方が撮影されることを想定し，さらにその映像記録が攻撃者に複数個奪取されることも考慮したうえで，ユーザの秘密情報の特定を困難にするため次の 2 つの工夫を施した．

1 つは，認証画面や操作から入力値の特定を困難にするユーザインタフェースである．fakePointer では，すべての回答候補がつねに選択されている画面を秘密情報の入力画面とすることで，認証行為の映像記録があったとしても，そこから入力値を特定することを困難にしている．もう 1 つは，回答方法のランダム化である．fakePointer では，認証のたびにランダムに生成される回答選択情報を取得し，それを用いて秘密情報を入力する．これにより，同一ユーザの認証行為に関する映像記録が複数個奪取されたとしても，出現頻度に基づく統計解析により秘密情報を特定することを困難にしている．

また fakePointer は，その利便性にも配慮している．覗き見攻撃に対する安全性向上のため，回答選択情報の記憶という新たな負担をユーザに強いることになるが，その負担が必要最低限になるよう配慮されており，また仮に回答選択情報を忘れたとしても，それが認証不能という事態を招かないような仕組みとなっている．また秘密情報の入力操作も 3 種類のキーのみで操作可能であるとともに，従来の対策手法と比較して直観的な回答方法となっている．またマウスやタッチパネルといった入力インタフェースでも操作可能なことから，携帯電話や PDA など覗き見攻撃を受けやすい環境下で使用される端末での認証手法としても適用可能である．

これまでの覗き見攻撃に対する対策は，実行主体が人間であると想定されていたが，ビデオカメラによる認証行為の全部撮りにより想定脅威が変化した．この新しい脅威に対する対策は急務であり，その 1 つとして本論文では fakePointer を提案した．今後は残された課題に対する改善策を模索するとともに，被験者による評価実験の実施を検討している．

謝辞　本研究においては，電気通信大学大学院情報システム学研究科小池英樹教授とセキュリティ研究グループの学生諸氏に有益なコメントをいただいた．また産業技術総合研究所の増井俊之氏，塚田浩二氏，田中哲氏にはシステムの改善における有益なコメントをいただいた．また本論文の執筆においては産業技術総合研究所の西村拓一氏にご指導いただいた．本研究の遂行においてお世話になったこれらの方々に対し，ここに感謝の意を述べる．

参 考 文 献

1) 横浜銀行：当行無人出張所（店舗外 ATM）に盗撮用機器が設置されていたことが判明した件（online）．available from http://www.boy.co.jp/oshirase/atm.pdf (accessed 2007-11-26).
2) 三菱東京 UFJ 銀行：当行 ATM コーナーにて盗撮されたとみられることが判明した件（online）．available from http://www.bk.mufg.jp/info/atm_20060112.html (accessed 2007-11-26).
3) 埼玉縣信用金庫：当金庫 ATM コーナーをご利用のお客様へ（online）．available from http://www.saishin.co.jp/news/1222/index.shtml (accessed 2007-11-26).
4) 金融庁：あなたのキャッシュカードが狙われています（online）．avaiable from http://www.fsa.go.jp/ordinary/card/index.html (accessed 2007-11-26).
5) トマト銀行，操作画面をすっぽり覆う「盗撮防止カバー」を ATM に設置，日経 BP，March 27 (2006)．（online）．available from http://www.nikkeibp.co.jp/archives/425/425911.html (accessed 2007-11-26).
6) シャープ株式会社：隣の人から見えにくい視野切替機能付き VeilView モバイル ASV 液晶（online）．available from http://www.sharp.co.jp/products/sh851i/text/veilview.html (accessed 2007-11-26).
7) Kurata, T., Kato, T., Kourogi, M., Keechul, J. and Endo, K.: A Functionally-Distributed Hand Tracking Method for Wearable Visual Interfaces and Its Applications, *Proc. IAPR Workshop on Machine Vision Applications* (*MVA2002*), pp.84–89 (2002).
8) 東洋通信機：暗証番号入力装置，特開 2001-147763 (2001).
9) 三菱電機：暗証番号入力装置，特開平 05-334334 (1993).
10) 日本信号：暗証番号を入力する装置，特開平 09-297875 (1997).
11) Tan, D.S., Keyani, P. and Czerwinsky, M.: Spy-resistant keyboard: more secure password entry on public touch screen display, *OZCHI'05: Proc. 19th conference of the computer-human interaction special interest group* (*CHISIG*) *of Australia on Computer-human interaction*, pp.1–10 (2005).
12) Roth, V., Richter, K. and Freidinger, R.: A PIN entry method resillient against shoulder surfing, *Proc. 11th ACM Conference on Computer and Communications Security* (*CCS2004*), pp.236–245 (Oct. 2004).
13) Matsumoto, T.: Human-computer cryptography: an attempt, *Proc. ACM Conf. on Computer and Communicaiton Security*, pp.68–75, ACM Press (1996).
14) 古原和邦，今井秀樹：均等写像を用いた質問応答型の直接個人認証方式ののぞき見攻撃に対するさまざまな安全特性について，電子情報通信学会論文誌 A，Vol.J79-A, No.8, pp.1352–1359 (1996).
15) 桜井鐘治，吉田真利子，撫中達司：モバイル個人認証方式の提案と評価，コンピュータセキュリティシンポジウム 2004，pp.625–630 (Oct. 2004).
16) 三菱電機：認証システム，認証装置，端末装置及び IC カード，特開 2006-018358 (2006).
17) Matsumoto, T. and Imai, H.: Human Identification Through Insecure Channel, *Advances in Cryptology – EUROCRYPT 91*, Lecture Notes in Computer Science,

pp.409–421, Springer-Verlag (1991).
18) 徐　強，西垣正勝：ニーモニックに基づくワンタイムパスワード型画像認証の実現可能性に関する検討，情報処理学会研究報告 2006-CSEC-32，pp.317–322 (2006).
19) Suo, X. and Zhu, Y.: Graphical Passwords: A Survey, *Proc. 21th Annual Computer Security Applications Conference* (*ACSAC21*) (Dec. 2005).
20) 原田篤史，漁田武雄，水野忠則，西垣正勝：画像記憶のスキーマを利用したユーザ認証システム，情報処理学会論文誌，Vol.46, No.8, pp.1997–2013 (2005).
21) Wiedenbeck, S., Waters, J., Sobrado, L. and Birget, J.C.: Design and Evaluation of a Shoulder-Surfing Resistant Graphical Password Scheme, *Proc. Advanced Visual Interface* (*AVI2006*), pp.23–26 (May 2006).
22) Davis, D., Monrose, F. and Reiter, M.K.: On User Choice in Graphical Password Schemes, *13th USENIX Security Symposium*, pp.151–164 (2004).
23) RSA Security Ltd.: RSA SecurID – Securing Your Future with Two Factor Authentication (online). available from http://japan.rsa.com/products/securid/index.html (accessed 2007-11-26).
24) 高田哲司：fakePointer 2：個人認証における覗き見攻撃への安全性を向上させるユーザインタフェースの提案，暗号と情報セキュリティシンポジウム（SCIS2007）(2007).

(平成 19 年 11 月 30 日受付)
(平成 20 年 6 月 3 日採録)

高田　哲司（正会員）

2000 年電気通信大学大学院情報システム学研究科情報システム運用学専攻博士課程修了．工学博士．同年電気通信大学サテライトベンチャビジネスラボラトリ研究員．2003 年ソニーコンピュータサイエンス研究所入所．2005 年産業技術総合研究所入所，現在，同研究所情報技術研究部門研究員．情報セキュリティの研究に従事．情報視覚化，Usable Security System に関心を持つ．IEEE/CS 会員．