RM-001

音声提示と相対値入力による覗き見に強い認証方式の提案

The Strong Authentic Method by Voice Navigation and Relative Value Input Preventing from Peeping Attack: Invisible Authentication

近藤 潤† 平野 学‡ 神谷 直希‡

Jun Kondo Manabu Hirano Naoki Kamiya

1. はじめに

近年、携帯電話やスマートフォン（以下、携帯端末）は多機能化が進み、さらなる進化を遂げている。画面は大きくなり、また解像度も飛躍的に高くなってきた。携帯端末の OS は統一化されつつあり、カメラ、GPS、音楽再生、インターネットアクセス等は必須の機能となってきている。しかしながら、携帯端末本体の認証方式は、他機能が高機能化しているにも関わらず未だ 4 桁の数字を暗証番号として直接キーパッド、若しくはソフトウェアキーボードによって入力するものが主流である。指紋や顔の特徴を用いて認証する、生体認証の可能な携帯端末[1]もあるが、指紋認証に関してはなりすましなどの危険[2]もあり、依然として暗証番号を直接入力する方式が利用されている。

また、携帯端末本体の認証だけではない。公共の場で携帯端末を使った認証を利用する機械が増えてきている。多くの銀行では、オンラインバンキングと呼ばれるインターネットを介して個人の口座へ接続する手段を提供している。また、ソーシャルネットワークサービスや各種利用料金案内のような個人向けサービスへの接続も携帯端末から行えるようになってきた[3]。これらのサービスは大変便利である一方、公共の場での認証に対する危険性も懸念される[4]。

例えば、電車内でユーザーが銀行口座にアクセスしようとしているとき、誰かが暗証番号を盗みとるためにその認証画面やユーザーの入力を覗いているかもしれない。この類の犯罪は、肩越しに覗かれることが多いことから「Shoulder-Surfing Attack（ショルダー・サーフィング アタック）」や、単に「覗き見攻撃」と呼ばれる。本研究では、だれもが簡単に利用することができる、覗き見攻撃に耐性のある暗証番号入力方式を提案する。

まず、2 章では「覗き見攻撃」を明確にし、3 章で関連研究を、4 章で本提案を述べる。5 章で実験項目を示し、 6 章で結果を、また 7 章で実験結果と関連研究とを比較する。8 章では実験から分かった課題を、9 章で利用例を、最後に 10 章でまとめを述べる。

2. 覗き見攻撃の種類

覗き見攻撃には、大きく分けて 2 種類の覗き見があると考える。画面を覗き見る攻撃「画面の覗き見」と入力行為を覗き見る攻撃「入力の覗き見」である。

2.1 画面の覗き見

画面の覗き見は、画面上に表示される情報を覗き見る行為である。図 1 のように肩越しに直接画面を覗き込む攻撃の他、スクリーンロガーやビデオカメラ撮影による覗き見攻撃も含まれる。

図 1 画面の覗き見攻撃のイメージ

攻撃者（画像手前）と被害者（奥）

図 2 操作の覗き見攻撃のイメージ

2.2 操作の覗き見

操作の覗き見は、キーボードや入力行為を覗き見する攻撃である。（図 2）キーロガーのような特殊なツールの他、前述の画面の覗き見同様、直接覗き込んだりビデオカメラで撮影したりして秘密情報を盗難する攻撃もこれに含まれる。

3. 関連研究

文献[5]によると認証に利用される因子とその具体例は次のようなものがある。

†豊田工業高等専門学校情報科学専攻 Computer Science Course, Advanced Engineering Course for Bachelor Degree, Toyota National College of Technology

‡豊田工業高等専門学校情報工学科 Dept. of Information and Computer Engineering, Toyota National College of Technology

(1) ユーザーの知識

ユーザーの知識によるものは、主にパスワードや暗証番号、ダイヤル錠などを指す。また、最近はユーザーの記憶、例えば家族や友人の写真などを用いて認証するものもある。安価に実装でき、持ち運びの問題がないことが挙げられるが、覗き見などの攻撃により盗難される可能性がある。

(2) ユーザーの所有物

ユーザーの所有物によるものは、トークン、スマートカード、ファイルや機器に組み込まれた秘密データ、メカニカルキーなどである。悪用が最も困難であるが、高価であったり、紛失の可能性があったりと、必ずしも持ち運べるとは限らない。

(3) ユーザーの生体情報

生体情報とは、ユーザーの本人の情報、例えば指紋、虹彩、静脈、音声認識、写真付き証明書などを指す。ユーザーにとっては最も認証が簡単であり、持ち運びの問題がない。しかし、身体的特徴は変更がきかなかったり、正規ユーザーを誤認識したりする可能性がある。

どの認証因子も利点・欠点が存在するが、本稿では (1) のユーザーの知識による認証方式のセキュリティー向上を目指す。暗証番号（数字）4 桁を入力する認証を想定し、認証時の画面の覗き見・操作の覗き見攻撃への耐性を高める。以下に、従来の覗き見に耐性のある認証・暗証番号入力方式を提案した関連研究を示す。

3.1 fakePointer[6]

秘密情報に加え、「回答選択情報」と呼ばれる使い捨ての記号によるパスワードを導入し、それを秘密情報の入力に利用する。回答選択情報は、星や丸などを用い、暗証番号が数字 10 種類の場合 10 種類の記号が必要となる。ユーザーは、覗き見のされることのない安全な場所で、認証の度に事前に何らかの方法を用いて回答選択情報を設定、または知っている必要がある。fakePointer の認証画面（図 3）では、画面上のテンキーの背景に、10 種類の記号が描画され、その上に 0 から 9 の数字が表示されている。この数字配列を左右キーで移動させ、予め取得しておいた回答選択情報の記号と重なったら決定キーを押下し入力を確定する。例えば、図では、暗証番号が 4 で記号が▲であるとすると、「左」を 3 回入力する。また、高田氏は回答選択情報を記号 2 種類・数字 2 桁とし、数字 2 桁は画面上に表示されている数字の背景を回答選択情報として、ビデオカメラによる撮影にも耐性を有する認証手法、fakePointer 2 も提案している[7]。

3.2 Volker Roth's PIN-ENTRY METHOD[8]

図 4、図 5 に示すようにテンキーの背景を白と黒に塗り分け、ユーザーの暗証番号がどちらの背景色かを示して回答する。この暗証番号入力方式は基本的には同じだが、2 種類の入力方式が提案されている。

3.2.1 Immediate Oracle Choice (IOC)

IOC は画面が変更される度に背景色を回答する方式である。（図 4）表示された直後に回答するので、後述の DOC のように背景色を記憶しておく必要はない。ただし、覗き見攻撃による暗証番号の推測が DOC に比べ容易である。図 4 の例では 4 画面の写真と回答を比較すれば、「3」が入力されていることが一目瞭然である。

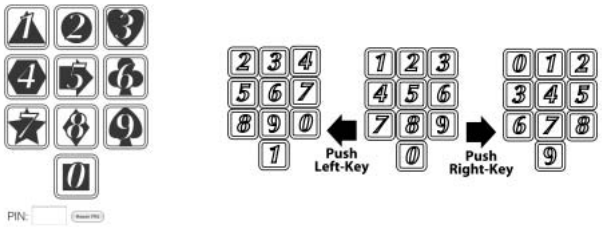

図 3 高田氏による fakePointer 操作画面例（左）とユーザーによる数字配置操作例（右）

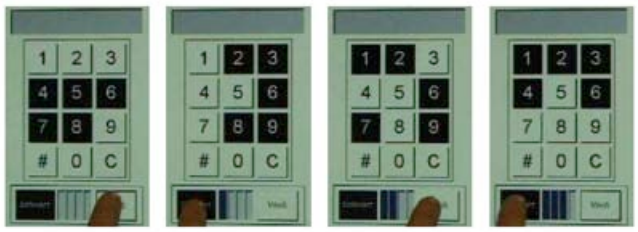

図 4 Roth 氏らによる PIN-ENTRY METHOD Immediate Oracle Choice

図 5 Roth 氏らによる PIN-ENTRY METHOD Delayed Oracle Choice

3.2.2 Delayed Oracle Choice (DOC)

DOC は 4 回画面が切り替わった後、4 回分の背景色をまとめて回答する方式であるので記憶しておかなければならないため記憶負担は増加するが、回答する際には画面が既に切り替わっているため、IOC と比較し暗証番号の推測を困難にしている。

画面を覗き見る時間が一瞬ならば IOC より暗証番号の推測が難しいが、しかしながら、ビデオカメラ撮影による覗き見攻撃では、IOC と安全性は変わらず暗証番号は推測される可能性がある。

4. 提案する認証方式

3 章にて示した 2 つ関連研究には弱点がある。fakePointer においてはユーザーの記憶負担の増加や操作の複雑化、Roth 氏らによる PIN-ENTRY METHOD では、そもそも瞬間的な覗き見への耐性はあるものの、ビデオカメラによる覗き見攻撃への耐性はない。

提案する Invisible Authentication（インビジブル・オーセンティケーション）では覗き見攻撃に耐性をもち、かつユーザーが記憶しなければならない情報を増やすことなく認証を強化することが目的である。

本研究では、2 つの機能により、見えない認証ユーザーインターフェース可能としている。「音声提示」により認証行為そのものを隠蔽し、「相対値入力」によって、入力やユーザーの暗証番号の覗き見を防ぐ。

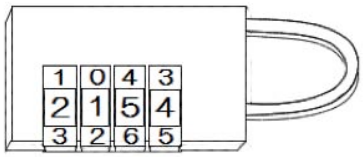

図 7　仮想的なダイヤルロックのイメージ

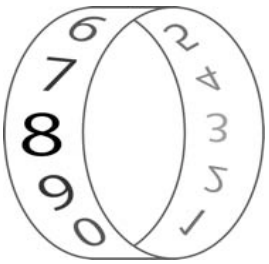

図 8　環状に配置された数字

それにより、2 章で述べた 2 種類の覗き見攻撃への対策を施す。

4.1 音声提示

音声提示とは、画面表示の代わりとなるものである。本来画面に表示されるべき情報、認証画面そのものや、アスタリスクなどで代替表示される入力済みの桁数を、携帯端末に接続されたイヤーフォンや受話部など音声再生手段を通じてユーザーに音声で伝送される。画面上には何も表示がされない。例えば、1 桁目を入力しようとする際、音声再生手段からは「1 桁目」と再生される。

4.2 相対値入力

相対値入力とは、暗証番号と予め端末内で生成された乱数（初期値）との差分値を入力することである。相対値の入力はキーボードを搭載した端末であれば矢印キー、タッチスクリーン式の端末ではフリック入力やソフトウェアキーボードにより行う。そのため、機種には依存せず、極論を言えば、画面のない端末でも暗証番号入力による認証を行うことが可能である。

4.3 コンセプト

この認証方式は、2 つの脅威に対して有効である。一つ目の脅威はユーザーが認証行為をしている画面を直接、またはビデオカメラで撮影し覗き見る攻撃である。もう一つの脅威は、スクリーンロガーやキーロガーといった、ユーザーの画面やキー入力の盗聴の脅威である。本提案は、携帯端末に接続されたイヤーフォンや受話部など音声再生手段を通じて音声提示を行う。操作しているユーザーのみが何が行われているか分かる仕組みである。無論、画面上には何も表示されない。

提案システムは、仮想的なダイヤルロック（図 6）を想定して設計されており、誰でも使いやすいユーザーインターフェースを持っている。図 7 のように 0 から 9 の次は再び 0 と、値は環状に入力できる仕様である。それに加え、ユーザーは相対値入力について考える必要はなく、ただダイヤルロックを頭の中で想像しながら利用すればよい。ユーザーは仮想的なダイヤルロックを暗証番号に合わせるようにして入力すれば、相対値は自動的に入力される仕組みである。

```
1:  A[4] ← random numbers[4]
2:  D ← 1
3:  voiceover D, A[D]
4:  while 1≦D ∧ D≦4
5:      input direction ∈ (up, down, right, left)
6:      if direction = up then
7:          A[D] ← (A[D] + 1) modulo 10
8:      else if direction = down then
9:          A[D] ← (A[D] + 9) modulo 10
10:     else if direction = right then
11:         D ← D + 1
12:         voiceover D, A[D]
13:     else
14:         D ← D - 1
15:         voiceover D, A[D]
16:     end if
17: end while
18: return A
```

図 6　Invisible Authentication のアルゴリズム

A は各桁の値、D は入力中の桁を示す。random numbers[4]には 4 桁の乱数が予め生成され、voiceover は引数の読み上げ、modulo 10 は法 10 を示す。

4.4 認証手順

一連の流れとして、端末内ではまず乱数が 4 桁分生成されユーザー入力の初期値としてセットされる。ユーザーの上下入力により、入力値を増減させる。4 桁分入力し終えたら、認証する。図 8 に提案する Invisible Authentication のアルゴリズムを示す。

1 行目で各桁（配列 *A*）に 0 から 9 の乱数を代入し、*D*（入力中の桁）が 1 から 4 の間、ユーザーの入力を受け付ける。ユーザーの入力された方向で操作を決定する。7 行目で入力桁の値を増加した後、10 の法を代入しているのは、ダイヤルロックの様に値「9」を 1 増加した後、0 に戻るようにするためである。同様に、9 行目では値「0」から 1 減少した値が「9」となるように現在の入力値に 9 を足した後、10 の余りを代入し実現している。12 行目の voiceover で、入力しようとしている桁、その桁の値（初期状態では代入された乱数）が音声提示される。

4.5 利用方法

認証を開始すると、音声提示により一番左側の桁、1 桁目の乱数が伝えられる。ユーザーはダイヤルロックをロックナンバーに合わせると同様、左の桁から順に暗証番号を合わせるようにして入力していく。「上下」入力で値を増減させ、「右」（若しくは決定キー）の入力で次の桁に進む。予め決められた桁数分入力し終えたら、最後に「右」（若しくは決定キー）の入力をして暗証番号入力を終了する。端末内で生成された乱数と入力された相対値を足し合わせると、端末内で暗証番号が生成され、認証が開始される。図 9 に暗

証番号を 1234、乱数を 2154 としたときの認証手順の例を示す。

「1 桁目、2」と音声提示されると、ユーザーは暗証番号の一桁目である「1」を入力するため値を減らす操作、「下」入力を行う。1 桁目は入力を終え、次の桁へ移動するため「右」入力。2 桁目も同様に「2 桁目、1」と、現在入力している桁数と、初期値が音声提示される。4 桁入力し終えると、最後に「右」を入力し認証が開始される。

5. 実験

実験をするにあたり、テスト用のアプリケーションを作成した。開発環境は、Mac OSX(10.6.6)、開発言語は Objective-C を使用した。今回の実験に利用した機種は Apple 社の iPhone 3G (iOS 4.2.1) / iPhone 4 (iOS 4.2.1)である。図 10 に iPhone 4 でのアプリケーション実行例を示す。

公共の場で暗証番号 4 桁を入力する事を想定し、以下 2 種類の実験を行った。なお、被験者は 20 代前半の男女学生 6 名であり、スマートフォン利用者 3 名、未利用者 3 名である。各者、セッティング画面（図 10 左端）にて任意の暗証番号を設定し、実験に臨んだ。今回の実験では iPhone を利用したため、入力はフリック操作にて行う。図 10 の認証画面の画面中央にある十字はフリック入力時の目安である。

図 9　認証手順例

5.1 覗き見耐性

1 章で示した電車内での認証例のように、実際の覗き見攻撃を想定し、他ユーザーが操作しているのを周りから覗き見る。図 1 のように操作しているユーザーの後ろに立ち、画面を覗き見る。認証がひと通り終了した時点で覗き見できたかどうかを問う。また、ビデオカメラを用いて認証中の画面を撮影し、被験者らに見てもらい実際に暗証番号を予測できたかどうかを問う。

5.2 認証時間

認証にかかる時間を計測する。1 回認証する毎に認証時間を測定し、平均でどのくらい時間を要するかを確認する。ここで言う 1 回の認証時間とは、1 桁目の音声提示が開始されてから 4 桁目の入力を終え、「右（決定）」を入力した時点までの時間である。

6. 結果

6.1 覗き見耐性

被験者全員、画面を肩越しに覗き見るだけでは暗証番号の推測は不可能と回答した。また、ビデオカメラで撮影した映像についても、暗証番号の推測は不可能と回答した。

図 10　テストアプリケーションの実行例

左から、テストデータ設定画面、認証開始確認画面、Invisible Authentication 画面、認証成功時のメッセージ

表 1　本研究と関連研究との比較

比較項目	覗き見攻撃への耐性		覗き見による暗証番号の推測	記憶負担	平均認証時間	特記事項
	画面	操作				
本研究 Invisible Authentication	非常に強い	非常に強い	不可能	数字4桁	11.7秒	音声再生手段が必要
一般的な暗証番号入力	弱い	弱い	簡単	数字4桁	0.7秒	
高田氏による fakePointer	強い	強い	難しい	数字4桁及び回答選択情報4種	17.35秒	使い捨ての回答選択情報を事前に取得する必要がある
Roth氏らによる PIN-ENTRY METHOD	強い	強い	簡単	数字4桁	IOC 23秒 DOC 25秒	入力回数が4倍になる

6.2 認証時間

実験結果は図 11 の通りである。3 回の認証時間の平均は 11.73 秒、およそ 12 秒以下であった。また、実験を通しての最大（最遅）で 19 秒、最小（最短）で 7.0 秒であった。

7. 関連研究との比較

本提案を利用することで、音声提示によりユーザー以外の第三者が、その端末上で何が入力されているのか全く分からなくなる。また、万が一攻撃者によってユーザーの入力した値が盗まれたとしても決して外部に漏れることはない。認証の際、ユーザーは相対値のみを入力すればよく、暗証番号が画面に表示されることもない。

本研究と関連研究との比較を表 1 に示す。以下に比較した項目を考察する。なお、この表でいう「一般的な暗証番号入力」は ATM などに採用されているテンキーでの暗証番号入力を示す。fakePointer については文献[6],[7]を、Roth 氏らによる PIN-ENTRY METHOD については文献[8]を元に作成している。

7.1 覗き見攻撃への耐性

一般的な暗証番号入力は覗き見に大変弱く、入力操作を覗き見るだけで暗証番号が分かってしまう。fakePointer や Roth 氏らによる PIN-ENTRY METHOD も直接的な覗き見には強いがビデオカメラによる撮影では、暗証番号を推測される可能性がある。

本研究では、操作と音声を同時に録画・録音しない限り暗証番号は推測される心配がない。音声提示により画面には何も暗証番号を推測できるようなものは表示されず、また相対値を入力するので操作のみを覗き見されても特に問題はない。

7.2 覗き見による暗証番号の推測

他研究では、画面への覗き見攻撃と操作への覗き見攻撃が同時に行われた場合、少なからず暗証番号が推測される危険性がある。しかし、本研究では暗証番号はまったく推測されず安全な認証方式と言える。

7.3 記憶負担

本研究では一般的な暗証番号入力方式と同じく 4 桁の数値のみ記憶すればよく、fakePointer のように暗証番号以外のものを記憶する必要はない。よって、記憶の負担を増加させることなく実装できた。

7.4 平均認証時間

一般的な暗証番号入力を除く、他の関連研究よりも認証にかかる時間は平均して少ないことが分かる。ただ、図 11 から分かるように、一般的な暗証番号入力よりおよそ 15 倍かかっていることから、認証時間について今後改善する必要がある。具体的な改善方法については 7.6 章にて述べる。

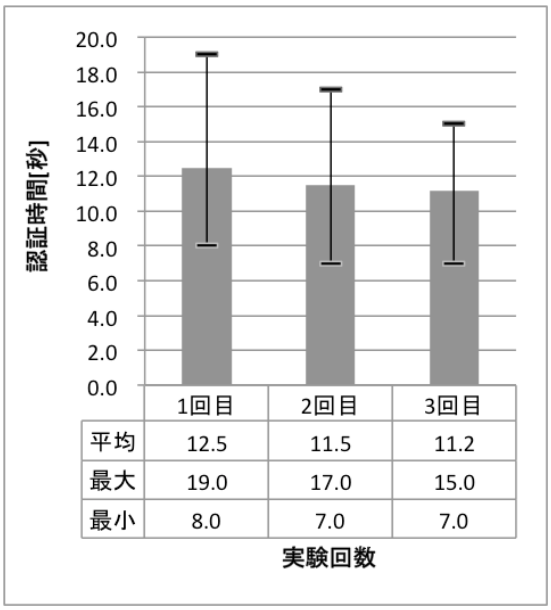

図 11　認証時間計測結果

7.5 特記事項

特記事項では、その研究における欠点を述べる。各研究にはそれぞれ一長一短あることがわかる。本研究に関しては、近年スマートフォンには音楽が再生できる機能が標準で利用できることから音声再生手段、例えばイヤーフォンやヘッドフォンは携帯しており、課題にはならないと考える。

7.6 改善点

本研究では、fakePointer のようにユーザーの記憶負担を増加させず、また Roth 氏による PIN-ENTRY METHOD と異なり、画面の表示や操作の覗き見からの暗証番号推測は、完全に不可能である。従って、本提案は覗き見攻撃に耐性がある認証方式である。

また本提案の平均入力操作回数は、理論値は一桁あたり値増減 2.5 回[1]と桁を確定する入力 1 回の合計 3.5 回、4 桁入力する 1 度の認証で合計 14 回となる。Roth 氏の提唱する PIN-ENTRY METHOD では、1

[1] 現実にあるダイヤルロックと同様に 0 から 9 の次は再び 0 に戻るようになっているため、(10/2)を入力する平均は 2.5 回となる。

桁につき 4 回の入力なので、4 桁の暗証番号を入力する際は計 16 回の入力が必要となるため、入力操作の回数も改善されたと言える。

8. 課題

テストアプリケーションを被験者に利用してもらったところ、次のような課題があった。

(1) フリック操作で入力する場合、入力が正しく行われたかどうかが分からない
(2) 素早く認証したいが、桁数の音声提示に時間がかかる
(3) 上下のどちらが値を増加し、減少するのか忘れてしまう

そこで、まず(1)については、上下の入力に対し、入力されるごとにバイブレートするようにした。また、(2)については入力している桁の音声提示をするか否かをユーザーが設定することにより改善した。ただし、(3)については、画面表示が何もなく、操作に慣れるのまでの間が問題であり、今後改善し再検証する必要がある。

9. 利用例

本研究では、携帯端末上での暗証番号 4 桁の認証についてセキュリティーの向上を図ったが、携帯端末以外にも応用できると考える。以下に 3 つの利用例を示す。

9.1 現金自動預け払い機（ATM）での利用

本提案は、ATM にも本提案は導入できると考えている。ソフトウェアの開発は必要であるが ATM には視覚障害者用の受話器が付いているものがあり、受話器を音声提示の音声再生手段として利用できるのではないかと考える。これにより、真後ろに立たれ肩越しに覗かれていても暗証番号が漏洩する危険性がない。

9.2 金庫やドアロックでの利用

現在のロックを仮想的なダイヤルロック、Invisible Authentication に置き換えることを提案する。例えば、店舗で金庫を開ける際、限られた従業員のみで金庫の開閉を行いたい場合に暗証番号を操作者以外に知られる心配がない。また、ビルの裏口にあるような暗証番号入力方式のドアロックは監視カメラに似せたビデオカメラによって覗き見られる危険性があるが、本提案を導入することにより、暗証番号の盗難を防ぐことができると考えられる。

10. まとめ

本論文で示した Invisible Authentication は、音声提示と相対値入力という 2 種類の方式を採用することにより、実証実験から覗き見攻撃に耐性のある暗証番号入力方式の一つとして有効であることを示した。音声提示が何らかの方法で記録されても、仮想的なダイヤルロックの初期値のみが再生されるため、暗証番号が攻撃者に漏れることはない。また、相対値入力では初期値が毎回異なるため、複数回操作を覗き見されても暗証番号が推測されることはない。仮想的なダイヤルロックを想定して実装した提案システムは、誰もが特別な練習なしに利用することができる利点がある。将来的に更なる安全な認証方式が必要とされ、本研究の成果はその安全性の向上に貢献できると考えられる。近年、モバイル端末における認証の強化は注目されており[9],[10]、今後それらの研究と比較し、本研究の有用性を検証する必要がある。

謝辞

本研究を行うにあたり、終始適切な助言を賜り、丁寧に指導してくださった平野学先生に感謝します。また実験にお手伝いいただいた平野研究室・神谷研究室の学生のみなさんに感謝いたします。

文献

[1] 内田薫, “携帯電話における生体認証技術,” 琉球大学総合情報処理センター広報 第 5 号, April, 2008.

[2] 平林昌志, 田辺壮宏, 松本勉, “指紋認証装置は人工指を受け入れるか（その６）,” 電子情報通信学会技術研究報告. ISEC, 情報セキュリティ 103(713), pp.151-154, March, 2004.

[3] 桜井鐘冶, 高橋渉, “モバイル個人認証方式の提案と実装,” 情報処理学会研究報告. CSEC, [コンピュータセキュリティ], pp. 49-54, December, 2002.

[4] Ross Anderson, “情報セキュリティ技術大全,” 日経 BP 社, p. 43, November, 2002.

[5] Richard E. Smith, “認証技術　パスワードから公開鍵まで,” オーム社, pp. 25-28, April, 2003.

[6] 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, September, 2008.

[7] 高田哲司, “fakePointer2: 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), 電子情報通信学会 情報セキュリティ研究専門委員会, January 25, 2007.

[8] Volker Roth, Kai Richter, and Rene Freidinger. “A PIN entry method resilient against shoulder surfing,” *In Proc. 11th ACM Conference on Computer and Communications Security*, Washington, DC, USA, October, 2004.

[9] Bianchi, A., Oakley, I., Kostakos, V., Kwon, D. S., “The Phone Lock: Audio and Haptic Shoulder-Surfing Resistant PIN Entry Methods for Mobile Devices,” *In Proc. ACM TEI 2011*.

[10] Kim, D., Dunphy, P., Briggs, P., Hook, J., Nicholson, J., Nicholson, J., Oliver, P. “Multi-touch authentication on tabletops,” *In Proc. of CHI* 2010, pp. 1093-1102.