

# 視覚障害者の暗証番号入力時におけるのぞき見防止方法の検討

榊原 直樹<sup>†1</sup>

**概要：**暗証番号を入力する際に、のぞき見を防ぐために ATM などでは番号入力の手元が見えないように衝立を設ける対策や、腕の動きから入力した番号が推測されないように、タッチパネル上にランダムに数字を割り当てたキーで入力させてのぞき見を防止する方法などが利用されている。ATM にはハンドセットが設置されており、視覚障害者は音声ガイドを頼りにハンドセットのテンキーを用いて操作する暗証番号や引き落とし額などを入力するが、背後に人が立っても気がつかない場合があり、衝立の効果が低い。またランダムなキー配列での入力は、タッチパネルを用いるため、適切なキーを選択する事ができない。

本研究では視覚障害者がのぞき見されないための方法について検討するため、視覚障害者に対してセキュリティに関する聞き取り調査を行った。また既存のハンドセットを用いたままのぞき見を防止する方法について検討し、暗証番号を加工してから入力する方法を考案した。

**キーワード：**視覚障害者、のぞき見防止、暗証番号

## Study on shoulder surfing prevention method for blind person

Naoki Sakakibara<sup>†1</sup>

**Abstract:** In order to prevent shoulder surfing when entering PIN code. A blind person is not enough with conventional shoulder surfing prevention measures. In this study, we conducted an interview survey on security concerning blind person in order to examine a method to prevent from shoulder surfing.

**Keywords:** Blind Person, Shoulder surfing, PIN Code

### 1. はじめに

様々な個人認証の仕組みが実用化されているが、現在でもなお、暗証番号やパスワードを用いた認証方式が広く使われている。生体認証の仕組みが徐々に普及してきているが、未だ置き換わるまでには至っていない。

暗証番号は手軽に利用できる反面、情報漏洩の対策が必要なことや、暗証番号を覚える必要があるために、利用者に認知的負荷がかかることになる。

暗証番号の問題の1つに、入力時にのぞき見される危険があることである。古典的なソーシャルエンジニアリングの手法として、ショルダーサーフィンやショルダーハッキングなどと呼ばれるものがある。他人が暗証番号を入力するところを、肩越しにのぞき見して、暗証番号を不正に取得する方法である。

ショルダーサーフィンを防ぐために、PC や ATM などの入力時にいくつかの対策が施されている。

PC の場合には、入力されたパスワードが他人に読み取られないように、文字をアスタリスクに変換されて、画面に表示している。

ATM では衝立を設置し、のぞき見をする不審者の視線を遮っている。また直接入力の手元を見る事ができなくても、手の動きから暗証番号を予測できるので、それを防ぐ

ために、タッチパネルに表示するテンキーの配列をランダムに変化させている ATM もある。

ショルダーサーフィンの被害にあう可能性が高い人に、視覚に障害のある人がいる。特に全盲の人の場合、のぞき見されていること自体に気がつかず、暗証番号を読み取られてしまう危険性が高い。衝立で視線を遮っても、気がつかないように近づいてのぞき見すれば、効果は低いだろう。タッチパネルを使用できない視覚障害者は、ランダム表示するテンキーを利用することができない。

現状では視覚障害者が ATM を利用するときは、機械的なテンキーを利用して暗証番号を入力するしかない。もし視覚障害者が ATM を利用しているときに暗証番号をのぞき見され、その後にクレジットカードを奪われた場合、容易に現金を引き出すことが可能になる。こうした犯罪を防ぐために、視覚障害者が安全に利用できる暗証番号の入力方法について検討する必要がある。

生体認証の普及が、のぞき見対策として有効と考えられるが、一部の生体認証は視覚障害者に利用できないものがあるため、補助的な認証方式として暗証番号が使われる可能性がある。例えば Apple の iPhoneX に搭載されている FaceID は、認証にあたって端末を注視する必要がある。これは寝ているときなどに、第3者に端末のロックを解除されないようにするためのものであるが、視線を向けること

<sup>†1</sup> 清泉女学院大学 人間学部 文化学科  
Department of Culture, Faculty of Human Studies, Seisen Jogakuin college.

ができない視覚障害者は利用できない。注視機能を解除することはできるが、セキュリティ強度は下がることになる。

また、単一の生体認証ではアメリカのリハビリテーション法 508 条の技術基準や、EU の EN301 549 などの公共調達に関するアクセシビリティ基準を満たすことができないため、複数の個人認証の方式を用意し、ユーザーに合わせて選択できるようにする必要がある。この時に暗証番号が選択肢の一つとして利用される可能性もある。こうした状況を踏まえると、暗証番号の入力時ののぞき見を防止する方法は、今後もしばらく必要な状況であると考えられる。

## 2. 視覚障害者のセキュリティ状況

視覚障害者にとって安全な暗証番号の入力方法を検討するために、まずは現状のセキュリティの利用状況について調査した。ここでは PC/スマートフォンと ATM を利用する際の暗証番号の扱いについて記述する。

### 2.1 PC

視覚障害者がコンピュータを利用する際は、画面の文字を読むことができないため、代わりにスクリーンリーダーと呼ばれるソフトウェアで、画面の文字を合成音声に変換し、耳で聞いて状況を確認する。操作のときは、カーソルの場所が見えないため、マウスは使用せずにキーボードのみで入力操作を行う。

キーボードから入力した暗証番号は、画面上では「\*」として表示されるが、スクリーンリーダーでは、設定により、文字をそのまま読み上げる場合と、画面通り「アスタリスク」と読み上げる場合がある。一般的にスクリーンリーダーの標準設定は「アスタリスク」と読み上げるようになっているため、スクリーンリーダーの読み上げた音声によって第 3 者にパスワードが漏れ聞こえることはない。

室内などで一人で使う場合やヘッドフォンを使用している場合などでは、第 3 者に聞かれる可能性が低いので、そのまま読み上げる設定にしている人もいる。

画面が表示された状態で操作している場合は、画面のパスワード入力のフォームの状態と、キーボードの操作から入力した文字を読み取ることが十分可能である。このため、全盲の人の場合、モニター画面をオフにしている使用していることがある。ノート PC の場合は、画面の輝度を最低に設定し、省電力とのぞき見の対策としている人もいる。

### 2.2 スマートフォン

視覚障害者には Apple 社の iPhone を利用している人が多い。2013 年度の調査[1]によれば、“スマートフォンについての回答者 81 人の 72.8%”と 7 割以上の視覚障害者が iPhone を利用していると回答している。この理由は Android 端末に比べ、iOS 端末の方がアクセシビリティ機能が豊富で、なおかつ洗練されており、視覚障害者にとって使いやすいたことが挙げられる。

視覚障害者にインタビューした中では、スマートフォン

の機種選定に際し、音声読み上げの機能である VoiceOver に対応したアプリが多く存在するため、iPhone を選んだとの回答があった。また iPhone X と iPhone8 を比較した結果、iPhone X は FaceID が視覚障害者にとって使いにくいと判断し、指紋認証でロックを解除できる iPhone8 を選択した人もいた。

今回のインタビューの中で、スマートフォンをのぞき見された人はいなかったが、公共の場所でスマートフォンを利用しているときに、周囲の人から見られていると感じている人は多かった。白杖を持っている視覚障害者が、見えない状態で、どのようにスマートフォンを利用しているのか、好奇心から注目するのであろう。ある人は、電車内で iPhone 利用中に画面をオフにする「スクリーンカーテン」の機能を利用していたところ、隣の人が iPhone の電源が落ちていると勘違いし、親切にモバイルバッテリーを貸してくれたというエピソードを話してくれた。これは裏を返せばスマートフォンの画面をのぞいていたことがわかるエピソードである。

### 2.3 ATM

金融庁が 2010 年に出した「視覚障がい者に配慮した取組みの積極的な推進について（要請）」[2]では、“視覚障がい者対応 ATM の増設と機能の充実(画面のコントラストの調整や操作方式をタッチパネル式ではなくボタン式にするなど)”が求められたため、ATM の視覚障害者対応が広まっている。

視覚障害者が ATM を利用する時には、付属するハンドセットを使って操作する。ハンドセットから音声による操作の選択肢が流れ、希望する操作に対応する番号を、ハンドセットのテンキーから入力する。このとき、タッチパネルは外部から操作を邪魔されないように、タッチパネルの機能がオフになり、触っても操作ができないようになるが、画面の表示は、通常の利用時と同じように操作にあわせて変化するようになっている。これは弱視の人に対して画面を見せる目的がある。弱視の場合、ATM の表示を確認するために、画面に目を近づけ過ぎて髪の毛や鼻先で画面をタッチしてしまい誤操作を引き起こすことがある。そのため、視力が残っていてもハンドセットを利用する場合がある。

画面をオフにしまえば、ハンドセットのテンキーの操作から、パスワードを読み取ることは難しい。これは、振り込みや引き落としなど、操作を指示するときに、テンキー入力をするので、どのタイミングでパスワードを入力したかを読み取ることができなくなるからである。

しかし、現状では操作にあわせて画面が切り替わるので、パスワード入力のタイミングが、のぞいている人に分かってしまう。

## 3. 対応策の検討

現状の暗証番号の入力方式では、のぞき見される危険性

があるため、本研究ではこれらの対応策について検討する。

検討にあたり、できるだけ既存の技術や設備を使ってできる対策方法について検討した。暗証番号ののぞき見対策として生体認証の利用は有効であるが、普及するまでにまだしばらく時間がかかることや、簡易な方式であれば普及が容易になるためである。

### 3.1 防止策①

画面表示をオフにして、第三者に操作の状況を見られないようにする防止策。

画面をオフにする機能は iOS などでは「スクリーンカーテン」という名称で既に実装されている。この機能を使うと、パスワードを入力するタイミングが分からないので、キーボードをのぞき見しても、どのキー入力が暗証番号に相当するのかが推測することができない。

### 3.2 防止策②

暗証番号の前後に操作に関係のないダミーのキー入力を要求する防止策。

入力する暗証番号の前後にランダムでいくつかのダミーの文字入力の操作を要求する。例えばオリジナルの暗証番号が「4567」であれば、入力する前に3文字分「123」を入力させ、最後にまた2文字分「89」と入力するように音声で指示をだす。画面にはこれまで通りに、9文字分のアスタリスクが表示されるため、のぞき見をした場合、暗証番号を入力しているタイミングを知ることができる。また、それに対応したキーボード操作をのぞき見することができる。しかしのぞき見したときに得られた番号「123456789」は、前後に不要な文字が付加されており、どの部分が本当の暗証番号かを推測することができない。システム側は不要な文字を差し引いて暗証番号を認証することが可能である。

オリジナルの暗証番号「4567」

	音声の指示	キー操作	画面表示
1	次の番号を入力してください。 1, 2, 3	1, 2, 3	***
2	暗証番号を入力してください	4, 5, 6, 7	*****
3	次の番号を入力してください。 8, 9	8, 9	***** どこからが本当の暗証番号？

画面表示に対応したキー入力を読み取っても、前後に挿入される文字の数が毎回異なれば、どの部分が暗証番号かを推測する事は難しい

図 1 防止策②の操作イメージ

### 3.3 防止策③

パスワードが数字だけの場合、ダミーの数字を足し算した結果を入力し、元の暗証番号を予測できないようにする防止策。

ヘッドセットやヘッドフォンを通じて、コンピュータが音声でダミーの数字を読み上げる。元の暗証番号に、読み

上げられたダミーの数字を足した結果を入力する。

例えばオリジナルの暗証番号が「1234」とする。入力するときに、コンピュータからランダムな数字を読み上げさせる。ここでは「7」とする。元のパスワードと、ランダムな数字を足し算した結果を入力させる。ここでは計算結果が「1241」を入力することになる。

足し合わせる元の数字はヘッドセットから提示されるので、のぞき見されることはないため、オリジナルの暗証番号をのぞき見されることはない。

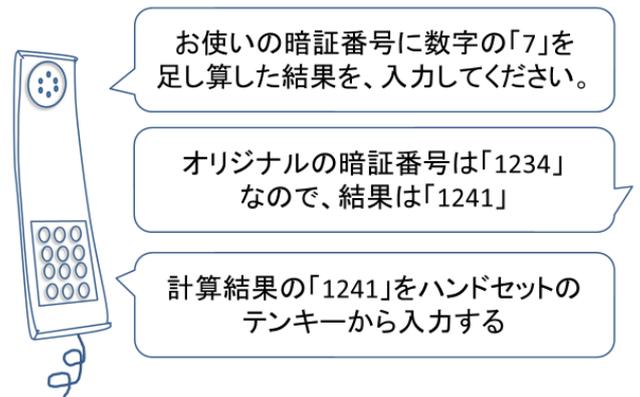


図 2 防止策③の操作イメージ

## 4. 視覚障害者による評価

検討した防止策の案の有用性を確認するために、プロトタイプを作成し、視覚障害者に評価してもらった。

### 4.1 情報提供者

今回の調査では3名の視覚障害者に協力して頂き、評価を実施した。内訳は以下の通りである。

表 1 ユーザビリティテストの情報提供者

	視力	年齢	性別	特記事項
A	弱視	30 歳代	男性	スクリーンリーダーと画面拡大を併用
B	全盲	40 歳代	男性	
C	全盲	50 歳代	男性	

### 4.2 プロトタイプ

暗証番号の入力評価のために、それぞれの防止案に関する入力画面を作成した。作成には HTML5/CSS3 を用いて、ウェブページとして作成し、視覚障害者が普段から使用している PC で表示できるようにした。パスワード入力のインタラクションは JavaScript で実装した。

作成したウェブページは、スクリーンリーダーで読み上げられるように「JIS X 8341-3:2016 高齢者・障害者等配慮設計指針—情報通信における機器、ソフトウェア及びサービス—第3部：ウェブコンテンツ」に基づき、アクセシビリティに配慮して作成した。

操作に必要な情報は音声もスクリーンリーダーで読み上げられるようにテキストを付与してある。

なお、防止策①は画面の表示全体をオフにする機能なの

で、モニターをオフにした状態で操作する前提で、通常のパスワード入力画面を操作してもらって意見を聞いたので、実際に作成したプロトタイプは防止案②と③の2つである。

#### 4.3 ユーザビリティ評価

情報提供者に3つの防止案を提示し、操作の分かりやすさや、有効性について意見を聞いた。

防止案②と③については、試作したプロトタイプを、情報提供者が普段から使用しているPCのブラウザで表示し、スクリーンリーダーで動作を確認して意見を聞いた。それぞれの回答を元に防止案の有効性について定性的な評価を行った。

##### 4.3.1 結果-防止案①

全盲の人にとっては、通常のパスワード入力の操作と同じで、使い勝手には変化がない。iOSで同様の機能が既に実装されていることから、全盲者にとっては低コストで安全を確保できる方法であると考えられる。

弱視の人の場合、画面拡大ソフトを利用するので、画面をオフにして操作することはできないとの回答であったが、ATMの操作に限定すれば、音声のみで操作できるので、画面がオフでも構わないようである。ただし音声操作ではATMで利用できるサービスが限られているので、画面と音声を併用して、通常のサービスも受けられるようになることを希望していた。また、画面がオフになった状態で操作していると、かえって目立つことになり犯罪を誘発してしまうのではないかと不安があるという回答もあった。

全盲者からは、ATMの操作は選択肢が少なく、あらかじめ操作内容と選択するキーを調べておけば、どのキーを何回押したか数えれば、パスワードを読み取ることができるという脆弱性の指摘があった。

##### 4.3.2 結果-防止案②

実際に操作する前に、操作の概要を説明した時点では、ランダムな数を入力する操作の意図が伝わりにくかった。しかし実際に操作をした結果では全員が入力を完了できた。暗証番号の前後に数字を付加したものを、一度に入力する操作だと受け取られたようである。実際の操作は、ランダムな数字の入力と暗証番号の入力は別々に行われるため、操作回数は増えるが、認知的な負荷は少ないと判断される。

この方式の脆弱性として、入力した番号を2回読み取られた場合、2つを比較すると共通する部分から暗証番号を推測することが可能なことである。ただし、2回続けて読み取られるようなときは、標的として狙われている状態なので、別の自衛手段が必要になるだろうと考えられる。

##### 4.3.3 結果-防止案③

評価の際には、4桁の数字を暗証番号として使用したが、この程度であれば暗算で対応できる範囲であるとの回答であった。全盲の人の場合、先天的な場合は暗算の習慣が付いているので問題ないが、病気などで中途視覚障害になった人には難しいかもしれないとの回答もあった。計算の場

合、元の暗証番号やランダムで提示される数字によって桁上がりが発生すると、難易度が変わってくるなどの指摘もあった。4桁の数字であれば対応できるが、これ以上桁が増えた場合には、困難になる可能性も指摘された。

この方式は、平文の暗証番号を読み取ることができないので、他の方式より脆弱性の低い方式と言えるが、計算による認知的負荷がかかるため、ユーザビリティとのトレードオフが発生する。また、文字を使ったパスワードでは使えないなどの欠点がある。

#### 4.4 結果の総評

3つの方式を比較し、使いやすい順位を付けた場合、3名が皆②の方式がもっとも使いやすいと答えた。ただし4桁の数字に限定するという条件付きであれば全盲の2名は③の方式がよいと回答した。理由としては、キー操作が増えることで、人を待たせてしまうのではないかと思うからというものであった。

①の方式の評価が低いのは、利用する場面によって向き不向きがあるので、必要に応じてオンオフを切替えられるとよいとのことだった。

#### 5. まとめ

視覚障害者にとって安全であり、なおかつ低コストで対策ができる方法について検討した。既存の端末に大きな変更を加えなくても利用可能な方法として3つの方式を考案し、ユーザビリティ評価を行った。いずれの方法も利用可能であったが、長所短所があり使用場面を検討して用いる必要があった。

今後は、調査結果を元に、更にユーザビリティの高いセキュリティの方式について検討する。また情報提供者の人数が少なかったため定性的な調査としたが、人数を増やして、改めて定量的な比較を実施したい。

ヒアリングでは暗証番号の入力以外にも、セキュリティに関する問題について、ウィルススキャンソフトのアクセシビリティ対応や、ロボットによるアクセス防止のためのCAPTCHAの問題など、数多くの問題点の指摘を頂いたので、それらについても検討を進める。

#### 謝辞

本研究にご協力頂いた視覚障害者の方に感謝の意を表します。

#### 参考文献

- [1] 渡辺哲也,山口俊光,南谷和範. 視覚障害者の携帯電話・スマートフォン・タブレット・パソコン利用状況調査2013,新潟大学学術リポジトリ.
- [2] “視覚障がい者に配慮した取組みの積極的な推進について(要請)” <https://www.fsa.go.jp/news/22/ginkou/20100826-1/01.pdf>, (参照 2019-08-20)