筑波大学大学院博士課程

システム情報工学研究科修士論文

振動を用いた安全なPIN入力システム

栗原 拓郎

修士（工学）

（コンピュータサイエンス専攻）

指導教員　志築 文太郎

2015年3月

概要

コンピュータ機器の多くは、認証システムによってユーザの機密データやサービスを守っている。この認証システムをユーザが用いる際、ユーザは特定のデータ（パスワード）をシステムに与え、システムはそのパスワードがあらかじめ設定されていたものと同一であるか確認し、同一であればユーザの情報へのアクセスを許可する。ユーザがシステムに対してパスワードを与える際、このパスワードを盗み見られる（ショルダーサーフィン）危険がある。特に、電車内など周囲に人が多くいる公共の場において利用されることも多い携帯情報端末にはこの問題が顕著となる。この問題を解決するために、本研究では、携帯情報端末の振動パターンと視覚情報を元に PIN 入力を安全に行うシステムである VibraInput を開発した。 VibraInput ではランダムに提示される 4 種類の振動パターンに対応する記号を入力したい数字に合わせる行為を 2 回行うことによって PIN 入力を行う。4 種類の振動パターンのみを使用するため、ユーザは簡単にパターンを覚えられ、識別することができる。また、本システムは既存の携帯情報端末が備える振動モータのみを用いて十分に実現することができる。振動パターンは目視では確認することができないため、ショルダーサーフィンを行う攻撃者は、ユーザの入力を知ることができない。本論文では、VibraInput の設計を行った後に、人が識別しやすい振動パターンを調査し、その結果を元に 2 種類の VibraInput のプロトタイプを Android アプリケーションとして実装した。また、これらのプロトタイプを用いて 4 桁の PIN 入力の容易性を調べる実験および安全性に関する実験を行った。 その結果、平均認証成功率は 96.0%と高く、ショルダーサーフィンに対しても安全であった。また、これらの実験（予備調査）から得られたフィードバックを元にシステムの改良を行い、評価実験を行った。その結果、平均認証成功率は 95.6%と予備調査とほぼ同じであり、平均認証時間は 23.8 秒から 20.1 秒に改良された。また安全性に関する実験では、ビデオ録画によるショルダーサーフィンの実験も行い、これらに対しても安全であることを確認した。

目 次

図目次

表 目 次

第1章　序論

コンピュータ機器の多くは、認証システムによってユーザの機密データやサービスを守っている。この認証システムをユーザが用いる際、ユーザは特定のデータ（パスワード）をシステムに与え、システムはそのパスワードがあらかじめ設定されていたものと同一であるか確認し、同一であればユーザの情報へのアクセスを許可する。本研究ではこの認証の流れのうち、ユーザがパスワードをシステムに与える部分を対象にする。本章では、最初に現在の認証手法を述べ、次に認証システムとその危険性を述べる。そして、危険性の 1 つであるショルダーサーフィンを述べ、現在のショルダーサーフィンへの対策とその問題点を述べる。最後に、本研究の目的と本研究の貢献を述べる。

1.1　認証手法

現在使われている認証手法として、パターンロック認証、生体（バイオメトリクス）認証、および PIN（Personal Identification Number）認証がある。

パターンロック認証（Gesture Pattern Lock）[MT11] とは、Android 端末に標準搭載されている認証手法である。パターンロック認証では、ユーザは 4 個以上 9 個以下の点を、任意の順になぞることにより認証を行う。この際、同じ点は 2 度選択できず、また途中で指を画面から離さず一筆書きで行う。PIN 認証と同様に、システムはユーザの入力したパターンがあらかじめ登録されているパターンであるか比較を行い、同一であればユーザの情報へのアクセスを許可する。パターンロック認証では、ユーザは点をなぞるだけという手軽な入力にて認証を行うことができるが、使用環境がタッチパネル上に限定される。

生体認証とは、人間の身体的な特徴情報を用いて行う手法である。例として網膜認証や、指紋認証がある。他の認証と同様に生体認証においても、システムはユーザの生体情報があらかじめ登録されているものか比較を行い、同一であればユーザの情報へのアクセスを許可する。生体認証は他の 2 つの認証と比べ、ユーザがあらかじめ覚えておく必要のある情報が少ないという利点がある（例えば、パターンロック認証ではパターンを覚えておく必要があり、PIN 認証では数字を覚えておく必要がある）が、認証システムに加えて生体情報を取得するための特殊なデバイスが必要となる。

PIN 認証とは、0 から 9 までの数で構成された数字を用いた認証であり、銀行の ATM 等に用いられる。PIN 認証では、ユーザはあらかじめ設定されている桁数の数字を入力し、システム側はその数字が登録されている数字と同一であるか比較を行う。同一であればユーザの情報へのアクセスを許可し、同一でない場合、アクセスを許可しない。この PIN 認証はスマー

トフォンに代表される携帯情報端末においても使用されている。パターンロック認証や生体認証に比べて PIN 認証は利用される環境が多いため、本研究ではこの PIN 認証を対象とする。

1.2 認証システムとその危険性

認証システムによってユーザの機密データやサービスを守っているコンピュータ機器の 1 つに、ATM などの金融端末がある。この金融端末には PIN 認証が用いられており、ユーザは 4 桁の PIN 入力を認証システムから求められる。この金融端末では不正が行われることも多く、例えばアメリカにおいては年に 6000 万ドルの不正が起こっている [Gie06]。この不正の原因の 1 つに、ユーザが認証システムを用いてパスワードを入力する際、その入力を盗み見る攻撃（ショルダーサーフィン）がある [TOH06, DLvZH09]。ショルダーサーフィンとは、ユーザのパスワード入力の様子を覗き見ることによってそのパスワードを不正に取得する攻撃である。

図 1.1: ショルダーサーフィンの例。

ショルダーサーフィンは、金融端末だけではなく、ユーザのパスワード入力が求められる多くの環境において行われる危険がある。例えば、ユーザはパソコンや携帯情報端末から Facebook などの SNS へログインする際、パスワードの入力が求められる。このショルダーサーフィンは、フィッシング [DTH06] 詐欺のようなソーシャル・エンジニアリング攻撃にも応用される危険がある。

1.3 ショルダーサーフィンへの対策

ショルダーサーフィンへの対策として、いくつかの Web サイトでは、ユーザが入力したパスワードがマスクされて表示される。この手法は、ディスプレイのみが盗み見られる環境においては有用であるが、ショルダーサーフィンを行う人物（攻撃者）がユーザの手元も盗み見た場合、キーボードを用いてパスワードを入力する際のユーザの指の動きから、ユーザのパスワードが盗み見られてしまう危険がある。

また、他のショルダーサーフィン対策として、攻撃者の覗き見を困難にする手法もいくつか提案されている。たとえば、入力部分を箱の内部に配置する手法 [松下 01]、入力部分および手を覆うに不透明のカバーを設け、入力部の上方以外の覗き見を防ぐ手法 [伸洋 01]、入力部分の側面および上面をカバーで覆うことにより、操作者も含めて覗き見を防ぐ手法 [日立 08]、並列する複数の傾斜面で入力部を覆うことにより、上部も含めて覗き見を防ぐ手法 [沖電 12]、ユーザの入力中に二人以上の視線を検知した際に入力処理を停止する手法 [日本 06] などがある。これらの手法は一定の効果が認められるものの、完全に攻撃者の覗き見を防ぐことはできず、またシステムが使用される環境も限定される。

1.4 本研究の目的

本研究の目的は、パスワード入力の際にショルダーサーフィンに対して安全な PIN 入力システムを示すことである。このシステムにおいては、攻撃者の覗き見を困難にするのではなく、覗き見はされることを前提として安全性を確保する。特に、公共の場において使われることが多く、かつ多くのセキュリティ上のリスクがあることが指摘されている [BAKS$^+$11, KBS09]、携帯情報端末を対象とする。この際、既存の携帯情報端末に追加のデバイスを加えることなく実現できる入力システムを示し、その入力の容易性、安全性を調べて有用性を示すことも本研究の目的である。

1.5 本研究における用語の定義

本研究における携帯情報端末とは、スマートフォンなどのタッチパネル搭載端末であると定義する。また、ショルダーサーフィンを行う人物を攻撃者と定義する。

1.6 本研究の貢献

本研究の貢献は以下の通りである。

- 振動情報と視覚情報を組み合わせたショルダーサーフィンに対して安全な PIN 入力システムを示した。

- 振動情報と視覚情報を組み合わせることにより、入力したい数字を絞り込んでいくという入力手法を示した。
- ユーザが感じることのできる振動パターンを調査し、それに基づいた 2 種類のプロトタイプシステムを示した。
- 評価実験により、本システムがショルダーサーフィンに対して安全であることを示した。

1.7 本論文の構成

本論文においては、最初に第 2 章にて関連研究の分析を行い、本研究の位置づけを述べる。第 3 章では、提案する入力システムである VibraInput の設計を示す。第 4 章にて本システムの予備調査を示し、第 5 章では第 4 章の結果を元に改良したシステムを述べる。第 6 章にて評価実験を述べ、第 7 章にて実験結果を元に議論する。最後に第 8 章にて結論を述べる。

第2章　関連研究

本章においては、本研究に関連する従来研究を述べる。最初に認証の種類による分類を行う。その後、本研究では追加のハードウェアを必要としない振動を用いた安全な PIN 入力システムを提案しているため、追加のハードウェアを必要とない認証手法および、振動を用いた認証手法に関する関連研究を述べる。最後に本研究の位置づけを述べる。

2.1　認証の種類による分類

本節では、数多くの研究が行われており、かつショルダーサーフィン対策についての研究も行われている認証手法として、画像認証、パターン認証、生体認証を述べる。

2.1.1　画像認証

アルファベットよりも画像の方が覚えやすい [Yui83] ことから、画像を用いた認証の研究は数多く行われており、Biddle らが画像認証の研究に関する調査報告を述べている [BCVO12]。武田らはお気に入りの絵を決めておき、画像セットの中からその絵を選ぶ認証システムを示した [TK03]。Dunphy らは携帯情報端末において画像認証システムに関する大規模な実験を行った [DHA10]。また、ショルダーサーフィンへの対策を行った研究もいくつか存在する [WWSB06, Wei06] が、これらの手法では複数回ショルダーサーフィンを行うことによってパスワードが攻撃者に盗み見られるという問題がある。

2.1.2　パターン認証

Draw-a-Secret[JMM+99] はストロークによる認証として初めての研究であり、この手法を改良した研究もいくつか存在する [DY07, SZO05]。これらの手法は、手軽である反面、ショルダーサーフィンに弱いことが指摘されている [AAIM08]。そこで、携帯情報端末の背面をなぞることにより指の動きを隠し、ショルダーサーフィン対策を行う研究 [DLHvZ+14, DLvZN+13] も行われている。ただし、これらの研究は実装に特殊なハードウェアを用いる、あるいは 2 台の携帯情報端末を組み合わせている。さらに、パターン認証には、携帯情報端末の表面を指にてなぞった際にできる汚れからパターンを知られてしまう “Smudge attack”の危険も存在する [AGM+10]。

2.1.3 生体認証

画像認証やパターン認証では、ショルダーサーフィンに対して安全性を保てないため、De Luca らはパターン認証と共に、タッチパネル上のユーザのタッチの動きを利用した認証システムを示した [DLHB+12]。このような生体認証として、ユーザのネットワークへのアクセス方法およびファイルシステムの利用方法を用いた認証 [YCDS09]、足に取り付けたセンサの加速度を用いて足の動きを取得し、それを用いた認証 [GHS06] がある。また、Aumi らは空中でうごかす手の動きを距離センサにて検知することによって認証するシステムを示した [AK14]。このように、身体動作を用いた研究は他にもいくつか提案されている [PPA04, CM09, MG09]。さらに、生体認証の中には、ユーザが動かすマウスの動きを用いた認証 [JY11] やユーザのキーストロークを用いた認証 [CF06]、タッチパネル上での指の動きを用いた認証 [居城 13, 井芹 11] も存在する。これらの認証手法は、ショルダーサーフィンに対して耐性がある一方、あらかじめ生体情報を登録する必要がある。

2.2 追加のハードウェアを必要とない認証手法

追加のハードウェアを必要とない認証手法の研究は数多く行われている。

渡邉ら [渡邊 13] や Luca ら [DLvZPH13] は、複数のカーソルを用いたパスワード入力を示した。これは、複数のダミーカーソルを表示することによって、マウスの操作者は自身が操作するカーソルを見つけられるものの、攻撃者は操作者が動かしているカーソルを特定できず、その結果何を入力しているかがわからなくなるという手法である。また、Spy Resistant Keyboard[TKC05] はキーの配置をランダムにしたソフトウェアキーボードによるパスワード入力手法である。キーボードには 3 つのシンボルが割り当てあられており、シフトキーによりユーザはどのシンボルを入力するか決定する。その後、カーソルを入力したいキーまでドラッグする。ドラッグすると、キーボードに表示されているキーの表示が消えるため、他者にはドラッグして到達した位置にどのような文字があったかわからない。テキスト入力を用いたパスワードは未だに数多いことも報告されており [HvOP09]、これらのシステムは PIN のみではなく、テキストによるパスワードにも対応している。Roth ら [RRF04] は、入力したい数字の背景色を複数回選択することにより数字を入力する手法を提案している。これらの研究では、一度見る覗き見攻撃に対しては有効であるものの、録画して見直すことにより、パスワードを識別することができる。一方本研究では、攻撃者に入力の様子を複数回見られたとしても安全に PIN を入力することができる。

高田 [高田 08, 産業 08] は入力の様子が録画されたとしても安全な入力手法を提案している。これは、ランダムに生成された情報をユーザがあらかじめ覚えておき、その情報を入力したいキーに合わせることによりパスワード入力を行うという手法である。この手法ではあらかじめ情報を覚えておく必要があり、また覚えていた情報が知られた場合に見破られるという危険がある。一方、本研究では振動情報と視覚情報を併用してショルダーサーフィンへの対策を行う。これにより、ユーザは録画に対しても安全にパスワードを入力することができ、かつあらかじめ攻撃者に知られてはいけない特定の情報を覚えておく必要がない。

2.3 振動を用いた認証手法

振動を用いる認証手法はいくつか研究されている。

追加のデバイスに振動センサを埋めこみ、パスワードを入力する手法として、ホイール型のデバイスに埋め込む研究 [BOLK10] やキーボードに埋め込む研究 [BOK10] がある。これらの研究と異なり、本研究では携帯情報端末の振動パターンのみを利用する。

携帯情報端末とパスワード入力を必要とする端末を組み合わせた手法として VibraPass[DLvZH09] がある。この研究では、ATM などの端末において PIN 入力を行っている際に、ポケットに入れておいた携帯情報端末が振動した場合、偽の PIN を、起こらない場合は本当の PIN を入力する。この研究に対し、本研究では振動パターンを元に PIN 入力を行う.

Phone Lock[BOKK11] は携帯情報端末をなぞる動作と振動を組み合わせることによってショルダーサーフィン対策を行っている。この手法では 10 種類の振動パターンが 10 箇所に割り当てられており、指を移動させるとその区画ごとに異なる振動パターンが発生する。ユーザは自身が探していた振動パターンを感知した時に指を中央に動かしてその振動パターンを選択する。なお、この振動パターンと区画の対応は選択が終了する度にランダムに変化する。Spinlock[BOK11] も同様に振動を組み合わせているが、Phone Lock に比べて使用する振動パターンの種類を減らしている。これらの研究では、携帯情報端末に外部の振動モータを取り付けているため、内蔵された振動モータを用いた場合の安全性については未確認である。

また、石塚らは携帯情報端末に内蔵された振動センサを用いてパスワードを入力する手法を示した [石塚 14]。この研究では、認証開始時にインジケータが回転し、9 箇所ある特定の数字マスにインジケータが到達すると携帯情報端末が振動する。この振動が発生するマスはランダムになっており、ユーザはその位置に入力したい数字を合わせることによって PIN を入力する。この研究では、9 箇所ある特定の数字マスをインジケータが通り過ぎるのを待つ必要があるため、4 桁の PIN 入力に平均 34 秒の時間がかかる。一方、本研究では振動を用いて入力したい数を絞り込んでいくため、石塚らの研究と異なり振動を待つ必要が無く、素早く PIN を入力することができる。

2.4 本研究の位置づけ

本研究では、記号を選択するシステムを提案しているため、ユーザが普段使用している認証の入力に置き換えることができる。すなわち PIN 認証における PIN の選択や、画像認証における画像の選択に本システムを利用することが可能である。また、本システムの実装方法によっては、パターン認証のようになぞる入力を必要とせず、さらに、生体認証のようにあらかじめ生体情報を登録する必要もない。

本研究では、携帯情報端末の振動情報を用いているため、あらかじめ知られてはいけない情報を必要とせず、一回の覗き見だけではなく録画に対しても安全な入力システムを示している。また、この振動には振動携帯情報端末に内蔵された振動モータを用いているため、追加のハードウェアを必要としない。さらに、振動情報と視覚情報を用いて入力したい数を絞り込んでいくため、石塚らの研究と異なり振動を待つ必要が無く、素早く PIN を入力できる。

第3章　VibraInput：振動情報と視覚情報を組み合わせた安全なPIN入力システム

本章においては提案システムである VibraInput を述べる。VibraInput においてはランダムに提示される 4 種類の振動パターンに対応する記号（正しいカーソル）を入力したい数字に合わせる行為を 2 回行うことによって PIN 入力を行う。4 種類の振動パターンのみを使用するため、ユーザは簡単にパターンを覚えられ、かつ識別することができる。また、本システムは既存の携帯情報端末が備える振動モータのみを用いて十分に実現することができる。本章では、最初に安全な PIN 入力の要件について述べ、次に VibraInput の設計方針を述べ、最後に入力手法について述べる。

3.1　安全な PIN 入力の要件

本節では、ショルダーサーフィンに対して安全な PIN 入力の要件を述べる。ここでは、本システムのデザインモデルの参考にした、金庫などに用いられるダイヤル式暗号を例に説明する。最初にショルダーサーフィンに対して安全ではないダイヤル式暗号を述べ、次に、ダミーカーソルを持つダイヤル式暗号について述べる。最後に、これまでの例を元に、安全な PIN 入力を実現するための仕組みを述べる。

3.1.1　ショルダーサーフィンに対して安全ではないダイヤル式暗号

ショルダーサーフィンに対して安全ではない、通常のダイヤル式暗号を図 3.1 に示す。図 3.1a が初期状態であり、ここから図 3.1b のようにユーザがカーソルを右回りに数字 3 つ分回転させたとする。この時、ユーザはカーソルが 9 にあるため、9 が選択されるのが分かる。また同時に、ショルダーサーフィンを行う攻撃者も、カーソルが 9 にあることが目視できるため、9 が選択されることが分かる。そのため、このシステムではショルダーサーフィンに対して安全では無い。

3.1.2　ダミーカーソルを持つダイヤル式暗号

ダミーのカーソルがあるダイヤル式暗号を述べる。図 3.2 にダミーカーソル付きのダイヤル式暗号を示す。数字の周りに円形に配置された 10 種類の数字のうち、9 種類がダミーカー

図 3.1: ダイヤル式暗号。a）初期状態、b）カーソルを 3 個分動かして 9 を選択した状態。

ソルであり、1 種類が正しいカーソルである。図 3.2a が初期状態であり、ここから図 3.2b に示すようにユーザがカーソルを右回りに数字 3 つ分回転させたとする。ここでユーザが「@」が正しいカーソルであると知っていた場合、ユーザには「@」が指し示す 5 が選択されたのが分かる。しかし攻撃者はカーソルが全ての位置にあるように見えるため、何が選択されているかわからない。そのため、このシステムでは「どの数字が選択されているか」を攻撃者に対して隠すことができる。

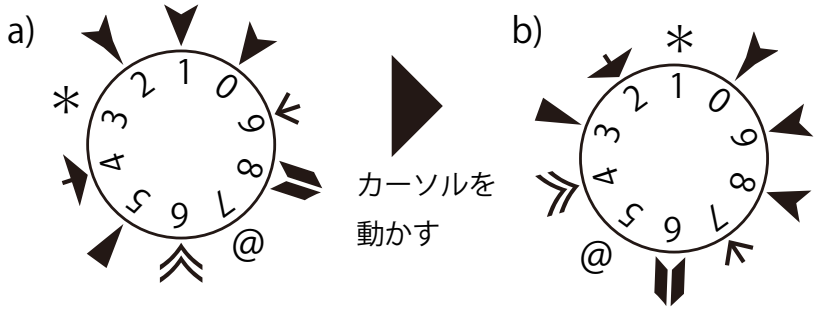


図 3.2: ダミーカーソル付きのダイヤル式暗号。a）初期状態、b）カーソルを 3 個分動かした状態。

しかし、図 3.2 の例では、攻撃者は目視によって「カーソルを右回りに数字 3 つ分回転させた」という情報を知ることができる。ダイヤル式暗号では、正しいカーソルを正しい数字に合わせることによって暗号を解除できる。そのため、攻撃者はどの数字を入力しているかわからなかったとしても、「カーソルを右回りに数字 3 つ分回転させる」ことによって、正しいカーソルが正しい数字に合ってしまい、暗号を解除されてしまう危険がある。そこで、図 3.3a に示すようにカーソルの位置を毎回変更することや、図 3.3b のように、数字の位置を毎回変更するという解決案が考えられる。これにより、攻撃者はカーソルの移動量を知ることができたとしても、同じ移動量によって正しいカーソルが正しい数字に合うとは限らないため、暗号を解除することができない。よって、攻撃者がユーザの入力の様子を 1 度しか確認しないと仮定した場合、攻撃者はユーザの数字を盗むことができず、ショルダーサーフィンに対して安全であると言える。

しかし、暗号は何度も入力されるものであるため、図 3.3 の解決案であっても複数回入力

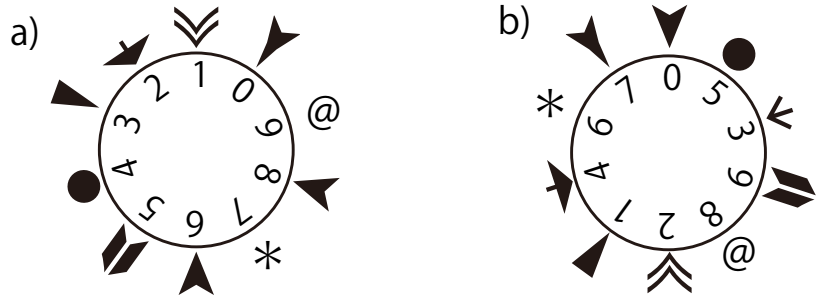


図 3.3: ショルダーサーフィン対策を行ったダミーカーソル付きダイヤル式暗号。a）ランダムなカーソル配置、b）ランダムな数字配置。

の様子を見られてしまうと、「このカーソルは毎回この数字を指している」という情報が知られてしまう。図 3.4 のように、数字配置が毎回ランダムに変わるシステムを例に解説する。この例では、ユーザは正しいカーソルである「＊」を正しい数字である「5」に毎回合わせている。この時、カーソルの移動量はそれぞれ「右に 1」、「右に 4」、「右に 6」と毎回異なっているため、攻撃者はカーソルの移動量だけでは正しいカーソルと正しい数字を知ることはできない。しかし、これらの入力では、攻撃者は毎回「＊」が「5」を指していることが分かるため、カーソルが「＊」であることおよび、ユーザが入力している数字は「5」であることが分かる。そのため、このシステムは複数回目視による攻撃に対して安全ではない。

この問題は、正しいカーソルが毎回固定であるために起こるものであるため、カーソルが毎回ランダムであればこの問題を解決することができる。

3.1.3 正しいカーソルを伝える手段

第 3.1.2 節の例にて述べたように、ダイヤル式暗号に限らず、正しいカーソルが入力のたびに変わることによってショルダーサーフィンへの耐性を持つ入力となる。本節では、ショルダーサーフィン対策として、入力の度に変わる正しいカーソルを、ユーザにのみに伝える手段を示す。

ショルダーサーフィンに対して安全なシステムのフローチャートを図 3.5 に示す。ここで、図 3.5a の部分を攻撃者に知られなければ、図 3.5b が攻撃者に知られたとしてもパスワードを安全に入力することができる。すなわち、ショルダーサーフィンできない情報を（a）にてユーザに与え、（b）にてユーザは入力したい数字にカーソルを合わせれば良い。この（a）の部分の正しいカーソルを伝える手段として、本システムでは振動情報を用いる。振動情報とは、携帯情報端末に搭載されたバイブレーション機能を用いてユーザに提示する振動のことである。バイブレーションのパターンを変えることによってユーザに「正しいカーソル」を提示し、ユーザは視覚情報を元に、正しいカーソルを入力したい数字に合わせる。振動情報は見ていてもわからないため、攻撃者は正しいカーソルを知ることができず、数字を盗むことができない。

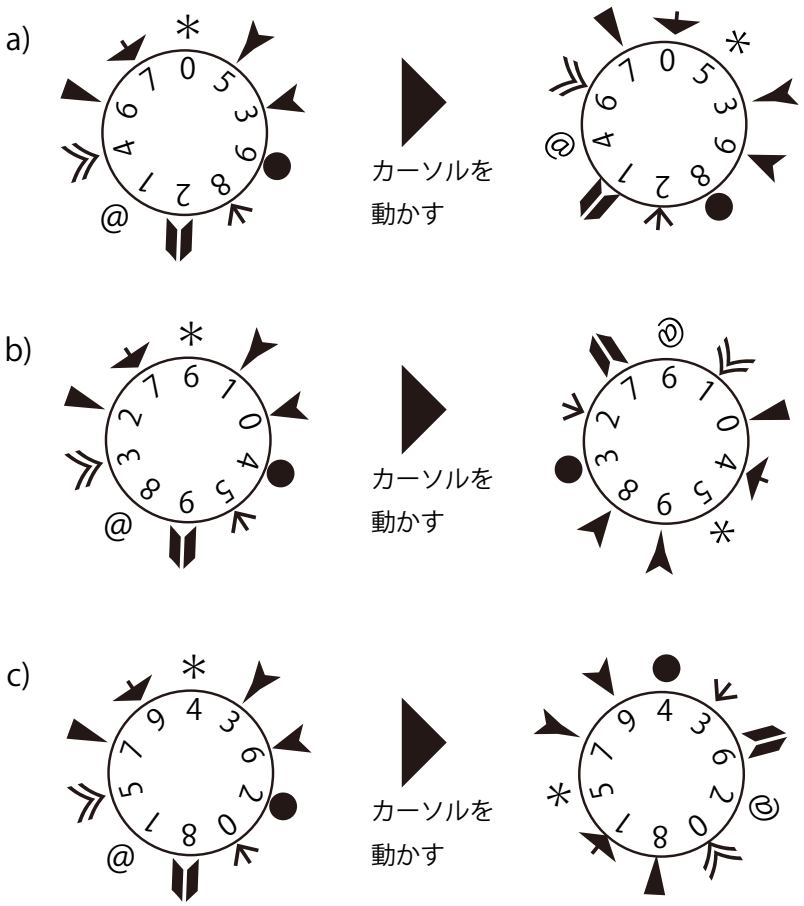


図 3.4: ランダムな数字配置によるダミーカーソル付きダイヤル式暗号。a）1 回目の入力、b）2 回目の入力、c）3 回目の入力。これらの入力では「＊」が毎回 5 を指していることが分かる。

3.2 設計方針

VibraInput では、ユーザは携帯情報端末上の振動を用いて PIN 入力を行う。ここで、振動パターンを 10 種類用意し、それぞれの数字に対応させて入力させることも考えられるが、ユーザに 10 種類の振動パターンを覚えてもらうことは難しいと考えられる。また、携帯情報端末に内蔵されている振動モータは、特殊なハードウェアに比べて様々な振動パターンを生み出すことが難しい。そこで本研究では少ないパターンに基づく入力を組み合わせることにより 10 種類の入力を行う方針をとることにした。

10 種類の入力を行うために必要な振動パターンを述べる。2 種類の振動パターンを組み合わせた場合、$2^4 > 10$ となるため、4 回入力する必要がある。同様に、3 種類では 3 回、4 から 9 種類では 2 回の入力が必要になる。そこで本システムでは 2 回の入力であればユーザに対して大きな負担にならないと考え、2 回の入力にて数字入力が行える最低の数である 4 種類の振動パターンを組み合わせることにより PIN 入力を行うこととした。

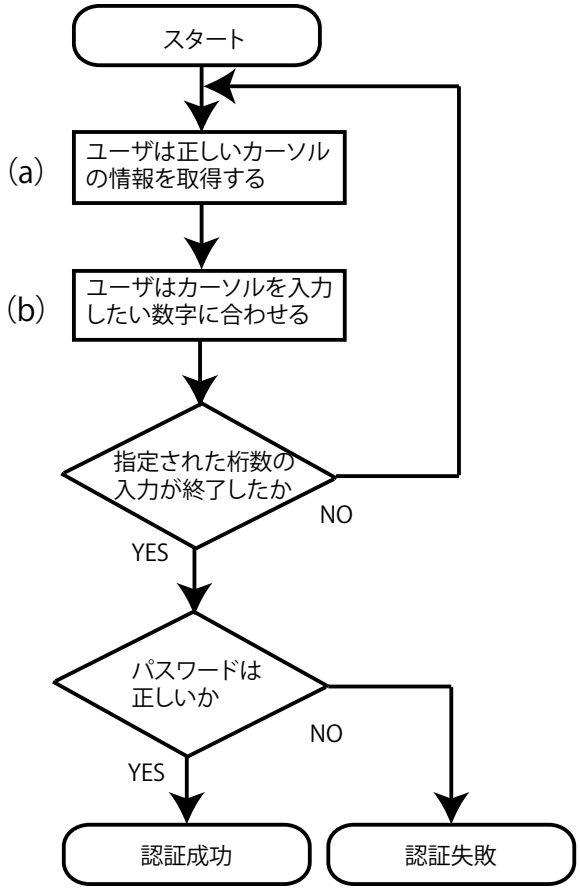


図 3.5: 認証の流れ。(a) の部分を隠すことにより、(b) を知られたとしても安全にパスワードを入力できる。

VibraInput では入力したい数字を 1 回目の選択により絞り込み、2 回目の選択により決定するという手法をとる。すなわち、2 回の入力によって 1 つの数字を入力する。つまり、図 3.5b にあたるユーザがカーソルを入力したい数字に合わせる部分を 2 回行うことになる。また VibraInput では図 3.5a にあたる、ユーザが正しいカーソルの情報を取得するために、振動情報と視覚情報を用いる。VibraInput では、振動パターンと記号の対応が攻撃者に知られたとしても入力している数字が見破られることはない。何故ならば振動パターンが分からなければ入力している数字を見破ることができないためである。

図 3.6 に本システムの認証の流れを示す。図 3.6a にて数字を絞り込み図 3.6b にて数字を決定する。

3.3 入力手法

本システムを使用する前提として、ユーザは自身の入力したい数字を覚えており、携帯情報端末が提示する 4 種類の振動パターンを知っているものとする。

入力方法を図 3.7 に示す。ユーザは携帯情報端末の振動を感知し、4 種類の振動パターンに対応する記号（図 3.7 ではアルファベット）のうち、現在の振動パターンを表す記号を入力したい数字に合わせることによって数字を入力する。

1 回目の入力の際に 4 種類の振動パターンのいずれかがランダムに発生する。図 3.7b に示すように、最初にユーザは円を回転させることによって現在の振動パターンを示す記号を入力したい数字がある位置に移動させる。図 3.7c に回転が完了した様子を示す。ユーザはこの状態になった時に、2 もしくは 3 個の数字のいずれかを選択した状態になる（例えばこの時の振動パターンが A であれば、1 もしくは 5 である）。攻撃者は記号と数字の対応は分かるものの、どの記号を合わせているか分からない。これはどの振動であるかを示す振動パターンを知ることができないためである。入力を確定させると振動が終了し、2 回目の入力に状態が遷移する。

2 回目の入力の際にも 4 種類の振動パターンのいずれかがランダムに発生する。図 3.7e に示すように、ユーザは 1 回目と同様に現在の振動パターンを示す記号を入力したい数字がある位置に移動させる。この時、記号の配置は図 3.7a とは異なり、1 回目の入力と 2 回目の入力を合わせて一意に数字を決定できる位置となる。図 3.7f に回転が完了した様子を示す。入力を確定させると振動が終了し、数字が確定する。(この時の振動パターンが D であれば、先ほどの結果と合わせて 1 に確定される)。なお、1 回目と同様に、ユーザ以外の人はどの記号を合わせているか分からないため、入力された数字を見破ることはできない。

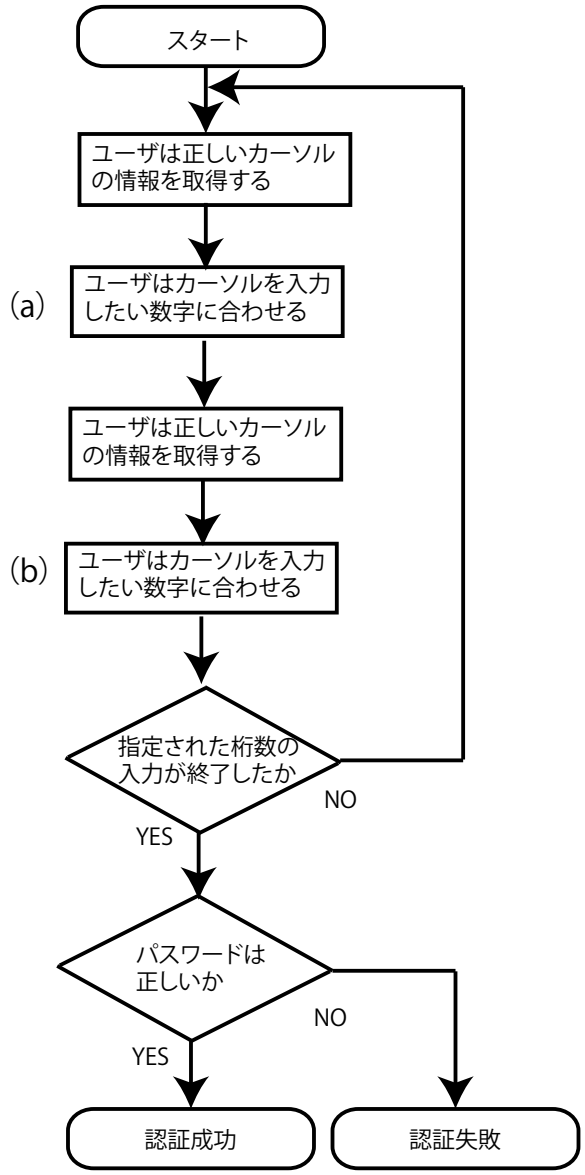


図 3.6: VibraInput の認証の流れ。(a) にておおよその数字を絞り込み、(b) にて入力する数字を決定する。

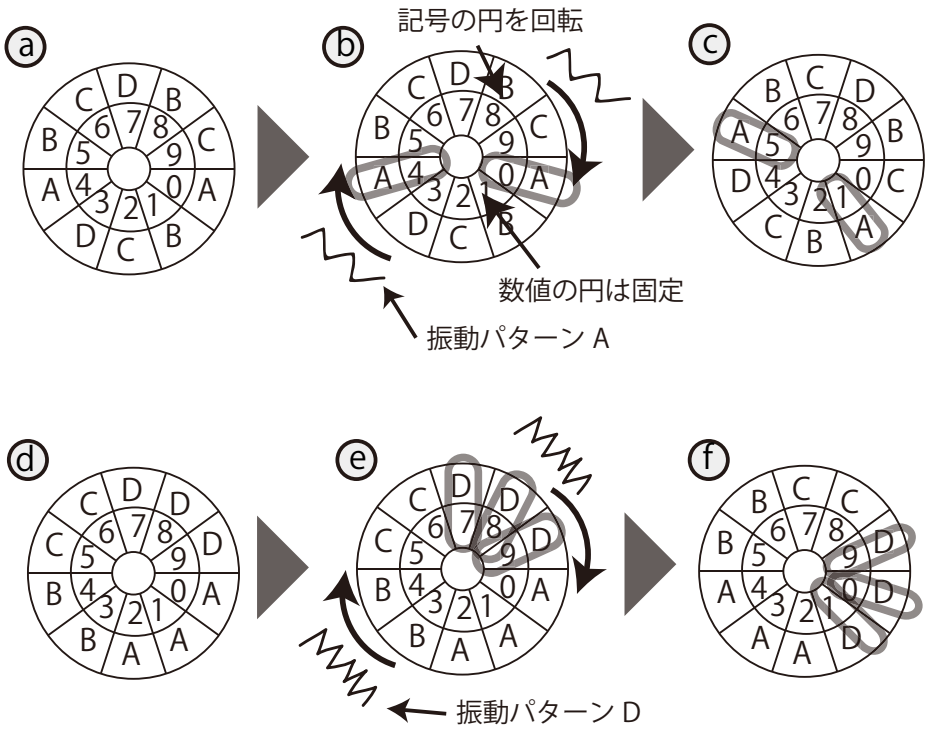


図 3.7: 入力方法（1 を入力する例）。a）1 回目の初期状態。b）ユーザがタッチすると振動が開始される。ユーザは携帯情報端末の振動パターンに対応する記号 A を 1 に合わせる。c）リリースにより入力候補（1、5）が確定し、d に状態が遷移。d）2 回目の初期状態。e）振動が開始される。ユーザは携帯情報端末の振動パターンに対応する記号 D を 1 に合わせる。f）リリースにより 1 が確定し、状態は a に遷移。

第4章　予備調査

本章では最初にユーザが識別しやすい振動パターンの調査を述べ、それを元に作成した VibraInput のプロトタイプ 1 とその評価を述べる。なお、この予備調査に使用した書類は付録 A として添付する。

4.1　予備実験 1：ユーザが識別しやすい振動パターンの調査

ユーザが識別しやすい振動パターンを調査する予備実験 1 を行った。今回、振動パターンとして、最も単純なパルス状の振動を用いることとした。使用する振動パターンを図 4.1 に示す。パルス状の振動を表現するために、振動の ON/OFF を切り替える間隔（これを振動間隔と呼ぶ、図 4.1 中の A）を 6 種類用意し、どの程度の間隔であればユーザが識別することができるか、またその識別速度を調べた。

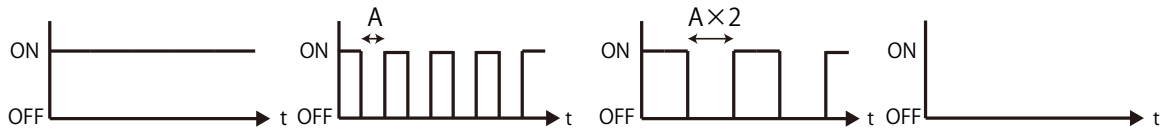


図 4.1: 使用する振動パターン。左から ON、Short、Long、OFF。

4.1.1　被験者

22 歳から 24 歳までの大学生、大学院生のボランティア 8 名（男性 8 名）を被験者とした。被験者には携帯情報端末を自由に把持してもらった。

4.1.2　実験設計

実験には Android 2.3.4 を搭載した Google Nexus S を携帯情報端末として用いた。被験者には図 4.2 に示すように椅子に座り、携帯情報端末を把持してもらった。

被験者がスタートボタンを押すと実験が開始され、4 種類の振動パターンのいずれかがランダムに開始される。被験者には振動パターンを識別してもらい、対応するボタンをできるだけ正確に、また正確さを失わない程度に素速く押してもらった。

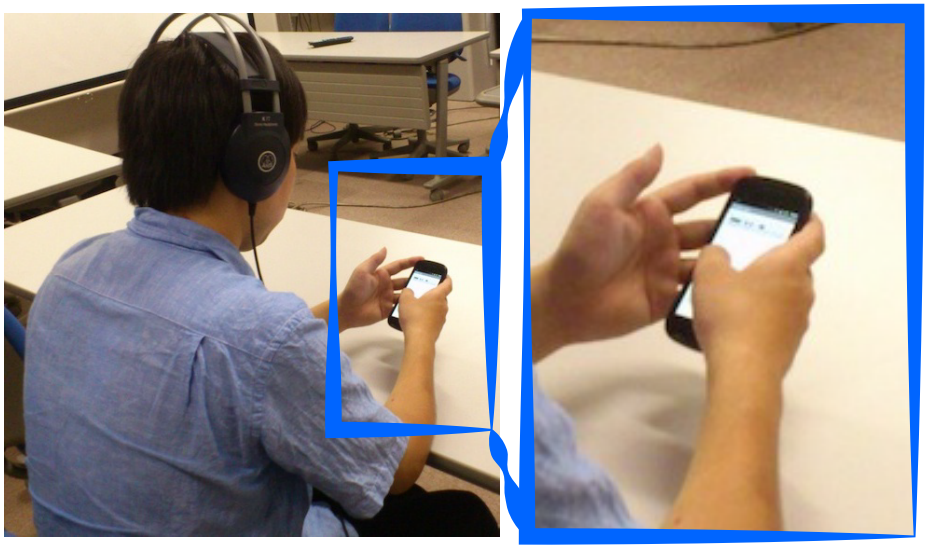


図 4.2: 被験者が実験を行っている様子。

各被験者にはタスクとして 4 種類の振動パターンの中からランダムに 1 つの振動を提示した。このタスクを 20 回行ってもらうことを 1 ブロックとし、これを 3 ブロック行ってもらった。そのうち、最初の 1 ブロックを練習とした。また、提示する 4 種類の振動パターンには、振動間隔 A を変えた 6 種類の組み合わせ（25、50、75、100、125、150 ミリ秒）を用意した。各々の組み合わせを与える順序はランダムとした。

提示する 4 種類の振動パターンは、常に ON、振動間隔 A、振動間隔 A×2、常に OFF の 4 種類である。今後それぞれ ON、Short、Long、OFF と呼ぶ。使用する 4 種類の振動パターンを図 4.1 に、使用したボタンを図 4.3 に示す。以上より各被験者毎に計 360 回（20 タスク × 3 ブロック × 6 種類）振動を提示した。

また、使用したアプリケーションを図 4.4 に示す。図 4.4a が初期状態であり、被験者が図 4.4a の Start を押すことによって振動が開始される。振動開始後、図 4.4b に示すように Start ボタンが薄くなり、画面上部のボタンが濃く変化し、画面上部のボタンが押せるようになる。被験者は図 4.4b の上部のボタンの中から現在の振動に対応するボタンを押すことにより終了する。

実験開始前に被験者には振動パターンとボタンの対応を実際に触れてもらうことにより覚えてもらった。また、振動から発生する音により被験者が振動パターンを識別することを防ぐために、先行研究 [SPHZ13, BOKK11] と同様に被験者にはピンクノイズが流れるヘッドホンを装着してもらった。実験後にはアンケートを行った。被験者 1 人あたりの実験時間は約 20 分であった.

図 4.3: 実験に使用したボタン。振動パターンとの対応は左から ON、Short、Long、OFF。

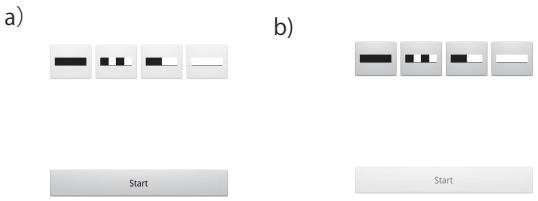


図 4.4: 実験時に使用したアプリケーション。a)Start を押すと振動が発生、b) 現在の振動パターンに対応するボタンを押す。

4.1.3 実験結果および考察

それぞれの振動間隔毎の識別率および平均速度を図 4.5、および図 4.6 に示す。

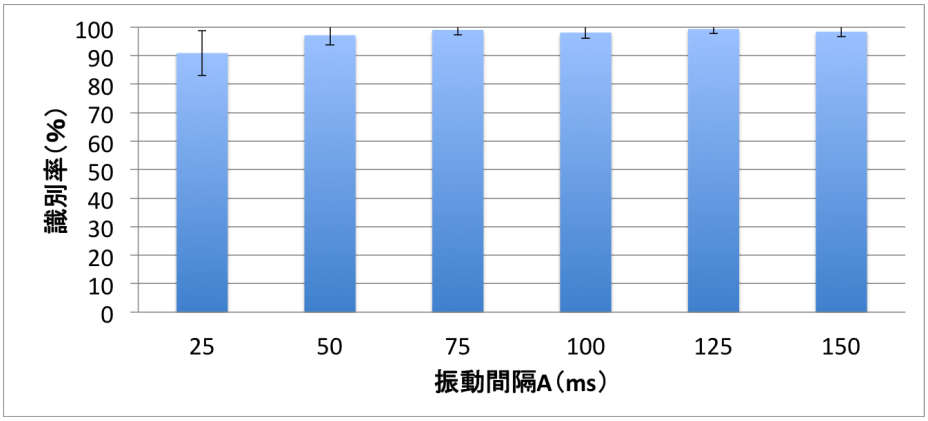


図 4.5: 予備実験 1 の振動パターンの識別率。

分散分析の結果、識別率（$F_{5,42}$ = 4.8、p=.002 < .05）および速度（$F_{5,42}$ = 3.9、p= .005 < .05）に有意差が見られた。25 ミリ秒が他の間隔に比べて有意に精度が悪く（90.1%、$p < .05$）、また、150 ミリ秒を除く他の間隔に比べて有意に遅かった（1.36 秒、$p < .05$）。すなわち 25 ミリ秒は有意に悪いが、それ以外に有意差は見られなかった。しかし振動間隔 A が 75 ミリ秒の時、識別率が 99.1%と高く、かつ平均識別速度が最も速い結果となった。そのため、プロトタイプ 1 では 75 ミリ秒を振動間隔 A として採用することとした。

4.2 プロトタイプ 1

本節では、Wheel タイプおよび Bar タイプと呼ぶ 2 種類の VibraInput のプロトタイプ（プロトタイプ 1）を示す。Wheel タイプはダイヤル式の鍵をモデルにしており、ユーザはダイヤル式の鍵を利用する場合と同様に円をタッチし、回転させることによって数字を入力する。Bar

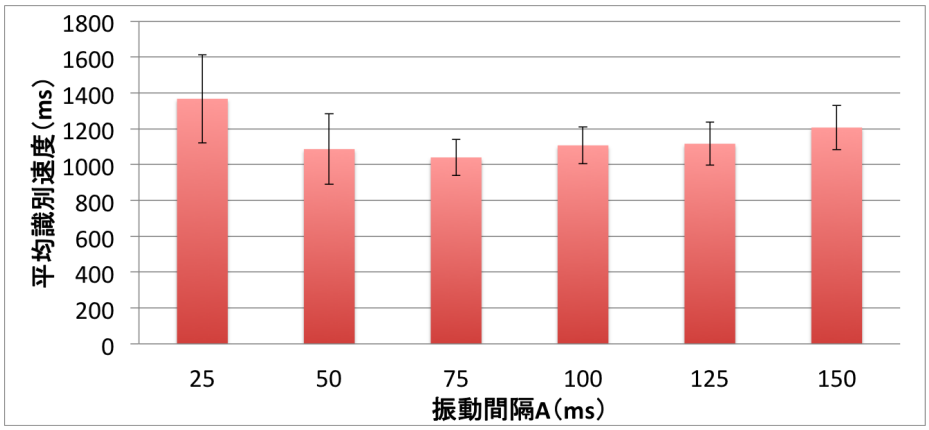


図 4.6: 予備実験 1 の振動パターンの識別速度。

タイプは Wheel タイプと比べて安全性が高いモデルであり、ユーザはバーをタッチし、スライドさせることによって数字を入力する。

これらのプロトタイプ 1 において、振動パターンに対応する記号は色の明度により表現している。高い明度は振動間隔が短いことを示し、低い明度は振動間隔が長いことを示す。

4.2.1 Wheel タイプ

図 4.7 に示すように Wheel タイプは 10 種類の数字と振動パターンを示す記号（色）から構成されている。外側の円はユーザのドラッグによって回転するようになっている。すなわち、ユーザはタッチパネルに表示された外側の円をタッチし、円を回転させるように指を動かすことによって、外側の円が回転する。これにより、ユーザは正しいカーソルを内側の円に書かれた入力したい数字に合わせることによって数字を入力する。

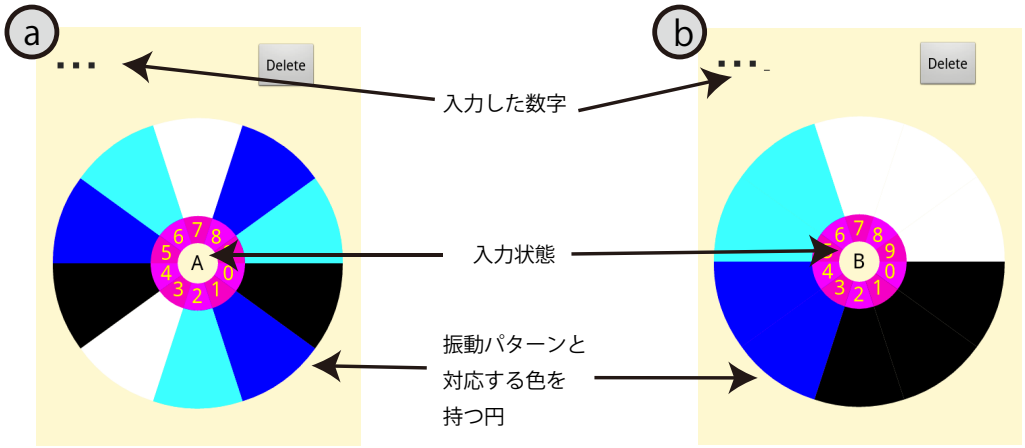


図 4.7: Wheel タイプ。a）1 回目の選択における初期状態、b）2 回目の選択における初期状態。

図 4.7a に 1 回目の初期状態を示す。1 回目の選択により、入力する数字の候補が決まり、2 回目の選択により、入力する数字が確定される。なお、2 回目の選択時、色は図 4.7b に示すように再配置される。

Wheel タイプにおいて、ユーザが不要な回転を行うと仮定した場合、全ての数字が PIN 候補となるため、PIN 入力を見られていない場合と同等の安全性を持つことができる。その一方、2 回目の入力の際に回転操作を行う必要があり、さらに不要な回転をユーザが行わない場合、回転を止める直前と止めた後が違う色になる位置にある数字が PIN 候補であると見破られてしまう。振動パターンは 4 種類であるため、一度の回転にて振動パターンに対応する記号が 1 個分回転する場合、候補が 4 種類となる。1 桁の PIN 入力において回転が必要な確率は 3/4 であり、その際の候補が 4 種類となるため、1 桁の PIN 入力が攻撃者に盗まれる可能性は $(3/4) \times (1/4) + (1/4) \times (1/10)$ より、21.3%である。また、4 桁の PIN 入力であれば $21.3\%^4 = 0.2\%$ より、攻撃者に盗まれる可能性は 0.2%となる。

4.2.2 Bar タイプ

Bar タイプは、Wheel タイプよりも安全性が高いモデルであり、図 4.8 に示すように 10 種類の数字と振動パターンを示す記号（色）から構成される。また、Wheel タイプと異なり、円ではなく 2 種類のバーを使用する。バーに表示されている色はユーザのドラッグによって移動するようになっている。なお、ユーザがバーをドラッグした際、バーの位置は変わらず、バーに表示されている色の位置のみが変化する。ユーザはバーをドラッグし、内側に書かれた数字に現在の振動パターンに対応する色の列（2 回目の選択であれば行）を合わせることによって数字の選択を行う。図 4.8a に 1 回目の初期状態を示す。1 回目の選択により、入力する数字の候補が決まり、2 回目の選択により、入力する数字が確定される。なお、2 回目の選択時、図 4.8b に示すように縦のバーは消え、横のバーが表示される。

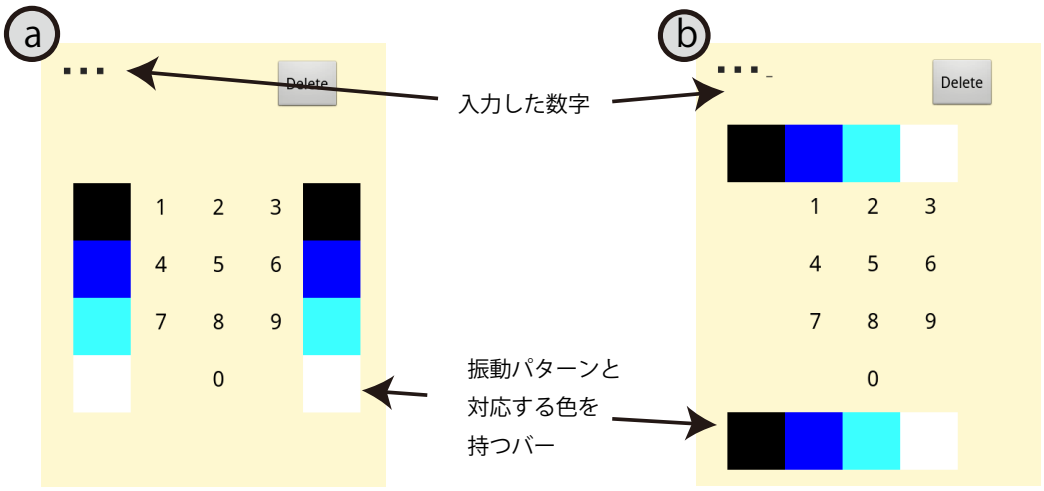


図 4.8: Bar タイプ。a）1 回目の選択における初期状態、b）2 回目の選択における初期状態。

Bar タイプの入力の様子を図 4.9 に示す。1 回目の入力の際に 4 種類の振動パターンのいずれかがランダムに発生する。図 4.9b に示すように、最初にユーザはバーを移動させることによって現在の振動パターンを示す記号を入力したい数字がある行に移動させる。図 4.9c に移動が完了した様子を示す。ユーザはこの状態になった時に、2 もしくは 3 個の数字のいずれかを選択した状態になる。ユーザ以外の人は記号と数字の対応は分かるものの、どの記号を合わせているか分からない。入力を確定させると振動が終了し、2 回目の入力に状態が遷移する.

2 回目の入力の際にも 4 種類の振動パターンのいずれかがランダムに発生する。図 4.9d に示すように縦のバーは消え、横のバーが表示される図 4.9e に示すように、ユーザは 1 回目と同様に現在の振動パターンを示す記号を入力したい数字がある列に移動させる。図 4.9f に移動が完了した様子を示す。入力を確定させると振動が終了し、数字が確定する。なお、1 回目と同様に、ユーザ以外の人はどの記号を合わせているか分からないため、入力された数字を見破ることはできない。

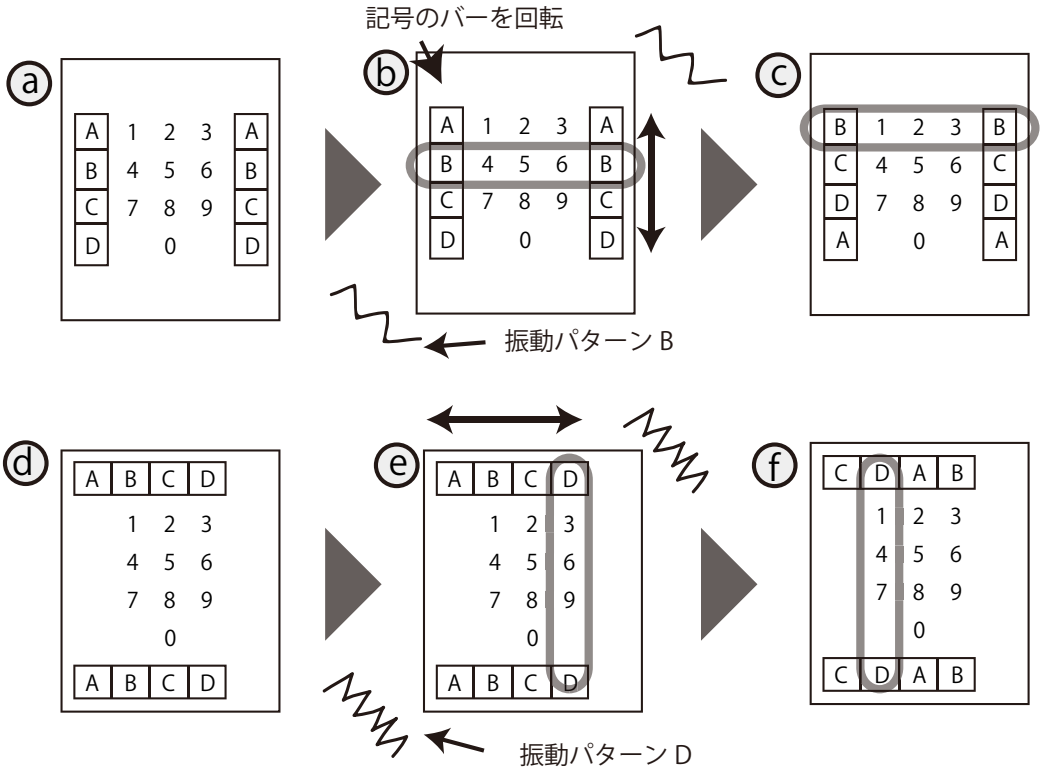


図 4.9: Bar タイプの入力方法（1 を入力する例）。a）1 回目の初期状態。b）ユーザがタッチすると振動が開始される。ユーザは携帯情報端末の振動パターンに対応する記号 B の列を 1 に合わせる。c）リリースにより入力候補（1、2、3）が確定し、d に状態が遷移。d）2 回目の初期状態。e）振動が開始される。ユーザは携帯情報端末の振動パターンに対応する記号 D を 1 の行に合わせる。f）リリースにより 1 が確定し、状態は a に遷移。

Bar タイプの安全性について述べる。Wheel タイプでは、1 桁の PIN が攻撃者に知られる可能性は 21.3%であり、4 桁の PIN であれば、0.2%であった。一方、Bar タイプでは、 1 桁の PIN が攻撃者に知られる可能性は $(1/10) = 0.1$ より、10%である。また、4 桁の PIN であれば $10\%^4 = 0.1\%$ となり、0.1%である。そのため、Wheel タイプに比べて Bar タイプは安全性が高いといえる。

4.3 4 桁の PIN 入力の容易性を調べる実験 1

VibraInput を 4 桁の PIN 入力にて使用した場合の入力の容易性を調べる実験を行った。

4.3.1 被験者

22 歳から 25 歳までの大学生、大学院生のボランティア 24 名（男性 21 名、女性 3 名）を被験者とした。また、被験者を 2 つのグループに分け、片方のグループには Wheel タイプを、もう片方のグループには Bar タイプを使用してもらった。被験者には携帯情報端末を自由に把持してもらった。

4.3.2 実験設計

実験には Android 2.3.4 を搭載した Google Nexus S と、プロトタイプ 1 を用いた。被験者に一般的なパスワード認証にて使われる 4 桁の PIN 入力を行ってもらった。被験者には椅子に座り、携帯情報端末を把持してもらった。また、予備実験と同様に被験者にはピンクノイズの流れるヘッドホンを装着してもらった。実験の様子を図 4.10 に示す。被験者が携帯情報端末の画面に触れると実験が開始され、4 種類の振動パターンのいずれかが発生する。

実験に用いたアプリケーションを図 4.11 に示す。入力してもらう PIN はあらかじめランダムに作成された番号であり、この PIN を携帯情報端末の画面上部に表示した。また、入力するべき PIN の下部には現在の入力状態を表示し、入力した数字は黒い四角として表示した。最後の PIN 入力が終わった際に、入力するべき PIN と照合し、合っていれば次の PIN 入力へ移動した。また、間違っていた場合は最初から同じ PIN 入力を行ってもらった。

実験の最初に被験者にはプロトタイプ 1 の入力方法の説明とタスクの説明、また、色と振動パターンの対応の説明を行った後、最大 3 分間、実際に使用してもらった。その後、4 桁の PIN 入力を行ってもらうタスクを 5 回成功するまで行ってもらった。これを 1 ブロックとし、合計 3 ブロック行ってもらった。実験結果のうち、最初のブロックを練習とし、以降の 2 ブロックを分析対象とした。また、実験終了後にアンケート調査を行った。被験者 1 人あたりの実験時間は約 20 分であった.

図 4.10: 4 桁の PIN 入力の容易性を調べる実験 1 において、被験者が PIN を入力している様子。

4.3.3 実験結果および考察

Wheel タイプの認証成功率を図 4.12 に、Bar タイプの認証成功率を図 4.13 に示す。また、図 4.14 に示すように、2 種類のプロトタイプ 1 の平均認証成功率は 96%であった。認証成功率とは、被験者の全ての 4 桁の PIN 入力のうち、正しく入力できた 4 桁の PIN 入力の割合である。すなわち、被験者が 4 桁の PIN 入力の途中にて誤りに気づき、Delete キーを押して入力をやり直した場合であっても、入力しなおした 4 桁の PIN 入力が正しい場合、認証成功となる。認証に失敗した被験者の内 4 名は Short と Long の違いが分かりにくいと述べていた。

また、自由アンケートにて被験者から以下の意見が得られた。

- 色と振動パターンの対応を覚えるのが難しく考えてしまった。
- Short と Long の違いを識別するのが難しかった。
- OFF の時にシステムが動いているのか不安になった。

Wheel タイプの平均認証時間を図 4.15 に、Bar タイプの平均認証時間を図 4.16 に示す。また、2 種類の平均認証時間は図 4.17 に示すように、23.8 秒であった。平均認証時間とは 4 桁の PIN 入力にかかる時間であり、認証に成功した場合の時間の平均を示している。また、被験者が Delete キーを用いて数字を消し、再度入力した場合であっても、認証に成功した場合は認証時間に含めている。すなわち、被験者が Delete キーを使った場合、被験者は 5 桁以上の PIN を入力することになる。著者はこれが認証時間の分散が大きくなった原因であると考えている。また Bar タイプに比べて、Wheel タイプは被験者ごとに平均認証時間が大きく異なることがわかった。

Welch の t 検定を行った結果、Bar タイプは Wheel タイプよりも有意に速かった（$t(9) = 2.72, p = .011 < .05$）。Wheel タイプを利用した 3 人の被験者は円を回転させるのが難しいと

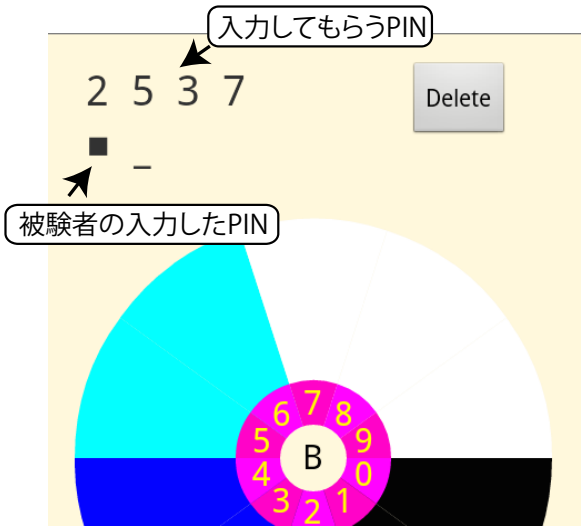


図 4.11: 実験に用いたアプリケーション。画面上部に入力してもらう PIN が表示される。

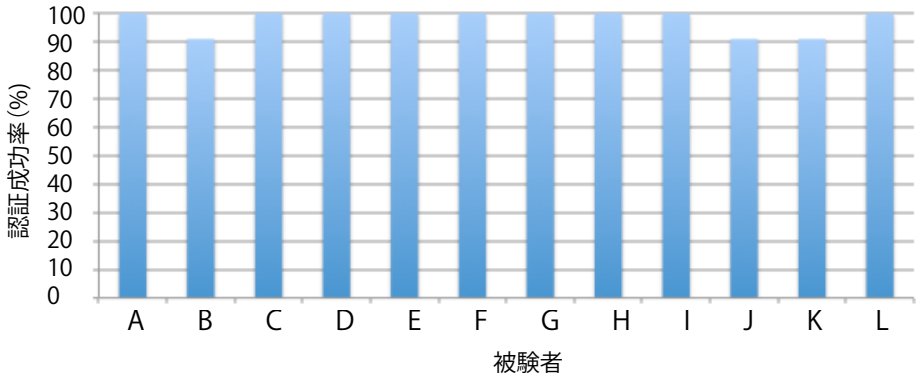


図 4.12: プロトタイプ 1 の Wheel タイプの認証成功率。

コメントしていたため、これが Wheel タイプにおいて入力が遅くなった原因であると考えられる。また、Wheel タイプにおいて、不要な回転を行うユーザと、必要最低限の回転しか行わないユーザの両方が見られた。円のデザインは第 7.3 節にて議論する。

4.4 安全性に関する実験 1

本システムに対してショルダーサーフィンを行った場合、PIN を見破ることができるかの実験を行った。

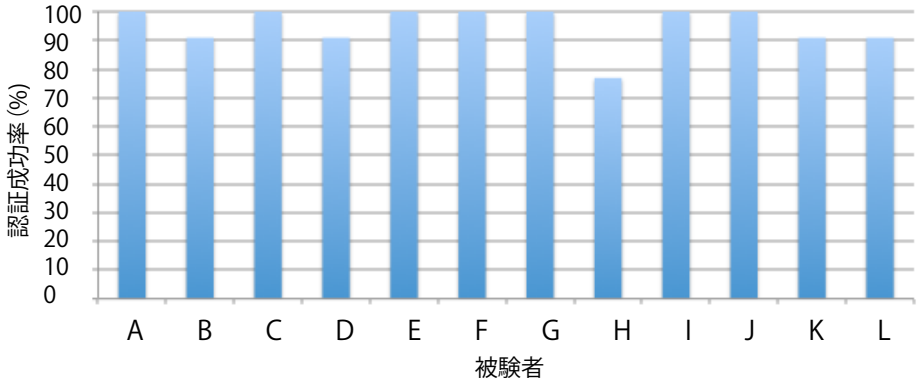


図 4.13: プロトタイプ 1 の Bar タイプの認証成功率。

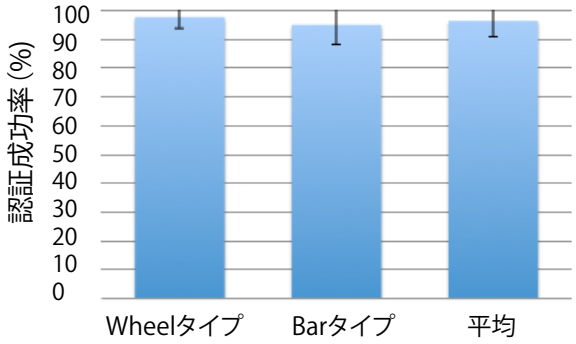


図 4.14: 2 種類のプロトタイプ 1 の平均認証成功率。

4.4.1 被験者

4 桁の PIN 入力の容易性を調べる実験 1 を行った 24 名を被験者とした。被験者には、4 桁の PIN 入力の容易性を調べる実験 1 にて使用したプロトタイプ 1 に対して、ショルダーサーフィンを行ってもらった。すなわち、全ての被験者はプロトタイプ 1 を実際に触って入力したことがあり、プロトタイプ 1 の入力方法および色と振動パターンの対応が分かっていた。

4.4.2 実験設計

実験には Android 2.3.4 を搭載した Google Nexus S を用いた。被験者にはプロトタイプを座りながら使用する実験者（著者）の肩越しに立ち、PIN を推測してもらった。実験の様子を図 4.18 に示す。

実験者は被験者に入力画面が見やすくなるように、携帯情報端末を把持するよう努めた。また、被験者には入力画面が見にくい場合それを指摘してもらい、実験者は見やすく把持するように修正した。入力時には円と指の位置を見やすくするため、1 回毎に指を 3 秒以上静止し、その後に入力を確定させた。また、円を必要以上に動かさないよう注意した。

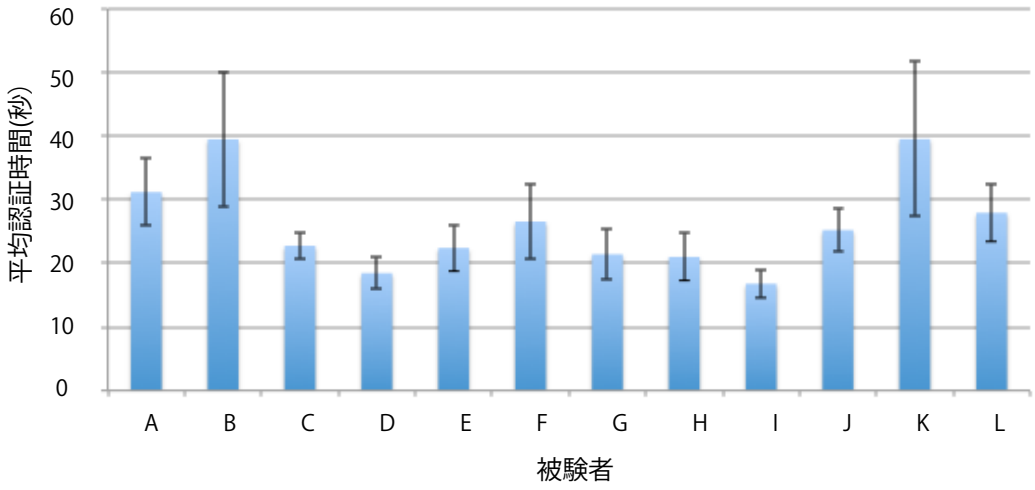


図 4.15: プロトタイプ 1 の Wheel タイプの平均認証時間。

実験者は 4 桁の PIN 入力を 3 回行い、被験者には番号を推測したものを回答用紙に記入してもらった。その後、被験者に携帯情報端末の振動音が聞こえるかを聞いた。また、空調を切った静かな部屋（デジタル騒音計 [1] にて 34dB から 38dB）を占有して実験を行った。

4.4.3 実験結果および考察

入力された 4 桁の PIN を当てることができた被験者はいなかった。また、アンケートより 23 名の被験者は振動音を聞くことができなかったと述べた。1 名の被験者は一時振動音を聞くことができたが、その種類を識別することができなかったと述べた。この結果より、本システムに対してショルダーサーフィンを行っても PIN を見破ることはできないと言える。

4.5 予備調査のまとめ

認証失敗率が低いことから、ユーザは本システムを容易に使うことができ、ショルダーサーフィンに成功した被験者はいなかったことから、ショルダーサーフィンに対して安全であることを確認できた。

また、録画に対して安全であるかを調べるため、第 4.4 節と同じ環境にて本システムの入力の様子を録画した。ビデオを確認した結果、目視では携帯情報端末が振動している様子を確認することができなかった。また、振動音についても確認することはできなかった。この結果から、録画に対しても安全である可能性が見られた。録画に対する安全性のより詳しい実験を第 6 章にて述べる。

[1] サンコー 小型デジタル騒音計 RAMA11O08

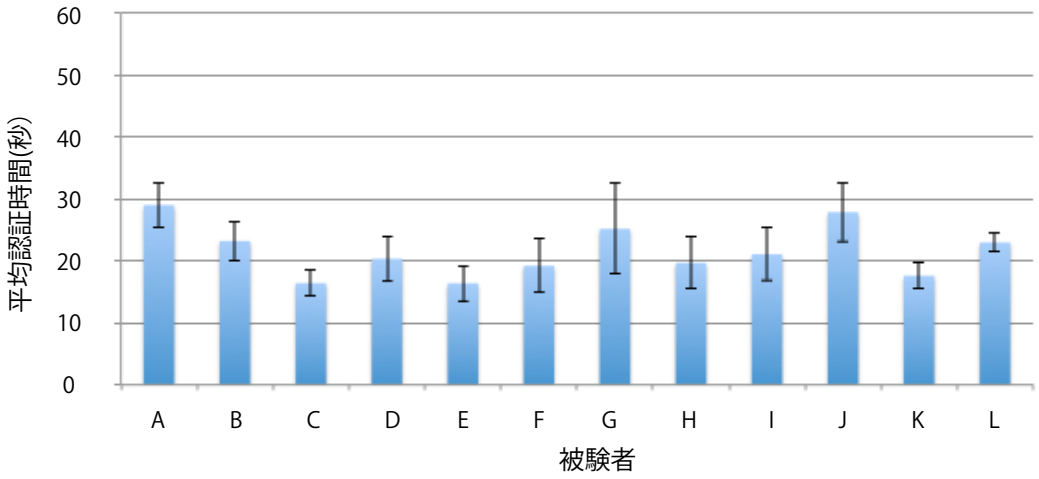


図 4.16: プロトタイプ 1 の Bar タイプの平均認証時間。

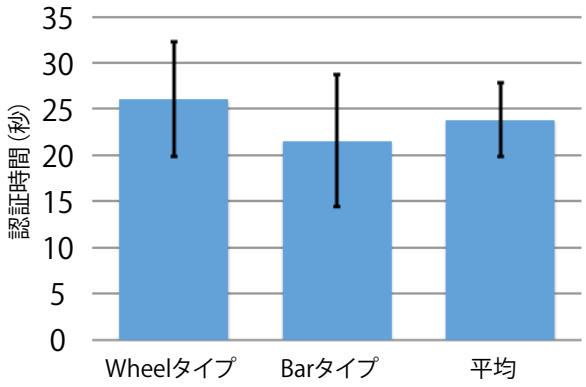


図 4.17: 2 種類のプロトタイプの平均認証時間。

さらに、今回の実装では見やすさを考慮し、振動パターンを表す記号を色として表現した。しかし、ユーザから「色と振動パターンの対応を覚えるのが難しく考えてしまった」という意見を得た。また、色盲のユーザには今回の実装は適切ではない。そこで、振動パターンを表す記号を色ではなく図にした実装について、第 5 章にて述べる。

なお、今回は短い時間にて実験が行えるよう、被験者間実験を行ったが、2 種類のプロトタイプ（Wheel タイプおよび Bar タイプ）の詳細な比較を行うためには被験者内実験を行う必要がある。そこで、被験者内実験を第 6 章にて述べる。

図 4.18: 被験者がショルダーサーフィンを行っている様子。

第5章　VibraInputの改良

本章では、最初に予備調査から得られたフィードバックと改良案を延べ、それを元に行った、ユーザが識別しやすい振動パターンを調査した予備実験 2 を述べる。その後、その結果を元に作成したプロトタイプ 2 を述べ、次にそのプロトタイプ 2 を用いて行った 4 桁の PIN 入力の容易性を調べる実験 2 を述べる。最後に、ユーザが識別しやすい振動パターンを調査した予備実験 3 を述べ、それを元に作成したプロトタイプ 3 を述べる。

5.1　予備調査から得られたフィードバックと改良案

予備調査より、本システムの基本的な設計は正しいことが確認できた。また、以下の 3 点には改良の余地があることも同時に確認できた。

課題 1　色と振動パターンの対応を覚えるのが難しい。

課題 2　Short と Long の違いを識別するのが難しい。

課題 3　OFF の時にシステムが動いているのか不安になる。

課題 1 と 2 に関しては複数の被験者から意見が得られた一方、課題 3 に関しては 1 人の被験者のみから得られた。

本節では、最初に課題 1 の解決案を述べ、次に課題 2 の解決案を述べる。最後に研究室内実験より得られた意見について述べる。課題 3 の解決案は第 5.5 節にて述べる。

5.1.1　課題 1 の解決案

課題 1 に対して、振動の幅を変えるという解決案と振動の回数を変えるという解決案がある。なお比較のために、図 5.1 に予備調査に用いた振動をパターンを示す。

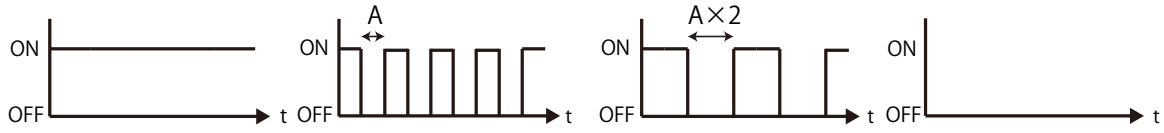


図 5.1: 予備調査にて使用した振動パターン。

図 5.2 に振動の幅を変える方法を用いた場合の振動パターンを示す。これは、予備調査においては Short に振動パターン A を、Long にその 2 倍を使用していたが、これを Short に振動パターン A を、Long にその 3 倍を使用するという解決案である。これにより Short と Long の違いを明確にする。この解決案は単純であるが、Short と Long のパルスの形が同じであるため、システムを数日間触らなかった場合などに、間違いを起こす場合がある。すなわち、ユーザは Short や Long 単体のパルスの速さを忘れた場合、本システムを使うために 1 度両方を比較する必要がある。

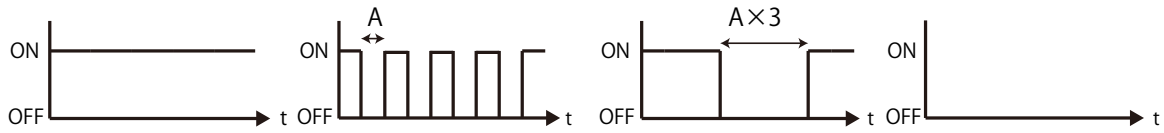


図 5.2: 振動の幅を変える方法を用いた場合の振動パターン。

この問題を解決するために、振動の回数を変える方法を用いた場合の振動パターンを図 5.3 に示す。これは Short と Long のパルスの形が異なるため、ユーザは Short と Long を比較することなく違いを感じることができる。

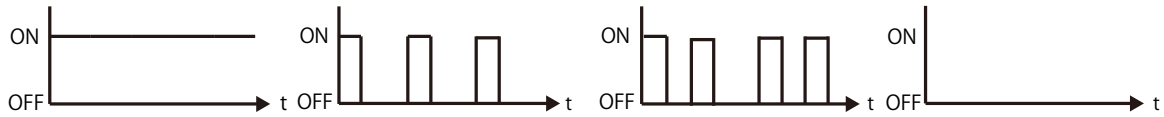


図 5.3: 振動の回数を変える方法を用いた場合の振動パターン。

5.1.2 課題 2 の解決案

本節では、課題 2 の解決案として、図も同時に表示するという解決案を示す。

第 5.1.1 節にて述べた、解決案を元に Wheel タイプを改良した。振動の幅を変えた場合の Wheel タイプを図 5.4 に示す。この時、図はパルス幅をそのまま表示することとした。また、振動の回数を変えた場合の Wheel タイプを図 5.5 に示す。この時、振動の回数を円の数により表現することとした。

5.1.3 研究室内実験より得られた意見

これらの改良したシステムを研究室内の被験者に実際に使用してもらい、その使用感を調査した。その結果、どちらのシステムにおいてもユーザは予備調査にて作成したプロトタイプ 1 よりもわかりやすいという意見が得られた。そこで、第 5.1.1 節の解決案のうち、より単純な方法である、振動の幅を変える方法を用いて、ユーザが識別しやすい振動パターンを調査する予備実験 2 を行い、それを元にプロトタイプ 2 を作成することとした。

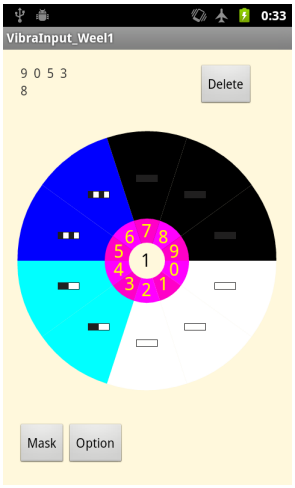


図 5.4: 振動の幅を変えた場合の Wheel タイプ。

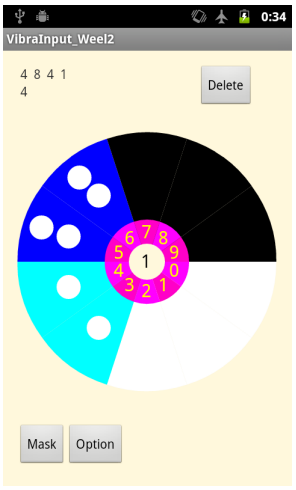


図 5.5: 振動の回数を変えた場合の Wheel タイプ。

5.2 予備実験 2：ユーザが識別しやすい振動パターンの調査

本節では、ユーザが識別しやすい振動パターンを調査する予備実験 2 を述べる。振動パターンには、第 5.1.1 節にて述べた振動の幅を変える方法を用いた。

本実験では、5 名の被験者を対象に、ユーザが識別しやすい振動パターンを調査する予備実験を行った。実験には Android 2.3.4 を搭載した Google Nexus S を携帯情報端末として用いた。

被験者がスタートボタンを押すと実験が開始され、4 種類の振動パターンのいずれかがランダムに開始される。被験者には振動パターンを識別してもらい、対応するボタンをできるだけ正確に、また正確さを失わない程度に素早く押してもらった。

各被験者にはタスクとして 4 種類の振動パターンの中からランダムに 1 つの振動を提示した。このタスクを 20 回行ってもらうことを 1 ブロックとした。提示する 4 種類の振動パターンには、振動間隔を変えた 3 種類の組み合わせを用意した。

提示する 4 種類の振動パターンは、常に ON、振動間隔 A、振動間隔 $A \times 3$、常に OFF の 4 種類である. 今後それぞれ ON、Short、Long、OFF と呼ぶ。

以上より、各被験者毎に計 60 回（20 タスク $\times$ 1 ブロック $\times$ 3 種類）振動を提示した。実験開始前に被験者には振動パターンとボタンの対応を実際に触れてもらうことにより覚えてもらった。使用した振動パターンを図 5.6 に示す。

第 4.1 節の実験にて最適な振動間隔 A は 75 ミリ秒であったため、本実験においては 75 ミリ秒とその前後である 50 ミリ秒および 100 ミリ秒を使用した。

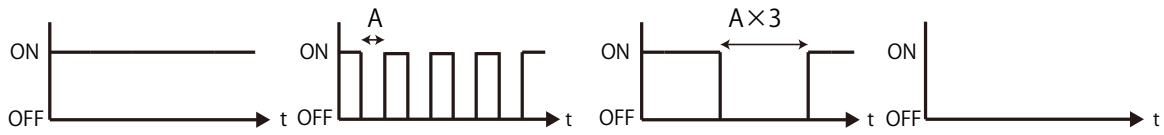


図 5.6: 予備実験 2 に使用した振動パターン。左から ON、Short、Long、OFF。第 4.1 節の実験に用いた振動パターンより、Long が長くなっている。

5.2.1　実験結果および考察

今回の識別率を図 5.7 に、識別速度を図 5.8 に示す。今回も振動間隔 A に関して有意差は見られなかった。また、各振動間隔につき 1 人の被験者が複数回、選択を間違えていた。これは、3 ブロック行い、そのうち最初の 1 ブロックを練習とした前回と比較して、今回は 1 ブロックしか行わなかったことが原因の 1 つであると考えられる。有意差は見られなかったものの、75 ミリ秒の識別率が最も高かったため、以降の実験では振動間隔 A を 75 ミリ秒とした。

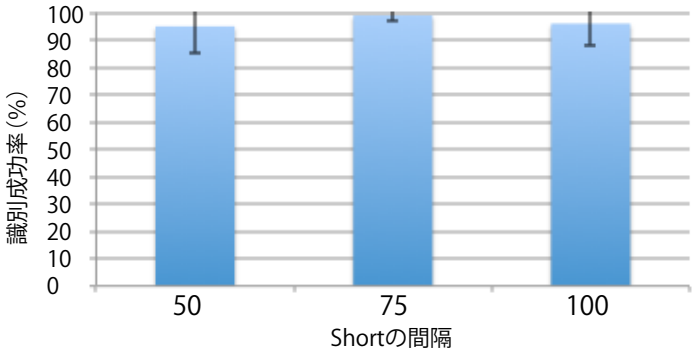


図 5.7: 予備実験 2 の識別率。

5.3　プロトタイプ 2

本節では、第 5.2 節の結果より、振動間隔 A に 75 ミリ秒を採用したプロトタイプ 2 について述べる。

第 5.1 節にて述べた課題 2 に関して、プロトタイプ 1 では振動を表す色の変化が激しかった（黒、青、水色、白）ため、振動が早いほど濃いという変化（黒が最も早く、白が最も遅い）が分かりにくかった。そこで、青を基準とし、色を振動が早い方から薄い明度になるように変更した。また、第 5.1.2 節にて述べたように、色と同時に記号も表示し、記号によっても振動が識別できるように変更した。

図 5.9 に改良した Wheel タイプを示す。この Wheel タイプでは、1 回目のパターンと 2 回目のパターンが逆になり、1 回目のパターンでは同じ色が隣に、2 回目のパターンでは色が交互に配置されている。すなわち、ユーザは 1 回目の選択により隣り合った数字を入力の候補に

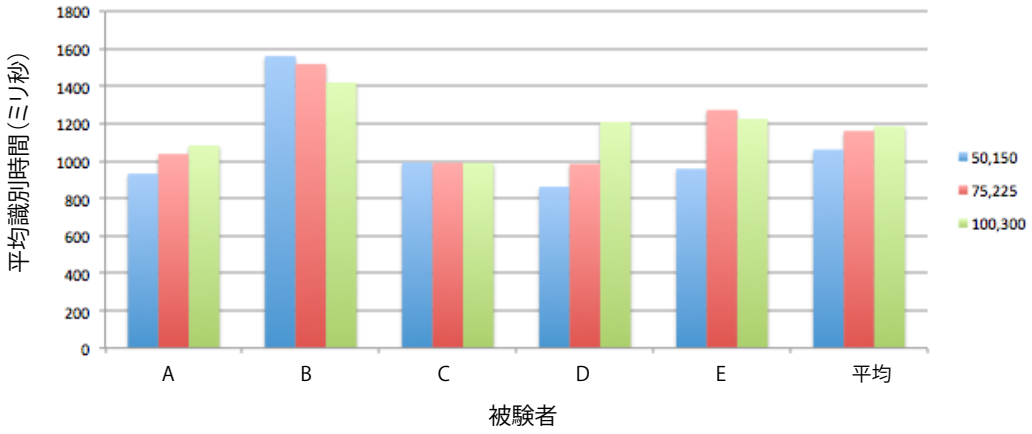


図 5.8: 予備実験 2 の識別速度。

し、2 回目の選択により、隣り合った数字の中から入力する数字を確定させる。これにより、現在が何度目の入力であるかがわかりやすくなったため、画面中央にて A と B によって現在の入力状態を表現していたものを削除した。

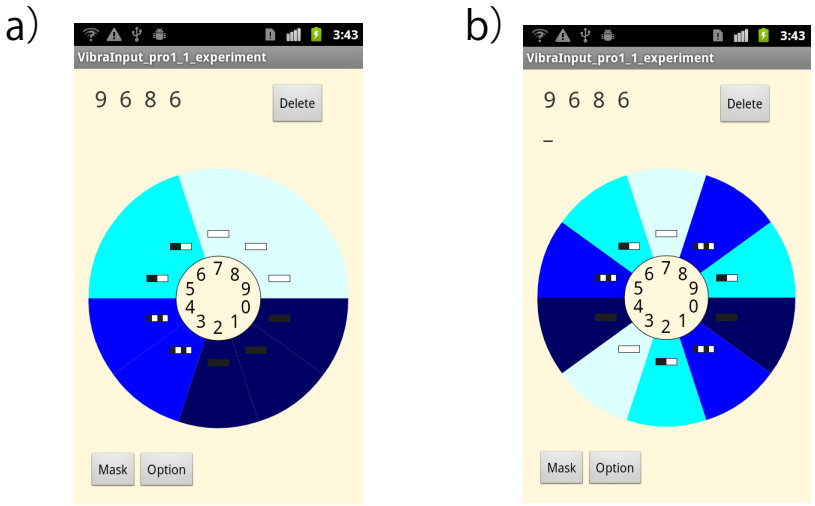


図 5.9: 改良した Wheel タイプ。1 回目と 2 回目のパターンが逆になり、色の変化を少なくした。a）1 回目の選択における初期状態、b）2 回目の選択における初期状態。

また、図 5.10 に改良した Bar タイプを示す。Wheel タイプと同様に、振動パターンの表現に図も併用している。

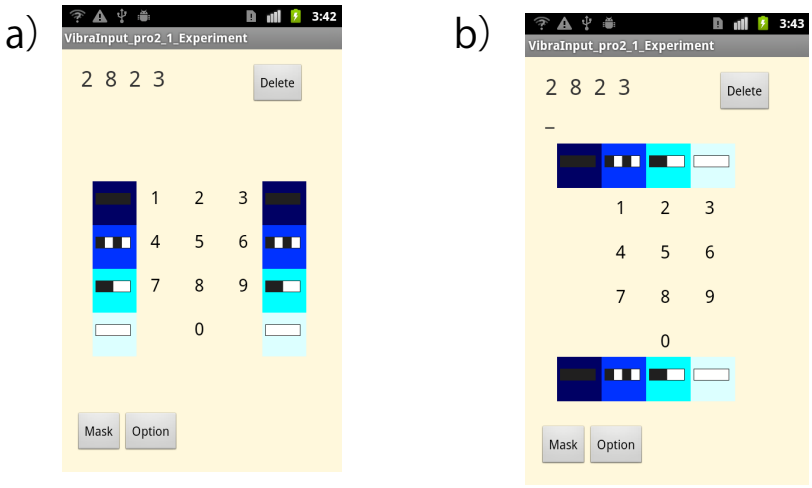


図 5.10: 改良した Bar タイプ。Wheel タイプと同様に色の変化を少なくした。a）1 回目の選択における初期状態、b）2 回目の選択における初期状態。

5.4　4 桁の PIN 入力の容易性を調べる実験 2

第 5.3 節にて述べたプロトタイプ 2 を用いて、4 桁の PIN 入力の容易性を調べる実験 2 を行った。

5.4.1　被験者

23 歳と 25 歳の大学院生 2 名を被験者とした。各被験者は第 4.3 節の実験に参加したことがある人物である。

5.4.2　実験設計

実験には Android 2.3.4 を搭載した Google Nexus S とプロトタイプ 2 を用いた。被験者には一般的なパスワード認証にて使われる 4 桁の PIN 入力を行ってもらった。被験者には椅子に座り、携帯情報端末を把持してもらった。また、第 4.3 節の実験と同様に被験者にはピンクノイズの流れるヘッドホンを装着してもらった。被験者が携帯情報端末の画面に触れると実験が開始され、4 種類の振動パターンのいずれかが発生する。

入力してもらう 4 桁の PIN はあらかじめランダムに作成された番号であり、この PIN を携帯情報端末の画面上部に表示した。また、入力するべき PIN の下部には現在の入力状態を表示し、入力した数字は黒い四角として表示した。最後の PIN 入力が終わった際に、入力するべき PIN と照合し、合っていれば次の PIN 入力へ移動した。また、間違っていた場合は最初から同じ PIN 入力を行ってもらった。

実験の最初に被験者にはプロトタイプ 2 の入力方法の説明とタスクの説明、また、色と振動パターンの対応の説明を行った後、最大 3 分間、実際に使用してもらった。その後、4 桁の PIN 入力を行ってもらうタスクを 5 回成功するまで行ってもらった。これを 1 ブロックとし、合計 3 ブロック行ってもらった。実験結果のうち、最初のブロックを練習とし、以降の 2 ブロックを分析対象とした。これを、Wheel タイプ、Bar タイプそれぞれ行ってもらった。なお、振動パターンとして Short は 75 ミリ秒、Long は 225 ミリ秒とした。被験者 1 人あたりの実験時間は約 30 分であった.

5.4.3　実験結果および考察

プロトタイプ 2 の平均認証時間を図 5.11 に示す。予備調査の Wheel タイプ時と比べ、両被験者ともプロトタイプ 2 の方が認証時間が速くなっていた。この実験結果から、プロトタイプ 2 はプロトタイプ 1 に比べ、認証時間が一定時間速くなることが予想される。

しかし予備調査と同じ被験者による実験結果である為、予備調査にて行った実験の経験から速くなったとも考えられる。なお、認証失敗（エラー）は Wheel タイプにて、被験者 1 名による 2 回のみであった。

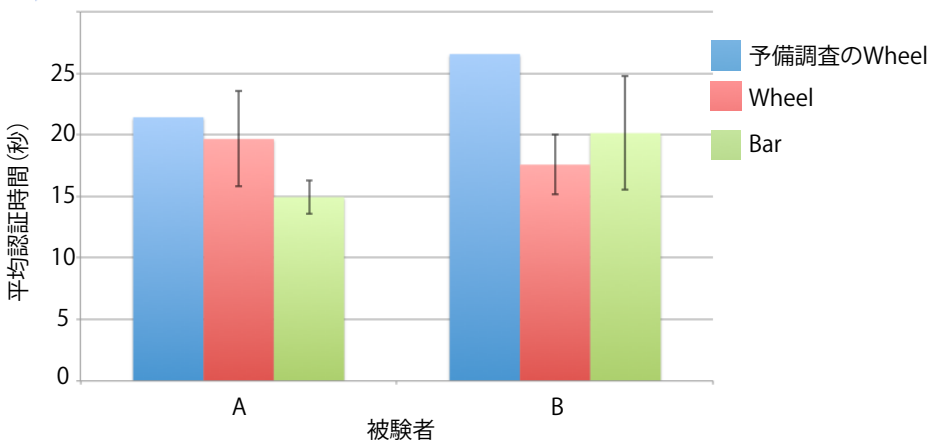


図 5.11: プロトタイプ 2 の平均認証時間。

この結果から、プロトタイプ 1 と比べ、プロトタイプ 2 は改良されたことがわかった。また、第 5.1 節にて述べた課題 1 および課題 2 が解決されたことが示唆される。

しかし、課題 3 である「OFF の時にシステムが動いているのか不安になる」という課題の解決できていない。そこで次節では、この課題の解決を目指す。

5.5　予備実験 3：ユーザが識別しやすい振動パターンの調査

本節では、第 5.1 節にて述べた課題 3 である「OFF の時にシステムが動いているのか不安になる」という課題を解決するために行った、ユーザが識別しやすい振動パターンを調査す

る予備実験 3 を述べる。

本実験に使用する振動パターンを図 5.12 に示す。前節までの実験では OFF 状態を含めていたが、今回は常に OFF 状態を削除した。

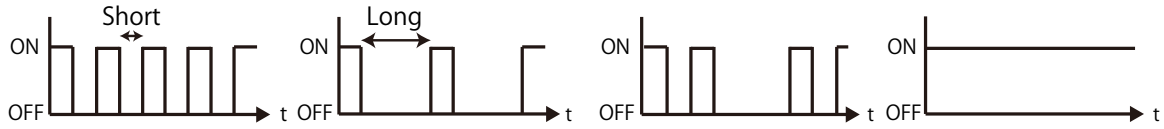


図 5.12: 予備実験 3 に用いる振動パターン。a）振動パターン A、b）振動パターン B、c）振動パターン C、d）振動パターン D。

なお、切り替えるタイミングである Short と Long はそれぞれ振動間隔 A と振動間隔 $A \times 6$ とした。前回までの実験では、Short と Long を振動間隔 A と振動間隔 $A \times 3$ にしていたが、研究室内のユーザから、振動間隔 A と振動間隔 $A \times 3$ では、振動パターン A と振動パターン B の違いがわかりにくいという意見を得たためである。

5.5.1 被験者

22 歳から 25 歳までの大学生、大学院生のボランティア 12 名を被験者とした。

5.5.2 実験設計

実験には Android 2.3.4 を搭載した Google Nexus S を携帯情報端末として用いた。被験者には椅子に座り、携帯情報端末を自由に把持してもらった。

被験者がスタートボタンを押すと実験が開始され、4 種類の振動パターンのいずれかがランダムに開始される。被験者には振動パターンを識別してもらい、対応するボタンをできるだけ正確に、また正確さを失わない程度に素早く押してもらった。

各被験者にはタスクとして 4 種類の振動パターンの中からランダムに 1 つの振動を提示した。このタスクを 20 回行ってもらうことを 1 ブロックとした。これを 3 ブロック行い、最初の 1 ブロックを練習、残りの 2 ブロックを本番とした。また、提示する 4 種類の振動パターンには、振動間隔を変えた 3 種類の組み合わせを用意した。

提示する 4 種類の振動パターンは、図 5.12 に示す 4 種類であり、振動間隔は 50 ミリ秒、75 ミリ秒、100 ミリ秒とした。

以上より、各被験者毎に計 180 回（20 タスク $\times$ 3 ブロック $\times$ 3 種類）振動を提示した。実験開始前に被験者には振動パターンとボタンの対応を実際に触れてもらうことにより覚えてもらった。また、提示する振動パターンの順序は被験者ごとにランダムとした。一人あたりの実験時間はおよそ 15 分であった。

5.5.3 実験結果

識別率を図 5.13 に示す。平均識別率に関して分散分析を行った結果、有意差がみられた（$F_{2,33} = 10$、p=.002 < .05）。50 ミリ秒が 75 ミリ秒および 100 ミリ秒に比べて有意に精度が悪く（88.8%、$p < .05$）、75 ミリ秒（96.3%）と 100 ミリ秒（98.75%）の間に有意差は見られなかった。

次に、識別速度を図 5.14 に示す。また、平均識別速度に関して分散分析を行った結果、有意差は見られなかった（$F_{2,33} = 2.1$、p=.13 > .05）。しかし、75 ミリ秒の時が最も早く（1088 ミリ秒）、標準偏差も最も少なかった（63 ミリ秒）。

そこで以降の実装では、50 ミリ秒に比べて精度が有意に高く、かつ識別速度の早い 75 ミリ秒を採用することにした。

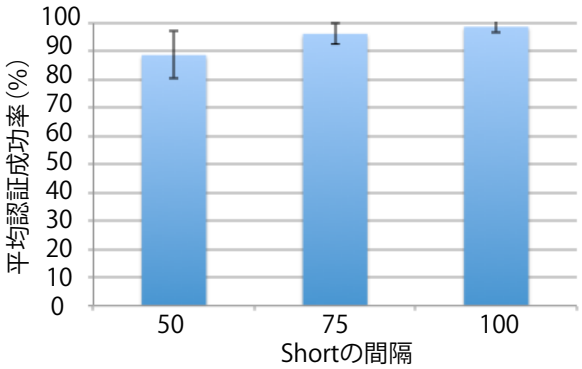


図 5.13: 予備実験 3 の識別率。

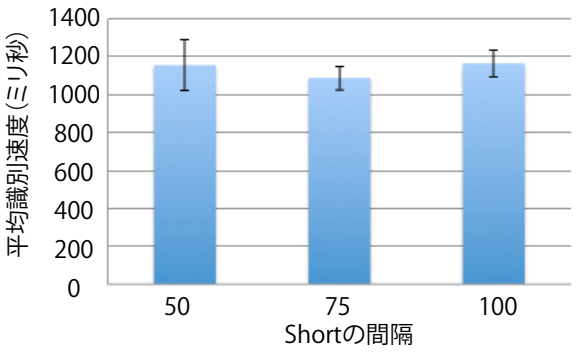


図 5.14: 予備実験 3 の識別速度。

次に、振動パターン別の識別速度について解析する為に、Short が 75 ミリ秒の時の振動パターン別識別速度を図 5.15 に示す。この結果について分散分析を行った結果、有意差がみられた（$F_{3,44}$ = 5.4, p=.002 < .05）。振動パターン D が他の振動パターンに比べて有意に早く（921.4 ミリ秒, $p < .05$）、他の振動パターンには有意差が見られなかった。この結果より、振動パターン D が最も識別が容易であること、また他の 3 つの識別速度はほとんど変わらないことがわかった。

5.6 プロトタイプ 3

本節では、予備実験 3 にて用いた振動パターンを用いたプロトタイプ 3 について述べる。プロトタイプ 3 の Wheel タイプを図 5.16 に、Bar タイプを図 5.17 示す。第 5 章までのデザインでは、色の明度を変えることにより振動間隔を表していた。これは、使用していた振動パターンが単純に振動間隔を変えていたものであったため、色の明度と振動パターンの速さを対応づけることができたためである。しかし、今回の振動パターンは単純に振動間隔を変えているものではないため、色の明度と振動パターンを対応付けることが難しかった。そこで、今回は色相差が 90 度ある 4 色の色（テトラード配色）を使用した。

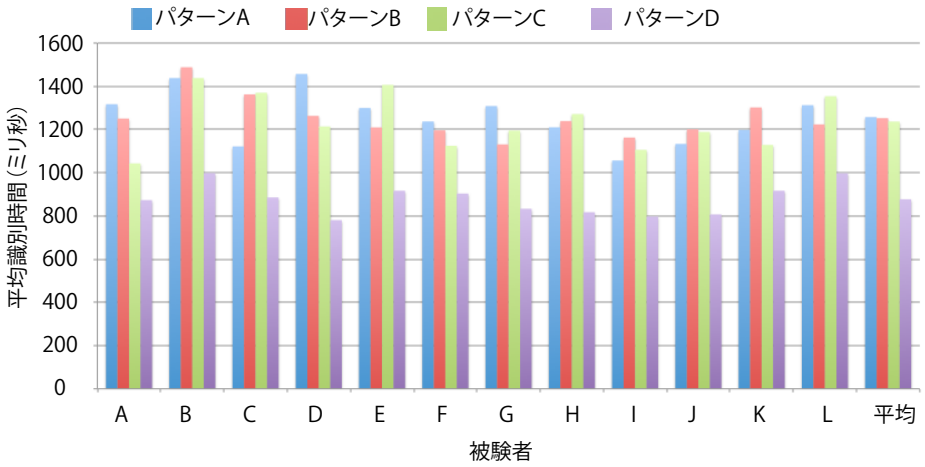


図 5.15: 予備実験 3 における Short が 75 ミリ秒の時の振動パターン別識別速度。

ユーザは第 5 章のデザインと同様に、振動を表す記号を元に、振動パターンとの対応を取ることを想定している。しかし、ユーザが本システムを長期間使用することによって、振動を表す記号だけではなく、色を補助的に使うことも予想される。

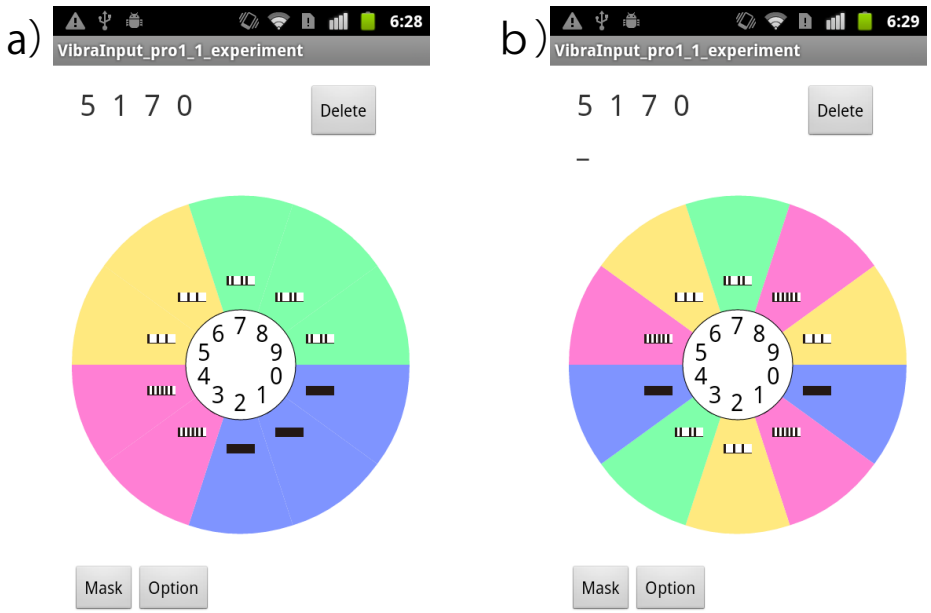


図 5.16: プロトタイプ 3 の Wheel タイプ。a）1 回目の入力、b）2 回目の入力。

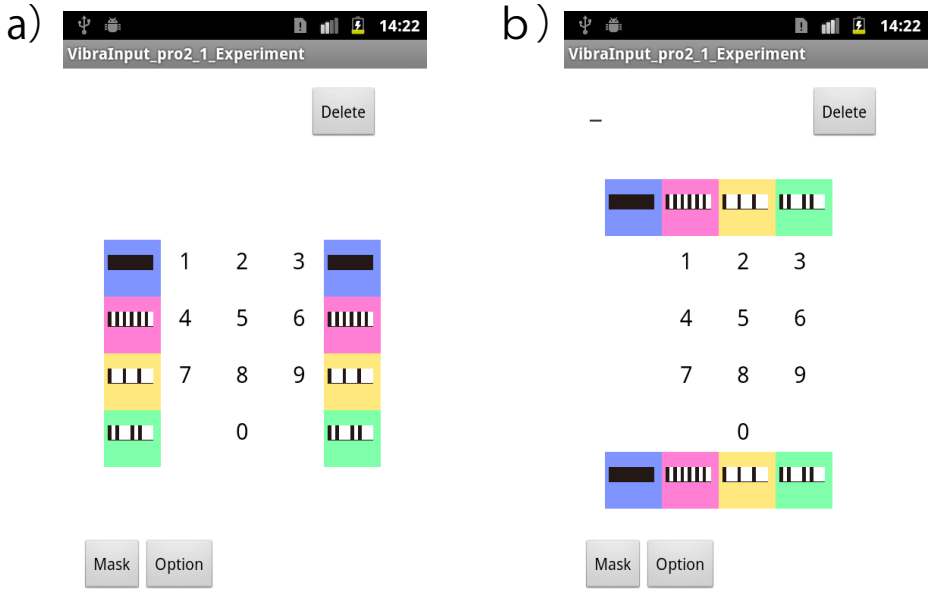


図 5.17: プロトタイプ 3 の Bar タイプ。a）1 回目の入力、b）2 回目の入力。

第6章　評価実験

本章では第5.6節のプロトタイプ3を用いて行った評価実験を述べる。この評価実験は4桁のPIN入力の容易性を調べる実験3および、安全性に関する実験2から構成される。

6.1　4桁のPIN入力の容易性を調べる実験3

第5.6節のプロトタイプ3を用いて4桁のPIN入力の成功率を調べる評価実験を行った。なお、この実験に使用した書類は付録Bとして添付する。

6.1.1　被験者

20歳から24歳までの学生12名（男性12名）を被験者とした。その内6名は大学生、6名は大学院生であった。被験者のうち、右利きの被験者は11名、左利きの被験者は10名であった。彼らは一度もセキュリティに関する実験に参加したことがなく、振動を用いた実験にも参加したことはなかった。また、本システムに関する事前知識をもっていなかった。カウンターバランスを取るために被験者を2グループに分け、片方のグループには最初にWheelタイプを、もう片方のグループには最初にBarタイプを使用してもらった。被験者には携帯情報端末を自由に把持してもらった。

6.1.2　実験設計

実験にはAndroid 2.3.4を搭載したGoogle Nexus Sを携帯情報端末として用いた。被験者には図6.1に示すように椅子に座り、携帯情報端末を把持してもらった。また、予備実験1と同様に被験者には椅子に座ってもらい、ピンクノイズの流れるヘッドホンを装着してもらった。

最初に、実験者は被験者に対してプロトタイプ3の使用方法を説明した。また、実験中に被験者背後からビデオ録画を行い、それを解析に用いることを被験者に伝えた。録画にはVICTOR GZ-E565-N Everio[1]を用いて、被験者の背後50 cmの距離から録画を行った。しかし録画したビデオを用いて安全性を調べる実験を行うということ被験者に伝えなかった。なお、この実験設計は先行研究 [DLHvZ+14] を参考にしている。

[1] http://www3.jvckenwood.com/dvmain/gz-e565/

図 6.1: 実験の様子。被験者はピンクノイズの流れるヘッドホンを装着して実験を行った。またその様子を被験者背後からビデオカメラによって録画した。

説明後、被験者に実際に触ってもらい、システムの使い方を学んでもらった、この時、基本的な誤りが起こらないよう、システムについてわからないことがあったら聞くように指示した。この練習は 2 分から 4 分の間で行ってもらった。

メインタスクでは、4 桁の PIN 入力を行ってもらうタスクを 5 回成功するまで行ってもらった。これを 1 ブロックとし、合計 3 ブロック行ってもらった。実験結果のうち、最初のブロックを練習とし、以降の 2 ブロックを分析対象とした。これを Wheel タイプと Bar タイプそれぞれについて行ってもらった。

また、入力してもらう PIN はあらかじめランダムに作成された番号であり、この PIN をあらかじめ被験者に覚えてもらった。また、入力した数字は黒い四角として表示した。最後の PIN 入力が終わった際に、入力するべき PIN と照合し、合っていれば次のタスクへ移動した。また、間違っていた場合は最初から同じ PIN 入力を行ってもらった。PIN はプロトタイプを変える時にランダムに作成しなおした。

タスクが全て終了した後、被験者には本システムに関するアンケートに答えてもらった。全てのタスクを終了するのにおよそ 40 分かかった。また被験者には実験後に報酬として 820 円を支給した。これらの実験は、予備実験 1 と同様、空調を切った静かな部屋（デジタル騒音計にて 34dB から 38dB）を占有して実験を行った。

6.1.3 実験結果および考察

被験者が 12 名おり、システムが 2 パターン、5 回の 4 桁 PIN 入力を 2 回行ってもらったため、$12 \times 2 \times 5 \times 2 = 240$ 回の認証に成功したデータが集められた。これらのデータの解析を

行った。

Wheel タイプの認証成功率を図 6.2 に、Bar タイプの認証成功率を図 6.3 に示す。Wheel タイプでは 4 名の被験者がそれぞれ 1 回ずつ認証に失敗した。また、Bar タイプでは 4 名の被験者が 1 回ずつ認証に失敗し、2 名の被験者が 2 回ずつ認証に失敗した。

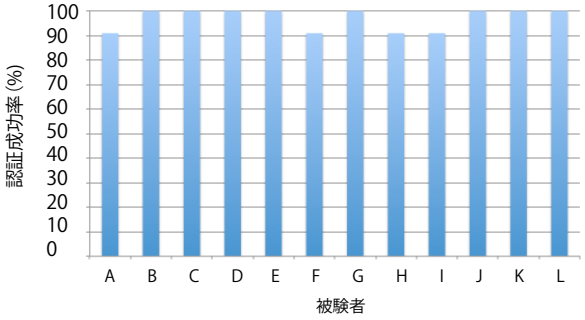


図 6.2: プロトタイプ 3 の Wheel タイプの認証成功率。

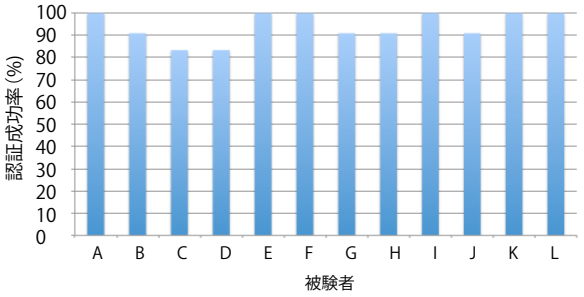


図 6.3: プロトタイプ 3 の Bar タイプの認証成功率。

また、それぞれを比較した図を図 6.4 に示す。Wheel タイプは 97.0%、Bar タイプは 94.2%、平均認証成功率は 95.6%であった。また、それぞれ t 検定を行った結果、有意差は見られなかった（$t(22) = 2.07, p = .32 > .05$）。よってどちらのシステムも認証成功率に関しては同程度であるといえる。またこの認証成功率は予備調査での結果（96.0%）とほぼ同じであった。この結果から、ユーザはプロトタイプ 3 をプロトタイプ 1 と同様にほとんど間違えること無く使用できるといえる。

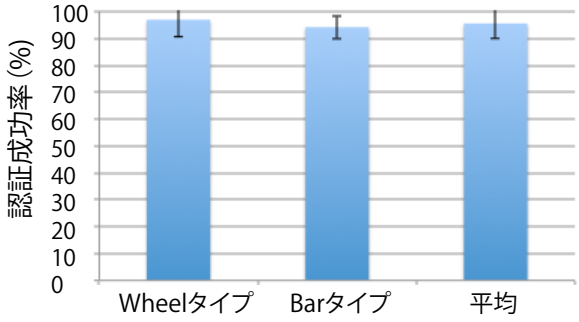


図 6.4: プロトタイプ 3 の平均認証成功率。

Wheel タイプの認証速度を図 6.5 に、Bar タイプを図 6.6 に示す。平均認証時間は被験者ごとに大きな違いが見られた。認証速度の遅かった Wheel タイプでの被験者 B は、認証中に自身の入力ミスに気づき、Delete キーを押すことによって再度入力していた。これは Bar タイプの被験者 C、被験者 I にも見られた。再度入力することにより、被験者は 5 桁以上の PIN を入力していることになる。これが認証速度が遅くなった原因であると考えられる。

また、Wheel タイプと Bar タイプを合わせた平均認証速度を図 6.7 に示す。t 検定を行った

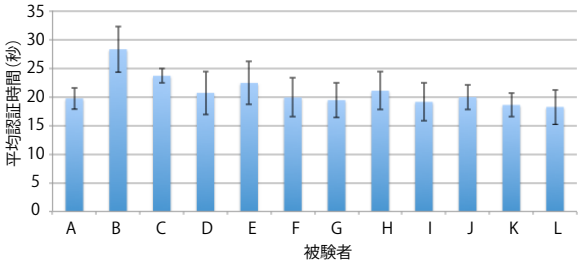


図 6.5: プロトタイプ 3 の Wheel タイプの認証速度。

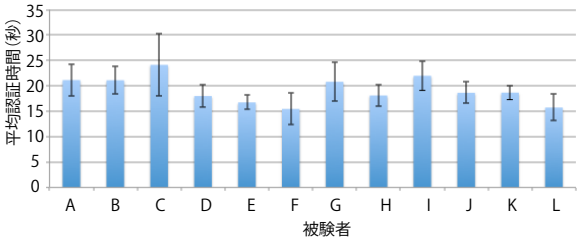


図 6.6: プロトタイプ 3 の Bar タイプの認証速度。

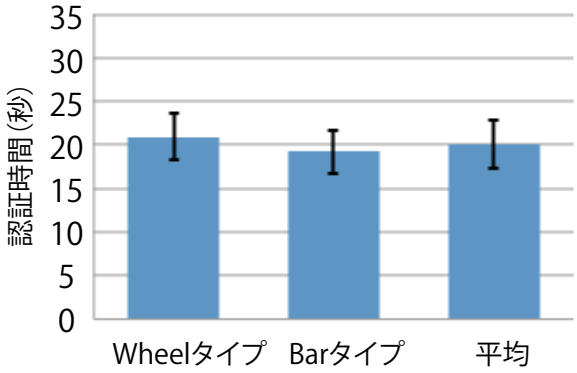


図 6.7: プロトタイプ 3 の平均認証速度。

結果、これらのタイプ間に差は見られなかった。

実験中に見られた被験者の携帯情報端末の把持方法を図 6.8 に示す。12 名の被験者のうち、6 名の被験者が図 6.8a に示すような片手把持を、残りの 6 名の被験者が図 6.8b に示すような両手把持を行っていた。この結果より、本手法はどちらの把持方法であっても利用できると言える。

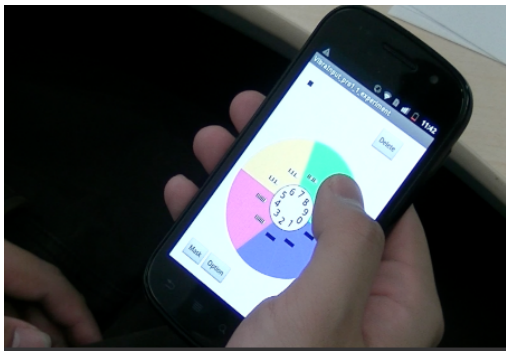
6.1.4 アンケート結果および考察

Wheel タイプと Bar タイプを比較してどちらが入力しやすかったかのアンケート結果を図 6.9 に示す。7 人の被験者が Wheel タイプが入力しやすいと答え、5 人の被験者が Bar タイプが入力しやすいと答えた。

Wheel タイプの利点として被験者から以下の意見が得られた。

- 今何回目の入力かわかりやすい。
- 1 回目はおおよその位置に移動するだけでよいので早く入力できた。
- 1 回目が大雑把で良いので楽だった。

a)



b)

図 6.8: 実験中に見られた被験者の携帯情報端末の把持方法。a）片手把持。b）両手把持。

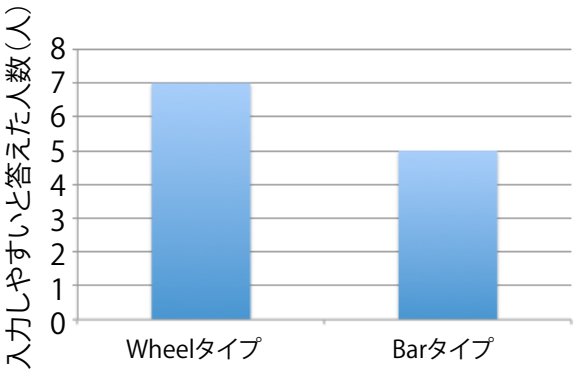


図 6.9: もう片方のプロトタイプと比較して、入力しやすいと答えた人数。

また Wheel タイプの欠点として被験者から以下の意見が得られた。

- 戻す方向が動かしづらい。
- 手で数字が隠れてしまった（3 名）。
- 180 度以上回そうとすると上手く回せなかった。

Wheel タイプでは、ユーザが何回目の入力か迷わないよう、数字を絞り込んでいくようにデザインしている。アンケート結果より、このデザインを好む被験者が複数人いることがわかった。その一方、直接ダイヤルを回すデザインにしていたため、手で数字が隠れてしまうという問題点を上げる被験者も見られた。この Wheel タイプのデザインについては第 7.3 節にて詳しく述べる。

同様に、Bar タイプの利点として被験者から以下の意見が得られた

- 見慣れている数字表記だったのでわかりやすかった。

また、Bar タイプの欠点として被験者から以下の意見が得られた。

- 左右、上下の入力の時、何番目の数を入力していたかわからなかった（3 名）。
- Wheel タイプと比較して、1 回目から数字を正確に合わせる必要があり面倒だった。
- Bar が動かしにくかった。(2 名）

プロトタイプ 3 の実装では、誤った移動による入力が起こりにくいよう、僅かな指の動きでは Bar が動かないように閾値を設定していた。しかし 2 名の被験者からは、この閾値により Bar が動かしにくかったという意見が得られた。そのため、今後は閾値の設定を見直す予定である。

6.2 安全性に関する実験 2

本システムに対してショルダーサフィンを行った場合、PIN を見破ることができるかの評価実験を行った。安全性に関する実験 1 では、被験者に後ろに立ってもらい、暗証番号を見てもらった。今回は被験者の入力の様子をビデオに録画し、それを本システムについて知識のある被験者に見てもらった。これにより、システムに詳しい実験者ではなく、初めて本システムを知り、利用した被験者の入力を対象とすることになり、予備実験よりも高い精度にて安全性を調べることができる。なお、この実験設計は先行研究 [DLHvZ+14] を参考にしている。また、この実験に使用した書類は付録 C として添付する。

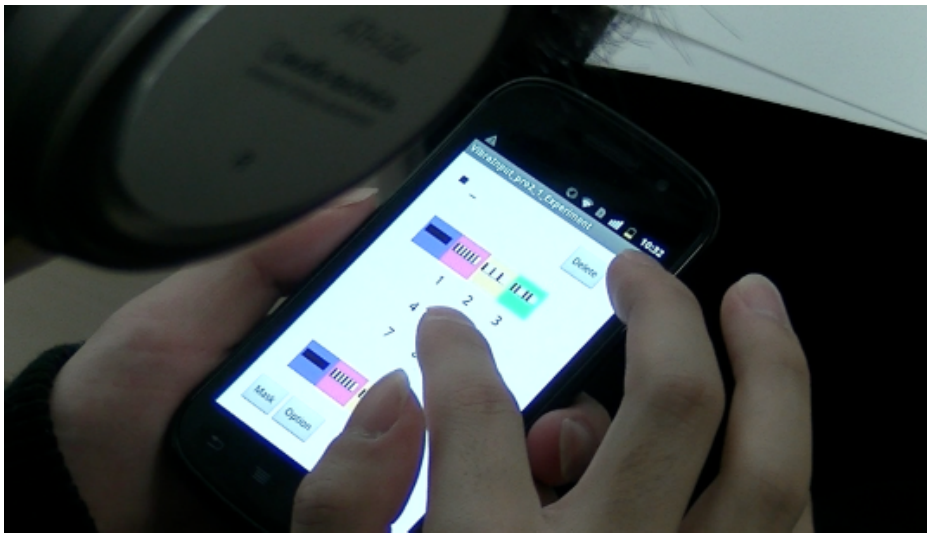


図 6.10: 録画されたビデオの例。ユーザの手元の手元が拡大され、ユーザの手の動きおよび携帯情報端末の画面が見えるようになっている。

6.2.1 被験者

23 歳と 26 歳の計 2 名の被験者に本実験を行ってもらった。この被験者は、予備調査において、本システムを実際に触っており、かつ本システムの改良にあたり意見をくれた 2 名である。被験者には基本給として 820 円を支払い、4 桁の PIN を当てることができた場合、1 種類のビデオにつき、謝礼金として 820 円払うこととした。また、実験後に、どのような観点から 4 桁の PIN を予想したかというアンケートを行った。

6.2.2 実験設計

4 桁の PIN 入力の容易性を調べる実験 3 において、12 人のユーザが Wheel タイプ、Bar タイプの両方を用いて PIN を入力したため、24 種類のビデオがあった。24 種類のビデオを 2 つのグループにランダムに分け、それぞれの被験者が各グループに対してショルダーサーフィンを行った。

対象とするビデオはユーザが最後に成功した 4 桁の PIN 入力の様子であり、それ以外のビデオはカットした。これはユーザがシステムに一定時間触り、慣れてきた所を攻撃の対象とする為である。さらに、ユーザには録画したビデオを用いてショルダーサーフィンの実験を行うことを伝えていないため、ビデオにはユーザが攻撃者を意識せずに入力している様子が録画されている。録画されたビデオの例を図 6.10 に示す。また被験者にはシステムについて説明し、プロトタイプ 3 を触ってもらった。すなわち、被験者はプロトタイプ 3 を熟知しており、攻撃対象のビデオにはプロトタイプ 3 を初めて触ったユーザの入力の様子が録画されている。そのため、この実験環境はユーザにとって悪いシナリオとなる。

図 6.11: 安全性に関する実験 2 の様子。被験者はヘッドホンをして音を聞きつつ、ショルダーサーフィンを行った。

被験者には 2 種類の攻撃を行ってもらった。1 つ目は目視によるショルダーサーフィンを想定した攻撃であり、2 つ目は録画によるショルダーサーフィンを想定したものである。目視によるショルダーサーフィンを想定した攻撃は 1 度のみの攻撃であり、ビデオを一度だけ見てもらった。実験の様子を図 6.11 に示す。この時、ビデオには音声も録音されているため、ユーザはヘッドホンをし、その音量は自由に操作できるものとした。ビデオ視聴後、ビデオに写っているユーザが入力している 4 桁の PIN を 3 通り予想してもらった。予想が外れた場合、被験者には録画によるショルダーサーフィンを想定した攻撃を行ってもらった。この実験では、被験者はビデオを自由に操作できた（スロー再生、一時停止、コマ送り、最初から見直す等のビデオプレイヤーにて行うことができる全ての操作)。被験者には好きな時間ビデオを操作してもらい、ビデオに写っているユーザが入力している 4 桁の PIN を 3 通り予想してもらった。

6.2.3 実験結果

両被験者とも、どのビデオに対してもショルダーサーフィンできなかった。すなわち、目視によるショルダーサーフィンおよび録画によるショルダーサーフィンどちらも成功しなかった。よって、本システムに対してショルダーサフィンを行ったとしても、攻撃者は PIN を見破ることができないといえる。

どのような観点から 4 桁の PIN を予想したかというアンケートに対して、両被験者とも携帯情報端末の音を聞くことにより予想しようとしたが、聞くことはできなかったと述べた。また、被験者のうち 1 名は、識別のために「ユーザの指を離す位置」や「指をタッチパネルにおいてから指を動かし始めるまでの時間（振動パターンの識別にかかった時間)」を用いたが、わからなかったと述べた。録画に関する詳しい議論は第 7.2 節に示す。

第7章　議論

本章では VibraInput の覗き見に対する安全性および録画に対する安全性を議論する。その後、Wheel タイプの改良、振動モータ、認証時間およびその短縮案を議論する。最後に、画像選択への応用とボタン式の認証システムへの応用を議論する。

7.1　覗き見に対する安全性

振動は毎回ランダムに発生するため、4 桁の PIN 入力を n 回見られた時に 4 桁の PIN が見破られる確率は Wheel タイプにて $(1-(1-0.002)^n)$、Bar タイプにて $(1-(1-0.0001)^n)$ となる。これは、4 桁の PIN 入力を 1 回見られた時に 4 桁の PIN が見破られる確率が、Wheel タイプにて 0.002 (0.2^4)、Bar タイプにて 0.0001 (0.1^4) だからである。

7.2　録画に対する安全性

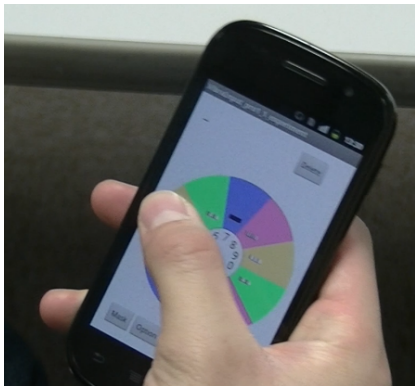
第 6.2 節の実験では、空調を切った静かな部屋にて、被験者の背後 50cm の距離から、被験者の手元をズームして録画した。電車の中や繁華街といった公共の場では、実験環境よりも雑音が多いことが予想されるため、公共の場においても本システムは録画に対しても強い耐性があるといえる。

しかしながら、さらに至近距離から録画を行った場合や、指向性マイクを用いて録画を行った場合の安全性については未調査である。また、ビデオに対するショルダーサーフィンの方法として、再生ソフトを操作することによるショルダーサーフィンではなく、特殊なソフトウェアを用いた解析への安全性も未調査である。よって今後はこれらを調査したい。

7.3　Wheel タイプの改良

プロトタイプ 1 からプロトタイプ 3 までの Wheel タイプでは「円が回しにくい問題」および図 7.1 に示すような「指にて隠れた数字を確認するような動作によるおおよその位置の特定という問題」があった。この問題を解決するため、円を直接タッチすることによる回転から、円の下に表示したバーを操作することによる回転に変更する予定である。バーを実装した Wheel タイプを図 7.2 に示す。ユーザはバーをタッチし、バーに表示されているカーソルを左右に移動させる。このカーソルの移動に連動して円が回転する。

a)



b)

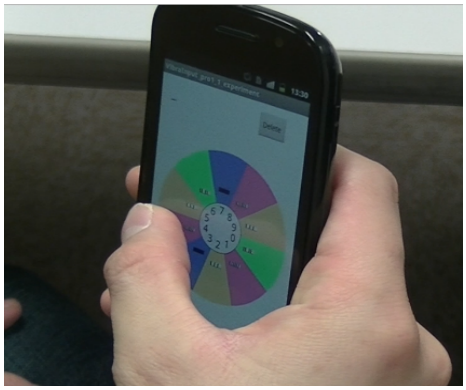


図 7.1: 指にて隠れた数字を確認するような動作。a）1、2、3、4 がユーザの指によって隠れてしまっているため、b）携帯情報端末を傾けてこれらの数字を確認している。

また、バーによる回転実装時には、2 回目の入力の際の回転量を一度に 2 個分回転するよう実装する。これにより、3 個連続にて並んでいる記号の中の一箇所を除く全ての位置にて回転を止める直前と止めた後が違う色になる。3 個連続にて並んでいる記号は 2 つあるため、候補は 7 種類となる。そのため、ユーザが必要以上の回転を行わない場合でも 1 桁の PIN を当てられる可能性は $(3/4) \times (1/7) + (1/4) \times (1/10)$ より 13.2%であり、4 桁であれば $13.2\%^4$ より 0.03%となる。これにより、第 4.2.1 節にて述べた以上の安全性が得られる。

7.4 振動モータ

携帯情報端末に搭載されている振動モータには大きな駆動音を出すものもあるため、全ての携帯情報端末において本システムが使えるとは限らない。しかし音を出しても良い環境（例えば、繁華街や路上など）下であれば、PIN 入力時に携帯情報端末からノイズを流すことにより、振動音の種類の識別を難しくすることができる。振動していることがわかったとしても、その振動パターンがわからなければ本システムは見破られることが無いためである。

また、今回の被験者は 20 代であるため、その結果として今回採用した振動間隔も 20 代に適したものと言える。しかし年齢によって識別できる振動間隔が異なる可能性がある. 同様に、振動モータの違いによっても識別できる振動間隔が異なる可能性もある。よって今後はこれらを調査したい。

7.5 認証時間

ショルダーサーフィンに対して安全であり、かつ 0 から 9 までの PIN を入力可能な携帯情報端末を対象としたシステムとの認証時間の比較の表を 7.1 に示す。VibraInput は先行研究と比較して、認証時間は速く、また認証成功率は高いという結果になった。なお、Phone

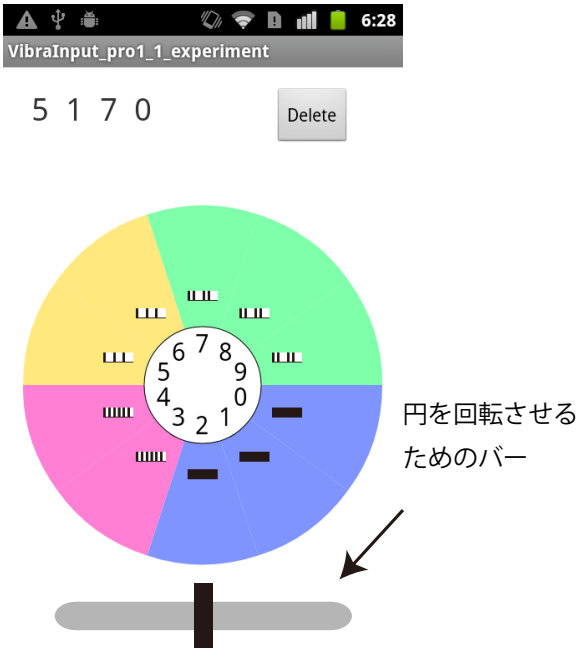


図 7.2: バーを実装した Wheel タイプ。バーを操作して円を回転させる。

Lock [BOKK11] は特殊なハードウェアを用いて実験を行っているため、特殊なハードウェアを用いない場合、実験の結果は異なることが考えられる。今後は、同一の被験者にて本システムとの比較調査を行いたい。

表 7.1: 認証時間の比較。

	認証時間（秒）	認証成功率（%）
VibraInput	20.1	95.6
Phone Lock [BOKK11]	28.2	89.6
CCC [石塚 14]	33.3	91.0

VibraInput は標準的な PIN 認証時間（1.7 秒）に比べると非常に遅いという欠点はあるが、予備調査において、10 人の被験者は覚えやすく使いやすいと答えていた。また、著者は 4 桁の PIN 入力を 12.4 秒にて入力可能であるため、「ユーザが覚えやすい記号を用いる」といった改良により、認証時間を改善できると考えている。著者はこのシステムは携帯情報端末のロックを解除するには遅いが、オンラインバンクの支払いなど重要かつ使用頻度の少ない場面においては有用であると考えている。

7.6 認証時間の短縮案

本節では、認証時間を短縮するための案を 2 種類示す。

1 つ目は、1 種類の振動パターンを用いて 2 度の入力を行い、1 つの数字を入力するシステムである。現在は 2 種類の振動パターンを用いて 1 つの数字を入力している。これに対して、1 種類の振動パターンを用いて 2 度の入力を行い、1 つの数字を入力することにより、安全性は低下するものの、認証時間が短縮されること予想される。なぜならば、ユーザが振動を識別する回数が、1 桁の PIN につき 2 回から 1 回に減る為である。入力の流れは以下の通りである。なお、この場合、4 桁の PIN を表すパターンは $4^4 = 256$ 通りとなる。以下にシステムの流れを示す。

1. 振動パターンがランダムに発生する。
2. 振動を表す記号を入力したい数字に合わせる。
3. 記号の配列が変わる、振動パターンは変わらない。
4. 振動を表す記号（2 と同じ記号）を入力したい数字に再度合わせる。

2 つ目は、振動パターンと指の動きを併用するシステムである。このシステムを図 7.3 に示す。また、認証の流れを以下に示す。

1. 画面をタッチすると振動が発生する。
2. 振動と現在の入力回数に対応したジェスチャを行う。
3. これを 3 回行う。

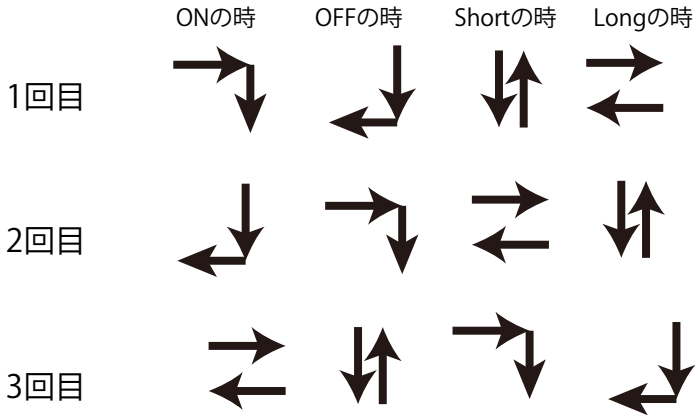


図 7.3: 振動パターンと指の動きを併用するシステム。

ユーザはあらかじめ振動パターンと指の動き（ジェスチャ）の対応を決めておき、振動パターンに合わせてあらかじめ決めておいた指の動きを行う。このシステムではショルダーサー

フィンに対する安全性は大きく低下するものの、認証時間の短縮が予想される。なぜならば、1 回の入力につき、ユーザが振動を識別する回数が 2 回から 1 回に減り、タッチパネルの操作が 2 回から 1 回に減るからである。なお、この場合のパターンの組み合わせは、4 方向への移動と一度移動した方向を除く 3 方向への移動を 1 回のジェスチャとすると、1 回のジェスチャは $4 \times 3 = 12$ 通りとなる。また、このジェスチャを 4 種類の振動と組み合わせた場合、$12 \times 4 = 48$ 通りとなる。さらに、これを 3 回行った場合、$48^3 = 110592$ 通りとなる。しかし、攻撃者はショルダーサーフィンを何度も行うことによって $4 \times 4 \times 4 = 64$ 通りまで絞ることができる。

7.7 画像選択への応用

本システムを用いて、ユーザは PIN 入力だけではなく、画像認証における画像の選択を行うことができる。図 7.4 に画像選択の例を示す。PIN 入力の際と同様にユーザは、1 回目の入力では現在の振動パターンを表す記号を入力したい画像がある列に移動させ、2 回目の入力では現在の振動パターンを表す記号を入力したい画像がある行に移動させる。これにより、ユーザは画像認証の覚えやすいという利点を活かしつつ、本システムを用いて安全に認証を行うことができる。

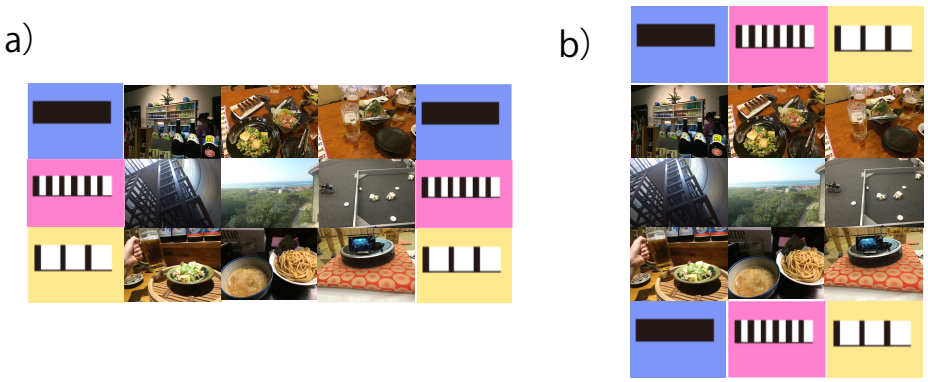


図 7.4: 画像の選択の例。a）1 回目の入力、b）2 回目の入力。

7.8 ボタン式の認証システムへの応用

タッチパネル式の携帯情報端末ではなく、ボタン式の認証システムに本システムを用いる応用を示す。図 7.5 にボタン式の認証システムに用いた場合の本システムを示す。なお、この図では振動パターンを表す記号にプロトタイプ 3 と同様のものを使用している。ユーザは現在の振動パターンの記号が書かれた行を確認し、入力したい数字が書かれている列のボタンを押すことによって、数字を選択することができる。

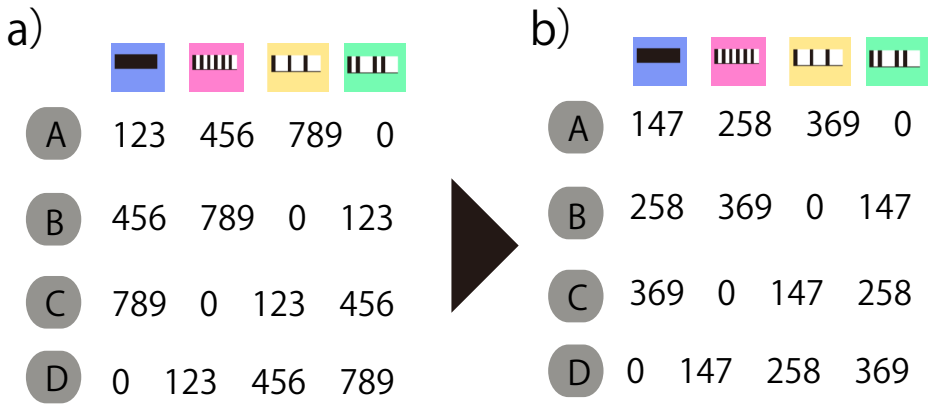


図 7.5: ボタン式の認証システムへの応用。ABCD がそれぞれボタンを表している。a）1 回目の入力、b）2 回目の入力。

1 を入力する例を示す。1 回目の入力にて、振動パターン B が発生したとする。図 7.5a に示すように、振動パターン B の列にある「123」はボタン D の行にあるため、ユーザはボタン D を押す。これによって「123」が候補になる。その後、画面が図 7.5b の様に変化する。次に 2 回目の入力にて、振動パターン D が発生したとする。振動パターン D の列にある「147」はボタン B の行にあるため、ユーザはボタン B を押す。これにより、2 回の選択の両方にて選ばれた数字である「1」が入力される。

第8章　結論

本研究では、パスワードを入力する際、ショルダーサーフィンによってパスワードを盗まれる危険があるという問題を解決するためのシステムである VibraInput を述べた。本システムでは、携帯情報端末の振動パターンと視覚情報を元に PIN 入力を安全に行うことができる。本システムを利用するユーザは、ランダムに提示される 4 種類の振動パターンに対応する記号を、入力したい数字に合わせる行為を 2 回行うことによって PIN 入力を行う。本システムでは 4 種類の振動パターンのみを使用するため、ユーザは簡単にパターンを覚えられ、識別することができる。また、本システムは既存の携帯情報端末が備える振動モータのみを用いて十分に実現することができる。振動パターンは目視では 確認することができないため、ショルダーサーフィンを行う攻撃者は、ユーザの入力を知ることができない。

本研究では VibraInput の設計を行った後に、予備調査として VibraInput のプロトタイプを設計しその評価を行った。その結果、平均認証成功率は 96.0%と高く、ショルダーサーフィンに対しても安全であった。その後、予備調査から得られたフィードバックを元にシステムの改良を行い、評価実験を行った。その結果、平均認証成功率は 95.6%と高い認証率を維持しつつ、平均認証時間を 23.8 秒から 20.1 秒に改良することができた。またビデオ録画によるショルダーサーフィンの実験も行い、これに対しても安全であることを確認した。

謝辞

本研究を遂行するにあたり、先生方、先輩方、同期、後輩と多くの方にお力添えを頂きました。3 年間研究活動を続けてこられたのは、皆様のおかげと感じております。ご助力くださった皆様に感謝申し上げます。

志築文太郎先生には、本研究の着手から本論文を締めるまで、懇切丁寧なご指導とご協力を頂きました。本研究のみに限らず、様々な研究を遂行することができたのは、先生の研究への取り組み方を教わることができたためです。提案から実験、論文執筆まで含めてとても長い時間お付き合い頂き、ご指導頂いたことに深く感謝いたします。

田中二郎先生、三末和男先生、高橋伸先生、Simona Vasilache 先生、嵯峨智先生には、ゼミや中間発表において、様々な視点からのご意見と研究発表に関する多くのご助言を頂きました。チーム内とは異なる視点からの意見を頂けたことにより、研究を進めるにあたって大変参考になりました。心より感謝いたします。

インタラクティブプログラミング研究室の皆様には研究活動と日常生活の両面において大変お世話になりました。特に、WAVE チームの皆様には日常的に行われる議論を通して多くのアドバイスを頂きました。このような恵まれた環境にて研究活動を遂行できたことは大変幸せだったと思います。特に、同期である大野誠氏、黒澤敏文氏、深津佳智氏とは互いに切磋琢磨し、お互いに助け合いながら研究活動を進めることができました。こうした同期の皆様の存在が研究を進める原動力となっていました。また、吉川拓人氏には卒業後も研究発表にあたりご協力頂きました。箱田博之氏、大西主紗氏には精神面、生活面でも大変お世話になりました。ここに感謝致します。

また、研究において欠かすことのできない被験者実験にご協力頂いた皆様に感謝致します。自身も忙しい身でありながら、様々な実験にお付き合い頂きました。皆様のご協力のおかげで研究の質を高めることができました。

最後に、両親を含め大学院生活においてお世話になった全ての方々に心よりお礼申し上げます。本当にありがとうございました。

参考文献

[AAIM08] Muhammad Daniel Hafiz Abdullah, Abdul Hanan Abdullah, Norafida Ithnin, and Hazinah Kutty Mammi. Towards identifying usability and security features of graphical password in knowledge based authentication technique. *Asia International Conference on Modeling & Simulation*, pp. 396–403, 2008.

[AGM+10] Adam J. Aviv, Katherine Gibson, Evan Mossop, Matt Blaze, and Jonathan M. Smith. Smudge attacks on smartphone touch screens. In *Proceedings of the 4th USENIX Conference on Offensive Technologies*, WOOT'10, pp. 1–7, Berkeley, CA, USA, 2010. USENIX Association.

[AK14] Md Tanvir Islam Aumi and Sven Kratz. Airauth: Towards attack-resilient biometric authentication using in-air gestures. In *CHI '14 Extended Abstracts on Human Factors in Computing Systems*, CHI EA '14, pp. 1585–1590, New York, NY, USA, 2014. ACM.

[BAKS+11] Noam Ben-Asher, Niklas Kirschnick, Hanul Sieger, Joachim Meyer, Asaf Ben-Oved, and Sebastian Möller. On the need for different security methods on mobile phones. In *Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services*, MobileHCI '11, pp. 465–473, New York, NY, USA, 2011. ACM.

[BCVO12] Robert Biddle, Sonia Chiasson, and P.C. Van Oorschot. Graphical Passwords: Learning from the first twelve years. *ACM Computing Surveys*, Vol. 44, No. 4, pp. 19:1–19:41, September 2012.

[BOK10] Andrea Bianchi, Ian Oakley, and Dong Soo Kwon. The secure haptic keypad: A tactile password system. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '10, pp. 1089–1092, New York, NY, USA, 2010. ACM.

[BOK11] Andrea Bianchi, Ian Oakley, and Dong Soo Kwon. Spinlock: A single-cue haptic and audio PIN input technique for authentication. In *Proceedings of the 6th international conference on Haptic and audio interaction design*, HAID'11, pp. 81–90, Berlin, Heidelberg, 2011. Springer-Verlag.

[BOKK11] Andrea Bianchi, Ian Oakley, Vassilis Kostakos, and Dong Soo Kwon. The Phone Lock: Audio and haptic shoulder-surfing resistant PIN entry methods for mobile devices. In *Proceedings of the fifth international conference on Tangible, embedded, and embodied interaction*, TEI '11, pp. 197–200, New York, NY, USA, 2011. ACM.

[BOLK10] Andrea Bianchi, Ian Oakley, Jong Keun Lee, and Dong Soo Kwon. The Haptic Wheel: Design & evaluation of a tactile password system. In *CHI '10 Extended Abstracts on Human Factors in Computing Systems*, CHI EA '10, pp. 3625–3630, New York, NY, USA, 2010. ACM.

[CF06] Nathan L. Clarke and Steven M Furnell. Authenticating mobile phone users using keystroke analysis. *International Journal of Information Security*, Vol. 6, No. 1, pp. 1–14, December 2006.

[CM09] Ming Ki Chong and Gary Marsden. Exploring the use of discrete gestures for authentication. In Tom Gross, Jan Gulliksen, Paula Kotzë, Lars Oestreicher, Philippe A. Palanque, Raquel Oliveira Prates, and Marco Winckler, editors, *INTERACT (2)*, Vol. 5727 of *Lecture Notes in Computer Science*, pp. 205–213. Springer, 2009.

[DHA10] Paul Dunphy, Andreas P. Heiner, and N. Asokan. A closer look at recognition-based graphical passwords on mobile devices. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, SOUPS '10, pp. 3:1–3:12, New York, NY, USA, 2010. ACM.

[DLHB+12] Alexander De Luca, Alina Hang, Frederik Brudy, Christian Lindner, and Heinrich Hussmann. Touch me once and i know it's you!: Implicit authentication based on touch screen patterns. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '12, pp. 987–996, New York, NY, USA, 2012. ACM.

[DLHvZ+14] Alexander De Luca, Marian Harbach, Emanuel von Zezschwitz, Max-Emanuel Maurer, Bernhard Ewald Slawik, Heinrich Hussmann, and Matthew Smith. Now You See Me, Now You Don'T: Protecting smartphone authentication from shoulder surfers. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '14, pp. 2937–2946, New York, NY, USA, 2014. ACM.

[DLvZH09] Alexander De Luca, Emanuel von Zezschwitz, and Heinrich Hussmann. VibraPass: Secure authentication based on shared lies. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '09, pp. 913–916, New York, NY, USA, 2009. ACM.

[DLvZN+13] Alexander De Luca, Emanuel von Zezschwitz, Ngo Dieu Huong Nguyen, Max-Emanuel Maurer, Elisa Rubegni, Marcello Paolo Scipioni, and Marc Langheinrich.

Back-of-device authentication on smartphones. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '13, pp. 2389–2398, New York, NY, USA, 2013. ACM.

[DLvZPH13] Alexander De Luca, Emanuel von Zezschwitz, Laurent Pichler, and Heinrich Hussmann. Using fake cursors to secure on-screen password entry. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '13, pp. 2399–2402, New York, NY, USA, 2013. ACM.

[DTH06] Rachna Dhamija, J. D. Tygar, and Marti Hearst. Why phishing works. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '06, pp. 581–590, New York, NY, USA, 2006. ACM.

[DY07] Paul Dunphy and Jeff Yan. Do background images improve "draw a secret" graphical passwords? In *Proceedings of the 14th ACM Conference on Computer and Communications Security*, CCS '07, pp. 36–47, New York, NY, USA, 2007. ACM.

[GHS06] Davrondzhon Gafurov, Kirsi Helkala, and Torkjel Søndrol. Biometric gait authentication using accelerometer sensor. *Journal of Computers (JCP)*, Vol. 1, No. 7, pp. 51–59, 2006.

[Gie06] Lauri Giesen. ATM Fraud: Does it warrant the expense to fight it? *Banking Strategies*, Vol. 82, No. 6, 2006.

[HvOP09] Cormac Herley, Paul C. van Oorschot, and Andrew S. Patrick. Passwords: If we're so smart, why are we still using them? In *Financial Cryptography and Data Security, 13th International Conference, FC 2009, Accra Beach, Barbados, February 23-26, 2009. Revised Selected Papers*, pp. 230–237, 2009.

[JMM+99] Ian Jermyn, Alain Mayer, Fabian Monrose, Michael K. Reiter, and Avi Rubin. The design and analysis of graphical passwords. In *8th USENIX Security Symposium*, pp. 1–14, 1999.

[JY11] Zach Jorgensen and Ting Yu. On mouse dynamics as a behavioral biometric for authentication. In *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*, ASIACCS '11, pp. 476–482, New York, NY, USA, 2011. ACM.

[KBS09] Amy K. Karlson, A. J. Bernheim Brush, and Stuart Schechter. Can I Borrow Your Phone?: Understanding concerns when sharing mobile phones. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '09, pp. 1647–1650, New York, NY, USA, 2009. ACM.

[MG09] Rene Mayrhofer and Hans Gellersen. Shake well before use: Intuitive and secure pairing of mobile devices. *IEEE Transactions on Mobile Computing*, Vol. 8, No. 6, pp. 792–806, 2009.

[MT11] James B. Miller and Jean-Michel Trivi. Touch gesture actions from a device's lock screen, 2011. US Patent App. 12/780,659.

[PPA04] Shwetak N. Patel, Jeffrey S. Pierce, and Gregory D. Abowd. A gesture-based authentication scheme for untrusted public terminals. In *Proceedings of the 17th Annual ACM Symposium on User Interface Software and Technology*, UIST '04, pp. 157–160, New York, NY, USA, 2004. ACM.

[RRF04] Volker Roth, Kai Richter, and Rene Freidinger. A PIN-entry method resilient against shoulder surfing. In *Proceedings of the 11th ACM conference on Computer and communications security*, CCS '04, pp. 236–245, New York, NY, USA, 2004. ACM.

[SPHZ13] Bahador Saket, Chrisnawan Prasojo, Yongfeng Huang, and Shengdong Zhao. Designing an effective vibration-based notification interface for mobile phones. In *Proceedings of the 2013 conference on Computer supported cooperative work*, CSCW '13, pp. 149–1504, New York, NY, USA, 2013. ACM.

[SZO05] Xiaoyuan Suo, Ying Zhu, and G. Scott Owen. Graphical passwords: A survey. In *In Proceedings of Annual Computer Security Applications Conference*, pp. 463–472, 2005.

[TK03] Tetsuji Takada and Hideki Koike. Awase-E: Image-based authentication for mobile phones using user's favorite images. In Luca Chittaro, editor, *Mobile HCI*, Vol. 2795 of *Lecture Notes in Computer Science*, pp. 347–351. Springer, 2003.

[TKC05] Desney S. Tan, Pedram Keyani, and Mary Czerwinski. Spy-Resistant Keyboard: More secure password entry on public touch screen displays. In *Proceedings of the 17th Australia conference on Computer-Human Interaction*, OZCHI '05, pp. 1–10, Narrabundah, Australia, Australia, 2005. Computer-Human Interaction Special Interest Group (CHISIG) of Australia.

[TOH06] Furkan Tari, A. Ant Ozok, and Stephen H. Holden. A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords. In *Proceedings of the second symposium on Usable privacy and security*, SOUPS '06, pp. 56–66, New York, NY, USA, 2006. ACM.

[Wei06] Daphna Weinshall. Cognitive authentication schemes safe against spyware (short paper). In *IEEE Symposium on Security and Privacy*, pp. 295–300. IEEE Computer Society, 2006.

[WWSB06] Susan Wiedenbeck, Jim Waters, Leonardo Sobrado, and Jean-Camille Birget. Design and evaluation of a shoulder-surfing resistant graphical password scheme. In *Proceedings of the Working Conference on Advanced Visual Interfaces*, AVI '06, pp. 177–184, New York, NY, USA, 2006. ACM.

[YCDS09] Sausan Yazji, Xi Chen, Robert P. Dick, and Peter Scheuermann. Implicit user re-authentication for mobile devices. In *Proceedings of the 6th International Conference on Ubiquitous Intelligence and Computing*, UIC '09, pp. 325–339, Berlin, Heidelberg, 2009. Springer-Verlag.

[Yui83] John Yuille. *Imagery, Memory, and Cognition: Essays in Honor of Allan Paivio*. Lawrence Erlbaum Associates, 1983.

[井芹 11] 井芹隼人, 岡本栄司. タッチパネルを用いた行動的特徴に基づくバイオメトリクスに関する一考察. In *CSS2011*, pp. 84–88. 情報処理学会, 2011.

[沖電 12] 沖電気工業株式会社. 自動取引装置、情報処理端末および覗き見防止カバー. 特開 2012-243112, 2012.

[居城 13] 居城秀明, 金岡晃, 岡本栄司, 金山直樹. タッチパネルによる手指の行動的特徴を用いた生体認証に関する一考察. 第 60 回 CSEC 研究会, pp. 1–8. 情報処理学会, 2013.

[高田 08] 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. 29–52, 2008.

[松下 01] 松下電器産業株式会社. 暗証番号入力装置. 特開 2001-147763, 2001.

[伸洋 01] 伸洋産業株式会社. カード暗証番号打機に使用されるキー隠しカバー及びキー隠しカバーが付設されたカード暗証番号打機. 特開 2001-325665, 2001.

[石塚 14] 石塚正也, 高田哲司. CCC:振動機能を応用した携帯端末での個人認証における覗き見攻撃対策手法の提案. インタラクション 2014, p. 3 pages. 情報処理学会, 2014.

[渡邊 13] 渡邊恵太, 石川直樹, 栗原一貴, 稲見昌彦, 五十嵐健夫. 複数ダミーカーソル中における自分自身のカーソル特定. インタラクション 2013 論文集, インタラクション 2013, pp. 25–31, 2013.

[産業 08] 独立行政法人産業技術総合研究所. フェイクポインタによる暗証番号入力装置および暗証番号入力方法. 特開 2008-33924, 2008.

[日本 06] 日本電気株式会社. 顔検知により盗み見を防止する処理装置、処理システム、現金自動預け入れ支払機、処理方法、及びプログラム. 特開 2006-39841, 2006.

[日立 08] 日立オムロンターミナルソリューションズ株式会社. 自動取引装置. 特開 2008-287646, 2008.

付 録A　予備調査に使用した書類

第 4 章における実験の際に使用した誓約書、実験手順書およびアンケートを付録として以下に示す。

A.1　誓約書

誓約書

携帯情報端末上の振動を用いた PIN 入力におけるデータ収集

文責：栗原拓郎

この度は実験にご協力いただき、ありがとうございます。

○本実験は、携帯情報端末上の振動を用いた PIN 入力について調査することを目的とします。

○実験途中には、各ブロックの間であれば自由に休憩を取ることが可能です。

○実験への参加は協力者の自由意志によるものであり、
実験への参加を随時拒否・撤回することが可能です。

○この実験によって得られたデータは、個人が特定できないように処理を行います。

○学内外にて発表する論文に実験結果を利用することがありますが、
いかなる場合においても協力者のプライバシーは保全されます。

実験に関して、上記内容を十分に理解し、同意していただけましたら下部の署名欄に
署名をお願いいたします。

平成　　年　　月　　日

所属＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

署名＿＿＿＿＿＿＿＿＿＿＿＿

説明者　所属　システム情報工学研究科　コンピュータサイエンス専攻

氏名＿＿＿＿＿＿＿＿＿＿＿＿

A.2　実験手順書

実験手順書

携帯情報端末上の振動を用いた PIN 入力に関する実験手順

文責：栗原拓郎

この度は実験にご協力いただき、ありがとうございます。
実験は 3 セットあります。
なお、実験の所要時間は合計で 20 分程度です。

◎実験内容

本実験は、携帯情報端末上の振動を用いて PIN 入力をしてもらう実験です。実験開始前に振動と対応する色を覚えてもらいます。

1.　入力方法
- 外側の円にタッチすることにより振動が開始されます
- 外側の円をタッチしたまま指を動かすことにより外側の円も回転します。
- 振動と対応する色を入力したい数値に合わせてください。
- これを 2 回行うことにより数値がひとつ入力されます

2.　実験手法
- 画面上部に入力してほしい PIN 番号が表示されます。
- また入力状態も画面上部に表示されます。
- PIN 入力はできる限り正確に行って下さい。
- 正確さを第一に、押し間違えをしない程度に素早く PIN 番号を入力して下さい。
- 1 回の PIN 入力終了後から次の PIN 入力開始までの間は休憩をとってもらってかまいません。
- 5 回 PIN 入力に成功すると 1 セットが終了します。
- これを 3 セット行ってもらいます

A.3　アンケート 1

携帯端末上の振動を用いた PIN 入力に関するアンケート

携帯端末上の振動を用いた PIN 入力に関する実験にご協力いただきありがとうございます。
アンケートにご協力をお願いします。

性別　男 ・ 女　　利き手　右 ・ 左　　年齢

使用している携帯情報端末名：　　携帯使用歴

気になる点がありましたらお応え下さい

A.4　アンケート 2

1 回目に入力したと思われる PIN 番号をご記入下さい

2 回目に入力したと思われる PIN 番号をご記入下さい

3 回目に入力したと思われる PIN 番号をご記入下さい。

振動音は聞こえましたか？　　はい・いいえ

振動音の種類はわかりましたか？　　はい・いいえ

付 録B　評価実験に使用した書類

第 6 章の 4 桁の PIN 入力の容易性を調べる実験 3 に使用した誓約書、実験手順書およびアンケートを付録として以下に示す。

B.1　誓約書

誓約書

携帯情報端末上の振動を用いた PIN 入力におけるデータ収集

文責：栗原拓郎

この度は実験にご協力いただき、ありがとうございます。

○本実験は、携帯情報端末上の振動を用いた PIN 入力について調査することを目的とします。

○実験途中には、各ブロックの間であれば自由に休憩を取ることが可能です。

○実験への参加は協力者の自由意志によるものであり、
実験への参加を随時拒否・撤回することが可能です。

○この実験によって得られたデータは、個人が特定できないように処理を行います。

○学内外にて発表する論文に実験結果を利用することがありますが、
いかなる場合においても協力者のプライバシーは保全されます。

実験に関して、上記内容を十分に理解し、同意していただけましたら下部の署名欄に
署名をお願いいたします。

平成　　年　　月　　日

所属＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

署名＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

説明者　所属　システム情報工学研究科　コンピュータサイエンス専攻

氏名＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

B.2　実験手順書

実験手順書

携帯情報端末上の振動を用いた PIN 入力に関する実験手順

文責：栗原拓郎

この度は実験にご協力いただき、ありがとうございます.
実験は 2 種類あり，実験前に 2〜4 分間入力の練習をしてもらいます.
実験の所要時間は合計で 1 時間程度です.
実験後にアンケートを行います.

◎実験内容

本実験は，携帯情報端末上の振動を用いて PIN 入力をしてもらう実験です.
実験開始前に 4 種類の振動パターンと対応する記号を覚えてもらいます.

1.　入力方法：Wheel Type
・ 入力したい数字を絞り込んでいく手法です.
・ 円にタッチすることによりランダムに振動パターンが発生します.
　　注：タッチした位置に書かれた記号と発生する振動パターンに対応はありません.
・ 円をタッチしたまま指を動かすことにより円が回転します.
・ 現在の振動パターンに対応する記号を入力したい数字に合わせてください。
・ 指を離すと入力が確定し，振動パターンを表す記号の位置が変わります.
・ 以上を 2 回行うことによって数字がひとつ入力されます．つまり，1 回目の入力により
おおよその位置を確定し，2 回目の入力によって入力する PIN を確定します.
・
2.　入力方法：Bar Type
・ 交互にバーに書かれた記号を移動させて数字を入力する手法です.
・ 縦の棒にタッチすることによりランダムに振動パターンが発生します.
注：タッチした位置に書かれた記号と発生する振動パターンに対応はありません.
・ 縦の棒をタッチしたまま指を動かすことにより記号が移動します.
・ 振動と対応する記号を入力したい数字の列 (2 回目であれば行) に合わせてください。
・ これを 2 回行うことにより数値がひとつ入力されます

3. 実験手法

- 4 種類の振動パターンと記号の対応を覚えてもらいます.
- Wheel タイプ，Bar タイプそれぞれについて次の実験をしてもいます.
- 入力してほしい 4 桁の PIN（以降，PIN）を予めテーブルの上においておくため，PIN 入力前に覚えてください
- PIN 入力はできる限り正確にかつ素早く行って下さい。
- 1 回の PIN 入力終了後から次の PIN 入力開始までの間は休憩をとってもらってかまいません。
- 5 回 PIN 入力に成功すると 1 セットが終了します。
- これを 3 セット行ってもらいます.

B.3　アンケート

携帯端末上の振動を用いた PIN 入力に関するアンケート

携帯端末上の振動を用いた PIN 入力に関する実験にご協力いただきありがとうございます。
アンケートにご協力をお願いします。

性別　男 ・ 女　利き手　右 ・ 左　年齢

専攻

使用している携帯情報端末名：

携帯使用歴：　　スマートフォン使用歴：

端末のロック方法（パターンロック，PIN 等）：

Wheel タイプと Bar タイプどちらが入力しやすかったですか　Wheel ・ Bar

Wheel タイプについて気になる点がありましたらお応え下さい.

Bar タイプについて気になる点がありましたらお応え下さい.

他に何か気になる点がありましたらお応え下さい.

付 録C　評価実験に使用した書類

第 6 章の安全性に関する実験 2 に使用した誓約書、実験手順書およびアンケートを付録として以下に示す。

C.1　誓約書

誓約書

ショルダーサーフィンへの安全性に関する実験手順

文責：栗原拓郎

この度は実験にご協力いただき、ありがとうございます。

○本実験は、提案システムである VibraInput のショルダーサーフィンへの安全性を調査することを目的とします。

○実験途中には、各ブロックの間であれば自由に休憩を取ることが可能です。

○実験への参加は協力者の自由意志によるものであり、
実験への参加を随時拒否・撤回することが可能です。

○この実験によって得られたデータは、個人が特定できないように処理を行います。

○学内外にて発表する論文に実験結果を利用することがありますが、
いかなる場合においても協力者のプライバシーは保全されます。

実験に関して、上記内容を十分に理解し、同意していただけましたら下部の署名欄に
署名をお願いいたします。

平成　　年　　月　　日

所属＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

署名＿＿＿＿＿＿＿＿＿＿＿＿

説明者　所属　システム情報工学研究科　コンピュータサイエンス専攻

氏名＿＿＿＿＿＿＿＿＿＿＿＿

C.2　実験手順書

実験手順書

ショルダーサーフィンへの安全性に関する実験手順

文責：栗原拓郎

この度は実験にご協力いただき、ありがとうございます。
実験の所要時間は 1 時間程度です。
実験後にアンケートを行います。

◎実験内容

本実験は、提案システムである VibraInput のショルダーサーフィンへの安全性を調査する実験になります。
VibraInput を用いて PIN を入力している動画を見て、入力している 4 桁の PIN を当ててもらいます。

なお、入力方法は以下の通りです。

1. 入力方法：Wheel Type

・ 入力したい数字を絞り込んでいく手法です。
・ 円にタッチすることによりランダムに振動パターンが発生します。
　注：タッチした位置に書かれた記号と発生する振動パターンに対応はありません。
・ 円をタッチしたまま指を動かすことにより円が回転します。
・ 現在の振動パターンに対応する記号を入力したい数字に合わせてください。
・ 指を離すと入力が確定し、振動パターンを表す記号の位置が変わります。
・ 以上を 2 回行うことによって数字がひとつ入力されます。つまり、1 回目の入力によりおおよその位置を確定し、2 回目の入力によって入力する PIN を確定します。
・

2. 入力方法：Bar Type

・ 交互にバーに書かれた記号を移動させて数字を入力する手法です。
・ 縦の棒にタッチすることによりランダムに振動パターンが発生します。
　注：タッチした位置に書かれた記号と発生する振動パターンに対応はありません。
・ 縦の棒をタッチしたまま指を動かすことにより記号が移動します。
・ 振動と対応する記号を入力したい数字の列（2 回目であれば行）に合わせてください。
・ これを 2 回行うことにより数値がひとつ入力されます

3. 実験手法

- 4 種類の振動パターンと記号の対応を覚えてもらいます。
- Wheel タイプおよび Bar タイプの入力方法を確認してもらいます。
- 動画を 1 度見てもらいます。この時、ヘッドホンをして動画の音も同時に聞いてもらいます。音量は自由に操作できるものとします。
- 動画視聴後、3 回入力している 4 桁の PIN を予想してもらいます。
- （予想が外れた場合）動画を自由に操作してもらい、改めて 3 回入力している PIN を予想してもらいます。この自由に操作とは、再生、スロー再生、一時停止、コマ送り、逆再生など動画プレイヤーにて行うことができる全ての操作です。
- 以上を 12 種類の動画に対して行ってもらいます。
- 4 桁の PIN を当てることができた場合、1 種類の動画につき、謝礼金を 820 円増やします。つまり最大 820 円 x12 種類 = 9840 円増額されます。

C.3　アンケート

ショルダーサーフィンへの安全性に関する実験手順

ショルダーサーフィンへの安全性に関する実験にご協力いただきありがとうございます。
アンケートにご協力をお願いします。

性別　男 ・ 女　利き手　右 ・ 左　年齢

携帯使用歴：　スマートフォン使用歴：

端末のロック方法（パターンロック，PIN 等）：

どのような観点から 4 桁の PIN を予想しましたか。