携帯情報端末上の振動と視覚情報を組み合わせた 2段階PIN入力システム

栗原 拓郎[*1]　志築 文太郎[*2]　田中 二郎[*1]

Two-step PIN Entry System for Smartphones based on Vibration and Visual Information

Takuro Kuribara[*1], Buntarou Shizuki[*2] and Jiro Tanaka[*1]

Abstract – **Current PIN entry systems for smartphones suffer from shoulder surfing. In this paper, we present VibraInput, a two-step PIN entry system for smartphones based on the combination of vibration and visual information. In this system, users can safely enter a digit by two distinct selections. In addition, this system only uses four vibration patterns. Therefore, we believe that this design allows users to easily remember and recognize the patterns. Moreover, the vibration patterns can be generated on current off-the-shelf smartphones. We designed two kinds of prototypes of VibraInput. We conducted experiments to measure its usability and security problem. As a result, the mean failure rate is 4.0%; moreover the system shows good security properties.**

Keywords : **Security, privacy, authentication.**

1. はじめに

携帯情報端末（端末）には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おり [2], [12]，端末をパスワードによりロックすることは重要であると言える．しかし，電車内など周囲に人が多くいる公共の場において，端末のロックを解除する際，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 [7], [17]．この危険は端末を用いてメール，SNSおよびオンラインバンクを利用する際のパスワード入力においても存在する．

そこで我々は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を示す．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．

我々は，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するための予備実験を行った．実験結果を元に，図1に示すように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入力を行う評価実験およびショルダーサーフィンに対する安全性の評価実験を行った．その結果，平均認証失敗率は4%と低く，ショルダーサーフィンに対しても安全であった．本稿では，これらについて報告する．

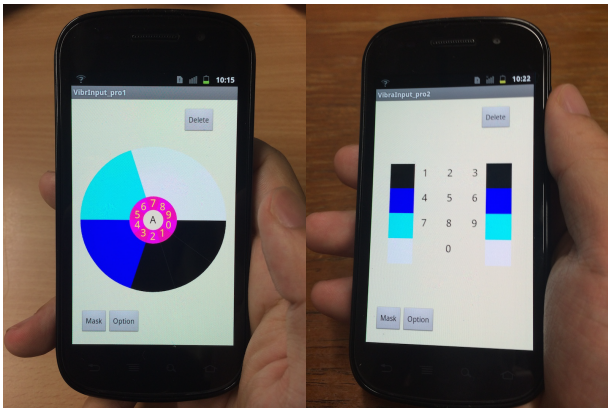

図1　VibraInputのプロトタイプ
Fig. 1　Two prototypes of VibraInput.

2. 関連研究

本研究ではショルダーサーフィン対策として振動を用いた安全なPIN入力システムを提案している．また，数字を入力する際は，端末をなぞることによって対応する記号を入力したい数字に移動させる．そこでショルダーサーフィン対策および端末をなぞるパスワード入力手法について述べる．

*1: 筑波大学 システム情報工学研究科 コンピュータサイエンス専攻
*2: 筑波大学 システム情報系
*1: Department of Computer Science, Graduate School of Systems and Information Engineering, University of Tsukuba.
*2: Faculty of Engineering, Information and Systems, University of Tsukuba.

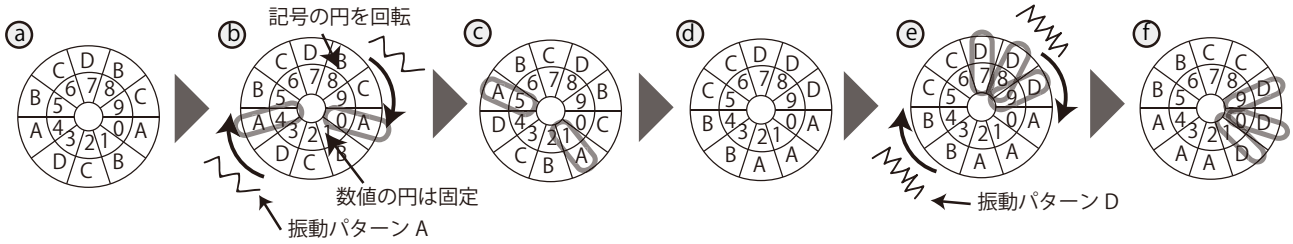

図 2　入力方法（1 を入力する例）．a）1 回目の初期状態，b）ユーザがタッチすると振動が開始される．ユーザは端末の振動パターンに対応する記号 A を 1 に合わせる．c）リリースにより入力候補（1，5）が確定し，d に状態が遷移．d）2 回目の初期状態，e）振動が開始される．ユーザは端末の振動パターンに対応する記号 D を 1 に合わせる．f）リリースにより 1 が確定し，状態は a に遷移．

Fig. 2　Example of entering ‘1’, a) initial state of the first selection, b) vibration pattern A is started. c) users can move a symbol A to ‘1’. When users release, ‘1’ and ‘5’ become the candidates and the state changes to the second selection, d) initial state of the second selection, e) vibration pattern D is started, e) users can move a symbol D to ‘1’, f) when users release, ‘0’, ‘1’ and ‘9’ become the candidates, f) ‘1’ is entered as a PIN and the state changes to a.

2.1　ショルダーサーフィン対策

渡辺ら [18] や Luca ら [9] は，複数のカーソルを用いたパスワード入力を提案している．Spy Resistant Keyboard [16] 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．また，Luca ら [5] は，視線をパスワード入力に用いる手法を提案している．Roth ら [13] 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．これらの研究と比較し，我々のシステムでは録画に対しても安全性を持つ．

振動を用いた認証システムとして VibraPass [7] がある．この研究では，PIN 入力の際に端末の振動が起こった場合，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，我々は振動パターンを元に PIN 入力を行う．

高田ら [19] 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予め覚えておき，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．この手法では予め覚えていた情報が知られた場合に見破られるが，我々のシステムでは振動パターンと振動パターンを表す記号の対応が知られたとしても PIN が見破られることはない．

2.2　端末をなぞるパスワード入力手法

Draw-a-Secret [11] は端末をなぞるパスワード入力手法として初のものであり，この手法を改良した研究もいくつか存在する [10], [15]．しかし，これらの研究はショルダーサーフィンに弱いことが指摘されている [1]．

Phone Lock [3] は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．Spinlock [4] 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．また，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 [6], [8] も存在する．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 台の端末を組み合わせている．一方，我々は端末に内蔵された振動モータのみを用いて実装を行っている．

3.　VibraInput

本節では提案システムである VibraInput における PIN 入力方法および設計方針を述べる．

3.1　入力手法

一般的な PIN は 0 から 9 までの数字から成るため，本システムも一般的な PIN 入力が行えるよう，10 種類の数字を入力できるよう設計する．本システム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．つまり，2 回の入力によって 1 つの数字を入力する．また，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 4 桁の PIN を覚えており，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 2 に示す．ユーザは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 2 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 2b 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 2c 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．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 2e 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 2a とは異なっている．図 2f 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．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．

3.2 設計方針

VibraInput は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，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．そこで我々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．そこで我々は 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．

4. 予備実験

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．今回，我々は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．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（振動間隔）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．

4.1 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．被験者には端末を自由に把持してもらった．

4.2 実験設計

実験には Android 2.3.4 を搭載した Google Nexus S を端末として用いた．被験者には図 3 に示すように椅子に座り，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．

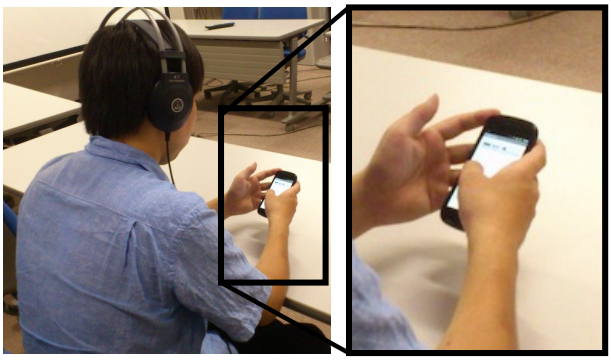

図 3 椅子に座り，端末を把持しながら予備実験 1 を行っている様子．
Fig. 3 A participant sits on a chair and holds the mobile device in the preliminary experiment.

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，振動間隔を変えた 6 種類の組み合わせを用意した．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 と呼称する．また，使用する 4 種類の振動パターンを図 4 に，使用したボタンを図 5 に示す．なお，振動間隔 A は 25ms，50ms，75ms，100ms，125ms，150ms の 6 種類とした．

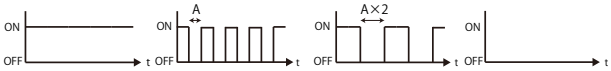

図 4 使用する振動パターン．左から ON，Short，Long，OFF．
Fig. 4 Using vibration patterns. From left to right: ON, Short, Long, OFF.

図 5 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
Fig. 5 The buttons which participants used in the experiment. From left to right: ON, Short, Long, OFF.

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．

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 [3], [14] 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．

4.3 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 6，および図 7 に示す．

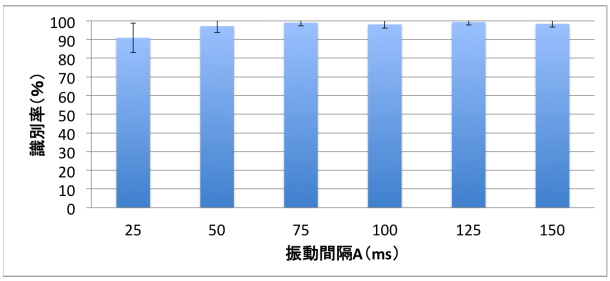

図 6　振動パターンの識別率
Fig. 6　Mean accuracy rates in the preliminary experiment.

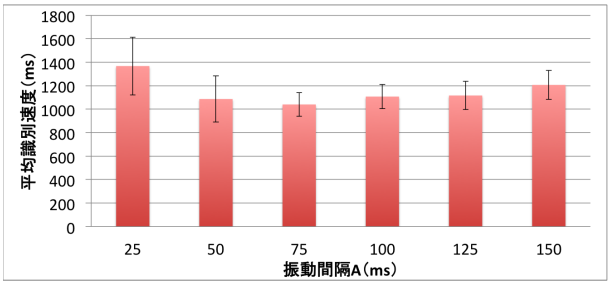

図 7　振動パターンの平均識別速度
Fig. 7　Mean times required to recognize in the preliminary experiment.

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．25ms が他の間隔に比べて有意に精度が悪く（90.1%, $p < .05$），また，150ms を除く他の間隔に比べて有意に遅かった（1.36 秒, $p < .05$）．有意差は見られなかったものの，以降の実装では，99.1%と識別率が高くかつ，平均識別速度が最も速い 75ms を振動間隔 A として採用することとした．

4.4 プロトタイプ

我々は bar タイプおよび wheel タイプと呼称する 2 種類の VibraInput のプロトタイプを実装した．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回転させることによって数字を入力する．bar 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．このデザインにおいて，振動パターンと記号の対応が他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．

4.5 wheel タイプ

図 8 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．外側の円を回転させ，内側の円に書かれた数字に現在の振動パターンに対応する色を合わせることによって数字の選択を行う．

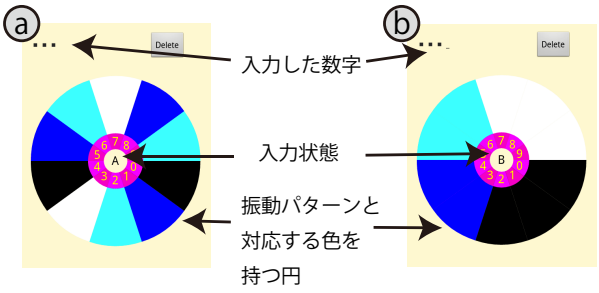

図 8　wheel タイプ．a）1 回目の選択における初期状態，b）2 回目の選択における初期状態
Fig. 8　Prototype of VibraInput: wheel type. a) initial state of the first selection, b) initial state of the second selection.

図 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，色は図 8b 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 入力が見破られる可能性は $(3/4) \times (1/4) + (1/4) \times (1/10)$ より，21.3%である．

また，4 桁の PIN 入力であれば 21.3%[4] より，見破られる可能性は 0.2%となる．

4.6 bar タイプ

図 9 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．

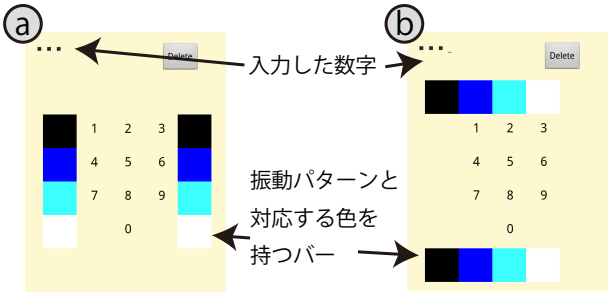

図 9　bar タイプ．a）1 回目の選択における初期状態，b）2 回目の選択における初期状態
Fig. 9　Prototype of VibraInput: bar type. a) initial state of the first selection, b) initial state of the second selection.

図 9a 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 9b に示すように縦のバーは消え，横のバーが表示される．

5. 評価実験 1：4 桁の PIN 入力の成功率

VibraInput を 4 桁の PIN 入力にて使用した場合の成功率を調べるための評価実験を行った．

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 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．被験者には端末を自由に把持してもらった．

5.2 実験設計

実験には Android 2.3.4 を搭載した Google Nexus S と，本システムのプロトタイプを用いた．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，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 10 に示す．被験者が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．

図 10　評価実験 1 において，被験者が PIN を入力している様子
Fig. 10　A participant entering PINs using VibraInput in Experiment 1.

入力してもらう PIN は予めランダムに作成された番号であり，この PIN を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．

5.3 実験結果および考察

図 11 に示すように，平均認証失敗率は 4%であった．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，図 12 に示すように，平均認証時間は 23.8 秒であった．また数人の被験者から，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および振動により手がしびれて振動パターンの識別に時間がかかったという意見が得られた．

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

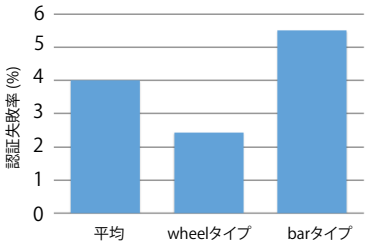

図 11　2 種類のプロトタイプの平均認証失敗率
Fig. 11　Mean failure rates of two prototypes of VibraInput.

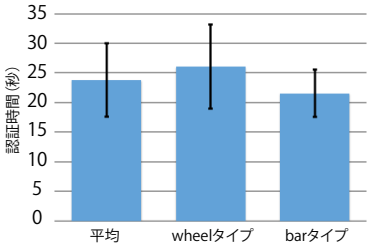

図 12　2 種類のプロトタイプの平均認証時間
Fig. 12　Mean authentication times of two prototypes of VibraInput.

回転させるのが難しいとコメントしていた為，これが wheel タイプにおいて入力が遅くなった原因だと考えられる．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 7.2 節にて議論する．

6.　評価実験 2：ショルダーサーフィン

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について評価実験を行った．

6.1　被験者

評価実験 1 を行った 24 名を被験者とした．被験者には，評価実験 1 にて使用したプロトタイプに対して，ショルダーサーフィンを行ってもらった．その為，全ての被験者はプロトタイプ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．

6.2　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 13 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，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．

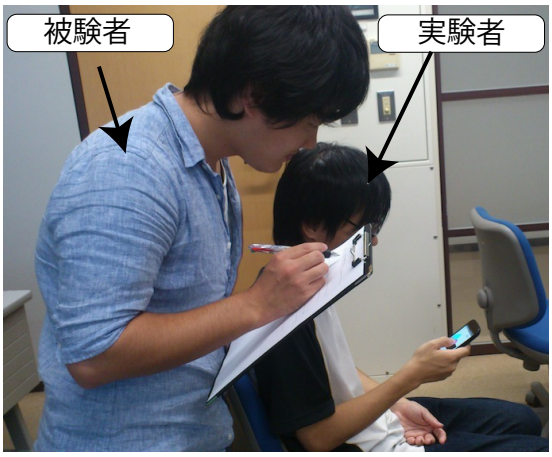

図 13　評価実験 2 において，被験者がショルダーサーフィンを行っている様子
Fig. 13　A participant conducting shoulder surfing from a position directly behind the researcher's shoulder in Experiment 2.

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．

6.3　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．

しかし，wheel タイプにおいて，実験者が入力する際，自身の指にて数字を隠してしまい，手の隙間から数字を確認している様子からおおよその位置を当てられてしまうことがあった．これについては 7.2 節にて議論する．

7.　議論

本節では VibraInput の安全性および wheel タイプの改良，振動パターン，認証時間について議論する．

7.1　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．

1: サンコー 小型デジタル騒音計 RAMA11O08

また，録画に対して安全であるかを調べるため，評価実験 2 と同じ環境にて本システムの入力の様子を録画した．動画を確認したところ，目視では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．今後，録画に対しての安全性についても詳しく評価実験を行う予定である．

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，色ではなくアルファベットや図にした実装も行い，振動との対応を覚えやすい記号や見やすい記号について今後調査したい．

7.2 wheel タイプの改良

今回の実装では「円が回しにくい問題」および「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，円の回転を直接タッチではなく，円の下にシークバーを表示し，シークバーをスライドさせることにより円を回転させる実装を行う予定である．

また，シーク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，4.5 節にて述べた以上の安全性を確立することができる．

7.3 振動パターン

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下であれば，PIN 入力時に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．さらに，今回は Short と Long を振動間隔 A とその 2 倍に設定したが，これを大きく変えた振動間隔にすること（例：振動間隔 A とその 3 倍にする）や，複数の振動間隔を組み合わせたパターンも考えられる．今後はこれらを調査したい．

7.4 認証時間

VibraInput は先行研究に近い認証時間（23.8 秒）となった（例：Bianchi ら [3]： 20.2 秒，Roth ら [13]： 23.3 秒）．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，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，著者は評価実験 1 と同条件にて 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．我々はこのシステムは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．

8. まとめと今後の課題

我々は振動を用いた安全な PIN 入力システムである VibraInput を示した．また，本システムを 2 種類のプロトタイプとして実装し，4 桁の PIN 入力の認証失敗率およびショルダーサーフィンに対して安全であるかの評価実験を行った．その結果，VibraInput は認証失敗率が低く，ショルダーサーフィンに対して安全であることが確認できた．

また，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，今後は，2 種類のプロトタイプの詳細な比較を行うために，被験者内実験を行う予定である．また，今回の評価実験では振動間隔を定め，振動パターンを表す記号に色を用いたが，これを異なる振動間隔や振動パターンを表す別の記号を使用した場合の，PIN 入力の認証失敗率および認証時間を今後調査したい．

参考文献

[1] M. D. H. Abdullah, A. H. Abdullah, N. Ithnin, and H. K. 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).

[2] N. Ben-Asher, N. Kirschnick, H. Sieger, J. Meyer, A. Ben-Oved, and S. 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 (2011).

[3] A. Bianchi, I. Oakley, V. Kostakos, and D. S. Kwon. The Phone Lock: Audio and haptic shoulder-surfing resistant PIN entry methods for mobile devices. In *Proceedings of the fifth interna-*

tional conference on Tangible, embedded, and embodied interaction, TEI '11, pp. 197–200 (2011).

[4] A. Bianchi, I. Oakley, and D. S. 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 (2011).

[5] A. De Luca, M. Denzel, and H. Hussmann. Look into My Eyes!: Can you guess my password? In *Proceedings of the 5th Symposium on Usable Privacy and Security*, SOUPS '09, pp. 7:1–7:12 (2009).

[6] A. De Luca, M. Harbach, E. von Zezschwitz, M.-E. Maurer, B. E. Slawik, H. Hussmann, and M. 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 (2014).

[7] A. De Luca, E. von Zezschwitz, and H. 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 (2009).

[8] A. De Luca, E. von Zezschwitz, N. D. H. Nguyen, M.-E. Maurer, E. Rubegni, M. P. Scipioni, and M. Langheinrich. Back-of-device authentication on smartphones. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '13, pp. 2389–2398 (2013).

[9] A. De Luca, E. von Zezschwitz, L. Pichler, and H. 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 (2013).

[10] P. Dunphy and J. 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 (2007).

[11] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. Rubin. The design and analysis of graphical passwords. In *8th USENIX Security Symposium*, pp. 1–14 (1999).

[12] A. K. Karlson, A. B. Brush, and S. 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 (2009).

[13] V. Roth, K. Richter, and R. 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 (2004).

[14] B. Saket, C. Prasojo, Y. Huang, and S. 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 (2013).

[15] X. Suo, Y. Zhu, and G. S. Owen. Graphical passwords: A survey. In *In Proceedings of Annual Computer Security Applications Conference*, pp. 463–472 (2005).

[16] D. S. Tan, P. Keyani, and M. Czerwinski. Spy-Resistant Keyboard: More secure password entry on public touch screen displays. In *Proceedings of the 17th Australia conference on Computer-Human Interaction: Citizens Online: Considerations for Today and the Future*, OZCHI '05, pp. 1–10 (2005).

[17] F. Tari, A. A. Ozok, and S. 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 (2006).

[18] 渡邊, 石川, 栗原, 稲見, 五十嵐. 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).

[19] 高田. 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).