同時押し認証: 暗証番号認証の改善を目指した一つの試み

国 分 佑 樹[†1]　高 田 哲 司[†1]

情報セキュリティにおいては，より安全性の高いシステムの実現も重要だが，既存のシステムの安全性を向上していくことも全体的な安全性を向上させるという観点からは重要である．これは最弱環理論と呼ばれ，特に最も脆弱なシステムの改善はシステム全体の安全性を底上げするという意味で重要である．これを個人認証手法の分野で考え，本研究では暗証番号認証の改善に取り組んだ．

そこで我々は，暗証番号の入力方法において数字を１つずつ入力することに着目し，１つずつの入力だけでなく複数の数字を同時に入力することも可能な認証手法を「同時押し認証」として考案した．この方法を用いることで，秘密情報の種類数を増加させることができ，結果として安全性を向上させることが可能になる．また提案手法に基づくプロトタイプを実装し，被験者による被験者実験を実施したところ，既存の暗証番号認証と同程度の負担で使用できる可能性があることを明らかにした．

Designing a Better PIN Authentication by Allowing to Input More Than One Numbers at Once

Yuki KOKUBUN[†1] and Tetsuji TAKADA[†1]

In an information security, inventing a novel scheme or a system with a higher security level than that of current systems is an important work, but it is also important to improve a security level of traditional systems, especially, they has a poor security level. We tried to realize a better PIN (Personal Indentification Number) authentication because this authentication has been pointed out various vulnerabilities in spite of it has widely been used in various scenes.

We change an input rule in a PIN authentication. Our proposal allows users to input more than one numbers at a time. Although this scheme increases user's memory load, it realizes a better security level. We implemented a prototype web application based on the proposed scheme and conducted a user study using it. The result of evaluation indicates that a PIN input time of the proposed scheme is almost same with a traditional PIN input scheme.

1. はじめに

本研究では暗証番号認証の改善に取り組んだ．その理由は２つある．

- 広範な場面で利用されている個人認証手法
- 既存の認証手法の中で安全性が低いとされる個人認証手法

暗証番号認証は，銀行 ATM，クレジットカードから運転免許証，携帯端末のロックなどの個人認証として幅広く使用されていることは周知の事実である．その一方で，その安全性には様々な指摘がなされており，暗証番号が 4 桁の数字であれば，適当に選んだ数字が暗証番号である確率は $1/10,000$ であることは誰もが知る事実である．また記憶保持のため，望ましくないことだとは知りつつも暗証番号をメモに書き留めたり，自身に関連の深い数字を流用することが行われているのが現実である[6]．

情報セキュリティにおいて，より安全性の高いシステムを実現していくことはもちろん重要である．しかしその一方で，既存のシステムの改良も重要である．特に最も脆弱であると考えられているシステムの改良を行うことは安全性の底上げにつながるため有益である．英語の格言に “A chain is no stronger than its weakest link.”[1] や “The strength of the Chain is in the Weakest Link.”[2] という言葉があるが，情報セキュリティ分野において安全性を向上させるという観点からも同様のことが言えよう．

この点をふまえた上で個人認証について考えると，暗証番号認証は利便性に配慮した手法であり，それゆえに安全性が高いとは言いがたい．したがって，これを改良することは認証システムの安全性を底上げすることになると考えられる．そこで本研究では，暗証番号の入力方法に工夫を行うことで，よりよい安全性を提供しうる暗証番号認証を提案する．

2. 関連研究

暗証番号認証をベースに，その改良を試みた研究事例を 2 つ紹介する．

１つめは荒川らが提案している「入力位置情報付きパスワード認証方式」である．この手法は図 1 にあるように，テンキー配列のキーボードを認証画面内に複数用意し，秘密情報として暗証番号の各数字にその数字を入力するキーボードの入力位置を追加することにより暗証番号認証の改良を試みた手法である．

†1 電気通信大学
The Univ. of Electro-Communications

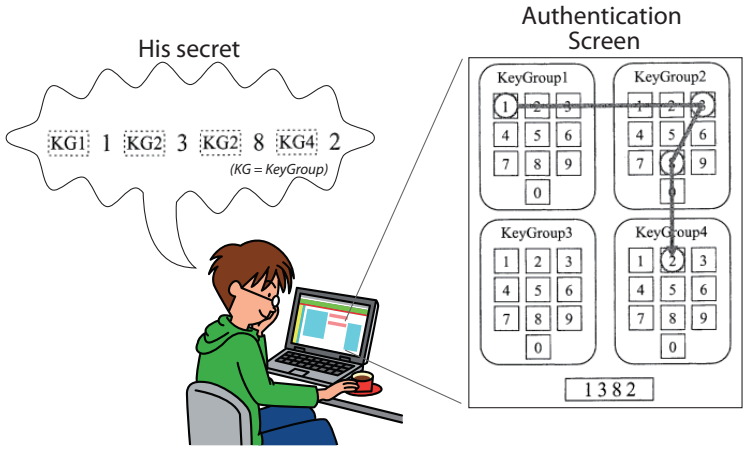

図 1 入力位置情報付きパスワード認証手法
Fig. 1 An Overview of the Individual Authentication by Input Location Information

この方法の問題点は，暗証番号の各数字に対し入力するキーボードの位置という情報が秘密情報として必要になるため記憶負担が増えることと，複数のキーボードを入力インタフェースとして用意する必要があるため，画面の物理的な大きさに制約が出てしまう点である．

もう一つは西坂らが提案している「携帯電話を対象とした PIN 認証向け日本語パスワードの提案[5]」である．この手法は暗証番号を利用者に決定させることは安全性確保の上で望ましくないことに注目し，暗証番号を携帯電話にてランダム生成させることにする．しかし，ランダム生成した暗証番号を利用者に記憶保持させるのは困難なため，それを日本語の単語に変換して利用者に提供することでユーザの記憶負担を軽減するという工夫がなされている．認証の際，利用者はパスワードとなった単語を携帯電話に入力する．すると携帯電話は，入力された単語を暗証番号に変換し，照合側に送付するという仕組みである．

この提案を利用者側から見ると，これは単語によるパスワード認証であり，暗証番号認証ではない．内部でパスワードを暗証番号に変換していても，その暗証番号に利用者がアクセスすることはないため，暗証番号であれば得られるであろう利点を利用者が享受する事ができなくなるという問題点がある．例えば暗証番号であれば数字キーだけで入力できていたが，単語パスワードであれば “ひらがな” 入力の操作ができる必要がある．評価実験の結果，記憶負担，入力試行回数，入力時間の 3 点について任意に決定した暗証番号認証とほぼ同等の結果を得ているが，被験者が学生以外になった際に違う評価結果になる可能性がある．

3. 同時押し認証: 暗証番号入力に関する新たな提案

暗証番号認証は利便性を重視した個人認証手法である．それゆえにその安全性は高くなく，いくつかの問題点が指摘されている．また秘密情報を増やすことは安全性向上につながるが，利便性，特に記憶負担や入力時間に悪影響を与えることとなる．そこで本研究における改良案の方針としては，これ以上の利便性向上を目指すのではなく，いかに利便性への悪影響を押さえつつ，秘密情報を増やして安全性を向上させるかという点を目指すこととした．そこで本研究では，複数の暗証番号の同時入力を考えた．つまり「暗証番号は，事前に決定した数字を 1 つずつ入力する」という暗証番号入力の前提条件を変更し「暗証番号の複数の数字を一度に入力することも可能」とするのである．これをその操作方法に基づき「同時押し認証」と名付けた．

同時押し認証の入力方法は至って簡単である．複数の数字キーを同時に押下することで入力する．

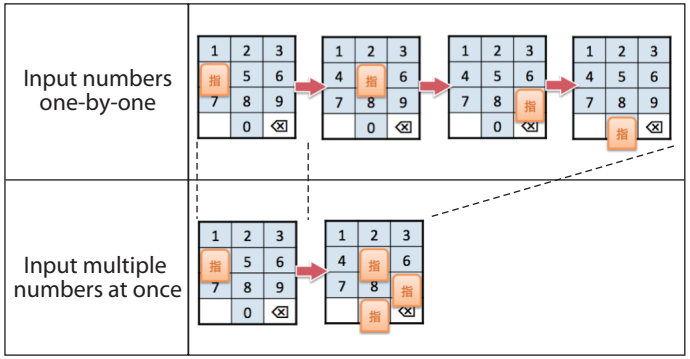

図 2 通常の暗証番号入力と同時押しを許容した暗証番号入力
Fig. 2 A Comparison of one-by-one PIN input scheme with multiple PIN input scheme

この入力方法を暗証番号認証に適用することにより，以下の 2 つの利点が得られると考える．

- 秘密情報のバリエーション数増加

- 暗証番号入力時間の短縮

秘密情報のバリエーション数が増えることについて説明する．ここでは，とある暗証番号利用者の暗証番号が「１２３４」だった場合を考える．この場合において暗証番号の数字を１つずつ入力する場合，場合の数は１つである．つまり入力方法は一意であるため，暗証番号が決定すれば秘密情報のバリエーション数は１である．これに対し，同時押し認証の場合は暗証番号が決定したとしても，その暗証番号に対して複数の入力方法が考えられるため，秘密情報のバリエーション数は増える．この場合には１つの暗証番号に対し表 1 に示す通り８通りの秘密情報が考えられる．

ここで表 1 の「具体例」列に書かれている記法について説明する．暗証番号の数値の一部または全てが丸括弧で囲まれているが，これは丸括弧内の数値を同時押しで入力することを意味する．つまり丸括弧内の数字は，一度に入力することを示している．具体例を基に説明する.「(12)34」は，1 と 2 の数字を同時押しで一度に入力し，3 と 4 はそれぞれ一つずつ入力することを示す．つまり 3 回の入力操作で 4 桁の暗証番号を入力することを意味する．一方，既存の暗証番号入力方法は同時押しがないので 1234 と記述する．また図 2 の下の入力例は「4(590)」と記述する．

表 1 より，同時押し認証は暗証番号を１つずつ入力する既存の入力方法を包含しているのは明らかである (入力操作回数 4 回に該当)．したがって既存の暗証番号認証と同等の安全性を保持していることは明らかである．同時押し認証は，暗証番号認証の入力方法を拡張したものであり，その拡張より１つずつ入力のほかに同時押し入力による秘密情報も利用可能になるため，秘密情報のバリエーションが増加することになる．

表 1 入力方法の全バリエーション (暗証番号が 1234 の場合)
Table 1 All input patterns in Douji-Oshi authentication (PIN is 1234, in this case)

入力操作回数	入力バリエーション数	具体例
4 回	1 個	1234
3 回	3 個	(12)34，1(23)4，12(34)
2 回	3 個	(123)4，1(234)，(12)(34)
1 回	1 個	(1234)

本改善手法により暗証番号の入力時間が短縮される可能性がある．表 1 にも示した通り，同時押しによる入力を許容することにより入力回数が削減されうるからである．したがって，入力に必要な時間が入力操作回数に比例するのであれば，入力時間は短縮されると考える．

3.1 同一 Key の複数個同時入力について

入力用インタフェースをテンキー配列のキーボードを仮定すると，同時押し認証では一つの問題が生じる．それは同一 Key を複数個同時に入力できない問題である．以下に２つの具体例を挙げる．

一つ目の例は，秘密情報 (1111) の場合である．この例では “1” を同時押しで 4 つ入力する必要があるが，既存のテンキー配列のキーボードでは数値 “1” の Key は一つしかないため “1” を 4 つ同時に入力することは不可能である．もう一つの例は，秘密情報 (122)3 の場合である．この例では “1” を 1 つと “2” を 2 つ，合計 3 つの数値を同時に入力する必要がある．しかし，1 つめの例と同様の理由で “1” と “2” を 1 つずつしか入力することができない．

この問題を改善する最も簡単な方法は，各数字 Key を 4 個ずつ持つ新たな入力装置を作成することである．しかし，このような入力装置は一定程度の広さを持つ表示画面またはデバイスサイズが必要となる．またそのようなものを作成したとしても同時入力という操作方法を考慮すると入力のしやすさに悪影響を及ぼすとともに，多くの入力場面でそのようなデバイスの大部分は使用されず無駄になる可能性が高いと考えた．そこで我々は「代用キー」と呼ぶ入力 Key を数字 Key の他に 3 個追加することでこの問題を改善する方法を考案した．このアイデアを基に実装した同時押し認証の認証画面を図 3 に示す．

図 3 にある通り，通常のテンキー配列のキーボードの上部に “S”, “M”, “L” とラベルのついた３つの Key が用意されている．これらが代用キーである．これらはそれぞれ Small, Medium, Large という意味の頭文字となっている．これらを使用して前述の２つの場面でどのようにして入力を行うかを説明する．

- 秘密情報 (1111) の場合
  数字の “1” を押すと同時に “S”,“M”,“L” のすべての Key を押すことにより (1111) の同時入力がなされる．つまり [(1111) → (1**SML**)] となる．
  代用キーが押された際に，同時に押されている数字 Key が 1 種類の場合は，各代用キーは押されている数字と同じ数字 Key の役割を果たす．したがって (222) の場合は，数字の “2” を押すと同時に “S”,“M” の Key を押せばよい．また上記の定義から “S”,“M” Key を押すかわりに “S”,“L” Key でも “M”,“L” Key の組み合わせでもよい．
- 秘密情報 (122)3 の場合
  数字の “1”, “2” を押すと同時に，“L” Key を押すことにより (122) の同時入力がなされる．つまり [(122) → (12**L**)] となる．

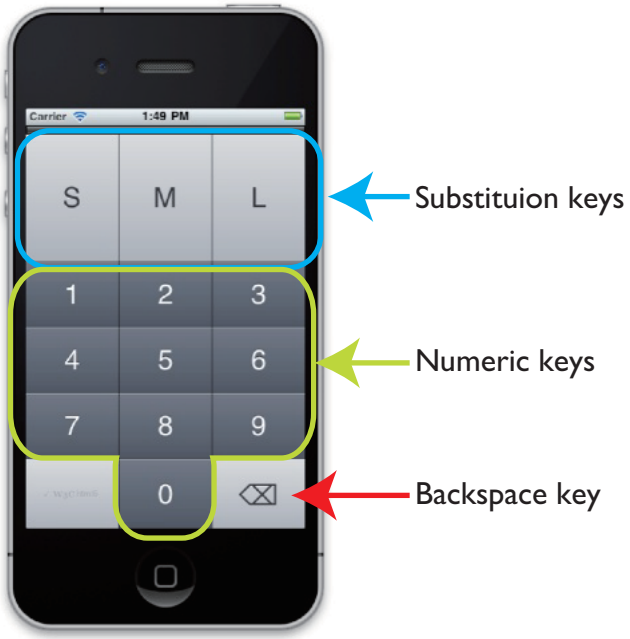

図 3 同時押し認証の秘密情報入力画面
Fig. 3 An PIN Input interface of a Douji-Oshi Authentication

“S” や “M” でなくて “L” Key である理由は，現在押されている数字 Key の中で大きい方の数値を入力するためである．“L” Key を押した時点で同時に押されている数字 Key は “1” と “2” であるが，今回複数個入力したいのは “2” の方である．現在押されている複数の数字の大小関係を考慮すると，複数個入力したい数字 Key は大きい方の数字であるため Large を意味する “L” Key を押すのである．

この代用キーのアイデアにより，4 桁の暗証番号すべてにおいて，考えうる 8 パターンの同時押しによる番号入力が可能になる．

4. 評価実験

同時押し認証について，被験者による評価実験を実施した．本章では評価実験の実験方法とその結果について述べる．

4.1 実験内容

我々は，2 種類の実験を通じて以下に述べる 3 つの項目を評価した．まずはじめに 2 種類の実験方法について述べる．

1 つめの実験は，記憶保持可能性を主たる評価対象として実施した実験である (以降，この実験を実験 A と呼ぶ)．まず最初に練習を実施し，各被験者に最低 3 回は同時押し認証の操作を実施させた．その直後，各被験者に自身で好きな同時押し認証用の秘密情報を決定させ，その直後に第一回目の同時押し認証実験を実施した．そのあと中二日をあけて秘密情報設定日から四日目と，さらに中四日あけて九日目に第二回目と第三回目の認証実験を実施した (図 4)．認証実験はそれぞれ三回までの試行を認め，三回連続で認証に失敗したらその実験では認証失敗と判定した．これは銀行 ATM での認証における条件と同等である．

図 4 実験 A におけるタイムライン
Fig. 4 An experiment timeline for a human memory evaluation

2 つめの実験は，入力時間と入力ミスを主たる評価対象とした実験である (以降，この実験を実験 B と呼ぶ)．この実験では被験者に対し，ランダムに生成した秘密情報を口頭で通知し，その場でその秘密情報を使用して同時押し認証による入力操作を実施させた．各被験者には秘密情報を 1 つ割り当てるたびに，入力操作を 5 回繰り返すよう指示した．また各被験者には 3 つの秘密情報を割り当てた．また通知した秘密情報を単なる 4 桁の暗証番号として解釈し，通常の暗証番号認証と同じ操作で同様に 5 回ずつ入力操作をするように指示して情報を収集し，比較用データを取得した．

被験者は全員が大学学部生で男性のみ．人数は実験 A は 6 名，実験 B は 7 名である．このうち 5 名が双方の実験に参加し，実験 A は 1 名が，実験 B は 2 名がそれぞれの実験だけ参加した被験者である．なお双方の実験に参加した被験者 5 名は，全員が実験 A を先に実施し，実験 A 完了後に実験 B を行った．

これら 2 つの実験を通じて，以下に挙げる 3 点の評価を目指した．

(1) 記憶保持可能性

今回の実験では，被験者に自身で秘密情報を決定してもらい，それを 9 日間の間に記憶し続けられるかどうかを評価した．各試行では 2 回までの失敗を許容し，3 回連続で失敗した場合に認証失敗と判定した．条件としては銀行 ATM と同じである．

(2) 入力時間

ユーザ名入力後，認証画面が表示されてから暗証番号が入力完了するまでの時間で評価した．計測は実装した認証システムで自動的に計測される．

(3) 入力ミス

この評価項目は，認証操作中において被験者がバックスペースを押した回数を入力ミスとしてデータを取得した．

4.2 実験環境

被験者による評価実験を行うため，本提案に基づく認証システムを Web アプリケーションとして実装した．クライアント端末は Apple 社の iPod touch(4th generation/iOS 5) を使用し，Web ブラウザである Safari を通じて認証システムを被験者に使用させた．図 3 は認証画面である．なおこの認証画面を用いて，通常の暗証番号認証の評価も実施した．これは暗証番号認証と同時押し認証を比較するためである．なお実験を実施した Network 環境は，Web サーバ計算機とクライアント端末である iPod touch の双方を無線 LAN アクセスポイントで接続したものである．

4.3 実験結果

実験結果について述べる．

4.3.1 記憶保持について

記憶保持については，実験 A で評価した．結果としては被験者 6 人が 9 日間にわたってそれぞれ 3 回の検証実験を行った．結果としては，2 回目 (4 日目) の検証実験までは被験者全員が認証に成功したが，3 回目 (9 日目) の実験では 6 人の被験者のうち 1 名が認証に失敗した．

4.3.2 入力時間について

実験 B の実験結果から平均入力時間とその標準偏差を算出したのが表 2 である．またそれらの値をグラフ化したものが図 5 になる．

また同時押し認証と暗証番号認証の結果を両側 t 検定したところ，P=0.0456 となった．したがって有意水準 5%で秘密情報の入力時間には差があると言える．

4.3.3 入力ミスについて

実験 B の結果から，入力ミスを集約したデータが以下の表 3 になる．今回の実験では，暗証番号認証 (同時押しなし) の場合には入力ミスは発生しなかった．一方，同時押し認証の場合は合計で 6 回の入力ミス (入力値の修正) が発生した．なおこれらの修正回数は，表に記載している特定の秘密情報を 5 回連続で入力する過程で発生した入力値修正の回数であり，またすべて異なる被験者により発生したものである．

表 2 入力時間に関する実験結果値
Table 2 An input time by Douji-Oshi authentication and traditional PIN authentication

	平均入力時間 (sec)	標準偏差 (msec)	最短時間 (sec)	最長時間 (sec)
同時押し認証	3.012	1342	1.393	9.496
暗証番号認証	2.742	861	1.407	5.488

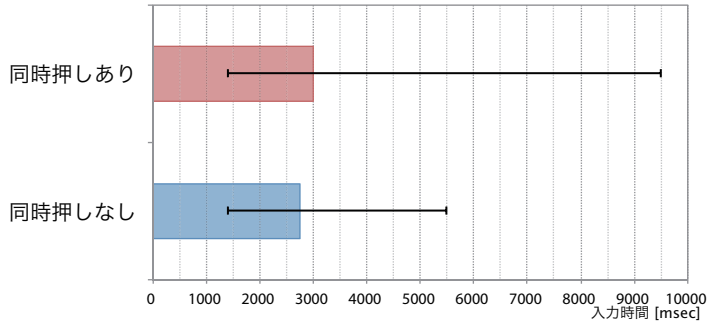

図 5 同時押し認証と暗証番号認証 (同時押しなし) の入力時間
Fig. 5 A Comparison of one-by-one PIN input scheme with multi Number inputtable PIN input scheme

表 3 同時押し認証における入力値修正回数と秘密情報の関係
Table 3 The number of re-typing times in Douji-Oshi authentication

秘密情報	修正回数
(013)9	4
(357)9	1
0(15)2	1

5. 考　　察

本章では，同時押し認証における安全性と利便性について議論する．

5.1 安全性について

ここでは同時押し認証の安全性について議論する．なおこの節ではどちらの認証手法でも暗証番号は 4 桁と仮定して議論を進める．同時押し認証が「同時押しなし」認証よりも安全性が高いことは自明である．なぜならば同時押し認証は「同時押しなし」認証を含んだ手法だからである (図 6)．本節で明らかにすべきは，この図 6 での χ に値する数値がいくつか，すなわち同時押し認証の秘密情報数はいくつになるのかを明らかにすることである．

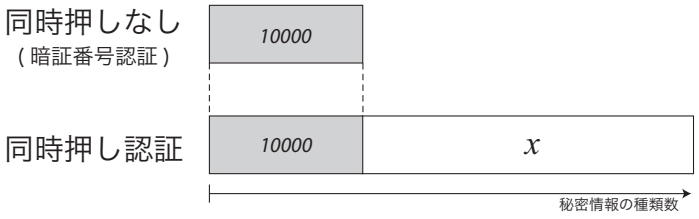

図 6　秘密情報の種類数比較
Fig. 6　A comparison of the number of secret variation

同時押し認証の秘密情報は，同時押しの部分と 1 つずつ入力している部分に分類することができる．このうち同時押しの部分は複数の数字を一度に入力するため，順列ではなく組み合わせとなる．例えば (112) と (121) と (211) は同一入力値となる．また同じ数字を繰り返し入力することも認めているので (例: (111), (7766))，単なる組み合わせではなく「重複組み合わせ」になる．n 種類の記号から重複を許して r 個のものを取り出す組み合わせ χ は以下の式で表すことができる．

$$\chi =_n H_r =_{n+r-1} C_r \tag{1}$$

よって 10 種類の数値から重複を許して 4 つを取り出す組み合わせは式 (1) より 715 通りとなる．また同時押しのパターンは表 4 に示す通り以下の 8 通りある．このうち入力パータン (1) は同時押しのない入力，すなわち既存の暗証番号入力のことを意味するので，これを除いて計算をすると χ の値は 24,600 となる． したがって同時押し認証における秘密情報の種類数は全部で 34,600 となり，暗証番号認証の約 3.5 倍となる．仮に同時押しなしの場合を秘密情報として使用禁止したとしても，約 2.5 倍の安全性を確保しうる．

表 4　同時押し認証における全入力パターン
Table 4　All Patterns of Multi PIN Input

	入力パターン		入力パターン		入力パターン		入力パターン
(1)	****	(2)	**(**)	(3)	*(**)*	(4)	*(***)
(5)	(**)**	(6)	(**)(**)	(7)	(***)*	(8)	(****)

5.2 記憶保持について

実験 A の結果から，秘密情報設定後 4 日目までは 6 名の被験者全員が記憶保持に成功し，認証できていたものの，9 日目の実験では 6 人中 1 名が認証に失敗した．この結果から「暗証番号+同時押しパターン」という同時押し認証の秘密情報は，短期記憶においてその記憶保持が困難な情報ではないと考える．また今回の検証で被験者が考え出した興味深い記憶方法として，代用キーのシンボルを使用して同時押しパターンを暗証番号と同一化して記憶するという方法がある．例えば (1677) という秘密情報は,「4 桁数字」と「同時入力パターン」の 2 種類の情報を記憶するのではなく ”167L” の 4 文字シンボルとして記憶する方法である．こう記憶するだけで，同時押しパターンは 1(67L) か (167L) のどちらかにおのずと限定される．したがって 2 種類の情報を記憶するという負担を軽減できると考えたそうである．また長期的な記憶保持の検証は今後の課題である．

5.3 入力時間について

秘密情報の入力時間についてであるが，同時押し認証の入力時間は仮説とは異なり暗証番号認証の入力時間よりも長くなるという結果になった．この原因としては，2 つの要因が考えられる．

(1)　入力操作の習熟度
(2)　代用キーの解釈
(3)　入力ミス

暗証番号認証と同時押し認証の間で習熟度の差があることは明白である．未確認ではあるが，被験者は大学生であるため，通常の暗証番号認証は銀行 ATM や携帯端末のロック等を通じて普段からその操作を行っていると推測される．一方，今回の提案手法のように複数の数字を同時に入力する方法は，ほとんどの被験者において初めての体験であると推測され

る．このことを踏まえて考えると，実験結果は好意的に見ることも可能だと考える．実験結果から平均入力時間の差は 1 秒未満であり，最短入力時間については「ほぼ同じ」である．このことから「同時押し認証は通常の暗証番号認証と同等の入力速度で暗証番号入力が可能」という仮説の実現可能性は高いと考える．また記憶している暗証番号を入力文字に置き換える際の手間として，4 桁数字の代用キーへの置換作業がある．これも入力時間を遅延させる要因の一つと考えられるが，入力操作に習熟するにつれて改善されると推測する．

なお入力ミスの発生は入力時間を長くする一因であることに疑いの余地はない．入力ミスについては次の節で詳しく述べる．

5.4 入力ミスについて

実験結果から，暗証番号認証 (同時押しなし) の場合はミスタイプによる修正がなかったのに対し，同時押し認証では 7 人の被験者がそれぞれ 15 回ずつ認証行為を実施した中で入力値の修正行為が 6 回発生した．これについて考察をする．原因としては以下の 4 点が考えられる．

(1) 既存のテンキー配列キーボード
(2) 手指の可動域
(3) タッチパッドの特性
(4) 画面領域の大きさ

もっとも大きな問題は入力用インタフェースにある．今回は入力用インタフェースについて代用キーを追加すること以外は既存のテンキー配列のキーボードを踏襲した．これが上記の (1)(2) に関する問題を引き起こしたと言える．同時押し認証では，複数の指を使用して複数の数字キーを押すことが必要となる．この操作を考えると入力ミスの発生した事例では，多かれ少なかれ無理のある同時押し入力を利用者に強いるようになっている．また指の可動域や利き手についても配慮をする必要があるだろう．そこで今後の課題としては，同時押し入力に適した入力用インタフェースを考えていく必要がある．現時点では，図 7 に示すような改善策を提案している． 図 7 の (1) は現時点でのユーザインタフェース画面である．これに対して (2), (3) は改善案である．これらはどちらも右利きの利用者を想定したものである．実際に複数の指を入力に使用すると，手の軸は右利きだと右に少し傾くことが被験者実験からわかったので，テンキー配列をベースに少しだけ右に傾けたテンキーとしたのが図中の (2) である．また人間の手指とは手を少し開いた状態で指先をすべて平面につけると円形状になることに着目し考えた配列が図中 (3) である．

また今回の実験では記録を取らなかったのだが，同時押し入力を片手で行うか両手で行うかによっても入力ミスの割合は変化すると推測する．また以下の 2 つの点も入力ミス削減に影響すると考えている．

- 物理的な画面の大きさ
- タッチパネルかキーボードか？

開発者の中で iPod touch ではなく iPad 2 を用い，画面サイズを 2 倍にして同時押し認証の入力を行ったところ，iPod touch よりも容易であるという感触を得ている．その理由は，比較的狭い空間内に複数の指を寄せ集めて入力をするよりも，物理的に広い画面にインタフェースを表示して使用することにより比較的ゆとりをもって同時押しが可能になるからである．

もう一つは，タッチパネルに由来する入力ミスである．同時押し認証の入力では秘密情報によっては指が図 8 のよう立ってしまうことがある．この状況は，タッチパネルによる認識ミスを発生しやすいということがわかった．利用者はキーを押しているつもりでも，システム側では認識されないという事態が発生する傾向にあった．これを改善する方法としては，前述の物理的に大きな画面を利用するのも一つ方法法である．キー間の間隔が広くなることで指を立たせて入力する必要性を減らすことが可能になる．また別の改善方法として，タッチパネルではなく通常の機械式キーボードを利用する方法がある．この入力方法であれば，この問題に関しては根本的な解決になると考える．

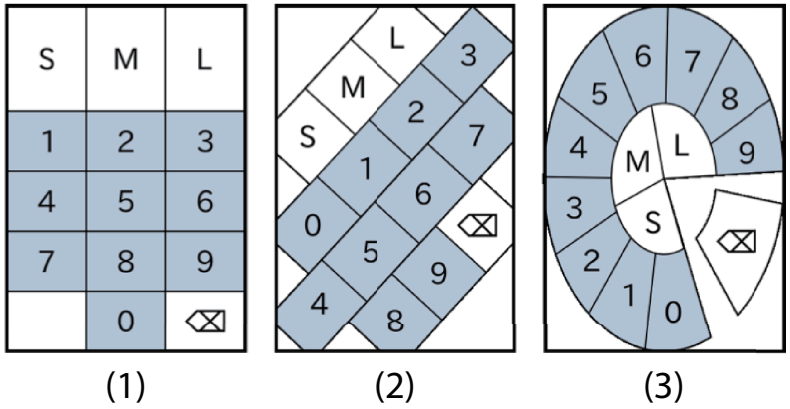

図 7 同時押し認証における入力インタフェースの改善案
Fig. 7 An Another User Interface Design of Douji-oshi Input Authentication

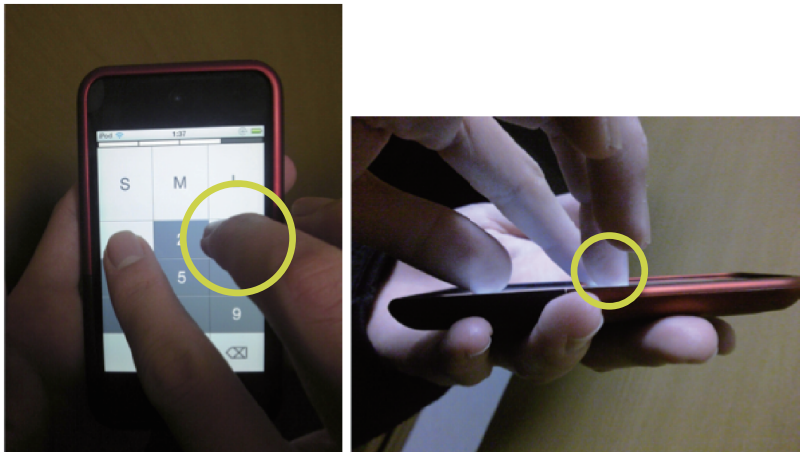

図 8 入力ミスの事例 (2): タッチインタフェースに起因する入力ミス
Fig. 8 An input miss exmaple 2

またさらに別の改善方法としては，通常の Caps キーのような状態保持機能付きキーを導入することも考えられる．入力方法としては次のようになる．キーボードの状態保持機能を有効にした上で，同時押しする対象のキーを一つつつ押した状態にする．そのあとで状態保持機能を無効にし，同時押しする最後のキーを押して離す．この方法により，「同時押しなし」の入力と同様の方法でキーを一つずつ押しながら同時押し入力が可能になる．ただし，この方法だと入力ミスが低減可能になったとしても入力速度の改善は望めなくなると推測する．

6. おわりに

本論文では，様々な認証手法がある中で様々な場面で採用されていながらもその安全性には問題があると指摘されている認証手法である暗証番号認証に着目し，その改善を試みた．そこで我々は「暗証番号を 1 つずつ入力する」という入力方法上の制約をとりはらい，暗証番号の一部または全てを一度に入力することも可能にした新たな認証手法「同時押し認証」を提案した．またこの入力手法を通常のテンキー配列のキーボードに適用すると入力困難な場合があることを指摘し，その問題を改善する方法として代用キーという手法を提案した．これらの提案を基にプロトタイプシステムを Web アプリケーションとして実装し，記憶保持，入力時間，入力ミスの 3 つの評価項目を設けて被験者による評価実験を実施した．実験結果から入力ミスが多く発生する傾向があるものの記憶保持と入力時間については既存の暗証番号認証と同等レベルの負担で操作可能である可能性を示した．また安全性については，既存の暗証番号認証よりも安全性が高いことを明確にした．今後の課題としては，ユーザインタフェースの改善と長期記憶に関する検証を行いたいと考えている．

参 考 文 献

1) 'Idiom: A chain is no stronger than its weakest link', UsingEnglish.com (オンライン), <http://www.usingenglish.com/reference/idioms/a+chain+is+no+stronger+than+its+weakest+link.html>, (参照 2012-05-14).
2) "The Strength of the Chain is in the Weakest Link', English for Students (オンライン), <http://www.english-for-students.com/The-Strength-Of-The-Chain-Is-In-The-Weakest-Link.html>, (参照 2012-05-14).
3) Adams, A. and Sasse, M.A., Users are not the enemy, Comm. ACM, Vol.42, No.12, pp.40-46, (1999).
4) 荒川 豊，竹森 敬祐，笹瀬 巌: 入力位置情報を付加したパスワード認証方式，情報処理学会 研究報告 Vol.2003-CSEC-21, No.45, pp.35-40, (2003).
5) 西坂 健太郎，寺田 真敏，土井 範久: 携帯電話を対象とした PIN 認証向け日本語パスワードの提案，情報処理学会 研究報告 Vol.2010-CSEC-48, No.22, pp.1-8, (2010).
6) Joseph Bonneau, Sören Preibusch and Ross Anderson: A birthday present every eleven wallets? The security of customer-chosen banking PINs, FC'12:The 16th Int'l Conf. on Financial Cryptography, (2012).