Vol.2010-DPS-142 No.22
Vol.2010-CSEC-48 No.22
2010/3/4

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

西坂健太郎† 寺田真敏† 土居範久†

携帯電話の高機能化やネットワークサービスの増加にともない携帯電話から個人認証をおこなう機会が多くなってきている．しかし，PIN 認証には自分のパーソナルデータを PIN に設定する利用者が多く，なりすまし被害にあう危険性が大きいという問題がある．

本稿では，携帯電話から利用する PIN 認証システムに対して，携帯電話の文字入力方式を用いてランダムな PIN を日本語パスワードに変換することで利用者の負担が少なく安全性の高いパスワードを利用者に提供するシステムを提案する．提案方式の有効性を確認するために日本語パスワードに関する調査をおこなった．つぎに，提案方式を実装した認証システムと評価を通して提案方式の有効性を示す．

Proposal of a Password authentication in Japanese combined with PIN for a Mobile phone

Kentaro Nishizaka† Masato Terada† Norihisa Doi†

As a mobile phone functions highly and network service increases, opportunities to perform the personal certification from a mobile phone increase. However, there are issues of spoofing attacks in PIN authentication because many users register one's personal data as a password.

By this report, we suggest a system providing a safer password with a few burdens of users by converting random PIN to Japanese password with text input method for a mobile phone, for PIN authentication system with a mobile phone. We investigated a Japanese password to confirm the effectiveness of the suggestion system. In addition, We show the effectiveness of the suggestion method through evaluation of the authentication system that implemented a suggestion method.

1. はじめに

携帯電話の高機能化やネットワークサービスの増加にともない，オンラインショッピングなどの電子商取引やサービスを携帯電話などからも利用する機会が多くなってきている．また，利用者が個人認証をおこなって各種サービスや取引を利用することも多くなる一方，他人の ID やパスワードを不正に利用して個人情報の盗用や悪事を働くなりすまし被害なども増えてきている．

個人認証には，クレジットカードなどの所有物を用いて認証をおこなう方式や指紋などの生体情報を用いた生体認証方式など様々な認証方式が存在するが，社会的に最も認知され普及している認証方式は利用者の ID とパスワードを用いた認証方式である．このため，利用者がどのようなパスワードを設定するかということは非常に重要な問題となる．安全なパスワードを実現するためにはランダムなパスワードが望ましい．しかし，ランダムなパスワードは利用者にとって記憶しづらく，利用者の多くは記憶しやすい自分のパーソナルデータをパスワードとして設定してしまうことになる．結果として，自分のパーソナルデータを由来とするパスワードは他者にとって推測が容易であるため，なりすまし被害にあう危険性が大きくなる．

利用者の確認に 4 桁の数字を暗証番号（Personal Identification Number：PIN）として使用する金融機関のキャッシュカードでは，なりすまし被害にあった全体の約 4 割が生年月日に由来する PIN を設定していたという報告がある[1]．キャッシュカードと同様にパスワード入力の煩雑性を低減させるために 4 桁程度の PIN を用いて利用者を特定することの多い携帯電話の個人認証においても，安全性の低いパスワードを設定してしまうことによるなりすましの危険性は大きいと考えられる．

本稿では，携帯電話から利用する PIN 認証システムに対して，携帯電話の文字入力方式を用いてランダムな PIN を日本語によるパスワード（以降，日本語パスワード）に変換することで利用者の負担が少なく安全性の高いパスワードを利用者に提供するシステムを提案する．次に，提案方式の有効性を確認するために日本語パスワードに関する調査と，提案方式を実装した認証システムの評価を通して提案方式の有効性を示す．

† 中央大学大学院 理工学研究科
Graduate School of Science Engineering, Chuo University.

Vol.2010-DPS-142 No.22
Vol.2010-CSEC-48 No.22
2010/3/4

2. 関連研究

2.1 携帯電話の文字入力方式[1]と認知度

携帯電話の文字入力方式といえば，かな文字入力方式が一般的であるが他にも様々な文字入力方式が提案されて採用されている．本節では，代表的な携帯電話の文字入力方式とその認知度について調査した結果を述べる．

2.1.1 携帯電話の文字入力方式

(1) かな文字入力方式

かな文字入力方式は，1 つのキーに複数の文字が割当てられており，アの段なら 1 回，イの段というようにボタンを押すごとに文字が変わり，必要な回数だけボタンを押すことで語句に置換する．この文字入力方式は，他の文字入力方式と比較してキーの打鍵数が多く利用者の負担が大きいという問題がある．かな文字入力方式における数字から日本語への文字変換について例を挙げると（2222|11|4|11 : けいたい）となる．かな文字入力方式の変換文字コード表を表 1 に示す．

表 1　かな文字入力方式の変換文字コード表

かな文字入力方式		数字キーの入力回数				
		1	2	3	4	5
入力する数字キー	1	あ	い	う	え	お
	2	か	き	く	け	こ
	3	さ	し	す	せ	そ
	4	た	ち	つ	て	と
	5	な	に	ぬ	ね	の
	6	は	ひ	ふ	へ	ほ
	7	ま	み	む	め	も
	8	や	ゆ	よ		
	9	ら	り	る	れ	ろ
	0	わ	を	ん		

(2) ポケベル文字入力方式

ポケベル入力方式は，ポケベル文字コード表に基づいて語句に変換する入力方式である．かな文字入力と比較すると文字の打鍵数は低減しているが，ポケベル文字コード表を記憶する必要があるため利用者の負担が大きい．ポケベル入力方式における数字から日本語への文字変換について例を挙げると（24|12|41|12：けいたい）となる．ポケベル入力方式の変換文字コード表を表 2 に示す．

表 2　ポケベル入力方式の変換文字コード表

ポケベル入力方式		2回目に入力する数字キー				
		1	2	3	4	5
1回目に入力する数字キー	1	あ	い	う	え	お
	2	か	き	く	け	こ
	3	さ	し	す	せ	そ
	4	た	ち	つ	て	と
	5	な	に	ぬ	ね	の
	6	は	ひ	ふ	へ	ほ
	7	ま	み	む	め	も
	8	や	ゆ	よ		
	9	ら	り	る	れ	ろ
	0	わ	を	ん		

(3) T9 文字入力方式[3]

米 Tegic Communications 社が開発した単語予測型の文字入力方式で，携帯電話のように限られたキーの中で効率よく文字入力を行なうために考案された方法である．文字を入力する際には，子音のみを入力すると予測単語が候補として表示され，その中から入力したい単語を選択する．T9 入力方式では 1 文字入力する際にキーを押す回数が 1 回で済むため，素早く入力を行なうことができる．T9 入力方式と同様の入力方式に米 Motorola 社が開発した iTAP などがある．T9 入力方式における数字から日本語への文字変換について例を挙げると（2|1|4|1：かいたい，けいたい，こうたい，など）となる．T9 入力文字コード表を表 3 に示す．

表 3　T9 入力方式の変換文字コード表

T9入力方式		数字キーの入力回数
		1
入力する数字キー	1	あ行
	2	か行
	3	さ行
	4	た行
	5	な行
	6	は行
	7	ま行
	8	や行
	9	ら行
	0	わ行

Vol.2010-DPS-142 No.22
Vol.2010-CSEC-48 No.22
2010/3/4

2.1 なりすまし被害にあった暗証番号

近年，金融機関のキャッシュカードは，なりすましなどによる不正利用が問題になっている. 特に, キャッシュカードが盗難, 偽造されることで第 3 者が金融機関や ATM などから不正な現金の引き出しや振り込みがおこなわれていたり，ネットバンキングなどでもなりすましによる不正引き出し被害が発生したりしている. 平成 17 年から平成 20 年の間に偽造キャッシュカードなどを用いた被害は 29,267 件に上る[4]. さらに，平成 17 年の金融庁による実態調査[1]によれば, なりすまし被害にあった利用者の PIN の全体の約 4 割，不明な場合を除くと約 6 割が生年月日などの利用者のパーソナルデータから類推可能な PIN を使用していることを指摘している.

2.2 解決したい課題

金融庁の調査が示すように，利用者は数字をパスワードとして設定する際に自分のパーソナルデータを由来とする PIN を設定してしまうことが多く，パーソナルデータを由来とする PIN はなりすましに対して脆弱であることがわかる．通常 4 桁の数字からなる暗証番号には 1 万通りのバリエーションがある．しかし，暗証番号に生年月日を使用しているとすると 1 月 1 日から 12 月 31 日までの 366 通りと，かなり限定されてしまいパスワードとしての安全性が低くなってしまう．これらの問題はキャッシュカードと同様に PIN 認証を用いて個人認証をおこなっていることの多い携帯電話においても同じ危険性を持っていると考えられる.
そこで，本稿では，利用者が使い慣れたパスワード認証方式を用いて安全性が高く利用者の負担が少ない認証システムを提案する.

3. PIN 認証向け日本語パスワードシステム

3.1 課題解決のアプローチ

PIN 認証の課題について 2.3 節で述べたように，この問題は利用者が複雑な PIN を記憶しづらいため，記憶しやすいパーソナルデータを設定することで起きる.
提案方式では，①システムがランダムな PIN を選択し，②PIN を変換し，日本語パスワードとして利用者に提供する．③入力された日本語パスワードを PIN に変換することで，問題解決を図る(図 1).

① システムがランダムな PIN を選択する

利用者が自分でパスワードを設定するのではなくシステムがランダムな PIN を利用者に指定することでなりすまし被害などにあう危険性を低減させる.

② PIN を変換し，日本語パスワードとして利用者に提供する

ランダムな PIN は利用者にとって記憶しづらく，利用者への負担が大きいが，日本語パスワードに変換することで記憶負荷を軽減する.

③ 入力された日本語パスワードを PIN に変換する

任意の文字入力方式によって入力された日本語パスワードを T9 入力方式によって日本語パスワードを入力されたときの PIN に変換することで，①の PIN に復元する.

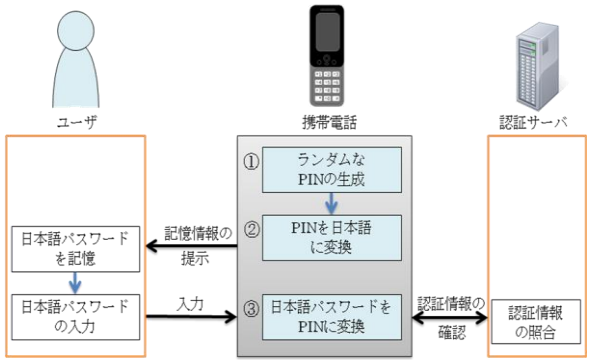


図 1 提案方式の流れ

3.2 提案方式

本節では提案方式の特徴である「②PIN から日本語パスワードへの変換」と「③入力された日本語パスワードから PIN への変換」について述べる.

3.2.1 PIN から日本語パスワードへの変換

システムが生成したランダムな PIN の日本語パスワードへの変換には，PIN を数字列辞書に対して完全一致と前方一致の 2 通りの方法で検索して日本語に変換する.

(1) 数字列辞書

数字列辞書とは，百科辞書や ICOT 形態素辞書などの辞書データを用いて，辞書に記載されている日本語を T9 入力方式によって入力するときの数字列を名詞や形容詞，動詞などの品詞ごとにまとめたものである．このとき，T9 入力方式を用いて数字列辞書を作成するのは, T9 入力方式は他の文字入力方式と比較して PIN から日本語パスワードへの変換が容易であるためである．数字列辞書の一部を表 4 に示す.

Vol.2010-DPS-142 No.22
Vol.2010-CSEC-48 No.22
2010/3/4

表 4　数字列辞書（名詞）

T9数字列長	T9数字列	日本語	ふり仮名	品詞コード
4	6250	箱庭	ハコニワ	0010
4	4749	血祭	チマツリ	0010
4	4419	鉄色	テツイロ	0010
4	1239	アクセル	アクセル	0010

(2)　数字列辞書への検索方法

PIN の日本語パスワードへの変換は，数字列辞書から完全一致と前方一致検索をおこなうことで PIN に対応する日本語を見つける．完全一致検索とは，数字列辞書に数字列 X を検索するとき，数字列 X と T9 数字列の全桁が等しくなる日本語を見つけることである．また，PIN の日本語パスワードへの変換効率を向上するために前方一致検索を使用する．前方一致検索は，数字列辞書に n 桁の数字列 X を検索するとき，数字列 X と T9 数字列の前方 n 桁が等しい日本語を検索することである．完全一致と前方一致を図 2 に示す．

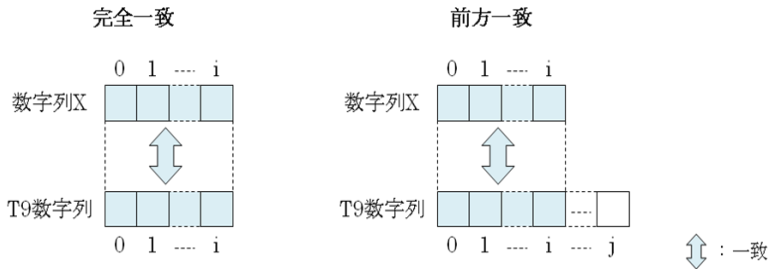


図 2　完全一致と前方一致

(3)　数字列辞書を用いた日本語への変換

PIN から日本語パスワードへの変換は，(a)変換される日本語が 1 単語である場合，(b)変換される日本語が修飾語と被修飾語で構成されている場合，(c)変換される日本語が関連性の無い複数の単語で構成されている場合，にわけておこなう．

(a)　変換される日本語が 1 単語である場合

PIN を日本語パスワードに変換するために，全ての品詞の数字列辞書に PIN を完全一致と前方一致による検索をおこない，PIN に対応する日本語がないか調べていく．数字列辞書を検索した結果，PIN に対応する日本語が見つかった場合，利用者に日本語パスワードとして提示する．全ての数字列辞書を検索しても見つからなかった場合は手順(b)に進む．

(b)　変換される日本語が修飾語と被修飾語で構成されている場合

本手順では，PIN を 2 つの前半数字列と後半数字列に分割して，前半数字列を完全一致，後半数字列を前方一致で改めて検索する．このとき，前半数字列は連体詞，形容詞，形容動詞などの体言を修飾できる連体修飾語，または，副詞，形容詞，形容動詞などの用言を修飾できる連用修飾語になることができる品詞の数字列辞書から検索する．後半数字列は，連体修飾語となる品詞の数字列辞書から前半数字列に対応する日本語が見つかった場合，名詞の数字列辞書から後半数字列を検索する．連用修飾語となる品詞の数字列辞書から前半数字列に対応する数字列が見つかった場合，動詞の数字列辞書から後半数字列を検索する．PIN の分割は数字列の後方から 1 桁ずつずらして 2 つに分割していく．そして，分割した PIN の前半と後半の数字列にそれぞれ対応する日本語が見つかった場合，利用者に PIN に対応する日本語をパスワードとして提示する．PIN を修飾語と被修飾語の 2 つにわけても見つからなかった場合は手順(c)に進む．

(c)　変換される日本語が関連性の無い複数の単語で構成されている場合

本手順では，PIN を半分の長さで分割して，分割した PIN をそれぞれ全ての品詞の数字列辞書へ完全一致検索をおこなう．分割した PIN に対応する日本語が見つからなかった場合，分割した PIN をさらに半分の長さで分割して，対応する日本語が見つかるまで繰り返していく．そして，分割した PIN にそれぞれ対応する日本語を日本語パスワードとして利用者に提示する．

3.2.2 入力された日本語パスワードから PIN への変換

利用者が任意の文字入力方式で入力した日本語パスワードからシステムが生成したランダムな PIN へと復元する．このとき，日本語パスワードは前方一致検索によって PIN から変換された可能性があるため，指定された桁数を超えて入力された日本語パスワードは削除する．PIN への変換は，入力された日本語パスワードを表 3 で述べた T9 文字入力方式の変換文字コード表に従っておこなう．そして，復元された PIN を認証情報として認証サーバへ利用者の確認をおこなう．

Vol.2010-DPS-142 No.22
Vol.2010-CSEC-48 No.22
2010/3/4

4. 評価

本章では，提案方式で採用している日本語パスワードを用いた認証について，日本語パスワードが認証においてどのように選択されるのかという視点から評価をおこなう．つぎに，提案方式を実装した認証システムを用いて使い勝手の視点から評価をおこなう．

4.1 日本語パスワードの選択傾向

4.1.1 調査概要

(1) 調査目的

数字をパスワードとする PIN 認証では，利用者がパーソナルデータをパスワードとして設定したとき，なりすまし被害などにあう危険性が大きいことを 2.2 節で述べた．同様に日本語をパスワードとして使用した場合でも，パーソナルデータをパスワードとしたとき，ランダムな日本語パスワードと比較して危険性は大きいと考えられる．そこで，パスワードに日本語を使用できるとしたとき，利用者が設定するパスワードの調査を通して提案方式の有効性を示す．

(2) 調査対象

調査は，本学学生および教員，事務員，筆者が参加した研究会の学生および教員など合計 55 名に協力を依頼した．

(3) 調査方法

調査方法は，調査用紙を直接配布，またはメールを用いて調査用紙を配布して後日回収をおこなった．調査内容は，被験者に日本語のパスワードを 3 個考えてもらい，それぞれに対して，パスワードの由来と構成，文字数を回答する形式とした．

4.1.2 調査結果と考察

① 調査結果

日本語をパスワードとして使用した場合において被験者がどのようなパスワードを設定するか調査を行った結果，数字をパスワードとして使用したときと同様に自分のパーソナルデータを由来とする日本語パスワードを設定する被験者が全体の 35%であった．また，そのパスワードの構成についてみるとパスワードに 1 単語を設定した被験者は全体の 56%を占めた．パスワードの文字数は平均 6.81 文字で 3 文字から 10 文字程度のパスワードを設定する被験者が多かった．日本語の由来と構成を図 3 に，日本語パスワードの文字列長を図 4 に示す．

図 3 日本語パスワードの由来と構成

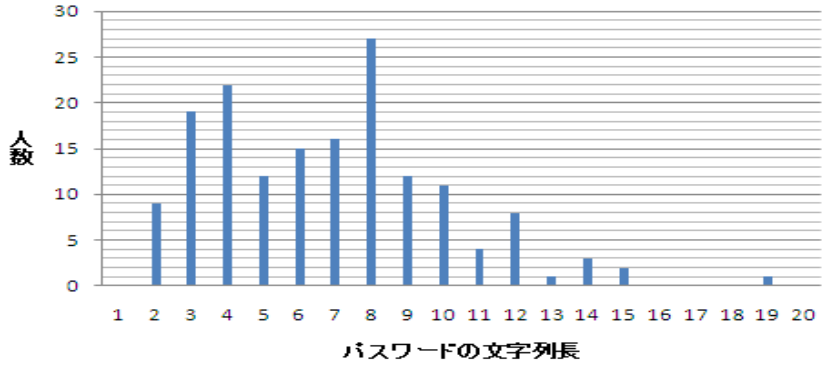


図 4 日本語パスワードの文字数

② 考察

調査結果より，利用者が任意にパスワードを設定した場合，日本語パスワードも数字をパスワードとして用いたときと同様に自分のパーソナルデータをパスワードに設定する利用者が多いと考えられるため，なりすましなどにあう危険性は大きい．また，利用者が自分で日本語パスワードを設定した場合，1 単語をパスワードとして利用する利用者も多いと考えられるため辞書攻撃に対して脆弱である．これらの調査結果から，任意に日本語パスワードを設定した場合，安全性の低いパスワードを設定する利用者は多いと考えられるため，利用者に依存しないランダムな日本語パスワードを生成する本提案方式は有効であると考えられる．

Vol.2010-DPS-142 No.22
Vol.2010-CSEC-48 No.22
2010/3/4

4.2 提案方式の記憶負荷と操作性

4.2.1 実験概要

(1) 実験の目的

提案方式は，ランダムな PIN から日本語パスワードに変換して利用者にパスワードとして記憶してもらうため，既存の認証システムと比較して利用者の負担が大きいと考えられる．そこで，提案方式を実装し，記憶負荷と操作性を代表的な既存の認証システムと比較することで，提案方式の利用者への負担を評価する．

(2) 提案方式の実装概要

提案方式の実装には携帯電話での利用を踏まえ Willcom Advanced/W-ZERO3［es］[5]を使用した．提案方式を実装したシステム(以下，実装システム)では，PIN を日本語パスワードへ変換する機能，入力された日本語パスワードを PIN に変換する機能，および，入力された日本語パスワードを用いて利用者の確認をおこなう認証サーバの機能を携帯電話上に実装した．実装システムにおける日本語パスワードの入力は，Advanced/W-ZERO3［es］がサポートする文字入力方式から，かな文字入力方式によっておこなう．実装システムのパスワード登録画面を図 5 に示す．

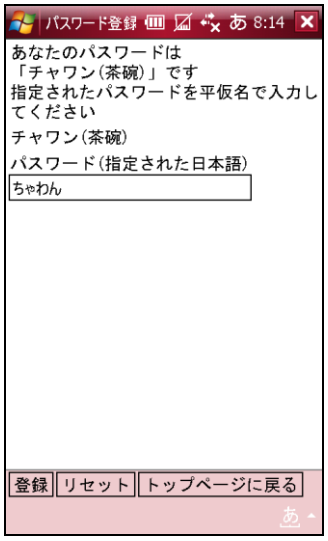


図 5　実装システムのパスワード登録画面

提案方式は，数字列辞書のデータ数によって PIN から日本語パスワードへの変換できる確率が変動する．今回，実装したシステムでは，著作権フリーである PDD(PUBLIC DOMAIN DATA)百科辞書[6]と morphdic＋から作られた辞書パッケージ[7]を用いて 203,837 語からなる数字列辞書を作成した．実装したシステムにおいて，ランダムな PIN から 1 単語の日本語に変換できる確率を図 6 に示す．

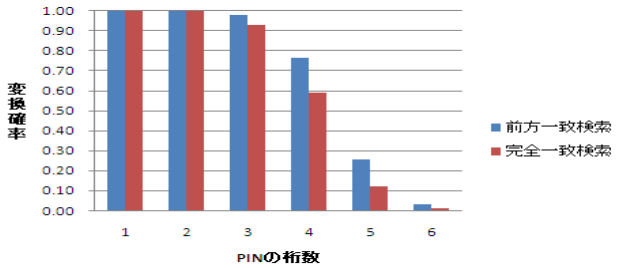


図 6　1 単語の日本語への変換確率

(3) 実験対象

学生を対象に合計 17 名を被験者として実験をおこなった．

(4) 評価項目

提案方式を実装したシステムの記憶負荷と操作性を，既存の認証システムと比較するための評価項目は，次の通りである．

- 認証成功率:3 回の再入力の機会がある中で被験者が認証に成功した割合
- 平均試行回数:3 回の再入力の機会の内，何回目に認証に成功したかの平均
- 平均入力時間:パスワード入力画面が表示されてから，パスワードを入力して認証ボタンを押すまでの平均時間

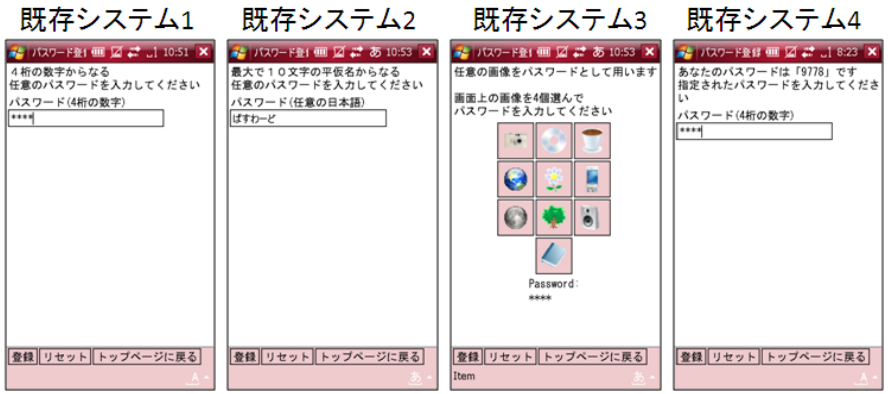
(5) 実験方法

本実験では，実装システムと既存の 4 種類の認証システムを用いて，被験者自身が実際に認証操作する方法をとった．被験者は実験に関して十分に理解した上で，パスワードの登録日，1 週間後，3 週間後の合計 3 回でパスワードを入力し，パスワードを忘れていないを確認する．このとき，認証に成功するまでに 3 回以上失敗してしまった被験者は，該当する認証システムに関する実験は終了とした．

提案方式を評価するために比較対象として用意した既存の認証システムは 4 つである．また，実験のために用意した提案方式と既存の認証システムのパスワード登録画面を示す．(図 7)

Vol.2010-DPS-142 No.22
Vol.2010-CSEC-48 No.22
2010/3/4

- 既存システム 1:任意の 4 桁の数字をパスワードとする認証システム
- 既存システム 2:任意の 10 文字以内の日本語をパスワードとする認証システム
- 既存システム 3:任意に選択した 4 つ画像と順番をパスワードとする認証システム
- 既存システム 4:被験者に 4 桁の乱数をパスワードとして指定する認証システム



- 図 7　既存システムのパスワード登録画面

4.2.2 実験結果

4.2.1 節で述べた評価項目に対して認証成功率の実験結果を図 8 に，平均試行回数の実験結果を図 9 に，平均入力時間の実験結果を図 10 に示す．

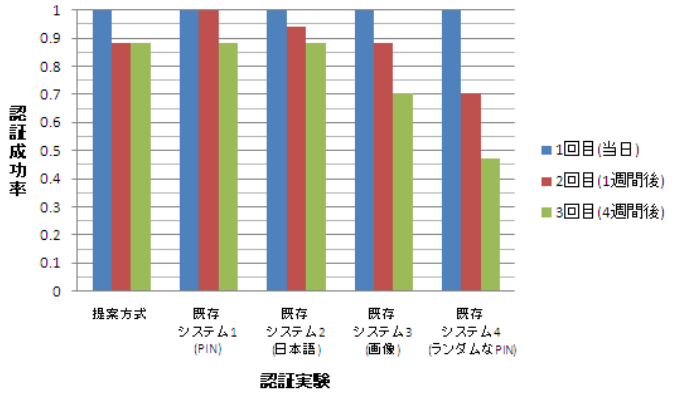


図 8　認証成功率

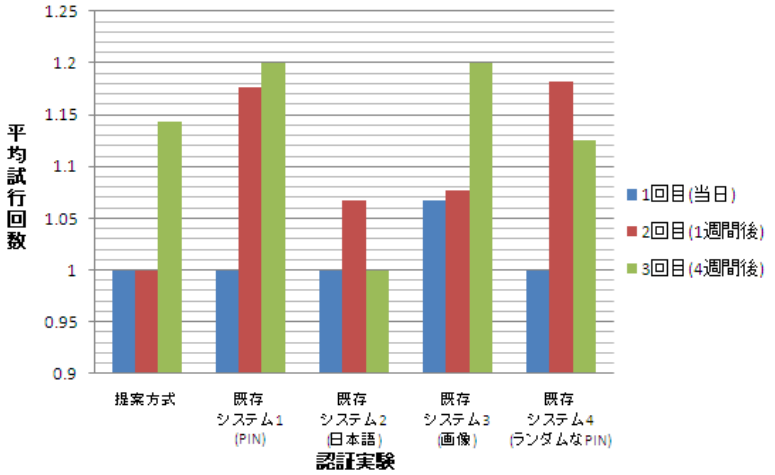


図 9　平均試行回数

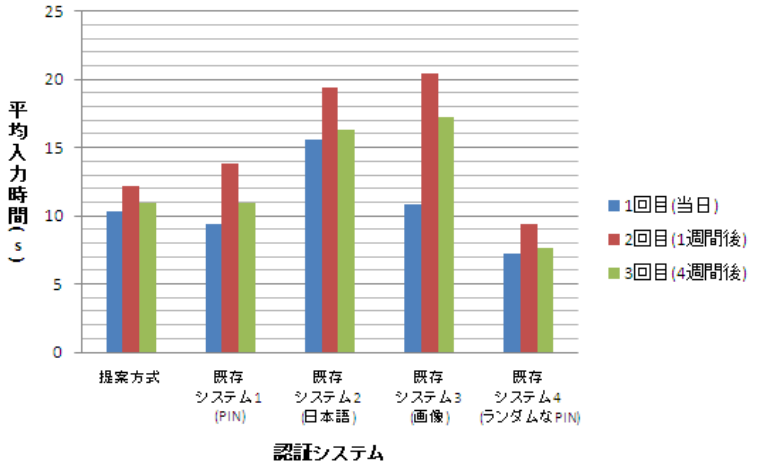


図 10　平均入力時間

Vol.2010-DPS-142 No.22
Vol.2010-CSEC-48 No.22
2010/3/4

図 8 から実装システムと同様に被験者に対してランダムなパスワードを指定する認証システムでも，乱数よりランダムな日本語の方が利用者にとってパスワードを記憶しやすいという結果が得られた．また，実装システムを使用した被験者の記憶負荷は社会的に最も認知されている任意の PIN を用いる既存システム 1 や任意の日本語をパスワードして用いる既存システム 2 とほぼ同等の結果が得られた．

図 9 と図 10 からは，実装システムは既存システム 2 と比較して平均入力時間では優れた結果が得られたが，平均入力回数をみると任意の日本語をパスワードとして利用できる既存システム 2 の方が入力ミスは少ないことがわかった．実装システムを既存システム 1 と比較してみると平均試行回数に関しては実装システムの方が入力ミスは少なく，平均入力時間に関しては同等の結果が得られた．

4.2.3 考察

提案方式は利用者の記憶負荷や操作性において，任意の日本語パスワードを使用する認証方式を除く既存の認証システムと同等の結果を得ることができた．

今回の実験では被験者が入力するパスワードの長さや伏字の使用を統一していなかった．そのため，利用者の操作性に関しては単純に比較することは難しい．また，任意の日本語をパスワードとする認証システムは，4.1 節の考察で述べたようにパーソナルデータをパスワードに設定する利用者が多いためなりすまし被害にあう危険性が大きいといえる．このことから，ランダムな PIN から日本語に変換する提案方式は有効であると考えられる．

また，本実験では，提案方式の PIN から日本語パスワードへの変換に対して T9 入力方式を用いて作成した数字列辞書のみを使用した．日本語への変換は，同じ PIN を使用しても何の文字入力方式によって作られた数字列辞書を使用するかで変換結果の日本語が変わってくる．このことを踏まえると，複数の文字入力方式を使用できる利用者に対しては，他の文字入力方式を用いて作成した数字列辞書を使用することで PIN から変換される日本語の数が増え，日本語への変換確率を向上できると考えられる．

5. おわりに

本稿では，携帯電話における PIN 認証システムに対して，ランダムな PIN を日本語パスワードに変換することで安全性が高く，利用者の負担が少ない認証システムを提案した．まずは，金融機関のキャッシュカードを例に挙げて PIN 認証システムにおいてパーソナルデータをパスワードに設定することの危険性について述べた．つぎに，提案方式を評価する上で，利用者の日本語パスワードの選択傾向と提案方式を実装したシステムの使い勝手の 2 つの視点から提案方式を評価した．評価を通して，提案方式は既存の認証システムに比べ，ほぼ同等の記憶負荷と操作性でランダムな PIN による認証を実現できることを示した．

提案方式には，つぎのような改善すべき課題がある．まず，PIN から日本語パスワードに変換精度を向上させ，より利用者にとって記憶しやすい日本語パスワードへの変換を可能にする．つぎに，複数の認証システムにおいて提案方式を使用した場合においても，利用者の記憶負荷が大きくならないような日本語パスワードに変換することである．

謝辞　本研究を推進するにあたり，有益な助言と協力を頂いた KDDI 研究所の山田明氏，三宅優氏に深く感謝いたします．また，調査に協力して頂いた中央大学，東海大学ならびに，ISS スクエアの関係者各位に深く感謝致します．

参考文献

1)　偽造キャッシュカード問題に関する実態調査について
http://www.fsa.go.jp/news/newsj/17/ginkou/f-20051014-5.html
2)　携帯電話の文字入力における利用形態とその問題点
http://www.sonoda-u.ac.jp/dic/kenkyu/2003/27.pdf
3)　ENTER｜1 文字 1 押し T9
http://www.jt9.jp/
4)　偽造キャッシュカード等による被害発生等の状況について
http://www.fsa.go.jp/news/20/ginkou/20090630-1.html#bessi
5)　WILLCOM｜THE SMART PHONE　Advanced/W-ZERO3［es］
http://www.willcom-inc.com/ja/lineup/ws/011sh/index.html
6)　the private PUBLIC DOMAIN DATA LIBRARY
http://pddlib.v.wol.ne.jp/
7)　Wise FreeWnn/Wnn4.2/Egg
http://www.remus.dti.ne.jp/~endo-h/wnn/