2003－CSEC－21 (6)
2003／5／15

入力位置情報を付加したパスワード認証方式

荒川 豊[†] 竹森敬祐[†,††] 笹瀬 巌[†]

あらまし 現在，銀行やクレジットカード等に用いられている 4 桁の暗証番号によるユーザ認証の脅威についてまとめ，これまで提案されてきた対策手法について長所，短所の考察を交えて紹介する．これらの対策手法の中から，利便性とセキュリティ強度の兼ね合いを考慮した上で，入力位置情報を付加したパスワード認証方式を実装し，その操作性について評価する．その結果，いくつか問題点が明らかになったため，その改善策を提案し，実装と評価を行い，利便性とセキュリティ強度が向上されることを示す．

Individual Authentication by Input Location Information

Yutaka Arakawa ,[†] Keisuke Takemori [†,††] and Iwao Sasase[†]

Abstract We summarize dangers on authentication system used at a bank or credit card, and introduce several measures against them. We implement and evaluate one of these measures, authentication system using input location information, in consideration of the balance between security intensity and usability. Consequently, some problems became clear. In this paper, we propose the authentication system that can improve these problem. By using our authentication system, it is possible to improve security intensity without spoiling usability.

1. はじめに

インターネットの急速な拡大を背景に，オンラインバンキング等の各種サービスをインターネット介して利用する機会が増加している．インターネットは世界中の利用者に開かれたネットワークであるため，利便性と効率性が高い反面，セキュリティ上のさまざまな脅威が存在する．インターネットを介してユーザ個別の情報を提供するサービスにおいて，それらの脅威から逃れるためには利用者を認証する必要がある．現在，インターネット上では，パスワードや乱数表を組み合わせた認証方式が主流であり，パスワードとして英数字の大文字小文字を組合せた文字列を用いる方法あるいは 4 桁の数字のパスワード（以後，暗証番号と呼ぶ）などが用いられている．

一般的にセキュリティと利便性は相反するため，セキュリティを考える場合，利便性との兼ね合いを考慮しなければならない．英数字混合の長い文字列パスワードはセキュリティ強度が高い反面覚えにくく，ユーザの利便性が低下する．そのため，銀行の ATM のように利便性が重要視される分野においては，セキュリティ強度が低いにもかかわらず，記憶しやすい暗証番号による認証が根強く用いられているのが現状である．この利便性を重視する傾向は，インターネットにおいても同様であり，多くの銀行がオンラインバンキングにおいても 4 桁の暗証番号を用いている．また，銀行に限らず，航空会社のマイレージなどインターネット上でユーザ個別のサービスを行う場合，暗証番号を用いている場合も少なくない．暗証番号は，10000 通りの組合せしかなく，誕生日といった個人情報が用いられている可能性も高いため，幾通りかの試行によりパスワードが破られる可能性が高い．また，オンライン認証においては，プログラム等を用いることで 10000 通りの試行は容易であるため，セキュリティ強度はきわめて低いと考えられる．そこで，試行回数を制限するシステム的なガードが設けられているが，このガードを逆手にとり，すべてのアカウントをロックするような DoS 攻撃（Denial of Service attack）なども考えられる．このようなさまざまな脅威に対して，暗証番号の利便性を損なうことなくセキュリティ強度を向上させることは重要な研究課題となっている [1)]．

そこで本研究では，オンラインサービスにおけるユーザ認証の脅威についてまとめ，これまで提案されてきた対策手法について長所，短所の考察を交えて紹介する．これらの対策手法の中から，利便性とセキュリティ強度の兼ね合いを考慮した上で，入力位置情報を付加したパスワード認証方式を実装し，その操作性について評価す

† 慶應義塾大学
〒 223-8522 横浜市港北区日吉 3-14-1
Keio University, 3-14-1 hiyoshi, kouhoku-ku, yokohama-shi, 223-8522
†† (株)KDDI 研究所
〒 356-8502 上福岡市大原 2-1-15
KDDI R&D Labs. Inc., 2-1-15 Ohara Kamifukuoka-shi, 356-8502

る．その結果，いくつか問題点が明らかになったため，その改善策を提案し，実装と評価を行い，操作面での利便性とセキュリティ強度が向上されることを示す．以下，2 章で 4 桁の暗証番号の危険性及びそれに対する攻撃について述べ，3 章でさまざまなセキュリティ向上のための手法について述べる．そして 4 章において，入力位置情報を付加したパスワード認証方式を実装し，有効性ならびに問題点について述べる．5 章で従来の問題点を改善した認証方式を提案し，実装および評価を行い，最後に 6 章でまとめる．

2. 4 桁暗証番号の危険性

4 桁の暗証番号は覚えやすく，多くの機関で共通という高い利便性の反面,「0000」から「9999」までの 10000 通りの番号を総当りで入力するブルートフォースアタックにより暗証番号を特定することが可能である．また，暗証番号として誕生日を用いている人が多いため [2]，月を 2 桁，日を 2 桁で表した「0101」から「1231」までの 366 通りの番号を試せば，さらに効率よく攻撃することが可能な場合もある．従来，店舗型のサービスの場合，暗証番号を入力する以前にカードが必要であり，何らかの形でカードを入手した場合でも暗証番号を数回誤入力するとカードが利用できなくなるため，上述のような脅威は考えられていなかった．ただし，店舗型特有の脅威として，ショルダーハッキングの危険性がある．これに対し，インターネット上で暗証番号による認証を行う場合，脅威はより深刻なものとなる．インターネットからのアクセスの場合，カードのような物理媒体がないため暗証番号だけでなくユーザ ID を偽り他人に成り済ますことが可能である．さらに，コンピュータを利用することでスクリプト等を用いて，一瞬にして膨大な試行を行うことが可能である．そのため，インターネット経由でも同一のユーザ ID に対してパスワードの誤入力の回数によりそのユーザ ID に対するサービスを停止するシステム的なガードが設けられている．しかし，パスワードを探索する際に，ユーザ ID を固定せず，さまざまなユーザ ID とパスワードをランダムに組合せて数多くの探索を行った場合,「多くの利用者がたまたまパスワードを入力ミスした」という状態と区別がしにくく，システム的なガードが機能しない可能性があることが指摘されている [1]．これは，ユーザ ID を自由に入力可能であるインターネット特有の脅威である．また，このシステム的なガードを逆手に取り，ある銀行のすべての口座を凍結させるような DoS 攻撃の脅威も考えられる．また，インターネット経由であれば世界中のどの端末からもアクセスすることが可能であるため，上述のような脅威に対して従来の店舗型のように監視，抑制をすることができない．接続元を偽ることも容易であるため，犯人を特定することは非常に困難であると考えられる．

	ア	イ	ウ	エ
1	25	36	76	45
2	11	13	20	52
3	30	80	46	23
4	49	72	55	37

図 1 銀行で用いられる乱数表の例

3. さまざまな対策手法

本節では，上述のさまざまな脅威の中で，特にブルートフォースアタック，ショルダーハッキングに対する対策についてそれぞれ述べる．

3.1 ブルートフォースアタック対策

同一ユーザ ID に対する単位時間あたりのパスワードの試行回数を制限するようなシステム的なガードが一般的な対策である．この方式は，店舗型でカードを用いる場合に有効であるが，オンラインバンキングのように物理媒体によるユーザ ID の特定手段がなく，ユーザ ID の方を変更できるシステムにおいては，パスワードを固定しユーザ ID を変化させるといった攻撃も可能であり，あまり有効とは言えない．そのため，そのようなシステムでは，パスワードの桁数を増加させるあるいは英数字を織り交ぜることにより組合せの数を増加させる方式が取られている．しかし，そうした場合，4 桁である利便性が損なわれるいう問題点がある．そこで，暗証番号を用いたまま組合せを増加させる方式として以下のような方式が提案されている．

3.1.1 乱数表を用いる方式

オンラインバンキングにおける暗証番号のセキュリティを向上させるための手段として，認証手段を二重化し，ログイン用のパスワードに加えて，特に重要な操作の際に，図 1 に示すような「乱数表☆によるチャンレンジ・レスポンス方式」を用いる方式が導入されている [3)4)]．この方式は，あらかじめ利用者ごとにランダムな数値を記載した乱数表を作成して利用者に配布しておき，資金振替指図の入力など，特にセキュリティの要求が高い局面で，その表の中の位置情報をランダムに質問（この質問を「チャレンジ」という）し，それに該当する数値（この数値を「レスポンス」という）を応答させる手法であ

☆ ここで言う「乱数表」は，金融機関により「お客様カード」「確認番号表」等と呼称しているものであるが，通称としてよく利用されている表現であるため，以下では「乱数表」と呼ぶ．

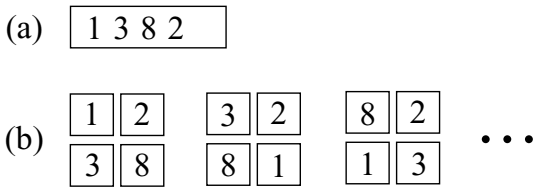

図 2 入力位置情報を付加した認証方式

る．この方式は，取引の都度，異なる暗証番号を利用することになるため，盗聴や偶然の一致により認証をパスしたとしても，次の取引では同一のチャレンジが出されない限り認証をパスできないという効果がある．また，利用者側に特別なハードウェアやソフトウエアが必要ないため，普及しやすいというメリットがある．しかしながら，乱数表を導入することによって，逆にリスクを高めている部分があることにも注意が必要である [5]．例えば，乱数表は利用者ごとに事前に作成し郵送するものであるが，作成，搬送のプロセスで秘密が漏洩するリスクがある．また，ある程度長い期間，同一の乱数表が利用され続けることが想定されており，秘密情報が漏洩した場合のリスクも，利用を継続する期間に応じて高くなる．また，乱数表が利用者の手に渡った後も，暗証番号のように情報を記憶しておくことができないため，かえって財布等に保管することによる盗難・紛失のリスクが高くなる．

3.1.2 入力位置情報を付加したパスワード認証方式

乱数表を用いずに 4 桁のままセキュリティ強度を向上可能な方式として，複数の入力欄に対してパスワードを分割して入力する方式が提案されている（公開特許報：特開 2000-339084）．入力位置に意味を持たせることにより，ユーザが普段用いているパスワードの組合せを増加させ，セキュリティ強度を向上させることが可能となる．パスワード「1382」を「1」「3」「8」「2」という 4 つの数字の組合せと考えると今までは「入力順序」のみを考慮した方式と定義できる．一方，入力位置情報を用いた方式は，これに「入力位置」という情報を付加することにより,「入力順序」と「入力位置」の組み合わせ方式と定義できる． 図 2 のように入力欄を 4 つとし，暗証番号を 1 入力欄に対して 1 桁ずつ入力する場合，暗証番号の組合せを 4!(24) 倍にすることが可能である．また，1 マスに複数桁の入力を可能とすると 4^4(256) 倍強度が増す．この方式は，従来の暗証番号をそのまま利用できるだけでなく，乱数表のように携帯する必要がなく，盗難や紛失に対して強いと言う利点がある．しかしながら，入力欄を分割して複数にしたために，入力の際にマウスあるいは十字キーを用いて入力欄を移動しなければならないため，操作性が低下するという問題点もあり実用化に至っていないと考えられる．われわれは本手法が将来的に広く利用されると考え，次節において実装および評価を行う．

3.1.3 冗長なユーザ ID の利用

ユーザ ID の桁数を増加し，冗長性を高めることにより，ランダムなユーザ ID が有効なユーザ ID である確率を低下させ，ブルートフォースアタックに対する耐性を高めることが可能である．例えば，1 万人のユーザがいる銀行において，5 桁の暗証番号（00000 番〜99999 番）のユーザ ID を順番に付与した場合，ランダムに発生した 5 桁の番号が 1 割の確率でユーザ ID として利用できる．しかし，ユーザ ID を 10 桁の乱数とした場合，ランダムに発生させた 10 桁の番号がたまたまユーザ ID として実際に利用されている確率は 10^{-6} 以下であるため，試行錯誤が極めて非効率となる．

またこの方式は，アカウントロックを行う DoS 攻撃に対しても有効であると考えられる．DoS 攻撃では，ユーザ ID が利用可能かどうかにかかわらずすべてのユーザ ID に対して攻撃を試みるため，ユーザ ID の桁数を増加させることで，短時間にすべてのアカウントをロックすることが困難になる．

3.2 ショルダーハッキング対策

店舗型のサービス特有の脅威として，入力キーを盗み見されパスワードが漏洩するショルダーハッキングの危険性があり．それを防ぐ方法としてさまざまな方式が提案されている．

3.2.1 物理的に入力キー隠す方法

入力キーをケースで覆い，手を中に入れて入力する方式が提案されている（公開特許報：特開 2001-147763）．この方式は，入力キーをケースで覆うため他人から盗み見されない反面，自分が何を入力しているのかわかりずらいという欠点がある．コンビニの ATM やデビットカードを利用する際の入力キーには，ある程度フードのようなものがついているものが見受けられる．

3.2.2 入力キーの配置を変更する方式

0〜9 の数字で構成されるテンキーのキーの配置を毎回変更することにより，横から覗かれた場合でもどの数字を入力しているのか推測不可能とする方式である．また，各キーだけでなく，テンキーそのものの画面内での表示位置を変化させる方式も提案されている（公開特許報：特開平 05-334334）．さらに，0〜9 の数字を表す入力キーを各数字に対して複数設けることにより，入力位置の変化を大きくする方式も提案されている（公開特許報：特開平 09-297875）．これらの方式は，ショルダーハッキング対策として有効であると考えれられるがキーを探さなければならないため操作性が低下する．それを改善する方式として，各数字に色を付加し探しやすくする方式が提案されている（公開特許報：特開 2002-287871）．

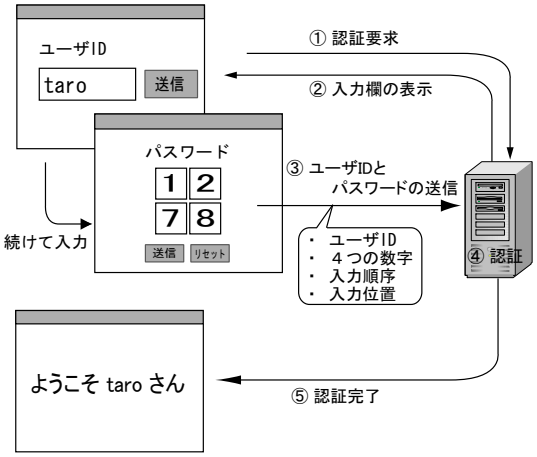

図 3 実装したシステムの構成

図 4 パスワード入力画面

4. 入力位置情報を付加したパスワード認証方式の実装および評価

3 節で述べたさまざまな方式の中で，複数の入力欄に対してパスワードを分割して入力する方式は，暗証番号の利便性を損なうことなくセキュリティを強度を高めることができるため今後の利用が期待される．しかしながら，この方式は実装されていないため，本研究では，この方式を実装し，その有効性及び実用性について検討する．

4.1 実　　装

図 3 に，実装したシステムの構成を示す．サーバマシンとして Pentium III 833Mhz, メモリ 512MB の PC を用いた．OS は Windows2000 とし，ASP（Active Server Pages）☆を用いて入力画面の表示及び認証部を実装した．クライアントからサーバに対して認証要求に対してサーバ側はユーザ ID 入力欄を表示する．クライアントの入力に引き続き，サーバはパスワード入力欄を表示する．このとき，ユーザ ID が間違っている場合でもパスワード入力欄を表示する．これは、侵入者にユーザ ID とパスワードのどちらが誤っているかを探索させない為である．その後，入力された情報（ユーザ ID，4 つの数字，入力順序，入力位置）を元にサーバ側で認証を行い，すべてが一致した場合にのみアクセスを許可する．

4.2 評　　価

図 4 に，実装したシステムにおけるパスワード入力画面を示す．本研究では，暗証番号に対し，図に示すような配置で 4 つの入力欄を設け，それぞれの入力欄に 1 桁ずつ入力するものとした．この方式は，さらに入力欄を複数にし，3 × 3, 4 × 4, 5 × 5 のマス目を用いることで組合せが増加し，セキュリティ強度を向上できることが示されている．しかしながら，マス目が増加することで入力位置を記憶することが困難になるとともに，マウスあるいは十字キーを用いたカーソルの移動が増加するため，非実用的と考え本研究では 2 × 2 のマス目を用いた．また，1 入力欄に複数桁を入力可能とすることも提案されているが，それによりさらに操作性が低下すると考えられる．従来暗証番号を入力するための打鍵回数は 4 回であるが，例えば 2 × 2 の入力欄において 1 入力欄に 1 桁入力する場合，最低 3 回，最大 6 回のカーソル移動が必要となり，平均打鍵回数は 2 倍以上となる．また，5 × 5 の入力欄の場合，最低 3 回，最大では 24 回のカーソル移動が必要となり，平均打鍵回数は極めて増大する．

このように，この方式を実用化する上では，入力位置の移動による操作性の低下を改善することが必要であると考える．そこで，本研究では，打鍵回数を増加させることなく入力位置情報を付加可能なパスワード方式を提案する．

5. 操作性とパスワード強度を考慮した認証方式の実装および評価

従来方式は入力欄を複数に分割していたが，ここでは入力欄を 1 つとし，入力キーを複数にする手法を提案する．これにより，従来の打鍵回数が増加し，操作性が低下するという問題点を改善することが可能となる．打鍵回数とは，入力キーを押した回数を表し，マウスを用いる場合はクリック数を表すものとする．また，ユーザはあらかじめ同様の入力インターフェースを用いてパスワードの登録を行うものとする．

☆ ASP とは，Microsoft 社の WWW サーバである Internet Information Server が備える，サーバー上でスクリプトを実行する機能およびそれに付随する技術の総称．http://www.microsoft.com/japan/msdn/vstudio/techinfo/articles/clients/default.asp

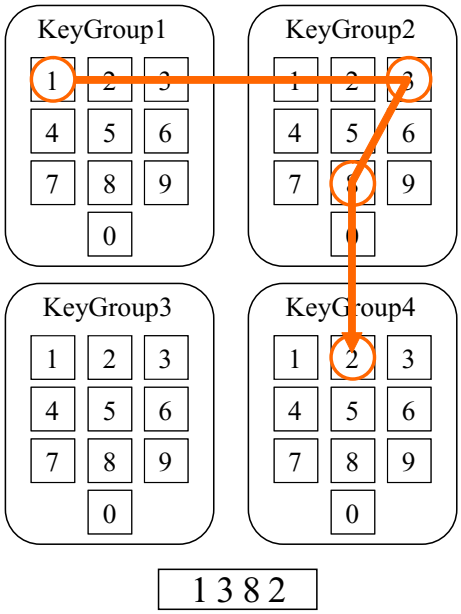

図 5 提案システムの概念図

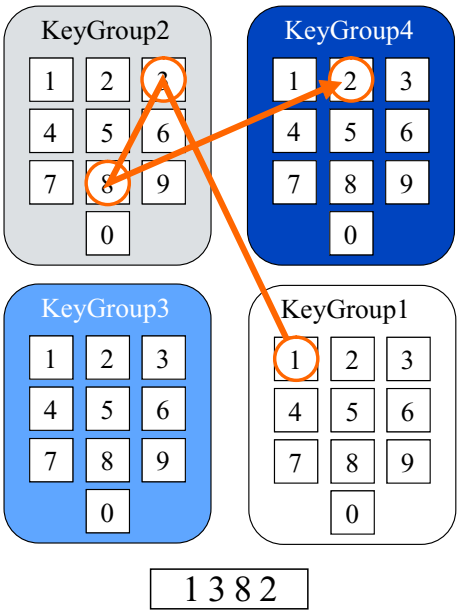

図 8 KG の配置換え

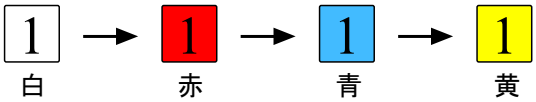

図 6 打鍵回数による色の変化

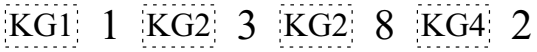

図 7 提案方式における入力情報

5.1 提案および実装

提案方式では，画面上に表示された複数のテンキーを用いてパスワードの入力を行う．各テンキーを，KeyGroup i（以降，KG i と表記）と定義し，ある数字に対してどの KG に所属しているかという情報を付加する．これにより 1 つの数字が KG 数分あるため，1 つの暗証番号に対して打鍵回数を増加させることなく 4^{KG} 通りの入力を行うことが可能となる．提案方式は，入力したい数字をクリックするだけであるためカーソルの移動が不必要であるため，従来方式と比較して操作性が向上すると考えられる．また，1 つの KG 内の同一の数字を複数回選択することを可能とするために，1 回押す毎に入力キーの色が変化する方式を提案する．図 6 にある KG 内の入力キー「1」を連続して押した場合の，打鍵回数による色の変化の様子について示す．1 回押すごとに色が赤，青，黄と変化し，同じキーを複数回入力していることを視覚的に認識することが可能となる．図 5 に，KG 数が 4，パスワードが「1382」の場合について示す．図 5 の場合,「1382」の各桁をそれぞれ KG1，KG2，KG2，KG4 の順で入力している．図 5 における入力欄は 1 つであり，そこには「1382」と表示されるが，実際は各桁に対してそれぞれ KG の情報が入るので，図 7 に示す情報がサーバに送信される．サーバ側では，入力された数字に加えて，それぞれの数字がどの KG に所属しているかという入力位置情報を確認し，双方ともが事前に登録したものと一致した場合にアクセスを許可する．提案方式は，入力位置がパスワードとなるため，ショルダーハッキングによるパスワード漏洩の危険性がある．そこで，KG そのものの配置をランダムにする方式を提案する．図 8 に示すような配置にした場合，先ほどと同様の入力順序（図 7）で入力したとしても，手の動作が異なるためショルダーハッキングされにくくなると考えられる．また，KG を表すものとして，色（濃淡あるいは 4 色）を用いることにより，KG の配置が変更された場合においても入力順序を思い出すことが容易になると考えられる．図 8 では，KG1，KG2，KG3，KG4 の順で，KG の色が濃くなり，ユーザは色を見て視覚的に KG を判断することが可能である．

図 9 に，図 5 で提案した手法を実装したときのパスワード入力画面を示す．このとき，実装のシステム構成は，図 3 と同じである．

5.2 評　　価

本節では，操作性を検証する指標として，打鍵回数について従来方式と提案方式を比較し評価する．また，パスワードの組合せ数，拡張性についても比較する．

5.2.1 操作性について

表 1 に，2×2 の入力欄を用い暗証番号を入力した場合について，従来方式および提案方式のパスワード入力完了までの平均打鍵回数を示す．前提条件とし，従来方

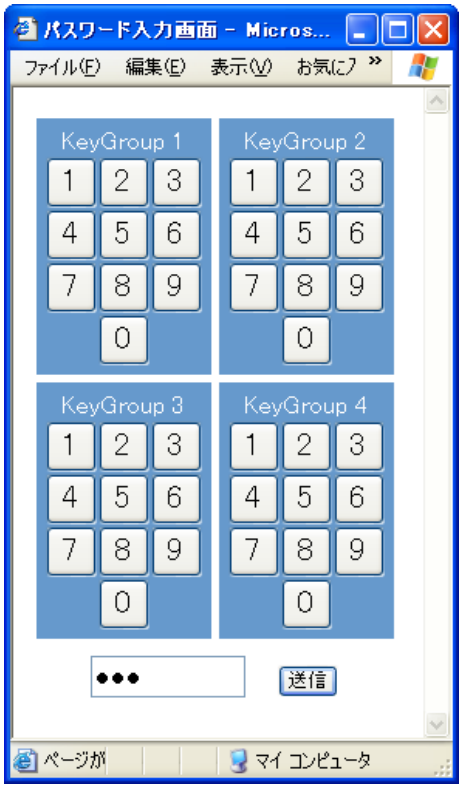

図 9 実装したシステムにおけるパスワード入力画面

表 1 平均打鍵回数の比較

	提案方式	従来方式
1 桁／1 入力欄	4	9
複数桁／1 入力欄	4	8

式においてカーソルの初期位置は左上のマスとする．打鍵回数とは，従来方式においてはカーソルを 1 マス移動するために十字キーを押す動作及び数字の入力のための動作をそれぞれ 1 回と数える．提案方式においては，数字を選択するために画面をクリックする回数を表す．提案方式は，カーソルの移動を必要としないため，暗証番号を入力するために 4 回のクリックで良いことがわかる．これは，ATM で現在用いられている暗証番号を入力する場合と同じであり，打鍵回数が増加しないことがわかる．一方，従来方式では，4 桁の数字の入力に加えて，所望の入力欄までカーソルを移動しなければならないため，平均打鍵回数が 2 倍以上となることがわかる．

5.2.2 パスワードの強度について

パスワードの強度を図る指標として，入力位置の組合せ数を考える．従来方式において，入力欄を 2×2 とし 1 つの入力欄に 1 桁入力した場合，ある暗証番号に対して 4!通りの入力位置の組合せを作ることが可能である．また，1 つの入力欄に複数桁入力した場合，4^4 通りとなる．一方，提案方式において KG 数を 4 とした場合，4^4 通りとなり，パスワードの強度は同等であることがわかる．

5.2.3 拡張性について

従来方式は，3×3，4×4 のように拡張するほど，パスワードの入力位置の組合せが増加しセキュリティ強度が向上するが，その分カーソルの移動が困難となり，パスワードの入力に必要な平均打鍵回数が指数関数的に増加する．そのため，実用面での拡張性が低いと考えられる．一方，提案方式は画面表示の際に面積が必要であるものの，現行の ATM のようなタッチパネルであれば KG 数を拡張することが可能であると考えられる．それにより，パスワードの入力位置の組合せを増加させることが可能であるとともに，その場合も打鍵回数が増加せず操作性が劣化しないため拡張性に優れていると言える．

6. ま と め

本研究では，頻繁に用いられている暗証番号に対して，利便性を損なうことなくセキュリティ強度を向上させる方式として，入力位置情報を付加したパスワード認証方式を実装した．実装を行い評価した結果，操作面での問題点が判明したため，新たに操作性とパスワード強度を考慮したパスワード認証方式を提案した．提案方式では，パスワードの入力用のテンキー（KeyGroup）を複数用意し，どの KeyGroup に所属するかという情報を付加することで，パスワードの組合せの数を増加させることができた．さらにこの方式は，従来方式と比較して，操作性，拡張性に優れていることを確認した．

7. 今後の予定

今回，実装したパスワード認証を実際に使用してもらい，位置情報を記憶することの負担の度合い，色を用いる有効性などについて評価実験を行う予定である．

参 考 文 献

1) 高木 浩光, “安全な Web アプリ開発 31 箇条の鉄則”, http://www.jnsa.org/seminar_20021217.html, Internet Week 2002.
2) 中川 靖司，小松 尚久，“バイオメトリクスによる個人認証技術の現状と課題 －金融サービスへの適用の可能性－”，日本銀行金融研究所，Discussion Paper 1999-J-43.
3) ご契約者カードについて, http://direct.btm.co.jp/qa/secure.htm, 東京三菱銀行.
4) “主なネットバンキングのセキュリティ対策と保険”, 日経パソコン, pp.24-25, 2003 年 3 月 31 日号
5) 松本 勉, 岩下 直行, “インターネットを利用した金融サービスの安全性について”, 日本銀行金融研究所，Discussion Paper 2002-J-12.