2004年度 卒業論文

ゲーム性を持った認証方式の提案と実装

提出日： 2005 年 2 月 2 日

指導： 村岡洋一教授

早稲田大学 理工学部 情報学科
学籍番号： 1G01P027-1
春日　友樹

目 次

図 目 次

表 目 次

第1章　序論

本論文では、人間の特性の「手続記憶」を利用して、Web 上で最も一般的に使われている従来のパスワード認証より覚えやすく、それでいて認証の耐性が落ちない画像認証方式の手法について述べる。

1.1　はじめに

近年インターネットの普及に伴い、インターネット上で買い物や銀行の預金確認など、個人の特定ができればさまざまなサービスを受けることができる。個人を特定するために Web 上の情報サービスサイトや通信販売サイトの多くで行われている現在のユーザ認証は、パスワードによる認証が主流になっている。認証とはある行為を行う者が正当な権利を持つ者であるということを確認する技術のことである。確かにパスワード認証は実装が簡単で、汎用性が高い。しかし、これはユーザにとって使いやすいものとは必ずしも言えない。パスワードに自分の誕生日や家族の名前などに関連するものを使う人がいる。しかし、ユーザが簡単に記憶できるような文字列は他人にも簡単に見破られる可能性がある。だからといって、他人には推測しにくい文字列は、同時にユーザ本人にとっても覚えにくいため、紙に書き留めたり、ファイルとして保存したり、複数のサービスのパスワードを統一しているなどパスワード認証が本来もっている安全性を損なうようなことをしているのが現状である。また、パスワードの定期的な変更を促してるが、ユーザが覚えなおすのが面倒などの理由でなかなか行われていない。既存の認証技術は主に、１．知識や記憶を使った認証（アカウント名＋パスワード)、２．所有物を使った認証（ＩＣカード、鍵)、３．生体情報を使った認証（指紋、静脈、虹彩）の３種類に分けることができる。

まず所有物による認証は、紛失したら耐性がなくなってしまい他人になりすまされてしまう。さらに本人も認証ができないので、他人に使われて、自分は使えないという状況になる。銀行のＡＴＭなどは、(所有物による認証＋知識や記憶を使った認証）の二つを組み合わせて使っている。どちらが欠けても認証成功しないので、所有物による認証の欠点を補っているといえる。しかし、知識や記憶を使った認証の方を自分の誕生日や、覚えやすい数字＝推測されやすい数字にしていることがあると簡単に他人になりすまされてしまう。

生体情報を使った認証は、最も個人を特定しやすく、なりすましが難しい認証

技術である。しかし、この技術にも問題点いくつかあ。１．認証する際に専用の機器の導入が必要であり非常にコストがかかる。２．指紋や静脈の場合はいろいろな人が触るので衛生的な心理的抵抗が少なからず生じる。３．生体情報なので個人情報として最も慎重に扱わなければいけないので、名簿流出とは次元が違い、生体情報の流出は絶対に許されない。４.本人拒否率をゼロにできない。

知識や記憶を使った認証は、いわば脳内の情報（アカウント名＋パスワード）を使うので当分は最も安全だと思われる。しかし、覚えにくいなどの欠点もある。この欠点を解消し、ユーザの負担を軽くできれば認証技術として非常に有効な方法であると言える。

現在、知識と記憶を使った認証方式においてパスワードを画像にする、画像認証というものが多く研究されてきている。これは、パスワードがランダムな文字列だと覚えにくいので、人間は物事を正確に記憶することが不得意であり正確に覚えるより、全体をあいまいに覚えるほうが得意であるという考えから画像を使っている。これに人間が本来持っている特性を活用してユーザの負担を減らすためにエピソード記憶を加えて忘れにくくする方法も研究されている。ただ、既存の画像認証は Brute-force 攻撃と Observation 攻撃に弱い。特に画像を選ぶところを後ろから見られたら簡単にパスワードを盗まれてしまう。

この問題点を解決するために、本研究ではパスワードに画像だけでなく、パスワードをユーザ独自のアルゴリズムで変換することにより Observation 攻撃に対抗する。また、Bruete-force 攻撃にもパスワード認証以上の耐性を持たせた。提案手法は、1 回の認証作業をキャラクタ画像 200 体で行い合計 2 回認証作業を行う。下にそのユーザ登録の手順を示した。

1. ユーザ名を決める。

2. キャラクタ 200 体が表示されるので、その中から好きなキャラクタを 1 体選ぶ（以降、正解キャラクタと呼ぶ）。

3. パスワード変換番号（5 桁）を決める。パスワード変換番号の変換の仕方は図 1.1 に示すようになっている。

4. 2. で表示された 200 体のキャラクタがランダムに配置されているので、その中から正解キャラクタを探し、場所を覚えて正解キャラクタをクリックする。

5. ここからログイン作業に入る。まず 4. と同じ 200 体のキャラクタがランダムに配置された画像が表示される、違うのは正解キャラクタが表示されていない部分。ユーザ本人なら正解キャラはわかるはずなので、表示しない。その中から正解キャラクタを探す。見つけたら「切替ボタン」をクリックする。

6. 200 体のキャラクタがすべて 10 桁の英数字に変化するので、3. で決めたパスワード変換番号で正解キャラクタが変化した英数字を並び変えて、パスワードを入力する。

7. 2.〜6. の作業をもう一度行い、計 2 回行うことで登録完了となる。

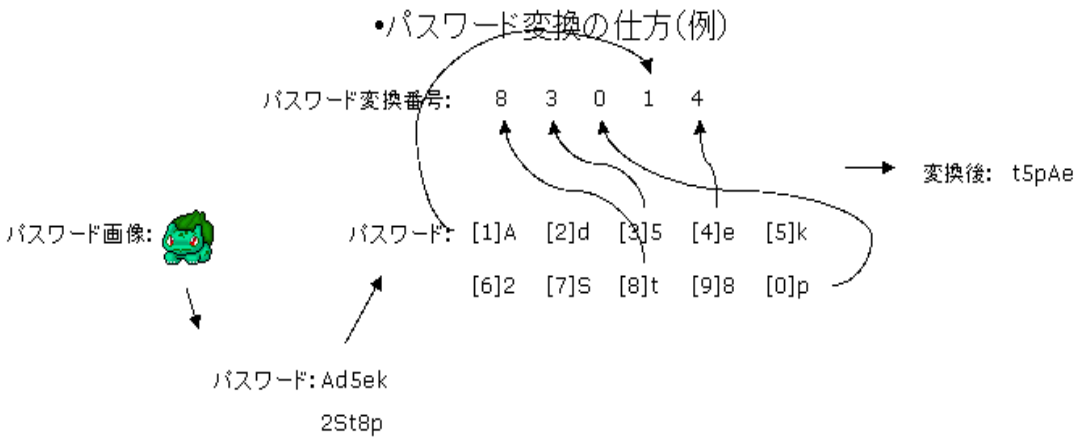

図 1.1: パスワード変換方法

認証作業は、上記の 5. 〜6. をセットで 2 回行う。

画像認証で起こりうる 4 つの攻撃の内、本研究手法が力を入れた Brute-force 攻撃と Observation 攻撃の 2 つに対する耐性を述べる。1 つ目の Brute-force 攻撃はしらみつぶしにパスワードを試す攻撃である。この攻撃に対してはまず、選ぶ画像が 200 体なので 200 通り、次に正解キャラクタの英数字をパスワード変換番号（5 桁）で変換するので 00000〜99999 までの 1 万通り確保できる。これを計算すると 200 × 1 万=200 万通りになる。認証作業はこれをもう一度行うので 200 万× 200 万=400 兆通りの総当り数を確保できることになる。2 つ目の Observation 攻撃とは、第三者によるユーザ本人の認証作業の覗き見である。本研究手法にこの攻撃をしようとすると、パスワードを入力する際の手の動きから入力した文字を読み取りその文字を 200 体のキャラクタが変化した各々10 桁の英数字と比較しなければならないので、非常に困難である。

また、既存の一般的なパスワード認証で用いられるランダムな英数字 8 桁と本研究手法ではどちらパスワードを忘れにくいかを実際に使ってもらい実験した。実験 1 結果表を見ると、パスワード認証の方は時間がたつにつれて完全にパスワードを記憶している人数が減っていった (1 週間後にはパスワードを記憶している人は半分に) のに対し、本研究方式はパスワードを忘れた人はいなかった。実験の詳細は第 4 章のパスワードの記憶率実験を参照。

以上のことから本研究手法を利用することで、覗き見によるパスワード漏洩の防止など、より安全な Web 認証を提供することができる可能性が示された。ただ、今回の実験はユーザの数が 8 人と少ないので、パスワードの覚えやすさの優位性

	直後	3時間後	1日後	1週間後
本研究手法	8人	8人	8人	8人
パスワード認証	8人	6人	6人	4人

表 1.1: 実験1結果表

に関しては可能性が示されただけである。しっかりとパスワードの記憶しやすさの優位性を証明するためにはユーザを年齢層などでわけていろいろな特性のあるユーザをさらに多く調べる必要がある。

1.2 本研究の位置づけ

従来研究では、認証作業の際に正解画像を選ぶ作業だけで、認証している。これでは認証作業を覗き見されるとパスワードがばれていまうので、正解画像を選ばなくても認証作業できるようにした。なので、画像だけの認証よりはユーザに覚えてもらうことが増える。しかし、今回はパスワードの安全性を考慮した結果、画像だけでは安全性を保てないという結論にいたり、もうひとつユーザ独自のパスワード変換アルゴリズムを取り入れた。

1.3 研究の意義

本論文で提案する、画像とパスワード変換を使う認証方式を利用することで総当り数を400兆通り確保できるので、既存のパスワード認証（英数字8文字）の総当り数、約218兆3401億通り以上を確保しながら覗き見されてもパスワードが他人にわからないようにすることができる。さらに長期記憶の中の手続記憶を用いることでパスワードを忘れにくくすることができる。

1.4　本論文の構成

本論文は以下の 6 章からなる。

第 1 章　序章

本論文の概要、目的、構成について述べる。

第 2 章　従来の関連研究

従来の関連研究を紹介し、その問題点について述べる。

第 3 章　本研究が解決する問題点の定義と仮定

本手法で目的とする、問題点の定義について述べ。各種用語を定義する。また、提案する手法を利用する際の前提となる仮定について述べる。

第 4 章　ゲーム性を持った画像認証方式の手法

本手法について述べ、その実現方法について述べる。

第 5 章　ゲーム性を持った画像認証方式の実験と考察

提案した手法に対しての実験を行った結果とその評価について述べる。

第 6 章　結論

本論文のまとめを述べ、今後の課題を述べる。

第2章　画像認証に関する関連研究

本章では、まず本研究が対象とする画像認証に使われている、パスワードを忘れにくくする方法として、人間の特性である長期記憶 [8] を利用する。そこで人間の長期記憶であるエピソード記憶と意味記憶、手続記憶の 3 つについて説明する。次に画像認証の既存の関連研究を紹介し、既存の認証方式の比較を行い、問題点を明らかにする。

2.1　長期記憶

本節では、人間の特性である長期記憶を分類し、エピソード記憶と意味記憶と手続記憶の 3 つに分けて説明する。

2.1.1　エピソード記憶

エピソード記憶とは、「先週の日曜日は、友達とディズニーランドに行き、その後、ワインを飲みながらフランス料理を食べて、11 時に家に帰った」というような特定の時、人、出来事についての記憶である。エピソード記憶は個人的な体験に基づいた記憶である。

2.1.2　意味記憶

意味記憶とは、「常用漢字は 1945 字ある」とか、「『目』という漢字は絵からできた象形文字だ」といったような、知識としての記憶であり、学習された一般的に認められているものである。意味記憶は一般的な知識についての記憶である。

2.1.3　手続記憶

手続記憶とは、やり方の知識で,「自転車乗り」とか「スキーを滑る」といったような体に身についている技能の記憶である。特定の事実やデータ，特定の時間に特定の場所で生じた出来事とは関係がなく，学習された技能や認知的操作の変容に関わる記憶で損なわれることがない。つまりやり方が「わかっている」「できる」ことである。手続記憶はやり方の知識についての記憶である。

これら 3 つのうち、もっともももろいのがエピソード記憶で、もっとも崩れにくいのが手続記憶だと言われている。本研究では、もっとも忘れにくい「手続記憶」を用いる。

2.2 関連研究

本節では、画像認証に関する関連研究を紹介する。まず、パスワードを画像に変更した「Deja Vu[1]」、意味記憶を利用した「ニーモニックガード [3]」と「あわせ絵 [4]」について紹介し、それらを比較することでそれらの手法の問題点と本研究との相違点を挙げる。

2.2.1 Deja Vu

代表的な画像認識システムの研究として Deja Vu がある。Deja Vu はコンピュータによって生成された人口画像を選択する画像認証システムである。登録フェーズで計算機で自動生成した数千枚の画像の中から、パスワードの代わりに 5 枚の画像を画集として登録する。認証時にはパスワード画像をおとり画像（自分の選んだ画集に登録されていない画像）と混ぜて 25 枚表示する。その中から正確に登録画像を選ぶことができるユーザが正規ユーザになる。

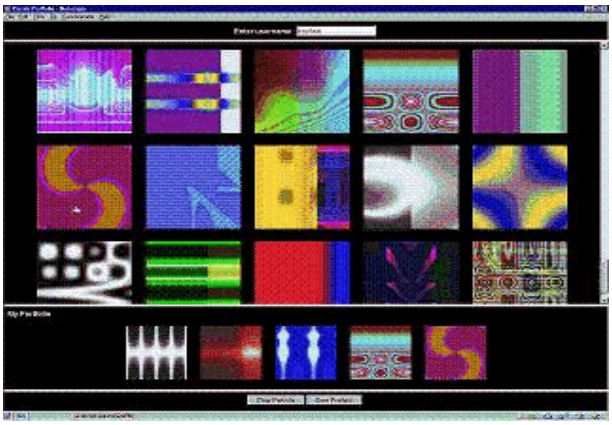

図 2.1: Deja Vu のログイン画面

（出典：http://www.sims.berkeley.edu/ rachna/dejavu/）

画像の細部を正確に思い出すのではなく、以前に見た画像のイメージに基づくユーザ認証を実現していることが Deja Vu の特徴である。個々のユーザにとって人口画像は認識の仕方が異なるので、紙に書きとめたり、他人に伝えるのが難しいと思われる。

本研究の目的としているパスワードを忘れにくいものにするというテーマを、人間の特性である物事を正確に記憶するよりあいまいに全体を記憶する方が得意であるという特性を用いて解決を試みているが、覚える画像が人工的にランダム生成されたものなのでランダムな文字列よりはましだが、やはり覚えにくいものである。さらに、覗き見に対する対策がされていないので覗き見されるとパスワードが他人にばれてしまう。

2.2.2 ニーモニックガード

ニーモニックガードという画像認証システムでは、認証フェーズに人や動物や乗り物などのイラストの一覧が表示される。ユーザは登録フェーズでいくつかの画像を登録する。登録順番通りに選択できればユーザを正規ユーザとする。ニーモニックガードが優れている点はイラストを意味のある文章として記憶できるところにある。例えば「男の子のイラスト→女の子のイラスト→飛行機のイラスト→南の島のイラスト」と選ぶとする。これを「僕と彼女が飛行機で南の島へ旅行」という意味のある文章に関連付けて意味記憶を利用した認証システムである。

この方式は、パスワードを意味記憶に関連付けて記憶することにより、パスワードを忘れにくくしている。後ろからの覗き見に弱い点は「Deja Vu」と同じである。

図 2.2: ニーモニックガードのログイン画面

（出典：http://www.mneme.co.jp/neme/neme.html）

2.2.3 あわせ絵

他にもあわせ絵という画像認証方式がある。ユーザ本人にとって意味のある画像を認証の画像パスワードに設定するというものである。Deja Vu と違いユーザ自

評価項目	Deja Vu	ニーモニックガード	あわせ絵	本研究方式
Brute-force 攻撃	×	△	△	○
Educated Guess 攻撃	○	○	×	○
Observation 攻撃	×	×	×	○
Intersection 攻撃	×	○	○	○

表 2.1: 関連研究との安全性の比較

身が撮影した画像を使うので、エピソード記憶としてユーザの頭に強く残る。登録フェーズで画像をメールでサーバに送信して、その中から自分の好きな画像を 2 枚選択する。認証フェーズで 4 回の照合作業を行って本人認証をする。ユーザが写真を登録することにより使えば使うほどおとり画像が増えるという優れた点がある。

この方式は意味記憶を用いているが、パスワードとなる画像を自分の関連のある画像にしているのでより忘れにくいものになっている。しかし、この方式は携帯電話を想定して作られているのでパスワードとなる画像をユーザが携帯の中に残している可能性がある。さらにユーザのことを知っている人間であれば比較的パスワードを推測することができると思われる。この方式も覗き見に対する対策はされていない。

2.3 関連研究の比較と問題点

本節では、前の節であげた、Deja Vu、ニーモニックガード、あわせ絵の 3 方式と本研究方式について、画像認証でおこりうる攻撃 4 種、Brute-force 攻撃、Educated Guess 攻撃、Observation 攻撃、Intersection 攻撃の 4 項目について分類し、比較する。

Brute-force 攻撃とは、すべてのパスワードをしらみつぶしに試す攻撃である。Educated Guess 攻撃とは、あるユーザに関する情報を持つ第三者がその情報を基にパスワード情報を推測することでなりすましを行う攻撃である。Observation 攻撃とは、第三者によるユーザ本人の認証作業の覗き見である。Intersection 攻撃とは、画像認証に特有の攻撃で「パスワード画像が照合時には必ず提示される」という前提に絵の比較を行い、その差異を見てパスワード画像を見破る攻撃である。

Brute-force 攻撃の項目は、パスワード認証で確保されている総当り数（約 218 兆 3401 億通り以上）を確保できている場合のみ○をつけた。ニーモニックガードとあわせ絵は試行回数を制限するようになっているがそのガードを逆手にとり、多数のアカウントをロックするような DoS 攻撃なども考えられるので△をつけた。

Observation 攻撃の項目は、認証作業を除き見されても推測が非常に困難である場合のみ○をつけた。

そこで本論文では、関連研究ではすべて × がついている Observation 攻撃に強く、Brute-force 攻撃にも強い画像認証方式である本研究方式を提案する。

2.4 本章のまとめ

本章ではまず人間の長期記憶をエピソード記憶と意味記憶と手続記憶の 3 つに分けて説明した。また、画像認証の関連研究として、「Deja Vu」、「ニーモニックガード」、「あわせ絵」について述べた。これらの方式はパスワード自体は覚えやすいが、安全性がパスワード認証ほど確保されていないことを述べた。最後に、関連研究を比較し、解決すべき問題点を明らかにした。

次章では、以上を参考に、本研究手法であるゲーム性を持った認証方式の詳細について述べる。

第3章　ゲーム性を持ちObservation攻撃に強い認証方式

本章では、本論文で提案するゲーム性を持ちObservation攻撃に強い認証方式の概要と、実装環境、さらに実装の詳細のアルゴリズムについて述べる。

3.1　本研究手法の概要

本節では、本研究手法の概要として、本手法を利用する上での仮定、本手法のシステム構成、動作の全体の流れを示す。

3.1.1　仮定

本節では、いくつかの前提となる仮定を定義する。本研究手法を利用する際、以下に示す仮定の下で行うものとする。

1. Web上でのオンライン決済など高いセキュリティレベルが求められる認証に使用するものとする。
2. パスワードの入力を他人に後ろから見られることがあるものとする。
3. パスワードを書き留めたり、ファイルに保存してはいけないこととする。
4. 認証作業中のＰＣの映像と手の動きの両方をビデオなどで記録されないものとする。
5. 登録作業は他人には見られない場所で行うものとする。

3.1.2　本手法の構成

本手法の構成を登録フェーズと認証フェーズに分けて述べる。
本手法の構成は図3.1に示すようになっている。

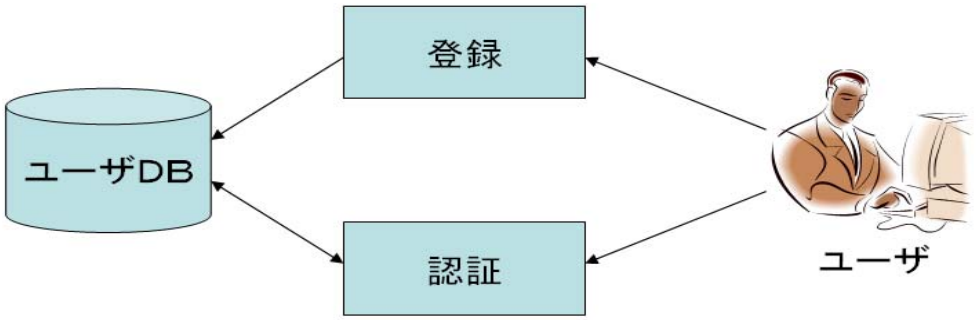

図 3.1: System 構成

3.1.3 全体の流れ

登録フェーズの処理の流れは以下のようである。

1. ユーザ名を決める。
2. キャラクタ 200 体が表示されるので、その中から好きなキャラクタを 1 体選ぶ（以降、正解キャラクタと呼ぶ)。
3. パスワード変換番号（5 桁）を決める、後でパスワードの変換で使用するのでしっかり記憶しておく。パスワード変換番号の変換の仕方は図??に示すようになっている。
4. 2. で表示された 200 体のキャラクタがランダムに配置されているので、その中から正解キャラクタを探し、場所を覚えて正解キャラクタをクリックする。
5. ここからログイン作業に入る。まず 4. と同じ 200 体のキャラクタがランダムに配置された画像が表示される、違うのは正解キャラクタが表示されていない部分。ユーザ本人なら正解キャラはわかるはずなので、表示しない。その中から正解キャラクタを探す。見つけたら「切替ボタン」をクリックする。
6. 200 体のキャラクタがすべて 10 桁の英数字に変化するので、3. で決めたパスワード変換番号で正解キャラクタが変化した英数字を並び変えて、パスワードを入力する。
7. 2.〜6. の作業をもう一度行い、計 2 回行うことで登録完了となる。

次に、認証フェーズの処理の流れは以下のようである。

1. ユーザ名を入力する。
2. 登録フェーズで使った 200 体のキャラクタがバラバラに並べられた同じ画像が表示されるので、その中から正解キャラクタを探し、「切替ボタン」をクリックする。
3. 200 体のキャラクタがすべて 10 桁の英数字に変化するので、パスワード変換番号で正解キャラクタが変化した英数字を並び替えて、パスワードを入力する。
4. 2.〜3. の作業を計 2 回繰り返し行い、2 回とも成功して認証成功となる。

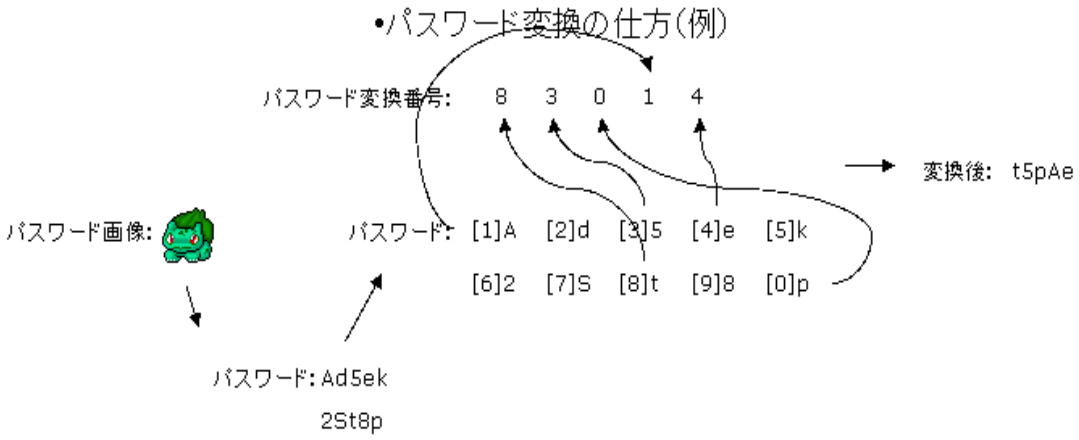

図 3.2: パスワード変換方法 (再掲)

3.1.4 ランダムな数字の記憶法 [7]

パスワード変換番号（5 桁）の効率的な記憶方法について述べる。

つがわ式暗証番号の作り方の方法を使う。数字の代わりに、昔好きだった歌手やタレント、ひそかに思いを寄せている人の名前、仲の良かった親友の名前、好きな番組名や食べ物を数字の代わりに暗証番号として、頭の中 に登録する。これは他人にはわからない上、自分は絶対に忘れることはない。

名前を下記の方法で数字に変換する。その法則は、”ア・カ・サ・タ・ナ・ハ・マ・ヤ・ラ・ワ”の 各行と数字”１・２・３・４・５・６・７・８・９・０”と 対応させる法則である。つまり、ア行の文字は、全て「１」を 意味する。カ行の文字は全て「２」を意味する。同様に、 サ行は「３」、タ行は「４」、ナ行は「５」、

ハ行は「６」、マ 行は「７」、ヤ行は「８」、ラ行は「９」、ワ行は「０」を意味する。それが覚えれない人は、手の指を右手の親指から順に、「アカ サタナ…」と折っていけば覚えなくても、すぐに数字に変換できる。

例えば絶対にバレない名前として、「”長嶋”さん」 を暗証番号にしたいと思ったら、数字は「５２３７」を登録する。「”ながしま”さん」の「な」はナ行の「５」、「が」 はカ行の「２」、「し」はサ行の「３」、「ま」はマ行の「７」 と言うわけです。つまり、登録した数字は忘れても、「ながしま」さえ忘れなければ、いつでも数字に返還できることになる。桁の調整は、はじめは７や５にするなど自分で決めておけば５桁のランダムな数字を簡単に作れる。

	あ行	か行	さ行	た行	な行	は行	ま行	や行	ら行	わ行
数字	1	2	3	4	5	6	7	8	9	0

表 3.1: つがわ式暗証番号の作り方の対応表

3.2 本研究システムの実装

本節では、本研究システムであるゲーム性を持った認証方式の詳細な実装について述べる。

まず実装環境について述べる。そして本研究システムを構成する、登録部、認証部の実装について説明する。

3.2.1 実装環境

本手法利用のための登録部、認証部の実装には図 3.2 に示す環境で行った。

CPU	Pentium M 1.80GHz
RAM	1280MB
OS	Windows XP

表 3.2: 実装環境

3.2.2 登録部

入力画面の表示、及び認証部はすべて FLASH で実装した。

1. ユーザ名を入力してＯＫボタンを押すと、checkData(oSharedObject.data.user) でユーザＤＢ（00000001.sol）にアクセスして、同じユーザ名がないか if 文でチェックする。同じユーザ名がない場合、gotoAndPlay() でキャラクタ選びのページにとぶ。

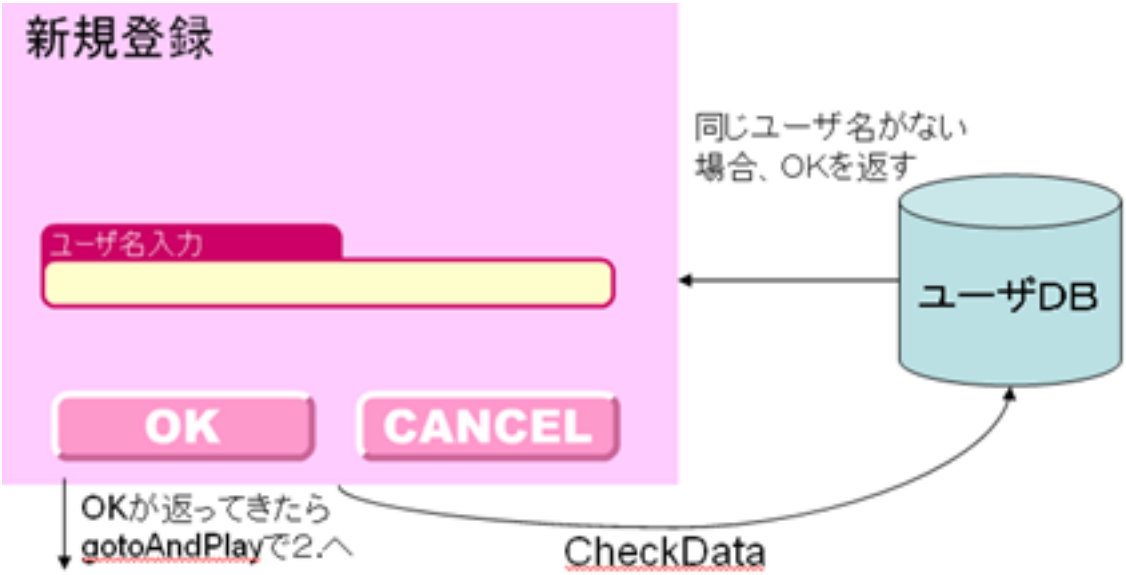

図 3.3: 画面 1

2. 200 体のキャラクタがすべてムービークリップボタンになっている。正解キャラクタを決めてキャラクタボタンが押すとその画像の画像番号を_global 変数 gazou_num に格納して、gotoAndPlay() でパスワード変換番号を登録するページにとぶ。

図 3.4: 画面 2

3. パスワード変換番号が入力されるたら、パスワード変換番号を_global 変数 pass_num に格納して、gotoAndPlay() で正解キャラクタを探すページにとぶ。

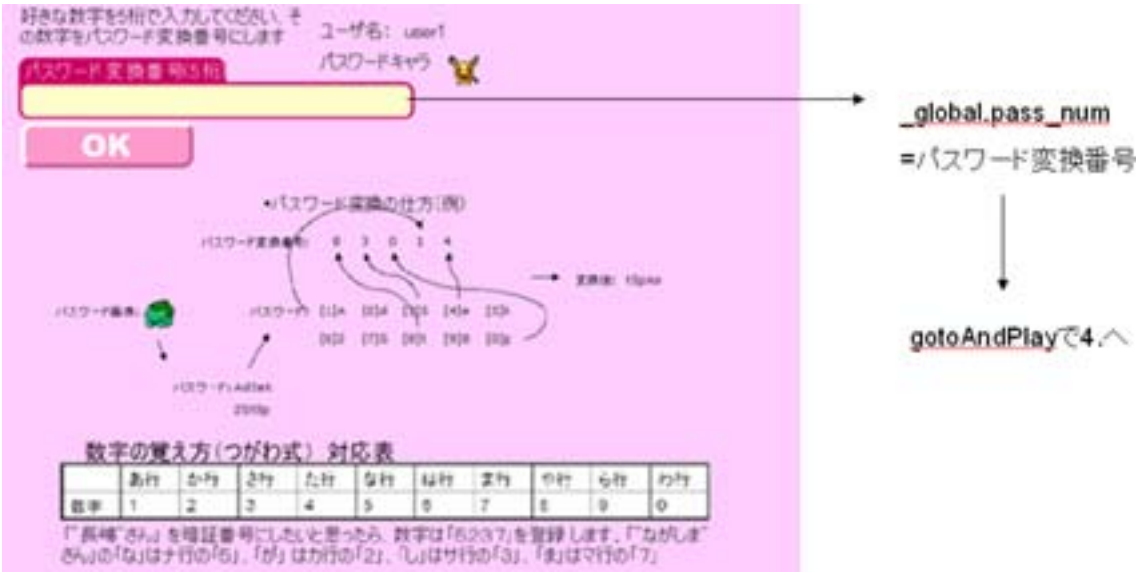

図 3.5: 画面 3

4. 2. で表示された 200 体のキャラクタがバラバラに配置されている。このキャラクタもすべてムービークリップボタンになっているので、正解キャラクタをその中から探して、場所を覚えてキャラクタボタンを押すと、gotoAndPlay() でログイン画面にとぶ。

図 3.6: 画面 4

5. 4.で表示された画像と同じ画像が表示される。正解キャラクタはユーザ本人はわかっているので表示しない。正解キャラを見つけたら、「切替ボタン」を押す。すると 200 体のキャラクタすべてのムービーが始まり、10 桁のランダムな英数字に切り替わる、このときパスワード変換番号を使って並び替えたパスワードを変数に格納する。このパスワードとユーザの入力したパスワードが一致すれば認証成功。

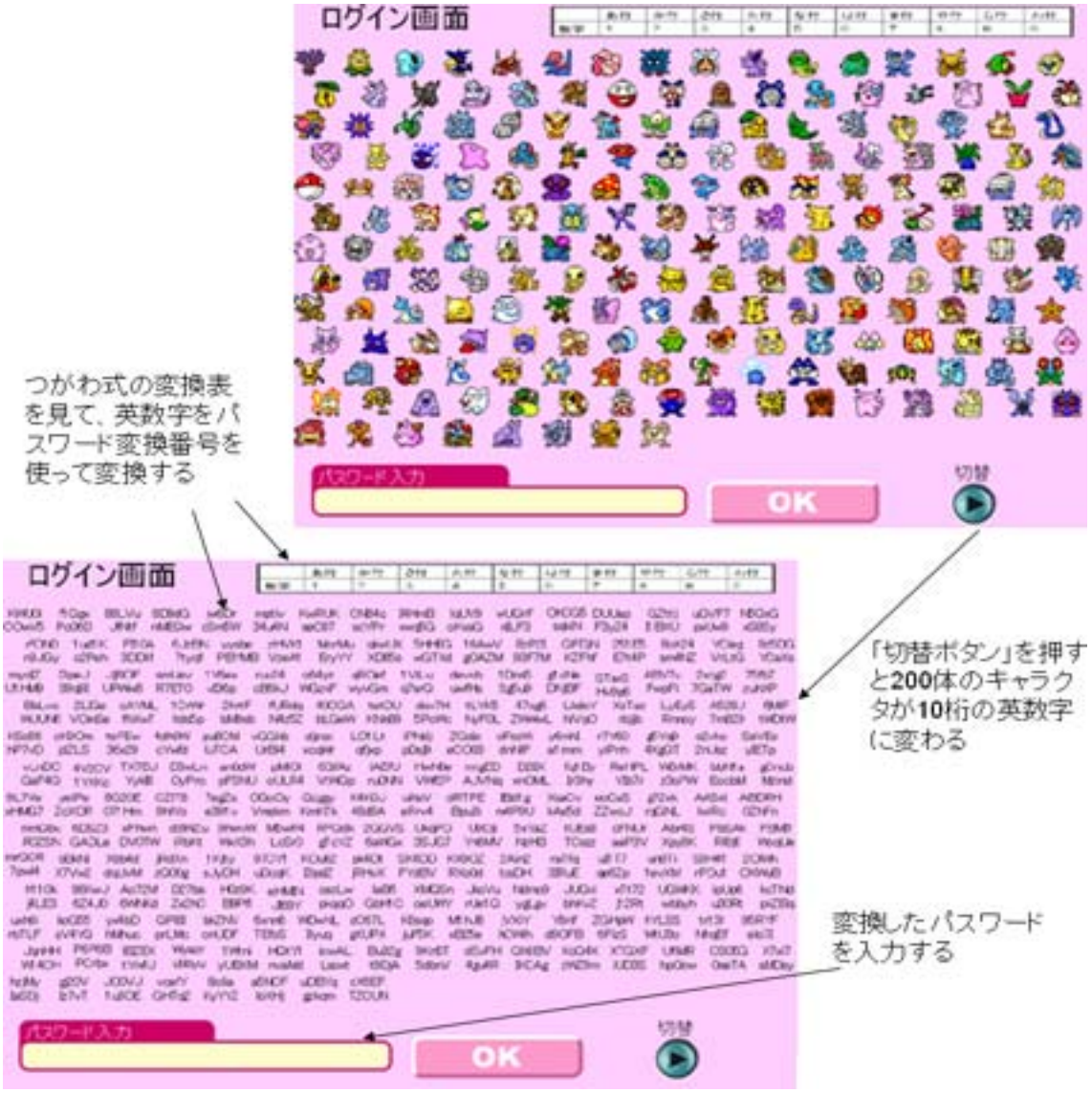

図 3.7: 画面 5

6. 2.〜5. の作業をもう一度行い、計２回で登録完了となる。

登録するデータは、ユーザ名、1 つ目の正解キャラクタの画像番号、1 つ目のパスワード変換番号、2 つ目の正解キャラクタの画像番号、2 つ目のパスワード変換

番号である。

3.2.3 認証部

1. ユーザ名を入力してＯＫボタンを押すと、checkData(oSharedObject.data.user)でユーザＤＢ（00000001.sol）にアクセスして、同じユーザ名がないか if 文でチェックする。同じユーザ名あった場合、そのユーザの 1 つ目の正解キャラクタの画像番号、1 つ目のパスワード変換番号、2 つ目の正解キャラクタの画像番号、2 つ目のパスワード変換番号の 4 つを各々の配列に格納する。

2. 配列の値を使い、登録部の 4.〜5. の作業を 2 回行い、2 回とも成功した場合認証成功となる。

ユーザ名を入力して、ユーザＤＢにアクセスしてユーザ名があればそのユーザの 1 つ目の正解キャラクタの画像番号、1 つ目のパスワード変換番号、2 つ目の正解キャラクタの画像番号、2 つ目のパスワード変換番号の 4 つを取ってくる。そのデータを下に認証画面を再現し、認証する。

3.3 本章のまとめ

本章では、本手法であるゲーム性を持った認証方式のプログラムの詳細を全体の流れに沿って述べた。次章では、本手法の評価を行う。

第4章　本研究手法の評価と考察

本章では、3 章で述べたゲーム性を持った認証方式の評価と考察を行う。

4.1　4 つの安全指標

本節では、画像認証でおこりうる代表的な 4 つの攻撃からの本研究手法の耐性について述べる。下記に 4 つの攻撃を箇条書きにした。

- Brute-force 攻撃
- Educated Guess 攻撃
- Observation 攻撃
- Intersection 攻撃

4.1.1　Brute-force 攻撃

Brute-force 攻撃とは、すべてのパスワードをしらみつぶしに試す攻撃である。画像認証は基本的に総当り数を現在の英数字 8 文字のパスワード認証並み（総当り数 218 兆 3401 億通り以上）を確保するのは非常に難しい。これに対抗するために、他の画像認証方式は試行回数に制限を設けたり、選んではいけない画像を混ぜることにより対処している。しかし、この方法では多数のアカウントをロックするような Dos 攻撃による被害を受ける可能性があるので、よい方法とは言えない。そこで本研究方式は、画像認証の弱点である Brute-force 攻撃に対抗するために、パスワード認証以上の総当り数を確保できるようにした。まず、選ぶ画像が 200 体なので 200 通り、次に正解キャラクタの英数字をパスワード変換番号（5 桁）で変換するので 00000〜99999 までの 1 万通り確保できる。これを計算すると 200 × 1 万=200 万通りになる。認証作業はこれをもう一度行うので 200 万× 200 万=400 兆通りの総当り数を確保できることになる。また、画像は無視して、パスワード (5 桁) の入力だけ行う方法で Brute-force 攻撃も考えられるが、この場合は 5 桁の入力が 2 回なので、実質 10 桁のパスワード認証に Brute-force 攻撃をすることになるので十分 Brute-force 攻撃に耐えうるといえる。

4.1.2 Educated Guess 攻撃

Educated Guess 攻撃とは、あるユーザに関する情報を持つ第三者がその情報を基にパスワード情報を推測することでなりすましを行う攻撃である。本研究方式では、使用する画像が写真ではなくキャラクタである。第三者による推測の容易さを考えた場合、写真の場合、多くのユーザはその記憶が容易であるため、何らかのかたちで自分に関連のある写真を選んでしまう傾向がある。これに対して、キャラクタの方は自分に関連のあるキャラクタというものは写真ほど明確にはならないので写真を使うよりは安全である。他にも定期的なパスワードの更新も有効である。本研究方式である、ゲーム性を持った認証方式はその名のとおり登録作業にゲーム性を持たせている。これはパスワードの記憶に手続記憶を利用するためだけではなく、ユーザに少しでも多くパスワードの定期的な更新を自発的に行ってもらうためでもある。パスワードの更新が増えれば、パスワードの強度は一気に上がるためパスワードの更新を促すことは重要なことである。

4.1.3 Observation 攻撃

Observation 攻撃とは、第三者によるユーザ本人の認証作業の覗き見である。本研究では、画像認証とパスワード認証の最大の弱点であるこの Observation 攻撃からの耐性を十分に上げたことが最も大切な部分である。まず、パスワードを見破るためには正解キャラクタの場所を特定しなければならない。見破るためのヒントは、まず目線が考えられる。しかし認証作業中のユーザ目線を確認するためにはユーザの視界に入らなければいけない。ＰＣに向かっているユーザの視界に入るというのはあきらかに不自然であるため、たとえそのような状況が起こって注意することができる。もう一つ見破るためのヒントとして、パスワードを入力する際の手の動きから文字を読み取りその文字を 200 体のキャラクタが変化した各々 10 桁の英数字と比較するいう方法があるが、これも非常に困難である。当然、パスワードは毎回変わるので手の動きだけ見ても見破ることはできない。以上のことから、Observation 攻撃に対しては非常に高い耐性があると考えられる。

4.1.4 Intersection 攻撃

Intersection 攻撃とは、画像認証に特有の攻撃で「パスワード画像が照合時には必ず提示される」という前提に絵の比較を行い、その差異を見てパスワード画像を見破る攻撃である。本研究方式は、画像を選ぶだけの画像認証方式ではないので、表示される画像は毎回同じである。よって、Intersection 攻撃を受けることはない。

4.2　5ユーザでテストすれば十分な理由

参考文献9の調査でLandauerとNielsenはn人のユーザをテストしてわかるユーザビリティ問題の数は、次の式で求められることを明らかにした。

$$N(1-(1-L)^n) \tag{4.1}$$

数式のNはデザイン上のユーザビリティ問題の数であり、Lはひとりのユーザをテストして発見できるユーザビリティ問題が全体に占める割合を示している。参考文献より、数多くのプロジェクトを調査した結果、典型的なLの値は平均して31 %であることがわかったようだ。L=31 %として曲線を描いてみると、次のようになる。

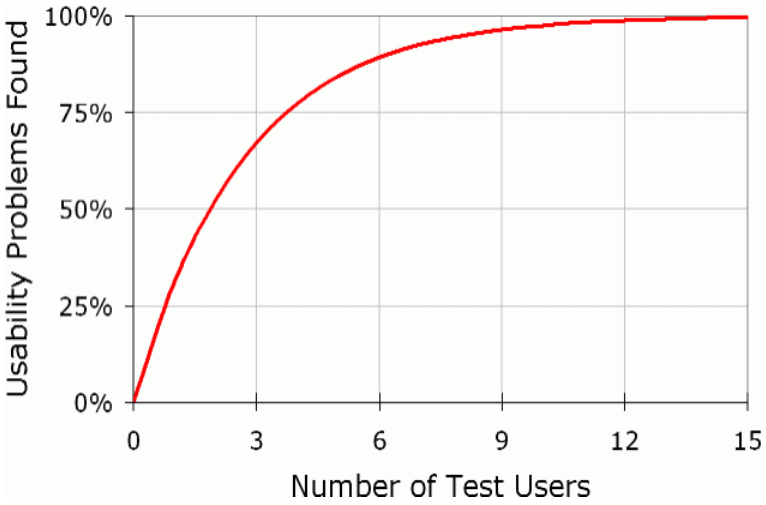

図 4.1: ユーザビリティ調査

図4.1を見ればわかるように、ユーザ5人で80 %くらいのユーザビリティの問題を発見できる。と同時にユーザ15人で実験すればほぼ100 %のユーザビリティの問題を発見できる。なぜ15人ではなく5人でテストを行うのがよいかというと最大の理由は、1回だけ徹底的な調査をやるよりも、その予算を振り分けて小さなユーザテストをたくさんやったほうがいいからである。新しいデザインが出来上がったら、もう一度テストする必要がある。完璧なユーザインターフェイスをデザインできる者などいないのだから再度テストして新たな問題が出ていないかを調べる必要がある。それなので、小さなテストをたくさん行ったほうがよいのである。ユーザ1人でテストをしない理由は明白でたまたま選んだユーザが変わった趣味の持ち主だった場合、誤った方向に結果が出てしまう可能性があるからである。ユーザ5人でテストすれば、どれがユニークな結果で、どれが一般的な結果なのかも十分わかる。
本論文の実験ではユーザを8人で行っている。図4.1を見ると、ユーザ8人だと

のユーザビリティの問題は90〜95％発見できることになる。テストしたサイトのユーザビリティの問題を90％以上発見できるのであれば、かなりそのサイトを熟知していることになる。このLandauerとNielsenらの研究結果から、8人のテストでも優位性の可能性があるという程度であれば示せると考え、本論文では8人でのユーザビリティのテストを行った。
また、Nielsenらはかなりはっきりした違いのあるユーザ集団がいくつか存在することがわかったらユーザを追加してテストする必要があるとしている。これは、子供と大人の両方が利用するサイトなら、2つのユーザ集団はかなり異なった行動をとるだろうから、両方のグループから人を招いてテストする必要があるということである。ただ、ユーザ集団の違いがあるにせよ、同じ人間なので観察結果に大きな違いはでないとしている。
より多くのタイプの人間が利用することを考える場合、その優位性を証明するためにはユーザのタイプ別でユーザテストを多く行った方がよい。

4.3 パスワードの記憶率実験

本節では、現在広く一般的に使われているパスワード認証で覚える必要のある英数字8桁と、キャラクタ画像1体と数字5桁をセットで2つ記憶することを比較した場合どちらが忘れにくいか、本学部生8人に実際に試してもらい比較してもらった。比較はパスワード登録直後、1日後、1週間後で比較した。

4.3.1 実験条件

1. パスワードは一度もメモしてはいけない。
2. パスワードはランダム性のあるものを記憶するものとする
3. 画像を見るのは認証の時だけで、それ以外は見ることはない。
4. パスワードも覚えるのは認証の時だけで、それ以外では見ることはない。

4.3.2 実験方法

各ユーザにはそれぞれ自分でパスワードを決めてもらう。パスワード認証の方は、ユーザにＰＣに入力してもらい、登録したパスワードと一致するかを確かめた。次に実際に本研究システムを使ってもらいパスワードを登録してもらった。パスワード登録直後、1日後、1週間後にパスワード認証のパスワード確認と、本研究システムを使ってもらい登録後どのくらいでパスワードを忘れるかを比較した。実験後に被験者が主観的にパスワードを覚える負荷が少なく感じたかを聞いた。

4.3.3 実験結果

パスワード登録直後、1 日後、1 週間後に分けてパスワードを完全に覚えている者の人数を表にした。

	直後	3 時間後	1 日後	1 週間後
本研究手法	8 人	8 人	8 人	8 人
パスワード認証	8 人	6 人	6 人	4 人

表 4.1: 実験 1 結果表 (再掲)

また、「パスワード認証」と「本研究手法」ではどちらがパスワードを覚える負荷が少なかったと感じたかという質問には 7 人の被験者が本研究手法と答えた。

4.3.4 考察

実験結果からわかるように、パスワード認証は時間がたつにつれて覚えている人数が減ったのに対して、本研究手法は 1 週間しても全員が覚えているという結果がでた。これにより、本研究手法の方がパスワード認証よりパスワードを忘れにくいことが示せた。ただ、本研究手法の認証システムを使ってみた直後に感想を聞いたところ、ほとんどのユーザがややこしくて複雑、わかりにくいという意見が多かった。1 週間後にまだややこしくてわかりにくいかと聞いた所、ほとんどのユーザから慣れてきたという意見が聞けた。この意見からはじめはややこしくて使いにくいが、一度使い方を理解すれば問題なく使えるようだ。今回の実験はユーザの数が 8 人と少ないので、しっかりとした優位性を証明するためにはすべての年齢層のユーザを大量に調べる必要がある。

4.4 判別しやすい画像の種類の比較実験

本節では、本研究で使用する画像の種類を、「顔写真」、「キャラクタ」の二つを比べてどちらが覚えやすく、200 体並べたときに正解の 1 体を探しやすいか、どちらが忘れにくいかを、本学部生 8 人に実際に見比べて、比較しもらった。

4.4.1 実験条件

1. 顔写真はユーザとは無関係のものを使用する
2. キャラクタもユーザとは無関係のものを使用する
3. 実験の時以外、ユーザは画像を見ることはない

4.4.2 実験方法

各キャラクタや顔写真のサイズは 30 ピクセル× 30 ピクセルのものを使用した。200 体がランダムに並んだ画像を見せて、こちらで正解画像を指定するので探してもらう。見つけるまでにかかった時間を計測する。さらに後日同じ画像を見せてどのくらい正解画像を見つけるまでに時間がかかるかを計測する。

4.4.3 実験結果

初見時、直後、1 日後、1 週間後に分けて画像発見の時間を計る実験を行い計測した時間を表とグラフにした。数値は被験者 8 人の平均値を取った。

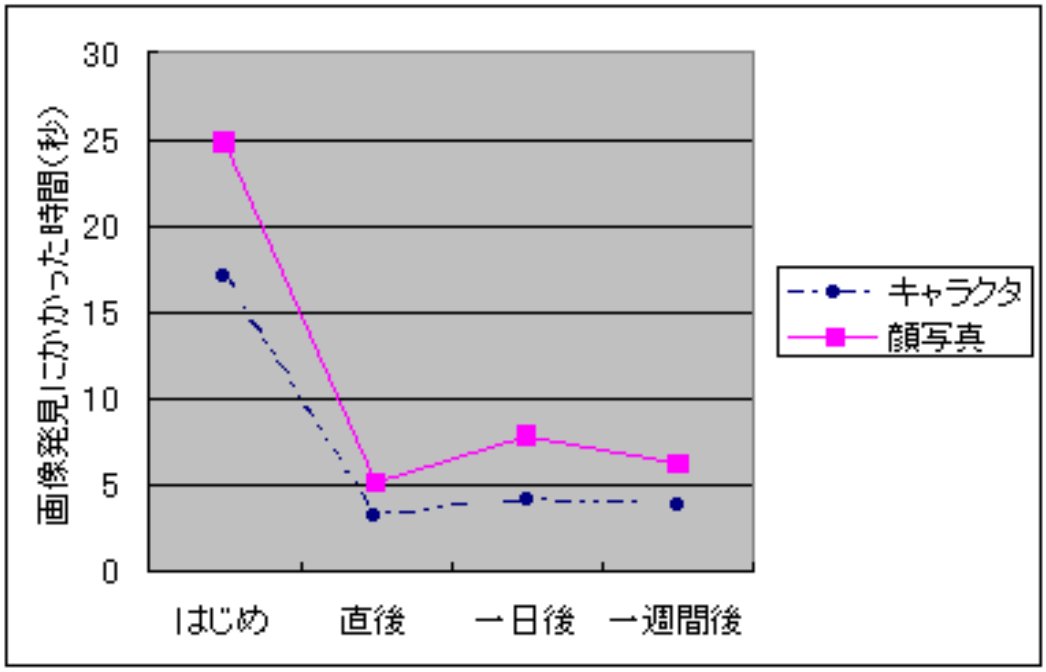

図 4.2: 実験 2 結果

	はじめ	直後	1 日後	1 週間後
キャラクタ	17.1 秒	3.2 秒	4.1 秒	3.8 秒
顔写真	24.8 秒	5.2 秒	7.8 秒	6.2 秒

表 4.2: 実験 2 結果表 (平均値)

4.4.4 考察

今回の「キャラクタ」と「顔写真」のどちらが正解キャラクタを探しやすいかの実験では、はじめに正解キャラクタを探す場合、「キャラクタ」が 17.1 秒で「顔写真」が 24.8 秒と 7.7 秒の差が出た。これは、使っている画像の種類によることもあるが、30 ピクセル× 30 ピクセルの画像サイズでは、「顔写真」よりも「キャラクタ」の方が認識しやすいのではないかと思われる結果になった。キャラクタは形そのものが違うのが多いのに対して、顔写真は一人一人違うといっても、写っているのは人間の顔なので「キャラクタ」よりは似かよった画像になってしまう。本研究方式では、画像は似ているものよりは判別がしやすい似ていない画像の方が好ましいので、使用する画像は「顔写真」よりは「キャラクタ」の方がいいと思われる。ただし、「キャラクタ」も画像が似通っていると、判別しにくいのでなるべく似ていない画像を使用すべきである。また、「キャラクタ」と「顔写真」の両方とも正解キャラクタの発見が直後では大幅に短縮されて、「キャラクタ」では 3.2 秒、「顔写真」では 5.2 秒と大幅に短縮されている。つまり、一度キャラクタを発見するという行為は 15〜20 秒程度の頭脳労働に匹敵していると考えられる。次に、1 日経過すると記憶が薄れるため正解キャラクタの発見時間が直後と比べて両方とも 1〜2 秒ほど増加する。しかし、その増加時間はわずかであるので複数の画像の中から一つの指定された画像を探すというタスクは、人間にとって忘れにくいタスクであることが考えれらる。さらに、1 週間経過した後では、両方とも正解キャラクタの発見時間はほとんど変わらないか、短縮されていることがわかる。このようなことから、人間は一度学習した内容を反復することにより記憶が強化されるという長期記憶の特性が実験結果に表れたことがわかる。これも実験 1 と同様、今回の実験はユーザの数が 8 人と少ないので、しっかりとした優位性を証明するためにはすべての年齢層のユーザを大量に調べる必要がある。

4.5 長所と短所

本節では、本研究手法を使った場合の長所と短所について述べる。

4.5.1 長所

1. パスワードを覚えるのが楽
   実験 1 の実験結果から本研究手法は、一般的なパスワード認証よりパスワードを記憶する負荷が少ないことがわかった。つまりパスワードの更新をする負荷が減ったことになる。また、ゲーム感覚でパスワードを更新できるようにしてユーザのパスワード更新を促した。

2. Observation 攻撃に強い
   安全性の部分で述べたように、Observation 攻撃の方法である「ユーザの手の動きをみる」、「認証画面を見る」などを他人にされてもパスワードがバレないようになっているので人の目が多い場所でも安全に使える。

3. Brute-force 攻撃に強い
   2 枚の画像と 2 つのパスワード変換番号で総当り数を 400 兆通り確保しているので、パスワード認証の約 218 兆通りを大きく上回る総当り数を確保できた。

4.5.2 短所

1. 覚えることが複雑である
   実験 1 の考察でも述べたように本研究方式は、パスワード認証より認証手段が複雑になっているのではじめて使うときは十分な説明が必要である。

2. 画像が大量に必要
   最低 400 枚の画像が必要になる。さらにパスワードの更新ごとに新しい画像を使う方が毎回ゲーム性の部分の新鮮味が出る。毎回新しくなるほうがより、Educated Guess 攻撃に対する安全性が高まる。これらを満たすために画像を大量に用意するのが大変である。

3. 認証作業に時間がかかる
   一般的なパスワード認証は認証回数が 1 回なのに対して、本研究方式は認証回数が 2 回なので、認証時間にかかる時間が増える。

4.6 関連研究との比較による評価

本節では、本研究手法を画像認証の関連研究と一般的なパスワード認証と比較する。比較項目は、Brute-force 攻撃、Educated Guess 攻撃、Observation 攻撃、Intersection 攻撃それぞれに対する耐性とパスワードの覚えやすさの 5 項目である。またそれらを比較した表を 4.3 に示す。

まず、Brute-force 攻撃はパスワード認証（約 200 兆）以上の総当り数 400 兆を確保することで関連研究の中でも最高の総当り数を確保できた。また、Educated Guess 攻撃は本研究手法でも、認証に使用する画像に自分に関連のある写真を使う場合は推測されてしまうが、今回の実装ではキャラクタを使用したため他人による推測はできなくなる。Observation 攻撃には、パスワード変換を用いることで認証画面や手の動きを他人に見られてもパスワードを推測することは極めて困難になった。パスワードの覚えやすさは、実験 1 の実験結果からもパスワード認証よりも簡単に覚えられることが示せた。

評価項目	Deja Vu	ニーモニックガード	あわせ絵	password 認証	本研究
Brute-force 攻撃	×	△	△	○	○
Educated Guess 攻撃	○	○	×	△	○
Observation 攻撃	×	×	×	×	○
Intersection 攻撃	×	○	○		○
password の記憶	×	○	○	×	○

表 4.3: 関連研究の比較

4.7 本章のまとめ

本章では、本論文で提案する、ゲーム性をを持ち Observation 攻撃に強い認証方式について、実験、比較評価した。まず、一般的なパスワード認証と本研究手法を比べてどちらがパスワードを忘れにくいかを比較する実験を行った。この実験により、時間がたつにつれてパスワード認証は完全に覚えている人が減っていったのに対し、本研究方式は時間がたっても忘れた人がいなかった。このことから本研究方式はパスワードを覚える負荷が少ないことがわかった。また、本研究で使う画像を写真とキャラクタではどちらが正解画像を探しやすいかという実験では、キャラクタの方が判別しやすいという実験結果が得られた。このことから本研究手法を使う場合、画像はキャラクタを使用したほうがよいことがわかった。

第5章　結論

本章では、本論文についてのまとめを述べる。また、今後の課題について述べる。

5.1　まとめ

本論文では、Web 上の認証手段において、現在一般的に使用されているパスワード 8 桁のパスワード認証より、ユーザにとって負荷が少なく、安全性を損なわない認証方式を提案した。本手法を利用することで、覗き見によるパスワード漏洩の防止など、より安全な Web 認証を提供することができる。パスワードの覚えやすさの優位性についてはさらに多くのユーザ数で実験を行う必要がある。

5.2　今後の課題

第 4 章の実験 1 の結果から、はじめて使う時は使い方を理解するまでは、仕組みがわかりにくいという意見が聞けた。このことから実際に利用する際には、はじめのわかりにくさを改善する必要がある。また、今回の実験はユーザの数が 8 人と少ないので、あくまで優位性は可能性が示されただけである。しっかりとした優位性を証明するためにすべての年齢層のユーザをさらに多く調べる必要がある。

関連図書

[1] R.Dhamjia and A. Perring:Deja Vu:A User Study Using Images for Authentication, 9th Usenix Security Symposium, pp. 45-58,Aug,(2000).

[2] 増井　俊之：インターフェースの街角 (43) ー明るい認証システム, UNIX MAGAZINE, (株) アスキー, Vol.16, No.7, pp.185-189, July,(2001).

[3] 有限会社ニーモニックセキュリティ：モバイル端末の盗用・データ漏洩防止ソフト「ニーモニックガード」(2001),http://www.mneme.co.jp/

[4] 高田哲司, 小池秀樹：あわせ絵：登録と通知による画像認証方式の強化法, 情報処理学会論文誌, Vol.44, No.8, pp.2002-2012(2002).

[5] みゅうはぁと（素材集）,http://www.mewheart.com/

[6] 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，情報処理学会論文誌，研究報告「コンピュータセキュリティ」No.21-006，(2003).

[7] 大人の記憶法,http://www.tsugawashiki.com/merumagakiokuhou/002kiokuhou.html

[8] 長期記憶の分類,http://www.yume-net.ne.jp/dome/worldpl/

[9] Nielsen, Jakob, and Landauer, Thomas K.: "A mathematical model of the finding of usability problems," Proceedings of ACM INTERCHI'93 Conference (Amsterdam, The Netherlands, 24-29 April 1993), pp. 206-213.

謝辞

本学士論文の作成にあたって、日頃より御指導・御助言を頂いた村岡洋一教授に深く感謝いたします。

また、村岡研究室の諸氏には議論、助言、示唆という形で、また、研究室での生活でも非常にお世話になりました。上野和風氏には、研究の方向性を見据える上で多方面での相談にのって頂きました。

実験に協力していただいた学部の同級の方々、ありがとうございました。

最後に、経済面・精神面で学生生活を援助してくれた両親に深く感謝いたします。本当にありがとうございました。