社団法人 情報処理学会　研究報告
IPSJ SIG Technical Report

2004－ＤＰＳ－117　(34)
2004－CSEC－　24　(34)
2004／3／5

経験による想起の容易さを利用した認証方式

花井 將臣*，中村 逸一，吉田 英樹**，曽我 正和***，西垣 正勝***
*静岡大学情報学部，**NTT データ，***岩手県立大学ソフトウェア情報学部**

あらまし

パスワード認証は汎用性や利便性が高いが，意味のないパスワードを正確に覚えることは容易ではない。近年，この問題に対処するために，人間の記憶負荷を軽減する様々な認証方式が提案されてきており，人間が比較的得意とされる画像やエピソードの記憶を利用する方法がその好例である。本稿の目的も，人間の特性の活用によってユーザ認証を進化させることにある。一般的に人間は，過去に解いた経験のある問題に再度直面したとき，以前の経験から，初見のときよりもこれを早く解くことができる。本稿では，この人間の特性をユーザ認証に利用する一手法を提案する。本方式は様々な認証に応用でき得ると考えるが，本稿では特に画像を用いた認証システムについて検討する。基礎実験を行い，提案システムの可用性を検証する。

A user authentication system based on prior experience of the authentication task

Masaomi Hanai*, Itsukazu Nakamura, Hideki Yoshida**, Masakazu Soga***, Masakatsu Nishigaki***
*Shizuoka University, **NTT Data Corp. ***Iwate Prefectural University**

Abstract

Although password can be very useful and widely used in all kind of authentication, one problem with password is the human limitation to remember secure passwords. In recent years, several user authentication systems such as image-based authentication and episodic-memory-based authentication have been studied for reducing the load to human memory. Here we focus on another kind of human characteristic: the second trial is easier than the first trial. In general, when people face some task again which he/she has complete before, he/she would be able to finish the task faster than before. In this paper, this human characteristic is exploited to make authentication systems more effective.

１．はじめに

現在のユーザ認証は，パスワードや暗証番号（以下，パスワードという言葉に暗証番号も含める）が主流となっている。確かにパスワード認証は汎用性および利便性が高い。しかし，人間は物事を正確に記憶することは不得手であり，あいまいに覚えているほうが得意である。また，文字情報よりも視覚情報のほうが記憶に残ると言われている。すなわち人間は，ランダム（意味をもたない）で

長い文字列や数字列を覚えることは容易ではない。総当たり攻撃に対処するためにパスワードは頻繁に変更するよう推奨されているが，人間にとってそのようなことは事実上，不可能であろう。

近年，この問題に対処するために，人間の記憶負荷を軽減する様々な認証方式が提案されてきている。人間が比較的得意とされる画像やエピソードの記憶を利用する方法[1] [2] などがその好例である。著者らのグループも本稿とは別に，「パスワードを覚える」から「覚えていることをパスワードとして使う」というコンセプトの転換を提唱しており，それを人間の行動履歴に基づく認証システムとして実装している[3] 。これらの方式に共通するのは「人間の特性の把握とその活用」であり，本稿も人間が元来持ちあわせている何らかの特性を活用することによってユーザ認証を進化させることを目的としている。

一般に人間は，過去に解いた経験のある問題に再度直面したとき，以前の経験から初見のときよりもこれを早く解くことができる。また，与えられたタスクを実行するにあたり，要領を得るまではその動きがたどたどしいが，そのタスクに慣れるにつれて処理効率が向上していく。

本稿では，この人間の特性をユーザ認証に利用する一手法を提案する。本方式は様々な認証に応用でき得ると考えるが，本稿では特に画像を用いた認証システムについて検討する。基礎実験を行い，提案システムの可用性を検証する。

2．既存のユーザ認証の改良方式

2.1　画像の記憶に基づく方式

代表的な画像認証システムの研究として Déjà Vu[1] （図 1）がある。Déjà Vu はコンピュータによって生成された人工画像を選択する認証システムである。登録時に複数の人工画像が提示され，ユーザは印象が強かった何枚かを選び，画集として登録する。認証時には，登録画像がおとり画像（画集として登録されていない画像）と混在して表示される。登録画像を正しく答えることができるユーザが正規ユーザである。

一般に，人間は文字の記憶能力よりも画像の認識能力の方が優れていることが知られている[4] 。細部を正確に思い出すのではなく，以前に見たイメージを「認識」する能力に基づくユーザ認証を実現していることが Déjà Vu の特徴である。また，個々のユーザによって人工画像をどのように認識するかが異なる（例えば青色をベースとした画像があった場合，それを海のようだと認識するユーザもいるだろうし，空だと認識する者もいるだろう）ので，パスワードや暗証番号のようにこれを書き下したり，他人に伝えたりすることも難しいと思われる。

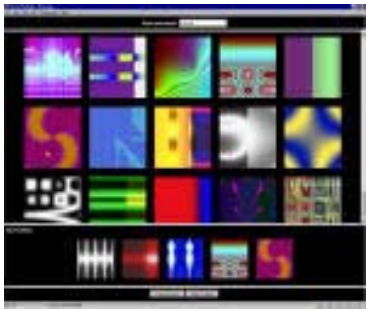


図 1　Déjà Vu の画面イメージ

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

2.2　エピソード記憶や意味記憶に基づく方式

Déjà Vu の人工画像の代わりに，ユーザがディジタルカメラで撮影した写真を使用する画像認証システムが，あわせ絵[2] である。Déjà Vu のような機械的に作られた模様はユーザにとって何の関連性もない。一方, ユーザが自ら撮影した写真は，ユーザ自信が体験した思い出の一部であり，エピソード記憶としてユーザの頭に強く残る[5] 。また，ユーザが次々と写真を登録することにより，画像の総数が増え，パスワードとなる空間が広がっていくという長所もある。

ニーモニックガード[6]（図 2）という認証システムでは，認証時に人や動物，乗り物や花のイラストの一覧が表示される。ユーザは前もって，いくつかのイラストとその順序を登録しておき，登録した順番どおりにイラストを選択できるか否かにより本人認証を行う。ユーザは，例えば「男の子のイラスト→女の子のイラスト→公園のイラスト→アイスクリームのイラスト」を「太郎と花子が公園でアイスクリームを食べた」というような意味のある文章と関連させて覚えることができる。すなわち，ニーモニックガードは意味記憶に基づく認証方式である。

図 2　ニーモニックガードの画面イメージ

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

2.3　既知情報に基づく方式

すでに複数の WEB サイトなどで，ユーザがパスワードを忘れてしまった場合に備え，前もってユーザに「本人に関する質問とその回答」を幾つか登録させておくという措置がとられている。万一，ユーザがパスワードを忘れても，登録されている質問に対して高い確率で正答すれば，本人と認証され，パスワードが再発行される。

また，著者らのグループも本稿とは別に，人間の行動履歴に基づく認証システムを提案している[3]。ユーザの PC や家電の使用履歴を逐次ロギングしておき，「昨晩 8 時から見た TV 番組は？」などといった質問をユーザに提示し，正答できた者を本人と認証する。すなわち履歴認証方式は，WEB サイトのパスワード救済措置の方式を，「本人に関する質問とその回答」が刻一刻と変わっていくように改良したものであるととらえることができる。

以上の方式は，「パスワードを覚える」から「覚えていることをパスワードとして使う」というコンセプトの転換により，ユーザ認証を改良する方法である。

3．経験による想起の容易さを利用した認証方式の提案

3.1　コンセプト

一般に人間は，過去に解いた経験のある問題に再度直面したとき，以前の経験から初見のときよりもこれを早く解くことができる。

例として，Martin Handford 著の「ウォーリーを探せ」という本[7] を考えてみよう。1 枚の絵の中に大勢の人間が細かに描かれており，その群集の中にまぎれたただ一人のウォーリーという人物を探すという一種のゲームである。初めて探すときにはウォーリーがどこにいるか分からず，必死になって全ての人間をしらみつぶしに探さないとウォーリーを発見することができない。しかし，一度ウォーリーを発見してしまえば，二回目は即座にウォーリーの場所を特定することができる。著者らの経験上，ある程度の日数が経過した後にも，一度発見したウォーリーを再度特定することは比較的容易である。

他にも，知恵の輪を解いたり，手品の種を考えたりすることなどもこの範疇に含まれる。解法や種をひらめくまでは時間がかかるが，一旦それが分かってしまえば，それ以降，同じ問題を解くことは非常に簡単である。

よって，正規ユーザにはあらかじめ一旦ある問題を解かせておき，認証時に，その問題を解く時間が早いか遅いかによって本人か否かを識別することが可能であると期待できる。

ウォーリーを実際に探したという経験はエピソ

ード記憶として頭に残ると思われる。一方，ウォーリーを発見した際に,「ウォーリーがその絵の中のどの場所にいて何をしていたか」という情報は意味記憶として頭に残ると思われる。すなわち，本認証方式はエピソード記憶と意味記憶の両方を利用した方式と言えるのではないだろうか。

また，人間は与えられたタスクを実行するにあたり，要領を得るまではその動きがたどたどしいが，そのタスクに慣れるにつれて処理効率が向上していく。例えば，子供は自転車に初めて乗るときは転んでしまうが，いつのまにか上手に乗れるようになる。PC のキーボードも，練習をすることによりタッチタイピングの速度が向上する。

よって，あるタスクに対して「ユーザがどれくらいそれに慣れているか」を指標にして，本人か否かを認証することが可能となるかも知れない。「慣れ」は，長期の学習による脳のシナプス結合強度の再調整の結果，生まれると考えられており，これに基づく認証は人間の長期記憶を利用した方式に分類されるのではないかと考える。

3.2　認証システムの実装

3.1 に示した人間の特性は様々な認証に応用でき得ると考えるが，本稿では特に,「ウォーリーを探せ」をモチーフにした画像認証システムを実装する。

本認証システムでは，300 体の異なる TV キャラクタを用いて「ウォーリーを探せ」に類似した問題を実現する。システムは「登録フェーズ」と「認証フェーズ」から成る。

(1) 登録フェーズ：

1－a) キャラクタ選択：キャラクタ一覧画面が表示され，ユーザは自分の好きなキャラクタを選択する。ユーザが選んだキャラクタが「正解キャラクラ」であり，その他の 299 体は全て「おとりキャラクタ」となる。

1-b) 出題：ある背景画像の上に 300 体の全てのキャラクタがランダムに配置された画像が「クイズ画像」（図 3）として表示される。クイズ画像のどこかに正解キャラクタが存在している。ユーザはクイズ画像の中から正解キャラクタを探し，発見したらそのキャラクタの位置をマウスでクリックする。ユーザは正解キャラクタの場所を覚える。

(2) 認証フェーズ：

登録フェーズの出題時に表示された画像と同一のクイズ画像が表示される。制限時間内に正解キャラクタを探し出して，その位置をマウスでクリックすることができれば，本人として認証する。

実際の「ウォーリーを探せ」では，正解キャラクタはウォーリーであることが自明となっているが，正解キャラクタが不正者に知られてしまうと，認証フェーズのクイズ画像から正解キャラクタの位置が特定されてしまう。そこで，本システムでは，登録フェーズのキャラクタ選択時にその都度の正解キャラクタを指定し，認証フェーズではどのキャラクタが正解であるかという情報を秘密にしている。

現在の試作システムでは 300 体の TV キャラクタ[8] を利用したが，その数や種類には制限はなく，ユーザが任意のアイコンをキャラクタとして追加してよい。背景となる画像もユーザが自由に設定することができる。なお，現在の 300 体のキャラクタは，酷似したキャラクタが相当数含まれるものの，全て異なっている。1 枚のクイズ画像の中に同一のキャラクタを複数表示させるという応用も可能であろう。

また，必要に応じて複数のクイズ画像を使用してよい。この場合，異なる背景画像を用い，各々のクイズ画像ごとに独立に登録フェーズを実行しておく。全てのクイズ画像において，それぞれの正解キャラクタを制限時間内に回答できれば本人として認証される。

図 3 クイズ画面の一例

４．基礎実験

基礎実験として，登録フェーズにおいて一度クイズ画像から正解キャラクタを発見した経験が，一定期間後にも保たれているかどうかを調査した。

３枚の異なる背景を用いて，3 枚のクイズ画像を生成し，登録フェーズにおいて初めての試行で正解キャラクタを見つけるまでの時間，および，認証フェーズにおいて登録直後, 1 日後, 1 週間後, 2 週間後の試行で正解キャラクタを見つけるまでの時間を測定した。なお，登録フェーズにおいては，正規ユーザは自分が満足するまで正解キャラクタを探す試行を繰り返すことができる。また，認証フェーズにおいては，3 枚のクイズ画像はその都度，ランダムな順序で提示される。

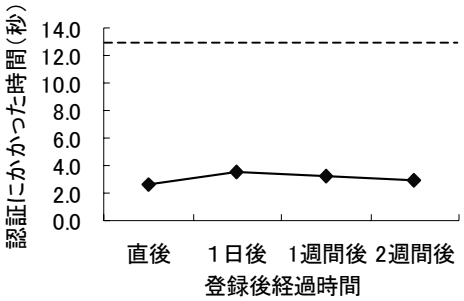
被験者は，本学情報学部の男子学生 9 名である。正解キャラクタを発見するまでの時間は，9 名の被験者の平均値を用いる。各被験者は，登録フェーズの試行，および認証フェーズにおける登録直後，1 日後，1 週間後，2 週間後の試行の時間を除き，本クイズ画像を見ることはない。

基礎実験の結果を図 4 に示す。

まず，登録フェーズでの初めての試行において正解キャラクタを発見するまでの時間の平均はおよそ 12.9 秒であった。一方，登録フェーズ終了直後の試行では，正解キャラクタの発見に要する時間は 2.7 秒程度にまで短縮されており，一度クイズを解くという経験は，およそ 10 秒程度の頭脳労働に匹敵していると見積もることができる。

登録フェーズから１日経過すると，記憶の忘却が起こるため，正解キャラクタ発見の所要時間は 3.3 秒程度に微増する。しかし，その増加時間量はわずかであり，「ウォーリーを探せ」的なタスクは人間にとって覚えやすい（忘れにくい）タスクであるということが認められる。

更に，登録フェーズから 1 週間，2 週間を経過した後では，所要時間はそれぞれ，およそ 3.2 秒，2.9 秒となった。人間は，一度学習した内容を復習することにより記憶が強化されるという特性を有しており[9]，1 日後および 1 週間後の認証の試行によって記憶が強化され，正解キャラクタを発見するまでの時間が少しずつ短縮されていっていることが分かる。



（—●—:認証時間，----:初見時にかかった時間）

図４ 認証にかかった時間の経過推移

本実験結果より，登録フェーズから 2 週間が経過してもなお，正解キャラクタを見つけるまでの所要時間は初めてときの時間よりも十分に短いということが確かめられた。よって，正規ユーザにはあらかじめ一旦ある問題を解かせておき，認証時に，その問題を解く時間が早いか遅いかによって本人か否かを識別することができる可能性が示された。

５．考察

代表的な攻撃を挙げ，それぞれについて本認証

システムの安全性を考察する。

Brute-force 攻撃は，全てのキャラクタを片っ端から試す攻撃である。試作システムでは，1 枚のクイズ画像上に表示されるキャラクタは 300 体であるので，クイズ画像を例えば 3 枚用いることにより，確率を$(1/300)^3$に ，すなわち 1/9000000 程度の総当たり数を確保することができる。

Observation 攻撃は，不正者による正規ユーザの認証作業の覗き見である。本方式は正解キャラクタの位置が漏洩すると，耐性が完全に消失してしまう。正解キャラクタの位置を正規ユーザのみが知っている何らかの法則にしたがって変更する，または認証動作を覗かれてもマウスのクリック位置が分からないようにするなどの方策を施す必要がある。

Educated Guess 攻撃は, 不正者が正規ユーザに関する情報を推測し，なりすます攻撃である。不正者が正解キャラクタを推測することができると，認証フェーズのクイズ画像から正解キャラクタの位置が特定されてしまう。よって，ある程度の頻度で登録フェーズを再実行してもらい，正解キャラクタを変更してもらうなどの工夫が必要となる。正解キャラクタを探すという行為はゲーム感覚であるため，登録フェーズの再実行はパスワードの変更などと比べ，ユーザが負荷を感じる度合いが少ないのではないかと期待される。

Intersection 攻撃は複数のクイズ画面の比較を行い，その差異を見出すことで画像パスワードを破る攻撃である。本システムにおいては，毎回の認証におけるクイズ画像は正解キャラクタもおとりキャラクタもその位置が全く変化しないため，Intersection 攻撃には耐えることができる。

６．まとめ

人間の特性を活用してユーザ認証を簡便にする一つの試みとして，経験による想起の容易さを利用した認証方式を提案した。一例として，本方式を画像認証システムに応用し，プロトタイプの実装を行った。まだ基礎実験の段階ではあるが，実験結果より本認証システムの可用性が示された。

謝辞

記憶に関し，静岡大学情報学部漁田武雄教授にご教授を頂きました。ここに謝意を表します。

参考文献

[1] Rachna Dhamija，Adrian Perrig：Déjà Vu：A User Study Using Images for Authentication，9th Usenix Security Symposium, pp.45-58 (2002)

[2] 高田哲司，小池英樹：あわせ絵：画像登録と利用通知を用いた正候補選択方式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)

[3] 小池誠，中村逸一，曽我正和，田窪昭夫，西垣正勝：ユーザの生活履歴を用いた認証方式，コンピュータセキュリティシンポジウム 2003 論文集，pp.1-6 (2003)

[4] 太田信夫，多鹿秀継 編著：記憶研究の最前線「5 章 非言語情報の記憶，2 節視覚的記憶の特性」，pp.102-114，北大路書房 (2001)

[5] 藤井俊勝：記憶を画像で見る，第 6 回若手研究者のための薬理学セミナー (2003)，http://www.banyu-zaidan.or.jp/symp/yakuri/img/fujii.pdf

[6] 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/

[7] Martin Handford(著)，唐沢 則幸 (翻訳)：新ウォーリーを探せ！，フレーベル館（2000）

[8] けらちん：ほそ目の CURSOR（キャラクタ素材），http://earth.endless.ne.jp/users/keira/

[9] Hermann Ebbinghaus ： Memory ： A Contribution to Experimental Psychology，Classics in the History of Psychology (1885) http://psychclassics.yorku.ca/Ebbinghaus/