パスワードとの闘い - パスワードなし認証システムの運用報告

増井 俊之 †

† 慶應義塾大学 環境情報学部
〒 252-8520 神奈川県藤沢市遠藤 5322

masui@pitecan.com

あらまし　計算機やサービスを使用する際の個人認証の手段としてパスワードが広く使われているが、パスワードは忘れやすいうえに安全な運用が難しいという問題がある。使い方を忘れて困ることがなく誰でも簡単に使える認証手法として、エピソード記憶にもとづく画像認証手法を提案し、数年にわたり良好な運用実績を得ている。このような「なぞなぞ画像認証」手法について述べる。

Fighting with Passwords - Lessons Learned from Password-free Authentication Systems

Toshiyuki Masui†

†Keio University
5322 Endo, Fujisawa, 252-8520 Japan

masui@pitecan.som

Abstract　Passwords are widely used for identifying users on various computer systems and Internet services. However, password-based authentication systems are far from ideal, since passwords are hard to remember, difficult to enter without a keyboard, vulnerable to attacks, and easily stolen. Various alternative authentication methods have been proposed, but they are still not as popular as password-based systems.

We have constructed various authentication systems which do not force users to remember passwords, and conducted experiments in the real world and on the Web for more than five years. In this paper, we present the advantages and disadvantages of the methods, and discuss the hope to the ideal authentication method in the future.

1　はじめに

計算機やサービスを使用する際の個人認証の手段としてパスワードが広く使われているが、パスワードは認証手段として多くの欠陥を持っている。記憶しやすいパスワードは簡単に推測されてしまうので、ランダム性が高いものでないと充分な強度を得ることはできないが、推測が困難なパスワードは記憶も困難であるから、書留めたりする必要があり、漏洩の危険が多くなってしまう。充分な記憶力や情報管理能力のある人でないと安全に運用することはできないし、文字入力装置が必要であるからユビキタスコンピューティング環境ではうまく使えない場合も多い。

パスワードを用いないで個人認証を行なう方法として、カードや鍵などの装置を用いる方法

や、指紋や光彩のようなバイオメトリクスデータを使う方法があるが、認証装置は携帯が面倒であり紛失/盗難の恐れがあるし、バイオメトリクスデータを利用する場合は高度なセンサが必要であるうえに、怪我や病気で使えなくなる可能性があり、何か問題が発生しても変更が不可能だという本質的な問題がある。

特殊な装置を用いずに安全な個人認証を行なうためには、個人の頭の中のみに存在する情報を使う方法が、現状では最も簡便かつ安全であると思われる。パスワードもこのような手法の一種であるが、情報の型式が脳で記憶/処理しにくいことが問題である。忘れる可能性が低く、外部から推測しにくいような脳内情報を認証に用いることが望ましい。人間の長期記憶は、個人の体験と関連した「**エピソード記憶**」と、学習して覚える「**意味記憶**」に分類されると言われている。学校で習う知識やパスワードは意味記憶であり、思い出すのに苦労したり忘れてしまうこともあるが、体験にもとづくエピソード記憶は年月を経ても忘れる可能性が低いし、個人体験は読み取ることもコピーすることもできないので安全に運用しやすい。エピソード記憶にもとづく「なぞなぞ問題」への回答で認証を行なうことにすれば、忘れる可能性が低く安全な認証を行なえる可能性がある。

2　なぞなぞドア

エピソード記憶を利用する認証システムとして、図1のようにオフィスの入口に実装した「なぞなぞドア」を実装した。問題を表示する計算機とディスプレイがオフィス内部に置いてあり、回答用のテンキーがドアの外側に貼り付けてある。

なぞなぞ認証の手順は以下のようになる。

1. システムがなぞなぞ問題と回答候補を表示する
2. 正しい回答をユーザが選択する
3. 1, 2 を何回か繰り返す
4. 正答率により認証の成否を判断する

なぞなぞ問題としては、認証を解く人間にとっては回答が容易であるにもかかわらず他人にとっては回答が困難であるようなものを用意する。たとえば「前回の合宿の場所は?」という問題に対して「伊豆」「蓼科」「軽井沢」などの候補を表示する。計算機ディスプレイには通常は案内情報が表示されているが、テンキーの「*」キーを押すと図 2 のようななぞなぞが表示される。

図 1: なぞなぞドア

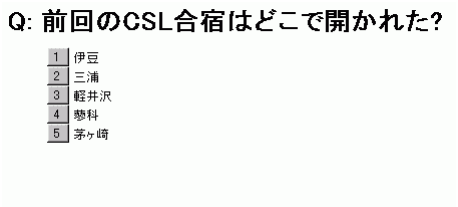

図 2: なぞなぞ問題の例

テンキーで回答すると次の問題が出題され、すべての問題に正答するとドアの電気錠が開く。

2.1　なぞなぞドアの運用経験

入室に必要なカードを忘れた場合でもなぞなぞを解くことにより認証を行なうことができるのは便利であった。電気錠の外側にあるトイレに行くとき入室カードを持っていくのを何度か忘れたことがあったが、特別なパスワードや認証装置を使わなくても再入室できたのはありがたいと感じられた。

なぞなぞドアをオフィスの入口に設置していたが、あまり好評ではなかったため一月ほどで撤収することになった。テキストを読んで / 内容を理解して / 5 個の選択肢を読んで / 内容

を理解して / 正しいものを選んで / ボタンを押すという操作は時間がかかるし頭を使う。また、なぞなぞの作成もあまり簡単ではないという問題も判明した。

3 画像を利用した認証

テキストを読んで理解してから正しい回答を選ぶのに時間と負荷がかかることがなぞなぞドアの最大の問題点であったため、テキストのかわりに画像を利用する手法について検討した。写真はエピソード記憶と結び付いていることが多いし、また、画像の特徴を利用した手法を利用することによって文字入力を使わない認証が可能となるため、画像を利用した各種の認証手法が提案されている。特に、強いエピソード記憶と結び付いており、忘れる可能性がほとんどない画像を用いて、簡単な選択をさせることにより認証を行なう方法が良いと思われる。

3.1 画像選択による認証

似たような画像を複数枚提示し、自分に関係する画像を選択するという操作を繰り返すことにより認証を行なうシステムを試作した。図 3 は、Firefox の拡張機能 Greasemonkey を利用することにより、画像選択によって Google の SNS システム「Orkut」へのログインを可能にしたシステムである。パスワード入力画面において複数の画像を表示し、自分に関係ある画像を選択することを何度か繰り返すと自動的にパスワード枠に正しいパスワードがコピーされ、ログインが可能になる。

正しい画像選択を行なうためには、正解画像をすぐに選択できること及びそれ以外の画像がまぎらわしいことが重要である。図 3 では左下の運動会の画像が正解画像である。この画像を選んだ時点では、この写真が自分のものであるという記憶が確かであったが、数年経過した後では記憶があまり確かとはいえなかった。この場合のように、自分撮影した写真でも時間がたつと状況を忘れてしまう可能性があるし、何度

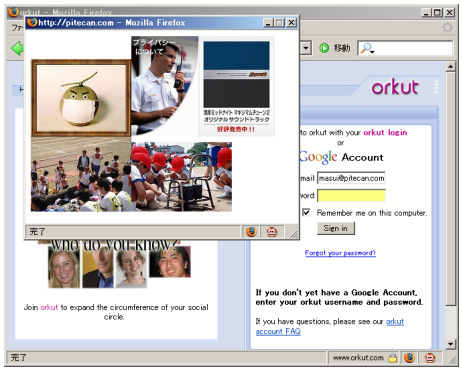

図 3: 画像選択による認証画面

も選択を繰り返すのには時間がかかるという問題もあった。

4 なぞなぞ画像認証

複数画像から選択する手法は問題が多いため、自分の強いエピソード記憶に結び付いた画像を使いつつ、その画像に関する質問をなぞなぞとして出題し、正解を選ばせるという方法を実験した。

図 4 は著者が運営する書籍情報共有サイト「本棚.org[1]」でこの認証手法を採用した例である。本棚.org ではユーザは「本棚」に書籍を登録してコメントなどを書き込むことができるようになっているが、認証を設定した場合は画像認証を解かなければ書込みができないようになっている。

図 4: 本棚.org の認証画面

本棚.org では、登録した複数の画像に対してテキストの答を複数個ずつ用意し、各画像に対

[1] http://hondana.org/

応したテキストを選択したときだけ認証に成功するようになっている。図 4 において、「小野」「高橋」などをクリックして選択した後数秒待つと、認証に成功して図 5 のような通常の書込み画面が出現する。

図 5: 認証成功後の画面

4.1　画像の登録手順

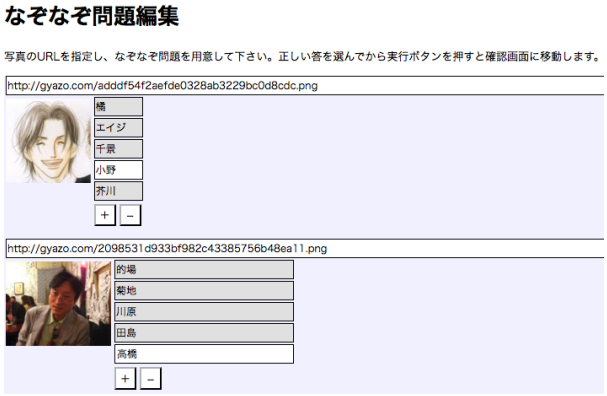

図 6: なぞなぞ問題作成

本棚.org のユーザは図 6 のような画面で認証用画像と選択枝を登録する。どのような画像と選択枝を利用してもかまわないが、ユーザのエピソード記憶に深く関連した画像と選択枝を利用すると忘れる可能性が低くなる。

ユーザの記憶に関連した画像としては、ユーザのデジカメ画像や、Web 上から捜してきた画像を利用するのが楽である。捜した画像を本棚.org に登録するための手間を小さくするため、計算機画面に表示された画像をネット上にすぐにアップロードできるようにするための「Gyazo[2]」というシステムも提供している。Gyazo アプリケーションを起動すると計算機画面の一部を切り出すためのカーソルが表示され、画面上でマウスをドラッグして領域を指定すると指定した範囲の画像が Gyazo.com にすぐにアップロードされ、図 6 の認証画像として利用できるようになる。

[2]http://Gyazo.com/

4.2　なぞなぞ画像認証の特徴

本手法は以下のような特徴を持っている。

- **認証を解くのが簡単**
  正答をクリックするだけでよいので処理が速い。またキーボード以外の入力装置を利用しやすい。
- **問題作成が比較的容易**
  デジカメが広く普及している現在、忘れる可能性が低い画像を選択は比較的容易である。
- **偽答の作成が容易**
  同カテゴリに属するテキストを偽答として用意しやすい。たとえば正答が「大阪」のときは「神戸」「京都」のような偽答を簡単に作れる。
- **強度の調整**
  画像と選択枝の選び方により、認証強度を調整したり、特定グループの人には解けるような問題を設定することができる。CAPTCHA[9] のかわりに利用することもできる。
- **他人との利用**
  グループ内で共有されている知識を利用すれば、問題や回答をあらかじめ伝えることなく他人と共用することができる。
- **テキスト問題の利用**
  テキストを画像化することにより、「母親の旧姓は?」のような典型的なチャレンジ問題も利用できる。

4.3　なぞなぞ画像認証の運用実績

本棚.org では 2 年以上なぞなぞ認証を運営しており、何人ものユーザが画像を登録して利用

している。ユーザが登録した認証画像と問題の例を図 7 に示す。簡単な問題を設定しているユーザもいるが、解くのが難しい問題を設定しているユーザが多い。

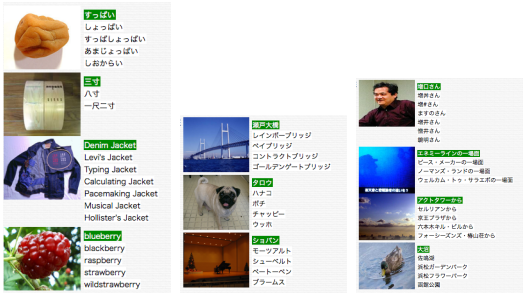

図 7: なぞなぞ問題の例

認証を必要と考えるユーザは多いと思われないし、画像を登録するのに手間がかかるためか、画像認証を利用しているユーザは多くはないが、一度画像認証を使いはじめたユーザはその機能を使い続けているようである。認証を解くための手間が小さいことの証明になっていると考えられる。

5 画像認証プラグイン

なぞなぞ画像認証を本棚.org 以外のサイトでも利用できるようにするために、一般的なパスワード入力画面を拡張して画像認証を可能にする仕組みを作成して IQAuth.com で運用している。Web ページにパスワード入力画面があるとき自動的に画像認証画面を表示し、選択した画像にもとづいて文字列を生成してパスワード枠にコピーする。正しい選択枝を選んだときに生成される文字列をパスワードとして利用することにより、ログインが可能になる。

IQAuth は Firefox の Greasemonkey 拡張機能で実装されている。IQAuth.com でユーザが登録した画像および選択枝は画像認証を行なうための JavaScript プログラムとともにブラウザに記録される。記録されるプログラムは画像と選択枝から文字列を生成するだけなので、どの選択枝が正しいパスワードを生成するのかはわからない。また、認証画像や選択枝を選ぶ操作はすべてブラウザ上で動作する JavaScript で実行されるため IQAuth.com との間で通信は行なわれず、画像や選択枝の情報が IQAuth.com に漏れる心配はない。

IQAuth を利用して mixi にログインを試みている様子を図 8 に示す。図 3 の場合と同様に、パスワード入力画面で本棚.org と同じような画像認証画面が表示される。

現在の実装では、なぞなぞ認証プログラムはブラウザに記録されるようになっているため異なる計算機やブラウザで利用することはできないが、生成した JavaScript を安全な方法で共有する仕組みを利用すれば共有は可能である。

図 8: mixi ログイン例

6 関連研究

これまで提案されている画像認証手法は、(1) 画像内の点を記憶しておき、それを指定するもの [2][5][10]、(2) 複数の画像を提示し、その中から選ぶもの [1][3][4][6][7][8]、(3) 画面上に秘密の絵を描くことにより認証するもの、に分類される。(1) の場合、画像内の特定の点を覚えておくことは難しいし、誰もが同じような点を選びがちだという問題がある。(2) の複数画像から選択する方式は、画像を大量に用意する必要があるし、何度も利用しているうちに混乱してくることも多い。(3) は描く絵を忘れてしまう可能性が高いし、操作が面倒である。

7 議論

画像とテキストを併用するなぞなぞ認証は、関連研究で述べたシステムに比べると多くの利

点を持っているが、ここでは本方式の問題点などについて議論する。

- **登録の面倒さ**
  なぞなぞ問題を考えて登録する手間はパスワード登録に比べるとかなり大きい。長い期間にわたり利用することを考えると初期投資は意味があるのだが、登録をさらに簡単にする工夫は必要であろう。
- **安心感の不足**
  なぞなぞ画像認証では、認証画面においてすべての情報が見えるようになっているうえに、ユーザにとっては画像も回答も自明であるから、「自分以外の人でも簡単に解けてしまうのではないか?」という不安を感じてしまうことが多い。ある情報を自分だけが知っていると確信することは難しい。問題を解くことが他人にとってどの程度難しいかを直感的に知る工夫が必要である。
- **強度について**
  なぞなぞ問題の数と選択枝を多くすれば、4 桁暗証番号と同程度の強度を持たせることは難しくないが、銀行口座の管理のように、本当に重要な情報の管理に利用するのは危険であろう。本棚.org のような Web サービス程度であれば、認証を破られた場合の被害は大きくないので、簡単に認証ができ、パスワードを忘れる心配のないなぞなぞ認証は有効である。
- **覗き見攻撃への耐性**
  画像から回答を選ぶ作業は見られないようにする必要がある。作業を見られても危険が少ないような画像認証方法も存在する [11] が、これらの方式ではユーザがかなり頭を使う必要があるので、頻繁に利用する操作には向いていない。

  パスワード入力画面において伏字を利用するのはユーザビリティの点で有害であるという意見[3]もあるほどなので、認証が必要な場所では物理的に覗き見攻撃ができないような工夫をするのがよいであろう。たとえばユビキタス環境で画像認証を利用したい場合、認証を行なおうとする人間以外には画像が見えないような装置を利用するとよいだろう。

[3] http://www.useit.com/alertbox/passwords.html

8 結論

パスワードにかわる認証手法として、エピソード記憶にもとづく各種の認証手法を実験を行なった結果、忘れる可能性が小さい画像を提示し、それに関連するテキストを選択するという手法が有効であることを検証した。問題を作成する手間及び安心感の問題についてさらに検討を加える予定である。

参考文献

[1] Dhamija, R. and Perrig, A.: Déjà Vu: A User Study Using Images for Authentication, *9th Usenix Security Symposium* (2000).

[2] Mininova Labs: Passclicks. http://labs.mininova.org/passclicks/.

[3] Mnemonic Security Limited: Mnemonic Guard. http://www.mneme.co.jp/.

[4] Passfaces Corporation: Passfaces. http://www.realuser.com/.

[5] SFR Software: visKey. http://www.sfr-software.de/cms/EN/pocketpc/viskey/.

[6] Sobrado, L. and Birget, J.-C.: Graphical Passwords (2002). http://rutgersscholar.rutgers.edu/volume04/sobrbirg/sobrbirg.htm.

[7] Takada, T. and Koike, H.: Awase-E: Image-Based Authentication for Mobile Phones Using Userrsquos Favorite Images, *Proceedings of the 5th International Symposium on Mobile Human-Computer Interaction (MobileHCI 2003)*, Lecture Notes in Computer Science, Vol. 2795, Springer, pp. 347–351 (2003).

[8] Vidoop LLC: Vidoop. http://vidoop.com/.

[9] von Ahn, L., Blum, M. and Langford, J.: Telling humans and computers apart automatically, *Communications of the ACM*, Vol. 47, No. 2, pp. 56–60 (2004).

[10] Wiedenbeck, S., Waters, J., Birget, J.-C., Brodskiy, A. and Memon, N.: PassPoints: Design and Longitudinal Evaluation of a Graphical Password System, *International Journal of Human-Computer Studies*, Vol. 63, No. 1-2, pp. 102–127 (2005).

[11] Wiedenbeck, S., Waters, J., Sobrado, L. and Birget, J.-C.: Design and Evaluation of a Shoulder-Surfing ResistantGraphical Password Scheme, *Proceedings of Advanced Visual Interfaces (AVI2006)*, pp. 177–184 (2006).