

安全で使いやすい認証方法

計算機にログインしたり、Web 上のサービスを利用したりするとき、ユーザーを認証する方法としてはパスワードがひろく使われています。

簡単なパスワードはすぐに破られてしまうので、安全のためには長い複雑な文字列を利用する必要があります。しかし、長い文字列は記憶するのも入力するのも難しく、なんらかの方法で盗まれてしまえば一巻の終りです。

最近パスワード解読技術が発達したため、意味のある文字列の多くはパスワードとして不適當になり、簡単には推測できないパスワードを設定しなければならなくなりました。しかし、そのようなパスワードは本人にとっても憶えにくいので、けっきょくはどこかに書き留めておいたりすることになり、かえって危険です。

私自身も、オフィスのイントラネットへのログインのためのパスワードの設定に苦労しています。どんな文字列を設定しても、“そのパスワードは単純すぎる”とシステムに怒られてしまうのです。最近意味のある文字列を憶えるのを断念し、ASCII キーボードをピアノの鍵盤に見立てて何かフレーズを弾いたときの文字列をパスワードとする (A、S、D、F……をド、レ、ミ、ファ……とみなしてフレーズを弾く) ことでようやく解決しました。

だいぶ前になりますが、2001 年 7 月号で、パスワードによる認証の問題点を解決する“なぞなぞ認証”というシステムを紹介しました。これは、世の中でひろく使われているパスワードの代わりにクイズ問題を用いて認証するものです。その後、2002 年 1 月号では、クイズ問題の代わ

りに画像を使う“画像なぞなぞ認証”を紹介しました。こちらは、複数の画像のなかから自分が見たことのあるものや自分が撮った写真を選び、本人かどうかを認証しようというシステムです。適当に決めたパスワードはすぐに忘れてしまう可能性がありますが、自分が撮影した写真や印象深い画像は頭に残りますし、他人には窺い知れない画像を手軽に使えるので、認証手法として有効なはずで

このところ、画像を認証に利用するさまざまな方法が考案されています。今回は、そのいくつかを紹介します。

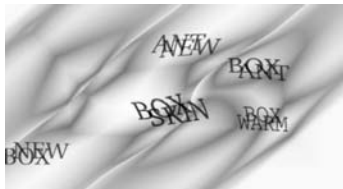
認証に画像を使う利点

個人の認証には、“その人が何を持っているか”よりも、“その人が何を知っているか”“その人に何ができるか”という情報を利用するほうがよいのは明らかでしょう。旧くから使われている鍵やメンバーズカードなどは紛失や偽造のおそれがありますから、信頼性が必要な場合は、クレジットカードや銀行カードのようにサインや暗証番号を併用するのが普通です。それにもかかわらずカードの不正利用があとを絶たない現状は、“持ち物”をベースとした認証があまり有効ではないことの証明といえるでしょう。

最近、指紋や虹彩などのパターンで個人を特定する手法が実用化され、注目を集めています。しかし、身体的特徴といえども人間の持ち物に違いはないので、つねにコピーや盗難 (!) の危険性があります。

これらにくらべると、脳内情報のコピーや盗難ははるかに困難ですから、脳内に蓄えられた知識や技能を認証に利用することは十分に意味があると思います。パスワード認証は脳内情報を使う点はいいのですが、有効なパスワード

図 1 CAPTCHA の利用例



を脳内に長期記憶として蓄えるのがひどく難しい点が問題だといえます。

人間の脳は、画像や音声を扱うパターン情報処理は得意ですが、単純計算やシンボル処理はどちらかといえば不得手です。したがって、パスワードに使われるような意味のない文字列の代わりに人間のパターン処理/記憶能力を活用すれば、より安全な認証が実現できると考えられます。

人間のパターン処理能力の活用

人間は、画像中の文字列を苦もなく読み取ることができますが、機械で文字列を認識するのは困難です。この事実を利用し、人間と機械を区別して扱う CAPTCHA (Completely Automated Public Turing Test To Tell Computers and Humans Apart)¹[2] というシステムが注目を集めています。このシステムでは、ユーザーがサービスを利用しようとする時図 1 のような画面を表示します。人間であれば、ここにどのような文字が表示されているかを簡単に読み取れますが、パターン認識による文字列の抽出はかなり難しいので、“bot”などのソフトウェアによる自動ログインを防ぐことができます。

このような画像を生成するため、カーネギーメロン大学の GIMPY² や、これを簡略化した ez-gimpy³ というシステムが開発されています。一方、カリフォルニア大学バークレイ校では、これを破るソフトウェアが開発されたそうです⁴。

計算機によるパターン認識が不可能な CAPTCHA 画像を生成できれば認証システムとして有用ですし、逆に、どんな CAPTCHA 画像でも認識するソフトウェアが開発されれば認識技術の進歩ということになり、どちらに転ん

1 <http://www.captcha.net/>

2 <http://www.captcha.net/captchas/gimpy/>

3 <http://openanonymity.sourceforge.net/HTML/scripts/ez-gimpy/ez-gimpy>

4 http://www.berkeley.edu/news/media/releases/2002/12/10_gimpy.html

図 2 PIX の問題例



でも成果が得られるのがおもしろいところです。

GIMPY の出力した文字列を計算機が認識できれば認証をパスしてしまいますが、人間のさらに高度な情報処理能力を利用して人間かどうかを判断する PIX⁵ というシステムも開発されています。PIX では、図 2 のような複数の画像がユーザーに示され、これらの画像に共通する単語(この例では“baby”)を答えると人間であることが証明されます。

人間のパターン記憶能力の利用

人間は、記号を憶えるよりも画像パターンを記憶するほうが得意です。とくに、印象的な場所や人などに関しては“エピソード記憶”として長期記憶となるため、簡単に忘れることはありません。

このため、文字列をパスワードとして利用する代わりに、人の顔や風景などの画像をパスワードとして使えば、パスワードを忘れるようなことは起こりにくくなるはずですが。

近年、このような手法を用いた個人認証手法がたくさん考案されています。以前に紹介したものも含め、これらの画像認証手法を以下に紹介します。

画像を用いた個人認証手法

Déjà Vu

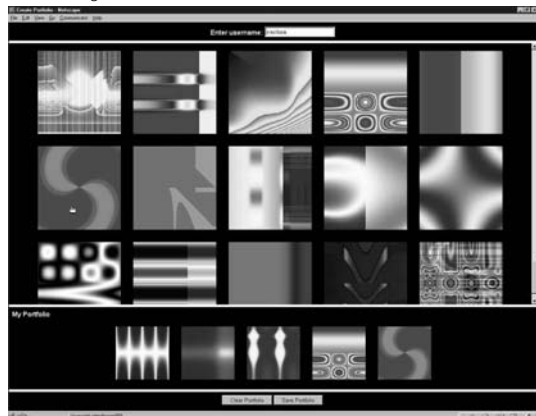
カリフォルニア大学バークレイ校の Adrian Perrig 氏と Rachna Dhamija 氏が開発した Déjà Vu というシステム⁶[1] は、画像を認証に利用した先駆的なシステムです。

このシステムでは、たくさんの画像のなかからユーザーがあらかじめ選択した任意の画像を用いて認証をおこないます。ユーザーは、計算機によって生成された何千枚もの画像のなかから、パスワードの代わりに“pass portfolio”

5 <http://www.captcha.net/captchas/pix/>

6 <http://www.sims.berkeley.edu/~rachna/dejavu/>

図3 Déjà Vu のログイン画面



と呼ばれる 5 枚の画像をあらかじめ選んでおきます。ユーザーがコンピュータにログインしようとする時、コンピュータはその 5 枚の画像を含む 25 枚の画像を提示し、ユーザーがそのなかから正しい 5 枚を選択できればログインを許可します。好きな画像は文字列よりも覚えやすいので、このような方法がうまく働くということです。

RealUser

Déjà Vu では、人工的に生成された画像のなかから自分が好きな画像を選択してパスワード代わりに利用します。しかし、好みの画像とはいえ、人工的なものを憶えておくのはそれほど簡単ではなさそうです。

これに対し、RealUser⁷では人間の顔の画像をパスワードとして利用します。たとえば、図4の5人の顔を“Passface”として記憶しておき、図5のような画面で自分の Passface を選択する操作を繰り返すことで Déjà Vu と同様の認証をおこなう仕組みになっています。

最初は、見知らぬ人の顔を 5 人ぶんも憶えられるものかと思いましたが、2~3 度練習しているうちになんとなく親近感が湧いてきて、すぐにみつけれられるようになりました。

私は人の顔を憶えるのが得意なほうとはいえませんが、それでもデモを試したかぎりではミスすることなく Passface を選びだせました。やはり、人間には生得的に顔を見分ける能力が備わっているのでしょう。

Passface として記憶した顔は、目で見ればすぐに認識できますが、どのような顔を言葉で表現したり、その顔を

7 <http://www.realuser.com/>

図4 記憶する 5 人の顔



図5 問題の例



紙に描いたりするのは普通の人にはかなり難しいでしょう。ですから、うっかり人に教えたり、紙に書いたりして秘密が漏れるようなことがなくなります。

ニーモニック認証

システムが提示した顔を憶えるよりは、ユーザー自身がよく知っている人や風景の写真や並べたほうがより効果的でしょう。ニーモニック セキュリティ⁸は、ユーザーが登録した画像を用いて Déjà Vu や RealUser と同様の認証をおこなうシステムを開発しています。同社の製品はソラン⁹や SKR テクノロジー¹⁰からシステムとして提供されています。また、NTT コミュニケーションズの CoDen というサービス¹¹のユーザー認証方式として使われているようです¹²。

図6は、ニーモニック認証のログイン画面の例です。64 枚の写真のなかに私が登録したものが 3 枚含まれており、

8 http://www.mneme.co.jp/index_net.html

9 http://www.sorun.co.jp/solution/se_nimo.html

10 <http://www.skr-tech.co.jp/nemeppt.htm>

11 <http://coden.ntt.com/>

12 <http://coden.ntt.com/service/coden-payment/answer.html#q6>

図 6 ニーモニック認証



図 7 画像なぞなぞ認証



これを選択すると認証が成功します。64 × 63 × 62 = 249,984 ですから、この画面を 1 回だけ利用する場合でも、そこそこの強度の認証がおこなわれることになります。

画像なぞなぞ認証

2002 年 1 月号で紹介した画像なぞなぞ認証システムでは、図 7 のような画像一覧の画面から自分に関係のある画像を選ぶ操作を繰り返すことによって認証をおこないます。

このシステムでは、自分の計算機内にある画像を自分に関係あるものとし、それ以外は Google のイメージ検索で取得した画像を利用します。このため、まったく推測できない画像の組合せのなかから自分の画像を選ぶこととなります。ニーモニック認証の場合は、最初から用意された写真やイラストを認証に利用するか、自分で写真などを登録して認証に利用する必要がありますが、なぞなぞ認証システムではユーザーが画像を選択する手間が少なくなっています。

図 8 GATESCENE



あわせ絵

Déjà Vu、RealUser、画像なぞなぞ認証システムの認証画面では、ユーザーが登録した画像がつねに認証画面中のどこかに表示されるため、何回も認証操作を繰り返していくうちに、“Intersection Attack”によって登録画像が判明してしまうおそれがあります。

このような問題を防ぐため、ソニーコンピュータサイエンス研究所の高田哲次氏は“あわせ絵”という手法を提案しています [4]。システムが提示した画像のなかにユーザーが登録したものがあれば、それを選択するのはほかのシステムと同じですが、あわせ絵では、提示される画像のなかに登録した画像が含まれないことがあります。その場合、ユーザーは選択すべき画像がない旨を回答し、これを繰り返すことで認証をおこないます。あわせ絵にはこのような特徴があるため、Intersection Attack を防ぐことができます。

すこし加筆しました

GATESCENE

富士通ソーシャルシステムエンジニアリングの鹿島一紀氏は、画像の位置情報を利用した“GATESCENE”という認証手法を開発しています [3]。GATESCENE の認証画面では図 8 のように暗証番号に加えて画像が表示されるようになっており、数字や記号だけを使う普通の認証方式に加えて、画像の位置も認証に利用できるようにしています。

たとえば、“1537”などの暗証番号を使う代わりに、“1りんご 3 パナナ”のように絵の場所と番号を併用したりすることができます。

意味のない数字を暗記しておくのは難しくても、画像情報と組み合わせれば、自分だけに分かる有効なパスワードが憶えやすくなるでしょう。

画像の特定の部分指定

Microsoft の Darko Kirovski 氏は、詳細な画像の特

定の部分をいくつか選択することによって認証をおこなうシステムを提案しています。詳細は不明ですが、ここまでに紹介したシステムとは異なり、詳細な画像を1枚だけ使うのが特徴で、その画像上のいくつかの特定の点を正確に指示することによって認証をおこなうようになっているようです。

おわりに

今後、新たな認証手法がいろいろと開発されるにしても、パスワードによる認証がなくなることはなさそうです。あらゆるシステムを画像認証にすることは不可能でしょうし、画像を用いる方法は目が見えない人には使えないという大きな問題があります¹³。いうまでもなく、こういった条件はユーザーごとに異なりますから、できるかぎり多様な認証手法を用意することが必須といえます。

その場合、今回紹介したようなさまざまな認証手法をパスワード文字列に変換するソフトウェアや機器があれば、より汎用的に使えるのではないかと思います。私自身も、画像認証をはじめとする各種の認証操作をパスワード文字列に変換する装置を作りたいと考えています。

(ますい・としゆき 産業技術総合研究所)

[参考文献]

- [1] Rachna Dhamija and Adrian Perrig, “Déjà Vu: A User Study Using Images for Authentication”, In *9th Usenix Security Symposium*, August 2000
- [2] Luis von Ahn, Manuel Blum, and John Langford, “Telling Humans and Computers Apart Automatically”, In *Communications of the ACM*, Vol.47, No.2, pp.56–60, February 2004
- [3] 鹿島一紀「画像の位置情報による本人認証方式の研究開発 画像パスワード gatescene(ゲートシーン)」, 情報処理学会コンピュータセキュリティ研究会研究報告、Vol.10、2000年6月
- [4] 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、2003年8月

¹³ <http://japan.cnet.com/news/media/story/0,2000047715,20059708,00.htm>