インターフェイスの街角– マイ認証

増井 俊之

パスワード認証の問題点及びそれを解決する「なぞなぞ認証」について 2001 年 7 月号で紹介しましたが、なぞなぞ認証を使うためには専用のサイトを構築する必要があり、一般の Web ページでは使えないという問題がありました。普通のパスワード認証を採用しているサイトにおいて、なぞなぞ認証のような認意の自前の認証手法を利用できるようにする方法を開発したので紹介します。

パスワード認証の問題点

パスワードを利用する認証システムは、長い間広く使われているため、システムの構築手法についても安全性についても広い知見が蓄積されており、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の認証手法の定番になっていますが、ユーザーにとっては非常に使いにくいのが実情です。

辞書にある単語や固有名詞の組み合わせによるパスワードは比較的簡単に破られてしまうことがわかっているため、安全性を保つためにはランダムに近い長いパスワードを利用する必要があります。しかし長いパスワードは入力するのも大変ですし、そもそも頭の中に覚えておくことが困難ですから、結局どこかに書きとめておかなければならなくなり、かえってセキュリティの問題が広がってしまうことになります。最近のブラウザはユーザ名やパスワードを記録してくれるので、この機能を利用すれば Web 上のサービスでパスワードを入力する必要は少なくなりますが、パスワードを記憶したノートパソコンを盗まれてしまうと、あらゆるサービスに自由にアクセス可能になってしまうわけですから、かなり危険だということができます。

長くないパスワードの場合でも、サービスごとに異なるパスワードを使おうとするとすぐにパスワードを忘れてしまいますから、そのたびにサービス提供者への問合せが必要になります。パスワード認証システムの構築手法について実績がある場合でも、パスワードを忘れてしまった場合の処理のために無駄な手間やコストがかかってしまうことになります。また、パスワードと生体認証や別の装置を併用することによって利便性と安全性を両立させようというシステムもありますが、複数のシステムを組み合わせるとかえって問題が増えることもあるので注意が必要です。このような認証システムの様々な問題点については、画像認証システムを開発しているニーモニック社の國米氏が詳しく問題点を指摘しています[1] 。

とはいえ、パスワード認証方式は実装手法も攻撃手法も対処手法も枯れていますから、使い勝手については大きな問題があるものの、適切に運用される限りは安全だという認識があり、今後も広く使われていくだろうことは間違いありません。2001 年 7 月号で紹介したような認証手法や、ニーモニック社の提案する画像認証手法、「あわせ絵」システム [1] のように、パスワードよりも効果的と思われる認証手法はいろいろ提案されていますが、このような認証手法を採用するためにはシステム全体を作りかえる必要があるため、実際のサービスで採用するにはかなりの困難があります。認証システム全体を最初から実装するのは大変ですし、新しいシステムの場合はバグなどによるセキュリティホールが存在する確率は、パスワード認証シス

1 http://www.mneme.co.jp/data/thesis.html

テムのような枯れたシステムに比べるとはるかに高くなるでしょう。また、新しい認証システムに困惑するユーザーも多いでしょう。認証システムはサービスの中核ではありませんし、システムの発注者も作成者もこういう面倒は避けたいでしょうから、優れた認証システムについての知識があった場合でも「まぁ認証はとりあえずパスワードでいこうや」ということになるのは目に見えています。

原理的に優れた認証システムであっても、コストや危険が高くユーザーの反発を招く可能性のある認証システムが急に普及することは考えられません。

パスワード認証システムの有効利用

このように、パスワード認証システムは今後も長く使われ続けると思われるので、パスワード認証システムの使い勝手を向上させる方法について考えた方がよさそうです。前述のように、パスワードを記憶できないこととパスワードの入力に手間がかかることがパスワード認証方式の最大の問題点ですから、パスワードを直接記憶したり入力したりするのをやめてしまい、なんらかの別の手段でパスワードを生成して入力できるようにすれば使い勝手はかなり向上する可能性があります。自分だけが持っている知識や能力のような属性を、なんらかの方法で文字列に変換してパスワードとして利用すれば、パスワード認証システムを変更することなく、異なる認証システムを利用することができるようになるわけです。

例えば、指紋を文字列に変換するシステムがあれば、変換された文字をパスワードとして利用することにより、通常のパスワード認証を利用したサービスにおいて指紋認証を利用することができるでしょう。また、鍵の形状を文字列に変換するシステムがあれば、鍵を使ってサービスにログインすることができるようになります。

このように、パスワードを中間言語のようなものと考え、別の方法でパスワードを生成して利用することにすれば、自前の認意の認証手法をパスワード認証システムで利用できることになります。このようなシステムでは、ユーザーは実際のパスワード文字列について知る必要すらありません。

このような「中間言語方式」は様々な手段で実装することができます。特殊な操作によってパスワードを生成する USB 装置のようなハードウェアを利用することもできますし、特殊なマウス操作によってパスワードを生成するソフトウェアを利用することもできるでしょう。2001 年で紹介したような「なぞなぞ認証」も当然使えます。

Greasemonkey によるマイ認証

1 月号で紹介した Greasemonkey を利用すると、パスワード認証を利用している認意のサービスにおいて前述の方式を適用し、パスワード入力を自前の認証システムに置き換えてしまうことができます。

自前の認証を行なう CGI と、認証結果を取得する CGI スクリプトを用意しておき、以下を実行する Greasemonkey スクリプトから両者を呼び出します。

- password 属性をもつフォームをページ内検索する
- そのようなフォームがあれば新しいウィンドウを開き、自前の認証を実行する CGI を呼び出す
- 同時に認証結果を取得する CGI を動かし、得られた結果をフォームにペーストする

画像なぞなぞ認証の実装

図 1 の imagequiz.user.js というスクリプトを Greasemonkey にインストールして図 2 のように設定してから Mixi[2] にアクセスすると、パスワード入力テキスト枠の色が変化して、imagequiz.cgi が呼び出され、図 3 のようになぞなぞ認証画面が表示されます。5 個の画像が表示されていますが、このうちひとつだけが私に関係する写真か画像です。それをクリックすると選択するとまた別の写真が表示されるので、再度私に関係する写真をクリックします。これに 5 回連続成功するとパスワードがパスワード入力テキスト枠にペーストされます。

この操作において、ユーザーはキーボードにアクセスしていないにもかかわらずパスワードを要求するサイトにログインすることができたことになります。

2 http://mixi.org/

図 1　imagequiz.user.js - なぞなぞ認証呼出しスクリプト

```
// imagequiz..user.js
// $Date: 2006-01-25 14:44:53 +0900 (Wed, 25 Jan 2006) $
// Copyright (c) 2005, Toshiyuki Masui
// Released under the GPL license
// http://pitecan.com
//
// ==UserScript==
// @name ImageQuiz
// @namespace http://pitecan.com/MyPassword
// @replace <input type="password"> with user password
// @include http://*
// ==/UserScript==

function getpassword(te){
  // マイ認証用のウィンドウを開いてマイ認証を実行する。
  // authcgi でマイ認証を行なった結果を getcgi で取得する。
  // getcgi は認証が終了するまで待つ。timeout でタイムアウト。

  authcgi = "http://pitecan.com/MyPassword/programs/imagequiz.cgi";
  getcgi = "http://pitecan.com/MyPassword/programs/getpassword.cgi";
  timeout = 20000;

  d = new Date;
  id = d.getTime();
  w = window.open(authcgi+"?url="+encodeURIComponent(location.href)+
      "&id="+id,"","width=400,height=400");

  setTimeout(function(){ w.close(); },timeout);
  setTimeout(function(){ te.value = ''; },2000); // 最初にパスワードをクリヤ

  GM_xmlhttpRequest({
    method:"GET",
    url:getcgi+"?id="+id,
    onload:function(details){
      te.value = details.responseText;
    }
  });
}

inputs = document.getElementsByTagName("input");
for (var i = 0; i < inputs.length; i++) {
  te = inputs[i];
  if(te.type == "password"){
    te.style.backgroundColor = "#ffff80"; // マイ認証の色
    te.value = '';
    getpassword(te);
  }
}
```

画像上の操作を利用する認証

なぞなぞ認証の場合はクリック操作を 5 回繰り返すという手順があるので、無限に操作を繰り返せば偶然認証に成功することも考えられますが、どういう操作でログインするかということがそもそも不明である場合は他人が認証に成功することはほとんど不可能になるでしょう。

画像を選択を繰り返す認証ではなく、画像の上で行なったマウス操作によって認証を行なう方法を実装してみました。imagequiz.user.js を書き換えて image-

図 2　Greasemonkey の設定

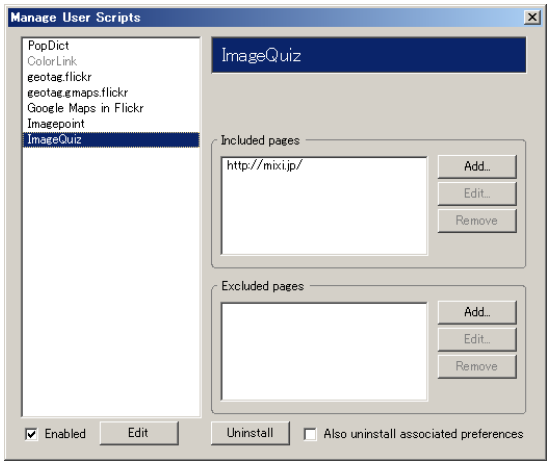
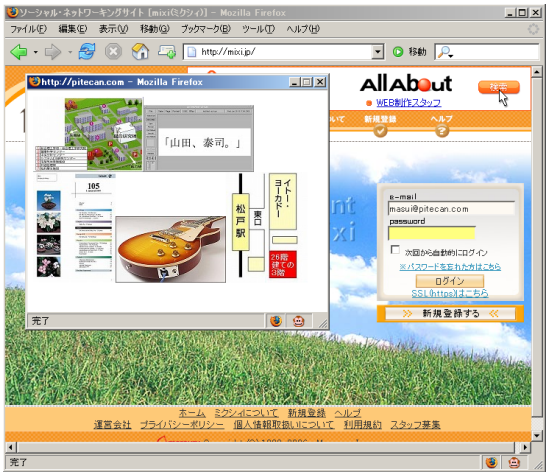


図 3　Mixi のログイン画面にアクセス



point.cgi を呼び出すようにした imagepoint.user.js を Greasemonkey に登録し、http://www.jal.co.jp/ にアクセスするとこれが呼び出されるようにします。

ここで JAL のサイトにアクセスすると図 4 のように 1 枚の画像が表示されます。写真があまりよくありませんが、これは越後湯沢駅にある新潟の酒の試飲システムで、いろんな酒を一杯 100 円で飲むことができるというものです。この画像の上でなんらかのマウス操作を行なうとパスワードが生成されて前述の例と同じようにパスワード入力枠にペーストされますが、どういう操作を行なえばよいかというてがかりが皆無であるため、知らない人がパスワード生成に成功する可能性はほとんどないといえるでしょう。銘柄を順に

クリックすればいいのかもしれませんし、「清泉」を連打すればいいのかもしれません。なぞなぞ方式に比べると操作を覚えにくく、忘れてしまう可能性は高いと思われますが、なぞなぞ方式より強くすることも弱くすることも簡単です。

図 4　JAL のログイン画面にアクセス

安全の工夫

今回の実装手法では、サーバから送られるパスワードを getpassword.cgi で取得しているため、タッピングなどによりパケットをモニタすればパスワードが判明してしまいます。ユーザーの操作をもとにローカルにパスワードを生成すればよいのですが、その場合はどういう操作によって認証が行なわれるのかがわかってしまいますし、画像なぞなぞ認証を実現することは困難です。パスワードを暗号化して送るという方法も考えられますが、パスワードをサーバのどこかに書いておく限り危険はなくなりません。実際に運用するにはもうひと工夫が必要でしょう。

楽しい認証

パスワードを思い出して使うという認証はあまり楽しいものではありませんが、画像なぞなぞ認証のように自分の能力や知識にもとづく認証は楽しいものにできる可能性があります。認証に使う写真を選ぶのは楽しい作業ですし、自分だけが解ける問題や技術を工夫するのも楽しいものです。知的なトリックを使うこともできますし、ゲーム的要素を持たせることもできます。自分だけが使える認証手法を考えるのは難しいかもしれませんが、覚えにくいパスワードを無理矢理設定させられることに比べればはるかに良いと私には感じられます。

パスワード認証では、入力しているところを他人から見られないように隠すのが普通ですが、見られてもわからないほどトリッキーな認証手法であれば、認証手順を人に見せて自慢することもできるでしょう。

認証手法は無限に考えられますが、誰にとってもベストな認証手法というものは難しく、楽しいもの/強力なもの/簡単なもの/面白いもの/など、場合に応じて適当な認証を利用することができます。たとえば以下のような認証手法が考えられるでしょう。

- 与えられた地名を地図上でクリックする。地名の知識が必要。
- 詰め将棋の問題を解く。将棋の実力が必要。
- 表示された楽譜を演奏する。楽器と譜読みの技術が必要。
- 聞こえる和音をそのまま弾く。絶対音感が必要。

パスワード認証の場合、認証は成功/失敗のふたとおりしかありませんが、知識や能力を問う認証手法の場合は知識や能力レベルに応じて認証レベルを変えることができるかもしれません。全問即答の場合は問題ありませんが、回答に時間がかかった場合はそれなりに注意してサービスを提供するとよいかもしれません。

おわりに

マイ認証システムの運用実績は長くありませんが、今回の方法を利用すると、実際に普段利用している様々なサイトで毎日有効性を実証できるため、各種の改善アイデアを出しやすいことを期待しています。新しいシステムの使い勝手を知るためには短期間の実験では不充分であり、実際に毎日のように利用してみるのが一番です。毎日様々な認証手法を利用していれば、より効果的な認証手法についての新しいアイデアがみつかる可能性が高くなるでしょう。

今回はソフトウェアによる実装だけ紹介しましたが、デスクトップマシンのような据え置きシステムで利用する場合は、自宅の鍵の形状をパスワードに変換する装置のような、特殊なハードウェアの利用も実用的かもしれません。様々なハードウェアやソフトウェアによる認証手法を実験していきたいと思っています。

[参考文献]

[1] 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, August 2003.