マルチメディア通信と分散処理　106－16
コンピュータセキュリティ　16－16
（２００２．２．１４）

グラフィックパスワードを用いたWeb個人認証システムの設計

勝田 亮*　　平石 広典　　溝口 文雄

東京理科大学 理工学部

概要

本論では個人認証方法について着目し、ユーザにとって負担の少ない簡単な認証方法としてグラフィックパスワードを用いた個人認証システムを提案する。本システムは、従来のテキストベースのパスワードに依存せず、ユーザが数枚の画像を示された画像群の中から選択することによって個人を認証することが出来るシステムである。画像を用いることにより、テキストパスワードを用いる場合のユーザへの負担を軽減させ、安全で簡単な認証方法を提供することが可能となる。また、本論ではシステム設計だけではなく、ユーザテストを行い携帯端末上での画像パスワードを用いた個人認証システムの有効性を示している。

Authentication System using Graphical password

Ryo Katsuta　　Hironori Hiraishi　　Fumio Mizoguchi

Faculty of Science and Engineering, Science University of Tokyo.

This pasper focuses Authentication System.We developed a authentication system using graphical password. This system authenticate user by choosing a images.This paper describe that graphical password is better for user than a character password.

1　はじめに

インターネットの普及により、我々の生活においてもインターネットサービスを利用する機会が増えてきた。オンラインショッピングや、オンラインバンキング、オンライントレードなどインターネットを介してさまざまなサービスを受けることが出来る。最近では、この類のサービスは携帯電話や、携帯端末などのインターネットに接続可能な小型デバイス向けにも提供されていて、いつでもどこででも簡単に利用できるようになった。この種の電子商取引サービスは、これからますます盛んになり、我々の生活に密着したものとなる。

現在、このようなサービスの利用者はたくさんのアカウントを持っている。しかし、ユーザはこのアカウントを覚えるのが大変なため、ほとんどのアカウント情報を同じにしてしまっていたり、誕生日や自分のパーソナルデータを使ってパスワードなどを設定している。

本研究では、こういった問題を解決するために、ユーザビリティーの面に最優先に考えて個人認証での問題解決策を提供する。Webサービスを中心とした、ネットワークサービスの個人認証を簡単かつ安全に行なえるシステムを提案する。また、携帯端末でも利用可能とし、携帯端末でのユーザビリティーも考慮し設計を行なっている。

2　本研究の背景と目的

本研究では、個人のアイデンティティーを識別する個人認証システムのユーザビリティーに着目した。一般的に認証方式には大きく分けて次の3つの種類がある。

1. 記憶による認証 (パスワード、暗証番号)
2. 持ち物による認証（Smart Card,IC Card）
3. バイオメトリックによる認証 (網膜、指紋)

*連絡先：東京理科大学理工学部経営工学科溝口研究室
〒278 千葉県野田市山崎2641　電話 (0471)24-7802

持ち物による認証では、銀行の ATM カードが一般的である。こういったカード類による認証では、カードだけでなく、暗証番号などの記憶による認証に依存するところが大きい。また、カード類を紛失したり、盗難にあうなどの問題もある。

バイオメトリックによる認証は、最近では盛んに研究されており、実用化されている。しかし、指紋や網膜の読みとり装置がまだ技術的にも普及していないため、高価であるのに加え、これらのデータはプライバシーに関わる情報であるので、管理にコストがかかり、こういった測定に抵抗を示すユーザも少なくない。

一般的に使われている記憶による認証は、簡単でコストが低いため一番使われている認証方法である。しかし、次のような重要な欠点を挙げることが出来る。

2.1 文字ベースアカウントの問題点

文字ベースのアカウント情報は以下のような安全性を低下させるいくつかの問題点がある。

- 記憶による負担
- 攻撃に弱い
- 第三者に漏洩する危険性がある
- 入力困難

パスワードは本来、自分の名前や、誕生日など個人情報を含まないのが好ましい。単語や、ユーザ自身に関する情報を利用することで、辞書検索によるパスワード解析が容易に出来てしまうためである。文字列や数字をランダムにした全く意味のない順列のものが好ましい。しかし、こういったパスワードはユーザにとって非常に覚えにくい。

そのため、ユーザはパスワードの記憶が困難なためにパスワードをメモに取り、メモを携帯しようとする。このメモが第三者に渡り、パスワードが漏洩してしまう危険性がある。また、文字ベースのパスワードでは具体化が可能である。誕生日や名前など具体的にして記憶しようとするため、他人と共有出来てしまう。実際、銀行の暗証番号を家族で共有したりする人が少なくない。そういった何気ない行為から秘密情報が漏洩する危険性が高い。アカウント情報が漏洩することで、ユーザに大きな損害が発生してしまう。

2.2 Web サービスの増加とアカウント管理の限界

インターネット上の Web サービスが増加すると、個人で利用する Web サービスの数も増加する。サービスの増加とともに、ユーザが記憶しておかなければならないアカウントの数も増大し、すでに個人では管理出来ないほとどのアカウント情報を持っているユーザがいる。

その結果、ユーザはアカウント情報を忘れないために異なるサービスのアカウント情報において、全く同じパスワードを他のサービスに設定する傾向がある。このことは、1 つのサービスのアカウント情報が漏洩することで、そのユーザが受けている他のサービスの利用が可能になることを意味する。

2.3 携帯情報端末の普及と m コマース

Web サービスを、携帯電話や PDA といった小型の携帯情報端末から利用することが多くなった。この種の携帯端末向けの電子商取引を総称して m コマース (モバイルコマース) と言う。しかし、携帯情報端末向けのサービスを利用するユーザのほとんどが、そのサービスを繰返し利用することが少ないことがわかってきた。その理由は、アカウント認証を行なうのが困難であるからである。小型情報端末の入力インタフェースは、テンキーによる入力か、ペン入力である。これらの入力インタフェースは習熟が必要で、あまり使い易いインタフェースであると言えない。したがって、認証時に必ず必要となる文字入力がユーザにとって負担となり、使いにくいのである。したがって、ユーザはサービスを利用しなくなってしまう。

以上述べたように、現在利用されている Web サービスでの一般的な認証プロセスはユーザビリティーが低いことが原因で安全性に問題がある。本研究では、これら問題に着目しユーザビリティーに優れた、セキュアな個人認証システムを設計・構築することを目的とする。

3 関連研究

3.1 DejaVu

DejaVu は、新しい認証インタフェースとして Rachna,Adrian らによって提案されている [1][2]。DejaVu システムはランダムアートと呼ばれる、特定のランダムシードから生成したランダム画像を用いて認証を行なう認証システムである。

ユーザはシステムが提示するおとり画像を含んだ画像集合の中から自分のパスワードとして設定されている画像を正確に選択することによって認証を行なうことが出来る。認証プロセスを文字入力から画像選択にすることによって、ユーザの文字列を記憶しなければならない負担を解消する。

しかし、DejaVu は認証インタフェースの提案であり、実際のサービスへの適応はされていない。

4 Web 個人認証システムの設計

本章では、Web 個人認証システムの設計ついて述べる。前章まで述べてきたように認証システムのインタフェースにはいくかの問題点がある。また、オンラインサービスがモバイル端末から利用されることにより認証機構もモバイル端末に対応しなくてはならない。これらを考慮しシステムの設計を行なう。

4.1 Web 個人認証システム

個人認証システムを設計する上で考慮すべき項目を挙げる。

1. 認証過程でのユーザの負担を軽減する
2. 分散したアカウントを一元管理
3. 現状のシステムを変更することなくサービスを提供する
4. PC 端末だけでなく、携帯端末でも利用可能

まず、認証インタフェースとしてのユーザビリティの向上をはかる。第 2 章でも述べたように、現状の個人認証技術ではユーザの負担となるところが多い。

したがって、本システムでは、文字ベースのアカウント情報から脱却し、ユーザの記憶に頼らない認証インタフェースを採用する。

次に、第 2 のシステム要件を満たすために、中間サーバ型のシステム構成を採用する。サービスの対象は HTTP ベースのサービスを対象とする。つまり、オンラインサービスなどの認証をすべて一括して扱えるようにする。Web メールや、オンライントレードなどのブラウザ上で行なえるサービスの認証を全て扱うようにする。

また、全てのサービスサーバの認証機関を再構築するのは莫大なコストとなるので、サービスサーバの認証機構を構築し直する必要がないよう設計する。これは中間サーバ型のシステムアーキテクチャとする。一種の Proxy サーバで、クライアントは、HTTP 経由の接続はこのサーバを介して接続を行なう。

第 3 に、携帯端末からの利用も可能とする。これは以上の 2 つの要件を満たすことで対応することが出来る。ユーザに負担を書けないユーザビリティ設計、Proxy サーバ型システムアーキテクチャを実現することで、携帯端末等にも対応することが出来る。

携帯端末である、携帯電話、PDA はすでにインターネットに接続することが可能で必要最低限の機能を持つブラウザが機器に埋め込まれている。本システムでは、インターネットに接続出来、ブラウザを内蔵するほとんどの携帯情報端末へサービスを提供することが出来る。

また、携帯電話のような劣悪なインタフェースでも、グラフィックパスワードの認証インタフェースを採用することで、文字入力の負担もなく、簡単にサービスを受けることが可能となる。

4.2 グラフィックパスワード

本システムでの認証インタフェースには、グラフィックパスワードを採用する。グラフィックパスワードは文字ベースのアカウントではなく、自分のパスワードとなる画像群を選択することによって認証を行なうものである。

本システムではランダムアートのアルゴリズムによって生成された画像を用いる [3](図 1)。

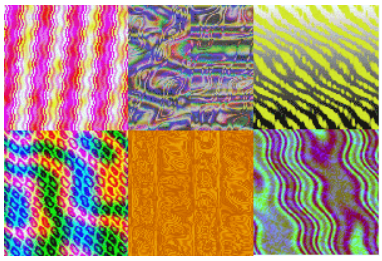

図 1: ランダムアート画像

この画像を 9 枚 1 組としてユーザに提示する (図 2)。ユーザはあらかじめ自分の 5 枚の画像群を設定したことがあり、自分のグラフィックパスワードがどういった画像であったか目にしたことがある。システムが提示する画像群には、ユーザが設定した画像群の中の順番的に一番はじめの画像が含めれていて、その他の画像はおとり画像として構成されている。その 9 枚の画像群の中からから自分の画像を 1 枚選択する。選択されるとシステムは、次のユーザの画像を含んだ 9 枚の画像群を提示する。また、この画像群からユーザは自分の 2 枚目の画像を選択する。これを 5 枚分繰り返す。選択した絵と順番が正確に選択されたならば、ユーザは認証される。

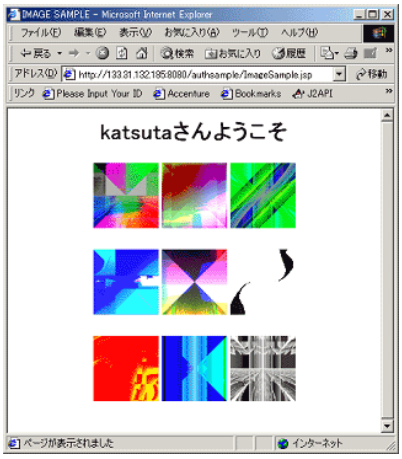

図 2: 認証画面

4.3 攻撃対策

0000 から 9999 までの 4 桁の暗証番号を、1 回で解く確率は 1/10000 である。銀行の ATM などは安全のため、3 回暗証番号を間違えると口座を凍結するなどの攻撃対策をしている。こういった、自転車のナンバーロックを開けるような攻撃を、ブルートフォースアタック (Brute force attack) と呼ぶ。本システムでは、9 枚の画像から 1 枚ずつ選択し、全部で 5 枚の画像を選択する。本システムの認証機構を 1 回で解く確率は、1/59049 となり、4 桁の暗証番号よりも安全である。本システムでも安全のため 3 回の画像選択を間違えるとユーザアカウントを凍結し、システム管理者の確認があるまでログインを受け付けない処理を行なう。

また、オブザーバアタック (Observer attack) と呼ばれる攻撃も考えられる。この攻撃は観察者による攻撃と呼ばれ、つまり、攻撃者は攻撃対象となるユーザの背後からログイン時の手の動きを観察する。そして、ユーザの手の動きから選択した数字を推測する攻撃である。これは、銀行 ATM などテンキーが固定されているものや、キーボードなど備え付けの入力デバイスを使用するシステムが攻撃を受けやすい。

本システムでは、この種の攻撃に対してはランダムレイアウトを利用することによって対応する。まず、ランダムレイアウトの機能として、おとり画像のランダム選択がある。サーバには、大量のランダム画像が登録されている。9 枚の画像群を生成する時に、ユーザの画像とおとり画像を大量の画像の中からランダムに選択する。したがって、ユーザ以外の人間から見ると毎回違う画像が表示される。また、9 枚の画像群の中のユーザの画像を表示する位置もランダムに決定する。したがって、ログイン毎にユーザの手の動きが変わるため、オブザーバアタックは不可能である。

4.4 Proxy サーバ型サービス

本システムでは、端末の型に依存しない、またどこからでもサービスを受けることが出来るために、サーバを中間サーバとすることでこの二つの要件を満たしている。

サービスが対象するのは HTTP プロトコル上での認証とする。したがって、クライアントは本システムのサーバを HTTPProxy サーバとして日常的に Web ブラウズを行なう。クライアントのブラウザは要求を Proxy サーバを通して実際のサービ

スを提供するサービスサーバへと送信される。通常のブラウザから Proxy サーバを設定するのは簡単で、設定項目に Proxy サーバの IP アドレスとポート番号を設定することで可能となる。

ブラウザを通して HTML 形式のファイルで画像とともにクライアントブラウザに返信するので、高機能なブラウザを持つ PC 端末はもちろん、あまり機能が充実していない携帯端末のブラウザで対応することが出来る。また、HTML 形式なので、現在普及している携帯端末であれば利用することが可能である。したがって、本システムは端末の機種に依存しないシームレスな認証サービスを提供することが可能である。

認証機構を Proxy サーバとして設けることにより、システム要件である、既存のサービスサーバの認証機構を再構築する必要がなくなる。Proxy サーバとして、サービスサーバのアカウント情報を登録し、本システムが提供する認証インタフェースによる認証をパスすれば、サービスサーバの認証は本システムが代行する。もちろん、サービスサーバの認証プロトコルが本システムの提供する認証プロトコルに対応していなければならない。したがって、既存のサービスサーバの認証機構を再構築することなく、サービスをユーザに提供することが出来る (図 3)。

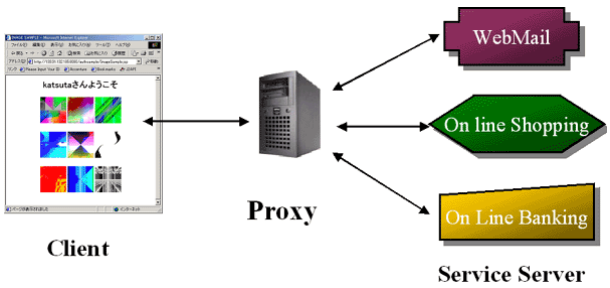

図 3: Proxy サーバ型サービス

この他にも中間サーバにすることで、複数のサービスサーバのアカウントを統一化出来たりすることでユーザの負担を軽減することが可能となる。

4.5 システム実装

本システムは、OS に FreeBSD 4.3 を用いて、Web サーバには Jakarta Tomcat3.2 を用いる。認証機構、Proxy 機構は全て Java にて記述されている。ブラウザとの通信に HTML 形式のファイルでやり取りを行なうため、JSP+Servlet を用いて実装している。図 4 に示すような処理を行なう。まず、ユーザが本サービスを利用するときは、端末のブラウザで Proxy 設定を行なう。Proxy 設定を行なったブラウザから接続要求があると、そのセッションにおいて本システムはユーザに認証を求める。ここで認証されなければ Proxy サーバとしても利用することが出来ない。

グラフィックパスワードによって認証が行なわれると、プロキシ機構へ認証機構がイベントを返し認証が取れたことを知らせる。認証が行なわれると、プロキシ機構はそのセッションにおいて接続を許可し、ユーザは接続が可能となる。

プロキシ機構はユーザの接続要求を常に監視している。ユーザがすでに登録されているサービスサイトに接続すると、登録されているサイトのアカウント情報を接続要求に付加しサービスサーバへ接続要求をリバインドする。これがシステムの代理認証となり、ユーザはアカウント情報を入力することなくサービスを受けることが可能となる。

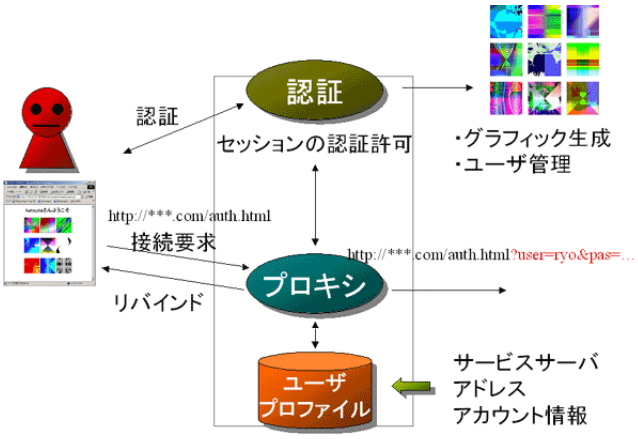

図 4: システムのフロー

5 評価実験

5.1 実験方法

実験 1 実験 1 では、ユーザにとってシステムが使いやすい認証方法であることを示すために、携帯電話端末上で行なったテキストパスワードと画像パスワードの認証時間の比較を示す。実験では、被験者に携帯電話を使いあらかじ

め指定した文字パスワード (3 文字から 7 文字) と画像パスワード (3 枚から 7 枚) の入力を行なってもらい、そのキーストローク時間を測定した。それぞれの被験者にそれぞれ 10 回づつ行なってもらった。この実験により、入力インタフェースがあまり優れていない携帯電話端末上でのテキストパスワードと画像パスワードでの入力負担の度合を図ることが出来る。

実験 2 実験 2 では、テキストパスワードと画像パスワードの記憶継続効率を比較するために、ユーザにテキストパスワード (8 文字)、画像パスワード (5 枚) を設定してもらい、パスワードを設定してもらった当日と、それから 1 週間後、2 週間後と同じパスワードで認証を行なってもらい認証の成功率を比較する。この実験によりテキストパスワードと画像パスワードとの記憶継続効率の比較が行なうことが出来る。

5.2 実験結果

表 1: 実験 1:パスワード長と打鍵平均時間 (s)

PW 長	3	4	5	6	7
画像	6.57	8.24	11.47	14.55	15.39
文字	10.94	15.36	14.62	16.11	16.97

表 2: 実験 2:認証成功率の時間推移 (%)

	文字	画像
当日	90	100
1 週間後	60	90
2 週間後	40	90

6 評価と考察

実験 1 から、本システムは従来のテキストパスワードと比べて短い時間で認証を行なうことが可能であることがわかった。特に携帯電話は文字入力が困難である。携帯電話の入力インタフェースはテンキーを使っている。文字入力を行なう場合は、テンキーに割り当てられたアルファベットに

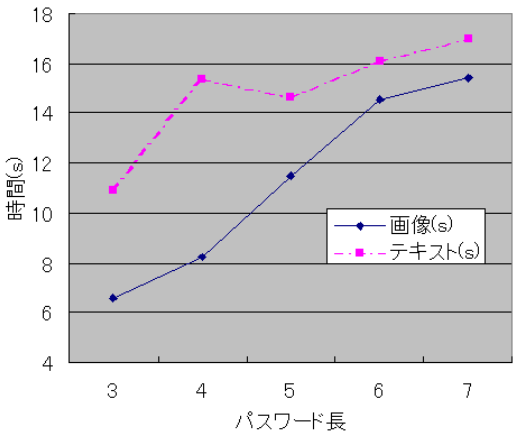

図 5: 実験 1:パスワード長と打鍵平均時間

従って入力を行なう。従って、文字によっては数回テンキーを押さなければ入力出来ない。しかし、本システムの画像選択は、1 回の認証過程でテンキーを押す回数は 5 回となっている。これ以上でもこれ以下でもない。しかし、文字ベースのパスワードでは、5 文字の入力を行なうためには、パスワードによって 5 回〜20 回程度のストロークが必要となる。

また、実験 2 からパスワードを設定してから時間が経過しても画像パスワードの方が文字パスワードに比べて認証成功率が高いことが示された。これは、画像パスワードが記憶に依存することなく、認証段階で認識して画像を選択しているためである。したがって、文字ベースのパスワードで記憶に頼るものよりもユーザにとって記憶する負担がを軽減することが出来る。

7 まとめ

本論では、グラフィックパスワードを用いた個人認証システムの提案し、その有効性を構築と実験によって示した。従来のテキストベースの認証システムに比べユーザにとって利用しやすい認証方式であることを示した。

参考文献

[1] Rachna Dhamija,Adrian Perrig,"DejaVu:A User Study Using Image for Authentication",Usenix,2000

[2] Rachna Dhamija,"Hash Visualization in User Authentication",CHI2000,April 2000

[3] Adrian Perrig,Dawn Song,"Hash Visualization:a way to improve real world security",International Workshop on Cryptographic Techniques and E-Commerce CrypTEC'99,1999