

ライフログを用いた認証システム

石原 雄貴[†] 小池 英樹[†]

近年, 生活のあらゆる場面で個人認証を行う機会が増加した. そして, 主に用いられている個人認証は 4 桁の暗証番号 (PIN) や英数字列を用いたパスワードである. これらの問題点として, ユーザ自身が覚えやすいように脆弱のあるパスワードを用いていることがあげられる. 本研究では, ライフログを用いた認証 (ライフログ認証) システムを考案, 実装した. 本システムの特徴は, 想起型の認証システムであること, 事前に準備をする必要がないこと, 特定のパスワードを覚える必要がないことがあげられる. また, 本システムの実験, アンケート調査, 考察を行なった.

The Authentication system using Lifelog

YUUKI ISHIHARA[†] and HIDEKI KOIKE[†]

Recently, A frequency of an individual authentication is increased. And, most popular individual authentication is PIN and password with number and word. These problem is weak password which user can keep in mind. In this paper, we propose an authentication system using Lifelog. It is given that the feature of this system is an authentication system of the recollection type, and need not prepare beforehand, and need not remember a specific password. And, we experiment, examine by questionnaire and consider our system.

1. はじめに

近年, インターネットの普及やモバイル端末の機能拡大により個人認証を行う機会が増えた. Web サービスでの個人認証には主に, ID と英数字を用いたパスワードによるものが多い. 携帯電話では, 4 桁番号 (PIN) によるパスワードが主に用いられている.

また, 最近では電子マネーやクレジットカードで買い物の支払いができる機能がついた携帯電話が増えてきた. この機能は, 店舗に置いてある読み取り装置に携帯電話をかざすだけで, 支払いの手続きが完了する. また, 自動販売機や駅の改札等で用いられるものもある. このような機能は非常に便利であり, 利用者が増えつつある. しかし, 安全性に関する問題がある. 例えば, 携帯電話を落としてしまったとき, 拾った第三者に簡単に利用されてしまう. このような機能には, 今後個人認証が必要になってくると考えられる.

個人認証は, 所有物方式, バイオメトリクス方式, 知識記憶方式の 3 つに大別できる¹⁾. 所有物方式の認証では, ID カードなどが相当する. この所有物による認証では, ID カード等を紛失してしまった場合, 第三

者に利用されてしまう問題がある. バイオメトリクス方式の認証では, 指紋や虹彩といった生体の特徴を用いた認証が相当する. この本人の特徴による認証では, 生体の特徴を用いているため, 一度紛失してしまうと変えることができないといった問題がある. 知識記憶方式の認証では, 英数字パスワードや PIN を用いた認証が相当し, 現在最も多く用いられている. この知識記憶方式の認証では, ユーザが忘れてしまったり第三者に簡単に推測されてしまうパスワードを利用して等の問題がある. 推測されにくいパスワードを利用すると, 利用者がパスワードを忘れてしまうといった問題が生じ, 特定のパスワードを覚える事は利用者の負担となる. また, 紙にメモをとることが可能で, そのメモからパスワードが第三者に渡る恐れがある.

知識記憶方式の新たな想起型認証方式で, 画像認証²⁾ やなぞなぞ認証³⁾ 等が行なわれている. 詳しくは 2 章で説明する. これらの認証の問題点として, 認証の前に準備や設定が必要ながあげられる.

本研究では, ライフログを用いた認証 (ライフログ認証) システムを考案, 実装した. 本システムの特徴は以下の 3 点である.

- 知識記憶方式で想起型の認証システムであること
- 事前に面倒な設定をする必要がないこと
- 認証の度にパスワードが変化すること

[†] 電気通信大学大学院 情報システム学研究所
The University of Electro-Communications

また、本研究におけるライフログとは、携帯電話を用いて買い物等を行なった際の記録のことである。今後、このようなログが取得できる事を想定して、認証システムを実装した。

2. 関連研究

従来のもの変わる認証として、画像認証、なぞなぞ認証、位置情報を用いた認証⁴⁾⁵⁾等の研究が進んでいる。

画像認証は、文字列のパスワードの代わりに画像を用いる認証である。画像を用いる利点としては、人間にとって画像は文字よりも記憶に適していることや、特定の画像を識別し選択すれば認証が行える等がある。複数枚の画像の中から特定の画像を選択するという方式が多く、操作性に優れ、携帯電話等のモバイル端末でも簡単に利用できる。また、画像はPINや文字列のパスワードとは違い、紙にメモをとることもできないため、第三者にパスワードが伝わりにくい。問題点としては、ユーザの好みでパスワードとなる画像に偏りがでてしまうこと等がある。偏りがでると、第三者による画像の推測が容易になる。

なぞなぞ認証は、クイズのようにある問題を提示し、それに解答するという人の知識や経験に頼った認証である。Webサービスの中にはパスワードの再発行をするために、予め質問とその答えを登録しておくものがある。これは、質問に答えることができればパスワードを得ることができてしまうので、パスワードの再発行時に用いるのではなく実際の認証で用いるということが、なぞなぞ認証の考えである。なぞなぞ認証の利点は、パスワードを暗記する必要がないことや、質問次第で認証の安全性が向上することがある。問題点として、優れた質問を考えることが難しく、安易な質問を用いると簡単に答えが推測されてしまうといったことや、認証に時間がかかること等がある。

位置情報を用いた認証は、ユーザの位置情報によりアクセスしてきたユーザが本人であるかを導きだし、認証に役立terというものである。日常的に位置情報を取りユーザの行動エリアを把握し、アクセスしてきた場所から本人であるかの確率をだす。本人である確率が高い場合は、システムへのアクセスを簡単な認証で行い、確率が低い場合はより複雑な認証を経てアクセスを認める。この認証の利点は、従来の認証システムの強度をアクセスしてきた人ごとに変えることができることである。問題点としては、本人であるかの導き方や確率の精度が、システムの管理者次第で変わる点である。

```
2007/01/10, Wed, 08:51:00, 改札, 新宿駅 (JR)
2007/01/10, Wed, 09:15:00, 改札, 調布駅 (京王線)
2007/01/10, Wed, 09:30:00, 自動販売機, 飲み物 (お茶)
2007/01/10, Wed, 11:44:00, コンビニ, 食べ物 (弁当)
2007/01/10, Wed, 19:12:00, 改札, 調布駅 (京王線)
2007/01/10, Wed, 19:37:00, 改札, 新宿駅 (JR)
2007/01/10, Wed, 21:25:00, 改札, 鴨宮駅 (JR)

2007/01/11, Thu, 07:04:00, 改札, 鴨宮駅 (JR)
2007/01/11, Thu, 08:48:00, 改札, 新宿駅 (JR)
2007/01/11, Thu, 09:10:00, 改札, 調布駅 (京王線)
2007/01/11, Thu, 12:00:00, コンビニ, 食べ物 (おにぎり)
```

図1 ライフログの例

本研究では、なぞなぞ認証を元に、ライフログから購入物や利用路線を問う質問型の認証システムを考案、実装した。

3. ライフログを用いた認証の提案

3.1 ライフログとは

携帯電話を使って個人の生活の動きを記録できる技術の開発という記事が日経産業新聞にあげられた⁷⁾。この記事によると、通話記録やインターネットの閲覧記録、携帯電話による商品の購買記録などを、全地球測位システム (GPS) の位置情報と関連づけて収集し、いつどこで何をしていたか分かるようになる技術の開発を進めていると紹介されている。現段階では、このような情報を自動的に利用できる手段は無いが、今後取得できるようになると想定している。そこで、本研究ではユーザの購入物情報と駅の改札情報に着目し、この情報の記録をライフログと定義した。今回利用したログは、購入や駅を利用した際に、携帯電話を用い手動でサーバにアップロードしたものである。図1はライフログの例である。

3.2 ライフログ認証の概念

ライフログ認証とは、ユーザの最新の購入物や利用路線名を問う質問型の認証である。図2はライフログ認証の方法である。購入物と路線名を6つのカテゴリーに分け、各カテゴリーに9つのメニューを用意した。カテゴリーは、飲み物、食べ物、お菓子、デザート、雑誌、路線である。(カテゴリー例: 飲み物, メニュー: コーヒー, お茶, スポーツ飲料, 炭酸飲料, ジュース, ミネラルウォーター, ビール, 焼酎, ワイン)。認証画面では、カテゴリーごとに表示され、9つのメニューの選択肢の中から前回購入した物を選択する。表示されるカテゴリー画面は、6つの中からランダムに4つ選ばれる。

ライフログ認証では、ライフログが更新される度に、認証時のパスワードが変わることとなる。また、6つのカテゴリーの中から4つのカテゴリーがランダムに

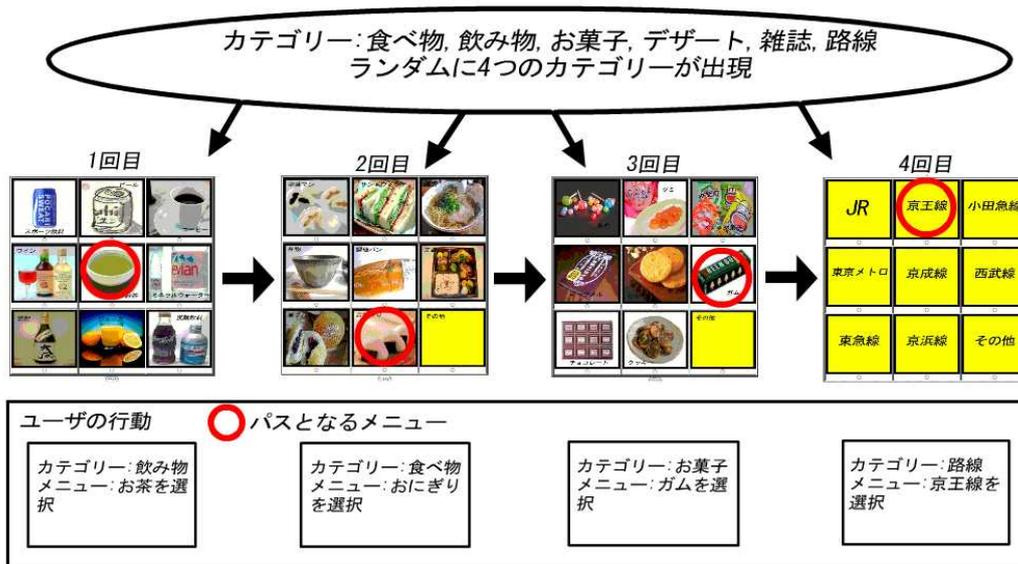


図 2 ライフログ認証の方法

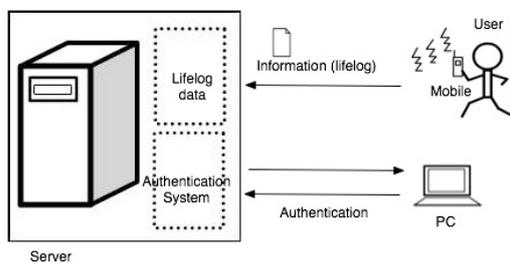


図 3 システム構成図

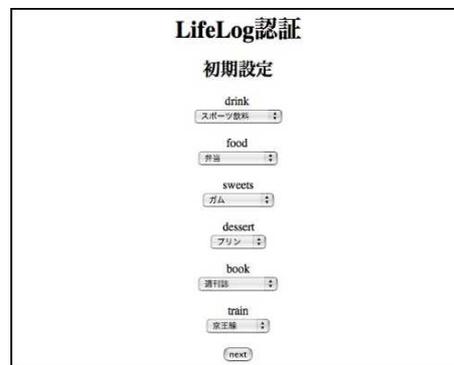


図 4 初期設定

出現するため、認証の度に表示される画面は変わる。また、認証時のパスワードは最新の購入物や利用路線名を選択であり、記憶が容易であると考えられる。

4. システム概要

4.1 システム構成

図 3 は、システム構成図である。サーバにはユーザの購入物や利用駅を記録するための CGI を設置した。ユーザは購入や駅を利用する度にこの携帯電話からこの CGI にアクセスをして、購入物や利用路線名をアップロードすることによりライフログを作成した。また、サーバにはライフログ認証システムを設置し、ユーザは認証を行う際にパソコンからアクセスをする。そして、サーバに保存してあるユーザのライフログを元に認証が行なわれる。

4.2 初期設定

各カテゴリのメニューを全て購入済みでないこの認証を行う事ができないため、初期設定に各カテ

ゴリーのメニューを1つずつ設定し、それを初期のパスワードとした。図 4 は初期設定画面である。

4.3 認証画面

図 5 は、ライフログ認証画面である。認証画面では、カテゴリごとに表示され、9つのメニューの選択肢の中から前回購入した物を選択する。カテゴリが路線の場合は、前回使用した路線を選択する。図 5 は、カテゴリが飲み物の例である。各メニューは画像で表示される。各カテゴリは、ランダムに4回出現し、4カテゴリ全てにおいて、正しいメニューが選択できた場合、認証が完了する。

5. 考察

5.1 実験

認証に成功する確率を調べるために、2人のユーザで実験を行なった。実験期間は2週間とした。表 1 は



図 5 認証画面

表 1 実験結果

	試行回数	成功回数	失敗回数	成功率 (%)
ユーザ 1	24	22	2	91.7
ユーザ 2	10	8	2	80.0

実験結果である。ユーザ 1 の成功率は 91.7% で、ユーザ 2 の成功率は 80% という結果になった。比較的新しい記憶がパスワードの情報となるため、認証は容易であったと考えられる。また、認証に失敗したときは、購入物や利用路線は覚えていたものの、ログのアップロードを忘れていたということもあった。今回 2 人のユーザで試した結果では、認証が容易であるという結果となったが、認証画面にあまり購入しないカテゴリーが出現してきた場合や購入してからしばらく期間があいたときにどのような結果となるかはわからない。より多くのユーザと長期間の実験が必要であるとされる。また、現段階ではログのアップロードは携帯電話を用いて手動で行なっているため、比較的購入物や利用路線を覚えやすかったとも考えられる。将来的にログが自動的に計測できるようになった場合に、どの程度覚えていられるかなどの検証が必要になってくる。

5.2 意識調査

ユーザが最新の購入物を覚えていられるかどうかの意識調査を行なった。Hatena⁸⁾ のアンケートを用いて、Hatena ユーザ 500 人を対象にした。アンケートは、最新の購入した品物を覚えていられるかどうか？、最新の購入した飲み物は何か？の 2 つである。図 6, 7 は意識調査の結果である。最新の購入した品物を覚えていられるか？という質問に対して、89.0% の人が確



図 6 はてなアンケート結果 1

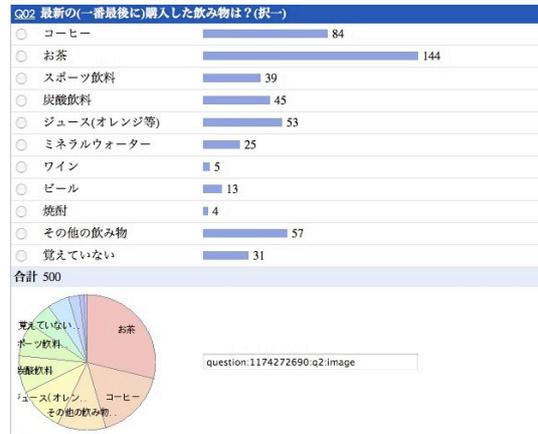


図 7 はてなアンケート結果 2

実に覚えているという回答だった。最新の購入した飲み物は?という質問に対しては、93.8% の人が覚えているという回答だった。後者の質問では、飲み物のメニューを選択する形式をとったが、この方が覚えている割合が高かった。今回の意識調査の結果を見る限りでは、本システムが有用であると言える。また、本システムを利用する際は、意識的に購入物や利用路線を覚えるようになり、今回のアンケート結果以上の期待がもてると考えられる。

5.3 有用性

最新の購入物、利用路線を問うため、記憶は比較的容易であると考えられる。意識調査の結果を見ても、9 割近くの人が最新の購入物、最新購入した飲み物を覚えているという結果となった。実験結果をみても、認証の成功率は高かった。しかし、今回は短期間の実験だったため、購入しなかったカテゴリーが出現しても、初期設定を簡単に覚えやすかったと考えられる。今後は長期的な実験、調査が必要である。

また、予めカテゴリーとメニューが決まってい、ユーザ自身がメニューを選択してサーバにアップロードしているため、直感的にメニューを選択しやすかったと考えられる。

現段階では、認証実験前にライフログが存在しなかつ

たため、本システムではパスワードとなるメニューの初期設定が必要となった。ライフログが存在すれば、この設定をする必要がなくなる。

今回実装したシステムでは認証画面のメニューは画像で表示している。これは、今後店頭等でタッチパネルを用いて認証を行うことや携帯電話を用いて簡単に認証を行えることを想定した。現在主に用いられている英数字列のパスワードの入力に比べ、入力の手間が少なく操作性は良い。

5.4 安全性

ライフログ認証では、ライフログが更新される度にユーザのパスワードが変化する。また、認証の度に表示される画面が変わるため、同一のパスワードを長期的に利用するよりも安全性が高いと考えられる。認証の強度としては、9つのメニューが4カテゴリー分ランダムに出現するため、パスワードの組み合わせはPIN程度の総数が期待できる。しかし、図7を見ると、メニューによって購入物の差がでることがわかる。図7では、飲み物の例であるが、お茶が圧倒的に多いことがわかる。メニューによって差が大きすぎると、第三者によるパスワードの推測が容易になってしまうことも考えられる。

また、ユーザの身内やユーザに詳しい人、ユーザの行動を監視している人には、その人のパスワードが推測できてしまう場合もでてくる。今回実装したシステムでは、最新の4種類の購入物、利用路線名がわかってしまえば、不正に認証が行なわれてしまう。今後このようなソーシャルハッキングへの対応が必要であると考えられる。

6. 今後の課題

今回実装したライフログ認証は、携帯電話のセキュリティへの応用を想定している。お財布携帯や携帯クレジットが普及し、携帯電話のセキュリティ対策は必要となってくると考えられる。本システムでは、携帯電話を落としてしまった場合、拾った人が各カテゴリーのメニューを購入すれば、パスワードが変更されるためその人に知られてしまうという問題点がある。表示手法に関しては、メインの認証画面はカテゴリー別になっている。今後は、問題解決と最適な表示手法を検討したいと考えている。

また、今回の認証実験では十分な試行回数を行うことができなかった。今後は、十分な人数、試行回数を行ない、本人許容率(成功率)だけでなく、本人拒否率、他人許容率等の実験を行いたいと考えている。

7. ま と め

本研究では、ライフログを用いた認証システムを考案、実装した。実際に、ライフログを計測し、認証の実験を行なった。また、現在このようなログを自動的に取得する手段が無いため、Hatena アンケートを用いて意識調査を行った。今後もライフログ認証の有用性、安全性の向上や携帯電話のセキュリティへの応用を目指したいと考えている。

参 考 文 献

- 1) 小池英樹, 増井俊之, 高田哲司, 画像を用いた個人認証手法, 会誌「情報処理」, Vol.47, No.5, 通巻495号, pp.479-484, 2006.
- 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, 2003.
- 3) 増井俊之, インターフェイスの街角 (43) - 明るい認証システム, UNIX MAGAZINE, Vol.16, No7, pp.185-189, (株) アスキー, (2001).
- 4) D.E. Denning, P.F. MacDoran, Location-Based Authentication: Grounding Cyberspace for Better Security, Computer Fraud and Security, Feb. 1996.
- 5) 田口浩平, 小池英樹, PHSを用いた個人認証に関する研究, マルチメディア, 分散, 協調とモバイル (DICOMO2001) シンポジウム, 情報処理学会, pp.458-465, 2001.
- 6) 石原雄貴, 小池英樹, Path-Pass:位置情報を用いた認証システム, コンピュータセキュリティシンポジウム (CSS2006), 情報処理学会, pp.537-542, 2006.
- 7) 携帯, 生活まるごと記録-何買った どこ行った, 日経産業新聞 2006年7月5日第1面朝刊.
- 8) はてな, <http://www.hatena.ne.jp/>