FeliCa の利用履歴を用いた個人認証

松村 智彰 †　　小池 英樹 †

† 電気通信大学 大学院情報システム学研究科
182-8585 東京都調布市調布ヶ丘 1-5-1

tsumura@vogue.is.uec.ac.jp , koike@is.uec.ac.jp

あらまし 近年非接触型 IC チップである FeliCa を利用したサービスが普及し、その ID を利用した認証が多く利用されている。しかし、ID のみを利用した認証では FeliCa 自体が盗難された場合になりすましの危険性がある。我々は、FeliCa に記録されている利用履歴を用いた個人認証について提案する。FeliCa の中でも特に利用されることが多い Suica 系のサービスには駅の入出場や物販の利用履歴が保存されている。本研究では FeliCa の利用履歴から特徴的なユーザの行動を抽出し、それを利用した認証を実現した。

User Authentication using Usage History of FeliCa Card

Tomoaki Matsumura†　　Hideki Koike†

†Graduate School of Information Systems, The University of Electro-Communications
1-5-1 Chofugaoka Chofu-shi Tokyo 182-8585

tsumura@vogue.is.uec.ac.jp , koike@is.uec.ac.jp

Abstract In this paper, we propose authentication system using usage history of FeliCa card. FeliCa is a contactless RFID smart card system and a de facto standard in Japan. However, when one's FeliCa card is stolen, there is a risk of abuse. General ID authentication system is vulnerable to impersonation of cards. Our authentication system makes use of buying history and train travel records stored in FeliCa cards. The proposed system prevents impersonation with feature of user's behavior from usage history.

1　はじめに

近年日本では、FeliCa[1] を利用したサービスが広く普及している。FeliCa とはソニー株式会社が開発した非接触 IC カードの技術方式であり、これを用いることでユーザは様々なサービスを「かざす」だけで利用できる。また、入退室管理システムなどの個人認証システムでも FeliCa が利用され始めている。しかし、FeliCa を用いた個人認証システムでは FeliCa の ID のみを利用した認証が用いられることが多く、FeliCa 自体が盗難された場合になりすましの危険性がある。

なりすましの対策としては、パスワードを利用した個人認証が考えられる。しかし、パスワードの利用には「パスワードを忘れる」、「パスワードが本人の属性情報（生年月日、電話番号など）に関連していて類推される」、「パスワードが更新されない」といった問題がある。

そこで我々はなりすましの対策として FeliCa に記録されている利用履歴を用いた個人認証について提案する。本研究では主に入退室管理などの FeliCa をかざすことで日常的に実行される個人認証を対象としている。この種の個人認証

ではユーザに負荷を掛けずに認証を行うことが求められる。そこで、我々は FeliCa に記録されている各種のログを認証に利用することを提案する。日常的に利用されている FeliCa からは、駅の利用や物販の履歴などが取得できる場合が多い。そのデータからユーザ本人にしかわからない情報を抽出し、認証に利用することで、なりすましの対策としてパスワードを利用しない個人認証の実現が可能になると考えられる。

2 関連研究

個人認証は、記憶 (知識) によるもの (Something You Know)、所有物によるもの (Something You Have)、本人の特徴によるもの (Something You Are) などに分けられる。パスワードは記憶による認証であり、これに代わる認証手法としては、画像認証 [2]、なぞなぞ認証 [3]、位置情報を用いた認証 [4] などがある。また、ユーザの行動を元にした個人認証に関連する研究としては、位置情報を利用した認証システム「Path-Pass」[5][6] がある。これは、GPS により取得したユーザの位置情報の変化 (行動履歴) をパスワードにした認証システムで、ユーザの行動履歴を過去に遡ることで個人認証を行っている。

Path-Pass で利用している GPS のログとは異なり、FeliCa から得られる各種のログには位置情報が記録されていないものが多い。しかし、駅の利用履歴や物販の履歴からユーザの行動を推測することができる。GPS のログは連続的な位置情報であり、認証に利用する場合は何らかの特徴を抽出する必要がある。また、その特徴をユーザが必ず記憶しているとは限らない。対して、FeliCa から得られるログは、”物を買う”、”電車に乗る”といったユーザのアクティブな行動に対応しており、記憶による認証に有効だと考えられる。また、本研究では認証に必要な情報は全て FeliCa から取得するため、FeliCa をかざす以外の特別な動作は不要でユーザの負荷が少ない。これらの特徴を利用することで、FeliCa の ID を利用した所有物による認証と、FeliCa の利用履歴を用いた記憶による認証を実現した。

3 認証システム

我々は提案した認証手法を実現するために、タッチされた FeliCa カードの利用履歴を読み取り認証問題を生成するシステムを開発した。このシステムの個人認証の流れを以下に示す。

1. ユーザはクライアントマシン (図 1) に FeliCa をタッチ。
2. クライアントマシンは読み取った履歴データを解析しサーバへ転送。
3. サーバは履歴データを保存。
4. クライアントマシンは認証に必要な情報をサーバから取得。
5. クライアントマシンは画面上に認証問題を生成・表示。

開発したシステムの構成を図 2 に示す。クライアント側のプログラムは Windows 上での動作を対象として実装を行った。ユーザの情報や FeliCa から取得した情報の管理には、サーバ上に構築した MySQL を利用した。認証を行う際は MySQL から認証に必要な情報を取得し、クライアントプログラムで問題生成と問題提示を行った。FeliCa から取得するデータについては 4 章に、認証手法については 5 章に示す。

図 1: クライアントマシン

4 利用するデータ

本研究では FeliCa の中でも利用者が多い Suica などの交通系カードの利用履歴を用いる。交通

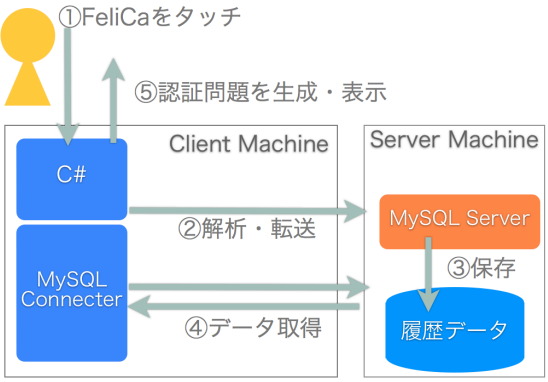

図 2: システム構成

系カードにはSuica、モバイルSuica、PASMO、ICOCA、 PiTaPa、TOICA などがある。これらのシステム・製品名は各社の商標または登録商標である。交通系カードから取得できるデータとしては、属性情報、利用履歴、改札入出場履歴がある。取得したデータを解析し得られる情報について以下に示す。

- 属性情報
  カードの種類や残高・取引連番などが記録されている。

- 利用履歴
  物販や電車移動の利用履歴が最大 20 件記録されている。電車利用の場合は、入場駅・出場駅と利用した日付・残高などが記録されている。利用履歴の例を表 1 に示す。

表 1: 利用履歴の例

日付	2010 年 8 月 15 日
機器種別	自動改札機
利用種別	自動改札機出場
支払種別	Suica
入出場種別	入場・出場
入場駅	京王線 新宿駅
出場駅	京王線 西調布駅
取引連番	272

- 改札入出場履歴
  電車移動の際の駅の改札の利用に関する履歴が最大 3 件記録されている。利用履歴と比べ、駅を利用した場合の詳細な時刻が含まれている。改札入出場履歴の例を表 2 に示す。

表 2: 改札入出場履歴の例

日付	2010 年 8 月 15 日 21 時 23 分
入出場	出場
駅	京王線 西調布駅
利用金額	230 円

5 認証手法

本研究で提案する認証手法では、4 章に示した履歴の中から、ライフログとして扱いやすい利用履歴 20 件と駅改札入出場履歴 3 件を主に利用する。

履歴だけを利用して認証を行う場合は、回答の選択肢は 1. 場所 (駅名・地域)、2. 時刻、3. 金額 の組み合わせとなる。それらの選択肢を利用する認証として、以下の 3 種類の認証方法を提案する。

- 最後に入場した駅認証
- 利用頻度が低い駅認証
- 利用した時刻認証

5.1 最後に入場した駅認証

改札入出場履歴 3 件には最後の移動で利用した駅の入出場の情報が含まれている。最も単純な認証として、その駅名を回答する方法を提案する。

最後に出場した駅を回答する場合、認証を実際に行う地点に近い駅が正解となってしまう可能性が高い。そのため、最後に入場した駅を正解データとする問題を生成する。

ダミーは日本全国の駅一覧からランダムに取得したものと、5.2 章のユーザ毎の駅の利用頻度から取得したものを組み合わせて利用している。今回は 1 件の正解と、3 件のダミーを用いた。

実際の認証画面を図 3 に示す。また、ヒントとしてユーザには利用日時を提示する。正解とダミーをランダムに並べ、その中からユーザが正しいと思う駅を選択することで認証を行う。

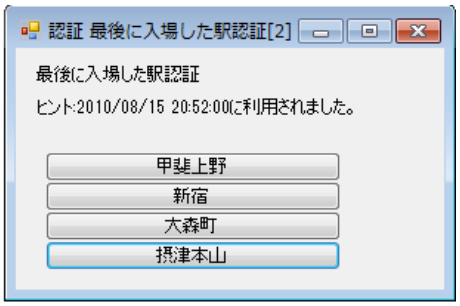

図 3: 最後に入場した駅認証の画面

図 4: 利用履歴の駅一覧

図 5: 一定期間収集した利用履歴の駅一覧

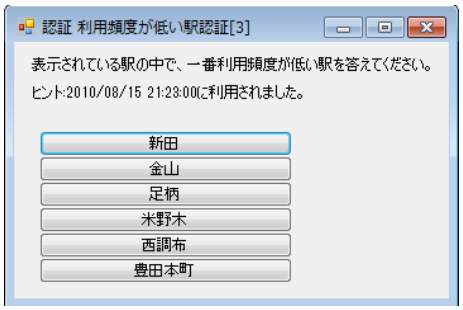

図 6: 利用頻度が低い駅認証の画面

5.2 利用頻度が低い駅認証

利用履歴には移動の際に利用した駅のデータが含まれている。普段から利用している利用頻度が高い駅は他者から類推される可能性が高い。逆に利用頻度が低ければ、他者から類推される可能性は低くなると考え、利用頻度が低い駅名を回答する認証手法を検討する。

FeliCa に保存される利用履歴の件数には制限があり、その件数以上は取得できない。例えば 1 週間分しか利用履歴が保存されていない場合、その前の週に B 駅を多く利用していても、認証時に B 駅が不正解の選択肢なってしまう。これを防ぐためには、過去の利用履歴を保存し利用頻度を生成する必要がある。そこで、FeliCa を認証する際に利用履歴をユーザ毎に保存し、一定の期間内の利用履歴に対して利用頻度を生成する。今回は 1ヶ月間以内の利用に対する利用頻度を生成し利用した。FeliCa の利用履歴に含まれる駅情報を Google マップに対応させ表示させたものを図 4 に示す。また、同じユーザの 1ヶ月分の利用履歴を収集し、集計し表示したものを図 5 に示す。赤い記号が利用した駅を、青線が入場駅と出場駅の関係を、青線の色の濃さが利用頻度を表している。図 4 と図 5 を比べると、利用履歴を継続して収集することで、より多くの駅に対する利用頻度が利用できることがわかる。

実際の認証画面を図 6 に示す。利用頻度が低く利用時刻からの時間経過が小さい駅を正解とする。ヒントとしてユーザには利用日を提示している。また、ダミーデータにはユーザ毎の駅の利用頻度から利用頻度の高い駅を複数取得し利用する。正解とダミーをランダムに並べ、その中からユーザが正しいと思う駅を選択することで認証を行った。

5.3 利用した時刻認証

改札入出場履歴 3 件には、改札を利用した詳細な時刻が記録されている。また、利用履歴 20 件には物販利用などで詳細な時刻が記録されている場合がある。改札入出場履歴と利用履歴に含まれる時間情報の中で、比較的新しい利用時刻をユーザが回答するという認証手法を提案する。

最新の利用時刻を正解データとする場合は、ユーザの最新の利用の種類を考慮する必要がある。利用が電車移動の場合は、定期利用の場合でも改札入出場履歴に必ず時刻が記録されている。一方、利用が物販の場合は、利用履歴の中に詳細な時刻が記録されている場合がある。また、利用がそれ以外の場合（チャージなど）は、必ずしも詳細な時刻が記録されているとは限らない。それらの利用履歴を比較し、その中から最新の利用時刻を抽出し認証に利用する。

実際の認証画面を図 7 に示す。ユーザの利用の詳細（例：西調布駅を出た）を表示し、ユーザがその利用時刻を入力することで認証を行う。今回は正解の時刻からの誤差が 1 時間以内であれば正解とする。

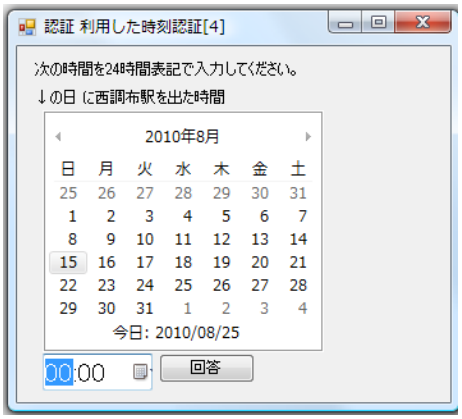

図 7: 利用した時刻認証の画面

6 評価実験

当研究室に所属する学生のうち、日常的に FeliCa を利用している 9 人を被験者として実験を行った。被験者全員に対して予め 1ヶ月の間 FeliCa の情報を定期的に収集し、データベースに利用履歴を蓄積した。その上で、「最後に入場した駅認証」・「利用頻度が低い駅認証」・「利用した時刻認証」を行った。また、実験後にどの程度の期間においてユーザが利用を正しく記憶しているかを確認するために、「X 月 X 日に利用した駅を答えよ」という利用駅についてのアンケートを実施した。アンケートで質問した利用履歴の件数はユーザにより異なるため、結果には回答数を付加している。

7 結果と考察

実験の結果を表 3 に、アンケートの結果を表 4 に示す。また、被験者 9 人から収集した駅の利用状況を図 8 に示す。

表 3: 実験結果

認証タイプ	正答率	平均回答時間
最後に入場した駅	100%	11.75s
利用頻度が低い駅	87.5%	26.65s
利用した時刻	87.5%	19.66s

表 4: 利用駅についてのアンケート結果

利用日からの時間経過	正答率	回答数
1 週間以内	100%	7
1 週間以上、2 週間以内	76.9%	13
2 週間以上、3 週間以内	41.6%	12
3 週間以上、4 週間以内	16.6%	6

表 3 の結果では、3 つの認証方法のうち、「最後に入場した駅認証」が最も平均回答時間が短く、正答率も高かった。逆に「利用頻度が低い駅認証」は最も平均回答時間が長かった。これは、この問題を回答するためには多くの場合 2、3 週間の電車移動を把握する必要があるためだと考えられる。回答時間は認証時のユーザに対する負荷であると考えられる。認証強度を強化すると、ユーザに対する負荷も同時に高まっていく。今後はこれらを考慮して適切な認証強度とユーザ負荷を持つように認証手法を改良する必要がある。

表 4 のアンケート結果からは、時間経過が 2 週間以内であれば駅名を正しく回答できる可能性が高いことがわかる。したがって、「最後に入場した駅認証」などで、最後の利用が 2 週間以上前であれば正答率が低下すると考えらる。これらの認証においては、時間経過に対する何らかの対策が必要になると考えられる。

また、アンケートと同時に行った被験者からの聞き込みでは、2 週間以内であれば利用した時間を記憶していることが多かった。また、駅の移動の目的についても多くの場合で明確な回答を得ることができた。したがって、回答の選

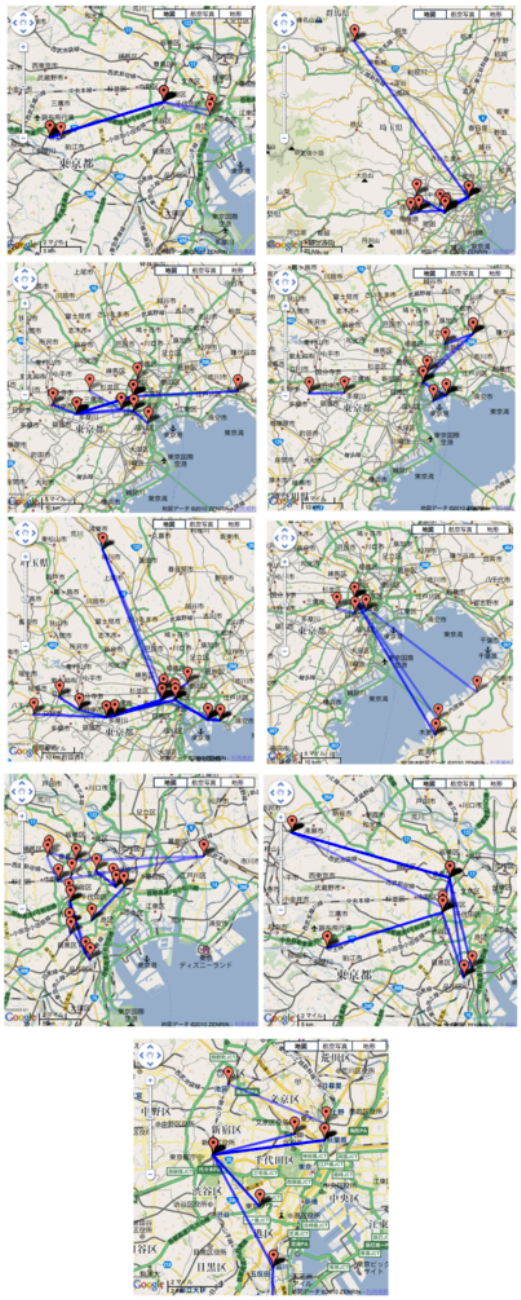

図 8: ユーザ毎の駅の利用状況

択肢として駅名や時刻ではなく、利用目的に関連する内容を出題する認証が実現できると考えられる。

図 8 のユーザ毎の駅の利用状況を見ると、それぞれのユーザ毎に駅の利用状況に明確な差が確認できる。今後、これらの経路を利用した個人認証の実現を目指す。

今回の評価実験では検証数が少ない上に、なりすましが実際に行われた場合の実験を行っていない。したがって、今後は更なる評価実験を行いより適切な問題の生成を目指す。また、今回あまり利用していない物販の履歴からも時刻や金額や物販端末などの情報が利用できるため、それを利用した認証の実現を目指す。

8 まとめ

本論文では、FeliCa の利用履歴を用いた認証手法について提案した。また 3 種類の異なる認証方法を実装し、実験を行った。今後は多くの実験と認証の改良を行い、より効果的な個人認証の実現を目指す。

参考文献

[1] Sony Corporation. Felica ホームページ http://www.sony.co.jp/products/felica/.

[2] Rachna Dhamija and Adrian Perrig. Déjà vu: a user study using images for authentication. In *SSYM'00: Proceedings of the 9th conference on USENIX Security Symposium*, pp. 4–4, Berkeley, CA, USA, 2000. USENIX Association.

[3] 増井俊之. インタフェースの街角 (43) - 明るい認証 システム. UNIX Magazine 2001 年 7 月号, Vol. 16, No. 7, pp. 185–189, 2001.

[4] D.E. Denning and P.F. MacDoran. Location-based authentication: Grounding cyberspace for better security. *Computer Fraud and Security*, Vol. 1996, No. 2, pp. 12–16, 1996.

[5] 石原雄貴, 小池英樹. Path-pass:位置情報を用いた認証システム. *Computer Security Symposium 2006 (CSS2006)*, pp. 537–542, 2006.

[6] 今澤貴夫, 小池英樹, 高田哲司. GPS データを用いた位置認証システムとその停留点算出方式. *Computer Security Symposium 2008 (CSS2008)*, pp. 707–712, October 2008.