FeliCa の利用履歴を用いた認証システム

User Authentication System using Usage History of FeliCa Card

松村 智彰　清野 祥之　国友 一生　小池 英樹*

Summary.　近年非接触型 IC カードの技術方式である 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。

1　はじめに

近年日本では、FeliCa 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。これは、ユーザの移動や購入というユーザの行動とそれに関する記憶を用いた認証方式である。同様に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、ユーザの位置情報の変化を利用した認証システム「Path-Pass」[2] や、ユーザの生活の履歴を利用した「電子メール履歴認証システム」[1] などがある。

* Tomoaki Matsumura and Yoshiyuki Seino and Kazuki Kunitomo and Hideki Koike 電気通信大学大学院 情報システム学研究科 情報メディアシステム学専攻

2　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 1 に示す。FeliCa から取得するデータについては 3 章に、認証手法については 4 章に示す。

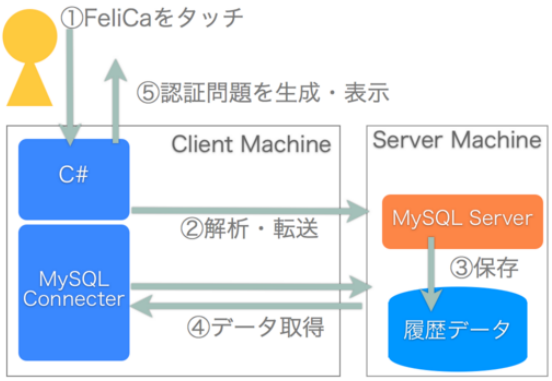

図 1. システム構成

3　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てある。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。今回の認証では以下の2種類の履歴情報を利用する。

- 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。
- 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。

4 認証手法

本研究で提案する認証手法では、3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と駅改札入出場履歴を利用する。それらを利用した認証として、3種類の認証方法を提案する。

4.1 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。不正解の選択肢としてのダミーデータには日本全国の駅一覧からランダムに取得したものと、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。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。

4.2 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提案する。

FeliCaに保存されている履歴の件数には制限があり、一回に取得できる利用履歴だけでは十分な精度の利用頻度が生成できない。これを防ぐためには、過去の利用履歴を保存し、その上で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。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う。

4.3 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。電車移動の場合は、改札入出場履歴に必ず時刻が記録されている。一方、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。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。

5 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開発を行った。今回は交通系カードのみを対象に開発を行ったが、電子マネー系カードの履歴の利用も有効だと考えられる。また、今回はFeliCaから得られるデータのみを利用しているが、それ以外のライフログを組み合わせた認証も考えられる。特に様々なWebサービスから得られるライフログと実生活から得られるライフログの組み合わせが有効だと考えられる。例えば、Twitterなどのマイクロブログサービスや、検索履歴、写真、メール、日記などの利用が考えられる。これらの手法を取り入れつつ、より多くの実験と認証の改良を行い、効果的な個人認証の実現を目指す。

参考文献

[1] 西垣 正勝, 小池 誠. ユーザの生活履歴を用いた認証方式—電子メール履歴認証システム. 情報処理学会論文誌, 47(3):945–956, Mar 2006.

[2] 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.