IC カード等を用いた多要素 Web 認証

松澤 英之, 園田 誠

宮崎大学 情報基盤センター

matuzawa@cc.miyazaki-u.ac.jp,sonoda@cc.miyazaki-u.ac.jp

概要：最近学生証として FeliCa (IC)カードを採用する大学が増えているが、FeliCa カードを自由に単独の認証に用いることは難しい。また、利用者の利便性およびセキュリティの向上等から統一認証が採用されるが、同一のセキュリティ強度となる統一認証だけでは、各システムの重要度に応じたセキュリティ強度の認証を行うことは難しい。この解決策として多要素(多段)認証がある。今回、IC カード等を用いた多要素(多段)Web 認証を開発した。

1 はじめに

最近、交通機関[1]や、コンビニ[2]、スーパー[3]など、様々な場所で FeliCa (IC)カードが利用されている。また、学生証として FeliCa カードを採用する大学が増えている。そのため、身近にある FeliCa カードを利用して認証を行えば利便性が向上するが、様々なアプリケーションの認証に自由に応用する事は難しい。

また、利用者の利便性およびセキュリティの向上等から統一認証が採用されることが多くなってきているが、統一認証は全てのシステムに対して同一のセキュリティ強度で提供されるため、各システムの重要度に応じてセキュリティ強度の変更を行うことは難しい。この解決策の一つとして複数の認証を組み合わせた多要素(多段)認証がある。

そこで、今回は IC カードと USB 機器を用いた多要素(多段)Web 認証システム(以下、IC カード認証)を開発した。

2 IC カード等を用いた多要素 Web 認証

2.1 FeliCa IC カード

IC カードの形式は世界でいくつかあるが、日本で一番普及している IC カードは、FeliCa カード[4]である。特に大都市圏では、交通系のカードとして、地方でもコンビニ、スーパーの支払いカードとして採用されている。また、近年大学の学生証、職員証を磁気カードから FeliCa カードに変更する例も多い。このように日本の様々な場所、場面で利用されている FeliCa カードであるが、FeliCa カードを情報システムの認証に利用した例はあまり聞かれない[5]。

FeliCa カードに保存されている情報は、大きく分けて 3 つに分けられる[6]。一つ目は、FeliCa カードと IC カードリーダ/ライタ(IC カード読み取り機)との間でネゴシエーション(Polling)を行う時に得られる製造 ID(IDm)と製造パラメータ(PMm)。二つ目は、フェリカネットワークスが運営・管理する共通領域。三つ目は、ユーザが自由に使えるプライベート領域である。

一つ目の領域は、Polling した際に得られる情報なので、情報機器で自由に読み取れる領域である。しかし、読み取り時に暗号化されていないことと IDm の一意性が保障されていないため[7]、セキュリティが要求されるサービスの認証情報としてこの情報を利用することは推奨されていない。

二つ目の共通領域は、暗号化されていて認証にも利用できる。しかし、この領域を利用するためには、フェリカネットワークスにサービスを登録する必要があり、自由に情報システムの認証に利用する用途に適していない。

三つ目のプライベート領域は、ユーザが自由に利用でき、読み取り可能つまりデータが公開さ

れている。通信経路も暗号化されていないので、ユーザがこのプライベート領域のデータを認証情報として単独で認証に利用する事は難しい。以上のようにFeliCaカードを単独でかつ”自由”に情報システムの認証キーをして利用することはできない。

2.2 USB 機器

USB 機器は、情報機器への接続時に情報機器との間でディスクリプタと呼ばれる情報をやり取りする。これらの情報には、USB 機器を特定するためのシリアル番号が含まれている。しかし、ディスクリプトはどの情報機器との間でもやり取りされるので、公開情報であり、認証情報として利用する事は難しい。

2.3 FeliCa カードと USB 機器を用いた多要素認証

実際 FeliCa カードを利用した認証ソリューションでは、暗号化が可能な FeliCa の共通領域に暗号化した認証情報を保存し、保存した情報を利用者本人が持ちうる認証情報として利用して認証を行う。同様に USB メモリーを利用した認証は、USB メモリーに暗号化した認証情報を保存して利用する。そのため、認証情報の漏えいは、死活問題となる。

では、公開されている FeliCa カードと USB 機器の情報を利用して、どのように認証を行うのか。まずもっとも身近なパスワード認証について考える。パスワード認証に使える文字数は多くても 80 文字程度であり、半角英数字と記号が使えることがわかっている。これらの文字の組み合わせ(長さと並び順)を本人しか知りえない認証情報として扱い認証を行っている。

FeliCa カードと USB 機器は、全世界で一意でないかもしれないが、FeliCa カードは IDm と PMm、USB 機器はシリアル番号といった無数の ID を持っている。これらの機器が持っている情報を認証パスワードの一文字と同様に組み合わせて認証を行えば、FeliCa カードと USB 機器が持っている(利用できる)情報が公開された情報だとしても十分にセキュリティ強度がある認証システムを構築できると考える。つまり、様々な種類の FeliCa カードと USB 機器の持つ情報を順番に組み合わせて認証を行うのである。FeliCa カードと USB 機器の持つ情報は、パスワード認証の文字一つ一つと同等で、その組み合わせ(認識個数と並び順)情報が本人しか知らない認証情報と考えていただければよい。パスワード認証と IC カード認証との比較は後程行う。

今回は、実証実験のユーザに受け入れやすいように、単独の認証ではなく、補助的な二要素(二段)認証の二要素目として、また比較的実装が自由に行える Web アプリケーションの認証として実装した。

2.4 IC カード等を利用した二要素 Web 認証システム

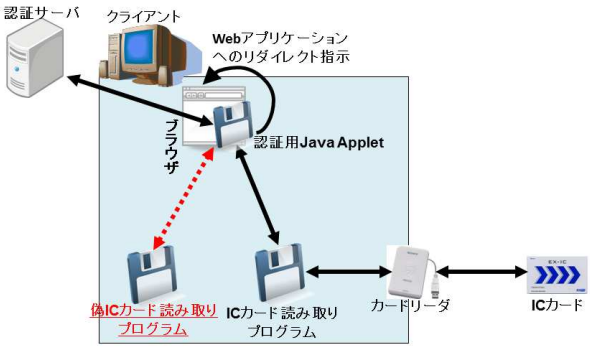
このシステムは大きく分けてシステムを利用するするパソコンで認証データを取得し認証システムサーバにデータを送るローカルプログラム、サーバプログラムとローカルプログラムとサーバプログラム間の認証情報の伝達を中継する Java Applet プログラムに分けられる。

IC カード等の情報を取得するローカルプログラムはサービスを利用するパソコン側にある点に注意する必要がある。つまり、サーバ側に送られる情報が必ずしも FeliCa カードや USB 機器から直接取り込んだ情報かどうか保障できないということである。極端な例を挙げれば正しい認証情報をサーバ側に送れるローカルプログラムを作れば認証できてしまう。しかし、Web ブラウザにパスワードを自動保存するプログラムがあるように、個々の FeliCa カードと USB 機器の情報は公開情報であるので、情報の出所は問題とならない。

動作手順を示す。まず、パスワードなどで第一要素目の認証を行う。認証が成功した場合は、通常のパスワード認証と同じようにブラウザに Cookie 情報を送り、ブラウザを IC カード認証

用 Web サイト(IC 認証 Applet サイト)にリダイレクトする。ブラウザは IC 認証 Applet 用サイトに含まれた Java Applet を起動する。次にローカルプログラムを起動して認証用の FeliCa カードと USB 機器を順に読み込み認証情報を取得する。個々の機器の認証情報を取得するたびに、Java Applet を経由してサーバ側プログラム(IC 認証サイト)に認証データを転送する。IC 認証サイトでは、保持している認証情報と送られてきた認証情報との照合を行う。サーバ側のプログラム(IC 認証サイト)は、ブラウザがアクセスしているサイト(IC 認証 Applet サイト)とは別である。Applet と IC 認証サイトとの間は、http(80 番ポート)で、Applet とローカルプログラムは TCP/IP 5555 ポートを利用した。認証情報を送り終わった時点でローカルプログラムからデータ入力終了のデータを IC 認証サイトに送り IC カード認証を終了する。認証が成功した場合は、IC 認証サイトから Java Applet に認証成功が通知され、この Java Applet から IC 認証 Applet サイトにある JavaScript を用いて利用できる Web アプリケーションサイトにリダイレクトされる。

IC カード認証時にユーザに見せる IC 認証 Applet サイトに Java Applet を記載したのには理由がある。ローカルプログラムとサーバで認証情報を直接やり取りする事はできるが、IC カード等を利用した認証の結果を一段目の認証情報を保持している Web ブラウザに反映する方法がない。そこで、一段目の認証情報を保持している Web ブラウザで Java Applet を起動してローカルプログラムとサーバ側との認証情報を中継。サーバ側で認証を行った後、Java Applet が IC カード等を用いた認証の結果をサーバから取得、IC 認証 Applet サイトに記載されている JavaScript を用いて Web ブラウザに対して一段目の認証結果を保持しつつ Web アプリケーションへリダイレクトするようにした。



3 考察

この IC カード等を用いた多要素 Web 認証とパスワード認証と比べてみる。一般に広く普及しているパスワード認証は、一定数の文字を組み合わせてユーザしか知らない秘密を作り出す。そのためセキュリティの強度を高めるためには扱える文字数を増やすか入力する文字数を増やす或いはなるべく予想できない難解なパスワードを作成することになる。一方、FeliCa カードや USB 機器は世界に無数にあるため、理論的には入力データのバリエーションはパスワード認証よりも高い。そのため、IC カード等を利用した認証は理論的にはパスワード認証と比べても遜色ないセキュリティ強度を持つことができると考える。

運用面の問題点について考察する。パスワード認証は認証情報を基本的に利用者が記憶するためどこでも使えるという利点がある。また、パスワード認証の実装はサービスを提供するサーバ側のみで完了する。しかし IC カード認証は、Web アプリケーションを利用するパソコンで FeliCa カードと USB 機器から情報を取得するため、パソコンに専用のプログラムをインストールする必要がある。加えて FeliCa カードと USB 機器を認識させるために、パスワード入力よりも時間が掛かることは否めない。

また、それほど嵩張るとは思われないが、IC カード等を用いた認証を利用している Web アプリケーションを様々な場所で利用する場合、認証情報を保持している FeliCa カードと USB 機器と IC カードリーダ/ライタを常に携帯する

必要がある。

最後に FeliCa カードと USB 機器のバリエーションは全世界には無数にあるが、一人が所持している FeliCa カードと USB 機器はそれほど多くはない。そのためセキュリティ強度は運用次第である。

認証破りについて考えてみる。パスワード認証を破る簡単な(しかし実行には CPU パワーが掛かる)方法として、ブルートフォース攻撃がある。パスワードに使える文字数は比較的少ないので、この様な攻撃も可能であるが、FeliCa カードと USB 機器が持つ情報は公開されているとはいえ闇雲な総当たり攻撃をするには複雑すぎる。

一方、キーロガーの様にローカルなパソコンの情報を記録して利用する攻撃に対しては、ローカルプログラムで暗号化を施せばある程度耐性ができる。しかし、IC カードリーダ/ライタと IC カードとの情報のやり取りは暗号化できないので、漏洩の可能性が残る。

FeliCa カードと USB 機器の紛失による認証情報の漏えいに関しては公開された情報を利用するので対策の立てようがない。また IC カード等を用いた認証で利用する秘密情報は、機器が所有する情報の組み合わせにある。認証時は、FeliCa カードと USB 機器を他人に見えないように認証を行う事が出来ないので、衆人環視の環境で認証を行う事には適していない。

これらの考察は、実証実験を経ていない段階での考察である。今後実証実験を行いこの認証の問題点を追及していく。

参考文献

[1] JR 東日本、Suica、
http://www.jreast.co.jp/suica/

[2] 株式会社セブン・カードサービス、電子マネー nanaco 【公式サイト】：トップページ、
http://www.nanaco-net.jp/index_pc.html

[3] イオンリテール株式会社、電子マネー｜WAON [ワオン] 公式サイト、
http://www.waon.net/index.html

[4] ソニー株式会社、Sony Japan | FeliCa ホームページ、
http://www.sony.co.jp/Products/felica/

[5] 株式会社ソリトンシステムズ、SmartOn シリーズ、
http://www.soliton.co.jp/products/pc_security/smarton/specification_on.html

[6] ソニー株式会社、フォーマット判別シーケンス設計ガイドライン、Version 1.1、1-2、2010、
http://www.sony.co.jp/Products/felica/business/tech-support/data/format_sequence_guidelines_1.1.pdf

[7] ソニー株式会社、FeliCa 技術方式の各種コードについて、Version 1.2、3、2010、
http://www.sony.co.jp/Products/felica/business/tech-support/data/code_descriptions_1.2.pdf