2006－CSEC－35 (6)
2006／12／8

携帯電話を用いたWebサイトにおけるユーザ認証システム

戸田英貴　宇田隆哉

東京工科大学コンピュータサイエンス学部

本論文では，携帯電話を用いて，電子署名によりユーザを認証し，Webサイトにアクセスする方式を提案する．現在，ネットワーク上の主な認証方式としては，IDとパスワードを用いるものが殆どである．しかし，インターネット社会の発展に伴い，多彩な攻撃方法が開発され，SSLによる暗号化通信に代表されるような，従来の認証による保護では完全に攻撃を防ぐことが出来ない．また，フィシング詐欺やスパイウェアによる攻撃や，キーロガーなどによる脅威を含めると，現状のPC単体での電子署名を用いた認証方式では，なりすましや盗聴を完全に防止することが出来ない状況である．そこで，身近なデバイスで耐タンパ性のある携帯電話でPKIに基づく電子署名を作成し，PCと赤外線通信端末で連携させてWebサイトアクセス時に用いることで，ユーザ認証を行う方式を提案する．

A User Authentication System for Web Sites Using Cellular Phone

Hidetaka Toda,　Ryuya Uda

Tokyo University of Technology School of Computer Science

In this paper, we propose a user authentication system for web sites using cellular phones and digital signature method. The most of existing authentication systems use IDs and passwords to authenticate users. However, the popularization of the internet has brought the creation of various attack methods which break the protection with traditional encrypted communication methods such as SSL. For example, user's password can be stolen through phishing attacks, key loggers and spywares with the aim of impersonating the user, even if authentication systems protect communication channels with encryption methods and digital signatures, since the information is directly stolen from the user or his/her PCs. To prevent such attacks, we propose a user authentication system with combination of PC and tamper resistant cellular phone. In this system, PKI-based digital signatures are calculated in a cellular phone which is more secure than a PC, and then transmitted to PCs via infrared channels. This robust system can be realized with a few additional costs by using cellular phones which are so much familiar with many users.

1. はじめに

近年，ネットワーク社会の進展に伴い，ショッピングサイトや，ネットバンク，行政取引，オンラインゲームなどネットワーク上で様々な取引が行われるようになってきている．殆どのネットワーク上のサービスでは，本人確認方式としてIDとパスワードを用いるのが一般的である．しかし，現状の認証方式では盗聴が容易である上に，なりすましなどを防ぐことが出来ず，パスワード忘却時の対処や，IDを持つデバイスの不正複製，パスワード入力時の利便性の低さなどの問題もある．特にここ数年は，フィッシング詐欺やスパイウェアなどによりIDやパスワードが流出する被害が増加する問題もある．

また，大半の本人認証方式には，SSL通信などにより暗号化された状態で行われているが，キーロガーやトロイの木馬などに代表されるスパイウェアや，コンピュータウィルスの感染により流出する可能性があり問題となっている．さらに，フィッシング詐欺などにより，本人が厳重に，IDやパスワードの管理を行っていても，知らないうちに情報を流出させてしまう可能性がある．

本提案では身近なデバイスで，耐タンパ性のあるハードウェアの携帯電話端末に着目し，PCと携帯電話端末を連携させたサイトログイン認証方式を提案する．PC端末単体で，電子署名による認証を行う方法は既に確立されているが，公開鍵暗号により秘密鍵を作成した際に，秘密鍵の管理が問題となる．そこで，携帯電話端末において，公開鍵暗号をソフトウェア実装し，耐タンパ性領域内に秘密鍵を保管させ管理を徹底する．PC端末と携帯電話端末を連携させて携帯電話端末内の鍵を使い，電子署名を行うことで，スパイウェアやコンピュータウィルスの脅威から保護する．実際にWebサイトにアクセスするPC端末と，認証に必要な電子署名を行う携帯電話端末と分けることでキーロガーなどに代

表される，スパイウェアの脅威に対抗する．

以下，本稿では第2章において関連研究について，第3章においては提案方式について，第4章において実装方式について解説し，第5章において考察を述べ，最後に第6章でまとめを述べる．

2. 関連研究

本章では，携帯電話端末を利用した認証システムについて解説を行う．既存の研究としては，携帯電話会社によって提供されている，ハードウェア実装による認証，携帯電話端末における，ソフトウェア実装による認証，携帯電話端末のQRコードリーダを利用した2次元コードによる認証などが行われている．

2.1 ハードウェア実装による認証方式

現在，携帯電話を用いた認証方式としては，NTT Docomoの FirstPass[1]や，KDDIの SecurityPass[2]などのサービスが実現されている．双方のサービスとも公開鍵暗号の利用可能な接触型ICチップ(SIMカード)を搭載したハードウェア実装を行っている．FirstPassは，FOMAカードと呼ばれるICチップを利用することによりクライアント認証を実現している．同様に，SecurityPassについてもICチップを利用したクライアント認証を実現しており，イーバンク銀行などのコンテンツに活用されている．

しかし，双方のサービスは携帯電話会社に依存された環境である為に，利用制限があり，利用出来るサービスや，利用事業者が限定されている．

2.2 ソフトウェア実装による認証方式

携帯電話会社に依存せずに認証を行う研究として，公開鍵暗号をソフトウェア実装し，Felicaによる相互認証するシステム[3]などや，携帯電話を用いて本人認証を行い，出席を管理するシステム[4]などの研究がある．Felicaによる相互認証システム[3]では，ソフトウェア実装により作成した公開鍵を認証局に登録し，クライアント証明書を発行する．発行された，クライアント証明書と公開鍵をFelicaチップの領域に格納し，ゲートに翳す時に双方の証明書と公開鍵を交換し，お互いに認証を行うという相互認証システムである．独自にソフトウェア実装を行うことで，携帯電話会社に依存せずに公開鍵暗号方式を適用させた研究である．

しかし，利用者制限の無いFelicaのフリー領域を対象とした研究である為，送受信可能なデータはわずか，512bitであり，使用出来る公開鍵暗号方式の種類が限られる．また，携帯電話とゲート間で相互認証する際には，ICチップの捕捉，対象領域の読込，演算，書込，解放といった流れを相互に複数回繰り返す必要があり，認証の際には通常のFelicaのように翳すだけでは処理出来ない．

出席管理の研究[4]は，公開鍵暗号のソフトウェア実装と，2次元バーコードの一つであるQRコードを利用した出席管理システムである．授業毎に異なる制限時間付きQRコードを発行し，携帯電話で読み取り，そのデータに対して署名を施す手法を用いている．署名はサーバに送信し，サーバ側で署名の検証をするというシステムである．この研究は，携帯電話の固体識別番号を利用している為，機種変更をした場合に申請をし直す必要がある．また，電波の入らない状況では，サーバと通信できないため正確に出席を判断することが出来ない．さらに，QRコードを用いた出席方法である為，QRコード自体を外部にメールなどで流した場合，外からでも出席が可能であるなどの問題点もある．

2.3 2次元コードリーダによる認証方式

携帯電話に対してハードウェア実装や，ソフトウェア実装することなく，2次元コード読取機能を使用したユーザ認証方式として，PCと携帯電話端末を連携させ2次元コードリーダを活用したユーザ認証方式[5]などがある．利用者端末のブラウザにワンタイムトークンである2次元コードを表示させ，携帯電話で2次元コードを読み取り，その内容を認証サーバに送信することにより認証を行う方式である．

PC端末上では，パスワードを入力することは無いので，キーロガーなどのスパイウェアやフィッシング詐欺によるユーザ認証情報の盗聴を防止出来る．しかし，通信経路上でのMan-in-the-middle-attack型のフィッシングによる盗聴は防ぐことが出来ない．また，この研究も携帯電話の電波が入らない所では使用することが出来ない．

3. 携帯電話を用いたWebサイト認証

本章では，2章で述べた関連研究での問題点である，公開鍵暗号方式の使用種類の制限，使用環境及び使用状況の制限，通信経路における盗聴，といった問題を踏まえて，携帯電話を用いたWebサイト

認証についての提案方式を説明する．携帯電話は，PC と比較すると使用可能なアプリケーションが限られており，アクセス制限も多い．また，携帯電話には不揮発性領域もあり，不揮発性領域を利用することでアクセスが困難になるので，耐タンパ性があると言える．そこで，携帯電話を鍵生成，署名生成，秘密鍵を保管する端末として扱い，実際の Web サイトへのアクセスはPC端末で行うシステムを提案する．実際アクセスする端末を分けることで，携帯電話の電波が届かない場所でも使えるように環境を整える．ただし，公開鍵の登録は電波の届く状況で行わなければならない．尚，PC 端末と携帯電話間は赤外線通信で接続する．赤外線通信は，一度の通信で送信できるデータ量に特に制限が設けられているわけではないためデータ量が増大したとしても複数回の通信を必要としない．

3.1 システム概要

本システムは，携帯電話，PC 端末，Web サイト，認証局から構成されており，携帯電話と PC 端末を連携させて認証を行う．利用者はあらかじめ，Web サイトへユーザ登録後，認証用アプリを携帯電話にダウンロードする．携帯電話端末では公開鍵暗号による鍵生成，署名の生成を行う．PC 端末では，赤外線通信を使用して，携帯電話からサイトログイン時に必要な電子書名などのやりとりを行う．PC 端末では，パスワードなどの情報の入力は一切行わない．図 1 にシステム全体の概要図を示す．

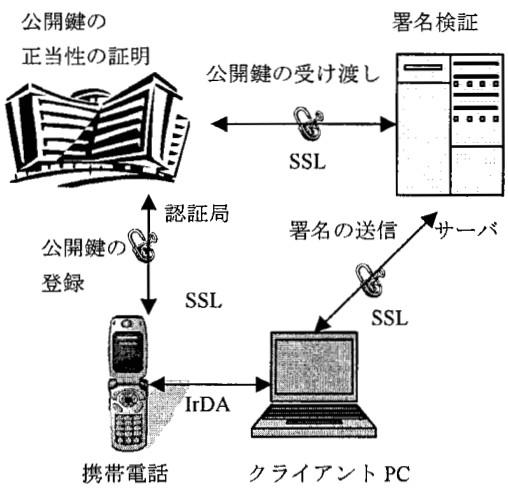

図 1　システム全体概要図

図 1 のように，利用者は携帯電話端末と PC 端末を利用する．認証に関しては，携帯電話端末に公開鍵暗号をソフトウェア実装させて，公開鍵，署名生成を行う．携帯電話端末は，認証局への公開鍵の登録以外に特に通信は行わない．認証に必要な電子署名は，PC 端末が Web サイトにアクセスする際に，セッション毎に Seed を生成し，Seed に対して，携帯電話により電子署名を生成する．作成された電子書名を，PC 端末を経由して Web サイトに送信し認証を行う．

3.2 公開鍵暗号のソフトウェア実装

既存研究[3][4]で取られている手法を参考に，BouncyCastle[6]を携帯電話アプリ用に移植する．電子署名には，RSA[7]と ECDSA[8]の双方を対象として実装する．公開鍵暗号をソフトウェア実装することで，携帯電話会社に依存せずにサービスを提供できる．

3.3 鍵生成と公開鍵の登録

鍵生成と公開鍵の登録は，携帯電話端末上で行われる．公開鍵暗号方式により，秘密鍵と公開鍵の鍵ペアを生成し，公開鍵は認証局に登録を行い，ユーザの公開鍵に対して認証局が正当性を証明する．秘密鍵を流出させてはならないので，携帯電話上のスクラッチパッド領域に保存する．スクラッチパッドとは，携帯電話におけるアプリ毎に割り当てられた，データ保存，データ取得が出来る不揮発メモリの一部を利用したものである．アプリ毎に，使用領域が割り当てられるので，他のアプリからデータにアクセスすることが出来ない．不揮発メモリを使用しているため，電源をオフにしてもデータは残される．現行機種である，NTT DoCoMo FOMA 902i シリーズでは，スクラッチパッド領域は 400KB である．秘密鍵をスクラッチパッド領域に保存させておくことで，次回以降の起動時に新たに鍵生成を行う必要がなくなる．図 2 に鍵生成と公開鍵登録の流れの詳細を示す．

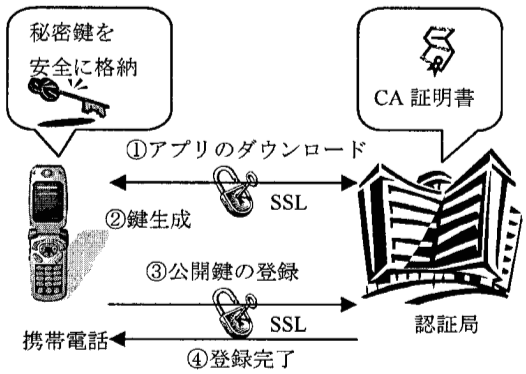

図 2 鍵生成と公開鍵の登録

鍵生成時に使用する暗号化方式は，RSA[7]または ECDSA[8]を使用する．RSA[7]については 1024bit 以上の鍵長を持たせる．ECDSA[8]については 160bit 以上の鍵長を持たせる．双方の鍵長は，電子署名法に基づく特定認証業務認定に係る指数に基づく．

3.4 PC とサーバのセッション確立

PC とサーバ間の通信経路では，Man-in-the-middle-attack や，Replay-attack などの攻撃が考えられるので，SSL による暗号化通信により通信を行う．図 3 に PC とサーバ間のセッション確立の流れの詳細を示す．

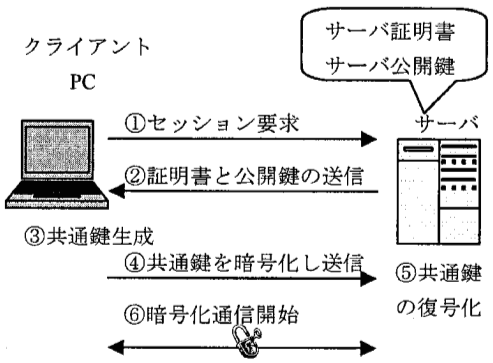

図 3 PC とサーバのセッション確立

サーバは上位認証局により認証されているものとする．サーバ公開鍵により，共通鍵を生成させることで，サーバにしか暗号を解くことが出来ない．

3.5 署名と検証

署名と検証については，3.4 節で述べたように通信経路内での攻撃が考えられるので，セッション毎に Seed を生成し，Seed に対して携帯電話内で秘密鍵により署名を施すことにより対処できると考えられる．図 4 に署名と検証の詳細を示す．

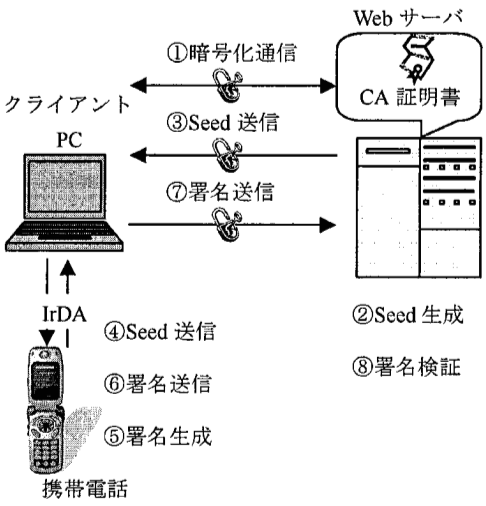

図 4 署名と検証

図 4 では，まず，クライアント PC とサーバ間で SSL による暗号化通信を行い，セッションを張る．サーバ側では，セッション毎に Seed を生成する．作成された Seed は，PC 端末を経由し，赤外線通信で携帯電話に送信する．携帯電話では 3.3 節で作成した秘密鍵により Seed から署名を生成し，PC 端末を経由してサーバに送信する．サーバは送信された署名を，署名検証時に，ユーザの公開鍵を認証局から取得し，検証を行う．検証が成功すれば，ログイン認証成功となる．

セッション毎に Seed を生成し，Seed に署名を付与することで，Replay-attack に対処出来る．

4. 実装

4.1 公開鍵暗号のソフトウェア実装

本研究の開発では，NTT DoCoMo の Java が動作する FOMA 端末を使用し，既存研究[3][4]を参考に，実装を行った．公開鍵暗号ライブラリは OpenSource で公開されている BouncyCastle[6]を使用した．BouncyCastle をベースに DoJa4.0 向けにコードの再構築を行い，NTT DoCoMo が提供する携帯電話に対応させている．公開鍵暗号方式は，電子署名法に基づく鍵長を持った，RSA[7]もしくは，ECDSA[8]を実装した．RSA は，RSA-PSS を使用し，ECDSA は，SEC1 及び，ANSI を使用した．SEC1 と ANSI

の署名スキームは同一である．SEC1 はランダム曲線の他に Koblitz 曲線を推奨し，ほとんどの曲線でパラメータ a を固定している．ANSI は，サンプルとしてランダム曲線と Weil 法によって生成された曲線を掲載し，曲線パラメータ a もランダムである．

4.2 公開鍵の登録

システムを利用する前に登録を行い，4.1 節での公開鍵暗号のソフトウェアを実装したアプリケーションをダウンロードし，鍵ペアの生成を行う．秘密鍵はスクラッチパッド領域内に保存させる．スクラッチパッド領域に保存させることで，秘密鍵漏洩を防止する．公開鍵は SSL 通信を利用し，認証局へと登録する．携帯電話上の i アプリ通信は，基本 i アプリのダウンロード先しか接続出来ないので，公開鍵登録の通信経路については通常の PC による接続より安全であると考えられる．公開鍵の登録には，ID として SIM カードの識別情報を用いて登録を行う．SIM カードを ID として用いることで，偽造防止や，複数 ID の生成を防ぐ．

4.3 署名と検証

署名と検証を行うために，サーバからの Seed を携帯電話に受け渡し，携帯電話からの署名をサーバに受け渡すクライアント PC 上のプログラムを作成する．サーバからクライアント PC 間の接続は，HTTP による通信で行う．クライアント PC から携帯電話間の通信は，USB の赤外線通信ポートを利用し，赤外線通信で通信を行う．クライアント PC 上のプログラムを起動させ，サーバにアクセスすると，暗号化通信経路を構築した上で，サーバから生成された Seed が送信される．この Seed は，サーバ上で自動的に生成されるセッション ID とは別物である．Seed は Secure Random を使用し，128bit の乱数を生成する．生成された Seed はプログラムが，サーバへのセッション保持中のみ有効となる．ただし，途中でプログラムが切断された場合は，新規セッションとなり，Seed 値は新しいものとなる．サーバはセッション毎に Seed を生成する．

Seed による署名作成方法については，図 5 に詳細を示す．サーバから送信された Seed を，クライアント PC を経由して赤外線通信を通し受信し，Seed をハッシュ化する．得られたハッシュ値に対して，ユーザの携帯電話内のスクラッチパッド領域内に保存された秘密鍵を用いて暗号化を行い，生成された署名をサーバに送信する．

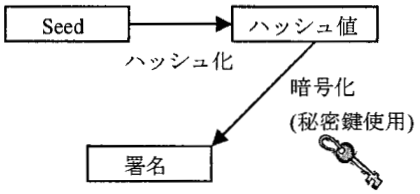

図 5　Seed による署名生成方法

サーバ側での署名検証方法を，図 6 に示す．携帯電話上で作成された，署名が付与された Seed を受信する．受信した Seed はハッシュ化し，ハッシュ値を得る．署名は，ユーザの公開鍵を認証局から請求し，ユーザの公開鍵により復号化する．復号化されたハッシュ値と，サーバ上での Seed のハッシュ値を比較し検証する．

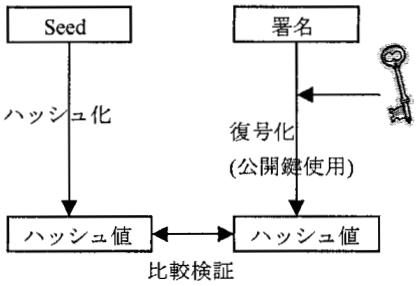

図 6　署名検証方法

署名検証の結果，検証に成功すれば，ログインの許可をクライアン PC に送信する．署名検証が失敗した場合は，ログインが出来ない．

5. 考察

本提案では，携帯電話端末を，Web サイトでのユーザ認証を行う為のデバイスとし，スクラッチパッド領域に秘密鍵を保管する．秘密鍵の格納場所を，PC 端末と分けることで PC 端末への攻撃に対処し，尚且つ，秘密鍵を安全に保管出来ると考えられる．また，SSL 上でセッション毎に，ワンタイム Seed を生成し，Seed を利用した署名による認証をすることで，データが途中で盗聴されることがないので Man-in-the-middle-attack や，Replay-attack に対処出来ると考えられる．PC 端末上では，ID やパスワードなどの情報を一切入力しないので，スパイウェアなどにも対処できると考えられる．

このシステムは赤外線通信を使用した認証システムである為，Felica などのように翳すだけでは通信が出来ない．そのため，赤外線通信を行うデバイス同士を探し出し，接続するまでに多少の時間を必要とする．しかし，赤外線通信は，Felica では扱える領域が限られていたが，送受信するデータ量に制限はない．

使用する際には，公開鍵登録時のみパケット通信を行う．Web サイトのユーザ認証に必要な電子署名の生成については，パケット通信を用いずに行うので，電波の届かない場所や，弱い場所でも使用出来ると考えられる．

通信経路においては，サーバ認証による SSL 通信を利用しているが，クライアント認証も取り入れることが可能である．クライアント認証も加えることで更に，盗聴などの攻撃が困難になると考えられる．

6. まとめ

現在の段階で，一部の機種で部分的に評価を取った状態であるので，今後は NTT DoCoMo の現行機種である 902i シリーズを中心に評価を取っていく予定である．実装し，性能評価をすることで問題点が新たに発生した場合は随時修正して完成度を高めていく．

また，本提案では，携帯電話会社に依存することなく，公開鍵暗号を実装しているので特に利用制限はない．また，Bluetooth などのデバイスが利用可能になれば，そちらにも対応可能である．今後は，赤外線通信以外での他のデバイスを用いた実装の検討を行っていく予定である．

今後の課題として，機種変更などに対応する為，902i シリーズから提供されている SD-Binding を使用し，アプリごと外部メモリである SD カードに保存することも検討中である．外部メモリに保存する場合は，SIM カードに関連付けして暗号化処理することで，暗号化した SIM カードにしかアプリを起動出来ない状況にする．秘密鍵の保管場所も，外部メモリに設定し，暗号化を施すことで情報漏洩の防止が出来ると考えられる．しかし，SIM カードに関連付けした暗号化がどれ程の耐性を持っているかは，未知数であるので今後の検討事項としたい．

参考文献

1 ） NTT DoCoMo FirstPass
http://www.nttdocomo.co.jp/service/other/firstpass/index.html

2 ） KDDI au SecurityPass
http://www.au.kddi.com/notice/securitypass/index.html

3 ） 尾崎啓，宇田隆哉，棟上昭男：公開鍵暗号による携帯電話を用いた相互認証システム，情報処理学会コンピュータセキュリティシンポジュウム 2005，pp.535-540 (2005)

4 ） 琴浦崇，宇田隆哉，星徹，松下温：携帯電話を用いた出席率を向上させる出席管理システム，情報処理学会 DICOMO2006 論文集，pp.881-884(2006)

5 ） 田中充，勅使河原海：携帯電話の 2 次元コードリーダを活用したユーザ認証方式と個人情報入力機構，情報処理学会コンピュータセキュリティシンポジュウム 2005，pp.691-696(2005)

6 ） BouncyCastle
http://www.bouncycastle.org/

7 ） R.L. Rivest, A. Shamir and L. Adleman : A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Communications of ACM, v. 21, n.2, pp. 120-126, Fed 1978

8 ） American National Standards Institute : Public Key Cryptography For Financial Services Industry, The Elliptic Curve Digital Signature Algorithm(ECDSA),1998