コンピュータセキュリティ 19－9
（２００２．１２．２０）

モバイル個人認証方式の提案と実装

桜井　鐘冶†　　高橋　渉‡

携帯電話を用いて個人認証を行う際には，入力上の制約から複雑なパスワードの入力は難しい．一方，モバイル環境ではパスワードの入力を悪意の第三者に盗み見られるショルダーハッキングの危険もあり，4 桁程度の固定の暗証番号による認証では企業内情報の参照やモバイルコマースの認証にはセキュリティが不十分である．本稿では，このような問題に対して，携帯電話上の Java アプリケーションを利用してサーバからのチャレンジ値を表示し，これに対し利用者が本人の記憶するパスワードをもとに入力する認証データをレスポンス値として利用する認証方式を提案し，その評価と実装時のポイントについて報告する．

Authentication Methods for Mobile Phones

Shoji Sakurai†　　Wataru Takahashi‡

For user authentication using a mobile phone, it is difficult to input a complicated password from a keypad. So, it is widely used to input a 4-digit number as a password. But in mobile environment, there is a risk of shoulder hacking which is the simplest way to steal a password. This paper presents authentication methods using challenge-response technique which protect password leak. By using these authentication methods, it is possible to input authentication data from a keypad safely whenever malicious people watch the input.

1. はじめに

近年，携帯電話のめざましい普及により，今や携帯電話は一人に一台の環境がごく普通に考えられるようになってきている．これに伴い，法人ユーザにおいては携帯電話を使って企業内情報をアクセスしたいというニーズが高まっている．また，個人ユーザにおいても携帯電話からオンラインショッピングやオンラインバンキング，オンライントレードなどのいわゆる e コマースを利用することが盛んに行われるようになっている．

しかしながら，携帯電話を用いて個人認証を行う際には，端末への入力上の制約からパソコン等で通常使用している英数字特殊文字が混在した複雑なパスワードの入力は難しい．このため，携帯電話ではパソコンでの認証パスワードとは別に４桁程度の数字からなる暗証番号が利用されているが，ユーザにとってはこの暗証番号を新たに記憶することを強いられる．また，モバイル環境ではパスワードの入力時に悪意の第三者にパスワードを盗み見られるショルダーハッキングなどの危険もあるため，入力数値を画面上に表示しないようにしても 4 桁程度の毎回同じ暗証番号では企業内の重要情報などにアクセスする際や e コマースを利用する際にはセキュリティが十分とは言い難い．

本稿では，モバイル環境において生じるこのような認証の問題点を解決するために，携帯電話で実現可能な認証方式を提案する．

以下，2 章では，モバイル環境での個人認証のモデルを定義し，3 章では認証に必要な要件を整理する．4

†三菱電機（株）情報技術総合研究所
〒247-8501 神奈川県鎌倉市大船 5-1-1,
Information Technology R & D Center,　Mitsubishi Electric Corporation
Ofuna 5-1-1, Kamakura, Kanagawa, 247-8501 Japan
‡三菱電機インフォメーションシステムズ（株）
〒247-8520 神奈川県鎌倉市上町屋 235
Mitsubishi Electric Information Systems Corporation
Kamimachiya 325, Kamakura Kanagawa, 247-8520 Japan

章ではこれらの要件を当てはめて従来認証方式の問題点を示す．5 章ではこれらの要件を満たす認証方式を提案する．6 章では提案認証方式のセキュリティ強度についての考察と実装時のポイントの検討を行う．最後に 7 章でまとめと今後の課題を示す．

2. モバイル環境での個人認証のモデル

モバイル環境を考えた場合には，ユーザが利用するデータやサービスはユーザが使用する携帯端末から無線ネットワークを介して接続されるサーバで提供される．このため，モバイル環境での個人認証のモデルは図 1 に示すように認証される主体のユーザとこれを認証するサーバとさらにこれらの間に位置する携帯端末から構成されると考えられる．

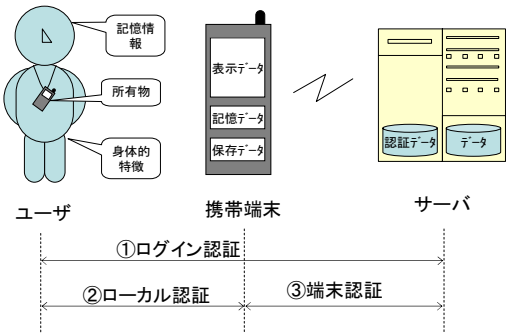

図 1　モバイル個人認証のモデル

サーバには，ユーザに提供されるサービスのデータとこれを利用するユーザを認証するための認証データが保存される．携帯端末には画面上の表示データ，揮発性メモリ上の記憶データ，不揮発性メモリ上の保存データの３種類のデータが存在する．ユーザには，大別すると,暗証番号やパスワードなど本人しか知り得ない記憶情報，物理的な鍵や ID カードなど本人しか持ち得ないはずの所有物，他人とは異なる指紋や虹彩など身体的特徴の三種類が存在する．

また認証の種類としては，

① サーバによるユーザの認証

② サーバによる端末の認証

③ 端末によるユーザの認証

の３つの認証が存在する．以降ではそれぞれを，ログイン認証, 端末認証, ローカル認証と呼び区別する．なお本稿では，ユーザを認証の主体とする①と③について要件を整理する．

3. モバイル個人認証に必要な要件

モバイル環境における個人認証に必要な要件として以下を設定する．

(1) 認証手順・操作を見られても構わないこと

モバイル環境での認証を考えた際に，認証の際に手順を第三者に見られることは普通に予想される．このため，仮に認証手順や操作を見られてもセキュリティ上問題が生じないことが必要である．

(2) 認証情報が漏洩しないこと

モバイル環境では常に携帯端末の紛失や盗難の危険がある．このため，紛失や盗難の際にもし携帯端末を分解されてもユーザの認証情報が漏洩しないことが必要である．

(3) 携帯端末上で実施可能なこと

モバイル環境での認証であるため，認証方式は携帯端末上で実施が可能な方式であることが必要である．

さらに，以下の要件を満たすこともモバイル認証には必要と考えられる．

(4) ローカル認証が可能であること

ログイン認証の際に必ず携帯端末とサーバの間で無線での通信が必要となるが，圏外などの場合もあり常に通信ができるとは限らない．このため，サービスに必要なデータが携帯端末上に存在する状態ではローカル認証が可能であることが必要である．

4. 従来の認証方式の問題点

携帯端末として普及台数が最も多い携帯電話を利用するとした際に，現在利用されている個人認証方式に 3 章で示した４つの要件を当てはめてみる．

● パスワードの入力による認証の問題点

パスワードの入力による認証方式は，企業や家庭の PC へのログインなど多くの場合に利用されているが，携帯電話の場合にはパスワードを携帯のキーからの入力する際に入力モードの切り替えが必要であり，入力文字を第三者に見られないように'＊'などに置き換えて表示すると正しく入力することが難しい．一方，入力されるパスワードをそのまま画面に表示するとパス

ワードを盗み見られる危険性があり，前述の要件(1)を満足できない．また，要件(4)のローカル認証を実施するためには，携帯電話に何らかの認証情報を格納することが必要であるが，この場合には携帯電話からの認証情報の漏洩が懸念されるため，要件(2)を満たすためには，携帯電話内に IC カード等の耐タンパ性のある記憶デバイスが必要となる．

- **暗証番号の入力による認証の問題点**

パスワードを４桁程度数字のみに限定した暗証番号による入力は，銀行の ATM などで利用されているが，入力が数字に限られているため，入力値を第三者に見られないよう多くの場合画面には'＊'に置き換えて表示される．モバイル環境を考えると，入力数字そのものを画面に表示しなくても，キー入力より暗証番号が盗み見られる危険性が高く要件(1)を満足できない．このため，最近モバイルバンキングなどでは暗証番号とあわせて，乱数カードが併用されているが，このカード上には第三者には公開してはならない情報が印刷してあるため，認証操作は他人に見られないように行うことが必要である．また，パスワードと同様にローカル認証を実施するためには，携帯電話内に耐タンパ性のある記憶デバイスが必要である．

- **生体情報による認証の問題点**

生体情報による認証は，建物での入室管理などで利用されているが，虹彩や声紋などを認証情報に使用したものについては装置が大掛かりになり高い処理能力も必要とされるため，携帯電話では大きさや処理能力が問題となり要件(4)を満足できない．指紋認証装置については近年その小型化が進んでおり，既に IC カードに内蔵されたものも登場している[1]．今後，体型の装置も携帯電話への搭載が期待されているが，一方では指紋認証のなりすましの危険も懸念されている[2]．このため，指の静脈パターンを利用した認証装置も開発されているが認証装置大きさの点で現状では要件(3)を満足できない．また，生体情報をネットワーク上で盗用された際に認証データの更新ができないことも問題点として指摘されている[3]．

このように現状の認証方式では，3 章に示したモバイル個人認証に必要な要件を満たしてはいない．

5. 認証方式の提案

5.1. 認証方式と認証画面

本稿では，3 章で示した要件を満たす認証方式として，ユーザの検索能力と計算能力を利用し，携帯端末への直接的なパスワードの入力を排除した認証方式を提案する．

提案方式では，携帯電話上の Java アプリケーションで画面上に複数のチャレンジ値を順次表示し，これに対してユーザが本人の記憶するパスワードをもとにキーから入力する認証データを使って認証を行う．

認証データを生成する方式としては，図 2 に示すように，キーから入力する１つの認証データを１つのチャレンジ値より生成する方式（以下，方式１と呼ぶ）と１つの認証データを２つのチャレンジ値より生成する方式（以下，方式２と呼ぶ）の２つの方式を提案する．図 3 と図 4 にそれぞれの認証画面を示す．いずれの方式においても，認証に使用するチャレンジ値を用いて生成される認証データに偏りが生じないように

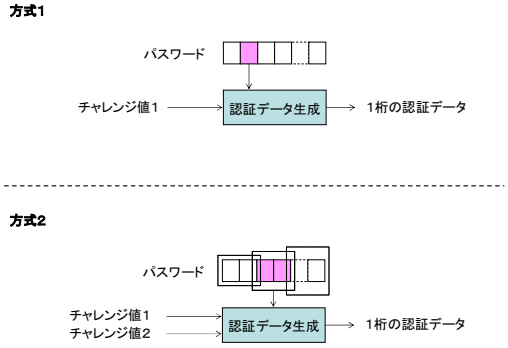

図 2　認証方式の種類

図 3　方式１の認証画面　図 4　方式２の認証画面

１つのチャレンジ値には 0 から 9 までの各数字を１つずつ含む 10 桁の乱数を使用する．

ログイン認証では，サーバで生成した複数のチャレンジ値をユーザに表示し，入力された認証データをチャレンジ値としてサーバに送信し認証を行う．

ローカル認証方式では，前回成功したログイン認証で使用したチャレンジ値とこれに対する認証データを再利用することでサーバとの通信を行わずに認証を行う．

5.2. 方式１の認証手順

図 3 に示す方式１の認証画面には，パスワードに使うことができる文字を含む定数部分の下に認証データを入力する度に毎回変わるチャレンジ値が１つ表示される．

認証を行うユーザは，本人が記憶するパスワードの 1 番目の文字を上段の定数部から探し，その文字と同じ列に位置するチャレンジ値の数値を求めてこれを最初の認証データ *A[1]*として携帯電話の数字キーより入力する．

キーから数字を入力すると，認証画面上のチャレンジ値は即座に次の乱数に更新される．次に，ユーザはパスワードの 2 番目の文字を上段の定数部から探し，同じ列に位置するチャレンジ値の数値を求め，これを２番目の認証データ *A[2]*として入力する．

パスワードの残りの文字についても同じように認証データの入力を繰り返す．図 3 のログイン認証画面の場合には，８番目の認証データ *A[8]*が入力された後にレスポンス値として *A[1]*から *A[8]*までの８桁の認証データがサーバに送られ，認証処理が行われる．

ローカル認証では, Java アプリケーションにより前回成功したログイン認証の *k* 番目のチャレンジ値 *CH[k]*に対し入力された認証データの数値 *A[k]*をもとに, 図 5 に示すチャレンジ値と認証データの変換処理を行う．

まず，*k* 番目のチャレンジ値 *CH[k]*の各桁を要素とする 1×10 の行列を生成し，各要素について，*A[k]*と等しいものを 1 に，それ以外のものを 0 に置き換えた乱数ベクトル *CV[k]*を生成する(a)．次に，新しい *k* 番目のチャレンジ値 *CH'[k]*として各桁の数字の重複のない 10 桁の乱数を生成する(b)．最後に乱数ベクトル

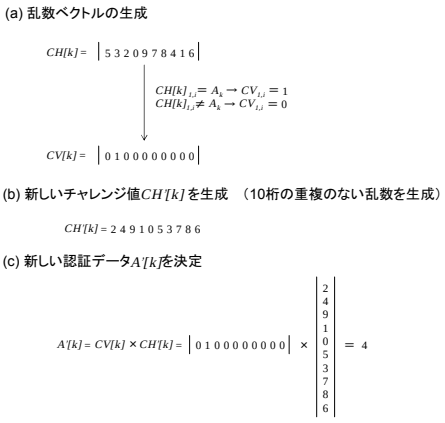

図 5 方式１のローカル認証における変換処理

*CV[k]*と *CH'[k]*の各桁を要素とする 1×10 の行列との積を *k* 番目新しい認証データ *A'[k]*をとする(c)．

ローカル認証では，認証画面の乱数として *CH'[k]*を表示し, これに対して入力される認証データが *A'[k]*に一致するか否かにより認証を行う．

5.3. 方式２の認証手順

図 4 に示す方式２の認証画面には，パスワードに使うことができる文字を含む定数部分の下に認証データを入力する度に毎回変わるチャレンジ値が２つ表示される（以下，*k* 番目の 2 つのチャレンジ値のうち，上を *CHU[k]*，下を *CHD[k]*で示す）．

認証を行うユーザは，本人が記憶するパスワードの最初の文字を上部の定数部から探してその文字と同じ列に位置する *CHU[1]*の数値を求め，次にパスワードの 2 番目の文字を上部の定数部から探してその文字と同じ列に位置する *CHD[1]*の数値を求め，これらの数値の和の一の位を最初の認証データ *A[k]*として携帯電話の数字キーより入力する．

キーから数字を入力すると，認証画面上の 2 つのチャレンジ値は即座に更新される．次に，ユーザはパスワードの 3 番目の文字と同じ列に位置する *CHU[2]*の数値とパスワードの 4 番目の文字と同じ列に位置する *CHD[2]*の数値の和の一の位の数値を 2 番目の認証データ *A[2]*として携帯電話の数字キーより入力する．

パスワードの残りの文字についても使用するパスワードを 2 文字ずつずらしながら同じように認証データの入力を繰り返す．図 4 の認証画面の場合には，4 番目の認証データ *A[k]*が入力された後にレスポンス値

として *A[1]*から *A[4]*の 4 桁の認証データがサーバに送られ，認証処理が行われる．

5.4. 方式２のローカル認証処理

ローカル認証では, Java アプリケーションにより前回ログイン認証に成功した際の *CHU[k]*と *CHD[k]*とこれらに対する認証データ *A[k]*をもとに，図 6 に示すチャレンジ値の変換処理を行いながら認証を行う．

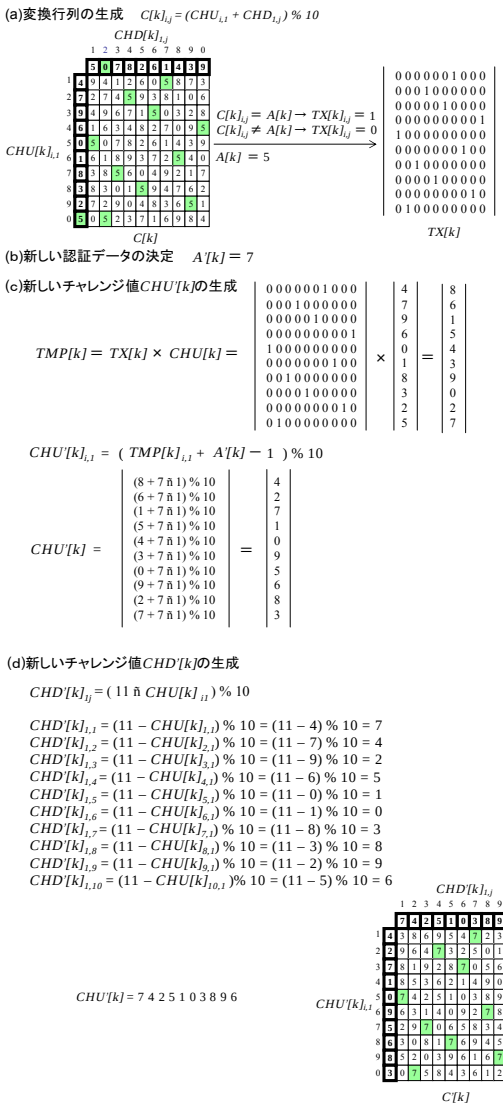

図 6　方式２のローカル認証における変換処理

まず, *CHU[k]*と *CHD[k]*の各桁の和の一の位を要素とする 10×10 の行列 *C[k]*を生成する．次に, 行列 *C[k]*に対して要素が *A[k]*と等しいものを 1 に，それ以外のもの 0 に置き換えた変換行列 *TX[k]*を生成する(a)．次に入力を期待する新たな認証データ *A'[k]*を 0 から 9 までの数値の中から 1 つ適当に選ぶ(b)．さらに *TX[k]*と *CHU[k]*の各桁を要素とする 10×1 の行列とした積 *TMP[k]*の各要素 $TMP[k]_{i,1}$ について先に選んだ *A'[k]*との和から 1 引いた値の一の位を新しいチャレンジ値 *CHU'[k]*とする(c)．最後に，*CHU[k]*の各桁を 11 補数(足して 11 になる値)の一の位の値で置き換えたものを新しいチャレンジ値 *CHD'[k]*とする(d)．

図 6 に示す変換処理により生成される新たなチャレンジ値 *CHU'[k]*と新たなチャンレンジ値 *CHD'[k]*による 10×10 の行列 *C'[k]*と期待する認証データ *A'[k]*から得られる変換行列 *TX'[k]*は先の変換行列 *TX[k]*と同じものになる．このことにより，異なるチャレンジ値を画面に表示しても，パスワードを記憶しているユーザであれば期待した認証データを入力することができるため，ローカルにはパスワードそのものは保存していなくても認証が可能となる．

6. 提案方式の評価

6.1. パスワードクラックに対する強度

ログイン認証のパスワードを 8 文字とすると，方式１は，認証データの桁数が 8 桁となるため，総当りによるパスワードクラックに対して１回の試行で認証が成功する確立は，1/1000 万であり，百分率で示すと 0.000001%である．一方，方式２では，認証データの桁数が 4 桁となるため，これらの値はそれぞれ，1/10000 と 0.01%となる．

通常のログイン認証で行われているように 3 回の連続した認証失敗により，ログインアカウントをロックする運用とすると，方式 1 では，3 回の試行で認証が成功する確率は，3/10000 万，0.000003%となる．一方, 方式２ではそれぞれは, 3/10000 と 0.03%となる．

6.2. 盗み見に対する強度

方式１の場合には，認証データを入力した際に瞬時にチャレンジ値が次の値に変更されるため，例え押下するキーが第三者に分かったとしても，変更される前に認証データを暗記し，認証データがその何桁目に位置していたかを言い当てることは難しく，通常の環境での利用では問題とはならないと考えられる．

しかしながら，ビデオカメラ等を使って認証手順を記録されるような攻撃までを考えた場合には，記録映

像から画面に表示された乱数とこれに対して入力された認証データとを抽出し解析することで，ユーザのパスワードの各文字が画面に表示される定数部分の 10 列の文字グループ中のどれ列属しているかが第三者に明らかにされる．この場合に，ユーザが記憶するパスワード自体は第三者からは一意に特定できないが，8 文字のパスワードでは，推測されるパスワードは 5^8(=390625)通りに限定される．また，不正にアクセスしようとしているものに対しては，パスワードそのものまでは特定できないが，どの列の数字が認証データかは判かるため，認証手順が撮影された場合には要件(1)を満足しておらず，なりすましが可能である．

方式２の場合には，認証データはユーザの記憶するパスワードとチャレンジ値１およびチャレンジ値２の２つの乱数を使って一意に決定されるが，各乱数には 0 から 9 までの各数字を１つずつ含む 10 桁の乱数を使用するため，認証データとして 0 から 9 までのどの数値を入力しても，第三者からはパスワードが何であるかを一意に特定することはできない．

また，ビデオカメラ等を使って認証手順を記録された場合にも，画面に表示される２つの乱数とこれらに対して入力された認証データとを記録映像から抽出しすることはできるが，実際のパスワードがどのグループに属しているかを特定することができないため，なりすましはできない．

6.3. 端末の紛失・盗難に対する強度

ローカル認証を行う際には，前回成功したログイン認証のチャレンジ値とこれに対する認証データを Java アプリケーションで再利用するため, 携帯電話上でこれら記憶する必要があるが，携帯電話の紛失や盗難の際には，端末の分解によりこれらの情報が第三者に知られることが懸念される．この場合に第三者が入手できる情報は，ビデオカメラなどで認証手順を撮影することにより，入手できる情報と同じである．

従って，端末の紛失や盗難の際には，方式１では要件(2)を満足しておらず，なりすましの危険性があるが，方式２ではなりすましの危険性はない．

6.4. 実装時のポイント

これまでの内容から，方式１および方式２を携帯電話上に実装する際のポイントを以下に示す．

方式１については，1 回の認証における全てのチャレンジ値とこれに対する全ての認証データが第三者に知られた際にはなりすましの危険性があるため，ローカル認証の際に再利用するチャレンジ値と認証データについては, Java アプリケーションの実装時にこれらを揮発性のメモリ上にのみ記憶することが必要である．このことにより携帯電話からこれらの情報が漏洩することを防ぎ，要件(2)を満足することができる．

また，ビデオカメラ等を使った認証手順の盗み見による攻撃に対しても要件(1)を満足するためには，ログイン認証の際には上段のパスワード文字の部分を固定とせずに認証毎に文字の並びを変えるようにするなどの工夫が必要である．

方式２については，チャレンジ値と認証データが第三者に知られても認証の強度は変わらない. このため，ローカル認証の際に再利用するチャレンジ値と認証データは Java アプリケーションの実装時に端末の電源を切った際にもデータが保存される不揮発性メモリ上に記憶することができる．これにより電源を立ち上げた直後でもローカル認証が可能となる．

7. まとめ

本稿では，ユーザの検索能力と計算能力を利用し，携帯端末への直接的なパスワードの入力を排除した２つの認証方式を提案し，それぞれのセキュ強度を評価し，実装時のポイントを考察した．特に，認証データの算出に２つの乱数を用いる二つ目の提案方式では，モバイル環境で懸念される認証情報の漏洩を防止するとともに必要とされるローカル認証の機能も提供しており, モバイル環境で有効な認証方法であるといえる．

今後は，携帯電話への搭載が期待されている IC カードとの連携などを検討する予定である．

参考文献

[1] 中川靖司，小松尚久, “ バイオメトリクスによる個人認証技術の現状と課題－金融サービスへの適用の可能性－ ”, 日本銀行金融研究所,Discussion Paper No.99-J-43, 1999

[2] 山田浩二，松本弘之，松本勉, “ 指紋照合装置は人工指を受け入れるか ”, 情報処理学会研究報告, コンピュータセキュリティ，No.10,pp.159-166, 2000

[3] 鹿島一紀, “ 画像の位置情報による本人認証方式の研究開発　画像パスワード GATESCENE(ゲートシーン)，情報処理学会研究報告，コンピュータセキュリティ，No.10,pp.121-127,2000