社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2007－ＣＳＥＣ－38（15）
2007／7／19

# ウェブアクセス時における携帯電話を用いた相互認証システム

澤谷 雪子　山田 明　三宅 優

株式会社 KDDI 研究所 〒356-8502 埼玉県ふじみ野市大原 2-1-15

E-mail: {yu-sawaya, yamada.akira, miyake}@kddilabs.jp

**あらまし** 現在，ウェブアクセス時におけるクライアント認証方法は，ウェブサーバが管理しているユーザ ID とパスワードをユーザがキーボードで入力し，ウェブサーバ側の認証システムが検証を行う方法が主流である．しかし，ユーザ ID とパスワードがスパイウェアやキーロガーなどにより盗聴される被害や，フィッシングサイトによりユーザが入力したユーザ ID とパスワードが盗難される被害が近年増加しているため，これらの対策として，サーバ認証方式及びクライアント認証方式の強化が求められている．そこで，パソコンのディスプレイに表示される QR コードを携帯電話が読み取り，読み込んだ情報から各携帯電話に割り当てられた固有の情報を基にしてクライアント認証情報を生成し，それを携帯電話会社が管理するキャリアサーバを経由してウェブサーバに送付する相互認証システムを提案する．提案システムは，携帯電話の一意性によるクライアント認証を実現するとともに，キャリアサーバ経由で認証情報を転送することにより，サーバ側の認証も実現した．また，携帯電話が通信圏内にある場合はパケット通信によりキャリアサーバと接続し，ユーザの利便性を向上させるとともに，通信圏外の場合においても，インターネット経由による相互認証を可能とするシステムとした．本稿では，提案方式のシステム構成，および，各構成要素間での処理手順について説明する．

**キーワード** クライアント認証，サーバ認証，相互認証，スパイウェア，フィッシング

# A Mutual Authentication System for Web Server Access by Using Cellar Phone

Yukiko SAWAYA　Akira YAMADA　Yutaka MIYAKE

KDDI R&D Laboratories, Inc.　2-1-15 Ohara, Fujimino-shi, Saitama, 356-8502 Japan

**Abstract** Password authentication is widely used for web accesses currently. However this authentication scheme becomes insecure, because attacks for stealing User ID and password are increasing, which use spyware or phishing sites. To resolve this problem, the safer server authentication and client authentication are required.

We propose a mutual authentication system for web server access by using cellar phone. This system has four phases. The first phase is that the cellar phone of the user gets the server information by taking a picture of QR code, which is offered by web server, and verifies whether the server is legitimate. The second phase is that the client information is made by cellar phone ID number and sent to the server which is located in carrier of the cellar phone. The third phase is that the carrier server specifies the user by the client information, and sends the client ID, which is shared between web server and carrier server, to the web server. The fourth phase is that the web server verifies the client ID, and the authentication is finished. This paper describes the components of the proposed system and the framework of communication for the mutual authentication.

**Keyword** client authentication, server authentication, mutual authentication, spyware, phishing

## 1. はじめに

現在，ウェブアクセス時におけるクライアント認証方法は，ウェブサーバが管理しているユーザ ID とパスワードをユーザがキーボードで入力し，ウェブサーバ側の認証システムが検証を行う方法が主流である．

近年，インターネットの普及により，ウェブアクセス時にクライアント認証を必要とするオンラインサービスが多様化しており，オンラインショッピングやインターネット銀行などの金銭を取り扱うサービスも年々増え続けている．それに伴い，ユーザ ID とパスワードがスパイウェアやキーロガーなどにより盗聴される被害や，フィッシングサイトにより盗難される被害の件数も増大している．これらの対策として，サーバ認証方式及びクライアント認証方式の強化が必要とされている．

サーバ認証方式としてドメイン名に対して発行される SSL サーバ証明書をクライアント側で検証する SSL 通信が広く利用されている．しかし，最近では SSL サーバ証明書を持ったフィッシングサイトも出現しており，SSL の信頼性が低下している．

また，クライアント認証方式として，ユーザ ID 入力による知識認証に加え，ワンタイムパスワード生成器が生成したパスワードの入力により所持認証を行う二要素認証が広く使われ始めた．ワンタイムパスワー

ドでは，パスワードが盗聴されたとしても問題は無いが，常にワンタイムパスワード生成器を所持する必要があるため，簡易性に欠ける．

そこで，現在インターネットユーザの大半が所持している携帯電話を利用し，ウェブサーバの認証と，携帯電話からの情報をウェブサーバ側の認証システムに送信するクライアント認証の両方の機能を持った相互認証方式が提案されている．

この方式において，認証サーバとユーザの携帯電話は認証情報を送受信するが，そのためには携帯電話と認証サーバはユーザのパソコンを介して通信を行うか，または携帯電話が直接パケット通信や電話回線網による通信を行い認証サーバと情報を送受信するかのいずれかの方法をとらなければならない．しかし，前者は携帯電話とパソコン間で赤外線や Bluetooth などの双方向通信デバイスを用いて双方向通信を行わなければならず，これらの双方向通信デバイスを持たないパソコンでは，新たな外部機器を準備しなければならない．また，USB ケーブルでパソコンと携帯電話を接続する方法も提案されているが，接続に手間が掛かる．後者は，認証サーバに携帯電話固有の ID 情報や携帯電話番号などの携帯電話に関する情報を提供しなければならず，さらに，海外や地階などの通信圏外にいる場合や，電波発信のモードをオフにしている場合などに利用ができない．

そこで，本稿では，パソコンのディスプレイに表示される QR コードを携帯電話が読み取り，読み込んだ情報からクライアント認証情報を生成し，携帯電話会社が管理するキャリアサーバを経由してウェブサーバに送付する相互認証システムを提案する．本方式では，携帯電話は QR コードを読み取る機能のみが必要となるため，パソコン側に対して赤外線や Bluetooth 等の双方向通信機能の具備を要求しない．また，ケーブル等によるパソコンと携帯電話との接続も不要である．サーバ認証に関しては，ウェブサーバの信頼性を携帯電話内のウェブサーバリスト，および，キャリアサーバで確認しているため，不正なウェブサーバへアクセスを行うと，ユーザに即座に警告される．また，クライアント認証は，携帯電話が無ければ認証されない仕組みとなっているため，パソコンの操作や表示される画面等が盗まれたとしても問題ない．さらに，通常の場合は QR コードを読み込んだ携帯電話がパケット通信によりキャリアサーバと情報を交換することを想定しているが，通信圏外においても，QR コードを読み込んだ後に携帯電話画面に表示される情報を，インターネットを経由してキャリアサーバに送付することにより，同等の認証が可能になっている．

本稿では，提案方式の構成，および，処理手順について説明を行う．

## 2. 携帯電話を利用した認証に関する従来技術

携帯電話を利用したクライアント認証では，以下の二つの認証方法を用いた二要素認証方式が用いられている．

(1)携帯電話を所持していること（所持認証）
(2)ユーザがパスワードを知っていること（知識認証）やユーザの生体情報（生体認証）

文献[1]の製品はユーザがパソコンからアクセスした際に認証サーバから提供されるセッション情報を含む QR コードを携帯電話で読み込み，携帯電話固有の ID 情報とともに暗証番号や声紋認証，指紋情報などのクライアント認証情報を認証サーバへ送信するクライアント認証システムである．このシステムはユーザがパスワードをパソコンのキーボードで入力する必要がないため，スパイウェアやキーロガーによるパスワードの盗聴は防止できるが，携帯電話が圏外である場合には利用できない．また，認証サーバがユーザの携帯電話の情報を管理する必要があるという問題点がある．

文献[2]のサービスは，パソコン画面に表示される QR コードを読み込むことによりセッション情報を取得し，携帯電話固有の ID 情報，および，固定パスワードとともに認証サーバへ送信するクライアント認証システムである．携帯電話が圏外の場合には，あらかじめ圏内にいる間に携帯電話が取得しているワンタイムパスワードと，固定パスワードをユーザがパソコンのキーボードで入力することにより認証を行う．これは，ワンタイムパスワードをあらかじめ入手しておく必要があり，そのワンタイムパスワードには期限が設けられているため，長期間の海外滞在の場合などには利用できない．

次に，携帯電話を利用したサーバ認証として，携帯電話がウェブサーバから得たサーバ情報を保存しているサーバ情報と照合することによりサーバの正当性を確認する方式がある．

文献[3]はウェブサーバから入手したサーバ認証情報をパソコンから Bluetooth を利用して携帯電話へ転送し，携帯電話がサーバの検証を行った後に携帯電話から署名と公開鍵証明書をパソコン経由でウェブサーバに送信するものである．このシステムは携帯電話が圏外の場合にも利用できるが，パソコンと携帯電話を接続する際に Bluetooth を利用しなければならず，さらにブラウザの修正を必要とするため，簡易性に欠ける．

文献[4]は，クライアント認証とサーバ認証を，携帯電話を利用して行う相互認証システムである．これはウェブサイトからの認証情報の要求をパソコンから携

帯電話へ赤外線通信を用いて送信し，あらかじめ携帯キャリア網経由で入手したウェブサイト検証情報を使ってサーバ認証を行い，ワンタイムパスワードを携帯電話内で生成しパソコン経由でウェブサーバへ送信する方法である．

このシステムは[3]同様，携帯電話が圏外の場合にも利用できるが，パソコンと携帯電話を接続する際に赤外線通信を行わなければならず，赤外線通信機能を持つパソコンでなければならない．

## 3. システム構成

本章では，2 章において明らかにした問題点を解決した相互認証システムの構成について述べる．

### 3.1. 要件

今回提案する相互認証システムは，クライアント認証の対象となる携帯電話を所有しており，それを操作可能であることを証明することによりクライアント認証を行い，かつ，フィッシングサイトへの誘導を防ぐためのサーバ認証の仕組みを持つこととする．

また本稿の目的とする相互認証システムは，上記の仕組みに加え，以下の要件を満たすことを条件とする．

(1) ユーザがウェブサーバに対して携帯電話の情報を提供しない．（プライバシ保護性）．

これは携帯電話の電話番号や E メールアドレス，携帯電話固有の ID 情報などの個人情報をウェブサーバで管理する必要性を排除し，情報漏洩によるリスクも低減させるためである．

(2) 携帯電話が通信圏外にある場合や，電波オフモードなどの場合においても相互認証を可能にする（環境柔軟性）．

これは，ユーザが海外や地階などの通信圏外にいる場合や，電波発信のモードをオフにしている場合などにおいても利用を可能とし，ユーザのいる場所に制限されないシステムとする目的である．

(3) 携帯電話とパソコン間の通信は USB ケーブルや赤外線通信，Bluetooth 通信などのすべてのパソコンで具備しているとは限らない機能を使用しない．また，携帯電話で文字を入力するなどの余分なキー操作をしない（簡易性）．

これは，新たな通信デバイスを必要とせず，かつユーザによる携帯電話及びパソコンの煩雑な操作を要さないシステムを目的とし，簡素化を図るための要件である．

### 3.2. システムの構成要素と関係

前節で設定した要件を満たすことを目的として提案する相互認証システムの構成を図 1 に示す．

システムはユーザが利用するパソコン，ユーザ携帯電話，ウェブサーバ，及び携帯電話キャリアサーバから構成される．ウェブサーバは，サービスを提供するサーバであり，ユーザは，このサーバ上のサービスを利用するために相互認証が行われることになる．また，キャリアサーバは，携帯電話事業者が管理するサーバであり，ウェブサーバとユーザ間の仲介を行うことにより，相互認証を成立させる役割を担っている．

キャリアサーバとウェブサーバは事前に契約を結んでおり，ユーザに関する ID（$ID_{client}$）を共有するものとする．また，ウェブサーバに携帯電話をクライアント認証のために登録する際に，携帯電話内にウェブサーバ情報と携帯電話キャリアサーバ情報を登録するものとする．

ユーザがパソコンからウェブサーバにアクセスした場合に，ウェブサーバはサーバ情報とセッション ID を組み込んだ QR コードをパソコンに送信する．ユーザはこれを携帯電話のカメラで読み取り，QR コードから得られるウェブサーバ情報を，登録しているウェブサーバ情報と比較し，検証を行う．携帯電話はウェブサーバがすでに登録されているサイトかどうかを検証した後，携帯電話が圏内の場合にはパケット通信でクライアント認証情報をキャリアサーバへ送信する．携帯電話が圏外の場合には，ワンタイムパスワード化したクライアント認証情報をユーザのパソコンのキーボードで打ち込み，パソコン経由でキャリアサーバに接続し，送信する．キャリアサーバは受け取ったクライアント認証情報を $ID_{client}$ へと変換し，対象のウェブサーバへ送信する．$ID_{client}$ を受信したウェブサーバはこれを検証し，セッション ID が一致するクライアント端末にログインが完了したことを通知することにより認証が終了する．携帯電話キャリアサーバを経由して認証を行うことにより，不正なサイトへのアクセスを防ぐことができる．

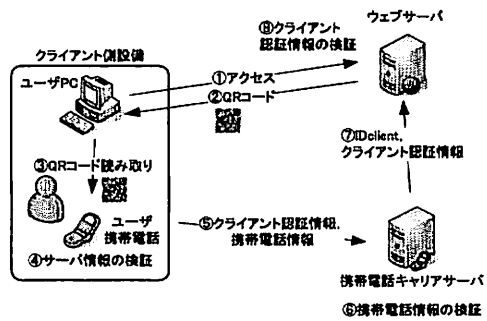



図 1　相互認証システム構成

このシステムは，「携帯電話を所持している」という所持認証情報の検証を，既に認証情報を管理している携帯電話会社のキャリアサーバにおいて行う．これにより，ユーザは認証システムに携帯電話の情報を提供する必要がなくなるため前節の要件(1)を満たすことができる．

また，ウェブサーバ情報をユーザの携帯電話がユーザのパソコン経由で取得し検証を行い，クライアント認証情報を携帯電話からキャリアサーバに送信する際の通信路として，携帯電話が圏内の場合にはパケット通信で行い，携帯電話が圏外の場合にはパケット通信の代替としてユーザのパソコンからキャリアサーバに接続する方法をとるため，環境柔軟性(2)を確保することができる．

さらに，ユーザのパソコンから携帯電話が情報を取得するためにウェブサーバが必要情報を QR コード化し，ユーザが携帯電話のカメラでそれを読み取ることにより行い，携帯電話からキャリアサーバにクライアント認証情報を送信する手段として携帯電話が通信圏内の場合にはパケット通信を行い，携帯電話が通信圏外の場合には，携帯電話内でワンタイムパスワードに変換したクライアント認証情報をユーザがパソコンのキーボードで打ち込むことによりキャリアサーバへ送信することとしたため，ユーザにとって簡易性(3)を確保できる．

## 4. 手順

本章では，前章で述べた構成の具体的な手順の説明を行う．

### 4.1. 事前登録

#### 4.1.1. 携帯アプリのダウンロード

ユーザは認証用アプリケーションソフトウェアを事前にキャリアサーバからダウンロードしておく．この認証用アプリには，

- QR コードを読み取ることによりウェブサーバ情報を受け取り，検証を行う機能
- 携帯電話の圏内・圏外判定機能
- 携帯電話が圏外の場合には認証情報をワンタイムパスワードに変換する機能
- 携帯電話が圏内の場合にはキャリアサーバに接続し，自動的に情報を送信する機能

を備えているものとする．

#### 4.1.2. キャリアサーバ・ウェブサーバ間の登録

本システムを導入するためには，ウェブサーバとキャリアサーバは事前に相互登録をする必要がある．相互登録の際には共有秘密鍵($K_{web\text{-}carrier}$)を生成して互いに保管し，キャリアサーバはウェブサーバにキャリアサーバのURL（$URL_{carrier}$）を，ウェブサーバはキャリアサーバにウェブサーバのURL（$URL_{web}$）を登録する．

#### 4.1.3. 携帯電話・ウェブサーバ間の登録

携帯電話を認証に利用するためには，対象となるサービスを提供するウェブサーバに置いて，利用者と携帯電話を関連づける登録を行う必要がある．図 2 にウェブサーバに携帯電話を使った認証の利用登録のフローを示す．

ユーザは信頼できるパソコンから既存のID・パスワード入力によるクライアント認証方式でウェブサーバにログインする．携帯電話のアプリケーションを起動し，ウェブサーバ上の携帯電話登録ページにおいて，ウェブサーバのURL情報が含まれる$URL_{web}$及びセッションIDから構成されるQRコードを携帯電話のカメラを使って読み取る．セッションIDは，ウェブサーバが独自に管理するIDで，現在使用中のセッションIDと重ならないものをランダムに生成することとする．携帯電話は$URL_{web}$を携帯電話の安全な領域に保存し，パケット通信で$URL_{web}$及びセッションIDをキャリアサーバへ送信する．このとき，携帯電話キャリアサーバは携帯電話固有のID情報を読み取る．キャリアサーバはウェブサーバのサービス毎に発行されるキャリアサーバに対するユーザID（$ID_{carrier\text{-}user}$）及び共有秘密鍵（$K_{carrier\text{-}user}$）を生成し，ユーザの携帯電話へ送信する．また，携帯電話キャリアサーバはユーザに関する$ID_{client}$を生成し，ウェブサーバにセッションIDとともに送信する．ウェブサーバはセッションIDが一致するユーザの情報として$ID_{client}$を登録する．

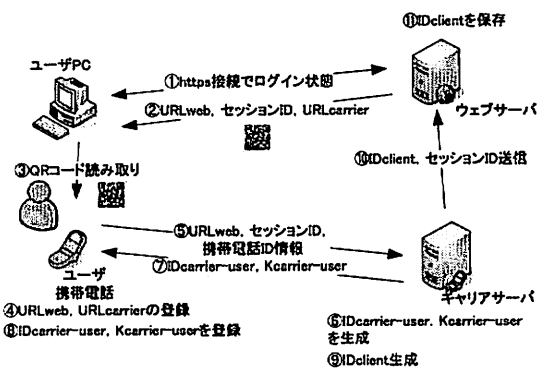



図２　ユーザ利用登録

### 4.2. 認証

図 3 にパソコンからアクセスした際の携帯電話を使った認証フローを示す．

#### 4.2.1. 携帯電話によるウェブサーバの確認

ユーザはパソコンからウェブサーバにアクセスす

る．ウェブサーバは$URL_{web}$とセッションIDから構成されるQRコードを生成しユーザパソコンに送信する．次に，ユーザの携帯電話はQRコードを読み込んでデコードし，$URL_{web}$とウェブサーバのセッションIDを取り出す．携帯電話は$URL_{web}$を携帯電話内に登録されているものと比較し，アクセス先のウェブサーバが登録済みのものかどうかの確認を行う．これによりフィッシングサイトではないことが，ユーザにはある程度の保証が与えられるが，QRコードを偽造しているフィッシングサイトが存在する可能性があるため，フィッシング対策はこれだけでは十分ではない．より確実なフィッシング対策の方法は 4.2.4 で述べる．

### 4.2.2. 携帯電話からの認証情報送信（携帯電話が通信圏内の場合）

携帯電話が通信圏内の場合は，携帯電話はセッションIDと$URL_{web}$をパケット通信でキャリアサーバへ送信する．このとき，携帯電話キャリアサーバは携帯電話固有のIDを読み取り，$URL_{web}$に対応した$ID_{client}$を呼び出す．

### 4.2.3. 携帯電話からの認証情報送信（携帯電話が通信圏外の場合）

携帯電話が通信圏外の場合は，インターネット経由でキャリアサーバに接続し，認証情報を送付する．ウェブサーバは，圏外の場合にユーザが認証情報をキャリアサーバ（$URL_{carrier}$）へ送付するためのページを用意し，ユーザは携帯電話が圏外である場合に，そのページを開く．このページにおいて，$ID_{carrier\text{-}user}$とパスワードの入力フォームがクライアントに表示される．

携帯電話では，$K_{carrier\text{-}user}$とQRコードから読み込んだセッションIDからワンタイムパスワードを生成し，$ID_{carrier\text{-}user}$とワンタイムパスワード，および，サーバ確認情報を生成し，表示する．

次にユーザがキーボードで$ID_{carrier\text{-}user}$とワンタイムパスワードを当該ページで打ち込み，ユーザパソコンはウェブサーバのセッションIDとともにキャリアサーバへインターネット経由で送信する．キャリアサーバは$ID_{carrier\text{-}user}$からユーザを特定し，$K_{carrier\text{-}user}$とセッションIDからワンタイムパスワードを計算し，送られてきたワンタイムパスワードが正しければ$URL_{web}$に対応した$ID_{client}$を呼び出す．

### 4.2.4. $ID_{client}$送信

キャリアサーバは$ID_{client}$をセッションIDとともに，相互登録されているウェブサーバへ送信する．次にウェブサーバは$ID_{client}$とセッションIDを確認し，$ID_{client}$からユーザを特定し，セッションIDが一致するパソコンへログイン後の画面を送信し，認証が成立する．

ウェブサーバがユーザに提供するQRコードをフィッシングサイトが偽造していた場合には，この処理において$ID_{client}$及びセッションIDがフィッシングサイトに送信されず，正規のウェブサーバに送信されるため，認証情報はウェブサーバに受け付けられず，フィッシングサイトであることを確認できる．キャリアサーバからウェブサーバへの通信路を堅固にすることにより，フィッシングサイトへのアクセスを遮断する機構である．

### 4.2.5. 通信経路の確認

ユーザがログイン後の画面を受信した場合，これがキャリアサーバを経由した認証か，フィッシングサイトが偽装した画面かを判断することは難しい．そこで，認証がキャリアサーバ経由で行われたことを確認するフェイズを設けた．

圏内の場合はウェブサーバから認証が成功したことを示す情報をキャリアサーバが受け取り，キャリアサーバは，携帯電話に対して認証成功との情報を送付する．これにより，ユーザは，認証プロセスが完了したウェブサーバからの画面が，キャリアサーバ経由で行われたことを確認できる．また，圏外の場合は，$K_{carrier\text{-}user}$を用いて携帯電話とキャリアサーバでしか生成ができない情報（キャリアサーバ検証ID）を携帯電話とキャリアサーバそれぞれにおいて生成する．キャリアサーバはこのキャリアサーバ検証IDをウェブサーバに送付し，ウェブサーバがこれを画面に表示する．また，携帯電話はワンタイムパスワードとともにキャリアサーバ検証IDを表示する．これにより，ユーザは携帯電話上に表示されているキャリアサーバ検証IDとパソコンの画面上に表示される検証IDを比較し，この認証がキャリアサーバ経由で行われたことを確認することができる．

## 4.3. ID及びパスワード生成

### 4.3.1. $ID_{client}$生成

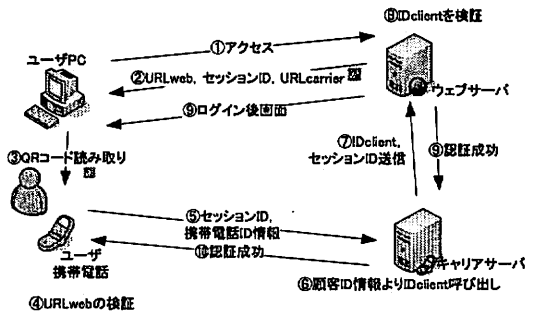
本システムでは，キャリアサーバとウェブサーバ間ではユーザに関する$ID_{client}$を所持する．$ID_{client}$は前述した$K_{web\text{-}carrier}$を鍵とし，携帯電話固有のID情報のHMACの値とする．$K_{web\text{-}carrier}$と，携帯電話固有のIDを利用して生成することにより，各ウェブサーバに対し，ユーザ毎に一意に$ID_{client}$を定めることができる．また，あるユーザに対してウェブサービス毎に異なる$ID_{client}$が割り振られるため，ウェブサービス間の$ID_{client}$によるユーザの関連づけは不可能となる．さらに，$ID_{client}$は携帯電話固有IDからHMACにより計算されるため，キャリアサーバは$ID_{client}$を管理する必要はない．

### 4.3.2. ワンタイムパスワード

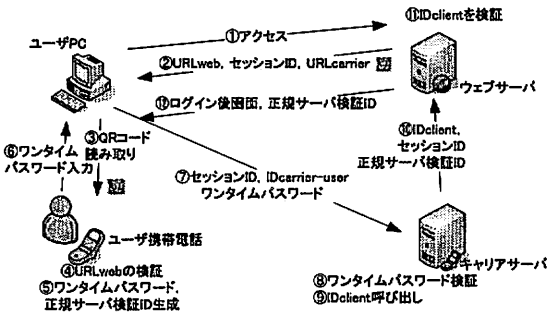
ユーザの携帯電話内で計算され，ユーザによるキーボード入力により，パソコンからキャリアサーバへ送信されるワンタイムパスワードは，ウェブサーバのセッションIDを鍵とし，$K_{carrier\text{-}user}$のHMACを計算することにより生成する．

これにより，ウェブサーバのセッション毎に毎回違うパスワードを生成することができるため，キーロガーやスパイウェアによる固定パスワード盗聴の危険性がなくなる．

キャリアサーバによるワンタイムパスワードの検証は，ワンタイムパスワードと同時にユーザから受信する$ID_{carrier\text{-}user}$からユーザを特定し，携帯電話固有のIDと$K_{web\text{-}carrier}$をキャリアサーバ内のデータベースから呼び出した後，セッションIDを鍵とした$K_{web\text{-}carrier}$のHMACを計算する．




(a) 携帯電話が圏内の場合




(b) 携帯電話が圏外の場合

図 3 相互認証の手順

## 5. 考察

### 5.1. クライアント認証

本システムは，キャリアサーバがユーザの携帯電話に関する情報を一元管理しており，ユーザからのクライアント認証要求の際には，$ID_{client}$をウェブサーバに送信することによりクライアント認証を行うため，ユーザがウェブサーバに対して携帯電話の情報を提供せずにクライアント認証を行うことができ，これによりプライバシが守られる．また，携帯電話が通信圏外にある場合や，電波発信のモードをオフにしている場合などには，パケット通信で送られるべきクライアント認証情報は安全な形でユーザのパソコン経由でキャリアサーバに送信されるため，携帯電話の電波状況に依存せず相互認証が可能である．そして，ユーザは携帯電話を所持しているだけで，携帯電話でのキー操作はほとんど行うことなく簡単に利用できる．

本システムにおいては，クライアント認証の際に，携帯電話を所持していることによる認証（所持認証）のみを行っているため，携帯電話が盗難された場合に悪用される恐れがある．これに関しては，携帯電話端末に独自に設けられているパスワード設定を行うことや，パスワード入力などの知識認証や生体認証を行うフェイズをシステムに組み込み，二要素認証を行う必要があると考えられる．

### 5.2. サーバ認証

本システムにおけるサーバ認証方式は，携帯電話においては，ウェブサーバから提供されるサーバ情報を携帯電話が検証を行い，さらに，キャリアサーバがアクセス先のウェブサーバの正当性を確認し，その結果をユーザに返す．すなわち，キャリアサーバが正当であることを認めていないウェブサーバとは，強制的に通信ができなくなっている．

現在サーバ認証方式として広く利用されている SSL では，ブラウザに認証局のルート証明書を組み込んでおき，認証局がウェブサーバを運営する組織の正当性を確認して，その URL に対して証明書を発行する．利用者は，SSL 通信において，利用されている URL が認証局により正当性が確認され，さらに，証明書を見ることにより，その URL を利用している組織名等を確認することができる．しかし，アクセス先の URL が正しく，SSL により認証されていることはユーザが行わなければならないため，SSL 情報の見逃し等により，フィッシングサイトへ誘導されてしまう．提案方式では，キャリアサーバがウェブサーバの正当性を確認していることは SSL と同様であるが，認証時にキャリアサーバを必ず経由し，不正なサーバへの誘導やウェブサーバが発行していないセッション ID を利用したアクセスは，ユーザに対してエラーが通知される．そのため，SSL によるサーバ認証より確実な方法と言える．

## 6. おわりに

本稿では，携帯電話を利用した相互認証システムにおいて，確実にフィッシング対策を行うことができ，

携帯電話を持つユーザのクライアント認証を行うことができるシステムを提案した．このシステムは，プライバシ保護性，環境柔軟性，及び簡易性を考慮している．

本システムにおいては，クライアント認証の際に，携帯電話を所持していることによる認証（所持認証）を行ったが，必要に応じてパスワード入力などの知識認証や生体認証を行うフェイズをシステムに組み込み，強固な二要素認証を利用することにより，より確実な認証が可能となると考えられる．

## 文　献


[1] ソフトバンク BB　SyncLock WEBaccess
http://www.synclock.jp/access/

[2] メディアスティック　ログイン認証 ASP サービス・ログイン認証組込みシステム
http://www.mediastick.co.jp/pdf/login_auth.pdf

[3] B. Parno, C. Kuo, and A. Perrig. Phoolproof Phishing Prevention. Financial Cryptography and Data Security 10th International Conference, February 27 - March 2, 2006, Anguilla, British West Indies.

[4] NEC プレスリリース　携帯電話を用いて PC からの Web サイトアクセスの安全性を向上
～スパイウェアによる情報漏洩防止とフィッシング詐欺対策を実現～
http://www.nec.co.jp/press/ja/0610/0203.html