(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2007-102777
(P2007-102777A)
(43)公開日　平成19年4月19日(2007.4.19)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/20	(2006.01)	G06F	15/00	330B	5B285
H04L 9/32	(2006.01)	H04L	9/00	673A	5J104

審査請求 有　請求項の数 8　ＯＬ　（全 14 頁）

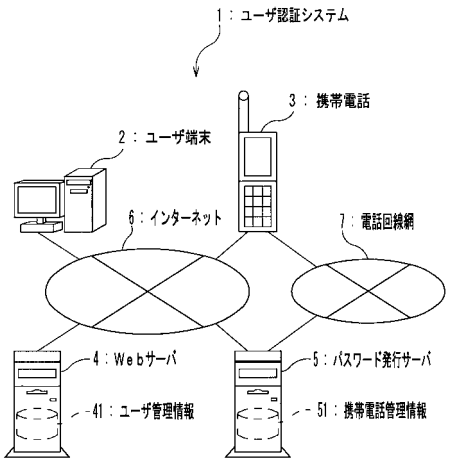
(21)出願番号　特願2006-262474 (P2006-262474)
(22)出願日　平成18年9月27日 (2006.9.27)
(31)優先権主張番号　60/722,989
(32)優先日　平成17年10月4日 (2005.10.4)
(33)優先権主張国　米国(US)

(71)出願人　506234284
株式会社フォーバルテクノロジー
東京都渋谷区神宮前五丁目５２番２号青山オーバルビル１３階
(74)代理人　100064414
弁理士　磯野　道造
(72)発明者　ウィリアム　エッチ　齋藤
東京都渋谷区神宮前５丁目５２番２号　青山オーバルビル１３階
株式会社フォーバルテクノロジー内

Ｆターム(参考)　5B285 AA01 BA01 CA02 CB02 CB05 CB52 CB62 CB72 CB85 CB95 DA03 DA05
5J104 KA01 KA06 NA05 PA02 PA07

(54)【発明の名称】ユーザ認証システムおよびその方法

(57)【要約】
【課題】高いセキュリティ性を維持しつつ、ログインに要するユーザ負荷を軽減できるユーザ認証システムを提供すること。
【解決手段】ユーザ端末、携帯電話、パスワード発行装置およびサービス提供装置から構成され、サービス提供装置は、ユーザ端末からユーザ識別情報を取得すると、登録されたものであれば、パスワード発行装置に送信し、パスワード発行装置は、受信したユーザ識別情報に対応する携帯電話の接続情報を検索し、ワンタイムパスワードを生成して、携帯電話およびサービス提供装置に送信し、携帯電話は受信したワンタイムパスワードを表示し、ユーザ端末は携帯電話に表示されたワンタイムパスワードをサービス提供装置に送信し、サービス提供装置はパスワード発行装置およびユーザ端末から送信されたワンタイムパスワードが一致した場合、ユーザ端末のアクセスを許可するユーザ認証システム。
【選択図】図１



【特許請求の範囲】
【請求項１】
認証に関する情報を入力するためのユーザ端末と、表示機能を有する携帯電話と、ワンタイムパスワードを生成するパスワード発行装置と、前記ユーザ端末にサービスを提供し、ユーザ認証を行なうサービス提供装置とを相互に接続して構成されるユーザ認証システムであって、
前記ユーザ端末は、ユーザからこのユーザを識別するユーザ識別情報を取得すると、このユーザ識別情報を前記サービス提供装置に送信し、前記携帯電話に表示された前記ワンタイムパスワードを取得すると、このワンタイムパスワードを前記サービス提供装置に送信し、
前記携帯電話は、前記パスワード発行装置から前記ワンタイムパスワードを受信すると、このワンタイムパスワードを表示し、
前記パスワード発行装置は、前記ユーザ識別情報に対応させて前記携帯電話の接続情報である第１接続情報を予め記憶し、前記サービス提供装置から前記ユーザ識別情報を取得すると、このユーザ識別情報に対応する前記第１接続情報を検索して、任意のワンタイムパスワードを生成して前記サービス提供装置に送信するとともに、前記第１接続情報を用いて、前記ワンタイムパスワードを前記携帯電話に送信し、
前記サービス提供装置は、前記ユーザ識別情報を予め記憶し、前記ユーザ端末から前記ユーザ識別情報を受信すると、前記サービス提供装置に記憶された前記ユーザ識別情報の中に、受信した前記ユーザ識別情報と一致するものがあるか否かを判定して、一致する前記ユーザ識別情報があると、このユーザ識別情報を前記パスワード発行装置に送信し、前記ユーザ端末および前記パスワード発行装置から前記ワンタイムパスワードを受信すると、２つの前記ワンタイムパスワードを比較して、一致した場合は、前記ユーザ端末のアクセスを許可すること、
を特徴とするユーザ認証システム。
【請求項２】
認証に関する情報を入力するためのユーザ端末と、ブラウザ機能を有する携帯電話と、ワンタイムパスワードを生成するパスワード発行装置と、前記ユーザ端末にサービスを提供し、ユーザ認証を行なうサービス提供装置とを相互に接続して構成されるユーザ認証システムであって、
前記ユーザ端末は、ユーザからこのユーザを識別するユーザ識別情報を取得すると、このユーザ識別情報を前記サービス提供装置に送信し、前記携帯電話に表示された前記ワンタイムパスワードを取得すると、このワンタイムパスワードを前記サービス提供装置に送信し、
前記パスワード発行装置は、前記ユーザ識別情報に対応させて、前記携帯電話の接続情報である第１接続情報を予め記憶し、前記サービス提供装置から前記ユーザ識別情報を取得すると、このユーザ識別情報に対応する前記第１接続情報を検索して、この第１接続情報を用いて前記携帯電話に、前記パスワード発行装置の接続情報である第２接続情報を送信し、前記携帯電話からのアクセスがあると、任意のワンタイムパスワードを生成して、このワンタイムパスワードを前記サービス提供装置に送信するとともに、前記ワンタイムパスワードを前記携帯電話に送信し、
前記携帯電話は、前記パスワード発行装置から前記第２接続情報を受信すると、この第２接続情報を用いて、前記パスワード発行装置にアクセスし、前記パスワード発行装置から前記ワンタイムパスワードを取得すると、このワンタイムパスワードを表示し、
前記サービス提供装置は、前記ユーザ識別情報が予め記憶され、前記ユーザ端末から前記ユーザ識別情報を受信すると、前記サービス提供装置に記憶された前記ユーザ識別情報の中に、取得した前記ユーザ識別情報と一致するものがあるか否かを判定して、一致する前記ユーザ識別情報がある場合に、この前記ユーザ識別情報を前記パスワード発行装置に送信し、前記ユーザ端末および前記パスワード発行装置から前記ワンタイムパスワードを受信すると、２つの前記ワンタイムパスワードを比較して、一致した場合は、前記ユーザ

端末のアクセスを許可すること、
を特徴とするユーザ認証システム。
【請求項３】
前記携帯電話は、この携帯電話を識別する携帯電話識別情報を記憶し、
前記パスワード発行装置は、前記ユーザ識別情報に対応させて前記携帯電話識別情報が予め記憶され、前記携帯電話からのアクセスがあった場合に、前記携帯電話に前記携帯電話識別情報の送信を要求し、これに応じて前記携帯電話から前記携帯電話識別情報を受信すると、受信した前記携帯電話識別情報と、前記パスワード発行装置が記憶している前記携帯電話識別情報とを比較して、一致する前記携帯電話識別情報がある場合に、前記ワンタイムパスワードを前記携帯電話に送信すること、
を特徴とする請求項２に記載のユーザ認証システム。
【請求項４】
前記携帯電話識別情報はこの携帯電話の電話番号であり、
前記パスワード発行装置が前記携帯電話に前記ワンタイムパスワードを送信する際に、電話回線網を介して送信すること、
を特徴とする請求項３に記載のユーザ認証システム。
【請求項５】
認証に関する情報を入力するためのユーザ端末と、表示機能を有する携帯電話と、ワンタイムパスワードを生成するパスワード発行装置と、前記ユーザ端末にサービスを提供し、ユーザ認証を行なうサービス提供装置とを相互に接続して構成されるユーザ認証システムにおけるユーザ認証方法であって、
ａ）前記ユーザ端末が、ユーザからこのユーザを識別するユーザ識別情報を取得すると、このユーザ識別情報を前記サービス提供装置に送信する手順と、
ｂ）前記ユーザ識別情報を予め記憶した前記サービス提供装置が、前記ユーザ端末から前記ユーザ識別情報を受信すると、前記サービス提供装置に記憶された前記ユーザ識別情報の中に、受信した前記ユーザ識別情報と一致するものがあるか否かを判定して、一致する前記ユーザ識別情報があると、このユーザ識別情報を前記パスワード発行装置に送信する手順と、
ｃ）前記ユーザ識別情報に対応させて前記携帯電話の接続情報である第１接続情報が予め記憶された前記パスワード発行装置が、前記サービス提供装置から前記ユーザ識別情報を取得すると、このユーザ識別情報に対応する前記第１接続情報を検索して、任意のワンタイムパスワードを生成して前記サービス提供装置に送信するとともに、前記第１接続情報を用いて、前記ワンタイムパスワードを前記携帯電話に送信する手順と、
ｄ）前記携帯電話が、前記パスワード発行装置から前記ワンタイムパスワードを受信すると、このワンタイムパスワードを表示する手順と、
ｅ）前記ユーザ端末が、前記携帯電話に表示された前記ワンタイムパスワードを取得すると、このワンタイムパスワードを前記サービス提供装置に送信する手順と、
ｆ）前記サービス提供装置が、前記ユーザ端末および前記パスワード発行装置から前記ワンタイムパスワードを受信すると、受信した２つの前記ワンタイムパスワードを比較して、一致した場合は、前記ユーザ端末のアクセスを許可する手順とを含むこと、
を特徴とするユーザ認証方法。
【請求項６】
認証に関する情報を入力するためのユーザ端末と、表示機能を有する携帯電話と、ワンタイムパスワードを生成するパスワード発行装置と、前記ユーザ端末にサービスを提供し、ユーザ認証を行なうサービス提供装置とを相互に接続して構成されるユーザ認証システムにおけるユーザ認証方法であって、
ａ）前記ユーザ端末が、ユーザからこのユーザを識別するユーザ識別情報を取得すると、このユーザ識別情報を前記サービス提供装置に送信する手順と、
ｂ）前記ユーザ識別情報が予め記憶された前記サービス提供装置が、前記ユーザ端末から前記ユーザ識別情報を受信すると、前記サービス提供装置に記憶された前記ユーザ識別

情報の中に、受信した前記ユーザ識別情報と一致するものがあるか否かを判定して、一致する前記ユーザ識別情報があると、このユーザ識別情報を前記パスワード発行装置に送信する手順と、

ｃ）前記ユーザ識別情報に対応させて、前記携帯電話の接続情報である第１接続情報が予め記憶された前記パスワード発行装置が、前記サービス提供装置から前記ユーザ識別情報を取得すると、このユーザ識別情報に対応する前記第１接続情報を検索して、この第１接続情報を用いて前記携帯電話に、前記パスワード発行装置の接続情報である第２接続情報を送信し、

ｄ）前記携帯電話が、前記パスワード発行装置から前記第２接続情報を受信すると、この第２接続情報を用いて、前記パスワード発行装置にアクセスする手順と、

ｅ）前記パスワード発行装置が、前記携帯電話からのアクセスがあると、任意のワンタイムパスワードを生成して、このワンタイムパスワードを前記サービス提供装置に送信するとともに、前記ワンタイムパスワードを前記携帯電話に送信する手順と、

ｆ）前記携帯電話が、前記パスワード発行装置から前記ワンタイムパスワードを受信すると、このワンタイムパスワードを表示する手順と、

ｇ）前記ユーザ端末が、前記携帯電話に表示された前記ワンタイムパスワードを取得すると、このワンタイムパスワードを前記サービス提供装置に送信する手順と、

ｈ）前記サービス提供装置が、前記ユーザ端末および前記パスワード発行装置から前記ワンタイムパスワードを受信すると、受信した２つの前記ワンタイムパスワードを比較して、一致した場合は、前記ユーザ端末のアクセスを許可する手順とを含むこと、

を特徴とするユーザ認証方法。

【請求項７】

前記携帯電話は、この携帯電話を識別する携帯電話識別情報を記憶し、前記パスワード発行装置には、前記携帯電話識別情報が予め記憶され、

前記手順ｅ）において前記パスワード発行装置は、アクセスした前記携帯電話に、前記携帯電話識別情報の送信を要求し、これに応じて前記携帯電話から前記携帯電話識別情報を受信すると、受信した前記携帯電話識別情報と、前記パスワード発行装置が記憶している前記携帯電話識別情報とを比較して、一致する前記携帯電話識別情報がある場合に、前記ワンタイムパスワードを前記サービス提供装置および前記携帯電話に送信すること、

を特徴とする請求項６に記載のユーザ認証方法。

【請求項８】

前記携帯電話識別情報はこの携帯電話の電話番号であり、

前記手順ｅ）において、前記パスワード発行装置が前記携帯電話に前記ワンタイムパスワードを送信する際に、電話回線網を介して送信すること、

を特徴とする請求項７に記載のユーザ認証方法。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明はインターネット上のユーザ認証技術に関し、特にセキュリティ強度を維持しつつ、ログインに要するユーザ負荷の軽減を図るユーザ認証システムおよびその方法に関する。

【背景技術】

【０００２】

従来、ユーザ認証後に使用が許可されるシステムにおいて、ユーザ認証を行うための代表的な手法として、ユーザが使用する端末から、予め登録されたユーザ名及びパスワードを入力させ、当該システムにおいて照合を行い、正しい組み合わせであった場合にユーザの使用を許可するという方法がある。

前記の認証方法では、セキュリティの確保のために、例えば、パスワードを長くしたり、大小英文字を混在させたりするなどパスワードを複雑にすることで、場当たり的な英数文字の組合せ入力によるパスワードの一致を発生しにくくしている。また、有効期間を短

くするなどして見破られたパスワードの再利用を防止している。

【０００３】

また、ＵＳＢ（Universal Serial Bus）端子にハードウェアトークンを差し込むことで、このハードウェアトークンに記録されたＩＤ（Identification）を読み取って認証を行なうシステムも実現されている。

【０００４】

しかしながら、前者の認証方法の場合、セキュリティを高めるために、パスワードを複雑化または定期的に変更すると、ユーザがパスワードを忘れたり、パスワードを紙などに記録して保管することでセキュリティ上の問題となることがあった。

また、後者の認証方法の場合、ハードウェアトークンを紛失したり、ハードウェアトークンに内蔵される電池を定期的に交換する必要があるなど、ハードウェアトークンの取り扱いが煩雑であった。

このような問題点に鑑み、非特許文献１には、ユーザが端末からログインを実行した際に、認証サーバが、電話回線網を介して携帯電話などにコールバックすることで別途の認証を行ない、端末および携帯電話における認証が成功した場合にのみ、システムの使用を許可するユーザ認証システムが開示されている。

【非特許文献１】“SecureCall”、サードネットワークス株式会社、［平成１７年８月１６日検索］、インターネット〈URL:http://www.thirdnetworks.co.jp/sc/03ser02.html〉

【発明の開示】

【発明が解決しようとする課題】

【０００５】

しかしながら、非特許文献１に記載のユーザ認証システムでは、端末において入力するユーザＩＤおよびパスワード、そして、さらに携帯電話から入力するパスワードの３つの組み合わせをユーザが記憶しておく必要があり、やはりユーザがパスワードを忘れてしまい、システムにログインできなくなる可能性があった。

本発明は前記の問題を解決するためになされたものであり、その目的は、高いセキュリティ性を維持しつつ、ログインに要するユーザ負荷を軽減することのできるユーザ認証システムおよびその方法を提供することにある。

【課題を解決するための手段】

【０００６】

前記の課題を解決するためになされた本発明に係るユーザ認証システムは、認証に関する情報を入力するためのユーザ端末と、表示機能を有する携帯電話と、ワンタイムパスワードを生成するパスワード発行装置と、前記ユーザ端末にサービスを提供し、ユーザ認証を行なうサービス提供装置とを相互に接続して構成され、ユーザ端末は、ユーザからこのユーザを識別するユーザ識別情報を取得すると、このユーザ識別情報をサービス提供装置に送信し、携帯電話に表示されたワンタイムパスワードを取得すると、このワンタイムパスワードをサービス提供装置に送信し、前記携帯電話は、パスワード発行装置からワンタイムパスワードを受信すると、このワンタイムパスワードを表示し、パスワード発行装置は、ユーザ識別情報に対応させてこの携帯電話の接続情報である第１接続情報を予め記憶し、サービス提供装置からユーザ識別情報を取得すると、このユーザ識別情報に対応する第１接続情報を検索して、任意のワンタイムパスワードを生成してサービス提供装置に送信するとともに、第１接続情報を用いて、ワンタイムパスワードを携帯電話に送信し、サービス提供装置は、ユーザ識別情報を予め記憶し、ユーザ端末からユーザ識別情報を受信すると、サービス提供装置に記憶されたユーザ識別情報の中に、受信したユーザ識別情報と一致するものがあるか否かを判定して、一致するユーザ識別情報があると、このユーザ識別情報をパスワード発行装置に送信し、ユーザ端末およびパスワード発行装置からワンタイムパスワードを受信すると、２つのワンタイムパスワードを比較して、一致した場合は、ユーザ端末のアクセスを許可することを特徴としている。

本発明の他の形態については、実施の形態において説明する。

【発明の効果】

【０００７】
本発明によると、携帯電話を用いることで、専用のハードウェアトークンなどを用いることなくセキュリティ強度を高めることができ、ユーザはユーザＩＤのみを記憶しておけばよく、システムへのログインに要するユーザ負荷を大幅に軽減することができる。
【発明を実施するための最良の形態】
【０００８】
以下、添付した図面を参照しつつ、本発明の実施の形態を詳しく説明する。
図１は、本実施の形態に係るユーザ認証システムの概略構成図である。図１に示すように、本実施の形態に係るユーザ認証システム１は、ユーザの使用するユーザ端末２と、ユーザの使用する携帯電話３と、ユーザがログインを所望するＷｅｂサーバ４と、ユーザ端末２とＷｅｂサーバ４との認証を仲介するパスワード発行サーバ５とがインターネット６を介して相互に接続されている。
さらに、携帯電話３とパスワード発行サーバ５とは電話回線網７を介して接続されている。
【０００９】
（ユーザ端末）
ユーザ端末２は、ユーザがインターネット６に接続してサービスの提供を受けるためのものであり、記憶装置のＲＡＭ（Random Access Memory）、ＲＯＭ（Read Only Memory）およびハードディスク、演算装置のＣＰＵ（Central Processing Unit）、入力装置のマウスおよびキーボード、表示装置のディスプレイ、そして通信インタフェースのＬＡＮ（Local Area Network）カードなどを含んだ端末装置であり、例えば、パーソナルコンピュータにより具現される。
ユーザ端末２の記憶装置には、ＯＳ（Operating System）のほかに、Ｗｅｂブラウザソフトが記憶されており、これらのソフトウェアをＲＡＭに展開してＣＰＵが実行することで、インターネット６に接続可能な端末装置として動作する。
【００１０】
（携帯電話）
携帯電話３は、ワンタイムパスワード取得のために利用され、記憶装置のＲＡＭおよびＲＯＭ、演算装置のＣＰＵ、入力装置のテンキー、表示装置のディスプレイ、そして通信インタフェースの通信回路を有している。
携帯電話３のＲＯＭは、携帯電話３を統括して制御するプログラムや、この携帯電話３で使用する画像データなどの他に、ウェブを閲覧するためのブラウザプログラムなどが記録されている。テンキーの操作により生成される操作情報は、ＣＰＵに入力され、ＣＰＵが生成した画像情報は、ディスプレイに出力される。
また、本実施の形態の携帯電話３のＲＯＭには、ショートメッセージを送受信するためのプログラムがさらに記憶されており、携帯電話会社が提供するショートメッセージサービスにより、携帯電話３の電話番号をアドレスとして電話回線網７を介してショートメッセージを送受信することができる。
なお、本実施の形態では、説明を容易にするために、図１において携帯電話３が直接インターネット６に接続されているように示したが、実際には、携帯電話３は電話回線網７に接続され、この電話回線網７に接続された図示しないゲートウェイを介してインターネット６に接続されている。
【００１１】
（Ｗｅｂサーバ）
Ｗｅｂサーバ４は、インターネット６上でユーザに対してサービスを提供する装置であり、記憶装置のＲＡＭ、ＲＯＭ、ハードディスク、演算装置のＣＰＵ、および通信インタフェースのＬＡＮカードを含んだ端末装置であり、例えば、サーバ用コンピュータにより具現される。
Ｗｅｂサーバ４のハードディスクにはサービス提供のためのサービスプログラム、ワンタイムパスワードを用いてユーザ認証を行なうユーザ認証プログラムおよびユーザに関す

る情報が含まれるユーザ管理情報４１が記録されている。

【００１２】

ここで、図２は、ユーザ管理情報４１に含まれる情報の例を示したテーブルである。図２に示すように、ユーザ管理情報４１には、Ｗｅｂサーバ４のサービスを利用可能なユーザについての情報が記録されており、ユーザごとに固有なユーザＩＤと対応付けて、ユーザ名、ユーザのプロフィールなどが含まれている。

このユーザ管理情報４１は、ユーザ認証システム１を利用する前に、Ｗｅｂサーバ４の管理者などにより予め登録されたものである。

なお、Ｗｅｂサーバ４は、特許請求の範囲のサービス提供装置に相当している。また、ユーザＩＤは、特許請求の範囲のユーザ識別情報に相当している。

【００１３】

（パスワード発行サーバ）

パスワード発行サーバ５は、Ｗｅｂサーバ４と同様に、記憶装置のＲＡＭ、ＲＯＭ、ハードディスク、演算装置のＣＰＵ、および通信インタフェースのＬＡＮカードを含んだ端末装置であり、例えば、サーバ用コンピュータにより具現される。

パスワード発行サーバ５のハードディスクには、ユーザの使用する携帯電話３を識別する情報が含まれる携帯電話管理情報５１およびランダムなワンタイムパスワードを発行するパスワード発行プログラムが記憶されている。このワンタイムパスワード発行プログラムは、ワンタイムパスワードを発行し、電話回線網７を介して携帯電話３にワンタイムパスワードを送信する。

【００１４】

ここで、図３は、携帯電話管理情報５１に含まれる情報の例を示したテーブルである。図３に示すように、携帯電話管理情報５１には、携帯電話３のユーザごとに固有なユーザＩＤと対応付けて、その携帯電話３の電話番号、ＭＡＣ（Media Access Control）アドレスなどが含まれている。また、この他に携帯電話３のＥＳＮ（Electronic Serial Number）を含んでもよい。

この携帯電話管理情報５１は、ユーザ認証システム１を利用する前に、パスワード発行サーバ５の管理者などにより予め登録されたものである。このパスワード発行サーバ５は、特許請求の範囲のパスワード発行装置に相当し、携帯電話３の電話番号は特許請求の範囲の第１接続情報に相当している。

なお、本実施の形態のユーザ認証システム１において、各構成要素間のインターネット６を介した通信は、例えば、ＳＳＬ（Secure Socket Layer）を用いた暗号化通信によりなされる。

【００１５】

（第１実施形態例）

以下に、前記したユーザ認証システム１において実行されるユーザ認証方法について、２つの実施形態例を説明する。

【００１６】

はじめに、第１実施形態例に係るユーザ認証方法について、ユーザ認証システム１の動作を説明するシーケンス図である図４Ａおよび図４Ｂを参照しつつ、詳しく説明する（適宜、図２、図３参照）。

本実施形態例では、ユーザＩＤを入力したユーザの認証を、ユーザが入力したワンタイムパスワードを照合することで行なう。

【００１７】

はじめに、Ｗｅｂサーバ４のサービスを利用したいユーザは、ユーザ端末２からＷｅｂサーバ４にアクセスする（ステップＳ１０１）。これに応じて、Ｗｅｂサーバ４は、ユーザ端末２にＩＤ入力画面および、ユーザ端末２とＷｅｂサーバ４とのセッションを識別するセッションＩＤを送信する（ステップＳ１０２）。ここで、図５は、Ｗｅｂサーバ４が送信するＩＤ入力画面の例である。図５に示したＩＤ入力画面１００には、ユーザ自身に割り当てられたユーザＩＤを入力するＩＤボックス１０１と、ＩＤボックス１０１に入力

されたユーザＩＤをＷｅｂサーバ４に送信する際に選択する送信ボタン１０２とが含まれて構成されている。

【００１８】

次に、ユーザ端末２は、受信したＩＤ入力画面１００をディスプレイに表示する（ステップＳ１０３）。そして、ユーザはこのＩＤ入力画面１００のＩＤボックス１０１に自身のユーザＩＤを入力して、送信ボタン１０２を選択する。これにより、ユーザ端末２は、ユーザＩＤを取得して、この取得したユーザＩＤをＷｅｂサーバ４に送信する（ステップＳ１０４）。

そして、ユーザＩＤを受信したＷｅｂサーバ４は、ユーザ管理情報４１を参照して、ユーザ管理情報４１に受信したユーザＩＤと一致するユーザＩＤがあるか否かを判定する（ステップＳ１０５）。ここで、一致するユーザＩＤがない場合は（ステップＳ１０５で‘Ｎｏ’の場合）、ステップＳ１０２に戻って、ユーザＩＤの入力を促す。また、一致するユーザＩＤがある場合は（ステップＳ１０５で‘Ｙｅｓ’の場合）、ワンタイムパスワードの入力を促すパスワード入力画面をユーザ端末２に送信する（ステップＳ１０６）。ここで、図６はパスワード入力画面の例を示す図面である。図６に示すように、パスワード入力画面２００は、後記する手順により携帯電話３のディスプレイに表示されるワンタイムパスワードを入力するパスワードボックス２０１と、パスワードボックス２０１に入力したワンタイムパスワードをＷｅｂサーバ４に送信する際に選択する認証ボタン２０２から構成されている。

【００１９】

次に、Ｗｅｂサーバ４は、パスワード発行サーバ５に、ユーザ端末２とＷｅｂサーバ４とのセッションＩＤおよび受信したユーザＩＤを送信する（ステップＳ１０７）。

そして、パスワード発行サーバ５は、受信したユーザＩＤをキー情報として、携帯電話管理情報５１から当該ユーザＩＤに対応する携帯電話３の電話番号を検索する（ステップＳ１０８）。

【００２０】

次に、図４Ｂに移って、パスワード発行サーバ５は、ランダムにワンタイムパスワードを生成して（ステップＳ１０９）、このワンタイムパスワードと、ステップＳ１０７で受信したセッションＩＤとをＷｅｂサーバ４に送信する（ステップＳ１１０）。

そして、パスワード発行サーバ５は、ステップＳ１０９で生成したワンタイムパスワードを携帯電話３に送信する（ステップＳ１１１）。このとき、携帯電話３へのワンタイムパスワードの送信は、携帯電話会社が提供している電話回線網７を介したショートメッセージサービスを利用して送信することが望ましい。これは、クッキー情報に含まれる電話番号を確認することができるためである。また、パスワード発行サーバ５に音声合成手段を備えて、電話回線網７を介して携帯電話３にコールバックを行い、音声合成によりワンタイムパスワードを送信する構成としても同様の効果が得られる。

なお、インターネット６を介して、ワンタイムパスワードを携帯電話３に送信することももちろん可能である。

【００２１】

次に、携帯電話３は受信したワンタイムパスワードをディスプレイに表示する（ステップＳ１１２）。そしてユーザは、図６に示したパスワード入力画面２００のパスワードボックス２０１に、携帯電話３のディスプレイに表示されたワンタイムパスワードを入力して、認証ボタン２０２を選択する。これにより、ユーザ端末２は、ワンタイムパスワードを取得し（ステップＳ１１３）、このワンタイムパスワードと、ステップＳ１０２で取得したＷｅｂサーバ４のセッションＩＤとをＷｅｂサーバ４に送信する（ステップＳ１１４）。

そして、ワンタイムパスワードおよびセッションＩＤを受信したＷｅｂサーバ４は、ステップＳ１１０で取得したパスワード発行サーバ５から送信されたワンタイムパスワードおよびセッションＩＤとステップＳ１１４で取得したユーザ端末２から送信されたワンタイムパスワードおよびセッションＩＤとを比較して一致するか否かを判定する（ステップ

Ｓ１１５）。
【００２２】
ステップＳ１１５の判定の結果、ワンタイムパスワードおよびセッションＩＤが一致しない場合は（ステップＳ１１５で‘Ｎｏ’の場合）、ステップＳ１０２に戻って（ステップＳ１１６）認証をやり直す。
また、ワンタイムパスワードおよびセッションＩＤが一致する場合は（ステップＳ１１５で‘Ｙｅｓ’の場合）、認証に成功したとして、ユーザ端末２のアクセスを許可する（ステップＳ１１７）。その後、ユーザは、ユーザ端末２を介して、Ｗｅｂサーバ４から所望のサービスを受けることになる。
【００２３】
以上、説明したように、本実施形態例のユーザ認証方法によると、予め登録された携帯電話３にパスワード発行サーバ５が発行したワンタイムパスワードを送信し、このワンタイムパスワードを用いて、Ｗｅｂサーバ４において、ユーザの認証を行なう。これにより、たとえ他人のユーザＩＤを用いて、第三者がＷｅｂサーバ４へのアクセスを試みた場合であっても、パスワードを入力することはできず、ハードウェアトークンを用いた場合と同様の高いセキュリティが確保できる。また、携帯電話３のディスプレイに表示されるワンタイムパスワードをパスワード入力画面２００に入力することで、認証が行なえるため、複雑なパスワードを覚える必要がなく、ログインに要するユーザ負荷が著しく軽減される。
【００２４】
（第２実施形態例）
次に、第２実施形態例に係るユーザ認証方法について、ユーザ認証システム１の動作を説明するシーケンス図である図７Ａないし図７Ｃを参照しつつ、詳しく説明する（適宜、図２、図３参照）。
本実施形態例は、ショートメッセージサービスを用いて、携帯電話３にパスワード発行サーバ５のアドレスおよびワンタイムパスワードを送信し、携帯電話３とパスワード発行サーバ５との間で認証を行い、Ｗｅｂサーバ４において、ワンタイムパスワードを照合することでユーザ認証を行なう。
【００２５】
本実施形態例において、図７Ａに示したステップＳ２０１ないしステップＳ２０８に係る動作は、第１実施形態例のステップＳ１０１ないしステップＳ１０８（図４Ａ参照）と同様であるため、その説明は省略する。
次に、図７Ｂに移って、ステップＳ２０８において電話番号を検索したパスワード発行サーバ５は、この電話番号を用いて、携帯電話３に、ショートメッセージサービスにより、パスワード発行サーバ５のアドレスを送信する（ステップＳ２０９）。
そして、パスワード発行サーバ５のアドレスを受信した携帯電話３は、このアドレスを用いて、パスワード発行サーバ５にアクセスする（ステップＳ２１０）。
なお、パスワード発行サーバのアドレスは特許請求の範囲の第２接続情報に相当している。
【００２６】
次に、携帯電話３からのアクセスを受けたパスワード発行サーバ５は、携帯電話３にクッキー情報の送信を要求する（ステップＳ２１１）。
そしてクッキー情報の送信を要求された携帯電話３は、パスワード発行サーバ５にクッキー情報を送信する（ステップＳ２１２）。ここで、携帯電話３が送信するクッキー情報には、その携帯電話３のＭＡＣアドレス、電話番号およびＥＳＮなどが含まれている。
なお、ＭＡＣアドレス、電話番号およびＥＳＮは、特許請求の範囲の携帯電話識別情報に相当している。
【００２７】
携帯電話３からクッキー情報を受信したパスワード発行サーバ５は、携帯電話管理情報５１に登録された携帯電話３のＭＡＣアドレス、電話番号およびＥＳＮなどと照合するこ

とで、携帯電話管理情報５１に、該当するユーザＩＤがあるか否かを判定する（ステップＳ２１３）。

ここで、携帯電話管理情報５１に該当するユーザＩＤがない場合は（ステップＳ２１３で‘Ｎｏ’の場合）、携帯電話管理情報５１に登録された携帯電話３からのアクセスを受け付けるために、ステップＳ２０９に戻る。

【００２８】

一方、図７Ｃに移って、携帯電話管理情報５１に該当するユーザＩＤがある場合は（ステップＳ２１３で‘Ｙｅｓ’の場合）、パスワード発行サーバ５は、ランダムにワンタイムパスワードを生成して（ステップＳ２１４）、このワンタイムパスワードと、ステップＳ２０７で受信したＷｅｂサーバ４のセッションＩＤとをＷｅｂサーバ４に送信する（ステップＳ２１５）。

そして、パスワード発行サーバ５は、ステップＳ２１４で生成したワンタイムパスワードを携帯電話３に送信する（ステップＳ２１６）。このとき、携帯電話３へのワンタイムパスワードの送信は、携帯電話会社が提供している電話回線網７を介したショートメッセージサービスを利用して送信することが望ましい。

【００２９】

次に、携帯電話３は受信したワンタイムパスワードをディスプレイに表示する（ステップＳ２１７）。そしてユーザは、図６に示したパスワード入力画面２００のパスワードボックス２０１に、携帯電話３のディスプレイに表示されたワンタイムパスワードを入力して、認証ボタン２０２を選択する。これにより、ユーザ端末２は、ワンタイムパスワードを取得し（ステップＳ２１８）、このワンタイムパスワードと、ステップＳ２０２で取得したＷｅｂサーバ４のセッションＩＤとをＷｅｂサーバ４に送信する（ステップＳ２１９）。

そして、ワンタイムパスワードおよびセッションＩＤを受信したＷｅｂサーバ４は、ユーザ管理情報４１を参照して、取得したユーザＩＤからユーザを特定して、ステップＳ２１５で取得したパスワード発行サーバ５から送信されたワンタイムパスワードおよびセッションＩＤとステップＳ２１９で取得したユーザ端末２から送信されたワンタイムパスワードおよびセッションＩＤとを比較して一致するか否かを判定する（ステップＳ２２０）。

【００３０】

ステップＳ２２０の判定の結果、ワンタイムパスワードおよびセッションＩＤが一致しない場合は（ステップＳ２２０で‘Ｎｏ’の場合）、エラーと判断して、ステップＳ２０２に戻って（ステップＳ２２１）認証をやり直す。

また、ワンタイムパスワードおよびセッションＩＤが一致する場合は（ステップＳ２２０で‘Ｙｅｓ’の場合）、認証に成功したとして、ユーザ端末２のアクセスを許可する（ステップＳ２２２）。その後、ユーザは、ユーザ端末２を介して、Ｗｅｂサーバ４から所望のサービスを受けることになる。

【００３１】

以上、説明したように、本実施形態例のユーザ認証方法によると、パスワード発行サーバ５において、携帯電話３からクッキー情報を取得し、予め登録された携帯電話３であるか否かを判定するため、ワンタイムパスワードを送信する携帯電話３の素性を確認することで、高いセキュリティが実現される。

また、パスワード発行サーバ５が発行するワンタイムパスワードを照合することで認証を行うため、ユーザはユーザＩＤのみを記憶しておけばよく、認証に係るユーザの負担を大幅に軽減することができる。

【００３２】

なお、本実施の形態では、Ｗｅｂサーバ４およびパスワード発行サーバ５を動作させる各プログラムを、ハードディスクに記憶させることとしたが、それらのプログラムは、プログラムが記憶されたＣＤ－ＲＯＭから読み出してハードディスクにインストールされる。また、ＣＤ－ＲＯＭ以外に、フレキシブルディスク、ＩＣカード等のプログラムをコン

ピュータ可読の記録媒体からインストールすることもできる。さらに、通信回線を用いてプログラムをダウンロードするようにすることもできる。

【００３３】

以上、本発明の実施の形態を説明したが、本発明は、前記した実施の形態に限定されることなく、本発明の趣旨を逸脱しない範囲内で様々に変形して実施可能である。

例えば、本実施の形態ではＷｅｂサーバ４とパスワード発行サーバ５とを異なるサーバとして示したが、Ｗｅｂサーバ４にパスワード発行サーバ５の機能を持たせて、１台のサーバとすることも可能である。

また、例えば、さらに高いセキュリティが必要となる場合には、本発明に従来技術のパスワードによる認証を組み合わせて実行することも可能である。

【図面の簡単な説明】

【００３４】

【図１】ユーザ認証システムの概略構成図である。

【図２】ユーザ管理情報に含まれる情報の例である。

【図３】携帯電話管理情報に含まれる情報の例である。

【図４Ａ】第１実施形態例によるユーザ認証システムの動作を説明するシーケンス図である。

【図４Ｂ】第１実施形態例によるユーザ認証システムの動作を説明するシーケンス図である。

【図５】ＩＤ入力画面の例を示す図面である。

【図６】パスワード入力画面の例を示す図面である。

【図７Ａ】第２実施形態例によるユーザ認証システムの動作を説明するシーケンス図である。

【図７Ｂ】第２実施形態例によるユーザ認証システムの動作を説明するシーケンス図である。

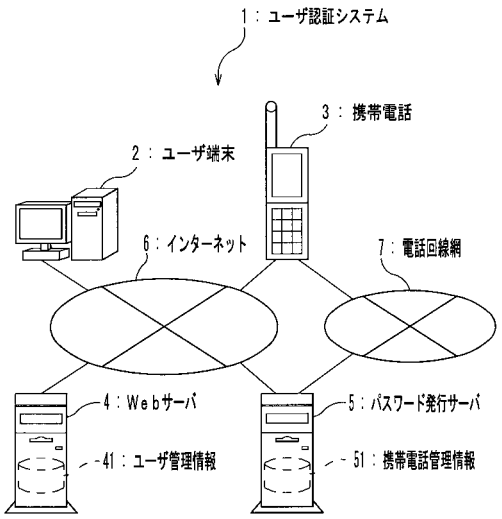
【図７Ｃ】第２実施形態例によるユーザ認証システムの動作を説明するシーケンス図である。

【符号の説明】

【００３５】

１　ユーザ認証システム
２　ユーザ端末
３　携帯電話
４　Ｗｅｂサーバ
５　パスワード発行サーバ
６　インターネット
７　電話回線網
４１　ユーザ管理情報
５１　携帯電話管理情報

【図１】



【図２】

41：ユーザ管理情報

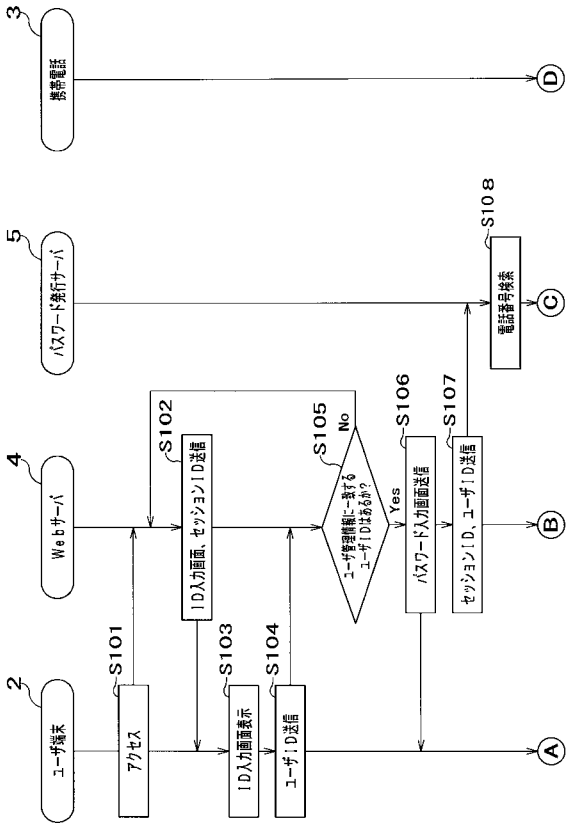
ユーザＩＤ	ユーザ名	プロフィール	…
○○	○○　○○	・・・	…
△△	△△　△△	・・・	…
□□	□□　□□	・・・	…
⋮	⋮	⋮	…

【図３】

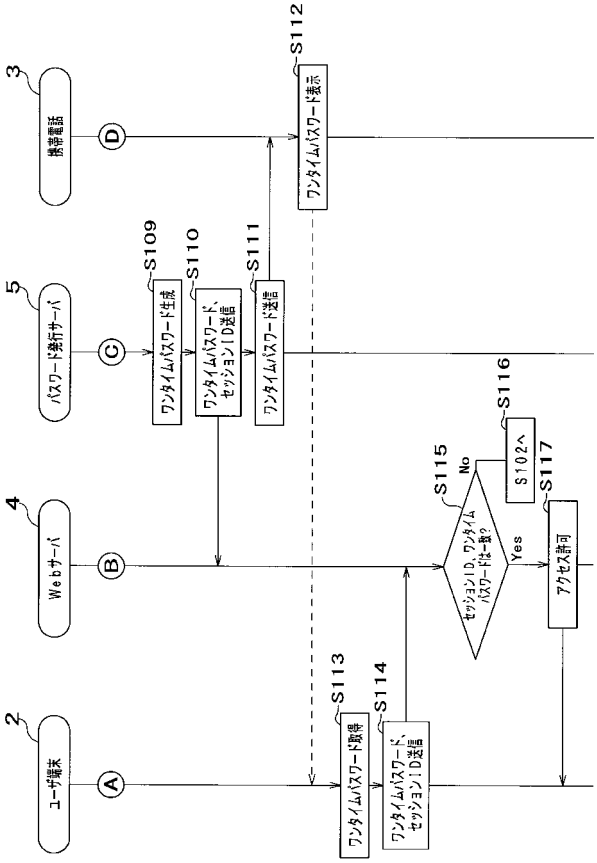
51：携帯電話管理情報

ユーザＩＤ	電話番号	ＭＡＣアドレス	…
○○	111-1111111	11-11-11-11-11-○	…
△△	222-2222222	22-22-22-22-22-△	…
□□	333-3333333	33-33-33-33-33-□	…
⋮	⋮	⋮	…

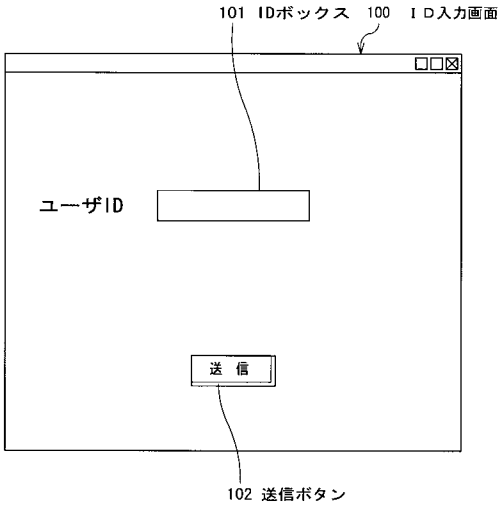
【図４Ａ】



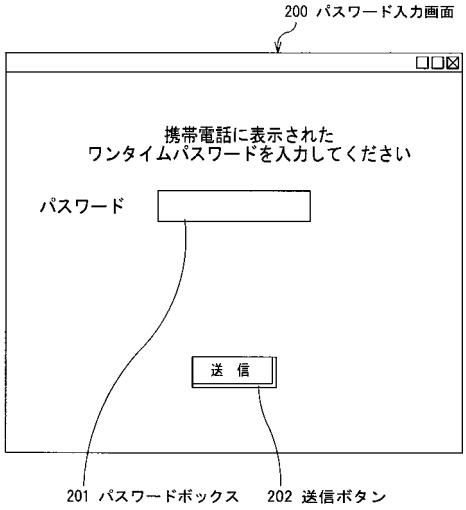
【図４Ｂ】



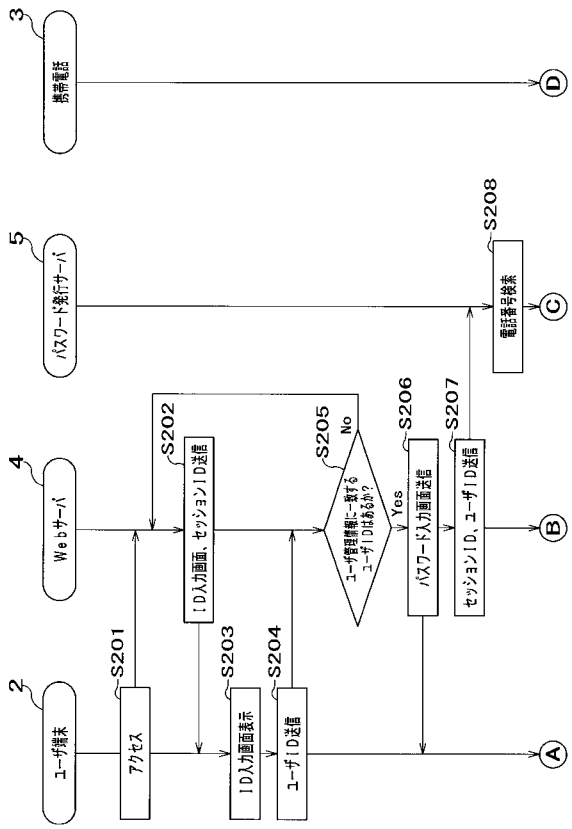
【図５】


101 IDボックス
100 ＩＤ入力画面
ユーザID
送 信
102 送信ボタン

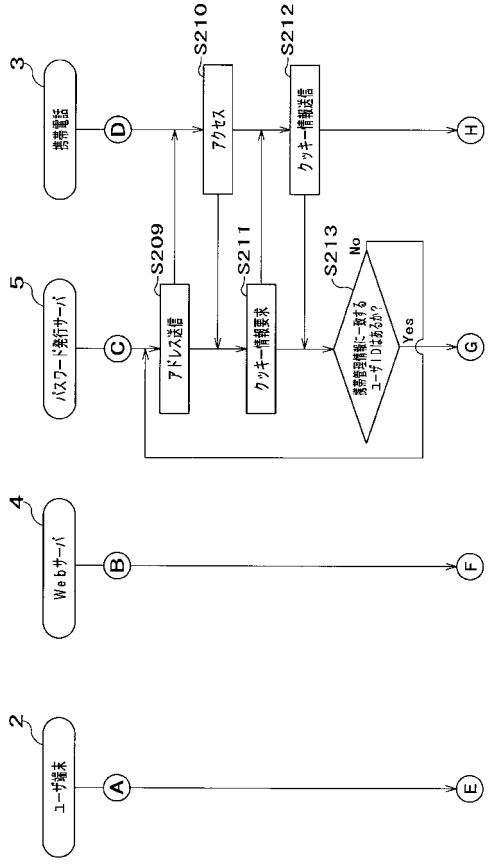
【図６】


200 パスワード入力画面
携帯電話に表示された
ワンタイムパスワードを入力してください
パスワード
送 信
201 パスワードボックス
202 送信ボタン

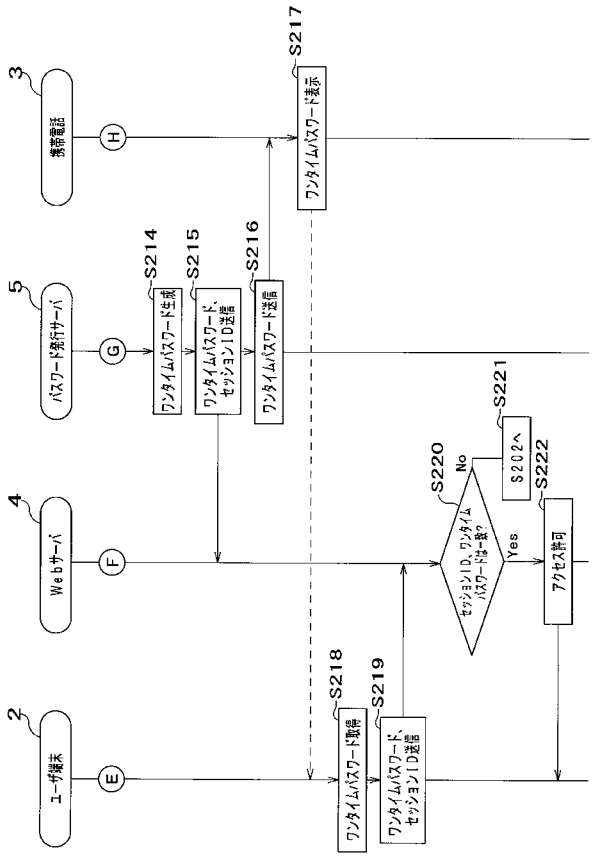
【図７Ａ】


3
携帯電話
D
5
パスワード発行サーバ
S208
電話番号検索
C
4
Webサーバ
S202
ＩＤ入力画面、セッションID送信
S205
No
ユーザ管理情報に一致するユーザIDはあるか？
Yes
S206
パスワード入力画面送信
S207
セッションID、ユーザID送信
B
2
ユーザ端末
S201
アクセス
S203
ＩＤ入力画面表示
S204
ユーザID送信
A

【図７Ｂ】


3
携帯電話
D
S210
アクセス
S212
クッキー情報送信
H
5
パスワード発行サーバ
C
S209
アドレス送信
S211
クッキー情報要求
S213
No
携帯管理情報に一致するユーザIDはあるか？
Yes
G
4
Webサーバ
B
F
2
ユーザ端末
A
E

【図７Ｃ】


3
携帯電話
H
S217
ワンタイムパスワード表示
5
パスワード発行サーバ
G
S214
ワンタイムパスワード生成
S215
ワンタイムパスワード、セッションID送信
S216
ワンタイムパスワード送信
4
Webサーバ
F
S220
No
セッションID、ワンタイムパスワード一致?
Yes
S221
S202へ
S222
アクセス許可
2
ユーザ端末
E
S218
ワンタイムパスワード取得
S219
ワンタイムパスワード、セッションID送信