(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第5100345号
(P5100345)

(45)発行日　平成24年12月19日(2012.12.19)　(24)登録日　平成24年10月5日(2012.10.5)

(51)Int.Cl.　　F I
G06Q 10/02 (2012.01)　G06F 17/60 146A
G06Q 20/06 (2012.01)　G06F 17/60 410A
G06Q 10/00 (2012.01)　G06F 17/60 506

請求項の数 3　(全 15 頁)

(21)出願番号　特願2007-317492 (P2007-317492)
(22)出願日　平成19年12月7日 (2007.12.7)
(65)公開番号　特開2009-140352 (P2009-140352A)
(43)公開日　平成21年6月25日 (2009.6.25)
審査請求日　平成22年3月19日 (2010.3.19)

(73)特許権者　000211307
中国電力株式会社
広島県広島市中区小町４番３３号
(74)代理人　100126561
弁理士　原嶋　成時郎
(72)発明者　久安　弘容
広島県広島市中区小町４番３３号　中国電力株式会社内

審査官　宮下　浩次

最終頁に続く

(54)【発明の名称】サービス消費の確認システム

(57)【特許請求の範囲】
【請求項１】
サービスを提供するサービス事業者に利用者が申し込んだサービスを確認するサービス消費の確認システムであって、
前記利用者を認証する際に用いられる認証用データを前もって記憶し、前記利用者が識別情報を用いてサービスを申し込むと、該識別情報が適正であるときに、サービスの申し込みを前記サービス事業者に転送し、前記利用者が申し込んだサービスの申請データを前記サービス事業者から受け取ると、該申請データを記憶すると共に、該サービスを消費する直前に、該申請データを前記利用者の携帯端末に送信し、かつ、該サービスに関連する代金の支払い期日やクレジット会社から受信したクレジットカードが利用停止になった日付けを含む利用期限を関連情報として記憶する第１の処理手段と、
サービス消費の際に前記携帯端末から申請データを読み取って前記第１の処理手段に送ると共に、前記携帯端末の所有者から認証用データを読み取って前記第１の処理手段に送る第２の処理手段と、を備え、
前記第１の処理手段は、前記第２の処理手段から受け取った申請データと、記憶している申請データとを比較して認証を行い、かつ、前記関連情報を基にして申請データの利用期限の認証を行い、さらに、前記第２の処理手段から受け取った認証用データと、前もって記憶している認証用データとを比較して認証を行い、認証結果を前記第２の処理手段に送り、
前記第２の処理手段は、前記第１の処理手段から受け取った認証結果を基にして、サー

ビスが消費可能かどうかを判断することを特徴とするサービス消費の確認システム。
【請求項２】
前記利用者を認証する際に用いられる認証用データは、該利用者の生体データであることを特徴とする請求項１に記載のサービス消費の確認システム。
【請求項３】
第１の処理手段は、前記サービス事業者から受け取った申請データを二次元コードに変換して記憶すると共に、該二次元コードの申請データを前記利用者の携帯端末に送信することを特徴とする請求項１または２のいずれか１項に記載のサービス消費の確認システム。

【発明の詳細な説明】
【技術分野】
【０００１】
この発明は、各種のサービスを利用者が使用して消費する場合に利用される、サービス消費の確認システムに関する。

【背景技術】
【０００２】
利用者がサービスを使用して消費（以下、「サービス消費」という）をするために、前もってサービスを使用するための申し込みを行って、サービス消費の権限（以下、「消費権限」という）を利用者が取得しておく場合がある。こうした消費権限の取得には、例えばキャッシュカードを用いたチケットの予約がある。後日、利用者が窓口でチケットを購入する際にカード決裁を利用すると、店舗側では利用者が本人であるかどうかを確認する。
【０００３】
このために例えば、認証サービスを提供する認証装置を用いた確認方法がある（例えば、特許文献１参照。）。この場合、携帯電話機を所持した利用者が店舗に行き商品などを購入する場合、利用者は携帯電話機を操作して認証装置に配信要求を送信する。認証装置は配信要求を受信した際に、あらかじめ登録してある利用者つまり被認証者の情報を読み出し、この情報から二次元コードを生成する。この後、認証装置は、生成した二次元コードを配信要求元の携帯電話機へ送信する。携帯電話機は表示部に二次元コードを表示する。店舗に設置されている端末装置のコードリーダに対して、二次元コードが表示された携帯電話機の表示部を利用者がかざすと、端末装置は、二次元コードを携帯電話機から読み取り、この二次元コードを基にして認証を行う。
【特許文献１】特開２００６－４０１１７号公報
【発明の開示】
【発明が解決しようとする課題】
【０００４】
ところで、先に述べた認証装置を利用する確認方法には次の課題がある。利用者がサービス消費をするときには本人確認がないので、別人がサービス消費を行ってしまう、というリスクがある。また、チケットの予約などをして消費権限を取得したときには消費権限が利用者にあったが、その後、例えばクレジット会社に対する支払いが滞ったりすると、取得した消費権限を失うことがある。こうした場合でも、本人によってサービス消費が行われる、というリスクもある。
【０００５】
この発明の目的は、前記の課題を解決し、サービス消費の権限が本人にあるかどうかを確認することを可能にする、サービス消費の確認システムを提供することにある。

【課題を解決するための手段】
【０００９】

前記の課題を解決するために、請求項１の発明は、サービスを提供するサービス事業者に利用者が申し込んだサービスを確認するサービス消費の確認システムであって、前記利用者を認証する際に用いられる認証用データを前もって記憶し、前記利用者が識別情報を用いてサービスを申し込むと、該識別情報が適正であるときに、サービスの申し込みを前記サービス事業者に転送し、前記利用者が申し込んだサービスの申請データを前記サービス事業者から受け取ると、該申請データを記憶すると共に、該サービスを消費する直前に、該申請データを前記利用者の携帯端末に送信し、かつ、該サービスに関連する代金の支払い期日やクレジット会社から受信したクレジットカードが利用停止になった日付けを含む利用期限を関連情報として記憶する第１の処理手段と、サービス消費の際に前記携帯端末から申請データを読み取って前記第１の処理手段に送ると共に、前記携帯端末の所有者から認証用データを読み取って前記第１の処理手段に送る第２の処理手段と、を備え、前記第１の処理手段は、前記第２の処理手段から受け取った申請データと、記憶している申請データとを比較して認証を行い、かつ、前記関連情報を基にして申請データの利用期限の認証を行い、さらに、前記第２の処理手段から受け取った認証用データと、前もって記憶している認証用データとを比較して認証を行い、認証結果を前記第２の処理手段に送り、前記第２の処理手段は、前記第１の処理手段から受け取った認証結果を基にして、サービスが消費可能かどうかを判断することを特徴とするサービス消費の確認システムである。

【００１０】
請求項１の発明では、第１の処理手段（認証装置）は、利用者が申し込んだサービスを表す申請データをサービス事業者から受け取ると、この申請データを記憶すると共に、サービスを消費する直前に、この申請データを利用者の携帯端末に送信する。また、第１の処理手段（認証装置）は、申請データをサービス事業者から受け取ると、サービスに関連する関連情報を記憶する。

【００１１】
この後、利用者がサービス事業者に申し込んだサービスを使用して消費する際に、第２の処理手段（端末装置）は、携帯端末から申請データを読み取って第１の処理手段（認証装置）に送る。第１の処理手段（認証装置）は、第２の処理手段（端末装置）から受け取った申請データと、記憶している申請データとを比較して認証を行い、かつ、関連情報を基にして申請データの利用期限の認証を行い、第２の処理手段から受け取った認証用データと、前もって記憶している認証用データとを比較して認証を行う。第２の処理手段（端末装置）は、第１の処理手段（認証装置）から受け取った認証結果を基にして、サービスが消費可能かどうかを判断する。

【００１３】
請求項２の発明は、請求項１に記載のサービス消費の確認システムにおいて、前記利用者を認証する際に用いられる認証用データは、該利用者の生体データであることを特徴とする。

【００１４】
請求項３の発明は、請求項１または２のいずれか１項に記載のサービス消費の確認システムにおいて、第１の処理手段は、前記サービス事業者から受け取った申請データを二次元コードに変換して記憶すると共に、該二次元コードの申請データを前記利用者の携帯端末に送信することを特徴とする。

【発明の効果】
【００１９】
請求項１の発明によれば、識別情報による利用者の認証と、申請データおよびこの申請

データの関連情報による認証とのダブルチェックを行い、サービスの消費権限が本人にあるかどうか、サービス消費が可能かどうかを確認することを可能にする。

【００２０】
また、識別情報による利用者の認証と、申請データによる認証とのダブルチェックを行い、加えて、サービス消費のときに、利用者から取得した認証用データによって本人であるかどうかを確認するので、サービスの消費権限が本人にあるかどうか、サービス消費が可能かどうかを、さらに確実に確認することを可能にする。

【００２１】
請求項２の発明によれば、利用者を認証する際に用いられる認証用データとして、利用者の生体データを利用するので、パスワードのように他人に使用されることを防ぎ、別人がサービス消費を行ってしまう、というリスクを確実に防ぐことができる。

【００２２】
請求項３の発明によれば、サービス事業者から受け取った申請データを二次元コードに変換して記憶し、二次元コードの申請データを利用者の携帯端末に送信するので、申請データをパターンにして処理することを可能にする。

【発明を実施するための最良の形態】
【００２５】
次に、この発明の実施の形態について、図面を用いて詳しく説明する。
【００２６】
（実施の形態１）
この実施の形態では、イベントのチケットの予約を例として説明する。このイベントには、前もってチケットを予約した応募者の中からイベント会場に所定の先着人数が参加できる。この実施の形態によるサービス消費の確認システムは、図１に示すように、端末装置１０、携帯端末２０、認証装置３０およびサービス提供装置４０を備えている。端末装置１０、携帯端末２０、認証装置３０およびサービス提供装置４０は通信網１００に接続してデータ通信が可能な状態にある。通信網１００は有線通信および無線通信を含むものである。
【００２７】
携帯端末２０は利用者によって所持される携帯電話機やＰＡＤ（Ｐｅｒｓｏｎａｌ　Ｄｉｇｉｔａｌ　Ａｓｓｉｓｔａｎｔｓ）などである。携帯端末２０は、図２に示すように、処理部２１、表示部２２、入力部２３、通信部２４およびメモリ２５を備えている。入力部２３は、利用者によって操作されるキーを備えている。入力部２３には、各種のデータが入力される。表示部２２は液晶ディスプレイのような表示装置であり、処理部２１の制御によって、入力部２３に入力されたデータや、通信部２４が受信したデータなど、各種のデータを表示する。通信部２４は、処理部２１の制御によって、通信網１００とデータの送受信をする。メモリ２５は処理部２１の制御によってデータを記憶する。
【００２８】
処理部２１は、携帯端末２０に関する各種の制御を行う。特にこの実施の形態では、利用者が入力部２３を操作してパスワードを入力すると、処理部２１は、通信部２４を制御して、このパスワードを認証装置３０に送信する。また、通信網１００を経て認証事業者の認証装置３０から二次元コードを通信部２４が受信すると、処理部２１は、この二次元コードをメモリ２５に記憶する。この後、二次元コードの読み出し指示が入力部２３に入力されると、処理部２１は、メモリ２５から二次元コードを読み出し、表示部２２を制御して二次元コードを表示部２２に表示する。この実施の形態では、二次元コードには、チケットデータが認証事業者の認証装置３０でコード化されている。この実施の形態では、チケットデータが申請データに該当する。なお、二次元コードの他にも、チケットデータ

のデータ長によっては、一次元コード（バーコード）も使用可能である。

【００２９】

端末装置１０は、サービス消費が行われる場所、この実施の形態では、イベント会場の窓口に設置されているコンピュータである。端末装置１０は、処理部１１、通信部１２、表示部１３、入力部１４、二次元コード読み取り部１５および生体情報読み取り部１６を備えている。入力部１４は、利用者によって操作されるキーを備えている。入力部１４には、各種のデータが入力される。表示部１３は液晶ディスプレイのような表示装置であり、処理部１１の制御によって、入力部２３に入力されたデータや、通信部１２が受信したデータなど、各種のデータを表示する。通信部１２は、処理部１１の制御によって、通信網１００とデータの送受信をする。

【００３０】

二次元コード読み取り部１５は、処理部１１の制御によって動作し、二次元コードを読み取ってデータ化する装置である。この実施の形態では、二次元コード読み取り部１５は、携帯端末２０の表示部２２に表示された二次元コードを読み取る。生体情報読み取り部１６は、処理部１１の制御によって動作し、利用者の所定の指の静脈（以下、「指静脈」という）のパターンを読み取ってデータ化する装置である。なお、生体情報としては、指静脈以外にも、指紋、瞳の虹彩などが利用可能である。

【００３１】

処理部１１は、端末装置１０に関する各種の制御を行う。特に、この実施の形態では、二次元コード読み取り部１５が読み取った二次元コードを、通信部１２を制御して認証事業者の認証装置３０に送信する。また、処理部１１は、生体情報読み取り部１６が読み取って生成した指静脈データを、通信部１２を制御して認証装置３０に送信する。さらに、処理部１１は、認証装置３０が送信した、指静脈データの認証結果と、二次元コードの認証結果とを通信部１２から受信すると、受付処理を行う。処理部１１は、受付処理を開始すると、受け取った認証結果を基にして、サービス消費が可能であるかどうかを判断する。つまり、２つの認証結果に含まれる顧客番号が一致したときに、サービス消費が可能であると判断し、それ以外はサービス消費が不可であると判断する。

【００３２】

サービス提供装置４０はチケットの予約を行うサービス事業者に設置されているコンピュータである。サービス提供装置４０は、図３に示すように、処理部４１と通信部４２と管理データベース（ＤＢ）４３を備えている。通信部４２は、処理部４１の制御によって、通信網１００とデータの送受信をする。管理データベース４３は、利用者によって予約されたチケットのデータを、チケットの管理テーブルに記録する。この管理テーブルの一例を図４に示す。この管理テーブルには、予約されたチケットのチケット番号と申し込みの年月日が記録されている。また、管理テーブルには、チケットを予約した利用者の氏名、住所、電話番号などが記録されている。

【００３３】

認証事業者の認証装置３０からの接続要求を通信部４２が受信すると、処理部４１はチケット発券処理を行う。処理部４１は、チケット発券処理を開始すると、利用者の携帯端末２０に通信部４２を接続し、チケットの予約を行うための案内画面を、通信部４２を制御して携帯端末２０に表示する。処理部４１は、この案内画面に対する操作結果である入力データを、携帯端末２０から受信すると、この入力データを基にして、管理テーブルを更新し、新たなチケットデータを作成して、チケット発券処理を終了する。図４では、チケット番号「ＴＫ１００１」のチケットに関するチケットデータが例示されている。

【００３４】

処理部４１は、チケット発券処理を終了すると送信処理を行う。処理部４１は、送信処理を開始すると、管理テーブルに新たに作成したチケットデータを読み出し、認証事業者の認証装置３０に送信して、送信処理を終了する。

【００３５】

認証装置３０は認証サービスを行う認証事業者に設置されているコンピュータである。

認証装置３０は、処理部３１、二次元コード生成部３２、通信部３３、顧客データベース（ＤＢ）３４、生体データベース（ＤＢ）３５および申請データベース（ＤＢ）３６を備えている。通信部３３は、処理部３１の制御によって、通信網１００とデータの送受信をする。二次元コード生成部３２は、処理部３１の制御によって、データを二次元コードに変換して、二次元コードを作成する。この実施の形態では、二次元コード生成部３２はチケットデータを二次元コードに変換する。

【００３６】

顧客データベース３４は、認証事業者を利用する利用者である顧客のデータを顧客テーブルに記録している。この顧客テーブルの一例を図５に示す。この顧客テーブルには、利用者を識別するための顧客番号と、利用者の氏名、住所および電話番号などが記録されている。さらに、顧客テーブルには、認証事業者が利用者に対して発行したパスワードが記録されている。図５では、顧客番号「Ａ０００１」の利用者に関するデータが例示されている。

【００３７】

生体データベース３５は、利用者を確認するための指静脈のパターンを、指静脈テーブルに記録している。この指静脈テーブルの一例を図６に示す。この指静脈テーブルには、顧客番号と共に指静脈のパターンが記録されている。図６では、顧客番号「Ａ０００１」の指静脈データが例示されている。

【００３８】

申請データベース３６は、サービス事業者が発行したチケットを申請テーブルに記録している。この申請テーブルの一例を図７に示す。この申請テーブルには、チケットデータから作成された二次元コードが、チケットデータを受信した日付けである受け付け年月日と共に記録されている。図７では、顧客番号「Ａ０００１」のデータが例示されている。

【００３９】

処理部３１は、通信部３３を経て、利用者の携帯端末２０からパスワードを受信すると、第１の認証処理を行う。処理部３１は、第１の認証処理を開始すると、顧客データベース３４の顧客テーブル（図５）を参照して、携帯端末２０から受け取ったパスワードが顧客テーブルにあるかどうかを調べることにより、パスワードによる個人認証を行う。個人認証が終了すると、処理部３１は、通信部３３を制御して認証結果を携帯端末２０に送信し、第１の認証処理を終了する。

【００４０】

第１の認証処理による本人確認が適正であると、処理部３１は次の画面表示処理を行う。処理部３１は、画面表示処理を開始すると、このパスワードを送信した携帯端末２０に、図８に示すメニュー画面を表示するためのデータを、通信部３３を制御して送信する。この後、メニュー画面に表示された項目の選択結果を表す選択データを携帯端末２０から受信すると、この選択データに応じたサービス事業者を選び出し、選出したサービス事業者のサービス提供装置４０に対して携帯端末２０を接続するための接続要求を送信し、画面表示処理を終了する。

【００４１】

画面表示処理が終了した後、処理部３１は、通信部３３を経て、サービス事業者のサービス提供装置４０からチケットデータを受信すると、登録処理を行う。処理部３１は、登録処理を開始すると、受信したチケットデータに含まれる氏名、住所、電話番号などを利用して顧客データベース３４の顧客テーブル（図５）を参照し、該当する顧客の顧客番号を抽出する。この後、処理部３１は、二次元コード生成部３２を制御して、チケットデータの二次元コードを生成し、生成した二次元コードを顧客番号と共に申請テーブル（図７）に記録し、登録処理を終了する。

【００４２】

登録処理が終了すると、処理部３１は、作成した二次元コードを直ちに携帯端末２０に送信する。

【００４３】

この後、処理部３１は、通信部３３を経て、端末装置１０から指静脈データと二次元コードを受信すると、第２の認証処理を行う。処理部３１は、第２の認証処理を開始すると、受信した指静脈データと、生体データベース３５の指静脈テーブル（図６）とを照合し、受信した指静脈データが表すパターンが一致した場合に、この一致したパターンの顧客番号を読み出して指静脈データの認証結果とする。また、一致したパターンがない場合には、指静脈データの不一致を表すメッセージを作成して指静脈データの認証結果とする。同様にして、受信した二次元コードと、申請データベース３６の申請テーブル（図７）とを照合し、受信した二次元コードが表すパターンが一致した場合に、この二次元コードの顧客番号を読み出して二次元コードの認証結果とする。また、一致した二次元コードがない場合には二次元コードの不一致を表すメッセージを作成して二次元コードの認証結果とし、第２の認証処理を終了する。

【００４４】

こうして認証結果を作成すると、処理部３１は、通信部３３を制御して、作成した認証結果を端末装置１０に送信する。

【００４５】

次に、この実施の形態によるサービス消費の確認システムを用いたサービス消費の確認方法について説明する。サービス消費の確認システムを利用する利用者は、あらかじめ認証事業者にサービス利用の登録を行っておく。これにより、利用者は認証事業者からパスワードを受け取る。

【００４６】

ところで、チケットを予約した応募者の中から所定の先着人数が参加できるイベントに利用者が応募しようとすると、利用者は携帯端末２０を操作して認証事業者の認証装置３０に接続し、携帯端末２０にパスワードを入力する。この後、図９に示すように、認証装置３０は、携帯端末２０からパスワードを受け取ると（ステップＳ１）、第１の認証処理を行い（ステップＳ２）、パスワードによる本人確認を行う。この後、認証装置３０は認証結果を携帯端末２０に送る（ステップＳ３）。携帯端末２０は認証結果を受信すると、この認証結果を表示して、認証結果を利用者に通知する。

【００４７】

第１の認証処理で本人確認が適正であると判明すると、認証装置３０は画面表示処理を行う（ステップＳ４）。この画面表示処理により、携帯端末２０にはメニュー画面（図８）が表示される。メニュー画面（図８）から選択された項目、この実施の形態ではチケット予約が選択されて選択データを受け取ると、認証装置３０は選択された項目に該当するサービス事業者のサービス提供装置４０に接続要求を出し、携帯端末２０をサービス提供装置４０に接続する。

【００４８】

携帯端末２０がサービス提供装置４０に接続されると、サービス提供装置４０はチケット発券処理を行う（ステップＳ５）。このチケット発券処理により、携帯端末２０には案内画面が表示される。サービス提供装置４０は、案内画面に対する入力データを携帯端末２０から受信すると、この入力データを基にしてチケットデータを作成し、作成したチケットデータを認証事業者の認証装置３０に送信する（ステップＳ６）。

【００４９】

認証装置３０は、チケットデータを受信すると登録処理を行う（ステップＳ７）。この登録処理により、認証装置３０は、チケットデータの二次元コードを作成し、この二次元コードを申請データベース３６に登録すると共に、この二次元コードを携帯端末２０に直ちに送信する（ステップＳ８）。携帯端末２０は、二次元コードを受信すると、この二次元コードを保存する。

【００５０】

こうして、携帯端末２０にパスワードを入力してから、二次元コードを受信するまでの一連の処理が終了する。この一連の処理では、パスワードによる本人確認やチケットの予約が行われる。

【００５１】
ところで、イベントの当日になると、応募者でもある利用者は携帯端末２０を持ってイベント会場に行く。イベント会場では、利用者は携帯端末２０を操作して二次元コードを読み出し、この二次元コードを携帯端末２０に表示させる。そして、図１０に示すように、イベント会場に設置されている端末装置１０に携帯端末２０の二次元コードを読み取らせる（ステップＳ２１）。また、利用者は指静脈を端末装置１０に読み取らせる（ステップＳ２２）。この後、端末装置１０は読み取った二次元コードと指静脈を認証事業者の認証装置３０に送信する（ステップＳ２３）。
【００５２】
認証装置３０は二次元コードと指静脈を受け取ると、第２の認証処理を行う（ステップＳ２４）。第２の認証処理により、認証装置３０は、受信した指静脈データと、生体データベース３５の指静脈テーブル（図６）とが一致した場合に、この一致したパターンの顧客番号を指静脈データの認証結果とする。一致したパターンがない場合には、指静脈データの不一致を表すメッセージを認証結果とする。同様にして、受信した二次元コードと、申請データベース３６に記憶されている申請テーブル（図７）の二次元コードとが一致した場合に、この一致した二次元コードの顧客番号を読み出して指静脈データの認証結果とする。一致した二次元コードがない場合には二次元コードの不一致を表すメッセージを認証結果とする。
【００５３】
第２の認証処理が終了すると、認証装置３０は認証結果をサービス消費場所の端末装置１０に送信する（ステップＳ２５）。端末装置１０は、認証結果を受信すると受付処理を行い（ステップＳ２６）、受け取った認証結果を基にして、サービス消費が可能であるかどうかを判断する。
【００５４】
こうして、二次元コードと指静脈の読み取り後、サービス消費が可能であるかどうかを決めるまでの一連の処理が終了する。この一連の処理では、二次元コードと指静脈とにより、本人確認と、チケットが本人のものであるかどうかの確認とが行われる。
【００５５】
なお、ステップＳ２６の受付処理でサービス消費が可能であると判明した場合、図示を省略しているが、サービス消費場所では、受付人数が所定数に満たないとき、端末装置１０は利用者を入場させるための処理を行い、利用者に入場券を発行し、それ以外はサービス消費を停止する。
【００５６】
こうして、この実施の形態によれば、チケットを予約する際には、パスワードによる本人確認が行われる。また、予約したチケットを使用する際には、二次元コードおよび指静脈の認証により本人確認が行われ、かつ、二次元コードの認証によりチケットが本人のものであるかどうかの確認が行われる。つまり、サービス消費に関するダブルチェックにより、サービス消費の権限（予約チケットの使用）が本人にあるかどうかを、確実に確認することを可能にする。また、この実施の形態では、予約が終了すると、二次元コードが直ちに携帯端末２０に送信されるので、その場で利用者がチケットの予約ができたかどうかを確認することができる。
【００５７】
（実施の形態２）
この発明の実施の形態２について、図面を用いて詳しく説明する。この実施の形態では、コンサートチケットの予約販売を例として説明する。この実施の形態によるサービス消費の確認システムは、図１１に示すように、端末装置１０、携帯端末２０、認証装置３０、サービス提供装置４０および管理装置５０を備えている。なお、この実施の形態では、先に説明した実施の形態１と同一もしくは同一と見なされる構成要素には、それと同じ参照符号を付けて、その説明を省略する。
【００５８】

管理装置５０は、金融機関、この実施の形態ではクレジット会社に設置されたコンピュータである。管理装置５０は、利用者の支払い状況や、クレジットカートの利用状況などを管理する。管理装置５０は、通信網１００とデータの送受信をする機能を持つ。

【００５９】

この実施の形態によるサービス提供装置４０の管理データベース４３は、申込者によって予約されたコンサートチケットのデータを、コンサートチケットの管理テーブルに記録する。この管理テーブルの一例を図１２に示す。この管理テーブルには、予約されたコンサートチケットのチケット番号と申し込みの年月日が記録されている。また、管理テーブルには、コンサートチケットを予約した申込者の氏名、住所、電話番号が記録されている。さらに、管理テーブルには、コンサートチケットの代金の支払方法が記録されている。図１２では、チケット番号「ＴＫ２００１」のチケットに関するチケットデータが例示されている。

【００６０】

処理部４１は、認証装置３０から接続要求を通信部４２が受信すると、チケット発券処理を行う。このチケット発券処理により、処理部４１は、携帯端末２０から受け取ったチケットデータを基にして管理テーブル（図４）を更新し、新たなチケットデータを作成してチケット発券処理を終了する。

【００６１】

チケット発券処理が終了すると、サービス事業者がクレジット会社のサービス提供装置４０に対して、予約販売をしたコンサートチケットの支払依頼を行う。この支払依頼は、サービス事業者の担当者がクレジット会社の担当者と直接行ってもよく、また、サービス提供装置４０と管理装置５０によって行うようにしてもよい。

【００６２】

さらに、サービス提供装置４０の処理部４１は、クレジット会社から、キャッシュカードの状況を知らせるカード状況を受け取ると、通信部４２を制御して、このカード状況を認証事業者の認証装置３０に送信する。カード状況は、キャッシュカードの利用不可や、利用不可になった日付けなどを知らせる。

【００６３】

認証装置３０の申請データベース３６は、サービス事業者が予約販売したコンサートチケットを申請テーブルに記録している。この申請テーブルの一例を図１３に示す。この申請テーブルには、チケットデータを基にして処理部３１により記録された二次元コードが、チケットデータを受信した日付けである受け付け年月日と共に記録されている。さらに、この申請テーブルには、コンサートチケットの利用期限が記録されている。利用期限は、処理部３１が生成した二次元コードの有効な日付けであり、チケットデータと共にサービス提供装置４０から受け取ったデータである。利用期限としては、コンサートチケットの代金の支払い期日やコンサート当日がある。また、クレジット会社から受信したカード利用状況を基にして、クレジットカードが利用停止になった日付けでもよい。

【００６４】

登録処理が終了した後、もし、サービス事業者のサービス提供装置４０からカード状況を通信部３３が受信すると、処理部３１は、カード状況の内容に応じて申請データベース３６の申請テーブル（図１３）を更新する。つまり、先に述べたように、クレジットカードが使用不可であると、処理部３１は、クレジットカードが使用不可になった日付けを申請テーブル（図１３）に記録する。

【００６５】

実施の形態１では登録処理が終了すると、処理部３１は、作成した二次元コードを直ちに携帯端末２０に送信した。しかし、この実施の形態では、サービス消費の直前、つまり二次元コードの消費の直前として例えばコンサート当日になると、処理部３１は、申請データベース３６の申請テーブル（図１３）から二次元コードを読み出して携帯端末２０に送信する。

【００６６】

処理部３１は、通信部３３を経て、端末装置１０から指静脈データと二次元コードを受信すると、第２の認証処理を行う。処理部３１は、第２の認証処理を開始すると、実施の形態１と同様にして認証結果を生成する。さらに、処理部３１は、二次元コードを受信した日付けと、申請データベース３６の申請テーブル（図１３）の利用期限とを比較し、受信した日付けが利用期限を過ぎているかどうかを判断して、期限確認を行う。処理部３１は、受信した日付けが利用期限以内であると、二次元コードの消費可を確認結果とする。また、受信した日付けが利用期限を過ぎていると、二次元コードの消費不可を確認結果として、第２の認証処理を終了する。

【００６７】

次に、この実施の形態によるサービス消費の確認システムを用いたサービス消費の確認方法について、図１４を用いて説明する。なお、図１４では、先の図９と同一もしくは同一と見なされる処理には、それと同じ参照符号を付けて、その説明を省略する。サービス事業者のサービス提供装置４０は、ステップＳ５のチケット発券処理が終了した後、クレジット会社の管理装置５０に対してコンサートチケットの代金の支払い依頼をする（ステップＳ８）。

【００６８】

一方、認証装置３０は、ステップＳ７の登録処理が終了すると、コンサート当日になるまで、時間経過を待つ。この間に、サービス提供装置４０は、クレジット会社の管理装置５０からカード状況を受信すると（ステップＳ９）、このカード状況を認証事業者の認証装置３０に送信する（ステップＳ１０）。このとき、クレジットカードが使用不可であると、認証装置３０は、クレジットカードが利用不可になった日付けを申請データベース３６の申請テーブル（図１３）に記録する。

【００６９】

コンサート当日の様子を図１５を用いて説明する。なお、図１５では、先の図１０と同一もしくは同一と見なされる処理には、それと同じ参照符号を付けて、その説明を省略する。コンサート当日になると、認証事業者の認証装置３０は、申請データベース３６の申請テーブル（図１３）から二次元コードを読み出し、この二次元コードを携帯端末２０に送信する（ステップＳ２０）。この後は実施の形態１と同様の処理が行われるが、ステップＳ２４の第２の認証処理で、処理部３１は、二次元コードを受信した日付けと、申請データベース３６の申請テーブル（図１３）の利用期限とを比較して期限確認を行う。処理部３１は、受信した日付けが利用期限以内であると、二次元コードの消費可を確認結果とする。また、受信した日付けが利用期限を過ぎていると、二次元コードの消費不可を確認結果とする。

【００７０】

こうして、この実施の形態によれば、チケットを予約する際には、パスワードによる本人確認が行われる。また、予約したチケットを使用する際には、二次元コードと指静脈により、本人確認が行われ、かつ、チケットが本人のものであるかどうかの確認が行われる。つまり、ダブルチェックにより、サービス消費の権限（予約チケットの使用）が本人にあるかどうかを、確実に確認することを可能にする。さらに、二次元コードの消費直前に、この二次元コードを携帯端末２０に送信するので、二次元コードの消費直前まで更新される、認証装置３０の最新の申請テーブル（図１３）を用いて、二次元コードの利用期限を確認することができる。これにより、チケットの予約をしたとき、つまり、二次元コードを作成したときには利用者にこの二次元コードの消費権限があったが、二次元コードの消費時には権限がなくなった場合に、本人により二次元コードが消費されてしまう、というリスクを回避することができる。

【００７１】

以上、この発明の各実施の形態を詳述してきたが、具体的な構成は各実施の形態に限られるものではなく、この発明の要旨を逸脱しない範囲の設計の変更等があっても、この発明に含まれる。例えば、サービス消費の場所で本人認証を必要とするものには、この発明

が適用可能である。つまり、先の図８に示すように、航空機・鉄道チケット予約、…、受験申請などにこの発明が適用可能である。

【図面の簡単な説明】

【００７２】

【図１】この発明の実施の形態１によるサービス消費の確認システムを示す構成図である。

【図２】図１の端末装置および携帯端末を示す構成図である。

【図３】図１の認証装置およびサービス提供装置を示す構成図である。

【図４】管理テーブルの一例を示す図である。

【図５】顧客テーブルの一例を示す図である。

【図６】指静脈テーブルの一例を示す図である。

【図７】申請テーブルの一例を示す図である。

【図８】メニュー画面の一例を示す図である。

【図９】サービス消費の確認方法を説明するためのシーケンス図である。

【図１０】サービス消費の確認方法を説明するためのシーケンス図である。

【図１１】この発明の実施の形態２によるサービス消費の確認システムを示す構成図である。

【図１２】実施の形態２で用いられる管理テーブルの一例を示す図である。

【図１３】実施の形態２で用いられる申請テーブルの一例を示す図である。

【図１４】実施の形態２によるサービス消費の確認方法を説明するためのシーケンス図である。

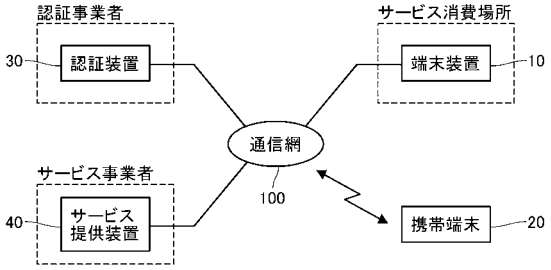
【図１５】実施の形態２によるサービス消費の確認方法を説明するためのシーケンス図である。

【符号の説明】

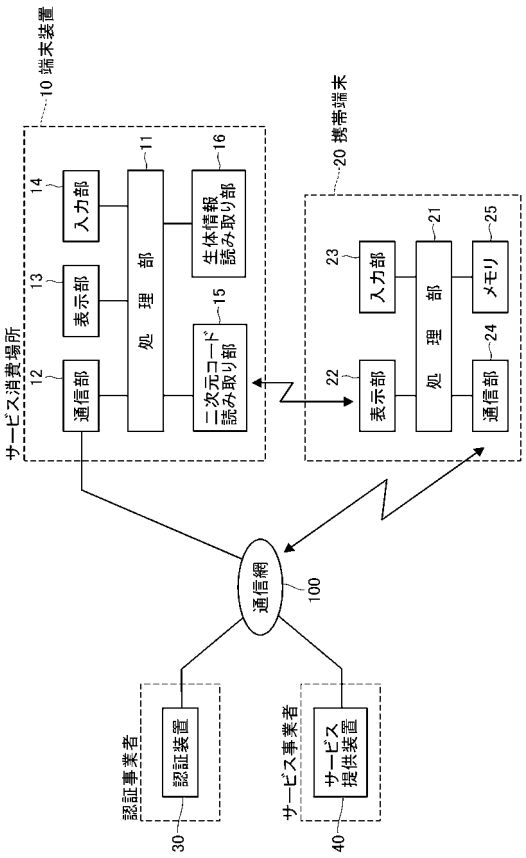
【００７３】

１０　端末装置（第２の処理手段）
２０　携帯端末
３０　認証装置（第１の処理手段）
４０　サービス提供装置
５０　管理装置

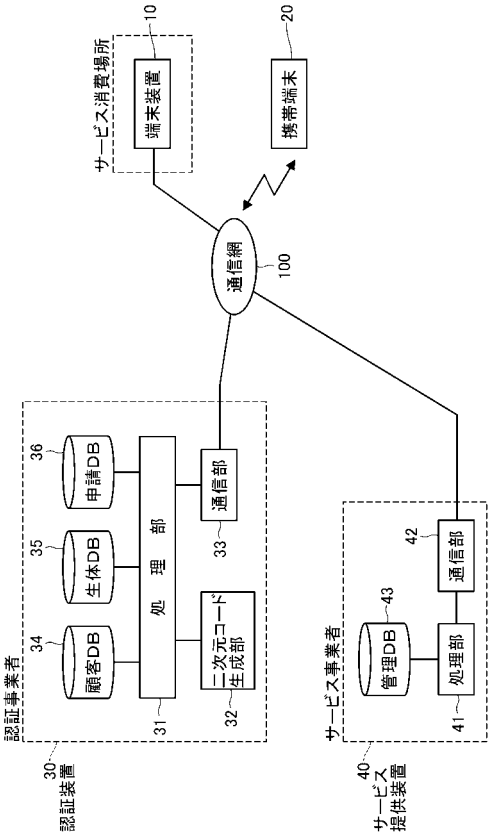
【図１】



【図２】



【図３】



【図４】

管理テーブル

チケット番号	申し込み年月日	氏名	住所	電話番号	…
TK1001	200△年12月1日	△△△△	△△県△△市△△1−1−1	090−1234−5678	
…					

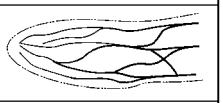
【図５】

顧客テーブル

顧客番号	氏名	住所	電話番号	パスワード	…
A0001	△△△△	△△県△△市△△1−2−3	090−1234−5678	1234	
…					

【図６】

指静脈テーブル

顧客番号	パターン
A0001	
…	…

【図７】

申請テーブル

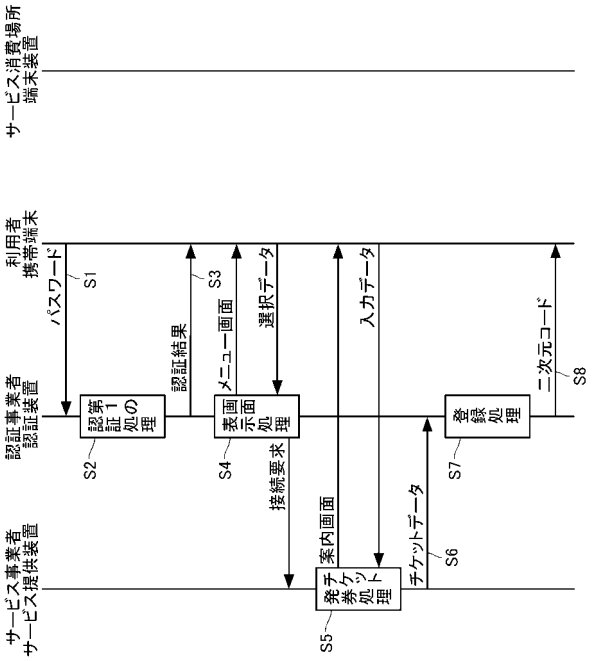
顧客番号	受け付け年月日	二次元コード	…
A0001	200△年12月1日		
…			

【図８】

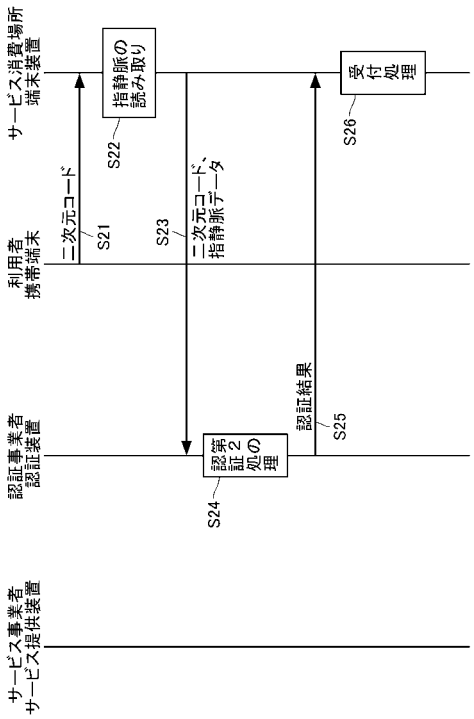
メニュー画面

サービスメニュー選択
①航空機・鉄道チケット予約
②病院予約，ホテル予約
③クレジット支払（電子カード）
④株式配当申請（郵便為替）
⑤共有サービスの利用申請
（カーシェアリング）
⑥受験申請
⑦チケット予約

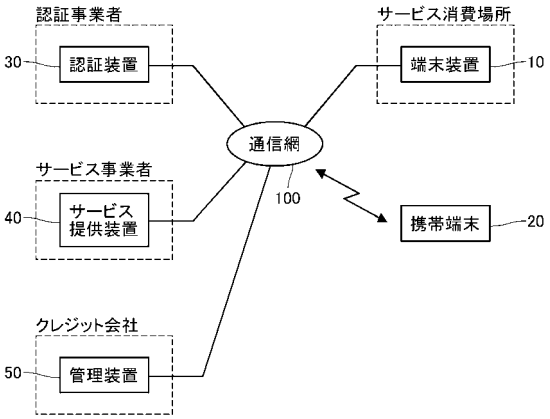
【図９】



【図１０】



【図１１】



【図１２】

管理テーブル

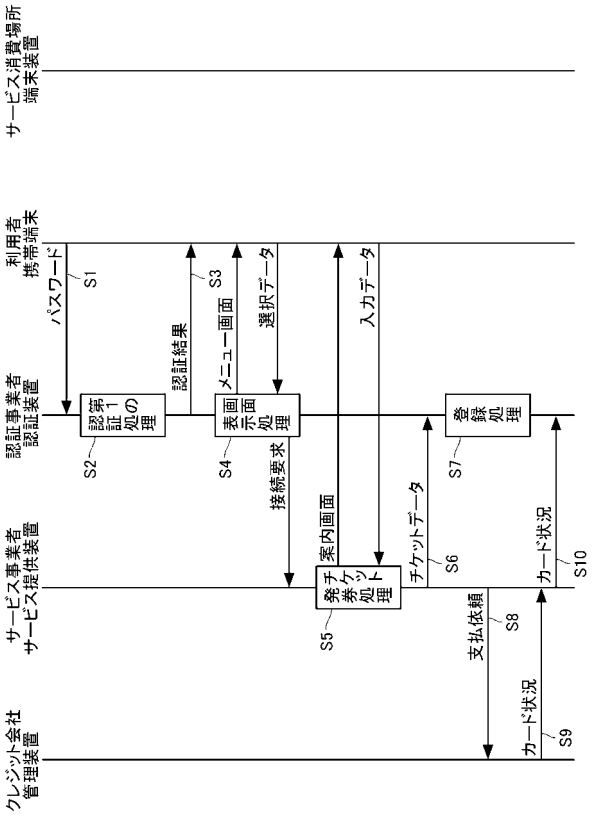
チケット番号	申し込み年月日	氏名	住所	電話番号	支払い方法	…
TK2001	200△年12月1日	△△△△	△△県△△市△△1−1−1	090−1234−5678	ABCクレジット	
…						

【図１３】

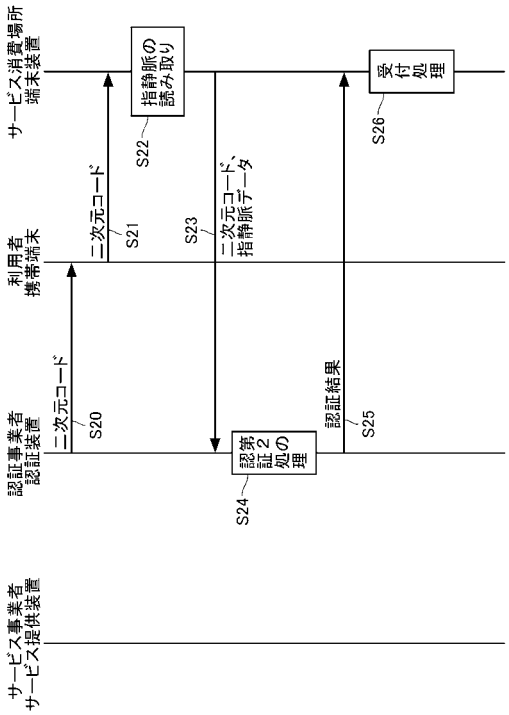
申請テーブル

識別番号	受け付け年月日	二次元コード	利用期限	…
A0001	200△年12月1日		200△年12月20日	
…				

【図１４】



【図１５】



フロントページの続き

(56)参考文献 特開２００６－０４８３９０（ＪＰ，Ａ）
特開２００２－１８３３６０（ＪＰ，Ａ）
特開２００６－２９３８１９（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｑ １０／００ － ５０／３４