(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2004-178338
(P2004-178338A)
(43)公開日　平成16年6月24日(2004.6.24)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G06K 19/10	G06K	19/00 R	5B035
G06F 17/60	G06F	17/60 414	5B058
G06K 17/00	G06F	17/60 510	5J104
G07B 15/00	G06K	17/00 L	
H04L 9/32	G07B	15/00 510	

審査請求 未請求　請求項の数 19　ＯＬ　（全 25 頁）　最終頁に続く

(21)出願番号　特願2002-344813(P2002-344813)
(22)出願日　平成14年11月28日(2002.11.28)

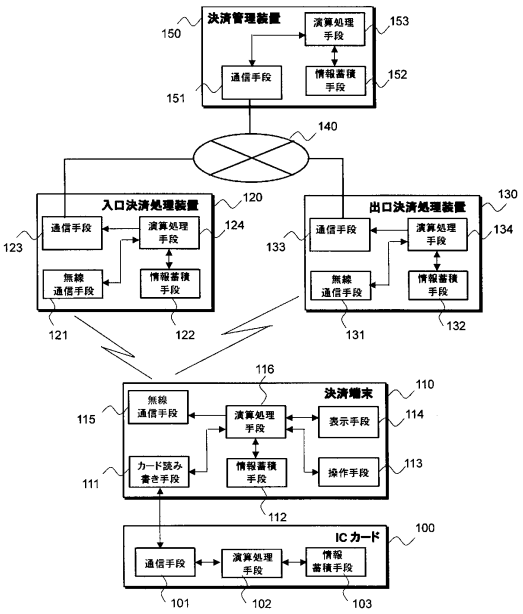
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(74)代理人　100075096
弁理士　作田　康夫
(72)発明者　相川　慎
神奈川県横浜市戸塚区吉田町２９２番地
株式会社日立製作所デジタルメディア開発本部内
(72)発明者　高見　穣
神奈川県横浜市戸塚区吉田町２９２番地
株式会社日立製作所デジタルメディア開発本部内

最終頁に続く

(54)【発明の名称】認証システム、および決済システム

(57)【要約】
【課題】本発明は、ＩＣカードを用いた高速な決済システムを提供することを目的とする。
【解決手段】本発明による決済システムは、決済端末が入場時に入口装置で生成した乱数を入口装置から受信し、退場時に暗号化した乱数を出口装置へ送信し、入口装置と出口装置に接続された管理装置にて入口装置で生成した乱数と出口装置で受信した暗号化した乱数を用いてＩＣカードの認証をする。乱数の暗号化は入場後退場前にＩＣカードにて行い、決済端末に格納しておく。決済に関する情報は入場前にＩＣカードから決済端末に送信して決済端末が格納しておき、決済端末が入場時に入口装置に送信し、入口装置は管理装置に送信し、管理装置は上記認証が成功した場合に決済に関する情報を用いて決済処理をする。
【選択図】図１

図 1



【特許請求の範囲】
【請求項１】
特定エリアの入口に設置される入口装置と、前記特定エリアの出口に設置される出口装置と、前記入口装置および前記出口装置に接続される管理装置と、を備え、前記入口装置および前記出口装置と無線通信する認証端末と通信するＩＣカードを認証する認証システムであって、
前記認証端末が前記入口装置と無線接続している間に、前記入口装置は前記入口装置で生成した乱数を前記認証端末に送信し、
前記認証端末が前記入口装置と無線接続した後前記出口装置と無線接続する前に、前記認証端末は前記乱数を前記ＩＣカードに送信し、前記ＩＣカードは前記乱数を暗号化して暗号化された乱数を前記認証端末に送信し、前記認証端末は前記暗号化された乱数を記憶し、
前記認証端末が前記出口装置と無線接続している間に、前記認証端末は前記暗号化された乱数を前記出口装置に送信し、
前記入口装置は前記入口装置で生成した乱数を前記管理装置に送信し、
前記出口装置は前記認証端末から受信した前記暗号化された乱数を前記管理装置に送信し、
前記管理装置は前記入口装置から受信した乱数を用いて前記出口装置から受信した暗号化された乱数を検証することにより前記ＩＣカードを認証すること、
を特徴とする認証システム。
【請求項２】
特定エリアに入退場することによって発生する料金の決済をする決済システムであって、
前記特定エリアの入口に設置される入口装置と、前記特定エリアの出口に設置される出口装置と、前記入口装置および前記出口装置に接続される管理装置と、前記入口装置および前記出口装置と無線通信する決済端末と、前記決済端末と通信するＩＣカードと、を備え、
前記決済端末が前記入口装置と無線接続する前に、前記ＩＣカードは前記決済を行うために使用するデータである決済関連データを前記決済端末に送信し、前記決済端末は前記決済関連データを記憶し、
前記決済端末が前記入口装置と無線接続している間に、前記決済端末は前記決済関連データを前記入口装置に送信し、前記入口装置は前記入口装置で生成した乱数を前記決済端末に送信し、
前記決済端末が前記入口装置と無線接続した後前記出口装置と無線接続する前に、前記決済端末は前記乱数を前記ＩＣカードに送信し、前記ＩＣカードは前記乱数を暗号化して暗号化された乱数を前記決済端末に送信し、
前記出口装置と無線接続している間に、前記決済端末は前記暗号化された乱数を前記出口装置に送信し、
前記入口装置は前記決済関連データと前記入口装置で生成した乱数とを前記管理装置に送信し、
前記出口装置は前記決済端末から受信した前記暗号化された乱数を前記管理装置に送信し、
前記管理装置は前記入口装置から受信した乱数を用いて前記出口装置から受信した暗号化された乱数を検証することにより前記ＩＣカードを認証し、認証に成功した場合に前記決済関連データを用いて前記料金の決済をすること、
を特徴とする決済システム。
【請求項３】
特定のエリアに入退場することによって発生する料金の決済をする決済端末に使用するＩＣカードであって、
前記決済端末と通信する通信手段と、
決済を行うために使用するデータである決済関連データと、前記決済端末から受信する乱

数を暗号化する際に使用する署名生成鍵データと、を格納する情報蓄積手段と、
前記入口装置と無線接続する前に、前記決済関連データを決済端末に送信し、前記入口装置と無線接続した後前記出口装置と無線接続する前に、前記決済端末から乱数を受信し、前記乱数を前記署名生成鍵データを用いて暗号化し、前記暗号化した乱数を前記決済端末に送信するように制御する演算手段と、
を備えることを特徴とするＩＣカード。
【請求項４】
特定のエリアに入退場することによって発生する料金の決済を行う、移動可能な決済端末で使用するＩＣカードであって、
前記決済端末と通信する通信手段と、
決済を行うために使用するデータである決済関連データを格納する決済関連データ格納領域と、認証処理を行うために使用するデータである認証関連データを格納する認証関連データ格納領域と、前記認証処理で使用する署名データを生成するために使用する署名生成鍵データを格納する署名生成鍵格納領域を含んだ情報蓄積手段と、
前記署名データを生成する演算処理手段と、
を有し、
前記決済関連データを前記決済関連データ格納領域に予め保持しておき、前記決済端末が前記エリアの入口に設置されている入口装置と通信する前に前記決済関連データを前記決済端末に送信し、
前記決済端末が前記入口装置と通信した後、前記認証関連データを前記決済端末から取得し、前記認証関連データから前記署名作成鍵データを用いて署名データを計算し、前記署名データを前記決済端末に出力すること、
を特徴とするＩＣカード。
【請求項５】
請求項４において、
前記決済関連データは、決済を一意的に識別するための番号である決済識別子と、前記ＩＣカードの保有者を識別する番号であるユーザ識別子を含んでいること、
を特徴とするＩＣカード。
【請求項６】
請求項４において、
前記決済端末が前記エリアに滞在している間に、前記決済端末との通信が途切れた後、再び通信を開始した場合に、前記決済端末に、前記決済関連データと前記認証関連データを送信し、前記決済関連データと前記認証データを前記決済端末から取得し、前記決済関連データと前記認証関連データから前記署名作成鍵データを用いて前記署名関連データを計算し、前記署名関連データを前記決済端末に出力すること、
を特徴とするＩＣカード
【請求項７】
特定のエリアに入退場することによって発生する料金の決済を、ＩＣカードを用いて行う決済端末であって、
前記ＩＣカードと通信するカード読み書き手段と、
前記エリアの入口に設置されている入口決済処理装置および前記エリアの出口に設置されている出口決済処理装置と無線通信を行う無線通信手段と、
決済を行うために使用するデータである決済関連データと、前記入口装置から送信された乱数が前記ＩＣカードにて暗号化された乱数と、を格納する情報蓄積手段と、
前記入口決済処理装置と無線接続する前に、前記ＩＣカードから前記決済関連データを受信して前記情報蓄積手段に格納し、前記入口決済処理装置と無線接続している間に、前記決済関連データを前記入口決済処理装置に送信し、前記入口決済処理装置から乱数を受信し、前記入口決済処理装置と無線接続した後前記出口決済処理装置と無線接続する前に、前記ＩＣカードに前記乱数を送信し、前記ＩＣカードにて暗号化された乱数を前記ＩＣカードから受信し、前記暗号化された乱数を前記情報蓄積手段に保存し、前記出口決済処理

装置と無線接続している間に、前記暗号化された乱数を前記出口決済処理装置に送信するように制御する演算手段と、
を備えることを特徴とする決済端末。
【請求項８】
特定のエリアに入退場することによって発生する料金の決済を、ＩＣカードを用いて行う決済端末であって、
前記ＩＣカードと通信するカード読み書き手段と、
決済を行うために使用するデータである決済関連データと認証処理において使用するデータである署名関連データとを格納する情報蓄積手段と、
前記エリアの入口に設置されている入口決済処理装置および前記エリアの出口に設置されている出口決済処理装置と無線通信を行う無線通信手段と、
を有し、
前記入口決済処理装置と無線接続する前に、前記ＩＣカードから前記決済関連データを受信して前記情報蓄積手段に格納し、
前記入口決済処理装置と無線接続している間に、前記決済関連データを前記入口決済処理装置に送信し、前記入口決済処理装置から乱数を受信し、
前記入口決済処理装置と無線接続した後前記出口決済処理装置と無線接続する前に、前記ＩＣカードに前記決済関連データと前記乱数を送信し、前記ＩＣカードで計算された署名データを前記ＩＣカードから受信し、前記決済関連データと前記乱数と前記署名データから署名関連データを生成し、前記署名関連データを情報蓄積手段に保存し、
前記出口決済処理装置と無線接続している間に、前記署名関連データを前記出口決済処理装置に送信すること、
を特徴とする決済端末。
【請求項９】
請求項８において、
前記決済端末は、前記入口決済処理装置と無線接続した後前記出口決済処理装置と無線接続する前に、前記ＩＣカードとの通信が途切れた後、再び通信を開始した場合に、前記ＩＣカードから前記決済関連データを受信して前記決済関連データ格納領域に保存すると共に、前記ＩＣカードから前記認証関連データを受信し、次に、前記ＩＣカードに、前記決済関連データと前記認証関連データを送信し、次に、前記ＩＣカードから、前記署名データを受信し、次に、前記決済関連データと前記認証関連データと前記署名データから、署名関連データを生成し、次に、前記署名関連データを決済関連データ格納領域に保存すること、
を特徴とする決済端末。
【請求項１０】
特定のエリアに入退場することによって発生する料金の決済を行うために使用するデータである決済関連データを記憶しているＩＣカードを用いて、前記決済を行う決済端末であって、
前記ＩＣカードから前記決済関連データを読み出すカード読み書き手段と、
前記ＩＣカードから読み出した前記決済関連データを格納する情報蓄積手段と、
前記エリアの入口に設置されている入口決済処理装置と無線通信し、無線通信が確立すると、前記情報蓄積手段に格納してある前記決済関連データを前記入口決済処理装置に送信する無線通信手段と、
を備えることを特徴とする決済端末。
【請求項１１】
特定のエリアに入退場することによって発生する料金の決済をＩＣカードを用いて行う決済端末であって、
前記エリアの入口に設置されている入口決済処理装置および前記エリアの出口に設置されている出口決済処理装置と無線通信し、前記入口決済処理装置から乱数を受信する無線通信手段と、

前記受信した乱数を前記ＩＣカードに送信し、前記ＩＣカードにて暗号化された乱数を前記ＩＣカードから受信するカード読み書き手段と、
前記受信した暗号化された乱数を格納する情報蓄積手段と、を備え、
前記無線通信手段は、前記出口決済処理装置と無線通信が確立すると、前記情報蓄積手段に格納してある暗号化された乱数を前記出口決済処理装置に送信すること、
を特徴とする決済端末。
【請求項１２】
特定のエリアの入口に設置され、ＩＣカードと通信可能な決済端末が前記エリアに入退場することによって発生する料金の決済を処理する入口決済処理装置であって、
前記決済端末と無線通信を行う無線通信手段と、
決済を行うために使用するデータである決済関連データと、認証処理を行うために使用するデータである認証関連データとを格納する情報蓄積手段と、
前記決済を集中管理する装置である決済管理装置と通信を行う通信手段と、
前記認証関連データを生成する演算処理手段と、
を有し、
前記決済端末と無線接続している間に、該無線接続の前に前記ＩＣカードから前記決済端末へ送信され前記決済端末に記憶されていた前記決済関連データを前記決済端末から受信して前記情報蓄積手段に保存し、前記認証関連データを生成して前記情報蓄積手段に保存し、前記決済端末に前記認証関連データを送信し、
前記決済端末と無線接続した後に、前記決済管理装置に前記決済関連データと前記認証関連データを送信すること、
を特徴とする入口決済処理装置。
【請求項１３】
請求項１２において、
前記決済関連データは、前記ＩＣカードの保有者を識別する番号である、ユーザ識別子を含んでおり、
前記決済処理装置は、前記決済管理装置から、過去に不正決済を行ったＩＣカードの前記ユーザ識別子を受信しておき、前記決済端末が前記入口決済処理装置と通信している間に、前記決済端末から受信した前記決済関連データに含まれる前記ユーザ識別子が不正であるかどうかを検証する機能を有すること、
を特徴とする入口決済処理装置。
【請求項１４】
特定のエリアの出口に設置され、ＩＣカードと通信可能な決済端末が前記エリアに入退場することによって発生する料金の決済を処理する出口決済処理装置であって、
前記決済端末と無線通信を行う無線通信手段と、
認証処理において使用するデータである署名関連データを格納する情報蓄積手段と、
前記決済を集中管理する装置である決済管理装置と通信を行う通信手段と、
を有し、
前記決済端末と無線接続している間に、前記決済端末と無線接続する前に前記ＩＣカードから前記決済端末へ送信され前記決済端末が記憶していた前記署名関連データを前記決済端末から受信して前記情報蓄積手段に保存し、前記決済端末と無線接続した後に、前記決済管理装置へ前記署名関連データを送信すること、
を特徴とする出口決済処理装置。
【請求項１５】
特定のエリアに決済端末が入退場することによって発生する料金の決済を管理する決済管理装置であって、
前記エリアの入口に設置されている決済処理装置である入口決済処理装置および前記エリアの出口に設置されている決済処理装置である出口決済処理装置と通信を行う通信手段と、
決済を行うために使用するデータである決済関連データと、認証処理を行うために使用す

るデータである認証関連データと、前記認証処理において使用するデータである署名関連データと、前記署名関連データに含まれる署名データを検証するために使用する署名検証鍵データとを格納する情報蓄積手段と、
前記署名データを検証する演算処理手段と、
を有し、
前記決済端末が入口決済処理装置と無線接続した後に、前記入口決済処理装置から前記決済関連データと前記認証関連データとを受信して前記情報蓄積手段に保存し、
前記決済端末が出口決済処理装置と無線接続した後に、前記出口決済処理装置から前記署名関連データを受信して前記情報蓄積手段に保存し、前記署名検証鍵データを用いて、前記決済関連データと、前記認証関連データと、前記署名データを検証すること、
を特徴とする決済管理装置。
【請求項１６】
請求項１５において、
前記決済関連データは、前記ＩＣカードの保有者を識別する番号である、ユーザ識別子を含んでおり、
同一の値を有する前記ユーザ識別子に関する前記署名データの検証に、一定の回数以上失敗したら、前記ユーザ識別子を、過去に不正決済を行ったＩＣカードの前記ユーザ識別子として、前記入口決済処理装置に送信すること、
を特徴とする決済管理装置。
【請求項１７】
特定エリアの入口に設置される入口装置と、前記特定エリアの出口に設置される出口装置と、前記入口装置および前記出口装置に接続される管理装置と、前記入口装置および前記出口装置と無線通信する決済端末と、前記決済端末と通信するＩＣカードと、を備え、前記特定エリアに入退場することによって発生する料金の決済をする決済システムにおける決済方法であって、
前記決済端末が前記入口装置と無線接続する前に、前記ＩＣカードが前記決済を行うために使用するデータである決済関連データを前記決済端末に送信し、前記決済端末が前記決済関連データを記憶するステップと、
前記決済端末が前記入口装置と無線接続している間に、前記決済端末が前記決済関連データを前記入口装置に送信し、前記入口装置が前記入口装置で生成した乱数を前記決済端末に送信するステップと、
前記決済端末が前記入口装置と無線接続した後前記出口装置と無線接続する前に、前記決済端末が前記乱数を前記ＩＣカードに送信し、前記ＩＣカードが前記乱数を暗号化して暗号化された乱数を前記決済端末に送信するステップと、
前記出口装置と無線接続している間に、前記決済端末が前記暗号化された乱数を前記出口装置に送信するステップと、
前記入口装置が前記決済関連データと前記入口装置で生成した乱数とを前記管理装置に送信するステップと、
前記出口装置が前記決済端末から受信した前記暗号化された乱数を前記管理装置に送信するステップと、
前記管理装置は前記入口装置から受信した乱数を用いて前記出口装置から受信した暗号化された乱数を検証することにより前記ＩＣカードを認証し、認証に成功した場合に前記決済関連データを用いて前記料金の決済をするステップと、
を備えることを特徴とする決済方法。
【請求項１８】
特定エリアの入口に設置される入口装置と、前記特定エリアの出口に設置される出口装置と、前記入口装置および前記出口装置に接続される管理装置と、を備え、前記入口装置および前記出口装置と無線通信する決済端末および前記決済端末と通信するＩＣカードが用いられる決済システムにおける、前記特定エリアに入退場することによって発生する料金の決済をする決済方法であって、

前記入口装置が、前記決済端末が前記入口装置と無線接続している間に、前記決済を行うために使用するデータであり、前記決済端末が前記ＩＣカードから予め受信して記憶している決済関連データを前記決済端末から受信するステップと、
前記入口装置が、前記決済端末が前記入口装置と無線接続している間に、前記入口装置で生成した乱数を前記決済端末に送信するステップと、
前記入口装置が、前記決済関連データと前記入口装置で生成した乱数とを前記管理装置に送信するステップと、
前記出口装置が、前記決済端末が前記出口装置と無線接続している間に、予め前記ＩＣカードが前記決済端末から前記乱数を受信して暗号化して前記決済端末に送信して前記決済端末が記憶しておいた暗号化された乱数を前記決済端末から受信するステップと、
前記出口装置が、前記決済端末から受信した前記暗号化された乱数を前記管理装置に送信するステップと、
前記管理装置が、前記入口装置から受信した乱数と前記出口装置から受信した暗号化された乱数を用いて前記ＩＣカードを認証するステップと、
前記管理装置が、前記認証に成功した場合に前記決済関連データを用いて前記料金の決済をするステップと、
を備えることを特徴とする決済方法。
【請求項１９】
認証端末に接続されたＩＣチップを認証する認証システムであって、
特定エリアの入口に設置され、認証に用いる認証情報を前記認証端末に送信する入口装置と、
前記特定エリアの出口に設置され、前記ＩＣチップに固有の情報を用いて前記ＩＣチップにて前記認証情報から生成された応答情報を前記認証端末から受信する出口装置と、
前記入口装置と前記出口装置とに接続され、前記入口装置から前記認証情報を受信し、前記出口装置から前記応答情報を受信し、前記受信した認証情報と前記受信した応答情報を用いて前記ＩＣチップを認証する管理装置と、
を備え、
前記認証端末は、前記入口装置と通信を開始すると前記入口装置から前記認証情報を受信し、前記認証情報を前記ＩＣチップに送信し、前記出口装置と通信を開始する前に前記ＩＣチップから前記応答情報を受信して記憶し、前記出口装置と通信を開始すると前記記憶した応答情報を前記出口装置に送信し、
前記ＩＣチップは、前記認証端末から前記認証情報を受信し、前記認証情報を用いて前記応答情報を生成し、前記応答情報を前記認証端末に送信すること、
を特徴とする認証システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明はＩＣカードを用いた決済システムに関する。
【０００２】
【従来の技術】ＩＣカードを用いた決済システムの従来技術として、例えば特開２０００－１９６５８８号公報（特許文献１）に記載の技術がある。該公報に記載の技術は、「ＩＣカードの正当性を路側機および中央処理装置が直接的に認証することができるＥＴＣ認証システム及び認証方法を提供する」ことを課題とし、「料金所路側機を通過する際、ＩＣカードに記憶されたレスポンスデータ、すなわち料金所路側機を通過した際に当該路側機で生成した乱数（ＲＮＤ）がチャレンジデータとして車載機経由でＩＣカードに伝送され、それを正規の秘密鍵Ｋｉｃｃで暗号化したもの、が料金所路側機に送信される。この際、ＩＣカードのＩＤ（ＩＣＣＩＤ）とＩＣカード個別鍵証明書ＣＥＲＴ－Ｋｉｃｃが共に送信される。路側機では、送られてきたデータを３つに分割、すなわちレスポンスデータであるＥ（Ｋｉｃｃ，ＲＮＤ）と、ＩＣＣＩＤと、ＩＣカード個別鍵証明書ＣＥＲＴ－Ｋｉｃｃに分割する。次にＩＣカード個別鍵証明書ＣＥＲＴ－Ｋｉｃｃ　を検証鍵ＰＣに基づいて復号処理すると、ＫｉｃｃとＩＣＣＩＤという情報を取り出すことができる。こ

のＩＣＣＩＤと、上記に分割して取り出したＩＣＣＩＤを比較してその一致判定を行ない、一致していればＩＣカードＩＤの署名確認を行なうことができる」という技術である。

【０００３】

なお、ＩＣカードを用いた決済システムの仕様として、例えばＥＭＶ仕様（非特許文献１参照（ｈｔｔｐ：／／ｗｗｗ．ｅｍｖｃｏ．ｃｏｍ／にて入手可））がある。

【０００４】

【特許文献１】

特開２０００－１９６５８８号公報

【非特許文献１】

ＥＭＶ２０００，Ｉｎｔｅｇｒａｔｅｄ Ｃｉｒｃｕｉｔ Ｃａｒｄ Ｓｐｅｃｉｆｉｃａｔｉｏｎ ｆｏｒ Ｐａｙｍｅｎｔ Ｓｙｓｔｅｍ Ｂｏｏｋ１－４，Ｖｅｒｓｉｏｎ ４．０，２０００

【０００５】

【発明が解決しようする課題】ＩＣカードには、記憶容量が大きい、暗号処理などを行うための演算処理装置（マイクロプロセッサ）を備えている、容易に内部を観察できない（耐タンパ性を有している）、といった特徴がある。しかし、ＩＣカードのマイクロプロセッサはリーダーライターのマイクロプロセッサより処理速度が遅く、またＩＣカードとリーダーライターとの通信速度も遅いのが一般的である。

【０００６】

特許文献１に記載の技術では、入退場時に車載機を介してＩＣカードと料金所路側機が通信をしており、上記の通りＩＣカードの処理速度や通信速度が遅いために、車が料金所を通過するのに時間がかかってしまう。即ち、特許文献１に記載の技術は、ＩＣカードの処理速度や通信速度を踏まえて、車が料金所を通過する短時間の間に決済の処理を高速でする点について考慮されてない。また高速化するためにＩＣカードの処理の一部を車載機のＬＳＩで処理することも考えられるが、この場合、車載機のＬＳＩは耐タンパモジュールにする必要があり、車載機のコストアップの要因となってしまう。このような高速でない、またはコストアップの要因となるシステムは実用的ではない。

【０００７】

なお、決済処理をＩＣカードで行う場合は、実績のあるＥＭＶ仕様に基づいた処理を行えることが実用的である。

【０００８】

本発明は、上記課題に鑑み、高速な決済システムを提供することを目的とする。

【０００９】

【課題を解決するための手段】上記目的を達成するために、本発明による決済システムは、決済端末が入場時に入口装置で生成した乱数を入口装置から受信し、退場時に暗号化した乱数を出口装置へ送信し、入口装置と出口装置に接続された管理装置にて入口装置で生成した乱数と出口装置で受信した暗号化した乱数を用いてＩＣカードの認証をすることを特徴とする。乱数の暗号化は入場後退場前にＩＣカードにて行い、決済端末に格納しておくことを特徴とする。決済に関する情報は入場前にＩＣカードから決済端末に送信して決済端末が格納しておき、決済端末が入場時に入口装置に送信し、入口装置は管理装置に送信し、管理装置は上記認証が成功した場合に決済に関する情報を用いて決済処理をすることを特徴とする。

【００１０】

【発明の実施の形態】

以下、本発明の実施形態について説明していく。

【００１１】

まず、第１の実施形態について説明する。図１に、本実施形態に係わる決済システムの構成要素ブロック図を示す。図１において、１００はＩＣカード、１１０は決済端末、１２０は入口決済処理装置、１３０は出口決済処理装置、１４０はネットワーク、１５０は決済管理装置である。決済端末１１０は、ＩＣカード１００と通信することが可能であり、

例えば、ＰＤＡなどの携帯端末や、ＥＴＣで用いる車載器などが考えられる。あるいは、パーソナルコンピュータのような汎用装置に、無線通信モジュールとＩＣカード通信モジュールを接続した構成であっても良い。この場合、後述する決済端末１１０の機能を果たすプログラムを汎用装置にインストールすることにより決済端末１１０を実現する。入口済処理装置１２０は、あるエリアの入口に設置され、決済端末１１０が入口を通過する時に、決済端末１１０と無線通信を行うことが可能な装置であり、例えばＥＴＣで用いる入口料金所に設置された路側器が考えられる。出口決済処理装置１３０は、あるエリアの出口に設置され、決済端末１１０が出口を通過する時に、決済端末１１０と無線通信を行うことが可能な装置であり、例えばＥＴＣで用いる出口料金所に設置された路側器が考えられる。決済管理装置１５０は、決済処理装置Ａ１２０と決済処理装置Ｂ１３０とネットワーク１４０で接続されており、入口決済処理装置１２０と出口決済処理装置１３０が行う決済処理を集中管理する。ここで、上記無線通信の方式はどのようなものであっても、本発明の範囲であり、例えば、ＥＴＣで持ちられるＤＳＲＣでもよい。また、ＩＥＥＥ８０２．１１．ｂなどの無線ＬＡＮであってもよい。あるいは、非接触ＩＣカードの通信仕様であるＩＳＯ／ＩＥＣ１４４４３であってもよい。また、ネットワーク１４０の通信方式はどのようなものであっても、本発明の範囲である。

【００１２】

次に、ＩＣカード１００の内部構成について説明する。ＩＣカード１００は、通信手段１０１と、演算処理手段１０２と、情報蓄積手段１０３を含んだ構成となっている。通信手段１０１は、決済端末１１０と通信を行い、決済端末１１０からコマンドを受信したり、決済端末１１０にレスポンスを返信したりする機能を有する。情報蓄積手段１０３は、ＩＣカードが内蔵するプログラムやデータ、あるいは決済端末１１０から取得した情報等を一時的あるいは永続的に格納する機能を有し、例えば、ＲＯＭ（Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）、ＲＡＭ（Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）、フラッシュメモリ等の半導体メモリから構成される。演算処理手段１０３は、マイクロプロセッサを用い、情報蓄積手段１０３に格納されているプログラムを実行することで、ＩＣカード全体の制御を司る。ここで、ＩＣカードはその通信方式により、接触型と非接触型に分類される。それぞれの仕様はすでに標準化されており、例えば、接触型ＩＣカードは、ＩＳＯ（Ｉｎｔｅｒｎａｔｉｏｎａｌ Ｏｒｇａｎｉｚａｔｉｏｎ ｆｏｒ Ｓｔａｎｄａｒｄｉｚａｔｉｏｎ：国際標準化機構）で、ＩＳＯ／ＩＥＣ７８１６として標準化されている。また、非接触型ＩＣカードは、ＩＳＯ／ＩＥＣ１４４４３で標準化されている。ＩＳＯ／ＩＥＣ７８１６およびＩＳＯ／ＩＥＣ１４４４３に基づくＩＣカードは、端末から送信するコマンドに従って内部で演算を行い、結果をレスポンスとして返すということを順次行っていくことで、サービスを実現するための処理を遂行していく。ここで、ＩＣカード－端末間で送受信するコマンドとレスポンスは、ＡＰＤＵ（Ａｐｐｌｉｃａｔｉｏｎ Ｐｒｏｔｏｃｏｌ Ｄａｔａ Ｕｎｉｔ）という形式としてＩＳＯ／ＩＥＣ７８１６で規定している。本発明においては、通信手段１０１は接触型と非接触型のどちらの方式であっても良く、またＩＣカード１００と決済端末１１０の間で、ＡＰＤＵを用いても本発明の適用範囲である。

【００１３】

次に、決済端末１１０の内部構成について説明する。決済端末１１０は、カード読み書き手段１１１と、情報蓄積手段１１２と、操作手段１１３と、表示手段１１４と、無線通信手段１１５と、演算処理手段１１６とを含んだ構成となっている。カード読み書き手段１１１は、ＩＣカード１００と通信するために、ＩＣカード１００にコマンドを送信（書込み）したり、ＩＣカード１００からレスポンスを受信（読み込み）したりする機能を有する。情報蓄積手段１１２は、ＩＣカード１００、入口決済処理装置１２０、出口決済処理装置１３０から取得した情報、ユーザが入力した情報、あるいはプログラム等を一時的あるいは永続的に蓄積する機能を有し、例えばハードディスクや半導体メモリ等から構成される。操作手段１１３はユーザが決済端末１１０を操作したり、認証のためのパスワードを入力したりするために用いる。表示手段１１４はユーザに対して、例えば決済金額等の

各種情報を表示する。無線通信手段１１５は、入口決済処理装置１２０あるいは出口決済処理装置１３０と無線で通信する機能を有している。演算処理手段１１６は、マイクロプロセッサを用いることで、情報蓄積手段１１２に格納されているプログラムに基づいて、決済端末１１０全体を制御し、決済処理を遂行する機能を有している。

【００１４】

次に、入口決済処理装置１２０の内部構成について説明する。入口決済処理装置１２０は、無線通信手段１２１と、情報蓄積手段１２２と、通信手段１２３と、演算処理手段１２４とを含んだ構成になっている。無線通信手段１２１は、決済端末１１０と無線で通信する機能を有している。情報蓄積手段１２２は、決済端末１１０から取得した情報、決済管理装置１５０から取得した情報、あるいはプログラム等を一時的あるいは永続的に蓄積する機能を有し、例えばハードディスクや半導体メモリ等から構成される。通信手段１２３は、決済管理装置１５０と通信する機能を有している。演算処理手段１２４は、マイクロプロセッサを用いることで、情報蓄積手段１２２に格納されているプログラムに基づいて、入口決済処理装置１２０全体を制御し、決済処理を遂行する機能を有している。

【００１５】

次に、出口決済処理装置１３０の内部構成について説明する。出口決済処理装置１３０は、無線通信手段１３１と、情報蓄積手段１３２と、通信手段１３３と、演算処理手段１３４とを含んだ構成になっている。無線通信手段１３１は、決済端末１１０と無線で通信する機能を有している。情報蓄積手段１３２は、決済端末１１０から取得した情報、決済管理装置１５０から取得した情報、あるいはプログラム等を一時的あるいは永続的に蓄積する機能を有し、例えばハードディスクや半導体メモリ等から構成される。通信手段１３３は、決済管理装置１５０と通信する機能を有している。演算処理手段１３４は、マイクロプロセッサを用いることで、情報蓄積手段１３２に格納されているプログラムに基づいて、出口決済処理装置１３０全体を制御し、決済処理を遂行する機能を有している。

【００１６】

次に、決済管理装置１５０の内部構成について説明する。決済管理装置１６０は、通信手段１５１と情報蓄積手段１５２と、演算処理手段１５３とを含んだ構成になっている。通信手段１５１は、入口決済処理端末１２０あるいは、出口決済処理端末１３０と通信する機能を有している。情報蓄積手段１５２は入口決済処理端末１２０から取得した情報、出口決済処理端末１３０から取得した情報、あるいはプログラム等を一時的あるいは永続的に蓄積する機能を有し、例えばハードディスクや半導体メモリ等から構成される。演算処理手段１５３は、マイクロプロセッサを用いることで、情報蓄積手段１５２に格納されているプログラムに基づいて、決済管理装置１５０全体を制御し、決済処理を遂行する機能を有している。

【００１７】

次に、本実施例に係わる決済システムを構成する装置が、決済で用いる情報を格納する領域について説明していく。まず、ＩＣカード１００が有する情報蓄積手段１０２に含まれるデータ格納領域を図２に示す。図２において、情報蓄積手段１０２は、決済関連データ格納領域２０１と、認証関連データ格納領域２０２と、署名生成鍵格納領域２０３を含んだ構成になっている。ここで、決済関連データ格納領域２０１は、決済を識別するために必要なデータである決済関連データを格納する領域である。また、認証関連データ格納領域２０２は、認証処理を行うために必要なデータである認証関連データを格納する領域である。また、署名作成鍵格納領域２０３は、認証処理において用いる署名データを、ＩＣカード１００が生成するために使用する鍵データを格納する領域である。ここで、署名作成鍵格納領域２０３に格納される鍵データは、共通鍵暗号方式に基づいていても、あるいは公開鍵暗号方式に基づいていても、本発明の適用範囲である。

【００１８】

次に、決済端末１１０が有する情報蓄積手段１１２に含まれるデータ格納領域を図３に示す。図３において、情報蓄積手段１１２は、決済関連データ格納領域２１１と、署名関連データ格納領域２１２を含んだ構成になっている。ここで、決済関連データ格納領域２１

１は決済関連データを格納する領域であり、署名関連データ格納領域２１２は、認証処理において生成される署名データを検証するために必要なデータである、署名関連データを格納する領域である。

【００１９】

次に、入口決済処理装置１２０が有する情報蓄積手段１２２に含まれるデータ格納領域を図４に示す。図４において、入口決済処理装置１２０は、決済関連データ格納領域２２１と、認証関連データ格納領域２２２を含んだ構成になっている。ここで、決済関連データ格納領域２２１は決済関連データを格納する領域であり、認証関連データ格納領域２２２は、認証関連データを格納する領域である。

【００２０】

次に、出口決済処理装置１３０が有する情報蓄積手段１３２に含まれるデータ格納領域を図５に示す。図５において、出口決済処理装置１３０は、署名関連データ格納領域２３１と、出口関連データ格納領域２３２を含んだ構成になっている。ここで、署名関連データ格納領域２３１は署名関連データを格納する領域であり、出口関連データ格納領域２３２は、決済端末１１０が出口決済処理装置１３０を通過した時に生成されるデータである出口関連データを格納する領域である。

【００２１】

次に、決済管理装置１５０が有する情報蓄積手段１５２に含まれるデータ格納領域を図６に示す。図６において、情報蓄積手段１５２は、ユーザの情報を管理するユーザ管理レコード２５０を、ユーザの数だけ格納している。ユーザ管理レコードはユーザ識別子により分類され、各ユーザ管理レコード２５０は、決済関連データ格納領域２５１と、認証関連データ格納領域２５２と、署名関連データ格納領域２５３と、出口関連データ格納領域２５４と、署名検証鍵格納領域２５５と、決済履歴データ格納領域２５６を含んだ構成になっている。ここで、決済関連データ格納領域２５１は決済関連データを格納する領域であり、認証関連データ格納領域２５２は、認証関連データを格納する領域であり、署名関連データ格納領域２５３は署名データを格納する領域である。また、出口関連データ格納領域２５４は出口関連データを格納する領域であり、署名検証鍵格納領域２５５は、決済管理装置１５０が署名データを検証するために用いる鍵データを格納する領域である。ここで、署名検証鍵格納領域２５４に格納される鍵データは、共通鍵暗号方式に基づいていても、あるいは公開鍵暗号方式に基づいていても、本発明の適用範囲である。また、鍵データは全ユーザで同一の値であっても、ユーザ毎に異なっていても、本発明の適用範囲である。決済履歴データ格納領域２５６は、決済管理装置１５０が、署名検証を行った履歴に関する情報を格納する領域である。

【００２２】

次に、本実施例に係わる決済システムで、決済を行うために用いる情報について説明していく。まず、決済関連データの構成を図７に示す。図７において、決済関連データ３０１は決済識別子３０２と、ユーザ識別子３０３と、状態フラグ３０４を含んだ構成になっている。ここで、決済識別子３０２は、現在実行している決済を識別するための番号を表す。また、ユーザ識別子３０３は、ＩＣカード１００の保有者を一意的に識別するための番号を表す。また、状態フラグ３０４は、ＩＣカード１００の現在の状態を表し、ＩＣカード１００の決済処理が実行中であるか否かを検出することができる。なお、決済関連データ３０１は元々、ＩＣカード１００内部に保持されているデータであり、外部から読み出すことが可能であるものとする。

【００２３】

次に、認証関連データの構成を図８に示す。図８において、認証関連データ３１０は、入口識別子３１１と、入場日時３１２と、乱数データ３１３を含んだ構成になっている。入口識別子３１１は、入口決済処理装置１２０に一意的に付与された番号である。入場日時３１２は、決済端末１１０が入口決済処理装置１２０を通過した日時の値を表す。また、乱数データ３１３は、チャレンジ・レスポンス型の認証処理を行うために使用するデータである。ここで、装置間でチャレンジ・レスポンス型の認証処理を行う場合は、予め、認

証を行う装置が署名検証鍵データを保持し、認証される装置が署名生成鍵データを保持しておき、まず、認証を行う装置が乱数データを生成して認証される装置に送信し、次に、認証される装置は、受信した乱数データと、署名作成鍵データを用いて、暗号処理に基づき署名データを作成し、認証する装置に返送する。次に、認証を行う装置は受信した署名データを、署名検証鍵データを用いて、暗号処理に基づいた検証処理を行い、検証結果が正しければ、認証成功と見なす。チャレンジ・レスポンス型の認証処理では、認証処理毎に異なる乱数を使用することで、乱数を使用しない静的な認証処理に比べて、セキュリティを向上することができるため、様々な決済処理で用いられている。例えば、前述したＩＣカードクレジット決済仕様であるＥＭＶ仕様でも、チャレンジ・レスポンス型の認証処理が用いられている。なお、チャレンジ・レスポンス型の認証処理で、署名作成および署名検証を行うために使用する暗号方式は、公開鍵暗号方式であっても、共通鍵暗号方式であっても、本発明の範囲であるものとする。

【００２４】

次に、署名関連データの構成を図９に示す。図９において、署名関連データ３２０は、決済関連データ３０１と、認証関連データ３１０と、署名データ３２１を含んだ構成になっている。ここで、署名データ３２１は、ＩＣカード１００が作成する署名データである。

【００２５】

次に、出口関連データの構成を図１０に示す。図１０において、出口関連データ３３０は、退場日時３３１と、出口識別子３３１を含んだ構成になっている。退場日時３１２は、決済端末１１０が出口決済処理装置１３０を通過した日時の値を表す。出口識別子３１１は、出口決済処理装置１３０に一意的に付与された番号である。

【００２６】

次に、本実施例に係わる決済システムの決済処理手順について説明していく。まず、決済端末１１０と、ＩＣカード１００が通信を開始した時に実行される処理フローを、図１１を用いて説明する。この処理は、ＩＣカード１００の通信方式が接触型の場合は、ＩＣカード１００を決済端末１１０に挿入し、ＩＣカード１００の通信手段１０１と、決済端末１１０のカード読み書き手段１１１を物理的に接触させ、通信処理の初期化が完了した後に行う。また、ＩＣカード１００の通信方式が非接触型の場合は、ＩＣカード１００を決済端末１１０に翳して、ＩＣカード１００の通信手段１０１と、決済端末１１０のカード読み書き手段１１１との間の通信が、電磁波を介して初期化された後に行う。図１１において、まず、決済端末１１０は処理Ｓ８１１として、ＩＣカード１００に格納されている決済アプリケーションを起動する要求を、ＩＣカード１００に送信する。次に、ＩＣカード１００は、処理Ｓ８０１として、決済端末１１０が指定した決済アプリケーションを起動する。次に、決済端末１１０は、処理Ｓ８１２として、決済関連データ３０１の読み出し要求を、ＩＣカード１００に送信する。次に、ＩＣカード１００は、処理Ｓ８０２として、決済関連データ３０１を決済関連データ格納領域２０１から読み出して、決済端末１１０に送信する。次に、決済端末１１０は、処理Ｓ８１３として、決済関連データ３０１を決済関連データ格納領域２１１に格納する。ここで、ＩＣカード１００から読み出した決済関連データ３０１には、状態フラグ３０４が含まれており、決済端末１１０は状態フラグをチェックすることで、ＩＣカード１００の決済処理が実行中であるか否かを検出することができる。図１１に示した処理フローにおいては、決済端末１１０がＩＣカード１００から読み出した状態フラグ３０４は、ＩＣカード１００の決済処理がまだ実行中でない場合であるとする。次に、決済端末１１０は、ＩＣカード１００の正当性を検証する為に、処理Ｓ８１４として、カード認証処理を開始し、ＩＣカード１００は、処理Ｓ８０３として、カード認証処理を行う。例えば、処理Ｓ８１４および処理Ｓ８０３で行うカード認証処理として、チャレンジ・レスポンス型の認証処理を用いることが考えられる。あるいは他の認証方法であっても、本発明の適用範囲である。処理Ｓ８１４および処理Ｓ８０３で実施したカード認証処理が成功したら、次に、決済端末１１０はカード１００の保有者の正当性を検証する為に、処理Ｓ８０４としてカード保有者検証処理を開始し、ＩＣカード１００は処理Ｓ８０４としてカード保有者検証処理を実施する。カード保有者検証の

方法としては、例えば、予めＩＣカード１００の内部に暗証番号データが格納されていて、処理Ｓ８１５として、カード１００の保有者が決済端末１１０の操作手段１１３を用いて入力した暗証番号を、ＩＣカード１００に送信し、処理Ｓ８０４として、受信した暗証番号が、内部に保持している暗証番号と等しいかを検証することが考えられる。以上、決済端末１１０と、ＩＣカード１００が通信を開始した時に実行される処理フローを説明したが、処理Ｓ８１４、処理Ｓ８０３、処理Ｓ８１５、処理Ｓ８０４を実行しなくても、本発明の適用範囲である。

【００２７】

次に、決済端末１１０が、あるエリアの入口を通過する時に実行する、入口決済処理装置１２０との通信処理フローを、図１２を用いて説明する。図１２において、まず、決済端末１１０は、入口決済処理装置１２０に対し、処理Ｓ９１１として、無線接続要求を送信する。そして、入口決済処理装置１２０は、処理Ｓ９２１として、無線接続処理を行い、決済端末１１０と入口決済処理装置１２０の間の無線通信路を確立する。ここで、不図示のセンサを用いて決済端末が入口を通過しようとしていることを検知し、かつ、決済端末１１０の電源がオフになっているなどして、入口決済処理装置１２０に無線接続要求が届かない場合は、遮断機等を用いて入口を閉鎖することが考えられる。次に、決済端末１１０は、処理Ｓ９１１として、決済関連データ格納領域２１１に保持している決済関連データ３０１を、入口決済処理装置１２０に送信する。そして、入口決済処理装置１２０は、処理Ｓ９２２として、決済関連データ３０１を受信し、処理Ｓ９２３として、決済関連データ３０１を、決済関連データ格納領域２２１に保存する。次に、入口決済処理装置１２０は、処理Ｓ９２４として、認証関連データ３１０を生成し、認証関連データ格納領域２２２に保存する。そして、入口決済処理装置１２０は、処理Ｓ９２５として、認証関連データ３１０を、決済端末１１０に送信する。決済端末１１０は、処理Ｓ９１３として認証関連データ３１０を受信すると、処理Ｓ９１４として、ＩＣカード１００に、決済関連データ３０１と認証関連データ３１０を送信することで、署名データ３２１の計算要求を行う。そして、ＩＣカード１００は、処理Ｓ９０１として、決済関連データ３０１と認証関連データ３１０を用いて、署名データ３２１を計算し、決済端末１１０に送信する。ここで、ＩＣカード１００は、署名データ３２１を計算するために、署名生成鍵格納領域２０３に格納されている署名生成鍵を使用するものとする。また、ＩＣカード１００は、署名データ３２１を計算したら、ＩＣカード１００が保持している状態フラグ３０４を、決済処理実行中の状態に変更する。次に、決済端末１１０は、処理Ｓ９１５として、署名データ３２１と、決済関連データ３０１と、認証関連データ３１０から、署名関連データ３２０を生成し、署名関連データ格納領域２１２に保存する。次に、決済端末１１０は、処理Ｓ９１６として、認証関連データ３１０を、ＩＣカード１００に保存する要求を発行する。次に、ＩＣカード１００は、処理Ｓ９０２として、受信した認証関連データ３１０を、認証関連データ格納領域２０２に保存する。

【００２８】

以上説明した処理において、ＩＣカード１００が計算した署名データ３２１は、決済関連データ３０１と認証関連データ３１０から作成されたものであり、認証関連データ３１０は、入口識別子３１１と、入場日時３１２と、乱数データ３１３を含んでいるため、署名データ３２１は、決済端末１１０が入口決済端末処理装置１２０を通過したことをチャレンジ・レスポンス型認証で、証明するためのデータとなっていることが分かる。

【００２９】

次に、決済端末１１０が入口決済処理装置１２０を通過後に、入口決済処理装置１２０が決済管理装置１５０と行う通信処理フローを、図１３を用いて説明する。図１３では、まず、入口決済処理装置１２０は、処理Ｓ１００１として、決済関連データ格納領域２２１に保存してある決済関連データ３０１を、決済管理装置１５０に送信する。そして、決済管理装置１５０は、処理Ｓ１０１１として、決済関連データ３０１を受信し、処理Ｓ１０１２として、決済関連データ３０１を、対応するユーザ管理レコード２５０内の決済関連データ格納領域２５１に保存する。次に入口決済処理装置１２０は、処理Ｓ１００２とし

て、認証関連データ格納領域２２２に保存してある認証関連データ３１０を、決済管理装置１５０に送信する。そして、決済管理装置１５０は、処理Ｓ１０１３として、認証関連データ３１０を受信し、処理Ｓ１０１４として、認証関連データ３１０を、対応するユーザ管理レコード２５０内の認証関連データ格納領域２５２に保存する。

【００３０】

次に、決済端末１１０が、入口決済処理端末１２０を通過後に、ＩＣカード１００が決済端末１１０から引き抜かれ、ＩＣカード１００と決済端末１１０との通信が切断してしまったり、決済端末１１０の電源がオフになってしまったりした時に、ＩＣカード１１０と決済端末１１０の通信を再開する場合の処理フローを図１４に示す。図１４においては、まず、決済端末１１０は処理Ｓ１１１１として、ＩＣカード１００に格納されている決済アプリケーションを起動する要求を、ＩＣカード１００に送信する。次に、ＩＣカード１００は、処理Ｓ１１０１として、決済端末１１０が指定した決済アプリケーションを起動する。次に、決済端末１１０は、処理Ｓ１１１２として、決済関連データ３０１の読み出し要求を、ＩＣカード１００に送信する。次に、ＩＣカード１００は、処理Ｓ１１０２として、決済関連データ３０１を決済関連データ格納領域２０１から読み出して、決済端末１１０に送信する。次に、決済端末１１０は、処理Ｓ１１１３として、決済関連データ３０１を決済関連データ格納領域２１１に格納する。ここで、ＩＣカード１００から読み出した決済関連データ３０１には、状態フラグ３０４が含まれており、図１４に示した処理フローにおいては、ＩＣカード１００から読み出した状態フラグは、決済処理実行中である状態を示しているものとする。

【００３１】

次に、決済端末１１０は、ＩＣカード１００の正当性を検証する為に、処理Ｓ１１１４として、カード認証処理を開始し、ＩＣカード１００は、処理Ｓ１１０３として、カード認証処理を行う。次に、決済端末１１０はカード１００の保有者の正当性を検証する為に、処理Ｓ１１０４としてカード保有者検証処理を開始し、ＩＣカード１００は処理Ｓ１１０４としてカード保有者検証処理を実施する。

図１４において、ここまでの処理は、先に図１１を用いて説明した決済端末１１０と、ＩＣカード１００が通信を開始した時に実行される処理フローと同じである。次に、決済端末１１０は、処理Ｓ１１１６として認証関連データ３１０の読み出し要求を、ＩＣカード１００に送信する。次に、ＩＣカード１００は、処理Ｓ１１０５として、認証関連データ３１０を認証関連データ格納領域２０２から読み出して、決済端末１１０に送信する。次に、決済端末１１０は、認証関連データ３１０を受信すると、処理Ｓ１１１７として、ＩＣカード１００に、決済関連データ３０１と認証関連データ３１０を送信することで、署名データ３２１の計算要求を行う。そして、ＩＣカード１００は、処理Ｓ１１０６として、決済関連データ３０１と認証関連データ３１０を用いて、署名データ３２１を計算し、決済端末１１０に送信する。ここで、ＩＣカード１００は、署名データ３２１を計算するために、署名生成鍵格納領域２０３に格納されている署名生成鍵を使用するものとする。次に、決済端末１１０は、処理Ｓ１１１８として、署名データ３２１と、決済関連データ３０１と、認証関連データ３１０から、署名関連データ３２０を生成し、署名関連データ格納領域２１２に保存する。

【００３２】

以上の処理を行うことで、決済端末１１０を、入口決済処理装置１２０を通過した直後の状態に戻すことが可能になる。

【００３３】

次に、決済端末１１０が、あるエリアの出口を通過する時に実行する、出口決済処理装置１３０との通信処理フローを、図１５を用いて説明する。図１５において、まず、決済端末１１０は、出口決済処理装置１３０に対し、処理Ｓ１２１１として、無線接続要求を送信する。そして、出口決済処理装置１３０は、処理Ｓ１２２１として、無線接続処理を行い、決済端末１１０と出口決済処理装置１３０の間の無線通信路を確立する。ここで、不図示のセンサを用いて決済端末が入口を通過しようとしていることを検知し、かつ、決済

端末１１０の電源がオフになっているなどして、出口決済処理装置１３０に無線接続要求が届かない場合は、遮断機等を用いて入口を閉鎖することが考えられる。次に、決済端末１１０は、処理Ｓ１２１２として、署名関連データ格納領域２１２に保持している署名関連データ３２０を、出口決済処理装置１３０に送信する。そして、出口決済処理装置１３０は、処理Ｓ１２２２として、署名関連データ３２０を受信し、処理Ｓ１２２３として、署名関連データ３２０を、署名関連データ格納領域２３１に保存する。次に、出口決済処理装置１３０は、処理Ｓ１２２４として、出口関連データ３３０を発行し、処理Ｓ１２２５として、出口関連データ３３０を、決済端末１１０に送信する。そして、出口決済処理装置１３０は、処理Ｓ１２２６として、出口関連データ３３０を出口関連データ格納領域２３２に保存する。次に、決済端末１１０が、処理Ｓ１２１３として、出口関連データ３３０を受信すると、決済端末１１０は、処理Ｓ１２１４として、決済終了処理を実行する。また、処理Ｓ１２１４では、ＩＣカード１００に対して、決済終了処理要求を発行する。これにより、ＩＣカード１００は、処理Ｓ１２０１として、決済終了処理を行う。ここで、決済端末１１０は、処理Ｓ１２１４で、出口関連データ３３０の保存を行っても良い。あるいは、出口関連データ３３０をＩＣカード１００に送信し、ＩＣカードが処理Ｓ１２０１で、出口関連データ３３０の保存を行っても、本発明の適用の範囲である。

【００３４】

次に、決済端末１１０が出口決済処理装置１３０を通過後に、出口決済処理装置１３０が決済管理装置１５０と行う通信処理フローを、図１６を用いて説明する。図１６では、まず、出口決済処理装置１３０が、処理Ｓ１３０１として、署名関連データ格納領域２３１に保持している署名関連データ３２０を、決済管理装置１５０に送信する。そして、決済管理装置１５０は、処理Ｓ１３１１として署名関連データ３２０を受信し、処理Ｓ１３１２として署名関連データ３２０を、対応するユーザ元利レコード２５０内の署名関連データ格納領域２５３に保存する。次に、出口決済処理装置１３０が、処理Ｓ１３０２として、出口関連データ格納領域２３２に保持している出口関連データ３３０を、決済管理装置１５０に送信する。そして、決済管理装置１５０は、処理Ｓ１３１３として出口関連データ３３０を受信し、処理Ｓ１３１４として出口関連データ３３０を、対応するユーザ管理レコード２５０内の出口関連データ格納領域２５４に保存する。

【００３５】

次に、決済管理装置１５０は、処理Ｓ１３１５として、署名関連データの検証処理を行う。ここで、決済管理装置１５０が処理Ｓ１３１５で行う署名関連データの検証処理を、図１７を用いて説明する。ここで、署名関連データの検証処理は、対応するユーザ管理レコード２５０に含まれる各種情報を用いて実施する。まず、処理Ｓ１４０１として、署名関連データ格納領域２５３から読出した署名関連データ３２０は、決済関連データ格納領域２５１から読出した決済関連データ３０１と同じ値を含んでいることを確認する。もし処理Ｓ１４０１が失敗したら検証失敗とする。もし処理Ｓ１４０１が成功したら、次に、処理Ｓ１４０２として、署名関連データ３２０は、認証関連データ２５２から読出した認証関連データ３１０と同じ値を含んでいることを確認する。もし処理Ｓ１４０２が失敗したら検証失敗とする。もし処理Ｓ１４０２が成功したら、次に処理Ｓ１４０３として、署名関連データ３２０内の決済関連データ３０１に含まれるユーザ識別子３０３に対応する署名検証鍵４０１を、署名検証鍵格納領域２５５から取り出す。そして、署名関連データ３２０内に含まれる署名データ３２１の検証を、署名検証鍵４０１を用いて行う。ここで、前述したように、署名データ３２１は、ＩＣカード１００が、決済関連データ３０１と認証関連データ３１０から作成したものであり、認証関連データ３１０は、入口識別子３１１と、入場日時３１２と、乱数データ３１３を含んでおり、出口関連データ格納領域２５４に格納されている出口関連データ３３０は、退場日時３３１と、出口識別子３３２を含んでいるため、署名データ３２１の検証が成功すれば、ＩＣカード１００は正当なカードであり、且つ、決済端末１１０は、入口決済端末処理装置１２０を正常に通過した後に、出口決済処理装置１３０を通過したことが証明できる。また、入口識別子３１１と、出口識別子３３２を用いて、エリアの通行料金を算出することが可能である。したがって、も

し処理Ｓ１４０４が成功したら、入口識別子３１１と、出口識別子３３２より算出した通行料金をＩＣカード１００の保有者の決済口座から特定の金額を引き落とすなどして、決済処理を完了させる。なお、決済管理装置１５０には、ユーザから徴収した金額を記憶管理する、徴収料金データ記憶手段を設け、徴収料金データ記憶手段に、各ユーザから徴収した通行料金の合計を記憶しておき、徴収料金管理を行うという構成であっても良い。ここで、本発明は、ＥＭＶ仕様が適用可能な処理フローとなっているため、例えば、ＥＭＶ仕様に基づいたクレジットカード決済やデビットカード決済を行うことが考えられる。この場合、決済管理装置１５０は、クレジット会社や銀行のセンターコンピュータとしての機能を有する構成であっても良いし、クレジット会社や銀行のセンターコンピュータに、ネットワークで接続し、決済処理を代行してもらうという構成であっても良い。あるいはもし、処理Ｓ１４０４が失敗したら、不正決済と見なす。ここで、不正決済が発生したら、ユーザ識別子３０３から、ＩＣカード１００の保有者を特定するなどして、不正決済の事後処理を実行する。なお、決済管理装置１５０が署名関連データ３２０の検証処理を実行した結果は、決済履歴データ格納領域２５６に格納しておき、後から履歴を調べられるようにしておく。

【００３６】

以上、図１１から図１７を用いた説明した処理フローを実行することで、決済端末１１０と入口決済処理装置１２０の間の通信処理時間を短くすることができる。また、決済端末１１０と出口決済処理装置１３０の間の通信処理時間を短くすることができる。したがって、本発明は、美術館やコンサート会場などの施設、鉄道駅の改札、あるいは、有料道路への入退場等に伴って発生する決済処理を、高速に行う場合に適している。

【００３７】

このような決済処理では、利便性の観点から入退場時の処理時間が、約０．５秒未満であることが望ましい。もし入退場時にＩＣカードとの通信が発生する場合、セキュリティを高め、それにともないデータ量が増加すると、ＩＣカード内の演算速度やＩＣカードとの通信速度が遅いため、入退場時の処理時間が０．５秒を下回るのは非常に困難である。一方で、本発明では、入退場時に、ＩＣカードとの通信が発生しないため、入退場時の処理時間を０．５秒より短くすることは容易である。

【００３８】

なお、本実施例では、入口決済処理装置１２０と出口決済処理装置１３０は、別装置として説明を行ってきたが、同じ地点に入口と出口がある場合は、入口決済処理装置１２０と出口決済処理装置１３０の機能を併せ持つ装置を用いて、入退場に伴う決済処理を行う構成であっても、本発明の適用範囲である。

【００３９】

また、決済端末１１０が、図１１の処理Ｓ８１４、および図１３の処理Ｓ１１１４として行うカード認証処理を実行しない場合も本発明の適用範囲であるが、この場合、決済端末１１０の内部で暗号処理を行う必要は無く、また、機密性のあるデータを保存する必要も無い。さらに、決済端末１１０の内部モジュールを、耐タンパモジュールにする必要は無い。したがって、この場合は、決済端末１１０を低コストで生産することが可能になる。

【００４０】

さらに、本発明に係わる処理フローは、ＥＭＶ仕様が適用可能な処理フローとなっている。例えば、図１１で示した処理Ｓ８１２として行う決済関連データ３０１の読出し処理は、ＥＭＶ仕様における「カードデータ読出し処理」に相当する。また、図１２で示した処理Ｓ９１４として行う署名データの生成処理は、ＥＭＶ仕様における「カードアクション分析」に相当する。また、図１５で示した処理Ｓ１２１２で行う署名関連データの送信処理および処理Ｓ１２１３で行う出口関連データの受信処理は、ＥＭＶ仕様における「オンライン処理」に相当する。また、図１５で示した処理Ｓ１２１４で行う決済終了処理は、ＥＭＶ仕様における「終了処理」に相当する。したがって、本発明を適用することで、ＥＭＶ仕様に準拠した決済システムを構築することが可能になる。

【００４１】

次に、本発明に係わる第２の実施例について説明する。図１８は、有料道路の通行料を、自動車を停止させることなく徴収する、自動料金徴収システムに、本発明を適用したブロック図である。図１８において、１０は自動車、１００はＩＣカード、１１０は決済端末、１２０は入口決済処理装置、１３０は出口決済処理装置、１４０はネットワーク、１５０は決済管理装置、１６０と１７０は無線アンテナである。ここで、ＩＣカード１００の内部構成は第１の実施例で説明したＩＣカードと同じである。また、決済端末１１０の内部構成は第１の実施例で説明した決済端末と同じであり、自動車１０に搭載して用いるものとする。また、入口決済処理装置１２０の内部構成は、第１の実施例で説明した入口決済処理装置と同じであり、有料道路の入口料金所に設置されているものとする。そして、入口決済処理装置１２０は無線アンテナ１６０と接続され、入口料金所を通過する自動車１０に搭載されている決済端末１１０と無線通信できるようになっている。

また、出口決済処理装置１３０の内部構成は、第１の実施例で説明した出口決済処理装置と同じであり、有料道路の出口料金所に設置されている。そして、出口決済処理装置１３０は無線アンテナ１７０と接続され、出口料金所を通過する自動車１０に搭載されている決済端末１１０と無線通信できるようになっている。また、決済管理装置１５０の内部構成は、第１の実施例で説明した決済管理装置と同じであり、入口決済処理装置１２０と出口決済処理装置１３０とネットワーク１４０で接続されており、決済に関する通信を行うことができる。

【００４２】

ここで、本実施例においては、入口決済処理装置１２０が有する情報蓄積手段１２２に含まれるデータ格納領域は図１９に示した構成であるものとする。図１９において、情報蓄積手段１２２は、決済関連データ格納領域２２１と、認証関連データ格納領域２２２と、不正ユーザ識別子格納領域２２３と、センタ公開鍵格納領域２２４を含んだ構成になっている。ここで、決済関連データ格納領域２２１は決済関連データを格納する領域であり、認証関連データ格納領域２２２は、認証関連データを格納する領域である。また、不正ユーザ識別子格納領域２２３は、不正決済を行う可能性のあるユーザ識別子を格納している。なお、不正ユーザ識別子格納領域２２３に格納する不正なユーザ識別子は、入口決済処理装置１２０が決済管理装置１５０と通信を行うときに、決済管理装置１５０から取得する。また、センタ公開鍵格納領域２２４は、決済管理装置１５０を運用している組織が、公開鍵暗号方式に基づいて発行した、公開鍵を格納している。ここで、センタ公開鍵格納領域２２４に格納する公開鍵は、どのような公開鍵暗号方式を用いて生成したものであったも、本発明の適用範囲であるものとする。

【００４３】

また、本実施例においては、ＩＣカード１００が保持する決済関連データ３０１は、図２０に示す構成になっているものとする。図２０において、決済関連データ３０１は、は決済識別子３０２と、ユーザ識別子３０３と、状態フラグ３０４と、ユーザ証明書３０５を含んだ構成になっている。ここで、決済識別子３０２は、現在実行している決済を識別するための番号を表す。また、ユーザ識別子３０３は、ＩＣカード１００の保有者を一意的に識別するための番号を表す。また、状態フラグ３０４は、ＩＣカード１００の現在の状態を表す。また、ユーザ証明書３０５は、ユーザ識別子３０３が正当な値であることを検証するためのデジタル署名を含んでいる。ここで、このデジタル署名は、公開鍵暗号方式に基づき、決済管理装置１５０を運用している組織が管理している秘密鍵により生成されるものとする。またユーザ証明書３０５は、予めＩＣカード１００に格納しておき、入口決済処理装置１２０のセンタ公開鍵格納領域２２４に格納されている公開鍵を用いて、検証を行うことができるものとする。

【００４４】

本実施例に係わる自動料金徴収システムでは、自動車１０に搭載されている決済端末１１０に、ＩＣカード１００を挿入した時に、ＩＣカード１００と決済端末１１０は、図１１を用いて説明した処理フローを実施する。また、自動車１０が入口料金所を通過する時に、決済端末１１０と入口決済処理装置１２０は、図１２を用いて説明した処理フローを実

施する。また、自動車１０が入口料金所を通過した後に、入口決済処理装置１２０と決済管理装置１５０は、図１３を用いて説明した処理フローを実施する。また、自動車１０が有料道路上を走行している時に、ＩＣカード１００が決済端末１１０から引き抜かれ、ＩＣカード１００と決済端末１１０との通信が切断してしまったり、決済端末１１０の電源がオフになってしまったりした場合に、ＩＣカード１１０と決済端末１１０は、図１４を用いて説明した処理フローを実施する。また、自動車１０が出口料金所を通過する時に、決済端末１１０と出口決済処理装置１３０は、図１５を用いて説明した処理フローを実施する。また、自動車１０が出口料金所を通過した後に、出口決済処理装置１３０と決済管理装置１５０は、図１６を用いて説明した処理フローを実施する。

【００４５】

ここで、本実施例においては、上述したように、車１０が入口料金所を通過する時に、決済端末１１０と入口決済処理装置１２０との間で、図１２を用いて説明した処理フローを実施するが、図１２に示した処理Ｓ９２２では、入口決済処理装置１２０は決済端末１１０から決済関連データ３０１を受信するが、決済関連データ３０１を受信後、まず、決済関連データ３０１に含まれるユーザ証明書３０５を、センタ公開鍵格納領域２２４に格納されている公開鍵を用いて検証する。もし検証に失敗したら、不正決済が実施される可能性があるので、入口料金所に設置されている遮断機を下ろすなどして、車１０を停止させる。あるいはもし、ユーザ証明書３０５の検証に成功したら、次にユーザ識別子３０３が、不正ユーザ識別子格納領域２２３に格納されているかどうかを確認する。もし、格納されているならば、不正決済が実施される可能性があるので、入口料金所に設置されている遮断機を下ろすなどして、車１０を停止させる。これによって、不正決済を防止することが可能になる。あるいは、もし格納されていなければ、次の処理Ｓ９２３に進む。ここで、入口料金所で車１０を停止させる方法については、どのような方法であっても、本発明の適用範囲である。

【００４６】

なお、本実施例において、不正ユーザ識別子格納領域２２３に格納する不正なユーザ識別子は、入口決済処理装置１２０が決済管理装置１５０と通信を行うときに、決済管理装置１５０から取得する。この時、決済管理装置１５０が、どのユーザ識別子を、不正なユーザ識別子として、入口決済処理装置１２０に送信するかを決定する方法としては、以下のものが適用できる。まず、決済管理装置１５０が検証に失敗した署名関連データに含まれるユーザ識別子を、必ず不正なユーザ識別子として、入口決済処理装置１２０に送信するという方法を本実施例に適用できる。この方法を用いると、不正決済を防止するためのセキュリティは向上するが、一方で、ある車が、正しいＩＣカードと決済端末を用いたのにもかかわらず、無線通信などのノイズの影響により、たまたま署名検証が失敗してしまった場合は、次に、この車は入口料金所で必ず停止させられてしまうことになり、ユーザの利便性が低下する可能性がある。これを解決するために、決済管理装置１５０は、特定のユーザ識別子に対応する署名関連データの検証が、ある回数以上失敗した場合に、そのユーザ識別子を、不正なユーザ識別子として、入口決済処理装置１２０に送信する方法も、本実施例に適用可能である。この方法を用いると、繰り返し不正決済を行う決済端末およびＩＣカードだけを取り締まることが可能になる。

【００４７】

次に、本発明に係わる第３の実施例について説明する。図２１は、本実施形態に係わる決済システムの構成要素ブロック図である。図２１に示したブロック図は、先に第１の実施例の説明した図１のブロック図の構成に、不正端末取締装置１８０を追加した構成になっている。ここで、不正端末取締装置１８０は、出口決済処理装置と共に、出口に設置され、不正決済を行った決済端末１１０を取り締まる機能を有する。不正端末取締装置１８０は、無線通信手段１８１と、情報蓄積手段１８２と、通信手段１８３と、演算処理手段１８４とを含んだ構成になっている。無線通信手段１８１は、決済端末１１０と無線で通信する機能を有している。情報蓄積手段１８２は、決済端末１１０から取得した情報、決済管理装置１５０から取得した情報、あるいはプログラム等を一時的あるいは永続的に蓄積

する機能を有し、例えばハードディスクや半導体メモリ等から構成される。通信手段１８３は、決済管理装置１５０と通信する機能を有している。演算処理手段１８４は、マイクロプロセッサを用いることで、情報蓄積手段１８２に格納されているプログラムに基づいて、不正端末取締装置１８０全体を制御する。

【００４８】

本実施例においては、決済端末１１０が不正端末取締装置１８０を通過する時に、不正決済を行っていたら、通行を取り締まることができる。具体的な方法としては、第２の実施例で説明したように決済管理装置１５０で署名検証に失敗したユーザに対応するユーザ識別子を、不正な決済をユーザ識別子とする。そして、決済管理装置１５０から不正端末取締装置１８０に不正ユーザ識別子を配信しておく。そして、第２の実施例で説明した、入口決済処理装置１２０が、決済端末１１０が不正なユーザ識別子を送信した場合に取り締まるのと同じ方法で、不正端末取締装置１８０は、決済端末１１０が通過する時に、不正な決済端末１１０を取り締まる。例えば、出口に、ユーザが通過しなければならない、２つのゲートを設け、ユーザが最初に通過するゲートに出口決済処理装置を設置し、次のゲートに不正端末取締装置１８０を設置することで、不正な決済端末１１０を取り締まることができる。

【００４９】

なお、以上説明した全ての実施例において、不正な決済端末を取り締まることに加え、本発明による決済システムを利用するユーザからデポジットを予め受け取っておく方法により、不正取引による損失を補償することができる。例えば、平均的な支払額が１０００円である有料道路において、本発明による決済システムを利用するユーザからデポジットとして１０００円を事前に受け取る。不正取引のなかったユーザには本システムから退会する際にデポジットの１０００円を返却する。不正取引を行ったユーザに対しては、上記実施例の通り不正ユーザを取り締まると同時にデポジットを返却しない。

【００５０】

また、上記実施例ではＩＣカードを用いる実施例として説明したが、これをＩＣチップを備えＩＣカード同様の機能を有する物であれば形態を問わずあらゆる物に代えて構わない。

【００５１】

【発明の効果】以上説明したように、本発明によれば、高速な決済システムを提供することができる。

【図面の簡単な説明】

【図１】第１の実施例に係わる、決済システムの構成要素ブロック図である。

【図２】ＩＣカード１００が有する情報蓄積手段１０２に含まれるデータ格納領域の構成図である。

【図３】決済端末１１０が有する情報蓄積手段１１２に含まれるデータ格納領域の構成図である。

【図４】入口決済処理装置１２０が有する情報蓄積手段１２２に含まれるデータ格納領域の構成図である。

【図５】出口決済処理装置１３０が有する情報蓄積手段１３２に含まれるデータ格納領域の構成図である。

【図６】決済管理装置１５０が有する情報蓄積手段１５２に含まれるデータ格納領域の構成図である。

【図７】決済関連データの構成図である。

【図８】認証関連データの構成図である。

【図９】署名関連データの構成図である。

【図１０】出口関連データの構成図である。

【図１１】決済端末１１０とＩＣカード１００との通信処理フロー図である。

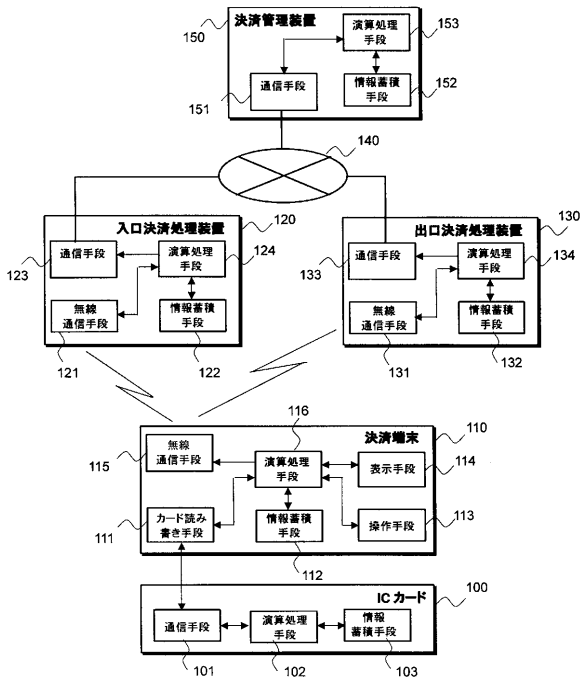
【図１２】決済端末１１０と入口決済処理装置１２０との通信処理フロー図である。

【図１３】入口決済処理装置１２０と決済管理装置１５０との通信処理フロー図である。

【図１４】決済端末１１０とＩＣカード１００との通信処理フロー図である。
【図１５】決済端末１１０と出口決済処理装置１３０との通信処理フロー図である。
【図１６】出口決済処理装置１３０と決済管理装置１５０との通信処理フロー図である。
【図１７】決済管理装置１５０が行う署名関連データの検証処理フロー図である。
【図１８】第２の実施例に係わる、自動料金徴収システムの構成要素ブロック図である。
【図１９】入口決済処理装置１２０が有する情報蓄積手段１２２に含まれるデータ格納領域の構成図である。
【図２０】決済関連データの構成図である
【図２１】第３の実施例に係わる、決済システムの構成要素ブロック図である。
【符号の説明】
１００…ＩＣカード、１０１…通信手段、１０２…演算処理手段、１０３…情報蓄積手段、１１０…決済端末、１１１…カード読み書き手段、１１２…情報蓄積手段、１１３…操作手段、１１４…表示手段、１１５…無線通信手段、１１６…演算処理手段、１２０…入口決済処理装置、１２１…無線通信手段、１２２…情報蓄積手段、１２３…通信手段、１２４…演算処理手段、１３０…出口決済処理装置、１３１…無線通信手段、１３２…情報蓄積手段、１３３…通信手段、１３４…演算処理手段、１４０…ネットワーク、１５０…決済管理装置、１５１…通信手段、１５２…情報蓄積手段、１５３…演算処理手段

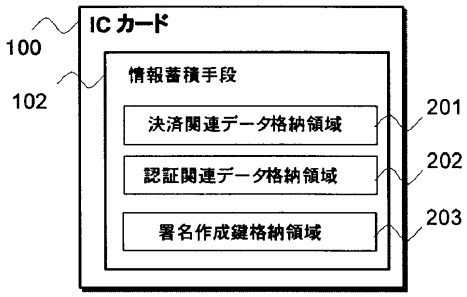
【図１】

図 1



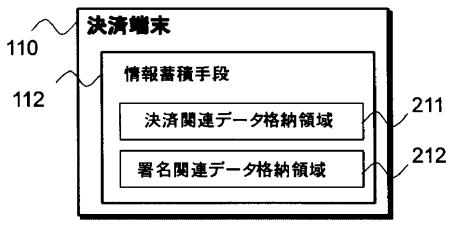
【図２】

図 2



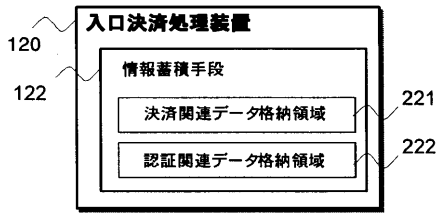
【図３】

図 3



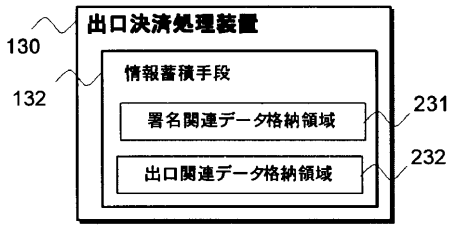
【図４】

図 4



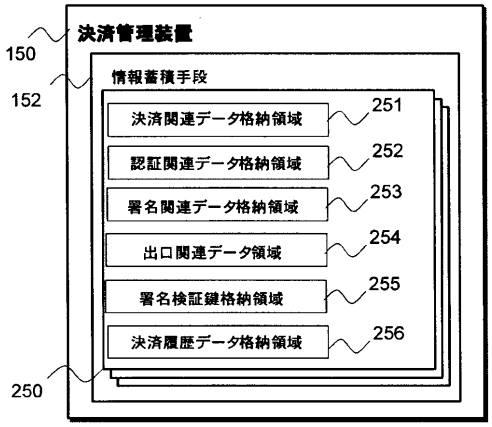
【図５】

図 5



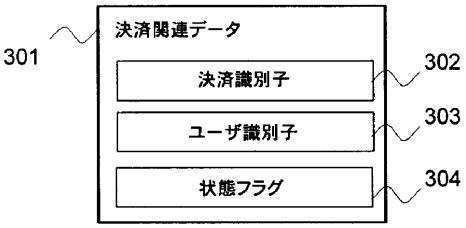
【図６】

図 6



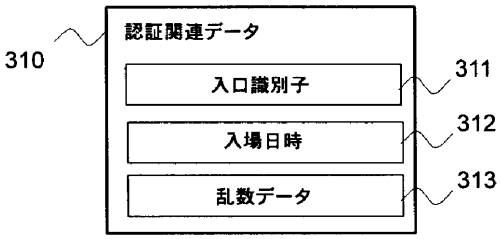
【図７】

図 7



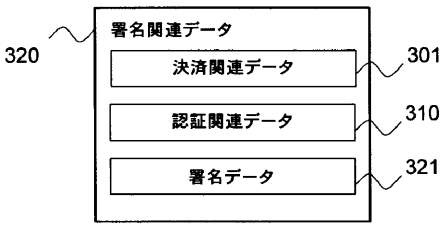
【図８】

図 8



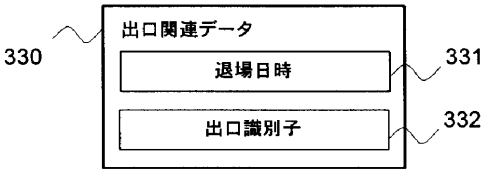
【図９】

図 9



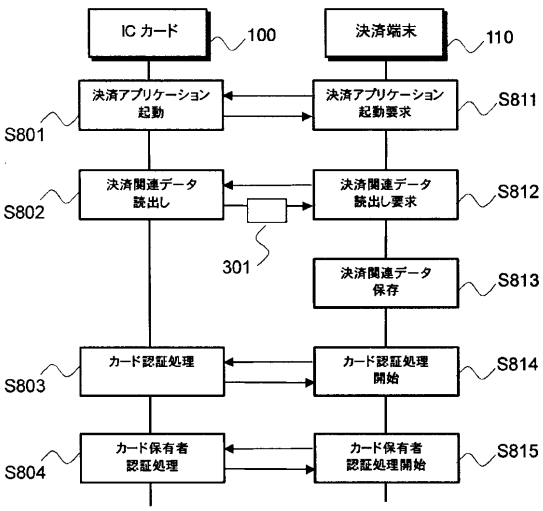
【図１０】

図 10



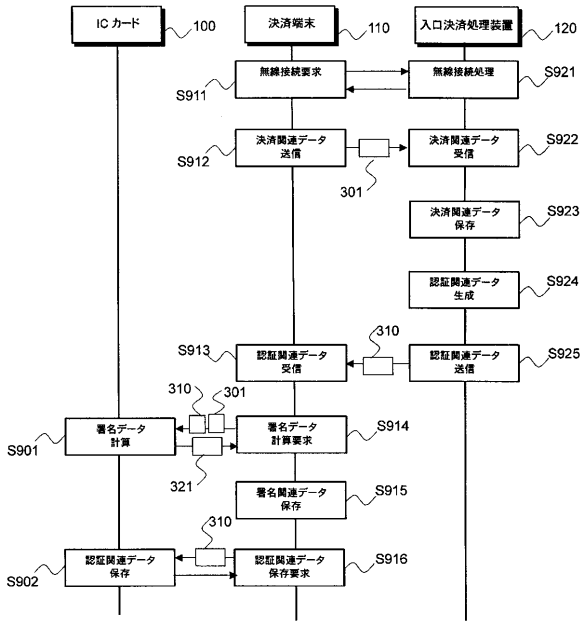
【図１１】

図 11



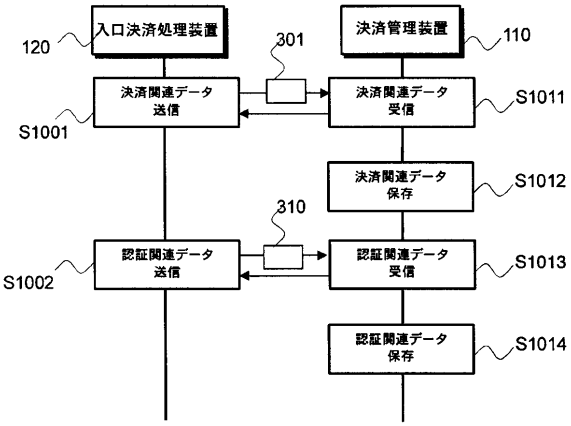
【図１２】

図 12



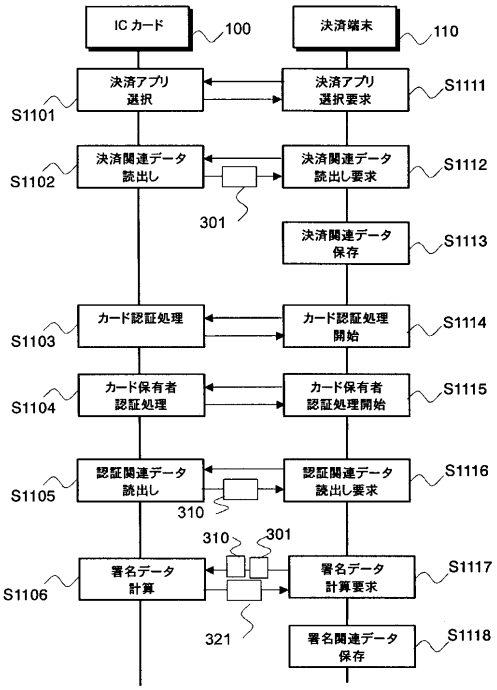
【図１３】

図 13



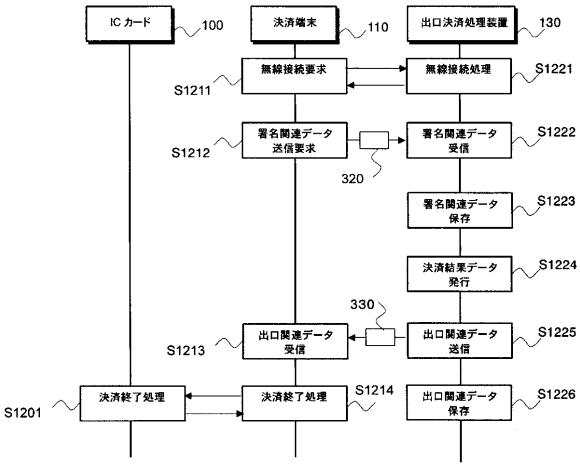
【図１４】

図 14



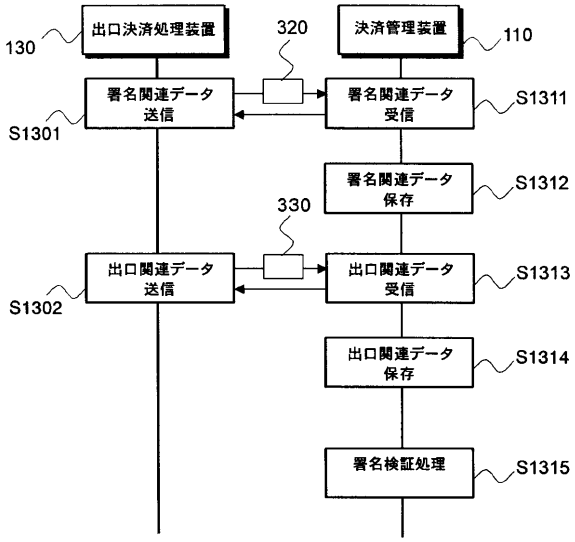
【図１５】

図 15



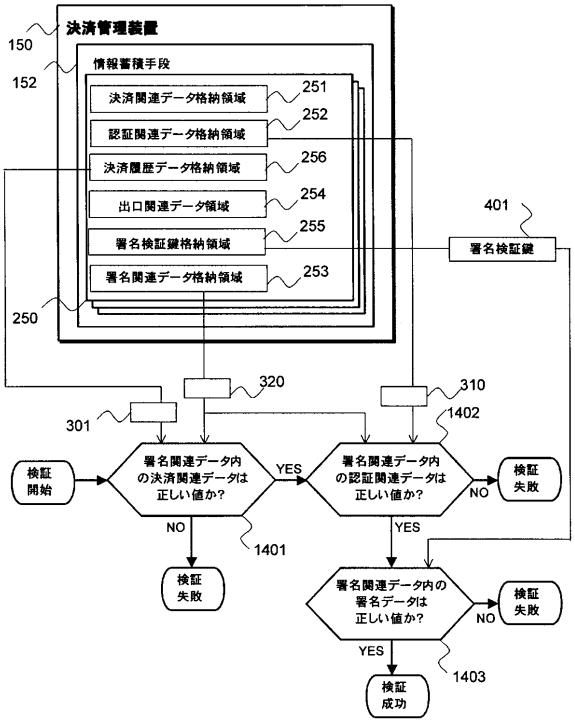
【図１６】

図 16



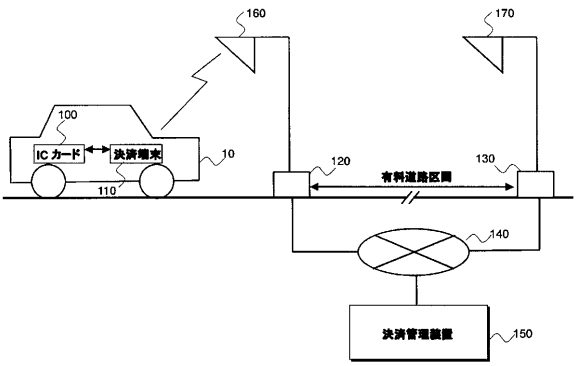
【図１７】

図 17



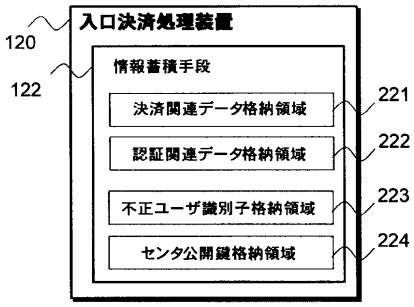
【図１８】

図 18



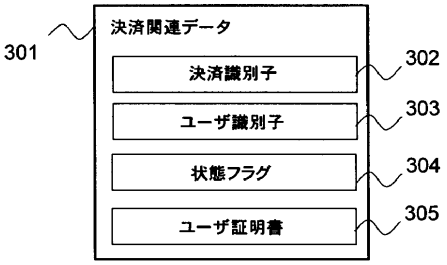
【図１９】

図 19



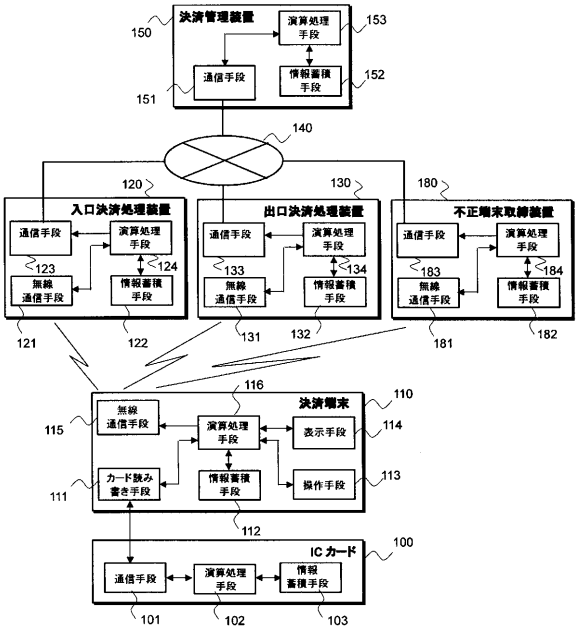
【図２０】

図 20



【図２１】

図 21


決済管理装置
演算処理手段
153
通信手段
情報蓄積手段
152
150
151
140
120
130
180
入口決済処理装置
出口決済処理装置
不正端末取締装置
通信手段
演算処理手段
無線通信手段
情報蓄積手段
123
124
133
134
183
184
121
122
131
132
181
182
116
決済端末
110
無線通信手段
演算処理手段
表示手段
114
115
カード読み書き手段
情報蓄積手段
操作手段
113
111
112
ICカード
100
通信手段
演算処理手段
情報蓄積手段
101
102
103

フロントページの続き

(51)Int.Cl.[7]	FI		テーマコード（参考）
	Ｇ０７Ｂ 15/00	ＺＥＣＭ	
	Ｈ０４Ｌ 9/00	６７５Ｚ	
	Ｈ０４Ｌ 9/00	６７３Ｅ	

(72)発明者 中野 哲夫
神奈川県横浜市戸塚区吉田町２９２番地 株式会社日立製作所デジタルメディア開発本部内
(72)発明者 福島 真一郎
神奈川県横浜市戸塚区吉田町２９２番地 株式会社日立製作所デジタルメディア開発本部内
(72)発明者 橋本 和則
神奈川県横浜市戸塚区吉田町２９２番地 株式会社日立製作所デジタルメディア開発本部内

Ｆターム(参考) 5B035 AA13 BB09 BB11 BC00 CA11 CA29
5B058 CA23 CA25 KA02 KA04 KA06 YA11 YA20
5J104 AA07 FA10 KA02 KA21 NA35 NA38 PA11