(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2007-41863
(P2007-41863A)
(43)公開日　平成19年2月15日(2007.2.15)

(51)Int.Cl.		F I			テーマコード（参考）
G07B 11/00	(2006.01)	G07B	11/00	501	5B058
G06K 17/00	(2006.01)	G06K	17/00	E	5J104
G09C 1/00	(2006.01)	G09C	1/00	660A	
G06Q 40/00	(2006.01)	G09C	1/00	660B	
G06Q 10/00	(2006.01)	G06F	17/60	242	

審査請求 未請求　請求項の数 6　ＯＬ　（全 28 頁）　最終頁に続く

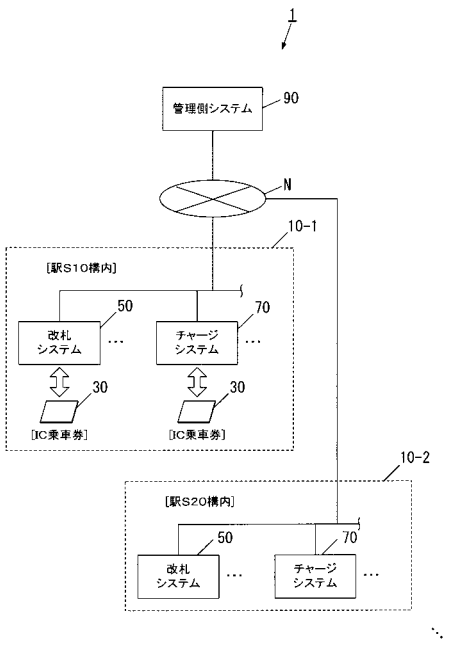
(21)出願番号　特願2005-225511 (P2005-225511)
(22)出願日　平成17年8月3日 (2005.8.3)

(71)出願人　000173784
財団法人鉄道総合技術研究所
東京都国分寺市光町２丁目８番地３８
(74)代理人　100090033
弁理士　荒船　博司
(74)代理人　100093045
弁理士　荒船　良男
(72)発明者　荻野　隆彦
東京都国分寺市光町二丁目８番地３８　財団法人鉄道総合技術研究所内

Ｆターム(参考)　5B058 CA25 CA27 KA13 KA35 YA12
5J104 AA07 AA12 JA03 KA02 KA04 NA02 NA05 NA27 NA35 NA36 NA37 NA38 NA40 PA10 PA15

(54)【発明の名称】ＩＣカード管理システム

(57)【要約】
【課題】　管理側システムにおいて、ＩＣカードの使用履歴の特定を基本的に不能として蓄積管理されるデータ自体を無意味化する一方、ユーザが希望した場合等必要に応じて使用履歴の特定が可能な仕組みを実現すること。
【解決手段】　管理側システム９０は、改札システム５０から受信したカード使用情報に設定されているカードＩＤによって定まる乱数ＩＤ列に従った新たな乱数ＩＤを発行させ、カードＩＤを発行させた乱数ＩＤと置き換えたカード使用履歴データを生成してカード使用履歴ファイルとして管理する。ユーザ操作によってカードＩＤが入力されたならば、入力されたカードＩＤによって定まる乱数ＩＤ列を発生させ、カード使用履歴ファイルから、使用順に並べたときの乱数ＩＤの順番が発生させた乱数ＩＤ列の順番通りになるカード使用履歴データを抽出することで当該カードＩＤが割り当てられたＩＣ乗車券３０の使用履歴を特定する。
【選択図】　図１



【特許請求の範囲】
【請求項１】
固有の識別ＩＤが割り当てられたＩＣカードの使用位置に設置され、前記ＩＣカードとの間で近距離無線通信を行って前記ＩＣカード内のデータを書き換えるとともに、前記ＩＣカードから識別ＩＤを含むカード情報を取得するカード使用装置と、当該カード使用装置から送信されるカード情報をカード情報記憶手段に蓄積記憶して前記ＩＣカードの使用履歴を管理する管理側システムとが通信接続されて構成されるＩＣカード管理システムであって、
前記カード使用装置は、前記ＩＣカードから取得したカード情報に時刻情報及び所定の発信データを含めて前記管理側システムに送信するカード情報送信手段を備え、
前記管理側システムは、
前記カード使用装置から受信したカード情報に含まれる識別ＩＤに基づき、当該識別ＩＤによって定まる乱数ＩＤ列に従った新たな乱数ＩＤを発行する乱数ＩＤ発行手段と、
前記受信したカード情報に含まれる識別ＩＤを前記乱数ＩＤ発行手段により発行された乱数ＩＤと置き換えて前記カード情報記憶手段に書き込むカード情報書込手段と、
ユーザ操作に従って前記ＩＣカードの識別ＩＤを入力する識別ＩＤ入力手段と、
前記識別ＩＤ入力手段により入力された識別ＩＤに基づいて、前記乱数ＩＤ発行手段によって発行される乱数ＩＤ列と同じ乱数ＩＤ列を発生するＩＤ列発生手段と、
前記ＩＤ列発生手段により発生された乱数ＩＤ列の各乱数ＩＤと同一の乱数ＩＤを含むカード情報であって、時刻情報に従った乱数ＩＤの羅列が前記発生された乱数ＩＤ列と一致するカード情報を、前記カード情報記憶手段に記憶されているカード情報の中から抽出する抽出手段と、
前記抽出手段により抽出されたカード情報に基づき、前記識別ＩＤ入力手段により入力された識別ＩＤが割り当てられたＩＣカードの使用履歴を特定する特定手段と、
を備えることを特徴とするＩＣカード管理システム。
【請求項２】
前記管理側システムは、
前記カード使用装置から受信したカード情報に含まれる識別ＩＤにそれぞれ固有の暗号鍵を割り当てて、復号鍵とともに管理する鍵管理手段と、
前記カード使用装置から受信したカード情報に含まれる発信データを、当該カード情報に含まれる識別ＩＤと対応付けられて前記鍵管理手段に管理されている暗号鍵で暗号化する暗号化手段と、
を更に備え、
前記カード情報書込手段が、前記暗号化手段により発信データが暗号化されたカード情報を、受信順とは異なる順番で前記カード情報記憶手段に書き込む書込順制御手段を有する、
ことを特徴とする請求項１に記載のＩＣカード管理システム。
【請求項３】
前記抽出手段が、カード情報に含まれる発信データを、前記識別ＩＤ入力手段により入力された識別ＩＤと対応付けられて前記鍵管理手段に管理されている復号鍵で復号し、当該復号の良否に基づいて抽出するカード情報の絞り込みを行う絞り込み手段を有する、
ことを特徴とする請求項２に記載のＩＣカード管理システム。
【請求項４】
前記ＩＣカードは、前記カード使用装置における使用によって減額される残高の情報を記憶する残高記憶手段を更に備え、
前記カード使用装置は、
前記ＩＣカードとの間で近距離無線通信を行う当該ＩＣカードの使用時に、当該ＩＣカードの残高記憶手段に記憶されている残高を所定額減額して更新させる残高更新手段を更に備え、
前記カード情報送信手段が、前記残高更新手段による更新後の残高を前記発信データに

含めて前記管理側システムに送信する手段であり、
前記管理側システムは、
前記特定手段が、前記抽出手段により抽出されたカード情報のうち、時刻情報が最新のカード情報の発信データに含まれる残高によって、当該ＩＣカードの使用残高を特定する残高特定手段を有する、
ことを特徴とする請求項１～３の何れか一項に記載のＩＣカード管理システム。
【請求項５】
前記管理側システムは、
残高情報として、ランダムに決定した第１の数値、及び、第１の数値と前記カード使用装置から受信したカード情報の発信データに含まれる残高との差である第２の数値を決定する残高情報決定手段を更に備え、
前記暗号化手段が、前記残高情報決定手段により決定された残高情報を暗号化する残高暗号化手段を有する、
ことを特徴とする請求項４に記載のＩＣカード管理システム。
【請求項６】
積み増し額を入金する入金手段と、
前記ＩＣカードとの間で無線通信を行い、当該ＩＣカードの残高記憶手段に記憶されている残高を、前記入金手段により入金された積み増し額分増額して更新する積み増し時書込手段と、
前記ＩＣカードから識別ＩＤを取得し、当該取得した識別ＩＤと前記積み増し時書込手段が書き込んだ結果増額された残高とを入金情報として、前記管理側システムに送信する入金情報送信手段と、
を備えて前記管理側システムと通信接続された入金装置を更に具備し、
前記管理側システムは、
前記入金装置から入金情報を受信した際に新たな入金ＩＤを発行し、前記受信した入金情報に含まれる識別ＩＤと対応付けて管理する入金ＩＤ管理手段と、
前記受信した入金情報に含まれる識別ＩＤを、当該識別ＩＤと対応付けられて前記入金ＩＤ管理手段に管理されている入金ＩＤと置き換えて入金情報を記憶する入金情報記憶手段と、
前記カード使用装置からカード情報を受信した際に、当該カード情報に含まれる識別ＩＤと対応付けられて前記入金ＩＤ管理手段に管理されている入金ＩＤを特定する入金ＩＤ特定手段と、
前記入金情報記憶手段の中から前記入金ＩＤ特定手段により特定された入金ＩＤと対応付けられて記憶されている残高を読み出し、前記カード使用装置から受信したカード情報の発信データに含まれる残高と比較することによって、前記ＩＣカードの不正使用を検出する不正使用検出手段と、
を更に備えることを特徴とする請求項４又は５に記載のＩＣカード管理システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、固有の識別ＩＤが割り当てられたＩＣカードの使用位置に設置されるカード使用装置と、当該カード使用装置で使用されるＩＣカードの使用履歴を管理する管理側システムとが通信接続されて構成されるＩＣカード管理システムに関する。
【背景技術】
【０００２】
従来から、データ管理やデータ通信等においては、データの漏洩等を防止してセキュリティ上の信頼性を向上させるため、様々な方式による暗号化の技術が用いられている。
例えば、証票に印字される識別番号の偽造によるコンピュータシステムへの不正アクセスを防止するため、暗号化パターンを複数用意し、識別番号を、乱数により決定されたパターンで暗号化する技術が知られている（特許文献１参照。）。

【０００３】
一方従来から、ＩＣカードと、所定位置に設置されたリーダ（ＩＣカード通信機）との間で近距離無線通信を行う、非接触式のデータキャリアを利用した様々な技術が知られている。例えば鉄道施設では、利用者が所持するＳｕｉｃａ（Super urban intelligent card：登録商標）等のプリペイド式のＩＣ乗車券に記憶されている残高の情報を読み取ることにより、当該利用者による鉄道施設内への入場や鉄道施設内からの出場を自動的に管理する技術が知られている。
【特許文献１】特開平８－９６０４９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、上記したＩＣ乗車券のようなプリペイド式のＩＣカードの発行を管理する管理側システムにあっては、例えば利用者が当該ＩＣカードを紛失した際に残額を返金する場合等に備えて、残高を含む使用履歴を管理する場合がある。具体的には、使用時にＩＣカードが残高を含むデータを発信するように構成し、発信したデータを管理側システムで蓄積して管理する。
【０００５】
しかしながらこの使用履歴によれば、当該ＩＣカードを購入した利用者が、いつどこに位置したかを識別できてしまう。この問題を解決するため、当該ＩＣカードの使用履歴を特定するためにＩＣカードから発信されるデータを暗号化する等の方法が考えられるが、管理側システムから使用履歴が不正に参照されたり、人的に不正に持ち出される事態は避けられない。
【０００６】
そこで本発明は、管理側システムにおいて、ＩＣカードの使用履歴の特定を基本的に不能として蓄積管理されるデータ自体を無意味化する一方、ユーザが希望した場合等必要に応じて使用履歴の特定が可能な仕組みを実現することを目的とする。
【課題を解決するための手段】
【０００７】
以上の課題を解決するための第１の発明のＩＣカード管理システムは、
固有の識別ＩＤが割り当てられたＩＣカードの使用位置に設置され、前記ＩＣカードとの間で近距離無線通信を行って前記ＩＣカード内のデータを書き換えるとともに、前記ＩＣカードから識別ＩＤを含むカード情報を取得するカード使用装置と、当該カード使用装置から送信されるカード情報をカード情報記憶手段（例えば、図８に示すカード使用履歴ファイル９４０）に蓄積記憶して前記ＩＣカードの使用履歴を管理する管理側システムとが通信接続されて構成されるＩＣカード管理システムであって、
前記カード使用装置は、前記ＩＣカードから取得したカード情報に時刻情報及び所定の発信データを含めて前記管理側システムに送信するカード情報送信手段（例えば、図４に示す処理装置５１０）を備え、
前記管理側システムは、
前記カード使用装置から受信したカード情報に含まれる識別ＩＤに基づき、当該識別ＩＤによって定まる乱数ＩＤ列に従った新たな乱数ＩＤを発行する乱数ＩＤ発行手段（例えば、図８に示すカード使用履歴管理サーバ９３０）と、
前記受信したカード情報に含まれる識別ＩＤを前記乱数ＩＤ発行手段により発行された乱数ＩＤと置き換えて前記カード情報記憶手段に書き込むカード情報書込手段（例えば、図８に示すカード使用履歴管理サーバ９３０）と、
ユーザ操作に従って前記ＩＣカードの識別ＩＤを入力する識別ＩＤ入力手段（例えば、図８に示すカード使用履歴管理サーバ９３０）と、
前記識別ＩＤ入力手段により入力された識別ＩＤに基づいて、前記乱数ＩＤ発行手段によって発行される乱数ＩＤ列と同じ乱数ＩＤ列を発生するＩＤ列発生手段（例えば、図８に示すカード使用履歴管理サーバ９３０）と、

前記ＩＤ列発生手段により発生された乱数ＩＤ列の各乱数ＩＤと同一の乱数ＩＤを含むカード情報であって、時刻情報に従った乱数ＩＤの羅列が前記発生された乱数ＩＤ列と一致するカード情報を、前記カード情報記憶手段に記憶されているカード情報の中から抽出する抽出手段（例えば、図８に示すカード使用履歴管理サーバ９３０）と、

前記抽出手段により抽出されたカード情報に基づき、前記識別ＩＤ入力手段により入力された識別ＩＤが割り当てられたＩＣカードの使用履歴を特定する特定手段（例えば、図８に示すカード使用履歴管理サーバ９３０）と、

を備えるものである。

【０００８】

この第１の発明によれば、カード使用装置は、使用されたＩＣカードから取得した当該ＩＣカードの識別ＩＤを含むカード情報に、時刻情報及び所定の発信データを含めて管理側システムに送信することができる。一方管理側システムでは、カード使用装置から受信したカード情報に含まれる識別ＩＤによって定まる乱数ＩＤ列に従った新たな乱数ＩＤを乱数ＩＤ発行手段により発行させ、当該受信したカード情報に含まれる識別ＩＤを発行させた乱数ＩＤと置き換えてカード情報記憶手段に書き込むことによって、カード使用装置から送信されるカード情報を蓄積記憶しておく。そして、ユーザ操作に従って識別ＩＤが入力された場合には、入力された識別ＩＤに基づいて前記乱数ＩＤ発行手段によって発行される乱数ＩＤ列と同じ乱数ＩＤ列を発生させ、カード情報記憶手段に蓄積記憶されているカード情報の中から、時刻情報に従った乱数ＩＤの羅列が発生させた乱数ＩＤ列と一致するカード情報を抽出することによって、入力された識別ＩＤが割り当てられたＩＣカードの使用履歴を特定することができる。

これによれば、管理側システムにおいて、カード情報記憶手段に蓄積記憶されるデータを無意味化してＩＣカードの使用履歴の特定を不能とする一方、ユーザ操作によって発行パスワードの入力が行われた場合には当該ＩＣカードの使用履歴の特定が可能な仕組みを実現することができる。

【０００９】

第２の発明は、第１の発明のＩＣカード管理システムであって、

前記管理側システムは、

前記カード使用装置から受信したカード情報に含まれる識別ＩＤにそれぞれ固有の暗号鍵を割り当てて、復号鍵とともに管理する鍵管理手段（例えば、図８に示す暗号キー発生サーバ９７０，キーテーブル９７３）と、

前記カード使用装置から受信したカード情報に含まれる発信データを、当該カード情報に含まれる識別ＩＤと対応付けられて前記鍵管理手段に管理されている暗号鍵で暗号化する暗号化手段（例えば、図８に示す窓口サーバ９１０）と、

を更に備え、

前記カード情報書込手段が、前記暗号化手段により発信データが暗号化されたカード情報を、受信順とは異なる順番で前記カード情報記憶手段に書き込む書込順制御手段（例えば、図８に示すカード使用履歴管理サーバ９３０）を有するものである。

【００１０】

この第２の発明によれば、管理側システムでは、ＩＣカードの識別ＩＤ毎に固有の暗号鍵を復号鍵とともに管理し、カード使用装置から受信したカード情報に含まれる発信データを、当該カード情報に含まれる識別ＩＤの暗号鍵で暗号化することができる。そして、発信データが暗号化されたカード情報を、カード使用装置からの受信順とは異なる順番でカード情報記憶手段に書き込むことによって、データの書き込まれている順番を無意味化することができる。

【００１１】

第３の発明は、第２の発明のＩＣカード管理システムであって、

前記抽出手段が、カード情報に含まれる発信データを、前記識別ＩＤ入力手段により入力された識別ＩＤと対応付けられて前記鍵管理手段に管理されている復号鍵で復号し、当該復号の良否に基づいて抽出するカード情報の絞り込みを行う絞り込み手段（例えば、図

８に示すカード使用履歴管理サーバ９３０）を有するものである。

【００１２】

この第３の発明によれば、ユーザ操作に従って入力された識別ＩＤが割り当てられたＩＣカードの使用履歴を特定する際に、当該入力された識別ＩＤの復号鍵による発信データの復号の良否に基づいて、抽出するカード情報を絞り込むことができる。

【００１３】

第４の発明は、第１～第３の何れかの発明のＩＣカード管理システムであって、

前記ＩＣカードは、前記カード使用装置における使用によって減額される残高の情報を記憶する残高記憶手段（例えば、図３に示す残高３９３）を更に備え、

前記カード使用装置は、

前記ＩＣカードとの間で近距離無線通信を行う当該ＩＣカードの使用時に、当該ＩＣカードの残高記憶手段に記憶されている残高を所定額減額して更新させる残高更新手段（例えば、図４に示す処理装置５１０）を更に備え、

前記カード情報送信手段が、前記残高更新手段による更新後の残高を前記発信データに含めて前記管理側システムに送信する手段であり、

前記管理側システムは、

前記特定手段が、前記抽出手段により抽出されたカード情報のうち、時刻情報が最新のカード情報の発信データに含まれる残高によって、当該ＩＣカードの使用残高を特定する残高特定手段（例えば、図８に示すカード使用履歴管理サーバ９３０）を有するものである。

【００１４】

この第４の発明によれば、カード使用装置では、当該カード使用装置での使用によって減額されるＩＣカードの残高を発信データに含めて管理側システムに送信することができる。一方管理側システムでは、ユーザ操作に従って入力された識別ＩＤが割り当てられたＩＣカードの使用履歴を特定する際に抽出したカード情報のうち、時刻情報が最新のカード情報に含まれる残高によって、当該ＩＣカードの残高を特定することができる。

【００１５】

第５の発明は、第４の発明のＩＣカード管理システムであって、

前記管理側システムは、

残高情報として、ランダムに決定した第１の数値、及び、第１の数値と前記カード使用装置から受信したカード情報の発信データに含まれる残高との差である第２の数値を決定する残高情報決定手段（例えば、図８に示す窓口サーバ９１０）を更に備え、

前記暗号化手段が、前記残高情報決定手段により決定された残高情報を暗号化する残高暗号化手段（例えば、図８に示す窓口サーバ９１０）を有するものである。

【００１６】

この第５の発明によれば、管理側システムでは、カード使用装置から受信したカード情報の発信データに含まれる残高をもとにランダムに決定した第１の数値、及び第１の数値と当該残高との差である第２の数値を残高情報として決定した後、暗号化することができる。これによれば、第１の数値及び第２の数値の桁数がランダムになる。したがって、カード情報記憶手段に蓄積記憶されているカード情報が、残高が高いＩＣカードから発信されたカード情報なのか残高が低いＩＣカードから発信されたカード情報なのか判別できず、データを無意味化できる。

【００１７】

第６の発明は、第４又は第５の発明のＩＣカード管理システムであって、

積み増し額を入金する入金手段（例えば、図６に示す入金装置７１０）と、

前記ＩＣカードとの間で無線通信を行い、当該ＩＣカードの残高記憶手段に記憶されている残高を、前記入金手段により入金された積み増し額分増額して更新する積み増し時書込手段（例えば、図６に示す処理装置７３０）と、

前記ＩＣカードから識別ＩＤを取得し、当該取得した識別ＩＤと前記積み増し時書込手段が書き込んだ結果増額された残高とを入金情報として、前記管理側システムに送信する

入金情報送信手段（例えば、図６に示す処理装置７３０）と、
を備えて前記管理側システムと通信接続された入金装置を更に具備し、
前記管理側システムは、
前記入金装置から入金情報を受信した際に新たな入金ＩＤを発行し、前記受信した入金情報に含まれる識別ＩＤと対応付けて管理する入金ＩＤ管理手段（例えば、図８に示す入金ＩＤ管理サーバ９５０，入金ＩＤテーブル９５３）と、
前記受信した入金情報に含まれる識別ＩＤを、当該識別ＩＤと対応付けられて前記入金ＩＤ管理手段に管理されている入金ＩＤと置き換えて入金情報を記憶する入金情報記憶手段（例えば、図８に示す入金履歴ファイル９２０）と、
前記カード使用装置からカード情報を受信した際に、当該カード情報に含まれる識別ＩＤと対応付けられて前記入金ＩＤ管理手段に管理されている入金ＩＤを特定する入金ＩＤ特定手段（例えば、図８に示す窓口サーバ９１０）と、
前記入金情報記憶手段の中から前記入金ＩＤ特定手段により特定された入金ＩＤと対応付けられて記憶されている残高を読み出し、前記カード使用装置から受信したカード情報の発信データに含まれる残高と比較することによって、前記ＩＣカードの不正使用を検出する不正使用検出手段（例えば、図８に示す窓口サーバ９１０）と、
を更に備えるものである。

【００１８】

この第６の発明によれば、入金装置は、積み増し額が入金されて残高が増額されたＩＣカードの識別ＩＤを取得し、取得した識別ＩＤと増額後の残高とを入金情報として管理側システムに送信する。一方管理側システムでは、入金装置から入金情報を受信した際に、新たな入金ＩＤを発行して当該受信した入金情報に含まれる識別ＩＤと対応付けて管理するとともに、当該受信した入金情報に含まれる識別ＩＤを、当該識別ＩＤの入金ＩＤと置き換えて入金情報記憶手段に記憶しておく。そして、カード使用装置からカード情報を受信した場合には、当該カード情報に含まれる識別ＩＤの入金ＩＤを特定し、入金情報記憶手段に記憶されている特定した入金ＩＤの残高を、受信したカード情報の発信データに含まれる残高と比較することによって、ＩＣカードの不正使用を検出することができる。

【発明の効果】

【００１９】

本発明によれば、カード使用装置は、使用されたＩＣカードから取得した当該ＩＣカードの識別ＩＤを含むカード情報に、時刻情報及び所定の発信データを含めて管理側システムに送信することができる。一方管理側システムでは、カード使用装置から受信したカード情報に含まれる識別ＩＤによって定まる乱数ＩＤ列に従った新たな乱数ＩＤを乱数ＩＤ発行手段により発行させ、当該受信したカード情報に含まれる識別ＩＤを発行させた乱数ＩＤと置き換えてカード情報記憶手段に書き込むことによって、カード使用装置から送信されるカード情報を蓄積記憶しておく。そして、ユーザ操作に従って識別ＩＤが入力された場合には、入力された識別ＩＤに基づいて前記乱数ＩＤ発行手段によって発行される乱数ＩＤ列と同じ乱数ＩＤ列を発生させ、カード情報記憶手段に蓄積記憶されているカード情報の中から、時刻情報に従った乱数ＩＤの羅列が発生させた乱数ＩＤ列と一致するカード情報を抽出することによって、入力された識別ＩＤが割り当てられたＩＣカードの使用履歴を特定することができる。

これによれば、管理側システムにおいて、カード情報記憶手段に蓄積記憶されるデータを無意味化してＩＣカードの使用履歴の特定を不能とする一方、ユーザ操作によって発行パスワードの入力が行われた場合には当該ＩＣカードの使用履歴の特定が可能な仕組みを実現することができる。

【発明を実施するための最良の形態】

【００２０】

以下、図面を参照し、本発明の好適な実施形態について詳細に説明する。尚、本実施形態は、本発明のＩＣカード管理システムを鉄道施設に利用されるシステムに適用した場合の実施形態である。

【００２１】
［全体構成］
図１は、ＩＣカード管理システム１の全体構成の一例を示す図である。本実施形態では、駅構内１０（１０－１，１０－２，・・・）に、カード使用装置としての改札システム５０及び入金装置としてのチャージシステム７０が設置され、これらが通信回線Ｎを介して管理側システム９０と接続されてＩＣカード管理システム１を構成している。ここで、通信回線Ｎとは、データ授受が可能な通信路を意味する。すなわち、通信回線Ｎとは、直接接続のための専用線（専用ケーブル）やイーサネット（登録商標）等によるＬＡＮの他、電話通信網やケーブル網、インターネット等の通信網を含む意味であり、また、通信方法については有線／無線を問わない。
【００２２】
改札システム５０は、各駅の改札に設置されて改札業務を実現する改札装置に具備されるものであり、改札装置が備えるゲート扉の開閉を制御して利用者の通行を規制し、利用者の鉄道施設内への入場や鉄道施設内からの出場をコンピュータ制御によって管理する。
【００２３】
具体的には、改札システム５０は、利用者が所持する例えばＳｕｉｃａ（登録商標）等の非接触型のＩＣチップを内蔵したプリペイド式のＩＣカード（以下、「ＩＣ乗車券」という。）３０に記憶されている残高を読み出すことによって精算処理を行い、処理結果に基づいて当該利用者の通行を規制する。
【００２４】
チャージシステム７０は、例えば各駅の券売機等に設置されるものであり、利用者からの現金払いやクレジットカード払い等によるチャージ金の入金に応じて、当該ＩＣ乗車券３０に対して積み増し額をチャージする公知のチャージシステムである。このチャージシステム７０によって、利用者は、その残高を増額することによりＩＣ乗車券３０を繰り返し使用することができる。
【００２５】
管理側システム９０は、例えば鉄道会社の管理側に設置されてＩＣカード管理システム１を統括的に制御する。また、管理側システム９０は、改札システム５０から送信されるカード使用情報に基づくカード使用履歴を管理するとともに、チャージシステム７０から送信される入金情報に基づく入金履歴を管理する。
【００２６】
また本実施形態では、後述するようにＩＣ乗車券３０の発行時において当該ＩＣ乗車券３０に固有に割り当てられるＩＤ情報（識別ＩＤ：以下、「カードＩＤ」という。）が利用者に提示されるが、管理側システム９０は、ユーザ操作によって前述のカードＩＤが入力された場合に、管理しているカード使用履歴をもとに、当該利用者が所持するＩＣ乗車券３０（すなわち、入力されたカードＩＤが割り当てられたＩＣ乗車券３０）の使用履歴を特定する。
【００２７】
図２は、このＩＣカード管理システム１におけるデータの流れを説明するための図である。図２に示すように、利用者が駅改札を通過する際、当該利用者が所持するＩＣ乗車券３０と改札システム５０との間で近距離無線通信が行われ、Ａ）当該ＩＣ乗車券３０に記憶されているカードＩＤ及び残高が改札システム５０に発信される。これに応じて、改札システム５０では精算処理が実行され、Ｂ）精算処理後の残高がＩＣ乗車券３０に書き込まれて残高が精算額分減額された額に更新される。
【００２８】
そして、改札システム５０により、当該ＩＣ乗車券３０のカードＩＤと、発信データとしての精算処理後の残高、使用日時、及び当該改札システム５０の設置位置に係る情報とが対応付けられたカード使用情報が生成され、Ｃ）管理側システム９０に送信される。
【００２９】
一方管理側システム９０では、改札システム５０から送信されたカード使用情報に基づ

いて、後述するＩＣ乗車券３０の不正使用を検出する処理（不正使用検出処理）が実行される。そして、当該不正使用検出処理の結果、残高が不正に積み増されていると判断された場合には、Ｈ）当該カード使用情報に設定されているカードＩＤが、不正カードＩＤとして管理側システム９０に接続されている全ての改札システム５０に配信される。各改札システム５０では、この不正カードＩＤの一覧が管理され、不正カードＩＤが割り当てられたＩＣ乗車券の使用を禁止するようになっている。

【００３０】

また、利用者が券売機等でチャージ金を入金した際には、ＩＣ乗車券３０とチャージシステム７０との間で近距離無線通信が行われ、Ｄ）当該ＩＣ乗車券３０に記憶されているカードＩＤ及び残高がチャージシステム７０に発信される。これに応じて、チャージシステム７０ではチャージ処理が実行され、Ｅ）チャージ処理後の残高がＩＣ乗車券３０に書き込まれて残高が積み増し額分増額された額に更新される。

【００３１】

そして、チャージシステム７０により、当該ＩＣ乗車券３０のカードＩＤ及びチャージ処理後の残高（以下、「入金時残高」という。）に入金日時が対応付けられた入金情報が生成され、Ｆ）管理側システム９０に送信される。

【００３２】

［内部構成］

次に、図３～図１３を参照して、ＩＣ乗車券３０、改札システム５０、チャージシステム７０、及び管理側システム９０の内部構成について順に説明する。

【００３３】

１．ＩＣ乗車券

図３は、ＩＣ乗車券３０の主要内部構成の一例を示すブロック図である。ＩＣ乗車券３０は、アンテナ３１０、電源回路３３０、送受信回路３５０、制御回路３７０、メモリ３９０等を備えて構成されている。

【００３４】

アンテナ３１０は、改札システム５０が備えるＩＣカード通信機５７０（図４参照）やチャージシステム７０が備えるＩＣカード通信機７９０（図６参照）との間で近距離無線通信を行うためのものであり、ＩＣカード通信機５７０やＩＣカード通信機７９０との間で電波信号を送受信する。

【００３５】

電源回路３３０は、アンテナ３１０において生じた電磁誘導による電流によってＩＣ乗車券３０の各部に電力を供給する回路である。

【００３６】

送受信回路３５０は、アンテナ３１０を介してＩＣカード通信機５７０，７９０から発信された信号を復調して制御回路３７０に出力する。また、送受信回路３５０は、制御回路３７０から入力される制御信号を変調増幅し、アンテナ３１０を介してＩＣカード通信機５７０，７９０に発信する。

【００３７】

制御回路３７０は、改札システム５０やチャージシステム７０との近距離無線通信を制御し、ＩＣカード通信機５７０，７９０からの指示に基づくデータの発信動作、ＩＣカード通信機５７０，７９０から送信されたデータのメモリ３９０への書き込み動作等を行う。

【００３８】

メモリ３９０は、不揮発性の半導体メモリ等であり、カードＩＤ３９１及び残高３９３が格納される。

カードＩＤ３９１は、当該ＩＣ乗車券３０に固有に割り当てられたＩＤ情報であり、例えばカード発行時において当該ＩＣ乗車券３０に書き換え不能に書き込まれるとともに、利用者に提示される。

残高３９３は、当該ＩＣ乗車券３０の残額であり、駅改札において使用される度に改札

システム５０によってその額が減額されて更新される。また、券売機等で積み増し額がチャージされる度にチャージシステム７０によってその額が増額されて更新される。

【００３９】

２．改札システム

図４は、改札システム５０の主要内部構成の一例を示すブロック図である。改札システム５０は、処理装置５１０、通信装置５３０、記憶装置５５０、ＩＣカード通信機５７０、利用者の通行を規制するゲート扉５９０等を備えて構成されている。尚、入力装置や表示装置等を適宜備えた構成としても構わない。

【００４０】

処理装置５１０は、ＣＰＵ等で構成され、改札システム５０を構成する各機能部への指示やデータの転送等を行って改札システム５０を統括的に制御する。具体的には、ＩＣカード通信機５７０から入力されるデータ等に応じた処理プログラムを記憶装置５５０から読み出して実行し、処理結果を記憶装置５５０に格納する。この処理装置５１０は、当該改札システム５０が設置された駅改札でＩＣ乗車券３０が使用された際に、当該ＩＣ乗車券３０の残高３９３（図３参照）を取得して精算処理を実行し、処理結果に基づいて当該ＩＣ乗車券３０の残高３９３を精算額分減額して更新させる。

【００４１】

通信装置５３０は、装置内部で利用される情報を通信回線を介して外部とやりとりするための装置であり、他の装置（例えば管理側システム９０）との通信を行うための制御を行う。この通信装置５３０の機能は、無線通信モジュール、モデム、ＴＡ、有線用の通信ケーブルのジャックや制御回路等によって実現される。

【００４２】

記憶装置５５０は、更新記憶可能なフラッシュメモリ等のＲＯＭやＲＡＭといった各種ＩＣメモリ、或いはハードディスクドライブ等で構成され、改札システム５０の動作に係る各種処理プログラムや当該処理プログラムによる処理結果等のデータを記憶する。特に、カード使用情報送信プログラム５５１と、不正使用カード管理プログラム５５３と、不正カードＩＤ一覧５５５と、当該改札システム５０の設置位置を特定する改札機ＩＤ５５７とを含む。

【００４３】

カード使用情報送信プログラム５５１は、ＩＣ乗車券３０が使用された際に実行される精算処理の後、当該ＩＣ乗車券３０から取得したカードＩＤ及び残高をカード情報とし、使用日時及び当該改札システム５０の改札機ＩＤと対応付けたカード使用情報を生成して管理側システム９０に送信するためのプログラムである。

【００４４】

図５は、管理側システム９０に送信されるカード使用情報のデータ構成例を示す図であり、カード使用情報は、カードＩＤ及び残高であるカード情報と、使用日時と、改札機ＩＤとが対応付けられたものである。処理装置５１０は、精算処理の後、当該ＩＣ乗車券３０から取得したカードＩＤ及び精算処理後の残高に、当該使用時（精算時）の時刻情報である使用日時、及び改札機ＩＤ５５７を対応付けたカード使用情報を生成して、通信装置５３０及び通信回線Ｎを介して管理側システム９０に送信する。

【００４５】

不正使用カード管理プログラム５５３は、管理側システム９０から通知される不正カードＩＤを管理するためのプログラムである。この不正使用カード管理プログラム５５３に従って、処理装置５１０は、管理側システム９０から通知された不正カードＩＤを不正カードＩＤ一覧５５５に登録して管理し、不正カードＩＤ一覧５５５に含まれるカードＩＤのＩＣ乗車券３０が使用された場合には、ゲート扉５９０を閉鎖させて利用者の通行を禁止する。

【００４６】

不正カードＩＤ一覧５５５は、管理側システム９０から通知された不正カードＩＤの一覧を記憶する。

【００４７】
ＩＣカード通信機５７０は、図示しないアンテナ、制御回路、メモリ等で構成される。このＩＣカード通信機５７０は、近接されたＩＣ乗車券３０との間で近距離無線通信を行い、ＩＣ乗車券３０から取得したデータを処理装置５１０に出力するとともに、処理装置５１０から入力されたデータをＩＣ乗車券３０に書き込むための制御を行う。
【００４８】
３．チャージシステム
図６は、チャージシステム７０の主要内部構成の一例を示すブロック図である。チャージシステム７０は、入金装置７１０、処理装置７３０、通信装置７５０、記憶装置７７０、ＩＣカード通信機７９０等を備えて構成されている。尚、入力装置や表示装置等を適宜備えた構成としても構わない。
【００４９】
入金装置７１０は、チャージ金を入金するための装置であり、入金されたチャージ金の額を積み増し額として処理装置７３０に出力する。
【００５０】
処理装置７３０は、ＣＰＵ等で構成され、チャージシステム７０を構成する各機能部への指示やデータの転送等を行ってチャージシステム７０を統括的に制御する。具体的には、入金装置７１０から入力される積み増し額や、ＩＣカード通信機７９０から入力されるデータ等に応じた処理プログラムを記憶装置７７０から読み出して実行し、処理結果を記憶装置７７０に格納する。この処理装置７３０は、当該チャージシステム７０が設置された券売機等で積み増し額がチャージされた際に、当該ＩＣ乗車券３０から残高３９３（図３参照）を取得してチャージ処理を実行し、当該ＩＣ乗車券３０の残高３９３を積み増し額分増額して更新させる。
【００５１】
通信装置７５０は、装置内部で利用される情報を通信回線を介して外部とやりとりするための装置であり、他の装置（例えば管理側システム９０）との通信を行うための制御を行う。この通信装置７５０の機能は、無線通信モジュール、モデム、ＴＡ、有線用の通信ケーブルのジャックや制御回路等によって実現される。
【００５２】
記憶装置７７０は、更新記憶可能なフラッシュメモリ等のＲＯＭやＲＡＭといった各種ＩＣメモリ、或いはハードディスクドライブ等で構成され、チャージシステム７０の動作に係る各種処理プログラムや当該処理プログラムによる処理結果等のデータを記憶する。特に、入金情報送信プログラム７７１を含む。
【００５３】
入金情報送信プログラム７７１は、積み増し額がチャージされた際に実行されるチャージ処理の後、入金情報を生成して管理側システム９０に送信するためのプログラムである。
【００５４】
図７は、管理側システム９０に送信される入金情報のデータ構成例を示す図であり、入金情報は、カードＩＤと、入金時残高と、入金日時とが対応付けられたものである。処理装置７３０は、チャージ処理の後、当該ＩＣ乗車券３０から取得したカードＩＤ及びチャージ処理後の入金時残高に、当該チャージ時の時刻情報である入金日時を対応付けた入金情報を生成して、通信装置７５０及び通信回線Ｎを介して管理側システム９０に送信する。
【００５５】
ＩＣカード通信機７９０は、図示しないアンテナ、制御回路、メモリ等で構成される。このＩＣカード通信機７９０は、ＩＣ乗車券３０との間で無線通信を行い、ＩＣ乗車券３０から取得したデータを処理装置７３０に出力するとともに、処理装置７３０から入力されたデータをＩＣ乗車券３０に書き込むための制御を行う。
【００５６】

４．管理側システム

図８は、管理側システム９０の主要内部構成の一例を示すブロック図である。図８に示すように、管理側システム９０は、窓口サーバ９１０、カード使用履歴管理サーバ９３０、入金ＩＤ管理サーバ９５０、暗号キー発生サーバ９７０、及び乱数ＩＤ管理サーバ９９０の各部が接続されたサーバシステムにより実現されるものであり、それぞれＣＰＵ等の処理装置、ハードディスク等の記憶装置、通信回線Ｎに接続するための通信装置、入力装置や表示装置等を備えた公知の汎用サーバ装置によって構成されている。

【００５７】

（窓口サーバ）

窓口サーバ９１０は、管理側システム９０を構成する各部への指示やデータの転送等を行って、管理側システム９０全体を統括的に制御する。また、窓口サーバ９１０は、ＩＣ乗車券３０に対するチャージ金の入金履歴を管理するとともに、残高が不正に積み増されたＩＣ乗車券３０の検出を行う。

【００５８】

この窓口サーバ９１０の記憶装置には、入金管理プログラム９１１と、不正使用検出プログラム９１３と、暗号化プログラム９１５とが格納されている。

【００５９】

入金管理プログラム９１１は、チャージシステム７０から受信した入金情報に基づいて入金履歴データを生成し、入金履歴ファイル９２０として管理するためのプログラムであり、窓口サーバ９１０は、この入金管理プログラム９１１に従って入金管理処理を実行する。

【００６０】

具体的には、窓口サーバ９１０は、チャージシステム７０から入金情報を受信したならば、当該入金情報に設定されているカードＩＤとともに入金ＩＤ発行要求を入金ＩＤ管理サーバ９５０に通知し、当該カードＩＤに対する新たな入金ＩＤを入金ＩＤ管理サーバ９５０に発行させて取得する。そして、窓口サーバ９１０は、当該入金情報のカードＩＤを取得した入金ＩＤと置き換えた入金履歴データを生成して、入金履歴ファイル９２０として管理する。

【００６１】

図９は、入金履歴ファイル９２０のデータ構成例を示す図である。図９に示すように、入金履歴ファイル９２０は、入金ＩＤと、入金時残高と、入金日時とが対応付けられたデータテーブルであり、前述の入金管理処理の結果生成された入金履歴データが格納される。また、詳細は後述するが、前述の入金ＩＤ発行要求に応じて、入金ＩＤ管理サーバ９５０からは、新たな入金ＩＤとともに前回のチャージの際に当該カードＩＤに対して発行された旧入金ＩＤが返信されるようになっており、返信された旧入金ＩＤが設定された入金履歴データは、入金履歴ファイル９２０から削除される。

【００６２】

不正使用検出プログラム９１３は、改札システム５０から受信したカード使用情報に設定されている残高が不正に積み増されたものかを検出するためのプログラムであり、窓口サーバ９１０は、この不正使用検出プログラム９１３に従って不正使用検出処理を実行する。

【００６３】

具体的には、窓口サーバ９１０は、受信したカード使用情報に設定されているカードＩＤを処理対象として以下の処理を実行する。

すなわち、処理対象のカードＩＤとともに入金ＩＤ問合せ要求を入金ＩＤ管理サーバ９５０に通知し、当該カードＩＤに対する入金ＩＤを取得する。次いで、入金履歴ファイル９２０を参照して取得した入金ＩＤに対応する入金時残高を読み出す。そして、受信したカード使用情報に設定されている残高が読み出した入金時残高より増額されている場合には、残高が不正に積み増されたと判断して処理対象のカードＩＤを不正カードＩＤとし、管理側システム９０と接続されている全ての改札システム５０に配信する。

【００６４】
暗号化プログラム９１５は、改札システム５０から受信したカード使用情報に設定されている残高、使用日時、及び改札機ＩＤを暗号化するためのプログラムであり、窓口サーバ９１０は、この暗号化プログラム９１５に従って暗号化処理を実行する。
【００６５】
具体的には、窓口サーバ９１０は、受信したカード使用情報に設定されているカードＩＤを処理対象として以下の処理を実行する。
すなわち、処理対象のカードＩＤとともに暗号化キー問合せ要求を暗号キー発生サーバ９７０に通知し、当該カードＩＤに対する暗号化キーを取得する。そして、取得した暗号キーを用いて各データを所定の暗号方式によって暗号化する。このとき、残高の暗号化は次のようにする。すなわち、先ず残高情報として、ランダムに決定した第１の数値としての数値Ａ、及び数値Ａと残高との差である第２の数値としての数値Ｂを決定する。そして、決定した数値Ａ及び数値Ｂである残高情報を前述のように取得した暗号キーを用いて暗号化する。この暗号化処理の結果、残高、使用日時、及び改札機ＩＤが暗号化されたカード使用情報は、履歴書込要求とともにカード使用履歴管理サーバ９３０に転送される。
【００６６】
（カード使用履歴管理サーバ）
カード使用履歴管理サーバ９３０は、ＩＣ乗車券３０のカード使用履歴を管理するとともに、所定のユーザ操作によってカードＩＤの入力を受け付け、入力されたカードＩＤが割り当てられたＩＣ乗車券３０の使用履歴を特定する。カードＩＤの入力は、例えばカード使用履歴管理サーバ９３０の入力装置から入力されることとしてもよいし、当該カード使用履歴管理サーバ９３０と通信接続される端末装置で入力されたものであってもよい。
【００６７】
このカード使用履歴管理サーバ９３０の記憶装置には、履歴書込制御プログラム９３３と、使用履歴特定プログラム９３５と、使用履歴特定用テーブル９３７とが格納される。
【００６８】
履歴書込制御プログラム９３３は、窓口サーバ９１０から転送されるカード使用情報に基づいてカード使用履歴データを生成し、カード使用履歴ファイル９４０として管理するためのプログラムであり、カード使用履歴管理サーバ９３０は、窓口サーバ９１０から当該カードＩＤが設定されたカード使用情報が転送されたタイミングで、履歴書込制御プログラム９３３に従って履歴書込制御処理を実行する。
【００６９】
具体的には、カード使用履歴管理サーバ９３０は、先ず、当該転送されたカード使用情報に設定されているカードＩＤとともに、乱数ＩＤ発行要求を乱数ＩＤ管理サーバ９９０に通知し、新たな乱数ＩＤを取得する。次いで、カード使用履歴管理サーバ９３０は、当該カード使用情報のカードＩＤを取得させた乱数ＩＤと置き換えたカード使用履歴データを生成する。これにより、同一のカードＩＤが設定されたカード使用情報をもとに生成したカード使用履歴データを転送されてきた順に並べれば、その乱数ＩＤの順番は、当該カードＩＤによって定まる乱数ＩＤ列と同一の順番となる。
【００７０】
続いて、カード使用履歴管理サーバ９３０は、生成したカード使用履歴データを一時的に記憶装置内に保持しておく。そして、所定のタイミングで、例えば使用日時に設定されている時刻（年月日時分）別にカード使用履歴データを分類する。そして、分類毎にカード使用履歴データを生成された順番（窓口サーバ９１０からの転送順）とは異なる順番にランダムに並び替えて、各カード使用履歴データをカード使用履歴ファイル９４０に書き込んでいく。このとき、カード使用履歴管理サーバ９３０は、書込順に従って各カード使用履歴データを、カード使用履歴ファイル９４０に書き込んでいく。
【００７１】
図１０は、カード使用履歴ファイル９４０のデータ構成例を示す図である。図１０に示すように、カード使用履歴ファイル９４０は、通し番号と、乱数ＩＤと、暗号化残高情報

と、使用日時と、暗号化改札機ＩＤとが対応付けられたデータテーブルであり、前述の履歴書込制御処理の結果書き込まれたカード使用履歴データが、書込順を示す通し番号と対応付けられて格納される。すなわち、カード使用履歴ファイル９４０の１レコード分が１つのカード使用情報に対応しており、１つのレコードは通し番号で特定される。尚、通し番号は、レコードを特定するための識別情報であるため、通し番号の代わりにレコードＩＤ等の別の識別情報を用いてもよい。

【００７２】

使用履歴特定プログラム９３５は、ユーザ操作によってカードＩＤが入力された際に、当該カードＩＤが割り当てられたＩＣ乗車券３０の使用履歴を特定するためのプログラムであり、カード使用履歴管理サーバ９３０は、この使用履歴特定プログラム９３５に従って使用履歴特定処理を実行する。この使用履歴特定処理によれば、カード使用履歴ファイル９４０の中から、入力されたカードＩＤが割り当てられたＩＣ乗車券３０から発信されたデータを含むカード使用情報をもとに生成されたカード使用履歴データが抽出されて、当該ＩＣ乗車券３０の使用履歴が特定される。

【００７３】

具体的には、カード使用履歴管理サーバ９３０は、先ず入力されたカードＩＤとともに復号キー問合せ要求を暗号キー発生サーバ９７０に通知し、当該カードＩＤに対する復号キーを取得する。次いで、カード使用履歴管理サーバ９３０は、入力されたカードＩＤとともに乱数ＩＤ列発生要求を乱数ＩＤ管理サーバ９９０に通知し、当該カードＩＤによって定まる乱数ＩＤ列を取得する。

【００７４】

そして、カード使用履歴管理サーバ９３０は、カード使用履歴ファイル９４０に設定されている各カード使用履歴データを使用日時順に並べたときの乱数ＩＤの順番が、入力されたカードＩＤによって定まる乱数ＩＤ列の順番通りになるカード使用履歴データを抽出して当該ＩＣ乗車券３０の使用履歴の候補（使用履歴候補）とする。そして、カード使用履歴管理サーバ９３０は、取得した復号キーで暗号化残高情報、及び暗号化改札機ＩＤの復号が全て成功したか否かによって使用履歴候補を絞り込む。次いで、カード使用履歴管理サーバ９３０は、使用履歴候補をユーザ操作によって入力される絞り込み条件をもとに絞り込んでいくことで、最終的に特定する。

【００７５】

使用履歴特定用テーブル９３７は、使用履歴特定処理によってユーザ操作により入力されたカードＩＤが割り当てられたＩＣ乗車券３０の使用履歴が特定されるまでの間適宜参照されて更新されるデータテーブルである。図１１は、使用履歴特定用テーブル９３７のデータ構成例を示す図である。この使用履歴特定用テーブル９３７は、ユーザ操作によってカードＩＤが入力された際に生成される。

【００７６】

すなわち、この使用履歴特定用テーブル９３７には、ユーザ操作によってカードＩＤが入力された際に、前述のように乱数ＩＤ管理サーバ９９０から取得した乱数ＩＤ列が設定されるとともに、選出されたカード使用履歴データを組み合わせた使用履歴候補が設定される。詳細には、使用履歴候補は、当該使用履歴候補を構成するカード使用履歴データに割り振られた通し番号の順番によって定義される。

【００７７】

（入金ＩＤ管理サーバ）

入金ＩＤ管理サーバ９５０は、ＩＣ乗車券３０に対するチャージ（入金）に係る固有の入金ＩＤを発行して管理する。この入金ＩＤ管理サーバ９５０の記憶装置には、入金ＩＤ発行プログラム９５１と、入金ＩＤテーブル９５３とが格納されている。

【００７８】

入金ＩＤ発行プログラム９５１は、入金ＩＤを発行させるためのプログラムである。発行させた入金ＩＤは、入金ＩＤテーブル９５３に登録されるようになっている。図１２は、入金ＩＤテーブル９５３のデータ構成例を示す図である。図１２に示すように、入金Ｉ

Ｄテーブル９５３は、カードＩＤと、入金ＩＤとが対応付けられたデータテーブルである。

【００７９】

入金ＩＤ管理サーバ９５０は、窓口サーバ９１０から入金ＩＤ発行要求が通知されたならば、当該入金ＩＤ発行要求とともに通知されるカードＩＤを処理対象として以下の処理を実行する。

すなわち、先ず、入金ＩＤ発行プログラム９５１に従って処理対象のカードＩＤに対する新たな入金ＩＤを発行させる。次いで、処理対象のカードＩＤに対する入金ＩＤとして発行させた新たな入金ＩＤを登録し、入金ＩＤテーブル９５３を更新する。そして、発行させた入金ＩＤを、更新前に当該処理対象のカードＩＤと対応付けられて設定されていた入金ＩＤ（旧入金ＩＤ）とともに窓口サーバ９１０に返信する。このとき、処理対象のカードＩＤに対する入金ＩＤが入金ＩＤテーブル９５３に登録されていない場合には、当該カードＩＤと発行した入金ＩＤとを対応付けたレコードを追加して登録し、発行させた入金ＩＤを窓口サーバ９１０に返信する。

【００８０】

また、入金ＩＤ管理サーバ９５０は、窓口サーバ９１０から入金ＩＤ問合せ要求が通知された際には、当該入金ＩＤ問合せ要求とともに通知されるカードＩＤに対する入金ＩＤを入金ＩＤテーブル９５３から読み出して窓口サーバ９１０に返信する。

【００８１】

（暗号キー発生サーバ）

暗号キー発生サーバ９７０は、カード使用情報の暗号化に係るキーデータを管理する。この暗号キー発生サーバ９７０の記憶装置には、キーデータ発生プログラム９７１と、キーテーブル９７３が格納されている。

【００８２】

キーデータ発生プログラム９７１は、暗号化キー及び復号キーを発生させるためのプログラムである。発行させた暗号化キー及び復号キーは、キーテーブル９７３に登録されるようになっている。図１３は、キーテーブル９７３のデータ構成例を示す図である。図１３に示すように、キーテーブル９７３は、カードＩＤと、暗号化キー及び復号キーであるキーデータとが対応付けられたデータテーブルである。

【００８３】

暗号キー発生サーバ９７０は、窓口サーバ９１０から暗号化キー問合せ要求が通知されたならば、当該暗号化キー問合せ要求とともに通知されるカードＩＤを処理対象として以下の処理を実行する。

すなわち、処理対象のカードＩＤに対する暗号化キーをキーテーブル９７３から読み出して窓口サーバ９１０に返信する。このとき、処理対象のカードＩＤに対するキーデータがキーテーブル９７３に登録されていない場合には、キーデータ発生プログラム９７１に従って当該カードＩＤに固有の暗号化キー及び復号キーを発生させてキーテーブル９７３に登録し、発生させた暗号化キーを窓口サーバ９１０に返信する。尚、復号キーはユニークであってもよいが、復号キーを重複して割り当てることとしてもよい。何故ならば、カード使用履歴ファイル９４０が不正に持ち出された場合、復号キーが特定できれば、該当するカードＩＤが割り当てられたＩＣ乗車券３０の使用履歴が特定されてしまうからである。

【００８４】

また、暗号キー発生サーバ９７０は、カード使用履歴管理サーバ９３０から復号キー問合せ要求が通知された際には、当該復号キー問合せ要求とともに通知されるカードＩＤに対する復号キーをキーテーブル９７３から読み出してカード使用履歴管理サーバ９３０に返信する。

【００８５】

（乱数ＩＤ管理サーバ）

乱数ＩＤ管理サーバ９９０は、カードＩＤによって定まる乱数ＩＤを管理する。この乱

数ＩＤ管理サーバ９９０の記憶装置には、乱数ＩＤ列発生プログラム９９１が格納されている。

【００８６】

乱数ＩＤ列発生プログラム９９１は、カードＩＤによって定まる乱数ＩＤ列を発生させるためのプログラムである。乱数ＩＤ管理サーバ９９０は、カード使用履歴管理サーバ９３０から乱数ＩＤ発行要求が通知されたならば、乱数ＩＤ列発生プログラム９９１に従って、当該乱数ＩＤ発行要求とともに通知されるカードＩＤを処理対象として以下の処理を実行する。

すなわち、処理対象のカードＩＤによって定まる固有の乱数ＩＤ列に従った新たな乱数ＩＤを、乱数ＩＤ発行要求が通知されたタイミングで順次発行していく。また発行した乱数ＩＤをカード使用履歴管理サーバ９３０に返信する。

【００８７】

また、乱数ＩＤ管理サーバ９９０は、カード使用履歴管理サーバ９３０から乱数ＩＤ列発生要求が通知されたならば、乱数ＩＤ列発生プログラム９９１に従って、当該乱数ＩＤ列発生要求とともに通知されるカードＩＤによって定まる乱数ＩＤ列を発生させる。また発生させた乱数ＩＤ列をカード使用履歴管理サーバ９３０に返信する。

【００８８】

［処理の流れ］

次に、図１４～図２１を参照して、ＩＣカード管理システム１における処理の流れについて説明する。

【００８９】

先ず、改札システム５０が設置された駅改札でＩＣ乗車券３０が使用された際のＩＣカード管理システム１における処理の流れについて、図１４を参照して説明する。

【００９０】

図１４に示すように、改札システム５０において利用者の入出場を検知した場合には（ステップｂ１０：ＹＥＳ）、処理装置５１０は、ＩＣ乗車券３０との近距離無線通信を制御し、当該ＩＣ乗車券３０にカードＩＤ３９１及び残高３９３を発信させて取得する（ステップａ１０）。続いて処理装置５１０は、取得したカードＩＤが不正カードＩＤ一覧５５５において管理されている不正カードＩＤと一致するか否かを判定し、一致した場合には（ステップｂ２０：ＹＥＳ）、通行させないと判定してゲート扉５９０を閉鎖させ（ステップｂ３０）、処理を終了する。

【００９１】

一方、一致しなかった場合には（ステップｂ２０：ＮＯ）、処理装置５１０は、ステップａ１０の結果取得した残高に基づいて精算処理を実行し（ステップｂ４０）、当該利用者の通行許否を判定する。このとき、処理装置５１０は、残高が不足している場合には通行させないと判定し（ステップｂ５０：ＮＯ）、ゲート扉５９０を閉鎖させる（ステップｂ６０）。

【００９２】

当該利用者を通行させる場合には（ステップｂ５０：ＹＥＳ）、処理装置５１０は、当該ＩＣ乗車券３０の残高３９３を精算額分減額して更新させる制御を行う（ステップｂ７０）。この改札システム５０の制御により、ＩＣ乗車券３０では、残高３９３が更新される（ステップａ２０）。そして、処理装置５１０は、ステップａ１０の結果取得したカードＩＤ及び精算処理後の残高をカード情報とし、当該使用時（精算時）の時刻情報である使用日時及び改札機ＩＤ５５７と対応付けたカード使用情報を生成して（ステップｂ８０）、管理側システム９０に送信する（ステップｂ９０）。

【００９３】

そして、管理側システム９０では、改札システム５０からカード使用情報を受信したならば（ステップｃ１０：ＹＥＳ）、カード使用時処理を実行する（ステップｃ２０）。

【００９４】

ここで、管理側システム９０において実行されるカード使用時処理について、図１５～

図１７を参照して説明する。

【００９５】

図１５は、カード使用時処理の流れを説明するためのフローチャートである。図１５に示すように、カード使用時処理では、窓口サーバ９１０が不正使用検出処理を実行し（ステップｄ１０）、続いて暗号化処理を実行する（ステップｅ１０）。そして、カード使用履歴管理サーバ９３０が履歴書込制御処理を実行する（ステップｆ１０）。以下、順に説明する。

【００９６】

（不正使用検出処理）

図１６は、不正使用検出処理の流れを説明するための図である。

窓口サーバ９１０は、ｄ１１）改札システム５０からカード使用情報が送信されると、不正使用検出処理を実行する。すなわち、窓口サーバ９１０は、ｄ１３）受信したカード使用情報に設定されているカードＩＤとともに入金ＩＤ問合せ要求を入金ＩＤ管理サーバ９５０に通知する。

【００９７】

これに応答して、入金ＩＤ管理サーバ９５０は、ｄ１５）通知されたカードＩＤに対する入金ＩＤを入金ＩＤテーブル９５３から読み出して窓口サーバ９１０に返信する。

【００９８】

入金ＩＤ管理サーバ９５０から入金ＩＤを取得したならば、窓口サーバ９１０は、ｄ１７）入金履歴ファイル９２０を参照し、取得した入金ＩＤに対応する入金時残高を読み出す。そして、窓口サーバ９１０は、ｄ１９）受信したカード使用情報に設定されている残高が読み出した入金時残高よりも増額されているか否かを判定する。

【００９９】

このとき、窓口サーバ９１０は、増額されているならば（ｄ１９：ＹＥＳ）、残高が不正に積み増されたと判断して当該カードＩＤを不正カードＩＤとする。この場合には、窓口サーバ９１０は、ｄ２１）不正カードＩＤを管理側システム９０と接続されている全ての改札システム５０に配信する。これに応答して、各改札システム５０では、ｄ２３）当該不正カードＩＤを不正カードＩＤ一覧５５５に登録する。

【０１００】

一方、受信したカード使用情報に設定されている残高が読み出した入金時残高以下であれば（ｄ１９：ＮＯ）、次に説明する暗号化処理に移行する。

【０１０１】

（暗号化処理）

図１７は、暗号化処理及び後述する履歴書込制御処理の流れを説明するための図である。

窓口サーバ９１０は、ｅ１１）受信したカード使用情報に設定されているカードＩＤとともに暗号化キー問合せ要求を暗号キー発生サーバ９７０に通知する。

【０１０２】

これに応答して、暗号キー発生サーバ９７０は、ｅ１３）通知されたカードＩＤに対する暗号化キーをキーテーブル９７３から読み出して窓口サーバ９１０に返信する。

【０１０３】

暗号キー発生サーバ９７０から暗号化キーを取得したならば、窓口サーバ９１０は、ｅ１５）受信したカード使用情報に設定されている残高、使用日時、及び改札機ＩＤを、取得した暗号キーを用いて暗号化する。そして、窓口サーバ９１０は、ｅ１７）残高、使用日時、及び改札機ＩＤが暗号化されたカード使用情報をカード使用履歴管理サーバ９３０に転送して、履歴書込要求を通知する。これに応答して、カード使用履歴管理サーバ９３０は、履歴書込制御処理を実行する。

【０１０４】

（履歴書込制御処理）

履歴書込制御処理では、カード使用履歴管理サーバ９３０は、履歴書込要求とともに窓

口サーバ９１０から転送されたカード使用情報に設定されているカードＩＤを読み出し、ｆ１１）乱数ＩＤ発行要求を読み出したカードＩＤとともに乱数ＩＤ管理サーバ９９０に通知する。

【０１０５】

これに応答して、乱数ＩＤ管理サーバ９９０は、乱数ＩＤ列発生プログラム９９１に従い、通知されたカードＩＤをもとに新たな乱数ＩＤを発行させて、ｆ１２）発行させた乱数ＩＤをカード使用履歴管理サーバ９３０に返信する。

【０１０６】

乱数ＩＤ管理サーバ９９０から乱数ＩＤを取得したならば、カード使用履歴管理サーバ９３０は、ｆ１３）カードＩＤを取得した乱数ＩＤと置き換えたカード使用履歴データを生成し、生成したカード使用履歴データをカード使用履歴ファイル９４０に書き込む。このとき、カード使用履歴管理サーバ９３０は、生成したカード使用履歴データを一時的に記憶装置内に保持しておく。そして、所定のタイミングで、例えば使用日時に設定されている時刻（年月日時分）が同一のカード使用履歴データ毎に分類し、分類毎にカード使用履歴データを生成された順番（窓口サーバ９１０からの転送順）とは異なる順番にランダムに並び替えることにより、書込順を制御してカード使用履歴ファイル９４０に書き込む。

【０１０７】

次に、チャージシステム７０が設置された券売機等で積み増し額がチャージされた際のＩＣカード管理システム１における処理の流れについて、図１８を参照して説明する。

【０１０８】

図１８に示すように、チャージシステム７０においてチャージ金の入金を検知した場合には（ステップｌ１０：ＹＥＳ）、処理装置７３０は、ＩＣ乗車券３０との近距離無線通信を制御し、当該ＩＣ乗車券３０にカードＩＤ３９１及び残高３９３を発信させて取得する（ステップｋ１０）。

【０１０９】

続いて処理装置７３０は、取得した残高に基づいてチャージ処理を実行する（ステップｌ２０）。そして、処理装置７３０は、チャージ処理の結果に基づいて、当該ＩＣ乗車券３０の残高３９３を積み増し額分増額して更新させる制御を行う（ステップｌ３０）。このチャージシステム７０の制御により、ＩＣ乗車券３０では、残高３９３が更新される（ステップｋ２０）。そして、処理装置７３０は、ステップｋ１０の結果取得したカードＩＤ及びチャージ処理後の残高を、当該入金時の時刻情報である入金日時と対応付けた入金情報を生成して（ステップｌ４０）、管理側システム９０に送信する（ステップｌ５０）。

【０１１０】

そして、管理側システム９０では、チャージシステム７０から入金情報を受信したならば（ステップｍ１０：ＹＥＳ）、入金時処理を実行する（ステップｍ２０）。

【０１１１】

ここで、管理側システム９０で実行される入金時処理について、図１９及び図２０を参照して説明する。

【０１１２】

図１９は、入金時処理の流れを説明するためのフローチャートであり、チャージ処理として、窓口サーバ９１０が入金管理処理を実行する（ステップｎ１０）。

【０１１３】

（入金管処理）

図２０は、入金管理処理の流れを説明するための図である。

窓口サーバ９１０は、ｎ１１）チャージシステム７０から入金情報が送信されると、入金管理処理を実行する。すなわち、窓口サーバ９１０は、ｎ１３）受信した入金情報に設定されているカードＩＤとともに入金ＩＤ発行要求を入金ＩＤ管理サーバ９５０に通知する。

【０１１４】
これに応答して、入金ＩＤ管理サーバ９５０は、ｎ１５）入金ＩＤ発行プログラム９５１に従って通知されたカードＩＤに対する新たな入金ＩＤを発行させ、当該カードＩＤに対する入金ＩＤとして発行させた入金ＩＤを登録して入金ＩＤテーブル９５３を更新する。そして、入金ＩＤ管理サーバ９５０は、ｎ１７）発行させた入金ＩＤを、旧入金ＩＤとともに窓口サーバ９１０に返信する。
【０１１５】
入金ＩＤ管理サーバ９５０から入金ＩＤ及び旧入金ＩＤを取得したならば、窓口サーバ９１０は、ｎ１９）受信した入金情報のカードＩＤを取得した入金ＩＤと置き換えた入金履歴データを生成し、入金履歴ファイル９２０に書き込む。またこのとき、窓口サーバ９１０は、入金ＩＤとともに取得した旧入金ＩＤが設定された入金履歴データを入金履歴ファイル９２０から削除する。
【０１１６】
次に、カード使用履歴管理サーバ９３０において実行される使用履歴特定処理の流れについて、図２１を参照して説明する。尚、ここで説明する処理は、カード使用履歴管理サーバ９３０の処理装置が使用履歴特定プログラム９３５を読み出して実行することにより実現される。
【０１１７】
図２１に示すように、カード使用履歴管理サーバ９３０は、先ず、ユーザ操作に従ってカードＩＤを入力する（ステップｏ１０）。次いで、カード使用履歴管理サーバ９３０は、入力されたカードＩＤとともに復号キー問合せ要求を暗号キー発生サーバ９７０に通知する（ステップｏ２０）。これに応答して、暗号キー発生サーバ９７０は、通知されたカードＩＤに対する復号キーをキーテーブル９７３から読み出し（ステップｐ１０）、カード使用履歴管理サーバ９３０に返信する（ステップｐ２０）。
【０１１８】
暗号キー発生サーバ９７０から復号キーを取得したならば（ステップｏ３０：ＹＥＳ）、カード使用履歴管理サーバ９３０は、続いて前記入力されたカードＩＤとともに乱数ＩＤ列発生要求を乱数ＩＤ管理サーバ９９０に通知する（ステップｏ３５）。これに応答し、乱数ＩＤ管理サーバ９９０は、通知されたカードＩＤによって定まる乱数ＩＤを乱数ＩＤ列発生プログラム９９１に従って発生させて（ステップｑ１０）、カード使用履歴管理サーバ９３０に返信する（ステップｑ２０）。尚このとき、カード使用履歴管理サーバ９３０において、乱数ＩＤ管理サーバ９９０から取得された乱数ＩＤ列が使用履歴特定用テーブル９３７に保持される。
【０１１９】
乱数ＩＤ管理サーバ９９０から乱数ＩＤ列を取得したならば（ステップｏ４０：ＹＥＳ）、カード使用履歴管理サーバ９３０は、続いてカード使用履歴ファイル９４０を参照し、発生させた乱数ＩＤ列に基づいて使用履歴候補を生成する（ステップｏ６０）。具体的には、先ず、使用日時に従った乱数ＩＤの順番がステップｏ４０で取得した乱数ＩＤ列の順番通りになるカード使用履歴データの組合せを全て作成して、使用履歴候補とする。生成した使用履歴候補は、使用履歴特定用テーブル９３７に格納される。
【０１２０】
尚このときに、カード使用履歴管理サーバ９３０は、連続するカード使用履歴データに含まれる使用日時及び改札機ＩＤによって当該駅間の移動が可能かどうかを判断し、当該ＩＣ乗車券３０の使用履歴候補を絞り込むこととしてもよい。
【０１２１】
次に、カード使用履歴管理サーバ９３０は、使用履歴特定用テーブル９３７に設定されている各使用履歴候補それぞれを処理対象として以下の処理を実行する。すなわち、処理対象の使用履歴候補を構成するカード使用履歴データそれぞれの暗号化残高情報、及び暗号化改札機ＩＤをステップｏ３０で取得した復号キーで復号し、復号が全て成功したカード使用履歴データを選出する（ステップｏ６５）。ここで、暗号化残高情報の復号が成功

したか否かは、復号して得られた数値Ａ及び数値Ｂの値が数値であるか、数値Ａから数値Ｂを差し引いた値が正の値であるか等によって判断される。

【０１２２】

そして、カード使用履歴管理サーバ９３０は、使用履歴候補が１つに絞り込まれるまで、以下の処理を繰り返し実行する。

すなわち、カード使用履歴管理サーバ９３０は、ユーザ操作に従って絞り込み条件を入力し（ステップｏ８０）、入力された絞り込み条件に従って、使用履歴候補を絞り込む（ステップｏ９０）。

【０１２３】

例えば、カード使用履歴管理サーバ９３０は、過去に当該ＩＣ乗車券３０を使用した駅や当該駅改札の通過時間帯の指定を受け付ける。そして、使用履歴特定用テーブル９３７に設定されている各使用履歴候補それぞれを処理対象とし、処理対象の使用履歴候補を構成するカード使用履歴データの何れかが、指定された駅に設置された改札システム５０を識別するための改札機ＩＤや、指定された通過時間帯となる使用日時を含むか否かを判定して絞り込む。この際、絞り込まれた使用履歴候補以外の使用履歴候補を削除して使用履歴特定用テーブル９３７を更新する。

【０１２４】

使用履歴候補が１つに絞られた場合には、カード使用履歴管理サーバ９３０は確定と判断し（ステップｏ７０：ＹＥＳ）、当該使用履歴候補を構成するカード使用履歴データの使用日時の順番に従って、その使用履歴を特定する（ステップｏ１００）。そして、カード使用履歴管理サーバ９３０は、使用日時が最新のカード使用履歴データに含まれる残高情報を読み出し、ステップｏ１０で入力されたカードＩＤが割り当てられたＩＣ乗車券３０の残高を特定する（ステップｏ１１０）。

【０１２５】

以上説明したように、本実施形態によれば、駅改札でＩＣ乗車券３０が使用された際に、当該駅改札に設置された改札システム５０は、ＩＣ乗車券３０から取得したカードＩＤ及び精算処理後の残高に、使用日時及び改札機ＩＤを対応付けたカード使用情報を生成して管理側システム９０に送信することができる。一方管理側システム９０では、カード使用情報を受信したならば、先ず窓口サーバ９１０が、当該受信したカード使用情報に設定されている残高、及び改札機ＩＤを暗号化する。続いてカード使用履歴管理サーバ９３０が、当該カード使用情報に設定されているカードＩＤによって定まる固有の乱数ＩＤ列に従った新たな乱数ＩＤを発行させて、カードＩＤを発行させた乱数ＩＤと置き換えたカード使用履歴データを生成し、カード使用履歴ファイル９４０として管理する。このとき、生成したカード使用履歴データをカード使用履歴ファイル９４０に書き込む順番を、生成された順番とは異なる順番で書き込むことができる。

【０１２６】

これによれば、カード使用履歴データに含まれるＩＤは乱数ＩＤであるため、カード使用履歴ファイル９４０を参照するだけでは当該ＩＣ乗車券３０の識別を不能とすることができ、当該カード使用履歴ファイル９４０を意味のないものとすることができる。また、カード使用履歴ファイル９４０に書き込まれている順番をも無意味化することができる。

【０１２７】

また、カード使用履歴管理サーバ９３０では、ユーザ操作によってカードＩＤが入力された場合に、入力されたカードＩＤによって定まる乱数ＩＤ列を発生させる。そして、発生させた乱数ＩＤ列に基づいて、カード使用履歴ファイル９４０の中から、入力されたカードＩＤが割り当てられたＩＣ乗車券３０から発信されたカード情報を含むカード使用情報をもとに生成されたカード使用履歴データを抽出することによって、その使用履歴を特定することができる。

【０１２８】

このように、管理側システム９０（カード使用履歴管理サーバ９３０）では、ユーザ操作によってカードＩＤが入力された場合を除いて、利用者によるＩＣ乗車券３０の使用履

歴の特定を不能とすることができる。そして、ユーザ操作によってカードＩＤが入力された場合には、特定された使用履歴によって、当該ＩＣ乗車券３０の残高を特定することができるので、例えば利用者が当該ＩＣ乗車券を紛失した際に残額を返金することが可能となる。

【０１２９】

また、チャージシステム７０は、当該チャージシステム７０が設置された券売機等で積み増し額がチャージされた際に、ＩＣ乗車券３０から取得したカードＩＤ及びチャージ処理後の入金時残高に、入金日時を対応付けた入金情報を生成して管理側システム９０に送信することができる。一方管理側システム９０では、窓口サーバ９１０が、入金情報の受信の度に入金ＩＤ管理サーバ９５０に入金ＩＤを発行させ、当該入金情報に設定されているカードＩＤを発行させた入金ＩＤと置き換えた入金履歴データを入金履歴ファイル９２０として管理する。そして、チャージ後にＩＣ乗車券３０が使用された場合には、窓口サーバ９１０は、その残高が、入金履歴ファイル９２０として管理されている入金時残高よりも増額されているか否かを判定することによって、ＩＣ乗車券３０への不正なチャージを検出することができる。これによれば、不正使用が検出されたならば当該ＩＣ乗車券３０の使用を禁止することが可能である。

【０１３０】

尚、上記した実施形態では、管理側システム９０を構成する各部をそれぞれ専用のサーバ装置によって実現することとしたが、必ずしも別個独立の装置とする必要はなく、１台又は複数台の装置で実現することとして構わない。

【図面の簡単な説明】

【０１３１】

【図１】ＩＣカード管理システムの全体構成の一例を示す図。
【図２】ＩＣカード管理システムにおけるデータの流れを説明するための図。
【図３】ＩＣ乗車券の主要内部構成の一例を示すブロック図。
【図４】改札システムの主要内部構成の一例を示すブロック図。
【図５】カード使用情報のデータ構成例を示す図。
【図６】チャージシステムの主要内部構成の一例を示すブロック図。
【図７】入金情報のデータ構成例を示す図。
【図８】管理側システムの主要内部構成の一例を示すブロック図。
【図９】入金履歴ファイルのデータ構成例を示す図。
【図１０】カード使用履歴ファイルのデータ構成例を示す図。
【図１１】使用履歴特定用テーブルのデータ構成例を示す図。
【図１２】入金ＩＤテーブルのデータ構成例を示す図。
【図１３】キーテーブルのデータ構成例を示す図。
【図１４】ＩＣ乗車券が使用された際のＩＣカード管理システムにおける処理の流れを説明するためのフローチャート。
【図１５】カード使用時処理の流れを説明するためのフローチャート。
【図１６】不正使用検出処理の流れを説明するための図。
【図１７】暗号化処理及び履歴書込制御処理の流れを説明するための図。
【図１８】ＩＣ乗車券に積み増し額がチャージされた際のＩＣカード管理システムにおける処理の流れを説明するためのフローチャート。
【図１９】入金時処理の流れを説明するためのフローチャート。
【図２０】入金管理処理の流れを説明するための図。
【図２１】使用履歴特定処理の流れを説明するためのフローチャート。

【符号の説明】

【０１３２】

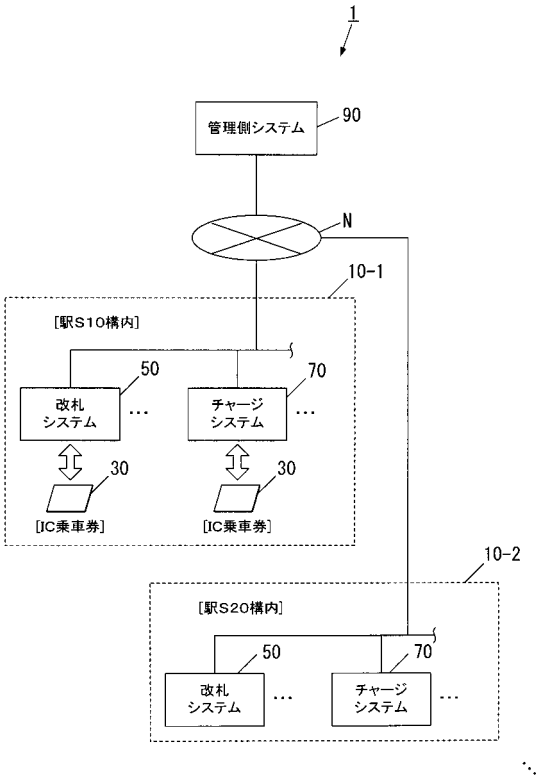
３０　　ＩＣ乗車券
３１０　　アンテナ
３３０　　電源回路

３５０　送受信回路
３７０　制御回路
３９０　メモリ
３９１　カードＩＤ
３９３　残高

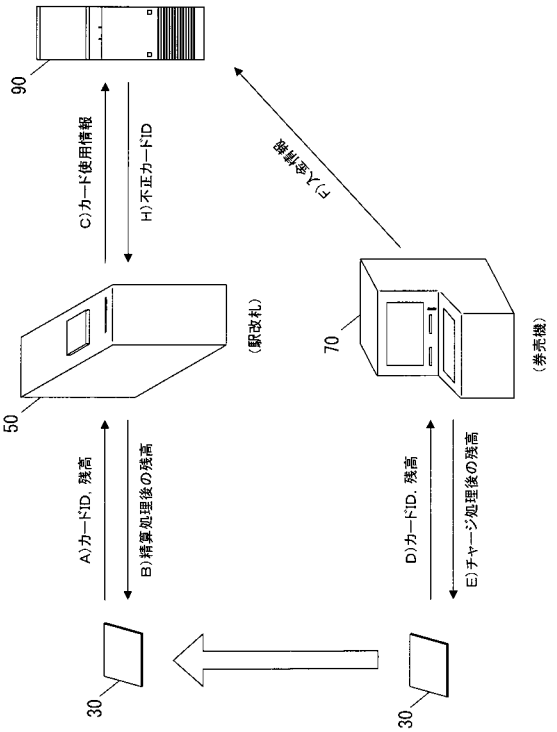
【０１３３】

１　ＩＣカード管理システム
５０　改札システム
５１０　処理装置
５３０　通信装置
５５０　記憶装置
５５１　カード使用情報送信プログラム
５５３　不正使用カード管理プログラム
５５５　不正カードＩＤ一覧
５５７　改札機ＩＤ
５７０　ＩＣカード通信機
５９０　ゲート扉
７０　チャージシステム
７１０　入金装置
７３０　処理装置
７５０　通信装置
７７０　記憶装置
７７１　入金情報送信プログラム
７９０　ＩＣカード通信機
９０　管理側システム
９１０　窓口サーバ
９１１　入金管理プログラム
９１３　不正使用検出プログラム
９１５　暗号化プログラム
９２０　入金履歴ファイル
９３０　カード使用履歴管理サーバ
９３３　履歴書込制御プログラム
９３５　使用履歴特定プログラム
９３７　使用履歴特定用テーブル
９４０　カード使用履歴ファイル
９５０　入金ＩＤ管理サーバ
９５１　入金ＩＤ発行プログラム
９５３　入金ＩＤテーブル
９７０　暗号キー発生サーバ
７１　キーデータ発生プログラム
９７１　キーテーブル
９９０　暗号キー発生サーバ
９９１　乱数ＩＤ列発生プログラム
Ｎ　通信回線

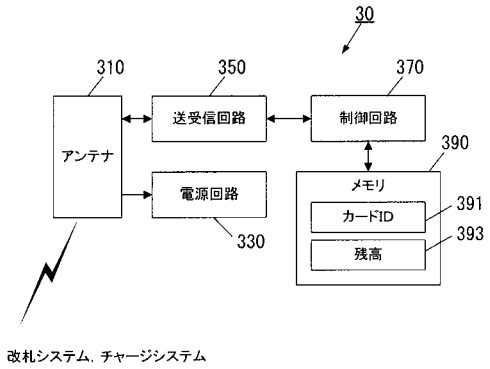
【図１】



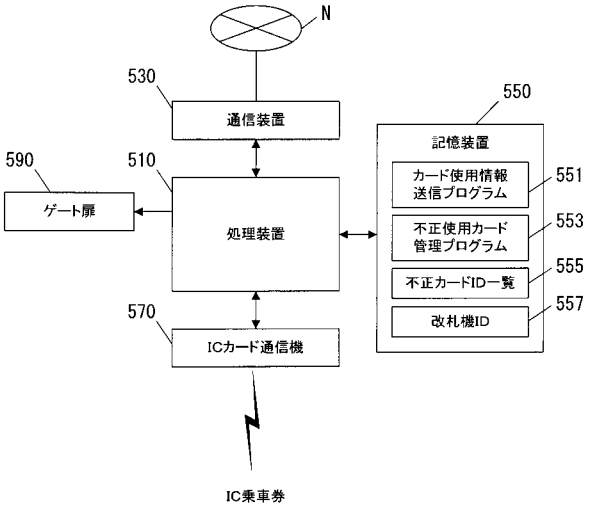
【図２】



【図３】



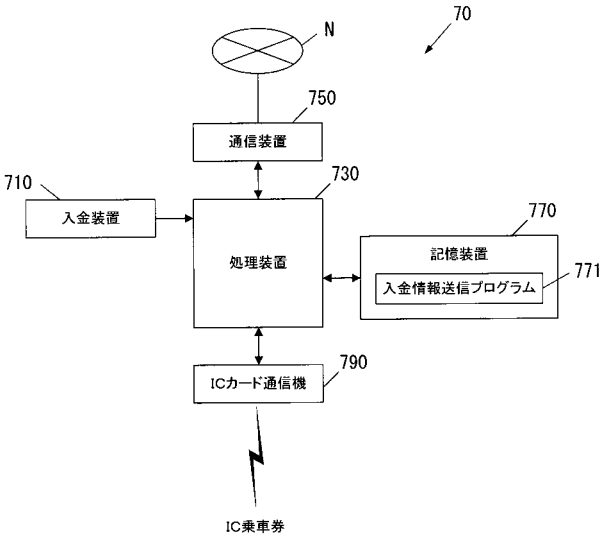
【図４】



【図５】

カード情報		使用日時	改札機ID
カードID	残高		
ID_04562	2,195	2005.4.13.8:22	ID_g00154

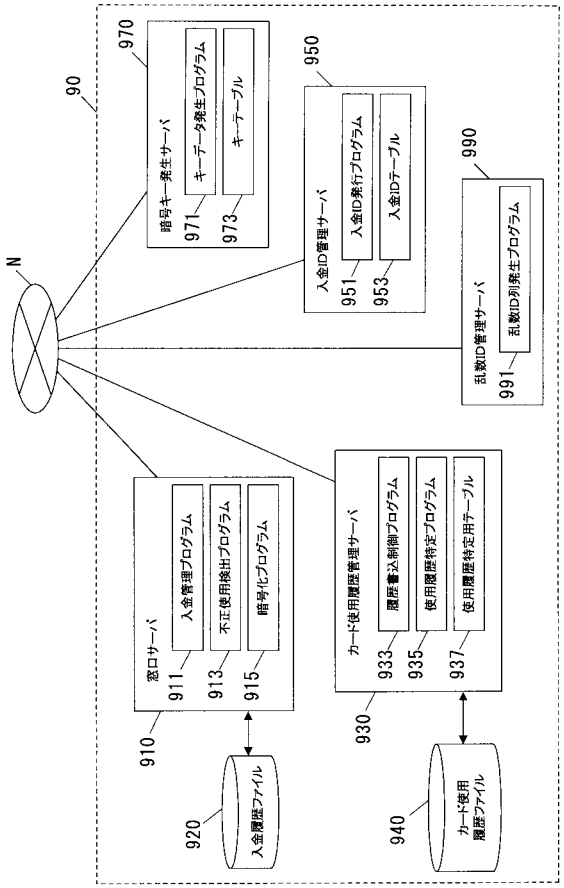
【図６】



【図７】

入金情報		
カードID	入金時残高	入金日時
ID_04562	7,195	2005.4.13.15:02

【図８】



【図９】

920

入金ID	入金時残高	入金日時
cID_00045	10,880	2005.1.14.8:04
⋮	⋮	⋮
cID_00351	7,195	2005.4.13.15:02
cID_00352	10,610	2005.4.13.15:03
⋮	⋮	⋮

【図１０】

940

通し番号	乱数ID	暗号化残高情報 A	暗号化残高情報 B	使用日時	暗号化改札機ID
…	…	…	…	…	…
0000548	413	XXXX	XXXXXXX	2005.4.13.8:22	XXXXX
0000549	217	YYY	YY	2005.4.13.8:22	YYYYY
0000550	871	ZZZZZZZ	ZZZZZZZ	2005.4.13.8:23	ZZZZZ
…	…	…	…	…	…

【図１１】

937

乱数ID列	135	413	918	643	・・・
使用履歴候補	0000081	0000102	0000223	0000310	・・・
	0000081	0000191	0000347	0000378	・・・
	0000081	0000222	0000289	0000511	・・・
	・ ・ ・				

【図１２】

953

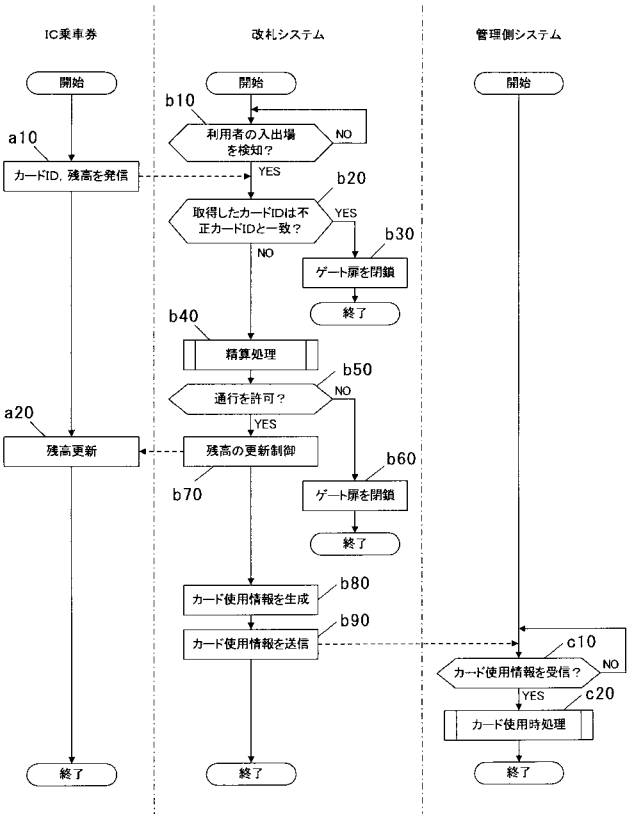
カードID	入金ID
⋮	⋮
ID_04562	cID_00351
ID_04565	cID_00119
⋮	⋮

【図１３】

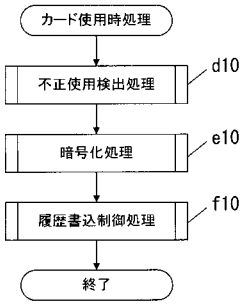
973

カードID	キーデータ	
	暗号化キー	復号キー
⋮	⋮	⋮
ID_04562	xxxx	xxxxxx
ID_04565	yyyy	yyyyyy
⋮	⋮	⋮

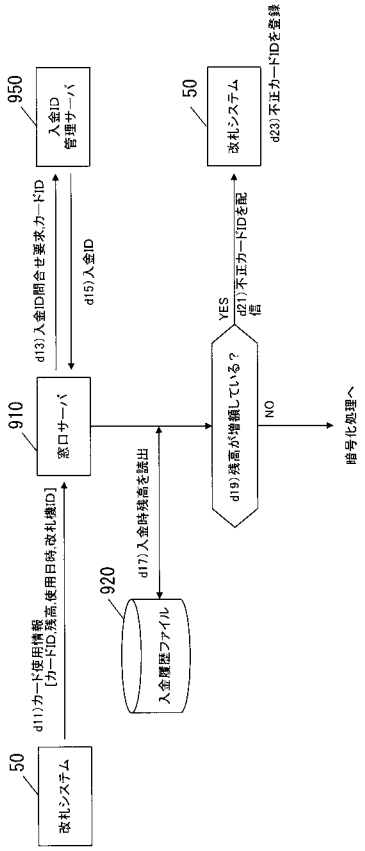
【図１４】



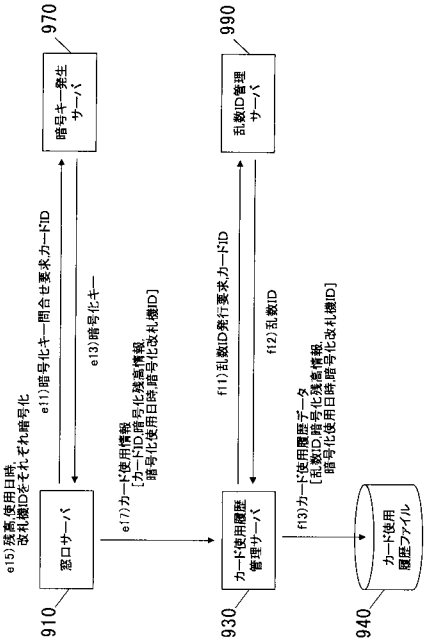
【図１５】



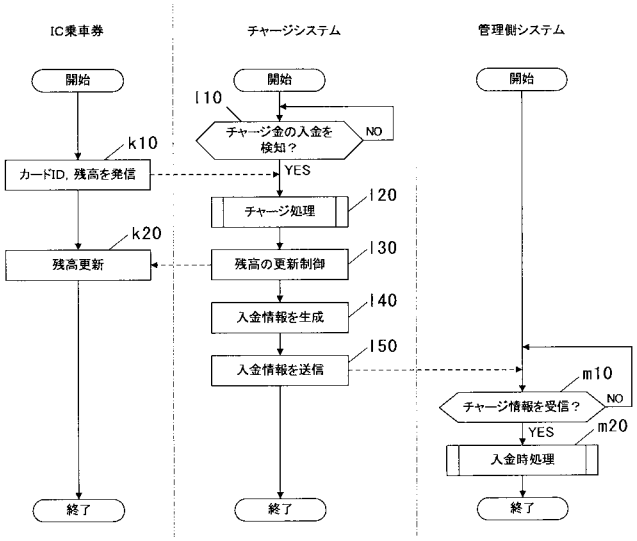
【図１６】



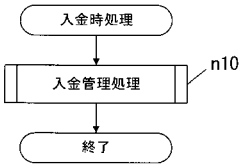
【図１７】



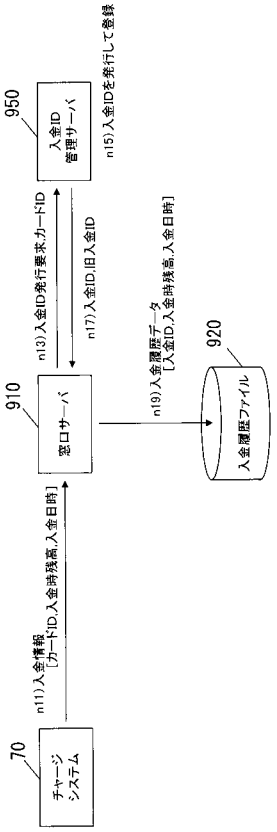
【図１８】



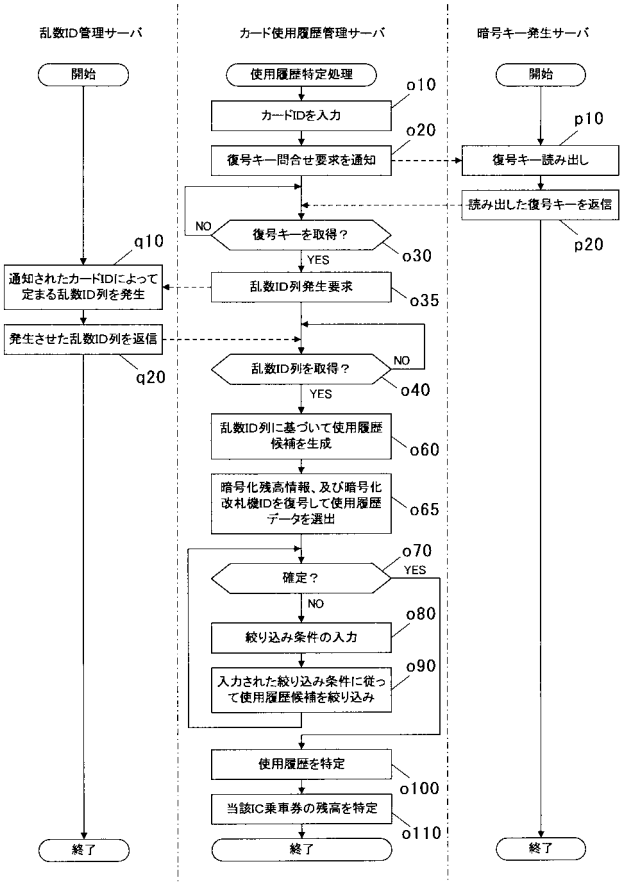
【図１９】



【図２０】


950
入金ID
管理サーバ
n15)入金IDを発行して登録
n13)入金ID発行要求,カードID
n17)入金ID,旧入金ID
910
窓口サーバ
n19)入金履歴データ
[入金ID,入金時残高,入金日時]
920
入金履歴ファイル
n11)入金情報
[カードID,入金時残高,入金日時]
70
チャージ
システム

【図２１】


乱数ID管理サーバ
カード使用履歴管理サーバ
暗号キー発生サーバ
開始
使用履歴特定処理
o10
カードIDを入力
o20
復号キー問合せ要求を通知
開始
p10
復号キー読み出し
読み出した復号キーを返信
p20
NO
復号キーを取得？
o30
YES
q10
通知されたカードIDによって定まる乱数ID列を発生
乱数ID列発生要求
o35
発生させた乱数ID列を返信
q20
乱数ID列を取得？
NO
o40
YES
乱数ID列に基づいて使用履歴候補を生成
o60
暗号化残高情報、及び暗号化改札機IDを復号して使用履歴データを選出
o65
o70
確定？
YES
NO
o80
絞り込み条件の入力
o90
入力された絞り込み条件に従って使用履歴候補を絞り込み
使用履歴を特定
o100
当該IC乗車券の残高を特定
o110
終了
終了
終了

フロントページの続き

(51)Int.Cl.	FI		テーマコード（参考）
	Ｇ０６Ｆ 17/60	５１０	
	Ｇ０６Ｆ 17/60	５１２	
	Ｇ０６Ｋ 17/00	Ｌ	