

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第4747279号
(P4747279)

(45) 発行日 平成23年8月17日(2011.8.17)

(24) 登録日 平成23年5月27日(2011.5.27)

(51) Int.Cl.	F I				
G07B 11/00	(2006.01)	G07B 11/00	501		
G06K 17/00	(2006.01)	G06K 17/00	E		
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		
請求項の数 6 (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)
 (65) 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)
 審査請求日 平成19年11月15日(2007.11.15)

(73) 特許権者 000173784
 公益財団法人鉄道総合技術研究所
 東京都国分寺市光町二丁目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
 審査官 大谷 光司

最終頁に続く

(54) 【発明の名称】 ICカード管理システム

(57) 【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によって定まる固有の乱数ID列に従った新たな乱数IDを順次発行する乱数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前記暗号化手段により暗号化された前記発信データを、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よって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、前記第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、前記発信データに含まれる残高を前記残高情報決定手段により決定

10

20

30

40

50

された前記残高情報と置き換えたものを暗号化する、

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

10

20

30

40

50

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。

【 0 0 0 5 】

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。

【 0 0 0 6 】

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】

【 0 0 0 7 】

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によって定まる固有の乱数ＩＤ列に従った新たな乱数ＩＤを順次発行する乱数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。

【 0 0 0 8 】

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

10

20

30

40

50

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前記暗号化手段により暗号化された前記発信データを、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よって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、暗号化された発信データの当該入力された識別IDに対応付けて管理されている復号鍵による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、

10

20

30

40

50

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（例えば、図 8 に示す窓口サーバ 910）が、前記発信データに含まれる残高を前記残高情報決定手段により決定された前記残高情報と置き換えたものを暗号化

することを特徴としている。

【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 の数値を決定し、これらの第 1 の数値、及び第 2 の数値を元の残高と置き換えた後、カード情報の発信データを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、

10

20

30

40

50

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]

10

20

30

40

50

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

10

20

30

40

50

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。

10

【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

20

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。

30

【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。

40

【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。

50

【 0 0 3 9 】

2 . 改札システム

図 4 は、改札システム 5 0 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 5 0 は、処理装置 5 1 0、通信装置 5 3 0、記憶装置 5 5 0、IC カード通信機 5 7 0、利用者の通行を規制するゲート扉 5 9 0 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。

【 0 0 4 0 】

処理装置 5 1 0 は、CPU 等で構成され、改札システム 5 0 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 5 0 を統括的に制御する。具体的には、IC カード通信機 5 7 0 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 5 5 0 から読み出して実行し、処理結果を記憶装置 5 5 0 に格納する。この処理装置 5 1 0 は、当該改札システム 5 0 が設置された駅改札で IC 乗車券 3 0 が使用された際に、当該 IC 乗車券 3 0 の残高 3 9 3 (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 3 0 の残高 3 9 3 を精算額分減額して更新させる。

【 0 0 4 1 】

通信装置 5 3 0 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 9 0) との通信を行うための制御を行う。この通信装置 5 3 0 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。

【 0 0 4 2 】

記憶装置 5 5 0 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 5 0 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 5 5 1 と、不正使用カード管理プログラム 5 5 3 と、不正カード ID 一覧 5 5 5 と、当該改札システム 5 0 の設置位置を特定する改札機 ID 5 5 7 とを含む。

【 0 0 4 3 】

カード使用情報送信プログラム 5 5 1 は、IC 乗車券 3 0 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 3 0 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 5 0 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 9 0 に送信するためのプログラムである。

【 0 0 4 4 】

図 5 は、管理側システム 9 0 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 5 1 0 は、精算処理の後、当該 IC 乗車券 3 0 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 ID 5 5 7 を対応付けたカード使用情報を生成して、通信装置 5 3 0 及び通信回線 N を介して管理側システム 9 0 に送信する。

【 0 0 4 5 】

不正使用カード管理プログラム 5 5 3 は、管理側システム 9 0 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 5 5 3 に従って、処理装置 5 1 0 は、管理側システム 9 0 から通知された不正カード ID を不正カード ID 一覧 5 5 5 に登録して管理し、不正カード ID 一覧 5 5 5 に含まれるカード ID の IC 乗車券 3 0 が使用された場合には、ゲート扉 5 9 0 を閉鎖させて利用者の通行を禁止する。

【 0 0 4 6 】

不正カード ID 一覧 5 5 5 は、管理側システム 9 0 から通知された不正カード ID の一覧を記憶する。

【 0 0 4 7 】

IC カード通信機 5 7 0 は、図示しないアンテナ、制御回路、メモリ等で構成される。

10

20

30

40

50

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

10

20

30

40

50

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。

10

【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】

20

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。

30

【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】

40

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を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

50

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。

10

【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。

20

【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。

30

【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。

40

【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

50

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。

10

【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。

20

【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。

30

【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。

40

【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 ID 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。

50

【 0 0 7 9 】

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、まず、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。

10

【 0 0 8 0 】

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。

【 0 0 8 1 】

(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。

20

【 0 0 8 2 】

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。

【 0 0 8 3 】

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。

30

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。

40

【 0 0 8 4 】

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。

【 0 0 8 5 】

(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。

50

【 0 0 8 6 】

乱数 I D 列発生プログラム 9 9 1 は、カード I D によって定まる乱数 I D 列を発生させるためのプログラムである。乱数 I D 管理サーバ 9 9 0 は、カード使用履歴管理サーバ 9 3 0 から乱数 I D 発行要求が通知されたならば、乱数 I D 列発生プログラム 9 9 1 に従って、当該乱数 I D 発行要求とともに通知されるカード I D 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 I D によって定まる固有の乱数 I D 列に従った新たな乱数 I D を、乱数 I D 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 I D をカード使用履歴管理サーバ 9 3 0 に返信する。

【 0 0 8 7 】

また、乱数 I D 管理サーバ 9 9 0 は、カード使用履歴管理サーバ 9 3 0 から乱数 I D 列発生要求が通知されたならば、乱数 I D 列発生プログラム 9 9 1 に従って、当該乱数 I D 列発生要求とともに通知されるカード I D によって定まる乱数 I D 列を発生させる。また発生させた乱数 I D 列をカード使用履歴管理サーバ 9 3 0 に返信する。

【 0 0 8 8 】

[処理の流れ]

次に、図 1 4 ~ 図 2 1 を参照して、I C 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。

【 0 0 8 9 】

まず、改札システム 5 0 が設置された駅改札で I C 乗車券 3 0 が使用された際の I C カード管理システム 1 における処理の流れについて、図 1 4 を参照して説明する。

【 0 0 9 0 】

図 1 4 に示すように、改札システム 5 0 において利用者の入出場を検知した場合には (ステップ b 1 0 : Y E S)、処理装置 5 1 0 は、I C 乗車券 3 0 との近距離無線通信を制御し、当該 I C 乗車券 3 0 にカード I D 3 9 1 及び残高 3 9 3 を発信させて取得する (ステップ a 1 0)。続いて処理装置 5 1 0 は、取得したカード I D が不正カード I D 一覧 5 5 5 において管理されている不正カード I D と一致するか否かを判定し、一致した場合には (ステップ b 2 0 : Y E S)、通行させないと判定してゲート扉 5 9 0 を閉鎖させ (ステップ b 3 0)、処理を終了する。

【 0 0 9 1 】

一方、一致しなかった場合には (ステップ b 2 0 : N O)、処理装置 5 1 0 は、ステップ a 1 0 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 b 4 0)、当該利用者の通行可否を判定する。このとき、処理装置 5 1 0 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 b 5 0 : N O)、ゲート扉 5 9 0 を閉鎖させる (ステップ b 6 0)。

【 0 0 9 2 】

当該利用者を通行させる場合には (ステップ b 5 0 : Y E S)、処理装置 5 1 0 は、当該 I C 乗車券 3 0 の残高 3 9 3 を精算額分減額して更新させる制御を行う (ステップ b 7 0)。この改札システム 5 0 の制御により、I C 乗車券 3 0 では、残高 3 9 3 が更新される (ステップ a 2 0)。そして、処理装置 5 1 0 は、ステップ a 1 0 の結果取得したカード I D 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 I D 5 5 7 と対応付けたカード使用情報を生成して (ステップ b 8 0)、管理側システム 9 0 に送信する (ステップ b 9 0)。

【 0 0 9 3 】

そして、管理側システム 9 0 では、改札システム 5 0 からカード使用情報を受信したならば (ステップ c 1 0 : Y E S)、カード使用時処理を実行する (ステップ c 2 0)。

【 0 0 9 4 】

ここで、管理側システム 9 0 において実行されるカード使用時処理について、図 1 5 ~ 図 1 7 を参照して説明する。

【 0 0 9 5 】

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。

10

【0097】

これに回答して、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。

20

【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。これに回答して、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】

これに回答して、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。これに回答して、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。

40

【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

50

通知する。

【 0 1 0 5 】

これに回答して、乱数 I D 管理サーバ 9 9 0 は、乱数 I D 列発生プログラム 9 9 1 に従い、通知されたカード I D をもとに新たな乱数 I D を発行させて、f 1 2) 発行させた乱数 I D をカード使用履歴管理サーバ 9 3 0 に返信する。

【 0 1 0 6 】

乱数 I D 管理サーバ 9 9 0 から乱数 I D を取得したならば、カード使用履歴管理サーバ 9 3 0 は、f 1 3) カード I D を取得した乱数 I D 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 9 4 0 に書き込む。このとき、カード使用履歴管理サーバ 9 3 0 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 9 1 0 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 9 4 0 に書き込む。

10

【 0 1 0 7 】

次に、チャージシステム 7 0 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 I C カード管理システム 1 における処理の流れについて、図 1 8 を参照して説明する。

【 0 1 0 8 】

図 1 8 に示すように、チャージシステム 7 0 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 l 1 0 : Y E S ）、処理装置 7 3 0 は、I C 乗車券 3 0 との近距離無線通信を制御し、当該 I C 乗車券 3 0 にカード I D 3 9 1 及び残高 3 9 3 を発信させて取得する（ステップ k 1 0 ）。

20

【 0 1 0 9 】

続いて処理装置 7 3 0 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 l 2 0 ）。そして、処理装置 7 3 0 は、チャージ処理の結果に基づいて、当該 I C 乗車券 3 0 の残高 3 9 3 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 l 3 0 ）。このチャージシステム 7 0 の制御により、I C 乗車券 3 0 では、残高 3 9 3 が更新される（ステップ k 2 0 ）。そして、処理装置 7 3 0 は、ステップ k 1 0 の結果取得したカード I D 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 l 4 0 ）、管理側システム 9 0 に送信する（ステップ l 5 0 ）。

30

【 0 1 1 0 】

そして、管理側システム 9 0 では、チャージシステム 7 0 から入金情報を受信したならば（ステップ m 1 0 : Y E S ）、入金時処理を実行する（ステップ m 2 0 ）。

【 0 1 1 1 】

ここで、管理側システム 9 0 で実行される入金時処理について、図 1 9 及び図 2 0 を参照して説明する。

【 0 1 1 2 】

図 1 9 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 9 1 0 が入金管理処理を実行する（ステップ n 1 0 ）。

40

【 0 1 1 3 】

（入金管処理）

図 2 0 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 9 1 0 は、n 1 1) チャージシステム 7 0 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 9 1 0 は、n 1 3) 受信した入金情報に設定されているカード I D とともに入金 I D 発行要求を入金 I D 管理サーバ 9 5 0 に通知する。

【 0 1 1 4 】

これに回答して、入金 I D 管理サーバ 9 5 0 は、n 1 5) 入金 I D 発行プログラム 9 5

50

1 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。

10

【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、まず、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)。これに回答して、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)。

20

【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)。これに回答し、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。

30

【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、まず、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。

40

【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。

50

【 0 1 2 2 】

そして、カード使用履歴管理サーバ 9 3 0 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 9 3 0 は、ユーザ操作に従って絞り込み条件を入力し（ステップ 0 8 0 ）、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 0 9 0 ）。

【 0 1 2 3 】

例えば、カード使用履歴管理サーバ 9 3 0 は、過去に当該 IC 乗車券 3 0 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 9 3 7 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 5 0 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 9 3 7 を更新する。

10

【 0 1 2 4 】

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 9 3 0 は確定と判断し（ステップ 0 7 0 : Y E S ）、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 0 1 0 0 ）。そして、カード使用履歴管理サーバ 9 3 0 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 0 1 0 で入力されたカード ID が割り当てられた IC 乗車券 3 0 の残高を特定する（ステップ 0 1 1 0 ）。

20

【 0 1 2 5 】

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 3 0 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 5 0 は、IC 乗車券 3 0 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 9 0 に送信することができる。一方管理側システム 9 0 では、カード使用情報を受信したならば、先ず窓口サーバ 9 1 0 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 9 3 0 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 9 4 0 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 9 4 0 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。

30

【 0 1 2 6 】

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 9 4 0 を参照するだけでは当該 IC 乗車券 3 0 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 9 4 0 を意味のないものとする事ができる。また、カード使用履歴ファイル 9 4 0 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。

【 0 1 2 7 】

また、カード使用履歴管理サーバ 9 3 0 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 9 4 0 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 3 0 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。

40

【 0 1 2 8 】

このように、管理側システム 9 0（カード使用履歴管理サーバ 9 3 0）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 3 0 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 3 0 の残高を特定することが

50

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。

【 0 1 2 9 】

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。

10

【 0 1 3 0 】

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 】

【 0 1 3 1 】

【 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 】

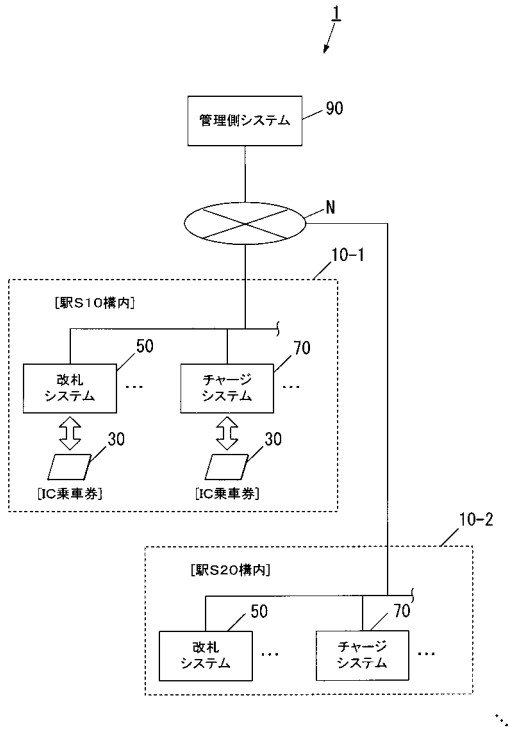
【 0 1 3 2 】

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

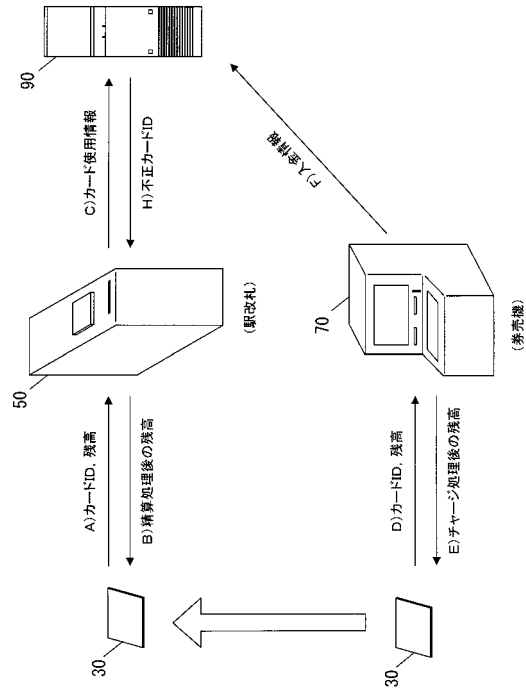
40

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	10
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	20
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	30
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	40
991	乱数ID列発生プログラム	
N	通信回線	

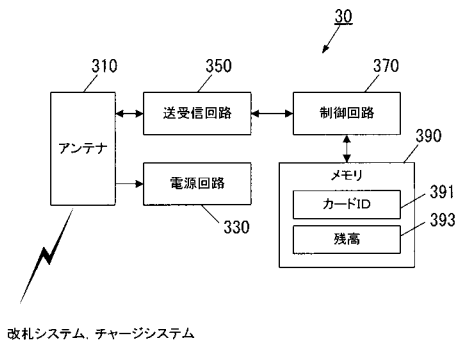
【図1】



【図2】



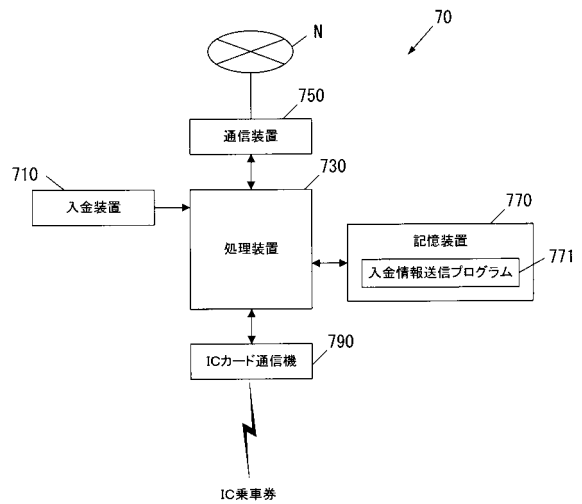
【図3】



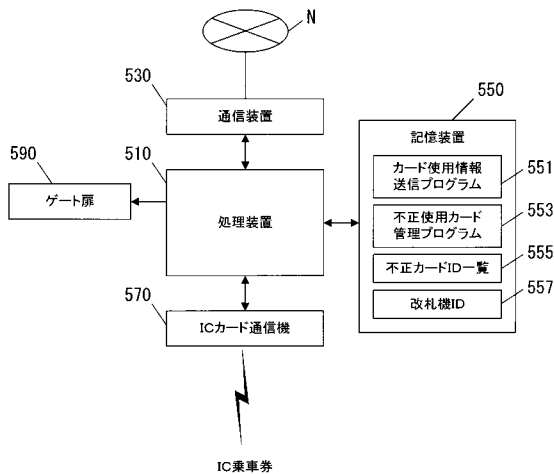
【図5】

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】



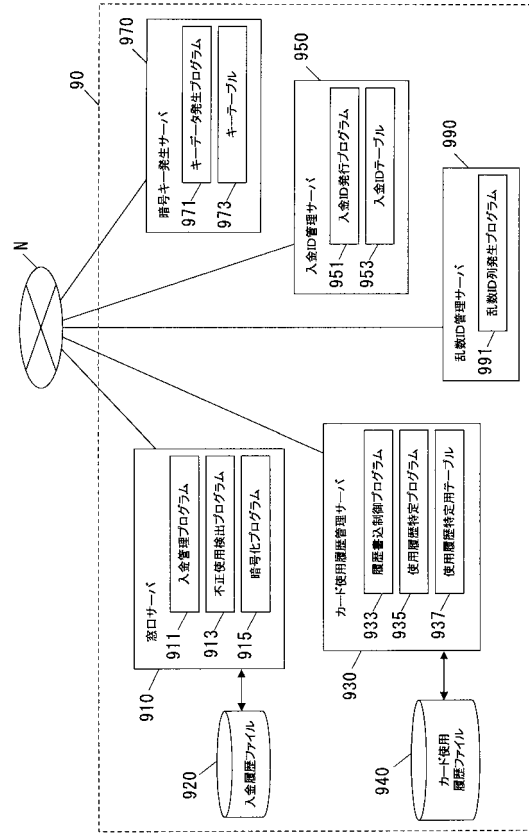
【図4】



【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		使用日時	暗号化改札機ID
		A	B		
⋮	⋮	⋮	⋮	⋮	⋮
0000548	413	XXXX	XXXXXXX	2005.4.13.8:22	XXXXX
0000549	217	YYY	YY	2005.4.13.8:22	YYYYY
0000550	871	ZZZZZZ	ZZZZZZ	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

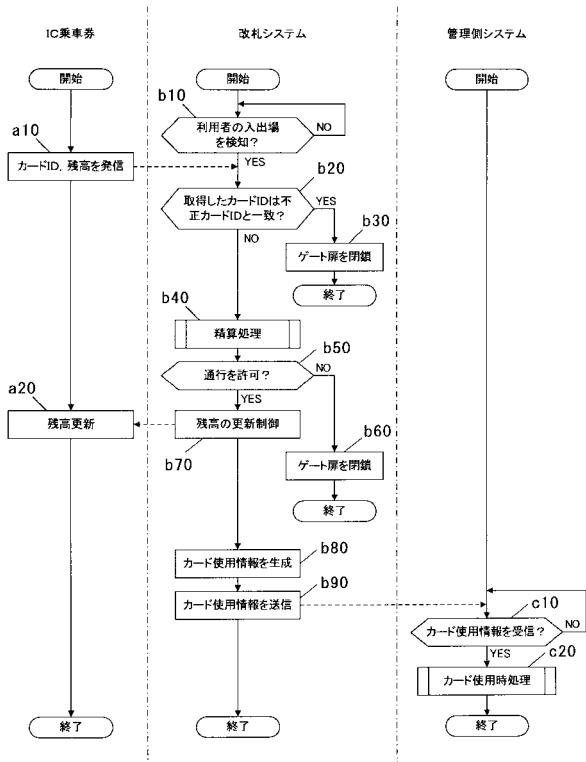
カードID	キーデータ	
	暗号化キー	復号キー
⋮	⋮	⋮
ID_04562	xxxx	xxxxxx
ID_04565	yyyy	yyyyyy
⋮	⋮	⋮

【図12】

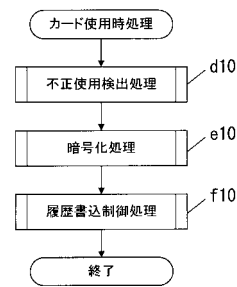
953

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

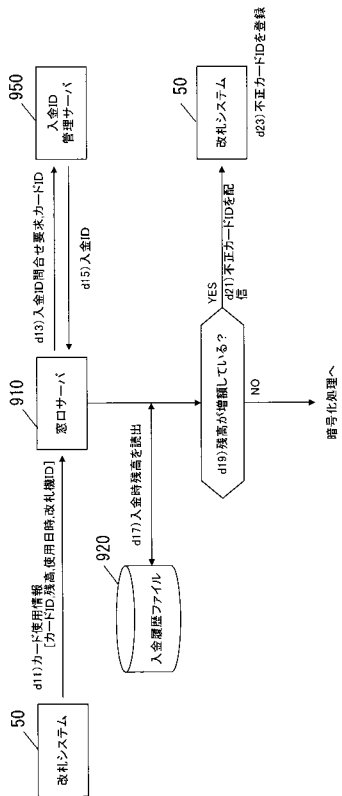
【図14】



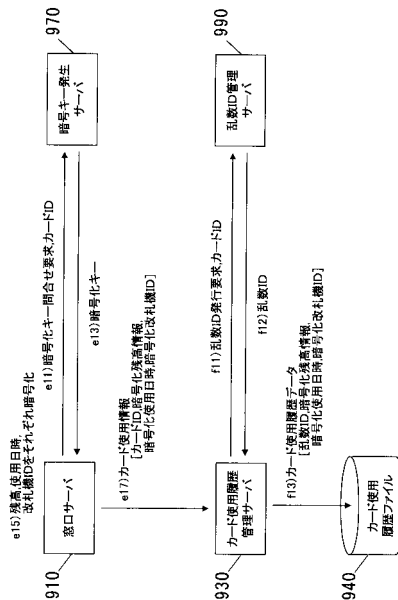
【図15】



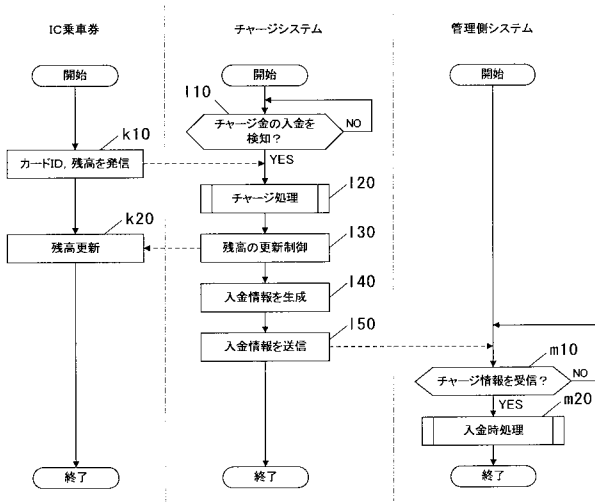
【図16】



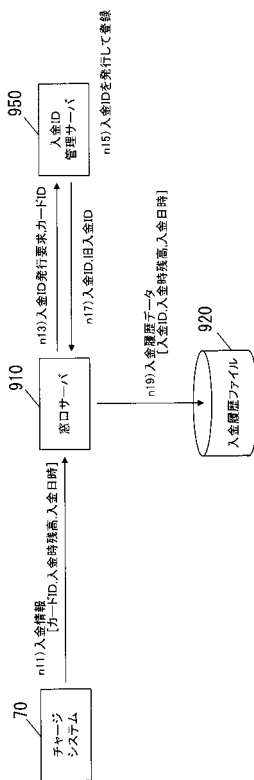
【図17】



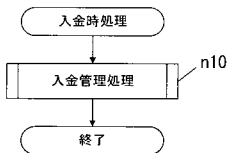
【図18】



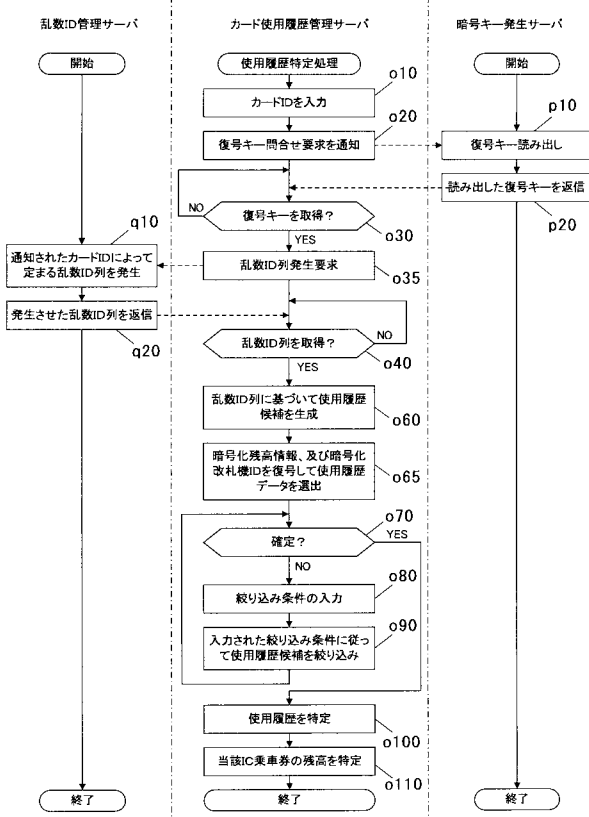
【図20】



【図19】



【図 21】



フロントページの続き

(51)Int.Cl. F I
G 0 6 F 17/60 5 1 0
G 0 6 F 17/60 5 1 2
G 0 6 K 17/00 L

(56)参考文献 特開平 1 0 - 1 5 4 1 9 3 (J P , A)
特開平 0 5 - 2 7 4 2 1 9 (J P , A)
特開平 1 1 - 2 0 3 2 0 7 (J P , A)
特開 2 0 0 4 - 2 0 1 0 3 8 (J P , A)
特開 2 0 0 4 - 1 5 1 8 1 8 (J P , A)
特開 2 0 0 0 - 0 9 9 6 0 3 (J P , A)

(58)調査した分野(Int.Cl. , DB名)
G 0 6 F 1 2 / 1 4 , 2 1 / 0 2 , 2 1 / 0 6 , 2 1 / 2 4
G 0 6 K 1 7 / 0 0
G 0 6 Q 1 0 / 0 0 , 4 0 / 0 0 , 5 0 / 0 0
G 0 7 B 1 / 0 0 ~ 1 7 / 0 4
G 0 9 C 1 / 0 0 ~ 5 / 0 0
H 0 4 K 1 / 0 0 ~ 3 / 0 0
H 0 4 L 9 / 0 0 ~ 9 / 3 8