

(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2013-84032

(P2013-84032A)

(43) 公開日 平成25年5月9日(2013.5.9)

(51) Int.Cl.	F I	テーマコード (参考)
G06F 21/31 (2013.01)	G06F 21/20 131E	3E142
G06Q 20/24 (2012.01)	G06F 17/60 402	5B058
H04L 9/32 (2006.01)	H04L 9/00 673C	5J104
G07G 1/12 (2006.01)	G07G 1/12 321P	
G07G 1/14 (2006.01)	G07G 1/14 ZEC	
審査請求 未請求 請求項の数 4 O L (全 16 頁) 最終頁に続く		

(21) 出願番号 特願2011-221645 (P2011-221645)
 (22) 出願日 平成23年10月6日 (2011.10.6)

(71) 出願人 000116987
 旭精工株式会社
 東京都港区南青山2丁目24番15号
 (72) 発明者 宮地 勝
 埼玉県さいたま市岩槻区古ヶ場一丁目3番
 地の7 旭精工株式会社埼玉工場内
 Fターム(参考) 3E142 AA01 AA08 CA13 EA04 FA03
 GA05 GA06 HA13 JA04
 5B058 CA25 KA02 KA08 KA31 KA35
 YA02
 5J104 AA01 AA07 AA16 EA04 EA15
 JA03 KA02 KA04 NA02 NA05
 NA27 NA33 NA37 PA10

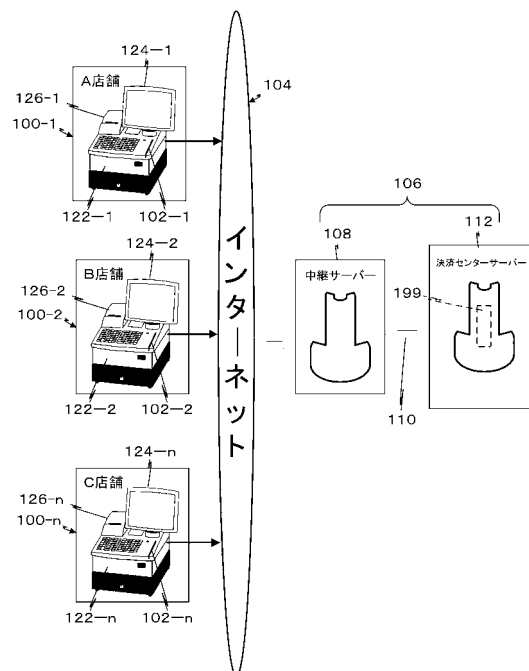
(54) 【発明の名称】 クレジットカードの決済システム及び決済方法

(57) 【要約】 (修正有)

【課題】 クレジット決済に関する暗号化鍵情報をスキミングされないようにしてクレジット決済に関する暗号化された情報を復号化されないようにするクレジットカードの決済システム及び決済方法を提供する。

【解決手段】 クレジットカードから決済端末機102-1～102-nのカードリーダーの磁気ヘッドによって認識情報が読み込まれる。当該認識情報はROMに記録された暗号化鍵によって暗号化され、決済端末機に個別に付与された端末番号と共にインターネット通信回線104によって中継サーバ108へ送られる。中継サーバは自己のROMに記録される復号化鍵テーブルから決済端末機の端末番号に相対して記録されている復号化鍵を呼び出し、暗号化された認識情報を復号化する。復号化された認識情報は専用回線110を通じて決済センターサーバ112に送信され、決済処理が行われる。決済処理結果は、中継サーバを経由して決済端末機に送信される。

【選択図】 図1



【特許請求の範囲】

【請求項 1】

決済端末機(102)においてクレジットカード(114)から読み込んだ認識情報(132)を暗号化して決済サーバ(106)に送信し、当該決済サーバ(106)において復号化し、当該復号化した認識情報(132)に基づいて決済処理の可否を判断するようにしたクレジットカードの決済システムにおいて、

前記決済端末機(102)は、少なくともクレジットカード(114)に記録されている前記認識情報(132)を読み込むカードリーダー(128)、前記カードリーダー(128)によって読み込んだ前記認識情報(132)を暗号化鍵情報記録装置(146)に記録された暗号化鍵情報(154)に基づいて暗号化する暗号化装置(144)、及び、前記決済端末機(102)に対し個別に付与された端末機識別情報(156)を記録する端末機識別情報記録装置(164)を有して成り、

前記決済サーバ(106)は、少なくとも中継サーバ(108)と決済センターサーバ(112)を含み、

前記中継サーバ(108)は、前記端末機識別情報(156)と復号化鍵情報(186)との復号化鍵情報テーブル記録装置(195)、前記決済端末機(102)から受信した端末機識別情報(156)に対応する前記復号化鍵情報テーブル記録装置(195)に記録された復号化鍵情報(186)を出力する復号化鍵情報出力装置(197)と、前記復号化鍵情報出力装置(197)からの復号化鍵情報(186)に基づいて前記認識情報(132)を復号化する復号化装置(194)を含み、

前記決済センターサーバ(112)は前記復号化された前記認識情報(132)に基づいてクレジット決済処理を行うクレジット処理装置(200)を含んでいる

クレジットカードの決済システム。

【請求項 2】

請求項1のクレジットカードの決済システムにおいて、

前記認識情報(132)はクレジットカード(114)に付与された個別の番号であることを特徴とする。

【請求項 3】

請求項2のクレジットカードの決済システムにおいて、

前記暗号化鍵情報(154)は不揮発性ICチップに記録されていることを特徴とする。

【請求項 4】

決済端末機(102)においてクレジットカード(114)から読み込んだ認識情報(132)を暗号化して決済サーバ(106)に送信し、当該決済サーバ(106)において復号化し、当該復号化した前記認識情報(132)に基づいて決済処理の可否を判断するようにしたクレジットカードの決済システムにおいて、

前記クレジットカード(114)に記録されている前記認識情報(132)を前記決済端末機(102)に設けられたカードリーダー(128)によって読み込み、

当該読み込んだ認識情報(132)を前記決済端末機(102)に内蔵された不揮発性記録装置(146)に記録された暗号化鍵情報(154)を用いて所定の暗号方式によって暗号化した後、前記決済端末機(126)毎に設定されている端末機識別情報(156)と共にインターネット通信回線(104)を経由して中継サーバ(108)に送信し、

前記中継サーバ(108)において、前記端末機識別情報(156)に対応して復号化鍵情報(186)が記録されている復号化鍵情報テーブル(195)を用いて受信した前記端末機識別情報(156)に基づいて前記復号化鍵情報(186)を検索し、当該検索した復号化鍵情報(186)を用いて前記受信した暗号化された認識情報(132)を復号化した後、専用回線(110)を用いて決済センターサーバ(112)に復号化された前記認識情報(132)を送信し、

前記決済センターサーバ(112)は受信した前記復号化された前記認識情報(132)に基づいてクレジット決済処理を行うことを特徴とする

クレジットカードの決済方法。

【発明の詳細な説明】

【技術分野】

【0001】

10

20

30

40

50

本発明はクレジットカードを用いたクレジット決済におけるスキミングに対する安全性を向上させたクレジット決済システム及び決済方法に関する。

特に、インターネット通信回線を経由して行うクレジットカードを用いたクレジット決済のスキミングに対する安全性を向上させた決済システム及び決済方法に関する。

また、本発明は暗号化及び復号化のための鍵情報を通信回線に載せないことによりスキミング対策を向上させたクレジットカードの決済システム及び決済方法に関する。

さらには、電気自動車用課金型充電機に適したクレジットカード決済におけるスキミング対策を向上させたクレジットカードの決済システム及び決済方法に関する。

なお、本明細書において、クレジットカードとは、一般的に用いられている、磁気カード方式、ICカード方式、バーコードカード方式等何れでもよく、また、カードの形状としては矩形の他、コイン型等何れであってもよい。

10

【0002】

本明細書において、スキミングとは、クレジットカードに書き込まれている情報(記録又は記憶されている情報)を抜き出し、全く同じ情報を持つクレジットカードを複製することであるが、本明細書においては、主にクレジットカードに書き込まれている認識情報(例えば、カード番号)が通信回線において通信される際に不正に盗みとることを意味している。

認識情報とは、クレジットカードに記録(記憶を含み、以下「記録」という)されたクレジットカードの真偽判別のための情報をいう。例えば、カード番号、暗証番号等である。

端末機識別情報とは、カードリーダを含むクレジット決済のための端末機に個別に付与された識別のための情報をいう。

20

中継サーバとは、決済端末機と決済センターサーバとの間に介在されるサーバであって、決済端末機識別情報に対応して復号化鍵情報が記録されている復号化鍵情報テーブルを有するサーバをいう。

決済センターサーバとは、クレジット決済のための与信、決済処理等のクレジット決済のための処理を行うサーバをいう。

また、番号とは、一般的には数字により構成されるが、アルファベット、ギリシャ文字、又はカタカナ等の文字のみの組み合わせ、又はアルファベット文字等と数字の組み合わせを含むものである。

最後に、生情報とは、電子計算機において処理可能な二進数の情報、又は、容易に復号化され得る暗号化された二進数の情報をいう。

30

【背景技術】

【0003】

第1の従来技術として、クレジットカードによって料金を支払う電気自動車バッテリー充電用の充電システムが知られている(例えば、特許文献1参照)。

第2の従来技術として、カードキーのみを記録させたカードを設け、カードキーと顧客固有のカード番号と暗証番号とを対応させて独立したホストコンピュータのデータベース7に記録させ、取引に際し、カードデータ読み取り装置5を介して当該カードから読み取ったカードキーと顧客が入力した暗証番号とをホストコンピュータに転送し、ホストコンピュータ側の処理でカードおよび顧客の真贋を判定し、その判定結果のみを店舗用端末に送り返してクレジット決済の実行の可否を決定することが知られている(例えば、特許文献2参照)。

40

さらに、第3の従来技術として、クレジットカード等のカードを用いて取引を行うカード取引照合システムにおいて使用されるカード取引処理端末であって、少なくともカード取引の取引データ、そのカード取引に使用されたカードの暗証番号を入力可能な入力手段と、この入力手段により入力された上記取引データ、上記暗証番号、および、固有のシステムキーに基づいて取引正当性確認コードを演算する演算手段と、この演算手段により生成された取引正当性確認コードと取引データ等のデータを送受信する接続手段と、を備えたことを特徴とするカード取引処理端末が知られている(例えば、特許文献3参照)。

【先行技術文献】

50

【特許文献】

【0004】

【特許文献1】特許第2546594号（図5、0013～0016）

【特許文献2】特開2003-271885（図1～図11、0022～0074）

【特許文献3】特開平6-150081（図1～図4、0008～0018）

【発明の概要】

【発明が解決しようとする課題】

【0005】

第1の従来技術においては、電気自動車の充電代金決済手段としてクレジットカードを用いることは記載されているが、クレジットカードによる決済時のスキミング等の不正防止手段は何ら開示されていない。

10

換言すれば、スキミング防止対策がなされていないので、カード番号、暗証番号等の決済サーバにおける個人認証に必要な情報を認識情報の送信中にスキミングされてしまう問題がある。

そこで第2の従来技術のように、クレジットカードにはカードキーのみが記録され、クレジットの決済に際し、このカードキーをクレジット会社の決済ホストコンピュータに記録されたカードキーテーブルに存在するか確認し、存在する場合に始めて決済可能とすることができる。

【0006】

第2の従来技術を用いた場合、カードキーのみによってホストコンピュータにおける認証を行うので、この際にはスキミングされた場合であっても、カードキーのみが漏れるだけであって、カード番号や暗証番号は漏れることがない。

20

しかし、認証後はカード番号及び暗証番号を通信回線に載せるため、通信時にこれらをスキミングされる恐れがある

これを防止するため、通信回線を専用回線にすることが出来るが、専用回線を用いる場合、通信料が割高になることから、更なるコスト低減が要望されている。

【0007】

コスト低減のため、インターネット通信回線を用いることができるが、スキミングの危険性が増加するため、通常は第2の従来技術に開示されるように認識情報を暗号化して送信している。しかし、暗号化した場合であっても、暗号化情報は一定の法則によって暗号化されているので、当該法則が特定された場合、容易に復号化され、カード番号等の認識情報がスキミングされてしまうという問題がある。

30

【0008】

そこで第2の従来技術においては、クレジットカードにはカードキーのみを記録し、当該カードキーと顧客固有のカード番号と暗証番号とを対応させて独立したホストコンピュータのデータベースに記録させておく。そして、取引に際し、カードデータ読取装置でクレジットカードから読み取ったカードキーと顧客が入力した暗証番号とをホストコンピュータ2に転送し、ホストコンピュータ(決済サーバ)におい当該カードキーと暗証番号に対応するカード番号とが存在する場合のみ、当該カード番号を真正として認証するものである。第2の従来技術においては、カード番号は通信回線によって通信されないので格段にスキミングに対する安全性は向上する。

40

【0009】

しかし、決済サーバは、全国又は全世界から寄せられるクレジット決済のためのカードキーと暗証番号の照合を行わねばならず、極めて大量の処理が必要となり、認証遅れにより迅速なクレジット処理ができない恐れがあり、俄に採用できない。

【0010】

第3の従来技術においては、このような決済サーバにおける処理の増大を回避するため、クレジット端末の演算手段に記録されたシステムキーを用いて暗証番号を暗号化して決済サーバに通信し、決済サーバに記録されているシステムキーを用いて復号化することが行われている。

50

換言すれば、暗号化及び復号化のシステムキーは一つであるため、スキミングによる解読の機会が増加し、暗号解読の危険性が増加するおそれがある。また、決済サーバにおいて復号化処理を行うので、決済サーバの負担が増加し、当該処理が集中した場合迅速な処理ができない問題がある。

【0011】

本発明の第1の目的は、クレジット決済に関する認識情報をスキミングされないようにしたクレジットカードの決済システム及び決済方法を提供することである。

本発明の第2の目的は、暗号化鍵情報をスキミングされないようにしてクレジット決済に関する情報を復号化されないようにしたクレジットカードの決済システム及び決済方法を提供することである。

本発明の第3の目的は、復号化鍵情報をスキミングされないようにしたクレジットカードの決済システム及び決済方法を提供することである。

本発明の第4の目的は、暗号化された情報の復号化処理を中継サーバで行うことにより、決済センターサーバでの決済処理に悪影響を及ぼさないようにしたクレジットカードの決済システム及び決済方法を提供することである。

【課題を解決するための手段】

【0012】

この目的を達成するため、本発明に係る第1の発明は以下のように構成されている。

決済端末機においてクレジットカードから読み込んだ認識情報を暗号化して決済サーバに送信し、当該決済サーバにおいて復号化し、当該復号化した認識情報に基づいて決済処理の可否を判断するようにしたクレジットカードの決済システムにおいて、前記決済端末機は、少なくともクレジットカードに記録されている前記認識情報を読込むカードリーダー、前記カードリーダーによって読込んだ前記認識情報を暗号化鍵情報記録装置に記録された暗号化鍵情報に基づいて暗号化する暗号化装置、及び、前記決済端末機に対し個別に付与された端末機識別情報を記録する端末機識別情報記録装置を有して成り、前記決済サーバは、少なくとも中継サーバと決済センターサーバを含み、前記中継サーバは、前記端末機識別情報と復号化鍵情報との復号化鍵情報テーブル記録装置、前記決済端末機から受信した端末機識別情報に対応する前記復号化鍵情報テーブル記録装置に記録された復号化鍵情報を出力する復号化鍵情報出力装置と、前記復号化鍵情報出力装置からの復号化鍵情報に基づいて前記認識情報を復号化する復号化装置を含み、前記決済センターサーバは前記復号化された前記認識情報に基づいてクレジット決済処理を行うクレジット処理装置を含んでいるクレジットカードの決済システムである。

【0013】

第2の発明は、第1の発明において、前記認識情報はクレジットカードに付与された個別の番号であることを特徴とする。

【0014】

第3の発明は、第2の発明において、前記認識情報は不揮発性ICチップに記録されていることを特徴とする。

【0015】

第4の発明は、決済端末機においてクレジットカードから読み込んだ認識情報を暗号化して決済サーバに送信し、当該決済サーバにおいて復号化し、当該復号化した認識情報に基づいて決済処理の可否を判断するようにしたクレジットカードの決済システムにおいて、クレジットカードに記録されている認識情報を決済端末機に設けられたカードリーダーによって読込み、当該読込んだ認識情報を前記決済端末機に内蔵された不揮発性記録装置に記録された暗号化鍵情報を用いて所定の暗号化方式によって暗号化した後、前記決済端末機毎に設定されている決済端末機識別情報と共にインターネット通信回線を経由して中継サーバに送信し、前記中継サーバにおいて、前記決済端末機識別情報に対応して記録されている復号化鍵情報テーブルを用いて受信した前記端末機識別情報に基づいて復号化鍵情報を検索し、当該検索した復号化鍵情報を用いて前記受信した暗号化された認識情報を復号化した後、専用回線を用いて前記決済センターサーバに復号化された前記認識情報を送

信し、前記決済センターサーバは受信した前記復号化された前記認識情報に基づいてクレジット決済処理を行うことを特徴とするクレジットカードの決済方法である。

【発明の効果】

【0016】

第1の発明において、クレジットカード利用者は、クレジットカードをカードリーダーにおいてスライドさせ、又は所定の位置に挿入する。これにより、クレジットカードに記録されている認識情報が読み込まれる。

読み込んだ認識情報は、決済端末機に内蔵された個別暗号化鍵記録装置に記録された暗号化鍵情報を用いて所定の暗号化方式にしたがって暗号化される。

暗号化された認識情報は、決済端末機(最小単位としてはカードリーダー)に対し個別に付与された決済端末機識別情報と共に中継サーバに送信される。

中継サーバは決済端末機毎に付された決済端末機識別情報に対応して復号化鍵情報が記録されている復号化鍵情報テーブルを有する。

【0017】

中継サーバにおいて、復号化鍵情報出力装置は受信した決済端末機識別情報に対応する復号化鍵情報が、復号化鍵テーブル記憶装置に記録された復号化鍵情報テーブルに存在するかを検索する。該当する決済端末機識別情報が存在しない場合、復号化鍵情報出力装置は復号化鍵情報を出力しない。したがって、受信した暗号化された認識情報は復号化されず、処理不能(エラー)として扱われる。

決済端末機識別情報が復号化鍵情報テーブルに存在する場合、復号化鍵情報出力装置は対応する復号化鍵情報を出力する。これにより、復号化装置194は当該決済端末機識別情報と共に受信した暗号化された認識情報を当該復号化鍵情報を用いて所定の復号化方式によって復号化する。

【0018】

復号化された認識情報は専用回線によって決済センターサーバに送信される。決済センターサーバは受信した認識情報に基づいてその真偽を判別し、クレジット決済が可能か否か判別し、クレジット決済可能である場合は与信情報等の決済処理がなされ、その結果が中継サーバを経由して決済端末機へ送信される。

これによって、決済端末機においてクレジット決済処理が可能になる。

なお、決済端末機から認識情報を送信する全ての場合、認識情報は決済端末機に内蔵された暗号化鍵記録装置に記録された暗号化鍵情報を用いて暗号化され、決済端末機識別情報と共に送信される。

【0019】

したがって、認識情報は生情報のまま通信回線によって送信されることはなく、また、暗号化鍵情報は決済端末機の個別に暗号鍵記録装置に記録され、及び復号化鍵情報も中継サーバの復号化鍵情報テーブルにおいて記録されて何れも通信回線によって通信されないで、スキミングされる恐れは極めて小さい。

換言すれば、認識情報はインターネット通信回線において送信されてスキミングされる恐れはあるが、暗号化されると共に暗号化鍵情報及び復号化鍵情報は通信回線には載らないので、暗号化された認識情報が復号化される恐れは極めて小さい。

【0020】

一方、決済のための端末機識別情報は暗号化されずにインターネット通信回線によって送信されるが、認識情報、暗号化鍵情報、復号化鍵情報等の情報とは何らのつながりもないので、認識情報がスキミングされる恐れは極めて小さい。

また、中継サーバは、大量の情報処理を集中して行うので、効率的に不正アクセス対策を取ることができるので、スキミング等に対する高度の対策を取ることができ、復号化鍵情報のスキミングの恐れも極めて小さい。

さらに、決済センターサーバも中継サーバと同様にスキミング等に対する高度の対策を取ることができる。

さらに、中継サーバと決済センターサーバとの間は専用回線で接続されているので、高

10

20

30

40

50

度のスキミング対策を取ることが出来る。

以上より、本決済システムは高度のスキミング対策をとることができるので、スキミングされる恐れは極めて小さい。

【0021】

第2の発明によれば、第1の発明における認識情報は、クレジットカードに付与された個別の番号である。

すなわち、個別の番号とは、カード会員を特定するための固有の番号であり、所謂カード番号ともいわれ、そのクレジットカードに関わる全てのクレジット決済処理は、原則としてこのカード番号に基づいて行われる。したがって、一つのカード番号に関する決済処理をこのカード番号によって行うことにより容易に集約できる利点がある。

そして、カード番号に加えて、さらに、暗証番号も用いることによって、本人認証の安全性を高めることができる利点がある。

【0022】

第3の発明によれば、第2の発明において、暗号化鍵情報が不揮発性ICチップに記録されていることから、当該不揮発性ICチップを製造した者のみが知りうる状態に置くことができる。したがって、当該不揮発性ICチップに記録された暗号化鍵情報の漏洩を一層防止することができるので、スキミングされる恐れは極めて小さい。

【0023】

第4の発明によれば、決済端末機での決済に際し、カードリーダーによってクレジットカードに記録された認識情報が読み込まれる。この認識情報は決済端末機に内蔵された不揮発性記録装置に記録された暗号化鍵情報を用いて所定の暗号化方式によって暗号化された後、決済端末機に個別に設定された決済端末機識別情報と共にインターネット通信回線を經由して中継サーバに送信される。

そして、中継サーバにおいて、決済端末機識別情報を基準として復号化鍵情報テーブルに記録されている復号化鍵情報を検索し、検索した復号化鍵情報によって受信した暗号化された認識情報を復号化する。

そして、復号化した認識情報が専用回線を通じて決済センターサーバに送信され、クレジット決済に必要な処理が行なわれる。

これにより、認識情報がインターネット通信回線に載せられる場合、必ず暗号化され、また、暗号化鍵情報は不揮発性記録装置に記録されているのでスキミングされることはない。さらに復号化鍵情報も中継サーバにおいて復号化鍵情報テーブルに記録されているのでスキミングされることはない。さらに、中継サーバと決済センターサーバとの間は専用回線によって生の認識情報が通信されるが、専用回線であるので安全性を高めることができる。

よって、クレジット決済処理における認識情報をスキミングされる恐れは極めて低くなる利点がある。

【図面の簡単な説明】

【0024】

【図1】図1は、本発明にかかる実施例のクレジットカード決済システムの全体概要図である。

【図2】図2は、本発明にかかる実施例のクレジットカード決済システムの決済端末機の構成概要図である。

【図3】図3は、本発明にかかる実施例のクレジットカード決済システムの中継サーバの構成概要図である。

【図4】図4は、本発明にかかる実施例のクレジットカード決済システムの中継サーバにおける復号化鍵情報テーブルの例である。

【図5】図5は、本発明にかかる実施例のクレジットカード決済システムの作用を説明するための説明図である。

【発明を実施するための形態】

【0025】

本発明の最良の形態は、決済端末機においてクレジットカードから読み込んだ認識情報を暗号化して決済サーバに送信し、当該決済サーバにおいて復号化し、当該復号化した認識情報に基づいて決済処理の可否を判断するようにしたクレジットカードの決済システムにおいて、

決済端末機は、少なくともクレジットカードに記録されている個別の番号を読み込むカードリーダー、前記カードリーダーによって読み込んだ個別番号を不揮発性ICチップに記録された暗号化鍵情報に基づいて暗号化する暗号化装置、及び、前記決済端末機に対し個別に付与された端末機識別情報を記録する端末機識別情報記録装置を有して成り、前記決済サーバは、少なくとも中継サーバと決済センターサーバを含み、前記中継サーバは、前記端末機識別情報と復号化鍵情報との復号化鍵情報テーブル記録装置、前記決済端末機から受信した端末機識別情報に対応する前記復号化鍵情報テーブル記録装置に記録された復号化鍵情報を出力する復号化鍵情報出力装置と、前記復号化鍵情報出力装置からの復号化鍵情報に基づいて前記暗号化された認識情報を復号化する復号化装置を含み、前記決済センターサーバは前記復号化された前記認識情報に基づいてクレジット決済処理を行うクレジット処理装置を含んでいるクレジットカードの決済システムである。

【実施例】

【0026】

本発明に係るクレジットカード決済システムは、大まかには、個別の店舗100-1、100-2～100-nに設置されたクレジット決済のための決済端末機102-1、102-2～102-n、インターネット通信回線104、当該インターネット通信回線104に接続された決済サーバ106を含んでいる。決済サーバ106は、中継サーバ108及び当該中継サーバ108に対し専用回線110を介して接続された決済センターサーバ112を有する。また、本実施例においては、クレジットカード114として磁気ストライプ116に認識情報132を記録させた磁気ストライプカード118が用いられる。

【0027】

まず決済端末機102-1、102-2～102-n(決済端末機を総称する場合、符号は102を用いる)を説明する。

決済端末機102-1、102-2～102-nは、各店舗100-1、100-2～100-nにおいて個別に設置され、クレジットカード114による決済をするための端末である。各店舗100-1、100-2～100-nにおいては、決済端末機102が1台のみ配置される場合もあるし、100台以上配置される場合もある。

決済端末機102-1、102-2～102-nは、図1に示すように、キャッシュレジスタ122-1～122-n(総称する場合は符号122を用いる)に一体化されたもの、クレジットカード決済端末機として個別独立に設けられたもの(図示なし)等、何れの形式のものを用いることができる。

本実施例においては、キャッシュレジスタ122-1～122-nにそれぞれ決済端末機102-1、102-2～102-nが一体化されたものが採用されている。

これら決済端末機102-1、102-2～102-nは全て同一構成である。

なおキャッシュレジスタ122-1～122-nには、それぞれ表示装置124-1、124-2・・・124-n(総称する場合は符号124を用いる)、及び領収書発行のためのプリンタ126-1、126-2・・・126-n(総称する場合は符号126を用いる)が設けられている。

【0028】

決済端末機102は、クレジットカード114の磁気ストライプ116に記録された認識情報132を読み込んで決済サーバ106によって与信等のクレジット処理を可能にする信号を受けた場合、初めてクレジット決済処理を実行する機能を有する。本決済端末機102は、前記機能と同一の機能を有すれば実施例以外のものを採用することができる。

【0029】

上記のように、決済端末機102が設置される形態は種々存在するが、その基本構成は同一であるので、図2を参照して決済端末機102の基本的構成を説明する。

決済端末機102は、大まかにはカードリーダー128、本実施例では磁気カードリーダー129及

び端末制御装置130を含んで(内蔵して)いる。

【0030】

まず磁気カードリーダー129を説明する。

磁気カードリーダー129は、磁気ストライプカード118から読みとった認識情報132を暗号化して出力する機能を有する。

換言すれば、磁気カード118の磁気ストライプ116には通常、認識情報132として個別のカード番号136が記録されているので、このカード番号136を用いる。しかし、このカード番号136に代えて異なる認識情報132、例えば、カード番号136に対し全く異なる番号を用いることができる。即ち、この認識情報132は、世界で唯一の個別情報であれば良い。

磁気カードリーダー129は、上記機能と同一の機能を有すれば実施例以外のものを用いることができる。

10

磁気カードリーダー129は、カードリーダー本体138、復調装置142、暗号化装置144及び暗号化鍵情報記録装置146を含んでいる。

【0031】

カードリーダー本体138は、磁気ストライプカード118の磁気ストライプ116から認識情報132を読みとる機能を有する。換言すれば、磁気ストライプ116における磁性体の配列を読みとって、アナログ情報を取得し、次工程へ出力する機能を有する。

本実施例において、カードリーダー本体138は、角柱状のカードリーダー本体138の一面に形成した縦長のスリット148によって、断面凹型のスライド溝152が形成されている。

スライド溝152を構成する側壁の裏面側には磁気ヘッド(図示せず)が配置され、磁気ストライプ116に記録された認識情報132、本実施例ではカード番号136を読みとる。したがって、カードリーダー本体138からは、磁気ヘッド(図示せず)によって取得したカード番号136に関するアナログ信号が出力される。

20

このカードリーダー本体138は、一般的に販売されている規格品を使用することができる。

【0032】

次に復調装置142を説明する。

復調装置142は、磁気ヘッド(図示せず)からのアナログ信号をデジタル信号に変換して出力する機能を有する。

復調装置142は、上記機能と同一の機能を有すれば、実施例以外のものを用いることができる。

30

復調装置142は、一般的に販売されている集積回路を用いることができる。

【0033】

次に暗号化装置144を説明する。

暗号化装置144は、所定の暗号化プロトコルに基づいて、復調装置142から出力されたデジタルのカード番号136を暗号化し、出力する機能を有する。暗号化装置144は、前記機能を有すれば実施例以外の装置を採用することができる。

暗号化装置144は、専用の集積回路を用いることができ、所定の暗号化プロトコルとしては、RSA暗号方式等が用いられる。

本発明においては、暗号化装置144は、暗号化鍵情報記録装置146に記録された暗号化(公開)鍵情報154に基づいて暗号化する。

40

【0034】

次に暗号化鍵情報記録装置146を説明する。

暗号化鍵情報記録装置146は、暗号化装置144において認識情報132を暗号化する際に用いる暗号化(公開)鍵情報154を記録し、出力する機能を有する。暗号化鍵情報記録装置146は、前記機能と同一の機能を有すれば実施例以外の装置を採用することができる。

暗号化鍵情報記録装置146は、暗号化鍵情報154を記録及び出力するリードオンリーメモリ(Read Only Memory)であり、不揮発性記録装置である不揮発性の半導体メモリ、例えば不揮発性ICチップ、又は半導体メモリ以外の読み出し専用媒体を用いることができる。

記録の安全性を考慮すれば記録内容が書き換え出来ない読み出し専用の装置、即ち、最

50

も好ましいのは、記録内容が変更できないマスクROMである。しかし、コスト面を考慮すれば、ワンタイム(One Time Programmable) ROMが好ましく、更なるコストダウンのためにはUV-EEPROMなどのEEPROMを用いることができる。さらにコストダウンするには、組み込んだ回路上で書き込み可能なフラッシュメモリ等のEEPROMを用いることができる。

暗号化鍵情報記録装置146に記録される暗号化鍵情報154は、決済端末機102の製造メーカーが、最も小さい単位においてはカードリーダー本体138の製造メーカーが暗号化鍵情報記録装置146に暗号化鍵情報154を記録させる。したがって、当該決済端末機102に記録されている暗号化鍵情報154は、当該製造メーカーが厳重に管理し、秘密裏に保持する。換言すれば、暗号化鍵情報154はカードリーダー本体138又は決済端末機102の製造メーカーのみが知る

10

ことができる。一方、暗号化鍵情報154に対応する復号化鍵情報186は、対応する端末機識別情報156と共に中継サーバ108の運営者に秘密裏に通知される。

【0035】

次に端末制御装置130を説明する。

端末制御装置130は、クレジット決済のための端末処理機能を有し、詳しくは、暗号化装置144から出力された暗号化された認識情報132を決済端末機102に個別に付与された端末機識別情報156と共に中継サーバ108に送信し、中継サーバ108からの信号に基づいて所定の決済端末処理を行う機能を有する。端末制御装置130は、前記機能と同一の機能を有すれば実施例以外の装置を採用することができる。

20

本実施例において、端末制御装置130は、読出制御装置158、端末マイクロプロセッサ162、端末機識別情報記録装置164、端末照会制御装置166、端末ROM168、端末RAM172、端末通信インターフェース174及びそれら間の通信の用に供する端末バスライン176を含んでいる。

端末制御装置130は専用基板による電気回路として構成することができるが、汎用性を高めるため端末マイクロプロセッサ162を用い、端末ROM168に記録されたプログラムに基づいて、端末RAM172に随時必要な情報を書き込み、読み出しつつ制御することが好ましい。

【0036】

読出制御装置158を説明する。

30

読出制御装置158は、端末マイクロプロセッサ162からの指令に基づいて、暗号化装置144から出力される暗号化された認識情報132(カード番号136)を読み込むか否か制御する機能を有する。読出制御装置158は、前記機能をと同一の機能を有すれば実施例以外の装置を採用することができる。

端末マイクロプロセッサ162からの指令により読出制御装置158が読み込んだ暗号化された認識情報132は、RAM172に一時保留される。

【0037】

次に端末機識別情報記録装置164を説明する。

端末機識別情報記録装置164は、記録した端末機識別情報156を端末マイクロプロセッサ162からの指令に基づいて端末バスライン176に出力する機能を有する。端末機識別情報記録装置164は、前記機能と同一の機能を有すれば実施例以外の装置を採用することができる。

40

端末機識別情報156は、数字の組み合わせだけでなく、アルファベット等の文字を含んでいる場合も含む概念である。例えば、ABC12345も端末機識別情報156に含まれる。

端末機識別情報記録装置164は、例えばOTP ROM、EEPROM等、書き込みは可能であるが、消去は出来ない記録装置を用いることが好ましい。

この端末機識別情報156は、決済端末機102毎に個別に付与された番号であり、世界で唯一の番号である。端末機識別情報156は、決済端末機102の工場出荷時に端末機識別情報記録装置164に書き込まれると共に、中継サーバ108における後述の復号化鍵情報テーブル182に追加されるよう処置する。例えば、当該決済端末機102が接続される中継サーバ108を

50

運営する中継サーバ業者に秘密裏に連絡され、復号化鍵情報テーブル182に秘密裏に記憶される。

【0038】

次に端末照会制御装置166を説明する。

端末照会制御装置166は、端末RAM172に一時保留された暗号化された認識情報132と、端末機識別情報記録装置164に記録された端末機識別情報156とを中継サーバ108に送信する機能を有する。

また、中継サーバ108から送信された決済情報を受け入れる機能を有する。端末照会制御装置166は、前記機能と同一の機能を有すれば、実施例と異なる装置を採用することができる。

10

【0039】

次に端末通信インターフェース174を説明する。

端末通信インターフェース174は、POS端末との通信を司る機能を有する。端末通信インターフェース174は、前記機能と同一の機能を有すれば、実施例と異なる装置を採用することができる。

【0040】

次にPOS(point of sale system)端末177を説明する。

POS端末177は、本実施例ではキャッシュレジスタ122である。

したがって、本システムではキャッシュレジスタ122からの情報もインターネット通信回線104を介して一つの管理サーバ(図示せず)に送信可能である。

20

具体的には、キャッシュレジスタ122から出力される決済金額204を出力する。

【0041】

次にインターネット通信回線104を説明する。

インターネット通信回線104は、情報を高速通信する回線であり、ADSLや光通信回線等の有線回線、又はWi-Fi等の無線通信回線である。

【0042】

次に中継サーバ108を説明する。

中継サーバ108は、中継演算装置196が中継ROM178に記録している中継サーバプログラムに基づいて中継RAM198に随時書き込みつつ所定の処理を行う。

決済端末機102からインターネット通信回線104を通じて送られてきた端末機識別情報156に基づいて復号化のための復号化鍵情報テーブル182から復号化鍵情報186を検索し、当該端末機識別情報156に対応する復号化鍵情報186が存在する場合、受信した暗号化された認識情報132を復号化し、決済センターサーバ112へ送信する機能を有する。中継サーバ108は、前記機能と同一の機能を有すれば、実施例以外の装置を採用することができる。

30

中継サーバ108は、被照会制御装置192、復号化鍵情報テーブル記録装置195、中継演算装置196、復号化鍵情報出力装置197、中継RAM198、中継ROM178、通信制御装置199及びそれらの間の通信を司る中継バスライン202を含んでいる。

【0043】

まず被照会制御装置192を説明する。

被照会制御装置192は、インターネット通信回線104を介して送信される決済端末機102からの情報を中継サーバ108に取り込んで中継バスラインに載せる機能を有する。被照会制御装置192は、前記機能と同一の機能を有すれば、実施例以外の装置を採用することができる。

40

被照会制御装置192は、集積回路や論理回路の組み合わせ、又はマイクロプロセッサとソフトウェアとにより構成できる。

【0044】

次に復号化鍵情報テーブル記録装置195を説明する。

復号化鍵情報テーブル記録装置195は、復号化のための復号化鍵情報テーブル182が記録する機能を有する。復号化鍵情報テーブル記録装置195は、前記機能と同一機能を有すれば、実施例と異なる装置を採用することができる。

50

図4に示すように、復号化鍵情報テーブル182は、端末機識別情報156に基づいて復号化鍵情報186を検索できるように構成されている。

決済端末機製造業者又はカードリーダーの製造業者によって中継サーバ108の運営業者に秘密裏に通知された端末機識別情報156及び復号化鍵情報186は、中継サーバ108の運営業者によって中継サーバ108の復号化鍵情報テーブル182に記録(記憶)される。この登録も、秘密裏に行われ、かつ、予め登録されたアクセス許可者のみがアクセス権限を与えられたシステム機器を用いて端末機識別情報156に対応する復号化鍵情報186が記録される。

【0045】

次に復号化鍵情報出力装置197を説明する。

復号化鍵情報出力装置197は、復号化鍵情報テーブル記録装置195に記録された復号化鍵情報テーブル182に、受信し端末機識別情報156に対応する復号化鍵情報186が存在するか検索し、存在する場合は当該復号化鍵情報186を出力し、存在しない場合はエラー信号を出力する機能を有する。復号化鍵情報出力装置197は、前記機能と同一の機能を有すれば、実施例以外の装置を採用することができる。

【0046】

次に復号化装置194を説明する。

復号化装置194は、復号化鍵情報出力装置197から出力された復号化鍵情報186を用いて、決済端末機102から送信された暗号化された認識情報132(カード番号136)を復号化する機能を有する。復号化装置194は、前記機能と同一の機能を有すれば、実施例以外の装置を採用することができる。

復号化された認識情報132は、専用回線110を介して決済センターサーバ112へ送られ、決済センターサーバ112における与信等のクレジット決済処理に活用する。

【0047】

次に中継演算装置196を説明する。

中継演算装置196は、中継ROM178に記録されたプログラムに基づいて中継RAM198に随時書き込み消去しつつ中継サーバ108における所定の処理を制御する機能を有する。

【0048】

次に中継RAM198を説明する。

中継RAM198は、中継演算装置196での処理に必要な情報を適時に記録する機能を有する。

【0049】

次に中継ROM178を説明する。

中継ROM178は、中継サーバ108での処理に供するプログラムが書き込まれている。

【0050】

次に通信制御装置199を説明する。

通信制御装置199は、中継サーバ108側において決済センターサーバ112との専用回線110を介した通信を制御する機能を有する。

【0051】

次に中継バスライン202を説明する。

中継バスライン202は、中継サーバ108での処理に必要な情報を伝達する機能を有する。

【0052】

次に決済センターサーバ112を説明する。

決済センターサーバ112は、日本全国又は外国に設置された複数の中継サーバ108から専用回線110を介して送られた認識情報132に基づいて与信処理、売買代金処理等の決済処理を行う機能を有する。

換言すれば、決済センターサーバ112はクレジット決済処理を実行するクレジット処理装置200を含んでいる。決済センターサーバ112、換言すればクレジット処理装置200は、例えば高速の演算処理装置によって構成される。

【0053】

10

20

30

40

50

次に、図5のフローチャートを参照しつつ本実施例の作用、換言すればクレジットカードの決済方法を説明する。

まず決済端末機102における、ステップS1においてキャッシュレジスタ122における決済金額204が確定し、クレジットカード決済が選択された場合、ステップS2へ進んで端末制御装置130は認識情報要求命令206を出力する。

認識情報要求命令206によって、カードリーダー128は磁気ストライプカード118が読込可能状態になる。

ステップS3において、作業者が磁気ストライプカード118をカードリーダー本体138のスライド溝142においてスライドさせる。

これによって、ステップS4においてカードリーダー本体138の磁気ヘッド(図示せず)によって、磁気ストライプ116に記録されている認識情報132たるカード番号136がアナログ信号として読みとられる。

【0054】

読みとられたカード番号136は、復調装置142において復調されて後、デジタル化されて暗号化装置144に出力される。

【0055】

ステップS5において、暗号化装置144は、暗号化鍵情報記録装置146に記録されている暗号化鍵情報154に基づいてカード番号136を所定の暗号化方式によって暗号化する。

【0056】

ステップS6において、端末制御装置130における読出制御装置158は所定のタイミングで暗号化装置144から出力される暗号化されたカード番号136を読み込み、及び端末機識別情報記録装置164から端末機識別情報156を読込んだ後、端末照会制御装置166が当該暗号化されたカード番号136、端末機識別情報156及び決済金額204をインターネット通信回線104を介して中継サーバ108に送信する。

【0057】

決済端末機102からの情報を受信した中継サーバ108において、ステップS7において復号化鍵情報出力装置197が受信した端末機識別情報156に基づいて復号化鍵情報186を復号化鍵情報テーブル182において検索する。

復号化鍵情報テーブル182に端末機識別情報156が登録されていない場合、及び、端末機識別情報156は存在するが復号化鍵情報186が登録されていない場合、エラー(異常)であると判断してエラー信号を出力する。このエラー信号は被照会制御装置192からインターネット通信回線104を介して該当する決済端末機102に送信される。

エラー信号を受信した決済端末機102は、POS端末177であるキャッシュレジスタ122へ送信し、キャッシュレジスタ122はその表示装置124にエラー表示をする。

復号化鍵情報テーブル182に端末機識別情報156が存在する場合、復号化鍵情報出力装置197はステップS7において端末機識別情報156に対応する復号化鍵情報186を出力する。

【0058】

次いで復号化装置194は、ステップS8において、当該端末機識別情報156と共に受信した暗号化されたカード番号136を復号化鍵情報186を用いて所定の方式で復号化する。

【0059】

次ぎにステップS9において、通信制御装置144は復号化されたカード番号136、端末機識別情報156及び決済金額204を専用回線110を経由して決済センターサーバ112へ送信する。

【0060】

専用回線110においては、カード番号136が生情報であるので、スキミングされた場合、直ぐさまカード番号136が特定されてしまう。しかし、専用回線110を用いるので、不正アクセスに対する防御態勢を十分に取れるので、スキミングの恐れは極めて小さい。

【0061】

決済センターサーバ112は、ステップS10において、送信されたカード番号136等を用いて決済処理を行い、それが終了した後、ステップS11において決済情報を中継サーバ108へ送信する。

10

20

30

40

50

【 0 0 6 2 】

決済情報を受信した中継サーバ108は、ステップS12において該当する決済端末122へ決済処理情報(例えば与信情報)を出力する。

【 0 0 6 3 】

決済処理情報を受信した決済端末機102は、POS端末177の表示装置124に決済処理が終了したことを表示すると共に、決済内容を小形のプリンタ126によって印刷する。印刷された決済内容はクレジットカードの所持者へ渡される。

【符号の説明】

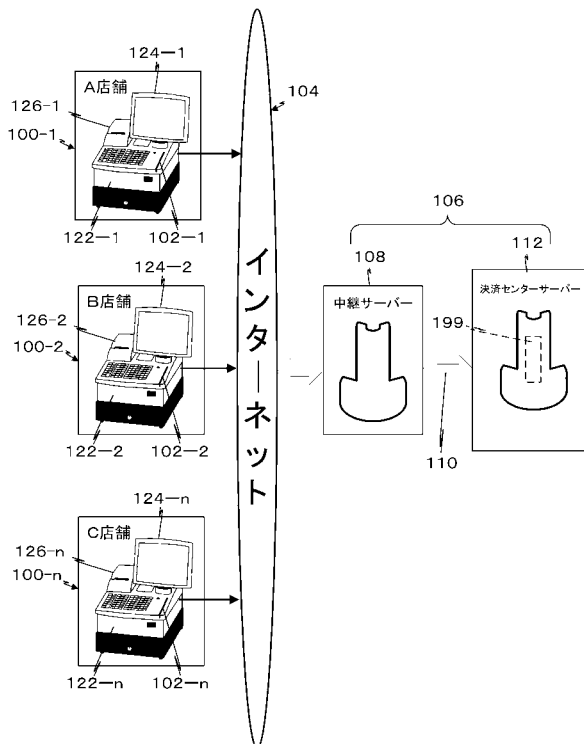
【 0 0 6 4 】

- | | |
|-----|----------------|
| 102 | 決済端末機 |
| 106 | 決済サーバ |
| 108 | 中継サーバ |
| 112 | 決済センターサーバ |
| 114 | クレジットカード |
| 128 | カードリーダー |
| 132 | 認識情報 |
| 144 | 暗号化装置 |
| 146 | 暗号化鍵情報記録装置 |
| 154 | 暗号化鍵情報 |
| 156 | 端末機識別情報 |
| 164 | 端末機識別情報記録装置 |
| 186 | 復号化鍵情報 |
| 194 | 復号化鍵情報出力装置 |
| 195 | 復号化鍵情報テーブル記録装置 |

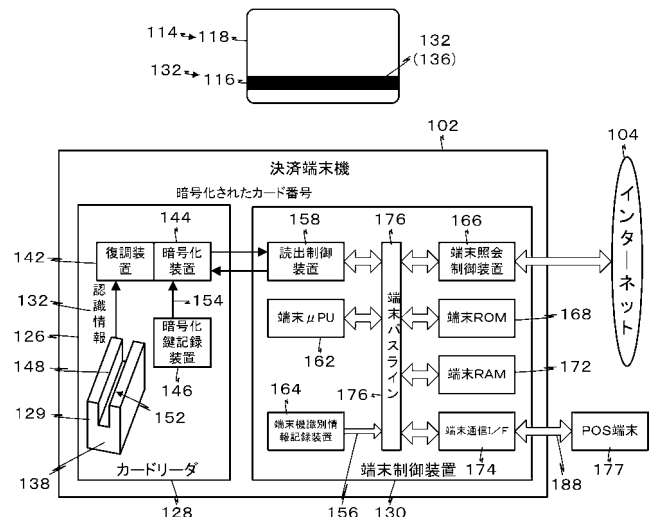
10

20

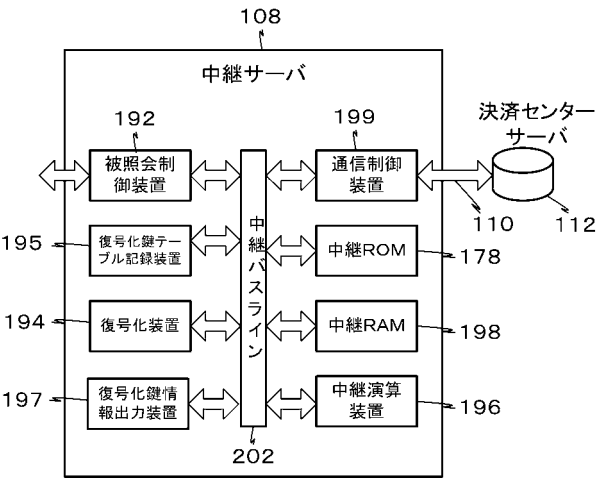
【 図 1 】



【図 2】



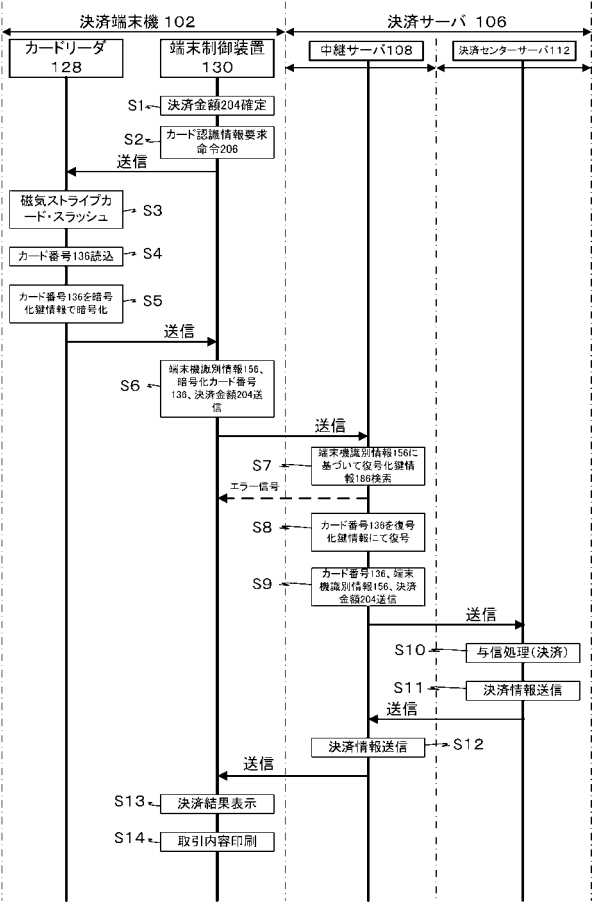
【図 3】



【図 4】

156 端末機識別情報	186 復号化鍵情報	
000001	◇◇◇◇	182
000002	□□□□	
000003	△△△△	
000004	○ ○ ○ ○	

【図 5】



フロントページの続き

(51)Int.Cl.		F I		テーマコード (参考)
G 0 6 K 17/00	(2006.01)	G 0 6 K 17/00	T	