(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2014-194792
(P2014-194792A)
(43)公開日　平成26年10月9日(2014.10.9)

(51)Int.Cl.		F I			テーマコード（参考）
G06Q 20/40	(2012.01)	G06Q	20/40	110	3E142
G06Q 20/34	(2012.01)	G06Q	20/34		5B058
G06Q 20/26	(2012.01)	G06Q	20/26		
G06K 17/00	(2006.01)	G06K	17/00	L	
G07G 1/12	(2006.01)	G06K	17/00	T	

審査請求 有　請求項の数 36　OL　（全 33 頁）　最終頁に続く

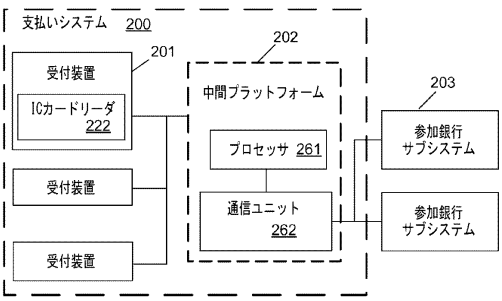
(21)出願番号　特願2014-95358(P2014-95358)
(22)出願日　平成26年5月2日(2014.5.2)
(62)分割の表示　特願2010-512326(P2010-512326)の分割
原出願日　平成20年6月11日(2008.6.11)
(31)優先権主張番号　200710112394.X
(32)優先日　平成19年6月13日(2007.6.13)
(33)優先権主張国　中国(CN)

(71)出願人　510330264
アリババ・グループ・ホールディング・リミテッド
ＡＬＩＢＡＢＡ　ＧＲＯＵＰ　ＨＯＬＤＩＮＧ　ＬＩＭＩＴＥＤ
英国領，ケイマン諸島，グランド・ケイマン，ジョージ・タウン，ワン・キャピタル・プレイス，フォース・フロア，ピー．オー．ボックス　８４７
(74)代理人　110001243
特許業務法人　谷・阿部特許事務所

最終頁に続く

(54)【発明の名称】ＩＣ識別カードを使用した支払いシステムおよび方法

(57)【要約】
【課題】支払いシステムは、ユーザを識別するためにＩＣ識別カードを利用し、ユーザの銀行口座を検索および検証する。
【解決手段】システムは、ＩＣ識別カードリーダを使用してユーザ身元情報を読み取り、それをユーザ銀行口座情報とともに、処理するように中間プラットフォームへ送信する。中間プラットフォームは、受信されたユーザ身元情報を、銀行取引要求の一部として、他の銀行取引情報とともに、処理される参加銀行サブシステムに送信する。参加銀行サブシステムは、ユーザ身元と銀行口座との間のマッピング関係に基づいて、中間プラットフォーム、または参加銀行サブシステムのいずれかによって、ユーザ識別に従って判断されるユーザの銀行口座との要求された銀行取引を実行する。ユーザ識別情報の復号化は、ＩＣ識別カードリーダによって、または中間プラットフォームにおいてのいずれかで行われる。
【選択図】図２



【特許請求の範囲】
【請求項１】
ＩＣ識別カードを使用した商取引のための支払いシステムであって、
暗号化されたユーザ身元情報をＩＣ識別カードから受信するためのＩＣ識別カードリーダを有する受付装置であって、ユーザ銀行口座情報をさらに受信して前記ユーザ銀行口座情報を暗号化するように適合される、受付装置と、
中間プラットフォームであって、
複数の銀行口座番号と複数のユーザ身元情報との間のマッピング関係を格納するデータベースを備え、
前記受付装置から送信された前記暗号化されたユーザ身元情報および前記暗号化されたユーザ銀行口座情報を受信し、
前記暗号化されたユーザ身元情報を復号化し、
前記データベースに前記ユーザ身元情報に対応する銀行口座番号が含まれる場合、
前記マッピング関係から、前記ユーザ身元情報に対応する銀行口座番号を調べ、
前記銀行口座番号および前記ユーザ銀行口座情報を含む銀行取引情報を、銀行取引を要求するように、参加銀行サブシステムに通信し、
前記データベースに前記ユーザ身元情報に対応する銀行口座番号が含まれない場合、
前記ユーザ身元情報および前記ユーザ銀行口座情報を含む銀行取引情報を、銀行取引を要求するように、参加銀行サブシステムに通信し、
前記参加銀行サブシステムに、前記ユーザ身元情報に対応する銀行口座番号を調べさせ、
前記参加銀行サブシステムから銀行取引結果を受信し、
前記銀行取引結果を前記受付装置に通信する、中間プラットフォームと
を備えるシステム。
【請求項２】
前記中間プラットフォームは、前記暗号化されたユーザ銀行口座情報を復号化するように適合される、請求項１に記載の支払いシステム。
【請求項３】
前記受付装置は、前記ユーザ銀行口座情報を受信するための前記ＩＣ識別カードリーダから分離した入力ユニットをさらに有する、請求項１に記載の支払いシステム。
【請求項４】
前記入力ユニットは、取引金額を含む販売業者取引情報をさらに受信するために使用される、請求項３に記載の支払いシステム。
【請求項５】
前記受付装置によって受信された前記ユーザ銀行口座情報は、前記ユーザによって入力された銀行口座パスワードを含む、請求項１に記載の支払いシステム。
【請求項６】
前記受付装置によって受信された前記ユーザ銀行口座情報は、前記ユーザによって選択された前記参加銀行の情報と、前記ユーザによって入力された銀行口座パスワードとを含む、請求項１に記載の支払いシステム。
【請求項７】
前記参加銀行に送信される前記ユーザ銀行口座情報は、前記参加銀行にある前記ユーザの銀行口座番号を含む、請求項１に記載の支払いシステム。
【請求項８】
前記参加銀行に送信される前記ユーザ銀行口座情報が、前記参加銀行の前記ユーザの銀行口座番号を含まない場合、前記支払いシステムは、前記参加銀行サブシステムに、前記ユーザ識別カード番号に対応する銀行口座番号を調べさせ、銀行口座パスワードを含む前記ユーザ銀行口座情報を検証させるように構成される、請求項１に記載の支払いシステム。

【請求項９】
前記受付装置は、前記参加銀行または第３者機関のいずれかによって提供された銀行暗号化キーを使用して、前記ユーザ銀行口座情報を暗号化するための暗号部を有する、請求項１に記載の支払いシステム。
【請求項１０】
前記受付装置は、前記受付装置によって受信された取引金額を暗号化するための暗号部を有する、請求項１に記載の支払いシステム。
【請求項１１】
前記受付装置は、
前記参加銀行または第３者機関のいずれかによって提供された銀行暗号化キーを使用して、前記ユーザ銀行口座情報を暗号化するために使用される第１の暗号部と、
前記受付装置によって受信される取引金額を暗号化するために使用される第２の暗号部と、をさらに含む、請求項１に記載の支払いシステム。
【請求項１２】
前記第１の暗号部および前記第２の暗号部は、前記ＩＣ識別カードリーダに接続された処理ユニットの一体部分である、請求項１１に記載の支払いシステム。
【請求項１３】
前記第１の暗号部および前記第２の暗号部のうちの少なくとも１つは、前記ＩＣ識別カードリーダの一体部分である、請求項１１に記載の支払いシステム。
【請求項１４】
前記第１および前記第２の暗号部は、それぞれソフトウェアモジュールである、請求項１１に記載の支払いシステム。
【請求項１５】
前記第１の暗号部および前記第２の暗号部のうちの少なくとも１つは、前記ＩＣ識別カードリーダから分離した暗号化ユニットである、請求項１１に記載の支払いシステム。
【請求項１６】
前記受付装置は、前記ＩＣ識別カードリーダに接続された販売業者処理ユニットを備え、前記販売業者処理ユニットは、
前記ＩＣ識別カードリーダの外部から入力された外部情報を受信するために使用される入力ユニットであって、前記外部情報は、販売業者によって入力された取引金額、前記ユーザによって入力された銀行口座パスワード、および前記ユーザによって選択された参加銀行の情報のうちの少なくとも１つを含む、入力ユニットと、
取引結果を出力するために使用される出力ユニットと、
入力ユニットによって受信された前記外部情報、および／または前記ＩＣ識別カードリーダによって受信された前記暗号化されたユーザ身元情報を処理するために使用されるプロセッサと、
処理情報を前記中間プラットフォームに通信するために使用される通信ユニットと、を含む、請求項１に記載の支払いシステム。
【請求項１７】
前記販売業者処理ユニットは、前記ＩＣ識別カードリーダとインターフェース接続するコンピューティング装置に実装され、前記出力ユニットは、表示画面を含む、請求項１６に記載の支払いシステム。
【請求項１８】
前記中間プラットフォームは、
前記銀行取引情報を前記参加銀行サブシステムに送信する前に、前記参加銀行によって合意された暗号化キーを使用して、前記銀行取引情報を暗号化し、
前記参加銀行によって合意された復号化キーを使用して、前記参加銀行サブシステムから通信された前記銀行取引結果を復号化する、ようにさらに適合される、請求項１に記載の支払いシステム。
【請求項１９】

前記受付装置は、販売業者処理ユニットと前記中間プラットフォームとの間をインターフェース接続するＡＰＩインターフェースを有する、請求項１に記載の支払いシステム。
【請求項２０】
前記受付装置は、通常の電話回線、任意のネットワークのダイヤルアップモデム、またはＬＡＮを介する接続に対応する通信ユニットを有する、請求項１に記載の支払いシステム。
【請求項２１】
ＩＣ識別カードを使用した商取引のための支払いシステムであって、
識別カードリーダおよび第１のプロセッサを有する受付装置であって、
前記識別カードリーダを介して、暗号化されたユーザ識別情報をＩＣ識別カードから受信し、
銀行口座パスワードを含むユーザ銀行口座情報を受信し、
前記第１のプロセッサを使用して、前記ユーザ銀行口座情報を暗号化し、前記暗号化されたユーザ識別情報および前記暗号化されたユーザ銀行口座情報を送信するように適合される、受付装置と、
暗号化装置と、第２のプロセッサと、複数の銀行口座番号と複数のユーザ識別情報との間のマッピング関係を格納するデータベースと、を有する中間プラットフォームであって、前記暗号化装置は、前記受付装置から送信された少なくとも前記暗号化されたユーザ識別情報を復号化するために使用され、前記中間プラットフォームは、
前記データベースに前記ユーザ識別情報に対応する銀行口座番号が含まれる場合、
前記第２のプロセッサを使用して、前記マッピング関係から、前記ユーザ識別情報に対応する銀行口座番号を調べ、
前記銀行口座番号および前記ユーザ銀行口座情報を含む銀行取引情報を、参加銀行サブシステムに通信して、銀行取引を要求し、
前記データベースに前記ユーザ識別情報に対応する銀行口座番号が含まれない場合、
前記ユーザ識別情報および前記ユーザ銀行口座情報を含む銀行取引情報を、参加銀行サブシステムに通信して、銀行取引を要求し、
前記参加銀行サブシステムに、前記ユーザ識別情報に対応する銀行口座番号を調べさせ、
前記参加銀行サブシステムから銀行取引結果を受信し、
前記銀行取引結果を、前記受付装置に通信する、ようにさらに適合される、システム。
【請求項２２】
ＩＣ識別カードを使用した商取引のための支払い方法であって、
識別カードリーダを介してユーザの暗号化されたユーザ身元情報を受信するステップであって、前記暗号化されたユーザ身元情報は、ユーザ識別カード番号を含む、ステップと、
前記ユーザによって入力された銀行口座パスワードを含む銀行口座情報を受信するステップと、
前記銀行口座情報を暗号化するステップと、
販売業者によって入力された取引金額を受信するステップと、
前記暗号化されたユーザ身元情報、前記暗号化された銀行口座情報、および前記取引金額を、中間プラットフォームに送信するステップと、
少なくとも前記中間プラットフォームによって受信された前記暗号化されたユーザ身元情報を復号化するステップと、
前記中間プラットフォームにおいて、ユーザ識別カード番号と銀行口座番号との間のマッピング関係を格納するステップと、
前記マッピング関係から前記ユーザ識別カード番号に対応する前記銀行口座番号を調べ、かつ見つかった場合、前記銀行口座番号を、銀行取引情報の一部とするステップと、
銀行取引を要求するために、前記中間プラットフォームから、前記ユーザ身元情報、前

記銀行口座パスワード、および前記取引金額を含む前記銀行取引情報を、参加銀行サブシステムに送信するステップと、
前記銀行取引情報が銀行口座番号を含む場合、前記銀行口座パスワードを検証し、前記参加銀行サブシステムで前記要求された銀行取引を処理し、銀行取引結果を前記中間プラットフォームに返送する一方で、
前記銀行取引情報が銀行口座番号を含まない場合、前記参加銀行サブシステムで、前記ユーザ身元情報に対応する前記銀行口座番号を検索し、前記銀行口座パスワードを検証し、前記要求された銀行取引を処理し、銀行取引結果を前記中間プラットフォームに返送するステップと
を含む方法。

【請求項２３】
取引暗号化キーを使用して前記取引金額を暗号化するステップと、
前記参加銀行または第３者機関のいずれかによって提供される銀行暗号化キーを使用して前記銀行口座パスワードを暗号化するステップと、をさらに含む、請求項２２に記載の支払い方法。

【請求項２４】
前記参加銀行または第３者機関のいずれかによって提供される銀行暗号化キーを使用して前記銀行口座パスワードを暗号化するステップと、
前記暗号化された銀行口座パスワードを、前記参加銀行に送信される前記銀行取引情報に含めるステップと、をさらに含む、請求項２２に記載の支払い方法。

【請求項２５】
前記参加銀行に、前記ユーザ識別カード番号に対応する複数の銀行口座番号が存在する場合、前記支払いのための特定の銀行口座番号を提供するように前記ユーザに要求する通知を送信するステップをさらに含む、請求項２２に記載の支払い方法。

【請求項２６】
ＩＣ識別カードを使用した商取引のための支払いシステムであって、
暗号化されたユーザ身元情報をＩＣ識別カードから受信するためのＩＣ識別カードリーダを有する受付装置であって、ユーザ銀行口座情報をさらに受信して前記ユーザ銀行口座情報を暗号化するように適合される受付装置と、
中間プラットフォームであって、
複数の銀行口座番号と複数のユーザ身元情報との間のマッピング関係を格納するデータベースを備え、
前記受付装置から送信された前記暗号化されたユーザ身元情報および前記暗号化されたユーザ銀行口座情報を受信し、
前記データベースに前記ユーザ身元情報に対応する銀行口座番号が含まれる場合、
前記マッピング関係から、前記ユーザ身元情報に対応する銀行口座番号を調べ、
銀行取引を要求するために、前記銀行口座番号および前記ユーザ銀行口座情報を含む銀行取引情報を、参加銀行サブシステムに通信し、
前記データベースに前記ユーザ身元情報に対応する銀行口座番号が含まれない場合、
銀行取引を要求するために、前記ユーザ身元情報および前記ユーザ銀行口座情報を含む銀行取引情報を、参加銀行サブシステムに通信し、
前記参加銀行サブシステムに、前記ユーザ身元情報に対応する銀行口座番号を調べさせ、
前記参加銀行サブシステムから銀行取引結果を受信し、
前記銀行取引結果を前記受付装置に通信する、中間プラットフォームと
を備えるシステム。

【請求項２７】
前記受付装置は、前記ユーザ銀行口座情報を受信するための前記ＩＣ識別カードリーダから分離した入力ユニットをさらに有する、請求項２６に記載の支払いシステム。

【請求項２８】
前記入力ユニットは、さらに取引金額を受信するために使用される、請求項２７に記載の支払いシステム。
【請求項２９】
前記受付装置によって受信された前記ユーザ銀行口座情報は、前記ユーザによって入力された銀行口座パスワードを含む、請求項２６に記載の支払いシステム。
【請求項３０】
前記受付装置は、前記参加銀行または第３者機関のいずれかによって提供される銀行暗号化キーを使用して、前記ユーザ銀行口座情報を暗号化するための暗号部を有する、請求項２６に記載の支払いシステム。
【請求項３１】
前記受付装置は、
前記ユーザ身元情報を復号化するために使用される、第１の暗号部と、
前記参加銀行または第３者機関のいずれかによって提供される銀行暗号化キーを使用して、前記ユーザ銀行口座情報を暗号化するために使用される第２の暗号部と、をさらに含む、請求項２６に記載の支払いシステム。
【請求項３２】
前記第１の暗号部および前記第２の暗号部のうちの少なくとも１つは、前記ＩＣ識別カードリーダの一体部分である、請求項３１に記載の支払いシステム。
【請求項３３】
前記受付装置は、前記受付装置によって受信される取引金額を暗号化するために使用される第３の暗号部をさらに含む、請求項３１に記載の支払いシステム。
【請求項３４】
前記受付装置は、前記ＩＣ識別カードリーダに接続された販売業者処理ユニットをさらに備え、前記販売業者処理ユニットは、
前記ＩＣ識別カードリーダの外部から入力された外部情報を受信するために使用される入力ユニットであって、前記外部情報は、販売業者によって入力された取引金額、前記ユーザによって入力された銀行口座パスワード、および前記ユーザによって選択された参加銀行の情報のうちの少なくとも１つを含む、入力ユニットと、
取引結果を出力するために使用される出力ユニットと、
入力ユニットによって受信された前記外部情報、および／または前記ＩＣ識別カードリーダによって受信された前記ユーザ身元情報を処理するために使用されるプロセッサと、
処理情報を前記中間プラットフォームに通信するために使用される通信ユニットと、を含む、請求項２６に記載の支払いシステム。
【請求項３５】
前記販売業者処理ユニットは、前記ＩＣ識別カードリーダとインターフェース接続するコンピューティング装置内に実装され、前記出力ユニットは表示画面を含む、請求項３４に記載の支払いシステム。
【請求項３６】
ＩＣ識別カードを使用した商取引のための支払い方法であって、
識別カードリーダを介してユーザの暗号化されたユーザ身元情報を受信するステップであって、前記暗号化されたユーザ身元情報は、ユーザ識別カード番号を含む、ステップと、
前記ユーザによって入力された銀行口座パスワードを含む銀行口座情報を受信するステップと、
前記銀行口座情報を暗号化するステップと、
販売業者によって入力された取引金額を受信するステップと、
前記暗号化されたユーザ身元情報、前記暗号化された銀行口座情報、および前記取引金額を、中間プラットフォームに送信するステップと、
前記中間プラットフォームにおいて、ユーザ識別カード番号と銀行口座番号との間のマ

ッピング関係を格納するステップと、
前記マッピング関係から前記ユーザ識別カード番号に対応する前記銀行口座番号を調べ、かつ見つかった場合、前記銀行口座番号を、銀行取引情報の一部とするステップと、
銀行取引を要求するために、前記中間プラットフォームから、前記ユーザ身元情報、前記銀行口座パスワード、および前記取引金額を含む前記銀行取引情報を、参加銀行サブシステムに送信するステップと、
前記銀行取引情報が銀行口座番号を含む場合、前記銀行口座パスワードを検証し、前記参加銀行サブシステムで前記要求された銀行取引を処理し、銀行取引結果を前記中間プラットフォームに返送する一方で、
前記銀行取引情報が銀行口座番号を含まない場合、前記参加銀行サブシステムで、前記ユーザ身元情報に対応する前記銀行口座番号を検索し、前記銀行口座パスワードを検証し、前記要求された銀行取引を処理し、銀行取引結果を前記中間プラットフォームに返送するステップと
を含む方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、データ処理技術分野に関連し、具体的には、ＩＣ識別カードを使用した商取引のための支払いシステムおよび支払い方法に関する。
【０００２】
[関連出願]
本出願は、２００７年６月１３日に出願された中国特許出願、出願番号第２００７１０１１２３９４．Ｘ号、名称「ＰＡＹＭＥＮＴ　ＳＹＳＴＥＭ　ＡＮＤ　ＭＥＴＨＯＤ　ＵＳＩＮＧ　ＩＣ　ＩＤＥＮＴＩＦＩＣＡＴＩＯＮ　ＣＡＲＤ」からの優先権を主張する。
【背景技術】
【０００３】
多額の現金を持ち歩くことは不便かつ危険であるため、多くの異なる取引の場面のために、銀行カードが広く使用されている。ますます多くの人々が、買い物に銀行カードを使用するようになっている。図１は、取引を処理するために銀行カードを使用する既存の支払いシステムの略ブロック図を示す。この既存のシステムには、銀行カード情報を読み取る受信端末１１３、販売業者サブシステム１１２、および取得サブシステム１１１が存在する。販売業者サブシステム１１２は、通常、サーバおよびいくつかの顧客端末（図示せず）を有する。販売業者サブシステム１１２における顧客端末は、受信端末１１３に接続するが、販売業者サブシステム１１２のサーバは、特別な専用ラインを介して取得者の取得サブシステム１１１に接続する。取得サブシステム１１１の取得者と参加銀行とが同一でない場合、提携銀行（中国のＵｎｉｏｎＰａｙ等）の銀行間取引サブシステムを介して、取得サブシステム１１１から参加銀行の取得サブシステム（図示せず）にさらに接続される。
【０００４】
ユーザが、図１の支払いを使用して支払いを行うために銀行カードを使用する場合、受信端末１１３（例えば、キャッシュレジスタ）は、まず、銀行カードの可読性に基づいて、銀行カードの信頼性について検証する。その後、販売業者サブシステム１１２の顧客端末は、身元情報（ユーザの身元を提示するためにユーザによって入力されている）、銀行カード番号、および他の販売業者取引情報を、販売業者サブシステム１１２のサーバに伝送する。続いて、販売業者サブシステム１１２のサーバは、取得サブシステム１１１に情報を送信する。取得者および参加銀行が同じ場合、取得サブシステム１１１は、取引を直接処理する。これが同じでなければ、本情報は、銀行間取引サブシステムを介して参加銀行に送信される。参加銀行サブシステムは、銀行カード情報および身元情報を使用して、ユーザの身元を検証する。身元が認証された場合、参加銀行サブシステムは、カード番号の口座からの引き落としを処理し、この引き落としに関する銀行取引結果を返送する。検

証に失敗した場合、参加銀行サブシステムは、身元が検証不可能であることを示すメッセージを返送する。引き落としが成功したというメッセージを、販売業者サブシステム１１２が受信した後、販売業者は、認証のために、販売伝票に顧客（ユーザ）の署名を取ることができる。

【０００５】

上記説明は、既存の技術において最も一般的な支払い取引プロセスを示す。しかしながら、本支払いプロセスは、後述のような特定の欠点を有する。

【０００６】

図１の支払いプロセスにおいて、口座名義およびパスワードの組み合わせとともに銀行カードを使用して、取引全体におけるユーザの身元を認証する。既存の技術における店舗販売時点情報管理（ＰＯＳ）および現金自動預け払い機（ＡＴＭ）等の端末による、銀行カードの認証の方法は、非常に高い危険性をもたらしている。現在の銀行カードは、磁気帯カード技術を使用して作製されている。磁気帯カードの偽造防止能力は低いため、これらのカードは、容易に模造または偽造される可能性がある。

【０００７】

結果として、近年、銀行カードの新世代として、磁気帯カードに取って替わるスマートカードが提案されている。チップカード、集積回路（ＩＣ）カード、または単にＩＣカードとも呼ばれるスマートカードは、情報を処理可能である集積回路を内蔵するポケットサイズのカードである。スマートカードは、入力を受信し、その入力を処理し、それを出力として配信することができる。カードは、一般的にはＰＶＣであるが、場合によりＡＢＳである、プラスチックから作製される。カードは、偽造を阻止するためにホログラムを内蔵し得る。例えば、スマートカードを作製するために、ＥＭＶ技術を使用することができる。ＥＭＶは、ユーロペイ、マスター、およびビザ等の国際銀行カード組織によって共同して開発されたスマートＩＣ銀行カード技術の規格である。本規格は、スタンドアロン型動作、暗号化機能および復号化機能、ならびにストレージ能力を有する銀行カードのＣＰＵチップを必要とし、これによって、より高レベルの安全性を達成する。

【０００８】

しかしながら、磁気帯カードからスマートカードへの銀行カードの移行には、多額の費用がかかり、かつ時間がかかることが判明している。スマートカードの製造費用は、磁気帯カードの製造費用よりも何倍も高い。加えて、スマートカードを読み取り可能にするように既存のＰＯＳおよびＡＴＭを改造するには、多額の費用がかかる。費用とリソースが莫大であるにもかかわらず、磁気帯カードからスマートカードへ銀行カードを移行したとしても、侵入者は、大きな利益が存在することから、依然としてスマートカードを偽造しようとし得る。さらに、ＡＴＭおよびＰＯＳ等の端末が、銀行カードを読み取り、銀行カードの信頼性を検証することが可能であっても、該銀行カードが、金融機関によってユーザに対して発行された同一の銀行カードであるか否か、または正当なユーザが、金融機関により発行されたスマートカードを使用しているか否かを確認することは不可能である。ユーザの身元を検証する他の実用的な方式が存在しないため、侵入者がパスワード等のユーザ情報を入手した場合、ユーザおよび販売業者にとって重大な金銭的損失がもたらされ得る。既存の技術において、ＡＴＭおよびＰＯＳが、ユーザが入力した銀行口座パスワードを受信し、銀行カードの銀行口座情報を読み取ると、通常、ネットワーク上を伝送される前に銀行口座パスワードのみが暗号化される。銀行口座番号および取引金額等の重要な金融情報は、プレーンテキスト形式で送信される。侵入者が非合法的手段によって銀行口座パスワードを入手した場合、銀行口座番号等の金融情報を入手することが非常に容易になり、潜在的に、実際のユーザに対する金銭的損失がもたらされ、また、銀行取引の安全性が大幅に低下する。

【０００９】

別の観点から考えると、磁気帯カードからスマートカードへの銀行カードの移行は、短期間で終わるものではない。したがって、取引の安全性を保証するために、支払いプロセスにおいてユーザの身元を検証する別の実用的な方法が必要とされる。

【発明の概要】
【００１０】
本開示は、取引を処理するために銀行カードを使用する既存の技術における低安全性に関する問題を解決するために、ＩＣ識別カードを使用して商取引するための支払いシステムおよび支払い方法を提供する。
【００１１】
支払いシステムは、ユーザを識別するために、ＩＣ識別カードを利用し、ユーザの銀行口座を検索および検証する。該システムは、ＩＣ識別カードリーダを使用してユーザ身元情報を読み取り、それをユーザ銀行口座情報とともに、中間プラットフォームに送信し、処理する。中間プラットフォームは、受信したユーザ身元情報を、他の銀行取引情報とともに、銀行取引要求の一部として、参加銀行サブシステムに送信し、処理する。参加銀行サブシステムは、ユーザ身元と銀行口座との間のマッピング関係に基づき、中間プラットフォーム、または参加銀行サブシステムのいずれかにより、ユーザ識別に従って判断されるユーザ銀行口座との要求された銀行取引を実行する。ユーザ識別情報の復号化は、ＩＣ識別カードリーダによって、または中間プラットフォームにおいて行われる。
【００１２】
中間プラットフォームは、ユーザ身元情報と銀行口座との間のマッピング関係に基づいて、ユーザ銀行口座番号を入手し、参加銀行サブシステムに送信される銀行取引情報内にユーザ銀行口座番号を含み得る。銀行取引情報が銀行口座番号を含まない場合、参加銀行サブシステムは、ユーザ識別カード番号に対応する銀行口座番号を調べることができ、復号化後に銀行口座パスワードを検証し、取引を処理し、銀行取引結果を返送する。
【００１３】
一部の実施形態において、入力ユニットは、銀行口座パスワード等のユーザ銀行口座情報を受信するために使用される。入力ユニットはまた、取引金額等の販売業者取引情報を受信するために使用され得る。
【００１４】
安全性を強化するために、種々の暗号化スキームを使用することができる。ＩＣ識別カードは、印刷された写真等の暗号化されていないユーザ識別情報に加え、ユーザ識別カード番号等の暗号化されたユーザ識別情報を含み得る。復号化システムは、暗号化されたユーザ識別情報を復号化することによって、ＩＣ識別カードの信頼性を検証するために使用される。ある実施形態において、ユーザ識別情報の復号化は、中間プラットフォームで行われる。代替の実施形態において、ユーザ識別情報の復号化は、ＩＣ識別カードリーダによって行われる。
【００１５】
一実施形態において、支払いシステムの受付装置は、参加銀行または第３者機関のいずれかによって提供される銀行暗号化キーを使用して、ユーザ銀行口座情報（ユーザ銀行口座パスワード等）を暗号化するために使用される暗号部を有する。別の暗号部も、取引金額を暗号化するために任意で使用される場合がある。中間プラットフォームにおいて、ユーザ識別情報および取引金額は、一致する復号化キーによって復号化される。暗号化されたユーザ銀行口座パスワードは、復号化および検証されるために、中間プラットフォームによって、参加銀行サブシステムに送られ得る。代替的に、ユーザ銀行口座パスワードは、中間プラットフォームによって復号化され、その後、参加銀行サブシステムに送信され得る。さらに、中間プラットフォームは、参加銀行サブシステムに送信して復号化、検証、および適用される前に、銀行取引情報もまた暗号化し得る。
【００１６】
支払い取引のためのＩＣ識別カードを使用した、開示される支払いシステムおよび支払い方法は、ＩＣ識別カード（一部の国における第２世代識別カード）の高品質暗号化、高安全性、および広範囲な使用から、費用の削減および安全性の強化の利益を受ける。
【００１７】
この発明の概要は、下記の発明を実施するための形態においてさらに説明される選択さ

れた概念を、簡略な形式で紹介するために提供される。この発明の概要は、請求される主題の重要な特徴または本質的な特徴を識別することを意図せず、また、請求される主題の範囲を判断するための補助として使用されることを意図しない。

【図面の簡単な説明】

【００１８】

発明を実施するための形態について、付随の図面を参照して説明する。図面において、参照番号の一番左の桁は、参照番号が最初に出現する図面を識別する。異なる図面における同一の参照番号は、類似項目または同一項目を示す。

【図１】取引を処理するために銀行カードを使用する既存の支払いシステムの略ブロック図を示す図である。

【図２】本開示に従うＩＣ識別カードを使用する例示的な支払いシステムの略ブロック図である。

【図２Ａ】図２の例示的な支払いシステムのＩ型の実現形態の略ブロック図である。

【図２Ｂ】図２の例示的な支払いシステムのＩＩ型の実現形態の略ブロック図である。

【図３Ａ】本開示に従う受付装置の一例を示す図である。

【図３Ｂ】本開示に従う受付装置の一例を示す図である。

【図３Ｃ】本開示に従う受付装置の一例を示す図である。

【図３Ｄ】本開示に従う受付装置の一例を示す図である。

【図３Ｅ】本開示に従う受付装置の一例を示す図である。

【図４】本開示に従う例示的な受付装置の略図である。

【図５】ＩＣカードリーダとインターフェース接続するコンピュータを使用する例示的な受付装置の略ブロック図を示す図である。

【図６】分離した暗号化ユニットを有する例示的な受付装置の略ブロック図である。

【図７】本支払いシステムの中間プラットフォームの更なる詳細を示す図である。

【図８】ＩＣ識別カードを使用した支払い方法の例示的なプロセスのフローチャートである。

【図９】中間プラットフォームとしてＡｌｉｐａｙ支払いプラットフォームを使用する支払い方法の例示的なプロセスを示す図である。

【発明を実施するための形態】

【００１９】

支払いシステムおよび支払い方法は、支払い取引を処理するために一部の国（例えば、中国）において使用される第２世代識別カード等の、ＩＣ識別カード（識別として使用されるＩＣチップまたはＩＣカードを有する識別カード）を使用する。開示される支払いシステムおよび支払い方法は、ＩＣ識別カードの特徴（高品質暗号化および広範な使用等）を利用する。このＩＣ識別カードは、一部の国および地域において既に広く使用されており、また、急速にさらに多くの国および地域で使用されるようになりつつある。ＩＣ識別カードがスマート銀行カードより優れている利点の１つは、前者のカードが、既に広範囲で使用されている場合があり、使用されていない場合でも、商取引のためにそのカードを商業的に何らかの使用をするか否かにかかわらず、一部の国ではすぐに使用されるであろうことである。ＩＣ識別カードは、政府によって実施されるため、人々に対する普及率が高く、また、ハードウェアおよびソフトウェアの両方の実施における統一規格の達成に対する障害が少ない傾向にある。対照的に、スマート銀行カードは、しばしば、既存のＩＣ識別カードに加えて、各々の発行元の金融機関毎に金融機関の顧客に対して製造および発行される。複数の銀行の顧客であるユーザのためには、複数のスマート銀行カードの作製が必要であり得る。銀行が相互に協力しない場合、スマート銀行カードの多様性が生じるだけでなく、異なるスマート銀行カードに使用する異なる規格および技術が存在するようになる。

【００２０】

以下に説明するように、開示される支払いシステムおよび支払い方法は、スマート銀行カードの作製に高い費用をかけずに、また、スマート銀行カード用の受付機の別々のネッ

トワークを確立せずに、スマート銀行カードと少なくとも同じ安全性を有する支払い手順を確立する。一部の実施形態において、取引プロセス全体において暗号化キーを使用することによって、安全性をさらに強化することができる。開示される支払いシステムおよび支払い方法は、さらに便宜を図るため、既存の銀行カード（従来の磁気帯カード等）の使用と組み合わせ得る。

【００２１】

第１世代識別カードと比べると、第２世代識別カードの偽造防止機能は改善されている。例示的な第２世代識別カードの１つは、９つの層から構成されている。２つの最外層は、層上に印刷される個人の身元情報を記録する。平衡層と呼ばれる別の層が存在し、静電気から保護するために使用される。平衡層上に、しばしばホログラフィックであることが可能である画像および／またはロゴを有する偽造防止膜が存在する。例えば、中国で使用される第２世代識別カードは、万里の長城の画像と、「中国」（漢字）のロゴを有する。この偽造防止膜は、オレンジ色および緑色の偽造防止マークから成り、比較的高度な技術により開発される。この平衡層は、長さが８ミリメートル、幅が５ミリメートル、および厚さが０．４ミリメートルのＩＣチップを有する。また、平衡層は、コイルである２つのアンテナを有する。平衡層を使用して、個人情報漏洩を回避するとともに、指定のカードリーダによる個人情報の読み取りが可能になる。

【００２２】

安全性機能の観点から考えると、新世代ＩＣ識別カードは、２つの偽造防止策を有する。１つは、個人情報をデジタル暗号化した後に、チップに書き込むデジタル偽造防止策である。この部分で使用される偽造防止デジタル暗号化は、概して、認定者によって適切かつ合法的に情報が暗号化されない限り、認定ＩＣカードリーダがチップ内の情報を認識しないようにするために、政府機関によって開発および／または認可される。例えば、中国で使用される第２世代識別カードの偽造防止技術は、国家の安全性を考慮して開発され、非常に高い安全性特徴を有する。一例において、各地理的領域（例えば、州）は、地理的領域のパスワードを有し、各住民が個別のパスワードを有する。

【００２３】

新世代ＩＣ識別カードに使用される別の偽造防止策は、偽装防止印刷技術である。ＩＣ識別カードの両側は、再現が困難である印刷パターンを有することが可能である。この偽装防止印刷技術は、ホログラムを含む多くの異なる策を使用することができる。

【００２４】

デジタル偽造防止策および偽装防止印刷策の採用により、ＩＣ識別カードの安全性は、大幅に高められる。加えて、全国で使用される個人識別カードは、国家の安全性に関する重要な問題に触れることから、対応するカードリーダも、政府による厳重な安全性制御下にあるため、さらに安全性が高まる。例えば、中国において、次世代の国家個人識別カードの安全性を改善するために、カードリーダは、中国公安部のみによって開発され、政府指定の契約第３者機関のみにしか提供されず、カードリーダが危険にさらされる可能性はほとんど無い。

【００２５】

一部の国および地域における第２世代識別カードの出現とともに、ＩＣ識別カードを読み取り可能なカードリーダが、ますます入手可能になってきている。

【００２６】

図２は、本開示に従うＩＣ識別カードを使用する例示的な支払いシステムの略ブロック図である。支払いシステム２００は、いくつかの受付装置２０１および中間プラットフォーム２０２を含む。支払いシステム２００は、参加銀行サブシステム２０３と通信して、支払いを行うための銀行取引を実行する。各受付装置２０１は、販売業者が、参加銀行の銀行口座を有する顧客（ユーザ）と商取引することを表し得る。

【００２７】

受付装置２０１は、ユーザ身元情報、ユーザ銀行口座情報を受信するように適合される。ユーザ身元情報は、ユーザのＩＣ識別カードからＩＣ識別カードリーダ２２２によって

読み取られるユーザ識別カード番号を含むが、肉眼、またはＩＣ識別カードからＩＣ識別カードリーダ２２２のいずれかによって読み取られるか、または他の手段によって入力され得る他のユーザ識別情報（例えば、カード所有者の印刷された写真またはデジタル写真）を含み得る。非常に基本的な形態において、ＩＣ識別カードは、販売業者によるカード所有者の視覚的な検証に使用することができる、カード所有者の印刷された写真を有し得る。好ましい実施形態において、ＩＣ識別カードに格納されたユーザ識別情報の少なくとも一部が暗号化される。ユーザ識別情報の暗号化により、視覚的な検証に加え、またはその代わりに、ＩＣ識別カードの信頼性のより安全な検証を提供する。

【００２８】

中間プラットフォーム２０２は、プラットフォームプロセッサ２６１および通信ユニット２６２を含む。中間プラットフォーム２０２は、受付装置２０１から送信されたユーザ身元情報およびユーザ銀行口座情報を受信する。中間プラットフォーム２０２は、ユーザ身元情報およびユーザ銀行口座情報を含む銀行取引情報を、参加銀行システム２０３と通信して、銀行取引を要求する。その後、中間プラットフォーム２０２は、参加銀行システム２０３から銀行取引結果を受信し、さらに、支払いを完了するために、銀行取引結果を受付装置２０１に通信する。

【００２９】

中間プラットフォーム２０２は、受付装置２０１と参加銀行サブシステム２０３との通信の間に介在する。受付装置２０１は、銀行に直接接続する必要はなく、代わりに、中間プラットフォーム２０２を介して銀行と通信する。

【００３０】

以下に示すとおり、暗号化されたユーザ識別情報の復号化様態に応じて、２つの異なる型の実現形態が存在し得る。

【００３１】

図２Ａおよび２Ｂは、図２の例示的な支払いシステム２００のＩ型およびＩＩ型の実現形態の略ブロック図である。図２Ａの支払いシステム２００Ａは、Ｉ型の実現形態であり、図２Ｂの支払いシステム２００Ｂは、ＩＩ型の実現形態である。図２Ａに示されるＩ型の実現形態において、ユーザ識別情報の復号化は、復号化チップ２２４を有するそれぞれのＩＣ識別カードリーダ２２２を使用する各受付装置２０１Ａにて行われる。中間プラットフォーム２０２Ａが、ユーザ識別情報を復号化する復号化装置を有することは必要ではない（ユーザ識別情報が、中間プラットフォーム２０２Ａに送信される前に、受付装置２０１Ａにおいて再び暗号化されない限り）。ＩＩ型の実現形態において、ユーザ識別情報の復号化は、その内部の復号化チップアセンブリ２７０を使用する中間プラットフォーム２０２Ｂにおいて行われる。受付装置２０１Ｂは、復号化するように単に暗号化されたユーザ識別情報を中間プラットフォーム２０２Ｂに送り、したがって、ユーザ識別情報を復号化するための復号化装置を有する必要はない。

【００３２】

Ｉ型の実現形態の１つの利点は、ＩＣ識別カード内のユーザ識別情報を復号化する能力を有するＩＣ識別カードリーダが、すでに一部の国（例えば、中国）において商業的に利用可能であり、本明細書に説明する支払いシステムを実施する上での障壁がより低いということである。しかしながら、Ｉ型の実現形態は、各支払い受付ユニット（販売業者の場所における）の復号化モジュール（例えば、復号化チップ２２４）を必要とするローカル復号化の使用により、より高い費用という不利点を有し得る。ローカル復号化により、各支払い受付ユニットに組み込まれる復号化機器が、十分な使用量を有しない可能性がある。さらに、ローカル復号化により、販売業者によるカード所有者の安全な検証を提供し得るが、別の人物の識別情報を使用して支払いシステムを使用して詐欺を働く可能性がある販売業者によって悪用される可能性がある。

【００３３】

対照的に、ＩＩ型の実現形態は、多くの支払い受付ユニット（販売業者）との取引を実行する中間プラットフォーム（２０２Ｂ）において実施される復号化モジュール（２６３

）による集中復号化を用いる。複数の平行復号化モジュール（チップ）を、効率的かつ高速な復号化のために、中間プラットフォームにおいて一緒に使用することができる。さらに、ＩＩ型の実現形態において、販売業者は、ＩＣ識別カード上の識別情報の復号化のための技術および機器へのアクセスを有していないので、販売業者が暗号化されたユーザ識別情報を偽造することによって、支払いシステムを悪用することが困難であり、したがって、支払いシステムをより安全なものにする。しかしながら、ＩＩ型の実現形態は、中間プラットフォームにおける復号化のための商業的に利用可能な既製の解決策が存在しない可能性があるので、第１の型よりも高い技術面での障壁に直面する可能性がある。代わりに、支払いシステムの所有者は、まず政府の承認機関と協働して、復号化モジュールおよび中間プラットフォームを実現する許可を受け、その後、ＩＣ識別カードから読み取られる識別情報を復号化する能力を有するこのような中間プラットフォームを開発する必要がある可能性がある。

【００３４】

一実施形態において、Ｉ型およびＩＩ型の両方の組み合わせは、受付装置および中間プラットフォームの両方が、ユーザ識別情報を復号化および／または暗号化する能力を有する場合に使用され得る。例えば、ユーザ認証情報は、ＩＣ識別カードの暗号化アルゴリズムに一致する第１の復号化アルゴリズムを使用して復号化され得る。復号化された識別情報は、ＩＣ識別カードの信頼性を検証するために、受付装置において販売業者によって使用され得る。その後、復号化された識別情報は、安全なデータ伝送のために、中間プラットフォームへ送信される前に、第２の暗号化アルゴリズムを使用して再び暗号化され得る。第２の暗号化アルゴリズムは、第１の暗号化アルゴリズムと同一であってもなくてもよい。特に、第２の暗号化アルゴリズムは、中間プラットフォームの所有者によって決定され、販売業者によって同意され得、ＩＣ識別カードに使用される元の暗号化アルゴリズムに一致するための、ＩＣカード元（通常は政府機関）によって課される基準および要件を満たす必要はない。

【００３５】

受付装置

以下では、Ｉ型の実現形態およびＩＩ型の実現形態の両方を、図３～６を参照しながら例示的な実施形態を用いて説明する。

【００３６】

図３Ａ、３Ｂ、３Ｃ、３Ｄおよび３Ｅは、本開示に従う受付装置のいくつかの異なる構成を示す。図３Ａ、３Ｂ、３Ｃ、３Ｄおよび３Ｅの受付装置３０１Ａ、３０１Ｂ、３０１Ｃ、３０１Ｄおよび３０１Ｅは、図２、２Ａおよび２Ｂの受付装置２０１のうちの１つを、図３Ａ、３Ｂ、３Ｃ、３Ｄまたは３Ｅのそれぞれの受付装置３０１Ａ、３０１Ｂ、３０１Ｃ、３０１Ｄまたは３０１Ｅに置き換えられることを、図２、２Ａおよび２Ｂの支払いシステム２００を参照しながら理解されたい。

【００３７】

Ｉ型の実現形態において、受付装置（図３Ａ、３Ｂおよび３Ｃの３０１Ａ、３０１Ｂおよび３０１Ｃ等）は、ＩＣ識別カードから読み取られた身元情報を復号化するのに好適な復号化装置の第１の暗号部３７１を有する。この場合、復号化結果（例えば、復号化が成功したかどうか）は、ＩＣ識別カードの信頼性を検証するために、受付装置によって使用される。復号化された識別情報は、さらなる行為のために中間プラットフォームに送信され得る。中間プラットフォームの構成および要件に依存して、ユーザ識別情報は、中間プラットフォームに送信される前に再び暗号化され得る。

【００３８】

ＩＩ型の実現形態において、受付装置（図３Ｄおよび３Ｅの３０１Ｄおよび３０１Ｅ等）は、ＩＣ識別カードに読み取られた身元情報を復号化するための暗号部を有しない。この場合、暗号化された身元情報は、中間プラットフォーム２０２Ｂに送られ、復号化チップアセンブリ２６３によって復号化される。

【００３９】

図３Ａは、本開示に従う受付装置の第１の例示的な構成の略ブロック図を示す。受付装置３０１Ａは、識別カードリーダ３１０Ａと、受付部プロセッサ３２１、通信ユニット３２５、入力ユニット３２３、および出力ユニット３２４を含む販売業者処理ユニット３２０Ａと、を有する。

【００４０】

識別カードリーダ３１０Ａを使用して、ユーザのＩＣ識別カードのユーザ身元情報を読み取る。例示的な種類のユーザ識別情報は、ユーザ識別カード番号である。一部のＩＣ識別カードは、ユーザ身元情報にカード所有者（ユーザ）の印刷された写真またはデジタル写真も含み得る。ユーザ識別カード番号、カード所有者の個人情報（名前、生年月日等）、およびデジタル写真等のデジタルユーザ身元情報は、指定された暗号化技術を用いて暗号化され得る。一部の実施形態において、識別カードリーダ３１０Ａは、ユーザのＩＣ識別カードを読み取ることに加え、ユーザの銀行口座情報を取り込むために、従来の銀行カードを読み取る能力も組み込み得る。

【００４１】

入力ユニット３２３は、取引金額等の販売業者取引情報をさらに受信するために使用される。さらなる情報をユーザから受信するために、入力ユニット３２３も使用することができる。例えば、従来の銀行カードに関連する銀行口座情報を入力するために、入力ユニット３２３を使用することができる。

【００４２】

また、ユーザは、構成に応じて、入力ユニット３２３またはＩＣカードリーダ３１０Ａのいずれかを介して、銀行口座パスワードを入力することができる。ＩＣカードリーダ３１０Ａがユーザ入力部と一体型でない場合、銀行口座パスワード等のかかる情報を入力するために、別々の入力ユニット３２３を使用することができる。また、支払いのためにユーザによって選択された参加銀行の情報を受信するために、入力部３２３を使用することができる。

【００４３】

識別カードリーダ３１０Ａは、ＩＣ識別カードのユーザ身元情報を読み取る。図３Ａの識別カードリーダ３１０Ａは、アンテナ３１１、ＲＦモジュール３１２、および制御器３１３を有する。アンテナ３１１は、ＲＦモジュール３１２に接続し、一方、ＲＦモジュール３１２は、制御器３１３に接続する。アンテナ３１１およびＲＦモジュール３１２は、主に、識別カードにおける身元情報を受信するために使用される。動作中、ＲＦモジュールは、固定周波数で電磁励起信号を連続的に送信する。ＩＣ識別カードが識別カードリーダ３１０Ａに近接して配置される場合、識別カード内のコイルは、電磁励起信号の効果により弱電流を生成する。この弱電流は、識別カード内のＩＣチップの電源としての役割を果たす。

【００４４】

ＩＣ識別カードはまた、ＲＦ周波数を介する代わりに、直接接触を介して、好適なＩＣカードリーダによって読み取ることもできることを理解されたい。加えて、ＲＦ周波数を使用する実装であっても、ＩＣ識別カードを励起するために必要なカードのスロットへの挿入の際に、励起領域は非常に低く維持し得る。

【００４５】

識別カードのＩＣチップは、暗号化された形のユーザ身元情報を有する。電磁励起信号の効果により、識別カードのチップは、ＩＣチップに格納された暗号化されたユーザ身元情報を、識別カードリーダ３１０Ａに送信することができる。識別カードリーダ３１０Ａのアンテナ３１１およびＲＦモジュール３１２によって、暗号化されたユーザ身元情報を受信した後、ユーザ身元情報は制御器３１３によって取得され得、次いで中間プラットフォーム２０２に送信することができる。

【００４６】

一実施形態において、ＩＣ識別カードリーダ３１０Ａは、好適な暗号化技術およびカード暗号化キーを使用してユーザ身元情報を復号化するために使用される、第１の暗号部３

７１を有する。販売業者処理ユニット３２０Ａは、第２の暗号部３７２および第３の暗号部３７３を有する。第２の暗号部３７２は、銀行暗号化キーを使用して銀行口座パスワードを暗号化するために使用される。第３の暗号部３７３は、取引暗号化キーを使用して取引金額を暗号化するために使用され、これは、一実施形態において、第１の暗号部３７１によって使用されるカード暗号化キーと同一であることが可能である。

【００４７】

暗号化された銀行口座パスワードは、中間プラットフォーム２０２を介して参加銀行サブシステム２０３に送信され、中間プラットフォーム２０２は、まず、検証のために、銀行口座パスワードを復号化してもよく、または復号化しなくてもよく、次いで、参加銀行サブシステム２０３に送信する前に、銀行口座パスワードを暗号化してもよく、または暗号化しなくてもよい。一般に、暗号化された銀行口座パスワードが、参加銀行サブシステム２０３によって復号化および検証される場合、受付装置２０１（例えば、図３Ａにおける３０１Ａ）と中間プラットフォーム２０２との間において安全な伝送を確実にする何らかの理由がない限り、中間プラットフォーム２０２による銀行口座パスワードの復号化および暗号化の追加の層は、不必要であり得る。

【００４８】

身元情報の復号化に使用されるカード暗号化キーは、ＩＣカード発行元（通常は政府機関）と、Ｉ型の実現形態におけるＩＤカードリーダの製造者またはＩＩ型の実現形態における中間プラットフォームの所有者との間で合意される。

【００４９】

銀行口座パスワードを暗号化するために第２の暗号部３７２によって使用される銀行暗号化キーは、参加銀行によって提供されるか、または第３者機関によって提供されるかのいずれかであり得る。第３者機関の銀行暗号化キーを使用する場合、第３者機関は、対応する復号化キーも契約参加銀行に送信する。発行銀行が中間プラットフォームを介して受付装置から受信した暗号化された情報を復号化するために、適切な一致が提供される限り、異なる銀行が同一または異なる暗号化キーを使用することができる。

【００５０】

このような暗号化キーおよび復号化キーを提供するために、中間プラットフォーム２０２が、販売業者と銀行との間の第３者機関としての役割を果たし得ることを理解されたい。各参加銀行の銀行復号化キーは、各参加銀行が、銀行口座パスワードを復号化するために、受信した銀行復号化キーを使用することができる限り、異なるまたは同一であることが可能である。

【００５１】

取引暗号化キーは、中間プラットフォーム２０２と、受付装置３０１Ａ（図２の２０１）を使用する販売業者との間で合意されたキーであり、中間プラットフォームと販売業者との間の安全な通信のために使用される。各取引暗号化キーは、中間プラットフォーム２０２に格納された対応する復号化キーを有する。受付装置３０１Ａによって使用される取引暗号化キーが私的なキーである場合、取引暗号化キーは、受付装置３０１Ａを識別するために使用可能である。一部の実施形態において、一意的な識別を確実にするために、取引暗号化キーと受付装置３０１Ａとの間の一意的な対応を使用する。言い換えると、各取引暗号化キーは、１つの受付装置３０１Ａに対応する。暗号化された情報を受付装置３０１Ａから受信すると、中間プラットフォーム２０２は、取引暗号化キーに対応する復号化キーを検索し、受信した暗号化された情報を復号化する。取引暗号化キーが私的キーである場合、中間プラットフォーム２０２に格納された復号化キーは、支払いシステムへのいずれかの受付装置によって独自の暗号化された販売業者取引情報を復号化するために使用される公共キーであってもよい。中間プラットフォーム２０２はまた、中間プラットフォーム２０２、受付装置３０１Ａ（図２の２０１）、および参加銀行サブシステム２０３間の後の調整のための参照として使用される復号化された情報を保存し得る。

【００５２】

特に参加銀行および中間プラットフォームの提供者が、同一のエンティティであるか、

同一のエンティティによって制御される場合、参加銀行サブシステム２０３は、中間プラットフォーム２０２に組み込まれ得る。この場合、取引暗号化キーおよび銀行暗号化キーは同一であってもよい。受付装置３０１Ａは、取引暗号化キーを使用して、銀行口座パスワードおよび取引金額の両方を暗号化することができ、中間プラットフォーム２０２は、公共キーを使用して、取引を完了するために暗号化された情報を復号化することができる。

【００５３】

第１の暗号部３７１は、制御器３１３にインストールされたセキュリティアクセスモジュール（ＳＡＭ）に内蔵され得る。異なるＩＣ識別カードには異なる型の暗号化が必要になり得るため、制御器３１３の選択は、支払いシステムにおいて使用されるＩＣ識別カードの特徴に依存し得る。制御器３１３の一例は、中国における第２世代識別カードに使用される。この例示的な制御器３１３は、中国公安部指定の限られた数の業者によって提供される。

【００５４】

第１、第２、および第３の暗号部３７１、３７２、および３７３は、それぞれの構成要素に組み込まれたソフトウェアモジュールであってもよい。図３Ａに示される例示的な実施形態において、例えば、第１の暗号部３７１は、ＩＣカードリーダ３１０Ａ内の制御器３１３に組み込まれたソフトウェアモジュールであり、一方、第２の暗号部３７２および第３の暗号部３７３は、受付部プロセッサ３２１に組み込まれたソフトウェアモジュールである。カード暗号化キーは、制御器３１３に予めインストールされ、一方、取引暗号化キーおよび銀行暗号化キーは、受付部プロセッサ３２１にインストールされる。

【００５５】

第１の暗号部３７１が、カード暗号化キーを使用してユーザ身元情報を復号化した後、制御器３１３は、復号化されたユーザ身元情報を受付部プロセッサ３２１に送信する。受付部プロセッサ３２１の第２の暗号部３７２は、銀行暗号化キーを使用して銀行口座パスワードを暗号化する。第３の暗号部３７３は、取引暗号化キーを使用して、取引金額を暗号化する。その後、受付部プロセッサ３２１は、ユーザ身元情報、暗号化された銀行口座パスワード、および暗号化された取引金額を、事前に確立した形式で、通信ユニット３２５を介して中間プラットフォーム２０２に送信する。

【００５６】

図３Ｂは、本開示に従う受付装置の第２の例示的な構成の略ブロック図を示す。受付装置３０１Ｂは、ＩＣカードリーダ３１０Ｂおよび販売業者処理ユニット３２０Ｂを含み、３つの暗号部３７１、３７２および３７３の構成が異なる状況であることを除き、受付装置３０１Ａに類似している。受付装置３０１Ｂにおいて、第１の暗号部３７１および第３の暗号部３７３は、制御器３１３に組み込まれ、一方、第２の暗号部３７２は、受付部プロセッサ３２１に組み込まれる。カード暗号化キーおよび取引暗号化キーは、制御器３１３にインストールされ、一方、銀行暗号化キーは、受付部プロセッサ３２１にインストールされる。

【００５７】

第１の暗号部３７１は、ＩＣ識別カードから読み取られたユーザ識別情報を復号化する。制御器３１３は、ユーザ身元情報を受付部プロセッサ３２１に伝送する。入力ユニット３２３を介して販売業者によって入力された取引金額を受信すると、受付部プロセッサ３２１は、取引金額を制御器３１３に伝送する。次いで制御器３１３内の第３の暗号部３７３は、取引金額を暗号化する。制御器３１３は、暗号化された取引金額を受付部プロセッサ３２１に伝送する。第２の暗号部３７２は、銀行口座パスワードを暗号化する。次いで、受付部プロセッサ３２１は、ユーザ身元情報、取引金額、および銀行口座パスワードを、事前に確立された形式で、通信ユニット３２５を介して中間プラットフォーム２０２に送信する。

【００５８】

図３Ｃは、本開示に従う受付装置の第３の例示的な構成の略ブロック図を示す。受付装

置３０１Ｃは、ＩＣカードリーダ３１０Ｃおよび販売業者処理ユニット３２０Ｃを含み、３つの暗号部３７１、３７２および３７３の構成が異なる状況であることを除き、受付装置３０１Ａおよび３０１Ｂと類似している。受付装置３０１Ｃにおいて、第１の暗号部３７１、第２の暗号部３７２、および第３の暗号部３７３は、すべて、ＩＣカードリーダ３１０Ｃの制御器３１３に組み込まれる。カード暗号化キー、銀行暗号化キー、および取引暗号化キーは、すべて、制御器３１３に組み込まれる。

【００５９】

第１の暗号部３７１は、ＩＣ識別カードから読み取られたユーザ識別情報を復号化する。制御器３１３は、ユーザ身元情報を受付部プロセッサ３２１に伝送する。入力ユニット３２３から、ユーザによって入力された銀行口座パスワード、および販売業者によって入力された取引金額等の、情報を受信すると、受付部プロセッサ３２１は、暗号化のため、この情報を制御器３１３に送信する。暗号化の後、暗号化された情報は、受付部プロセッサ３２１に返送され、受付部プロセッサ３２１は、暗号化された情報をユーザ身元情報とともに、通信ユニット３２５を介して中間プラットフォーム２０２に送信する。

【００６０】

図３Ｄは、本開示に従う受付装置の第４の例示的な構成の略ブロック図を示す。受付装置３０１Ｄは、ＩＣカードリーダ３１０Ｄおよび販売業者処理ユニット３２０Ｄを含み、暗号部構成において受付装置３０１Ａ、３０１Ｂおよび３０１Ｃとは異なる。受付装置３０１Ｄは、ＩＣ識別カードリーダ３１０Ｄから読み取られた識別情報を復号化する第１の暗号部３７１を有しない。この構成は、中間プラットフォーム２０２Ｂが、識別情報を解読する暗号部アセンブリ２７０を具備する、図２ＢのＩＩ型の実現形態に好適である。例えば、受付装置３０１Ｄは、図２の支払いシステム２００Ｂ内の受付装置２０１Ｂの代わりに使用され得る。

【００６１】

動作中、ＩＣカードリーダ３１０Ｄは、ＩＣカードから、暗号化された識別情報を読み取り、識別情報を販売業者処理ユニット３２０Ｄに送信し、次いで、販売業者処理ユニット３２０Ｄは、識別情報を中間プラットフォーム２０２Ｂに送信して復号化する。

【００６２】

受付装置３０１Ｄは、依然として第２の暗号部３７２および第３の暗号部３７３を有する。一実施形態において、第２の暗号部３７２および第３の暗号部３７３は、販売業者処理ユニット３２０Ｄの受付部プロセッサ３２１に組み込まれる。銀行暗号化キーおよび取引暗号化キーは、すべて、受付部プロセッサ３２１に組み込まれる。

【００６３】

入力ユニット３２３から、ユーザによって入力された銀行口座パスワード、および販売業者によって入力された取引金額等の情報を受信すると、第２の暗号部３７２および第３の暗号部３７３は、ユーザによって入力された情報を暗号化する。例えば、第２の暗号部３７２は、対応する発行銀行または第３者機関によって提供される銀行暗号化キーを使用して銀行口座パスワードを暗号化する。第３の暗号部３７３は、取引暗号化キーを使用して販売業者取引情報を暗号化する。暗号化の後、受付部プロセッサ３２１は、暗号化された情報をユーザ身元情報とともに、通信ユニット３２５を介して中間プラットフォーム２０２に送信する。第２の暗号部３７２および第３の暗号部３７３の動作は、図３Ａの受付装置３０１Ａの文脈で説明されるものと類似しているので、ここでは繰り返さない。

【００６４】

識別情報を復号化するために備えられる中間プラットフォーム２０２Ｂの詳細は、本説明の後の項で説明する。

【００６５】

第２の暗号部３７２および第３の暗号部３７３の他の代替構成を使用することができることを理解されたい。例えば、第２の暗号部３７２および第３の暗号部３７３は、受付部プロセッサ３２１に組み込まれる代わりに、別々のユニットとして実現され得る。第２の暗号部３７２および第３の暗号部３７３のうちの少なくとも１つはまた、ＩＣ識別カード

リーダ３１０Ｄ内に実装され得る（例えば、カードリーダ制御器３１３に組み込まれる）。

【００６６】

図３Ｅは、本開示に従う受付装置の第５の例示的な構成の略ブロック図を示す。受付装置３０１Ｅは、ＩＣカードリーダ３１０Ｅおよび販売業者処理ユニット３２０Ｅを含む。他の受付装置３０１Ａ、３０１Ｂ、３０１Ｃおよび３０１Ｄと比較して、受付装置３０１は、受付部プロセッサ３２１に組み込まれる代わりに、別々のユニットである暗号化ユニット３７０を有する。暗号化ユニット３７０は、１つ以上の暗号部を有し得る。

【００６７】

一実施形態において、受付装置３０１Ｅは、ＩＣ識別カードリーダ３１０Ｄから読み取られた識別情報を復号化するための第１の暗号部３７１を有しない。この構成は、受付装置３０１Ｄに類似しており、中間プラットフォーム２０２Ｂが、識別情報を解読するための暗号部アセンブリ２７０を具備する、図２ＢのＩＩ型の実現形態に好適である。例えば、受付装置３０１Ｅは、図２の支払いシステム２００Ｂ内の受付装置２０１Ｂの代わりに使用され得る。

【００６８】

上に説明する例示的な構成において、入力ユニット３２３は、外部から入力された情報を受信するために使用される。外部から入力される情報の例として、販売業者によって入力された取引金額、ユーザによって入力された銀行口座パスワード、およびユーザによって入力された銀行口座パスワードとユーザによって選択された参加銀行の情報との組み合わせが挙げられる。入力ユニット３２３は、キーボードまたはタッチスクリーン等の任意の入力装置であることが可能である。通常の条件下で、入力ユニット３２３は、ユーザにより入力された銀行口座パスワード、参加銀行の情報、および販売業者により入力された取引金額を受信する。参加銀行に対応する銀行暗号化キーは、ユーザにより入力された銀行口座パスワードを暗号化するために使用される。

【００６９】

出力ユニット３２４は、取引の結果を出力するために使用される。出力ユニット３２４は、ディスプレイまたはプリンタ等の任意の出力装置であることが可能である。出力ユニット３２４が、支払い取引の結果を出力する（例えば、画面上に表示またはプリンタを介して印刷）ために使用され、販売業者およびユーザは、銀行口座引き落としが正常に行われたか否かに基づいて取引が成功か否かを判断できる。取引が失敗した場合、出力ユニット３２４は、取引が失敗に終わった理由を出力し得る。加えて、出力ユニット３２４は、取引完了の証拠としてまたは文書化のために、取引結果を印刷することが可能である。

【００７０】

受付部プロセッサ３２１は、入力ユニット３２３、出力ユニット３２４、および制御器２２３に接続する。受付部プロセッサ３２１は、取引における販売業者の異なる動作を制御するために使用される。このような動作の例として、入力ユニット３２３から暗号部３７１へ情報を伝送すること、暗号部３７１により暗号化された情報を通信ユニット３２５へ伝送すること、および通信ユニット３２５から返送された処理結果（銀行取引結果等）を出力ユニット３２４へ伝送することが挙げられる。受付部プロセッサ３２１は、既存のプログラム可能論理素子（ＰＬＤ）から作製可能である。例えば、プロセッサは、５１シリーズ（８９Ｓ５２、８０Ｃ５２、８７５２等）等のシングルチップマイクロプロセッサ、または任意の他の好適なマイクロプロセッサを使用することが可能である。

【００７１】

受付部プロセッサ３２１は、ユーザ身元情報およびユーザの名前等の情報を、識別カードリーダ（３１０Ａ、３１０Ｂ、３１０Ｃ、３１０Ｄまたは３１０Ｅ）から受信し、出力ユニット３２４を介してこの情報を表示することができる。識別カードリーダが識別カードを読み取る際に、機械可読情報または機械可読画像が表示不可能である場合、識別カードを拒絶する可能性がある。これは、通常、識別カードが適切に暗号化された情報を有しないこと（これは、偽造識別カードを示す可能性が高い）、またはカードが損傷している

ことにより発生する。この場合、取引は、拒否され得る。さらに、身元情報を読み取るために識別カードリーダ３１０を使用する販売業者の担当者（例えば、レジ係）は、識別カードリーダ３１０に表示される顧客（ユーザ）の写真を比較することができる。写真および顧客の外見が一致しない（つまり、機械可読情報が、担当者が見るユーザの視覚的提示に類似しない）場合、販売業者の担当者は、識別カードが、この顧客に属するものではないという結論を下し、取引を拒否することができる。

【００７２】

受付部プロセッサ３２１は、外部から入力されたコマンドを受信および実行し、対応するタスクを完了することができる。外部コマンドの例として、識別カードリーダにより読み取られたコンテンツを別の外部機器に出力すること、および参加銀行の更新された銀行暗号化キーを受信したときに、局所的に保存された銀行暗号化キーを更新することが挙げられる。

【００７３】

開示する支払いシステムは、受付装置２０１にインストールされたＡＰＩインターフェースを使用して、受付装置の高い拡張性および互換性を達成することができる。例えば、受付部プロセッサ３２１は、受付装置２０１（図３の３１０Ａ、３１０Ｂ、３１０Ｃ、３１０Ｄまたは３１０Ｅのうちのいずれかであることが可能）と、中間プラットフォーム２０２との間の接続を確立するためのＡＰＩインターフェースを有し得る。これは、ユーザ身元情報、ならびに入力された取引金額を、受付装置２０１と中間プラットフォーム２０２との間で通信することを含む。また、受付装置上のＡＰＩインターフェースは、他の手順を実行することができる。ＡＰＩインターフェースを介して、受付装置２０１は、中間プラットフォーム２０２とのシームレスな接続を確立することが可能である。また、受付装置２０１と他の外部機器との間の接続は、このＡＰＩインターフェースを介しても確立可能である。

【００７４】

通信ユニット３２５は、中間プラットフォームとのインタラクションを確立するために使用される。通信ユニット３２５は、暗号化された情報を中間プラットフォーム２０２に送信し、中間プラットフォーム２０２から受付部プロセッサ３２１に処理結果を伝送する。通信ユニット３２５は、通常の電話、任意のネットワークのダイヤルアップモデム、またはＬＡＮを介するネットワーク接続に対応する専用のインターフェースを有し得る。通信ユニット３２５は、主に、受付装置と中間プラットフォーム２０２との間の接続を確立するために使用される。例えば、受付装置上の通信ユニット３２５は、通常の電話、ＧＰＲＳ、およびＣＤＭＡ等の異なるダイヤルアップ、および他の専用の通信ポートのモデムを介する通信に対応するように、中間プラットフォーム２０２の通信ユニットに一致させることができる。

【００７５】

本開示における暗号部は、シングルチップＭＣＳ等のシングルチップマイクロプロセッサであってもよく、さらに、図６を参照して説明するように、制御器３１３または受付部プロセッサ３２１に組み込まれるよりも、むしろ別々の構成要素として具現化され得る。

【００７６】

図４は、本開示に従う例示的受付装置の略図である。受付装置４０１は、図２、図３、図５、および図６等の本説明の他の図面を参照して理解されたい。受付装置４０１は、箱型であり、ケースおよび内部構造を含む。表示画面４３１は、出力ユニット（３２４）の一部であり、ケースの上側正面に設置され、情報を表示するために使用される。例えば、ＩＣ識別カードが読み取られる場合、ＩＣ識別カード内の情報は、表示画面４３１上に表示される。表示画面４３１の下に、ユーザまたは販売業者により情報を入力するための入力ユニット（３２３）の一部であるキーボード４３３が存在する。さらに、キーボード４３３の下に、識別カードリーダ４１０が設置される。ＩＣ識別カードが読み取りゾーン４３４に配置されると、ＩＣ識別カード上の情報は、識別カードリーダ４１０によって読み取られる。ＩＣ識別カードの読み取りは、ＩＣ識別カードと識別カードリーダ４１０との

間を直接接触させずに完了することが可能である。識別カードリーダ４１０は、そのコイルを介して電磁励起信号を連続的に送信する。識別カードがカードリーダの読み取りゾーン４３４に配置されると、識別カード内のコイルは、電磁励起信号の効果により弱電流を発生する。この電流は、ＩＣ識別カード内のＩＣチップの電源としての役割を果たす。該チップは、ユーザ身元情報を含む。識別カードのＩＣチップは、ユーザ身元情報を識別カードリーダ４１０に送信し、電磁励起信号の効果による、読み取り操作を完了する。

【００７７】

受付装置４０１がユーザ識別情報を復号化する能力を有するＩ型の実現形態において、識別カードリーダ４１０は、暗号化されたユーザ身元情報を、復号化するために暗号部（３７１）に送信する。復号化されたユーザ識別情報は、受付装置４０１の内部構造に設置されたプロセッサ（３２１）に送信される。プロセッサ（３２１）は、受信した情報を、表示するための表示画面４３１に送信する。

【００７８】

受付装置４０１がユーザ識別情報を復号化する能力を有しないＩＩ型の実現形態において、識別カードリーダ４１０は、暗号化されたユーザ識別情報を、プロセッサ（３２１）に送信し、中間プラットフォームに通信して復号化する。中間プラットフォームは、復号化されたユーザ識別情報を受付装置４０１に返送して、表示画面４３１に表示し得る。復号化されたユーザ識別情報を受付装置４０１に表示することは任意選択であることを理解されたい。ＩＣ識別カードは、カード所有者の印刷された写真等の暗号化されていない識別情報を有し得、これは、販売業者による検証のために使用することができる。

【００７９】

また、プロセッサ（３２１）は、ユーザに対して銀行口座パスワードを入力するように要求するメッセージと、販売業者に対して取引金額を入力するように要求するメッセージとを、送信し得る。該要求するメッセージは、表示画面に送信され、表示され得る。これにより、ユーザに、銀行口座パスワードの入力を促し、販売業者に取引金額の入力を促す。

【００８０】

プロセッサ（３２１）は、キーボード４３３を介して、ユーザにより入力された銀行口座パスワードと、販売業者により入力された取引金額とを受信する。暗号部を使用して、銀行口座パスワードおよび取引金額を暗号化すると、プロセッサ（３２１）は、この暗号化された情報をユーザ識別情報（Ｉ型の実現形態において復号化、ＩＩ型の実現形態において暗号化された）とともに、通信ユニット（３２５）に伝送する。この例示的な実施形態において、通信ユニットは、ＬＡＮを介して反対端に接続する特別な専用ポート４３２を使用し得る。

【００８１】

受付装置４０１の識別カードリーダ４１０は、指定の業者により提供を受けることが可能である。ＩＩ型の実現形態では、識別カードリーダ４１０または受付装置４０１によってユーザ識別情報を復号化する能力を有する必要がないので、識別カードリーダ４１０を有する受付装置４０１の製造に関し、より多くの設計の自由および低コストが可能となり得る。

【００８２】

ユーザ識別情報、取引金額、および銀行口座パスワードは、データの安全を確実とするために、送信前に暗号化することができる。特に、暗号部（３７１、３７２、および３７３）がＩＣカードリーダ３１０の制御器（３１３）に組み込まれている実施形態においては、販売業者は、制御器内の情報を修正することができない。したがって、暗号化された情報の安全性は、本構成においてさらに強化される。ＩＩ型の実現形態において、ユーザ識別情報は、受付装置４０１にある間、暗号化されたままであることが可能なので、販売業者側でのプライバシーの侵害の機会はより少なくなる。

【００８３】

図５は、ＩＣカードリーダにインターフェース接続するコンピュータを使用する例示的

な受付装置の略ブロック図を示す。受付装置５０１は、図２の受付装置２０１のうちの１つと受付装置５０１とを置き換えることによって、図２の支払いシステム２００を参照しながら理解されたい。

【００８４】

受付装置５０１は、識別カードリーダ５１０およびコンピューティング端末５２０を有する。受付装置５０１は、受付装置３０１Ｄと類似している。実際、受付装置５０１は、処理ユニット３２０Ｄがコンピュータ端末５２０とともに実装される受付装置３０１Ｄの特別な事例として理解され得る。識別カードリーダ５１０は、アンテナ５１１、ＲＦモジュール５１２、制御器５１３、およびインターフェースユニット５１４を含む。インターフェースユニット５１４は、コンピュータ端末５２０とインターフェース接続するように設計される。ＲＦモジュール５１２は、アンテナ５１１および制御器５１３に別々に接続し、一方、制御器５１３は、インターフェースユニット５１４に接続する。識別カードリーダ５１０は、ユーザ識別カード上のユーザ身元情報を読み取るために使用される。

【００８５】

２つの暗号部である、第２の暗号部５１６および第３の暗号部５１７は、暗号化および復号化のために使用される。第２の暗号部５１６は、参加銀行または第３者機関のいずれかにより提供される銀行暗号化キーを使用して銀行口座パスワードを暗号化するために使用される。第３の暗号部５１７は、取引暗号化キーを使用して取引金額を暗号化するために使用される。

【００８６】

コンピューティング端末５２０は、識別カードリーダ５１０に接続し、入力ユニット５２３、出力ユニット５２４、プロセッサ５２１、ならびに２つの通信ユニット５２５および５２６を含む。通信ユニット５２５は、インターフェースユニット５１４を介して識別カードリーダ５１０に接続し、一方、通信ユニット５２６は、中間プラットフォーム（２０２）に接続する。

【００８７】

入力ユニット５２３は、外部から入力された情報を受信するために使用される。外部から入力される情報の例として、販売業者により入力された取引金額、ユーザにより入力された銀行口座パスワード、およびユーザにより入力された銀行口座パスワードとユーザにより選択された参加銀行の情報との組み合わせが挙げられる。出力ユニット５２４（通常はコンピュータ画面）は、取引結果を出力するために使用される。

【００８８】

プロセッサ５２１は、入力ユニット５２３、出力ユニット５２４、ならびに通信ユニット５２５および５２６に接続する。プロセッサ５２１は、ユーザ識別情報、暗号化された銀行口座情報、および暗号化された販売業者取引情報を、通信ユニット５２６に送信し、中間プラットフォーム（２０２）に伝送し、中間プラットフォーム（２０２）および通信ユニット５２６を介して参加銀行サブシステム（２０３）から返送された銀行取引結果を受信し、受信した銀行取引結果を出力ユニット５２４に送信する。

【００８９】

通信ユニット５２５および５２６は、プロセッサ５２１に接続し、他の機器とのインタラクションを確立するために使用される。通信ユニット５２５は、識別カードリーダ５１０に接続し、識別カードリーダ５１０内のインターフェースユニット５１４に一致するポートを使用することが可能である。このような一致するポートの一例としてＵＳＢポートが挙げられる。通信ユニット５２６は、中間プラットフォーム（２０２）に接続し、通常の電話、任意のネットワークのダイヤルアップモデム、またはＬＡＮを介する反対端へのネットワーク接続に対応する専用インターフェースとすることができる。

【００９０】

受付装置５０１Ａ、５０１Ｂ、または５０１Ｃにおいて、識別カードリーダ５１０およびコンピューティング端末５２０は、相互に接続された２つの個別の構成要素であってもよい。識別カードリーダ５１０は、モジュラーであることが可能であり、インターフェー

スの必要条件を満たす任意のコンピューティング端末とともに作動して支払い要求を完了させるように設計可能である。

【００９１】

図６は、別々の暗号化ユニットを有する例示的な受付装置の略ブロック図である。受付装置６０１は、識別カードリーダ６１０、暗号化ユニット６３０、およびコンピューティング端末６２０を有する。

【００９２】

識別カードリーダ６１０は、アンテナ６１１、ＲＦモジュール６１２、制御器６１３、およびインターフェースユニット６１５を有する。ＲＦモジュール６１２は、アンテナ６１１および制御器６１３（制御器６１３は、同様にインターフェースユニット６１５に接続する）に接続する。識別カードリーダ６１０は、ユーザ識別カード上のユーザ身元情報（ユーザ識別カード番号等）を読み取るために使用される。

【００９３】

暗号化ユニット６３０は、識別カードリーダ６１０およびコンピューティング端末６２０に接続されるが、これらに組み込まれていない別々のユニットである。暗号化ユニット６３０は、シングルチップマイクロプロセッサ６３１、ならびに２つのインターフェース６３２および６３３を有する。シングルチップマイクロプロセッサ６３１は、各インターフェース６３２および６３３に接続する。２つのインターフェース６３２および６３３は、コンピューティング端末６２０および識別カードリーダ６１０にそれぞれ接続する。

【００９４】

原則として、暗号化ユニット６３０は、ＩＣ識別カードから読み取られるユーザ識別情報の復号化、ならびに銀行口座情報および販売業者取引情報の暗号化を含む、販売業者側でのすべての必要な暗号化および復号化を実施するように設計され得る。一実施形態において、暗号化ユニット６３０は、銀行口座情報および販売業者取引情報のみの暗号化を行い、ユーザ識別情報の復号化は行わない。この実施形態は、上に述べる支払いシステムのＩＩ型の実現形態に好適である。

【００９５】

例えば、一実施形態において、シングルチップマイクロプロセッサ６３１は、取引暗号化キーを使用して取引金額を暗号化し、参加銀行または第３者機関のいずれかにより提供される銀行暗号化キーを使用して、銀行口座パスワードを暗号化するために使用される。

【００９６】

コンピューティング端末６２０は、入力ユニット６２３、出力ユニット６２４、プロセッサ６２１、ならびに通信ユニット６２５および６２６を有し、コンピューティング端末５２０と類似の機能を実行する。加えて、コンピューティング端末６２０は、同一の通信ユニット６２６を介して、またはコンピューティング端末６２０にインストールされている別の通信ユニット（図示せず）を介して、識別カードリーダ６１０とも直接インタラクトし得る。

【００９７】

中間プラットフォームに接続する通信ユニット６２６は、通常の電話、任意のネットワークのダイヤルアップモデム、またはＬＡＮを介する反対端へのネットワーク接続に対応する特別な専用インターフェースであってもよい。暗号化ユニット６３０および識別カードリーダ６１０とインタラクトする通信ユニット６２５は、ＵＳＢポートまたはこのような通信を確立することができる任意の他の適切なポートであることが可能である。暗号部ユニット６３０のシングルチップマイクロプロセッサ６３１は、ＭＣＳ５１モデル、または別の型もしくは別のモデルのシングルチップマイクロプロセッサであってもよい。

【００９８】

上記説明は、本開示に従う受付装置２０１のいくつかの例示的な実施形態を単に提供するだけである。受付装置２０１は、図４に示すように、全ての構成要素（図３、図５、および図６に示す構成要素等）をその中に設置するのに十分な空間を有する容器において具現化され得る。代替的に、受付装置は、２つの個別の構成要素から構成され得る。例えば

、図５の入力ユニット、出力ユニット、プロセッサ、暗号部、および通信ユニットは、コンピューティング端末５２０に組み込まれ、一方、識別カードリーダ５１０は、別の構成要素として具現化される。識別カードリーダ５１０およびコンピューティング端末５２０は、そのそれぞれのインターフェースを介して互いに相互接続される。代替的に、受付装置は、３つの個別の構成要素から構成され得る。例えば、図６のように、入力ユニット、出力ユニット、プロセッサ、および通信ユニットを、コンピューティング端末６２０に組み込む。暗号化ユニット６３０および識別カードリーダ６１０は、各々個別の構成要素として具現化される。暗号部ユニット６３０およびコンピューティング端末６２０は、それぞれのインターフェースを介して互いに相互接続されるが、一方、暗号部ユニット６３０および識別カードリーダ６１０は、それらのインターフェースを介して互いに相互接続される。

【００９９】

加えて、受付装置は、販売業者と中間プラットフォームとの間の接続の確立に使用されるＡＰＩインターフェースもまた有し得る。ＡＰＩインターフェースを介して実行される機能は、ユーザ身元情報ならびに受付装置から入力された取引金額の取得を含む。また、受付装置上のＡＰＩインターフェースは、他の機能を実行し得る。ＡＰＩインターフェースを介して、受付装置は、中間プラットフォームとのシームレスな接続を確立することができる。受付装置と他の外部機器との間の接続も、このＡＰＩインターフェースを介して確立可能である。ＡＰＩインターフェースは、高い拡張性および互換性を実現するために、受付装置に事前にインストールされ得る。

【０１００】

上に開示される受付装置に関連して、本開示における中間プラットフォーム２０２および参加銀行サブシステム２０３を以下に説明する。

【０１０１】

図２、２Ａおよび２Ｂを再び参照すると、中間プラットフォーム（２０２、２０２Ａまたは２０２Ｂ）は、主に、販売業者と参加銀行との間の取引を確立するために使用される。中間プラットフォーム（２０２、２０２Ａまたは２０２Ｂ）の例としては、本件特許出願人のＡｌｉｐａｙプラットフォームが挙げられる。ユーザはまず、中間プラットフォーム上で、識別カードを使用する支払い方法を有効にすることができる。これは、口座を開設し、ユーザ識別情報を中間プラットフォームに登録することによって実行可能である。参加銀行サブシステム２０３の参加銀行は、ユーザ口座情報等の情報ならびに暗号化キーおよび復号化キーを提供する契約を、中間プラットフォーム２０２と締結することができる。支払い取引中、参加銀行の銀行口座を有するユーザは、支払いおよびクレジットカード事前承認等の操作を完了させるためには、受付装置で銀行名を選択または提供し、かつ銀行口座パスワードを入力することのみが必要である。

【０１０２】

中間プラットフォーム

図７は、本支払いシステムの中間プラットフォームのさらなる詳細を示す。中間プラットフォーム７０２は、銀行口座処理ユニット７６３を含むプラットフォームプロセッサ７６１と、通信インターフェース７６２と、暗号化ユニット７７０とを有する。暗号化ユニット７７０は、受付装置２０１から送信された暗号化された情報を復号化するために使用される。

【０１０３】

プラットフォームプロセッサ７６１は、受付装置（例えば、２０１、２０１Ａまたは２０１Ｂ）からデータを受信し、該データをユーザ識別情報、銀行口座情報、課金情報、取引金額等の種々の種類に分解する。受付装置の構成に依存して、かかる情報は暗号化、復号化、または非暗号化され得る。図２ＢのＩＩ型の実現形態において、例えば、受付装置２０１Ｂから受信されたユーザ識別情報は暗号化されている。プラットフォームプロセッサ７６１は、受信した暗号化されたユーザ識別情報を復号化チップアセンブリ７７３に送信して復号化する。

【０１０４】
以下において、中間プラットフォーム７０２を、中間プラットフォームがユーザ識別情報を復号化する能力を有するＩＩ型の実現形態を想定して説明する。しかしながら、ユーザ識別情報の復号化以外の、以下の説明のほとんどが、Ｉ型の実現形態にも適用される。
【０１０５】
中間プラットフォーム７０２のデータストレージ７６５は、ＩＣ識別カード復号化キー、および各契約している受付装置２０１の取引暗号化キーに対応する取引復号化キー等の復号化キーをその上に格納している。銀行情報（銀行口座パスワード等）の復号化が、暗号化ユニット７７０によって中間プラットフォーム７０２で行われる場合、データストレージ７６５は、銀行復号化キーも格納し得る。代替的に、復号化キーは、暗号化ユニット７７０に含まれるメモリに格納され得る。
【０１０６】
暗号化ユニット７７２は、暗号化アルゴリズムおよびＩＣカード復号化キーに不適切なユーザ識別情報を復号化する。暗号化ユニット７７０の例示的な実施形態は、図２Ｂの復号化チップアセンブリ２７０である。復号化チップアセンブリ２７０は、識別情報を復号化するためのそれ自身の復号化機器を有しない場合がある受付装置２０１Ｂから送信された識別情報の復号化を、中間プラットフォーム２０２Ｂが行う、ＩＩ型の実現形態のためのものである。復号化チップアセンブリ２７０は、通常は政府機関（例えば、中国公安部）であるＩＣ識別カード発行元によって課される、基準および要件によって製造される、１つ以上の復号化チップを有し得る。復号化チップアセンブリ２７０内の各復号化チップは、ＩＣ識別カードを暗号化するために使用される暗号化アルゴリズムに一致する復号化アルゴリズムを使用する復号化能力を有するように製造される。復号化チップアセンブリ２７０内の復号化チップは、ＩＣ識別カードを作製する同一の政府指定の製造者によって製造され得る。代替的に、これらの製造者は、一致する復号化アルゴリズムを提供することによって、中間プラットフォームの所有者と協働してもよい。
【０１０７】
ユーザ識別情報の復号部として使用する場合、複数の受付装置から送信された多数の復号化要求をより良好に対応するために、暗号化ユニット７７０では、並行して動作する複数の復号化チップが好ましい。一実施形態において、暗号化ユニット７７０は、大容量の並行処理のためのサーバで具現化される。別の実施形態において、暗号化ユニット７７０は、プラットフォームプロセッサ７６１に組み込まれた暗号化モジュール（例えば、ソフトウェアモジュール）を有する。
【０１０８】
暗号化された販売業者取引情報を受信すると、中間プラットフォーム７０２は、暗号化された情報を復号化するために対応する復号化キーを検索する。販売業者取引情報は一般的には、取引金額を含む。中間プラットフォーム７０２は、復号化の後、暗号化キー、ユーザ身元情報、および取引金額を保存する。参加銀行サブシステム２０３が、銀行取引（例えば、ユーザの銀行口座からの引き落とし）が成功したか否かに関する銀行取引結果を返送する場合、中間プラットフォーム７０２は、受信した銀行取引結果も保存する。中間プラットフォーム７０２は、この保存された情報を使用して、後に販売業者および参加銀行との調整を実施する場合がある。取引暗号化キーは、私的キーであることが可能であり、対応する取引復号化キーは公共キーであることが可能である。私的な取引暗号化キーにより、中間プラットフォーム７０２は、受付装置、および取引を実行する関連の販売業者の識別を容易に検証することができる。
【０１０９】
プラットフォームプロセッサ７６１は、データベース７６６とインタラクトする銀行口座処理ユニット７６３をさらに含む。データベース７６６は、ユーザ識別カード番号とユーザ銀行口座との間のマッピング関係を含む。取引を行う前に、ユーザはまず、中間プラットフォーム７０２に、ユーザ識別カード番号と対応する銀行口座番号を登録することができる。ユーザ識別カード番号が、特定の参加銀行の１つの銀行口座番号のみに対応する

場合、このような登録は、必要ない場合がある。しかしながら、支払いのためにユーザが選択した参加銀行において、複数の銀行口座番号が同一の識別カード番号に対応する場合、ユーザは、通常、中間プラットフォーム７０２において銀行口座番号を１つだけ設定するか、または支払い取引中に受付装置２０１において支払い銀行を１つだけ選択する必要がある。

【０１１０】

プラットフォームプロセッサ７６１が、受付装置２０１からの暗号化された情報を復号化した後、プラットフォームプロセッサ７６１は、ユーザ識別カード番号を使用して、データベース７６６において対応する銀行口座を検索する。対応する銀行口座が見つかると、プラットフォームプロセッサ７６１は、銀行口座番号を、銀行取引情報の一部として、参加銀行サブシステム２０３に送信する。中間プラットフォーム７０２および参加銀行２０３は、事前に合意した、伝送のためのデータ構造を有し得る。該データ構造は、銀行口座番号用のフィールドを含み得る。見つかった銀行口座番号は、参加銀行サブシステム２０３による銀行口座番号の識別および読み取りを容易にするように、それぞれのフィールドに位置することができる。

【０１１１】

プラットフォームプロセッサ７６１は、復号化された情報をデータストレージ７６５に保存し、銀行取引情報（復号化された情報および暗号化された情報の両方を含み得る）を参加銀行サブシステム（例えば、２０３）に送信する。プラットフォームプロセッサ７６１はまた、参加銀行サブシステムから返送された銀行取引結果を、銀行取引結果を格納した後に、受付装置に送信する。

【０１１２】

通信インターフェース７６２は、受付装置（例えば、２０１Ｂ）と参加銀行サブシステム（例えば、２０３）との通信を確立する。

【０１１３】

中間プラットフォーム７０２から送信された銀行取引情報が、銀行口座番号を含まない場合、参加銀行サブシステムは、それ自身のデータベース内でユーザ識別番号に対応する銀行口座番号を調べ、復号化された銀行口座パスワードを検証することができる。復号化された銀行口座パスワードを検証すると、参加銀行サブシステムは、取引を処理し、銀行取引結果を返送する。

【０１１４】

参加銀行サブシステムは通常、銀行プロセッサおよび銀行データベースを有する。銀行データベースは、銀行口座の口座所有者、銀行口座番号、銀行口座パスワード、および残高に関する情報を含む銀行口座情報を格納する。銀行プロセッサは、データ読み取りモジュール、復号化モジュール、および取引処理モジュールを有し得る。データ読み取りモジュールは、中間プラットフォーム７０２からの取引要求を読み取り、該取引要求からユーザ身元情報、暗号化された銀行口座パスワード、および他の銀行口座情報等の情報を分析して取り出すために使用される。復号化モジュールは、銀行口座パスワードを取得するために、暗号化された銀行口座パスワードを復号化する。

【０１１５】

銀行取引情報が銀行口座情報（例えば、銀行口座番号）を含む場合、取引処理モジュールは、銀行口座情報によって銀行口座を識別し、復号化された銀行口座パスワードを、銀行データベースに格納されている銀行口座パスワードと比較する。パスワードの一致が見られた場合、検証は成功し、次いで、取引処理モジュールは、デビット取引を処理する。パスワードの相違が見られた場合、認証は失敗する。銀行取引情報が、銀行口座情報を含まない場合、取引処理モジュールは、銀行データベース内でユーザ識別カード番号に従って、銀行口座を検索し得る。参加銀行において、複数の銀行口座番号が、同一の識別カード番号に対応することが見つかった場合、参加銀行サブシステムは、支払い取引を終了するか、またはこの支払いに関する特定の銀行口座番号を提供するようにユーザに要求するメッセージを中間プラットフォームに送信するか、のいずれかを行うことができる。支払

い取引を終了するか、またはこの支払いに関する特定の銀行口座番号を提供するようにユーザに要求するメッセージを中間プラットフォームに送信するか、のいずれかを行うことができる。

【０１１６】

中間プラットフォーム７０２の一実施形態において、暗号化ユニット７７０は、情報を参加銀行サブシステムに送信する前に、以前に格納された暗号化キーを使用して、銀行取引情報をさらに暗号化する。以前に格納された暗号化キーは、参加銀行と合意された暗号化キーである。したがって、参加銀行サブシステムは、対応する復号化キーを使用して受信された銀行取引情報を復号化するための暗号化ユニットを有し得る。参加銀行サブシステムは、結果を中間プラットフォーム７０２に送信する前に、銀行取引結果を暗号化することができる。暗号化ユニット７７０は、以前に格納された復号化キーを使用して、参加銀行サブシステム２０３から受信した銀行取引結果を復号化する。以前に格納された復号化キーは、通常、参加銀行によって合意されている（および提供され得る）。

【０１１７】

図８は、本説明に従う、ＩＣ識別カードを使用した支払い方法の例示的なプロセスのフローチャートである。本説明において、プロセスが説明されている順番は、限定するものとして解釈されることを意図しておらず、よって任意の数の説明されているプロセスブロックを、任意の順番で組み合わせて、方法または代替方法を実施してもよい。例示的なプロセスの主なブロックについて以下に説明する。

【０１１８】

Ｓ１１０において、受付装置の識別カードリーダは、カード所有者（顧客）によって提示されたＩＣ識別カードからのユーザ識別カード番号を含む、ユーザ身元情報を読み取る。上に説明するＩ型の実現形態では、ユーザ識別情報が識別カードリーダによって読み取られる際、識別カードリーダの暗号部は、ユーザ識別情報を復号化する。上に説明するＩＩ型の実現形態では、暗号化されたユーザ識別情報は、中間プラットフォームに送信され暗号化される。

【０１１９】

特定の状況下において、受付装置は、販売業者が、カード所有者の情報と顧客の情報とを比較できるように、ユーザ身元情報を表示する必要があり得る。このため、受付装置は、ユーザ身元情報を、受付装置内に含まれるプロセッサに送信し、出力ユニットを介して情報を表示する。顧客の身元情報がカード所有者の提示と一致しないと販売業者が判断する場合、販売業者は、支払いを拒否し得る。追加的にまたは代替的に、販売業者は、ＩＣ認証カード上の印刷された写真を使用してカード所有者の身元を視覚的に検証することができる。

【０１２０】

受付装置はまた、ユーザ銀行口座情報（銀行口座パスワード等）および販売業者取引情報（取引金額等）を受信する。例えば、ユーザは、出力ユニットにおいて促されて、銀行口座パスワードおよびそれぞれの銀行名を入力する。販売業者は、出力ユニットにおいて促されて、取引金額を入力する。入力ユニットを介して入力された銀行口座パスワードを受信すると、受付装置は、参加銀行によって提供されたまたは第３者機関によって提供された、いずれかの銀行暗号化キーを使用して、銀行口座パスワードを暗号化する。入力ユニットを介して入力された取引金額を受信すると、受付装置は、取引暗号化キーを使用して、入力された取引金額を暗号化する。

【０１２１】

Ｓ１２０において、販売業者によって入力された取引金額、およびユーザによって入力された銀行口座パスワードは、暗号化され、中間プラットフォームに送信される。ユーザ識別情報も中間プラットフォームに送信される。Ｉ型の実現形態において、ユーザ識別情報は、まず、中間プラットフォームに送信される前に、暗号化される。ＩＩ型の実現形態において、暗号化されたユーザ識別情報は、中間プラットフォームに送られ、復号化される。

【０１２２】
Ｓ１３０において、中間プラットフォームは、受信したユーザ識別情報、銀行口座情報、および販売業者取引情報を処理する。該情報を処理するために、中間プラットフォームは、受信した暗号化された情報の一部を復号化し得る。Ｉ型の実現形態において、中間プラットフォームは、暗号化された銀行口座情報および販売業者取引情報を復号化し得る。ＩＩ型の実現形態において、中間プラットフォームは、暗号化されたユーザ身元情報、銀行口座情報、および販売業者取引情報を復号化し得る。一実施形態において、中間プラットフォームは、銀行暗号化キーに対応する銀行復号化キーを使用して銀行口座情報を復号化し、取引暗号化キーに対応する取引復号化キーを使用して販売業者取引情報を復号化し、復号化された情報を格納する。別の実施形態において、中間プラットフォームは銀行口座情報を復号化しないが、代わりに、それを参加銀行サブシステムに送り復号化する。
【０１２３】
次いで、中間プラットフォームは、銀行取引情報（識別情報、銀行口座パスワード、および取引金額を含む）をそれぞれの参加銀行サブシステムに伝送する。
【０１２４】
Ｓ１４０において、銀行取引情報が銀行口座番号を含まない場合、参加銀行サブシステムは、ユーザ識別番号に対応する銀行口座番号を調べて、復号化された銀行口座パスワードを検証する。復号化された銀行口座パスワードを検証すると、参加銀行サブシステムは、取引を処理し、銀行取引結果を返送する。さらに、参加銀行サブシステムが、参加銀行において、同一の識別カード番号に対応する複数の銀行口座番号を見つけた場合、参加銀行サブシステムは、支払い取引を終了させるか、またはこの支払いに関する特定の銀行口座番号を提供するようにユーザに要求するメッセージを、中間プラットフォームに送信するかの、いずれかとすることができる。
【０１２５】
一実施形態において、ユーザ銀行口座は、中間プラットフォームによって識別され得る。この場合、プロセスは、以下の動作をさらに含み得る。（１）中間プラットフォームにおいて、ユーザ識別カード番号とユーザ銀行口座間とのマッピング関係を事前に格納すること、および（２）マッピング関係からユーザ識別カード番号に対応する銀行口座番号を調べて、見つかった場合、銀行口座番号を、銀行取引情報の一部として参加銀行サブシステムに送信すること。
【０１２６】
図９は、Ａｌｉｐａｙ支払いプラットフォームを中間プラットフォームとして使用する支払い方法の例示的プロセスを示す。例示的なプロセスを以下に説明する。
【０１２７】
Ｓ１１において、識別カードリーダは、顧客によって提供されたＩＣ識別カードを受信する。
【０１２８】
Ｓ１２において、識別カードリーダは、ＩＣ識別カードから読み取られた識別情報を、受付部プロセッサに伝送する。
【０１２９】
Ｓ１３において、販売業者は、入力ユニットを介して現在の取引金額を入力する。
【０１３０】
Ｓ１４において、顧客は、入力ユニットを介して、取引に関して支払う銀行名、およびそれぞれの銀行口座パスワードを選択または入力する。
【０１３１】
プロセッサは、銀行暗号化キー（参加銀行に対応し、銀行により提供され、かつ局所的に事前に格納される場合がある）を使用して、銀行口座パスワードを暗号化する。プロセッサはまた、事前に格納された取引暗号化キーを使用して、取引金額を暗号化する。
【０１３２】
Ｓ１５において、プロセッサは、通信ユニットを介して、識別情報を、他の暗号化され

た情報とともに、Ａｌｉｐａｙ支払いプラットフォームに送信する。

【０１３３】

Ｓ１６において、Ａｌｉｐａｙ支払いプラットフォームは、受信した情報を復号化する。ＩＩ型の実現形態では、例えば、Ａｌｉｐａｙ支払いプラットフォームは、複数の受付装置から受信したユーザ識別情報の並行復号化を行うために、復号化チップアセンブリ（別々のサーバに実装されるか、またはプラットフォームプロセッサに組み込まれるかのいずれか）を有する。Ａｌｉｐａｙ支払いプラットフォームは、暗号化された銀行口座情報および販売業者取引情報をさらに復号化し得る。

【０１３４】

受信した情報が、ユーザにより選択された銀行に関する情報を含む場合、Ａｌｉｐａｙは、処理するために、ユーザ身元情報および取引金額等の銀行取引情報を、選択された銀行の参加銀行サブシステムに送信する。受信した情報が、参加銀行情報（例えば、銀行名）を含まない場合、Ａｌｉｐａｙは、ユーザ識別に一致することができ、かつ銀行取引を成功して処理することが可能である参加銀行を識別するために、銀行取引要求を多数の参加銀行に送信することができる。銀行取引要求は、一致する参加銀行が識別されるまで、複数の銀行に１つずつ送信され得る。銀行取引要求の一例として、ユーザ銀行口座から引き落として支払いを行う要求が挙げられる。要求された銀行取引が、いずれの参加銀行によってもうまく処理できない場合、Ａｌｉｐａｙ支払いプラットフォームは、取引失敗を示す銀行取引結果を返送し得る。

【０１３５】

Ｓ１７において、Ａｌｉｐａｙは、参加銀行によって返送された銀行取引結果（例えば、銀行口座引き落とし要求の結果）を、それぞれの販売業者のプロセッサに返送する。受信した銀行取引結果に依存して、プロセッサは、取引を継続可能であるか否かを判断する。

【０１３６】

銀行取引結果は、Ａｌｉｐａｙ支払いプラットフォームを介して送信され得る。代替的に、銀行取引結果は、参加銀行によって、販売業者およびユーザに直接送信され得る。

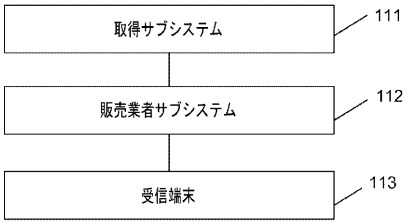
【０１３７】

本明細書において論じられた潜在的利益および利点は、付随の請求項の範囲に対する限定および制限として解釈されるべきではないことを理解されたい。

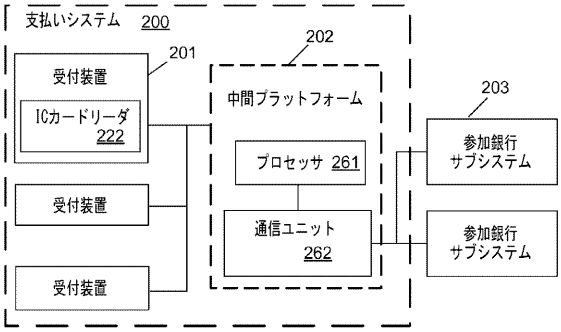
【０１３８】

主題は、構造的特徴および／または方法論的動作に特有の表現を用いて説明されているが、付随の請求項において定義される主題は、説明される具体的な特徴または動作に限定されるとは限らないことを理解されたい。むしろ、具体的な特徴および動作は、請求項を実施する例示的形態として開示される。

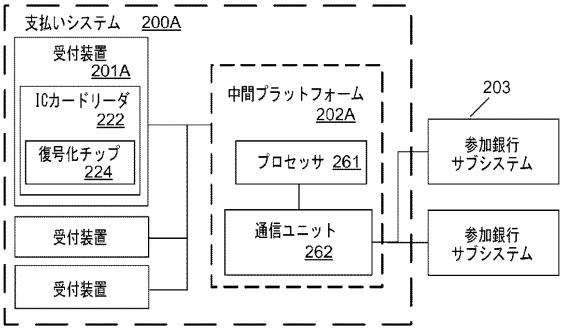
【図１】



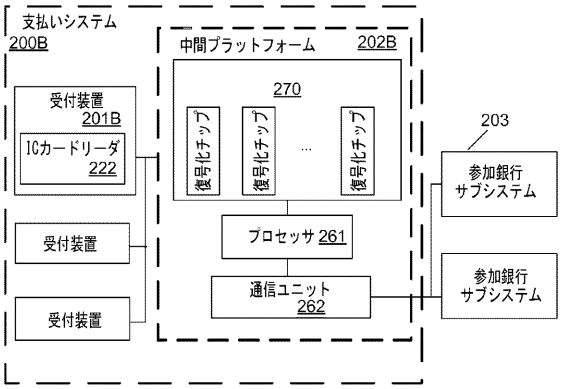
【図２】



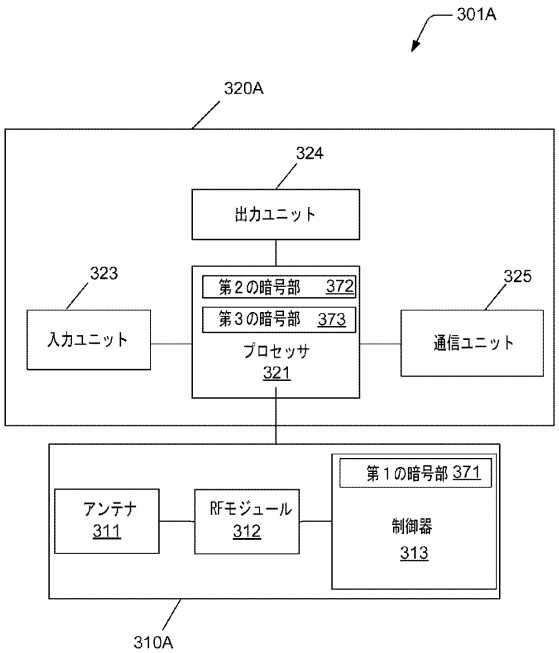
【図２Ａ】



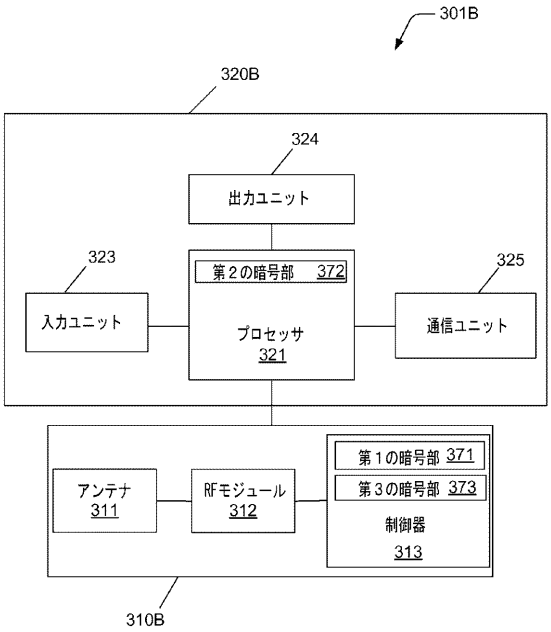
【図２Ｂ】



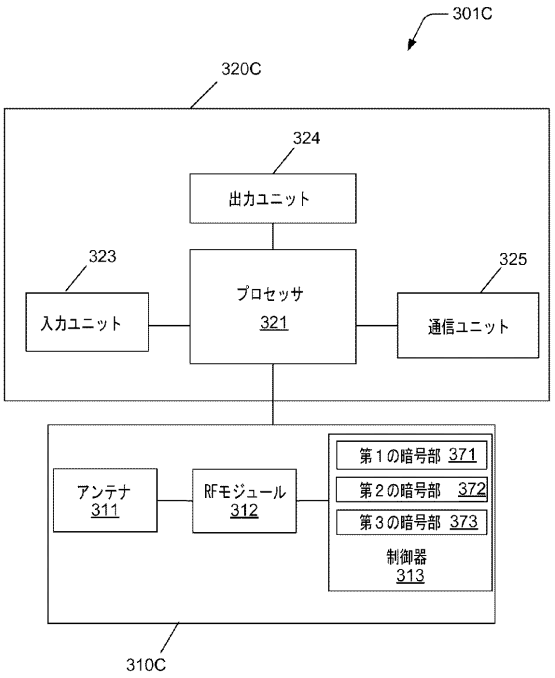
【図３Ａ】



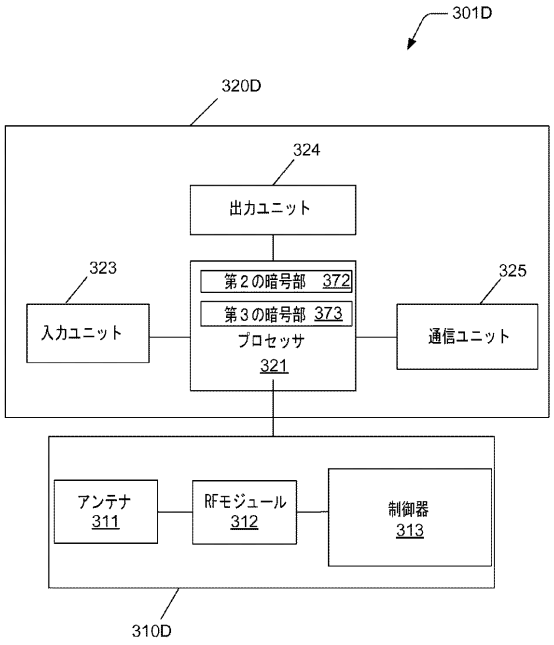
【図３Ｂ】



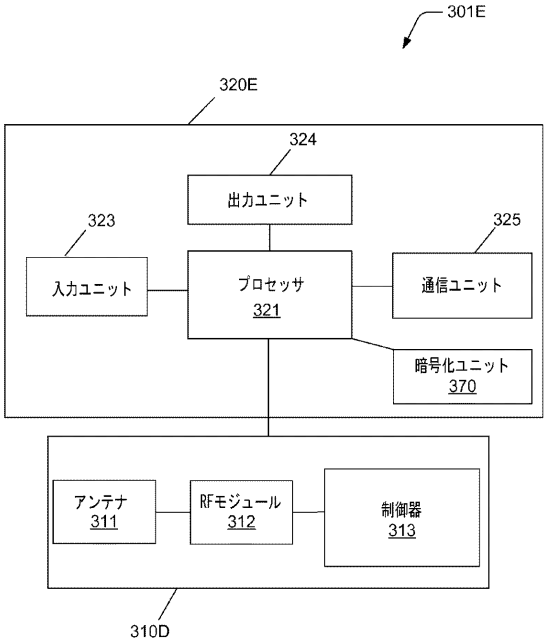
【図３Ｃ】



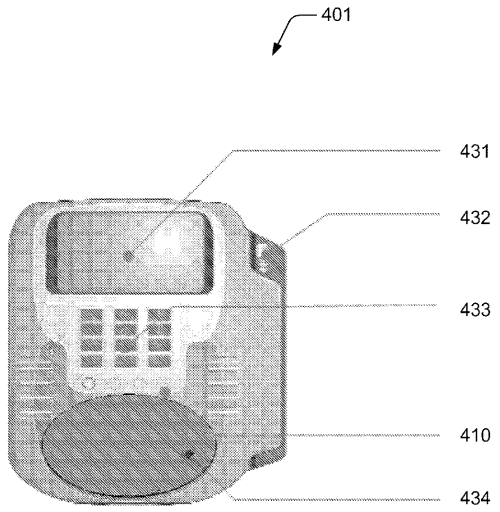
【図３Ｄ】



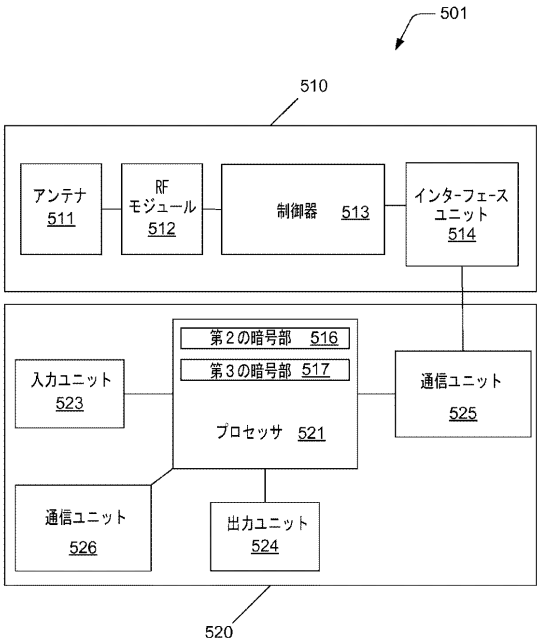
【図３Ｅ】



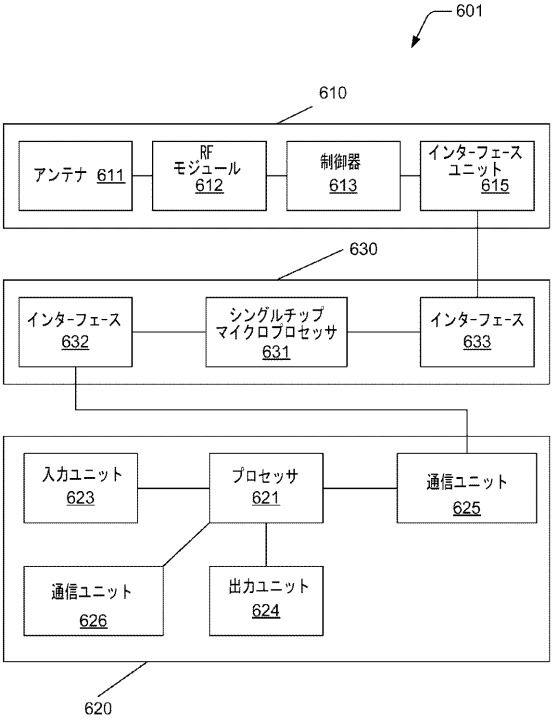
【図４】



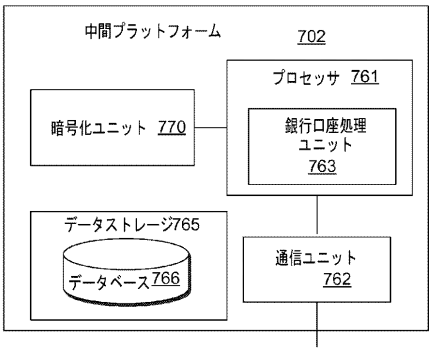
【図５】


501
510
アンテナ 511
RF モジュール 512
制御器 513
インターフェースユニット 514
第２の暗号部 516
第３の暗号部 517
入力ユニット 523
プロセッサ 521
通信ユニット 525
通信ユニット 526
出力ユニット 524
520

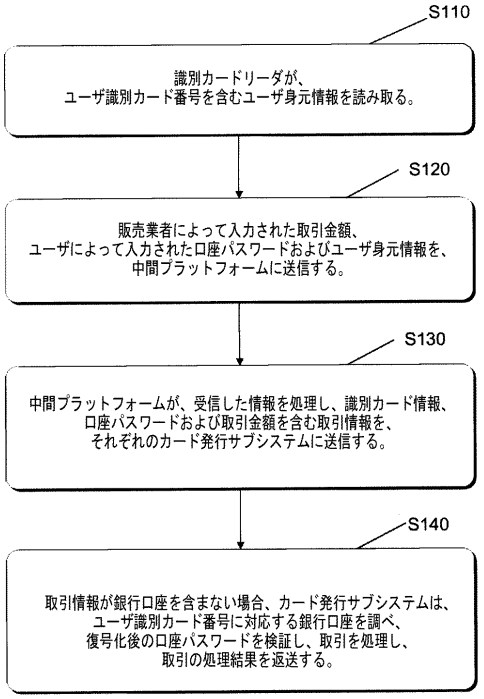
【図６】


601
610
アンテナ 611
RF モジュール 612
制御器 613
インターフェースユニット 615
630
インターフェース 632
シングルチップマイクロプロセッサ 631
インターフェース 633
入力ユニット 623
プロセッサ 621
通信ユニット 625
通信ユニット 626
出力ユニット 624
620

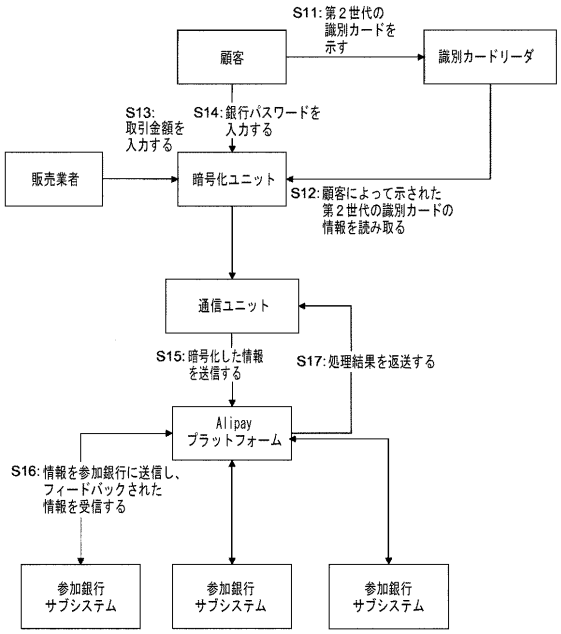
【図７】


中間プラットフォーム 702
プロセッサ 761
暗号化ユニット 770
銀行口座処理ユニット 763
データストレージ765
データベース 766
通信ユニット 762

【図８】


S110
識別カードリーダが、
ユーザ識別カード番号を含むユーザ身元情報を読み取る。
S120
販売業者によって入力された取引金額、
ユーザによって入力された口座パスワードおよびユーザ身元情報を、
中間プラットフォームに送信する。
S130
中間プラットフォームが、受信した情報を処理し、識別カード情報、
口座パスワードおよび取引金額を含む取引情報を、
それぞれのカード発行サブシステムに送信する。
S140
取引情報が銀行口座を含まない場合、カード発行サブシステムは、
ユーザ識別カード番号に対応する銀行口座を調べ、
復号化後の口座パスワードを検証し、取引を処理し、
取引の処理結果を返送する。

【図９】


S11:第２世代の
識別カードを
示す
顧客
識別カードリーダ
S13:
取引金額を
入力する
S14:銀行パスワードを
入力する
販売業者
暗号化ユニット
S12:顧客によって示された
第２世代の識別カードの
情報を読み取る
通信ユニット
S15:暗号化した情報
を送信する
S17:処理結果を返送する
Alipay
プラットフォーム
S16:情報を参加銀行に送信し、
フィードバックされた
情報を受信する
参加銀行
サブシステム
参加銀行
サブシステム
参加銀行
サブシステム

フロントページの続き

(51)Int.Cl.		F I			テーマコード（参考）
G07G 1/14	*(2006.01)*	G07G	1/12	321P	
		G07G	1/14		

(72)発明者 ユアン レイミン
中華人民共和国 310099 ジャージャン ハンチョウ ホアシン ロード ナンバー 99
イースト ソフトウェア パーク チュアンイェ マンション 6／エフ

Fターム(参考) 3E142 FA04 FA06 FA27 JA02
5B058 CA01 CA13 CA17 KA13 KA32 KA35 YA02 YA03