(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第5981507号
(P5981507)

(45)発行日　平成28年8月31日(2016.8.31)　(24)登録日　平成28年8月5日(2016.8.5)

(51)Int.Cl.		F I		
G06Q 20/40	(2012.01)	G06Q	20/40	300
G06Q 20/24	(2012.01)	G06Q	20/24	
G06Q 20/26	(2012.01)	G06Q	20/26	
G06Q 20/32	(2012.01)	G06Q	20/32	

請求項の数 16　外国語出願　(全 27 頁)

(21)出願番号　特願2014-184000 (P2014-184000)
(22)出願日　平成26年9月10日 (2014.9.10)
(65)公開番号　特開2015-62116 (P2015-62116A)
(43)公開日　平成27年4月2日 (2015.4.2)
審査請求日　平成26年10月22日 (2014.10.22)
(31)優先権主張番号　102132767
(32)優先日　平成25年9月11日 (2013.9.11)
(33)優先権主張国　台湾 (TW)
(31)優先権主張番号　103130383
(32)優先日　平成26年9月3日 (2014.9.3)
(33)優先権主張国　台湾 (TW)

(73)特許権者　512293389
楊　建綱
台湾台北市敦化南路二段６７號１９樓
(74)代理人　100099759
弁理士　青木　篤
(74)代理人　100092624
弁理士　鶴田　準一
(74)代理人　100114018
弁理士　南山　知広
(74)代理人　100165191
弁理士　河合　章
(74)代理人　100151459
弁理士　中村　健一
(72)発明者　楊　建綱
台湾台北市敦化南路二段６７號１９樓

最終頁に続く

(54)【発明の名称】支払いを処理する方法

(57)【特許請求の範囲】
【請求項１】
携帯支払装置（２）に取り外し可能に接続されるとともに銀行のサーバ（５）と通信を行う電子装置（１）を用いて実施される支払いを処理する方法において、前記携帯支払装置（２）は、プラグアンドプレイ装置であり、かつ、ペイメントカード（２２）が備えられ、
（ａ）前記電子装置（１）によって、取引及び取引に対する支払いに関連した取引情報を受信するステップと、
（ｂ）前記電子装置（１）によって、前記携帯支払装置（２）を介して前記ペイメントカード（２２）にアクセスするステップと、
（ｃ）前記電子装置（１）によって、少なくとも取引情報を含む支払コマンドを生成するよう前記ペイメントカード（２２）に協力するステップと、
（ｄ）前記電子装置（１）によって、前記銀行のサーバ（５）とのセッションを確立するステップであって、前記セッションは、前記電子装置（１）と前記銀行のサーバ（５）との間の安全な通信チャネルを提供するステップと、
（ｅ）前記電子装置（１）によって、ステップ（ｄ）で確立された前記セッションの下で前記銀行のサーバ（５）に支払コマンドを送信するステップであって、前記銀行のサーバ（５）は、支払コマンドの受信に応答して前記支払コマンドに基づいて前記ペイメントカード（２２）の有効性を確認するとともに前記ペイメントカード（２２）が有効であると確認した後に前記支払コマンドに含まれる取引情報に従って支払いを処理するよう構成

されるステップと、
（ｆ）前記電子装置（１）によって、前記ステップ（ｄ）で確立された前記セッションの下で前記銀行のサーバ（５）から支払結果を受信するステップであって、前記支払結果は、支払いを完了した後に前記銀行のサーバ（５）によって生成されるステップと、
を備え、
ステップ（ｄ）は、
（ｄ１）前記電子装置（１）によって、前記ペイメントカード（２２）からバーチャル口座を取得するサブステップであって、前記バーチャル口座は、前記携帯支払装置（２）のユーザと前記銀行のサーバ（５）を操作する銀行との間にあり、かつ、前記支払いのために用いられる銀行預金口座に関連するサブステップと、
（ｄ２）前記電子装置（１）によって、セッション要求を前記銀行のサーバ（５）に送信するサブステップであって、前記セッション要求は前記バーチャル口座を有するサブステップと、
（ｄ３）前記銀行のサーバ（５）によって、前記セッション要求の受信に応答してセッション識別（ＩＤ）を生成するとともに前記セッションＩＤを前記電子装置（１）に送信するサブステップと、
（ｄ４）前記電子装置（１）によって、前記セッションＩＤを前記ペイメントカード（２２）に送信するサブステップであって、前記ペイメントカード（２２）は、前記セッションＩＤに基づいて、第１の認証コード及び前記ペイメントカード（２２）に格納されるカード識別鍵を生成し、前記第１の認証コードを前記電子装置（１）に送信するように構成されるサブステップと、
（ｄ５）前記電子装置（１）によって、前記第１の認証コードを前記銀行のサーバ（５）に送信するサブステップと、
（ｄ６）前記銀行のサーバ（５）によって、サブステップ（ｄ２）で前記電子装置（１）から受信した前記セッション要求に含まれる前記バーチャル口座に従って、格納されたユーザ識別鍵を見つけ出すサブステップであって、前記ユーザ識別鍵は、前記カード識別鍵に対応し、前記バーチャル口座に専用のものであるサブステップと、
（ｄ７）前記銀行のサーバ（５）によって、サブステップ（ｄ３）で生成した前記セッションＩＤ及びサブステップ（ｄ６）で見つけた前記ユーザ識別鍵に基づいて、第２の認証コードを生成するサブステップと、
（ｄ８）前記銀行のサーバ（５）によって、サブステップ（ｄ５）で前記電子装置（１）から受信した前記第１の認証コードがサブステップ（ｄ７）で生成した前記第２の認証コードに一致するか否かを決定するサブステップと、
（ｄ９）前記第１の認証コードが前記第２の認証コードに一致することをサブステップ（ｄ８）で決定したときに前記セッションを確立するために、前記銀行のサーバ（５）によって、セッション応答を前記電子装置（１）に送信するサブステップと、
を有することを特徴とする方法。
【請求項２】
携帯支払装置（２）に取り外し可能に接続されるとともに銀行のサーバ（５）と通信を行う電子装置（１）を用いて実施される支払いを処理する方法において、前記携帯支払装置（２）は、プラグアンドプレイ装置であり、かつ、ペイメントカード（２２）が備えられ、
（ａ）前記電子装置（１）によって、取引及び取引に対する支払いに関連した取引情報を受信するステップと、
（ｂ）前記電子装置（１）によって、前記携帯支払装置（２）を介して前記ペイメントカード（２２）にアクセスするステップと、
（ｃ）前記電子装置（１）によって、少なくとも取引情報を含む支払コマンドを生成するよう前記ペイメントカード（２２）に協力するステップと、
（ｄ）前記電子装置（１）によって、前記銀行のサーバ（５）とのセッションを確立するステップであって、前記セッションは、前記電子装置（１）と前記銀行のサーバ（５）

との間の安全な通信チャネルを提供するステップと、
（ｅ）前記電子装置（１）によって、ステップ（ｄ）で確立された前記セッションの下で前記銀行のサーバ（５）に支払コマンドを送信するステップであって、前記銀行のサーバ（５）は、支払コマンドの受信に応答して前記支払コマンドに基づいて前記ペイメントカード（２２）の有効性を確認するとともに前記ペイメントカード（２２）が有効であると確認した後に前記支払コマンドに含まれる取引情報に従って支払いを処理するよう構成されるステップと、
（ｆ）前記電子装置（１）によって、前記ステップ（ｄ）で確立された前記セッションの下で前記銀行のサーバ（５）から支払結果を受信するステップであって、前記支払結果は、支払いを完了した後に前記銀行のサーバ（５）によって生成されるステップと、
を備え、
ステップ（ｂ）は、
（ｂ１）前記携帯支払装置（２）が前記電子装置（１）に接続されたときに、前記電子装置（１）によって、前記ペイメントカード（２２）が検出されたか否かを決定するステップと、
（ｂ２）前記ペイメントカード（２２）が検出されたことの決定に応答して、前記電子装置（１）によって、アクセスパスワードの入力をユーザに要求する命令を出力するステップと、
（ｂ３）前記アクセスパスワードの受信に応答して、前記電子装置（１）によって、前記アクセスパスワードを前記ペイメントカード（２２）に送信するステップであって、前記ペイメントカード（２２）は、前記アクセスパスワードを確認するとともに前記アクセスパスワードが正しいときにアクセス許可命令を前記電子装置（１）に送信するように構成されるステップと、
（ｂ４）前記アクセス許可命令の受信に応答して、前記電子装置（１）によって、格納されたアクセスパスワードを一時的にクリアにするステップと、
を有することを特徴とする方法。
【請求項３】
ステップ（ｃ）は、
（ｃ１）前記電子装置（１）によって、認証すべきデータを前記ペイメントカード（２２）に送信するサブステップであって、前記認証すべきデータは前記取引情報を有し、前記ペイメントカード（２２）は、前記認証すべきデータに基づいて取引認証コード（ＴＡＣ）を生成するとともに前記ＴＡＣを前記電子装置（１）に送信するように構成されるサブステップと、
（ｃ２）前記電子装置（１）によって、前記ＴＡＣを用いて前記支払コマンドを構成するサブステップと、
を有することを特徴とする請求項１と２のうちのいずれか一項に記載の方法。
【請求項４】
前記ペイメントカード（２２）は、前記ペイメントカード（２２）に格納された秘密鍵を用いて前記ＴＡＣを生成するように構成され、ステップ（ｅ）において、前記銀行のサーバ（５）は、
同一の秘密鍵を用いて、前記支払コマンドに含まれる前記認証すべきデータを用いながら確認コードを生成し、
前記ＴＡＣと前記確認コードとを比較することによって、
前記ペイメントカード（２２）の有効性を確認することを特徴とする請求項３に記載の方法。
【請求項５】
ステップ（ａ）の後に、取引情報で行われる調整を無効にするステップを更に備えることを特徴とする請求項１から４のうちのいずれか一項に記載の方法。
【請求項６】
電子装置（１）を有するシステム（１）であって、前記電子装置（１）は、

プロセッサ（１１）と、
前記プロセッサ（１１）に結合され、トランザクションアプリケーション（１２０）を格納する記憶装置（１２）と、
前記プロセッサ（１１）に結合された第１の接続インタフェース（１３）と、
前記プロセッサ（１１）に結合され、銀行のサーバ（５）と通信を行うように構成された通信装置（１５）と、
プラグアンドプレイ装置であり、前記電子装置（１）に取り外し可能に接続された携帯支払装置（２）と、を有し、前記携帯支払装置（２）は、
ペイメントカード（２２）を含むためのカードインタフェースを設けたカードスロット（２０１）と、
前記電子装置（１）の前記第１の接続インタフェース（１３）に電気的に接続して、前記電子装置（１）を用いた前記ペイメントカード（２２）へのアクセスを可能にする第２の接続インタフェース（２３）と、を有するシステム（１００）において、
前記トランザクションアプリケーション（１２０）は、前記プロセッサ（１１）によって実行されるときに、請求項１と２のうちのいずれか一項の方法を実行するように前記電子装置（１）を前記ペイメントカード（２２）及び前記銀行のサーバ（５）に協力させることを特徴とするシステム（１００）。
【請求項７】
前記電子装置（１）は、現金自動預け払い機（ＡＴＭ）であり、少なくとも現金自動支払機を有する入出力（Ｉ／Ｏ）装置（１４）を更に有することを特徴とする請求項６に記載のシステム（１００）。
【請求項８】
前記電子装置（１）は、自動販売機であり、少なくとも物理的／仮想的なボタン及び商品ディスペンサーを有する入出力（Ｉ／Ｏ）装置（１４）を更に有することを特徴とする請求項６に記載のシステム（１００）。
【請求項９】
プロセッサ（１１）と、
前記プロセッサ（１１）に結合され、トランザクションアプリケーション（１２０）を格納する記憶装置（１２）と、
前記プロセッサ（１１）に結合され、ペイメントカード（２２）が設けられた携帯支払装置（２）に取り外し自在に結合するための第１の接続インタフェース（１３）と、
前記プロセッサ（１１）に結合され、銀行のサーバ（５）と通信を行うように構成された通信装置（１５）と、
を有する電子装置（１）において、
前記トランザクションアプリケーション（１２０）は、前記プロセッサ（１１）によって実行されるときに、請求項１と２のうちのいずれか一項の方法を実行するように前記電子装置（１）を前記ペイメントカード（２２）及び前記銀行のサーバ（５）に協力させることを特徴とする電子装置（１）。
【請求項１０】
前記電子装置（１）は、現金自動預け払い機（ＡＴＭ）であり、少なくとも現金自動支払機を有する入出力（Ｉ／Ｏ）装置（１４）を更に有することを特徴とする請求項９に記載の電子装置（１）。
【請求項１１】
前記電子装置（１）は、自動販売機であり、少なくとも物理的／仮想的なボタン及び商品ディスペンサーを有する入出力（Ｉ／Ｏ）装置（１４）を更に有することを特徴とする請求項９に記載の電子装置（１）。
【請求項１２】
電子装置（１）に結合されたペイメントカード（２２）であって、前記電子装置（１）は、前記ペイメントカード（２２）に対してパーソナライゼーションプロセスを実行するためにアプリケーション（１２０）を実行し、前記ペイメントカード（２２）は、

コントローラチップ（２２２）、コントローラファームウェア（２２４）及びアプリケーションプログラムインタフェース（ＡＰＩ）（２２３）を有する制御モジュール（２２０）と、
所定のオーソライゼーションシーケンスが行われた後のみ前記コントローラファームウェア（２２４）及び前記ＡＰＩ（２２３）を介して前記アプリケーション（１２０）にアクセスすることができる隠し領域（２２８）を有する記憶装置（２２５）と、
を有するペイメントカード（２２）において、
前記隠し領域（２２８）は、複数の隠しデータブロック（５Ａ～５Ｈ）に分割され、前記隠しデータブロック（５Ａ～５Ｈ）の各々は、ストレージセキュリティレベルに関連し、かつ、予め決定されたデータタイプのパーソナライゼーションデータを格納するように構成され、
前記隠しデータブロック（５Ａ～５Ｈ）の各々に対して、前記コントローラチップ（２２２）は、前記隠しデータブロックの前記ストレージセキュリティレベルに対応する複数のセキュリングメカニズムのうちの予め決定されたセキュリングメカニズムによって前記パーソナライゼーションデータを格納するためのパーソナライゼーションプロセスを実行するように構成されることを特徴とするペイメントカード（２２）。
【請求項１３】
前記パーソナライゼーションプロセスは、
前記パーソナライゼーションデータを記憶するのに用いるために前記隠しデータブロック（５Ａ～５Ｈ）の一つを選択する登録ステップと、
前記パーソナライゼーションデータを格納できるようにするために、前記隠しデータブロック（５Ａ～５Ｈ）のうちの指定された隠しデータブロックを、前記予め決定されたデータタイプに一致するようにフォーマットするフォーマットステップと、
前記ペイメントカード（２２）が、前記隠しデータブロック（５Ａ～５Ｈ）のうちの指定された隠しデータブロックに前記パーソナライゼーションデータを格納するパーソナライゼーションステップと、
を有することを特徴とする請求項１２記載のペイメントカード（２２）。
【請求項１４】
前記隠しデータブロック（５Ａ～５Ｈ）の各々は、複数の隠しデータサブブロックに分割され、前記登録ステップにおいて、前記ペイメントカード（２２）は、前記パーソナライゼーションデータを記憶するのに用いるために、前記隠しデータブロック（５Ａ～５Ｈ）のうちの指定された隠しデータブロックの前記隠しデータサブブロックのうちの一つを更に指定し、前記フォーマットステップにおいて、前記隠しデータサブブロックのうちの指定された隠しデータサブブロックをフォーマットし、
前記隠しデータサブブロックの各々は、前記登録ステップを許可するための前もってセットした登録ＩＤ／パスワードの組合せ及び前記フォーマットステップを許可するための前もってセットしたフォーマットＩＤ／パスワードの組合せが格納され、
前記ペイメントカード（２２）は、登録許可ＩＤ／パスワードの組合せを受信し、前記登録許可ＩＤ／パスワードの組合せが前記前もってセットした登録許可ＩＤ／パスワードの組合せと一致するときのみ前記登録ステップを実行し、
前記ペイメントカード（２２）は、フォーマット許可ＩＤ／パスワードの組合せを受信し、前記フォーマット許可ＩＤ／パスワードの組合せが前記前もってセットしたフォーマット許可ＩＤ／パスワードの組合せと一致するときのみ前記フォーマットステップを実行することを特徴とする請求項１３に記載のペイメントカード（２２）。
【請求項１５】
前記ペイメントカード（２２）は、第１のセキュリングメカニズム、第２のセキュリングメカニズム、第３のセキュリングメカニズム及び第４のセキュリングメカニズムのうちの一つに従って前記パーソナライゼーションプロセスを実行し、
前記第１のセキュリングメカニズムにおいて、前記登録許可ＩＤ／パスワードの組合せ、前記フォーマット許可ＩＤ／パスワードの組合せ及び前記パーソナライゼーションデー

タをプラットホームサーバ（３）から受信し、
前記第２のセキュリングメカニズムにおいて、前記登録許可ＩＤ／パスワードの組合せ及び前記パーソナライゼーションデータを前記プラットホームサーバ（３）から受信し、前記フォーマット許可ＩＤ／パスワードの組合せを、前記フォーマット許可ＩＤ／パスワードの組合せを提供するために前記プラットホームサーバ（３）によって許可される許可された組織サーバ（３２）から受信し、
前記第３のセキュリングメカニズムにおいて、前記登録許可ＩＤ／パスワードの組合せ及び前記パーソナライゼーションデータを前記プラットホームサーバ（３）から受信し、前記フォーマット許可ＩＤ／パスワードの組合せを、第三者から受信し、前記フォーマット許可ＩＤ／パスワードの組合せを、前記プラットホームサーバ（３）及び協力する組織サーバ（３３）によって協力して生成し、
前記第４のセキュリングメカニズムにおいて、前記登録許可ＩＤ／パスワードの組合せ及び前記フォーマット許可ＩＤ／パスワードの組合せを前記プラットホームサーバ（３）から受信し、前記パーソナライゼーションデータを、前記コントローラファームウェア（２２４）及び前記ＡＰＩ（２２３）を介して前記アプリケーション（１２０）から受信することを特徴とする請求項１４に記載のペイメントカード（２２）。
【請求項１６】
前記登録ステップは、
登録コマンドの受信に応答して、前記隠しデータブロック（５Ａ～５Ｈ）のうちの一つから分割した隠しデータサブブロックを指定するサブステップと、
前記隠しデータブロック（５Ａ～５Ｈ）のうちの指定された隠しデータブロックの前記セキュリングメカニズムの一つの下で操作する第一者からフォーマット許可ＩＤ／パスワードの組合せを受信するサブステップと、
を有し、
前記フォーマットステップにおいて、受信したフォーマット許可ＩＤ／パスワードの組合せが前もってセットしたフォーマット許可ＩＤ／パスワードの組合せと一致することを決定したときに、指定された隠しデータサブブロックをフォーマットし、
前記パーソナライゼーションステップにおいて、前記指定された隠しデータサブブロックに前記パーソナライゼーションデータを格納することを特徴とする請求項１３に記載のペイメントカード（２２）。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、支払いを処理する方法に関し、更に詳しくは、支払いを処理するためのプラグアンドプレイ装置を用いる方法に関する。
【背景技術】
【０００２】
現在、商品及び／又はサービスの支払いを、プラスチック製メモリカード（例えば、クレジットカード、デビットカード等）を用いて行うことができる。プラスチック製メモリカードを支払いの手段として受け入れるために、商店主は、カード発行者（例えば、銀行）と合意するとともにカード発行者とやり取りをするための処理装置（例えば、ペイメントカードを読み取ることができるカードリーダ）を提供する必要がある。その結果、低収益及び／又は低利益幅で活動する商店主は、プラスチック製メモリカードを受け入れることに消極的になるかもしれない。
【０００３】
オンライン取引に関して、クレジットカードを用いたオンライン決済は、一般的にパーソナルコンピュータ又はモバイル機器（例えば、スマートホン）で実行される。オンライン決済を実行するとき、ユーザは、先ず、ユーザ名及びユーザの身元を確認するための関連のパスワードを含む個人の情報をインタフェース（例えば、パーソナルコンピュータに表示されたウェブページ）を介して入力するよう命令される。ユーザの身元が確認された

後に、インタフェースは、カード番号、有効期限等を含むことができるクレジットカード情報を入力するようユーザに対して更に命令する。そのような支払いを実行するための従来のシステムは、例えば、台湾特許第４７３６８１号及び台湾特許公開第２００８１６０９９号で開示されているように見ることができる。

【０００４】

しかしながら、コンピュータ又はモバイル機器が利用できない又は（インターネット接続がない又は不十分な電力のような理由のために）機能しない場合、オンライン決済を行うことができなくなることがある。

【発明の概要】

【発明が解決しようとする課題】

【０００５】

したがって、本発明の目的は、上述した従来技術の欠点に対処することができる方法を提供することである。

【課題を解決するための手段】

【０００６】

その結果、本発明の方法は、支払いを処理するためのものである。方法は、携帯支払装置に取り外し可能に接続されるとともに銀行のサーバと通信を行う電子装置を用いて実施される。携帯支払装置は、プラグアンドプレイ装置であり、かつ、ペイメントカードが備えられる。方法は、

（ａ）電子装置によって、取引及び取引に対する支払いに関連した取引情報を受信することと、

（ｂ）電子装置によって、携帯支払装置を介してペイメントカードにアクセスすることと、

（ｃ）電子装置によって、少なくとも取引情報を含む支払コマンドを生成するようペイメントカードに協力することと、

（ｄ）電子装置によって、銀行のサーバとのセッションを確立することであって、セッションは、電子装置と銀行のサーバとの間の安全な通信チャネルを提供することと、

（ｅ）電子装置によって、ステップ（ｄ）で確立されたセッションの下で銀行のサーバに支払コマンドを送信することであって、銀行のサーバは、支払コマンドの受信に応答して支払コマンドに基づいてペイメントカードの有効性を確認するとともにペイメントカードが有効であると確認した後に支払コマンドに含まれる取引情報に従って支払いを処理するよう構成されることと、

（ｆ）電子装置によって、ステップ（ｄ）で確立されたセッションの下で銀行のサーバから支払結果を受信することであって、支払結果は、支払いを完了した後に銀行のサーバによって生成されることと、

を備える。

【０００７】

本発明の他の目的は、上述した方法を実行するために銀行のサーバと通信を行うように構成されたシステムを提供する。

【０００８】

その結果、本発明のシステムは、電子装置及び携帯支払装置を有する。

【０００９】

電子装置は、プロセッサと、プロセッサに結合するとともにトランザクションアプリケーションを格納する記憶装置と、プロセッサに結合した第１の接続インタフェースと、プロセッサに結合するとともに銀行のサーバと通信を行うように構成された通信装置と、を有する。

【００１０】

携帯支払装置は、プラグアンドプレイ装置であり、電子装置に取り外し可能に接続される。携帯支払装置は、ペイメントカードを含むためにカードインタフェースが設けられたカードスロットと、電子装置の第１の接続インタフェースに電気的に接続され、電子装置

を用いたペイメントカードのアクセスを可能にする第２の接続インタフェースと、を有する。

【００１１】

トランザクションアプリケーションにより、プロセッサによって実行されるときに、電子装置は、本発明の方法を実行するようペイメントカード及び銀行のサーバに協力する。

【００１２】

本発明の更に別の目的は、方法を実行することができる電子装置を提供することである。

【００１３】

その結果、本発明の電子装置は、プロセッサと、プロセッサに結合するとともにトランザクションアプリケーションを格納する記憶装置と、プロセッサに結合するとともにペイメントカードが設けられた携帯支払装置に取り外し可能に結合する第１の接続インタフェースと、プロセッサに結合するとともに銀行のサーバと通信を行うように構成された通信装置と、を有する。

【００１４】

トランザクションアプリケーションにより、プロセッサによって実行されるときに、電子装置は、本発明の方法を実行するようペイメントカード及び銀行のサーバに協力する。

【００１５】

本発明の更に別の目的は、異なるソースからのデータを管理する種々のセキュリングメカニズムを用いるように構成されたペイメントカードを提供することである。

【００１６】

その結果、本発明のペイメントカードは、ペイメントカードに対するパーソナライゼーションプロセスを実行するためのアプリケーションを実行する電子装置に結合される。ペイメントカードは、制御モジュール及び記憶装置を有する。

【００１７】

制御モジュールは、コントローラチップ、コントローラファームウェア及びアプリケーションプログラムインタフェース（ＡＰＩ）を有する。

【００１８】

記憶装置は、所定のオーソライゼーションシーケンスが行われた後のコントローラファームウェア及びＡＰＩを介したアプリケーションへのアクセスのみが可能な隠し領域を有する。

【００１９】

隠し領域は、複数の隠しデータブロックに分割される。隠しデータブロックの各々は、ストレージセキュリティレベルに関連し、予め決定されたデータタイプのパーソナライゼーションデータを記憶するように構成される。

【００２０】

隠しデータブロックの各々に対して、コントローラチップは、隠しデータブロックのストレージセキュリティレベルに対応する複数のセキュリングメカニズムの予め決定されたものとともにパーソナライゼーションデータを格納するパーソナライゼーションプロセスを実行するよう構成される。

【図面の簡単な説明】

【００２１】

本発明の他の特徴及び利点は、添付図面に関連する好適な実施の形態の以下の詳細な説明で明らかになるであろう。

【図１】図１は、本発明によるシステムの好適な実施の形態のブロック図である。

【図２】図２は、図１のシステムの種々の電子装置と通信を行うように構成されたインタフェース機器の略図である。

【図３Ａ】図３Ａは、図１のシステムを用いて支払いを処理する方法のステップを示すフローチャートである。

【図３Ｂ】図３Ｂは、図１のシステムを用いて支払いを処理する方法のステップを示すフ

ローチャートである。
【図３Ｃ】図３Ｃは、図１のシステムを用いて支払いを処理する方法のステップを示すフローチャートである。
【図４】図４は、方法の種々の段階において電子装置の入出力装置によって出力される種々のメッセージを示す。
【図５】図５は、方法の種々の段階において電子装置の入出力装置によって出力される種々のメッセージを示す。
【図６】図６は、方法の種々の段階において電子装置の入出力装置によって出力される種々のメッセージを示す。
【図７】図７は、方法の種々の段階において電子装置の入出力装置によって出力される種々のメッセージを示す。
【図８】図８は、本発明によるペイメントカードの記憶装置のブロック図である。
【図９】図９は、本発明によるペイメントカードのパーソナライゼーションプロセスのフローチャートである。
【図１０】図１０は、第１のセキュリングメカニズムを用いて実施されるパーソナライゼーションプロセスのフローチャートである。
【図１１】図１１は、第２のセキュリングメカニズムを用いて実施されるパーソナライゼーションプロセスのフローチャートである。
【図１２】図１２は、第３のセキュリングメカニズムを用いてパーソナライゼーションプロセスを実施するための情報を生成するためにプラットホームサーバ及び組織サーバに協力する銀行のサーバを示すフローチャートである。
【図１３Ａ】図１３Ａは、第３のセキュリングメカニズムを用いて実施されるパーソナライゼーションプロセスのフローチャートである。
【図１３Ｂ】図１３Ｂは、第３のセキュリングメカニズムを用いて実施されるパーソナライゼーションプロセスのフローチャートである。
【図１４Ａ】図１４Ａは、第４のセキュリングメカニズムを用いて実施されるパーソナライゼーションプロセスのフローチャートである。
【図１４Ｂ】図１４Ｂは、第４のセキュリングメカニズムを用いて実施されるパーソナライゼーションプロセスのフローチャートである。
【発明を実施するための形態】
【００２２】
図１に示すように、本発明によるシステム１００の好適な実施の形態は、取引に関連した支払いを処理する方法を実施するためのものである。システム１００は、銀行のサーバ５と通信を行うことができる電子装置１と、ペイメントカード２２が設けられ、電子装置１に取り外し可能に接続され、かつ、電子装置１にペイメントカード２２を結合するためのインタフェース機器としての役割を果たす携帯支払装置２と、を有する。
【００２３】
本実施の形態において、電子装置１を、パーソナルコンピュータ、ラップトップコンピュータ、タブレット型コンピュータ、モバイル機器、現金自動預け払い機（ＡＴＭ）及び自動販売機のうちの一つを用いて具体化することができる（図２参照）。パーソナルコンピュータ、ラップトップコンピュータ、タブレット型コンピュータ及びモバイル機器は顧客と商店主のいずれかの所有とすることができることに留意されたい。電子装置１は、支払いを処理する方法を電子装置１に実行させるように設計されたアプリケーションを実行するネットワーク接続及びメカニズムを有する必要がある。
【００２４】
電子装置１は、ネットワーク上で銀行のサーバ５と通信を行うよう作動する。銀行のサーバ５を、ペイメントカードを顧客に発行するマスターバンク又はメンバーバンクによって操作することができる。本実施の形態において、銀行のサーバ５は、電子装置と通信を行うためのプラットホームサーバ３と、プラットホームサーバ３に結合される銀行システム４と、を有する。種々の実施の形態において、プラットホームサーバ３及び銀行システ

ム４を、単一の構成要素（例えば、サーバ）として統合し又は専用のチャネル若しくはセッション上で通信を行う二つの個別の構成要素として実現することができる。プラットホームサーバ３及び銀行システム４を個別の構成要素として実現する場合、プラットホームサーバ３を、銀行以外の第三者によって操作することができる。

【００２５】

電子装置１は、プロセッサ１１と、プロセッサ１１に結合されるとともにトランザクションアプリケーション１２０を格納する記憶装置１２と、プロセッサ１１に結合される第１の接続インタフェース１３と、プロセッサ１１に結合される入出力（Ｉ／Ｏ）装置１４と、プロセッサ１１に結合される通信装置１５と、を有する。

【００２６】

本実施の形態において、第１のコネクタ１３を、ユニバーサルシリアルバス（ＵＳＢ）２．０，ＵＳＢ３．０，ＭｉｎｉＵＳＢ又はＵＳＢポートを用いて具体化することができる。Ｉ／Ｏ装置１４は、マウス／キーボードの組合せ、タッチスクリーン、スピーカ／ディスプレイの組合せ又はその組み合わせを有することができるが、それに限定されない。電子装置１が自動販売機を用いて具体化される場合、Ｉ／Ｏ装置１４は、複数の物理的／仮想的なボタン、コントロールパネル、商品ディスペンサー又はその組み合わせを有することができる。電子装置を現金自動預け払い機（ＡＴＭ）を用いて具体化する場合、Ｉ／Ｏ装置１４は、タッチスクリーン、キーボード及び現金自動支払機を有することができる。

【００２７】

携帯支払装置２は、プラグアンドプレイ装置（例えば、ユニバーサルシリアルバス（ＵＳＢ）２．０，ＵＳＢ３．０，ＭｉｎｉＵＳＢ又はＵＳＢ接続を有する装置）を用いて具体化される。携帯支払装置２は、支払いを処理する方法を実行するために電子装置１に取り外し可能に接続される。

【００２８】

携帯支払装置２を、ポケット又は財布に合う及び／又は装備品として財布、携帯機器等の他の物に取り付けるように十分に寸法を決めることができる。携帯支払装置２は、カードスロット２０１とともに形成されたハウジング２０と、ハウジング２０に配置された回路基板２１と、回路基板２１の上に配置されるとともに電子装置１の第１の接続インタフェース１３に電気的に接続されるように構成された第２の接続インタフェース２３と、を有する。カードスロット２０１には、ペイメントカード２２を含むためのカードインタフェースが設けられる。カードインタフェースは、ペイメントカード２２と第２の接続インタフェース２３との間の通信インタフェースを提供し、その結果、携帯支払装置２が電子装置１に結合されたときに、ペイメントカード２２に対するアクセスが、電子装置１を用いることによって可能になる。ペイメントカード２２が携帯支払装置２に接続されないときに携帯支払装置２に演算機能が設けられないことに留意されたい。

【００２９】

本実施の形態において、ペイメントカード２２は、マイクロセキュアデジタル（ＳＤ）カードを用いることによって具体化される。ペイメントカード２２は、制御モジュール２２０と、財務データチップ２２１と、記憶装置２２５と、を有する。財務データチップ２２１（図１参照）は、ＦＩＳＣ　ＩＩ仕様によりコンパイルできる。

【００３０】

制御モジュール２２０は、コントローラチップ２２２と、読み出し専用メモリ（ＲＯＭ）（図示せず）に配置されたコントローラファームウェア２２４と、アプリケーションプログラミングインタフェース（ＡＰＩ）２２３と、を有する。コントローラチップ２２２及びＲＯＭを、集積回路パッケージングを用いて集積することができ、かつ、記憶装置２２５と並置することができる。

【００３１】

携帯支払装置２が電子装置１に結合されるとき、プロセッサ１１は、コントローラファームウェア２２４を通じて財務データチップ２２１及び記憶装置２２５にアクセスするよ

う作動する。ＡＰＩ２２３及び制御ファームウェア２２４は、トランザクションアプリケーション１２０の命令に従って動作することができる。ＡＰＩ２２３は、トリプルデータ暗号化アルゴリズム対象鍵ブロック暗号（３ＤＥＳ）、高度暗号化標準（ＡＥＳ）、ＲＳＡ暗号等のアルゴリズムを用いて暗号化を実行できる機能を有する。

【００３２】

記憶装置２２５は、システム部２２６と、記憶部２２７と、を有する。システム部２２６は、基本操作情報によって構築される。記憶部２２７は、隠し領域２２８と、可視領域２２９と、を有する。可視領域２２９は、電子装置１のオペレーティングシステム（ＯＳ）によるアクセスを許可する。例えば、マイクロソフトのウィンドウズ（登録商標）システムについては、ファイル管理プログラムを用いることによって、可視領域２２９にアクセスすることができる。

【００３３】

隠し領域２２８は、ＯＳにアクセスすることができず、隠し領域２２８に格納されたファイルの内容のＯＳを介した読出し、書込み又は変更のような動作を実行することを許可されない。代わりに、隠し領域２２８は、所定のオーソライゼーションシーケンスが行われた後のコントローラファームウェア２２４を介したトランザクションアプリケーション１２０へのアクセスのみが可能である。具体的に説明すると、携帯支払装置２が電子装置１に結合されるとき、コントローラファームウェア２２４は、可視領域２２９のみが検出されることをＯＳに報告する。その結果、ＯＳは、隠し領域２２８をユーザに対して表示しない。隠し領域２２８は、ユーザがトランザクションアプリケーション１２０を実行するときのみアクセス可能であり、オーソライゼーションシーケンスをパスする。オーソライゼーションシーケンスに関する詳細は当業者によって容易に理解することができるので、簡潔のためにここでは詳細を論じない。

【００３４】

隠し領域２２８は、携帯支払装置２のユーザと銀行のサーバ５を操作する銀行との間にある銀行預金口座に関連したバーチャル口座を格納する。銀行預金口座に関するデータは、財務データチップ２２１に格納される。実際には、隠し領域２２８は、複数の銀行預金口座にそれぞれ関連した複数のバーチャル口座を格納することができる。

【００３５】

さらに、図３Ａを参照しながら、支払いを処理する方法の実施の形態を説明する。以下の例において、電子装置１を、コンピュータを用いて実現することができ、取引を、台湾高速鉄道の乗車券の購入とする。

【００３６】

最初に、ユーザは、乗車券の購入を処理するウェブサイトに接続するために電子装置１を操作することができる（図４参照）。ウェブサイトは、取引及び取引に対する支払に関連した取引情報を入力するためのインタフェースをユーザに提供することができる。ここで、取引情報は、旅行に関する詳細（例えば、ユーザ、出発時刻、出発地、行き先、鉄道運賃等の情報）を含む。

【００３７】

取引情報がユーザによって与えられた後、ウェブサイトは、支払いを行うための複数の方法（例えば、コンビニエンスストア又は鉄道駅での支払い、通常のクレジットカード又はペイメントカード２２の使用）をユーザに提供する。ここでは、この場合において、ユーザは、ペイメントカード２２を用いた支払いを行うことを選択する。それに応じて、電子装置１のプロセッサ１１は、トランザクションアプリケーション１２０を実行するよう作動する（ステップＳ１１）。

【００３８】

ステップＳ１２において、プロセッサ１１は、取引情報を受信する。その後、プロセッサ１１は、ステップＳ１３において認証すべきデータを生成するとともにステップＳ１４において取引情報で行われる調整を無効にするためにトランザクションアプリケーション１２０に含まれるセキュリティ機能１２１を実行する。具体的に説明すると、認証すべき

データは、取引情報を含み、ステップＳ１４の後、ユーザは、取引情報に任意の変更を行うことを許可されない。ステップＳ１３及びステップＳ１４を任意の順序で実行でき又は同時に実行できることに留意されたい。

【００３９】

その後、プロセッサ１１は、（ペイメントカード２２が設けられた）携帯支払装置２を電子装置１に接続するためにユーザに対する命令を生成する（図５参照）。ステップＳ１５でプロセッサ１１が携帯支払装置２を通じてペイメントカード２２を検出するとき、フローはステップＳ１６に進む。そうでない場合、プロセッサ１１は、携帯支払装置２が接続されるまでアイドル状態になる。

【００４０】

ステップＳ１６において、プロセッサ１１は、Ｉ／Ｏ装置１４を介して、確認のためにユーザに対して再び取引情報を出力し、ペイメントカード２２に格納されたバーチャル口座のリストを、選択のためにユーザに提供する。具体的に説明すると、ペイメントカード２２は、先ず、マスターバンクに関連したマスターバーチャル口座を格納し、種々のメンバーバンクに関連した追加のメンバーバーチャル口座を格納することができる。

【００４１】

バーチャル口座の一つを選択した後、ステップＳ１７において、プロセッサ１１は、ペイメントカード２２に関連したアクセスパスワードのユーザ入力を指示する命令を出力する（図６参照）。

【００４２】

アクセスパスワードの受信（ステップＳ１８）後、プロセッサ１１は、次に、アクセスパスワードを、第１の接続インタフェース１３及び第２の接続インタフェース２３を通じてペイメントカード２２に送信する。ステップＳ１９において、ペイメントカード２２は、アクセスパスワードを確認するよう作動する。アクセスパスワードが正しいことがペイメントカード２２によって確認されたとき、ペイメントカード２２は、アクセス許可命令を電子装置１に送信し、フローはステップＳ２３に進む。そうでない場合、フローは、ペイメントカード２２がアクセス拒否命令を電子装置１に送信するステップＳ２０に進み、ステップＳ２１において、ペイメントカード２２は、誤ったアクセスパスワードを受信する連続的な出来事の回数をカウントする。回数がしきい値（例えば、３）より小さいとき、フローは、他のアクセスパスワードを入力することをユーザに許可するためにステップＳ１７に戻る。そうでない場合、フローは、ペイメントカード２２がロックされるとともにペイメントカード２２に対するアクセスが禁止されるステップＳ２２に進む。

【００４３】

ステップＳ２３において、電子装置１は、（ステップＳ１８で受信した）一時的に格納したアクセスパスワードをクリアする。このステップは、アクセスパスワードが他者によって読み出されないようにするために実行される。これは、方法を実行するために公共の電子装置又は商店主が所有する電子装置が用いられる場合にさらにいっそう重要である。

【００４４】

ステップＳ２４において、プロセッサ１１は、ステップＳ１３で生成された認証すべきデータ及びステップＳ１６でユーザによって確認された取引情報を比較するよう作動する。認証すべきデータが取引情報と一致すると決定されたとき、フローはステップＳ２５に進む。そうでない場合、フローはステップＳ１２に戻る。

【００４５】

ステップＳ２５において、プロセッサ１１は、認証すべきデータをペイメントカード２２に送信する。その後、ステップＳ２６において、ペイメントカード２２は、認証すべきデータ及び秘密鍵に基づいて取引認証コード（ＴＡＣ）を生成するとともにＴＡＣを電子装置１に送信する。

【００４６】

具体的に説明すると、ペイメントカード２２は、マスターバーチャル口座に対応するマスター秘密鍵を財務データチップ２２１に格納する。ペイメントカード２２は、メンバー

バーチャル口座に対応する追加のメンバー秘密鍵を隠し領域２２８に格納することができる。そのように、ペイメントカード２２は、ＴＡＣを生成するためのステップＳ２６で選択したバーチャル口座に基づいて（マスター秘密鍵及びメンバー秘密鍵を含む）秘密鍵のうちの対応するものを選択する。

【００４７】

ステップＳ２７において、取引ソフトウェア１２０を実行するプロセッサ１１は、ＴＡＣを用いて支払コマンドを構成する。支払コマンドは、少なくとも取引情報及びＴＡＣを含み、暗号化される。

【００４８】

図３Ｂを参照すると、ステップＳ２７の後、電子装置１は、プラットホームサーバ３とのセッションを確立することを試みる。セッションは、電子装置１とプラットホームサーバ３との間の安全な通信チャネルを設けるとともにペイメントカード２２の有効性を確認するためのものである。

【００４９】

ステップＡ１において、トランザクションアプリケーション１２０を実行するプロセッサ１１は、ステップＳ１６で用いられたバーチャル口座をペイメントカード２２から取得する。他の実施の形態において、携帯支払装置２のユーザを確認することができる種々のコード又は符号を用いることができることに留意されたい。

【００５０】

ステップＡ２において、プロセッサ１１は、セッション要求をプラットホームサーバ３に送信する。セッション要求は、バーチャル口座を有する。

【００５１】

ステップＡ３において、プラットホームサーバ３は、セッション要求の受信に応答してセッション識別（ＩＤ）を生成し、セッションＩＤを電子装置１に送信する。電子装置１は、セッションＩＤを受信し、ステップＡ４でセッションＩＤをペイメントカード２２に送信する。

【００５２】

ステップＡ５において、ペイメントカード２２は、セッションＩＤ及びペイメントカード２２の物的生産中に隠し領域２２８に格納されるカード識別鍵に基づいて第１の認証コードを生成するよう作動する。その後、ペイメントカード２２は、第１の認証コードを電子装置１に送信する。

【００５３】

カード識別鍵はペイメントカード２２及びプラットホームサーバ３のみに知られており、かつ、方法の初めから終わりまで電子装置１に送信されないことに留意されたい。さらに、第１の認証コードの生成は、ペイメントカード２２内で行われる。これは、電子装置１が第１の認証コードの生成に介入することができず、かつ、カード識別鍵なしでは有効な第１の認証コードを生成することができないことを保証する。したがって、有効なペイメントカード２２のみが有効な第１の認証コードを生成することができる。

【００５４】

次に、ステップＡ６において、電子装置１は、第１の認証コードをプラットホームサーバ３に送信する。

【００５５】

次に、ステップＡ７において、プラットホームサーバ３は、ステップＡ２で電子装置１から受信したセッション要求に含まれるバーチャル口座に従って、格納されたユーザ識別鍵を見つける。ユーザ識別鍵は、カード識別鍵に対応し、バーチャル口座に専用のものである。

【００５６】

ステップＡ８において、プラットホームサーバ３は、ステップＡ３で生成したセッションＩＤ及びステップＡ７で見つけたユーザ識別鍵に基づいて第２の認証コードを生成する。

【００５７】
ステップＡ９において、プラットホームサーバ３は、ステップＡ６で電子装置１から受信した第１の認証コードがステップＡ８で生成した第２の認証コードと一致するか否かを決定する。第１の認証コードが第２の認証コードと一致した（すなわち、ペイメントカード２２が銀行から発行されたものである）と決定したとき、フローはステップＡ１０に進む。そうでない場合、プラットホームサーバ３は、ペイメントカード２２が有効な第１の認証コードを生成できなかった（、したがって、銀行から発行されたものでない）と決定し、フローを終了する。
【００５８】
ステップＡ１０において、プラットホームサーバ３は、セッションを確立するとともに取引を進めることができるようにするためにセッション応答を電子装置１に送信する。
【００５９】
図３Ｃを参照すると、プラットホームサーバ３が取引を進めるのを許可した後、ステップＳ２８において、セッションの下で、ステップＳ２７で構成された支払コマンドを、プロセッサ１１により通信装置１５を介してプラットホームサーバ３に送信する。具体的に説明すると、送信は、セキュアソケットレイヤー（ＳＳＬ）プロトコルを用いて実行される。次に、ステップＳ２９において、プラットホームサーバ３は、支払コマンドを、専用チャネルを通じて銀行システム４に送信する。
【００６０】
支払コマンドの受信に応答して、ステップＳ３０において、銀行システム４は、受信した支払コマンドを解読し、支払コマンドに基づいてペイメントカード２２の有効性を確認するよう作動する。具体的に説明すると、銀行システム４は、ペイメントカード２２（例えば、財務データチップ２２１又は隠し領域２２８）に格納された同一の秘密鍵を用いることによって、支払コマンドに含まれる認証すべきデータを用いて確認コードを生成する。一部の実施の形態において、確認コードを生成するための秘密鍵を、支払コマンドに含めるとともにプラットホームサーバ３によって銀行システム４に送信することができる。
【００６１】
その後、銀行システム４は、ＴＡＣと確認コードとを比較する。確認コードがＴＡＣと一致することが決定されたとき、銀行システム４は、ペイメントカード２２が有効であると決定し、取引情報は、取引中に変更されなかった。その後、フローはステップＳ３１に進む。そうでない場合、フローはステップＳ３６に進む。
【００６２】
ステップＳ３１において、銀行システムは、支払コマンドに含まれる取引情報に従って支払いを処理する。この場合、鉄道運賃の料金（この場合、１６０ニュー台湾ドル）が、バーチャル口座によって表される銀行預金口座から引き落とされ、台湾高速鉄路公司によって所有される口座に送金される。
【００６３】
その後、ステップＳ３２において、銀行システム４は、取引が処理されたことを示す支払結果を生成し、支払結果をプラットホームサーバ３に送信する。
【００６４】
次に、ステップＳ３３において、支払結果が電子装置１に送られる。支払結果は、セッションの下では同様であり、ＳＳＬプロトコルを用いる。その後、ステップＳ３４において、電子装置１は、携帯支払装置２を切り離すようユーザに命令する警告を出力することができる（図７参照）。
【００６５】
支払結果は、ステップＳ３５でユーザに提供される認証情報を含むことができる。認証情報を、物理的な鉄道乗車券と引き換えるためにコンビニエンスストア若しくは駅で用いるためのクイックレスポンス（ＱＲ）コード若しくは一連のコードの形態又は携帯機器にダウンロードしたときに駅で直接用いることができる電子的な鉄道乗車券の形態とすることができる。

【００６６】
ステップＳ３０において、確認コードがＴＡＣに一致しないと決定されたとき、銀行システム４は、ペイメントカード２２が有効でない又は取引情報が送信中に変えられたことを決定する。その結果、ステップＳ３６において、銀行システム４は、エラーメッセージを生成し、セラーメッセージをプラットホームサーバ３に送信する。ステップＳ３７において、プラットホームサーバ３は、エラーメッセージを電子装置１に送り、電子装置１は、ステップＳ３８でエラーメッセージを出力する。その結果、取引は処理されない。
【００６７】
上述した方法を、小売店のような場所で採用することができる。そのような場合、顧客が商品及び／又はサービスを購入するとき、商店主は、トランザクションアプリケーションを実行する（ステップＳ１１）ために電子装置１（例えば、パーソナルコンピュータ）を操作することができる。ステップＳ１２において、取引情報を、例えば、商品及び／又はサービスに関連するバーコードを走査することによって電子装置１に入力することができる。その後、顧客は、ステップＳ１５において、ペイメントカード２２を有する携帯支払装置２を商店主に提供し、ステップＳ１６において、取引情報を確認し、ステップＳ１７において、電子装置１にアクセスパスワードを提供する。
【００６８】
電子装置１は、プラットホームサーバ３及び銀行システム４とともに自動的に後続ステップを実行する。その後、ステップＳ３４において、支払いが処理され、顧客は、携帯支払装置２を検索するとともに商品／サービスを取得することができる。
【００６９】
例えば、方法は、商品／サービスが配達によって顧客に提供されるとともに商品／サービスが配達された後に支払いを行う場合に適用できる。配達職員は、第１の接続インタフェース１３を有するとともにトランザクションアプリケーション１２０がインストールされた電子装置１を携えて行き、顧客が商品／サービスを確認した後に、方法を実行するために電子装置１を操作することができる。その結果、配達職員は、訪問中に現金を持つ必要がない。
【００７０】
方法は、商品／サービスが自動販売機によって顧客に提供される場合に適用することもできる。支払いがステップＳ３５で行われた後、自動販売機は商品を提供する。
【００７１】
さらに、携帯支払装置２を、現金を銀行預金口座から引き落とすために現金自動預入支払機とともに用いることができる。そのような場合において、方法が実行された後、ＡＴＭは、現金を顧客に支払う。
【００７２】
一部の実施の形態において、ペイメントカード２２を、記憶装置２２５に追加データ（例えば、医療健康情報、ライセンス又は識別情報、会員情報等）を格納するように構成することができる。追加データを、アプリケーション１２０を実行する電子装置１によって記憶装置２２５に格納することができ、アプリケーション１２０は、更に（「パーソプロセス」（ｐｅｒｓｏ　ｐｒｏｃｅｓｓ）と称する）パーソナライゼーションプロセスを実行することができる。
【００７３】
パーソプロセスにおいて、ペイメントカード２２に格納されるデータを種々のセキュリティレベルを用いて処理する必要があると仮定する（例えば、銀行の口座情報は他の一般的な情報より高いセキュリティレベルを要求するかもしれない。）。その結果、本発明のペイメントカード２２は、更に安全であるとともに更に適用性のあるデータ管理を提供するようにも構成される。
【００７４】
一部の実施の形態において、ペイメントカード２２の隠し領域２２８は、複数の隠しデータブロックに分割される。隠しデータブロックの各々は、ストレージセキュリティレベ

ルに関連し、予め決定されたデータタイプのパーソナライゼーションデータを記憶するように構成される。その結果、隠しデータブロックの各々に対して、コントローラチップ２２２は、ストレージセキュリティレベルに対応する複数のセキュリングメカニズムの予め決定されたものとともにパーソナライゼーションデータを格納するパーソプロセスを実行するよう構成される。

【００７５】

図８に示す例において、ペイメントカード２２の隠し領域２２８は、入力データに対する８個の隠しデータブロック（５Ａ～５Ｈ）に分割される。具体的に説明すると、隠しデータブロック５Ａは、ユーザの（一つ以上の）緊急連絡先、大病歴、薬物に対するアレルギー等のペイメントカード２２のユーザに関する応急処置情報を格納するためのものである。

【００７６】

隠しデータブロック５Ｂは、ユーザの健康診断及び血液検査結果、電子機器による医療記録（ＥＭＲ）等のユーザに関する基本健康及び医療情報を格納するためのものである。

【００７７】

隠しデータブロック５Ｃは、身分証明書、パスポート、運転免許等のユーザ及び／又は親類によって保持される電子本人書類及びライセンスを格納するためのものである。

【００７８】

隠しデータブロック５Ｄは、プリペイド鉄道乗車券又はイベントチケット、電子インボイス等の電子チケット及びレシートを格納するためのものである。隠しデータブロック５Ｅは、ユーザのプライベートデータを確認するものである。

【００７９】

隠しデータブロック５Ｆは、種々の社会組織のユーザの登録データを格納するためのものである。隠しデータブロック５Ｇは、種々の銀行のユーザの口座情報を格納するためのものである。隠しデータブロック５Ｈは、その他の情報を格納するためのものである。

【００８０】

例えば、四つの異なるセキュリングメカニズムが、異なるストレージセキュリティレベルに対するパーソプロセスを実現するために設けられる。さらに、関係者は、セキュリティレベルに基づいて隠しデータブロックの一部にアクセスするための認可を有することができる。

【００８１】

異なるセキュリングメカニズムにおいて、ペイメントカード２２に対して、パーソナライゼーションプロセスを実現するための許可を得るために種々の第三者との通信を確立することを要求することができる。

【００８２】

具体的に説明すると、セキュリングメカニズムの各々において、ペイメントカード２２は、パーソプロセスを許可するための許可情報の少なくとも一部及び／又はパーソナライゼーションデータを格納するプラットホームサーバ３との通信が要求される。

【００８３】

一部のセキュリングメカニズムにおいて、ペイメントカード２２は、許可情報の他の部分を取得するために、許可された組織サーバ３２、協力する組織サーバ３３又は銀行システム４のような他の第三者との通信を行うことを更に要求される。

【００８４】

許可された組織サーバ３２を、パーソプロセスに関連した情報を提供するためにプラットホームサーバ３によって許可された第三者によって操作することができる。協力する組織サーバ３３は、パーソプロセスに関連した情報を生成するためにプラットホームサーバ３に協力する第三者によって操作される。

【００８５】

セキュリングメカニズムの一部において、パーソナライゼーションデータのユーザ入力が許可され（すなわち、パーソナライゼーションデータを、コントローラファームウェア

２２４及びＡＰＩ２２３を介してアプリケーソン１２０から受信することができ）、それに対し、他のセキュリングメカニズムにおいて、パーソナライゼーションデータを、第三者から受信し、ユーザによって変更することができない。

【００８６】

例えば、図８に示す例において、隠しデータブロック５Ａについては、パーソナライゼーションデータをユーザによって入力／変更することができ、それに対するアクセスを全ての人に許可することができる。隠しデータブロック５Ｃ～５Ｅについては、パーソナライゼーションデータをユーザによって入力／変更することができ、パーソナライゼーションデータは、ユーザによってのみアクセス可能である。隠しデータブロック５Ｂ，５Ｆ及び５Ｇについては、パーソナライゼーションデータを第三者から受信し（すなわち、ユーザはデータを修正することができない。）、パーソナライゼーションデータは、ユーザによってのみアクセス可能である。隠しデータブロック５Ｈについては、パーソナライゼーションデータを第三者から受信し、それに対するアクセスを全ての人に許可することができる。

【００８７】

本実施の形態において、隠しデータブロック（５Ａ～５Ｈ）の各々は、パーソナライゼーションデータを格納するための複数の隠しデータサブブロックに更に分割される（例えば、隠しデータブロック５Ｇの下の隠しデータサブブロックの各々は、ある特定の銀行の登録されたデータ及び口座番号を格納する。）。特定の隠しデータブロックの下の全ての隠しデータサブブロックが同一のセキュリティレベルに関連し、かつ、同一のセキュリングメカニズムを用いることに留意されたい。

【００８８】

他の実施の形態において、追加の隠しデータブロックを更に分割することができ、存在する隠しデータサブブロックを、種々の他の情報を格納するために用いることができる。追加のセキュリングメカニズムを設けることもできる。

【００８９】

使用の際に、ペイメントカード２２のシステム部２２６は、隠しデータサブブロックのリスト６１及び隠しデータサブブロック５Ａ～５Ｈの各々の下の隠しデータサブブロックのサブリスト６２を維持することができる。隠しデータサブブロックの各々に対して、パーソナライゼーションデータを隠しデータサブブロックに格納するために特定のパーソプロセスを実行する。

【００９０】

図９を参照すると、パーソプロセスは、登録ステップと、フォーマットステップと、パーソナライゼーションステップと、を有する。

【００９１】

登録ステップにおいて、ペイメントカード２２は、隠しデータブロック５Ａ～５Ｈのうちの一つを指定し、パーソナライゼーションデータを格納するために用いるべき隠しデータサブブロックの一つを割り当てる。

【００９２】

フォーマットステップにおいて、隠しデータブロック５Ａ～５Ｈのうちの指定された隠しデータブロックは、パーソナライゼーションデータをそこに格納するのを許可するために予め決定されたデータタイプに一致するようにフォーマットされる。

【００９３】

パーソナライゼーションステップにおいて、ペイメントカード２２は、隠しデータブロック（５Ａ～５Ｈ）のうちの指定された隠しデータブロック（５Ａ～５Ｈ）のにパーソナライゼーションデータを格納する。

【００９４】

本実施の形態において、隠しデータサブブロックの各々は、登録ステップを許可するための前もってセットした登録ＩＤ／パスワードの組合せ及びフォーマットステップを許可するための前もってセットしたフォーマットＩＤ／パスワードの組合せが格納される。

【００９５】
パーソプロセスの登録ステップを実行する前に、ペイメントカード２２は、登録を許可するＩＤ／パスワードの組合せを受信し、登録を許可するＩＤ／パスワードの組合せが前もってセットした登録ＩＤ／パスワードの組合せと一致するときのみ登録ステップを実行する。同様に、パーソプロセスのフォーマットステップを実行する前に、ペイメントカード２２は、フォーマット許可ＩＤ／パスワードの組合せを受信し、フォーマット許可ＩＤ／パスワードの組合せが前もってセットしたフォーマットＩＤ／パスワードの組合せと一致するときのみ登録ステップを実行する。
【００９６】
更に図１及び図１０を参照しながら、第１のセキュリングメカニズムによって実現されるパーソプロセスを詳細に説明する。
【００９７】
ステップＳ４０において、ユーザは、コンピュータ機器１のアプリケーション１２０を操作し、コンピュータ機器１は、それに応答してステップＳ４１でパーソプロセスを起動する。ステップＳ４２において、ユーザは、ペイメントカード２２に格納されるデータのタイプに従って隠しデータブロック（５Ａ～５Ｈ）のうちの一つ及び隠しデータブロック（５Ａ～５Ｈ）の選択した隠しデータブロックの隠しデータサブブロックのうちの一つを選択する。選択に応答して、ペイメントカード２２は、隠しデータブロック（５Ａ～５Ｈ）のうちの選択された隠しデータブロック及び隠しデータサブブロックのうちの選択された隠しデータサブブロックを指定する。例えば、隠しデータブロック（５Ｈ）の隠しデータサブブロックの一つは、パーソプロセスが課されるように指定される。
【００９８】
ステップＳ４３において、ユーザは、起動パスワードを入力するように命令される。その後、起動パスワードを受信するコンピュータ機器１は、ステップＳ４４において、起動パスワードをペイメントカード２２に送信する。ステップＳ４５において、ペイメントカード２２は、起動パスワードが正しいか否か決定する。起動パスワードが正しいと決定されたとき、フローはステップＳ４６に進む。そうでない場合、フローを終了する。
【００９９】
ステップＳ４６において、コンピュータ機器１は、指定された隠しデータサブブロックに対応する登録許可ＩＤ／パスワードの組合せを要求するためにプラットホームサーバ３と通信を行う。ステップＳ４７において、プラットホームサーバ３は、登録ステップのために、例えば、隠しデータブロック（５Ｈ）に関連した第三者によってペイメントカード２２が許可されたか否かを決定する。ペイメントカード２２が登録ステップを許可されたと決定したとき、フローはステップＳ４８に進む。そうでない場合、プロセスを終了する。
【０１００】
ステップＳ４８において、プラットホームサーバ３は、指定された隠しデータサブブロックに対応する登録許可ＩＤ／パスワードの組合せ及び他の関連の情報をコンピュータ機器１に送信する。その後、コンピュータ機器１は、ステップＳ４９において登録コマンドをペイメントカード２２に送信するために登録許可ＩＤ／パスワードの組合せを用いる。
【０１０１】
ステップＳ５０での登録コマンドの受信に応答して、ペイメントカード２２は、ステップＳ５１において、受信した登録許可ＩＤ／パスワードの組合せと前もってセットした登録ＩＤ／パスワードの組合せとを比較することによって、登録ＩＤ／パスワードの組合せが正しいか否かを決定する。登録ＩＤ／パスワードの組合せが前もってセットした登録ＩＤ／パスワードの組合せと一致すると決定したとき、フローはステップＳ５２に進む。そうでない場合、プロセスを終了する。
【０１０２】
ステップＳ５２において、ペイメントカード２２は、隠しデータブロック５Ｈ内の指定された隠しデータサブブロックを物理的に割り当て、指定された隠しデータサブブロック

に関連の情報を格納する。具体的に説明すると、コントローラファームウェア２２４は、関連の情報をコントローラチップ２２２に送信し、コントローラチップ２２２は、指定された隠しデータサブブロックの物理アドレスを、リスト６１を介して識別し、識別した物理アドレスに関連の情報を書き込み、これによって、登録ステップを完了する。

【０１０３】

その後、プロセスはフォーマットステップに進む。ステップＳ５３において、コンピュータ機器１は、指定された隠しデータサブブロックに対応するフォーマット許可ＩＤ／パスワードの組合せを要求するためにプラットホームサーバ３と通信を行う。プラットホームサーバ３は、ステップＳ５４において、ペイメントカード２２にフォーマットステップを許可するか否かを決定する。ペイメントカード２２が、例えば、隠しデータブロック（５Ｈ）に関連した第三者によってフォーマットステップを許可されることを決定したとき、フローはステップＳ５５に進む。そうでない場合、プロセスを終了する。

【０１０４】

ステップＳ５５において、プラットホームサーバ３は、指定された隠しデータサブブロックに対応するフォーマット許可ＩＤ／パスワードの組合せ及びパーソナライゼーション情報を、コンピュータ機器１に送信し、その後、コンピュータ機器１は、ステップＳ５６において、ペイメントカード２２にコマンドを送信するためにフォーマット許可ＩＤ／パスワードの組合せを使用する。

【０１０５】

それに応答して、ペイメントカード２２は、ステップＳ５７において、フォーマット許可ＩＤ／パスワードの組合せをコンピュータ機器１から受信し、その後、ステップＳ５８において、受信したフォーマット許可ＩＤ／パスワードの組合せを前もってセットしたフォーマット許可ＩＤ／パスワードの組合せと比較することによって、フォーマット許可ＩＤ／パスワードの組合せが正しいか否かを決定する。フォーマット許可ＩＤ／パスワードの組合せが前もってセットしたフォーマット許可ＩＤ／パスワードの組合せがと一致することが決定されたとき、フローはステップＳ５９に進む。そうでない場合、プロセスを終了する。

【０１０６】

ステップＳ５９において、ペイメントカード２２は、指定された隠しデータサブブロックをフォーマットし、指定された隠しデータサブブロックにパーソナライゼーションデータを格納する。

【０１０７】

本実施の形態において、パーソプロセスを反映するためにリスト６１の更新もされる。

【０１０８】

図１１は、第２のセキュリングメカニズムを用いるパーソプロセスのステップを示す。図１１に示す例において、ユーザは、「Ｘ１」という名前のクラブのユーザの会員情報をペイメントカード２２に入力しようとすることができ、その結果、隠しデータブロック５Ｆの隠しデータサブブロックの一つにパーソナライゼーションプロセスが課される。

【０１０９】

本例において、登録ステップ（すなわち、ステップＳ４１～Ｓ５２）は、第１のセキュリングメカニズムを用いる登録ステップと同様に実行されるので、その詳細を、簡潔のためにここでは省略する。

【０１１０】

第１のセキュリングメカニズムの使用と第２のセキュリングメカニズムの使用との間の主な違いは、以下の通りである。ステップＳ５３において、コンピュータ機器１は、指定された隠しデータサブブロックに対応するフォーマット許可ＩＤ／パスワードの組合せを要求するために、許可された組織サーバ３２（この場合、クラブＸ１によって操作されるサーバ）と通信を行う。許可された組織サーバ３２は、プラットホームサーバ３の代わりに、ステップＳ５４において、ペイメントカード２２にフォーマットステップを許可するか否かを決定する。

【０１１１】
さらに、この場合のパーソナライゼーションデータは、アクセスのために全ての人に対して明らかにしようとしないので、指定された隠しデータサブブロックに対して、許可されていないアクセスの試みをブロックするためのアクセスＩＤ／パスワードの組合せを更に割り当てることができる。
【０１１２】
図１３Ａ及び図１３Ｂは、第３のセキュリングメカニズムを用いるパーソプロセスのステップを示す。図１３Ａ及び図１３Ｂに示すような例において、ユーザは、銀行の口座情報を入力しようとすることができ、その結果、隠しデータブロック５Ｇの隠しデータサブブロックの一つにパーソプロセスが課される。
【０１１３】
本例において、登録ステップ（すなわち、ステップＳ４１～Ｓ５２）は、第１のセキュリングメカニズム及び第２のセキュリングメカニズムを用いる登録ステップと同様に実行されるので、その詳細を、簡潔のためにここでは省略する。
【０１１４】
第１のセキュリングメカニズムの使用と第３のセキュリングメカニズムの使用との間の主な違いは、以下の通りである。
【０１１５】
フォーマットステップで用いられるフォーマット許可ＩＤ／パスワードの組合せは、プラットホームサーバ３及び協力する組織サーバ３３（この場合、銀行システム４以外の第三者によって操作されるサーバ）によって協力して生成される。
【０１１６】
フォーマット許可ＩＤ／パスワードの組合せの生成を、図１２に示すステップを用いて行うことができる。ステップＳ６１において、銀行システム４は、プラットホームサーバ３及び協力する組織サーバ３３の両方に対して、フォーマット許可ＩＤ／パスワードの組合せを生成するのに必要なデータの要求を送信する。それに応答して、プラットホームサーバ３及び協力する組織サーバ３３はそれぞれ、ステップＳ６２及びステップＳ６３において、フォーマット許可ＩＤ／パスワードの組合せを生成するのに必要なデータの一部を銀行システム４に戻す。その後、銀行システム４は、ステップＳ６４において、受信したデータを用いてフォーマット許可ＩＤ／パスワードの組合せを生成する。
【０１１７】
その後、（図１３Ａで示すような）フォーマットステップでは、ステップＳ５３において、コンピュータ機器１は、銀行システム４からのフォーマット許可ＩＤ／パスワードの組合せを要求する。その後、ステップＳ７１において、銀行システム４は、プラットホームサーバ３及び協力する組織サーバ３３から、フォーマットステップが許可されたか否かを問い合わせる。
【０１１８】
（図１３Ｂを参照すると、）それに応答して、プラットホームサーバ３及び協力する組織サーバ３３はそれぞれ、ステップＳ７２ａ及びステップＳ７２ｂにおいて、フォーマットステップが許可されたか否かを決定する。具体的に説明すると、プラットホームサーバ３及び協力する組織サーバ３３のそれぞれについて、フォーマットステップが許可されていないと決定されたとき、否定応答が銀行システム４に送信される（ステップＳ７３ａ及びステップＳ７３ｂ）。それに対し、フォーマットステップが許可されたと決定されたとき、肯定応答が銀行システム４に送信される（ステップＳ７４ａ及びステップＳ７４ｂ）。協力する組織サーバ３３がフォーマットステップが許可されたことを決定するときにステップＳ７４ｂでパーソナライゼーションデータも銀行システム４に送信されることに留意されたい。
【０１１９】
銀行システム４は、ステップＳ７５で応答を受信し、ステップＳ７６で両方の応答が肯定であるか否かを決定し、両方の応答が肯定であるときにステップＳ７７に進む。応答の

少なくとも一方が否定である時、ステップＳ７８において、銀行システム４は、応答をコンピュータ機器１に戻し、プロセスを終了することを知らせる。

【０１２０】

銀行システム４は、ステップＳ７７において、ステップＳ６４で生成したフォーマット許可ＩＤ／パスワードの組合せを取得し、ステップＳ７９において、フォーマット許可ＩＤ／パスワードの組合せをパーソナライゼーションデータとともにコンピュータ機器１に送信する。その後、コンピュータ機器１は、上述したようなパーソプロセスを継続する。

【０１２１】

図１４は、第４のセキュリングメカニズムを用いるパーソプロセスのステップを示す。図１４に示す例において、ユーザは、ユーザの応急処置情報をペイメントカード２２に入力しようとすることができ、その結果、隠しデータブロック５Ａの隠しデータサブブロックの一つにパーソプロセスが課される。

【０１２２】

本例において、登録ステップ（すなわち、ステップＳ４１～Ｓ５２）は、第１のセキュリングメカニズムを用いる登録ステップと同様に実行されるので、その詳細を、簡潔のためにここでは省略する。

【０１２３】

第１のセキュリングメカニズムの使用と第４のセキュリングメカニズムの使用との間の主な違いは、以下の通りである。ステップＳ５３において、コンピュータ機器１は、プラットホームサーバ３からのパーソナライゼーションデータを要求しない。代わりに、ペイメントカード２２がステップＳ５９でフォーマットされた後に、コンピュータ機器１は、ステップＳ８１において、応急処置情報を入力することをユーザに許可する。その後、ステップＳ８２において、コンピュータ機器１は、隠しデータブロック５Ａの指定された隠しデータサブブロックに（パーソナライゼーションデータとして用いられる）応急処置情報を格納する。

【０１２４】

パーソナライゼーションデータをプラットホームサーバ３から受信する場合に、受信したパーソナライゼーションデータは指定された隠しデータサブブロック（５Ａ）の次のアクセスに対するアクセスコードを有することができることに留意されたい。パーソナライゼーションデータがユーザによって入力される場合、アクセスコードもユーザによって決定される。したがって、パーソプロセスを完了した後、隠しデータサブブロックには、用いられるセキュリングメカニズムに基づく特定のアクセスレベルが割り当てられる。

【０１２５】

例えば、ペイメントカード２２を所持する人は誰でも、隠しデータブロック５Ａの隠しデータサブブロックの読出しが許可されるが、ユーザのみが、隠しデータブロック５Ａの隠しデータサブブロックの書込みが許可される。

【０１２６】

ユーザは、隠しデータブロック５Ｂ及び５Ｆの隠しデータサブブロックの読出しが許可されるが、許可された組織（病院又は社会組織）のみが、隠しデータブロック５Ｂ及び５Ｆの隠しデータサブブロックの書込みが許可される。

【０１２７】

ユーザは、隠しデータブロック５Ｃ～５Ｅの隠しデータサブブロックの読出し及び書込みが許可される。

【０１２８】

ユーザは、隠しデータブロック５Ｇの隠しデータサブブロックの読出しが許可されるが、協力する組織（銀行）のみが、隠しデータブロック５Ｇの隠しデータサブブロックの書込みが許可される。

【０１２９】

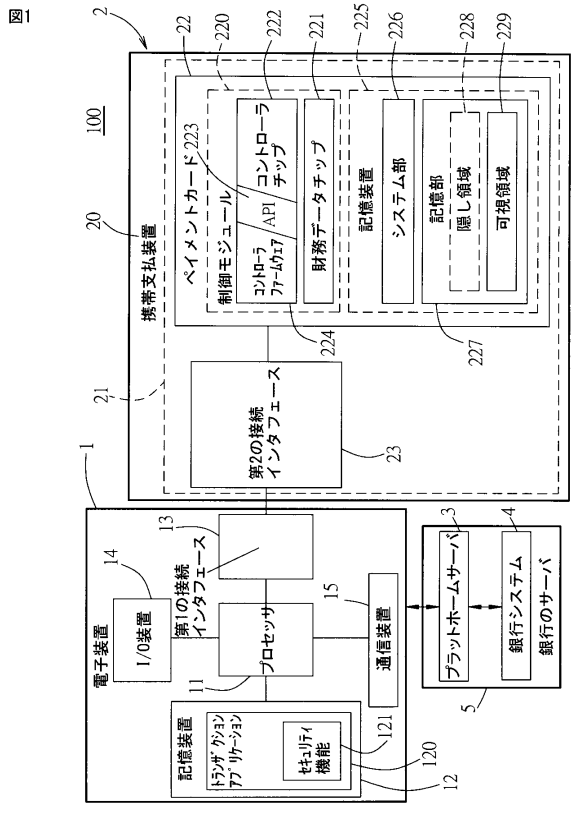
ペイメントカード２２を所持する人は誰でも、隠しデータブロック５Ｈの隠しデータサブブロックの読出しが許可されるが、プラットホームサーバ３のみが、隠しデータブロッ

ク５Ｈの隠しデータサブブロックの書込みが許可される。

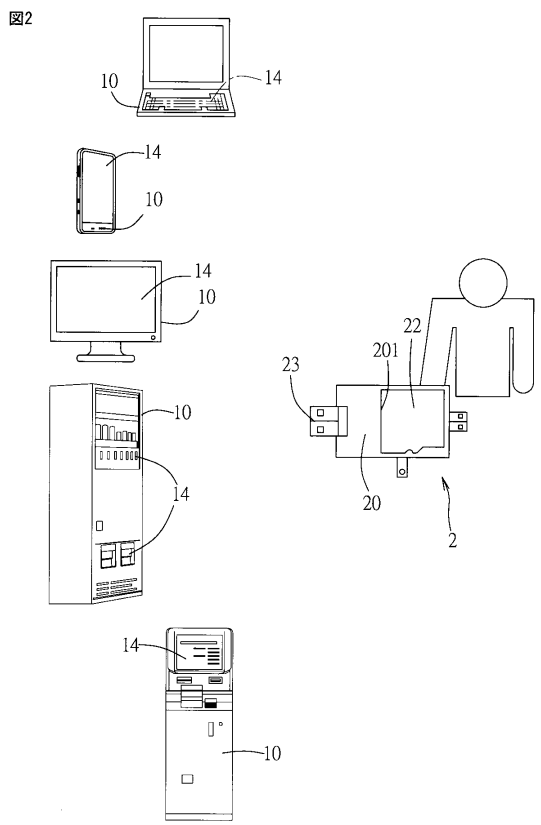
【０１３０】

要約すれば、本発明の方法は、通常のクレジットカードを使用するために商店主は特定の処理装置を提供する必要がない。携帯支払装置２がプラグアンドプレイ装置を用いて実現されるので、第１の接続インタフェース１３を有するとともにトランザクションアプリケーション１２０がインストールされた任意の電子装置を、電子装置１として用いることができる。その結果、方法は、通常のクレジットカードが適用できない場合にペイメントカード２２の使用を拡張するのに有益である。さらに、ペイメントカード２２の隠し領域２２８を、各々がストレージセキュリティレベルに関連した複数の隠しデータブロックに分割することができる。隠しデータブロックの各々を、各々が起動すべきパーソナライゼーションプロセスを要求する複数の隠しデータサブブロックに更に分割することができる。その結果、隠し領域２２８を、向上したセキュリティを有する拡張した情報バンクと考えることができる。

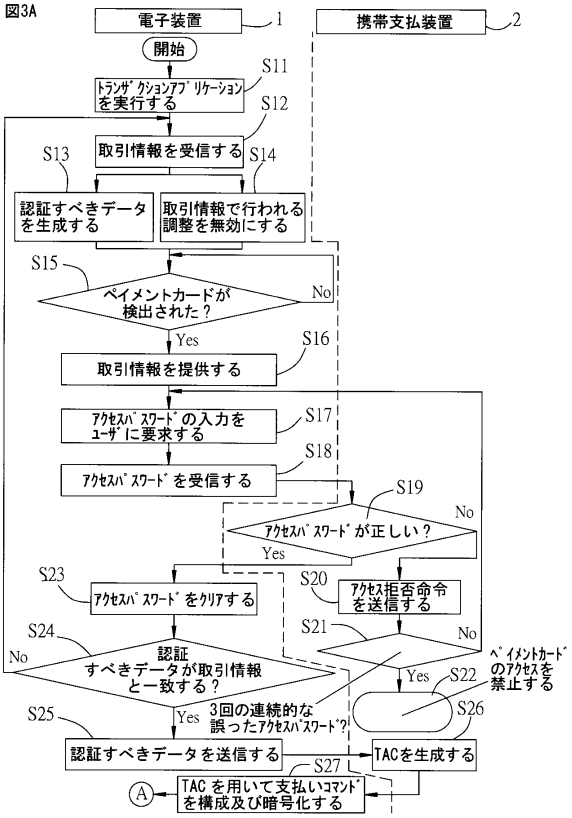
【図１】



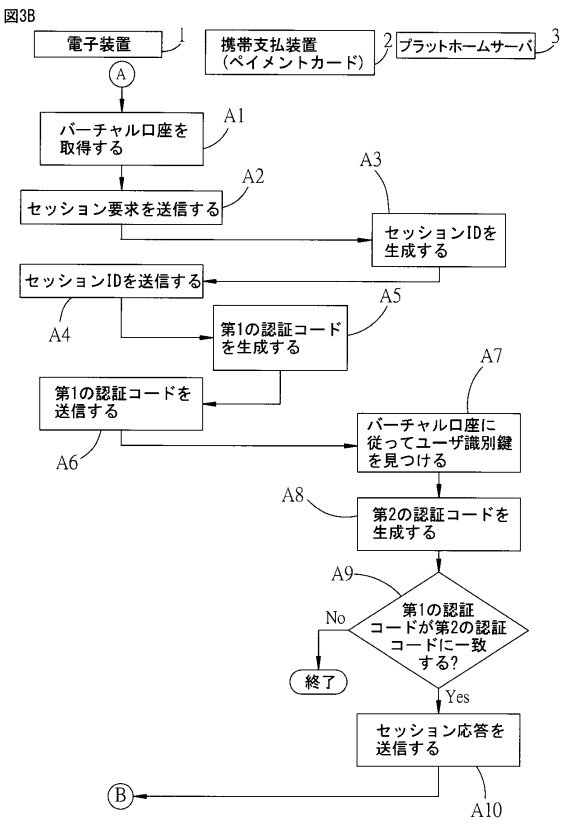
【図２】



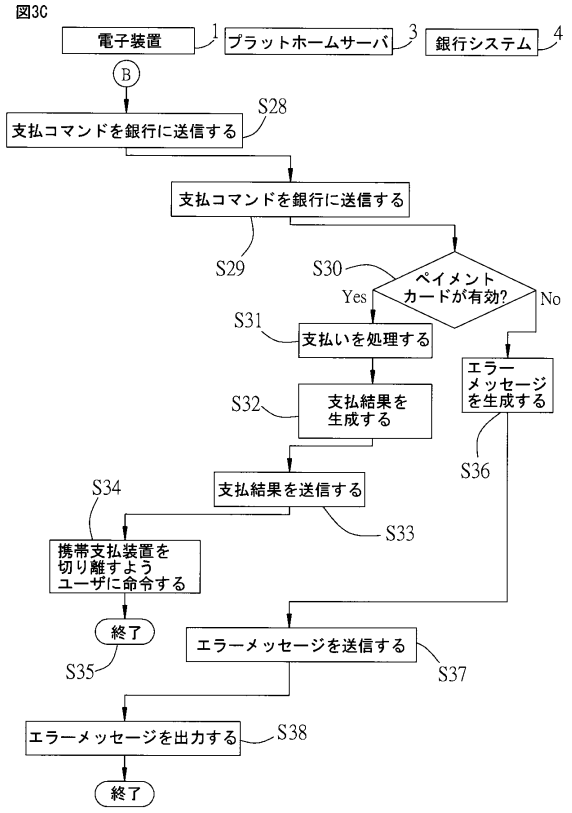
【図３Ａ】



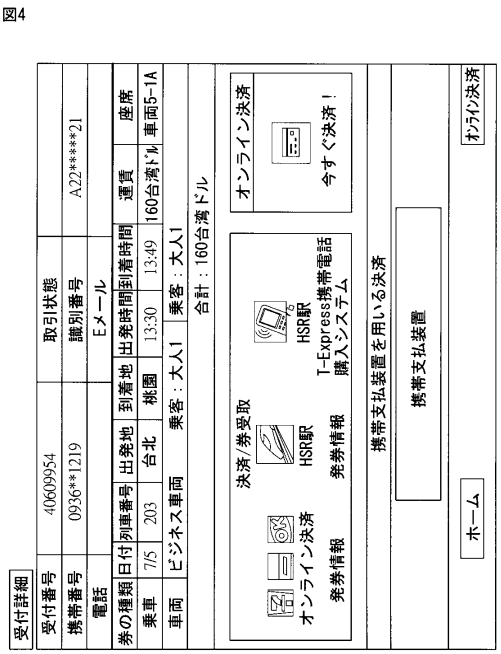
【図３Ｂ】



【図３Ｃ】

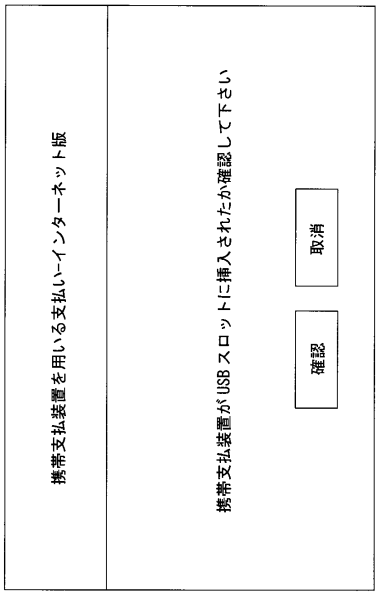


【図４】



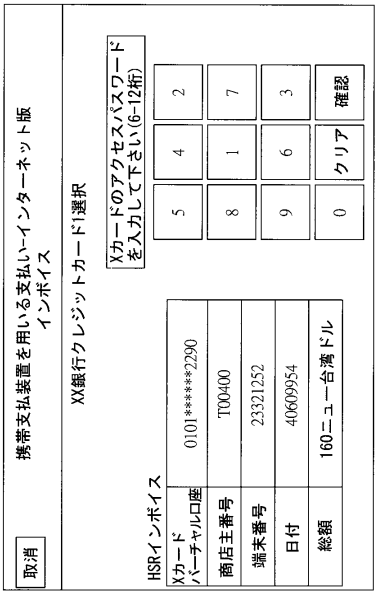
【図５】

図5



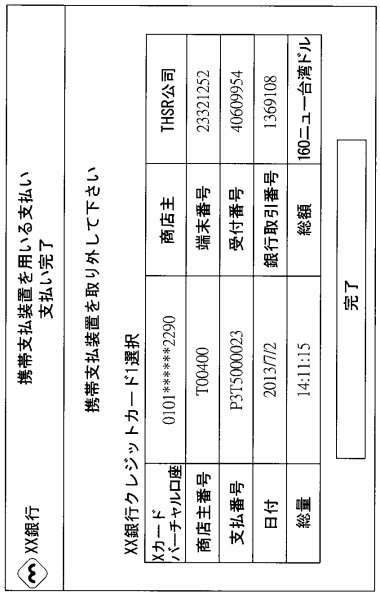
【図６】

図6



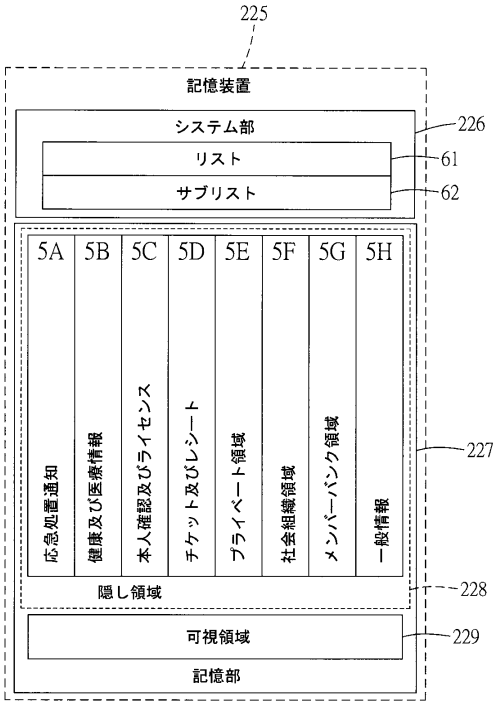
【図７】

図7



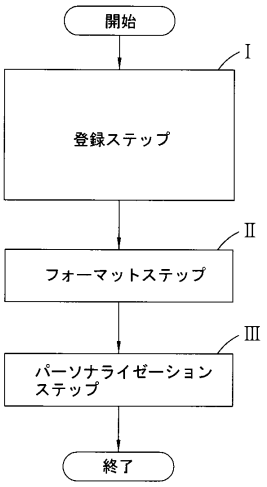
【図８】

図8



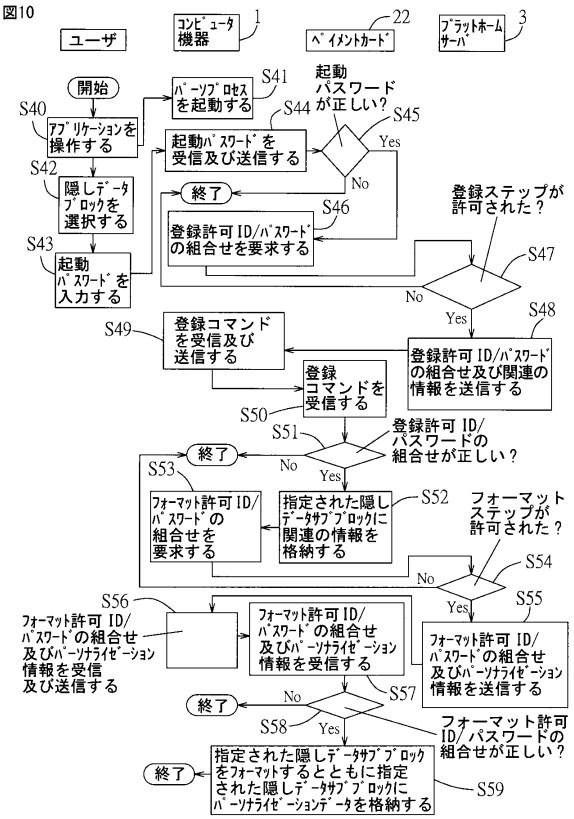
【図９】

図9



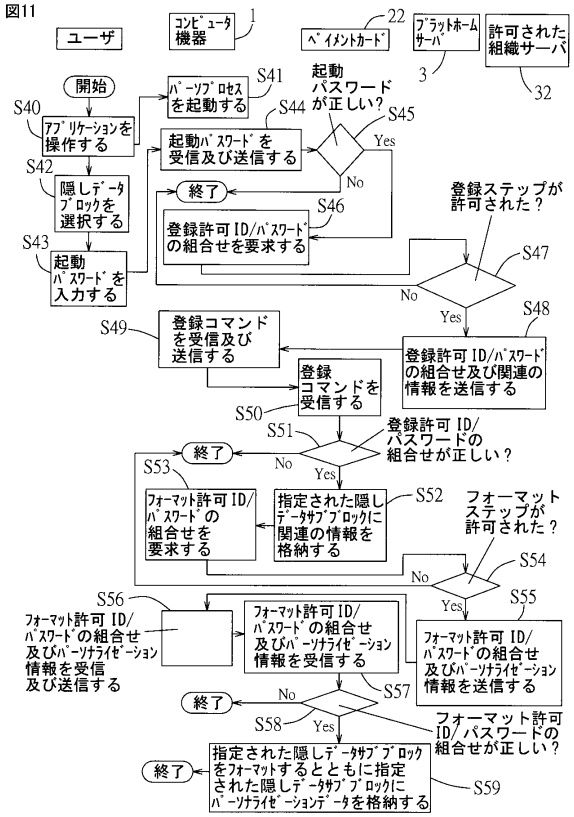
【図１０】

図10



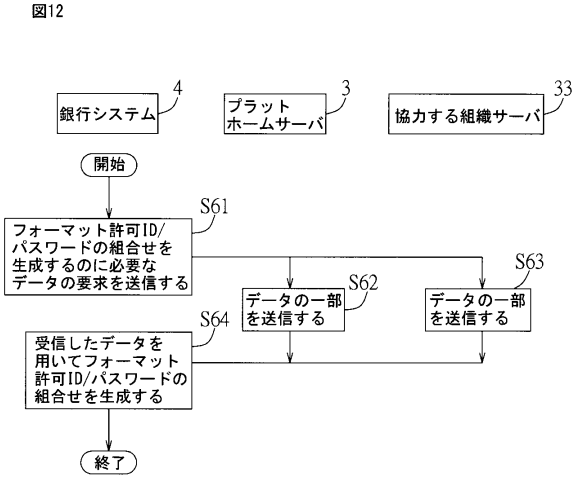
【図１１】

図11

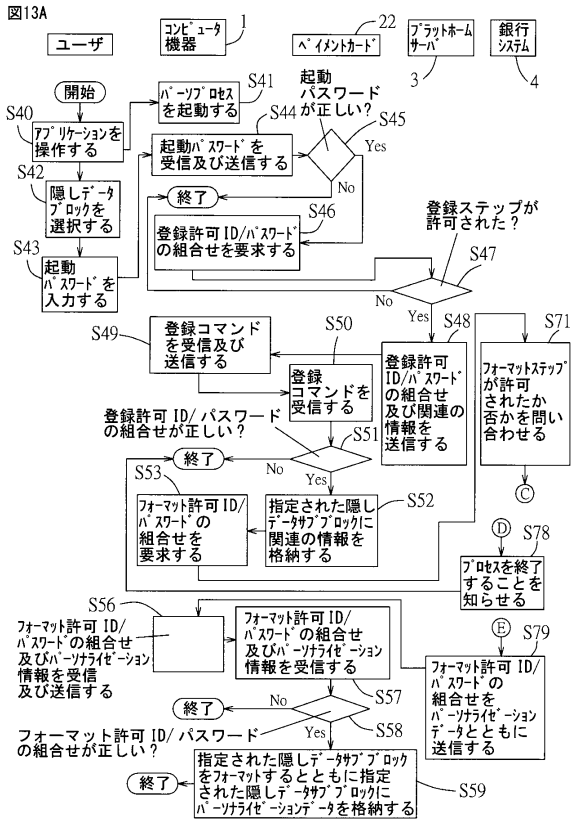


【図１２】

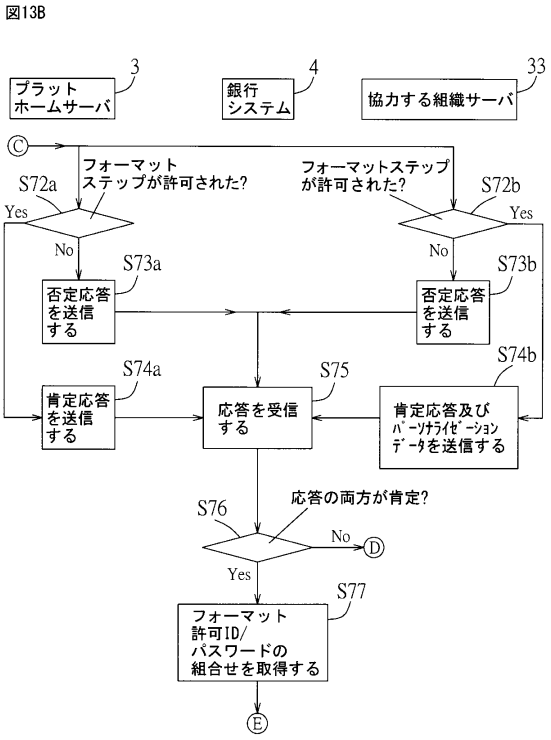
図12



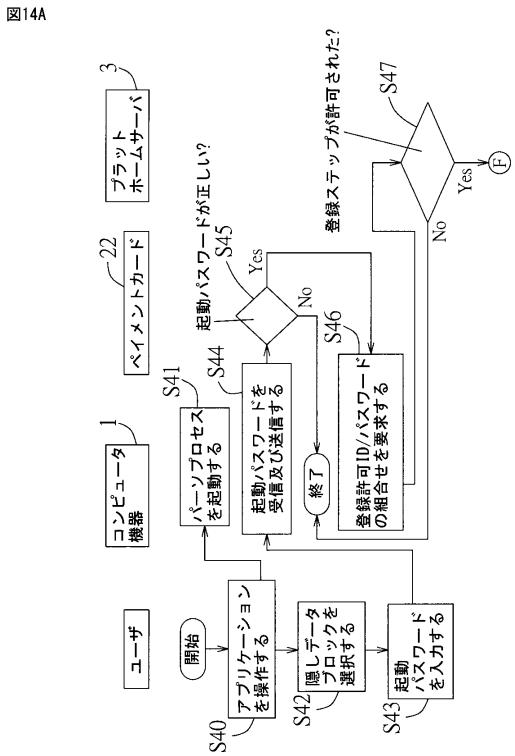
【図１３Ａ】



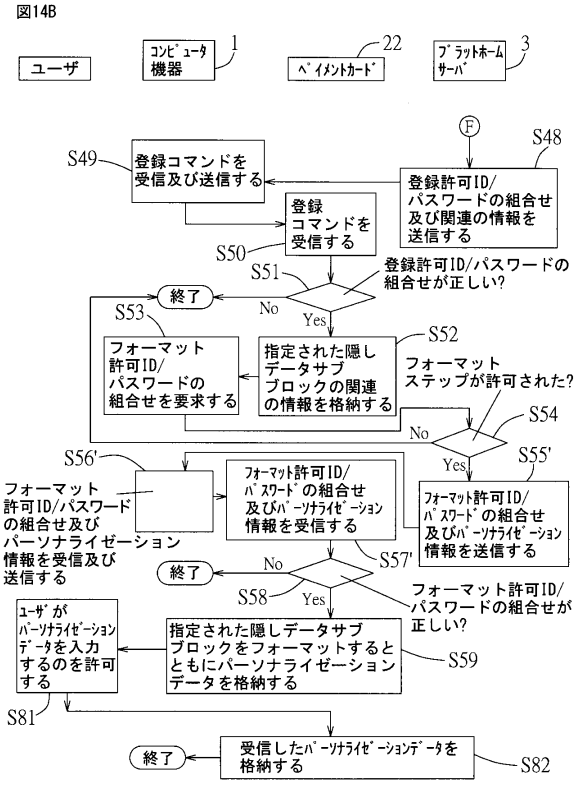
【図１３Ｂ】



【図１４Ａ】



【図１４Ｂ】



フロントページの続き

審査官　大野　朋也

(56)参考文献　特開２００３－２９６６４９（ＪＰ，Ａ）
特開２００３－３４６０６２（ＪＰ，Ａ）
特表２０１２－５０３２４３（ＪＰ，Ａ）
米国特許出願公開第２０１０／００６３８９３（ＵＳ，Ａ１）
特表２０１２－５２６３０６（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｑ　１０／００－９９／００