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

特許第4763163号
(P4763163)

(45)発行日　平成23年8月31日(2011.8.31)　(24)登録日　平成23年6月17日(2011.6.17)

(51)Int.Cl.		F I		
G07G 1/00	(2006.01)	G07G	1/00	311D
G06F 21/24	(2006.01)	G06F	12/14	560A
G06Q 40/00	(2006.01)	G06F	12/14	540A
G06Q 20/00	(2006.01)	G06F	17/60	224
G06K 17/00	(2006.01)	G06F	17/60	242

請求項の数 4　(全 9 頁)　最終頁に続く

(21)出願番号　特願2001-195270(P2001-195270)
(22)出願日　平成13年6月27日(2001.6.27)
(65)公開番号　特開2003-16527(P2003-16527A)
(43)公開日　平成15年1月17日(2003.1.17)
審査請求日　平成20年4月24日(2008.4.24)

(73)特許権者　000237639
富士通フロンテック株式会社
東京都稲城市矢野口１７７６番地
(74)代理人　100094514
弁理士　林　恒徳
(74)代理人　100094525
弁理士　土井　健二
(72)発明者　笠作　貴弥
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

審査官　植前　津子

最終頁に続く

(54)【発明の名称】取引端末装置

(57)【特許請求の範囲】

【請求項１】

顧客との取引処理を実行する取引端末装置において、

耐タンパ性を有しないで構成される本体と、

当該本体に脱着可能に取り付けられ、耐タンパ性を有して構成されるモジュールとを備え、

前記モジュールは、前記取引処理に必要な前記顧客に関する機密情報を取得する取得部と、当該機密情報を暗号化する暗号化部とを有し、

前記本体は、前記暗号化部によって暗号化された機密情報を受信し、当該機密情報を利用して前記取引処理を実行する制御部を有することを特徴とする取引端末装置。

【請求項２】

請求項１において、

前記機密情報は、前記顧客の個人情報を有し、

前記取得部は、前記顧客の個人情報を記憶する取引媒体から当該個人情報を読み取る読み取り部を有することを特徴とする取引端末装置。

【請求項３】

請求項１又は２において、

前記機密情報は、前記顧客の暗証情報を有し、

前記取得部は、前記暗証情報を入力するための入力部を有することを特徴とする取引端末装置。

【請求項４】
請求項１乃至３のいずれかにおいて、
前記制御部によって実行される取引処理は、前記機密情報を、暗号化されたまま、通信回線を介して所定のサーバに送信する第一の処理と、
当該サーバによって実行される前記機密情報の復号化処理、及び当該復号化された機密情報に基づいた所定の信用確認処理の結果情報を、前記通信回線を介して前記サーバから受信する第二の処理を含むことを特徴とする取引端末装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、顧客との取引を実行する取引端末装置に関し、特に、機密情報の漏洩を防止する機能である耐タンパ性を有する取引端末装置に関する。
【０００２】
【従来の技術】
従来より、クレジットカードによる決済や、銀行のキャッシュカードによるいわゆるデビットカード決済に用いられる取引端末装置が知られている。
【０００３】
図７は、決済機能を有する従来の取引端末装置の簡単なブロック構成図である。図７において、取引端末装置（単に、取引端末と称す場合がある）は、例えば、携帯端末であって、液晶のような表示部１０、決済プログラムや暗号化プログラムなどを格納するＲＯＭ１１、一時的なデータを格納するＲＡＭ１２、決済プログラムを実行するＣＰＵ１３、クレジットカードやキャッシュカードのカード番号を含むカード情報を読み取るカードリーダ１４、顧客が暗証情報（ＰＩＮ）を入力するためのキーボード１５、及び通信回線を通じて、所定の決済サーバと通信を行う回線部１６を備える。回線部１６は、ＲＯＭ１１に格納される暗号化プログラムによって暗号化された暗証情報やカード情報を決済サーバに送信する。決済サーバは、例えば、銀行やクレジット会社のホストコンピュータであって、取引端末からの暗号化されたカード番号や暗証情報を復号し、その照合を行い、決済許可判定のための信用確認処理などを行い、所定の応答データを取引端末に返信する。取引端末では、ＣＰＵ１３が決済プログラムを実行し、その応答データに対する決済処理を行う。
【０００４】
このような取引端末においては、キーボード１５から入力される暗証情報や、カードリーダ１４から読み取られるカード情報などの個人情報への不正アクセスを防止し、それらの機密性を担保する必要がある。すなわち、暗証情報やカード情報自体や、これらの暗号化プログラムなどがなんらかの手段により盗まれないようにする耐タンパ性が必要である。耐タンパ性は、取引端末の筐体のこじ開けなどの不正アクセスから機密情報の漏洩を防止する能力であって、例えば、配線を樹脂で固めることで、配線からの信号盗聴を不可能にしたり、所定の検知手段により端末の筐体が開けられたことが検知されると、内部のＲＯＭ１１やＲＡＭ１２の内容を破壊する機能を付加することなどにより実現されている。
【０００５】
そのため、従来においては、取引端末全体を、耐タンパ性を有する構造にする必要があり、決済機能を有する取引端末を専用装置として開発する必要があり、コスト高を招いていた。
【０００６】
【発明が解決しようとする課題】
また、取引端末は、決済機能のみならず、その汎用性を高めるために、他の機能を有してもよい。他の機能は、例えば、取引端末にバーコードリーダが設けられている場合に、商品のバーコード読み取り機能や、POS(Point of Sales)端末として機能するためのプライスルックアップ(PLU)機能や、商品の発注業務機能などが挙げられる。
【０００７】

このように、取引端末が決済機能を含む複数の機能を有する場合、その機能を実現するための複数のアプリケーションプログラムはＲＯＭ１１に格納され、各アプリケーションプログラムは、ＣＰＵ１３により実行される。

【０００８】

しかしながら、取引端末全体が耐タンパ性を有するように構成されると、その内部構造にアクセスできないので、例えば、取引端末に追加機能を付加したり、既に搭載されているアプリケーションプログラムをアップデートする場合のように、アプリケーションプログラムの追加・変更できない。例えば、取引端末の筐体が開けられると、ＲＯＭ１１の内容が消去されてしまう場合、ＲＯＭ１１に、新たにすべてのアプリケーションプログラムを組み込み直す必要がある。また、ＲＯＭ１１などの内部構成要素が樹脂で覆われている場合、それらをすべて交換する必要がある。

【０００９】

このように、顧客の個人情報のような機密情報の処理を含む取引（例えば決済取引）を実行する従来の取引端末装置は、装置全体が耐タンパ性構造を有するため、汎用性、拡張性に乏しく、またコスト高であった。

【００１０】

そこで、本発明の目的は、セキュリティを確保しつつ、汎用性、拡張性が高く、また、比較的コストの安い取引端末装置を提供することにある。

【００１１】

【課題を解決するための手段】

上記目的を達成するために、本発明では、顧客との取引処理を実行する取引端末装置の構成要素のうち、耐タンパ性を必要とする要素を、取引端末装置の本体に脱着可能なモジュールとして構成し、モジュールを耐タンパ性を有するように構成する。このように、耐タンパ性が必要な要素をモジュール化して、本体から分離することで、取引端末装置の本体は、耐タンパ性を備えなくともよくなり、本体に格納される各種取引に関するアプリケーションプログラムを容易に追加、変更、修正、更新することができ、汎用性、拡張性が向上する。

【００１２】

例えば、上記目的を達成するための本発明の取引端末装置の構成は、顧客との取引処理を実行する取引端末装置において、耐タンパ性を有しないで構成される本体と、当該本体に脱着可能に取り付けられ、耐タンパ性を有して構成されるモジュールとを備え、前記モジュールは、前記取引処理に必要な前記顧客に関する機密情報を取得する取得部と、当該機密情報を暗号化する暗号化部とを有し、前記本体は、前記暗号化部によって暗号化された機密情報を受信し、当該機密情報を利用して前記取引処理を実行する制御部を有することを特徴とする。

【００１３】

機密情報は、顧客のクレジットカードやキャッシュカードに記憶される個人情報（カード情報）や、顧客の暗証情報などである。また、取得部は、カード情報を読み取るためのカードリーダ（読み取り部）や、暗証情報を入力するためのキーボード（入力部）を備える。

【００１５】

【発明の実施の形態】

以下、本発明の実施の形態について説明する。しかしながら、本発明の技術的範囲が、本実施の形態に限定されるものではない。

【００１６】

図１は、本発明の実施の形態における取引端末装置のブロック構成図である。本実施の形態における取引端末装置は、携帯端末として例示され、取引端末の内部構成要素のうち、耐タンパ性が必要な一部の要素だけをモジュール化し、耐タンパ性の必要ない他の要素を有する取引端末の本体と脱着可能にする。

【００１７】

図１において、取引端末は、本体１と、それに脱着可能に取り付けられるモジュール２とから構成される。モジュール２は、図示されるように、クレジットカードやキャッシュカードのような取引媒体に記憶される情報（例えば、カード番号などの個人情報、以下、カード情報と称す場合もある）を読み取るカードリーダ１４、顧客が暗証情報(Personal Identification Number)を入力するためのキーボード（ＫＢ）１５、読み取られたカード情報及び入力された暗証情報を暗号化する暗号化部１８とを備え、さらに、これらを搭載するモジュール２は、耐タンパ性を有するように構成される。

【００１８】

暗号化部１８は、例えば、暗号化プログラムを格納するＲＯＭとそれを実行するＣＰＵ、一時的なデータを格納するＲＡＭを有する構成であってもよいし、論理回路で構成される暗号化回路で構成されてもよい。

【００１９】

また、モジュール２を耐タンパ性に構成するには、例えば、モジュール２に搭載されるカードリーダ１４やキーボード１５からの配線及び暗号化部１８を、樹脂で固める。これにより、物理的な信号盗聴が防止され、耐タンパ性が担保される。また、暗号化部１８が、ＣＰＵ、ＲＯＭ、ＲＡＭで構成される場合、所定の検知手段によりモジュール２のこじ開けが検知されると、ＲＯＭやＲＡＭのデータを破壊する手段を設けることで、耐タンパ性を担保する。

【００２０】

一方、本体１は、液晶のような表示部１０、決済プログラムやその他のアプリケーションプログラムを格納するＲＯＭ１１、一時的なデータを格納するＲＡＭ１２、決済プログラムやその他のアプリケーションプログラムを実行するＣＰＵ１３、及び通信回線を通じて、所定の決済サーバと通信を行う回線部１６などを備える。暗号化部１８が、モジュール２に設けられているので、本体１のＲＯＭ１１には、暗号化プログラムは格納されず、本体１のＣＰＵ１３は、カード情報や暗証情報の暗号化処理を実行しない。

【００２１】

図２は、本発明の実施の形態における取引端末を利用した決済処理例のフローチャートである。なお、本例では、取引端末の本体１のＣＰＵ１３に、決済金額（及び、好ましくは、さらに商品名（又は商品番号）など）が既に登録されているものとする。例えば、取引端末が、バーコードスキャナを搭載し、且つＰＯＳ機能を有する場合は、商品のバーコードをスキャンすることで、商品名及び金額などの情報を取得することができる。もちろん、バーコードスキャナを備えていなくとも、ＰＯＳ機能により、取引端末又は商品サーバ（図示せず）に登録されている商品情報を、キーボード１５を利用した選択操作により取得してもよし、ＰＯＳ機能もない場合であっても、キーボード１５から商品番号や金額などの商品情報が直接入力されてもよい。図２において、本体１のＣＰＵ１３は、決済金額が確定すると、まず、カード情報の読み取りを指示する（Ｓ１０）。指示は、例えば、本体１の表示部１０に表示される。顧客からカードを預かった店員の操作により、カードリーダ１４は、カード情報を読み取る（Ｓ１１）。カード情報は、クレジットカードの場合は、カード番号、キャッシュカードの場合は、口座番号を少なくとも含む顧客の個人情報である。

【００２２】

読み取られたカード情報は、機密情報であるので、モジュールの暗号化部１８によって暗号化され、本体１のＣＰＵ１３に送られる（Ｓ１２）。続いて、ＣＰＵ１３は、暗証情報の入力を指示する（Ｓ１３）。この入力指示に従って、顧客は、キーボード１５を操作して、自己の暗証情報を入力する（Ｓ１４）。

【００２３】

入力された暗証情報は、機密情報であるので、モジュール２の暗号化部１８によって暗号化され、本体１のＣＰＵ１３に送られる（Ｓ１５）。

【００２４】

本体１のＣＰＵ１３は、暗号化されたカード情報及び暗証情報を受信すると、それらと決

済金額（合わせて決済情報と称す場合がある）を、回線部１６から通信回線を介して、決済サーバに送信する（Ｓ１６）。カード情報及び暗証情報は、モジュール２から出力された後は、暗号化された状態で処理されるので、本体１が耐タンパ性を備えていなくとも、カード情報及び暗証情報の機密性は保持される。通信回線上においても、暗号化された状態なので、他人による盗聴が行われても、同様に機密性は維持される。なお、送信先の決済サーバは、クレジットカードやキャッシュカードの種類によって異なる。

【００２５】

決済サーバは、決済情報を受信すると、そのうちのカード情報と暗証情報を復号し（Ｓ１７）、信用確認処理を実行する（Ｓ１８）。信用確認処理は、少なくとも暗証情報の照合処理、決済金額の承認処理を含み、その結果、決済許可又は不許可を決定する。そして、決済サーバは、信用確認処理の結果に基づいて、決済許可／不許可情報を取引端末に送信する（Ｓ１９）。このとき、決済許可／不許可情報は、決済を許可するか又は決済を許可しないかの情報を少なくとも含み、カード情報や暗証情報のような機密情報は含まれない。取引端末の本体１のＣＰＵ１３は、決済許可／不許可情報により、決済処理の確認を行う（Ｓ２０）。

【００２６】

このように、本実施の形態例では、取引端末の構成要素のうち、カードリーダ１４やキーボード１５のように、カード情報や暗証情報などの機密情報を取得する要素と、この機密情報を暗号化する要素とをモジュール化し、そのモジュールを耐タンパ性に構成することで、取引端末全体の耐タンパ性を担保することができる。

【００２７】

また、耐タンパ性の必要な要素をモジュール化し、取引端末の本体１のＣＰＵ、ＲＯＭ、ＲＡＭから分離することで、本体１は、耐タンパ性を備えなくともよくなるので、取引端末で実行される機能を自由に追加、変更、修正、更新することが可能となり、取引端末の汎用性、拡張性が向上する。すなわち、本体１を簡単に開けることができ、本体１内部のＲＯＭ１１に簡単にアクセスすることができ（又は、本体１を開けても、ＲＯＭ１１の記憶内容は破壊されないので）、ＲＯＭ１１に格納するアプリケーションプログラムを容易に追加、変更、修正、更新することができる。

【００２８】

さらに、例えば決済機能を有さない取引端末、すなわち、耐タンパ性を必要としない取引端末については、耐タンパ性を備えない一般的なモジュールを用意することで、本体１を共通化することができる。具体的には、決済機能の必要性に応じて、耐タンパ性を有するモジュールか、耐タンパ性を有さないモジュールかを交換可能とする。さらに好ましくは、取引端末により実行可能な機能に応じて、様々なモジュールが提供され、機能に応じたモジュールを利用することで、本体１を共通化しつつ、様々な機能に対して適応可能となる。また、本体１を共通化できることから、取引端末のコストダウンが図られる。

【００２９】

図３は、本発明の実施の形態における取引端末装置の外観斜視図である。図３では、表示部１０を備える本体１に、カードリーダ１４やキーボード１５を備えるモジュールが脱着可能に取り付けられる。図４は、図３に示すモジュール２単体の外観図を示す図であり、図４は、図３に示されるモジュール２の上面図（ａ）及び側面図（ｂ）である。図４（ｂ）に示されるように、接点部（インターフェース）２１がモジュール２に設けられ、それと、本体１に設けられる接点部（図示せず）とを接触させることによって、モジュール２と本体１とは電気的に接続する。本体１とモジュール２間のインターフェースは、電気的な接点に限られず、別の形態であってもよい。このモジュール２と本体１の接点部（インターフェース）を介して、モジュール２で暗号化された情報が本体１に送信される。また、モジュール２を本体１に脱着可能に固定する取り付け機構（図示せず）も設けられる。

【００３０】

図５は、モジュール２単体の別の構成例を示す図である。図５に示すモジュール２は、ＰＣカードタイプで構成される。この場合、取引端末の本体１は、ＰＣカードスロットを有

し、取引端末の本体１は、例えば、ノートパソコンのような汎用コンピュータ装置であってもよい。

【００３１】

図６は、本発明の実施の形態における別の取引端末装置の外観斜視図である。図６の取引端末装置は、ノートパソコンである本体１に図５のモジュール２が挿入された構成を有する。具体的には、図５に示されるモジュール２を、取引端末の本体１のＰＣカードスロットに挿入すると、モジュール２は、カードリーダ１４及びキーボード１５が、ＰＣカードスロットの挿入口から突起するように、本体１に取り付けられる。

【００３２】

本発明の実施の形態では、耐タンパ性を必要とする処理として、カード情報や暗証情報を取り扱う決済処理を例に説明したが、耐タンパ性を必要とする処理は、これに限られず、例えば、キャッシュカードを利用して金融機関の口座残高を確認する処理など、機密情報を取り扱う取引処理であればよい。そして、本実施の形態は、機密情報を取り扱う取引処理を実行する取引端末装置すべてに適用可能である。また、本実施の形態の取引端末装置は、携帯端末に限らず、据置型の端末装置であってもよい。

【００３３】

また、顧客の個人情報を記憶する取引媒体は、クレジットカードやキャッシュカードに限られず、例えば、他の形態の取引媒体（例えば、カード形状でないＩＣメモリなど）であってもよい。

【００３４】

本発明の保護範囲は、上記の実施の形態に限定されず、特許請求の範囲に記載された発明とその均等物に及ぶものである。

【００３５】

【発明の効果】

以上、本発明によれば、顧客との取引処理を実行する取引端末装置の構成要素のうち、耐タンパ性を必要とする要素を、取引端末装置の本体に脱着可能なモジュールとして構成し、モジュールを耐タンパ性を有するように構成する。このように、耐タンパ性が必要な要素をモジュール化して、本体から分離することで、取引端末装置の本体は、耐タンパ性を備えなくともよくなり、本体に格納される各種取引に関するアプリケーションプログラムを容易に追加、変更、修正、更新することができ、汎用性、拡張性が向上する。

【００３６】

また、耐タンパ性を必要としない取引端末については、耐タンパ性を備えない一般的なモジュールを用意するなど、取引の種類に応じたモジュールを提供することで、取引端末装置の本体を共通化することができ、取引端末装置の低コスト化が図られる。

【図面の簡単な説明】

【図１】本発明の実施の形態における取引端末装置のブロック構成図である。

【図２】本発明の実施の形態における取引端末を利用した決済処理例のフローチャートである。

【図３】本発明の実施の形態における取引端末装置の外観斜視図である。

【図４】図３に示すモジュール２単体の外観図を示す図である。

【図５】モジュール２単体の別の構成例を示す図である。

【図６】本発明の実施の形態における別の取引端末装置の外観斜視図である。

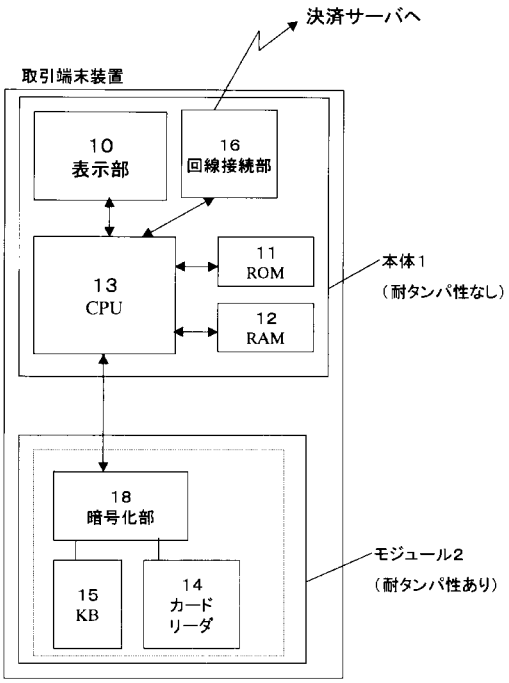
【図７】決済機能を有する従来の取引端末装置の簡単なブロック構成図である。

【符号の説明】

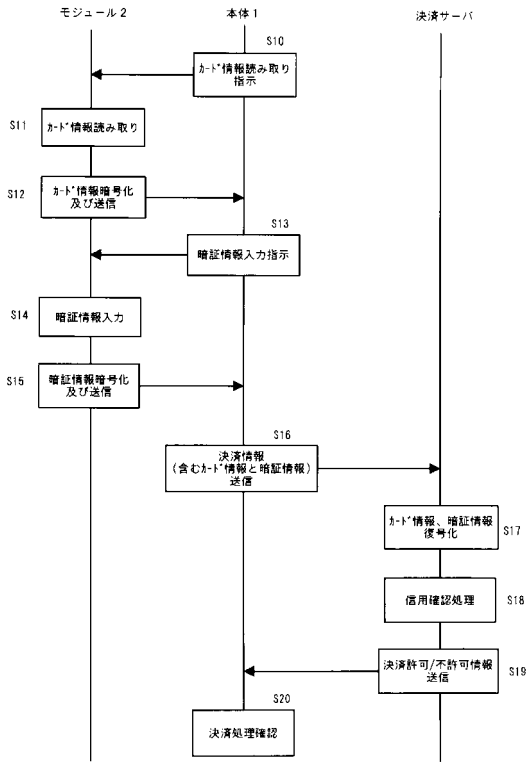
１　本体
２　モジュール
１１　ＲＯＭ
１２　ＲＡＭ
１３　ＣＰＵ
１４　カードリーダ

１５　キーボード
１８　暗号化部
２１　接点部（インターフェース）

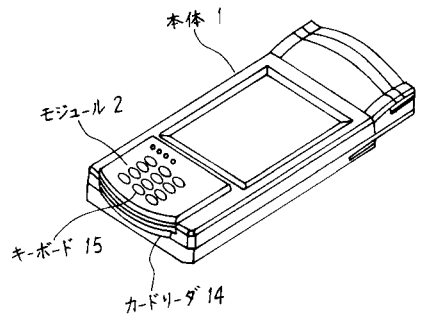
【図１】



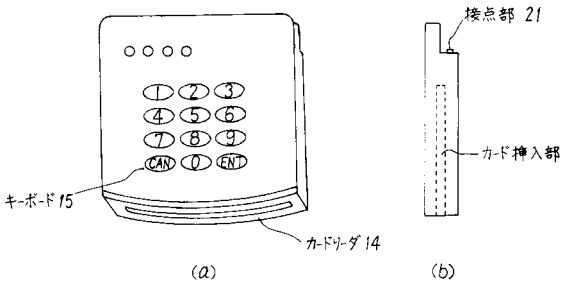
【図２】



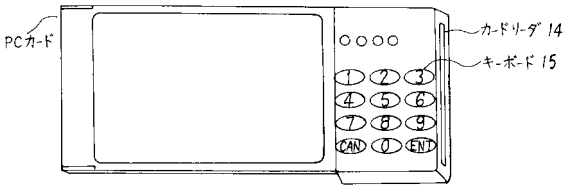
【図３】


本体 1
モジュール 2
キーボード 15
カードリーダ 14

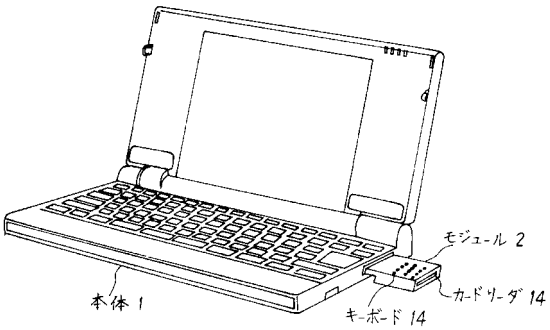
【図４】


キーボード15
カードリーダ 14
(a)
接点部 21
カード挿入部
(b)

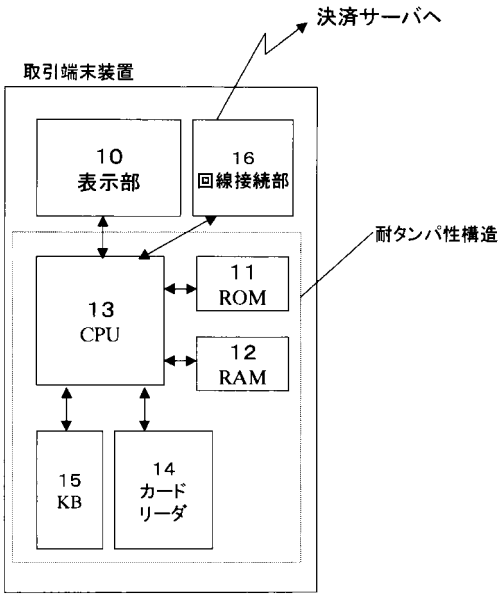
【図５】


PCカード
カードリーダ 14
キーボード 15

【図６】


モジュール 2
本体 1
カードリーダ 14
キーボード 14

【図７】


決済サーバへ
取引端末装置
10
表示部
16
回線接続部
耐タンパ性構造
11
ROM
13
CPU
12
RAM
15
KB
14
カード
リーダ

フロントページの続き

(51)Int.Cl.			FI		
G07G 1/12		*(2006.01)*	G06F	17/60	414
			G06F	17/60	432Z
			G06K	17/00	X
			G06K	17/00	Y
			G07G	1/12	321P

(56)参考文献 特開平02－075062（JP，A）
特開平11－024916（JP，A）
特開平08－255199（JP，A）
特開2001－014388（JP，A）
特開2000－068997（JP，A）

(58)調査した分野(Int.Cl.，DB名)
G07G 1/00-1/12
G06F 21/22