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

特許第4271576号
(P4271576)

(45)発行日　平成21年6月3日(2009.6.3)　(24)登録日　平成21年3月6日(2009.3.6)

(51)Int.Cl.		F I		
G06K 17/00	(2006.01)	G06K	17/00	S
G06F 3/08	(2006.01)	G06K	17/00	B
G06F 21/20	(2006.01)	G06K	17/00	V
G06K 19/07	(2006.01)	G06F	3/08	A
G06K 19/10	(2006.01)	G06F	15/00	330G

請求項の数 41　(全 18 頁)　最終頁に続く

(21)出願番号	特願2003-546284 (P2003-546284)
(86)(22)出願日	平成14年11月19日 (2002.11.19)
(65)公表番号	特表2005-509981 (P2005-509981A)
(43)公表日	平成17年4月14日 (2005.4.14)
(86)国際出願番号	PCT/US2002/037048
(87)国際公開番号	WO2003/044721
(87)国際公開日	平成15年5月30日 (2003.5.30)
審査請求日	平成17年11月18日 (2005.11.18)
(31)優先権主張番号	60/333,035
(32)優先日	平成13年11月19日 (2001.11.19)
(33)優先権主張国	米国(US)

(73)特許権者　504193228
ロバート　エル．バーチェット　ジュニア
アメリカ合衆国　２９３２３　サウスカロライナ州　チェスニー　バーチェット　ロード　１９８
(74)代理人　100077481
弁理士　谷　義一
(74)代理人　100088915
弁理士　阿部　和夫
(72)発明者　ロバート　エル．バーチェット　ジュニア
アメリカ合衆国　２９３２３　サウスカロライナ州　チェスニー　バーチェット　ロード　１９８

審査官　日下　善之

最終頁に続く

(54)【発明の名称】不正使用を防ぐ安全性を備えるトランザクションカードシステム

(57)【特許請求の範囲】

【請求項１】

ホストと、

ドローンメモリを有するドローンカードと

を備えたトランザクションカードシステムであって、

前記ホストは、前記ホストから前記ドローンカードへのデータ転送動作の間、前記ドローンカードの一部を物理的に収納するように適合され、

前記ホストは、

少なくとも１つのトランザクションカードに関するアカウント情報を記憶するように構成されたホストメモリと、

前記メモリに記憶された前記少なくとも１つのトランザクションカードに対応する可読の識別子を生成するように構成された出力回路と、

前記メモリに記憶されたトランザクションカードを選択するように構成されたユーザ入力装置と、

前記メモリ、出力回路、およびユーザ入力装置に動作可能なように結合されたプロセッサと

を備え、

前記出力回路は、前記ユーザ入力装置から受け取られた入力に応答して可読の識別子を生成し、

前記可読の識別子は、前記ホストによって自動的に生成されたセキュリティコードを含

み、かつ前記ドローンカードに転送され、

前記セキュリティコードは、トランザクションを認証するためにリモートコンピュータに転送可能であり、前記ホスト及び前記リモートコンピュータによって知られるランダムに変化するコードパターンであり、トランザクションごとに異なることを特徴とするトランザクションカードシステム。

【請求項２】

前記プロセッサに動作可能なように結合されたセキュリティ入力装置をさらに備え、

前記セキュリティ入力装置は、前記セキュリティ入力装置によって受け取られた入力に基づいて、前記メモリに記憶されたアカウント情報へのアクセスを制限することを特徴とする請求項１に記載のシステム。

【請求項３】

前記セキュリティ入力装置は認証センサであることを特徴とする請求項２に記載のシステム。

【請求項４】

前記認証センサは生体認証センサであることを特徴とする請求項３に記載のシステム。

【請求項５】

第１のユーザは、前記認証センサによって受け取られる入力に基づいて、前記メモリに記憶された第１のアカウント情報のセットへのアクセス権を有し、第２のユーザは、前記認証センサによって受け取られる入力に基づいて、第２のアカウント情報のセットへのアクセス権を有することを特徴とする請求項３に記載のシステム。

【請求項６】

前記認証センサは指紋センサであることを特徴とする請求項５に記載のシステム。

【請求項７】

前記出力回路によって生成される前記可読の識別子は磁気信号であることを特徴とする請求項１に記載のシステム。

【請求項８】

前記出力回路によって生成される前記可読の識別子はバーコードであることを特徴とする請求項１に記載のシステム。

【請求項９】

前記セキュリティコードは、暗号化アルゴリズムに基づくことを特徴とする請求項１に記載のシステム。

【請求項１０】

前記プロセッサに動作可能なように結合されたステータス表示をさらに備え、

前記ステータス表示は、使用不可の状態と使用可能な状態とで切り替わるように構成され、前記ステータス表示は、前記出力回路が可読の識別子を生成すると使用可能になることを特徴とする請求項１に記載のシステム。

【請求項１１】

前記ステータス表示は、カードリーダによって読み取られると使用不可になることを特徴とする請求項１０に記載のシステム。

【請求項１２】

前記ステータス表示は、前記出力回路が可読の識別子を生成した後に所定の時間が経過すると使用不可になることを特徴とする請求項１０に記載のシステム。

【請求項１３】

前記ステータス表示は、前記ステータス表示が使用可能な時に点灯する照明であることを特徴とする請求項１０に記載のシステム。

【請求項１４】

前記ステータス表示は、前記ステータス表示が使用可能である時には第１の色を点灯し、前記ステータス表示が使用不可である時には第２の色を点灯する照明であることを特徴とする請求項１０に記載のシステム。

【請求項１５】

前記ステータス表示は、前記ステータス表示が使用可能である時には第１の可聴音を提供し、前記ステータス表示が使用不可の時には第２の可聴音を提供することを特徴とする請求項１０に記載のシステム。

【請求項１６】

アカウント情報をダウンロードする、前記プロセッサに動作可能なように結合されたインタフェースをさらに備えたことを特徴とする請求項１に記載のシステム。

【請求項１７】

前記プロセッサに動作可能なように結合されたディスプレイをさらに備え、

前記ディスプレイは、前記ユーザ入力装置に応答して、前記メモリに記憶されたアカウント情報を表示することを特徴とする請求項１に記載のシステム。

【請求項１８】

ドローンメモリ、ドローンインタフェース、および前記ドローンメモリに記憶されたアカウント情報に対応する可読の識別子を生成するように構成された出力回路を有するドローンカードと、

前記ドローンカードを収納するスロットを有するホストであって、

少なくとも１つのトランザクションカードについてのアカウント情報を記憶するように構成されたホストメモリと、

前記ドローンインタフェースと通信して前記ドローンカードにアカウント情報を転送するように構成されたホストインタフェースと、

生体認証センサと、

前記ホストメモリ、前記ホストインタフェース、および前記生体認証センサに動作可能なように接続されたプロセッサと、

前記ホストと通信可能なユーザ入力装置と、前記ホストの前記スロット内に収納されるように構成されたカード様部分とを有する登録装置と

を有するホストと

を備え、

前記ホストは、前記生体認証センサを介してユーザが確認されると前記ドローンメモリにアカウント情報を転送し、

前記ホストは、前記ホストの使用を防止する使用不可の状態と前記ホストの使用を可能にする使用可能な状態との間を切り替わるように構成され、前記登録装置のユーザ入力装置から受け取られた入力に応答して前記使用可能状態に切り替わることを特徴とするトランザクションカードシステム。

【請求項１９】

前記生体認証センサは指紋センサであることを特徴とする請求項１８に記載のシステム。

【請求項２０】

第１のユーザは、前記生体認証センサによって受け取られる入力に基づいて、前記メモリに記憶された第１のアカウント情報のセットへのアクセス権を有し、第２のユーザは、前記生体認証センサによって受け取られる入力に基づいて、第２のアカウント情報のセットへのアクセス権を有することを特徴とする請求項１８に記載のシステム。

【請求項２１】

前記ドローンカードの前記出力回路によって生成される前記可読の識別子は磁気信号であることを特徴とする請求項１８に記載のシステム。

【請求項２２】

前記ドローンカードの前記出力回路によって生成される前記可読の識別子はバーコードであることを特徴とする請求項１８に記載のシステム。

【請求項２３】

前記ドローンカードによって生成される前記可読の識別子はセキュリティコードを含むことを特徴とする請求項１８に記載のシステム。

【請求項２４】

前記セキュリティコードはトランザクションごとに異なることを特徴とする請求項２３に記載のシステム。

【請求項２５】

前記セキュリティコードはトランザクションごとに連続的に変わることを特徴とする請求項２３に記載のシステム。

【請求項２６】

前記セキュリティコードは、暗号化アルゴリズムに基づくことを特徴とする請求項２３に記載のシステム。

【請求項２７】

前記ドローンカードはさらにステータス表示を備え、

前記ステータス表示は、使用不可の状態と使用可能な状態とを切り替わるように構成され、前記ステータス表示は、前記ドローンカードの前記出力回路が可読の識別子を生成すると使用可能になることを特徴とする請求項１８に記載のシステム。

【請求項２８】

前記ステータス表示は、出力回路が可読の識別子を生成した後に所定の時間が経過すると使用不可になることを特徴とする請求項２７に記載のシステム。

【請求項２９】

前記ステータス表示は、前記ステータス表示が使用可能の時に点灯する照明であることを特徴とする請求項２７に記載のシステム。

【請求項３０】

前記ドローンインタフェースと前記ホストインタフェースは電気接点を使用して通信することを特徴とする請求項１８に記載のシステム。

【請求項３１】

前記ドローンインタフェースと前記ホストインタフェースはワイヤレス通信を使用して通信することを特徴とする請求項１８に記載のシステム。

【請求項３２】

前記ドローンインタフェースと前記ホストインタフェースはレーザ通信を使用して通信することを特徴とする請求項１８に記載のシステム。

【請求項３３】

前記ドローンインタフェースと前記ホストインタフェースは赤外線通信を使用して通信することを特徴とする請求項１８に記載のシステム。

【請求項３４】

前記ホストは、電源として太陽電池を含むことを特徴とする請求項１８に記載のシステム。

【請求項３５】

前記太陽電池に動作可能なように接続された光増幅器をさらに備えたことを特徴とする請求項３４に記載のシステム。

【請求項３６】

前記光増幅器は、前記太陽電池を覆う少なくとも１つのプリズムであることを特徴とする請求項３５に記載のシステム。

【請求項３７】

前記ホストは、前記ホストが損傷した場合に前記ホストメモリを消去する改ざん防止手段を含むことを特徴とする請求項１８に記載のシステム。

【請求項３８】

前記ドローンカードは、前記ドローンカードが損傷した場合に前記ドローンメモリを消去する改ざん防止手段を含むことを特徴とする請求項１８に記載のシステム。

【請求項３９】

前記ドローンカードは、標準的なクレジットカードとほぼ同じ厚みを有することを特徴とする請求項１８に記載のシステム。

【請求項４０】

前記ホストは、標準的なクレジットカードの約３倍の厚みを有することを特徴とする請求項３９に記載のシステム。

【請求項４１】

前記ホストメモリに記憶されたトランザクションカードのアカウント情報を選択するように構成されたユーザ入力装置をさらに備えたことを特徴とする請求項１８に記載のシステム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、一般には、トランザクションカードの技術分野に関する。より詳細には、本発明は、不正使用を防止するセキュリティ機能を備えた改良されたトランザクションカードシステムに関する。

【背景技術】

【０００２】

クレジットカード、デビットカード、アクセスカードなどのトランザクションカードが普及している。トランザクションカードは利用者に利便性をもたらす一方で、不正な使用も頻繁に発生している。不正な使用は、郵便物の盗難、偽造、および盗難カードを通じて行われる可能性がある。クレジットカード会社が詐欺行為のために被る損害は毎年数億ドルに上るものと思われる。この損害は、最終的には、価格に上乗せされるという形で顧客が負担しなければならない。

【０００３】

いくつかの文献に上述のような従来の技術に関連した技術内容が開示されている（例えば、特許文献１参照）。

【０００４】

【特許文献１】米国特許第６，０８９，４５１号明細書

【発明の開示】

【発明が解決しようとする課題】

【０００５】

トランザクションカードの不正使用を防止する試みは複数行われているが、新規のトランザクションカードシステムに対するさらなる必要性が存在する。

【課題を解決するための手段】

【０００６】

本発明は、従来技術の構造と方法の各種の欠点を認識し、対処する。したがって、本発明の目的は、不正使用を防止するセキュリティ機能を有する改良されたトランザクションカードシステムを提供することである。

【０００７】

本発明は、少なくとも１つのトランザクションカードアカウントに関する情報を有するホストを備えるシステムを提供する。ホストは、ホスト内に担持されるドローン（drone）カードにカードデータを転送するように機能する。ホストは、ドローンカードの使用の前にユーザを認証する生体認証センサまたは他の適切な識別子手段を含む。ユーザが認証されると、ドローンカードは、ユーザによって選択されたトランザクションカードアカウントに対応する可読の識別子を提供する。当業者には、代替としてホストの機能はドローンカード中に組み込んでもよいことが理解されよう。

【０００８】

本発明のこの他の目的、特徴、および態様は、下記でより詳細に述べる、ここに開示される要素の各種の組み合わせおよびサブコンビネーションによって達成される。

【０００９】

当業者に対する、本発明の最良の形態を含む完全で、本発明を可能にする開示を添付図面を参照して本明細書の以下の部分でより詳細に説明する。

【００１０】

本明細書および図面で参照符号を繰り返し使用することは、本発明の同一または同様の特徴または要素を表すものとする。

【発明を実施するための最良の形態】

【００１１】

本発明の現在の時点で好適実施形態を詳細に参照し、そのような実施形態の１つまたは複数の例を添付図面に示す。各例は、本発明の説明として提供し、本発明を限定するものではない。実際、当業者には、本発明の範囲または趣旨から逸脱することなく、本発明の変更形態および変形形態を作成できることが明らかであろう。例えば、ある実施形態の一部として図示または説明する特徴を別の実施形態で使用して、さらなる実施形態を得ることができる。

【００１２】

一実施形態では、本発明は、１つまたは複数のカードアカウントに関する情報を収容するホストを提供する。カードアカウントには、これらに限定しないが、クレジットカード、デビットカード、図書館カード、ソーシャルセキュリティカード、医療保険カード、電話カード、アクセスカード、割引カード、および特定の人またはグループに関連する識別情報を含んでいるその他のカードが含まれる。ホスト内に担持されるドローンカードは、カードアカウントに対応するように構成することができる。多くの場合、ホストは、ユーザが数個のカードアカウントから特定のカードアカウントを選択できるように構成することができる。登録装置が動作して、個人またはグループが使用するためにホスト上の各種のカードアカウントに関する情報をプログラムする。

【００１３】

登録装置によって初期化されると、ホストは、認証のために必要なユーザ情報と、カードアカウントに関連するデータを含む。ホストに記憶された特定のカードアカウントを使用するには、まずホストの認証センサを使用してユーザを認証する。所望のカードアカウントが選択されると、ホストは、選択されたカードアカウントに関連するデータをドローンカードにアップロードする。ドローンカードは、選択されたカードアカウントに対応する可読の識別子（すなわち磁気信号、バーコードなど）を生成する出力回路を含むことができる。ドローンカードが特定の期間中に使用されない場合、ドローンカードは使用不可にされ、使用するには再度認証を必要とすることが好ましい。同様に、ドローンカードは、トランザクションが完了すると使用不可にすることができる。

【００１４】

図１Ａ、１Ｂ、および１Ｃに、本発明によるドローンカード１００を担持するホスト１０を示す。ホスト１０は、前面１２と、ドローンカード１００を収納するスロット１４を有する。ホスト１０は、比較的硬質の材料から形成されることが好ましく、ドローンカード１００を収納し、必要な電子回路を収容するのに必要な厚み以下の厚みであることが好ましい。多くの場合、ホスト１０の厚みは、標準的なクレジットカードの厚みの約３倍以下である。図ではスロット１４がホスト１０の短辺の側についているが、スロット１４はホスト１０のどの側に位置してもよいことを理解されたい。例えば、一部の事例では、左利きの人でも右利きの人でもドローンカード１００をより容易に取り出せるようにするために、ホスト１０の長端にスロット１４を配置することが望ましい場合がある。スロット１４の近くにある切り込み部分１６は、ユーザの指がドローンカード１００に届くようにして、カード１００をホスト１０から容易に取り出せるようにする。ホスト１０は、携帯電話や携帯情報端末（ＰＤＡ）などの他の電子機器中に組み込むこともできる。

【００１５】

ホスト１０の内部は、何者かがホストに記憶されたアカウント情報を入手しようとするのを防止する適切な改ざん防止機構を備えることができる。例えば、図のホスト１０の実施形態は、表面のすぐ下に目の細かい網目状の針金１８を含んでいる。網目状の針金１８は、連続的につなげて、網目が破壊されるとホスト１０に記憶されたすべての情報が削除されるようにすることができる。ホスト１０を開けようと試みると網目が破壊することを理解されたい。

【００１６】
ホスト１０は、ユーザの識別を検証する、一体化して取り付けられた認証センサ２０を含むことが好ましい。認証センサ２０は、指紋センサなど適切な生体認証センサであることが好ましい。この目的に使用することが可能な指紋センサの１つは、フロリダ州メルボルンのＡｕｔｈｅｎＴｅｃ社から販売されるＦＩＮＧＥＲＬＯＣ（商標）と称するものである。認証センサ２０は、個人識別番号（ＰＩＮ）のキーパッドなどユーザの識別を検証する他の適切な手段でもあってよいことを理解されたい。
【００１７】
図の実施形態で、ホスト１０は、ユーザがホスト１０に記憶された各種のカードアカウントに関連する情報を見られるディスプレイ３０を含む。ディスプレイ３０は、キャラクタ液晶ディスプレイ（「ＬＣＤ」）であることが好ましいが、任意の他の適切なディスプレイを使用することができる。特定の文字を用いてＬＣＤを駆動する方法は当技術分野では周知である。
【００１８】
ホスト１０の前面１２に装着されたスクロールボタン４０は、ユーザがアクセス権を有するホスト１０に記憶された各種のカードアカウントの名前をスクロールして見ることを可能にする。ユーザがカードアカウントの名前をスクロールすると、各アカウント名をディスプレイ３０に表示することができる。ユーザが使用する特定のカードアカウントを決定すると、入力ボタン５０を使用して所望のカードアカウントを選択する。下記で詳細に述べるように、次いで、選択されたカードアカウントに一致する情報がセキュリティコードとともにドローンカード１００にアップロードされる。特定のカードアカウントに関する情報も、表示ボタン６０を選択することによりディスプレイ３０で見ることができる。ディスプレイスクロールボタン４０、入力ボタン５０、および表示ボタン６０は、スライドスイッチまたは他のユーザ入力装置として形成できることを理解されたい。
【００１９】
ホスト１０は、登録装置２００（図５）からユーザデータをダウンロードし、ドローンカード１００にデータをアップロードするインタフェース７０を含む。カードデータは、特定のカードアカウントに対応するデータを含み、一方、ユーザデータは、指紋の画像などユーザを確認するために必要な情報と、ユーザに関連付けられた各カードアカウントについてのカードデータを含む。データを交換するための多数の機器および技術に照らして、インタフェースは、電気的接触、赤外線通信、あるいはレーザ通信を使用するなど、各種方式で実施することができる。ドローンカード１０に１つのみのカードアカウントを転送することが意図される場合、ホスト１０は、ドローンカード１００に恒久的にアカウントデータを書き込むことができる。電気的接触のインタフェースに関しては、ホスト１０は、登録装置２００およびドローンカード１００上の電気接点とインタフェースを取ることができる内部の電気接点７２を含む。登録装置２００は、ホスト１０に必要なデータを提供するためにスロット１４に挿入することができるカード状のコネクタを含むことが好ましい。
【００２０】
次いで図２を参照すると、ホスト１０は、オンボードメモリ８２と電気通信する内部のマイクロプロセッサ８０を有する。メモリ８２は、適切なＥＥＰＲＯＭ（Electronically Erasable and Programmable Read Only Memory）であることが好ましく、カードデータ、ユーザデータ、およびセキュリティコードを記憶するように機能する（これらについては下記でより完全に説明する）。好ましくはバッテリである電源９０が、マイクロプロセッサ８０およびメモリ８２に電力を提供する。この目的には、イスラエルのＫｉｂｂｕｔｚ ＥｉｎａｔのＰｏｗｅｒ Ｐａｐｅｒ Ｌｔｄ．から販売されるバッテリなど、超薄型のバッテリを利用することが望ましい。電源９０は、充電可能であり、太陽電池９２を使用して補充的な充電を受け取ることができる。光学式表示灯（図示せず）によっても、バッテリの電力が低下したことを知らせることができる。
【００２１】

任意で、太陽電池９２に利用できる周辺光を増大あるいは増幅する手段を提供してもよい。例えば、一実施形態では、図１Ｄに示すように、太陽電池９２を覆うようにホスト１０の前面１２中に光学プリズム９３を成型してもよい。適切な光増幅器の構成と選択は、当業者には理解されよう。バッテリの寿命を延ばすために、マイクロプロセッサ８０は、認証センサ２０またはスクロールボタン４０によって起動されるまでは「スリープ」モードを保つことが好ましい。用語「スリープ」モードとは、入力によって中断されるまでマイクロプロセッサによって維持される低電力状態を意味する。

【００２２】

認証センサ２０、スクロールボタン４０、入力ボタン５０、および表示ボタン６０は、マイクロプロセッサ８０に入力データを提供する。インタフェース７０もマイクロプロセッサ８０に入力データを提供し、また出力データを受け取る。マイクロプロセッサ８０は、入力データに応答して機能する。

【００２３】

マイクロプロセッサ８０は、入力データをメモリ８２に記憶されたユーザデータと比較して入力データが有効なユーザを表すかどうかを判定することにより、認証センサ２０からの入力データに応答する。複数のユーザをホストに関連付けることができ、したがって、ホストのユーザデータは複数の者に対応する可能性がある。例えば、認証センサ２０が指紋センサである場合は、ホスト１０に関連付けられた各人の指紋が、ホスト１０に記憶されている選択されたカードアカウントへのアクセス権を提供する。

【００２４】

次いで図６を参照すると、ユーザを認証する際の最初のステップは、ユーザの指紋をスキャンするなどにより認証センサ２０からのユーザの入力データを読み取ることである。次いで、ホストは、認証センサ２０によってスキャンされたデータを、ホストのメモリに記憶されたユーザデータと比較する。スキャンされたデータがメモリに記憶されたユーザデータと一致しない場合、ユーザはカードアカウントへのアクセスを許可されない。あるいは、スキャンされたデータがメモリに記憶されたユーザデータと一致する場合は、ユーザには、そのユーザがアクセス権を有するすべてのカードアカウントへのアクセス権が与えられる。

【００２５】

ホストに関連付けられたすべてのユーザが、ホストに記憶された各カードに必ずしもアクセスできる訳ではない。ホストは、複数レベルのセキュリティを提供して、特定のユーザが特定のカードアカウントへのアクセス権を得られないように制限することができる。例えば、「ユーザＡ」と「ユーザＢ」のユーザデータとともに「カードＡ」（例えばＶｉｓａ）と「カードＢ（例えばＡｍｅｒｉｃａｎ　Ｅｘｐｒｅｓｓ）についてのカードデータがメモリに記憶され、認証センサとして指紋センサを含むホストを考えられたい。したがって、「ユーザＡ」と「ユーザＢ」の両方が各自の指紋を使用してホストを起動することができる。この例のユーザデータに基づくと、「ユーザＡ」は「カードＡ」に関連付けられ、「カードＡ」にアクセスすることができるが、「カードＢ」には関連付けられておらず、アクセスすることができない。「ユーザＡ」がホストで利用できるカードをスクロールして見る際には「カードＡ」だけが表示される。しかし、ユーザデータは、「ユーザＢ」を「カードＡ」と「カードＢ」の両方に関連付けている。その結果、「ユーザＢ」は「カードＡ」と「カードＢ」の両方を見、使用することができる。

【００２６】

認証が終わると、マイクロプロセッサ８０は、ユーザに関連付けられたユーザデータ中の次のカードアカウントの識別をもってディスプレイ３０を駆動することにより、スクロールボタン４０からの入力に応答する。スクロールボタンを選択し続けることにより、ユーザは、自身がアクセス権を有するホスト１０に記憶されたカードアカウントの全リストを見ることができる。表示ボタン６０からの入力に応答して、マイクロプロセッサ８０は、セキュリティコードと併せて、選択されたカードアカウントのカードデータ（例えばアカウント番号）を表示する。マイクロプロセッサ８０は、インタフェース７０を介してセ

キュリティコードとともにカードデータをドローンカード１００にアップロードすることにより、入力ボタン５０からの入力に応答する。任意で、ドローンカード１００は、カードデータが入ったメモリを有することができ、セキュリティコードだけがドローンカード１００にアップロードされる。

【００２７】

セキュリティコードは、カードアカウントおよびトランザクションに関連付けられた一意のコードである。カードアカウントは不変であるが、セキュリティコードは通例トランザクションごとに異なる。誰かがセキュリティコードの再使用を試みると、そのトランザクションは不正として拒否される。例えば選択されたカードアカウントが電話カードである場合、電話会社は、カードアカウント番号と所定のセキュリティコードの両方が提供されなければ、課金を認可しない。第３者がカード番号と以前のセキュリティコードを後に使用するために傍受した場合、電話会社は課金を拒否する。この認証プロセスを図８の表に示す。

【００２８】

セキュリティコードは、ホストに存在するアルゴリズムに基づいて生成された４桁の英数文字コードであることが好ましい。例えば、セキュリティコードは、ホスト１０に存在する内部クロックに基づいて無作為に変化することができる。セキュリティコードは２０秒間など一定の時間間隔中に変化してセキュリティの増大を提供することができる。セキュリティコードを検証する中央コンピュータをホストと同期させて、セキュリティコードを認識することができる。あるいは、ホストのメモリに複数のセキュリティコードを記憶してもよい。セキュリティコードを検証するために、トランザクションを行うリーダは、現在のセキュリティコードを発行元エンティティの中央コンピュータに提供し、中央コンピュータは予想されるコードと一致するかどうかを調べる。このコンピュータは、行われる次のトランザクションの特定のセキュリティコードを予想するようにプログラムされる。

【００２９】

図３Ａおよび３Ｂから分かるように、ドローンカード１００は、標準的なクレジットカードとほぼ同じサイズと厚みを有することが好ましい。ただし、クレジットカードを見る誰にでも見えるアカウント番号を保持するクレジットカードと異なり、ドローンカード１００は、ドローンカードに関連付けられたユーザまたはグループの名前を任意で除いては、目に見える情報を含まないことが好ましい。任意で、権限のあるユーザの写真１０２がホスト１２あるいはドローンカード上１００に提供される。写真１０２は、権限のあるユーザの恒久的な静止写真とするか、または、権限のあるユーザの電子写真を一時的に表示する電子ディスプレイとしてもよい。電子写真を使用する場合は、ホスト１００によって権限のあるユーザに一致する写真が表示される。したがって、ホストには複数のユーザの写真を記憶することができ、許可された特定のユーザに基づいて該当する写真がドローンカード１００に転送され、表示される。

【００３０】

ドローンカード１００を用いてトランザクションを行うのに必要なすべてのデータは、アクティブ状態時には可読の識別子１３０に提供される。アクティブ状態では、可読の識別子１３０はユーザがトランザクションを行うことを可能にする。その他の時には、可読の識別子１３０は使用不可にされ、トランザクションを行うことはできない。可読の識別子１３０の状態を知らせるためにステータス表示灯１１０を提供することができる。例えば、表示灯１１０は、可読の識別子がアクティブな時に点灯する緑色ＬＥＤとすることができる。視覚障害者のために、音声による指示を提供して、可読の識別子１３０の状態の変化を知らせることもできる。

【００３１】

ドローンカード１００は、ホスト１０からカードデータを受け取るインタフェース１２０を含む。上記のようにデータ交換には多数の装置と技術があるので、インタフェース１２０は、電気的接触、赤外線通信、あるいはレーザ通信を使用するなど各種の方式で実施

することができる。電気的接触のインタフェースについては、ドローンカード１００は、ホスト１０上の電気接点７２とインタフェースを取ることが可能な電気接点１２２を含む。

【００３２】

次いで図４を参照し、ドローンカード１００の好適な一実施形態の内部構造を説明する。この場合、ドローンカード１００は、好ましくは揮発性メモリであるオンボードメモリ１５０と電気通信する内部コントローラ１４０を有する。この実施形態では、ドローンカード１００は、セキュリティコードと併せてカードデータを記憶するのに十分なメモリを有する。上記のように超薄型のバッテリであることが好ましい電源１６０が、コントローラ１４０およびメモリ１５０に電力を提供する。電源１６０は、ガルバニック接続、静電誘導、あるいはその他の適切な手段を通じてホスト１０から電力を受け取ることにより充電可能とすることができる。

【００３３】

上記のように、ドローンカード１００は、ホスト１０から受け取ったカードデータをメモリ１５０に記憶するために転送するコントローラ１４０と電気通信するインタフェース１２０を含む。先に述べたように、当技術分野には、電気的接触、レーザ通信、および赤外線通信を使用するなど、多数のデータ転送技術がある。

【００３４】

コントローラ１４０は、ホスト１０から受け取ったカードデータに基づいて可読の識別子１３０をアクティブ化する信号を生成する。可読の識別子１３０は、図７に示す従来型のカードリーダ１６５などの既存のリーダと互換性のある形態であることが好ましい。可読の識別子１３０は、例えば、一時的な磁気ストライプ、あるいは認証後に一時的にアクティブ化されるバーコードである。

【００３５】

一時的な磁気ストライプを生成するために、ドローンカードは、カードアカウントに対応する磁気信号を生成する電気的配列を含むことができる。電気的配列を使用した一時的な磁気信号の生成に関する解説を得るには、参照により本明細書に組み込まれる特許を参照されたい（特許文献１）。

【００３６】

あるいは、可読の識別子１３０は、ドローンカード１００内に収納された磁性粉あるいはその他の材料を使用して生成することもできる。ホスト１０は、磁性粉の物理的位置あるいは形状を変えて各種の可読の識別子を生成することができる。例えば、磁性粉を配向して、標準的なカードリーダで読み取れる一時的な磁気ストライプを生成することができる。

【００３７】

あるいは、可読の識別子１３０は、カードデータに対応するバーコードを生成するＬＣＤあるいはその他の適切な表示であってもよい。カードデータに基づいて、ホスト１０は、対応するバーコードを生成するのに十分なデータを、ＬＣＤに表示するためにドローンカード１００に転送する。可読の識別子１３０に示されるバーコードは、ドローンカード１００に転送されるカードアカウントごとに異なる。

【００３８】

このタイプのドローンカード１００に磁気カードリーダを使用するのに代えて、バーコードリーダでドローンカードをスキャンすることもできる。例えば、ドローンカードのメモリに存在するカードアカウントがクレジットカードである場合は、そのクレジットカードに対応するバーコードが可読の識別子として表示される。バーコードリーダは、可読の識別子を読み取り、必要な信用機関と通信して該当するアカウントに課金する。

【００３９】

上記のように、ステータス表示灯１１０の状態でドローンカードが使用できる状態かどうかを知らせる。カードデータが最初にドローンカード１００に転送される時、ステータス表示灯１００は点灯した状態になることができる。そのような実施形態では、ステータ

ス表示灯１１０は、可読の識別子が使用不可になるまで点灯状態であることが好ましい。可読の識別子は、（１）トランザクションが完了した時、または（２）一定の時間が経過した時、に使用不可になることができることが好ましい。多くの実施形態では、コントローラ１４０は、可読の識別子を使用不可にするには単に可読の識別子への電力を切断すればよい。

【００４０】

ドローンカード１００は、ドローンカードを用いたトランザクションが試みられたことを検出するトランザクションセンサ１７０を含むことができる。例えば、ドローンカードが磁気リーダでスキャンするように構成された場合、トランザクションセンサ１７０は、磁気リーダによるドローンカードのスキャンを検出する。ドローンカードがスキャンされると、可読の識別子は使用不可になることが好ましい。

【００４１】

別の実施形態では、ドローンカード１００は内部電源を含まなくともよい。例えば、ドローンカード１００は、可読の状態を保つのに連続的な電力を必要としない磁気ストリップなどの可読の識別子を有するように構成することができる。そのような実施形態では、ホスト１０は、磁気ストリップにカードアカウントデータを書き込む磁気ヘッドなどの出力回路を含む。ドローンカード１００がホスト１０から引き出される時に、磁気ヘッドは磁気ストリップにカードアカウントデータを書き込むことができる。セキュリティコードもドローンカードに書き込むことができる。ホスト１０中のローラ（ｒｏｌｌｅｒ）または生成器を提供してドローンカード１００へのデータの書き込みを同期することができる。

【００４２】

次いで図５を参照すると、登録装置２００は、ユーザデータおよびカードデータ（および事例によってはセキュリティコード）でホスト１０を初期化する。登録装置２００は、独立型デバイス、または汎用コンピュータ３００の周辺装置でよい。後者の場合、登録装置２００は、インタフェース２３０を介してコンピュータ３００と通信する。当業者には理解されるように、インタフェース２３０は、シリアルライン、ワイヤレス通信、あるいはその他適切なデータ転送技術など多数の技術を使用して実施することができる。

【００４３】

汎用コンピュータ３００は、ユーザを認証するのに必要な情報の収集などユーザデータを集めるソフトウェアを含む。名前、住所、社会保障番号などユーザについての一般的情報を汎用コンピュータ３００中に入力（ｋｅｙ）することができる。登録装置２００は、ユーザの認証に必要な情報を収集する認証センサ２１０を含む。例えばホスト１０が指紋センサを含む場合、登録装置２００は、ユーザから指紋の画像を収集する。登録装置２００は、この機能を行う別個の指紋センサを有するか、あるいはホスト１０上に存在する指紋センサを使用することができる。登録装置２００は、ホストに記憶される各「カード」のカードデータを収集するセンサ２４０も含むことができる。センサ２４０は、標準的なトランザクションカードリーダでよい。

【００４４】

インタフェース２２０は、ホスト１０にユーザデータ（および可能性としてはセキュリティコード）を転送する。先に述べたように、当技術分野にはデータ転送のデバイスおよび技術が多数ある。例えば、登録装置２００は、ホスト上の電気接点を使用して通信することができる。

【００４５】

図１０～１２に、登録装置５００の別の実施形態を示す。この実施形態では、登録装置５００は、ホスト１０のスロット１４に収納されることが可能なカード様部分５０２を有することができる。登録装置５００全体はカード様部分５０２と同じ厚みとすることができることを理解されたいが、ホスト１０に収納されない部分は、耐久性のためなどにより厚くすることができる。登録装置５００は、ロック解除コードをホスト１０に入力するためのキーパッドなどのユーザ入力装置５０６を含む。登録装置５００は、ホスト１０と通

信するインタフェース（図示せず）も含む。登録装置５００は、電気的接触、レーザ通信、赤外線通信、あるいはその他の通信手段を使用するなど、ドローンカード１００と同様の方式でホスト１０とインタフェースを取ることができる。

【００４６】

この実施形態では、使用不可状態にしたホスト１０とドローンカード１００を登録装置５００とともにユーザに配送することができる。ホスト１０を使用可能にするには、ユーザは、ホスト１０およびドローンカード１００の発行者からロック解除コードを入手しなければならない。したがって、ユーザは、ホスト１０およびドローンカード１００の発行者と通信してロック解除コードを受け取る。ユーザは、発行者のウェブサイトを使用してロック解除コードを入手しても、あるいは単に電話を用いて発行者に電話してもよい。ロック解除コードを入手するには、ユーザは、ユーザを認証するための一連のセキュリティ上の質問に答えることを求められる。セキュリティ上の質問への返答に満足すると、発行者は、ロック解除コードをユーザに発行することができる。ユーザは、登録装置５００がホスト１０内に収納された状態で登録装置５００にロック解除コードを入力し、それによりホスト１０をロック解除する。ホスト１０は特定の登録装置５００と組み合わせることができることは理解されたい。さらに、登録装置５００は、１つの登録装置が複数のホストで使用されるのを防ぐために、一回限りの使用とするように設計することができる。

【００４７】

ホスト１０が使用可能になった状態で、ユーザは登録プロセスを進めることができる。例えば、ユーザは、ホスト１０の認証センサ２０を使用してアカウントを設定し、登録装置５００のユーザ入力装置５０６にカードアカウントについての情報をタイプ入力することができる。登録プロセスについての指示をホスト１０のディスプレイ３０に表示することができる。また、登録装置５００は、ユーザのデジタル写真をホスト１０に転送するデジタルカメラ手段５０８を含むことができる。

【００４８】

ホストを使用するには、ユーザは認証センサを使用して検証されなければならない。例えば認証センサが指紋センサである場合は、ホストに記憶されたカードアカウントにアクセスするにはユーザの指紋を検証しなければならない。認証されると、ユーザは、スクロールボタンを使用して、そのユーザがアクセス権を有するホストに記憶されたすべてのカードアカウントの識別を表示することができる。所望のカードアカウントの識別が表示されると、ユーザは、表示ボタンを使用して、選択した「カード」のカードデータをセキュリティコードと併せて表示することができる。カードデータとセキュリティコードをドローンカードにアップロードするには、ユーザは入力ボタンを選択する。

【００４９】

ホストがカードデータとセキュリティコードをドローンカードに転送すると、ステータス表示灯が点灯する（ドローンカードに電力が供給されており、そのように点灯する装備になっている場合）。トランザクションのためにカードを使用するには、ユーザはホストからカードを取り出し、可読の識別子がリーダに曝されるようにする。可読の識別子がリーダに対して曝されると、可読の識別子は使用不可になることが好ましく、ステータス表示灯が消える。可読の識別子がリーダに曝される前に一定の時間が経過した場合も可読の識別子は使用不可になることが好ましく、ステータス表示灯が消える。ユーザは次いで、別のトランザクションに必要になるまでドローンカードをホストに戻しておく。ディスプレイによりアカウント番号とセキュリティコードを見ることができ、（めったにないことであるが）ベンダが適切なカードリーダを持たない場合など、必要な際には電話（ｃａｌｌ－ｉｎ）によって処理を達成することができることは理解されよう。

【００５０】

図９Ａおよび９Ｂに、先に述べたホストとドローンカードの機能を１つの符号化カード４００に統合した代替の実施形態を示す。符号化カード４００は、標準的なクレジットカードとほぼ同じ厚みであることが好ましい。

【００５１】

符号化カード４００は、ユーザの識別を検証する、カードと一体化して取り付けられた認証センサ４１０を含むことが好ましい。生体認証センサなどユーザを識別することが可能な任意の適切なセンサを使用することができる。

【００５２】

任意で、権限のあるユーザの写真４０２が符号化カード４００に提供される。写真４０２は、権限のあるユーザの恒久的な静止写真であっても、権限のあるユーザの電子写真を一時的に表示する電子ディスプレイであってもよい。電子写真を使用する場合は、認証されたユーザに一致する写真が表示される。したがって、符号化カード４００には複数のユーザの写真を記憶することができ、許可された特定のユーザに基づいて該当する写真が表示される。

【００５３】

符号化カード４００は、ユーザが、符号化カード４００に記憶された各種のカードアカウントに関連する情報を見ることができるディスプレイ４２０を含む。符号化カード４００に装着されたスクロールボタン４３０により、ユーザは、自身がアクセス権を有する符号化カード４００に記憶された各種のカードアカウントの名前をスクロールして見ることができる。ユーザがカードアカウントの名前をスクロールすると、各アカウント名がディスプレイ４２０に表示される。

【００５４】

ユーザが使用する特定のカードアカウントを決定すると、入力ボタン４４０を使用して所望のカードアカウントを選択する。その結果、可読の識別子４８０（図９Ｂ）が一時的な磁気ストライプか、認証後に一時的にアクティブ化されるバーコード表示などの信号を提供し、それによりトランザクションが完了することができる。所望のカードアカウントを選択すると、表示灯４５０が可読の識別子の状態を表示する。先に述べたように、表示灯は、可読の識別子が使用可能な状態であるか、使用不可の状態であるかを示す。符号化カードを用いたトランザクションが試みられたことを検出するトランザクションセンサ４９０を提供することができる。特定のカードアカウントに関する情報も、表示ボタン４７０を選択することによりディスプレイ４２０で見ることができる。バッテリ寿命を延ばすために、太陽電池４６０を含めて符号化カード４００に電力を供給することができる。図９Ｃに示すように、プリズム４６２または他の適切な手段を提供して、太陽電池４６０に利用できる光を増すことができる。

【００５５】

このように、本発明は、新規の特性を有するトランザクションカードシステムを提供することが理解できよう。本発明の好適実施形態を図に示し、説明したが、当業者により、本発明の趣旨および範囲から逸脱することなく、変更および変形を加えてよい。また、各種実施形態の態様は、そのすべてまたは一部を入れ替えてもよいことを理解されたい。さらに、当業者は、前述の説明は例証に過ぎず、本発明を制限するものではないことを理解されよう。

【図面の簡単な説明】

【００５６】

【図１Ａ】本発明の一実施形態によるホストおよび挿入されたドローンカードの正面透視図であり、各種の内部構成要素を示すためにホストの一部分を切り開いた図である。

【図１Ｂ】ホストからドローンカードを取り出した状態を示す図１Ａのホストとドローンカードの透視図である。

【図１Ｃ】図１Ａの線１Ｃ－１Ｃに沿って見たホストの側面図である。

【図１Ｄ】図１Ａの線１Ｄ－１Ｄに沿って見たホストの一部分の断面図である。

【図２】図１Ａ～Ｃのホストの各種の機能構成要素を図式的に表す図である。

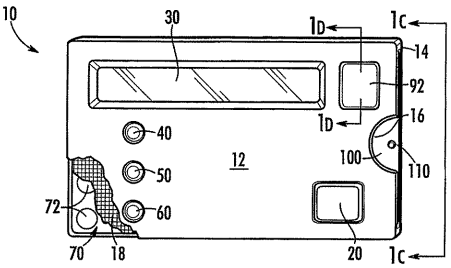
【図３Ａ】図１Ａ～Ｃのホストとともに使用することが可能なドローンカードの正面図である。

【図３Ｂ】図３Ａのドローンカードの背面図である。

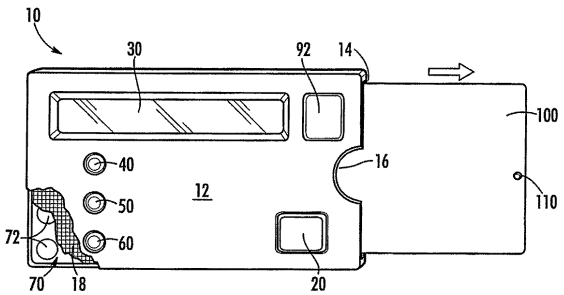
【図４】図３Ａおよび３Ｂのドローンカードの各種の機能構成要素を図式的に表す図であ

る。
【図５】本発明の一実施形態によるホストとのインタフェースをとる登録装置の図式表現図である。
【図６】認証プロセスを説明する流れ図である。
【図７】現在普及しているタイプのクレジットカードリーダでスキャンされるドローンカードの透視図である。
【図８】ドローンカードのトランザクションの試みを示す表の図である。
【図９Ａ】代替実施形態による符号化カードの正面図である。
【図９Ｂ】図９Ａの符号化カードの背面図である。
【図９Ｃ】図９Ａの線９Ｃ－９Ｃに沿って見たカードの一部分の断面図である。
【図１０】代替実施形態による登録装置の透視図である。
【図１１】ホスト中に収納された図１０の登録装置の透視図である。
【図１２】図１０および１１の実施形態による登録プロセスを説明する流れ図である。

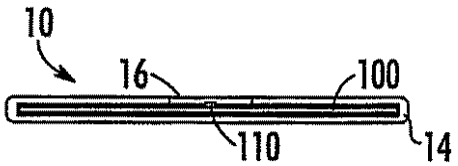
【図１Ａ】



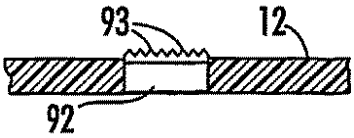
【図１Ｂ】



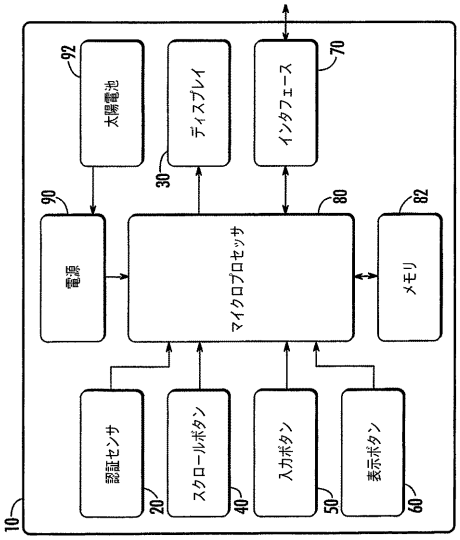
【図１Ｃ】



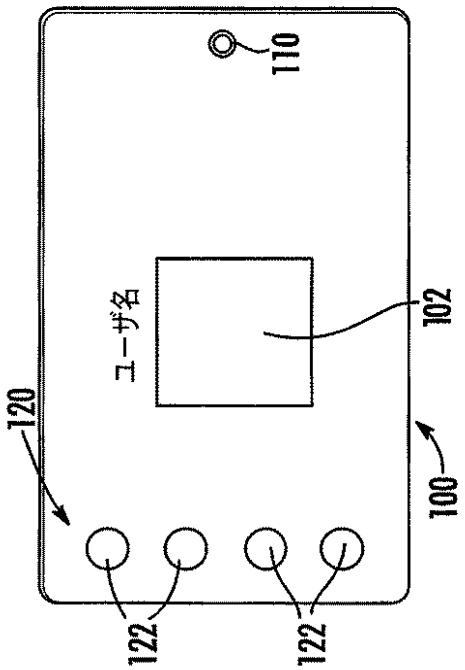
【図１Ｄ】



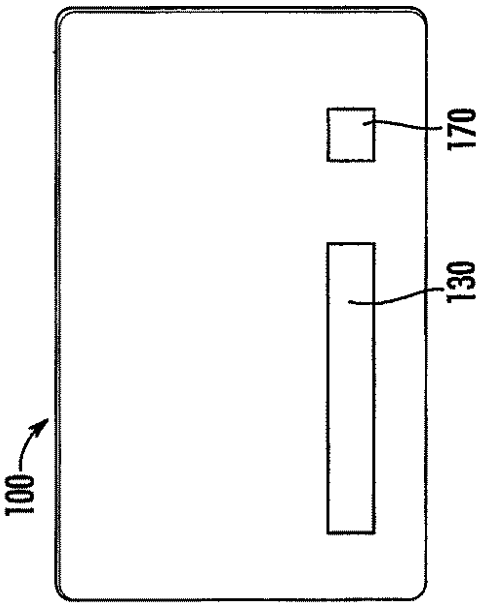
【図２】



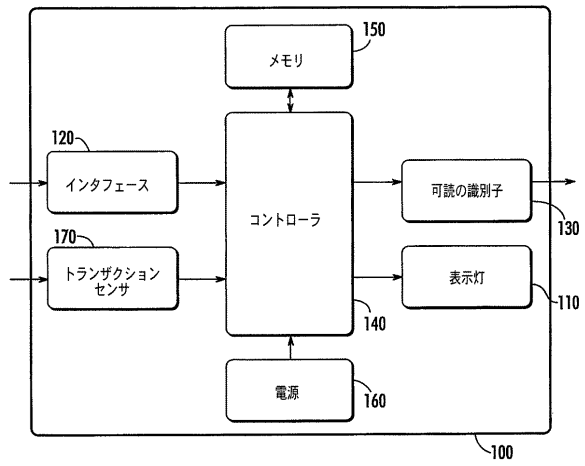
【図３Ａ】



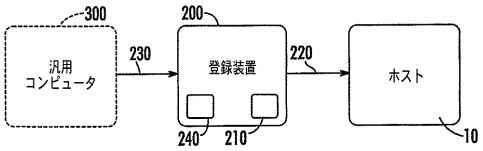
【図３Ｂ】



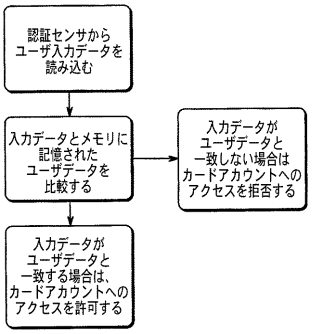
【図４】



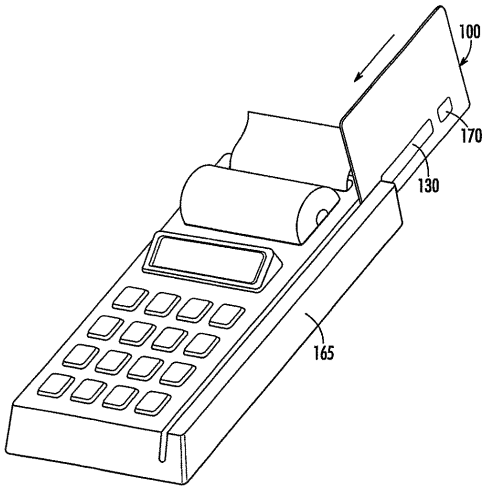
【図５】



【図６】



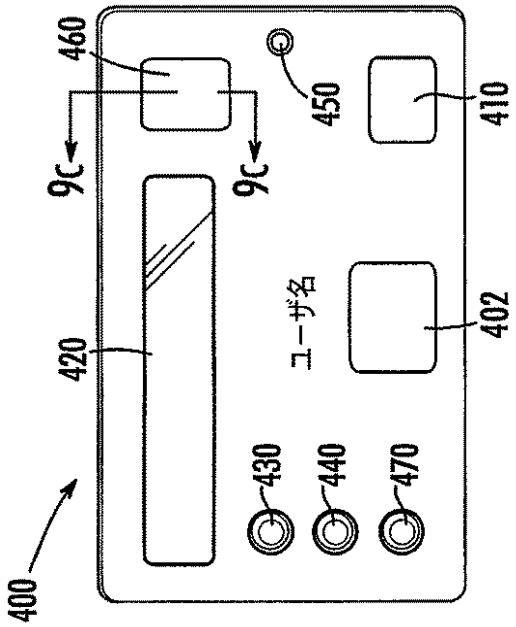
【図７】



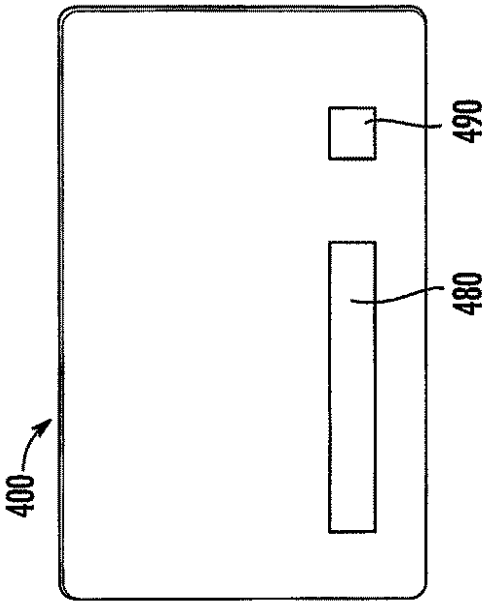
【図８】

予想されるセキュリティコード	読み取られたセキュリティコード	一致／不一致
1234	1234	一致
4582	4582	一致
3657	3657	一致
9878	9878	一致
2464	4462	不一致
2255	2256	不一致
5746	7657	不一致
・	・	・
・	・	・
・	・	・
・	・	・

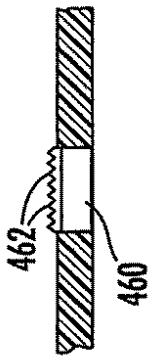
【図９Ａ】



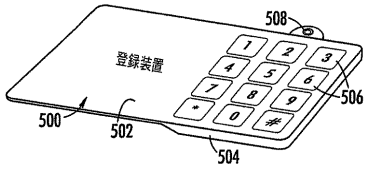
【図９Ｂ】



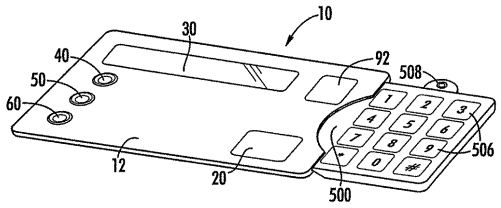
【図９Ｃ】



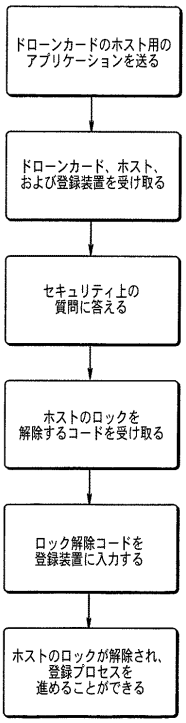
【図１０】



【図１１】



【図１２】



フロントページの続き

(51)Int.Cl.			FI		
H04L	*9/32*	*(2006.01)*	G06K	19/00	J
			G06K	19/00	R
			H04L	9/00	673E

(56)参考文献 特開平10－255120（JP，A）
特開2001－005921（JP，A）

(58)調査した分野(Int.Cl.，DB名)
G06K 17/00
G06F 3/08
G06F 21/20
G06K 19/07
G06K 19/10
H04L 9/32