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

特許第4607975号
(P4607975)

(45)発行日　平成23年1月5日(2011.1.5)　(24)登録日　平成22年10月15日(2010.10.15)

(51)Int.Cl.　F I
G06F 21/20 (2006.01)　G06F 15/00 330G
G06F 3/041 (2006.01)　G06F 3/041 380M

請求項の数 18　(全 38 頁)

(21)出願番号　特願2008-58071(P2008-58071)
(22)出願日　平成20年3月7日(2008.3.7)
(62)分割の表示　特願2003-202408(P2003-202408)の分割
原出願日　平成10年4月7日(1998.4.7)
(65)公開番号　特開2008-226243(P2008-226243A)
(43)公開日　平成20年9月25日(2008.9.25)
審査請求日　平成20年4月2日(2008.4.2)
(31)優先権主張番号　特願平9-264839
(32)優先日　平成9年9月10日(1997.9.10)
(33)優先権主張国　日本国(JP)

(73)特許権者　508135264
ドーサ　アドバンスズ　エルエルシー
アメリカ合衆国　ネバダ州　ラスベガス　８９１１９　ルネッサンス　ドライブ２２　１５－Ｂ　スイート５
(74)代理人　100147485
弁理士　杉村　憲司
(74)代理人　100070150
弁理士　伊東　忠彦
(72)発明者　久保　毅
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
(72)発明者　五十嵐　一浩
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

最終頁に続く

(54)【発明の名称】認証装置、ユーザ認証方法、ユーザ認証用カード及び記憶媒体

(57)【特許請求の範囲】

【請求項１】

認証装置であって、

複数の不連続な異なる座標を指定する部材を介して入力された複数の座標を検出するタッチパネルを有し、前記部材は該タッチパネル上に置かれると共に前記複数の不連続な異なる座標を指定する複数の打ち抜き可能な部分又は突起を有し、

前記タッチパネルは、前記部材を介して１個或いは複数の任意個の入力によって指示された位置にキーボードを仮想的に設定し、前記タッチパネルは、当該仮想的に設定したキーボードをもとに前記１個或いは複数の任意の入力が行われた位置の各キーに対応するコードを検出し、

前記認証装置は、

前記検出したコードのそれぞれと登録したコードとを比較する比較手段と、

該比較手段が比較した結果をもとに認証を行う認証手段と、を備えた認証装置。

【請求項２】

前記部材は、複数の不連続な突起により前記複数の不連続な座標を指定する、請求項１記載の認証装置。

【請求項３】

前記複数の不連続な突起は、前記部材の任意の位置に設けられている、請求項２記載の認証装置。

【請求項４】

前記検出した複数の座標の入力間隔が所定の間隔よりも長くなったとき、或いは、前記検出した複数の座標の入力間隔が入力間隔の平均値より長くなったときに前記複数の座標の入力が終了したと判定する判定手段を更に備えた、請求項１乃至３のいずれか１項記載の認証装置。

【請求項５】

前記タッチパネルは、前記部材が置かれるべき領域を指定する、請求項１乃至４のいずれか１項記載の認証装置。

【請求項６】

前記登録した複数の座標、登録した座標のパターン、或いは、登録したコード値について、ユーザレベルと、ユーザレベルの全てに共通の管理者レベルとを登録する登録手段を更に備えた、請求項１乃至５のいずれか１項記載の認証装置。

【請求項７】

前記部材は抵抗膜内に前記不連続な異なる座標にある複数の抵抗値を有し、

前記タッチパネルは、前記入力された座標に対応する抵抗値を検出し、前記比較手段は、前記抵抗値と登録した抵抗値とを比較することで前記検出した各コードを比較する、請求項１記載の認証装置。

【請求項８】

前記複数の不連続な座標を指定するよう構成されたポインティングデバイスを更に備え、

前記タッチパネルは、前記ポインティングデバイスが前記タッチパネルに接触したことを検出することにより、前記ポインティングデバイスにより前記部材を介して入力された座標を検出する、請求項１乃至７のいずれか１項記載の認証装置。

【請求項９】

前記ポインティングデバイスは、ペン又はスタイラスである、請求項８記載の認証装置。

【請求項１０】

コンピュータによるユーザ認証方法であって、

互いに異なる不連続な座標に対応する複数の不連続な突起を有する部材が、前記複数の不連続な突起がタッチパネルと接するように該タッチパネル上に置かれた際に、該複数の不連続な突起により指定された複数の点の加重平均座標を検出し、

前記検出した複数の点の加重平均座標と予め登録されている加重平均座標とを比較して比較結果を出力し、

前記比較結果に基づいて認証を行うことを特徴とする、ユーザ認証方法。

【請求項１１】

前記部材は、複数の不連続な突起により前記複数の不連続な座標を指定する、請求項１０記載のユーザ認証方法。

【請求項１２】

前記複数の不連続な突起は、前記部材の任意の位置に設けられている、請求項１１記載のユーザ認証方法。

【請求項１３】

前記認証ステップは、前記検出した複数の座標の順序と登録した座標の順序とをそれぞれ比較し、これら比較したそれぞれの結果をもとに認証を行う、請求項１０乃至１２のいずれか１項記載のユーザ認証方法。

【請求項１４】

前記検出した複数の座標の入力間隔が所定の間隔よりも長くなったとき、或いは、前記検出した複数の座標の入力間隔が入力間隔の平均値より長くなったときに前記複数の座標の入力が終了したと判定する判定ステップを更に含む、請求項１０乃至１３のいずれか１項記載のユーザ認証方法。

【請求項１５】

前記登録した複数の座標、登録した座標のパターン、或いは、登録したコード値につい

て、ユーザレベルと、ユーザレベルの全てに共通の管理者レベルとを登録する登録ステップを更に含む、請求項１０乃至１４のいずれか１項記載のユーザ認証方法。
【請求項１６】
前記比較ステップは、前記１個或いは複数の点によって指示された位置及び登録パターンから前記加重平均座標を求める、請求項１０記載のユーザ認証方法。
【請求項１７】
前記検出ステップは、前記タッチパネル上に置かれて前記複数の点を指示する前記部材を介した１個或いは複数の任意個の入力により指定された位置にキーボードを仮想的に設定し、当該仮想的に設定したキーボードをもとに前記１個或いは複数の任意個の入力が行われた位置の各キーに対応するコードを検出し、
前記比較ステップは、前記検出したコードのそれぞれと登録したコードとを比較する、請求項１０記載のユーザ認証方法。
【請求項１８】
前記検出ステップは、抵抗膜座標検出器上から前記部材を介して入力された点に対応する抵抗を検出し、前記比較ステップは、前記検出した抵抗と登録した抵抗とを比較することで前記検出した加重平均座標と前記登録した加重平均座標とを比較する、請求項１０記載のユーザ認証方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は認証装置、ユーザ認証方法、ユーザ認証用カード及び記憶媒体に係り、特に認証装置、認証装置によるユーザ認証方法、ユーザ認証用カード及びユーザ認証のためのプログラムを記憶した記憶媒体に関する。
【技術背景】
【０００２】
従来、パーソナルコンピュータ（パソコン又はＰＣと言う）で用いるセキュリティはキーボードからパスワードやユーザＩＤを入力して認証を得ることが一般的である。この方法では、ユーザが定義したパスワードやユーザＩＤを第三者に秘密にし、パソコンなどの画面上から入力して認証を受けて起動したり各種アクセスを行うようにしていた。
【発明の開示】
【発明が解決しようとする課題】
【０００３】
しかし、上記文字列や数字列のパスワードやユーザＩＤが第三者に知られてしまうと簡単に破られてしまうため、セキュリティとしての信頼性に問題があった。
【０００４】
本発明は、これらの問題を解決するため、タブレットを持つ装置やペン入力型のパソコン（以下、ペンＰＣと言う）等の座標検出が可能な装置のタッチパネルまたはタブレット上で入力された座標パターン又はカードの穴又は孔、切り欠きやマークなどから入力された座標パターンと登録座標パターン等とを照合して認証を行い、ユーザ独自のキーを用いてセキュリティの信頼性を高めると共にキーを設定したカードを携帯し簡易にセキュリティの高い認証を行うことを目的としている。
【課題を解決するための手段】
【０００５】
図１を参照して課題を解決するための手段を説明する。
【０００６】
図１において、中央処理装置（ＣＰＵ）１は、プログラムに従い各種処理を行うものであって、ここでは、読み取った座標と登録した座標とを比較したり、比較した結果をもとに認証を行ったりなどするものである。
【０００７】
座標検出マイコン４は、プログラムに従い座標検出器６からの信号をもとに座標を検出

したりなどするものである。また、比較認証するのはＣＰＵ１のみではなく、座標検出マイコン４のローカル処理で比較した結果をもとに認証を行ったりする。

【０００８】

座標検出器６は、画面上で入力された座標を検出するためのものである。ここで、画面とは、ＣＲＴや液晶などで像を表示する画面や、タブレットなどの座標を検出する面などを含めた画面、タッチパネルが表示装置上に設けられたものを言う。従って、図１に示す座標検出器６は、表示部と入力部とを含む。

【０００９】

次に、動作を説明する。

【００１０】

座標検出マイコン４が座標検出器６上から入力された座標を読み取り（又は、検出し）、ＣＰＵ１が読み取った（又は、検出した）複数の座標と登録した複数の座標とを比較し、比較した結果をもとに認証を行うようにしている。

【００１１】

この際、ＣＰＵ１は読み取った複数の座標の順序と登録した座標の順序とをそれぞれ比較し、これら比較したそれぞれの結果をもとに認証を行うようにしている。

【００１２】

また、座標検出マイコン４は読み取った複数の座標の入力間隔の平均値あるいは所定の間隔よりも長くなったときに上記複数の座標の入力が終了したと判定するようにしている。

【００１３】

また、複数の不連続な穴又は孔、切り欠き或るいはマークを設けたカードを座標検出器６上に置いて穴又は孔、切り欠き或いはマークをもとに入力された座標を座標検出マイコン４が読み取るようにしている。

【００１４】

即ち、座標が指定できれば良く、カードを貫通する孔でも良く、貫通しない窪み状の穴でも良い。後述するペンＰＣでは、抵抗膜方式、静電結合方式、電磁誘導方式等があるが、例えば、電磁誘導方式は、画面の下方に配置した座標検出器により、ペン（又はスタイラス）の磁気を感知して座標を検出するので、ペンが直接画面に触れなくても、磁気を感知する。従って、この場合は、カードに設けるものは、必ずしも貫通する孔で無くとも良く、窪みや穴でも良い。又、単にマークでも良い。

【００１５】

また、座標検出マイコン４が複数の不連続な穴又は孔、切り欠き或いはマークを設けたカードが座標検出器６上の指定領域に置かれて穴又は孔、切り欠き或いはマークをもとに入力された座標を読み取り、ＣＰＵ１が読み取った座標のパターンと登録した座標のパターンとを比較し、比較した結果をもとに認証を行うようにしている。

【００１６】

また、カードの複数の不連続な穴又は孔、切り欠き或いはマークを任意に設けるようにしている。

【００１７】

また、画面上の指定領域を乱数で決めた所定領域とするようにしている。

【００１８】

また、画面上の指定領域を４隅のいずれかを乱数で決めるようにしている。

【００１９】

また、座標検出マイコン４が複数の不連続な穴又は孔、切り欠き或いはマークを設けたカードを座標検出器６上の任意に移動された指定領域に置いて当該穴又は孔、切り欠き或いはマークをもとに入力された座標を読み取り、ＣＰＵ１が読み取った座標のパターンと登録した座標のパターンとを比較し、比較した結果をもとに認証を行うようにしている。

【００２０】

また、座標検出マイコン４が複数の不連続な穴又は孔、切り欠き或いはマークを設けた

カードを座標検出器６上に表示されたキーボードの枠に置いて穴又は孔、切り欠き或いはマークをもとに入力されたキーボードの非表示のキーに対応するコード値を読み取り（出力し）、ＣＰＵ１が読み取った（出力した）コードと登録したコードとを比較し、比較した結果をもとに認証を行うようにしている。　この際、ＣＰＵ１が登録した複数の座標、登録した座標のパターン、あるいは登録したコード値について、ユーザレベルと、ユーザレベルの全てに共通の管理者レベルとを登録するようにしても良い。

【００２１】

また、座標検出マイコン４が複数の不連続な穴又は孔、切り欠き或いはマークを設けたカードが座標検出器上に置かれて当該穴又は孔、切り欠き或いはマークをもとに入力された座標を読み取り、ＣＰＵ１が読み取った座標のパターンの任意番目の１個あるいは任意番目の任意個によって指示された位置をもとに、読み取った座標のパターンと上記指示された位置および登録パターンから決まるパターンと比較し、比較した結果をもとに認証を行うようにしている。

【００２２】

また、座標検出マイコン４が複数の不連続な穴又は孔、切り欠き或いはマークを設けたカードが座標検出器上に置かれて当該穴又は孔、切り欠き或いはマークをもとに入力された任意番目の１個あるいは任意番目の複数個によって指示された位置にキーボードを仮想的に設定し、当該仮想的に設定したキーボードをもとに上記入力された位置のキーに対応するコードを読み取り、ＣＰＵ１が読み取ったコードと登録したコードとを比較し、比較した結果をもとに認証を行うようにしている。

【００２３】

また、座標検出マイコン４が抵抗膜型の座標検出器６上から入力された１つあるいは複数の座標に対応する抵抗値を読み取り、ＣＰＵ１が読み取った抵抗値と登録した抵抗値とを比較し、比較した結果をもとに認証を行うようにしている。　従って、カードの複数の不連続な穴又は孔、切り欠きやマークなどから入力された座標パターンと登録座標パターンなどとを照合して認証を行うことにより、ユーザ独自のキーを用いてセキュリティの信頼性を高めると共にキーを設定したカードを携帯し簡易にセキュリテの高い認証を行うことが可能となる。

【００２４】

また、図２９に本発明をペンＰＣに適用した例を示す。ここでは、ペンＰＣ３１の画面３２上にカード（又はＩＤカード）３４等のカードを当ててその穴又は孔、切り欠き或いはマークを、ペン３３で押下することにより、画面３２上に配置した透明な座標検出器あるいは電磁誘導方式の場合には画面３２の下方の配置した非透明な座標検出器によってペンからの磁気を感知することによりその座標がそれぞれ検出され、既述したようにして登録したＩＤなどと比較して認証を行うことが可能となる。この際、画面上３２にはカード枠やカードを置く位置を示す位置マーカ等を表示して、例えばそのカード枠内にカード３４を配置してペン３３で穴又は孔、切り欠き或いはマーク部分を押下してもよいし、また、カード枠を表示しなく、当該カード３４の所定番目の１個或いは複数の穴又は孔、切り欠き或いはマーク部分の押下をもとにカード枠あるいはソフト１０キーの枠などを仮想的に設定してもよい。いずれにしても、表示した枠や位置マーカあるいは内部で仮想的に設定した枠や位置マーカをもとに押下された座標を検出し、登録した座標と比較して認証を行う。

【００２５】

カード（又はＩＤカード）３４は、例えば一般的に使用されているクレジットカードと略同じ形状及び寸法とすると、携帯に便利である。

【００２６】

また、図３０に本発明の応用例を示す。携帯可能な図示のようなペン入力型コンピュータ４１が既に開発されている。例えば薄いＢ５やＡ４サイズの液晶表示板からなる表示部４２が取り付けられている。この表示部４２の前面を覆うように図示外の透明なタッチパネルを装着し、当該タッチパネルを入力ペン４３で近接、接触又は軽く押下することによ

って、接触した位置の座標の検出が可能となる。ここで、表示部４２は、液晶表示としたが、本発明はそれだけでなく、プラズマ放電パネルやＣＲＴでもよい。このようなペン入力コンピュータ４１は既述した図１の構成を内部に持つことが可能である。また、本発明は、ペン入力コンピュータ４１のみではなく、ワードプロセッサ、電子手帳、座標検出装置を接続したデスクトップ装置、キャッシュディスペンサ等の座標検出装置を持つ各種プログラム可能な装置等にも適用可能である。

【００２７】

また、コンピュータ入力方式としては、抵抗膜方式、静電結合方式、電磁誘導方式等に大別できるが、本発明ではどの入力方式を取ってもよい。更に、ペン入力がなく、指でタッチするタッチパネル等に適用してもよい。

【発明の効果】

【００２８】

以上説明したように、本発明によれば、カードの穴や切り欠きなどから入力された座標パターンと登録座標パターンなどとを照合して認証を行う構成を採用しているため、ユーザ独自のキーを用いてセキュリティの信頼性を高めると共にキーを設定したカードを携帯し簡易にセキュリティの高い認証を行うことができる。

【発明を実施するための最良の形態】

【００２９】

次に、図１から図３０を用いて本発明の実施の形態および動作を順次詳細に説明する。

【実施例】

【００３０】

図１は、本発明のシステム構成図を示す。

【００３１】

図１において、ＣＰＵ１は、プログラムに従って各種処理を行うものである。ここで、ＣＤ－ＲＯＭ装置８によってＣＤ－ＲＯＭ８ａから読み取ったプログラム、フロッピィディスク（ＦＤ）装置９によってフロッピィディスク（ＦＤ）９ａから読み取ったプログラム、あるいは通信装置７を介してセンタからダウンロードしたプログラムを、ハードディスク装置１０のハードディスクにローディングしてＣＰＵ１がこれを読み出して図２ないし図２２によって説明する各種処理を行うようにしている。

【００３２】

各種回路２は、ＣＰＵ１が各種処理を行う上で必要な各種回路である。各種回路２は、例えば表示制御部やキーボード（図示せず）の制御部等の入出力（Ｉ／Ｏ）制御部を含む。

【００３３】

システムメモリ３やハードディスク装置１０のハードディスクは、プログラムやデータを格納するメモリである。

【００３４】

座標検出マイコン４は、フラッシュＲＯＭ５などに格納されたプログラムに従い各種処理を行うものである。

【００３５】

フラッシュＲＯＭ５は、プログラムなどを格納する不揮発メモリであって、ＥＥＰＲＯＭ、マスクＲＯＭなどの不揮発性にメモリのうちの１例を挙げたものである。また、座標検出マイコンの内部に持つＲＯＭに置き換えてもよい。尚、実際には、タブレットなどの座標入力装置は、座標検出時の補正データ、即ち、タブレット毎の特性を表す補正データを、フラッシュＲＯＭ、ＥＥＰＲＯＭ等の書き換え可能な不揮発性メモリに格納してこれを使用して座標検出の補正を行っているので、本願発明で説明する登録データを一緒に格納して以下使用することもできる。

【００３６】

座標検出器６は、入力された座標値を検出したり、抵抗式の場合には入力された座標に対応する抵抗値を検出したりなどするものである。この座標検出器６は、ＣＲＴ上に表示

された画面、液晶上に表示された画面、タブレットなどの入力された座標値を検出するものである。これらの、ＣＲＴ上に表示された画面、液晶ディスプレイ上に表示された画面、タッチパネル、タブレット、抵抗式のタブレットなどの全ての座標を検出するものを含めて本願発明では座標検出器と呼んでいる。例えば、液晶ディスレイ、プラズマ放電パネルの上に薄膜抵抗式のデジタイザを配したタッチパネルや、液晶ディスプレイやプラズマ放電パネルの下に電磁誘導方式のデジタイザを配したタッチパネル等でも良い。電磁誘導方式の場合は、画面（例えば液晶ディスプレイ）の下方に配置した座標検出器により、ペン（又はスタイラス）からの磁気を感知して座標を検出する。

【００３７】

本発明の認証装置は、少なくとも座標検出マイコン４、フラッシュＲＯＭ５（又はメモリ）及び座標検出器６からなり、ペンパソコンやタブレットを表示装置に備えたパーソナルコンピュータに適用可能である。好ましい実施例では、携帯型のペンパソコンや電子手帳のように表示画面上にペンや手で直接ポイントして入力可能なタブレットやタッチパネルを有する型のパソコンである。

【００３８】

通信装置７は、センタとの間でプログラムやデータの授受を行うものである。　ＣＤ－ＲＯＭ装置８は、ＣＤ－ＲＯＭ８ａからプログラムを読み出してシステムメモリ３に格納したりなどするものである。

【００３９】

ＦＤ装置９は、ＦＤ９ａからプログラムを読み出してシステムメモリ３に格納したりなどするものである。以下順次詳細に説明する。

【００４０】

尚、図１において、通信装置７、ＣＤ－ＲＯＭ装置８やＦＤ装置９等は、パソコン等の装置に対して接続される外部装置であっても良く、又、ＣＰＵ１及び座標検出マイコン４を単一のＣＰＵで構成しても良いことは、言うまでもない。同様に、システムメモリ３及びフラッシュＲＯＭ５は、単一のメモリで構成しても良い。

【００４１】

図２は、本発明の全体の動作説明フローチャートを示す。

【００４２】

図２において、ステップＳ１は、システムのブートアップを行う。

【００４３】

ステップＳ２は、入出力制御プログラム（ＢＩＯＳ）のローディングを行う。これは、図１のＣＰＵ１が動作できるようにするために、各種回路２中のフラッシュメモリ等の不揮発性メモリからＢＩＯＳを読み出してシステムメモリ３にローディングし、起動する。

【００４４】

ステップＳ３は、ユーザＩＤの入力を行う。これは、本発明に係る図３ないし図２２を用いて後述する座標検出器６上で座標値を入力してユーザＩＤの入力を行う。

【００４５】

ステップＳ４は、ＩＤ認証を行う。これは、ステップＳ３で入力されたユーザＩＤのＩＤが登録されているものと一致するかの認証を行う。

【００４６】

ステップＳ５は、ＯＫか判別する。これは、ステップＳ４で認証した結果、ＯＫか判別する。ステップＳ５の判別結果がＹＥＳの場合には、ステップＳ６に進む。ステップＳ５の判別結果がＮＯの場合には、ステップＳ１２で不一致と決定して処理は終了し、次のステップＳ６に進めないように禁止する。

【００４７】

ステップＳ６は、ステップＳ５でユーザＩＤのＩＤが認証されたので、オペレーティングシステム（ＯＳ）のローディングを行う。

【００４８】

ステップＳ７は、アプリ起動する。尚、アプリ起動時にもＯＳローディグ時と同様なＩ

Ｄ認証を行うことができる。
【００４９】
ステップＳ８は、ユーザＩＤの入力を行う。
【００５０】
ステップＳ９は、ＩＤの認証を行う。
【００５１】
ステップＳ１０は、ステップＳ９で認証した結果、ＯＫか判別する。ステップＳ１０の判別結果がＹＥＳの場合には、ステップＳ１１でアプリの実起動を行う。ステップＳ１０の判別結果がＮＯの場合には、ステップＳ１３で不一致と決定して処理は終了し、ステップＳ１１に進むことを禁止する。ここで、ステップＳ８～Ｓ１０，Ｓ１３は、既述したステップＳ３～ステップＳ５，Ｓ１２に対応するので詳細な説明は省略する。
【００５２】
以上によって、図１を構成するコンピュータシステムを起動する際に、ＢＩＯＳをローディングした後、ＯＳをローディングする前に本発明に係るユーザＩＤ入力、ＩＤ認証を行うと共に、アプリ起動時にも本発明に係るユーザＩＤ入力、ＩＤ認証を行うようにしている。この際のユーザＩＤ入力、ＩＤ認証について、従来の数字やアルファベットなどからなるテキストデータによるユーザＩＤに比し、本発明ではユーザがＩＤとして唯一持つものを用いて座標値を入力して当該座標値あるいは座標値パターンが正しいときにユーザＩＤの認証ＯＫと判定することによってセキュリティを高めるようにしている。以下ユーザＩＤ入力およびＩＤ認証について順次詳細に説明する。
【００５３】
図３は、本発明のカード位置変更フローチャートを示す。ここで、ＣＰＵ上のソフトウェアは図１のＣＰＵ１がシステムメモリ３からプログラムを読み込んで処理を行うときのソフトウェア（プログラム）であり、座標検出マイコンは図１のフラッシュＲＯＭ５から読み出したプログラムで動作する座標検出マイコン４である。これらＣＰＵ上のソフトウェアおよび座標検出マイコンは、それぞれ下段に記載した処理を行う。
【００５４】
図３において、ステップＳ２１は、場所Ｎｏとして乱数を発生する。これは、後述する図４の画面１１上の例えば４隅に場所Ｎｏ１、２、３、４を付与し、１ないし４内で乱数を発生させ、いずれかの場所を乱数によって選択する。
【００５５】
ステップＳ２２は、座標検出マイコン４に場所Ｎｏを通知し、座標検出マイコンにＩＤ認証処理の起動を通知する。これにより、ステップＳ２１で乱数で選択した場所Ｎｏを通知して座標検出マイコン４のＩＤ認証処理が起動されることとなる。
【００５６】
ステップＳ２３は、場所Ｎｏに対応したカード枠を表示する。これは、ステップＳ２１で乱数によって選択された場所、例えば図４の場所Ｎｏ１にカード枠を表示し、ユーザにそのカード枠に合わせてカードの穴又は孔、切り欠き或いはマーク等を介した座標の入力を促す。
【００５７】
ステップＳ３１は、ステップＳ２２によって座標検出マイコンのＩＤ処理が起動される。
【００５８】
ステップＳ３２は、指定された場所Ｎｏに対応する登録データを比較データとする。これは、ステップＳ２２で通知された場所Ｎｏに対応する登録データとして、後述する図５の（ｂ）の登録データから当該場所Ｎｏに対応する登録データを取り出して比較データとする。
【００５９】
ステップＳ３３は、座標チェックを行う。これは、ステップＳ２３でタッチパネル又はタブレットの画面１１上に図４に示すようにカード枠を表示し、ユーザがこのカード枠に

カードを当ててその穴又は孔、切り欠き或いはマークの部分をペンなどで押下して画面上の押下された座標値を検出し、当該検出した座標値と、ステップＳ３２で取り出した登録データとが一致するか比較してチェックする。

【００６０】

ステップＳ３４は、認証結果をＣＰＵ１上のソフトへ通知する。

【００６１】

ステップＳ２４は、認証が済か判別する。ステップＳ２４は、ステップＳ３４の認証結果が得られるまで繰り返される。ステップＳ３４から認証結果が得られると、認証が済であるので処理はステップＳ２５に進む。

【００６２】

ステップＳ２５は、認証結果に対応した処理を行う。例えば認証結果がＯＫの場合には図２のＯＳあるいはアプリをローディング／起動し、ＮＧの場合には図２のＯＳあるいはアプリのローディング／起動を行わなく、エラーなどとする。　以上によって、乱数によって場所を選択、例えば図４の場所Ｎｏ１を選択し、当該場所Ｎｏ１にカード枠を表示して当該カード枠にユーザがカードを置いて当該カードの穴又は孔、切り欠き或いはマークをペンなどで押下し、その座標値を読み取って当該場所Ｎｏに対応する登録データとを照合して一致するときに認証ＯＫ、不一致のときに認証ＮＧと判定することが可能となる。

【００６３】

また、本発明は、上述した座標入力をペンで行うだけで容易に座標を入力することができ、その座標を用いて認証を行うので、ペン入力機器、タッチパネルなどの後述する図２９や図３０のような携帯型ペン入力機器の操作性に合致した認証の手法を提供できる。特に、ペン入力機器、タッチパネルなどの後述する図２９や図３０のような携帯型ペン入力機器は、キーボードを持たない場合もあり、また、持っていてもユーザが日頃キーボードを使用しないケースも多い。そのような機器の使用状況下において、ペン入力機器又はペンコンピュータの使用形態に合致した認証を行うことができ、操作性を損なうことのない、認証が可能となる。

【００６４】

図４は、本発明のユーザＩＤ入力画面イメージ例を示す。このユーザＩＤ入力画面イメージ例は、図示のように、「カードを当て、ペンで入力して下さい」というメッセージに対応して図示のカード枠１２が乱数によって選択して表示されるので、ユーザはカード枠１２にカードを当て、ペンで当該カードの穴又は孔、切り欠き或いはマークの部分を押下する。装置は画面１１上で押下された座標値を読み取って、登録データと比較し、一致しているときに認証ＯＫ、不一致のときに認証ＮＧと判定することが可能となる。

【００６５】

図５は、本発明のカードを当てる位置を変更可能にする場合の説明図である。　図５の（ａ）は、タッチパネルの画面イメージ例を示す。このタッチパネルはＣＲＴ、液晶のディスプレイ、プラズマ放電パネル等のディスプレイ上に透明なデジタイザやタブレット（抵抗膜）を配したものや、ディスプレイの下に電磁誘導方式のデジタイザを配したものなどがある。電磁誘導方式の場合は、画面（例えば液晶ディスプレイ）の下方に配置した座標検出器により、ペン（又はスタイラス）からの磁気を感知して座標を検出する。この画面１１上の４隅に、カード枠１２の場所Ｎｏ１、場所Ｎｏ２、場所Ｎｏ３、場所Ｎｏ４を図示のように決め、それぞれに図示のように２点（点Ｎｏ１、点Ｎｏ２）がそれぞれ基準座標値として指定して登録すると、図５の（ｂ）のようになる。

【００６６】

図５の（ｂ）は、登録データ例を示す。この登録データ例は、図５の（ａ）の画面１１上の４隅に場所Ｎｏ１、場所Ｎｏ２、場所Ｎｏ３、場所ｏ４を図示のように決め、各場所で点１、点２の座標を指定して図示のように登録したものである。例えば場所Ｎｏ１の点Ｎｏ１は座標（ｘ11，ｙ11）、Ｎｏ２は座標（ｘ12，ｙ12）とそれぞれ決めて登録したものである。尚、各場所内の登録する点の数は任意に決めればよい。

【００６７】

以上のように画面１１上のカード枠１２を乱数で決定、表示する位置をここでは４隅の場所Ｎｏ１、場所Ｎｏ２、場所Ｎｏ３、場所Ｎｏ４と決め、更に各場所で点Ｎｏ１、点Ｎｏ２の座標をそれぞれ指定して登録する。これにより、カードを図示の４つのいずれかに乱数で決定、表示されたカード枠に当ててペンで点Ｎｏ１、点Ｎｏ２の位置に開けられた穴又は孔、切り欠き或いはマークを押下して座標を入力し、登録データと比較して一致しているときに認証ＯＫと判定することにより、同じ場所にカードを当てたときに画面１１に傷が付くなどしてカード枠が判ってしまったり、第三者に場所を覚えられてしまったりする事態を無くすことができる。　図６は、本発明の登録データの構造説明図を示す。

【００６８】

図６の（ａ）は、画面左下原点の例を示す。これは、既述した図５の４隅の４つの場所にカード枠１２を表示する場合において、左下の場所の図示の位置を原点（０，０）とした例を示す。ここでは、図示の点１ないし点４の座標を指定して登録する。

【００６９】

図６の（ｂ）は、登録データ例を示す。これは、図６の（ａ）に示すようにカード枠１２を表示し、点１（ｘ１　，ｙ１　）、点２（ｘ２　，ｙ２　）、点３（ｘ３　，ｙ３　）、点４（ｘ４　，ｙ４　）を登録した例を示す。

【００７０】

以上のようにカード枠１２に４つの点１、点２、点３、点４の座標を登録データとして登録しておき、タッチパネルの画面１１上に表示されたカード枠の穴又は孔、切り欠き或いはマークをペンで４個所押下し、その押下した点の座標が、登録データの点１、点２、点３、点４の座標値と一致したときに認証ＯＫとし、不一致のときに認証ＮＧと判定することが可能となる。

【００７１】

図７は、本発明の入力順を問わない場合の動作説明フローチャートを示す。

【００７２】

図７において、ステップＳ４１は、１回目の座標入力か判別する。ステップＳ４１の判別結果がＹＥＳの場合には、ステップＳ４２で座標値をセーブする。ステップＳ４１の判別結果がＮＯの場合には、ステップＳ４１を繰り返して待機する。１回目の入力にはタイムアウトを設けず、ユーザの入力開始をずっと待つようにする。

【００７３】

ステップＳ４３は、座標入力有か判別する。ステップＳ４３の判別結果がＹＥＳの場合には、ステップＳ４４で座標をセーブし、ステップＳ４３に戻り繰り返す。一方、ステップＳ４３の判別結果がＮＯの場合には、処理はステップＳ４５に進む。

【００７４】

ステップＳ４５は、入力待ちタイムアウト（一定時間経過）か判別する。ステップＳ４５の判別結果がＹＥＳの場合には一定時間経過して座標入力が終了したと判明したので、処理はステップＳ４７に進む。一方、ステップＳ４５の判別結果がＮＯの場合には、一定時間経過していなく座標入力の終了でないと判明したので、処理はステップＳ４３に戻り繰り返す。

【００７５】

ステップＳ４６は、ステップＳ４５の判別結果がＹＥＳで座標入力の終了と判明したので、登録データと比較する。これは、入力された座標値と、登録データとを比較する。

【００７６】

ステップＳ４７は、一致か判別する。ステップＳ４７の判別結果がＹＥＳの場合には、ステップＳ４８でＩＤ認証出力する。ステップＳ４７の判別結果がＮＯの場合には、ＩＤ不一致出力する。ＩＤ認証出力及びＩＤ不一致出力は、ＣＰＵ１に通知されるが、例えばＩＤ不一致出力の場合はＣＰＵ１がこれに応答してＩＤ不一致を表示するように制御を行っても良く、以下の説明でも同様の制御を行っても良い。

【００７７】

以上によって、カードを画面１１上のカード枠１２に当ててペンで１回目の座標が入力

された後、座標入力が順次行われ、一定時間経過しても座標入力が行われないときに座標入力が終了したと判定し、入力された座標値と登録データとを比較して一致のときにＩＤ認証出力し、不一致のときにＩＤ不一致出力することにより、カードを画面１１上のカード枠１２に当てて穴又は孔、切り欠き或いはマークをペンで押下して座標値を入力してセキュリティの高いＩＤ認証を行うことが可能となる。

【００７８】

図８は、本発明の入力順を問う場合の動作説明フローチャートを示す。

【００７９】

図８において、ステップＳ５１は、１回目の座標入力か判別する。ステップＳ５１の判別結果がＹＥＳの場合には、ステップＳ５２で座標値をセーブする。ステップＳ５１の判別結果がＮＯの場合には、ステップＳ４１を繰り返して待機する。

【００８０】

ステップＳ５３は、１回目の登録データと比較する。これは、ステップＳ５２でセーブした１回目の入力した座標値と、登録データの１回目の登録値とを比較する。

【００８１】

ステップＳ５４は、一致か判別する。ステップＳ５４の判別結果がＹＥＳの場合には、一致と判明したので、処理はステップＳ５６に進む。ステップＳ５４の判別結果がＮＯの場合には、不一致と判明したので不一致出力をして処理は終了する。

【００８２】

ステップＳ５５は、座標入力有か判別する。ステップＳ５５の判別結果がＹＥＳの場合には、ステップＳ５６で座標をセーブし、処理はステップＳ５７に進む。ステップＳ５５の判別結果がＮＯの場合には、処理はステップＳ６１に進む。　ステップＳ５７は、入力回数と登録回数とを比較する。

【００８３】

ステップＳ５８は、入力回数が登録回数をオーバーしたか判別する。ステップＳ５８の判別結果がＹＥＳの場合には、入力回数が登録回数をオーバーしたと判明したので、不一致出力をし処理は終了する。ステップＳ５８の判別結果がＮＯの場合には、処理はステップＳ５９に進む。

【００８４】

ステップＳ５９は、座標入力に基づいた入力データと登録データとを比較する。

【００８５】

ステップＳ６０は、ステップＳ５９で比較した入力データと登録データとが一致するか判別する。ステップＳ６０の判別結果がＹＥＳの場合には、一致と判明したので、処理はステップＳ５５に戻り次の座標の入力を待つ。ステップＳ６０の判別結果がＮＯの場合には、不一致と判明したので、不一致出力をして処理は終了する。

【００８６】

ステップＳ６１は、ステップＳ５５のＮＯで座標の入力がないと判明したので、入力待ちタイムアウト（一定時間経過）か判別する。ステップＳ６１の判別結果がＹＥＳの場合には一定時間経過して座標入力が終了したと判明したので、処理はステップＳ６２に進む。一方、ステップＳ６１の判別結果がＮＯの場合には、一定時間経過していなく座標入力の終了でないと判明したので、処理はステップＳ５５に戻り次の座標の入力を待機する。

【００８７】

ステップＳ６２は、入力個数と登録個数を比較する。

【００８８】

ステップＳ６３は、ステップＳ６２で比較された入力個数と登録個数とが一致するか判別する。ステップＳ６３の判別結果がＹＥＳの場合には、ＩＤ認証出力をする。ステップＳ６３の判別結果がＮＯの場合には、不一致出力をする。

【００８９】

以上によって、カードをタッチパネルの画面１１上のカード枠１２に当ててペンで規定された順番で座標が入力されるとその入力された座標と登録データとを順番に比較し、所

定時間経過しても座標入力がないときに座標入力の終了と判定し、これまでに入力された座標と登録データとを順次比較して一致しかつ個数が等しいときにＩＤ認証出力し、不一致のときに不一致出力することにより、カードを画面１１上のカード枠１２に当てて穴又は孔、切り欠き或いはマークをペンで所定の順番で押下して座標値を順次入力してセキュリティの高いかつＩＤ数の多いＩＤ認証を行うことが可能となる。

【００９０】

図９は、本発明のカード位置変更フローチャートを示す。

【００９１】

図９において、ステップＳ７１は、カード位置（ｘ０　，ｙ０　）を乱数で決定する。

【００９２】

ステップＳ７２は、座標検出マイコンにカード位置座標（ｘ０　，ｙ０　）を通知し、座標検出マイコンにＩＤ認証処理の起動を通知する。

【００９３】

ステップＳ７３は、カード位置に対応するカード枠を表示する。尚、カード枠の代わりに、カードを置くべき位置を示すことのできる任意の位置マーカを表示しても良い。

【００９４】

ステップＳ８１は、ステップＳ７２の通知に対応して座標検出マイコン４のＩＤ認証処理を起動する。

【００９５】

ステップＳ８２は、登録データとカード位置座標から比較座標を算出する。これは、登録データについて、ステップＳ７２で通知を受けたカード位置座標（ｘ０　，ｙ０　）をもとに比較座標値を算出する。

【００９６】

ステップＳ８３は、座標チェックを行う。これは、ステップＳ７３で画面上に後述する図１０の（ａ）に示すようにカード枠１２を表示し、ユーザがこのカード枠１２にカードを当ててその穴又は孔、切り欠き或いはマークの部分をペンなどで押下して画面１１上の押下された座標値を検出し、当該検出した座標値と、ステップＳ８２で算出した比較座標値とが一致するか比較してチェックする。

【００９７】

ステップＳ８４は、認証結果をＣＰＵ１上のソフトへ通知する。

【００９８】

ステップＳ７４は、認証済か判別する。ステップＳ７４は、ステップＳ８４の認証結果が得られるまで繰り返される。ステップＳ８４から認証結果が得られると、認証が済であるので処理はステップＳ７５に進む。

【００９９】

ステップＳ７５は、認証結果に対応した処理を行う。例えば認証結果がＯＫの場合には図２のＯＳあるいはアプリをローディング／起動し、ＮＧの場合には図２のＯＳあるいはアプリのローディング／起動を行わなく、エラーなどとする。　以上によって、乱数によってカード位置（ｘ０，ｙ０）を決定、例えば図１０のカード位置（ｘ０　，ｙ０　）と決定し、カード位置（ｘ０　，ｙ０　）にカード枠１２を表示して当該カード枠１２にユーザがカードを置いて当該カードの穴又は孔、切り欠き或いはマークをペンなどで押下し、その座標値を読み取って登録データとカード位置（ｘ０　，ｙ０　）から算出した比較座標値とを照合して一致するときに認証ＯＫ、不一致のときに認証ＮＧと判定することが可能となる。

【０１００】

図１０は、本発明のＣＰＵ上のソフトウェアがカードの位置を通知する場合のデータ構造説明図を示す。

【０１０１】

図１０の（ａ）は、タッチパネルの画面上のカード位置例を示す。このカード位置（ｘ０，ｙ０）は、乱数によって任意に決定したものである。このカード位置（ｘ０　，ｙ０

）を原点にカード枠１２を図示のように表示する。そして、カード枠１２にカードを当ててその穴又は孔、切り欠き或いはマークからペンで座標を入力する。

【０１０２】

図１０の（ｂ）は、カード内座標の例を示す。カードの左下を原点（０，０）とし、４つの点の座標をそれぞれ図示のように設定する。図１０の（ａ）のカード枠１２は、このカードの原点（０，０）を、画面１１上の乱数で決めた原点（ｘ０　，ｙ０　）に一致するように配置し、４つの点の座標は原点（ｘ０　，ｙ０　）の座標を加算して算出する（図９のステップＳ８２）。

【０１０３】

図１０の（ｃ）は、登録データの例を示す。ここで、点Ｎｏは、図１０の（ｂ）のカード内に指定した４つの点Ｎｏに対応する。カード原点（ｘ０　，ｙ０　）は、図１０の（ａ）の画面１１上でカード枠１２を表示する乱数で決めた原点である。カード内穴座標値は、図１０の（ｂ）の４つのカード内穴座標値である。比較座標値は、図１０の（ｂ）の４つのカード内座標値に、図１０の（ａ）の画面１１上で乱数によって決めた原点（ｘ０　，ｙ０　）を加算してそれぞれ算出したものである。

【０１０４】

以上のように、乱数で図１０の（ａ）のカード位置（ｘ０　，ｙ０　）を決めてカード枠１２を表示すると共に当該カード位置（ｘ０　，ｙ０　）をカード内座標に加算して画面１１上の穴の座標値を求めて比較座標値しておき、実際に検出された座標値と比較座標値とが一致したときに認証ＯＫとし、不一致のときに認証ＮＧとすることが可能となる。

【０１０５】

図１１は、本発明のソフトＫＢを利用するフローチャートを示す。

【０１０６】

図１１において、ステップＳ９１は、カードのサイズに対応した１０×ｎのソフト１０キーを画面上に設定する。これは、後述する図１２の（ｂ）の０、１、２、３・・・９の１０個からなるキーをｎ行配置したものを、図１２の（ａ）の画面１１上の乱数で決めた原点（ｘ０　，ｙ０　）の位置に設定する。

【０１０７】

ステップＳ９２は、ソフト１０キー位置座標と登録データから比較座標を算出する。これは、既述したように、原点（ｘ０　，ｙ０　）を、ソフト１０キー位置にそれぞれ加算して画面１１上の座標を比較座標として算出する。

【０１０８】

ステップＳ９３は、ソフト１０キー自身は画面に表示せず、カードの枠のみを表示する。

【０１０９】

ステップＳ１０１は、画面上で入力があったら入力座標をＣＰＵ上のソフトへ通知する。

【０１１０】

ステップＳ１０２は、入力有りか判別する。ステップＳ１０２の判別結果がＹＥＳの場合には、ステップＳ１０３で座標を検出し、ステップＳ１０４でＣＰＵ上のソフトに通知する。

【０１１１】

ステップＳ９４は、座標チェックと１０キー解析を行う。これは、ステップＳ１０４の入力座標の通知をもとに当該入力座標がいずれの１０キーの座標に対応するかをチェックして１０キーに変換する。

【０１１２】

ステップＳ９５は、パスワード型セキュリティを行う。これは、ステップＳ９４で１０キーに変換された数値（０、１、２・・・９）の列について、登録データと比較して一致するか判別するという、いわゆるパスワード型セキュリティを行う。

【０１１３】

ステップＳ９６は、認証結果に対応した処理を行う。

【０１１４】

以上によって、ソフト１０キーの枠を画面１１の乱数で決めた原点（ｘ０，ｙ０）をもとに設定して１０キーの枠のみを表示し、１０キー自身は非表示とし、当該枠の上に既述したカードを当てて穴又は孔、切り欠き或いはマークをペンで押下して座標入力し、読み取った座標値をもとに１０キーのいずれが押下されたかに変換した後、登録データと比較して一致したときに認証ＯＫ、不一致のときに認証ＮＧと判定することにより、画面上から任意の数字列などを順次入力して認証することが可能となる。

【０１１５】

図１２は、本発明の非表示のソフト１０キー上にカードを当ててキーコードを通知する場合のデータ構造の説明図を示す。

【０１１６】

図１２の（ａ）は、座標検出マイコンの座標検出例を示す。この画面１１は、乱数で決めた原点（ｘ０　，ｙ０　）を基準にソフト１０キーの枠のみを表示したイメージを示す。このソフト１０キーの枠内に図示のように、１行に１点、計４行に４点の座標値を図示のように決める。

【０１１７】

図１２の（ｂ）は、ＣＰＵ上のソフトによるソフト１０キーの座標値例を示す。ここでは、ソフト１０キーが０、１、２・・・９の１行当たり１０個とし、４行分を図示のように座標値をそれぞれ設定する。左下の隅が原点（０，０）である。

【０１１８】

図１２の（ｃ）は、座標検出マイコンがＣＰＵ上のソフトに通知する入力座標値の例を示す。ここでは、点１、２、３、４について、図１２の（ａ）のカードの枠内の点１、２、３、４の座標値をＣＰＵ上のソフトに通知するようにしている。

【０１１９】

図１２の（ｄ）は、ＣＰＵ上のソフトによる比較の説明図を示す。点Ｎｏおよび受け取った座標は、図１２の（ｃ）で座標検出マイコンから受け取った入力座標の値である。ソフト１０キーの原点座標は乱数で決めた原点（ｘ０　，ｙ０　）である。ソフト１０キー比較座標は受け取った座標から原点座標をｘ、ｙについてそれぞれ減算し、ソフト１０キー内の座標に変換したものである。比較結果は、ソフト１０キー比較座標が、図１２の（ｂ）のソフト１０キー内のいずれの座標値を一致するかを比較し、一致した座標値を取り出したものである。結果は、比較結果の座標値を０、１、２・・・９までの該当する数字に変換したものである。図では結果が“２６９２”であったのでこれのキーコードを送り出す。

【０１２０】

以上によって、画面１１上に乱数で決めた原点（ｘ０　，ｙ０　）を基準にソフト１０キーの枠のみを表示し、当該枠に当てたカードの穴又は孔、切り欠き或いはマークをペンで押下したときにその入力座標を取り込み、いずれのソフト１０キーが押下されたかに変換して結果を求め、この結果に対応するキーコードを送り出す。これにより送り出されたキーコードに対応する複数の数字と、登録データとが一致したときに認証ＯＫ、不一致のときに認証ＮＧと判定することが可能となる。

【０１２１】

図１３は、本発明の非表示のソフト１０キー上にカードを当ててキーコードを通知する場合のデータ構造の説明図（他の例）を示す。

【０１２２】

図１３の（ａ）は、既述した図１２の（ｄ）のデータと同一である。図１２ではＣＰＵ上のソフトがソフト１０キーの制御を行ったが、この図１３では座標検出マイコンがソフト１０キーの制御を行うようにした。そのため、ＣＰＵ上のソフトは画面１１上にカード枠１２を表示およびソフト１０キーの乱数で決めた原点（ｘ０　，ｙ０　）を座標検出マイコン４に通知する。通知を受けた座標検出マイコン４は、既述したようにして得られた結

果（例えば図示の“２６９２”）のキーコードを通常のキーボードインタフェースに変換し、図１３の（ｂ）のハードブロック図に示すＫＢマイコン１３の外付ＫＢ用インタフェースへ送信する。ＫＢマイコン１３は、以降キーコードをＯＳ経由でＣＰＵ１上のソフトの入力部へ通知する。

【０１２３】

図１３の（ｂ）は、ハードブロック図を示す。これは、上述したように、座標検出マイコン４で図１２で既述したＣＰＵ１上のソフトが行っていたソフト１０キーの制御を行うようにした場合のハードブロック図であって、ＫＢマイコン１３を設けて当該ＫＢマイコン１３経由でデータをＣＰＵ１上のソフトの入力部に送るようにしている。タブレット１５は、図１の座標検出器６の例である。

【０１２４】

図１４は、本発明のソフトＫＢを利用するフローチャートを示す。

【０１２５】

図１４において、ステップＳ１１１は、カード位置（ｘ０　，ｙ０　）を乱数で決定する。

【０１２６】

ステップＳ１１２は、座標マイコンに通知してＩＤ認証処理を起動する。

【０１２７】

ステップＳ１１３は、カード位置に対応するカード枠を表示する。

【０１２８】

ステップＳ１２１は、ＩＤ認証処理を起動する。

【０１２９】

ステップＳ１２２は、カード位置（ｘ０　，ｙ０　）に対応した１０×ｎのソフト１０キーを画面上に設定する。

【０１３０】

ステップＳ１２３は、座標検出と１０キー解析を行う。これは、既述したようにしてカード枠にカードを当てて当該カードの穴又は孔、切り欠き或いはマークをペンで押下したときに入力座標を検出して該当するソフト１０キー上の位置を求めて対応する数値（結果）に変換する。

【０１３１】

ステップＳ１２４は、キーコードを送出する。これは、ステップＳ１２３で求めた数値（結果）をキーコードに変換して送出する。

【０１３２】

ステップＳ１１４は、パスワード型セキュリティを行う。これは、既述したように、ステップＳ１２３で１０キーに変換された数値（０、１、２・・・９）の列について、登録データと比較して一致するか判別するという、いわゆるパスワード型セキュリティを行う。

【０１３３】

ステップＳ１１５は、認証結果に対応した処理を行う。

【０１３４】

以上によって、ソフト１０キーの枠を画面１１の乱数で決めた原点（ｘ０　，ｙ０　）をもとに設定して１０キーの枠のみを表示し、１０キー自身は非表示とし、当該枠の上に既述したカードを当てて穴又は孔、切り欠き或いはマークをペンで押下して座標入力し、読み取った座標値をもとに１０キーのいずれが押下されたかに変換した後、登録データと比較して一致したときに認証ＯＫ、不一致のときに認証ＮＧと判定することにより、画面上から任意の数字列などを入力して認証することが可能となる。

【０１３５】

尚、具体例では１０×ｎで説明したが、ソフト１０キーはｍ×ｎと配置することも可能である。又、ソフト１０キーの代わりに、アルファベット、かな、記号等の通常のキーボードにあるキーからなるソフトキーボードを用いても良いことは言うまでもない。

【０１３６】
図１５は、本発明のカードの構造例を示す。
【０１３７】
図１５の（ａ）は、ｍ×ｎのグリッド上の任意の位置に穴を開けたカードの例を示す。図では、穴を４個開けてコンピュータシステムと一緒に出荷する。この際、内部のテーブルに登録データとして図示の４個の穴の位置の座標値を登録データとして登録しておく。
【０１３８】
図１５の（ｂ）は、ｍ×ｎのグリッドの交点部分の任意の個所をユーザが簡単に打ち抜くことができるようにしたカードの例を示す。
【０１３９】
図１５の（ｂ－１）は、ｍ×ｎのグリッドの交点部分に簡単に打ち抜きできるようにしたカードの様子を示す。
【０１４０】
図１５の（ｂ－２）は、図１５の（ｂ－１）のグリッドの交点部分の拡大図を示す。拡大図に示すように、グリッドの交点部分は円形状の一部を残し他を打ち抜いておき、ユーザが所望のグリッドの交点部分をペン等で押下して打ち抜き、任意の個所に穴を開けることができるようにしたものである。
【０１４１】
図１５の（ｂ－３）は、１０列×ｎ行のグリッドの図示の部分を打ち抜き、“１６９０”を設定した例を示す。ユーザは任意に作成した唯一のカードを装置にＩＤ登録させることができる。
【０１４２】
以上のように、カードをｎ×ｍのグリッドにして任意の座標位置に穴を開けることにより、当該カードを既述したように画面１１上に表示されたカード枠１２に当てて穴をペンで押下して所定の座標値を入力することが可能となる。
【０１４３】
次に、本発明において、今まで説明してきたカード以外のカードの形状について、図１６と共に説明する。抵抗膜方式において、カードに図１６のような複数の突起がある場合を説明する。画面１１上に透明な抵抗膜を置き、表示されたカード枠に図示のようにピンのでたカード３４を押下することにより、図では３つのピンで抵抗膜が押下され、図示の下段の式に示すように、３点の加重平均座標に相当する抵抗値が検出される。このため、カード３４の複数のピンの位置によって所望の加重平均座標が得られるように予め設定し、登録データと比較して一致したときに認証ＯＫ、不一致のときに認証ＮＧと判定することが可能となる。　図１７は、本発明の比較説明図（固定値）を示す。位置検出装置で検出した座標には、検出誤差が含まれ、かつユーザ個人のペンの当て方にもクセがあり、検出座標と登録座標の比較には必ず許容範囲を設ける必要がある。
【０１４４】
図１７において、ステップＳ１２１は、許容範囲Δｘ、Δｙを設定する。これは、既述した画面１１上に表示されたカード枠１２にカードを当ててペンで押下して座標入力して検出ときの許容範囲を固定値のΔｘ、Δｙと設定する。
【０１４５】
ステップＳ１２２は、Ｘとｘｎ±Δｘの比較を行う。これは、入力座標（Ｘ，Ｙ）のうちのＸと、ｎ個目の登録データ（ｘｎ，ｙｎ）のうちのｘｎに±Δｘを加算した値とを比較する。
【０１４６】
ステップＳ１２３は、ｘｎ－Δｘ≦Ｘ≦ｘｎ＋Δｘの範囲内か判別する。これは、入力座標のＸがステップＳ１２１で設定した許容誤差Δｘの範囲内にあるか判別する。ステップＳ１２３の判別結果がＹＥＳの場合には、許容範囲内にあると判明したので、処理はステップＳ１２４に進む。ステップＳ１２３の判別結果がＮＯの場合には、許容範囲外と判明したので、不一致出力をし、処理は終了する。

【０１４７】
ステップＳ１２４は、ステップＳ１２２と同様に、Ｙとｙｎ±Δｙの比較を行う。これは、入力座標（Ｘ，Ｙ）のうちのＹと、ｎ個目の登録データ（ｘｎ，ｙｎ）のうちのｙｎに±Δｙを加算した値とを比較する。
【０１４８】
ステップＳ１２５は、ｙｎ－Δｙ≦Ｙ≦ｙｎ＋Δｙの範囲内か判別する。これは、入力座標のＹがステップＳ１２１で設定した許容誤差Δｙの範囲内にあるか判別する。ステップＳ１２５の判別結果がＹＥＳの場合には、許容範囲内にあると判明したので、ステップＳ１２６で座標一致出力し、処理は終了する。ステップＳ１２５の判別結果がＮＯの場合には、許容範囲外と判明したので、不一致出力をし、処理は終了する。
【０１４９】
以上によって、許容範囲Δｘ、Δｙ（固定値）を設定し、画面１１上から検出した座標入力（Ｘ、Ｙ）が登録データの許容範囲Δｘ、Δｙにあるときに座標一致として判定し、座標入力時の誤差がある程度あっても許容範囲内のときは正しく判定されることとなる。
【０１５０】
図１８は、本発明のセキュリティレベル設定説明図を示す。
【０１５１】
図１８の（ａ）は、フローチャートを示す。
【０１５２】
図１８の（ａ）において、ステップＳ１３１は、セキュリティレベルをチェックする。
【０１５３】
ステップＳ１３２は、セキュリティレベルに合った許容範囲Δｘｍ、Δｙｍを設定する。例えばセキュリティレベルを高くするために許容範囲Δｘｍ、Δｙｍを小さく設定し、セキュリティレベルを低くするために許容範囲Δｘｍ、Δｙｍを大きく設定する。
【０１５４】
ステップＳ１３３は、比較を行う。これは、ステップＳ１３２でセキュリティレベルに応じて設定された許容範囲Δｘｍ、Δｙｍをもとに、既述した図１７のフローチャートに従い比較を行い、座標一致出力あるいは座標不一致出力を行う。
【０１５５】
以上によって、セキュリティレベルの高い／低いに応じて許容範囲Δｘ、Δｙを小さく／大きく設定することにより、入力座標値の比較判定を厳しく／緩やかに任意の設定することが可能となる。
【０１５６】
図１８（ｂ）において、セキュリティレベル１は判定を最も緩やかに、セキュリティレベルｌ（エル）は最も厳しくした場合を示している。
【０１５７】
図１９は、本発明の相対座標の範囲設定の説明図を示す。表示されたカード枠に対して、ユーザが当てたカード位置には必ず位置決め誤差が含まれる。これはカード原点座標（ｘ０ ，ｙ０ ）に対する許容範囲の設定により吸収できる。
【０１５８】
図１９の（ａ）は、データ例を示す。ここで、点Ｎｏはカード内に設定した点Ｎｏ１、２、３、４である。カード原点は画面１１上のカード枠を表示する原点（ｘ０ ，ｙ０ ）およびその許容範囲（Δｘ０ ，Δｙ０ ）である。カード内穴座標の登録データはカード内の穴座標の登録データである。比較座標範囲のｍｉｎ（最小値）は図示のようにカード原点（ｘ０ ，ｙ０ ）から許容範囲（Δｘ０ ，Δｙ０ ）を減算し当該減算した値に各点の座標を加算した値である。比較座標範囲のｍａｘ（最大値）は図示のようにカード原点（ｘ０，ｙ０）に許容範囲（Δｘ０，Δｙ０）を加算し当該加算した値に各点の座標を加算した値である。
【０１５９】
図１９の（ｂ）は、フローチャートを示す。

【０１６０】
図１９の（ｂ）において、ステップＳ１４１は、登録データとカード原点、許容範囲から比較座標ｍｉｎ／ｍａｘを算出する。これは、図１９の（ａ）で説明したように登録データ（カード内の穴の登録データ）とカード原点と許容範囲から比較座標ｍｉｎ／ｍａｘを算出する。
【０１６１】
ステップＳ１４２は、座標チェックを行う。画面１１上で表示されたカード枠にカードを当てて穴又は孔、切り欠き或いはマークをペンで押下して座標入力し、当該座標入力が比較座標のｍｉｎとｍａｘの範囲にあるか判別し、範囲内にあるときに認証ＯＫ、範囲外のときに認証ＮＧと決定する。
【０１６２】
ステップＳ１４３は、認証結果をＣＰＵ上のソフトに通知する。
【０１６３】
以上によって、カード内の登録データとカードの原点と許容範囲をもとに比較座標範囲（ｍｉｎ／ｍａｘ）を算出し、画面１１上で表示されたカード枠にカードを当てて穴又は孔、切り欠き或いはマークをペンで押下して座標入力したときの当該座標入力が比較座標のｍｉｎとｍａｘの範囲にあるか判別し、範囲内のときに認証ＯＫ、範囲外のときに認証ＮＧと判定することが可能となる。
【０１６４】
図２０は、本発明の許容範囲の学習説明図を示す。
【０１６５】
図２０において、ステップＳ１５１は、ｎ回入力を行う。これは、画面１１上で表示されたカード枠にカードを当てて穴又は孔、切り欠き或いはマークをペンで押下して座標入力することをｎ回繰り返す。
【０１６６】
ステップＳ１５２は、統計的解析を行う。
【０１６７】
ステップＳ１５３は、許容範囲（Δｘ，Δｙ）を算出する。これらステップＳ１５２及びＳ１５３は、ステップＳ１５１でｎ回座標入力した値をもとに統計的解析し、例えば平均値を求め、登録データからこの求めた平均値の周りの一定範囲を許容範囲として算出する。
【０１６８】
以上によって、画面１１上で表示されたカード枠１２にカードを当ててペンで穴又は孔、切り欠き或いはマークを押下して座標入力したときに、座標入力の平均値を求めて登録データから当該平均値の一定範囲を許容範囲と算出することにより、ユーザ毎のクセにより座標入力する点がずれてもユーザ個別に予め許容範囲を求めて狭く設定することが可能となり、セキュリティレベルを高めることができる。
【０１６９】
図２１は、本発明の検出終了の動作説明フローチャート（順序なしの場合）を示す。ユーザ本人は自分のＩＤ入力時よどみなく一連の動作で入力できる。そこで、終了検出を固定値のタイムアウトではなく、ユーザ自身の入力の平均より求めることで、入力途中で今までの入力速度に対して長い入力なし時間が現れた時点で終了検出させることにより、本人確認のセキュリティを上げることができる。
【０１７０】
図２１において、ステップＳ１６１は、入力待ちタイムアウトｔに初期値ｔ０　を設定する。
【０１７１】
ステップＳ１６２は、１回目の座標入力か判別する。ステップＳ１６２の判別結果がＹＥＳの場合には、ステップＳ１６３で座標をセーブ（保存）し、処理はステップＳ１６４に進む。ステップＳ１６２の判別結果がＮＯの場合には、処理はステップＳ１６２に戻り

待機する。

【０１７２】

ステップＳ１６４は、座標入力か判別する。ステップＳ１６４の判別結果がＹＥＳの場合には、ステップＳ１６５で座標をセーブし、ステップＳ１６６で前回入力からの時間間隔より平均入力間隔ｔAVE　を算出し、入力待ちタイムアウトｔを更新する。これにより、入力待ちタイムアウトｔが平均入力間隔ｔAVE　に更新されることとなる。そして、ステップＳ１６４に戻り繰り返す。一方、ステップＳ１６４の判別結果がＮＯの場合には、処理はステップＳ１６７に進む。

【０１７３】

ステップＳ１６７は、入力待ちタイムアウトｔ×ｎ倍をオーバーしたか判別する。ステップＳ１６７の判別結果がＹＥＳの場合には、現在の待ち時間が、入力待ちタイムアウトｔ×ｎ倍をオーバーしたと判明したので、座標入力が終了したと判定し、ステップＳ１６８で登録データと比較する。一方、ステップＳ１６７の判別結果がＮＯの場合には、ステップＳ１６４に戻り座標入力を待つ。

【０１７４】

ステップＳ１６９は、一致するか判別する。ステップＳ１６９の判別結果がＹＥＳの場合には、ＩＤ認証出力する。ステップＳ１６９の判別結果がＮＯの場合には、不一致出力をする。

【０１７５】

以上によって、座標入力の間隔の平均値を求め、求めた平均値のｎ倍の時間間隔の間以上、座標入力がなかったときに座標入力の終了と判定し、座標入力された座標値と登録データとを比較して一致したときに認証ＯＫ、不一致のときに認証ＮＧと判定することが可能となる。

【０１７６】

図２２は、本発明の検出終了の動作説明フローチャート（順序ありの場合）を示す。

【０１７７】

図２２において、ステップＳ１７１は、入力待ちタイムアウトｔに初期値ｔ０　を設定する。

【０１７８】

ステップＳ１７２は、１回目の座標入力か判別する。ステップＳ１７２の判別結果がＹＥＳの場合には、処理はステップＳ１７３に進む。ステップＳ１７２の判別結果がＮＯの場合には、処理はステップＳ１７２に戻り待機する。

【０１７９】

ステップＳ１７３は、座標をセーブ（保存）する。

【０１８０】

ステップＳ１７４は、１回目の座標入力による入力データと登録データとを比較する。これは、ステップＳ１７３でセーブした座標入力と、登録データとを比較する。

【０１８１】

ステップＳ１７５は、一致か判別する。ステップＳ１７５の判別結果がＹＥＳの場合には、処理はステップＳ１７６に進む。ステップＳ１７５の判別結果がＮＯの場合には、不一致出力をし、処理は終了する。

【０１８２】

ステップＳ１７６は、座標入力か判別する。ステップＳ１７６の判別結果がＹＥＳの場合には、処理はステップＳ１７７に進む。ステップＳ１７６の判別結果がＮＯの場合には、処理はステップＳ１８３に進む。

【０１８３】

ステップＳ１７７は、ステップＳ１７６で座標入力があったと判明したので、座標入力をセーブする。

【０１８４】

ステップＳ１７８は、入力個数と登録個数を比較する。

【０１８５】
ステップＳ１７９は、入力個数が登録個数をオーバーしたか判別する。ステップＳ１７９の判別結果がＹＥＳの場合には、不一致出力をし、処理は終了する。ステップＳ１７９の判別結果がＮＯの場合には、処理はステップＳ１８０に進む。
【０１８６】
ステップＳ１８０は、前回の入力からの時間間隔より平均入力間隔ｔAVE　を算出し、入力待ちタイムアウトｔを更新する。これにより、入力待ちタイムアウトｔが平均入力間隔ｔAVE　に更新されることとなる。
【０１８７】
ステップＳ１８１は、座標入力と登録データとを比較する。
【０１８８】
ステップＳ１８２は、ステップＳ１８１で比較した座標入力と登録データとが一致か判別する。ステップＳ１８２の判別結果がＹＥＳの場合には、処理はステップＳ１７６に戻り待機する。ステップＳ１８２の判別結果がＮＯの場合には、不一致出力をし、処理は終了する。
【０１８９】
ステップＳ１８３は、入力待ちタイムアウトｔ×ｎ倍をオーバーしたか判別する。ステップＳ１８３の判別結果がＹＥＳの場合には、現在の待ち時間が、入力待ちタイムアウトｔ×ｎ倍をオーバーしたと判明したので、座標入力が終了したと判定し、処理はステップＳ１８４に進む。ステップＳ１８３の判別結果がＮＯの場合には、処理はステップＳ１７６に戻り座標入力を待つ。
【０１９０】
ステップＳ１８４は、入力回数と登録回数を比較する。
【０１９１】
ステップＳ１８５は、一致か判別する。ステップＳ１８５の判別結果がＹＥＳの場合には、入力回数と登録回数が一致すると判明したので、ＩＤ認証出力をし、処理は終了する。ステップＳ１８５の判別結果がＮＯの場合には、不一致出力をし、処理は終了する。
【０１９２】
以上によって、座標入力の間隔の平均値を求め、求めた平均値のｎ倍の時間間隔の間以上、座標入力がなかったときに座標入力の終了と判定し、座標入力された座標値と登録回数について登録データと比較して一致したときに認証ＯＫ、不一致のときに認証ＮＧと判定することが可能となる。
【０１９３】
次に、図２３のフローチャートに示す順序に従い、図２４を参照して座標検出器上のカード３４の枠を表示しなく、カード３４を例えばタブレット等の座標検出器上に置いて穴又は孔、切り欠き或いはマークをペンで押下する場合の動作を順次詳細に説明する。
【０１９４】
図２３は、本発明のタブレットやタッチパネル上の任意位置にカード３４を当てるフローチャートを示す。
【０１９５】
図２３において、ステップＳ１９１は、ＣＰＵ１上のソフトウェアが座標検出マイン４のＩＤ認証処理を起動する。
【０１９６】
ステップＳ１９２は、座標検出マイコン４がＩＤ認証を開始する。
【０１９７】
ステップＳ１９３は、カード原点（ｘ00，ｙ00）とカード上の他の特定点（ｘ01，ｙ01）よりカード位置を検出する。これは、後述する例えば図２４の（ａ）のタブレット２１上に示すように、第１番目にペンを押下しカード３４の左下の座標（ｘ00，ｙ00）、および第２番目にペンで押下したカード３４の右下の座標（ｘ01，ｙ01）をそれぞれカード原点（ｘ00，ｙ00）および他の特定点（ｘ01，ｙ01）として検出する。

【０１９８】
ステップＳ１９４は、検出したカード位置に対応した１０×ｎのソフト１０キーを画面上に設定する。ここで、ソフト１０キーは、仮想的に画面上に設定され、カードの枠は非表示である。
【０１９９】
ステップＳ１９５は、座標検出と１０キー解析する。これは、カード３４の穴又は孔、切り欠き或いはマークをペンで押下したときに入力座標を検出して該当するソフト１０キー上の位置を求めて対応する数値（結果）に変換する。
【０２００】
ステップＳ１９６は、キーコードを送出する。これは、ステップＳ１９５で求めた数値（結果）をキーコードに変換して送出する。
【０２０１】
ステップＳ１９７は、パスワード型セキュリティを行う。これは、既述したように、ステップＳ１９５で１０キーに変換された数値（０、１、２・・・９）の列について、登録データと比較して一致するか判別するという、いわゆるパスワード型セキュリティを行う。
【０２０２】
ステップＳ１９８は、認証結果に対応した処理を行う。
【０２０３】
以上によって、タブレットやタッチパネルなどの座標入力装置上で原点（ｘ00，ｙ00）および他の特定点（ｘ01，ｙ01）を入力してソフト１０キーを仮想的に設定し、１０キーの枠および１０キー自身の両者を非表示とし、カード３４を当てて穴又は孔、切り欠き或いはマークをペンで押下して座標入力し、読み取った座標値をもとに１０キーのいずれが押下されたかに変換した後、登録データと比較して一致したときに認証ＯＫ、不一致のときに認証ＮＧと判定することにより、カード枠などを表示できないタブレット上から任意の数字列などを入力して認証することが可能となる。
【０２０４】
尚、図２３に示すフローチャートにおけるソフト１０キーによる認証方法は、前述の他の方法と置き換えても良いことは言うまでもない。
【０２０５】
図２４は、本発明のカード位置をタブレットやタッチパネル上の任意位置とする場合のデータ構造の説明図を示す。
【０２０６】
図２４の（ａ）は、タブレットやタッチパネル上の座標入力のイメージを示す。タブレット２１上にカード３４を当てて当該カードの左下隅および右下隅の穴又は孔、切り欠き或いはマークをペンで順次押下してカード原点（ｘ00，ｙ00）および他の特定点（ｘ01，ｙ01）を入力する。これら２つのカード原点（ｘ00，ｙ00）および他の特定点（ｘ01，ｙ01）の座標値および傾きからカード３４の位置を決める。次に、カード３４上の４点の穴又は孔、切り欠き或いはマークをペンで順次押下して座標入力（ｘ０，ｙ０）、（ｘ１，ｙ１）、（ｘ２，ｙ２）、（ｘ３，ｙ３）を行う。
【０２０７】
図２４の（ｂ）は、登録データ例を示す。
【０２０８】
図２４の（ｂ）において、点Ｎｏは、図２４の（ａ）でカード３４上の穴又は孔、切り欠き或いはマークを押下して座標を入力したシーケンシャルに付与した数であって、ここでは、１ないし４の４個である。
【０２０９】
検出座標は、点Ｎｏ１ないし４のときに検出した検出座標（ｘ１，ｙ１）、（ｘ２，ｙ２）、（ｘ３，ｙ３）、（ｘ４，ｙ４）である。
【０２１０】

カード位置検出座標は、図２４の（ａ）で入力したカード３４の左下隅のカード原点（ｘ00，ｙ00）および他の特定点（ｘ01，ｙ01）の座標値をもとに、カードの傾きｓｉｎΔθ、ｃｏｓΔθおよび距離ｌ０　を図示のように求めたものである。　ソフト１０キー比較座標は、点Ｎｏ１ないし４の各点の座標（ｘ１　，ｙ１　）、（ｘ２　，ｙ２　）、（ｘ３　，ｙ３　）、（ｘ４　，ｙ４　）について、カード位置検出座標をもとにソフト１０キー上の座標値（ｘ１　’，ｙ１　’）、（ｘ２　’，ｙ２　’）、（ｘ３　’，ｙ３　’）、（ｘ４　’，ｙ４　’）に図示の式によって変換したものである。

【０２１１】

比較結果は、ソフト１０キー比較座標（ｘ１　’，ｙ１　’）、（ｘ２　’，ｙ２　’）、（ｘ３　’，ｙ３　’）、（ｘ４　’，ｙ４　’）が属するソフト１０キー上の座標として図示のような例えば値（ｘ12，ｙ12）（ここでは、添字は“１２”は１、２、３、４、５、６、７、８、９、０と配置した１０キーを４行設定したうちの、１行目の２番目のキー（数値“２”）を表す）となる。

【０２１２】

数値は、比較結果を数値で表したものであって、ここでは、“２６９２”となる。

【０２１３】

以上のように、タブレット２１やタッチパネル上の任意の位置にカード３４を当てて例えば左下隅および右下隅の穴又は孔、切り欠き或いはマークを第１番目、第２番目にペンで押下してカード原点（ｘ00，ｙ00）および他の特定点（ｘ01，ｙ01）を指定してソフト１０キーをシステム内部で仮想的に設定し、次に、カード３４上の点Ｎｏ１ないしＮｏ４の穴又は孔、切り欠き或いはマークについてペンで第３番目から第６番目を順次押下すると、その結果が数値例えば“２６９２”として出力されることとなる。

【０２１４】

図２５は、本発明の座標検出マイコンでのローカルなＩＤ認証フローチャートを示す。

【０２１５】

図２５において、ステップＳ２０１は、座標検出マイコン４が入力ありか判別する。ステップＳ２０１の判別結果がＹＥＳの場合には、処理はステップＳ２０２に進む。ステップＳ２０１の判別結果がＮＯの場合には、待機する。

【０２１６】

ステップＳ２０２は、座標検出する。これは、後述する図２６に示すように、タブレット２１上にカード３４を当てて当該カードの穴又は孔、切り欠き或いはマークをペンで押下した座標を検出する。

【０２１７】

ステップＳ２０３は、ＩＤ認証／入力終了領域か判別する。これは、ステップＳ２０２で座標検出された座標値がらＩＤ認証を開始する領域かあるいは入力終了する領域かを判別する。ステップＳ２０３の判別結果がＹＥＳの場合には、処理はステップＳ２０４に進む。ステップＳ２０３の判別結果がＮＯの場合には、他の処理を行う。

【０２１８】

ステップＳ２０４は、ＩＤ認証処理を行う。これは、ステップＳ２０２で検出された座標値をもとに、既述した図２３および図２４のように、カード原点（ｘ00，ｙ00）および他の特定点（ｘ01，ｙ01）をもとにソフト１０キーをシステム内部で仮想的に設定し、次に、カード上の点Ｎｏ１ないしＮｏ４の穴又は孔、切り欠き或いはマークについてペンで第３番目から第６番目（ｘ１　，ｙ１　）、（ｘ２　，ｙ２　）、（ｘ３　，ｙ３　）、（ｘ４　，ｙ４　）を順次押下すると、その結果を数値に変換してキーコードを順次送出する。

【０２１９】

以上によって、座標検出マイコン４側で図２６に示すタブレット２１上にカード３４を当てて左下隅および右下隅の穴又は孔、切り欠き或いはマークをペンで押下して原点および他の特定点を指定してソフキーを仮想的に配置し、次に点Ｎｏ１ないしＮｏ４の４点のカード３４の穴又は孔、切り欠き或いはマークをペンで押下してこれら座標値をもとに数値に変換したキーコードで出力することがローカル（座標検出マイコン４側でローカル）

に可能となる。

【０２２０】

ステップＳ２０５は、パスワード型セキュリティを行う。これは、既述したように、ステップＳ２０４で１０キーに変換された数値（０、１、２・・・９）の列について、登録データと比較して一致するか判別するという、いわゆるパスワード型セキュリティを行う。

【０２２１】

ステップＳ２０６は、認証結果に対応した処理を行う。

【０２２２】

以上によって、タブレットやタッチパネルなどの座標入力装置上で原点（ｘ00，ｙ00）および他の特定点（ｘ01，ｙ01）を入力してソフト１０キーを仮想的に設定し、１０キーの枠および１０キー自身の両者を非表示とし、カード３４を当てて穴又は孔、切り欠き或いはマークをペンで押下して座標入力し、読み取った座標値をもとに１０キーのいずれが押下されたかに変換することをローカルに座標検出マイコン４側で行った後、ＣＰＵ上のソフトウェア側で登録データと比較して一致したときに認証ＯＫ、不一致のときに認証ＮＧと判定することにより、カード枠などを表示できないタブレットやタッチパネル上から任意の数字列などを入力して認証することが可能となる。

【０２２３】

図２６は、本発明のＩＤ認証起動／ＩＤ入力終了の定義説明図を示す。ここで、左下隅のＩＤ認証／入力終了の領域を設け、既述した図２５のステップＳ２０３のＩＤ認証の開始あるいはＩＤ入力終了を指示する（詳細は図２７を用いて後述する）。ここでは、タブレット２１やタッチパネル上の左下隅の特定領域をペンで押下して座標検出マイコン４のＩＤ認証処理ステップＳ２０４を起動する。次に、タブレット２１やタッチパネル上に当てたカード３４の左下隅および右下隅の穴又は孔、切り欠き或いはマークをペンで順次押下してカード原点（ｘ00，ｙ00）および他の特定点（ｘ01，ｙ01）を入力し、これらカード原点（ｘ00，ｙ00）および他の特定点（ｘ01，ｙ01）の座標値および傾きからカード３４の位置を決める。続いて、カード３４上の４点の穴又は孔、切り欠き或いはマークをペンで順次押下して座標入力（ｘ０ ，ｙ０ ）、（ｘ１ ，ｙ１ ）、（ｘ２ ，ｙ２ ）、（ｘ３ ，ｙ３ ）を行う。そして、タブレット２１やタッチパネル上の左下隅の特定領域をペンで再度押下してＩＤ入力が終了したことをマイコンに通知する。

【０２２４】

図２７は、本発明のタブレットやタッチパネル上の特定領域からの座標入力による終了検出フローチャート（順序を問う場合）を示す。

【０２２５】

図２７において、ステップＳ２１１は、ｎ回目の入力か判別する。これは、既述した図２６の例では、座標入力の４点分の４回目の入力か判別する。ステップＳ２１１の判別結果がＹＥＳの場合には、処理はステップＳ２１３に進む。ステップＳ２１１の判別結果がＮＯの場合には、処理はステップＳ２１２に進む。

【０２２６】

ステップＳ２１２は、終了入力か判別する。これは、タブレット２１やタッチパネル上の左下隅の終了領域内の座標が入力されたか判別する。ステップＳ２１２の判別結果がＮＯの場合には、処理はステップＳ２１１に戻る。ステップＳ２１２の判別結果がＹＥＳの場合には、ステップＳ２１７で入力個数と登録個数を比較し、ステップＳ２１８で一致したときにＩＤ認証出力をし、ＮＯのときには不一致出力をする。

【０２２７】

ステップＳ２１３は、座標をセーブする。

【０２２８】

ステップＳ２１４は、入力個数と登録個数を比較する。

【０２２９】

ステップＳ２１５は、入力数が登録個数をオーバーしたか判別する。ステップＳ２１５

の判別結果がＹＥＳの場合には、不一致出力をする。ステップＳ２１５の判別結果がＮＯの場合には、処理はステップＳ２１６に進む。

【０２３０】

ステップＳ２１６は、ｎ回目の入力と登録データとを比較する。

【０２３１】

ステップＳ２１９は、ステップＳ２１６での比較結果が一致か判別する。ステップＳ２１９の判別結果がＹＥＳの場合には、処理はステップＳ２１１に戻り次の入力を待機する。ステップＳ２１９の判別結果がＮＯの場合には、不一致出力をする。

【０２３２】

以上によって、タイウアウトではなく、タブレット２１やタッチパネル上の特定領域からの座標入力による終了検出を行うことによって（ステップＳ２１２のＹＥＳ）、入力された座標の順番に登録データと比較し、一致したときにＩＤ認証出力をし、不一致のときに不一致出力をする。

【０２３３】

図２８は、本発明の認証ＩＤの数を増やす説明図を示す。これは、登録データの例であって、下記の内容を持つものである。

【０２３４】

図２８において、点Ｎｏは、図２４の（ａ）、図２６でカード上の穴又は孔、切り欠き或いはマークを押下して座標を入力したシーケンシャルに付与した数であって、ここでは、説明の都合上、例えば１ないし４の４個である。

【０２３５】

検出座標は、点Ｎｏ１ないし４のときに検出した検出座標（ｘ１　，ｙ１　）、（ｘ２　，ｙ２　）、（ｘ３　，ｙ３　）、（ｘ４　，ｙ４　）である。

【０２３６】

カード位置検出座標は、図２４の（ａ）で入力したカードの左下隅のカード原点（ｘ00，ｙ00）および他の特定点（ｘ01，ｙ01）の座標値をもとに、カードの傾きｓｉｎΔθ、ｃｏｓΔθおよび距離ｌ０　を図示のように求めたのである。　比較座標（ソフト１０キー比較座標）は、点Ｎｏ１ないし４の各点の座標（ｘ１　，ｙ１　）、（ｘ２　，ｙ２　）、（ｘ３　，ｙ３　）、（ｘ４　，ｙ４　）について、カード位置検出座標をもとにソフト１０キー上の座標値（ｘ１　’，ｙ１　’）、（ｘ２　’，ｙ２　’）、（ｘ３　’，ｙ３　’）、（ｘ４　’，ｙ４　’）に図示の式によって変換したものである。

【０２３７】

登録座標は、登録した座標であって、検出座標に対応するものである。

【０２３８】

この方式はソフトキーを使わない方式である。４行×１０列の場合、ソフト１０キー方式では各行から１個づつ任意のキー（数字）を選択する。従って、１０４　＝１万通りとなる。一方、本発明の方式は、各行から１個づつの制約を取り払い、１回目の入力は４０個の穴の中から任意の１個、２回目の入力は残りの１３９個の穴から任意の１個というように選択するト、４０×３９×３８×３７＝２，１９３，３６０通りとなる。１度選択した点を除いたのは、ペン押下時のバウンドで同じ座標が複数入力される可能性があるためである。座標検出マイコンは、各座標の比較の結果、一致したと判断した場合には別途登録してあるキーコードを出力する。

【０２３９】

一方、本願発明のソフトキー１０キーの４行列を、カードの左下隅のカード原点（ｘ00，ｙ00）および右下隅の他の特定点（ｘ01，ｙ01）で仮想的に同時にタブレット２１やタッチパネル上に対応づけて設定した場合には、４行×１０列中の任意の全て穴又は孔、切り欠き或いはマークから任意の４つを選択するから、１０進４桁のＩＤを入力するときの全ＩＤの組み合わせは、４０×３９×３８×３７＝２，１９３，３６０通りとなる（従来の１０キーを用いて順次入力した場合に比して全ＩＤの組み合わせ数が２１９倍にもなる）。この際、カード原点および他の特定点にそれぞれ１点の合計２点を使うとすると、残

りが３８点となり、全ＩＤの組み合わせ数は、３８×３７×３６×３５＝１，７７１，５６０通りとなる（従来の１０キーを用いて順次入力した場合に比して全ＩＤの組み合わせ数が１７７倍にもなる）。

【０２４０】

以上のように、タブレット２１やタッチパネル上に仮想的にソフト１０キーを非表示で設定し、カードをタブレット２１に当てて当該カードの任意の２点（例えばカードの左下隅のカード原点（ｘ00，ｙ00）および右下隅の他の特定点（ｘ01，ｙ01）の２点）を指定し仮想的にソフトキー１０キーを設定し、座標入力した座標値をもとに数値に変換することにより、従来の１０キーを押下して入力する場合に比して極めてＩＤ数の組み合わせ回数を数百倍以上に増大させて信頼性を向上させたり、第三者の盗用の防止を実現することが可能となる。

【０２４１】

図２９は、本発明の応用例（その１）を示す。上述した本発明をペンＰＣ（ペン入力型のパーソナルコンピュータ）に適用した例を示す。ここでは、ペンＰＣ３１の画面３２上にカード（又はＩＤカード）３４などのカードを当ててその穴又は孔、切り欠き或いはマークを、ペン３３で押下することにより、画面３２上に配置した透明な座標検出器あるいは電磁誘導方式の場合には画面３２の下方の配置した非透明な座標検出器によってその座標がそれぞれ検出され、既述したようにして登録したＩＤなどと比較して認証を行うことが可能となる。この際、画面上３２にはカード枠を表示してそのカード枠内にカード３４を配置してペン３３で穴又は孔、切り欠き或いはマークを押下してもよいし、また、カード枠を表示しなく、当該カード３４の所定番目の１個の穴又は孔、切り欠き或いはマーク、或いは、複数の穴又は孔、切り欠き或いはマークの押下をもとにカード枠あるいはソフト１０キーの枠などを仮想的に設定してもよい。いずれにしても、表示した枠あるいは内部で仮想的に設定した枠をもとに押下された座標を検出し、登録した座標と比較して認証を行う。

【０２４２】

図３０は、本発明の応用例（その２）を示す。携帯可能な図示のようなペン入力コンピュータ４１が既に開発されている。例えば薄いＢ５やＡ４サイズの液晶表示板からなる表示部４２が取り付けられている。この表示部４２の前面を覆うように図示外の透明なタッチパネルを装着し、当該タッチパネルを入力ペン４３で接触（軽く押下）することによって、接触した位置の座標の検出が可能となる。ここで、表示部４２は、液晶表示としたが、本発明はそれだけでなく、プラズマ放電パネルやＣＲＴでもよい。このようなペン入力コンピュータ４１は既述した図１の構成を内部に持つことが可能である。また、本発明は、ペン入力コンピュータ４１のみではなく、ワードプロセッサ、電子手帳、座標検出装置を接続したデスクトップ装置、キャッシュディスペンサ等の座標検出装置を持つ各種プログラム可能な装置等にも適用可能である。また、ペンコンピュータの入力方式としては、抵抗膜方式、静電結合方式、電磁誘導方式等に大別できるが、本発明ではどの入力方式を取っても良い。電磁誘導方式の場合は、画面（例えば液晶ディスプレイ）の下方に配置した座標検出器により、ペン（又はスタイラス）からの磁気を感知して座標を検出する。更に、ペン入力がなく、指でタッチするタッチパネル等に適用してもよい。

【０２４３】

本発明の他の実施の形態では、上記の如き本発明のユーザ認証方法をコンピュータに行わせるプログラムが、コンピュータ読み取り可能な記憶媒体に格納されている。つまり、図１に示す座標検出マイコン４、又は、ＣＰＵ１及び座標検出マイコン４、又は、ＣＰＵ１及び座標検出マイコン４の機能が単一のＣＰＵで実現される場合にはこの単一のＣＰＵに上記の如きユーザ認証方法を行わせるプログラムが、ＣＤ－ＲＯＭ８ａやＦＤ９ａ等の記憶媒体に格納されている。記憶媒体はＣＤ－ＲＯＭやＦＤに限定されず、ＲＯＭ、ＥＰＲＯＭ、ＥＥＰＲＯＭ、ＲＡＭ等の半導体記憶装置、光ディスク、光磁気ディスクや磁気ディスク等の各種ディスク、カード状記録媒体等の、プログラムを格納可能な記憶媒体であれば良い。

【０２４４】
次に、本発明のユーザ認証用カードについて、図３１～図３４と共に説明する。
【０２４５】
図３１は、ユーザ認証用カードの第１実施例を示す図である。同図中、カード３４－１は、右上の角に切り欠き３４１を有し、中央部分にはユーザＩＤを入力するための穴又は孔、切り欠き、マーク或いは図１５と共に説明した打ち抜き可能な部分が設けられたＩＤ入力領域３５０が設けられている。このように、カード３４－１の形状を上下左右に対して非対称とすることにより、ユーザは容易にカード３４－１の表裏及び上下を正しく認識することができる。図３１に示すカード３４－１の場合、ユーザは、カード３４－１を座標検出器の画面に置く場合に切り欠き３４１がカード３４－１の右上の角にくるように置かなければいけないことを予め知らされている。従って、ユーザは、カード３４－１を座標検出器の画面に置く場合に切り欠き３４１がカード３４－１の右上の角にくるように置くことで、カード３４－１の表裏及び上下の方向が自動的に正しい状態で置かれることになり、カード３４－１の表裏や上下の方向が誤っていることによるユーザＩＤの誤入力を確実に防止することができる。
【０２４６】
ユーザＩＤ等を入力するためには、座標が指定できれば良く、カードを貫通する孔でも良く、貫通しない窪み状の穴でも良い。即ち、穴、窪み状の穴、貫通した孔、切り欠き印刷等されたマーク、突起状の物等でも良い。ペンコンピュータに使用される座標入力装置は、抵抗膜方式、静電結合方式、電磁誘導方式等があるが、例えば電磁誘導方式は、画面の下方に配置した座標検出器により、ペン（又はスタイラス）の磁気を感知して座標を検出するので、ペンが直接画面に触れなくても、座標検出器は磁気を感知し、座標を検出する。従って、この場合は、カードに設けるものは、必ずしも貫通する孔で無くとも良く、窪みや穴、又、単に印刷等されたマークでも良い。
【０２４７】
図３２は、ユーザ認証用カードの第２実施例を示す図である。カード３４－２の表面には、同図（ａ）に示すように、表を示すＡなるマーク３４２が印刷されており、カード３４－２の裏面には、同図（ｂ）に示すように、裏を示すＢなるマーク３４３が印刷されている。尚、例えば裏面のマーク３４３は省略して、カード３４－２の表面、裏面の一方のみにマークを設けても良い。又、マーク３４２，３４３は、例えば凹凸等の幾何学的形状変化としてカード３４－２に形成されていても良い。カード３４－２の中央部分にはユーザＩＤを入力するための穴又は孔、切り欠き、マーク或いは図１５と共に説明した打ち抜き可能な部分が設けられたＩＤ入力領域３５０が設けられている。ユーザは、カード３４－２を座標検出器の画面に置く場合にマーク３４２が正しい向きでＡと読めるように置くことで、カード３４－２の表裏及び上下の方向が自動的に正しい状態で置かれることになり、カード３４－２の表裏や上下の方向が誤っていることによるユーザＩＤの誤入力を確実に防止することができる。
【０２４８】
尚、図３１及び図３２に示すカード３４－１，３４－２のＩＤ入力領域３５０は、画面がペン等により直接接触された場合にのみ座標入力が可能な構成を用いている場合には複数の不連続な穴又は孔、切り欠き或いは図１５と共に説明した打ち抜き可能な部分からなり、カード３４－１，３４－２は透明な部材から形成されていても、不透明な部材から形成されていても良い。他方、カード３４－１，３４－２のＩＤ入力領域３５０は、画面がペン等により直接接触されなくても座標入力が可能な構成を用いている場合には複数の不連続な穴又は孔、切り欠き、マーク或いは図１５と共に説明した打ち抜き可能な部分からなり、カード３４－１，３４－２は透明な部材から形成されていても、不透明な部材から形成されていても良い。
【０２４９】
図３３は、ユーザ認証用カードの第３実施例を示す図である。同図中、カード３４－３には、穴３４４ａ，３４４ｂが上下左右に対して非対称な位置に形成されている。カード

３４－３の中央部分にはユーザＩＤを入力するための穴又は孔、切り欠き、マーク或いは図１５と共に説明した打ち抜き可能な部分が設けられたＩＤ入力領域３５０が設けられている。穴３４４ａ，３４４ｂは、例えば図５と共に説明したように、カード３４－３の位置に関するデータを座標検出マイコン４に入力する際に用いられる。又、カード３４－３の右上の角に形成された穴３４４ａは、図３１又は図３２と共に示したような、ユーザがカード３４－３の表裏及び上下を正しく認識するための向き指示手段としても機能する。このように、カード３４－１の穴３４４ａ，３４４ｂの位置を上下左右に対して非対称とすることにより、ユーザは容易にカード３４－３の表裏及び上下を正しく認識することができる。図３３に示すカード３４－３の場合、ユーザは、カード３４－３を座標検出器の画面に置く場合に穴３４４ａがカード３４－３の右上の角にくるように置かなければいけないことを予め知らされている。従って、ユーザは、カード３４－３を座標検出器の画面に置く場合に穴３４４ａがカード３４－３の右上の角にくるように置くことで、カード３４－３の表裏及び上下の方向が自動的に正しい状態で置かれることになり、カード３４－３の表裏や上下の方向が誤っていることによるユーザＩＤの誤入力を確実に防止することができる。

【０２５０】

図３４は、ユーザ認証用カードの第４実施例を示す図である。同図中、カード３４－４には、マーク３４５ａ，３４５ｂが上下左右に対して非対称な位置に印刷又は幾何学的形状変化として形成されている。カード３４－３の中央部分にはユーザＩＤを入力するための穴又は孔、切り欠き、マーク或いは図１５と共に説明した打ち抜き可能な部分が設けられたＩＤ入力領域３５０が設けられている。マーク３４５ａ，３４５ｂは、例えば図５と共に説明したように、カード３４－４の位置に関するデータを座標検出マイコン４に入力する際に用いられる。又、カード３４－４の右上の角に形成されたマーク３４５ａは、図３１又は図３２と共に示したような、ユーザがカード３４－４の表裏及び上下を正しく認識するための向き指示手段としても機能する。このように、カード３４－４のマーク３４５ａ，３４５ｂの位置を上下左右に対して非対称とすることにより、ユーザは容易にカード３４－４の表裏及び上下を正しく認識することができる。図３４に示すカード３４－４の場合、ユーザは、カード３４－４を座標検出器の画面に置く場合に穴３４５ａがカード３４－４の右上の角にくるように置かなければいけないことを予め知らされている。従って、ユーザは、カード３４－４を座標検出器の画面に置く場合にマーク３４５ａがカード３４－４の右上の角にくるように置くことで、カード３４－４の表裏及び上下の方向が自動的に正しい状態で置かれることになり、カード３４－４の表裏や上下の方向が誤っていることによるユーザＩＤの誤入力を確実に防止することができる。

【０２５１】

尚、図３３に示すカード３４－３のＩＤ入力領域３５０は、画面がペン等により直接接触された場合にのみ座標入力が可能な構成を用いている場合には複数の不連続な穴又は孔、切り欠き或いは図１５と共に説明した打ち抜き可能な部分からなり、カード３４－３は透明な部材から形成されていても、不透明な部材から形成されていても良い。他方、図３４に示すカード３４－４のＩＤ入力領域３５０は、画面がペン等により直接接触されなくても座標入力が可能な構成を用いている場合には複数の不連続な穴又は孔、切り欠き、マーク或いは図１５と共に説明した打ち抜き可能な部分からなり、カード３４－４は透明な部材から形成されていても、不透明な部材から形成されていても良い。

【０２５２】

又、画面に表示される位置マーカがカードの外形内に表示される場合には、カードを透明な部材で形成することが望ましい。この場合、表示された位置マーカがカードを透過して見えるので、表示された位置マーカに対してカードを画面上で動かしながら、カードに設けられた穴又は孔、切り欠き或いはマークを位置マーカの位置と一致させやすい。

【０２５３】

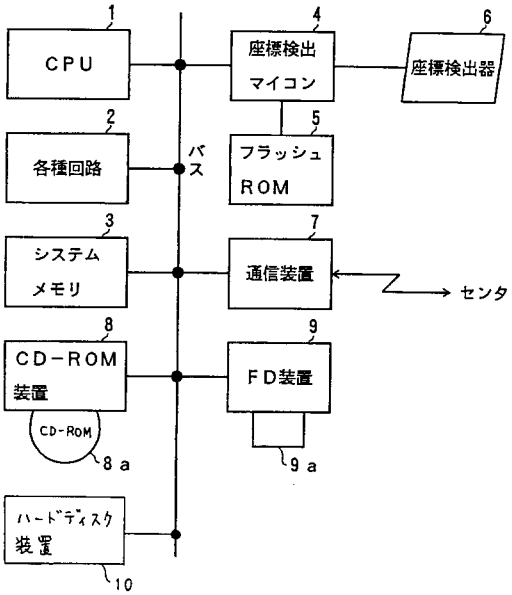
更に、上記カードの各種実施例を任意に組み合わせ、カードに穴又は孔、切り欠き、マーク及び／又は打ち抜き可能な部分を混在させても良いことは言うまでもない。

【０２５４】
以上、本発明を実施例により説明したが、本発明は上記実施例に限定されるものではなく、本発明の範囲内で種々の変形及び改良が可能であることは言うまでもない。
【図面の簡単な説明】
【０２５５】
【図１】本発明のシステム構成図である。
【図２】本発明の全体の動作説明フローチャートである。
【図３】本発明のカード位置変更フローチャートである。
【図４】本発明のユーザＩＤ入力画面イメージ例である。
【図５】本発明のカードを当てる位置を変更可能にする場合の説明図である。
【図６】本発明の登録データの構造説明図である。
【図７】本発明の入力順序を問わない場合の動作説明フローチャートである。
【図８】本発明の入力順序を問う場合の動作説明フローチャートである。
【図９】本発明のカード位置変更フローチャートである。
【図１０】本発明のＣＰＵ上のソフトウェアがカードの位置を通知する場合のデータ構造説明図である。
【図１１】本発明のソフトＫＢを利用するフローチャートである。
【図１２】本発明の非表示のソフト１０キー上にカードを当ててキーコードを通知する場合のデータ構造の説明図である。
【図１３】本発明の非表示のソフト１０キー上にカードを当ててキーコードを通知する場合のデータ構造の説明図（他の例）である。
【図１４】本発明のソフトＫＢを利用するフローチャートである。
【図１５】本発明のカードの構造例である。
【図１６】本発明の抵抗膜方式の場合の説明図である。
【図１７】本発明の比較説明図（固定値）である。
【図１８】本発明のセキュリティレベル設定説明図である。
【図１９】本発明の相対座標の範囲設定の説明図である。
【図２０】本発明の許容範囲の学習説明図である。
【図２１】本発明の検出終了の動作説明フローチャート（順序なしの場合）である。
【図２２】本発明の検出終了の動作説明フローチャート（順序ありの場合）である。
【図２３】本発明のタブレット上の任意位置にカードを当てるフローチャートである。
【図２４】本発明のカード位置をタブレット上の任意位置とする場合のデータ構造の説明図である。
【図２５】本発明の座標検出マイコンでのローカルなＩＤ認証フローチャートである。
【図２６】本発明のＩＤ認証起動／ＩＤ入力終了の定義説明図である。
【図２７】本発明のタブレット上の特定領域からの座標入力による終了検出フローチャート（順序を問う場合）である。
【図２８】本発明の認証ＩＤの数を増やす説明図である。
【図２９】本発明の応用例（その１）である。
【図３０】本発明の応用例（その２）である。
【図３１】ユーザ認証用カードの第１実施例を示す図である。
【図３２】ユーザ認証用カードの第２実施例を示す図である。
【図３３】ユーザ認証用カードの第３実施例を示す図である。
【図３４】ユーザ認証用カードの第４実施例を示す図である。
【符号の説明】
【０２５６】
１　ＣＰＵ
２　各種回路
３　システムメモリ
４　座標検出マイコン

５　フラッシュＲＯＭ
６　座標検出器
７　通信装置
８　ＣＤ－ＲＯＭ装置
９　ＦＤ装置
１０　ハードディスク装置
１１　画面
１２　カード枠
１３　ＫＢマイコン
２１　タブレット
３１　ペンＰＣ
３２　画面
３３　ペン
３４，３４－１～３４－４　カード（ＩＤカード）
４１　ペン入力コンピュータ
４２　表示部（パネル）
４３　入力ペン

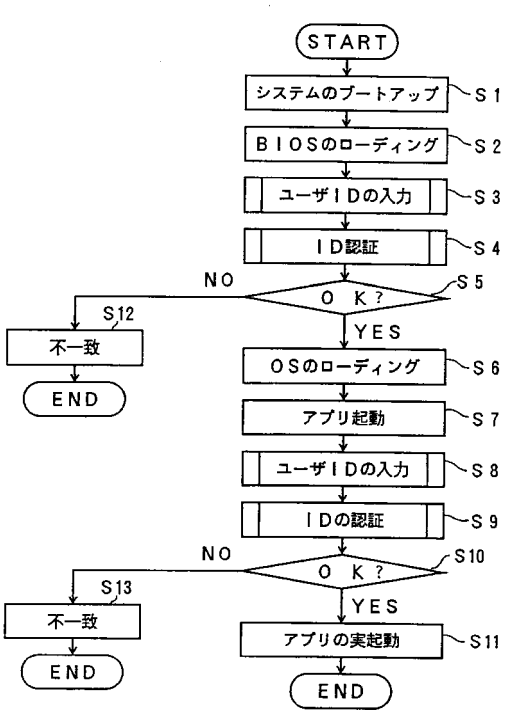
【図１】

本発明のシステム構成図



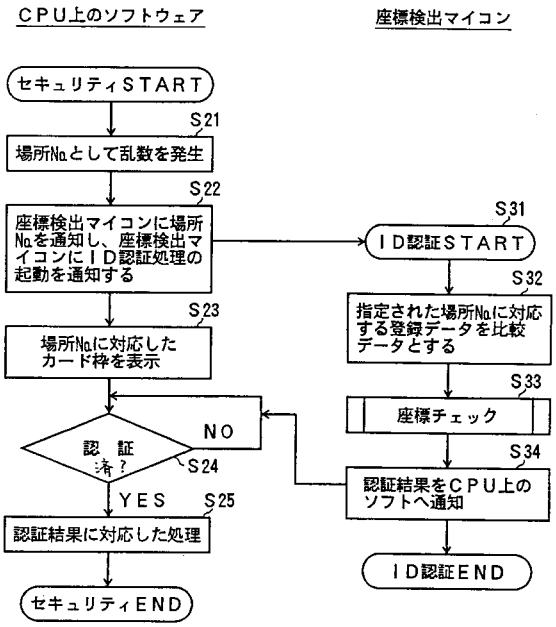
【図２】

本発明の全体の動作説明フローチャート



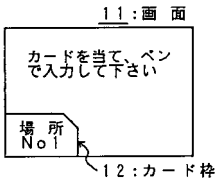
【図３】

本発明のカード位置変更フローチャート



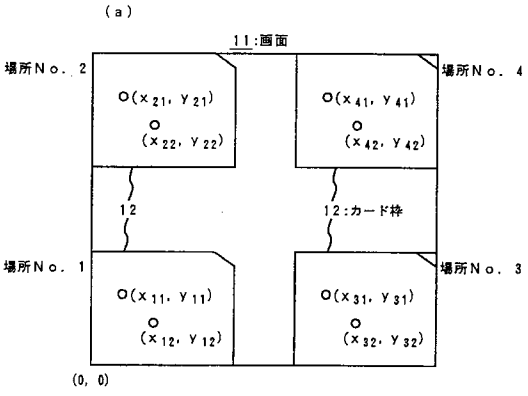
【図４】

本発明のユーザＩＤ入力画面イメージ例



【図５】

本発明のカードを当てる位置を変更可能にする場合の説明図



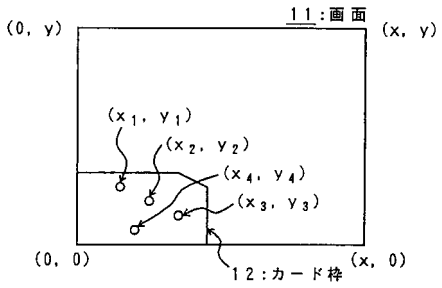
(b) 登録データ例

場所No.	点No.	座 標
1	1	(x_{11}, y_{11})
	2	(x_{12}, y_{12})
2	1	(x_{21}, y_{21})
	2	(x_{22}, y_{22})
3	1	(x_{31}, y_{31})
	2	(x_{32}, y_{32})
4	1	(x_{41}, y_{41})
	2	(x_{42}, y_{42})

【図６】

本発明の登録データの構造説明図

(a) 画面左下原点の例

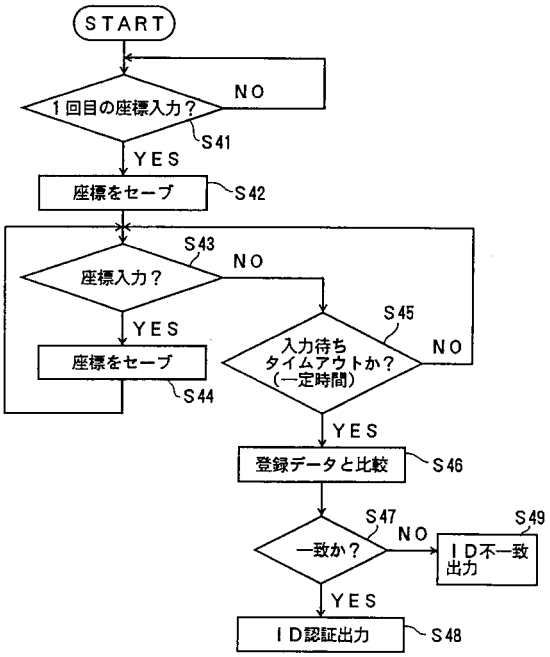


(b) 登録データ例

No.	座 標
1	(x_1, y_1)
2	(x_2, y_2)
3	(x_3, y_3)
4	(x_4, y_4)

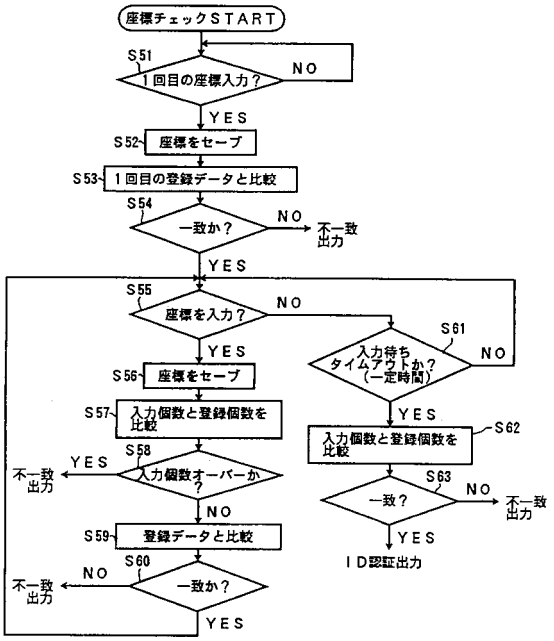
【図７】

本発明の入力順序を問わない場合の動作説明フローチャート



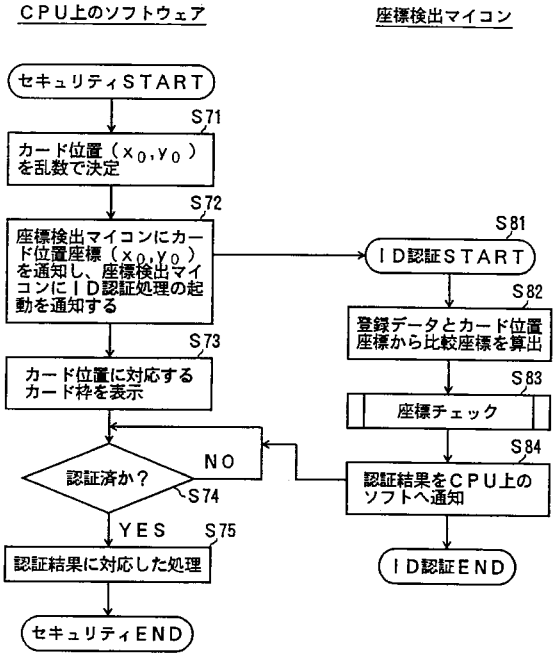
【図８】

本発明の入力順序を問う場合の動作説明フローチャート



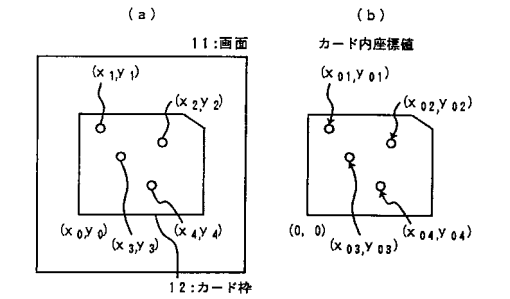
【図９】

本発明のカード位置変更フローチャート



【図１０】

本発明のＣＰＵ上のソフトウェアーがカードの位置を通知する場合のデータ構造説明図



（ｃ）登録データ

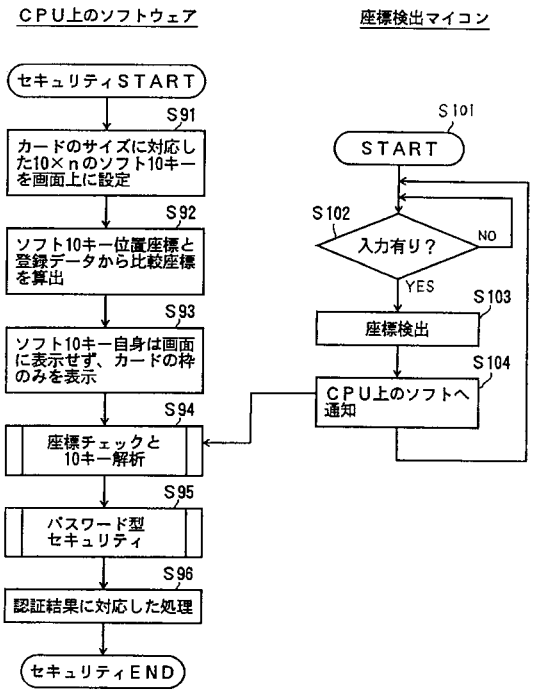
点Ｎｏ.	カード原点	カード内穴座標値	比較座標値
1	(x_0,y_0)	(x_{01},y_{01})	$(x_1,y_1)=(x_0+x_{01},\ y_0+y_{01})$
2		(x_{02},y_{02})	$(x_2,y_2)=(x_0+x_{02},\ y_0+y_{02})$
3		(x_{03},y_{03})	$(x_3,y_3)=(x_0+x_{03},\ y_0+y_{03})$
4		(x_{04},y_{04})	$(x_4,y_4)=(x_0+x_{04},\ y_0+y_{04})$

登録データ　CPUから受取るデータ

認証のために実際の検出座標と比較するデータを認証前に演算して求める

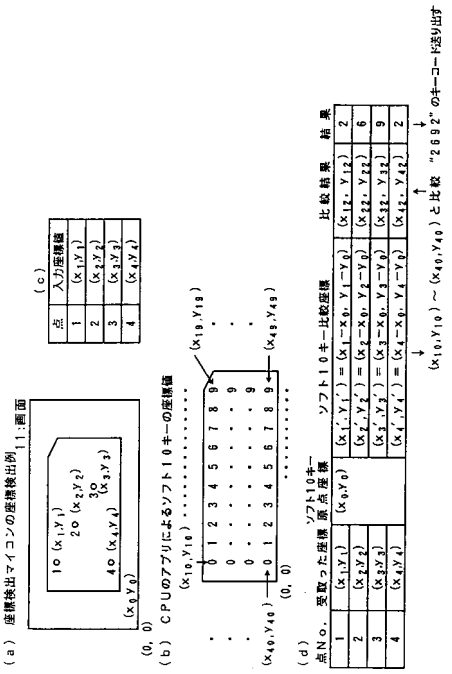
【図１１】

本発明のソフトＫＢを利用するフローチャート



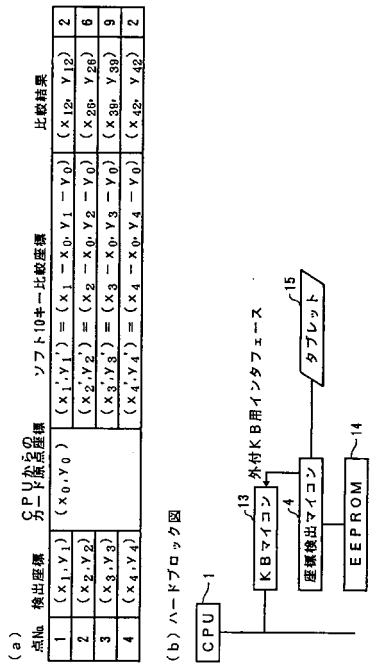
【図１２】

本発明の非表示のソフト１０キー上にカードを当ててキーコードを通知する場合のデータ構造の説明図



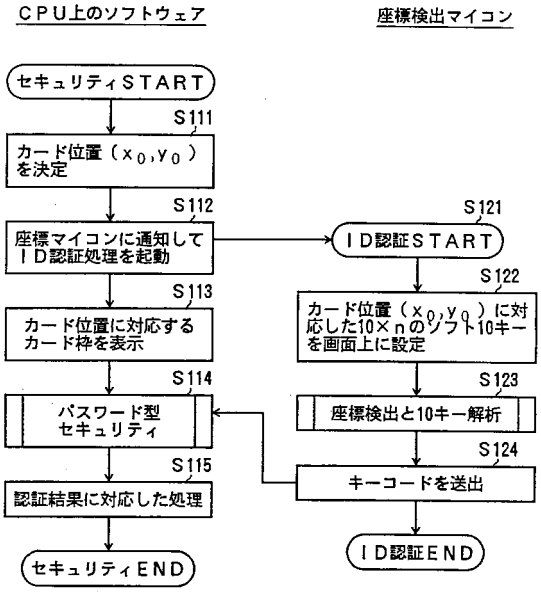
【図１３】

本発明の非表示のソフト10キー上にカードを当てて
キーコードを通知する場合のデータ構造の説明図（他の例）



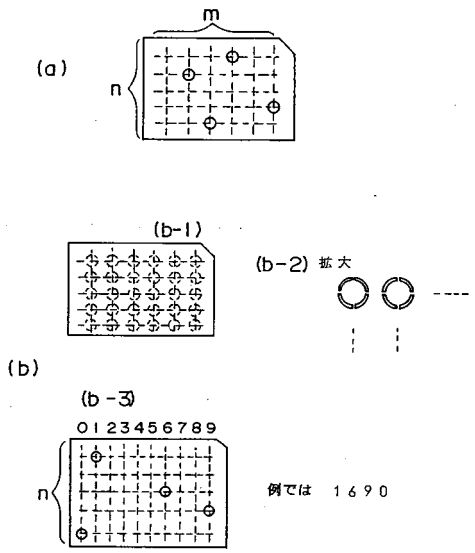
【図１４】

本発明のソフトＫＢを利用するフローチャート



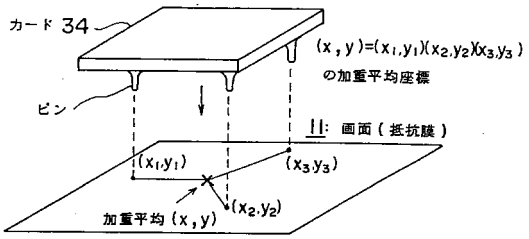
【図１５】

本発明のカードの構造例



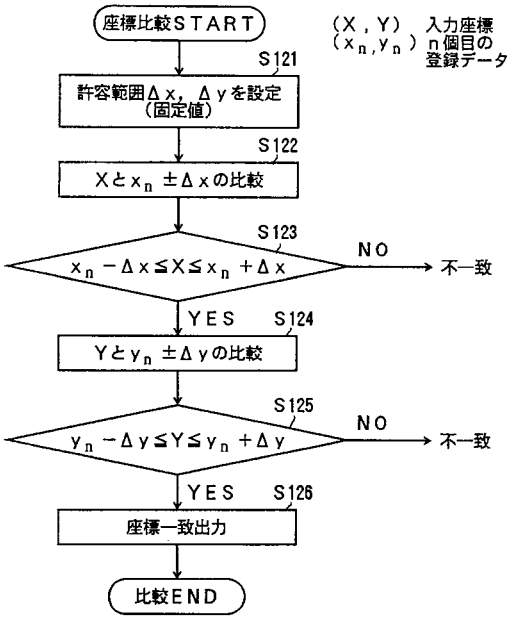
【図１６】

本発明の抵抗膜方式の場合の説明図



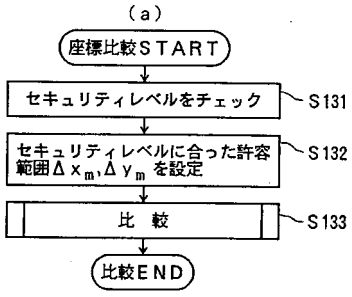
【図１７】

本発明の比較説明図（固定値）



【図１８】

本発明のセキュリティレベル設定説明図



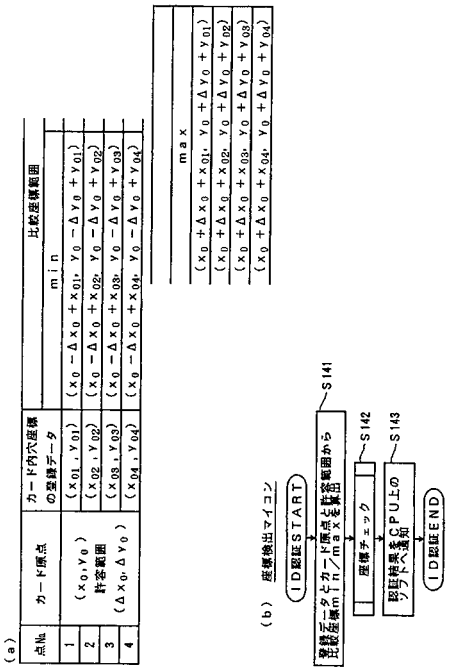
(b) データ構造例

セキュリティレベル	許容範囲
1	$(\Delta x_1, \Delta y_1)$
⋮	⋮
m	$(\Delta x_m, \Delta y_m)$
⋮	⋮
ℓ	$(\Delta x_\ell, \Delta y_\ell)$

ただし $\Delta x_1 > \cdots > \Delta x_m > \cdots > \Delta x_\ell$
$\Delta y_1 > \cdots > \Delta y_m > \cdots > \Delta y_\ell$

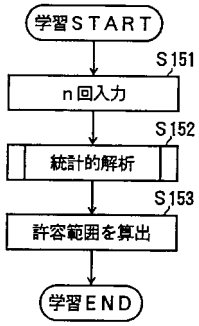
【図１９】

本発明の相対座標の範囲設定の説明図



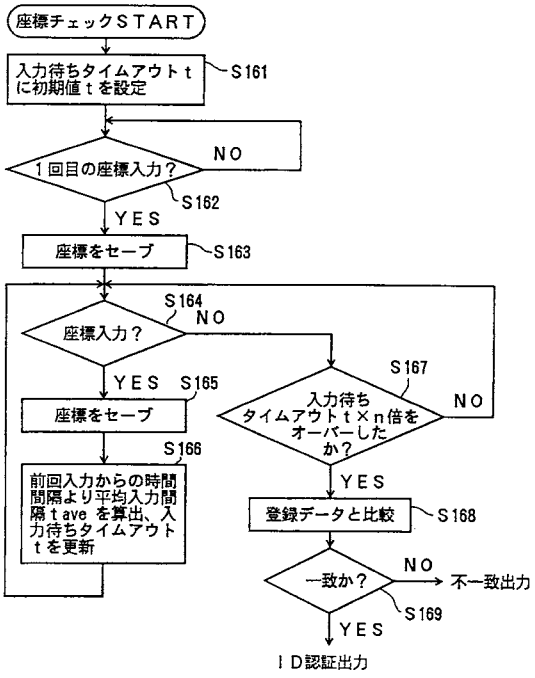
【図２０】

本発明の許容範囲の学習説明図



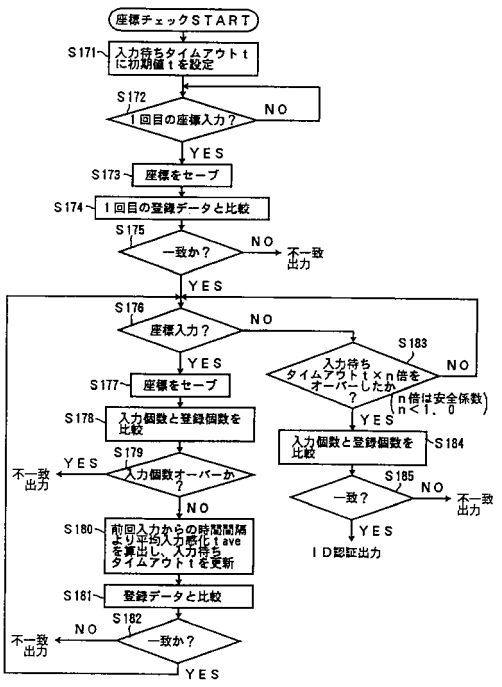
【図２１】

本発明の検出終了の動作説明フローチャート
（順序なしの場合）



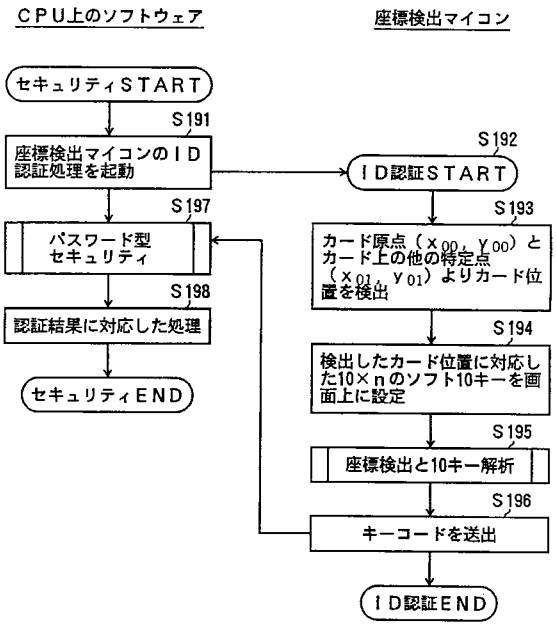
【図２２】

本発明の検出終了の動作説明フローチャート
（順序ありの場合）



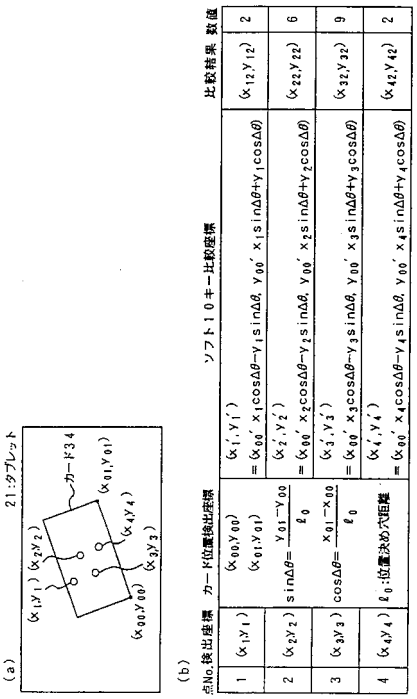
【図２３】

本発明のタブレット上の任意位置に
カードを当てるフローチャート



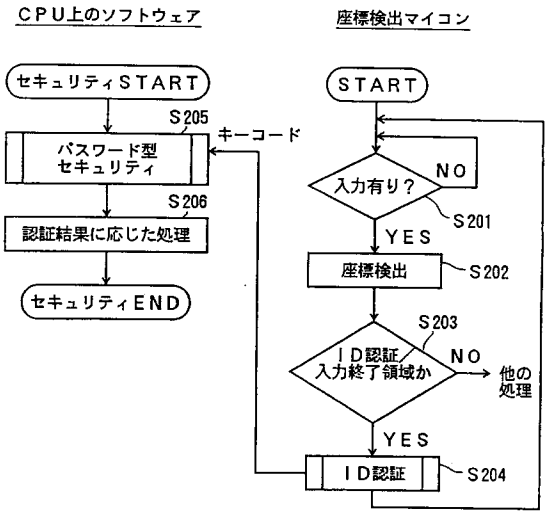
【図２４】

本発明のカード位置をタブレット上の任意位置とする場合のデータ構造の説明図



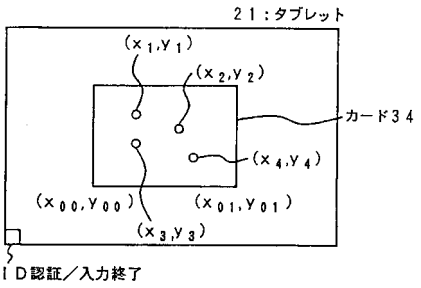
【図２５】

本発明の座標検出マイコンでのローカルな
ＩＤ認証フローチャート



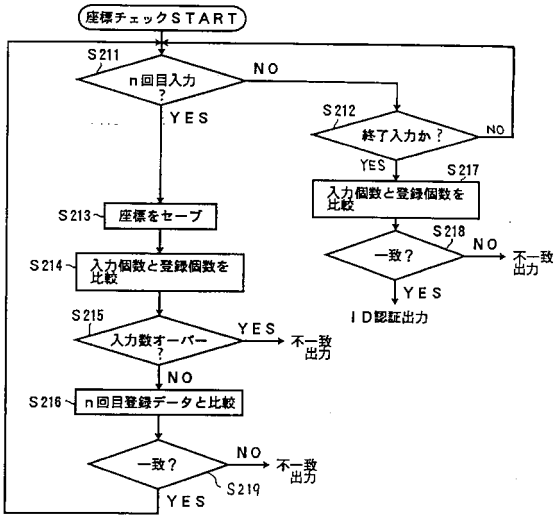
【図２６】

本発明のＩＤ認証起動／ＩＤ入力終了の定義説明図



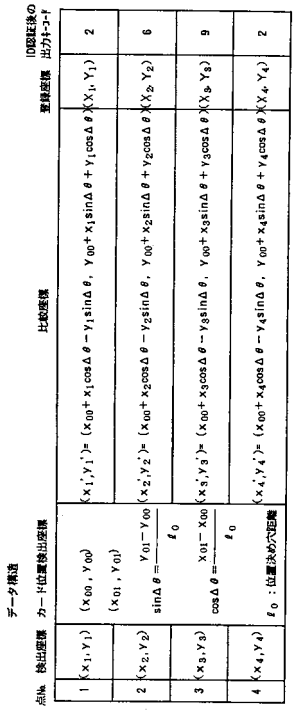
【図２７】

本発明のタブレット上の特定領域からの座標入力による終了検出フローチャート（順序を問う場合）



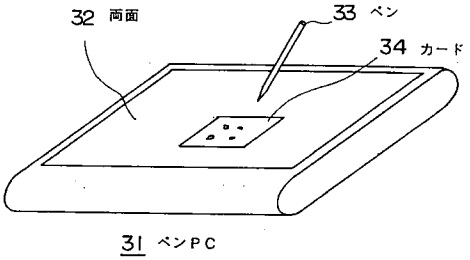
【図２８】

本発明の認証ＩＤの数を増やす説明図



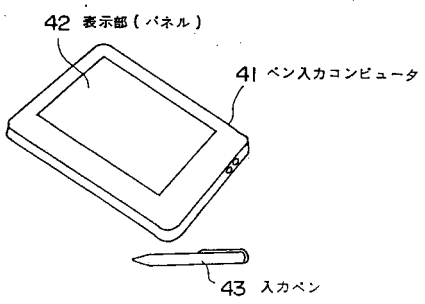
【図２９】

本発明の応用例（その１）



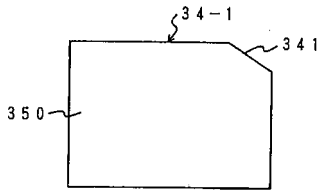
【図３０】

本発明の応用例（その２）



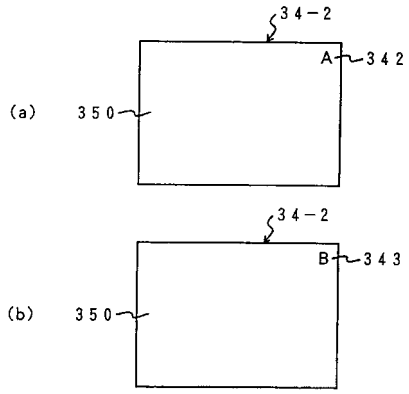
【図３１】

ユーザ認証用カードの第１実施例を示す図



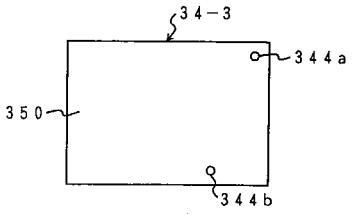
【図３２】

ユーザ認証用カードの第２実施例を示す図



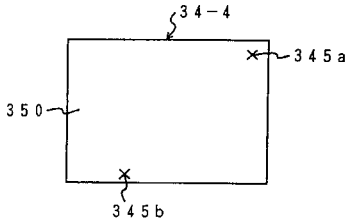
【図３３】

ユーザ認証用カードの第３実施例を示す図



【図３４】

ユーザ認証用カードの第４実施例を示す図



フロントページの続き

(72)発明者　佐相　秀幸
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　鳥居　稔

(56)参考文献　特開平０７－０８４６６１（ＪＰ，Ａ）
特開平０７－２５４９５５（ＪＰ，Ａ）
特開平０９－０５４８６２（ＪＰ，Ａ）
特開平０８－３２８７２５（ＪＰ，Ａ）
特開平０８－２４９２８４（ＪＰ，Ａ）
特開平０７－２００１２９（ＪＰ，Ａ）
特開平０６－２３０８４６（ＪＰ，Ａ）
実開昭６０－０７１９５２（ＪＰ，Ｕ）
特開平０７－１８２０９８（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／００－２４
Ｇ０６Ｆ　３／０４１