(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2008-77256
(P2008-77256A)
(43)公開日　平成20年4月3日(2008.4.3)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/20	(2006.01)	G06F	15/00	330F	5B285
H04Q 7/38	(2006.01)	H04B	7/26	109R	5J104
H04L 9/32	(2006.01)	H04B	7/26	109H	5K027
H04M 1/00	(2006.01)	H04L	9/00	673A	5K067
H04M 1/66	(2006.01)	H04M	1/00	B	

審査請求 未請求　請求項の数 12　ＯＬ　（全 11 頁）　最終頁に続く

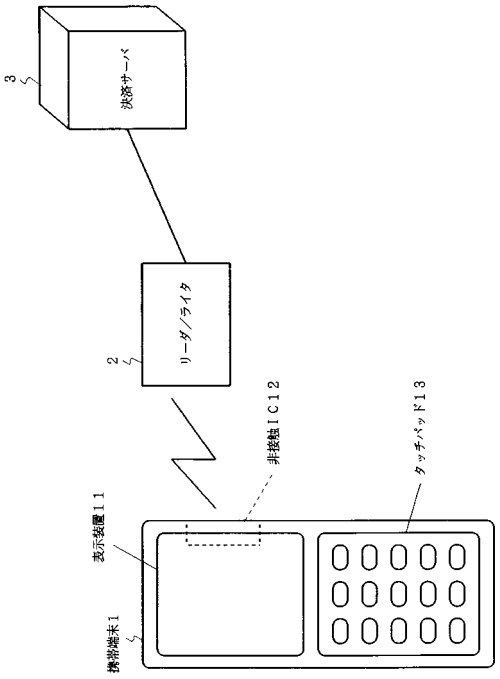
(21)出願番号　特願2006-253655 (P2006-253655)
(22)出願日　平成18年9月20日 (2006.9.20)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(74)代理人　100088812
弁理士　▲柳▼川　信
(72)発明者　藤本　英男
東京都港区芝五丁目７番１号　日本電気株式会社内

Ｆターム(参考)　5B285 AA01 BA01 CA02 CB24 CB52 CB56 CB63 CB74 CB83 DA10
5J104 AA07 KA01 KA04 NA05 NA38 PA01
5K027 AA11 BB01 BB09 FF22 HH23 HH26
5K067 AA30 BB21 DD51 EE02 FF02 FF23 HH22 HH23

(54)【発明の名称】携帯端末装置及びそれに用いるセキュリティ確保方法並びにそのプログラム

(57)【要約】
【課題】　電子マネー機能や個人情報の使用許可の認証を煩わしい登録処理や認証処理を行うことなく、即時にかつ簡便に行うことが可能な携帯端末装置を提供する。
【解決手段】　携帯端末装置１では支払い金額がタッチパッド１３もしくはテンキーによって入力されると、タッチパッド１３上で入力されたサインの情報とサイン情報保持部の認証用データとを比較し、一致しているかどうかを確認する。携帯端末装置１では、それらのデータが一致していれば、電子マネー機能の使用を許可し、携帯端末装置１をリーダ／ライタ２に近付けて決済サーバ３との間で決済を行う。携帯端末装置１は上記の認証が３回連続で失敗した場合、他人が電子マネー機能を不正使用していると判断してエラー終了とする。
【選択図】　図１



【特許請求の範囲】
【請求項１】
少なくとも電子マネー機能を搭載する携帯端末装置であって、
手書きのサインを入力する入力手段と、前記入力手段にて予め入力されたサインの情報を記憶する記憶手段と、前記電子マネー機能の使用時に前記入力手段から入力されたサインの情報と前記記憶手段に記憶したサインの情報とを比較してそれらが一致した時に前記電子マネー機能の使用を許可する許可手段とを有することを特徴とする携帯端末装置。
【請求項２】
前記電子マネー機能の使用時に金額設定を行うことを特徴とする請求項１記載の携帯端末装置。
【請求項３】
前記許可手段は、自端末に予め保持された個人情報の使用時に前記入力手段から入力されたサインの情報と前記記憶手段に記憶したサインの情報とを比較してそれらが一致した時に前記個人情報の使用を許可することを特徴とする請求項１または請求項２記載の携帯端末装置。
【請求項４】
前記入力手段は、前記電子マネー機能の使用における支払金額の確認の後に前記手書きのサインの入力を行うことを特徴とする請求項１から請求項３のいずれか記載の携帯端末装置。
【請求項５】
少なくとも個人情報を保持する携帯端末装置であって、
手書きのサインを入力する入力手段と、前記入力手段にて予め入力されたサインの情報を記憶する記憶手段と、前記個人情報の使用時に前記入力手段から入力されたサインの情報と前記記憶手段に記憶したサインの情報とを比較してそれらが一致した時に前記個人情報の使用を許可する許可手段とを有することを特徴とする携帯端末装置。
【請求項６】
少なくとも電子マネー機能を搭載する携帯端末装置に用いるセキュリティ確保方法であって、
前記携帯端末装置が、手書きのサインを入力する入力処理と、前記入力処理にて予め入力されたサインの情報を記憶手段に記憶する処理と、前記電子マネー機能の使用時に前記入力処理にて入力されたサインの情報と前記記憶手段に記憶したサインの情報とを比較してそれらが一致した時に前記電子マネー機能の使用を許可する処理とを実行することを特徴とするセキュリティ確保方法。
【請求項７】
前記携帯端末装置において前記電子マネー機能の使用時に金額設定を行うことを特徴とする請求項６記載のセキュリティ確保方法。
【請求項８】
前記携帯端末装置が、前記電子マネー機能の使用を許可する処理において、自端末に予め保持された個人情報の使用時に前記入力処理にて入力されたサインの情報と前記記憶手段に記憶したサインの情報とを比較してそれらが一致した時に前記個人情報の使用を許可することを特徴とする請求項６または請求項７記載のセキュリティ確保方法。
【請求項９】
前記携帯端末装置が、前記入力処理において、前記電子マネー機能の使用における支払金額の確認の後に前記手書きのサインの入力を行うことを特徴とする請求項１から請求項３のいずれか記載のセキュリティ確保方法。
携帯端末装置。
【請求項１０】
少なくとも個人情報を保持する携帯端末装置に用いるセキュリティ確保方法であって、
前記携帯端末装置が、手書きのサインを入力する入力処理と、前記入力処理にて予め入力されたサインの情報を記憶手段に記憶する処理と、前記個人情報の使用時に前記入力処

理にて入力されたサインの情報と前記記憶手段に記憶したサインの情報とを比較してそれらが一致した時に前記個人情報の使用を許可する処理とを実行することを特徴とするセキュリティ確保方法。

【請求項１１】

少なくとも電子マネー機能を搭載する携帯端末装置が実行するプログラムであって、

前記携帯端末装置の中央処理装置に、手書きのサインを入力する入力処理と、前記入力処理にて予め入力されたサインの情報を記憶手段に記憶する処理と、前記電子マネー機能の使用時に前記入力処理にて入力されたサインの情報と前記記憶手段に記憶したサインの情報とを比較してそれらが一致した時に前記電子マネー機能の使用を許可する処理とを実行させるためのプログラム。

【請求項１２】

少なくとも個人情報を保持する携帯端末装置が実行するプログラムであって、

前記携帯端末装置の中央処理装置に、手書きのサインを入力する入力処理と、前記入力処理にて予め入力されたサインの情報を記憶手段に記憶する処理と、前記個人情報の使用時に前記入力処理にて入力されたサインの情報と前記記憶手段に記憶したサインの情報とを比較してそれらが一致した時に前記個人情報の使用を許可する処理とを実行させるためのプログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は携帯端末装置及びそれに用いるセキュリティ確保方法並びにそのプログラムに関し、特に携帯端末装置上での電子マネー機能や個人情報の使用時におけるセキュリティの確保に関する。

【背景技術】

【０００２】

従来、携帯端末装置のセキュリティを確保する方法としては、指紋認証や顔認証等の認証方法がある。しかしながら、指紋認証の場合には、指紋を検出するセンサを専用に必要とするため、部品コストが高くなり、顔認証の場合には、認証精度が高くないという課題がある。

【０００３】

この問題を解決するために、従来の認証方法としては、手書きのサインを入力するための入力部を携帯端末装置に設け、互いに相手端末装置のサインが登録された機器間での無線接続の際に認証を行う方法（例えば、特許文献１参照）、手書きのサインの波形等を認証サーバに登録しておいて認証を行う際に手書きのサインを携帯端末装置から認証サーバに送って認証を行う方法（例えば、特許文献２参照）等が提案されている。

【０００４】

【特許文献１】特開２００２－３１５０５５号公報

【特許文献２】特開２００２－１４２２５５号公報

【発明の開示】

【発明が解決しようとする課題】

【０００５】

しかしながら、上述した従来の認証方法では、上記の特許文献１，２に記載の技術において、例えば、非接触ＩＣ（集積回路）等による電子マネー機能を搭載した携帯端末装置においてその電子マネー機能の使用を許可するかどうかの認証に使用することも、また個人情報の使用のを許可するかどうかの認証に使用することも考慮されておらず、専用部品を必要とする指紋認証や認証精度の荒い顔認証を用いざるを得ない。

【０００６】

つまり、上記の特許文献１，２に記載の技術を用いる場合には、電子マネー機能や個人情報を使用する際の相手側の装置に予めサインを登録しておかなければならず、即時性や簡便性が要求される電子マネー機能や個人情報の使用に際して煩わしい登録処理や認証処

理を行わなければならない。

【０００７】

そこで、本発明の目的は上記の問題点を解消し、電子マネー機能や個人情報の使用許可の認証を煩わしい登録処理や認証処理を行うことなく、即時にかつ簡便に行うことができる携帯端末装置及びそれに用いるセキュリティ確保方法並びにそのプログラムを提供することにある。

【課題を解決するための手段】

【０００８】

本発明による第１の携帯端末装置は、少なくとも電子マネー機能を搭載する携帯端末装置であって、

手書きのサインを入力する入力手段と、前記入力手段にて予め入力されたサインの情報を記憶する記憶手段と、前記電子マネー機能の使用時に前記入力手段から入力されたサインの情報と前記記憶手段に記憶したサインの情報とを比較してそれらが一致した時に前記電子マネー機能の使用を許可する許可手段とを備えている。

【０００９】

本発明による第２の携帯端末装置は、少なくとも個人情報を保持する携帯端末装置であって、

手書きのサインを入力する入力手段と、前記入力手段にて予め入力されたサインの情報を記憶する記憶手段と、前記個人情報の使用時に前記入力手段から入力されたサインの情報と前記記憶手段に記憶したサインの情報とを比較してそれらが一致した時に前記個人情報の使用を許可する許可手段とを備えている。

【００１０】

本発明による第１のセキュリティ確保方法は、少なくとも電子マネー機能を搭載する携帯端末装置に用いるセキュリティ確保方法であって、

前記携帯端末装置が、手書きのサインを入力する入力処理と、前記入力処理にて予め入力されたサインの情報を記憶手段に記憶する処理と、前記電子マネー機能の使用時に前記入力処理にて入力されたサインの情報と前記記憶手段に記憶したサインの情報とを比較してそれらが一致した時に前記電子マネー機能の使用を許可する処理とを実行している。

【００１１】

本発明による第２のセキュリティ確保方法は、少なくとも個人情報を保持する携帯端末装置に用いるセキュリティ確保方法であって、

前記携帯端末装置が、手書きのサインを入力する入力処理と、前記入力処理にて予め入力されたサインの情報を記憶手段に記憶する処理と、前記個人情報の使用時に前記入力処理にて入力されたサインの情報と前記記憶手段に記憶したサインの情報とを比較してそれらが一致した時に前記個人情報の使用を許可する処理とを実行している。

【００１２】

本発明による第１のプログラムは、少なくとも電子マネー機能を搭載する携帯端末装置が実行するプログラムであって、

前記携帯端末装置の中央処理装置に、手書きのサインを入力する入力処理と、前記入力処理にて予め入力されたサインの情報を記憶手段に記憶する処理と、前記電子マネー機能の使用時に前記入力処理にて入力されたサインの情報と前記記憶手段に記憶したサインの情報とを比較してそれらが一致した時に前記電子マネー機能の使用を許可する処理とを実行させている。

【００１３】

本発明による第２のプログラムは、少なくとも個人情報を保持する携帯端末装置が実行するプログラムであって、

前記携帯端末装置の中央処理装置に、手書きのサインを入力する入力処理と、前記入力処理にて予め入力されたサインの情報を記憶手段に記憶する処理と、前記個人情報の使用時に前記入力処理にて入力されたサインの情報と前記記憶手段に記憶したサインの情報とを比較してそれらが一致した時に前記個人情報の使用を許可する処理とを実行させている

。
【００１４】
すなわち、本発明の携帯端末装置は、電子マネー機能や個人情報の使用時に、その使用許可の認証を手書きのサインの確認にて行うことによって、他人による電子マネー機能や個人情報の不正使用を防ぐことが可能となる。
【００１５】
また、本発明の携帯端末装置は、電子マネー機能の使用時に、その使用許可の認証を手書きサインの確認にて行うとともに、金額設定を携帯端末装置で行うことによって、誤って間違った金額を支払うことを防ぐことが可能となる。
【００１６】
より具体的に説明すると、本発明の携帯端末装置では、表示装置、非接触ＩＣ（集積回路）、タッチパッド等を備え、電子マネー機能や個人情報の使用時にサイン入力画面を表示し、使用者がタッチパッドを用いてサインを入力すると、その入力されたサインと予め入力していたデータとを比較し、データが一致した時に電子マネー機能や個人情報の使用を許可している。
【００１７】
例えば、電子マネー機能を使用する場合、携帯端末装置の非接触ＩＣがリーダ／ライタと通信することで、リーダ／ライタが非接触ＩＣの情報を入手して決済サーバに情報を確認することで、電子マネー機能による決済を行う。その際、携帯端末装置は支払う金額を自端末装置に入力もしくは了承してからサインの記入、支払いを行う。
【００１８】
上記のように、本発明の携帯端末装置では、電子マネー機能や個人情報の使用時にサインによる本人認証を行って電子マネー機能や個人情報の使用許可を判断しているので、他人による電子マネー機能や個人情報の無断使用を防ぐことが可能となり、また金額設定を携帯端末装置で行っているため、誤って間違った金額を支払うことを防ぐことが可能となる。
【００１９】
よって、本発明の携帯端末装置では、電子マネー機能や個人情報の使用許可の認証を煩わしい登録処理や認証処理を行うことなく、即時にかつ簡便に行うことが可能となる。
【発明の効果】
【００２０】
本発明は、上記のような構成及び動作とすることで、電子マネー機能や個人情報の使用許可の認証を煩わしい登録処理や認証処理を行うことなく、即時にかつ簡便に行うことができるという効果が得られる。
【発明を実施するための最良の形態】
【００２１】
次に、本発明の実施例について図面を参照して説明する。
【実施例１】
【００２２】
図１は本発明の第１の実施例による携帯端末装置を含む決済システムの構成を示すブロック図である。図１において、本発明の第１の実施例による決済システムは携帯端末装置１と、携帯端末装置１の非接触ＩＣ（集積回路）１２との間で通信を行うリーダ／ライタ２と、リーダ／ライタ２との間で通信を行う決済サーバ３とから構成されている。
【００２３】
携帯端末装置１はキー入力結果を表示する表示装置１１、リーダ／ライタ２との間で近接距離にて通信を行う非接触ＩＣ１２、ユーザが指でサインを書くことによって携帯端末装置１に対して個人認証情報を入力可能なタッチパッド１３等を備えている。
【００２４】
また、リーダ／ライタ２は携帯端末装置１の非接触ＩＣ１２と通信し、非接触ＩＣ１２の情報を入手し、決済サーバ３に情報を確認して携帯端末装置１による決済を行う。尚、

本実施例では、タッチパッド１３について、スタイラスペン等による入力としても適用可能である。

【００２５】

図２は図１の携帯端末装置１の構成例を示すブロック図である。図２において、携帯端末装置１は、アンテナ１０と、表示装置１１と、非接触ＩＣ１２と、タッチパッド１３と、ＣＰＵ（中央処理装置）１４と、アンテナ１０を通して無線通信を行う無線部１５と、ＣＰＵ１４が実行する制御プログラム１６ａを格納するメインメモリ１６と、予めタッチパッド１３から入力されたサイン等の個人認証情報を保持するサイン情報保持部１７１を含む記憶部１７とから構成されている。

【００２６】

図３は本発明の第１の実施例による携帯端末装置１の電子マネー機能の利用許可動作を示すフローチャートであり、図４は本発明の第１の実施例による携帯端末装置１での個人認証情報の登録動作を示すフローチャートである。これら図１～図４を参照して本発明の第１の実施例による決済動作について説明する。尚、図３及び図４に示す処理動作はＣＰＵ１４が制御プログラム１６ａを実行して携帯端末装置１内の各部を制御することでも実現可能である。

【００２７】

図３を用いて、本実施例による電子マネー機能使用時の動作について説明する。まず、支払い金額をタッチパッド１３もしくはテンキー（図１参照）によって携帯端末装置１に入力する（図３ステップＳ１）。

【００２８】

次に、携帯端末装置１ではタッチパッド１３上でサインを入力し（図３ステップＳ２）、入力されたサインの情報とサイン情報保持部１７１の認証用データとを比較し、一致しているかどうかを確認する（図３ステップＳ３）。それらのデータが一致していなければ、上記のステップＳ２の処理に戻り、再度、サインの入力から行う。

【００２９】

携帯端末装置１では、それらのデータが一致していれば、電子マネー機能の使用を許可し、携帯端末装置１をリーダ／ライタ２に近付けて決済サーバ３との間で決済を行う（図３ステップＳ４）。また、携帯端末装置１では、ステップＳ３の処理において認証を３回連続で失敗した場合（図３ステップＳ５）、他人が電子マネー機能を不正使用していると判断してエラー終了とする。

【００３０】

続いて、図４を用いて携帯端末装置１におけるサイン登録時の動作について説明する。まず、携帯端末装置１では、サイン入力画面で使用者がタッチパッド１３を用いてサインを入力すると、その時のサインの筆記速度、筆圧、筆順等の情報がサイン情報保持部１７１に記録される（図４ステップＳ１１～Ｓ１３）。この記録された情報が上記で説明した電子マネー機能の使用時の認証用データとなる。

【００３１】

携帯端末装置１では、認証データの精度を高めるため、上記と同様のデータの記録を３回行った後（図４ステップＳ１４）、登録を完了する。また、携帯端末装置１では、３回入力したデータに差分が大きい場合、そのデータを無効とし、もう一度サインの入力を行う（図４ステップＳ１２）。

【００３２】

このように、本実施例では、電子マネー機能の使用時に、サイン入力による本人認証を行って電子マネー機能の使用許可の判断を行うので、他人による電子マネー機能の不正使用を防ぐことができ、電子マネー機能の安全性を高めることができる。

【００３３】

また、本実施例では、携帯端末装置全体の機能にロックをかけるのではなく、電子マネー機能を使用する前に必ず認証を必要としているので、ロックがかかっていない時に電子マネー機能が使われてしまう機会を少なくすることができる。

【００３４】
さらに、本実施例では、指紋認証方式等と比べて、使用するデバイスに汎用性があるので、タッチパッド１３を文字入力手段等の他の目的にも使用することができ、実装コストを削減することができる。
【００３５】
さらにまた、本実施例では、電子マネー支払い時に、自端末装置に入力された支払い金額を確認してからサインを行うことができるので、間違った金額を支払ってしまうという間違いをなくすことができる。
【実施例２】
【００３６】
図５は本発明の第２の実施例による携帯端末装置の個人情報の利用許可動作を示すフローチャートである。本発明の第２の実施例による携帯端末装置は、図２に示す本発明の第１の実施例による携帯端末装置１と同様の構成となっている。これら図２及び図５を参照して本発明の第２の実施例による携帯端末装置１の個人情報の利用許可動作について説明する。尚、図５に示すに示す処理動作はＣＰＵ１４が制御プログラム１６ａを実行して携帯端末装置１内の各部を制御することでも実現可能である。
【００３７】
本発明の第２の実施例では、電子マネー機能使用時ではなく、ＰＩＭ（Ｐｅｒｓｏｎａｌ　Ｉｎｆｏｒｍａｔｉｏｎ　Ｍａｎａｇｅｒ）情報（携帯端末装置１内の記憶部１７に記憶された電話帳、スケジューラ、メモ等の情報）（個人情報）にアクセスする時に、その個人情報の使用を許可するかどうかの認証にサイン認証を用いている。その動作例を図５に示すが、図５において、図３の電子マネー機能使用時の認証動作との差分はステップＳ２３においてＰＩＭ情報にアクセスすることであり、サイン認証そのものの動作は、上記の本発明の第１の実施例によるサイン認証との違いはない。
【００３８】
すなわち、携帯端末装置１ではタッチパッド１３上でサインを入力し（図４ステップＳ２１）、入力されたサインの情報とサイン情報保持部１７１の認証用データとを比較し、一致しているかどうかを確認する（図４ステップＳ２２）。それらのデータが一致していなければ、上記のステップＳ２１の処理に戻り、再度、サインの入力から行う。
【００３９】
携帯端末装置１では、それらのデータが一致していれば、ＰＩＭ情報へのアクセスを許可する（図４ステップＳ２３）。また、携帯端末装置１では、ステップＳ２２の処理において認証を３回連続で失敗した場合（図４ステップＳ２４）、他人が不正使用していると判断してエラー終了とする。
【実施例３】
【００４０】
図６は本発明の第３の実施例による携帯端末装置の電子マネー機能の利用許可動作を示すフローチャートである。本発明の第３の実施例による携帯端末装置は、図２に示す本発明の第１の実施例による携帯端末装置１と同様の構成となっている。これら図２及び図６を参照して本発明の第３の実施例による携帯端末装置１の個人情報の利用許可動作について説明する。尚、図６に示すに示す処理動作はＣＰＵ１４が制御プログラム１６ａを実行して携帯端末装置１内の各部を制御することでも実現可能である。
【００４１】
まず、非接触ＩＣ１２をリーダ／ライタ２に近付けることによって、携帯端末装置１における電子マネー機能の使用が開始される（図６ステップＳ３１）。非接触ＩＣ１２とリーダ／ライタ２との間の認証が完了すると、支払金額が表示装置１１上に表示され（図６ステップＳ３２）、その金額に問題がなければ（図６ステップＳ３３）、タッチパッド１３上でサインを入力する（図６ステップＳ３４）。
【００４２】
携帯端末装置１は入力されたサインの情報とサイン情報保持部１７１の認証用データと

を比較し、一致しているかどうかを確認する（図６ステップＳ３５）。それらのデータが一致していなければ、上記のステップＳ３４の処理に戻り、再度、サインの入力を行う。

【００４３】

携帯端末装置１では、それらのデータが一致していれば、決済が完了する。また、携帯端末装置１では、ステップＳ３５の処理において認証を３回連続で失敗した場合（図６ステップＳ３６）、他人が電子マネー機能を不正使用していると判断してエラー終了とする。

【産業上の利用可能性】

【００４４】

本発明は、携帯端末装置上に搭載された電子マネー機能や、携帯端末装置上に記憶された個人情報の使用時等、携帯端末装置１において高いセキュリティを確保する必要性がある機能の使用許可の判断に適用することができる。

【図面の簡単な説明】

【００４５】

【図１】本発明の第１の実施例による携帯端末装置を含む決済システムの構成を示すブロック図である。

【図２】図１の携帯端末装置の構成例を示すブロック図である。

【図３】本発明の第１の実施例による携帯端末装置の電子マネー機能の利用許可動作を示すフローチャートである。

【図４】本発明の第１の実施例による携帯端末装置での個人認証情報の登録動作を示すフローチャートである。

【図５】本発明の第２の実施例による携帯端末装置の個人情報の利用許可動作を示すフローチャートである。

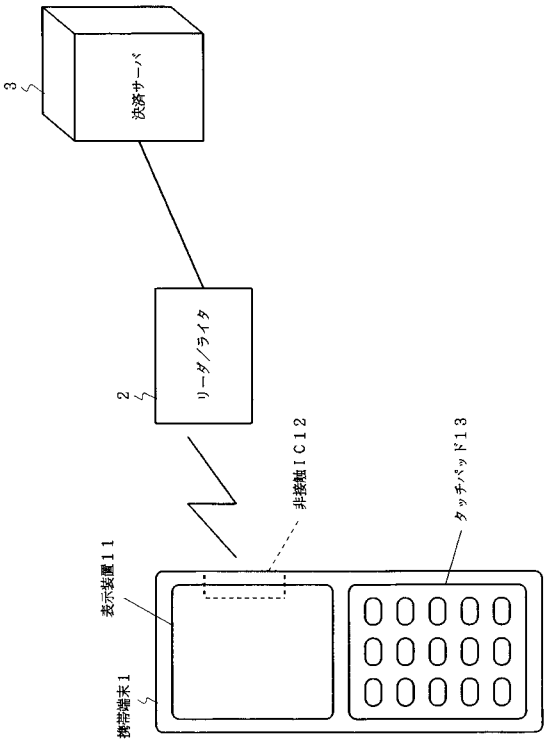
【図６】本発明の第３の実施例による携帯端末装置の電子マネー機能の利用許可動作を示すフローチャートである。

【符号の説明】

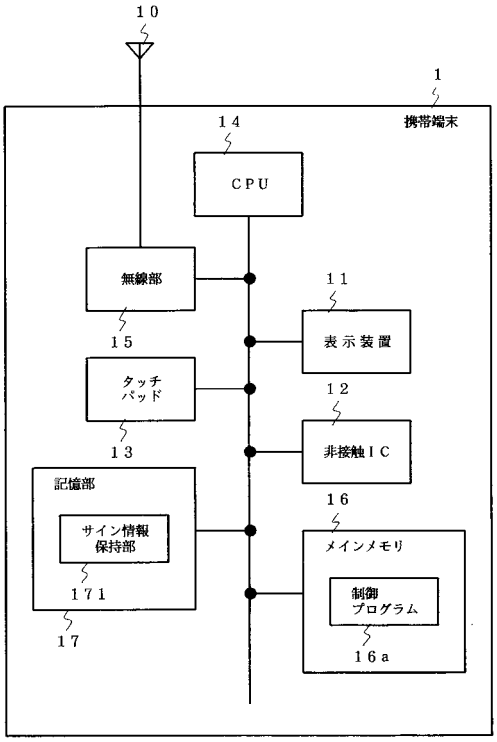
【００４６】

１　携帯端末装置
２　リーダ／ライタ
３　決済サーバ
１０　アンテナ
１１　表示装置
１２　非接触ＩＣ
１３　タッチパッド
１４　ＣＰＵ
１５　無線部
１６　メインメモリ
１６ａ　制御プログラム
１７　記憶部
１７１　サイン情報保持部

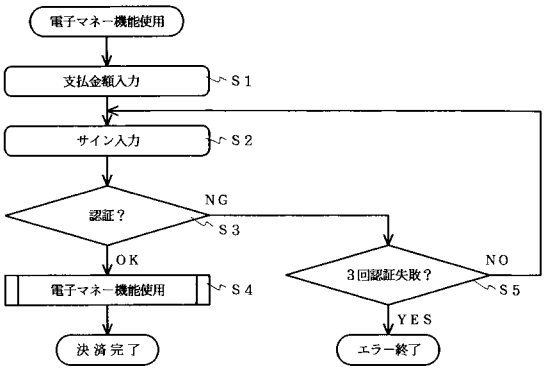
【図１】


3
決済サーバ
2
リーダ／ライタ
非接触ＩＣ12
タッチパッド13
表示装置11
携帯端末1

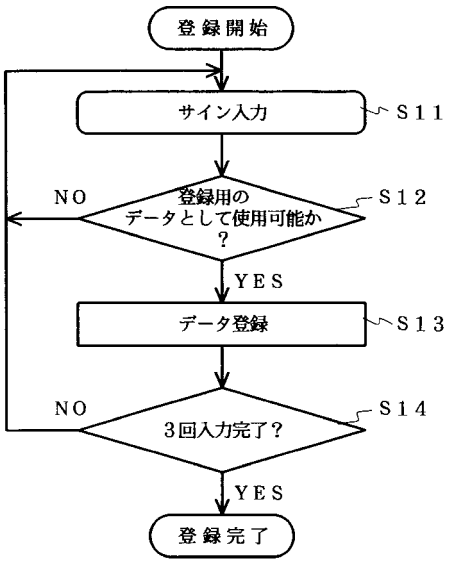
【図２】


10
1
携帯端末
14
CPU
無線部
15
11
表示装置
タッチ
パッド
13
12
非接触ＩＣ
記憶部
サイン情報
保持部
171
16
メインメモリ
制御
プログラム
16a
17

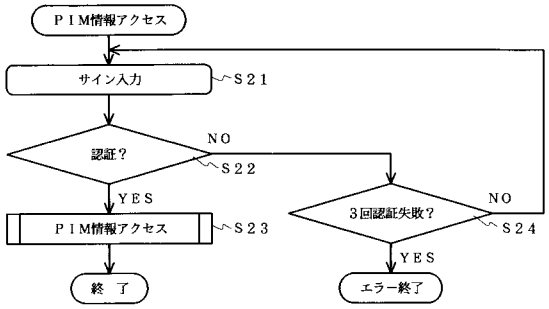
【図３】


電子マネー機能使用
支払金額入力
S1
サイン入力
S2
認証？
NG
S3
OK
電子マネー機能使用
S4
決済完了
3回認証失敗？
NO
S5
YES
エラー終了

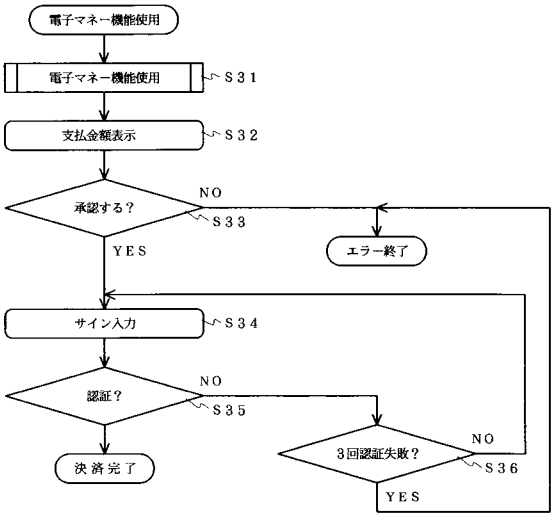
【図４】


登録開始
サイン入力
S11
NO
登録用の
データとして使用可能か
？
S12
YES
データ登録
S13
NO
3回入力完了？
S14
YES
登録完了

【図５】


ＰＩＭ情報アクセス
サイン入力
Ｓ２１
認証？
ＮＯ
Ｓ２２
ＹＥＳ
３回認証失敗？
ＮＯ
Ｓ２４
ＹＥＳ
ＰＩＭ情報アクセス
Ｓ２３
終　了
エラー終了

【図６】


電子マネー機能使用
電子マネー機能使用
Ｓ３１
支払金額表示
Ｓ３２
承認する？
ＮＯ
Ｓ３３
ＹＥＳ
エラー終了
サイン入力
Ｓ３４
認証？
ＮＯ
Ｓ３５
ＹＥＳ
３回認証失敗？
ＮＯ
Ｓ３６
ＹＥＳ
決済完了

フロントページの続き

(51)Int.Cl.		F I		テーマコード（参考）
H04M 1/725	*(2006.01)*	H04M	1/66	
		H04M	1/725	