(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2010-239229
(P2010-239229A)
(43)公開日　平成22年10月21日(2010.10.21)

(51)Int.Cl.			F I			テーマコード（参考）
H04M	1/67	(2006.01)	H04M	1/67		5K027
H04M	1/00	(2006.01)	H04M	1/00	U	

審査請求 未請求　請求項の数 6　OL　（全 10 頁）

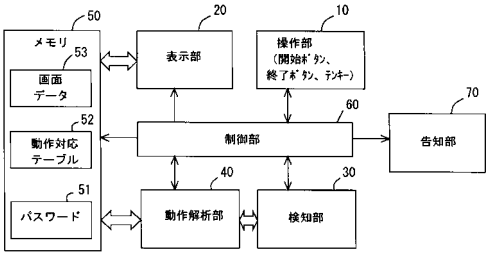
(21)出願番号　特願2009-82458(P2009-82458)
(22)出願日　平成21年3月30日(2009.3.30)

(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　100084250
弁理士　丸山　隆夫
(72)発明者　遠藤　一夫
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)　5K027 AA11　BB02　BB09　EE11　FF22
HH24　HH26

(54)【発明の名称】携帯電子機器、携帯電子機器の制御方法、及びプログラム

(57)【要約】
【課題】閉状態でも認証パスワードの入力を可能とし、利便性を向上させた携帯電子機器、携帯電子機器の制御方法、及びプログラムを提供することにある。
【解決手段】携帯電子機器本体に与えられた物理的な動作を検知する検知手段と、検知手段による検知結果を解析して得られた数値と予め入力したパスワードとしての数値とを照合することによりパスワードを認証する認証手段と、を備えた。
【選択図】図１



【特許請求の範囲】
【請求項１】
携帯電子機器本体に与えられた物理的な動作を検知する検知手段と、該検知手段による検知結果を解析して得られた数値と予め入力したパスワードとしての数値とを照合することによりパスワードを認証する認証手段と、を備えたことを特徴とする携帯電子機器。
【請求項２】
前記携帯電子機器本体の物理的な動作を表示する表示手段を備えたことを特徴とする請求項１に記載の携帯電子機器。
【請求項３】
前記パスワードの認証結果を、操作者に告知する告知手段を備えたことを特徴とする請求項２に記載の携帯電子機器。
【請求項４】
筐体の外部に通話の開始ボタン及び終了ボタンを備えたことを特徴とする請求項１に記載の携帯電子機器。
【請求項５】
携帯電子機器本体に与えられた物理的な動作を検知し、検知結果を解析して得られた数値と予め入力したパスワードとしての数値とを照合することによりパスワードを認証することを特徴とする携帯電子機器の制御方法。
【請求項６】
コンピュータに、
検知手段が、携帯電子機器本体に与えられた物理的な動作を検知する手順、
認証手段が、該検知手段による検知結果を解析して得られた数値と予め入力したパスワードとしての数値とを照合することによりパスワードを認証する手順、
を実行させることを特徴とするプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、携帯電子機器、携帯電子機器の制御方法、及びプログラムに関する。
【背景技術】
【０００２】
携帯電話やＰＤＡ（Ｐｅｒｓｏｎａｌ　Ｄｉｇｉｔａｌ　Ａｓｓｉｓｔａｎｔ）等の携帯電子機器は、一般に手のひらサイズのため、紛失したり、盗難にあったりするおそれがある。携帯電子機器の紛失や盗難時に携帯通信端末内のデータ（個人データ、業務データ）の流出や悪用を防ぐために、４桁程度の数値のパスワードにより携帯通信端末のキー操作や特定の機能の利用に制限をかける認証方式が用いられている。
【０００３】
携帯通信端末に認証方式を用いた技術が特許文献１～９に開示されている。
特許文献１に記載の発明は、可搬型情報処理装置及びシステムクロックプログラムに関する発明である。具体的には、可搬型情報処理装置の移動距離の累積値を求める距離計測部と、この可搬型情報処理装置で動作可能な情報処理機のうちの少なくとも一部の情報処理を使用不能状態に変更するロックを行うロック制御部とを備えたものである。
【０００４】
特許文献１に記載の発明によれば、情報盗用の危険性を低減させることができるとしている。
【０００５】
特許文献２に記載の発明は、情報処理システム及び情報入力端末に関する発明である。具体的には、情報コードを読み取る読取手段と、読み取ったデータを出力する情報出力手段とを備えた情報入力端末と、表示手段と、情報入力端末が出力したデータを入力する情報入力手段とを備えたものである。同発明は、入力されたデータに対して所定の処理を実行するように構成された情報処理装置とから構成され、情報処理装置は、入力されたデー

タの処理方法を選択する選択項目を表示手段に表示するように構成されている。同発明は、これと共に、情報入力端末は、表示手段に表示された選択項目を選択する選択情報を情報出力手段に出力するように構成されている。同発明は、情報処理装置は、情報入力手段から入力された選択情報に基づいてデータ処理を実行する情報処理手段を備えるように構成されている。

【０００６】

特許文献２に記載の発明によれば、情報入力端末によって、情報処理装置の表示手段に表示された選択項目を選択することが可能な構成となるので、情報入力端末の読取操作と情報処理装置の操作を交互に繰り返す必要があるときでも、情報入力端末を置いたり、持ったりする作業をなくすことができるとしている。

【０００７】

特許文献３に記載の発明は、携帯型電子装置に関する発明である。具体的には、少なくとも二つの筐体と、連結手段と、第１の操作手段と、第２の操作手段と、機能ロック手段と、第１のロック解除モード、配置状態が少なくとも第１の配置状態であるときには、第１のロック解除モードに動作モードを制御する動作モード制御手段とを有する。

【０００８】

特許文献３に記載の発明によれば、セキュリティ機能を維持しつつ、電子財布機能等の所定機能のロック解除を簡単かつスピーディに行うことが可能になっているとしている。

【０００９】

特許文献４に記載の発明は、携帯端末に関する発明である。具体的には、筐体と、加速度センサーと、加速度情報検出部と、加速度個人認証情報登録部と、個人認証情報記憶部と、個人認証情報認証部とを具備したものである。

【００１０】

特許文献４に記載の発明によれば、認証情報の組み合わせを無限にでき、加速度センサーで携帯電話の動きを検出するため、筐体を開くことなく、携帯を持って動かすことで認証情報を検出することができるとしている。

【００１１】

特許文献５に記載の発明は、携帯表示装置に関する発明である。具体的には、加速度計測手段と、外部情報認識手段と、移動量演算手段と、移動量演算手段により算出された３次元的変位量に基づいて表示手段への表示内容を制御する表示制御手段と、を備えたものである。

【００１２】

特許文献５に記載の発明によれば、加速度の検出だけでは筐体移動による表示制御が正確にできない状況でも、筐体移動により表示内容の操作を正確に行うことができ、インタフェースを意識させることのない自然な操作感で表示内容の操作ができるとしている。

【００１３】

特許文献６に記載の発明は、認証装置に関する発明である。具体的には、被認証者の顔を撮像する撮像手段と、撮像方向判定手段と、斜め下方向から撮像していないと撮像方向判定手段が判定した場合に、当該被認証者は本人ではないと判断する判断手段とを備える。

【００１４】

特許文献６に記載の発明によれば、撮像方向を本人なりすましが行われているか否かを判断する基準として撮像方向を用いることができ、本人なりすましに対する耐性を高めることができるとしている。

【００１５】

特許文献７に記載の発明は、移動体端末装置に関する発明である。具体的には、接触対象物との接触の有無を示す接触情報を取得する接触情報取得手段と、接触対象物との接触位置から装置本体の移動情報を取得する移動情報取得手段と、接触情報及び移動情報に基づいて入力情報を認識する認識手段と、を具備する。

【００１６】

特許文献７に記載の発明によれば、タッチスクリーン等のデバイスを必要としないため、移動体端末装置を用いた手書き動作により手軽に情報を入力することが可能となるとしている。

【００１７】

特許文献８に記載の発明は、携帯電話機に関する発明である。具体的には、加速度センサ部と、基準用認証データを記憶する記憶部と、文字列データを含む認証データと、基準用認証データとを照合する認証部と、セキュリティロックを解除する制御部と、を備える。

【００１８】

特許文献８に記載の発明によれば、加速度センサを用いることにより、携帯性を損なうことなく簡単な操作で認証を行うことができる。同発明は、文字列データによる認証に加えて筆跡データによる筆跡鑑定の二重ロックを行うので、より高精度な本人照合を行うとしている。

【００１９】

特許文献９に記載の発明は、加速度計に基づいてポータブル・デバイスを操作する方法および装置に関する発明である。具体的には、ポータブル・デバイスに取り付けられた加速度計を使用してポータブル・デバイスの移動を検出するステップと、１つまたは複数の所定のユーザ構成可能なアクションを実行するために機械実行可能コードを実行するステップとを含む。

【００２０】

特許文献９に記載の発明によれば、携帯性を損なうことなく簡単な操作で高精度な認証を可能とする携帯電話機を提供することができるとしている。

【００２１】

また、携帯通信端末の中には折り畳み式やスライド式といった１台で複数の形態を持つものがあるが、これら携帯通信端末においてはテンキーが隠れた、いわゆる閉状態がある。閉状態においても通話やメールの閲覧など特定の機能の利用を可能とし、ユーザの利便性の向上が図られている。

【先行技術文献】

【特許文献】

【００２２】

【特許文献１】再特ＷＯ２００２１０３４９７号公報
【特許文献２】特開２００６－２０１９４７号公報
【特許文献３】特開２００６－２２９７３０号公報
【特許文献４】特開２００７－１１６３１８号公報
【特許文献５】特開２００７－１２１４８９号公報
【特許文献６】特開２００７－２４９５８６号公報
【特許文献７】特開２００８－０７０９２０号公報
【特許文献８】特開２００８－０７８７６３号公報
【特許文献９】特表２００７－５２５７７５号公報

【発明の概要】

【発明が解決しようとする課題】

【００２３】

ところが、折りたたみ式携帯通信端末においては、パスワードにより操作に制限がかかった状態では、パスワードを入力するテンキーが蓋部で隠れているため、操作制限を解除できず、閉状態での機能を利用できないという課題がある。

また、上述した特許文献１～９に記載の発明にはパスワードの入力が可能でないものがあり、いずれも利便性に改善の余地が見られる。

【００２４】

そこで、本発明の目的は、閉状態でも認証パスワードの入力を可能とし、利便性を向上させた携帯電子機器、携帯電子機器の制御方法、及び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】
【００２５】
本発明の第１の装置は、携帯電子機器本体に与えられた物理的な動作を検知する検知手段と、検知手段による検知結果を解析して得られた数値と予め入力したパスワードとしての数値とを照合することによりパスワードを認証する認証手段と、を備えたことを特徴とする。
【００２６】
本発明の第１の方法は、携帯電子機器本体に与えられた物理的な動作を検知し、検知結果を解析して得られた数値と予め入力したパスワードとしての数値とを照合することによりパスワードを認証することを特徴とする。
【００２７】
本発明の第１のプログラムは、コンピュータに、検知手段が、携帯電子機器本体に与えられた物理的な動作を検知する手順、認証手段が、検知手段による検知結果を解析して得られた数値と予め入力したパスワードとしての数値とを照合することによりパスワードを認証する手順、を実行させることを特徴とする。
【発明の効果】
【００２８】
本発明によれば、閉状態でも認証パスワードの入力を可能とし、利便性を向上させた携帯電子機器、携帯電子機器の制御方法、及びプログラムの提供を実現することができる。
【図面の簡単な説明】
【００２９】
【図１】本発明に係る携帯電子機器の一実施の形態を示すブロック図である。
【図２】図１に示した携帯電子機器においてパスワードを１桁分、入力する場合の動作の一例を示す図である。
【図３】図１に示した携帯電子機器におけるパスワード入力のフローチャートの一例である。
【図４】図１に示した携帯電子機器の画面データの一例である。
【発明を実施するための形態】
【００３０】
＜本発明の特徴＞
本発明は、複数の形態を持つ携帯電子機器においてテンキーが無い形態においても認証パスワードの入力を可能とすることを特徴としている。
【００３１】
＜構　成＞
図１は、本発明に係る携帯電子機器の一実施の形態を示すブロック図である。
本実施形態では、携帯電子機器が携帯通信端末の場合について述べる。
図１に示す携帯電子機器としての携帯通信端末は、操作部１０、表示手段としての表示部２０、検知部３０、動作解析部４０、メモリ５０、認証手段としての制御部６０、及び告知手段としての告知部７０で構成されている。
【００３２】
図１に示す携帯通信端末は、「０」から「９」までの１０個の数値に、携帯通信端末の傾斜、回転、振動、衝撃等の物理的な動作が割り当てられている。表示部２０に数値と、携帯通信端末の物理的な動作との関係を表示することにより、操作者にパスワードの入力を促す。
検知部３０は、操作者が携帯通信端末を傾けたり、振ったり、衝撃を与えたりする物理的な動作を検出するものであり、例えば加速度センサが用いられる。
検知部３０で検出した動作は動作解析部４０で解析し、動作ごとに割り当てられた数値情報に変換する。
制御部６０は、一連の操作において各部の制御を行うと共に、動作解析部４０で得られた数値と、予め操作者によってメモリ５０に保存されている数値（パスワード）５１と一

致しているか否かを判断する。これによりテンキー無しでの認証パスワード入力を実現することができる。

本発明に係る携帯通信端末を動かすことによって認証パスワード入力が可能となる。

【００３３】

図１を参照すると、数値のパスワードを入力するためのテンキーが操作できない形態ではあるが、限定された最低限の数のキーやタッチセンサといった操作部１０により、携帯通信端末の操作が可能となっている。

【００３４】

ここで、「最低限の数のキー」とは、例えば、電話の着信があったときに通話を始める（いわゆる電話をとる）通話キーや、通話を終了するキーのことを意味している。「０」～「９」のボタン、「数値のパスワードを入力するためのテンキー」は、例えば折りたたみ式の携帯電話で、折りたたんだ形態で内側に入ってしまうために操作できない状態にあることを想定している。

【００３５】

また、「タッチセンサ」とは、静電式のキーで数字以外のキーが割り当ててあるものを想定した。液晶パネルにタッチセンサを設けたものもあり得るが、ポイントは、「数値のパスワードを入力するためのテンキー」が無い状態であることである。

【００３６】

表示部２０は、例えば、液晶表示装置（ＥＬ（Ｅｌｅｃｔｒｏ　Ｌｕｍｉｎｅｓｃｅｎｃｅ）もしくは、プラズマディスプレイでもよい。）からなる。表示部２０は、メモリ５０（例えば、ＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓ　Ｍｅｍｏｒｙ））に保存されている画面データ５３を表示する。ここで画面データ５３は、操作者にパスワードの入力を促す画面を持つ。

【００３７】

メモリ５０は、キー操作や特定の機能の利用に制限をかける、数値からなるパスワード情報５１と、携帯通信端末の動作と対応して割り振られている数字の対応テーブル５２、画面データ５３を保持する。

【００３８】

告知部７０は、例えば音声を発するブザーもしくは振動を発するバイブレータが挙げられる。

【００３９】

＜動作の説明＞

次に本実施形態の動作を図１、図２、及び図３を使用して説明する。

図２は、図１に示した携帯通信端末においてパスワードを１桁分、入力する場合の動作の一例を示す図である。図３は、図１に示した携帯通信端末におけるパスワード入力のフローチャートの一例である。

【００４０】

操作者は、例えば電話帳を参照するために操作部（図１の１０）を操作する（図３のＳ１）。ここで電話帳を参照するために認証パスワードによる操作制限がかかっている場合、パスワードを入力し、制限を解除する操作が必要となる（図３のＳ２）。

【００４１】

制御部（図１の６０）はメモリ(図１の５０)に保持してある画面データ（図１の５３）を表示部(図１の２０)に表示するように制御する（図３のＳ３）。

【００４２】

画面データの一例を示す（図２の５３）。矢印は携帯通信端末を動かす方向を示しており、動作に応じた数字が選択される。ここで、数字の「５」を選択する場合の動作を説明する。操作者は画面データの「５」が示されている方向へ端末を動かす。一方向の動作で指定可能であるが、例では携帯通信端末の姿勢を元に戻す動作としている（図２の１１）。検知部（図１の３０）は携帯通信端末の物理的な動作を検出する（図２の３１）（図３のＳ４）。

【００４３】
動作解析部（図１の４０）は、検知部（図１の３０）が検出した携帯通信端末の物理的な動作（図２の３１）を元に動作対応テーブル（図２の５２）より操作者が選択しようとした数字が何かを解析する（図３のＳ５）。ここでは「５」であったと判断し、メモリ（図１の５０）に保持する（図３のS６）。
【００４４】
パスワードの入力操作を桁数分実施し(図３のＳ７)、メモリ（図１の５０）に保存されているパスワード（図２の５１）としての数値と一致しているか否かを判定する(図３のＳ８)。
【００４５】
正しいパスワードが入力された場合は、操作制限を解除し、該当の機能が利用可能となる（図３のＳ１０）。
操作制限が解除されると、操作者は図示しない通話の開始ボタンを押すことにより通話が可能となり、通話が終了したときは図示しない通話の終了ボタンを押すことにより通話が終了する。
パスワードが誤りだった場合は、その旨を表示し、パスワードの入力待ちとなる（図３のＳ９）。
【００４６】
＜効果の説明＞
以上説明したように、本発明においては、以下に記載するような効果を奏する。
第１の効果はテンキーが無くてもパスワードの入力ができるので、パスワードの入力のためにテンキーが利用可能な端末形態に変形する必要が無く、操作性を損なわずにパスワードによる操作制限のついた機能を利用できることである。
【００４７】
第２の効果はパスワードによる認証方式が利用できるので、例えば、顔認証や同じ加速度センサを用いて個人の癖を鍵にする認証方式の様に、状況によって認証されないケースを避けることができることである。
ここで、「個人の癖を鍵にする」とは「操作者の筆跡を識別可能な筆跡情報にする」ことを意味する。
【００４８】
＜プログラム及び記憶媒体＞
以上で説明した本発明にかかる携帯電子機器は、コンピュータで処理を実行させるプログラムによって実現されている。コンピュータとしては、例えばマイクロプロセッサのような汎用的なものが挙げられるが、本発明はこれに限定されるものではない。よって、一例として、プログラムにより本発明を実現する場合の説明を以下で行う。
【００４９】
コンピュータに、
（１）検知手段が、携帯電子機器本体に与えられた物理的な動作を検知する手順、
（２）認証手段が、検知手段による検知結果を解析して得られた数値と予め入力したパスワードとしての数値とを照合することによりパスワードを認証する手順、
を実行させるプログラムが挙げられる。
【００５０】
これにより、プログラムが実行可能なコンピュータ環境さえあれば、どこにおいても本発明にかかる携帯通信端末を実現することができる。
このようなプログラムは、コンピュータに読み取り可能な記憶媒体に記憶されていてもよい。
ここで、記憶媒体としては、例えば、ＣＤ－ＲＯＭ（Ｃｏｍｐａｃｔ　Ｄｉｓｃ－ＲＯＭ）、フレキシブルディスク（ＦＤ）、ＣＤ－Ｒ（ＣＤ－Ｒｅｃｏｒｄａｂｌｅ）などの記憶媒体が挙げられる。また、フラッシュメモリ、ＲＡＭ、ＲＯＭ、ＦｅＲＡＭ（強誘電体メモリ）等の半導体メモリやＨＤＤ（Ｈａｒｄ　Ｄｉｓｃ　Ｄｒｉｖｅ）が挙げられる

。

【００５１】

なお、上述した実施の形態は、本発明の好適な実施の形態の一例を示すものであり、本発明はそれに限定されることなく、その要旨を逸脱しない範囲内において、種々変形実施が可能である。また、上述した実施の形態では、携帯通信端末の場合で説明したが、これに限定されるものではない。

【００５２】

＜他の実施の形態＞

次に本発明の他の実施の形態を示す。

本発明の他の実施の形態は、パスワードの桁ごとに入力が認識されたことを操作者に表示、音およびバイブレータによる振動で知らせるものである。すなわち操作者が行った数字を選択する動作が、動作対応テーブル(図１の５２)に存在した事を知らせる(図３のＳ５)。これにより、操作者の動かし方が正確でなく、動作が認識できなかった事に操作者自身が気づかない事を防ぐ。

【００５３】

本発明の他の実施の形態は、画面データ（図１の５３）に端末を動かした方向を判り易くする為にマークを表示するものである。

ここで、「マークを表示する」とは、図４の「☆：星マーク」を意味する。

【００５４】

図４は、図１に示した携帯通信端末の画面データの一例である。

図４を参照すると、動作の開始時を基本の端末の姿勢とし、画面の中央に星マークを表示する（図４の５３）。操作者が携帯通信端末を動かした方向に合わせて（図４の１１）星マークを移動して表示する（図４の５４）。これにより、操作者が動かす方向を導くことができ、入力の確実性が増す。

【００５５】

本発明の他の実施の形態は、動作対応テーブル（図１の５２）が認証の度に変わる。すなわち、画面データ(図１の５３)で示される数字と携帯通信端末の動作方向とが都度変わる。これにより、操作者以外の人に認証操作を盗み見されてパスワードが漏洩するのを防ぐことができる。

【００５６】

本発明の他の実施の形態は、携帯通信端末の機能ばかりではなく、例えばブラウザを利用したネットワークサービス中のパスワード入力において本発明のパスワードの入力方式を利用する。

ここでは認証を行うのはネットワークサービス側のため、パスワードの入力（図３のＳ７）で必要な桁数、パスワードを入力後、ネットワークに対して入力したパスワードを送出する。これにより、パスワード入力のためにテンキーを利用可能な端末形態に変える必要が無くなる。すなわち、ネットワーク接続中（例えば蓋を開けた状態）にテンキーを押す代わりに携帯通信端末を振ればよいことを意味する。

【００５７】

本発明の他の実施の形態は加速度センサではなくカメラを用いる。携帯通信端末の動作をカメラに映った映像の変化で検出する。これにより、加速度センサを搭載していない携帯通信端末でも本発明の認証方式を利用可能となる。

ここで、「カメラに映った」とはシャッターを押す前のプレビュー状態を意味する（実際には表示部に必ずしも映像を映す必要はない。）。例えば、携帯通信端末に内蔵されたカメラで人の顔を撮影したとする。次に携帯通信端末を左に動かすと、人の顔は映像上、右に動く。これが「カメラに写った映像の変化」であり、最初に写った映像であり、画像検出により、ある特定のポイントを決め、携帯通信端末の動きによりその特定のポイントが動いたことを検出することで、携帯通信端末自体の動作（方向）を検出する。

【００５８】

また、暗い環境下ではカメラが映像の変化を認識できないため、パスワード入力時はラ

イトを点灯することで、映像の変化を検出可能とする。

【００５９】

本発明の他の実施の形態はテンキーが操作可能な開状態でも本認証方式が可能である。情報通信端末の形態に拠らず、統一した認証操作が可能である。

【００６０】

本発明の他の実施形態は、パスワードの入力を１桁だけ取り消したい場合の操作を持つ。例えば、携帯通信端末をある一定時間内に、２度振る。これにより、クリアキー操作無しに入力をやり直すことが可能である。

【００６１】

本発明の他の実施の形態は、パスワードの入力を最初からやり直したい場合の操作を持つ。例えば、携帯通信端末をある一定時間内に、２度大きく振る。これにより、クリアキーの長押しや中断キーの操作無しに入力をやり直すことが可能である。

【００６２】

本発明の他の実施の形態は、パスワードの入力を確定する操作を持つ。例えば、端末をある一定時間内に、２回回す。これにより、キー操作なしに確定動作の実行が可能である。

【００６３】

さらに、本発明の他の実施の形態は、携帯端末を振る他、例えば、プッシュボタンを一つ設けておくか、カバーを指先で叩くことにより、モールス信号で入力するように構成してもよい（この場合、数字の他、アルファベット、カタカナ入力も可能である。）。あるいは蓋自体を数ｍｍ程度開いた状態を保持できるようにしておき、電鍵(いわゆるトンツーの入力手段である。)のように動作させてもよい。

例えばパスワードを「１２３４」とすると、

「・－－－－　・・－－－　・・・－－　・・・・－」となる。

尚、モールス通信の場合、１を・－（Ａ）、９を－・（Ｎ）、０を－－－（Ｏ）と略す場合がある。その場合には、「１２３４」は、

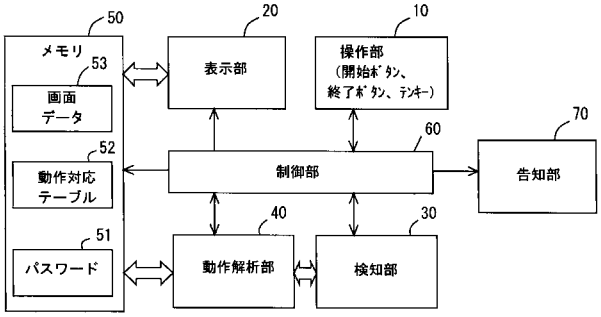
「・－　・・－－－　・・・－－　・・・・－」となる。

【符号の説明】

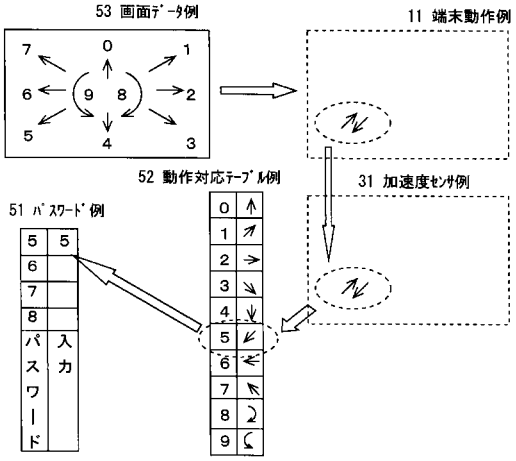
【００６４】

１０　操作部
２０　表示部
３０　検知部
４０　動作解析部
５０　メモリ
５１　パスワード
５２　動作対応テーブル
５３　画面データ
６０　制御部
７０　告知部

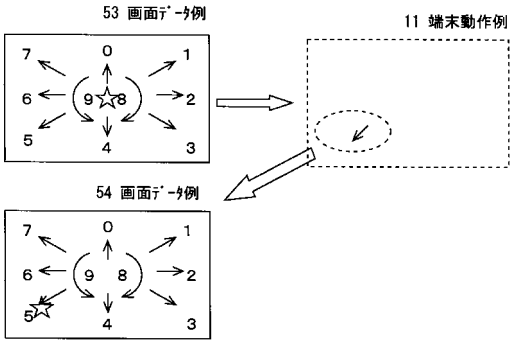
【図１】


メモリ
50
画面データ
53
動作対応テーブル
52
パスワード
51
表示部
20
操作部（開始ﾎﾞﾀﾝ、終了ﾎﾞﾀﾝ、ﾃﾝｷｰ）
10
制御部
60
告知部
70
動作解析部
40
検知部
30

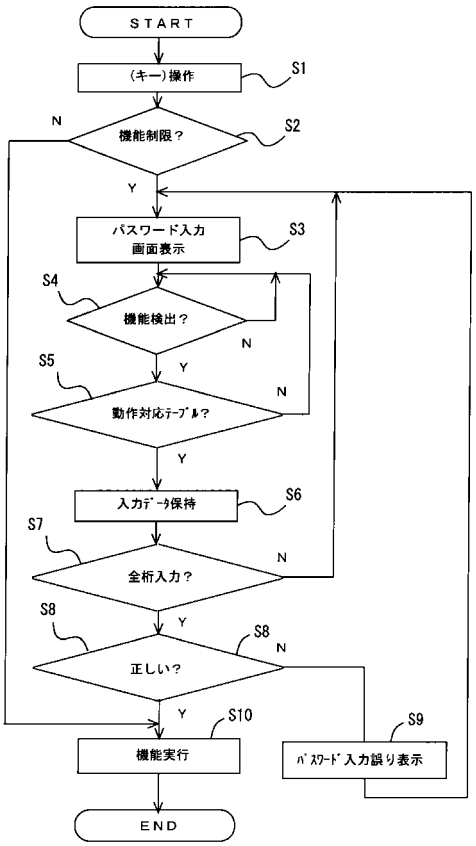
【図２】


53 画面ﾃﾞｰﾀ例
11 端末動作例
52 動作対応ﾃｰﾌﾞﾙ例
31 加速度ｾﾝｻ例
51 ﾊﾟｽﾜｰﾄﾞ例
パスワード
入力

【図３】


53 画面ﾃﾞｰﾀ例
11 端末動作例
54 画面ﾃﾞｰﾀ例

【図４】


START
(キー)操作
S1
機能制限？
S2
N
Y
パスワード入力画面表示
S3
S4
機能検出？
N
Y
S5
動作対応ﾃｰﾌﾞﾙ？
N
Y
入力ﾃﾞｰﾀ保持
S6
S7
全桁入力？
N
Y
S8
正しい？
S8
N
Y
S10
機能実行
S9
ﾊﾟｽﾜｰﾄﾞ入力誤り表示
END