

添付公開書類:

— 国際調査報告 (条約第 21 条(3))

明 細 書

発明の名称：

携帯端末及びそれを用いたキーレスエントリシステムまたはセキュリティシステム及びその認証方法

技術分野

[0001] 本発明は個人認証機能と所定の通信機能を備えた携帯端末によるキーレスエントリシステムまたはセキュリティシステムに適用されるものである。

背景技術

[0002] 近年、個人認証機能を備えたスマートフォン等の携帯端末が広く普及している。特に指紋認証や指静脈認証、あるいは眼の虹彩の特徴点を検出することで個人認証を行う虹彩認証などの生体認証による個人認証機能を備えた携帯端末が普及している。この生体認証機能と携帯端末の通信機能を利用して自宅玄関ドア等の自動開錠／施錠を実現するキーレスエントリシステムや、銀行の現金自動預け払い機（以下ＡＴＭと略す。）用セキュリティシステム等が実用化されつつある。

[0003] 本技術分野の背景技術として、例えば、特開２００３－２５３９４０号公報（特許文献１）がある。特許文献１では、携帯端末で取得した生体認証情報を所定の鍵装置に送信し、鍵装置内で個人認証を行いその結果に基づいて解錠／施錠を行うことでキーレスエントリを実現する例が開示されている。

先行技術文献

特許文献

[0004] 特許文献１：特開２００３－２５３９４０号公報

発明の概要

発明が解決しようとする課題

[0005] 特許文献１に開示されている従来のキーレスエントリシステムやセキュリティシステムでは、個々のセキュリティ解除操作を行う度に、その直前に所

定の生体認証操作を行う必要があり、例えば前記ＡＴＭのセキュリティシステムの場合などでは、使用者が携帯端末をＡＴＭ端末に近接させた不自然な体勢で生体認証作業を行う必要があるなど使用者の利便性の面で大きな課題がある。

課題を解決するための手段

[0006] 上記課題を解決するため、本発明は、その一例を挙げるならば、個人認証装置を備えた携帯端末であって、使用者が携帯端末を手に保持し続けている状態を検知する保持検知装置を備え、使用者が個人認証装置により認証操作を行ったのち保持検知装置の検知結果により携帯端末を手に保持している状態を検知し続けている間は認証操作の認証結果を保持し続ける機能を備えた。

発明の効果

[0007] 本発明によれば、高いセキュリティ性能と共に、使用者にとって高い利便性を備えたキーレスエントリシステムまたはセキュリティシステムを実現することができる。

図面の簡単な説明

[0008] [図1]実施例１における携帯端末とそれを保持する使用者を示した概略図である。

[図2]実施例１における携帯端末の操作を説明するための概略図である。

[図3]実施例１における携帯端末のブロック図である。

[図4]実施例１における処理フローチャートである。

[図5]実施例２における携帯端末の操作を説明するための第１の概略図である。

[図6]実施例２における携帯端末の操作状説明するための第２の概略図である。

[図7]実施例２における携帯端末のブロック図である。

[図8]実施例２における処理フローチャートである。

[図9]実施例３における携帯端末の操作を説明するための第１の概略図である。

。

[図10]実施例3における携帯端末の操作を説明するための第2の概略図である。

[図11]実施例3における携帯端末のブロック図である。

[図12]実施例3における処理フローチャートである。

[図13]実施例3における携帯端末の操作を説明するための第3の概略図である。

[図14]実施例3における携帯端末の操作を説明するための第4の概略図である。

[図15]実施例3における携帯端末の操作を説明するための第5の概略図である。

[図16]実施例3における携帯端末の操作を説明するための第6の概略図である。

[図17]実施例4における携帯端末のブロック図である。

[図18]実施例5におけるシステムのブロック図である。

発明を実施するための形態

[0009] 以下、図面を用いて本発明の実施例について説明する。

実施例 1

[0010] 図1は本実施例における携帯端末1とそれを保持する使用者10を示している。本実施例では携帯端末1として、例えばスマートフォンなどの携帯型通信端末装置を例に挙げて説明するが、当然これに限定されるものではなく、手首に巻く腕時計型の通信端末装置やタブレット型のパーソナルコンピュータなどでも構わない。

[0011] 本実施例における携帯端末1は、例えば指紋認証などの所定の生体認証装置を備えている。そして、例えば自宅やホテル等の玄関ドアあるいは自家用車やレンタカー等のフロントドア等のドアロック自動施錠／解錠機能、さらにはドアの自動開閉機能を備えたいわゆるキーレスエントリシステム、あるいは銀行ATM等に用いられる個人認証セキュリティシステム等を所定の相

互通信を通じて遠隔操作する機能を備える。なお相互通信方式としては、例えばBluetooth(登録商標)あるいはNFCなどで代表される近距離無線通信方式を用いるのが一般的であるが、本実施例はそれに限定されるものでない。

[0012] 図2は本実施例における携帯端末1の使用状態を示すため、使用者10の手元を拡大した概略図である。図2において、使用者10はその右手11で本実施例における携帯端末1を保持し、左手12の人差し指で携帯端末1の液晶画面に触れている状態を示している。

[0013] 本実施例における携帯端末1は、例えば液晶画面などで構成される情報表示画面2の全面またはその一部領域内の任意の位置に指を接触させると、接触させた指の指紋形状パターンから所定の指紋特徴点を検知して、使用者を識別し個人認証を行なう機能を備えている。

[0014] 前記のように情報表示画面2の全面またはその一部領域内の任意位置に接触させた手指の指紋形状パターンを検知するためには所定の指紋パターン検知センサ(以下、指紋センサと略す。)が必要であるが、この指紋センサとしては、例えば光センサを内蔵した液晶型表示パネル装置や超音波によって指紋パターンを3次的に検知する装置など公知の装置を含め、指紋の形状パターンを検知できるセンサであればどのようなセンサであっても構わない。

[0015] さらに本実施例における携帯端末1は、前記の指紋認証装置に加えて使用者10が例えば図2に示す例の如く携帯端末1を手元に保持している状態を検知する端末保持センサも備えている。この端末保持センサの具体例としては、例えば携帯端末1の側面に設けた圧力センサから使用者10が携帯端末1を握り締めている状態か否かを検知するセンサ装置や、携帯端末1内に設けた振動センサにより、人が手で物を保持する時に生じる生理的な微小振動を検知することで携帯端末1が保持状態か否かを検知するセンサ装置等公知の装置を含めどのようなセンサ装置であっても構わない。

[0016] 前記端末保持センサを用いて使用者10が携帯端末1を手元に保持し続け

ている状態か否かを検知できれば、例えば使用者 10 が指紋認証等により個人認証を行った後、携帯端末 1 を保持し続けている期間は個人認証結果を有効状態に保ち、保持を解除すなわち手に保持し続けている事を止めて、例えばポケットやカバンの中へ収納したりあるいは机上に放置したような場合は、自動的に個人認証結果が解除され無効にリセットされるような機能を持たせることが可能である。

[0017] このように、携帯端末 1 が保持継続状態か否かを検知することにより、個人認証結果の有効／無効を切替える機能を携帯端末 1 に備えさせることが出来れば、例えば使用者 10 がキーレスエントリ操作あるいはセキュリティ解除操作を行う対象物から離れた位置において楽な体勢で指紋認証等による個人認証操作を行い、その後認証済みの携帯端末 1 を保持したまま対象物に近づくだけで対象物と携帯端末 1 間で自動的にセキュリティ解除のための相互通信が行われ、自動的にキーレスエントリ操作あるいはセキュリティ解除操作が実行できる。これにより、不正乱用防止など高いセキュリティ性能を保持したまま使用者 10 にとって非常に利便性が高いキーレスエントリ操作あるいはセキュリティ解除操作を行うことができる。

[0018] さらに前記した携帯端末 1 の保持継続状態の検知に加え、予め一定の認証結果有効状態保持時間を設定しておき、前記指紋認証等による個人認証後に前記保持時間が経過すると、携帯端末 1 が保持継続状態であっても個人認証結果が有効から無効にリセットされるようにしておく、さらに不正乱用防止効果を向上させることができる。

[0019] 図 3 は、本実施例を具体的に実現するための携帯端末のブロック図の一例を示している。図 3 において、情報表示画面 2 の所定位置に接触した手指から指紋形状パターンを検知する指紋センサ 100 で得られた指紋形状パターン情報は、指紋特徴点抽出部 101 に送られ、ここで所定の指紋特徴点情報が抽出されて認証部 102 に送られる。

[0020] この認証部 102 では、指紋特徴点抽出部 101 で得られた接触手指の指紋特徴点情報とメモリ 103 に格納されている認証許可対象者個々人の指紋

特徴点情報とを照合することにより、手指を接触させた使用者 10 の個人認証合否判定を実行する。そして、その結果が『認証許可』すなわち使用者 10 がセキュリティ解除対象者であるとの認証結果、あるいは逆に『認証不許可』、すなわちセキュリティ解除非対象者であるとの認証結果はメモリ 103 に格納される。

[0021] 一方、本実施例における携帯端末には前記したような端末保持センサ 104 が装備されており、この端末保持センサ 104 で検知された所定の端末保持情報が端末保持状態判定部 105 に送られる。そして、この端末保持状態判定部 105 において、使用者 10 が携帯端末 1 を手元に保持し続けている状態か否かが判定される。

[0022] その上でメモリ 103 に格納された前記認証結果が『認証許可』で、かつ使用者 10 が携帯端末 1 を手元に保持し続けている状態と判定された場合、セキュリティ解除が許可され、所定のセキュリティ解除信号がセキュリティデータ送受信部 106 より対象となる外部のキーレスエントリシステムあるいはセキュリティシステムへ無線送信される。

[0023] また、前記 100 乃至 106 の各ブロックは制御部 110 と双方向に結ばれ、その機能や動作が制御部 110 によって適宜制御されるようになっている。

[0024] なお、図 3 に示した例では、認証許可対象者個々人の指紋特徴点情報は携帯端末 1 内に装備されたメモリ 103 に格納されているが、本実施例は勿論これに限定されるものではなく、例えば、認証許可対象者個々人の指紋特徴点情報を外部のデータセンタ等に登録しておき、個人認証操作を行う度にセキュリティデータ送受信部 106 を経由してデータセンタから登録済みの指紋特徴点情報を呼び出す仕組みであっても一向に構わない。

[0025] 次に、図 4 のフローチャートを用いて、本実施例を実現するための処理フローの一例を示す。図 4 において、フローが開始されると、まず S201 で個人認証モードを実行するか否かが選択される。選択結果が「Yes」すなわち個人認証モードを実行する場合は、次の S202 で前記指紋センサに手

指が接触した事を検知し接触手指から所定の指紋形状パターン情報が取得される。

[0026] 次に、S 2 0 3 で取得された指紋形状パターン情報から指紋特徴点が抽出される。そして、次のS 2 0 4 において、携帯端末の内部メモリまたは外部のデータセンタに登録されている認証許可対象者の指紋特徴点情報と照合することで使用者の個人認証合否判定が実行される。判定が「Y e s」すなわち個人認証が合格した場合は、次のS 2 0 5 で認証許可情報が内部メモリに格納される。逆に判定が「N o」すなわち個人認証が不合格の場合は、S 2 0 9 で内部メモリに格納されている認証許可情報が解除（リセット）されてフローが終了する。

[0027] 次にS 2 0 6 では前記認証許可を保持するモードが選択される。この選択結果が「Y e s」すなわち認証許可保持モードを選択した場合は、次のS 2 0 7 で使用者 1 0 がこの携帯端末 1 を手元に保持し続けている状態か否かが判定され、さらにS 2 0 8 で前回個人認証合否判定後からの経過時間が予め定められた認証結果保持時間内か否かが判定される。

[0028] そしてこの両方の判定結果が「Y e s」すなわち携帯端末 1 が使用者 1 0 の手元に保持され続けている状態であつ前記経過時間がまだ前記認証結果保持時間内である場合は、内部メモリに格納されている認証許可を保持し、逆にどちらか一方の判定結果が「N o」となった場合は、次のS 2 0 9 で前記認証許可情報が解除（リセット）されたうえでフローが終了する。なお、認証結果の保持時間経過後の認証N Gの場合は、ユーザに所定時間経過した旨を知らせることで、なぜ認証N Gになったかを理解することができ、ユーザは再度認証を行う等の対応を図ることができる。

[0029] 一方、前記S 2 0 6 の選択結果が「N o」すなわち認証許可保持モードを選択しなかった場合は、次のS 2 1 0 で前記指紋センサに手指が接触され続けている状態か否かを判定し、判定結果が「Y e s」すなわち前記指紋センサに手指が接触し続けている間は内部メモリに格納されている認証許可を保持し続け、判定結果が「N o」すなわち手指が前記指紋センサから離れると

、S 2 0 9 で前記認証許可情報が解除（リセット）されたうえでフローが終了する。

[0030] なお、最初のS 2 0 1 での選択結果が「N o」の場合は、フローはS 2 1 1 へ飛びここでセキュリティ解除（あるいはキーレスエントリ）モードに移行するか否かが判定される。なおこのセキュリティ解除モードへの移行判定は、使用者1 0 自身が入力した所定の割り込み命令、あるいは携帯端末1 自身が外部の対象キーレスエントリシステムまたはセキュリティシステム等から受信した所定の割り込み信号によってなされる。従って前記S 2 0 7 およびS 2 0 8 間あるいは前記S 2 1 0 におけるフィードバックループ中においても、前記割り込み信号によりフローは強制的にセキュリティ解除モードに移行する。

[0031] S 2 1 1 での判定結果が「Y e s」すなわちセキュリティ解除モードに移行すると、次のS 2 1 2 で内部メモリに格納されている認証結果（前記の認証許可情報）が読み出され、さらに次のS 2 1 3 で認証結果が許可か否かが判定される。そして判定結果が「Y e s」すなわち認証結果が『認証許可』である場合は、次のS 2 1 4 で前記の対象キーレスエントリシステムあるいはセキュリティシステムへ所定のキーレスエントリ許可信号あるいはセキュリティ解除信号が送信され、実際にキーレスエントリあるいはセキュリティ解除が実行される。

[0032] 一方、前記S 2 1 1 またはS 2 1 3 での判定結果が「N o」の場合は、一連のキーレスエントリあるいはセキュリティ解除は実行されないままフローが終了する。

[0033] ところで、以上図1 乃至図4 を用いて説明した実施例は、携帯端末1 が装備している個人認証手段として指紋認証を例にあげて説明したが、勿論本実施例はこれに限定されるものではない。例えば指紋認証の代わりに使用者1 0 の手指や手のひら内の静脈パターンから個人認証を行う静脈認証、あるいは使用者1 0 の眼の虹彩の特徴点を検出することで個人認証を行う虹彩認証や顔の造作の特徴点から個人認証を行う顔認証など携帯端末1 に装備される

如何なる生体認証手段に対しても本実施例を適用することができる。さらにはパスワード入力など携帯端末 1 に装備できる個人認証手段であればどのようなものを対して本実施例を適用しても一向に構わない。

[0034] また、様々なセキュリティ解除対象物に対し、個々の対象物に要求されるセキュリティ度に応じて個人認証のセキュリティ性能を変えられるような機能が望ましいが、従来の認証機能付き携帯端末では、使用者に対して特に認証操作の煩わしさを増やすことなくそのようなセキュリティ性能を可変できる機能を備えたものは無かった。そこで、本実施例における携帯端末による個人認証機能を用いたキーレスエントリシステムやセキュリティシステムにおいて、そのシステムごとに要求されるセキュリティレベルに応じ、上記の指紋認証以外に、上記、静脈認証や虹彩認証、顔認証などを用いた複数種類の認証モードを選択して使用することが出来れば、使用者に対して高いセキュリティ性能を保持しつつ使用者にとって柔軟で高い利便性を持ったキーレスエントリシステムあるいはセキュリティシステムを提供できる。例えば、指紋認証のみで使用者の個人認証をおこなう第 1 の認証モードと、虹彩認証または顔認証のみで使用者の個人認証をおこなう第 2 の認証モードと、指紋認証と虹彩認証または顔認証の両方から使用者の個人認証をおこなう第 3 の認証モードを備え、対象セキュリティ機器に応じて複数の認証モードから使用認証モードを任意に選択できるようにしても良い。

[0035] 以上のように、本実施例は、個人認証装置を備えた携帯端末であって、使用者が携帯端末を手保持し続けている状態を検知する保持検知装置を備え、使用者が個人認証装置により認証操作を行ったのち保持検知装置の検知結果により携帯端末を手保持している状態を検知し続けている間は認証操作の認証結果を保持し続ける機能を備えた。

[0036] また、個人認証装置を備えた携帯端末を用いたシステムの認証方法であって、使用者が個人認証装置により認証操作を行ったのち携帯端末を手保持し続けている間は認証操作の認証結果を保持し続け、認証結果を通信することによりシステムの解除操作を行うように構成した。また、そのシステムは

、キーレスエントリシステムやセキュリティシステムである。

[0037] これにより、使用者にとって高い利便性を備えたキーレスエントリシステムまたはセキュリティシステムを実現することができる。

実施例 2

[0038] 次に、本発明の第2の実施例について図5および図6を用いて説明する。

図5および図6は、本実施例における携帯端末1の使用状態を示すため使用者10の手元を拡大した概略図であり、実施例1の図2に記した構成要素と同じ構成要素には同じ番号を付している。また図5、図6においては、携帯端末を保持する使用者10の右手11は省略している。

[0039] 本実施例における携帯端末1も実施例1と同様、例えば液晶画面などで構成される情報表示画面2の全面またはその一部領域内の任意位置に手指を接触させた場合、接触手指の指紋形状パターンから所定の指紋特徴点を検知し、その検知情報を用いて使用者個人の認証を行なう機能を備えている。

[0040] しかも本実施例における携帯端末1は、以下に示すような機能を備えている。すなわち、図5に示すように、情報表示画面2上に1本の手指を接触させ、その1本の手指の指紋特徴点から使用者10の個人認証を行う第1の指紋認証モードと、図6に示すように、情報表示画面2上に2本以上の手指を同時に接触させ、その全ての手指の指紋特徴点から使用者の個人認証を行う第2の指紋認証モードとの少なくとも2種類の指紋認証モードを備え、使用者10がそれらの指紋認証モードから自由に認証モードを選択して実行できるようになっている。

[0041] 指紋認証においては、1本の手指の指紋特徴点から認証を行う第1の指紋認証モードよりも、複数の手指の指紋特徴点全てから認証を行う第2の指紋認証モードの方が、明らかに認証許可対象者の個人識別能力や非認証許可対象者の排除能力などのセキュリティ性能は格段に高くなる。

[0042] さらに、前記第2の指紋認証モードに加え、接触させた手指の本数やその手指の種別が事前登録された認証許可対象者の接触手指の本数、種別のデータと一致するか否かの照合結果も個人認証の合否判定に用いる第3の認証

モードも可能である。つまりこの第3の指紋認証モードは、接触手指の本数や種別をある種の暗号もしくはパスワードとして機能させることで、前記第1および第2の指紋認証モードに対してさらにセキュリティ性能を向上できる。

[0043] そこで、本実施例における携帯端末による個人認証機能を用いたキーレスエントリシステムやセキュリティシステムにおいて、そのシステムごとに要求されるセキュリティレベルに応じ前記複数種類の認証モードから使用者が自由に認証モードを選択して使用することが出来れば、使用者に対して高いセキュリティ性能を保持しつつ使用者にとって柔軟で高い利便性を持ったキーレスエントリシステムあるいはセキュリティシステムを提供できる。

[0044] なお、図5に示した第1の指紋認証モードの例では、左手12の人指し指を接触させたケースを示しているが、当然本実施例はそれに限定されるものではなく、どの手指であっても事前にその手指の指紋特徴点を登録しておけば使用可能である。また同じく、図6に示した第2の指紋認証モードの例では、左手12の人指し指、中指、薬指の3本的手指を接触させた場合を示しているが、当然本実施例はそれに限定されるものではなく、2本以上の複数の手指であればその手指の本数や手指の種別に制限は無い。

[0045] 図7は本実施例を実現するための携帯端末のブロック図の一例を示している。なお図7において、図3に示したブロック図と同じブロックには同じ番号を付している。また図3と同じブロックの機能については、その説明を省略する。図7において、指紋センサ100および指紋特徴点抽出部101は、複数の手指が接触した場合においても各手指の指紋形状パターンおよび指紋特徴点を全て抽出できる機能を備えている。また図7では、図3に示した各ブロックに加えて、新たに接触手指本数／種別検知部108が配備されている。この接触手指本数／種別検知部108は、指紋センサ100によって検知された複数の手指の指紋形状パターンからその接触手指の本数およびその手指の種別を検知する機能を備えている。

[0046] この接触手指本数／種別検知部108で検知された接触手指の本数および

種別情報は、指紋特徴点抽出部 101 で抽出された全ての接触手指に関する指紋特徴点情報と共に認証部 102 に送られ、この認証部 102 において両情報の照合結果から手指を接触させた使用者 10 の個人認証合否判定が実施される。

[0047] 次に図 8 のフローチャートを用いて、本実施例を実現するための処理フローの一例を示す。なお図 8 において、図 4 に示したフローチャートと同じ処理フローには同じ番号を付している。また図 4 と同じ処理フローについては、その説明を省略する。

[0048] 図 8 において、S204 において個人認証合否判定を行う際、S203 で抽出された全ての接触手指の指紋特徴点と合わせて、S215 で検知された接触手指の本数および種別情報が事前登録された認証許可対象者の接触手指本数や種別と一致するか否かによっても個人認証合否判定が実施される。

[0049] 以上のように、本実施例は、個人認証装置を備えた携帯端末であって、使用者が携帯端末を手保持している状態を検知する保持検知装置を備え、使用者が個人認証装置により認証操作を行ったのち保持検知装置の検知結果により携帯端末を手保持している状態を検知し続けている間は認証操作の認証結果を保持し続ける機能を備え、個人認証装置は、生体特徴情報を用いて個人を識別、認証する生体認証装置であり、生体認証装置は携帯端末の情報表示画面の全面もしくはその一部内の任意位置に接触させた使用者の手指から指紋特徴点を検知し個人識別する指紋認証装置であって、かつ 1 本の手指のみを接触させてその指紋特徴点から使用者の個人認証を行う第 1 の指紋認証モードと、2 本以上の手指を接触させてその全ての手指の指紋特徴点から使用者の個人認証を行う第 2 の指紋認証モードとの少なくとも 2 種類の指紋認証モードを備え、対象セキュリティ機器に応じて複数の指紋認証モードから使用認証モードを任意に選択できる機能を備えた。

[0050] これにより、使用者にとって高い利便性を備え、かつ、セキュリティ性能を向上できるという効果がある。

実施例 3

- [0051] 次に本発明の第3の実施例について、図9および図10を用いて説明する。これらの図は、本実施例における携帯端末1の使用状態を示すため使用者10の手元を拡大した概略図であり、前記図2、図5および図6中に記した構成要素と同じ構成要素には同じ番号を付している。また、図9、図10においても携帯端末を保持する使用者10の右手11は省略している。
- [0052] 本実施例における携帯端末1も実施例1、2と同様、情報表示画面2の全面またはその一部領域内の任意の位置に手指を接触させた場合、接触させた手指の指紋形状パターンから所定の特徴点を検知して使用者個人の識別、認証を行なう機能を備えている。
- [0053] しかも本実施例では、携帯端末1にその情報表示画面2の全面またはその一部領域内の任意の位置に接触させた手指の接触位置情報（例えば情報表示画面内に定めた限定に対する相対座標等）を検知する装置を備えている。
- [0054] このような手指の接触位置情報を検知する装置を用いると、その接触位置検知情報と接触させた手指の指紋認証結果の両方から個人認証を実行させることができる。
- [0055] すなわち図9の例に示すように、例えば前記情報表示画面2の左上隅にある破線で囲まれた所定領域21内に使用者の左手12の人指し指を接触させた場合には、その領域21内に接触させた人指し指の接触位置検知情報と該人指し指から得られる指紋特徴点情報の両方を、事前に登録されている認証許可対象者の接触位置検知情報と指紋特徴点情報と照合することで個人認証を行う。したがって例えば図10に示す例のように、前記領域21とは異なる領域22内に手指を接触させた場合には、たとえ指紋認証の結果が『有効』であっても、個人認証としては無効として排除することができる。
- [0056] 図11は本実施例を実現するための携帯端末のブロック図の一例を示している。なお図11において、図3および図7に示したブロック図と同じブロックには同じ番号を付している。また図3および図7と同じブロックの機能については、その説明を省略する。
- [0057] 図11において、図7に示した各ブロックに加えて、新たに情報表示画面

2上の所定位置に接触した手指の接触位置情報、例えば情報表示画面2上の相対座標等、を検知する機能を備えた手指接触位置検知部109が配備されている。

[0058] この手指接触位置検知部109で検知された接触手指の接触位置情報は認証部102に送られ、この認証部102において、前記指紋特徴点抽出部101で抽出された接触手指の指紋特徴点情報および前記接触手指本数／種別検知部108で検知された接触手指の本数および種別の情報等と組合わせて事前登録された認証許可対象者の各情報と照合することで、使用者10の個人認証合否判定を実施することができる。

[0059] 次に図12のフローチャートを用いて、本実施例を実現するための処理フローの一例を示す。なお図12において、図4および図8に示したフローチャートと同じ処理フローには同じ番号を付している。また図4および図8と同じ処理フローについては、その説明を省略する。

[0060] 図12において、S204で個人認証合否判定を行う際、S203で抽出された指紋特徴点情報、およびS215で検知された接触手指の本数および種別情報と合わせて、S216において検知された各接触手指の接触位置情報が事前登録された認証許可対象者の接触位置情報と一致するか否かによっても個人認証合否判定が実施される。

[0061] 以上述べたように、指紋特徴点情報や接触手指の本数および種別情報に加え、手指の接触位置情報も用いて個人認証を行うことで、個人認証機能がさらに多重化されることになり、認証許可対象者の個人識別能力や非認証許可対象者の排除能力などセキュリティ性能を更に向上させることができる。

[0062] ところで、前記のような手指の接触位置情報を検知する装置が備わっていると、手指を2箇所以上の領域に順番に接触させることで、各接触位置情報に加えさらにその接触順の情報についても登録情報と照合することで、さらに多重化された個人認証を行うことができる。

[0063] 例えば図13に示す実施例では、まず使用者10はその左手12の人指し指を(a)図に示すように携帯端末1の情報表示画面2の左上隅にある破線

で囲まれた所定領域 2 1 内に接触させ、次に (b) 図に示すように人指し指を移動させて前記情報表示画面 2 の右下隅にある破線で囲まれた所定領域 2 2 内に接触させる。この最初に領域 2 1 内に接触させ、次に領域 2 2 内に接触させたという接触順情報とそれぞれの接触位置検知情報、そして接触させた手指の指紋特徴点情報の全てについて、事前登録された認証許可対象者の各情報と照合することで、使用者 1 0 の個人認証合否判定を実施することができる。このような多重化された個人認証を用いれば、セキュリティ性能を更に高くすることができる。

[0064] また同様に前記のような手指の接触位置情報を検知する装置が備わっていると、複数の手指をそれぞれ異なる所定領域に接触させることで、セキュリティ性能を更に高くすることも可能である。

[0065] 例えば図 1 4 に示す例では、使用者 1 0 はその左手 1 2 の人指し指を携帯端末 1 の情報表示画面 2 の左上隅にある破線で囲まれた所定領域 2 1 内に接触させると同時に親指を前記情報表示画面 2 の右下隅にある破線で囲まれた所定領域 2 2 内に接触させている。この領域 2 1 内接触させた人指し指の位置情報、領域 2 2 内に接触させた親指の位置情報、そしてそれぞれの領域における人指し指と親指の指紋特徴点情報の全てについて、事前登録された認証許可対象者の各情報と照合することで、使用者 1 0 の個人認証合否判定を実施することも可能である。

[0066] さらに前記のような手指の接触位置情報検知装置に加え、情報表示画面 2 に接触させた手指の指紋パターンから該情報表示画面 2 に対する相対的な方向や向きを検知する機能を備えると、セキュリティ性能はさらに向上させることができる。

[0067] 前記のように接触させた手指の指紋パターンから該情報表示画面 2 に対する相対的な方向や向きを検知できれば、例えば図 1 5 のように携帯端末 1 を横向きして手指を接触させたり、図 1 6 のように携帯端末 1 の天地を逆向きにして手指を接触させることで、接触手指の前記情報表示画面 2 に対する相対的な方向や向きの検知情報と指紋特徴点情報の両方について、事前登録さ

れた認証許可対象者の各情報と照合することで、使用者10の個人認証合否判定を実施することも可能である。

[0068] なお図9乃至図16で示した各実施例はあくまで一例であって、当然のことながら本実施例はこれらに限定されるものではない。各実施例における接触手指の本数や数、接触領域の位置や数、接触手指の接触方向や向きは使用者が自由に選択して構わない。

[0069] また図9乃至図16で示した各実施例はそれぞれ単独で用いても構わないし、これら複数種類の個人認証方法を組み合わせて用いても一向に構わない。

[0070] なお、認証方法が複雑になると、その方法を忘れた場合の対策が必要となる。そこで、例えば、最初の生体認証時にのみ認証方法、手順が確認できるようにしても良い。

[0071] 以上のように、本実施例は、個人認証装置を備えた携帯端末であって、使用者が携帯端末を手に保持し続けている状態を検知する保持検知装置を備え、使用者が個人認証装置により認証操作を行ったのち保持検知装置の検知結果により携帯端末を手に保持している状態を検知し続けている間は認証操作の認証結果を保持し続ける機能を備え、個人認証装置は、生体特徴情報を用いて個人を識別、認証する生体認証装置であり、生体認証装置は携帯端末の情報表示画面の全面もしくはその一部内の任意位置に接触させた使用者の手指から指紋特徴点を検知し個人識別する指紋認証装置であって、かつ使用者が接触させた手指の情報表示画面内の接触位置情報を検知する装置を備え、指紋認証装置で得られた指紋認証情報と接触位置情報の両方から使用者の個人認証をおこなう機能を備えた。

[0072] また、個人認証装置を備えた携帯端末であって、使用者が携帯端末を手に保持し続けている状態を検知する保持検知装置を備え、使用者が個人認証装置により認証操作を行ったのち保持検知装置の検知結果により携帯端末を手に保持している状態を検知し続けている間は認証操作の認証結果を保持し続ける機能を備え、個人認証装置は、生体特徴情報を用いて個人を識別、認証

する生体認証装置であり、生体認証装置は携帯端末の情報表示画面の全面もしくはその一部内の任意位置に接触させた使用者の手指から指紋特徴点を検知し個人識別する指紋認証装置であって、かつ情報表示画面に対する接触手指の方向または向きを検知する装置を備え、指紋認証装置で得られた指紋認証情報と接触手指の方向または向き情報の両方から使用者の個人認証をおこなう機能を備えた。

[0073] これにより、使用者にとって高い利便性を備え、かつ、さらにセキュリティ性能を向上できるという効果がある。

実施例 4

[0074] 従来の携帯端末では、その内部に組み込まれた所定の生体認証装置を通じて個人認証合否判定を行う個人認証部、あるいは外部のキーレスエントリシステムまたはセキュリティシステム間と所定のセキュリティ信号を無線相互通信することでキーレスエントリシステムまたはセキュリティシステムセキュリティを遠隔操作する信号通信部、さらにはこれら個人認証関連の各部の機能や動作を制御する制御部などを駆動するための電力は、他の全ての端末機能と同様に携帯端末内に収納された主電源から供給されるのが一般的であった。しかしながらこれでは、主電源の電力が喪失すると他の全ての端末機能と同様に認証機能やセキュリティ信号通信機能も駆動しなくなってしまうという問題が生じる。

[0075] そこで本実施例では、例えば図 17 に示すように、携帯端末 1 の内部に装備された個人認証機能 201、セキュリティ信号通信機能 202 およびこれら各部の制御を担う制御部 203 を専用に駆動するための補助電源 301 を、前記各部を除いた携帯端末の主要機能を駆動する主要機能部 200 用の主電源 300 とは別に装備することにより、たとえ主電源 300 の電力が喪失しても、個人認証機能とセキュリティ信号通信機能を用いたキーレスエントリまたはセキュリティ解除だけは駆動させることができる。

[0076] なお補助電源 301 としては、携帯端末に収納できるように小型化されたボタン電池などでもよいし、携帯端末表面の所定位置に設置された太陽電池

パネルなどでも構わない。

[0077] 以上のように、本実施例は、個人認証装置を備えた携帯端末であって、使用者が携帯端末を手に保持し続けている状態を検知する保持検知装置を備え、使用者が個人認証装置により認証操作を行ったのち保持検知装置の検知結果により携帯端末を手に保持している状態を検知し続けている間は認証操作の認証結果を保持し続ける機能を備え、個人認証装置は、生体特徴情報を用いて個人を識別、認証する生体認証装置であり、生体認証装置以外の装置あるいは機能を駆動するための主電源とは別に生体認証装置を駆動するための電源を収納する。

[0078] これにより、たとえ主電源の電力が喪失しても、個人認証機能とセキュリティ信号通信機能を用いたキーレスエントリまたはセキュリティ解除だけは駆動させることができる。

実施例 5

[0079] 図 18 は、実施例 1 乃至 4 で説明した携帯端末 1 と、携帯端末 1 との間で所定のセキュリティ情報を無線相互通信することにより、所定のキーレスエントリを実施するキーレスエントリシステムまたはセキュリティ解除を実施するセキュリティシステムの本実施例を示したブロック図である。

[0080] 図 18 において、キーレスエントリシステムまたはセキュリティシステム 400（以下、簡単のためシステム 400 と記す。）は、携帯端末 1 との無線相互通信をおこなうための送受信部 401 と、通信信号の復号化あるいは暗号化を行う復号／暗号部 402 と、所定の対象物 405 に対してキーレスエントリまたはセキュリティ解除を実行するセキュリティ駆動部 403 が配備され、これらは制御部 404 によってそれぞれの機能や動作が逐次制御されている。

[0081] セキュリティ解除モードに設定されている携帯端末 1 がシステム 400 に所定距離まで近接すると、自動的にシステム 400 との無線相互通信が開始され、その送受信部 401 を通じてセキュリティ解除問い合わせ信号が携帯端末 1 に送信される。この時、携帯端末 1 での認証結果が『認証許可』であ

る場合は、携帯端末 1 からセキュリティ解除許可信号がシステム 400 に向けて送信される。

[0082] なおセキュリティ解除問い合わせ信号およびセキュリティ解除許可信号については、不正使用や「なりすまし」防止の観点から所定の暗号化を施された信号であることが望ましい。このセキュリティ解除問い合わせ信号やセキュリティ解除許可信号を暗号化したり暗号化されたこれら各信号を復号化するのが、復号／暗号部 402 である。

[0083] システム 400 内の送受信部 401 で受信されたセキュリティ解除許可信号は復号／暗号部 402 に送られ暗号化された信号が復号化され制御部 404 に送られる。制御部 404 はこの復号化されたセキュリティ解除許可信号を受けてセキュリティ駆動部 403 に所定の駆動動作を実行するよう指令信号を送る。

[0084] 指令信号を受けたセキュリティ駆動部 403 は、具体的には以下のような駆動動作をおこなう。例えばシステム 400 が自宅の玄関ドアやホテルの客室ドアあるいは自家用車やレンタカー等のフロントドアなどに対するキーレスエントリシステムである場合は、その対象物であるドア 405 を自動的に開錠／施錠、あるいは自動的に開閉する等の一連のキーレスエントリ動作を実施する。

[0085] また、システム 400 が例えば A T M などのセキュリティシステムである場合は、対象物である A T M 405 に対して現金の預け払いが可能な状態にするための一連のセキュリティ解除動作を実施する。

[0086] このように、実施例 1 乃至 4 における携帯端末 1 と本実施例で示したようなシステム 400 を組み合わせることにより、使用者が個人認証許可済みの携帯端末を保持したままシステム 400 に近接するだけで、一連のキーレスエントリあるいはセキュリティ解除が実行される。このため高いセキュリティ性を保持しつつ使用者にとって高い利便性を備えたキーレスエントリシステムまたはセキュリティシステムを実現することができる。

[0087] 本発明は上記した実施例に限定されるものではなく、様々な変形例が含ま

れる。例えば、上記した実施例は本発明を分かりやすく説明するために詳細に説明したものであって、必ずしも説明した全ての構成を備えるものに限定されるものではない。また、ある実施例の構成に他の実施例の構成を加えることも可能である。また、各実施例の一部について、他の構成の追加・削除・置換をすることが可能である。

符号の説明

[0088] 1…携帯端末、2…情報表示画面、3…携帯端末使用者、11…携帯端末使用者の右手、12…携帯端末使用者の左手、200…携帯端末内の主要機能部、201…携帯端末内の生体認証部、300…携帯端末の主電源、301…携帯端末の補助電源

請求の範囲

- [請求項1] 個人認証装置を備えた携帯端末であって、
 使用者が該携帯端末を手保持し続けている状態を検知する保持検知装置を備え、
 前記使用者が前記個人認証装置により認証操作を行ったのち前記保持検知装置の検知結果により前記携帯端末を手保持している状態を検知し続けている間は前記認証操作の認証結果を保持し続ける機能を備えたことを特徴とする携帯端末。
- [請求項2] 請求項1に記載の携帯端末であって、
 前記個人認証装置は、生体特徴情報を用いて個人を識別、認証する生体認証装置であり、
 セキュリティ機器との間でセキュリティ情報を通信する装置を備え、
 使用者が前記生体認証装置により認証操作を行ったのちに前記セキュリティ機器との通信操作が一定時間以上行われなかった場合に前記認証操作による認証結果が無効となる機能を備えたことを特徴とする携帯端末。
- [請求項3] 請求項1に記載の携帯端末であって、
 前記個人認証装置は、生体特徴情報を用いて個人を識別、認証する生体認証装置であり、
 前記生体認証装置は前記携帯端末の情報表示画面の全面もしくはその一部内の任意位置に接触させた使用者の手指から指紋特徴点を検知し個人識別する指紋認証装置であって、かつ1本の手指のみを接触させてその指紋特徴点から使用者の個人認証を行う第1の指紋認証モードと、2本以上の手指を接触させてその全ての手指の指紋特徴点から使用者の個人認証を行う第2の指紋認証モードとの少なくとも2種類の指紋認証モードを備え、対象セキュリティ機器に応じて前記複数の指紋認証モードから使用認証モードを任意に選択できる機能を備えた

ことを特徴とする携帯端末。

[請求項4]

請求項 1 に記載の携帯端末であって、

前記個人認証装置は、生体特徴情報を用いて個人を識別、認証する生体認証装置であり、

前記生体認証装置は前記携帯端末の情報表示画面の全面もしくはその一部内の任意位置に接触させた使用者の手指から指紋特徴点を検知し個人識別する指紋認証装置であって、かつ使用者が接触させた手指の前記情報表示画面内の接触位置情報を検知する装置を備え、前記指紋認証装置で得られた指紋認証情報と前記接触位置情報の両方から使用者の個人認証をおこなう機能を備えたことを特徴とする携帯端末。

[請求項5]

請求項 1 に記載の携帯端末であって、

前記個人認証装置は、生体特徴情報を用いて個人を識別、認証する生体認証装置であり、

前記生体認証装置は前記携帯端末の情報表示画面の全面もしくはその一部内の任意位置に接触させた使用者の手指から指紋特徴点を検知し個人識別する指紋認証装置であって、かつ前記情報表示画面に対する前記接触手指の方向または向きを検知する装置を備え、前記指紋認証装置で得られた指紋認証情報と前記接触手指の方向または向き情報の両方から使用者の個人認証をおこなう機能を備えたことを特徴とする携帯端末。

[請求項6]

請求項 1 に記載の携帯端末であって、

前記個人認証装置は、生体特徴情報を用いて個人を識別、認証する生体認証装置であり、

前記生体認証装置として、使用者の手指から指紋特徴点を検知し個人識別する指紋認証装置と、使用者の眼の虹彩の特徴点を検知し個人識別する虹彩認証装置または使用者の顔面から特徴点を検知し個人識別する顔認証装置の両方を備え、前記指紋認証装置のみで使用者の個人認証をおこなう第 1 の認証モードと、前記虹彩認証装置または前記

顔認証装置のみで使用者の個人認証をおこなう第2の認証モードと、前記指紋認証装置と前記虹彩認証装置または前記顔認証装置の両方から使用者の個人認証をおこなう第3の認証モードを備え、対象セキュリティ機器に応じて前記複数の認証モードから使用認証モードを任意に選択できる機能を備えたことを特徴とする携帯端末。

[請求項7] 請求項1に記載の携帯端末であって、
前記個人認証装置は、生体特徴情報を用いて個人を識別、認証する生体認証装置であり、

前記生体認証装置以外の装置あるいは機能を駆動するための主電源とは別に前記生体認証装置を駆動するための電源を収納していることを特徴とする携帯端末。

[請求項8] 請求項1から7の何れか1項に記載の携帯端末と、該携帯端末間で所定の個人認証情報またはセキュリティ情報を通信することにより所定の解錠／施錠操作をおこなう鍵装置と、からなることを特徴とするキーレスエントリシステム。

[請求項9] 請求項1から7の何れか1項に記載の携帯端末と、該携帯端末間で所定の個人認証情報またはセキュリティ情報を通信することにより所定のセキュリティ解除操作をおこなうセキュリティ装置と、からなることを特徴とするセキュリティシステム。

[請求項10] 個人認証装置を備えた携帯端末を用いたシステムの認証方法であって、

使用者が前記個人認証装置により認証操作を行ったのち前記携帯端末を手保持し続けている間は前記認証操作の認証結果を保持し続け、

該認証結果を通信することにより前記システムの解除操作を行うことを特徴とする認証方法。

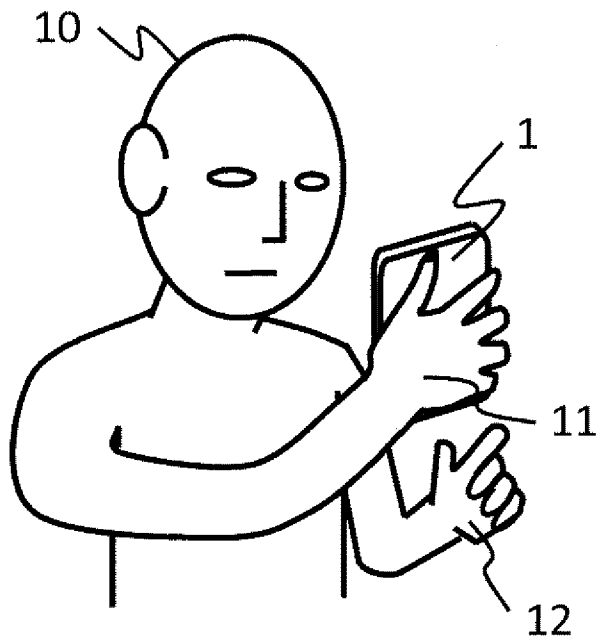
[請求項11] 請求項10に記載の認証方法であって、
前記システムはキーレスエントリシステムであることを特徴とする

認証方法。

[請求項12] 請求項10に記載の認証方法であって、
前記システムはセキュリティシステムであることを特徴とする認証
方法。

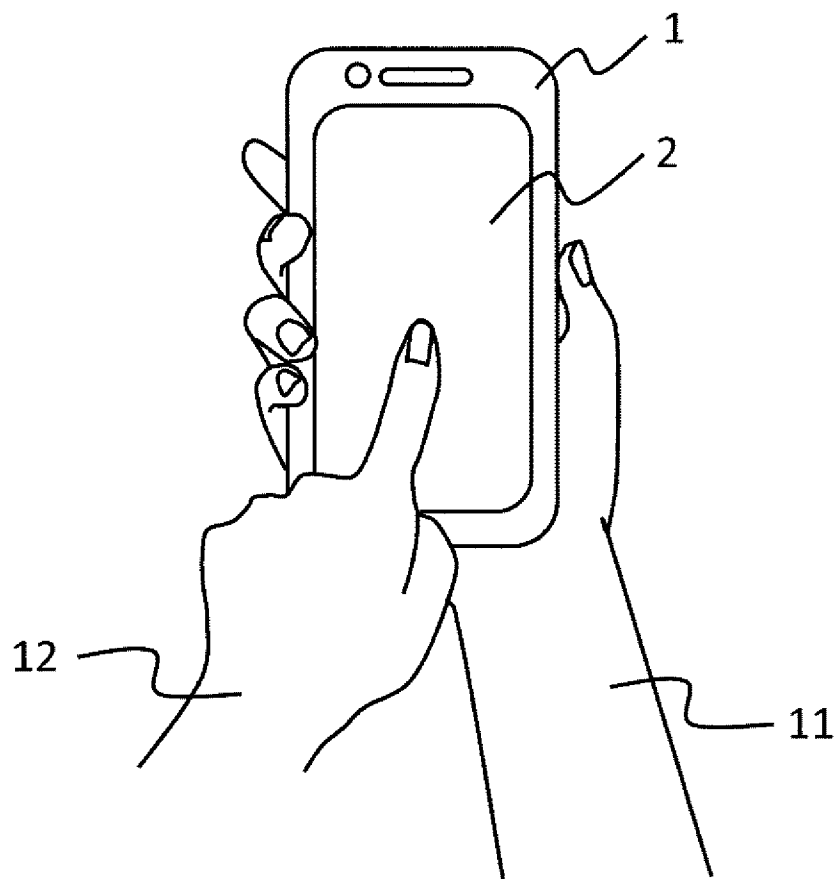
[図1]

図1

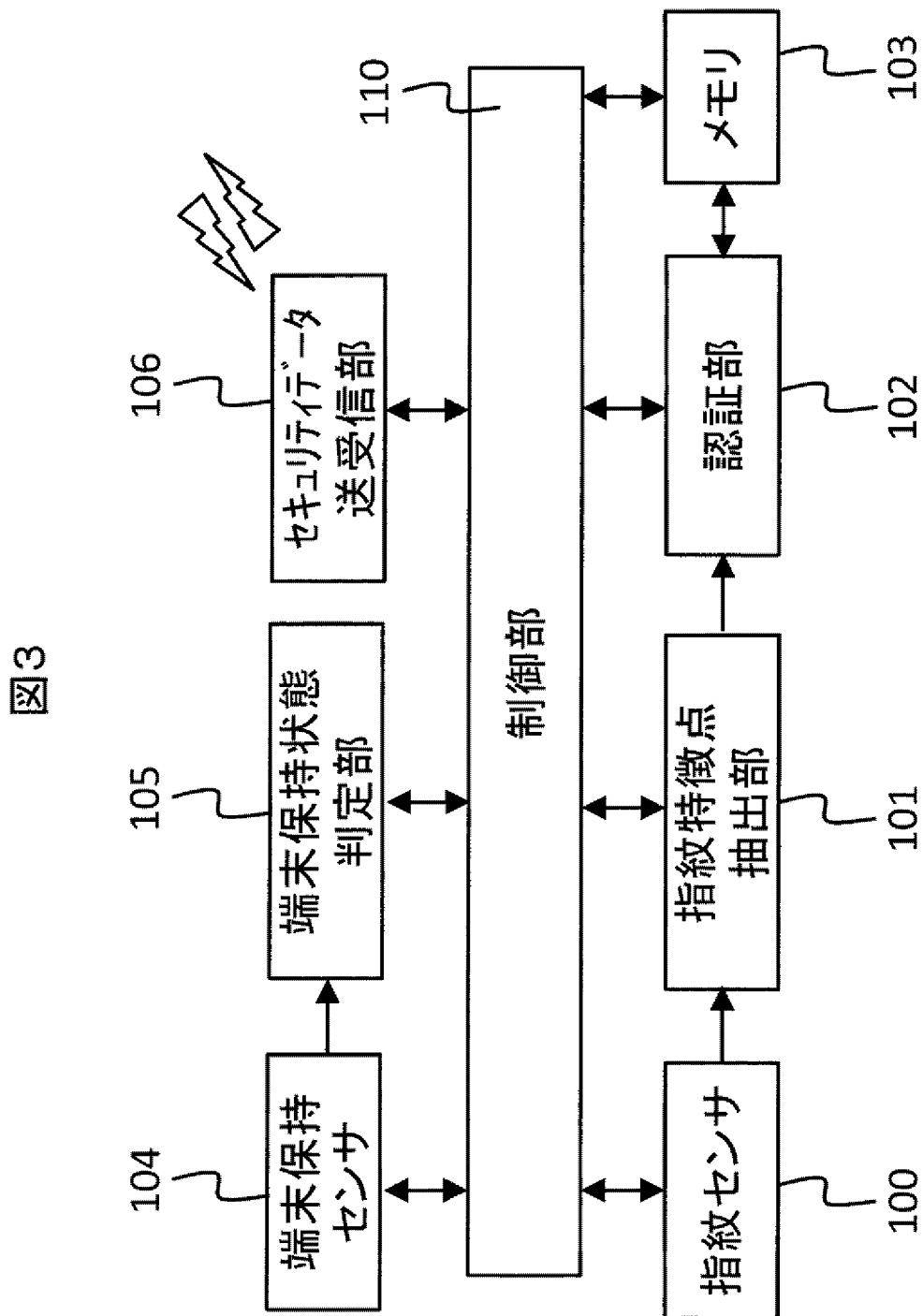


[図2]

図2

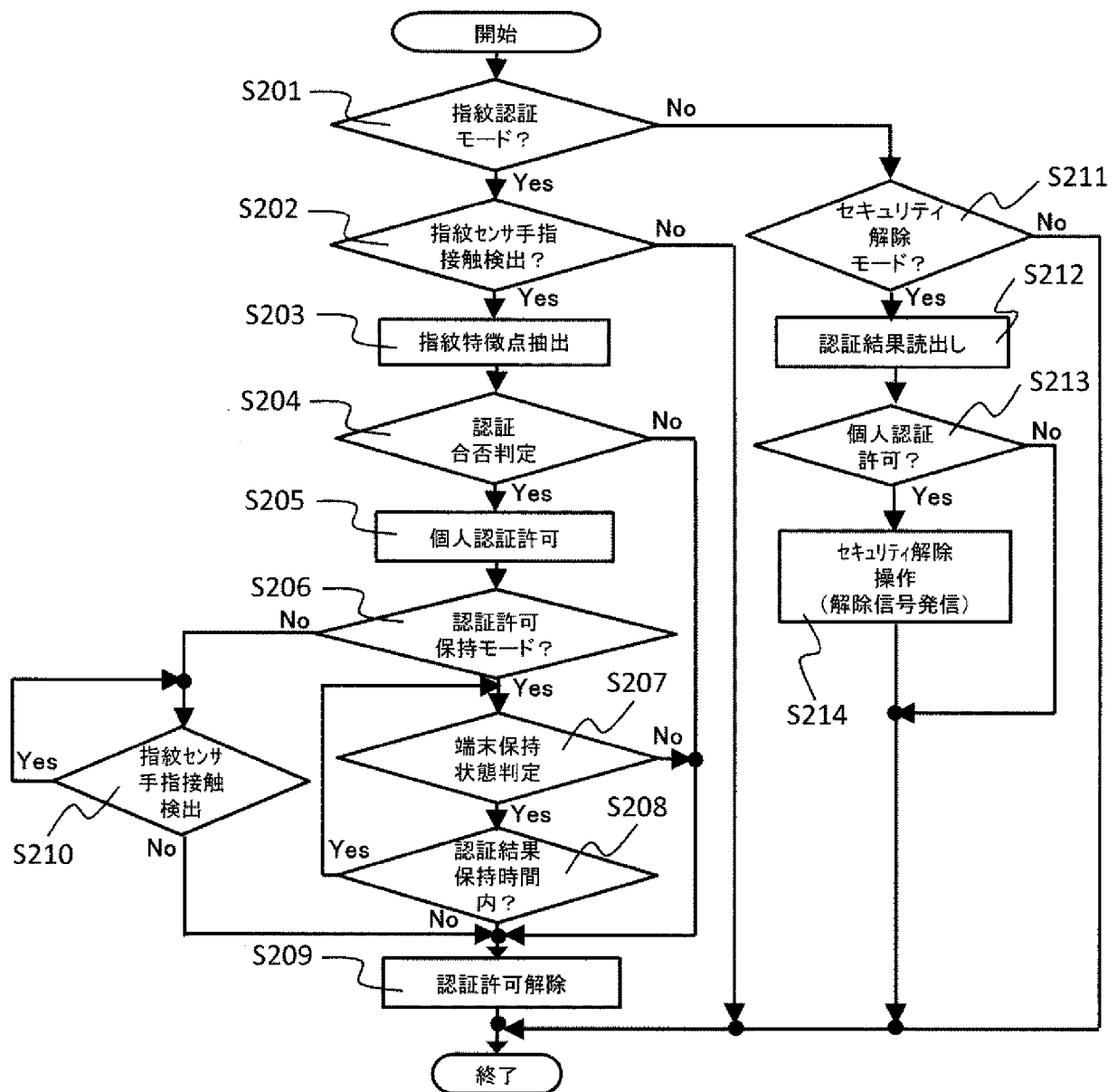


[図3]



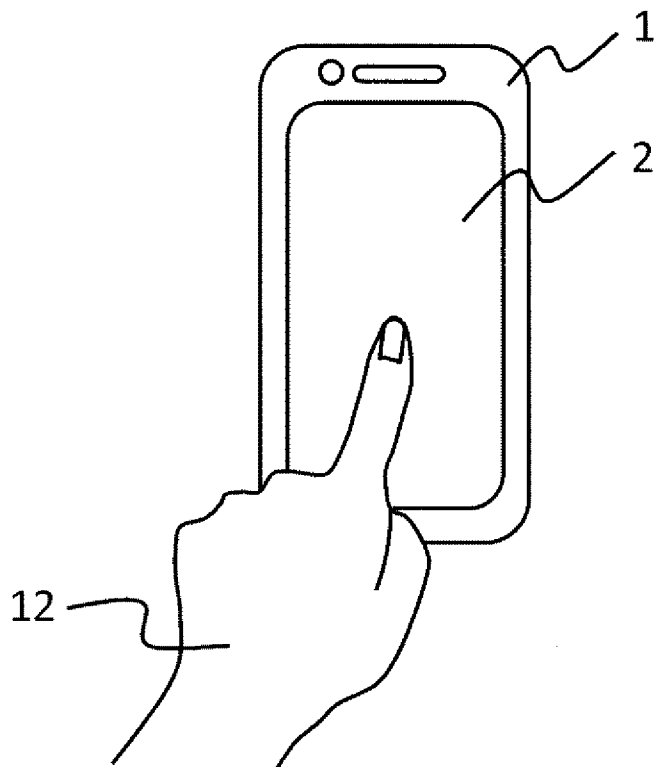
[図4]

図4



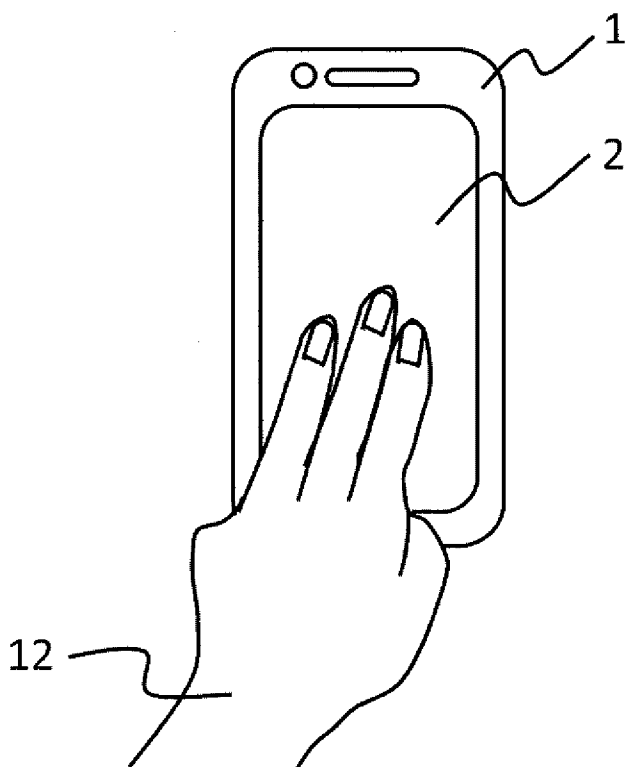
[図5]

図5

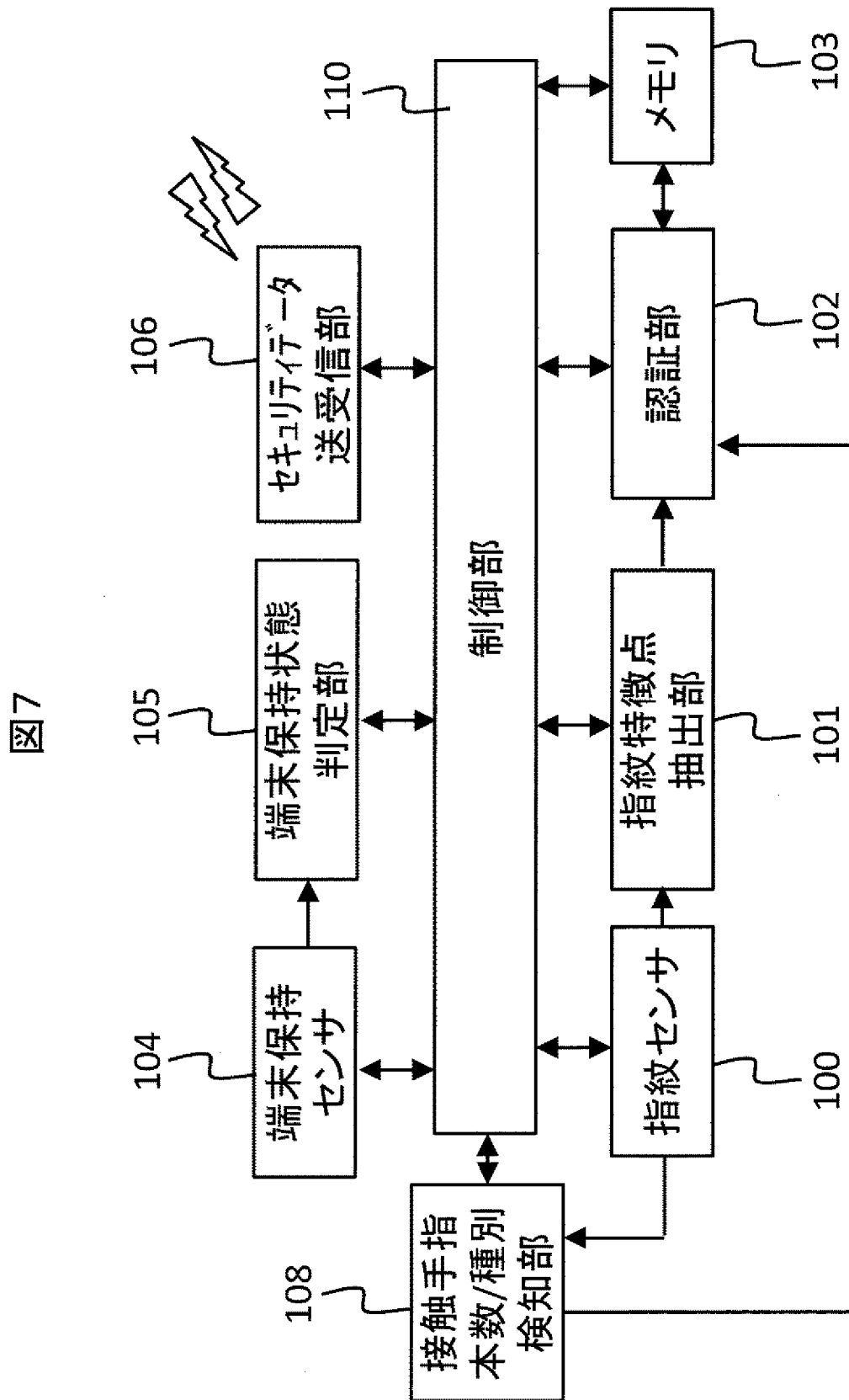


[図6]

図6

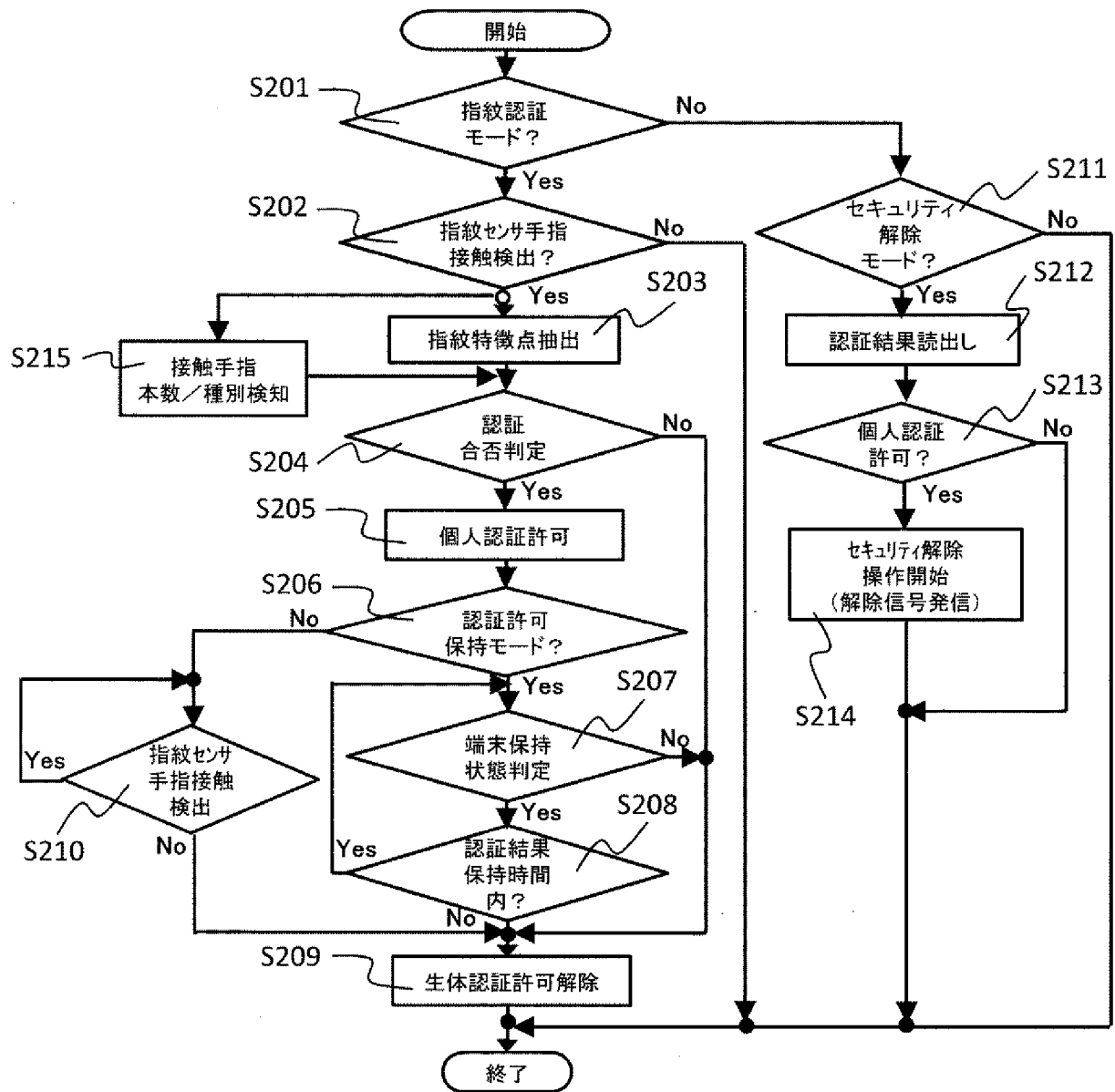


[図7]



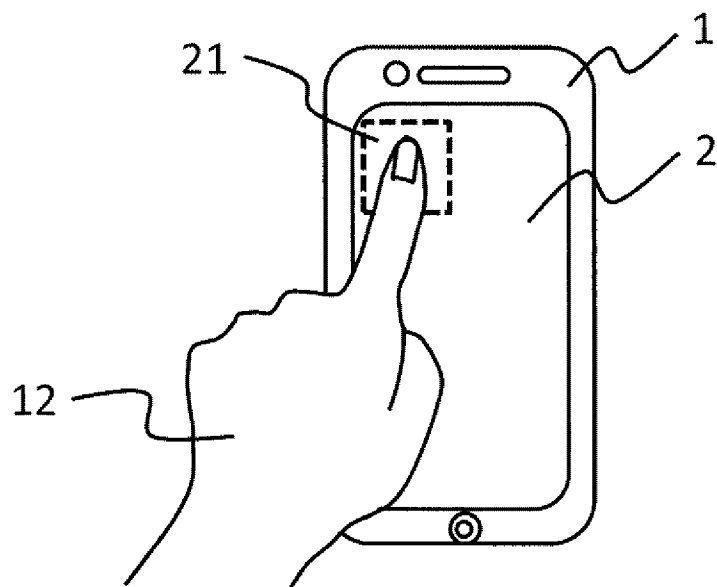
[図8]

図8



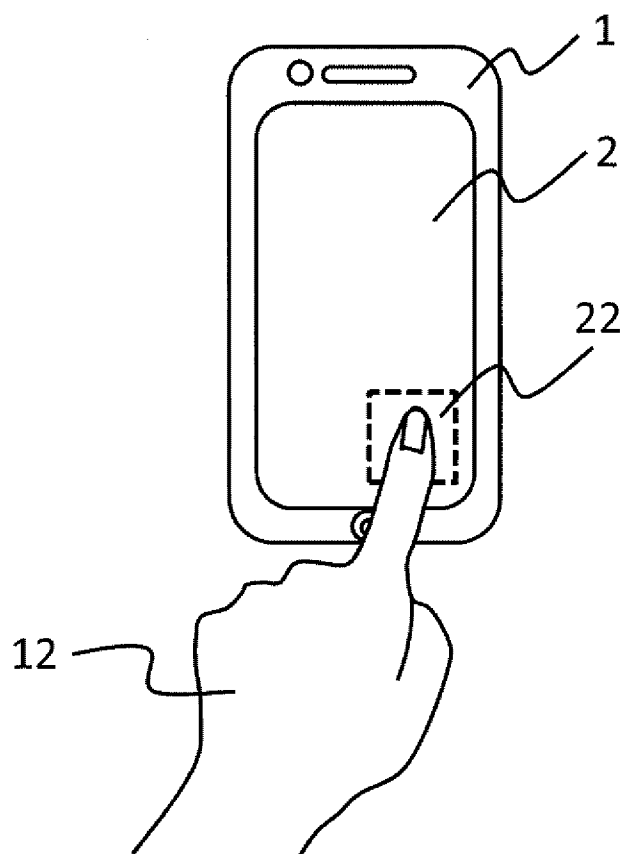
[図9]

図9



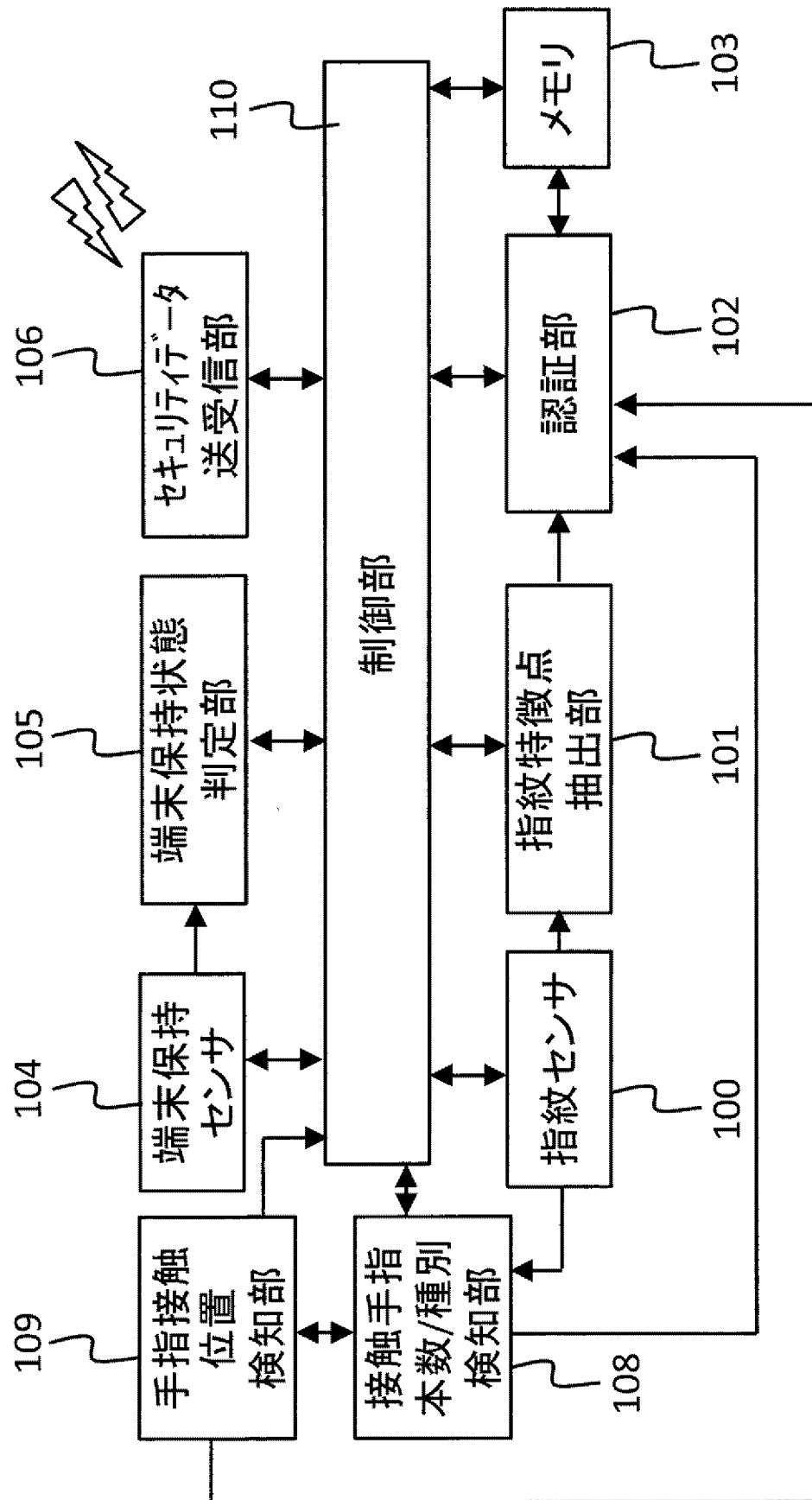
[図10]

図10



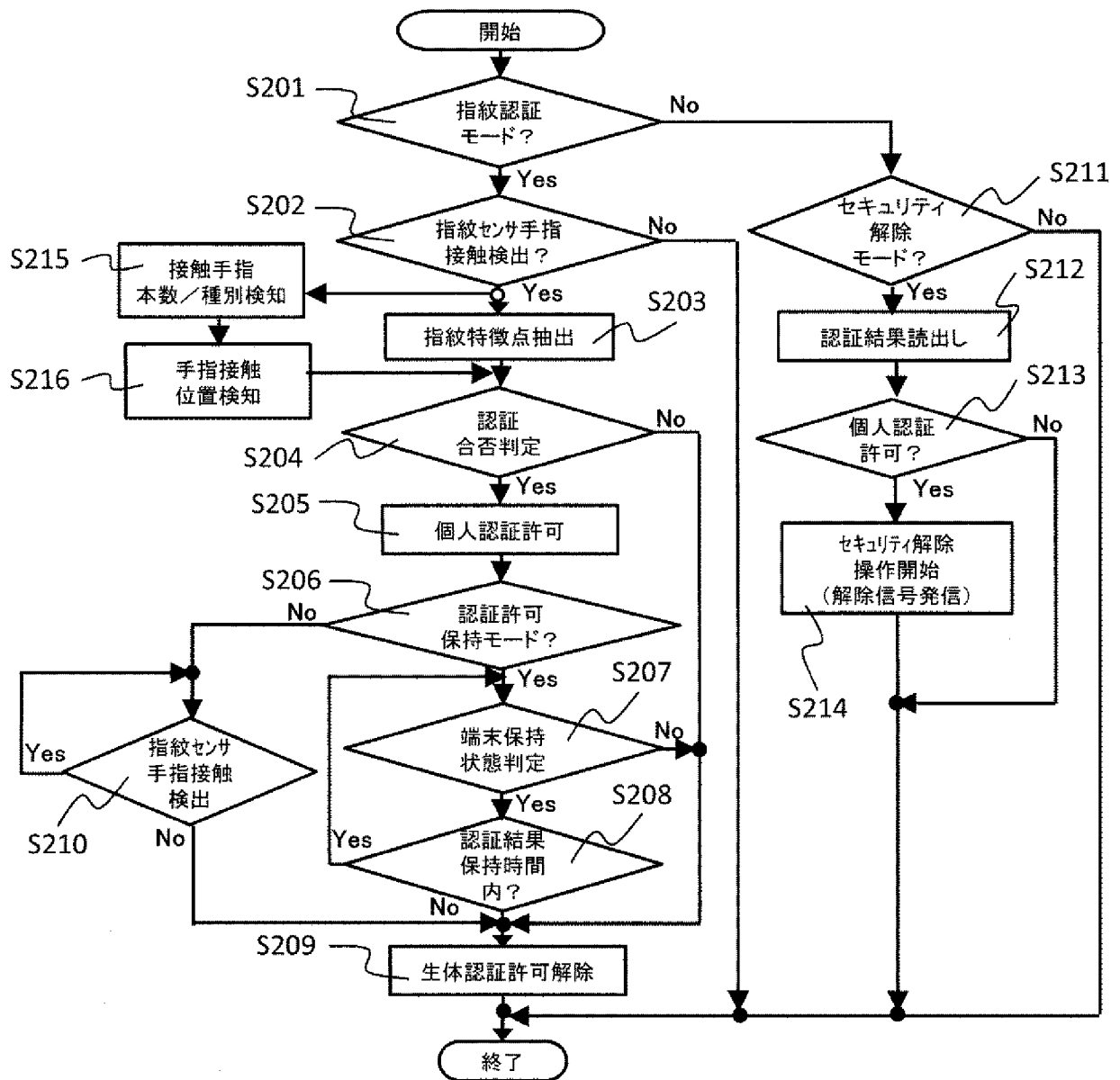
[図11]

図11



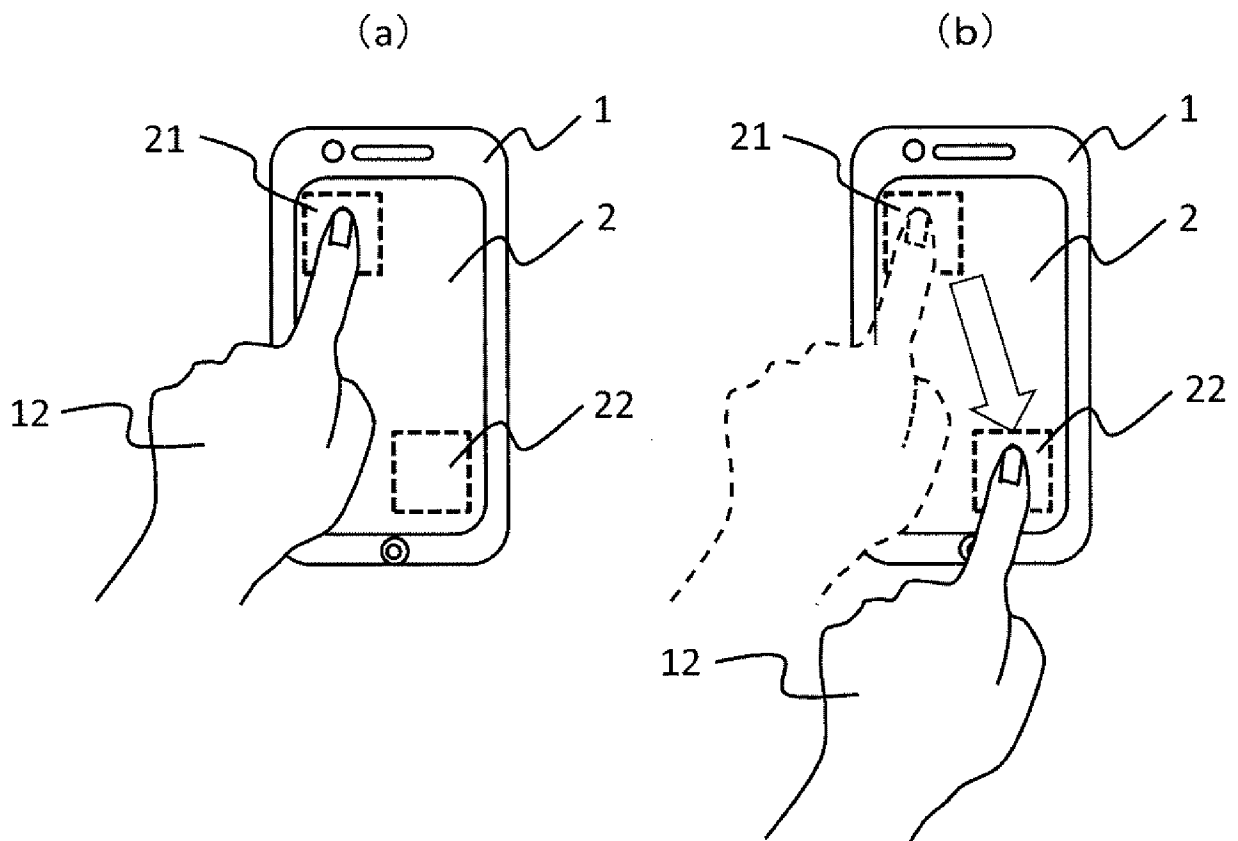
[図12]

図12



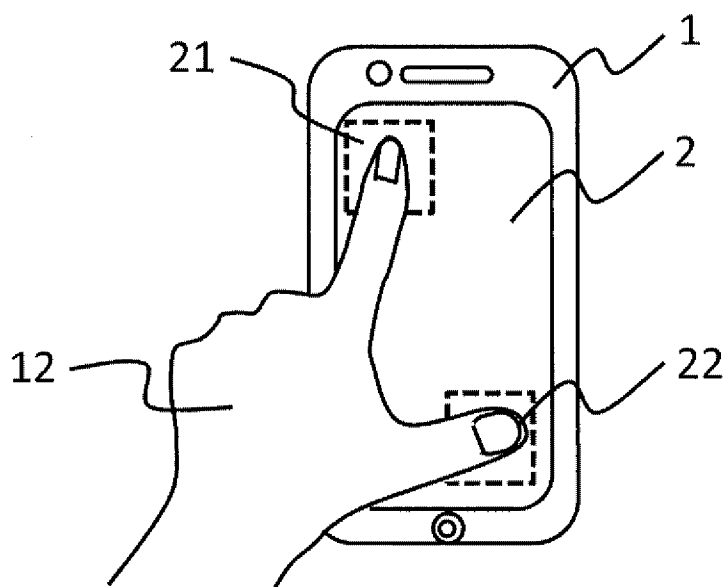
[図13]

図13



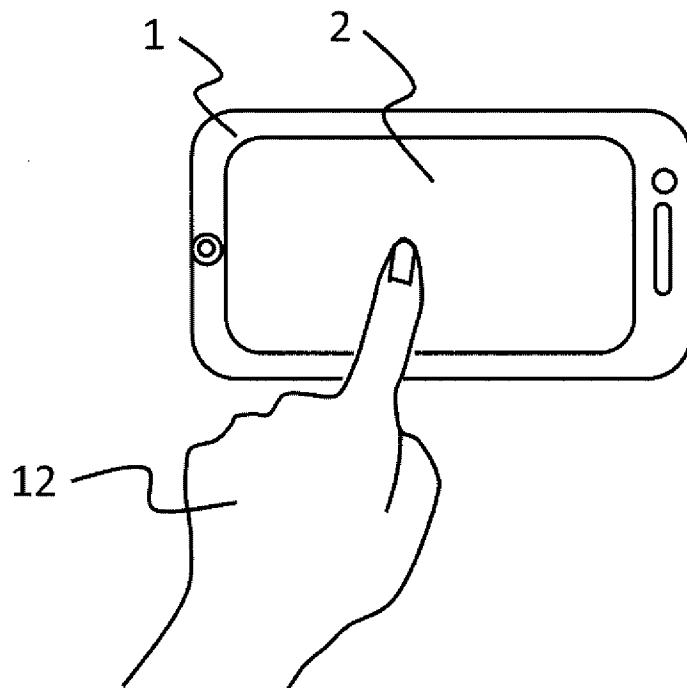
[図14]

図14



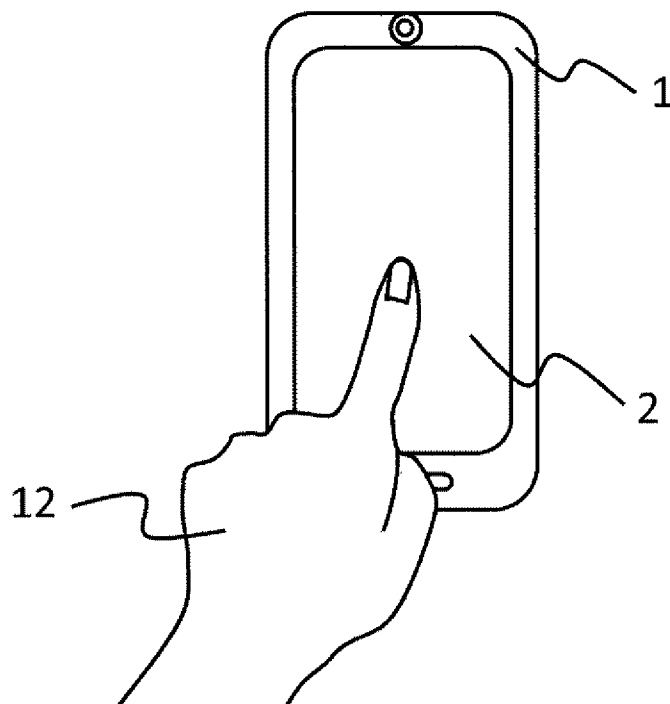
[図15]

図15



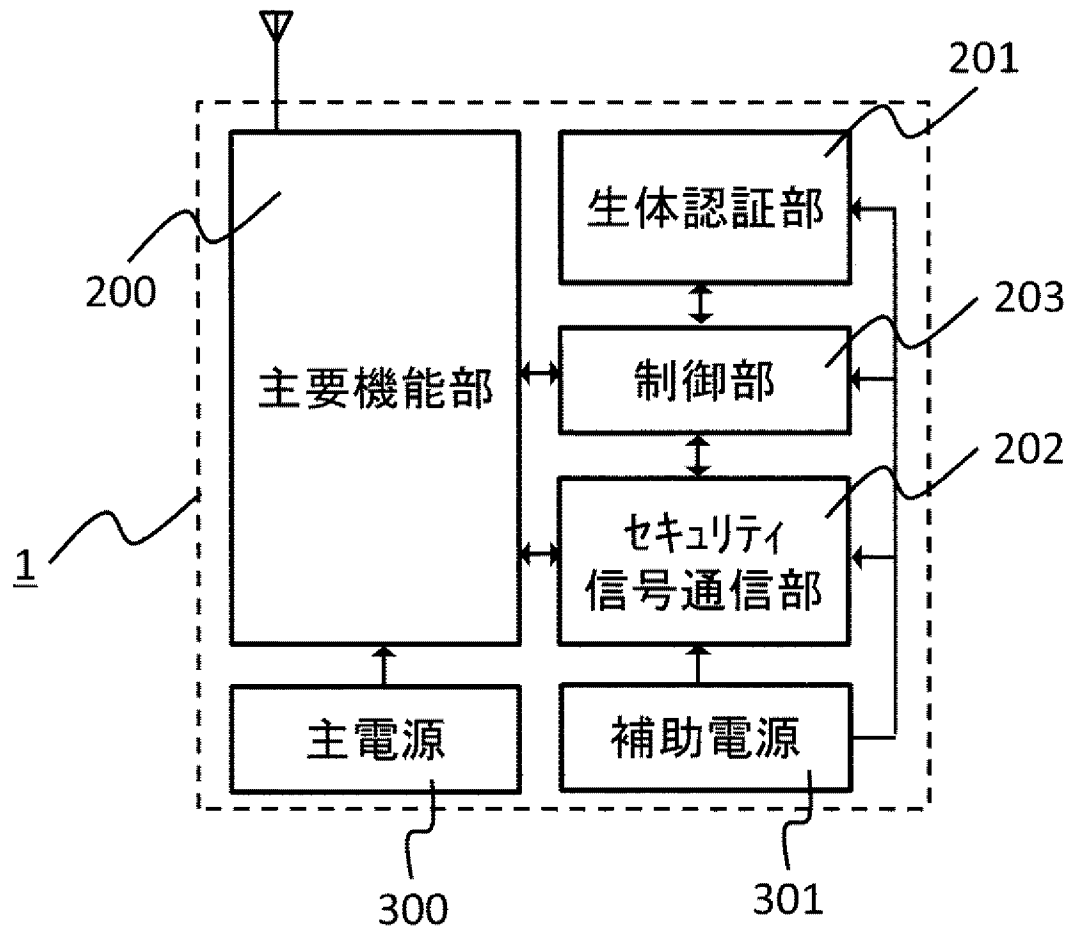
[図16]

図16



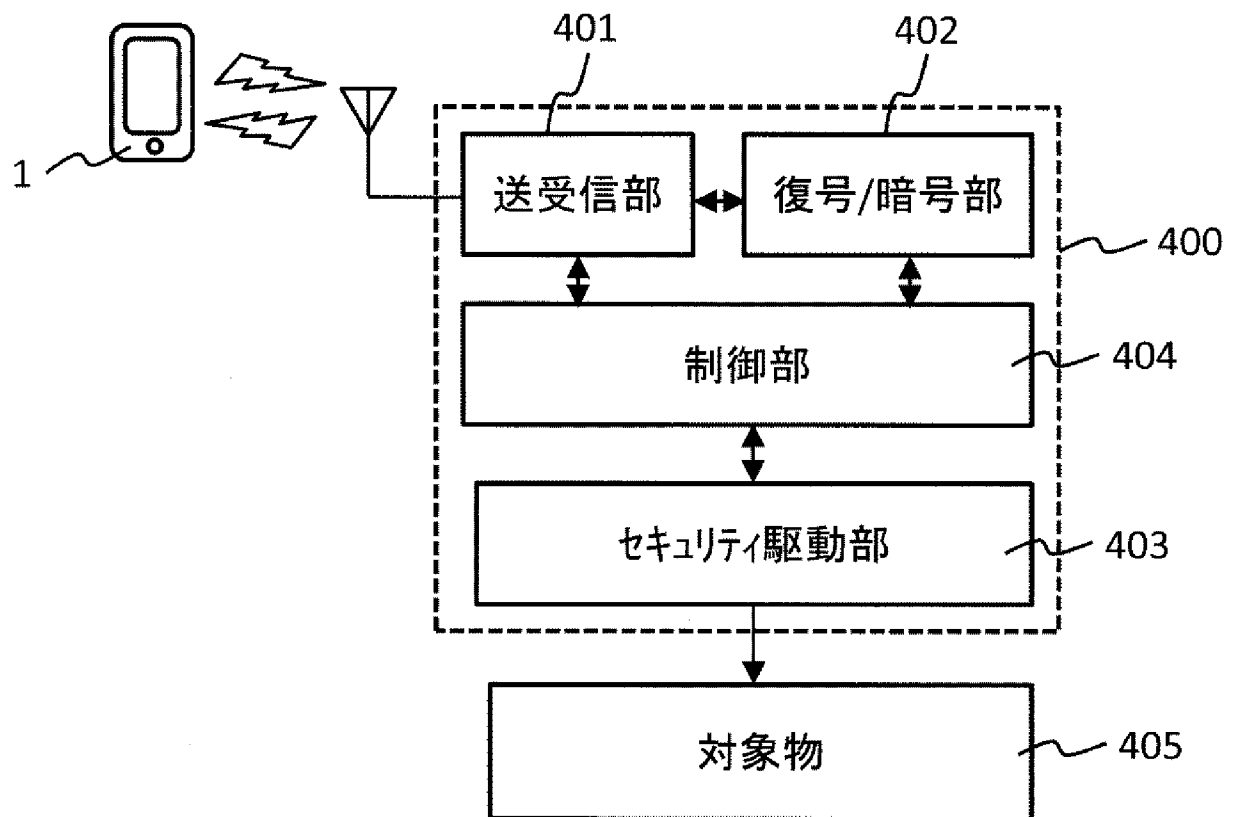
[図17]

図17



[図18]

図18



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2015/083535

A. CLASSIFICATION OF SUBJECT MATTER

G06F21/31(2013.01) i, G06F21/32(2013.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F21/31, G06F21/32

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2016

Kokai Jitsuyo Shinan Koho 1971-2016 Toroku Jitsuyo Shinan Koho 1994-2016

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP 2005-71225 A (Sony Corp.), 17 March 2005 (17.03.2005), paragraphs [0012] to [0057]; fig. 1 to 6	1, 3-4, 6, 9-10, 12
Y	& US 2005/0071647 A1 paragraphs [0013] to [0066]; fig. 2 to 7 & TW 259967 B & KR 10-2005-0021270 A & CN 1591269 A	2, 5, 7-8, 11
Y	JP 2003-58269 A (Mitsubishi Heavy Industries, Ltd.), 28 February 2003 (28.02.2003), paragraphs [0039] to [0048]; fig. 3 (Family: none)	2



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

05 February 2016 (05.02.16)

Date of mailing of the international search report

16 February 2016 (16.02.16)

Name and mailing address of the ISA/

Japan Patent Office

3-4-3, Kasumigaseki, Chiyoda-ku,

Tokyo 100-8915, Japan

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2015/083535

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2003-346133 A (NEC Infrontia Corp.), 05 December 2003 (05.12.2003), paragraph [0039] (Family: none)	5
Y	JP 2003-298733 A (Denso Corp.), 17 October 2003 (17.10.2003), abstract (Family: none)	7
Y	JP 2001-241230 A (Matsushita Electric Works, Ltd.), 04 September 2001 (04.09.2001), paragraphs [0018] to [0019], [0032] to [0033], [0041] (Family: none)	8, 11
A	JP 2001-142849 A (NTT Docomo Inc.), 25 May 2001 (25.05.2001), paragraphs [0006] to [0046]; fig. 1 to 3 (Family: none)	1-12

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int.Cl. G06F21/31(2013.01)i, G06F21/32(2013.01)i

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int.Cl. G06F21/31, G06F21/32

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922-1996年
日本国公開実用新案公報	1971-2016年
日本国実用新案登録公報	1996-2016年
日本国登録実用新案公報	1994-2016年

国際調査で利用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
X	JP 2005-71225 A (ソニー株式会社) 2005.03.17, 段落 [0012] - [0057], 図1-6 & US 2005/0071647 A1, 段落 [0013] - [0066], 図2-7 & TW 259967 B & KR 10-2005-0021270 A & CN 1591269 A	1, 3-4, 6, 9-10, 12
Y		2, 5, 7-8, 11
Y	JP 2003-58269 A (三菱重工業株式会社) 2003.02.28, 段落 [0039] - [0048], 図3 (ファミリーなし)	2

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」同一パテントファミリー文献

国際調査を完了した日

05.02.2016

国際調査報告の発送日

16.02.2016

国際調査機関の名称及びあて先

日本国特許庁 (ISA/J P)

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

打出 義尚

電話番号 03-3581-1101 内線 3546

5 S

4440

C (続き) . 関連すると認められる文献		
引用文献の カテゴリ*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
Y	JP 2003-346133 A (NECインフロンティア株式会社) 2003.12.05, 段落 [0039] (ファミリーなし)	5
Y	JP 2003-298733 A (株式会社デンソー) 2003.10.17, 要約 (ファミ リーなし)	7
Y	JP 2001-241230 A (松下電工株式会社) 2001.09.04, 段落 [001 8] - [0019], [0032] - [0033], [0041] (フ ァミリーなし)	8, 11
A	JP 2001-142849 A (株式会社エヌ・ティ・ティ・ドコモ) 2001.05.25, 段落 [0006] - [0046], 図1-3 (ファミリーなし)	1-12