(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2016-119095
(P2016-119095A)
(43)公開日　平成28年6月30日(2016.6.30)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/31	(2013.01)	G06F	21/31		5B020
G06F 3/0488	(2013.01)	G06F	3/0488	160	5B087
G06F 3/023	(2006.01)	G06F	3/023	310L	5E555
H03M 11/04	(2006.01)	G06F	3/01	514	
G06F 3/01	(2006.01)	G06F	3/0346	422	

審査請求 未請求　請求項の数 15　ＯＬ　（全 37 頁）　最終頁に続く

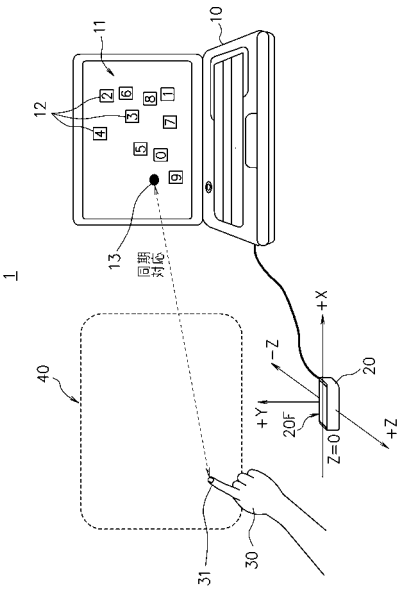
(21)出願番号　特願2015-247761 (P2015-247761)
(22)出願日　平成27年12月18日 (2015.12.18)
(31)優先権主張番号　特願2014-257583 (P2014-257583)
(32)優先日　平成26年12月19日 (2014.12.19)
(33)優先権主張国　日本国 (JP)

(71)出願人　504258527
国立大学法人　鹿児島大学
鹿児島県鹿児島市郡元一丁目２１番２４号
(74)代理人　100090273
弁理士　國分　孝悦
(72)発明者　佐藤　公則
鹿児島県鹿児島市郡元一丁目２１番２４号
国立大学法人　鹿児島大学内
(72)発明者　渡邊　睦
鹿児島県鹿児島市郡元一丁目２１番２４号
国立大学法人　鹿児島大学内
(72)発明者　鹿嶋　雅之
鹿児島県鹿児島市郡元一丁目２１番２４号
国立大学法人　鹿児島大学内

最終頁に続く

(54)【発明の名称】認証処理装置及び認証処理方法

(57)【要約】
【課題】認証用センサ等に触れることなく、非常に高いセキュリティ性を確保した個人認証を可能とすることを課題とする。
【解決手段】
三次元空間内における手３０の三次元座標をフレーム周期で検出する距離センサ２０と、複数のキー画像１２を画面内に表示するディスプレイ１１と、三次元空間内にディスプレイ１１の画面に対応付けられたバーチャルタッチパネル４０を設定するとともに、指先３１によりバーチャルタッチパネル４０内でキーをエアクリックしたことが検出されたとき、そのキーが認証対象者により選ばれたと判定し、選ばれたキーに対応した数字と予め登録されているＰＩＮコードとの比較により認証処理を行う。
【選択図】　図１



【特許請求の範囲】
【請求項１】
三次元空間内における検出対象物の三次元座標を所定の時間周期ごとに検出する座標検出手段と、
認証コードに用いられる複数のコード情報にそれぞれ対応した複数の選択対象画像を画面内に表示する画像表示手段と、
前記三次元空間内に仮想二次元平面を設定するとともに、前記画面内における前記複数の選択対象画像の表示座標と仮想二次元平面内における仮想座標とを対応させる仮想平面設定手段と、
前記検出対象物の三次元座標を解析することにより、前記検出対象物を構成している複数の部位を識別し、前記識別した部位の座標が前記仮想二次元平面内で前記仮想座標に対応している状態で、前記三次元空間内にて前記識別した部位による所定の動きを検出したとき、前記識別した部位により前記選択対象画像が選ばれたと判断する解析手段と、
前記解析手段で選ばれたと判断された選択対象画像に対応したコード情報と、予め登録されている認証コードのコード情報とに基づいて、認証判定を行う認証判定手段と
を有することを特徴とする認証処理装置。
【請求項２】
前記認証コードに用いられる複数のコード情報は０から９の数字であり、
前記画像表示手段は、前記複数の選択対象画像として０から９の数字の画像を前記画面内にランダムに配置して表示し、
前記解析手段は、前記検出対象物が認証対象者の手である場合に、各手指部位を個別に識別して各手指部位の識別情報を取得すると共に、前記個別に識別した手指部位により順に選ばれた前記複数の選択対象画像に対応した数字の配列を取得し、
前記認証判定手段は、前記解析手段により個別に識別された手指部位によって順に選ばれた複数の選択対象画像に対応した複数の数字の配列と、前記選択対象画像を順に選んだ手指部位の識別情報と、予め登録されている認証コードの数字の配列と、前記認証コードの各数字に対応して予め登録されている手指部位の識別情報との一致判定により、前記認証対象者の認証判定を行うことを特徴とする請求項１記載の認証処理装置。
【請求項３】
前記認証コードに用いられる複数のコード情報は０から９の数字であり、
前記画像表示手段は、前記複数の選択対象画像として０から９の数字の画像を前記画面内にランダムに配置して表示し、
前記解析手段は、前記検出対象物が認証対象者の手である場合に、一つの手指部位によって順に選ばれた前記複数の選択対象画像に対応した数字の配列を取得し、
前記認証判定手段は、前記解析手段により取得された複数の選択対象画像に対応した複数の数字の配列と、予め登録されている認証コードの数字の配列との一致判定により、前記認証対象者の認証判定を行うことを特徴とする請求項１記載の認証処理装置。
【請求項４】
前記認証コードに用いられる複数のコード情報は０から９の数字であり、
前記画像表示手段は、前記複数の選択対象画像として０から９の数字の画像を前記画面内にランダムに配置して表示し、
前記解析手段は、前記検出対象物が認証対象者の手である場合に、認証処理に対して予め設定されているセキュリティレベルに応じた少なくとも一つの手指部位を、個別に識別して前記手指部位の識別情報を取得すると共に、前記個別に識別した手指部位により順に選ばれた前記複数の選択対象画像に対応した数字の配列を取得し、
前記認証判定手段は、前記解析手段により個別に識別された手指部位によって順に選ばれた複数の選択対象画像に対応した複数の数字の配列と、前記選択対象画像を順に選んだ手指部位の識別情報と、予め登録されている認証コードの数字の配列と、前記認証コードの各数字に対応して予めセキュリティレベルごとに登録されている手指部位の識別情報との一致判定により、前記認証対象者の認証判定を行うことを特徴とする請求項１記載の認

証処理装置。
【請求項５】
前記認証コードに用いられる複数のコード情報は０から９の数字であり、
前記画像表示手段は、前記複数の選択対象画像として０から９の数字の画像を前記画面内に配置して表示し、
前記解析手段は、前記検出対象物が認証対象者の手である場合に、各手指部位を個別に識別し、前記各手指部位のうち一つの手指部位による所定の動きが検出される毎に、前記手の全ての各手指部位に対応した選択対象画像の各数字と前記各数字にそれぞれ対応した各手指部位の各識別情報とからなる候補配列を取得し、
前記認証判定手段は、順に配列された各数字と前記各数字に対応した手指部位の各識別情報とが予め登録されている認証コードの中の前記配列の順番毎の数字及び識別情報と、前記所定の動きが検出された順番毎の前記候補配列の中の数字及び識別情報との一致判定により、前記認証対象者の認証判定を行うことを特徴とする請求項１記載の認証処理装置。
【請求項６】
前記認証コードに用いられる複数のコード情報は、少なくとも０から９の数字と所定の記号とを含み、
前記画像表示手段は、前記複数の選択対象画像として０から９の数字の画像を前記画面内に配置すると共に、前記数字の画像を除くエリアを前記所定の記号に対応した選択対象画像として表示し、
前記解析手段は、前記検出対象物が認証対象者の手である場合に、各手指部位を個別に識別し、前記各手指部位のうち一つの手指部位による所定の動きが検出される毎に、前記手の全ての各手指部位に対応した選択対象画像の各数字又は記号と前記各数字又は記号にそれぞれ対応した各手指部位の各識別情報とからなる候補配列を取得し、
前記認証判定手段は、順に配列された各数字又は記号と前記各数字又は記号にそれぞれ対応した手指部位の各識別情報とが登録されている認証コードの中の前記配列の順番毎の数字及び識別情報と、前記所定の動きが検出された順番毎の前記候補配列の中の数字又は記号及び識別情報との一致判定により、前記認証対象者の認証判定を行うことを特徴とする請求項１記載の認証処理装置。
【請求項７】
前記仮想平面設定手段は、Ｘ軸とＹ軸とＺ軸で表される前記三次元空間内に、前記Ｘ軸とＹ軸とＺ軸の何れか二つの座標軸で表される前記仮想二次元平面を設定しており、
前記解析手段は、前記三次元空間内で前記識別された部位が静止した時間を計測し、前記部位が所定の時間だけ静止したことを検出したとき、前記三次元空間内にて前記仮想二次元平面と直交する座標軸の方向で前記部位の先端から所定距離だけ離れた座標値に所定の判定座標を設定し、前記三次元空間内で前記部位が動いたことで前記部位の先端が前記判定座標に達したときに、前記所定の動きを検出することを特徴とする請求項１乃至６のうち何れか１項に記載の認証処理装置。
【請求項８】
前記仮想平面設定手段は、Ｘ軸とＹ軸とＺ軸で表される前記三次元空間内に、前記Ｘ軸とＹ軸とＺ軸の何れか二つの座標軸で表される前記仮想二次元平面を設定しており、
前記解析手段は、前記三次元空間内にて前記仮想二次元平面と直交する座標軸の、当該仮想二次元平面内での座標を基準座標にすると共に当該基準座標に対して正側と負側を設定し、前記識別された部位の先端が前記基準座標に対して正側から前記基準座標を超えて負側へ移動したときに、前記所定の動きを検出することを特徴とする請求項１乃至６のうち何れか１項に記載の認証処理装置。
【請求項９】
前記解析手段は、前記三次元空間内で前記識別された各部位が静止した時間を計測し、前記各部位が所定の時間だけ静止したことを検出した後、前記三次元空間内で前記各部位の先端が動いた際の移動量が最も大きい部位を、前記所定の動きが検出された部位とする

ことを特徴とする請求項１乃至６のうち何れか１項に記載の認証処理装置。
【請求項１０】
前記画像表示手段は、前記検出対象物の三次元座標に基づいて、前記画像表示手段の画面上に前記検出対象物に対応した所定のマークを表示することを特徴とする請求項１乃至９のうち何れか１項に記載の認証処理装置。
【請求項１１】
前記画像表示手段の画面上に当該画面の表示画像を反射する反射板、若しくは、前記画面の表示画像を空中に仮想的な立体像として形成する光学結像プレートを配することを特徴とする請求項１乃至１０のうち何れか１項に記載の認証処理装置。
【請求項１２】
前記座標検出手段は、赤外光を出射して前記検出対象物により反射された赤外光を撮像した撮像信号に基づいて、前記三次元座標を算出することを特徴とする請求項１乃至１１のうち何れか１項に記載の認証処理装置。
【請求項１３】
三次元空間内における検出対象物の三次元座標を所定の時間周期ごとに検出する座標検出手段と、
認証コードに用いられる複数のコード情報にそれぞれ対応した複数の選択対象画像を画面内に表示する画像表示手段と、
前記三次元空間内に仮想二次元平面を設定するとともに、前記画面内における前記複数の選択対象画像の表示座標と仮想二次元平面内における仮想座標とを対応させる仮想平面設定手段と、
前記検出対象物の三次元座標を解析することにより、前記検出対象物の座標が前記仮想二次元平面内で前記仮想座標に対応している状態で、前記三次元空間内にて前記検出対象物による所定の動きを検出したとき、前記選択対象画像が選ばれたと判断する解析手段と、
前記解析手段で選ばれたと判断された選択対象画像に対応したコード情報と、予め登録されている認証コードのコード情報とに基づいて、認証判定を行う認証判定手段と
を有することを特徴とする認証処理装置。
【請求項１４】
認証処理装置が実行する認証処理方法であって、
三次元空間内における検出対象物の三次元座標を所定の時間周期ごとに検出する座標検出ステップと、
認証コードに用いられる複数のコード情報にそれぞれ対応した複数の選択対象画像を画面内に表示する画像表示ステップと、
前記三次元空間内に仮想二次元平面を設定するとともに、前記画面内における前記複数の選択対象画像の表示座標と仮想二次元平面内における仮想座標とを対応させる仮想平面設定ステップと、
前記検出対象物の三次元座標を解析することにより、前記検出対象物を構成している複数の部位を識別し、前記識別した部位の座標が前記仮想二次元平面内で前記仮想座標に対応している状態で、前記三次元空間内にて前記識別した部位による所定の動きを検出したとき、前記識別した部位により前記選択対象画像が選ばれたと判断する解析ステップと、
前記解析ステップで選ばれたと判定された選択対象画像に対応したコード情報と、予め登録されている認証コードのコード情報とに基づいて、認証判定を行う認証判定ステップと
を含むことを特徴とする認証処理方法。
【請求項１５】
認証処理装置が実行する認証処理方法であって、
三次元空間内における検出対象物の三次元座標を所定の時間周期ごとに検出する座標検出ステップと、
認証コードに用いられる複数のコード情報にそれぞれ対応した複数の選択対象画像を画

面内に表示する画像表示ステップと、
前記三次元空間内に仮想二次元平面を設定するとともに、前記画面内における前記複数の選択対象画像の表示座標と仮想二次元平面内における仮想座標とを対応させる仮想平面設定ステップと、
前記検出対象物の三次元座標を解析することにより、前記検出対象物の座標が前記仮想二次元平面内で前記仮想座標に対応している状態で、前記三次元空間内にて前記検出対象物による所定の動きを検出したとき、前記選択対象画像が選ばれたと判断する解析ステップと、
前記解析ステップで選ばれたと判定された選択対象画像に対応したコード情報と、予め登録されている認証コードのコード情報とに基づいて、認証判定を行う認証判定ステップと
を含むことを特徴とする認証処理方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、認証対象者の個人認証を行う認証処理装置及び認証処理方法に関するものである。
【背景技術】
【０００２】
従来より、銀行ＡＴＭなどにおいて、個人認証は、暗証番号として登録されている４桁のＰＩＮ（Ｐｅｒｓｏｎａｌ　Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ　Ｎｕｍｂｅｒ）コードの入力を認証対象者に対して求め、その認証対象者から入力されたＰＩＮコードが正しいか否かを判定することにより行われている。
【０００３】
また、一般的な銀行ＡＴＭは、テンキー画像等を表示するディスプレイ装置にタッチセンサが併設されており、ディスプレイ画面上を認証対象者がタッチしたときに、タッチセンサがそのタッチ位置を検出して何れのキー画像がタッチされたのかを判断することにより、どの数字が入力されたかを識別している。なお、数字等の入力装置として、例えば特許文献１には、非接触による入力を検知可能な装置が開示されている。
【先行技術文献】
【特許文献】
【０００４】
【特許文献１】特許第５５０９３９１号公報
【発明の概要】
【発明が解決しようとする課題】
【０００５】
ところで、従来の暗証番号を用いた個人認証は、例えば暗証番号を入力している様子が盗撮されたり背後から盗み見られたりすることで暗証番号が盗まれる虞がある。すなわち、暗証番号を用いた個人認証は、盗撮や盗み見という比較的簡単な方法で暗証番号が盗まれる虞があるため、セキュリティ性が高いとは言い難い。そして、暗証番号が盗まれた上に、例えばスキミング等によりカード情報が盗まれて偽造カードが作成されてしまうと、被害者は多大な損害を被ることになる可能性が高い。
【０００６】
このようなことから、近年は、例えば指紋や手の静脈模様、虹彩などに基づくバイオメトリクス情報を利用した個人認証を用いることで、高いセキュリティ性を確保した個人認証が行われるケースも増えてきている。
【０００７】
しかしながら、バイオメトリクス情報による認証は、セキュリティ性が高く安全、安心ではあるが、指紋センサや静脈センサ、虹彩センサのような特殊な認証用センサが必要になり、その導入コストはかなりの高額となる。

【０００８】
また例えば指紋を用いた場合において、例えば表面が非常に滑らかな金属やガラス等を指先で触れたような時に、それらガラス等の表面に皮脂による指紋パターンが残ってしまうこともあり、その指紋パターンが盗まれることも考えられる。また、手の静脈模様についても、例えば赤外線カメラなどにより撮影されることで静脈パターンが盗まれてしまう虞がある。
【０００９】
さらに、指紋等の生体情報は、各人に対して唯一の情報であって代替ができない情報であるため、例えばその情報が何らかの方法で盗まれてしまうと、新たに認証情報を登録し直すようなことが非常に難しくなるという問題もある。
【００１０】
その他にも、指紋を認証に使用する場合は指紋採取が行なわれることになるが、指紋採取に対して抵抗感を抱く人も多い。バイオメトリクス情報として指紋や手の静脈などの情報を用いる場合、認証対象者は、認証機器が備えている認証用センサ上に手指や手掌を接触させなければならない。しかしながら、不特定多数の人が触れた認証用センサに触れることに対して嫌悪感を抱く人が少なくなくない。
【００１１】
本発明はこのような問題点に鑑みてなされたものであり、認証用センサ等に触れることなく、非常に高いセキュリティ性を確保した個人認証を可能とする認証処理装置及び認証処理方法を提供することを目的とする。
【課題を解決するための手段】
【００１２】
本発明の認証処理装置は、三次元空間内における検出対象物の三次元座標を所定の時間周期ごとに検出する座標検出手段と、認証コードに用いられる複数のコード情報にそれぞれ対応した複数の選択対象画像を画面内に表示する画像表示手段と、前記三次元空間内に仮想二次元平面を設定するとともに、前記画面内における前記複数の選択対象画像の表示座標と仮想二次元平面内における仮想座標とを対応させる仮想平面設定手段と、前記検出対象物の三次元座標を解析することにより、前記検出対象物を構成している複数の部位を識別し、前記識別した部位の座標が前記仮想二次元平面内で前記仮想座標に対応している状態で、前記三次元空間内にて前記識別した部位による所定の動きを検出したとき、前記識別した部位により前記選択対象画像が選ばれたと判断する解析手段と、前記解析手段で選ばれたと判断された選択対象画像に対応したコード情報と、予め登録されている認証コードのコード情報とに基づいて、認証判定を行う認証判定手段とを有することを特徴とする。
【００１３】
また、本発明の認証処理装置は、三次元空間内における検出対象物の三次元座標を所定の時間周期ごとに検出する座標検出手段と、認証コードに用いられる複数のコード情報にそれぞれ対応した複数の選択対象画像を画面内に表示する画像表示手段と、前記三次元空間内に仮想二次元平面を設定するとともに、前記画面内における前記複数の選択対象画像の表示座標と仮想二次元平面内における仮想座標とを対応させる仮想平面設定手段と、前記検出対象物の三次元座標を解析することにより、前記検出対象物の座標が前記仮想二次元平面内で前記仮想座標に対応している状態で、前記三次元空間内にて前記検出対象物による所定の動きを検出したとき、前記選択対象画像が選ばれたと判断する解析手段と、前記解析手段で選ばれたと判断された選択対象画像に対応したコード情報と、予め登録されている認証コードのコード情報とに基づいて、認証判定を行う認証判定手段とを有することを特徴とする。
【００１４】
また、本発明の認証処理方法は、三次元空間内における検出対象物の三次元座標を所定の時間周期ごとに検出する座標検出ステップと、認証コードに用いられる複数のコード情報にそれぞれ対応した複数の選択対象画像を画面内に表示する画像表示ステップと、前記

三次元空間内に仮想二次元平面を設定するとともに、前記画面内における前記複数の選択対象画像の表示座標と仮想二次元平面内における仮想座標とを対応させる仮想平面設定ステップと、前記検出対象物の三次元座標を解析することにより、前記検出対象物を構成している複数の部位を識別し、前記識別した部位の座標が前記仮想二次元平面内で前記仮想座標に対応している状態で、前記三次元空間内にて前記識別した部位による所定の動きを検出したとき、前記識別した部位により前記選択対象画像が選ばれたと判断する解析ステップと、前記解析ステップで選ばれたと判定された選択対象画像に対応したコード情報と、予め登録されている認証コードのコード情報とに基づいて、認証判定を行う認証判定ステップとを含むことを特徴とする。

【００１５】

また、本発明の認証処理方法は、三次元空間内における検出対象物の三次元座標を所定の時間周期ごとに検出する座標検出ステップと、認証コードに用いられる複数のコード情報にそれぞれ対応した複数の選択対象画像を画面内に表示する画像表示ステップと、前記三次元空間内に仮想二次元平面を設定するとともに、前記画面内における前記複数の選択対象画像の表示座標と仮想二次元平面内における仮想座標とを対応させる仮想平面設定ステップと、前記検出対象物の三次元座標を解析することにより、前記検出対象物の座標が前記仮想二次元平面内で前記仮想座標に対応している状態で、前記三次元空間内にて前記検出対象物による所定の動きを検出したとき、前記選択対象画像が選ばれたと判断する解析ステップと、前記解析ステップで選ばれたと判定された選択対象画像に対応したコード情報と、予め登録されている認証コードのコード情報とに基づいて、認証判定を行う認証判定ステップとを含むことを特徴とする。

【発明の効果】

【００１６】

本発明によれば、認証センサ等に触れることなく、非常に高いセキュリティ性を確保した個人認証が可能となる。

【図面の簡単な説明】

【００１７】

【図１】第１,第２の実施形態の認証処理装置の概観の一例を示す模式図である。

【図２】バーチャルタッチパネル内にランダム配置される仮想キーの一配置例を示す図である。

【図３】ランダム配置されるキー画像の例を示す図である。

【図４】第１の実施形態の情報処理装置の各処理、制御、ハードウェア構成をそれぞれ機能ごとに分けた機能ブロック図である。

【図５】第１の実施形態の情報処理装置がＰＩＮコードを利用して認証対象者の個人認証を行う際の処理及び制御の流れをフローチャートである。

【図６】距離センサのセンサ面上の赤外線ＬＥＤと赤外線カメラの配置例を示す図である。

【図７】距離センサの有効範囲の説明に用いる図である。

【図８】距離センサのセンサ面上の三次元空間の座標説明に用いる図である。

【図９】バーチャルタッチパネル内で行われるエアクリックの説明に用いる図である。

【図１０】バーチャルタッチパネル内で行われるフェイククリックの説明に用いる図である。

【図１１】第１の実施形態の情報処理装置のメモリ部に格納されるテーブル情報の一例を示す図である。

【図１２】ディスプレイ画面の上に反射板を設置した構成例を示す図である。

【図１３】ディスプレイ画面の上に光学結像プレートを設置した構成例を示す図である。

【図１４】第２の実施形態の情報処理装置の各処理、制御、ハードウェア構成をそれぞれ機能ごとに分けた機能ブロック図である。

【図１５】第２の実施形態の情報処理装置がＰＩＮコードと指識別情報を利用して認証対象者の個人認証を行う際の処理及び制御の流れをフローチャートである。

【図１６】検出対象物である手をモデル化して説明する図である。
【図１７】第２の実施形態の情報処理装置のメモリ部に格納されるテーブル情報の一例を示す図である。
【図１８】第２の実施形態の情報処理装置がＰＩＮコードと指識別情報を用いて個人認証を行う際のＰＩＮコードと指識別情報の一例を示す図である。
【図１９】第３の実施形態における情報処理装置と距離センサとバーチャルタッチパネルの位置関係の説明に用いる図である。
【図２０】第３の実施形態におけるディスプレイの画面と距離センサとバーチャルタッチパネルの位置関係の説明に用いる図である。
【図２１】第３の実施形態において指先が静止した後に設定される各エアクリック判定座標と各指先座標の関係説明に用いる図である。
【図２２】第３の実施形態の情報処理装置の各処理、制御、ハードウェア構成をそれぞれ機能ごとに分けた機能ブロック図である。
【図２３】第３の実施形態の情報処理装置がＰＩＮコードと指識別情報を利用して認証対象者の個人認証を行う際の処理及び制御の流れをフローチャートである。
【図２４】第４の実施形態の場合の各仮想キーと認証対象者の親指～小指の五つの各指先の位置の一例を示す図である。
【図２５】第４の実施形態の場合に４回のエアクリックで得られる候補コードの例を示す図である。
【図２６】第５の実施形態の場合の各仮想キーと認証対象者の親指～小指の五つの各指先の位置の一例を示す図である。
【図２７】第５の実施形態の場合に４回のエアクリックで得られる候補コードの例を示す図である。
【図２８】本実施形態の認証処理装置が適用されて、サーバによりセキュリティ管理がなされるシステムの概略的な構成例を示す図である。
【発明を実施するための形態】
【００１８】
＜第１の実施形態＞
図１は、本発明の第１の実施形態の認証処理装置１の概観の一例を示す図である。図１に示すように、本実施形態に係る認証処理装置１は、ディスプレイ１１を備えていると共に仮想平面設定手段と解析手段と認証判定手段の機能を実現するための構成の一例である情報処理装置１０と、座標検出手段の機能を実現するための構成の一例である距離センサ２０とを有して構成されている。情報処理装置１０と距離センサ２０は、信号ケーブル若しくは無線により接続されている。
【００１９】
距離センサ２０は、検出対象物の三次元空間内における三次元座標を所定の時間周期ごとに検出するための座標検出手段の機能の一部を担っており、座標検出手段は、当該距離センサ２０と情報処理装置１０内の後述する座標算出部１１１により構成されている。また、ディスプレイ１１は、認証コードに用いられる複数のコード情報にそれぞれ対応した複数の選択対象画像を画面内に表示する画像表示手段の一例である。情報処理装置１０は、三次元空間内に仮想二次元平面を設定するとともに、前記画面内における前記複数の選択対象画像の表示座標と前記仮想二次元平面内における仮想座標とを対応させる仮想平面設定手段と、前記検出対象物の三次元座標を解析することにより、前記検出対象物の検出座標が前記二次元平面で前記仮想座標に対応している状態で、前記三次元空間内において前記検出対象物による所定の動きを検出したとき、認証対象者により前記選択対象画像が選ばれたと判断する解析手段と、前記解析手段で選ばれたと判断された選択対象画像に対応したコード情報と、予め登録されている認証コードのコード情報とに基づいて、認証判定を行う認証判定手段としての各機能を実現する装置の一例である。
【００２０】
本実施形態の認証処理装置１において、認証対象者の個人認証が、例えば４桁の数字が

コード情報として用いられる認証コードの一例であるＰＩＮコードにより行われる場合、情報処理装置１０は、その認証対象者から入力された４桁の数字からなるコード情報と、予め登録されている正規ユーザのＰＩＮコードとを比較し、それらが一致した場合に、当該認証対象者が正規のユーザであると認証する。

【００２１】

ここで、ＰＩＮコードを利用した個人認証を行う場合、情報処理装置１０は、先ず、認証対象者が予め登録されている複数ユーザのうちの一人であるか否かを判定するユーザ確認処理を行う。なお、予め登録されているユーザが一人のみである場合、ユーザ確認のための判定は省略することができる。予め登録されているユーザが複数である場合、例えばＰＩＮコードとは別に予め登録しておいたパスワード等を用いたユーザ確認や、予め各ユーザに配布している認証用カード等を用いたユーザ確認、或いは、各ユーザの生体情報等を用いたユーザ確認等を行うことができる。

【００２２】

そして、認証対象者が登録されたユーザの一人であると判定した時、情報処理装置１０は、距離センサ２０から供給される信号に基づいて、当該距離センサ２０のセンサ面２０Ｆの上方側の三次元空間に、仮想二次元平面の一例であるタッチパネル４０を設定する。以下の説明では、この仮想的なタッチパネル４０をバーチャルタッチパネル４０と表記する。当該バーチャルタッチパネル４０は、前記ディスプレイ１１の画面と仮想的に対応したパネルとして設定される。なお、バーチャルタッチパネル４０は、三次元空間内に仮想的に設定されるものであり、認証対象者や他の第三者が実際に見ることの出来るものではない。情報処理装置１０が前記距離センサ２０のセンサ面２０Ｆの上方側の三次元空間を、どのようにしてバーチャルタッチパネル４０として扱い得るのかについての詳細な説明は後述する。

【００２３】

次に、情報処理装置１０は、距離センサ２０から供給される信号に基づいて、認証対象者の手指の先端部（即ち、指先３１）などのように或る程度狭い範囲を指し示すことが可能な先端部を有する物体が、バーチャルタッチパネル４０の三次元空間内に存在するかを判断する。なお、この第１の実施形態の場合、前記先端部は手の指先に限定されず、例えばペン先などのように狭い範囲を指し示すことができるものであってもよい。そして、バーチャルタッチパネル４０の三次元空間内に前記指先３１等の先端部が存在している場合、情報処理装置１０は、ディスプレイ１１の画面上に、当該バーチャルタッチパネル４０上での指先３１等の先端部の位置に対応した指示マーク１３を表示する。また、情報処理装置１０は、バーチャルタッチパネル４０内で前記指先３１等が動かされた場合、当該指先３１の動きに同期させて、ディスプレイ１１の画面上の前記指示マーク１３の表示位置を移動させる。なお、バーチャルタッチパネル４０内での指先３１の動きと、ディスプレイ１１の画面上の指示マーク１３の同期表示の詳細な説明は後述する。

【００２４】

さらに、情報処理装置１０は、バーチャルタッチパネル４０の三次元空間内に指先３１等が存在していると判断した時、例えば「０～９」までの数字キーに対応したキー画像１２をディスプレイ１１の画面上に表示する。これらキー画像１２は、ディスプレイ１１の画面内に複数表示される選択対象画像の一例である。そして、本実施形態において、これらキー画像１２の画面上の配置は、ランダムな配置となされる。なお、図１のディスプレイ１１の画面例は、キー画像１２と指示マーク１３のみ表示されているが、それらと共に例えばキャンセルを指示するためのキャンセルキーも表示される。

【００２５】

また前述したように、バーチャルタッチパネル４０はディスプレイ１１の画面と仮想的に対応したパネルとなっているため、情報処理装置１０は、例えば図２に示すように、バーチャルタッチパネル４０の三次元空間内において、前記ディスプレイ１１の画面上にランダム配置された各キー画像１２にそれぞれ対応している位置に、仮想キーＶ１２を配置する。なお、これら仮想キーＶ１２についても、バーチャルタッチパネル４０と同様に、

三次元空間内に仮想的に配置されるものであり、認証対象者や他の第三者が実際に見ることの出来るものではない。また、前記ディスプレイ１１の画面上に表示されるキー画像１２は、図３の（ａ）～（ｃ）に一例として示すように、認証対象者に対する個人認証が行われる度に、それらの配置がランダムに変更される。したがって、バーチャルタッチパネル４０上における前記仮想キーＶ１２も、認証対象者に対する個人認証が行われる度にそれらの配置がランダムに変更される。なお、図２の例は、仮想キーＶ１２のみ描いているが、それらと共に例えばキャンセルの指示用の仮想キャンセルキーも配置される。

【００２６】

また、情報処理装置１０は、認証対象者が例えば手３０の指先３１等の先端部により、前記バーチャルタッチパネル４０上の所望の位置を指示する所定動作（所望の位置を指先３１等の先端部で突くような所定の動き）が行われた時、ユーザがその位置をクリックしたと認識する。なお、本実施形態では、バーチャルタッチパネル４０上の所望の位置を指示する所定の動作として、当該所望の位置を指先３１等の先端部で押すような動き（或いは、押し込む動作、突く動作）を例に挙げる。本実施形態では、前記先端部により所望の位置を指示するための所定の動きを、以下の説明ではエアクリックと表記する。情報処理装置１０は、距離センサ２０から供給される信号に基づいて、前記バーチャルタッチパネル４０の三次元空間内で前記エアクリックが行われたかを認識するが、その詳細な説明は後述する。また、エアクリックが確実に行われたかどうかについては、例えばディスプレイ１１の画面上にエアクリック完了通知用の所定の表示を行ったり、エアクリック完了通知用の所定の音を発生させるなどして、認証対象者へ知らせることも可能である。或いは、第三者への秘匿性を高めるために、それら通知が全く行われなくてもよい。

【００２７】

そして、情報処理装置１０は、認証対象者が前記バーチャルタッチパネル４０内の仮想キーＶ１２に対した位置でエアクリックを行い、そのエアクリックによってＰＩＮコードの正しい４桁の数字が順に入力されたとき、その認証対象者は正規のユーザであると判断する。

【００２８】

図４には、情報処理装置１０の概略的な構成を示している。図４の示した各構成は、本実施形態の情報処理装置１０にて行われる各処理や制御、実際のハードウェア構成をそれぞれ機能ごとに分けた機能ブロックとして表したものである。なお、図４には距離センサ２０も描かれている。また、図４において、表示部（ディスプレイ１１）は情報処理装置１０の外部に設けられていてもよいし、メモリ部１０７内に記憶されている情報は外部の記憶装置に格納されていてもよい。

【００２９】

図５には、ＰＩＮコードを利用して認証対象者の個人認証を行う際の情報処理装置１０の処理及び制御の流れをフローチャートにより示している。以下、図４の各構成の動作及び処理と制御について、図５のフローチャートを参照しながら説明する。

【００３０】

先ず、認証対象者の個人認証が行われる場合、情報処理装置１０のユーザ確認部１０６は、ステップＳ１の処理として、認証対象者が予め登録されている複数ユーザのうちの一人であるか否かのユーザ確認のための判定を行う。このユーザ確認の判定処理は、前述したように、パスワードや認証用カード、ユーザの生体情報等を用いて行われる。これらユーザ確認のための処理は既存の処理と同じであるため、その詳細な説明は省略する。

【００３１】

ステップＳ１において認証対象者が登録ユーザでないと判定された場合、制御部１０５は、ステップＳ１２として、認証は否定（ＮＧ）されたとして認証ＮＧ処理を行う。制御部１０５は、ステップＳ１２の認証ＮＧ処理として、例えばそれ以前の処理で取得された情報を全てクリアした後、処理をステップＳ１１へ進める。ステップＳ１１の処理へ進むと、制御部１０５の表示制御部１２１は、ディスプレイ１１の画面上に認証ＮＧ等の表示を行う。なお認証ＮＧの通知は音声により行われてもよい。一方、ステップＳ１において

認証対象者が登録ユーザであると判定された場合、制御部１０５は、ステップＳ２の処理として、距離センサ出力解析部１０２で行われる解析結果を基に、指先３１等のような狭い範囲を指し示すことのできる先端部が前記バーチャルタッチパネル４０の三次元空間内に存在しているか判断する。

【００３２】

ここで、距離センサ出力解析部１０２で行われる処理の詳細を述べる前に、距離センサ２０の構成と当該距離センサ２０から得られる信号について説明する。距離センサ２０は、図６に示すように、センサ面２０Ｆの側に、例えば三つの赤外線ＬＥＤ２２Ｌ，２２Ｃ，２２Ｒと、二つの赤外線カメラ２１Ｌ，２１Ｒが配されて構成されている。赤外線ＬＥＤ２２Ｌ，２２Ｃ，２２Ｒから出射された赤外光は、当該距離センサ２０のセンサ面２０Ｆ側に何らかの検出対象物が存在していた場合、その検出対象物により反射されて、赤外線カメラ２１Ｌ，２１Ｒへ入射する。赤外線カメラ２１Ｌ，２１Ｒは、それぞれ撮像光学系と撮像素子を備えており、検出対象物にて反射された赤外光からなる光像を、所定の時間周期ごとに撮像する。なお、本実施形態の場合、所定の時間周期は、一例として２９０ｆｐｓ（フレーム／秒）のフレームレートとなされている。

【００３３】

なお、距離センサ２０において、赤外線ＬＥＤ２２Ｌ，２２Ｃ，２２Ｒから出射された赤外光が検出対象物で反射されて赤外線カメラ２１Ｌ，２１Ｒが受光できる有効範囲は、例えば図７に示すように、センサ面２０Ｆ上での赤外線カメラ２１Ｌ，２１Ｒの中間点２０Ｃから、例えば２５ｍｍ～６００ｍｍまでの距離範囲ＤＲ内で且つ広がり角θが１５０度の逆ピラミッド状の範囲となされている。上述した距離センサ２０は、赤外線カメラ２１Ｌ，２１Ｒの撮像信号を、情報処理装置１０へ出力する。

【００３４】

距離センサ２０から出力された撮像信号は、本実施形態の情報処理装置１０の距離センサ出力受信部１０１により受信される。距離センサ出力受信部１０１は、距離センサ２０と情報処理装置１０との間を接続する信号ケーブル或いは無線等の通信方式に応じた受信部となっている。当該距離センサ出力受信部１０１にて受信された撮像信号は、距離センサ出力解析部１０２へ送られる。

【００３５】

距離センサ出力解析部１０２は、例えば、座標算出部１１１と対象認識部１１２と先端座標情報取得部１１３とＺ座標判定部１１４とを有して構成されている。座標算出部１１１は、距離センサ２０の二つの赤外線カメラ２１Ｌ，２１Ｒからの撮像信号の画像解析を行うことにより、図７及び図８に示すように、距離センサ２０の前記有効範囲内のＸ軸、Ｙ軸、Ｚ軸で表される三次元空間における検出対象物（図８の例では前記指先３１）の三次元座標を算出する。なお、距離センサ２０から供給される撮像信号は前述のように２９０ｆｐｓのフレームレートの信号となされているため、座標算出部１１１は、フレームごとに指先３１の三次元座標を算出する。また、座標算出部１１１は、検出対象物が複数存在する場合であっても、或いは、一つの検出対象物内にそれぞれ異なる動きをする複数の部位が存在する場合であっても、それらについてそれぞれの三次元座標を算出する。座標算出部１１１にて算出されたフレームごとの三次元座標情報は、対象認識部１１２へ送られる。

【００３６】

対象認識部１１２は、前記フレームごとの三次元座標情報を基に、前記距離センサ２０の有効範囲内の三次元空間における検出対象物がどのようなものであるかを認識する。ここで、距離センサ２０の赤外線カメラにより、例えば図１中の手３０の指先３１などのように或る程度狭い範囲を指し示すことが可能な先端部を有する物体が撮像されているとする。この場合、対象認識部１１２は、前記撮像信号と前記座標算出部１１１でフレームごとに算出された三次元座標とから、前記検出対象物の少なくとも当該先端部を認識する。すなわち、図１や図８の例の場合、対象認識部１１２は、手３０の少なくとも指先３１を認識する。なお、詳細については第２の実施形態において後述するが、対象認識部１１２

は、検出対象物として人の手が撮像されている場合、当該手を構成している手掌と５本の手指、及びそれら５本の手指の先端部（指先）や関節等もそれぞれ認識可能となされている。

【００３７】

対象認識部１１２にて検出対象物の先端部が認識されると、先端座標情報取得部１１３は、前記座標算出部１１１にて算出された三次元座標の中から、前記先端部の座標情報を取得する。この先端座標情報取得部１１３は、当該先端部の座標情報を取得すると、その座標情報を制御部１０５へ送る。すなわち、図５のステップＳ２において、制御部１０５は、距離センサ出力解析部１０２の対象認識部１１２による対象認識結果により、指先３１等のような先端部が前記バーチャルタッチパネル４０の三次元空間内に存在しているか判断可能となる。

【００３８】

図５のフローチャートへ説明を戻し、前記ステップＳ２にてバーチャルタッチパネル４０の三次元空間内に先端部が存在すると判定した場合、制御部１０５は、処理をステップＳ３へ進め、一方、バーチャルタッチパネル４０の三次元空間内に先端部が存在しないときにはステップＳ２の判定処理を繰り返す。

【００３９】

ステップＳ３へ処理を進めると、制御部１０５のキー配列制御部１２２は、前述したようにディスプレイ１１上にランダム配置するキー画像１２のデータを生成し、表示制御部１２１を介してそれらキー画像１２をディスプレイ１１の画面上に表示する。

【００４０】

その後、制御部１０５は、距離センサ出力解析部１０２の解析結果から、認証対象者がバーチャルタッチパネル４０を通じて入力した認証用の４桁分の数字を取得するための、ステップＳ４からステップＳ８の処理へ移行する。

【００４１】

ステップＳ４へ処理を進めると、制御部１０５は、距離センサ出力解析部１０２の先端座標情報取得部１１３に対し、バーチャルタッチパネル４０上で前記先端部の座標を取得させる。すなわち、このときの先端座標情報取得部１１３は、前記対象認識部１１２が認識した先端部の座標を取得する。

【００４２】

またこのとき、制御部１０５の表示制御部１２１は、指先３１等の先端部の座標情報を基に、ディスプレイ１１の画面上に表示する指示マーク１３の画像を生成する。なお、指先３１が三次元空間内で動かされている場合、指先３１等の先端部の座標値は、赤外線カメラ２１Ｌ，２１Ｒで撮像されるフレームごとに刻々と変化することになる。このため、ディスプレイ１１の画面上での指示マーク１３の表示位置は、三次元空間内での指先３１の動きに同期して変更されることになる。

【００４３】

さらに、制御部１０５は、ステップＳ５の処理として、先端座標情報取得部１１３が取得した先端部の座標が、バーチャルタッチパネル４０の三次元空間内に配置された何れかの仮想キーＶ１２の座標と一致したか判断する。なおこの場合の一致判定は、先端部のＸ，Ｙ座標が、仮想キーＶ１２のＸ，Ｙ座標の範囲内であるかの一致判定となる。そして、制御部１０５は、先端部の座標が、仮想キーＶ１２の座標と一致したと判断したときにはステップＳ６へ処理を進め、一方、一致していないと判断したときにはステップＳ４へ処理を戻す。

【００４４】

なお、前記仮想キーＶ１２は、実際には認証対象者から見えず且つ三次元空間上に仮想的に設定されるものであるため、認証対象者は前記先端部を仮想キーＶ１２の位置に正確に合わせ難いことも考えられる。この場合、一例として、前記仮想キーＶ１２の座標の周囲に所定の大きさの検出範囲を設定しておき、制御部１０５は、その検出範囲内に前記先端部の座標が入っているときに、当該先端部の座標が仮想キーＶ１２の座標に一致したと

判断してもよい。

【００４５】

次に、制御部１０５は、Ｚ座標判定部１１４でのＺ座標判定結果に基づいて、バーチャルタッチパネル４０上でエアクリックが行われたか判断する。ここで、Ｚ座標判定部１１４で行われるＺ座標判定処理について、図８と図９及び図１０を参照して説明する。Ｚ座標判定部１１４は、前記座標算出部１１１が算出した三次元座標のうち、距離センサ２０の前記センサ面２０Ｆの上方側三次元空間のＺ座標について基準座標を設定すると共に、そのＺ基準座標に対して正側（＋側）のＺ座標と、負側（－側）のＺ座標とを設定する。なお、図９、図１０の例では、バーチャルタッチパネル４０を、格子状の升目が配されたスクリーンとして描いているが、これらはパネルとその座標を判り易くするために描いているだけであり、それらは認証対象者から見えるものではない。

【００４６】

図８の例の場合、Ｚ座標軸は、Ｘ軸とＹ軸を含む仮想二次元平面であるバーチャルタッチパネル４０に対して直交する奥行き方向の座標軸となっており、基準座標（Ｚ＝０）は一例として、距離センサ２０のセンサ面２０Ｆの中央に相当するＺ座標となされている。また図８の例の場合、正側（＋側）のＺ座標は基準座標（Ｚ＝０）に対して手前側（認証対象者に近い方）、負側（－側）のＺ座標は基準座標（Ｚ＝０）に対して奥行き側（認証対象者から遠い方）となっている。

【００４７】

そして、Ｚ座標判定部１１４は、対象認識部１１２が認識した前記検出対象物の先端部のＺ座標が、図９に示すように、前記正側（＋側）から前記基準座標（Ｚ＝０）を通り過ぎて負側（－側）に変化したか否か判定する。ここで、前記先端部のＺ座標の変化があったと判定した時、Ｚ座標判定部１１４は、判定検出信号を制御部１０５へ送る。なお、Ｚ座標判定部１１４は、前記先端部のＺ座標が、前記正側（＋側）から前記基準座標（Ｚ＝０）を通り過ぎて負側（－側）に変化した後に、さらに例えば予め決められた時間内に正側（＋側）へ戻るように変化したか否かを判定してもよい。

【００４８】

そして、ステップＳ６において、前記Ｚ座標判定部１１４から当該判定検出信号を受け取ると、制御部１０５は、エアクリックが行われたと判断する。なお、エアクリックが行われていない場合、制御部１０５は、ステップＳ４へ処理を戻す。

【００４９】

このように、本実施形態においては、例えば図９に示したように、指先３１等の先端部のＺ座標が、前記正側（＋側）から基準座標（Ｚ＝０）を通り過ぎて負側（－側）に変化した後、さらに例えば正側（＋側）へ戻る変化であったときに、エアクリックがなされたと判断される。このため、例えば図１０に示すように、バーチャルタッチパネル４０上で、認証対象者が、指先３１等の先端部をＺ軸方向へ押し込む動作を行ったとしても、その際の前記先端部の押し込み動作が例えばＺ軸座標の正側（＋側）でのみ行われた場合には、エアクリックが行われたと判断しない。すなわち、指先３１等の押し込み動作が例えばＺ座標の正側（＋側）でのみ行われた場合、第三者からはエアクリックが行われているように見えているが、実際にはエアクリックは行われていないことになる。本実施形態では、このような見かけ上のエアクリック（フェイクエアクリック）が可能となされている。

【００５０】

なお、Ｚ座標軸の基準座標は、センサ面２０Ｆの中央に相当するＺ座標に限定されず、それよりも認証対象者側により近いＺ座標となされてもよいし、逆に遠いＺ座標となされてもよい。また、詳細は後述する第３の実施形態において説明するが、エアクリックが行われたか判断する際に使用する座標は、Ｚ座標軸で予め固定的に決められた基準座標に限定されない。すなわち、エアクリックが行われたか判断する際に使用する座標は、例えば認証対象者の手３０の指先３１がバーチャルタッチパネル４０の三次元空間内で検出された後、その手３０若しくは指先３１が三次元空間内で所定の時間だけ静止したときのＺ座標から、指先方向で且つＺ軸方向に所定距離だけ離れた座標に設定可能である。言い換え

ると、エアクリックの判定に使用される座標は、手３０若しくは指先３１が三次元空間内で静止したときのＺ座標に応じた可変の座標として設定可能である。

【００５１】

次に、ステップＳ６にてエアクリックが行われたと判断して、ステップＳ７へ処理を進めると、制御部１０５は、入力情報判定部１０３に対し、エアクリックにより入力された座標に対応した数字を、配列ＰＩＮ（ｎ）として保管させた後、「ｎ」に「１」を加えて、ステップＳ８へ処理を進める。

【００５２】

ステップＳ８へ処理が進むと、制御部１０５は、入力情報判定部１０３が保管している配列ＰＩＮ（ｎ）の「ｎ」が「ｍ」となったか否か判定する。なお「ｍ」は、ＰＩＮコードが４桁である場合は「４」となる。したがって、制御部１０５は、「ｎ」が「４」になるとステップＳ９へ処理を進める。すなわち、「ｎ」が「４」になったとき、入力情報判定部１０３が配列ＰＩＮ（ｎ）として保管している数字は４桁の数字となり、この４桁の数字が、バーチャルタッチパネル４０を用いて認証対象者により入力された数字となる。

【００５３】

次に、処理をステップＳ９へ進めると、制御部１０５は、入力情報判定部１０３に対し、例えばメモリ部１０７に保存されているユーザごとのＰＩＮコードの数字の配列と、前記バーチャルタッチパネル４０を介して認証対象者により入力された数字の配列が完全に一致しているか否か判定させる。

【００５４】

ここで、メモリ部１０７には、一例としてユーザ情報１３１とＰＩＮコード１３２が対応付けられたテーブル情報が登録されている。当該テーブル情報は、一例として図１１に示すように、複数のユーザをそれぞれ表すユーザ情報Ｕ１，Ｕ２，Ｕ３，・・・と、各ユーザの登録ＰＩＮコードとが対応付けられて登録されたものである。入力情報判定部１０３には、先のステップＳ１のユーザ確認の際に登録済みと判定されたユーザのＰＩＮコードがメモリ部１０７から渡されており、したがって、入力情報判定部１０３は、ステップＳ９において、そのＰＩＮコードと前記認証対象者が入力した数字との一致判定を行う。

【００５５】

そして、入力情報判定部１０３が前記認証対象者の入力数字とＰＩＮコードとが一致したと判定すると、制御部１０５は、ステップＳ１０として、認証は確認（ＯＫ）されたとして認証ＯＫ処理を行う。制御部１０５は、ステップＳ９からステップＳ１０へ進んだ場合、例えばそれ以前の処理で取得された座標の情報や配列ＰＩＮ（ｎ）に保管した数字の情報等を全てクリアした後、処理をステップＳ１１へ進める。ステップＳ１０からステップＳ１１へ処理が進むと、制御部１０５の表示制御部１２１は、ディスプレイ１１の画面上に認証ＯＫ等の表示を行う。なお、認証ＯＫの通知は音声により行われてもよい。

【００５６】

一方、ステップＳ９において入力数字とＰＩＮコードが一致しないと判定された場合、制御部１０５は、ステップＳ１２へ処理を進めて認証ＮＧ処理を行う。ステップＳ９からステップＳ１２へ進んだ場合、制御部１０５は、それ以前の処理で取得した座標の情報や配列ＰＩＮ（ｎ）に保管した数字の情報等を全てクリアした後、ステップＳ１１へ処理を進める。そして、ステップＳ１２からこのステップＳ１１へ処理が進むと、表示制御部１２１は、ディスプレイ１１の画面上に認証ＮＧの表示を行う。

【００５７】

なお、本実施形態の認証処理装置１が例えば入室時の認証を行うための装置であり、認証結果に応じて図示しない電気錠の開閉を制御する場合、解錠制御部１０４は、ステップＳ１０において、入力情報判定部１０３における判定結果に基づいて電気錠の開閉を制御する。すなわち、認証対象者が正規のユーザである場合、解錠制御部１０４は、ステップＳ１０において、電気錠を開制御して当該ユーザの入室を可能にする。

【００５８】

図１や図９、図１０では、認証対象者から見てディスプレイ１１の画面が例えば正対し

ている例を挙げているが、例えば図１２や図１３に示すようにディスプレイ１１の画面は、認証対象者側から直接見えないように配置されてもよい。

【００５９】

図１２の例は、ディスプレイ１１の画面に対して例えば４５度に傾けて配置した反射板５１により、ディスプレイ１１の表示画像を反射し、その反射された画像を認証対象者が見る構成例を示している。なお、この図１２の例の場合、ディスプレイ１１上の表示は鏡像とする。この図１２の構成の場合、距離センサ２０は、反射板５１により反射されたディスプレイ画面を認証対象者が見ることになる位置の手前に配されることになり、したがって、バーチャルタッチパネル４０もその距離センサ２０の上方の三次元空間に配置されることになる。この図１２の構成の場合、ディスプレイ１１の表示画面上には反射板５１が設けられ、そのディスプレイ１１の表示画面は反射板５１で反射されることになるため、例えば盗撮用の小型隠しカメラをディスプレイ１１画面上に秘かに配置するようなことはできない。

【００６０】

図１３の例は、ディスプレイ１１の画面に対して例えば４５度傾けて配置され、そのディスプレイ１１の表示画像を空中に仮想的な立体像として形成する光学結像プレート５０を配した構成例を示している。なお光学結像プレート５０としては、一例として特開２０１３-１２７６２５号公報に開示されているような光学結像装置を用いることができる。この図１３の構成の場合、距離センサ２０は、光学結像プレート５０により仮想的な立体像が形成される位置に配されることになり、バーチャルタッチパネル４０も距離センサ２０の上方の三次元空間に配置されることになる。また、当該光学結像プレート５０は、プレート面から４５度を基軸として±２０度が視野角となっており、そのような狭い視野角の範囲内でしかディスプレイ１１の表示画面を見ることができない。このため、例えば認証対象者の肩越し或いは横からディスプレイ１１の表示画面を盗み見るようなことはできず、また、小型隠しカメラによる盗撮も不可能である。

【００６１】

以上説明したように、第１の実施形態の認証処理装置１によれば、三次元空間上に仮想的に配置したバーチャルタッチパネル４０上に、ランダムに配置された仮想キーを指先３１等でクリック（エアクリック）することでＰＩＮコードの入力がなされるため、実際に入力されている数字を、第三者に盗み見られたり、盗撮されたりすることが無く、非常に高いセキュリティ性を確保可能となっている。

【００６２】

また、本実施形態の認証処理装置１によれば、確実なエアクリック動作が行われたかどうかは認証対象者本人のみが認識でき、例えばフェイククリックを行うことで、第三者に何れの数字がＰＩＮコードの数字であるかを知られる虞がない。

【００６３】

また、本実施形態の認証処理装置１によれば、認証対象者は、バーチャルタッチパネル４０でエアクリックを行うだけであり、指先で実際にタッチパネル等に触れる必要が全くないため、指紋パターンなどの痕跡が残らず、指紋パターンを盗まれることがない。

【００６４】

さらに、本実施形態の認証処理装置１において、図１２に示した反射板５１や図１３に示したような光学結像プレート５０を配した構成を用いれば、第三者によるＰＩＮコードの盗み見や盗撮を有効に防止することができる。

【００６５】

また、本実施形態の認証処理装置１によれば、ディスプレイ画面の明るい表示を見ることができるため、十分な明るさが得られていない暗い環境であっても、認証対象者はＰＩＮコードの入力が可能となる。

【００６６】

＜第２の実施形態＞

次に、本発明の第２の実施形態の認証処理装置１について以下に説明する。なお、第２

の実施形態の認証処理装置１の概略的な構成は図１と同様である。また、第２の実施形態において、距離センサ２０やディスプレイ１１の画面表示、バーチャルタッチパネル４０、ディスプレイ１１の画面上にランダム配置されるキー画像１２とバーチャルタッチパネル４０内に配される仮想キーＶ１２の対応関係、エアクリックとフェイククリックの区別、反射板５１や光学結像プレート５０等は、第１の実施形態と同様である。

【００６７】

ここで、前述した第１の実施形態の場合、バーチャルタッチパネル４０上でエアクリックが検出される際の検出対象物は、或る程度狭い範囲を指し示すことができる先端部を有する物体であればよく、指先に限定されるものではない。また第１の実施形態において、例えば指先によりエアクリックを行うことにした場合、認証対象者は、手の親指から小指までの何れの手指をどのように使ってもよく、ＰＩＮコードの数字順に入力できればよい。

【００６８】

これに対し、第２の実施形態の認証処理装置１は、認証対象者の手の５本の手指をそれぞれ個別に認識し、また、ＰＩＮコードの各数字のうちいずれの数字がどの手指を使って入力されたかを個別に認識することにより、セキュリティ性能をさらに高めている。

【００６９】

このようなことを実現するため、第２の実施形態において例えば４桁のＰＩＮコードにより個人認証が行われる場合、認証処理装置１には、ＰＩＮコードの各数字とその数字に対応した手指の情報が予め登録されている。

【００７０】

また、認証処理装置１は、バーチャルタッチパネル４０を介して認証対象者から４桁の数字が入力されたとき、それら４桁の各数字がそれぞれ何れの手指を用いて入力されたのかを認識可能となされている。そして、認証処理装置１は、入力された各数字及びそれら数字を入力した各手指の情報と、ＰＩＮコードとして登録されている各数字及びそれら数字に対応して登録されている各手指の情報とを比較し、それらが全て一致した場合にのみ、認証対象者が正規のユーザであると認証する。

【００７１】

図１４には、第２の実施形態の場合の情報処理装置１０の概略的な構成を示している。図１４の示した各構成は、本実施形態の情報処理装置１０にて行われる各処理や制御、実際のハードウェア構成をそれぞれ機能ごとに分けた機能ブロックとして表したものである。なお、図１４において、前述の図４と同じ機能ブロックには図４と同一の符号を付してそれらの説明は省略する。

【００７２】

すなわち、第２の実施形態の情報処理装置１０は、第１の実施形態の情報処理装置１０とは異なる機能として、検出対象物の三次元座標を解析することにより、前記検出対象物が認証対象者の手３０である場合に手３０の各手指部位を個別に識別し、前記識別した手指部位の座標が前記仮想二次元平面内で前記仮想座標に対応している状態で、前記三次元空間内において前記識別した手指部位による所定の動きを検出したとき、前記識別した部位により前記選択対象画像が選ばれたと判断する解析手段と、前記個別に識別した手指部位によって順に選ばれた複数の選択対象画像に対応した複数の数字の配列と、前記選択対象画像を順に選んだ手指部位の識別情報と、予め登録されている認証コードの数字の配列と、前記認証コードの各数字に対応して予め登録されている手指部位の識別情報との一致判定により、前記認証対象者の認証判定を行う認証判定手段としての各機能を実現する装置の一例である。

【００７３】

図１５には、第２の実施形態においてＰＩＮコードを用いた個人認証が行われる際の情報処理装置１０の処理及び制御の流れをフローチャートにより示している。以下、図１４の各構成の動作及び処理と制御について、図１５のフローチャートを参照しながら説明する。

【００７４】
先ず、ステップＳ１の確認処理でユーザ確認がなされると、制御部２０５は、ステップＳ２１の処理として、距離センサ出力解析部２０２で行われる解析結果から、認証対象者の前記手３０が前記バーチャルタッチパネル４０の三次元空間内に存在しているか判断する。
【００７５】
ここで、第２の実施形態の場合、距離センサ出力解析部２０２は、座標算出部２１１と対象認識部２１２と指識別情報取得部２１３と指先座標情報取得部２１４とＺ座標判定部２１５とを有して構成されている。
【００７６】
座標算出部２１１は、距離センサ２０の二つの赤外線カメラ２１Ｌ，２１Ｒからの撮像信号の画像解析を行うことにより、距離センサ２０の前記有効範囲内の三次元空間における検出対象物（本実施形態では前記手３０）の三次元座標を、フレームごとに算出する。なお、第２の実施形態において、検出対象物である手３０は、手掌と５本の手指からなる物体、すなわち一つの検出対象物内にそれぞれ異なる動きをする複数の部位が存在する物体である。したがって、座標算出部２１１は、手３０を構成している手掌及び５本の手指の三次元座標を算出する。座標算出部２１１にて算出されたフレームごとの三次元座標情報は、対象認識部２１２へ送られる。
【００７７】
対象認識部２１２は、前記フレームごとの撮像信号と三次元座標情報を基に、前記検出対象物がどのようなものであるかを認識する。ここで、距離センサ２０の赤外線カメラにより、手掌及び５本の手指からなる手３０が撮像されている場合、対象認識部２１２は、前記撮像信号と前記座標算出部２１１でフレームごとに算出された三次元座標とから、前記検出対象物が手３０であることを認識する。また、対象認識部２１２は、検出対象物である手３０を構成する各部位、すなわち手掌と５本の手指、それら５本の手指の先端（指先）、５本の手指の屈曲部である各関節等を認識する。このように、対象認識部２１２は、検出対象物が手３０であることを認識すると、その対象認識結果と当該手掌と５本の指からなる手３０の座標情報を制御部２０５へ送る。
【００７８】
ここで、対象認識部２１２において、検出対象物が人の手であること及び当該手を構成する手掌と５本の手指をどのように認識するかについて、図１６を参照しながら説明する。なお、以下の説明は概念説明であり、本発明はこの例に限定されるものではない。
【００７９】
対象認識部２１２は、距離センサ２０の赤外線カメラ２１Ｌ，２１Ｒにより人の手が撮像された場合、その撮像信号と前記座標算出部２１１でフレームごとに算出された三次元座標とから、検出対象物は他の部位よりも広い面積を有する部位（手掌に相当する部位）と、その広い部位から伸びて且つそれぞれが個別に屈曲可能な５本の部位（５本の手指に相当する部位）とからなることを認識する。
【００８０】
図１６は、検出対象物として認識された手をモデル化して説明するための図である。図１６の例では、検出対象物として認識された手掌部位を掌オブジェクトＰとしてモデル化し、５本の手指部位をそれぞれ指オブジェクトＦ０～Ｆ４としてモデル化して表している。なお、指オブジェクトＦ０は親指に対応しており、以下同様、指オブジェクトＦ１は人差し指、指オブジェクトＦ２は中指、指オブジェクトＦ３は薬指、指オブジェクトＦ４は小指にそれぞれ対応している。また、図１６の例では、各手指の関節を関節オブジェクトＦ０ｊ～Ｆ４ｊとしてモデル化し、各手指の指先を指先オブジェクトＦ０ｔ～Ｆ４ｔとしてモデル化し、それら各関節オブジェクトの間或いは指先オブジェクトから隣の関節オブジェクトまでの間をボーンオブジェクトとしてモデル化して表している。対象認識部２１２は、図１６に示すようにモデル化できる各部位を有した検出対象物が三次元空間内に存在していることを認識し、さらにそれら各部位の三次元空間内における配置関係から、当

該検出対象物が人の手であると認識する。

【００８１】

そして、制御部２０５は、対象認識部２１２から、検出対象物として人の手の認識結果を受け取ると、図１５のステップＳ２１において、前記バーチャルタッチパネル４０内で人の手３０を検出したと判断し、処理をステップＳ３へ進める。ステップＳ３へ処理を進めると、制御部２０５は、前述の第１の実施形態と同様に、ランダム配置したキー画像１２をディスプレイ１１の画面上に表示させる。

【００８２】

次に、制御部２０５は、ステップＳ２２へ処理を進め、距離センサ出力解析部１０２の指識別情報取得部２１３に対して手３０の各手指を識別するための指識別情報を取得させ、また、指先座標情報取得部２１４に対して各指先の座標情報を取得させる。この指識別情報は、部位識別情報の一例である。

【００８３】

すなわち、指識別情報取得部２１３は、対象認識部２１２が認識した手３０の各部位のうち、例えば図１６の指オブジェクトＦ０～Ｆ４のようにモデル化できる各部位を、それぞれ親指から小指までの手指部位であると識別する。そして、指識別情報取得部２１３は、それら手指部位を個別に識別した指識別情報を制御部２０５へ送る。また、指先座標情報取得部２１４は、前記指識別情報取得部２１３が識別した各手指部位のうち、例えば図１６の指先オブジェクトＦ０ｔ～Ｆ４ｔのようにモデル化できる先端部位の座標情報を取得し、それら各指先部位の座標情報を制御部２０５へ送る。

【００８４】

次に、制御部２０５は、ステップＳ２３の処理として、指識別情報取得部２１３からの指識別情報と指先座標情報取得部２１４からの指先の座標情報とにより識別されている手指の指先の座標が、バーチャルタッチパネル４０の三次元空間内に配置された何れかの仮想キーＶ１２の座標と一致したか判断する。なおこの場合の一致判定は、指先のＸ，Ｙ座標が、仮想キーＶ１２のＸ，Ｙ座標の範囲内であるかの一致判定となる。そして、制御部２０５は、前記識別されている手指の指先座標が、仮想キーＶ１２の座標に一致したと判断したときにはステップＳ２４へ処理を進め、一方、一致していないと判断したときにはステップＳ２２へ処理を戻す。なお、ステップＳ２３の判断の際も、前述の第１の実施形態で説明したのと同様に、仮想キーＶ１２の座標の周囲に所定の検出範囲を設けてもよい。

【００８５】

次に、制御部２０５は、Ｚ座標判定部２１５でのＺ座標判定結果に基づいて、バーチャルタッチパネル４０上でエアクリックが行われたか判断する。なお、Ｚ座標判定部２１５で行われるＺ座標判定処理については前述の第１の実施形態と同様である。そして、ステップＳ２４において、前記Ｚ座標判定部２１５から判定検出信号を受け取ると、制御部２０５は、エアクリックが行われたと判断する。なお、エアクリックが行われていない場合、制御部２０５は、ステップＳ２２へ処理を戻す。

【００８６】

次に、ステップＳ２４にてエアクリックが行われたと判断して、ステップＳ２５へ処理を進めると、制御部２０５は、入力情報判定部２０３に対し、エアクリックにより入力された座標に対応した数字を配列ＰＩＮ（ｎ）として保管させ、また、エアクリックした何れかの手指の識別情報を配列ＦＩＮＧＥＲ（ｎ）に保管した後、「ｎ」に「１」を加えて、ステップＳ２６へ処理を進める。

【００８７】

ステップＳ２６へ処理が進むと、制御部２０５は、入力情報判定部２０３が保管している配列ＰＩＮ（ｎ）の「ｎ」が「ｍ」となり、また、配列ＦＩＮＧＥＲ（ｎ）の「ｎ」が「ｍ」となったか否か判定する。なお「ｍ」は、ＰＩＮコードが４桁である場合は「４」となる。したがって、制御部２０５は、「ｎ」が「４」になると、処理をステップＳ２７へ進める。すなわち、「ｎ」が「４」になったとき、入力情報判定部２０３が前記配列Ｐ

ＩＮ（ｎ）として保管している数字は４桁の数字となり、この４桁の数字が、バーチャルタッチパネル４０を用いて認証対象者により入力された数字となる。また、「ｎ」が「４」になったとき、入力情報判定部２０３が前記配列ＦＩＮＧＥＲ（ｎ）にして保管している指識別情報の数は「４」となり、これにより、それぞれが個々に識別された手指による４回のエアクリックが認証対象者からなされたことになる。

【００８８】

次に、処理をステップＳ２７へ進めると、制御部２０５は、入力情報判定部２０３に対し、例えばメモリ部２０７に保存されているユーザごとのＰＩＮコード及び当該ＰＩＮコードの各数字に対応付けられた指識別情報と、前記バーチャルタッチパネル４０を介して認証対象者により入力された数字及びそれら数字を入力する際に使用された指識別情報とが、完全に一致しているか否か判定させる。

【００８９】

ここで、メモリ部２０７には、一例としてユーザ情報１３１とＰＩＮコード１３２と指識別情報１３３とが登録されたテーブル情報が格納されている。当該テーブル情報は、一例として図１７に示すように、複数のユーザをそれぞれ表すユーザ情報Ｕ１，Ｕ２，Ｕ３，・・・と、各ユーザの登録ＰＩＮコードと、それらＰＩＮコードの各数字を入力する手指の識別情報とが対応付けられて登録されてものである。入力情報判定部２０３には、先のステップＳ１のユーザ確認の際に登録済みと判定されたユーザのＰＩＮコード及び指識別情報がメモリ部１０７から渡されており、したがって、入力情報判定部２０３は、ステップＳ２７において、そのＰＩＮコードと当該ＰＩＮコードの各数字に対応した指識別情報と、前記認証対象者が入力した数字とそれら数字が入力された際の指識別情報との一致判定を行う。

【００９０】

そして、ステップＳ２７において、入力情報判定部２０３が前記認証対象者の入力数字とＰＩＮコードと指識別情報が全て一致したと判定したとき、制御部２０５は、ステップＳ１０として、認証は確認（ＯＫ）されたとして認証ＯＫ処理を行う。すなわち、例えば図１８に示すように、ＰＩＮコードが例えば「１，７，６，４」であり、それらＰＩＮコードの数字に対して指識別情報「Ｆ０（親指），Ｆ４（小指），Ｆ１（人差し指），Ｆ３（薬指）」が登録されていたような場合において、認証対象者から、親指により「１」、小指により「７」、人差し指により「６」、薬指により「４」の数字が、その順に入力されたとき、制御部２０５は、認証ＯＫ処理を行う。これ以降の処理は前述の図５のフローチャートと同様である。一方、ステップＳ２７において入力数字とＰＩＮコードと各指識別情報が完全に一致しなかったと判定された場合、制御部２０５は、ステップＳ１２へ処理を進めて認証ＮＧ処理を行う。すなわち、ＰＩＮコードが例えば「１，７，６，４」であり、それらＰＩＮコードの数字に対して指識別情報「Ｆ０，Ｆ４，Ｆ１，Ｆ３」が登録されていたような場合において、認証対象者から、例えば全て人差し指を用いて「１，７，６，４」の数字が入力されたとき、制御部２０５は、認証ＮＧ処理を行う。

【００９１】

なお、前述の説明では、５本の手指全てについて手指を識別する例を挙げたが、第２の実施形態の認証処理装置１は、必要とされるセキュリティレベル（セキュリティの度合い）に応じて、例えば手指２本のみを識別することにしたり、３本のみを識別するようなことも可能である。セキュリティレベルとしては、前述した第１の実施形態のように使用する手指を特定せずにＰＩＮコードの数字のみを入力するセキュリティレベルや、５本の手指のうち所定の２本や３本のみを識別するセキュリティレベル、５本の手指全てを識別するセキュリティレベルなどを挙げることができる。これらセキュリティレベルは、登録ユーザごとに設定してもよく、また、入室管理等される場所に応じて設定してもよい。例えばセキュリティレベルとして最高レベルが求められる場所やユーザに対しては、前記５本の手指全てを識別する設定とし、例えば最も緩いレベルでもよい場所やユーザに対しては、手指を特定しない設定とすることができる。

【００９２】

第２の実施形態の認証処理装置１によれば、前述の第１の実施形態で説明した認証処理装置１と同様に、実際に入力されている数字を、第三者に盗み見られたり、盗撮されたりすることが無くなり、非常に高いセキュリティ性を確保可能であり、また例えばフェイククリックが行われたときには第三者に何れの数字がＰＩＮコードの数字であるかを知られる虞がない。また、第２の実施形態の認証処理装置１によれば、第１の実施形態同様に、認証対象者は指先で実際にタッチパネル等に触れる必要がなく、したがって指紋パターンなどの痕跡が残らず、指紋パターンを盗まれることがない。さらに、第２の実施形態の認証処理装置１においても、第１の実施形態同様に、反射板５１や光学結像プレート５０を配した構成を用いれば、第三者によるＰＩＮコードの盗み見や盗撮を有効に防止することができる。また、第２の実施形態の認証処理装置１によれば、第１の実施形態同様に、暗い環境であっても、認証対象者はＰＩＮコードの入力が可能となる。

【００９３】

さらに、これら第１の実施形態同様の効果に加え、第２の実施形態の認証処理装置１においては、ＰＩＮコードの各数字に対し、その数字を入力する手指を個々に登録可能となされているため、より高いセキュリティ性を実現できる。例えば、ＰＩＮコードが４桁の数字であった場合、それら数字の組み合わせは１０の４乗で１００００通りしかないが、第２の実施形態のように、ＰＩＮコードの４桁の各数字の入力に対して５本の手指の何れを使用するかを登録した場合、それらの組み合わせは１０×５の４乗で６２５００００通りとなる。すなわち、第２の実施形態によれば、ＰＩＮコードの４桁の数字のみを用いた場合と比較して、セキュリティ強度が６２５倍となり、正規のユーザになりすまして不正を行うことが非常に難しくなる。

【００９４】

また、第２の実施形態の認証処理装置１の場合、前述のようにセキュリティレベルの設定が可能となされているため、登録ユーザごと、また入出管理する場所等に応じてセキュリティの度合いを変えることができる。

【００９５】

なお、第２の実施形態において、詳細は後述する第３の実施形態で説明するが、それぞれ認識された指先３１によりエアクリックが行われたか判断する際に使用する座標は、Ｚ座標軸で予め固定的に決められた基準座標に限定されない。すなわち、エアクリックが行われたか判断する際に使用する座標は、例えば、認証対象者の手３０の指先３１がバーチャルタッチパネル４０の三次元空間内で検出された後、その手３０の指先３１が三次元空間内で所定の時間だけ静止したときのそれぞれの指先３１の各Ｚ座標から、指先方向で且つＺ軸方向にそれぞれ所定距離だけ離れた座標に設定することもできる。言い換えると、エアクリックの判定に使用される座標は、それぞれの指先３１が三次元空間内で静止したときの各Ｚ座標に応じた可変の座標として設定可能である。

【００９６】

＜第３の実施形態＞

前述の第１、第２の実施形態では、バーチャルタッチパネル４０が、認証対象者に対して正対するように設定された例を挙げている。すなわち、第１、第２の実施形態は、例えば重力方向をＹ軸方向とした場合において、バーチャルタッチパネル４０がＸ軸とＹ軸を含む仮想二次元平面として設定された例を挙げている。

【００９７】

これに対し、第３の実施形態では、バーチャルタッチパネル４０の仮想二次元平面が、認証対象者から見て略々水平に設定される例について説明する。すなわち、第３の実施形態は、図１９に示すように、例えば重力方向をＹ軸方向とした場合において、バーチャルタッチパネル４０がＸ軸とＺ軸を含む仮想二次元平面として設定された例を挙げる。図１９に示した配置の場合、認証対象者から見たディスプレイ１１と距離センサ２０は、例えば図２０に示すような配置関係となり、バーチャルタッチパネル４０は、それらディスプレイ１１と距離センサ２０の上空側の三次元空間に設定されることになる。この図１９の例のように、バーチャルタッチパネル４０とディスプレイ１１の表示面を、認証対象者か

ら見て略々水平に設定した場合、認証対象者は、既存の銀行ＡＴＭを操作する場合と略々変わらぬ体勢で、バーチャルタッチパネル４０に対する操作が可能となる。

【００９８】

なお、図１９、図２０の場合、認証対象者から見て、ディスプレイ１１はその表示面が水平となるように設置され、同様に、距離センサ２０はセンサ面２０Ｆが水平となるように設置されているが、これはあくまで一例である。特に、バーチャルタッチパネル４０の仮想二次元平面は、距離センサ２０の有効範囲内であれば、例えば重力方向をＹ軸方向とした場合にそのＹ軸に対してどのような傾きであっても設定可能であり、Ｘ軸或いはＺ軸に対しても同様にどのような傾きにも設定可能である。また、図１９では、Ｙ軸方向が重力方向と一致した例を挙げて説明しているが、Ｙ軸方向は重力方向と一致している必要はなく、重力方向に対して傾いた軸として設定されていてもよい。これは第３の実施形態だけでなく、前述した第１、第２の実施形態においても同様である。

【００９９】

また、第３の実施形態の認証処理装置は、認証対象者の手３０の指先３１がバーチャルタッチパネル４０の三次元空間内で検出された後、その手３０の指先３１が三次元空間内で静止した時間を計測している。そして、認証処理装置は、指先３１が所定の時間（以下、静止判定時間と表記する。）だけ静止したことを検出したとき、各指先３１のＹ座標から、それらの各指先方向で且つＹ軸方向にそれぞれ所定距離だけ離れた座標を、エアクリックが行われたか判断する際に使用する座標（以下、エアクリック判定座標と表記する。）として設定する。すなわち、第３の実施形態の場合、エアクリック判定座標は、指先３１が三次元空間内で静止判定時間だけ静止したときのそれぞれの指先３１のＹ座標に応じた可変の座標として設定される。

【０１００】

また、エアクリック判定座標は、前記設定されたＹ座標を中心として、Ｘ軸方向とＺ軸方向の幅がそれぞれ所定の幅となされた判定エリアを有するように設定されることが望ましい。すなわち、指先３１は、静止した状態からＹ軸方向へ動かされたとき、必ずしもＹ軸に正確に沿って動くとは限らないためであり、指先３１がエアクリック判定座標に到達したことを有効に検出可能にするためである。

【０１０１】

図２１は、親指の指先座標ＦＣ０から所定距離ＤＹ０だけ離れたＹ座標値が親指用のエアクリック判定座標ＹＳ０として設定され、以下同様に、人差し指～小指の各指先座標ＦＣ１～ＦＣ４からそれぞれ所定距離ＤＹ１～ＤＹ４だけ離れたＹ座標値がそれぞれ人差し指～小指用のエアクリック判定座標ＹＳ１～ＹＳ４として設定された状態を概念的に示している。エアクリック判定座標ＹＳ０～ＹＳ４は、図２１のようにＸ軸方向とＺ軸方向が所定の幅となされた判定エリアを有している。

【０１０２】

そして、第３の実施形態の認証処理装置は、各指先座標ＦＣ１～ＦＣ４に対してそれぞれエアクリック判定座標ＹＳ０～ＹＳ４を設定した後、何れかの指先座標ＦＣがエアクリック判定座標ＹＳに達するか又は越えたとき、エアクリックが行われたと判定する。一方、第３の実施形態において、エアクリック判定座標ＹＳ０～ＹＳ４が設定された後、何れかの指先座標ＦＣがエアクリック判定座標ＹＳ付近まで移動してもエアクリック判定座標ＹＳにまで達していないか又は越えていない場合には、フェイククリックとなる。

【０１０３】

なお、各指先座標ＦＣ０～ＦＣ４からエアクリック判定座標ＹＳ１～ＹＳ４までの所定距離ＤＹ０～ＤＹ４は、一例として１．０ｃｍとする。所定距離を１．０ｃｍとしたのは、所定距離が１．０ｃｍよりも短く設定されていたとすると、例えば薬指等でエアクリックがなされる場合において、その薬指の動きにより中指と小指も一緒に動いてしまい、それら中指と小指でもエアクリックがなされたと誤って判定されてしまう可能性を少なくするためである。もちろん、所定距離の１．０ｃｍは一例であり、例えば親指や人差し指、中指などのように動かし易い手指に対する所定距離は長くし、薬指のように動かし難い手

指に対する所定距離は短くするような設定であってもよい。また例えば、要求されるセキュリティレベルに応じて、各指先に対する所定距離が変更されてもよい。

【０１０４】

また、指先３１が静止したか否かを判断する静止判定時間は、一例として１秒間など予め決められた時間として設定される。静止判定時間が予め決められた時間に設定されている場合、指先３１が静止した状態が静止判定時間以上になったことが検出されたときに、エアクリック判定座標が設定される。なお、静止判定時間は、各指先ごとに異なる時間に設定してもよいし、例えばセキュリティレベルに応じて異なる時間に設定してもよい。

【０１０５】

以下、本発明の第３の実施形態の認証処理装置１について以下に説明する。図２２は、第３の実施形態の情報処理装置１０の概略的な構成を示している。図２２の示した各構成は、本実施形態の情報処理装置１０にて行われる各処理や制御、実際のハードウェア構成をそれぞれ機能ごとに分けた機能ブロックとして表したものである。なお、図２２において、前述の図１４と同じ機能ブロックには図１４と同一の符号を付してそれらの説明は省略する。

【０１０６】

第３の実施形態の情報処理装置１０は、基本的な構成と処理は図１４と略々同様であるが、図１４のＺ座標判定部２１５に代えてＹ座標判定部２５５を備えており、また制御部２５０の処理も一部が異なる。また、第３の実施形態の場合、ディスプレイ１１の画面上にランダム配置されるキー画像１２とバーチャルタッチパネル４０内に配される仮想キーＶ１２の対応関係、認証対象者の各手指の認識と、エアクリックに使用される手指と４桁のＰＩＮコードとの対応付けによる個人認証等については第２の実施形態と同様であるが、バーチャルタッチパネル４０、距離センサ２０、ディスプレイ１１の配置関係等は図１９～図２１で示したようになされている。

【０１０７】

また、図２３には、第３の実施形態においてＰＩＮコードを用いた個人認証が行われる際の情報処理装置１０の処理及び制御の流れをフローチャートにより示している。なお、図２３において、前述の図１５と同じ処理ステップには図１５と同一の符号を付してそれらの説明は省略する。以下、図２２の各構成の動作及び処理と制御について、図２３のフローチャートを参照しながら説明する。

【０１０８】

図２３において、ステップＳ１からステップＳ２２を経てステップＳ３１に進むと、制御部２５０は、指先座標情報取得部２１４がフレームごとに取得している各指先の座標情報から、認証対象者の手３０の指先３１が三次元空間内で静止した時間を計測し、指先３１が静止判定時間だけ静止したか判定する。制御部２５０は、指先３１が静止判定時間になるまで静止していないと判断している間は、ステップＳ２２へ処理を戻し、静止判定時間以上静止したことを検出すると、ステップＳ３２へ処理を進める。

【０１０９】

ステップＳ３２へ処理を進めると、制御部２５０は、指識別情報取得部２１３からの指識別情報と指先座標情報取得部２１４からの指先の座標情報とにより識別されている手指の指先の座標が、バーチャルタッチパネル４０の三次元空間内に配置された何れかの仮想キーＶ１２の座標と一致したか判断する。なお第３の実施形態の場合の一致判定は、指先のＸ，Ｚ座標が、仮想キーＶ１２のＸ，Ｚ座標の範囲内であるかの一致判定となる。そして、制御部２５０は、前記識別されている手指の指先座標が、仮想キーＶ１２の座標に一致したと判断したときにはステップＳ３３へ処理を進め、一致していないと判断したときにはステップＳ２２へ処理を戻す。なお、ステップＳ３２の判断の際も、前述の第１の実施形態で説明したのと同様に、仮想キーＶ１２の座標の周囲に所定の検出範囲を設けてもよい。

【０１１０】

ステップＳ３３へ処理を進めると、制御部２５０は、前述のように、指先３１のＹ座標

から指先方向で且つＹ軸方向に所定距離だけ離れたエアクリック判定座標を設定する。そして、制御部２５０は、設定したエアクリック判定座標の情報をＹ座標判定部２５５へ渡す。そして、Ｙ座標判定部２５５は、指先３１の座標がエアクリック判定座標に達したか又は超えたとき、その旨を示すＹ座標判定結果を制御部２５０へ送る。

【０１１１】

制御部２５０は、指先３１の座標がエアクリック判定座標に達した旨のＹ座標判定結果を受け取ると、ステップＳ３４の処理としてエアクリックが行われたと判断した後、ステップＳ２５へ処理を進める。一方指先３１の座標がエアクリック判定座標に達していないとき、制御部２５０は、ステップＳ２２へ処理を戻す。ステップＳ２５以降の処理は図１５のフローチャートと同様であり、その説明は省略する。

【０１１２】

なお、この第３の実施形態においても前述の第２の実施形態同様に、必要とされるセキュリティレベル（セキュリティの度合い）に応じて認識する手指の本数を変更してもよく、また、セキュリティレベルを登録ユーザごとに設定してもよく、入室管理等される場所に応じて設定してもよい。

【０１１３】

第３の実施形態の認証処理装置１によれば、前述の第１，第２の実施形態で説明したのと同様の効果を得ることができる。また、第３の実施形態の認証処理装置１においては、認証対象者は既存の銀行ＡＴＭ等を操作する場合と略々変わらぬ体勢でバーチャルタッチパネル４０に対する操作が可能となり、さらに、エアクリック判定座標の設定によりエアクリックの誤判定を少なくすることができる。

【０１１４】

＜第４の実施形態＞

次に、本発明の第４の実施形態の認証処理装置１について以下に説明する。なお、第４の実施形態の認証処理装置１の概観は前述の図１と同様であり、また情報処理装置１０の概略的な構成は前述の第２の実施形態の図１４や第３の実施形態の図２２と同様であるため、それらの図示は省略する。第４の実施形態の認証処理装置１は、認証対象者の手の５本の手指をそれぞれ個別に認識し、その中の所定の手指によりエアクリックが行われたかを認識し、所定の手指によるエアクリックが行われた際に、手の５本全ての手指にそれぞれ対応した各仮想キーＶ１２の各数字等の情報を取得する。以下、第４の実施形態について、前述した第２，第３の実施形態とは異なる部分のみ説明する。

【０１１５】

ここで、第４の実施形態の場合、情報処理装置１０は、ＰＩＮコードの入力がなされる際に、認証対象者が所定の手指（本実施形態では人差し指とする。）によりエアクリックが行われた場合、５本の手指の識別情報と共に、そのエアクリック時点における５本の全ての手指の指先がそれぞれ位置している仮想キーＶ１２の各数字の情報をも取得する。なお、エアクリックしていない残りの手指の指先がいずれの仮想キーＶ１２内にも入っていない場合には、各仮想キーＶ１２のいずれの数字でもないことを示す情報を取得する。本実施形態では、各仮想キーＶ１２のいずれの数字でもないことを示す情報として記号＃を用いることにする。第４の実施形態の場合、各仮想キーＶ１２外のエリア、つまりディスプレイ１１の画面に表示されている画像におけるキー画像１２外の画像エリアは、各仮想キーＶ１２のいずれの数字でもないことを示す情報（記号＃）に対応した選択対象画像のエリアとなされている。

【０１１６】

そして、第４の実施形態の情報処理装置１０は、エアクリックを行った１本の手指（人差し指）の指識別情報及びその指先に対応した仮想キーＶ１２の数字と、エアクリックしていない残り４本の手指の各識別情報及びそれらの指先の位置に対応した四つの情報（数字や記号＃等からなる四つ情報）とからなる五つの情報を、例えば４桁のＰＩＮコードのうちの一つのコードを決める際の候補コード（候補配列）として取得する。

【０１１７】

図２４（ａ）～図２４（ｄ）には、第４の実施形態において、バーチャルタッチパネル４０の三次元空間内に配置された各仮想キーＶ１２と、バーチャルタッチパネル４０内における認証対象者の親指～小指の五つの各指先Ｆ０～Ｆ４の位置の一例を示している。なお、各仮想キーＶ１２内の各数字は、それら各仮想キーＶ１２に各々対応付けられている数字であるとする。図の例では、説明を判り易くするために、各仮想キーＶ１２に対応した各数字が０～９の順に配置されているが、前述の各実施形態で説明したのと同様にそれらの数字はランダムに配置されてもよい。図２４（ａ）～図２４（ｄ）において、エアクリックを行うのは人差し指であり、一方、図２４（ａ）～図２４（ｄ）の円マークＥＣは、順番に人差し指によるエアクリックがなされた各時点において、正しいＰＩＮコードとして登録されている各数字に対応した仮想キーＶ１２を示している。

【０１１８】

図２４（ａ）の例は、４桁のＰＩＮコードのうち、１番目のコード（ＰＩＮ＝１）が入力される際（１回目のエアクリックがなされた際）の、５つの指先Ｆ０～Ｆ４の位置の例を示している。また、図２４（ａ）の例では、人差し指（Ｆ１）による１回目のエアクリックがなされた時点で、入力されるべき正しいＰＩＮコード（１番目のＰＩＮコード）が数字「１」で且つその数字「１」を入力するべき手指が中指（Ｆ２）として予め登録されているとする。図２４（ａ）の例では、例えば親指の指先Ｆ０が数字「３」の仮想キーＶ１２内に位置し、以下同様に、人差し指の指先Ｆ１が数字「０」、中指の指先Ｆ２が数字「１」、薬指の指先Ｆ３が数字「２」、小指の指先Ｆ４が数字「６」の仮想キーＶ１２内に位置している。したがって、図２５に示すように、４桁のＰＩＮコードのうち、１番目のコード（ＰＩＮ＝１）を決める際の候補コードは、親指～小指の各指先Ｆ０～Ｆ４に対応した五つのコード「３，０，１，２，６」となる。

【０１１９】

また、図２４（ｂ）の例は、４桁のＰＩＮコードのうち、２番目のコード（ＰＩＮ＝２）が入力される際（２回目のエアクリックがなされた際）の、５つの指先Ｆ０～Ｆ４の位置の例を示している。また、図２４（ｂ）の例では、人差し指（Ｆ１）による２回目のエアクリックがなされた時点で、入力されるべき正しいＰＩＮコード（２番目のＰＩＮコード）が数字「５」で且つその数字「５」を入力するべき手指が薬指（Ｆ３）として予め登録されているとする。図２４（ｂ）の例では、例えば親指の指先Ｆ０が仮想キーＶ１２外となっており、人差し指の指先Ｆ１が数字「３」の仮想キーＶ１２内に位置し、以下同様に、中指の指先Ｆ２が数字「４」、薬指の指先Ｆ３が数字「５」、小指の指先Ｆ４が数字「９」の仮想キーＶ１２内に位置している。したがって、図２５に示すように、４桁のＰＩＮコードのうち、２番目のコード（ＰＩＮ＝２）を決める際の候補コードは、親指～小指の各指先Ｆ０～Ｆ４に対応した五つのコード「＃，３，４，５，９」となる。

【０１２０】

同様に、図２４（ｃ）の例は、４桁のＰＩＮコードのうち、３番目のコード（ＰＩＮ＝３）が入力される際（３回目のエアクリックがなされた際）の、５つの指先Ｆ０～Ｆ４の位置の例を示している。また、図２４（ｃ）の例では、人差し指（Ｆ１）による３回目のエアクリックがなされた時点で、入力されるべき正しいＰＩＮコード（３番目のＰＩＮコード）が数字「３」で且つその数字「３」を入力するべき手指が人差し指（Ｆ１）として予め登録されているとする。図２４（ｃ）の例では、例えば親指の指先Ｆ０が仮想キーＶ１２外、人差し指の指先Ｆ１が数字「３」、中指の指先Ｆ２と薬指の指先Ｆ３が共に数字「４」、小指の指先Ｆ４が数字「８」の仮想キーＶ１２内に位置している。したがって、図２５に示すように、４桁のＰＩＮコードのうち、３番目のコード（ＰＩＮ＝３）を決める際の候補コードは、親指～小指の各指先Ｆ０～Ｆ４に対応した五つのコード「＃，３，４，４，８」となる。

【０１２１】

同様に、図２４（ｄ）の例は、４桁のＰＩＮコードのうち、４番目のコード（ＰＩＮ＝４）が入力される際（４回目のエアクリックがなされた際）の、５つの指先Ｆ０～Ｆ４の位置の例を示している。また、図２４（ｃ）の例では、人差し指（Ｆ１）による４回目の

エアクリックがなされた時点で、入力されるべき正しいＰＩＮコード（４番目のＰＩＮコード）が数字「８」で且つその数字「８」を入力するべき手指が小指（Ｆ４）として予め登録されているとする。図２４（ｄ）の例では、親指の指先Ｆ０が仮想キーＶ１２外、人差し指の指先Ｆ１が数字「３」、中指の指先Ｆ２と薬指の指先Ｆ３が共に数字「４」、小指の指先Ｆ４が数字「８」の仮想キーＶ１２内に位置している。したがって、図２５に示すように、４桁のＰＩＮコードのうち、４番目のコード（ＰＩＮ＝４）を決める際の候補コードは、親指～小指の各指先Ｆ０～Ｆ４に対応した五つのコード「＃，３，４，４，８」となる。

【０１２２】

第４の実施形態の情報処理装置１０は、前述のように、４桁のＰＩＮコードの１番目のコード（ＰＩＮ＝１）～４番目のコード（ＰＩＮ＝４）を決めるための４回のエアクリックがなされた場合、エアクリックがなされるごとに、それぞれ各指先Ｆ０～Ｆ４に対応した五つの候補コードを取得する。そして、これら五つの候補コードにおける各数字には、各指先Ｆ０～Ｆ４の各手指の識別情報が対応付けられている。

【０１２３】

図２４（ａ）～図２４（ｄ）及び図２５の例の場合、ＰＩＮコードの１番目のコード（ＰＩＮ＝１）を決めるために取得された候補コード「３，０，１，２，６」の中で、ＰＩＮ＝１に登録された数字は「１」であり、その数字「１」に対応した手指は中指（Ｆ２）となされている。以下同様に、ＰＩＮコードの２番目のコード（ＰＩＮ＝２）を決める際に取得された候補コード「＃，３，４，５，９」の中で、ＰＩＮ＝２に登録された数字は「５」であり、その数字「５」に対応した手指は薬指（Ｆ３）となされており、ＰＩＮ＝３を決める際に取得された候補コード「＃，３，４，４，８」の中で、ＰＩＮ＝３に登録された数字は「３」であり、その数字「３」に対応した手指は人差し指（Ｆ１）となされており、ＰＩＮ＝４を決める際に取得された候補コード「＃，３，４，４，８」の中で、ＰＩＮ＝４に登録された数字は「８」であり、その数字「８」に対応した手指は小指（Ｆ４）となされている。

【０１２４】

このため、図２４（ａ）～図２４（ｄ）及び図２５の例の場合、４回のエアクリックによる入力順の４桁のＰＩＮコードとして「１，５，３，８」が取得され、また１回目のエアクリックによるコード「１」については中指（Ｆ２）の指識別情報が得られ、２回目のエアクリックによるコード「５」については薬指（Ｆ３）、３回目のエアクリックによるコード「３」については人差し指（Ｆ１）、４回目のエアクリックによるコード「８」については小指（Ｆ４）の各指識別情報が得られる。ここで、本実施形態では、認証対象者について登録されているＰＩＮコードが例えば「１，５，３，８」の順であり、それら各コードに対応した指識別情報の順番が「中指（Ｆ２）、薬指（Ｆ３）、人差し指（Ｆ１）、小指（Ｆ４）」となされているため、その登録されたＰＩＮコード及び指識別情報と、図２４（ａ）～図２４（ｄ）及び図２５の例で４回のエアクリックにより得られたＰＩＮコード及び指識別情報とは一致し、したがって、その認証対象者は正当な登録者であると認証されることになる。

【０１２５】

また前述したように、第４の実施形態の場合、４桁のＰＩＮコードの１番目のコード（ＰＩＮ＝１）～４番目のコード（ＰＩＮ＝４）を決めるための４回のエアクリックがなされた際に、エアクリックごとに五つの候補コードが取得される。ここで、第４の実施形態の場合、エアクリックごとに取得された五つの候補コードのなかで、予め登録されている手指に対応した一つの候補コードのみが入力されたコードとして扱われ、それ以外の四つの手指による四つの各候補コードは全てフェイクコードとして扱われる。また、第４の実施形態の場合、エアクリックは所定の手指である人差し指のみで行われ、登録されたコードを入力する手指が人差し指として登録されていない場合には、そのエアクリックを行った人差し指によるエアクリック自体がフェイクとなる。図２４（ａ）～図２４（ｄ）及び図２５の例の場合、１回目のエアクリックでは、中指（Ｆ２）に対応した数字「１」のみ

が入力されたコードとして扱われ、残りの親指（Ｆ０）に対応した数字「３」、エアクリックを行った人差し指（Ｆ１）に対応した数字「０」、薬指（Ｆ３）に対応した数字「２」、小指（Ｆ０）に対応した数字「６」は全てフェイクコードとして扱われる。同様に、２回目のエアクリックでは、薬指（Ｆ３）に対応した数字「５」のみが入力されたコードとなされ、残りの親指（Ｆ０）による記号「＃」、エアクリックを行った人差し指（Ｆ１）による数字「３」、中指（Ｆ２）による数字「４」、小指（Ｆ０）による数字「９」は全てフェイクコードとして扱われる。３回目と４回目のエアクリックについても同様のことが行われる。

【０１２６】

このように、第４の実施形態によれば、エアクリック自体がフェイクとして扱われ、五つの候補コードのなかで入力コードとして扱われるのは、予め登録された手指により選ばれた一つの候補コードのみであり、残りの四つの各候補コードは全てフェイクコードとなされる。第４の実施形態によれば、４桁のＰＩＮコードの１番目のコード（ＰＩＮ＝１）～４番目のコード（ＰＩＮ＝４）を決めるための４回のエアクリックごとに五つの候補コードが取得されるため、ＰＩＮコードの候補は、５×４×４×４＝３２０通りとなる。このため、例えば悪意を持った者によりハッキング等が行われたとしても、登録されたＰＩＮコードがどのようなコードであるかを知られてしまう虞は非常に少ない。

【０１２７】

第４の実施形態の情報処理装置１０では、概ね前述した図１５や図２３のフローチャートで説明したのと同様の流れで認証処理が行われるが、第４の実施形態の場合には、図１５や図２３のステップＳ２５の処理が異なる。以下、以下、第４の実施形態における認証処理について、図１５や図２３のフローチャートとは異なる処理について説明する。

【０１２８】

第４の実施形態の場合、図１５や図２３のステップＳ２５で説明した処理に代えて、制御部２０５は、入力情報判定部２０３に対し、前述したような人差し指による１回目～４回目のエアクリックがなされた際の５本の手指により取得された候補コードを、配列ＰＩＮ（Ｍ，Ｎ）として保管させる。「Ｍ」は１回目～４回目のエアクリックの回数（ＰＩＮ＝１～ＰＩＮ＝４における「１～４」）の値となる。そして、制御部２０５は、入力情報判定部２０３に対し、配列ＰＩＮ（Ｍ，Ｎ）の「Ｍ」に「１」を加えて、ステップＳ２６へ処理を進める。第４の実施形態の場合、ステップＳ２６に処理が進むと、制御部２０５は、入力情報判定部２０３が保管している配列ＰＩＮ（Ｍ，Ｎ）の「Ｍ」が「４」となったか否か判定する。

【０１２９】

ここで、配列ＰＩＮ（Ｍ，Ｎ）の「Ｎ」は、各手指に対応した値として親指の場合は「１」、人差し指の場合は「２」、中指の場合は「３」、薬指の場合は「４」、小指の場合は「５」の値となり、また「Ｎ」が「１：５」と表現される場合には５本の手指による個々の数字や記号が入ることを表す。

【０１３０】

一例として、前述の図２４（ａ）～図２４（ｄ）及び図２５を用いて説明する。

１回目の人差し指によるエアクリックがなされた際、配列ＰＩＮ（１，１）が「３」、配列ＰＩＮ（１，２）が「０」、配列ＰＩＮ（１，３）が「１」、配列ＰＩＮ（１，４）が「２」、配列ＰＩＮ（１，５）が「６」となり、この場合、ＰＩＮ（１，１：５）は（３，０，１，２，６）となる。

２回目の人差し指によるエアクリックがなされた際、配列ＰＩＮ（２，１）が「＃」、配列ＰＩＮ（２，２）が「３」、配列ＰＩＮ（２，３）が「４」、配列ＰＩＮ（２，４）が「５」、配列ＰＩＮ（２，５）が「９」となり、この場合、ＰＩＮ（２，１：５）は（＃，３，４，５，９）となる。

３回目の人差し指によるエアクリックがなされた際、配列ＰＩＮ（３，１）が「＃」、配列ＰＩＮ（３，２）が「３」、配列ＰＩＮ（３，３）が「４」、配列ＰＩＮ（３，４）が「４」、配列ＰＩＮ（３，５）が「８」となり、この場合、ＰＩＮ（３，１：５）は（

＃，３，４，４，８）となる。
４回目の人差し指によるエアクリックがなされた際、配列ＰＩＮ（４，１）が「＃」、配列ＰＩＮ（４，２）が「３」、配列ＰＩＮ（４，３）が「４」、配列ＰＩＮ（４，４）が「４」、配列ＰＩＮ（４，５）が「８」となり、この場合、ＰＩＮ（４，１：５）は（＃，３，４，４，８）となる。

【０１３１】
これら１回目～４回目のエアクリックがなされた際の４回の候補コード入力の結果は、
ＰＩＮ（１，１：５）＝（３，０，１，２，６）、
ＰＩＮ（２，１：５）＝（＃，３，４，５，９）、
ＰＩＮ（３，１：５）＝（＃，３，４，４，８）、
ＰＩＮ（４，１：５）＝（＃，３，４，４，８）となる。
このような組み合わせは前述したように３２０通りになり、そのうち正しいＰＩＮコードは一つのみ、すなわち、一回目のエアクリックの際にはＰＩＮ（１，３）＝「１」、２回目のエアクリックではＰＩＮ（２，４）＝「５」、３回目のエアクリックではＰＩＮ（３，２）＝「３」、４回目のエアクリックではＰＩＮ（４，５）＝８であり、したがって、この例の場合の入力されたＰＩＮコードは「１，５，３，８」となる。

【０１３２】
そして、第４の実施形態において、制御部２０５は、図１５や図２３のステップＳ２７において、エアクリックが行われた順番のＰＩＮ（Ｍ，Ｎ）で得られた各候補コード及び指識別情報と、予め登録されているＰＩＮコード及び指識別情報との一致判定を行う。第４の実施形態の場合、１番目のＰＩＮコード「１」に対しては中指、２番目のＰＩＮコード「５」に対しては薬指、３番目のＰＩＮコード「３」に対しては人差し指、４番目のＰＩＮコード「８」に対しては小指が登録されており、ステップＳ２７では、それらＰＩＮコード「１，５，３，８」と各登録された手指とが一致するか否かの判断が行われる。

【０１３３】
＜第５の実施形態＞
前述した第４の実施形態では、ＰＩＮコードとして仮想キーＶ１２に対応した数字のみが用いられる例を挙げたが、第５の実施形態では、仮想キーＶ１２外のエリアに対応した前述の記号「＃」をもＰＩＮコードとして扱う。第５の実施形態の場合、各仮想キーＶ１２外のエリア、つまりディスプレイ１１の画面に表示されている画像におけるキー画像１２外の画像エリアが、各仮想キーＶ１２の各数字以外のコード（記号＃）が設定された選択対象画像となされている。したがって、第５の実施形態の情報処理装置１０は、各仮想キーＶ１２外のエリアに対応した記号＃のコードをもユーザによる選択（入力）が可能となされている。

【０１３４】
図２６（ａ）～図２６（ｄ）及び図２７には、第５の実施形態のように仮想キーＶ１２外のエリアに対応した記号「＃」が、ＰＩＮコードの中の一つのコードとして登録された場合の認証例を示している。なお、第５の実施形態は、前述した第４の実施形態に対して、仮想キーＶ１２外の記号「＃」をＰＩＮコードの中の一つのコードとして扱うようにした場合の例である。

【０１３５】
図２６（ａ）～図２６（ｄ）は、第５の実施形態において、前述の図２４（ａ）～図２４（ｄ）の例と同様に、各仮想キーＶ１２と、認証対象者の各指先Ｆ０～Ｆ４の位置の一例を示している。図２６（ａ）～図２６（ｄ）の円マークＥＣは、それぞれＰＩＮコードとして登録されている数字に対応した仮想キーＶ１２を示すために描かれている。

【０１３６】
図２６（ａ）の例は、４桁のＰＩＮコードのうち、人差し指による１回目のエアクリックがなされた際、つまり１番目のコード（ＰＩＮ＝１）の入力がなされる際の各指先Ｆ０～Ｆ４の位置の例を示している。図２６（ａ）の例では、人差し指（Ｆ１）による１回目のエアクリックがなされた時点で、入力されるべき正しいＰＩＮコード（１番目のＰＩＮ

コード）が数字「１」で且つその数字「１」を入力するべき手指が中指（Ｆ２）として予め登録されているとする。図２６（ａ）の例では、親指（Ｆ０）が数字「３」、人差し指（Ｆ１）が数字「０」、中指（Ｆ２）が数字「１」、薬指（Ｆ３）が数字「２」、小指（Ｆ４）が数字「６」を指している。このため、図２７に示すように、１番目のコード（ＰＩＮ＝１）を決める際の候補コードは「３，０，１，２，６」となる。

【０１３７】

図２６（ｂ）の例は、２回目のエアクリックがなされた際、つまり２番目のコード（ＰＩＮ＝２）の入力がなされる際の各指先Ｆ０～Ｆ４の位置の例を示している。図２６（ｂ）の例では、人差し指（Ｆ１）による２回目のエアクリックがなされた時点で、入力されるべき正しいＰＩＮコード（２番目のＰＩＮコード）が記号「＃」で且つその記号「＃」を入力するべき手指が親指（Ｆ０）として予め登録されているとする。図２６（ｂ）の例では、親指（Ｆ０）が仮想キーＶ１２外、人差し指（Ｆ１）が数字「７」、中指（Ｆ２）が数字「８」、薬指（Ｆ３）が数字「９」、小指（Ｆ４）が仮想キーＶ１２外を指している。このため、図２７に示すように、２番目のコード（ＰＩＮ＝２）を決める際の候補コードは「＃，７，８，９，＃」となる。

【０１３８】

図２６（ｃ）の例は、３回目のエアクリックがなされた際、つまり３番目のコード（ＰＩＮ＝３）が入力された際の各指先Ｆ０～Ｆ４の位置の例を示している。図２６（ｃ）の例では、人差し指（Ｆ１）による３回目のエアクリックがなされた時点で、入力されるべき正しいＰＩＮコード（３番目のＰＩＮコード）が数字「３」で且つその数字「３」を入力するべき手指が人差し指（Ｆ１）として予め登録されているとする。図２６（ｃ）の例では、親指（Ｆ０）が仮想キーＶ１２外、人差し指（Ｆ１）が数字「３」、中指（Ｆ２）が数字「４」、薬指（Ｆ３）が数字「５」、小指（Ｆ４）が数字「９」を指している。このため、図２７に示すように、３番目のコード（ＰＩＮ＝３）を決める際の候補コードは「＃，３，４，５，９」となる。

【０１３９】

図２６（ｄ）の例は、４回目のエアクリックがなされた際、つまり４番目のコード（ＰＩＮ＝４）が入力された際の各指先Ｆ０～Ｆ４の位置の例を示している。図２６（ｄ）の例では、人差し指（Ｆ１）による４回目のエアクリックがなされた時点で、入力されるべき正しいＰＩＮコード（４番目のＰＩＮコード）が数字「８」で且つその数字「８」を入力するべき手指が小指（Ｆ４）として予め登録されているとする。図２６（ｄ）の例では、親指（Ｆ０）と人差し指（Ｆ１）が共に仮想キーＶ１２外、中指（Ｆ２）が数字「３」、薬指（Ｆ３）が数字「４」、小指（Ｆ４）が数字「８」を指している。このため、図２７に示すように、４番目のコード（ＰＩＮ＝４）を決める際の候補コードは「＃，＃，３，４，８」となる。

【０１４０】

図２６（ａ）～図２５（ｄ）及び図２７の例の場合、１回目のエアクリックの際に取得されたＰＩＮ＝１の各候補コード「３，０，１，２，６」の中で、ＰＩＮ＝１に登録された数字は「１」であり、その数字「１」に対応した手指は中指（Ｆ２）となされている。以下同様に、２回目のエアクリックの際に取得されたＰＩＮ＝２の各候補コード「＃，７，８，９，＃」の中で、ＰＩＮ＝２に登録されているのは記号「＃」であり、その記号「＃」に対応した手指は親指（Ｆ０）となされており、３回目のエアクリック（ＰＩＮ＝３）の際に取得された候補コード「＃，３，４，５，９」の中で、ＰＩＮ＝３に登録されているのは数字「３」であり、その数字「３」に対応した手指は人差し指（Ｆ１）となされており、４回目のエアクリック（ＰＩＮ＝４）の際に取得された各候補コード「＃，＃，３，４，８」の中で、ＰＩＮ＝４に登録されているのは数字「８」であり、その数字「８」に対応した手指は小指（Ｆ４）となされている。

【０１４１】

このため、図２６（ａ）～図２６（ｄ）及び図２７の例の場合、４回のエアクリックによる入力順の４桁のＰＩＮコードとして「１，＃，３，８」が取得され、また１番目のＰ

ＩＮコード「１」については中指（Ｆ２）、２番目のＰＩＮコード「５」については親指（Ｆ０）、３番目のＰＩＮコード「３」については人差し指（Ｆ１）、４番目のＰＩＮコード「８」については小指（Ｆ４）の各指識別情報が得られる。そして、認証対象者について登録されているＰＩＮコードが例えば「１，＃，３，８」の順であり、それら各コードに対応した指識別情報の順番は「中指（Ｆ２）、親指（Ｆ０）、人差し指（Ｆ１）、小指（Ｆ４）」として登録されていた場合、その登録されたＰＩＮコード及び指識別情報と、図２６（ａ）～図２６（ｄ）及び図２７の例で得られたＰＩＮコード及び指識別情報とは一致するため、その認証対象者は正当な登録者であると認証されることになる。

【０１４２】

第５の実施形態の場合、前述の第４の実施形態と同様の効果が得られるだけでなく、仮想キーＶ１２外のエリアについても、ＰＩＮコードの中の一つのコードとして扱っているため、４桁のＰＩＮコードに対し、５の４乗＝６２５通りの候補コードが取得され、第４の実施形態の場合の３２０通りより更に、ハッキング等に対する耐性が高くなる。なお、第５の実施形態の場合のフローチャートは、前述の第４の実施形態の場合と略々同様であるため、その説明は省略する。

【０１４３】

＜その他の実施形態＞

前述した各実施形態では、認証対象者の手３０若しくは指先３１が三次元空間内で所定の時間だけ静止したときに、指先方向に所定距離だけ離れた座標をエアクリック判定のための座標として設定可能となされているが、他の例として、前記静止したと判定された後に、例えば幾つかの指先３１が移動した場合、それら移動した指先３１の中で移動量が最も大きい指によりエアクリックがなされたと判定してもよい。すなわち、前述の図２２の構成を例に挙げて説明すると、前記認証対象者により所望の仮想キーＶ１２に所定の指先３１が合わされた状態で、前述のように手３０等が所定の時間だけ静止された後に、親指から小指までの手指の指先３１が三次元空間内で動いた場合、制御部２５０は、それらの移動量（座標の変化量）をそれぞれ比較して、変化量が最も大きい指先３１によりエアクリックが行われたと判定する。すなわち、この場合における前記変化量が最も大きい指先３１は、前記所望の仮想キーＶ１２に合わせられていた所定の指先３１であり、認証対象者は、その指先３１を大きく動かすことなく、少ない動きでエアクリックを行えることになる。またこの例の場合、例えば認証対象者の肩越しに第三者が覗き見ていたとしても、認証対象者の指先の動きは少なく、また複数の指先が同時に動いているため、どの指でエアクリックが行われたのかを第三者は知ることができない。この例は、前述の各実施形態に適用可能である。

【０１４４】

前述した各実施形態の認証処理装置１は、例えば銀行ＡＴＭや研究所等のような高度なセキュリティ管理が必要とされるシステムに適用可能である。図２８には、各実施形態の個人認証が適用され、サーバによりセキュリティ管理がなされるシステムの概略的な構成例を示している。

【０１４５】

図２８のセキュリティシステムにおいて、サーバ３００は、大別してシステム情報蓄積部３０１、システム制御部３０２、ネットワークＩ／Ｆ部３０３を有して構成されている。ネットワークＩ／Ｆ部３０３は、ネットワーク３０４を介して、サーバ３００によりセキュリティ管理がなされる端末３１０との間で通信可能となされている。各端末３１０には前述した距離センサ２０が併設されている。システム制御部３０２は、このセキュリティシステム全体を制御し、また、ネットワーク３０４を通じて接続されている端末３１０との間で送受信される情報の管理等も行う。

【０１４６】

サーバ３００内のシステム情報蓄積部３０１は、システム全体を管理するための様々な情報とともに、このセキュリティシステムに登録されている全てのユーザの前記ユーザ情報と、全ユーザのＰＩＮコードの情報と、前述した指識別情報とからなる前述のテーブル

情報を蓄積している。このセキュリティシステムの場合、各端末３１０は、全ユーザのテーブル情報を内部に保持しておらず、認証対象者の個人認証が行われる際に当該認証に必要となる情報のみを、ネットワーク３０４を介してサーバ３００から取得する。そして端末３１０は、距離センサ２０の出力信号に対して前述の距離センサ出力解析部と同様の解析のみ行い、サーバ３００は、その解析情報を用いて前述した各実施形態同様にして認証対象者の個人認証を行う。そして、認証対象者が正規のユーザであると判定したとき、サーバ３００は、その認証対象者に対して、例えば銀行ＡＴＭを使用した入出金等の操作を許可したり、室内への出入りを許可（解錠等）したりする。

【０１４７】

なお、前述した情報処理装置１０のように端末３１０が個人認証まで行う場合、前述のステップＳ１にて認証対象者が登録ユーザであると確認できたとき、当該端末３１０は、サーバ３００に蓄積されている全ての登録ユーザのテーブル情報の中で、ステップＳ１で確認したユーザ用に登録されているＰＩＮコードと指識別情報のみをサーバ３００から受け取る。そして、認証対象者が正規のユーザであると端末３１０で判定されたとき、サーバ３００は、その認証対象者に対して、例えば銀行ＡＴＭを使用した入出金等の操作や室内への出入りを許可（解錠等）する。

【０１４８】

また、第２～第５の実施形態では、手の５本の手指を認識する例を挙げたが、例えば左右の手をそれぞれ識別し、さらにそれら左右の手の各５本の手指を個別に識別することも可能である。左右の手の識別は、例えば前述の図１６に示したモデルを例に挙げた場合、親指に相当する指オブジェクトＦ０が左側になっており、小指に相当する指オブジェクトＦ４が右側になっているような場合、右手であると認識することができる。同様に、親指の指オブジェクトＦ０が左側で、小指の指オブジェクトＦ４が右側の場合、左手であると認識することができる。このように、左右の手と合計１０本の手指の全てを識別可能とした場合は、片手の５本の手指を用いる場合よりも更に高いセキュリティレベルを設定することが可能となる。

【０１４９】

また、前述した各実施形態では、ＰＩＮコードの数字をバーチャルタッチパネル４０により入力する例を挙げているが、本発明は数字の入力に限定されず他の文字やアイコンなどをバーチャルタッチパネル４０により入力することで個人認証を行う場合にも適用可能である。

【０１５０】

また、前述の実施形態ではバーチャルタッチパネル４０は仮想二次元パネルとなされているが、三次元的な奥行きを有した仮想三次元パネルであってもよく、この場合、一例として各仮想キーＶ１２を当該仮想三次元パネル内のＺ軸方向の異なる場所に配置してもよい。さらにこの場合、前記基準座標やエアクリック判定座標は、仮想キーＶ１２ごとに設定されていてもよく、それら仮想キーＶ１２ごとに設定されている基準座標やエアクリック判定座標に対してエアクリックが行われたときに、当該仮想キーＶ１２の入力がなされたと判断してもよい。またこの例の場合、ディスプレイ１１に表示されるキー画像１２は、前記仮想三次元パネル内に配された仮想キーＶ１２の奥行きに合わせて、その表示の大きさを変更して、仮想キーＶ１２の奥行きを認証対象者に推測できるようにしてもよい。すなわち、例えば仮想キーＶ１２が奥行き方向の近い場所に配置されるときには、ディスプレイ１１上の該当するキー画像１２を大きく表示し、逆に仮想キーＶ１２が遠い場所に配置されるときには、該当するキー画像１２を小さく表示すれば、認証対象者は、ディスプレイ１１のキー画像１２の大きさにより、仮想キーＶ１２の奥行き方向の配置場所を推測しやすくなると考えられる。

【０１５１】

なお、本実施形態では、バーチャルタッチパネル４０上の所望の位置を指示する所定動作として、当該所望の位置を指先３１等の先端部で押す（或いは、押し込む、突く）動作を例に挙げたが、例えば指先３１で弾く動作（フリック動作）や触れる動作（タッチ動作

）などであってもよい。

【０１５２】

その他、本発明は、以下の処理を実行することによっても実現される。すなわち、上述した実施形態の機能を実現するソフトウェア（プログラム）を、ネットワーク又は各種記録媒体を介してシステム或いは装置に供給し、そのシステム或いは装置のコンピュータ（又はＣＰＵやＭＰＵ等）がプログラムを読み出して実行する処理である。このプログラム及び当該プログラムを記憶したコンピュータ読み取り可能な記録媒体は、本発明に含まれる。

【０１５３】

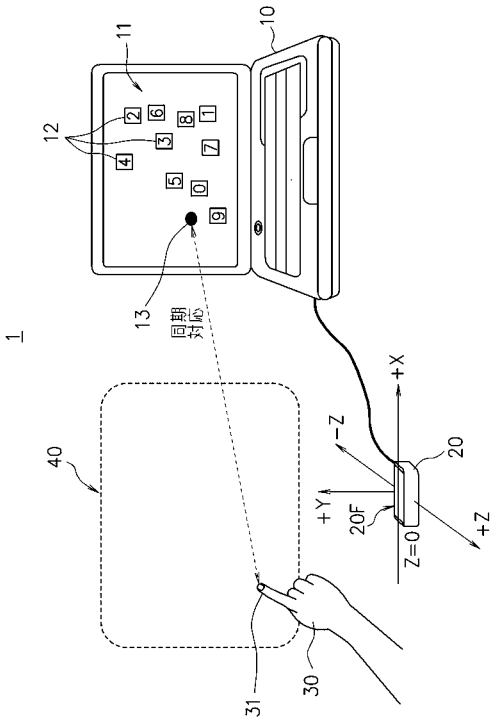
なお、上述した本発明の実施形態は、何れも本発明を実施するにあたっての具体化の例を示したものに過ぎず、これらによって本発明の技術的範囲が限定的に解釈されてはならないものである。すなわち、本発明はその技術思想、又はその主要な特徴から逸脱することなく、様々な形で実施することができる。

【符号の説明】

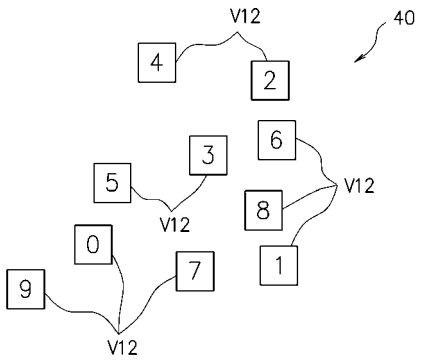
【０１５４】

１：認証処理装置、１０：情報処理装置、１１：ディスプレイ、１２：キー画像、１３：指示マーク、２０：距離センサ、２０Ｆ：センサ面、３０：手、３１：指先、４０：バーチャルタッチパネル、５０：光学結像プレート、５１：反射板、Ｖ１２：仮想キー、１０１：距離センサ出力受信部、１０２，２０２：距離センサ出力解析部、１０３，２０３：入力情報判定部、１０４：解錠制御部、１０５，２０５，２５０：制御部、１０６：ユーザ確認部、１０７，２０７：メモリ部、１１１，２１１：座標算出部、１１２，２１２：対象認識部、１１３：先端座標情報取得部、１１４，２１５：Ｚ座標判定部、１３１：ユーザ情報、１３２：ＰＩＮコード、１３３：指識別情報、１２１：表示制御部、１２２：キー配置制御部、１３１：ユーザ情報、２１３：指識別情報取得部、２１４：指先座標情報取得部、２５５：Ｙ座標判定部

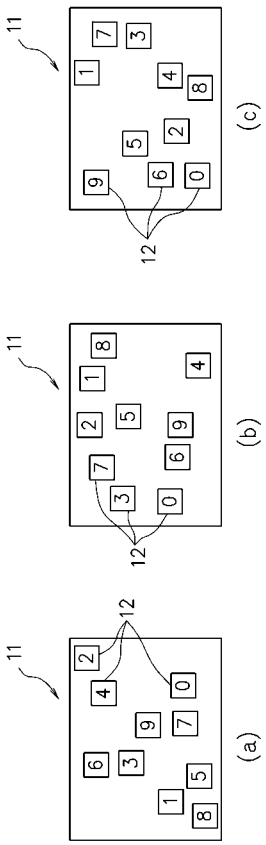
【図１】



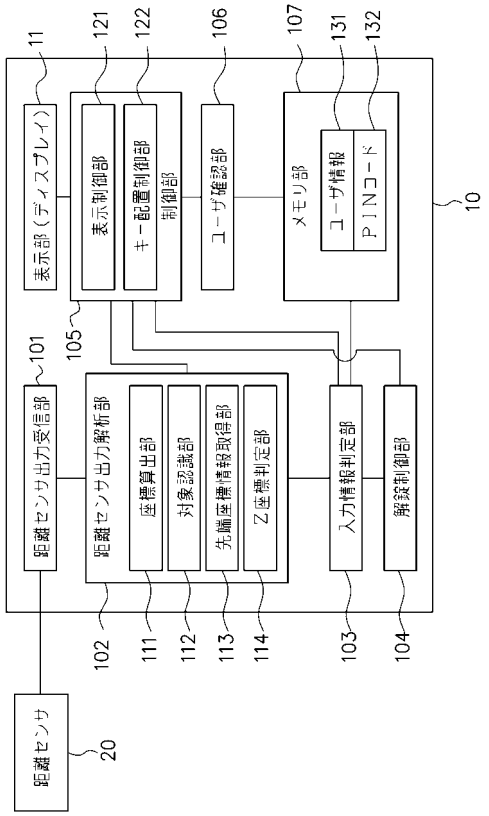
【図２】



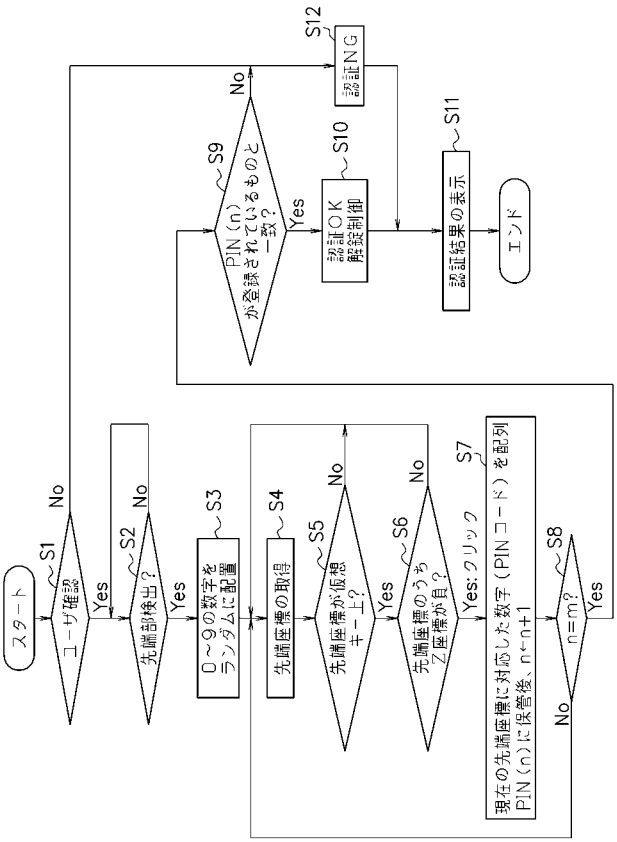
【図３】


11
12
(a)
(b)
(c)

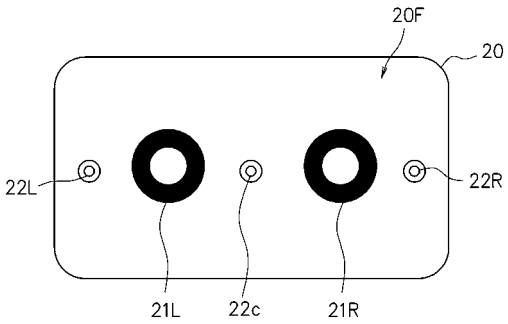
【図４】


表示部（ディスプレイ）
表示制御部
キー配置制御部
制御部
ユーザ確認部
メモリ部
ユーザ情報
ＰＩＮコード
距離センサ出力受信部
距離センサ出力解析部
座標算出部
対象認識部
先端座標情報取得部
乙座標判定部
入力情報判定部
解錠制御部
距離センサ
10
11
20
101
102
103
104
105
106
107
111
112
113
114
121
122
131
132

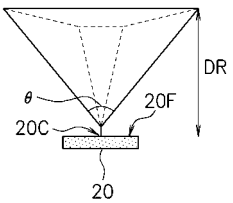
【図５】


スタート
ユーザ確認
先端部検出？
０～９の数字をランダムに配置
先端座標の取得
先端座標が仮想キー上？
先端座標のうち乙座標が負？
Yes：クリック
現在の先端座標に対応した数字（PINコード）を配列PIN（n）に保管後、n←n+1
n=m？
PIN（n）が登録されているものと一致？
認証ＯＫ解錠制御
認証ＮＧ
認証結果の表示
エンド
S1
S2
S3
S4
S5
S6
S7
S8
S9
S10
S11
S12
Yes
No

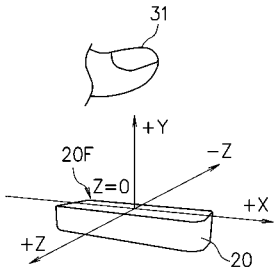
【図６】


20F
20
22L
22R
21L
22c
21R

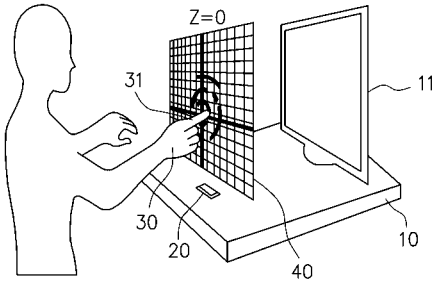
【図７】


DR
θ
20C
20F
20

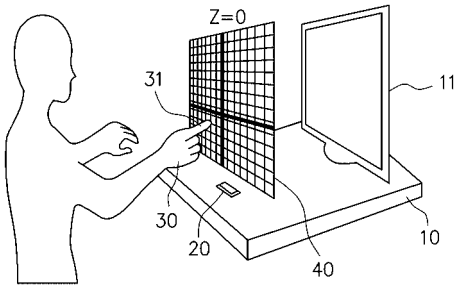
【図８】



【図９】



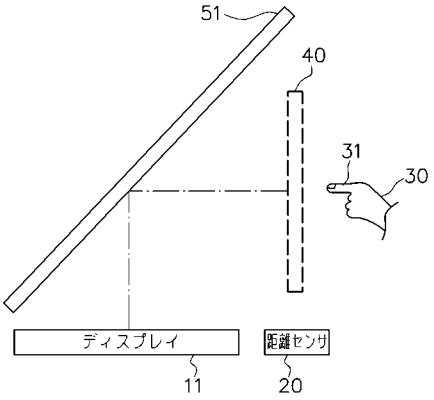
【図１０】



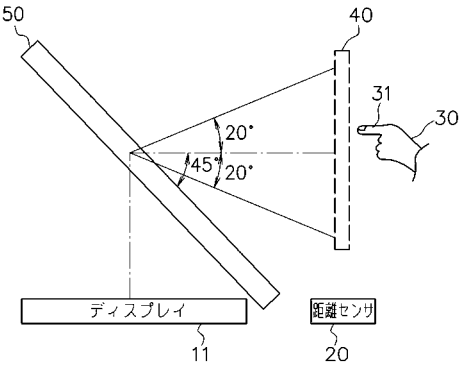
【図１１】

ユーザ情報	U1	U2	U3	U4	.....
PINコード	1,7,6,4	5,3,2,8	1,9,0,4	1,7,6,4	.....

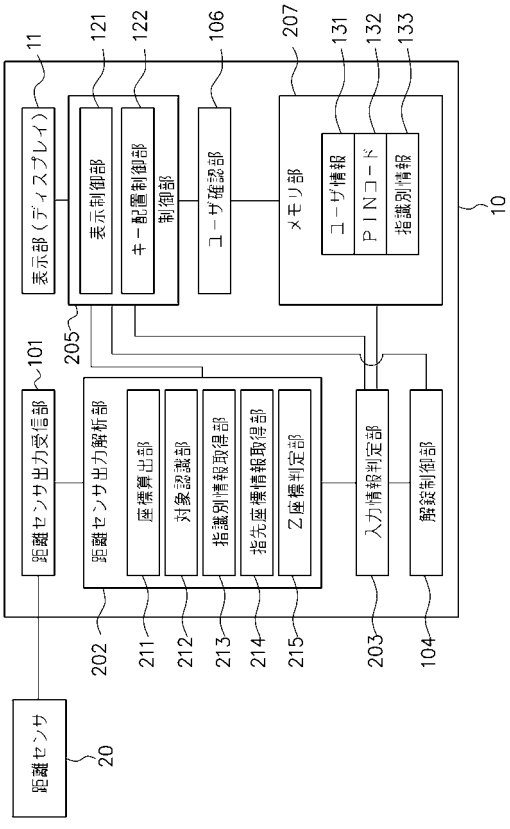
【図１２】



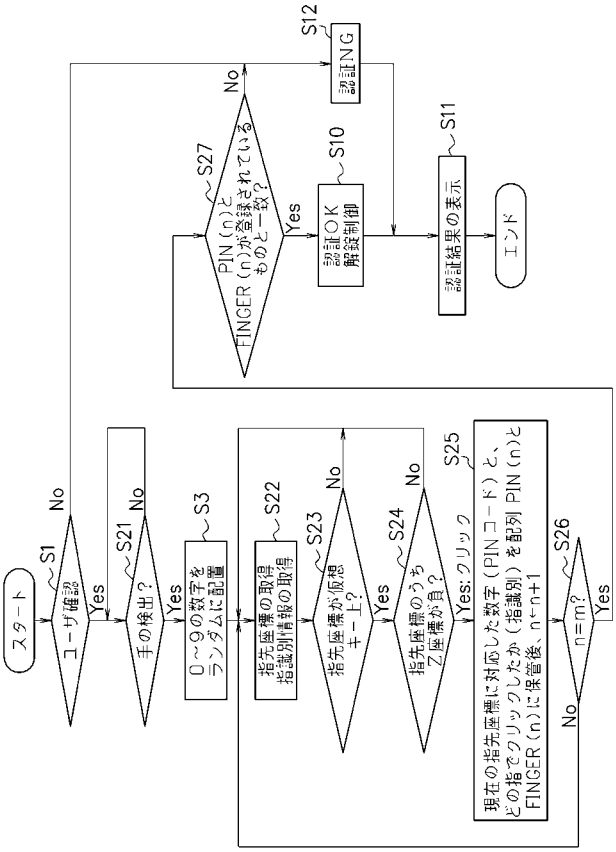
【図１３】



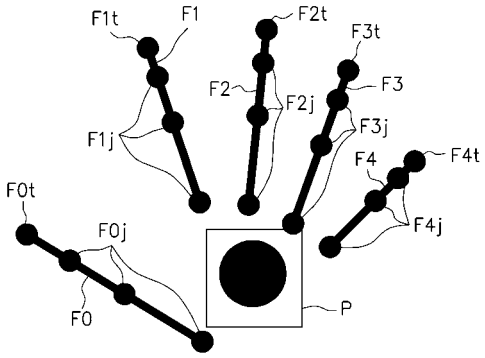
【図１４】



【図１５】



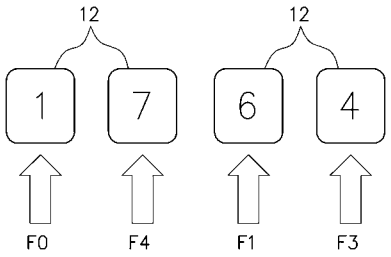
【図１６】



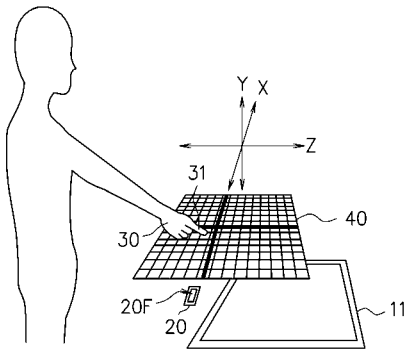
【図１７】

ユーザ情報	U1	U2	U3	U4	.....
PINコード	1,7,6,4	5,3,2,8	1,9,0,4	1,7,6,4	.....
指識別情報	F0,F4,F1,F3	F2,F1,F4,F3	F3,F0,F4,F2	F4,F2,F0,F1	.....

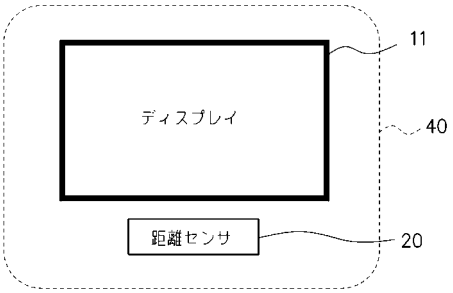
【図１８】



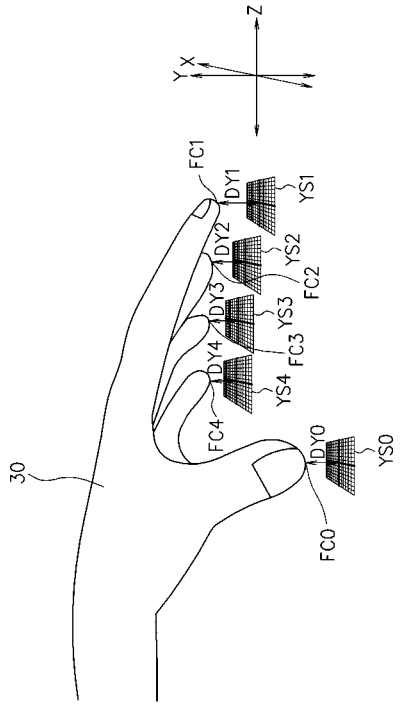
【図１９】



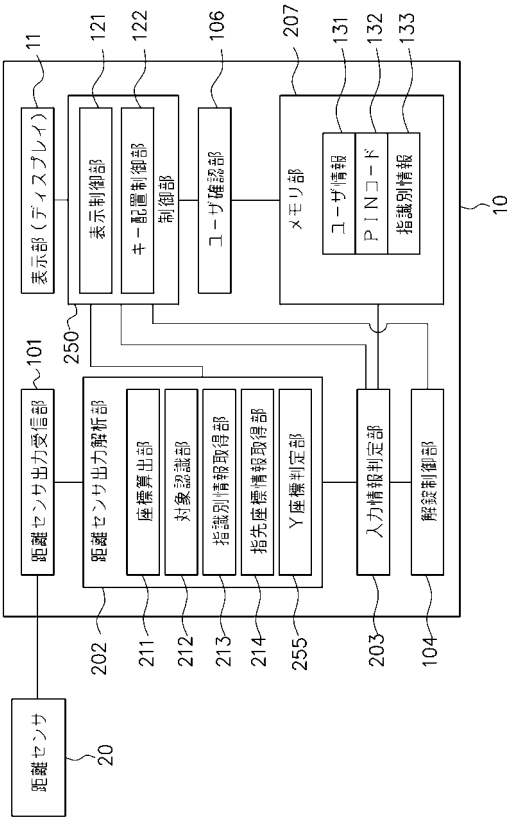
【図２０】



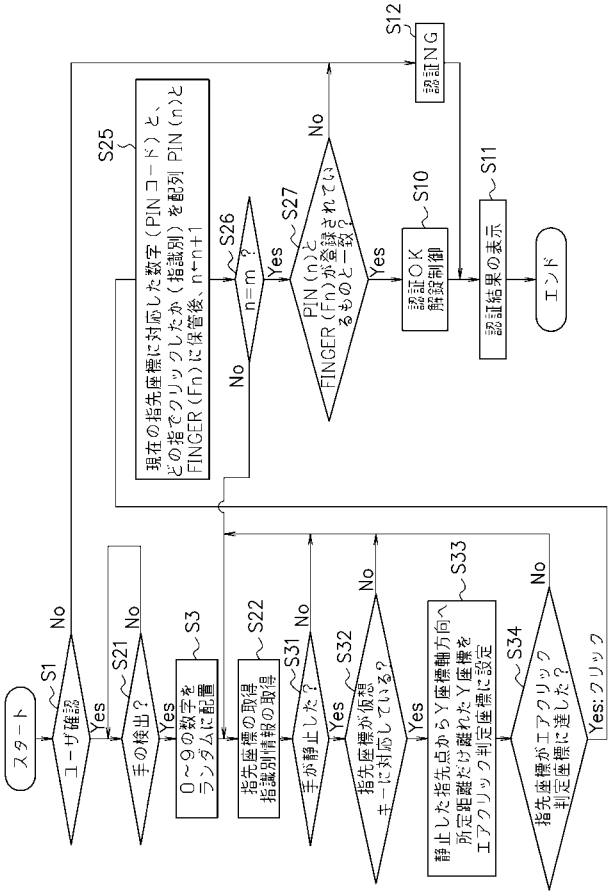
【図２１】



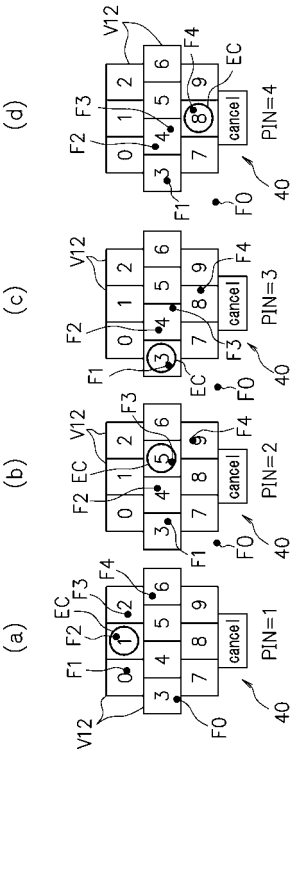
【図２２】



【図２３】

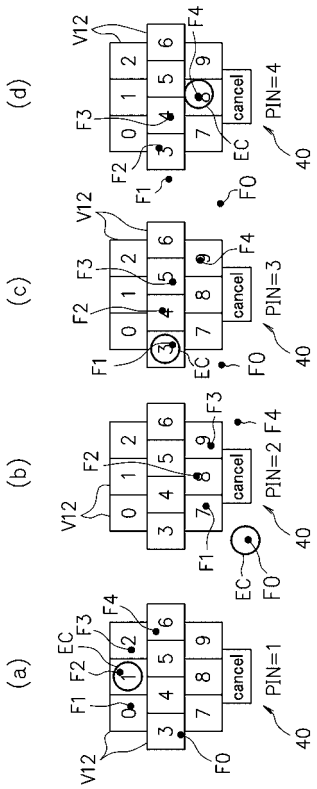


【図２４】



【図２５】

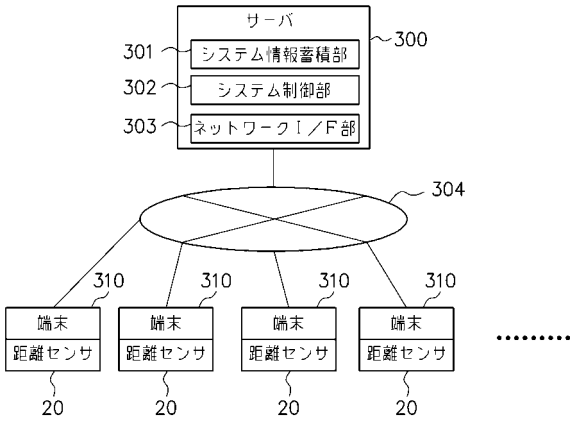
【図２６】



【図２７】

	F0	F1	F2	F3	F4
PIN=1	3	0	①	2	6
PIN=2	⑭	7	8	9	#
PIN=3	#	③	4	5	9
PIN=4	#	#	3	4	⑧

【図２８】



フロントページの続き

(51)Int.Cl. F I テーマコード（参考）
Ｇ０６Ｆ 3/0346 (2013.01)

(72)発明者 田中 亮佑
鹿児島県鹿児島市郡元一丁目２１番２４号 国立大学法人 鹿児島大学内

Ｆターム(参考) 5B020 AA01 DD29
5B087 AA07 AB09
5E555 AA11 AA53 BA03 BB03 BC16 CA12 CA22 CA41 CA42 CB05
CB12 DB20 DB51 EA22 FA00