(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2004-355253
(P2004-355253A)
(43)公開日　平成16年12月16日(2004.12.16)

(51)Int.Cl.[7]	F I			テーマコード（参考）
G06F 15/00	G06F	15/00	330F	5B057
G06T 1/00	G06T	1/00	340A	5B085
H04L 9/32	H04L	9/00	673D	5J104

審査請求 未請求　請求項の数 18　ＯＬ　（全 14 頁）

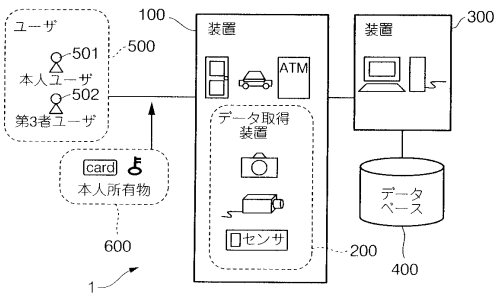
(21)出願番号　特願2003-151165(P2003-151165)
(22)出願日　平成15年5月28日(2003.5.28)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(74)代理人　100064908
弁理士　志賀　正武
(74)代理人　100108453
弁理士　村山　靖彦
(72)発明者　山田　理絵
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　加藤　晃市
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

最終頁に続く

(54)【発明の名称】セキュリティ装置、セキュリティ方法、プログラム、及び記録媒体

(57)【要約】
【課題】ユーザに負担をかけることなく装置の利用を可能にしつつ、不正に装置を利用した人物を特定できるようにする。
【解決手段】ユーザ５００の顔や指紋など本人確認用データを装置１００のデータ取得装置２００によって取得し、取得した本人確認用データを装置３００へ送信する。装置３００は、それが備えるデータ識別手段によって本人確認用データが本人確認可能な生体情報を含んでいるか否かを識別し、含んでいると識別された場合に本人確認用データを認証情報としてデータベース４００に格納するとともに装置１００の使用を許可する。
【選択図】　図１



【特許請求の範囲】
【請求項１】
装置を利用した利用者を認識するための認証情報を蓄積し、前記装置の悪用を防ぐセキュリティ装置であって、
取得された前記利用者の本人確認用データが本人確認可能な生体情報を含んでいるか否かを識別するデータ識別手段と、
前記データ識別手段により前記本人確認用データが前記本人確認可能な生体情報を含んでいると識別された場合に前記本人確認用データを前記認証情報として格納するデータ記憶手段と、
前記データ識別手段により前記本人確認用データが前記本人確認可能な生体情報を含んでいると識別された場合に前記装置の使用を許可する使用許可手段と、
を備えたことを特徴とするセキュリティ装置。
【請求項２】
前記本人確認用データは、顔データであることを特徴とする請求項１に記載のセキュリティ装置。
【請求項３】
前記本人確認用データは、指紋データであることを特徴とする請求項１に記載のセキュリティ装置。
【請求項４】
前記データ識別手段は、予め遮蔽されていない顔部品から作成された辞書用画像データと、前記顔データの部分画像とに基づいて、顔部品が遮蔽されていないかを判断することによって識別を行うことを特徴とする請求項２に記載のセキュリティ装置。
【請求項５】
利用者に行わせる顔の動作を生成する動作生成手段と、前記動作生成手段によって生成された顔の動作が行われたか否かを検出する動作検出手段とをさらに備えており、
前記データ記憶手段は、前記動作検出手段によって前記生成された顔の動作が行われたと検出された場合に前記本人確認用データを前記認証情報として格納することを特徴とする請求項２に記載のセキュリティ装置。
【請求項６】
前記動作生成手段によって生成される顔の動作は、口の開閉、目の開閉、又は目及び口の開閉であることを特徴とする請求項５に記載のセキュリティ装置。
【請求項７】
前記動作生成手段によって生成される顔の動作は、単語の発音であることを特徴とする請求項５に記載のセキュリティ装置。
【請求項８】
前記データ識別手段は、前記指紋データが擬似指紋と生体指紋との何れであるかを判別することによって識別を行うことを特徴とする請求項３に記載のセキュリティ装置。
【請求項９】
装置を利用した利用者を認識するための認証情報を蓄積し、前記装置の悪用を防ぐセキュリティ方法であって、
取得された前記利用者の本人確認用データが本人確認可能な生体情報を含んでいるか否かを識別するデータ識別ステップと、
前記データ識別ステップにおいて前記本人確認用データが前記本人確認可能な生体情報を含んでいると識別された場合に前記本人確認用データを前記認証情報として格納するデータ記憶ステップと、
前記データ識別ステップにおいて前記本人確認用データが前記本人確認可能な生体情報を含んでいると識別された場合に前記装置の使用を許可する使用許可ステップと、
を有することを特徴とするセキュリティ方法。
【請求項１０】
前記本人確認用データは、顔データであることを特徴とする請求項９に記載のセキュリテ

ィ方法。
【請求項１１】
前記本人確認用データは、指紋データであることを特徴とする請求項９に記載のセキュリティ方法。
【請求項１２】
前記データ識別ステップは、予め遮蔽されていない顔部品から作成された辞書用画像データと、前記顔データの部分画像とに基づいて、顔部品が遮蔽されていないかを判断することによって識別を行うことを特徴とする請求項１０に記載のセキュリティ方法。
【請求項１３】
利用者に行わせる顔の動作を生成する動作生成ステップと、前記動作生成ステップにおいて生成された顔の動作が行われたか否かを検出する動作検出ステップとをさらに有しており、
前記データ記憶ステップは、前記動作検出ステップにおいて前記生成された顔の動作が行われたと検出された場合に前記本人確認用データを前記認証情報として格納することを特徴とする請求項１０に記載のセキュリティ方法。
【請求項１４】
前記動作生成ステップにおいて生成される顔の動作は、口の開閉、目の開閉、又は目及び口の開閉であることを特徴とする請求項１３に記載のセキュリティ方法。
【請求項１５】
前記動作生成ステップにおいて生成される顔の動作は、単語の発音であることを特徴とする請求項１３に記載のセキュリティ方法。
【請求項１６】
前記データ識別ステップは、前記指紋データが擬似指紋と生体指紋との何れであるかを判別することによって識別を行うことを特徴とする請求項１１に記載のセキュリティ方法。
【請求項１７】
装置を利用した利用者を認識するための認証情報を蓄積し、前記装置の悪用を防ぐコンピュータを、
取得された前記利用者の本人確認用データが本人確認可能な生体情報を含んでいるか否かを識別するデータ識別手段、
前記データ識別手段により前記本人確認用データが前記本人確認可能な生体情報を含んでいると識別された場合に前記本人確認用データを前記認証情報として格納するデータ記憶手段、及び
前記データ識別手段により前記本人確認用データが前記本人確認可能な生体情報を含んでいると識別された場合に前記装置の使用を許可する使用許可手段、
として機能させることを特徴とするプログラム。
【請求項１８】
装置を利用した利用者を認識するための認証情報を蓄積し、前記装置の悪用を防ぐコンピュータを、
取得された前記利用者の本人確認用データが本人確認可能な生体情報を含んでいるか否かを識別するデータ識別手段、
前記データ識別手段により前記本人確認用データが前記本人確認可能な生体情報を含んでいると識別された場合に前記本人確認用データを前記認証情報として格納するデータ記憶手段、及び
前記データ識別手段により前記本人確認用データが前記本人確認可能な生体情報を含んでいると識別された場合に前記装置の使用を許可する使用許可手段、
として機能させるプログラムを記録したことを特徴とするコンピュータが読み取り可能な記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】

本発明は、装置を利用するためにユーザ本人のみが用いるカードや鍵などの所有物が盗難や紛失などにより第３者に悪用された場合に、悪用した人物を特定することのできるセキュリティ装置、セキュリティ方法、プログラム、及び記録媒体に関する。

【０００２】

【従来の技術】

銀行のＡＴＭや車、入退出システムなどの装置を使用する場合には、ユーザ本人以外の第３者に悪用されないようにするために、利用時にユーザ本人のみが用いるカードや鍵などの所有物が利用される。しかし、ユーザ本人のみが用いる所有物が盗難や紛失などによって第３者に渡った場合には、その第３者の手によって所有物が悪用されて装置が使用される恐れがある。

【０００３】

そのため、従来から、ユーザ本人のみが用いる所有物の盗難や紛失などによる被害防止のためのシステムが提案されている。

例えば、装置を利用する様子をビデオカメラ等で撮影し、撮影した画像を記録として保存する方法がある（例えば、特許文献１参照）。しかし、装置利用時の様子をビデオカメラ等で撮影し保存するだけでは、保存したデータごと盗難にあう恐れがある。このような盗難対策として、撮影した画像をネットワークを介して記録する方法もあるが、いずれの方法においても記録時に人物を特定するために必要な情報を含んでいるかどうかを判断していないという問題があった。

【０００４】

これに対して、装置を利用する人物を特定する方法が提案されている。

例えば、予め装置を利用する人物を登録し、登録された人物以外によって装置が利用されたことを検知した場合、通信装置により登録された人物に対してその旨を通知する盗難対策の技術が開示されている（例えば、特許文献２参照）。

また、車のエンジンをかける際に、ユーザの特微量を捉えることによってユーザ認証を行い登録者本人であると確認された場合にのみ車の使用を許可する技術も開示されている（例えば、特許文献３参照）。

しかし、装置利用時にバイオメトリックスを用いた本人認証を行うためには、ユーザに対して本人認証のための登録を求める必要がある。また、装置を本人以外のユーザが、本人の了承を得て使用するような場合、利用するユーザ全員に必ず事前に登録してもらうことが必要である。このように、ユーザ側の負担が大きいという問題がある。

【０００５】

【特許文献１】

特開平９－２２４２３８号公報

【特許文献２】

特開平１１－２９８６４０号公報

【特許文献３】

特開２００１－６３４００号公報

【０００６】

【発明が解決しようとする課題】

上述したように、ユーザ本人のみが用いる所有物の盗難や紛失などによる被害防止のためのシステムが提案されている。しかし、装置を利用した人物を特定できる情報を獲得して装置が悪用されることに備えており、しかもユーザの許可を得た第３者が装置を容易に使用できるシステムが現状にない。また、このようなシステムでは、獲得した情報そのものの盗難に対しても対策を施す必要がある。

【０００７】

本発明の目的は、本人や本人から装置の使用許可を受けた家族などの第３者などのユーザに負担をかけることなく装置の利用を可能にしつつ、装置を利用した人物を特定できる情報を記録して装置の悪用に対処することが可能なセキュリティ装置、セキュリティ方法、プログラム、及び記録媒体を提供することである。

【０００８】
【課題を解決するための手段】
請求項１に記載のセキュリティ装置は、装置を利用した利用者を認識するための認証情報を蓄積し、前記装置の悪用を防ぐセキュリティ装置であって、取得された前記利用者の本人確認用データが本人確認可能な生体情報を含んでいるか否かを識別するデータ識別手段と、前記データ識別手段により前記本人確認用データが前記本人確認可能な生体情報を含んでいると識別された場合に前記本人確認用データを前記認証情報として格納するデータ記憶手段と、前記データ識別手段により前記本人確認用データが前記本人確認可能な生体情報を含んでいると識別された場合に前記装置の使用を許可する使用許可手段と、を備えたことを特徴とする。
【０００９】
請求項２に記載のセキュリティ装置は、前記本人確認用データは、顔データであることを特徴とする。また、請求項３に記載のセキュリティ装置は、前記本人確認用データは、指紋データであることを特徴とする。
【００１０】
請求項４に記載のセキュリティ装置は、前記データ識別手段は、予め遮蔽されていない顔部品から作成された辞書用画像データと、前記顔データの部分画像とに基づいて、顔部品が遮蔽されていないかを判断することによって識別を行うことを特徴とする。
【００１１】
請求項５に記載のセキュリティ装置は、利用者に行わせる顔の動作を生成する動作生成手段と、前記動作生成手段によって生成された顔の動作が行われたか否かを検出する動作検出手段とをさらに備えており、前記データ記憶手段は、前記動作検出手段によって前記生成された顔の動作が行われたと検出された場合に前記本人確認用データを前記認証情報として格納することを特徴とする。
【００１２】
請求項６に記載のセキュリティ装置は、前記動作生成手段によって生成される顔の動作は、口の開閉、目の開閉、又は目及び口の開閉であることを特徴とする。
【００１３】
請求項７に記載のセキュリティ装置は、前記動作生成手段によって生成される顔の動作は、単語の発音であることを特徴とする。また、請求項８に記載のセキュリティ装置は、前記データ識別手段は、前記指紋データが擬似指紋と生体指紋との何れであるかを判別することによって識別を行うことを特徴とする。
【００１４】
請求項９に記載のセキュリティ方法は、装置を利用した利用者を認識するための認証情報を蓄積し、前記装置の悪用を防ぐセキュリティ方法であって、取得された前記利用者の本人確認用データが本人確認可能な生体情報を含んでいるか否かを識別するデータ識別ステップと、前記データ識別ステップにおいて前記本人確認用データが前記本人確認可能な生体情報を含んでいると識別された場合に前記本人確認用データを前記認証情報として格納するデータ記憶ステップと、前記データ識別ステップにおいて前記本人確認用データが前記本人確認可能な生体情報を含んでいると識別された場合に前記装置の使用を許可する使用許可ステップと、を有することを特徴とする。
【００１５】
請求項１０に記載のセキュリティ方法は、前記本人確認用データは、顔データであることを特徴とする。また、請求項１１に記載のセキュリティ方法は、前記本人確認用データは、指紋データであることを特徴とする。
【００１６】
請求項１２に記載のセキュリティ方法は、前記データ識別ステップは、予め遮蔽されていない顔部品から作成された辞書用画像データと、前記顔データの部分画像とに基づいて、顔部品が遮蔽されていないかを判断することによって識別を行うことを特徴とする。
【００１７】

請求項１３に記載のセキュリティ方法は、利用者に行わせる顔の動作を生成する動作生成ステップと、前記動作生成ステップにおいて生成された顔の動作が行われたか否かを検出する動作検出ステップとをさらに有しており、前記データ記憶ステップは、前記動作検出ステップにおいて前記生成された顔の動作が行われたと検出された場合に前記本人確認用データを前記認証情報として格納することを特徴とする。

【００１８】

請求項１４に記載のセキュリティ方法は、前記動作生成ステップにおいて生成される顔の動作は、口の開閉、目の開閉、又は目及び口の開閉であることを特徴とする。また、請求項１５に記載のセキュリティ方法は、前記動作生成ステップにおいて生成される顔の動作は、単語の発音であることを特徴とする。

【００１９】

請求項１６に記載のセキュリティ方法は、前記データ識別ステップは、前記指紋データが擬似指紋と生体指紋との何れであるかを判別することによって識別を行うことを特徴とする。

【００２０】

請求項１７に記載のプログラムは、装置を利用した利用者を認識するための認証情報を蓄積し、前記装置の悪用を防ぐコンピュータを、取得された前記利用者の本人確認用データが本人確認可能な生体情報を含んでいるか否かを識別するデータ識別手段、前記データ識別手段により前記本人確認用データが前記本人確認可能な生体情報を含んでいると識別された場合に前記本人確認用データを前記認証情報として格納するデータ記憶手段、及び前記データ識別手段により前記本人確認用データが前記本人確認可能な生体情報を含んでいると識別された場合に前記装置の使用を許可する使用許可手段、として機能させることを特徴とする。

【００２１】

請求項１８に記載のコンピュータが読み取り可能な記録媒体は、装置を利用した利用者を認識するための認証情報を蓄積し、前記装置の悪用を防ぐコンピュータを、取得された前記利用者の本人確認用データが本人確認可能な生体情報を含んでいるか否かを識別するデータ識別手段、前記データ識別手段により前記本人確認用データが前記本人確認可能な生体情報を含んでいると識別された場合に前記本人確認用データを前記認証情報として格納するデータ記憶手段、及び前記データ識別手段により前記本人確認用データが前記本人確認可能な生体情報を含んでいると識別された場合に前記装置の使用を許可する使用許可手段、として機能させるプログラムを記録したことを特徴とする。

【００２２】

これらによると、取得した利用者の本人確認用データが本人確認可能な生体情報を含んでいるか否かを識別し、含まれていると識別された場合に本人確認用データを認証情報として記憶するとともに、装置の使用を許可する。このように、利用者の確認ができる場合にのみ装置の使用が許可されるので、ユーザ本人のみが用いる所有物が盗難や紛失などによって悪用された場合には、記憶した認証情報に基づいて、悪用した利用者を特定することが可能になる。また、ユーザ本人やユーザ本人の許可を得た第３者がユーザ本人のみが用いる所有物を使用する場合にも、登録作業など特別な作業を行う必要がなく、ユーザに負担をかけることなく装置の利用が可能になる。

【００２３】

尚、本人確認用データを認証情報として蓄積している事実を公開することによって、装置の悪用を効果的に防止することができる。また、前記本人確認用データをネットワークを介して保存することが可能であり、本人確認用データの盗難などの恐れがある場合には、取得された本人確認用データの識別も含めてネットワークを介して行うことができる。

【００２４】

【発明の実施の形態】

以下、本発明の好適な実施の形態について図面を参照しつつ説明する。

まず、本発明の実施の形態におけるセキュリティシステムのシステム構成について図１を

参照しつつ説明する。図１は、本実施の形態におけるセキュリティシステムのシステム構成を示す図である。

【００２５】

セキュリティシステム１は、図１に示すように、装置１００、装置３００、及びデータベース（データ記憶手段）４００を備えており、装置３００は装置１００を利用する利用者の認証可能な情報をデータベース４００に格納し、これによって装置１００の悪用を防止するものである。尚、装置１００のユーザをユーザ５００、ユーザ本人が用いるＩＤカードや鍵などの所有物を本人所有物６００、本人所有物６００の所有者本人を本人ユーザ５０１、本人ユーザ５０１などにより装置１００の使用が許可された第３者及び装置１００の使用が許可されていない第３者の双方を第３者ユーザ５０２とする。

【００２６】

装置１００は、カメラ、ビデオカメラ、センサ、録音機器などのデータ取得装置２００を備えている。装置１００は、ユーザ５００が本人所有物６００を用いて自機器を利用しようとした場合、装置３００に対して装置利用要請を送信する。また、装置１００は、装置３００からデータ取得指令を受信すると、データ取得装置２００によってユーザ５００の本人確認用データを取り込み、取り込んだ本人確認用データを装置３００へ送信する。尚、装置１００は、例えば、入退室管理システム、銀行などのＡＴＭ、車、コンピュータなど、ユーザ本人及びユーザ本人から使用が許可された第３者以外の者による使用が好ましくない装置である。また、データ取得装置２００によって取得する本人確認用データは、指紋データや顔データなど、ユーザ個人を特定することができるデータである。

【００２７】

装置３００は、装置１００から装置利用要請を受けると、装置１００に対して本人確認用データの取得指令を行い、この応答として装置１００から本人確認用データを取得する。装置３００のデータ識別手段は、取得した本人確認用データが本人確認可能な生体情報を含んでいるか否かを識別する。つまり、本人確認用データにより個人認証が可能であるか否かを判断する。そして、装置３００は、データ識別手段によって個人認証可能であると判断された場合には取得した本人確認用データを認証情報としてデータベース４００へ保存するとともに、装置１００の使用を許可する（使用許可手段）。これによって、ユーザ５００は装置１００を利用することができるようになる。一方、装置３００は、データ識別手段によって個人認証可能でないと判断された場合には再度装置１００に対して本人確認用データの取得指令を行い、装置１００から本人確認用データを再取得する。

【００２８】

図１のセキュリティシステム１では、例えば、本人所有物６００の盗難や紛失などにより本人所有物６００が悪用された場合、本人所有物６００を悪用したユーザをデータベース４００に認証情報として保存された本人確認用データにより特定することが可能である。

【００２９】

次に、上述のセキュリティシステム１における処理について図２を参照しつつ説明する。図２は、セキュリティシステムにおける処理の流れを示すフローチャートである。

まず、装置３００は、装置１００からユーザ５００による装置利用要請を受信する（ステップＳ１）。

【００３０】

装置３００は、装置１００に対してデータ取得指令を行い、この応答として装置１００からデータ取得装置２００により取り込まれたユーザ５００の本人確認用データを取得する（ステップＳ２）。続いて、装置３００のデータ識別手段は、装置１００から取得した本人確認用データが本人確認可能な生体情報を含んでいるか否かを識別し、つまり本人確認用データが個人認証に使用できるか否かを判断する（ステップＳ３）。そして、ステップＳ３において個人認証に使用できないと判断された場合には（ステップＳ４：ＮＯ）、ステップＳ２の処理へ戻り、本人確認用データが個人認証に使用できると判断されるまで、ステップＳ２からステップＳ４の処理を繰り返す。一方、個人認証に使用できると判断された場合には（ステップＳ４：ＹＥＳ）、ステップＳ５の処理へ移行する。

【００３１】
装置３００は、ステップＳ２で取得した本人確認用データを認証情報としてデータベース４００へ保存する（ステップＳ５）とともに、装置３００の使用許可手段は装置１００の利用を許可し（ステップＳ６）、図２の処理を終了する。
【００３２】
但し、ステップＳ３の判断は、取得した本人確認用データが指紋データである場合には、例えば、特開２００２－２７９４１３号公報に開示されている既知の技術を利用して、取得した指紋データが擬似指紋であるか生体指紋であるかを判断することによって行うことができ、生体指紋であると判断された場合に本人確認可能な生体情報を含んでいると識別する。このように判断することによって、人工的に造られた擬似指紋を利用した装置の悪用を防ぐことができる。
また、ステップＳ３の判断は、取得した本人確認用データが顔データである場合、例えば、特開平０９－９１４３２号公報に開示されている既知の技術（遮蔽されていない目や口などの顔部品の小領域から予め作成された辞書用画像データと、背景画像と人物画像（利用者を撮影した本人確認用データ）とを利用して取り出した目や口などの顔部品の小領域の部分画像との相関をとり、相関値が予め定められた閾値以上であれば、遮蔽されていないと判断する技術）を利用して、本人確認可能な程度に目や口、鼻などの顔部品が遮蔽されているか否かを判断することによって行うことができ、本人確認可能な程度に目や鼻、顔などの顔部品が遮蔽されていないと判断された場合に本人確認可能な生体情報を含んでいると識別する。尚、ユーザを特定することなしにステップＳ３の判断を行うことができる。
【００３３】
さらに、上述したセキュリティシステム１における装置１００と装置３００との間で行われる処理について図３を参照しつつ説明する。図３は、セキュリティシステムの装置間で行われる処理のダイアグラムを示す図である。
装置１００は、ユーザ５００により本人所有物６００を用いて自機器の利用が求められると、装置３００へ装置利用要請を送信する。装置利用要請を受信した装置３００は、装置利用要請を送信した装置１００に対してデータ取得指令を送信する。データ取得指令を受信した装置１００は、それが備えるデータ取得装置２００によって利用者の本人確認用データを取り込み、取り込んだ本人確認用データを装置３００へ送信する。
【００３４】
本人確認用データを受信した装置３００は、それが備えるデータ識別手段により受信した本人確認用データが本人確認可能な生体情報を含んでいるか否かを識別し、つまり、個人認証に使用できるか否かを判断する。個人認証に使用できないと判断された場合には、装置３００は装置１００に対して再度データ取得指令を送信し、装置１００から本人確認用データを再度取得する。個人認証に使用できると判断された場合には、装置３００は、装置１００から受信した本人確認用データを認証情報としてデータベース４００へ保存するとともに、それが備える使用許可手段は装置１００に対して装置１００の利用許可を送信する。
【００３５】
上述した説明から分かるように、本人や本人などから装置の使用許可を受けた第３者に負担をかけることなく装置１００の利用を可能にしつつ、データベース４００に記憶された認証情報としての本人確認用データに基づいて装置を悪用した人物を特定することができ、セキュリティの向上が図られる。
【００３６】
以下、上述したセキュリティシステム１の装置１００の一例について図４を参照しつつ説明する。図４は、指紋データを本人確認用データとして取得する銀行のＡＴＭ装置の一例を示す図である。
ＡＴＭ装置は、図１の装置１００に対応し、確認ボタンにはデータ取得装置２００としての指紋センサが組み込まれている。このＡＴＭ装置は、カードが挿入されると装置３００

に対して装置利用要請を送信し、装置３００からデータ取得指令を受信するように構成されている。

【００３７】

ユーザ５００が入力動作終了の際に確認ボタンを押すと、指紋センサは自動的に指紋データを取得する。ＡＴＭ装置は取得した指紋データを装置３００へ送信し、装置３００において指紋データが個人認証に利用することができるか否かが判断され、個人認証に利用することができると判断された場合には装置３００によってＡＴＭ装置の利用が許可されて、ＡＴＭ装置における処理が続行される。一方、個人認証に利用できないと判断された場合には、ＡＴＭ装置はその旨と解決方法（てぶくろをはずすなど）をディスプレイに表示するとともに、ユーザ５００に再操作を促す。

【００３８】

次に、セキュリティシステム１において行われる処理の一例について図５を参照しつつ説明する。図５は、顔データを本人確認用データとした場合のセキュリティシステム１における処理の一例を説明するための図である。尚、図５は、個人認証できる程度に顔が遮蔽されておらず、かつ、顔の動作が正しく行われた場合に顔データを認証情報としてデータベース４００へ保存する例である。

【００３９】

ユーザ５００が、銀行のＡＴＭ装置（図１の装置１００）を使用する場合、ＡＴＭ装置はユーザ５００の所有物６００であるカードを認識するとともに、それが備えるデータ取得装置２００であるカメラによってユーザ５００の顔を撮影し、撮影した顔データを装置１００が備える通信機器によりネットワークを介して装置３００へ送信する。尚、ＡＴＭ装置は、カードを認識すると装置３００へ装置利用要請を送信し、その後装置３００からデータ取得指令を受け取るとカメラによるユーザ５００の顔の撮影を開始する。また、装置３００はデータ取得指令を送信するのに併せて装置３００の動作生成手段によって生成されたユーザに行わせる顔の動作を装置１００へ送信する。

【００４０】

装置３００は、それが備えるデータ識別手段によって装置１００から受信した顔データが個人認証に使用できるか否かを判断する。ここで、ユーザ５００がサングラス、マスク、帽子、面などにより個人認証を行うことができないほど顔を遮蔽していると判断された場合には、ＡＴＭ装置はユーザ５００にその旨を知らせるとともに、再度ユーザ５００の顔を撮影し、撮影した顔データを装置３００へ送信する。

【００４１】

ＡＴＭ装置のカメラによるユーザ５００の顔の撮影は、装置３００の動作生成手段によって生成されたユーザ５００に行わせる顔の動作をユーザ５００に提示しながら行われ、撮影ごとに顔データは装置３００へ送信される。そして、装置３００の動作検出手段によって、顔を撮影した時刻と顔の画像とに基づいて、顔の動作が提示に従って正しく行われたかを検出する。これによってカメラによって撮影されたユーザ５００の顔が写真や擬似顔でないことを確認することができ、写真や擬似顔を利用したＡＴＭ装置の悪用を防ぐことができる。

但し、個人認証に使用できないほど顔が遮蔽されているか否かの判断には顔の動作を提示しながら撮影された顔データが利用される。尚、判断するためにのみ用いるユーザの顔を撮影し、それを利用するようにしてもよい。

【００４２】

装置３００は、個人認証を行うことができる程度に顔が遮蔽されておらず、顔の動作が正しく行われたことが検出された場合に、顔データをデータベース４００へ保存し、ユーザ５００のＡＴＭ装置の使用を許可する。

【００４３】

例えば、本人ユーザ５０１のカードが盗難や紛失などにより本人ユーザ５０１の許諾を得ていない第３者ユーザ５０２によって使用され、そのことが後で判明した場合、銀行関係者などデータベース４００にアクセス権限を持つ者は、データベース４００を参照し本人

ユーザ５０１の許諾なく本人所有物６００を用いた者を特定することができる。
【００４４】
但し、保存する顔データは、保存毎に更新されるものであってもよく、予め設定された回数分を蓄積保存し、以後更新されていくものであってもよく、蓄積し続けるようなものであってもよい。また、装置３００による処理、蓄積、データベース４００の参照などのいずれか、あるいは複数をネットワークを介して行うようにしてもよい。
【００４５】
ここで、装置３００によって行われる顔の動作確認の処理について図６を参照しつつ説明する。図６は、装置３００において行われる顔の動作確認の処理の流れを示すフローチャートである。尚、この処理は、装置１００から装置利用要請があった場合に開始される。装置３００の動作生成手段は、ユーザ５００に行わせる顔の動作、例えば、目の開閉動作、口の開閉動作、又は目及び口の開閉動作を生成する（ステップＳ１１）。そして、装置３００は、ステップＳ１１において生成した顔の動作を装置１００へ送信する（ステップＳ１２）。装置１００は、装置３００から受信した顔の動作に従い、ユーザ５００に対してユーザが行うべき顔の動作を提示し、装置１００が備えるカメラは提示した動作ごとにユーザ５００の顔を撮影し、撮影した顔データを装置３００へ送信し、装置３００は受信した顔データをユーザによる顔の動作として保存する（ステップＳ１３）。そして、装置３００の動作検出手段は、保存した顔データに基づいて、ユーザ５００によって提示した時刻から所定の時間内に提示した動作が正しく行われたか否かを検出する（ステップＳ１４）。
【００４６】
但し、目の開閉動作を指示する場合、動作生成手段は、例えば、右目、左目、両目の瞬き動作をユーザに行わせる顔の動作として生成する。また、口の開閉動作を指示する場合、動作生成手段は、例えば、「ば行」、「ぱ行」、「ま行」などの破裂音を含む単語の発音をユーザに行わせる顔の動作として生成する。例えば、「開口音」、「閉口音」、「破裂音」を組み合わせた単語を予め用意し、或いは任意に作成し、ユーザの発音単語とする。発音単語が「今晩は」であった場合、口の動作は、開口、閉口、開口、閉口、開口となる。このような顔の動作をユーザに提示し、ユーザの顔を撮影し、撮影した顔の画像から目や口の開閉動作を検知し、それが提示された時刻から所定の時間内に行われたものであることを確認する。この顔の画像からの動作の検知は、例えば、特開平０６－７６０５８号公報に開示された既知の技術を利用することによって行うことができる。
【００４７】
ここで、顔の動作を識別する様子について図７を参照しつつ説明する。図７は、顔の動作を単語の発音とした場合における顔の動作を識別する様子の一例を示す図である。
例えば、ユーザに「こんばんは」という単語を発音させる場合には、１文字ずつはっきり発音させるために、左から順にユーザに発音させる文字を提示し（ユーザに発音させる文字のみが見え、それ以外の文字は見えないように表示することによって、ユーザに発音させる文字を提示する。）、データ取得装置２００であるカメラによってユーザの顔を撮影する。装置３００の動作検出手段は、その撮影された画像において、撮影したユーザの顔の口の形からユーザが開口音、閉口音、破裂音の何れを発音したか識別し、提示した文字と比較してユーザが提示した文字を発音しているか否かを判断するとともに、提示した時刻と撮影した時刻との差を検出する。そして、ユーザが提示した文字を発音したと判断され、撮影が提示から予め指定された時間内に行われたと判断された場合には、動作検出手段はユーザによって正しく口の開閉が行われていると判断する。そして、全ての文字が正しく発音されたと判断されると、装置３００の使用許可手段は装置１００の使用を許可する。
図７において、入力パターン１の場合には正しく動作が行われたと検出されて装置の利用が許可され、入力パターン２の場合には「こ」と「は」とが正しく発音されていないと検出されて再度動作を求め撮影を行う。
【００４８】

尚、１文字でも正しく発音されなかった場合には、正しく発音されなかった文字のみを再度発音させてもよいし、単語全ての文字を最初から発音させてもよい。また、装置１００の使用を許可しないようにしてもよい。

【００４９】

上述の装置３００及びデータベース４００は内部に、コンピュータシステムを有している。そして、上述した本人確認可能なデータを認証データとしてデータベース４００に記録するとともに装置１００の使用を許可する処理の過程は、プログラムの形式でコンピュータ読み取り可能な記録媒体に記憶されており、このプログラムをコンピュータが読み出して実行することによって、上記処理が行われる。ここでコンピュータ読み取り可能な記録媒体とは、磁気ディスク、光磁気ディスク、ＣＤ－ＲＯＭ、ＤＶＤ－ＲＯＭ、半導体メモリ等をいう。また、このコンピュータプログラムを通信回線によってコンピュータに配信し、この配信を受けたコンピュータが当該プログラムを実行するようにしても良い。

【００５０】

以上、本発明の好適な実施の形態について説明したが、本発明は上述の実施の形態に限られるものではなく、特許請求の範囲に記載した限りにおいて様々な設計変更が可能なものになっている。

【００５１】

【発明の効果】

以上説明したように、本発明によれば、取得した利用者の本人確認用データが本人確認可能な生体情報を含んでいるか否かを識別し、含まれていると識別された場合に本人確認用データを認証情報として記憶するとともに、装置の使用を許可する。このように、利用者の確認ができる場合にのみ装置の使用が許可されるので、ユーザ本人のみが用いる所有物が盗難や紛失などによって悪用された場合には、記憶した認証情報に基づいて、悪用した利用者を特定することが可能になる。また、ユーザ本人やユーザ本人の許可を得た第３者がユーザ本人のみが用いる所有物を使用する場合にも、登録作業など特別な作業を行う必要がなく、ユーザに負担をかけることなく装置の利用が可能になる。

【図面の簡単な説明】

【図１】本実施の形態におけるセキュリティシステムのシステム構成を示す図である。

【図２】セキュリティシステムにおける処理の流れを示すフローチャートである。

【図３】セキュリティシステムの装置間で行われる処理のダイアグラムを示す図である。

【図４】セキュリティシステムを構成する指紋データを本人確認用データとして取得する装置の一例を示す図である。

【図５】顔データを本人確認用データとした場合のセキュリティシステムにおける処理の一例を説明するための図である。

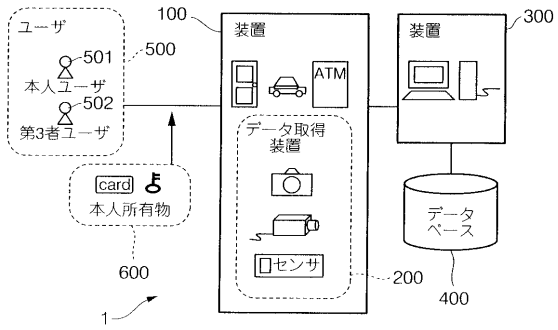
【図６】セキュリティシステムを構成する装置において行われる顔の動作確認の処理の流れを示すフローチャートである。

【図７】顔の動作を単語の発音とした場合における顔の動作を識別する様子の一例を示す図である。

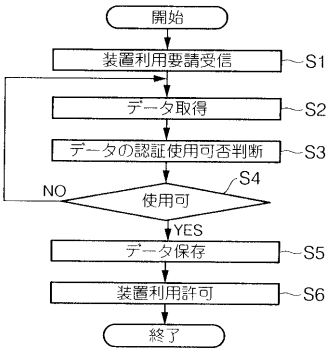
【符号の説明】

１　セキュリティシステム、　１００　装置、　２００　データ取得装置、　３００　装置、　４００　データベース

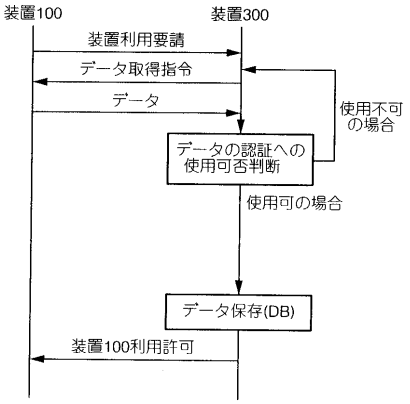
【図１】



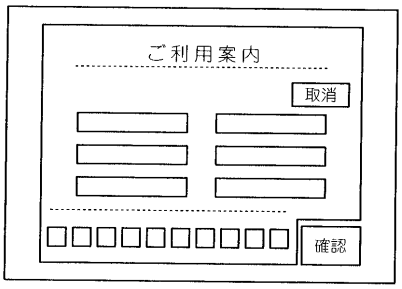
【図２】



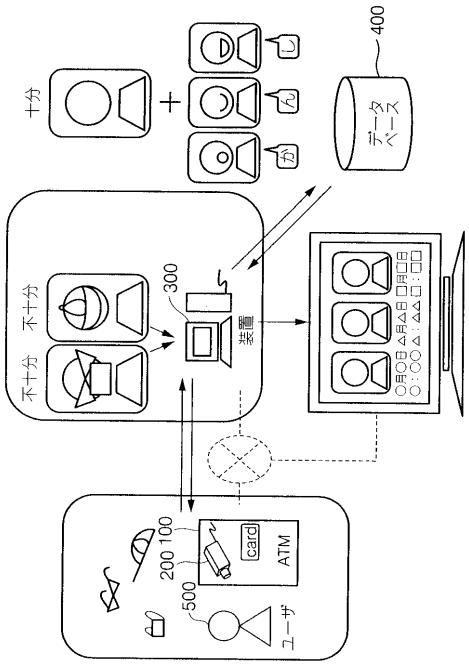
【図３】



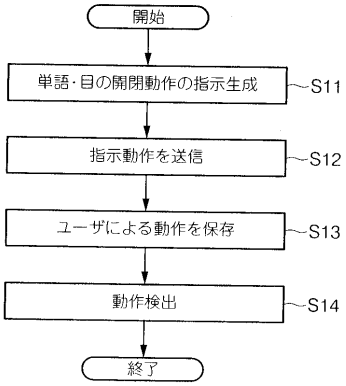
【図４】



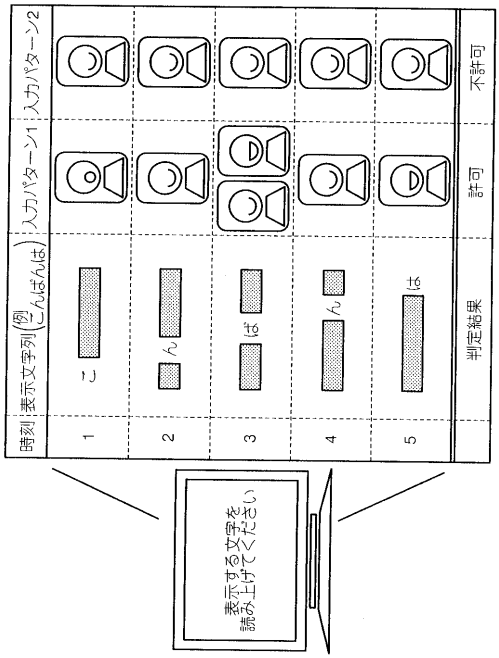
【図５】



【図６】



【図７】


時刻
表示文字列(例:こんばんは)
入力パターン1
入力パターン2
判定結果
1
2
3
4
5
こ
ん
ば
ん
は
許可
不許可
表示する文字を
読み上げてください

フロントページの続き

(72)発明者　荒川　賢一
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

Ｆターム(参考) 5B057 AA20 DA12 DB02 DB09 DC01 DC32 DC33
5B085 AA08 AE25 AE26 BA06
5J104 KA01 KA17