(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5739336号
(P5739336)
(45)発行日　平成27年6月24日(2015.6.24)　(24)登録日　平成27年5月1日(2015.5.1)

(51)Int.Cl.　F I
G06K 19/10 (2006.01)　G06K 19/10

請求項の数 22　(全 17 頁)

(21)出願番号　特願2011-530326(P2011-530326)
(86)(22)出願日　平成21年10月7日(2009.10.7)
(65)公表番号　特表2012-517626(P2012-517626A)
(43)公表日　平成24年8月2日(2012.8.2)
(86)国際出願番号　PCT/AT2009/000388
(87)国際公開番号　WO2010/040162
(87)国際公開日　平成22年4月15日(2010.4.15)
審査請求日　平成24年10月9日(2012.10.9)
(31)優先権主張番号　A1570/2008
(32)優先日　平成20年10月7日(2008.10.7)
(33)優先権主張国　オーストリア(AT)

前置審査

(73)特許権者　511088483
アスマク－ホールディング　ゲゼルシャフト　ミット　ベシュレンクテル　ハフツング
オーストリア国，４６４５　グリューナウ　イム　アルムタル，ヘッケナウ　３４
(74)代理人　100099759
弁理士　青木　篤
(74)代理人　100092624
弁理士　鶴田　準一
(74)代理人　100114018
弁理士　南山　知広
(74)代理人　100165191
弁理士　河合　章

最終頁に続く

(54)【発明の名称】識別手段

(57)【特許請求の範囲】
【請求項１】
認証に基づいて人間を識別する識別手段（１）であって、支持層（２）と、再書き込み可能な不揮発性半導体メモリ（５）を有する認証デバイス（４）と、人間に関する特徴（３）と、通信コネクタ（８）を有する通信システム（７）とを具備し、前記識別手段（１）が前記人間に関する特徴（３）によって個人設定されるとともに、法的権限者（１８）が、前記法的権限者（１８）に前記識別手段（１）を提示した人間の身元を、チェックした後、前記人間に関する特徴（３）にリンクされる第１の電子キー（６）は、前記再書き込み可能な不揮発性半導体メモリ（５）に記憶され、前記第１の電子キー（６）は、前記法的権限者（１８）によって発行され、
前記人間に関する特徴（３）は、人間の画像であり、前記画像は、人間の画像を管理する国際的に認められる規格を満たし、具体的にはＩＣＡＯの要求を満たし、
第２の電子キー（１１）が記憶され、
前記第２の電子キー（１１）は、前記第１の電子キー（６）にリンクされ、
前記第２の電子キー（１１）は、第３者に前記識別手段（１）を提示する人間の身元をチェックするために、発行認証及び証明機関とともに前記第３者によってチェックされることを特徴とする識別手段。
【請求項２】
認証に基づいて人間を識別する識別手段であって、人間に関する特徴（３）の電子画像及び第１の電子キー（６）が記憶される電子データセットを具備し、前記第１の電子キー

（６）は、前記人間に関する特徴（３）にリンクされ、前記第１の電子キー（６）は、法的権限者（１８）によって発行されることを特徴とする識別手段。
【請求項３】
前記支持層（２）は、身分証明書、バンクタイプのデータカード、携帯型データメモリを含むグループから選択される請求項１に記載の識別手段。
【請求項４】
前記人間に関する特徴（３）は、バイオメトリックの特徴である請求項１～３のいずれか一項に記載の識別手段。
【請求項５】
前記第１の電子キー（６）は、認証及び証明機関（２１）が発行するキーである請求項１～４のいずれか一項に記載の識別手段。
【請求項６】
前記認証デバイス（４）は、データ処理ユニット、及び暗号化モジュール（１０）を有する請求項３～５のいずれか一項に記載の識別手段。
【請求項７】
前記通信コネクタ（８）は、無線通信により動作するように配置される請求項３～５のいずれか一項に記載の識別手段。
【請求項８】
前記リンクは、単方向操作により設定される請求項１～７のいずれか一項に記載の識別手段。
【請求項９】
前記第２の電子キー（１１）は、法的権限者（１８）により発行される電子キーである請求項１～８のいずれか一項に記載の識別手段。
【請求項１０】
前記人間に関する特徴（３）のデジタル画像（３１）は、前記再書き込み可能な不揮発性半導体メモリ（５）に記憶される請求項３～９のいずれか一項に記載の識別手段。
【請求項１１】
前記第１の電子キー（６）は、コードフォーマットで前記デジタル画像（３１）に記憶される請求項１０に記載の識別手段。
【請求項１２】
前記電子データセットは、データ処理ユニットの再書き込み可能な不揮発性半導体メモリに記憶される請求項２～１１のいずれか一項に記載の識別手段。
【請求項１３】
前記データ処理ユニットは、遠隔データセンタが前記電子データセットにアクセス可能なように配置される通信コネクタを有する請求項１２に記載の識別手段。
【請求項１４】
前記電子データセットは、携帯型データメモリに記憶される請求項２～１３のいずれか一項に記載の識別手段。
【請求項１５】
具体的には請求項１～１４のいずれか一項に記載される識別手段である識別手段によって、人間を識別及び認証する方法であって、
再書き込み可能な不揮発性半導体メモリ（５）又は電子データセットに人間に関する特徴（３）及び（９）を記憶する工程と、
法的権限者（１８）によって、人間（１５）を正当化する工程と、
前記再書き込み可能な不揮発性半導体メモリ（５）又は前記電子データセットに法的権限者（１８）の第１のキー（６）を記憶する段階と、
前記人間に関する特徴（３）に前記第１のキー（６）をリンクする段階と、
を含む方法。
【請求項１６】
認証及び証明機関（２０）の第２の電子キー（１１）が前記再書き込み可能な不揮発性

半導体メモリ（５）又は前記電子データセットに記憶される請求項１５に記載の方法。
【請求項１７】
人間に関するデータの基準セットが外部メモリユニットに記憶される請求項１５又は１６に記載の方法。
【請求項１８】
人間に関するデータの基準セットが前記識別手段（１）、具体的には前記再書き込み可能な不揮発性半導体メモリ（５）に記憶される請求項１５～１７のいずれか一項に記載の方法。
【請求項１９】
人間に関するデータの記憶される基準セットが物理的に存在する人間に関するデータセットと比較される請求項１７又は１８に記載の方法。
【請求項２０】
前記記憶される人間に関する特徴（３）及び（９）は、人間を識別及び認証する手段として前記検出された特徴と比較される請求項１５～１９のいずれか一項に記載の方法。
【請求項２１】
前記人間に関する特徴は、検出直後に前記第１の電子キー（６）にリンクされる請求項１５～２０のいずれか一項に記載の方法。
【請求項２２】
前記人間に関する特徴は、法的権限者の前で、又は法的権限者により、リアルタイムに検出される請求項２１に記載の方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、認証に基づいて人間を識別する識別手段であって、支持層と、再書き込み可能な不揮発性半導体メモリの形式で提供されるメモリ手段を有する認証デバイスと、人間に関する特徴と、通信コネクタを有する通信システムとを具備する識別手段に関する。さらに、本発明は、認証に基づいて人間を識別する識別手段であって、人間に関する特徴の電子画像及び第１の電子キーが記憶される電子データセットを具備する識別手段に関する。また、本発明は、識別手段により人間を識別及び認証する方法に関する。
【背景技術】
【０００２】
人間を識別する識別手段は、公知であり、大抵は、識別手段に記憶される人間のデータと、識別手段を持ち歩く人間の特徴との一致のための光学的チェックに基づき、それを調査権限者に提示する。大抵は、この一致チェックは、人間により実行されるが、自動システムが少なくとも一部を読み込んで、処理できる識別手段によるシステムもまた既知である。人間による光学的な視覚比較チェックの場合、既知の情報の特徴の欠点がある。すなわち、潜在的な加害者がこの種の特徴を偽造して、有効な識別手段を操作することよって、不正の意図を有する他人が使用することが可能である。さらにまた、一致に使用される評価基準は、人間の主観的な評価にある程度依存し、とりわけその時点でのそれぞれの条件に依存する。したがって、客観的なチェックは、保証できない。
【発明の概要】
【発明が解決しようとする課題】
【０００３】
したがって、本発明の根本的な目的は、人間の識別及び認証を一義的に保証する識別手段を提案することである。
【０００４】
この目的は、本発明では、人間に関する特徴にリンクする第１の電子キーが、識別手段のメモリ手段に記憶されることにより、達成される。
【課題を解決するための手段】
【０００５】

有利には、この実施形態は、操作に対して非常に保護される。潜在的な加害者が成功するためには、人間に関する特徴と、随意的には第１の電子キーであるリンクとの双方を操作しなければならないためである。人間に関する特徴は、第１の電子キーは、メモリ手段、すなわち認証デバイスに記憶されるので、潜在的な加害者は、認証デバイスを操作しなければならないが、認証デバイスでは、非常な努力にかかわらず成功する可能性が非常に小さい。

【０００６】

第１の電子キーは、英数字コードなどの擬似乱数コードの形式で提供してもよい。このようなキーは、アルゴリズムによって、規定の方法で生成されるが、観察者にはランダムな文字配置である印象を与えることができる。具体的には、これによって、いわゆるブルートフォースアタックが通過できない一義的かつ固有な電子キーを生成することが可能になる。具体的には、このようなキーの可能な全ての組み合わせをチェックするために必要であろう努力は、加害者が対応可能な時間及び技術を超えることになる。

【０００７】

人間に関する特徴を電子キーにリンクすることにより、人間に関する特徴と組み合わせる偽造に対する保護の観点で、電子キーという利点を有する特徴の組み合わせが提供される。したがって、有利には、識別手段は、人間を固有に識別及び認証することにおいて、セキュリティの著しい向上を提供するように配置される。

【０００８】

また、本発明の目的は、電子データセットを組み込む識別手段によって達成される。この場合でも、第１の電子キーは、人間に関する特徴に再びリンクされる。この配置の利点は、電子データセットは、好適にはデータ処理ユニットを有する自動検出システムによって直接的に処理できることにある。具体的には、身元チェックを実行するために、識別手段に接続される通信を確立する検出デバイスを提供する必要がない。この配置の他の利点は、識別する特徴が、データ処理に伝送され、かつデータ処理に置かれることである。具体的には、これは、記憶される人間に関する特徴に基づいて、識別及び／又は認証を実行するために使用できる公知のデバイスであって、かつ広く使用される利用可能なデバイスであることを意味する。

【０００９】

法律的な理由、すなわち法定の理由により、人間が識別手段を持ち運ぶ必要があるかもしれない。このため、他の実施形態では、支持層が身分証明書の形式で提供される。したがって、識別手段は、運転者の運転免許証などにしてもよく、国境を越えて旅行するための旅券の配置に基づいてもよい。人間を識別するシステムの信頼性を向上させる観点から、チェックポイントのネットワーク化を可能にするために、識別手段は、自動検出システムで処理可能なように配置してもよい。具体的には、人間に関する特徴は、機械可読な検出処理の要件を充足することが可能である。人間に関する特徴を検出する光学システムなどの場合、人間に関する特徴は、特徴の構成要素が種々のスペクトル成分に適用されるように配置される。これは、人間に関する特徴が、光学的な可視領域でチェック可能なだけでなく、ＩＲ領域及びＵＶ領域などの特徴成分を作り出し、かつ検出して比較できることを意味する。機械可読な身分証明書に基づく配置において、人間に関する特徴のチェックは、再生可能な同一の基準に基づいて常に実行され、権限者が適用する個々の評価基準による不確実な要素は、排除されるという他の利点を有する。

【００１０】

支持層がバンクタイプのデータカードとして配置される実施形態では、特有の利点を有する。この場合、チップカードに基づく配置が特に好適である。主張される実施形態では、バンクカードが特に小型であるので、大きさ及び／又は形状によって移動の自由を制約することなしに人間が常に持ち運ぶことができるという明確な利点を提示する。具体的には、財布など常に持ち運ぶものに入れて持ち運ぶことができることが、バンクカードに基づく配置の利点である。

【００１１】

また、支持層は、ＵＳＢスティック又はメモリカードなど、当業者に公知の形式の携帯型データメモリの形式で提供できる。技術的進歩により、このような携帯型データメモリデバイスは、非常に小さく、かつ強力になっているので、より大きな記憶能力を提供する。このため、携帯型データメモリデバイスは、非常に多くのユーザが既に持ち運んでおり、有利には、本発明が提案する識別手段の支持層として使用可能である。

【００１２】

１つの実施形態に基づくと、人間に関する特徴は、人間の画像の形式で提供される。具体的には写真である人間の画像によって、人間に関する特徴と、識別手段を物理的に提示する人間との間の一致を、非常に迅速にチェックすることが可能になる。有利には、本発明が提案する第１の電子キーへのリンクにより、この形式の人間に関する特徴は、改良され、人間に関する特徴及び識別手段を操作することが非常に困難であるが、簡明かつ迅速な視覚的比較が可能になる。

【００１３】

好適には、人間に関する特徴の画像は、支持層上に配置される。この利点は、画像と物理的に存在する人間との比較により、人間の迅速な視覚的なチェックが保証できることである。

【００１４】

信頼性が高い検出を保証し、かつ画像による人間の識別及び認証を保証するために、画像が人間の画像を管理する国際的に認められる規格に従う１つの実施形態では、非常に明確な利点が提示される。好適には、国際民間航空機関（International Civil Aviation Organization、ＩＣＡＯ）の要求が使用される。ＩＣＡＯは、人間の顔が撮影されるべき方法を具体的に規定し、かつ人間の表情に関連する従うべき要求を特定する。この国際的に許容される規格によって、自動化された基準などで人の画像を処理することが可能になる。国際的な規格に従うことにより、国際的に許容され、かつ国際的な規格による比較が世界中で使用できることを保証することは、他の主要な利点である。

【００１５】

人間に関する特徴として人間の画像を使用することに加えて、人間に関する特徴は、バイオメトリックの特徴にしてもよい。バイオメトリックの特徴は、操作することが極めて困難又は不可能であるので、人間を識別及び認証することに対して非常に程度が高いセキュリティを提示することは、利点である。バイオメトリックの特徴は、指紋、虹彩画像、肌構造、血管構造、又は代替的には音声にできる。バイオメトリックの特徴は、電子的なフォーマットに変換されて、本発明で提案される識別手段に記憶できる。

【００１６】

識別手段のセキュリティの観点から、第１のキーが認証及び証明機関のキーの形式で提供される１つの実施形態では、具体的な利点を有する。通常、このような機関は、電子キーの発行及び管理に関して非常に高い規格を設定する国際的に認められる組織である。しかしながら、このような機関が他の組織に依存しないキーを発行及び管理することによって、非常に高い程度の独立性を保証するので、外部の影響が非常に低いことを保証することは、非常に重要である。例えば、第１の電子キーは、いわゆる公開鍵システムの一部にしてもよい。ここで、キーの１つの部分は、公開的に知られるが、秘密鍵の部分は、認証及び証明機関のユーザにのみ知られる。

【００１７】

例えば、第１の電子キー及びリンクは、潜在的な加害者が操作を試みた場合、第１のキー又はリンクを不可逆的に破壊するように構成してもよい。

【００１８】

第１のキー及び人間に関する特徴は、認証デバイスのメモリ手段に記憶される。このため、認証デバイスがデータ処理ユニット又は暗号化モジュールを有する場合は、記憶される特徴に直接アクセスする手段を防止できることは、有利である。セキュリティ上の理由により、自動化された人間識別機関などの外部チェックデバイスが、記憶されるキー、人間に関する特徴、又はリンクに直接的にアクセスしないことは、特に実用的である。主張

される実施形態では、記憶される特徴は、暗号化されて、潜在的な加害者が利益を得ないようにできる。この配置は、記憶される特徴が高い秘密を維持することによって、不正アクセスの可能性を防止するという具体的な利点を有する。例えば、電子キーは、単方向の暗号化アルゴリズムにより暗号化される。識別手段にアクセスして、人間に関する特徴をチェックするとき、認証デバイスの人間識別機関は、識別手段にアクセスするために正確なキーリザルトを提示しなければならない。総当たり攻撃の場合、可能なキーリザルトを試みることによって、アクセスを得ることが試みられる。いくつかの不正確なアクセスの試みが誤ったキーリザルトを生じた後、認証デバイスは、アクセスを完全にブロックする保護メカニズムを始動する。これにより、例えば、第１の電子キーの新しいリンクを人間に関する特徴に要求することができる。しかしながら、認証デバイスは、第１のキー及び／又は人間に関する特徴を破壊するなどによって、識別手段を使用不可にすることもまた可能であろう。

【００１９】

本発明が提案する識別手段を可能な限りユーザフレンドリに使用及び展開する観点から、通信コネクタが無線接続を確立するように配置できる１つの実施形態では、利点がある。この場合、本発明が提案する識別手段を実行するユーザは、検出デバイスの横を通り抜けることが可能であり、検出デバイスは、通信システムを介して認証デバイスと無線通信することによって、互換性などによって、第１のキー及び／又は随意的には他の人間に関する特徴をチェック又は検証することが可能である。具体的には非常に多くの人が通る領域において、この配置は、識別手段を示すために人間の流れが減速しないという具体的な利点を提示する。人々が検出デバイスを通ることにより、関連する特徴を読み出し、人々の自動識別又は認証を実行される。

【００２０】

１つの実施形態において、検出デバイスは、データ処理ユニットに接続できる。例えば、データ処理ユニットは、第１の電子キーを読み込んで、チェックした後に、記憶される識別手段の基準データを読み出す中央データ記憶デバイスにアクセスする。これらの基準の特徴は、これらの特徴と、現に存在する人間の特徴とを比較する検査官に表示できる。

【００２１】

確実に人間を認証及び識別する観点から、識別手段のセキュリティが、第２の電子キーを記憶する場合、識別手段のセキュリティを向上できる。第１の実施形態に基づくと、第２の電子キーは、認証デバイスのメモリ手段に記憶できる。また、第２の実施形態に基づくと、第２の電子キーは、電子データセットに記憶できる。この第２の電子キーは、第１の電子キーに依存しないため、他の認証及び証明機関の付加的なセキュリティ特徴を識別手段に記憶できる。本発明が提案する識別手段をチェックするとき、制御センタは、互いに独立な２つの電子キーをチェックすることができる能力を有する。このため、高い程度のセキュリティで人間を識別及び認証する。また、この実施形態は、規定された方法で同時に２つのキーを操作する必要があり、誤った身元を取得するので、潜在的な加害者が本発明が提案する識別手段を操作することは、非常に困難になる。

【００２２】

第２のキーが第１のキーにリンクする場合、２つのキーの不可逆性の固有なリンクがあるので、特に有利な実施形態が取得される。これは、人間を識別及び認証する処理の信頼性の観点から特に実用的利益を有する。また、これによって、潜在的な操作がより困難になる。リンクは、例えば、逆転できないキーの生産物を作り出すように設定できる。言い換えると、リンクの生産物から２つのキー部に遡ることができないキーの生産物を作り出すように設定できる。

【００２３】

人間に関する特徴と、第１のキーとの間のリンクは、単方向操作に基づいて設定できる。これにより、リンクの生産物から元の初期生産物に遡ることが不可能になる。特に単方向のリンクの場合、記憶されるリンクの生産物のみである。人間を識別及び認証するとき、リンクは、適当なチェックアルゴリズムなどにより認証センタにより再作成又は生成さ

れて、記憶されるリンクと比較される。これによって、セキュリティに関連する本質的な具体的特徴をチェックすることなしに、固有の一致をチェックすることが可能である。

【００２４】

第１及び／又は第２の電子キーが法的権限を有する人間の電子キーの形式で提供される実施形態は、特に実用的利点を有する。法的権限を有する人間は、弁護士又は公証人などにしてもよい。とにかく、法的権限を有する人間は、識別手段の認証に関する法的拘束力を有する証明書を発行する法的地位の権限を使用できる人間である。例えば、人間は、法的権限を有する人間に識別手段を示すことになる。法的権限を有する人間は、電子キーに記憶されることによって正当化されていて、特定の人間に識別手段が固有に割り当てていることを確認する。この主要な態様は、法的権限の人間によるこの一度限りの確認を使用して、識別手段の固有、かつ十分に追跡可能な割り当てを特定の人間に設定する。この固有の割り当ては、人間を識別又は認証する後続の手順の間に固有に取り戻すことができる。識別手段をチェックしている第３者は、信頼性が高い一義的な方法でこの識別手段を示す人間を識別及び認証できることになる。具体的には、法的拘束力がある識別及び認証を取得することが可能になる。

【００２５】

具体的には、法的権限者は、認められる確認証、具体的には人間の身元に関連する法的拘束力を有する確認証を発行する権限を有する団体として広く受け入れられる組織にしてもよい。例えば、これは、全国的及び／又は国際的に活動する認証又は証明機関にしてもよい。

【００２６】

識別手段のセキュリティの観点から、人間に関する特徴のデジタル画像がメモリ手段に記憶される１つの実施形態は、具体的な利点を有する。潜在的な加害者が識別手段の支持層を操作して、改ざんされた人間に関する特徴が適用又は付加できるようにする可能性がある。支持層上の人間に関する特徴に加えて、この特徴のデジタル画像が認証デバイスのメモリ手段に記憶される場合、人間の識別に関する後続のアクセスにおいて支持層に現在配置される特徴と比較可能な基準画像が常にある。これにより、いずれの操作の試みが速やかに検出可能になる。この配置は、いわゆるオフラインで人間の認証が可能であるという具体的な利点を有する。チェック及び比較される基準特徴が識別手段において利用可能であり、かつ中央証明又は認証機関に通信リンクを確立する必要がないためである。

【００２７】

適当なアクセス保護システムを認証デバイスに選択することによって、この基準特徴へのアクセスが読み出しのみに基づいて可能であることを保証し、書き込みを含むアクセスは、認証デバイスの特徴及び認証デバイスのセキュリティシステムにより防止されることを保証することをさらに可能にする。また、１つの実施形態において、認証デバイスは、書き込みを含む記憶された特徴へのアクセスにより、記憶される情報及びリンクが破壊され、随意的には識別手段が破壊されるように配置できる。

【００２８】

第１の電子キーがエンコードされたフォーマットでデジタル画像に記憶される場合に、１つの特に実用的な実施形態が取得される。例えば、このエンコードは、ステガノグラフィを使用して実行してもよい。この利点は、記憶された画像を視覚的に観察するときに、エンコードされたキーが見えないように、第１の電子キーがデジタル画像に記憶されることである。また、デジタル画像が操作できないことは、有利である。操作が試みされると、人間に関する特徴と、第１の電子キーとの間のリングを自動的に無効になるためである。具体的には、この実施形態は、この形式のエンコードが通常は可逆的でないという特別な利点を提示する。すなわち、エンコードを除去し、人間に関する特徴を変更し、再びエンコード動作及びリンク動作を再実行して操作することは、不可能である。

【００２９】

１つの実施形態に基づくと、電子データセットは、データ処理ユニットのメモリ手段に記憶される。例えば、記憶された電子データセットを保護するために、データ処理ユニッ

トは、選ばれた数人の人間のみがアクセス可能である保護区域に配置してもよい。また、いくつかの電子データセットをデータ処理ユニットに記憶することが可能である。これによって、数人の人間に関連する電子データセットを管理することができる。

【００３０】

遠隔データセンタが電子データセットにアクセス可能なように構成される通信コネクタをデータ処理ユニットが有する他の実施形態は、利点がある。例えば、データ処理ユニットは、異なる複数の電子データセットを識別手段として記憶し、グローバルな通信ネットワークを介してアクセス可能なサーバの形式で提供されてもよい。複数の識別及び認証機関が識別手段にアクセスし、かつ人間を識別又は認証する処理を実行することができることになるであろう。

【００３１】

使用を簡明にし、かつ本発明が提案する識別手段は好適に実行すべきであることを考慮すると、電子データセットが携帯型データメモリデバイスに記憶される１つの実施形態は、利点がある。上述のように、携帯型データメモリデバイスは、日常生活で使用されるので常に持ち運ぶデバイスとして位置付けられる。

【００３２】

また、本発明の目的は、以下に説明する方法の工程を具備する識別及び認証方法により達成される。

【００３３】

メモリ手段又は電子データセットに人間に関する特徴を記憶することによって、ユーザがいつでも実行可能であり、かつユーザがいつでもアクセスできるので、人間をいつでも識別できる識別手段が取得される。

【００３４】

人間の身元が保護されることを保証するために、人間の身元は、法的権限により正当化される。これは、人間の身元を立証する法的権限者に法的に有効な書類を提示する人間によって行うことができる。

【００３５】

情報特徴のメモリ手段又は電子データセットに法的権限者の第１のキーを記憶し、次いで人間に関する特徴に第１のキーをリンクすることによって、法律的に有効な関係は、物理的な識別手段と、この特徴の運搬者又は所有者の人間との間で確立される。

【００３６】

検査のために識別手段を提示することによって、人間は、法的に認証された身元を有することができる。人間が識別手段を第３者に提示するとき、第３者は、法的権限者の前で法的に割り当てられた人間に、その特定の識別手段が一義的に対応することを、法的拘束力に基づいて具体的に見なすことができる。

【００３７】

識別手段の第１の実施形態に基づくと、識別手段を提示することは、チェックされる人間が持ち運ぶ支持層及び／又はチェックデバイスの支持層が既に証明されていることを意味することができる。電子データセットの形式の第２の実施形態に基づくと、チェックデバイス又はチェックを持ち運ぶ人間は、データセットが記憶されるメモリ位置に照会されて提示されてもよい。ここで、識別手段は、通信手段を介してメモリ位置にアクセスできる。

【００３８】

セキュリティを強化するため、また多段の認証処理を設定するために、認証及び証明機関の第２の電子キーを記憶する実施形態を選択する利点を有する。この実施形態では、人間の識別及び認証に含まれるセキュリティの著しい向上が提示される。識別手段を提示する人間が、第２の電子キーを申請した人間と一致するか否かを確認するために発行認証及び証明機関とともにキーをチェックすることによって、識別手段に提示される第３者がチェックを実行できるためである。通常このような機関は、特に全国的に認識される評価を有し、好適には国際的に認識される評価を有する。このため、人間の識別又は認証を確立

することことによって、法的権限者により記憶された第１の電子キーによって第１に確認され、認証及び証明機関の第２の電子キーによって第２に確認される。これは、人間の信頼性の高い識別を保証する観点から相当の利点を示し、かつ発明が提案する方法が広く受け入れられることになる。

【００３９】

また、この実施形態は、種々のセキュリティ段階を設定する可能性を提示する。例えば、セキュリティの観点では重要ではない、より単純な応用の場合、第２のキーによる認証は、十分であろう。より高いセキュリティが必要な場合、第１のキーもチェックできる。

【００４０】

人間の信頼性のある識別及び認証を保証するとともに、可能な限り迅速に実行するという観点から本発明が提示する方法のセキュリティを著しく向上させるために、人間に関するデータの基準データを外部メモリユニットに記憶する実施形態を選択する利点がある。例えば、この外部メモリユニットは、デバイスに接続される中央データ処理ユニットの形式で提供してもよい。中央データ処理ユニットは、人間に関する特徴及び電子キーとともに識別手段から暗号化生産物を読み出すことができるように接続される。例えば、基準セットは、識別手段に人間に関する特徴の画像を含んでもよい。これにより、正当化処理の間に人間に関する特徴に法的権限者によりリンクされた元の特徴セットにアクセス可能になり、いつでも人間を認証することができる。潜在的な加害者が識別手段を操作する可能性があるが、操作の試みはすぐに露見するので、記憶される基準セットにはアクセスされず、次いで人間の認証が実行される。人間を認証するために、操作が不可能であるか又は著しく困難である基準セットを利用することにより、セキュリティが著しく向上し、かつ第３者のための人間の識別処理の信頼性が著しく向上する。

【００４１】

また、本発明が提示する方法の信頼性及び容認性を向上させる観点から、人間に関するデータの基準セットが識別手段に記憶され、具体的にはメモリ手段に記憶される実施形態は、利点がある。この実施形態は、検出システムが「オフライン」動作する場合、すなわち中央管理機関に直接的なアクセスがない場合に利点を有する。

【００４２】

いくつかの実施形態において、これらの基準セットは、単方向の暗号化などによる適当な暗号化フォーマット又は符号化フォーマットで当然に記憶されてもよい。これにより、潜在的な加害者が打開することがさらに困難なセキュリティが提示される。

【００４３】

１つの実施形態に基づくと、記憶される人間に関する特徴が、検出される特徴と比較されて、人間が識別又は認証される。有利には、この実施形態は、本発明が提案する識別手段が、特徴の検出と、記憶される特徴との比較とに基づいて、人間の信頼性の高い識別及び／又は認証を可能にするのに十分セキュリティ特性を有することを保証する。この比較は、検査官が直接行うことができ、及び／又は自動制御システムにより行うこともできる。このチェックは、識別手段を実行する人間又は基準を提示する人間が第３者に委ねる場合であって、その人間自身を識別又は認証しようとする場合に特に実行されることになる。次いで、検出システムは、人間に関する特徴を検出し、現在検出されるデータを処理機関又は制御者に伝送して、記憶される基準データと比較できる。現在物理的に存在する人間が、法的権限者により識別手段が確認又は発行した人間と一致することにより一致が保証されることになる。

【００４４】

識別手段のセキュリティの特に実効的な向上は、検出時に人間に関する特徴が第１の電子キーに速やかにリンクする実施形態により取得される。これにより、人間に関する特徴は、検出と、記憶と、リンクとの間で操作できないことが一義的に保証される。

【００４５】

セキュリティの特に実効的な向上は、法的権限者の前で、又は法的権限者により、人間に関する特徴がリアルタイムに検出される場合、電子キーに記憶及びリンクする人間に関

する特徴の検出に応じて取得できる。これによって、検出される人間に関する特徴の認証が一義的に確認される。人間に関する特徴は、識別手段の主要な特徴であるので、この実施形態は、セキュリティの特に実効的な向上を示す。検出される特徴が監視下で検出され、記憶され、かつ操作の可能性がなくキーにリンクされるためである。

【００４６】

より明確な理解を提供するために、本発明は、添付図面を参照してより詳細に以下に説明されることになる。

【００４７】

図面は、非常に概略的であり、簡明化される。

【図面の簡単な説明】

【００４８】

【図１】本発明が提案する識別手段の実施形態を示す図である。

【図２】人間を固有に識別及び認証する識別手段を作り出すために使用される方法の工程を示す図である。

【図３】人間の身元をチェックすることにより、アクセスを保証するために使用されるデバイスを示す図である。

【図４】身元の特徴を認証するデバイスを示す図である。

【発明を実施するための形態】

【００４９】

まず、異なる実施形態に記載される同一部は、同一の符号及び同一の素子名が付され、説明による開示において、同一部を意味するという観点から、同一の符号又は同一の素子名は交換できる。さらにまた、特に記載される図面に関して、上部、下部、及び側部など、記載されるために選択される位置は、他の位置に記載されているときは新しい位置を意味するという観点から、交換できる。図示及び説明される種々の実施形態のそれぞれの特徴又は特徴の組み合わせは、それ自体の権利において、本発明が提案する発明の単数又は複数の独立する解決手段として理解できる。

【００５０】

説明における値の範囲に関する数量は、いずれの部分の範囲を含み、かつ全ての部分の範囲を含むことを意味するとして理解すべきである。この場合、例えば１～１０の範囲は、下限である１から始まり上限である１０までの全ての部分の範囲を含むものとして理解すべきである。すなわち、１～１．７、３．２～８．１、又は５．５～１０などの下限の１以上から始まり上限の１０以下で終了する全ての部分の範囲である。

【００５１】

図１は、本発明が提案する識別手段１の１つの実施形態を示し、支持層２と、具体的には人間の画像である人間に関する特徴３とともに、第１の電子キー６が記憶されるメモリ手段５を有する認証デバイス４を具備する。さらに、識別手段１は、通信コネクタ８を有する通信システム７を有する。また、人間に関する他の特徴、すなわち組織化された特徴９は、識別手段１に配置され及び／又は組み込まれてもよい。

【００５２】

特に支持層において、識別手段１は、好適には身分証明書として配置され、この識別手段を持ち運ぶ人に領域へのアクセス、すなわち入場許可を与えるか、又は一般にアクセスできない情報を与える。本発明が提案する識別手段は、恒久的に持ち運ばなければならない方式にできるので、好適には、バンクカードの形式に配置できる。このため、支持層は、移動の自由を制限せず、また人間の移動により識別手段が構造的な損傷を受ける危険を冒さない。具体的には、バンクカードに基づくフォーマットは、いずれにせよ人間が常に持ち運ぶＩＤカードケース又は財布の中に識別手段を置くことができるという利点を有する。チップカードに基づく配置は、広く使用されるので、非常に低いコストで利用可能であるという他の具体的な利点を提示する。具体的には、本発明が提示する識別及び認証方法を実行する手段として特に実用的である構成素子又はモジュールを組み込むことにより、識別又は認証をチェックする検出デバイスにより提供される必要がない。

【００５３】
公知の識別手段の場合、具体的には識別手段が割り当てている人間の画像である人間に関する特徴３及び９が、不正な意図により操作される可能性がある。これは、識別手段を使用して虚偽の身元を作り出すことが可能であることを意味する。特に多くの人々が通過する領域において、人間に関する特徴を視覚的にチェックしなければならない検査官が誤る可能性がある。これは、加害者が神経質な領域に特定の環境の下で侵入する可能性があることを意味する。本発明が提案する識別手段の明確な利点は、第１の電子キー６が人間に関する特徴３にリンクし、随意的には他の特徴９にリンクすることである。好適には、人間に関する特徴３は、人間の画像の形式で提供される。識別手段に提示される人間と視覚的に比較することに加えて、記憶された画像と比較できるという利点がある。電子キー６は、人間に関する特徴３の電子的表示を作り出すことなどによって、人間に関する特徴３にリンクされる。例えば、電子キー６とともに暗号化されて、メモリ手段５に記憶される。しかしながら、好適な実施形態において、人間の画像３のデジタル表示は、メモリ手段に記憶され、第１の電子キーがデジタル画像に隠れるように、デジタル画像は、ステガノグラフィーにより第１に電子キー６にリンクされる。しかしながら、チェックサムを画像から決定することも可能であろう。例えば、チェックサムは、第１のキーとともに暗号化され、デジタル画像に隠される。これらは、人間に関する特徴に電子キーをリンクさせる実施形態の単なる例示である。当業者は、好適には操作の試みを非常に難しくする電子的に処理できるフォーマットである人間に関する特徴に電子キーをリンクする他の可能な方法を熟知しているであろう。具体的には、本発明が提案するように人間に関する特徴３に第１の電子キー６をリンクすることにより、人間に関する特徴３を操作する試みがされた場合、電子キー６へのリンクが無効になり、操作の試みを一義的に検出できるという利点を有する。

【００５４】
識別手段１と、検出システムとの間にデータ通信リンクを確立させるために、識別手段は、通信コネクタ８を備える通信手段７を有する。規格ＩＳＯ／ＩＥＣ７８１０などに従うバンク型のスマートカードである好適な実施形態に基づくと、支持層２上の通信コネクタ８の配置は、支持層の配置自体と同様に固定される。通信コネクタ８は、必要な接点の配置又は無線配置に基づくので、認証処理は、検出システムに挿入しなければならない識別手段なしに実行可能にすることができる。例えば、規格ＩＳＯ／ＩＥＣ１４４４３は、接点なしに読み出し可能なチップカードの配置を規定する。

【００５５】
認証デバイス４は、人間に関する特徴３と、第１の電子キー６との間のリンクの特性を通信システム７を介して検出システムに利用可能なように配置してもよい。しかしながら、認証デバイスが、検出されたばかりの人間に関する特徴と、記憶される人間に関する特徴とを比較して、一致点が見つけられなかったとのメッセージを検出システムに伝送することも可能であろう。この実施形態において、リンク又はキーの特徴は、識別手段から外部に伝送されない。

【００５６】
記憶される電子キーと、随意的に記憶されてもよい人間に関する特徴の画像とを保証する手段として、１つの実施形態の認証デバイス４は、データ処理ユニット、すなわち暗号化モジュール１０を有する。認証デバイス４は、記憶される特徴又は電子キーにアクセスする加害者がアクセスによりいずれの利益も得ないように、記憶される特徴又は電子キーが保証されるように構成できる。これは、暗号化モジュールで実行される単方向の暗号化などに基づいて達成される。セキュリティロックを有するので、元の特徴に遡ることは不可能である。しかしながら、認証デバイスは、複雑なタスクを取り扱うこともできる。例えば、人間に関する特徴を検出することを随意的には含む多段特徴チェックを取り扱うことができ、認証処理デバイスがデータ処理ユニットを有する場合、このようなデバイスは、複雑な処理工程を実行する能力を通常有するので有利である。これに関して、上述のように、チップカード又はスマートカードに基づく配置は、データ処理ユニットが通常カー

ドに組み込まれているという利点を提示する。
【００５７】
さらなるセキュリティ特性を提供するために、第２の電子キー１１は、認証デバイス４のメモリ手段５に配置できる。第１及び／又は第２の電子キーの主要な態様は、認証又は証明機関により発行又は供給され、この証明又は認証機関は、生成される電子キーの信頼性に関して高い国際規格に従うことである。具体的には、これらの機関は、電子キーを生成するために使用されるユーザデータの創出及び管理を統制する特定の要求を満足する。
【００５８】
図２は、本発明が提案する識別手段であって、人間を一義的に識別及び認証可能な識別手段を作り出す方法の動作を概略的に示す図である。第１のステップ１２において、個人設定されていない識別手段１３を、人間に関する特徴３及び９によって個人設定する。すなわち、特徴３及び９は、識別手段１３に適用又は記憶される。第２のステップ１４において、ユーザ１５は、法的に有効な書類１７とともに個人設定された識別手段を持ち込んで、人間１５の身元を権限者１８に確立する。好適には、権限者１８は、弁護士又は公証人などの法的権限者である。権限者１８は、提示される書類によって人間１５の身元をチェックする。次いで、個人設定された識別手段１６、具体的にはメモリ手段に適当な第１の電子キー６を記憶することによって、正当化する。本発明が提案する方法の本質的な工程は、認証する権限者１８が識別手段１６に記憶される第１の電子キー６を人間に関する特徴３及び９にリンクさせることにより、不可逆的な接続１９を確立することである。
【００５９】
識別手段を個人設定すること１２又は識別手段に認証を与えること１４に使用される方法の工程では、識別手段は、図示されないアクセス制御又は制御システムに配置される必要がある。制御システムは、通信システムに結合して、通信が可能なデータ処理ユニットにしてもよい。これにより、通信コネクタ８を介して認証デバイス４にデータ接続が確立する。本発明が提案するこの方法の主要な技術的な効果は、人間に関する特徴３を第１の電子キー９にリンクすること１９によって、識別手段の操作がこのリンクによってほぼ防止され、人間の識別及び認証を一義的にでき、法的に確立できることである。
【００６０】
また、識別手段１３の個人設定１２は、第２の電子キー１１が認証デバイス４のメモリ手段５に記憶される工程を含んでもよい。好適には、第１の電子キー６及び随意的には第２の電子キー１１は、外部の証明及び認証機関２０及び２１により供給及び管理される。上述のように、この機関は、セキュリティに関して高い程度の許容性を享受し、電子キーを生成及び管理することに適用される。このような機関の例として、ＲＳＡ又はベリサイン（登録商標）がある。これらの機関は、登録されたユーザに固有に割り当てられる電子キーセットを管理する。好適には、これに関して、秘密鍵と、公開鍵とからなるいわゆる公開鍵システムに従って使用される。公開鍵システムは当業者に既知なので、ここでは、より詳細な説明は与えられないことになる。具体的は、このようなキーシステムの利点は、第３者が独立な証明及び認証デバイス２０及び２１から電子キーの信頼性を確立できることである。
【００６１】
図３は、本発明が提案する方法の応用であって、本発明が提案する識別手段１によって、人間１５の固有な識別及び認証を提供するために使用される方法の応用を説明する図である。例えば、一般にアクセスできない機関へのアクセスは、アクセス制御手段２２によって保証できる。アクセス制御システム２２を解放するために、人間１５を固有に識別及び認証する必要がある。このため、人間１５は、識別手段１を評価する検出システムに識別手段１を提示する。例えば、識別手段１は、読み出しデバイス２４に配置され、通信接続が通信コネクタ８を介して認証デバイスに確立する。検出システム２３は、人間の自動識別及び認証を実行するように構成できる。例えば、好適には光学的な画像検出システムである検出手段２５が人間の画像を検出することによって実行し、評価及び比較モジュール２６によって、識別手段１に記憶される人間に関する特徴と比較される。好適には、人

間に関する特徴３は、具体的にはＩＣＡＯである国際的に認められた規格に従う画像である。評価及び比較モジュール２６は、現在検出される画像と、記憶される人間に関する特徴との比較を完全な自動化に基づいて実行できる。識別手段１が調整されていないことを保証するために、検出システム２３は、外部の証明及び認証機関２１によって、第１の電子キー６の有効性及び信頼性をチェックすることができる。同様に、第２の電子キー１１は、他の証明及び認証機関２０によってチェックされる。

【００６２】

しかしながら、第１の実施形態において、識別手段１に記憶される人間に関する特徴が検出システム２３に読み出せないことが可能である。現在検出される人間の画像が検出システム２３の暗号化モジュール２７などによって作り出され、かつ処理され、識別手段１に伝送される。次いで、識別手段１の認証デバイスは、検出され新たに作り出された人間の画像が、記憶される人間に関する特徴３に一致するか否かを解明するためにチェックされる。そして、これに基づいて、認証信号を生成し、検出システム２３に伝送し返して、次いでアクセス制御システム２２を解放する。

【００６３】

図４は、本発明が提案する識別手段１を作り出すデバイスを示す図である。具体的には、人間に関する特徴を第１の電子キーにリンクして、識別手段に記憶する手段として作り出すデバイスである。識別手段に個人設定し、かつ正当化するために必要な処理工程は、データ処理ユニット２８によって実行される。この形式のシステムは広く利用可能であり、具体的には、電子的なデジタルデータユニットにより処理される機関が提案されるためである。具体的には、このようなシステムは、画像検出ユニット３０により検出される人間１５の画像をさらに処理できるフォーマット３１に変換する画像処理モジュール２９を有する。カメラなどの画像検出ユニット３０は、通信コネクタを介してデータ処理ユニット２８に接続される。好適には、画像は、具体的にはＩＣＡＯである自動画像検出のための認められた規格に従わなければならない。このため、画像処理モジュール２９は、画像検出ユニット３０を制御して、画像に必要な規格を取得できる。好適には、画像処理モジュールは、検出した画像データを規格化された画像フォーマットに変換する。これにより、種々の数多くのデータ処理システムによる処理が可能になる。

【００６４】

本発明が提案する識別手段及び方法の本質的な態様は、改ざんを防止するセキュリティに関して高い規格を満足する電子キーが、具体的には画像である人間に関する特徴にリンクすることである。リンクを作り出すことができる方法のいくつかの例が以下に説明されるが、データシステムにより処理できるフォーマットに基づいて人間に関する特徴に電子キーをリンクする方法についての情報に関連する技術文献が参照される。例えば、第１の電子キー６は、ステガノグラフィによってデジタル画像データに配置できる。この利点は、人間に関する特徴を人間が観察するときに、知覚可能な障害がなく、第１の電子キーは全ての画像データに亘って適用されることである。しかしながら、他のオプションは、ハッシュ値などの作り出された画像からの参照値を決定することになる。暗号化モジュール３２を介して第１の電子キーとともに参照値が実行されて、暗号化の結果が取得される。この暗号化の結果は、元の画像データ及び電子キーに遡ることが不可能なように、設定してもよい。識別手段が権限者により認証されていると、人間に関する特徴は、再びクエリーする必要はなく、続いて人間を識別及び認証するとき、人間の画像は、第３者により検出され、暗号化の結果を取得するように同一の暗号の暗号方法により処理されることは、このアプローチの利点である。次いで、この結果は、識別手段に記憶される暗号化の結果と比較されて人間の身元を認証できる。また、識別手段１の認証デバイス４及び認証デバイスのメモリ手段は、第１の電子キーの所有者である権限者が、記憶される人間に関する特徴を処理又は変更するためにアクセス可能なように構成されてもよい。１つの有利な実施形態に基づくと、第１の電子キー６は、証明及び認証機関が実行及び／又は管理するキーシステムの一部にしてもよい。この証明及び認証機関は、データ処理ユニット２８の一部にしてもよく、ローカルに接続されてもよい。しかしながら、インタネットなどの公衆

通信媒体を介してデータ処理ユニット２８により通信リンクが確立できる遠隔の証明及び認証機関２１を選択することも可能であろう。例えば、いわゆる公開鍵システムは、認識手段が認証する処理の間に権限者によって、画像が秘密鍵にリンクされ、識別手段に記憶されるような事例に使用できる。潜在的な加害者は、権限者の秘密鍵を決して知ることができないので、第１の電子キーへのリンクが無効になるため人間に関する特徴を操作することは不可能である。第３者は、暗号化された人間に関する画像が証明及び認証機関に提示されることにより、識別手段に提示される人間の識別及び認証を確立できる。これにより、識別手段に記憶される人間に関する特徴の認証を完全な自動化に基づいて確認できる。物理的に存在する人間の特性を識別手段に記憶される基準特徴に対してチェックすることにより、物理的に存在する人間の身元の一義的な認証が可能になる。

【００６５】

記憶される基準特徴にアクセスし、参照特徴を記憶し第１の電子キーへのリンクを可能にするために、識別手段１は、アクセスユニット３４に配置される。アクセスユニット３４は、具体的には接続コネクタ８である通信システムを介して、データ処理ユニット２６と、識別手段１の認証デバイス４との間のデータ接続を確立する。

【００６６】

本発明が提示する識別手段は、割り当てられる人間自身が他の特徴を認証する他の実施形態に基づくこともできる。このため、人間又は画像は、データ処理ユニットの画像検出ユニットにより検出し、記憶される特徴との比較に基づいて自分自身の身元を認証することができる。これに関して、識別手段が支持層を使用する配置に基づくか、又は電子キーセットに基づくかは重要ではない。認証が成功裡に終了すると、人間は他の識別手段などを作り出すことができる。一般に広く使用される形式のデータ処理ユニットは、本実施形態に基づく方法の工程を実行するために必要な全ての構成素子を有する。

【００６７】

例示として説明される実施形態は、人間を認証及び識別する手段及び方法の可能な変形を提示する。この段階で、本発明は、具体的に説明される変形に特に限定されず、変形それぞれは、互いに異なる組み合わせで使用でき、これら可能な変形は、開示される技術的教示を受ける当業者が理解可能な範囲内にあることを指摘すべきである。したがって、説明及び図示される変形の詳細それぞれを組み合わせることにより取得できる想像可能なすべての変形は、本発明の範囲で可能であり、かつ本発明の範囲に含まれる。

【００６８】

最後に、良好な順序のために、識別手段の構造及び方法のより明確な理解を提供するために、これらの構成部は、スケール及び／又は拡張スケール及び／又は縮小スケールにおいてある程度の広がりで図示されることを指摘すべきである。

【００６９】

発明の独立の解決手段が内在する対象を本明細書に見つけることができる。

【００７０】

何よりも、図１～４に示す対象の実施形態それぞれは、それ自体の権利において、本発明が提案する発明の独立の解決手段を構成する。本発明が提案する目的及び関連する解決手段は、本明細書の詳細な説明で見つけることができる。

【符号の説明】

【００７１】

１　識別手段
２　支持層
３　人間に関する特徴
４　認証デバイス
５　メモリ手段
６　第１の電子キー
７　通信システム
８　通信コネクタ

９　人間の特定又は組織化された特徴
１０　データ処理ユニット、暗号化モジュール
１１　第２の電子キー
１２　識別手段の個人設定
１３　個人設定されていない識別手段
１４　識別手段の認証
１５　人間
１６　個人設定された識別手段
１７　書類
１８　認証権限者
１９　リンク
２０　証明機関、認証機関
２１　証明機関、認証機関
２２　アクセス制御システム
２３　検出システム
２４　読み出しデバイス
２５　検出手段
２６　評価及び比較モジュール
２７　暗号化モジュール
２８　データ処理ユニット
２９　画像処理モジュール
３０　画像検出ユニット
３１　処理画像データ、デジタル画像
３２　暗号化モジュール
３３　ローカルの証明機関、認証機関
３４　アクセスユニット

【図１】

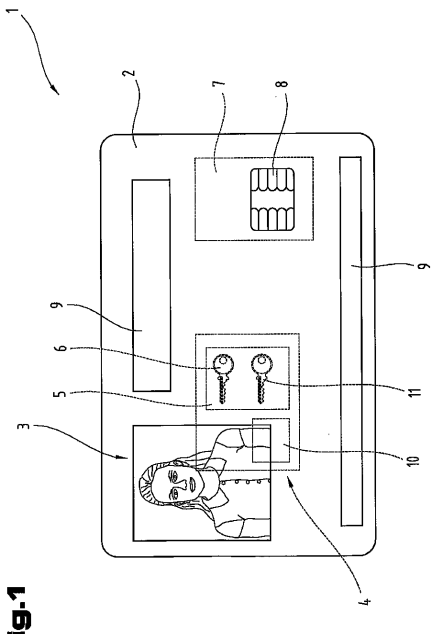

Fig.1

【図２】

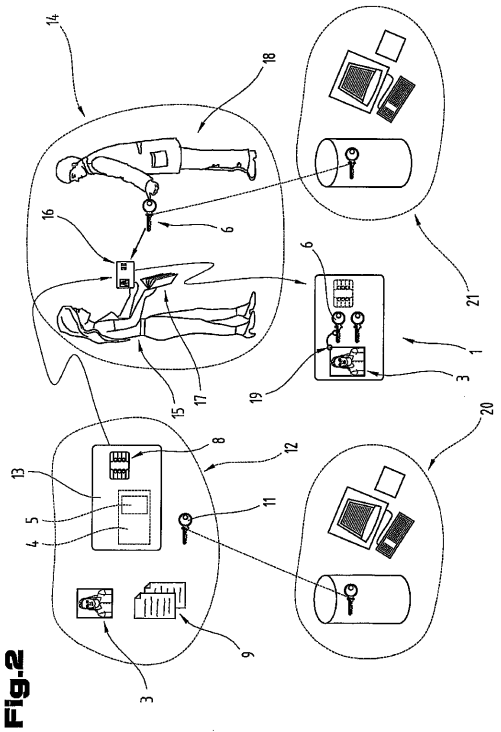

Fig.2

【図３】

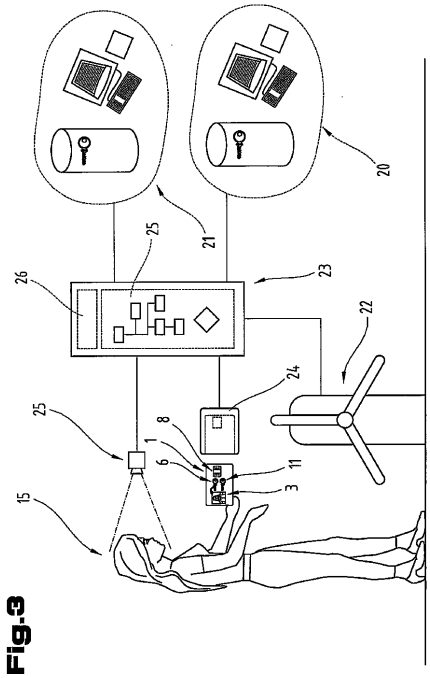

Fig.3

【図４】

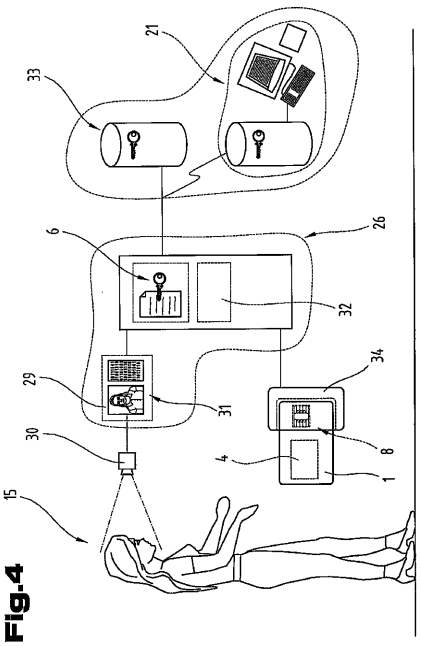

Fig.4

フロントページの続き

(74)代理人 100151459
弁理士 中村 健一
(74)代理人 100190632
弁理士 山▲崎▼ 誠也
(72)発明者 シュレーター, クラウス
ドイツ連邦共和国, １０７０７ ベルリン, ポメルシェ シュトラーセ １１
(72)発明者 チャン, ホー ビー.
スイス国, ツェーハー－６０４８ ホル, アウフ オーベルリュティ １３

審査官 和田 財太

(56)参考文献 国際公開第２００８／０００７６４（WO, Ａ１）
佐原 道子, ＩＣカードビジネス・イヤーブック２００６, ＣａｒｄＷａｖｅ, 日本, （株）シーメディア, ２００６年 2月２０日, Ｖｏｌ．１９, Ｎｏ．３, ｐ．５２－ｐ．５５

(58)調査した分野(Int.Cl., ＤＢ名)
Ｇ０６Ｋ １９／００－１９／１０