

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第4223243号

(P4223243)

(45) 発行日 平成21年2月12日(2009.2.12)

(24) 登録日 平成20年11月28日(2008.11.28)

(51) Int.Cl.

F I

E O 5 B 49/00 (2006.01)

E O 5 B 49/00 R

G O 7 C 9/02 (2006.01)

G O 7 C 9/02

請求項の数 6 (全 13 頁)

(21) 出願番号	特願2002-228920 (P2002-228920)	(73) 特許権者	000006013
(22) 出願日	平成14年8月6日(2002.8.6)		三菱電機株式会社
(65) 公開番号	特開2004-68411 (P2004-68411A)		東京都千代田区丸の内二丁目7番3号
(43) 公開日	平成16年3月4日(2004.3.4)	(74) 代理人	100110423
審査請求日	平成17年7月22日(2005.7.22)		弁理士 曾我 道治
		(74) 代理人	100071629
			弁理士 池谷 豊
		(74) 代理人	100084010
			弁理士 古川 秀利
		(74) 代理人	100094695
			弁理士 鈴木 憲七
		(74) 代理人	100111648
			弁理士 梶並 順
		(74) 代理人	100109287
			弁理士 白石 泰三

最終頁に続く

(54) 【発明の名称】 出入管理装置

(57) 【特許請求の範囲】

【請求項1】

個人の身体上の特徴を抽出する個人識別装置及び電気錠が接続され、通行可否設定テーブルを参照し個人の特徴情報に対応する個人番号に基づいて通行の可否を判断して前記電気錠を施解錠する個人識別コントローラと、

前記個人識別装置により抽出した個人の特徴情報の認証を行い特定した個人番号を返信する複数のバイオメトリクス認証サーバーと、

前記個人識別コントローラ、及び前記複数のバイオメトリクス認証サーバーを相互に接続するネットワークと

を備え、

前記個人識別コントローラは、前記個人識別装置により抽出した個人の特徴情報を、前記複数のバイオメトリクス認証サーバーへ送信し、前記複数のバイオメトリクス認証サーバーのうち所定数から認証結果が返信された場合には、前記通行の可否を判断する

ことを特徴とする出入管理装置。

【請求項2】

個人の身体上の特徴を抽出する個人識別装置及び電気錠が接続され、通行可否設定テーブルを参照し個人の特徴情報に対応する個人番号に基づいて通行の可否を判断して前記電気錠を施解錠する個人識別コントローラと、

個人番号をキーとして登録済みの個人の特徴情報と前記個人識別装置により抽出した個人の特徴情報の照合認証を行い、一致するかどうかを判断し、認証結果を返信する複数の

バイオメトリクス認証サーバーと、

前記個人識別コントローラ、及び前記複数のバイオメトリクス認証サーバーを相互に接続するネットワークと

を備え、

前記個人識別コントローラは、入力した個人番号及び前記個人識別装置により抽出した個人の特徴情報を、前記複数のバイオメトリクス認証サーバーへ送信し、前記複数のバイオメトリクス認証サーバーのうち所定数から認証結果が返信された場合には、前記通行の可否を判断する

ことを特徴とする出入管理装置。

【請求項 3】

10

前記個人識別コントローラは、個人識別装置毎に、前記個人の特徴情報を送信すべきバイオメトリクス認証サーバーを記述したサーバーテーブルを有する

ことを特徴とする請求項 1 又は 2 記載の出入管理装置。

【請求項 4】

前記個人識別コントローラは、前記所定数の認証結果のいずれか 1 つに基づいて、あるいは前記所定数の認証結果が全て一致している場合に一致した認証結果に基づいて、前記通行の可否を判断する

ことを特徴とする請求項 1 又は 2 記載の出入管理装置。

【請求項 5】

前記個人識別コントローラは、前記複数のバイオメトリクス認証サーバーの一部がダウンした場合には、前記所定数を変更する

20

ことを特徴とする請求項 1 又は 2 記載の出入管理装置。

【請求項 6】

前記個人識別コントローラは、前記複数のバイオメトリクス認証サーバーの一部がダウンした場合には、前記所定数の認証結果のいずれか 1 つに基づいて、前記通行の可否を判断する

ことを特徴とする請求項 1 又は 2 記載の出入管理装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

30

この発明は、人や物の出入りを管理する出入管理装置に関するものである。

【0002】

【従来の技術】

近年、ビルや建物の扉にカード読取り装置や電気錠を備え、カードの ID 番号により人や物の通行を許可したり、禁止したりする出入管理装置やアクセスコントロール装置が普及してきている。

【0003】

また、人の身体上の特徴（例えば、指紋、顔、虹彩、掌形、声紋など）をとらえ、個人を特定するバイオメトリクスの技術が発展し、カードの代りにバイオメトリクスにより通行を管理する出入管理装置やアクセスコントロール装置も実用化されている。

40

【0004】

従来の出入管理装置について図面を参照しながら説明する。図 7 は、従来の出入管理装置の構成を示す図である。この図 7 は、バイオメトリクス認証を利用した一般的な出入管理システムである。

【0005】

図 7 において、1（1 A、1 B）は個人識別コントローラ、2（2 A、2 B）は個人識別装置、3（3 A、3 B）は電気錠、4 はデータ設定端末、5 はバイオメトリクス認証サーバー、6 はイーサネット（登録商標）などの汎用ネットワークである。なお、1 台の個人識別コントローラ 1 には、複数台の個人識別装置 2 が接続される。

【0006】

50

イーサネット（登録商標）などの汎用ネットワーク 6 に接続された複数台の個人識別コントローラ 1 には、1 台毎に人の身体上の特徴を抽出する個人識別装置 2 と電気錠 3 が接続されており、個人識別コントローラ 1 は、認証された個人がその扉を通行可能かどうか判定し、電気錠 3 の解錠、施錠により通行の管理を行う。

【0007】

一般に、出入管理を行う個人識別コントローラ 1 は、設定スペースや取扱いの簡便さよりマイコン制御のコントローラが利用される。この個人識別コントローラ 1 は、その扉の通行を可能とする個人のデータを備えており、そのデータは汎用ネットワーク 6 に接続されているデータ設定端末 4 により設定される。カードを利用したシステムやバイオメトリクス認証が個人識別コントローラ 1 内で認証処理できるようなシステムの場合は、この構成でシステムを実現できる。

10

【0008】

しかし、バイオメトリクス認証が高度な機能であったり、認証する人数が多い場合には、個人識別コントローラ 1 内では認証処理が納まらず、汎用ネットワーク 6 上に別途専用のバイオメトリクス認証サーバー 5 を設置する必要がある。

【0009】

つぎに、従来の出入管理装置の動作について図面を参照しながら説明する。図 8 は、従来の出入管理装置の動作を示すフローチャートである。

【0010】

図 8 は、バイオメトリクス認証サーバー 5 を設置した場合の個人識別コントローラ 1 の処理動作を示すフローチャートである。

20

【0011】

まず、ステップ 901 において、個人識別コントローラ 1 は、個人識別装置 2 により個人の特徴情報を抽出する。

【0012】

次に、ステップ 902 において、個人識別装置 2 により抽出した個人の特徴情報を、汎用ネットワーク 6 を通じてバイオメトリクス認証サーバー 5 へ送信する。個人の特徴情報を受信したバイオメトリクス認証サーバー 5 は、認証を行い特定した個人番号を返信する。

【0013】

次に、ステップ 903 において、個人識別コントローラ 1 は、バイオメトリクス認証サーバー 5 からの応答を待つ。応答が有る場合には、次のステップ 904 へ進む。

30

【0014】

次に、ステップ 904 において、バイオメトリクス認証サーバー 5 から返信された個人番号に基づいて、図 2 に示す通行可否設定テーブルを参照し、該当の扉を解錠してよいか判断する。通行可の場合には、つまり通行可否設定テーブルにおいて該当個人番号の該当扉番号が○印の場合には、次のステップ 905 へ進む。一方、通行不可の場合は、つまり通行可否設定テーブルにおいて該当個人番号の該当扉番号が×印の場合は、ステップ 908 へ進む。

【0015】

次に、ステップ 905 において、通行可の場合には、個人識別コントローラ 1 は、電気錠 3 を解錠し、個人識別装置 2 に通行可能であることを表示する。

40

【0016】

次に、ステップ 906 において、個人識別コントローラ 1 は、該当の扉の開閉による通行を待ち、通行が完了したら、次のステップ 907 へ進む。

【0017】

そして、ステップ 907 において、個人識別コントローラ 1 は、通行が完了した場合には、電気錠 3 を施錠して処理を終了し、次の操作を待つ。

【0018】

ステップ 908 において、個人識別コントローラ 1 は、ステップ 904 で通行不可と判断された場合は、通行できないことを個人識別装置 2 に表示し、処理を完了する。

50

【0019】

【発明が解決しようとする課題】

上述したような従来の出入管理装置では、扉の数が多く個人識別コントローラ1の数が多い場合には、バイオメトリクス認証サーバー5に処理が集中し、応答が遅くなるという問題点があった。

【0020】

また、バイオメトリクス認証サーバー5がダウンすると、システム全体がダウンしてしまうという問題点があった。

【0021】

さらに、バイオメトリクスはどの方式もまだ完全ではなく、認証アルゴリズムにより認証の精度の違いや、特定の条件の個人に対して認証しづらいなどの弱点があるという問題点があった。

10

【0022】

この発明は、前述した問題点を解決するためになされたもので、複数のバイオメトリクス認証サーバーを設置し、各個人識別コントローラから、適切な複数のバイオメトリクス認証サーバーに認証要求を送信し、返信された結果により通行可否の判断ができるようにしたものである。これにより、個人識別コントローラの論理とバイオメトリクス認証サーバーの組合せにより、応答を早くすることができ、認証の精度を向上することができる出入管理装置を得ることを目的とする。

20

【0023】

また、一部のバイオメトリクス認証サーバーがダウンした場合には、個人識別コントローラの論理やバイオメトリクス認証サーバーの組合せを変更することで、システム全体がダウンに至らないようにすることができる出入管理装置を得ることを目的とする。

【0024】

【課題を解決するための手段】

この発明の請求項1に係る出入管理装置は、個人の身体上の特徴を抽出する個人識別装置及び電気錠が接続され、通行可否設定テーブルを参照し個人の特徴情報に対応する個人番号に基づいて通行の可否を判断して前記電気錠を施解錠する個人識別コントローラと、前記個人識別装置により抽出した個人の特徴情報の認証を行い特定した個人番号を返信する複数のバイオメトリクス認証サーバーと、前記個人識別コントローラ、及び前記複数のバイオメトリクス認証サーバーを相互に接続するネットワークとを備え、前記個人識別コントローラは、前記個人識別装置により抽出した個人の特徴情報を、前記複数のバイオメトリクス認証サーバーへ送信し、前記複数のバイオメトリクス認証サーバーのうち所定数から認証結果が返信された場合には、前記通行の可否を判断するものである。

30

【0025】

この発明の請求項2に係る出入管理装置は、個人の身体上の特徴を抽出する個人識別装置及び電気錠が接続され、通行可否設定テーブルを参照し個人の特徴情報に対応する個人番号に基づいて通行の可否を判断して前記電気錠を施解錠する個人識別コントローラと、個人番号をキーとして登録済みの個人の特徴情報と前記個人識別装置により抽出した個人の特徴情報の照合認証を行い、一致するかどうかを判断し、認証結果を返信する複数のバイオメトリクス認証サーバーと、前記個人識別コントローラ、及び前記複数のバイオメトリクス認証サーバーを相互に接続するネットワークとを備え、前記個人識別コントローラは、入力した個人番号及び前記個人識別装置により抽出した個人の特徴情報を、前記複数のバイオメトリクス認証サーバーへ送信し、前記複数のバイオメトリクス認証サーバーのうち所定数から認証結果が返信された場合には、前記通行の可否を判断するものである。

40

【0026】

この発明の請求項3に係る出入管理装置は、前記個人識別コントローラが、個人識別装置毎に、前記個人の特徴情報を送信すべきバイオメトリクス認証サーバーを記述したサーバーテーブルを有するものである。

【0027】

50

この発明の請求項 4 に係る出入管理装置は、前記個人識別コントローラが、前記所定数の認証結果のいずれか 1 つに基づいて、あるいは前記所定数の認証結果が全て一致している場合に一致した認証結果に基づいて、前記通行の可否を判断するものである。

【0028】

この発明の請求項 5 に係る出入管理装置は、前記個人識別コントローラが、前記複数のバイオメトリクス認証サーバーの一部がダウンした場合には、前記所定数を変更するものである。

【0029】

この発明の請求項 6 に係る出入管理装置は、前記個人識別コントローラが、前記複数のバイオメトリクス認証サーバーの一部がダウンした場合には、前記所定数の認証結果のい 10 ずれか 1 つに基づいて、前記通行の可否を判断するものである。

【0030】

【発明の実施の形態】

実施の形態 1.

この発明の実施の形態 1 に係る出入管理装置について図面を参照しながら説明する。図 1 は、この発明の実施の形態 1 に係る出入管理装置の構成を示す図である。なお、各図中、同一符号は同一又は相当部分を示す。

【0031】

図 1 において、1 (1 A、1 B) は個人識別コントローラ、2 (2 A、2 B) は個人識別装置、3 (3 A、3 B) は電気錠、4 はデータ設定端末、5 A はバイオメトリクス認証サ 20 ーバー、5 B はバイオメトリクス認証サーバー、6 はイーサネット (登録商標) などの汎用ネットワークである。なお、1 台の個人識別コントローラ 1 には、複数台の個人識別装置 2 が接続される。

【0032】

イーサネット (登録商標) などの汎用ネットワーク 6 に接続された複数台の個人識別コントローラ 1 には、人の身体上の特徴を抽出する個人識別装置 2 と、電気錠 3 が接続されており、認証された個人がその扉を通行可能かどうか判定し、電気錠 3 の解錠、施錠により通行の管理を行う。

【0033】

この個人識別コントローラ 1 は、その扉の通行を可能とする個人のデータ (例えば、通行可否設定テーブル) を備えており、そのデータは汎用ネットワーク 6 に接続されているデ 30 ータ設定端末 4 により設定される。

【0034】

バイオメトリクス認証のためのバイオメトリクス認証サーバー 5 は、システムの規模、登録される人数、バイオメトリクスの種類などにより適切な台数だけ設置される。なお、バイオメトリクス認証サーバー 5 は、同一のハードウェアにプログラムとして複数実行される場合もある。

【0035】

一つのシステムで複数の手法のバイオメトリクスを利用する場合も、同様に、それぞれの個人識別装置 2 に対応したバイオメトリクス認証サーバー 5 を設定すればよい。また、同じ 40 バイオメトリクス手法であっても、アルゴリズムやチューニングが異なるバイオメトリクス認証サーバー 5 を設置して相互補完することもできる。

【0036】

つぎに、この実施の形態 1 に係る出入管理装置の動作について図面を参照しながら説明する。

【0037】

図 2 は、この発明の実施の形態 1 に係る出入管理装置の通行可否設定テーブルの構成を示す図である。また、図 3 は、この発明の実施の形態 1 に係る出入管理装置のサーバーテ 50 ーブルの構成を示す図である。

【0038】

図４～図６は、この発明の実施の形態１に係る出入管理装置の動作を示すフローチャートである。

【００３９】

図４と図５は、複数台のバイオメトリクス認証サーバー５を設置した場合の個人識別コントローラ１の処理動作を示すフローチャートである。図４は、バイオメトリクス技術だけで個人を識別する場合の処理動作を示すフローチャートであり、図５は、テンキーやカードにより個人を特定した後、その個人と身体上の特徴が一致しているかを判断する場合の処理動作を示すフローチャートである。

【００４０】

図６は、一部のバイオメトリクス認証サーバーがダウンした場合の処理動作を示すフローチャートである。

10

【００４１】

最初に、ステップ１０１において、個人識別コントローラ１は、個人識別装置２により個人の特徴情報を抽出する。

【００４２】

次に、ステップ１０２において、個人識別装置２により抽出した個人の特徴情報を、個人識別装置２毎に、図３のサーバーテーブルで指定されたそれぞれのバイオメトリクス認証サーバー５へ汎用ネットワーク６を通じて送信する。例えば、個人識別装置２が指紋照合装置Ａである場合には、図３に示すように、サーバー１（バイオメトリクス認証サーバー５Ａ）及び２（バイオメトリクス認証サーバー５Ｂ）へ個人の特徴情報を送信する。

20

【００４３】

データの送信を早くするため、複数の相手に同時に送信できるマルチキャストや同報通信を使用することができる。個人の特徴情報を受信したバイオメトリクス認証サーバー５は、認証を行い特定した個人番号を返信する。

【００４４】

次に、ステップ１０３において、個人識別コントローラ１は、バイオメトリクス認証サーバー５からの応答を待つ。応答が有る場合には、次のステップ１０４へ進む。

【００４５】

次に、ステップ１０４において、個人識別コントローラ１は、図３のサーバーテーブルで指定されたそれぞれのバイオメトリクス認証サーバー５のうち、あらかじめ設定されている所定数の認証結果が返信されたかどうかを判断する。所定数に達していない場合は、ステップ１０３に戻り、返信を待つ。一方、所定数の返信が届いた場合には、次のステップ１０５へ進む。

30

【００４６】

次に、ステップ１０５において、認証結果の判断論理がＯＲかＡＮＤかを判断する。どちらの論理で判断するかは、あらかじめ個人識別コントローラ１毎に設定しておく。認証論理がＯＲの場合は、次のステップ１０６へ進む。一方、認証論理がＡＮＤの場合には、ステップ１０７へ進む。

【００４７】

次に、ステップ１０６において、認証論理がＯＲの場合は、複数台のバイオメトリクス認証サーバー５から返信された個人番号に基づいて、順に、図２に示す通行可否設定テーブルを参照し、個人番号のいずれかで該当の扉を解錠してよいか判断する。通行可の場合には、つまり通行可否設定テーブルにおいていずれかの該当個人番号の該当扉番号が○印の場合には、次のステップ１０９へ進む。一方、通行不可の場合は、つまり通行可否設定テーブルにおいていずれの該当個人番号の該当扉番号が×印の場合は、ステップ１１２へ進む。

40

【００４８】

次に、ステップ１０９において、通行可の場合には、個人識別コントローラ１は、電気錠３を解錠し、個人識別装置２に通行可能であることを表示する。

【００４９】

50

次に、ステップ110において、個人識別コントローラ1は、該当の扉の開閉による通行を待ち、通行が完了したら、次のステップ111へ進む。

【0050】

そして、ステップ111において、個人識別コントローラ1は、通行が完了した場合には、電気錠3を施錠して処理を終了し、次の操作を待つ。

【0051】

また、ステップ112において、個人識別コントローラ1は、ステップ106で通行不可と判断された場合は、通行できないことを個人識別装置2に表示し、処理を完了する。

【0052】

ステップ107において、認証論理がANDの場合には、複数台のバイオメトリクス認証サーバー5で認証され返信された個人番号が全て一致しているかを判断する。一致している場合には、次のステップ108へ進む。一方、一致していない場合は、ステップ112へ進む。

10

【0053】

次に、ステップ108において、個人番号が全て一致している場合には、この個人番号に基づいて、図2に示す通行可否設定テーブルを参照し、該当の扉を解錠してよいか判断する。通行可の場合には、つまり通行可否設定テーブルにおいて該当個人番号の該当扉番号が○印の場合には、ステップ109へ進む。一方、通行不可の場合は、つまり通行可否設定テーブルにおいて該当個人番号の該当扉番号が×印の場合は、ステップ112へ進む。

【0054】

20

ここで、ステップ104の所定数を1にすれば、もっとも早い認証結果で判断を行うことができ、操作上の速度を優先した処理になる。

【0055】

また、一部のバイオメトリクス認証サーバー5がダウンした場合には、個人識別コントローラ1は、図6に示す処理を行うことにより、図4のステップ104の所定数（応答待数）を変更（減らし）したり、ステップ105の認証論理（認証条件）を変更（ORにしたり）したりして、機能を縮退しての運用も可能となる。

【0056】

さらに、個人識別コントローラ1に複数種類のバイオメトリクス手法の個人識別装置2が接続されている場合には、それぞれの個人識別装置2からの身体上の特徴情報の入力を得て、図3のサーバーテーブルに従い、それぞれの手法のバイオメトリクス認証サーバー5に特徴情報を送信することにより複合的なバイオメトリクス認証も安易に実現することができる。

30

【0057】

つづいて、図5により、テンキーやカードにより個人を特定した後、そ個人と身体上の特徴が一致しているかを判断する場合の処理動作について説明する。

【0058】

図4の処理動作と類似しているので、相違点について説明する。

【0059】

最初に、ステップ201において、個人識別コントローラ1は、例えば、テンキーやカード読み取り機で個人番号を入力する。

40

【0060】

次に、ステップ202において、個人識別装置2により個人の身体上の特徴情報を抽出する。

【0061】

次に、ステップ203において、個人番号と個人の特徴情報を合せて、バイオメトリクス認証サーバー5に送信する。つまり、個人識別装置2毎に、図3のサーバーテーブルで指定されたそれぞれのバイオメトリクス認証サーバー5へ汎用ネットワーク6を通じて送信する。

【0062】

50

バイオメトリクス認証サーバー５は、個人番号をキーとして既に登録済みの個人の特徴情報と、今回、個人識別装置２により抽出された個人の特徴情報の照合を行い、一致するかどうかを判断し、結果を返信する。

【００６３】

ステップ２０４～２０６は、図４のステップ１０３～１０５と同様である。

【００６４】

ステップ２０７において、個人識別コントローラ１は、認証論理がＯＲの場合は、いずれかのバイオメトリクス認証サーバー５から認証ＯＫが返信されているかを判断する。認証ＯＫが返信されている場合には、ステップ２０９へ進む。一方、認証ＯＫが返信されていない場合は、ステップ２１３へ進む。

10

【００６５】

ステップ２０８において、個人識別コントローラ１は、認証論理がＡＮＤの場合には、全てのバイオメトリクス認証サーバー５から認証ＯＫが返信されているかを判断する。認証ＯＫが返信されている場合には、ステップ２０９へ進む。一方、認証ＯＫが返信されていない場合は、ステップ２１３へ進む。

【００６６】

ステップ２０９において、個人番号に基づいて、図２に示す通行可否設定テーブルを参照し、該当の扉を解錠してよいか判断する。通行可の場合には、つまり通行可否設定テーブルにおいて該当個人番号の該当扉番号が○印の場合には、ステップ２１０へ進む。一方、通行不可の場合は、つまり通行可否設定テーブルにおいて該当個人番号の該当扉番号が×

20

印の場合には、ステップ２１３へ進む。

【００６７】

以下、ステップ２１０～２１３は、図４のステップ１０９～１１２と同様である。

【００６８】

以上のように、この発明の実施の形態１に係る出入管理装置は、バイオメトリクス認証サーバー５をシステムの規模、信頼性、応答性、複合認証などの要望に合わせて、複数台設置し、個人識別コントローラ１より適切なバイオメトリクス認証サーバー５に特徴情報を送信し、その認証結果を判定し、個人を識別することができる。

【００６９】

また、この発明の実施の形態１に係る出入管理装置は、一部のバイオメトリクス認証サーバー５がダウンしても、運用を継続することができる。

30

【００７０】

また、複数のバイオメトリクス手法の組み合わせによる照合や、アルゴリズムやチューニングの異なる認証方法の組み合わせによる認証結果により個人を識別することができる。

【００７１】

これらにより、応答性が良く、信頼性が高く、高機能な出入管理装置を実現することができる。

【００７２】

【発明の効果】

この発明の請求項１に係る出入管理装置は、以上説明したとおり、個人の身体上の特徴を抽出する個人識別装置及び電気錠が接続され、通行可否設定テーブルを参照し個人の特徴情報に対応する個人番号に基づいて通行の可否を判断して前記電気錠を施解錠する個人識別コントローラと、前記個人識別装置により抽出した個人の特徴情報の認証を行い特定した個人番号を返信する複数のバイオメトリクス認証サーバーと、前記個人識別コントローラ、及び前記複数のバイオメトリクス認証サーバーを相互に接続するネットワークとを備え、前記個人識別コントローラは、前記個人識別装置により抽出した個人の特徴情報を、前記複数のバイオメトリクス認証サーバーへ送信し、前記複数のバイオメトリクス認証サーバーのうち所定数から認証結果が返信された場合には、前記通行の可否を判断するので、応答を早くすることができ、認証の精度を向上することができるという効果を奏する。

40

【００７３】

50

この発明の請求項 2 に係る出入管理装置は、以上説明したとおり、個人の身体上の特徴を抽出する個人識別装置及び電気錠が接続され、通行可否設定テーブルを参照し個人の特徴情報に対応する個人番号に基づいて通行の可否を判断して前記電気錠を施解錠する個人識別コントローラと、個人番号をキーとして登録済みの個人の特徴情報と前記個人識別装置により抽出した個人の特徴情報の照合認証を行い、一致するかどうかを判断し、認証結果を返信する複数のバイオメトリクス認証サーバーと、前記個人識別コントローラ、及び前記複数のバイオメトリクス認証サーバーを相互に接続するネットワークとを備え、前記個人識別コントローラは、入力した個人番号及び前記個人識別装置により抽出した個人の特徴情報を、前記複数のバイオメトリクス認証サーバーへ送信し、前記複数のバイオメトリクス認証サーバーのうち所定数から認証結果が返信された場合には、前記通行の可否を判断するので、応答を早くすることができ、認証の精度を向上することができるという効果を奏する。

10

【0074】

この発明の請求項 3 に係る出入管理装置は、以上説明したとおり、前記個人識別コントローラが、個人識別装置毎に、前記個人の特徴情報を送信すべきバイオメトリクス認証サーバーを記述したサーバーテーブルを有するので、応答を早くすることができ、認証の精度を向上することができるという効果を奏する。

【0075】

この発明の請求項 4 に係る出入管理装置は、以上説明したとおり、前記個人識別コントローラが、前記所定数の認証結果のいずれか 1 つに基づいて、あるいは前記所定数の認証結果が全て一致している場合に一致した認証結果に基づいて、前記通行の可否を判断するので、応答を早くすることができ、認証の精度を向上することができるという効果を奏する。

20

【0076】

この発明の請求項 5 に係る出入管理装置は、以上説明したとおり、前記個人識別コントローラが、前記複数のバイオメトリクス認証サーバーの一部がダウンした場合には、前記所定数を変更するので、応答を早くすることができ、認証の精度を向上することができるという効果を奏する。

【0077】

この発明の請求項 6 に係る出入管理装置は、以上説明したとおり、前記個人識別コントローラが、前記複数のバイオメトリクス認証サーバーの一部がダウンした場合には、前記所定数の認証結果のいずれか 1 つに基づいて、前記通行の可否を判断するので、応答を早くすることができ、認証の精度を向上することができるという効果を奏する。

30

【図面の簡単な説明】

【図 1】 この発明の実施の形態 1 に係る出入管理装置の構成を示す図である。

【図 2】 この発明の実施の形態 1 に係る出入管理装置の通行可否設定テーブルの構成を示す図である。

【図 3】 この発明の実施の形態 1 に係る出入管理装置のサーバーテーブルの構成を示す図である。

【図 4】 この発明の実施の形態 1 に係る出入管理装置の動作を示すフローチャートである。

40

【図 5】 この発明の実施の形態 1 に係る出入管理装置の動作を示すフローチャートである。

【図 6】 この発明の実施の形態 1 に係る出入管理装置の動作を示すフローチャートである。

【図 7】 従来の出入管理装置の構成を示す図である。

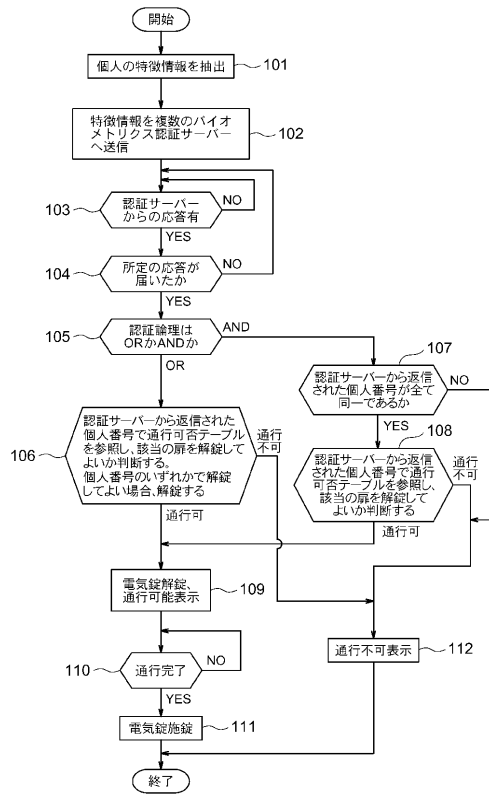
【図 8】 従来の出入管理装置の動作を示すフローチャートである。

【符号の説明】

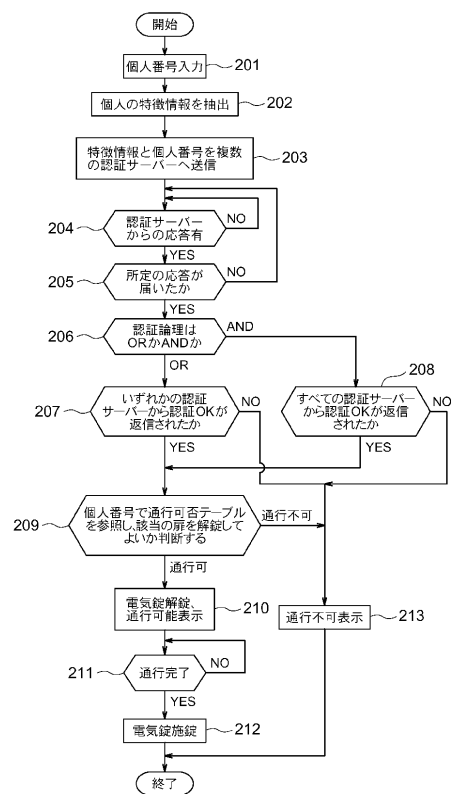
1、1 A、1 B 個人識別コントローラ、2、2 A、2 B 個人識別装置、3、3 A、3 B 電気錠、4 データ設定端末、5 A バイオメトリクス認証サーバー、5 B バイオ

50

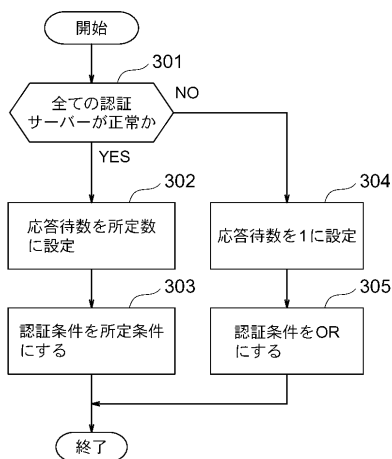
【図 4】



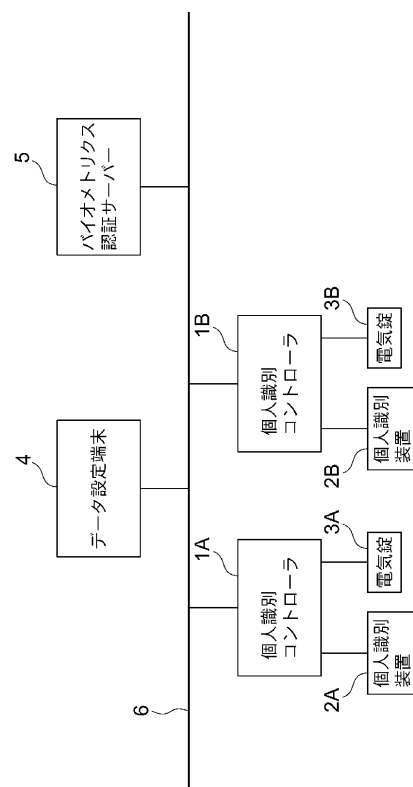
【図 5】



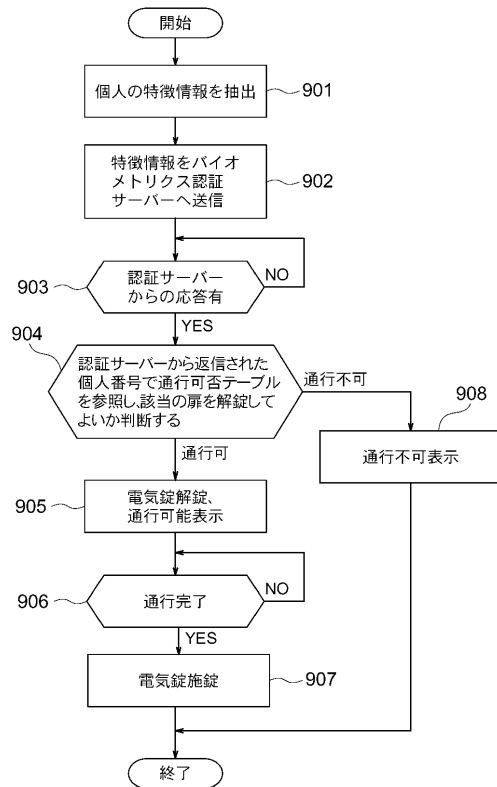
【図 6】



【図 7】



【図 8】



フロントページの続き

(72)発明者 高部 克則
東京都千代田区丸の内二丁目2番3号 三菱電機株式会社内

審査官 井上 博之

(56)参考文献 特開2001-040924 (JP, A)
特開2002-213125 (JP, A)
特開2001-325569 (JP, A)
実開平05-094473 (JP, U)

(58)調査した分野(Int.Cl., DB名)
E05B 49/00