

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第5297397号
(P5297397)

(45) 発行日 平成25年9月25日 (2013. 9. 25)

(24) 登録日 平成25年6月21日 (2013. 6. 21)

(51) Int. Cl.	F 1
E 0 5 B 49/00 (2006. 01)	E O 5 B 49/00 Z
G 0 6 F 21/32 (2013. 01)	G O 6 F 21/20 1 3 2
G 0 6 F 21/34 (2013. 01)	G O 6 F 21/20 1 3 4
G 0 6 K 7/00 (2006. 01)	G O 6 K 7/00 W

請求項の数 7 (全 16 頁)

(21) 出願番号	特願2010-11531 (P2010-11531)	(73) 特許権者	000005108
(22) 出願日	平成22年1月22日 (2010. 1. 22)		株式会社日立製作所
(65) 公開番号	特開2011-149204 (P2011-149204A)		東京都千代田区丸の内一丁目6番6号
(43) 公開日	平成23年8月4日 (2011. 8. 4)	(74) 代理人	100064414
審査請求日	平成23年11月2日 (2011. 11. 2)		弁理士 磯野 道造
		(74) 代理人	100111545
			弁理士 多田 悦夫
		(72) 発明者	鈴木 亮介
			茨城県ひたちなか市市毛1070番地 株
			式会社日立製作所 都市開発システム社内
		審査官	深田 高義

最終頁に続く

(54) 【発明の名称】 ドアセキュリティシステムおよびその制御装置

(57) 【特許請求の範囲】

【請求項 1】

ユーザが携帯する認証用の二次元情報を読み取って、ドアのセキュリティを解除するか否かを判定するドアセキュリティシステムであって、

撮像装置と制御装置とを備え、

前記制御装置は前記撮像装置と通信可能に接続され、

前記制御装置は、

前記二次元情報から抽出される識別情報と、その識別情報を取得したときにセキュリティを解除可能なドアとを関連付けた認証テーブルを記憶しており、

前記ユーザの移動中に前記撮像装置によって撮影された前記二次元情報を含む映像を画像情報として取得し、

その取得した画像情報に対して所定の画像解析を行ってその二次元情報を取得し、

その取得した二次元情報から識別情報を抽出し、

当該抽出した識別情報と前記認証テーブルとを用いて、そのドアのセキュリティを解除するか否かの判定を行い、

前記二次元情報は、前記二次元情報以外の手段で記録された第2の識別情報を有する認証媒体に印刷されており、

前記ドアセキュリティシステムは、さらに、前記ドアの近傍に設置され、前記ユーザによって提示される前記認証媒体から前記第2の識別情報を読み取る読取装置を備え、

前記読取装置は、通信可能に前記制御装置と接続され、

10

20

前記撮像装置による前記二次元情報の読み取りが正しく行えなかった場合、
前記制御装置は、
前記ユーザによって前記読取装置に対して提示され、その読取装置が読み取った前記第
2の識別情報に基づいてそのドアのセキュリティを解除するか否かの判定を行う
ことを特徴とするドアセキュリティシステム。

【請求項2】

前記撮像装置は、防犯用に設置されている防犯カメラである
ことを特徴とする請求項1に記載のドアセキュリティシステム。

【請求項3】

前記制御装置は、さらに、
前記撮像装置から送信される画像情報に対して画像解析を行って前記ユーザの顔を抽出
し、
前記二次元情報から抽出された識別情報と前記認証テーブルとを用いた判定でそのドア
のセキュリティを解除すると判定された場合であって、かつ、前記ユーザの顔が抽出され
たときに、そのドアのセキュリティを解除する
ことを特徴とする請求項1および請求項2に記載のドアセキュリティシステム。

【請求項4】

前記二次元情報は、物に印刷されており、
前記制御装置は、前記撮像装置によって撮影された画像情報から前記物を検出したとき
、当該物に印刷されている二次元情報に焦点を合わせて、当該二次元情報を撮影する
ことを特徴とする請求項1ないし請求項3のいずれか一項に記載のドアセキュリティシス
テム。

【請求項5】

前記二次元情報は、可視光下では印字が見えず、赤外線光下でのみ印字が見えるインク
によって前記物に印刷されており、
前記撮像装置は、赤外線光を用いて撮影する
ことを特徴とする請求項4に記載のドアセキュリティシステム。

【請求項6】

前記二次元情報は、複写機によって複写できないインクを用いて印刷されている
ことを特徴とする請求項4に記載のドアセキュリティシステム。

【請求項7】

ユーザが携帯する認証用の二次元情報を読み取って、ドアのセキュリティを解除するか
否かを判定するドアセキュリティシステムにおいて用いられる制御装置であって、

前記制御装置は、
撮像装置と通信可能に接続され、
前記二次元情報から抽出される識別情報と、その識別情報を取得したときにセキュリ
ティを解除可能なドアとを関連付けた認証テーブルを記憶する記憶部と、
前記ユーザの移動中に前記撮像装置によって撮影される前記二次元情報を含む映像を画
像情報として取得し、その取得した画像情報に対して所定の画像解析を行ってその二次元
情報を取得する画像解析部と、

前記取得した二次元情報から識別情報を抽出する識別情報抽出部と、
前記識別情報抽出部によって抽出した識別情報と前記認証テーブルとを用いて、そのド
アのセキュリティを解除するか否かの判定を行う認証部と、を備え、

さらに、前記二次元情報が前記二次元情報以外の手段で記録された第2の識別情報を有
する認証媒体に印刷されていて、

前記制御装置は、
前記ドアの近傍に設置され、前記ユーザによって提示される前記認証媒体から前記第2
の識別情報を読み取る読取装置と通信可能に接続され、

前記撮像装置による前記二次元情報の読み取りが正しく行えなかった場合、
前記ユーザによって前記読取装置に対して提示され、その読取装置が読み取った前記第

10

20

30

40

50

2の識別情報に基づいてそのドアのセキュリティを解除するか否かの判定を行う
を備えることを特徴とする制御装置。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、二次元情報を利用したドアセキュリティシステムおよびその制御装置に関する。

【背景技術】

【0002】

ドアセキュリティシステムは、一般的に、一戸建住宅、集合住宅、事務所ビル等の出入口において、通行者が、正しい通行者であることを示す情報を提示して、ドアセキュリティシステムが、その提示情報を予め登録されている登録情報と照合し、提示情報と登録情報とが一致した場合に、ドアの解錠を行う。

【0003】

特許文献1および特許文献2には、提示情報として、二次元コードを用いた電気錠制御システムが開示されている。このシステムでは、出入口に設置してある来訪者認識用カメラを装備した認証端末は、遠距離の合焦範囲の光学特性を備えた通常モードと、接写可能な接写モードとを備え、それぞれのモードがスイッチによって切り替えられる構成となっている。そこで、来訪者は、出入口の端末のスイッチを操作して、接写モードを選択し、予め割り当てられている二次元コードを来訪者認識用カメラに提示する。そして、端末によって読み取られた二次元コードと予め登録されている登録情報とが照合され、照合された二次元コードと登録情報とが一致している場合に、ドアが解錠される。

【先行技術文献】

【特許文献】

【0004】

【特許文献1】特開2004-238965号公報

【特許文献2】特開2006-090006号公報

【発明の概要】

【発明が解決しようとする課題】

【0005】

しかしながら、特許文献1および特許文献2で開示されている発明では、来訪者は、二次元コードを認証端末に提示するために、出入口の認証端末の前で一旦立ち止まらなければならない。したがって、セキュリティの掛けられたドアの数が多くなるに従って、立ち止まる回数が増加し、通行に要する時間が増加するという問題がある。そこで、本発明は、ユーザが移動しながら認証できる、二次元情報を利用したドアセキュリティシステムおよびその制御装置を提供することを課題とする。

【課題を解決するための手段】

【0006】

前記課題を解決するために、本発明は、ユーザが携帯する認証用の二次元情報を読み取って、ドアのセキュリティを解除するか否かを判定するドアセキュリティシステムであって、撮像装置と制御装置とを備え、前記制御装置が前記撮像装置と通信可能に接続され、前記制御装置が、前記二次元情報から抽出される識別情報と、その識別情報を取得したときにセキュリティを解除可能なドアとを関連付けた認証テーブルを記憶しており、前記ユーザの移動中に前記撮像装置によって撮影された前記二次元情報を含む映像を画像情報として取得し、その取得した画像情報に対して所定の画像解析を行ってその二次元情報を取得し、その取得した二次元情報から識別情報を抽出し、当該抽出した識別情報と前記認証テーブルとを用いて、そのドアのセキュリティを解除するか否かの判定を行い、前記二次元情報は、前記二次元情報以外の手段で記録された第2の識別情報を有する認証媒体に印刷されており、前記ドアセキュリティシステムが、さらに、前記ドアの近傍に設置され、前記ユーザによって提示される前記認証媒体から前記第2の識別情報を読み取る読取装置

を備え、前記読取装置が、通信可能に前記制御装置と接続され、前記撮像装置による前記二次元情報の読み取りが正しく行えなかった場合、前記制御装置が、前記ユーザによって前記読取装置に対して提示され、その読取装置が読み取った前記第2の識別情報に基づいてそのドアのセキュリティを解除するか否かの判定を行うことを特徴とする。

【発明の効果】

【0007】

本発明によれば、ユーザが移動しながら認証できる、二次元情報を利用したドアセキュリティシステムおよびその制御装置を提供することが可能となる。

【図面の簡単な説明】

【0008】

10

【図1】第1実施形態におけるドアセキュリティシステムの構成の一例を示す図である。

【図2】第1実施形態における制御装置の機能例を示す図である。

【図3】第1実施形態の制御装置の記憶する認証テーブルの一例を示す図である。

【図4】第1実施形態における認証用制御装置の機能例を示す図である。

【図5】第1実施形態の認証用制御装置の記憶する、(a)認証テーブルの一例、(b)撮像装置ネットワークアドレステーブルの一例、(c)制御装置ネットワークアドレステーブルの一例、を示す図である。

【図6】第1実施形態における、撮像装置を用いた画像情報の取得からドア解錠に至る処理の流れを示す図である。

【図7】ドアセキュリティ解除指示情報の一例を示す図である。

20

【図8】第1実施形態における、第2の識別情報の読取装置を用いた第2の識別情報の認証からドア解錠に至る処理の流れを示す図である。

【図9】第2実施形態におけるドアセキュリティシステムの構成の一例を示す図である。

【図10】第2実施形態における制御装置の機能例を示す図である。

【図11】第2実施形態における、撮像装置を用いた画像情報の取得からドア解錠に至る処理の流れを示す図である。

【発明を実施するための形態】

【0009】

次に、本発明を実施するための形態（以降、「本実施形態」と称す）について、適宜図面を参照しながら詳細に説明する。

30

【0010】

（第1実施形態）

第1実施形態におけるドアセキュリティシステム1Aの構成について、図1を用いて説明する。図1に示すように、ドアセキュリティシステム1Aは、通路に設置された自動ドア（ドア）11、21、31、41と、各自動ドア11、21、31、41の近傍に設置されるカードリーダー（読取装置）12、22、32、42と、自動ドア11、21、31、41とカードリーダー12、22、32、42とを制御する制御装置100、200、300と、防犯のために自動ドア付近に設置される撮像装置13、23、33、43と、ネットワーク500を介して制御装置100、200、300や撮像装置13、23、33、43と通信可能に接続される認証用制御装置（制御装置）400と、ユーザH1が携帯する認証用の二次元情報（以降、二次元コードと称す）が印刷された認証カード（認証媒体）C1と、で構成される。なお、自動ドアの台数、制御装置の台数、撮像装置の台数、認証用制御装置の台数、および認証カードの枚数は、図1に示した数に限られることはない。尚、認証用制御装置400も制御装置の一種であり、制御装置100、200、300と、認証用制御装置400とをまとめて、ドアセキュリティシステム1Aの制御装置と呼ぶこともある。

40

【0011】

図1に示すドアセキュリティシステム1Aの最小単位の構成は、（1）自動ドア11、カードリーダー12、制御装置100、撮像装置13、ネットワーク500、認証用制御装置400、および認証カードC1の組、（2）自動ドア21、カードリーダー22、制御装

50

置 200、撮像装置 23、ネットワーク 500、認証用制御装置 400、および認証カード C1 の組、(3) 自動ドア 31、カードリーダー 32、制御装置 300、撮像装置 33、ネットワーク 500、認証用制御装置 400、および認証カード C1 の組、(4) 自動ドア 41、カードリーダー 42、制御装置 300、撮像装置 43、ネットワーク 500、認証用制御装置 400、および認証カード C1 の組、のいずれかである。どの組についても、処理の流れは同様になるので、以降の説明では、自動ドア 11、カードリーダー 12、制御装置 100、撮像装置 13、ネットワーク 500、認証用制御装置 400、および認証カード C1 の組について記載する。

【0012】

(ドアセキュリティシステムの動作の概要)

10

撮像装置 13 は、防犯用のカメラであって、自動ドア 11 付近のエリア A10 の風景を撮影して、その撮影した画像情報を認証用制御装置 400 に、通信線 L13、ネットワーク 500、および通信線 L400 を介して送信している。ユーザ H1 が認証カード C1 を携帯してエリア A10 内に侵入してくると、その画像情報が認証用制御装置 400 に送信される。認証用制御装置 400 は、防犯のための公知のアプリケーションを起動しており、例えば、人や物がエリア A10 内に侵入して来たときの画像情報の変化を検出する。なお、画像情報の変化の検出には、例えば、特開昭 61-119580 号公報等が開示されている技術を用いることができる。

【0013】

また、認証用制御装置 400 は、例えば、公知の画像解析用のアプリケーション（例えば、特開平 7-288732 号公報参照）を起動しており、画像情報の変化を検出したとき、撮像装置 13 から送信されてくる画像情報を解析して、認証カード C1 を検出する。そして、認証用制御装置 400 は、検出した認証カード C1 に印刷されている認証用の二次元コードを読み取るために、撮像装置 13 を制御して、認証カード C1 を自動的に追尾して焦点を調整する。なお、特開平 7-288732 号公報には、移動する被写体を自動追尾して焦点を合わせ続けるとともに、被写体を追尾動作可能な範囲を可能な限り広くとることができる技術が開示されている。

20

【0014】

いま、図 1 に示すように、ユーザ H1 は、認証用の二次元コードが印刷された認証カード C1（物）を携帯している。そして、ユーザ H1 が、エリア A10 内で、移動しながら（歩きながら）認証カード C1 を撮像装置 13 に提示する。撮像装置 13 は、ユーザ H1 と認証カード C1 とを含む風景を画像情報として認証用制御装置 400 に送信する。認証用制御装置 400 は、受信した画像情報に対して画像解析を行って、認証カード C1 を検出する。そして、認証用制御装置 400 は、撮像装置 13 を制御して、認証カード C1 に自動的に焦点を合わせて、認証カード C1 に印刷されている認証用の二次元コードの画像情報を取得する。次に、認証用制御装置 400 は、その取得した認証用の二次元コードの画像情報から、カード ID（識別情報、コード ID）を抽出する（ここでは二次元コードのコード ID（識別情報）がカードに印刷されているのでカード ID と呼ぶこととする）。

30

【0015】

そして、認証用制御装置 400 は、当該カード ID が登録済みか否かを判定する。登録済みの場合、認証用制御装置 400 は、当該画像情報を送信してきた撮像装置 13 の設置位置によって関連付けられている、制御対象となる自動ドア 11 を特定し、その特定された自動ドア 11 が当該カード ID に対してドアセキュリティ解除を許可されているか否かを判定する。ドアセキュリティ解除が許可されていると判定した場合、認証用制御装置 400 は、該当する自動ドア 11 を制御している制御装置 100 に、通信線 L400、ネットワーク 500、および通信線 L100 を介して、ドアセキュリティ解除指示情報を送信する。制御装置 100 は、ドアセキュリティ解除指示情報を受信すると、通信線 L11 を経由して、自動ドア 11 にドアセキュリティ解除指示を送信し、自動ドア 11 のドアセキュリティ解除（ドアの解錠）を実行する。

40

50

【0016】

また、認証用制御装置400は、受信した画像情報から、認証カードC1とともに撮影されているユーザH1の顔も抽出し、顔が隠されているか否かを判定する。すなわち、認証用制御装置400における、ドアセキュリティ解除を許可するか否かの判定において、カードIDに基づく判定だけでなく、顔が隠されていないことを許可条件として付加してもよい。この場合、二次元コードから抽出されたカードIDに基づいて自動ドア11のセキュリティを解除しても良いと判定され、かつ、ユーザの顔が抽出された（顔が隠されていない）場合に、ドアのセキュリティを解除する。そして、ユーザの顔が抽出できない（ユーザの顔が隠されている）場合には、例えば二次元コードから抽出されたカードIDがセキュリティ解除可能なものであったとしても、セキュリティ解除を行わない。これにより、セキュリティを向上させることができる。尚、ここでは顔が抽出できたか否かのみで判定すれば十分であるため、顔から個人を特定する処理までは行っていない。なお、顔の抽出および顔が隠されていないことの判定には、例えば、特開2000-251077号公報に開示されている、撮影されたユーザの顔画像において、目と口の画像が正確に検出されているか否かを判定する技術を用いることができる。

10

【0017】

また、撮像装置13による二次元コード情報の読み取りが正しく行えなかった場合には、ユーザH1にカードリーダー12を利用した認証を行ってもらふ。その場合、ユーザH1に、カードリーダー12に認証カードC1をかざしてもらふ。二次元コードが印刷された認証媒体である認証カードC1には、二次元コード以外の手段、例えばICチップなどによりカードID（第2の識別情報）が記録されている。この第2の識別情報は、二次元コードによる識別情報と同じ情報であることが望ましいが、別途第2の識別情報に対応した認証テーブルを設けるか、別途設けられたテーブルなどにより二次元コードによる識別情報と第2の識別情報とが関連付けられていれば、異なる情報であっても良い。ここでは、この第2の識別情報は、二次元コードによる識別情報と同じ情報であると仮定して説明する。カードリーダー12は、認証カードC1に設けられたICチップなどからカードIDに係る情報（第2の識別情報）を取得し、当該カードIDに係る情報を通信線L12を介して制御装置100に送信する。制御装置100は、受信したカードIDに係る情報に含まれる当該カードIDが登録済みか否かを判定する。登録済みの場合、制御装置100は、ドアセキュリティ解除を許可されているドアか否かを判定する。制御装置100は、ドアセキュリティ解除を許可されているドアであると判定した場合には、該当の自動ドア11のドアセキュリティ解除を実行する。

20

30

【0018】

《制御装置の機能》

次に、制御装置100の機能について、図2を用いて説明する。制御装置100は、記憶部110、通信部120、制御部130、および認証部140を備え、バスSB1を介して各部間で相互に情報を送受信する。

【0019】

記憶部110は、認証情報全体を格納した認証テーブル111を記憶している。認証テーブル111は、図3に示すように、カードID（識別情報）と、そのカードIDが取得されたときにセキュリティを解除可能なドアとを関連付けて記憶したものである。図3では、セキュリティ解除可能なドア識別情報の一例として、ドア1、ドア2、ドア3、ドア4（それぞれ、自動ドア11、21、31、41に対応）が登録されており、ドアセキュリティ解除を許可する箇所には、フラグとして「1」が付けられている。

40

【0020】

図2に戻って、通信部120は、カードリーダー12と通信を行うカードリーダー通信部121と、自動ドア11と通信を行うドア通信部122と、ネットワーク500を経由する通信を行うネットワーク通信部123とを備える。

【0021】

制御部130は、制御装置100の処理全体の制御を司る。また、制御部130は、カ

50

ードリーダー12の制御を行うカードリーダー制御部131と、自動ドア11の制御を行うドア制御部132と、記憶部110に記憶するテーブルの登録、更新、削除等を行うテーブル制御部133とを備える。

【0022】

認証部140は、カードリーダー12経由で取得した認証用のカードIDを用いて、記憶部110の認証テーブル111を参照して、カードIDが認証テーブル111に登録されているか否かの判定、および、登録されている場合にフラグに基づいてドアセキュリティ解除を許可しているドアか否かの判定を実行する。

【0023】

《認証用制御装置の機能》

次に、認証用制御装置400の機能について、図4を用いて説明する。認証用制御装置400は、記憶部410、通信部420、制御部430、画像解析部440、カードID抽出部450、および認証部460を備え、バスSB2を介して各部間で相互に情報を送受信する。

【0024】

記憶部410は、認証情報全体を格納した認証テーブル411、各撮像装置13、23、33、43のネットワークアドレスを格納した撮像装置ネットワークアドレステーブル412、および各制御装置100、200、300のネットワークアドレスを格納した制御装置ネットワークアドレステーブル413を記憶している。図5(a)は、認証テーブル411の一例を示している。認証テーブル411は、図3に示す認証テーブル111と同様に、カードID（二次元コードから抽出される識別情報）と、そのカードIDが取得されたときにセキュリティを解除可能なドアとを関連付けて記憶したものである。ここでは、セキュリティ解除可能なドア識別情報の一例として、ドア1、ドア2、ドア3、ドア4（それぞれ、自動ドア11、21、31、41に対応）が登録されており、ドアセキュリティ解除を許可する箇所には、フラグとして「1」が付けられている。図5(b)は、撮像装置ネットワークアドレステーブル412の一例を示している。撮像装置ネットワークアドレステーブル412は、撮像装置ネットワークアドレスと、撮像装置13、23、33、43と、制御対象ドア情報のドア識別情報とを関連付けて記憶している。図5(c)は、制御装置ネットワークアドレステーブル413の一例を示している。制御装置ネットワークアドレステーブル413は、制御装置ネットワークアドレスと、制御装置100、200、300と、制御対象ドア情報のドア識別情報とを関連付けて記憶している。

【0025】

図4に戻って、通信部420は、ネットワーク500を経由する通信を行うネットワーク通信部421を備える。

【0026】

制御部430は、制御装置400の処理全体の制御を司る。また、制御部430は、記憶部410に記憶するテーブルの登録、更新、削除等を行うテーブル制御部431と、各撮像装置13、23、33、43のズームやパン等の制御を行う撮像装置制御部432とを備える。

【0027】

画像解析部440は、各撮像装置13、23、33、43から受信した画像情報の画像解析を実行する。カードID抽出部450は、画像解析結果に基づいて、二次元コードからカードIDの抽出を行う。認証部460は、抽出したカードIDを用いて、記憶部410の認証テーブル411を参照して、カードIDが認証テーブル411に登録されているか否かの判定、および、登録されている場合にフラグに基づいてドアセキュリティ解除を許可するドアか否かの判定を実行する。

【0028】

《認証カード》

図1に示す認証カードC1（物、認証媒体）には、二次元コード（二次元情報）が印刷されている。この二次元コードは、例えば数字や文字などの情報を符号化し、二次元的に

10

20

30

40

50

配列された所定のパターンで表したものである。例えば、QRコードなどのように、白と黒の格子状のパターンで情報を表すマトリックス型二次元コードなどを用いることができる。あるいは、二次元コードの一例として、認証カードの縦横方向に、数字や文字を配列させたものや、パターンを配置させたものでもよい。なお、二次元コードは、可視光下では人間の目には見えず、赤外線光下でのみ見えるインクを用いて印刷されている場合、認証カードC1は、赤外線光を撮影する機能を備えた撮像装置13、23、33、43を用いて撮影される。また、二次元コードは、複写機によって複写できないインクを用いて印刷されている場合、また、二次元コードは、複写機によって複写できないようにするために、複写機の解像度よりも小さなドットで構成されている牽制文字によって印刷されている場合、

10

また、既に説明した通り、二次元コードが印刷された認証媒体である認証カードC1には、二次元コード以外の手段、例えばICチップなどによりカードID（第2の識別情報）が記録されている。この第2の識別情報は、二次元コードによる識別情報と同じ情報であることが望ましい。その場合は、認証テーブル111と認証テーブル411を同じものにする事ができる。尚、認証テーブル111として、別途図示しない第2の識別情報に対応した認証テーブルを設けるか、図示しない別途設けられたテーブルなどにより二次元コードによる識別情報と第2の識別情報とが関連付けられていれば、第2の識別情報は、二次元コードによる識別情報と異なる情報であっても良い。

【0029】

20

《第1実施形態におけるドアセキュリティ解除の流れ》

次に、図6を用いて、第1実施形態におけるドアセキュリティ解除の流れについて説明する（適宜図4、5参照）。

【0030】

まず、ステップS601では、認証用制御装置400の画像解析部440は、撮像装置13から送信されてくる画像情報を取得する。なお、画像情報は、送信元の撮像装置13の撮像装置ネットワークアドレスとともに送信されてくる。ステップS602では、画像解析部440は、受信した画像情報を画像解析して、二次元コード（二次元情報）を抽出する。そして、二次元コードが抽出された場合（ステップS602でYES）、ステップS603では、カードID抽出部450は、抽出した二次元コードからカードID（識別情報）を抽出する。次に、カードIDが抽出された場合（ステップS603でYES）、ステップS604では、認証部460は、抽出したカードIDを用いて、認証テーブル411を参照し、認証テーブル411中に抽出したカードIDが有るか否かを判定する。

30

【0031】

認証テーブル411中にカードIDが有る場合（ステップS604でYES）、ステップS605では、認証部460は、そのカードIDに対応して、解除許可（ドアのセキュリティ解除を許可する）か否かを判定する。具体的には、認証部460は、認証テーブル411を参照して、カードIDに関連付けられているドア識別情報の中から、フラグ「1」が付されているドア識別情報を抽出する。また、認証部460は、ステップS601において受信した撮像装置ネットワークアドレスを用いて、撮像装置ネットワークアドレステーブル412を参照して、受信した撮像装置ネットワークアドレスに関連付けられている制御対象ドア情報のドア識別情報を取得することによって、画像情報を送信してきた撮像装置13に対応するドア識別情報を特定する。次に、認証部460は、その特定したドア識別情報が、フラグ「1」が付されているドア識別情報の中に存在するか否かを判定する。そして、存在すると判定した場合に、認証部460は、解除許可と判定する。

40

【0032】

ステップS605で解除許可と判定された場合（ステップS605でYES）、ステップS606では、認証部460は、制御装置100にドアセキュリティ解除を指示するドアセキュリティ解除指示情報を送信する。具体的には、認証部460は、ステップS605で特定したドア識別情報を用いて、制御装置ネットワークアドレステーブル413を参

50

照し、制御対象ドア情報のドア識別情報に関連付けられている制御装置ネットワークアドレスを抽出する。そして、認証部460は、ドアセキュリティ解除指示情報を当該制御装置ネットワークアドレスを宛先として、ネットワーク通信部421を介して送信する。なお、ドアセキュリティ解除指示情報の一例を図7に示す。図7に示すように、ドアセキュリティ解除指示情報701は、制御対象ドアのドア識別情報およびドアセキュリティ解除指示を格納する。

【0033】

なお、ステップS602～S605においてNOの場合、およびステップS606終了後には、処理は、いずれもステップS601へ戻る。また、顔の抽出および顔が隠されていないことの判定を含める場合には、何れかの位置、例えば、ステップS604でYESの次などでその処理を実行すればよい。

10

【0034】

次に、制御装置100の処理について説明する（適宜図2，7参照）。ステップS611では、制御装置100の認証部140は、認証用制御装置400からドアセキュリティ解除指示情報701を取得したか否かを継続的に判定している。そして、ドアセキュリティ解除指示情報を取得したと判定した場合（ステップS611でYES）、ステップS612では、認証部140は、ドアセキュリティ解除指示を、制御対象となる自動ドア11に送信する。なお、ステップS611では、ドアセキュリティ解除指示情報を取得しない場合（ステップS611でNO）、処理はステップS611へ戻る。また、ステップS612での送信の終了後にも、処理はステップS611へ戻る。

20

【0035】

次に、自動ドア11の処理について説明する。ステップS621では、自動ドア11は、制御装置100からドアセキュリティ解除指示を取得したか否かを継続的に判定している。そして、ドアセキュリティ解除指示を取得したと判定した場合（ステップS621でYES）、ステップS622では、自動ドア11は、ドアセキュリティ解除を実行する。ステップS623では、自動ドア11は、ドアセキュリティ解除の状態のまま一定時間待機する。そして、ステップS624では、自動ドア11は、ドアセキュリティをセット（施錠）する。そして、処理は、ステップS621へ戻る。なお、ステップS621においてドアセキュリティ解除指示を取得したと判定されない場合（ステップS621でNO）、処理はステップS621へ戻る。

30

【0036】

次に、撮像装置13による二次元コード情報の読み取りが正しく行えなかった場合に備えて設けられたカードリーダー12によって、カード認証を実行する処理の流れについて、図8を用いて説明する（適宜図2，3参照）。なお、図6と同じ処理については、同じ符号を付し説明を省略する。なお、前記撮像装置13による二次元コード情報の読み取りが正しく行えなかった場合、とは、図6のステップS602～S605においてNOとなった場合のことである。

【0037】

ステップS801では、カードリーダー12は、認証カードC1に設けられたICチップなどからカードIDに係る情報（第2の識別情報）を読み取り、カードIDを取得したか否かを判定する。カードIDを取得したと判定した場合（ステップS801でYES）、ステップS802では、カードリーダー12は、カードIDに係る情報を、制御装置100に送信する。また、ステップS801においてカードIDを取得したと判定されなかった場合（ステップS801でNO）、処理はステップS801へ戻る。また、ステップS802での送信の終了後にも、処理はステップS801へ戻る。

40

【0038】

なお、カードリーダー12が制御装置100に送信する情報には、カードIDに係る情報以外に、カードリーダー12を識別するカードリーダー識別情報を含むものとする。この理由は、図1に示す制御装置300では、複数のカードリーダー32，42が接続されている場合があり、それらのカードリーダーを識別する必要があるからである。

50

【0039】

次に、ステップS811では、制御装置100の認証部140は、カードリーダー12からカードIDを取得したか否かを継続的に判定している。そして、カードIDを取得したと判定した場合（ステップS811でYES）、ステップS812では、認証部140は、取得したカードIDを用いて、認証テーブル111を参照し、認証テーブル111中に抽出したカードIDが有るか否かを判定する。

【0040】

認証テーブル111中にカードIDが有る場合（ステップS812でYES）、ステップS813では、認証部140は、カードIDに対応して、解除許可（ドアのセキュリティ解除を許可する）か否かを判定する。具体的には、認証部140は、認証テーブル111を参照して、カードIDに関連付けられているドア識別情報の中から、フラグ「1」が付されているドア識別情報を抽出する。また、認証部140は、ステップS811において受信したカードリーダー識別情報を用いて、そのカードリーダー識別情報に関連付けられている制御対象ドア情報のドア識別情報を特定する。次に、認証部140は、その特定したドア識別情報が、フラグ「1」が付されているドア識別情報の中に存在するか否かを判定する。そして、存在すると判定された場合に、認証部140は、解除許可と判定する。

【0041】

ステップS813において解除許可と判定された場合（ステップS813でYES）、ステップS814では、認証部140は、ドアセキュリティ解除指示を、制御対象となる自動ドア11に送信する。なお、ステップS811～S813においてNOの場合には、処理はステップS811へ戻る。また、ステップS814での送信の終了後にも、処理はステップS811へ戻る。

【0042】

また、自動ドア11のステップS621～S624は、図6と同様であるので、説明を省略する。

【0043】

（第2実施形態）

次に、第2実施形態におけるドアセキュリティシステム1Bの構成を、図9に示す。第2実施形態では、第1実施形態の認証用制御装置400が存在せず、その認証用制御装置400の機能を、各制御装置100a、200a、300aが備えている。そして、各制御装置100a、200a、300a以外は図1と同じであり、同じ符号を付し、説明を省略する。

【0044】

図10は、制御装置100aの機能の一例を示している。制御装置100aの機能は、図2に示す制御装置100の機能と図4に示す認証用制御装置400の機能とを併合したものである。そして、図2と同じ機能については、それと同じ符号を付し、図4と同じ機能については、それと同じ符号に「b」を付し説明を省略する。

【0045】

《第2実施形態におけるドアセキュリティ解除の流れ》

図11を用いて、第2実施形態におけるドアセキュリティ解除の流れを説明する（適宜図5、10参照）。なお、図6および図8と同じ処理ステップについては、同じ符号を付し、説明を省略する。

【0046】

まず、ステップS1101では、制御装置100aの画像解析部440bは、撮像装置13から送信されてくる画像情報を取得する。なお、画像情報は、送信元の撮像装置13の撮像装置ネットワークアドレスとともに送信されてくる。ステップS1102では、画像解析部440bは、受信した画像情報を画像解析して、二次元コード（二次元情報）を抽出する。そして、二次元コードが抽出された場合（ステップS1102でYES）、ステップS1103では、カードID抽出部450bは、抽出した二次元コードからカードID（識別情報）を抽出する。次に、カードIDが抽出された場合（ステップS1103

でYES)、ステップS1104では、認証部140は、抽出したカードIDを用いて、認証テーブル111を参照し、認証テーブル111中に抽出したカードIDが有るか否かを判定する。

【0047】

ステップS1104以降のステップS813、S814および自動ドア11におけるステップS621～S624は、前記した処理と同じであるので説明を省略する。また、前記撮像装置13による二次元コード情報の読み取りが正しく行えなかった場合に備えて設けられたカードリーダー12によって、ドアセキュリティ解除を実行する処理の流れについては、図8における処理と同様であるので、図示および説明を省略する。

【0048】

以上、各実施形態では、ドアセキュリティシステム1A(1B)が、撮像装置13と認証用制御装置400(制御装置100a)とを備え、認証用制御装置400(制御装置100a)が、自動ドア11を制御するとともに、撮像装置13と通信可能に接続されて構成される。認証用制御装置400(制御装置100a)は、二次元コードのコードID(識別情報)(カードに印刷されている場合にはカードID)と、そのコードIDを取得したときにセキュリティ解除可能なドアとを関連付けた認証テーブル411(認証テーブル111)を予め記憶している。また、認証用制御装置400(制御装置100a)は、ユーザH1の移動中に自動追尾かつ自動焦点機能を備えた撮像装置13によって撮影される二次元コードを画像情報として取得する。そして、認証用制御装置400(制御装置100a)は、取得した画像情報に対して画像解析を行って当該二次元コードを抽出し、さらに抽出した二次元コードからコードIDを抽出し、そのコードIDと認証テーブル411(認証テーブル111)とを用いて、そのドアのセキュリティ解除を行うか否かの判定を行う。このような構成を備えているため、ユーザの移動中に二次元コードを撮像装置13の撮影範囲内に入るように身につける、あるいはかざすことで、コードIDの認証を行って、セキュリティを解除することができ、ユーザH1がドアの前で停止する必要がなくなる。

【0049】

また、本実施形態の撮像装置13は、防犯用のカメラと兼用することができるため、新たに二次元コード読み取り専用の接写型のカメラを設置する必要がない。また、遠方を撮影できるため、接写型のカメラを通常の高さに設置するのとは別に、車椅子利用者の高さに合わせて接写型のカメラを設置する必要がないという効果がある。

【0050】

撮像装置13は、自動ドア11に向かって移動してくるユーザH1の正面方向から撮影する場合には、認証カードC1をネックストラップ等を用いて首からぶら下げたり、胸の位置に装着させたりするだけで、認証カードC1を撮影しやすくなる。このことにより、ユーザH1がわざわざ認証カードC1を撮像装置13に提示しなくとも、本実施形態における認証用制御装置400(制御装置100a)は、カードIDの認証を行うことができる。

【0051】

また、ユーザの顔が隠されていないことをドアセキュリティ解除の条件の一つに加えることによって、二次元コードによるコードIDのみの認証より、セキュリティの向上を図ることができる。

【0052】

また、本実施形態では、ドアとして自動ドアの場合を例として説明したが、ドアが電気錠付ドアであった場合には、必要に応じて、制御装置100(100a)は、セキュリティセット(施錠)のための指示を電気錠に送信する処理を追加して、ドアセキュリティを作動させればよい。

【0053】

また、本実施形態では、二次元コードが認証カードC1に印刷されている場合について説明したが、二次元コードが印刷される認証媒体はカードに限定されない。また、二次元

10

20

30

40

50

コードが携帯電話機や携帯端末の画面に表示されていてもよい。携帯電話機や携帯端末が非接触式のＩＣチップを内蔵していれば、カードリーダー１２等による認証も可能である。

また、本発明ではカードリーダー１２を用いる場合について説明したが、認証媒体を読み取れるものであればカードリーダーに限定されない。

【００５４】

また、本実施形態は、一戸建住宅、集合住宅、事務所ビル等の出入口において適用できるだけでなく、例えば、駅や劇場等の改札口においても適用できる。

【符号の説明】

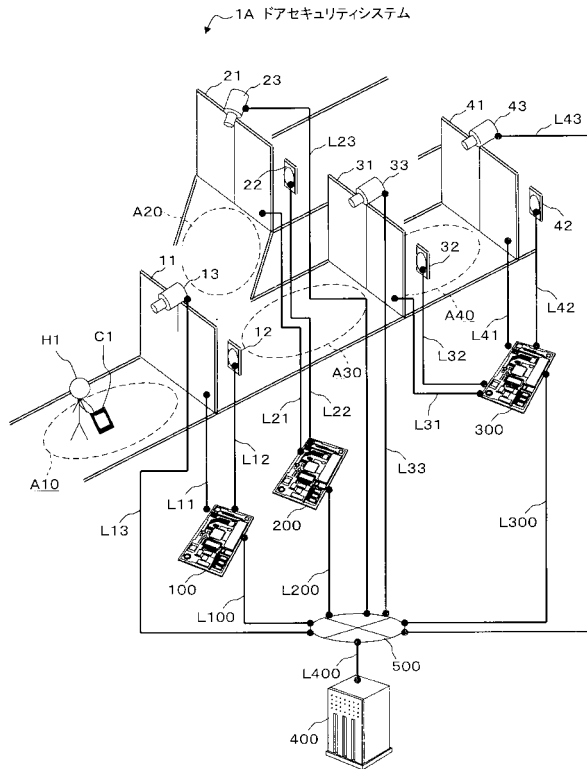
【００５５】

- １Ａ，１Ｂ ドアセキュリティシステム
- １１，２１，３１，４１ 自動ドア（ドア）
- １２，２２，３２，４２ カードリーダー（読取装置）
- １３，２３，３３，４３ 撮像装置
- １００，２００，３００ 制御装置
- １００ａ，２００ａ，３００ａ 制御装置
- １１０，４１０ 記憶部
- １１１，４１１ 認証テーブル
- １４０，４６０ 認証部
- ４００ 認証用制御装置（制御装置）
- ４３２，４３２ｂ 撮像装置制御部
- ４４０，４４０ｂ 画像解析部
- ４５０，４５０ｂ カードＩＤ抽出部（識別情報抽出部）
- ５００ ネットワーク
- Ｃ１ 認証カード
- Ｈ１ ユーザ

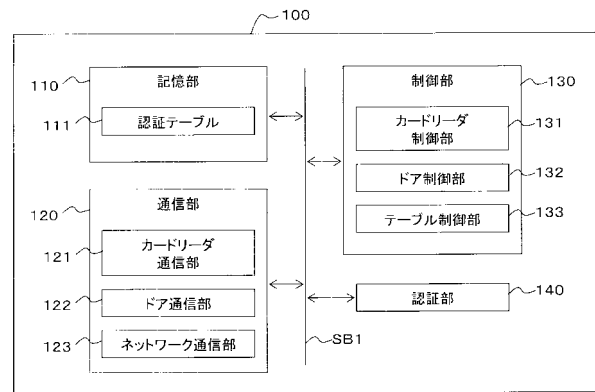
10

20

【図 1】



【図 2】



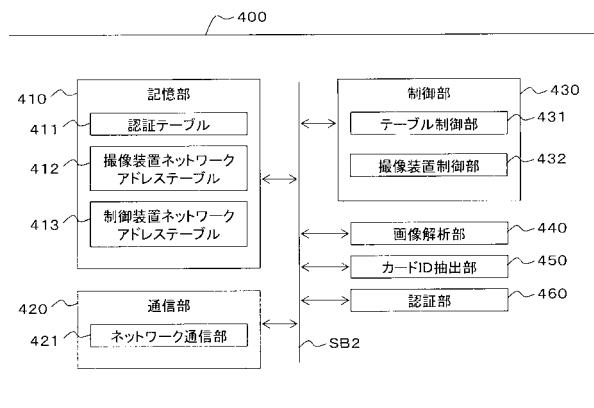
【図 3】

111 認証テーブル

カードID	ドア識別情報			
	ドア1	ドア2	ドア3	ドア4
0123456789	1	1	1	1
1111111111	1	1	1	1
2233445566	1	—	1	1
...				
9876543211	1	1	—	—

(フラグ「1」はドアセキュリティ解除を許可することを表す)

【図 4】



【図 5】

(a)

411 認証テーブル

カードID	ドア識別情報			
	ドア1	ドア2	ドア3	ドア4
0123456789	1	1	1	1
1111111111	1	1	1	1
2233445566	1	—	1	1
...				
9876543211	1	1	—	—

(フラグ「1」はドアセキュリティ解除を許可することを表す)

(b)

412 撮像装置ネットワークアドレステーブル

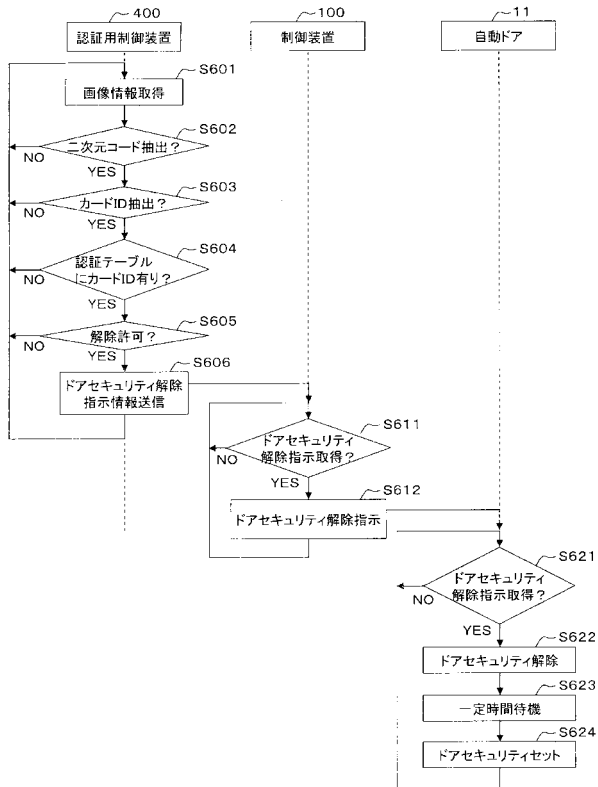
撮像装置ネットワークアドレス	撮像装置	制御対象ドア情報
xxx. xxx. xxx. xxx	13	ドア1
xxx. xxx. xxx. xxx	23	ドア2
xxx. xxx. xxx. xxx	33	ドア3
xxx. xxx. xxx. xxx	43	ドア4

(c)

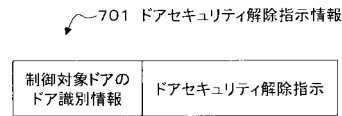
413 制御装置ネットワークアドレステーブル

制御装置ネットワークアドレス	制御装置	制御対象ドア情報
xxx. xxx. xxx. xxx	100	ドア1
xxx. xxx. xxx. xxx	200	ドア2
xxx. xxx. xxx. xxx	300	ドア3, ドア4

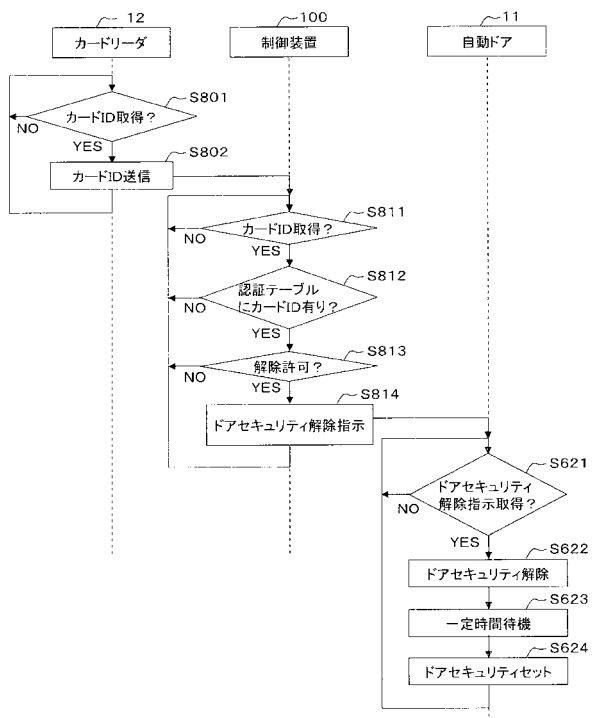
【図 6】



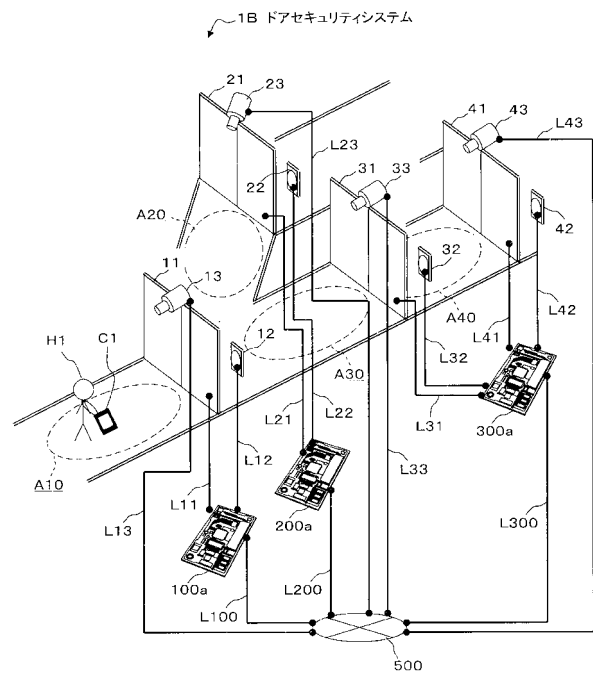
【図 7】



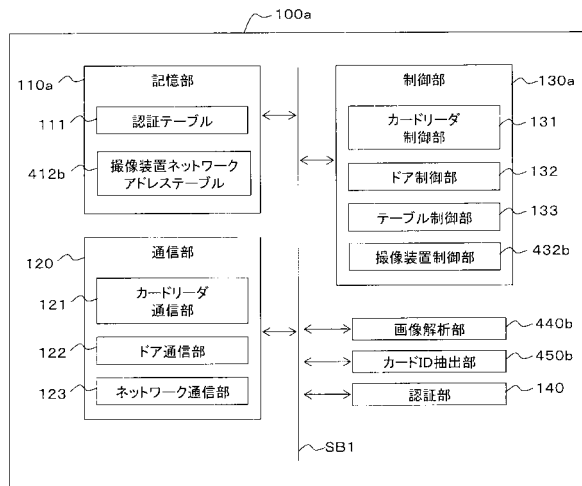
【図 8】



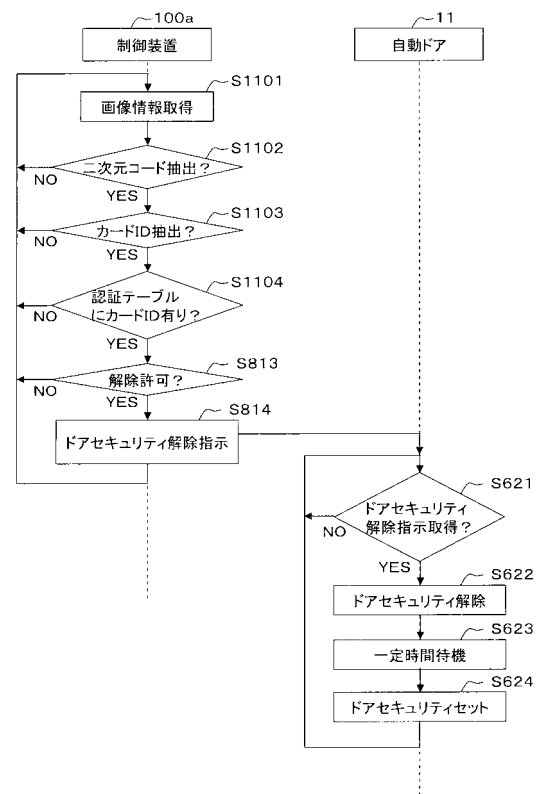
【図 9】



【図10】



【図11】



フロントページの続き

- (56)参考文献 特開平05-079232 (JP, A)
特開2009-215797 (JP, A)
特開2010-010900 (JP, A)
国際公開第2007/114288 (WO, A1)
特開2005-169633 (JP, A)

- (58)調査した分野(Int.Cl., DB名)
E05B 49/00
G06F 21/32
G06F 21/34
G06K 7/00