(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2010-112002
(P2010-112002A)
(43)公開日　平成22年5月20日(2010.5.20)

(51)Int.Cl.		F I			テーマコード（参考）
E05B 49/00	(2006.01)	E05B	49/00	F	2E250
G07C 9/00	(2006.01)	E05B	49/00	J	3E038
G08B 25/04	(2006.01)	E05B	49/00	R	5C087
G08B 25/08	(2006.01)	G07C	9/00	Z	
		G08B	25/04	F	

審査請求 未請求　請求項の数 9　ＯＬ　（全 12 頁）　最終頁に続く

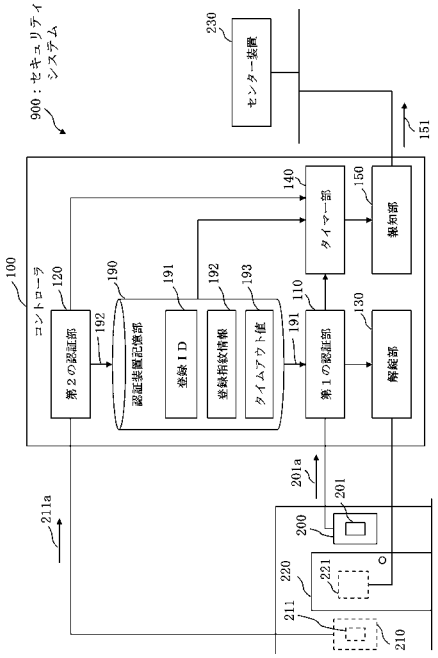
(21)出願番号　特願2008-282992 (P2008-282992)
(22)出願日　平成20年11月4日 (2008.11.4)

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目７番３号
(74)代理人　100099461
弁理士　溝井　章司
(74)代理人　100122035
弁理士　渡辺　敏雄
(72)発明者　田島　規弘
愛知県名古屋市東区矢田南五丁目１番１４号　三菱電機メカトロニクスソフトウエア株式会社内

最終頁に続く

(54)【発明の名称】認証装置およびセキュリティシステム

(57)【要約】
【課題】扉が施錠するまでの間に不審者に侵入された場合に通報を行うセキュリティシステムを安価に構築できるようにすることを目的とする。
【解決手段】利用者は入室するために認証端末装置２００のカードリーダ２０１にＩＤを読み取らせ、所定時間内に部屋内の出側認証端末装置２１０の指紋読取装置２１１に指紋情報を読み取らせる。第１の認証部１１０は、読取ＩＤ２０１ａを入力した場合、読取ＩＤ２０１ａを登録ＩＤ１９１と照合し、認証許可するか判定する。第１の認証部１１０が認証許可した場合、解錠部１３０は電気錠２２１を解錠し、タイマー部１４０はタイマーをセットする。第２の認証部１２０は、読取指紋情報２１１ａを入力した場合、読取指紋情報２１１ａを登録指紋情報１９２と照合し、認証許可するか判定する。第２の認証部１２０により認証許可される前にタイムアウトした場合、報知部１５０はセンター装置２３０に警報通知１５１を送信する。
【選択図】図１



【特許請求の範囲】
【請求項１】
電気錠により施錠された部屋への入室を承認する認証装置であり、
前記部屋の外側に設けられる第１の認証端末装置に所定の第１のデータが入力されたかＣＰＵを用いて判定する第１の認証部と、
前記部屋の内側に設けられる第２の認証端末装置に所定の第２のデータが入力されたかＣＰＵを用いて判定する第２の認証部と、
前記第１の認証部により所定の第１のデータが入力されたと判定された場合、前記電気錠を解錠する解錠部と、
前記第１の認証部により所定の第１のデータが入力されたと判定されてから所定の時間内に前記第２の認証部により所定の第２のデータが入力されたと判定されなかった場合、入室の非承認を所定の装置を用いて報知する報知部と
を備えたことを特徴とする認証装置。
【請求項２】
前記第１の認証端末装置に入力されるデータと前記第２の認証端末装置に入力されるデータとが異なる種類のデータである
ことを特徴とする請求項１記載の認証装置。
【請求項３】
前記第１の認証端末装置に入力されるデータは、前記第２の認証端末装置に入力されるデータより入力に要する時間が短い種類のデータである
ことを特徴とする請求項１～請求項２いずれかに記載の認証装置。
【請求項４】
前記第１の認証部は、前記第１の認証端末装置に入力されたデータが前記所定の第１のデータと一致するか判定し、
前記第２の認証部は、前記第２の認証端末装置に入力されたデータを前記所定の第２のデータと一致するか判定し、
前記第１の認証端末装置に入力されるデータは、前記第２の認証端末装置に入力されるデータより一致判定に要する時間が短い種類のデータである
ことを特徴とする請求項１～請求項３いずれかに記載の認証装置。
【請求項５】
前記第１の認証端末装置と前記第２の認証端末装置とには特定者を識別する識別データが入力され、
前記第２の認証端末装置に入力される識別データは、識別データの入力者と入力される識別データにより識別される特定者との一致を保証する信頼度が前記第１の認証端末装置に入力される識別データより高い種類のデータである
ことを特徴とする請求項１～請求項４いずれかに記載の認証装置。
【請求項６】
前記第１の認証端末装置は、利用者を識別するＩＤが記録されているＩＤカードから前記ＩＤをデータとして読み取るカードリーダを備え、
前記第１の認証部は、前記カードリーダにより読み取られたＩＤが前記所定の第１のデータと一致するか判定する
ことを特徴とする請求項１～請求項５いずれかに記載の認証装置。
【請求項７】
前記第２の認証端末装置は、利用者から生体情報をデータとして読み取る生体情報読取装置を備え、
前記第２の認証部は、前記生体情報読取装置により読み取られた生体情報が前記所定の第２のデータと一致するか判定する
ことを特徴とする請求項１～請求項６いずれかに記載の認証装置。
【請求項８】
前記第２の認証部は、前記第２の認証端末装置に特定の操作が行われたか判定し、

前記報知部は、前記第２の認証部により特定の操作が行われたと判定された場合、入室の非承認を所定の装置を用いて報知する
ことを特徴とする請求項１～請求項７いずれかに記載の認証装置。
【請求項９】
請求項１～請求項８いずれかに記載の認証装置と、
前記解錠部により解錠される電気錠と、
前記報知部による報知に用いられる報知装置と
を備えたことを特徴とするセキュリティシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、例えば、不正入室を検出する認証装置およびセキュリティシステムに関するものである。
【背景技術】
【０００２】
特許文献１には、脅迫などの不正な状況に置かれている場合の入室時に認証端末装置に特別な操作を行うことで通報できるようにする方法が開示されている。
【０００３】
しかし、入室するために認証端末装置に正規の操作をして扉を解錠し、開けられた扉が閉じて施錠するまでの間に不審者に侵入された場合、通報することはできない。これは、複数人の入室を検出して通報する共連れ検知のシステムで防ぐことが可能である。但し、入室人数を検出するためにカメラが必要であるため、共連れ検知システムは高価である。
【特許文献１】特開平６－１７５６５号公報
【発明の開示】
【発明が解決しようとする課題】
【０００４】
本発明は、例えば、扉が施錠するまでの間に不審者に侵入された場合に通報を行うセキュリティシステムを安価に構築できるようにすることを目的とする。
【課題を解決するための手段】
【０００５】
本発明の認証装置は、電気錠により施錠された部屋への入室を承認する認証装置であり、前記部屋の外側に設けられる第１の認証端末装置に所定の第１のデータが入力されたかＣＰＵを用いて判定する第１の認証部と、前記第１の認証部により所定の第１のデータが入力されたと判定された場合、前記電気錠を解錠する解錠部と、前記解錠部により前記電気錠が解錠されてからの所定時間の経過をＣＰＵを用いて検出するタイマー部と、前記部屋の内側に設けられる第２の認証端末装置に所定の第２のデータが入力されたかＣＰＵを用いて判定する第２の認証部と、前記第２の認証部により所定の第２のデータが入力されたと判定される前に前記タイマー部により所定時間の経過が検出された場合、入室の非承認を所定の装置を用いて報知する報知部とを備える。
【発明の効果】
【０００６】
本発明によれば、例えば、扉が閉じて施錠するまでの間に不審者に侵入された場合でも通報を行うことができる。また、カメラおよび共連れ検知システムが不要なため、セキュリティシステムを安価に構築できる。
【発明を実施するための最良の形態】
【０００７】
実施の形態１．
電気錠により施錠された部屋（建物）への入室（入館）を承認する認証装置およびセキュリティシステムについて説明する。
【０００８】

図１は、実施の形態１におけるセキュリティシステム９００の構成図である。
実施の形態１におけるセキュリティシステム９００の構成について、図１に基づいて以下に説明する。

【０００９】

セキュリティシステム９００は、コントローラ１００（認証装置）、入側認証端末装置２００（第１の認証端末装置）、出側認証端末装置２１０（第２の認証端末装置）、ドア２２０およびセンター装置２３０（報知装置）を有する。
コントローラ１００は、入側認証端末装置２００、出側認証端末装置２１０およびセンター装置２３０と通信ケーブルや通信回線を介して接続する。

【００１０】

部屋のドア２２０は、電気錠２２１により施錠される。

【００１１】

入側認証端末装置２００は、カードリーダ２０１を備え、部屋の外側のドア脇に設置される。
カードリーダ２０１は、特定の人を識別するＩＤ（識別データの一例）が予め記録されているＩＤカードからＩＤを読み取る装置である。例えば、カードリーダ２０１は、ＲＦＩＤ（Ｒａｄｉｏ　Ｆｒｅｑｕｅｎｃｙ　Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ）の通信方式により、ＩＤカードからＩＤを読み取る。
入側認証端末装置２００は、カードリーダ２０１により読み取られたＩＤ（以下、「読取ＩＤ２０１ａ」という）をコントローラ１００に出力する。

【００１２】

出側認証端末装置２１０は、指紋読取装置２１１を備え、部屋の内側のドア脇に設置される。
指紋読取装置２１１は、利用者の指から指紋情報（識別データの一例）を読み取る装置である。
出側認証端末装置２１０は、指紋読取装置２１１により読み取られた指紋情報（以下、「読取指紋情報２１１ａ」という）をコントローラ１００に出力する。
指紋読取装置２１１は利用者から生体情報を読み取る装置の一例である。出側認証端末装置２１０は、指紋読取装置２１１の代わりに、利用者の顔画像を撮像する装置や眼から虹彩情報を読み取る装置などを備えても構わない。

【００１３】

コントローラ１００は、第１の認証部１１０、第２の認証部１２０、解錠部１３０、タイマー部１４０、報知部１５０および認証装置記憶部１９０を備える。
コントローラ１００は、入側認証端末装置２００から出力された読取ＩＤ２０１ａと出側認証端末装置２１０から出力された読取指紋情報２１１ａとに基づいて、利用者の入室を承認するか否かを決定する。第１の認証部１１０により読取ＩＤ２０１ａに基づいて「認証許可」されてから所定の時間内に第２の認証部１２０により読取指紋情報２１１ａに基づいて「認証許可」された場合、コントローラ１００は利用者の入室を承認する。第１の認証部１１０により読取ＩＤ２０１ａに基づいて「認証許可」されてから所定の時間内に第２の認証部１２０により読取指紋情報２１１ａに基づいて「認証許可」されなかった場合、コントローラ１００は利用者の入室を承認しない（非承認）。

【００１４】

第１の認証部１１０は、入側認証端末装置２００から出力された読取ＩＤ２０１ａを登録ＩＤ１９１（所定の第１のデータ）と照合して第１の認証処理を行う。
以下、読取ＩＤ２０１ａと一致する登録ＩＤ１９１が有る場合の第１の認証処理の結果を「認証許可」、読取ＩＤ２０１ａと一致する登録ＩＤ１９１が無い場合の第１の認証処理の結果を「認証不許可」とする。

【００１５】

第２の認証部１２０は、出側認証端末装置２１０から出力された読取指紋情報２１１ａを登録指紋情報１９２（所定の第２のデータ）と照合して第２の認証処理を行う。

以下、読取指紋情報２１１ａと一致する登録指紋情報１９２が有る場合の第２の認証処理の結果を「認証許可」、読取指紋情報２１１ａと一致する登録指紋情報１９２が無い場合の第２の認証処理の結果を「認証不許可」とする。

【００１６】

解錠部１３０は、第１の認証処理の結果が「認証許可」の場合、ドア２２０の電気錠２２１を解錠する。

解錠部１３０は、第１の認証処理の結果が「認証不許可」の場合、ドア２２０の電気錠２２１を解錠しない。

【００１７】

タイマー部１４０は、解錠部１３０により電気錠２２１が解錠されてから所定時間の経過を検出する。

【００１８】

報知部１５０は、第２の認証処理の結果が「認証許可」になる前にタイマー部１４０により所定時間の経過が検出された場合、利用者の入室を非承認とし、不正入室が起きたことを通知する警報通知１５１をセンター装置２３０に送信する。

報知部１５０は、タイマー部１４０により所定時間の経過が検出される前に第２の認証処理の結果が「認証許可」になった場合、利用者の入室を承認し、警報通知１５１をセンター装置２３０に送信しない。

【００１９】

認証装置記憶部１９０は、コントローラ１００で使用されるデータ（例えば、登録ＩＤ１９１、登録指紋情報１９２、タイムアウト値１９３）を記憶媒体を用いて記憶する。

登録ＩＤ１９１は、入室を認められた者に割り当てられたＩＤであり、認証装置記憶部１９０に予め登録（記憶）される。

登録指紋情報１９２は、入室を認められた者から取得された指紋情報であり、認証装置記憶部１９０に予め登録される。

タイムアウト値１９３は、タイマー部１４０により検出される所定時間を示し、認証装置記憶部１９０に予め記憶される。

【００２０】

センター装置２３０は、管理者が駐在する管理センターに設置される。

センター装置２３０は、コントローラ１００から警報通知１５１が送信された場合、警報通知１５１を出力装置（例えば、ディスプレイ、スピーカー、プリンタ）に出力して管理者に不正入室を知らせる。

【００２１】

コントローラ１００は、ＣＰＵ（中央処理装置）、ＲＯＭ、ＲＡＭを備える（図示省略）。ＣＰＵは、バスを介してＲＯＭ、ＲＡＭと接続され、これらを制御する。

ＲＯＭやＲＡＭには、実施の形態において「～部」として説明する機能を実行するプログラム、「～部」で使用されるデータが記憶される。

実施の形態において「～部」として説明するものは、「～回路」、「～装置」、「～機器」であってもよく、また、「～ステップ」、「～手順」、「～処理」であってもよい。すなわち、「～部」として説明するものは、ハードウェア、プログラム、ハードウェアとプログラムとの組み合わせのいずれで実現されても構わない。

プログラムはＣＰＵにより読み出され、ＣＰＵにより実行される。プログラムは、「～部」としてコンピュータを機能させるものであり、「～部」の手順や方法をコンピュータに実行させるものである。

【００２２】

図２は、実施の形態１におけるコントローラ１００の認証方法を示すフローチャートである。

実施の形態１におけるコントローラ１００の認証方法について、図２に基づいて以下に説明する。

コントローラ１００の各「～部」は、以下の処理をＣＰＵを用いて実行する。

【００２３】
コントローラ１００の認証方法を説明する前に、利用者の動作について説明する。
利用者は、入室の承認を受けるために、入室前に部屋外で第１の認証（ＩＤ認証）により認証許可を受け、入室後の所定時間内に部屋内で第２の認証（指紋認証）により認証許可を受ける。
利用者は、第１の認証（ＩＤ認証）を受けるために、ドア２２０の脇に設置されている入側認証端末装置２００のカードリーダ２０１にＩＤカードを近づけて、入側認証端末装置２００にＩＤを入力する。カードリーダ２０１はＩＤカードからＩＤを読み取り、入側認証端末装置２００はカードリーダ２０１により読み取ったＩＤ（読取ＩＤ２０１ａ）をコントローラ１００に出力する。コントローラ１００の第１の認証部１１０は入側認証端末装置２００から出力された読取ＩＤ２０１ａを入力する。
利用者は、第２の認証（指紋認証）を受けるために、部屋内に設置されている出側認証端末装置２１０の指紋読取装置２１１に指をセットして、出側認証端末装置２１０に指紋情報を入力する。指紋読取装置２１１は指から指紋情報を読み取り、出側認証端末装置２１０は指紋読取装置２１１により読み取った指紋情報（読取指紋情報２１１ａ）をコントローラ１００に出力する。コントローラ１００の第２の認証部１２０は出側認証端末装置２１０から出力された読取指紋情報２１１ａを入力する。
【００２４】
コントローラ１００の認証方法の概要について説明する。
第１の認証部１１０は、読取ＩＤ２０１ａを入力した場合（Ｓ１１０）、読取ＩＤ２０１ａを登録ＩＤ１９１と照合し（Ｓ１１１）、認証許可するか判定する（Ｓ１１２）。
第１の認証部１１０が認証許可した場合、解錠部１３０は電気錠２２１を解錠し（Ｓ１２０）、タイマー部１４０はタイマーをセットする（Ｓ１３０）。
第２の認証部１２０は、読取指紋情報２１１ａを入力した場合（Ｓ１４０）、読取指紋情報２１１ａを登録指紋情報１９２と照合し（Ｓ１４１）、認証許可するか判定する（Ｓ１４２）。
第２の認証部１２０により認証許可される前にタイムアウトした場合（Ｓ１５０）、報知部１５０はセンター装置２３０に警報通知１５１を送信する（Ｓ１５１）。
【００２５】
次に、各処理（Ｓ１１０～Ｓ１５１）の詳細について説明する。
【００２６】
利用者は、第１の認証（Ｓ１１０～Ｓ１１２）を受けるために、ドア２２０の脇に設置されている入側認証端末装置２００のカードリーダ２０１にＩＤカードを近づけて、入側認証端末装置２００にＩＤを入力する。カードリーダ２０１はＩＤカードからＩＤを読み取り、入側認証端末装置２００はカードリーダ２０１により読み取ったＩＤ（２０１ａ）をコントローラ１００に出力する。コントローラ１００の第１の認証部１１０は入側認証端末装置２００から出力された読取ＩＤ２０１ａを入力する。
【００２７】
＜Ｓ１１０＞
第１の認証部１１０は、読取ＩＤ２０１ａの入力を待つ。
読取ＩＤ２０１ａを入力した場合（ＹＥＳ）、処理はＳ１１１に進む。
【００２８】
＜Ｓ１１１＞
Ｓ１１０において読取ＩＤ２０１ａを入力した場合（ＹＥＳ）、第１の認証部１１０は、入力した読取ＩＤ２０１ａを各登録ＩＤ１９１と照合する。登録ＩＤ１９１は、入室が認められている人毎に認証装置記憶部１９０に予め記憶されている。
Ｓ１１１の後、処理はＳ１１２に進む。
【００２９】
＜Ｓ１１２＞
Ｓ１１１において読取ＩＤ２０１ａを登録ＩＤ１９１と照合した後、第１の認証部１１

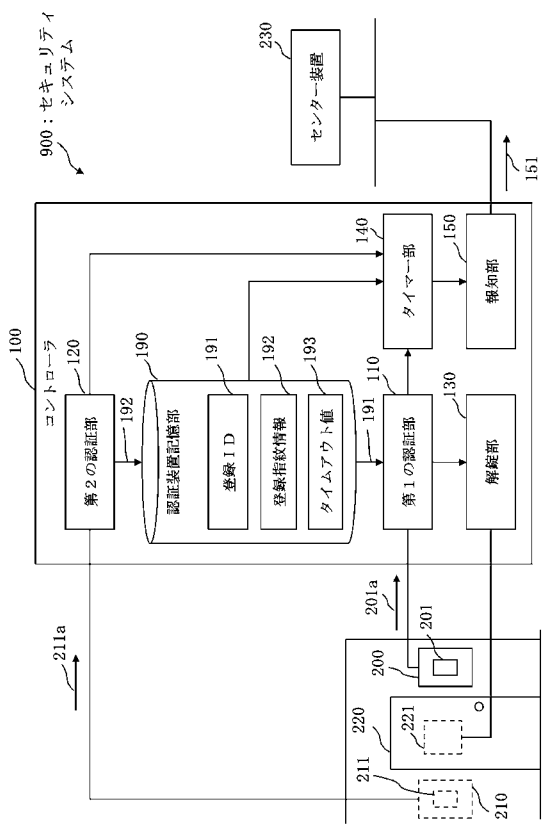
０は、照合結果に基づいて、読取ＩＤ２０１ａと一致する登録ＩＤ１９１が有るか否かを判定する。
読取ＩＤ２０１ａと一致する登録ＩＤ１９１が有る場合、第１の認証の結果は「認証許可」であり、読取ＩＤ２０１ａと一致する登録ＩＤ１９１が無い場合、第１の認証の結果は「認証不許可」である。
第１の認証の結果が「認証不許可」の場合、第１の認証部１１０は入側認証端末装置２００に「認証不許可」の表示を命令し、命令を受けた入側認証端末装置２００はディスプレイ（図示省略）に「認証不許可」になったことを表示して利用者にＩＤの再入力を促す。
第１の認証の結果が「認証許可」の場合（ＹＥＳ）、処理はＳ１２０に進み、第１の認証の結果が「認証不許可」の場合（ＮＯ）、処理はＳ１１０に戻る。
【００３０】
＜Ｓ１２０＞
Ｓ１１２において第１の認証の結果が「認証許可」の場合（ＹＥＳ）、解錠部１３０は、ドア２２０の電気錠２２１を制御して解錠する。
電気錠２２１が解錠されることにより、利用者はドア２２０から入室することができる。
Ｓ１２０の後、処理はＳ１３０に進む。
【００３１】
＜Ｓ１３０＞
Ｓ１２０において電気錠２２１が解錠された後、タイマー部１４０は、所定時間の経過を検出するタイマーをセットする。タイマーにより検出される所定時間（３分、１０分など）は、タイムアウト値１９３として認証装置記憶部１９０に予め記憶されている。
Ｓ１３０の後、処理はＳ１４０に進む。
【００３２】
利用者は、第２の認証（指紋認証）（Ｓ１４０～Ｓ１４２）を受けるために、部屋内に設置されている出側認証端末装置２１０の指紋読取装置２１１に指をセットして、出側認証端末装置２１０に指紋情報を入力する。指紋読取装置２１１は指から指紋情報を読み取り、出側認証端末装置２１０は指紋読取装置２１１により読み取った指紋情報（読取指紋情報２１１ａ）をコントローラ１００に出力する。コントローラ１００の第２の認証部１２０は出側認証端末装置２１０から出力された読取指紋情報２１１ａを入力する。
【００３３】
＜Ｓ１４０＞
第２の認証部１２０は、読取指紋情報２１１ａを入力したか判定する。
読取指紋情報２１１ａを入力した場合（ＹＥＳ）、処理はＳ１４１に進み、読取指紋情報２１１ａを入力していない場合（ＮＯ）、処理はＳ１５０に進む。
【００３４】
＜Ｓ１４１＞
Ｓ１４０において読取指紋情報２１１ａを入力した場合（ＹＥＳ）、第２の認証部１２０は、入力した読取指紋情報２１１ａを登録指紋情報１９２と照合し、読取指紋情報２１１ａと一致する登録指紋情報１９２を検索する。登録指紋情報１９２は、入室が認められている人毎に認証装置記憶部１９０に予め記憶されている。
Ｓ１４１の後、処理はＳ１４２に進む。
【００３５】
＜Ｓ１４２＞
Ｓ１４１において読取指紋情報２１１ａを登録指紋情報１９２と照合した後、第２の認証部１２０は、照合結果に基づいて、読取指紋情報２１１ａと一致する登録指紋情報１９２が有るか否かを判定する。
読取指紋情報２１１ａと一致する登録指紋情報１９２が有る場合、第２の認証の結果は「認証許可」であり、読取指紋情報２１１ａと一致する登録ＩＤ１９１が無い場合、第２

の認証の結果は「認証不許可」である。
　第２の認証の結果が「認証不許可」の場合、第２の認証部１２０は出側認証端末装置２１０に「認証不許可」の表示を命令し、命令を受けた出側認証端末装置２１０はディスプレイ（図示省略）に「認証不許可」になったことを表示して利用者に指紋情報の再入力を促す。
　第２の認証の結果が「認証許可」の場合（ＹＥＳ）、処理は終了し、第２の認証の結果が「認証不許可」の場合（ＮＯ）、処理はＳ１５０に進む。
【００３６】
＜Ｓ１５０＞
　Ｓ１４０において読取指紋情報２１１ａを入力していない場合（ＮＯ）またはＳ１４２において第２の認証の結果が「認証不許可」の場合（ＮＯ）、タイマー部１４０は、Ｓ１３０においてセットしたタイマーがタイムアウトしたか判定する。タイムアウトは、電気錠２２１が解錠されてから所定時間が経過したことを意味する。
　タイムアウトした場合（ＹＥＳ）、処理はＳ１５１に進み、タイムアウトしていない場合（ＮＯ）、処理はＳ１４０に戻る。
【００３７】
＜Ｓ１５１＞
　Ｓ１５０においてタイムアウトした場合（ＹＥＳ）、報知部１５０は、Ｓ１２０での電気錠２２１の解錠を不正入室と判断し、不正入室があったことを通知する警報通知１５１をセンター装置２３０に送信する。
　不正入室とは、何らかの理由により、入室している人が入室の承認を受けていないこと（入室の非承認）を意味する。
　センター装置２３０は、報知部１５０から警報通知１５１を受信した場合、警報通知１５１を出力装置（例えば、ディスプレイ、スピーカー、プリンタ）に出力して不正入室を管理者に知らせる。
　また、報知部１５０は、警報器（図示省略）を鳴動させて不正入室があったことを報知しても構わない。
　Ｓ１５１の後、処理は終了する。
【００３８】
　Ｓ１１０～Ｓ１５１により、コントローラ１００は、利用者の入室を管理すると共に不正入室を検出して通報することができる。
【００３９】
　実施の形態１では、以下のようなセキュリティシステム９００について説明した。
　扉の入側と出側に認証端末を設置し、入側認証端末で認証後、一定時間内に出側認証端末で認証を行わないと正常な操作と判断せず警報を通知する。
　セキュリティシステム９００は、以下のような不審者対策効果を奏する。
１）利用者は、入室時に不審者に気付いた場合、出側認証端末で認証を行わないことで警報を通知することができる。
２）入側認証端末の認証方法がカード認証である場合、不審者は、カードを拾ったり盗んだりして不正取得すれば入室が可能となる。しかし、セキュリティシステム９００は、出側認証端末の認証方法が指紋、顔認証などの生体認証であることにより、不審者を出側で認証ＮＧとし、警報を通知することができる。
３）利用者は、入側で認証を強要された場合、入側認証端末で認証後に出側の認証を行わないことで警報を通知することができる。
　セキュリティシステム９００は、以下のように正確な入室を判断できる。
４）利用者の認証端末操作を正常な操作（第１の認証許可＋一定時間内の第２の認証許可）と判断した後で入室を正常なものとして扱うことで、より正確に入室を判断できる。
５）入側認証端末にＲＦＩＤを使用して複雑な認証操作を行うことなく利用者を自動判別することで、利用者に通行を簡易かつ確実に行わせることができる。
【００４０】

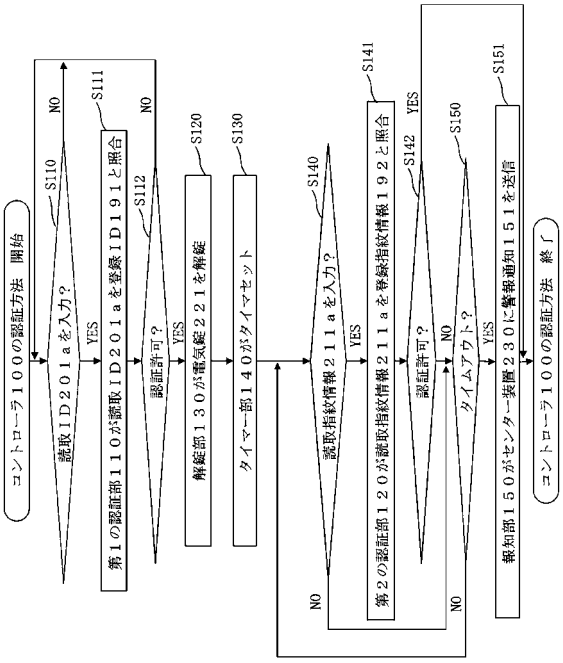
セキュリティシステム９００は、以下の特徴を有する。
入側認証端末装置２００に入力されるデータ（ＩＤ）と出側認証端末装置２１０に入力されるデータ（指紋情報）とが異なる種類のデータである。
これにより、異なる複数の認証処理が行われ、セキュリティ性が高まる。例えば、不正に取得されたＩＤカードが用いられＩＤ認証が認証許可になっても、指紋認証では認証不許可となるため、不正入室を通報することができる。
【００４１】
入側認証端末装置２００に入力されるデータ（ＩＤ）は、出側認証端末装置２１０に入力されるデータ（指紋情報）より入力に要する時間が短い種類のデータである。
また、入側認証端末装置２００に入力されるデータは、出側認証端末装置２１０に入力されるデータより一致判定（照合）に要する時間が短い種類のデータである。
これにより、利用者の入室を円滑にし、利便性の低下を抑えると共に利用者の安全性を高めることができる。例えば、利用者が入側認証端末装置２００で認証を受けている間に不審者に襲われる、ということを防ぐことができる。
【００４２】
出側認証端末装置２１０に入力される識別データ（指紋情報）は、識別データの入力者と識別データにより識別される特定者との一致を保証する信頼度が入側認証端末装置２００に入力される識別データ（ＩＤ）より高い種類のデータである。
これにより、入室の承認結果の信頼度が高まり、セキュリティ性が向上する。
【００４３】
入側認証端末装置２００に入力されるデータと出側認証端末装置２１０に入力されるデータとの組み合わせは、ＩＤと指紋情報との組み合わせに限らない。例えば、ＩＤとパスワードとの組み合わせ、指紋情報と虹彩情報との組み合わせ、第１パスワード（数字のみ）と第２パスワード（英数字＋記号）との組み合わせでも構わない。
【００４４】
実施の形態２．
認証端末装置に特定の操作がされた場合に通報を行う形態について説明する。
以下、実施の形態１と異なる事項について主に説明し、説明を省略する事項は実施の形態１と同様であるものとする。
【００４５】
実施の形態２におけるセキュリティシステム９００の構成は、実施の形態１と同じである。
【００４６】
図３は、実施の形態２におけるコントローラ１００の認証方法を示すフローチャートである。
実施の形態２におけるコントローラ１００の認証方法について、図３に基づいて以下に説明する。
【００４７】
図３に示すフローチャートは、実施の形態１のフローチャート（図２参照）にＳ１６０およびＳ１６１が加わったものである。
以下、Ｓ１６０およびＳ１６１について説明する。
【００４８】
＜Ｓ１６０＞
Ｓ１２０において電気錠２２１が解錠されると共にＳ１３０においてタイマーがセットされた後、第２の認証部１２０は、出側認証端末装置２１０に特定の操作がされたか判定する。
特定の操作として、特定のボタン（図示省略）の押下、特定指の指紋情報の入力などが挙げられる。
例えば、出側認証端末装置２１０は特定のボタンが押下された場合に第２の認証部１２０へ特定の操作を通知し、第２の認証部１２０は出側認証端末装置２１０から通知を受け

た場合に特定の操作がされたと判定する。
　また例えば、利用者は、第２の認証（指紋認証）の認証許可を受けたい場合、人差し指を指紋読取装置２１１にセットし、通報したい場合、中指を指紋読取装置２１１にセットする。認証装置記憶部１９０には人差し指の登録指紋情報１９２と中指の登録指紋情報１９２とが予め記憶され、第２の認証部１２０は読取指紋情報２１１ａが中指の登録指紋情報１９２と一致した場合に特定の操作がされたと判定する。
　特定の操作がされた場合（ＹＥＳ）、処理はＳ１６１に進み、特定の操作がされていない場合（ＮＯ）、処理はＳ１４０に進む。
【００４９】
＜Ｓ１６１＞
　Ｓ１６０において特定の操作がされた場合（ＹＥＳ）、報知部１５０は、Ｓ１５１と同じく、警報通知１５１をセンター装置２３０に送信する。
　Ｓ１６１の後、処理は終了する。
【００５０】
　実施の形態２により、セキュリティ性をさらに向上させることができる。
　例えば、利用者は、入側と出側との両方の認証を強要された場合、出側認証端末装置２１０に特別な操作を行うことで警報を通知することができる。
【００５１】
　第２の認証部１２０と同様、第１の認証部１１０は、入側認証端末装置２００に特定の操作がされた場合に警報通知１５１をセンター装置２３０に送信しても構わない。
【図面の簡単な説明】
【００５２】
【図１】実施の形態１におけるセキュリティシステム９００の構成図。
【図２】実施の形態１におけるコントローラ１００の認証方法を示すフローチャート。
【図３】実施の形態２におけるコントローラ１００の認証方法を示すフローチャート。
【符号の説明】
【００５３】
　１００　コントローラ、１１０　第１の認証部、１２０　第２の認証部、１３０　解錠部、１４０　タイマー部、１５０　報知部、１５１　警報通知、１９０　認証装置記憶部、１９１　登録ＩＤ、１９２　登録指紋情報、１９３　タイムアウト値、２００　入側認証端末装置、２０１　カードリーダ、２０１ａ　読取ＩＤ、２１０　出側認証端末装置、２１１　指紋読取装置、２１１ａ　読取指紋情報、２２０　ドア、２２１　電気錠、２３０　センター装置、９００　セキュリティシステム。

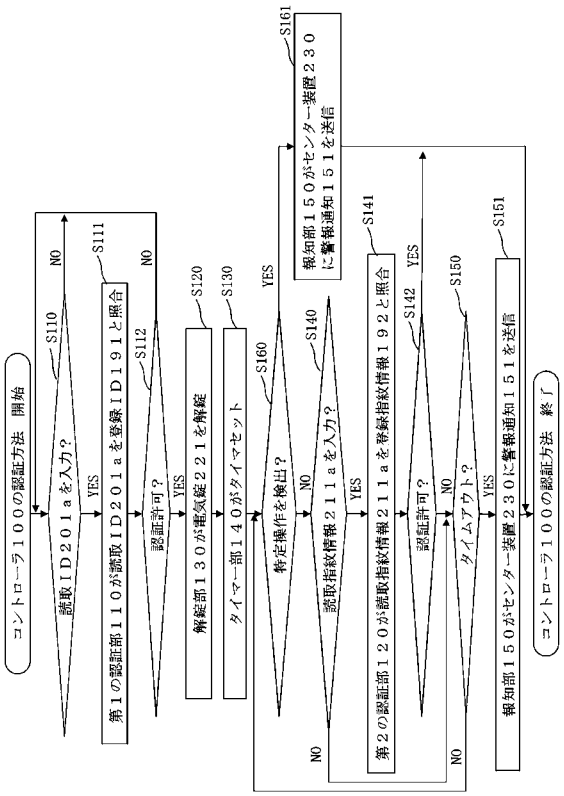
【図１】


900：セキュリティシステム
コントローラ
100
第２の認証部
120
192
認証装置記憶部
190
登録ＩＤ
191
登録指紋情報
192
タイムアウト値
193
第１の認証部
110
191
タイマー部
140
150
報知部
130
解錠部
161
センター装置
230
211a
201a
201
200
220
221
211
210

【図２】


コントローラ１００の認証方法　開始
読取ＩＤ２０１ａを入力？
S110
NO
YES
第１の認証部１１０が読取ＩＤ２０１ａを登録ＩＤ１９１と照合
S111
NO
認証許可？
S112
YES
解錠部１３０が電気錠２２１を解錠
S120
タイマー部１４０がタイマセット
S130
読取指紋情報２１１ａを入力？
S140
NO
YES
第２の認証部１２０が読取指紋情報２１１ａを登録指紋情報１９２と照合
S141
NO
認証許可？
S142
YES
タイムアウト？
S150
NO
YES
報知部１５０がセンター装置２３０に警報通知１５１を送信
S151
コントローラ１００の認証方法　終了

【図３】


コントローラ１００の認証方法　開始
読取ＩＤ２０１ａを入力？
S110
NO
YES
第１の認証部１１０が読取ＩＤ２０１ａを登録ＩＤ１９１と照合
S111
NO
認証許可？
S112
YES
解錠部１３０が電気錠２２１を解錠
S120
タイマー部１４０がタイマセット
S130
特定操作を検出？
S160
NO
YES
報知部１５０がセンター装置２３０に警報通知１５１を送信
S161
読取指紋情報２１１ａを入力？
S140
NO
YES
第２の認証部１２０が読取指紋情報２１１ａを登録指紋情報１９２と照合
S141
NO
認証許可？
S142
YES
タイムアウト？
S150
NO
YES
報知部１５０がセンター装置２３０に警報通知１５１を送信
S161
コントローラ１００の認証方法　終了

フロントページの続き

(51)Int.Cl.	F I		テーマコード（参考）
	Ｇ０８Ｂ 25/04	G	
	Ｇ０８Ｂ 25/08	A	

Ｆターム(参考) 2E250 AA02 AA03 AA12 BB05 BB08 BB09 BB10 BB15 BB22 CC13
CC14 CC28 DD01 DD06 DD08 DD09 EE03 FF05 FF06 FF08
FF13 FF18 FF28 FF44
3E038 AA01 BB01 HA07
5C087 AA02 BB11 BB20 BB74 DD06 DD20 EE07 FF01 FF02 FF04
FF16 FF25 GG02 GG08 GG19 GG40