

(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2014-105437
(P2014-105437A)

(43) 公開日 平成26年6月9日(2014.6.9)

(51) Int.Cl.
E05B 49/00 (2006.01)

F I
E O 5 B 49/00

テーマコード (参考)
2 E 2 5 O

審査請求 未請求 請求項の数 7 O L (全 22 頁)

(21) 出願番号 特願2012-257031 (P2012-257031)
(22) 出願日 平成24年11月26日 (2012.11.26)

(71) 出願人 000005108
株式会社日立製作所
東京都千代田区丸の内一丁目6番6号
(74) 代理人 100100310
弁理士 井上 学
(74) 代理人 100098660
弁理士 戸田 裕二
(74) 代理人 100091720
弁理士 岩崎 重美
(72) 発明者 嶋野 和樹
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

最終頁に続く

(54) 【発明の名称】 入退室管理システムおよびそのプログラム

(57) 【要約】

【課題】

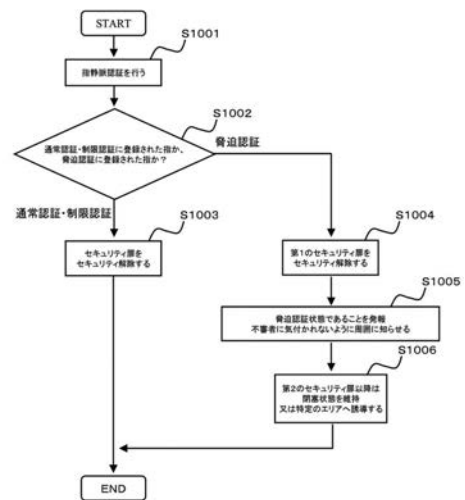
利用者の利便性を実現するとともに、セキュリティレベルに応じたエリアへ容易に入室することが可能な入退室管理システムを提供することを目的とする。

【解決手段】

複数の管理区域を有する入退室管理システムにおいて、管理区域に入室する入室者の生体情報を読み取り、生体情報と予め登録された生体情報とに基づいて入室者の認証を行い、認証結果に基づいてセキュリティの解除又は非解除の制御を行うセキュリティ制御装置を有し、セキュリティ制御装置は、入室者を特定する生体情報として複数の生体情報を使用し、認証が行われた生体情報毎に、セキュリティの解除が行われる管理区域のエリアが異なることを特徴とする。

【選択図】 図10

【図10】



【特許請求の範囲】**【請求項 1】**

複数の管理区域を有する入退室管理システムにおいて、

前記管理区域に入室する入室者の生体情報を読み取り、前記生体情報と予め登録された生体情報とに基づいて前記入室者の認証を行い、認証結果に基づいてセキュリティの解除又は非解除の制御を行うセキュリティ制御装置を有し、

前記セキュリティ制御装置は、前記入室者を特定する生体情報として複数の生体情報を使用し、前記認証が行われた生体情報毎に、前記セキュリティの解除が行われる管理区域のエリアが異なることを特徴とする入退室管理システム。

【請求項 2】

請求項 1 に記載の入退室管理システムにおいて、

前記複数の生体情報のうち、第一の生体情報に基づいて認証を行った場合には、前記入室者が脅迫状態にある脅迫認証状態であると判定し、前記脅迫認証状態では、前記入室者の安全が確保されるエリアに入室可能となるようにセキュリティ解除を行うことを特徴とする入退室管理システム。

【請求項 3】

請求項 2 に記載の入退室管理システムにおいて、

前記脅迫認証状態であると判定される場合には、脅迫認証が行われた領域における画像データを取得することを特徴とする入退室管理システム。

【請求項 4】

請求項 2 又は 3 に記載の入退室管理システムにおいて、

前記脅迫認証状態であると判定される場合には、警報を発報することを特徴とする入退室管理システム。

【請求項 5】

請求項 1 ~ 4 に記載の入退室管理システムにおいて、

前記生体認証装置は、指静脈認証装置であることを特徴とする入退室管理システム。

【請求項 6】

請求項 5 に記載の入退室管理システムにおいて、

前記複数の生体情報は、前記入室者の指毎の静脈パターンであることを特徴とする入退室管理システム。

【請求項 7】

請求項 1 から請求項 6 の何れかの入退室管理システムをコンピュータに実現させるためのプログラム。

【発明の詳細な説明】**【技術分野】****【0001】**

本発明は、生体認証を用いた入退室管理システムおよびそのプログラムに関する。

【背景技術】**【0002】**

入退室管理システムは、オフィスビル等を中心にセキュリティ強化と利便性を目的とし標準的に導入される設備になりつつある。

【0003】

本技術分野の背景技術として、特開 2010 - 15320 号公報（特許文献 1）がある。この公報には、「不正入室を制限でき、より高いセキュリティレベルを有するとともに、入室者別にきめ細かな入室管理を行い得るセキュリティシステムおよびそのプログラムを提供する」ために、「本発明のセキュリティシステムは、建物を含む管理区域の入室を管理するセキュリティシステムであって、入室に際して入室者がかざす非接触式認証媒体の認証媒体識別情報を読み取るリーダと、入室に際して入室者の生体情報を読み取る生体認証装置と、リーダおよび生体認証装置に接続され、リーダで読み取った認証媒体識別情報と生体認証装置で読み取った生体情報とに基づいて入室の可否の認証を行い、セキュリテ

10

20

30

40

50

ィの解除または非解除の制御を行うセキュリティ制御装置とを備えている。」と記載されている（要約参照）。

【先行技術文献】

【特許文献】

【0004】

【特許文献1】特開2010-15320号公報

【発明の概要】

【発明が解決しようとする課題】

【0005】

上記特許文献1には、入室者別にきめ細かな入室管理を行い得るセキュリティシステムおよびそのプログラムを提供する仕組みが記載されており、具体的には、入室者の建物への入館に際し、入室するセキュリティレベルに応じて、入室認証方法を変化させるものである。例えば、セキュリティレベルが比較的低いエリアのセキュリティ解除においては、認証のうち生体認証のみを行い、一方、セキュリティレベルが比較的高いエリアのセキュリティ解除においては、認証のうち生体認証および非接触式認証媒体を読み取るリーダの認証を行う必要がある。

10

【0006】

しかしながら、入室するセキュリティレベルを考慮して入室認証方法を変更することに関する開示はあるものの、入室者がセキュリティレベルの比較的高いエリアへ入室するためには、別途非接触式認証媒体と非接触式認証媒体を読み取るリーダが必要となる課題がある。

20

【0007】

そこで、本発明は、利用者の利便性を実現するとともに、セキュリティレベルに応じたエリアへ容易に入室することが可能な入退室管理システムを提供することを目的とする。

【課題を解決するための手段】

【0008】

上記課題を解決するために、本発明は、複数の管理区域を有する入退室管理システムにおいて、管理区域に入室するに際して入室者の生体情報を読み取る生体認証装置に基づいて入室の可否の認証を行い、セキュリティの解除または非解除の制御を行うセキュリティ制御装置を有し、生体認証装置においては、入室者の指の生体情報に基づいて認証を行い、指毎にセキュリティの解除が行われる管理区域のエリアの大きさが異なることを特徴とする。

30

【発明の効果】

【0009】

本発明によれば、利用者の利便性を実現するとともに、生体認証操作時に認証操作を行う指によって、容易にそれぞれのセキュリティレベルに応じたエリアのセキュリティ解除を行うことが可能な入退室管理システムを提供することができる。上記した以外の課題、構成および効果は、以下の実施形態の説明により明らかにされる。

【図面の簡単な説明】

【0010】

40

【図1】本発明に係わる第1の実施形態の入退室管理システム全体の概要構成図である。

【図2】第1の実施形態における入退室管理システムのシステム構成図である。

【図3】第1のセキュリティ扉1における入退室管理システムの入退室管理制御の流れを示すフローチャートである。

【図4】入室者が事前に特定されていない場合において、登録された静脈データとの照合方法を示すフローチャートである。

【図5】入室者が事前に特定されている場合において、登録された静脈データとの照合方法を示すフローチャートである。

【図6】本発明に係わる第2の実施形態の入退室管理システム全体の概要構成図である。

【図7】第1のセキュリティ扉1における通常認証又は制限認証時における入退室管理シ

50

システムの入退室管理制御の流れを示すフローチャートである。

【図 8】指毎の、認証の対応状態、入室可能エリア数、及び入室可能エリアの対応を示した表である。

【図 9】脅迫認証時の入室可能エリア例である。

【図 10】指静脈認証を行う指によってセキュリティ解除されるパターンが異なる場合のフローチャートである。

【図 11】脅迫モード時の特定エリアへの誘導例である。

【発明を実施するための形態】

【実施例 1】

【0011】

10

本発明を実施するための形態（以降、「実施例 1」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。

【0012】

<入退室管理システムの概要>

図 1 は、実施例 1 の入退室管理システム全体の概要構成図である。

実施例 1 に係わる入退室管理システムは、ビルや工場、店舗、マンション等の建物の入退室を行う際に、特定の認証操作を行い、認証可とみなされた場合のみセキュリティを解除し、入館及び退館することを許可し、認証不可の場合は入館及び退館することを許可しないシステムである。

【0013】

20

<入退室管理システムの全体構成>

実施例 1 の入退室管理システムは、第 1 のセキュリティ扉 1 と第 2 以降のセキュリティ扉 2 を備えた入退室管理システムであり、入室者 10 が第 1 のセキュリティ扉 1 を通過するためには、扉近傍にある指静脈認証装置 11 で認証操作を行う必要がある。ここでは、指静脈認証装置 11 を例に出しているが、掌や指紋などその他個人を特定することが可能な生体認証装置であれば何でも良い。

【0014】

これらの指静脈認証装置 11 などの生体認証装置の情報を収集し、第 1 のセキュリティ扉 1 となる自動ドアや電気錠、ゲート等からなる制御端末 1 t や、第 2 以降のセキュリティ扉となる自動ドアや電気錠、ゲート、エレベータ等からなる制御端末 2 t の施解錠制御する制御盤 20（後述）が、入退室管理システムに備えられている。

30

【0015】

以下、入退室管理システムの各部の構成について説明する。

【0016】

<指静脈認証装置 11>

生体認証装置の一例として用いられる指静脈認証装置 11 は、例えば、近赤外線を指に透過させて得られる静脈パターンの画像から静脈の部分から鮮明な静脈パターンとして検出する装置を採用する。指静脈認証装置 11 は、予め登録された静脈パターンと、図 1 に示す第 1 のセキュリティ扉 1 のセキュリティ解除を行うための指静脈認証装置 11 で検出した入室者 10 の静脈パターンとを照合して個人の認証を行う装置である。

40

【0017】

指静脈認証装置 11 は、その認証可否の結果のみを、例えば、認証可は「1」、認証否は「0」のデジタル信号と、認証可の場合には認証された指静脈パターンに対応する個人情報とを制御盤 20 に送信する。

【0018】

予め登録された静脈パターンは、個人を特定するための ID や番号などとともに、指静脈認証装置 11 に搭載された RAM（Random Access Memory）などの記憶媒体に格納されている。

【0019】

ここで、認証に用いる予め登録される静脈パターンは、予め建屋内への入室を許可する

50

個人の静脈パターンを指静脈認証装置 1 1 内の記憶部に登録しておく。認証方法として、入室者 1 0 の静脈パターンが、予め指静脈認証装置 1 1 内に登録された静脈パターンの中に含まれるか否かを確認する方法がある。確認する方法は、予め指静脈認証装置 1 1 内に登録された静脈パターンの中よりカードリーダー 1 3 などにより個人を特定し、対応した静脈パターンと入室者 1 0 の静脈パターンが一致するか否かを確認する方法であってもよい。

【 0 0 2 0 】

また、指静脈認証装置 1 1 はスタンドアローン、即ちネットワークを介して周囲のコントローラに接続することなく、指静脈認証装置 1 1 単独で認証を行い、認証結果を出力してもよい。或いは、指静脈認証装置 1 1 に通信ネットワークを介して接続される制御盤に
10
予めセキュリティ扉 1 のセキュリティ解除を許可する個人の静脈パターンを登録し、認証時に該制御盤に登録される既登録の静脈パターンを指静脈認証装置 1 1 が取得し、認証を行うネットワーク構成としてもよい。または、指静脈認証装置 1 1 で撮影した静脈パターンを該制御盤に送り、制御盤内で認証を行い指静脈認証装置 1 1 に認証結果を返してもよい。

【 0 0 2 1 】

なお、指静脈認証装置 1 1 を用いる指静脈認証は、認証ログ機能、すなわち指静脈認証の履歴情報が記録されており、該ログを確認することで誰が入室したか確認することができるように構成されている。

【 0 0 2 2 】

< 入退室管理システムのシステム構成図 >

図 2 は、実施例 1 における入退室管理システムのシステム構成図である。

図 2 に示す制御盤 2 0 は、指静脈認証装置 1 1、第 1 のセキュリティ扉 1 となる自動ドアや電気錠、ゲート等からなる制御端末 1 t や、第 2 以降のセキュリティ扉となる自動ドアや電気錠、ゲート、エレベータ制御盤等からなる制御端末 2 t などと通信を行い、指静脈認証装置 1 1、などのデータを受信する。これにより、制御端末 1 t や、制御端末 2 t などの開閉制御を行う。この際、指静脈認証装置 1 1 の近傍に設置されたカメラ 1 2 は、指静脈認証装置 1 1 で認証を行う入室者 1 0 の画像データを撮影してもよい。

【 0 0 2 3 】

入室者 1 0 は、制御端末 1 t が解錠されることにより、例えば図 1 におけるエリア 1 に
30
入室可能となる。また、制御端末 2 t が解錠されることにより、例えば図 1 におけるエリア 2、3、4、5 に入室可能となるとともに、エレベータ 3 を操作するエレベータ操作部を操作可能にしたりすることができる。

【 0 0 2 4 】

また、制御盤 2 0 には、非接触式カードリーダー 1 3 やスイッチ類、ライトなどのビル設備類などの機器のほか、管制センター 2 2 やデータセンター 2 3 などの外部管理施設や建屋内の管理室などのサーバー、パソコンなど（図示せず）に接続されてもよい。

【 0 0 2 5 】

制御盤 2 0 は、これらの端末の制御を行うマイコンと、端末からの信号をマイコンに適合した入力信号に変換する増幅回路、A / D 変換回路等の入力インターフェースと、マイ
40
コンからの制御信号である出力信号に応じて制御端末 1 t、2 t などを制御するための出力インターフェースとから構成されている（図示せず）。

【 0 0 2 6 】

制御盤 2 0 のマイコンの R O M (Read Only Memory) または外付けの R O M には、制御プログラムが格納され、該制御プログラムが実行されることにより、指静脈認証装置 1 1、非接触式カードリーダー 1 3 などからの信号に応じて、認証を行う。そして、認証可の場合には、制御端末 1 t、2 t を開放制御したり、エレベータ 3 の制御盤を制御してエレベータ操作盤を操作可能とする一方、認証否の場合には、制御端末 1 t、2 t を閉塞制御したままとしたり、エレベータ 3 の制御盤を制御しエレベータ操作盤を操作不可とする制御等の入退室管理制御が行われる。

10

20

30

40

50

【 0 0 2 7 】

なお、制御盤に搭載されているROMやRAMなどの記憶媒体には、入退室管理制御に使用される静脈データや、カードデータ、個人を特定するデータのほか、認証可否を判別するフラグ、その他制御データなど各種データが記録されるデータベース（図示せず）が格納されている。

【 0 0 2 8 】

< 入退室管理システムの入退室管理制御 >

次に、図1に示す入退室管理システムの入退室管理制御について、図3に従って説明する。

図3は、第1のセキュリティ扉1におけるフローチャートを示す。

10

まず、指静脈認証操作によって得られた静脈データ（ステップ301）と、予め指静脈認証装置11または制御盤20などの記憶媒体に格納された静脈データとの照合を行う（ステップ302）。この照合において、静脈データが一致すれば次のステップに遷移し（ステップ302のYES）、認証OKランプやブザーの鳴動を行った後（ステップ303）、第1のセキュリティ扉のセキュリティ解除を行い（ステップ304）、入退室管理制御を終了させる。

【 0 0 2 9 】

一方、認証操作によって得られた静脈データが予め登録されていない場合は（ステップ302のNO）、認証NGランプ、ブザー鳴動などで照合しない旨を入室者10に知らせたり、制御盤20などの記憶媒体に認証NGの履歴を残したり、サーバーや管制センターなどに認証NGを知らせるために発報を行う（ステップ305）。その後、第1のセキュリティ扉1は閉塞維持し（ステップ306）、入退室管理制御を終了させる。

20

なお、ステップ305では、カメラ12で認証NGとなった入室者10の画像データを、履歴や発報とともに残しても良い。または、指静脈認証装置11による認証操作を予め何回実施できるか設定しておき、1回目の認証時と同じ指または異なる指により再度認証操作をできるようにしてもよい。

【 0 0 3 0 】

次に、本実施形態の入退室管理システムの入退室管理制御において、指静脈認証を行う際に予め登録された静脈データとの照合方法において、入室者が事前に特定されていない場合の認証方法について説明する。

30

【 0 0 3 1 】

図4は、入室者が事前に特定されていない場合における、登録された静脈データとの照合方法を示すフローチャートである。

まず、指静脈認証装置11で認証操作を行い（ステップ401）、予め指静脈認証装置11のRAMに登録された全静脈データの中から一致する静脈データがあるか照合を行う（ステップ402）。認証された静脈データに一致する静脈データが存在する場合（ステップ402のYES）、静脈データに紐付けられた個人を特定するデータ及び「認証可」を表すコード、例えば「1」「0」などのデジタル信号を制御盤20などに送信し、「認証可」を表すコードを受信した制御盤20は、第1のセキュリティ扉1のセキュリティを解除する（ステップ403）。その後、入退室管理制御を終了させる。ここで、個人を特定するデータ及び「認証可」を表すコードは、どちらか一方でも構わない。「認証可」を表すコードを受信した制御盤20は、第1のセキュリティ扉1のセキュリティを解除する。

40

【 0 0 3 2 】

一方、一致する静脈データが存在しなかった場合は（ステップ402のNO）、「認証否」を表すコードを制御盤20に送信し、「認証否」を表すコードを受信した制御盤20は、認証NGランプ、ブザー鳴動などで照合しない旨を入室者10に知らせたり、制御盤20などの記憶媒体に認証NGの履歴を残したり、サーバーや管制センター22などに認証NGを知らせるために発報する（ステップ404）。そして、第1のセキュリティ扉1を閉塞維持し（ステップ405）、入退室管理制御を終了させる。

50

なお、指静脈認証装置 1 1 による認証操作を予め何回実施できるか設定しておき、1 回目の認証時と同じ指または異なる指により再度認証操作をできるようにしてもよい。

【0033】

次に、本実施形態の入退室管理システムの入退室管理制御において、指静脈認証を行う際に予め登録された静脈データとの照合方法において、入室者が事前に特定されている場合の認証方法について説明する。

【0034】

図 5 は、入室者が事前に特定されている場合における、登録された静脈データとの照合方法を示すフローチャートである。

まず、指静脈認証装置 1 1 近傍に設置された第 2 の認証端末、例えば非接触式カードリーダー 1 3 などを用いて、予め指静脈認証装置 1 1 で認証を行う入室者 1 0 が特定する（ステップ 5 0 1）。次に、個人を特定するデータは指静脈認証装置 1 1 に通知され、予め指静脈認証装置 1 1 の R A M に登録された全静脈データの中から、特定された個人のデータに紐付けられた静脈データを準備しておく（ステップ 5 0 2）。このとき、特定された個人のデータに紐付けられた静脈データは、1 指でも 2 指以上でも構わない。入室者 1 0 が引き続き指静脈認証装置 1 1 で認証操作を行った際は（ステップ 5 0 3）、特定された個人のデータに紐付けられた静脈データのみと照合を行う。よって、照合結果が判定されるまでの時間が、図 4 のパターンよりも早くなることが期待できる。

【0035】

ステップ 5 0 3 の認証において、静脈データが一致した場合（ステップ 5 0 4 の Y E S）、静脈データに紐付けられた個人を特定するデータ及び「認証可」を表すコード、例えば「1」「0」などのデジタル信号を制御盤 2 0 などに送信する。「認証可」を表すコードを受信した制御盤 2 0 は、第 1 のセキュリティ扉 1 のセキュリティを解除する（ステップ 5 0 5）。

【0036】

一方、一致する静脈データがなかった場合は（ステップ 5 0 4 の N O ）、「認証否」を表すコードを制御盤 2 0 に送信し、「認証否」を表すコードを受信した制御盤 2 0 は、認証 N G ランプ、ブザー鳴動などで照合しない旨を入室者 1 0 に知らせる（ステップ 5 0 6）。その後、第 1 のセキュリティ扉 1 は閉塞維持し（ステップ 5 0 7）入退室管理制御を終了させる。

なお、不審者 9 9 として画像データを保存したり、制御盤 2 0 などの記憶媒体に認証 N G の履歴を残したり、サーバーや管制センター 2 2 などに認証 N G を知らせるために発報しても良い。また、指静脈認証装置 1 1 による認証操作を予め何回実施できるか設定しておき、1 回目の認証時と同じ指または異なる指により再度認証操作をできるようにしてもよい。

【実施例 2】

【0037】

< 入退室管理システムの全体構成 >

次に、本実施形態の入退室管理システムにおいて、認証操作に応じて入室許可エリアが異なる場合の例（以降、「実施例 2」と称す。）を、図 6 および図 7 を用いて説明する。

【0038】

図 6 は、実施例 2 の入退室管理システム全体の概要構成図を示しており、入退室管理システムを、複数の階数を有する建物に適用した場合を示している。

【0039】

図 7 は、第 1 のセキュリティ扉 1 における通常認証又は制限認証時における入退室管理システムの入退室管理制御の流れを示すフローチャートである。

【0040】

図 6 において、入室者 1 0 が外部からビル内部に入館する場合を、図 7 を参照しながら説明する。

ビルに入館する入室者 1 0 は、まず、第 1 のセキュリティ扉 1 の扉近傍にある指静脈認

10

20

30

40

50

証装置 11 で認証操作を行う (ステップ 701)。指静脈認証操作によって得られた静脈データが予め指静脈認証装置 11 または制御盤 20 などの記憶媒体に格納された静脈データと照合を行い (ステップ 702)、一致すれば (ステップ 702 の YES) 次のステップに遷移する。

【0041】

一方、認証操作によって得られた静脈データが予め登録されていない場合は (ステップ 702 の NO)、認証 NG ランプ、ブザー鳴動などで照合しない旨を入室者 10 に知らせたり、制御盤 20 などの記憶媒体に認証 NG の履歴を残したり、サーバーや管制センターなどに認証 NG を知らせるために発報を行い (ステップ 710)、第 1 のセキュリティ扉 1 を閉塞維持する (ステップ 711)。なお、ステップ 710 では、カメラ 12 で認証 NG となった入室者 10 の画像データを、履歴や発報とともに残しても良い。または、指静脈認証装置 11 による認証操作を予め何回実施できるか設定しておき、1 回目の認証時と同じ指または異なる指により再度認証操作をできるようにしてもよい。

10

【0042】

本実施例においては、第 1 のセキュリティ扉 1 の扉近傍にある指静脈認証装置 11 で認証操作を行う際、予め 2 指以上の静脈データを指静脈認証装置 11 に登録することを特徴とする。すなわち、指毎に異なる認証状態を登録するものであり、例えば、人差し指で認証操作を行った場合には、第 1 のセキュリティ扉 1 のセキュリティを解除するとともに、第 1 のセキュリティ扉 1 を解除した後の、第 2 以降のセキュリティ扉 2 も解除するようにする。このような認証状態を「通常認証」として登録する。一方で、薬指では、第 1 のセキュリティ扉 1 のセキュリティを解除するが、第 1 のセキュリティ扉 1 を解除した後の、第 2 以降のセキュリティ扉 2 は解除しないように登録することができる。このような認証状態を「制限認証」として登録する。通常認証および制限認証として登録する指は、それぞれ 1 指でも良いし、2 指以上であっても良い。

20

【0043】

図 7 に戻り、ステップ 702 の YES と判定された後、ステップ 703 において、上述の「通常認証」であると判断された場合には (ステップ 703 の通常認証)、第 1 のセキュリティ扉をセキュリティ解除し (ステップ 705)、第 2 以降のセキュリティ扉の認証権限を付与し (ステップ 706)、入退室管理制御を終了させる。

【0044】

一方、ステップ 703 において、「制限認証」であると判断された場合には (ステップ 703 の制限認証)、第 1 のセキュリティ扉をセキュリティ解除し (ステップ 708)、第 2 以降のセキュリティ扉の認証権限を付与せずに (ステップ 706)、入退室管理制御を終了させる。なお、ステップ 708 では、第 1 のセキュリティ扉 1 は「通常認証状態」同様にセキュリティを解除するが、同時に「制限認証状態」であることを制御盤 20 やサーバーに通知する。

30

【0045】

この「制限認証」を採用することにより、セキュリティ解除される扉は、第 1 のセキュリティ扉 1 と通常使用するルートのみセキュリティ解除とし、通常使用しない扉は解除不可とすることができる。すなわち、不審者が万が一指静脈データを不当に入手して、「制限認証」において入室可能なエリアとして登録されていない扉のセキュリティを解除しようとしても、セキュリティ解除権限を得ていないことから、不審者が不正にセキュリティ解除することを防ぐことができる。ここで、第 1 のセキュリティ扉 1 は指静脈認証装置と記載しているが、これ以降のセキュリティ扉がカードリーダー 13 であった場合も同様の効果を奏することができる。

40

【0046】

次に、本実施例において、認証の対応状態として、上述の通常認証、制限認証に加え、脅迫認証を採用する場合について、図 8 ~ 11 に従って説明する。

【0047】

図 8 のパターンでは、指毎における認証の対応状態 (通常認証、制限認証、脅迫認証)

50

、入室可能エリア数、及び入室可能エリアを示している。

図 8 の例では、入室者 10 は、薬指以外の 4 指の場合 (No. 1、2、3、5) は、通常認証または制限認証として登録し、薬指の場合 (No. 4) は、脅迫認証として登録している。

通常、入館する際は、通常認証または制限認証に対応した指である薬指以外の 4 指の内 1 指 (No. 1、2、3、5 のいずれか) によって認証操作を行う。例えば、人差し指で認証した場合は、10 エリア (全エリア) の入館許可が認められ、第 1 のセキュリティ扉 1 がセキュリティ解除されるとともに、第 2 以降のセキュリティ扉 2 も通常仕様通り指静脈認証によってセキュリティ解除されるようになる (通常認証)。一方、親指で認証した場合には、3 エリアの入館が認められ、第 1 のセキュリティ扉 1 がセキュリティ解除されるとともに、入室可能エリア 1、5、6 に入室するためのセキュリティ扉がセキュリティ解除される (制限認証)。

10

【0048】

一方、第 3 者や不審者による脅迫・強要によって意図せず指静脈認証を行った場合は、脅迫認証として登録してある指で認証操作を行う (脅迫認証)。例えば、薬指を脅迫認証として登録している場合には、1 エリアの入室許可が認められる。よって、薬指での認証操作を行うと、第 1 のセキュリティ扉 1 がセキュリティ解除されると同時に、第 2 のセキュリティ扉 2 は閉塞維持し、不審者 99 をセキュリティ解除された 1 エリアから内部に侵入できないようにする。このように、脅迫認証においては、入室可能エリアが制限させているので、不審者が脅迫・強要によって重要エリアに侵入、犯行に及ぶことを防ぐことができる。

20

【0049】

また、脅迫認証であると認められる場合には、「脅迫認証状態」であることを管制センターや警備会社などに発報することができる。さらに、指静脈認証装置 11 近傍に設置されたカメラ 12 a から取得された画像データを保存したり、警備室や屋外、事務所内などで警報を鳴らしたり、ランプなどを点灯させて、周囲に異常を知らせることもできる。

【0050】

図 9 は、脅迫認証時の入室可能エリア数、入室可能エリア、及びその効果の例を示す。なお、入室可能エリアについては、図 11 を用いて説明する。

【0051】

図 9 の No. 1 に示すように、例えば、入室可能エリアが図 11 に記載のエリア 1 のみの 1 エリアの場合には、セキュリティ解除された第 1 のセキュリティ扉 1 につながるエリア 1 のみのセキュリティ解除とする。そして、それ以降のセキュリティ扉はセキュリティ解除権限を与えないようにしている。このことにより、第 3 者や不審者はエリア 1 のみ入室できるに留まるので、入室できるエリアが最小限に抑えられ、盗難や人的被害を最小限に抑えることが期待できる。

30

【0052】

また、No. 2 に示すように、入室可能エリアが 2 エリアの例では、第 1 のセキュリティ扉 1 のセキュリティ解除に加え、図 11 に記載の特定のエリア 4 につながるセキュリティ扉のみセキュリティ解除権限を付与する。エリア 4 は、警備室や、非常口につながるエリアであり、退避可能とすることができる。図 11 の破線は、認証者 10 が、ビル外部の扉 1 において、不審者 99 に脅迫された際に、脅迫認証時 (エリア 1、4 のみ解除) の特定エリアへの誘導例を示したものである。入室可能エリアが 1 及び 4 のみであるため、エリア 1 を通過した後は、特定のエリア 4 へ誘導することが可能である。ここで、エリア 4 からエリア 1 へ移動する際には、エリア 4 内に設けられている認証装置 11 における認証操作が必要となっているが、この認証操作のセキュリティ解除権限を付与しないことで、エリア 4 へ不審者 99 を閉じ込めることができる。このような構成を有することにより、警備員が到着するまで不審者 99 を閉じ込めておくことが可能でありながら、金銭被害や人的被害、情報や電氣的設備のない部屋へ誘導することで被害を最小限に抑えることが期待できる。

40

50

【 0 0 5 3 】

No. 3では、入室エリアが4エリアの例では、図11に記載のエリア1から4まではセキュリティ解除権限を付与し、セキュリティ解除して自由に入退室することが可能である。しかしながら、エレベータがあるエリア5以降へのセキュリティ解除権限は付与していないため、脅迫・強要によってセキュリティ解除操作をさせられても、エリア5のセキュリティ解除することはできないため、エレベータを使用して他階へ移動することができず、被害を最小限に抑えることが期待できる。

【 0 0 5 4 】

その他にも、入室可能エリアが9エリアの例では（No. 4）、エリア10を除いてセキュリティ解除権限を付与しており、脅迫認証として通知、発報してから警備員が到着するまで、通常のセキュリティ解除と同様のセキュリティ権限付与しているため、エリア10を除いて自由に行き来できる。しかしながら、エリア10のみはセキュリティ解除権限を付与しておらず、入室することはできない。そのため、エリア10が、例えばサーバ室や金庫、重要人物室等の最重要室である場合、重大な被害を抑えることが期待できると共に、不審者99には脅迫認証モードであることを気付かせにくいメリットがある。

10

【 0 0 5 5 】

図10は、指静脈認証を行う指によってセキュリティ解除されるパターンが異なる場合のフローチャートを示している。

【 0 0 5 6 】

まず、指静脈認証装置11において認証を行う（ステップ1001）。次に、認証された指が通常認証・制限認証に登録された指か、脅迫認証に登録された指か、を判定する（ステップ1002）。判定によって、通常認証又は制限認証が行われたと判断された場合には（ステップ1002の通常認証・制限認証）、それぞれの認証に対応するセキュリティ扉のセキュリティ解除を行い（ステップ1003）、制御を終了させる。

20

【 0 0 5 7 】

一方、脅迫認証と判定された場合には（ステップ1002の脅迫認証）、第1のセキュリティ扉をセキュリティ解除した後（ステップ1004）、脅迫認証状態であることを発報し、不審者に気づかれないように周囲に知らせるようにする（ステップ1005）。次に、認証された指毎に決められた入室可能エリアに従う。例えば、第2のセキュリティ扉以降は閉塞状態を維持する、又は特定のエリアへ誘導するように、セキュリティ扉の解除を行い（ステップ1006）、入退室管理制御を終了する。

30

【 0 0 5 8 】

以上より、指毎に異なる対応状態を設定し、指毎に異なる入室許可エリアに登録することにより、不審者等による不正行為を最小限に抑えることができる。例えば、許可エリアを最小範囲に押さえた場合には、当該許可エリア以外で不審者による不正が行われたとしても、そもそも許可エリアとして認められない。よって、不正行為を最小限に抑えることが可能となる。

また、認証操作がカードや暗証番号によるものだと、カードを複数所持することや複数の暗証番号を暗記する必要が生じ、認証操作が煩わしくなり使い勝手がよくない。一方、生体認証装置を用いると、例えば指毎に異なる入室許可エリアの登録を行うことができるので、上記のような認証操作の煩わしさを解消することができる。

40

その他にも、第三者や不審者による脅迫・強要が行われた場合に、特定の指静脈認証操作を行う構成を採用して脅迫認証状態であると判定することで、不審者に気付かれず、即時に周囲に知らせることができる。また、脅迫認証状態では、入室者の安全を確保しながらも、入館エリアを限定することで、被害を最小限に抑えることが期待できる。また、特定のエリアへ不審者を誘導することで安全を確保できることが期待できる。

【 0 0 5 9 】

なお、本発明は上記した実施例に限定されるものではなく、様々な変形例が含まれる。例えば、上記した実施例は本発明を分かりやすく説明するために詳細に説明したものであり、必ずしも説明した全ての構成を備えるものに限定されるものではない。また、ある実

50

施例の構成の一部を他の実施例の構成に置き換えることが可能であり、また、ある実施例の構成に他の実施例の構成を加えることも可能である。また、各実施例の構成の一部について、他の構成の追加・削除・置換をすることが可能である。

【0060】

また、上記の各構成、機能、処理部、処理手段等は、それらの一部又は全部を、例えば集積回路で設計する等によりハードウェアで実現してもよい。また、上記の各構成、機能等は、プロセッサがそれぞれの機能を実現するプログラムを解釈し、実行することによりソフトウェアで実現してもよい。各機能を実現するプログラム、テーブル、ファイル等の情報は、メモリや、ハードディスク、SSD (Solid State Drive) 等の記録装置、または、ICカード、SDカード、DVD等の記録媒体に置くことができる。

10

【0061】

また、制御線や情報線は説明上必要と考えられるものを示しており、製品上必ずしも全ての制御線や情報線を示しているとは限らない。実際には殆ど全ての構成が相互に接続されていると考えてもよい。

【符号の説明】

【0062】

- A 本実施形態における入退室管理システム
- 1 第1のセキュリティ扉
- 2 第2以降のセキュリティ扉
- 3 エレベータ
- 10 入室者
- 11 指静脈認証装置
- 12 カメラ
- 13 非接触式カードリーダー
- 20 制御盤
- 21 データベース
- 22 管制センター
- 23 データセンター
- 99 不審者

20

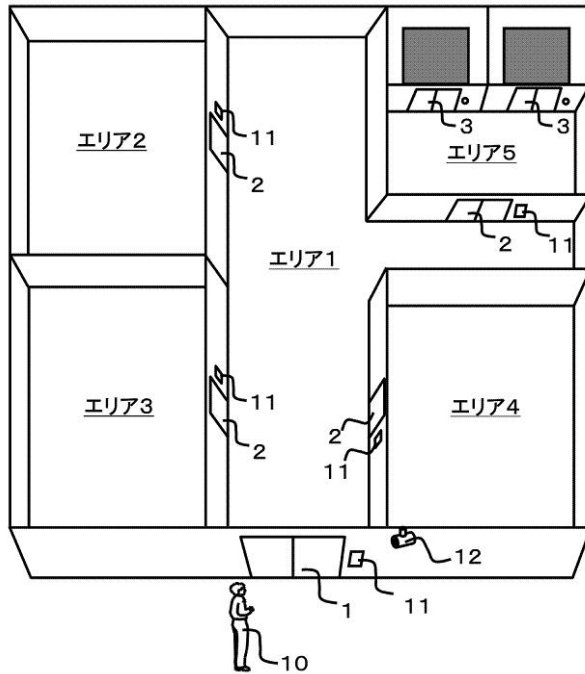
【 図 8 】

[図 8]

No.	登録指	対応状態	入室可能エリア数	入室可能エリア
1	規指	制限認証4	3エリア	エリア1、5、6
2	入差し指	通常認証1	10エリア(全エリア)	エリア1～10
3	中指	制限認証2	4エリア	エリア1～4
4	兼指	脅迫認証	1エリア	エリア1
5	小指	制限認証3	9エリア	エリア1～9

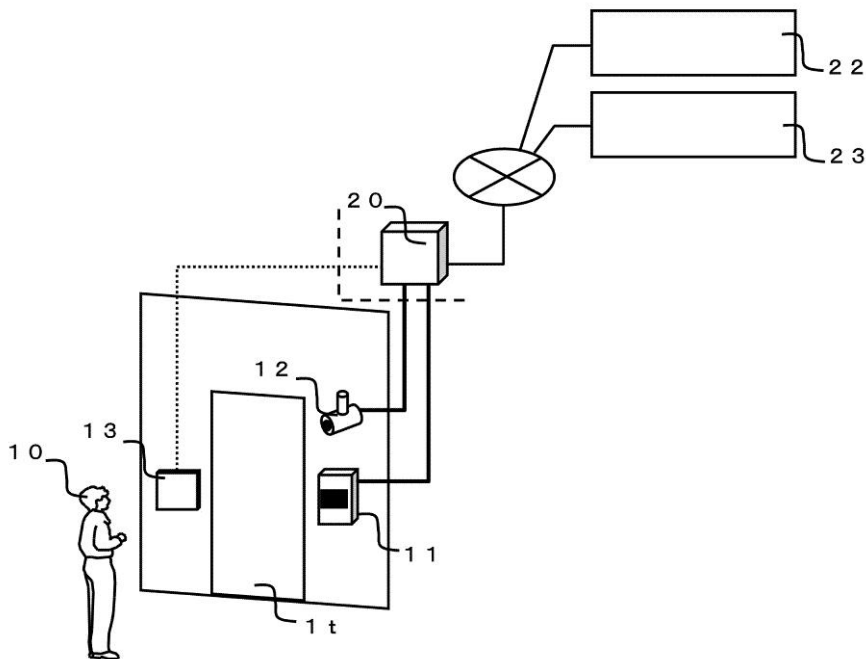
【 図 1 】

【 図1】



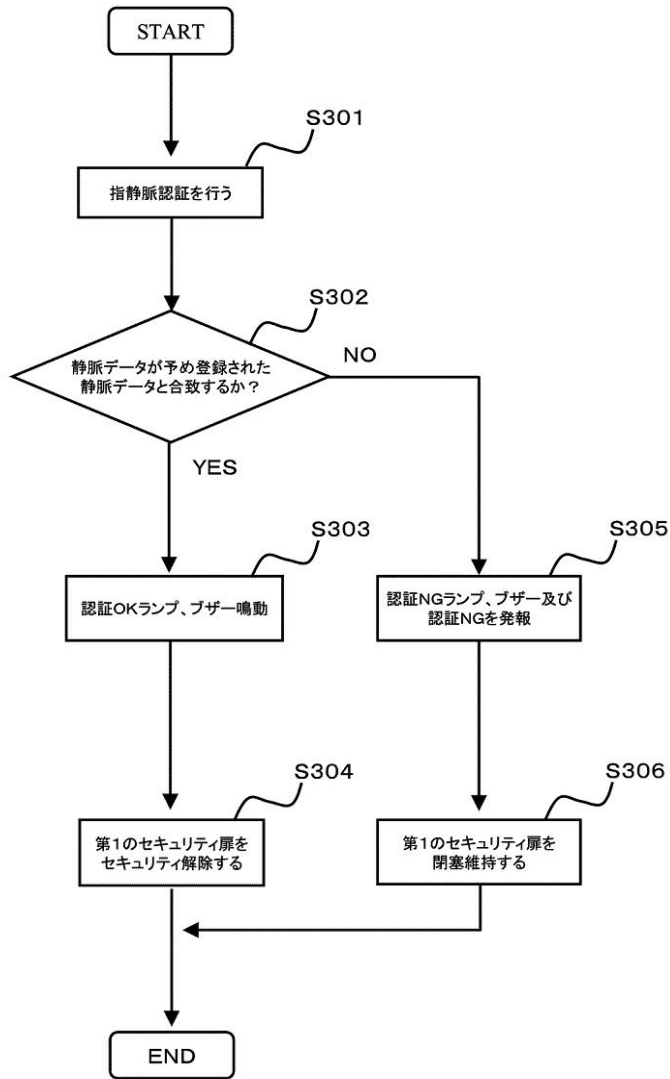
【 図 2 】

【 図2】



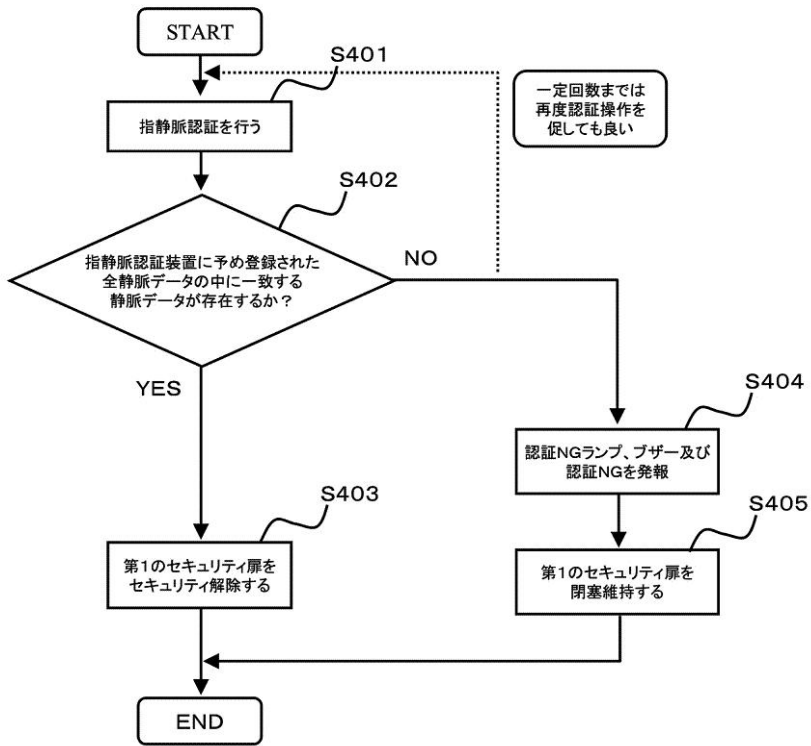
【 図 3 】

【図3】



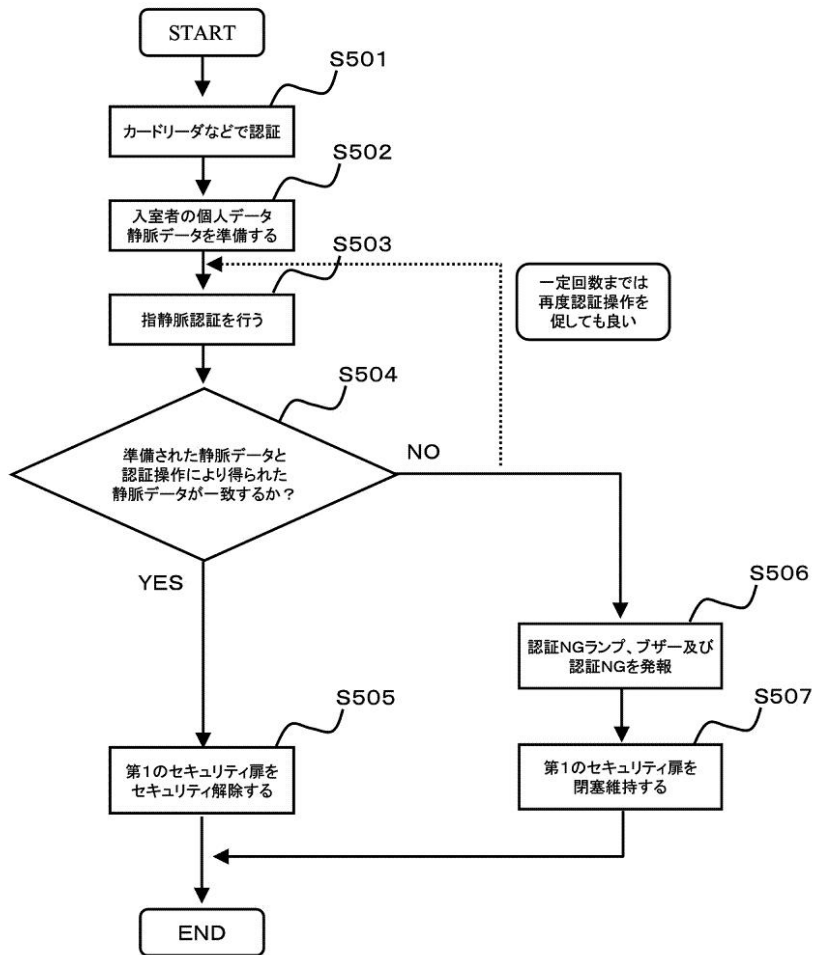
【 図 4 】

【図4】



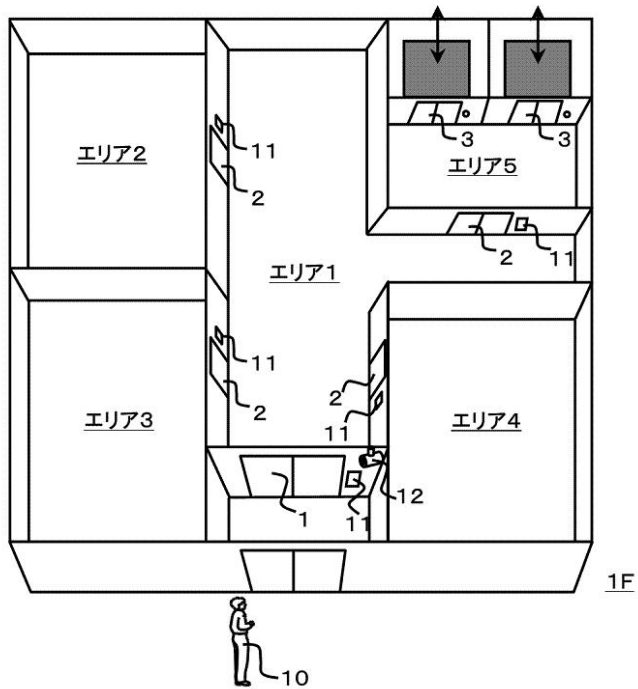
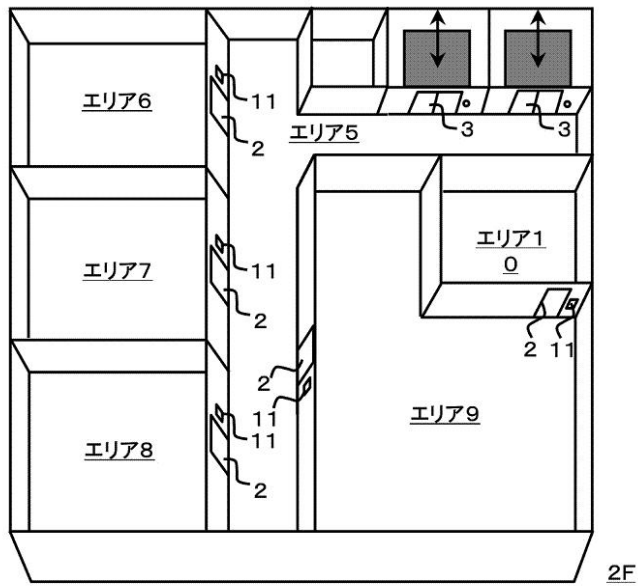
【 図 5 】

【図5】



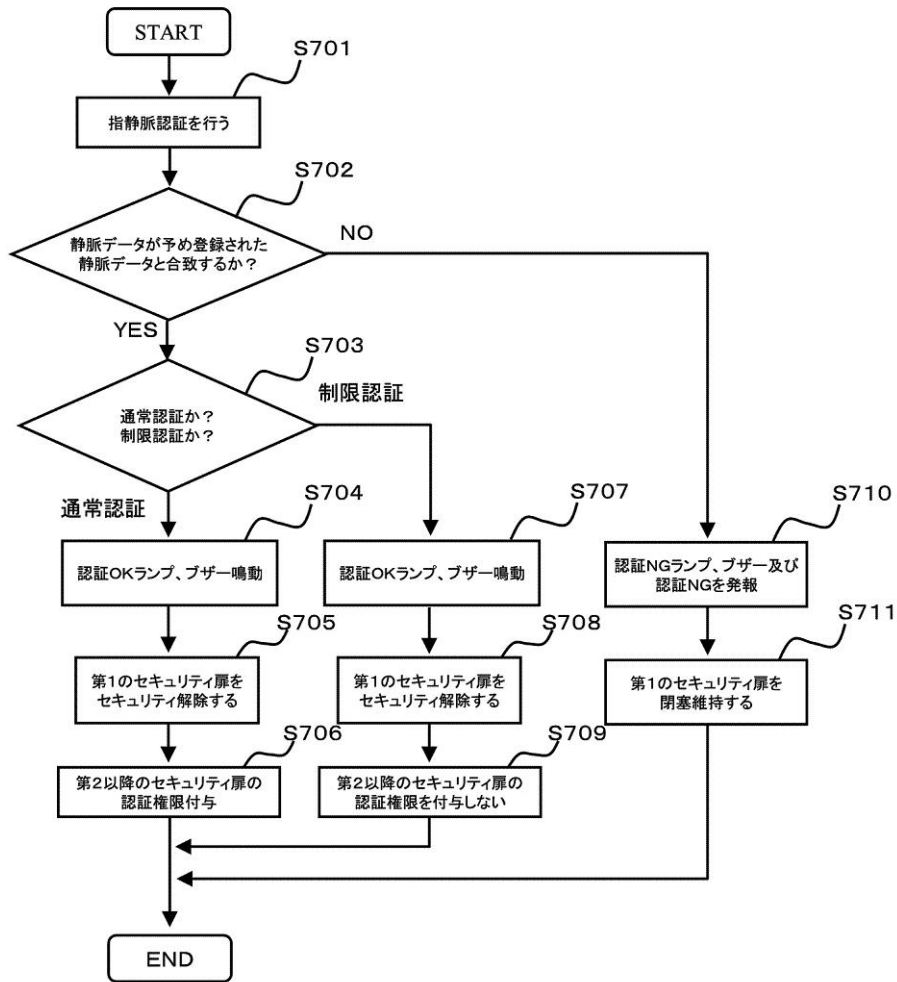
【 図 6 】

【 図6】



【 図 7 】

【 図7】



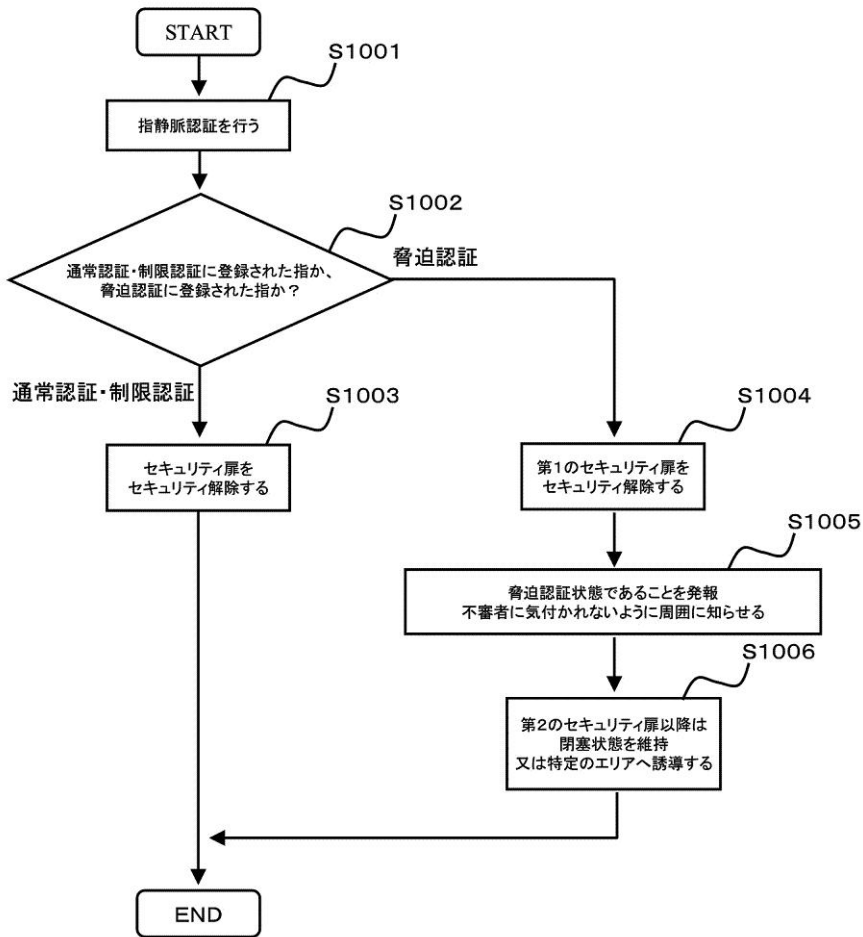
【 図 9 】

【図9】

No.	入室可能エリア数	入室可能エリア	効果
1	1エリア	エリア1	第1の扉のみ解除
2	2エリア	エリア1、4	警備室等4への誘導
3	4エリア	エリア1～4	エレベータ使用不可
4	9エリア	エリア1～9	重要エリア10の入室不可

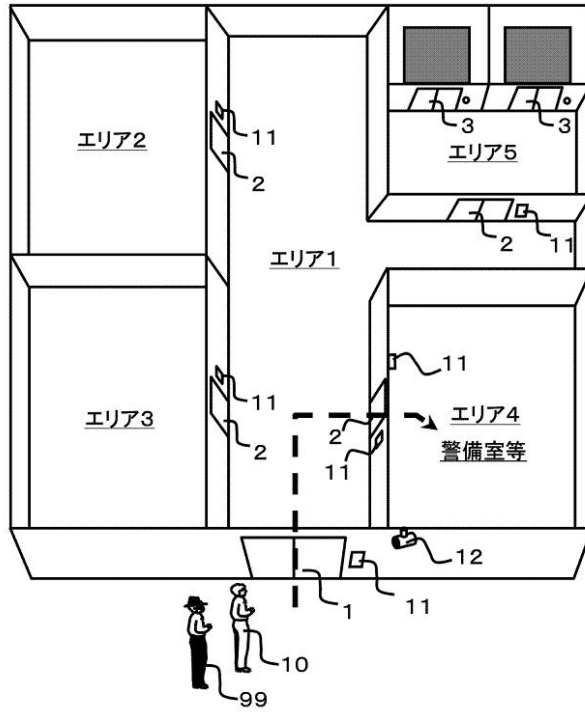
【図10】

【図10】



【図 11】

【図11】



フロントページの続き

(72)発明者 三坂 智也

茨城県ひたちなか市市毛1070番地
テム社内

株式会社日立製作所都市開発シス

(72)発明者 徳永 素克

茨城県ひたちなか市市毛1070番地
テム社内

株式会社日立製作所都市開発シス

Fターム(参考) 2E250 AA03 AA12 BB46 BB47 DD08 EE03