

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第5733802号
(P5733802)

(45) 発行日 平成27年6月10日 (2015. 6. 10)

(24) 登録日 平成27年4月24日 (2015. 4. 24)

(51) Int. Cl.

F 1

G 0 8 B 25/00 (2006. 01)

G 0 8 B 25/00 5 1 0 M

G 0 8 B 13/196 (2006. 01)

G 0 8 B 13/196

G 0 8 B 25/04 (2006. 01)

G 0 8 B 25/04 F

G 0 8 B 25/04 G

請求項の数 3 (全 18 頁)

(21) 出願番号 特願2013-50165 (P2013-50165)
 (22) 出願日 平成25年3月13日 (2013. 3. 13)
 (65) 公開番号 特開2014-174963 (P2014-174963A)
 (43) 公開日 平成26年9月22日 (2014. 9. 22)
 審査請求日 平成25年3月13日 (2013. 3. 13)
 審判番号 不服2014-927 (P2014-927/J1)
 審判請求日 平成26年1月17日 (2014. 1. 17)

早期審査対象出願

(73) 特許権者 507184096
 日本テクノ株式会社
 東京都新宿区西新宿一丁目25番1号
 (74) 代理人 100109553
 弁理士 工藤 一郎
 (72) 発明者 馬本 英一
 東京都新宿区西新宿1-25-1 新宿セ
 ンタービル 日本テクノ株式会社内

合議体

審判長 島田 信一

審判官 中川 隆司

審判官 小関 峰夫

最終頁に続く

(54) 【発明の名称】 防犯装置及び防犯装置を利用可能で出入口の施錠装置を有する建築構造物

(57) 【特許請求の範囲】

【請求項 1】

無人の施設に対して機能する防犯機能を動作させ、防犯空間を撮影するための撮影部を有する防犯動作部と、

防犯動作部を制御し、防犯動作部による防犯空間の撮影が開始される場合に防犯機能起動時と非正常事態検知時のみに撮影を可能とすることで省エネルギーにて防犯をするための制御部と、

防犯動作部の起動中を知らせるとともに当該施設内に人がいない間の省エネ目標の設定や目標達成度合いの状況を表示するためのディスプレイと、

ディスプレイ周辺面に備えられ、制御部に対する防犯動作部の起動操作があった場合に前記施設の最終退出者となる操作者を撮影するための操作者撮影部と、

操作者撮影部の記録を保持する記録保持部と、
 を有する防犯装置。

【請求項 2】

操作者撮影部は、顔画像認識手段を有し、操作があった場合に、顔画像認識手段が顔画像を認識できない場合には操作を無効とする請求項 1 に記載の防犯装置。

【請求項 3】

請求項 1 又は 2 に記載の防犯装置を利用可能で出入口の施錠装置を有する建築構造物。

【発明の詳細な説明】

【技術分野】

10

20

【 0 0 0 1 】

本発明は、防犯装置及び防犯装置を利用可能で出入口の施錠装置を有する建築構造物に関する。

【背景技術】

【 0 0 0 2 】

営業時間や就業時間が定められている商業施設やオフィスなどの各種施設においては、当該営業時間外あるいは就業時間外（主に夜間）になると、基本的には当該施設から人がいなくなる。そのため、当該時間帯における施設内への不審者の侵入防止を目的として、従来から様々な防犯装置ないし防犯システムに関する技術が開示されている。

【 0 0 0 3 】

それらの多くは、各種センサを用いて不審者による施設内への侵入を事前または事後に検知し、警報を発信する構成を採用している。具体的には、特許文献1において、センサによって侵入者を検知して警報を発するのみならず、当該侵入者の身体的特徴をも記録する防犯装置に関する技術が開示されている。この防犯装置は、記録した侵入者の身体的特徴があらかじめ登録された身体的特徴を有する人物と同一人物であると判断される場合には、警報を発信しないような機能を有しており、家人や当該施設のスタッフ等の出入りについてむやみに警報を発信しないように作用する点を特徴として備えている。

【先行技術文献】

【特許文献】

【 0 0 0 4 】

【特許文献1】特開2004-348407公報

【発明の概要】

【発明が解決しようとする課題】

【 0 0 0 5 】

ここで、従来から存在する防犯装置ないし防犯システムにおいては、防犯対策の対象はあくまで施設外部から侵入する不審者であった。しかしながら、防犯装置および防犯システムを稼働させるのは当該施設の関係者であって、特に防犯装置を起動させて同施設を最後に退出する人物は施設の防犯管理上重要な地位にあることはこれまであまり注目されてこなかった。具体的にいえば、施設を最後に退出する人物は、施設の施錠を行うべき立場にあるし、また、誰もいない施設内にて何らかの事故・事件が発生した場合には、当該事故等の責任の所在を把握、分析するうえで施設を最後に退出した人物を特定しておく意義は決して小さくない。

【 0 0 0 6 】

ここで、従来技術が最終的に退出する施設スタッフの特定に関心がなかったことの一例として、前記特許文献1を挙げる。同文献には、あらかじめ身体的特徴を登録しておいた人物の存在を検知しても警報等を鳴らさないことを特徴とする防犯装置に関する技術が開示されているところ、同装置の稼働中に万が一施設関係者が施設内にて窃盗などの犯行に及んだとしても、施設関係者であるがゆえに当該犯行に及んだ者の身体的特徴があらかじめ登録されており、同特徴が登録された特徴と同一であるがゆえに警報等が発せられない事態が生じてしまい、防犯装置としての体をなさないこととなってしまう。

【課題を解決するための手段】

【 0 0 0 7 】

以上のような事態を回避し従来の防犯装置にはない新しい機能を付加すべく、本発明は、防犯機能を動作させるための防犯動作部と、防犯動作部を制御するための制御部と、制御部に対する操作があった場合に操作者を撮影するための操作者撮影部と、操作者撮影部の記録を保持する記録保持部と、を有する防犯装置などを提案する。

【発明の効果】

【 0 0 0 8 】

主に以上のような構成をとる本発明によって、施設内における強固な防犯対策を構築することが可能になる。

10

20

30

40

50

【図面の簡単な説明】

【 0 0 0 9 】

【図 1】実施形態 1 の防犯装置の実施の一例を説明するための概念図

【図 2】実施形態 1 の防犯装置の機能ブロックの一例を示す図

【図 3】実施形態 1 の防犯装置の実施の別の一例を説明するための概略図

【図 4】実施形態 1 の防犯装置の機能的な各構成をハードウェアとして実現した際の構成の一例を示す概略図

【図 5】実施形態 1 の防犯装置の処理の流れの一例を示す図

【図 6】実施形態 2 の防犯装置の機能ブロックの一例を示す図

【図 7】実施形態 2 の防犯装置の処理の流れの一例を示す図

10

【図 8】実施形態 3 の防犯装置の機能ブロックの一例を示す図

【図 9】実施形態 3 の防犯装置の処理の流れの一例を示す図

【図 10】実施形態 4 の防犯装置の機能ブロックの一例を示す図

【図 11】実施形態 4 の防犯装置の処理の流れの一例を示す図

【図 12】実施形態 5 の防犯装置の機能ブロックの一例を示す図

【図 13】実施形態 5 の防犯装置の処理の流れの一例を示す図

【図 14】実施形態 1 の防犯装置のディスプレイおよびその周辺面の一例を示した正面概略図

【発明を実施するための形態】

【 0 0 1 0 】

20

以下、本発明の各実施形態について図面と共に説明する。実施形態と請求項の相互の関係は、以下のとおりである。まず、実施形態 1 は、主に請求項 1、3 などに関連する。実施形態 2 は、主に請求項 2 などに関連する。実施形態 3 は、主に請求項 1 などに関連する。実施形態 4 は、主に請求項 1 などに関連する。実施形態 5 は、主に請求項 1 などに関連する。なお、本件発明はこれらの実施形態に何ら限定されるものではなく、その要旨を逸脱しない範囲内において、種々な態様で実施し得る。

【 0 0 1 1 】

<<実施形態 1>>

<概要>

30

図 1 は、本実施形態の防犯装置の実施の一例を説明するための概念図である。この図において示すように、本実施形態の「防犯装置」0101 は、操作者が防犯機能を動作させるために操作を行うと、防犯機能を動作させるのみならず当該操作者を撮影し、その記録を保持することを特徴としている。ここで防犯装置は、防犯空間を動画撮影するための「防犯カメラ」0102 や「施錠装置」0103 等を備える建築構造物内に設置され、当該施錠装置その他の機器と相互にネットワーク上にて情報の送受信を行うように構成されていてもよい。いずれにせよ、このような特徴を備える構成を採用することにより、防犯管理の観点から重要な地位にある施設最終退出者を特定することが可能になる。

【 0 0 1 2 】

<機能的構成>

40

図 2 は、本実施形態の防犯装置の機能ブロックの一例を示す図である。この図にあるように、本実施形態の「防犯装置」0200 は、「制御部」0201 と、「防犯動作部」0202 と、「操作者撮影部」0203 と、「記録保持部」0204 と、から構成される。

【 0 0 1 3 】

なお、以下に記載する防犯装置の機能ブロックは、いずれもハードウェア、ソフトウェア、又はハードウェア及びソフトウェアの両方として実現され得る。コンピュータを利用するものであれば、具体的な構成としては、CPU やメインメモリ、GPU、画像メモリ、グラフィックボード、バス、あるいは二次記憶装置（ハードディスクや不揮発性メモリ、CD や DVD、SD カードなどの記憶メディアとそれらのメディアの読取ドライブなど）、カメラ、センサ、情報入力に利用される入力デバイス、スキャナ装置、プリンタ、そ

50

他の外部周辺装置などのハードウェア構成部、およびその外部周辺装置用のインターフェース、通信用インターフェース、それらハードウェアを制御するためのドライバプログラムやその他アプリケーションプログラムなどが挙げられる。そして、メインメモリ上に展開したプログラムに従ったCPUの演算処理によって、入力デバイスやその他インターフェースなどから入力されメモリやハードウェア上に保持されているデータなどが加工、蓄積されたり、前記各ハードウェアやソフトウェアを制御するための命令が生成されたりする。ここで、上記プログラムは、モジュール化された複数のプログラムとして実現されてもよいし、2以上のプログラムを組み合わせる一のプログラムとして実現されてもよい。

【0014】

ここで図14は、本実施形態の防犯装置の一例として、省エネ目標の達成度合いを監視するための機能を兼ね備えた防犯装置のディスプレイおよびその周辺面を示した正面概略図である。この図において示されている防犯装置は、「操作ボタン」1402の操作によって入力された省エネ目標の設定や目標達成度合いの状況などを「ディスプレイ」1404に表示するいっぽう、当該操作を行ったユーザを「カメラ」1405にて撮影し、「センサ」1403などによって非正常事態の発生を検知すると当該検知結果を出力するよう構成することが考えられる。施設内に人がいない間の省エネ目標達成度合いをも監視することを可能とする機能を備えた当該構成をとることにより、施設内に人がいない間にも必要とされる待機電力量の無駄をチェックしつつ防犯体制を強固なものとすることが可能になる。

【0015】

また、本発明は装置として実現できるのみならず、方法としても実現可能である。そして、このような装置の一部をソフトウェアとして構成することも可能である。さらに、そのようなソフトウェアが記録された記録媒体も当然に本発明の技術的な範囲に含まれる。

【0016】

そしてさらには、図3において示すように、本発明の防犯装置を他の電気機器やスマートメーター、ホームゲートウェイなどの外部装置との間で相互に通信可能な構成をとることにより、いわゆるBEMS (Building Energy Management System) やFEMS (Factory Energy Management System)、HEMS (Home Energy Management System) といったエネルギー管理のための各種システムの一部を構成することも可能である。エネルギー消費量と防犯体制とを一元的に管理可能とする構成を採用することによって、施設管理の効率化を実現することが可能になる。

【0017】

「防犯動作部」0202は、防犯機能を動作させる機能を有する。ここでいう「防犯機能」とは、具体的には、施設内における非正常事態の発生を検知し当該検知結果を出力するための一連の機能をさす。そして「検知結果の出力」には、警備会社などの管理担当者が管理する端末装置（管理担当者端末）への検知信号の送信出力や音声出力、表示出力、印刷出力、警告ランプ出力などの各手段が含まれ、これらを単独で用いるほか複数を組み合わせる用いてももちろんよい。

【0018】

ちなみに、ここでいう「施設」とは、オフィスや店舗のような屋内空間である商業施設のみならず、学校や病院、美術館、博物館などの文教施設、さらにはスタジアムや遊園地、公園など一定範囲に限定された屋外空間である施設をも含んでいる。

【0019】

非正常事態の発生を検知するための具体的な機能としては、例えば、赤外線や光、超音波、温度、振動などを用いた各種センサを稼働させることが考えられる。当該方法を採用することにより、施設内への不審者の侵入や不審物の投下、投入などの非正常事態の発生を、前記各種センサが作動することにより的確に把握することが可能になる。したがってこの一例の場合において「防犯機能を動作させる」とは、各種センサに対し種々の内容の指示を行うことを意味している。

【 0 0 2 0 】

なお、前記検知結果は、ディスプレイやスピーカなど防犯装置に接続される外部周辺装置を通じて出力されるほか、ネットワークを通じ、施設管理者が管理する端末装置に対して出力されることも考えられる。防犯装置がこれらの各種手段を用いて検知結果を出力することにより、施設管理者に対し非正常事態発生的事实を迅速に把握させることが可能になり、他方、非正常事態を生じさせた不審者に対しては施設管理者による前記把握の事実を認識させることも可能となり、結果として施設侵入等の目的遂行を断念させることが可能になる。

【 0 0 2 1 】

ちなみに、ここでいう「防犯」の対象となる非正常行為とは、字義通りの犯罪行為に限定されるものではなく、非倫理的行為や就業規則や職場内ルール等一定の決まりごとに違反する行為などのような非常事態を伴う行為が広く対象となりうる。

10

【 0 0 2 2 】

「制御部」0201は、防犯動作部を制御する機能を有する。ここでいう「制御する」とは、防犯動作部に対し、センサ等非正常事態の発生を検知するための各種手段を起動し、稼働させ、停止させるまでの間になしうる種々の指示を行うことを意味している。具体的な制御の内容としては、例えば、防犯動作部の起動、防犯対象となる防犯空間の範囲の設定、非正常事態の発生を検知するセンサ等（どの場所の、どの種類の、どれだけの数のセンサを対象とするか等）の特定、非正常事態発生を検知結果の出力方法（検知信号の出力、音声出力等）、出力形態（出力を継続する時間、出力のタイミング等）及び出力先の選択、検知、検知結果の出力、稼働の停止などが考えられる。

20

【 0 0 2 3 】

なお、施設内における人の出入りや繁閑期の変化、管理体制の変更等に代表されるように、防犯のための環境は常時変わりうることから、制御部にて制御すべき内容は適宜変更可能なように構成されているほうが望ましい。

【 0 0 2 4 】

「操作者撮影部」0203は、制御部に対する操作があった場合に操作者を撮影する機能を有する。「制御部に対する操作」とはすなわち、操作者が防犯機能の動作を目的として行うあらゆる操作のことを意味しており、制御部に対する操作が操作者撮影のトリガーとして機能している。そして制御部に対し複数の操作がなされた場合においては、そのすべての操作がなされた各時点において操作者を撮影するような構成をとってもよいし、所定時間内に連続的に操作が行われる場合にそのうちのタイミングにおいてのみ撮影を行い、それ以外のタイミングでは撮影を行わない構成をとってもよい。

30

【 0 0 2 5 】

なお、ここでいう「操作者」とは、防犯機能の制御を意図する者のことを指しており、正常時であればこのような意図をもつ者は、施設内において防犯機能を作動させる最終退出者あるいは翌営業開始時等において防犯機能を停止させる最早入室者となる。また、非正常事態時において当該意図をもつ者としては、施設内への不正侵入者等が考えられる。

【 0 0 2 6 】

ここで、撮影するタイミングとしては、制御部に対する操作を受け付け始めた時点とするほか当該操作が完了した時点としてもよく、そのほか操作者の容姿を的確に撮影することが可能となるあらゆるタイミングとすることが可能である。例えば、制御部に対する操作を行うために予め所定の暗証番号の入力を要するものとし、操作者による当該暗証番号の入力を受け付けるタイミングで撮影を行うことなどが考えられる。このように、必須の操作手順を定めておき、当該操作手順が取られる間に撮影を行う構成を採用することにより、操作者撮影の実効性をより高めることが可能になる。

40

【 0 0 2 7 】

なお、「操作者を撮影する」とは、撮影者の具体的な容姿を捉えその全身を撮影することまでを要求するものではない。撮影者撮影部においては「誰が」操作者であるかを特定することができればよいとため、具体的な撮影手段はその要求を満たす限りであれば、いか

50

なる手段によっても構わない。たとえば、撮影者の全身のほか、顔や撮影者が身につけている名札、服装その他操作者を特定するための少なくとも一の判断要素を撮影する方法を採用することが考えられる。そして具体的な撮影方式としては、例えば、赤外線ライトを用いる撮影方式を採用することも考えられる。このような撮影方式を採用することによって、施設内の明るさに影響されることなく操作者の容姿を撮影し、誰が操作者であるかを記録することが可能になる。

【 0 0 2 8 】

また、操作者撮影部はあくまで操作者を撮影するための機能であり、防犯空間を撮影することを主眼としたものではない。したがって、特定の防犯空間内において、本実施形態の防犯装置とは別個に単数あるいは複数台の防犯カメラを設ける構成があってもよい。既に示した図 1 においては、前記のとおり「防犯装置」0 1 0 1 とは別に「防犯カメラ」0 1 0 2 を設けた実施形態を図示している。

10

【 0 0 2 9 】

さらに、ここでいう「撮影する」とは画像と動画とを特段区別しておらず、いずれの態様にて撮影を行うことをも意味として包含している。したがって、静止画像のみあるいは動画のみを撮影する形態のみならず、画像と例えば比較的短時間の動画とを組み合わせる撮影する形態であってもここでいう「撮影する」には含まれる。このように画像と動画とを組み合わせる操作者を撮影することにより、静止画像のみの記録ではブレにより撮影対象者の特定が困難になるという事態を回避し、操作者が誰であるかをより明確に特定することが可能になる。

20

【 0 0 3 0 】

また、ここでいう「撮影する」とは、必ずしも防犯装置内にて直接撮影を行うことのみを意味するものではない。例えば、防犯装置と前記管理担当者端末とをネットワークで接続し、防犯装置にて把握した操作者の画像情報を管理担当者端末に送信し、当該端末にて前記画像情報を撮影する処理を促すこともここでいう「撮影する」に含まれる（後記記録保持部においても同様である。）。現に撮影を行う機能を防犯装置外部に備えることをも可能とする構成を採用することにより、被撮影者等が防犯装置を破壊するなどして撮影した画像情報を消去、損壊する事態を回避することができる。

【 0 0 3 1 】

「記録保持部」0 2 0 4 は、操作者撮影部にて撮影された記録を保持する機能を有する。「撮影された記録」としては、例えば、撮影された画像を画像ファイルや動画ファイルなどのファイル形式とすることが考えられる。ここで、前記ファイルは、撮影日時やその日に施設内で起こった主なイベント（忘年会、ノー残業デー、プロジェクト納期締切日）、撮影時に操作者が行っていた操作の内容などの情報をそれぞれ紐づけて記録してもよい。このような構成をとることにより、操作者による操作日時や操作内容が合理的なものであるか、すなわち、不自然な時間帯に不適切な操作していないかどうかをチェックすることが可能になる。

30

【 0 0 3 2 】

なお、記録保持部は、防犯を実効性あるものとするために極めて重要な情報の保持に関する機能なので、その取扱いは慎重になされなければならない。したがって、当該機能により防犯装置内の機構にて前記記録を保持する際には、防犯装置においては、当該記録保持機構が外部から容易に取り出しができないような構造を採用していることが求められる。具体的には、他の機構と遮蔽されるような物理的構造をとるほか、外部通信手段からの侵入を防ぐため、シールド構造を採用することなどが考えられる。当該構成をとることにより、保持された記録を外部から容易に把握することができず、有事、すなわち非正常事態発生後に記録を把握する必要がある場合に限り当該記録を把握することが可能になる。かかる効果を期待することにより、操作者等のプライバシーにかかわるような画像が無用に外部に公開される事態を抑制することも可能となる。

40

【 0 0 3 3 】

また、前記管理担当者端末へ非正常事態を検知した旨の信号の送信出力を行う場合にお

50

いて、当該信号のみならず、操作者撮影部にて撮影された記録をも一緒に送信する構成をとってもよい。このような構成をとることにより、前記検知信号を受信した管理担当者が、当該施設を最後に退出したと考えられる人物をすぐに特定できることから、当該人物にすぐに連絡を入れるなどして警備上要求される確認を迅速にとることが可能になり、非正常事態検知時の初動対応を適切に行うことが可能になる。

【0034】

ここで、本実施形態の防犯装置は、出入口に施錠装置を有する建築構造物内にて利用可能なように設けられてもよい。ここでいう「利用可能なように」の一例としては、防犯装置および施錠装置が双方あるいは他の装置との間でネットワーク上で情報の送受信を行うことが可能となるような状態にあることが考えられる。この時例えば、防犯装置の起動操作が行われた所定時間以内に出入口の開閉が行われた場合には、当該防犯装置の操作者が退出したものと認識し、施錠装置を起動させ、出入口の施錠処理を行う構成をとることなどが考えられる。このような構成をとることにより、防犯装置に対する操作が行われた後に施錠装置の操作が行われるという各装置の操作手順を把握することが可能になり、防犯装置の操作者がすなわち当該防犯空間の最終退出者であることがより明確になる。

【0035】

<具体的な構成>

図4は、本実施形態の防犯装置の機能的な各構成をハードウェアとして実現した際の構成の一例を示す概略図である。この図を利用して、それぞれのハードウェア構成部の働きについて説明する。

【0036】

この図にあるように、防犯装置は、各種演算処理を実行するための「CPU」0401と、「記憶装置（記憶媒体）」0402と、「メインメモリ」0403と、「出力インターフェース」0404と、「入力インターフェース」0414と、を備え、入出力インターフェースを介して、例えば「カメラ」0405や「ディスプレイ」0406、「プリンタ」0407、「管理担当者端末」0408などの外部周辺装置と情報の送受信を行う。なお、記憶装置には以下で説明するような各種プログラムが格納されており、CPUはこれら各種プログラムをメインメモリのワーク領域内に読み出して展開、実行する。なお、これらの構成は、「システムバス」0409などのデータ通信経路によって相互に接続され、情報の送受信や処理を行う。

【0037】

（制御部の具体的な処理）

CPUは、「制御プログラム」0410を実行し、入力インターフェースを通じて入力される信号に応じて後記防犯動作プログラムや操作者撮影プログラムを制御する処理を行う。

【0038】

（防犯動作部の具体的な処理）

CPUは、制御プログラムの実行により得られた情報を読み出して「防犯動作プログラム」0411を実行し、当該情報に基づいて防犯機能を動作させる処理を行う。

【0039】

（操作者撮影部の具体的な処理）

CPUは、制御プログラムを実行するべきとの信号を受け付けると「操作者撮影プログラム」0412を実行し、操作者を撮影するための処理を行う。

【0040】

（記録保持部の具体的な処理）

CPUは、操作者撮影プログラムの実行により得られた画像や撮影日時等の情報を読み出して「記録保持プログラム」0413を実行し、当該各情報を相互に紐づけてメインメモリの所定のアドレスに格納する。

【0041】

<処理の流れ>

図5は、本実施形態の防犯装置の処理の流れの一例を示す図である。同図の処理の流れは以下のステップからなる。最初にステップS0501では、防犯装置に対し何らかの操作があったかどうかを判断する処理を行う。操作があったとの判断がある場合にはステップS0502の処理に移行し、操作がないとの判断である場合には再びステップS0501の処理にもどる。ステップS0502では操作者を撮影する処理を行う（操作者撮影ステップ）。ステップS0503では、操作者撮影ステップにて撮影された画像を記録する（記録保持ステップ）。そしてステップS0504では、前記ステップS0501にて受け付けたと判断された操作内容に従い防犯機能を動作させる（防犯動作ステップ）。なお、図5においては、防犯動作ステップ処理は記録保持ステップの後に行われるものとして示したが、これはあくまで一例であり、防犯動作ステップは、ステップS0501の後であれば、どの段階で処理されてもよい。

10

【0042】

<効果>

以上の構成を有する本件発明により、防犯管理の観点から重要な地位にある施設最終退出者を特定することが可能になる。

【0043】

<<実施形態2>>

<概要>

本実施形態の防犯装置は、基本的に実施形態1の防犯装置と同様であるが、人間の顔画像を認識する機能を有し、前記制御操作があった場合に操作者の顔画像が認識できない場合には操作を無効とすることをさらなる特徴として備えている。当該構成を備えることにより、他人による操作者の「なりすまし」を防止し、施設内の防犯管理上重要な地位を占める防犯装置の操作者が誰であるかを正確かつ確実に捉えることが可能になる。

20

【0044】

<機能的構成>

図6は、本実施形態の防犯装置の機能ブロックの一例を示す図である。この図にあるように、本実施形態の「防犯装置」0600は、「制御部」0601と、「防犯動作部」0602と、「操作者撮影部」0603と、「記録保持部」0604と、「顔画像認識手段」0605と、を有する。基本的な構成は実施形態1の図2を用いて説明した防犯装置と共通するため、以下では相違点である顔画像認識手段の機能について説明する。

30

【0045】

「顔画像認識手段」0605は、操作者の顔を識別する機能を有している。「顔を識別する」とは、例えば、あらかじめ人間の顔を構成する目や鼻、あごなどの各パーツが位置する平均的な座標の位置情報を記憶しておき、当該位置情報を参照して撮影された映像のうち人間の顔と思われる部分を抽出し、画像中の顔に相当する部分を特定する方法が考えられる。そして、具体的な識別方法としては、前記特徴的なパーツの相対位置や大きさなどの情報に基づき、撮影された顔画像をあらかじめ登録している顔画像データベースと照合する方法が考えられる。顔画像データベースにはスタッフの顔画像のデータをスタッフの氏名や性別、所属部署、役職、勤務年数、スタッフIDなどとともに登録しておき、撮影された顔画像が当該データベースに登録されているデータとの整合性を判断することが考えられる。

40

【0046】

ここで、考えられる処理の一例としては、整合性があると判断される場合には当該操作者における操作を有効なものとして操作内容に従った処理を行い、前記データベースに登録されていない顔画像であると判断される場合には、当該操作者による操作を無効とし、何らの制御も行わないものとすることが考えられる。何らの制御も行わないのみならず、不審者による操作がなされたものと判断し、非正常事態が生じているものとして当該検知結果の出力処理をおこなってもよい。なおこのとき、本実施形態の防犯装置の記録保持部においては、前記スタッフIDを撮影した画像等とともに記録する構成をとってもよい。当該構成をとることにより、例えば、他の施設スタッフの制服や名札を着用し、当該名札

50

等のみを撮影させることで自らが防犯装置を操作した事実を隠ぺいする「なりすまし」を排除することが可能になる。

【 0 0 4 7 】

なお、顔識別のアルゴリズムとしては、上述した幾何学的方法に限られるものではなく、例えば、一般的な人間の顔画像および各個人の顔画像の情報を統計的に数値化してテンプレートとして保持しておき、撮影された顔画像を数値化したものと比較する方法であってもよく、その他、特定のアルゴリズムを排除するものではない。

【 0 0 4 8 】

<具体的な構成>

本実施形態の防犯装置のハードウェア構成は、基本的には図4を用いて説明した実施形態1の防犯装置のハードウェア構成と同様であるので、以下では、これまで説明していない顔画像認識手段の具体的な処理について説明する。

【 0 0 4 9 】

(顔画像認識手段の具体的な処理)

CPUは、制御プログラムを実行すべきとの信号を受け付けると「顔画像認識プログラム」を実行し、操作者の顔を認識する処理を行い、その処理結果をメインメモリの所定のアドレスに格納する。そしてCPUは、前記処理結果が顔画像を認識できた場合に限り操作内容を実行する処理を行う。

【 0 0 5 0 】

<処理の流れ>

図7は、本実施形態の防犯装置の処理の流れの一例を示す図である。同図の処理の流れは、以下のステップからなる。最初にステップS0701では、防犯装置に対し何らかの操作があったかどうかを判断する処理を行う。操作があったとの判断がある場合にはステップS0702の処理に移行し、操作がないとの判断である場合には再びステップS0701の処理に戻る。ステップS0702では操作者を撮影する処理を行い(操作者撮影ステップ)、ステップS0703の処理に移行する。ステップS0703では、操作者撮影ステップにて撮影された画像を記録する(記録保持ステップ)。その後ステップS0704では、操作者撮影ステップにて撮影された画像を顔画像として認識できるかどうかを判断する処理を行う(顔画像認識ステップ)。ここで認識できないとの判断結果である場合には、ステップS0701の処理に戻り、認識可能であるとの判断結果である場合にはステップS0705の処理に移行する。そしてステップS0705では、入力を受け付けた操作内容に従い防犯機能を動作させる(防犯動作ステップ)。なお、図7においては、記録保持ステップは、顔画像認識ステップ以前の処理として示したが、これはあくまで一例であり、記録保持ステップは、操作者撮影ステップの後であれば、どの段階で処理されてもよい。

【 0 0 5 1 】

<効果>

本実施形態の防犯装置によって、実施形態1において説明した効果のほか、施設内の防犯管理上重要な地位を占める防犯装置の操作者が誰であるかを正確かつ確実に捉えることが可能になる。

【 0 0 5 2 】

<<実施形態3>>

<概要>

本実施形態の防犯装置は、基本的に実施形態1又は2の防犯装置と同様であるが、制御をおこなう際に防犯機能を起動させる機能を有する点を特徴として備えている。当該特徴を備える構成とすることにより、防犯機能を起動させる内容の入力操作が行われた際に当該操作者を撮影することが可能になり、防犯対策の構築上極めて重要な立場にある防犯機能起動操作者をピンポイントで特定することが可能になる。

【 0 0 5 3 】

<機能的構成>

図 8 は、本実施形態の防犯装置の機能ブロックの一例を示す図である。この図にあるように、本実施形態の「防犯装置」0800は、「制御部」0801と、「防犯動作部」0802と、「操作者撮影部」0803と、「記録保持部」0804と、「起動手段」0805と、を有する。基本的な構成は実施形態1の図2を用いて説明した防犯装置と共通するため、以下では相違点である起動手段について説明する。

【0054】

「起動手段」は、防犯動作部を起動させるための機能を有する。既に説明したように、前記操作者撮影部は、制御部に対する操作があった場合に操作者を撮影する機能を有している。本実施形態の防犯装置においては制御部が起動手段を有しているため、防犯動作部を起動させることを目的として制御部に対する操作があった際に操作者撮影部にて操作者の撮影が行われることとなる。防犯装置の起動は通常、施設内に最後に残った人物が退出の際に行う操作内容であることから、当該人物を撮影する構成を備えることにより、施設内を最後に退出した人物を明確に特定することが可能になる。

10

【0055】

<具体的な構成>

本実施形態の防犯装置のハードウェア構成は、基本的に図4を用いて説明した実施形態1の防犯装置のハードウェア構成と同様である。そこで以下では、これまで説明していない起動手段の具体的な処理について説明する。

【0056】

(起動手段の具体的な処理)

CPUは、防犯機能を起動させるべきとの信号の入力を受け付けると「起動プログラム」を実行し、防犯動作プログラムを実行するよう処理を行う。

20

【0057】

<具体的な処理>

図9は、本実施形態の防犯装置の処理の流れの一例を示す図である。同図の処理の流れは、以下のステップからなる。最初にステップS0901では、防犯装置に対し防犯機能の起動を促す内容の操作があったかどうかを判断する処理を行う。操作があったとの判断がある場合にはステップS0902の処理に移行し、操作がないとの判断である場合には再びステップS0901の処理にもどる。ステップS0902では操作者を撮影する処理を行う(操作者撮影ステップ)。ステップS0903では、操作者撮影ステップにて撮影された画像を記録する(記録保持ステップ)。いっぽうステップS0904では、入力を受け付けた操作内容に従い防犯機能を起動させる(防犯動作起動ステップ)。なお、図9においては、記録保持ステップは、防犯動作起動ステップ以前の処理として示したが、これはあくまで一例であり、記録保持ステップは、操作者撮影ステップの後であれば、どの段階で処理されてもよい。

30

【0058】

<効果>

本実施形態の防犯装置によって、防犯対策の構築上極めて重要な立場にある防犯機能起動操作者をピンポイントで特定することが可能になる。

【0059】

<<実施形態4>>

<概要>

本実施形態の防犯装置は、基本的に実施形態1から3のいずれか一に記載の防犯装置と同様であるが、防犯空間を撮影する機能をさらに有する点を特徴としている。当該構成を特徴として備えることにより、防犯機能作動後に防犯装置の操作が行われていない状態であっても、防犯空間の様子を映像で確認することが可能になる。

【0060】

<機能的構成>

図10は、本実施形態の防犯装置の機能ブロックの一例を示す図である。この図にあるように、本実施形態の「防犯装置」1000は、「制御部」1001と、「防犯動作部」

40

50

１００２と、「操作者撮影部」１００３と、「記録保持部」１００４と、「撮影部」１００５と、を有する。基本的な構成は実施形態１の図２を用いて説明した防犯装置と共通するため、以下では相違点である撮影部について説明する。

【００６１】

「撮影部」１００５は、防犯空間を撮影する機能を有する。ここでいう「防犯空間」は、防犯装置の動作対象として期待されるあらゆる空間を含む概念であり、屋内空間であると屋外空間であるとを特に問わない。具体的な撮影の方法については操作者撮影部に関する説明において既に説明した内容と同様であり、静止画や動画の種別を問わない。なお、撮影部にて撮影された記録は、前記記録保持部にて保持される構成をとることが考えられる。

10

【００６２】

なお、「防犯空間を撮影する」とは、前記防犯対象と位置付けられる特定の空間を撮影することを指しており、操作者のみを撮影する機能を備える前記操作者撮影部の機能とは区別される。しかし、操作者撮影部において撮影部の有する機能をも併せ備えるような構成、すなわち両部の機能を一の機能ブロックにて実現可能とする構成をとってもよい。このような構成を採用することにより、防犯装置全体の構造を簡略化することが可能になる。

【００６３】

<具体的な構成>

本実施形態の防犯装置のハードウェア構成は、基本的に図４を用いて説明した実施形態１の防犯装置のハードウェア構成と同様である。そこで以下では、これまで説明していない撮影部の具体的な処理について説明する。

20

【００６４】

（撮影部の具体的な処理）

ＣＰＵは、制御プログラムの実行により得られた情報を読み出して「撮影プログラム」を実行し、防犯空間を撮影するための処理を行う。そして撮影の結果得られた情報をメインメモリの所定のアドレスに格納する。

【００６５】

<処理の流れ>

図１１は、本実施形態の防犯装置の処理の流れの一例を示す図である。同図の処理の流れは以下のステップからなる。最初にステップＳ１１０１では、防犯装置に対し何らかの操作があったかどうかを判断する処理を行う。操作があったとの判断がある場合にはステップＳ１１０２の処理に移行し、操作がないとの判断である場合には再びステップＳ１１０１の処理にもどる。ステップＳ１１０２では操作者を撮影する処理を行う（操作者撮影ステップ）。ステップＳ１１０３では、操作者撮影ステップにて撮影された画像を記録する（記録保持ステップ）。いっぽうステップＳ１１０４では、入力を受け付けた操作内容に従い防犯空間の撮影処理を行う（撮影ステップ）。なお、図１１においては、記録保持ステップは、撮影ステップ以前の処理として示したが、これはあくまで一例であり、記録保持ステップは、操作者撮影ステップの後であれば、どの段階で処理されてもよい。

30

【００６６】

<効果>

以上のような構成を備える防犯装置により、実施形態１において説明した効果のほか、防犯機能作動後に防犯装置の操作が行われていない状態であっても、防犯空間の様子を映像で確認することが可能になる。

40

【００６７】

<<実施形態５>>

<概要>

本実施形態の防犯装置は、基本的に実施形態３および４のいずれに記載の機能をも備えた防犯装置と同様であるが、撮影開始からの時間経過に応じて撮影機能を制御することを特徴としている。当該構成を特徴として備えることにより、防犯機能起動時から操作者退

50

出時までの施設内の様子をチェックすることが可能になる。

【 0 0 6 8 】

<機能的構成>

図 1 2 は、本実施形態の防犯装置の機能ブロックの一例を示す図である。この図にあるように、本実施形態の「防犯装置」1 2 0 0 は、「制御部」1 2 0 1 と、「防犯動作部」1 2 0 2 と、「操作者撮影部」1 2 0 3 と、「記録保持部」1 2 0 4 と、「起動手段」1 2 0 5 と、「経過時間制御手段」1 2 0 6 と、「撮影部」1 2 0 7 と、を有する。基本的な構成は実施形態 1 の図 2 を用いて説明した防犯装置と共通するため、以下では相違点である経過時間制御手段について説明する。

【 0 0 6 9 】

「経過時間制御手段」1 2 0 6 は、制御部の起動手段が操作されることによって防犯動作部による防犯空間の撮影が開始される場合に、撮影開始からの時間経過に応じて撮影部を制御する機能を有する。「撮影開始からの時間経過に応じて撮影部を制御する」とは、撮影を行う時間やタイミング等を制御することが考えられ、例えば、撮影開始後所定時間撮影を継続し（例えば、1 コマ / 秒の間隔で 1 0 秒間撮影を行う）その後は各種センサ等により非正常事態を検知するまで撮影をおこなわないなどといったタイミングで撮影部を制御することが考えられる。撮影部にて動画を撮影する場合においては、防犯動作中動画を継続的に撮影することとなるが、このような場合、たとえ正常状態が長時間継続していてもその間絶えず動画撮影を行うこととなり、撮影のために要する電力等のエネルギーが無駄になってしまっていた。しかしながら当該構成を採用することにより、防犯機能起動時と非正常事態検知時とのみに焦点を絞ったピンポイント撮影が可能になるため、防犯の目的を省エネルギーにて実現することが可能になる。

【 0 0 7 0 】

<具体的な構成>

本実施形態の防犯装置のハードウェア構成は、基本的に図 4 を用いて説明した実施形態 1 の防犯装置のハードウェア構成と同様である。そこで以下では、これまで説明していない経過時間制御手段の具体的な処理について説明する。

【 0 0 7 1 】

（経過時間制御手段の具体的な処理）

C P U は、撮影プログラムを実行するとともに「経過時間制御プログラム」を実行し、撮影開始以降時間経過に応じて撮影を行うよう撮影プログラムを制御する処理を行う。

【 0 0 7 2 】

<処理の流れ>

図 1 3 は、本実施形態の防犯装置の処理の流れの一例を示す図である。同図の処理の流れは以下のステップからなる。最初にステップ S 1 3 0 1 では、防犯装置に対し防犯機能の起動を促す内容の操作があったかどうかを判断する処理を行う。操作があったとの判断がある場合にはステップ S 1 3 0 2 の処理に移行し、操作がないとの判断である場合には再びステップ S 1 3 0 1 の処理にもどる。ステップ S 1 3 0 2 では操作者を撮影する処理を行う（操作者撮影ステップ）。ステップ S 1 3 0 3 では、操作者撮影ステップにて撮影された画像を記録する（記録保持ステップ）。いっぽうステップ S 1 3 0 4 では、撮影開始時からの時間経過に応じた所定の時間及びタイミングにて撮影を行う（経過時間撮影ステップ）。なお、図 1 3 においては、記録保持ステップは、経過時間撮影ステップ以前の処理として示したが、これはあくまで一例であり、記録保持ステップは、操作者撮影ステップの後であれば、どの段階で処理されてもよい。

【 0 0 7 3 】

<効果>

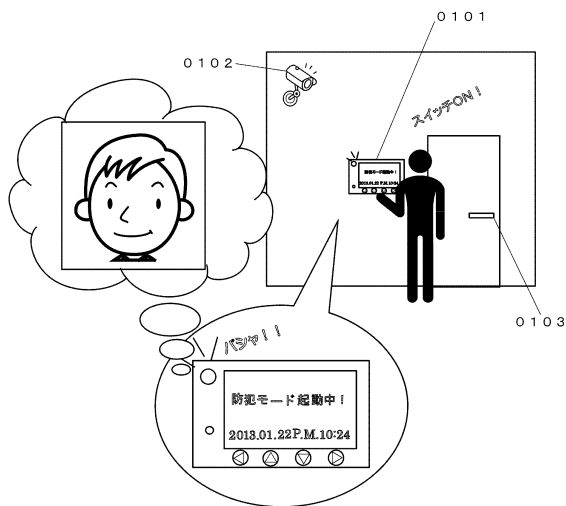
以上のような構成を備える防犯装置により、実施形態 3 や 4 などにおいて説明した効果のほか、防犯機能起動時から操作者退出時までの施設内の様子をチェックすることが可能になる。

【符号の説明】

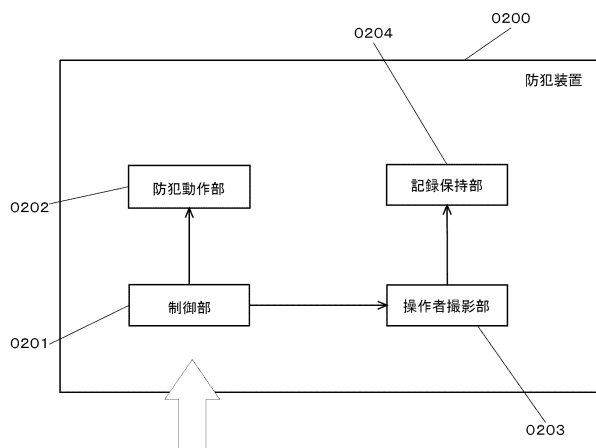
【 0 0 7 4 】

0 3 0 1 ... エアコン、0 3 0 2 ... 防犯装置、0 3 0 3 ... テレビ、0 3 0 4 ... P C、0 3
0 5 ... 照明器具、0 3 0 6 ... 電気自動車、0 3 0 7 ... ホームゲートウェイ、0 3 0 8 ... ス
マートメーター、0 4 2 0 ... 施設スタッフ I D、0 4 2 1 ... 撮影記録情報、1 4 0 1 ... 電
源起動ボタン

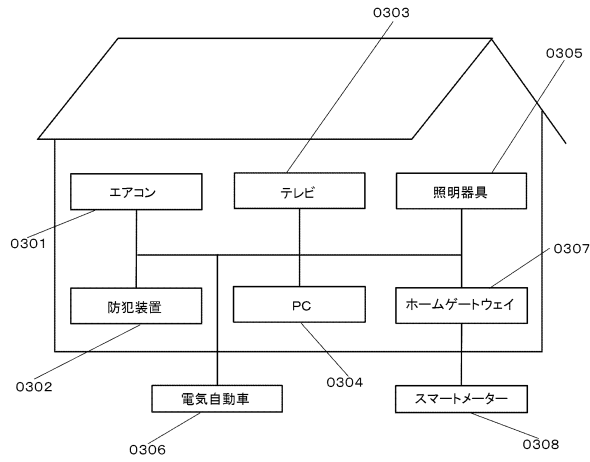
【 図 1 】



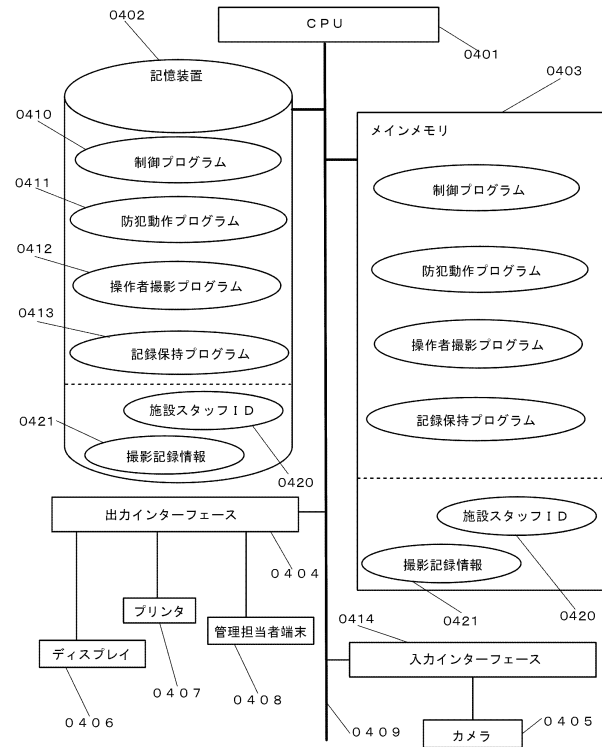
【 図 2 】



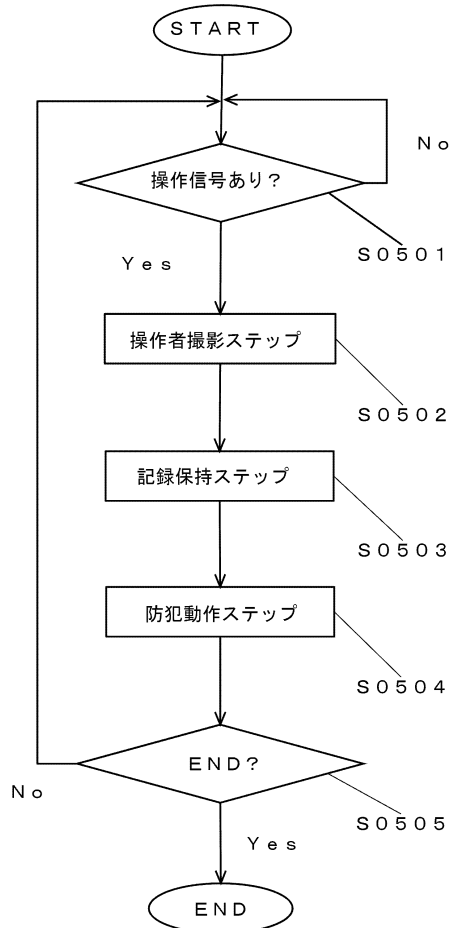
【図 3】



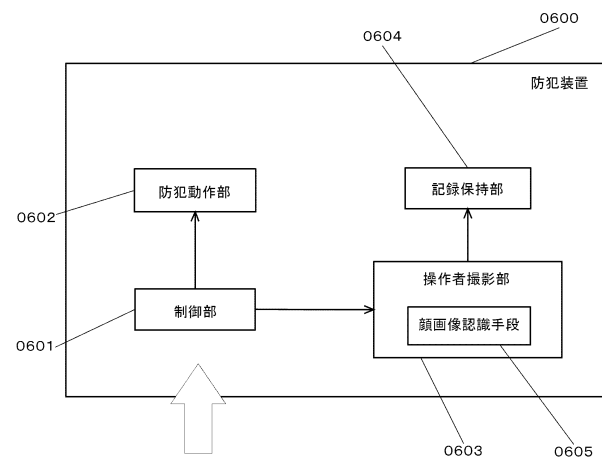
【図 4】



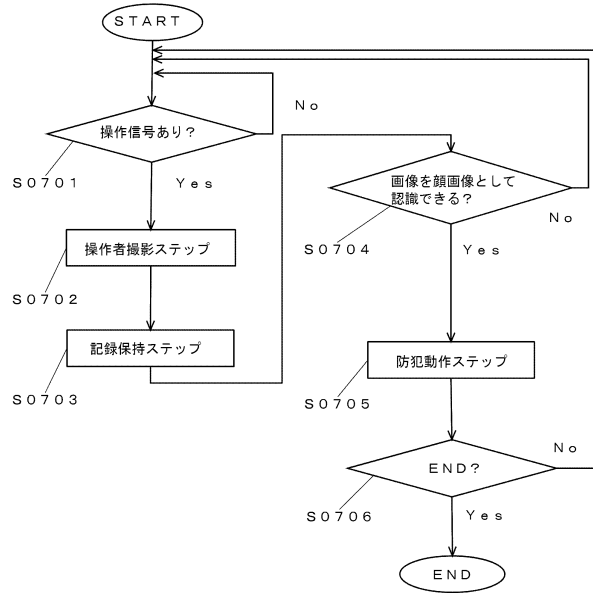
【図 5】



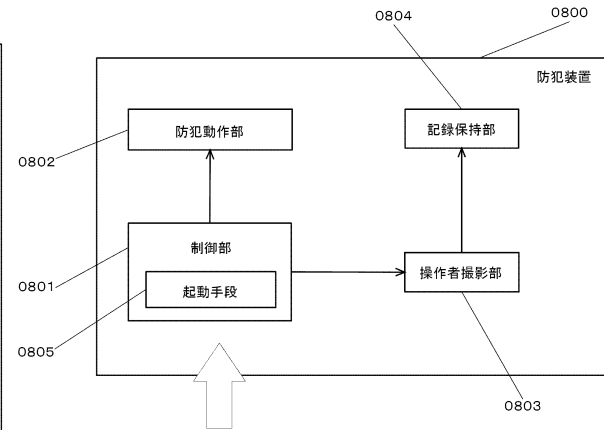
【図 6】



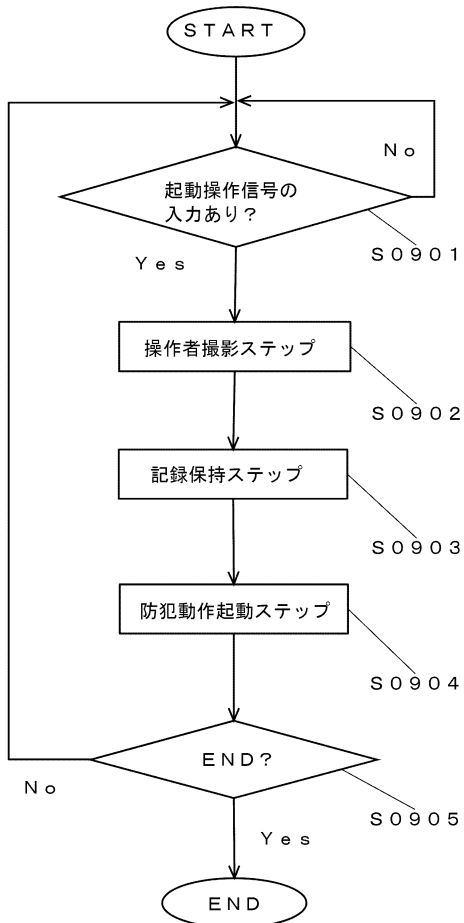
【図 7】



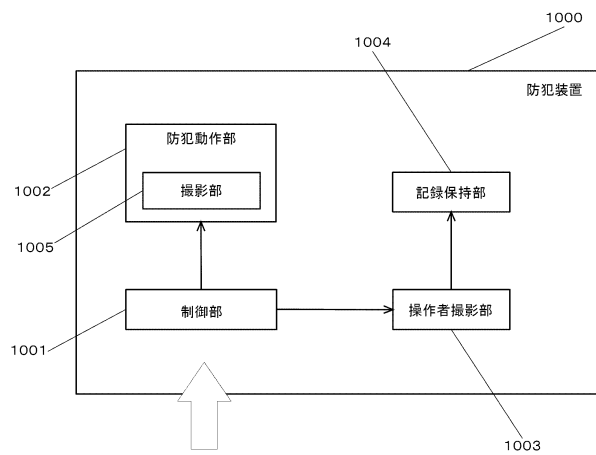
【図 8】



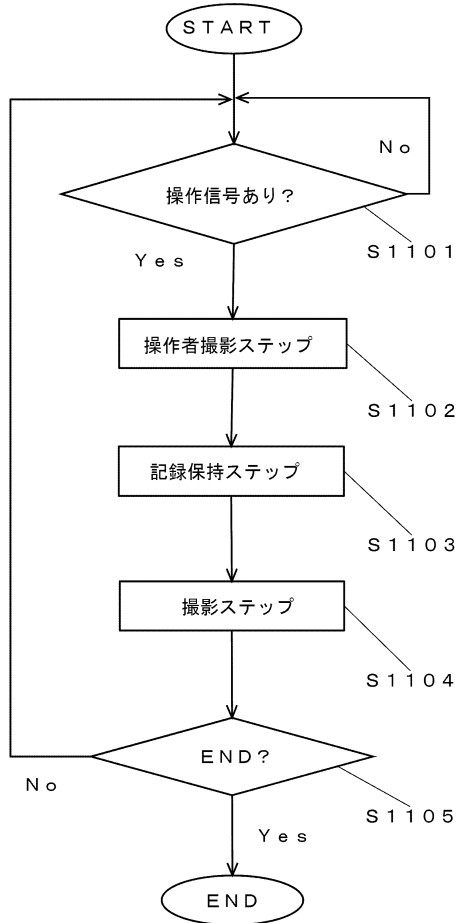
【図 9】



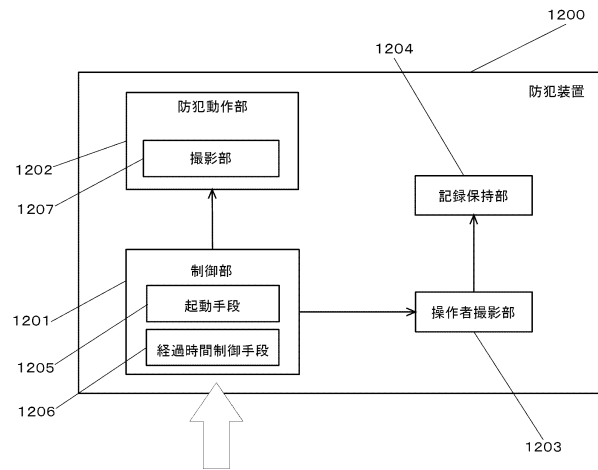
【図 10】



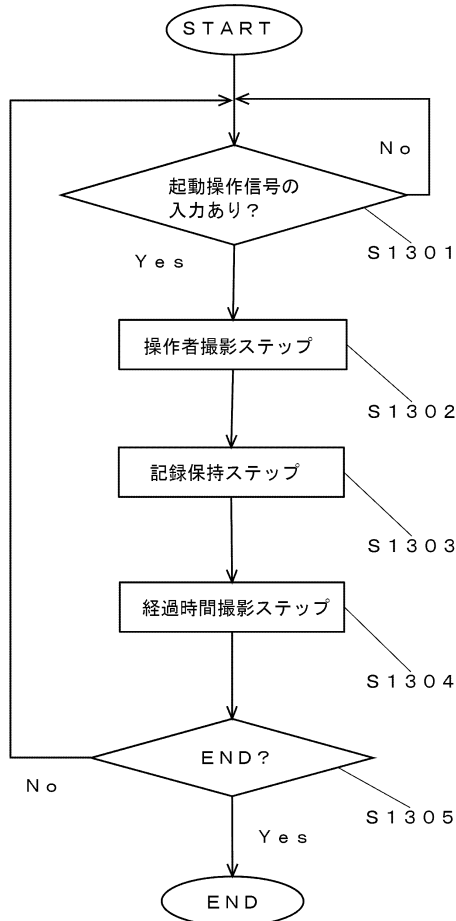
【図 1 1】



【図 1 2】



【図 1 3】



1404



防犯キー一下
(長押し)

● — 電源



省工本

COO 總辦

電氣 料金

デマンド

家毛一卜
(長押し)



1401

1402

1403

フロントページの続き

- (56)参考文献 特開2004-260438(JP,A)
特開平7-29074(JP,A)
特開2003-228780(JP,A)
特開2012-182547(JP,A)
特開2007-201994(JP,A)
特開2002-207999(JP,A)
特開平11-288488(JP,A)
特開2001-52272(JP,A)
特開2005-61011(JP,A)
特開2004-260406(JP,A)
特開2004-252745(JP,A)
特開2003-30706(JP,A)

(58)調査した分野(Int.Cl., DB名)

G08B25/00, G08B13/196, G08B25/04