(19)日本国特許庁(JP)

再公表特許(A1)

(11)国際公開番号
WO2020/174634

発行日　令和3年3月11日(2021.3.11)

(43)国際公開日　令和2年9月3日(2020.9.3)

(51)Int.Cl.		F I			テーマコード（参考）
H04N 7/18	(2006.01)	H04N	7/18	D	5C054
G08B 13/196	(2006.01)	G08B	13/196		5C084
G08B 25/00	(2006.01)	G08B	25/00	510M	5C087
G08B 25/08	(2006.01)	G08B	25/08	A	

審査請求 有　予備審査請求 未請求　（全 38 頁）

出願番号　特願2019-518115 (P2019-518115)
(21)国際出願番号　PCT/JP2019/007706
(22)国際出願日　平成31年2月27日 (2019.2.27)
(11)特許番号　特許第6529062号 (P6529062)
(45)特許公報発行日　令和1年6月12日 (2019.6.12)

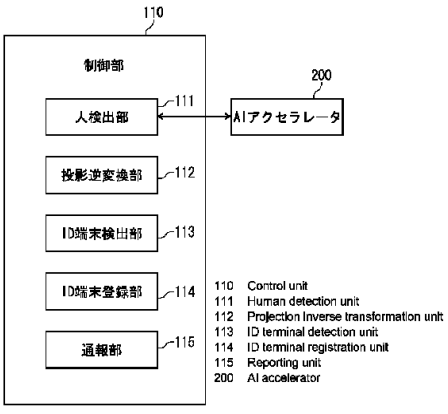
(71)出願人　505048518
株式会社　テクノミライ
東京都新宿区高田馬場１－３３－１３
(74)代理人　100110191
弁理士　中村　和男
(72)発明者　三輪　和夫
東京都新宿区高田馬場１－３３－１３　株式会社　テクノミライ内

Fターム(参考)　5C054 CF06 DA09 FC12 FE16 FE17 FF06 HA18
5C084 AA02 AA07 BB21 DD11 EE03 EE04 FF02 GG17 GG18 GG19 GG51 GG75 HH02 HH12 HH13

最終頁に続く

(54)【発明の名称】デジタルアキュレート・セキュリティシステム、方法及びプログラム

(57)【要約】
低コストで３次元位置を検出して、３次元のセキュリティ区域内の侵入者を正確に検出して高度なセキュリティを確立することができるデジタルアキュレート・セキュリティシステム、方法及びプログラムを提供する。デジタルアキュレート・セキュリティシステム（１０００）は、監視カメラ（１１）によって撮影された３次元空間内の各位置とを対応付けて記憶する投影記憶部（１３５）と、監視カメラ（１１）によって撮影された画像から人を検出する人検出部（１１１）と、人検出によって検出された人の２次元の位置と人の大きさとに基づいて、投影記憶部（１３５）によって人の３次元空間内の位置を検出する投影逆変換部（１１２）と、投影逆変換部（１１２）によって検出された人の３次元空間内の位置が３次元のセキュリティ区域内であることを受けて、不審者の存在を通報する通報部（１１５）とを備える。



【特許請求の範囲】
【請求項１】
３次元のセキュリティ区域の画像を撮影する撮影手段と、
前記撮影手段によって撮影された前記画像の２次元の各位置と前記撮影手段によって撮影された３次元空間内の各位置とを対応付けて記憶する投影記憶手段と、
前記撮影手段によって撮影された前記画像から人を検出する人検出手段と、
前記人検出によって検出された人の２次元の位置と人の大きさとに基づいて、前記投影記憶手段によって前記人の３次元空間内の位置を検出する投影逆変換手段と、
前記投影逆変換手段によって検出された人の３次元空間内の位置が３次元のセキュリティ区域内であることを受けて、不審者の存在を通報する通報手段と
を備えることを特徴とするデジタルアキュレート・セキュリティシステム。
【請求項２】
前記通報手段は、前記検出された人の３次元空間内の位置の時間的経緯によって不審者の存在を判断し、その存在を通報することを特徴とする請求項１記載のデジタルアキュレート・セキュリティシステム。
【請求項３】
前記人の大きさが人の頭の大きさであることを特徴とする請求項１記載のデジタルアキュレート・セキュリティシステム。
【請求項４】
前記通報手段は、前記不審者の位置に基づく危険度を通報することを特徴とする請求項１記載のデジタルアキュレート・セキュリティシステム。
【請求項５】
前記通報手段は、前記不審者の動きに基づく危険度を通報することを特徴とする請求項１記載のデジタルアキュレート・セキュリティシステム。
【請求項６】
非侵入者が所持するＩＤ（Identification）端末を検出するＩＤ端末検出手段を備え、
前記通報手段は、前記ＩＤ端末検出手段が検出した前記ＩＤ端末を所持している人を通報しないことを特徴とする請求項１記載のデジタルアキュレート・セキュリティシステム。
【請求項７】
非侵入者が所持するＩＤ（Identification）端末を登録するＩＤ端末登録手段を備え、
前記通報手段は、前記ＩＤ端末登録手段が登録した前記ＩＤ端末を所持している人を通報しないことを特徴とする請求項１記載のデジタルアキュレート・セキュリティシステム。
【請求項８】
３次元のセキュリティ区域の画像を撮影する撮影ステップと、
前記撮影ステップによって撮影された前記画像の２次元の各位置と前記撮影ステップによって撮影された３次元空間内の各位置とを対応付けて記憶する投影記憶ステップと、
前記撮影ステップによって撮影された前記画像から人を検出する人検出ステップと、
前記人検出ステップによって検出された人の２次元の位置と人の大きさとに基づいて、前記投影記憶ステップによって前記人の３次元空間内の位置を検出する投影逆変換ステップと、
前記投影逆変換ステップによって検出された人の３次元空間内の位置が３次元のセキュリティ区域内であることを受けて、不審者の存在を通報する通報ステップと
を備えることを特徴とするデジタルアキュレート・セキュリティ方法。
【請求項９】
コンピュータを、
３次元のセキュリティ区域の画像を撮影する撮影手段と、前記撮影手段によって撮影された前記画像の２次元の各位置と前記撮影手段によって撮影された３次元空間内の各位置とを対応付けて記憶する投影記憶手段と、前記撮影手段によって撮影された前記画像から

人を検出する人検出手段と、前記人検出によって検出された人の２次元の位置と人の大きさとに基づいて、前記投影記憶手段によって前記人の３次元空間内の位置を検出する投影逆変換手段と、前記投影逆変換手段によって検出された人の３次元空間内の位置が３次元のセキュリティ区域内であることを受けて、不審者の存在を通報する通報手段とを備えるデジタルアキュレート・セキュリティシステム
として機能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、監視カメラによりセキュリティ区域内を撮影して防犯を行うデジタルアキュレート・セキュリティシステム、方法及びプログラムに関する。
【背景技術】
【０００２】
特許文献１には、「２つのカメラを備え、注視領域の３次元情報に基づいて侵入した物体を検知すること」が記載されている。特許文献１の技術は、３次元情報の変化状況に基づいて、注視領域に侵入した物体を検知するものである。
【０００３】
特許文献２には、「投光から受光までの時間差により物体までの距離を検出して、３次元の警戒エリアと３次元の監視エリアを設定すること」が記載されている。特許文献２の技術は、距離画像センサから時間経過に伴って出力される複数の距離画像により警戒エリアと監視エリアとにおける物体の振る舞いを監視し、物体の振る舞いから物体の種別を判別するものである。
【先行技術文献】
【特許文献】
【０００４】
【特許文献１】特開２０１８－１７３９７６号公報
【特許文献２】特開２０１１－４８５９４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１，２に記載の警報装置では、３次元位置を検出するための構成が複雑でコストがかさむ課題がある。
本発明の目的は、低コストで３次元位置を検出して、高度なセキュリティを確立することができるデジタルアキュレート・セキュリティシステム、方法及びプログラムを提供することにある。
【課題を解決するための手段】
【０００６】
本発明に係るデジタルアキュレート・セキュリティシステムは、３次元のセキュリティ区域の画像を撮影する撮影手段と、前記撮影手段によって撮影された前記画像の２次元の各位置と前記撮影手段によって撮影された３次元空間内の各位置とを対応付けて記憶する投影記憶手段と、前記撮影手段によって撮影された前記画像から人を検出する人検出手段と、前記人検出によって検出された人の２次元の位置と人の大きさとに基づいて、前記投影記憶手段によって前記人の３次元空間内の位置を検出する投影逆変換手段と、前記投影逆変換手段によって検出された人の３次元空間内の位置が３次元のセキュリティ区域内であることを受けて、不審者の存在を通報する通報手段とを備えることを特徴とする。
【０００７】
この構成により、低コストで３次元位置を検出して、高度なセキュリティを確立することができる。
【０００８】

前記通報手段は、前記検出された人の３次元空間内の位置の時間的経緯によって不審者の存在を判断し、その存在を通報することで、時間的経緯を考慮して、侵入者の３次元位置を判定することができる。

【０００９】

前記人の大きさが人の頭の大きさであることで、人の大きさを示す指標として、人の年齢や性別等であまり変化のない個人差によらない情報をもとに、侵入者の３次元位置を判定することができる。

【００１０】

前記通報手段は、前記不審者の位置に基づく危険度を通報することで、危険度に合わせてより迅速に侵入犯罪に対応することができる。また、危険度に合わせたテロップの送信や関係機関への通報を行うことができる。

【００１１】

前記通報手段は、前記不審者の動きに基づく危険度を通報することで、不審者の動きを判定条件に加えて危険度の判定をより精度良く行うことができ、高度なセキュリティを確立することができる。例えば、不審者の動きをもとに、善意の人か悪意のある侵入者かの区別、さらに侵入者の場合には危険度を判定し、危険度に合わせて警戒の状態をランク付けすることができる。

【００１２】

非侵入者が所持するＩＤ（Identification）端末を検出するＩＤ端末検出手段を備え、前記通報手段は、前記ＩＤ端末検出手段が検出した前記ＩＤ端末を所持している人を通報しないことで、例えば家族及び関係者のスマートフォンを検出して不審者から除外し、無駄な通報を削減して監視の実効を図ることができる。また、監視におけるリソースを低減して、低コスト化を図ることができる。

【００１３】

非侵入者が所持するＩＤ（Identification）端末を登録するＩＤ端末登録手段を備え、前記通報手段は、前記ＩＤ端末登録手段が登録した前記ＩＤ端末を所持している人を通報しないことで、例えば来客のＩＤを登録して不審者から除外し、無駄な通報を削減して監視の実効を図ることができる。また、監視におけるリソースを低減して、低コスト化を図ることができる。

【００１４】

また、本発明のデジタルアキュレート・セキュリティ方法は、３次元のセキュリティ区域の画像を撮影する撮影ステップと、前記撮影ステップによって撮影された前記画像の２次元の各位置と前記撮影ステップによって撮影された３次元空間内の各位置とを対応付けて記憶する投影記憶ステップと、前記撮影ステップによって撮影された前記画像から人を検出する人検出ステップと、前記人検出ステップによって検出された人の２次元の位置と人の大きさとに基づいて、前記投影記憶ステップによって前記人の３次元空間内の位置を検出する投影逆変換ステップと、前記投影逆変換ステップによって検出された人の３次元空間内の位置が３次元のセキュリティ区域内であることを受けて、不審者の存在を通報する通報ステップとを備えることを特徴とする。

【００１５】

また、本発明は、コンピュータを、３次元のセキュリティ区域の画像を撮影する撮影手段と、前記撮影手段によって撮影された前記画像の２次元の各位置と前記撮影手段によって撮影された３次元空間内の各位置とを対応付けて記憶する投影記憶手段と、前記撮影手段によって撮影された前記画像から人を検出する人検出手段と、前記人検出によって検出された人の２次元の位置と人の大きさとに基づいて、前記投影記憶手段によって前記人の３次元空間内の位置を検出する投影逆変換手段と、前記投影逆変換手段によって検出された人の３次元空間内の位置が３次元のセキュリティ区域内であることを受けて、不審者の存在を通報する通報手段とを備えるデジタルアキュレート・セキュリティシステムとして機能させるためのプログラムである。

【発明の効果】

【００１６】
本発明によれば、１つのカメラによって低コストで不審者の３次元位置を検出して、高度なセキュリティを確立することができる。
【図面の簡単な説明】
【００１７】
【図１】本発明の実施の形態に係るデジタルアキュレート・セキュリティシステムの構成を示すブロック図である。
【図２】本発明の実施の形態に係るデジタルアキュレート・セキュリティシステムの制御部のブロック図である。
【図３】本発明の実施の形態に係るデジタルアキュレート・セキュリティシステムを用いた全体を示す構成図である。
【図４】本発明の実施の形態に係るデジタルアキュレート・セキュリティシステムのセキュリティアプリ動作を示す図である。
【図５】本発明の実施の形態に係るデジタルアキュレート・セキュリティシステムの警備モード設定処理を示すフローチャートである。
【図６】本発明の実施の形態に係るデジタルアキュレート・セキュリティシステムの個人住宅における警備の例を示す図である。
【図７】本発明の実施の形態に係るデジタルアキュレート・セキュリティシステムの集合住宅における警備の例を示す図である。
【図８Ａ】本発明の実施の形態に係るデジタルアキュレート・セキュリティシステムのデジタルアキュレート・セキュリティ処理を示すフローチャートである。
【図８Ｂ】本発明の実施の形態に係るデジタルアキュレート・セキュリティシステムのデジタルアキュレート・セキュリティ処理を示すフローチャートである。
【図９】本発明の実施の形態に係るデジタルアキュレート・セキュリティシステムの投影逆変換部による３次元位置検出処理を示すフローチャートである。
【図１０】本発明の実施の形態に係るデジタルアキュレート・セキュリティシステムの平面における侵入者検出の例を示す図である。
【図１１】本発明の実施の形態に係るデジタルアキュレート・セキュリティシステムの立面における侵入者検出の例を示す図である。
【図１２】本発明の実施の形態に係るデジタルアキュレート・セキュリティシステムの時間による侵入者検証の例を示す図である。
【図１３】本発明の実施の形態に係るデジタルアキュレート・セキュリティシステムが敷地境界をカメラ画像にマッピングする例を示す図である。
【図１４】本発明の実施の形態に係るデジタルアキュレート・セキュリティシステムが敷地内にあらかじめあるものの高さを登録する例を説明する図である。
【図１５】本発明の実施の形態に係るデジタルアキュレート・セキュリティシステムにおける人間の状態による高さの変化を説明する図である。
【図１６】本発明の実施の形態に係るデジタルアキュレート・セキュリティシステムにおける人間の状態による高さの変化を説明する図である。
【図１７】本発明の実施の形態に係るデジタルアキュレート・セキュリティシステムにおける瞳と首の動きの変化による判断を説明する図である。
【図１８】本発明の実施の形態に係るデジタルアキュレート・セキュリティシステムのBLEによる一時的な警備解除を説明する図である。
【図１９】本発明の実施の形態に係るデジタルアキュレート・セキュリティシステムによる侵入検出の適用例１を説明する図である。
【図２０】図１９の適用例１において、デジタルアキュレート・セキュリティシステム、家族、不審者の動作の概要を示すフローチャートである。
【図２１】本発明の実施の形態に係るデジタルアキュレート・セキュリティシステムによる侵入検出の適用例２を説明する図である。
【図２２】図２１の適用例２において、デジタルアキュレート・セキュリティシステムの

動作を示すフローチャートである。
【図２３】本発明の実施の形態に係るデジタルアキュレート・セキュリティシステムによる侵入検出の適用例３を説明する図である。
【図２４】図２３の適用例３において、デジタルアキュレート・セキュリティシステムの動作を示すフローチャートである。
【図２５】本発明の実施の形態に係るデジタルアキュレート・セキュリティシステムの適用例４において、注意度に応じて利用者に通知する処理を示すフローチャートである。
【発明を実施するための形態】
【００１８】
以下、添付図面を参照しながら本発明を実施するための形態について詳細に説明する。
（実施の形態）
図１は、本発明の実施の形態に係るデジタルアキュレート・セキュリティシステムの構成を示すブロック図である。
本デジタルアキュレート・セキュリティシステムは、住居、企業の事務所、工場、研究所、情報処理室、金銭集計室等の高度の管理を要する事業所等に適用して好適である。
【００１９】
図１に示すように、デジタルアキュレート・セキュリティシステム１０００は、セキュリティ区域のそれぞれに設置された１つの監視カメラ１１（撮影手段）と、人感センサ２０と、セキュリティ区域内に設置されたＷｉ-Ｆｉ（Wireless Fidelity）ターミナル（以下「Ｗｉ-Ｆｉ親機」という）３０と、ビーコン親機４０と、関係者（家族）が携帯する携帯端末装置５０（ＩＤ（Identification）端末）と、システム全体を制御する監視装置１００と、ＡＩ（Artificial Intelligence：人工知能）アクセラレータ（Accelerator）２００（人検出手段）と、を備える。セキュリティ区域は、警戒エリア（警備対象エリア）であり、例えば、住居であれば敷地や玄関先・ベランダ、オフィスであればエレベータホール・ベランダ・窓などを含む。
【００２０】
なお、監視装置１００は、セキュリティ区域内に設置されているが、図示しないネットワークを介して外部に設置してもよい。監視装置１００を、ネットワーク上のサーバに設置すると、複数のセキュリティ区域を監視対象とすることができる。
【００２１】
＜監視カメラ１１＞
監視カメラ１１は、３次元で特定されるセキュリティ区域の画像（２次元）を撮影する。
監視カメラ１１の一部又は全部は、ＰＴＺ（パン・チルト・ズーム）機能を有するＰＴＺカメラであり、監視装置１００により遠隔操作される。監視カメラ１１は、セキュリティ該当建物の警備対象の外壁周囲、例えば侵入者が出入可能な出入口、窓開口部、敷地境界外周部、該当敷地エリアの各所に設置される。監視カメラ１１が撮影した画像は、監視装置１００に出力され、録画部１６０に記録される。
【００２２】
＜人感センサ２０＞
人感センサ２０は、サーモカメラや赤外線カメラ等であり、セキュリティ区域内の感知対象物の温度を検出して、セキュリティ区域内の不審者を検出する。
【００２３】
＜Ｗｉ-Ｆｉ親機３０＞
Ｗｉ-Ｆｉ親機３０は、Ｗｉ-Ｆｉを用いて携帯端末装置５０のＷｉ-Ｆｉ子機５１との間で情報をやり取りする。また、Ｗｉ-Ｆｉ親機３０は、Ｗｉ-Ｆｉ測位による位置情報取得、すなわちＷｉ-Ｆｉアクセスポイントと所定の位置情報サービスを利用した位置情報を取得できる。
【００２４】
＜ビーコン親機４０＞

BLE（Bluetooth Low Energy）は、近接を検知する無線技術である。BLEは、発信側のビーコン機器であるビーコン親機４０と、ビーコン親機４０からの電波受信に対応した携帯端末装置５０のアプリ（後記ビーコン子機５２に対応する）の組み合わせによって構成される。BLEは、識別に必要な固有のＩＤ情報を発信し、携帯端末装置５０の当該ＩＤ情報に紐付けられたアプリにしか反応しない。携帯端末装置５０のアプリは、ビーコン親機４０と同じ識別子を登録しておく。携帯端末装置５０のアプリ（ビーコン子機５２）は、BLE機能を搭載したアプリケーション実行によりバックグラウンドで待機し、ビーコン親機４０のビーコンに近接したときに所定アクションを励起する。

【００２５】

［携帯端末装置５０］

携帯端末装置５０は、家族などがそれぞれ携帯する。携帯端末装置５０は、例えばスマートフォン５０ａ、タブレット５０ｂ、又はノートパソコン５０ｃなどである。携帯端末装置５０は、このほか、携帯電話、ＰＨＳ（Personal Handy-Phone System）、ＰＤＡ（Personal Digital Assistants）、又は専用端末などである。本実施の形態では、携帯端末装置５０は、家族などが様々な場所（すなわち現在位置）で使用可能であり、図示しない電話回線を介して監視装置１００からのメール又は動画を含む映像等を受信可能である。

【００２６】

本実施の形態では、携帯端末装置５０は、スマートフォン５０ａ（ＩＤ端末）の利用を想定しており、各個人が様々な場所（すなわち現在位置）で使用可能である。携帯端末装置５０のうちの一つは、図示しない警備会社に配置される。

【００２７】

スマートフォン５０ａは、デジタルアキュレート・セキュリティアプリ（以下、「セキュリティアプリ」という）を有する。セキュリティアプリを、例えば各アプリのバックグランド処理で起動させておくと、通信キャリア網（固定網）、ウェブサービスクラウド３００（後記図３参照）、又はインターネット３０３（後記図３参照）を経由して、ウェブサービスクラウド３００上のクラウドサーバ３０１（後記図３参照）に接続でき、クラウドサーバ３０１から不審者に関するテロップを受け取ることができる。スマートフォン５０ａは、待受け画面等に不審者を検出したテロップを通知できる。

【００２８】

スマートフォン５０ａは、Ｗｉ-Ｆｉ個別識別機（以下「Ｗｉ-Ｆｉ子機」という）５１と、関係者の位置を捕捉するＧＰＳ５３と、を備える。

なお、スマートフォン５０ａは、ビーコン子機５２を備えているものでもよい。又は、スマートフォン５０ａは、Ｗｉ-Ｆｉ子機５１と、ビーコン子機５２と、ＧＰＳ５３とのいずれか一つを備えるものでもよい。

【００２９】

＜Ｗｉ-Ｆｉ子機５１＞

Ｗｉ-Ｆｉ子機５１は、業務施設に設置されたＷｉ-Ｆｉ親機３０の電波を受信及び個別識別する。監視装置１００は、施設内に設置されたＷｉ-Ｆｉ親機３０の配置情報をセフティ関連情報として記憶している。Ｗｉ-Ｆｉ子機５１がＷｉ-Ｆｉ親機３０に近接すると、携帯端末装置５０を携帯する関係者のＩＤと位置を判定することができる。

【００３０】

＜ビーコン子機５２＞

ビーコン子機５２は、ビーコン親機４０からの電波受信に対応した携帯端末装置５０のアプリである。ビーコン親機４０は、ビーコン（識別に必要な固有のＩＤ情報）を発信し、携帯端末装置５０のアプリ（ビーコン子機５２）は、ビーコン親機４０のビーコンに近接したときに所定アクションを励起する。

【００３１】

＜ＧＰＳ５３＞

ＧＰＳ５３は、位置情報の電波をＧＰＳ衛星等から受信する。ＧＰＳ５３は、ＧＰＳアンテナを介して受信した情報より、現在位置情報を、緯度、経度及び高度の３つのパラメ

ータとして算出して位置情報を取得する。取得した位置情報は、適時、監視装置１００に送信される。

【００３２】

なお、本実施形態では、位置情報を取得する手段として、ＧＰＳ衛星を利用した例を示したが、ＧＰＳ以外の、基地局との位置関係を利用した方式でもよい。例えば、モバイル端末である携帯端末装置５０として、Ａｎｄｒｏｉｄ（登録商標）スマートフォンやカメラ付き高機能携帯電話機を使用する場合、ＧＰＳ５３に代えて又は併用して、基地局及び携帯電話通信網（図示省略）を介して携帯電話会社サーバと情報の送受信を行い、接近確認から自端末の現在位置情報を取得することも可能である。

【００３３】

また、Ｗｉ-Ｆｉ測位による位置情報取得、すなわちＷｉ-Ｆｉアクセスポイントと所定の位置情報サービスを利用した位置情報取得を用いてもよい。

【００３４】

［監視装置１００］

監視装置１００は、関係者（例えば家族）の住居に設置され、セキュリティ区域内を集中管理する。監視装置１００は、一般的なサーバ計算機、又はパーソナルコンピュータ等であってよい。

【００３５】

監視装置１００は、制御部１１０と、入力部１２０と、記憶部１３０と、投影記憶部１３５（投影記憶手段）と、表示部１４０と、出力部１５０と、録画部１６０（録画手段）と、顔情報ＤＢ（データベース）１６５と、画像処理部１７０と、インタフェース（Ｉ／Ｆ）部１８０と、通信部１９０と、を備え、各部はバス１９５により接続される。

【００３６】

以降、「○○部は」と主体を記した場合は、制御部１１０が必要に応じＲＯＭから各プログラムを読み出した上でＲＡＭにロードし、各機能（後記）を実行するものとする。各プログラムは、予め記憶部１３０に記憶されていてもよいし、他の記憶媒体又は通信媒体を介して、必要なときに監視装置１００に取り込まれてもよい。

【００３７】

制御部１１０は、ＣＰＵ（Central Processing Unit）等により構成され、監視装置１００全体を制御するとともに、制御プログラムを実行して、デジタルアキュレート・セキュリティシステムとして機能させる。制御部１１０の詳細な構成については、後記する。

【００３８】

入力部１２０は、キーボード、マウス、表示部１４０の画面上に設けられたタッチパネル、マイクなど、監視装置１００のユーザが指示などを入力するための入力機器である。

【００３９】

記憶部１３０は、ＲＯＭ（Read Only Memory）、ＲＡＭ（Random Access Memory）、ＥＰＲＯＭ（Electrically Erasable Programmable Read-Only Memory）などのメモリからなり、制御部１１０が用いる各種データ及びプログラムなどを記憶する。記憶部１３０は、監視カメラ１１から受信した静止画又は動画、制御部１１０が用いる各種データ及びプログラムなどを記憶する。

【００４０】

投影記憶部１３５は、監視カメラ１１によって撮影された画像の２次元の各位置と監視カメラ１１によって撮影された３次元空間内の各位置とを対応付けて記憶する。投影記憶部１３５は、３次元空間内に定義した形状を２次元面上に投影する投影変換によって対応付けて記憶する。

なお、投影記憶部１３５は、記憶部１３０のメモリ領域の一部を使用するものでもよい。

【００４１】

表示部１４０は、監視装置１００の動作状況をはじめ、監視カメラ１１から受信した画像、又は監視装置１００を操作するためのＧＵＩ（Graphical User Interface）などを表

示する。

【００４２】

出力部１５０は、例えばオーディオインタフェースであり、セキュリティ区域内の音響システム１５８に対して監視装置１００からの音声信号を出力する。監視装置１００から音響システム１５８へ出力する音声信号としては、例えば、入力部１２０に設けられたマイクなどの音声入力装置から入力された音声信号、又は記憶部１３０に記憶された音楽データを制御部１１０が再生した音声信号であってよい。音響システム１５８は、アンプ及び敷地内に配置された複数のスピーカを備え、監視装置１００から入力された信号を敷地内に発声する。

【００４３】

録画部１６０は、ＨＤＤ（Hard Disk Drive）などの外部記憶装置により構成され、監視カメラ１１が撮影したセキュリティ区域内の画像を記録する。録画部１６０は、撮影後所定の短時間は高画質で録画し、その所定の短時間経過後は低画質に変換して所定の長時間まで録画する。

【００４４】

顔情報ＤＢ１６５は、不審者、及び店舗関係者等の顔画像（顔情報）を蓄積する。顔情報ＤＢ１６５に登録されている人物の顔などの基礎データは、Ｉ／Ｆ部１８０を介して図示しない本部、本社又は警備会社などからデータを入手して、顔情報ＤＢ１６５が構築される。また、図示しない本部、本社又は警備会社などと情報を交換して、相互の顔情報ＤＢが最新の顔画像（顔情報）に更新可能である。

【００４５】

画像処理部１７０は、ＤＳＰ（Digital Signal Processor）等により構成され、受信した画像に対して予め定められた処理を行う。予め定められた処理には、輪郭抽出、画像のリサイズ、又は解像度変換処理などがある。

【００４６】

監視カメラ１１で１秒間に撮影する画像が例えば５コマの画像である場合、１／５秒画像、２／５秒画像、３／５秒画像、４／５秒画像、５／５秒画像の動きで、１秒間に１０コマの画像である場合には、１０個の画像の動きで、対象物の外形形状線を入力すれば、動く対象物の大きさが分かる。

画像処理部１７０は、監視カメラ１１で撮影された画像データを処理し、セキュリティ区域内の画像を出力する。

【００４７】

Ｉ／Ｆ部１８０は、セキュリティ区域内に配置された各監視カメラ１１と監視装置１００とを接続する。また、Ｉ／Ｆ部１８０は、図示しない本部、本社又は警備会社などにネットワーク又は専用回線により接続する。

通信部１９０は、基地局を介して携帯端末装置５０とデータを送受信する。通信部１９０は、無線通信機能を有し、例えばＵＡＲＴ（Universal Asynchronous Receiver Transmitter）を用いて制御基板に接続される。

【００４８】

［制御部１１０］

図２は、本発明の実施の形態に係るデジタルアキュレート・セキュリティシステムの制御部１１０のブロック図である。

図２に示すように、制御部１１０は、ＣＰＵ（Central Processing Unit）等により構成され、監視装置１００全体を制御するとともに、制御プログラムを実行して、デジタルアキュレート・セキュリティシステムとして機能させる。

制御部１１０は、人検出部１１１（人検出手段）と、投影逆変換部１１２（投影逆変換手段）、と、ＩＤ端末検出部１１３（ＩＤ端末検出手段）と、ＩＤ端末登録部１１４（ＩＤ端末登録手段）と、通報部１１５（通報手段）とを備える。

【００４９】

制御部１１０は、投影逆変換部１１２が投影変換の逆変換をしたことを受けて、３次元

上の特定のエリア（セキュリティ区域内）に不審者が侵入したことを判定する。
【００５０】
制御部１１０は、人の大きさを人の頭の大きさなどによって判定する。
制御部１１０は、不審者の位置に基づいて危険度を判定する。
制御部１１０は、不審者の動きに基づいて危険度を判定する。
【００５１】
制御部１１０は、ＩＤ端末検出部１１３が検出したＩＤ端末を所持している人を不審者から除外する。
制御部１１０は、ＩＤ端末登録部１１４が登録した登録した前記ＩＤ端末を所持している人を不審者から除外する。
【００５２】
人検出部１１１は、監視カメラ１１によって撮影された画像から人を検出し、その人の大きさを検出する。具体的には、人検出部１１１は、ＡＩアクセラレータ２００（後記）を用いてセキュリティ区域内の人を検出する。人検出部１１１は、ＡＩアクセラレータ２００に対して人検出要求を発行し、ＡＩアクセラレータ２００は、ＣＰＵ以外でＡＩの計算を実行して、人検出結果を人検出部１１１に送信する。人検出には高速性が求められるので、人検出にＡＩアクセラレータ２００を用いている。
【００５３】
デジタルアキュレート・セキュリティシステム１０００は、ＡＩアクセラレータ２００を用いた人検出によりセキュリティ区域内への侵入者を検出する。
デジタルアキュレート・セキュリティシステム１０００は、ＡＩアクセラレータ２００による深層学習において、特に、人のみを監視対象とすることで、従来の画像差分を用いた動体検出型の監視カメラによる画像認識に比べて極めて高い精度での侵入者の検出を行うことができる。
【００５４】
本実施形態では、人検出部１１１は、ＡＩアクセラレータ２００を用いて人を検出しているが、サーモカメラ（又は人感センサ２０）で人を検出するようにしてもよい。すなわち、人感センサ２０は、セキュリティ区域内の温度を検出する。そして、人検出部１１１は、人感センサ２０が人の体温を検出し、かつ、監視カメラ１１がその撮影画像の変化を検出したことによって人（不審者候補）の存在を検出する。
【００５５】
なお、人検出部１１１は、ＡＩアクセラレータ２００を用いた人検出と、サーモカメラ（又は人感センサ）を用いた人検出とを組み合わせてもよい。例えば、セキュリティ区域内のうち、人検出の高速性が要求される、玄関先やベランダ、窓についてはＡＩアクセラレータ２００を用い、人検出の高速性が要求されない敷地と外部の境界の敷地内はサーモカメラ（又は人感センサ）を使用する。
【００５６】
投影逆変換部１１２は、人検出によって検出された人の２次元の位置と人の大きさ（特に、人の頭の大きさ）とに基づいて、投影記憶部１３５によって人の３次元空間内の位置を検出する。具体的には、投影逆変換部１１２は、１つの監視カメラ１１の画像から投影変換の逆変換をすることによって、３次元位置を検出する（図９で詳述する。）。
【００５７】
ＩＤ端末検出部１１３は、非侵入者が所持するＩＤ（Identification）端末を検出する。
ＩＤ端末登録部１１４は、来客等が所持するＩＤ端末を登録する。
通報部１１５は、投影逆変換部１１２によって検出された人の３次元空間内の位置が３次元のセキュリティ区域内であることを受けて、不審者の存在を通報する。さらに、通報部１１５は、検出された人の３次元空間内の位置の時間的経緯によって不審者の存在を判断し、その存在を通報することが望ましい（図１２で詳述する。）。
【００５８】

［ＡＩアクセラレータ２００］
ＡＩアクセラレータ２００は、人を検出する専用プロセッサであり、ＣＰＵ以外の計算リソースを用いる。ＡＩアクセラレータ２００は、例えば、ＧＰＵ（Graphics Processing Unit）を強化したプロセッサよる画像処理、ＦＰＧＡ（Field Programmable Gate Array）を用いた信号処理のアクセラレートである。また、ＡＩアクセラレータ２００は、専用ハード（例えば、ＧＰＵ）上でＡＩ（Artificial Intelligence：人工知能）の計算を実行する。

【００５９】
通常のＰＣによるコンピュータの処理では、デジタル画像一枚あたり人（人体）の検出の処理を行うのに約１．５秒かかる。このため、本実施形態では、人の検出プロセッサであるＡＩアクセラレータ２００を利用することで、ＰＣによるコンピュータの処理の約１０倍のパフォーマンスを得、侵入検出を迅速に実行する。また、本実施形態では、計算負荷が高いＡＩの計算を専用ハードであるＡＩアクセラレータ２００に任せている。これにより、市販のカメラと安価な機器用いた構成であっても、リアルタイムに挙動不審を検出し、不審者を登録可能であることが実証できた。

【００６０】
［デジタルアキュレート・セキュリティシステム］
図３は、本発明の実施形態に係るデジタルアキュレート・セキュリティシステムを用いた全体を示す構成図である。
図３に示すように、デジタルアキュレート・セキュリティシステム１０００は、ウェブサービスクラウド３００上に、デジタルアキュレート・セキュリティサービスを提供するクラウドサーバ（商用サーバ）３０１、クラウドサーバ３０１に連携して能動的に情報を取得してユーザのスマートフォン５０ａ（携帯端末装置；ＩＤ端末）に通知するＰｕｓｈ通知サーバ３０２を有する。ウェブサービスクラウド３００は、インターネット３０３に接続される。スマートフォン５０ａは、インターネット３０３を経由してウェブサービスクラウド３００上のクラウドサーバ３０１にテキスト及び画像を送信することができる。また、スマートフォン５０ａは、インターネット３０３を経由してＰｕｓｈ通知サーバ３０２からＰｕｓｈ通知を受信する。さらに、クラウドサーバ３０１及びＰｕｓｈ通知サーバ３０２は、ＬＴＥ／３Ｇ網などの通信キャリア網（固定網）（図示省略）を経由して、セキュリティアプリが搭載されたスマートフォン５０ａに接続する。

【００６１】
図３に示すように、デジタルアキュレート・セキュリティシステム１０００は、不審者の敷地内への侵入を検知し、本人・家族等が所持するスマートフォン５０ａにプッシュ通知する。
スマートフォン５０ａに来た通知をユーザがタップすると、セキュリティアプリが起動して不審者のズーム画面を表示し、「１Ｆ玄関にて不審者が検知されました」というテロップが流れる。同時にその内容が音声で読み上げられる。このように、スマートフォン５０ａの画面のテロップと音声とで不審者の通知が行われる。さらに、スマートフォン５０ａのユーザの操作により、例えば緊急時には関係機関（警察・消防）に通知する。この場合、警備会社や関係企業本社にも自動的に通知される。また、緊急性がない場合や確認したい場合には、警備会社のみに通知する。

【００６２】
［セキュリティアプリ動作］
図４は、本発明の実施の形態に係るデジタルアキュレート・セキュリティシステムのセキュリティアプリ動作を示す図である。
図４左に示すように、スマートフォン５０ａの待受け画面等に不審者を検出したテロップが通知される。ユーザのタップにより、図４中に示すように、スマートフォン５０ａの表示はセキュリティアプリ動作表示に切り替わり、不審者のズーム画面を表示し、不審者の位置と状況「１Ｆ玄関に不審者」を表示する。また、このテロップを自動音声で読み上げる。さらに、ユーザのタップにより、図４右に示すように、スマートフォン５０ａの表

示を時系列の４画面に表示する。
【００６３】
以下、上述のように構成されたデジタルアキュレート・セキュリティシステムの動作について説明する。
［デジタルアキュレート・セキュリティ処理］
まず、デジタルアキュレート・セキュリティシステムの警備モード設定について説明する。
【００６４】
図５は、デジタルアキュレート・セキュリティシステムの監視装置１００の警備モード設定処理を示すフローチャートである。本フローは、監視装置１００の制御部１１０（図２参照）により実行される。
【００６５】
ステップＳ１では、警備モードを定義する。
ステップＳ２では、時間により警備モードを変更する。
ステップＳ３では、スマートフォン５０ａ（携帯端末装置５０）から警備モードの変更を受信したか否かを判別する。
スマートフォン５０ａ（携帯端末装置５０）から警備モードの変更を受信した場合（ステップＳ３：Ｙｅｓ）、ステップＳ４で指示された警備モードで警備を実行する。
警備モードの変更を受信しない場合（ステップＳ３：Ｎｏ）、本フローを終了して定義された警備モードで時間による警備モードを実行する。
上記警備モードを定義することにより、無駄な処理をなくすことができ、結果的には計算リソースの低減により低コスト化及び処理の高速化を図ることができる。
【００６６】
［デジタルアキュレート・セキュリティシステムの警備例］
デジタルアキュレート・セキュリティシステムの警備例について説明する。
＜ホーム＆ビルディング＞
図６は、個人住宅における警備の例を示す図である。
デジタルアキュレート・セキュリティシステムは、個人向けに個人住宅及びオフィス・店舗・金融機関向け等の防犯システムを提供する。主な機能は、以下の通りである。
警備モード（在室警備、外出警備等）を定義し、警備モードに応じて防犯機能を提供する。
時間により警備モードを変更する機能を備える。
家屋外周に設置された監視カメラ１１の映像から侵入者を検出・登録する。
検出された侵入者の危険度（注意度、緊急度）を判定し、危険度（注意度、緊急度）に応じて利用者に通知する。
BLEを使いスマートフォン５０ａにより屋外から警備モードを変更する。
スマートフォン５０ａ、又は監視カメラのスピーカなどを通して侵入者に警告を通知する。
【００６７】
図７は、集合住宅における警備の例を示す図である。
例えば、集合住宅向けの防犯システムを提供する。主な機能は、以下の通りである。
警備モードを定義し、警備モードに応じて防犯機能を提供する。
時間により警備モードを変更する機能を備える。
居住部外周に設置された監視カメラ１１の映像から侵入者を検出・登録する。
検出された侵入者の危険度（注意度、緊急度）を判定し、危険度（注意度、緊急度）に応じて利用者に通知する。
BLEを使いスマートフォン５０ａにより屋外から警備モードを変更する。
スマートフォン５０ａ、又は監視カメラのスピーカなどを通して侵入者に警告を通知する。
【００６８】

［デジタルアキュレート・セキュリティ処理］

次に、デジタルアキュレート・セキュリティシステムのデジタルアキュレート・セキュリティ処理について説明する。

【００６９】

図８Ａ及び図８Ｂは、デジタルアキュレート・セキュリティシステムのデジタルアキュレート・セキュリティ処理を示すフローチャートである。本フローは、監視装置１００の制御部１１０（図２参照）により図５で設定された「警備モード」で実行される。

【００７０】

ステップＳ１１では、３次元で特定されるセキュリティ区域（特定エリア）の画像を撮影する。監視カメラ１１は、例えばＰＴＺカメラであり、監視装置１００により遠隔操作される。監視カメラ１１が撮影した画像は、監視装置１００に出力される。

ステップＳ１２で、制御部１１０の人検出部１１１は、監視カメラ１１によって撮影された画像から人を検出する。本実施形態では、人検出部１１１は、ＡＩアクセラレータ２００に対してＡＩによる［人の検出処理］を要求し、人検出部１１１は、ＡＩアクセラレータ２００からの人の検出結果を待つ。なお、人検出部１１１は、サーモカメラ（又は人感センサ２０）による人検出を併用するようにしてもよい。

【００７１】

ステップＳ１３で制御部１１０は、監視カメラ１１によって撮影された画像に人が検出されたか否かを判別する。

監視カメラ１１によって撮影された画像に人が検出された場合（ステップＳ１３：Ｙｅｓ）、ステップＳ１４に進む。監視カメラ１１によって撮影された画像に人を検出しない場合（ステップＳ１３：Ｎｏ）、本フローを終了する。

【００７２】

ステップＳ１４で制御部１１０は、ＩＤ端末検出部１１３が検出したＩＤ端末（携帯端末装置５０；スマートフォン５０ａ）を所持している人（家族など所定のＩＤを所持している人など）か否かを判別する。制御部１１０は、ＩＤ端末検出部１１３が検出したＩＤ端末を所持している人を不審者から除外して（ステップＳ１４：Ｙｅｓ）、ステップＳ１５に進む。

【００７３】

ステップＳ１５で制御部１１０は、ＩＤ端末登録部１１４が登録したＩＤ端末（来客などのＩＤ）を所持している人か否かを判別する。制御部１１０は、ＩＤ端末（来客などのＩＤ）を登録している人を不審者から除外して（ステップＳ１５：Ｙｅｓ）、ステップＳ１６に進む。

このように、家族等がＩＤ端末を所持している場合及び来客等のＩＤ端末をあらかじめ登録した場合、後段の処理をスキップして処理の迅速化を図る。

【００７４】

ステップＳ１６で制御部１１０の投影逆変換部１１２は、人検出によって検出された人の２次元の位置と人の大きさとに基づいて、投影記憶部１３５によって人の３次元空間内の位置を検出する。上記人の大きさは、身長などでもよいが、人の頭の大きさが望ましい。人の年齢や性別等であまり変化のない人の頭の大きさを人の大きさの指標として用いることができる。

【００７５】

ステップＳ１７で制御部１１０は、投影逆変換部１１２によって検出された人の３次元空間内の位置が３次元のセキュリティ区域内であることを受けて、不審者の侵入を判定する。例えば、隣家の駐車場の屋根から塀を超えて侵入する場合などを検出することができる。

【００７６】

セキュリティ区域内に不審者が侵入した場合、ステップＳ１８で制御部１１０は、不審者の位置及び／又は不審者の動きに基づいて侵入の危険度を判定する。セキュリティ区域内に不審者の侵入がない場合、本フローの処理を終了する。

【００７７】
（１）不審者の位置よって、危険度（注意度、緊急度）を判定する。例えば、前記図６及び図７のようにイエローベルト（後記）内に人が検出された場合、危険度は中程度、またレッドベルト（後記）内に人が検出された場合、危険度は高いと判定できる。また、イエローベルト外で人が検出された場合は、危険度は小さいと判定できる。これに対し、３次元上の不審者の位置から、侵入者（不審者）が隣家の駐車場の屋根から塀を超えて侵入する場合などは、危険度（緊急度）が非常に高いと判定できる。
【００７８】
（２）不審者の動きよっても、危険度（注意度、緊急度）を判定することができる。不審者の動きは、例えば瞳の動きと首の動きである（詳細後記）。不審者の動きが不自然である場合、危険度（注意度、緊急度）が高いと判定できる。
【００７９】
ステップＳ１９で通報部１１５は、危険度（注意度、緊急度）に応じた通報を行う。通報は、例えば関係者のスマートフォン５０ａに、不審者に関する情報を送信する。この通報は、侵入犯罪の危険度（危険の度合いのクラス分け）に対応して、危険の度合いを示すメッセージやマーク、強調文字、色分けを付すようにする。また、危険度又は緊急度に対応して、通報先を変える。例えば、侵入者（不審者）が隣家の駐車場の屋根から塀を超えて侵入する場合などは、侵入者が危険で緊急度が高いと判定し、侵入者に関する最も緊急度の高いテロップを通知する。さらに、通報先の関係機関に警察等を入れる。そしてこの通報は、不審者の自動登録処理などより優先して行う。また、レッドベルト内に人が検出された場合、侵入の緊急度が高いテロップを、イエローベルト外で人が検出された場合は、侵入の緊急度は中程度のテロップを通知する（図４参照）。
【００８０】
上述したように、図４左に示すスマートフォン５０ａの待受け画面等に不審者の存在を通報するテロップを送信する。ユーザのタップにより、図４中に示すように、不審者のズーム画面を表示し、不審者の位置と状況「１Ｆ玄関に不審者」を表示するとともに、このテロップを自動音声で読み上げる。
【００８１】
ステップＳ２０で制御部１１０は、セキュリティ区域内の不審者の情報を記憶部１３０に登録して本フローの処理を終了する。これにより、不審者の侵入情報が記録され、防犯上有益な情報となる。
上記ステップＳ１３で監視カメラ１１によって撮影された画像から人が検出されない場合、上記ステップＳ１４で家族等のＩＤ端末を所持している人である場合、又は上記ステップＳ１５で来客等のＩＤ端末を登録した人である場合、本フローを終了する。
【００８２】
［投影逆変換部１１２による３次元位置検出］
次に、投影逆変換部１１２による３次元位置検出について説明する。
【００８３】
図９は、デジタルアキュレート・セキュリティシステムの投影逆変換部１１２による３次元位置検出処理を示すフローチャートである。図９のフローは、図８Ａのステップ Ｓ１６のサブルーチンである。
ステップＳ１６のサブルーチンコールによりスタートし、ステップＳ３１で投影逆変換部１１２は、投影記憶部１３５から、あらかじめ３次元空間内に投影した形状として定義して記憶しておいた形状を読み込む。
【００８４】
ステップＳ３２で投影逆変換部１１２は、投影記憶部１３５から人の大きさ情報を読み込む。
ステップＳ３３で投影逆変換部１１２は、セキュリティ区域内で検出した人の２次元画像と人の大きさをもとに、「３次元空間内に定義した形状を２次元面上に投影する投影変換」の逆変換を行う。投影逆変換部１１２は、１つの監視カメラ１１の画像から投影変換

の逆変換をすることによって、３次元位置を検出する。原理的には、２次元画像で３次元の位置を検出することはできないはずであるが、人の大きさが既知であるとすると（人による頭の大きさの違いはほとんどないことを前提とする）、１つの監視カメラ１１が撮影した２次元画像と、検知した人の大きさ情報とをもとに３次元位置を検出することができる。すなわち、３次元空間内に定義した形状を２次元面上に投影する変換を「投影変換」というとすると、投影逆変換部１１２は、検知した人情報に、人の大きさ情報を付加することによって、カメラ画像から投影変換の逆変換（「投影逆変換」）を行い、３次元位置を検出することができる。

ステップＳ３４で投影逆変換部１１２は、投影変換の逆変換結果を出力して、図８のステップＳ１６に戻る。

【００８５】

［デジタルアキュレート・セキュリティの特徴］

次に、デジタルアキュレート・セキュリティシステムのデジタルアキュレート・セキュリティの特徴について説明する。

【００８６】

デジタルアキュレート・セキュリティシステム１０００は、敷地内侵入検知・登録機能として、平面的に侵入を判定する技術と、立面的に侵入を判定する技術、平面的、立面的に検知されたものを、時間による侵入を検証する技術を、１つ又は複数組合せて用いる。以下、詳細に説明する。

【００８７】

不審者を検出するには、まず人間が敷地内に侵入したかどうかをカメラ画像から判定する。この判定ののち、その人間が不審者であるかどうかを検証し登録・通知する。

【００８８】

警戒領域を２次元、３次元、４次元（３次元＋時間）的に検査し危険度を評価・登録する

【００８９】

敷地境界内を平面的に危険度に応じて以下の３つに分類する。

・セキュリティ・イエローベルト：例えば敷地境界の内側３０ｃｍのゾーン（～３ｍ、４ｍ程度）

・セキュリティ・オレンジゾーン：セキュリティ・イエローベルトとセキュリティ・レッドベルトの間

・セキュリティ・レッドベルト　：例えば家屋の壁面から水平３０ｃｍ以内（～３ｍ、４ｍ程度）の領域

【００９０】

＜セキュリティベルトについて＞

セキュリティ・イエローベルト（以下、図中はＹにより表記）は、早期警戒レベルの状態である。この部分への侵入は危険度イエローで通知されるが、３次元的、４次元的な追加情報を付加して検証し、検証の結果として侵入があれば通知することにより、検出の正確さと早期に対処を行うことが可能となる。また、セキュリティ・レッドベルト（以下、図中はＲにより表記）では領域への侵入があれば直ちに通知の対応が必要となるレベルである。

【００９１】

＜平面における検出＞

図１０は、平面における侵入者検出の例を示す図であり、図１０左は平面における正常な状態、図１０右は平面における異常な状態を示す。

図１０左に示すように、敷地境界の内側にセキュリティ・イエローベルトを設定し、セキュリティゾーンを挟んで、玄関ドア及び窓を有する家屋の壁面を囲むようにセキュリティ・レッドベルト設定する。

図１０右には、平面における異常な状態を示している。セキュリティ・イエローベルトを越えて、セキュリティ・レッドベルトの外側まで侵入者が侵入している。

【００９２】
平面における侵入者検出では、侵入者と境界との包含関係を評価する。例えば、図１０右の符号ａに示すように、監視カメラ１１が１０コマ／秒で撮影するものであれば、１０コマの画像から侵入された動体を検出し（図１０右のフレーム参照）、その平面状での位置を計算する。その１０コマ内で（秒５コマの監視カメラなら５コマ）その侵入者が確かに検出されるのであれば、侵入者が存在する可能性があると判断する。
【００９３】
＜立面における検出＞
図１１は、立面における侵入者検出の例を示す図であり、図１１左は立面における正常な状態、図１１右は立面における異常な状態をそれぞれ示す。
図１１左に示すように、敷地境界の内側にセキュリティ・イエローベルトを設定し、セキュリティゾーンを挟んで、家屋の壁面を囲むようにセキュリティ・レッドベルトを設定する。
立面における検出では、監視カメラ１１の画像から高さ（図１１右のフレーム参照）を評価する。この高さが標準的な人間の高さかどうかを評価する。例えば、図１１右の符号ｂに示すように、監視カメラ１１の１秒間の画像数を評価し。確かに侵入者が人間であることを判断する。
【００９４】
ここで、監視カメラ１１の画像から高さを評価することは、上述した図８のステップＳ１６で投影逆変換部１１２が、人検出によって検出された人の２次元の位置と人の大きさとに基づいて、投影記憶部１３５によって人の３次元空間内の位置を検出する。そして、図８のステップＳ１７で制御部１１０が、投影逆変換部１１２によって検出された人の３次元空間内の位置が３次元のセキュリティ区域内であることを受けて、不審者の侵入を判定する処理に対応する。図１１の例では、侵入者がセキュリティ・イエローベルトを超えて侵入することを検出する。
立面における侵入者検出により、動物の侵入や、植栽の風による動きの誤検知を除去する。
【００９５】
＜時間による検証＞
図１２は、時間による侵入者検証の例を示す図であり、図１２左は時間における正常な状態、図１２右は時間における異常な状態をそれぞれ示す。
図１２右の符号ｃに示すように、デジタルアキュレート・セキュリティシステム１０００は、立面における侵入者検出により、得られた侵入者の検出について、一秒毎に評価を繰り返す。図１２右に示すように、侵入者はセキュリティ・イエローベルト上を歩いている。デジタルアキュレート・セキュリティシステム１０００は、侵入者がセキュリティ・イエローベルト上で継続して侵入検出されたことを受けて、侵入者が確かに侵入したと判断する。
【００９６】
＜立面的に侵入を判定する技術：マッピング＞
立面的に侵入を判定する技術を説明する。
立面的に侵入を判定する技術として、敷地境界の平面配置情報をカメラ画像にマッピングする。
図１３は、敷地境界をカメラ画像にマッピングする例を示す図であり、図１３左はその敷地境界の平面図、図１３右はその敷地境界をカメラ画像にマッピングした例を示す。マッピングはＣＧ（computer graphics）で生成された画像を写真画像に合成する技術である。合成する時、ＣＧの背景部分を透過させることによりＣＧを写真画像に自然に重畳合成できる。
【００９７】
図１３左に示すように、監視カメラ（図１３左の×印参照）を設置するに当たり、警戒区域（自宅敷地境界などアウトラインとなる形状）の平面図を正確に作成する。また、監

視カメラの設置位置、高さ及び向き（ロール、ピッチ、ヨー情報）も与える。上記ロール、ピッチ、ヨーは、３次元空間における視線の回転角を表す。視線方向をＸ軸、それに直行する左手方向をＹ軸、視点の上方向をＺ軸とすると、Ｘ軸周りの回転をロール、Ｙ軸周りの回転をピッチ、Ｚ軸周りの回転をヨーという。

【００９８】

図１３右は、図１３左の符号ｄの監視カメラの画像をマッピングした例を示している。

警戒区域の位置情報をカメラのパラメータから、投影変換とビューポートによるクリッピングを行い監視カメラから得られる画像のどこが敷地内になるのかを求める（図１３右参照）。上記ビューポートは、３次元空間を２次元として認識する場合の２次元の限界を表す。これは監視カメラで写真を取った時の写真に映る範囲に相当する。ビューポートは、監視カメラで撮影できる範囲を表す。また、上記クリッピングは、３次元データで表現されたコンピュータグラフィックス等のようなオブジェクトをビューポートの大きさに切りだす処理をいう。

【００９９】

＜立面的に侵入を判定する技術：あらかじめ登録した物体との大きさ比較＞

マッピングされたセキュリティ区域である敷地内にある門扉の高さ、車の高さ、植生の高さ、及び人の高さ（頭の大きさ、直立した高さ、しゃがんだ高さなどの既知の人の大きさ）を比較する。

【０１００】

図１４は、敷地内にあらかじめあるものの高さを登録する例を説明する図である。

図１４に示すように、マッピングされたセキュリティ区域である敷地内にある門扉の高さ、車の高さ、植生の高さを登録する。また、人が有してる基準となるサイズを、すなわち人の高さ（頭の大きさ、直立した高さ、しゃがんだ高さなどの既知の人の大きさ）を投影記憶部１３５にあらかじめ記憶しておく。人が侵入する場合はあらかじめ登録したセキュリティ区域である敷地内にある門扉の高さ、車の高さ、植生の高さ以外で人間的な高さがあるものが人であり、その形状の複数の画像によって侵入者（図１４のフレーム参照）を判定する。

【０１０１】

ここで、立面的に侵入を判定するには、上述した図９のステップＳ３１，ステップＳ３２で投影逆変換部１１２が、投影記憶部１３５から、あらかじめ３次元空間内に投影した形状として定義して記憶しておいた投影形状と人の大きさ情報を読み込む。そして、ステップＳ３３で、セキュリティ区域内で検出した人の２次元画像と人の大きさをもとに、１つの監視カメラ１１の画像から投影変換の逆変換をすることによって、３次元位置を検出する。

【０１０２】

図１５は、人間の状態による高さの変化を説明する図である。図１５の符号ｅは、高さに変化のある異常な状態を示す。図１５の符号ｆは、投影記憶部１３５（図２参照）に登録されている色々な高さの物体（門扉など）を示し、図１５の符号ｇは、投影記憶部１３５（図２参照）に登録されている正常な状態の人の大きさ（高さ）を示す。

図１５に示すように、人間的な位置の正確さと３次元的な高さを（伏せる姿勢、座る姿勢、中腰の姿勢、立脚の姿勢等を判断するため、人間の５体すなわち、頭部、顔の各部部品、体、足などの厚さ、高さとの対比を正しく表せるようにする）反映する。これにより、注意度判断の精度を１００％近くまで高める。

人間の高さは、監視カメラから得られた画像の内の動体を囲む領域（一次ライン）(図１４のフレーム参照)のボックスの高さにより求める。

【０１０３】

＜時間による侵入検証＞

立面における侵入者検出を、時間による侵入でより精度よく検証する技術を説明する。

図１６は、人間の状態による高さの変化を説明する図である。図１６の符号ｈは、侵入者が停止している状態、図１６の符号ｉは、侵入者がゆっくり移動している状態、図１６

の符号ｊは、侵入者が早く移動している状態をそれぞれ示す。

【０１０４】

前記立面における侵入者検出では、ある一瞬間に人間が警戒領域(敷地境界内)に侵入しているかどうかを判断することはできるものの、何らかの目的を持って侵入しているかどうかは判別できない。つまり、たまたま一時的に警戒領域(敷地境界内)に侵入してしまったケースを除去できない。このため、デジタルアキュレート・セキュリティシステム１０００では、時間的な継続性を加味する。

【０１０５】

図１６に示すように、人間が敷地内に侵入したことを判別した情報が短い時間の間に連続して得られた場合。例えば２秒間に連続して検知されたとすると、それは侵入者が意図をもって侵入したと判断できる。この時間による侵入を検証技術を用いて「人現が意図を持って敷地内に侵入した」という事実を判断でき、その状態情報を登録することができる。

【０１０６】

［検出された侵入者の注意度評価］

デジタルアキュレート・セキュリティシステム１０００は、検出された侵入者の注意度を評価し、注意度に応じて利用者に通知する。上述した、図８Ｂのフローのステップ Ｓ１９の「危険度（注意度、緊急度）に応じた通報」に対応する。

具体的には、瞳の動きによる判断技術と、首の動きによる判断技術を用いる。これにより、デジタルアキュレート・セキュリティシステムは、警戒領域に侵入検知された対象の心理状態を危険度として評価を行うことができる。

【０１０７】

＜瞳の動きによる判断＞

図１７上段は、瞳の動き（左右）による判断を説明する図である。

画像処理の技術を用いると顔は「顔器官検出（Facial Landmark Detection）」によって、目鼻口の位置を獲得できる。次の技術により瞳の場所を判断する。

まず、（１）目の画像を切り出す。これを一次ラインと呼称する。（２）次にその画像を二値化する。瞳は黒くなり、白眼は白となる。（３）目を水平の３つの領域に分ける（右、中央、左）。このそれぞれの領域の黒の画素を数える。この最も多い領域を二次ラインと呼称するこの二次ラインに瞳が有ると判断する。つまり、瞳が右に寄っているか、左に寄っているか、中央にあるかを判断できる。

【０１０８】

＜首の動き（左右）による判断＞

図１７中段は、首の動き（左右）による判断を説明する図である。

首の動き、つまり左右を見渡したり、上をうかがう時、人は首を動かす。この首の動きは顔の向きという形であらわされる。顔器官検出で得られる点を内包する矩形を一次ラインとし、目鼻口を内包する矩形を二次ラインとすると、この一次ラインと二次ラインに囲まれる領域の重心座標の隔たりにより顔の向きをベクトルとして数値的にあらわすことができる。

【０１０９】

図１７中段の矩形枠に示す顔全体の位置に対して、目・眉・鼻・口・顎の輪郭を抽出することで、図１７中段の中央のニュートラルな状態から、左に顔を向けるように首を動かす状態と、右に顔を向けるように首を動かす状態とが段階的に判定される。なお、この技術を用いて、ある角度から撮影された顔画像をもとに、ニュートラルな状態の顔画像を生成することもできる。

【０１１０】

＜首の動き（上下）による判断＞

図１７下段は、首の動き（上下）による判断を説明する図である。

この首の動き（上下）も首の動き（左右）と同様に判断することができる。

＜時間の経過による判断＞

図１７上段に示す瞳の位置による判断だけでは、瞬間的な状況だけしかわからない。このため、短い時間における状態を追跡する。例えば、１秒間に秒５フレーム又は１０フレームで目の位置情報を取得・記録し右、中央、左と判断される状況が混在した場合、目が激しく動いていると判断できる。これにより、デジタルアキュレート・セキュリティシステムは、「人が悪意を持つことにより目を激しく動かせた」と考えられる状態を判断でき、その状態を登録することができる。

【０１１１】

また、首の位置についても同様に、首の動き時間の変化を用いることにより動きを判断できる。例えば２秒という短い時間にベクトルが右方向から左方向、或いは上方向から下方向に変化した場合、首が激しく動いたと判断できる。これにより、デジタルアキュレート・セキュリティシステムは、「人が悪意を持つことにより首を激しく動かせた」と考えられる状態を判断でき、その状態を登録することができる。

なお、図１７の瞳と首の動きの変化による判断処理は、図２５の適用例４において後記する。

【０１１２】

［BLEによる警備解除］

図１８は、BLEによる一時的な警備解除を説明する図である。

BLE（Bluetooth Low Energy）は、近接接近を検知する技術である。デジタルアキュレート・セキュリティシステムは、利用者がスマートフォンにデジタルアキュレート・セキュリティシステム専用のアプリケーションをインストールすることにより、利用者・その家族が警戒範囲に侵入することを許す機能を持つ。利用者はあらかじめ定められた解除コードを持ち（アプリの中にインストールされている）、近接を感知すると、この解除コードがBLEによりデジタルアキュレート・セキュリティシステムに送信され、一時的に警戒モードを解除する（図１６参照）。これにより、利用者・その家族が敷地内でする行動について検知対象外とすることが可能になり、精度の高い侵入検知を行うことができる。

【０１１３】

［適用例］

デジタルアキュレート・セキュリティシステムによる侵入検出の適用例について説明する。

＜適用例１＞

図１９は、デジタルアキュレート・セキュリティシステム１０００による侵入検出の適用例１を説明する図である。

図１９に示すように、敷地境界の内側にセキュリティ・イエローベルトを設定し、セキュリティゾーンを挟んで、玄関ドア及び窓を有する家屋の壁面を囲むようにセキュリティ・レッドベルトを設定する。図１９は、平面図であるが、立面による侵入者の検出を示すために、侵入者については、(1)水平位置（Ｘ軸，Ｙ軸）と水平位置に垂直な(2)垂直位置（Ｚ軸）を破線により表している。すなわち、侵入者は、上述した「投影逆変換部１１２によって３次元空間内の位置」が検出される。図１９の西側スペース及び南側スペースのセキュリティゾーンにいる不審者（しゃがんだ不審者、伏した不審者）についても同様に、立面における侵入者検出が実行される。

【０１１４】

図２０は、図１９の適用例１において、デジタルアキュレート・セキュリティシステム１０００、家族、不審者の動作の概要を示すフローチャートである。図２０の家族及び不審者のフローは、ＣＰＵ処理ではないが、便宜上ステップ番号を付して説明する。家族（family）はステップＦ、不審者（Suspicious person）はステップＳＰを付している。

【０１１５】

《デジタルアキュレート・セキュリティシステム》

ステップＳ１０１でデジタルアキュレート・セキュリティシステム１０００が警備を開始する（ステップＳ１）。

ステップＳ１０２で時間により警備モードを変更する（ステップＳ２）（図５のステッ

プＳ２に対応）。
【０１１６】
設定した任意の条件判定を行う（ステップＳ１０３）。
２２：００以降など家族全員が帰宅済みの場合、ステップＳ１０４で在宅警備を自動開始する。
夜２３：００などの場合、ステップＳ１０５で在宅警備を自動開始する。
朝５：００などの場合、ステップＳ１０６で在宅警備を自動解除する。
【０１１７】
監視カメラから画像を得る（ステップＳ１０７）。
画像の中で人間を囲む矩形を得る（ステップＳ１０８）。
家屋外周に設置された監視カメラの映像から、侵入者を検出・登録する（ステップＳ１０９）。
家族のスマートフォンにBLE信号を送る（ステップＳ１１０）。
【０１１８】
BLEによる警備の一時解除が行われたか否か判定する（ステップＳ１１１）。
警備の一時解除が行われた場合、警備を一時解除する（ステップＳ１１２）。
警備の一時解除が行われない場合、ステップＳ１１３で侵入者の水平位置、垂直位置を取得する。
【０１１９】
不審者による敷地内への侵入が行われたか否かを判別する（ステップＳ１１４）。
不審者による敷地内への侵入が行われた場合、ステップＳ１１５で検出された侵入者の注意度（図８のステップＳ１７の「危険度判定」に対応）を評価し、注意度に応じて利用者に通知する情報を作成する。
ステップＳ１１６で家族のスマートフォンに発報して通知して（図８のステップＳ１８の「通報」に対応）上記ステップＳ１０２に戻る。
【０１２０】
《家族》
家族又は関係者が警備モードを設定する（ステップＦ１）。家族が不在の時は外出警備にし、家族が在宅の時は在宅警備にする。家族による警備モードの設定（ステップＦ１）情報は、デジタルアキュレート・セキュリティシステム１０００に送信され、デジタルアキュレート・セキュリティシステム１０００が警備を開始する（ステップＳ１）。
【０１２１】
セキュリティ・イエローベルト内に侵入者が侵入する（ステップＦ２）。例えば、図１９に示す北側のセキュリティ・イエローベルトに不審者が侵入する。デジタルアキュレート・セキュリティシステム１０００は、監視カメラから画像を得る（ステップＳ１０７）。
【０１２２】
侵入者は家族であるか否かを判定する（ステップＦ３）。
侵入者が家族の場合、セキュリティ・イエローベルト内に家族が立ち入っている（ステップＦ４）。例えば、図１９に示す北側のセキュリティ・イエローベルト内に家族が立ち入っている。
【０１２３】
デジタルアキュレート・セキュリティシステム１０００は、家族のスマートフォンにBLE信号を送り（ステップＳ１１０）、家族のスマートフォンがBLE信号を受信する（ステップＦ５）。
【０１２４】
これを受けて、家族又は関係者はBLEを使いスマートフォンにより屋外から警備モードを変更する（ステップＦ６）。家族が警備強化の必要があると判断したためである。
敷地内で自由に行動する（ステップＦ７）。
【０１２５】

スマートフォンで通知を受け取る（ステップＦ８）。
スマートフォン、監視カメラのスピーカから侵入者に警告を通知する（ステップＦ９）。
【０１２６】
《侵入者》
セキュリティ・イエローベルト内に侵入者が侵入し、侵入者が家族でない場合、セキュリティ・イエローベルト内に不審者が立ち入っている（ステップＳＰ１）。
敷地内で不審者が伏せる姿勢、座る姿勢、中腰の姿勢、立脚の姿勢等をとる（ステップＳＰ２）。
不審者の目が左右にきょろきょろする（ステップＳＰ３）。
不審者が首を左右に素早く振る（ステップＳＰ４）。
不審者が首を上下に素早く振る（ステップＳＰ５）。
これら不審者の動きは、デジタルアキュレート・セキュリティシステム１０００に送られ、デジタルアキュレート・セキュリティシステム１０００は、不審者の動きに基づいて危険度（注意度、緊急度）を判定する。デジタルアキュレート・セキュリティシステム１０００は、家族や関係機関に、危険度（注意度、緊急度）に応じたレベルの通知を行うことができる。
【０１２７】
＜適用例２＞
図２１は、デジタルアキュレート・セキュリティシステム１０００による侵入検出の適用例２を説明する図である。図２１は、家屋外周に設置された監視カメラの映像から侵入者を検出・登録する例を示している。図２２は、図２１の適用例２において、デジタルアキュレート・セキュリティシステム１０００の動作を示すフローチャートである。
図２１左は、不審者侵入前（Before）の１秒間に１０コマの場合の画像である。図２１左に示すように、不審者は、セキュリティ・イエローベルトゾーンへ侵入していない。
【０１２８】
図２１右は、不審者侵入後（After）の１秒間に１０コマの場合の画像である。図２１右に示すように、不審者は、セキュリティ・イエローベルトゾーンへ侵入した。デジタルアキュレート・セキュリティシステム１０００の制御部１１０（図２参照）の人検出部１１１は、監視カメラ１１によって撮影された画像から人（不審者）を検出する。図２１右において検出された不審者は、矩形の枠で示され、セキュリティ・レッドベルトまでのおおよその２次元距離は破線で示される。図２１右に示すように、セキュリティ・イエローベルトを越えて侵入した不審者は、セキュリティ・レッドベルトに近づいて来ている。
【０１２９】
図２２において、ステップＳ２０１でセキュリティ・レッドベルトへの侵入者を検出する。上述したように、デジタルアキュレート・セキュリティシステム１０００の制御部１１０（図２参照）の人検出部１１１は、監視カメラ１１によって撮影された画像から人を検出する。
ステップＳ２０２でセキュリティ・レッドベルト（家屋の壁面等から例えば３０ｃｍ～４ｍの範囲）への侵入者検出を開始する。
【０１３０】
以下、立面における侵入者検出（ステップＳ２０３～ステップＳ２０９）と、平面における侵入者検出（ステップＳ２１０～ステップＳ２１４）と、に分岐して、立面と平面のそれぞれにおいて侵入者を検出する。本実施形態は、投影逆変換部１１２（図２参照）が、人検出によって検出された人の２次元の位置と人の大きさとに基づいて、投影記憶部１３５によって人の３次元空間内の位置を検出する。そして、制御部１１０（図２参照）が、投影逆変換部１１２によって検出された人の３次元空間内の位置が３次元のセキュリティ区域内であることを受けて、不審者の存在を通報することに特徴がある。このため、立面における侵入者検出が主要動作であり、図２１も立面における侵入者の画像を示している。

【０１３１】
ステップＳ２０３で立面における侵入者検出を開始（１秒間に５～１０コマの画像）する。
ステップＳ２０４で１秒間の画像、例えば１０コマ／秒の場合１／１０～１０／１０の画像を立面上で検査する。
【０１３２】
ステップＳ２０５で侵入検知されたか否かを判定する。
ステップＳ２０５で侵入検知されない場合、ステップＳ２０６で侵入なしと判定し、ステップＳ２０７で正常と判断して本フローの処理を終了する。
ステップＳ２０５で侵入検知された場合、ステップＳ２０８で侵入ありと判定し、ステップＳ２０９で異常（要注意）と判断して本フローの処理を終了する。
【０１３３】
一方、ステップＳ２１０で平面における侵入者検出を開始（１秒間に５～１０コマの画像）する。
ステップＳ２１１で１秒間の画像、例えば１秒間に１０コマの場合１／１０～１０／１０の画像を平面上で検査する。
【０１３４】
ステップＳ２１２で侵入検知されたか否かを判定する。
ステップＳ２１２で侵入検知されない場合、ステップＳ２１３で侵入なしと判定し、ステップＳ２０７で正常と判断して本フローの処理を終了する。
ステップＳ２１２で侵入検知された場合、ステップＳ２１４で侵入ありと判定し、ステップＳ２０９で異常（要注意）と判断して本フローの処理を終了する。
【０１３５】
適用例２では、立面における侵入者検出と平面における侵入者検出とを併用しているので、立面における侵入者検出単体よりも検出の精度を高めることができる。
【０１３６】
＜適用例３＞
図２３は、デジタルアキュレート・セキュリティシステム１０００による侵入検出の適用例３を説明する図である。図２３左は平面における侵入者検出を示す平面図、図２３右は立面における侵入者検出を示す立面図である。
【０１３７】
図２３右は、図２３左の平面図を、上述した「立面的に侵入を判定する技術（図１３～図１４参照）」により立面による侵入者の検出の３次元空間に投影変換した立面図である。図２３右は、カーゲートより内側に侵入者が入っている様子を示す。侵入者は、水平位置（Ｘ軸，Ｙ軸）と垂直位置（Ｚ軸）を破線により表される。
【０１３８】
図２４は、図２３の適用例３において、デジタルアキュレート・セキュリティシステム１０００が家屋外周に設置された監視カメラの映像から侵入者を検出・登録する動作を示すフローチャートである。
ステップＳ３０１でセキュリティ・イエローベルト（セキュリティ該当敷地内、道路境界、隣地境界から例えば３０ｃｍ～４ｍの範囲）への侵入者検出を開始する。
【０１３９】
以下、立面における侵入者検出（ステップＳ３０２～ステップＳ３１１）と、平面における侵入者検出（ステップＳ２１０～ステップＳ２１４）と、に分岐して、立面と平面のそれぞれにおいて侵入者を検出する。
【０１４０】
ステップＳ３０２で立面における侵入者検出を開始（５～１０コマ／秒の画像）する。
ステップＳ３０３で１秒間の画像（例えば、１秒間に１０コマの場合１／１０～１０／１０の画像）を立面上で検査する。
ステップＳ３０４で１秒後から２秒後までの１秒間の画像（例えば、１０コマの画像）

を立面上で検査する。

【０１４１】

ステップＳ３０５で１秒経過後、２秒以内に２コマ以上検知されたか否かを判定する。

１秒経過後、２秒以内に２コマ以上検知されない場合、ステップＳ３０６で侵入がないと判断し、ステップＳ３０７で正常と判断して本フローの処理を終了する。

【０１４２】

上記ステップＳ３０５で１秒経過後、２秒以内に２コマ以上検知された場合、ステップＳ３０８で侵入の可能性があると判断し、ステップＳ３０９で時間的検証を開始する。立面における時間的検証は、下記の通りである。

すなわち、ステップＳ３１０で次の１秒間の画像（例えば、１０コマ）を立面上で検査する。次いで、ステップＳ３１１で上記ステップＳ３１０の時間的検証を１～２分間繰り返し行って精度を高める。

【０１４３】

ステップＳ３１２で侵入者検出を示す画像が一定時間連続検知されたか否かを判定する。

一定時間連続検知された場合、ステップＳ３１３で異常（要注意）と判定して本フローの処理を終了する。

【０１４４】

一方、ステップＳ３１４で平面における侵入者検出を開始（５～１０コマ／秒の画像）する。

ステップＳ３１５で１秒間の画像（例えば、１秒間に１０コマの場合１／１０～１０／１０の画像）を平面上で検査する。

ステップＳ３１６で１秒後から２秒後までの１秒間の画像（例えば、１０コマの画像）を平面上で検査する。

【０１４５】

ステップＳ３１７で１秒経過後、２秒以内に２コマ以上検知されたか否かを判定する。

１秒経過後、２秒以内に２コマ以上検知されない場合、ステップＳ３１９で侵入がないと判断し、ステップＳ３０７で正常と判断して本フローの処理を終了する。

【０１４６】

上記ステップＳ３１７で１秒経過後、２秒以内に２コマ以上検知された場合、ステップＳ３１９で侵入の可能性があると判断し、ステップＳ３０９で時間的検証を開始する。平面における時間的検証は、下記の通りである。

すなわち、ステップＳ３２０で次の１秒間の画像（例えば、１０コマ）を平面上で検査する。次いで、ステップＳ３２１で上記ステップＳ３２０の時間的検証を１～２分間繰り返し行って精度を高める。

【０１４７】

ステップＳ３１２で侵入者検出を示す画像が一定時間連続検知されたか否かを判定する。

一定時間連続検知された場合、ステップＳ３１３で異常（要注意）と判定して本フローの処理を終了する。

【０１４８】

適用例３では、適用例２と同様に、立面における侵入者検出と平面における侵入者検出とを併用しているので、立面における侵入者検出単体よりも検出の精度を高めることができる。

また、適用例３では、侵入の可能性がある場合、時間的検証を行っているので、侵入者の侵入があることをより確実に検出することができ、検出の精度を高めることができる。

【０１４９】

＜適用例４＞

図２５は、適用例４において、デジタルアキュレート・セキュリティシステム１０００の注意度に応じて利用者に通知する処理を示すフローチャートである。図２５のフローは

、図１７の瞳と首の動きの変化による判断処理を示している。
ステップＳ４０１で顔器官を検出する。
【０１５０】
以下、瞳の動きによる侵入者検出と、首の左右の動きによる侵入者検出と、首の上下の動きによる侵入者検出と、に分岐して、侵入者を検出する。
《瞳の動き》
ステップＳ４０２で１秒間に５～１０コマの画像をもとに、瞳の左右の場所を判断する。
ステップＳ４０３で１秒間の画像、例えば１秒間に１０コマの場合１／１０～１０／１０の画像を検査する。
ステップＳ４０４で１秒後から２秒後までの１秒間の画像（例えば、１０コマ）を検査する。
【０１５１】
ステップＳ４０５で１秒経過後、２秒以内に２コマ以上検知されたか否かを判定する。
１秒経過後、２秒以内に２コマ以上検知されない場合、ステップＳ４０６で正常と判断して本フローの処理を終了する。
【０１５２】
上記ステップＳ４０５で１秒経過後、２秒以内に２コマ以上検知された場合、ステップＳ４０７で異常の可能性があると判断してステップＳ４０８に進む。
ステップＳ４０８で時間的検証を開始する。瞳の動きによる時間的検証は、下記の通りである。
すなわち、ステップＳ４０９で次の１秒間の画像（例えば、１０コマ）を検査する。次いで、ステップＳ４１０で上記ステップＳ４０９の時間的検証を１～２分間繰り返し行って精度を高める。
【０１５３】
ステップＳ４１１で侵入者検出を示す画像が一定時間連続検知されたか否かを判定する。
一定時間連続検知されなかった場合、ステップＳ４１２で正常と判定して本フローの処理を終了する。一定時間連続検知された場合、ステップＳ４１３で異常（要注意）と判定して本フローの処理を終了する。
【０１５４】
《首の左右の動き》
ステップＳ４１４で１秒間に５～１０コマの画像をもとに、首の左右の場所を判断する。
ステップＳ４１５で１秒間の画像、例えば１秒間に１０コマの場合１／１０～１０／１０の画像を検査する。
ステップＳ４１６で１秒後から２秒後までの１秒間の画像（例えば、１０コマ）を検査する。
【０１５５】
ステップＳ４１７で１秒経過後、２秒以内に２コマ以上検知されたか否かを判定する。
１秒経過後、２秒以内に２コマ以上検知されない場合、ステップＳ４１８で正常と判断して本フローの処理を終了する。
【０１５６】
上記ステップＳ４１９で１秒経過後、２秒以内に２コマ以上検知された場合、ステップＳ４１９で異常の可能性があると判断してステップＳ４０８に進む。
ステップＳ４０８で時間的検証を開始する。首の左右の動きによる時間的検証は、下記の通りである。
すなわち、ステップＳ４２０で次の１秒間の画像（例えば、１０コマ）を検査する。次いで、ステップＳ４２１で上記ステップＳ４０９の時間的検証を１～２分間繰り返し行って精度を高める。

【０１５７】
ステップＳ４１１で侵入者検出を示す画像が一定時間連続検知されたか否かを判定する。
一定時間連続検知されなかった場合、ステップＳ４１２で正常と判定して本フローの処理を終了する。一定時間連続検知された場合、ステップＳ４１３で異常（要注意）と判定して本フローの処理を終了する。
【０１５８】
《首の上下の動き》
ステップＳ４２２で１秒間に５～１０コマの画像をもとに、首の上下の場所を判断する。
ステップＳ４２３で１秒間の画像、例えば１秒間に１０コマの場合１／１０～１０／１０の画像を検査する。
ステップＳ４２４で１秒後から２秒後までの１秒間の画像（例えば、１０コマ）を検査する。
【０１５９】
ステップＳ４２５で１秒経過後、２秒以内に２コマ以上検知されたか否かを判定する。
１秒経過後、２秒以内に２コマ以上検知されない場合、ステップＳ４２６で正常と判断して本フローの処理を終了する。
【０１６０】
上記ステップＳ４２５で１秒経過後、２秒以内に２コマ以上検知された場合、ステップＳ４２７で異常の可能性があると判断してステップＳ４０８に進む。
ステップＳ４０８で時間的検証を開始する。首の上下の動きによる時間的検証は、下記の通りである。
すなわち、ステップＳ４２８で次の１秒間の画像（例えば、１０コマ）を検査する。次いで、ステップＳ４２９で上記ステップＳ４２８の時間的検証を１～２分間繰り返し行って精度を高める。
【０１６１】
ステップＳ４１１で侵入者検出を示す画像が一定時間連続検知されたか否かを判定する。
一定時間連続検知されなかった場合、ステップＳ４１２で正常と判定して本フローの処理を終了する。一定時間連続検知された場合、ステップＳ４１３で異常（要注意）と判定して本フローの処理を終了する。
【０１６２】
上記フローにより、瞳の動き、首の左右の動き、首の上下の動きを判定することで、善意の人か悪意のある侵入者かの判断する際の確度を高めることができ、危険度の判定をより精度良く行うことができる。
【０１６３】
以上詳細に説明したように、本実施の形態によれば、デジタルアキュレート・セキュリティシステム１０００（図１参照）は、３次元のセキュリティ区域の画像を撮影する監視カメラ１１と、監視カメラ１１によって撮影された画像の２次元の各位置と監視カメラ１１によって撮影された３次元空間内の各位置とを対応付けて記憶する投影記憶部１３５と、監視カメラ１１によって撮影された画像から人を検出する人検出部１１１と、人検出によって検出された人の２次元の位置と人の大きさとに基づいて、投影記憶部１３５によって人の３次元空間内の位置を検出する投影逆変換部１１２と、投影逆変換部１１２によって検出された人の３次元空間内の位置が３次元のセキュリティ区域内であることを受けて、不審者の存在を通報する通報部１１５とを備える。
【０１６４】
この構成により、低コストで３次元位置を検出して、高度なセキュリティを確立することができる。
【０１６５】

本実施形態では、人の大きさが人の頭の大きさであることで、人の大きさを示す指標として、人の年齢や性別等であまり変化のない個人差によらない情報をもとに、侵入者の３次元位置を判定することができる。

【０１６６】

本実施形態では、不審者の位置に基づいて危険度を判定することで、危険度に合わせて警戒の状態をランク付けすることができる。これにより、セキュリティ区域へ侵入者に対して、通常の警戒と、よりランクの高いランクの警戒を通知することで、住居の所有者は対応した動作を行え、より高い精度での脅威の排除ができる。

【０１６７】

本実施形態では、制御部１１０が、不審者の動きに基づいて危険度を判定することで、不審者の動きを判定条件に加えて危険度の判定をより精度良く行うことができ、高度なセキュリティを確立することができる。例えば、不審者の動きをもとに、善意の人か悪意のある侵入者かの区別、さらに侵入者の場合には危険度を判定し、危険度に合わせて警戒の状態をランク付けすることができる。

【０１６８】

本実施形態では、デジタルアキュレート・セキュリティシステム１０００は、非侵入者が所持するＩＤ端末を検出するＩＤ端末検出部１１３を備え、制御部１１０は、ＩＤ端末検出部１１３が検出したＩＤ端末を所持している人を不審者から除外する。ＩＤ端末を所持している人を不審者から除外することで、無駄な通報を削減して監視の実効を図ることができる。また、監視におけるリソースを低減して、低コスト化を図ることができる。

【０１６９】

本実施形態では、デジタルアキュレート・セキュリティシステム１０００は、非侵入者が所持するＩＤ端末を登録するＩＤ端末登録部１１４を備え、制御部１１０は、ＩＤ端末登録部１１４が検出したＩＤ端末を所持している人を不審者から除外する。ＩＤ端末を登録している人を不審者から除外することで、無駄な通報を削減して監視の実効を図ることができる。また、監視におけるリソースを低減して、低コスト化を図ることができる。

【０１７０】

本実施形態では、デジタルアキュレート・セキュリティシステム１０００は、ＣＰＵ以外の計算リソースであるＡＩアクセラレータ２００を備え、制御部１１０の人検出部１１１は、ＡＩアクセラレータ２００を用いて、セキュリティ区域内の人を検出する。ＡＩアクセラレータ２００は、ＣＰＵ処理とは別に人の検出処理を専用ハードで実行することで、広範なセキュリティ区域内に存在する人を実時間で検出することができる。また、安価なカメラ機器用いた構成であっても、リアルタイムで人を検出することができる。

また、ＡＩアクセラレータ２００であることで、従来の画像差分を用いた動体検出型の監視カメラによる画像認識に比べて極めて高い精度での侵入者の検出を行うことができる。

【０１７１】

以上の説明は本発明の好適な実施の形態の例証であり、本発明の範囲はこれに限定されることはない。

【０１７２】

また、上記実施の形態ではデジタルアキュレート・セキュリティシステム及び方法という名称を用いたが、これは説明の便宜上であり、監視システム、セキュリティシステム、サーチ・セキュリティ方法等であってもよい。

【０１７３】

また、本発明のデジタルアキュレート・セキュリティシステム及び方法は、コンピュータを本デジタルアキュレート・セキュリティシステム又は方法として機能させるためのプログラムでも実現される。このプログラムは、コンピュータで読み取り可能な記録媒体に格納されていてもよい。

【０１７４】

このプログラムを記録した記録媒体は、本デジタルアキュレート・セキュリティシステ

ムのＲＯＭそのものであってもよいし、また、外部記憶装置としてＣＤ－ＲＯＭドライブ等のプログラム読取装置が設けられ、そこに記録媒体を挿入することで読み取り可能なＣＤ－ＲＯＭ等であってもよい。

【０１７５】

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、実行するための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、又は、ＩＣ（Integrated Circuit）カード、ＳＤ（Secure Digital）カード、光ディスク等の記録媒体に保持することができる。

【０１７６】

本明細書で引用したすべての刊行物、特許及び特許出願は、そのまま参考として、ここにとり入れるものとする。

【産業上の利用可能性】

【０１７７】

本発明に係るデジタルアキュレート・セキュリティシステム、方法及びプログラムは、住居、企業の事務所、工場、研究所、情報処理室、金銭集計室等の高度の管理を要する事業所等への設置が期待される。さらに、住宅、商業施設、事務所、病院、ホテル、金融機関、工場、研究所、発電所、エアーターミナル、集会場、競技場、美術館等の建物屋内外、交通機関の電車、フェリー、飛行機の車内等も対象である。

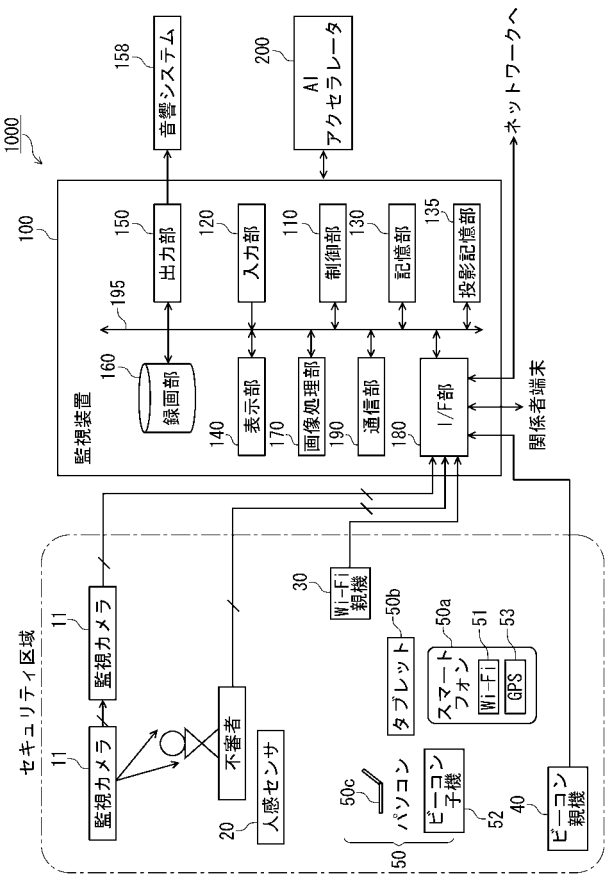
【符号の説明】

【０１７８】

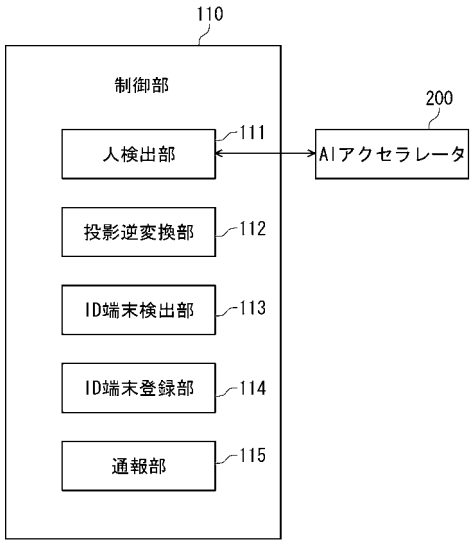
１１　監視カメラ（撮影手段）
２０　人感センサ
３０　Ｗｉ-Ｆｉ親機
４０　ビーコン親機
５０　携帯端末装置（ＩＤ端末）
５０ａ　スマートフォン（携帯端末装置；ＩＤ端末）
５１　Ｗｉ-Ｆｉ子機
５２　ビーコン子機
５３　ＧＰＳ
１００　監視装置
１１０　制御部
１１１　人検出部（人検出手段）
１１２　投影逆変換部（投影逆変換手段）
１１３　ＩＤ端末検出部（ＩＤ端末検出手段）
１１４　ＩＤ端末登録部（ＩＤ端末登録手段）
１１５　通報部（通報手段）
１２０　入力部
１３０　記憶部
１３５　投影記憶部（投影記憶手段）
１４０　表示部
１５０　出力部
１６０　録画部
１６５　顔情報ＤＢ
１７０　画像処理部
１８０　インタフェース（Ｉ／Ｆ）部
１９０　通信部
２００　ＡＩアクセラレータ（人検出手段）

１０００　デジタルアキュレート・セキュリティシステム

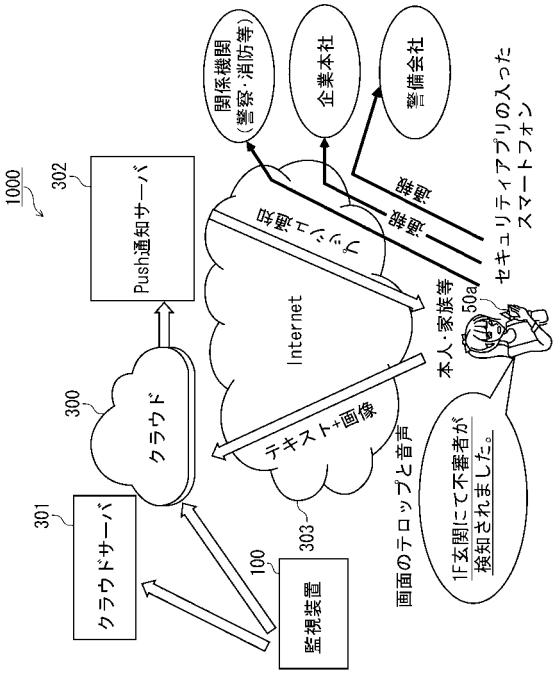
【図１】



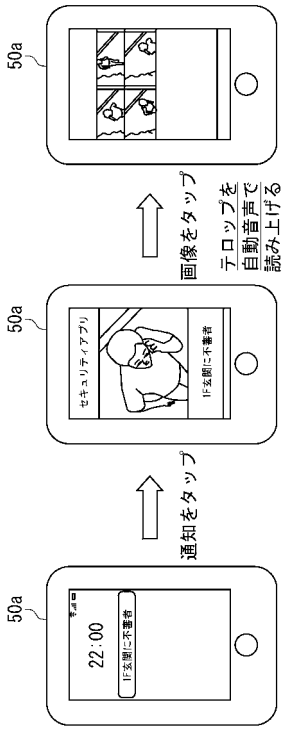
【図２】



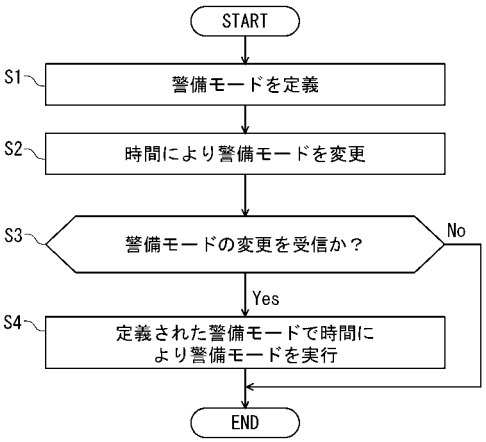
【図３】


1000
302
Push通知サーバ
300
クラウド
301
クラウドサーバ
100
監視装置
303
Internet
関係機関
（警察・消防等）
企業本社
警備会社
通報
通報
プッシュ通知
テキスト+画像
本人・家族等
50a
セキュリティアプリの入った
スマートフォン
画面のテロップと音声
1F玄関にて不審者が
検知されました。

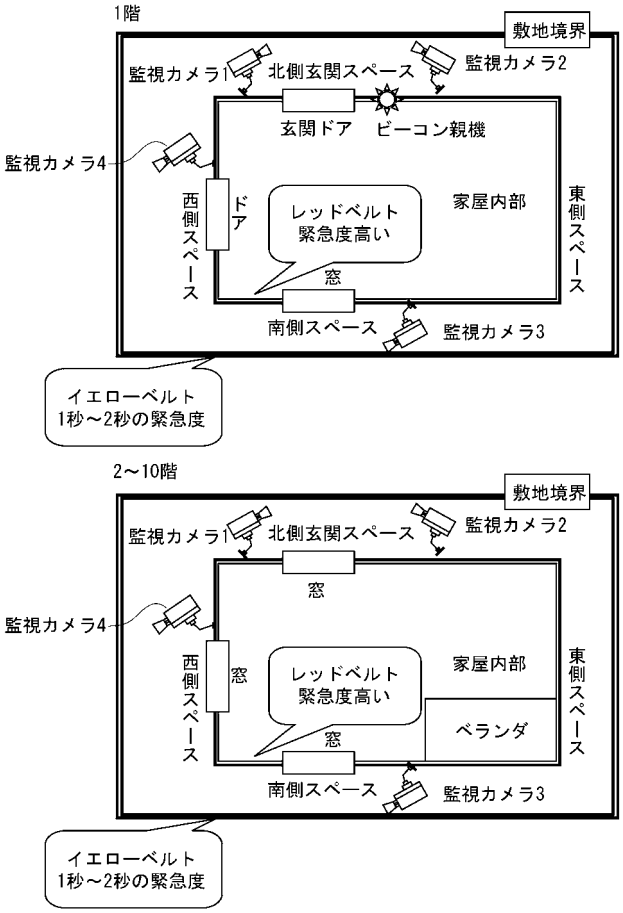
【図４】


50a
画像をタップ
テロップを
自動音声で
読み上げる
セキュリティアプリ
1F玄関に不審者
通知をタップ
22:00
1F玄関に不審者

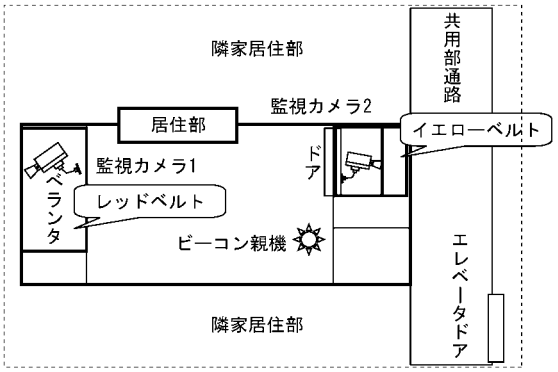
【図５】


START
S1
警備モードを定義
S2
時間により警備モードを変更
S3
警備モードの変更を受信か？
No
Yes
S4
定義された警備モードで時間に
より警備モードを実行
END

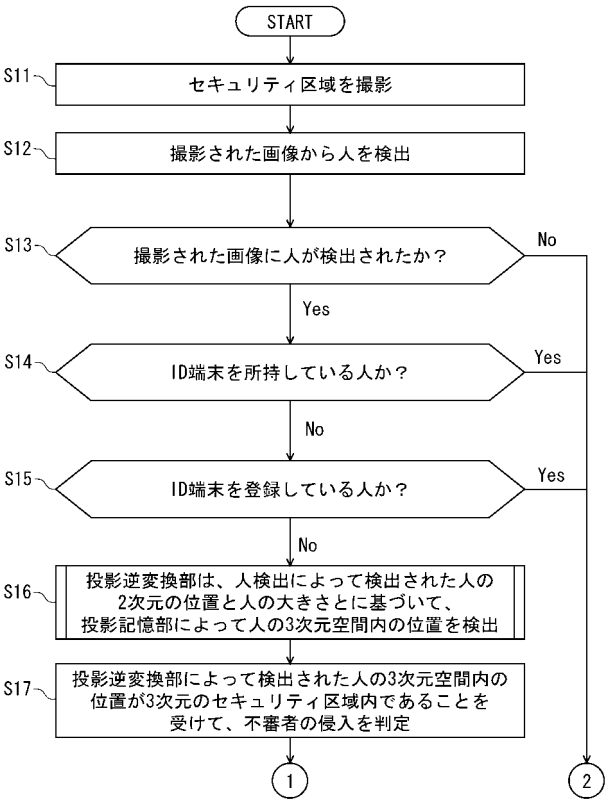
【図６】


1階
敷地境界
監視カメラ1
北側玄関スペース
監視カメラ2
玄関ドア
ビーコン親機
監視カメラ4
西側スペース
ドア
レッドベルト
緊急度高い
家屋内部
東側スペース
窓
南側スペース
監視カメラ3
イエローベルト
1秒～2秒の緊急度
2～10階
敷地境界
監視カメラ1
北側玄関スペース
監視カメラ2
窓
監視カメラ4
西側スペース
窓
レッドベルト
緊急度高い
家屋内部
ベランダ
東側スペース
窓
南側スペース
監視カメラ3
イエローベルト
1秒～2秒の緊急度

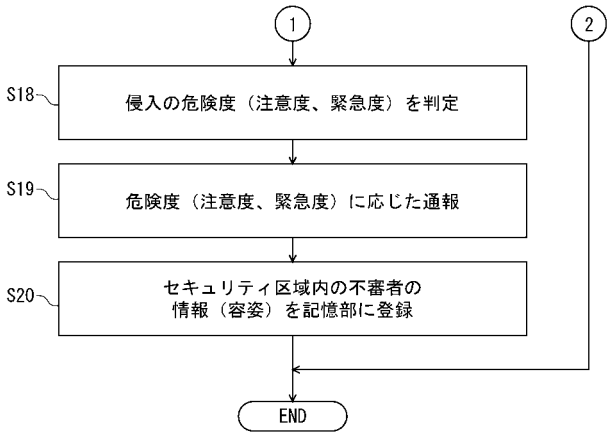
【図７】


隣家居住部
共用部通路
監視カメラ2
居住部
イエローベルト
ドア
監視カメラ1
ベランダ
レッドベルト
ビーコン親機
エレベータドア
隣家居住部

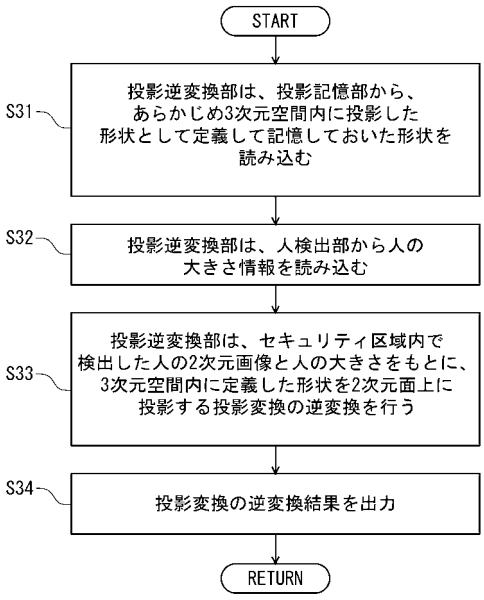
【図８Ａ】


START
S11
セキュリティ区域を撮影
S12
撮影された画像から人を検出
S13
撮影された画像に人が検出されたか？
No
Yes
S14
ID端末を所持している人か？
Yes
No
S15
ID端末を登録している人か？
Yes
No
S16
投影逆変換部は、人検出によって検出された人の
2次元の位置と人の大きさとに基づいて、
投影記憶部によって人の3次元空間内の位置を検出
S17
投影逆変換部によって検出された人の3次元空間内の
位置が3次元のセキュリティ区域内であることを
受けて、不審者の侵入を判定
1
2

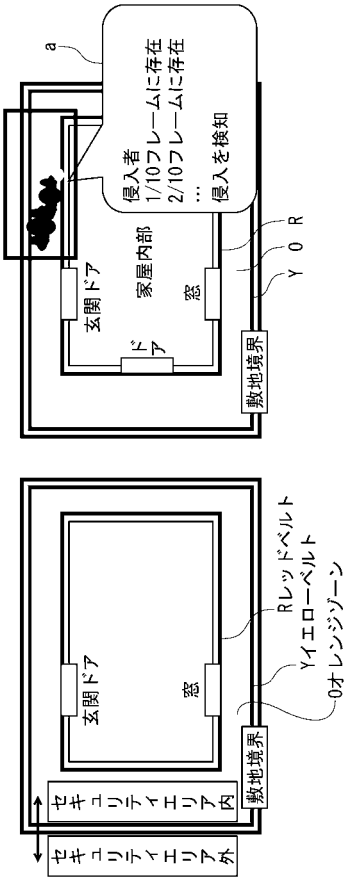
【図８Ｂ】


1
2
S18
侵入の危険度（注意度、緊急度）を判定
S19
危険度（注意度、緊急度）に応じた通報
S20
セキュリティ区域内の不審者の
情報（容姿）を記憶部に登録
END

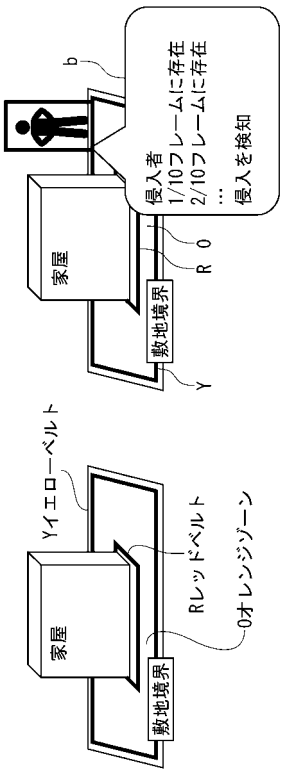
【図９】


START
S31
投影逆変換部は、投影記憶部から、
あらかじめ3次元空間内に投影した
形状として定義して記憶しておいた形状を
読み込む
S32
投影逆変換部は、人検出部から人の
大きさ情報を読み込む
S33
投影逆変換部は、セキュリティ区域内で
検出した人の2次元画像と人の大きさをもとに、
3次元空間内に定義した形状を2次元面上に
投影する投影変換の逆変換を行う
S34
投影変換の逆変換結果を出力
RETURN

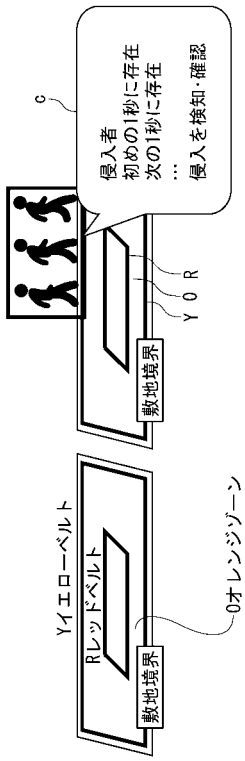
【図１０】



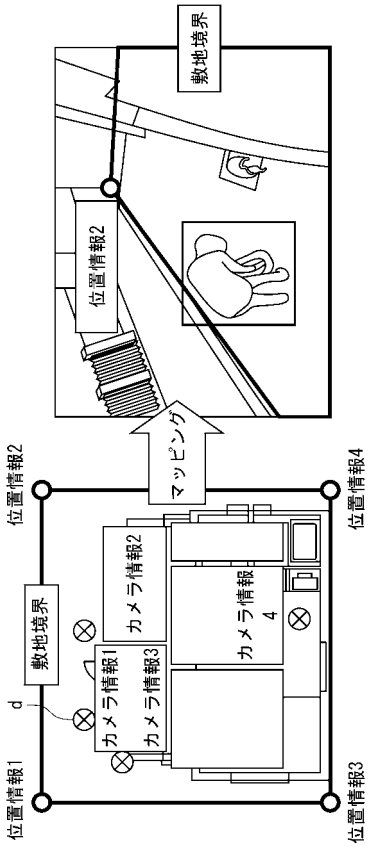
【図１１】



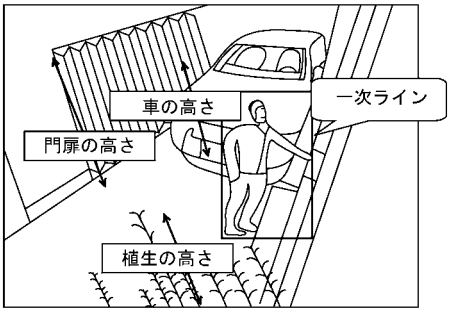
【図１２】



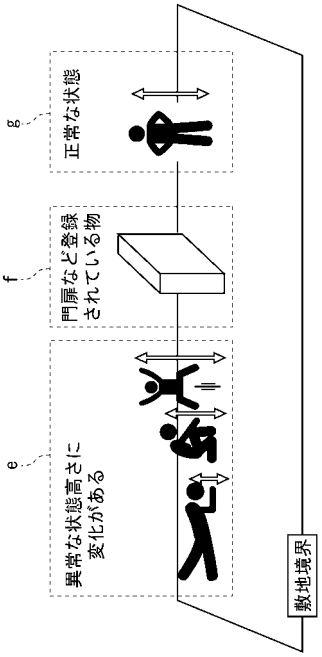
【図１３】



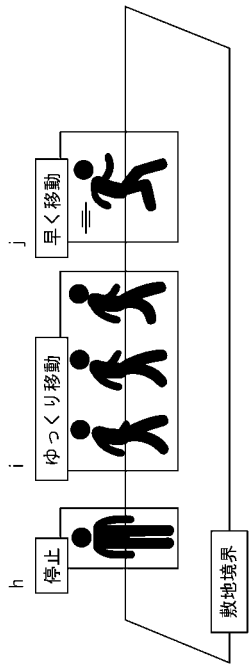
【図１４】



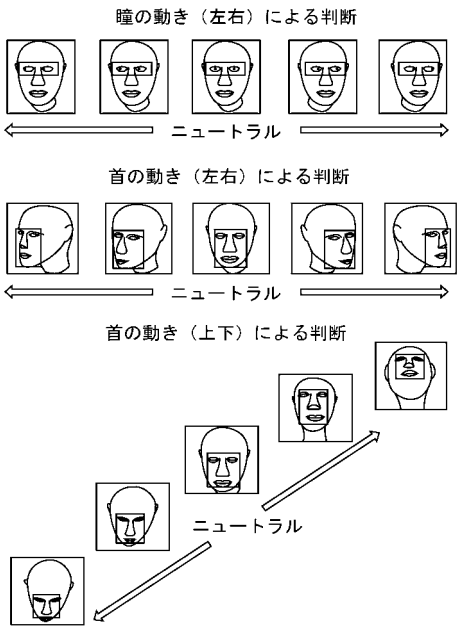
【図１５】



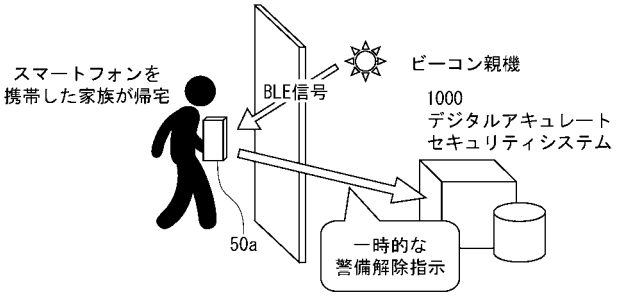
【図１６】



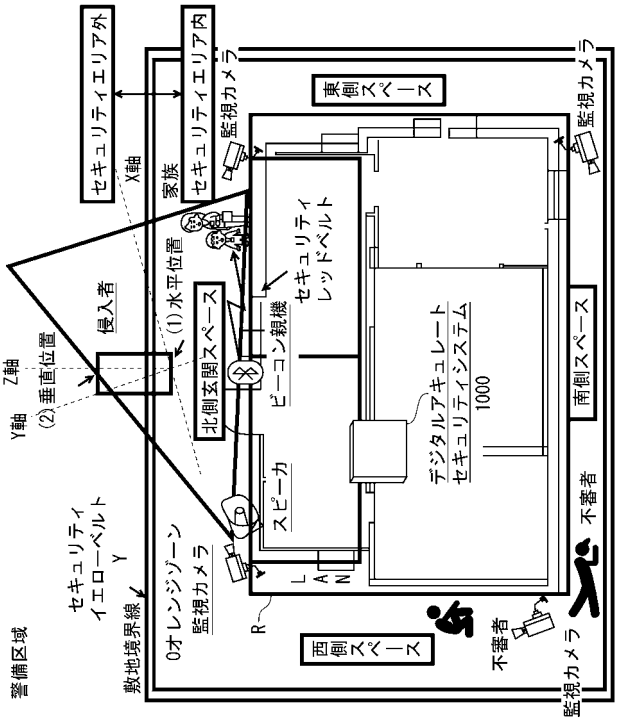
【図１７】



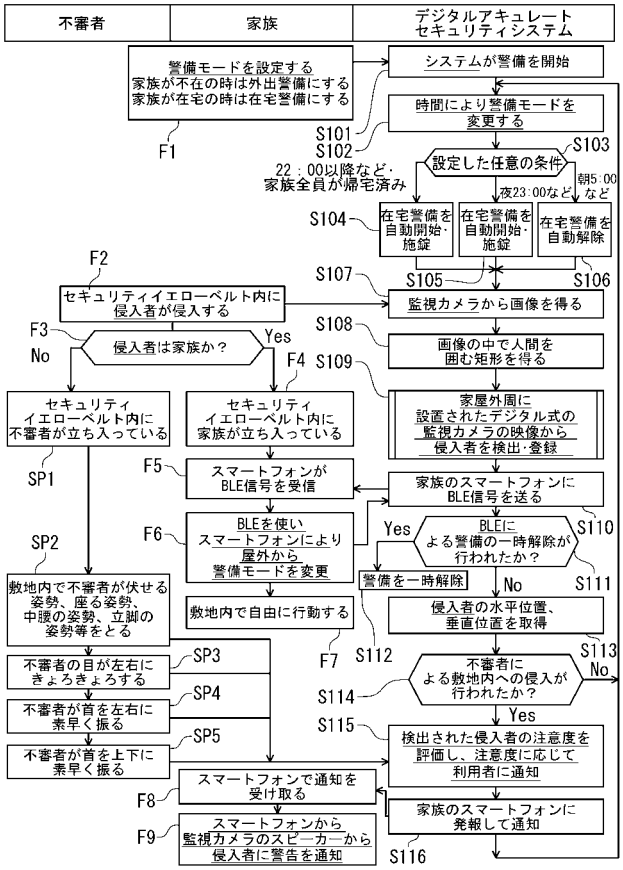
【図１８】



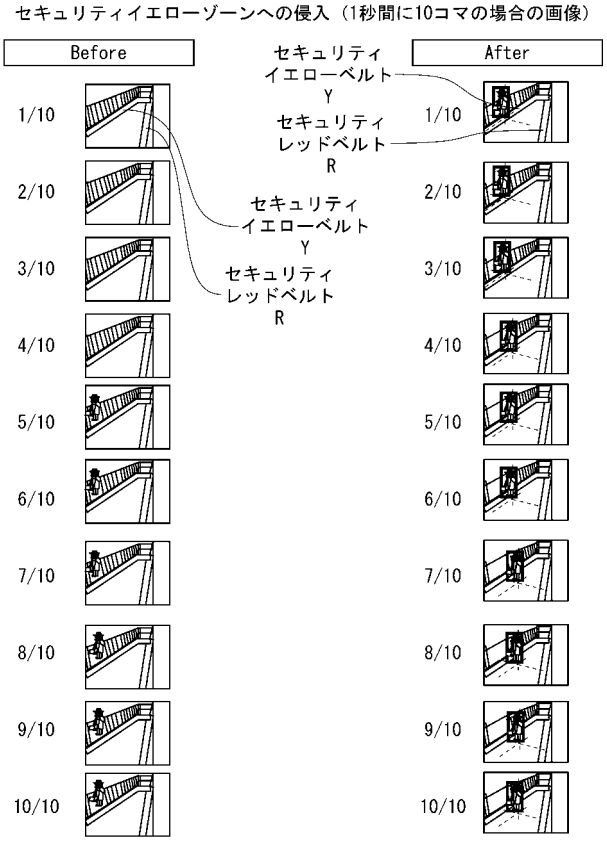
【図１９】



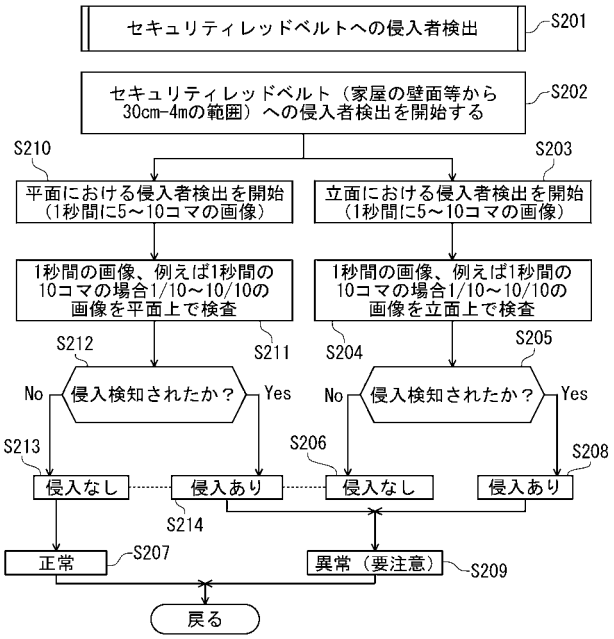
【図２０】



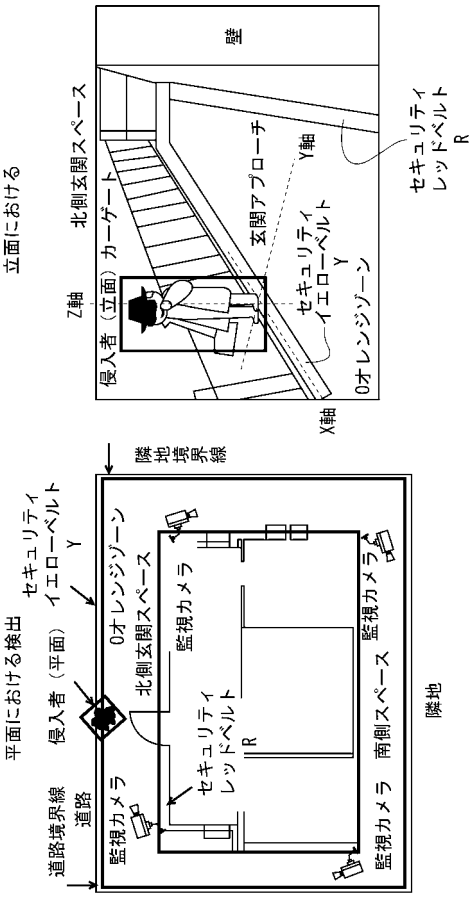
【図２１】



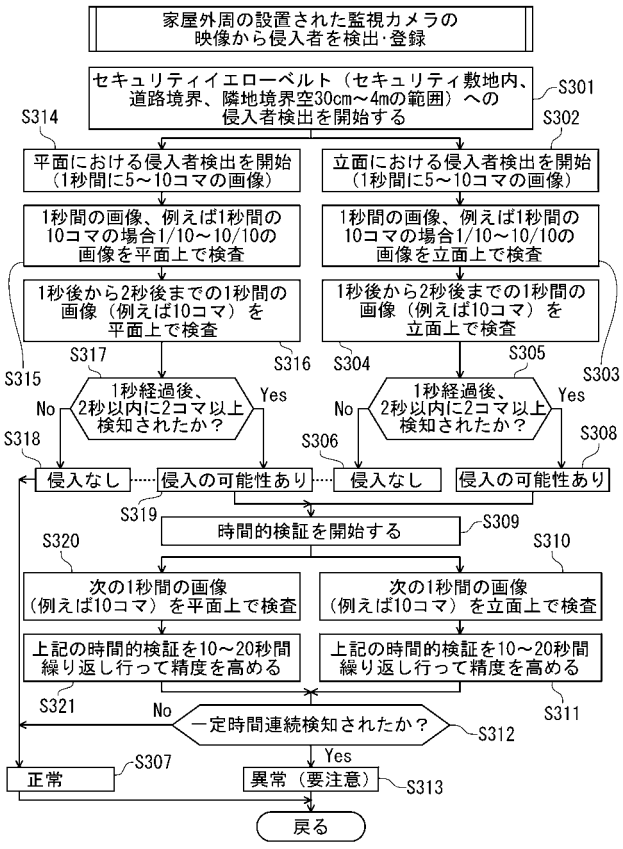
【図２２】



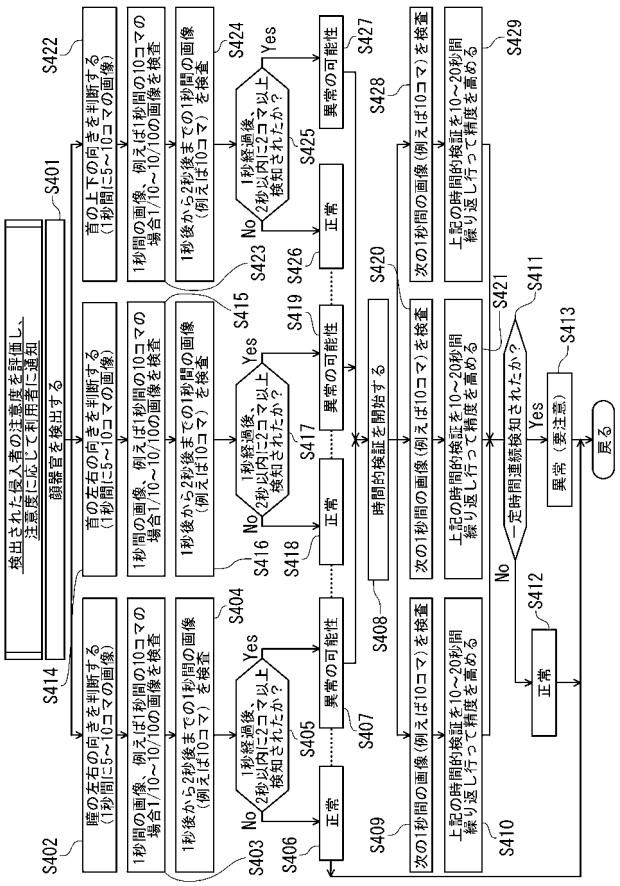
【図２３】



【図２４】



【図２５】



【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2019/007706

A. CLASSIFICATION OF SUBJECT MATTER
Int. Cl. G08B13/196(2006.01)i, G06T7/70(2017.01)i, G08B21/00(2006.01)i, G08B25/00(2006.01)i, H04N7/18(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int. Cl. G08B13/196, G06T7/70, G08B21/00, G08B25/00, H04N7/18

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Published examined utility model applications of Japan 1922-1996
Published unexamined utility model applications of Japan 1971-2019
Registered utility model specifications of Japan 1996-2019
Published registered utility model applications of Japan 1994-2019

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2019-009752 A (JAPAN IMAGE ANALYSIS ASS) 17 January 2019, paragraphs [0049], [0063]-[0073], [0093], fig. 22-24 (Family: none)	1-9
A	JP 2011-018094 A (NEC CORPORATION) 27 January 2011, paragraphs [0040]-[0044], [0058]-[0067] (Family: none)	1-9
A	JP 2016-085602 A (HITACHI, LTD.) 19 May 2016, paragraphs [0045], [0046], [0050], [0052] (Family: none)	1-9

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20.03.2019	02.04.2019
Name and mailing address of the ISA/ Japan Patent Office 3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (January 2015)

国際調査報告	国際出願番号　ＰＣＴ／ＪＰ２０１９／００７７０６

A.　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　G08B13/196(2006.01)i, G06T7/70(2017.01)i, G08B21/00(2006.01)i, G08B25/00(2006.01)i, H04N7/18(2006.01)i

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.　G08B13/196, G06T7/70, G08B21/00, G08B25/00, H04N7/18

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２０１９年
日本国実用新案登録公報	１９９６－２０１９年
日本国登録実用新案公報	１９９４－２０１９年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
A	JP 2019-009752 A (一般社団法人　日本画像認識協会) 2019.01.17, 段落[0049], [0063]-[0073], [0093], 図 22-24 (ファミリーなし)	1-9
A	JP 2011-018094 A (日本電気株式会社) 2011.01.27, 段落[0040]-[0044], [0058]-[0067] (ファミリーなし)	1-9

☒ Ｃ欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
２０．０３．２０１９	０２．０４．２０１９

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）	５Ｊ	５２８９
日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	白川　瑞樹 電話番号　０３－３５８１－１１０１　内線　３５３４		

様式ＰＣＴ／ＩＳＡ／２１０（第２ページ）（２０１５年１月）

国際調査報告 国際出願番号 PCT／JP2019／007706

C（続き）． 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
A	JP 2016-085602 A (株式会社日立製作所) 2016.05.19, 段落[0045],[0046],[0050],[0052] (ファミリーなし)	1-9

フロントページの続き

(81)指定国・地域 AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA,RW,SD,SL,ST,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(AL,AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,KM,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BN,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,CZ,DE,DJ,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IR,IS,JO,JP,KE,KG,KH,KN,KP,KR,KW,KZ,LA,LC,LK,LR,LS,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PA,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SA,SC,SD,SE,SG,SK,SL,SM,ST,SV,SY,TH,TJ,TM,TN,TR,TT

（特許庁注：以下のものは登録商標）
１．ＢＬＵＥＴＯＯＴＨ

Ｆターム(参考) 5C087 AA02 AA03 AA10 AA16 AA19 AA37 BB11 BB20 BB73 BB74
DD05 DD23 DD24 EE02 FF01 FF02 FF16 FF23 GG02 GG06
GG12 GG17 GG22 GG38 GG70

（注）この公表は、国際事務局（ＷＩＰＯ）により国際公開された公報を基に作成したものである。なおこの公表に係る日本語特許出願（日本語実用新案登録出願）の国際公開の効果は、特許法第１８４条の１０第１項(実用新案法第４８条の１３第２項）により生ずるものであり、本掲載とは関係ありません。