

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7201748号
(P7201748)

(45)発行日 令和5年1月10日(2023.1.10)

(24)登録日 令和4年12月26日(2022.12.26)

(51)国際特許分類

F I

G 0 7 C 9/37 (2020.01)

G 0 7 C 9/37

G 0 7 C 9/38 (2020.01)

G 0 7 C 9/38

G 0 8 B 25/00 (2006.01)

G 0 8 B 25/00 5 1 0 M

請求項の数 8 (全51頁)

(21)出願番号	特願2021-102415(P2021-102415)	(73)特許権者	320008672
(22)出願日	令和3年6月21日(2021.6.21)		i - P R O株式会社
(62)分割の表示	特願2019-124579(P2019-124579)		東京都港区港南二丁目15番1号
	)の分割	(74)代理人	110002000
原出願日	令和1年7月3日(2019.7.3)		弁理士法人栄光事務所
(65)公開番号	特開2021-168153(P2021-168153)	(72)発明者	河本 耕治
	A)		福岡県福岡市博多区美野島四丁目1番6
(43)公開日	令和3年10月21日(2021.10.21)		2号 パナソニック i - P R Oセンシン
審査請求日	令和3年6月21日(2021.6.21)		グソリューションズ株式会社内
		(72)発明者	宮田 英作
			福岡県福岡市博多区美野島四丁目1番6
			2号 パナソニック i - P R Oセンシン
			グソリューションズ株式会社内
		(72)発明者	神尾 崇
			福岡県福岡市博多区美野島四丁目1番6
			最終頁に続く

(54)【発明の名称】 情報処理装置、判定方法、およびプログラム

(57)【特許請求の範囲】

【請求項1】

建物の複数のゾーンの各々を撮影するカメラから、顔画像データを受信する通信部と、複数のカメラ各々のカメラ識別情報と、前記複数のゾーンとを紐付けた第1のテーブルと、

登録顔画像データと、前記登録顔画像データの人物の立ち入りが許可されたゾーンとを紐付けた第2のテーブルと、

前記顔画像データに基づいて前記第2のテーブルを参照し、前記顔画像データの人物の立ち入りが許可された許可ゾーンを取得してから、前記カメラ識別情報に基づいて前記第1のテーブルを参照して前記顔画像データの人物が撮影された撮影ゾーンを取得し、前記許可ゾーンと前記撮影ゾーンとに基づいて前記顔画像データの人物の立ち入りの許可／不許可を判定する制御部と、を有する、

情報処理装置。

【請求項2】

前記制御部は、前記許可ゾーンに一致する前記撮影ゾーンが存在する場合、前記顔画像データの人物の前記撮影ゾーンへの立ち入りの許可を判定する、

請求項1に記載の情報処理装置。

【請求項3】

前記制御部は、前記顔画像データに一致する前記登録顔画像データが前記第2のテーブルに登録されていない場合、前記顔画像データの人物の前記複数のゾーンへの立ち入りの

不許可を判定する、

請求項 1 に記載の情報処理装置。

【請求項 4】

コンピュータが行う判定方法であって、

建物の複数のゾーンの各々を撮影するカメラから、顔画像データを受信し、

前記顔画像データに基づいて、登録顔画像データと、前記登録顔画像データの人物の立ち入りが許可されたゾーンとを紐付けた第 2 のテーブルを参照し、前記顔画像データの人物の立ち入りが許可された許可ゾーンを取得し、

前記顔画像データの人物を撮影したカメラのカメラ識別情報に基づいて、前記複数のカメラ各々のカメラ識別情報と、前記複数のゾーンとを紐付けた第 1 のテーブルを参照して前記顔画像データの人物が撮影された撮影ゾーンを取得し、

前記許可ゾーンと前記撮影ゾーンとに基づいて前記顔画像データの人物の立ち入りの許可／不許可を判定する、

判定方法。

【請求項 5】

コンピュータに、

建物の複数のゾーンの各々を撮影するカメラから、顔画像データを受信し、

前記顔画像データに基づいて、登録顔画像データと、前記登録顔画像データの人物の立ち入りが許可されたゾーンとを紐付けた第 2 のテーブルを参照し、前記顔画像データの人物の立ち入りが許可された許可ゾーンを取得し、

前記顔画像データの人物を撮影したカメラのカメラ識別情報に基づいて、前記複数のカメラ各々のカメラ識別情報と、前記複数のゾーンとを紐付けた第 1 のテーブルを参照して前記顔画像データの人物が撮影された撮影ゾーンを取得し、

前記許可ゾーンと前記撮影ゾーンとに基づいて前記顔画像データの人物の立ち入りの許可／不許可を判定する、処理を実行させる、

プログラム。

【請求項 6】

建物の複数のゾーンの各々を撮影するカメラから、顔画像データを受信する通信部と、

複数のカメラ各々のカメラ識別情報と、前記複数のゾーンとを紐付けた第 1 の情報と、登録顔画像データと、前記登録顔画像データの人物の立ち入りが許可されたゾーンとを紐付けた第 2 の情報を保存するメモリと、

前記顔画像データに基づいて前記第 2 の情報を参照し、前記顔画像データの人物の立ち入りが許可された許可ゾーンを取得してから、前記カメラ識別情報に基づいて前記第 1 の情報を参照して前記顔画像データの人物が撮影された撮影ゾーンを取得し、前記許可ゾーンと前記撮影ゾーンとに基づいて前記顔画像データの人物の立ち入りの許可／不許可を判定する制御部と、を有する、

情報処理装置。

【請求項 7】

コンピュータが行う判定方法であって、

建物の複数のゾーンの各々を撮影するカメラから、顔画像データを受信し、

前記顔画像データに基づいて、登録顔画像データと、前記登録顔画像データの人物の立ち入りが許可されたゾーンとを紐付けた第 2 の情報を参照し、前記顔画像データの人物の立ち入りが許可された許可ゾーンを取得し、

前記顔画像データの人物を撮影したカメラのカメラ識別情報に基づいて、前記複数のカメラ各々のカメラ識別情報と、前記複数のゾーンとを紐付けた第 1 の情報を参照して前記顔画像データの人物が撮影された撮影ゾーンを取得し、

前記許可ゾーンと前記撮影ゾーンとに基づいて前記顔画像データの人物の立ち入りの許可／不許可を判定する、

判定方法。

【請求項 8】

10

20

30

40

50

コンピュータに、

建物の複数のゾーンの各々を撮影するカメラから、顔画像データを受信し、

前記顔画像データに基づいて、登録顔画像データと、前記登録顔画像データの人物の立ち入りが許可されたゾーンとを紐付けた第2の情報を参照し、前記顔画像データの人物の立ち入りが許可された許可ゾーンを取得し、

前記顔画像データの人物を撮影したカメラのカメラ識別情報に基づいて、前記複数のカメラ各々のカメラ識別情報と、前記複数のゾーンとを紐付けた第1の情報を参照して前記顔画像データの人物が撮影された撮影ゾーンを取得し、

前記許可ゾーンと前記撮影ゾーンとに基づいて前記顔画像データの人物の立ち入りの許可／不許可を判定する、処理を実行させる、

プログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本開示は、情報処理装置、判定方法、およびプログラムに関する。

【背景技術】

【0002】

従来、ゲートを通過するそれぞれの利用者に対して、顔認証による認証結果を報知・伝達することが可能な入退場管理システムが提供されている（例えば、特許文献1を参照）。

【先行技術文献】

【特許文献】

【0003】

【文献】特開2018-92293号公報

【発明の概要】

【発明が解決しようとする課題】

【0004】

ところで、ホワイトリストを用いて、ゾーンへの人の立ち入りを判定する監視カメラシステムが要望されている。このような監視カメラシステムでは、ホワイトリストに登録顔画像データを登録する場合、例えば、ハンディカメラを用いて顔を撮影し、撮影した顔画像データを、監視カメラシステムに接続された端末装置に読み込む。そして、端末装置から、監視カメラシステムのホワイトリストに顔画像データを登録するため手間を要する。

【0005】

また、会社等では、例えば、フロアまたは部屋等のゾーンごとにおいて、立ち入ることができる人を区別している場合がある。例えば、人Aは、部屋Xおよび部屋Yに入室でき、人Bは、部屋Xに入室できるが、部屋Yには入室できないように区別している場合がある。このように、ゾーンごとにおいて、立ち入ることができる人を区別する施設等では、ゾーンごとに決められた人以外の人、ゾーンに立ち入っていないか管理することが重要となる。

【0006】

本開示の非限定的な実施例は、ホワイトリストへの登録顔画像データの登録を容易にできる情報処理装置、判定方法、およびプログラムの提供に資する。

【0007】

本開示の非限定的な実施例は、ゾーンごとに決められた人以外の人、ゾーンに立ち入っていないかを判定する情報処理装置、判定方法、およびプログラムの提供に資する。

【課題を解決するための手段】

【0008】

本開示は、建物の複数のゾーンの各々を撮影するカメラから、顔画像データを受信する通信部と、複数のカメラ各々のカメラ識別情報と、前記複数のゾーンとを紐付けた第1のテーブルと、登録顔画像データと、前記登録顔画像データの人物の立ち入りが許可されたゾーンとを紐付けた第2のテーブルと、前記顔画像データに基づいて前記第2のテーブル

10

20

30

40

50

を参照し、前記顔画像データの人物の立ち入りが許可された許可ゾーンを取得してから、前記カメラ識別情報に基づいて前記第1のテーブルを参照して前記顔画像データの人物が撮影された撮影ゾーンを取得し、前記許可ゾーンと前記撮影ゾーンとに基づいて前記顔画像データの人物の立ち入りの許可／不許可を判定する制御部と、を有する、情報処理装置。

【0009】

また、本開示は、コンピュータが行う判定方法であって、建物の複数のゾーンの各々を撮影するカメラから、顔画像データを受信し、前記顔画像データに基づいて、登録顔画像データと、前記登録顔画像データの人物の立ち入りが許可されたゾーンとを紐付けた第2のテーブルを参照し、前記顔画像データの人物の立ち入りが許可された許可ゾーンを取得し、前記顔画像データの人物を撮影したカメラのカメラ識別情報に基づいて、前記複数のカメラ各々のカメラ識別情報と、前記複数のゾーンとを紐付けた第1のテーブルを参照して前記顔画像データの人物が撮影された撮影ゾーンを取得し、前記許可ゾーンと前記撮影ゾーンとに基づいて前記顔画像データの人物の立ち入りの許可／不許可を判定する、判定方法を提供する。

【0010】

また、本開示は、コンピュータに、建物の複数のゾーンの各々を撮影するカメラから、顔画像データを受信し、前記顔画像データに基づいて、登録顔画像データと、前記登録顔画像データの人物の立ち入りが許可されたゾーンとを紐付けた第2のテーブルを参照し、前記顔画像データの人物の立ち入りが許可された許可ゾーンを取得し、前記顔画像データの人物を撮影したカメラのカメラ識別情報に基づいて、前記複数のカメラ各々のカメラ識別情報と、前記複数のゾーンとを紐付けた第1のテーブルを参照して前記顔画像データの人物が撮影された撮影ゾーンを取得し、前記許可ゾーンと前記撮影ゾーンとに基づいて前記顔画像データの人物の立ち入りの許可／不許可を判定する、処理を実行させる、プログラムを提供する。

【0011】

建物の複数のゾーンの各々を撮影するカメラから、顔画像データを受信する通信部と、複数のカメラ各々のカメラ識別情報と、前記複数のゾーンとを紐付けた第1の情報と、登録顔画像データと、前記登録顔画像データの人物の立ち入りが許可されたゾーンとを紐付けた第2の情報とを保存するメモリと、前記顔画像データに基づいて前記第2の情報を参照し、前記顔画像データの人物の立ち入りが許可された許可ゾーンを取得してから、前記カメラ識別情報に基づいて前記第1の情報を参照して前記顔画像データの人物が撮影された撮影ゾーンを取得し、前記許可ゾーンと前記撮影ゾーンとに基づいて前記顔画像データの人物の立ち入りの許可／不許可を判定する制御部と、を有する、情報処理装置を提供する。

【0012】

また、本開示は、コンピュータが行う判定方法であって、建物の複数のゾーンの各々を撮影するカメラから、顔画像データを受信し、前記顔画像データに基づいて、登録顔画像データと、前記登録顔画像データの人物の立ち入りが許可されたゾーンとを紐付けた第2の情報を参照し、前記顔画像データの人物の立ち入りが許可された許可ゾーンを取得し、前記顔画像データの人物を撮影したカメラのカメラ識別情報に基づいて、前記複数のカメラ各々のカメラ識別情報と、前記複数のゾーンとを紐付けた第1の情報を参照して前記顔画像データの人物が撮影された撮影ゾーンを取得し、前記許可ゾーンと前記撮影ゾーンとに基づいて前記顔画像データの人物の立ち入りの許可／不許可を判定する、判定方法を提供する。

【0013】

また、本開示は、コンピュータに、建物の複数のゾーンの各々を撮影するカメラから、顔画像データを受信し、前記顔画像データに基づいて、登録顔画像データと、前記登録顔画像データの人物の立ち入りが許可されたゾーンとを紐付けた第2の情報を参照し、前記顔画像データの人物の立ち入りが許可された許可ゾーンを取得し、前記顔画像データの人物を撮影したカメラのカメラ識別情報に基づいて、前記複数のカメラ各々のカメラ識別情

報と、前記複数のゾーンとを紐付けた第1の情報を参照して前記顔画像データの人物が撮影された撮影ゾーンを取得し、前記許可ゾーンと前記撮影ゾーンとに基づいて前記顔画像データの人物の立ち入りの許可／不許可を判定する、処理を実行させる、プログラムを提供する。

【0014】

なお、これらの包括的または具体的な態様は、システム、装置、方法、集積回路、コンピュータプログラム、または、記録媒体で実現されてもよく、システム、装置、方法、集積回路、コンピュータプログラムおよび記録媒体の任意の組み合わせで実現されてもよい。

【発明の効果】

【0015】

本開示の一実施例によれば、ホワイトリストへの登録顔画像データの登録を容易にできる。

【0016】

本開示の一実施例によれば、ゾーンごとに決められた人以外の人が、ゾーンに立ち入っていないかを判定できる。

【0017】

本開示の一実施例における更なる利点および効果は、明細書および図面から明らかにされる。かかる利点および／または効果は、いくつかの実施形態並びに明細書および図面に記載された特徴によってそれぞれ提供されるが、1つまたはそれ以上の同一の特徴を得るために必ずしも全てが提供される必要はない。

【図面の簡単な説明】

【0018】

【図1】第1の実施の形態に係る監視カメラシステムの一例を示した図

【図2】ゾーンに設置された監視カメラの映像例を示した図

【図3】監視カメラのブロック構成例を示した図

【図4】サーバのブロック構成例を示した図

【図5】端末装置のブロック構成例を示した図

【図6】サーバの記憶部に記憶されるテーブルの一例を示した図

【図7】サーバの記憶部に記憶されるテーブルの一例を示した図

【図8】監視カメラシステムの動作例を示したシーケンス図

【図9】第2の実施の形態に係るサーバの記憶部に記憶されるテーブルの一例を示した図

【図10】顔データおよび時間の登録における監視カメラシステムの動作例を示したシーケンス図

【図11】第3の実施の形態に係る監視カメラシステムの一例を示した図

【図12】カードリーダーのブロック構成例を示した図

【図13】サーバの記憶部に記憶されるテーブルの一例を示した図

【図14】監視カメラシステムの動作例を示したシーケンス図

【図15】第4の実施の形態に係る監視カメラシステムの一例を示した図

【図16】監視カメラシステムの概略動作を説明する図

【図17】サーバの記憶部に記憶されるテーブルの一例を示した図

【図18】サーバの記憶部に記憶されるテーブルの一例を示した図

【図19】監視カメラシステムの動作例を示したシーケンス図

【図20】ブラックリスト方式における判定方法を説明する図

【図21】ホワイトリスト方式における判定方法を説明する図

【図22】ブラックリスト方式における判定処理例を示したシーケンス図

【図23】ホワイトリスト方式における判定処理例を示したシーケンス図

【図24】ブラックリスト方式によってアラーム信号が出力されたときの端末装置の画面例を示した図

【図25】ホワイトリスト方式によってアラーム信号が出力されたときの端末装置の画面例を示した図

10

20

30

40

50

【図 2 6】アラーム信号が出力されたときの端末装置の画面例を示した図
【図 2 7】第 5 の実施の形態に係る監視カメラシステムの一例を示した図
【図 2 8】第 5 の実施の形態に係る監視カメラシステムの一例を示した図
【図 2 9】監視カメラシステムの動作例を示したシーケンス図
【図 3 0】監視カメラシステムの動作例を示したシーケンス図
【図 3 1】第 6 の実施の形態に係る監視カメラシステムの動作例を示したシーケンス図
【図 3 2】第 7 の実施の形態に係る監視カメラシステムの一例を示した図
【図 3 3】テーブルのアクセス例を説明する図
【図 3 4】テーブルのアクセス例を説明する図
【図 3 5】監視カメラシステムの動作例を示したシーケンス図
【発明を実施するための形態】

10

【0019】

以下、図面を適宜参照して、本発明の実施の形態について、詳細に説明する。但し、必要以上に詳細な説明は省略する場合がある。例えば、既によく知られた事項の詳細説明や実質的に同一の構成に対する重複説明を省略する場合がある。これは、以下の説明が不必要に冗長になるのを避け、当業者の理解を容易にするためである。

【0020】

なお、添付図面および以下の説明は、当業者が本開示を十分に理解するために、提供されるのであって、これらにより特許請求の範囲に記載の主題を限定することは意図されていない。

20

【0021】

（第 1 の実施の形態）

図 1 は、第 1 の実施の形態に係る監視カメラシステムの一例を示した図である。図 1 に示すように、監視カメラシステムは、監視カメラ 1 a ～ 1 d と、サーバ（情報処理装置）2 と、端末装置 3 と、を有している。図 1 には、監視カメラシステムの他に、建物 A 1 が示してある。建物 A 1 は、例えば、会社、マンション、または商業施設等である。

【0022】

ゾーン A ～ C は、建物 A 1 の部屋、エントランス、廊下、階段、フロア、またはエレベータ等であってもよい。また、ゾーン A ～ C は、建物 A 1 が建っている敷地であってもよい。すなわち、ゾーン A ～ C は、人の立ち入り（進入）が許可されるか否かが判定される領域と捉えてもよい。ゾーンは、エリアと呼ばれてもよい。以下では、ゾーン A ～ C は、建物 A 1 の部屋として説明する。

30

【0023】

監視カメラ 1 a ～ 1 d は、ゾーン A ～ C に設置される。例えば、監視カメラ 1 a は、建物 A 1 のゾーン A に設置される。監視カメラ 1 b 、 1 c は、建物 A 1 のゾーン B に設置される。監視カメラ 1 d は、建物 A 1 のゾーン C に設置される。

【0024】

監視カメラ 1 a ～ 1 d は、ゾーン A ～ C 内にいる人を撮影するように設置される。例えば、監視カメラ 1 a ～ 1 d は、ゾーン A ～ C 内の全体を撮影するように設置される。

【0025】

図 2 は、ゾーン A に設置された監視カメラ 1 a の映像例を示した図である。監視カメラ 1 a は、例えば、図 2 に示すように、室内を広範囲にわたって撮影する。

40

【0026】

図 1 の説明に戻る。サーバ 2 は、例えば、LAN（Local Area Network）またはインターネット等のネットワークによって、監視カメラ 1 a ～ 1 d と接続されている。サーバ 2 は、建物 A 1 内に設置されてもよいし、建物 A 1 とは別の場所に設置されてもよい。

【0027】

サーバ 2 は、ゾーン A ～ C ごとにおいて、ゾーン A ～ C に立ち入ることが（入室）できる人の顔の画像データ（以下、顔データと呼ぶことがある）を記憶（登録）している。サーバ 2 は、監視カメラ 1 a ～ 1 d が撮影した人の顔データと、登録されている顔データと

50

の照合を行う。サーバ２は、照合した結果を、端末装置３に送信する。

【００２８】

端末装置３は、ＬＡＮまたはインターネット等のネットワークによって、サーバ２と接続されている。端末装置３は、建物Ａ１内に設置されてもよいし、建物Ａ１とは別の場所に設置されてもよい。端末装置３は、例えば、パーソナルコンピュータ、スマートホン、またはタブレット端末等であってもよい。

【００２９】

なお、監視カメラ１ａ～１ｄは、ゾーンＡ～Ｃに入室する人を撮影するように設置されてもよい。例えば、監視カメラ１ａ～１ｄは、ゾーンＡ～Ｃの入り口付近を撮影するように設置されてもよい。

【００３０】

また、監視カメラ１ａ～１ｄには、ゾーンＡ～Ｃに既に設置されている監視カメラが用いられてもよい。例えば、監視カメラ１ａ～１ｄには、ゾーンＡ～Ｃの映像を録画する録画システムの一部として、既にゾーンＡ～Ｃに設置されている監視カメラを用いてもよい。この場合、監視カメラ１ａ～１ｄの出力を、録画システムとサーバ２とに分岐させてもよい。

【００３１】

図３は、監視カメラ１ａのブロック構成例を示した図である。図３に示すように、監視カメラ１ａは、撮像部１１と、制御部１２と、通信部１３と、記憶部１４と、を有している。

【００３２】

撮像部１１は、例えば、レンズおよび撮像素子（図示せず）を有している。撮像部１１のレンズは、撮像素子の受光面に被写体の像を結像する。レンズには、監視カメラ１ａの設置場所または撮影用途等に応じて、様々な焦点距離または撮影範囲のレンズを用いることができる。

【００３３】

撮像部１１の撮像素子は、受光面に受けた光を電気信号に変換する。撮像素子は、例えば、ＣＣＤ（Charge Coupled Device）またはＣＭＯＳ（Complementary Metal Oxide Semiconductor）等のイメージセンサである。撮像部１１は、撮像素子の受光面において受けた光に応じた電気信号（アナログ信号）をデジタル信号に変換して、制御部１２に出力する。

【００３４】

制御部１２は、監視カメラ１ａ全体を制御する。制御部１２は、例えば、ＣＰＵ（Central Processing Unit）またはＤＳＰ（Digital Signal Processor）によって構成されてもよい。制御部１２は、撮像部１１から出力される映像から、人の顔を判別する。制御部１２は、判別した人の顔を切り出し、切り出した顔の顔データ（静止画像）を、通信部１３を介してサーバ２に送信する。

【００３５】

通信部１３は、サーバ２と通信する。通信部１３は、例えば、イーサネット（登録商標）ケーブル等のネットワークケーブル（有線）を介して、サーバ２と通信してもよい。また、通信部１３は、例えば、Ｗｉ－Ｆｉ（登録商標）またはブルートゥース（登録商標）等の近距離無線通信を介して、サーバ２と通信してもよい。

【００３６】

記憶部１４は、制御部１２が動作するためのプログラムが記憶される。また、記憶部１４には、制御部１２が計算処理を行うためのデータ、または、制御部１２が各部を制御するためのデータ等が記憶される。記憶部１４は、ＲＡＭ（Random Access Memory）、ＲＯＭ（Read Only Memory）、フラッシュメモリ、およびＨＤＤ（Hard Disk Drive）などの記憶装置によって構成されてもよい。

【００３７】

なお、監視カメラ１ｂ～１ｄは、監視カメラ１ａと同様のブロック構成を有している。

10

20

30

40

50

従って、監視カメラ 1 b ～ 1 d のブロック構成の説明を省略する。

【 0 0 3 8 】

図 4 は、サーバ 2 のブロック構成例を示した図である。図 4 に示すように、サーバ 2 は、制御部 2 1 と、通信部 2 2 と、記憶部 2 3 と、を有している。

【 0 0 3 9 】

制御部 2 1 は、サーバ 2 全体を制御する。制御部 2 1 は、例えば、C P U によって構成されてもよい。

【 0 0 4 0 】

通信部 2 2 は、監視カメラ 1 a ～ 1 d および端末装置 3 と通信する。通信部 2 2 は、例えば、イーサネットケーブル等のネットワークケーブルを介して、監視カメラ 1 a ～ 1 d および端末装置 3 と通信してもよい。また、通信部 2 2 は、例えば、W i - F i (登録商標) またはブルートゥース (登録商標) 等の近距離無線通信を介して、監視カメラ 1 a ～ 1 d および端末装置 3 と通信してもよい。

【 0 0 4 1 】

記憶部 2 3 は、制御部 2 1 が動作するためのプログラムが記憶される。また、記憶部 2 3 には、制御部 2 1 が計算処理を行うためのデータ、または、制御部 2 1 が各部を制御するためのデータ等が記憶される。記憶部 2 3 は、R A M、R O M、フラッシュメモリ、および H D D などの記憶装置によって構成されてもよい。

【 0 0 4 2 】

図 5 は、端末装置 3 のブロック構成例を示した図である。図 5 に示すように、端末装置 3 は、制御部 3 1 と、入力部 3 2 と、表示部 3 3 と、通信部 3 4 と、記憶部 3 5 と、を有している。

【 0 0 4 3 】

制御部 3 1 は、端末装置 3 全体を制御する。制御部 3 1 は、例えば、C P U によって構成されてもよい。

【 0 0 4 4 】

入力部 3 2 は、例えば、キーボード、表示装置の画面上に重畳されたタッチパネル、またはマウス等の入力装置 (図示せず) に接続されている。入力部 3 2 は、入力装置から出力された、ユーザの操作に応じた信号を受信し、制御部 3 1 に出力する。

【 0 0 4 5 】

表示部 3 3 は、端末装置 3 が備える表示装置 (図示せず) に接続されている。表示部 3 3 は、制御部 3 1 から出力される画像データを表示装置に出力する。

【 0 0 4 6 】

以下では、説明を簡単にするため、ゾーン A とゾーン B とにおける入室者の検知について説明する。図 1 で説明したように、ゾーン A には、監視カメラ 1 a が設置され、ゾーン B には、監視カメラ 1 b , 1 c が設置されている。

【 0 0 4 7 】

図 6 は、サーバ 2 の記憶部 2 3 に記憶されるテーブルの一例を示した図である。図 6 に示すテーブル T B 1 は、例えば、監視カメラ 1 a ～ 1 c が建物 A 1 に設置されるときに、サーバ 2 の記憶部 2 3 に記憶される。テーブル T B 1 は、端末装置 3 によって作成され、サーバ 2 の記憶部 2 3 に記憶されてもよい。また、テーブル T B 1 の情報は、例えば、端末装置 3 によって追加、変更、または削除されてもよい。

【 0 0 4 8 】

テーブル T B 1 は、ゾーン識別情報 4 1 a と、顔データ 4 1 b と、を有している。ゾーン識別情報 4 1 a は、ゾーン A , B を識別する識別情報である。例えば、テーブル T B 1 の「A」は、ゾーン A の識別情報を示す。テーブル T B 1 の「B」は、ゾーン B の識別情報を示す。顔データ 4 1 b は、人の顔データである。

【 0 0 4 9 】

テーブル T B 1 は、ゾーンごとの入室が許可された人を示した情報と言ってもよい。例えば、テーブル T B 1 の丸が付されている行の顔データ 4 1 b の人は、丸が付されている

10

20

30

40

50

列のゾーン識別情報 4 1 a が示すゾーンに入室できることを示している。また、テーブル T B 1 のバーが付されている行の顔データ 4 1 b の人は、バーが付されている列のゾーン識別情報 4 1 a が示すゾーンに入室できないことを示している。

【 0 0 5 0 】

より具体的には、図 6 の顔データ 4 1 b a の顔の人は、ゾーン A , B に入室できる。図 6 の顔データ 4 1 b b の顔の人は、ゾーン A に入室できるが、ゾーン B には入室できない。図 6 の顔データ 4 1 b c の顔の人は、ゾーン A に入室できないが、ゾーン B に入室できる。

【 0 0 5 1 】

図 7 は、サーバ 2 の記憶部 2 3 に記憶されるテーブルの一例を示した図である。図 7 に示すテーブル T B 2 は、例えば、監視カメラ 1 a ~ 1 c が建物 A 1 に設置されるときに、サーバ 2 の記憶部 2 3 に記憶される。テーブル T B 2 は、端末装置 3 によって作成され、サーバ 2 の記憶部 2 3 に記憶されてもよい。また、テーブル T B 2 の情報は、例えば、端末装置 3 によって追加、変更、または削除されてもよい。

【 0 0 5 2 】

テーブル T B 2 は、ゾーン識別情報 4 2 a と、カメラ識別情報 4 2 b と、を有している。ゾーン識別情報 4 2 a は、ゾーンを識別する識別情報である。カメラ識別情報 4 2 b は、監視カメラ 1 a ~ 1 c を識別する識別情報である。例えば、カメラ識別情報 4 2 b の「 1 a 」は、監視カメラ 1 a の識別情報を示す。カメラ識別情報 4 2 b の「 1 b 」は、監視カメラ 1 b の識別情報を示す。カメラ識別情報 4 2 b の「 1 c 」は、監視カメラ 1 c の識別情報を示す。

【 0 0 5 3 】

テーブル T B 2 は、監視カメラ 1 a ~ 1 c のゾーンにおける設置場所を示した情報と言ってもよい。例えば、テーブル T B 2 の丸が付されている行のカメラ識別情報 4 2 b の監視カメラは、丸が付されている列のゾーン識別情報 4 2 a が示すゾーンに設置されていることを示している。また、テーブル T B 2 のバーが付されている行のカメラ識別情報 4 2 b の監視カメラは、バーが付されている列のゾーン識別情報 4 2 a が示すゾーンに設置されていないことを示している。

【 0 0 5 4 】

より具体的には、図 7 のカメラ識別情報 4 2 b a の監視カメラ 1 a は、ゾーン A に設置されている。図 7 のカメラ識別情報 4 2 b b の監視カメラ 1 b は、ゾーン B に設置されている。図 7 のカメラ識別情報 4 2 b c の監視カメラ 1 c は、ゾーン B に設置されている。

【 0 0 5 5 】

図 6 および図 7 では、テーブル T B 1 , T B 2 は、サーバ 2 の記憶部 2 3 に記憶されるとしたが、これに限られない。テーブル T B 1 およびテーブル T B 2 の両方または一方は、サーバ 2 とは別体のデータベースに記憶されてもよい。以下では、テーブル T B 1 は、登録 D B (D B : データベース) に記憶され、テーブル T B 2 は、サーバ 2 の記憶部 2 3 に記憶されとする。登録 D B は、例えば、サーバ 2 の一部と捉えてもよい。

【 0 0 5 6 】

図 8 は、監視カメラシステムの動作例を示したシーケンス図である。端末装置 3 の制御部 3 1 は、オペレータの操作に応じて、サーバ 2 に対し、ゾーン A , B と、監視カメラ 1 a ~ 1 c とのグルーピング設定を行う (ステップ S 1) 。すなわち、端末装置 3 の制御部 3 1 は、サーバ 2 に対し、ゾーン A , B と、監視カメラ 1 a ~ 1 c との対応付けの設定を行う。これにより、サーバ 2 の記憶部 2 3 には、例えば、図 7 に示したテーブル T B 2 が記憶される。

【 0 0 5 7 】

端末装置 3 の制御部 3 1 は、オペレータの操作に応じて、登録 D B に対し、ゾーン A , B への顔登録を行う (ステップ S 2 a , S 2 b) 。すなわち、端末装置 3 の制御部 3 1 は、登録 D B に対し、ゾーン A , B と、ゾーン A , B に入室できる人の顔データとの対応付けの設定を行う。これにより、登録 D B には、例えば、図 6 に示したテーブル T B 1 が記

10

20

30

40

50

憶される。なお、登録DBの情報登録は、サーバ2を経由して行われる。また、端末装置3の制御部31は、登録DBに登録する顔データを、他のシステムの顔データベースから入手してもよい。

【0058】

ゾーンAの監視カメラ1aの撮像部11は、人を撮影したとする。監視カメラ1aの制御部12は、撮像部11が撮影した映像の中から人の顔を切り出し、切り出した顔の顔データと、監視カメラ1aのカメラ識別情報とをサーバ2に送信する（ステップS3）。

【0059】

サーバ2の制御部21は、ステップS3にて送信された顔データと、監視カメラ1aのカメラ識別情報とを受信する（ステップS4）。

【0060】

サーバ2の制御部21は、記憶部23のテーブルTB2を参照し、ステップS4にて受信したカメラ識別情報に対応するゾーン識別情報を取得する（ステップS5）。

【0061】

図8の例では、サーバ2の制御部21は、ステップS4にて、監視カメラ1aのカメラ識別情報「1a」を受信している。従って、サーバ2の制御部21は、図7のテーブルTB2から、ゾーンAのゾーン識別情報「A」を取得する。これにより、サーバ2の制御部21は、ステップS4にて受信した顔データ51は、ゾーンAに設置された監視カメラ1aにおいて撮影されたものと特定（判定）できる。言い換えれば、サーバ2の制御部21は、ステップS4にて受信した顔データ51の顔の人は、ゾーンAに居ると特定できる。

【0062】

サーバ2の制御部21は、ステップS5にて、ゾーンを特定すると、登録DBのテーブルTB1を参照して、特定したゾーンに対応する顔データを取得する。そして、サーバ2の制御部21は、テーブルTB2から取得した顔データと、ステップS4にて受信した顔データとを照合する（ステップS6）。

【0063】

図8の例では、サーバ2の制御部21は、ステップS5にて、顔データ51の顔の人は、ゾーンAに居ると特定している。従って、サーバ2の制御部21は、図6に示したテーブルTB1のゾーンAに対応する顔データ41ba、41bbと、ステップS4にて受信した顔データ51とを照合する。顔データ51は、図6に示したテーブルTB1のゾーンAに対応する顔データ41baに一致するので、サーバ2の制御部21は、顔照合が一致したと判定する。すなわち、サーバ2の制御部21は、顔データ51の人は、ゾーンAへの立ち入りが許可された人と判定する。

【0064】

サーバ2の制御部21は、ステップS6の照合結果（顔照合OK）を端末装置3に送信する（ステップS7）。なお、サーバ2の制御部21は、顔照合OKを判定した場合、照合結果を端末装置3に送信しなくてもよい。言い換えれば、サーバ2の制御部21は、顔照合NGを判定した場合のみ、照合結果を端末装置3に送信してもよい。また、端末装置3の制御部31は、図8のステップS7において、顔照合OKの照合結果を受けると、その旨を表示装置に表示してもよい。

【0065】

ゾーンAの監視カメラ1aの撮像部11は、人を撮影したとする。監視カメラ1aの制御部12は、撮像部11が撮影した映像の中から人の顔を切り出し、切り出した顔の顔データと、監視カメラ1aのカメラ識別情報とをサーバ2に送信する（ステップS8）。

【0066】

サーバ2の制御部21は、ステップS8にて送信された顔データと、監視カメラ1aのカメラ識別情報とを受信する（ステップS9）。

【0067】

サーバ2の制御部21は、記憶部23のテーブルTB2を参照し、ステップS9にて受信したカメラ識別情報に対応するゾーン識別情報を取得する（ステップS10）。

10

20

30

40

50

【0068】

図8の例では、サーバ2の制御部21は、ステップS9にて、監視カメラ1aのカメラ識別情報「1a」を受信している。従って、サーバ2の制御部21は、図7のテーブルTB2から、ゾーンAのゾーン識別情報「A」を取得する。これにより、サーバ2の制御部21は、ステップS9にて受信した顔データ52は、ゾーンAに設置された監視カメラ1aにおいて撮影されたものと特定できる。言い換えれば、サーバ2の制御部21は、ステップS9にて受信した顔データ52の顔の人は、ゾーンAに居ると特定できる。

【0069】

サーバ2の制御部21は、ステップS10にて、ゾーンを特定すると、登録DBのテーブルTB1を参照して、特定したゾーンに対応する顔データを取得する。そして、サーバ2の制御部21は、テーブルTB2から取得した顔データと、ステップS9にて受信した顔データとを照合する（ステップS11）。

【0070】

図8の例では、サーバ2の制御部21は、ステップS10にて、顔データ52の顔の人は、ゾーンAに居ると特定している。従って、サーバ2の制御部21は、図6に示したゾーンAに対応する顔データ41ba, 41bbと、ステップS9にて受信した顔データ52とを照合する。顔データ52は、図6に示したゾーンAに対応する顔データ41ba, 41bbに一致しないので、サーバ2の制御部21は、顔照合が一致しないと判定する。すなわち、サーバ2の制御部21は、顔データ52の人は、ゾーンAへの立ち入りが許可されていない人と判定する。

【0071】

サーバ2の制御部21は、ステップS11の照合結果（顔照合NG）を端末装置3に送信する（ステップS12）。端末装置3の制御部31は、顔照合NGの照合結果を受けて、例えば、表示装置にアラートを表示する。なお、サーバ2の制御部21は、例えば、ゾーンAに設置されたスピーカ等の音声出力装置に、ステップS11の照合結果を送信してもよい。ゾーンAに設置された音声出力装置は、ステップS11の照合結果を受信すると、警告音等を出力してもよい。

【0072】

以上説明したように、サーバ2の通信部22は、建物A1の複数のゾーンA～Cを撮影する複数のカメラ1a～1dから、顔画像データを受信する。制御部21は、通信部22が受信した顔画像データと、ゾーンへの立ち入りが許可された人物の登録顔画像データとを照合し、顔画像データの人物が撮影されたゾーンにおける、顔画像データの人物の立ち入りの許可および不許可を判定する。これにより、サーバ2は、ゾーンA～Cごとに決められた人以外の人が、ゾーンA～Cに立ち入っていないかを判定できる。

【0073】

また、サーバ2は、複数の監視カメラ1a～1dの映像を集積し、建物A1のゾーンごとの立ち入りを判定する。これにより、監視カメラシステムを利用するユーザは、建物A1のゾーンごとにおける人の立ち入りの設定をサーバ2に対して行えばよく、ゾーン設定が容易となる。

【0074】

（変形例）

上記では、監視カメラ1a～1dが人の顔を切り出し、顔データをサーバ2に送信したがこれに限られない。監視カメラ1a～1dは、ゾーンの映像データをサーバ2に送信し、サーバ2が人の顔を検知して、切り出してもよい。この場合、監視カメラ1a～1dからサーバ2に送信される映像データには、顔データが含まれていると捉えてもよい。

【0075】

（第2の実施の形態）

第2の実施の形態では、人がゾーンに立ち入ってもよい時間も判定する。以下では、第1の実施の形態と異なる部分について説明する。

【0076】

図9は、第2の実施の形態に係るサーバ2の記憶部23に記憶されるテーブルの一例を示した図である。図9に示すテーブルTB11は、例えば、監視カメラ1a～1cが建物A1に設置されるときに、サーバ2の記憶部23に記憶される。テーブルTB11は、端末装置3によって作成され、サーバ2の記憶部23に記憶されてもよい。テーブルTB11の情報は、例えば、端末装置3によって追加、変更、または削除されてもよい。

【0077】

テーブルTB11は、図6で説明したテーブルTB1と同様に、ゾーン識別情報41aと、顔データ41bと、を有している。テーブルTB11は、ゾーンごとの入室が許可された人を示すとともに、その人のゾーンに滞在してもよい時間を示した情報と言ってもよい。例えば、テーブルTB11に示す時間は、その時間の行の顔データ41bの人が、その時間の列のゾーン識別情報41aが示すゾーンに入室できる時間を示している。

10

【0078】

より具体的には、図9の顔データ41baの顔の人は、9:00から19:00の間であれば、ゾーンAに入室できる。図9の顔データ41baの顔の人は、13:00から17:00の間であれば、ゾーンBに入室できる。図9の顔データ41bbの顔の人は、9:00から19:00の間であれば、ゾーンAに入室できる。図9の顔データ41bbの顔の人は、一日中ゾーンBに入室できない。図9の顔データ41bcの顔の人は、一日中ゾーンAに入室できない。図9の顔データ41bcの顔の人は、15:00から17:00の間であれば、ゾーンBに入室できる。

【0079】

上記では、テーブルTB11は、サーバ2の記憶部23に記憶されるとしたがこれに限られない。テーブルTB11は、登録DBに記憶されてもよい。

20

【0080】

第2の実施の形態のサーバ2の動作は、第1の実施の形態に対し、図8で説明したステップS6の顔照合の処理が異なる。サーバ2の制御部21は、ステップS6の顔照合の処理において、ステップS4にて受信した顔データ51の人の、ゾーンに居てもよい時間を判定する。

【0081】

例えば、サーバ2の制御部21は、ステップS5にて、顔データ51の顔の人は、ゾーンAに居ると特定している。従って、サーバ2の制御部21は、図9に示すゾーンAに対応する顔データ41ba、41bbと、ステップS4にて受信した顔データ51とを照合する。顔データ51は、図9に示したゾーンAに対応する顔データ41baに一致するので、サーバ2の制御部21は、顔照合が一致した顔データ41baのゾーンAに居てもよい時間（9:00から19:00）を判定する。サーバ2の制御部21は、現在時刻が9:00から19:00の間であれば、顔照合OKと判定する。一方、サーバ2の制御部21は、現在時刻が9:00から19:00の間でなければ、顔照合NGと判定する。

30

【0082】

以上説明したように、サーバ2の制御部21は、顔画像データの人物が撮影されたゾーンにおいて、顔画像データの人物が立ち入り許可された時間であるか否かを、顔画像データと現在時刻とを用いて判定する。これにより、サーバ2は、ゾーンA～Cごとに決められた人以外の人、ゾーンA～Cに立ち入っていないかを判定できる。

40

【0083】

（変形例）

ゾーンに居てもよい人の顔データおよび時間の登録は、端末装置3とは別の装置によって、サーバ2または登録DBに記憶されてもよい。

【0084】

図10は、顔データおよび時間の登録における監視カメラシステムの動作例を示したシーケンス図である。図10に示す端末装置61は、例えば、映画館、レストラン、マンション、事務所、またはコンサート会場等の、ゾーンが設定された施設を予約する人によって使用される端末である。施設を予約する人が、端末装置61を用いて、顔データおよび

50

施設のゾーンに立ち入る時間を登録する。図10に示す端末装置3は、例えば、映画館、レストラン、マンション、事務所、またはコンサート会場等の施設の管理者によって管理される。

【0085】

端末装置61は、例えば、スマートホン、タブレット端末、またはパーソナルコンピュータ等であってもよい。端末装置61には、顔データおよび時間をサーバ2または登録DBに登録するアプリケーションが搭載されてもよい。アプリケーションは、各施設の管理者によって提供されてもよい。端末装置61は、図5に示したブロック構成と同様のブロック構成を有する。

【0086】

以下、図10のシーケンスを説明する。図10では、施設に設置された監視カメラ1a～1dの図示を省略している。

【0087】

端末装置3の制御部31は、オペレータの操作に応じて、サーバ2に対し、ゾーンA、Bと、監視カメラ1a～1cとのグルーピング設定を行う（ステップS21）。すなわち、端末装置3の制御部31は、サーバ2に対し、ゾーンA、Bと、監視カメラ1a～1cとの対応付けの設定を行う。これにより、サーバ2の記憶部23には、例えば、図7に示したテーブルTB2が記憶される。

【0088】

ゾーンが設置された施設を予約する人（例えば、映画館を予約する人）は、例えば、端末装置61に顔データ、施設を利用する人の名前、利用するゾーンの情報（例えば、映画が上映される部屋の名前等）、およびゾーンに入る時間等の予約情報を入力する。端末装置61は、入力された予約情報をサーバ2に送信する（ステップS22）。

【0089】

サーバ2の制御部21は、端末装置61から送信された予約情報に基づいて、登録DBに対し、顔登録を行う（ステップS23）。すなわち、サーバ2の制御部21は、登録DBにおいて、図9に示したテーブルTB11を生成する。なお、サーバ2の制御部21は、記憶部23において、テーブルTB11を生成してもよい。

【0090】

サーバ2の制御部21は、ステップS22にて受信した予約情報を端末装置3に送信する（ステップS24）。端末装置3の管理者は、端末装置3が受信した予約情報によって、施設を利用する人の予約内容を把握できる。

【0091】

このように、ゾーンが設定された施設を利用する人が、端末装置61を用いて、顔データおよびゾーンに立ち入る時間をサーバ2または登録DBに設定してもよい。

【0092】

なお、例えば、レストランを予約する人が、レストランの予約をする際に、端末装置61を用いて、顔データおよび予約時間をサーバ2または登録DBに登録してもよい。ゾーンは、レストランの食事を提供する部屋ごとに設定されてもよい。

【0093】

また、例えば、マンションの住人が、端末装置61を用いて、来訪者の顔データおよび来訪時間をサーバ2または登録DBに登録してもよい。ゾーンは、マンションのエントランスごとおよびフロアごとに設定されてもよい。

【0094】

また、例えば、事務所の所員が、端末装置61を用いて、来訪者の顔データおよび来訪時間をサーバ2または登録DBに登録してもよい。ゾーンは、事務所のエントランスごと、フロアごと、または部屋ごとに設定されてもよい。

【0095】

また、例えば、コンサートを予約する人が、コンサートのチケットを予約する際に、端末装置61を用いて、顔データおよびコンサートを見る時間等をサーバ2または登録DB

10

20

30

40

50

に設定してもよい。ゾーンは、コンサート会場の席のクラスごとおよびボックスごとに設定されてもよい。

【0096】

(第3の実施の形態)

会社等では、社員は、所持するカードによって、入室できるゾーンが区別される場合がある。例えば、或る社員は、或る部屋の入口に設けられているカードリーダーにカードをかざすと、或る部屋に入室できるが、別の社員は、カードリーダーにカードをかざしても、或る部屋に入室できない。第3の実施の形態では、このようなカードのカード情報を用いて、顔データの登録を行う。

【0097】

図11は、第3の実施の形態に係る監視カメラシステムの一例を示した図である。図11において、図1と同じものには同じ符号が付してある。図11では、建物A1の図示を省略している。

【0098】

図11の監視カメラシステムは、図1に示した監視カメラシステムに対し、カードリーダー71a～71cを有している。

【0099】

カードリーダー71aは、例えば、ゾーンAの入り口扉の横に設置されている。カードリーダー71aには、ゾーンAのゾーン識別情報が紐付けられている。

【0100】

カードリーダー71bは、例えば、ゾーンBの入り口扉の横に設置されている。カードリーダー71bには、ゾーンBのゾーン識別情報が紐付けられている。

【0101】

カードリーダー71cは、例えば、ゾーンCの入り口扉の横に設置されている。カードリーダー71cには、ゾーンCのゾーン識別情報が紐付けられている。

【0102】

カードリーダー71aは、例えば、社員が所持するカードと近距離無線通信を行う。カードリーダー71aは、カードリーダー71aにかざされたカードから情報を読み取り、カードを所持する者がゾーンAに入室できる社員か否かを判定する。カードリーダー71b、71cもカードリーダー71aと同様に、かざされたカードから情報を読み取り、カードを所持する者がゾーンB、Cに入室できる社員か否かを判定する。

【0103】

カードリーダー71aは、読み取ったカード情報から、カードを所持する者が、ゾーンAに入室できる者と判定した場合、ゾーンAの入り口扉を解錠する。一方、カードリーダー71aは、読み取ったカード情報から、カードを所持する者が、ゾーンAに入室できない者と判定した場合、ゾーンAの入り口扉を解錠しない。カードリーダー71b、71cもカードリーダー71aと同様に、読み取ったカード情報から、ゾーンB、Cの入り口扉の解錠を制御する。

【0104】

社員が所持するカードには、社員の顔写真が付されている。カードリーダー71aは、カメラを備えている。カードリーダー71aは、ゾーンAの入り口扉を解錠する場合、カメラによって、カードに付されている社員の顔写真を撮影する(顔写真の静止画像を取得する)。そして、カードリーダー71aは、撮影した顔写真の顔データと、ゾーンAのゾーン識別情報とを、サーバ2に送信する。つまり、カードを所持する者が、カードを用いてゾーンAに入室できる場合、カードに付されている顔写真と、ゾーンAのゾーン識別情報とが紐付けられて、サーバ2に送信される。

【0105】

カードリーダー71b、71cもカードリーダー71aと同様に、カメラを備えている。カードリーダー71b、71cは、ゾーンB、Cの入り口扉を解錠する場合、カメラによって、カードに付されている社員の顔写真を撮影する。そして、カードリーダー71b、71c

10

20

30

40

50

は、撮影した顔写真の顔データと、ゾーンB，Cのゾーン識別情報とを、サーバ2に送信する。

【0106】

図12は、カードリーダー71aのブロック構成例を示した図である。図12に示すように、カードリーダー71aは、撮像部81と、制御部82と、カード通信部83と、通信部84と、記憶部85と、を有している。

【0107】

撮像部81は、例えば、レンズおよび撮像素子（図示せず）を有している。撮像部81のレンズは、撮像素子の受光面に被写体の像を結像する。レンズには、カードリーダー71aの設置場所または撮影用途等に応じて、様々な焦点距離または撮影範囲のレンズを用いることができる。

【0108】

撮像部81の撮像素子は、受光面に受けた光を電気信号に変換する。撮像素子は、例えば、CCDまたはCMOS等のイメージセンサである。撮像部81は、撮像素子の受光面において受けた光に応じた電気信号（アナログ信号）をデジタル信号に変換して、制御部82に出力する。

【0109】

制御部82は、カードリーダー71a全体を制御する。制御部82は、例えば、CPUまたはDSPによって構成されてもよい。制御部82は、撮像部81から出力される映像から、人の顔を判別する。制御部82は、判別した人の顔を切り出し、切り出した顔の顔データ（静止画像）を、通信部84を介してサーバ2に送信する。

【0110】

カード通信部83は、カードリーダー71aにかざされたカードと近距離無線通信を行う。

【0111】

通信部84は、サーバ2と通信する。通信部84は、例えば、イーサネットケーブル等のネットワークケーブルを介して、サーバ2と通信してもよい。また、通信部84は、例えば、Wi-Fi（登録商標）またはブルートゥース（登録商標）等の近距離無線通信を介して、サーバ2と通信してもよい。

【0112】

記憶部85は、制御部82が動作するためのプログラムが記憶される。また、記憶部85には、制御部82が計算処理を行うためのデータ、または、制御部82が各部を制御するためのデータ等が記憶される。記憶部85は、RAM、ROM、フラッシュメモリ、およびHDDなどの記憶装置によって構成されてもよい。

【0113】

以下では、説明を簡単にするため、ゾーンAとゾーンBとにおける入室者の検知について説明する。

【0114】

図13は、サーバ2の記憶部23に記憶されるテーブルの一例を示した図である。テーブルTB21は、図6で説明したテーブルTB1と同様に、ゾーン識別情報41aと、顔データ41bと、を有している。

【0115】

図13に示すテーブルTB21は、カードリーダー71a～71cから送信される顔データと、ゾーン識別情報とに基づいて生成される。顔データとゾーン識別情報は、上記したように、人がゾーンA，Bに入室できた場合に、カードリーダー71a～71cから送信される。従って、テーブルTB21は、ゾーンA，Bに入室できた人を示した情報と言ってもよい。

【0116】

例えば、顔データ41baの顔写真が付されたカードによって、人がゾーンAに入室したとする。この場合、サーバ2は、ゾーンAの入り口に設けられたカードリーダー71aから、顔データ41baと、ゾーン識別情報Aとを受信する。これにより、図13のテーブ

10

20

30

40

50

ル T B 2 1 には、点線枠 A 1 1 に示す情報が登録される。

【0117】

また、顔データ 4 1 b b の顔写真が付されたカードによって、人がゾーン A に入室したとする。この場合、サーバ 2 は、ゾーン A の入り口に設けられたカードリーダー 7 1 a から、顔データ 4 1 b b と、ゾーン識別情報 A とを受信する。これにより、図 1 3 のテーブル T B 2 1 には、点線枠 A 1 2 に示す情報が登録される。

【0118】

また、顔データ 4 1 b c の顔写真が付されたカードによって、人がゾーン B に入室したとする。この場合、サーバ 2 は、ゾーン B の入り口に設けられたカードリーダー 7 1 b から、顔データ 4 1 b c と、ゾーン識別情報 B とを受信する。これにより、図 1 3 のテーブル T B 2 1 には、点線枠 A 1 3 に示す情報が登録される。

【0119】

図 1 3 では、テーブル T B 2 1 は、サーバ 2 の記憶部 2 3 に記憶されとしたが、これに限られない。テーブル T B 2 1 は、登録 D B に記憶されてもよい。以下では、テーブル T B 2 1 は、登録 D B に記憶されとする。

【0120】

図 1 4 は、監視カメラシステムの動作例を示したシーケンス図である。図 1 4 では、ゾーン A、B と、カメラ 1 a ~ 1 c とのグルーピング設定（例えば、図 8 のステップ S 1 の処理）は、完了しているとする。すなわち、サーバ 2 の記憶部 2 3 には、図 7 に示したテーブル T B 2 が記憶されているとする。図 1 4 では、ゾーン B に設置された監視カメラ 1 b、1 c およびカードリーダー 7 1 b の処理の説明を省略する。

【0121】

カードリーダー 7 1 a は、かざされたカードのカード情報を取得する。カードリーダー 7 1 a は、取得したカード情報に基づいて、ゾーン A の入り口扉を解錠し、かざされたカードを撮影する。カードリーダー 7 1 a の制御部 8 2 は、撮影されたカードから、カードに付されている顔写真を切り出し、切り出した顔写真の顔データと、ゾーン A のゾーン識別情報とをサーバ 2 に送信する（ステップ S 3 1）。

【0122】

サーバ 2 の制御部 2 1 は、ステップ S 3 1 にて送信された情報に基づいて、登録 D B に対し、顔登録を行う（ステップ S 3 2）。例えば、サーバ 2 の制御部 2 1 は、登録 D B のテーブル T B 2 1 に対し、図 1 3 に示した点線枠 A 1 1 の情報を登録する。

【0123】

ここで、ステップ S 3 1 において、カードリーダー 7 1 a にかざされたカードは、盗難カードであったとする。例えば、図 1 4 に示す顔データ 9 1 の顔の人が、図 1 4 に示す顔データ 9 2 の顔の人になりすまし、盗難カードを用いて、ゾーン A に入室しているとする。

【0124】

ゾーン A の監視カメラ 1 a の撮像部 1 1 は、人（顔データ 9 1 の顔の人）を撮影したとする。監視カメラ 1 a の制御部 1 2 は、撮像部 1 1 が撮影した映像の中から人の顔を切り出し、切り出した顔の顔データと、監視カメラ 1 a のカメラ識別情報とをサーバ 2 に送信する（ステップ S 3 3）。

【0125】

サーバ 2 の制御部 2 1 は、ステップ S 3 3 にて送信された顔データと、監視カメラ 1 a のカメラ識別情報とを受信する（ステップ S 3 4）。

【0126】

サーバ 2 の制御部 2 1 は、記憶部 2 3 のテーブル T B 2 を参照し、ステップ S 3 4 にて受信したカメラ識別情報に対応するゾーン識別情報を取得する（ステップ S 3 5）。

【0127】

図 1 4 の例では、サーバ 2 の制御部 2 1 は、ステップ S 3 3 にて、監視カメラ 1 a のカメラ識別情報「1 a」を受信している。従って、サーバ 2 の制御部 2 1 は、図 7 のテーブル T B 2 から、ゾーン A のゾーン識別情報「A」を取得する。これにより、サーバ 2 の制

10

20

30

40

50

御部 2 1 は、ステップ S 3 4 にて受信した顔データ 9 1 は、ゾーン A に設置された監視カメラ 1 a において撮影されたものと特定できる。言い換えれば、サーバ 2 の制御部 2 1 は、ステップ S 3 4 にて受信した顔データ 9 1 の顔の人は、ゾーン A に居ると特定できる。

【0128】

サーバ 2 の制御部 2 1 は、ステップ S 3 5 にて、ゾーンを特定すると、登録 DB のテーブル T B 2 1 を参照して、特定したゾーンに対応する顔データを取得する。そして、サーバ 2 の制御部 2 1 は、テーブル T B 2 1 から取得した顔データと、ステップ S 3 4 にて受信した顔データとを照合する（ステップ S 3 6）。

【0129】

図 1 4 の例では、サーバ 2 の制御部 2 1 は、ステップ S 3 5 にて、顔データ 9 1 の顔の人は、ゾーン A に居ると特定している。従って、サーバ 2 の制御部 2 1 は、図 1 3 に示したテーブル T B 2 1 のゾーン A に対応する顔データ 4 1 b a , 4 1 b b と、ステップ S 3 4 にて受信した顔データ 9 1 とを照合する。顔データ 9 1 は、図 1 3 に示したゾーン A に対応する顔データ 4 1 b a , 4 1 b b に一致しないので、サーバ 2 の制御部 2 1 は、顔照合が一致しないと判定する。すなわち、サーバ 2 の制御部 2 1 は、顔データ 9 1 の人は、ゾーン A への立ち入りが許可されていない人と判定する。

【0130】

サーバ 2 の制御部 2 1 は、ステップ S 3 6 の照合結果を端末装置 3 に送信する（ステップ S 3 7）。端末装置 3 の制御部 3 1 は、顔照合 N G の照合結果を受けて、例えば、表示装置にアラートを表示する。

【0131】

以上説明したように、サーバ 2 の通信部 2 2 は、複数のゾーン A ~ C の各々に対応して設けられたカードリーダー 7 1 a ~ 7 1 c から、カードに付された顔写真の顔画像データを受信する。サーバ 2 の制御部 2 1 は、受信された顔画像データを、テーブル T B 2 1 の顔データとして記憶する。これにより、サーバ 2 は、ゾーン A ~ C ごとに決められた人以外の人、ゾーン A ~ C に立ち入っていないかを判定できる。

【0132】

（変形例 1）

カードリーダー 7 1 a ~ 7 1 c は、カードに付されている顔写真を撮影し、顔写真の顔データをサーバ 2 に送信するとしたがこれに限られない。例えば、カードは、I C（Integrated Circuit）を搭載していてもよい。I C には、カードを所持する社員の顔データが記憶されていてもよい。カードリーダー 7 1 a ~ 7 1 c は、カードに搭載されている I C から顔データを取得し、サーバ 2 に送信してもよい。

【0133】

（変形例 2）

カードリーダー 7 1 a ~ 7 1 c は、カードから読み取った名前またはカードのカード識別情報をサーバ 2 に送信してもよい。サーバ 2 の制御部 2 1 は、カードリーダー 7 1 a ~ 7 1 c から送信された名前またはカード識別情報を受信すると、カード情報を管理するサーバから、名前またはカード識別情報に対応する顔データを受信してもよい。そして、サーバ 2 の制御部 2 1 は、受信した顔データと、カードリーダー 7 1 a ~ 7 1 c から受信したゾーン識別情報とに基づいて、図 1 3 に示したテーブル T B 2 1 を生成してもよい。なお、カード情報を管理するサーバには、カードを所持する人の顔データと、名前またはカード識別情報とが対応付けられて記憶されている。

【0134】

（変形例 3）

カードリーダー 7 1 a ~ 7 1 c を含む監視カメラシステムは、会社設置される例について説明したがこれに限られない。カードリーダー 7 1 a ~ 7 1 c を含む監視カメラシステムは、マンションまたは商業施設等に設置されてもよい。

【0135】

（第 4 の実施の形態）

10

20

30

40

50

第4の実施の形態では、ゾーンごとにおいて、人の立ち入り監視の条件が異なる場合について説明する。例えば、監視カメラシステムは、或るゾーンでは、ブラックリスト方式で人の立ち入りを判定し、別のゾーンでは、ホワイトリスト方式で人の立ち入りを判定する。

【0136】

図15は、第4の実施の形態に係る監視カメラシステムの一例を示した図である。図15に示すように、監視カメラシステムは、監視カメラ101a、101bと、サーバ102と、端末装置103と、警報装置104a、104b、105a、105bと、を有している。図15には、監視カメラシステムの他に、建物A101の内部の平面図が示してある。

10

【0137】

建物A101は、ゾーンA、Bを有している。ゾーンA、Bは、隣接している。建物A101は、例えば、建物A101の外からゾーンAに入るための入り口A102aと、ゾーンAを経由してゾーンBに入るための入り口A102bとを有している。ゾーンBには、ゾーンAを通過すると立ち入ることができる。

【0138】

建物A101は、例えば、スーパーまたはコンビニエンスストア等の店舗である。建物A101のゾーンAは、例えば、商品の売り場である。ゾーンBは、例えば、在庫を保管し、または、商品を加工するバックヤードである。

【0139】

監視カメラ101aは、建物A101のゾーンAに設置される。監視カメラ101bは、建物A101のゾーンBに設置される。

20

【0140】

監視カメラ101a、101bは、ゾーンA、B内に居る人を撮影するように建物A101に設置される。例えば、監視カメラ101aは、ゾーンA内の全体を撮影するように、ゾーンAの天井または壁等に設置される。監視カメラ101bは、ゾーンB内の全体を撮影するように、ゾーンBの天井または壁等に設置される。

【0141】

サーバ102は、例えば、LANまたはインターネット等のネットワークによって、監視カメラ101a、101bと接続されている。サーバ102は、建物A101内に設置されてもよいし、建物A101とは別の場所に設置されてもよい。

30

【0142】

サーバ102は、ゾーンAに立ち入ることができない人の顔データと、ゾーンBに立ち入ることができる人の顔データとを記憶（登録）している。言い換えれば、サーバ102は、ゾーンAに立ち入ることができない人のブラックリストと、ゾーンBに立ち入ることができる人のホワイトリストとを有している。サーバ102は、監視カメラ101a、101bが撮影した人の顔データと、登録されている顔データとの照合を行う。サーバ102は、照合結果を、端末装置103および警報装置104a、104b、105a、105bに送信する。

【0143】

端末装置103は、LANまたはインターネット等のネットワークによって、サーバ102と接続されている。端末装置103は、建物A101内に設置されてもよいし、建物A101とは別の場所に設置されてもよい。端末装置103は、例えば、パーソナルコンピュータ、スマートフォン、またはタブレット端末等であってもよい。

40

【0144】

警報装置104a、104bは、サーバ102から出力されるアラーム信号を受信する。警報装置104a、104bは、例えば、警報ランプである。警報装置104a、104bは、アラーム信号を受信すると発光する。警報装置104aは、ゾーンAに設置され、警報装置104bは、ゾーンBに設置される。

【0145】

50

警報装置 105a, 105b は、サーバ 102 から出力されるアラーム信号を、無線通信によって受信する。警報装置 105a, 105b は、例えば、建物 A 101 のスタッフが所持する携帯型の警報装置である。警報装置 105a, 105b は、アラーム信号を受信すると振動する。また、警報装置 105a, 105b は、アラーム信号を受信すると発光または音を出力してもよい。図 15 では、警報装置 105a は、ゾーン A に位置し、警報装置 105b は、ゾーン B に位置しているが、これに限られない。警報装置 105a, 105b の位置は、警報装置 105a, 105b を所持するスタッフの移動に応じて変わる。

【0146】

なお、監視カメラ 101a, 101b は、ゾーン A, B に入室する人を撮影するように設置されてもよい。例えば、監視カメラ 101a は、ゾーン A の入り口 A 102a 付近を撮影するように設置されてもよい。監視カメラ 101b は、ゾーン B の入り口 A 102b 付近を撮影するように設置されてもよい。

【0147】

また、ゾーン A, B の各々には、複数の監視カメラが設置されてもよい。ゾーン A, B の各々は、複数の監視カメラによって、ゾーン A, B 内にいる人を撮影するように設置されてもよい。

【0148】

また、監視カメラ 101a, 101b には、ゾーン A, B に既に設置されている監視カメラが用いられてもよい。例えば、監視カメラ 101a, 101b には、ゾーン A, B の映像を録画する録画システムの一部として、既にゾーン A, B に設置されている監視カメラを用いてもよい。この場合、監視カメラ 101a, 101b の出力を、録画システムとサーバ 102 とに分岐させてもよい。

【0149】

また、ゾーンの数、2 つに限られない。ゾーンは、3 以上であってもよい。3 以上のゾーン各々に設置される監視カメラは、サーバ 102 に接続される。サーバ 102 は、3 以上のゾーン各々において、ブラックリストおよびホワイトリストのいずれか一方を用いて、ゾーンへの人の立ち入りを判定する。

【0150】

また、監視カメラシステムは、監視カメラ 101a, 101b が撮影した映像データを録画するレコーダを備えてもよい。監視カメラシステムは、監視カメラ 101a, 101b が撮影した映像データをリアルタイムで表示するモニタリング装置を備えてもよい。モニタリング装置は、例えば、パーソナルコンピュータ、スマートフォン、またはタブレット端末等であってもよい。

【0151】

また、監視カメラ 101a, 101b は、図 3 で説明した監視カメラ 1a と同様の構成を有し、その説明を省略する。サーバ 102 は、図 4 で説明したサーバ 2 と同様の構成を有し、その説明を省略する。端末装置 103 は、図 5 で説明した端末装置 3 と同様の構成を有し、その説明を省略する。

【0152】

以下では、建物 A 101 を店舗として説明する。

【0153】

図 16 は、監視カメラシステムの概略動作を説明する図である。図 16 において、図 15 と同じものには同じ符号が付してある。図 16 には、人の顔データ 111 ~ 113 が示してある。

【0154】

顔データ 111 は、例えば、以前に万引きをした疑いのある人物または万引きを行った人物等の注意人物の顔データである。注意人物は、商品売り場であるゾーン A に立ち入ると、端末装置 103 および警報装置 104a, 104b, 105a, 105b に報知（アラーム信号が出力）される。これにより、例えば、店舗の従業員は、注意人物が商品売り

10

20

30

40

50

場であるゾーンAに出現したことを認識でき、注意人物を監視できる。なお、注意人物は、バックヤードであるゾーンBに立ち入っても、端末装置103および警報装置104a, 104b, 105a, 105bに報知される。

【0155】

顔データ112は、店舗と取引する業者の顔データである。業者は、商品売り場であるゾーンAに立ち入っても端末装置103および警報装置104a, 104b, 105a, 105bに報知されないが、バックヤードのゾーンBに立ち入ると、端末装置103および警報装置104a, 104b, 105a, 105bに報知される。これにより、例えば、店舗の従業員は、業者がバックヤードであるゾーンBに出現したことを認識でき、業者に対し、ゾーンBは関係者以外立ち入り禁止であることを伝えることができる。

10

【0156】

顔データ113は、店舗の従業員である。従業員は、商品売り場であるゾーンAおよびバックヤードであるゾーンBに立ち入っても、端末装置103および警報装置104a, 104b, 105a, 105bに報知されない。すなわち、従業員は、ゾーンAおよびゾーンBを自由に行き来できる。

【0157】

サーバ102は、売り場であるゾーンAにおいては、ブラックリストを用いて、特定人物のゾーンAへの立ち入りを判定する。

【0158】

例えば、注意人物の顔データ111は、ブラックリストに登録される。従って、ブラックリストに登録された注意人物が、監視カメラ101aによって撮影された場合、監視カメラ101aによって撮影された注意人物の顔データと、ブラックリストに登録されている顔データ111とが一致し、サーバ102は、アラーム信号を端末装置103および警報装置104a, 104b, 105a, 105bに出力する。

20

【0159】

サーバ102は、バックヤードであるゾーンBにおいては、ホワイトリストを用いて、特定人物のゾーンBへの立ち入りを判定する。

【0160】

例えば、従業員の顔データ113は、ホワイトリストに登録される。従って、ホワイトリストに登録されていない、従業員以外の人物が、監視カメラ101bによって撮影された場合、監視カメラ101bによって撮影された人物の顔データと、ホワイトリストに登録されている従業員の顔データ113とが一致しないため、サーバ102は、アラーム信号を端末装置103および警報装置104a, 104b, 105a, 105bに出力する。

30

【0161】

すなわち、サーバ102は、ブラックリストに登録された人物がゾーンAに出現した場合、アラーム信号を端末装置103および警報装置104a, 104b, 105a, 105bに出力する。また、サーバ102は、ホワイトリストに登録されていない人物がゾーンBに出現した場合、アラーム信号を端末装置103および警報装置104a, 104b, 105a, 105bに出力する。

【0162】

図17は、サーバ102の記憶部に記憶されるテーブルの一例を示した図である。図17に示すテーブルTB101は、例えば、監視カメラ101a, 101bが建物A101に設置されるときに、サーバ102の記憶部に記憶される。テーブルTB101は、端末装置103によって作成され、サーバ102の記憶部に記憶されてもよい。また、テーブルTB101の情報は、例えば、端末装置103によって追加、変更、または削除されてもよい。

40

【0163】

テーブルTB101は、ゾーン識別情報121aと、カメラ識別情報121bと、を有している。ゾーン識別情報121aは、ゾーンA, Bを識別する識別情報である。例えば、ゾーン識別情報121aの「A」は、ゾーンAの識別情報を示す。ゾーン識別情報12

50

1 aの「B」は、ゾーンBの識別情報を示す。

【0164】

カメラ識別情報121bは、監視カメラ101a, 101bを識別する識別情報である。例えば、カメラ識別情報121bの「101a」は、監視カメラ101aの識別情報を示す。カメラ識別情報121bの「101b」は、監視カメラ101bの識別情報を示す。

【0165】

テーブルTB101は、監視カメラ101a, 101bのゾーンにおける設置場所を示した情報と捉えてもよい。例えば、図17に示すカメラ識別情報「101a」の監視カメラ101aは、ゾーンAに設置されていることを示す。図17に示すカメラ識別情報「101b」の監視カメラ101bは、ゾーンBに設置されていることを示す。

10

【0166】

図18は、サーバ102の記憶部に記憶されるテーブルの一例を示した図である。図18に示すテーブルTB102は、例えば、監視カメラ101a, 101bが建物A101に設置されるときに、サーバ102の記憶部に記憶される。テーブルTB102は、端末装置103によって作成され、サーバ102の記憶部に記憶されてもよい。また、テーブルTB102の情報は、例えば、端末装置103によって追加、変更、または削除されてもよい。

【0167】

テーブルTB102は、ゾーン識別情報131aと、リスト情報131bと、顔データ131cと、を有している。ゾーン識別情報131aは、ゾーンA, Bを識別する識別情報である。例えば、ゾーン識別情報131aの「A」は、ゾーンAの識別情報を示す。ゾーン識別情報131aの「B」は、ゾーンBの識別情報を示す。

20

【0168】

リスト情報131bは、対応するゾーンにおける判定種別を示す情報である。図18に示すBLは、ブラックリスト方式によって、対応するゾーンの立ち入りを判定することを示す。WLは、ホワイトリスト方式によって、対応するゾーンの立ち入りを判定することを示す。

【0169】

例えば、図18の例の場合、ゾーンAのリスト情報131bは、「BL」である。従って、ゾーンAでは、ブラックリスト方式によって、人の立ち入りが判定される。また、ゾーンBのリスト情報131bは、「WL」である。従って、ゾーンBでは、ホワイトリスト方式によって、人の立ち入りが判定される。

30

【0170】

顔データ131cは、人の顔データである。顔データ132aは、例えば、図16で説明した顔データ113に対応し、従業員の顔データである。顔データ132bは、例えば、図16で説明した顔データ111に対応し、注意人物の顔データである。

【0171】

テーブルTB102は、ゾーンごとにおいて、顔データの人物がブラックリスト方式によって判定されるのか、ホワイトリスト方式によって判定されるのかを規定したテーブルと捉えてもよい。

40

【0172】

例えば、テーブルTB102の顔データ132aの人は、ゾーンB（ホワイトリスト）に丸が付されている。従って、顔データ132aの人は、ゾーンBに立ち入ってもアラーム信号が出力されない。一方、図18のゾーンBの列に丸が付されていない人物およびテーブルTB102に顔データが登録されていない人物は、ゾーンBに立ち入るとアラーム信号が出力される。

【0173】

また、テーブルTB102の顔データ132bの人は、ゾーンA（ブラックリスト）に丸が付されている。従って、顔データ132bの人は、ゾーンAに立ち入るとアラーム信号が出力される。一方、図18のゾーンAの列に丸が付されていない人物およびテーブル

50

T B 1 0 2 に顔データが登録されていない人物は、ゾーン A に立ち入ってもアラーム信号が出力されない。

【 0 1 7 4 】

なお、「人物がブラックリストに登録された」とは、その人物の顔データがテーブル T B 1 0 2 に登録され、リスト情報 1 3 1 b のブラックリストの列に情報（図 1 8 では丸）が登録されることを意味してもよい。また、「人物がホワイトリストに登録された」とは、その人物の顔データがテーブル T B 1 0 2 に登録され、リスト情報 1 3 1 b のホワイトリストの列に情報（図 1 8 では丸）が登録されることを意味してもよい。

【 0 1 7 5 】

図 1 7 および図 1 8 では、テーブル T B 1 0 1 , T B 1 0 2 は、サーバ 1 0 2 の記憶部に記憶されたとしたが、これに限られない。テーブル T B 1 0 1 およびテーブル T B 1 0 2 の両方または一方は、サーバ 1 0 2 とは別体のデータベースに記憶されてもよい。別体のデータベースは、サーバ 1 0 2 の一部と捉えてもよい。以下では、テーブル T B 1 0 1 , T B 1 0 2 は、登録 D B に記憶されとする。

【 0 1 7 6 】

図 1 9 は、監視カメラシステムの動作例を示したシーケンス図である。端末装置 1 0 3 の制御部は、例えば、店舗の従業員等であるオペレータの操作に応じて、サーバ 1 0 2 を経由し、登録 D B に対し、ゾーン A , B と、監視カメラ 1 0 1 a , 1 0 1 b との紐付けを行う（ステップ S 4 1 , S 4 2 ）。また、端末装置 1 0 3 の制御部は、オペレータの操作に応じて、サーバ 1 0 2 を経由し、登録 D B に対し、ゾーン A , B と、ブラックリストおよびホワイトリストとの紐付けを行う（ステップ S 4 1 , S 4 2 ）。

【 0 1 7 7 】

すなわち、端末装置 1 0 3 の制御部は、登録 D B に対し、ゾーン A , B と、監視カメラ 1 0 1 a , 1 0 1 b との対応付けの設定を行う。これにより、登録 D B には、例えば、図 1 7 に示したテーブル T B 1 0 2 が記憶される。また、端末装置 1 0 3 の制御部は、登録 D B に対し、ゾーン A , B と、ブラックリストおよびホワイトリストとの対応付けの設定を行う。これにより、登録 D B には、例えば、図 1 8 に示したテーブル T B 1 0 2 のゾーン識別情報 1 3 1 a と、リスト情報 1 3 1 b とが記憶される。

【 0 1 7 8 】

端末装置 1 0 3 の制御部は、オペレータの操作に応じて、サーバ 1 0 2 を経由し、登録 D B に対し、顔データを登録する（ステップ S 4 3 , S 4 4 ）。これにより、登録 D B には、例えば、図 1 8 に示したテーブル T B 1 0 2 の顔データ 1 3 1 c が記憶される。

【 0 1 7 9 】

端末装置 1 0 3 の制御部は、オペレータの操作に応じて、サーバ 1 0 2 を経由し、登録 D B に登録した顔データと、ゾーンとの紐付けを行う（ステップ S 4 5 , S 4 6 ）。例えば、端末装置 1 0 3 の制御部は、登録 D B に登録した顔データ 1 3 2 b をゾーン A （ブラックリスト）と紐付ける。また、端末装置 1 0 3 の制御部は、登録 D B に登録した顔データ 1 3 2 a をゾーン B （ホワイトリスト）と紐付ける。これにより、登録 D B には、例えば、図 1 8 に示したテーブル T B 1 0 2 の丸とバーに関する情報が記憶される。

【 0 1 8 0 】

ゾーン A の監視カメラ 1 0 1 a の撮像部は、人を撮影したとする。監視カメラ 1 0 1 a の制御部は、撮像部が撮影した映像の中から人の顔を切り出し、切り出した顔の顔データと、監視カメラ 1 0 1 a のカメラ識別情報とをサーバ 1 0 2 に送信する（ステップ S 4 7 ）。

【 0 1 8 1 】

サーバ 1 0 2 の制御部は、ステップ S 4 7 にて送信された顔データと、登録 D B に記憶されている顔データとを照合する（ステップ S 4 8 ）。

【 0 1 8 2 】

例えば、サーバ 1 0 2 の制御部は、登録 D B のテーブル T B 1 0 1 を参照し、ステップ S 4 7 にて送信されたカメラ識別情報に対応するゾーン識別情報を取得する。図 1 9 の例

10

20

30

40

50

では、ステップS 4 7にて、監視カメラ1 0 1 aのカメラ識別情報「1 0 1 a」が送信されている。従って、サーバ1 0 2の制御部は、図1 7のテーブルTB 1 0 1から、ゾーンAのゾーン識別情報「A」を取得する。これにより、サーバ1 0 2の制御部は、ステップS 4 7にて送信された顔データ1 4 1は、ゾーンAに設置された監視カメラ1 0 1 aにおいて撮影されたものと特定（判定）できる。言い換えれば、サーバ1 0 2の制御部は、ステップS 4 7にて送信された顔データ1 4 1の顔の人は、ゾーンAに居ると特定できる。

【0 1 8 3】

サーバ1 0 2の制御部は、ゾーンを特定すると、登録DBのテーブルTB 1 0 2を参照して、特定したゾーンに対応する顔データおよびリスト情報を取得する。そして、サーバ1 0 2の制御部は、テーブルTB 1 0 2から取得した顔データと、ステップS 4 7にて送信された顔データとを照合し、テーブルTB 1 0 2から取得したリスト情報の方式（ブラックリスト方式またはホワイトリスト方式）に従って、人のゾーンA，Bへの立ち入りを判定する。

【0 1 8 4】

図1 9の例では、サーバ1 0 2の制御部は、顔データ1 4 1の顔の人は、ゾーンAに居ると特定している。ゾーンAのリスト情報は、ブラックリストである。従って、サーバ1 0 2の制御部は、図1 8に示したテーブルTB 1 0 2のゾーンAに対応する顔データ1 3 2 bと、ステップS 4 7にて送信された顔データ1 4 1とを照合する。顔データ1 4 1は、図1 8に示したテーブルTB 1 0 2の顔データ1 3 2 bに一致するので、サーバ1 0 2の制御部は、顔照合が一致したと判定する。すなわち、サーバ1 0 2の制御部は、ステップS 4 7にて送信された顔データ1 4 1の人は、ブラックリストに登録された人物と判定する。

【0 1 8 5】

サーバ1 0 2の制御部は、ステップS 4 8の照合結果（登録顔検知のアラーム信号）を端末装置1 0 3および警報装置1 0 4 a，1 0 5 a，1 0 5 bに送信する（ステップS 4 9）。なお、サーバ1 0 2の制御部は、登録顔検知を判定した場合、監視カメラ1 0 1 aが撮影した顔データ1 4 1または顔データ1 4 1に一致したテーブルTB 1 0 2に記憶されている顔データ1 3 2 bを端末装置1 0 3に送信する。端末装置1 0 3の制御部は、サーバ1 0 2から送信された顔データ1 4 1または顔データ1 3 2 bを表示装置に表示する。

【0 1 8 6】

ゾーンAの監視カメラ1 0 1 aの撮像部は、人を撮影したとする。監視カメラ1 0 1 aの制御部は、撮像部が撮影した映像の中から人の顔を切り出し、切り出した顔の顔データと、監視カメラ1 0 1 aのカメラ識別情報とをサーバ1 0 2に送信する（ステップS 5 0）。

【0 1 8 7】

サーバ1 0 2の制御部は、ステップS 5 0にて送信された顔データと、登録DBに記憶されている顔データとを照合する（ステップS 5 1）。

【0 1 8 8】

例えば、サーバ1 0 2の制御部は、登録DBのテーブルTB 1 0 1を参照し、ステップS 5 0にて送信されたカメラ識別情報に対応するゾーン識別情報を取得する。図1 9の例では、ステップS 5 0にて、監視カメラ1 0 1 aのカメラ識別情報「1 0 1 a」が送信されている。従って、サーバ1 0 2の制御部は、図1 7のテーブルTB 1 0 1から、ゾーンAのゾーン識別情報「A」を取得する。これにより、サーバ1 0 2の制御部は、ステップS 5 0にて送信された顔データ1 4 2は、ゾーンAに設置された監視カメラ1 0 1 aにおいて撮影されたものと特定できる。言い換えれば、サーバ1 0 2の制御部は、ステップS 5 0にて送信された顔データ1 4 2の顔の人は、ゾーンAに居ると特定できる。

【0 1 8 9】

サーバ1 0 2の制御部は、ゾーンを特定すると、登録DBのテーブルTB 1 0 2を参照して、特定したゾーンに対応する顔データおよびリスト情報を取得する。そして、サーバ1 0 2の制御部は、テーブルTB 1 0 2から取得した顔データと、ステップS 5 0にて送

10

20

30

40

50

信された顔データとを照合し、テーブルＴＢ１０２から取得したリスト情報の方式に従って、人のゾーンＡ，Ｂへの立ち入りを判定する。

【０１９０】

図１９の例では、サーバ１０２の制御部は、顔データ１４２の顔の人は、ゾーンＡに居ると特定している。ゾーンＡのリスト情報は、ブラックリストである。従って、サーバ１０２の制御部は、図１８に示したテーブルＴＢ１０２のゾーンＡに対応する顔データ１３２ｂと、ステップＳ５０にて送信された顔データ１４２とを照合する。顔データ１４２は、図１８に示したテーブルＴＢ１０２の顔データ１３２ｂに一致しないので、サーバ１０２の制御部は、顔照合が一致しないと判定する。すなわち、サーバ１０２の制御部は、顔データ１４２の人は、ブラックリストに登録されていない人物と判定する。

10

【０１９１】

なお、顔データ１４２の人は、ブラックリストに登録されていない人物なので、サーバ１０２の制御部は、アラーム信号を端末装置１０３および警報装置１０４ａ，１０５ａ，１０５ｂに送信しない。

【０１９２】

ゾーンＢの監視カメラ１０１ｂの撮像部は、人を撮影したとする。監視カメラ１０１ｂの制御部は、撮像部が撮影した映像の中から人の顔を切り出し、切り出した顔の顔データと、監視カメラ１０１ｂのカメラ識別情報とをサーバ１０２に送信する（ステップＳ５２）。

【０１９３】

サーバ１０２の制御部は、ステップＳ５２にて送信された顔データと、登録ＤＢに記憶されている顔データとを照合する（ステップＳ５３）。

20

【０１９４】

例えば、サーバ１０２の制御部は、登録ＤＢのテーブルＴＢ１０１を参照し、ステップＳ５２にて送信されたカメラ識別情報に対応するゾーン識別情報を取得する。図１９の例では、ステップＳ５２にて、監視カメラ１０１ｂのカメラ識別情報「１０１ｂ」が送信されている。従って、サーバ１０２の制御部は、図１７のテーブルＴＢ１０１から、ゾーンＢのゾーン識別情報「Ｂ」を取得する。これにより、サーバ１０２の制御部は、ステップＳ５２にて送信された顔データ１４３は、ゾーンＢに設置された監視カメラ１０１ｂにおいて撮影されたものと特定できる。言い換えれば、サーバ１０２の制御部は、ステップＳ５２にて送信された顔データ１４３の顔の人は、ゾーンＢに居ると特定できる。

30

【０１９５】

サーバ１０２の制御部は、ゾーンを特定すると、登録ＤＢのテーブルＴＢ１０２を参照して、特定したゾーンに対応する顔データおよびリスト情報を取得する。そして、サーバ１０２の制御部は、テーブルＴＢ１０２から取得した顔データと、ステップＳ５２にて送信された顔データとを照合し、テーブルＴＢ１０２から取得したリスト情報の方式に従って、人のゾーンＡ，Ｂへの立ち入りを判定する。

【０１９６】

図１９の例では、サーバ１０２の制御部は、顔データ１４３の顔の人は、ゾーンＢに居ると特定している。ゾーンＢのリスト情報は、ホワイトリストである。従って、サーバ１０２の制御部は、図１８に示したテーブルＴＢ１０２のゾーンＢに対応する顔データ１３２ｂと、ステップＳ５２にて送信された顔データ１４３とを照合する。顔データ１４３は、図１８に示したテーブルＴＢ１０２の顔データ１３２ａに一致しないので、サーバ１０２の制御部は、顔照合が一致しないと判定する。すなわち、サーバ１０２の制御部は、顔データ１４３の人は、ホワイトリストに登録されていない人物と判定する。

40

【０１９７】

サーバ１０２の制御部は、ステップＳ５３の照合結果（未登録顔検知のアラーム信号）を端末装置１０３および警報装置１０４ａ，１０５ａ，１０５ｂに送信する（ステップＳ５４）。なお、サーバ１０２の制御部は、未登録顔検知を判定した場合、監視カメラ１０１ｂが撮影した顔データ１４３を端末装置１０３に送信する。端末装置１０３の制御部は

50

、サーバ１０２から送信された顔データ１４３を表示装置に表示する。

【０１９８】

ゾーンＢの監視カメラ１０１ｂの撮像部は、人を撮影したとする。監視カメラ１０１ｂの制御部は、撮像部が撮影した映像の中から人の顔を切り出し、切り出した顔の顔データと、監視カメラ１０１ｂのカメラ識別情報とをサーバ１０２に送信する（ステップＳ５５）。

【０１９９】

サーバ１０２の制御部は、ステップＳ５５にて送信された顔データと、登録ＤＢに記憶されている顔データとを照合する（ステップＳ５６）。

【０２００】

例えば、サーバ１０２の制御部は、登録ＤＢのテーブルＴＢ１０１を参照し、ステップＳ５５にて送信されたカメラ識別情報に対応するゾーン識別情報を取得する。図１９の例では、ステップＳ５５にて、監視カメラ１０１ｂのカメラ識別情報「１０１ｂ」が送信されている。従って、サーバ１０２の制御部は、図１７のテーブルＴＢ１０１から、ゾーンＢのゾーン識別情報「Ｂ」を取得する。これにより、サーバ１０２の制御部は、ステップＳ５５にて送信された顔データ１４４は、ゾーンＢに設置された監視カメラ１０１ｂにおいて撮影されたものと特定できる。言い換えれば、サーバ１０２の制御部は、ステップＳ５５にて送信された顔データ１４４の顔の人は、ゾーンＢに居ると特定できる。

【０２０１】

サーバ１０２の制御部は、ゾーンを特定すると、登録ＤＢのテーブルＴＢ１０２を参照して、特定したゾーンに対応する顔データおよびリスト情報を取得する。そして、サーバ１０２の制御部は、テーブルＴＢ１０２から取得した顔データと、ステップＳ５５にて送信された顔データとを照合し、テーブルＴＢ１０２から取得したリスト情報の方式に従って、人のゾーンＡ，Ｂへの立ち入りを判定する。

【０２０２】

図１９の例では、サーバ１０２の制御部は、顔データ１４４の顔の人は、ゾーンＢに居ると特定している。ゾーンＢのリスト情報は、ホワイトリストである。従って、サーバ１０２の制御部は、図１８に示したテーブルＴＢ１０２のゾーンＢに対応する顔データ１３２ａと、ステップＳ５５にて送信された顔データ１４４とを照合する。顔データ１４４は、図１８に示したテーブルＴＢ１０２の顔データ１３２ａに一致するので、サーバ１０２の制御部は、顔照合が一致したと判定する。すなわち、サーバ１０２の制御部は、顔データ１４４の人は、ホワイトリストに登録された人物と判定する。

【０２０３】

なお、顔データ１４４の人は、ホワイトリストに登録された人物なので、サーバ１０２の制御部は、アラーム信号を端末装置１０３および警報装置１０４ａ，１０５ａ，１０５ｂに送信しない。

【０２０４】

図２０は、ブラックリスト方式における判定方法を説明する図である。図２０の矢印Ａ１１１～Ａ１１３は、人がゾーンＡに立ち入る様子を示している。また、図２０には、テーブルＴＢ１０２のゾーンＡ（ブラックリスト）に登録された顔データ１５１が示してある。また、図２０には、ゾーンＡに設置された監視カメラ１０１ａが撮影した顔データ１５２～１５６が示してある。

【０２０５】

監視カメラ１０１ａの制御部は、人の顔を検知すると顔画像を切り出し、切り出した顔画像の顔データをサーバ１０２に送信する。例えば、監視カメラ１０１ａの制御部は、時刻 t において人の顔を検知した場合、顔データ１５２をサーバ１０２に送信する。

【０２０６】

監視カメラ１０１ａの制御部は、人の顔を検知した後、２秒後に、検知した人の顔データを２枚切り出し、サーバ１０２に送信する。例えば、監視カメラ１０１ａの制御部は、時刻 t の２秒後である時刻 $t+2$ において、２枚の顔データ１５３，１５４を連続して切

10

20

30

40

50

り出し、サーバ102に送信する。2秒は一例であり、この秒数に限られない。

【0207】

また、監視カメラ101aの制御部は、人の顔を検知した後、4秒後に、検知した人の顔データを2枚切り出し、サーバ102に送信する。例えば、監視カメラ101aの制御部は、時刻 t の4秒後である時刻 $t+4$ において、2枚の顔データ155, 156を連続して切り出し、サーバ102に送信する。4秒は一例であり、この秒数に限られない。

【0208】

サーバ102の制御部は、監視カメラ101aが送信した顔データと、テーブルTB102に記憶された顔データとの照合し、監視カメラ101aが送信した顔データが、テーブルTB102に記憶された顔データと一致するか否かを判定する。このとき、サーバ102の制御部は、監視カメラ101aが送信した顔データと、テーブルTB102に記憶された顔データとの類似度を算出し、算出した類似度が閾値を超えた場合、監視カメラ101aが送信した顔データは、テーブルTB102に記憶された顔データに一致したと判定する。

【0209】

なお、オペレータが端末装置103を用いて閾値を設定してもよい。閾値は、例えば、テーブルTB102に登録する顔データの精度（粗さ）に基づいて設定されてもよい。図20の例では、閾値は、1.04に設定されている。

【0210】

例えば、サーバ102の制御部は、監視カメラ101aが送信した顔データ152と、テーブルTB102に記憶された顔データ151との類似度を算出する。図20の例において、顔データ152と顔データ151との類似度は0.80であり、閾値1.04を超えていない。従って、サーバ102の制御部は、顔データ152と顔データ151とは一致しないと判定する。

【0211】

また、サーバ102の制御部は、監視カメラ101aが送信した顔データ153, 154と、テーブルTB102に記憶された顔データ151との類似度を算出する。図20の例において、顔データ153と顔データ151との類似度は0.90であり、閾値1.04を超えていない。また、顔データ154と顔データ151との類似度は0.95であり、閾値1.04を超えていない。従って、サーバ102の制御部は、顔データ153, 154と顔データ151とは一致しないと判定する。

【0212】

また、サーバ102の制御部は、監視カメラ101aが送信した顔データ155と、テーブルTB102に記憶された顔データ151との類似度を算出する。図20の例において、顔データ155と顔データ151との類似度は1.15であり、閾値1.04を超えている。従って、サーバ102の制御部は、顔データ155と顔データ151とは一致していると判定する。すなわち、サーバ102の制御部は、監視カメラ101aが撮影した人物は、ブラックリストに登録された人物と判定する。

【0213】

なお、サーバ102の制御部は、ブラックリスト判定においては、監視カメラ101aが撮影した顔データ155と、テーブルTB102に記憶された顔データ151との類似度が閾値を超えた時点で、アラーム信号を出力する。

【0214】

図21は、ホワイトリスト方式における判定方法を説明する図である。図21の矢印A121~A123は、人がゾーンBに立ち入る様子を示している。また、図21には、テーブルTB102のゾーンB（ホワイトリスト）に登録された顔データ161が示してある。また、図21には、ゾーンBに設置された監視カメラ101bが撮影した顔データ162~166が示してある。

【0215】

監視カメラ101bの制御部は、監視カメラ101aと同様に、顔画像を切り出し、顔

10

20

30

40

50

データをサーバ１０２に送信する。

【０２１６】

図２０で説明したブラックリスト判定では、サーバ１０２の制御部は、監視カメラ１０１ａから顔データを受信すると、逐次類似度を算出し、算出した類似度が閾値を超えた時点で、監視カメラ１０１ａから受信した顔データの人物はブラックリストに登録された人物であると判定する。

【０２１７】

一方、ホワイトリスト判定では、サーバ１０２の制御部は、一定数の一連の顔データを監視カメラ１０１ｂから受信してから、監視カメラ１０１ｂが撮影した人物がホワイトリストに登録された人物であるか否かを判定する。例えば、サーバ１０２の制御部は、監視カメラ１０１ｂから、５枚の一連の顔データ１６２～１６６（同じ人物における顔データ１６２～１６６）を受信すると、監視カメラ１０１ｂが撮影した５枚の顔データ１６２～１６６の人物がホワイトリストに登録された人物であるか否かを判定する。

【０２１８】

サーバ１０２の制御部は、５枚の顔データ１６２～１６６を受信すると、受信した顔データ１６２～１６６の各々と、テーブルＴＢ１０２に記憶された顔データ１６１との類似度を算出する。サーバ１０２の制御部は、算出した類似度の平均値を算出し、算出した平均値に基づいて、監視カメラ１０１ｂが撮影した人物は、ホワイトリストに登録された人物であるか否かを判定してもよい。

【０２１９】

例えば、サーバ１０２の制御部は、図２１に示す顔データ１６２～１６６の類似度０．５０、０．３０、０．３５、０．２０、０．２５の平均値を算出し、算出した平均値が閾値１．０４以下の場合、監視カメラ１０１ｂが撮影した人物は、ホワイトリストに登録された人物ではないと判定してもよい。なお、平均値の算出に用いる類似度は、５個に限られない。平均値の算出に用いる類似度の数は、可変されてもよく、例えば、端末装置１０３から設定されてもよい。

【０２２０】

また、サーバ１０２の制御部は、算出した類似度の中央値が閾値１．０４以下の場合、監視カメラ１０１ｂが撮影した人物は、ホワイトリストに登録された人物ではないと判定してもよい。

【０２２１】

このように、ホワイトリスト判定では、サーバ１０２の制御部は、一定数の一連の顔データを監視カメラ１０１ｂから受信してから、監視カメラ１０１ｂが撮影した人物がホワイトリストに登録された人物であるか否かを判定する。これにより、サーバ１０２の制御部は、ホワイトリスト判定の誤判定を抑制できる。

【０２２２】

例えば、ホワイトリストに登録された人物が監視カメラ１０１ｂによって撮影された場合でも、１枚目の顔データでは、類似度が低い場合がある。例えば、１枚目の顔データ１６２の顔は、ゾーンＢの入り口Ａ１０２ｂの扉によって一部が隠れ、類似度が低い場合がある。この場合、ホワイトリストに登録された人物であるにも関わらず、アラーム信号が出力される。

【０２２３】

しかし、上記したように、サーバ１０２の制御部は、一定数の一連の顔データを監視カメラ１０１ｂから受信してから、監視カメラ１０１ｂが撮影した人物がホワイトリストに登録された人物であるか否かを判定する。そのため、サーバ１０２の制御部は、１枚目の顔データ１６２の類似度が閾値以下であっても、アラーム信号を出力しない。これにより、サーバ１０２の制御部は、ホワイトリスト判定の誤判定を抑制できる。

【０２２４】

図２２は、ブラックリスト方式における判定処理例を示したシーケンス図である。端末装置１０３の制御部は、オペレータの操作に応じて、サーバ１０２を経由し、登録ＤＢに

10

20

30

40

50

対し、顔データを登録する（ステップ S 6 1，S 6 2）。このとき、端末装置 1 0 3 の制御部は、オペレータの操作に応じて、閾値も送信する。これにより、登録 DB には、例えば、図 1 8 に示したテーブル T B 1 0 2 の顔データ 1 3 1 c が記憶される。また、顔データ 1 3 1 c に付随して閾値が登録される。以下では、閾値を 1. 0 4 とする。

【0 2 2 5】

ゾーン A の監視カメラ 1 0 1 a の撮像部は、人を撮影したとする。監視カメラ 1 0 1 a の制御部は、撮像部が撮影した映像の中から人の顔を切り出し、切り出した顔の顔データと、監視カメラ 1 0 1 a のカメラ識別情報とをサーバ 1 0 2 に送信する（ステップ S 6 3）。

【0 2 2 6】

サーバ 1 0 2 の制御部は、ステップ S 6 3 にて送信された顔データと、登録 DB に記憶されている顔データとを照合する（ステップ S 6 4）。登録 DB に記憶されている顔データの取得方法は、図 1 9 のステップ S 4 8 で説明した方法と同様であり、その説明を省略する。

【0 2 2 7】

サーバ 1 0 2 の制御部は、ステップ S 6 3 にて送信された顔データと、登録 DB に記憶されている顔データとのスコア（類似度）を算出する（ステップ S 6 5）。ここで、ステップ S 6 3 にて送信された顔データのスコアは、0. 8 0 とする。スコア 0. 8 0 は、閾値 1. 0 4 を超えていないので、サーバ 1 0 2 の制御部は、アラーム信号を出力しない。

【0 2 2 8】

ステップ S 6 3 の顔データの送信後、2 秒経過すると、監視カメラ 1 0 1 a の制御部は、2 枚の顔データを送信する（ステップ S 6 6，S 6 9）。

【0 2 2 9】

ステップ S 6 6 にて送信された顔データの照合およびスコア算出（ステップ S 6 7，S 6 8）は、ステップ S 6 4，S 6 5 と同様であり、その説明を省略する。また、ステップ S 6 9 にて送信された顔データの照合およびスコア算出（ステップ S 7 0，S 7 1）は、ステップ S 6 4，S 6 5 と同様であり、その説明を省略する。

【0 2 3 0】

ステップ S 6 3 の顔データの送信後、4 秒経過すると、監視カメラ 1 0 1 a の制御部は、2 枚の顔データを送信する（ステップ S 7 2，S 7 6）。

【0 2 3 1】

サーバ 1 0 2 の制御部は、ステップ S 7 2 にて送信された顔データと、登録 DB に記憶されている顔データとを照合する（ステップ S 7 3）。

【0 2 3 2】

サーバ 1 0 2 の制御部は、ステップ S 7 2 にて送信された顔データと、登録 DB に記憶されている顔データとのスコア（類似度）を算出する（ステップ S 7 4）。ここで、ステップ S 7 2 にて送信された顔データのスコアは、1. 1 5 とする。スコア 1. 1 5 は、閾値 1. 0 4 を超えているので、サーバ 1 0 2 の制御部は、登録顔の検知を判定し、登録顔検知のアラーム信号を端末装置 1 0 3 に出力する（ステップ S 7 5）。

【0 2 3 3】

ステップ S 7 6 にて送信された顔データの照合およびスコア算出（ステップ S 7 7，S 7 8）は、ステップ S 6 4，S 6 5 と同様であり、その説明を省略する。

【0 2 3 4】

図 2 3 は、ホワイトリスト方式における判定処理例を示したシーケンス図である。図 2 3 のステップ S 8 1，S 8 2 の顔登録処理は、図 2 2 のステップ S 6 1，S 6 2 と同様であり、その説明を省略する。また、図 2 3 のステップ S 8 3，S 8 6，S 8 9，S 9 2，S 9 5 の顔データの送信処理は、図 2 2 のステップ S 6 3，S 6 6，S 6 9，S 7 2，S 7 6 と同様であり、その説明を省略する。ただし、図 2 3 では、ゾーン B に設置された監視カメラ 1 0 1 b が、顔データをサーバ 1 0 2 に送信する。

【0 2 3 5】

10

20

30

40

50

図 2 3 のステップ S 8 4 , S 8 7 , S 9 0 , S 9 3 , S 9 6 の顔照合処理は、図 2 2 のステップ S 6 4 と同様であり、その説明を省略する。また、図 2 3 のステップ S 8 5 , S 8 8 , S 9 1 , S 9 4 , S 9 7 のスコア算出処理は、図 2 2 のステップ S 6 5 と同様であり、その説明を省略する。

【 0 2 3 6 】

ホワイトリスト方式では、サーバ 1 0 2 の制御部は、監視カメラ 1 0 1 b から 5 枚の顔データを受信してから、監視カメラ 1 0 1 b が撮影した顔データの人物がホワイトリストに登録されているか否かの判定をする。

【 0 2 3 7 】

ここで、ステップ S 8 3 , S 8 6 , S 8 9 , S 9 2 , S 9 5 にて送信された顔データのスコアを、0 . 5 0 , 0 . 3 0 , 0 . 3 5 , 0 . 2 0 , 0 . 2 5 とする。サーバ 1 0 2 の制御部は、例えば、5 つのスコアの中央値を用いて、監視カメラ 1 0 1 b が送信した顔データの人物がホワイトリストに登録されているか否かの判定をする。図 2 3 の例では、中央値は、0 . 3 5 であり、閾値 1 . 0 4 を超えていないので、サーバ 1 0 2 の制御部は、監視カメラ 1 0 1 b が撮影した顔データの人物はホワイトリストに登録されていないと判定する。

【 0 2 3 8 】

サーバ 1 0 2 の制御部は、監視カメラ 1 0 1 b が撮影した顔データの人物がホワイトリストに登録されていないと判定すると、未登録検知のアラーム信号を端末装置 1 0 3 に送信する（ステップ S 9 8 ）。

【 0 2 3 9 】

なお、図 2 2 および図 2 3 のシーケンスにおいて、監視カメラ 1 0 1 a , 1 1 0 b は、最初の顔データの送信後、2 秒後に 2 枚の顔データをサーバ 1 0 2 に送信し、4 秒後に 2 枚の顔データをサーバ 1 0 2 に送信したがこれに限られない。顔データを送信する秒数および枚数は、可変されてもよく、例えば、端末装置 1 0 3 から設定されてもよい。

【 0 2 4 0 】

また、顔データを送信する秒数の数は、3 以上であってもよい。例えば、監視カメラ 1 0 1 a , 1 0 1 b は、最初の顔データの送信後、2 秒後、4 秒後、6 秒後と、3 回顔データをサーバ 1 0 2 に送信してもよい。顔データを送信する秒数の数は、可変されてもよく、例えば、端末装置 1 0 3 から設定されてもよい。

【 0 2 4 1 】

図 2 4 は、ブラックリスト方式によってアラーム信号が出力されたときの端末装置 1 0 3 の画面例を示した図である。ブラックリスト方式によってアラーム信号が出力されたとき、端末装置 1 0 3 の表示装置には、図 2 4 に示す画像が表示される。画像には、監視カメラ 1 0 1 a が撮影した閾値を超えた顔画像と、テーブル T B 1 0 2 に登録されている顔画像とが表示される。

【 0 2 4 2 】

なお、図 2 4 に示すライブボタンがクリックされた場合、端末装置 1 0 3 の表示装置には、監視カメラ 1 0 1 a が撮影している現在の映像が表示される。再生ボタンがクリックされた場合、端末装置 1 0 3 の表示装置には、監視カメラ 1 0 1 a が撮影した人物がブラックリストに登録されていると判定されたときの前後の映像が再生される。

【 0 2 4 3 】

図 2 5 は、ホワイトリスト方式によってアラーム信号が出力されたときの端末装置 1 0 3 の画面例を示した図である。ホワイトリスト方式によってアラーム信号が出力されたとき、端末装置 1 0 3 の表示装置には、図 2 5 に示す画像が表示される。画像には、監視カメラ 1 0 1 b が撮影した閾値を超えなかった顔画像が表示される。

【 0 2 4 4 】

ホワイトリスト方式によってアラーム信号が出力された人物の顔データは、テーブル T B 1 0 2 に登録されていない。従って、端末装置 1 0 3 の表示装置には、未登録顔の人物が検出されたことを示す画像 1 7 1 が表示される。

10

20

30

40

50

【0245】

なお、図25に示すライブボタンがクリックされた場合、端末装置103の表示装置には、監視カメラ101bが撮影している現在の様子が表示される。再生ボタンがクリックされた場合、端末装置103の表示装置には、監視カメラ101bが撮影した人物がホワイトリストに登録されていないと判定されたときの前後の映像が再生される。

【0246】

端末装置103の表示装置には、ブラックリスト方式およびホワイトリスト方式に関わらず、アラーム信号が出力されたときの顔画像が表示されてもよい。

【0247】

図26は、アラーム信号が出力されたときの端末装置103の画面例を示した図である。図26に示す端末装置103の表示装置には、ブラックリスト方式によってアラーム信号が出力されたときの画像と、ホワイトリスト方式によってアラーム信号が出力されたときの画像とが表示されている。すなわち、端末装置103の表示装置には、売り場エリア（ゾーンA）にブラックリストに登録された人物が出現したときの画像と、従業員エリア（ゾーンB）にホワイトリストに登録されていない人物が出現したときの画像とが混在して表示される。

【0248】

以上説明したように、サーバ102は、ゾーンAに設置された監視カメラ101aから第1顔データを受信し、ゾーンBに設置された監視カメラ101bから第2顔データを受信する通信部を有する。また、サーバ102は、第1顔データと、ブラックリストに登録された登録顔データとを照合して、ブラックリストに登録された登録顔データの人物のゾーンAへの立ち入りを判定し、第2顔データと、ホワイトリストに登録された登録顔データとを照合して、ホワイトリストに登録されていない登録顔データの人物のゾーンBへの立ち入りを判定する制御部を有する。

【0249】

これにより、サーバ102は、ゾーンごとにおいて、人の立ち入りを監視する条件が変わる場合でも、ゾーンへの人の立ち入りを適切に監視できる。例えば、サーバ102は、売り場であるゾーンAにおいては、注意人物の立ち入りを、ブラックリストを用いて判定し、バックヤードであるゾーンBにおいては、従業員以外の人物の立ち入りを、ホワイトリストを用いて判定し、ゾーンA、Bへの人の立ち入りを適切に監視できる。

【0250】

（変形例）

監視カメラシステムは、例えば、会社またはマンションに用いられてもよい。例えば、監視カメラシステムは、会社の入り口のゾーンを、ブラックリストを用いて判定し、建物内の各部署のゾーンを、ホワイトリストを用いて判定してもよい。また、例えば、監視カメラシステムは、マンションの入り口の共用ゾーンを、ブラックリストを用いて判定し、建物内の各階のゾーンを、ホワイトリストを用いて判定してもよい。

【0251】

（第5の実施の形態）

第5の実施の形態では、第4の実施の形態で説明したゾーンBに、ホワイトリストに登録されていない人物が立ち上がった場合、端末装置103からの指示に応じて、ゾーンBに立ち上がったその人物の顔データを、ホワイトリストに登録する。また、第5の実施の形態では、第4の実施の形態で説明したゾーンBに、ホワイトリストに登録されていない人物が立ち上がった場合、端末装置103からの指示に応じて、ゾーンBに立ち上がったその人物の顔データを、ゾーンAのブラックリストに登録する。

【0252】

図27は、第5の実施の形態に係る監視カメラシステムの一例を示した図である。図27において、図15と同じものには同じ符号が付してある。図27には、人の顔データ201が示してある。

【0253】

顔データ 201 は、例えば、店舗の従業員である。従業員は、商品売り場であるゾーン A に立ち入ることができるため、ブラックリストには登録されていない。従業員は、バックヤードであるゾーン B に立ち入ることができるが、ホワイトリストに登録されていないとする。

【0254】

顔データ 201 の従業員は、ブラックリストに登録されていない。従って、顔データ 201 の従業員がゾーン A に立ち入っても、サーバ 102 の制御部は、アラーム信号を端末装置 103 および警報装置 104 a, 104 b, 105 a, 105 b に出力しない。

【0255】

顔データ 201 の従業員は、ホワイトリストに登録されていない。従って、顔データ 201 の従業員がゾーン B に立ち入ると、サーバ 102 の制御部は、アラーム信号を端末装置 103 および警報装置 104 a, 104 b, 105 a, 105 b に出力する。また、サーバ 102 の制御部は、監視カメラ 101 b が撮影した顔データ 201 を端末装置 103 に出力する。

【0256】

端末装置 103 は、アラーム信号と、監視カメラ 101 b が撮影した顔データ 201 とを受信すると、受信した顔データ 201 の画像を表示装置に表示する。端末装置 103 を操作するオペレータは、端末装置 103 の表示装置に表示された顔データ 201 の人物が、例えば、ゾーン B に立ち入ることのできる従業員であるという確認が取れると、端末装置 103 を操作して、従業員の顔データ 201 をホワイトリストに登録するよう、サーバ 102 に指示する。

【0257】

サーバ 102 の制御部は、端末装置 103 からの登録指示に応じて、端末装置 103 の表示装置に表示された顔データ 201 をホワイトリストに登録する。すなわち、サーバ 102 の制御部は、アラーム信号の送信契機となった従業員の顔データ 201 をホワイトリストに登録する。これにより、サーバ 102 の制御部は、顔データ 201 の従業員が、次にゾーン B に立ち入っても、端末装置 103 および警報装置 104 a, 104 b, 105 a, 105 b にアラーム信号を出力しない。

【0258】

監視カメラシステムの上記処理によって、端末装置 103 のオペレータは、ゾーン B に立ち入ることができる従業員の顔データを、例えば、従業員から受領しなくても、監視カメラ 101 b が撮影した顔データ 201 を用いて容易にホワイトリストに登録できる。また、従業員は、従業員の顔を撮影し、撮影した顔データを端末装置 103 に送信しなくてもよい。

【0259】

なお、顔データ 201 は、最初、ホワイトリストに登録されていない。従って、顔データ 201 が、端末装置 103 によってホワイトリストに登録されるまでは、サーバ 102 から端末装置 103 および警報装置 104 a, 104 b, 105 a, 105 b にアラーム信号が送信される。

【0260】

図 28 は、第 5 の実施の形態に係る監視カメラシステムの一例を示した図である。図 28 において、図 15 と同じものには同じ符号が付してある。図 28 には、人の顔データ 202 が示してある。

【0261】

顔データ 202 は、例えば、店舗に来店した人物の顔データである。来店者は、サーバ 102 のブラックリストおよびホワイトリストに登録されていないとする。

【0262】

顔データ 202 の来店者は、ブラックリストに登録されていない。従って、顔データ 202 の来店者がゾーン A に立ち入っても、サーバ 102 の制御部は、アラーム信号を端末装置 103 および警報装置 104 a, 104 b, 105 a, 105 b に出力しない。

10

20

30

40

50

【0263】

顔データ202の来店者は、ホワイトリストに登録されていない。従って、顔データ202の従業員がゾーンBに立ち入ると、サーバ102の制御部は、アラーム信号を端末装置103および警報装置104a, 104b, 105a, 105bに出力する。また、サーバ102の制御部は、監視カメラ101bが撮影した顔データ202を端末装置103に出力する。

【0264】

端末装置103は、アラーム信号と、監視カメラ101bが撮影した顔データ202とを受信すると、受信した顔データ202の画像を表示装置に表示する。端末装置103を操作するオペレータは、端末装置103の表示装置に表示された顔データ202の人物が、例えば、ゾーンBに立ち入ることのできる従業員でないという確認が取れると、端末装置103を操作して、来店者の顔データ202をブラックリストに登録するよう、サーバ102に指示する。

10

【0265】

サーバ102の制御部は、端末装置103からの登録指示に応じて、端末装置103の表示装置に表示された顔データ202をブラックリストに登録する。すなわち、サーバ102の制御部は、アラーム信号の送信契機となった来店者の顔データ202をブラックリストに登録する。これにより、関係者以外が立ち入れないゾーンBに立ち入った来店者が、例えば、再来店してゾーンAに立ち入ると、サーバ102の制御部は、端末装置103および警報装置104a, 104b, 105a, 105bにアラーム信号を出力する。店舗の従業員は、関係者以外が立ち入れないゾーンBに立ち入った来店者を監視することができる。

20

【0266】

監視カメラシステムの上記処理によって、端末装置103のオペレータは、ゾーンAの立ち入りを監視したい人物の顔データを、例えば、従業員等から受領しなくても、監視カメラ101bが撮影した顔データ202を用いて容易にブラックリストに登録できる。また、従業員は、ゾーンAへの立ち入りを監視したい人物の顔を撮影し、撮影した顔データを端末装置103に送信しなくてもよい。

【0267】

図29は、監視カメラシステムの動作例を示したシーケンス図である。図29は、図27で説明したホワイトリスト登録に対応するシーケンス図である。図29に示すステップS101～S106の処理は、図19で説明したステップS41～S46と同様であり、その説明を省略する。

30

【0268】

ゾーンBの監視カメラ101bの撮像部は、従業員を撮影したとする。従業員は、例えば、初めて建物A101の店舗に来訪した従業員であり、ホワイトリストに登録されていないとする。監視カメラ101bの制御部は、撮像部が撮影した映像の中から人の顔を切り出し、切り出した顔の顔データと、監視カメラ101bのカメラ識別情報とをサーバ102に送信する（ステップS107）。

【0269】

サーバ102の制御部は、ステップS107にて送信された顔データ206と、登録DBに記憶されている顔データとを照合する（ステップS108）。顔データの照合方法は、図19のステップS53で説明した方法と同様であり、その説明を省略する。なお、顔データ206の従業員は、ホワイトリストに登録されていないので、サーバ102の制御部は、顔データ206はホワイトリストに登録されていない（未登録顔検知）と判定する。

40

【0270】

サーバ102の制御部は、ステップS108の照合結果（未登録顔検知のアラーム信号）を端末装置103および警報装置104a, 105a, 105bに送信する（ステップS109）。なお、サーバ102の制御部は、未登録顔検知を判定した場合、監視カメラ101bが撮影した顔データ206を端末装置103に送信する。端末装置103の制御

50

部は、サーバ１０２から送信された顔データ２０６を表示装置に表示する。

【０２７１】

端末装置１０３の制御部は、オペレータから、顔データ２０６をホワイトリストに登録する操作を受けると、顔登録指示をサーバ１０２に送信する（ステップＳ１１０）。

【０２７２】

サーバ１０２の制御部は、ステップＳ１１０にて送信された顔登録指示の受信に応じて、ステップＳ１０９のアラーム信号の送信契機となった顔データ２０６を登録ＤＢのテーブルＴＢ１０２に登録する（ステップＳ１１１）。

【０２７３】

ゾーンＢの監視カメラ１０１ｂの撮像部は、従業員を撮影したとする。従業員は、ステップＳ１１１の顔登録処理によって、ホワイトリストに登録された従業員である。監視カメラ１０１ｂの制御部は、撮像部が撮影した映像の中から人の顔を切り出し、切り出した顔の顔データと、監視カメラ１０１ｂのカメラ識別情報とをサーバ１０２に送信する（ステップＳ１１２）。

【０２７４】

サーバ１０２の制御部は、ステップＳ１１２にて送信された顔データ２０７と、登録ＤＢに記憶されている顔データとを照合する（ステップＳ１１３）。顔データ２０７は、ステップＳ１１１にて登録ＤＢのテーブルＴＢ１０２に登録された顔データ２０６と一致する。従って、サーバ１０２の制御部は、顔データ２０７の従業員は、ホワイトリストに登録された人物と判定する。

【０２７５】

図３０は、監視カメラシステムの動作例を示したシーケンス図である。図３０は、図２８で説明したブラックリスト登録に対応するシーケンス図である。図３０に示すステップＳ１２１～Ｓ１２６の処理は、図１９で説明したステップＳ４１～Ｓ４６と同様であり、その説明を省略する。

【０２７６】

ゾーンＢの監視カメラ１０１ｂの撮像部は、来店者を撮影したとする。来店者は、ブラックリストおよびホワイトリストに登録されていないとする。監視カメラ１０１ｂの制御部は、撮像部が撮影した映像の中から人の顔を切り出し、切り出した顔の顔データと、監視カメラ１０１ｂのカメラ識別情報とをサーバ１０２に送信する（ステップＳ１２７）。

【０２７７】

サーバ１０２の制御部は、ステップＳ１２７にて送信された顔データ２０８と、登録ＤＢに記憶されている顔データとを照合する（ステップＳ１２８）。顔データの照合方法は、図１９のステップＳ５３で説明した方法と同様であり、その説明を省略する。なお、顔データ２０８の来店者は、ホワイトリストに登録されていないので、サーバ１０２の制御部は、顔データ２０８はホワイトリストに登録されていない（未登録顔検知）と判定する。

【０２７８】

サーバ１０２の制御部は、ステップＳ１２８の照合結果（未登録顔検知のアラーム信号）を端末装置１０３および警報装置１０４ａ，１０５ａ，１０５ｂに送信する（ステップＳ１２９）。なお、サーバ１０２の制御部は、未登録顔検知を判定した場合、監視カメラ１０１ｂが撮影した顔データ２０８を端末装置１０３に送信する。端末装置１０３の制御部は、サーバ１０２から送信された顔データ２０８を表示装置に表示する。

【０２７９】

端末装置１０３の制御部は、オペレータから、顔データ２０８をブラックリストに登録する操作を受けると、顔登録指示をサーバ１０２に送信する（ステップＳ１３０）。

【０２８０】

サーバ１０２の制御部は、ステップＳ１３０にて送信された顔登録指示の受信に応じて、ステップＳ１２９のアラーム信号の送信契機となった顔データ２０８を登録ＤＢのテーブルＴＢ１０２に登録する（ステップＳ１３１）。

【０２８１】

10

20

30

40

50

ゾーンAの監視カメラ101aの撮像部は、来店者を撮影したとする。来店者は、ステップS131の顔登録処理によって、ブラックリストに登録された来店者である。監視カメラ101aの制御部は、撮像部が撮影した映像の中から人の顔を切り出し、切り出した顔の顔データと、監視カメラ101aのカメラ識別情報とをサーバ102に送信する（ステップS132）。

【0282】

サーバ102の制御部は、ステップS132にて送信された顔データ209と、登録DBに記憶されている顔データとを照合する（ステップS133）。顔データ209は、ステップS131にて登録DBのテーブルTB102に登録された顔データ208と一致する。従って、サーバ102の制御部は、顔データ209の来店者は、ブラックリストに登録された人物と判定する。サーバ102の制御部は、ステップS133の照合結果（不審者通知のアラーム信号）を端末装置103および警報装置104a, 105a, 105bに送信する（ステップS134）。

10

【0283】

以上説明したように、サーバ102は、監視カメラ101aから受信した第1顔データと、ホワイトリストに登録された第1登録顔データとを照合して、第1登録顔データの人物以外の人物のゾーンBへの立ち入りを判定する制御部と、第1登録顔データの人物以外の人物のゾーンBへの立ち入りが判定された場合、アラーム信号を端末装置103に送信する通信部と、を備える。サーバ102の制御部は、アラーム信号を受信した端末装置103からの指示に応じて、アラーム信号の送信契機となった人物の第1顔データを、ホワイトリストに登録する。これにより、オペレータは、登録顔データのホワイトリストへの登録を容易にできる。

20

【0284】

また、サーバ102の制御部は、アラーム信号を受信した端末装置からの指示に応じて、アラーム信号の送信契機となった人物の第1顔データを、ブラックリストに登録する。これにより、オペレータは、登録顔データのブラックリストへの登録を容易にできる。

【0285】

（第6の実施の形態）

第1の実施の形態では、サーバ2の制御部21は、テーブルTB2を参照し、顔データが撮影された人物のゾーンを特定する。そして、サーバ2の制御部21は、テーブルTB1を参照して、特定したゾーンに対応する顔データを取得し、取得した顔データと、監視カメラ1a～1cが撮影した顔データとを照合する。

30

【0286】

これに対し、第6の実施の形態では、サーバ2の制御部21は、監視カメラ1a～1cが撮影した顔データに基づいてテーブルTB1を参照し、顔データの人物の立ち入りが許可された許可ゾーンを取得する。そして、サーバ2の制御部21は、カメラ識別情報に基づいてテーブルTB2を参照し、顔データの人物が撮影された撮影ゾーンを取得し、許可ゾーンと撮影ゾーンとに基づいて顔データの人物の立ち入りの許可／不許可を判定する。

【0287】

第6の実施の形態における監視カメラシステムの構成および各装置のブロック構成は、第1の実施の形態における監視カメラシステムの構成および各装置のブロック構成と同様であり、その説明を省略する。

40

【0288】

図31は、第6の実施の形態に係る監視カメラシステムの動作例を示したシーケンス図である。図31のシーケンス図において、図8のシーケンス図の処理と同じ処理には、同じ符号が付してある。以下では、図8のシーケンス図の処理と異なる処理について説明する。

【0289】

サーバ2の制御部21は、テーブルTB1に記憶されている顔データと、ステップS4にて受信した顔データ51とを照合する（ステップS141）。

50

【0290】

サーバ2の制御部21は、ステップS141の照合により、ステップS4にて受信した顔データ51の人物の入室が許可された許可ゾーンを取得する（ステップS142）。

【0291】

図31の例では、ステップS4にて受信した顔データ51は、図6に示したテーブルTB1の顔データ41baに一致する。顔データ41baに一致する顔データ51の人物は、図6に示したテーブルTB1より、ゾーンA，Bに入室できる。従って、ステップS4にて受信した顔データ51の人物の許可ゾーンは、ゾーンA，Bである。

【0292】

サーバ2の制御部21は、ステップS4にて受信したカメラ識別情報に基づいて、テーブルTB2を参照し、ステップS4にて受信した顔データ51の撮影された撮影ゾーンを取得する（ステップS143）。

【0293】

図31の例では、サーバ2の制御部21は、ステップS4にてカメラ識別情報「1a」を受信している。従って、サーバ2の制御部21は、ゾーンAを撮影ゾーンとして取得する。

【0294】

サーバ2の制御部21は、ステップS142にて取得した許可ゾーンと、ステップS143にて取得した撮影ゾーンとに基づいて、ステップS4にて受信した顔データ51の人物のゾーンA，Bへの立ち入りの許可を判定する。図8の例の場合、顔データ51の人物の許可ゾーンは、ゾーンA，Bである。また、顔データ51の人物の撮影ゾーンは、ゾーンAである。従って、顔データ51の人物は、ゾーンA，Bへの立ち入りが許可された人物であって、ゾーンAに居るので、サーバ2の制御部21は、顔データ51の人物は、ゾーンAへの立ち入りが許可された人物と判定する。すなわち、サーバ2の制御部21は、許可ゾーンに一致する撮影ゾーンが存在する場合、監視カメラによって撮影された人物は、撮影ゾーンへの立ち入りが許可された人物と判定する。

【0295】

サーバ2の制御部21は、ゾーンA，Bへの立ち入り許可判定結果を端末装置3に送信する（ステップS144）。図31の例では、サーバ2の制御部21は、顔データ51の人物を、ゾーンAへの立ち入りが許可された人物と判定するので、立ち入りOKを示す情報を端末装置3に送信する。

【0296】

サーバ2の制御部21は、テーブルTB1に記憶されている顔データと、ステップS8にて受信した顔データ52とを照合する（ステップS145）。

【0297】

サーバ2の制御部21は、ステップS145の照合により、ステップS9にて受信した顔データ52の人物の入室が許可された許可ゾーンを取得する（ステップS146）。

【0298】

図31の例では、ステップS9にて受信した顔データ52は、図6に示したテーブルTB1の顔データ41ba，41bb，41bcに一致しない。顔データ41ba，41bb，41bcに一致しない顔データ52の人物は、ゾーンA，Bに入室できない。従って、ステップS9にて受信した顔データ52の人物の許可ゾーンは無く、サーバ2の制御部21は、顔データ52の人物は、ゾーンA，Bへの立ち入りが許可されていない人物と判定する。

【0299】

サーバ2の制御部21は、ゾーンA，Bへの立ち入り許可判定結果を端末装置3に送信する（ステップS147）。図31の例では、サーバ2の制御部21は、顔データ52の人物を、ゾーンA，Bへの立ち入りが許可されていない人物と判定するので、立ち入りNGを示す情報を端末装置3に送信する。

【0300】

以上説明したように、サーバ２は、建物Ａ１の複数のゾーンＡ～Ｃの各々を撮影する監視カメラ１ａ～１ｃから、顔データを受信する通信部２２を備える。サーバ２は、複数の監視カメラ１ａ～１ｃ各々のカメラ識別情報と、複数のゾーンＡ～Ｃとを紐付けたテーブルＴＢ２と、登録顔データと、登録顔データの人物の立ち入りが許可されたゾーンＡ～Ｃとを紐付けたテーブルＴＢ１と、を備える。サーバ２は、顔データに基づいてテーブルＴＢ１を参照して、顔データの人物の立ち入りが許可された許可ゾーンを取得してから、カメラ識別情報に基づいてテーブルＴＢ２を参照して顔データの人物が撮影された撮影ゾーンを取得し、許可ゾーンと撮影ゾーンとに基づいて顔データの人物の立ち入りの許可／不許可を判定する制御部２１を備える。これにより、サーバ２は、ゾーンＡ～Ｃごとに決められた人以外の人、ゾーンＡ～Ｃに立ち入っていないかを判定できる。

10

【０３０１】

(第７の実施の形態)

第７の実施の形態では、２つのテーブルにアクセスする端末装置が異なる。

【０３０２】

図３２は、第７の実施の形態に係る監視カメラシステムの一例を示した図である。図３２に示すように、監視カメラシステムは、監視カメラ３０１ａ、３０１ｂと、サーバ３０２と、端末装置３０３、３０４と、を有している。

【０３０３】

図３２には、監視カメラシステムの他に建物Ａ３０１の内部の平面図が示してある。建物Ａ３０１は、例えば、コンサート会場である。以下では、建物Ａ３０１をコンサート会場として説明する。

20

【０３０４】

建物Ａ３０１は、ゾーンＡ、Ｂを有している。ゾーンＡには、Ａ席が設定される。ゾーンＢには、Ｂ席が設定される。Ｂ席は、Ａ席よりステージから遠い。Ａ席とＢ席は、例えば、コンサート料金が異なる。

【０３０５】

監視カメラ３０１ａは、建物Ａ３０１のゾーンＡに設置される。監視カメラ３０１ｂは、建物Ａ３０１のゾーンＢに設置される。

【０３０６】

監視カメラ３０１ａ、３０１ｂは、ゾーンＡ、Ｂ内に居る人を撮影するよう建物Ａ３０１に設置される。例えば、監視カメラ３０１ａは、ゾーンＡ内の全体を撮影するように、ゾーンＡの天井または壁等に設置される。監視カメラ３０１ｂは、ゾーンＢ内の全体を撮影するように、ゾーンＢの天井または壁等に設置される。

30

【０３０７】

サーバ３０２は、例えば、ＬＡＮまたはインターネット等のネットワークによって、監視カメラ３０１ａ、３０１ｂと接続されている。サーバ３０２は、建物Ａ３０１内に設置されてもよいし、建物Ａ３０１とは別の場所に設置されてもよい。

【０３０８】

サーバ３０２は、ゾーンＡ、Ｂに立ち入ることができる人の顔データを記憶（登録）している。言い換えれば、サーバ３０２は、ゾーンＡ、Ｂに立ち入ることができる人のホワイトリストを有している。サーバ３０２は、監視カメラ３０１ａ、３０１ｂが撮影した人の顔データと、登録されている顔データとの照合を行う。サーバ３０２は、照合結果を、端末装置３０３に送信する。

40

【０３０９】

端末装置３０３は、ＬＡＮまたはインターネット等のネットワークによって、サーバ３０２と接続されている。端末装置３０３は、建物Ａ３０１内に設置されてもよいし、建物Ａ３０１とは別の場所に設置されてもよい。端末装置３０３は、例えば、パーソナルコンピュータ、スマートフォン、またはタブレット端末等であってもよい。端末装置３０３は、例えば、コンサートを運営する会社のオペレータによって使用される。

【０３１０】

50

端末装置 303 は、例えば、コンサートを運営する会社のオペレータによって使用される。オペレータは、端末装置 303 を用いて、監視カメラ 301a, 301b の設定に関する情報を入力する。例えば、オペレータは、端末装置 303 を用いて、ゾーン A, B と監視カメラ 301a, 301b のグルーピング設定を行う。また、オペレータは、例えば、端末装置 303 を用いて、ゾーン A, B に不適切な人が居ないかを監視する。例えば、オペレータは、端末装置 303 を用いて、ゾーン A に立ち入ることができない人がゾーン A に居ないかを監視する。また、オペレータは、端末装置 303 を用いて、ゾーン B に立ち入ることができない人がゾーン B に居ないかを監視する。

【0311】

端末装置 304 は、LAN またはインターネット等のネットワークによって、サーバ 302 と接続されている。端末装置 304 は、例えば、パーソナルコンピュータ、スマートフォン、またはタブレット端末等であってもよい。

10

【0312】

端末装置 304 は、例えば、コンサートを視聴するユーザによって使用される。ユーザは、例えば、コンサートを視聴するため、端末装置 304 を用いて、コンサートのチケットを予約または購入する。

【0313】

なお、ゾーン A, B の各々には、複数の監視カメラが設置されてもよい。ゾーン A, B の各々は、複数の監視カメラによって、ゾーン A, B 内にいる人を撮影するように設置されてもよい。

20

【0314】

また、監視カメラ 301a, 301b には、ゾーン A, B に既に設置されている監視カメラが用いられてもよい。例えば、監視カメラ 301a, 301b には、ゾーン A, B の映像を録画する録画システムの一部として、既にゾーン A, B に設置されている監視カメラを用いてもよい。この場合、監視カメラ 301a, 301b の出力を、録画システムとサーバ 302 とに分岐させてもよい。

【0315】

また、ゾーンの数、2 つに限られない。ゾーンは、3 以上であってもよい。3 以上のゾーン各々に設置される監視カメラは、サーバ 302 に接続される。サーバ 302 は、3 以上のゾーン各々において、ブラックリストおよびホワイトリストのいずれか一方を用いて、ゾーンへの人の立ち入りを判定する。

30

【0316】

また、監視カメラシステムは、監視カメラ 301a, 301b が撮影した映像データを録画するレコーダを備えてもよい。監視カメラシステムは、監視カメラ 301a, 301b が撮影した映像データをリアルタイムで表示するモニタリング装置を備えてもよい。モニタリング装置は、例えば、パーソナルコンピュータ、スマートフォン、またはタブレット端末等であってもよい。

【0317】

また、監視カメラ 301a, 301b は、図 3 で説明した監視カメラ 1a と同様の構成を有し、その説明を省略する。サーバ 302 は、図 4 で説明したサーバ 2 と同様の構成を有し、その説明を省略する。ただし、サーバ 302 の通信部は、端末装置 303, 304 と通信する。端末装置 303, 304 は、図 5 で説明した端末装置 3 と同様の構成を有し、その説明を省略する。

40

【0318】

図 33 は、テーブル TB 301 のアクセス例を説明する図である。図 33 に示すテーブル TB 301 は、図 7 で説明したテーブル TB 2 と同様である。ただし、図 7 のテーブル TB 2 は、3 つのカメラ識別情報を有しているが、図 33 のテーブル TB 301 は、2 つのカメラ識別情報を有している点が異なる。また、図 33 に示すカメラ識別情報「a」は、監視カメラ 301a のカメラ識別情報であり、カメラ識別情報「b」は、監視カメラ 301b のカメラ識別情報である。

50

【0319】

端末装置303は、テーブルTB301にアクセスできる。端末装置304は、テーブルTB301にアクセスできない。テーブルTB301は、端末装置303によって作成され、サーバ302の記憶部23に記憶される。また、テーブルTB2の情報は、例えば、端末装置303によって追加、変更、または削除されてもよい。

【0320】

図34は、テーブルTB302のアクセス例を説明する図である。図34に示すテーブルTB302は、図9で説明したテーブルTB11と同様である。ただし、図34のテーブルTB301に登録されている時刻は、図9のテーブルTB11に登録されている時刻と異なっている。

10

【0321】

端末装置304は、テーブルTB302にアクセスできる。例えば、コンサートを視聴しようとするユーザは、端末装置304を用いて、ユーザの顔データ、席、および視聴しようとするコンサートの日時をテーブルTB302に登録できる。また、ユーザは、端末装置303を用いて、テーブルTB302の情報を追加、変更、または削除してもよい。

【0322】

端末装置303は、テーブルTB302にアクセスできてもよい。例えば、権限を持ったオペレータは、端末装置303を用いて、テーブルTB302の情報を閲覧、追加、変更、または削除してもよい。

【0323】

テーブルTB301、TB302は、サーバ302の記憶部に記憶されてもよい。また、テーブルTB301およびテーブルTB302の両方または一方は、サーバ302とは別体のデータベースに記憶されてもよい。別体のデータベースは、サーバ302の一部と捉えてもよい。以下では、テーブルTB301、TB302は、登録DBに記憶されとする。

20

【0324】

図35は、監視カメラシステムの動作例を示したシーケンス図である。端末装置303の制御部は、オペレータの操作に応じて、サーバ302を介して登録DBに対し、ゾーンA、Bと、監視カメラ301a、301bとのグルーピング設定を行う（ステップS151、S152）。すなわち、端末装置303の制御部は、登録DBに対し、ゾーンA、Bと、監視カメラ301a、301bとの対応付けの設定を行う。これにより、登録DBには、例えば、図33に示したテーブルTB301が記憶される。

30

【0325】

コンサートを予約する人は、例えば、端末装置304に顔データ、名前、予約するゾーンの情報（コンサート会場の席の情報）、およびコンサート会場に入る時間等の予約情報を入力する。端末装置304は、入力された予約情報をサーバ302に送信する（ステップS153）。

【0326】

サーバ302の制御部は、端末装置304から送信された予約情報に基づいて、登録DBに対し、顔登録を行う（ステップS154）。すなわち、サーバ302の制御部は、登録DBにおいて、図34に示したテーブルTB302を生成する。

40

【0327】

例えば、図35の顔データ311の人物は、端末装置304を用いて、2019年xx月yy日の13:00から15:00に演奏されるコンサートを予約する。また、顔データ311の人物は、端末装置304を用いて、A席を予約する。この場合、テーブルTB302には、例えば、図34の点線枠A401に示す情報が記憶される。

【0328】

サーバ302の制御部は、ステップS154の顔登録が完了すると、テーブルTB302に登録した予約情報を端末装置303に送信する（ステップS155）。端末装置303の管理者は、端末装置303が受信した予約情報によって、コンサート会場を予約した人の

50

予約内容を把握できる。

端末装置 303 は、オペレータの操作に応じて、予約情報要求をサーバ 302 に送信する（ステップ S156）。オペレータは、要求する予約情報として、例えば、日時または席（ゾーン）の情報を指定できる。

【0329】

サーバ 302 の制御部は、端末装置 303 から予約情報を受信すると、登録 DB のテーブル TB302 にアクセスし、予約情報を取得する（ステップ S157）。

【0330】

サーバ 302 の制御部は、テーブル TB302 から取得した予約情報を端末装置 303 に送信する（ステップ S158）。

【0331】

以上説明したように、サーバ 302 は、建物 A301 の複数のゾーン A、B の各々を撮影する監視カメラ 301a、301b から、顔データを受信する通信部と、顔データと、ゾーン A、B ごとの立ち入りが許可された人物の登録顔データとを照合し、顔データが撮影されたゾーンにおける、顔データの人物の立ち入りの可否を判定する制御部と、を備える。通信部は、端末装置 303 から、監視カメラ 301a、301b の設定に関する情報を受信し、端末装置 304 から、複数のゾーン A、B のうちの少なくとも 1 つのゾーンへの立ち入り許可を求める人物の登録顔データを受信する。これにより、ゾーンへの立ち入りを求める人物が直接登録顔データを監視カメラシステムに登録でき、便利となる。

【0332】

（変形例）

上記では、監視カメラシステムは、コンサート会場に適用されたとしたがこれに限られない。監視カメラシステムは、例えば、有料講座の会場、遊園地のアトラクション、映画館、新幹線等の列車、または飛行機等にも適用できる。

【0333】

例えば、監視カメラシステムを有料講座の会場に適用する場合、サーバ 302 は、人が適切な席（ゾーン）に座っているか否かを判定する。サーバ 302 は、有料講座の空席状況を把握してもよい。また、サーバ 302 は、どの席に誰が座っているかを判定してもよい。また、サーバ 302 は、成績と席との相関関係を算出してもよい。また、サーバ 302 は、有料講座の講師ごとにおける出席率を算出してもよい。

【0334】

また、監視カメラシステムを遊園地のアトラクションに適用する場合、監視カメラ 301a、301b は、アトラクション（ゾーン）ごとに設置されてもよい。サーバ 302 は、人が適切なアトラクションに居るか否かを判定してもよい。

【0335】

また、監視カメラシステムを映画館に適用する場合、監視カメラ 301a、301b は、上映される部屋（ゾーン）ごとに設置されてもよい。サーバ 302 は、人が適切な部屋の席に座っているか否かを判定してもよい。

【0336】

また、監視カメラシステムを新幹線に適用する場合、監視カメラ 301a、301b は、車両（ゾーン）ごとに設置されてもよい。サーバ 302 は、人が適切な車両の席に座っているか否かを判定してもよい。これにより、検札を簡素化できる。

【0337】

以上、実施の形態について説明した。上記の各実施の形態は組み合わせられてもよい。

【0338】

上述の各実施の形態において、テーブルに登録される登録顔データは、例えば、社員カードに付された写真であってもよい。例えば、カードリーダーは、カメラを備え、社員カードに付された写真を撮影し、サーバに送信してもよい。

【0339】

また、テーブルに登録される登録顔データは、レコーダに記憶された映像から取得され

10

20

30

40

50

てもよい。例えば、オペレータは、レコーダに記憶された映像を端末装置で再生し、再生した映像から、テーブルに登録したい人物の顔を切り取り、切り取った顔の顔データをテーブルに登録してもよい。

【0340】

また、テーブルに登録される登録顔データは、顔認証ゲートで撮影された顔データであってもよい。オペレータは、顔認証ゲートで撮影された顔データの画像を端末装置に表示し、表示した画像から、テーブルに登録したい人物の顔を切り取り、切り取った顔の顔データをテーブルに登録してもよい。

【0341】

上述の実施の形態においては、各構成要素に用いる「・・・部」という表記は、「・・・回路(circuitry)」、「・・・デバイス」、「・・・ユニット」、又は、「・・・モジュール」といった他の表記に置換されてもよい。

10

【0342】

以上、図面を参照しながら実施の形態について説明したが、本開示はかかる例に限定されない。当業者であれば、特許請求の範囲に記載された範疇において、各種の変更例または修正例に想到し得ることは明らかである。そのような変更例または修正例についても、本開示の技術的範囲に属するものと了解される。また、本開示の趣旨を逸脱しない範囲において、実施の形態における各構成要素は任意に組み合わせられてよい。

【0343】

本開示はソフトウェア、ハードウェア、又は、ハードウェアと連携したソフトウェアで実現することが可能である。上記実施の形態の説明に用いた各機能ブロックは、部分的に又は全体的に、集積回路であるLSIとして実現され、上記実施の形態で説明した各プロセスは、部分的に又は全体的に、一つのLSI又はLSIの組み合わせによって制御されてもよい。LSIは個々のチップから構成されてもよいし、機能ブロックの一部または全てを含むように一つのチップから構成されてもよい。LSIはデータの入力と出力を備えてもよい。LSIは、集積度の違いにより、IC、システムLSI、スーパーLSI、ウルトラLSIと呼称されることもある。

20

【0344】

集積回路化の手法はLSIに限るものではなく、専用回路、汎用プロセッサ又は専用プロセッサで実現してもよい。また、LSI製造後に、プログラムすることが可能なFPGAや、LSI内部の回路セルの接続や設定を再構成可能なリプログラマブル・プロセッサを利用してもよい。本開示は、デジタル処理又はアナログ処理として実現されてもよい。

30

【0345】

さらには、半導体技術の進歩または派生する別技術によりLSIに置き換わる集積回路化の技術が登場すれば、当然、その技術を用いて機能ブロックの集積化を行ってもよい。バイオ技術の適用等が可能性としてありえる。

【0346】

サーバが有すべき機能の処理内容を記述したプログラムが提供される。そのプログラムをコンピュータで実行することにより、上記処理機能がコンピュータ上で実現される。

40

【産業上の利用可能性】

【0347】

本開示の監視カメラシステムは、ゾーンごとに決められた人以外の人、ゾーンに立ち入っていないかを判定する監視カメラシステムにおいて有用である。

【符号の説明】

【0348】

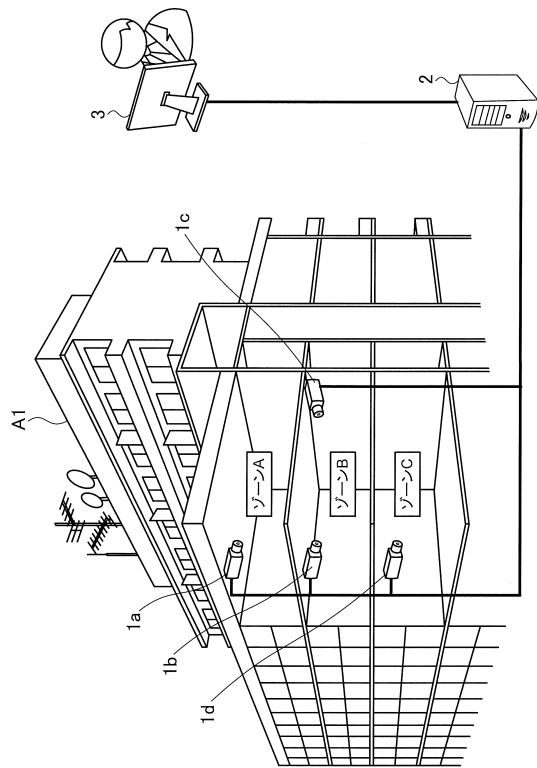
- 1a～1d, 101a, 101b, 301a, 301b 監視カメラ
- 2, 102, 302 サーバ
- 3, 61, 103, 303, 304 端末装置
- 11, 81 撮像部

50

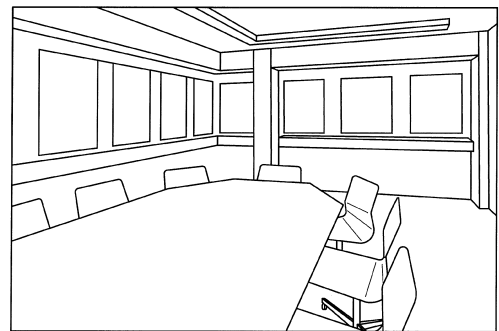
- 1 2, 2 1, 3 1, 8 2 制御部
- 1 3, 2 2, 3 4, 8 4 通信部
- 1 4, 2 3, 3 5, 8 5 記憶部
- 3 2 入力部
- 3 3 表示部
- 4 1 a, 4 2 a, 1 2 1 a, 1 3 1 a ゾーン識別情報
- 4 1 b, 4 1 b a ~ 4 1 b c, 5 1, 5 2, 9 1, 9 2, 1 1 1 ~ 1 1 3, 1 3 1 c, 1 3 2 a, 1 3 2 b, 1 4 1 ~ 1 4 4, 1 5 1 ~ 1 5 6, 1 6 6 ~ 1 6 6, 2 0 1, 2 0 2, 2 0 6, 2 0 7, 2 0 8, 2 0 9, 3 1 1 顔データ
- 4 2 b, 4 2 b a ~ 4 2 b c, 1 2 1 b カメラ識別情報
- 7 1 a ~ 7 1 c カードリーダー
- 8 3 カード通信部
- 1 0 4 a, 1 0 4 b, 1 0 5 a, 1 0 5 b 警報装置
- 1 3 1 b リスト情報
- T B 1, T B 2, T B 1 1, T B 2 1, T B 1 0 1, T B 1 0 2, T B 3 0 1, T B 3
- 0 2 テーブル
- A ~ C ゾーン
- A 1, A 1 0 1, A 3 0 1 建物

【図面】

【図 1】



【図 2】



10

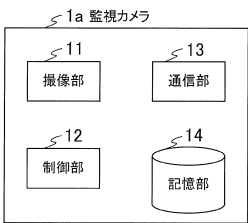
20

30

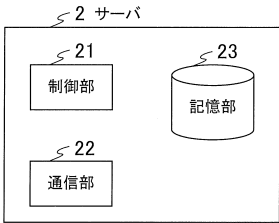
40

50

【図 3】

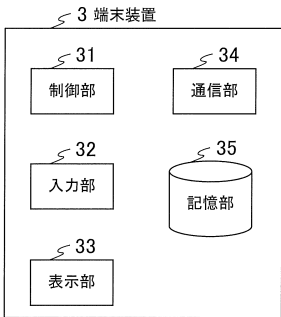


【図 4】

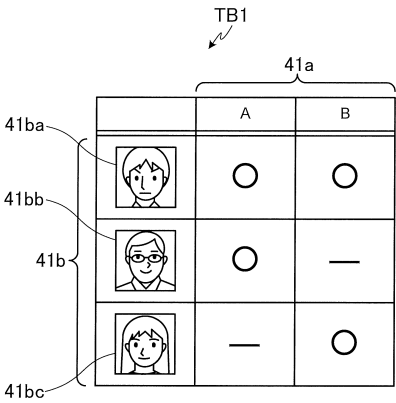


10

【図 5】



【図 6】



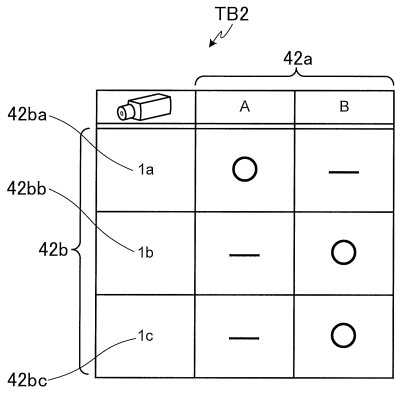
20

30

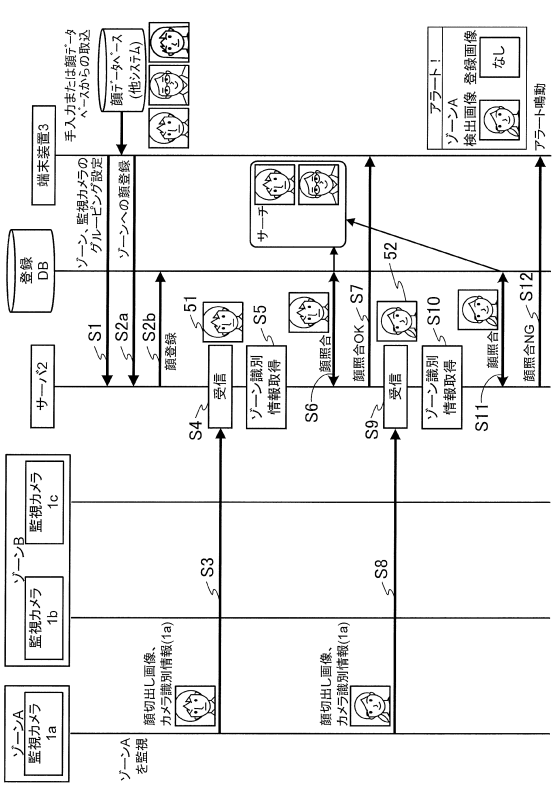
40

50

【図 7】



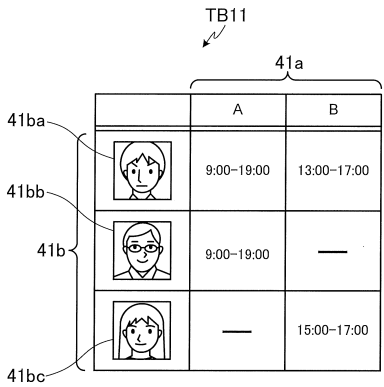
【図 8】



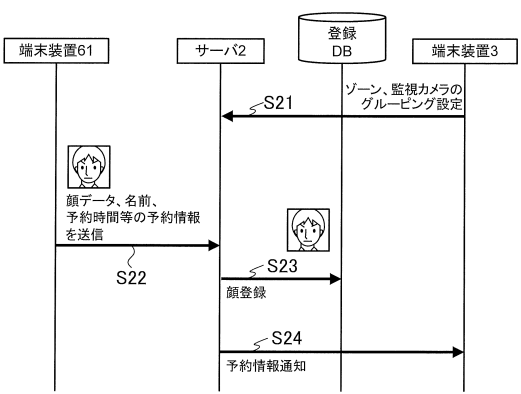
10

20

【図 9】



【図 10】

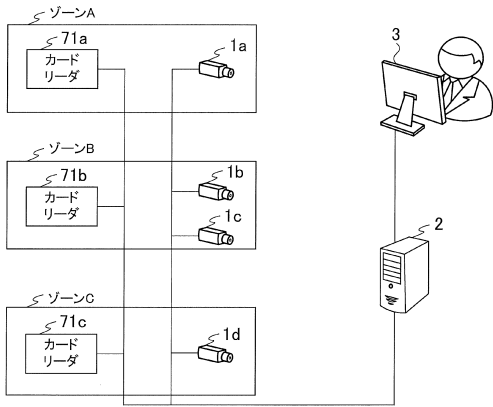


30

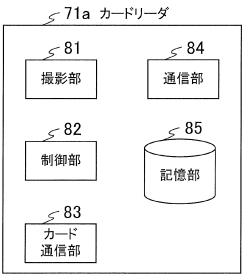
40

50

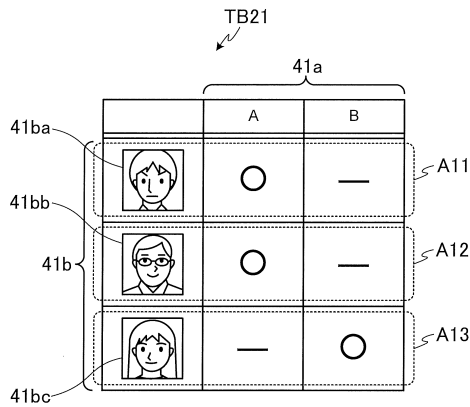
【図 1 1】



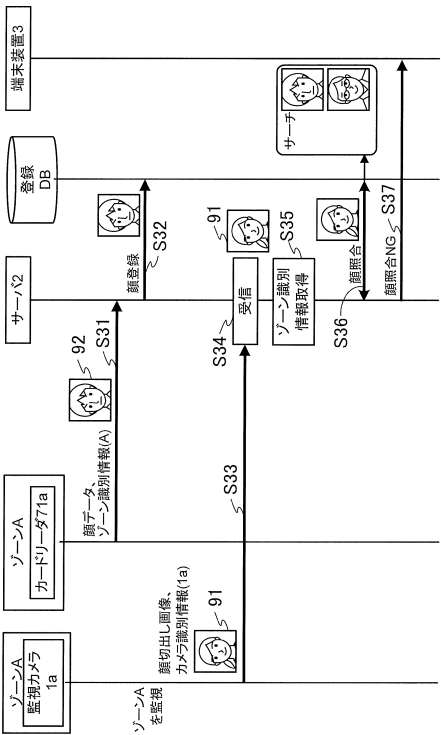
【図 1 2】



【図 1 3】



【図 1 4】



10

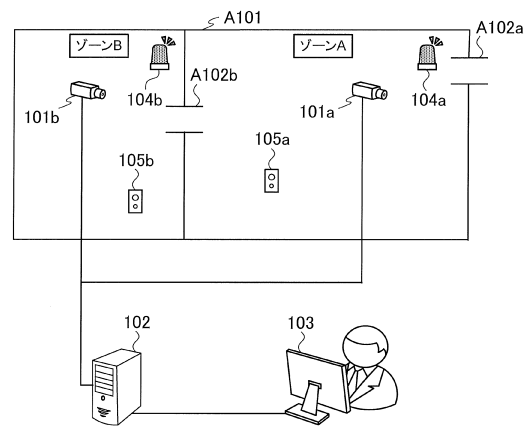
20

30

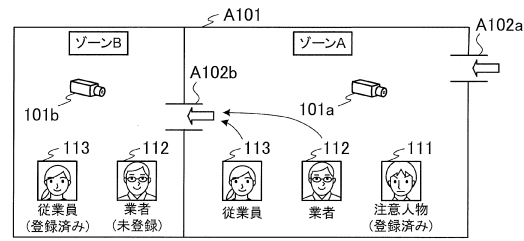
40

50

【図 15】

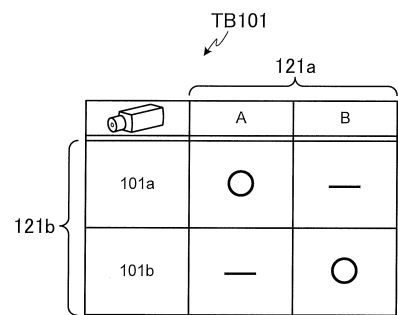


【図 16】

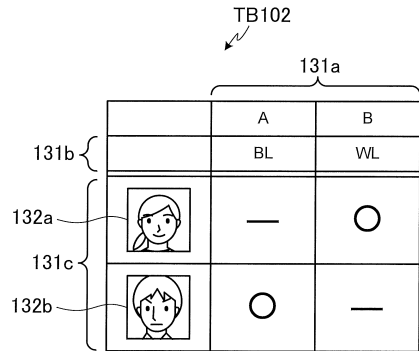


10

【図 17】



【図 18】



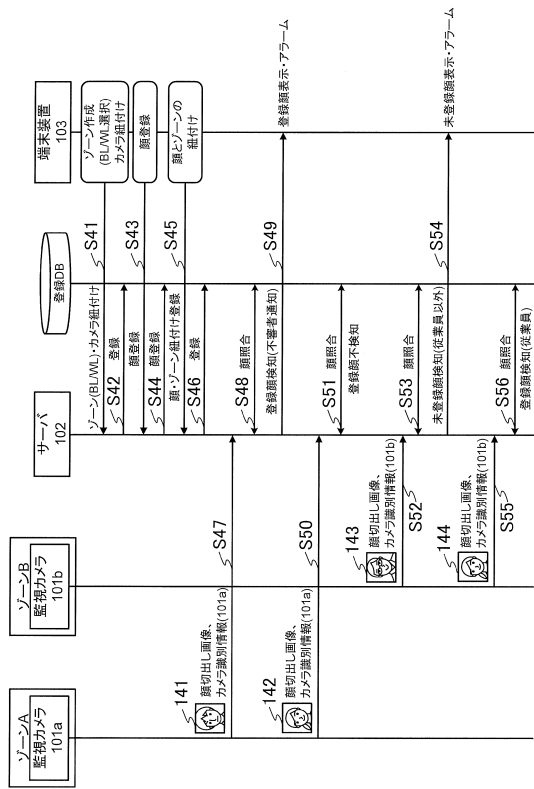
20

30

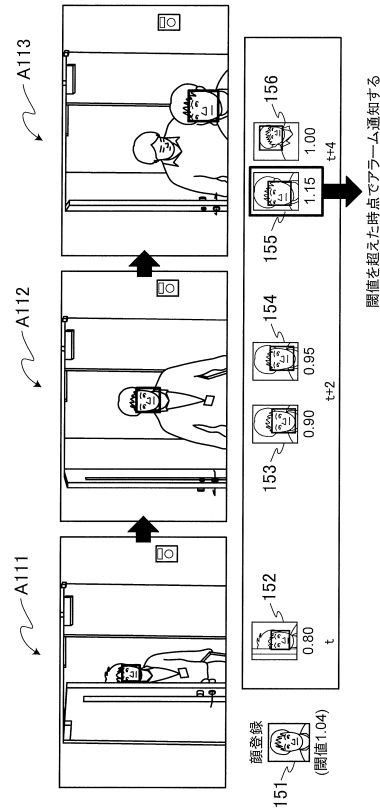
40

50

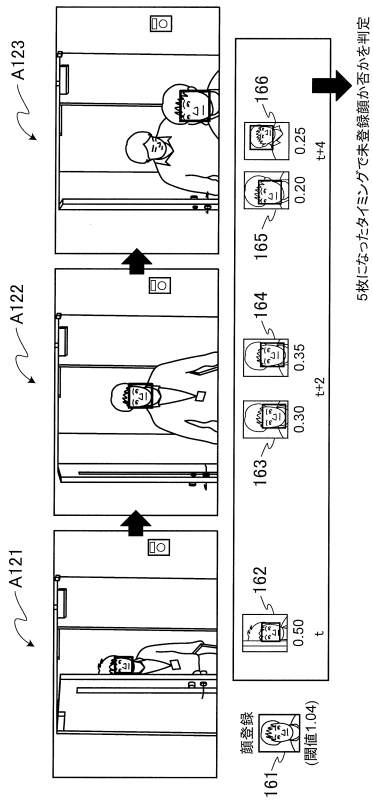
【図 19】



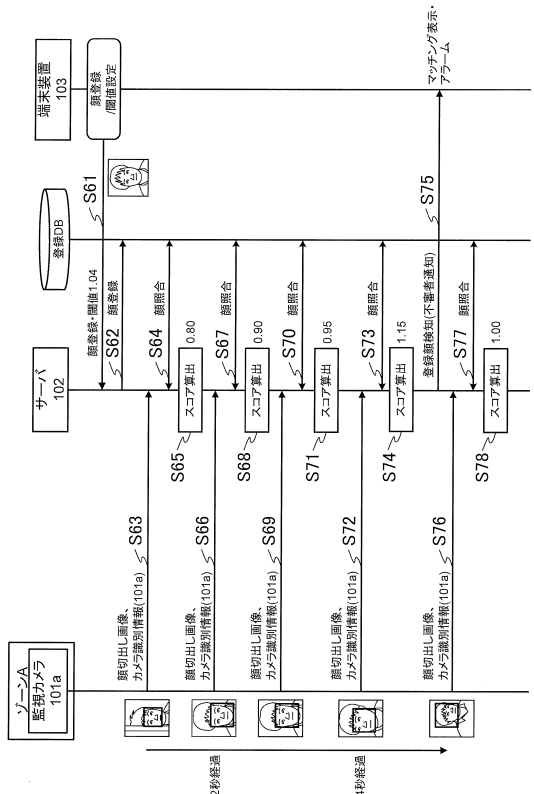
【図 20】



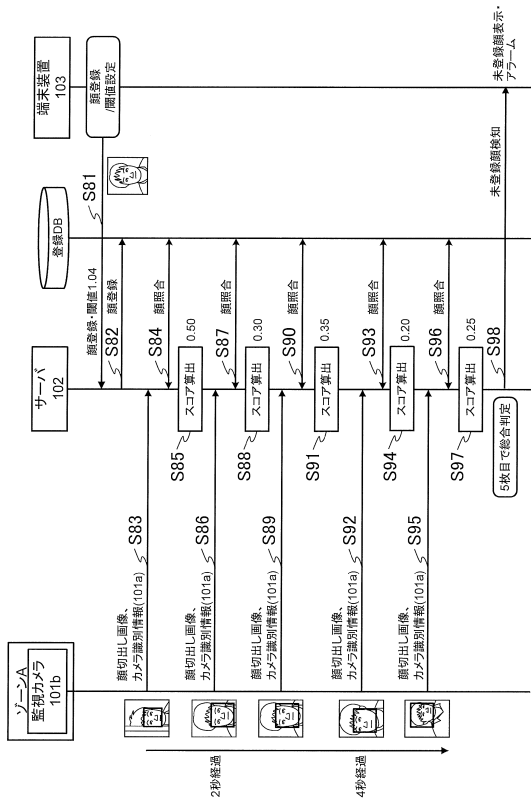
【図 21】



【図 22】



【図 2 3】



【図 2 4】



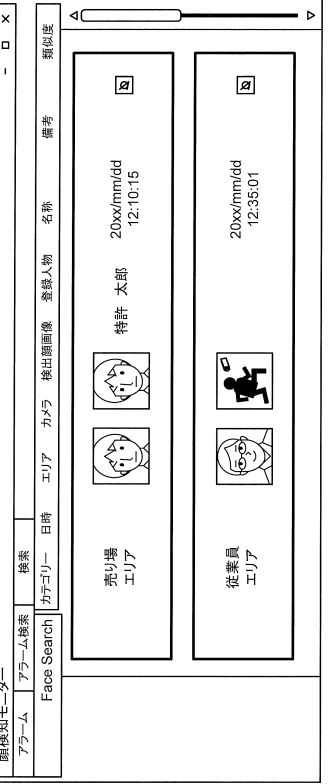
10

20

【図 2 5】



【図 2 6】

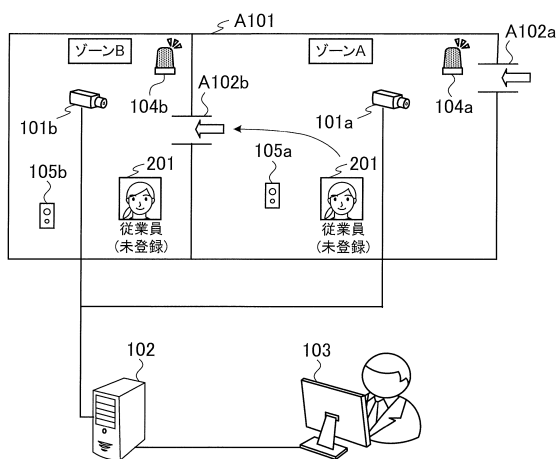


30

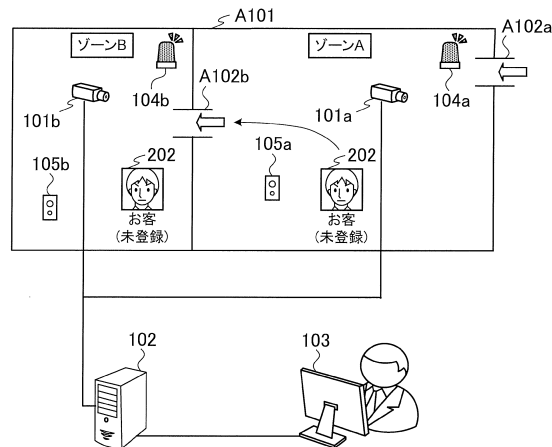
40

50

【図 27】



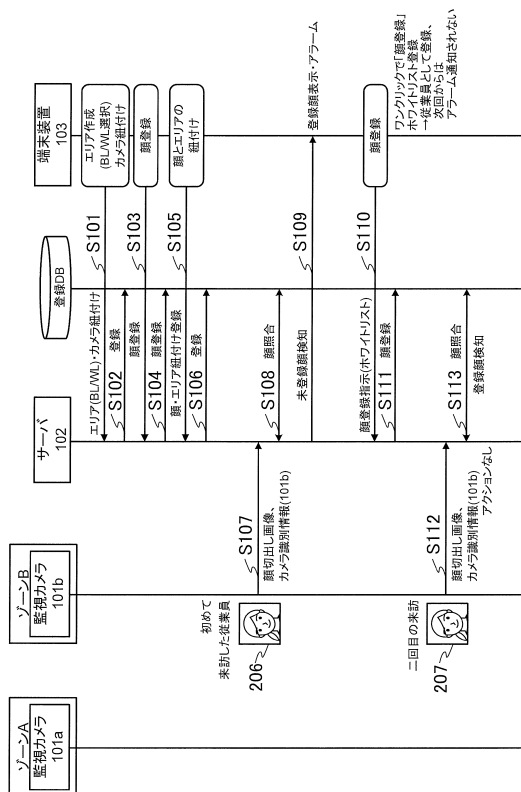
【圖 28】



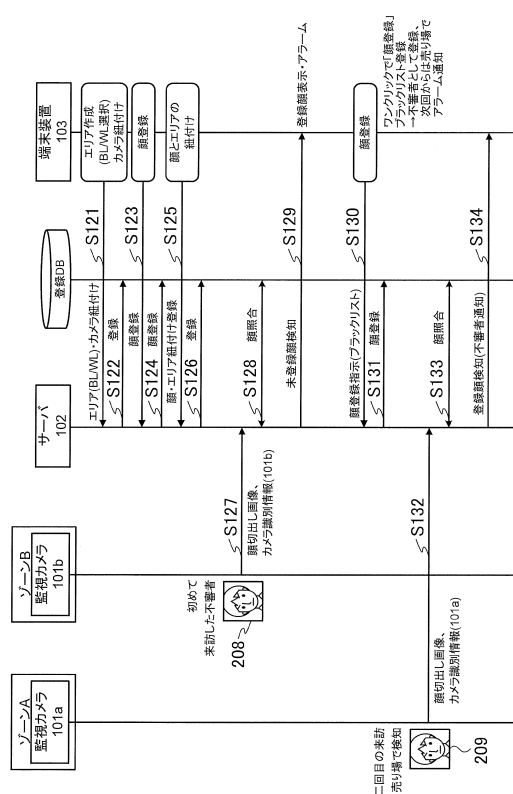
10

20

【圖 29】



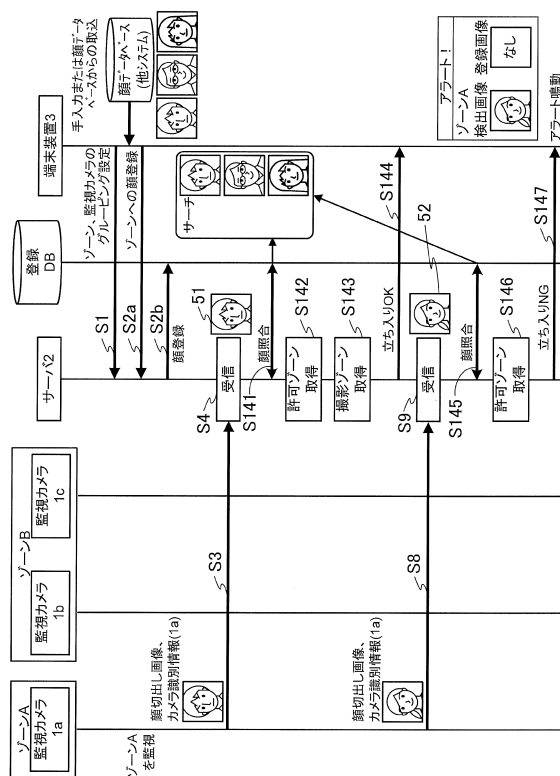
【図 30】



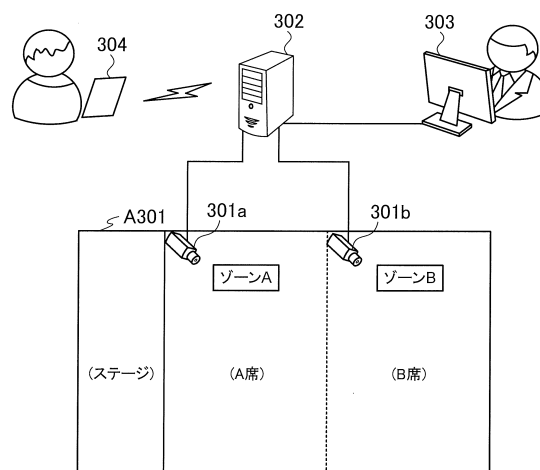
30

40

【図 3 1】



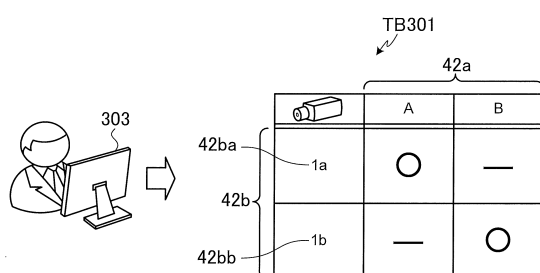
【図 3 2】



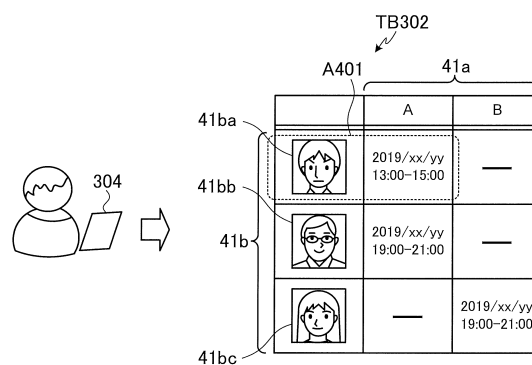
10

20

【図 3 3】



【図 3 4】

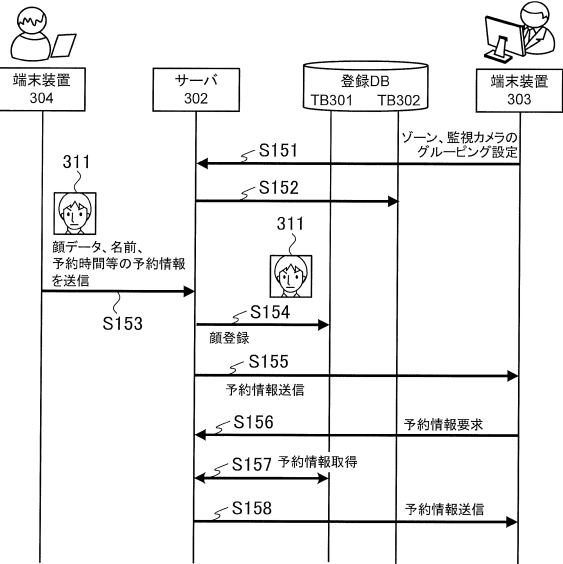


30

40

50

【図 35】



10

20

30

40

50

フロントページの続き

2号 パナソニック i-PRO センシングソリューションズ株式会社内

(72)発明者 関 信人

大阪府門真市大字門真1006番地 パナソニック株式会社内

審査官 中村 泰二郎

(56)参考文献 特開2004-280477 (JP, A)

国際公開第2018/193813 (WO, A1)

特開2012-226485 (JP, A)

特開2016-110308 (JP, A)

特開2008-141386 (JP, A)

特開2018-128970 (JP, A)

特開2010-026956 (JP, A)

(58)調査した分野 (Int.Cl., DB名)

G07C 9/00-9/38

G07B 15/00-15/06

G08B 23/00-31/00

E05B 49/00

G06T 1/00

G06Q 50/26

H04N 7/18