



## 【特許請求の範囲】

## 【請求項 1】

予め定められた所定の範囲を撮影する撮影手段と、  
 ユーザごとに画像のマスクパターンを保存する手段と、  
 前記撮影手段で撮影した画像を前記マスクパターンを用いて所定範囲の画像のみを抽出する切り出し手段と、  
 抽出後の画像を自動的にまたは要求時に配信する配信手段と、  
 を備えたことを特徴とする防犯装置。

## 【請求項 2】

前記抽出後の画像において、人などの特定のパターンに該当する動体を検出する変化検出手段を備え、

10

前記配信手段は、前記変化検出手段からの指令によって抽出後の画像を配信することを特徴とする請求項 1 記載の防犯装置。

## 【請求項 3】

前記撮影手段で撮影された画像をユーザごとに予め定められた補正方法によって画像を補正する画像補正手段を備えたことを特徴とする請求項 1 または 2 記載の防犯装置。

## 【請求項 4】

前記撮影手段を所定の範囲で自由に首振りして撮影する首振り手段と、

前記切り出し手段または前記画像補正手段の処理用として撮像した画像に関連付けて首振り角度情報を出力する制御手段を備えたことを特徴とする請求項 3 記載の防犯装置。

20

## 【請求項 5】

撮影希望・不可情報を保存する IC タグなどの無線発信手段から送られてくる前記撮影希望・不可情報を受信する受信手段と、

前記無線発信手段の発信位置を特定する手段と、

前記受信手段によって受信した撮影希望・不可情報に基づいて、撮影希望の場合は、当該無線発信手段の発信位置を含む所定エリアの撮影を行う撮影手段と、

撮影中に他の無線発信手段から送られてくる撮影不可情報を受信した場合は、当該他の無線発信手段の発信位置を含む前記所定エリアよりも狭い特定エリアをマスクして撮影する撮影制御手段と、

を備えたことを特徴とする防犯装置。

30

## 【請求項 6】

前記マスクには、ぼかしフィルタを用い、

前記撮影不可情報の発信位置と前記撮影希望情報の発信位置との距離に基づいて、前記ぼかしフィルタのぼかしの程度を変化させ、距離の接近に伴って、ぼかしの程度を弱くすることを特徴とする請求項 5 記載の防犯装置。

## 【請求項 7】

所定エリアごとにマスクパターンを保存する手段と、

前記撮影手段は、所定エリアを該マスクパターンを用いて所定エリアの一部をマスクした画像を生成することを特徴とする請求項 5 または 6 に記載の防犯装置。

## 【請求項 8】

40

ユーザへ監視用の画像を提供する画像提供方法であって

予め定められた所定の範囲を撮影するステップと、

ユーザごとに画像のマスクパターンを保存するステップと、

撮影した画像を前記マスクパターンを用いて所定範囲の画像のみを抽出するステップと

、  
 撮影範囲において人などの特定のパターンに該当する動体を検出するステップと、

動体を検出したときに、または、ユーザからの要求によって前記抽出後の画像を前記ユーザの端末装置へ送信するステップと、

を含むことを特徴とする画像提供方法。

## 【発明の詳細な説明】

50

**【技術分野】****【0001】**

本発明は、電柱などの屋外に設置された家や遊園地などを写すことのできるカメラにおいて、防犯契約などした特定の個人の家や領域のみを撮影して、その家庭の端末や警備会社に配信し、監視する防犯装置および画像提供方法に関する。

**【背景技術】****【0002】**

従来、屋内やエレベータなどの特定の場所の防犯カメラのプライバシーを保護した監視技術が提案されている。たとえば、特許文献1には、エレベータ内の監視において、予め登録されたIDをICタグなどに記録して、それを、プライバシーが保護されたそのマンションなどの住人に携帯させ、携帯しない人がエレベータに搭乗するとカメラが作動して、監視所などにその画像を送信する技術や、また携帯した人が前記携帯していない人と同乗した場合、携帯した人の部分の画像がマスクされて監視所などに送信され、プライバシーが保護された防犯装置の技術が提案されている。

10

**【0003】**

すなわち、屋内の狭い箇所に設置されたカメラで監視が必要な人と不要な人の区別を特別な識別手段を装備させて、その識別手段の有無でマスクすべきか否かを判定している。

**【0004】**

ところで、マンションやエレベータのような中に設置されたカメラと同様に、一般の個人住宅においても、複数の個人住宅を写すことのできる電柱などに設置されたカメラで前記と同様なプライバシーが保護された防犯システムが要求されている。

20

**【0005】**

しかしながら、電柱などの屋外に設置された広い範囲を写すカメラで、許可された個人住宅などのみを写して監視するためには、監視対象物がカメラより距離がある場合が多いため前記の従来技術である一般的なICタグのような識別手段では判定できない。また、一式ないし少ない数のカメラで複数の許可された住宅などを写して監視することは、経済的に有効であり、この技術が要望されている。

【特許文献1】特開2004-48519号公報

**【発明の開示】****【発明が解決しようとする課題】**

30

**【0006】**

本発明は上述のかかる事情に鑑みてなされたものであり、電柱などに設置した監視カメラで特定の複数の住宅や場所のみを写した画像より切り出して、その他の家などのプライバシーを保護しながら監視する防犯装置および画像提供方法を提供することを目的とする。

**【課題を解決するための手段】****【0007】**

上記目的を達成するため、本発明に係わる防犯装置は、予め定められた所定の範囲を撮影する撮影手段と、ユーザごとに画像のマスクパターンを保存する手段と、前記撮影手段で撮影した画像を前記マスクパターンを用いて所定範囲の画像のみを抽出する切り出し手段と、抽出後の画像を自動的または要求時に配信する配信手段と、を備えたことを特徴とする。

40

**【0008】**

本発明では、防犯などの監視するための家などを撮影するときに、監視の不要またはプライバシー保護のため撮影してはならない隣家などがやむを得ず撮影されてしまう場合、切り出し手段により、必要な画像部分のみを切り出し、切り出した画像を配信手段により必要な監視する家の人のパソコンや端末に配信することができる。このとき、ユーザごとにマスクパターンを予め設定しておき、このパターンによって対象部分以外をマスクすることによって簡便に他人のプライバシーを担保することができる。

**【0009】**

50

ここで、「切り出し」とは、画像そのものをカットする場合のみならず、所定サイズの画像の必要な部分のみを残して他をマスクするという処理も含む。

【0010】

本発明に係わる防犯装置は、前記の防犯装置に、さらに切り出し後の画像を保存して、前記配信手段により自動的に、または要求時に必要な箇所に配信させるため一時的に保存しておく保存手段を備えたことを特徴とする。

【0011】

本発明では、前記の作用に加えて、保存手段により防犯装置内に切り出した画像を保存し、その保存画像も要求時に必要な箇所に配信することができる。

【0012】

本発明に係わる防犯装置は、前記のものに、さらに切り出し後の画像に動く人などが写ったことを検出し、その画像を配信または保存するために前記配信手段や保存手段に起動信号を与える変化検出手段を備えたことを特徴とする。

【0013】

本発明では、前記の作用に加えて、変化検出手段で切り出した画像内に人などが入り、変化を検出したときの画像を即配信手段により配信したり、保存手段で保存した後、その画像を配信したりすることにより、防犯などに必要な画像の記憶容量と配信する情報量を少なくできる。なお、ICタグに被写体の識別情報を保存しておいて、その識別情報を受信した場合は、変化検出手段は動体の検出とみなさないようにしてもよい。これによって登録されたもののみICタグを携帯することによって監視対象から除外することができる。

【0014】

また、ICタグに被写体の識別情報を保存しておいて、その識別情報を受信した場合のみ、その周辺の限定エリアを監視可能とし、それ以外は監視できなくするようにしてもよい。これによって登録されたもののみICタグを携帯することによって、公共エリアなどにその人が入った場合だけ監視を許可され見ることができる。

【0015】

具体的には、本発明に係る防犯装置は、撮影希望・不可情報を保存するICタグなどの無線発信手段から送られてくる前記撮影希望・不可情報を受信する受信手段と、前記無線発信手段の発信位置を特定する手段と、前記受信手段によって受信した撮影希望・不可情報に基づいて、撮影希望の場合は、当該無線発信手段の発信位置を含む所定エリアの撮影を行う撮影手段と、撮影中に他の無線発信手段から送られてくる撮影不可情報を受信した場合は、当該他の無線発信手段の発信位置を含む前記所定エリアよりも狭い特定エリアをマスクして撮影する撮影制御手段と、を備えたことを特徴とする。

【0016】

公園などの公共のエリアでは、監視を希望するユーザのみにICタグなどの無線発信手段を携帯させて、その無線を受信している場合にのみ撮影を実行する。このとき、同じ公園に撮影を希望しないユーザが存在する場合は、そのユーザをマスクして撮影を行う。

【0017】

なお、撮影希望・不可情報は、撮影を希望するか、希望しないかという直接的な情報のみならず、間接的にこの情報が抽出できるような情報も含む趣旨である。たとえば、防犯装置が別のサーバで、ユーザ識別情報と撮影希望・不可情報とを関連付けておき、ユーザ識別情報を受信したときに、この関連付けによって撮影希望・不可情報を抽出するような場合におけるユーザ識別情報も含む。

【0018】

好ましくは、前記マスクには、ぼかしフィルタを用い、前記撮影不可情報の発信位置と前記撮影希望情報の発信位置との距離に基づいて、前記ぼかしフィルタのぼかしの程度を変化させ、距離の接近に伴って、ぼかしの程度を弱くするようにするとよい。これにより公共の場における安全監視において、防犯の効果と他人のプライバシーとの調和を図ることができる。

10

20

30

40

50

## 【 0 0 1 9 】

ここで、「ぼかし」とは、いわゆる分解能を荒くすることのみならず、たとえば特定エリアを黒くするなど、視認性をコントロールする処理全般を意味する。

## 【 0 0 2 0 】

本発明に係わる防犯装置は、前記のものに、さらにカメラで撮影された画像を前記切り出し手段などに入力する前に、見やすいように画像を補正する画像補正手段を備えたことを特徴とする。

## 【 0 0 2 1 】

本発明では、前記の作用に加えて、魚眼レンズや首振りにより広範囲を撮影することができるカメラの場合、監視する家などが斜めや歪んで撮影され、その家にとっては非常に見にくい画像を、画像補正手段により補正して見えやすい画像にすることで監視が容易になるとともに、監視カメラの台数を削減できる。

10

## 【 0 0 2 2 】

本発明に係わる防犯装置は、前記のものに さらに前記カメラをある範囲を自由に首振り（パンニングあるいはチルティング）して撮影する首振り手段と、前記補正手段や切り出し手段の処理用として首振り角度情報を通知する制御手段を備えたことを特徴とする。

## 【 0 0 2 3 】

本発明では、前記の作用に加えて、カメラを首振り手段とその制御手段により1台のカメラで広範囲な地域を撮影できるとともに、首振り角度情報により前記画像補正手段と切り出し手段の処理が容易にできる。

20

## 【 0 0 2 4 】

また、本発明に係る画像提供方法は、ユーザへ監視用の画像を提供する画像提供方法であって、予め定められた所定の範囲を撮影するステップと、ユーザごとに画像のマスクパターンを保存するステップと、撮影した画像を前記マスクパターンを用いて所定範囲の画像のみを抽出するステップと、撮影範囲において人などの特定のパターンに該当する動体を検出するステップと、動体を検出したときに、または、ユーザからの要求によって前記抽出後の画像を前記ユーザの端末装置へ送信するステップと、を含むことを特徴とする。

## 【 0 0 2 5 】

本発明では、ユーザごとのマスクパターンによって他人のプライバシーに係る部分は除外することができ、また撮影範囲内の動体の検出によって画像を保存ないし送信することによって効率的に防犯監視を行うことができる。なお、撮影範囲内に動体を検出したときに、ユーザの携帯電話等へメールあるいは音声で通知し、ユーザからのアクセスによって抽出画像を提供するようにしても良い。

30

## 【 発明の効果 】

## 【 0 0 2 6 】

本発明によれば、カメラで監視する防犯装置に、撮影された画像の中の必要な部分のみを切り出すか、または不要な部分をマスクする機能を装備させることによって少ない監視カメラで複数の住宅や場所を、プライバシーを保護しながら監視することが可能となり、経済性の優れた防犯システムが可能となる。

## 【 発明を実施するための最良の形態 】

40

## 【 0 0 2 7 】

以下、本発明の実施の形態を説明する。

## （第1の実施の形態）

図1は、第1の実施の形態による防犯装置のシステム構成図である。図4は、実際に使用されるシステムの鳥瞰図の例である。

## 【 0 0 2 8 】

図1で防犯装置1を中心に通信N1で接続されたカメラ2と、カメラ2で撮影された画像G0から必要な部分を切り出す切り出し手段10と、切り出した画像に人などが動く変化を検出して配信や保存を促す変化検出手段15と、切り出した画像または前記変化した画像を保存する保存手段12と、切り出した現在の画像または前記保存した画像を、該当

50

する画像の家のパソコンや携帯電話などの端末H 1 1、H 1 2や警備会社K 1に電話回線やIP回線などの通信手段N 2により配信する配信手段1 1から構成される。そして、切り出し手段1 0は、撮影された画像G 0から前記端末H 1 1、H 2 1毎に必要な画像G 1、G 2を切り出すためマスク手段1 0 1, 1 0 2, 1 0 3を持つ。なお、マスク情報は、形状、切り出しサイズごとにパターン化して保存するようにしても良い。

#### 【0029】

図1と、図2のマスク原理図で動作を説明する。まず、防犯のための撮影と監視を契約したお宅をA宅H 1とB宅H 2とし、その両宅とも遊園地H 3の監視も行うよう依頼されているとする。そしてA宅H 1は、警備会社K 1とも契約しており、A宅の端末H 1 1に送信される同じ画像を警備会社K 1にも配信するよう契約されているとする。

10

#### 【0030】

次に、カメラ2で撮影される画像には、監視の契約していなく、その家のプライバシーが保護さなければならぬC宅H 4もやむを得ず撮影されてしまうとする。この状態で、図2では、カメラ2で撮影された全体画像G 0から切り出し手段1 0により、A宅H 1用には、マスク手段1 0 1と1 0 3とによりA宅H 1の画像G 1と遊園地H 3の画像G 3が切り出され、その現在画像、または前記変化検出手段1 5により変化を検出したときの画像を、A宅の端末H 1 1と警備会社K 1に配信手段1 1により通信手段N 2を介して配信するとともに保存手段1 2に保存する。B宅H 2用としては、同様にマスク手段1 0 2と1 0 3により必要な画像G 2、G 3が切り出され、前記と同じ処理がなされる。C宅H 4は、配信の契約をしていないので画像の切り出しや保存および配信はしない。

20

#### 【0031】

保存手段1 2で保存された各契約宅H 1、H 2の画像は、後で確認する必要が発生したとき、各宅の端末H 1 1、H 2 1や警備会社K 1からの要求により配信手段1 1を介して送信させる。

#### 【0032】

(第2の実施の形態)

図3は、第2の実施形態による装置構成図である。図1と同じ部分は同じ記号を使用しているので説明を省く。図1の構成と異なる箇所は、カメラ2の首振り制御などする首振り手段2 1と、これを制御する制御手段1 4と、首振りなどにより斜めに写された生画像を見やすいよう、たとえば正面から撮影しているように補正する画像補正手段1 3とを防犯装置1内に設けたものである。

30

#### 【0033】

動作をこの図3と、図4のマスク原理図で説明する。ここでは、カメラ2の首振り手段2 1により撮影できる範囲が、前記したA宅からF宅まで8箇所まで広がるとし、A、B、E宅H 1、H 2、H 6が監視の契約をしているとする。この中でB宅が前記した自宅H 2と遊園地H 3の画像を処理する動作を説明する。カメラ2の首振りは、制御手段1 4の指令により首振り手段2 1を介して、通常左右にゆっくり振られているとする。まず、カメラ2の斜めの位置にある宅などを撮影した生画像G<sub>n</sub>を画像補正手段1 3により、たとえば、正面から見たような画像に補正した後の画像G 0を作る。B宅H 2用のマスク手段1 0 2と1 0 3は、A宅～F宅までの全体の画像に対して固定されたB宅H 2と遊園地H 3位置に常にあるよう制御手段1 4からの首振り角度情報により撮影された補正画像G 0に対して、相対的に逆に移動して切り出し画像の位置を変化させない。すなわち、B宅H 2が真ん中に撮影されていれば、マスク手段1 0 2も真ん中にあり、横にずれて撮影されたならその分ずれて切り出されるようマスク手段1 0 2を制御手段1 4からの首振り角度情報により切り出し手段1 0が制御する。保存手段1 2の機能は、前記した図1ものと同じである。

40

#### 【0034】

他の実施例として、前記マスクによる切り出し手段1 0でなく、前記カメラ2の倍率を大きくして、ある宅の一部分程度しか撮影されない状態にして、前記首振り手段2 1の首振り角度をその宅以外を写さないよう前記制御装置1 4が制限することで、マスクと同じ

50

機能を持つことができる。

【0035】

また、カメラ2の種類として、通常のカメラの代わりに、魚眼レンズのような広範囲を同時に撮影できるものでも良い。このようなカメラも、前記画像補正手段13により正常に見えるようにできる。

【0036】

この他、監視対象物が、カメラと近い位置にある場合、その家の人にICタグなどの無線タグを携帯させ、登録された無線タグ以外の人々が画像に写ったら撮影するようにしてもよい。

【0037】

以上、本実施の形態によれば、図5に示すような屋外の電柱などに設置したカメラと通信設備により、他人の家などの画像をマスクして、自宅や共有の場所の画像のみを配信したり、保存しておくことにより、プライバシーが保護されながら携帯電話などの画面でいつでも現在の状態や過去の状態を確認できるので、防犯に役立てることができる。

【0038】

(第3の実施の形態)

また、監視要求対象が通学路・公園などのように連続で撮影するとプライバシーでコンセンサスが得られない場合など、子どもにICタグを携帯させ、登録された無線タグの人がその画像に入っている時だけ、その付近(限定された範囲)の画像監視を可能とするサービスで、公共のエリアを個人が家族の安全のために限定的に監視するというポリシーで理解が得やすくなる。

【0039】

以下、本サービスについて詳細に説明する。

まず、防犯装置1の基本的な構成は、第1または第2の実施の形態と同様である。本実施の形態では、図6に示すように撮影エリアごとに、マスクパターン(固定用、移動用)と、公共の場か否かを現す区分を関連付けて記憶した撮影エリア管理テーブル41を設ける。ここでマスクパターン(固定用)は、撮影エリアごとに固定的に定まるもので、図7に示すように、撮影エリアごとにマスク箇所31を記憶する。なお、カメラ2をパンニング、チルティングなどの動作をさせるときは、その動きに連動して、角度による画像の変形を計算して、マスク箇所も移動する。マスクパターン(移動用)は、マスク対象(たとえば人物)によって定まるもので、ICタグの位置によってマスク位置が変動する。

【0040】

次に、本実施の形態による防犯装置1の処理手順を図8を用いて説明する。

撮影エリア内に、ICタグを携帯したユーザが入ると、エリア内の複数箇所に設置されたICタグ情報の受信器を通して防犯装置1に通知される。防犯装置1では、ICタグ識別情報を取得して(S101)、監視希望者が否かを判定する(S102)。この判定は、ICタグ識別情報ごとに監視希望か、不可(拒否)かを示すフラグを関連付けて保存しておいて、このフラグによって判定してもよいし、ICタグから直接監視希望・不可情報を発信するようにしても良い。

【0041】

そして、監視希望者の場合は(S102で「YES」)、所定時間監視エリアの撮影を行う。このステップS101~S103の処理を繰り返すことによって、監視希望者が撮影エリア内にいる間は、撮影が続けられることになる。なお、撮影された映像は、防犯装置1内に保存されており、ICタグ識別情報に対応するユーザからのアクセス要求によって、配信される。このとき、第1または第2の実施の形態で説明したように、撮影エリアに対応するマスクパターン(固定用)によって予め決められた特定領域がマスクされた状態で配信される。

【0042】

一方、ステップS102で「NO」の場合は、次にICタグ識別情報によって監視非希望者が否かを判定し(S104)、監視非希望者の場合は、さらに当該エリアが撮影中か

10

20

30

40

50

否かを判定して、撮影中の場合は（S104で「YES」）、そのICタグ識別情報に対応するマスクパターン（移動用）を抽出する（S106）。通常は、人間の顔や全身をマスクするためのパターンで、カメラ2との距離や撮影倍率に応じてそのパターンを拡大縮小する。この場合パターン情報としては、ICタグの位置を中心とした半径（ $r$ ）で持たせるようにしても良い。

#### 【0043】

そして、監視エリア内に監視希望者が存在する場合は（S107で「YES」）、両者のICタグ位置をもとに監視希望者と監視非希望者の距離を演算して（S108）。その距離に応じて監視非希望者をマスクするための移動用マスクパターンのぼかし度合いを決定する（S109）。これは、たとえば、図9に示すようにマスク度合い管理テーブル42によって、距離に応じて決定するようにしてもよいし、距離をパラメータとした演算式によって、ぼかし度合い（たとえば画像合成におけるアルファブレンディングの値）を算定するようにしても良い。ぼかし度合いを距離が離れているときは大きく、距離が接近したときには小さく（即ち、より鮮明な画像）することによって、被害発生時の有効な解析が可能となる。

10

#### 【0044】

そして、監視非希望者の位置を中心にして、ステップS106で抽出・拡大縮小処理した特定範囲をステップS109で決定したぼかし度合いでぼかして保存する（S110）。この画像例を図10に示す。監視希望者32がこの撮影領域に入ることによって、撮影が行われ、監視非希望者33は、ステップS104～ステップS110の処理によって、監視希望者32との距離に応じたマスク度合いによってマスクされている。また、ICタグを携帯しない者34は、そのまま撮影される。プライベートな建物は、予め定められたパターン31によってマスクされている。

20

#### 【0045】

この撮影画像は、ユーザ32の要求によって配信される。あるいは、ユーザ32が子供であるような場合は、その保護者に配信されるようにするか、その保護者が子供の携帯するICタグに係り付けられたパスワードで防犯装置1にアクセスすることにより、リアルタイムに監視できるようにしてもよい。

#### 【0046】

以上、本実施の形態によれば、公共の場での撮影を拒否する人に対しては、撮影拒否用のICタグを携帯させ、その携行者が撮影範囲に入った場合は、ICタグ位置から所定範囲をぼかした状態で撮影し、監視希望者（あるいは監視対象者）と希望しない者（監視非希望者）との接近度合いに応じて、監視非希望者のぼかしの程度を変化させる（即ち、監視を希望しない者が監視を希望する者に接近するにしたがってぼかしの程度を弱くしていく）ので、公共の場における監視非希望者のプライバシーと、監視希望者の安全性の確保との調和を図ることができる。

30

#### 【産業上の利用可能性】

#### 【0047】

本発明は、地域や家庭の防犯監視システムに利用することができる。

#### 【図面の簡単な説明】

40

#### 【0048】

【図1】本発明の第1の実施の形態による防犯装置とそのシステムの構成図である。

【図2】図1の防犯装置のマスク原理図である。

【図3】本発明の第2の実施の形態による防犯装置とそのシステムの構成図である。

【図4】図2の防犯装置のマスク原理図である。

【図5】本発明のシステムの鳥瞰図である。

【図6】本発明の第3の実施の形態による撮影エリア管理テーブル41のデータ例である。

。

【図7】本発明の第3の実施の形態によるマスクパターンのデータ例である。

【図8】本発明の第3の実施の形態による防犯装置の処理手順を示すフローチャートであ

50

る。

【図9】本発明の第3の実施の形態によるマスク度合い管理テーブル42のデータ例である。

【図10】図8の処理によって作成される画像例である。

【符号の説明】

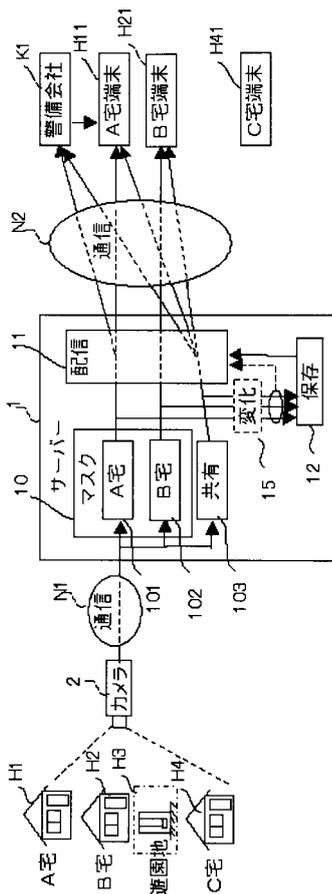
【0049】

- 1 防犯装置
- 2 カメラ
- 10 画像切り出し手段
- 11 配信手段
- 12 保存手段
- 13 画像補正手段
- 14 制御手段
- 15 変化検出手段
- 21 カメラ用首振り手段
- 41 撮影エリア管理テーブル
- 42 マスク度合い管理テーブル
- 101、・・・106 マスク手段
- G0, 1、・・・6 画像
- H1、・・・H8 撮影被写体
- H11, 21, 61 端末
- K1 警備会社

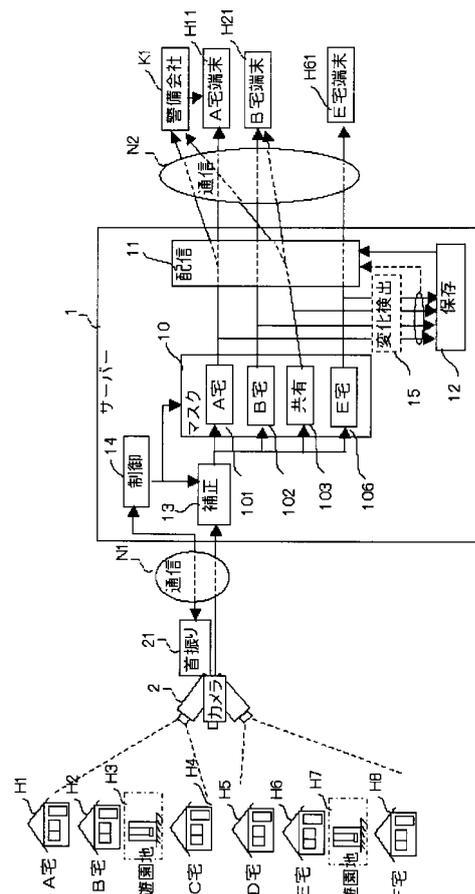
10

20

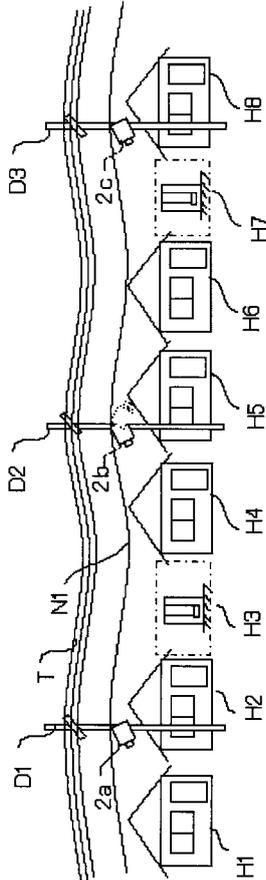
【図1】



【図3】



【 図 5 】

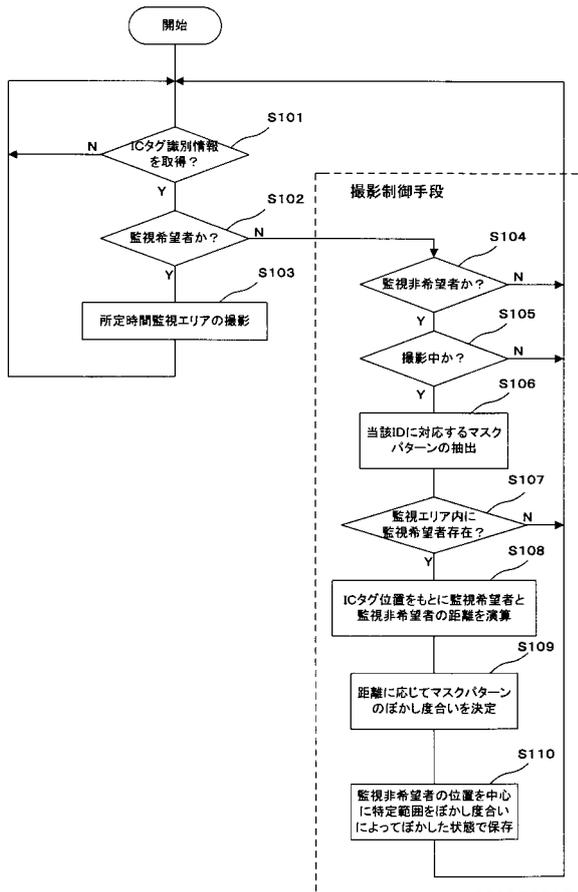


【 図 6 】

撮影エリア管理テーブル

撮影エリア	区分	マスクパターン (固定用)	マスクパターン (移動用)
AAA	0	X001	Y001
BBB	1	X002	Y002
CCC	1	X003	Y003
⋮	⋮	⋮	⋮

【 図 8 】

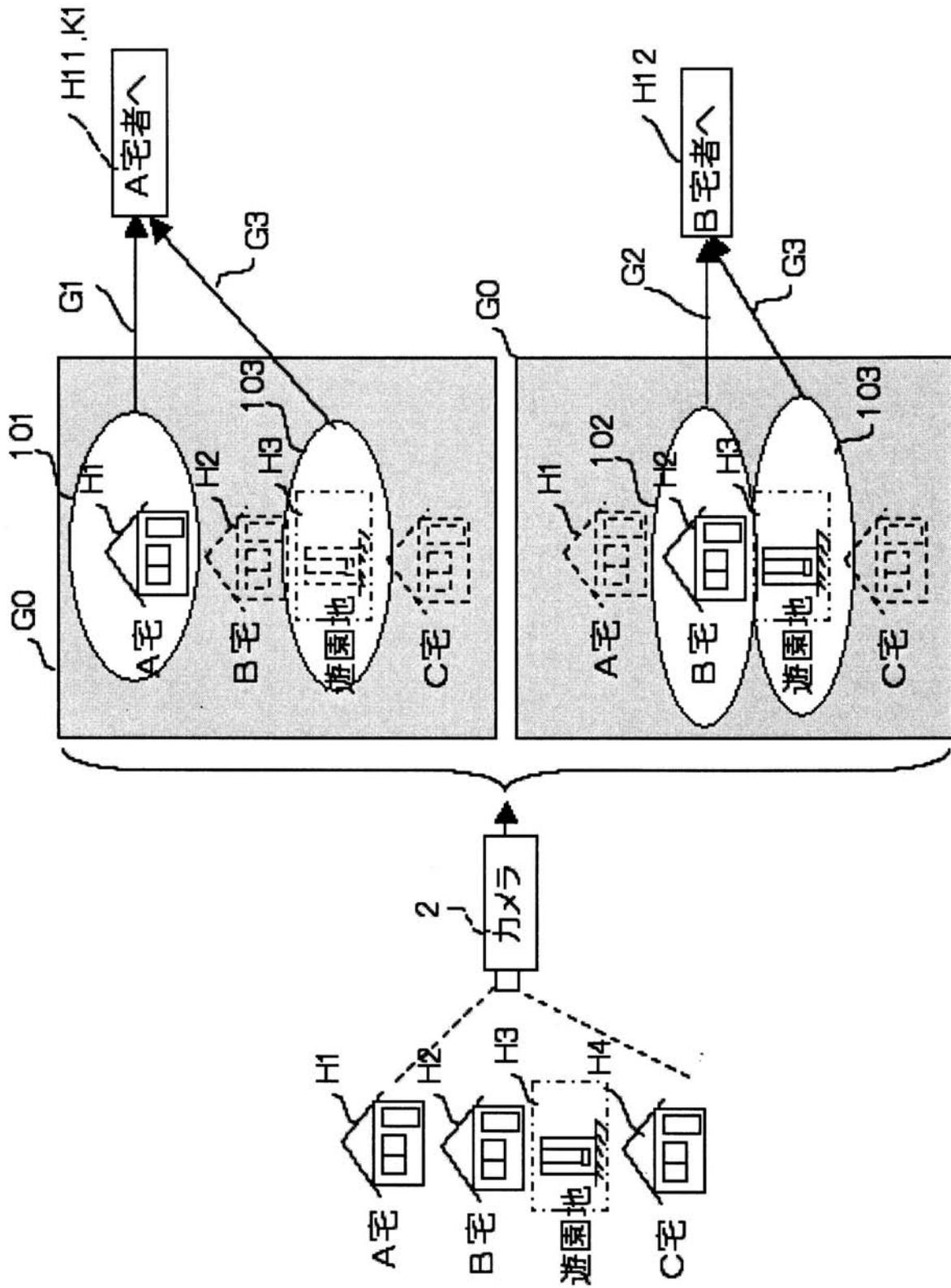


【 図 9 】

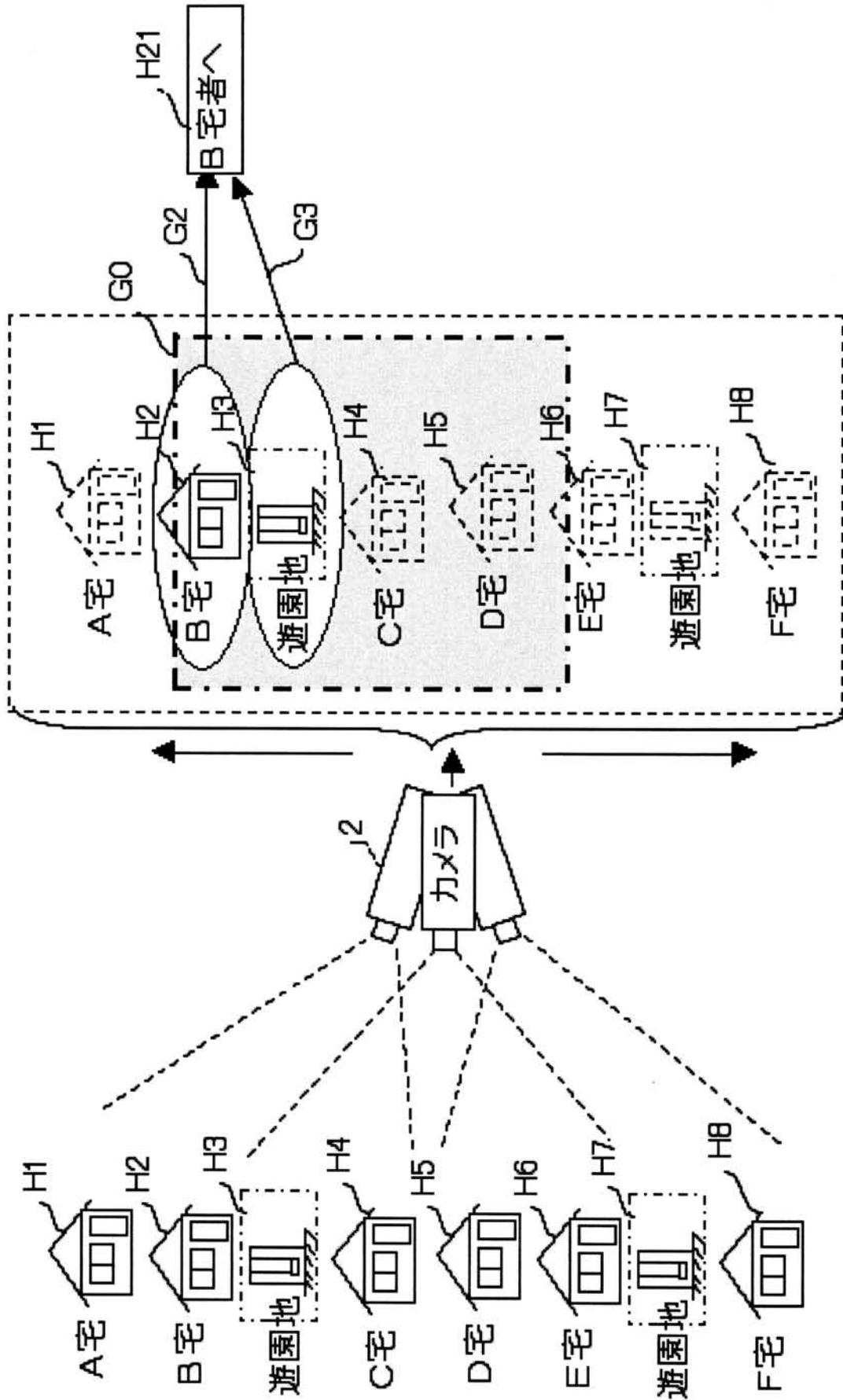
マスク度合い管理テーブル

距離	マスク度合い (ぼかし度合い)
〇〇~△△	0.7
△△~□□	0.6
⋮	⋮
⋮	⋮

【図2】

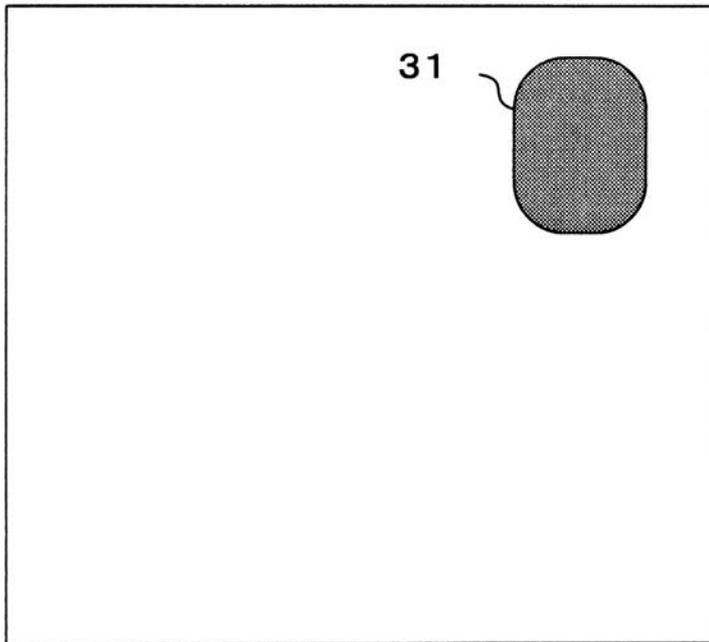


【 図 4 】



【図7】

マスクパターン(固定用) X002



マスクパターン(移動用) Y002

マスク領域 r=○○

【 図 1 0 】

