(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第3805036号

(P3805036)

(45)発行日　平成18年8月2日(2006.8.2)　(24)登録日　平成18年5月19日(2006.5.19)

(51)Int.Cl.			F I		
H04N	5/232	(2006.01)	H04N	5/232	B
H04N	7/14	(2006.01)	H04N	7/14	
H04N	7/18	(2006.01)	H04N	7/18	E

請求項の数 6　(全 12 頁)

(21)出願番号　特願平8-284447
(22)出願日　平成8年10月25日(1996.10.25)
(65)公開番号　特開平10-136247
(43)公開日　平成10年5月22日(1998.5.22)
審査請求日　平成15年10月22日(2003.10.22)

(73)特許権者　000001007
キヤノン株式会社
東京都大田区下丸子３丁目３０番２号
(74)代理人　100076428
弁理士　大塚　康徳
(74)代理人　100093908
弁理士　松本　研一
(72)発明者　中川　久雄
東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内

審査官　関谷　隆一

(56)参考文献　特開平０８－２３７５３２（ＪＰ，Ａ）

最終頁に続く

(54)【発明の名称】カメラ制御装置及び制御方法

(57)【特許請求の範囲】

【請求項１】

カメラのアングルを制御するカメラ制御装置であって、

前記カメラの撮影を不許可にする撮影不許可範囲を示す情報を記憶している記憶手段と、

入力された指示情報に基づいて前記カメラのアングルを制御する制御手段と、

前記撮影不許可範囲の両側に撮影可能範囲が存在する場合において、前記入力された指示情報が現在カメラの撮影している一方の撮影許可範囲から前記撮影不許可範囲に入るアングル変更の指示であった場合、前記アングル変更の方向に従って飛び越し方向を検出し、前記検出した飛び越し方向へと前記撮影不許可範囲を飛び越した位置にある他方の撮影許可範囲にカメラのアングルを自動制御する自動制御手段と、

を備えることを特徴とするカメラ制御装置。

【請求項２】

前記アングル変更はパン方向及びチルト方向の少なくとも１方向の変更であることを特徴とする請求項１に記載のカメラ制御装置。

【請求項３】

前記自動制御手段は、前記他方の撮影許可範囲に自動制御する際に前記撮影不許可範囲を撮影しないように、ズーム倍率を変更することを特徴とする請求項２に記載のカメラ制御装置。

【請求項４】

入力された指示情報と、予め記憶しておいたカメラの撮影を不許可にする撮影不許可範囲を示す情報とに基づき、前記カメラのアングルを制御するカメラ制御方法であって、

前記撮影不許可範囲の両側に撮影可能範囲が存在する場合において、入力された指示情報が現在カメラの撮影している一方の撮影許可範囲から前記撮影不許可範囲に入るアングル変更の指示であった場合、前記アングル変更の方向に従って飛び越し方向を検出し、前記検出した飛び越し方向へと前記撮影不許可範囲を飛び越した位置にある他方の撮影許可範囲にカメラのアングルを自動制御することを特徴とするカメラ制御方法。

【請求項５】

前記アングル変更はパン方向及びチルト方向の少なくとも１方向の変更であることを特徴とする請求項４に記載のカメラ制御方法。

【請求項６】

前記他方の撮影許可範囲に自動制御する際に前記撮影不許可範囲を撮影しないように、ズーム倍率を変更することを特徴とする請求項５に記載のカメラ制御方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明はカメラ制御装置及び制御方法に関するものである。

【０００２】

【従来の技術】

一般にテレビ電話、テレビ会議、或いは監視カメラ等の多地点間遠隔カメラ映像システムにおいては、映像または音声データを圧縮するなどして送受信するが、この時、カメラ装置等の画像入力装置や、音声入力装置等から入力された情報は全て相手側に送られていた。

【０００３】

しかしながら、近年では、映像入力装置の小型化、コンピュータのハードウェアの処理速度の向上、及び、ＯＳの発達により、専用のスペースを必要とせず、既設のネットワークを介して映像を伝送することも可能になってきた。

【０００４】

この結果、非常に安価な投資のみで、企業に張り巡らされたネットワークによる企業内のテレビ会議システムは勿論、企業間、企業自宅間でのテレビ会議も可能になる土台ができるようになっている。また、例えばインターネットを介して遠隔のカメラの映像を自宅から観賞することもできるようになってきている。

【０００５】

【発明が解決しようとする課題】

テレビ会議等では、業務上の会議という色合いも濃いので撮影される映像に関してはそれほど問題にはならないと考えられる。が、これが個人レベルまで普及するとなると、プライバシー保護、守秘義務といった問題がクローズアップされることになるであろう。

【０００６】

特に、雲台とカメラ部分が分かれており、パン、チルト、ズーム、フォーカス等がコンピュータ制御可能な映像入力装置を備えたシステムにおいては、ユーザが遠隔地からこの映像入力装置を制御可能にしてしまうと、意図しない領域へのアクセスも可能になり、上記の問題はもはや無視できないであろう。

【０００７】

【課題を解決するための手段】

本発明はかかる問題点に鑑みなされたものであり、撮影不許可範囲を設け、この不許可範囲に対するアクセスを禁止すると共に、その端末に対して警告してプライバシー保護、及び守秘義務を果たすことを可能にするカメラ制御システム及びカメラサーバ及びその制御方法及び記憶媒体及びカメラ制御装置を提供しようとするものである。

【０００８】

この課題を解決するため、例えば本発明のカメラ制御装置は以下の構成を備える。すな

わち、
カメラのアングルを制御するカメラ制御装置であって、
前記カメラの撮影を不許可にする撮影不許可範囲を示す情報を記憶している記憶手段と、
入力された指示情報に基づいて前記カメラのアングルを制御する制御手段と、
前記撮影不許可範囲の両側に撮影可能範囲が存在する場合において、前記入力された指示情報が現在カメラの撮影している一方の撮影許可範囲から前記撮影不許可範囲に入るアングル変更の指示であった場合、前記アングル変更の方向に従って飛び越し方向を検出し、前記検出した飛び越し方向へと前記撮影不許可範囲を飛び越した位置にある他方の撮影許可範囲にカメラのアングルを自動制御する自動制御手段とを備える。

【０００９】
【発明の実施の形態】
以下、添付図面に従って本発明に係る実施形態の一例を詳細に説明する。
【００１０】
図１は実施形態におけるテレビ会議システムの端末の構成を示している。図示において、１１は装置のＢＩＯＳやブートプログラムを記憶しているＲＯＭ、１２は装置全体の制御を司るＣＰＵ、１３は表示装置（図示ではＣＲＴ）である。１４はＣＰＵ１２が実行するＯＳやテレビ会議システムとして動作する各種プログラムを格納するＲＡＭであって、ＣＰＵ１２のワークエリアとしても使用する。１５はＯＳ、テレビ会議システム用のプログラム、更には各種情報ファイル（後述するアクセスコントロールテーブルを含む）を記憶している外部記憶装置である。１６はキーボード、１７はポインティングデバイスである。１８はネットワークインタフェース（ＮＩＣ）であって、テレビ会議を行なう他の端末がこのＮＩＣ１８を通じて接続されている。１９はビデオカメラであって、ＣＰＵ１２の制御に従ってズーム倍率が制御可能になっており、且つ、所定の雲台に搭載されていて、ＣＰＵ１２の制御の下で、パン及びチルトの制御も可能になっている。２０は音声入出力装置であって、不図示のマイク、スピーカを接続し、音（主に音声）の再生出力及び音の入力そしてデジタル化処理を行なうものである。
【００１１】
なお、テレビ会議システムを構成する他の端末も基本的に同じ構成であるので、ここでは１つの端末について説明した。
【００１２】
さて、上記構成において、装置の電源を投入し、キーボード１６もしくはマウス１７でもってテレビ会議システムに関するプログラムを実行が指示されると、ＣＰＵ１２は外部記憶装置１５よりテレビ会議システム用のプログラムをＲＡＭ１４に読出し、実行することになる。
【００１３】
実施形態の端末装置上で動作するＯＳはマルチウインドウタイプである。図２に従ってマルチウインドウシステムの概要を説明する。同図において、２０は１つの物理ディスプレイ表示画面、２１はマルチウィンドウを利用するアプリケーション、２２はディスプレイ装置２０の行数と桁数に対応する行数と桁数からなる論理画面バッファで、この論理画面バッファ２２内でアプリケーション２１が動作することになる。アプリケーション２１は、仮想ディスプレイである論理画面バッファ２２に結合している。
【００１４】
ディスプレイ表示装置２０上には、論理画面バッファ２２の内容を見るためのウインドウ２３が表示される。つまり、ウインドウ２３は論理画面バッファ２２の全部或いは一部を見るためのものであるとも言える。
【００１５】
また、マルチウインドウシステムでは、複数のアプリケーションを動作させることになるので（１つのアプリケーションで複数のウインドウを表示することもある）、それぞれに対して割り当てられたウインドウが図示の如く表示されることになる。また、ＯＳは、そ

れぞれのアプリケーション毎に割り当てたウインドウ単位に制御することになる。

【００１６】

図３は実施形態の端末上でテレビ会議用のプログラムを動作させた場合の構成概念図を示している。

【００１７】

図示の如く、画像入力装置３０、音声入出力装置３１、ネットワーク通信装置３２はハードウェア３３に接続されている。ハードウェア３３は画像入力装置３０、音声入出力装置３１、ネットワーク通信装置３２からの入力信号を検知するとハードウェア割り込みを生成する。次にこれら入力データはシステム（ＯＳもしくは各種デバイスを制御するデバイスドライバ）３４を通してテレビ会議システム３７、或いはカメラ制御サーバ３８に渡される。またカメラ制御サーバ３８は、カメラ制御記憶部３６に記憶されている、画像入力装置の撮影可能領域内のアクセス不可領域、及びアクセスコントロールレベル（ＡＣＬ）に従いカメラ制御管理部３５を制御し、カメラを管理する。カメラ制御サーバ３８は、このアクセスコントロールレベル、及びアクセス不可領域の値に応じて配送する画像、或いは音声データを決定する。このアクセスコントロールレベル（ＡＣＬ）を記述するアクセスコントロールリスト、及びアクセスコントロールデータの例を図１１に示す。

【００１８】

図示において、「Group List」は、本端末と接続される相手端末のネットワークのＩＰアドレス（複数を許容する）を、「Watch」は配送先のクライアントに映像データの配送をするかどうか（相手側で映像をみることができるか否か）、「Control」はパン、チルト、ズーム等の操作といったカメラ装置の制御を許可するか否か、「Security Area」は、撮影可能領域内に設定されたアクセス不可領域へのアクセスを許すかどうかと、不許可の場合にはそのアクセスコントロールデータへの格納先アドレスを、「Alert」は警告の種類（音声または映像による警告）を記憶している。

【００１９】

アクセスコントロールデータは、カメラ装置の最大移動範囲が値として格納されており、アクセスコントロールリストから参照される。このアクセスコントロールリスト、及びアクセス可能領域を示すアクセスコントロールデータは、カメラ制御サーバ上で設定・変更することが可能である。カメラ制御サーバ３８は、接続されている端末のアドレスを基にして、アクセスコントロールテーブルを参照し、「Security Area」がＮＧになっているものに対しては、画像入力装置の撮影可能領域内のアクセス不可領域へのカメラのアングルの要求があった場合にはそのアクセスを不許可にし、指定された「Alert」に従い警告情報をアクセス元の端末に向けて送信するよう指示することになる。なお、「Watch」で“NG”として設定された端末には、接続段階で警告情報を送信することになる。

【００２０】

なお、図示のアクセスコントロールデータ中、「Pan」はパン角を示し、「Tilt」はチルト角を示す。また、ズームは最大広角時での値である。従って、図示の場合には、最大広角時（ワイド端）で

abc≦パン角≦def　且つ、　ghi≦チルト角≦kim

の視野範囲（この場合は矩形範囲となる）を不許可範囲として設定されていることになる（図示のパン角における“-abc”の負号は不許可となる視野範囲の左側を意味するものであり、パン角が「-20°」という意味ではない。「＋」も同様である。

【００２１】

また、ズームをデフォルトで決めたのには理由があって、ワイド端とテレ端とではカメラの視野範囲が異なるからである。実施形態ではワイド端を規準にしているので、ズーム倍率を上げる（視野範囲を小さくする）と、そのズーム倍率に応じて上記不許可範囲を示すパン角、チルト角を微調整することになる。また、図示の矩形範囲を複数個設けることで、矩形範囲以外の領域を撮影不許可範囲として設定することもできるし、別な表現を用いることでその範囲を設定しても良い。

【００２２】

不許可範囲の設定は、カメラサーバとして動作するプログラムの中にあって、ユーザは自由に設定及び登録することが可能である。この際、撮影不許可範囲を設定するためには、自身に備えられたカメラを動作させ、その映像を見ながら行なえばよいであろう。

【００２３】

さて、実際に相手端末との接続を行なうと、テレビ会議システムは相手側のホストと接続した際に、アクセスレベルを設定する為の相手側のＩＰアドレスを参照する。このＩＰアドレスをもとにしてカメラ制御サーバに問い合わせを行い、カメラ制御サーバは、相手側のアクセスコントロールレベルとカメラ装置の最大移動可能範囲を設定し、結果をテレビ会議システムに返す。テレビ会議システムは、常時相手側からのカメラ制御を監視していて、ＩＰアドレスで決定された撮影不許可の範囲にアクセスしようとしていた場合には、それ以上のカメラアングルを無効にし、且つ、設定された形式の警告情報を作成して相手端末に向けて転送させる。

【００２４】

遠隔地からのアクセス不可領域へのアクセスに対する例を図４に、またその場合の動作処理内容を図５のフローチャートに示す。

【００２５】

今、遠隔地にあるホストＡから、遠隔操作可能なカメラをコントロールしている第三者がいる（ここでは、アクセスコントロールテーブルで「Wtach」が“OK”、「Contorol」が“OK”、そして、「Security Area」が“NG”（つまり、不許可範囲が有効に機能する）の場合である）。

【００２６】

この外部のホストＡはアクセスコントロールによりアクセス不可領域へのアクセス権を持たない。このとき、ホストＡの第三者がカメラを動かしてアクセス不可領域をアクセスすると、本テレビ会議システムはホストＡに向かって、アクセスコントロールテーブルに従って、通常の画像、或いは音声データとは別の警告画像メッセージ或いは警告音声メッセージをデータとして配信する。更に、カメラ制御サーバは、アクセス不可領域をアクセスしているカメラを所定の位置まで強制的に移動させる。

【００２７】

カメラ制御サーバの動作としては、最大移動可能範囲内にアクセス不可領域を含めて、アクセス不可領域へのアクセスがあった際に、警告メッセージを配信する上記例に限らず、最初からアクセス可能範囲内に最大移動可能範囲を設定しておく等、幾つかの方法が考えられる。

【００２８】

図５に従って説明すれば以下の通りである。

【００２９】

まず、ステップＳ１で、相手端末との接続を行なうと、ステップＳ２でＩＰアドレスを取得し、ステップＳ３で、そのＩＰアドレスに対応するアクセスコントロールテーブル（ＡＣＴ）内のデータを読み出す。

【００３０】

ステップＳ４に処理が進むと、そのユーザ（端末）がカメラの映像を見る権利を与えているか否かを判断し、否の場合には、ステップＳ５に進んでＡＣＴデータによって示されている形式の警告情報（実施形態では音声或いは映像）を送信し、ステップＳ６で接続断を行なう。

【００３１】

また、カメラの映像を見ることが許可されていると判断した場合には、ステップＳ７に進んで、カメラ製造送信を開始させ（これ以降、カメラで撮影された映像データは相手先に転送されることになる）、ステップＳ８のテレビ会議動作処理を行ない、それが終了したらステップＳ９で切断処理を行なう。

【００３２】

ステップＳ８のテレビ会議動作処理を、図６のフローチャートに従って説明する。

【００３３】
まず、ステップＳ１１では、相手先からのコマンドを受信するのを待つ。
【００３４】
受信したコマンドがテレビ会議の終了を意味すると判断した場合には、本処理を終了し、図５のステップＳ９の切断処理を行なう。
【００３５】
また、受信したコマンドがカメラ制御コマンド（カメラのパン角、チルト角及びズームに対する指示情報）であるか否かをステップＳ１３で判断し、カメラ制御コマンドではないと判断した場合には、ステップＳ１４に進み、対応する処理を行なう。
【００３６】
さて、カメラ制御コマンドであると判断した場合には、ステップＳ１５に進み、相手先が制御可能に設定されているかを、先に読出したＡＣＴデータに基づいて判断する。制御権を与えていないと判断した場合には、ステップＳ１６に進み、ＡＣＴデータで設定された形式の警告情報を送信し、ステップＳ１１に戻る。
【００３７】
また、カメラ制御権を与えていると判断した場合には、ステップＳ１７に進んで、その相手先に対して撮影不許可範囲を有効にするか否かをＡＣＴデータに基づいて判断する。
【００３８】
不許可データが有効であると判断した場合には、ステップＳ１８に進み、そのカメラ制御コマンドに対するカメラ制御を実行した場合に、不許可範囲に進入するかどうかを判断する。もし、不許可範囲に入ると判断した場合には、ステップＳ１９でその相手先にＡＣＴデータに基づく警告情報を送信し、ステップＳ２０でカメラを強制的に制御し、ステップＳ１１に戻る。
【００３９】
なお、カメラの強制制御についてであるが、例えば、最大ズーム倍率で撮影不許可範囲ぎりぎりの映像を転送しているときに、ズーム倍率を下げると、視野範囲が広くなり、結果的に不許可とされている映像の一部が撮影されてしまうからである。従って、このような場合を想定して、パン角及び／あるいはチルト角を調整する必要があるから設けた。
【００４０】
一方、不許可範囲を無効となっているユーザの場合、あるいは、そのカメラ制御コマンドを実行しても不許可範囲外にあると判断した場合には、その制御コマンドに従い、カメラの制御を行ない、ステップＳ１１に戻る。
【００４１】
以上説明したように本実施形態に従えば、接続相手毎にアクセスコントロールデータを設け、その中で許可された状態でのみカメラを制御でき、しかも、撮影不許可範囲に対してアクセスしようとした場合には、その旨の警告メッセージを送信することで、相手端末のユーザに注意を促すことが可能になる。
【００４２】
なお、実施形態では、テレビ会議システムを例にして説明したが、例えば、現在、注目されているインターネットにまで拡張し、例えば観光名所に設置したカメラサーバに対するアクセス時に機能するようにしてもよい。
【００４３】
特に、カメラを設置した場所付近に住居などがある場合も当然あるわけであるから、この問題は重要になるであろう。また、この場合、そのカメラの不許可範囲は、特定の特権を与えた者のみが変更できるようにした方が良いが、場合によっては設置する段階で設定したら外部から変更できないようにするようにした方が良いであろう。
【００４４】
なお、上記説明は、相手端末からのカメラ制御コマンドを受信した際の処理を説明したが、それは相手端末側としても同様である。また、相手端末のカメラのアングル（パン角、チルト角、ズーム）を変更する場合は、例えば画面にそれらのアングルを変更するための

各種ボタンを表示し、それをポインティングデバイス等で指示することで行なえばよい。

【００４５】

＜第２の実施形態＞

上記実施形態（第１の実施形態）は、カメラ制御サーバが動作するハードウェアに接続された、１台の画像入力装置のアクセスコントロールレベルを制御する例を説明した。本第２の実施形態では、同じハードウェアに接続された複数台の画像入力装置や同一ネットワーク内に接続されている他の画像入力装置をもアクセスコントロールの対象として制御を行うものである。

【００４６】

この場合、図７のようにカメラ・リストに設定されている１台のカメラ毎にアクセス・コントロール・テーブルを管理する。制御対象となるカメラが複数になるので、各々のカメラにはそれぞれＩＰアドレスを負荷し、それぞれに対するアクセスコントロールテーブルを設けるのである。このカメラ・リストは図８のように、カメラ管理部が管理を行う。

【００４７】

また、第１の実施形態では、図９、図１０における実際のアクセス可能領域にのみアクセス可能な制御方法を試みているが、論理的なアクセス可能域を全てアクセス可能にする、といったことも考えられる。更に、第１の実施形態では、アクセス不許可範囲をカメラの視野内に入るように制御したときに、その制御を無効にし、場合によってはカメラをその視野範囲からはずれるように強制制御させた。しかし、図１０に示す如く、アクセス不許可範囲でカメラの潜在視野範囲が分断される場合には、その不許可範囲を飛び越した許可範囲に一気にカメラアングルを制御しても良い。この場合には、アングルの変更方向に従って飛び越す方向を検出すれば良いであろう。また、図１０に示す実際に右側のアクセス可能領域ではズーム倍率が最大の場合でないとアクセス不許可範囲を含んでしまう場合も当然あるであろうから、その場合には指示コマンドにかかわらず、視野範囲に不許可範囲が入らない倍率になるよう制御してもよい。勿論、最大倍率でも、論理的なアクセス可能領域があったとしても、最大ズームで撮影した際に不許可範囲が入ってしまう場合には、たとえ論理的に許可されていようが、その範囲を不許可範囲として扱うことも必要である。

【００４８】

また、第１の実施形態ではアクセスの対象は画像のみであったが、会議スペースの側に本システムがある場合には、音声データに関しても何らかの制御を行うといったことも考えられる。例えば、指向範囲が固定のマイクロホンをカメラに搭載した場合にあっては、マイクロホンの指向範囲とカメラの視野範囲は異なる（ズームで可変）ので、それぞれ別々に制御することが必要になる。

【００４９】

なお、実施形態での端末装置の構成は格別特殊な装置でなければならないというわけではなく、制御可能なカメラ、マイク、スピーカを搭載した、例えばパーソナルコンピュータやワークステーションに上記実施形態で説明した処理を実現するためのプログラムを動作させても実現可能である。

【００５０】

従って、本発明は、複数の機器（例えばホストコンピュータ、カメラ、マイク、スピーカ等）から構成されるシステムに適用しても、一つの機器からなる装置に適用してもよい。

【００５１】

また、本発明の目的は、前述した実施形態の機能を実現するソフトウェアのプログラムコードを記録した記憶媒体を、システムあるいは装置に供給し、そのシステムあるいは装置のコンピュータ（またはＣＰＵやＭＰＵ）が記憶媒体に格納されたプログラムコードを読出し実行することによっても、達成されることは言うまでもない。

【００５２】

この場合、記憶媒体から読出されたプログラムコード自体が前述した実施形態の機能を実現することになり、そのプログラムコードを記憶した記憶媒体は本発明を構成することに

なる。

【００５３】

プログラムコードを供給するための記憶媒体としては、例えば、フロッピディスク，ハードディスク，光ディスク，光磁気ディスク，ＣＤ－ＲＯＭ，ＣＤ－Ｒ，磁気テープ，不揮発性のメモリカード，ＲＯＭなどを用いることができる。

【００５４】

また、コンピュータが読出したプログラムコードを実行することにより、前述した実施形態の機能が実現されるだけでなく、そのプログラムコードの指示に基づき、コンピュータ上で稼働しているＯＳ（オペレーティングシステム）などが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【００５５】

さらに、記憶媒体から読出されたプログラムコードが、コンピュータに挿入された機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに書込まれた後、そのプログラムコードの指示に基づき、その機能拡張ボードや機能拡張ユニットに備わるＣＰＵなどが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【００５６】

【発明の効果】

以上説明したように本発明によれば、撮影不許可範囲を設け、この不許可範囲に対するアクセスを禁止すると共に、その端末に対して警告してプライバシー保護、及び守秘義務を果たすことが可能になる。

【００５７】

【図面の簡単な説明】

【図１】実施形態におけるカメラ会議システムの端末装置の構成を示す図である。

【図２】マルチウィンドウシステムの特徴を表す概念図である。

【図３】実施形態の端末がテレビ会議システムの１端末として動作する場合の装置の概念構成を示す図である。

【図４】端末どうしのテレビ会議システムにおける警告情報発生時の動作を説明するための図である。

【図５】実施形態における動作処理手順を示すフローチャートである。

【図６】図６におけるステップＳ８の動作処理内容を示すフローチャートである。

【図７】第２の実施形態におけるアクセスコントロールテーブルの構成を示す図である。

【図８】第２の実施形態におけるカメラ制御サーバのレイヤ構成を示す図である。

【図９】実施形態のカメラ動作の説明するための図である。

【図１０】実施形態のカメラ動作の説明するための図である。

【図１１】第１の実施形態におけるアクセスコントロールテーブルの内容を示す図である。

【符号の説明】

３１　画像入力装置

３２　ネットワーク通信装置

３３　ハードウェア

３４　システム

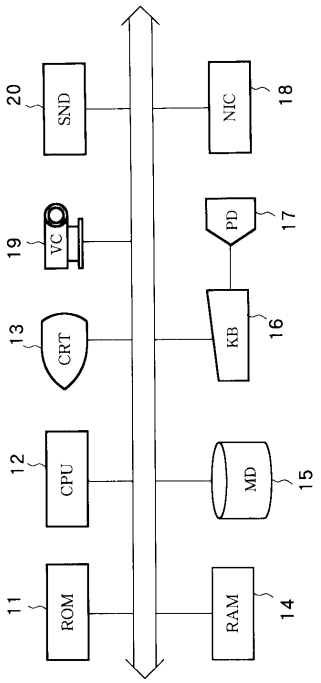
３５　カメラ制御管理部

３６　カメラ制御記憶部

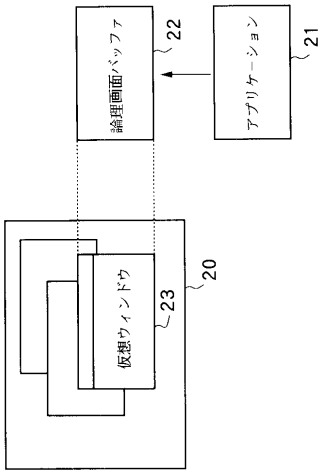
３７　テレビ会議システム

３８　カメラ制御サーバ

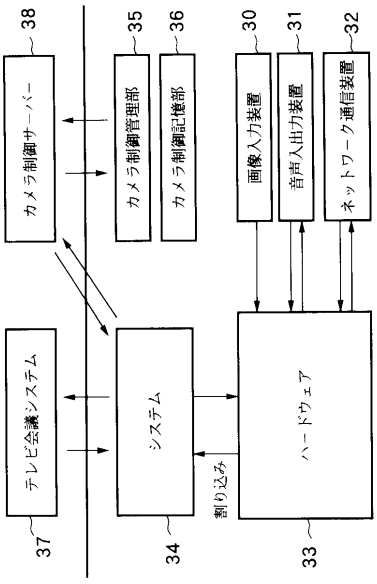
【図１】


20
SND
NIC
18
19
VC
PD
17
13
CRT
KB
16
12
CPU
MD
15
11
ROM
RAM
14

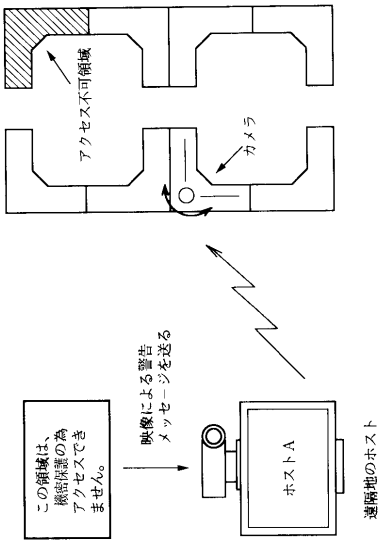
【図２】


論理画面バッファ
22
アプリケーション
21
仮想ウィンドウ
23
20

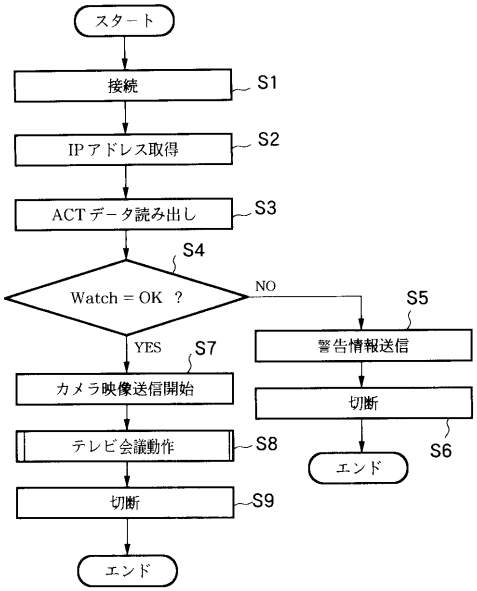
【図３】


38
35
36
30
31
32
カメラ制御サーバー
カメラ制御管理部
カメラ制御記憶部
画像入力装置
音声入出力装置
ネットワーク通信装置
テレビ会議システム
システム
割り込み
ハードウェア
37
34
33

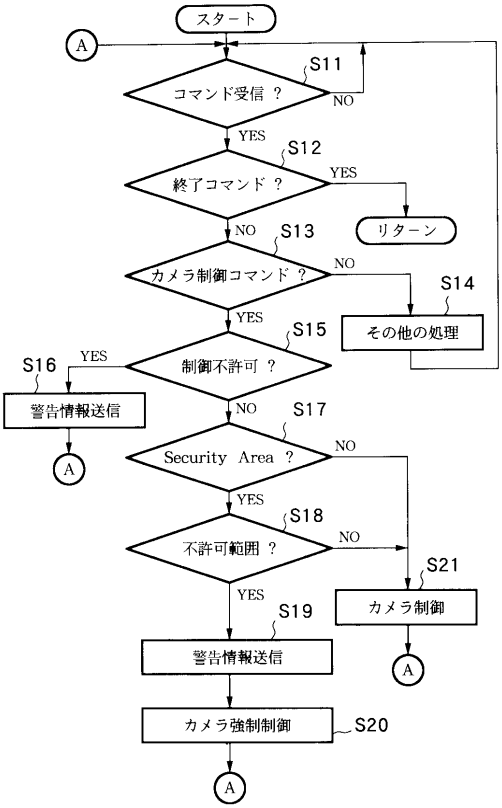
【図４】


アクセス不可領域
カメラ
この領域は、機密保護の為アクセスできません。
映像による警告メッセージを送る
ホストA
遠隔地のホスト

【図５】



【図６】



【図７】

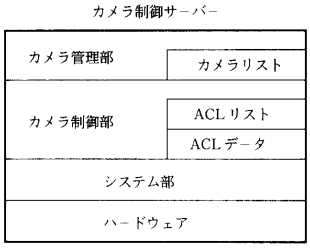
アクセス・コントロール・テーブル (Camera－1)

Group List	Watch	Control	Security Area	Alert
aaa, bbb, ccc, XXX	OK	OK	OK	....
aaa, bbb, XXX, XXX	OK	OK	NG	....
aaa, XXX, XXX, XXX	OK	NG	NG	....
XXX, XXX, XXX, XXX	NG	NG	NG	Sound

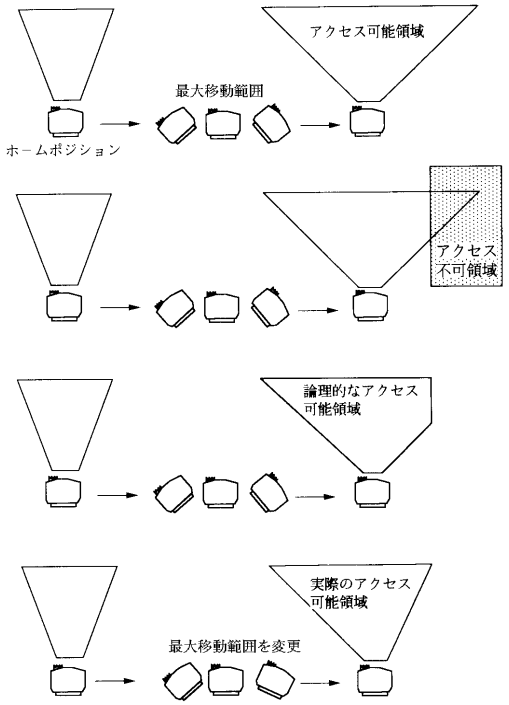
カメラ・リスト

Camera	Host－ID	Owner	Access Control
Camera－1	aaa, bbb, ccc, 101	Owner－A	Yes
Camera－2	aaa, bbb, ccc, 102	Owner－B	Yes
Camera－3	aaa, bbb, ccc, 103	Owner－C	No
Camera－4	aaa, bbb, ccc, 104	Owner－D	Yes
Camera－5	aaa, bbb, ccc, 105	Owner－E	No

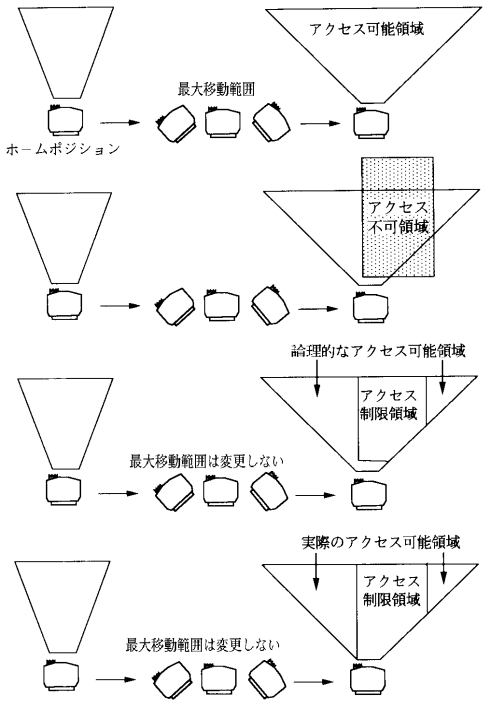
【図８】



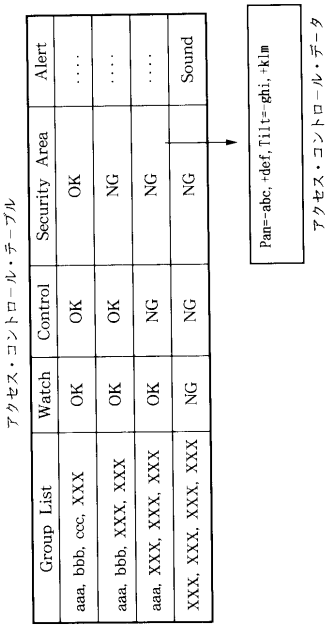
【図９】


アクセス可能領域
最大移動範囲
ホームポジション
アクセス
不可領域
論理的なアクセス
可能領域
実際のアクセス
可能領域
最大移動範囲を変更

【図１０】


アクセス可能領域
最大移動範囲
ホームポジション
アクセス
不可領域
論理的なアクセス可能領域
アクセス
制限領域
最大移動範囲は変更しない
実際のアクセス可能領域
アクセス
制限領域
最大移動範囲は変更しない

【図１１】


アクセス・コントロール・テーブル
Group List
Watch
Control
Security Area
Alert
aaa, bbb, ccc, XXX
OK
OK
OK
....
aaa, bbb, XXX, XXX
OK
OK
NG
....
aaa, XXX, XXX, XXX
OK
NG
NG
....
XXX, XXX, XXX, XXX
NG
NG
NG
Sound
Pan=abc, +def, Tilt=ghi, +klm
アクセス・コントロール・データ

フロントページの続き

(58)調査した分野(Int.Cl., ＤＢ名)
H04N 5/222～5/257