(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3634528号
(P3634528)
(45)発行日　平成17年3月30日(2005.3.30)　(24)登録日　平成17年1月7日(2005.1.7)

(51)Int.Cl.[7]　F I
H04N　5/232　H04N　5/232　B

請求項の数 14　(全 16 頁)

(21)出願番号　特願平8-320557
(22)出願日　平成8年11月29日(1996.11.29)
(65)公開番号　特開平10-161213
(43)公開日　平成10年6月19日(1998.6.19)
審査請求日　平成13年12月3日(2001.12.3)

(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　河合　智明
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
(72)発明者　矢野　晃一
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

最終頁に続く

(54)【発明の名称】カメラサーバ及びカメラクライアント及び制御方法及びシステム及び記憶媒体

(57)【特許請求の範囲】
【請求項１】
少なくとも撮像方向が変更可能な撮像装置を有し、接続している１つ或いは複数のクライアントに、前記撮像装置で撮像された映像データを転送するカメラサーバであって、
クライアントの属するグループと、当該グループ毎に決められた撮像許可範囲に基づく制御制限情報を記憶する記憶手段と、
接続されたクライアントの中の、前記撮像装置の制御権を有している第１クライアントがどのグループに属しているかを判断する判断手段と、
制御権を有する前記第１クライアントから前記撮像装置に対する制御要求があった場合、前記判断手段の判断結果に基づく制御制限情報に従って前記撮像装置の制御を行なう制御手段と、
前記第１クライアントと前記制御権を有していない第２クライアントに前記映像データを並列に転送する際に、前記第１クライアントによる撮像要求範囲が前記第２クライアントの撮像不許可範囲を含む場合は、前記第１クライアントには前記撮像要求範囲の映像データを転送し、前記第２クライアントには前記撮像不許可範囲に所定の処理を施した前記撮像要求範囲の映像データを転送する転送手段と
を備えることを特徴とするカメラサーバ。
【請求項２】
前記制御制限情報には、前記撮像装置のパン可能範囲、チルト可能範囲、及びズーム可能範囲が含まれることを特徴とする請求項第１項に記載のカメラサーバ。

【請求項３】
前記ズーム可能範囲は、撮像装置の視点方向によって変動することを特徴とする請求項第２項に記載のカメラサーバ。
【請求項４】
前記転送手段は、前記第２のクライアントには、前記撮像不許可範囲の撮像映像に対して解像度を下げる処理をした前記撮像要求範囲の映像データを転送することを特徴とする請求項第１乃至３項のいずれか１項に記載のカメラサーバ。
【請求項５】
前記転送手段は、前記第２クライアントには前記撮像不許可範囲の撮像映像をマスキングした前記撮像要求範囲の映像データを転送することを特徴とする請求項第１乃至３項のいずれか１つに記載のカメラサーバ。
【請求項６】
前記転送手段は、前記第２クライアントには前記撮像不許可範囲の撮像映像をぼかし処理した前記撮像要求範囲の映像データを転送することを特徴とする請求項第１乃至３項のいずれか１つに記載のカメラサーバ。
【請求項７】
前記第１クライアントは前記撮像許可範囲に制限のないクライアントであり、前記第２クライアントは所定の撮像範囲においてのみ撮像許可されるクライアントであることを特徴とする請求項第１乃至６項のいずれか１つに記載のカメラサーバ。
【請求項８】
少なくとも撮像方向が変更可能な撮像装置を有し、接続している１つ或いは複数のクライアントに、前記撮像装置で撮像された映像データを転送するカメラサーバの制御方法であって、
予めクライアントの属するグループと、当該グループ毎に決められた撮像許可範囲に基づく制御制限情報を記憶している記憶手段を参照して、接続しているクライアントの中の、前記撮像装置の制御権を有している第１クライアントがどのグループに属しているかを判断する判断工程と、
制御権を有する前記第１クライアントから前記撮像装置に対する制御要求があった場合、前記判断工程の判断結果に基づく制御制限情報に従って前記撮像装置の制御を行なう制御工程と、
前記第１クライアントと前記制御権を有していない第２クライアントに前記映像データを並列に転送する際に、前記第１クライアントによる撮像要求範囲が前記第２クライアントの撮像不許可範囲を含む場合は、前記第１クライアントには前記撮像要求範囲の映像データを転送し、前記第２クライアントには前記撮像不許可範囲に所定の処理を施した前記撮像要求範囲の映像データを転送する転送工程と
を備えることを特徴とするカメラサーバの制御方法。
【請求項９】
前記制御制限情報には、前記撮像装置のパン可能範囲、チルト可能範囲、及びズーム可能範囲が含まれることを特徴とする請求項第８項に記載のカメラサーバの制御方法。
【請求項１０】
前記ズーム可能範囲は、撮像装置の視点方向によって変動することを特徴とする請求項第９項に記載のカメラサーバの制御方法。
【請求項１１】
前記転送工程は、前記第２のクライアントには、前記撮像不許可範囲の撮像映像に対して解像度を下げる処理をした前記撮像要求範囲の映像データを転送することを特徴とする請求項第８乃至１０項のいずれか１項に記載のカメラサーバの制御方法。
【請求項１２】
前記転送工程は、前記第２クライアントには前記撮像不許可範囲の撮像映像をマスキングした前記撮像要求範囲の映像データを転送することを特徴とする請求項第８乃至１０項のいずれか１つに記載のカメラサーバの制御方法。

【請求項１３】
前記転送工程は、前記第２クライアントには前記撮像不許可範囲の撮像映像をぼかし処理した前記撮像要求範囲の映像データを転送することを特徴とする請求項第８乃至１０項のいずれか１つに記載のカメラサーバの制御方法。
【請求項１４】
前記第１クライアントは前記撮像許可範囲に制限のないクライアントであり、前記第２クライアントは所定の撮像範囲においてのみ撮像許可されるクライアントであることを特徴とする請求項８乃至１３のいずれか１つに記載のカメラサーバの制御方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明はカメラサーバ及びカメラクライアント及び制御方法及び記憶媒体及びシステムに関するものである。
【０００２】
【従来の技術】
本願出願人は、ビデオカメラの映像を遠隔地の多地点で観察できるシステム、より詳しくは、単にカメラ映像を観察するだけでなく遠隔からカメラのパン・チルト角度やズーム倍率を遠隔制御可能にした技術を提案した。例えば、インターネット上のＷＷＷ（Ｗｏｒｌｄ　Ｗｉｄｅ　Ｗｅｂ）上に、カメラを制御する装置（カメラサーバ）を接続し、遠隔の不特定多数の装置（クライアント）からカメラで撮影したリアルタイム映像をアクセス者に配送するだけでなく、そのうちの１つのクライアント装置では、そのカメラの制御（パン、チルト、ズーム）をも許可するシステムである。
【０００３】
【発明が解決しようとする課題】
ところで、配送映像に対して複数のクライアントが同時アクセスできる状況において、特定の人からの映像へのアクセスを拒否したい場合がある。カメラが制御可能である場合には、ある範囲は見せても良いが、ある範囲は見せたくない場合も当然有り得る。またその範囲に関しても、人、グループに応じてそれぞれ異なることもあるだろう。例えばグループＡに属する人には、パン角度Ｘ～Ｙの間は見せたくないが、グループＢに属する人には見られても構わない場合等である。
【０００４】
【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成されたものであり、クライアントを複数のグループ毎に管理し、それぞれのグループに属するクライアントに対してはそのグループの制限範囲内でカメラを制御を行なわせることを可能にするカメラサーバを提供しようとするものである。
【０００６】
上記発明を実現するため、例えばカメラサーバは以下の構成を備える。すなわち、
少なくとも撮像方向が変更可能な撮像装置を有し、接続している１つ或いは複数のクライアントに、前記撮像装置で撮像された映像データを転送するカメラサーバであって、
クライアントの属するグループと、当該グループ毎に決められた撮像許可範囲に基づく制御制限情報を記憶する記憶手段と、
接続されたクライアントの中の、前記撮像装置の制御権を有している第１クライアントがどのグループに属しているかを判断する判断手段と、
制御権を有する前記第１クライアントから前記撮像装置に対する制御要求があった場合、前記判断手段の判断結果に基づく制御制限情報に従って前記撮像装置の制御を行なう制御手段と、
前記第１クライアントと前記制御権を有していない第２クライアントに前記映像データを並列に転送する際に、前記第１クライアントによる撮像要求範囲が前記第２クライアントの撮像不許可範囲を含む場合は、前記第１クライアントには前記撮像要求範囲の映像デー

タを転送し、前記第２クライアントには前記撮像不許可範囲に所定の処理を施した前記撮像要求範囲の映像データを転送する転送手段とを備える。

【０００７】

【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を詳細に説明する。

【０００８】

先ず、本発明にかかる実施形態の概要を説明すると、本実施形態では、カメラ制御サーバに接続されたカメラからの映像を、ネットワークを介してカメラクライアントから眺める際に、カメラ映像をアクセスしているメンバーに応じて、カメラ制御可能範囲を動的に変更しようとするものである。

【０００９】

図１は本実施形態のシステムのブロック構成図を示している。図示で、１－１はカメラサーバ装置であり、１－２，１－３，１－４、…はカメラクライアント装置になっている。尚、以下ではカメラサーバ装置を単にカメラサーバ、カメラクライアント装置を単にカメラクライアントという。

【００１０】

カメラサーバ１－１ではビデオカメラからの映像を取り込みカメラクライアントへの配送を行うと共に、カメラクライアントからのカメラ制御指令を受け付けカメラを撮影状態（パン、チルト、ズーム等）を制御する機能を持つ。カメラクライアント装置の数は特に制限はないが、本実施形態では、図示の通り３つとする。カメラクライアント１－２，１－３，１－４では、カメラサーバ１－１からの映像配送を要求し映像を見ると共に、カメラ制御要求をカメラサーバ１－１に対して転送する。カメラサーバ１－１はこの要求に応じて、１つのカメラクライアントに対してのみ制御権を与え、他のカメラクライアントに対しては単に撮影された映像を転送する。すなわち、カメラ制御権は排他制御されている。

【００１１】

さて、カメラサーバ１－１の構成は以下のようになっている。

【００１２】

１－１１は固体撮像素子を有するビデオカメラで、撮影倍率（ズーム）を変化自在になっており、所定の雲台を有している。１－１２はビデオカメラ１－１１のズーム、雲台の水平方向の回動（パン）及び上下方向の回動（チルト）の駆動制御信号を供給するカメラ制御部である。１－１３はビデオカメラ１－１１より撮影された映像を取り込むビデオキャプチャ部であり、ビデオカメラ１－１１からの映像ＮＴＳＣ信号を取り込みＡ／Ｄ変換後、ＭｏｔｉｏｎＪＰＥＧ圧縮し出力する。なお、ここでは映像の圧縮形式として、ＭｏｔｉｏｎＪＰＥＧ圧縮としたが、本実施形態として圧縮形式にこだわるものではない。

【００１３】

１－１４は、本カメラサーバ１－１がネットワーク１－０と接続するためのネットワークインタフェースである。１－１６はカメラサーバ１－１全体の制御を行なうＣＰＵであって、２次記憶装置１－１７より主記憶メモリ１－１５に読み込まれたＯＳ，カメラ制御プログラムに従って制御動作する。主記憶メモリ１－１５は、上記のようなプログラムの格納領域とＣＰＵ１－１６のワークエリアとしても使用されるが、図示の如く、識別子バッファ１－１３１、許可テーブル１－１３２、制御範囲テーブル１－１３３、転送先テーブル１－１３４を有する。これらの各領域に相当する部分は、２次記憶装置１－１７にファイルとして記憶されているものであり、起動時に主記憶メモリ１－１５にロードされる。但し、ＲＡＭ１－１５がバックアップ電源によって常時電力の供給を受けている場合には、必ずしも２次記憶装置１－１７にファイルとして格納されている必要はない。

【００１４】

さて、上記構成において、ＣＰＵ１－１６はビデオキャプチャ部１－１３から出力された圧縮映像データをネットワークインタフェース１－１４を介して、カメラクライアントとして接続されている装置に向けて転送する。一方、制御権が与えられているカメラクライアントからカメラ制御指示要求があると、それを受取、カメラ制御部１－１２に対して指

示された内容に従ってズーム、パン、チルトを制御する。

【００１５】

なお、カメラサーバ１－１からカメラクライアントへの映像データの伝送フレームレートであるが、これはネットワーク１－０の形態（例えばイーサネットや回旋を介してのネットワーク等の違い）、及び、そのネットワークの混雑の具合によって変動する。

【００１６】

次に、カメラクライアントについて説明する。カメラクライアント１－３，１－４の構成及び動作は、いずれもカメラクライアント１－２と実質的に同じであるので、ここではカメラクライアント１－２についてのみ説明する。

【００１７】

カメラサーバ１－１から配送されてきた圧縮映像データは、ネットワークインターフェース１－２４を通じて受信され、ＣＰＵ１－２２により伸長され、ビットマップディスプレイ１－２１上に表示される。なお、ビットマップディスプレイ１－２１上には図２のようなユーザインターフェース画面が表示されているものとする。ここで映像は映像ウィンドウ２－１に表示されることになる。なお、カメラクライアント装置１－２上では、ウィンドウシステム（例えばマイクロソフト社のＭＳ－Ｗｉｎｄｏｗｓ）が稼働して、図２のような画面を構成できるアプリケーションプログラムが動作しているものとする（図２についての詳細については後述する）。

【００１８】

従って、カメラクライアント装置１－２における２次記憶装置１－２６にはウィンドウシステム（ＯＳ）をはじめとする、カメラクライアントとして稼働するアプリケーションプログラムが記憶されている。なお、１－２２はカメラクライアント装置１－２３の全体の制御を司るＣＰＵ、１－２３はＣＰＵ１－２２が処理するＯＳやカメラクライアントアプリケーションを展開する主記憶装置、１－２１はビットマップディスプレイ、１－２５はキーボードやポインティングデバイスの入力装置である。

【００１９】

図３は、本実施形態のプロセス構成図である。ここでプロセスとはＵＮＩＸ等のマルチタスクオペレーティングシステムのプロセスを意味する。カメラクライアント１－２上には、映像表示プロセス３－２１とカメラ制御プロセス３－２２が動作している。これらはＣＰＵ１－２２によるプログラム実行によって実現している。また、カメラサーバ１－１には映像送信サーバプロセス３－１１、およびカメラ制御サーバプロセス３－１２が動作している。これもカメラサーバ１－１のＣＰＵ１－１６でもって実現している。

【００２０】

映像送信サーバプロセス３－１１は映像の取り込み、圧縮、配送の制御を行っている。映像表示プロセス３－２１は映像送信サーバプロセス３－１１によって配送されてくる圧縮映像のネットワークからの取り込み、伸長、ビットマップディスプレイ１－２１への映像表示への制御を行なう。

【００２１】

また、カメラ制御サーバプロセス３－１２は、カメラクライアントで動作しているカメラ制御プロセス３－２２から発行されるカメラ制御命令を受け取り、実際にカメラ制御部１－１２を制御することでカメラ制御を行う。カメラ制御プロセス３－２２は、図２に示すカメラ制御ウィンドウ２－２をディスプレイ１－２１上に表示させ、ユーザからの各種カメラ操作のためのユーザインターフェースを提供する。例えば、図示のボタン２－２６ａ、２ー２６ｃのいずれかにポインティングデバイスに連動して表示するカーソルを位置させ、ポインティングデバイスに設けられたボタンを押下する操作（以下、この操作をクリックする、という）を行なうことで、カメラサーバ１－１に対してカメラのチルト角を制御する。また、ボタン２－２６ｂ，２ー２６ｄはパン角を制御する。

【００２２】

なお、パン角、及びチルト角の制御は、上記のボタン以外にも、例えばスクロールバー２－２１、２－２２にあるツマミ２－２１１ａ、２－２２ａを操作することでも実現する。

例えば、カーソルをいずれかのツマミの位置に移動させた後、ポインティングデバイスに設けられたボタンを押しながら上下、或いは左右に移動させることでチルト角、パン角を制御する（一般に、ボタンを押しながらカーソルを移動させる操作は“ドラッグ”として知られている）。換言すれば、ツマミ２－２１ａ、２－２２ａの位置は、カメラサーバ１－１のビデオカメラのアングルを変えたときの潜在的に撮影可能な範囲における現在のアングル位置を示していることになる。

【００２３】

また、スクロールバー２－２３はズームを制御するためのものであり、スクロールバー２－２１，２－２２等と同様に、ツマミ２－２３ａをドラッグ操作することで倍率を制御できるし、今現在の倍率を知ることができる。なお、ツマミ２－２３ａの位置は上にあればあるほど倍率が下がり（視野角は大きくなり）、下に位置するほど倍率は上がる（視野角は小さくなる）。

【００２４】

そして、２－２４は制御権を要求するためのボタン、２－２５は制御権を放棄するためのボタンであり、いずれもクリックすることで動作する。

【００２５】

さて、上記のようにして、パン角、チルト角及びズームを制御できるわけであるが、これらの操作が可能になるのはカメラサーバ１－１より制御権が与えられている場合であって、与えられていない場合には上記ボタン、或いはスクロールバーは表示されるものの、操作できない。但し、他のカメラクライアントが制御権を持っていて、そのカメラ制御に関する情報（パン角、チルト角、及びズーム値（ズーム倍率を示す値））は映像データと共に転送されてくるので、その情報に基づいて各スクロールバーのツマミ位置はその都度動作して見える。

【００２６】

カメラ制御権を設定するのは、先に説明したようにカメラサーバ１－１側で行なう。そのため、カメラサーバ１－１におけるカメラ制御サーバプロセス３－１２（カメラサーバのＣＰＵ１－１６が実行するプログラム）では制御権を有する者だけが操作可能となるよう排他制御を行う。

【００２７】

以下、カメラサーバ１－１におけるカメラ制御サーバプロセス３－１２の内容を図４のフローチャートに従って説明する。

【００２８】

先ず、ステップＳ４０２において初期化処理を行なう。この初期化処理には、例えばパン角、チルト角、ズーム値を所定値に設定してカメラのアングルを所定の方向に向け、ズーム率を初期化する処理を含んでいる。

【００２９】

次に、ステップＳ４０３でイベントを待つ。イベントとしては、カメラクライアントからの要求の有無等である。この要求には、先に説明した制御権獲得、制御権放棄、更にはカメラアングルの変更（パン角、チルト角、ズーム値の変更）が含まれる。

【００３０】

イベントの発生を検知すると、次にステップＳ４０４に進んで、認証処理を行ない、正規ユーザであるか否かを判断する。この判断は、主記憶メモリ１－１５内の許可テーブル１－１３２を参照して判断する。許可テーブル１－１３２は、例えば図６のような構造になっている。図示の左欄はネットワーク上のユーザ名、右側は特権レベルである。特権レベルはその数値が小さいほど高く、大きいほど低い。

【００３１】

さて、ステップＳ４０４では、受信した要求コマンドに付随するユーザ名がこの許可テーブル１－１３２に登録されているか否かを判断する。許可されていると判断した場合には、当該要求が接続要求である場合には、当該クライアントに対して撮影映像を転送することになるので、送信先テーブル１－１３４に接続ユーザとして登録する。図７は、この送

信先テーブル１－１３４の内容を示している。図示の場合には、３人（３つのカメラクライアント）がこのカメラサーバ１－１に接続されていることを示している。また、ユーザ“Ｓｕｚｕｋｉ”が制御権を有していることを示している。

【００３２】

さて、ステップＳ４０４で認証ができた場合には、要求内容に応じた処理を行なうことになる。

【００３３】

先ず、カメラ制御権の獲得要求であると判断した場合には、ステップＳ４０５からステップＳ４１０に進み、主記憶メモリ１－１５内の予め確保されたカメラ使用中フラグがＯＮになっているか否かを判断する。なお、このフラグはそのときにカメラの制御権を得ているクライアントがあるか否かを示すものであり、ＯＮの場合には存在し、ＯＦＦの場合には存在しないことを示す。

【００３４】

ステップＳ４１０でカメラ使用中フラグがＯＮになっていた場合には、少なくとも他のクライアントが既に制御権を得て操作していることになるので、制御権獲得要求には応えられないので、ステップＳ４０３に戻る。また、そのフラグがＯＦＦの場合には、ステップＳ４１１に進んで、カメラ使用中フラグをＯＮにし、主記憶メモリ１－１５中の識別子バッファ１－１３１に制御権獲得の要求元のユーザ名を格納する。

【００３５】

また、要求内容がパン角、チルト角、ズーム値（以下、これらを総称してアングルという）の変更指示命令であると判断した場合には、ステップＳ４０６からステップＳ４１３に進み、そのクライアントが制御権を得ているユーザであるか否かを判断する。制御権を得ているユーザ名は、識別子バッファ１－１３１に格納されているので、その照合を行なえば判明する。制御権を与えられていないクライアントからのものである場合には、カメラ制御は不可なので、そのままステップＳ４０３に戻る。

【００３６】

一方、制御権を得ているクライアントであると判明したら、処理はステップＳ４１４に進み、当該クライアントの登録されている特権レベルを許可テーブル１－１３２を参照することで判断する（許可テーブル１－１３２を参照すると、そのときの制御権を有するクライアントがどの特権レベルを有しているのか判断できる）。

【００３７】

特権レベルが“１”のクライアントであると判断した場合には、アングルに制限がないと判断し、ステップＳ４１６に進んで、指示されたアングル（パン角、チルト角、ズーム値）に従ってカメラを制御する。

【００３８】

一方、特権レベルが“２”以上の場合には、カメラの潜在的な視野範囲（最広角状態でパン、チルトを行なったときの視野）内でのアングルに制限が設けられているものと判断し、ステップＳ４１５に進んで、要求されたアングルが許容範囲を越える場合には、要求されたアングルを変更する処理を行ない、ステップＳ４１５の処理を行なう。

【００３９】

特権レベル（“２”以上）と許容されたアングル情報との関係を示す情報は、主記憶メモリ１－１５内の制限範囲テーブル１－１３３に格納されている。

【００４０】

実施形態の場合、特権レベルは１～３であり、そのうち、特権レベル“１”のユーザに対してはフルアクセス可能となっているので、このテーブル１－１３３には、特権レベル“２”、“３”の２つの制限範囲情報が格納されている。

【００４１】

図８を用いて詳しく説明する。図示は、例えば特権レベル“２”の制限範囲を示す情報の概要を示している。図中、８０はカメラサーバ１－１のビデオカメラのズーム値を“１”にして、パン角、チルト角を変化させた場合の撮影できる視野範囲（潜在的な視野範囲）

を示している。説明が前後するが、本実施形態のビデオカメラ１－１１は、ズーム値として１（最大視野角＝最低倍率）～１０（最低視野角＝最大倍率）の１０段階で制御できるものである。

【００４２】

図の説明に戻る。８２は特権レベル“２”におけるカメラの視野中心の取り得る最大範囲を示しており、８３はズーム値“１”において左上隅をカメラを向けた際の実撮影視野範囲を示している。従って、８４は特権レベル“２”における見ることができる潜在的な視野範囲となる。換言すれば、特権レベル“２”のクライアントが制御権を獲得したとしても、図示の領域８１を視野範囲に納めることができない。

【００４３】

実際に、制限範囲テーブル１－１３３には、図示の境界８４の座標位置を記憶しておくことになる。実撮影視野範囲８３の大きさは、ズーム値が大きければ大きいほど小さくなるからである。換言すれば、ズーム値に従って図示の枠８２の大きさは変動することになる。

【００４４】

なお、特権レベル“３”のクライアントの場合には、図８における枠８４の大きさが更に小さくなっていると考えて良い。

【００４５】

ところで、「もの」を良く見ようとすると、人間の心理ではその対象物を拡大して見ようとするだろう。図８の場合には、領域８１については積極的にカメラを向けることはできないものの、領域８１の境界付近では拡大して見えてしまうことになる。また、積極的に見せたくない領域は、図示のように必ずしも垂直線や水平線で区切ることが難しいこともあるだろう。かといって、確実性を重視するために、むやみに枠８４を小さくすると、ユーザに不満を与えかねない。そこで、本実施形態では、ズーム値についても視点位置に応じて、その許容範囲を設けた。

【００４６】

先の説明によれば、積極的に見てもらって構わない部分は、領域８２の中心付近であって、この付近ではカメラが備えるズーム値をその可動範囲で自由に変化させてもらって構わない。ところが、視野端では、本来見せたくはない領域に近づくわけであるから、倍率は大きくはできないようにすることが望ましい。

【００４７】

そこで、図８に示す如く、ビデオカメラの中心位置に応じてズーム値の取り得る範囲を規定する枠を決め、それぞれの枠で規定された領域８７、８８及び８９のように許容されるズーム値の範囲を設定した。

【００４８】

このようにすると、結局のところ、撮影可能な視野端に近づけば近づくほど、操作可能な最大ズーム値が徐々に小さくなり、極端に拡大できないように制御できる。先にステップＳ４１５におけるカメラ制御命令変更処理では、このズーム値の変更をも行なっているわけである。

【００４９】

以上のように、ユーザの特権レベル毎に管理、換言すれば、ユーザを階層的に管理することでし、カメラ制御にかかる許容範囲をそれぞれの階層別に異なるようにすることが可能になる。

【００５０】

先の図２のスクロールバー２－２１、２－２２及び２－２３におけるそれぞれの黒い部分はそれぞれのツマミがその黒い部分には移動できないことを示していることが、上記の説明で理解できよう。

【００５１】

図４のフローチャートに戻って説明を続ける。

【００５２】

クライアントからの要求が、カメラ制御権を有していたクライアントからの制御権開放の要求であった場合には、ステップＳ４０７からステップＳ４１７に進み、カメラ使用中フラグをＯＦＦにし、ステップＳ４０３に進む。識別子バッファ１－１３１の内容も消去しても構わないが、カメラ使用中フラグがＯＦＦになれば、識別子バッファは無意味になるので、消去処理は省いた。

【００５３】

そして、制限範囲テーブル１－１３３の変更命令を受けた場合には、ステップＳ４１９に進み、その要求がアクセス権設定プロセス３－１３からの要求である場合に、ステップＳ４２０に進んで、制限範囲テーブル１－１３３の内容を更新する（ステップＳ４２０）。

【００５４】

この制限範囲テーブル１－１３３の変更は、カメラサーバ１－１の不図示の操作部からの指示があった場合に行なうものであるが、場合によっては特権レベル“１”のユーザからの要求に応えるようにしてもよい。後者の場合には、特権レベル“１”のユーザがカメラ制御権を有していなくても受け付けるようにすることが望ましい。なぜなら、映像の送信には直接かかわるものではないからである。

【００５５】

次に、映像送信サーバプロセス３－１１の動作を図５のフローチャートに従って説明する。

【００５６】

ステップＳ５０４～Ｓ５０７では一定周期毎に映像取り込み、配送を行っている。送信先は、送信先テーブル１－１３４に登録されている、そのときに接続されているカメラクライアントに向けて送信することになる。

【００５７】

ここで問題になるのは、ビデオカメラ１－１１から取り込まれた映像を圧縮するにしても、そのまま接続している全クライアントに対して転送して良いのか、ということである。つまり、先に説明したように、制御権を獲得したクライアントは、そのクライアントの特権レベルで許可された範囲内でカメラアングルを操作できる。例えば特権レベル“１”のユーザがカメラ制御権を獲得した場合には、全ての制限がないので、ビデオカメラ１－１１の可動可能範囲の所望とする方向及びズーム値で映像をみることができる。これでは、特権レベル“２”以上のクライアントに対しても、本来見せたくない映像が転送されてしまう。

【００５８】

そこで、本実施形態では、撮影して得られた映像データに対して、各特権レベルで規定される不可視領域の映像部分についてはマスクするようにした。但し、マスク処理の種類としては、接続ユーザ数必要ではなく、特権レベル“２”、“３”の２種類で良い。すなわち、マスク無の映像データを１つ、マスク有りの映像データを２種類作成し、それぞれの接続クライアントに向けて転送する。

【００５９】

なお、特権レベル“２”、“３”のクライアント側の表示画面には、実際にカメラで撮影された映像中に、マスクされた領域が表示されることになるので、マスク領域については、例えばこの領域に「この領域の映像をお見せすることはできません」等のメッセージを付加した映像を送信しても良い。

【００６０】

説明が前後するが、図５におけるステップＳ５０３は、映像取り込みの時期になったときに不図示のタイマからイベントを発生させたり、或いは、配布先追加要求があった場合（新たに接続されたクライアントが発生した場合）、アクセス許可テーブルの変更要求（特権レベルとユーザ名の登録及び削除等）があった場合をイベント発生として判断する。

【００６１】

さて、配布先追加要求があった場合には、ステップＳ５０８からステップＳ５１０に進んで、許可テーブル１－１３２を参照して許可されたユーザであるか否かを判断し、登録ユ

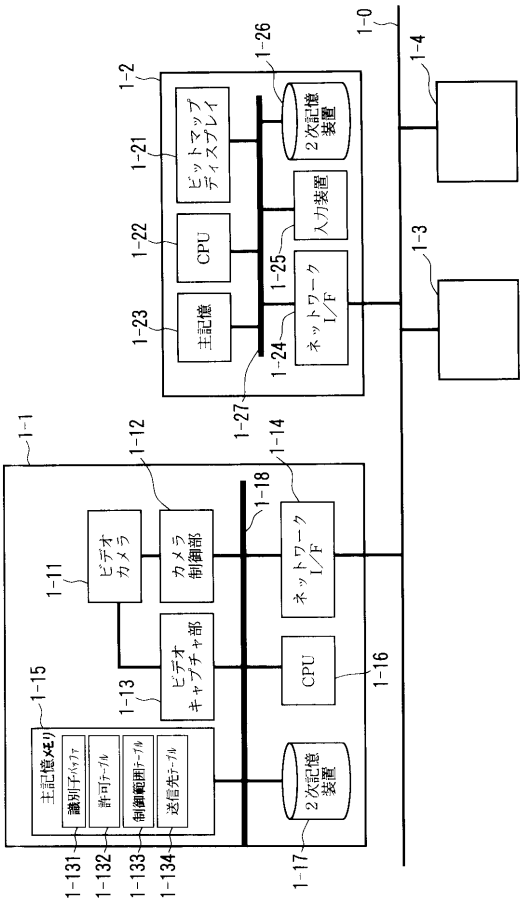
ーザであればステップＳ５１１に進んで送信先テーブル１－１３４に追加する。
【００６２】
また、アクセス許可テーブル変更要求（不図示の操作部からの指示、或いは特権レベル１のユーザからの要求）であると判断した場合には、ステップＳ５１２からステップＳ５１３に進み、許可テーブル１－１３２を更新（追加、削除）する。
【００６３】
次に、カメラクライアントの動作を図９、図１０のフローチャートに従って説明する。
【００６４】
先ず、カメラ制御プロセス３－２２の処理内容を図９を参照して説明する。
【００６５】
カメラ制御プロセスが起動すると、先ず、ステップＳ９０１において、初期化処理を行なって、図２に示すようなウインドウ２－３を表示させる。
【００６６】
次いで、ステップＳ９０２に進んで、所望とするカメラサーバに対する接続を試み、ステップＳ９０３で接続ができたか否かを判断する。接続できなかった場合には、本処理を終了する。
【００６７】
また、接続ができたら、映像表示プロセス３－３１を起動する（この映像表示プロセス３－３１については図１０で説明する）。これによって、カメラサーバからの映像を表示するプロセスが実行され、映像を表示することが可能になる。
【００６８】
ステップＳ９０５、９０９、９１３、９１６では、ウインドウ２－３における操作を監視する。
【００６９】
例えば、制御ＯＮボタン２－２４がクリックされたと判断したら、ステップＳ９０６に進んで制御権獲得要求を接続先のカメラサーバに転送する。そして、ステップＳ９０７で制御権が与えられたか否かを判断する。制御権が与えられたと判断した場合には、ステップＳ９０８に進んで制御権の有無を管理するためのフラグをＯＮにする。
【００７０】
一方、制御ＯＦＦボタン２－２５がクリックされたと判断した場合には、ステップＳ９１０に進んでフラグがＯＮになっているか否かを判断する。フラグがＯＦＦのままの場合には、最初から制御権が与えられていないのでステップＳ９０５に戻る。また、フラグがＯＮである場合には、接続先のカメラサーバに対して制御権開放要求を転送し、フラグをＯＦＦにする。
【００７１】
カメラのアングルの操作（ボタン２－２６ａ～２６ｄ、スクロールバー２－２１，２－２２，２－２３）が行われたと判断したら、ステップＳ９１４に進み、フラグがＯＮであると判断したときのみ、操作されたカメラ制御内容を接続先カメラサーバに転送する。但し、図２に示すように、黒い領域が操作された場合にはその操作内容は無視する。
【００７２】
また、本処理を終了する旨の指示があった場合には、ステップＳ９１６からステップＳ９１７に進み、映像表示プロセスを停止し、本処理を終了する。
【００７３】
次に、映像表示プロセス３－３１の動作処理手順を図１０のフローチャートに従って説明する。
【００７４】
ステップＳ１００１ではカメラサーバからのデータを受信する。受信したデータのヘッダには、その映像のカメラのアングル情報（パン角、チルト角、ズーム値、更には、これらの許容範囲を示す情報）が含まれるので、ステップＳ１００２でこれらの情報を基づいて、スクロールバーの各ツマミ位置は勿論、ツマミの可動不可範囲を示す領域を図２に示す

ように黒く塗り潰す処理を行なう。
【００７５】
そして、ステップＳ１００３に進んで、後続して送られてきた圧縮データを伸張し、映像を映像ウインドウ２－１に表示する。
【００７６】
以上説明したように本実施形態に従えば、複数のクライアントが接続されるカメラサーバにおけるカメラ制御の権限をランク付けし、そのランク内で許された範囲内でカメラ制御することができるようになる。
【００７７】
なお、上記実施形態では、例えば社内等における運用例を前提にして説明した。しかしながら、昨今注目を浴びているインターネット上にカメラサーバを設置し、一般に公開するようにしてもよい。この場合、ネットワークプロトコルはＴＣＰ／ＩＰになるので、ユーザ名はＩＰアドレスで管理することになる。また、不特定多数のユーザがログインできるようにすることが必要であるため、一人ひとりのユーザ毎の許可テーブルを作製することは現実問題として難しい。そこで、登録されていないユーザ（クライアント）に対しても一律に特権レベル“４”を与えるようにしてもよい。
【００７８】
本実施形態のように、特権レベルが“２”や“３”のカメラクライアントからの映像アクセスがあった時に、カメラ制御範囲を制限することで、映像の機密漏洩等を防止することができる。その一方で、特権レベルの高いグループからの映像アクセスがある場合には、カメラ制限範囲を制限がしないため、自由にカメラ制御することが可能になり、機密保持と情報提供の両立が図れる。
【００７９】
なお、本実施形態では、アクセス許可グループを３通りとしたが、グループを複数設定できるようにして、グループに応じてカメラ制御制限範囲を変えることで、よりきめ細かい機密保持と情報提供の両立が図れる。
【００８０】
＜第２の実施形態＞
本第２の実施形態は、上記実施形態（第１の実施形態）に対して、カメラ制御範囲を制限する代わりに、カメラ制限範囲を越えた場合に、ピントを故意にずらす、映像の解像度を下げる処理を施して（いわゆるモザイクをかける等）、映像をぼかすようにするものである。ピントを故意にずらす場合、ステップＳ４１５においてカメラ制御範囲を越えていればカメラ制御範囲に入るようにカメラ制御命令を変更するのではなく、ピントを故意にずらすことにより、映像内容を分からなくすることが可能である。制御範囲内に戻れば、ピントをオートフォーカスに戻しピントを合わせ、正確な映像を送信するようにする。
【００８１】
ピントのずらし量の設定は、例えば図８におけるズーム値の設定と同様に行なえば良いであろう。但し、ピントずらしに使用するフィルタマトリックスの大きさは、それぞれの特権レベルに応じて変動する。フィルタは、そのマトリックスで規定される範囲内では、全ての画素の平均値を各画素のデータとして出力することで実現できる。
【００８２】
本実施形態により、カメラ制限範囲を越えた場所の映像送信に関して、機密が判るほど明確には映像を確認できないが雰囲気が判る程度には映像を送ることができるように設定できるため、機密保持と映像アクセスの自由をバランスを保って両立することができる。
【００８３】
＜第３の実施形態＞
本第３の実施形態では、第２の実施形態でのピントを故意にずらす処理の代わりに、カメラ制限範囲を越えた場合に映像送信サーバからの映像を不明瞭にする映像処理機能を付加するものである。即ち、カメラ制限範囲を越えた場合に、特権レベル“１”以外のカメラクライアントへの送信映像に対してのみ、映像を不明瞭にする処理を施すものである。

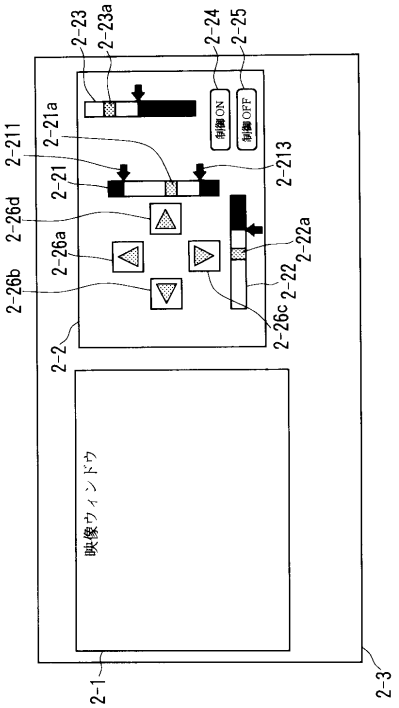
【００８４】
本実施形態では、図５のフローチャートのＳ５０６とＳ５０７の間に、映像送信先が特権レベル“１”のグループに属するか否かを判断し、その属する送信先の場合、映像をそのまま送信し、そのグループに属さない送信先であれば、画像のローバスフィルタを通すことで映像をぼかす。
【００８５】
なお、別な実施方法として、カメラサーバ１－１に、映像送信サーバとは別のプロセスとして映像変換サーバを設け、特権レベル“１”に属さない送信先の場合には、必ずこの映像変換サーバを経由するようにする方法もある。この場合、映像変換サーバでは、画像の解像度を下げる処理を施す。
【００８６】
本実施形態により、カメラ制限範囲を越えた場所の映像送信に関して、特定の利用者には機密が分かるほど明確には映像を確認できないが雰囲気が分かる程度には映像を送ることができるように設定でき、また別な特定の利用者には明瞭な映像を送信できるため、機密保持と映像アクセスの自由をバランスを保って両立することができる。
【００８７】
以上説明した各実施形態におけるカメラサーバはビデオカメラを接続して映像をキャプチャするハードとネットワークを実現するハード、カメラクライアントはネットワークを実現するハードが必要になるものの、基本的にはパーソナルコンピュータやワークステーション上で動作するアプリケーションで実現できる。
【００８８】
従って、本発明は、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。
【００８９】
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。
【００９０】
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。
【００９１】
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。
【００９２】
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。
【００９３】
【発明の効果】
以上説明したように本発明によれば、クライアントを複数のグループ毎に管理し、それぞれのグループに属するクライアントに対してはそのグループの制限範囲内でカメラを制御を行なわせることが可能になる。

【００９４】
また、他の発明によれば、カメラサーバに接続するカメラクライアントにおいて制限内容を把握できるようになる。
【００９５】
【図面の簡単な説明】
【図１】実施形態のブロック図である。
【図２】実施形態の画面例である。
【図３】実施形態のプロセス構成図である。
【図４】実施形態のカメラ制御サーバのフローチャートである。
【図５】実施形態の映像送信サーバのフローチャートである。
【図６】実施形態における許可テーブルの内容を示す図である。
【図７】実施形態における送信先テーブルの内容を示す図である。
【図８】実施形態における特権レベル”２”の制限内容を示す図である。
【図９】実施形態におけるカメラクライアントの動作処理内容を示すフローチャートである。
【図１０】実施形態におけるカメラクライアントの動作処理内容を示すフローチャートである。

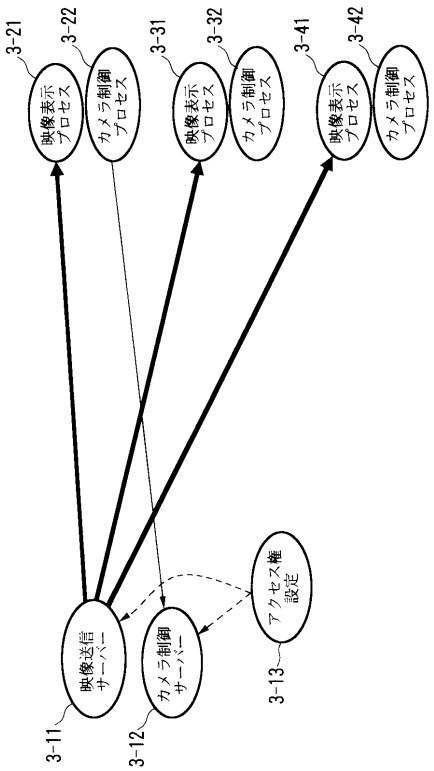
【図１】



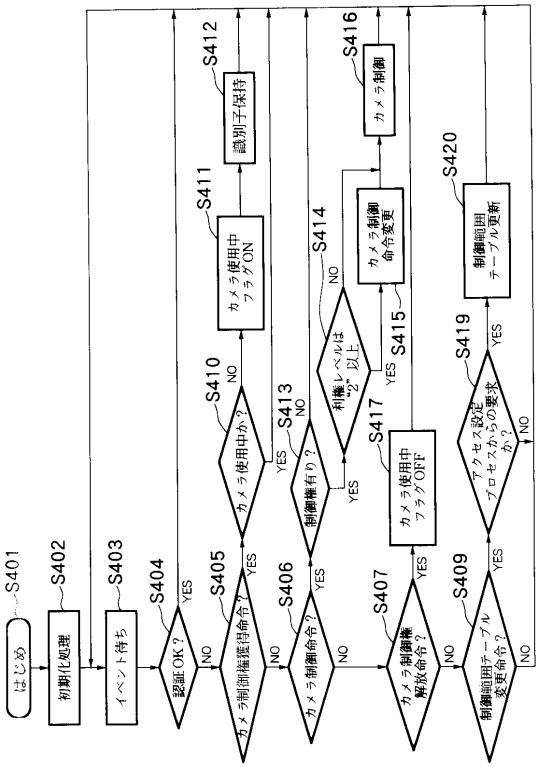
【図２】



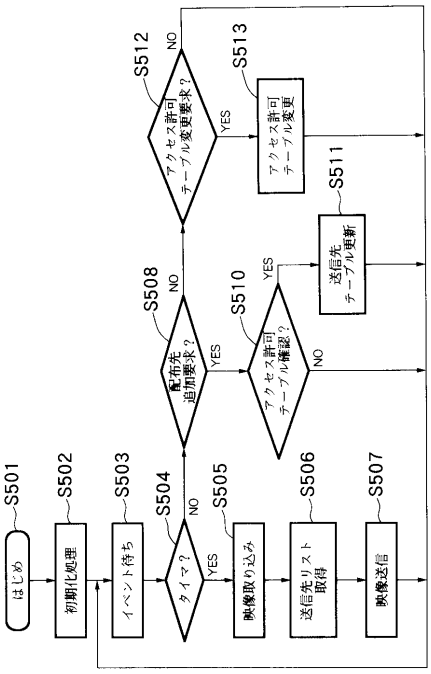
【図３】



【図４】



【図５】



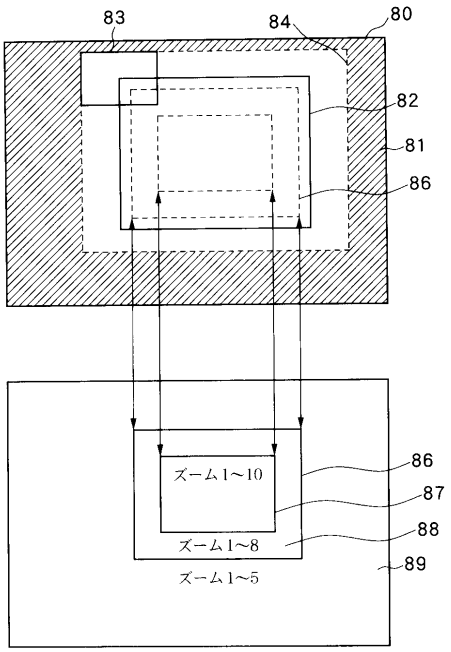
【図６】

Kazama	1
Nakagawa	1
.....	.....
Suzuki	2
Kuramata	2
.....	.....
Eda	3
Minami	3
Satoh	3
.....	.....

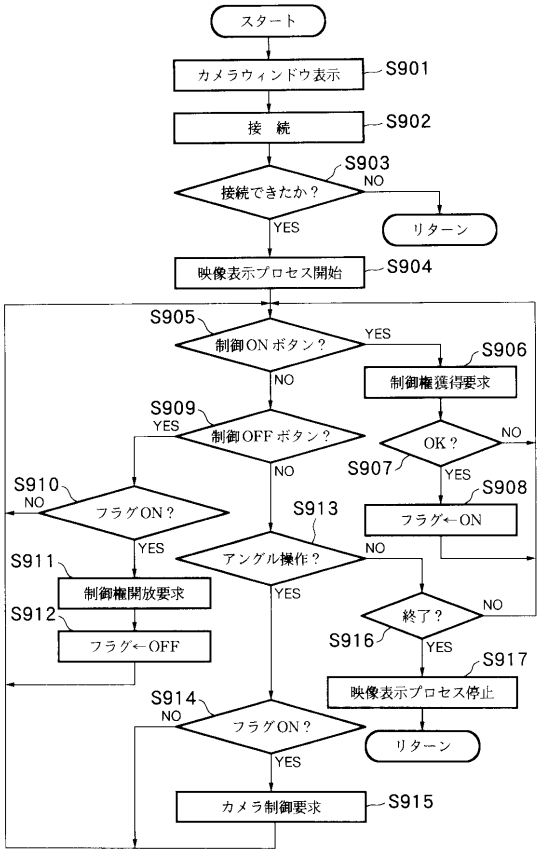
【図７】

Kazama	OFF
Suzuki	ON
Kuramata	OFF
———	———
⋮	⋮

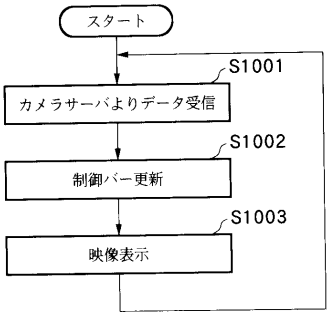
【図８】



【図９】



【図１０】



フロントページの続き

(72)発明者　瓜阪　真也
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　益戸　宏

(56)参考文献　特開平０８－２３７５３２（ＪＰ，Ａ）
特開平０６－１８１５３９（ＪＰ，Ａ）
特開平０８－０５１６１１（ＪＰ，Ａ）
特開平０５－１５３４５８（ＪＰ，Ａ）
特開平０７－１３５５９４（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.[7]，ＤＢ名)
H04N　5/222 - 5/257
H04N　7/18
H04N　7/14