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

特許第5037525号
(P5037525)

(45)発行日　平成24年9月26日(2012.9.26)　(24)登録日　平成24年7月13日(2012.7.13)

(51)Int.Cl.　F I
G06F 13/00 (2006.01)　G06F 13/00 510A
G06F 13/00 530A

請求項の数 18　(全 25 頁)

(21)出願番号	特願2008-547174 (P2008-547174)	(73)特許権者	502208205
(86)(22)出願日	平成18年12月22日 (2006.12.22)		アクシス　アーベー
(65)公表番号	特表2009-521744 (P2009-521744A)		スウェーデン国　２２３　６９　ルンド,
(43)公表日	平成21年6月4日 (2009.6.4)		エンダラヴェーイェン　１４
(86)国際出願番号	PCT/SE2006/001497	(74)代理人	100109726
(87)国際公開番号	WO2007/073314		弁理士　園田　吉隆
(87)国際公開日	平成19年6月28日 (2007.6.28)	(74)代理人	100101199
審査請求日	平成21年12月3日 (2009.12.3)		弁理士　小林　義教
(31)優先権主張番号	05112794.2	(74)代理人	100066692
(32)優先日	平成17年12月22日 (2005.12.22)		弁理士　浅村　皓
(33)優先権主張国	欧州特許庁 (EP)	(74)代理人	100072040
(31)優先権主張番号	60/776,976		弁理士　浅村　肇
(32)優先日	平成18年2月25日 (2006.2.25)	(74)代理人	100091339
(33)優先権主張国	米国 (US)		弁理士　清水　邦明

最終頁に続く

(54)【発明の名称】モニタシステムおよびモニタデバイスをサービスサーバーに接続するための方法

(57)【特許請求の範囲】

【請求項１】

モニタデバイスをリコンフィグレーションするための方法であって、

モニタデバイスが、制御サーバーに関するアドレスを前記モニタデバイスのメモリから検索するステップと、

前記モニタデバイスが、前記モニタデバイスで生じた接続事象に応答し、制御サーバーに関連するアドレスに前記モニタデバイスからの接続メッセージを送るステップと、

前記モニタデバイスと前記制御サーバーとが、前記モニタデバイスと前記制御サーバーとの間の接続を設定するステップと、

前記モニタデバイスが、前記モニタデバイスをユニークに識別するための識別子を前記モニタデバイスのメモリから検索するステップと、

前記モニタデバイスが、前記識別子を前記モニタデバイスから前記制御サーバーに送るステップと、

識別抽出器が、前記制御サーバーにおいて、前記モニタデバイスをユニークに識別する前記識別子を前記接続メッセージから抽出するステップと、

照合手段が、識別子のデータベースおよび関連するサーバーにアクセスすることにより、前記抽出した識別子とサービスサーバーとを照合することにより、前記制御サーバーにおいて、前記モニタデバイスをユニークに識別するための前記識別子に関連するサービスサーバーを識別し、前記モニタデバイスをユニークに識別するための前記識別子に関連するサービスサーバーへのアドレスを検索するステップと、

リコンフィギュレーションメッセージ発生器が、前記サービスサーバーへのアドレスと、サービスプロバイダーまたは前記デバイスに関連する他の当事者からの特定のリクエストに従ってカスタム化するための前記モニタデバイスのためのプログラムとを有するリコンフィギュレーションメッセージを発生させかつ送るステップと、

前記モニタデバイスが、前記サービスサーバーへのアドレスの受信に応答し、前記モニタデバイスから前記サービスサーバーへ、接続メッセージを送るステップと、

前記モニタデバイスと前記サービスサーバーとが、前記モニタデバイスと前記識別されたサービスサーバーとの間にサービス接続を設定するステップとを備える方法。

【請求項２】

モニタデバイスをリコンフィグレーションするための方法であって、

モニタデバイスが、制御サーバーに関するアドレスを前記モニタデバイスのメモリから検索するステップと、

前記モニタデバイスが、前記モニタデバイスで生じた接続事象に応答し、制御サーバーに関連するアドレスに前記モニタデバイスからの接続メッセージを送るステップと、

前記モニタデバイスと前記制御サーバーとが、前記モニタデバイスと前記制御サーバーとの間の接続を設定するステップと、

前記モニタデバイスが、前記モニタデバイスをユニークに識別するための識別子を前記モニタデバイスのメモリから検索するステップと、

前記モニタデバイスが、前記識別子を前記モニタデバイスから前記制御サーバーに送るステップと、

識別抽出器が、前記制御サーバーにおいて、前記モニタデバイスをユニークに識別するための前記識別子を前記接続メッセージから抽出するステップと、

照合手段が、識別子のデータベースおよび関連するサーバーにアクセスすることにより、前記抽出した識別子とサービスサーバーとを照合することにより、前記制御サーバーにおいて、前記モニタデバイスをユニークに識別するための前記識別子に関連するサービスプロバイダーを識別するステップと、

リコンフィギュレーションメッセージ発生器が、前記サービスサーバーへのアドレスと、サービスプロバイダまたは前記デバイスに関連する他の当事者からの特定のリクエストに従ってカスタム化するための前記モニタデバイスのためのプログラムとを有するリコンフィギュレーションメッセージを発生させかつ送るステップと、

前記モニタデバイスが、前記サービスサーバーへのアドレスの受信に応答し、前記モニタデバイスから前記サービスサーバーへ、接続メッセージを送るステップと、

前記モニタデバイスと前記サービスサーバーとが、前記モニタデバイスと前記識別されたサービスサーバーとの間にサービス接続を設定するステップとを備える方法。

【請求項３】

制御サーバーに関連するアドレスを前記モニタデバイスのメモリから初期検索する際に、前記モニタデバイスは、前記モニタデバイスの製造中に製造者により前記モニタデバイス内に与えられたアドレスを検索し、前記モニタデバイスから前記モニタデバイスの製造中に製造者により前記モニタデバイス内に与えられた前記アドレスへ接続メッセージを初期送信する際に、前記モニタデバイスは、前記モニタデバイスにおけるイニシエイション事象（ｉｎｉｔｉａｔｉｏｎ　ｅｖｅｎｔ）に応答して前記送信を行う、請求項１または２に記載の方法。

【請求項４】

前記モニタデバイスがネットワーク接続を検出することに応答し、前記モニタデバイスは、前記モニタデバイスから前記モニタデバイスの製造中に製造者により前記モニタデバイス内に与えられた前記アドレスへの接続メッセージの初期送信を実行する、請求項３記載の方法。

【請求項５】

前記識別抽出器が前記モニタデバイスをユニークに識別するための前記識別子はシリアル番号である、請求項１～４のいずれか１つに記載の方法。

【請求項６】
前記モニタデバイスが、前記識別されたサービスサーバーに関するアドレスに対し、イニシエイション事象に応答して使用されるアドレスを前記モニタデバイス内に設定することを更に含む、請求項１～５のいずれか１つに記載の方法。
【請求項７】
前記モニタデバイスが、設定されたサービス接続を通してモニタデータを前記モニタデバイスから前記サービスサーバーに通信するステップを更に含む、請求項１～６のいずれか１つに記載の方法。
【請求項８】
モニタデータを通信する前記ステップは、前記モニタデバイスが、設定されたサービス接続を通して前記モニタデバイスから前記サービスサーバーにビデオシーケンスを通信することを含む、請求項７記載の方法。
【請求項９】
前記モニタデバイスと制御サーバーとの接続のイニシエイションのための専用のボタンのマニュアル作動に応答し、前記モニタデバイスの製造中に製造者により前記モニタデバイス内に与えられた前記アドレスに前記モニタデバイスからの接続メッセージを送ることを実行する、請求項３記載の方法。
【請求項１０】
モニタシステムのための制御サーバーであって、
前記制御サーバーをネットワークに接続するインターフェースと、
モニタデバイスから受信した接続メッセージから識別子を抽出するようになっている識別抽出器であって、前記識別子は前記識別抽出器が前記モニタデバイスをユニークに識別するための識別子である、識別抽出器と、
前記抽出した識別子とサービスサーバーとを照合し、一致したサービスサーバーに対するアドレスを検索するようになっている照合手段であって、識別子のデータベースおよび関連するサービスサーバーにアクセスすることにより、前記モニタデバイスの前記識別子とサービスサーバーとを照合するようになっている照合手段と、
前記検索したアドレスとサービスプロバイダーまたは前記デバイスに関連する他の当事者からの特定のリクエストに従ってカスタム化するための前記モニタデバイスのためのプログラムとを含むメッセージを発生させかつ送るようになっているリコンフィギュレーションメッセージ発生器とを備えた、モニタシステムのための制御サーバー。
【請求項１１】
モニタシステムのための制御サーバーであって、
前記制御サーバーをネットワークに接続するインターフェースと、
モニタデバイスから受信した接続メッセージから識別子を抽出するようになっている識別抽出器であって、前記識別子は前記識別抽出器が前記モニタデバイスをユニークに識別するための識別子である、識別抽出器と、
前記抽出した識別子とサービスプロバイダーとを照合するようになっている照合手段であって、前記照合手段は、識別子のデータベースおよび関連するサービスプロバイダにアクセスすることにより、前記モニタデバイスの識別子をサービスプロバイダーと照合するようになっている、照合手段と、
前記サービスサーバーアドレスと、サービスプロバイダーまたは前記デバイスに関連する他の当事者からの特定のリクエストに従ってカスタム化するための前記モニタデバイスのためのプログラムとを含むメッセージを発生させかつ送るようになっているリコンフィギュレーションメッセージ発生器とを備えた、モニタシステムのための制御サーバー。
【請求項１２】
前記識別抽出器が前記モニタデバイスをユニークに識別するための前記識別子はシリアル番号である、請求項１０または１１に記載の制御サーバー。
【請求項１３】
前記リコンフィギュレーションメッセージ発生器により発生されたメッセージは、サー

ビスプロバイダーまたは前記デバイスに関連する他の当事者からの特定のリクエストに従ってカスタム化するための前記モニタデバイスのためのプログラムを自動的に変更する自動変更を含む、請求項１０、１１または１２に記載の制御サーバー。
【請求項１４】
モニタデバイスと、制御サーバーと、複数のサービスサーバーと、前記サーバーと前記モニタデバイスとを接続するネットワークとを備えたモニタシステムであって、
前記モニタデバイスは、
制御サーバーに関連するアドレスを含むメモリと、
イニシエイション事象に応答し、前記ネットワークを通して前記アドレスに接続メッセージを送るようになっているイニシエイション手段と、
前記ネットワークを介して受信されたメッセージの受信に応答し、受信された該メッセージ内のアドレスに新しい接続メッセージを送るようになっている手段と、
メモリ内に記憶され、前記モニタデバイスをユニークに識別するための識別子とを備え、
前記接続メッセージを送る先のアドレスに、この識別子を送るようになっており、
前記制御サーバーは請求項１０～１２のいずれか１つに記載の前記制御サーバーの機能を含み、
各サービスサーバーは、モニタデバイスからのモニタデータを受信し、処理するための手段を備える、
モニタシステム。
【請求項１５】
前記モニタデバイスの前記メモリは、可能性のある制御サーバーを表示するアドレスの優先リストを含む、請求項１４記載のモニタシステム。
【請求項１６】
前記モニタデバイスをユニークに識別するための前記識別子はシリアル番号である、請求項１４または１５に記載のモニタシステム。
【請求項１７】
前記イニシエイション手段はネットワーク接続検出器である、請求項１４～１６のいずれか１つに記載のモニタシステム。
【請求項１８】
前記イニシエイション手段は前記モニタデバイスの接続のイニシエイションのための専用のボタンである、請求項１４～１６のいずれか１つに記載のモニタシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
（発明の技術分野）
本発明は、モニタシステムおよびかかるシステムのデバイスに関し、特に本発明は、モニタデバイスをサービスサーバーに接続するための方法およびかかる接続を可能にするモニタシステムに関する。
【背景技術】
【０００２】
（発明の背景）
コンピュータネットワークを介し、モニタサーバーまたは監視サーバーに接続された、注目する建物、エリアおよび／またはプロセスをモニタするためのモニタシステムは、次第に普及している。特にかかるモニタシステムは、デジタルモニタカメラを含む。かかるシステムが普及する１つの理由は、コンピュータネットワークが既に設置されている場合に、広い範囲のシステムが既存のネットワークを利用できることにある。
【０００３】
一般的なコンピュータネットワークを監視ネットワークとして使用する別の理由は、モニタシステムのために構築しなければならないネットワークを使って、他のタイプの機器

、例えばコンピュータ、サーバーおよび周辺機器を接続できることにある。これら理由から、この技術は単一の、または数個のモニタデバイスを必要とする組織／個人だけでなく、多数のモニタデバイスを必要とする組織／個人も満たすことができる。

【０００４】

かかるモニタシステムでは、モニタデバイスはモニタデータをサービスサーバーに送るようになっており、サービスサーバーはモニタデータまたは情報を処理し、ユーザーがモニタデータにアクセスするためのデータを作成し、モニタ情報をロギングしたり、モニタデータを記憶したり、またはモニタシステムの当業者に知られている他の目的を果たすことができる。

【０００５】

一般的には、かかるシステムのモニタデバイスはある会社によって製造され、サービスサーバーは別の会社であるモニタサービスプロバイダによって維持される。このモニタサービスプロバイダは、かかるサービスを提供することを専門にする会社または組織とし得る。しかしながら、モニタサービスプロバイダは、モニタされる建物、エリアおよび／またはプロセスに関連する会社、例えばその建物を所有したり、またはモニタされるサイトで営業する会社でもある。今日のシステムでは、ユーザーがモニタデバイスに直接アドレスをキー入力することにより、サービスサーバーに対するアドレスを各モニタデバイスに提供できる。モニタデバイスとサービスサーバーの間との接続を達成する別の方法は、コンピュータネットワークに接続されたコンピュータを介し、サービスサーバーに接続し、サービスサーバーにモニタデバイスを登録することである。

【０００６】

今日、サービスサーバーのアドレスのかかるプログラミング、すなわちサービスサーバーへのモニタデバイスの登録は、モニタデバイスのインストールプロセス中にユーザーまたは個人がモニタデバイスをインストールすることによって実行されている。

【発明の開示】

【発明が解決しようとする課題】

【０００７】

上記モニタシステムに関連する一般的な問題は、インストールを実行する個人がモニタデバイスにプログラムを組み込んだ経験がないことがあり、プログラムに時間がかかり、インストールする個人がモニタデバイスにエラーデータを入力し得ることである。

【０００８】

本発明の目的は、改良されたモニタシステムを提供することにある。

【課題を解決するための手段】

【０００９】

この目的は、請求項１記載のモニタデバイスをサービスサーバーに接続する方法、および請求項１１記載のモニタシステム、請求項１８記載の制御サーバー、および請求項２１記載のモニタデバイスによって達成される。本発明の実施例は従属項に開示されている。

【００１０】

特に本発明の１つの様相によれば、特に本発明の第１の様相によれば、モニタデバイスをサービスサーバーに接続するための方法は、制御サーバーに関するアドレスを前記モニタデバイスのメモリから検索するステップと、前記モニタデバイスで生じた接続事象に応答し、制御サーバーに関連するアドレスに前記モニタデバイスからの接続メッセージを送るステップと、前記制御サーバーにおいて、前記モニタデバイスと前記制御サーバーとの間の通信から識別子を抽出するステップと、前記制御サーバーにおいて、前記抽出した識別子に関連するサービスサーバーを識別するステップと、前記制御サーバーから前記モニタデバイスに前記識別されたサービスサーバーに関連するアドレスを送るステップと、前記識別されたサービスサーバーに関連するアドレスの受信に応答し、前記モニタデバイスから前記識別されたサービスサーバーへ、接続メッセージを送るステップと、前記モニタデバイスと前記識別されたサービスサーバーとの間にサービス接続を設定するステップとを備える。

【００１１】
本発明の第２の様相によれば、モニタシステムは、モニタデバイスと、制御サーバーと、複数のサービスサーバーと、前記サーバーと前記モニタデバイスとを接続するネットワークとを備える。
【００１２】
前記モニタデバイスは、接続アドレスを含むメモリと、イニシエイション事象（ｉｎｉｔｉａｔｉｏｎ　ｅｖｅｎｔ：起動事象、スタート事象）に応答し、前記ネットワークを通して前記接続アドレスに接続メッセージを送るようになっているイニシエイション手段と、前記ネットワークを介し受信したメッセージ内のアドレスに、新しい接続メッセージを送るようになっている手段とを備える。
【００１３】
前記制御サーバーは、前記モニタデバイスと前記制御サーバーとの間の通信から識別子を抽出するようになっている識別抽出器と、前記抽出した識別子と制御サーバーまたはサービスサーバーとを照合し、一致したサービスサーバーに対するアドレスを検索するようになっている照合手段と、前記検索されたアドレスを含むメッセージを発生し、前記発生されたメッセージを前記モニタデバイスに送るようになっているメッセージ発生器とを備える。
【００１４】
各サービスサーバーは、モニタデバイスからのモニタデータを受信し、処理するための手段とを備える。
【００１５】
上記方法およびシステムの利点として、デバイスのメンテナンスおよび設置を容易にできることが挙げられる。その理由は、モニタデバイスは人が好ましいサービスサーバーに対するアドレスをキー入力しなくても、制御サーバーにより好ましいサービスサーバーにガイドされるからである。更にこのようにシステムをより効率的に維持できる。その理由は、制御サーバーはユーザーまたは人がモニタデバイスを維持するよりも新しいか、または変化するサービスサーバーのアドレスによって更新を維持することがより容易または効率的にできるからである。
【００１６】
別の利点は、モニタデバイスが制御サーバー（１つまたは複数）と、サービスサーバー（１つまたは複数）とのすべての接続をイニシエイト（ｉｎｉｔｉａｔｅ：スタート、起動）させ、これによってアクセス制限デバイス、例えばファイアーウォール、ＮＡＴ（ネットワークアドレス変換）、ＩＳＰ（インターネットサービスプロバイダ）の後方からのモニタデバイスの統合を促進し、かかるアクセス制限デバイス外に達するシステムにダイナミックアドレスを提供できることである。
【００１７】
本発明の別の実施例によれば、上記方法においてモニタデバイスのメモリから制御サーバーに関するアドレスを初期検索（ｉｎｉｔｉａｌ　ｒｅｔｒｉｅｖａｌ）すると、制御サーバーに関するあらかじめコンフィギュアされたアドレスが戻され、モニタデバイスからあらかじめコンフィギュアされたアドレスへの接続メッセージの初期の送信は、モニタデバイスのイニシエイション事象に応答して実行される。
【００１８】
このように初期制御サーバー（ｉｎｉｔｉａｌ　ｃｏｎｔｒｏｌ　ｓｅｒｖｅｒ）を構成する利点は、システムのモニタデバイスの設置およびカスタム化が容易となることである。モニタデバイスのイニシエイション時に、モニタデバイスのイニシエイションの結果、自動的に所定の制御サーバーにコンタクトするので、設置中にモニタデバイスへアドレスを提供する必要はなくなるので、設置は容易である。モニタデバイスと制御サーバー、例えば初期制御サーバーとの間の初期通信（ｉｎｉｔｉａｌ　ｃｏｍｍｕｎｉｃａｔｉｏｎ）時に、モニタデバイスに関する特定の属性（ｐｒｏｐｅｒｔｉｅｓ：プロパティ）を提供できるので、カスタム化が促進される。従って、モニタデバイスのメーカーはモニタ

デバイスの異なるロット（ｄｉｆｆｅｒｅｎｔ　ｂａｔｃｈｅｓ）に対し、異なる製造プロセスを有する必要はない。

【００１９】

換言すれば、本発明のこの実施例に係わるシステムは、デバイスのカスタム化に関するメーカーの問題を解消できる。例えば製造中、今日のモニタシステムのモニタデバイスを、異なるサービスプロバイダと関連付ける必要があり、関連するサービスプロバイダに対してカスタム化されたプロセス内で、サービスプロバイダに関連する各デバイスにプログラムを組まなければならない。従って、メーカーは異なるサービスプロバイダ用のデバイスに対し、複数の異なる製造プロセスを設けなければならない。更に、特定のサービスプロバイダに対してプログラムされたデバイスを特定のサービスプロバイダまたは特定のサービスプロバイダの顧客に出荷し、販売しなければならない。

【００２０】

この実施例の別の利点は、モニタデバイスを中央で管理できるようになることである。

【００２１】

更に別の実施例によれば、接続メッセージのモニタデバイスから制御サーバーへの送信は、サービスサーバーのアドレスをモニタデバイスに提供する制御サーバーに接続メッセージをモニタデバイスから送る前に、少なくとも１回行われる。

【００２２】

複数の制御サーバーを配置し、モニタデバイスを別の制御サーバーに向ける利点は、正しいサービスサーバーにモニタデバイスを向ける責任を、システムの一般的機能に責任のあるエンティティ、例えばモニタデバイスのメーカーから、必要なサービスを提供する責任があるエンティティ、例えばサービスプロバイダに変更できることである。

【００２３】

別の実施例によれば、サービスサーバーを識別する動作は、モニタデバイスと制御サーバーとの間の通信から、モニタデバイスに関するネットワークアドレスを抽出し、ネットワークアドレスとサービスプロバイダとを照合し、一致したサービスプロバイダに関連するサービスサーバーを選択する動作を更に含む。

【００２４】

少なくともネットワーク接続を行うサービスプロバイダがモニタサービスのプロバイダに関連している場合、またはそれらサービスプロバイダが同じ場合、このようにモニタデバイスに関係するネットワークアドレスを使用することにより、サービスプロバイダを識別することが容易となる。

【００２５】

更に別の実施例によれば、サービスサーバーを識別する動作は、モニタデバイスと制御サーバーとの間の通信において、モニタデバイスが含む識別コードを抽出し、この識別コードとサービスプロバイダとを照合し、一致したサービスプロバイダに関連するサービスサーバーを選択する動作を含む。

【００２６】

このように識別コードを使用することにより、種々の基準に基づき、モニタデバイスをカスタム化し、特定のモニタサービスプロバイダに接続できる。例えばモニタデバイスがモニタサービスプロバイダのサービスサーバーに接続されるという条件で、モニタデバイスを買う際に、モニタデバイスの１つのロット（ｂａｔｃｈ）を、ディスカウントを提供する特定のモニタサービスプロバイダ専用とすることができる。このようにサービスプロバイダはサービスプロバイダに属す識別コードとして制御サーバーに登録された識別コードを入手し、よってサービスプロバイダはモニタデバイスのサービスプロバイダのサービスへの接続を保証できる。更に、モニタデバイスのロットを自らの建物のモニタのために、自己のサービスサーバーを有する会社専用とすることができる。

【００２７】

すべての実施例において、接続メッセージを制御サーバーまたはサービスサーバーに送るのは、モニタデバイスである。この利点は、モニタデバイスからのメッセージに応答し

、例えばｈｔｔｐリクエストに応答し、サーバーは制御メッセージを送るように構成できることである。従って、制御サーバーはモニタデバイスとサーバーとの間に配置された、可能性のあるアクセス制限デバイス、例えばファイアーウォール、ＮＡＴサーバーなどにもかかわらず、モニタデバイスに対する制御を行うことができる。スウェーデン、Ｓ２２３　６９　ルンド、エムダラベーゲン１４、アキシスＡＢ社によって出願された国際特許出願第ＷＯ２００６／０７３３４８号に、かかる通信方式が開示されている。

【００２８】

一実施例によれば、このシステムは制御サーバーのヒエラルキー（階層）内で高レベルまたはトップレベルの制御サーバーである、少なくとも１つの初期制御サーバーを含む複数の制御サーバーを備える。かかる初期制御サーバーは、システム内の任意の制御サーバーおよびサービスサーバーへの少なくとも間接的な接続を可能にするアドレス情報にアクセスするようになっている。

【００２９】

このようにシステムを構成することにより、サーバー間に責任を分散させることが可能となる。例えばモニタデバイスに制御サーバーまたはサービスサーバーの正しいサブシステムに命令させる全責任を初期制御サーバーに与え、一方、かかるサブシステムにおける制御サーバーに、モニタデバイスが最も適したサービスサーバーに命令する責任を与えることができる。

【００３０】

次に示す詳細な説明から、本発明の実施可能性の別の範囲が明らかとなろう。しかしながら、本発明の好ましい実施例を示す詳細な説明および特定の例は、単に説明するために示したものに過ぎないと理解すべきである。その理由は、詳細な説明を当業者が読めば、当業者には本発明の範囲内で種々の変形および変更が明らかとなるからである。

【００３１】

添付図面を参照し、現時点で好ましい実施例の次の詳細な説明を読めば、本発明の別の特徴および利点が明らかとなろう。

【実施例】

【００３２】

（現時点で好ましい実施例の詳細な説明）

図１では、本発明の一実施例に係わるモニタシステム１０の概観が示されている。このモニタシステム１０は、モニタデバイス２０と、制御サーバー３０と、サービスサーバー４０と、クライアントコンピュータ４２またはモバイル電話４４としてのユーザーターミナルとを含む。モニタデバイス２０、制御サーバー３０およびサービスサーバー４０は、コンピュータネットワーク５０、例えばインターネット、ＬＡＮ（ローカルエリアネットワーク）、ＷＡＮ（ワイドエリアネットワーク）を介して互いに接続されている。コンピュータネットワーク５０は、無線および／または有線通信チャンネルを含むことができ、モニタデバイス２０は、デジタルカメラ、動き検出器、オーディオ検出器、ＩＲ検出器、通過制御（ｐａｓｓａｇｅ　ｃｏｎｔｒｏｌ）デバイス、電子ドアロック、エレベータ制御システム、カードリーダーなどとすることができる。ユーザーターミナル４２、４４はネットワークに接続されており、サービスサーバー４０と通信し、モニタデバイスへのアクセス、またはサービスサーバーで実行されるモニタサービスにアクセスするようになっている。

【００３３】

図２では、異なるデバイスの間の一般的なシグナリング方式が略図で示されている。デバイス間の通信の仕様は、使用される通信プロトコルおよび物理的ネットワークに応じて変わり得る。しかしながら、ネットワークを介し、一般的な通信をどのように実行するかに関する詳細については、コンピュータ通信の当業者には知られているので、この詳細については本明細書では説明しない。モニタデバイス２０は、イニシエイション動作またはイニシエイション事象に応答し、モニタデバイス２０内に記憶されているアドレスへ接続メッセージ６００を送るようになっている。この接続メッセージは、前記アドレスに常駐

する制御サーバー３０で受信される。この制御サーバー３０は、接続メッセージを受信し、モニタデバイス２０と制御サーバー３０とは、接続を設定する。制御サーバーは、モニタデバイス２０から受信した通信信号から識別子も抽出する。この識別子は、モニタデバイスとサービスプロバイダおよびサービスサーバーとを照合するのに使用される。制御サーバー３０が一致していると判断すると、この制御サーバー３０はメッセージ６０２内のアドレスをモニタデバイスに送る。このメッセージは、モニタデバイス２０でアドレスメッセージまたはリコンフィギュレーションメッセージの変更として識別される。このメッセージ６０２に応答し、モニタデバイス２０は新しいアドレスを記憶し、接続メッセージ６００または６０４を新しいアドレスに送る。接続サーバー３０から受信されたアドレスは、システムの構造に応じ、別の制御サーバー３０またはサービスサーバー４０をアドレス指定できるが、これについては後述する。

【００３４】

モニタデバイスで受信されたリコンフィギュレーションメッセージ６０２内のアドレスが、サービスサーバー４０に関連しており、従って、モニタデバイス２０から送られた次の接続メッセージ６０４がサービスサーバー４０に送られると、サービスサーバー４０とモニタデバイス２０はサービス接続６０６を設定し、モニタデータのサービスサーバー４０への伝送を可能にし、可能な場合にはモニタデバイスへのコンフィグレーションパラメータの伝送を可能にするが、このことは必ずしも必要ではない。こうして、モニタデバイス２０はモニタサービスを提供することが可能にされたサーバーへ接続される。次に、モニタデバイス２０が向けられたサービスサーバー４０は、地理的なロケーション、ネットワーク内のロケーション、利用できるサービスおよび／または顧客固有の理由に関し、最も適当なサービスサーバー４０となり得る。特定のモニタデバイス２０に関して適用できるこれら基準のうちのいずれか１つを、制御サーバー３０に提供されるデータにより制御してもよいし、または制御サーバー３０がモニタデバイス２０をサービスサーバー４０に向けることによって制御してもよい。

【００３５】

一実施例によれば、モニタデバイス２０は図３Ａおよび図３Ｂに示されるように入力手段２０２、処理手段２０４、不揮発性メモリ２０６、揮発性メモリ２０８、ネットワークインターフェース２１０、イニシエイション手段（ｉｎｉｔｉａｔｉｎｇ　ｍｅａｎｓ）２１２、モニタデバイス手段２１６を含むことができる。図３ａは、一般的なモニタデバイスの略図であり、図３ｂは、デジタルカメラであるモニタデバイス２０の略図である。本発明の理解を容易にするために、図３ａおよび３ｂは、正常な機能をデバイスが実行できるようにするのに必要なすべての手段を示しているわけではない。すなわちＩＲ検出機能をＩＲ検出器に実行させ、デジタルカメラ機能をデジタルカメラに実行させる手段のすべてを示しているわけではない。モニタデバイスをモニタデバイスとして作動させるのに必要なハードウェアおよびソフトウェアのようなすべての手段は、図３ａ内のモニタデバイス手段２１６により表示されており、図３ｂではカメラの対応する手段をビデオカメラ手段２１８と称す。通常のモニタデバイスネットワークをイネーブルするのに必要な手段および装置は、当業者に知られたものである。現在市販されている、かかるネットワークをイネーブルするモニタデバイスの一例として、スウェーデンＳ－２２３　６９、ルンド、エンダラベーゲン１４、アキシスコミュニケーションズＡＢ社（Ａｘｉｓ　ｃｏｍｍｕｎｉｃａｔｉｏｎｓ　ＡＢ）から市販されている、ネットワーク接続されるデジタルカメラを挙げることができる。

【００３６】

上記のように、モニタデバイス２０は複数のタイプのデバイスの任意のものでよく、モニタデバイス２０の入力手段２０２は、異なるタイプのモニタデバイスである。例えば図３ｂのデジタルカメラ２０ａの入力手段２０２を、イメージセンサ、例えばＣＣＤとすることができ、オーディオ検出器の入力手段をマイクなどとすることができる。入力手段２０２の主な機能は、モニタデバイス２０がモニタする特性を検出し、サンプリングし、または測定し、よってかかるデータを別の処理のための処理手段２０４へ送ることである。

【００３７】
処理手段２０４は、モニタデバイスの機能を制御し、本発明の機能およびモニタデバイス２０の一般的な機能に関連するプログラムコードを実行するようになっている。モニタデバイスの機能およびモニタシステムとの対話（ｉｎｔｅｒａｔｉｏｎ）に関連するデータおよび情報を記憶するために、モニタデバイス２０により不揮発性メモリ２０６を使用できる。特に本発明の一実施例によれば、この不揮発性メモリに、ネットワーク上のサーバーに対するアドレスのリスト２１４を記憶する。このアドレスのリスト２１４は優先マーカー（ｐｒｉｏｒｉｔｙ　ｍａｒｋｅｒ）によって各アドレスエントリーをマークすることにより優先度を決定できる。これらのマーカーは優先度を識別する番号とすることができる。メーカーから出荷されるモニタデバイス内のアドレスのリスト２１４は、制御サーバー３０に対する少なくとも１つのあらかじめプログラムされたアドレスを含み、このサーバーは一般にこのアプリケーションにおける初期制御サーバー（ｉｎｉｔｉａｌ　ｃｏｎｔｒｏｌ　ｓｅｒｖｅｒ）と称される。このリスト２１４は複数のアドレスを含むことができ、このリストでは、最高の優先度を有するとマークされたアドレスは、モニタデバイスが接続事象に応答し、接続メッセージを送る先の最初のアドレスである。この最初のアドレスが失敗した場合、優先リスト内の次のアドレスが試行され、接続メッセージが同じようにそのアドレスへ送られる。別の実施例によれば、最初のアドレスが失敗した場合、リスト２１４内で試行される次のアドレスがランダムに選択され、その結果、多くのデバイスに同じリストが設けられており、障害のあるアドレスに基本的に同時に接続しようとしている場合、ネットワーク内で負荷の分散が行われる。
【００３８】
この不揮発性メモリは、モニタデバイスをユニークに識別する識別コードおよび暗号化のためのユニークな鍵も含むことができる。制御サーバーまたはサービスサーバーにおいて、モニタデバイスを識別するのに使用でき、ユニークなキーは識別コードにより記述されるカメラとしてカメラを認証するのに使用できる。
【００３９】
処理手段２０４をサポートし、および／または制御サーバーから受信されたアドレスを一時的に記憶するのに、揮発性メモリ２０８を使用できる。従って、揮発性メモリ２０８は、処理手段２０４によりモニタデバイス２０４上で実行されるアプリケーションによって使用されるメモリでもよい。
【００４０】
ネットワークインターフェース２１０は、モニタデバイス２０とネットワーク５０との間のインターフェースであり、多数の異なるネットワークに対するネットワークインターフェース２１０を構成するのに使用できるハードウェアおよびソフトウェアは、コンピュータネットワークに精通する当業者には周知のものである。
【００４１】
イニシエイション手段２１２はイニシエイション事象を発生し、よって不揮発性メモリ２０６に記憶された優先アドレスへ初期接続メッセージを送ることをトリガーする手段である。一実施例によれば、イニシエイション手段２１２は、ネットワーク５０へのモニタデバイス２０の接続、すなわちネットワーク５０への電源をオンしたモニタデバイス２０の接続または既に物理的にネットワークに接続されているモニタデバイス２０の電源の投入のいずれかを検出するようにイネーブルされた検出器である。かかるイニシエイション手段２１２を構成することにより、適当なサービスサーバー４０のサーチおよびこれへの接続を完全に自動化できる。別の実施例によれば、イニシエイション手段２１２をモニタデバイス２０の電源ボタンとしてもよいし、サービスサーバー４０へのモニタデバイス２０の接続をイニシエイトする専用のボタンとしてもよい。
【００４２】
サービスサーバー４０へのアドレスを含むメッセージまたはかかるサーバーへのアドレスを含むリコンフィギュレーションメッセージに応答し、制御サーバー３０またはサービスサーバー４０へ接続メッセージを送るようになっている手段２１８を、処理手段２０４

によって実行されるプログラムコードによって実施してもよい。

【００４３】

不揮発性メモリ２０６に記憶されているユニークな鍵に関する説明に戻ると、この鍵は、送るべきメッセージの暗号化または受信したメッセージの解読のためにも使用できる。更にこの鍵を使って、スウェーデンＳ－２２３　６９、ルンド、エンダラベーゲン１４、アキシスコミュニケーションズＡＢ社により出願された国際特許出願第ＷＯ２００６／０７３３４８号に記載のようなオープンパスを生じさせる接続の設定中にカメラを認証することができる。この制御サーバーおよびサービスサーバーにはモニタデバイスからのメッセージを解読し、モニタデバイスに送られるメッセージを暗号化し、モニタデバイスを認証できるようにする鍵を設けることもできる。よって、モニタデバイスと制御サーバーおよび／またはサービスサーバーとの間のすべての通信を暗号化できる。製造される各モニタデバイスに対し、ユニークな鍵を設けることが好ましく、この鍵はデバイスの製造中にモニタデバイス内に記憶できる。これら鍵は、共有秘密システムの鍵、または公開鍵システムの鍵とすることができる。

【００４４】

一実施例によれば、これら鍵を設けるべきカメラを製造する前に、異なる鍵の極めて大きいリストを作成する。このリストの大きさは、何年もの間、新しいリストを作成する必要のない大きさとすべきである。各制御サーバーには、鍵のリストを設け、モニタデバイスの製造中、デバイスにはこれら鍵のうちの１つが設けられることになる。このように鍵を設けることにより、安全上の危険を生じさせ得るような鍵を配布する必要がなくなる。従って、モニタデバイスの認証および鍵の配布を簡略化できる。

【００４５】

図４ａには一実施例に係わる、サービスサーバー４０を探すモニタデバイス２０のプロセスが示されている。最初にオフラインまたはシャットオフされているモニタデバイス２０をイニシエイトする。すなわちネットワークに接続し、電源をオンにするか、上記他の方法でイニシエイトする（ステップ６２０）。

【００４６】

次にモニタデバイス２０は、不揮発性メモリ２０６内の優先リストから最初のアドレスを検索する（ステップ６２２）。このアドレスは、製造プロセス中にメーカーによって記憶されたアドレスとすることができる。しかしながら、本発明に係わるシステムにあらかじめモニタデバイス２０が接続されている場合、このアドレスはデバイスの製造中にモニタデバイス２０内に設けられたアドレスのサーバー以外の、より適当なサーバーに対するアドレスを含む、別のメッセージまたはリコンフィギュレーションメッセージに応答して記憶されたアドレスでもよい。

【００４７】

次にモニタデバイスは検索されたアドレスに関連するサーバーへネットワークインターフェース２１０を介し、接続メッセージを送る（ステップ６２４）。

【００４８】

接続メッセージが送られた後にモニタデバイスは、接続メッセージを受信したサーバーからの応答を待つ。

【００４９】

ステップ６２６において、応答が新しいサーバーへのアドレスを含むメッセージとなる場合、または応答が新しいサーバーへのアドレスを含むリコンフィギュレーションメッセージとなる場合、モニタデバイスは不揮発性メモリ２０６内にこのアドレスを記憶する（ステップ６２８）。このアドレスはリスト２１４内に、最も高い優先度のアドレスとして記憶できる。サーバーからの応答メッセージまたはリコンフィギュレーションメッセージは、特定の一実施例によれば、不揮発性メモリ２０６内の現在のリストの代わりとなるサーバーアドレスの完全に新しいリスト、または現在のリスト内のアドレスの一部に代わるアドレスのサブセットを含むことができる。

【００５０】

次に、モニタデバイスは新しいサーバーアドレスへ新しい接続メッセージを送る（ステップ６３０）か、または受信したメッセージに応答し、ステップ６２８でリストを変更した後に、優先リスト内の最初のアドレスを送る。次に、モニタデバイス２０は、接続メッセージを送った先のサーバーからの応答をもう１回待つ。

【００５１】

ステップ６２６において応答メッセージ内に新しいサーバーアドレスが識別されない場合、応答が自らの内部のサービスサーバー４０であるサーバーの表示を含むかどうかをモニタデバイス２０がチェックする（ステップ６３２）。応答がかかる表示を含む場合、モニタデバイス２０およびサービスサーバーはサービス接続を設定する（ステップ６３４）。

【００５２】

サーバーがサービスサーバーである表示を応答が含まない場合、モニタデバイスはサーバーからの別のメッセージを待つことができる。別の実施例では、応答メッセージがサーバーをサービスサーバーとして識別しないと判断したとき、または応答メッセージが新しいサーバーアドレスを識別しないと判断されたときに、モニタデバイスは接続メッセージを直接リスト内の別のアドレスに送る。別の実施例ではサーバーまたはアドレスがエラーである可能性が高い旨をカウンタまたはタイマーが表示した後に、リスト内の別のアドレスに、かかる接続メッセージが送られる。前記別のアドレスは、前に述べたように、優先リスト内の次のアドレスでもよいし、またはリスト内でランダム選択してもよい。

【００５３】

図４Ｂに示される別の実施例では、モニタデバイスの不揮発性メモリからのサーバーアドレスを検索するステップ６２２は、更に識別コードおよび認証コードを検索することを含む。この識別コードは、モニタデバイスをユニークに識別する識別子、例えばシリアル番号、アイテム固有のコードと組み合わせた製品コードなどである。認証コードは不揮発性メモリ２０６内に記憶された鍵によって暗号化されたコードとすることができる。識別子および認証コードは、次に接続メッセージ（ステップ６２４）内、またはサーバー３０との後の通信信号内のいずれかにおける検索されたアドレスのサーバー３０へ送られる（ステップ６２５）。更に、新しいサーバーアドレスを含む制御サーバーからの応答は、第２認証コードも含むことができ、この第２認証コードはサービスサーバーに接続されたときにモニタデバイスを認証するのに使用できる。この認証コードは、制御サーバーが発生する暗号化／解読鍵とすることができる。この第２認証コードの目的は、メイン認証コードまたは鍵の分散を防止することである。その理由は、かかる分散によってコードの安全性が脅かされる可能性があるからである。

【００５４】

図５には、制御サーバー３０の一実施例が略図で示されている。モニタデバイス２０によって設定された自動接続は制御サーバーで分析され、制御サーバー３０は、制御サーバーに利用できる他のサーバーの情報およびモニタデバイス２０との通信で提供される情報に基づき、最も適切な新しいサーバーへのアドレスをモニタデバイス２０に提供する。制御サーバー３０は、ネットワーク通信を行うためのネットワークインターフェース３１０と、制御サーバー３０を作動させるための処理手段３１２と、処理手段３１２が実行するアプリケーションプログラムをサポートし、記憶するためのメモリ３１４と、モニタデバイス２０と制御サーバー３０との間の通信からモニタデバイスの識別子を抽出するための識別抽出器３１６と、モニタデバイス２０の識別コードを認証するための認証器３１７と、識別コードとサーバーとを照合するための照合手段３１８と、抽出された識別子に一致するサーバーに関連するアドレスを発生し、これを送るためのリコンフィギュレーションメッセージ発生器３２０とを含む。

【００５５】

識別抽出器３１６は、制御サーバー３０に接続するモニタデバイスのアドレスを抽出することにより、制御サーバー３０とモニタデバイスとの間の通信から識別子を抽出するようにでき、このアドレスは、例えばモニタデバイス２０のＩＰアドレスとすることができ

る。このＩＰアドレスは、モニタデバイスが接続されているネットワークの運用者（ｏｐｅｒａｔｏｒ）を識別するのに使用できる。各運用者は、割り当てられたシリーズのＩＰアドレスを有するので、このような識別が可能である。この抽出は、モニタデバイス２０から発信されるメッセージに含まれる応答アドレスをピンポイントするようになっているＩＰアドレス３２２の抽出器によって実行される。別の実施例によれば、識別抽出器３１６は、制御サーバー３０とモニタデバイス２０との間の通信においてモニタデバイス２０によって送られる識別コードおよび認証コードを抽出するようになっている識別コード抽出器３２４を含む。一実施例では、制御サーバー３０はＩＰアドレス抽出器３２２および識別コード抽出器３２４の双方を含み、異なる方式に従ってこれらを使用できる。すなわち識別抽出器はデータベース３３０内のＩＰアドレスを抽出してそれがサーバーに関連しているかどうかのテストを開始でき、関連していない場合、識別コードチェックを続けるか、または識別抽出器は識別コードの、そして次にＩＰアドレスの抽出およびテストを開始するようになっている。

【００５６】

照合手段３１８は、識別抽出器３１６が抽出した識別子を活用し、モニタデバイスに最も適したサーバーを探す。この照合手段３１８は、識別子のリストまたはデータベース３３０および関連するサーバーにアクセスすることにより、モニタデバイスの識別子とサーバーとを照合するようになっている。リストまたはデータベースのアクセスは、データベースアクセス手段３２６によって行われる。照合に使用されるリストまたはデータベース３３０は、サーバーへの周辺機器としてサーバー内に配置してもよいし、またはネットワークを介してアクセスするようにもできる。後者の実施例は図５に示されている。リストまたはデータベース３３０は一実施例によれば、識別子のエントリーを含むことができ、各識別子は、少なくとも１つの制御サーバーまたはサービスサーバーに関連する。リストまたはデータベース３３０は、モニタデバイス２０を認証するための各識別子に関連する鍵も含むことができる。当業者にはリストまたはデータベース３３０の別の構造も知られている。

【００５７】

リストまたはデータベース３３０にアクセスすることにより、モニタデバイス２０の識別子と、鍵と、モニタデバイス２０の識別子および鍵を制御サーバーまたはサービスサーバーに関連付ける情報のエントリーを含むデータベース３３０またはリストを編集できる。データベース３３０またはリストは、だれかが編集できるようにするためには認証を必要とし得る。リストまたはデータベース３３０のかかる編集は、多くの異なる方法で実行できる。例えばモニタデバイスの製造に関連してこの編集を実行でき、かかる場合、モニタデバイスの識別コードを入力し、所定のサービスプロバイダまたはサービスプロバイダのサーバーと関連付ける。編集は、サービスプロバイダのサーバーのうちの１つまたは一組に関連付けるべきモニタデバイスの識別コードをサービスプロバイダが入力することによって実行でき、この編集はサービスプロバイダがプロバイダのネットワークのＩＰアドレスを入力することによって実行でき、編集はこれらアドレスとプロバイダのサーバーのうちの１つまたは一組とを関連付けできる。

【００５８】

図６ａには、モニタデバイスにサービスする制御サーバー３０のプロセスの一実施例が示されている。制御サーバー３０は、ネットワークおよびネットワークインターフェース３１０を介し、モニタデバイス２０からの接続メッセージを受信する（ステップ７１０）。モニタデバイス２０および制御サーバー３０は、通信のための接続を設定する（ステップ７１２）。次に、制御サーバー３０の識別抽出器３１６は、通信からモニタデバイスに関連する識別子および認証コードを抽出する（ステップ７１４）。次に、認証コードの手段により、識別子の認証をチェックする（ステップ７１５）。認証に失敗した場合、プロセスを終了する（ステップ７１７）。失敗しなかった場合、識別子と、この特定の実施例ではサービスプロバイダとを照合する照合手段３１８により、識別子を処理する（ステップ７１６）。

【００５９】
サービスプロバイダが識別子と一致しなかった場合（７１８）、制御サーバー３０はエラーメッセージを発生でき（ステップ７２０）、接続メッセージに応答し、モニタデバイス２０へこのメッセージを戻す。モニタデバイス２０は、特定のエラーコードをディスプレイするか、または一部のＬＥＤを附勢し、エラーのタイプを表示するようにできる。
【００６０】
かかるエラーが発生した場合、ユーザーはどの当事者がサポートを提供するかに応じ、モニタデバイスまたはサービスプロバイダのサポートを通知でき、これら当事者はモニタデバイス２０に関連した正しいアドレスまたはモニタデバイス２０のＩＰアドレスを入力し、データベース内にモニタデバイスの識別子を入力し、これをサーバーなどに関連付けできる。
【００６１】
ステップ７１８において、サービスプロバイダが識別子に一致している場合、照合手段３１７は、そのサービスプロバイダのサーバーへのアドレスを検索する（ステップ７２２）。
【００６２】
次に、リコンフィギュレーションメッセージ発生器３２０へ検索されたサーバーアドレスが送られ、メッセージ発生器は検索されたサーバーアドレスを含むリコンフィギュレーションメッセージまたは別のタイプのメッセージを発生する（ステップ７２４）。次にステップ７２６で、リコンフィギュレーションメッセージがモニタデバイス２０へ送られ、モニタデバイスは図３～４を参照してこれまで説明したように、リコンフィギュレーションメッセージに作用する。制御サーバー３０は、モニタデバイス２０へ送るための第２認証コードも発生でき、この認証コードはリコンフィギュレーションメッセージに関連し、ステップ７２６でモニタデバイス２０へ送ることができる。第２認証コードは、サービスサーバーへの接続時にモニタデバイスを認証するのに使用できる。この認証コードは制御サーバーが発生する暗号化／解読鍵とすることができる。この第２認証コードの目的は、メイン認証コードまたは鍵の分散を防止することである。その理由は、かかる分散がコードの機密性を犯す恐れがあるからである。
【００６３】
図６ａに表示されているプロセスは、初期制御サーバー内で実施することが好ましい。すなわちモニタデバイスの製造中に、モニタデバイスに入れられたアドレスによってアドレス指定される制御サーバーのタイプにより実施することが好ましい。かかる制御サーバーはモニタデバイスのメーカーによって制御でき、かかる制御サーバーは、デバイスをだれが買うか、モニタデバイスに関連するのはどのサービスプロバイダであるかとは無関係に、同じプロセス、プログラムおよびプロパティを使って、メーカーが大きなシリーズのモニタデバイスを構成することを可能にできるという利点を提供できる。最初に制御サーバー３０に接続されるときに、モニタデバイスのプログラムおよびプロパティを自動的に変更し、サービスプロバイダまたはデバイスに関連する他の当事者からの特定のリクエストに従ってカスタム化することができる。かかる自動変更はリコンフィギュレーションメッセージ内でモニタデバイス２０へ送られる。
【００６４】
図６ｂに示されるように制御サーバーのプロセスの別の実施例を構成でき、このプロセスは図６ａの実施例のプロセスに類似するので、図６ａのプロセスと同じステップに対して同じ参照番号を使用する。異なるステップも同じ参照番号を使用するが、番号の後に’記号をつける。従って、図６ｂのプロセスは、最初にサービスプロバイダを照合することによるサーバーの照合をせずに、サーバーは識別子に直接照合されるという点が違う。従って、抽出された識別子とデータベース内のサーバーとが照合される（ステップ７１８’）。サーバーが見つかった場合（ステップ７１８’）一致したサーバーに関連するサーバーアドレスが検索される（ステップ７２２’）。このプロセスの他の部分は図６ａのプロセスと同一である。

【００６５】
図５、６ａおよび６ｂを参照して説明したサーバーに類似した制御サーバー３０は、初期制御サーバー３０として使用できる。更にかかる制御サーバー３０は、後のステージの制御サーバー３０として有効である。すなわちすべてではないにしても、初期制御サーバー３０によって利用されるデータベース３３０内にサービスプロバイダのサービスサーバーのアドレスを記憶した場合、初期制御サーバー３０がアドレスを提供できるサブシステム内に配置された制御サーバー３０、またはサービスプロバイダの制御サーバー３０として有効である。このように、異なる当事者がそれらの目的に従って異なる組のサーバーを管理できる。例えばモニタデバイスのメーカーが一組の初期制御サーバーを管理し、サービスプロバイダがサービスサーバーおよび可能な場合には一部の制御サーバーを管理する場合、メーカーはサービスプロバイダおよびサービスプロバイダのサーバーのサブセットの追跡を維持するだけでよく、一方、サービスプロバイダはデータベースおよびメーカーの制御サーバーへの変更を検討することなく、サービスサーバーを設定することが認められる。

【００６６】
システム内のサービスサーバー４０は、モニタデバイス２３０とユーザーターミナルとの間でユーザーインターフェースを提供するサーバーと見なすことができる。このサービスサーバー４０は、モニタデータをサービスサーバーに転送するためにモニタデバイスへサービス接続するようになっている。更に、このサービスサーバーはモニタデバイス２０から受信したデータを処理し、そのデータを提供するか、またはユーザーのクライアントが提供することを可能にするようになっている。サービスプロバイダ４０は、モニタデバイスを制御するようにもできる。サービスサーバーは、例えばモニタデバイスと通信し、ユーザーターミナル、例えばクライアントコンピュータ、モバイル電話などと通信するための通信手段を含むサーバーとし得る。更に、サービスサーバーは認証されたユーザーだけをモニタデバイスに接続するための認証手段を含むことができる。この認証は、標準的なユーザーネームおよびパスワードのログインとして実行できる。発送時にモニタデバイスと共にまずユーザーネームおよびパスワードを提供できる。更に、サービスサーバーはモニタデバイスからのモニタ情報を記憶するデータベースを含むことができる。かかるモニタデバイスは、カメラからのビデオシーケンス、例えばドア内のＩＲ検出器またはセンサからのアラームをトリガーすることに関連する事象とすることができる。このサービスサーバーはユーザーターミナルからのリクエストおよび認証時にカメラからユーザーターミナルへ実質的にライブのビデオストリームを送るようにもできる。

【００６７】
アクセス制限デバイス、例えばファイアーウォール、ＮＡＴ（ネットワークアドレス変換）、ダイナミックアドレスを提供するＩＳＰ（インターネットサービスプロバイダ）の背部に配置されたモニタデバイスへ制御パラメータ、データ、更新などの送信を達成するために、サービスサーバー４０はモニタデバイスから送られたリクエストに応答し、かかる情報を送るようにできる。モニタデバイス２０は通信を開始するようになっているので、このことを容易に達成できる。

【００６８】
一実施例では、サービスサーバー（図７参照）は、ネットワーク５０を通してモニタデバイスとの通信を可能にするネットワークインターフェース４１０と、サービスサーバーでアプリケーションを実行するための処理手段４１２と、アプリケーションデータを記憶するためのメモリ４１４と、モニタデータ提示手段４１６とを含む。サービスサーバーは、モニタデバイス２０とサービスサーバー４０との間の通信からモニタデバイスの識別子を抽出するための識別抽出器４１８と、モニタデバイス２０の識別コードを認証するための認証器２３４も含むことができ、サービスサーバー内の認証のために使用される認証コードは前記第２認証コードとすることができる。識別抽出器は更に、ＩＰアドレス抽出器４２０および／または制御サーバー３０内と同じ機能性を有する識別コード抽出器４２２を含むことができる。モニタデータ提示手段４１６は、１つまたは複数のモニタデバイス

からのモニタデータのプレゼンテーションをイネーブルするための、１つまたは複数のアプリケーションを備える。モニタデータを受信し、このデータを処理し、ユーザーのためのデータを提示する可能性を提供するサービスサーバーは、当業者に知られたものである。使用可能なサービスサーバー４０の一例は、スウェーデン、Ｓ２２３　６９　ルンド、エンダラベーゲン１４、アキシスＡＢ社により出願された国際特許出願第ＷＯ２００６／０７３３４８号に記載されており、この出願は、アクセス制限デバイスを介した通信のための方法についても述べている。

【００６９】

図８には、サービスサーバーの発明に関連するプロセスの一実施例が示されている。このサービスサーバー４０は、モニタデバイス２０から接続メッセージを受信し（ステップ８１０）、モニタデバイスを識別し、認証する（ステップ８１１）。次にサービスサーバーとモニタデバイスとがサービス接続を設定する（ステップ８１２）。サービス接続が設定されると、サービスサーバー４０は、サービスサーバー４０の条件または最終ユーザーの要求に従って、モニタデバイスからのモニタデータの受信（ステップ８１４）、および受信したモニタデータの処理（ステップ８１６）をスタートできる。次に、サービスサーバー４０は、ユーザーのクライアントのために提示するための、またはクライアントもしくはユーザーのサーバーにダウンロードするためのモニタデータを記憶できる（ステップ８１８）。クライアントはワークステーションコンピュータ、デスクトップコンピュータ、ラップトップコンピュータ、ハンドヘルドコンピュータ、例えばＰＤＡ（パーソナルデジアルアシスタント）、モバイル電話などでよい。

【００７０】

モニタデバイスをサービスサーバーに接続するためのシステムは、複数のモニタデバイス２０と、複数の制御サーバーと、複数のサービスサーバーとを含むことができる。モニタデバイスはネットワーク５０に直接、別のネットワークを介し、アクセス制限デバイスなどを介して接続できる。

【００７１】

図９において、このシステムの一例は、３つのモニタデバイス２０～２２、２つのサービスサーバー４０～４１およびユーザーターミナル４２および４４を含む。この例では、視覚的に異なるように見たカメラの２つの図およびモニタデバイスを示す１つの一般的なボックスを使用することにより、モニタデバイスのうちの２つをモニタカメラとして示している。我々はこのシステムにおけるモニタデバイスは、ブランド、タイプまたはモニタ機能に関して必ずしも同一でないことを強調したい。すなわちモニタシステムはＩＲ検出器、広角カメラ、低解像度カメラを同時に含むことができる。図９に示された例では、モニタデバイス２０～２２の数だけでなく、サービスサーバー４０～４１の数も容易に増加してもよい。更に、このシステム例は、メーカーによって制御される制御サーバーとすることができる制御サーバー３０を含む。

【００７２】

更に、モニタデバイス２２のうちの１つはアクセス制限デバイス６０、例えばファイアーウォール、ＮＡＴ（ネットワークアドレス変換）サーバー、ダイナミックアドレスを提供するＩＳＰ（インターネットサービスプロバイダ）、ファイアーウォールを介し、ネットワークに接続されている。かかるアクセス制限デバイスは、例えばモニタデバイスからのメッセージまたはリクエストに応答し、情報または命令を提供することにより、かかるデバイスを通過するようにモニタデバイスへ情報または命令を送るようになっているので、サーバーからのモニタデバイスのアクセスを制限しない。例えばモニタデバイスの各々とサーバーとの照合プロセス中に制御サーバー３０がアクセスするデータベースは、モニタデバイス２０のＩＰアドレスがサービスサーバー４０に提供するインターネットアクセスプロバイダのＩＰアドレスであるという事実に基づき、モニタデバイス２０のＩＰアドレスをサービスサーバー４０に関連付ける情報を含むことができる。更に、またはこれとは異なり、データベースはモニタデバイス２１および２２の各々から送られた識別コードと、サービスサーバー４１とを関連付ける情報を含むことができる。従って、制御サーバ

ーのデータアドレスがモニタデバイス２０～２２とそれらのサービスサーバーとを関連付ける情報を含む場合、制御サーバー３０は、モニタデバイスの各々が送る接続メッセージに応答し、サービスサーバー４０のアドレスをモニタデバイス２０へ送り、サービスサーバー４１のアドレスをモニタデバイス２１および２２へ送ることができる。前に説明したように、モニタデバイスで受信したアドレスを不揮発性メモリに記憶し、将来のイニシエイション時に使用することができる。例えばモニタデバイス２０の接続が外されており、再接続された場合にサービスサーバー４０のアドレスを不揮発性メモリに記憶し、モニタデバイスが接続メッセージを制御サーバー３０に送る代わりに直接、サービスサーバー４０へ送ることができる。ユーザーターミナル４２および４４は、ネットワークを介してサービスサーバーと通信し、カメラからのモニタ情報または画像シーケンスを入手するか、またはモニタデバイスを制御するようになっている。アクセス制限デバイス、例えばファイアーウォールを介してネットワークにモニタデバイスが接続されている場合、サービスサーバー４０のようなサーバーを介し、モニタデバイスにアクセスしなければならない。

【００７３】

図１０では、更に別の可能なコンフィギュレーションが示されている。この場合、すべてが保護された６０の個人ネットワーク５１に接続されているような、自らの建物をモニタするために多数のモニタデバイス２０を必要とする会社はサービスサーバーを直接個人ネットワーク５１にも接続すると仮定できる。ユーザーターミナル４２および４４は、提供されるモニタサービスにアクセスするため、および／またはユーザーのモニタデバイスにアクセスするために、サービスサーバーに接続されている。モニタデバイス２０を購入したとき、これらデバイスは制御サーバーに登録されており、会社の内部サービスサーバーのアドレスに関連するカメラのシリアル番号を取り込むことができ、制御サーバーは初期制御サーバーとなり得る。このように、カメラの設置は大幅に簡略化される。その理由は、モニタデバイス２０を取り付け、個人ネットワーク５１に接続するだけでよく、モニタデバイス２０は自動的に制御サーバー３０により、使用を意図するサービスサーバー４０を探し、これに接続するようにリコンフィギュアされるからである。

【００７４】

図１１において、システムの更に別のコンフィギュレーションが示されている。モニタサービスプロバイダのサービス、例えばネットワークアクセス、すなわちインターネットアクセスのプロバイダであると仮定する。メーカーの制御サーバー３０に関連するデータベースにＩＰアドレス、ＩＰアドレスの一部または複数のＩＰアドレスが記憶される。すなわち制御サーバー３０のデータベースにＩＰアドレスの多数の情報、またはサービスプロバイダのＩＰアドレスに接続されているとしてモニタデバイスを識別するのに必要な多数のＩＰアドレスがロードされる。サービスプロバイダは制御サーバー３１にも関連しており、制御サーバー３１はサービスプロバイダによって運用される制御サーバーである。サービスプロバイダは何らかの理由から、２つのサービスサーバー４０および４１をインストールしている。

【００７５】

サービスプロバイダの制御サーバー３１にはサービスサーバーによって維持されるデータベースが提供され、このデータベースには各モニタデバイス２２～２５をサービスサーバー４０～４１のどれに（即ち、どの１つに）接続しなければならないかに関する情報を含む。モニタデバイス２２～２５を制御サーバー３１内のサービスサーバー４０～４１に関連付ける情報は、上記のようにＩＰアドレスに基づいていもよいし、または特定のモニタデバイスを識別するユニークなコードに基づいてもよい。従って、モニタデバイス２４がサービスプロバイダ５２のネットワークに接続されるとき、モニタデバイスはサービスプロバイダ５２のネットワークおよび別のネットワーク５０を介して制御サーバー３０へ接続メッセージを送る。ネットワーク５０は制御サーバーが接続される相手の先のインターネット、ＬＡＮ、ＷＡＮまたは他の任意のネットワークでよい。

【００７６】

制御サーバー３０は、例えばＩＰアドレスと、サービスプロバイダおよび制御サーバー

３１とを照合し、制御サーバー３１に関連するアドレスをモニタデバイス２４へ送る。次にモニタデバイス２４は接続メッセージを制御サーバー３１へ送る。次に、制御サーバー３１はＩＰアドレスまたは別の識別子とサービスサーバー４１とを照合し、サービスサーバー４１に関連するアドレスをモニタデバイス２４へ送る。次に、モニタデバイス２４は接続メッセージをサービスサーバー４１へ送り、サービスサーバー４１によりサービス接続を設定できる。

【００７７】

モニタデバイス２５および２２は、サービスプロバイダおよびサービスプロバイダの制御サーバー３１に同じように関連させることができる。しかしながら、制御サーバー３１は制御サーバー３１のデータベース内のエントリーに応じ、モニタデバイス２５および２２の各々とサービスサーバー４０および４１の任意のいずれか１つとを関連付けできる。モニタデバイスを特定のサービスサーバーに関連付ける理由は様々であってよい。１つの理由は、中小企業に対しては、あるサービスサーバーを提供し、より安価なホームソリューションに対しては、あるサービスサーバーを提供し、大企業に対しては、あるサービスサーバーを提供し、可能な場合にはカスタムアプリケーションを構成するからである。

【００７８】

２つのモニタデバイス２０および２１は、サービスプロバイダのネットワークを介し、共通ネットワーク、例えばインターネットに接続されることはない。図では、これらモニタデバイスを何らかの方法でサービスプロバイダに関連付けできる。例えば制御サーバー３０は、制御サーバー３０とモニタデバイスの各々との間の通信中に、制御サーバー３０へ送られた識別子により使用するためのサービスプロバイダを識別できる。

【００７９】

図１１は、サービスプロバイダのネットワーク５１に接続されたログインサーバー６２も開示している。ユーザーがサービスプロバイダに識別コードおよびユーザー認証コードを提供し、サービスプロバイダが、サービスプロバイダに対する識別コードにより識別されたモニタデバイスに関連付けるための命令と共に、識別コードおよびユーザー認証コードを制御サーバー３０へ送るようになっている実施例において、ログインサーバー６２を使用する。認証コードの目的は、モニタデバイスに対するアクセスの不正な関連付けを禁止することである。ログインサーバー６２はスタンドアローンデバイスとすることができる。しかしながら、サービスプロバイダのサービスサーバー４０、４１または制御サーバー３１内で構成することも可能である。

【００８０】

図１２では、サービスサーバーにモニタデバイスを接続し、ユーザーがモニタデバイスにアクセスするためのシナリオの一例が示されている。このシナリオでは、モニタデバイスを製造し、製造プロセスにおいてモニタデバイス内にユニークな識別コードおよびユニークな鍵を記憶する（ステップ８１０）。この識別コードおよびユニークな鍵については、本明細書において前に記載したものである。メーカーは、制御サーバーのデータベース内に識別コードおよびユニークな鍵も記憶する（ステップ８１２）。次に、インターネットアクセスのオペレータまたは監視ソリューションを提供する会社に対し、制御サーバーのデータベース内で識別コードをユニークな鍵を関連付ける（ステップ８１４）。これら会社のうちのいずれかに対するモニタデバイスの関連付けは、会社がモニタデバイスを購入した結果、または契約の結果として行われる。次に、ユーザーはカメラを購入し、恐らく監視サービスの一部としてモニタデバイスに関連する会社を取り扱い、カメラをネットワークに接続する（ステップ８１６）。モニタデバイス、制御サーバーおよびサービスサーバーは、本明細書で前に説明した実施例のうちのいずれかのステップを実行し、最終的にサービスサーバーへのサービス接続を行う（ステップ８１８）。サービス接続が起動され、作動すると、ユーザーはサービスの口座またはモニタデバイスを識別することにより、ユーザーターミナルからサービスサーバーへログインできる（ステップ８２０）。ユーザーはユーザー認証コードなどと組み合わせたモニタデバイスの識別子を入力することにより、ユーザーネームおよびユーザー認証コードを入力することによりログインできる。

ユーザーがログインすると、ユーザーはサービスサーバー内に記憶されたモニタデバイスからデータにアクセスし、モニタデバイスからライブのデータにアクセスするか、またはモニタデバイスに命令を送ることができる。

【００８１】

図１３において、サービスサーバーにモニタデバイスを接続し、ユーザーがモニタデバイスにアクセスできるようにするためのシナリオの別の例が示されている。このシナリオでは、モニタデバイスを製造し、製造プロセスにおいてユニークな識別コードおよびユニークな鍵をモニタデバイス内に記憶する（ステップ９１０）。識別コードおよびユニークな鍵については、本明細書で既に説明した通りである。メーカーも、制御サーバーのデータベース内に識別コードおよびユニークな鍵を記憶する（ステップ９１２）。ユーザーはカメラを購入し、これをネットワークに接続する（ステップ９１４）。ユーザーはカメラが提供する識別コードおよびユーザー認証コードを使ってサービスプロバイダのサイトにもログインする（ステップ９１６）。サービスプロバイダによって識別コードおよびユーザー認証コードが受信されると、サービスプロバイダはユーザーが入力した識別コードおよびユーザー認証コードを含む命令を制御サーバーに送り、識別コードに関連し、認証コードに対して有効な鍵を有するモニタデバイスを、命令を送信したサービスプロバイダに関連付ける（ステップ９１８）。ステップ９１６および９１８の後で、モニタデバイスをネットワークに接続するステップ９１４を実行できる。モニタデバイス、制御サーバーおよびサービスサーバーは、本明細書の前で説明した実施例のうちのいずれかのステップを実行し、最終的にサービスサーバーへのサービス接続を行う（ステップ８１８）。サービス接続が起動され、作動すると、ユーザーはサービスの口座またはモニタデバイスを識別することにより、ユーザーターミナルからサービスサーバーへログインできる（ステップ８２０）。ユーザーはユーザー認証コードなどと組み合わせたモニタデバイスの識別子を入力することにより、ユーザーネームおよびユーザー認証コードを入力することによりログインできる。ユーザーがログインすると、ユーザーはサービスサーバー内に記憶されたモニタデバイスからデータにアクセスし、モニタデバイスからライブのデータにアクセスするか、またはモニタデバイスに命令を送ることができる。

【００８２】

図１４にはサーバーから別のサーバーにモニタデバイスをハンドオーバーする一例が示されている。本願に関連し、モニタデバイスのハンドオーバーとは、モニタデバイスと通信中のサーバーがモニタデバイスにアドレスを提供し、モニタデバイスが受信したアドレスのサーバーに接続メッセージを送り、よってモニタデバイスが前のサーバーによって与えられた新しいサーバーと通信し始めることである。この図では、各矢印は、矢印が生じているサーバーが矢印の先のサーバーのアドレスをモニタデバイスに送り、次にモニタデバイスが接続メッセージをこのサーバーに送ることを示している。

【００８３】

図１２から、多数の異なる構造を構成するのに本発明のシステムを使用できることが、図１２から明らかであり、これら構造は必要であれば容易に変更できる。理解を容易にするために、図には限られた数のサーバーが示されているが、サーバーのうちの少なくとも一部は、恐らく図に示されている数よりも多いサーバーへの言及を含むことができる。

【００８４】

図１２の構造例では、システムは２つの初期制御サーバーを含む。例えば制御サーバー３０：１と、制御サーバー３０：２を含む。これらサーバーの双方は、初期のメーカーのサーバーでよい。すなわち製造中にモニタデバイス内にあらかじめプログラムされたアドレスを有するサーバーでよい。制御サーバー３０は、本発明による制御サーバー３０以外のサーバーとしては働かないようになっているサーバー、例えば制御サーバー３０：１でよいが、制御サーバーは他のタスクを同時に実行してもよい。すなわち制御サーバーは、別のタイプのサーバーとして同時に、かつ別の目的のために働くことができる。更に、前に説明したように、制御サーバーは同じサイト、同じ部屋または同じキャビネット内に配置されたサービスサーバー４０を有する制御サーバー３０として、例えば制御サーバー３

０：２、３０：３および３０：６として構成できる。更に、制御サーバー３０は組み合わせた制御サーバー３０およびサービスサーバー４０として、例えば制御サーバー３０：４、３０：７として構成できる。更に、初期制御サーバー３０は、図には示されていない組み合わされた制御サーバー３０とサービスサーバー４０として構成できる。

【００８５】

上記のように、制御サーバー３０：１および３０：２の双方は、モニタデバイスのメーカーまたはかかるモニタシステムのサービスおよび管理全体を提供することに関心を有する他の当事者によって管理される初期制御サーバー３０でよい。図１２およびシステムの機能および利点の理解を容易にするために、制御サーバーからのハンドオーバーのパスをフォローする。モニタデバイスはインストールされ、イニシエイトされる際に自動的に制御サーバー３０：１に接続される。すなわち制御サーバー３０：１のアドレスは、デバイスの製造に関連し、モニタデバイス内に記憶されたアドレスのリストの最優先度アドレスとなっている。この例では、制御サーバー３０：１に関連するデータベースだけが、２つのエントリーを含む。一方のエントリーは、サービスプロバイダの制御サーバー３０：３へのアドレスを含み、他方のエントリーは、サービスプロバイダの制御サーバー３０：４へのアドレスを含む。モニタデバイスの識別子とサービスプロバイダの制御サーバー３０：３とが一致していると仮定する。この場合、制御サーバー３０：１は制御サーバー３０：３のアドレスをモニタデバイスに送り、モニタデバイスは制御サーバー３０：３に接続メッセージを送る。サービスプロバイダの制御サーバー３０：３において、モニタデバイスの識別子と、データベース、このときはサービスプロバイダのデータベース内のエントリーとをもう１回照合する。モニタデバイスと最も適したサービスサーバー４０：１～４０：３、または更に別の制御サーバー３０：６～３０：７とを照合する。これらサーバーは、図のハンドオーバーの矢印に従って使用できるサーバーである。この例では、制御サーバーとモニタデバイスをサービスサーバー４０：３とを照合し、このサービスサーバーのアドレスをモニタデバイスに送る。次にモニタデバイスおよびサービスサーバーは上記のようにサービス接続を設定する。

【００８６】

モニタシステムにはバックアップサーバー、例えばシステム内に冗長性を提供する制御サーバーを容易に、かつ好ましく設けることができる。かかるバックアップサーバーはすべてのレベルで構成できる。例えば初期制御サーバーおよびより低いレベルの制御サーバーの双方に対して構成できる。このバックアップサーバーは専用バックアップサーバーでもよいし、通常別の領域または他のユーザーにサービスする制御サーバーでもよい。

【図面の簡単な説明】

【００８７】

【図１】本発明に係わるモニタシステムの該略図である。

【図２】本発明の一実施例における信号発生のタイミング略図である。

【図３ａ】本発明の一実施例に係わるモニタデバイスのブロック略図である。

【図３ｂ】本発明の一実施例に係わるモニタデバイスとして作動するビデオカメラのブロック略図である。

【図４ａ】本発明の一実施例に係わるモニタデバイスのプロセスの略フローチャートである。

【図４ｂ】本発明の別の実施例に係わるモニタデバイスのプロセスの略フローチャートである。

【図５】本発明の１つの様相に係わる制御サーバーのブロック略図である。

【図６ａ】本発明の一実施例に係わる制御サーバーのプロセスの略フローチャートである。

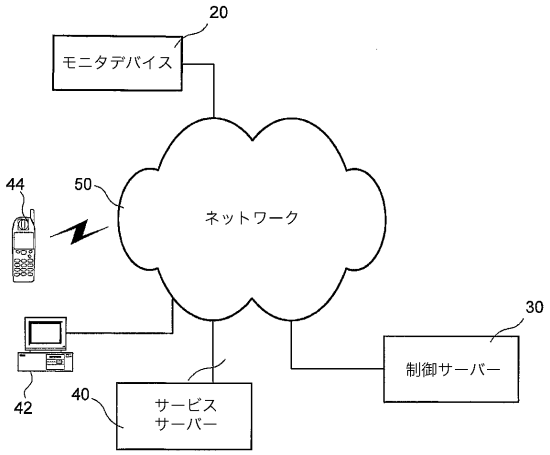
【図６ｂ】本発明の別の実施例に係わる制御サーバーのプロセスの略フローチャートである。

【図７】本発明の一実施例に係わるサービスサーバーのブロック略図である。

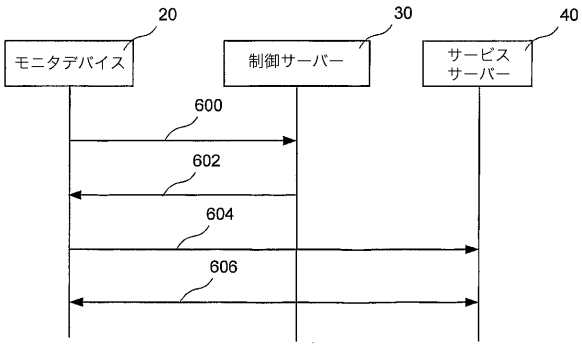
【図８】本発明の一実施例に係わるサービスサーバーのプロセスの略フローチャートであ

る。
【図９】本発明に係わるモニタシステムのコンフィギュレーションに関する略図である。
【図１０】本発明に係わるモニタシステムの別のコンフィギュレーションに関する略図である。
【図１１】本発明に係わるモニタシステムの更に別のコンフィギュレーションに関する略図である。
【図１２】モニタデバイスをサービスサーバーに接続し、モニタデバイスにユーザーアクセスするためのシナリオの概略フローチャートである。
【図１３】モニタデバイスをサービスサーバーに接続し、モニタデバイスにユーザーアクセスするための別のシナリオの概略フローチャートである。
【図１４】本発明に係わるモニタシステムの可能なコンフィギュレーションにおける可能なハンドオーバーの関係に関する略図である。

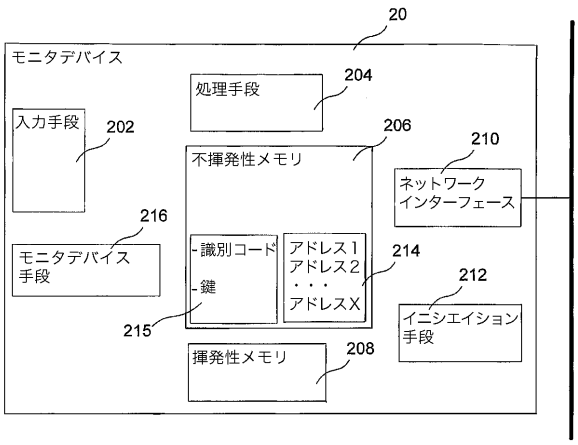
【図１】



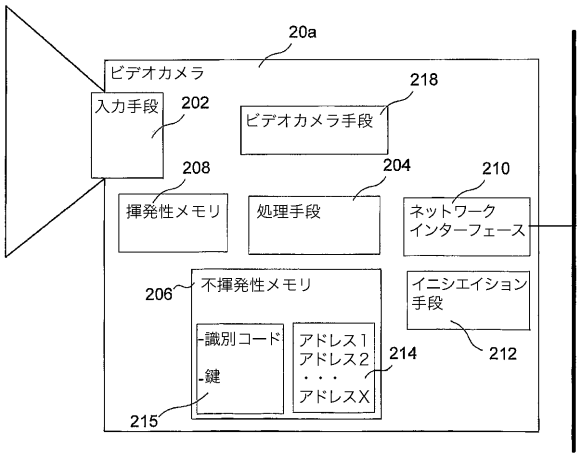
【図２】



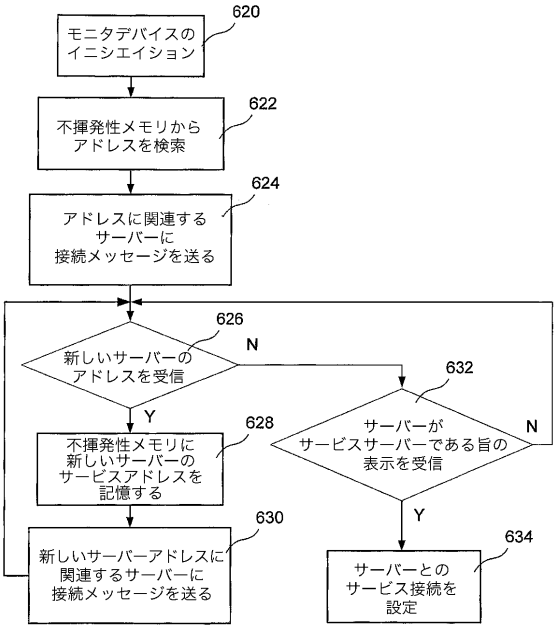
【図３ａ】



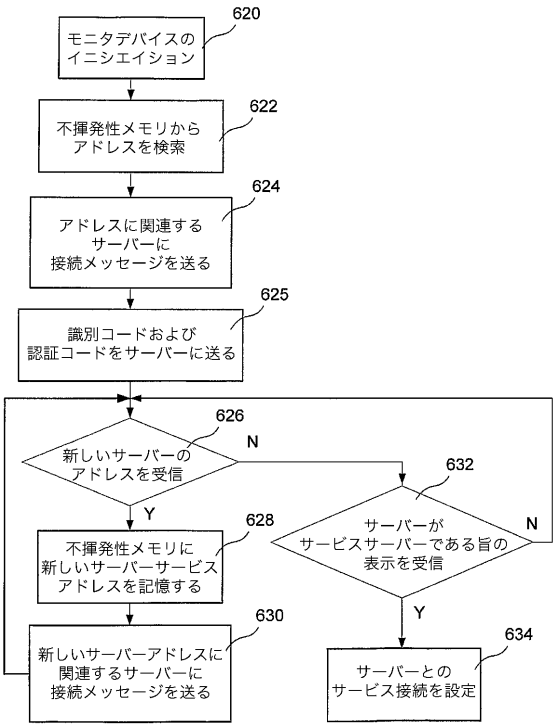
【図３ｂ】



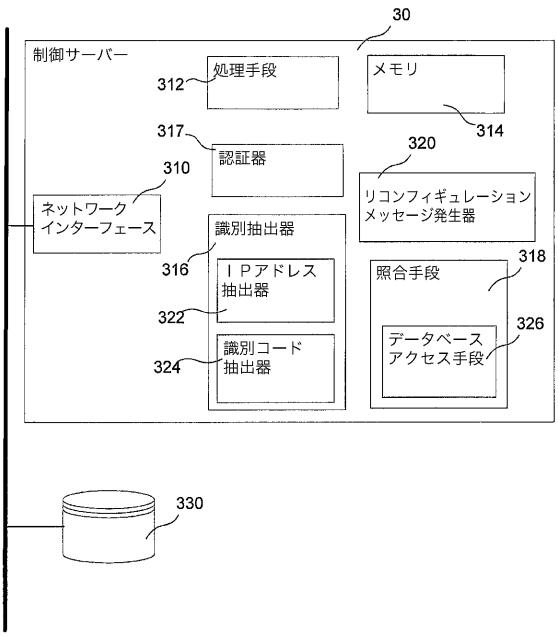
【図４ａ】



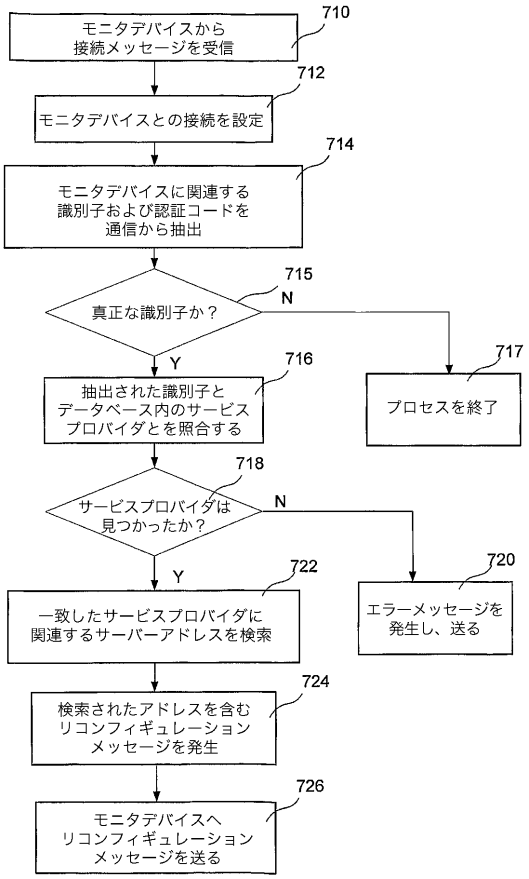
【図４ｂ】



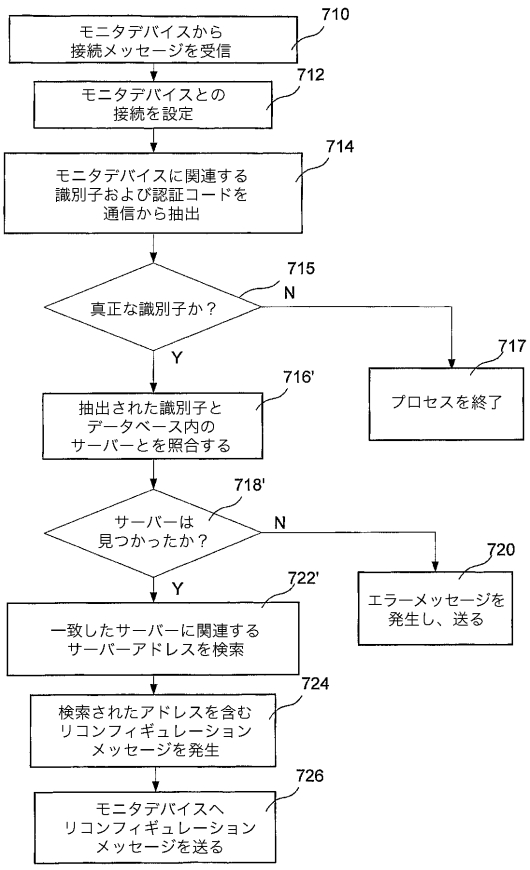
【図５】



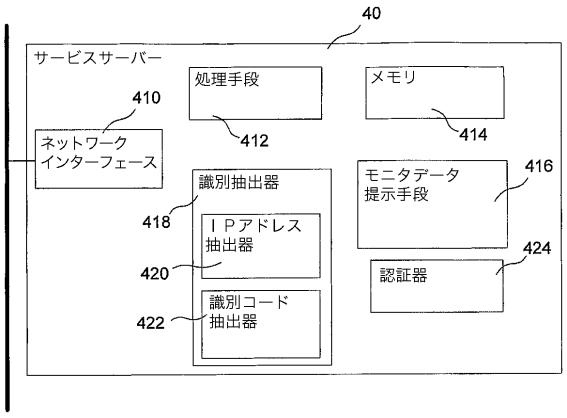
【図６ａ】



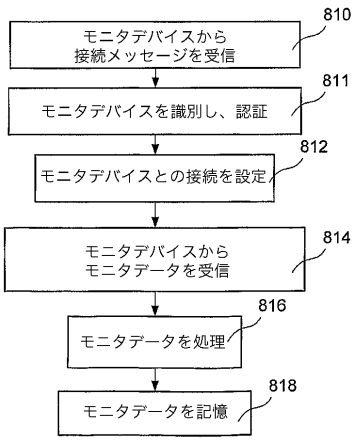
【図６ｂ】



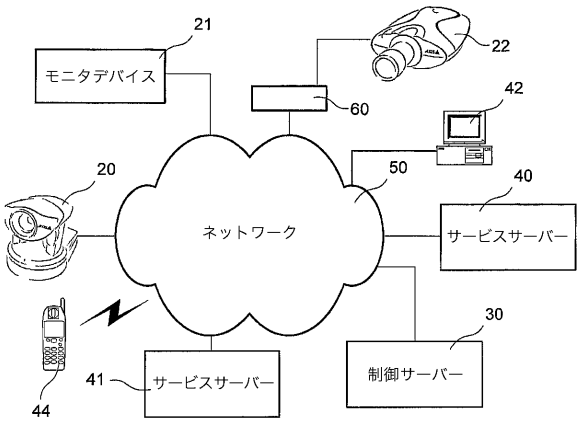
【図７】



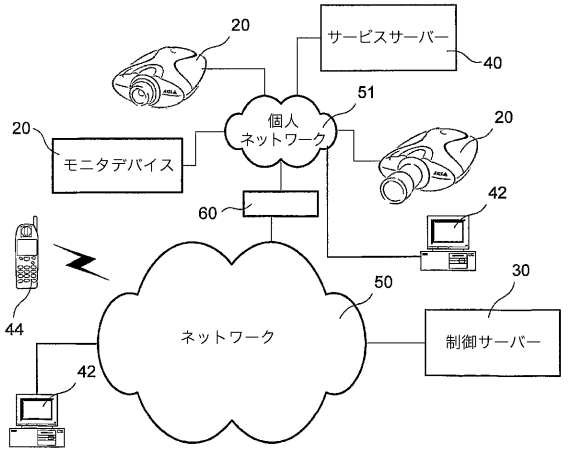
【図８】



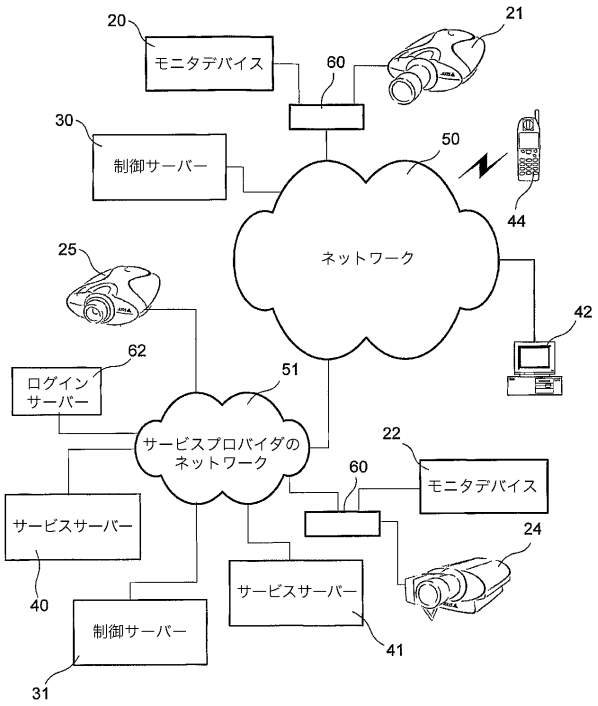
【図９】



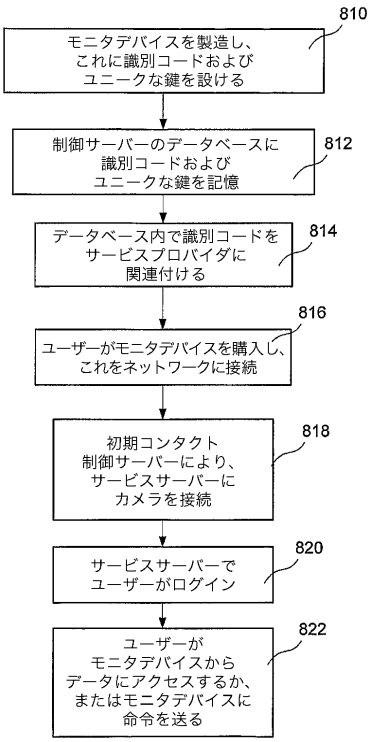
【図１０】



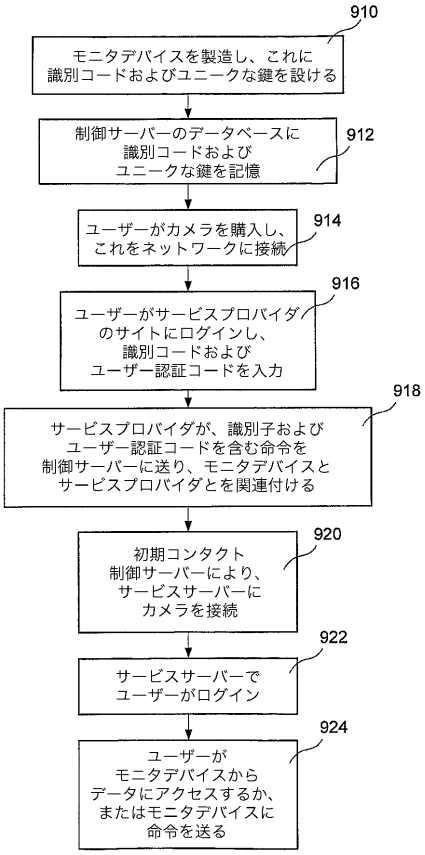
【図１１】



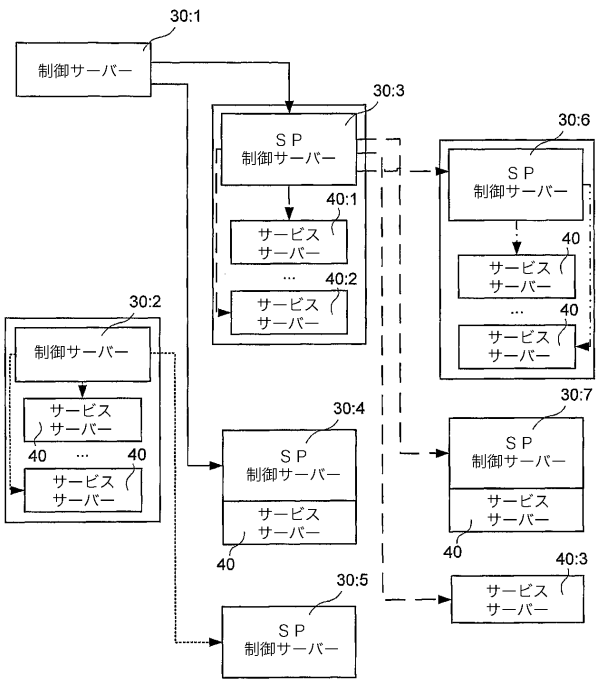
【図１２】



【図１３】



【図１４】



フロントページの続き

(74)代理人 100094673
弁理士 林 鈺三
(72)発明者 トゥルベルグ、ヨアキム
スウェーデン国、ルンド、ボーフスベーゲン 9
(72)発明者 アドルフソン、ヨハン
スウェーデン国、セドラ サンドビー、 クロッカレベーゲン １５ ジー
(72)発明者 グレン、マーティン
スウェーデン国、マルメ、ベレシェグスベーゲン ５０ エイ

審査官 小林 義晴

(56)参考文献 特開２００２－３２８８５６（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F 13/00