

令和3年3月16日判決言渡

令和元年（行ケ）第10141号 審決取消請求事件

口頭弁論終結日 令和3年1月19日

判 決

5

原 告 イッツ・コミュニケーションズ株式会社

同訴訟代理人弁護士 吉 田 和 彦

同 高 石 秀 樹

10

同 外 村 玲 子

同 岸 慶 憲

同訴訟代理人弁理士 須 田 洋 之

同 山 崎 貴 明

15

被 告 株 式 会 社 ア イ ペ ッ ク ス

同訴訟代理人弁護士 宍 戸 充

同訴訟代理人弁理士 重 信 和 男

同 堅 田 多 恵 子

20

同 林 道 広

同 林 修 身

同 大 久 保 岳 彦

主 文

1 原告の請求を棄却する。

25

2 訴訟費用は原告の負担とする。

事 実 及 び 理 由

第1 請求

特許庁が無効2018-800034号事件について令和元年9月18日にした審決を取り消す。

第2 事案の概要

5 1 特許庁における手続の経緯等

(1) 被告は、発明の名称を「通信回線を用いた情報供給システム」とする発明について、平成13年6月22日を出願日とする国際特許出願(PCT/JPO1/05380)に係る国内移行の特許出願(特願2002-505473号、以下「原出願」という。)をしたが、平成15年4月18日、原出願の一部を新たな特許出願とした出願(特願2003-114428号)をし、
10 さらに、平成15年8月13日、同出願の一部を新たな特許出願とした出願(特願2003-207491号)をし、さらに、平成15年12月17日、同出願の一部を新たな特許出願とした出願(特願2003-419617号)をした上で、さらに、平成17年2月15日、同出願の一部を新たな特許出願とした出願(特願2005-37081号、以下「本件出願」という。)をし、
15 同年7月22日、その設定登録(特許第3701963号。請求項の数1。)を受けた(甲2, 3, 17, 83。以下この登録を受けた特許を「本件特許」という。))。

(2) 原告は、平成30年3月23日、本件特許について特許無効審判を請求し
20 (甲33)、特許庁は、上記請求を無効2018-800034号事件として審理した上で、令和元年9月18日、「本件審判の請求は、成り立たない。」旨の審決(以下「本件審決」という。)をし、その謄本は、同月30日、原告に送達された。

(3) 原告は、令和元年10月25日、本件審決の取消しを求める本件訴訟を
25 提起した。

2 特許請求の範囲の記載

本件特許の特許請求の範囲の記載（本件審決において分説された後のもの）は、次のとおりである（以下「本件発明」といい、本件特許の明細書を図面を含めて「本件明細書」という。）。

【請求項 1】

- 5 《 1 A 》 インターネットや電話網からなる通信回線網の中に設置されている管理コンピュータに於ける通信回線を用いた情報供給システムであって、
- 《 1 B 》 前記管理コンピュータ側には、監視目的に応じて適宜選択される監視手段を有する監視端末側に対して付与された I P アドレスおよび監視端末 I D を含む監視端末情報が、利用者 I D に対応付けられて登録されている利用者データベースを備え、
- 10 《 1 C 》 前記監視端末は前記管理コンピュータ側と前記通信回線網を介して接続可能とされており、
- 《 1 D 》 前記管理コンピュータ側は、
- 《 1 D i 》 インターネットや電話網からなる通信回線網を利用してアクセス
- 15 してくる利用者の電話番号、I D 番号、アドレスデータ、パスワード、さらには暗号などの認証データの内少なくとも一つからなる利用者 I D である特定情報を入手する手段と、
- 《 1 D ii 》 この入手した特定情報が、前記利用者データベースに予め登録された監視端末情報に対応するか否かの検索を行う手段と、
- 20 《 1 D iii 》 前記特定情報に対応する監視端末情報が存在する場合、インターネットや電話網からなる通信回線網を利用して、この抽出された監視端末情報に基づいて監視端末の制御部に働きかけていく手段と、
- 《 1 D iv 》 インターネットや電話網からなる通信回線網を経由して、前記監視端末によって得られた情報を入手する手段と、
- 25 《 1 D v 》 この監視端末から入手した情報を、インターネットや電話網からなる通信回線網を用いて、前記特定情報を送信してアクセスした利用者へ供

給する手段と、

《 1 D vi 》 管理コンピュータ側と監視端末側との回線再接続時、特定できる監視端末側からの I P アドレス登録要求を受け付け、前記利用者データベースの前記監視端末情報である I P アドレスを登録処理する手段と、を備え、

5 《 1 E 》 前記監視端末側は、

内部にメモリーされた管理コンピュータ側のグローバル I P アドレスに対して自ら接続処理する自己接続機能と、

前記自己接続機能を使って、登録された前記監視端末 I D を管理コンピュータ側に送り、前記監視端末側の I P アドレスを登録するように要求する手段と、

10

《 1 F 》 を備えていることを特徴とする通信回線を用いた情報供給システム。

3 本件審決の理由の要旨

(1) 本件審決の理由のうち、本件における取消事由に係る部分の理由の要旨は、①本件発明と原出願の優先日前に頒布された刊行物である国際公開第 00/36807 号公報（甲 1）に記載された発明（以下「甲 1 発明」という。）との相違点は実質的なものであるから本件発明は新規性を欠如せず、②同相違点は当業者が容易に想到することができたとはいえず、本件発明は甲 1 発明に基づいて容易に発明することができたものとはいえず、進歩性を欠如しないというものである。

15

20

(2) 本件審決が認定した甲 1 発明、本件発明と甲 1 発明の一致点及び相違点は、次のとおりである。

ア 甲 1 発明

（ア）遠隔カメラの画像にアクセスするための暗号化 V P N（仮想私設網）であって、

25

（イ）保育所、例えば、センタ 1（130）、センタ 2（132）、セン

5

タN（134）と，センササーバ110との間，及び，センササーバ110とモニタ140における認証された観察者との間の通信は，公衆交換電話網（PSTN）などのパケット交換網を用いることによって促進され，電話事業者（Telco）アクセス装置，例えば，ルータ，DSLモデム，ISDNモデム・ルータ，ケーブルモデム，MLPPP（マルチリンク・ポイント・ツー・ポイント）モデムなどの利用を通じて，センタ130において，情報が公衆交換電話網（PSTN）に渡され，また，公衆交換電話網（PSTN）から取り出され，このデータは，長距離電話の会話や，企業データ，公開のインターネットのデータなどとともに，PSTN上を移動し，

10

（ウ） システム100は，2つの主要なネットワーク・セグメントを含み，

第1のネットワーク・セグメント120は，保育所，例えば，センタ130と，センササーバ110との間のリンクから構成され，

15

第2のネットワーク・セグメント120'は，センササーバ110と認証された観察者，例えば，コンピュータ322，326，329との間のリンクから構成され，

20

第1のネットワーク・セグメント120は，センタ，例えば，130から始まり，入りネットワーク接続（例えばDSL，ISDN）316は電話事業者アクセス装置388に接続され，例示的な電話事業者アクセス装置は，paradyne社HotWire5446型DSLモデム，型番5446-a2-200-0rm，3Com社56k MLPPPスイッチ，型番3c430000，Netgear社ISDNモデム，型番RT328が含まれ，

25

電話事業者アクセス装置388は，次に，暗号化装置386，例えば，Ravlin-4有線暗号化装置に，10base-Tケーブルで接続

され、

暗号化装置 386 は、それからハブ 382、例えば、イーサネット 10base-T 非スイッチングハブに、10base-T ケーブルで接続され、

5 ハブ 382 は、次に、1 台以上のカメラサーバ 380（遠隔センササーバ）、例えば、Axis 社 240 型、又は、200/200+ 型カメラに、10base-T ケーブルで接続され、

Axis 社のカメラサーバ 380 の各々は、電源供給及びメディアアグリゲータ装置 374 に、RCA 型ケーブルを介して接続され、

10 カメラ 370、371、372 のそれぞれは、メディアアグリゲータ 374 に、75Ω 映像用同軸ケーブルで接続され、

(エ) 他のレベルやタイプの暗号化方式を利用でき、

暗号化を、他のハードウェアデバイスで置き換えたり、ソフトウェアを利用することができ、

15 (オ) システム 100 の最上位レベルの動作フロープロセス 400 について、

スタート状態 402 から始まって、プロセス 400 は、ユーザが Web ブラウザ、例えば、ユーザのブラウザ 2 (522) にシステム 100 の WWW アドレスをタイプ入力することで、システムの Web サイトにアクセスする状態に移行し、

20

ここで応答は、Web サイトのホームページを構成する情報であって、要求と応答は、セグメント 120' を介して転送され、

状態 410 において Web サイトの情報領域をブラウジングでき、ユーザはホームページの任意のリンクをクリックして、リンクが向けられた情報を見ることができ、

25

ユーザが「親のログイン用」ボタンをクリックすると、プロセス 40

0は状態412に進み、ここでWebサーバ350は、応答として、クライアントコンピューティング装置上で実行中のブラウザ522とのセキュアな128ビットSSL接続を開始して、センタコード、ユーザ名、パスワード用のスペースを備えたログイン画面を生成し、

5 (カ) 状態412において、ユーザは、認証を実行するのに必要なデータ、例えば、センタコード、ユーザ名、パスワードを提供することで応答し、これらのデータは、線528上でデータベースサーバ360に送信され、

10 そして、データベースサーバ360は、そのセンタコードによりデータベース362にアクセスし、データベースサーバ360は、その特定のセンタについてのユーザ名及びパスワードの組み合わせの全てをチェックして、ユーザが入力したユーザ名を検索し、そして、判断状態414に進み、パスワードが比較され、

15 (キ) 判断状態414に戻り、ユーザ名とパスワードがデータベース362にあるユーザ名とパスワードと一致した場合、プロセス400は状態420に移動して、ユーザは、ウェブサイトのセキュアな部分について認証され、

20 (ク) データベース362は、データベースサーバ360によってアクセスされるものであって、他の全てのサーバに対して認証データとユーザ情報を提供するために使用され、Webサーバ350は、このデータベースに照会して、ある親がどのカメラの使用が許可されているかを判定し、ユーザ名やパスワードなどのログイン情報を検証し、

25 (ケ) データベースサーバ360が、ユーザ名とパスワードが有効であることを肯定したと仮定すると、Webサーバは、第1に、特定のユーザがアクセス可能なカメラ名のリストをデータベース・サーバ360に問い合わせ、ページの左下ペインに単にそれらのカメラ名を表示し、We

5 b サーバ 3 5 0 は、特定のカメラのリンクに対する要求を受信した後、データベースサーバ 3 6 0 に問い合わせ、特定のユーザが、カメラにアクセスできることを確認し、アクセスできるならば、Web サーバ 3 5 0 は、画像サーバ 3 3 0 のセンサ・プロセスへの要求によって画像の取得を開始すると同時に、配信サーバ 3 4 0 のユーザ・プロセスへの要求によって画像の配信を開始し、

10 (コ) 画像取得プロセスにおいて、画像取得プロセス 6 0 0 は、休止又は非アクティブ・モードになることはなく、常に画像サーバ 3 3 0 上で動作し、プロセス 6 0 0 は、スタート状態 6 0 2 で開始して、画像を取得する契機を受信する状態 6 0 4 に遷移し、

 センサ・スレッドは、カメラ／センサのアドレスが契機で特定されたカメラ／センサに対するサービスを提供するものであり、

15 状態 6 1 4 に進んで、プロセス 6 0 0 は選択されたセンサにアクセスし、それから、状態 6 1 6 において、画像を取得し、その画像、例えば、画像 5 1 2 を、データ記憶媒体 3 6 2 に格納し、

20 (サ) 画像サーバ 3 3 0 は、HTTP（ハイパーテキスト転送プロトコル）を用いて保育所のカメラへの接続を作成し、接続が作成できない場合、画像サーバ 3 3 0 は、（簡単に変更可能な）所定の時間間隔だけ待機してから、再試行を行い、画像サーバ 3 3 0 が、所定の回数だけ接続の作成に失敗した場合、カメラがダウンしていることを通知する一つの画像をユーザにまず表示した後に、その努力を終え、

25 (シ) このプロセスのどの段階でも、画像サーバ 3 3 0 がサイズが 0 である画像を受信したり、所定のログイン名とパスワードを用いてもカメラにログインできない場合、Telnet プロトコルによりカメラにログインしてリセット・コマンドを発行し、通常、これによって、カメラの有するどのような問題も解決し、

(ス) 画像発送プロセス 700 について、

プロセス 700 は、配信サーバ 340 上で実行される永続的なユーザ
プロセスであり、画像を取得して保管するプロセス 600 が動作中、遠
隔クライアント (Web ブラウザを有するユーザ) に画像を発送するプ
ロセス 700 も動作し、プロセス 700 もまた、外部ソースからの契機、
例えば、ウェブ・サーバ 350 からの要求を受け取り、プロセス 700
は、この契機に対して、取得プログラムが画像を投入するデータストア
362 の保管領域から、最新の画像を取り込み、そして、それを遠隔ク
ライアントに送信することで応答し、

(セ) 制限されたアクセスとして、システムの保育所に入所している子
を持つ親だけが、その保育所のカメラを見るためにアクセスするためのア
カウントが発行され、また、カメラへのアクセスは、カメラが設置され
た部屋にいる子を持つ親に限定され、

(ソ) ユーザが「センタコード」を入力したとき、特定の保育所が決定され
るが、どんなときも、そのセンタが実際の名称によって特定されること
はなく、また、カメラの実際のネットワークアドレスが明らかにされる
こともなく、これによって、不道德な意図を持つ認証されていないユー
ザが、彼らが見ている子供の居場所を特定することを困難にする、

(タ) VPN 監視システム 100。

イ 本件発明と甲 1 発明の一致点及び相違点

(ア) 一致点

《1A》 インターネットや電話網からなる通信回線網の中に設置されて
いる管理コンピュータに於ける通信回線を用いた情報供給システムであ
って、

《1B'》 前記管理コンピュータ側には、監視目的に応じて適宜選択さ
れる監視手段を有する監視端末に関する、監視端末 ID を含む監視端末

情報が、利用者 I D に対応付けられて登録されている利用者データベースを備え、

《 1 C 》 前記監視端末は前記管理コンピュータ側と前記通信回線網を介して接続可能とされており、

5 《 1 D 》 前記管理コンピュータ側は、

《 1 D i 》 インターネットや電話網からなる通信回線網を利用してアクセスしてくる利用者の電話番号、 I D 番号、アドレスデータ、パスワード、さらには暗号などの認証データの内少なくとも一つからなる利用者 I D である特定情報を入手する手段と、

10 《 1 D ii 》 この入手した特定情報が、前記利用者データベースに予め登録された監視端末情報に対応するか否かの検索を行う手段と、

《 1 D iii 》 前記特定情報に対応する監視端末情報が存在する場合、インターネットや電話網からなる通信回線網を利用して、この抽出された監視端末情報に基づいて監視端末の制御部に働きかけていく手段と、

15 《 1 D iv 》 インターネットや電話網からなる通信回線網を経由して、前記監視端末側によって得られた情報を入手する手段と、

《 1 D v 》 この監視端末側から入手した情報を、インターネットや電話網からなる通信回線網を用いて、前記特定情報を送信してアクセスした利用者に供給する手段と、

20 を備えている

《 1 F 》 ことを特徴とする通信回線を用いた情報供給システム。

(イ) 相違点

a 相違点 1

25 本件発明では、「前記管理コンピュータ側には、監視目的に応じて適宜選択される監視手段を有する監視端末側に対して付与された I P アドレスおよび監視端末 I D を含む監視端末情報が、利用者 I D に対

応付けられて登録されている利用者データベースを備え」る（構成要件 1 B）のに対し、甲 1 発明では、前記管理コンピュータ側には、監視端末側に対して付与された I P アドレスおよび監視端末 I D を含む監視端末情報が、利用者 I D に対応付けられて登録されている利用者データベースを備えることが特定されていない点。

b 相違点 2

本件発明では、「前記管理コンピュータ側は」，「管理コンピュータ側と監視端末側との回線再接続時、特定できる監視端末側からの I P アドレス登録要求を受け付け、前記利用者データベースの前記監視端末情報である I P アドレスを登録処理する手段」を備え（構成要件 1 D vi），「前記監視端末側は」，「内部にメモリーされた管理コンピュータ側のグローバル I P アドレスに対して自ら接続処理する自己接続機能と、前記自己接続機能を使って、登録された前記監視端末 I D を管理コンピュータ側に送り、前記監視端末側の I P アドレスを登録するように要求する手段」を備える（構成要件 1 E）のに対し、甲 1 発明では、管理コンピュータ側に、回線再接続時、I P アドレス登録要求を受け付けて、I P アドレスを登録処理する手段を備え、監視端末側に、自己接続機能と、登録処理するように要求する手段を備えることが特定されていない点。

4 取消事由

- (1) 甲 1 発明を主引用例とする新規性判断の誤りの有無（取消事由 1）
- (2) 甲 1 発明を主引用例とする進歩性判断の誤りの有無（取消事由 2）

第 3 当事者の主張

1 取消事由 1（甲 1 発明を主引用例とする新規性判断の誤りの有無）について

(1) 原告の主張

本件審決は、前記第 2 の 3 (2)イ(イ)のと通りの相違点を認定したが、本件

発明と甲１発明との間に相違点はなく，本件審決の相違点の認定には誤りがある。

ア 相違点１の認定について

5 本件発明は，管理コンピュータ側のいずれかの記憶部に記憶されている監視端末側のＩＰアドレスが利用者ＩＤに「対応付けられて」いればよいところ，これは何らかの形で両者が紐付けられるなど一定の関係にあれば足り，そのような場合は，「利用者データベース」を備えるといえる。

10 そして，甲１発明において，センササーバ１１０のどこかの記憶部にセンタ１３０のグローバルＩＰアドレスが記憶されていなければ，センササーバ１１０とセンタ１３０との間でインターネット通信を行うことは不可能であるから，「アクセス装置３３８」等にセンタ１３０のグローバル
15 ＩＰアドレスが登録されているはずであるところ，「アクセス装置３３８」等と「データベース３６２」とは相互に情報を交換し合ってセンタ１３０の監視端末との間でのインターネット通信を可能とするから，両者は一定
20 の関係にあるといえ，「データベース３６２」と「アクセス装置３３８」等とを合わせた集合体は，本件発明における管理コンピュータ側にあるデータベースとみることができる。そして，「アクセス装置３３８」などに登録されたセンタ１３０側（「監視端末側」）に対して付与されたＩＰアドレスは本件発明の「ＩＰアドレス」に相当し，また，「データベース３
25 ６２」に登録された「センタコード」又は「カメラ名」は，本件発明１の「監視端末ＩＤ」に相当し，「データベース３６２」に登録された「ユーザ名」は本件発明の「利用者ＩＤ」に相当する。そうすると，甲１発明は「利用者データベース」を備えているといえる。

イ 相違点２の認定について

25 本件発明の構成要件１Ｄvi及び１Ｅは，ＤＨＣＰ（「Ｄｙｎａｍｉｃ Ｈｏｓｔ Ｃｏｎｆｉｇｕｒａｔｉｏｎ Ｐｒｏｔｏｃｏｌ」。ＩＰアドレ

5 スを動的に割り当てるためのプロトコル。)により動的IPアドレスを用いたならば当然に備えているはずの手段、すなわち、回線再接続時、監視端末側から管理コンピュータ側に対するIPアドレスの登録要求を受け付けこれを登録処理する手段、及び、監視端末側から管理コンピュータ側に接続処理する自己接続機能とこの機能により管理コンピュータ側に登録された監視端末側のIPアドレスを変更するよう要求する手段を規定しているところ、本件審決は、甲1発明では、そのような回線再接続時のIPアドレス登録処理手段や監視端末側の自己接続機能や登録処理する要求手段を備えることが特定されていないとして、甲1発明が動的IPアドレスを用いることを否定し、本件発明と甲1発明とは相違点2の点において相違すると認定した。しかしながら、次のとおり、再接続のために監視端末側から接続処理をする自己接続機能や、変更された監視端末側のIPアドレスを管理コンピュータ側で登録処理することは、甲第1号証に開示されているに等しい事項か、又は、少なくとも示唆されている事項であるから、相違点2に係る本件発明の構成（構成要件1Dvi, 1E）は、実質的な相違点を構成しない。

10 (ア) 甲1発明における「電話事業者アクセス装置388」の例示として「3Com社56k MLPPPスイッチ、型番3c430000」及び「Netgear社ISDNモデム、型番RT328」が挙げられている（甲1の8頁24行ないし9頁8行目）。

20 「3Com社56k MLPPPスイッチ、型番3c430000」の紹介記事には、「Typically, the ISP assigns a single IP address via Dynamic Host Configuration Protocol」（インターネットサービスプロバイダは、通常、DHCPにより単一のIPアドレスを割り当てる。）と記載されているから（甲53の92頁右上欄の1ないし6行目）、「型番3c430000」の「電話事業者アクセス装置388」を用いる甲1発明にお

いて、動的 I P アドレスを用いることができる。

「N e t g e a r 社 I S D N モデム，型番 R T 3 2 8」のインストール・ガイドには，「If you are obtaining an ISDN account with an Internet service provider (ISP), order a single-user account that provides a single static or dynamic IP address unless you have a need for registered IP addresses.」（あなたがインターネット・サービス・プロバイダ（I S P）の I S D N アカウントを得ている場合，あなたが登録された I P アドレスを必要としていない限り，静的 I P アドレス又は動的 I P アドレスを提供する単一のユーザ・アカウントをオーダーしなさい。）と記載されているから（甲 5 4 の 6 頁），「型番 R T 3 2 8」の「電話事業者アクセス装置 3 8 8」を用いる甲 1 発明においては動的 I P アドレスを用いることができる。

（イ） 甲第 1 号証には，「例えば，R a v l i n - 4 有線暗号化装置に，1 0 b a s e - T ケーブルで接続される。」との記載（8 頁 2 4 行ないし 9 頁 8 行目）や「電話事業者アクセス装置 3 8 8」接続されているリンク 3 1 6 が V P N リンクであることが示されている（図 3）から，センタ 1 3 0 とセンササーバ 1 1 0 とのリンク 3 1 6 は「R a v l i n - 4」が採用する I P S e c に基づいて V P N 通信を実現するものである（甲 1 2 の 1 頁左欄第 2 段落下から 3 行から末行まで）ところ，I P s e c に基づく V P N 通信においては動的 I P アドレスが用いられる（甲 1 3，2 0 の 1 の 2 9 7 頁，2 0 の 2 の 2 8 5 頁，2 2 の 3 3 頁，2 5 の 3 頁，2 6 の 1 3 3 頁，2 8 の 1 3 6 頁）。

（ウ） 本件特許の優先日当時，I P s e c や，V P N で I P s e c を用いることは周知であり（甲 7 3 の 2 頁，7 4 の 6 2 ～ 6 3 頁，7 5 の 4 頁・7 頁，1 0 頁，甲 7 6 の 6 頁の図 6），I P s e c における自己接続機能も周知であった（甲 2 0 の 1 の 2 9 7 頁・3 0 2 頁・3 0 3 頁，

21の6-25頁～6-26頁，22の16頁，23の6頁，77の115頁の表1，118頁の表3，78，79の111頁，80の1～5）。

上記のような周知の自己接続機能の技術がある場合，複数のセンタと1つのセンササーバ110を備える構成の甲1発明において，センササーバ110と複数のセンタの内の1つとの接続が途切れて再度接続を行うとき，センササーバ110が複数のセンタの内の1つがいずれであるかを調査し，センササーバ110から調査により決定した1つのセンタに接続を行うことは，処理が複雑となるが，接続が途切れたセンタ側から1つしか存在しないセンササーバ110に接続を行うことは，明らかに単純な処理となる。そうすると，このようなセンタ側からセンササーバ110への接続の処理は，当業者であれば当然に採用する構成である。

(エ) 甲第1号証には「入りネットワーク接続（例えばDSL，ISDN）316」との記載があるが（8頁24行～9頁8行目），「DSL」においては，通常，電話事業者アクセス装置のIPアドレスは動的IPアドレスであった（甲55の2頁・4頁，56の155頁の図1，57の6頁，58の12頁右欄，59の36頁，甲60の11頁左欄，61）。また，「ISDN」においても，通常，電話事業者アクセス装置のIPアドレスは動的IPアドレスであった（甲62，63の86頁，64の208頁，65の54頁）。

(オ) 本件特許の優先日当時，IPアドレスの枯渇問題が広く懸念されており，IPアドレスの節約を行うために，DHCPにより動的IPアドレスを利用することが推奨されていた（甲68の1頁左欄，69の209頁，70の71頁，71の1頁・7頁，甲72の1頁右欄）。

ウ 小括

以上のとおり，本件審決における相違点の認定には誤りがあり，本件発

明と甲 1 発明との間には相違点が存しないから、本件発明は甲 1 発明である。

そうすると、本件発明が新規性を欠如するものではないとした本件審決の判断には、誤りがある。

したがって、本件審決は取り消されるべきである。

(2) 被告の主張

本件審決の相違点の認定には誤りはない。

ア 相違点1の認定について

10 甲 1 発明のセンササーバ 1 1 0 の「アクセス装置 3 3 8」等の記憶装置にセンタ 1 3 0 の「アクセス装置 3 8 8」の I P アドレスが記憶されているとしても、甲第 1 号証には、その「アクセス装置 3 8 8」の I P アドレスがユーザ名に対応付けられてデータベースとして登録されている点については、記載も示唆もない。

そして、甲 1 発明においては、ユーザ名及びパスワードからなる利用者 I D は認証用に用いられるにすぎず、甲第 1 号証に「このようにして、複数のユーザが特定のカメラを見ている、カメラとの接続は 1 つだけになる。」（13 頁 7 ～ 8 行目）との記載があるとおり、複数のユーザが特定のカメラを見ているてもそのカメラとの接続は 1 つだけでよいのだから、わざわざ、センタ 130 側に対して付与されたグローバル I P アドレスを（動的 I P アドレス・静的 I P アドレスのいずれであっても）ユーザ名及びパスワードのそれぞれに対応付けて記憶するという構成を採用する必要がない。また、甲 1 発明においては、V P N を利用して、端末が互いにあたかもプライベートネットワークで接続されているようにみえるようにしているため、V P N 内の装置は、互いにプライベート I P アドレスで他の装置を特定するのが通常であり、相手端末の特定に必要なないグローバル I P アドレスを（動的 I P アドレス・静的 I P アドレスのいずれであ

っても) をユーザ名に対応付ける意味もない。

したがって、甲 1 発明において、センササーバ 1 1 0 の「アクセス装置 3 3 8」などの記憶部に記憶されているセンタ 1 3 0 の I P アドレスがユーザ名と紐付けられていると理解することはできない。

5 イ 相違点 2 の認定について

前記アのとおり、甲 1 発明において、センササーバ 1 1 0 の「アクセス装置 3 3 8」等の記憶部に記憶されているセンタ 1 3 0 の I P アドレスがユーザ名と紐付けられているとの記載はなく、また、そのように構成する必要もないから、動的 I P アドレスであろうと静的 I P アドレスであろうと、甲 1 発明が「前記利用者データベースの前記監視端末情報である I P アドレスを登録処理する手段」(構成要件 1 D vi) を備えていないことは明らかである。また、甲第 1 号証にはセンタ 1 3 0 側からセンササーバ 1 1 0 へ接続する処理についての記載はないし、このような自己接続機能は本件特許の優先日当時の周知技術ではなかったから、構成要件 1 E に係る相違点 2 の認定にも誤りはない。

15 ウ 小括

以上のとおり、本件審決における相違点の認定に誤りはなく、本件発明と甲 1 発明との間には相違点 1 及び相違点 2 が存するから、本件発明は甲 1 発明ではない。

20 そうすると、本件発明が新規性を欠如するものではないとした本件審決の判断には、誤りはない。

したがって、原告主張の取消事由は理由がない。

2 取消事由 2 (甲 1 発明を主引用例とする進歩性判断の誤り) について

(1) 原告の主張

25 仮に、本件発明と甲 1 発明とが相違点 1 及び相違点 2 の点において相違するとしても、相違点 1 は本件特許の優先日当時の技術水準・周知技術から容

易想到であり，前記 1 (1)イの事情からすると，センササーバ 1 1 0 のいずれかの記憶部に記憶されたセンタ 1 3 0 の I P アドレスとして，静的 I P アドレスではなく動的 I P アドレスを用いることや，センタ 1 3 0 側からセンササーバ 1 1 0 へ接続処理をすることは当業者に容易に想到できた。

5 そうすると，相違点 1 及び相違点 2 を容易想到ではないとした本件審決の判断には，誤りがある。

したがって，本件審決は取り消されるべきである。

(2) 被告の主張

10 甲第 1 号証において，センタ 1 3 0 側の I P アドレスとして動的 I P アドレスを用いるという技術思想は，開示も想定もされておらず，仮に，動的 I P アドレスを用いるとしても，その動的 I P アドレスをユーザ名に対応付ける必要性がないから，そのような構成を採用する動機付けもないことからすると，甲 1 発明において，相違点 1 に係る「監視端末側に対して付与された I P アドレスおよび監視端末 I D を含む監視端末情報が，利用者 I D に対

15 応付けられて登録されている利用者データベース」（構成要件 1 B）を備え，かつ，相違点 2 のうち，構成要件 1 D iv に係る「前記利用者データベースの前記監視端末情報である I P アドレスを登録処理する手段」を備える構成とすることは容易想到ではない。また，甲第 1 号証にはセンタ 1 3 0 側からセンササーバ 1 1 0 へ接続処理をすることについての記載はないし，この

20 ような自己接続機能は本件特許の優先日当時の周知技術ではなかったから，構成要件 1 E に係る相違点 2 の構成も容易に想到することができない。

したがって，相違点 1 及び相違点 2 を容易想到ではないとした本件審決の判断には，誤りはなく，原告主張の取消事由は理由がない。

第 4 当裁判所の判断

25 1 本件明細書の記載事項について

本件明細書（甲 8 3）には，別紙 1 「本件明細書の記載事項」のと通りの記

載事項があり、これによると、本件明細書には、本件発明に関し、次のとおりの開示があることが認められる。

(1) 本件発明は、通信回線を用いて監視端末が設置された特定領域を、利用者が所有する電話やパソコン等の情報端末を用いて、外出先からでも監視することを可能とする通信回線を用いた情報供給システムに関するものである（【０００１】）。現状の警備システムとして、所定のセンサー等を配備し、そのセンサーの反応による警備会社への通報で警備会社の警備員がその家屋に急行するシステムがあるが、加入契約料が一般大衆にとって多大なものとなっており（【０００３】，【０００４】），通信回線を利用して、必要な時に限らず、頻繁に断続的にでも特定領域である例えば自宅内の様子を監視できるようにしたいといった要求がある（【０００５】）。

しかしながら、これら監視システムにおいては、監視端末に通信回線を介して特定以外の人間がアクセスして監視領域の画像等の監視情報を入手することができてしまうと、プライバシーが保護されなくなってしまうという問題があり、これら特定者以外の第三者が監視端末より監視情報を入手することが不可能なシステムが切望されていた（【０００６】）。

本件発明は、上記した問題点に着目してなされたもので、常時接続回線を利用しているにも関わらず、特定者以外の第三者が監視端末より監視情報を入手することがきわめて困難で、かつ登録された利用者には、きわめて迅速に必要な監視情報を供給できるようにした通信回線を用いた情報供給システムを提供することを目的としている（【０００７】）。

(2) 上記目的を達成するために、本件発明は請求項１の構成をとった（【０００８】）。

(3) 本件発明の実施例としての監視システムは、登録している多数の利用者が個々に監視したい場所、例えば自宅等の被監視領域に設置される監視端末４と、該監視端末４並びにサービス利用者が所有する情報端末とに通信回線網

5を介してデータ通信可能に接続されたサービス提供者が所有する管理コンピュータ3と、各監視端末側と基本的に常時接続されたインターネットサービスプロバイダー（ISP）である中継サーバ6と、監視サービスの利用者が操作するパソコン14やノートパソコン15や携帯電話11等の情報端末と、から主に構成され（【0011】，【図1】），監視端末4は、主に通信回線網5を介してサービス提供者が所有する前記管理コンピュータ3と原則、常時接続され（【0012】），監視端末4を構成する（【0012】）監視ユニット1は通信部71を有しており、監視ユニット1側にはIPアドレスが割り当てられており、管理コンピュータ3と常時接続状態であるため、このIPアドレスが監視領域の特定用に利用されることになる（【0020】）。

(4) 管理コンピュータ3は、①利用者からの接続による認証処理や、該利用者IDに対応して登録されている監視端末のIPアドレス（ここではグローバルIPアドレス）を検索する処理等を実施可能な演算能力に優れた中央演算処理装置（CPU）31や、②磁気ディスクや光磁気ディスクから成り、利用者を識別可能な識別符号（ID）に、該利用者の暗証番号並びに該利用者が監視したい場所に設置されている監視端末に付与されている前記したIPアドレスを対応付けている利用者データベース（なお、IDの基になるデータは利用者の電話番号、ID番号、アドレスデータ、パスワード、さらには暗号、人体の一部の違いを表現する指紋など）等が記憶されている記憶装置35等が接続されている（【0021】，【図5】）。

(5) 管理コンピュータ3側においては、利用者Aの前記携帯電話11より送信されてきた利用者IDと暗証番号とを、記憶装置35に記憶されている利用者データベースの登録データと比較し、比較が一致して正規利用者と判断された場合において、管理コンピュータは、利用者に対応する監視端末又は監視ユニットが複数あるか否かを検索し、複数ある場合、利用者に対してアク

セス可能な監視端末又は監視ユニットの種類やメニューを表示し、得たい情報の選択を促すようになっている。つづいて利用者データベースを用いて検索エンジンで検索を行い、この利用者データベースに利用者IDに対応付けて登録されている監視端末側のIPアドレス（常時接続のISPが割り振っているアドレス）を抽出し、例えば利用者Aに対応するものが監視端末4aである場合、該当する監視端末4aを構成する監視ユニット1に対して、通常常時接続状態のインターネット回線を利用して監視端末側のIPアドレスに特別な制御信号（コマンドデータ）を送信する。管理コンピュータ3がコマンドデータである制御信号を送信したことにより、各監視端末4から送信されてくる画像情報などは、監視端末側に振られたIPアドレスや所定のIDとが登録された利用者データベースを利用して処理される（【0026】，【0029】，【0030】，【図7】）。

2 「甲1の記載事項」について

甲第1号証には、別紙2「甲1の記載事項」のと通りの記載事項があり（訳は本件審決，甲84，乙1による。），これによると，本件審決が認定する前記第2の3(2)ア（甲1発明）のと通りの開示事項があると認められる。

3 取消事由1（甲1発明を主引用例とする新規性判断の誤りの有無）について

(1) 相違点1の認定について

ア 本件発明1の「利用者データベース」について

（ア）前記第2の2の特許請求の範囲の記載のとおり，構成要件1Bの「利用者データベース」は，管理コンピュータ側に備えられるものであり，「監視端末側に対して付与されたIPアドレスおよび監視端末IDを含む監視端末情報」が「利用者ID」に「対応付けられて登録」されているものと規定されている。

また，管理コンピュータ側は，「利用者の電話番号，ID番号，アドレスデータ，パスワード，さらには暗号などの認証データの内少なくとも

も一つからなる利用者 I D である特定情報」を入手し(構成要件 1 D i),
「この入手した特定情報が, 前記利用者データベースに予め登録された
監視端末情報に対応するか否かの検索を行」い(構成要件 1 D ii), 「前
記特定情報に対応する監視端末情報が存在する場合, …この抽出された
5 監視端末情報に基づいて監視端末側の制御部に働きかけていく」(構成
要件 1 D iii) と規定されている。

そうすると, 特許請求の範囲の記載からは, 「利用者データベース」
は, 記憶媒体の種類や構成等の限定は付されていないものの, 入手する
特定情報から, あらかじめ登録された監視端末情報を検索することがで
10 き, 入手した特定情報に対応する監視端末情報が存在する場合に当該監
視端末情報に含まれる I P アドレスを抽出し得る程度に, I P アドレス
および監視端末 I D を含む監視端末情報が利用者 I D に「対応付けられ
て登録されている」ものと理解することが相当である。

(イ) そこで, 次に, 本件明細書の記載をみると, 前記 1 のとおり, 本件発
15 明の実施例において, 「利用者データベース」は, 磁気ディスクや光磁
気ディスクからなる記憶装置 3 5 に記憶され, 利用者の電話番号, I D
番号, アドレスデータ, パスワード, 暗号, 指紋等を基にした利用者を
識別可能な符号である利用者 I D に, 該利用者の暗証番号並びに該利用
者が監視したい場所に設置されている監視端末に付与されている I P ア
20 ドレスを対応付けているものであり(【0 0 2 0】, 【0 0 2 1】, 【図
5】), 利用者の認証の際に参照されるとともに, 利用者がアクセス可
能な監視端末のグローバル I P アドレスを検索抽出するために参照され
るものとされている(【0 0 2 6】, 【0 0 2 9】, 【0 0 3 0】, 【図
7】)。

25 本件明細書の記載によっても, 「利用者データベース」は, 利用者を
識別できる情報(「利用者 I D」)に, 当該利用者が監視したい場所に

5 設置されている監視端末に付与されたグローバル I P アドレス（「監視
端末情報」）が検索できる程度に対応付けられることを要するものと理
解される（なお、実施例における記憶媒体の種類は単なる例示であるこ
とが明らかであるから、やはり、本件発明において、「利用者データベ
ース」の記憶媒体の種類や構成等に限定が付されたものと理解すること
はできない。）。

（ウ） 以上からすると、本件発明の「利用者データベース」は、利用者を
識別できる情報に、監視端末側に付与された I P アドレス等の情報が、
検索できる程度に対応付けて登録されていることを要するものの、それ
10 で足り、記憶媒体の種類や構成等が具体的に限定されているものではな
いと解されるが、利用者を識別できる情報と I P アドレスとが関連性な
く記憶され、両者がシステム動作中に単にあい続いて利用されているだ
けの関連性しか有しない場合には、前記(ア)において説示した意味合い
において、当該監視端末情報に含まれる I P アドレスを抽出し得る程度
15 に、I P アドレスを含む監視端末情報が利用者 I D に「対応付けられて
登録されている」ものということとはできないから、「利用者データベ
ース」が構成されているとはいえないと解するのが相当である。

イ 甲 1 発明における I P アドレスの記憶について

（ア） 甲 1 発明において、センタ 1 3 0 とセンササーバ 1 1 0 との間のリ
20 ンク 1 2 0 は、公衆交換電話網（P S T N）を横切る暗号化 V P N とな
っており（甲 1 の 4 頁 1 2 行ないし 5 頁 7 行目），そして、入りのネッ
トワーク接続 3 1 6 は電話事業者アクセス装置 3 8 8 に接続され、電話
事業者アクセス装置 3 8 8 は暗号化装置 3 8 6 に接続され、暗号化装置
3 8 6 はハブ 3 8 2 に接続され、ハブ 3 8 2 はカメラサーバ 3 8 0 に接
25 続され、カメラサーバ 3 8 0 はメディアアグリゲータ 3 7 4 に接続され、
メディアアグリゲータ 3 7 4 はカメラ 3 7 0 ～ 3 7 2 に接続されている

(同 8 頁 2 4 行ないし 9 頁 8 行目)。また、センササーバ 1 1 0 の画像サーバ 3 3 0 はインターネットプロトコルを用いた HTTP, T e l n e t で、保育所 (センタ 1 3 0) に配置されたカメラ (3 7 0, 3 7 1, 3 7 2) と通信を行う (同 1 6 頁 2 3 ないし 2 6 行目, 1 6 頁 3 2 ないし 3 5 行目)。

甲第 1 号証には、I P アドレスが記憶される記憶部に関する記載はないが、センササーバ 1 1 0 は、インターネットプロトコルを用いてセンタ 1 3 0 に配置されたカメラと通信を行うものであるから、宛先アドレスとしてセンタ 1 3 0 側に付与されたグローバル I P アドレスを必要とすることや、センタ 1 3 0 内の装置相互は通常プライベート I P アドレスで他の装置を特定することからみて、甲 1 発明において、センササーバ 1 1 0 のどこかの記憶部が、センタ 1 3 0 のアクセス装置 3 8 8 又はその先の暗号化装置 3 8 6 に付与されたグローバル I P アドレスを記憶していると認められる。

(イ) ここで、甲 1 発明は、ユーザがログインボタンをクリックするとプロセスは状態 4 1 2 に進み (1 1 頁 2 8 行ないし 1 2 頁 7 行目, 図 4), 状態 4 1 2 において、ユーザが「センタコード」, 「ユーザ名」, 「パスワード」を提供し、データベースサーバ 3 6 0 がデータベース 3 6 2 にアクセスし、その特定のセンタについてのユーザ名及びパスワードの組合せの全てをチェックして、ユーザが入力したユーザ名を検索し、パスワードを比較することによりユーザの認証を行い (1 2 頁 8 ないし 1 4 行目), W e b サーバ 3 5 0 は、センタコードにより識別されるセンタにおいて、特定のユーザが見ることのできるカメラ名のリストを得るために、データベース 3 6 2 をチェックすることをデータベースサーバ 3 6 0 に対して要求し、認証されたユーザに対して当該ユーザがアクセス可能なカメラ名のリストを表示するものであり (1 2 頁 1 8 ないし 2

6 行目, 図 4) , W e b サーバ 3 5 0 は, 特定のカメラのリンクに対する要求を受信した後, データベースサーバ 3 6 0 に問い合わせ, 特定のユーザがカメラにアクセスできることを確認し, アクセスできるならば, W e b サーバ 3 5 0 は, 画像サーバ 3 3 0 のセンサ・プロセスへの要求によって画像の取得を開始すると同時に, 配信サーバ 3 4 0 のユーザ・プロセスへの要求によって画像の配信を開始し (1 4 頁 9 ないし 2 2 行目) , 「If more than one user is trying to view images from that particular camera, the image server 330 does not contact the camera additional times, but rather the distribution server 340 just establishes more connections between the data storage 362 and the authorized viewers.」 (1 3 頁 4 - 7 行目。 (訳) 「複数のユーザがその特定のカメラからの画像を見ようとする場合, 画像サーバ 3 3 0 は, カメラに追加で接触するのではなく, むしろ, 配信サーバ 3 4 0 は, データストレージ 3 6 2 と認証視聴者との間のより多くの接続を確立する。」) , 「このようにして, 複数のユーザが特定のカメラを見ても, カメラとの接続は 1 つだけになる。」 (1 3 頁 7 - 8 行目) という構成になっている。

このように, 甲 1 発明は, 特定のセンタについてユーザの認証をし, 当該特定のセンタにおいて当該ユーザがアクセスできるカメラ名のリストを表示し, 当該ユーザがアクセスできるカメラの画像を当該ユーザに配信するものであるから, データベース 3 6 2 には, センタコードとユーザ名とパスワードとアクセス可能なカメラ名が対応付けられて記憶されていると理解することはできる。また, 甲 1 発明において, センタ 1 3 0 側に付与された I P アドレスをセンササーバ 1 1 0 側が記憶する場合, 直接対応するセンタコード又はアクセス対象であるカメラ名に対応付けて I P アドレスが記憶されていると理解するのが自然である。

他方、甲第1号証には、ユーザ名又はパスワードと、センタ130側に付与されたIPアドレスとを対応付けているとする記載はない。その上、上記の甲1発明の構成によれば、ユーザ名又はパスワードと、センタ130の電話事業者アクセス装置388又は暗号化装置386に付与されたIPアドレスとを対応付ける必要性はないから、甲1発明においてそのような対応付けがされていることを甲第1号証から読み取ることができない。

ウ 以上からすると、甲1発明については、本件発明の「監視端末情報」に相当するセンタコードと本件発明の「利用者ID」に相当するユーザ名、パスワードとが対応付けられて登録されているデータベースを有することは認められるが、監視端末側に対して付与された「IPアドレス」と「利用者ID」とが対応付けられていないから、この対応付けを登録したデータベースは存在しないことになる。そうすると、甲1発明は、前記ア(ウ)で示した「当該監視端末情報に含まれるIPアドレスを抽出し得る程度に、IPアドレスを含む監視端末情報が利用者IDに「対応付けられて登録されているもの」ということはできないから、本件発明は、本件審決の認定する相違点1の点において甲1発明と相違する。そして、本件発明は、「利用者データベース」を備え、「利用者データベース」の監視端末情報であるIPアドレスを登録処理する手段を備えることによって、登録された利用者に迅速に必要な監視情報を供給できるなどの作用効果を奏するものであるから（本件明細書【0007】、【0008】）、相違点1は実質的なものである。

エ 原告の主張について

原告は、本件発明の「利用者データベース」は、管理コンピュータ側のいずれかの記憶部に記憶されている監視端末側のIPアドレスと利用者IDとが紐付けられるなど一定の関係にあればよく、甲1発明の「アクセ

ス装置 338」等と「データベース 362」とは相互に情報を交換してインターネット通信を可能としているから、この両者を合わせた集合体が本件発明の「利用者データベース」に相当する旨主張する。

5 本件発明の「利用者データベース」は、前記アのとおり解釈すべきものであるところ、確かに、甲 1 発明において、センササーバ 110 の「データベース 362」に記憶されているセンタコード、ユーザ名、ユーザパスワード、カメラ名と、センササーバ 110 中に記憶されたセンタ 130 側に付与された IP アドレスとは、それらがあいまって利用されることでセンタ 130 のカメラ 370～372 の画像をセンササーバ 110 が入手
10 できることになるから、両者は無関係とはいえない。しかしながら、両者はただ単にあい続いて利用されたというだけであり、IP アドレスが直接に対応付けられているのはセンタコード又はそれぞれのカメラ名であって、「ユーザ名」等の情報をもってセンタ 130 側に付与された IP アドレス」情報が特定されるよう記録されるなどの関連性があるわけではない。
15 から、前者と後者は「対応付けられて登録されている」ものとは解し得ない。

原告の主張は、本件発明の特許請求の範囲の記載に基づく主張とはいえず、採用することができない。

オ まとめ

20 以上によれば、本件発明において、管理コンピュータ側に監視目的に応じて適宜選択される監視手段を有する監視端末側に対して付与された IP アドレス及び監視端末 ID を含む監視端末情報が、利用者 ID に対応付けられて登録されている利用者データベースを備えることが特定されていない点を相違点（相違点 1）と認定し、これを実質的な相違点と判断した本件審決の認定に誤りはない。
25

(2) 小括

以上のとおりであるから、相違点 2 の認定の当否を検討するまでもなく、
本件発明は新規性を欠如しないといえるから、本件審決の新規性判断に誤り
はなく、取消事由 1 は理由がない。

4 取消事由 2（甲 1 発明を主引用例とする進歩性判断の誤り）について

5 (1) 相違点 1 の容易想到性について

原告は、相違点 1 について、本件特許の優先日当時の技術水準・周知技術
から、容易想到である旨を主張するが、相違点 1 に関する上記優先日当時の
技術水準・周知技術について、これを具体的に主張、立証しない。いずれに
せよ、前記 3 において認定判断したとおり、甲 1 発明において、センタ 1 3
10 0 側に付与された I P アドレスをユーザ名やユーザパスワードといった利用
者 I D と対応させてセンササーバ 1 1 0 に記憶する技術的な必要性はなく、
このようにする動機付けはない。

したがって、相違点 1 に係る本件発明の構成は、当業者において容易に想
到できたものとはいえない。

15 (2) 小括

以上によれば、相違点 2 の容易想到性判断の当否を検討するまでもなく、
本件発明は進歩性を欠如しないといえるから、本件審決の進歩性判断に誤り
はなく、取消事由 2 は理由がない。

5 結論

20 よって、原告主張の取消事由はいずれも理由がないから、原告の請求を棄却
することとして、主文のとおり判決する。

知的財産高等裁判所第 4 部

裁判長裁判官

菅 野 雅 之

5

裁判官

本 吉 弘 行

10

裁判官

中 村 恭

(別紙 1)

本件明細書の記載事項

5 【発明の詳細な説明】

【技術分野】

【0001】

本発明は、通信回線を用いて監視端末が設置された特定領域を、利用者が所有する電話やパソコン等の情報端末を用いて、外出先からでも監視することを可能とする通信回線を用いた情報供給システムに関する。

【背景技術】

【0002】

従来より、家を留守にした場合、泥棒の侵入や火気の始末を気にしなければならず、今日のような治安情勢の悪化に伴い、ますますこのような心配は増すばかりである。そのため、近年警備会社と契約を行うことにより、泥棒の侵入や火災等の発生を未然に防止する警備代行業務を行ってもらい個人宅、会社等が増加している。

【0003】

現状の警備システムとして、所定のセンサー等を配備した家屋等に泥棒が侵入した場合、センサーの反応による警備会社への通報で警備会社の警備員がその家屋に急行するシステムがある。

【0004】

しかし、このようなマンパワーを利用するシステムであっては、警備員の人件費が極めて高い割合を占めるため、加入契約料が一般大衆にとって多大なものとなり、これ以上の急激な増加は望めないのが現状である。

25 【0005】

このため、通信回線（有線、無線を含む）を利用して、必要な時、また心配にな

った時に限らず、頻繁に断続的にでも特定領域である例えば自宅内の様子を監視できるようにしたいといった要求がある。

【発明の開示】

【発明が解決しようとする課題】

5 【0006】

しかしながら、これら監視システムにおいては、前記監視端末に通信回線を介して特定以外の人間がアクセスして監視領域の画像等の監視情報を入手することができてしまうと、プライバシーが保護されなくなってしまうという問題があり、これら特定者以外の第三者が監視端末より監視情報を入手することが不可能なシステム
10 が切望されていた。

【0007】

よって、本発明は上記した問題点に着目してなされたもので、常時接続回線を利用しているにも関わらず、特定者以外の第三者が監視端末より監視情報を入手することがきわめて困難で、かつ登録された利用者には、きわめて迅速に必要な監視情
15 報を供給できるようにした通信回線を用いた情報供給システムを提供することを目的としている。

【課題を解決するための手段】

【0008】

上記目的を達成するために、本発明の情報供給システムは、インターネットや電
20 話網からなる通信回線網の中に設置されている管理コンピュータに於ける通信回線を用いた情報供給システムであって、

前記管理コンピュータ側には、監視目的に応じて適宜選択される監視手段を有する監視端末側に対して付与されたIPアドレスおよび監視端末IDを含む監視端末情報が、利用者IDに対応付けられて登録されている利用者データベースを備え、
25 前記監視端末は前記管理コンピュータ側と前記通信回線網を介して接続可能とされており、

前記管理コンピュータ側は、

インターネットや電話網からなる通信回線網を利用してアクセスしてくる利用者の電話番号、ID番号、アドレスデータ、パスワード、さらには暗号などの認証データの内少なくとも一つからなる利用者IDである特定情報を入手する手段と、

5 この入手した特定情報が、前記利用者データベースに予め登録された監視端末情報に対応するか否かの検索を行う手段と、

前記特定情報に対応する監視端末情報が存在する場合、インターネットや電話網からなる通信回線網を利用して、この抽出された監視端末情報に基づいて監視端末の制御部に働きかけていく手段と、

10 インターネットや電話網からなる通信回線網を経由して、前記監視端末によって得られた情報を入手する手段と、

この監視端末から入手した情報を、インターネットや電話網からなる通信回線網を用いて、前記特定情報を送信してアクセスした利用者に供給する手段と、

15 管理コンピュータ側と監視端末側との回線再接続時、特定できる監視端末側からのIPアドレス登録要求を受け付け、前記利用者データベースの前記監視端末情報であるIPアドレスを登録処理する手段と、を備え、

前記監視端末側は、

内部にメモリーされた管理コンピュータ側のグローバルIPアドレスに対して自ら接続処理する自己接続機能と、

20 前記自己接続機能を使って、登録された前記監視端末IDを管理コンピュータ側に送り、前記監視端末側のIPアドレスを登録するように要求する手段と、を備えていることを特徴としている。

(関連する態様)

25 本発明の情報供給システムの態様として、インターネットや電話網からなる通信回線網の中に設置された管理コンピュータに於ける通信回線を用いた情報供給システムであって、

監視カメラ，監視ビデオ等の監視目的に応じて適宜選択される監視端末に対して付与された I P アドレスを含む監視端末情報が，利用者 I D に対応付けられて登録されている利用者データベースを備え，

5 インターネットや電話網からなる通信回線網を利用してアクセスしてくる利用者の電話番号， I D 番号，アドレスデータ，パスワード，さらには暗号などの認証データの内少なくとも一つからなる利用者 I D である特定情報を入手するステップと，
この入手した特定情報が，前記利用者データベースに予め登録された監視端末情報に対応するか否かの検索ステップと，

前記特定情報に対応する監視端末情報が存在する場合，前記管理コンピュータが
10 インターネットや電話網からなる通信回線網を利用して，この抽出された監視端末情報に基づいて監視端末の制御部に働きかけていくステップと，

前記管理コンピュータが，インターネットや電話網からなる通信回線網を経由して，前記監視端末によって得られた情報を入手するステップと，

この監視端末から入手した情報を，前記管理コンピュータが，インターネットや
15 電話網からなる通信回線網を用いて，前記特定情報を送信してアクセスした利用者に供給するステップと，

前記管理コンピュータが，特定できる監視端末側からの I P アドレス変更要求を受け付け，前記利用者データベースに登録されている前記監視端末情報である I P アドレスを変更処理するステップと，

20 からなる通信回線を用いた情報供給システムを特徴とするものであり，利用者データベースを状況によって素早く更新し，利用者の次なるアクセスに瞬時に対応できるようにできるものである。

ここで，監視端末からの I P アドレス変更要求を受け付ける際，前記利用者データベースに登録されている監視端末 I D を受け付け，この監視端末 I D が適正な場合
25 のみ， I P アドレス変更要求に応じるステップを有してなることが好ましく，このようにすればより確実な利用者データベースの管理ができることになる。

このシステムに必要な監視端末が、常時接続状態のまま、I Pアドレスが変更された場合は、前記監視端末は、古いI Pアドレスと新しく与えられたI Pアドレスとの違いを判断し、相違する場合は、内部にメモリーされた管理コンピュータのグローバルI Pアドレスに対して自ら接続処理し、自己の監視端末IDを基に新たなI Pアドレスを更新登録するように要求できる自己接続機能を有していることが好ましく、別の例として、監視端末が、インターネットの新たな接続または再接続可能時、監視端末は、その内部にメモリーされた管理コンピュータのグローバルI Pアドレスに対して自ら接続処理する機能が設けられており、自己の監視端末IDを基にその時点手付与されているI Pアドレスを更新登録するように要求できる自己接続機能を有していることが好ましく、さらに別の例として、監視端末が、常時接続状態のままI Pアドレスが変更された場合、またはインターネットの再接続可能時、監視端末は、その内部にメモリーされた管理コンピュータのグローバルI Pアドレスに対して自ら接続処理する機能が設けられており、自己の古いI Pアドレスを基にその時点手付与されているI Pアドレスを更新登録するように要求できる自己接続機能を有していることが好ましい。この例の場合は、既に利用者データベースに、監視端末に対応する古いI Pアドレスが存在しておりこれによっても監視端末の認証が可能である。

さらに、管理コンピュータは、利用者がアクセスしてきた際、利用者データベースの中から監視端末IDの検索により、利用者に対応する監視端末または監視ユニットが複数ある場合、利用者に対してアクセス可能な監視端末または監視ユニットの種類やメニューを表示し、得たい情報の選択を促すようになっており、管理コンピュータは登録された全ての監視端末の情報をとる必要がなく、指摘された監視端末のみへのアクセスが可能となる為、利用者に無駄な待ち時間などを与えないようにできる。

前記特定情報に対応する監視端末情報が存在する場合、前記管理コンピュータがインターネットや電話網からなる通信回線網を利用して、この抽出された監視端末

情報に基づいて監視端末の制御部に働きかけ、前記管理コンピュータが、インターネットや電話網からなる通信回線網を経由して、前記監視端末によって得られた情報を入手するステップ時、監視端末に接続不能な状態、若しくは監視端末からの情報が前記管理コンピュータに送信されてこない状態が、前記管理コンピュータで確認された時に、所定の異常通知をアクセスした利用者に送信できるようになっていると好ましい。すなわち管理コンピュータでデータを待つ時間を所定の時間と設定し、セッション管理することにより、待ち時間内にデータが得られないとき、アクセスしてきた利用者をいつまでもも待たせることなく情報が取れない旨のメッセージを送ることによりサービスの向上が図れる。

10 前記管理コンピュータが、インターネットや電話網からなる通信回線網を経由して、前記監視端末によって得られた情報を入手する際、この送信されてくる情報が所定の圧縮アルゴリズムにて圧縮処理された画像の圧縮データであり、前記管理コンピュータは、この圧縮データを記憶装置に一時記憶し、前記アクセスしてくる利用者の情報端末への通信回線のデータ伝送速度に合わせて、前記一時記憶された圧縮データを送信するようになっており、利用者のどのような機種

15 の端末にも対応できることになる。

少なくとも本発明の情報供給監視端末は、インターネットや電話網からなる通信回線網の中に設置された管理コンピュータを用いた情報供給システムに適用される監視端末であり、

20 特定できる前記監視端末側からのIPアドレス変更要求を受け付け、前記利用者データベースに登録されている前記監視端末情報であるIPアドレスを変更処理するステップを実行できるようになっている管理コンピュータに対して利用される監視端末であり、

前記管理コンピュータにIPアドレス変更要求する監視端末が、監視カメラ、監視ビデオ等の機能を有し、

25

この監視端末側のメモリーに、前記管理コンピュータのIPアドレスが記憶され、

この記憶された管理コンピュータの I P アドレスに対して、自己の監視端末 ID を
基にその時点で付与されている I P アドレスを更新登録するように要求できる機能
を有していることを特徴としている。

少なくとも本発明の情報供給監視端末は、インターネットや電話網からなる通信
5 回線網の中に設置された管理コンピュータを用いた情報供給システムに適用される
監視端末であり、

監視カメラ、監視ビデオ等の監視目的に応じて適宜選択される監視端末に対して
付与された I P アドレスを含む監視端末情報が、利用者 I D に対応付けられて登録
されている利用者データベースを備え、

10 インターネットや電話網からなる通信回線網を利用してアクセスしてくる利用者
の電話番号、I D 番号、アドレスデータ、パスワード、さらには暗号などの認証デ
ータの内少なくとも一つからなる利用者 I D である特定情報を入手するステップと、
この入手した前記特定情報が、前記利用者データベースに予め登録された前記監
視端末情報に対応するか否かの検索ステップと、

15 更に、特定できる前記監視端末側からの I P アドレス変更要求を受け付け、前記
利用者データベースに登録されている前記監視端末情報である I P アドレスを変更
処理するステップと、を少なくとも実行するようになっている管理コンピュータに
対して利用される監視端末であり、

前記管理コンピュータに I P アドレス変更要求する監視端末が、

20 この監視端末側のメモリーに、前記管理コンピュータの I P アドレスが記憶され、
この記憶された管理コンピュータの I P アドレスに対して、自己の監視端末 ID を
基にその時点で付与されている I P アドレスを更新登録するように要求できる機能
を有していることを特徴としている。

【発明を実施するための最良の形態】

25 【0009】

以下、図面に基づいて本発明の実施例を説明する。

【実施例 1】

【0010】

まず、図 1…は、本実施例の特定領域の監視システムの構成を示すブロック図であり、図 3 は、本実施例の特定領域の監視システムに用いた監視端末を示す外観斜
5 視図であり、図 4 は、前記本実施例において用いた監視端末の構成を示すブロック図であり、図 5 は、本実施例において用いた管理コンピュータの構成を示すブロック図であ…る。

【0011】

まず、本実施例の特定領域の監視システムは、図 1 に示すように、登録している
10 多数の利用者（A．B．C… Z…）が個々に監視したい場所、例えば自宅等の被監視領域（a．b．c… z…）に設置される監視端末 4（4 a．4 b．4 c… 4 z…）と、該監視端末 4 並びにサービス利用者が所有する情報端末とに通信回線網 5 を介してデータ通信可能に接続されたサービス提供者が所有する管理コンピュータ 3 と、各監視端末側と基本的に常時接続されたインターネットサービスプロ
15 バイダー（I S P）である中継サーバ 6，監視サービスの利用者が操作するパソコン 1 4 やノートパソコン 1 5 や携帯電話 1 1 等の情報端末と、から主に構成されている。

【0012】

また、本実施例に用いた監視端末 4（4 a．4 b．4 c… 4 z…）は、図 1 に
20 示すように、主に通信回線網 5 を介してサービス提供者が所有する前記管理コンピュータ 3 と原則、常時接続されている。この例によると、監視端末 4 a ～ 4 c は、ネットワークを介して管理コンピュータ 3 と常時接続を可能とする A D S L（D S L）、いわゆる非対称デジタル加入者線方式で接続されており、監視端末 4 a ～ 4 c は、データの送受信を実施する通信装置であるセットトップボックス 2 と、該セッ
25 トトップボックス 2 に接続されて特定領域の画像や音等の監視情報を収集する監視ユニット 1 とから構成されている。…

【0013】

この図1に示した本実施例において用いた監視ユニット1は、図3に示すように、天井等に配置可能な箱状の筐体50の下面に、透明なドーム状のカバー68が形成されているとともに、該カバー68の内部には監視手段である監視用CCDカメラ55と、該監視用CCDカメラ55の監視方向を左右上下に変更可能な方向変更装置58が内在されているとともに、前記筐体50の側面からは、前記セットトップボックス2と接続される通信ケーブル51が導出され、更に他の側面には、監視領域の音を集音可能な集音マイク53が設けられている。

【0014】

また、この監視ユニット1の筐体50内部の構成は、図4に示すように、データ通信を行う通信部71と、後述するMPU65が行う制御においてワークメモリとして使用されるとともに、後述するデジタルシグナルプロセッサ(DSP)56にて圧縮された画像データ或いは音声データを一時記憶するSRAM70と、前記集音マイク53に接続されて入力音をデジタルデータに変換するA/DコンバータであるPCMコーデック52と、内部にレンズにて結像された画像をデジタルのデータ列として出力可能な電荷結合素子(CCD)54を内蔵する監視用CCDカメラ55と、前記PCMコーデック52並びに電荷結合素子(CCD)54より出力された音声データ並びに画像データを所定の圧縮アルゴリズム(MPEG, JPEG等の方式)にて圧縮処理するデジタルシグナルプロセッサ(DSP)56や、前記監視用CCDカメラ55の撮影方向の移動を行う方向変更装置58や、パイロットランプ(LED)69の点灯するドライバ59や、これら各部に図4に示すように接続され、各部の制御等の処理を実施するMPU65とから構成され、該MPU65内部には、該MPU65が実施する前記監視用CCDカメラ55や方向変更装置58並びに集音マイク53等の監視手段並びに監視手段の周辺デバイスの起動や停止等の制御内容が記述された制御プログラム等が記憶された内部ROM66を有している。尚、図4において白矢印は制御信号を示し、黒矢印は主にデータ信号

を示す。

【 0 0 2 0 】

また、本実施例の監視ユニット 1 は前述のように通信部 7 1 を有しており、監視
ユニット 1 側には I P アドレスが割り当てられており、管理コンピュータ 3 と常時
5 接続状態であるため、この I P アドレスが監視領域の特定用に利用されることになる。

【 0 0 2 1 】

次いで、これら監視ユニット 1 とセットトップボックス 2 とから構成される各
監視端末 4 (4 a . 4 b . 4 c . . . 4 z . . .) からのデータ圧縮された画像 (並びに
10 音データ) が中継サーバ 6 を介してインターネット網で送信され、それを受信する
前記管理コンピュータ 3 の構成は、図 5 に示すように、コンピュータ内部にて比較
的高速にてデータの送受を行うデータバス 3 0 に、利用者からの接続による認証処
理や、該利用者 I D に対応して登録されている監視端末の I P アドレス (ここでは
グローバル I P) を検索する処理や、受信した画像並びに音データを該利用者の情
15 報端末である例えば携帯電話 1 1 に送信するデータ転送処理を実施可能な演算能力
に優れた中央演算処理装置 (C P U) 3 1 や、前記 C P U 3 1 のワークメモリ等に
使用される R A M 3 2 や、ディスプレイ等の表示装置 3 4 や、キーボードやマウス
等の入力装置 3 6 や、接続サービスの実施履歴等の登録に使用される現在の時刻情
報や任意の年月日の曜日等のカレンダー情報を出力可能なリアルタイムクロック
20 (R T C) 3 7、前記監視端末を構成するセットトップボックス 2 とのデータ通信
を比較的高速にて実施可能な回線が接続可能とされた監視端末用通信回線基板 3
8 と、利用者の情報端末である携帯電話 1 1 等とのデータ通信を比較的高速にて実
施可能な通信回線が接続可能とされた利用者用通信回線基板 3 3 と、磁気ディスク
や光磁気ディスクから成り、利用者を識別可能な識別符号 (I D) に対応付けて該
25 利用者の暗証番号並びに該利用者が監視したい場所に設置されている監視端末に付
与されている前記した I P アドレスに基づいた利用者データベース (D B) (なお、

I Dも基になるデータは利用者の電話番号，I D番号，アドレスデータ，パスワード，さらには暗号，人体の一部の違いを表現する指紋など）や，前記データ転送処理内容が記述されたデータ転送プログラム等が記憶されている記憶装置35と，が接続された比較的处理能力に優れたコンピュータとされている。

5 【0022】

尚，本実施例に用いた前記通信回線基板33からは，利用者が所持する情報端末である携帯電話11等からのアクセス時において，記憶装置35に登録されたデジタルデータに基づき，該利用者へ利用者I Dと暗証番号との入力を促すガイダンスが送信されるようになっている。なお携帯電話やP Cが所有するI D（グローバル
10 I Pアドレス，利用者I D）がアクセス信号に乗調されて送られ，管理コンピュータ3へのアクセス時に管理コンピュータ3がこのデータを受け取れるものであれば，利用者への負担をかけずにその利用者の権能やその利用者に対応する監視端末を検索できることになる。また所定のガイダンスを，音声として発呼者である利用者に送信することも出来，その場合，音声のデジタルデータをアナログの音声に変換し
15 て送信可能なA/D変換部（図示略）を設けるとよい。

【0025】

以下，本実施例の監視システムにおける監視処理の流れについて，図7のフロー図に基づき説明すると，まず利用者Aは，外出先等において，監視端末1が設置されている自宅の様子が不安になった場合に，例えば自分が所持している携帯電話1
20 1から前記監視サービス提供者が所有する管理コンピュータ3にインターネットアクセスし，ガイダンスに従って自分の利用者I Dと暗証番号とを，携帯電話11を操作して入力する。なお携帯電話やP Cが所有するI D（グローバルI Pアドレス，利用者I D）が，アクセス信号に乗調されて送られ，管理コンピュータ3へのアクセス時に管理コンピュータ3にこのデータが届けば，特別なガイダンスに従う認
25 証処理は利用者側には必要ない。

【0026】

管理コンピュータ 3 側においては、利用者 A の前記携帯電話 1 1 より送信されてきた利用者 I D と暗証番号とを、前記記憶装置 3 5 に記憶されている利用者 D B の登録データと比較し、比較が一致して正規利用者と判断された場合において、管理コンピュータは、利用者に対応する監視端末または監視ユニットが複数あるか否かを検索し、複数ある場合、利用者に対してアクセス可能な監視端末または監視ユニットの種類やメニューを表示し、得たい情報の選択を促すようになっている。この場合、管理コンピュータは登録された全ての監視端末の情報をとる必要がなく、指摘された監視端末のみへのアクセスが可能となる為、利用者に無駄な待ち時間などを与えないようにできる。つづいて該利用者 D B を用いて検索エンジンで検索を行い、この利用者 D B に利用者 I D に対応付けて登録されている監視端末側の I P アドレス（常時接続の I S P が割り振っているアドレス）を抽出し、例えば利用者 A に対応するものが監視端末 4 a である場合、該当する監視端末 4 a を構成するここでは監視ユニット 1 に対して、通常常時接続状態のインターネット回線を利用して監視端末側の I P アドレスに特別な制御信号（コマンドデータ）を送信する。この制御信号は、画像等の情報を取得して管理コンピュータ側へ送るよう指示する要求信号であればどのような信号でも良いが、不正アクセス防止のために暗号化され、監視端末側で復号化処理をすると好ましい。すなわち、管理コンピュータ 3 と監視端末 4 a 側の通信制御部、すなわち図 4 の M P U 6 5 と交信し、画像を要求できるシステムになっていればよい。なお、利用者 A に対応する監視端末が複数ある場合は、利用者に対してアクセス可能な監視端末の種類やメニューを表示し、得たい情報の選択を促すようになっている。後述するが、一個の通信部に対して監視端末が複数接続されていても良い。

【 0 0 2 7 】

前記制御信号（コマンドデータ）を受けて正規な管理コンピュータからの要求であると判断した監視ユニット 1 は、これら起動状態にある監視用 C C D カメラ 5 5 により撮影された画像データ、並びに前記集音マイク 5 3 により集音され前記 P C

Mコーデック 52によりデジタル化された音データは、前記DSP 56により所定のデータ圧縮方式であるMP E G方式（J P E G方式など）により圧縮データに変換され、該圧縮データが前記通信部 60よりセットトップボックス 2に送られ、管理コンピュータ 3にインターネット網を介して監視用通信回線基板 38を通じて送
5 られるようになっている。

【0028】

このように、本実施例においては前記起動コマンドデータの受信により前記監視用CCDカメラ 55等の監視手段の起動を実施すると、監視ユニット 1の消費電力を大幅に低減できるようになることから好ましいが、本発明はこれに限定されるもの
10 ではなく、これら監視手段の電力消費が少ないものである場合や、監視ユニット 1の動作電力として十分な電力が供給できる場合等においては、該監視ユニット 1の監視手段を常時動作状態おしておくようにする。但し常時画像データなどを管理コンピュータ側に送信すると管理コンピュータ側に多大な負荷がかかるため、必要な時にしかデータを送信しないようになっている。

【0029】

本例では中継サーバ 6を経由して監視ユニット 1と管理コンピュータが接続されているが、これは、監視ユニット側に常時固定のIPアドレスが存在していない為であり、中継サーバ 6が一般の常時接続ISP業務として、監視ユニット側に特定のIPアドレスを保証してインターネット網に向けて前記管理コンピュータのアド
20 レス、すなわちIPアドレスと交信を可能にしている。管理コンピュータ 3側の監視端末用通信回線基板 38およびCPU 31は、接続されている各監視端末 4の特定を行っており、管理コンピュータ 3がコマンドデータである制御信号を送信したことにより、各監視端末 4から送信されてくる画像情報などは、監視端末側に振られたIPアドレスや所定のIDとが登録された利用者データベース（DB）を利用して処理される。なお、監視端末の特定されない情報に対しては通信拒否を行う。
25

【0030】

つまりは前記において管理コンピュータ 3 が本来呼び出した所定の監視端末 4 a からの画像情報などは、監視端末側に振られた I P アドレスや所定の I D に基づいて、対応するアクセス者（利用者 A）にデータが送信される。なお、管理コンピュータと監視端末とがインターネットで常時繋がっており、相互通信で互いにコミュニケーション状態であるため、前記コマンドデータに続いていろいろなコマンドを相互にやりとりできることは明らかである。

【 0 0 3 1 】

この監視端末 4 a から送信された画像並びに音を含む圧縮データは、前記記憶装置 3 5 に一時記憶（蓄積）されて、通信回線基盤 3 3 を介してアクセスしてきた情報端末の機種情報（携帯電話、P C など）を得ると共に、この得られる情報に基づきアクセスしてくる利用者（ここでは利用者 A）の情報端末の機種情報（携帯電話、P C など）に対応させて画像フレーム調整などを施し、更に、利用者の情報端末へ、前記一時記憶（蓄積）された圧縮データが適宜なファイル形式、例えば携帯電話にあつては C - H T M L、パーソナルコンピュータにあつては H T M L 等に変換されて送信される。

【 0 0 3 2 】

また、前記管理コンピュータが、インターネットや電話網からなる通信回線網を経由して、前記監視端末 4 よって得られた情報を入手する際、この送信されてくる情報が所定の圧縮アルゴリズムにて圧縮処理された画像の圧縮データであり、前記管理コンピュータ 3 は、この圧縮データを記憶装置に一時記憶し、前記アクセスしてくる利用者の情報端末例えば携帯電話 1 1 への通信回線のデータ伝送速度に合わせて、前記一時記憶された圧縮データを送信するようになっている。

【 0 0 3 3 】

これら利用者の情報端末である携帯電話 1 1 へ送信された前記圧縮データを含む変換データは、適宜に解凍されて画像データが表示画面 1 6 に表示されるとともに、音データが D / A 変換されて前記イアホン端子口 1 7 より出力することもできる。

【0034】

なお、始めに管理コンピュータ3と監視端末4との回線接続を行うときは、管理コンピュータ3側の監視端末用通信回線基板38は、監視端末側から送信されるIPアドレスや所定のIDを受け付け、監視端末側に振られたIPアドレスや所定のIDとが登録された利用者データベース(DB)を利用して、前記CPU31で検索し、この送信内容が正規の監視端末4aからのものであるかを確認して回線接続を完了する。

【0035】

ここで、前記したように監視端末側はISPからIPアドレスが割り振られているが、ISPの都合や、停電や、一時的回線切断等が生じると、ISPであるプロバイダーは次に常時接続の状態に処理する際、監視端末側に新たなIPアドレスを振り直すことが多々生じる。このような事態になると、すでに管理コンピュータ側の利用者DBに登録された監視端末の住所であるIPアドレスの変更を余技なすされることになる。そこで監視ユニット1内の前記MPU65は、基本的に通信部71の制御を行っているわけであるが、IPアドレスの管理(図7に示されるIPアドレス管理部としての機能)も行っており、現在与えられたIPアドレスは常時メモリーされている。

【0036】

一時的回線切断時にあっては、このMPU65は、前述の接続開始時の処理と同様、インターネットの再接続時、必ず内部ROM66にメモリーされた管理コンピュータ3のグローバルIPアドレスに対して自ら接続処理する機能が設けられており、新たなIPアドレスを登録するように要求できる自己接続機能を有している。

【0037】

すなわちIPアドレスが変更された場合は、この新しいIPアドレスをメモリーし、更新処理を行う。続いて管理コンピュータ3のグローバルIPアドレスに対して自ら接続処理を開始する。この接続処理にあっては、利用者データベース(DB)

に記録されている監視端末側に振られた I P アドレスとともに登録された所定の I D, すなわち監視端末 I D を接続用のパラメータとして管理コンピュータに送り, 新たな I P アドレスを登録するように要求する。

【 0 0 3 8 】

- 5 接続状態で I P アドレスが変更された場合は, 前記 M P U 6 5 は, 現在の I P アドレスと新しく与えられた I P アドレスとの違いを判断し, 相違する場合は, 内部 R O M 6 6 にメモリーされた管理コンピュータ 3 のグローバル I P アドレスに対して自ら接続処理し, 新たな I P アドレスを登録するように要求できる自己接続機能を有している。

10 【 0 0 3 9 】

- すなわち図 8 に示されるように, M P U 6 5 の機能として, I P アドレスに変更が発生したか否かの判断をする。変更がない時には, 待機状態を維持する。変更された場合は, この新しい I P アドレスをメモリーし, 更新処理を行う。続いて管理コンピュータ 3 のグローバル I P アドレスに対して自ら接続処理を開始する。この
- 15 接続処理にあつては, 利用者データベース (D B) に記録されている監視端末側に振られた I P アドレスとともに登録された所定の I D, すなわち監視端末 I D を接続用のパラメータとして管理コンピュータに送り, 新たな I P アドレスを登録するように要求する。

【 0 0 4 0 】

- 20 管理コンピュータ側は, 図 9 に示されるように, 接続に際して監視端末 I D である接続用のパラメータの有無を判断する。接続用のパラメータが送られてこない場合は, アクセスの拒否を行う。接続用のパラメータが送られて来ており, この監視端末 I D が利用者データベース (D B) に登録されている場合は, 接続処理を行う。つづいて利用者データベース (D B) から対象の監視端末を検索, 抽出する。さら
- 25 に利用者データベース (D B) の古い I P アドレスに代えて新たな I P アドレスを更新処理する。

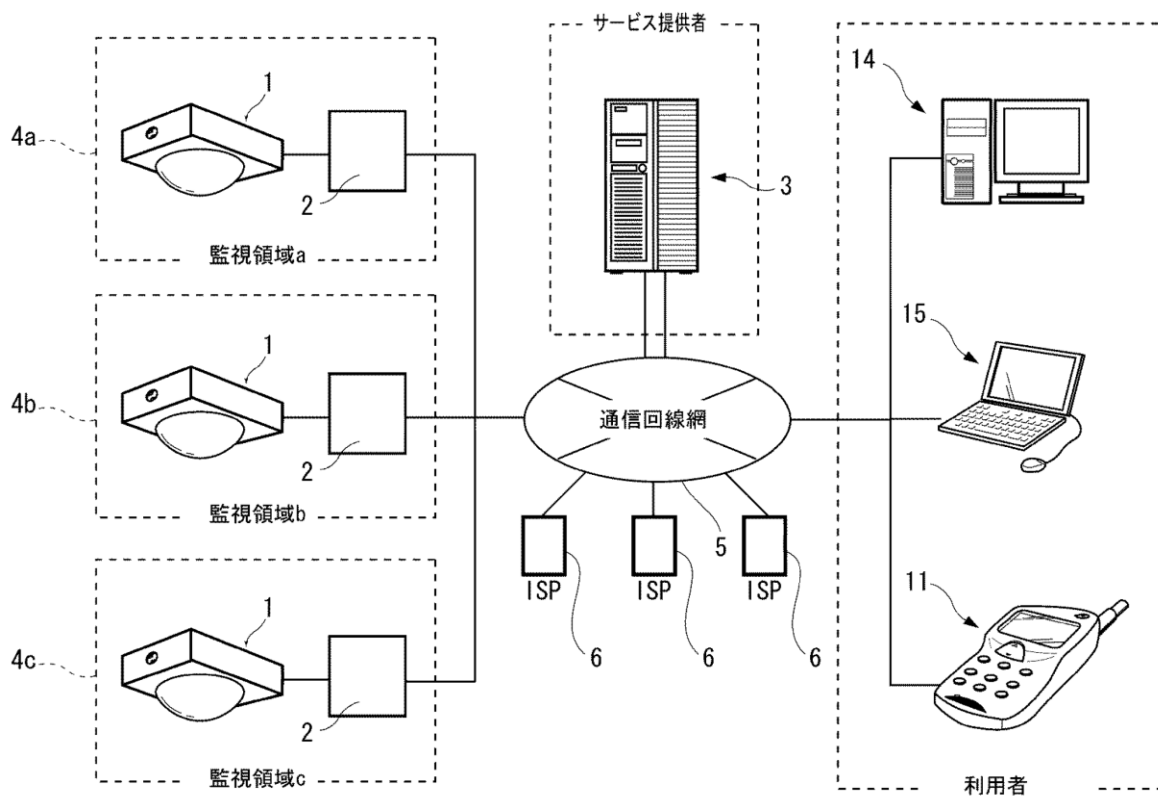
【 0 0 4 1 】

また、監視端末が、常時接続状態のまま I P アドレスが変更された場合、またはインターネットの再接続可能時、監視端末は、その内部にメモリーされた管理コンピュータのグローバル I P アドレスに対して自ら接続処理する機能が設けられており、自己の古い I P アドレスを基にその時点手付与されている I P アドレスを更新登録するように要求できる自己接続機能を持たせることもできる。この例の場合は、既に利用者データベース（D B）に、監視端末に対応する古い I P アドレスがメモリーされており、これによっても接続してくる監視端末の認証が可能である為、この認証で I P アドレスを更新登録要求に応じて良い。

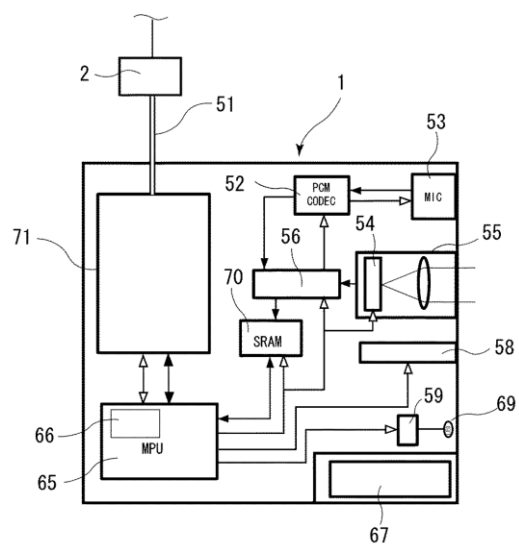
10 【 0 0 4 8 】

また、前記実施例では、セットトップボックス 2 に 1 つの監視端末 1 を接続しているが、本発明はこれに限定されるものではなく、同一のセットトップボックス 2 に複数の監視ユニット 1 それぞれにアドレスを振り接続するようにしても良い。さらに、電荷結合素子（C C D） 5 4 を内蔵する監視用 C C D カメラ 5 5 を一つの監視カメラユニットとし、このような監視カメラユニットの複数にそれぞれアドレスを振り、セットトップボックス 2 に接続された監視ユニット 1 に、複数個の監視カメラユニット（4 a a . 4 a b . 4 a c . 4 b a 等）を繋ぐようにして、それぞれの監視カメラユニット（4 a a . 4 a b . 4 a c . 4 b a 等）の情報を選択的に監視ユニット 1 側へ与えるようにしてもよい。

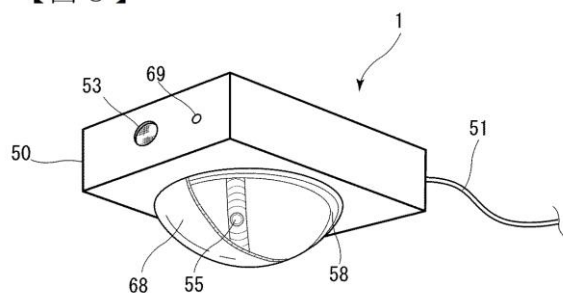
【図 1】



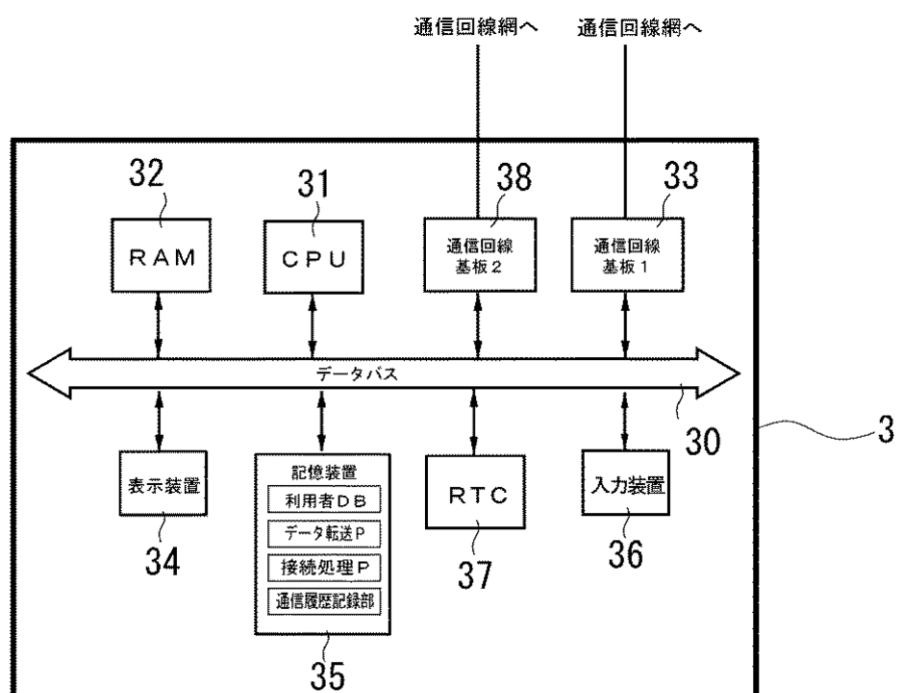
【図 4】



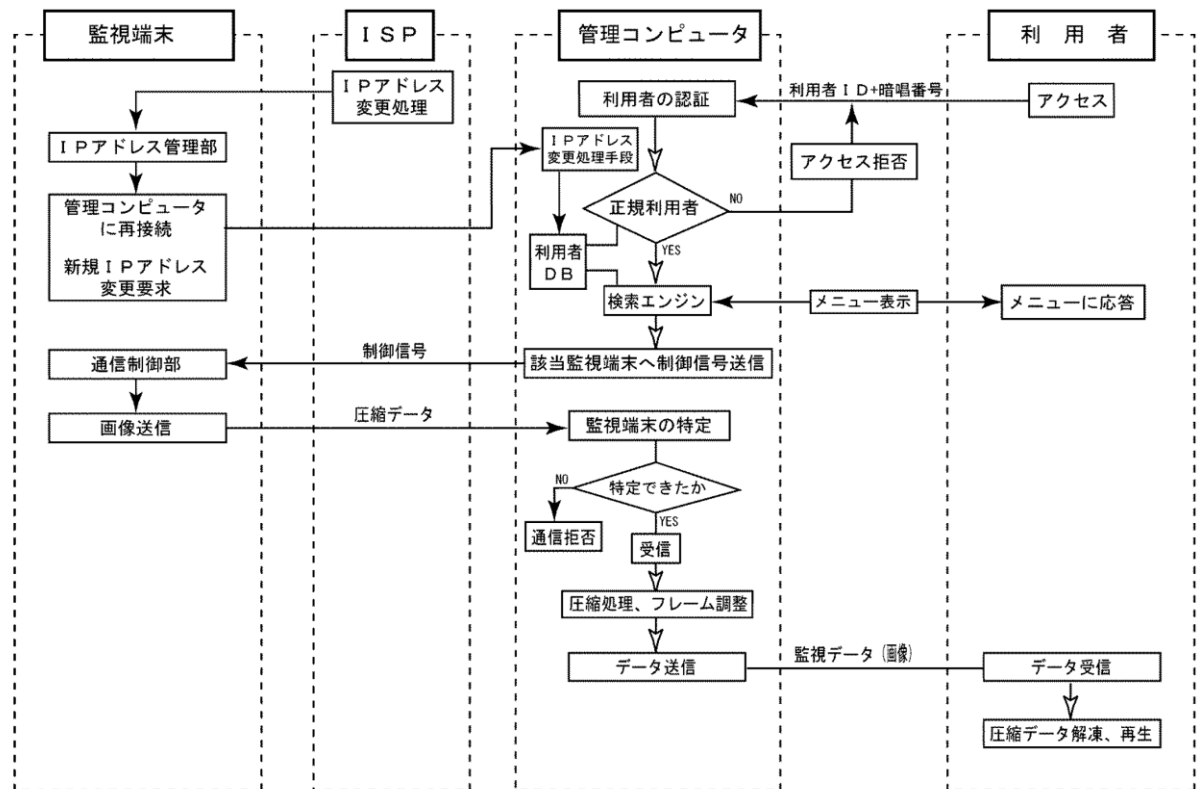
【図 3】



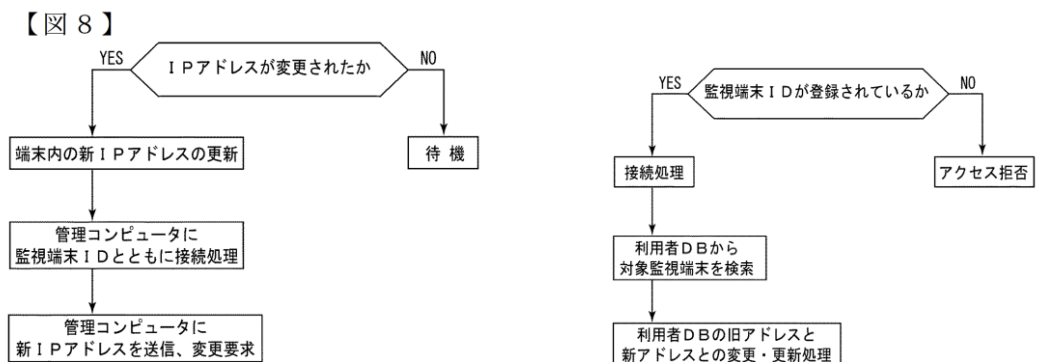
【図 5】



【図 7】



【図 9】



(別紙 2)

甲 1 の記載事項

[1 頁 4 - 1 8 行目]

5 Field of the Invention

The present invention generally relates to a system for accessing remote sensors, and more specifically, to an encrypted virtual private network for accessing images from remote cameras.

Description of the Related Technology

10 In today's world, both parents or a single parent of one or more children must work to support their family. Parents or legal guardians are increasingly concerned about the safety and well-being of their family members or possessions that may be at a day care center, preschool, or other similar facility. Parents also frequently worry about the professionalism
15 of the center employees. A system that would permit a working parent to remotely and securely monitor their children would provide much peace of mind. Such a system should be inexpensive for the parent, easy to use, not require any special equipment or training, and provide security against unauthorized people viewing their children. If a parent is traveling, this
20 monitoring system would allow monitor access of their children from anywhere in the world and also allow relatives that have permission from the parents to also monitor the children. Such access would be via plain old telephone service (POTS), digital subscriber line (DSL), integrated services digital network (ISDN), cable modem or similar connection to the internet, for
25 example. The use of such a monitoring system by a day care center will provide a competitive advantage over other centers that do not have a child

monitoring system.

(発明の分野)

本発明は、一般的には、遠隔センサにアクセスするためのシステムに関するものであり、そして、より具体的には、遠隔カメラの画像にアクセスするための暗号化
5 V P N (仮想私設網)に関するものである。

関連技術の説明

今日の世界では、一人またはそれ以上の子供を持つ両親や一人親は、家族を支えるために働かねばならない。親又は法的な保護者は、保育所(デイケアセンタ)、就
10 学前保育施設、他の同様の施設における家族や財産の安全と健康への関心が増して
いる。また、親は頻繁に、施設職員の専門的な技能を不安視する。工作中的親が、
遠隔的かつセキュアに我が子の監視ができるシステムがあったならば、非常な安心
感を与えるであろう。このようなシステムは、親にとって安価であり、使いやすく、
特別な機器やトレーニングを必要とせずに、かつ、不正者が子供を見ることに対す
るセキュリティを提供すべきである。親が旅行中の場合、この監視システムは、世
15 界中どこからでも我が子の監視アクセスを可能にし、また、親から許可された親戚
にも子供の監視を可能にする。そのようなアクセスは、例えば、P O T S (アナロ
グ公衆電話網)、D S L (デジタル加入者線)、I S D N (サービス統合デジタル網)、
ケーブルモデム、又は、同様のインターネットへの接続を介する。保育所(デイケ
アセンタ)は、このような監視システムを使用することによって、児童監視システ
20 ムを持たない他のセンタに対する競争上の優位が与えられる。)

[1 頁 3 4 - 3 5 行目]

Once a parent, guardian or relative has logged into the sensor server
and has been authorized, all communication is encrypted for security.

25 (一旦、親、あるいは、保護者、親戚が、センササーバにログインして認証された
ならば、すべての通信がセキュリティのために暗号化される。)

[4 頁 1 2 行－ 5 頁 7 行目]

System Overview

Referring to Figure 1, the top-level configuration of a VPN monitoring
5 system 100 will be described. The VPN system 100 comprises two network
segments. A first segment 120 exists between a child-care center, such as
center 1 (130), center 2 (132) or center N (134), and a centralized sensor
computing environment 110 at a central home office location. The centralized
sensor computing environment 110 may include a sensor server or one or more
10 networked servers, as will be described hereinbelow. A second segment 120'
exists between the sensor server 110 and an authorized viewer at a remote
sensor monitor, such as monitor 140, 142 or 144. The links that make up
these segments are differentiated in terms of transport and encryption.

In one embodiment, the link 120 between a child care center, e.g.,
15 center 130, and the sensor server 110 consists of an encrypted virtual
private network run across the public switched telephone network (PSTN). A
virtual private network is a network that is transposed on top of another
network, but separates itself by means of encryption or other means of
security. In this case, the data travels along data lines used for Internet,
20 long distance, etc. but the interception of all or part of the data would
not compromise the data since it is secured via encryption. The link 120'
between the sensor server 110 and a remote sensor monitor, e.g., 140, also
consists of an encrypted virtual private network. Because the system 100
consists of only two links, and because each link is a VPN obscured with
25 very strong encryption, the system 100 is invulnerable to attacks whose
goal would be to compromise the system and allow images to be viewed by

someone other than the authorized viewer.

Communications between the child care center 130 and the sensor server 110, and between the sensor server 110 and the authorized viewer at monitor 140 are facilitated through the use of a packet switched network such as the PSTN. Information is passed onto the PSTN and taken off of the PSTN through the use of telco access devices, such as routers, DSL modems, ISDN modem-routers, cable modems, and multi-link point-to-point (MLPPP) modems, at the center 130. The telco access devices are often referred to as 'routers' - for instance, a product available from Farallon is called a 'dual analog router'. A telco access device provides an access point from a smaller network at the center 130 to the larger network that is the PSTN. This data that is being passed between the nodes on the system network travels along the PSTN alongside long-distance telephone conversations, corporate data, and data comprising the public Internet. It is possible to safely transmit this data along these semi-public channels because the encryption of the data forms a VPN which cannot be accessed by other users of the PSTN, such as people placing telephone calls, for instance. Because of this, the system 100 isolates the images produced and transmitted only on the secure network, and never on the public Internet. Any mention of 'Internet Viewing' is simply intended as a means to convey the technology to unsophisticated users without confusing them. The only similarity between the technology of the system 100 and 'Internet Viewing' is that both are accomplished with web browsers.

(システム概要)

図 1 を参照して、VPN 監視システム 100 の最上位レベルの構成を説明する。VPN システム 100 は、2 つのネットワーク・セグメントを含む。第 1 のセグメ

セント 1 2 0 は、保育所、例えば、センタ 1 (1 3 0)、センタ 2 (1 3 2)、センタ N (1 3 4) と、中央ホームオフィス位置の中央センサコンピューティング環境 1 1 0 との間に存在する。以下で説明するように、中央センサコンピューティング環境 1 1 0 は、センササーバ、又は、1 台以上のネットワーク化サーバを含んでもよい。第 2 のセグメント 1 2 0' は、センササーバ 1 1 0 とリモートセンサモニタ、
5 例えば、モニタ 1 4 0、1 4 2、1 4 4 における認証された観察者との間に存在する。これらのセグメントを構成するリンクは、転送および暗号化の点で特徴付けられている。

一実施例において、保育所、例えばセンタ 1 3 0 などとセンササーバ 1 1 0 との
10 間のリンク 1 2 0 は、公衆交換電話網 (P S T N) を横切る暗号化 V P N からなる。V P N とは、別のネットワークの上位に置かれているが、暗号化その他のセキュリティ手段により分離されたネットワークである。この場合、データは、インターネット用や、長距離用などのデータ回線で運ばれるが、暗号化で保護されているために、データの全部や一部が傍受されても、データのセキュリティは破られない。センササーバ 1 1 0 と遠隔センサモニタ 1 4 0 などとの間のリンク 1 2 0' も暗号化
15 V P N からなる。システム 1 0 0 は、2 つのリンクだけから構成されており、各リンクが非常に強力な暗号化により掩蔽された V P N であるために、システム 1 0 0 は、認証された観察者以外の者が、システムのセキュリティを破壊して画像を見られるようにすることを目的とする攻撃に対して、頑強である。

20 保育所 1 3 0 とセンササーバ 1 1 0 との間、及び、センササーバ 1 1 0 とモニタ 1 4 0 における認証された観察者との間の通信は、公衆交換電話網 (P S T N) などのパケット交換網を用いることによって促進される。電話事業者 (T e l c o) アクセス装置、例えば、ルータ、D S L モデム、I S D N モデム・ルータ、ケーブルモデム、M L P P P (マルチリンク・ポイント・ツー・ポイント) モデムなどの
25 利用を通じて、センタ 1 3 0 において、情報が公衆交換電話網 (P S T N) に渡され、また、公衆交換電話網 (P S T N) から取り出される。電話事業者アクセスデ

バイスは、しばしば「ルータ」と呼ばれる — 例えば、F a r a l l o n社から市販されている製品は、「デュアルアナログルータ」と呼ばれる。電話事業者アクセス装置は、センタ 1 3 0 のより小規模なネットワークから、より大規模なネットワークである公衆交換電話網（P S T N）に対するアクセスポイントを提供する。システム5 のネットワークのノード間を通るこのデータは、長距離電話の会話や、企業データ、公開のインターネットのデータなどとともに、P S T N上を移動する。データを暗号化することによって、電話しているユーザなどP S T Nの他のユーザにはアクセスできないV P Nが形成されて、このデータをこれら半公開の回線上で安全に伝送できる。このことにより、システム 1 0 0 は、生成されて送信される画像は、10 セキュアなネットワーク上のみに隔離されて、公開のインターネット上には置かれない。「インターネット・ビューイング」として言及しているのは、単に技術に不慣れなユーザを混乱させずに技術を伝達するための手段として意図している。システム 1 0 0 の技術と、「インターネット・ビューイング」との間の類似点は、どちらもウェブブラウザを用いて実現されることのみである。）

15

[5 頁 8 – 3 0 行目]

In overview, the system 100 allows an authorized user to ask the sensor server 110 for a current picture, allows the sensor server 110 to fetch that picture from a sensor, e.g., a video camera, at the center 130, and 20 finally transports the requested image from the sensor server 110 to the authorized user at the monitor 140. In another embodiment, the sensor may comprise an infrared sensor, a motion sensor, a sound sensor, a tripwire, and so forth.

In this framework, the sensor server 110 acts as a middleman between 25 the camera and the user. The system 100 is designed such that the camera will only answer requests from the sensor server 110 and will discard the

requests of any other entity on the PSTN. The reason for this is twofold. First, by forcing users to authenticate themselves, it is determined that the user is actually an authorized user. In one embodiment, the sensor server 110 uses a three-tier authentication method that forces the user to
5 identify their user name, password (between 8 and 12 characters, letters and numbers), and center identification code. This authentication has an inactivity timeout of a predetermined time interval, such as 15 minutes, and allows the user to choose a camera and view current images from that camera. An inactivity timeout is a function that monitors the user for
10 actions related to the web site (e.g., clicking on a link, viewing a camera, etc.). If none of those actions take place, even if the user is actively using other programs on their computer, the timeout will occur and the user will need to log into the system network again to view a camera.

15 The second reason to force all users to use the sensor server 110 as a middleman is that it reduces the number of connections that a camera needs to support to one. If users were allowed to connect directly to cameras, each user would make a connection to the camera. This will not work efficiently, since the camera, in one embodiment, is physically limited to
20 receiving only a predetermined number, e.g., five, of concurrent connections. Furthermore, additional network capacity between the center 130 and the link 120 would need to be added at the center 130 to accommodate the increased number of users accessing the sensors in the center. Therefore, the authorized users make their connection to the sensor server 110, and
25 the sensor server 110 only opens one connection to each camera.

(概略的には、システム 100 は、認証されたユーザが、センササーバ 110 に現

時点の画像を要求できるようにして、センササーバがセンタ 1 3 0 のセンサ，例えば，ビデオカメラからの画像を取得して，最終的に，センササーバ 1 1 0 からモニタ 1 4 0 にいる認証された観察者へと，要求された画像を転送する。他の実施形態では，センサは，赤外線センサ，動きセンサ，音センサ，トリップワイヤなどを含むことができる。

このフレームワークにおいて，センササーバ 1 1 0 は，カメラとユーザ間の仲介者として機能する。このシステム 1 0 0 において，カメラは，センササーバ 1 1 0 からの要求のみに応答して，公衆交換電話網上の任意の他のエンティティからの要求は破棄するように設計されている。その理由は 2 つある。第 1 に，ユーザに自身を認証するように強制することによって，ユーザが実際に認証されたユーザであることが判定される。一実施形態では，センササーバ 1 1 0 は，ユーザがユーザ名，パスワード（8 - 1 2 文字の文字及び数字），センタ ID コードで識別するように強制する 3 段階の認証方式を使用する。この認証は，所定時間間隔，例えば，1 5 分等の非活動タイムアウトを備えており，また，1 台のカメラを選択して，そのカメラからの現在の画像を閲覧することを可能にする。非活動タイムアウトとは，そのウェブサイトに関連したアクション（例えば，リンクをクリックすること，カメラを見ることなど）を監視する機能である。これらのアクションのいずれも発生しない場合には，ユーザがそのコンピュータ上で他のプログラムを活発に利用中であっても，タイムアウトが発生して，カメラを再び見るためにはユーザは再度システムネットワークにログインする必要がある。

全てのユーザがセンササーバ 1 1 0 を仲介者として利用するように強制することの，第 2 の理由は，1 台のカメラについてサポートが必要とされる接続の数を 1 つに減らすことである。もしも各ユーザがカメラに直接接続することを許した場合，各ユーザがカメラとの接続を行う。これは効率的な動作ではない。なぜならば，一実施形態では，カメラは予め定められた数の同時接続，例えば 5 つのみを受信するように，物理的に制限されているからである。さらに，より多くのユーザがセンタ

のセンサにアクセスできるようにするためには，センタ 1 3 0 との間の追加のネットワーク容量とリンク 1 2 0 を，センタ 1 3 0 において追加することが必要とされるだろう。したがって，認証されたユーザは，センササーバ 1 1 0 に接続を行って，センササーバ 1 1 0 は，各カメラに対してただ 1 つの接続を設定する。)

5

[6 頁 1 - 1 1 行目]

When a center is initially setup, it is provided with a center identification code or school code. This is a code that is unique to each school or organization and is required to login.

10 The system 100 utilizes an on-line sign-up form for parents so as to capture vital information for advertising purposes and to alleviate the workload for the system administrator. When parents wish to obtain an account, they access the form from the system web page, home page, or hyperlinked page. Such a page may be provided via a hypertext transfer
15 protocol (HTTP). The parents then provide the requested information and answer a few questions on the form. After the form is submitted, they are provided with a temporary password that they can use to access the system once their account is activated. A message is immediately sent to the system administrator (via the "message area") that a new account is awaiting
20 activation. A welcome message is also sent to the new parent's account in their "message area". At this point the account status is "pending" or awaiting activation. To activate the account, the system administrator needs to login and assign a child and cameras to the account.

(あるセンタが最初に設定されるとき，当該センタにはセンタ I D コード又はスク
25 ールコードが与えられる。これはそれぞれの学校や組織にユニークなコードであつて，ログインするために必要とされる。

システム 100 は、広告の目的のために重要な情報を獲得するため、及び、システム管理者の作業負担を軽減するために、親用のオンライン・サインアップ・フォームを利用する。親はアカウントの取得を望む場合、システムのウェブページや、ホームページ、または、ハイパーリンクされたページから、フォームにアクセスする。そのようなページは、HTTP（ハイパーテキスト転送プロトコル）を介して提供されてもよい。親は、要求された情報を与え、フォーム上のいくつかの質問に回答する。フォームの提出後、そのアカウントが起動されたときに、システムにアクセスするために使用できる一時パスワードが提供される。直ちに新規のアカウントが起動を待っていることを伝えるメッセージが（「メッセージ領域」を介して）システム管理者に送られる。ウェルカム・メッセージも、その新規の親のアカウントの「メッセージエリア」に送信される。この状態ではアカウントの状態は「保留中」又は起動待ちである。アカウントを起動するために、システム管理者はログインして、子供とカメラをアカウントに割り当てる必要がある。）

15 [6 頁 22 - 27 行目]

Referring to Figure 2, an exemplary screen 200 that is displayed to a parent after login and authorization will now be described. The exemplary screen includes three frame windows; a top left pane 210, a lower left pane 220 and one pane 230 on the right. The top left pane 210 initially presents a tip of the day or an advertisement. Once a sensor is activated, this frame 210 presents images from the cameras. A time and date area 212 associated with the image may also be presented in pane 210. The lower left pane lists a group of sensors, e.g., cameras, available to be viewed by the parent, such as cameras in Room2 (222), Room3 (224), Gym (226) or Playground (228).

25]

（図 2 を参照すると、ログインと認証の後に、ある親に提示される例示的な画面

200が示される。例示的な画面は、左上ペイン（p a n e : 表示領域）210、左下ペイン220、右側に一つのペイン230がある3つのフレームウィンドウを有する。左上ペイン210には、初期状態で、今日の一言か広告を提示する。一旦センサが起動されると、フレーム210には、カメラからの画像を提示する。画像
5 に関連する日時エリア212も、ペイン210に提示される。左下ペインには、その親が視聴に利用できるセンサ、例えば、カメラのグループ、例えば、部屋2（222）、部屋3（224）、ジム（226）、プレイグラウンド（228）のカメラをリスト表示する。）

10 [7頁1－2行目]

When a parent clicks on a camera link, e.g., 222, in the lower-left pane 220, the sensor server 110 (Figure 1) gets images from the selected camera and sends them to the parent's browser as fast as possible.

（左下ペイン220において、ある親が、カメラのリンク、例えば222をクリックしたとき、センササーバ110（図1）は、選択されたカメラから画像を取得し
15 て、画像を親のブラウザにできるだけ速く送信する。）

[7頁12－14行目]

Occasionally, cameras may be inaccessible due to downed links or other
20 technical problems. When this happens, parents are given a message that the camera is temporarily unavailable and to try again later.

（時々、カメラは、リンクのダウンその他の技術的問題のためにアクセス不能となる。このようなことが起きた場合、親には、カメラが一時的に利用不能であって、後ほど再試行すべきとのメッセージが与えられる。）

25

[8頁24行－9頁8行目]

System Topology

Referring now to Figure 3 and also Figure 1, one embodiment of the hardware components of the system 100 will be described. As previously mentioned, the system 100 comprises two main network segments. The first network segment 120 consists of the link between a day care center, e.g., center 130, and the sensor server 110. The second network segment 120' consists of the link between the sensor server 110 and an authorized viewer, such as at a computer 322, 326 or 329.

The first network segment 120 begins in the center, e.g., 130. An incoming network connection (such as DSL or ISDN) 316 is connected to a telco access device 388. Exemplary telco access devices include a Paradyne HotWire 5446 DSL modem, model number 5446-a2-200-0rm, a 3Com 56K MLPPP switch, model number 3c430000, and a Netgear ISDN modem, model number RT328. The cabling used in this connection depends on the type of network service being provided. The telco access device 388 is then connected to an encryption device 386, such as a Ravlin-4 wireline encryption device, with a 10-base-T cable. The encryption device 386 is then connected to a hub 382, such as an Ethernet 10-Base-T non-switching hub, with a 10-base-T cable. For most installations, an 8-port hub is sufficient, but considerations such as center size, expansion, and so forth may dictate a 16-port hub or larger. The hub 382 is connected to a network computer/thin client device, such as a network computing device (NCD) 384, which includes a Microsoft Windows-based network computer running a compatible browser. The hub 382, in turn, is also connected to one or more camera servers 380 (remote sensor servers) such as the Axis model 240, or Axis model 200/200+ cameras, with 10-base-T cable(s). Each of the Axis camera servers 380 connects to a power

supply and media aggregator device 374 via RCA type cables, in one embodiment. Each of the cameras 370, 371, 372 connects to the media aggregator 374 with a 75 ohm coaxial video cable.

(システムのトポロジーについて)

5 図3, 及び, 図1を参照して, 今度は, システムのハードウェア構成要素の一実施形態100について説明する。前述したように, システム100は, 2つの主要なネットワーク・セグメントを含む。第1のネットワーク・セグメント120は, 保育所, 例えば, センタ130と, センササーバ110との間のリンクから構成される。第2のネットワーク・セグメント120'は, センササーバ110と認証さ
10 れた観察者, 例えば, コンピュータ322, 326, 329との間のリンクから構成される。

第1のネットワーク・セグメント120は, センタ, 例えば, 130から始まる。入りネットワーク接続(例えばDSL, ISDN)316は電話事業者アクセス装置388に接続されている。例示的な電話事業者アクセス装置は, p a r a d y n
15 e社H o t W i r e 5 4 4 6型DSLモデム, 型番5 4 4 6 - a 2 - 2 0 0 - 0 r m, 3 C o m社5 6 k M L P P Pスイッチ, 型番3 c 4 3 0 0 0 0, N e t g e a r社I S D Nモデム, 型番R T 3 2 8が含まれる。接続に使用されるケーブルは, 提供されるネットワークサービスのタイプに依存する。電話事業者アクセス装置388は, 次に, 暗号化装置386, 例えば, R a v l i n - 4有線暗号化装置に,
20 1 0 b a s e - Tケーブルで接続される。暗号化装置386は, それからハブ382, 例えば, イーサネット1 0 b a s e - T非スイッチングハブに, 1 0 b a s e - Tケーブルで接続される。大部分の設備では, 8ポートのハブで十分であるが, センタの規模や, 拡張などの考慮事項によっては, 1 6ポートかそれ以上のハブを指定することもある。ハブ382は, ネットワークコンピュータ/シンククライアント装置, 例えば, ネットワークコンピューティングデバイス(NCD)384に接
25 続され, これには, 互換性のあるブラウザを実行するM i c r o s o f t社W i n

d o w s ベースのネットワークコンピュータを含む。ハブ 3 8 2 は、次に、1 台以上のカメラサーバ 3 8 0 (遠隔センササーバ), 例えば, A x i s 社 2 4 0 型, 又は, 2 0 0 / 2 0 0 + 型カメラに、1 0 b a s e - T ケーブルで接続される。一実施形態では、A x i s 社のカメラサーバ 3 8 0 の各々は、電源供給及びメディアアグリ
5 ゲータ装置 3 7 4 に、R C A 型ケーブルを介して接続される。カメラ 3 7 0 , 3 7 1 , 3 7 2 のそれぞれは、メディアアグリゲータ 3 7 4 に、7 5 Ω 映像用同軸ケーブルで接続される。)

[10 頁 4 - 3 0 行目]

10 • in another embodiment, a Microsoft Windows based personal computer may be used in place of the network computer 384. Individual Axis model 200 or model 200+ cameras that can be wired directly to the hub 382 (with 10-base-T cable) may be used rather than using the camera server 380 and media aggregator 374. If the hub 382 can be wired directly to an existing incoming
15 Internet connection, the telco access device 388 may be deleted from the center network.

...

The second network segment 120' begins at the sensor server network. The second network connection comes from the same PSTN and leased data line
20 cloud that the outgoing center network is connected to. This second network connection is connected to a telco access device 338, which is in turn connected to the encryption device 336 with a 10-base-T cable. The encryption device 336 is then connected to a switched-hub 334 with another 10-base-T cable. The hub 334 is further connected to a sensor server network
25 332, such as a Fast-Ethernet network. The incoming data traffic flows on the second network segment in the order outlined above.

The outgoing data traffic travels a similar course, but in reverse: from the sensor server network 332 to the hub 334, and traveling through the encryption device 336. The outgoing data travels through the encryption device 336 in an unencrypted form when the data is not headed to a center, e.g., center 130. When data flows to one of the remote sensor monitors 140, it is encrypted by software via a 128-bit SSL connection 318 and travels out to the PSTN and leased data line cloud. Hence, the virtual line 318 indicates that the encryption device 336 passes the outgoing data traffic transparently to the telco access device 338. 128-bit SSL is currently the strongest level of this encryption supported by most major browsers. Other levels or types of encryption may be used in another embodiment. The destination of this outgoing traffic is the authorized viewers at the remote sensor monitors, e.g. 140. Authorized viewers may connect to the PSTN and leased data line cloud through any number of means - using their Internet service provider, using a private corporate network, or connecting directly through a long distance carrier such as MCI or Sprint. Of course, one skilled in communication technology could substitute other hardware devices or utilize software to perform some of the above tasks, e.g., the encryption.

The sensor server network 332 may include one or more servers to facilitate operation of the system.

(・他の実施形態では、ネットワーク・コンピュータ 384 の代わりに、Microsoft 社 Windows ベースのパーソナルコンピュータを使用できる。カメラサーバ 380 とメディア・アグリゲータ 374 とを使用することに替えて、(10 base-T ケーブルによって) ハブ 382 に直接配線できる Axis 社 200 型又は 200+ 型カメラを使用できる。もしもハブ 382 を既存の入りインターネット接続に直接配線できるならば、電話事業者アクセス装置 388 をセンタネットワ

ークから削除してもよい。

...

第2のネットワーク・セグメント120'は、センササーバ・ネットワークから始まる。第2のネットワークの接続は、外向きのセンタネットワークが接続される
5 のと同一の、PSTNと専用データ線のクラウドから入来する。この第2のネットワークの接続は、電話事業者アクセス装置338に接続され、これは次いで、10BaseTケーブルによって暗号化装置336に接続される。暗号化装置336は、次いで、別の10BaseTケーブルによってスイッチ・ハブ334に接続される。ハブ334は、さらに、例えば、高速イーサネットのネットワークなどである、センササーバネットワーク332に接続される。入りデータ・トラフィックは、上で
10 述べた順序で、第2のネットワークセグメント上を流れる。

外向きデータ・トラフィックは、同様の経路を通るが、その向きは逆である。すなわち、センササーバ・ネットワーク332からハブ334へと向かい、そして、暗号化装置336を通過する。外向きのデータは、例えば、センタ130などのセンタに向かわない場合には、暗号化されないフォーマットで暗号化装置336を通過する。リモートセンサモニタ140のいずれか1つに向けてデータが流れる場合は、ソフトウェアによって暗号化が行われ、128ビットSSL接続318を経由して、PSTNと専用データ線のクラウドに送られる。それゆえ、仮想線318は、暗号化装置336が、電話事業者アクセス装置338に向けて、透過的に外向きデータトラフィックを通過させることを図示している。128ビットSSL方式は、
15 現時点で主要なブラウザによってサポートされている、最も強力なレベルの暗号化方式である。別の実施形態では、他のレベルやタイプの暗号化方式を利用できる。この外向きのトラフィックの宛先は、例えば、140などのリモートモニタセンサの位置にいる、認証された観察者である。認証された観察者は、PSTNと専用データ線のクラウドに対して、任意の数の手段を介して接続できる。例えば、インターネット・サービス・プロバイダを使用したり、民間企業のネットワークを使用し
20

たり，または，MC I 社やS p r i n t 社のような長距離キャリアに直接的に接続できる。もちろん，通信技術の当業者であれば，上記のタスク，例えば暗号化を，他のハードウェアデバイスで置き換えたり，ソフトウェアを利用することができる。

センササーバネットワーク 3 3 2 は，システムの動作を容易にする 1 つまたは
5 複数のサーバを含むことができる。）

[1 1 頁 2 8 行－ 1 2 頁 7 行目]

Operational Flow and Server Configuration

Referring to Figures 4, a top-level operational flow process 400 of the
10 system 100 will be described. The servers, processes and threads used by
the operational flow process 400 are shown in Figure 5, which will also be
referred to in this description. Beginning at a start state 402, process
400 moves to state wherein a user accesses the system web site by typing
the world wide web address for the system 100 into their web browser, e.g.,
15 user browser 2 (522), which is running on the user's client computing device,
e.g., computer 329 (Figure 3). Line 526 shows this request and a response
by one of the web servers, e.g., web server 350, of the sensor server 110
(Figure 3). The request and the response, which is information that
comprises the web site home page, are transferred via segment 120' (Figure
20 1). The user can choose to leave the web site at state 406 and complete
process 400 at end state 408 or to browse informational areas of the web
site at state 410. The user can click on any link on the home page to view
the information that that link points to, however, one link (the 'parent
login' button) takes the user into an authentication mechanism, and
25 ultimately, into the secure portion of the web site. When the user clicks
on the 'parent login' button, process 400 proceeds to state 412, wherein

the web server 350 responds, in one embodiment, by initiating a secure 128-bit SSL connection with the browser 522 running on the client computing device and generating a login screen with spaces for center code, user name, and password.

5 (動作フローとサーバ構成)

図4を参照して、システム100の最上位レベルの動作フロープロセス400について説明する。動作フロープロセス400で使用するサーバ及び、複数のプロセスとスレッドは図5に示されており、本記載でも参照する。スタート状態402から始まって、プロセス400は、ユーザがWebブラウザ、例えば、ユーザのブラウザ2(522)にシステム100のWWWアドレスをタイプ入力することで、
10 システムのWebサイトにアクセスする状態に移行し、ここで、このブラウザは、クライアントのコンピューティング装置、例えば、コンピュータ329(図3)上で実行されている。線526は、この要求と、センサ・サーバ110(図3)のWebサーバの1つ、例えば、Webサーバ350の応答とを示している。ここで応答は、Webサイトのホームページを構成する情報であって、要求と応答は、セグメント120'(図1)を介して転送される。状態406においてWebサイトから立ち去ることを選ぶことができ、終了状態408でプロセス400を終えるか、または、状態410においてWebサイトの情報領域をブラウジングできる。ユーザはホームページの任意のリンクをクリックして、リンクが向けられた情報を見るこ
15 とができる。しかしながら、1つのリンク(「親のログイン用」ボタン)は、ユーザを認証メカニズムへと案内して、最終的には、Webサイトのセキュアな部分に案内する。ユーザが「親のログイン用」ボタンをクリックすると、プロセス400は状態412に進み、ここでWebサーバ350は、一実施形態では、応答として、クライアントコンピューティング装置上で実行中のブラウザ522とのセキュアな
20 128ビットSSL接続を開始して、センタコード、ユーザ名、パスワード用のスペースを備えたログイン画面を生成する。)

[12頁8－14行目]

The user responds at state 412 by providing the data needed to perform authentication, e.g., center code, user name, and password, which are sent
5 to the database server 360 on line 528. The database server 360 then accesses the database 362 by the center code. The database server 360 checks all of the user name and password combinations for that particular center and looks up the user name that the user entered. Proceeding to a decision state 414, the password is then compared. If the user-entered password does not match
10 the password in the database 362, process 400 advances to a decision state 416 to determine if the user has reached the limit for trying to enter the authentication data. If not, the user is allowed to try again at state 412.

(状態412において、ユーザは、認証を実行するのに必要なデータ、例えば、センタコード、ユーザ名、パスワードを提供することで応答し、これらのデータは、
15 線528上でデータベースサーバ360に送信される。そして、データベースサーバ360は、そのセンタコードによりデータベース362にアクセスする。データベースサーバ360は、その特定のセンタについてのユーザ名及びパスワードの組み合わせの全てをチェックして、ユーザが入力したユーザ名を検索する。そして、判断状態414に進み、パスワードが比較される。ユーザが入力したパスワードが
20 データベース362にあるパスワードと一致しない場合、プロセス400は、判定状態416に進み、認証データの输入の試行の限界に達しているか否かを判定する。もし達していなければ、ユーザは、状態412で、再試行が可能となる。)

[12頁18－26行目]

25 Returning to decision state 414, if the user name and password match the user name and password in the database 362 for the particular center,

process 400 moves to state 420 wherein the user is authorized for the secure portion of the web site. If the time interval since the date of the last password change exceeds the time allowed for a user to keep a single password, the web server 350 prompts the user to change their password. The web server
5 350 then requests the database server 360 to check the database 362 to obtain a list of camera names that the particular user is allowed to view at the center identified by the center code. Proceeding to state 422, the web server 350 generates a web page with three frames as seen in Figure 2. Frame 230 contains all of the support links (such as child information,
10 preferences, chat, etc.). The top-left frame 210 contains the space for a video image to be displayed, and the bottom-left frame 220 contains a list of all of the cameras names that the user has access to view.

(判断状態 4 1 4 に戻り，ユーザ名とパスワードがデータベース 3 6 2 にあるユーザ名とパスワードと一致した場合，プロセス 4 0 0 は状態 4 2 0 に移動して，ユーザは，ウェブサイトのセキュアな部分について認証される。もし，最後にパスワードを変更した日からの経過時間が，ユーザが 1 つのパスワードを保持できる許容時間を超える場合，Web サーバ 3 5 0 は，パスワードの変更をユーザに促す。Web
15 サーバ 3 5 0 は，センタコードにより識別されるセンタにおいて，特定のユーザが見ることのできるカメラ名のリストを得るために，データベース 3 6 2 をチェックすることを，データベースサーバ 3 6 0 に対して要求する。状態 4 2 2 に進み，
20 図 2 に示すように，Web サーバ 3 5 0 は，3 つのフレームを持つ Web ページを生成する。フレーム 2 3 0 には，すべてのサポート用リンク（例えば，子供の情報，プリファレンス，チャットなど）が含まれる。上部左フレーム 2 1 0 には，表示される映像のためのスペースが含まれており，下部左フレーム 2 2 0 は，ユーザが見
25 るためのアクセスを有するすべてのカメラ名のリストが含まれる。)

[13頁7－8行目]

In this way, only one connection is ever made with the camera even if several users are viewing the particular camera.

(このようにして、複数のユーザが特定のカメラを見ている、カメラとの接続は
5 1つだけになる。)

[13頁31－34行目]

Finally, the database 362, which is accessed by the database server 360, is used to provide authorization data and user information to all of the
10 other servers. The web server 350 queries this database to determine which cameras a parent is allowed to use, and verify login information such as user names and passwords.

(最後に、データベース362は、データベースサーバ360によってアクセスされるものであって、他の全てのサーバに対して認証データとユーザ情報を提供するため
15 ために使用される。Webサーバ350は、このデータベースに照会して、ある親がどのカメラの使用が許可されているかを判定し、ユーザ名やパスワードなどのログイン情報を検証する。)

[14頁9－22行目]

20 To clarify how these servers work together, the following discussion describes what happens, and what interactions take place, when a user attempts to use the system web site. First, a user at a remote location brings up their web browser and types in the web address of the system home page. This action causes the web server 350 to send a copy of the home page.
25 Next, the user clicks on a link leading to a "login" page that prompts them to enter their center code, user name and password to log into the system

web site. This action causes the web server 350 to query the database server 360. Presuming the database server 360 affirms that the user name and password are valid, the web server 350 sends a page to the user's browser that allows the user to select and view images from one of the cameras at the center identified by the center code. On this page, the user selects a camera link. The web server first checks with the database server 360 for a list of the camera names accessible by the particular user and just displays those camera names on the lower left pane of the page. The web server 350, after receiving the request for a particular camera link, checks with the database server 360 to confirm that the particular user has access to that camera. If so, the web server 350 then initiates image retrieval by a request to a sensor process at the image server 330, while, at the same time, initiating image distribution by a request to a user process at the distribution server 340.

（これらのサーバがどのようにして協働するかを明らかにするために、以下の説明では、ユーザがシステムのウェブサイトを利用しようとした場合に、何が起こるか、およびどのような相互作用が行われるかが記載される。まず、遠隔地のユーザがWebブラウザを呼び出して、前記システムのホームページのウェブ・アドレスをタイプ入力する。これにより、Webサーバ350は、ホームページのコピーを送信する。次に、ユーザは、システムウェブサイトログインするために、センタコード、ユーザ名、パスワードの入力を促す「ログイン」ページに通じるリンクをクリックする。これにより、Webサーバ350は、データベースサーバ360に照会を行う。データベースサーバ360が、ユーザ名とパスワードが有効であることを肯定したと仮定すると、Webサーバ350は、ユーザがセンタコードによって識別されるセンタのカメラの一台からの画像を選択して見るができるようにするページをユーザのブラウザに送信する。このページにおいて、ユーザはカメラのリ

リンクを選択する。Webサーバは、第1に、特定のユーザがアクセス可能なカメラ名のリストをデータベース・サーバ360に問い合わせ、ページの左下ペインに単にそれらのカメラ名を表示する。Webサーバ350は、特定のカメラのリンクに対する要求を受信した後、データベースサーバ360に問い合わせ、特定のユーザが、カメラにアクセスできることを確認する。アクセスできるならば、Webサーバ350は、画像サーバ330のセンサ・プロセスへの要求によって画像の取得を開始すると同時に、配信サーバ340のユーザ・プロセスへの要求によって画像の配信を開始する。)

10 [15頁8－15行目]

Fetch Images Process

Referring to Figure 6 and also to Figure 5, a Fetch Images process 600 will now be described. The process 600 that fetches images requires three things: a stimulus to begin fetching, a camera to fetch from, and a storage medium to place the images, once fetched. An example of a stimulus that would cause process 600 to begin fetching would be a user clicking on a sensor link on a web page, or a clock reaching a preset time. Cameras from which to fetch images are located in day care centers 130 (Figure 1) in remote locations that are accessible by the process through the computer network 120. An example of the data storage 362 (Figures 3 and 5) in which to store the images would be a disk drive residing on the data server 360.]

(画像取得プロセス

図6と、図5をも参照して、画像取得プロセス600が説明される。画像取得プロセス600は、以下の3つのものを必要とする：取得を開始させる契機、取得するカメラ、そして、取得された時点で、画像を置いておくストレージ媒体である。プロセス600に取得を開始させる契機の一例は、ユーザがウェブページ上のセン

サのリンクをクリックすること，又は，クロックが予め定められた時刻に到達することである。画像が取得されるカメラは，該プロセスがコンピュータネットワーク 1 2 0 を介してアクセスできる遠隔地の保育所 1 3 0（図 1）に配置される。画像を保存するデータストレージ 3 6 2（図 3 及び図 5）の一例は，データサーバ 3 6 0 上に存在するディスクドライブである。）

[1 5 頁 1 9 行－1 6 頁 2 行目]

Process 600 is running on the image server 330 at all times - it has no dormant, or inactive mode. Beginning at a start state 602, process 600 moves
10 to state 604 where a stimulus to begin fetching an image is received. Advancing to a decision state 606, if process 600 receives a stimulus to begin fetching and depositing images from a camera that already has a previous, un-expired thread that is fetching images, it will not duplicate the effort. Rather, it extends an expiration time (sensor timer) of the
15 existing thread at state 612, and then proceeds to state 614 to access the selected sensor. In this way, no matter how many users attempt to view a specific camera, only one thread is actually transferring the images. If the specified camera is not already active, as determined at state 606, process 600 continues at state 608 and spawns a sensor thread, e.g., thread
20 1 (550) for sensor (1) 370 (Figure 3), thread 2 (552) for sensor 2 (371), or thread N (554) for sensor N (372), to match that stimulus. That sensor thread services the camera/sensor whose address is specified in the stimulus. Moving to state 610, process 600 sets the sensor timer to a predetermined time and activates the sensor timer. These actions describe reacting to the
25 stimulus not by fetching and depositing a single image, but rather by fetching and depositing images for a set amount of time. In this manner,

the process receives the stimulus (for instance, a user clicking a link on a web page) and spawns a thread that would fetch and deposit images for 5 minutes, for example. At the end of the five minute period, the thread would terminate.

5 Proceeding to state 614, process 600 accesses the selected sensor, and then at state 616, fetches the image and places that image, e.g., image 512, in the data storage medium 362. Moving to a decision state 618, process 600 determines if a user action has occurred, such as clicking on a different sensor link. If so, process 600 proceeds to state 606 to determine if a
10 thread for the newly selected sensor is already active.

（プロセス600は、休止又は非アクティブ・モードになることはなく、常に画像サーバ330上で動作している。プロセス600は、スタート状態602で開始して、画像を取得する契機を受信する状態604に遷移する。判定状態606に進んで、プロセス600は、カメラからの画像の取得と保管の契機を受信して、そのカ
15 メラが、期限切れになっていない画像取得中のスレッドを既に保有している場合、プロセス600が重複する作業をすることはない。むしろ、プロセス600は、状態612において、既存のスレッドの有効期限（センサのタイマ）を延長してから、状態614に進んで、選択されたセンサにアクセスする。このようにして、どれほど多くのユーザが特定のカメラを見ようと試みていても、実際には、一つのスレ
20 ッドのみが画像を転送する。状態606での判定の結果、特定のカメラが既に起動していない場合には、プロセス600は、状態608へと続いて、センサ（1）370（図3）用のスレッド1（550）、センサ2（371）用のスレッド2（552）、及び、センサN（372）用のスレッドN（554）などの、契機と合致するセンサ・スレッドを生成する。センサ・スレッドは、カメラ／センサのアドレスが契機
25 で特定されたカメラ／センサに対するサービスを提供する。状態610に進み、プロセス600は、センサのタイマに所定の時間を設定してから、センサのタイマを

起動する。これらのアクションでは、契機に応答して、単一の画像の取得と保管を行うのではなく、むしろ、設定された時間の間、複数の画像の取得と保管を行う。このようにして、このプロセスは、契機（例えば、ユーザがウェブページ上のリンクをクリックすること）を受信して、例えば、5分間の間、画像の取得と保管を行
5 うスレッドを生成する。5分間が経過すれば、スレッドは終了する。

状態614に進んで、プロセス600は選択されたセンサにアクセスし、それから、状態616において、画像を取得し、その画像、例えば、画像512を、データ記憶媒体362に格納する。判定状態618に進み、プロセス600は、ユーザのアクション、例えば、異なるセンサへのリンクをクリックすることが、発生した
10 か否かを判定する。アクションが発生したならば、プロセス600は状態606に進んで、新たに選択されたセンサ用のスレッドがすでに起動されているかどうかを判定する。）

[16頁23－26行目]

15 In one embodiment, the image server 330 makes a connection to the camera at the day care center using the hypertext transfer protocol (HTTP). If a connection cannot be made, it will wait a specified interval (that can be easily changed) and try again. If it fails a predetermined number of times, it will discontinue its efforts after first displaying one image to the
20 user informing the user that the camera is down.

（一実施例において、画像サーバ330は、HTTP（ハイパーテキスト転送プロトコル）を用いて保育所のカメラへの接続を作成する。接続が作成できない場合、画像サーバ330は、（簡単に変更可能な）所定の時間間隔だけ待機してから、再試行を行う。画像サーバ330が、所定の回数だけ接続の作成に失敗した場合、カメラ
25 ラがダウンしていることを通知する一つの画像をユーザにまず表示した後に、その努力を終える。）

[16頁32－35行目]

If at any stage of this process the image server 330 receives an image of size zero, or cannot successfully log in to the camera using the predetermined login name and password, it will attempt to log in to the camera using the Telnet protocol and issue a reset command. This usually cures the camera of any problems it might be having.

(このプロセスのどの段階でも、画像サーバ330がサイズが0である画像を受信したり、所定のログイン名とパスワードを用いてもカメラにログインできない場合、Telnetプロトコルによりカメラにログインしてリセット・コマンドを発行する。通常、これによって、カメラの有するどのような問題も解決する。)

[17頁1－10行目]

Dispatch Images Process

Referring to Figure 7 and also to Figure 5, a Dispatch Images process 700 will now be described. The process 700 is a persistent user process running on the distribution server 340. In one embodiment, the distribution server 340 utilizes the Microsoft Windows NT Server version 4 SP3 with Internet Information Server 4.0 operating software. The process 700 is written in Java, perl, and C++ programming languages.

While process 600 (Figure 6), which fetches and deposits images, is running, process 700, which dispatches images to remote clients (users with web browsers), is also running. Process 700 also receives a stimulus from an outside source, i.e., a request from the web server 350. Process 700 responds to this stimulus by taking the most recent image from the depository area of data store 362 that the fetching program dumps its images in and

sending it to the remote client.

(画像発送プロセス)

図 7 と、図 5 をも参照して、次に画像発送プロセス 7 0 0 について説明する。プロセス 7 0 0 は、配信サーバ 3 4 0 上で実行される永続的なユーザプロセスである。

5 一実施形態では、配信サーバ 3 4 0 は、M i c r o s o f t W i n d o w s N Tサーバ V e r . 4 , S P 3 を、I I S (Internet Information Server) 4 . 0 オペレーティングソフトウェアとともに利用する。プロセス 7 0 0 は、J a v a , P e r l 及び C ++ プログラミング言語で記述される。

10 画像を取得して保管するプロセス 6 0 0 (図 6) が動作中、遠隔クライアント (W e b ブラウザを有するユーザ) に画像を発送するプロセス 7 0 0 も動作している。プロセス 7 0 0 もまた、外部ソースからの契機、例えば、ウェブ・サーバ 3 5 0 からの要求を受け取る。プロセス 7 0 0 は、この契機に対して、取得プログラムが画像を投入するデータストア 3 6 2 の保管領域から、最新の画像を取り込み、そして、それを遠隔クライアントに送信することで応答する。)

15

[2 1 頁 1 - 3 行]

• Restricted Access - Only parents with children enrolled in a system child care center are issued an account to access that center's cameras for viewing. Also, access to cameras is limited to parents who have children in
20 the room where the camera is installed.

(・制限されたアクセスシステムの保育所に入所している子を持つ親だけが、その保育所のカメラを見るためにアクセスするためのアカウントが発行される。また、カメラへのアクセスは、カメラが設置された部屋にいる子を持つ親に限定される。)

25

[2 2 頁 3 - 5 行]

The sensor server, after determining that the user has entered a valid

login and password, checks the database again to determine which of the cameras at that particular center the user has access to. In this manner, parents can be given access to all of the cameras at a center, or only a subset of the cameras at the center.

- 5 (センササーバは、有効なログインとパスワードをユーザが入力したと判定した場合、データベースを再び調べることによって、そのユーザがその特定の保育所のどのカメラへのアクセス権を有するかを決定する。このようにして、親には、ある保育所のすべてのカメラ、または、その保育所のカメラの一部のみについてのアクセス権が与えられる。)

10

[22頁22－25行目]

- A particular child care center is determined when the user enters the 'center code' but at no time is the center actually identified by name, nor are the actual network addresses of the cameras revealed. This makes it
15 difficult for an unauthorized user with unsavory intentions to determine where the children they are looking at are located.

- (ユーザが「センタコード」を入力したとき、特定の保育所が決定されるが、どんなときも、そのセンタが実際の名称によって特定されることはなく、また、カメラの実際のネットワークアドレスが明らかにされることもない。これによって、不道
20 徳な意図を持つ認証されていないユーザが、彼らが見ている子供の居場所を特定することを困難にする。)

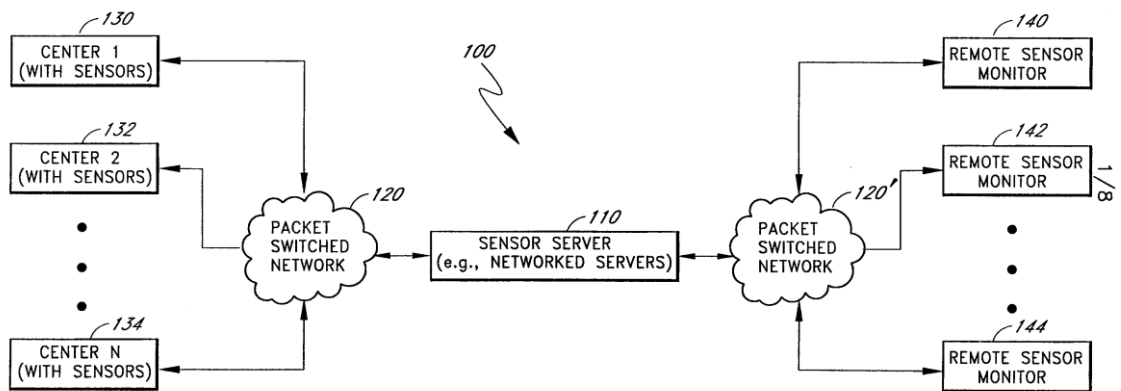


FIG. 1

5

(訳)

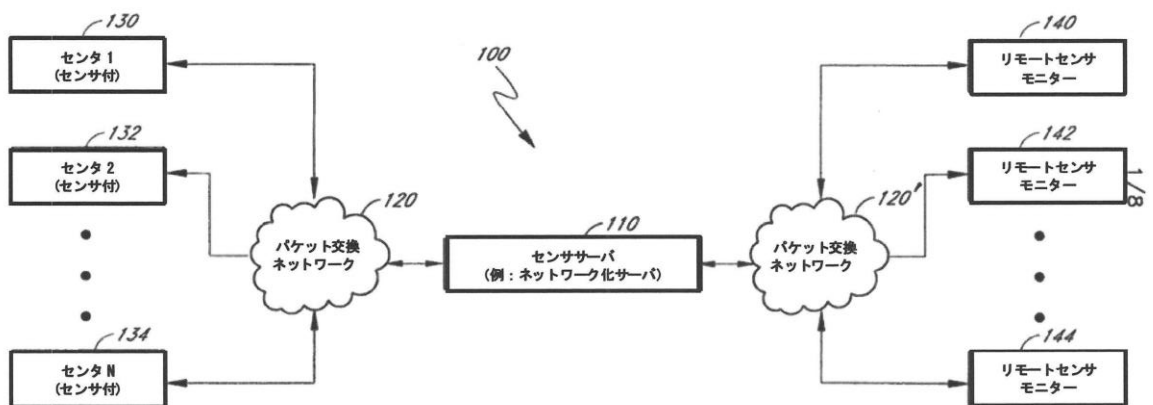


図 1

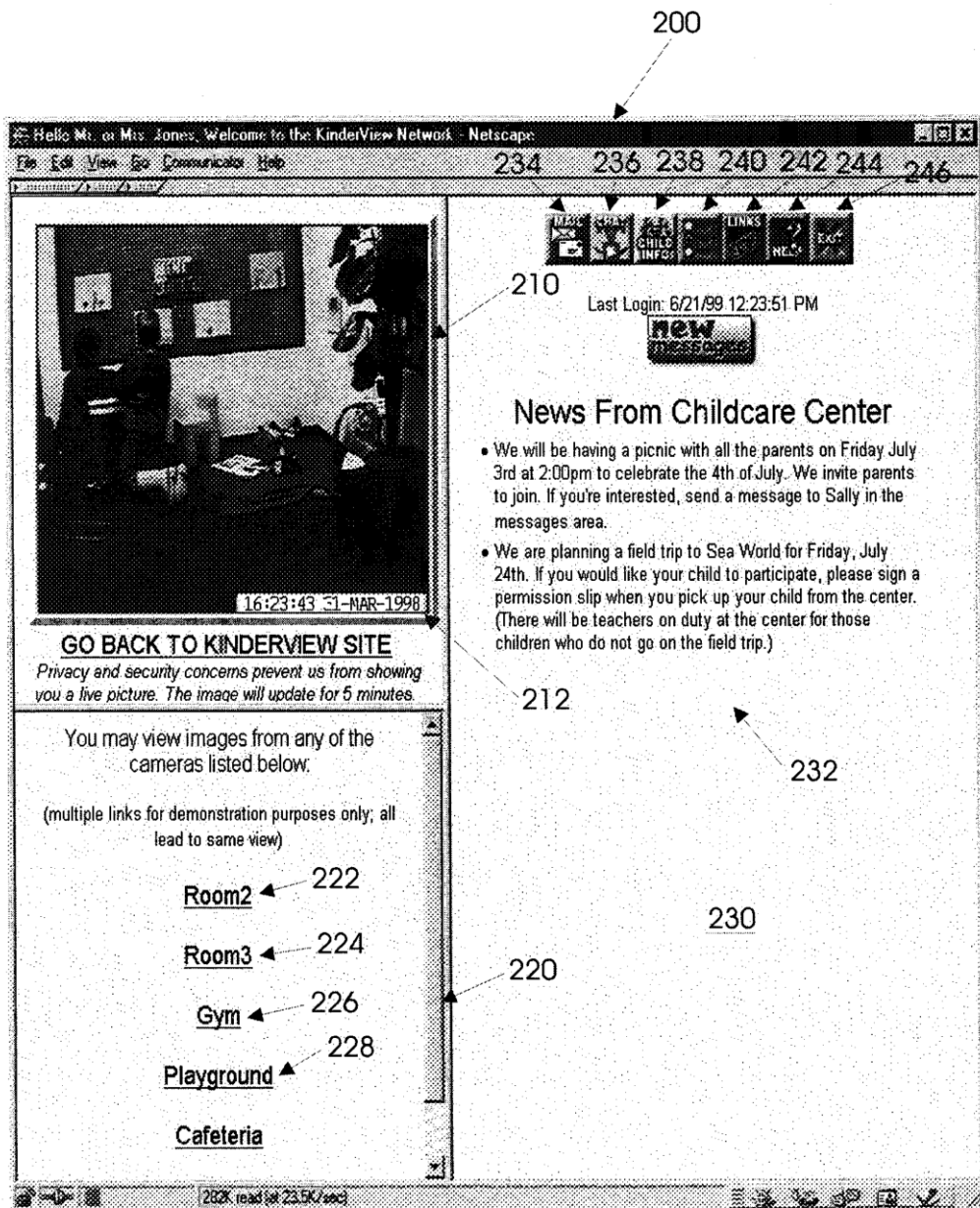


FIG.2

(訳)

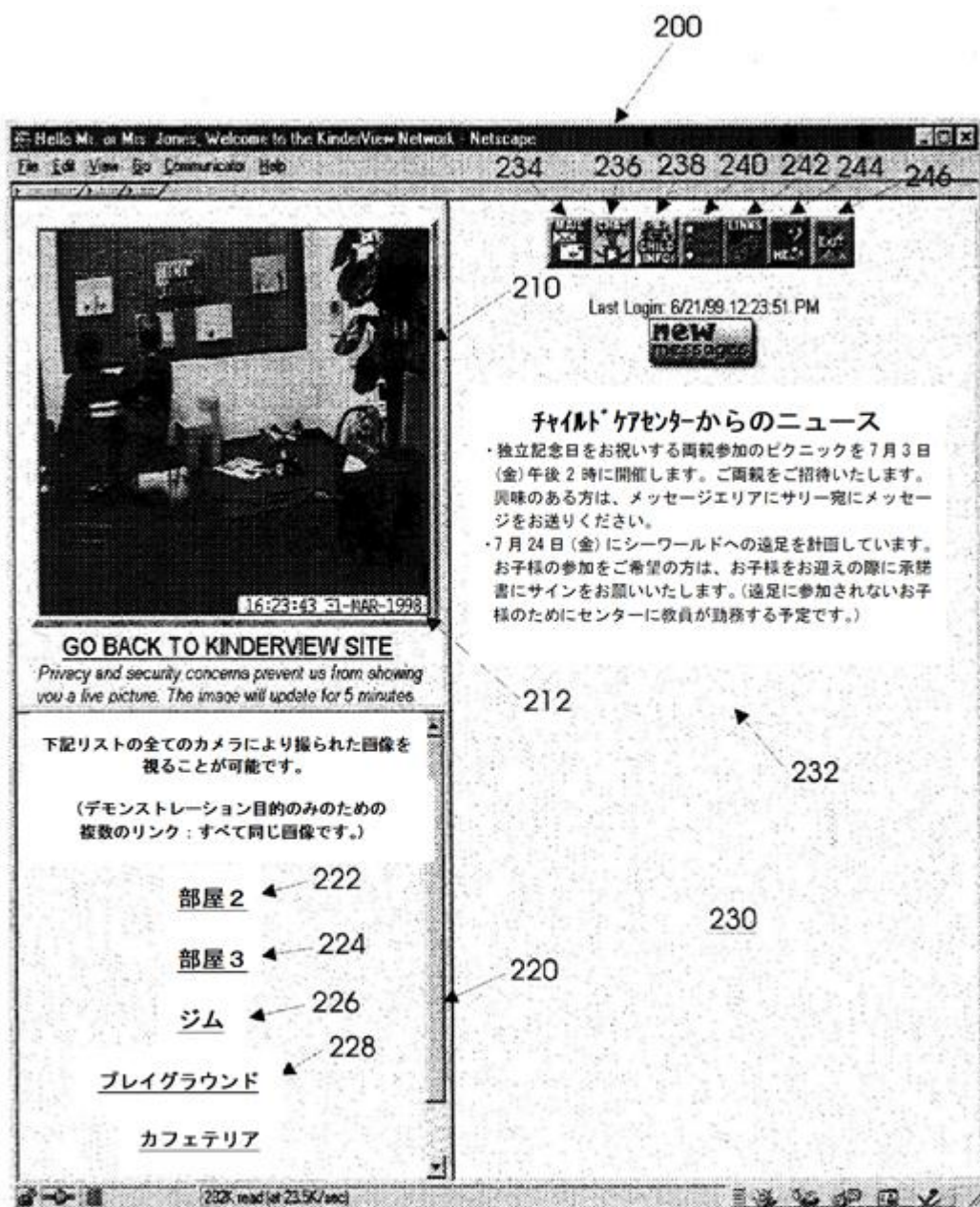
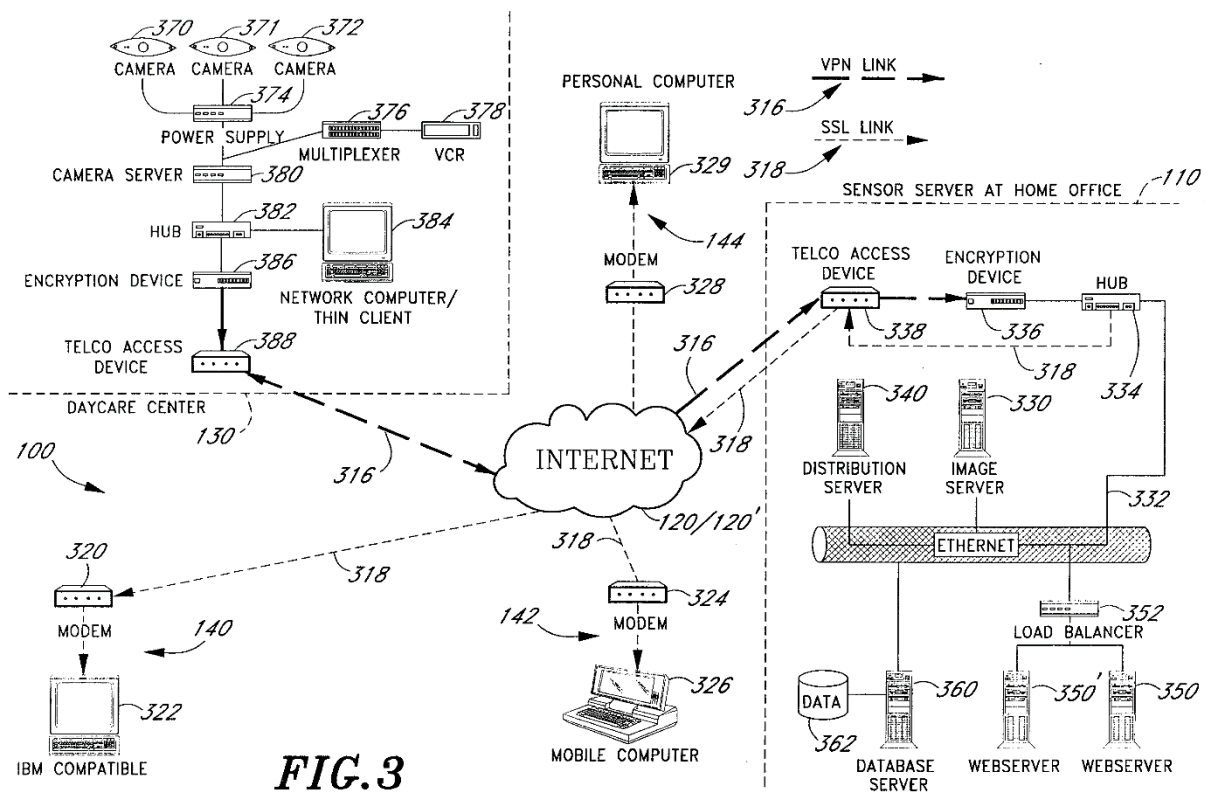


図 2



(訳)

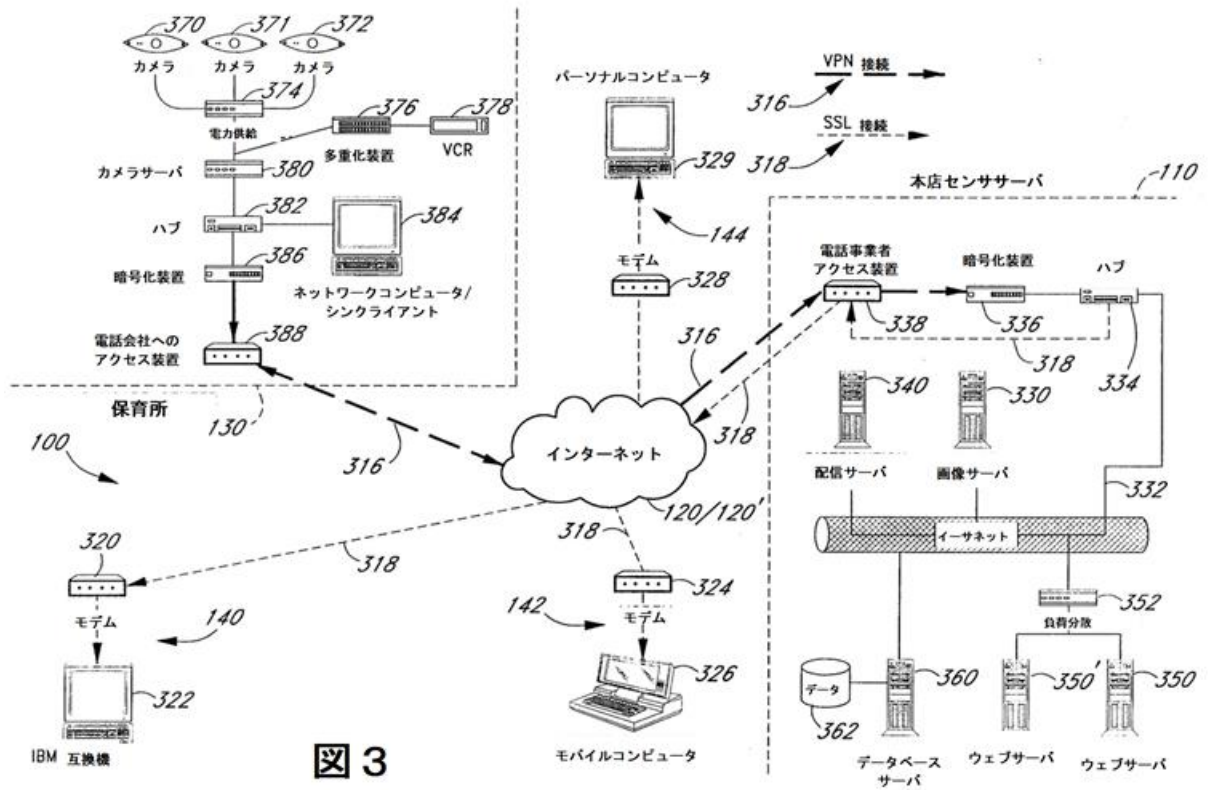


図 3

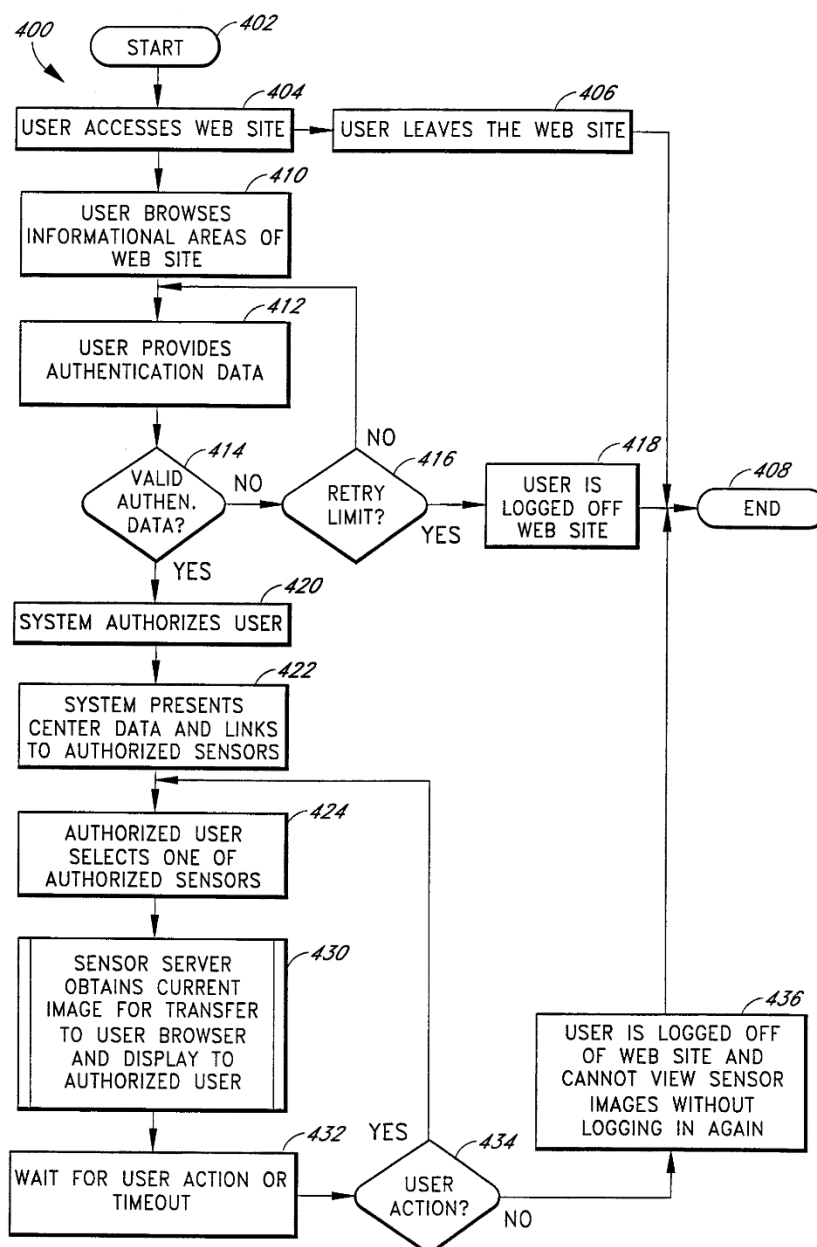


FIG.4

(訳)

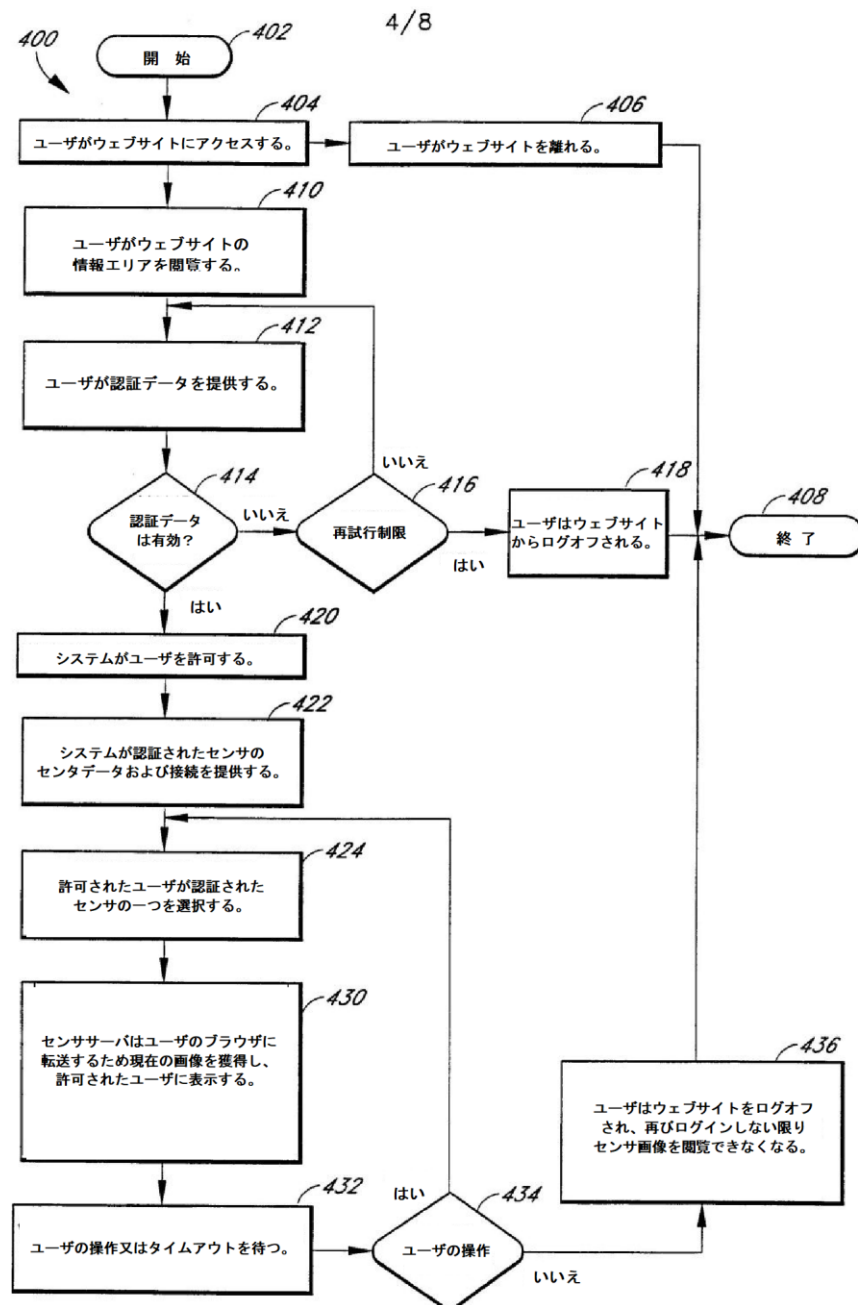
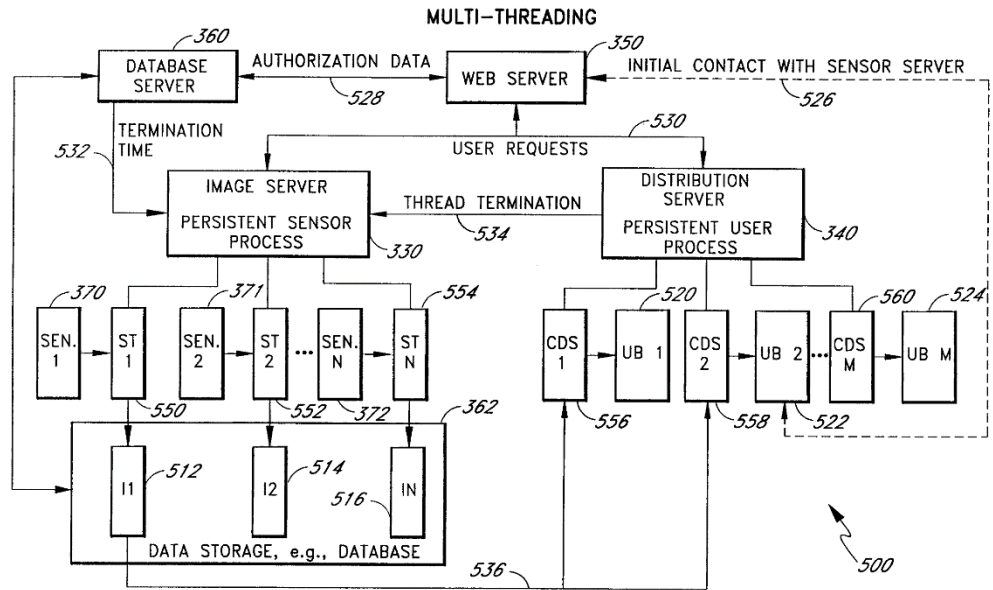


図 4



SEN=SENSOR AT REMOTE LOCATION(E.G., DAY CARE CENTER)
 ST=SENSOR THREAD
 I=IMAGE(S)
 CDS=CLIENT DATA STREAM
 UB=USER BROWSER AT REMOTE LOCATION (E.G., USER'S BUSINESS)

FIG.5

(訳)

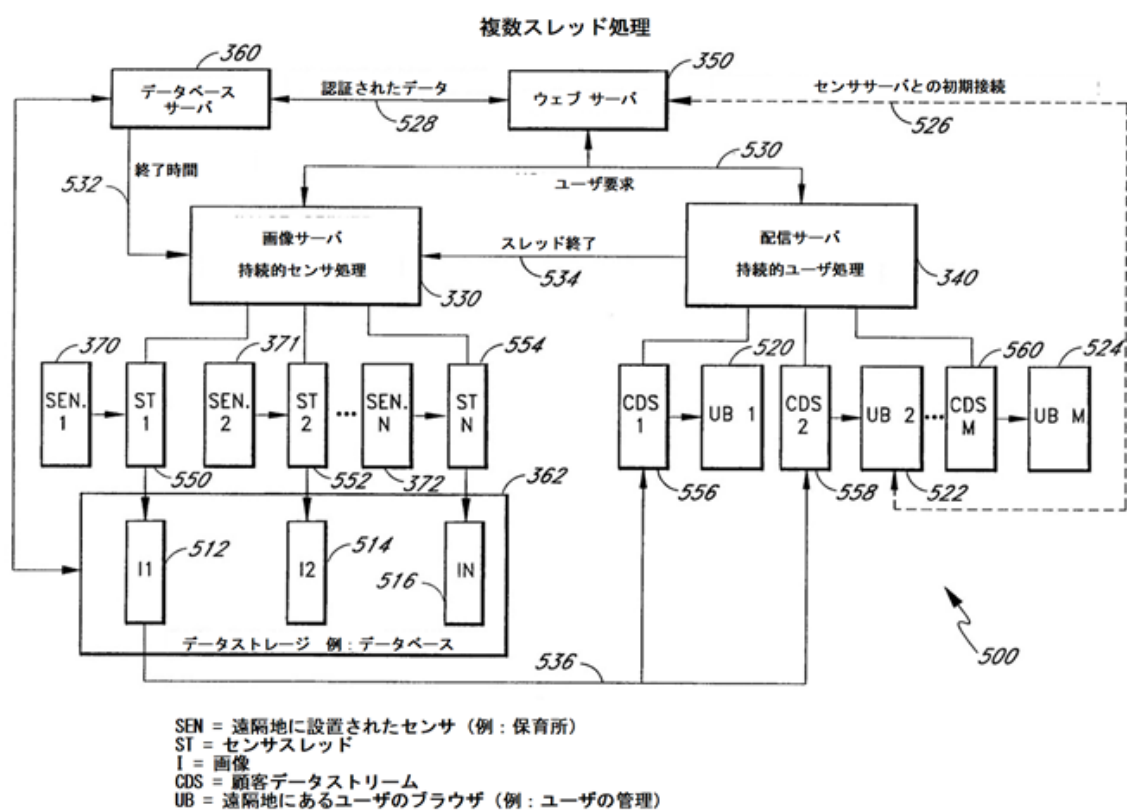


図 5

FETCH IMAGES

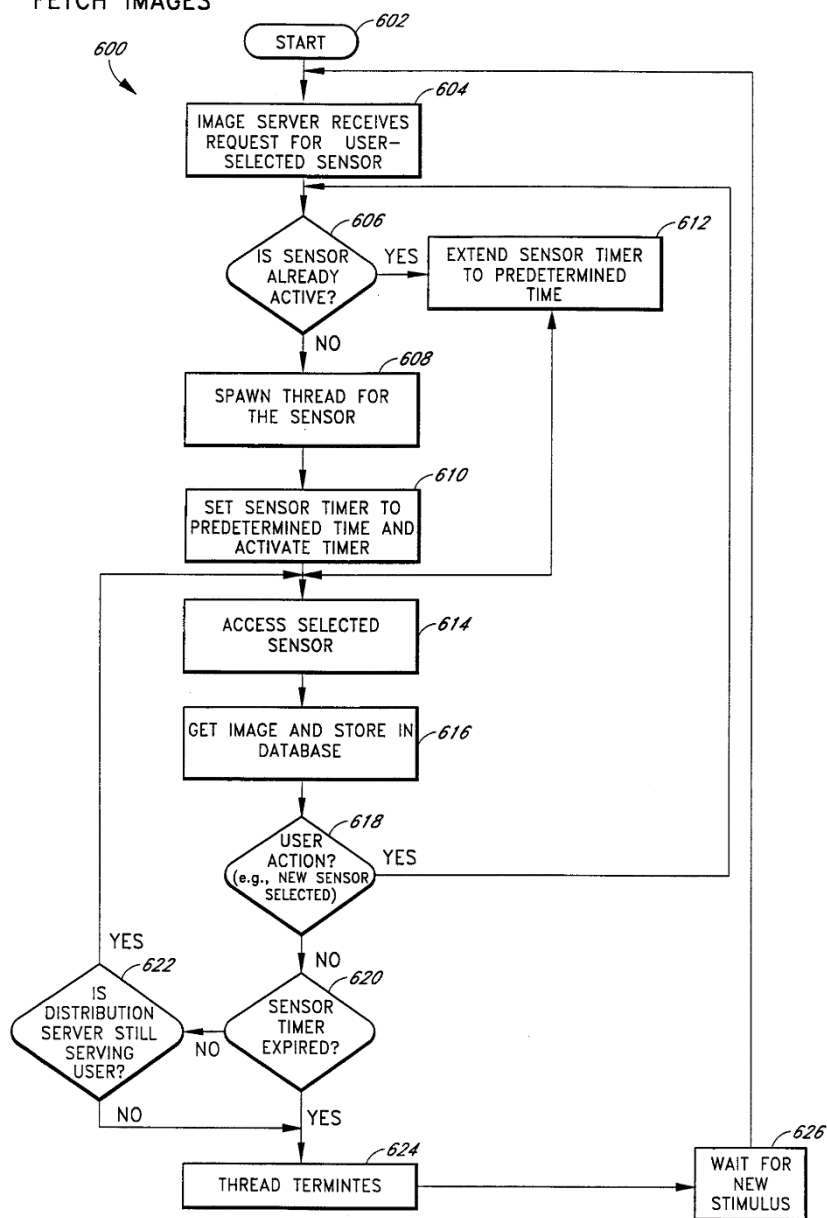


FIG. 6

(訳)

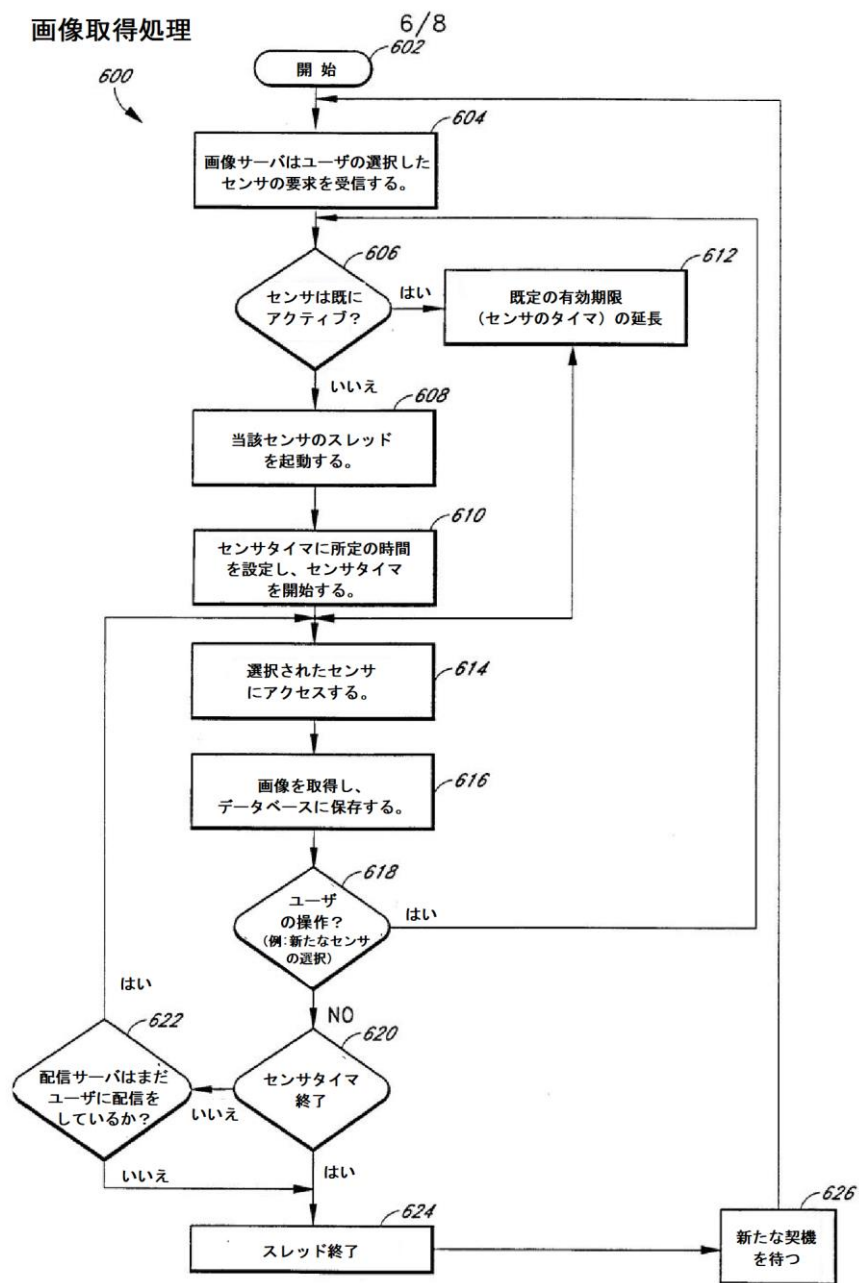


図 6

DISPATCH IMAGES

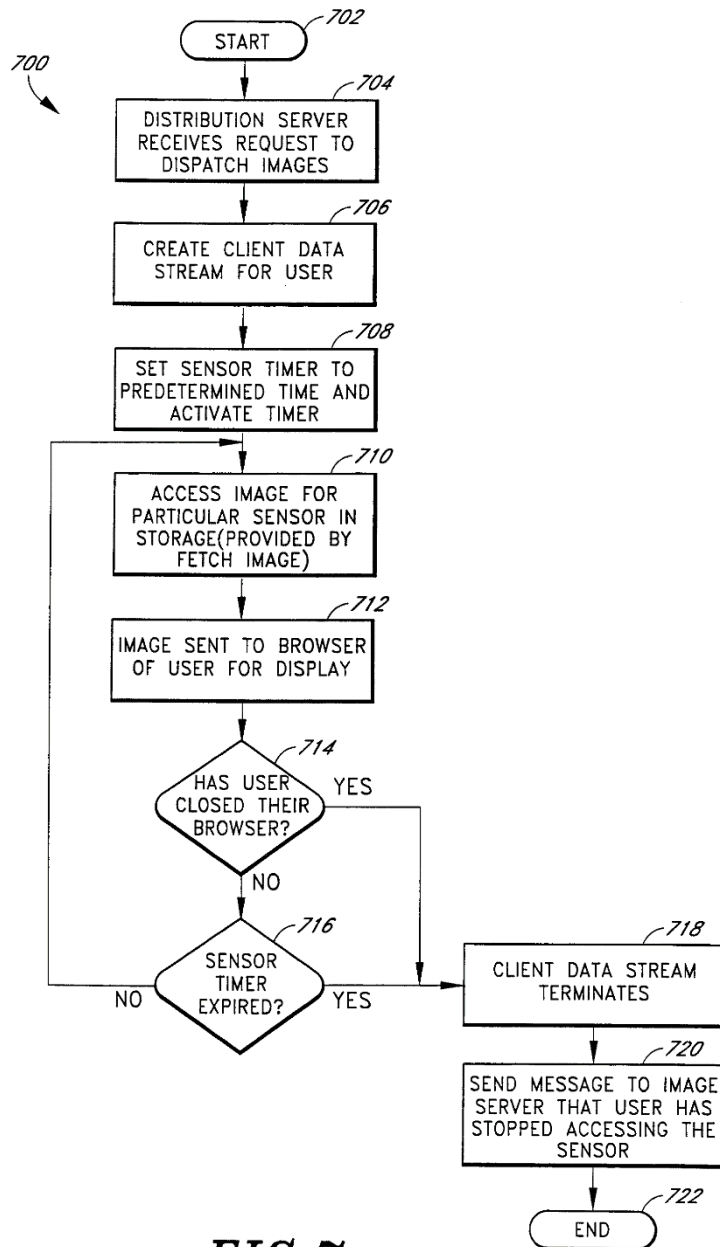


FIG.7

(訳)

画像送信処理

7/8

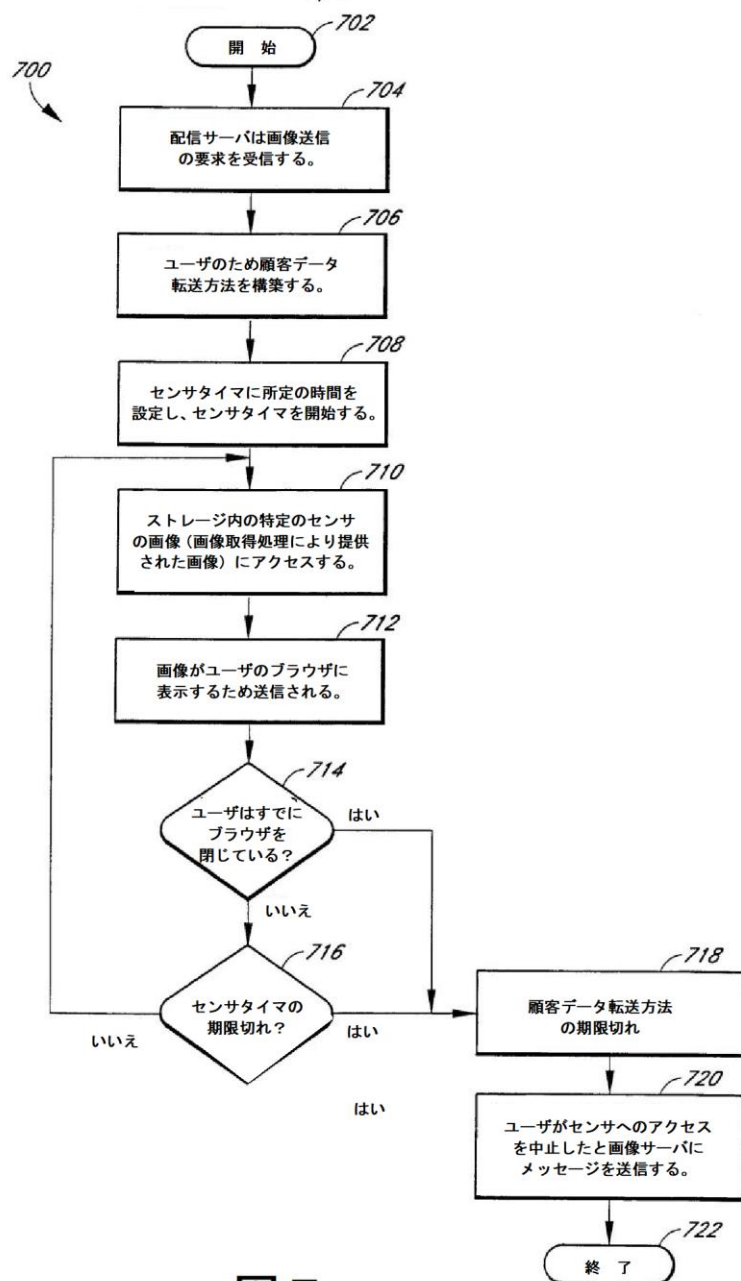


図 7

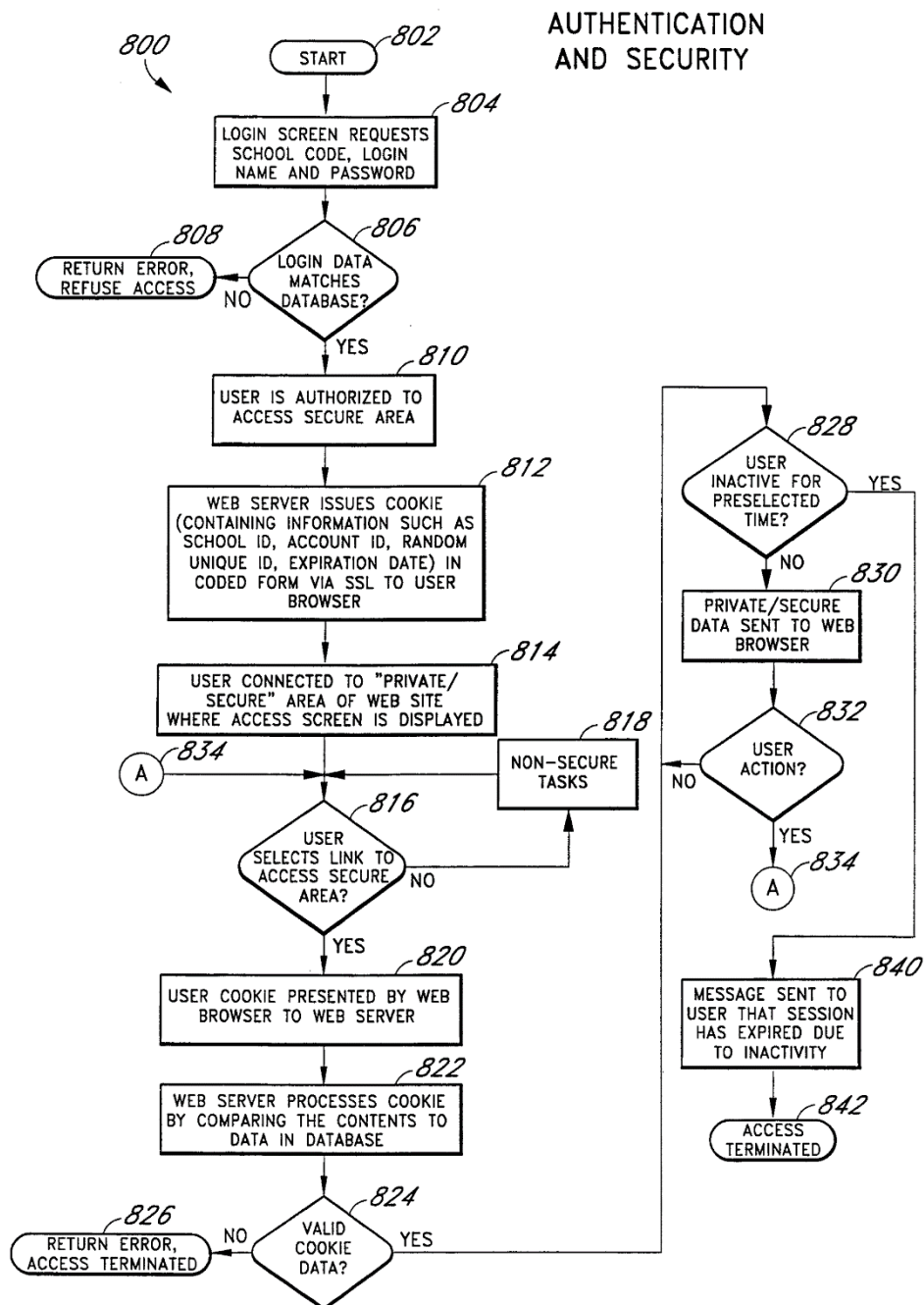


FIG. 8

(訳)

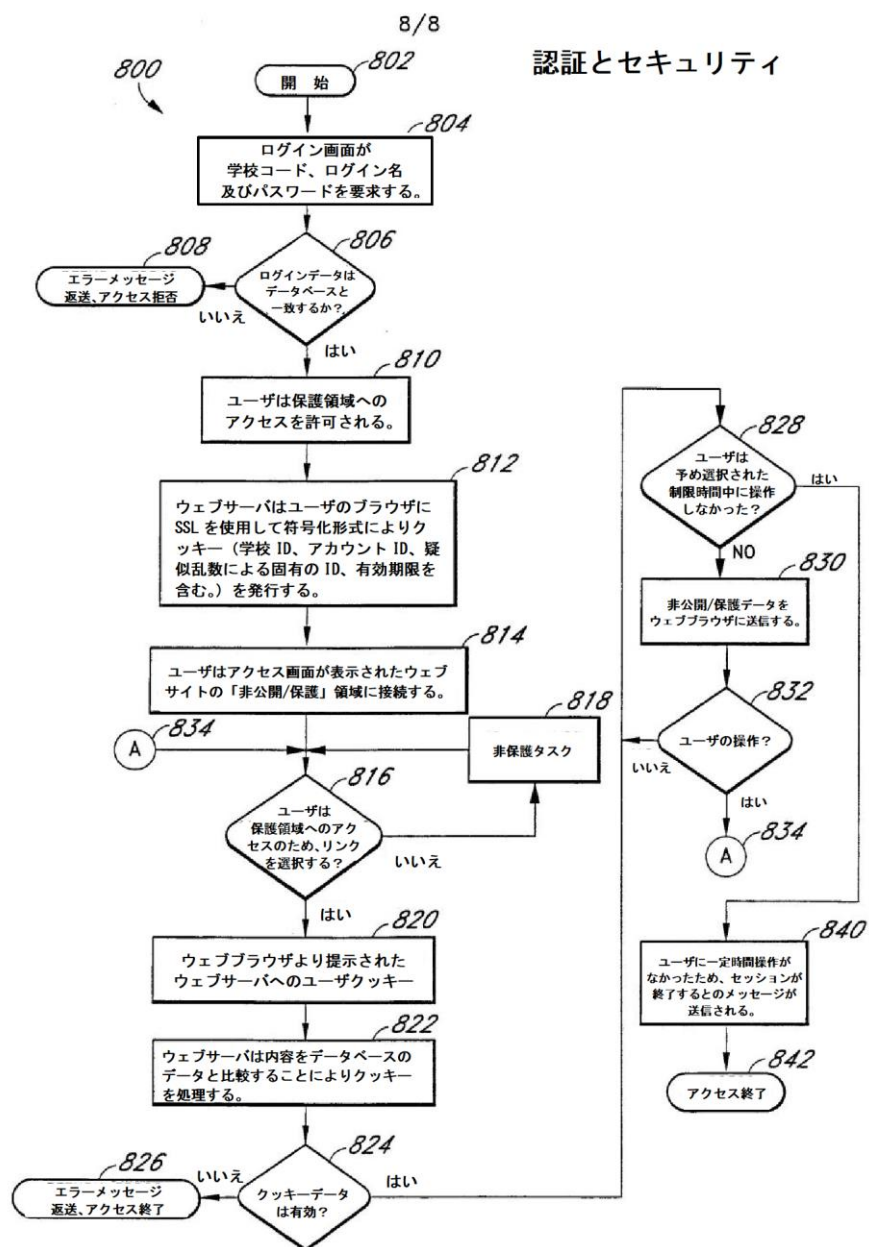


図 8