令和３年３月１６日判決言渡

令和元年（行ケ）第１０１４０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

| | | |
|---|---|---|
| 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 | |
| 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 | |
| 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 | |
| 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。

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２０１８－８０００３３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

１　特許庁における手続の経緯等

⑴　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/ＪＰ０１/０５３８０）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，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２００５－３７０７８号，以下「本件出願」という。）をし，同年７月２２日，その設定登録（特許第３７０１９６２号。請求項の数２。）を受けた（甲２，３，１３，１５，７９。以下この登録を受けた特許を「本件特許」という。）。

⑵　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（甲３３），特許庁は，上記請求を無効２０１８－８０００３３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。

⑶　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，請求項１に係る発明を「本件発明１」と，請求項２に係る発明を「本件発明２」といい，本件発明１と本件発明２を併せて「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】

≪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側に対して付与された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利用者データベースを備え，

≪１Ｃ≫　前記監視端末側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，

≪１Ｄ≫　前記管理コンピュータ側は，

≪１Ｄｉ≫　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，

≪１Ｄⅱ≫　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，

≪１Ｄⅲ≫　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側の制御部に働きかけていく手段と，

≪１Ｄⅳ≫　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，

≪１Ｄｖ≫　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，

≪１Ｄvi≫　特定できる監視端末側から前記管理コンピュータ側のグローバルＩＰアドレスに対して接続する接続処理を受け付け，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手段と，

を備えている

≪１Ｅ≫　ことを特徴とする通信回線を用いた情報供給システム。

【請求項２】

≪２Ａ≫　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側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側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，前記監視端末側によって得られた情報を入手するステップ時，

≪２Ｂ≫　監視端末側に接続不能な状態，若しくは監視端末側からの情報が前記管理コンピュータ側に送信されてこない状態が，前記管理コンピュータ側で確認された時に，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

≪２Ｃ≫　請求項１に記載の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

⑴　本件審決の理由のうち，本件における取消事由に関係する部分の理由の要旨は，①本件発明１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１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１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ない

から進歩性を欠如せず，③本件発明２は本件発明１に従属する請求項であるから，甲１発明が構成要件２Ａ及び２Ｂの構成を有するか否かを検討するまでもなく新規性を欠如しないことが明らかであり，構成要件２Ａ及び２Ｂの容易想到性を検討するまでもなく進歩性を欠如しないことが明らかであるというものである。

⑵　本件審決が認定した甲１発明，本件発明１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ＶＰＮ（仮想私設網）であって，

（イ）　保育所，例えば，センタ１（１３０），センタ２（１３２），センタ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，

（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，

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，

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，

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，

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，

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，

(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，

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，

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，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，

（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，

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，

（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，

（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，

（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，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に問い合わせて，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し，

（コ） 画像取得プロセスにおいて，画像取得プロセス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，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，

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に格納し，

(サ) 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し，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，再試行を行い，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，

(シ) 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，

（タ） ＶＰＮ監視システム１００。

イ　本件発明１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，

≪１Ｃ≫　前記監視端末側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，

≪１Ｄ≫　前記管理コンピュータ側は，

≪１Ｄｉ≫　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，

≪１Ｄⅱ≫　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，

≪１Ｄⅲ≫　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側の制御部に働きかけていく手段と，

≪１Ｄⅳ≫　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，

≪１Ｄｖ≫　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，

を備えている

≪１Ｅ≫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

本件発明１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利用者データベースを備え」る（構成要件１Ｂ）のに対し，甲１発明（構成要件１Ｂ’）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１では，「前記管理コンピュータ側は」（構成要件１Ｄ），「特定できる監視端末側から前記管理コンピュータ側のグローバルＩＰアドレスに対して接続する接続処理を受け付け，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手段」を備えている（構成要件１Ｄvi）のに対し，甲１発明では，接続処理を受け付けて，利用者データベースに登録されているＩＰアドレスを変更処理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

⑴　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）

⑵　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

⑴　原告の主張

本件審決は，前記第２の３⑵イ(イ)のとおりの相違点を認定したが，本件発明１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

本件審決は，①本件発明１の構成要件１Ｂは「監視端末側に対して付与された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」とされ，本件発明１では，「利用者データベース」で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ること，②本件発明１の「利用者データベース」に対応するのは甲１発明のセンササーバ１１０の「データベース３６２」であること，③甲１発明の「データベース３６２」は，「ユーザ名，パスワード」と「センタコード」との対応付けであるユーザ認証と，「ユーザ」と「カメラ名」との対応付けであるユーザ情報提供の機能しかないことから，本件発明１と甲１発明とが相違点１の点において相違すると認定した。

しかしながら，本件発明１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と「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。

そして，甲１発明において，センササーバ１１０中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１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」等にセンタ１３０側（「監視端末側」）に対して付与されたＩＰアドレスが登録されており，また，「データベース３６２」に登録された「センタコード，ユーザ名，パスワード，カメラ名」は，本件発明１の「監視端末情報」に相当するとともに「利用者ＩＤ」にも相当する。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

本件発明１の構成要件１Ｄviは，ＤＨＣＰ（「Ｄｙｎａｍｉｃ　Ｈｏｓｔ　Ｃｏｎｆｉｇｕｒａｔｉｏｎ　Ｐｒｏｔｏｃｏｌ」。ＩＰアドレ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，監視端末のＩＰアドレスが変更された時に，監視端末側から管理コンピュータ側に接続し，管理コンピュータ側のデータベースにおける監視端末側のＩＰアドレスを新たなＩＰアドレスに変更処理をすることを受け付ける機能を規定しているところ，本件審決は，甲１発明では，そのような変更処理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１と甲１発明とが相違点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，甲１発明に動的ＩＰアドレスが用いられることは，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１の構成

（構成要件１Ｄvi）は，実質的な相違点を構成しない。

（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３ｃ４３０００」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）。

「３Ｃｏｍ社５６ｋ　ＭＬＰＰＰスイッチ，型番３ｃ４３０００」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ＩＰアドレスを用いることができる。

「Ｎｅｔｇｅａｒ社ＩＳＤＮモデム，型番ＲＴ３２８」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（ＩＳＰ）のＩＳＤＮアカウントを得ている場合，あなたが登録されたＩＰアドレスを必要としていない限り，静的ＩＰアドレス又は動的ＩＰ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５４の６頁），「型番ＲＴ３２８」の「電話事業者アクセス装置３８８」を用いる甲１発明においては動的ＩＰ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，Ｒａｖｌｉｎ－４有線暗号化装置に，１０ｂａｓｅ－Ｔケーブルで接続される。」との記載（８頁２４行ないし９頁８行目）や「電話事業者アクセス装置３８８」接続されているリン

ク３１６がＶＰＮリンクであることが示されている（図3）から，センタ１３０とセンササーバ１１０とのリンク３１６は「Ｒａｖｌｉｎ－４」が採用するＩＰＳｅｃに基づいてＶＰＮ通信を実現するものである（甲１８の１頁左欄第２段落下から３行から末行まで）ところ，ＩＰｓｅｃに基づくＶＰＮ通信においては動的ＩＰアドレスが用いられる（甲１９，２０の１の２９７頁，２０の２の２８５頁，２２の３３頁，２５の３頁，２６の１３３頁，２８の１３６頁）。

（ウ） 本件特許の優先日当時，ＩＰｓｅｃや，ＶＰＮでＩＰｓｅｃを用いることは周知であり（甲７３の２頁，７４の６２～６３頁，７５の４頁・７頁・１０頁，甲７６の６頁の図６），ＩＰｓｅｃにおける自己接続機能も周知であった（甲２０の１の２９７頁，３０２頁，３０３頁，２１の６－２５頁～６－２６頁，２２の１６頁，２３の６頁）。

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，６０の１１頁左欄，６１，６

５の５４頁）。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１と甲１発明との間には相違点が存しないから，本件発明１は甲１発明である。

そうすると，本件発明１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並びに相違点１及び相違点２が存することから直ちに本件発明２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。

⑵　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

本件審決は，甲１発明において，「データベース３６２」に記憶されるユーザ認証用の「ユーザ名」と，利用の目的が異なる別の装置である「アクセス装置３３８」等の記憶装置に記憶されることが想定される相手装置との通信用のＩＰアドレスとを対応付けてデータベースとして構成する必要性がないとしたまでであり，原告の主張するような解釈をとったのではない。

甲１発明のセンササーバ１１０の「アクセス装置３３８」等の記憶装置

にセンタ１３０の「アクセス装置３８８」のＩＰ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３８８」等のＩＰ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ＩＤ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ても，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ＩＰアドレスを（動的ＩＰアドレス・静的ＩＰ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，ＶＰＮ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，ＶＰＮ内の装置は，互いにプライベートＩＰ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のないグローバルＩＰアドレスを（動的ＩＰアドレス・静的ＩＰ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１１０の「アクセス装置３３８」等の記憶部に記憶されているセンタ１３０のＩＰ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。

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１１０の「アクセス装置３３８」等の記憶部に記憶されているセンタ１３０のＩＰ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ＩＰアドレスであろうと静的ＩＰ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に登録されている前記監視端末端末情報であるＩＰアドレスを変更処理する手段」（構成要件１Ｄvi）を備えていないことは明らかである。

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１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１は甲１発明ではない。

そうすると，本件発明１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並びに相違点１及び相違点２が存することから本件発明２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

⑴　原告の主張

仮に，本件発明１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１⑴イの事情からすると，センササーバ１１０のいずれかの記憶部に記憶されたセンタ１３０のＩＰアドレスとして，静的ＩＰアドレスではなく動的ＩＰアドレスを用いることは当業者に容易に想到できた。

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並びに相違点１及び相違点２が容易想到ではないことから直ちに本件発明２が進歩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。

⑵　被告の主張

甲第１号証には，センタ１３０側のＩＰアドレスとして動的ＩＰ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ＩＰアドレスを用いるとしても，その動的ＩＰアドレスをユーザ名に対応付けす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利用者データベース」を備え，かつ，相違点２に係る「利用者データベースに登録されているＩＰアドレスを変更処理する手段」を備える構成とすることは容易想到ではない。

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並びに相違点１及び相違点２が容易想到ではないことから直ちに本件発明２は進歩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

１　本件明細書の記載事項について

本件明細書（甲７９）には，別紙１「本件明細書の記載事項」のとお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。

⑴　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者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】）。

⑵　上記目的を達成するために，本件発明は請求項１及び請求項２の構成をとった（【０００８】）。

⑶　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】）。

⑷　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】）。

⑸　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（【００２

６】，【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」のとおりの記載事項があり（訳は本件審決，甲８０，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３⑵ア（甲１発明）のとお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

⑴　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一つからなる利用者ＩＤである特定情報」を入手し（構成要件１Ｄⅰ），「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１Ｄⅱ），「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１Ｄⅲ）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３５に記憶され，利用者の電話番号，ＩＤ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ＩＰアドレスを対応付けているものであり（【００２０】，【００２１】，【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ＩＰ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（【００２６】，【００２９】，【００３０】，【図７】）。

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ＩＤ」）に，当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たグローバルＩＰ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１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１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ＩＰアドレス等の情報が，検索できる程度に対応付けられて登録されていることを要するものの，それで足り，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ＩＰアドレスが関連性な

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，「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ＩＰアドレスの記憶について

（ア）甲１発明において，センタ１３０とセンササーバ１１０との間のリンク１２０は，公衆交換電話網（ＰＳＴＮ）を横切る暗号化ＶＰＮとなっており（甲１の４頁１２行ないし５頁７行目），そして，入りネットワーク接続３１６は電話事業者アクセス装置３８８に接続され，電話事業者アクセス装置３８８は暗号化装置３８６に接続され，暗号化装置３８６はハブ３８２に接続され，ハブ３８２はカメラサーバ３８０に接続され，カメラサーバ３８０はメディアアグリゲータ３７４に接続され，メディアアグリゲータ３７４はカメラ３７０～３７２に接続されている（同８頁２４行ないし９頁８行目）。また，センササーバ１１０の画像サーバ３３０はインターネットプロトコルを用いたＨＴＴＰ，Ｔｅｌｎｅｔで，保育所（センタ１３０）に配置されたカメラ（３７０，３７１，３７２）と通信を行う（同１６頁２３ないし２６行目，１６頁３２ないし３５行目）。

甲第１号証には，ＩＰ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１１０は，インターネットプロトコルを用いてセンタ１３０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１３０側に付与されたグローバルＩＰアドレスを必要とすることや，センタ１３０内の装置相互は通常プライベートＩＰ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１１０のどこかの記憶部が，センタ１３０のアクセス装置３８８又はその先の暗号化装置３８６に付与されたグローバルＩＰ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４１２に進み（１１頁２８行ないし１２頁７行目，図４），状態４１２において，ユーザは，「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３６０がデータベース３６２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（１２頁８ないし１４行目，図４），Ｗｅｂサーバ３５０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３６２をチェックすることを，データベースサーバ３６０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し（１２頁１８ないし２６行目，図４），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に問い合わせて，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し（１４頁９ないし２２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.」（１３頁４ないし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３３０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３４０は，データストレージ３６２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いても，カメラとの接続は１つだけになる。」（１３頁７ないし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３６２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１３０側に付与されたＩＰアドレスをセンササーバ１１０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それぞれのカメラ名に対応付けてＩＰ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側に付与された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もできない。

ウ　以上からすると，甲１発明については，本件発明１の「監視端末情報」に相当するセンタコードと本件発明１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１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１は，「利用者データベース」を備えることによって，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，このＩＰアドレスを変更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１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１の「利用者データベース」に相当する旨主張する。

本件発明１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ているなどの関連性があるわけではないから，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１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

以上によれば，甲１発明において，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。

⑵　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１は新規性を欠如せず，また，本件発明２は本件発明１に従属する請求項であるから，甲１発明が，構成要件２Ａ及び２Ｂの構成を有するか否かを検討するまでもなく新規性を欠如しないことが明らかであり，本件審決の新規性判断に誤りはない。

したがって，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

⑴　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１３０側に付与されたＩＰ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ＩＤと対応させてセンササーバ１１０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１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。

⑵　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１は進歩性を欠如せず，また，本件発明２は本件発明１に従属する請求項であるから，甲１発明が，構成要件２Ａ及び２Ｂの構成を有するか否かを検討するまでもなく進歩性を欠如しないことが明らかであり，本件審決の進歩性判断に誤りはない。

したがって，取消事由２は理由がない。

５　結論

よって，原告主張の取消事由は理由がないから，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

裁判官　＿＿＿＿＿＿＿＿＿＿＿＿

本　　吉　　弘　　行

裁判官

中　　村　　恭

（別紙１）

本件明細書の記載事項

【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う個人宅，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。

【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】

【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，前記監視端末側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，

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側の制御部に働きかけていく手段と，

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，

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，

特定できる監視端末側から前記管理コンピュータ側のグローバルＩＰアドレスに対して接続する接続処理を受け付け，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）

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利用者データベースを備え，

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と，

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ＩＰ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 ID を受け付け，この監視端末 ID が適正な場合のみ，ＩＰ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，ＩＰアドレスが変更された場合は，前記監視端末は，古いＩＰアドレスと新しく与えられたＩＰ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ＩＰ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ＩＰ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，自己の監視端末 ID を基にその時点手付与されているＩＰ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ＩＰ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，自己の古いＩＰアドレスを基にその時点手付与されているＩＰ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ＩＰ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。

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いると好ましく，利用者のどのような機種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，

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，

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ＩＰ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ＩＰ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利用者データベースを備え，

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，

更に，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ＩＰアドレス変更要求する監視端末が，

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ＩＰ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ＩＰ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】

【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（４ａ．４ｂ．４ｃ... ４ｚ...）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，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，から主に構成されている。

【００１２】

また，本実施例に用いた監視端末４（４ａ．４ｂ．４ｃ... ４ｚ...） は，図１に示すように，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４ａ～４ｃ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ＡＤＳＬ（ＤＳＬ），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４ａ～４ｃ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。

【００１９】

次いで，この監視ユニット１に接続されるとともに，前記通信回線網５（ＡＤＳＬ回線）に接続されて，管理コンピュータ３との間にてデータの送受信を行う通信手段であるセットトップボックス２の構成は，図１０に示すように，前記監視ユニット１である監視端末や，パーソナルコンピュータを接続するＡＤＳＬ送受信機，およびアナログ電話機を接続する端子が設けられ，これらは交換局に繋がる電話回

線にフィルタを介して接続されている。ここで交換局においては，周波数帯域を基準にして電話交換機もしくはＡＤＳＬ送受信機とにフィルターを介して振り分けられる。このように，この実施例では，ＡＤＳＬを利用するため定料金で常時接続のサービスが可能となっており，管理コンピュータ３に新しい画像情報が逐次送信されてくることになる。

【００２０】

また，本実施例の監視ユニット１は前述のように通信部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。

【００２１】

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（４ａ．４ｂ．４ｃ... ４ｚ...）からのデータ圧縮された画像（ 並びに音データ）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３０に，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）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報端末である例えば携帯電話１１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（ＣＰＵ）３１や，前記ＣＰＵ３１のワークメモリ等に使用されるＲＡＭ３２や，ディスプレイ等の表示装置３４や，キーボードやマウス等の入力装置３６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（ＲＴＣ）３７，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３８と，利用者の情報端末である携帯電話１１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３３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（ＩＤ）に対応付けて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アドレスに基づいた利用者データベース（ＤＢ）（なお，ＩＤも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）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処理能力に優れたコンピュータとされている。

【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ＩＤ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ＰＣが所有するＩＤ（グローバルＩＰアドレス，利用者ＩＤ）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て送信可能なＡ／Ｄ変換部（図示略）を設けるとよい。

【００２３】

また前記通信回線基板３３には，アクセス者の電話番号データを取り出す電話情報受信手段としてのコールＩＤ検出部（図示略）を設けることもでき，アクセス者の電話番号データを前記中央演算処理装置（ＣＰＵ）３１に対して出力して利用者ＩＤを確認することもできる。

【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１１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ＩＤ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ＰＣが所有するＩＤ（グローバルＩＰアドレス，利用者ＩＤ）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１１より送信されてきた利用者ＩＤと暗証番号とを，前記記憶装置３５に記憶されている利用者ＤＢ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ＤＢを用いて検索エンジンで検索を行い，この利用者ＤＢ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。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に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４ａ側の通信制御部，すなわち図４のＭＰＵ６５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。

【００２７】

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ＣＣＤカメラ５５により撮影された画像データ，並びに前記集音マイク５３により集音され前記ＰＣＭコーデック５２によりデジタル化された音データは，前記ＤＳＰ５６により所定のデータ圧縮方式であるＭＰＥＧ方式（ＪＰＥＧ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を通じて送られるようになっている。

【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ＣＰＵ３１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。

【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４ａからの画像情報などは，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。

【００３１】

この監視端末４ａ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３５に一時記憶（蓄積）されて，通信回線基盤３３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，ＰＣ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，ＰＣ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ってはC-ＨＴＭＬ，パーソナルコンピュータにあってはＨＴＭＬ等に変換されて送信される。

【００３３】

これら利用者の情報端末である携帯電話１１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１６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ロ１７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ＩＰアドレスとともに登録された所定のＩＤ，すなわち監視端末ＩＤ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ＩＰアドレスを登録するように要求する。

【００３８】

接続状態でＩＰアドレスが変更された場合は，前記ＭＰＵ６５は，現在のＩＰアドレスと新しく与えられたＩＰアドレスとの違いを判断し，相違する場合は，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

て自ら接続処理し，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。

【００３９】

すなわち図８に示されるように，ＭＰＵ６５の機能として，ＩＰ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ＩＰアドレスとともに登録された所定のＩＤ，すなわち監視端末ＩＤ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ＩＰアドレスを登録するように要求する。

【００４０】

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ＩＤ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ＩＤが利用者データベース（ＤＢ）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（ＤＢ）から対象の監視端末を検索，抽出する。さらに利用者データベース（ＤＢ）の古いＩＰアドレスに代えて新たなＩＰアドレスを更新処理する。

【００４１】

また，監視端末が，常時接続状態のままＩＰ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，自己の古いＩＰアドレスを基にその時点手付与されているＩＰ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（ＤＢ）に，監視端末に対応する古いＩＰ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ＩＰアドレスを更新登録要求に応じても良い。

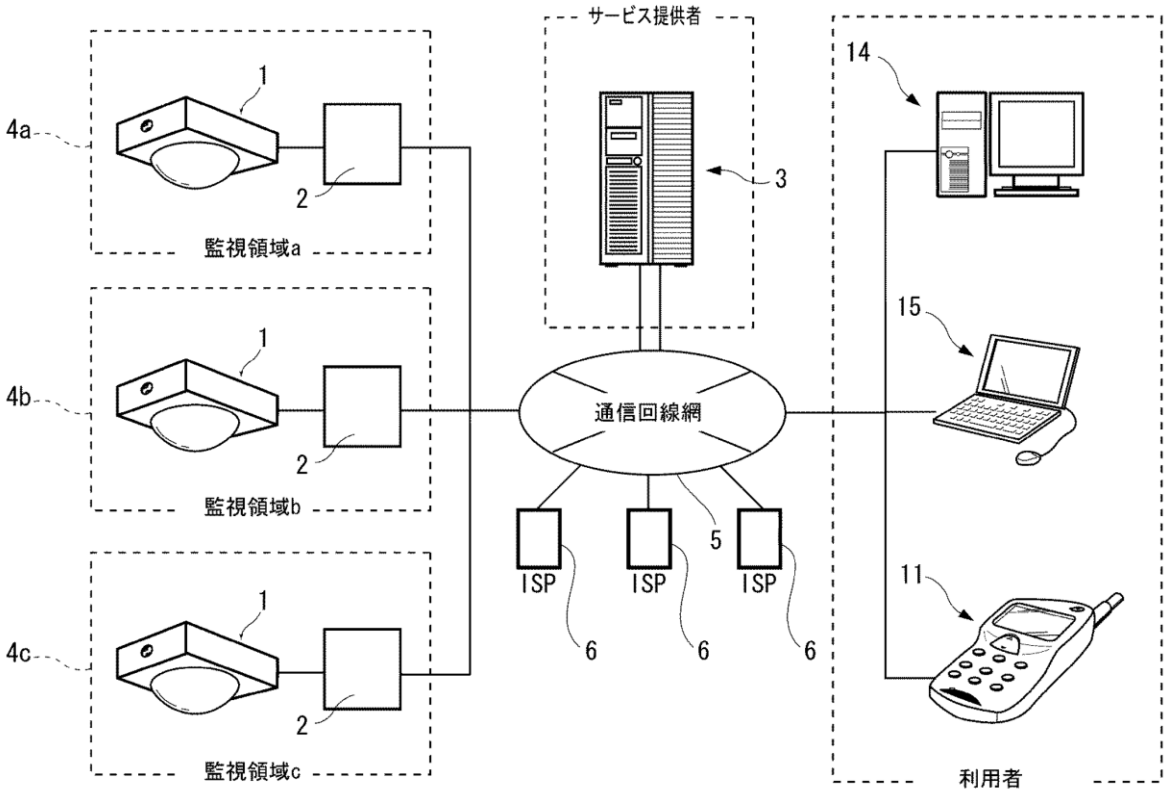
【００４２】

なお，管理コンピュータ３にあっては，インターネットを介して接続してきた情報端末と監視端末とをつなぐ処理を行うことを中心としたサービスを行ってもよく，利用者の情報端末である例えば携帯電話１１等に接続処理し，監視端末と利用者の情報端末からそれぞれ送信される所定のコマンドデータや画像（並びに音） データの送受信の仲介，接続を行うデータ転送処理を行うようになっている。ここで管理コンピュータ３ は，両者の接続に関し操作に関するガイダンスサービスを行う。例えばインターネット接続の許容時間を利用者に与えた場合，その残り時間のガイド，監視端末が接続不良になった場合のアナウンスなどを行う。

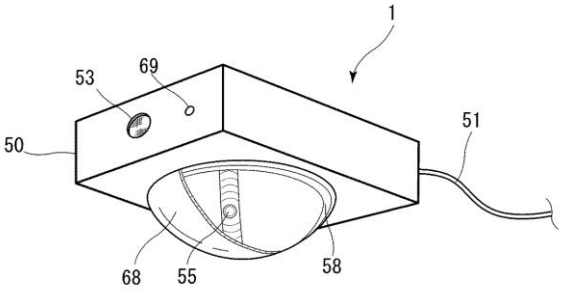
【００４３】

前記利用者ＩＤに対応する監視端末ＩＤ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４によって得られた情報を入手するステップ時，監視端末４に接続不能な状態，若しくは監視端末４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３で確認された時に，利用者との通信を一定時間で切らずに，所定の異常通知「例えば，データを取得できません」などのメッセージ（取得できない理由として，例えばインターネット通信環境が悪い，電源の入力忘れ，侵入者による切断行為などが考えられる）をアクセスした利用者に送信できるようになっている。

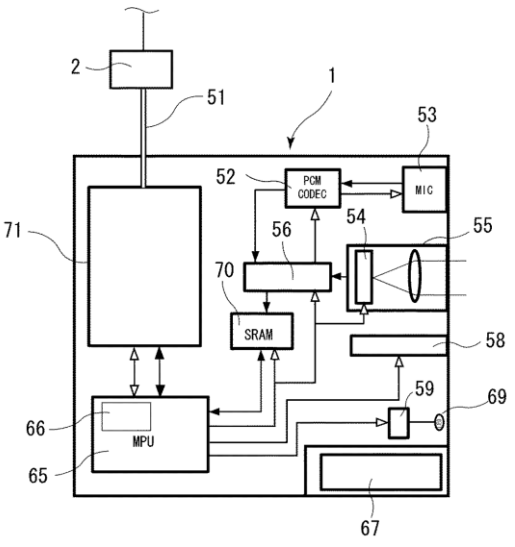
【図１】


サービス提供者
1
4a
2
監視領域a
3
14
4b
監視領域b
15
通信回線網
5
ISP
ISP
ISP
6
6
6
11
4c
監視領域c
利用者

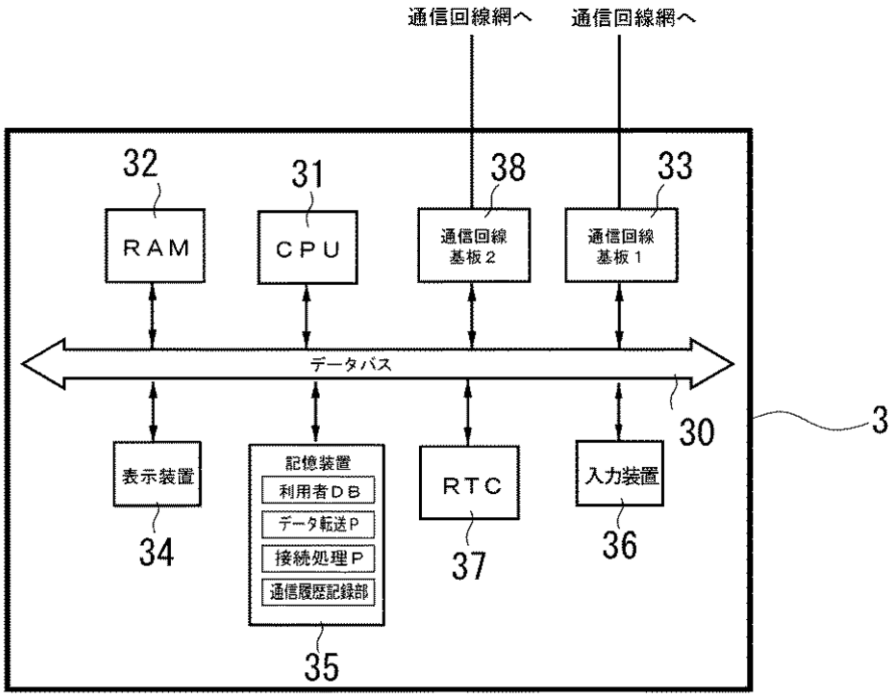
【図３】


1
53
69
50
51
68
55
58

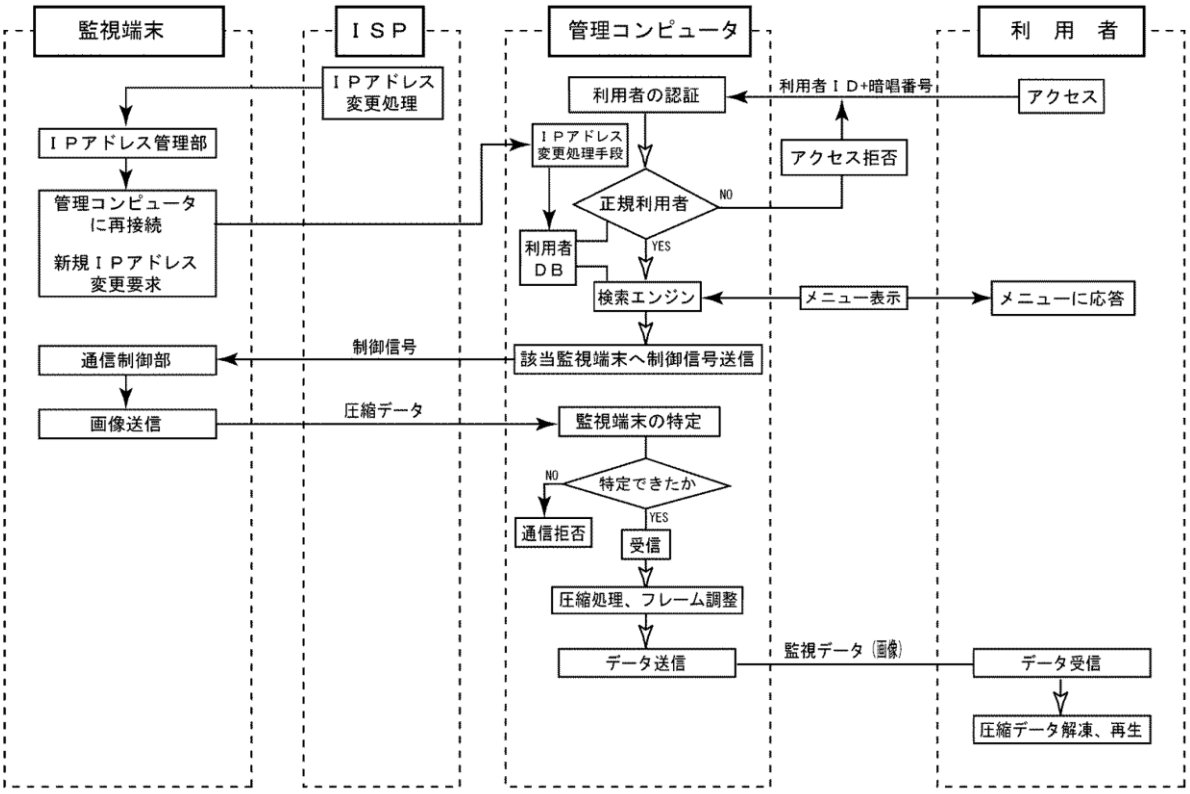
【図４】


2
51
1
53
52
PCM CODEC
MIC
71
56
54
55
70
SRAM
58
59
69
66
MPU
65
67

【図５】

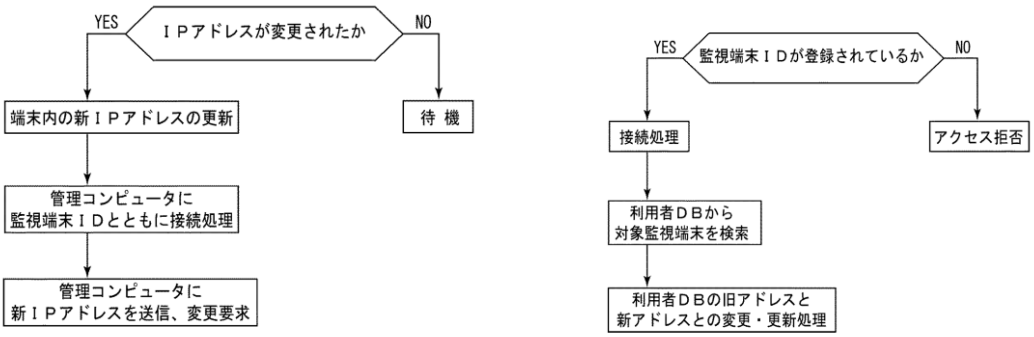

通信回線網へ
通信回線網へ
32
31
38
33
RAM
CPU
通信回線
基板２
通信回線
基板１
データバス
30
3
表示装置
34
記憶装置
利用者ＤＢ
データ転送Ｐ
接続処理Ｐ
通信履歴記録部
35
RTC
37
入力装置
36

【図７】


監視端末
ＩＳＰ
管理コンピュータ
利　用　者
ＩＰアドレス
変更処理
利用者の認証
利用者ＩＤ+暗唱番号
アクセス
ＩＰアドレス管理部
ＩＰアドレス
変更処理手段
アクセス拒否
管理コンピュータ
に再接続
新規ＩＰアドレス
変更要求
正規利用者
NO
YES
利用者
ＤＢ
検索エンジン
メニュー表示
メニューに応答
通信制御部
制御信号
該当監視端末へ制御信号送信
画像送信
圧縮データ
監視端末の特定
NO
特定できたか
YES
通信拒否
受信
圧縮処理、フレーム調整
データ送信
監視データ（画像）
データ受信
圧縮データ解凍、再生

【図９】

【図８】


YES
ＩＰアドレスが変更されたか
NO
端末内の新ＩＰアドレスの更新
待 機
管理コンピュータに
監視端末ＩＤとともに接続処理
管理コンピュータに
新ＩＰアドレスを送信、変更要求
YES
監視端末ＩＤが登録されているか
NO
接続処理
アクセス拒否
利用者ＤＢから
対象監視端末を検索
利用者ＤＢの旧アドレスと
新アドレスとの変更・更新処理

（別紙２）

甲１の記載事項

［１頁４－１８行目］

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

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 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 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 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ＶＰＮ（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。仕事中の親が，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，ＰＯＴＳ（アナログ公衆電話網），ＤＳＬ（デジタル加入者線），ＩＳＤＮ（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３４－３５行目］

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

（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１２行－５頁７行目］

System Overview

Referring to Figure 1, the top-level configuration of a VPN monitoring 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 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., 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, 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 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

ント１２０は，保育所，例えば，センタ１（１３０），センタ２（１３２），センタＮ（１３４）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１１０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１１０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１２０’は，センササーバ１１０とリモートセンサモニタ，例えば，モニタ１４０，１４２，１４４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１３０などとセンササーバ１１０との間のリンク１２０は，公衆交換電話網（ＰＳＴＮ）を横切る暗号化ＶＰＮからなる。ＶＰＮ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１１０と遠隔センサモニタ１４０などとの間のリンク１２０’も暗号化ＶＰＮからなる。システム１００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ＶＰＮであるために，システム１００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。

保育所１３０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る。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，Ｆａｒａｌｌｏｎ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１３０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（ＰＳＴＮ）に対するアクセスポイントを提供する。システム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，ＰＳＴＮ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ＰＳＴＮの他のユーザにはアクセスできないＶＰＮ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１００は，生成されて送信される画像は，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１００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。）

［５頁８－３０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 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 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 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 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.

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 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 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１３０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１１０からモニタ１４０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１１０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１００において，カメラは，センササーバ１１０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１１０は，ユーザがユーザ名，パスワード（８－１２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，１５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１１０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１３０との間の追加のネットワーク容量とリンク１２０を，センタ１３０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１１０に接続を行って，センササーバ１１０は，各カメラに対してただ１つの接続を設定する。）

［６頁１－１１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.

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 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 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ＩＤコード又はスク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って，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。）

［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).

」

（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（ｐａｎｅ：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。）

［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 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。）

［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

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，ｐａｒａｄｙｎｅ社ＨｏｔＷｉｒｅ５４４６型ＤＳＬモデム，型番５４４６－ａ２－２００－０ｒｍ，３Ｃｏｍ社５６ｋ　ＭＬＰＰＰスイッチ，型番３ｃ４３０００，Ｎｅｔｇｅａｒ社ＩＳＤＮモデム，型番ＲＴ３２８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，Ｒａｖｌｉｎ－４有線暗号化装置に，１０ｂａｓｅ－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１０ｂａｓｅ－Ｔ非スイッチングハブに，１０ｂａｓｅ－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，１６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に接続され，これには，互換性のあるブラウザを実行するＭｉｃｒｏｓｏｆｔ社Ｗｉｎ

ｄｏｗｓベースのネットワークコンピュータを含む。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る。一実施形態では，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る。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る。)

[１０頁４－３０行目]

・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 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 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 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,（１０ｂａｓｅ－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，ソフトウエ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，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

たり，または，ＭＣＩ社やＳｐｒｉｎｔ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３３２は，システムの動作を容易にする１つまたは複数のサーバを含むことができる。）

［１１頁２８行－１２頁７行目］

Operational Flow and Server Configuration

Referring to Figures 4, a top-level operational flow process 400 of the 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., 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 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 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.

（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で使用されるサーバ及び，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，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 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 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，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,認証データの入力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］

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 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, 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３５０は，パスワードの変更をユーザに促す。Ｗｅｂサーバ３５０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３６２をチェックすることを，データベースサーバ３６０に対して要求する。状態４２２に進み，図２に示すように，Ｗｅｂサーバ３５０は，３つのフレームを持つＷｅｂページを生成する。フレーム２３０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２１０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２２０は，ユーザが見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ても，カメラとの接続は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 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］

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. 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に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こと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

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に問い合わせて，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。）

［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１２０を介してアクセスできる遠隔地の保育所１３０（図１）に配置される。画像を保存するデータストレージ３６２（図３及び図５）の一例は，デークサーバ３６０上に存在するディスクドライブである。）

［１５頁１９行－１６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 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 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 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 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.

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 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］

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 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７００について説明する。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る。一実施形態では，配信サーバ３４０は，Ｍｉｃｒｏｓｏｆｔ　Ｗｉｎｄｏｗｓ　ＮＴサーバＶｅｒ．４，ＳＰ３を，ＩＩＳ（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７００は，Ｊａｖａ，Ｐｅｒｌ及びＣ＋＋プログラミング言語で記述される。

画像を取得して保管するプロセス６００（図６）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も動作している。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る。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する。）

［２１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 the room where the camera is installed.

（・制限されたアクセスー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。）

［２２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.

（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。）

［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 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。）

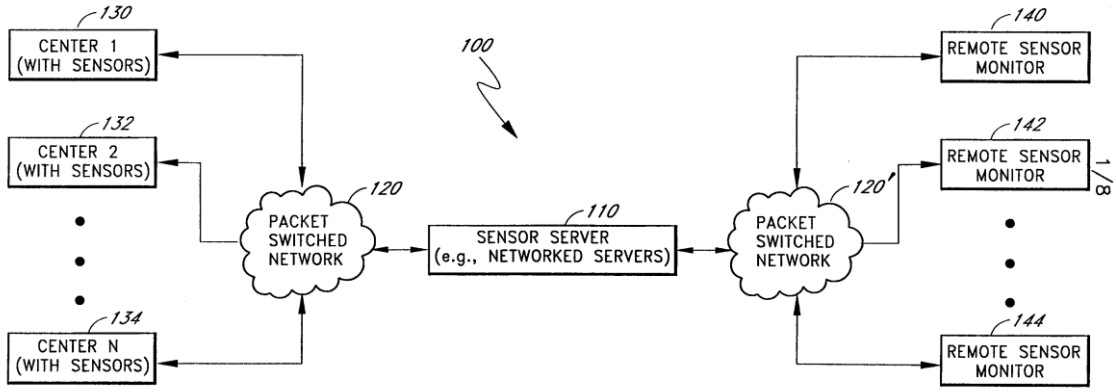

130
CENTER 1
(WITH SENSORS)
132
CENTER 2
(WITH SENSORS)
134
CENTER N
(WITH SENSORS)
100
120
PACKET
SWITCHED
NETWORK
110
SENSOR SERVER
(e.g., NETWORKED SERVERS)
120'
PACKET
SWITCHED
NETWORK
140
REMOTE SENSOR
MONITOR
142
REMOTE SENSOR
MONITOR
144
REMOTE SENSOR
MONITOR
1/8

*FIG. 1*

（訳）

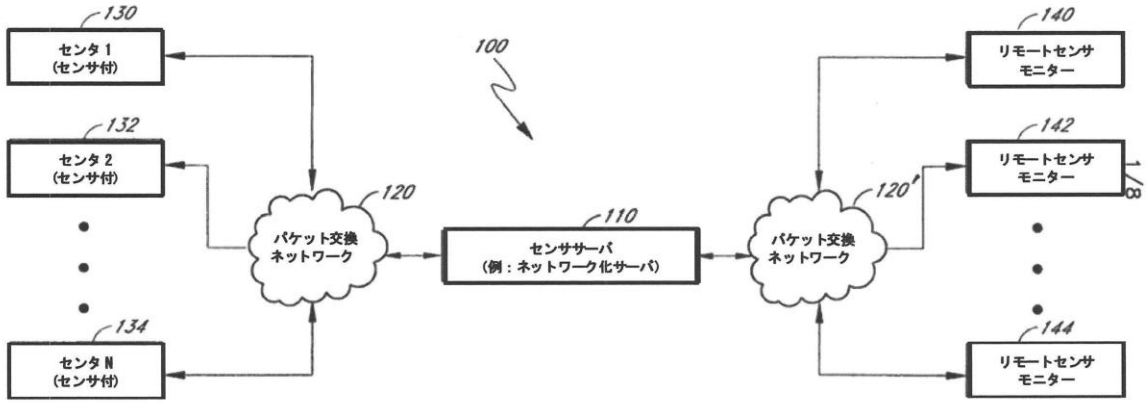

130
センタ 1
(センサ付)
132
センタ 2
(センサ付)
134
センタ N
(センサ付)
100
120
パケット交換
ネットワーク
110
センササーバ
(例：ネットワーク化サーバ)
120'
パケット交換
ネットワーク
140
リモートセンサ
モニター
142
リモートセンサ
モニター
144
リモートセンサ
モニター
1/8

図 1

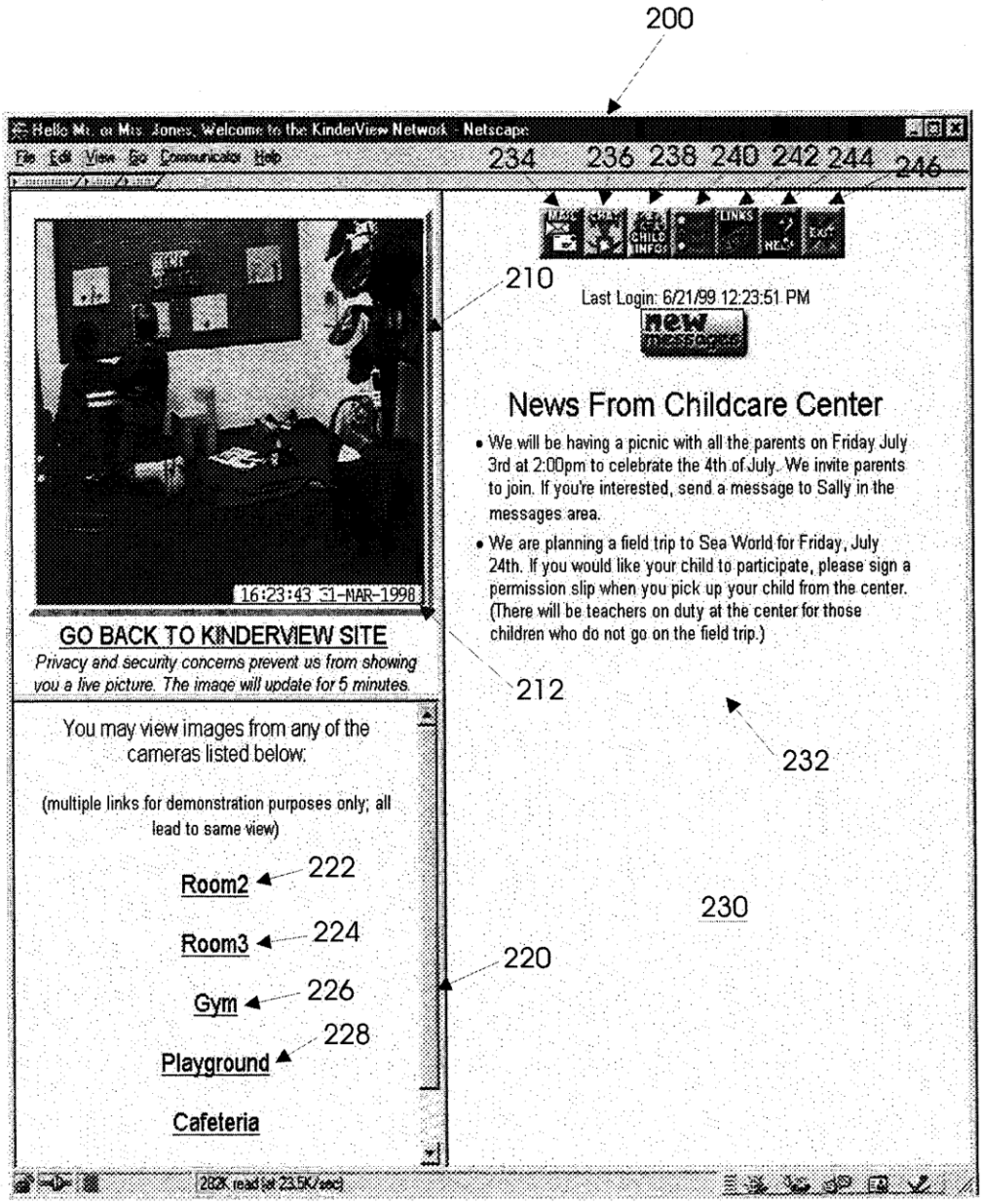

200
Hello Mr. or Mrs. Jones, Welcome to the KinderView Network - Netscape
File Edit View Go Communicator Help
234 236 238 240 242 244 246
LINKS
210
Last Login: 6/21/99 12:23:51 PM
new
News From Childcare Center
• We will be having a picnic with all the parents on Friday July 3rd at 2:00pm to celebrate the 4th of July. We invite parents to join. If you're interested, send a message to Sally in the messages area.
• We are planning a field trip to Sea World for Friday, July 24th. If you would like your child to participate, please sign a permission slip when you pick up your child from the center. (There will be teachers on duty at the center for those children who do not go on the field trip.)
16:23:43 31-MAR-1998
GO BACK TO KINDERVIEW SITE
Privacy and security concerns prevent us from showing you a live picture. The image will update for 5 minutes.
212
232
You may view images from any of the cameras listed below:
(multiple links for demonstration purposes only; all lead to same view)
Room2
222
Room3
224
Gym
226
Playground
228
Cafeteria
230
220
282K read at 23.5K/sec

FIG.2

（訳）

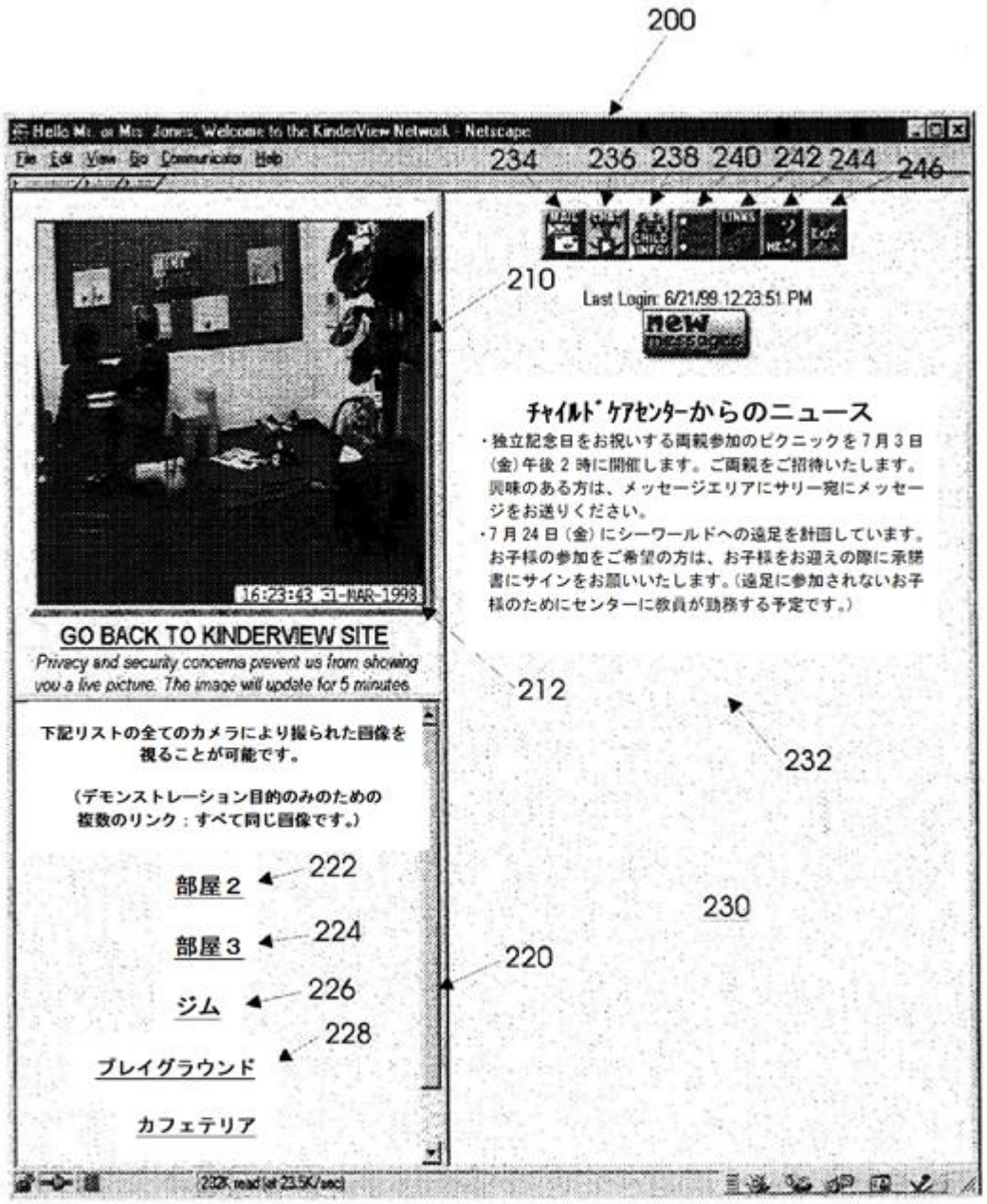

200
Hello Mr. or Mrs. Jones, Welcome to the KinderView Network - Netscape
File Edit View Go Communicator Help
234
236
238
240
242
244
246
210
Last Login: 6/21/99 12:23:51 PM
new messages
チャイルドケアセンターからのニュース
・独立記念日をお祝いする両親参加のピクニックを７月３日（金）午後２時に開催します。ご両親をご招待いたします。興味のある方は、メッセージエリアにサリー宛にメッセージをお送りください。
・７月24日（金）にシーワールドへの遠足を計画しています。お子様の参加をご希望の方は、お子様をお迎えの際に承諾書にサインをお願いいたします。（遠足に参加されないお子様のためにセンターに教員が勤務する予定です。）
16:23:43 31-MAR-1998
GO BACK TO KINDERVIEW SITE
Privacy and security concerns prevent us from showing you a live picture. The image will update for 5 minutes.
212
232
下記リストの全てのカメラにより撮られた画像を視ることが可能です。
（デモンストレーション目的のみのための複数のリンク：すべて同じ画像です。）
部屋２
222
部屋３
224
ジム
226
プレイグラウンド
228
カフェテリア
230
220

図２

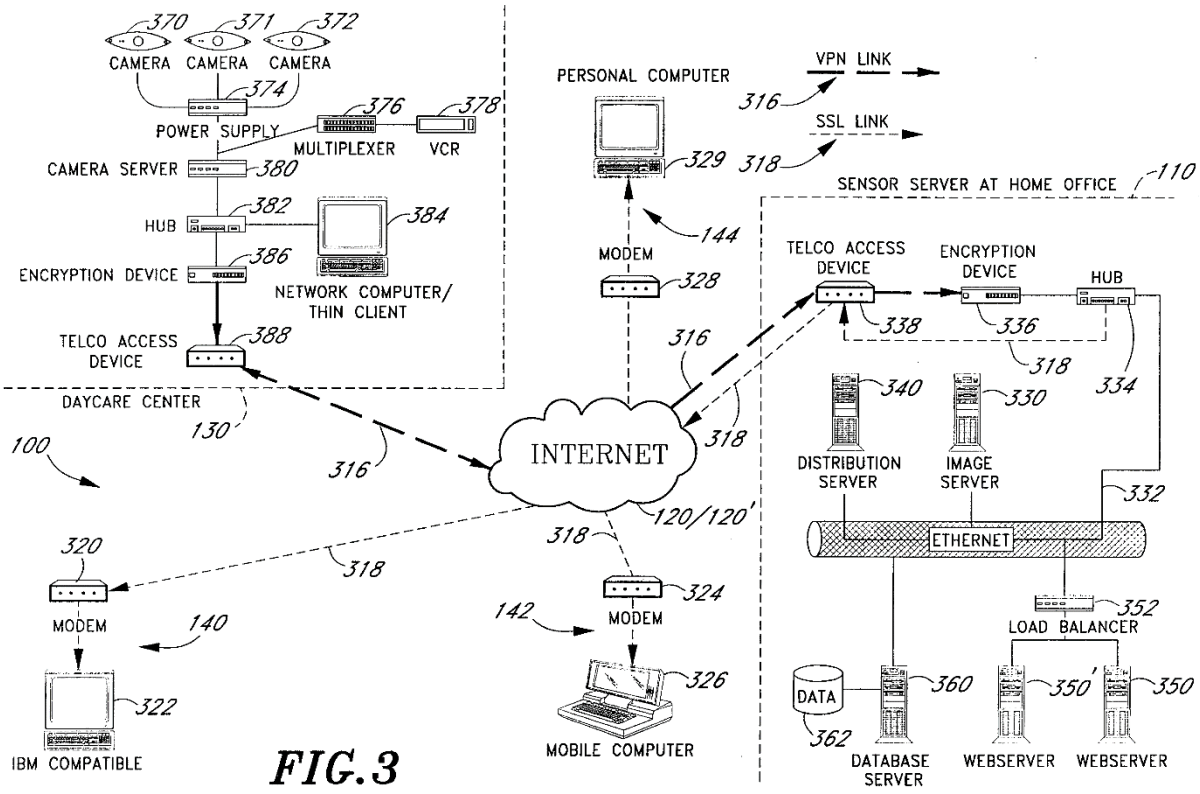

370
371
372
CAMERA
CAMERA
CAMERA
374
POWER SUPPLY
376
MULTIPLEXER
378
VCR
CAMERA SERVER
380
HUB
382
384
ENCRYPTION DEVICE
386
NETWORK COMPUTER/
THIN CLIENT
TELCO ACCESS
DEVICE
388
DAYCARE CENTER
130
100
316
INTERNET
318
120/120'
320
MODEM
140
322
IBM COMPATIBLE
PERSONAL COMPUTER
VPN LINK
316
SSL LINK
318
329
144
MODEM
328
316
318
324
MODEM
142
326
MOBILE COMPUTER
SENSOR SERVER AT HOME OFFICE
110
TELCO ACCESS
DEVICE
ENCRYPTION
DEVICE
HUB
338
336
318
334
340
330
DISTRIBUTION
SERVER
IMAGE
SERVER
332
ETHERNET
352
LOAD BALANCER
DATA
360
350'
350
362
DATABASE
SERVER
WEBSERVER
WEBSERVER

FIG.3

（訳）

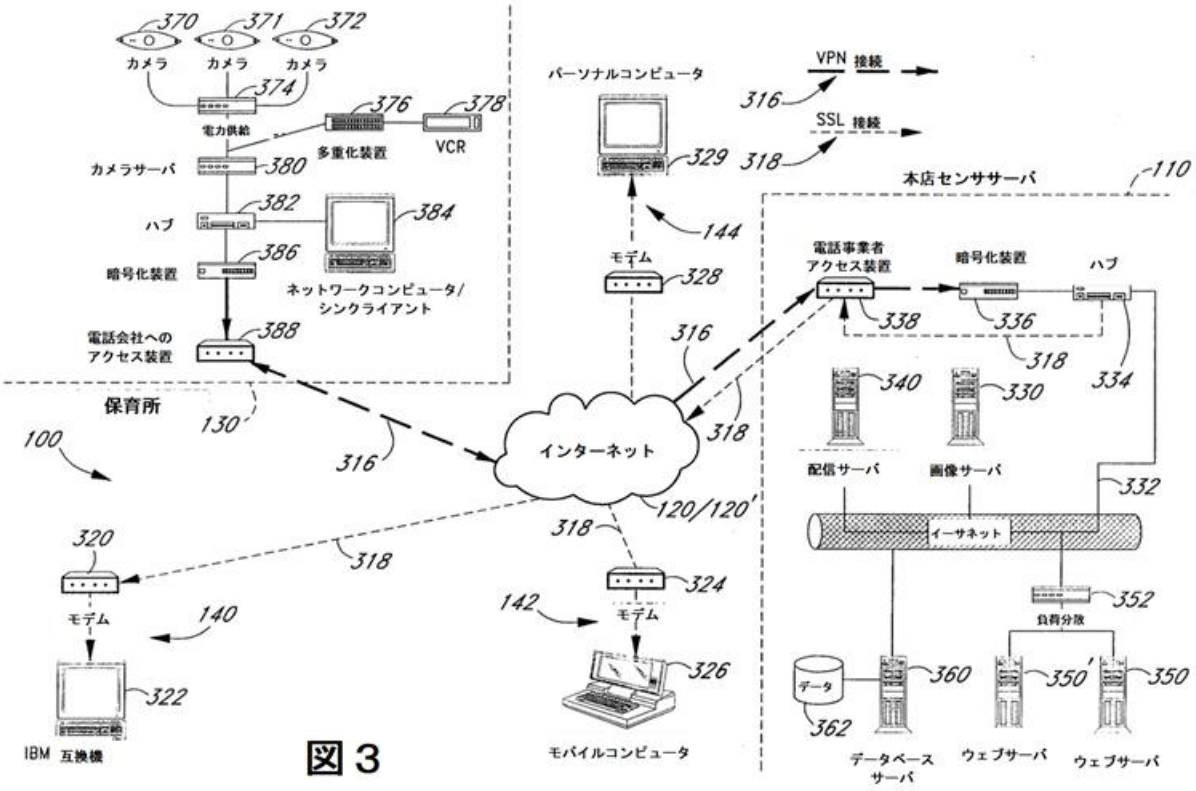

370
371
372
カメラ
カメラ
カメラ
374
電力供給
376
378
多重化装置
VCR
カメラサーバ
380
ハブ
382
384
暗号化装置
386
ネットワークコンピュータ/
シンクライアント
電話会社への
アクセス装置
388
保育所
130
100
316
インターネット
318
120/120'
パーソナルコンピュータ
VPN 接続
316
SSL 接続
318
329
本店センササーバ
110
144
モデム
328
電話事業者
アクセス装置
暗号化装置
ハブ
338
336
318
334
316
340
330
配信サーバ
画像サーバ
332
イーサネット
352
負荷分散
320
モデム
140
322
IBM 互換機
318
324
142
モデム
326
モバイルコンピュータ
データ
360
362
350'
350
データベース
サーバ
ウェブサーバ
ウェブサーバ

図 3

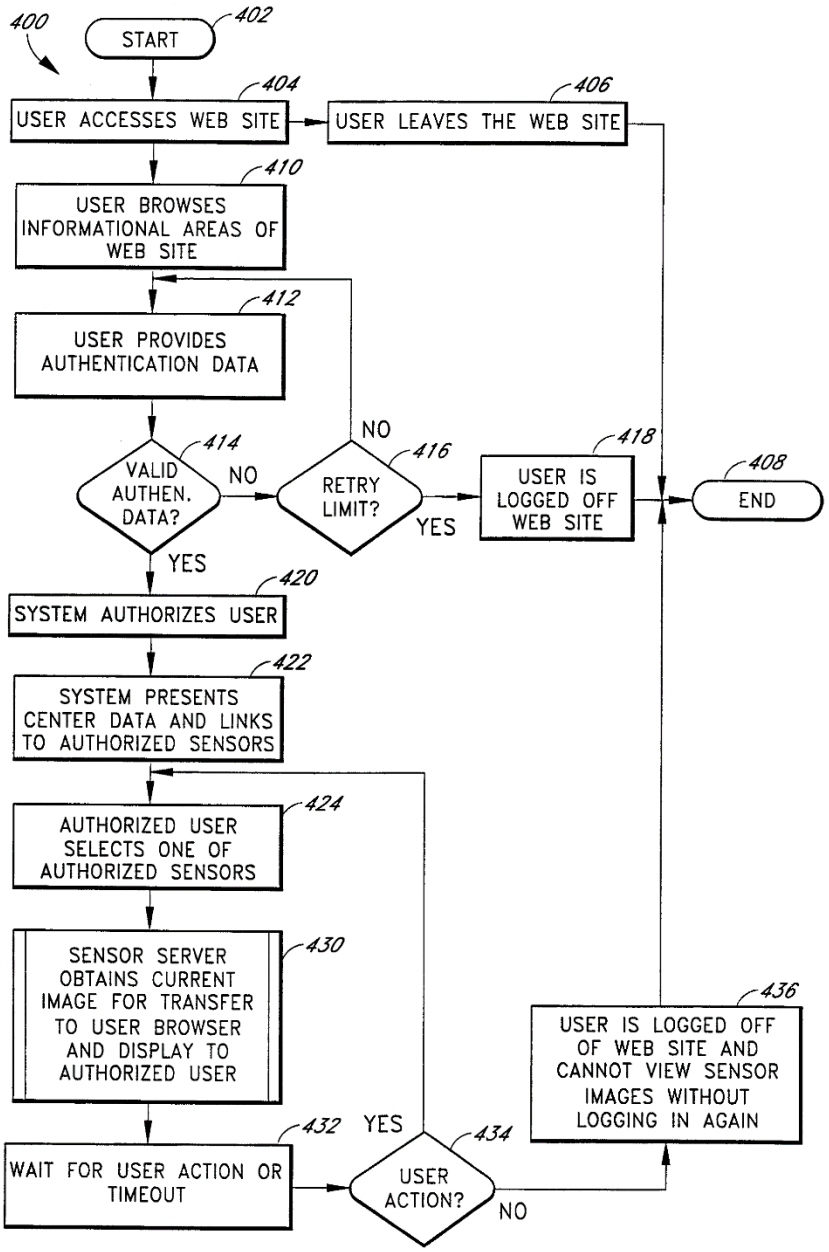

400
START
402
USER ACCESSES WEB SITE
404
USER LEAVES THE WEB SITE
406
USER BROWSES INFORMATIONAL AREAS OF WEB SITE
410
USER PROVIDES AUTHENTICATION DATA
412
VALID AUTHEN. DATA?
414
NO
RETRY LIMIT?
416
NO
YES
USER IS LOGGED OFF WEB SITE
418
END
408
YES
SYSTEM AUTHORIZES USER
420
SYSTEM PRESENTS CENTER DATA AND LINKS TO AUTHORIZED SENSORS
422
AUTHORIZED USER SELECTS ONE OF AUTHORIZED SENSORS
424
SENSOR SERVER OBTAINS CURRENT IMAGE FOR TRANSFER TO USER BROWSER AND DISPLAY TO AUTHORIZED USER
430
USER IS LOGGED OFF OF WEB SITE AND CANNOT VIEW SENSOR IMAGES WITHOUT LOGGING IN AGAIN
436
WAIT FOR USER ACTION OR TIMEOUT
432
YES
USER ACTION?
434
NO

*FIG. 4*

（訳）

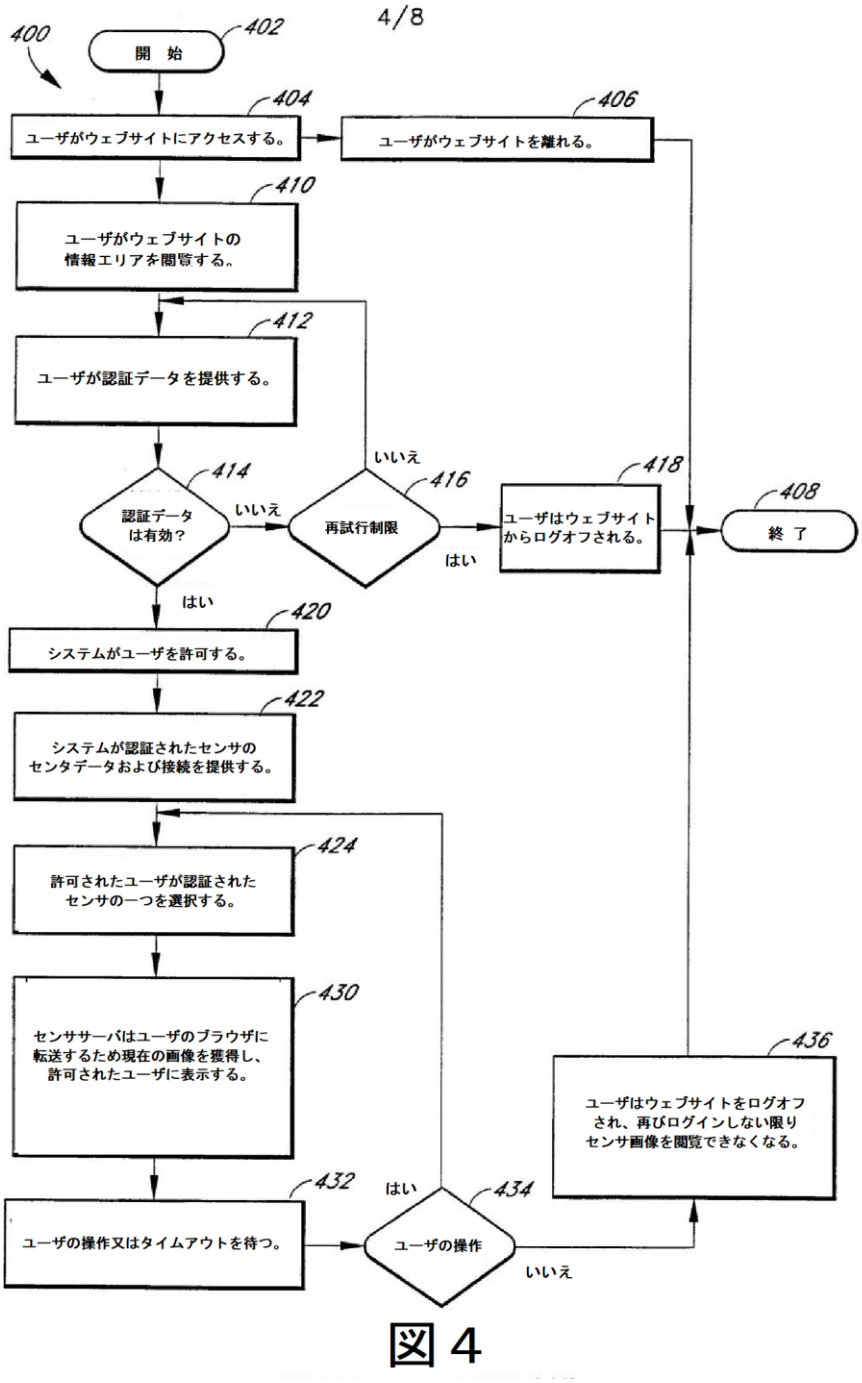
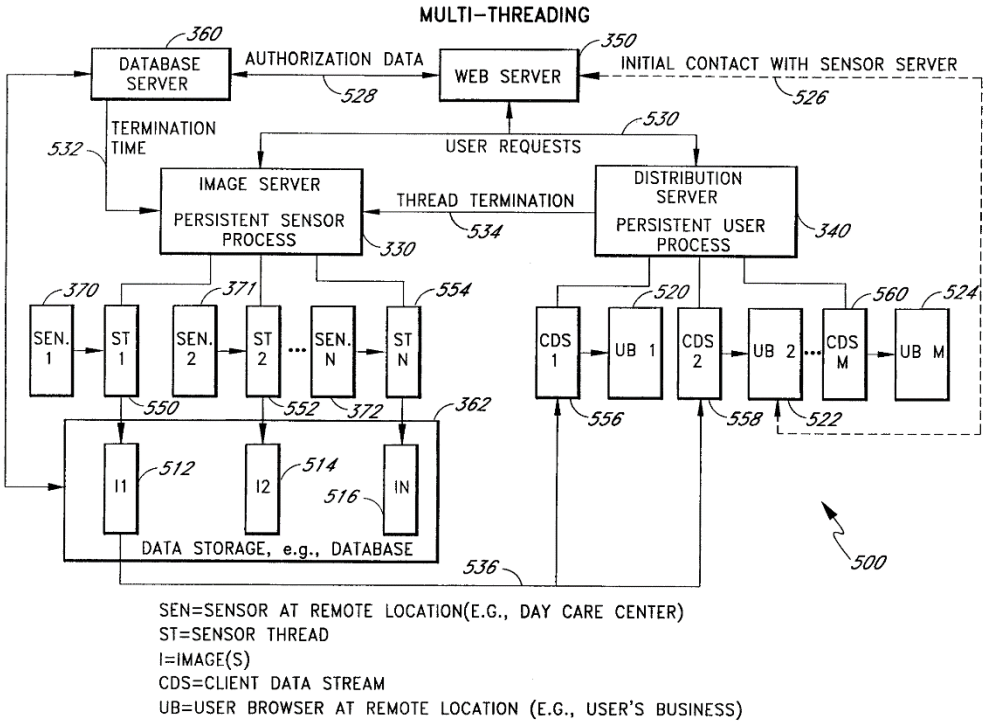

4/8
400
開 始
402
ユーザがウェブサイトにアクセスする。
404
ユーザがウェブサイトを離れる。
406
ユーザがウェブサイトの
情報エリアを閲覧する。
410
ユーザが認証データを提供する。
412
認証データ
は有効？
414
いいえ
再試行制限
416
いいえ
はい
ユーザはウェブサイト
からログオフされる。
418
終 了
408
はい
システムがユーザを許可する。
420
システムが認証されたセンサの
センタデータおよび接続を提供する。
422
許可されたユーザが認証された
センサの一つを選択する。
424
センササーバはユーザのブラウザに
転送するため現在の画像を獲得し、
許可されたユーザに表示する。
430
ユーザはウェブサイトをログオフ
され、再びログインしない限り
センサ画像を閲覧できなくなる。
436
ユーザの操作又はタイムアウトを待つ。
432
ユーザの操作
434
はい
いいえ

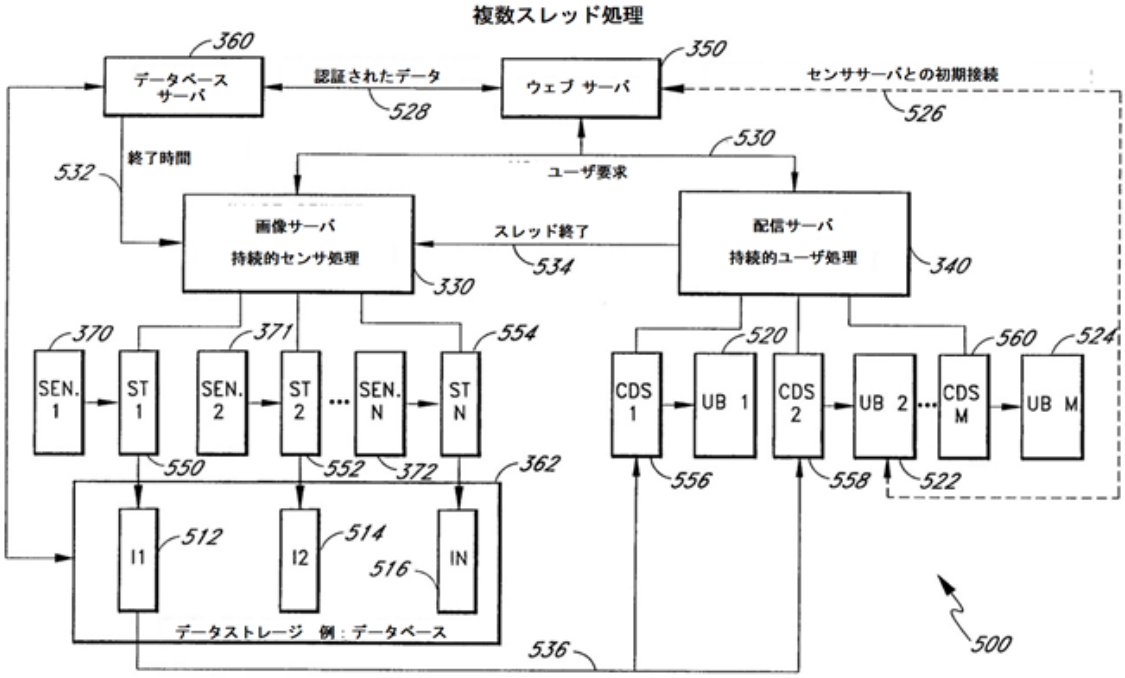
図４




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）




SEN = 遠隔地に設置されたセンサ（例：保育所）
ST = センサスレッド
I = 画像
CDS = 顧客データストリーム
UB = 遠隔地にあるユーザのブラウザ（例：ユーザの管理）

図５

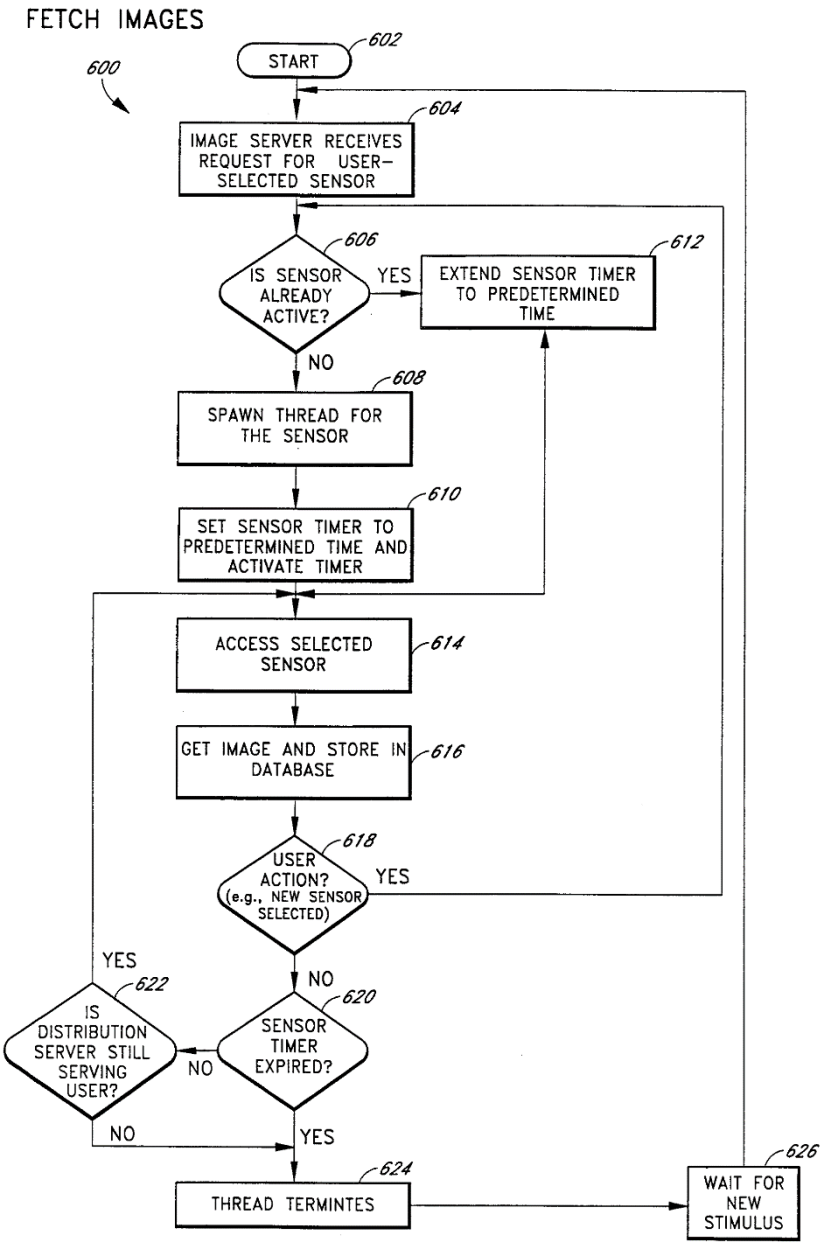

FETCH IMAGES
600
START
602
IMAGE SERVER RECEIVES REQUEST FOR USER-SELECTED SENSOR
604
IS SENSOR ALREADY ACTIVE?
606
YES
EXTEND SENSOR TIMER TO PREDETERMINED TIME
612
NO
SPAWN THREAD FOR THE SENSOR
608
SET SENSOR TIMER TO PREDETERMINED TIME AND ACTIVATE TIMER
610
ACCESS SELECTED SENSOR
614
GET IMAGE AND STORE IN DATABASE
616
USER ACTION? (e.g., NEW SENSOR SELECTED)
618
YES
NO
SENSOR TIMER EXPIRED?
620
NO
IS DISTRIBUTION SERVER STILL SERVING USER?
622
YES
NO
YES
THREAD TERMINTES
624
WAIT FOR NEW STIMULUS
626

*FIG. 6*

（訳）

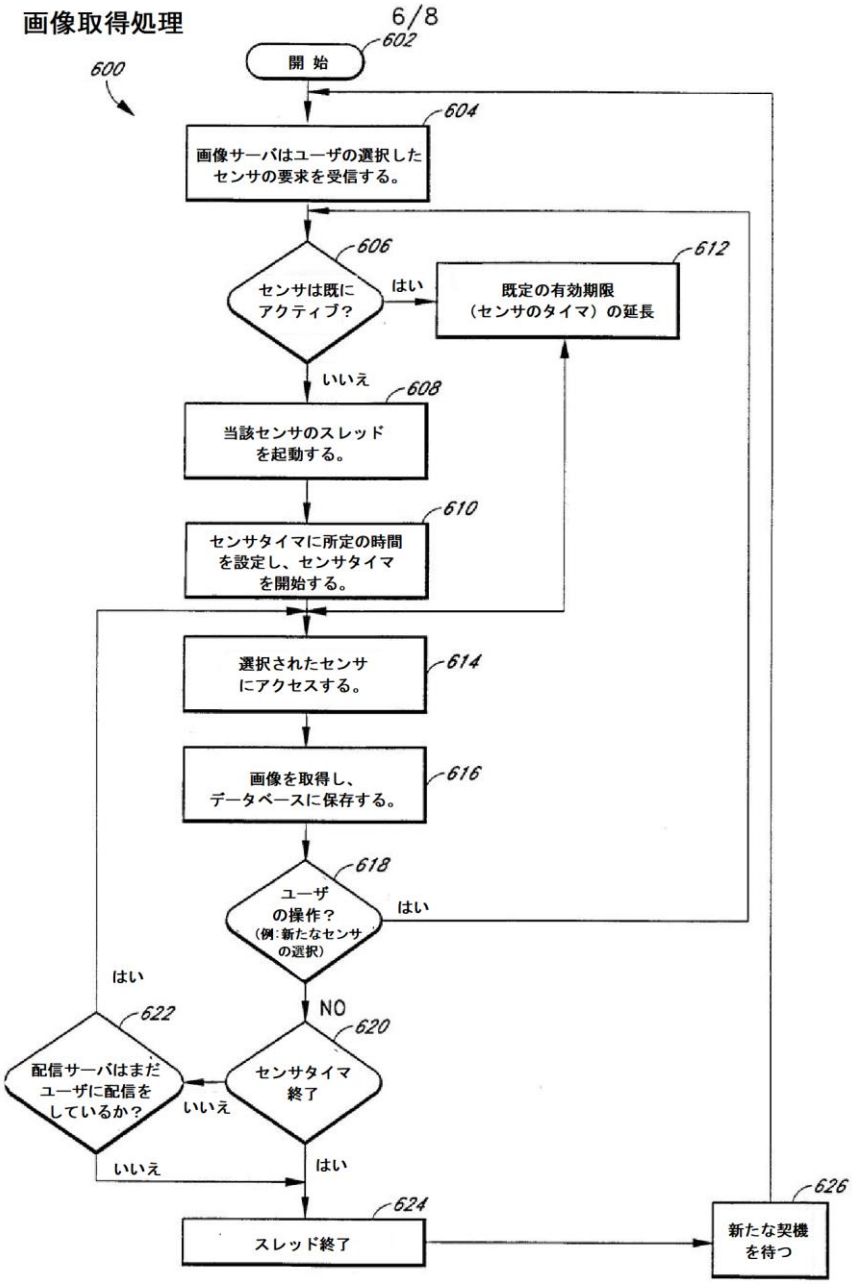

画像取得処理
6/8
600
602
開 始
604
画像サーバはユーザの選択した
センサの要求を受信する。
606
センサは既に
アクティブ?
はい
612
既定の有効期限
（センサのタイマ）の延長
いいえ
608
当該センサのスレッド
を起動する。
610
センサタイマに所定の時間
を設定し、センサタイマ
を開始する。
614
選択されたセンサ
にアクセスする。
616
画像を取得し、
データベースに保存する。
618
ユーザ
の操作?
（例:新たなセンサ
の選択）
はい
はい
NO
622
620
配信サーバはまだ
ユーザに配信を
しているか?
センサタイマ
終了
いいえ
いいえ
はい
624
626
スレッド終了
新たな契機
を待つ

図６

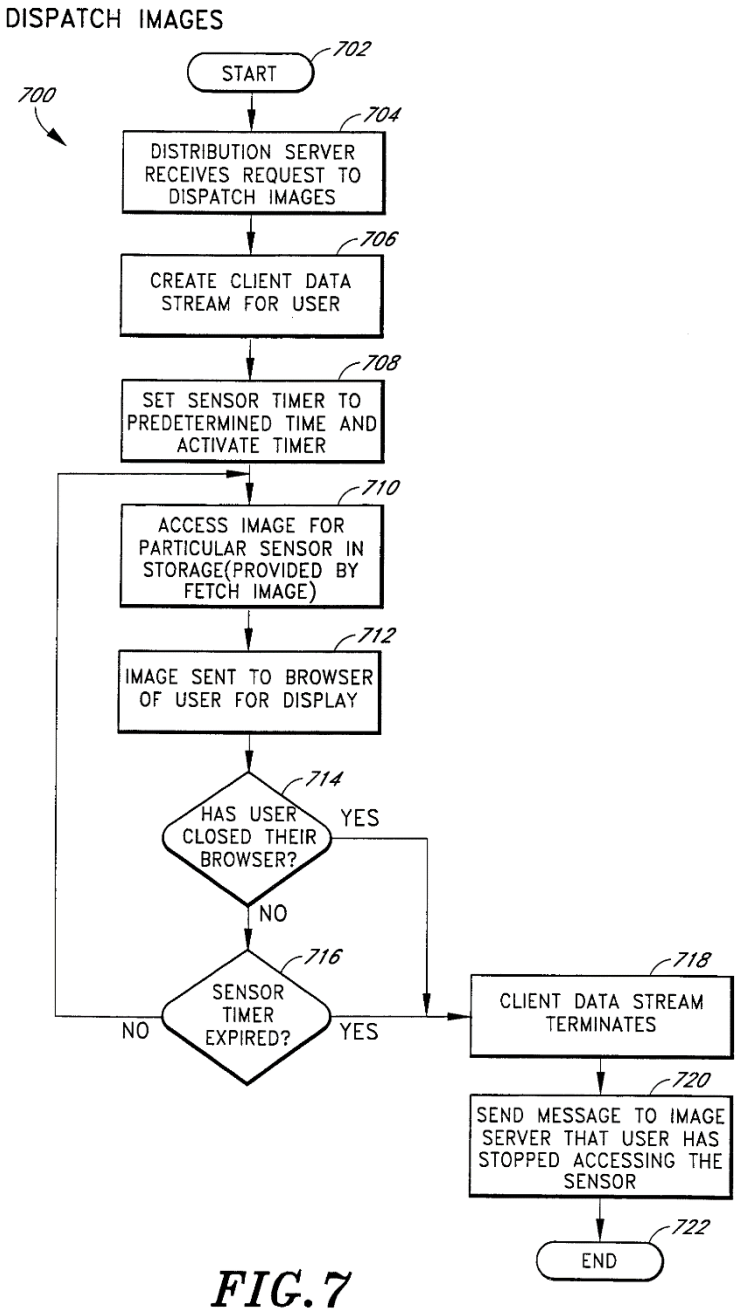

DISPATCH IMAGES
700
START
702
DISTRIBUTION SERVER RECEIVES REQUEST TO DISPATCH IMAGES
704
CREATE CLIENT DATA STREAM FOR USER
706
SET SENSOR TIMER TO PREDETERMINED TIME AND ACTIVATE TIMER
708
ACCESS IMAGE FOR PARTICULAR SENSOR IN STORAGE(PROVIDED BY FETCH IMAGE)
710
IMAGE SENT TO BROWSER OF USER FOR DISPLAY
712
HAS USER CLOSED THEIR BROWSER?
714
YES
NO
SENSOR TIMER EXPIRED?
716
NO
YES
CLIENT DATA STREAM TERMINATES
718
SEND MESSAGE TO IMAGE SERVER THAT USER HAS STOPPED ACCESSING THE SENSOR
720
END
722

*FIG. 7*

（訳）

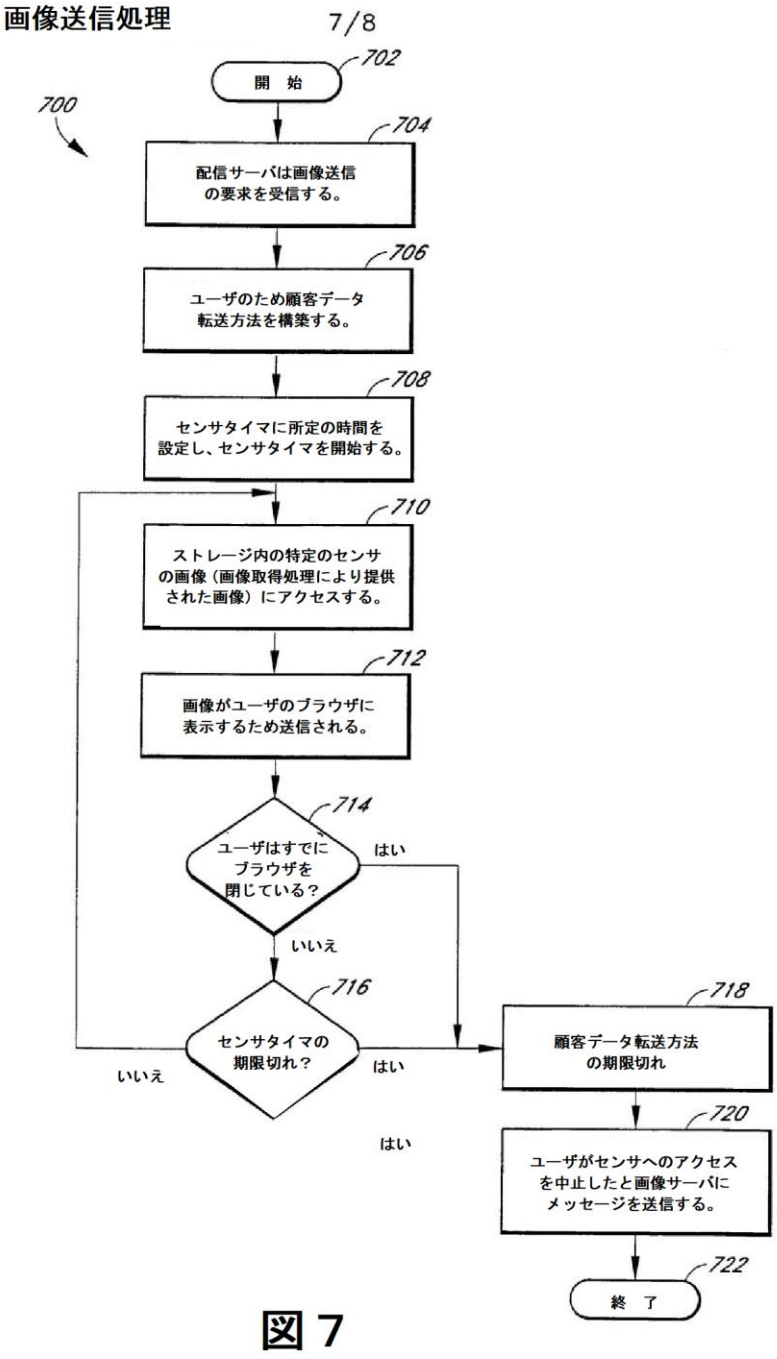

画像送信処理
7/8
700
開　始
702
配信サーバは画像送信の要求を受信する。
704
ユーザのため顧客データ転送方法を構築する。
706
センサタイマに所定の時間を設定し、センサタイマを開始する。
708
ストレージ内の特定のセンサの画像（画像取得処理により提供された画像）にアクセスする。
710
画像がユーザのブラウザに表示するため送信される。
712
ユーザはすでにブラウザを閉じている？
714
はい
いいえ
センサタイマの期限切れ？
716
いいえ
はい
顧客データ転送方法の期限切れ
718
はい
ユーザがセンサへのアクセスを中止したと画像サーバにメッセージを送信する。
720
終　了
722

図 7

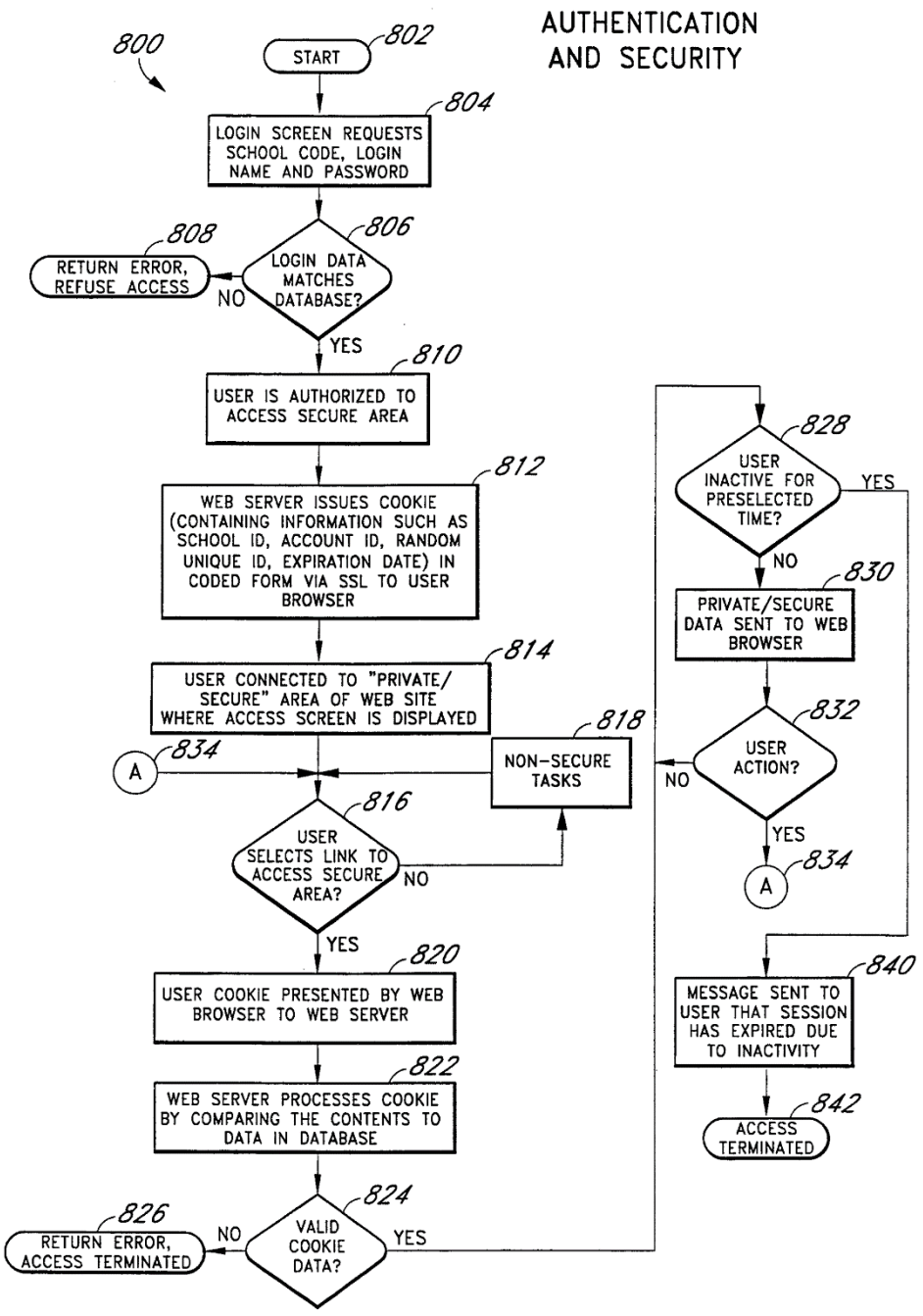

AUTHENTICATION AND SECURITY
800
START
802
LOGIN SCREEN REQUESTS SCHOOL CODE, LOGIN NAME AND PASSWORD
804
LOGIN DATA MATCHES DATABASE?
806
NO
RETURN ERROR, REFUSE ACCESS
808
YES
USER IS AUTHORIZED TO ACCESS SECURE AREA
810
WEB SERVER ISSUES COOKIE (CONTAINING INFORMATION SUCH AS SCHOOL ID, ACCOUNT ID, RANDOM UNIQUE ID, EXPIRATION DATE) IN CODED FORM VIA SSL TO USER BROWSER
812
USER CONNECTED TO "PRIVATE/ SECURE" AREA OF WEB SITE WHERE ACCESS SCREEN IS DISPLAYED
814
A
834
NON-SECURE TASKS
818
USER SELECTS LINK TO ACCESS SECURE AREA?
816
NO
YES
USER COOKIE PRESENTED BY WEB BROWSER TO WEB SERVER
820
WEB SERVER PROCESSES COOKIE BY COMPARING THE CONTENTS TO DATA IN DATABASE
822
VALID COOKIE DATA?
824
NO
RETURN ERROR, ACCESS TERMINATED
826
YES
USER INACTIVE FOR PRESELECTED TIME?
828
YES
NO
PRIVATE/SECURE DATA SENT TO WEB BROWSER
830
USER ACTION?
832
NO
YES
A
834
MESSAGE SENT TO USER THAT SESSION HAS EXPIRED DUE TO INACTIVITY
840
ACCESS TERMINATED
842

*FIG.8*

（訳）

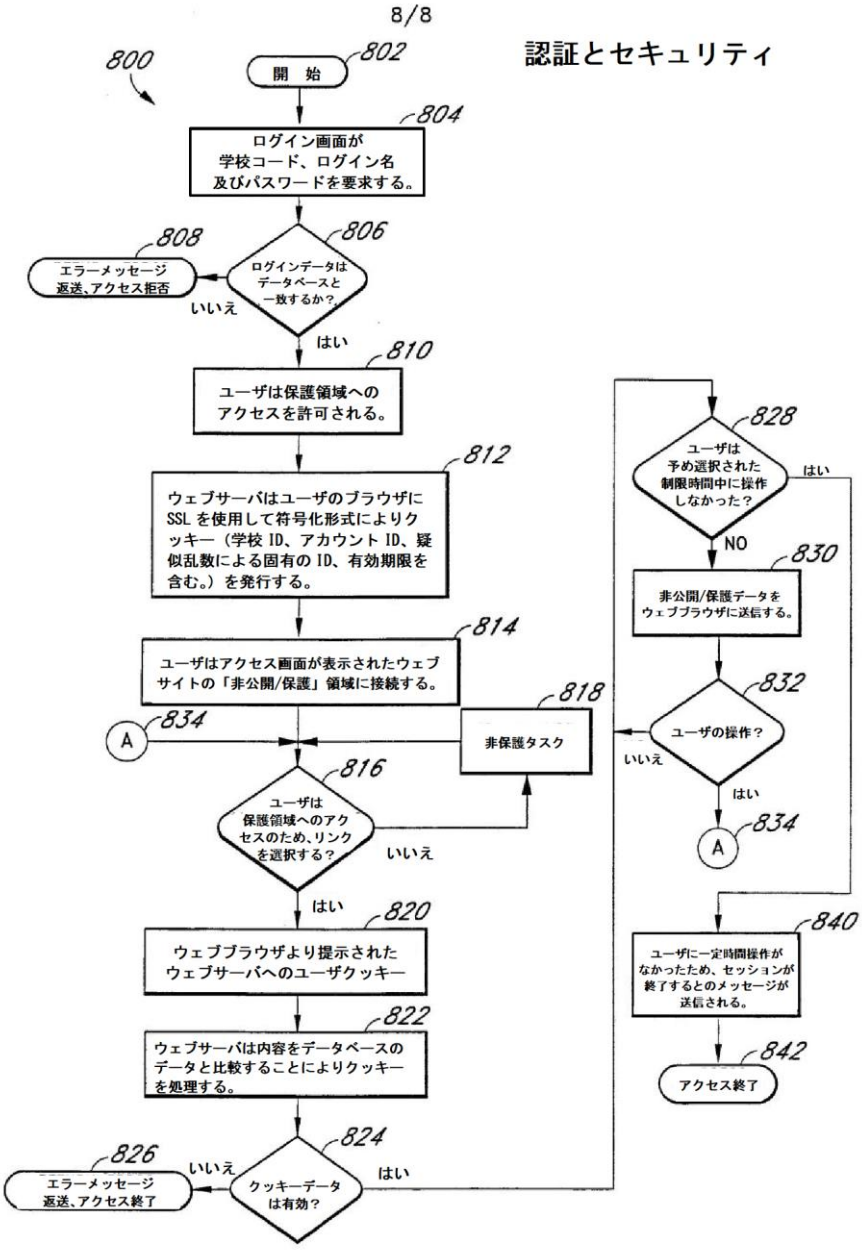

8/8
認証とセキュリティ
800
開　始
802
ログイン画面が
学校コード、ログイン名
及びパスワードを要求する。
804
ログインデータは
データベースと
一致するか？
806
エラーメッセージ
返送、アクセス拒否
808
いいえ
はい
ユーザは保護領域への
アクセスを許可される。
810
ウェブサーバはユーザのブラウザに
SSL を使用して符号化形式によりク
ッキー（学校 ID、アカウント ID、疑
似乱数による固有の ID、有効期限を
含む。）を発行する。
812
ユーザはアクセス画面が表示されたウェブ
サイトの「非公開/保護」領域に接続する。
814
A
834
非保護タスク
818
ユーザは
保護領域へのアク
セスのため、リンク
を選択する？
816
いいえ
はい
ウェブブラウザより提示された
ウェブサーバへのユーザクッキー
820
ウェブサーバは内容をデータベースの
データと比較することによりクッキー
を処理する。
822
クッキーデータ
は有効？
824
エラーメッセージ
返送、アクセス終了
826
いいえ
はい
ユーザは
予め選択された
制限時間中に操作
しなかった？
828
はい
NO
非公開/保護データを
ウェブブラウザに送信する。
830
ユーザの操作？
832
いいえ
はい
A
834
ユーザに一定時間操作が
なかったため、セッションが
終了するとのメッセージが
送信される。
840
アクセス終了
842

図 8