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

特許第4139623号
(P4139623)

(45)発行日　平成20年8月27日(2008.8.27)　(24)登録日　平成20年6月13日(2008.6.13)

(51)Int.Cl.		F I		
G08B 25/08	(2006.01)	G08B	25/08	E
G08B 25/00	(2006.01)	G08B	25/00	510M
G08B 25/04	(2006.01)	G08B	25/04	H
H04M 11/00	(2006.01)	H04M	11/00	301
H04Q 9/00	(2006.01)	H04Q	9/00	301D

請求項の数 2　(全 9 頁)　最終頁に続く

(21)出願番号　特願2002-137917(P2002-137917)
(22)出願日　平成14年5月14日(2002.5.14)
(65)公開番号　特開2003-331373(P2003-331373A)
(43)公開日　平成15年11月21日(2003.11.21)
審査請求日　平成17年1月24日(2005.1.24)

(73)特許権者　000005108
株式会社日立製作所
東京都千代田区丸の内一丁目６番６号
(74)代理人　110000350
ポレール特許業務法人
(72)発明者　長屋　茂喜
東京都国分寺市東恋ケ窪一丁目２８０番地
株式会社日立製作所中央研究所内
(72)発明者　影山　昌広
東京都国分寺市東恋ケ窪一丁目２８０番地
株式会社日立製作所中央研究所内
(72)発明者　宮武　孝文
東京都国分寺市東恋ケ窪一丁目２８０番地
株式会社日立製作所中央研究所内

最終頁に続く

(54)【発明の名称】警備システム

(57)【特許請求の範囲】
【請求項１】
監視領域の異常を検出するセンサと撮像手段に接続される伝送装置と、該伝送装置と通信網を介して接続される第１のサーバと、該第１のサーバと通信網を介して接続される第２のサーバとからなる監視システムであって、
上記伝送装置は、上記センサからの入力信号に上記撮像手段から入力された映像・音声データを対応付けるタイムコードを追加して、センサ毎の伝送パケットからなるセンサ情報を生成するインデクシング手段を有し、
上記第１のサーバは、上記伝送装置からの上記撮像手段で撮像された映像情報と上記インデクシング手段からのセンサ情報を蓄積する第１の記憶手段と、該撮像手段を制御する制御手段と、上記伝送装置から受信した上記センサ情報のうち、同一伝送装置から伝送され、かつ、一定時間内に生成された互いに異なる複数のセンサ情報から間引いて得た１つのセンサ情報を上記第２のサーバへ送信する送信手段とを有し、
上記第２のサーバは、上記第１のサーバからの上記センサ情報を蓄積する第２の記憶手段を有することを特徴とする警備システム。
【請求項２】
上記第２のサーバは上記第１のサーバからの各上記センサ情報について、処理の担当を割り当てる手段を有することを特徴とする請求項１記載の警備システム。
【発明の詳細な説明】
【０００１】

【発明の属する技術分野】
本発明は，インターネットを応用したホームセキュリティの新しいサービス形態に関わり、監視映像や防犯センサなどの信号を伝送・蓄積する制御方式に関る。
【０００２】
【従来の技術】
従来の警備業事業者は、顧客である事業所や一般家庭などの現地サイトを効率よく管理するため、機械警備と呼ばれる電話回線による遠隔システムを構築している。機械警備システムでは、現地サイトに防犯/防災センサを設置し、多数のオペレータが常駐する基地局（あるいはコールセンタ）と呼ばれる集中設備との間を、電話回線で接続して、各サイトに異常がないかを遠隔監視している。サイトから異常を示す信号が基地局に送られると、基地局内のオペレータが現地サイト（顧客）に連絡・状況を確認する。連絡がつかない等の必要が発生した場合、緊急発信基地（デポ）と呼ばれる、現地サイトに近く警備員が詰める設備に連絡を行い、警備員を現地サイトに派遣する。現地サイトに急行した警備員はサイトの状況を確認し、基地局に報告する。基地局は、必要に応じて警察署や消防署、ガス会社など関係各署に連絡を行う。遠隔システムの構築に用いられる電話回線は、常時接続のパケット通信網となっており、サイトから異常を示す信号はパケットデータとして基地局に送られる。回線障害による警備不備を防ぐため、定期的に基地局から現地サイトに確認パケットを送る機構を備えている。回線障害発生時には別途PHSなどで電話するなどして、基地局に障害を通知するサービスを備えたものもある。
一方、どうしても映像を記録する必要があるサイトでは記録装置を現地に設置し、事後的な犯罪抑止手段としてきた。例えば、銀行や消費者金融などの金融機関では証拠保持の必要性から、映像を録画する装置（VTRやハードディクスレコーダ）を現地に設置し、常時録画を行っている。
【０００３】
【発明が解決しようとする課題】
上記一般的な機械警備システムは、防犯/防災センサの信号を送るのみでその他の情報（例えば映像・音声など）を伝送しないため、発報があった場合現地サイトで起こっている状況を基地局が詳しく把握することが難しい。オペレータは、信号がセンサの誤動作などによっておきた誤報であるのか、事件・事故が本当に起こっているのか等を判断できず、とりあえず警備員を派遣せざるをえない。このため、出動が重なることを想定してデポに警備員を多めに配備することが必要で余分にコストにかかっている。一部の先進的なシステムでは、異常発生時に現地サイトに設置したカメラからコマ取り映像をISDNなどの別の広帯域回線を通じて基地局に伝送し、基地局が現地サイトの状況をより詳細に把握できるものもあるが、今度は基地局側へのデータ流入帯域が大量に必要となる（基地局の回線がボトルネックになる）など別の面の設備投資が要求されるためにサービス料金が極めて高く、普及は進んでいない。又、どうしても映像を記録する必要があるサイトでは記録装置を現地に設置する形態は伝送を伴わないため、安価にすむが、金融機関への放火など現地サイトが破壊されるような状況では、記録したデータが遺失してしまうという弱点もある。
以上のように従来の技術では、▲１▼伝送すべき情報の種別について配慮がされておらず、冗長な警備員配備が必要、▲２▼蓄積記録を行う装置が設置されるべき場所について配慮がされておらず記録データの遺失する、▲３▼通信帯域の最適化ついて配慮がされておらず基地局側の帯域が不足する、等の問題があった。
本発明の目的は、基地局への通信帯域増加を防ぎながら、現地サイトの映像音声情報を定期的に外部に蓄積し、基地局のオペレータが必要な際に現地サイトの情報セキュリティを破ることなく取得できるシステムを構築することにある。
また、本発明の別の目的は、上記の新たなシステムを用いて、機械警備事業にかかるコストを低減して利益率を高く維持しつつ、顧客へ安価にサービスを提供することにある。
【０００４】
【課題を解決するための手段】

上記の課題を解決するために、警備対象となる施設を遠隔で管理する機械警備システムであって、警備施設内に施設の状況を検知する手段とセンサ信号と映像情報を含む状況情報をIPデータとして伝送する手段とを有し、
警備施設をインターネットに接続する業者施設内に、上記手段より伝送された状況情報を蓄積する手段と、前記情報を警備業者の基地局に転送する手段とを有するサーバを有し、警備施設を遠隔管理する基地局において、上記手段より伝送されたセンサ信号を基地局内のオペレータに割り当てる手段を有する管理サーバを有し、これらの三つの手段が階層構造を構成することを特徴とする遠隔警備システム。

【０００５】

【発明の実施の形態】

以下、本発明の実施例を説明する。
図１は本発明を用いた機械警備システムとセキュリティサービスの一例である。
１００は監視対象となる現地サイトである。具体的には事務所や店舗、個人宅などが当てはまる。現地サイト１００内には、煙探知機や侵入検知器などのセンサ１０１や監視カメラ１０２、監視マイク１０３などが設置されており、異常発生時（センサ動作時）にはIP伝送装置からファイヤウォール１０５を通じて、警備業者へセンサ情報を送る。
現地サイト１００からのセンサ信号・映像音声情報は、インターネットへの接続サービスを提供する接続業者（ISP:Internet Service Provider）施設２００内のアクセスゲートウェイ２０２を通じて、蓄積サーバ２０１に記録される。現地サイト１００と接続業者施設２００は、ADSL（非対称DSL）やFTTH（Fiber To The Home:光ファイバ）などの広帯域の接続回線５００で接続される。蓄積サーバ２０１は、帯域の小さいイベント情報を相互接続網であるインターネット４００経由で警備業者基地局３００に転送する。
警備業者基地局３００に集まったセンサ信号は、ファイヤウォール３０２を通して基地局内の管理サーバ３０１に伝送される。管理サーバ３０１は基地局内の手の空いたオペレータにこれを伝送する。オペレータは従来の機械警備と同様に現地サイト１００に連絡をおこなったり、デポに現地サイト１００への出動を要請するなど警備業務を行う。この際、オペレータはセンサ信号が誤報でないかを現地サイト１００に電話し確認する。現地サイト１００が夜間の無人状態になっているなど連絡が取れない状況である場合には、インターネット接続業者施設２００内の蓄積サーバ２０１にアクセスし、発報センサ信号の履歴や直前に記録された映像・音声をインターネット経由で再生し、確認をとる。これにより警備員を無駄に現地へ動向させる機会を大幅に低減し、より効率的に配備をおこなうことが可能となる。
図2は、現地サイト１００に設置されているIP伝送装置１０４について詳しく説明するものである。
IP伝送装置１０４での動作例の一つは蓄積サーバ２０１の記録トリガとして動作するケースである。防犯／防災センサ101が異常を検知し、センサ・メディア入力インターフェイス１０４６にトリガ信号が入力されると、これをトリガにセンサ信号伝送制御部１０４３がセンサ・メディア入力インターフェイス１０４６を介してカメラ１０２やマイク１０３からキャプチャを開始し、これをISP施設２００内の蓄積サーバ２０１に伝送、センサ情報が解除されるまで記録を続けるというものである。これは、現地サイト１００とISP施設２００との間の接続回線５００の帯域が狭かったり、アクセスGW２０２の帯域が貧弱な場合に適した運用形態であるいえる。
IP伝送装置１０４の別の動作例は、カメラ１０２やマイク１０３から入力されたデータを蓄積サーバ２００に常時記録するケースで、通常時は比較的低いビットレート（あるいはフレーム間引き記録）で記録を行い、センサ・メディア入力インターフェイス１０４６にトリガ信号が入力されると、ビットレートを高くする（あるいはフルフレームで記録）というやり方である。
インデクシング１０４７は、センサ１０１からのセンサ信号と同時に入力された映像・音声を関連付けする。具体的にはセンサ入力を基に生成されたセンサ信号パケットに、映像・音声データのタイムコード（入力メディアＩＤ＋時刻）を追加する。これにより、蓄積

サーバ２０１はこのタイムコードから直接フレームデータを取り出すことができ、センサ情報と映像音声データとのリンクを容易に実現される。
IP伝送装置の動作中は、入力されたセンサ信号や映像・音声データは入力データ一時記録メディア１０４１に循環的に記録される。また、動作ログ記録メディア１０４２には動作ログが記録される。接続回線５００に何らかの理由で障害が発生し、センサ信号を伝送できなかった場合にこれらのデータが失われることを防ぐためである。
障害検知部１０４５は、ＩＰ伝送装置２００自身の故障、センサ１００からの異常（あるいはタンパ情報）、映像音声信号の入力異常、ＩＳＰ施設２００との間の回線５００の異常、現在接続している蓄積サーバ２０１の異常、などを検知するモジュールである。ネットワークインターフェイス１０４０や接続回線５００、蓄積サーバ２０１が正常で、残る部分に異常が発生した場合、推定される故障事由を示すコードをセンサ信号パケットに付与し、蓄積サーバ２０１⇒管理サーバ３０１と経由してオペレータに伝送する。これを受けてオペレータは警備員（メンテナンス員）を現地サイトに出動させ、修理を行わせる。
現在接続している蓄積サーバ２０１の異常や現在の接続回線５００の異常である場合には、別のＩＳＰ施設２００に接続し（当然回線５００も別となる）、そこにある蓄積サーバ２０１経由で基地局３００のオペレータに事由を伝達、異常があったと思われる回線５００や蓄積サーバ２０１の確認を行う。
現地サイト１００内のネットワークやファイヤウォール１０５、ネットワークインターフェイス１０４０の異常、ＩＳＰ業者での大規模な障害があった場合、無線インターフェイス１０４８を通じて、無線回線経由で蓄積サーバ２０１に接続し、前記と同様に異常が発生した旨を伝送する。
なお、ここでは、カメラ１０２やマイク１０３がセンサ・メディア入力インターフェイス１０４６からキャプチャ入力されるものとして説明したが、これらのデハイスでは直接ネットワークに出力できるものもあり、その場合でも全く同様にＩＰ伝送装置１０４でインデクシングなどが行われ蓄積サーバ２０１に送ることができる。もしこれらのマルチメディア・デバイスから蓄積サーバ２０１に直接伝送される場合にはインデクスシングは蓄積サーバ２０１で行われる。
また、IP伝送装置１０４と蓄積サーバ２０１との間で交わされる情報取得要求などはすべてパスワードや暗号化などの情報セキュリティ実現手段によって安全化されるものである。
図３は、蓄積サーバ２０１について詳しく説明するものである。
現地サイト１００のＩＰ伝送装置から送られてきたセンサ信号あるいは映像音声データは、ネットワークインターフェイス２０１０から取得され、センサ情報記録メディア２０１２、監視映像記録メディア２０１１にそれぞれ記録される。これらのデータは航空機に搭載されるボイスレコーダのように循環的に記録されるが、これを管理制御するのが循環記録制御２０１３である。
インデクシング２０１４は、カメラ１０２やマイク１０３から映像音声データが直接伝送された場合にセンサ信号との関連付けを行う。まず、映像音声データが循環記録管理２０１３によって監視映像記録メディア２０１１に記録し、その格納位置情報やこれを容易に割り出すことができるタイムコードなどをセンサ情報に付与して、センサ情報記録メディア２０１２に格納することによってこれを行う。
検索エンジン２０１５は、基地局３００のオペレータから現地サイト１００の状況を確認する際に行う、センサ情報の検索を実行する。オペレータからの検索要求が蓄積サーバ２０１に投げられると、検索エンジン２０１５に渡され、センサ情報の検索が実行され、検索結果が返される。そして検索結果に付与されたインデクス情報を基にオペレータから対応する映像音声データが要求され、オペレータのクライアントマシン上で再生される。
検索エンジン２０１５は、センサ情報記録メディア２０１２上のセンサ情報は循環記録されているため、一般的なデータベースで行われる検索時のレコードロックができない。このため検索時の状態変数を検索クライアントに持たせ、レコードをロックしないで動作するアルゴリズムとなっている。

間引転送２０１６は、IP伝送装置１０４から受けたセンサ信号を基地局３００にある管理サーバ３０１に転送する際に間引き処理を行う。これは一般的にセンサが動作する場合連続して信号が生起することが多いため、そのままの形で基地局３００のオペレータに送ると、現地サイト１００のチェックを開始した後も何度オペレータの端末に通知が生起してわずらわしいだけでなく、ISP施設２００⇒インターネット４００⇒基地局３００と無駄に通信帯域を使うことになる。そこで、同一現地サイトからのセンサ信号で一定時間内に生起した複数の信号はひとつのものとして間引きする。これにより、オペレータへのわずらわしさや通信帯域の削減を図ることができる。また、オペレータが詳細なセンサ信号の様子を知りたい場合には、蓄積サーバ２０１にアクセスして記録されているセンサ信号の履歴を取り出せばよい。

経路切替制御２０１７や障害検知２０１８の動作は、ＩＰ伝送装置２０１と基本的に同じである。ただこの場合、通信路の障害検出対象は現地サイト１００との接続回線５００とインターネット４００となる。接続回線５００に異常がある場合、基地局３００のオペレータ宛に異常を伝送する。インターネット４００側に異常がある場合には、ＩＰ伝送装置１０４側にネットワークが異常である旨の情報を送り返し、ランプ明滅やブザーなどで、現地サイトの顧客に監視できない状況であることを通知する。

図４は基地局３００に設置されている管理サーバ３０１について詳しく説明するものである。

蓄積サーバ２０１から管理サーバ３０１へ送られたセンサ信号はネットワークインターフェイス３０１０を介して監視イベントログ記録メディア３０１１に記録される。オペレータ割当部３０１３は記録されたログと出動応対ログ記録メディア３０１２とを比較し、まだオペレータが対応していない（出動応対記録メディア３０１２に記録されていない新しいもの）の中から古い順に選んで、手の空いているオペレータに割当を行う。ただし、割当済みの中に同一の現地サイト１００をチェックしているオペレータが居れば、そのオペレータに割り当てる。割り当てられた監視イベントは、オペレータが対応中であることを示すフラグと共に、出動応対ログ記録メディア３０１２に記録される。対応が終わった案件についてはオペレータの操作によって、対応状況を示すフラグが処理済に書き換えられる。また長時間対応中のままの監視イベントは、オペレータ割当部３０１３が長時間経過中の旨の情報と共に別のオペレータに割当ててフォローアップを行わせることにより、対応の遅れや放置などの基地局側の人的ミスを抑えることができる。

経路切替制御３０１４と障害検知３０１５は、IP伝送装置１０４や蓄積サーバ２０１との場合と同様、管理サーバ３０１自身や下流の蓄積サーバ２０１、IP伝送装置１０４、ならびに接続回線５００やインターネット４００などの各通信路の障害を検知し、必要に応じて通信経路の変更制御を行う。

図５は、現地サイト１００とISP施設２００、基地局３００の間でやり取りされるデータの特性について詳しく述べるものである。

個々別々の現地サイト１００にあるIP伝送装置１０４から、ISP施設２００に設置されている蓄積サーバ２０１に対して、センサ信号だけでなく映像や音声情報が伝送されるため、蓄積サーバに入力されるデータ帯域はかなり大きいものになる。しかし、帯域を消費する部分は、IP伝送装置⇒接続回線５００⇒アクセスGW２０２⇒蓄積サーバ２０１であり、通信データの集中が発生するアクセスGW２０２から蓄積サーバ２０１までのネットワークのみを補強するだけですむため、小額の設備投資で帯域問題を解決できる。

【０００６】

蓄積サーバ２０１に入力されたセンサ信号は間引転送２０１６によって間引かれ、基地局３００に伝送される。映像情報はそのまま蓄積サーバ２０１に記録される。これにより、ISP施設２００からインターネット４００を経由して基地局３００に送られる通信データ量はほとんどゼロに近くなるため、現地サイト１００からISP施設２００に集積した元のデータ量に比べてかなり少なくなる。これにより各ISP施設２００から基地局３００に集まるセンサ情報のデータ量も一般的なIP接続回線程度に収めることが可能になる。また、映像データは、基地局３００ではオペレータが間引かれたセンサ信号をチェックする際に

のみ取得されるため、最大でもオペレータが現地サイト１００のライブ映像を見るときと同程度の帯域しか使用しないですむ。
以上のように、本願では現地サイトの外部に、サイト内から発信される信号・映像・音声などを定期的に取り出し、記録・蓄積する手段（蓄積サーバ）と、上記蓄積手段を現地サイトが接続するISP（インターネットサービスプロバイダ）に設置することを可能にする情報セキュリティ実現手段（プロトコル）と、基地局あるいは基地局が接続するISPに配置する上記蓄積手段を管理する手段（管理サーバ）を提供する。
さらに、上記蓄積手段には、基地局オペレータが即座に現地サイト情報を確認できるようにするため、サイトからの情報を常時連続的上書きに記録する手段と、サイトからのセンサ情報をトリガとし上位の管理サーバにサイトからの発報を伝送する手段と、
記録した各種情報をネットワーク経由で再生する手段と、指定したサイト情報（映像や音声）を時刻やセンサの種別などで検索する手段とを備える。
さらに、上記蓄積手段には、現地サイトの状態を常に確認できるようにするため、現地サイト内でのセンサ自身の異常、または現地サイトまでの経路の通信障害を検出する手段と、基地局、あるいは外部（警察/消防）から、現地サイト内へのネットワークカメラ等に直接アクセスできるかどうかを制御する手段とを備える。
また、上記管理手段には、下流の蓄積サーバの障害を検出する手段と、上記手段にて検出した障害をトリガとし蓄積サーバを切り替える手段と、下流の蓄積サーバまでの経路の通信異常を検出する手段と、上記手段にて検出した障害をトリガとし蓄積サーバまでの経路を切り替える手段と、下流の蓄積サーバからの発報を手の空いているオペレータに分配する手段とを備える。
さらに、蓄積サーバは警備設備からの状況情報を基地局のオペレータへの通知に必要な情報のみを残して、縮小・単一化する手段を有することを特徴とする。又、警備設備の伝送装置において、状況情報のうち、入力されるセンサ情報と映像音声のストリーム上での位置とを関連付ける情報を生成する手段を有する。
さらに、伝送装置、蓄積サーバ、管理サーバにおいて、自分自身の障害と通信路の障害を検知する手段と、障害状況を自分の代替装置又は上位に位置するサーバに伝送する手段と、障害が起きた個所を適切な代替経路・装置に切り替える手段とを有することを特徴とする遠隔警備システムを開示する。
【０００７】
【発明の効果】
本発明によれば、現地サイトへの情報セキュリティを管理しつつ、高度な機械警備に必要なサイト情報を最も帯域を消費しない方法でサイト外部に蓄積できる。これにより、警備事業者はいったん蓄積したデータで確認できるためオペレータを減らし、無駄な出動を無くすことで警備員を減らすことが可能になり、顧客に安価な設備投資でサービスを提供できる。
また、現地サイト、蓄積サーバ、管理サーバ間の経路を分散・冗長に管理できるために、サイト情報の遺失を最小限に抑えて高信頼な強固な機械警備システムを構築することが可能となる。
【図面の簡単な説明】
【図１】ブロードバンドに適化した機会警備システムについて述べたものである。
【図２】センサ情報ならびに映像音声情報をIP伝送する装置について述べたものである。
【図３】蓄積サーバについて述べたものである。
【図４】管理サーバについて述べたものである。
【図５】IP伝送装置、蓄積サーバ、管理サーバ間のデータ特性について述べたものである。
【符号の説明】
１００　監視サイト
１０１　センサ
１０２　カメラ

１０３　マイク
１０４　IP伝送装置
１０５　ファイアウォール（FW）
２００　インターネット接続業者（ISP）施設
２０１　蓄積サーバ
２０２　アクセスゲートウェイ（GW）
３００　警備業者基地局
３０１　管理サーバ
３０２　ファイアウォール（FW）
４００　インターネット
５００　接続回線。

【図１】

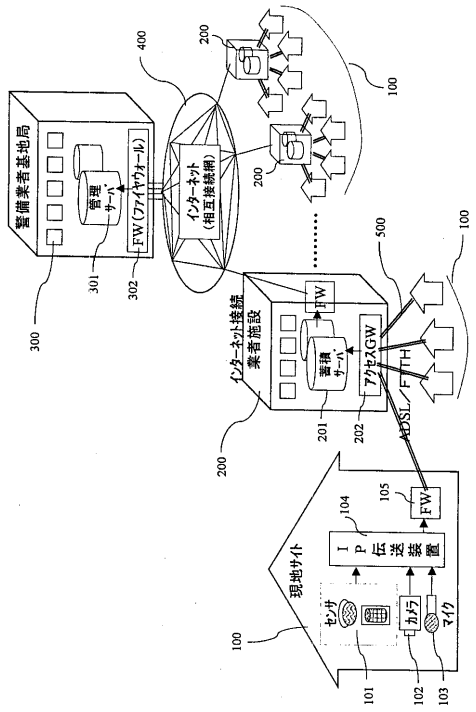


図１

【図２】

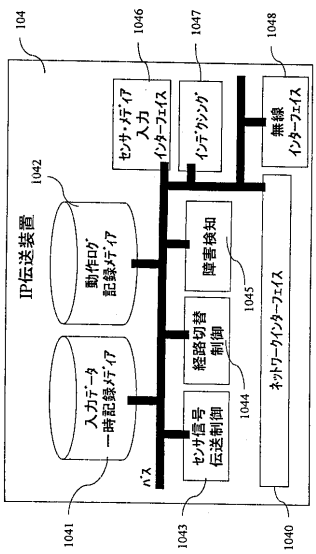
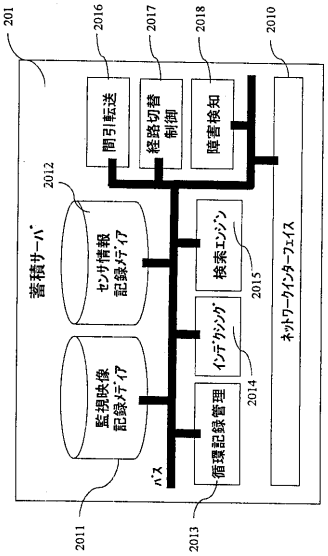


図２

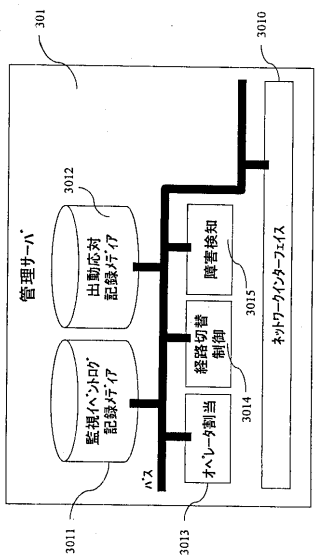
【図３】

図3



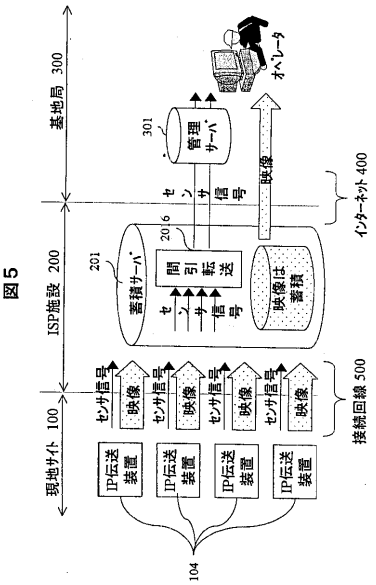
【図４】

図4



【図５】

図5



フロントページの続き

(51)Int.Cl. F I
H04Q 9/00 321Z

審査官 白石 剛史

(56)参考文献 特開２００１－０１６３４７（ＪＰ，Ａ）
特開２０００－２９５３７５（ＪＰ，Ａ）
特開２００１－３３３４１６（ＪＰ，Ａ）
特開２０００－０２３０９２（ＪＰ，Ａ）
特開２００２－０７７８８３（ＪＰ，Ａ）
特開平０４－０５４０９８（ＪＰ，Ａ）
特開平１１－１１２４０１（ＪＰ，Ａ）
特開２００１－２８３３５９（ＪＰ，Ａ）
特開２００１－３５８６３６（ＪＰ，Ａ）

(58)調査した分野(Int.Cl., ＤＢ名)
G08B 13/00-29/00
H04M 11/00
H04Q 9/00