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

特許第4781447号
(P4781447)

(45)発行日　平成23年9月28日(2011.9.28)　(24)登録日　平成23年7月15日(2011.7.15)

(51)Int.Cl.		F I		
G06F 21/20	(2006.01)	G06F	15/00	330C
H04N 7/18	(2006.01)	H04N	7/18	D
G08B 25/00	(2006.01)	G08B	25/00	510M
G08B 25/08	(2006.01)	G08B	25/00	520A
		G08B	25/08	

請求項の数 5　(全 23 頁)

(21)出願番号　特願2009-81307(P2009-81307)
(22)出願日　平成21年3月30日(2009.3.30)
(65)公開番号　特開2010-233167(P2010-233167A)
(43)公開日　平成22年10月14日(2010.10.14)
審査請求日　平成23年1月7日(2011.1.7)

早期審査対象出願

(73)特許権者　000108085
セコム株式会社
東京都渋谷区神宮前一丁目５番１号
(74)代理人　230104019
弁護士　大野　聖二
(74)代理人　100106840
弁理士　森田　耕司
(74)代理人　100117444
弁理士　片山　健一
(74)代理人　100131451
弁理士　津田　理
(72)発明者　藤沢　正幸
東京都三鷹市下連雀６－１１－２３　セコム株式会社内

最終頁に続く

(54)【発明の名称】監視システム

(57)【特許請求の範囲】
【請求項１】
監視対象に設けられた監視対象側の端末と、前記監視対象側の端末から受信した監視情報を利用する利用者側に設けられた利用者側の端末と、前記監視対象側の端末と前記利用者側の端末との通信を管理する通信管理装置と、を有した監視システムであって、
前記監視対象側の端末又は前記利用者側の端末の一方が他方に接続を要求するとき、該接続元の端末は、接続先の端末の識別情報を含むＳＩＰの招待メッセージを前記通信管理装置に送信するように構成され、
前記通信管理装置は、
ＳＩＰサーバと、
接続が認可されるべき監視対象側の端末と利用者側の端末とを対応付けた組合せを表す接続認可情報を記憶した認可情報記憶部と、
前記接続認可情報を参照して監視対象側の端末と利用者側の端末との接続を認可するか否かを判定する認可処理部と、
を有し、
前記ＳＩＰサーバは、前記接続元の端末から前記招待メッセージを取得したとき、前記招待メッセージに含まれる前記接続先の端末の識別情報を前記認可処理部に供給し、前記認可処理部が監視対象側の端末と利用者側の端末との接続を認可した場合に、前記ＳＩＰサーバが前記接続元の端末からの招待メッセージを前記接続先の端末へ供給し、
前記接続先の端末は、前記招待メッセージを前記通信管理装置から受信したときにＳＩ

ＰのＯＫメッセージを前記通信管理装置に送信し、
前記招待メッセージ及び前記ＯＫメッセージには、ＳＩＰセッション確立後に前記接続元及び接続先の端末間で前記通信管理装置を介さない端末間接続を確立するために使われる接続確立情報が付加されることを特徴とする監視システム。
【請求項２】
前記通信管理装置を介さない端末間接続は、端末間にＶＰＮを構築して接続する端末間ＶＰＮであることを特徴とする請求項１に記載の監視システム。
【請求項３】
前記招待メッセージは、前記接続元の端末のＩＰアドレスと電子証明書を前記接続確立情報として含み、前記ＯＫメッセージは、前記接続先の端末のＩＰアドレスと電子証明書を前記接続確立情報として含むことを特徴とする請求項２に記載の監視システム。
【請求項４】
前記通信管理装置と前記監視対象側又は利用者側の端末との接続は、前記通信管理装置と前記監視対象側又は利用者側の端末間にＶＰＮを構築したセンタ端末間ＶＰＮにより接続されており、前記ＳＩＰサーバは、前記センタ端末間ＶＰＮを介して前記監視対象側又は利用者側の端末とＳＩＰメッセージを通信することを特徴とする請求項１～３のいずれかに記載の監視システム。
【請求項５】
前記監視情報は、前記監視対象で撮影された画像、前記監視対象で検出された監視信号、前記利用者側にて生成された制御情報の少なくとも１つを含むことを特徴とする請求項１～４のいずれかに記載の監視システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、監視情報を取得する監視対象の端末と、監視情報を入手して利用する利用者側の端末とを通信で接続した監視システムに関する。
【背景技術】
【０００２】
従来、店舗、工場等の監視対象に監視カメラを設置し、監視映像を遠隔地で監視する監視システムが実用化されている。監視映像は、遠隔の監視センタに送信され、また、監視対象の所有者（オーナー）の事務所に送信される。監視映像の送信には、ＩＳＤＮなどの一般公衆回線が用いられる（例えば特許文献１）。
【０００３】
近年、ＡＤＳＬやＦＴＴＨといったブロードバンド回線の普及により、監視システムにおける監視映像等の送受信をインターネット上で実現することに対するニーズが高まっている。インターネットの利用により、コストの節減や、システムの柔軟性の向上が期待できる。
【０００４】
インターネット上で音声や映像を伝送する技術としては、ＳＩＰ（Session Initiation Protocol）と呼ばれるプロトコルが知られている。ＳＩＰは、ＩＰ電話やテレビ会議等に適用される。ＳＩＰで２拠点間を接続するためには、ＳＩＰサーバに各拠点のアドレスが登録される。これにより、アドレスが登録された拠点間でＳＩＰの通信が可能になる。
【先行技術文献】
【特許文献】
【０００５】
【特許文献１】特開２００１－５４１０２号公報
【発明の概要】
【発明が解決しようとする課題】
【０００６】
しかし、監視システムにＳＩＰを適用しようとすると、セキュリティ上の問題が考えら

れる。すなわち、監視対象の映像等を外部から監視する監視システムでは高いセキュリティ性が求められる。これに対して、ＳＩＰでは、アドレスを登録することによって任意の拠点間を接続できる。そのため、監視システムにＳＩＰをそのまま適用するのは、セキュリティ性の観点から望ましくない。

【０００７】

例えば、監視対象が店舗であり、複数の店舗の端末が監視センタに接続されたとする。監視センタは、各店舗のオーナーの端末とも接続される。この場合、各店舗の端末に接続できるのは、該当するオーナーの端末に限られるべきである。

【０００８】

しかし、従来のＳＩＰでは、ＳＩＰサーバにアドレスが登録されている任意の端末間で接続が可能である。ＳＩＰサーバは、基本的な認証機能として、パスワード及びＩＤの認証は行うことが可能である。しかし、これは、端末とＳＩＰサーバとの間の認証に限られる。端末とＳＩＰサーバの接続が許可されてしまうと、ＳＩＰサーバを介した端末同士の組合せを制限することはできない。したがって、店舗の端末とオーナー端末間の接続を制限することもできない。そのため、オーナーが自分以外の店舗の監視情報を入手できる可能性がある。

【０００９】

本発明は、上記背景の下でなされたもので、その目的は、監視システムにＳＩＰを適用する場合のセキュリティを向上できる監視システムを提供することにある。

【課題を解決するための手段】

【００１０】

本発明は、監視情報を通信する複数の端末と、前記複数の端末の通信を管理する通信管理装置を有し、前記複数の端末の各々が、監視対象側又は前記監視対象から受信した前記監視情報を利用する利用者側に設けられた監視システムであって、前記複数の端末の一つが他の端末に接続を要求するとき、該接続元の端末は、接続先の端末の識別情報を含むＳＩＰの招待メッセージを前記通信管理装置に送信するように構成され、前記通信管理装置は、ＳＩＰサーバと、接続が認可されるべき端末の組合せを表す接続認可情報を記憶した認可情報記憶部と、前記接続認可情報を参照して端末間の接続を認可するか否かを判定する認可処理部とを有し、前記ＳＩＰサーバは、前記接続元の端末から前記招待メッセージを取得したとき、前記招待メッセージに含まれる前記接続先の端末の識別情報を前記認可処理部に供給し、前記認可処理部が前記端末間の接続を認可した場合に、前記ＳＩＰサーバが前記接続元の端末からの招待メッセージを前記接続先の端末へ供給する。

【００１１】

上記のように本発明によれば、監視システムの複数の端末が、ＳＩＰサーバを備えた通信管理装置と接続される。通信管理装置は、ＳＩＰサーバに加え、接続が認可されるべき端末の組合せを表す接続認可情報を記憶した認可情報記憶部と、接続認可情報を参照して端末間の接続を認可するか否かを判定する認可処理部とを有する。ＳＩＰのシグナリングでは、招待メッセージが接続元の端末からＳＩＰサーバへ送られる。このとき、本発明では、認可処理部が、接続を認可するか否かを判定する。認可処理部が接続を認可した場合、ＳＩＰサーバが接続元の端末からの招待メッセージを接続先の端末に送り、ＳＩＰのシグナリングが成功する。

【００１２】

このように、本発明では、接続が認可されるべき端末の組合せの情報を予め記憶しておき、ＳＩＰのシグナリングの際に端末間の接続の認可を行う。これにより、端末とＳＩＰサーバ間の単なる認証ではなく、ＳＩＰサーバを介した端末間つまりＰ２Ｐについての認可を行うことができ、監視情報の利用者を好適に制限できる。こうして、監視システムにＳＩＰを適用する場合のセキュリティ性を向上できる。

【００１３】

前記接続先の端末は、前記招待メッセージを前記通信監理装置から受信したときにＳＩＰのＯＫメッセージを前記通信管理装置に送信してよく、前記招待メッセージ及び前記Ｏ

Ｋメッセージには、ＳＩＰセッション確立後に前記接続元及び接続先の端末間で前記通信管理装置を介さない端末間接続を確立するために使われる接続確立情報が付加されてよい。

【００１４】

これにより、ＳＩＰセッション確立後に、通信管理装置を介さずに端末間で監視情報を通信できる。この発明では、２段階の通信が行われる。１段階目の通信はＳＩＰであり、通信管理装置を介して行われる。２段階目の通信は、通信管理装置を介さない端末間接続である。ＳＩＰの接続の際にはシグナリングが行われ、シグナリングでは招待メッセージとＯＫメッセージが交換される。本発明は、ＳＩＰのシグナリングのメッセージを利用して、端末間接続の確立のための接続確立情報を交換する。こうして、ＳＩＰを上手く利用して、端末間接続を行うことができる。そして、通信管理装置と端末の通信量を低減し、通信管理装置の負荷を軽減できる。

【００１５】

前記通信監理装置を介さない端末間接続は、端末間にＶＰＮを構築して接続する端末間ＶＰＮであってよい。これにより、端末間通信（上記のＳＩＰ接続後の２段階目の通信）にＶＰＮ（仮想プライベートネットワーク）を適用することで、セキュリティ性を高くできる。ＳＩＰのシグナリングにおける双方向のメッセージ交換が、ＶＰＮ接続確立に必要な情報の交換に好適に利用される。

【００１６】

前記招待メッセージは、前記接続元の端末のＩＰアドレスと電子証明書を前記接続確立情報として含み、前記ＯＫメッセージは、前記接続先の端末のＩＰアドレスと電子証明書を前記接続確立情報として含んでよい。これにより、ＳＩＰを好適に利用して、ＶＰＮ接続に使う情報を交換し、端末間で安全な通信を行える。

【００１７】

前記通信管理装置は、前記複数の端末との通信を利用して前記監視対象を監視する監視センタに設けられてよい。これにより、通信管理装置を利用して、監視センタと端末の通信及び端末間の通信を好適に行うことができる。

【００１８】

前記通信管理装置と前記複数の端末との接続は、前記通信管理装置と前記複数の端末間にＶＰＮを構築したセンタ端末間ＶＰＮにより接続されてよく、前記ＳＩＰサーバは、センタ端末間ＶＰＮを介して前記複数の端末とＳＩＰメッセージを通信してよい。これにより、ＳＩＰ通信が、センタ端末間ＶＰＮ上で行われる。前述では、ＳＩＰセッション確立後に、端末間でＶＰＮ接続を行うことを述べた。ここでのセンタ端末間ＶＰＮは、センタと各々の端末の間のＶＰＮである。センタ端末間ＶＰＮを用いることにより、監視センタと各端末の通信のセキュリティを確保でき、そして、ＳＩＰ通信のセキュリティも確保できる。

【００１９】

前記監視情報は、前記監視対象で撮影された画像、前記監視対象で検出された監視信号、前記利用者側にて生成された制御情報の少なくとも１つを含んでよい。これにより、端末間で有用な監視情報を通信できる。

【００２０】

本発明の別の態様は、監視情報を通信する複数の端末の通信を管理する通信管理装置であって、ＳＩＰサーバと、接続が認可されるべき端末の組合せを表す接続認可情報を記憶した認可情報記憶部と、前記接続認可情報を参照して端末間の接続を認可するか否かを判定する認可処理部とを有し、前記ＳＩＰサーバが、前記複数の端末のうちの一つから、他の端末への識別情報を含むＳＩＰの招待メッセージを取得したとき、前記認可処理部が、前記招待メッセージに含まれる前記接続先の端末の識別情報に基づき、前記端末間の接続を認可するか否かを判定し、前記認可処理部が接続を認可した場合に、前記ＳＩＰサーバが、前記接続元の端末からの招待メッセージを前記接続先の端末へ供給する。この態様にも、上記の各種の構成が適用されてよい。

【００２１】
本発明は、上記監視システム及び通信管理装置の態様に限定されない。本発明の別の態様は、例えば端末装置である。また、本発明は、方法、プログラム、又は同プログラムを記録したコンピュータで読取可能な記録媒体のかたちで実現されてよい。
【発明の効果】
【００２２】
上述のように、本発明は、監視システムにＳＩＰを適用する場合のセキュリティを向上できる。
【図面の簡単な説明】
【００２３】
【図１】本発明の監視システムの全体的な構成を示す図である。
【図２】監視システムの構成をより具体的に示すブロック図である。
【図３】本発明の監視システムにおける主要な構成を示すブロック図である。
【図４】認可情報記憶部に記憶される接続認可情報のテーブルの例を示す図である。
【図５】監視システムにて端末間の通信を行うときの動作を示す図である。
【図６】監視装置が接続元になって端末間の通信を行う動作を示す図である。
【図７】利用者装置が接続元になって端末間の通信を行う動作を示す図である。
【発明を実施するための形態】
【００２４】
以下、本発明の実施の形態の監視システムについて、図面を用いて説明する。
【００２５】
図１は、本発明の監視システムの全体的な構成を示している。図示のように、監視システム１では、監視センタ３、監視対象５及び利用者拠点７の間で通信が行われる。ここで利用者とは、監視システム１による監視対象５の監視サービスの利用者を意味する。本実施の形態の例では、監視対象５が店舗であり、利用者拠点７は店舗のオーナーの事務所である。
【００２６】
監視センタ３には、通信管理装置１１及び複数のセンタ装置１３が備えられており、これらは通信可能に接続されている。通信管理装置１１及び複数のセンタ装置１３は、地理的には離れた場所に配置されてよい。複数のセンタ装置１３は、複数の担当地域にそれぞれ配置されてよい。また、複数のセンタ装置１３は機能を分担してよい。例えば、あるセンタ装置１３が、警備関連の信号を処理する管制センタ装置として機能してよく、別のセンタ装置１３が、監視映像を主に処理する画像センタ装置として機能してよい。なお、本発明の範囲でセンタ装置１３が一つでもよい。
【００２７】
監視対象５及び利用者拠点７には、それぞれ、監視装置１５及び利用者装置１７が設けられている。監視装置１５及び利用者装置１７は本発明の端末に相当する。監視装置１５は、監視情報をセンタ装置１３及び利用者装置１７へ送る。監視情報は、例えば、監視カメラの画像であり、また、監視対象５にて検出された監視信号である。監視信号は、例えば異常発生を示す警備信号であり、警備信号は、監視対象５に設置されたセンサからの検出信号に基づいて生成され、あるいは、警報ボタン（スイッチ）が操作されたときに生成される。また、利用者装置１７は、監視装置１５へ制御信号や、音声信号を送る。このような利用者装置１７から監視装置１５への信号も、監視情報に含まれる。
【００２８】
図１では、１つの監視対象５及び１つの利用者拠点７が示されている。しかし、実際には、監視センタ３は複数の監視対象５及び複数の利用者拠点７と通信する。したがって、通信管理装置１１も、複数の監視装置１５及び複数の利用者装置１７と通信する。各々の監視装置１５は関連づけられた利用者装置１７（店舗のオーナーの端末）と通信する。
【００２９】
図１の監視システム１によれば、例えば、監視装置１５がセンサ信号等により異常を検

出したとする。この場合、監視情報として警備信号が、監視対象５の映像と共に、監視センタ３へ送信される。監視センタ３では、オペレータがセンタ装置１３のモニタで警備信号や映像を確認し、警備員に必要な指示を出す。指示を受けた警備員が監視対象５に急行し、異常に対処する。

【００３０】

また例えば、監視装置１５は、監視対象５の映像等を定期的に、あるいはその他の設定に従って利用者装置１７へ送る。例えば、センサによって来客が検出されたときに、映像等が利用者装置１７へ送られる。また、利用者装置１７から映像等の送信が要求されることもある。オーナーは、映像等によって店舗の様子を把握できる。また、オーナーは、利用者装置１７から監視装置１５に音声等を送り、店員に必要事項を指示することができる。

【００３１】

次に、監視システム１の通信形態について説明する。通信管理装置１１、監視装置１５及び利用者装置１７は、インターネットに接続されている。

【００３２】

さらに、通信管理装置１１は、インターネット上でセンタ端末間ＶＰＮ（仮想プライベートネットワーク）２１によって監視装置１５及び利用者装置１７と接続される。センタ端末間ＶＰＮ２１を構築するために、通信管理装置１１にＶＰＮサーバ機能が備えられ、監視装置１５及び利用者装置１７にＶＰＮクライアント機能が備えられる。ＶＰＮでは、ＶＰＮトンネルが構築され、暗号化通信が行われ、高いセキュリティ性が実現される。

【００３３】

また、監視装置１５と利用者装置１７は、通信管理装置１１を介してＳＩＰ通信２３を行う。ＳＩＰ通信２３は、上記のセンタ端末間ＶＰＮ２１を介して行われる。通信管理装置１１にはＳＩＰサーバ機能が備えられている。

【００３４】

また、監視装置１５と利用者装置１７は、通信管理装置１１を介さずに、直接に端末間ＶＰＮ２５によって接続される。この端末間ＶＰＮ２５を構築するために、利用者装置１７にＶＰＮサーバ機能が備えられ、監視装置１５にＶＰＮクライアント機能が備えられる。

【００３５】

ここで、センタ端末間ＶＰＮ２１は、常時接続されＶＰＮトンネルが構築されており、センタ装置１３と監視装置１５及び利用者装置１７の間での通信に利用される。これに対して、端末間ＶＰＮ２５は、必要なときのみ構築される。

【００３６】

端末間ＶＰＮ２５を用いる理由を説明する。監視システム１では映像等の大容量のデータが通信される。センタ端末間ＶＰＮ２１がすべての通信に使われると、通信管理装置１１の負荷が膨大になる。そこで、監視装置１５と利用者装置１７の通信を端末間ＶＰＮ２５によって行うことで、セキュリティ性を確保しつつ、通信管理装置１１の負荷を軽減している。

【００３７】

また、本実施の形態におけるＳＩＰ通信２３の役割は、通常のＩＰ電話等とは異なる特別なものである。すなわち、本実施の形態は、ＳＩＰのシグナリングを、ＶＰＮ接続前の準備の処理として位置づけている。より詳細には、ＳＩＰ２３のセッションを確立するときには、シグナリングが行われる。このシグナリングにて双方向通信が行われ、招待メッセージとＯＫメッセージが交換される。一方、ＶＰＮ接続を確立するためには、情報の交換が必要である。本実施の形態では、ＩＰアドレス及び電子証明書が交換される。電子証明書は、電子署名等の正当性を検証する際に利用され、信頼のある第三者機関から発行されるものを用いる。そこで、ＳＩＰ通信２３のシグナリングが、ＶＰＮ接続確立のための情報交換の手段として利用される。

【００３８】

以上に、監視システム１の全体構成を説明した。上記のように、本実施の形態では、２種類のＶＰＮが使用される。一方は、通信管理装置１１と端末（監視装置１５又は利用者装置１７）を接続し、他方は、端末同士（監視装置１５と利用者装置１７）を接続する。そこで、図１では、これら２つのＶＰＮを区別するため、センタ端末間ＶＰＮ２１と端末間ＶＰＮ２５といった用語を用いている。ただし、単にＶＰＮ２１、ＶＰＮ２５といった用語が用いられてよい。

【００３９】

次に、図２を参照し、監視システム１の構成をより具体的に説明する。通信管理装置１１は、ファイアウォール３１、ＨＴＴＰサーバ３３、ＶＰＮサーバ３５、ＳＩＰサーバ３７、ＳＴＵＮサーバ３９、アカウント管理サーバ４１、データベース４３及びログサーバ４５を備える。

【００４０】

ファイアウォール３１は、通信管理装置１１と監視装置１５及び利用者装置１７との間で使用される通信データ以外のデータを遮断する装置である。ＨＴＴＰサーバ３３はインターネット接続のための構成である。ＶＰＮサーバ３５は、ＶＰＮトンネル構築のための認証と暗号化を行うサーバである。

【００４１】

ＶＰＮサーバ３５は、センタ端末間ＶＰＮ２１を実現する構成であり、通信管理装置１１と監視装置１５の間にＶＰＮを構築し、また、通信管理装置１１と利用者装置１７の間にＶＰＮを構築する。監視装置１５からの信号は、ＶＰＮサーバ３５で復号化されて、センタ装置１３へ送信される。また、センタ装置１３からの信号は、ＶＰＮサーバ３５で暗号化されて、監視装置１５へ送信される。また、通信管理装置１１が監視装置１５に信号を送るときも、ＶＰＮサーバ３５で暗号化が行われる。通信管理装置１１と利用者装置１７の通信でも、ＶＰＮサーバ３５が同様に暗号化及び復号化を行う。

【００４２】

ＳＩＰサーバ３７は、ＳＩＰプロトコルに従ってシグナリングの処理を行い、監視装置１５と利用者装置１７を接続する。ＳＩＰサーバ３７は、利用者装置１７が監視装置１５に接続を要求する場合に、もしくは、監視装置１５が利用者装置１７に接続を要求する場合に、ＳＩＰの接続制御の機能を果たす。

【００４３】

ＳＩＰのシグナリングでは、メッセージが交換される。具体的には、ＩＮＶＩＴＥ（招待）メッセージとＯＫメッセージが交換される。このメッセージ交換を利用して、前述したように、ＶＰＮ接続確立のためにＩＰアドレス及び電子証明書が交換される。

【００４４】

ＳＴＵＮサーバ３９は、監視装置１５及び利用者装置１７のルータのＮＡＴ機能に対応するためにＳＴＵＮ機能を提供する。

【００４５】

アカウント管理サーバ４１は、認証等の各種の情報を管理するサーバである。管理される情報は、データベース４３に格納される。管理される情報は、ＩＰ回線のアカウント、ＶＰＮ接続（トンネル構築）のための電子証明書、鍵ペアの情報を含む。また、本実施の形態では、ＳＩＰのシグナリングの過程で、端末間の接続について認証及び認可が行われる。この処理のための情報も、データベース４３に保持され、アカウント管理サーバ４１に使用される。尚、端末間の接続についての認証及び認可は、ＳＩＰサーバ自身が行うようにすることもでき、この場合は本発明の認可処理部及び認可情報記憶部がＳＩＰサーバに備えられることになる。

【００４６】

ログサーバ４５は、監視装置１５で生成したログを保存するためのサーバである。

【００４７】

センタ装置１３は、監視卓５１と回線接続装置５３を備える。監視卓５１が回線接続装置５３を介して通信管理装置１１に接続される。例えば、センタ装置１３が画像センタで

ある場合、監視映像が監視卓５１に供給され、監視卓５１にて管理される。また、センタ装置１３が管制センタである場合、警備関連の情報が監視卓５１に供給される。監視映像も管制センタのモニタに好適に表示される。監視映像等は、センタ装置同士の間でも通信されてよい。

【００４８】

次に、監視装置１５について説明する。監視装置１５は、コントローラ６１、ＩＰ回線ユニット６３、ルータ６５、周辺機器６７、マルチ回線アダプタ６９及び監視対象ＰＣ（パーソナルコンピュータ）７１で構成されている。

【００４９】

コントローラ６１はコンピュータで構成されており、周辺機器６７と連携して、監視機能を実現する。コントローラ６１は、監視センタ３とはＩＰ回線ユニット６３を介して接続される。また、コントローラ６１は、利用者装置１７とも、ＩＰ回線ユニット６３を介して接続される。

【００５０】

図２では、周辺機器６７として監視カメラ７３、センサ７５及び警報ボタン７７が例示されている。コントローラ６１は、監視映像に対して画像認識処理を施して異常を検出する。また、コントローラ６１は、センサ７５から入力される検出信号により、異常を検出する。警報ボタン７７が押されたときにも異常が検出される。その他の周辺機器が異常検出に用いられてよい。異常が発生すると、コントローラ６１はセンタ装置１３と通信し、警備信号と画像信号を送信する。監視カメラ７３と共にマイクが備えられており、音声信号も送信される。このようにして、コントローラ６１は監視対象５の警備機能を実現する。

【００５１】

また、監視映像及び音声は、センタ装置１３から要求されたときにも送信される。さらに、監視映像及び音声は、利用者装置１７にも送られる。利用者装置１７への送信は、例えば定期的に行われ、また、その他の設定に従って行われる。例えば、センサ７５により来客が検知されると、映像等が利用者装置１７に送られる。また、利用者装置１７から要求されたときも、監視装置１５は映像等を送信する。

【００５２】

ＩＰ回線ユニット６３は、コントローラ６１が通信管理装置１１と通信するためのＶＰＮトンネルを構築する。また、コントローラ６１が利用者装置１７と通信するためのＶＰＮトンネルを構築する。前者は、センタ端末間ＶＰＮ２１に対応し、後者は、端末間ＶＰＮ２５に対応する。これらの接続において、ＩＰ回線ユニット６３は、ＶＰＮクライアントの機能を実現する。

【００５３】

図２では、ＩＰ回線ユニット６３がコントローラ６１の内部構成として示されている。これは、物理的な配置を表現している。通信構成としては、ＩＰ回線ユニット６３は、コントローラ６１とルータ６５の間に配置されている。そして、ＩＰ回線ユニット６３は、コントローラ６１と、イーサネット（登録商標）でＬＡＮ接続されている。ルータ６５は、ブロードバンド回線用のルータである。

【００５４】

マルチ回線アダプタ６９は、携帯電話網を介してセンタ装置１３と接続される。マルチ回線アダプタ６９は、ブロードバンド回線が不通のときに警備信号を送信するために使用される。警備信号が、コントローラ６１からＩＰ回線ユニット６３を介してマルチ回線アダプタ６９に送られ、マルチ回線アダプタ６９からセンタ装置１３へと送信される。

【００５５】

監視対象ＰＣ７１は、監視対象５に設置されるＰＣである。本実施の形態の例では、監視対象５が店舗である。したがって、監視対象ＰＣ７１は店舗用のＰＣでよい。

【００５６】

次に、利用者装置１７について説明する。利用者装置１７は、ＶＰＮ終端装置（以下、

ＶＴＥ）８１、ルータ８３及び利用者ＰＣ（パーソナルコンピュータ）８５で構成されている。

【００５７】

ＶＴＥ８１は、ブロードバンド接続のための回線終端装置である。そして、ＶＴＥ８１は、通信管理装置１１のＶＰＮサーバ３５とＶＰＮトンネルを構築し、また、監視装置１５のＩＰ回線ユニット６３とＶＰＮトンネルを構築する。前者では、ＶＴＥ８１がＶＰＮクライアントとして機能し、後者では、ＶＴＥ８１がＶＰＮサーバとして機能する。ルータ８３は、ブロードバンド回線用のルータである。

【００５８】

ＶＴＥ８１は、利用者ＰＣ８５と接続される。ＶＴＥ８１は、監視装置１５のコントローラ６１から受信した映像、音声及び制御信号を利用者ＰＣ８５に転送する。また、ＶＴＥ８１は、利用者ＰＣ８５から受信した音声及び制御信号をコントローラ６１へ転送する。

【００５９】

本実施の形態では、利用者拠点７が、店舗のオーナーの事務所等である。したがって、利用者ＰＣ８５は、店舗のオーナーのＰＣでよい。利用者ＰＣ８５は、オーナーが監視対象５の監視映像を見るために用いられる。この機能を提供するために、利用者ＰＣ８５には、コントローラ６１と通信することによって監視対象５の監視映像を表示及び切り換えることができるアプリケーションソフトがインストールされている。

【００６０】

本実施の形態では、利用者装置１７が固定されている。しかし、利用者装置１７の機能が携帯端末等に組み込まれて、移動可能であってもよい。

【００６１】

以上に、監視システム１の全体的な構成を説明した。次に、本発明の特徴に係る構成について説明する。

【００６２】

図３は、図１及び図２に示された監視システム１の一部であって、本発明の主要な部分を示している。図３において、図１及び図２で説明された要素には、同一の符号が付されている。

【００６３】

図３に示すように、通信管理装置１１は、ＶＰＮサーバ３５、ＳＩＰサーバ３７に加えて、認可情報記憶部１０１及び認可処理部１０３を備えている。認可情報記憶部１０１は、接続が認可されるべき端末（監視装置１５及び利用者装置１７）の組合せを表す接続認可情報を記憶する。そして、認可処理部１０３は、接続認可情報を参照して端末間の接続を認可するか否かを判定する。認可情報記憶部１０１及び認可処理部１０３は、図２のデータベース４３及びアカウント管理サーバ４１によってそれぞれ実現される。

【００６４】

図４は、認可情報記憶部１０１に記憶されるべき接続認可情報の例を示している。この例では、接続認可情報が、端末ＩＤの組合せを表すテーブルである。このテーブルは、各利用者（店舗のオーナー）と、監視装置ＩＤ（監視装置１５のＩＤ）と、利用者装置ＩＤ（利用者装置１７のＩＤ）とを対応づけている。監視装置ＩＤ及び利用者装置ＩＤは、監視装置１５及び利用者装置１７を特定可能な任意の情報でよい。後述の例では、監視装置ＩＤがＩＰ回線ユニット６３のＩＤであり、利用者装置ＩＤがＶＴＥ８１のＩＤである。

【００６５】

一人のオーナーが複数の店舗を有する場合がある。この場合、一つの監視装置１５が、複数の利用者装置１７と組み合わせられる。図４の例では、利用者Ｃが２つの店舗を有しており、２つの監視装置１５（Ｃ０１、Ｃ０２）が、利用者装置１７（Ｃ１１）と対応づけられている。その他、一人のオーナーが複数の利用者装置１７を使う場合等は、一つの監視装置１５が複数の利用者装置１７と対応づけられてよい。

【００６６】

図３に戻り、監視装置１５において、ＩＰ回線ユニット６３は、ＳＩＰ処理部１１１、ＶＰＮ処理部１１３及び記憶部１１５を有する。ＳＩＰ処理部１１１及びＶＰＮ処理部１１３は、それぞれ、ＳＩＰ及びＶＰＮに関する処理を行う。記憶部１１５は、ＩＰ回線ユニット６３で処理される各種の情報を記憶する。特に、本発明に関連して、記憶部１１５は、ＩＰ回線ユニット６３のＩＰアドレスと電子証明書とを記憶している。これら情報は、本発明の接続確立情報に相当し、ＶＰＮ接続のために接続相手に提供される。また、記憶部１１５は、ＩＰ回線ユニットＩＤ（ＩＰ回線ユニット６３のＩＤ）を記憶しており、このＩＰ回線ユニットＩＤが監視対象５のＩＤとして用いられる。

【００６７】

図３に示すように、利用者装置１７のＶＴＥ８１も、ＳＩＰ処理部１２１、ＶＰＮ処理部１２３及び記憶部１２５を有している。記憶部１２５は、ＶＴＥ８１のＩＰアドレスと電子証明書とを記憶している。また、記憶部１２５は、ＶＴＥ－ＩＤ（ＶＴＥ８１のＩＤ）を記憶している。

【００６８】

次に、本実施の形態の動作を説明する。ここでは、端末間ＶＰＮ２５を構築するときの動作、すなわち、監視装置１５と利用者装置１７の間のＶＰＮ接続を行う際の動作を説明する。

【００６９】

まず、動作の概要を説明する。既に説明したように、通信管理装置１１と監視装置１５の間には、センタ端末間ＶＰＮ２１が常時構築されている。通信管理装置１１と利用者装置１７の間にもセンタ端末間ＶＰＮ２１が常時構築されている。これらのセンタ端末間ＶＰＮ２１とは別に、以下の動作により、監視装置１５と利用者装置１７の間に直接に端末間ＶＰＮ２５が構築される。

【００７０】

端末間ＶＰＮ２５を接続するときには、情報の交換が行われる。本実施の形態では、ＩＰアドレスと電子証明書が、監視装置１５と利用者装置１７の間で交換される。この情報交換の手段として、本実施の形態は、ＳＩＰに着目している。ＳＩＰのシグナリングでは、端末間でメッセージが交換される。これらのＳＩＰメッセージに、上記のＩＰアドレス及び電子証明書が組み込まれる。これにより、ＳＩＰのシグナリング過程にて、端末間ＶＰＮ２５の構築準備のための情報交換を行える。

【００７１】

ＳＩＰの基本的機能では、ＳＩＰサーバ３７に登録されている任意のアドレス間でＳＩＰの接続が確立される。この場合、監視装置１５が関係ない利用者装置１７と接続される可能性があり、セキュリティ上望ましくない。この点に配慮し、本実施の形態では、下記のようにしてシグナリングが行われる。以下では、監視装置１５及び利用者装置１７の一方を、ＳＩＰの接続元端末とし、他方をＳＩＰの接続先端末とする。また、ＳＩＰのメッセージは、センタ端末間ＶＰＮ２１上で送信される。

【００７２】

図５を参照すると、まず、接続元端末が、ＩＮＶＩＴＥメッセージ（詳細にはＳＩＰ ＩＮＶＩＴＥメッセージ、以下同じ）を、ＳＩＰサーバ３７に送る（Ｓ１）。ＩＮＶＩＴＥメッセージには、接続元端末のＩＤ及び接続先端末のＩＤと、接続元端末のＩＰアドレス及び電子証明書が付加される。

【００７３】

ＳＩＰサーバ３７は、ＩＮＶＩＴＥメッセージを受け取ると、接続元端末のＩＤと接続先端末のＩＤを認可処理部１０３に供給し、それら接続元端末と接続先端末の接続の可否を認可処理部１０３に問い合わせる（Ｓ３）。認可処理部１０３は、認可情報記憶部１０１の接続認可情報を参照し、接続を認可するか否かの判定を行う（Ｓ５）。接続元端末と接続先端末の組み合わせが認可情報記憶部１０１に登録されていれば、接続が認可される。

【００７４】

ＳＩＰサーバ３７は、認可処理部１０３から認可結果を受け取る（Ｓ７）。ＳＩＰサーバ３７は、認可処理部１０３によって接続が認可されると、ＩＮＶＩＴＥメッセージを接続先端末へ送信する（Ｓ９）。このＩＮＶＩＴＥメッセージは、接続元端末のＩＰアドレス及び電子証明書を含む。

【００７５】

接続先端末は、ＩＮＶＩＴＥメッセージを受信すると、ＳＩＰサーバ３７へＯＫメッセージ（詳細には、ＳＩＰ　２００ＯＫメッセージ、以下、同じ）を送る（Ｓ１１）。ＯＫメッセージには、接続先端末のＩＰアドレスと電子証明書が付加される。このＯＫメッセージがＳＩＰサーバ３７を介して接続元端末へ送信される（Ｓ１３）。こうして、ＳＩＰのシグナリングによってＩＰアドレス及び電子証明書が交換される。そして、端末間でＶＰＮを構築しようとするときは、接続要求に含まれる電子証明書と先に交換した電子証明書により認証を行い、端末間ＶＰＮ２５が構築される（Ｓ１５）。

【００７６】

上述のように、本実施の形態では、ＩＮＶＩＴＥメッセージがＳＩＰサーバ３７に受信されたときに、端末の組合せを認可する処理が行われる。接続が認可されなければ、ＩＮＶＩＴＥメッセージは接続先端末に送られず、その後のＳＩＰの処理も、ＶＰＮの処理も行われない。監視装置１５と利用者装置１７の組合せが適正である場合のみ、接続が認可され、ＩＮＶＩＴＥメッセージが接続先端末に送られ、その後のＳＩＰの処理が行われ、最終的にＶＰＮ接続が可能である。

【００７７】

次に、図６及び図７を参照し、監視システム１の動作の詳細を説明する。ここでは、まず、監視装置１５が接続元端末である場合について説明し、次に、利用者装置１７が接続元である場合について説明する。

【００７８】

図６のタイムチャートにおいて、コントローラ６１及びＩＰ回線ユニット６３が監視装置１５の構成であり、ＳＩＰサーバ３７及び認可情報記憶部１０１（アカウント管理サーバ４１）が通信管理装置１１の構成であり、ＶＴＥ８１及び利用者ＰＣ８５が利用者装置１７の構成である。

【００７９】

コントローラ６１は、ＶＴＥ－ＩＤ（ＶＴＥ８１のＩＤ）を含む接続指示（Ｐ２Ｐ接続指示）をＩＰ回線ユニット６３に送る（Ｓ１０１）。ここでは、ＶＴＥ－ＩＤが、接続先端末ＩＤとして用いられている。

【００８０】

ＩＰ回線ユニット６３は、記憶部１１５からＩＰ回線ユニットＩＰアドレス（ＩＰ回線ユニット６３のＩＰアドレス）及びＩＰ回線ユニット個別証明書を読み出す。ＩＰ回線ユニット個別証明書は、ＩＰ回線ごとに割り振られた電子証明書である。また、ＩＰ回線ユニット６３は、記憶部１１５から、接続元端末ＩＤとしてのＩＰ回線ユニットＩＤ（ＩＰ回線ユニット６３のＩＤ）を読み出す。そして、ＩＰ回線ユニット６３は、これら情報をＩＮＶＩＴＥメッセージに付加し、ＩＮＶＩＴＥメッセージをＳＩＰサーバ３７に送る（Ｓ１０３）。具体的には、ＩＮＶＩＴＥメッセージは、ＩＰ回線ユニットＩＰアドレス、ＩＰ回線ユニットＩＤ、ＶＴＥ－ＩＤ及びＩＰ回線ユニット個別証明書を含む。

【００８１】

ＳＩＰサーバ３７は、ＩＮＶＩＴＥメッセージを受信し、ＩＰ回線ユニットＩＤ及びＶＴＥ－ＩＤを認可処理部１０３に伝え、接続を認可するか否かを問い合わせる（Ｓ１０５）。認可処理部１０３は、認可情報記憶部１０１の接続認可情報を参照し、接続を認可するか否かを判定する（Ｓ１０７）。ここでは、図４のテーブルが読み出される。そして、認可処理部１０３は、問合せの端末ＩＤの組合せがテーブルに登録されているか否かを判定する。該当する組合せが登録されていれば、認可処理部１０３は接続を認可する。認可結果は、認可処理部１０３からＳＩＰサーバ３７へ伝えられる（Ｓ１０９）。ＳＩＰサーバ３７は、認可処理部１０３が接続を認可した場合に、ＩＮＶＩＴＥメッセージをＶＴＥ

８１へ送信する（Ｓ１１１）。このＩＮＶＩＴＥメッセージには、ＩＰ回線ユニットＩＰアドレス及びＩＰ回線ユニット個別証明書が付加される。

【００８２】

上記の処理において、ステップＳ１０７で接続が認可されなければ、ＳＩＰサーバ３７はＩＮＶＩＴＥメッセージをＶＴＥ８１へ送らない。したがって、その後のＳＩＰの処理は行われず、さらにその後のＶＰＮ接続も行われない。

【００８３】

ＶＴＥ８１は、ＩＮＶＩＴＥメッセージを受信すると、ＩＰ回線ユニットＩＰアドレス及びＩＰ回線ユニット個別証明書を記憶部１２５に保持し、利用者ＰＣ８５に接続要求（Ｐ２Ｐ接続要求）の問い合わせを行う（Ｓ１１３）。この接続要求には、ＩＰ回線ユニットＩＰアドレスが付加される。そして、利用者ＰＣ８５がＶＴＥ８１に接続応答を送る（Ｓ１１５）。

【００８４】

ＶＴＥ８１は、ＶＴＥ－ＩＰアドレス（ＶＴＥ８１のＩＰアドレス）及びＶＴＥ個別証明書（ＶＴＥ８１に割り振られた電子証明書）を記憶部１２５から読み出す。そして、ＶＴＥ８１は、ＯＫメッセージをＳＩＰサーバ３７に送信する（Ｓ１１７）。このＯＫメッセージには、ＶＴＥ－ＩＰアドレス、ＶＴＥ個別証明書が付加される。

【００８５】

ＳＩＰサーバ３７は、ＶＴＥ－ＩＰアドレス及びＶＴＥ個別証明書と共にＯＫメッセージをＩＰ回線ユニット６３に送信する（Ｓ１１９）。ＩＰ回線ユニット６３は、ＯＫメッセージを受信すると、ＶＴＥ－ＩＰアドレス及びＶＴＥ個別証明書を記憶部１１５に保持して、ＡＣＫメッセージをＳＩＰサーバ３７に送り（Ｓ１２１）、更にＳＩＰサーバ３７がＡＣＫメッセージをＶＴＥ８１へ送る（Ｓ１２３）。

【００８６】

上記の過程で、ＩＰ回線ユニット６３は、ＶＴＥ８１のＩＰアドレス及び電子証明書を取得している。また、ＶＴＥ８１は、ＩＰ回線ユニット６３のＩＰアドレス及び電子証明書を取得している。したがって、これら情報を用いて相手方を認識してＩＰ回線ユニット６３とＶＴＥ８１の間でＶＰＮ接続確立が可能となる。これが、端末間ＶＰＮ２５である。

【００８７】

図示のように、ＩＰ回線ユニット６３が、ＶＴＥ８１へＶＰＮ接続要求を行う（Ｓ１２５）。ここでは、ＳＩＰサーバ３７を介さずに、直接にＶＰＮ接続が要求される。ＶＴＥ８１は、ＶＰＮ接続要求に含まれるＩＰ回線ユニット個別証明書と記憶部１２５に保持してあるＩＰ回線ユニットの個別証明書により認証を行い、相手先のＩＰ回線ユニットＩＰアドレスを含む着信情報を利用者ＰＣ８５に送る（Ｓ１２７）。ＩＰ回線ユニットＩＰアドレスは、利用者ＰＣ８５にてＶＰＮ通信のために使用される。また、ＶＴＥ８１は、ＶＰＮサーバとして、ＶＰＮ接続の処理を行ったことをＩＰ回線ユニット６３に通知する（Ｓ１２９）。ＩＰ回線ユニット６３は、接続結果がＯＫであることをコントローラ６１に通知し、また相手先のＶＴＥ－ＩＰアドレスをコントローラ６１に通知する（Ｓ１３１）。ＶＴＥ－ＩＰアドレスは、コントローラ６１にてＶＰＮ通信のために使用される。こうして、ＶＰＮ接続が確立され、端末間ＶＰＮ２５を介して情報が通信される。監視映像及び音声等が、監視装置１５から利用者装置１７へと提供される。

【００８８】

次に、図７を参照し、利用者装置１７が接続元である場合について説明する。利用者（オーナー）が例えば映像表示の指示を利用者ＰＣ８５に入力したとする。利用者ＰＣ８５は、ＩＰ回線ユニットＩＤを含む接続指示（Ｐ２Ｐ接続指示）をＶＴＥ８１に送る（Ｓ２０１）。ここでは、ＩＰ回線ユニットＩＤが、接続先端末のＩＤとして用いられている。

【００８９】

ＶＴＥ８１は、記憶部１２５からＶＴＥ－ＩＰアドレス及びＶＴＥ個別証明書を読み出す。また、ＶＴＥ８１は、記憶部１２５から、接続元端末ＩＤとしてのＶＴＥ－ＩＤを読

み出す。そして、ＶＴＥ８１は、これら情報をＩＮＶＩＴＥメッセージに付加し、ＩＮＶＩＴＥメッセージをＳＩＰサーバ３７に送る（Ｓ２０３）。具体的には、ＩＮＶＩＴＥメッセージは、ＶＴＥ－ＩＰアドレス、ＶＴＥ－ＩＤ、ＩＰ回線ユニットＩＤ及びＶＴＥ個別証明書を含む。

【００９０】

ＳＩＰサーバ３７は、ＩＮＶＩＴＥメッセージを受信して、ＶＴＥ－ＩＤ、ＩＰ回線ユニットＩＤを認可処理部１０３に伝え、接続を認可するか否かを問い合わせる（Ｓ２０５）。認可処理部１０３は、前述と同様にして認可情報記憶部１０１の接続認可情報を参照し、接続を認可するか否かを判定し（Ｓ２０７）、認可結果をＳＩＰサーバ３７へ送る（Ｓ２０９）。すなわち、ＶＴＥ－ＩＤ、ＩＰ回線ユニットＩＤの組合せが登録されていれば、接続が認可される。ＳＩＰサーバ３７は、認可処理部１０３が接続を認可した場合に、ＩＮＶＩＴＥメッセージをＩＰ回線ユニット６３へ送信する（Ｓ２１１）。このＩＮＶＩＴＥメッセージには、ＶＴＥ－ＩＰアドレス及びＶＴＥ個別証明書が付加される。

【００９１】

上記の処理において、ステップＳ２０７で接続が認可されなければ、ＳＩＰサーバ３７はＩＮＶＩＴＥメッセージをＩＰ回線ユニット６３へ送らない。したがって、その後のＳＩＰの処理は行われず、さらにその後のＶＰＮ接続も行われない。

【００９２】

ＩＰ回線ユニット６３は、ＩＮＶＩＴＥメッセージを受信すると、ＶＴＥ－ＩＰアドレス及びＶＴＥ個別証明書を記憶部１１５に保持する。また、ＩＰ回線ユニット６３は、コントローラ６１に接続要求（Ｐ２Ｐ接続要求）の問い合わせを行う（Ｓ２１３）。この接続要求には、ＶＴＥ－ＩＰアドレスが付加される。そして、コントローラ６１がＩＰ回線ユニット６３に接続応答を送る（Ｓ２１５）。

【００９３】

ＩＰ回線ユニット６３は、ＩＰ回線ユニットＩＰアドレス及びＩＰ回線ユニット個別証明書を記憶部１１５から読み出す。そして。ＩＰ回線ユニット６３は、ＯＫメッセージをＳＩＰサーバ３７に送信する（Ｓ２１７）。このＯＫメッセージには、ＩＰ回線ユニットＩＰアドレス、ＩＰ回線ユニット個別証明書が付加される。

【００９４】

ＳＩＰサーバ３７は、ＩＰ回線ユニットＩＰアドレス及びＩＰ回線ユニット個別証明書と共にＯＫメッセージをＶＴＥ８１に送信する（Ｓ２１９）。ＶＴＥ８１は、ＯＫメッセージを受信すると、ＩＰ回線ユニットＩＰアドレス及びＩＰ回線ユニット個別証明書を記憶部１２５に保持して、ＡＣＫメッセージをＳＩＰサーバ３７へ返信し（Ｓ２２１）、また、利用者ＰＣ８５にＳＩＰ接続の確立を通知する（Ｓ２２３）。ＳＩＰサーバ３７は、ＡＣＫメッセージをＩＰ回線ユニット６３に送信する（Ｓ２２５）。

【００９５】

上記の過程で、ＩＰ回線ユニット６３とＶＴＥ８１の間で、ＩＰアドレス及び電子証明書が交換されている。ＩＰ回線ユニット６３は、ＡＣＫメッセージを受信すると、ＶＰＮ接続要求をＶＴＥ８１に対して行う（Ｓ２２７）。ＶＰＮ接続は、ＳＩＰサーバ３７を介さずに行われる。ＶＴＥ８１は、相手先のＶＴＥ－ＩＰアドレスを含む着信情報を利用者ＰＣ８５に送る（Ｓ２２９）。また、ＶＴＥ８１は、ＶＰＮサーバとして、ＶＰＮ接続の処理を行ったことをＩＰ回線ユニット６３に通知する（Ｓ２３１）。ＩＰ回線ユニット６３は、相手先のＶＴＥ－ＩＰアドレスを含む着信情報をコントローラ６１に送る（Ｓ２３３）。こうして、ＶＰＮ接続が確立され、端末間ＶＰＮ２５を介して情報が通信される。

【００９６】

図６、図７に示されるように、両図の処理で、ＶＰＮ接続要求は、ＩＰ回線ユニット６３からＶＴＥ８１へ送られている。この理由は以下の通りである。ＶＰＮでは、接続要求がクライアントからサーバへ送られる必要がある。本実施の形態では、ＶＰＮサーバの機能が、ＶＴＥ８１のみに設けられている。そのため、図６及び図７の双方において、ＶＰＮ接続要求がＩＰ回線ユニット６３からＶＴＥ８１へ送られる。

【００９７】
以上に本発明の好適な実施の形態について説明した。本実施の形態によれば、複数の端末（監視装置１５、利用者装置１７）が、ＳＩＰサーバ３７を備えた通信管理装置１１と接続される。図３に示したように、通信管理装置１１は、ＳＩＰサーバ３７に加え、認可情報記憶部１０１と認可処理部１０３とを有する。ＳＩＰのシグナリングでは、ＩＮＶＩＴＥ（招待）メッセージが接続元の端末からＳＩＰサーバへ送られる。このとき、認可処理部１０３が、接続を認可するか否かを判定する。認可処理部１０３が接続を認可した場合のみ、ＳＩＰサーバ３７が接続元の端末からのＩＮＶＩＴＥメッセージを接続先の端末に送り、ＳＩＰのシグナリングが成功する。

【００９８】
このように、本発明では、接続が認可されるべき端末の組合せの情報を予め記憶しておき、ＳＩＰのシグナリングの際に端末間の接続の認可を行う。これにより、端末とＳＩＰサーバ３７間の単なる認証ではなく、ＳＩＰサーバ３７を介した端末間つまりＰ２Ｐについての認可を行うことができ、監視情報の利用者を好適に制限できる。こうして、監視システム１にＳＩＰを適用する場合のセキュリティ性を向上できる。

【００９９】
また、本発明では、ＳＩＰのシグナリングにおけるＩＮＶＩＴＥメッセージとＯＫメッセージの交換に、通信管理装置１１を介さない端末間接続の確立に使う接続確立情報が付加されてよい。これにより、接続確立情報が端末間で交換され、端末間接続を確立できる。このようして、ＳＩＰを上手く利用して、端末間接続を行うことができる。そして、通信管理装置１１と端末の通信量を低減し、通信管理装置１１の負荷を軽減できる。

【０１００】
尚、本実施の形態では、接続確立情報としてＩＰアドレスと電子証明書を例に説明したが、電子証明書の代わりに他の情報を用いて相手方の認証を行うようにしても良い。例えば電子証明書に含まれるコモンネームなどを接続確立情報として用いても良い。

【０１０１】
また、本発明によれば、通信監理装置１１を介さない端末間接続が、端末間にＶＰＮを構築して接続する端末間ＶＰＮ２５であってよい。ＳＩＰのシグナリングにおける双方向のメッセージ交換を、ＶＰＮ接続確立に必要な情報の交換に好適に利用でき、そして、ＶＰＮの適用によりよりセキュリティ性を高くできる。

【０１０２】
また、本発明によれば、招待メッセージが接続元の端末のＩＰアドレスと電子証明書を接続確立情報として含み、ＯＫメッセージが接続先の端末のＩＰアドレスと電子証明書を接続確立情報として含んでよい。これにより、ＳＩＰを好適に利用して、ＶＰＮ接続に使う情報を交換し、端末間で安全な通信を行える。

【０１０３】
また、本発明によれば、通信管理装置１１が監視センタ３に設けられてよい。これにより、通信管理装置１１を利用して、監視センタ３と端末の通信及び端末間の通信を好適に行うことができる。

【０１０４】
また、本発明によれば、通信管理装置１１と複数の端末との接続は、通信管理装置１１と複数の端末間にＶＰＮを構築したセンタ端末間ＶＰＮ２１により接続されてよく、ＳＩＰサーバ３７は、センタ端末間ＶＰＮ２１を介して複数の端末とＳＩＰメッセージを通信してよい。これにより、ＳＩＰ通信が、センタ端末間ＶＰＮ２１上で行われる。ＳＩＰセッション後に確立される端末間ＶＰＮ２５が端末間のＶＰＮであるのに対して、センタ端末間ＶＰＮ２１は通信管理装置１１と端末の間のＶＰＮである。センタ端末間ＶＰＮ２１を用いることにより、監視センタ３と各端末の通信のセキュリティを確保でき、そして、ＳＩＰ通信のセキュリティも確保できる。

【０１０５】
また、本発明によれば、監視情報が、監視対象５で撮影された画像、監視対象５で検出

された監視信号、利用者側にて生成された制御情報の少なくとも１つを含んでよい。これにより、端末間で有用な監視情報を通信できる。

【０１０６】

以上に本発明の好適な実施の形態を説明した。しかし、本発明は上述の実施の形態に限定されず、当業者が本発明の範囲内で上述の実施の形態を変形可能なことはもちろんである。

【産業上の利用可能性】

【０１０７】

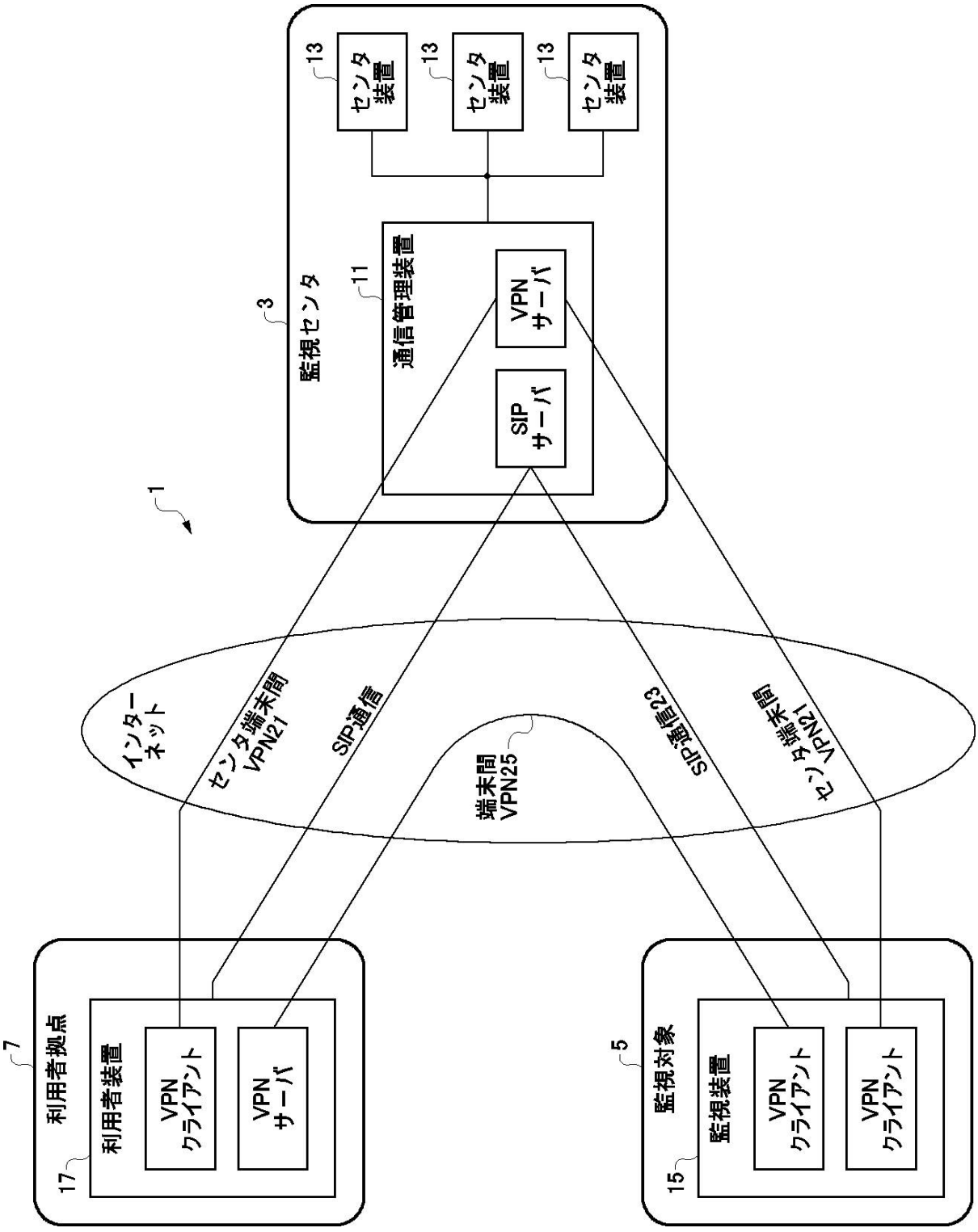
以上のように、本発明にかかる監視システムは、通信を使って遠隔地から店舗等を監視するために有用である。

【符号の説明】

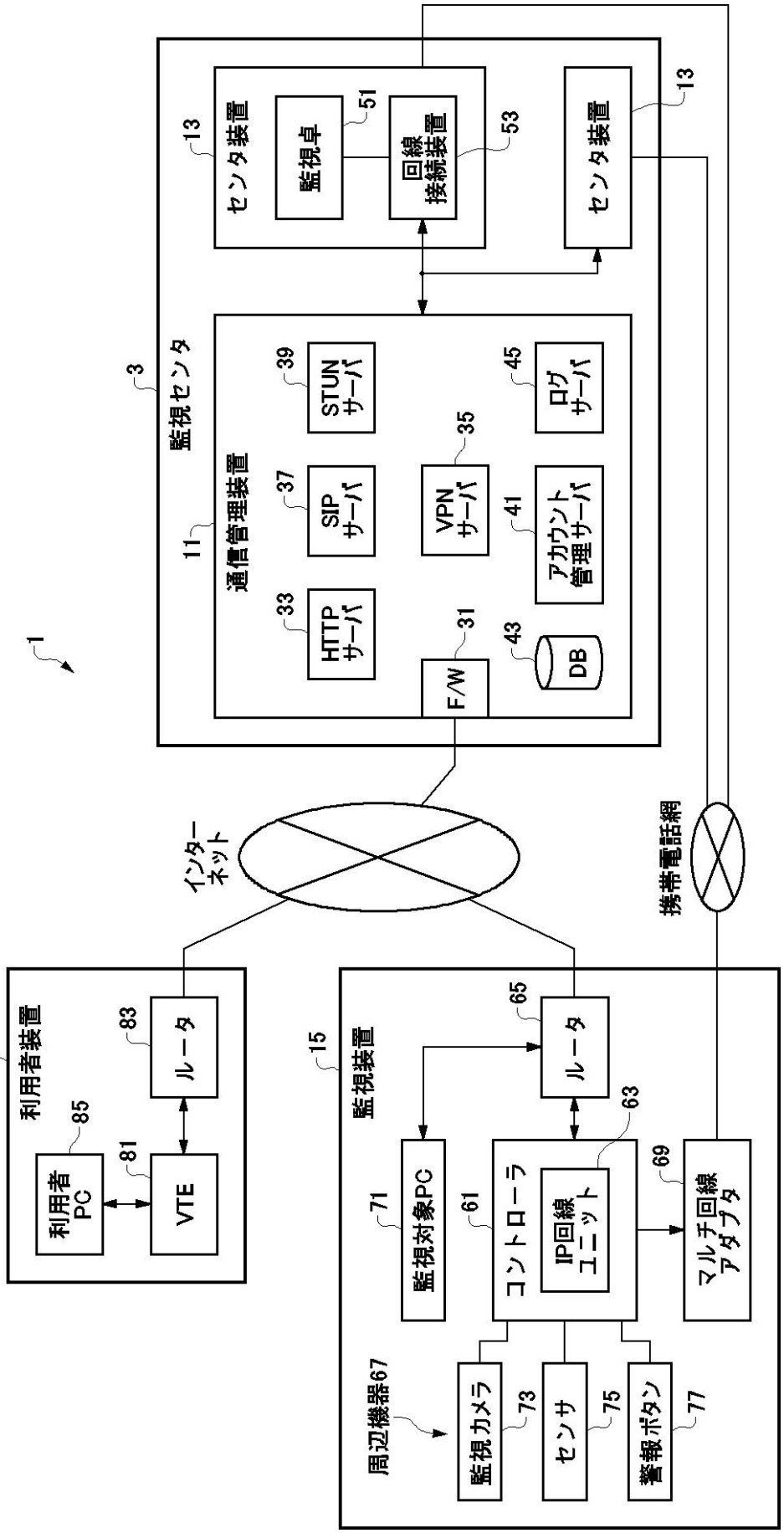
【０１０８】

１　監視システム
３　監視センタ
５　監視対象
７　利用者拠点
１１　通信管理装置
１３　センタ装置
１５　監視装置
１７　利用者装置
２１　センタ端末間ＶＰＮ
２３　ＳＩＰ通信
２５　端末間ＶＰＮ
３３　ＨＴＴＰサーバ
３５　ＶＰＮサーバ
３７　ＳＩＰサーバ
４１　アカウント管理サーバ
４３　データベース
６１　コントローラ
６３　ＩＰ回線ユニット
６５、８３　ルータ
６９　マルチ回線アダプタ
７３　監視カメラ
８１　ＶＰＮ終端装置（ＶＴＥ）
８５　利用者ＰＣ
１０１　認可情報記憶部
１０３　認可処理部

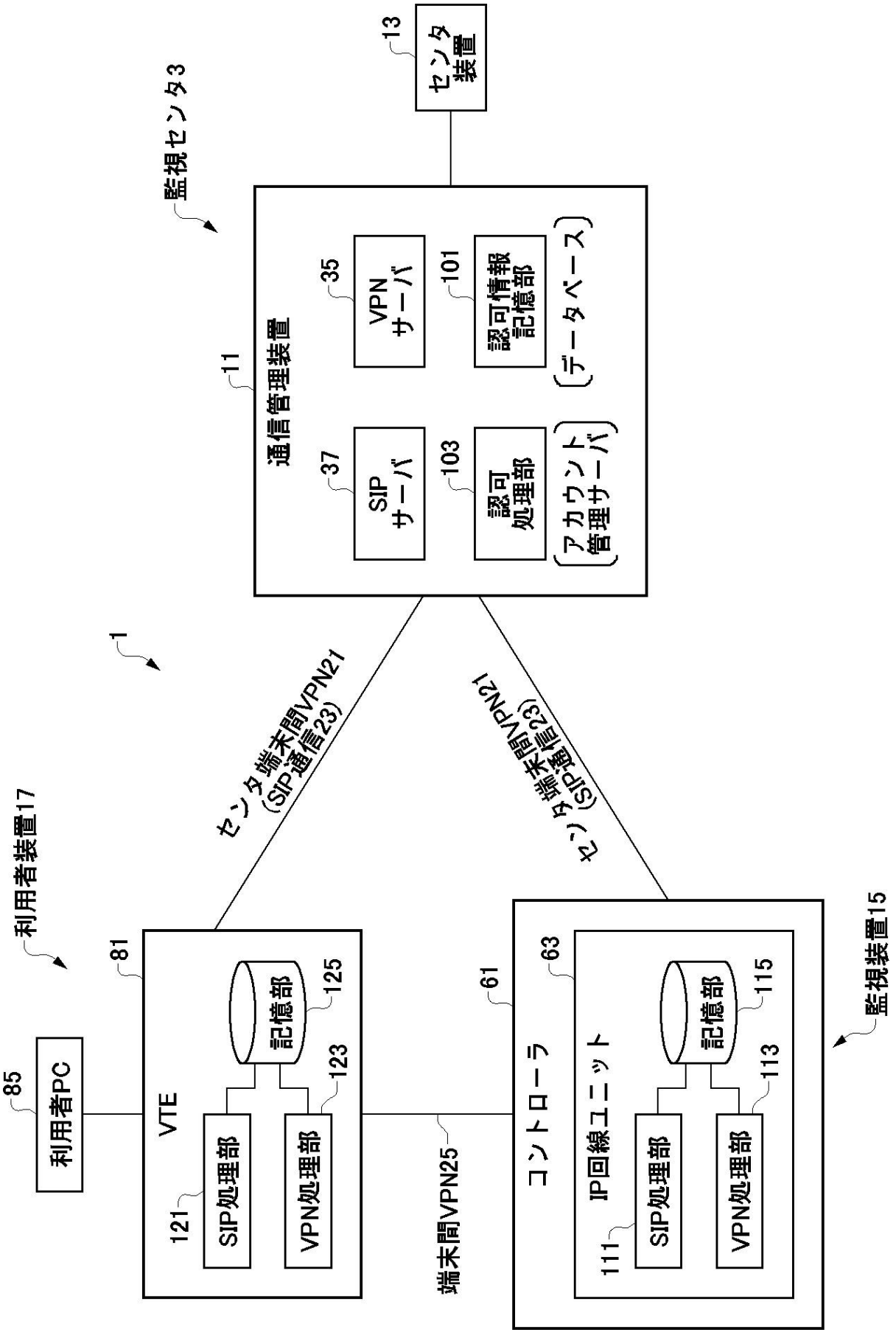
【図１】


1
3
監視センタ
11
通信管理装置
VPN
サーバ
SIP
サーバ
13
センタ
装置
13
センタ
装置
13
センタ
装置
インター
ネット
センタ端末間
VPN21
SIP通信
端末間
VPN25
SIP通信23
センタ端末間
VPN22
7
利用者拠点
17
利用者装置
VPN
クライアント
VPN
サーバ
5
監視対象
15
監視装置
VPN
クライアント
VPN
クライアント

【図２】


1
3
監視センタ
11
通信管理装置
13
センタ装置
51
監視卓
53
回線接続装置
13
センタ装置
39
STUN サーバ
45
ログ サーバ
37
SIP サーバ
35
VPN サーバ
41
アカウント管理サーバ
33
HTTP サーバ
31
F/W
43
DB
インターネット
携帯電話網
17
利用者装置
83
ルータ
85
利用者PC
81
VTE
15
監視装置
65
ルータ
63
71
監視対象PC
61
コントローラ
IP回線ユニット
69
マルチ回線アダプタ
周辺機器67
監視カメラ
73
センサ
75
警報ボタン
77

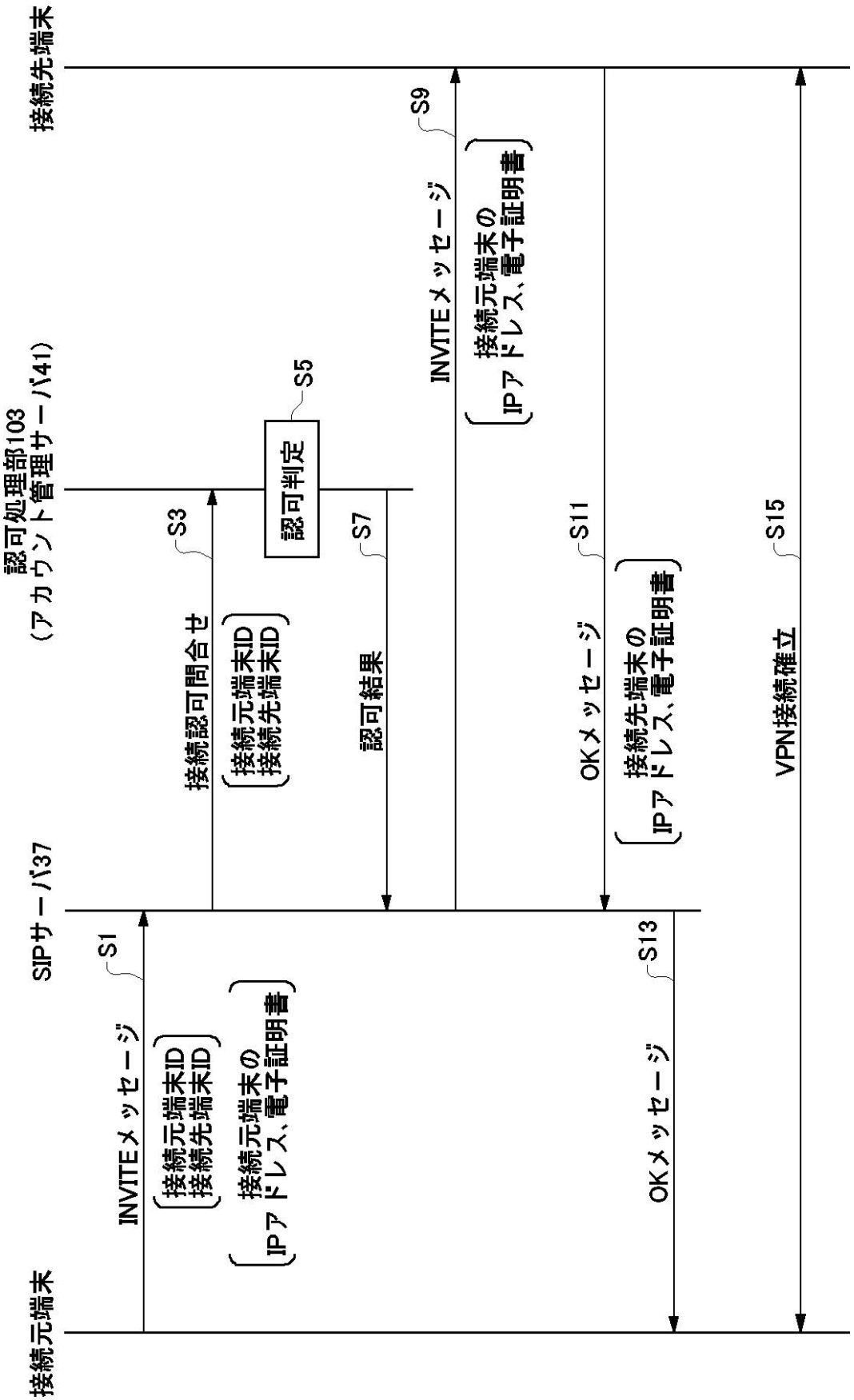
【図３】


監視センタ3
13
センタ装置
通信管理装置
11
35
VPN
サーバ
101
認可情報
記憶部
（データベース）
37
SIP
サーバ
103
認可
処理部
（アカウント
管理サーバ）
1
センタ端末間VPN21
（SIP通信23）
センタ端末間VPN21
（SIP通信23）
利用者装置17
81
VTE
記憶部
125
123
121
SIP処理部
VPN処理部
85
利用者PC
端末間VPN25
61
コントローラ
63
IP回線ユニット
記憶部
115
113
111
SIP処理部
VPN処理部
監視装置15

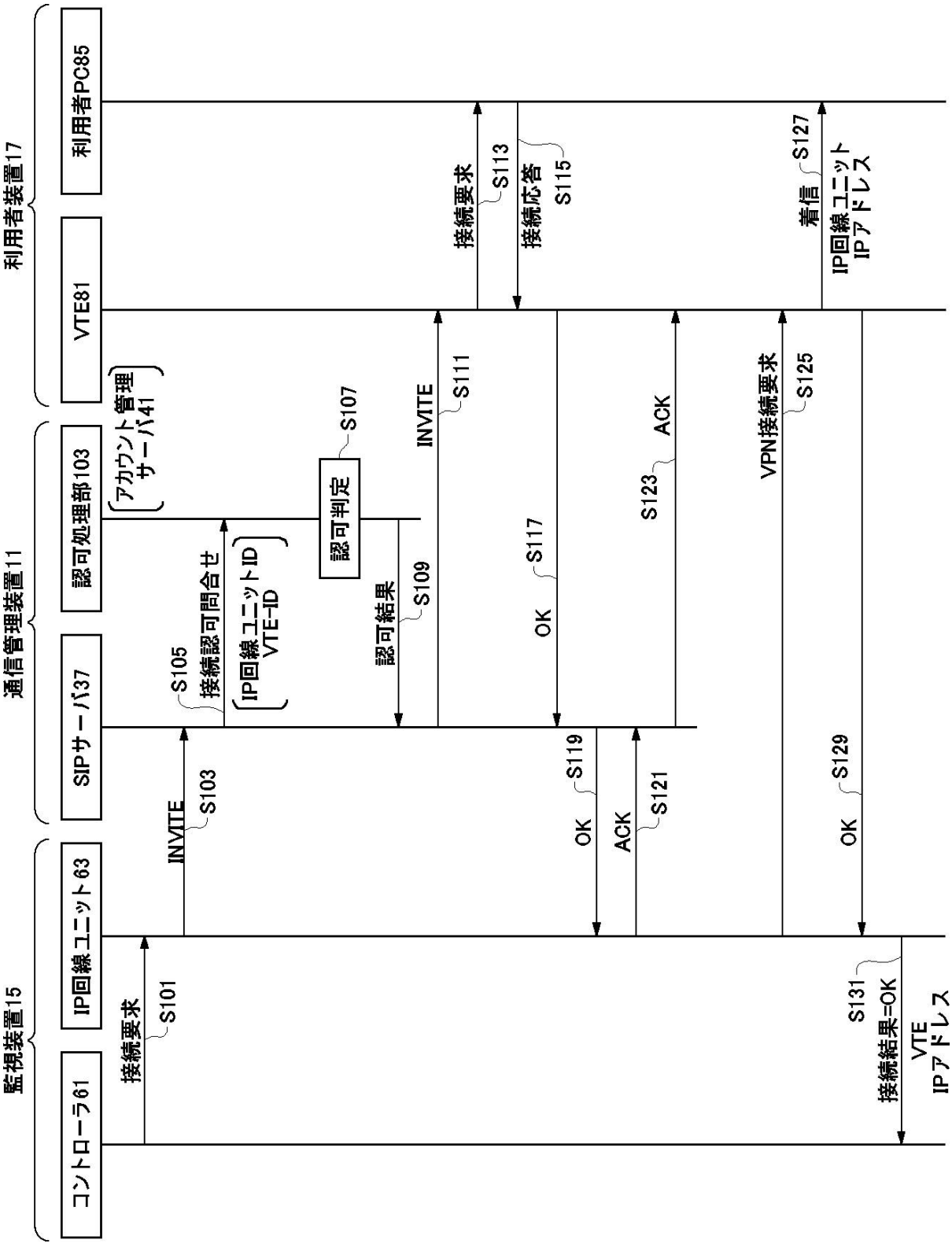
【図４】

利用者（オーナー）	端末ID	
	監視装置ID	利用者装置ID
A	A01	A11
B	B01	B11
C	C01	C11
C	C02	C11
⋮	⋮	⋮

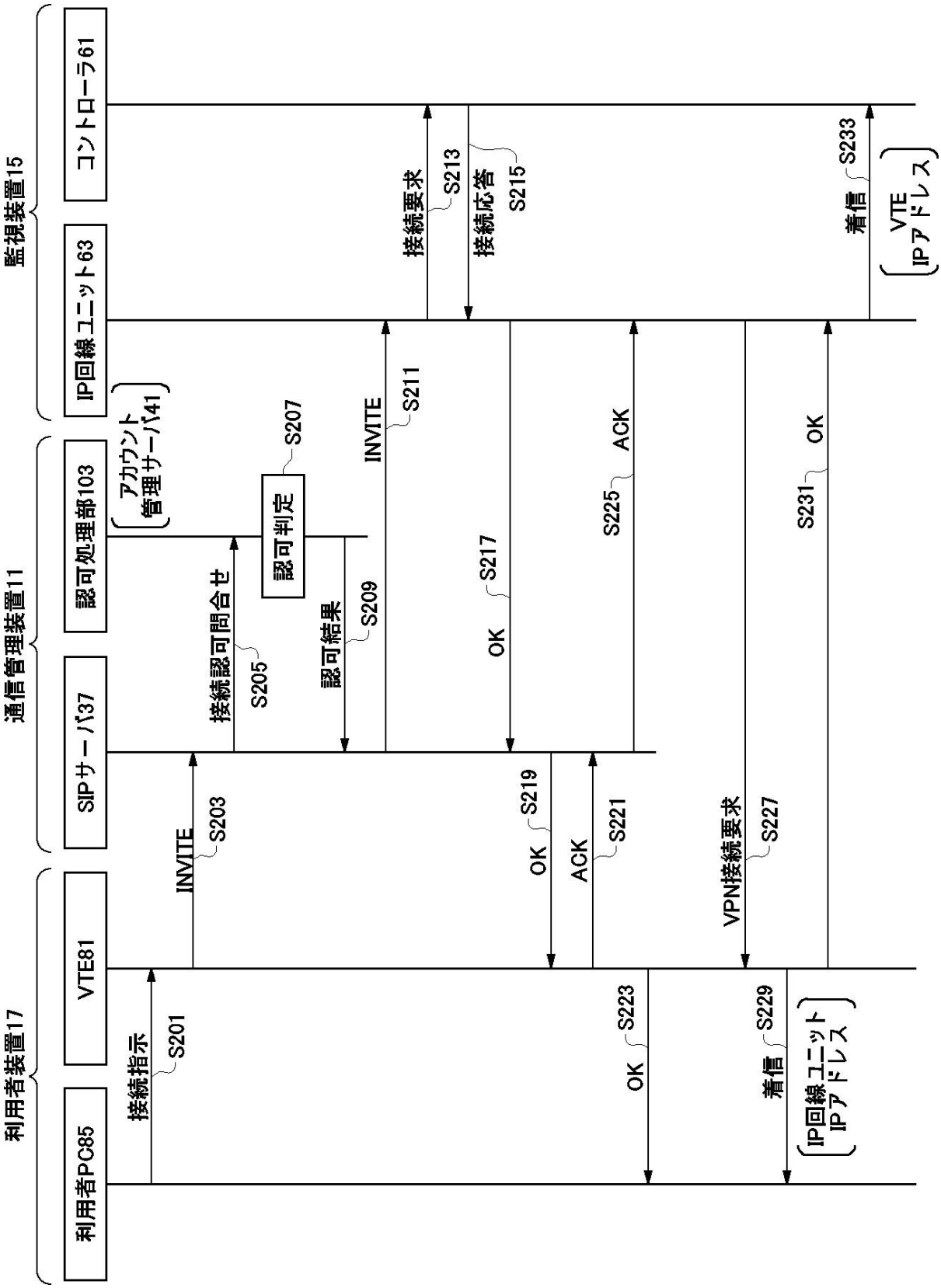
【図５】


接続元端末
SIPサーバ37
認可処理部103
（アカウント管理サーバ41）
接続先端末
S1
INVITEメッセージ
〔接続元端末ID
接続先端末ID〕
〔接続元端末の
IPアドレス、電子証明書〕
S3
接続認可問合せ
〔接続元端末ID
接続先端末ID〕
S5
認可判定
S7
認可結果
S9
INVITEメッセージ
〔接続元端末の
IPアドレス、電子証明書〕
S11
OKメッセージ
〔接続先端末の
IPアドレス、電子証明書〕
S13
OKメッセージ
S15
VPN接続確立

【図６】


監視装置15
通信管理装置11
利用者装置17
コントローラ61
IP回線ユニット63
SIPサーバ37
認可処理部103
VTE81
利用者PC85
アカウント管理サーバ41
接続要求
S101
INVITE
S103
S105
接続認可問合せ
IP回線ユニットID
VTE-ID
S107
認可判定
認可結果
S109
INVITE
S111
接続要求
S113
接続応答
S115
OK
S117
OK
S119
ACK
S121
ACK
S123
VPN接続要求
S125
着信
S127
IP回線ユニット
IPアドレス
OK
S129
S131
接続結果=OK
VTE
IPアドレス

【図７】


利用者装置17
通信管理装置11
監視装置15
利用者PC85
VTE81
SIPサーバ37
認可処理部103
IP回線ユニット63
コントローラ61
アカウント管理サーバ41
接続指示
S201
INVITE
S203
接続認可問合せ
S205
認可判定
S207
認可結果
S209
INVITE
S211
接続要求
S213
接続応答
S215
OK
S217
OK
S219
ACK
S221
ACK
S225
OK
S223
VPN接続要求
S227
着信
S229
IP回線ユニット IPアドレス
OK
S231
着信
S233
VTE IPアドレス

フロントページの続き

審査官　児玉　崇晶

(56)参考文献　特開２００９－０２７６５２（ＪＰ，Ａ）
特開２００７－１５８８６２（ＪＰ，Ａ）
特開２００１－０５４１０２（ＪＰ，Ａ）
特開２００８－２１９２３９（ＪＰ，Ａ）
特開２００５－２１０６７４（ＪＰ，Ａ）
水野　伸太郎　Shintaro　Mizuno，広帯域でセキュアな家庭ＬＡＮ間接続を実現するＶＰＮ接続方式，電子情報通信学会２００７年通信ソサイエティ大会講演論文集２　PROCEEDINGS OF THE 2007 IEICE COMMUNICATIONS SOCIETY CONFERENCE，日本，社団法人電子情報通信学会　THE INSTITUTE OF ELECTRONICS,INFORMATION AND COMMUNICATION ENGINEERS，２００７年　８月２９日，pp.S-47～S48
加藤　淳也　Jun-ya　Kato，ＳＩＰモビリティを用いた移動対応ＶＰＮ方式の実装と評価　Implementation and Evaluation of a Remote VPN Method with SIP Mobility，電子情報通信学会技術研究報告 IEICE Technical Report，日本，社団法人電子情報通信学会　The Institute of Electronics,Information and Communication Engineers，２００８年　２月２８日，Ｖｏｌ．１０７　Ｎｏ．５２５，pp.277-282
加藤　淳也　Jun-ya　Kato，端末とＶＰＮゲートウェイ間に介在する代理装置を用いたＶＰＮ接続の中継方式の検討　A relay method for VPN connection with a proxy-box intervening between user device and VPN gateway，電子情報通信学会技術研究報告 IEICE Technical Report，日本，社団法人電子情報通信学会　The Institute of Electronics,Information and Communication Engineers，２００８年　９月　４日，Ｖｏｌ．１０８　Ｎｏ．２０４，pp.87-92

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／２０
Ｈ０４Ｎ　７／１８