(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2010 年 10 月 14 日(14.10.2010)

PCT

(10) 国際公開番号
WO 2010/116642 A1

(51) 国際特許分類:
G06F 21/20 (2006.01) *H04N 7/18* (2006.01)

(21) 国際出願番号: PCT/JP2010/002119

(22) 国際出願日: 2010 年 3 月 25 日(25.03.2010)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願 2009-081307 2009 年 3 月 30 日(30.03.2009) JP

(71) 出願人 (米国を除く全ての指定国について): セコム株式会社 (SECOM CO., LTD.) [JP/JP]; 〒1500001 東京都渋谷区神宮前１丁目５番１号 Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 藤沢正幸 (FUJISAWA, Masayuki) [JP/JP]; 〒1810013 東京都三鷹市下連雀６－１１－２３ セコム株式会社内 Tokyo (JP).

(74) 代理人: 大野聖二, 外 (OHNO, Seiji et al.); 〒1000005 東京都千代田区丸の内１丁目６番５号 丸の内北口ビル２１階 大野総合法律事務所 Tokyo (JP).

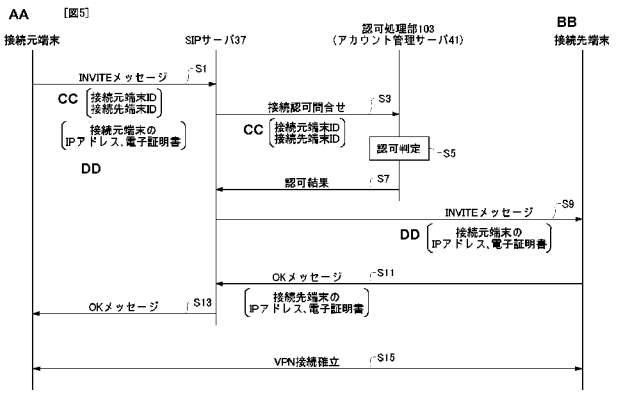
(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[続葉有]

(54) **Title**: MONITORING SYSTEM AND COMMUNICATION MANAGEMENT DEVICE

(54) 発明の名称 : 監視システムおよび通信管理装置



37 SIP SERVER
41 ACCOUNT MANAGEMENT SERVER
103 PERMISSION PROCESSING UNIT
S1 INVITE MESSAGE
S3 CONNECTION PERMISSION INQUIRY
S5 PERMISSION DETERMINATION
S7 PERMISSION RESULT
S9 INVITE MESSAGE
S11 OK MESSAGE
S13 OK MESSAGE
S15 VPN CONNECTION ESTABLISHMENT
AA CONNECTION SOURCE TERMINAL
BB CONNECTION DESTINATION TERMINAL
CC CONNECTION SOURCE TERMINAL ID, CONNECTION DESTINATION TERMINAL ID
DD IP ADDRESS AND ELECTRONIC CERTIFICATE OF CONNECTION SOURCE TERMINAL

(57) **Abstract**: A communication management device (11) is connected to a plurality of terminals. The plurality of terminals are a monitoring device (15) and a user device (17). When communication between terminals is performed, a connection source terminal transmits an invitation message of SIP to the communication management device (11). The communication management device (11) is provided with a permission information storage unit (101) which stores connection permission information storing a combination of terminals which should be permitted for connection, in addition to the SIP server (37); and a permission processing unit (103) which permits a connection between terminals with reference to the connection permission information. When the SIP server (37) acquires the invitation message from the connection source terminal, if the permission processing unit (103) permits the connection between the connection source and connection destination terminals, the SIP server (37) supplies the invitation message from the connection source terminal to the connection destination terminal. Thereby, a monitoring system capable of improving the security when applying the SIP to the monitoring system is provided.

(57) 要約:

[続葉有]

WO 2010/116642 A1

添付公開書類:

— 国際調査報告（条約第 21 条(3)）

— 補正された請求の範囲（条約第 19 条(1)）

通信管理装置（１１）は、複数の端末と接続される。複数の端末は、監視装置（１５）及び利用者装置（１７）である。端末間の通信を行うとき、接続元の端末が、ＳＩＰの招待メッセージを通信管理装置（１１）に送信する。通信管理装置（１１）には、ＳＩＰサーバ（３７）に加え、接続が認可されるべき端末の組合せを記憶した接続認可情報を記憶した認可情報記憶部（１０１）と、接続認可情報を参照して端末間の接続を認可する認可処理部（１０３）とが備えられる。ＳＩＰサーバ（３７）が接続元の端末から招待メッセージを取得したとき、認可処理部（１０３）が接続元及び接続先の端末の接続を認可した場合に、ＳＩＰサーバ（３７）が接続元の端末からの招待メッセージを接続先の端末へ供給する。これにより、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が提供される。

明　細　書

発明の名称 ： 監視システムおよび通信管理装置

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、通信可能に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。

[0005] 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。

[0006] 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

れたと仮定する。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。

[0007] 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。

先行技術文献

特許文献

[0008] 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

[0009] 本発明は、上記背景の下でなされたものである。本発明の目的は、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] 本発明の一の態様は、監視システムであり、この監視システムは、監視情報を通信する複数の端末と、複数の端末の通信を管理する通信管理装置と、を有し、複数の端末の各々が、監視対象側又は監視対象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監視システムであって、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通信管理装置に送信するように構成され、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、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、ＳＩＰサーバは、接続元の端末から招待メッセージを取得したとき、招待メッセージに含まれる接続先の端末の識別情報を認可処理部に供給し、認可処理部が端末間の接続を認可した場合に、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へ供給する。

[0011] 本発明の別の態様は、通信管理装置であり、この通信管理装置は、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、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、ＳＩＰサーバが、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、認可処理部が、招待メッセージに含まれる接続先の端末の識別情報に基づき、端末間の接続を認可するか否かを判定し、認可処理部が接続を認可した場合に、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へ供給する。

[0012] 以下に説明するように、本発明には他の態様が存在する。したがって、この発明の開示は、本発明の一部の態様の提供を意図しており、ここで記述され請求される発明の範囲を制限することは意図していない。

図面の簡単な説明

[0013] [図1]図１は、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]図２は、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]図３は、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]図４は、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]図５は、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]図６は、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]図７は、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

[0014] 以下に本発明の詳細な説明を述べる。ただし、以下の詳細な説明と添付の図面は発明を限定するものではない。

[0015] 本発明は、監視情報を通信する複数の端末と、複数の端末の通信を管理する通信管理装置を有し、複数の端末の各々が、監視対象側又は監視対象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監視システムであって、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通信管理装置に送信するように構成され、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、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、ＳＩＰサーバは、接続元の端末から招待メッセージを取得したとき、招待メッセージに含まれる接続先の端末の識別情報を認可処理部に供給し、認可処理部が端末間の接続を認可した場合に、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へ供給する。

[0016] 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。

[0017] 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。

[0018] 接続先の端末は、招待メッセージを通信管理装置から受信したときにＳＩＰのＯＫメッセージを通信管理装置に送信してよく、招待メッセージ及びＯＫメッセージには、ＳＩＰセッション確立後に接続元及び接続先の端末間で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。

[0019] 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。

[0020] 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。

[0021] 招待メッセージは、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メッセージは、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。

[0022] 通信管理装置は、複数の端末との通信を利用して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。

[0023] 通信管理装置と複数の端末との接続は、通信管理装置と複数の端末間にＶＰＮを構築したセンタ端末間ＶＰＮにより接続されてよく、ＳＩＰサーバは、センタ端末間ＶＰＮ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。

[0024] 監視情報は、監視対象で撮影された画像、監視対象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。

[0025] 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る。この通信管理装置は、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、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、ＳＩＰサーバが、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、認可処理部が、招待メッセージに含まれる接続先の端末の識別情報に基づき、端末間の接続を認可するか否かを判定し、認可処理部が接続を認可した場合に、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。

[0026] 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。

[0027] 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。

[0028] 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。

[0029] 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。

[0030] 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。

[0031] 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。

[0032] 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。

[0033] 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。

[0034] 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。

[0035] 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。

[0036] 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。

[0037] 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。

[0038] 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。

[0039] 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。

[0040] 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。

[0041] 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。

[0042] 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。

[0043] 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。

[0044] 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。

[0045] 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。

[0046] 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。

[0047] 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。

[0048] ＳＴＵＮサーバ３９は、監視装置１５及び利用者装置１７のルータのＮＡ

Ｔ機能に対応するためにＳＴＵＮ機能を提供する。

[0049] 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。

[0050] 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。

[0051] 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。

[0052] 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。

[0053] 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。

[0054] 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。

[0055] 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。

[0056] 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。

[0057] 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。

[0058] 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。

[0059] 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。

[0060] 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。

[0061] 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。

[0062] 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。

[0063] 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。

[0064] 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。

[0065] 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。

[0066] 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。

[0067] 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。

[0068] 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。

[0069] 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。

[0070] 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。

[0071] 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。

[0072] 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。

[0073] 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。

[0074] 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。

[0075] 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。

[0076] 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。

[0077] 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。

[0078] 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。

[0079] 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）。

[0080] 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。

[0081] 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。

[0082] 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。

[0083] 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。

[0084] 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。

[0085] 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ＶＴＥ８１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。

[0086] 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。

[0087] 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）。

[0088] 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。

[0089] 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）。

[0090] 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。

[0091] 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。

[0092] 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。

[0093] 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。

[0094] 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。

[0095] 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。

[0096] 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）。

[0097] 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。

[0098] 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）。

[0099] 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。

[0100] 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。

[0101] 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。

[0102] 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。

[0103] 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。

[0104] 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。

[0105] また、本発明によれば、通信管理装置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の適用によりセキュリティ性を高くできる。

[0106] 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。

[0107] 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。

[0108] 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。

[0109] 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。

[0110] 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。

[0111] 以上に現時点で考えられる本発明の好適な実施の形態を説明したが、本実施の形態に対して多様な変形が可能なことが理解され、そして、本発明の真実の精神と範囲内にあるそのようなすべての変形を添付の請求の範囲が含むことが意図されている。

産業上の利用可能性

[0112] 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

[0113] 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

請求の範囲

[請求項1] 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と、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ことを特徴とする監視システム。

[請求項2] 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ＳＩＰ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請求項１に記載の監視システム。

[請求項3] 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２に記載の監視システム。

[請求項4] 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３に記載の監視システム。

[請求項5] 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により接続されており、

前記ＳＩＰサーバは、前記センタ端末間ＶＰＮを介して前記複数の端末とＳＩＰメッセージを通信す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6] 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１～５のいずれかに記載の監視システム。

[請求項7] 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、

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とを特徴とする通信管理装置。

補正された請求の範囲
[2010年7月5日(05.07.2010)国際事務局受理]

[請求項1] （補正後） 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することを特徴とする監視システム。

[請求項2] 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ＳＩＰ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請求項1に記載の監視システム。

[請求項３] 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２に記載の監視システム。

[請求項４] 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３に記載の監視システム。

[請求項５] 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に記載の監視システム。

[請求項６] 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１～５のいずれかに記載の監視システム。

[請求項７] （補正後） 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の通信を管理する通信管理装置であって、

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、

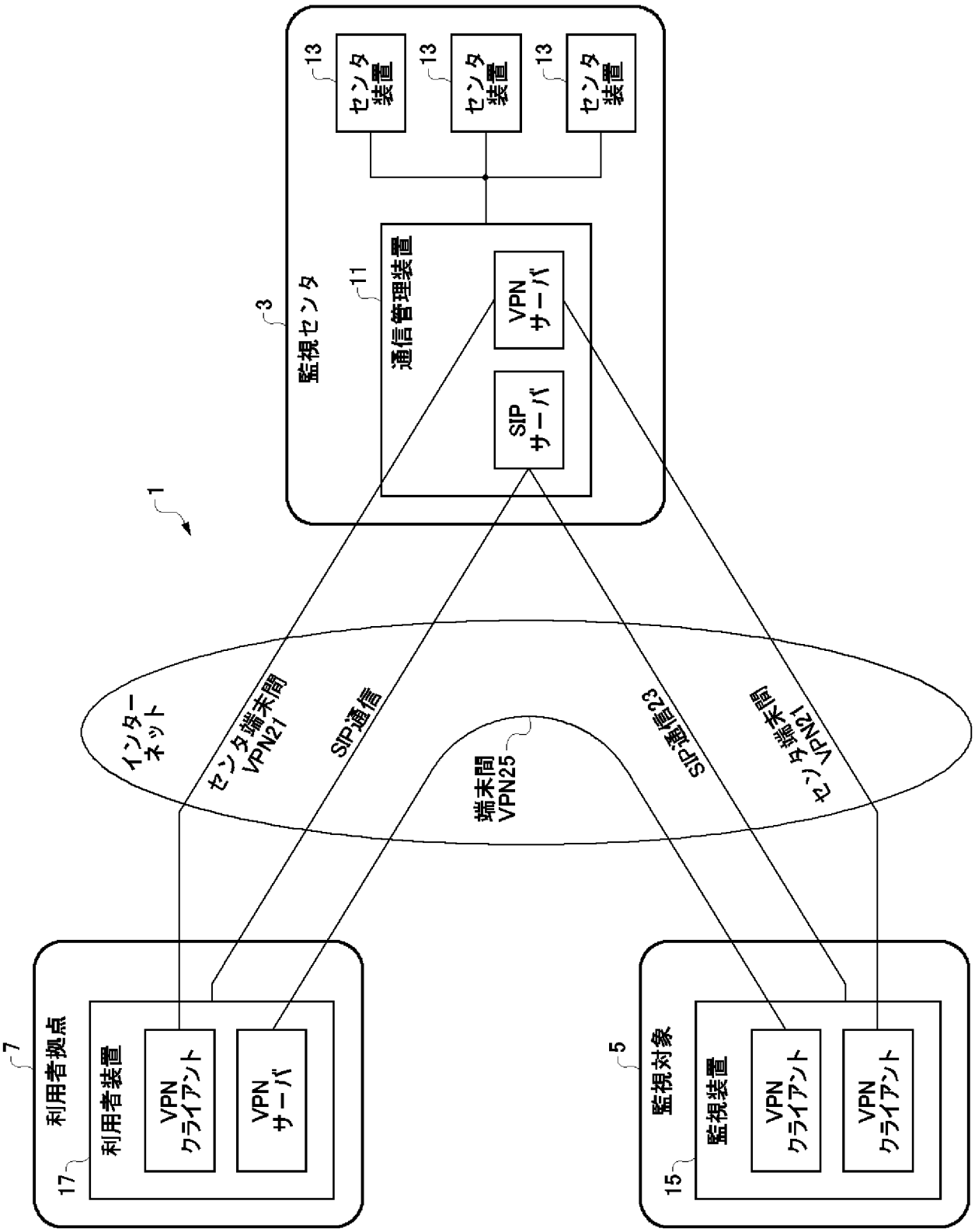
前記接続認可情報を参照して監視対象側の端末と利用者側の端末との接続を認可するか否かを判定する認可処理部と、を有し、

前記ＳＩＰサーバが、前記監視対象側の端末又は利用者側の端末の一方から他方へ宛てた識別情報を含むＳＩＰの招待メッセージを取得し

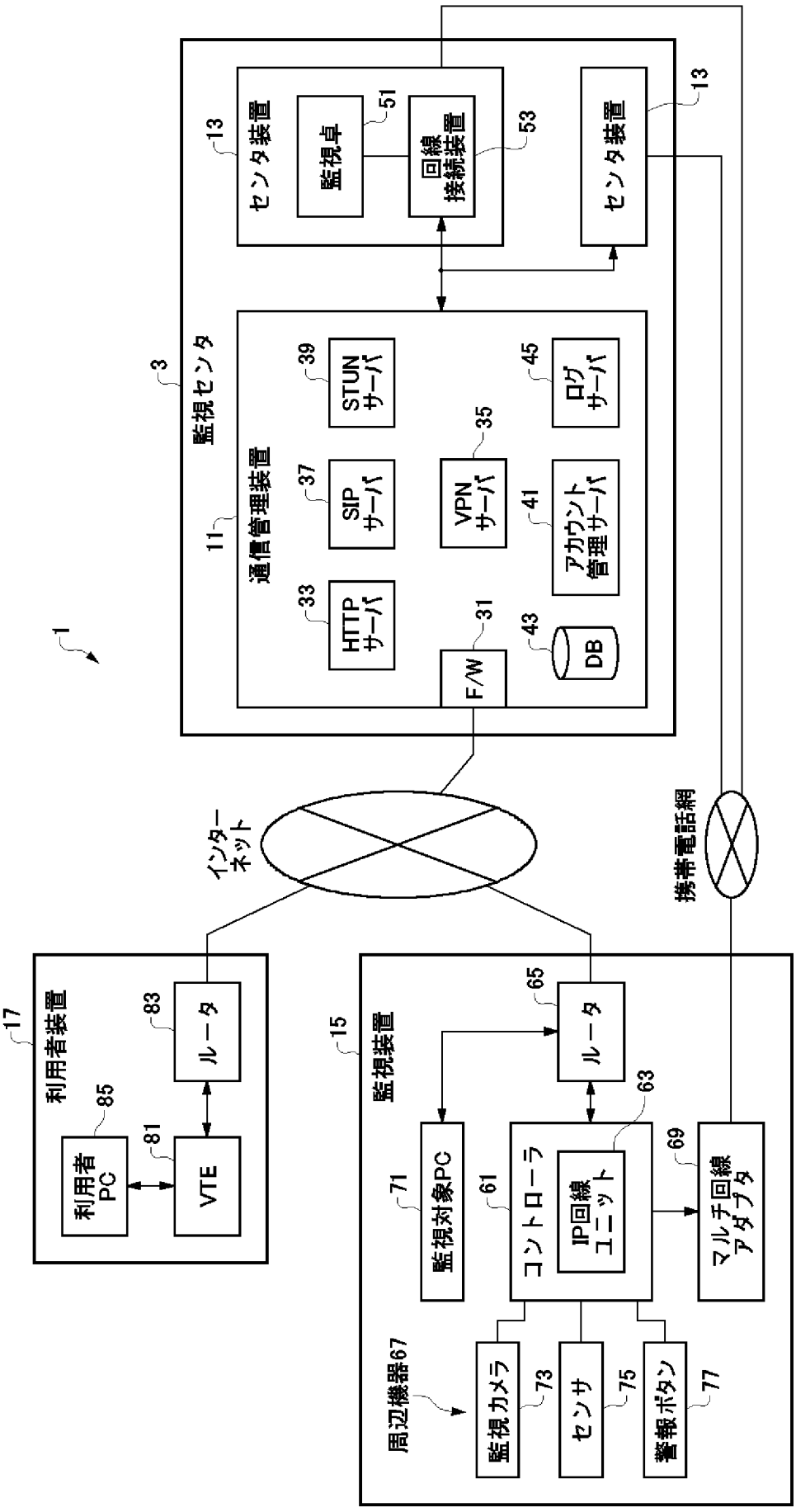
たとき、前記認可処理部が、前記招待メッセージに含まれる前記接続先の端末の識別情報に基づき、前記監視対象側の端末と利用者側の端末との接続を認可するか否かを判定し、

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とを特徴とする通信管理装置。

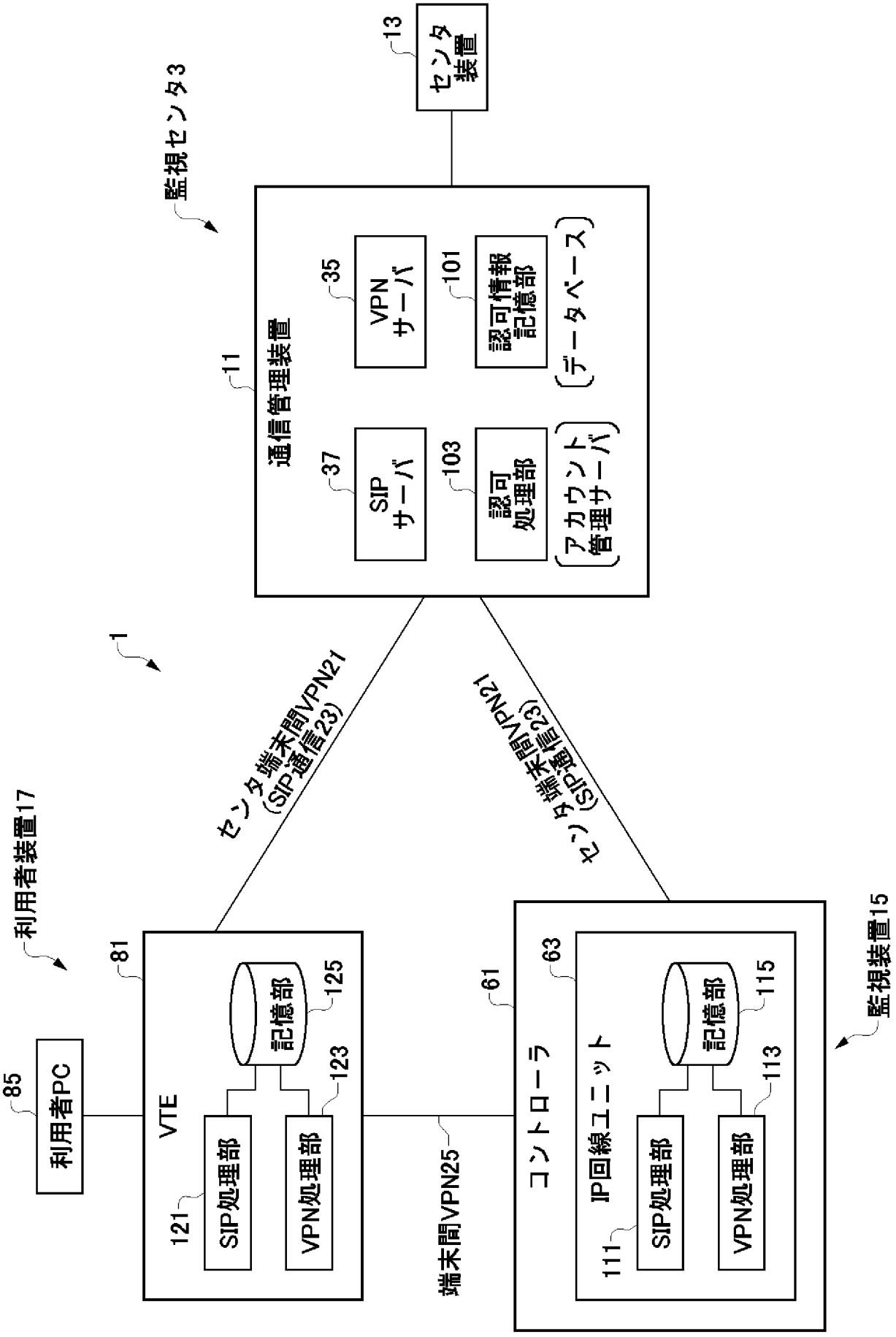
[図1]


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
VPN21
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
監視卓
51
回線接続装置
53
センタ装置
13
39
STUN サーバ
45
ログサーバ
35
37
SIP サーバ
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

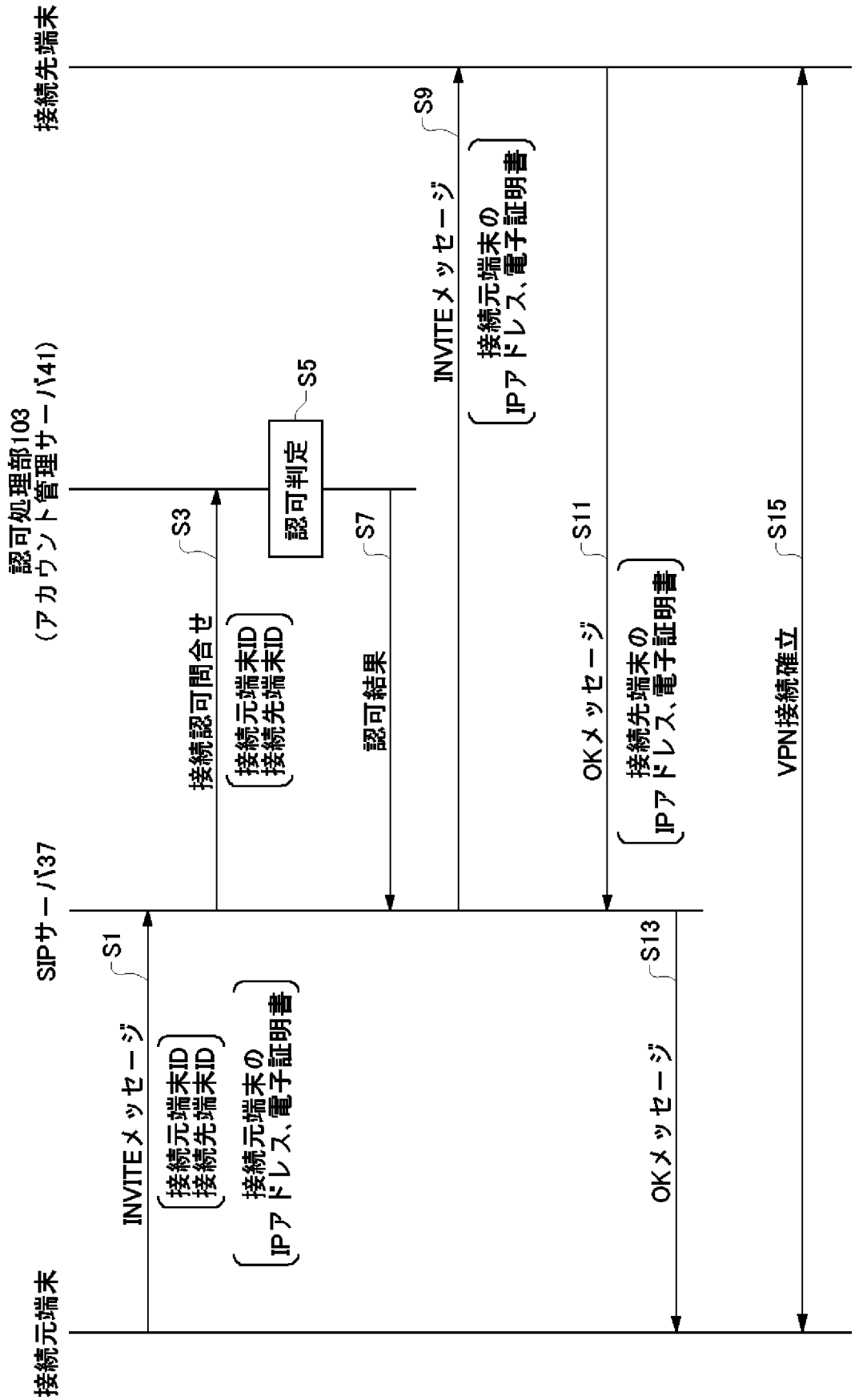
[図3]


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

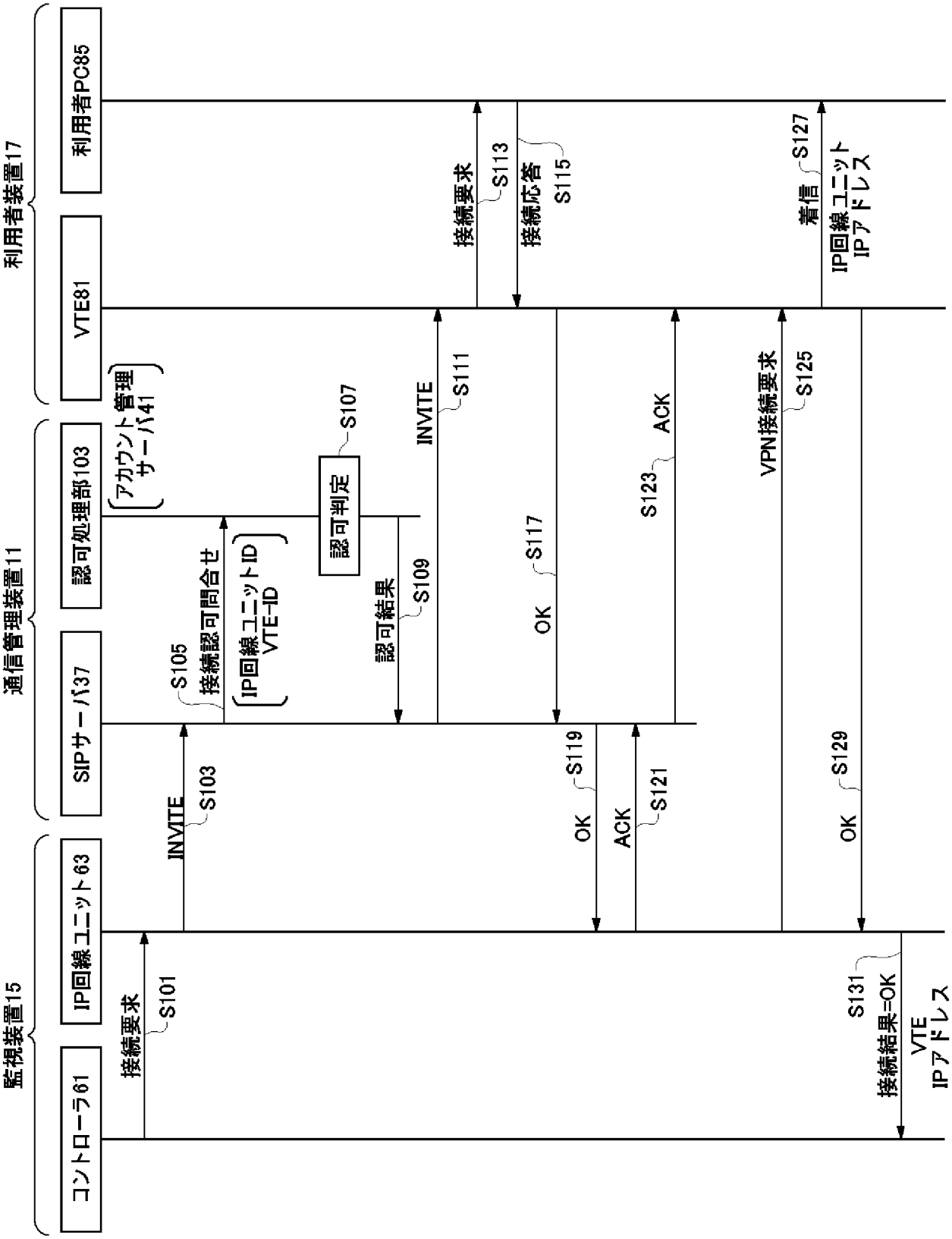
[図4]

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
⋮	⋮	⋮

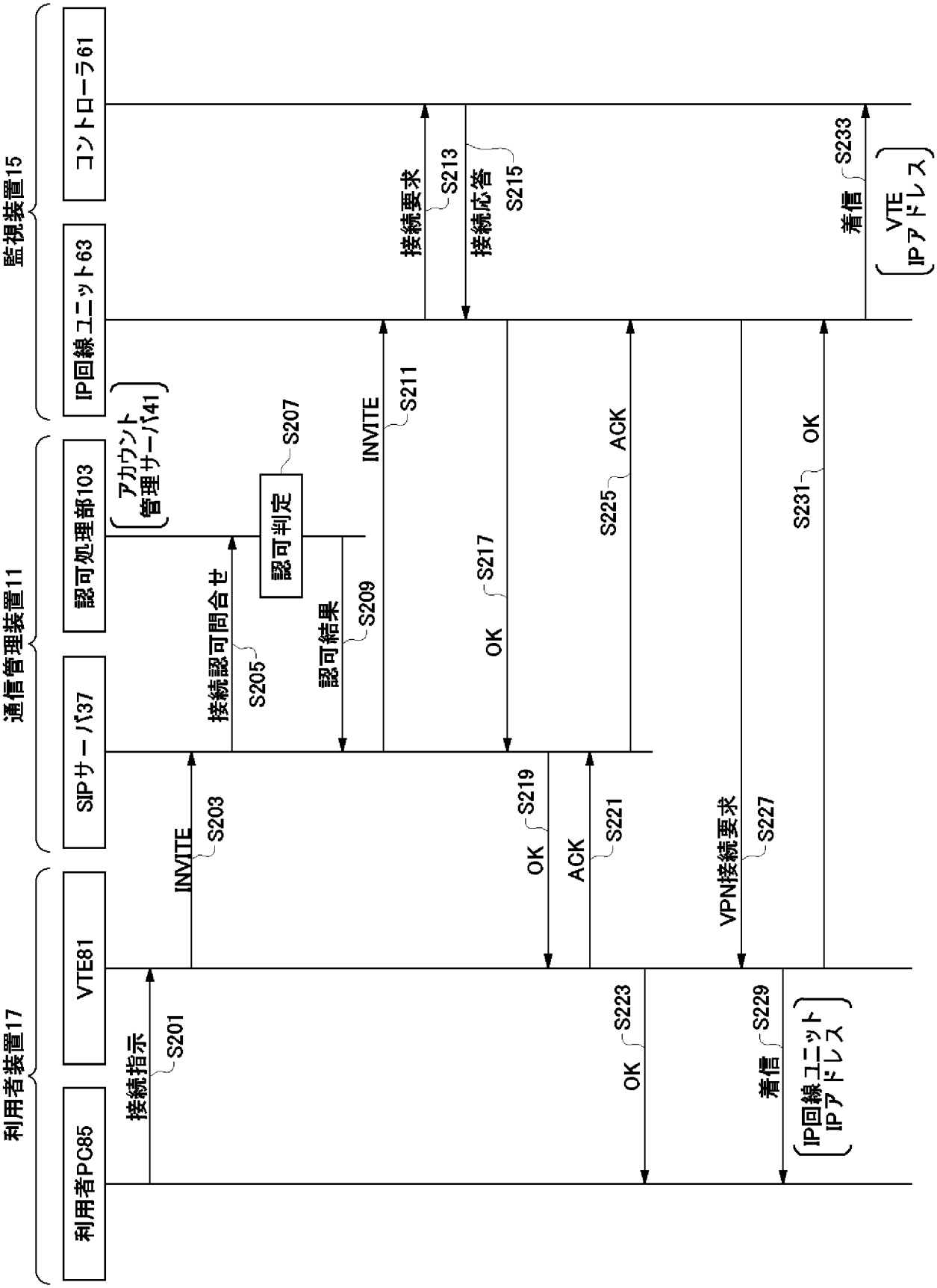
[図5]


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
認可判定
S107
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
利用者PC85
VTE81
通信管理装置11
SIPサーバ37
認可処理部103
アカウント管理サーバ41
監視装置15
IP回線ユニット63
コントローラ61
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

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2010/002119

A. CLASSIFICATION OF SUBJECT MATTER
G06F21/20(2006.01)i, *H04N7/18*(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F21/20, H04N7/18

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2010
Kokai Jitsuyo Shinan Koho	1971-2010	Toroku Jitsuyo Shinan Koho	1994-2010

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2009-27652 A (Nippon Telegraph And Telephone Corp.), 05 February 2009 (05.02.2009), paragraphs [0067] to [0078] (Family: none)	1-7
Y	JP 2008-219239 A (Yamaha Corp.), 18 September 2008 (18.09.2008), paragraph [0017] (Family: none)	1-7
Y	JP 2001-54102 A (Secom Co., Ltd.), 23 February 2001 (23.02.2001), claim 1 (Family: none)	1-7

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
13 May, 2010 (13.05.10)	25 May, 2010 (25.05.10)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１０／００２１１９

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　G06F21/20(2006.01)i, H04N7/18(2006.01)i

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.　G06F21/20, H04N7/18

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２０１０年
日本国実用新案登録公報	１９９６－２０１０年
日本国登録実用新案公報	１９９４－２０１０年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
Y	JP 2009-27652 A（日本電信電話株式会社）2009.02.05,　【００６７】－【００７８】段落（ファミリーなし）	1-7
Y	JP 2008-219239 A（ヤマハ株式会社）2008.09.18,　【００１７】段落（ファミリーなし）	1-7
Y	JP 2001-54102 A（セコム株式会社）2001.02.23,　請求項１（ファミリーなし）	1-7

☐　Ｃ欄の続きにも文献が列挙されている。

☐　パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー

「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの

「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「Ｏ」口頭による開示、使用、展示等に言及する文献

「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献

「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「＆」同一パテントファミリー文献

国際調査を完了した日 １３．０５．２０１０	国際調査報告の発送日 ２５．０５．２０１０
国際調査機関の名称及びあて先 日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員）　５Ｓ　３６５１ 児玉　崇晶 電話番号　０３－３５８１－１１０１　内線　３５４６