(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 102378982 B
(45)授权公告日 2015.05.27

(21)申请号 201080014851.1
(22)申请日 2010.03.25
(30)优先权数据
2009-081307 2009.03.30 JP
(85)PCT国际申请进入国家阶段日
2011.09.30
(86)PCT国际申请的申请数据
PCT/JP2010/002119 2010.03.25
(87)PCT国际申请的公布数据
WO2010/116642 JA 2010.10.14
(73)专利权人 西科姆株式会社
地址 日本东京
(72)发明人 藤沢正幸
(74)专利代理机构 中原信达知识产权代理有限责任公司 11219
代理人 关兆辉 穆德骏
(51)Int.Cl.
G06F 21/60(2013.01)
(56)对比文件
CN 1717913 A,2006.01.04, 说明书第2页第22行至第3页第3行,说明书第4页第13行至第7页第12行、附图1-3.
审查员 唐楹琰

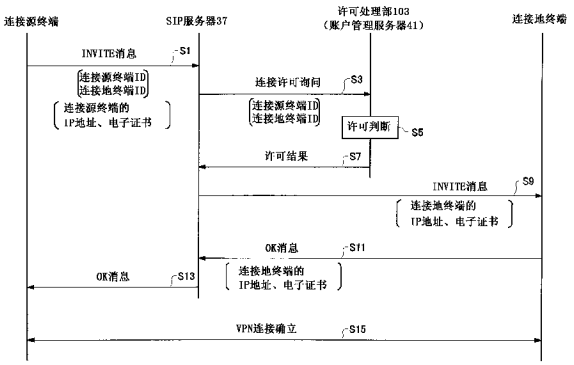
权利要求书1页 说明书12页 附图7页

(54)发明名称

监视系统及通信管理装置

(57)摘要

通信管理装置(11)连接到多个终端。多个终端是监视装置(15)和使用者装置(17)。当进行终端间的通信时,连接源终端将SIP的邀请消息发送到通信管理装置(11)。通信管理装置(11)中除了SIP服务器(37)之外还具有:许可信息存储部(101),存储了连接许可信息,该连接许可信息中存储了连接应被许可的终端的组合;和许可处理部(103),参照连接许可信息来许可终端间的连接。当SIP服务器(37)从连接源终端取得邀请消息时,在许可处理部(103)许可了连接源和连接地的终端的连接的情况下,SIP服务器(37)将来自连接源终端的邀请消息提供到连接地终端。由此,提供一种能够提高将SIP适用于监视系统时的安全性的监视系统。



CN 102378982 B

1. 一种监视系统，具有：设置于监视对象的监视对象侧终端；设置于使用者一侧的使用者侧终端，使用从上述监视对象侧终端接收的上述监视信息；和管理上述监视对象侧终端和上述使用者侧终端的通信的通信管理装置，上述监视系统的特征在于，

上述监视对象侧终端具有取得上述监视对象的上述监视信息并发送到上述使用者侧终端的功能，

上述使用者侧终端具有使用从上述监视对象侧终端接收的上述监视信息进行上述监视对象的监视的功能，

上述监视系统构成为：当上述监视对象侧终端或上述使用者侧终端的一方向另一方请求连接时，该连接源终端将包括自身的 IP 地址和电子证书以及连接地终端的识别信息在内的 SIP 的邀请消息发送到上述通信管理装置，上述监视对象侧终端和上述使用者侧终端作为相互具有不同功能的终端的组；

上述通信管理装置具有：SIP 服务器；

许可信息存储部，存储用于表示连接应被许可的作为相互具有不同功能的终端的组的监视对象侧终端和使用者侧终端的对应组合的连接许可信息；和

许可处理部，参照上述连接许可信息来判断是否许可监视对象侧终端和使用者侧终端间的连接，

上述 SIP 服务器，从上述连接源终端取得上述邀请消息时，将上述邀请消息中包含的上述连接地终端的识别信息提供到上述许可处理部，当上述许可处理部许可了监视对象侧终端和使用者侧终端间的连接时，上述 SIP 服务器将来自上述连接源终端的邀请消息提供到上述连接地终端，

上述连接地终端从上述通信管理装置接收到上述邀请消息时，将包含自身的 IP 地址和电子证书的 SIP 的 OK 消息发送到上述通信管理装置，

上述连接源和连接地的终端使用在上述邀请消息和上述 OK 消息中交换的各终端的 IP 地址和电子证书，在 SIP 会话确立后在上述连接源和连接地的终端间确立不介入上述通信管理装置的终端间连接。

2. 根据权利要求 1 所述的监视系统，其特征在于，

不介入上述通信管理装置的终端间连接是在终端间构筑 VPN 而进行连接的终端间 VPN。

3. 根据权利要求 1 所述的监视系统，其特征在于，

上述通信管理装置和上述监视对象侧终端或使用者侧终端之间的连接，通过在上述通信管理装置和上述监视对象侧终端或使用者侧终端间构筑了 VPN 的中心终端间 VPN 进行连接，

上述 SIP 服务器通过上述中心终端间 VPN 与上述监视对象侧终端或使用者侧终端进行 SIP 消息的通信。

4. 根据权利要求 1 ～ 3 的任意一项所述的监视系统，其特征在于，

上述监视信息包括由上述监视对象拍摄的图像、由上述监视对象检测出的监视信号和由上述使用者一侧生成的控制信息中的至少一个。

监视系统及通信管理装置

技术领域

[0001] 本发明涉及一种监视系统，其中监视对象的终端和使用者一侧的终端互相连接并能够通信，上述监视对象的终端取得监视信息，上述使用者一侧的终端获得监视信息并使用。

背景技术

[0002] 现有技术中，对店铺、工厂等监视对象设置监视照相机从而远程监视影像的监视系统已经实用化。监视影像发送到远程的监视中心，并发送到监视对象的所有者（主人）的办公室。监视影像的发送使用 ISDN 等普通公用线路（例如专利文献 1）。

[0003] 近年来，因 ADSL、FTTH 这样的宽带线路的普及，在因特网上实现收发监视系统中的监视影像等的需求增大。通过利用因特网有助于节约成本、提高系统灵活性。

[0004] 作为在因特网上传送声音、影像的技术，称为 SIP(Session Initiation Protocol：会话发起协议）的协议为人所知。SIP 适用于 IP 电话、电视会议等。为了通过 SIP 连接两个地点，在 SIP 服务器中注册各地点的地址。这样一来，在注册了地址的地点之间可进行 SIP 的通信。

[0005] 但是如果将 SIP 适用于监视系统则要考虑安全性的问题。即，在从外部对监视对象的影像等进行监视的监视系统中要求较高的安全性。与之相对，在 SIP 中，通过注册地址可连接任意的地点。因此，从安全性的角度出发不希望直接将 SIP 适用于监视系统。

[0006] 例如，假设监视对象是店铺，多个店铺的终端连接到监视中心。监视中心也连接到各店铺的店主的终端。此时，可连接到各店铺的终端的应仅限于对应的店主的终端。

[0007] 但是在现有的 SIP 中，在 SIP 服务器中注册了地址的任意的终端之间可进行连接。作为基本的认证功能，SIP 服务器可进行密码及 ID 的认证。但这仅限于终端和 SIP 服务器之间的认证。如果许可了终端和 SIP 服务器的连接，则无法限制经由 SIP 服务器的终端之间的组合。所以也无法限制店铺的终端和店主终端间的连接。因此，店主有可能获得自己之外的店铺的监视信息。

[0008] 专利文献 1：日本特开 2001-54102 号公报

发明内容

[0009] 本发明在以上背景下产生。本发明的目的在于提供一种可提高将 SIP 适用于监视系统时的安全性的监视系统。

[0010] 本发明的一个方式是一种监视系统，该监视系统具有：对监视信息进行通信的多个终端；管理多个终端的通信的通信管理装置，多个终端分别设置在监视对象一侧，或利用从监视对象接收的监视信息的使用者一侧，其构成是，当多个终端的一个终端向其他终端请求连接时，该连接源终端将包括连接地终端的识别信息在内的 SIP 的邀请消息发送到通信管理装置，通信管理装置具有：SIP 服务器；许可信息存储部，存储连接许可信息，该连接许可信息表示连接应被许可的终端的组合；许可处理部，参照连接许可信息判断是否许可

终端间的连接，当 SIP 服务器从连接源终端取得邀请消息时，将邀请消息中包含的连接地终端的识别信息提供到许可处理部，当许可处理部许可了终端间的连接时，SIP 服务器将来自连接源终端的邀请消息提供到连接地终端。

[0011] 本发明的另一方式是一种通信管理装置，该通信管理装置管理对监视信息进行通信的多个终端的通信，通信管理装置具有 ：SIP 服务器 ；许可信息存储部，存储连接许可信息，该连接许可信息表示连接应被许可的终端的组合 ；和许可处理部，参照连接许可信息判断是否许可终端间的连接，SIP 服务器从多个终端中的一个取得包括对其他终端的识别信息在内的 SIP 的邀请消息时，许可处理部根据邀请消息中含有的连接地终端的识别信息判断是否许可终端间的连接，当许可处理部许可了连接时，SIP 服务器将来自连接源终端的邀请消息提供到连接地终端。

[0012] 如下所述，本发明存在其他方式。因此，本发明的公开意在提供本发明的部分方式，并不限制在此记述请求的发明范围。

附图说明

[0013] 图 1 是表示本发明的监视系统的整体构成的图。

[0014] 图 2 是较具体的表示监视系统的构成的框图。

[0015] 图 3 是表示本发明的监视系统中的主要构成的框图。

[0016] 图 4 是表示许可信息存储部中存储的连接许可信息的表例的图。

[0017] 图 5 是表示在监视系统中进行终端间的通信时的动作的图。

[0018] 图 6 是表示监视装置作为连接源以进行终端间的通信的动作的图。

[0019] 图 7 是表示使用者装置作为连接源以进行终端间的通信的动作的图。

[0020] 标号说明

[0021] 1 监视系统

[0022] 3 监视中心

[0023] 5 监视对象

[0024] 7 使用者地点

[0025] 11 通信管理装置

[0026] 13 中心装置

[0027] 15 监视装置

[0028] 17 使用者装置

[0029] 21 中心终端间 VPN

[0030] 23 SIP 通信

[0031] 25 终端间 VPN

[0032] 33 HTTP 服务器

[0033] 35 VPN 服务器

[0034] 37 SIP 服务器

[0035] 41 账户管理服务器

[0036] 43 数据库

[0037] 61 控制器

[0038] 63 IP 线路单元

[0039] 65、83 路由器

[0040] 69 多线路适配器

[0041] 73 监视照相机

[0042] 81 VPN 终端装置 (VTE)

[0043] 85 使用者 PC

[0044] 101 许可信息存储部

[0045] 103 许可处理部

具体实施方式

[0046] 以下详细说明本发明。但以下的详细说明及附图不用于限定本发明。

[0047] 本发明是一种监视系统，具有 :对监视信息进行通信的多个终端 ;管理多个终端的通信的通信管理装置，多个终端分别设置在监视对象一侧或利用从监视对象接收的监视信息的使用者一侧，其构成是，当多个终端的一个终端向其他终端请求连接时，该连接源终端将包括连接地终端的识别信息在内的 SIP 的邀请消息发送到通信管理装置，通信管理装置具有 :SIP 服务器 ;许可信息存储部，存储连接许可信息，该连接许可信息表示连接应被许可的终端的组合 ;和许可处理部，参照连接许可信息，判断是否许可终端间的连接，SIP 服务器从连接源终端取得邀请消息时，将邀请消息中含有的连接地终端的识别信息提供到许可处理部，当许可处理部许可了终端间的连接时，SIP 服务器将来自连接源终端的邀请消息提供到连接地终端。

[0048] 如上所述，根据本发明，监视系统的多个终端连接到具有 SIP 服务器的通信管理装置。通信管理装置除了 SIP 服务器外还具有 :许可信息存储部，存储连接许可信息，该连接许可信息表示连接应被许可的终端的组合 ;和许可处理部，参照连接许可信息判断是否许可终端间的连接。在 SIP 的信令中，邀请消息从连接源终端发送到 SIP 服务器。此时，在本发明中，许可处理部判断是否许可连接。当许可处理部许可了连接时，SIP 服务器将来自连接源终端的邀请消息发送到连接地终端，SIP 的信令成功。

[0049] 因此，在本发明中，预先存储连接应被许可的终端的组合的信息，在 SIP 信令时进行终端间的连接的许可。这样一来，并非终端和 SIP 服务器之间的简单认证，而是可进行介入了 SIP 服务器的终端间即 P2P 的许可，可恰当限制监视信息的使用者。这样一来，可提高适用监视系统 SIP 时的安全性。

[0050] 连接地终端从通信管理装置接收到邀请消息时，可将 SIP 的 OK 消息发送到通信管理装置，可向邀请消息及 OK 消息附加连接确立信息，其用于在 SIP 会话确立后，在连接源及连接地终端间确立不介入通信管理装置的终端间连接。

[0051] 这样一来，在 SIP 会话确立后，可不借助通信管理装置而在终端间进行监视信息的通信。在本发明中，进行两个阶段的通信。第 1 阶段的通信是 SIP，借助通信管理装置进行。第 2 阶段的通信是不借助通信管理装置的终端间连接。在 SIP 连接时进行信令，在信令中交换邀请消息和 OK 消息。本发明利用 SIP 的信令的消息，交换用于终端间连接的确立的连接确立信息。这样一来，可良好地利用 SIP 进行终端间连接。并且，可降低通信管理装置和终端的通信量，降低通信管理装置的负荷。

[0052] 不介入通信管理装置的终端间连接可以是在终端间构筑 VPN 进行连接的终端间 VPN。这样一来，通过向终端间通信（上述 SIP 连接后的第 2 阶段的通信）适用 VPN（虚拟专用网络），可提高安全性。SIP 的信号通信中的双向消息交换可适用于 VPN 连接确立所需的信息交换。

[0053] 邀请消息可含有连接源终端的 IP 地址和电子证书作为连接确立信息，OK 消息可含有连接地终端的 IP 地址和电子证书作为连接确立信息。这样一来，可适当利用 SIP 交换 VPN 连接中使用的信息，在终端间进行安全的通信。

[0054] 通信管理装置可设置在监视中心上，该监视中心利用与多个终端的通信对监视对象进行监视。这样一来，可利用通信管理装置良好地进行监视中心和终端的通信及终端间的通信。

[0055] 通信管理装置和多个终端的连接可在通信管理装置和多个终端间通过构筑了 VPN 的中心终端间 VPN 连接，SIP 服务器可借助中心终端间 VPN 使多个终端和 SIP 消息通信。这样一来，SIP 通信在中心终端间 VPN 上进行。以上论述了 SIP 会话确立后在终端间进行 VPN 连接。这里的中心终端间 VPN 是中心和各终端间的 VPN。通过使用中心终端间 VPN，可确保监视中心和各终端的通信的安全性，并且也可确保 SIP 通信的安全性。

[0056] 监视信息可包括由监视对象拍摄的图像、由监视对象检测出的监视信号以及通过使用者一侧生成的控制信息中的至少一个。这样一来，可在终端间对监视信息进行通信。

[0057] 本发明的另一方式是一种通信管理装置，管理对监视信息进行通信的多个终端的通信，其中，通信管理装置具有：SIP 服务器；许可信息存储部，存储连接许可信息，该连接许可信息表示连接应被许可的终端的组合；和许可处理部，参照连接许可信息，判断是否许可终端间的连接，SIP 服务器从多个终端中的一个取得包括对其他终端的识别信息在内的 SIP 的邀请消息时，许可处理部根据邀请消息中含有的连接地终端的识别信息判断是否许可终端间的连接，当许可处理部许可了连接时，SIP 服务器将来自连接源终端的邀请消息提供到连接地终端。该方式中也可适用上述各种构成。

[0058] 本发明不限于上述监视系统及通信管理装置的方式。本发明的其他方式例如是终端装置。并且，本发明可通过方法、程序、或记录了该程序的计算机可读取的记录介质的形式来实现。

[0059] 如上所述，本发明可提高将 SIP 适用于监视系统时的安全性。

[0060] 以下参照附图说明本发明的实施方式的监视系统。

[0061] 图 1 表示本发明的监视系统的整体构成。如图所示，监视系统 1 中，在监视中心 3、监视对象 5 及使用者地点 7 之间进行通信。其中，使用者是指监视系统 1 中的监视对象 5 的监视服务的使用者。在本实施方式的例子中，监视对象 5 是店铺，使用者地点 7 是店铺主人的办公室。

[0062] 监视中心 3 中具有通信管理装置 11 及多个中心装置 13，它们连接为能够通信。通信管理装置 11 及多个中心装置 13 可配置在地理上远离的地点。多个中心装置 13 可分别配置在多个担当区域。并且，多个中心装置 13 可分担功能。例如，某中心装置 13 可作为处理警备相关的信号的管制中心装置发挥作用，其他中心装置 13 可作为主要处理监视影像的图像中心装置发挥作用。此外，在本发明的范围内，中心装置 13 也可以是一个。

[0063] 监视对象 5 及使用者地点 7 中分别设置监视装置 15 及使用者装置 17。监视装置

15 及使用者装置 17 相当于本发明的终端。监视装置 15 将监视信息发送到中心装置 13 及使用者装置 17。监视信息例如是监视照相机的图像，并且是由监视对象 5 检测出的监视信号。监视信号例如是表示发生异常的警备信号，根据来自设置在监视对象 5 上的传感器的检测信号生成警备信号，或者在操作警报按钮（开关）时生成。并且，使用者装置 17 向监视装置 15 发送控制信号或声音信号。这种从使用者装置 17 到监视装置 15 的信号也包含在监视信息中。

[0064] 图 1 中示出了一个监视对象 5 及一个使用者地点 7。但实际上，监视中心 3 与多个监视对象 5 及多个使用者地点 7 通信。因此，通信管理装置 11 也与多个监视装置 15 及多个使用者装置 17 通信。各监视装置 15 与建立关联的使用者装置 17（店铺主人的终端）通信。

[0065] 根据图 1 的监视系统 1，例如监视装置 15 通过传感器信号等检测异常。此时，作为监视信息的警备信号与监视对象 5 的影像一起被发送到监视中心 3。在监视中心 3，操作者通过中心装置 13 的监视器确认警备信号和影像，向警备人员发出必要的指示。接受到指示的警备人员快速到达至监视对象 5，处理异常。

[0066] 并且，例如监视装置 15 定期地或根据其他设定将监视对象 5 的影像等发送到使用者装置 17。例如，通过传感器检测出来客时，影像等被发送到使用者装置 17。并且，也存在使用者装置 17 要求发送影像等的情况。主人可根据影像等掌握店铺的情况。并且，主人能够从使用者装置 17 向监视装置 15 发送声音等，将必要事项指示给店员。

[0067] 接着说明监视系统 1 的通信方式。通信管理装置 11、监视装置 15 及使用者装置 17 连接到因特网。

[0068] 进一步，通信管理装置 11 在因特网上通过中心终端间 VPN（虚拟专用网络）21 与监视装置 15 及使用者装置 17 连接。为了构筑中心终端间 VPN21，使通信管理装置 11 具有 VPN 服务器功能，使监视装置 15 及使用者装置 17 具有 VPN 客户端功能。在 VPN 中，构筑 VPN 隧道，进行密码通信，实现较高的安全性。

[0069] 并且，监视装置 15 和使用者装置 17 借助通信管理装置 11 进行 SIP 通信 23。SIP 通信 23 借助上述中心终端间 VPN21 进行。通信管理装置 11 具有 SIP 服务器功能。

[0070] 并且，监视装置 15 和使用者装置 17 不借助通信管理装置 11 而是直接通过终端间 VPN25 连接。为构筑该终端间 VPN25，使用者装置 17 具有 VPN 服务器功能，使监视装置 15 具有 VPN 客户端功能。

[0071] 其中，中心终端间 VPN21 总是连接而构筑 VPN 隧道，用于中心装置 13 和监视装置 15 及使用者装置 17 之间的通信。而终端间 VPN25 仅在必要时构筑。

[0072] 说明使用终端间 VPN25 的理由。在监视系统 1 中进行影像等大容量的数据的通信。如果中心终端间 VPN21 用于所有通信，则通信管理装置 11 的负荷变得过大。因此，由终端间 VPN25 进行监视装置 15 和使用者装置 17 的通信，从而可确保安全性的同时减轻通信管理装置 11 的负荷。

[0073] 并且，本实施方式中的 SIP 通信 23 的作用是和普通的 IP 电话等不同的特别的作用。即，本实施方式中，将 SIP 的信令作为 VPN 连接前的准备的处理来定位。具体而言，确立 SIP23 的会话时，进行信息通知。在该信息通知中进行双向通信，交换邀请消息和 OK 消息。另一方面，为了确立 VPN 连接，需要交换信息。在本实施方式中，交换 IP 地址及电子证

书。电子证书用于验证电子签名等的正当性，使用由可靠的第三方机构发行的证书。因此，SIP 通信 23 的信令作为用于确立 VPN 连接的信息交换单元使用。

[0074] 以上说明了监视系统 1 的整体构成。如上所述，在本实施方式中，使用两种 VPN。一种连接通信管理装置 11 和终端（监视装置 15 或使用者装置 17），另一种连接终端之间（监视装置 15 和使用者装置 17）。因此，在图 1 中，为了区别这两个 VPN，使用中心终端间 VPN21 和终端间 VPN25 这两个用语。但也可简化使用 VPN21、VPN25 这两个用语。

[0075] 接着参照图 2 具体说明监视系统 1 的构成。通信管理装置 11 具有：防火墙 31、HTTP 服务器 33、VPN 服务器 35、SIP 服务器 37、STUN 服务器 39、账户管理服务器 41、数据库 43 及日志服务器 45。

[0076] 防火墙 31 用于屏蔽在通信管理装置 11 和监视装置 15 及使用者装置 17 之间使用的通信数据以外的数据。HTTP 服务器 33 用于因特网连接。VPN 服务器 35 是进行构筑 VPN 隧道的认证及加密的服务器。

[0077] VPN 服务器 35 用于实现中心终端间 VPN21，在通信管理装置 11 和监视装置 15 之间构筑 VPN，以及在通信管理装置 11 和使用者装置 17 之间构筑 VPN。来自监视装置 15 的信号通过 VPN 服务器 35 解密，发送到中心装置 13。并且，来自中心装置 13 的信号通过 VPN 服务器 35 加密，发送到监视装置 15。并且，在通信管理装置 11 向监视装置 15 发送信号时，也通过 VPN 服务器 35 进行加密。在通信管理装置 11 和使用者装置 17 的通信中，VPN 服务器 35 也同样进行加密及解密。

[0078] SIP 服务器 37 根据 SIP 协议进行信令的处理，连接监视装置 15 和使用者装置 17。在使用者装置 17 要求连接到监视装置 15 时，或监视装置 15 要求连接到使用者装置 17 时，SIP 服务器 37 起到 SIP 的连接控制的作用。

[0079] 在 SIP 的信令中，交换消息。具体而言，交换 INVITE（邀请）消息和 OK 消息。利用该消息交换，如上所述，为确立 VPN 连接而交换 IP 地址及电子证书。

[0080] STUN 服务器 39 为对应监视装置 15 及使用者装置 17 的路由器的 NAT 功能而提供 STUN 功能。

[0081] 账户管理服务器 41 是管理认证等各种信息的服务器。被管理的信息存储到数据库 43 中。被管理的信息包括 IP 线路的账户、用于 VPN 连接（隧道构筑）的电子证书、密钥对的信息。并且在本实施方式中，在 SIP 的信令过程中，对终端间的连接进行认证及许可。用于该处理的信息也由数据库 43 保存，用于账户管理服务器 41。此外，对终端间的连接的认证及许可可由 SIP 服务器自身进行，这种情况下，本发明的许可处理部及许可信息存储部设置在 SIP 服务器上。

[0082] 日志服务器 45 是保存通过监视装置 15 生成的日志的服务器。

[0083] 中心装置 13 具有监视台 51 和线路连接装置 53。监视台 51 借助线路连接装置 53 连接到通信管理装置 11。例如，当中心装置 13 是图像中心时，监视影像被提供到监视台 51，由监视台 51 管理。并且，当中心装置 13 是管制中心时，警备相关的信息被提供到监视台 51。监视影像也良好的显示于管制中心的监视器上。监视影像等也可在中心装置之间进行通信。

[0084] 接着说明监视装置 15。监视装置 15 包括：控制器 61、IP 线路单元 63、路由器 65、外围设备 67、多线路适配器 69 及监视对象 PC（个人计算机）71。

[0085] 控制器 61 由计算机构成，与外围设备 67 协作而实现监视功能。控制器 61 借助 IP 线路单元 63 与监视中心 3 连接。并且，控制器 61 也借助 IP 线路单元 63 与使用者装置 17 连接。

[0086] 在图 2 中，作为外围设备 67 示例了监视照相机 73、传感器 75 及警报按钮 77。控制器 61 对监视影像实施图像识别处理来检测异常。并且，控制器 61 通过从传感器 75 输入的检测信号来检测异常。当警报按钮 77 被按下时也检测出异常。其他外围设备也可用于检测异常。当发生异常时，控制器 61 与中心装置 13 通信，发送警备信号和图像信号。具有监视照相机 73 的同时还具有麦克风，也发送声音信号。这样一来，控制器 61 实现监视对象 5 的警备功能。

[0087] 并且，在中心装置 13 要求时也会发送监视影像及声音。进一步，监视影像及声音也发送到使用者装置 17。例如定期进行、或者也可根据其他设定来进行向使用者装置 17 的发送。例如，通过传感器 75 检测到来客时，影像等发送到使用者装置 17。并且，在使用者装置 17 要求时，监视装置 15 也发送影像等。

[0088] IP 线路单元 63 构筑用于控制器 61 与通信管理装置 11 通信的 VPN 隧道。并且，构筑用于控制器 61 与使用者装置 17 通信的 VPN 隧道。前者对应于中心终端间 VPN21，后者对应于终端间 VPN25。在这些连接中，IP 线路单元 63 实现 VPN 客户端的功能。

[0089] 在图 2 中，IP 线路单元 63 作为控制器 61 的内部构成被示出。这表现了物理配置。作为通信构成，IP 线路单元 63 配置在控制器 61 和路由器 65 之间。并且，IP 线路单元 63 与控制器 61 通过以太网（注册商标）LAN 连接。路由器 65 是宽带线路用的路由器。

[0090] 多线路适配器 69 借助移动电话网与中心装置 13 连接。多线路适配器 69 用于在宽带线路不通时发送警备信号。警备信号从控制器 61 借助 IP 线路单元 63 发送到多线路适配器 69，从多线路适配器 69 发送到中心装置 13。

[0091] 监视对象 PC71 是设置在监视对象 5 上的 PC。在本实施方式的例子中，监视对象 5 是店铺。因此，监视对象 PC71 可以是店铺用的 PC。

[0092] 接着说明使用者装置 17。使用者装置 17 由 VPN 终端装置（以下称 VTE）81、路由器 81 及使用者 PC（个人计算机）85 构成。

[0093] VTE81 是用于宽带连接的线路终端装置。并且，VTE81 构筑通信管理装置 11 的 VPN 服务器 35 和 VPN 隧道，并且构筑监视装置 15 的 IP 线路单元 63 和 VPN 隧道。在前者中，VTE81 作为 VPN 客户端作用，在后者中，VTE81 作为 VPN 服务器作用。路由器 83 是宽带线路用的路由器。

[0094] VTE81 与使用者 PC85 连接。VTE81 将从监视装置 15 的控制器 61 接收的影像、声音及控制信号转发到使用者 PC85。并且，VTE81 将从使用者 PC85 接收的声音及控制信号转发到控制器 61。

[0095] 在本实施方式中，使用者地点 7 是店铺主人的办公室等。因此，使用者 PC85 可以是店铺的主人的 PC。使用者 PC85 用于主人察看监视对象 5 的监视影像。为提供该功能，使用者 PC85 中安装应用程序，通过与控制器 61 进行通信可显示及切换监视对象 5 的监视影像。

[0096] 在本实施方式中，使用者装置 17 是固定的。但是使用者装置 17 的功能也可组装到移动终端等中，从而可以移动。

[0097] 以上说明了监视系统 1 的整体构成。接着说明本发明的特征性构成。

[0098] 图 3 表示图 1 及图 2 所示的监视系统 1 的一部分，是本发明的主要部分。在图 3 中，对在图 1 及图 2 中说明的要素标以同样的标号。

[0099] 如图 3 所示，通信管理装置 11 中除了 VPN 服务器 35 和 SIP 服务器 37 外，具有许可信息存储部 101 及许可处理部 103。许可信息存储部 101 存储连接许可信息，该连接许可信息表示连接待被许可的终端（监视装置 15 及使用者装置 17）的组合。并且，许可处理部 103 参照连接许可信息，判断是否许可终端间的连接。许可信息存储部 101 及许可处理部 103 分别通过图 2 的数据库 43 及账户管理服务器 41 实现。

[0100] 图 4 表示许可信息存储部 101 中应存储的连接许可信息的例子。在该例中，连接许可信息是表示终端 ID 的组合的表。该表使各使用者（店铺的主人）、监视装置 ID（监视装置 15 的 ID）以及使用者装置 ID（使用者装置 17 的 ID）建立对应。监视装置 ID 及使用者装置 ID 是能够确定监视装置 15 及使用者装置 17 的任意的信息。在后述例子中，监视装置 ID 是 IP 线路单元 63 的 ID，使用者装置 ID 是 VTE81 的 ID。

[0101] 存在一个主人拥有多个店铺的情况。此时，一个监视装置 15 与多个使用者装置 17 组合。在图 4 的例子中，使用者 C 具有两个店铺，两个监视装置 15(C01、C02) 与使用者装置 17(C11) 建立对应。此外，一个主人使用多个使用者装置 17 时，一个监视装置 15 与多个使用者装置 17 对应即可。

[0102] 返回到图 3，在监视装置 15 中，IP 线路单元 63 具有 SIP 处理部 111、VPN 处理部 113 及存储部 115。SIP 处理部 111 及 VPN 处理部 113 分别进行和 SIP 及 VPN 相关的处理。存储部 115 存储通过 IP 线路单元 63 处理的各种信息。特别是在本发明中，存储部 115 存储 IP 线路单元 63 的 IP 地址和电子证书。这些信息相当于本发明的连接确立信息，为了 VPN 连接而提供到连接对象。并且，存储部 115 存储 IP 线路单元 ID(IP 线路单元 63 的 ID)，该 IP 线路单元 ID 作为监视对象 5 的 ID 使用。

[0103] 如图 3 所示，使用者装置 17 的 VTE81 也具有 SIP 处理部 121、VPN 处理部 123 及存储部 125。存储部 125 存储 VTE81 的 IP 地址和电子证书。并且，存储部 125 存储 VTE-ID(VTE81 的 ID)。

[0104] 接着说明本实施方式的动作。在此说明构筑终端间 VPN25 时的动作、即进行监视装置 15 和使用者装置 17 之间的 VPN 连接时的动作。

[0105] 首先说明动作概要。如上所述，在通信管理装置 11 和监视装置 15 之间总是构筑中心终端间 VPN21。通信管理装置 11 和使用者装置 17 之间也总是构筑中心终端间 VPN21。与这些中心终端间 VPN21 不同，通过以下动作在监视装置 15 和使用者装置 17 之间直接构筑终端间 VPN25。

[0106] 连接终端间 VPN25 时进行信息的交换。在本实施方式中，在监视装置 15 和使用者装置 17 之间交换 IP 地址和电子证书。作为该信息交换的单元，本实施方式着眼于 SIP。在 SIP 的信息通知中，在终端间交换消息。在该 SIP 消息中加入上述 IP 地址及电子证书。这样一来，通过 SIP 的信息通知可进行用于准备构筑终端间 VPN25 的信息交换。

[0107] 在 SIP 的基本功能中，在 SIP 服务器 37 中所注册的任意的地址之间确立 SIP 的连接。在这种情况下，存在监视装置 15 与无关的使用者装置 17 连接的可能性，在安全性上不佳。考虑到这一点，在本实施方式中，如下所述进行信令。以下将监视装置 15 及使用者装

置 17 中的一个作为 SIP 的连接源终端，将另一个作为 SIP 的连接地终端。并且，SIP 的消息在中心终端间 VPN21 上发送。

[0108] 参照图 5，首先，连接源终端将 INVITE 消息（具体而言是 SIPINVITE 消息，以下相同）发送到 SIP 服务器 37(S1)。INVITE 消息中附加有连接源终端的 ID 及连接地终端的 ID、连接源终端的 IP 地址及电子证书。

[0109] SIP 服务器 37 接收到 INVITE 消息后，将连接源终端的 ID 和连接地终端的 ID 提供到许可处理部 103，询问许可处理部 103 是否可连接该连接源终端和连接地终端 (S3)。许可处理部 103 参照许可信息存储部 101 的连接许可信息，判断是否许可连接的 (S5)。如果连接源终端和连接地终端的组合注册在许可信息存储部 101 中，则许可连接。

[0110] SIP 服务器 37 从许可处理部 103 接收许可结果 (S7)。如果由许可处理部 103 许可了连接，则 SIP 服务器 37 将 INVITE 消息发送到连接地终端 (S9)。该 INVITE 消息包括连接源终端的 IP 地址及电子证书。

[0111] 连接地终端接收到 INVITE 消息后，向 SIP 服务器 37 发送 OK 消息（具体而言是 SIP 2000K 消息，以下相同）(S11)。OK 消息附加有连接地终端的 IP 地址和电子证书。该 OK 消息经由 SIP 服务器 37 发送到连接源终端 (S13)。由此，通过 SIP 的信息通知交换了 IP 地址及电子证书。并且，在终端间构筑 VPN 时，通过连接请求中含有的电子证书和之前交换的电子证书进行认证，构筑终端间 VPN25(S15)。

[0112] 如上所述，在本实施方式中，由 SIP 服务器 37 接收 INVITE 消息后进行许可终端的组合的处理。如果连接未被许可，则 INVITE 消息不会被发送到连接地终端，也不会进行之后的 SIP 处理和 VPN 处理。仅在监视装置 15 和使用者装置 17 的组合适当时，连接被许可，INVITE 消息被发送到连接地终端，进行之后的 SIP 处理，最终能够进行 VPN 连接。

[0113] 接着参照图 6 及图 7 详细说明监视系统 1 的动作。其中，首先说明监视装置 15 是连接源终端的情况，接着说明使用者装置 17 是连接源的情况。

[0114] 在图 6 的时间图中，控制器 61 及 IP 线路单元 63 是监视装置 15 的构成，SIP 服务器 37 及许可信息存储部 101（账户管理服务器 41）是通信管理装置 11 的构成，VTE81 及使用者 PC85 是使用者装置 17 的构成。

[0115] 控制器 61 将包括 VTE-ID(VTE81 的 ID) 的连接指示 (P2P 连接指示）发送到 IP 线路单元 63(S101)。这里，VTE-ID 用作连接地终端 ID。

[0116] IP 线路单元 63 从存储部 115 读出 IP 线路单元 IP 地址 (IP 线路单元 63 的 IP 地址）及 IP 线路单元个别证书。IP 线路单元个别证书是分配给各 IP 线路的电子证书。并且，IP 线路单元 63 从存储部 115 读出作为连接源终端 ID 的 IP 线路单元 ID(IP 线路单元 63 的 ID)。并且，IP 线路单元 63 将该信息附加到 INVITE 消息，然后将 INVITE 消息发送到 SIP 服务器 37(S103)。具体而言，INVITE 消息包括 IP 线路单元 IP 地址、IP 线路单元 ID、VTE-ID 及 IP 线路单元个别证书。

[0117] SIP 服务器 37 接收 INVITE 消息，将 IP 线路单元 ID 及 VTE-ID 发送到许可处理部 103，询问是否许可连接 (S105)。许可处理部 103 参照许可信息存储部 101 的连接许可信息来判断是否许可连接 (S107)。这里，读出图 4 的表。然后许可处理部 103 判断询问的终端 ID 的组合是否注册到了表中。如果对应的组合已被注册，则许可处理部 103 许可连接。许可结果从许可处理部 103 发送到 SIP 服务器 37(S109)。在许可处理部 103 许可了连接时，

SIP 服务器 37 将 INVITE 消息发送到 VTE81(S111)。该 INVITE 消息附加有 IP 线路单元 IP 地址及 IP 线路单元个别证书。

[0118] 在上述处理中，在步骤 S107 中如果未许可连接，则 SIP 服务器 37 不会将 INVITE 消息发送到 VTE81。因此，不会进行之后的 SIP 处理，也不进行之后的 VPN 连接。

[0119] VTE81 接收到 INVITE 消息后，由存储部 125 保存 IP 线路单元 IP 地址及 IP 线路单元个别证书，向使用者 PC85 进行连接请求 (P2P 连接请求) 的询问 (S113)。该连接请求附加有 IP 线路单元 IP 地址。之后使用者 PC85 向 VTE81 发送连接响应 (S115)。

[0120] VTE81 从存储部 125 读出 VTE-IP 地址 (VTE81 的 IP 地址) 及 VTE 个别证书 (分配给 VTE81 的电子证书)。然后，VTE81 将 OK 消息发送到 SIP 服务器 37(S117)。该 OK 消息附加有 VTE-IP 地址和 VTE 个别证书。

[0121] SIP 服务器 37 将 OK 消息与 VTE-IP 地址及 VTE 个别证书一起发送到 IP 线路单元 63(S 119)。IP 线路单元 63 接收到 OK 消息后，由存储部 115 保存 VTE-IP 地址及 VTE 个别证书，将 ACK 消息发送到 SIP 服务器 37(S121)，进一步，SIP 服务器 37 将 ACK 消息发送到 VTE81(S123)。

[0122] 在上述过程中，IP 线路单元 63 取得 VTE81 的 IP 地址及电子证书。并且，VTE81 取得 IP 线路单元 63 的 IP 地址及电子证书。因此，能够使用这些信息识别对方从而在 IP 线路单元 63 和 VTE81 之间确立 VPN 连接。这是终端间 VPN25。

[0123] 如图所示，IP 线路单元 63 向 VTE81 进行 VPN 连接请求 (S125)。这里，不借助 SIP 服务器 37 而是直接请求 VPN 连接。VTE81 通过 VPN 连接请求所包含的 IP 线路单元个别证书和存储部 125 中保存的 IP 线路单元的个别证书进行认证，将包括对象的 IP 线路单元 IP 地址在内的到达信息发送到使用者 PC85(S127)。IP 线路单元 IP 地址由使用者 PC85 在 VPN 通信时使用。并且，VTE81 作为 VPN 服务器，将进行了 VPN 连接处理的情况通知 IP 线路单元 63(S129)。IP 线路单元 63 将连接结果是 OK 的情况通知控制器 61，并且将对象的 VTE-IP 地址通知控制器 61(S131)。VTE-IP 地址由控制器 61 在 VPN 通信时使用。由此，确立了 VPN 连接，通过终端间 VPN25 进行通信。监视影像及声音等从监视装置 15 提供到使用者装置 17。

[0124] 接着参照图 7 说明使用者装置 17 是连接源的情况。使用者 (主人) 例如将显示影像的指示输入到使用者 PC85。使用者 PC85 将包括 IP 线路单元 ID 在内的连接指示 (P2P 连接指示) 发送到 VTE81(S201)。这里，IP 线路单元 ID 用作连接地终端的 ID。

[0125] VTE81 从存储部 125 读出 VTE-IP 地址及 VTE 个别证书。并且，VTE81 从存储部 125 读出作为连接源终端 ID 的 VTE-ID。并且，VTE81 将这些信息附加于 INVITE 消息，将 INVITE 消息发送到 SIP 服务器 37(S203)。具体而言，INVITE 消息包括 VTE-IP 地址、VTE-ID、IP 线路单元 ID 及 VTE 个别证书。

[0126] SIP 服务器 37 接收 INVITE 消息，将 VTE-ID 和 IP 线路单元 ID 发送到许可处理部 103，询问是否许可连接 (S205)。许可处理部 103 和上述同样参照许可信息存储部 101 的连接许可信息，判断是否许可连接 (S207)，将许可结果发送到 SIP 服务器 37(S209)。即，如果 VTE-ID 和 IP 线路单元 ID 的组合已经被注册，则许可连接。在许可处理部 103 许可了连接后，SIP 服务器 37 将 INVITE 消息发送到 IP 线路单元 63(S211)。该 INVITE 消息附加有 VTE-IP 地址及 VTE 个别证书。

[0127] 在上述处理中，在步骤 S207 中如果未许可连接，则 SIP 服务器 37 不会将 INVITE

消息发送到 IP 线路单元 63。因此，不进行之后的 SIP 的处理，也不进行之后的 VPN 连接。

[0128] IP 线路单元 63 接收到 INVITE 消息后，在存储部 115 中保存 VTE-IP 地址及 VTE 个别证书。并且，IP 线路单元 63 对控制器 61 进行连接请求 (P2P 连接请求) 的询问 (S213)。该连接请求附加有 VTE-IP 地址。然后控制器 61 向 IP 线路单元 63 发送连接响应 (S215)。

[0129] IP 线路单元 63 从存储部 115 读出 IP 线路单元 IP 地址及 IP 线路单元个别证书。并且，IP 线路单元 63 将 OK 消息发送到 SIP 服务器 37(S217)。该 OK 消息附加有 IP 线路单元 IP 地址和 IP 线路单元个别证书。

[0130] SIP 服务器 37 将 OK 消息和 IP 线路单元 IP 地址及 IP 线路单元个别证书一起发送到 VTE81(S219)。VTE81 接收到 OK 消息后，将 IP 线路单元 IP 地址及 IP 线路单元个别证书保存到存储部 125 中，向 SIP 服务器 37 返回 ACK 消息 (S221)，并且，向使用者 PC85 通知 SIP 连接确立 (S223)。SIP 服务器 37 将 ACK 消息发送到 IP 线路单元 63(S225)。

[0131] 在上述过程中，在 IP 线路单元 63 和 VTE81 之间交换 IP 地址及电子证书。IP 线路单元 63 接收到 ACK 消息后，对 VTE81 进行 VPN 连接请求 (S227)。VPN 连接不通过 SIP 服务器 37 而进行。VTE81 将包括对象的 VTE-IP 地址的到达信息发送到使用者 PC85(S229)。并且，VTE81 作为 VPN 服务器将进行了 VPN 连接的处理的情况通知 IP 线路单元 63(S231)。IP 线路单元 63 将包括对象的 VTE-IP 地址的到达信息发送到控制器 61(S233)。由此，VPN 连接确立，通过终端间 VPN25 进行通信。

[0132] 如图 6、图 7 所示，在两图的处理中，从 IP 线路单元 63 向 VTE81 发送 VPN 连接请求。其理由如下。在 VPN 中，需要从客户端向服务器发送连接请求。在本实施方式中，VPN 服务器的功能仅设置在 VTE81 中。因此，在图 6 及图 7 双方中，VPN 连接请求都是从 IP 线路单元 63 发送到 VTE81。

[0133] 以上说明了本发明的优选实施方式。根据本实施方式，多个终端 (监视装置 15、使用者装置 17) 连接到具有 SIP 服务器 37 的通信管理装置 11。如图 3 所示，通信管理装置 11 除了 SIP 服务器 37 之外还具有许可信息存储部 101 和许可处理部 103。在 SIP 的信息通知中，从连接源终端向 SIP 服务器发送 INVITE(邀请) 消息。此时，许可处理部 103 判断是否许可连接。仅在许可处理部 103 许可连接时，SIP 服务器 37 将来自连接源终端的 INVITE 消息发送到连接地终端，SIP 的信息通知成功。

[0134] 因此，在本发明中，预先存储连接应被许可的终端的组合的信息，在 SIP 信息通知时进行终端间的连接的许可。由此，并非终端和 SIP 服务器 37 之间的简单认证，而是能够进行介入了 SIP 服务器 37 的终端间即 P2P 的许可，可恰当限制监视信息的使用者。由此可提高监视系统 1 中适用 SIP 时的安全性。

[0135] 并且，在本发明中，SIP 的信息通知中的 INVITE 消息和 OK 消息的交换中可附加连接确立信息，该连接确立信息是不借助通信管理装置 11 的终端间连接的确立所使用的信息。由此，能够在终端间交换连接确立信息，从而确立终端间连接。因此，可良好地利用 SIP 进行终端间连接。并且，可降低通信管理装置 11 和终端的通信量，降低通信管理装置 11 的负荷。

[0136] 并且，在本实施方式中，以 IP 地址和电子证书作为连接确立信息为例进行了说明，也可代替电子证书而使用其他信息进行对象的认证。例如，也可将电子证书中含有的通用名等用作连接确立信息。

[0137] 并且，根据本发明，不介入通信管理装置 11 的终端间连接，可以是在终端间构筑 VPN 并连接的终端间 VPN25。可将 SIP 的信息通知中的双向的信息交换适用于 VPN 连接确立所需的信息的交换，并且，通过使用 VPN 可提高安全性。

[0138] 并且，根据本发明，邀请消息包括连接源终端的 IP 地址和电子证书作为连接确立信息，OK 消息包括连接地终端的 IP 地址和电子证书作为连接确立信息。由此，可良好地利用 SIP 交换 VPN 连接中使用的信息，在终端间可进行安全的通信。

[0139] 并且，根据本发明，通信管理装置 11 可设置于监视中心 3。由此，利用通信管理装置 11 可良好地进行监视中心 3 和终端的通信及终端间的通信。

[0140] 并且，根据本发明，通信管理装置 11 和多个终端的连接可通过在通信管理装置 11 和多个终端之间构筑了 VPN 的中心终端间 VPN21 来连接，SIP 服务器 37 可借助中心终端间 VPN21 与多个终端进行 SIP 消息通信。由此，SIP 通信在中心终端间 VPN21 上进行。SIP 通话后确立的终端间 VPN25 是终端间的 VPN，而中心终端间 VPN21 是通信管理装置 11 和终端间的 VPN。通过使用中心终端间 VPN21，可确保监视中心 3 和各终端的通信的安全性，并且可确保 SIP 通信的安全性。

[0141] 并且，根据本发明，监视信息可包括由监视对象 5 拍摄的图像、由监视对象 5 检测出的监视信号、由使用者一侧生成的控制信息中的至少一个。由此，可在终端间对监视信息进行通信。

[0142] 以上说明了本发明的优选实施方式。但本发明不限于上述实施方式，本领域技术人员在本发明的范围内当然可对上述实施方式进行变形。

[0143] 以上说明了目前考虑到的本发明的优选实施方式，但对本实施方式能够作多种变形，并且处于本发明的真实精神和范围内的所有变形均包含在权利要求的范围内。

[0144] 产业上利用的可能性

[0145] 如上所述，本发明涉及的监视系统适用于通过通信来远程监视店铺等。

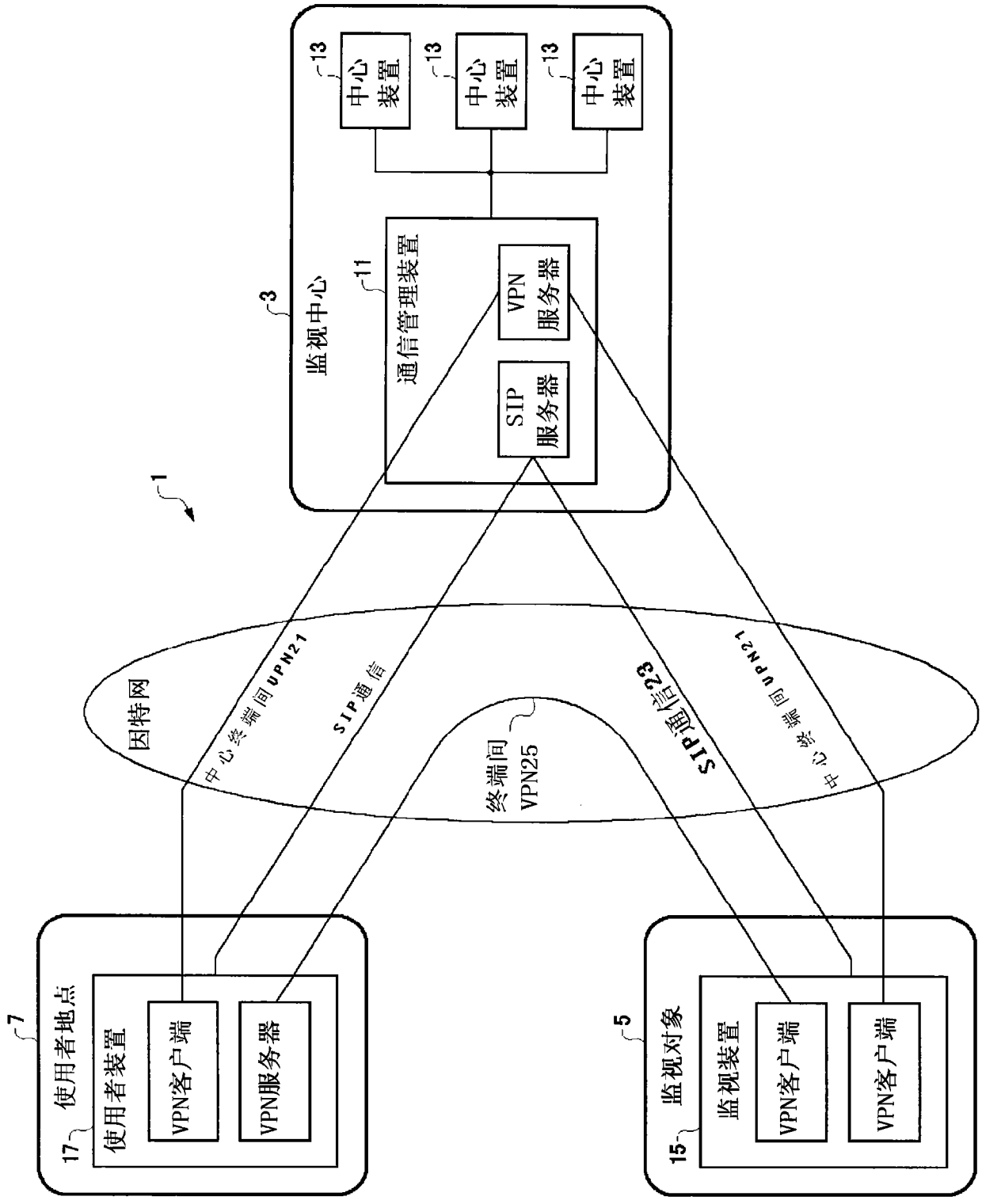

1
3
监视中心
11
通信管理装置
VPN
服务器
SIP
服务器
13
中心
装置
13
中心
装置
13
中心
装置
因特网
中心终端间VPN21
SIP通信
终端间
VPN25
SIP通信23
中心终端间VPN21
7
使用者地点
17
使用者装置
VPN客户端
VPN服务器
5
监视对象
15
监视装置
VPN客户端
VPN客户端

图 1

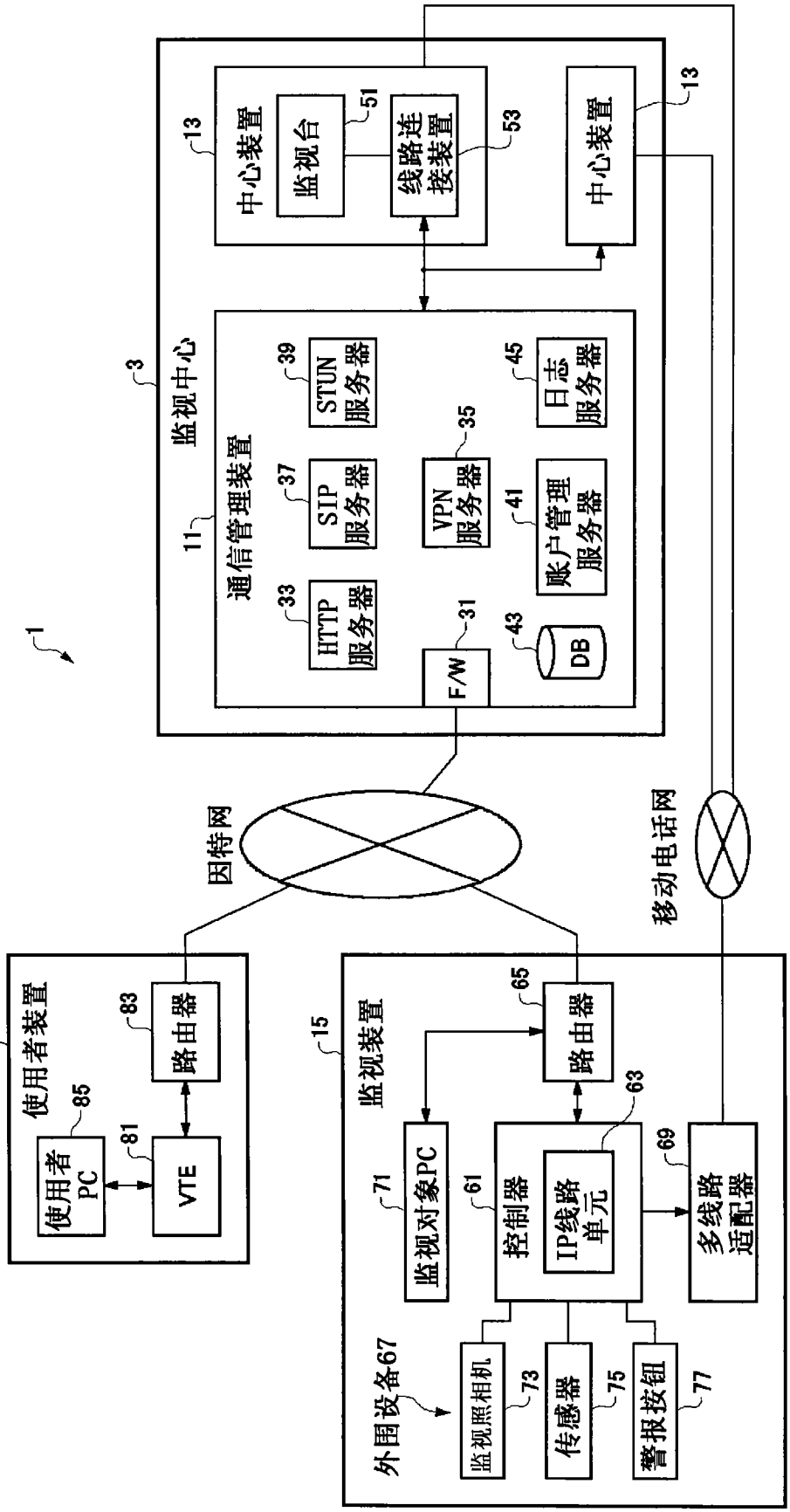

1
3
监视中心
11
通信管理装置
13
中心装置
监视台
51
线路连接装置
53
中心装置
13
39
STUN服务器
45
日志服务器
35
VPN服务器
37
SIP服务器
41
账户管理服务器
33
HTTP服务器
31
F/W
43
DB
因特网
移动电话网
17
使用者装置
83
路由器
85
使用者PC
81
VTE
15
监视装置
65
路由器
63
71
监视对象PC
61
控制器
IP线路单元
69
多线路适配器
外围设备67
监视照相机
73
传感器
75
警报按钮
77

图 2

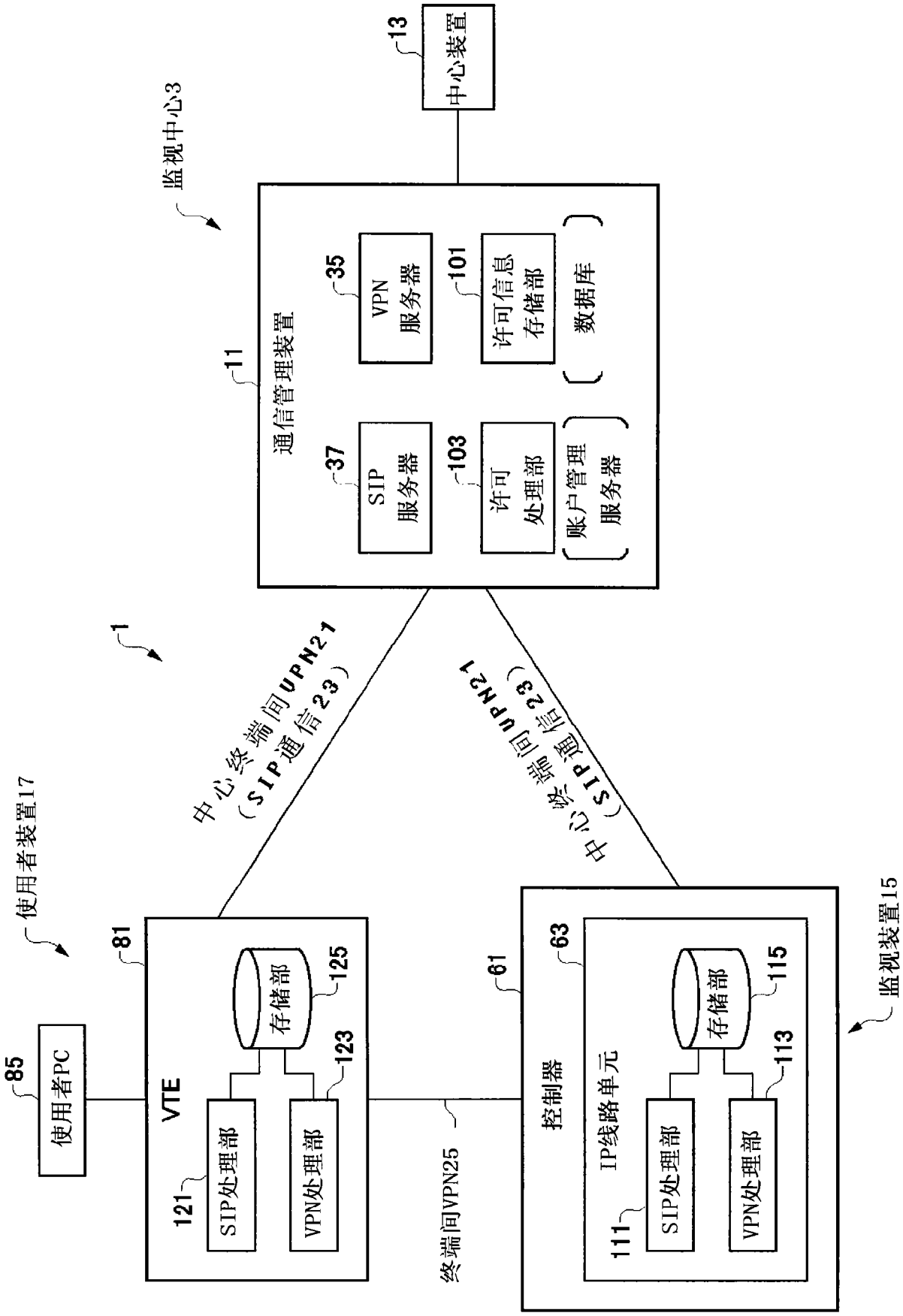

13
中心装置
监视中心3
11
通信管理装置
35
VPN
服务器
101
许可信息
存储部
数据库
37
SIP
服务器
103
许可
处理部
账户管理
服务器
1
中心终端间UPN21
（SIP通信23）
中心终端间UPN21
（SIP通信23）
使用者装置17
81
VTE
存储部
125
123
85
使用者PC
SIP处理部
121
VPN处理部
61
63
控制器
IP线路单元
存储部
115
113
SIP处理部
111
VPN处理部
终端间VPN25
监视装置15

图 3

使用者（主人）	终端ID	
	监视装置ID	使用者装置ID
A	A01	A11
B	B01	B11
C	C01	C11
C	C02	C11
⋮	⋮	⋮

图 4

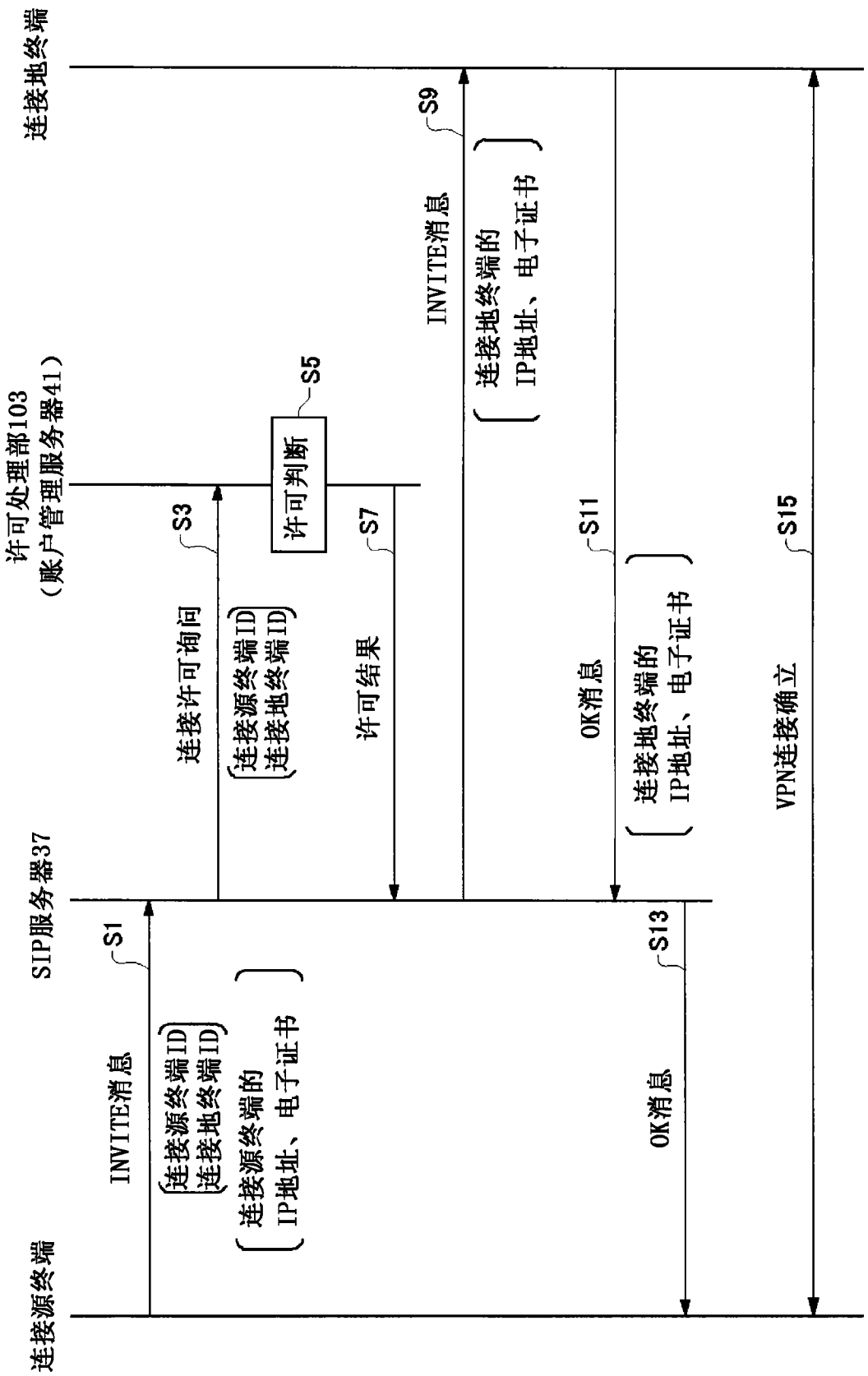

连接源终端
SIP服务器37
许可处理部103
（账户管理服务器41）
连接地终端
S1
INVITE消息
连接源终端ID
连接地终端ID
连接源终端的
IP地址、电子证书
S3
连接许可询问
连接源终端ID
连接地终端ID
S5
许可判断
S7
许可结果
S9
INVITE消息
连接地终端的
IP地址、电子证书
S11
OK消息
连接地终端的
IP地址、电子证书
S13
OK消息
S15
VPN连接确立

图 5

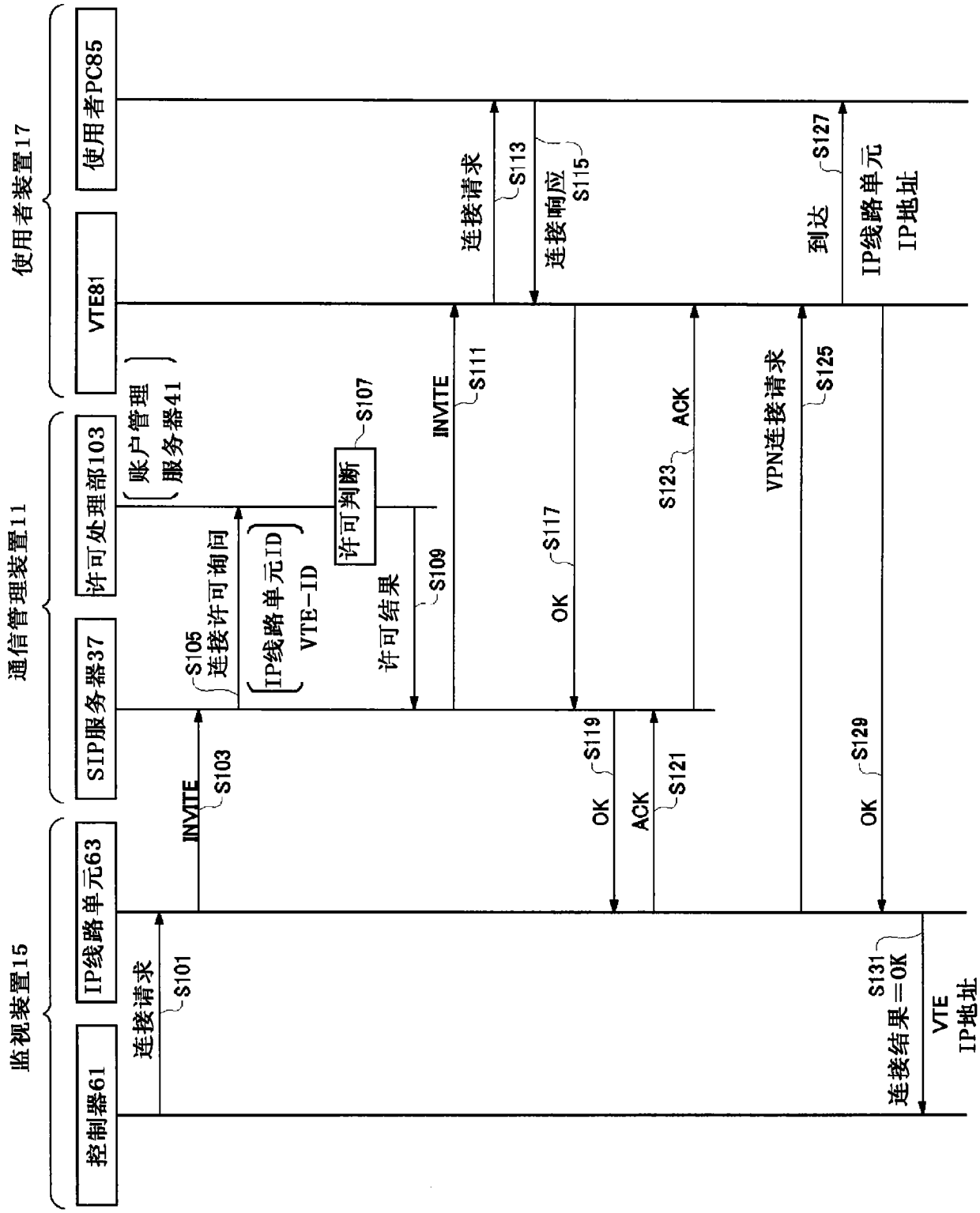

监视装置15
通信管理装置11
使用者装置17
控制器61
IP线路单元63
SIP服务器37
许可处理部103
账户管理服务器41
VTE81
使用者PC85
连接请求
S101
INVITE
S103
S105
连接许可询问
IP线路单元ID
VTE-ID
许可判断
S107
许可结果
S109
INVITE
S111
连接请求
S113
连接响应
S115
OK
S117
OK
S119
ACK
S121
ACK
S123
VPN连接请求
S125
到达
S127
IP线路单元
IP地址
OK
S129
连接结果=OK
S131
VTE
IP地址

图 6

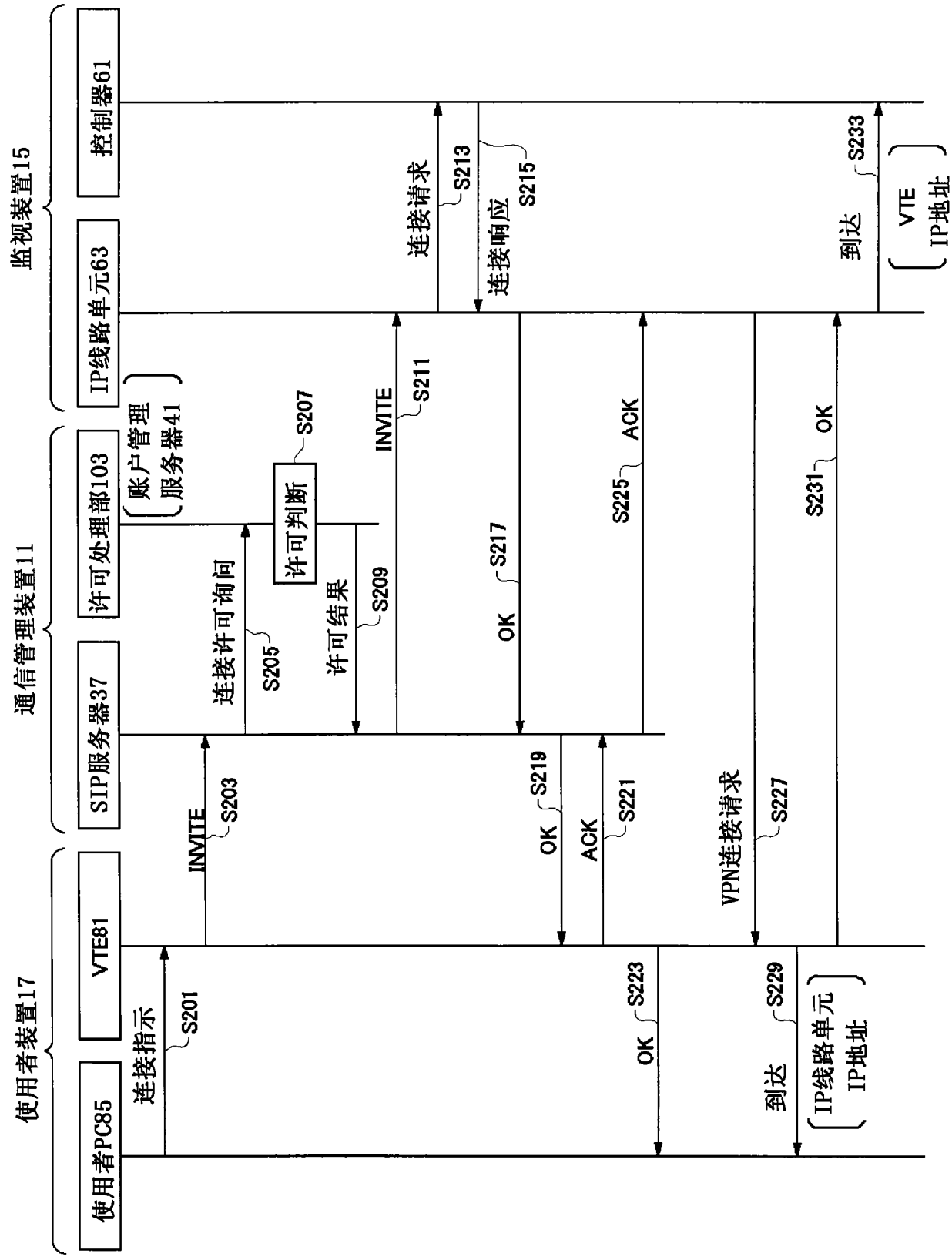

使用者装置17
使用者PC85
VTE81
通信管理装置11
SIP服务器37
许可处理部103
账户管理服务器41
监视装置15
IP线路单元63
控制器61
连接指示
S201
INVITE
S203
连接许可询问
S205
许可判断
S207
许可结果
S209
INVITE
S211
连接请求
S213
连接响应
S215
OK
S217
OK
S219
ACK
S221
ACK
S225
OK
S223
VPN连接请求
S227
OK
S231
到达
S229
IP线路单元
IP地址
到达
S233
VTE
IP地址

图 7