[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 12/24 (2006.01)
H04L 9/00 (2006.01)
H04L 9/32 (2006.01)
H04L 9/30 (2006.01)

[12] 发明专利说明书

专利号 ZL 200610085029.X

[45] 授权公告日 2009 年 6 月 17 日

[11] 授权公告号 CN 100502316C

[22] 申请日 2006.5.22
[21] 申请号 200610085029.X
[30] 优先权
[32] 2005.5.20 [33] JP [31] 147488/2005
[32] 2006.3.31 [33] JP [31] 096410/2006
[73] 专利权人 株式会社日立制作所
地址 日本东京都
[72] 发明人 桥本洋子 藤城孝宏 锻忠司
高田治 星野和义 中村信次
[56] 参考文献
EP12803002A2 2003.1.29
US 20030131259A1 2003.7.10
CN1681238A 2005.10.12
CN1528068A 2004.9.8
CN1202060A 1998.12.16
US20030070095A1 2003.4.10
审查员 彭 媛
[74] 专利代理机构 永新专利商标代理有限公司
代理人 胡建新

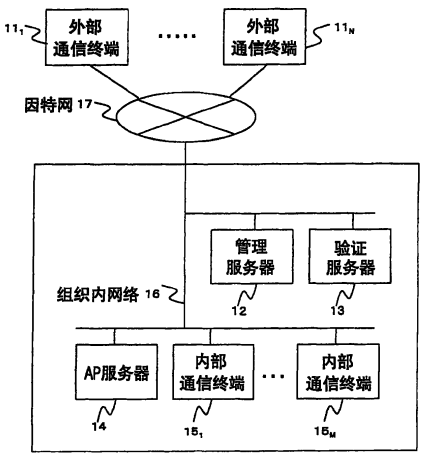
权利要求书 6 页 说明书 32 页 附图 18 页

[54] 发明名称

加密通信方法及系统

[57] 摘要

在利用 VPN 技术的加密通信中，通信终端增加时对 VPN 装置的负荷变大。此外，在外部终端经由内部终端连接到内部的应用服务器的情况下，除了 VPN 中的认证以外还需要进行应用服务器中的认证，处理变得烦杂。本发明中，设有对外部终端、内部终端、应用服务器进行管理的管理服务器，管理服务器对各通信终端的认证和各通信终端间的加密通信通路建立进行居间调节。各通信终端不经由管理服务器而进行加密通信。管理服务器中的各终端的认证委托给验证服务器。此外，在外部终端经由内部终端与应用服务器进行加密通信的情况下，建立外部终端—内部终端间和内部终端—应用服务器间的 2 个加密通信通路并使用它们。



1、一种通信系统，具有连接在组织内网络上的内部通信终端、从组织内网络的外部访问上述内部通信终端的外部通信终端、和管理上述内部通信终端和上述外部通信终端的管理服务器，其特征在于，

通信终端－管理服务器间加密通信通路包括内部通信终端－管理服务器间加密通信通路和外部通信终端－管理服务器间加密通信通路；

上述内部通信终端在与管理服务器之间预先进行认证，建立加密通信通路、即建立内部通信终端－管理服务器间加密通信通路；

上述外部通信终端与管理服务器之间建立外部通信终端－管理服务器间加密通信通路；

上述外部通信终端对管理服务器发送向上述内部通信终端的连接请求；

上述管理服务器生成用来对外部通信终端与内部通信终端间的通信进行加密的加密通信用键，利用预先建立的内部通信终端－管理服务器间加密通信通路，将从外部通信终端向内部通信终端的连接请求和所生成的加密通信用键发送给内部通信终端；

上述内部通信终端将对来自外部通信终端的连接请求的可否的判断应答给管理服务器；

上述管理服务器在从内部通信终端所收到的判断结果为可连接的情况下，利用预先建立的外部通信终端－管理服务器间加密通信通路，将所生成的加密通信用键发送给外部通信终端；

上述外部通信终端和上述内部通信终端分别利用从管理服务器收到的加密通信用键，在外部通信终端与内部通信终端间建立加密通信通路、即建立第一终端－终端间加密通信通路；

上述外部通信终端不经由上述管理服务器，而与内部通信终端之

间进行加密通信；

上述通信系统的结构为，在组织内网络上新连接有提供业务应用的应用服务器，

上述外部通信终端利用所建立的第一终端－终端间加密通信通路，对内部通信终端发送对应用服务器的连接请求；

上述内部通信终端与应用服务器之间建立第二终端－终端间加密通信通路；

上述外部通信终端利用外部通信终端与内部通信终端间的加密通信通路、和内部通信终端与应用服务器间的加密通信通路，经由内部通信终端与应用服务器进行通信。

2、如权利要求 1 所述的通信系统，其特征在于，

新设有进行证书的验证的验证服务器；

上述管理服务器在通信终端－管理服务器间加密通信通路的建立中进行各通信终端的认证时，将该通信终端的证书验证委托给上述验证服务器；

上述验证服务器将实施了该证书的验证处理的结果应答给管理服务器；

上述管理服务器仅在从验证服务器应答的验证结果为成功的情况下，判断为该通信终端的认证成功。

3、如权利要求 1 所述的通信系统，其特征在于，

上述内部通信终端为了与上述应用服务器之间建立第二终端－终端间加密通信通路，将带被认证对象信息的连接请求发送给管理服务器，该带被认证对象信息的连接请求记载有作为通信源终端信息的上述内部通信终端的信息、作为通信目的地终端信息的上述应用服务器的信息和作为被认证对象信息的上述外部通信终端的信息；

上述管理服务器从接收到上述带被认证对象信息的连接请求开始，进行对下述情况的确认，即已经通过上述管理服务器对作为通信

源的上述内部通信终端、作为通信目的地的上述应用服务器和作为被认证对象的上述外部通信终端进行认证的情况，以及作为通信源的上述内部通信终端与作为被认证对象的上述外部通信终端已经建立了上述第一终端－终端间加密通信通路的情况；

上述管理服务器如果进行了上述确认，则生成用来对上述内部通信终端与上述应用服务器间的通信进行加密的加密通信用键，利用预先建立的应用服务器－管理服务器间加密通信通路，将所生成的用来对上述内部通信终端与上述应用服务器间的通信进行加密的加密通信用键和上述带被认证对象信息的连接请求发送给上述应用服务器；

上述应用服务器对从上述内部通信终端发送的作为外部通信终端的连接请求的可否进行判断，将判断结果应答给管理服务器；

上述管理服务器在从上述应用服务器接收到的上述判断结果为可连接的情况下，利用预先建立的上述内部通信终端－管理服务器间加密通信通路将所生成的用来对上述内部通信终端与上述应用服务器间的通信进行加密的加密通信用键发送给上述内部通信终端，建立上述第二终端－终端间加密通信通路；

上述外部通信终端利用上述第一终端－终端间加密通信通路和上述第二终端－终端间加密通信通路，经由上述内部通信终端与上述应用服务器进行通信。

4、如权利要求3所述的通信系统，其特征在于，

上述管理服务器管理认证状态表，该认证状态表中注册有上述外部通信终端和上述内部通信终端和上述应用服务器的地址信息、认证状态、认证时刻；

上述管理服务器将与上述外部通信终端、上述内部通信终端和上述应用服务器的终端之间建立通信终端－管理服务器间加密通信通路中所实施的认证结果预先注册到上述认证状态表中；

上述管理服务器如果从上述内部通信终端接收到上述带被认证

对象信息的连接请求，则对上述通信源终端、上述通信目的地终端和上述被认证对象的终端已成功认证的情况是否注册在上述认证状态表中进行确认。

5、如权利要求3所述的通信系统，其特征在于，

在上述管理服务器对从上述内部通信终端接收的带被认证对象信息的连接请求中所记载的通信源终端和被认证对象的终端已经建立了通信终端－通信终端间加密通信通路的情况进行确认的步骤中，

上述管理服务器对注册有与已经建立的上述第一终端－终端间加密通信通路和上述第二终端－终端间加密通信通路的通信源地址信息、通信目的地地址信息、和通信开始时刻的通信状态表进行管理；

上述管理服务器如果从上述内部通信终端接收到上述带被认证对象信息的连接请求，则通过参照上述通信状态表，确认上述内部通信终端和作为被认证对象的上述外部通信终端是否已经建立了上述第一终端－终端间加密通信通路。

6、一种通信系统，具有连接在组织内网络上的内部通信终端、从组织内网络的外部对上述内部通信终端访问的外部通信终端、管理上述内部通信终端和上述外部通信终端的管理服务器、和提供服务的应用服务器，其特征在于，

上述管理服务器通过生成加密键、并发送给上述外部通信终端和上述内部通信终端，来建立第一终端－终端间加密通信通路，该加密键用来使上述外部通信终端和上述内部通信终端进行不经由该管理服务器的加密通信；

上述外部通信终端利用上述第一终端－终端间加密通信通路，向上述内部通信终端发送控制信息，该控制信息使对上述应用服务器的处理请求开始；

上述内部通信终端根据从上述外部通信终端收到的上述开始控制信息，对上述管理服务器发送向上述应用服务器的连接请求；

上述管理服务器：

通过生成加密键、并发送给上述内部通信终端和上述应用服务器，来建立第二终端－终端间加密通信通路，该加密键用来使上述内部通信终端和上述应用服务器进行不经由该管理服务器的加密通信；

应答从上述外部通信终端收到的开始控制信息，将已经建立了第二终端－终端间加密通信通路的情况通知给上述外部通信终端；

上述外部通信终端应答上述通知，对上述内部通信终端发送控制信息，该控制信息用来向上述应用服务器请求处理；

上述内部通信终端根据从上述外部通信终端收到的处理控制信息，利用上述第二终端－终端间加密通信通路，对上述应用服务器请求处理，

从上述应用服务器接收对上述请求的处理结果，

利用上述第一终端－终端间加密通信通路向上述外部通信终端发送基于上述处理结果的处理结果信息。

7、如权利要求 6 所述的通信系统，其特征在于，

上述处理控制信息是用来从上述外部通信终端操作上述内部通信终端的输入操作信息；

上述处理结果信息是为了在上述外部通信终端的显示画面上显示上述应用服务器的处理结果而由上述内部通信终端生成的画面显示信息。

8、如权利要求 6 所述的通信系统，其特征在于，

上述处理控制信息是上述外部通信终端对上述内部通信终端发行的处理请求命令；

上述处理结果信息是下述命令的返回值，该命令表示上述应用服务器的上述处理请求命令的处理结果。

9、如权利要求 6 所述的通信系统，其特征在于，

上述内部通信终端在发送对上述应用服务器的连接请求时，发送

带被认证对象信息的连接请求，该带被认证对象信息的连接请求表示上述外部通信终端被认证、与上述内部通信终端之间建立了上述第一终端－终端间加密通信通路。

10、如权利要求 7 所述的通信系统，其特征在于，

上述管理服务器在生成用来分别建立第一终端－终端间加密通信通路和第二终端－终端间加密通信通路的加密键时，

分别认证上述外部通信终端、上述内部通信终端、上述应用服务器，

并管理认证结果。

11、如权利要求 6 所述的通信系统，其特征在于，

上述管理服务器在认证上述外部通信终端时，认证上述外部通信终端的使用者。

12、如权利要求 6 所述的通信系统，其特征在于，

上述管理服务器将上述第一终端－终端间加密通信通路的通信状态和上述第二终端－终端间加密通信通路的通信状态建立关联来管理。

加密通信方法及系统

技术领域

本发明涉及经由因特网等通信网进行加密通信的技术。

背景技术

为了从自宅的通信终端适当地访问企业的信息资产、或将企业的各据点的局域网彼此安全地连接而利用 VPN（Virtual Private Network: 虚拟专用网）的技术。

例如，对连接在因特网等外部网络上的外部通信终端（以下有时称作外部终端）和连接公司等组织内网络上的内部通信终端（以下有时称作内部终端）进行安全通信的情况进行说明。

首先，外部通信终端从因特网对处于组织内网络的入口的 VPN 装置发送向内部通信终端的连接请求。这里，VPN 装置利用公钥证书（以下记作证书）等进行外部通信终端的认证，确认是能够对内部通信终端访问的终端。此外，外部通信终端利用证书等进行 VPN 装置的认证。

如果外部通信终端与 VPN 装置能够相互认证，则在外部通信终端与 VPN 装置间公用加密键（暗号化鍵），利用加密键将在该两者间交换的数据加密。此外，VPN 装置对内部通信终端连接、进行外部通信终端所需的数据的中介。

这样，外部通信终端能够经由 VPN 装置与内部通信终端进行通信。此外，在外部通信终端与 VPN 装置之间交换的数据由于被加密，所以能够进行安全的通信。

例如，在非专利文献 1 中公开了提供 VPN 技术的设备的功能说

明。

【非专利文献 1】NORTEL NETWORKS，“Alteon SSL VPN”，（在线），NORTEL NETWORKS，P.2-3，（平成 17 年 5 月 11 日检索），因特网 <http://www.nortel.com/products/01/alteon/sslvpn/collateral/nn102960-073103.pdf>

在采用以往的 VPN 技术的安全通信方法中，由于所交换的所有的数据都经由VPN装置收发，所以存在VPN装置的负荷变大的问题。

例如，在存在多台外部通信终端及内部通信终端、在各通信终端间进行多个安全通信的情况下，在 VPN 装置中进行多个外部通信终端的认证处理以及在通信终端间交换的所有数据的加密处理。因此，有 VPN 装置中的负荷变大的问题。

进而，作为另一个课题，在组织内网络上连接有提供业务应用（application）及数据库等的应用服务器（以下有时称作 AP 服务器）的情况下，在外部通信终端经由内部通信终端访问应用服务器时需要进行多个认证处理。

例如，在连接在因特网上的外部通信终端远程访问连接在公司内的网络上的内部通信终端而进行作业的情况下，在从内部通信终端利用应用服务器的服务的情况下，除了 VPN 装置中的认证处理之外，还需要应用服务器中的认证处理、例如输入用户 ID、密码等，存在密码的管理变得烦杂的问题。

此外，在以往的 VPN 技术中，存在下述课题，即若不预先考虑对 VPN 装置和内部通信终端之间以及内部通信终端和 AP 服务器之间的通信加密，而是为了确保安全性，对外部通信终端和 AP 服务器之间的通信通路整体进行加密，则为此的处理很繁琐。

发明内容

本发明是鉴于上述情况而做出的，其目的是提供一种分散安全通

信中的负荷、对通信通路整体加密的技术、以及/或在从外部通信终端经由内部通信终端访问应用服务器等组织内通信终端的情况下使认证简单化、并且能够确保更高的安全性的技术。

为了实现上述目地，在本发明中，提供一种配备有对外部通信终端、内部通信终端、和应用服务器进行管理的管理服务器的通信系统。

在本发明的通信系统中，通过进行以下的步骤，在外部通信终端和内部通信终端之间进行安全通信。此外，对于外部通信终端经由内部通信终端与应用服务器进行安全通信的步骤也进行说明。

首先，说明外部通信终端与内部通信终端开始安全通信的情况。

外部通信终端连接到与组织内网络的入口连接的管理服务器，外部通信终端和管理服务器相互进行认证。另外，在需要严格的认证的情况下只要进行利用公钥证书的认证就可以。

如果相互认证成功，则在外部通信终端与管理服务器之间共用用来将所交换的数据加密的加密键，建立外部通信终端与管理服务器间的加密通信通路。

此外，在内部通信终端和管理服务器之间，也预先进行与上述同样的处理，建立内部通信终端与管理服务器间的加密通信通路。

外部通信终端在建立了与管理服务器的加密通信通路之后，对管理服务器发送向内部通信终端的连接请求。管理服务器确认已经分别认证了外部通信终端及内部通信终端，生成在外部通信终端和内部通信终端通信之间的加密通信中所使用的加密键和设定信息。并且，通过与内部通信终端之间建立的加密通信通路，从外部通信终端发送对内部通信终端的连接请求、加密键和设定信息。

内部通信终端判断外部通信终端是否能向内部通信终端连接，将其结果发送给管理服务器。

在外部通信终端与内部通信终端为可连接的情况下，管理服务器将可以连接的消息和在外部通信终端与内部通信终端之间的加密通

信中使用的加密键及设定信息发送到外部通信终端。

此外，所谓的设定信息，例如是加密键的算法的种类以及键长、IP 地址及端口等为了进行加密通信所需的信息中的任意的一个以上的组合。

利用该加密键和设定信息，在外部通信终端与内部通信终端之间建立加密通信通路，进行安全的通信。另外，在本发明中，将进行通信的 2 个装置相互具有可加密通信的键的情况看作已建立了加密通信通路。

接着，对外部通信终端经由内部通信终端访问应用服务器的 2 个方法进行说明。例如，在外部通信终端远程访问内部通信终端、从内部通信终端利用应用服务器的情况下，进行以下的 2 个方法中的某一个来进行安全通信。

对第一个方法进行说明。首先，通过上述方法在外部通信终端与内部通信终端之间建立不经由管理服务器的加密通信通路。外部通信终端利用已建立的加密通信通路，对内部通信终端发送内容为指示向应用服务器的连接请求的键输入信息。

内部通信终端通过外部通信终端的操作，为了与应用服务器之间建立加密通信通路而执行上述同样的步骤。即，内部通信终端及应用服务器分别与管理服务器之间建立加密通信通路。另外，这里，假设应用服务器预先与管理服务器之间建立了加密通信通路。此外，在内部通信终端已经建立了与管理服务器的加密通信通路的情况下，不需要再次建立加密通信通路。

在建立了各个加密通信通路后，内部通信终端对管理服务器发送向应用服务器的连接请求。管理服务器检查是否已认证了应用服务器、在与应用服务器之间是否已经建立了加密通信通路，如果没有，则通过与内部通信终端的情况同样的处理进行认证及/或加密通信通路的建立，生成在内部通信终端与应用服务器间的加密通信中所使用

的加密键和设定信息。并且，经由与应用服务器之间建立的加密通信通路将来自内部通信终端的连接请求和加密键及设定信息发送给应用服务器。

应用服务器判断内部通信终端是否能够与应用服务器连接，将其结果发送给管理服务器。

在结果是可连接的情况下，管理服务器将可以连接的信息、在内部通信终端与应用服务器不经由管理服务器而进行的加密通信中所使用的加密键和设定信息发送给内部通信终端。

利用该加密键和设定信息，应用服务器和内部通信终端建立不经由管理服务器的加密通信通路。

在外部通信终端经由内部通信终端访问应用服务器的情况下，利用这些已建立的 2 个加密通信通路（外部通信终端－内部通信终端间以及内部通信终端－应用服务器间），进行安全的通信。

接着说明第二个方法。在第二个方法中，在第一个方法中并没有成为向应用服务器访问时的认证对象的外部终端新作为新的认证对象。

首先，通过与第一个方法同样的方法，在外部通信终端与内部通信终端之间建立不经由管理服务器的加密通信通路。外部通信终端利用已建立的加密通信通路对内部通信终端发送内容为指示经由内部通信终端向应用服务器连接的请求的键输入信息。

收到该信息后，内部通信终端为了在内部通信终端与应用服务器之间建立加密通信通路而执行以下的步骤。

内部通信终端及应用服务器分别与管理服务器建立加密通信通路。另外，这里假设应用服务器预先与管理服务器之间建立了加密通信通路。此外，在内部通信终端已经建立了与管理服务器的加密通信通路的情况下，不需要再次建立加密通信通路。

在建立了各个加密通信通路之后，内部通信终端对管理服务器基

于来自外部通信终端的操作发送对上述应用服务器的连接请求。在此时发送的连接请求中所记述的内容是对向应用服务器的连接请求源是外部通信终端。收到该连接请求的管理服务器对已分别认证外部通信终端、内部通信终端、应用服务器的情况、以及外部通信终端与内部通信终端处于加密通信中的情况进行确认。管理服务器如果确认了这些，则生成在内部通信终端与应用服务器间的通信中所使用的加密键和设定信息。并且，经由与应用服务器之间建立的加密通信通路，将从内部通信终端接收的、经由内部通信终端从外部通信终端向应用服务器连接的请求和加密键及设定信息发送给应用服务器。

应用服务器判断外部通信终端是否能够经由内部通信终端与应用服务器连接，将其结果发送给管理服务器。

在结果是可连接的情况下，即在应用服务器能够认证外部通信终端和内部通信终端这两者的情况下，管理服务器将可以连接的消息、在内部通信终端和应用服务器不经由管理服务器而进行的加密通信中所使用的加密键和设定信息，发送给内部通信终端。

应用服务器和内部通信终端利用该加密键建立不经由管理服务器的加密通信通路。

在外部通信终端经由内部通信终端访问应用服务器的情况下，利用这些已经建立的 2 个加密通信通路（外部通信终端－内部通信终端间以及内部通信终端－应用服务器间）进行安全通信。

这里，内部通信终端及应用服务器也可以不预先进行、而是根据外部通信终端的连接请求进行与管理服务器的认证和加密通信通路的建立。例如，可以在从多个通信终端频繁地接收连接请求的应用服务器中，预先建立了与管理服务器的加密通信通路，在从内部通信终端向管理服务器存在对应用服务器的连接请求的情况下，立即进行处理。此外，也可以在从确定的外部终端很少接收连接请求那样的应用服务器中，在进行连接请求的时刻进行与管理服务器的认证，建立加

密通信通路。

此外，内部通信终端和应用服务器之间的通信通路在没有必要时也可以不进行加密。

进而，在管理服务器进行外部通信终端、内部通信终端、应用服务器的认证时，也可以将证书的验证委托给验证证书的证书验证服务器装置（以下记作验证服务器）。通过验证服务器验证该证书，能够进行更可靠的认证。

此外，管理服务器也可以由第三方的组织运营。即，管理服务器也可以连接到与内部通信终端不同的组织内网络上。

根据上述技术方案，在建立了外部通信终端与内部通信终端间、以及内部通信终端与应用服务器间的加密通信通路后，能够不经由管理服务器进行加密通信。因此，与以往技术相比，能够减轻对管理服务器的负荷。进而，由于可以对通信通路整体进行加密，所以与以往的技术相比，可以进行更加安全的通信。

此外，根据本发明，在外部通信终端经由内部通信终端访问应用服务器的情况下，如果进行了通过管理服务器的外部通信终端、内部通信终端、应用服务器的认证，则能够基于该认证结果，通过外部通信终端的操作来访问应用服务器，而不需要另外进行 ID/密码等应用服务器固有的认证。即，管理服务器集中地进行外部通信终端、内部通信终端、应用服务器等各通信终端的认证，由此各通信终端不再需要进行多个认证处理。由此能够使认证简单化。

此外，在通过管理服务器进行的认证中，可以进行基于 PKI 的严格认证。

根据本发明，在外部通信终端与内部通信终端间以及内部通信终端与应用服务器间的加密通信中，能够减轻对管理服务器的负荷。进而，可以在从外部通信终端到应用服务器之间的通信通路整体中，进行更加安全的通信。

此外，根据本发明，在外部通信终端经由内部通信终端访问应用服务器的情况下，应用服务器不需要进行外部通信终端的认证。即，能够使认证处理简单化。

附图说明

图 1 是例示本发明的 2 个实施方式的通信系统的结构的图。

图 2 是例示外部终端 11、内部终端 15、AP 服务器 14 的概略结构的图。

图 3 是例示管理服务器 12 的概略结构的图。

图 4 是例示验证服务器 13 的概略结构的图。

图 5 是例示外部终端 11、内部终端 15、AP 服务器 14、管理服务器 12、验证服务器 13 各自的硬件结构例的图。

图 6 是例示到外部终端 11 和管理服务器 12 为了建立外部终端－管理服务器间加密通信通路而进行相互认证为止的处理顺序的流程图。

图 7 是例示到外部终端 11 和管理服务器 12 建立外部终端－管理服务器间加密通信通路、将其结束为止的处理顺序的流程图。

图 8 是例示内部终端 15 将内部终端 15 的地址注册到管理服务器 12 中的处理顺序的流程图。

图 9 是例示到在外部终端 11 与内部终端 15 进行连接处理时、管理服务器 12 对内部终端进行连接请求为止的处理顺序的流程图。

图 10 是例示到在外部终端 11 与内部终端 15 进行连接处理时、建立了外部终端 11 与内部终端 15 间的终端－终端间加密通信通路、将其结束为止的处理顺序的流程图。

图 11 是例示在实施方式 1 中、到外部终端 11 经由内部终端 15 向 AP 服务器 14 连接时、建立外部终端 11－内部终端 15 间、和内部终端－AP 服务器 14 间的内部终端－AP 服务器间加密通信通路为止

的处理顺序的流程图。

图 12 是例示在实施方式 1 中、到外部终端 11 经由内部终端 15 向 AP 服务器 14 连接时、利用加密通信通路发送信息为止的处理顺序的流程图。

图 13 是例示在实施方式 2 中、到外部终端 11 经由内部终端 15 向 AP 服务器 14 连接时、建立终端－终端间加密通信通路为止的处理顺序的流程图。

图 14 是例示在实施方式 2 中、到外部终端 11 经由内部终端 15 向 AP 服务器 14 连接时、建立内部终端－AP 服务器间加密通信通路为止的处理顺序的流程图。

图 15 是例示在实施方式 2 中、到外部终端 11 经由内部终端 15 向 AP 服务器 14 连接时、利用加密通信通路发送信息为止的处理顺序的流程图。

图 16 是例示在实施方式 2 中、管理服务器所保持的认证状态表的内容的图。

图 17 是例示在实施方式 2 中、管理服务器所保持的通信状态表的内容的图。

图 18 是例示在实施方式 2 中、例示外部终端 11 经由内部终端 15 向 AP 服务器 14 连接时、外部终端 11 的经由内部终端 15 与 AP 服务器 14 的连接请求的内容的图。

具体实施方式

下面说明本发明的 2 个实施方式。

此外，在以下的实施例中所使用的 ID、地址、域名等是为了说明而使用的虚构的名称，如果有实际存在者也与之没有关系。

<实施方式 1>

图 1 是例示有关本发明的一实施方式的通信系统的结构的图。

本实施例的通信系统具有因特网等外部网络（称作因特网）17、与因特网 17 连接的外部通信终端 11_1～外部通信终端 11_N（统称为“外部终端 11”）、和与因特网 17 连接的组织内网络 16。虽然没有图示，但因特网 17 与组织内网络 16 也可以经由称作防火墙的防止在相互间进行不正当的通信的装置来连接。在此情况下，外部终端 11 与管理服务器 12 之间的通信预先设定为不会被防火墙隔断。此外，各网络是有线、无线中的哪一种网络都可以。

此外，在组织内网络 16 上，连接着对组织内的利用者提供业务应用及数据库等的 AP 服务器 14、保管有组织内的利用者所利用的数据的内部通信终端 15_1～内部通信终端 15_M（统称为“内部终端 15”）、管理各通信终端间的通信的管理服务器 12、在通信终端的认证中验证证书的验证服务器 13。另外，管理服务器 12 及/或验证服务器 13 也可以是由与内部终端 15 及 AP 服务器 14 不同的组织来运营、连接在其他组织内网络上的结构。

接着说明构成图 1 的通信系统的各装置。

首先，利用图 2 说明外部终端 11、内部终端 15、AP 服务器 14。另外，在以下的说明中，在不区别这些装置时包括 AP 服务器 14 都单称作“通信终端”或“终端”。

通信终端具有处理部 20a、存储部 20b、进行通信结果的显示及来自用户的指示的受理的输入输出部 20c、和用来经由因特网 17 及组织内网络 16 与其他装置进行通信的通信部 20d。

处理部 20a 具有用来对确定该通信终端的网络上的位置的地址进行注册的地址注册申请部 21、进行与管理服务器 12 的针对通信处理的管理服务器通信处理部 22、进行与对方的通信终端的通信处理的针对终端通信处理部 23、和统一地控制通信终端的各部分的控制部 24。

存储部 20b 具有对在管理服务器 12 认证该通信终端时使用的该

通信终端的密钥与公钥证书进行保持的密钥·证书保持部 25、和在将通信加密中使用的加密键保持部 26。

接着利用图 3 说明管理服务器 12。

管理服务器 12 具有处理部 30a、存储部 30b、进行通信结果的显示及来自用户的指示的受理的输入输出部 30c、和用来经由组织内网络 16 与其他装置或连接在因特网 17 上的其他装置进行通信的通信部 30d。

处理部 30a 具有：地址注册/检索部 31，接受来自通信终端的地址注册申请，将地址注册在地址 DB37 中，或检索通信终端的地址；键生成·分发部 32，生成用来将通信终端一通信终端间的通信加密的加密键，向通信终端分发；针对终端通信处理部 33，进行与通信终端的通信处理；针对验证服务器通信处理部 34，进行与验证服务器 13 的通信处理；控制部 34，统一地控制管理服务器 12 的各部分。

存储部30b具有对在通信终端认证该管理服务器时所使用的该管理服务器 12 的密钥与公钥证书进行保持的密钥·证书保持部 36、和保持通信终端的地址的地址 DB37。

接着利用图 4 说明验证服务器 13。

验证服务器 13 具有处理部 40a、存储部 40b、进行验证结果的显示及来自用户的指示的受理的输入输出部 40c、和用来经由组织内网络 16 与其他装置或连接在因特网 17 上的其他装置进行通信的通信部 40d。

处理部 40a 具有：认证路径检索部 41，针对从管理服务器 12 受理的验证请求，检索认证路径，该认证路径表示从管理服务器所信赖的认证机构的证书到作为验证对象的通信终端的证书之间的信赖关系；认证路径验证部 42，验证由认证路径检索部 41 检索到的验证路径；针对管理服务器通信处理部 43，进行与管理服务器 12 的通信处理；控制部 44，统一地控制验证服务器 13 的各部分。

存储部 40b 具有在认证路径检索部 41 检索认证路径时保持从认证机关取得的证书及失效信息的证书保持部 45。

另外，图 2～图 4 所例示的通信终端、管理服务器 12、验证服务器 13 的各个处理部例如可以在图 5 所例示那样的介质一般的电子计算机中，通过 CPU51 执行装载在存储器 52 上的规定的程序来具体实现，该一般的电子计算机具备 CPU51、存储器 52、硬盘等外部存储装置 53、用来经由因特网 17 及组织内网络 16 与其他装置进行通信的通信装置 54、键盘及鼠标等输入装置 55、显示装置及打印机等输出装置 56、从具有可移动性的存储介质 58 读取信息的读取装置 57、和将这些各装置间连接的内部通信线 50。

这些程序也可以预先保存在上述电子计算机内的存储器 52 或外部存储装置 53 中，在需要时，也可以从上述电子计算机可利用的可拆装的存储介质 58、或经由通信介质（因特网 17 或组织内网络 16 等、或在它们上传输的载波或数字信号等）从其他装置导入。

此外，在本实施例中，通信终端可以通过图 5 所示那样的结构实现，但本发明并不限于此。图 2 所例示的通信终端也可以是具备与能够将因特网 17 及组织内网络 16 连接的通信装置 54 相当的功能的设备。例如，通过不仅使路由器、PC、PDA、而且使电视机、冰箱、空调、电灶等家用电器也具备类似于图 5 的结构，也可以成为通信终端。

此外，也可以将上述各个处理部作为硬件来构成。

接着说明本实施方式的通信系统的动作。

本实施方式的通信系统的动作包括通信终端－管理服务器间的加密通信通路建立动作、和通信终端－通信终端间的加密通信通路建立动作。

图 6 和图 7 是用来说明本实施方式的通信终端－管理服务器间的加密通信通路建立动作的流程图，是在内部终端 15 和管理服务器 12

之间建立加密通信通路（称作通信终端一管理服务器间加密通信通路）的情况的例子。

内部终端15的针对管理服务器通信处理部22为了认证管理服务器12而对管理服务器12发送管理服务器12证书的请求（图6的步骤1001）。接收到该请求的管理服务器12的针对终端通信处理部33（步骤1002）从密钥·证书保持部26取出该管理服务器的证书并应答，并且将对方的内部终端15的证书请求对内部终端15发送（步骤1003）。接收到该证书请求的内部终端15的针对管理服务器通信处理部22（步骤1004），从密钥·证书保持部36中取出该内部终端15的证书，对管理服务器12发送（步骤1005）。

内部终端15的针对管理服务器通信处理部22进行对在步骤1004中接收的管理服务器12的证书的验证（步骤1007），检查管理服务器12不是伪装的。在管理服务器12的证书验证失败的情况下（步骤1008中的否），由于不能进行管理服务器的认证，所以结束通信（步骤11071）。在管理服务器12的证书验证成功的情况下（步骤1008中的是），进入下一个步骤。

管理服务器12的针对终端通信处理部33从内部终端15接收证书（步骤1006），为了验证该证书，通过针对验证服务器通信处理部34对验证服务器13发送内部终端15证书的验证请求（步骤1009）。

证书验证服务器13接收验证请求（步骤1010），在认证路径检索部41中进行认证路径检索处理，在认证路径验证部42进行该检索到的认证路径的验证（步骤1011）。在内部终端15证书的验证成功的情况下（步骤1012中的是），验证服务器13的针对管理服务器通信处理部43将证书验证成功的内容的通知发送给管理服务器12（步骤1013）。在内部终端15证书的验证失败的情况下（步骤1012中的否），针对管理服务器通信处理部43将证书验证失败的内容的通知发送给管理服务器12（步骤1014）。

管理服务器12的针对终端通信处理部33经由针对验证服务器通信处理部34从验证服务器13接收验证结果（步骤1015），在该验证结果为失败的情况下（步骤 1016 中的否），由于不能进行内部终端15的认证，所以结束通信（图7中的步骤1107）。在内部终端15证书的验证结果为成功的情况下（步骤1016中的是），进入下一个步骤。

内部终端 15 与管理服务器 12 如果能够相互认证（在步骤 1008 中为是，并且在步骤1016中为是），则内部终端15的针对管理服务器通信处理部22和管理服务器12的针对终端通信处理部33互相共用用来对通信通路加密的密钥（图7中的步骤1101、步骤1102）。作为用来共用密钥的方法，例如可以使用作为RFC2246被IETF标准化的TLS（Transport Layer Security，传输层安全）。如果共用了密钥，则能够进行内部终端15与管理服务器12之间的认证及加密通信通路的建立，所以管理服务器12的地址注册/检索部31将内部终端15的IP 地址和认证结果（这里表示认证成功的内容）建立对应，注册到图16所示的认证状态表60中（步骤1103）。具体而言，将内部终端15的IP地址注册到终端的IP地址62中，将表示认证成功的内容的消息及其时刻注册到认证结果 63 及认证时刻 64 中。该认证状态表60是用来管理该管理服务器12通信的通信终端的状态的表，被保持在管理服务器12进行的地址DB37中。

通过进行到此为止的处理，内部终端15与管理服务器12之间的加密通信通路建立处理结束（步骤 1104），内部终端 15 的针对管理服务器通信处理部22和管理服务器12的针对终端通信处理部33利用该密钥进行加密通信（步骤1105、1106）。

加密通信结束后，内部终端15的针对管理服务器通信处理部22和管理服务器12的针对终端通信处理部33开放加密通信通路（步骤1107）。另外，例如可以通过使在加密通信中使用的加密键无效化来实现开放加密通信通路。

接着，管理服务器 12 的地址注册/检索部 31 将在步骤 1103 中注册的该内部通信终端 15 的 IP 地址和认证结果从保持在地址 DB37 中的认证状态表 60 中删除。另外，在将通信终端的 IP 地址固定地注册在认证状态表 60 中的情况下，也可以不删除通信终端的 IP 地址。

通过执行这样的步骤，内部终端 15 和管理服务器 12 在相互确认对方后，能够建立加密通信通路。

接着说明在通信终端一通信终端间的加密通信通路建立动作。

为了建立在通信终端一通信终端间的加密通信通路，需要预先将通信终端的地址信息注册在管理服务器 12 中。所谓的地址信息，是指将确定通信终端的信息（以下称作终端 ID）和表示网络上的地点的地址（例如 IP 地址）相对应的信息。在终端 ID 中可以使用在域内固定的 ID。此时的 ID 的固定是指能够在域内确定终端、且不变化。例如，在可携带的终端的情况下，IP 地址有可能根据连接到网络上的地点而变化，但可以将其他不变的信息、例如通信终端名、通信终端的 MAC 地址作为终端 ID 使用。此外，在公司内那样封闭的域中，也可以将通信终端的用户的邮件地址、通信终端的 SIP-URI、通信终端的 FQDN（完全资格域名，Fully Qualified Domain Name）那样的信息作为终端 ID 使用。在图 8 中进行地址注册动作的说明。

图 8 是用来说明通信终端将自己的地址向管理服务器 12 注册的动作的流程图，是内部终端 15 向管理服务器 12 注册地址的情况的例子。

首先，内部终端 15 与管理服务器 12 通过实施从图 6 的步骤 1001 到步骤 1016、从图 7 的步骤 1101 到步骤 1104，建立内部终端一管理服务器间加密通信通路（步骤 2001）。在内部终端一管理服务器间加密通信通路建立后，内部终端 15 的地址注册申请部 21 将该内部终端 15 的地址的注册申请发送给管理服务器 12（步骤 2002）。管理服务器 12 的地址注册/检索部 31 如果接收到注册申请（步骤 2003），则将

内部终端 15 的终端 ID 与 IP 地址建立对应，注册到保持在地址 DB37 中的认证状态表 60 中（步骤 2004）。具体而言，从认证状态表 60 的终端的 IP 地址 62 中检索该内部终端 15 的 IP 地址，与检索到的 IP 地址建立对应、将该内部终端的终端 ID 注册到终端的地址 61 中。在认证状态表 60 中没有检测到该内部终端的 IP 地址的情况下，将该内部终端 15 的终端 ID 和 IP 地址新注册到终端的地址 61 和终端的 IP 地址 62 中。在注册结束后，对内部终端 15 发送注册结束通知（步骤 2005）。内部终端 15 如果接收到注册结束通知（步骤 2006），则内部终端 15 与管理服务器 12 执行内部终端一管理服务器间加密通信通路的结束处理。通过执行上述步骤，能够将内部终端 15 的地址注册到管理服务器 12 中。

其他通信终端、例如外部终端 11 也可以通过执行与图 8 同样的步骤，将该外部终端 11 的地址注册到管理服务器 12 中。

进而，通信终端也可以将注册在管理服务器 12 中的地址删除。在删除的情况下，在图 8 所示的处理中进行将“注册”替换（换读）为“删除”的处理。

此外，在分配给该通信终端的地址发生了变化的情况下，需要再次执行图 8 的地址注册处理。例如，在通信终端动态地接受地址分配的情况下，如果将通信终端的电源关闭、开启、或将通信终端重启，则地址有可能变化。此外，在通信终端结束了与网络的连接并在移动目的地连接到其他网络上的情况下，地址有可能变化。在这样的情况下，通信终端通过再次进行图 8 的注册处理，将最新的地址注册到管理服务器 12 中。

进而，在固定地设定该通信终端的 IP 地址和终端 ID 的情况下，只要预先将该通信终端的地址注册就可以，在此情况下不需要删除地址信息。

图 9 和图 10 是用来说明在通信终端与通信终端间经由管理服务

器所进行的、建立不经由管理服务器的加密通信通路的动作的流程图，是在外部终端 11－内部终端 15 间建立加密通信通路（称作终端－终端间加密通信通路）时的例子。

首先，管理服务器 12 与内部终端 15 通过预先实施从图 6 的步骤 1001 到步骤 1016、从图 7 的步骤 1101 到步骤 1104，建立内部终端－管理服务器间加密通信通路（步骤 3001）。并且，在内部终端 15 还没有注册自身的地址的情况下，通过实施从图 8 的步骤 2002 到步骤 2006，将内部终端 15 的地址注册到管理服务器 12 中（步骤 3002）。

在外部终端 11 想要与内部终端 15 开始通信的时刻等，外部终端 11 和管理服务器 12 通过实施从图 6 的步骤 1001 到步骤 1016、从图 7 的步骤 1101 到步骤 1104，建立外部终端－管理服务器间加密通信通路（步骤 3003）。并且，在外部终端 11 还没有注册自身的地址的情况下、或者在需要进行注册地址的更新的情况下，通过实施从图 8 的步骤 2002 到步骤 2006 的步骤，将外部终端 11 的地址注册到管理服务器 12 中（步骤 3004）。

在建立了外部终端－管理服务器间加密通信通路后，外部终端 11 的针对管理服务器通信处理部 22 将向内部终端 15 的连接请求发送给管理服务器 12（步骤 3005）。另外，在连接请求中包含有作为确定连接对象（内部终端 15）的信息的终端 ID。

接收到连接请求的管理服务器 12 的针对终端通信处理部 33（步骤 3006）通过地址注册/检索部 31，以终端 ID 为键标从认证状态表 60 中检索内部终端 15 的地址（步骤 3007）。在认证状态表 60 中，在与该内部通信终端 15 相对应的认证结果 63 中没有注册表示认证成功内容的消息的情况下，即在没有建立加密通信通路的情况下（步骤 3008 中的否），管理服务器 12 的针对终端通信处理部 33 在与内部终端 15 之间进行加密通信通路建立处理（步骤 3009），进入步骤 3011。在认证状态表 60 中，在与该内部通信终端 15 相对应的认证结果 63

中注册有表示认证成功内容的消息的情况下（步骤 3008 中的是），管理服务器 12 的键生成·分发部 32 生成在将两终端间的通信通路加密中所利用的加密键及设定信息（步骤 3010）。接着，管理服务器 12 的针对终端通信处理部 33 对内部终端 15 发送从外部终端 11 对内部终端 15 的连接请求、和在步骤 3010 中生成的加密键及设定信息（步骤 3011）。此时，连接请求及加密键等利用内部终端一管理服务器间加密通信通路进行发送。

内部终端 15 的针对管理服务器通信处理部 22 将从管理服务器 12 接收到的加密键和设定信息（步骤 3012）保存到加密键保持部 26 中。接着，判断该外部终端 11 是否能够与该内部终端 15 连接（步骤 3013），将该判断结果发送给管理服务器 12（步骤 3014）。管理服务器 12 的针对终端通信处理部 33 从内部终端 15 接收判断结果（步骤 3015）。

管理服务器 12 的针对终端通信处理部 33 在判断结果是外部终端 11 不能与内部终端 15 连接的情况下（步骤 3101 中的否），将表示不能连接内容的判断结果发送给外部终端 11（步骤 3102），结束终端一终端间加密通信通路建立处理。

在外部终端 11 能够与内部终端 15 连接的情况下（步骤 3101 中的是），管理服务器 12 的针对终端通信处理部 33 将表示能够连接内容的判断结果、和在步骤 3010 中生成的加密键及设定信息发送给外部终端 11（步骤 3103）。此时，至少加密键使用外部终端一管理服务器间加密通信通路进行发送。

外部终端 11 的针对管理服务器通信处理部 22 从管理服务器 12 接收是否能够与内部终端 15 通信的判断结果，进而在接收到加密键的情况下，将该加密键保存到加密键保持部 26 中（步骤 3104）。

外部终端 11 及内部终端 15 在判断结果为不能连接的情况下（步骤 3105、3106 中为否），结束终端一终端间加密通信通路建立处理。在判断结果为能够通信的情况下（步骤 3105、3106 中为是），在外部

终端 11 与内部终端 15 之间建立终端－终端间加密通信通路（步骤 3107）。利用该终端－终端间加密通信通路，外部终端 11 的针对终端通信处理部 23 和内部终端 15 的针对终端处理部 23 能够交换信息（步骤 3108）。

如果不再需要外部终端 11 与内部终端 15 间的通信通路，则能够结束终端－终端间加密通信通路。在结束终端－终端间加密通信通路的情况下进行以下的步骤。

外部终端 11 的针对管理服务器通信处理部 22 对管理服务器 12 发送与内部终端 15 的加密通信的切断请求（步骤 3109）。管理服务器 12 的针对终端通信处理部 33（步骤 3110）将接收到的该连接请求向内部终端 15 传送（步骤 3111）。内部终端 15 的针对管理服务器通信处理部 22 如果接收到该切断请求（步骤 3112），则将与其对应的切断应答向管理服务器 12 发送（步骤 3113），针对终端通信处理部 23 结束与外部终端 11 的终端－终端间加密通信通路（步骤 3117）。此外，管理服务器 12 的针对终端通信处理部 33 如果从内部终端 15 接收到切断应答（步骤 3114），则将该切断应答向外部终端 11 传送（步骤 3115）。在外部终端 11 中，针对管理服务器通信处理部 22 如果从管理服务器 12 接收到切断应答（步骤 3116），则针对终端通信处理部 23 结束与内部终端 15 的终端－终端间加密通信通路（步骤 3117）。

另外，也可以不是从外部终端 11 发送切断请求，而是从内部终端 15 发送。在此情况下，只要将外部终端 11 与内部终端 15 替换来进行从步骤 3109 到步骤 3117 的处理就可以。

此外，外部终端 11 与内部终端 15 并不一定必须为了结束通信而进行从步骤 3109 到步骤 3117，也可以不进行该步骤来结束通信。

如图 9 和图 10 的流程图所例示那样，管理服务器 12 分别认证外部终端 11 和内部终端 15，在能够确认该各通信终端的正当性的情况

下，建立外部终端 11 与内部终端 15 间的加密通信通路。并且，由于在建立了终端－终端间加密通信通路后，能够不经由管理服务器 12 而在通信终端彼此间进行加密通信，所以能够不对管理服务器 12 施加负荷而进行安全通信。进而，由于终端－终端间加密通信通路整体被加密，所以可以进行比以往更加安全的通信。

在本实施方式中，在建立终端－终端间加密通信通路时，作为通信对方的通信终端（在上述实施例中为内部终端 15）和管理服务器 12 预先建立通信终端－管理服务器间加密通信通路，实施地址注册处理（步骤 3001、步骤 3002），但并不限于此。也可以预先实施作为通信对方的内部终端 15 的地址注册，或者在静态地进行了地址注册的状态下，通信源的通信终端（在上述实施例中为外部终端 11）向管理服务器 12 进行了向通信目的地的通信终端的连接请求后（步骤 3008 中的“是”的时刻），进行通信目的地通信终端与管理服务器 12 之间的加密通信通路建立。

例如，在为其他终端提供服务的应用服务器等从多个通信终端频繁地接收连接请求那样的通信终端的情况等，也可以与上述实施方式所示的内部终端的情况同样，预先建立与管理服务器 12 的加密通信通路，在从内部终端 15 有连接请求的情况下，马上与终端－终端间的情况同样地建立通信通路，从而能够提供服务。

与此相对，在内部终端 15 从外部终端 11 接收连接请求的频率较低的情况下，也可以是在从外部终端 11 向该内部终端 15 进行了连接请求的时刻进行内部终端 15 与管理服务器 12 间的加密通信通路建立处理的方式。

接着，在本实施方式的通信系统中，说明外部终端 11 经由内部终端 15 访问 AP 服务器 14 的情况的动作。例如，在连接在因特网上的外部终端 11 远程访问连接到公司内的网络上的内部终端 15 来进行作业的情况下，存在从内部终端 15 利用 AP 服务器 14 的服务的情况

等。在此情况下，从外部终端 11 对内部终端 15 发送键盘及鼠标的输入信息，根据该信息，内部终端 15 在与 AP 服务器 14 之间进行信息交换。此外，内部终端 15 将在与 AP 服务器 14 之间进行信息交换的结果的画面信息等从内部终端 15 发送给外部终端 11，提供给利用者。

图 11 和图 12 是在本实施方式中用来说明外部终端 11 经由内部终端 15 访问 AP 服务器 14 时的动作的流程图。

在图 11、图 12 的处理中，AP 服务器 14 只要看作内部终端 15 之一就可以。因而，AP 服务器 14 与管理服务器 12 首先通过实施图 6、图 7 的管理服务器 12 与内部终端 15 的从步骤 1001 到步骤 1016、从步骤 1101 到步骤 1104，预先建立管理服务器－AP 服务器间的加密通信通路（称作管理服务器－AP 服务器间加密通信通路）（步骤 4001）。并且，在 AP 服务器 14 还没有注册自身的地址的情况下，通过实施从图 8 的步骤 2002 到步骤 2006，将 AP 服务器 14 的地址注册到管理服务器 12 中（步骤 4002）。

同样，内部终端 15 和管理服务器 12 通过实施从图 6 的步骤 1001 到步骤 1016、从图 7 的步骤 1101 到步骤 1104，预先建立内部终端－管理服务器间加密通信通路（步骤 4003）。并且，在内部终端 15 还没有注册自身的地址的情况下，通过实施从图 8 的步骤 2002 到步骤 2006，将内部终端 15 的地址注册到管理服务器 12 中（步骤 4004）。

同样，外部终端 11 为了建立与内部终端 15 的终端－终端间加密通信通路而执行以下的步骤。

外部终端 11 和管理服务器 12 通过分别实施从图 6 的步骤 1001 到步骤 1016、从图 7 的步骤 1101 到步骤 1104 的步骤所示的内部终端 15 与管理服务器 12 的处理，建立外部终端－管理服务器间加密通信通路（步骤 4005）。并且，在外部终端 11 还没有注册自身的地址的情况下，通过实施从图 8 的步骤 2002 到步骤 2006，将外部终端 11 的地址注册到管理服务器 12 中（步骤 4006）。

在建立外部终端－管理服务器间加密通信通路后，外部终端 11 的针对管理服务器通信处理部22将对内部终端15的连接请求发送给管理服务器 12（步骤 4007）。管理服务器 12、外部终端 11、内部终端 15 通过实施从图 9、图 10 所示的步骤 3007 到步骤 3107，建立外部终端 11 与内部终端 15 之间的终端－终端间加密通信通路（步骤 4008）。

接着，外部终端 11 的针对终端通信处理部 23 为了经由内部终端 15 与 AP 服务器 14 通信，对内部终端 15 发送内容为指示对 AP 服务器 14 的连接请求的键输入信息（步骤 4009）。利用在步骤 4008 建立的终端－终端间加密通信通路来发送该连接请求。

内部终端 15 的针对终端通信处理部 23 如果从外部终端 11 接收到内容为指示向 AP 服务器 14 的连接请求的键输入信息，则为了在内部终端 15 与 AP 服务器 14 之间建立加密通信通路（称作内部终端－AP 服务器间加密通信通路），在从步骤 4007 到步骤 4008 中，内部终端 15 和 AP 服务器 14 分别进行相当于外部终端 11 和内部终端 15 的处理。该加密通信通路可以看作在内部终端 15 与 AP 服务器 14 之间建立的终端－终端间加密通信通路。

即，内部终端 11 的针对管理服务器通信处理部 22 对管理服务器 12 发送与 AP 服务器 14 的连接请求（步骤 4010）。如果管理服务器 12 从内部终端 15 接收到对 AP 服务器 14 的连接请求，则管理服务器 12、内部终端 15、AP 服务器 14 通过实施图 9、图 10 所示的从步骤 3007 到步骤 3107，建立内部终端－AP 服务器间加密通信通路（步骤 4011）。此外，由于已经在步骤 4001 和步骤 4003 中建立了内部终端－管理服务器间加密通信通路和 AP 服务器－管理服务器间加密通信通路，所以这里不需要再次建立加密通信通路。

利用通过执行以上的步骤而建立的 2 个加密通信通路、即外部终端－内部终端间加密通信通路、内部终端－AP 服务器间加密通信通

路，外部终端 11 能够经由内部终端 15 进行与 AP 服务器 14 的加密通信。

即，外部终端 11 的针对终端通信处理部 23 利用在与内部终端 15 之间建立的终端一终端间加密通信通路，对内部终端 15 发送内容为指示向 AP 服务器 14 的处理请求的键输入信息（步骤 4101）。内部终端 15 的针对终端通信处理部 23 如果从外部终端 11 接收到内容为指示向 AP 服务器 14 的处理请求的键输入信息，则利用在与 AP 服务器 14 之间建立的内部终端一AP 服务器间加密通信通路，将基于所接收到的键输入的处理请求发送给 AP 服务器 14（步骤 4102）。如果 AP 服务器 14 的针对终端通信处理部 23 从内部终端 15 接收到处理请求，则 AP 服务器 14 执行所请求的处理。接着，AP 服务器 14 的针对终端通信处理部 23 利用内部终端一AP 服务器间加密通信通路，将所请求的处理的执行结果发送给内部终端 15（步骤 4103）。内部终端 15 的针对终端通信处理部 23 接收到该结果，将该处理结果或根据该处理结果生成的对画面等的输出信息，利用终端一终端间加密通信通路发送给外部终端 11（步骤 4104）。外部终端 11 的针对终端通信处理部 23 接收该输出信息，从输入输出部 20c 对画面等输出。

通过执行以上的步骤，外部终端 11 能够经由内部终端 15 与 AP 服务器 14 进行安全的通信。

<实施方式 2>

下面说明第二实施方式。

在本实施方式中，在外部终端 11 经由内部终端 15 访问 AP 服务器 14 时进行图 13、图 14、图 15 所示那样的动作。

如图 13 所示，AP 服务器 14 和管理服务器 12 分别通过实施图 6、图 7 所示的内部终端 15 与管理服务器 12 的从步骤 1001 到步骤 1016、从步骤 1101 到步骤 1104，预先建立终端一服务器间加密通信通路（步骤 5001）。并且，在 AP 服务器 14 还没有注册自身的地址的情况下，

通过分别实施图 8 所示的从步骤 2002 到步骤 2006，将 AP 服务器 14 的地址注册到管理服务器 12 中（步骤 5002）。

在步骤 5001 及 5002 正常地进行的情况下，将 AP 服务器 14 的地址信息及认证结果注册到认证状态表 60 中。具体而言，AP 服务器 14 的地址信息作为终端的地址 61 及终端的 IP 地址 62 注册，作为与其对应的认证结果，表示认证成功内容的消息及其时刻被注册到认证结果 63 及认证时刻 64 中。

该认证状态表 60 是该管理服务器 12 进行认证并受理了地址信息的注册的、用于注册各种终端的状态的表，保持在管理服务器 12 的存储部 30b 中。

同样，内部终端 15 与管理服务器 12 通过分别实施图 6、图 7 的内部终端 15 与管理服务器 12 的从步骤 1001 到步骤 1016、从步骤 1101 到步骤 1104，预先建立内部终端一管理服务器间加密通信通路（步骤 5003）。并且，在内部终端 15 还没有注册自身的地址的情况下，通过分别实施图 8 所示的从步骤 2002 到步骤 2006，将内部终端 15 的地址注册到管理服务器 12 中（步骤 5004）。

在步骤 5003 及 5004 正常地进行的情况下，将内部终端 15 的地址信息及认证结果注册到认证状态表 60 中。

外部终端 11 为了与内部终端 15 建立终端一终端间加密通信通路而执行以下的步骤。

外部终端 11 和管理服务器 12 通过分别实施图 6、图 7 的内部终端 15 与管理服务器 12 的从步骤 1001 到步骤 1016、从步骤 1101 到步骤 1104，预先建立外部终端一管理服务器间加密通信通路（步骤 5005）。并且，在外部终端 11 还没有注册自身的地址的情况下，通过分别实施图 8 所示的从步骤 2002 到步骤 2006，将外部终端 11 的地址注册到管理服务器 12 中（步骤 5006）。

在步骤 5005 及 5006 正常地进行的情况下，将外部终端 11 的地

址信息及认证结果注册到认证状态表 60 中。

然后，外部终端 11 的针对管理服务器通信处理部 22 将向内部终端 15 的连接请求发送给管理服务器 12（步骤 5007）。管理服务器 12 的针对终端通信处理部 33 接收来自内部终端 15 的连接请求，确认外部终端 11、内部终端 15 的认证状态（步骤 5008）。具体而言，管理服务器 12 的针对终端通信处理部 33 参照认证状态表 60，对注册有外部终端 11 和内部终端 15 的地址信息的情况、和认证结果拦中注册有认证成功的内容的情况进行确认。在如果未注册有地址信息的情况下，管理服务器 12 对外部终端 11 应答拒绝连接请求的内容。此外，在虽然注册有地址信息、但在认证结果栏中未注册有认证成功的内容的情况下，管理服务器 12 的针对终端通信处理部 33 在与内部终端 15 之间进行加密通信通路建立处理，并进行认证状态的确认。如果不能再次进行认证状态的确认，则管理服务器 12 对外部终端 11 应答拒绝连接请求的内容。

如果进行了认证状态的确认，则管理服务器 12 的键生成・分发部 32 生成在终端－终端间加密通信通路中利用的加密键（步骤 5009）。接着，管理服务器 12 的针对终端通信处理部 33 将从外部终端 11 向内部终端 15 的连接请求、以及在步骤 5009 中生成的加密键及设定信息发送给内部终端 15（步骤 5010）。

接收到这些的内部终端 15 的针对管理服务器通信处理部 22 判断该外部终端 11 是否能够与内部终端 15 连接，将该连接可否判断结果发送给管理服务器 12（步骤 5011）。管理服务器 12 的针对终端通信处理部 33 将该连接可否判断结果、和在判断结果表示能够连接的情况下在步骤 5009 中生成的加密键及设定信息发送给外部终端 11（步骤 5012）。如果外部终端 11 的针对管理服务器通信处理部 22 接收到这些，则已建立终端－终端间加密通信通路，外部终端 11 的针对终端通信处理部 23 和内部终端 15 的针对终端通信处理部 23 能够利用

在步骤5010及步骤5012中分别接收到的加密键进行加密通信(步骤5013)。

管理服务器12的针对终端通信处理部33将在外部终端11与内部终端15之间建立了终端一终端间加密通信通路的情况注册到图17所示那样的通信状态表70中(步骤5014)。具体而言,连接请求源(这里是外部终端11)的地址注册到通信状态表70的通信源地址71中,将连接请求目的地(这里是内部终端15)的地址注册到通信目的地地址72中,将该终端一终端间的加密通路所建立的时刻(例如两终端接收到加密键和设定信息的时刻)注册到通信开始时刻73中。

该通信状态表70注册有管理服务器12认证并生成加密键而建立的终端一终端间加密通信通路的各个状态,保持在存储部30b中。

接着,外部终端11的针对终端通信处理部23为了经由内部终端15与AP服务器14通信,对内部终端15发送内容为指示向AP服务器14的连接请求的键输入信息(步骤5101)。另外,该连接请求利用在步骤5106中建立的终端一终端间加密通信通路,向内部终端15发送。

内部终端15的针对终端通信处理部23如果从外部终端11接收到内容为指示向AP服务器14的连接请求的键输入信息,则为了在内部终端15与AP服务器14之间建立内部终端一AP服务器间加密通信通路而进行下面的动作。

内部终端15的针对管理服务器通信处理部对管理服务器12发送外部终端11的经由内部终端15与AP服务器14的连接请求(步骤5102)。即,该连接请求是外部终端11为了向AP服务器14连接而请求内部终端15与AP服务器14之间的内部终端一AP服务器间加密通信通路的建立,所以作为被认证对象也包括外部终端11。因而,作为该连接请求,发送图18所示那样的除了通信源信息81和通信目的地信息82以外还包括被认证对象信息83的带被认证对象信息的连

接请求 80。此外，也包括其他通信所需的信息、及应用信息 84。

管理服务器 12 的针对终端通信处理部 33 接受该带被认证对象信息的连接请求 80，对作为通信源信息 81、通信目的地信息 82、被认证对象信息 83 而分别记载的外部终端 11、内部终端 15、AP 服务器 14 的认证状态进行确认（步骤 5103）。具体而言，管理服务器 12 参照认证状态表 60，对注册有外部终端 11、内部终端 15、和 AP 服务器 14 的地址信息的情况、以及在认证结果 63 的栏中注册有认证成功的内容的情况进行确认。在如果未注册有地址信息的情况下，管理服务器 12 对内部终端 15 应答拒绝连接请求的内容。此外，在虽然注册有地址信息、但在认证结果栏中未注册有认证成功的内容的情况下，管理服务器 12 的针对终端通信处理部 33 在与 AP 服务器 14 之间进行加密通信通路建立处理，进行认证状态的确认。如果不能再次进行认证状态的确认，则管理服务器 12 对内部终端 15 应答拒绝连接请求的内容。

本实施方式由于也将外部终端 11 作为被认证对象，所以如果进行了认证状态的确认，则管理服务器 12 的针对终端通信处理部 33 参照通信状态表 70 对在记载于带被认证对象信息的连接请求 80 中的通信源（内部终端 15）和被认证对象（外部终端 11）的终端间建立加密通信通路并正在通信的情况进行确认（步骤 5104）。具体而言，管理服务器 12 的针对终端通信处理部 33 参照通信状态表 70，确认内部终端 15 与外部终端 11 被分别记载于通信源地址和通信目的地地址中、并处于通信状态。如果进行了认证状态及通信状态的确认，则管理服务器 12 的键生成・分发部 32 生成在内部终端 15 与 AP 服务器 14 之间的内部终端－AP 服务器间加密通信通路中利用的加密键（步骤 5105）。接着，管理服务器 12 的针对终端通信处理部 33 将外部终端 11 的经由内部终端 15 与 AP 服务器 14 的连接请求以及在步骤 5105 中生成的加密键及设定信息发送给 AP 服务器 14（步骤 5106）。接收

到这些的 AP 服务器 14 的针对管理服务器通信处理部 22 判断外部终端 11 是否能够经由该内部终端 15 与 AP 服务器 14 连接，将该连接可否判断结果发送给管理服务器 12（步骤 5107）。管理服务器 12 的针对终端通信处理部 33 将该连接可否判断结果、和在判断结果表示可通信的情况下在步骤 5105 中生成的加密键及设定信息发送给内部终端 15（步骤 5108）。内部终端 15 的针对管理服务器通信处理部 22 接收到这些后，就建立了内部终端－AP 服务器间加密通信通路，内部终端 15 的针对终端通信处理部 23 和 AP 服务器 14 的针对终端通信处理部 23 能够利用在步骤 5106 及步骤 5108 中分别接收到的加密键进行加密通信（步骤 5109）。

管理服务器 12 的针对终端通信处理部 33 将在内部终端 15 和 AP 服务器 14 之间建立了内部终端－AP 服务器间加密通信通路的情况注册到图 17 所示那样的通信状态表 70 中（步骤 5110）。由此，即使在 AP 服务器 14 还对其他通信终端发行处理请求并从该其他通信终端取得处理结果那样的情况下，也能够通过重复与上述同样的处理，将外部通信终端作为被认证对象，来建立加密通信通路。

此外，通过参照通信状态表 70，管理服务器 12 能够使已建立的 2 个加密通信通路（外部终端 11－内部终端 15 间、内部终端 15－AP 服务器 14 间）建立对应，能够掌握哪 3 个装置在进行关联的处理。

内部终端 15 的针对终端通信处理部 23 如果建立了与外部终端 11 的终端－终端间加密通信通路，则向外部终端 11 应答连接结果（步骤 5111）。

利用通过执行以上的步骤而确立的 2 个加密通信通路（外部终端 11－内部终端 15 间、内部终端 15－AP 服务器 14 间），外部终端 11 能够经由内部终端 15 进行与 AP 服务器 14 的加密通信。即，外部终端 11 的针对终端通信处理部 23 利用在与内部终端 15 之间建立的终端－终端间加密通信通路，对内部终端 15 发送内容为向 AP 服务器

14 指示处理请求的键输入信息（步骤 5201）。

内部终端 15 的针对终端通信处理部 23 如果从外部终端接收到内容为向 AP 服务器 14 指示处理请求的键输入信息，则利用在与 AP 服务器 14 之间建立的内部终端－AP 服务器间加密通信通路，将基于所接收到的键输入的处理请求发送给 AP 服务器 14（步骤 5202）。AP 服务器 14 的针对终端通信处理部 23 如果接收到来自内部终端 15 的处理请求，则执行所请求的处理。接着，AP 服务器 14 的针对终端通信处理部 23 利用内部终端－AP 服务器间加密通信通路，将所请求的处理的执行结果发送给内部终端 15（步骤 5203）。内部终端 15 的针对终端通信处理部 23 接收到该结果，利用终端－终端间加密通信通路，将该处理结果或根据该处理结果而生成的向画面等的输出信息发送给外部终端 11（步骤 5204）。外部终端 11 的针对终端通信处理部 23 接收到该输出信息，通过输入输出部 20c 向画面等输出。

通过执行以上的步骤，外部终端 11 能够经由内部终端 15 与 AP 服务器 14 进行安全的通信。

另外，在上述 2 个实施方式的通信系统中，外部终端 11、内部终端 15、AP 服务器 14 的各通信终端只要进行一次与管理服务器 12 的认证就能够基于该结果而相互通信，并不需要另外进行 ID/密码等应用服务器固有的认证。即，管理服务器 12 通过集中地进行外部终端 11、内部终端 15、AP 服务器 14 的认证，不再像以往那样在外部终端 11 经由内部终端 15 向 AP 服务器 14 连接时进行多种认证，能够使认证信息的管理简单化。

另外，实施例 1 的结构没有包含通信状态表 70，但在实施例 1 中，也可以通过具备并参照通信状态表 70，管理服务器 12 能够将已建立的 2 个加密通信通路（外部终端 11－内部终端 15 间、内部终端 15－AP 服务器 14 间）建立对应，从而能够掌握是哪 3 个装置在进行关联的处理。

进而，无论在哪个实施例中，即使在外部终端 11、内部终端 15、AP 服务器 14 的至少一种有多个且相互进行加密通信的状态下，管理服务器 12 通过具备认证状态表 60 和通信状态表 70，也能够管理、掌握这些通信状态。

此外，具有如下特征：在 AP 服务器 14 进行认证处理时，在需要使用用户所拥有的 IC 卡等的基于 PKI 的严格认证的情况下，在实施例 1 的结构中，需要通过内部终端 15 操作 IC 卡，但在本实施例 2 中不需要，可以通过用户实际上使用的外部终端进行操作。即，在外部终端 11 经由内部终端 15 向 AP 服务器 14 连接的情况下，基于操作外部终端 11 的用户所拥有的 IC 卡的认证结果，能够向 AP 服务器 14 连接，所以实际上成为可以在该用户的权限下向 AP 服务器 14 连接，从而更加安全，并且用户能够利用位于各据点的各种外部终端向 AP 服务器 14 连接，具有提高了方便性的特征。

在实施方式 1 及实施方式 2 中，例示了指定了通信终端的通信，但也可以将利用通信终端的用户指定为通信对方。在将利用通信终端的用户指定为通信对方的情况下，只要如下这样构成就可以：将用户所持有的公钥证书和用户 ID 预先装入具有可移动性的存储介质 58 中，通信终端检测到存储介质 58 插入到通信终端的读取装置 57 中的情况，从而读取用户的属性并存储。通过该结构，通信终端能够确定正在利用的用户，受理作为通信对象的指定。并且，可以构成为，在用户将具有可移动性的存储介质 58 从读取装置 57 拔出时，通信终端将用户的属性从通信终端删除。

如果用户的属性被存储在通信终端中，则进行图 8 的地址注册处理，如果用户的属性被从通信终端删除，则进行将图 8 的“注册”替换为“删除”的处理，由此，利用管理服务器 12 管理用户 ID 和通信终端的地址，这样，管理服务器 12 在有来自其他通信终端的连接请求时，判断作为目的地的用户是否正在利用通信终端，在正在利用的

情况下，可以判断正在利用哪个通信终端，而不会当成进行连接请求的其他通信终端的利用者，所以具有连接处理变容易的特征。

另外，无论在哪个实施例中，都能够从外部终端 11 经由内部终端 15 利用多个 AP 服务器 14。例如，有时在内部终端上执行多个分别访问不同的 AP 服务器的应用程序，通过键盘等输入信息的发送和多窗口画面信息的接收来从外部终端操作它们。

在此情况下，外部终端－内部终端间的加密通信通路有一个就可以，内部终端－AP 服务器间加密通信通路为多个。即，只要如下这样构成就可以：在图 11 中，对每个 AP 服务器实施步骤 4001～4004，步骤 4009 以后的处理在内部终端上动作的每个应用程序中执行，在步骤 4104 中将多个应用程序所输出的画面信息作为一个画面发送。

此外，无论在哪个实施例中，都说明了通过外部终端 11 远程操作内部终端 15、即交换键盘及鼠标等的输入信息和画面等的输出信息、来从 AP 服务器 14 接受服务提供的结构。但是并不限于该结构，也可以是外部终端 11 对内部终端 15 发行处理请求命令、接收内部终端 15 与 AP 服务器 14 的信息交换的处理结果信息（例如表示处理结果的命令的返回值）的方式。

此外，将内部终端 15 作为预先进行加密通信通路建立和地址注册的终端进行了说明。但是，作为应用例，也可以在进行了从外部终端 11 对在管理服务器 12 中被地址注册的内部终端 15 的连接请求之后，管理服务器 12 进行与内部终端 15 的加密通信通路建立处理。

另外，在上述实施方式 1、2 中，管理服务器 12 发送加密键的同时也发送设定信息，但只要发送新开始的加密通信所需的信息就可以，例如在预先确定了算法及键长的情况下也可以不发送。

进而，在上述实施方式 1、2 中，总是将通信终端和通信终端间的通信加密，但也可以在没有必要加密的情况下不进行加密。例如，由于内部终端 15 和 AP 服务器 14 间的通信在组织内网络 16 内进行

交换，所以也可以在没有必要的情况下不进行加密。此时，在管理服务器 12 发送到各个通信终端的设定信息中作为表示加密算法的信息来设定表示“不加密”的消息。

此外，也可以将上述实施方式 1、2 适当地组合来实施。

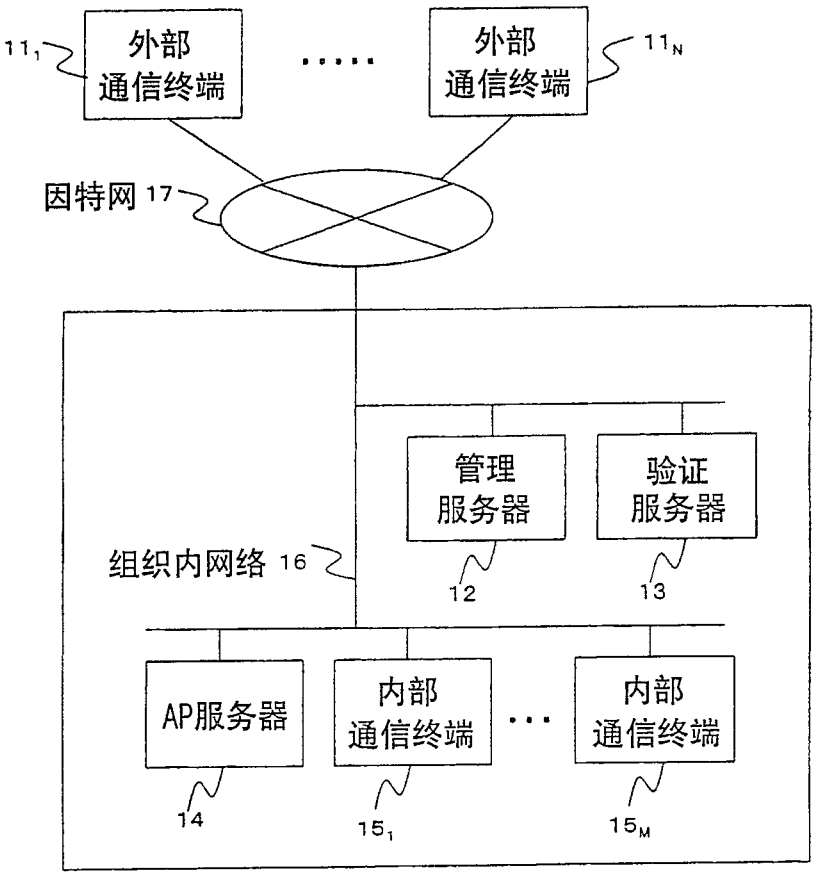

外部
通信终端
11₁
外部
通信终端
11N
因特网 17
管理
服务器
12
验证
服务器
13
组织内网络 16
AP服务器
14
内部
通信终端
15₁
内部
通信终端
15M

图1

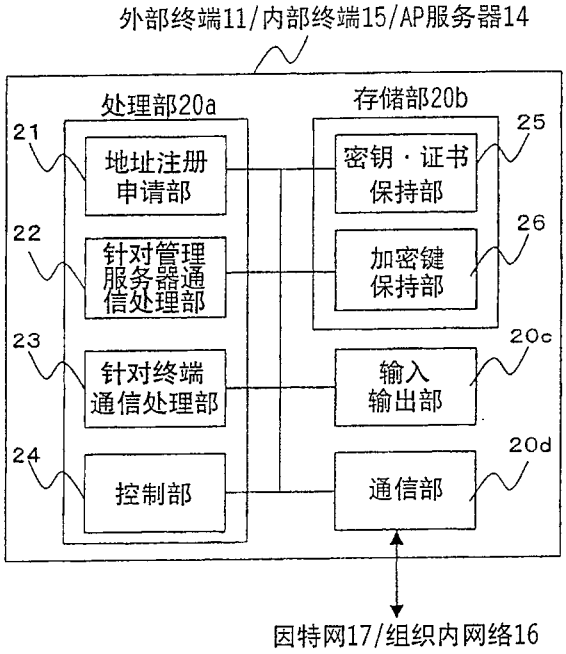

外部终端11/内部终端15/AP服务器14
处理部20a
存储部20b
21
地址注册申请部
22
针对管理服务器通信处理部
23
针对终端通信处理部
24
控制部
25
密钥·证书保持部
26
加密键保持部
20c
输入输出部
20d
通信部
因特网17/组织内网络16

图2

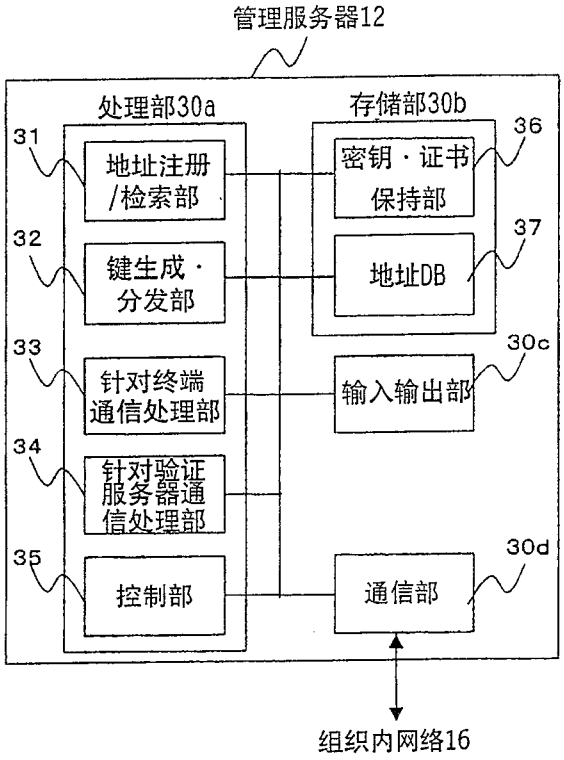

管理服务器12
处理部30a
存储部30b
31
地址注册/检索部
32
键生成·分发部
33
针对终端通信处理部
34
针对验证服务器通信处理部
35
控制部
36
密钥·证书保持部
37
地址DB
30c
输入输出部
30d
通信部
组织内网络16

图3

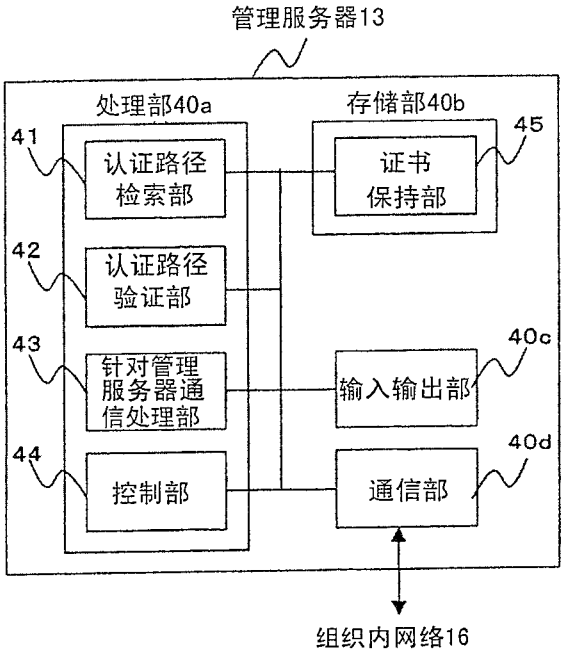

管理服务器13
处理部40a
存储部40b
41
认证路径检索部
45
证书保持部
42
认证路径验证部
43
针对管理服务器通信处理部
40c
输入输出部
44
控制部
40d
通信部
组织内网络16

图4

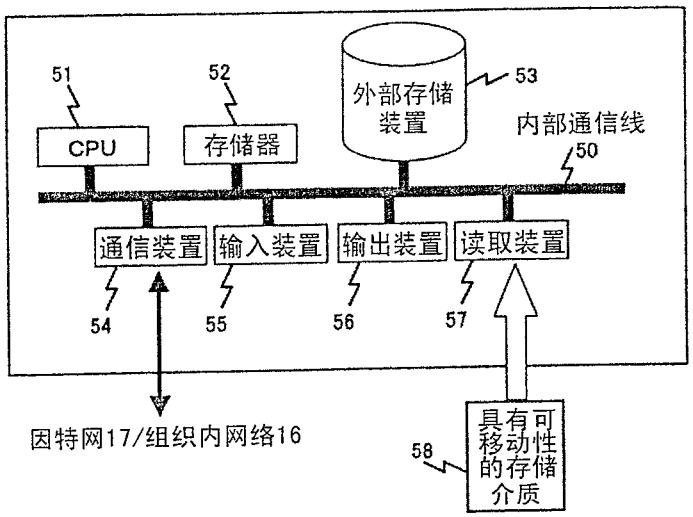

51
52
53
外部存储装置
内部通信线
50
CPU
存储器
通信装置
输入装置
输出装置
读取装置
54
55
56
57
因特网17/组织内网络16
58
具有可移动性的存储介质

图5

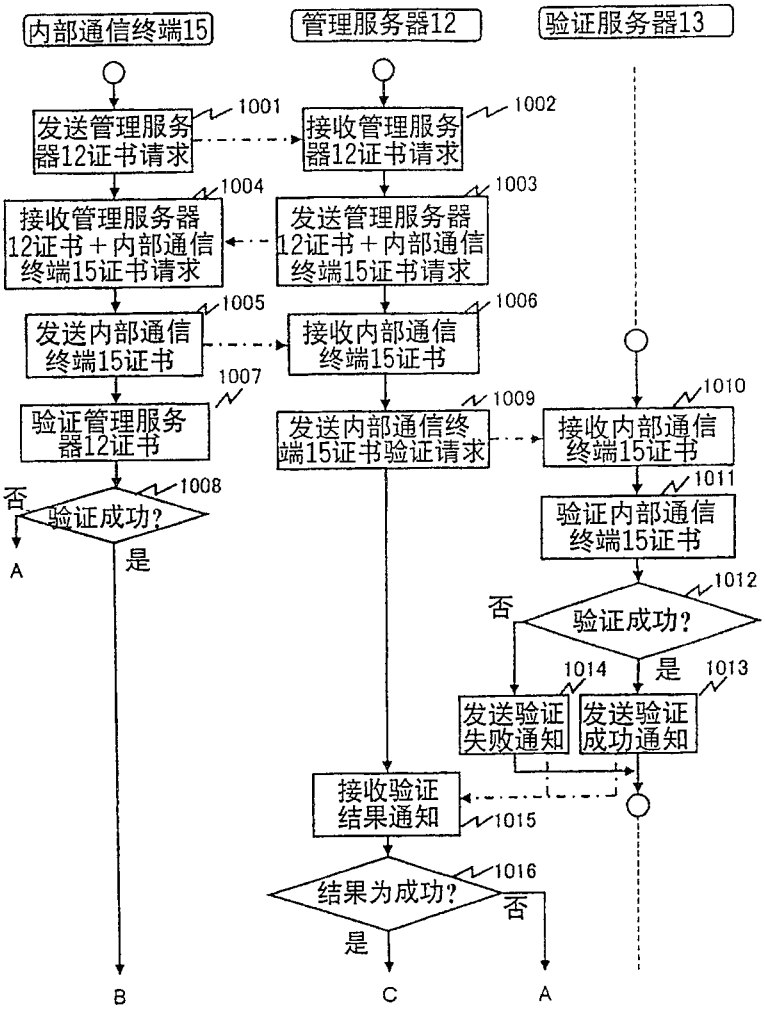

内部通信终端15
管理服务器12
验证服务器13
发送管理服务器12证书请求
1001
接收管理服务器12证书请求
1002
接收管理服务器12证书＋内部通信终端15证书请求
1004
发送管理服务器12证书＋内部通信终端15证书请求
1003
发送内部通信终端15证书
1005
接收内部通信终端15证书
1006
验证管理服务器12证书
1007
发送内部通信终端15证书验证请求
1009
接收内部通信终端15证书
1010
验证内部通信终端15证书
1011
验证成功?
1008
否
是
A
B
验证成功?
1012
否
是
发送验证失败通知
1014
发送验证成功通知
1013
接收验证结果通知
1015
结果为成功?
1016
否
是
C
A

图6

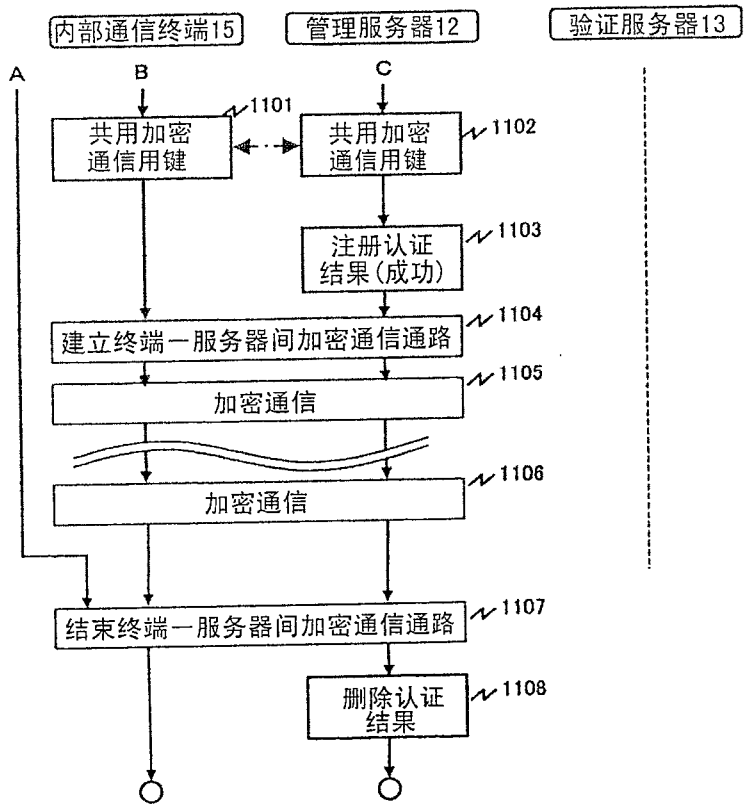

内部通信终端15
管理服务器12
验证服务器13
A
B
C
1101
共用加密通信用键
共用加密通信用键
1102
注册认证结果(成功)
1103
建立终端一服务器间加密通信通路
1104
加密通信
1105
加密通信
1106
结束终端一服务器间加密通信通路
1107
删除认证结果
1108

图7

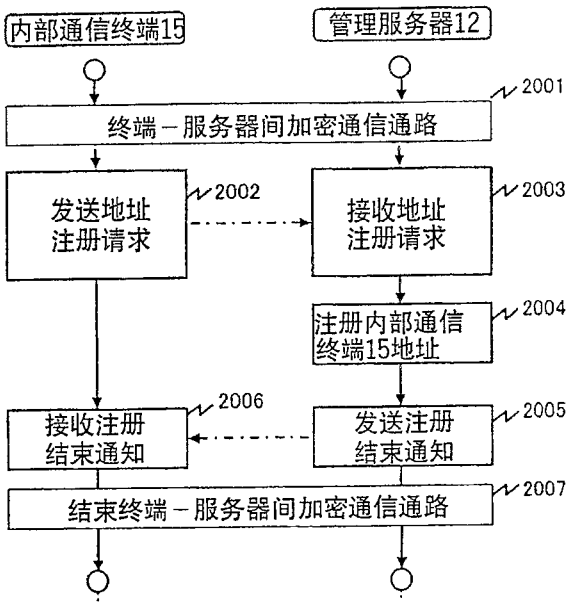

内部通信终端15
管理服务器12
2001
终端－服务器间加密通信通路
发送地址
注册请求
2002
接收地址
注册请求
2003
注册内部通信
终端15地址
2004
接收注册
结束通知
2006
发送注册
结束通知
2005
结束终端－服务器间加密通信通路
2007

图8

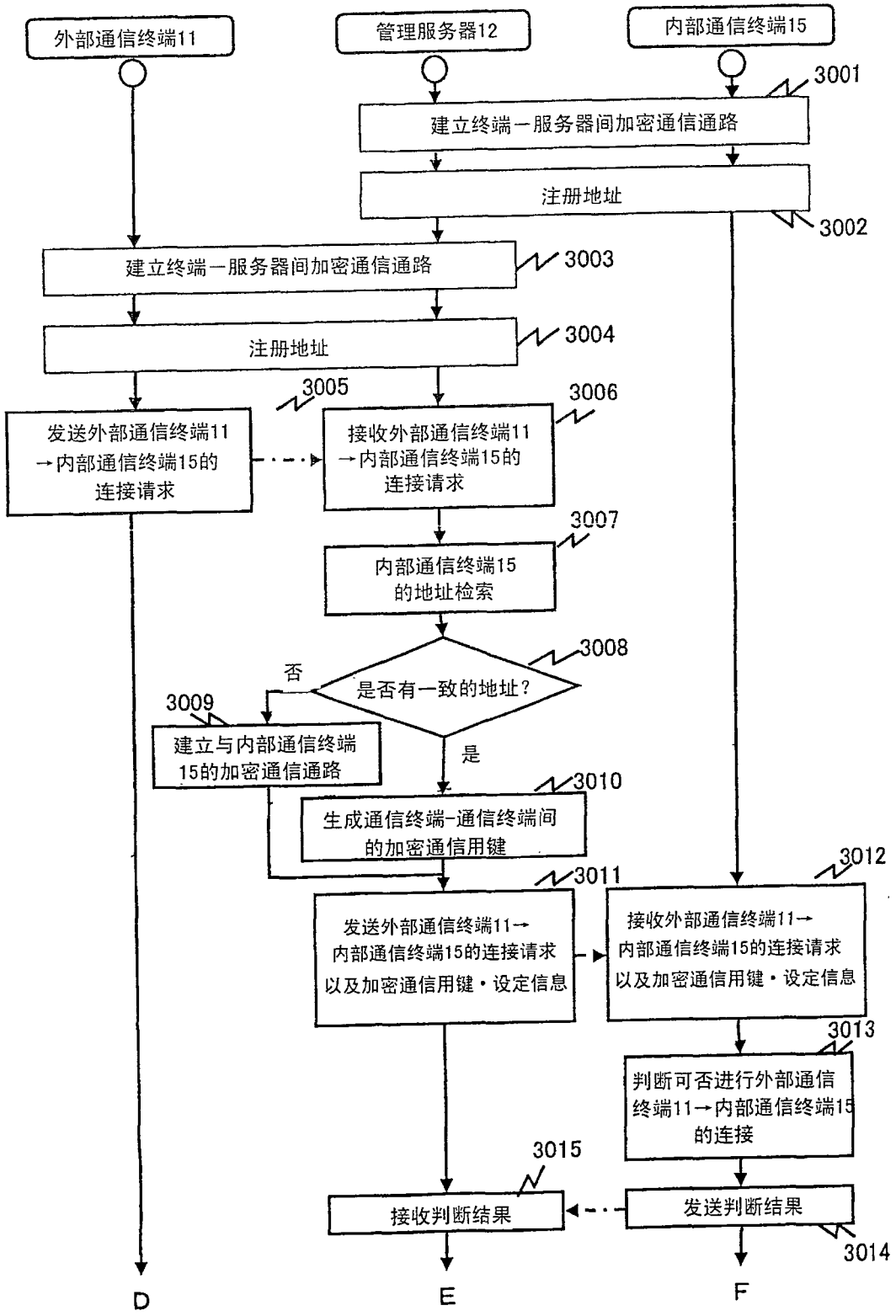

外部通信终端11
管理服务器12
内部通信终端15
3001
建立终端一服务器间加密通信通路
注册地址
3002
建立终端一服务器间加密通信通路
3003
注册地址
3004
3005
3006
发送外部通信终端11→内部通信终端15的连接请求
接收外部通信终端11→内部通信终端15的连接请求
3007
内部通信终端15的地址检索
3008
否
是否有一致的地址?
3009
建立与内部通信终端15的加密通信通路
是
3010
生成通信终端-通信终端间的加密通信用键
3011
3012
发送外部通信终端11→内部通信终端15的连接请求以及加密通信用键・设定信息
接收外部通信终端11→内部通信终端15的连接请求以及加密通信用键・设定信息
3013
判断可否进行外部通信终端11→内部通信终端15的连接
3015
接收判断结果
发送判断结果
3014
D
E
F

图9

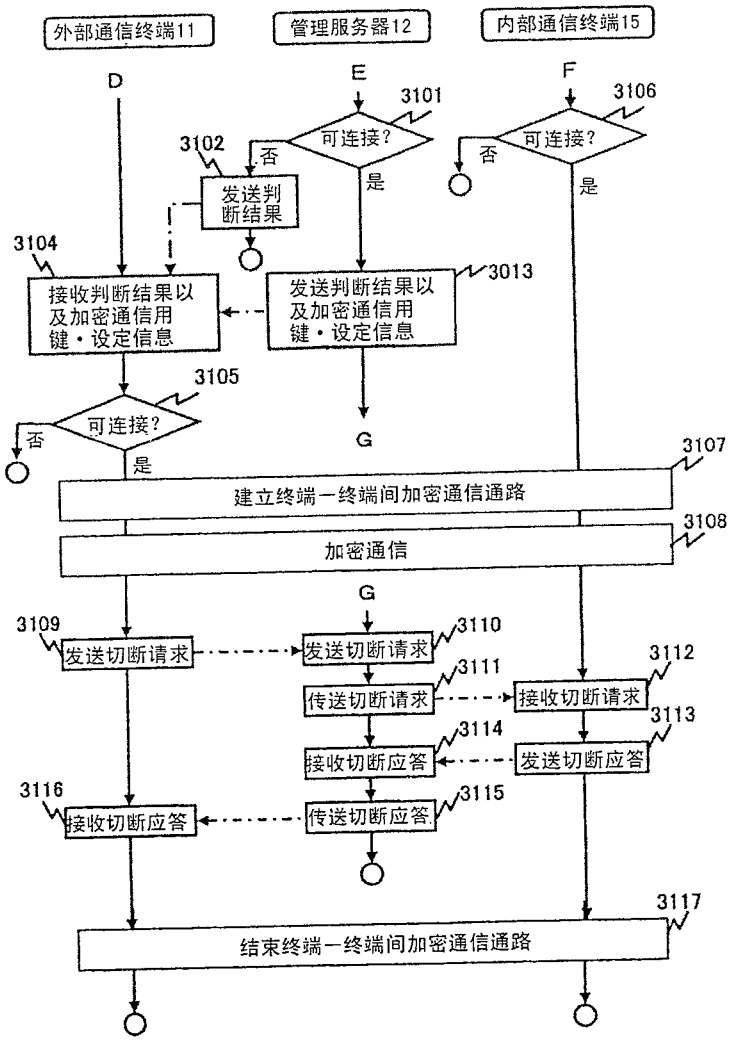

外部通信终端11
管理服务器12
内部通信终端15
D
E
F
3101
可连接?
否
是
3102
发送判断结果
3104
接收判断结果以及加密通信用键・设定信息
3013
发送判断结果以及加密通信用键・设定信息
3105
可连接?
否
是
G
3106
可连接?
否
是
3107
建立终端一终端间加密通信通路
3108
加密通信
G
3109
发送切断请求
3110
发送切断请求
3111
传送切断请求
3112
接收切断请求
3113
发送切断应答
3114
接收切断应答
3115
传送切断应答
3116
接收切断应答
3117
结束终端一终端间加密通信通路

图10

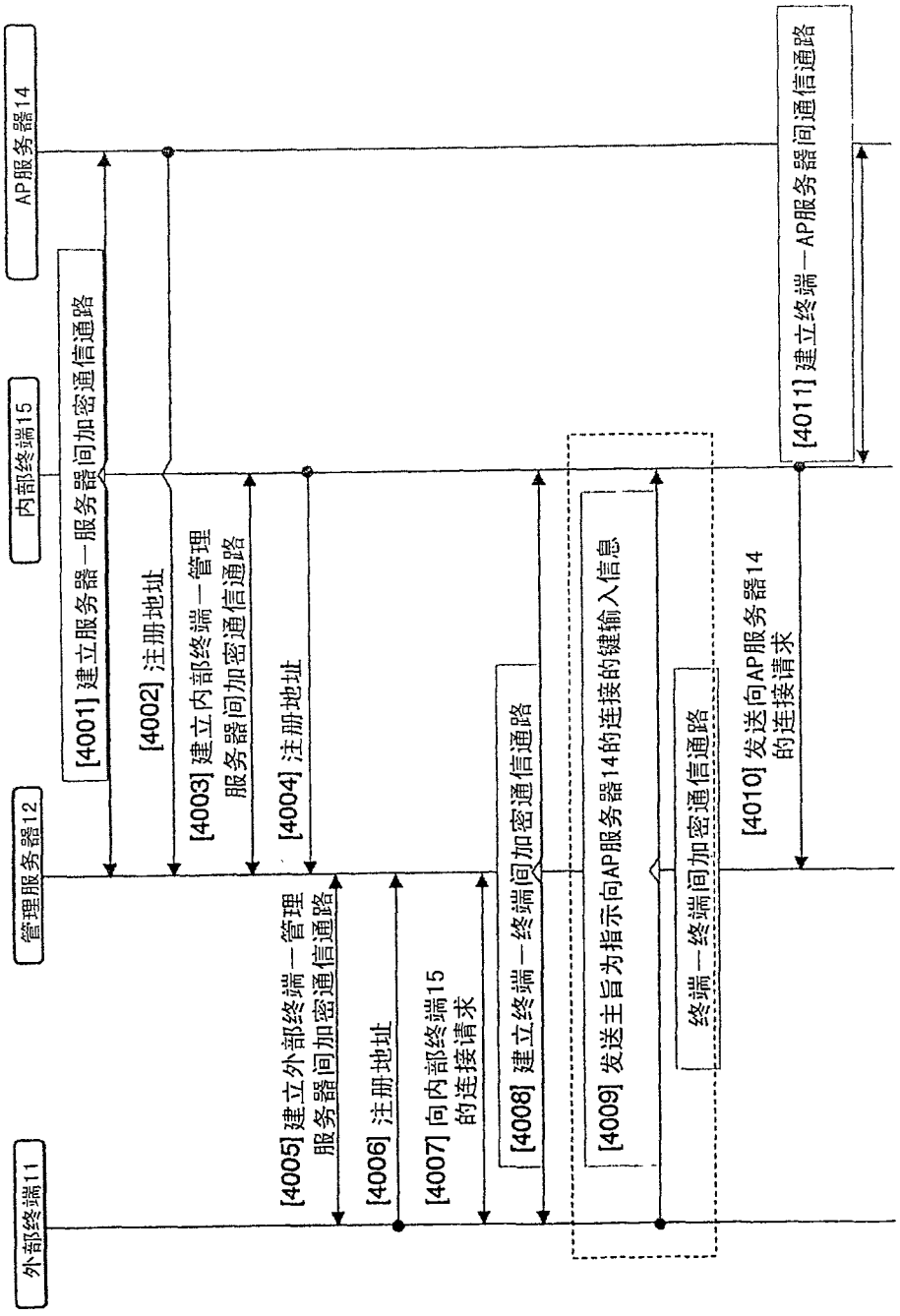

外部终端11
管理服务器12
内部终端15
AP服务器14
[4001] 建立服务器—服务器间加密通信通路
[4002] 注册地址
[4003] 建立内部终端—管理服务器间加密通信通路
[4004] 注册地址
[4005] 建立外部终端—管理服务器间加密通信通路
[4006] 注册地址
[4007] 向内部终端15的连接请求
[4008] 建立终端—终端间加密通信通路
[4009] 发送主旨为指示向AP服务器14的连接的键输入信息
终端—终端间加密通信通路
[4010] 发送向AP服务器14的连接请求
[4011] 建立终端—AP服务器间通信通路

图11

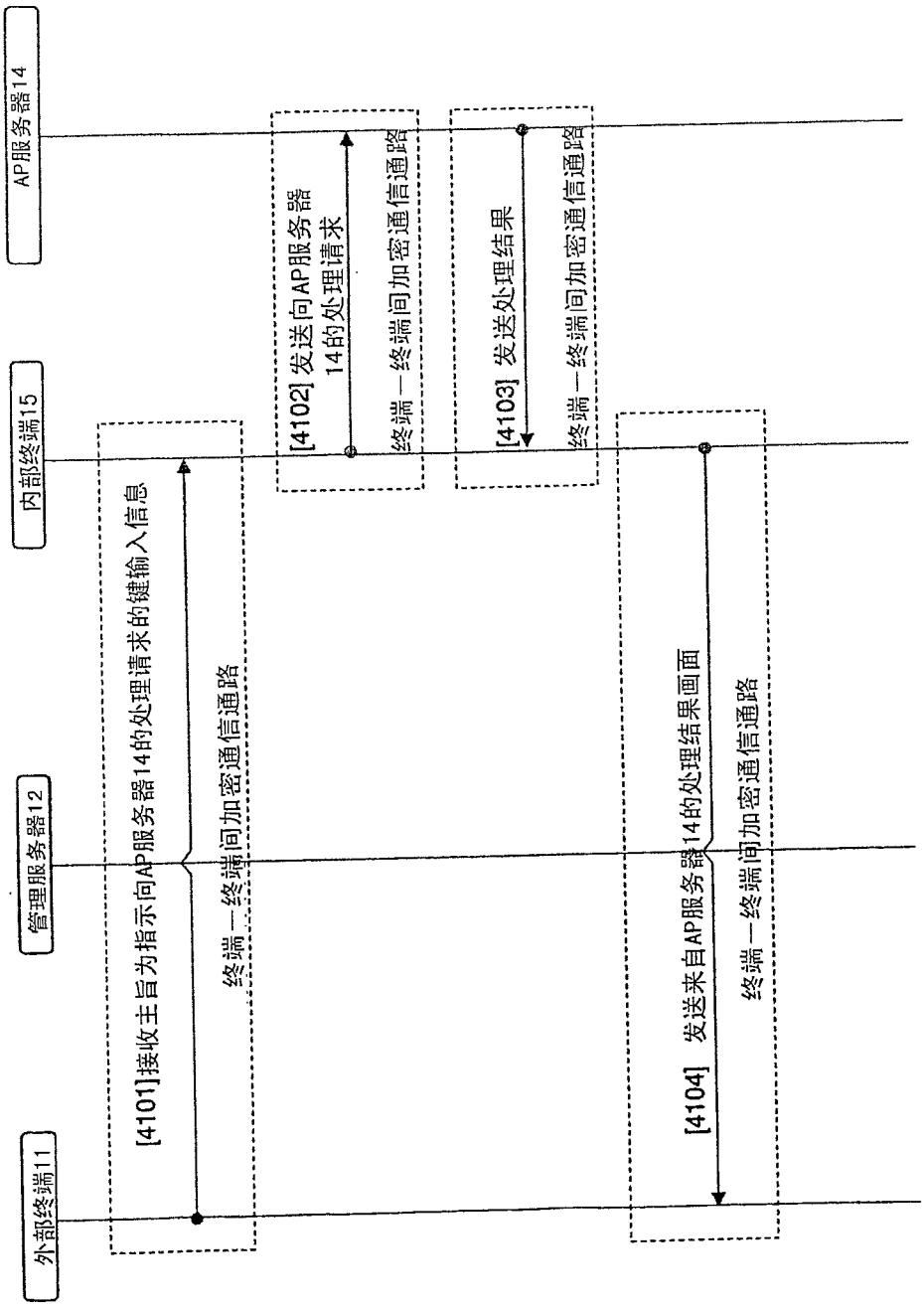

外部终端11
管理服务器12
内部终端15
AP服务器14
[4101]接收主旨为指示向AP服务器14的处理请求的键输入信息
终端—终端间加密通信通路
[4102] 发送向AP服务器14的处理请求
终端—终端间加密通信通路
[4103] 发送处理结果
终端—终端间加密通信通路
[4104] 发送来自AP服务器14的处理结果画面
终端—终端间加密通信通路

图12

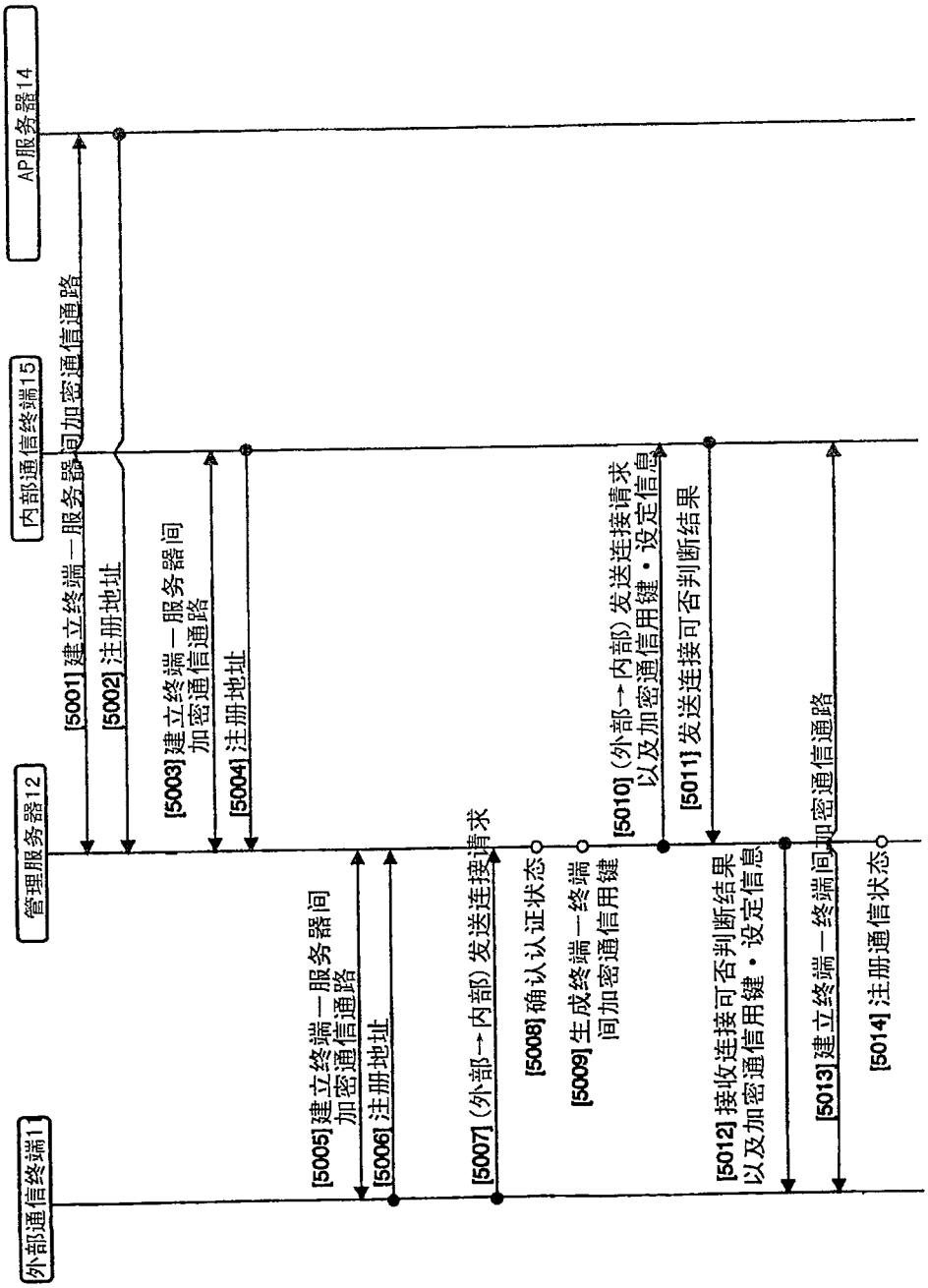

外部通信终端11
管理服务器12
内部通信终端15
AP服务器14
[5001] 建立终端—服务器间加密通信通路
[5002] 注册地址
[5003] 建立终端—服务器间加密通信通路
[5004] 注册地址
[5005] 建立终端—服务器间加密通信通路
[5006] 注册地址
[5007] (外部→内部) 发送连接请求
[5008] 确认认证状态
[5009] 生成终端—终端间加密通信用键
[5010] (外部→内部) 发送连接请求以及加密通信用键・设定信息
[5011] 发送连接可否判断结果
[5012] 接收连接可否判断结果以及加密通信用键・设定信息
[5013] 建立终端—终端间加密通信通路
[5014] 注册通信状态

图13

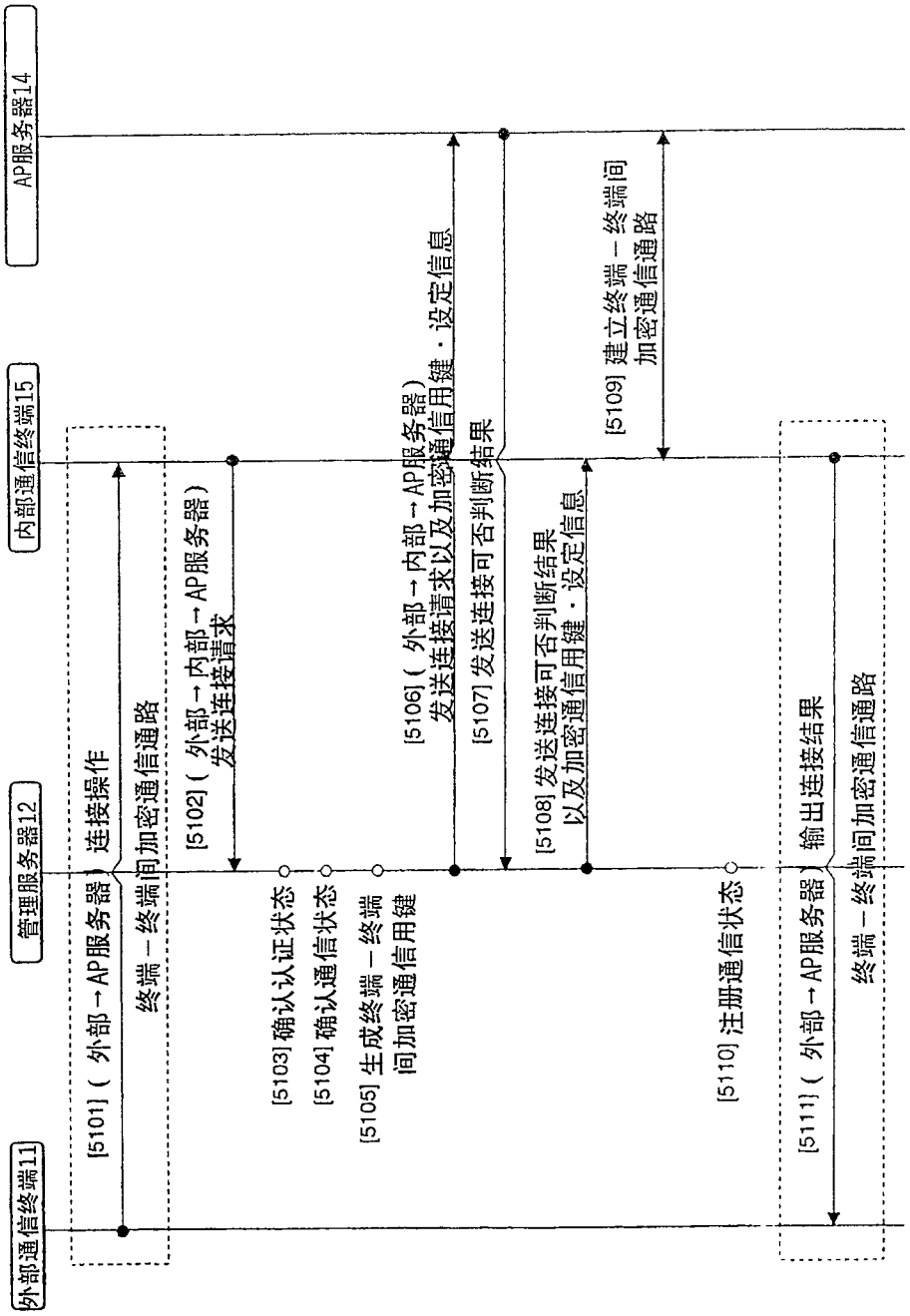

外部通信终端11
管理服务器12
内部通信终端15
AP服务器14
[5101]（外部→AP服务器）连接操作
终端－终端间加密通信通路
[5102]（外部→内部→AP服务器）
发送连接请求
[5103]确认认证状态
[5104]确认通信状态
[5105]生成终端－终端
间加密通信用键
[5106]（外部→内部→AP服务器）
发送连接请求以及加密通信用键・设定信息
[5107]发送连接可否判断结果
[5108]发送连接可否判断结果
以及加密通信用键・设定信息
[5109]建立终端－终端间
加密通信通路
[5110]注册通信状态
[5111]（外部→AP服务器）输出连接结果
终端－终端间加密通信通路

图14

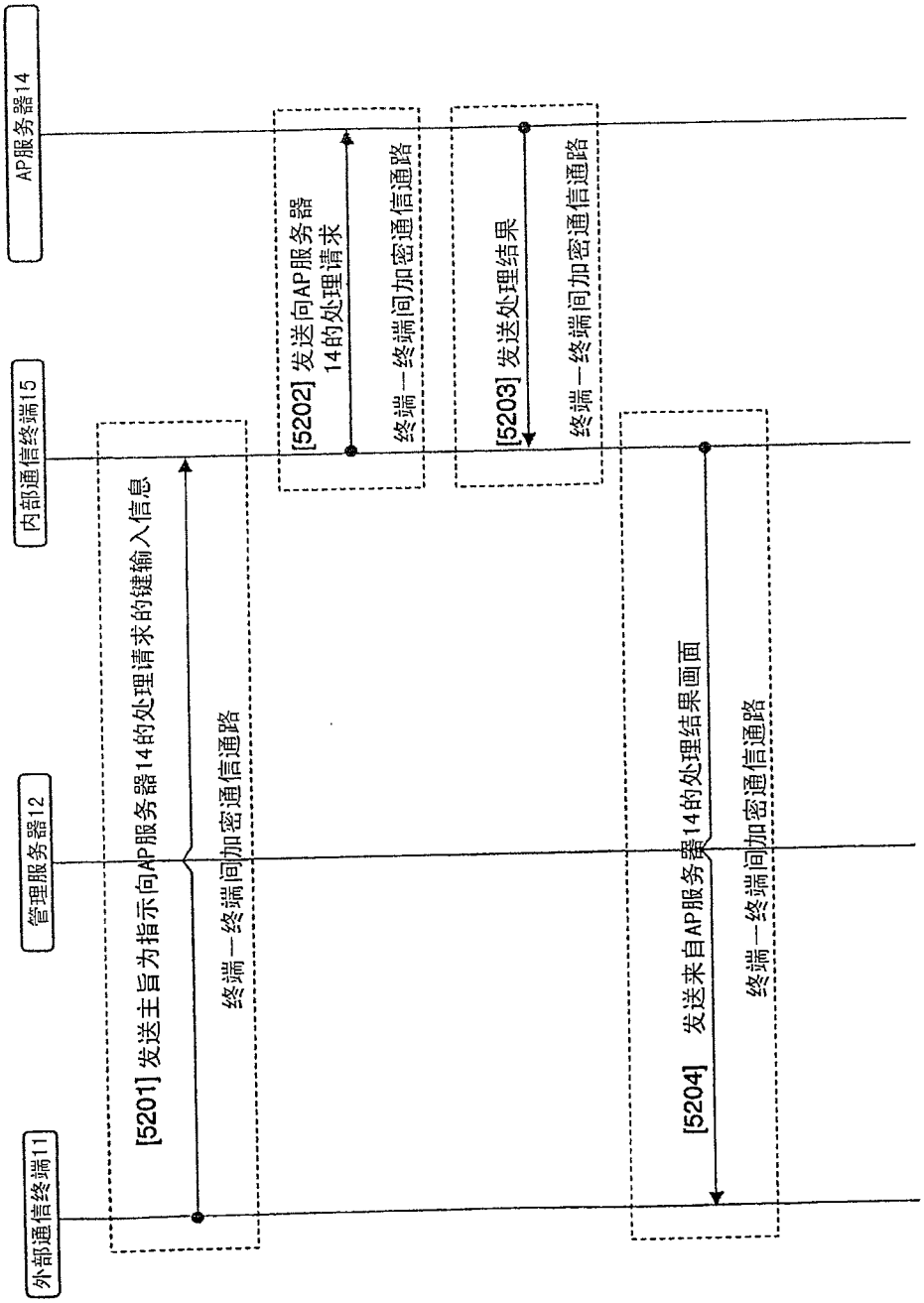

外部通信终端11
管理服务器12
内部通信终端15
AP服务器14
[5201] 发送主旨为指示向AP服务器14的处理请求的键输入信息
终端—终端间加密通信通路
[5202] 发送向AP服务器14的处理请求
终端—终端间加密通信通路
[5203] 发送处理结果
终端—终端间加密通信通路
[5204] 发送来自AP服务器14的处理结果画面
终端—终端间加密通信通路

图15

认证状态表60

61 终端的地址	62 终端的IP地址	63 认证结果	64 认证时刻
out1@aaa.bbb	133.144.6.4	OK	2005/06/28 15:22:01
out2@aaa.bbb	172.24.36.5	OK	2005/06/29 12:20:45
in1@aaa.bbb	192.168.3.59	OK	2005/06/30 10:02:01
...	...	...	...

图16

通信状态表70

71 通信源地址	72 通信目的地地址	73 通信开始时刻
out1@aaa.bbb	in1@aaa.bbb	2005/06/28 15:22:03
out2@aaa.bbb	in2@aaa.bbb	2005/06/29 12:20:48
...	...	...

图17

带被认证对象信息的连接请求80

81	通信源信息	内部通信终端(in1@aaa.bbb)
82	通信目的地信息	AP服务器(AP@aaa.bbb)
83	被认证对象信息	外部终端(out1@aaa.bbb)
84	其他通信信息、应用信息	客户端通信信息的选项、协议、格式等

图18