[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
G06F 1/00
G06F 9/06

[12] 发明专利申请公开说明书

[21] 申请号 03802032.7

[43] 公开日 2005 年 5 月 4 日

[11] 公开号 CN 1613040A

[22] 申请日 2003.1.7 [21] 申请号 03802032.7
[30] 优先权
[32] 2002. 1. 8 [33] JP [31] 1843/2002
[86] 国际申请 PCT/JP2003/000035 2003.1.7
[87] 国际公布 WO2003/058411 日 2003.7.17
[85] 进入国家阶段日期 2004.7.8
[71] 申请人 株式会社 NTT 都科摩
地址 日本东京
[72] 发明人 山田和宏 渡边信之 津田雅之
神谷大 浅井真生 三浦史光
鹫尾谕 富冈淳树 川端博史
近藤隆

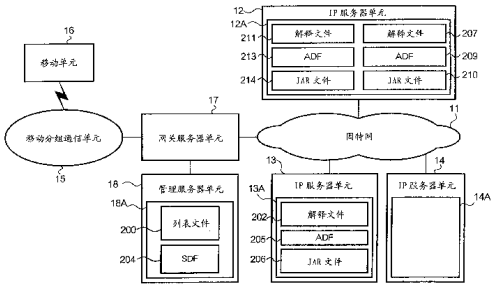
[74] 专利代理机构 北京三友知识产权代理有限公司
代理人 李 辉

权利要求书 4 页 说明书 24 页 附图 15 页

[54] 发明名称 内容传送方法和内容传送系统

[57] 摘要

能够激活 Java – AP 软件的移动设备(16)从管理服务器设备(18)接收 SDF(安全描述文件)(204)，通过使用包含在所述 SDF 中的 URL 从 IP 服务器设备(13)获得 ADF(205)，并且通过使用 ADF(205)从 IP 服务器设备(13)获得 Jar 文件(206)，并且在其自身中安装包含这些文件的 Java – AP，其中所述管理服务器设备(18)由一可信赖的组织进行管理，该可信赖的组织是管理移动分组通信网(15)的通信供应商。通过激活所安装的 Java – AP 软件而实现的 Java – AP 在由 SDF(204)中所包含的策略信息所表达的授权范围内进行操作。



ISSN1008-4274

1、一种传送方法，包括：

授权文件传送过程，用于在通信系统中传送授权文件，在该通信系统中，源发站发起一包括显示文件存储的信息的请求，并且响应于该请求所述文件被传送，所述授权文件传送过程包括：通过安全链路把一安全描述文件作为所述授权文件从存储该安全描述文件的管理服务器单元传送到终端单元，该安全描述文件包含第一标识信息和授权信息，第一标识信息显示应用程序描述文件的存储位置，所述应用程序描述文件具有与实体文件相关的信息以及显示所述实体文件的存储位置的信息，所述实体文件包括用于执行应用程序的软件，所述安全描述文件的授权信息指示根据所述软件执行的应用程序的操作允许范围，所述终端单元在所述授权信息所示的范围内执行所述应用程序的操作；

相关信息获得过程，用于使所述终端单元通过使用在所述授权文件传送过程中从所述通信系统传送的所述安全描述文件中包含的所述第一标识信息，从其中存储有所述应用程序描述文件的一个或多个服务器单元中获得所述应用程序描述文件；以及

程序获得过程，用于使所述终端单元通过使用在所述相关信息获得过程中获得的所述应用程序描述文件，从所述通信系统中获得所述实体文件。

2、根据权利要求1的传送方法，

其中，通过所述相关信息获得过程从所述管理服务器单元获得所述应用程序描述文件。

3、根据权利要求1的传送方法，

其中，通过所述程序获得过程从所述管理服务器单元获得所述实体文件。

4、根据权利要求1的传送系统，

其中，在所述相关信息获得过程中从所述管理服务器单元获得所述应用程序描述文件，以及

其中，在所述程序获得过程中从所述管理服务器单元获得所述实体文件。

5、根据权利要求1的传送方法，进一步包括：

加密过程，用于使所述通信系统对所述安全描述文件进行加密；以及

解码过程，用于使所述终端单元对在所述授权文件传送过程中由所述通信系统传送的所述安全描述文件进行解码，

其中，在所述授权文件传送过程中，将在所述加密过程中加密的所述安全描述文件传送至所述终端单元，以及

其中，在所述相关信息获得过程中，所述终端单元通过使用在所述解码过程中解码的所述安全描述文件来获得所述应用程序描述文件。

6、根据权利要求1的传送过程，其中所述授权信息显示对资源使用的限制。

7、根据权利要求6的传送方法，其中所述资源是所述终端单元内的硬件资源。

8、根据权利要求6的传送方法，其中所述资源是所述终端单元可以使用的位于所述终端单元之外的硬件资源。

9、根据权利要求6的传送方法，其中所述资源是所述终端单元内的软件资源。

10、根据权利要求6的传送方法，其中所述资源是所述终端单元可以使用的位于所述终端单元之外的软件资源。

11、根据权利要求6的传送方法，其中所述资源是所述终端单元可以使用的网络资源。

12、根据权利要求1的传送方法，其中所述授权信息显示资源使用的类型。

13、根据权利要求1的传送方法，其中对应于所述应用程序的应用程序描述文件由授证中心给予提供所述应用程序的信息供应商的秘密密钥来签名，

其中，对应于所述应用程序的安全描述文件包含授证中心给予所述

信息供应商的公开密钥，以及

其中，在所述程序获得过程中，所述终端单元通过使用所述公开密钥来检查在所述相关信息获得过程中获得的应用程序描述文件的可靠性，并且仅当可靠性得到验证时，通过使用所述应用程序描述文件从所述通信系统获得所述实体文件。

14、根据权利要求1的传送方法，

其中，所述应用程序描述文件和所述安全描述文件包含一由管理所述管理服务器单元的管理者给予的应用程序标识符，以及

其中，在所述程序获得过程中，所述终端单元将在所述授权文件传送过程中由所述管理服务器单元传送的安全描述文件中所包含的应用程序标识符与在所述相关信息获得过程中获得的应用程序描述文件中包含的应用程序标识符进行比较，并且仅当两个标识符匹配时，通过使用所述应用程序描述文件从所述通信系统中获得所述实体文件。

15、根据权利要求1的传送方法，

其中，所述通信系统进一步包括一信息提供服务器单元，在该信息提供服务器单元中用于下载的文件包含显示所述安全描述文件的存储位置的第二标识信息；

预先（advance）传送过程，用于使所述通信系统将所述用于下载的文件传送至一终端单元；以及

授权文件传送请求过程，用于使所述终端单元通过使用由所述通信系统在所述预先传送过程中传送的所述用于下载的文件，请求所述通信系统传送所述安全描述文件，

其中，在所述授权文件传送过程中，所述通信系统向所述终端单元传送由所述授权文件传送请求过程所请求的所述安全描述文件。

16、根据权利要求1的传送方法，

其中，仅当在所述相关信息传送过程中传送的安全描述文件存储在所述管理服务器单元之中时，执行一在所述相关信息获得过程之后的过程。

17、根据权利要求1至权利要求16中的任何一项的传送方法，

其中所述终端单元是移动单元。

18、一种传送系统，包括：

通信系统，用于在被告知一文件的存储位置时返回该文件，该通信系统包括：一个或多个服务器单元，其中存储有实体文件和应用程序描述文件，所述实体文件包含用于实现应用程序的软件，所述应用程序描述文件具有与所述实体文件相关的显示所述实体文件的存储位置的内容；和一管理服务器单元，其中存储有一安全描述文件，该安全描述文件包含用于显示所述应用程序描述文件的存储位置的第一标识信息，和用于显示当终端单元执行所述软件时实现的应用程序所被给予的授权的授权信息；以及

终端单元，根据应用程序所被给予的授权来批准所述应用程序的操作，

其中，所述管理服务器单元通过确保安全来向所述终端单元传送所述安全描述文件，以及

其中，所述终端单元通过使用在由所述通信系统传送的所述安全描述文件中所包含的所述第一标识信息，来获得所述应用程序描述文件，并且通过使用所述应用程序描述文件从所述通信系统获得所述实体文件。

19、根据权利要求18的传送系统，

其中，所述管理服务器单元存储所述应用程序描述文件。

20、根据权利要求18的传送系统，

其中，所述管理服务器单元存储所述实体文件。

21、根据权利要求18的传送系统，

其中，所述管理服务器单元存储所述应用程序描述文件，并且

其中，所述管理服务器单元存储所述实体文件。

内容传送方法和内容传送系统

技术领域

本发明涉及向终端单元传送应用软件。

背景技术

配备有通过执行根据Java（注册商标）编程语言编写的并且通过网络下载的程序来执行Java-AP（Java应用）软件的功能的移动单元正在得到广泛应用。

Java-AP软件包括Jar（Java档案文件）文件和ADF（应用程序描述符文件）。Jar文件包含为用户提供某个Java-AP的程序。ADF依赖于Jar文件，并且包含，例如，显示Jar文件存储位置的URL（在下文中，称为程序包（package）URL）、Jar文件的大小、Jar文件变化的最近日期及其他必要的信息。

移动单元按照如下所述的过程将有关的软件下载到希望的Java-AP。首先，移动单元从构成WWW（万维网）的服务器单元获得与希望的Java-AP有关的ADF。

获得ADF的移动单元检查ADF的内容，并且确定与希望的Java-AP有关的Jar文件是否可以安装在移动单元内。当移动单元确定可以安装Java-AP软件时，移动单元通过使用包含在ADF中的程序包URL从构成WWW的服务器单元处获得Jar文件。当获得Jar文件时，下载Java-AP软件的过程就完成了。在下文中，在移动单元中，执行下载的Java-AP软件的安装，并且当需要时可以激活该Java-AP软件。

顺便说一句，当把Java-AP软件安装在移动单元之中时，Java-AP的激活比移动单元的本机功能（如通信应用功能）的激活要受到更大的限制。Java-AP的激活受到的限制在于，它不能访问包括在移动单元内的某些数据，例如电话号码。通过以这种方式施加严格的限制，可以防止由

于误操作Java-AP或有意导致而发生的包括在移动单元内的机密数据的泄漏或篡改。

然而，同等地对所有Java-AP施加以上的限制不能充分地满足移动单元用户或IP（信息供应商）的需要。例如，一些用户似乎觉得只要安全有保证，就可以允许Java-AP访问存储在移动单元中的一些私人信息。此外，一些IP希望提供Java-AP，并且这些Java-AP可以使用存储在移动单元中的一些私人信息，或者移动单元配备有的功能中的一些。

为了满足这些要求，系统受托负责授权Java-AP以更大的灵活性进行操作，在该系统中，一个例如向移动单元用户提供通信业务的通信供应商的可信赖组织充当了管理者。通过为Java-AP设置的操作规则的授权来通知使用Java-AP的移动单元，并且移动单元可以根据规定的规则来限制Java-AP的操作。在此系统中，应当仅委托一个可信赖的组织来管理Java-AP更灵活操作的授权。

当上述系统被用于Java-AP软件的下载过程时，必须包括显示ADF或Jar文件中的授权的信息。由于按要求由IP更新Jar文件，并且对于IP来说适合于拥有Jar文件，所以对应的ADF适合于包含有关授权有效性的消息。

然而由于ADF的内容取决于Jar文件，所以一旦IP更新Jar文件，就需要更新可信任组织拥有的ADF。此外，有时即使没有更新Jar文件，更新ADF也成为必需的，如在以下情况下，对某个Jar文件的访问过多，以及Jar文件被移到IP中的另一个服务器单元。在这种情况下，由于存储Jar文件的位置变化了，所以需要改变包括在ADF内的程序包URL。然而，由于ADF是由可信赖的组织管理的并且排除了其他代理的介入，所以ADF的更新操作可能成为非常繁忙的操作。

发明内容

开发本发明是为了克服传统技术的所述问题，并且本发明的目的是提供一种传送方法和传送系统，用于在不限制IP的自由的情况下，向允许应用程序根据授权进行操作的终端单元传送软件，该软件用于实现通

过传送彼此相关的多个文件而传送的应用程序。

为了解决传统技术的上述问题，本发明提供了一种传送方法，包括：授权文件传送过程，用于在通信系统中传送授权文件，在该通信系统中，源发站发起一包括显示文件存储的信息的请求，并且响应于该请求所述文件被传送，所述授权文件传送过程包括：通过安全链路把一安全描述文件作为所述授权文件从存储该安全描述文件的管理服务器单元传送到终端单元，该安全描述文件包含第一标识信息和授权信息，第一标识信息显示应用程序描述文件的存储位置，所述应用程序描述文件具有与实体文件相关的信息以及显示所述实体文件的存储位置的信息，所述实体文件包括用于执行应用程序的软件，所述安全描述文件的授权信息指示根据所述软件执行的应用程序的操作允许范围，所述终端单元在所述授权信息所示的范围内执行所述应用程序的操作；相关信息获得过程，用于使所述终端单元通过使用在所述授权文件传送过程中从所述通信系统传送的所述安全描述文件中包含的所述第一标识信息，从其中存储有所述应用程序描述文件的一个或多个服务器单元中获得所述应用程序描述文件；以及，程序获得过程，用于使所述终端单元通过使用在所述相关信息获得过程中获得的所述应用程序描述文件，从所述通信系统中获得所述实体文件。

通过此传送方法，在获得应用程序描述文件和对应于应用程序的实体文件之前，终端单元获得安全描述文件，该安全描述文件由通信系统在已经确保安全性之后进行传送。在安全描述文件中，指示了应用程序被给予的授权，并且在终端单元中，允许对应于该安全描述文件的应用程序根据由所获得的安全描述文件指示的授权进行操作。

此外，本发明提供了一种传送系统，包括：通信系统，用于在被告知一文件的存储位置时返回该文件，该通信系统包括其中存储有实体文件和应用程序描述文件的一个或多个服务器单元，，所述实体文件包含用于实现应用程序的软件，所述应用程序描述文件具有与所述实体文件相关的显示所述实体文件的存储位置的内容，该通信系统还包括一其中存储有安全描述文件管理服务器单元，该安全描述文件包含用于显示所

述应用程序描述文件的存储位置的第一标识信息，和用于显示当终端单元执行所述软件时实现的应用程序所被给予的授权的授权信息；以及终端单元，根据所述应用程序所被给予的授权来批准应用程序的操作，其中，所述管理服务器单元通过确保安全性来向所述终端单元传送所述安全描述文件，并且其中，所述终端单元通过使用在由所述通信系统传送的所述安全描述文件中所包含的所述第一标识信息，来获得所述应用程序描述文件，并且通过使用所述应用程序描述文件从所述通信系统获得所述实体文件。

通过该传送系统，在获得应用程序描述文件和对应于应用程序的实体文件之前，终端单元获得在已经确保安全之后由传送系统传送的安全描述文件。在安全描述文件中，指示了应用程序被给予的授权，并且在终端单元中，对应于所述安全描述文件的应用程序被允许根据由获得的安全描述文件所指示的授权的许可进行操作。

附图说明

图 1是示出用于执行本发明的一个实施例的传送系统的配置的框图。

图 2是示出传送系统固有的ADF的数据配置的概念图。

图 3是示出构成传送系统的移动单元16的配置的框图。

图 4是示出移动单元16的功能结构的概念图。

图 5是示出移动单元16的用于下载和安装Java-AP软件的过程的流程图。

图 6是示出存储在传送系统中的管理服务器单元18中的SDF的数据配置的概念图。

图 7是示出包括在SDF内的策略信息的内容的概念图。

图 8是用于解释传送系统的操作的框图。

图 9是示出在传送系统中传送的列表页的示意图。

图 10是示出存储在构成传送系统的IP服务器单元12中的说明性文件的内容示意图。

图 11是示出在传送系统中传送的说明性页面的示意图。

图 12是示出存储在IP服务器单元12中的说明性文件的内容的示意图。

图 13是示出在传送系统中传送的说明性页面的示意图。

图 14是示出存储在构成传送系统的IP服务器单元13中的说明性文件的内容的示意图。

图 15是示出在传送系统中传送的说明性页面的示意图。

图 16是用于解释传送系统的操作的顺序图。

图 17是用于解释传送系统的操作的顺序图。

图 18是用于解释传送系统的操作的顺序图。

图 19是用于解释传送系统的另一个操作的框图。

图 20是用于解释传送系统的另一个操作的顺序图。

具体实施方式

在下文中，通过参照附图，解释了本发明的一个模式的传送系统。在图中，相同的附图标记指示共有的部分。

（1）配置

如图1所示，在所述传送系统中，IP服务器单元12到14被连接到互联网11。IP服务器单元12由第一IP（国际互联网供应商）管理，并且IP服务器单元13和14由不同于第一IP的第二IP管理。IP服务器单元12到14构成WWW，并且每个都配备了与通用WWW服务器单元类似的硬件与功能。移动分组通信网15是通信供应商用于提供移动分组通信服务的网络。移动单元16可以与移动分组通信网15进行无线分组通信。网关服务器单元17由与移动分组通信网15的通信供应商相同的通信供应商管理。网关服务器单元17是用于连接移动分组通信网15和国际互联网11的单元，并且具有与普通网关服务器单元类似的配置。管理服务器单元18由专用线路连接到网关服务器单元17。管理服务器单元18也构成WWW，并且具有与通用WWW单元类似的硬件和功能。网关服务器单元17执行移动分组通信网15与国际互联网11之间的分组通信、管理服务器单元18与移动分组通信网15之

间的分组通信，以及管理服务器单元18与国际互联网11之间的分组通信。通过使用中继功能，移动单元16能够经由移动分组通信网15和国际互联网11与IP服务器单元12到14进行分组通信。实际传送系统中存在若干个移动单元，但是为避免使图变复杂仅仅显示了一个移动单元16。为了同样的理由，仅仅显示了IP服务器单元12到14。

在传送系统中，移动单元16能够从国际互联网11上的希望站点接收Java-AP软件。在可信Java-AP相关软件与不可信Java-AP相关软件之间对移动单元16能够接收的软件进行区分。可信Java-AP软件是由管理移动分组通信网15的通信供应商基于与管理IP服务器单元12到14的IP的合同保证其可靠性的软件。不可信Java-AP软件是除了可信Java-AP软件之外的任何Java-AP软件。

管理服务器单元18存储与在传送系统中传送的每个可信Java-AP软件有关的每一个SDF（安全描述文件）。SDF是由管理移动分组通信网15的通信供应商产生的文件，并且是用于将使用移动单元的可信API（应用程序接口）的Java-AP软件下载到移动单元中所需的文件。稍后将解释可信API。如图6所示，SDF包含用于检测可信Java-AP软件的APID、策略信息、显示对应于Java-AP软件的ADF的存储位置的ADF-URL，以及CA（授证中心）给予提供Java-AP软件的IP的公开密钥。策略信息是显示对Java-AP的操作的限制的信息。后面将详细说明策略信息和根据策略信息执行的对Java-AP操作的限制。

在本实施例中，当可信Java-AP软件由IP服务器单元12到14中的一个传送到移动单元16时，响应于来自移动单元16的请求，由管理服务器单元18把对应于可信Java-AP软件的SDF传送到移动单元16。 在移动单元16中，当执行可信Java-AP软件时，根据对应于该可信Java-AP的SDF来执行对可信Java-AP操作的限制。这是本实施例的一个特征。如图1所示，通过移动分组通信网15执行SDF的传送，并且通过专用线路将管理服务器单元18和网关服务器单元17连接起来。此外，为了传送，对SDF进行加密。

在下文中，针对与特征的相关性，对所述传送系统的每个要素的配置进行解释。

IP服务器单元12、13和14分别配备了固定存储器12A、13A和14A。

固定存储器12A、13A和14A是诸如硬盘的固定存储器，并且存储有构成Jar文件和ADF的Java-AP软件以及为移动单元用户提供的关于Java-AP软件内容的说明性文件。

存储在固定存储器12A、13A和14A的每个Java-AP软件可能是可信Java-AP软件或者不可信Java AP软件。不论Java-AP是可信Java-AP还是不可信Java-AP，在Java-AP软件的每个ADF中，存储有例如显示WWW中的Jar文件的存储位置的程序包URL的信息、显示Jar文件的大小的信息，以及显示写入最近更新的日期的信息。这样的信息通常被称为将要写入Java-AP软件的ADF中的项目。此外，可信Java-AP软件的ADF，如图2所示，包含除所述通常已知的信息之外的可信Java-AP的APID和Jar文件的散列值（hash value）。此外，通过CA给予提供软件的IP的秘密密钥来对可信Java-AP软件的ADF进行加密。

此外，说明性文件是根据HTML写入的文本文件。当下载某个Java-AP软件时，移动单元需要提前下载对应于该Java-AP软件的说明性文件。说明性文件包含用于形成UI(用户界面)以接收来自用户的用于下载Java-AP软件的命令的信息。移动单元16根据该信息显示UI屏面。用户可以在移动单元16上执行操作以在UI屏面上指定显示所述希望的Java-AP的对象。为用户如此指定的对象而写入的说明性文件对应于显示与作为下载对象的Java-AP软件对应的SDF（ 如果SDF不存在，则是ADF)在WWW中的位置的URL。

IP服务器单元12到14中的每一个都根据IP的命令配备了产生和更新上述每一个文件的功能。

管理服务器单元18配备了固定存储器18A，例如硬盘。管理服务器单元18建立与对方（party）的TCP连接。当管理服务器单元18通过TCP连接从对方接收使用HTTP的GET方法的请求消息时，管理服务器单元18从固定存储器18A中读出由GET方法指定的URL所标识的文件，并且返回包含该文件的HTTP的响应消息，并且断开连接。

此外，在上述固定存储器I8A中存储了用于向移动单元16的用户介绍

可下载的Java-AP软件的列表文件200，和对应于在列表文件200中所列出的每个Java-AP软件的相应的SDF。

列表文件200，如SDF，是由通信供应商根据对IP服务器单元12到14进行管理的每个IP和对管理服务器单元18进行管理的通信供应商签署的合同而产生的。列表文件200是根据HTML编写的文本文件。如已经解释过的，移动单元需要获得包含SDF的URL的说明性文件以下载某个Java-AP软件的SDF。移动单元16可以通过访问其中存储有说明性文件的IP服务器单元来直接获得所述说明性文件。然而，在本实施例中，移动单元16还可以通过与以上直接方法相反的下列过程来获得所希望的Java-AP软件的说明性文件。首先，移动单元16通过访问管理服务器单元18来获得列表文件200，并且据此显示UI屏面。用户可以在移动单元16上执行操作以在UI屏面上指定显示所希望的Java-AP的目标。 列表文件200把用户指定的目标与一URL进行匹配，该URL显示了作为下载目标的Java-AP软件的说明性文件在WWW中的位置。移动单元16通过使用经由列表文件200获得的URL来从IP服务器单元获得所述说明性文件。

如图3所示，移动单元16包括：OS (操作系统)软件；ROM 16A，在其中存储了用于建立Java -AP的执行环境的Java-AP环境软件，和几种类型的本机AP软件；CPU 16B，连接到ROM 16A，用于从ROM I6A读出程序并且执行该程序；连接到CPU 16B的显示单元16C；固定存储器16D；RAM 16E；通信单元16F；以及操作单元16G。

显示单元I6C具有例如液晶显示面板，并且把CPU 16B提供的数据显示为图像。 固定存储器16D是例如SRAM或EEPROM，并且由CPU 16B来读取和写入数据。固定存储器16D 用来存储从构成WWW的服务器单元(在下文中，称为网络（Web）服务器单元)下载的Java-AP软件(ADF和Jar)，以及SDF。

通信单元16F执行与移动分组通信网15的无线分组通信，并且在CPU 16B与移动分组通信网15之间中继分组。此外，通信单元16F除配备有天线或无线发送和接收单元之外，还配备有用于通信的 CODEC、麦克风、扬声器等等。因此，移动单元16借助于通信单元16F，可以经由移动通信

网络(未显示)通过电路交换来执行通信。操作单元16G配备有操作控制器，并且根据操作控制器执行的操作来向CPU 16B提供信号。

接通开关（未显示)时，CPU 16B从ROM 16A中读出包括在OS软件内的程序，并且以RAM I6E作为工作区来执行该程序。结果，在CPU 16B 中执行了用于提供UI等的功能。换句话说，CPU 16B激活OS软件，并且在移动单元16中执行图4的OS。OS根据由操作单元16G提供的信号和UI的状态来识别用户的命令，并且根据该命令执行所述过程。

当用户的命令请求激活作为本机AP软件的通信软件时，OS激活该通信软件，并且在移动单元16中执行通信AP。通过使用通信AP，用户可以与对方进行通信。

当用户的命令请求激活作为本机AP软件的电话号码簿AP时，OS激活该电话号码簿软件，并且在移动单元16中执行电话号码簿AP。通过使用电话号码簿AP，用户可以查阅、使用以及改变存储在固定存储器16D中的电话号码簿的内容（在下文中，称为电话号码簿数据）。

当用户的命令请求激活作为本机AP软件的Web浏览器软件时，OS激活该Web浏览器软件，并且在移动单元16中执行Web浏览器。而且，Web浏览器提供UI。然后，当用户通过对操作单元16G进行操作来发出命令时，Web浏览器根据UI的状态和操作单元16G提供的信号来识别用户的命令，并且根据该命令来执行所述过程。例如，当命令用于从WWW获得指定的文件时，通过操作通信单元16F建立与其中存储有文件的Web服务器单元的TCP连接，通过显示指定位置的URL来传送使用GET方法的HTTP请求消息，接收对应于该请求消息的响应消息，并且断开连接。此外，Web浏览器根据HTML解释包括在接收到的响应消息内的文件，产生包含网页的UI，并且提供给用户。此外，当用户发送用于下载Java-AP软件的命令时，向JAM (Java应用程序管理器)报告该命令。具体来说，在网页中，当指定说明对象标记的锚标记时，通过点击或按下，Web浏览器提取作为对象标记的数据属性而指定的URL，并且通知JAM请求通过URL来下载Java-AP软件。

当用户的命令请求激活作为本机AP软件的JAM软件时，OS激活JAM软件，并且在移动单元16中执行JAM。JAM向用户显示在移动单元16中安装

的Java-AP软件的列表，并且激活由用户指定的Java-AP软件。具体来说，当发向JAM的用户命令请求激活Java-AP软件时，激活Java-AP环境软件，并且在移动单元16中执行Java-AP环境。然后，激活所指定的Java-AP软件，并且在Java-AP环境中执行Java-AP。 Java-AP环境包括KVM和为Java-AP提供的API，所述KVM是适合于蜂窝终端的轻量级Java虚拟机。为Java-AP提供的API被分成可信API和不可信API，只有那些由通信供应商根据与IP签订的合同保证其可靠性的Java-AP（下文中，被称为可信AP）才被允许使用可信API,任何Java-AP都允许使用不可信API。

（2）操作

在下文中将解释本实施例的操作。当Web浏览器报告了用于请求下载Java-AP的命令时， JAM执行用于将Java-AP软件下载和安装到移动单元16中的过程。在图5中显示了所述过程的流程。在图5中，省略了移动单元16的用于获得说明性文件的过程。因为对于获得说明性文件的过程存在一些不同的模式，稍后以该操作的一些具体示例来对所述过程进行说明。如图5所示，JAM首先确定即将下载的Java-AP软件是不是可信Java-AP软件(步骤S11)。具体来说，当移动单元16获得所述说明性文件时，Web浏览器向用户提供对应于该说明性文件的UI，并且从用户处接收用于下载Java-AP软件的命令。Web浏览器向JAM报告由用户指定的Java-AP软件的URL。JAM参照位于由Web浏览器报告的URL的结尾的文件名，并且如果文件的扩展名是“sdf”，则确定软件是可信Java-AP软件，如果文件的扩展名不是“sdf”，则确定软件为不可信Java-AP软件。当即将下载的Java-AP软件被确定为可信Java-AP软件时，执行与常规过程相同的下载和安装过程（步骤S12）。

当即将下载的Java-AP软件被确定为可信Java-AP软件时，JAM从管理服务器单元18获得对应于所述软件的SDF（步骤S13）。换句话说，JAM建立与管理服务器单元18的TCP连接，经由该TCP连接产生并传送一请求消息，以请求管理服务器单元18传送存储在由Web浏览器报告的URL所显示的位置中的SDF，接收所述请求消息的响应消息，并且断开上述连接。

然后，JAM从包括在所述响应消息内的SDF中提取APID、ADF-URL和公

开密钥，并且把SDF写入固定存储器16D中。

接下来，JAM获得ADF（步骤S14）。具体来说，JAM建立与Web服务器单元的TCP连接，在该Web服务器单元中存储有由从SDF中提取的ADF-URL所标识的ADF，JAM还产生并发送用于请求传送ADF的请求消息，接收该请求消息的响应消息，并且断开所述TCP连接。

如已经解释过的，对应于可信Java-AP软件的ADF包括APID的散列值和Jar文件，并且进一步由CA给予提供可信Java-AP软件的IP的秘密密钥来签名（加密）。然后，JAM通过使用从SDF中提取的公开密钥来检查(解码)包括在所述响应消息内的ADF的签名，并且确定该ADF的可靠性(步骤S15)。

当确定一ADF可靠时，JAM将从SDF中提取的APID与包括在所述ADF内的APID进行比较，并且确定这些APID是否匹配(步骤S16)。当确定这些APID匹配时，JAM根据所述ADF的内容确定是否可以将可信Java-AP软件安装在移动单元16中（步骤S17)。确定的根据与传统的根据相同。

当确定可以安装时，JAM获得所述Jar文件。具体来说，JAM把所述ADF写入移动单元16中，并且从所述ADF中提取散列值和程序包URL。此外，JAM建立与其中存储有由程序包URL所标识的Jar文件的Web服务器单元的TCP连接，产生并发送用于请求传送所述Jar文件的请求消息，接收所述请求消息的响应消息，并且断开所述TCP连接(步骤S18)。

此外，JAM计算所获得的Jar文件的散列值(步骤S19)。可以使用任何散列函数来计算该散列值，但是由所述移动单元使用的散列值与IP用于计算包括在ADF内的散列值的散列值必须相同。

JAM将由JAM计算出的散列值与从所述ADF中提取的散列值进行比较(步骤S20)，当这些散列值匹配时把所获得的Jar文件写入管理服务器单元18，执行若干种与安装可信Java-AP软件有关的步骤(步骤S21)，并且通知用户安装成功（步骤S22）。

当确定一ADF不可靠时，当SDF的APID和ADF的APID不匹配时，当确定即将安装的Java-AP软件不可安装时，以及当所计算出的散列值和ADF的散列值不匹配时，JAM通知用户安装失败，并且把移动单元16的状态返回

到开始获得SDF之前的状态。

此外，JAM监督Java-AP的操作，并且限制可信API的使用。根据存储在固定存储器16D中的SDF中的策略信息来实施所述限制。例如，SDF中的策略信息是在图7中概念性地显示的内容。在图7所示的策略信息中，允许使用用于查阅电话号码簿数据的必要的可信API“getPhoneList()”，以及用于获得存储在移动单元中的移动单元状态的必要的可信API“getMsStatus()”，禁止使用用于查阅存储在移动单元中的发送和接收历史记录数据“getCallHistory()”的必要的可信API。

（3）具体操作

接下来，解释上述系统的操作。

在以下解释的操作中，建立TCP连接和断开操作是HTTP的普通操作；因此，省略了对这些操作的说明。此外，由OS、Web浏览器、JAM、Java-AP、本机AP等执行的以上操作是移动单元16的操作；因此，在下面的解释中，执行操作的主要单元是移动单元16。

在下文中所解释的操作中，下列情况是先决条件。首先，如图8所示，在管理服务器单元18的固定存储器18A中，存储有列表文件200和SDF 204。在此阶段，当由移动单元16解释和执行列表文件200时，写入列表文件200以提供图9中所显示的列表页201。此外，当通过点击或者按键指定构成列表页201的选项201A时，写入列表文件200，以产生包括说明性文件202的URL（“http://www.main.bbb.co.jp/ghi.html”）的请求消息作为GET方法的参数。此外，当指定构成列表页201的选项201B时，写入列表文件200，以产生包括说明性文件207的URL（“http://www.ccc.co.jp/jkl.html”）的请求消息作为GET方法的参数。

此外，SDF 204包含作为APID的“0001”、作为策略信息的显示在图7中的信息、作为ADF－URL的“http://www.main.bbb.co.jp/viewer.jam”，以及CA给予对IP服务器单元13和IP服务器单元14进行管理IP的公开密钥。

此外，在IP服务器单元12的固定存储器12A中，存储有与标题“tsume-shogi”（类似于“象棋“的游戏）的Java-AP软件（在下文中，称为第

—Java-JP软件)对应的说明性文件211、ADF 213以及Jar文件214。 由管理IP服务器单元12的IP产生说明性文件211、ADF 213和Jar文件214。说明性文件211的内容显示在图10中。当由移动单元16解释和执行说明性文件211时，写入说明性文件211以提供在图11中显示的说明性页面212。此外，ADF 213包括作为程序包URL的Jar文件214的URL（“http://www.ccc.co.jp/shogi.jar”）。

同时，在IP服务器单元12的固定存储器12A中，存储有与标题“horoscope”的Java-AP软件(在下文中，称为第二Java-AP软件)对应的说明性文件207、ADF209，以及Jar文件210。 由对IP服务器单元12进行管理的IP产生说明性文件207、ADF 209和Jar文件210。说明性文件207的内容显示在图12中。当由移动单元16解释和执行说明性文件207时，写入说明性文件207以提供显示在图13中的说明性页面208。此外，ADF 209包括作为程序包URL的Jar文件210的URL(“http://www.ccc.co.jp/horoscope.jar”)。

此外，在IP服务器单元13的固定存储器13A中，存储有与标题“电话号码簿查阅器”的Java-AP软件(在下文中，称为第三Java-AP软件)对应的说明性文件202、ADF205，以及Jar文件206。由对IP服务器单元13和IP服务器单元14进行管理的IP产生说明性文件202、ADF 205和Jar文件206。说明性文件202的内容显示在图14中。当移动单元16解释和执行说明性文件202时，写入说明性文件202以提供在图15中显示的说明性页面203。ADF 205包括作为APID的“0001”、Jar文件206的散列值、作为程序包URL的Jar文件206的URL（“http://www.main.bbb.co.jp/viewer.jar”），并且由CA给予对IP服务器单元13和IP服务器单元14进行管理的IP的秘密密钥进行签名。

此外，移动单元16处于其中可以下载第一到第三Java-AP软件的状态。

（2-1）安装操作

首先，参照每个Java-AP软件来说明在移动单元16中安装Java-AP软件的操作。

（2-1-1）第一Java-AP软件

当用户发现了其中存储有他/她所期望的Java软件的IP服务器单元时，开始第一Java-AP软件的安装操作，然后通过操作移动单元16来尝试获得Web浏览器中的说明性文件211。首先，在移动单元16中，产生包括作为GET方法的参数的说明性文件211的URL（“http://www.ccc.co.jp/mno.html”）的请求消息tm 12。 如图16所示，请求消息tm 12由移动单元16发送，并且由IP服务器单元12接收。在IP服务器单元12中，响应于请求消息tm 12的内容产生包括说明性文件211的响应消息tm 13。 响应消息tm 13由IP服务器单元12发送，并且由移动单元16接收。在移动单元16中，为用户提供与说明性文件211的内容对应的UI。结果，在显示单元16C中，例如，显示了在图11中所示的说明性页面212 。

当用户看到说明性页面212，并且操作移动单元16以命中说明性页面212中的锚212A时，被指定为写入在图10的说明性文件211中的锚标记（以“<A”开始的标记）的ijam属性对被指定为移动单元16中的id属性（以“<OBJECT”开始的标记）的对象标记进行识别。然后，提取被指定为所述对象标记的数据属性的URL（“http://www.ccc.co.jp/shogi.jam”），并且执行图5中的步骤S11的判定。在本示例中，由于URL的扩展名不是sdf，所以执行常规过程(步骤S12)。换句话说，按如下执行所述过程。首先，产生用于请求传送由所述URL标识的ADF 213的请求消息tm 16。 响应消息tm 16由移动单元16发送，并且由IP服务器单元12接收。在IP服务器单元12中，响应于请求消息tm 16的内容，产生包括ADF 213的响应消息tm 17。响应消息tm 17由IP服务器单元12发送，并且由移动单元16接收。

在移动单元16中，根据ADF 213的内容，确定是否可以安装第一Java-AP软件。如上所述，由于移动单元16处于可以安装第一Java-AP软件的状态，所以确定可以在移动单元16中安装第一Java-AP软件。

然后，在移动单元16中，将ADF 213写入固定存储器16D1中。此外，在移动单元16中，从ADF 213中提取程序包URL（“http://www.ccc.co.jp/shogi.jar”），并且产生请求传送由该程序包URL所标识的Jar文件2

14的请求消息tm 18。响应消息tm 18由移动单元16发送，并且由IP服务器单元12接收。在IP服务器单元12中，响应于请求消息tm 18的内容产生包括Jar文件214的响应消息tm 19。响应消息tm 19由IP服务器单元12发送，并且由移动单元16接收。在移动单元16中，将Jar文件214写入固定存储器16D1中，并且完成第一Java-AP软件的安装。

当确定不可在移动单元16中安装第一Java-AP软件时，移动单元16的状态返回到开始获得ADF 213之前就存在的状态。

（2-1-2）第二Java-AP软件

当用户通过操作移动单元16来尝试获得说明性文件207时，开始第二Java-AP软件的安装操作。如已经解释过的，通过直接访问有关的IP服务器或者通过列表文件200可以获得说明性文件207，但是只对以尝试获得列表文件200而开始的操作进行说明。

如图17所示，在移动单元16中，产生包括作为GET方法的参数的列表文件200的URL（“http://www.aaa.co.jp/def.html”）的请求消息tm 20。请求消息tm 20由移动单元16发送，并且是由管理服务器单元18接收。在管理服务器单元18中，响应于请求消息tm 20的内容产生包括列表文件200的响应消息tm 21。响应信息tm 21由管理服务器单元18发送，并且由移动单元16接收。在移动单元16中，当接收到响应消息tm 21时，根据HTML对响应消息tm 21中的列表文件200进行解释，并且向移动单元16的用户提供与列表文件200的内容对应的UI。结果，在移动单元16的显示单元16C中，显示了例如在图9中所示的列表页201。

当用户在看到列表页201之后操作移动单元16以命中列表页201内的选项201B时，产生包括作为GET方法的参数的对应于选项201B的URL（“http://www.ccc.co.jp.jkl.html”）的请求消息tm 22。请求消息tm 22由移动单元16发送，并且由IP服务器单元12接收。在IP服务器单元12中，响应于请求消息tm 22的内容产生包括说明性文件207的响应消息tm 23。响应消息tm 23由IP服务器单元12发送，并且由移动单元16接收。在移动单元16中，为用户提供与说明性文件207的内容对应的UI。结果，在显示单元16C中，显示了例如在图13中所示的说明性页面208。

当用户在看到说明性页面208以后，操作移动单元16以命中说明性页面208中的锚208A时，被指定为在图12的说明性文件207中写入的锚标记(以“<A”开始的标记)的ijam属性的值对被指定为id属性的对象标记(以“<OBJECT”开始的标记)进行识别。然后，提取被指定为所述对象标记的数据属性的URL(“http://www.ccc.co.jp/horoscope.jam”)，并且执行图5中的步骤S11的判定。在本示例中，由于URL的扩展名不是sdf，所以执行常规过程（步骤S12)。换句话说，按如下执行所述过程，首先，产生请求传送由所述URL标识的ADF 209的请求消息tm 26。请求消息tm 26由移动单元16发送，并且由IP服务器单元12接收。在IP服务器单元12中，产生包括与请求消息tm 26的内容对应的ADF 209的响应消息tm 27。响应消息tm 27由IP服务器单元12发送，并且由移动单元16接收。

在移动单元16中，根据ADF 209的内容，确定是否可以安装第二Java-AP软件。如上所述，由于移动单元16处于可以安装第二Java-AP软件的状态，所以第二Java-AP软件被确定为可在移动单元16中安装。

接下来，在移动单元16中，将ADF 209写入固定存储器16D1中。此外，在移动单元16中，从ADF 209中提取程序包URL（“http://www.ccc.co.jp/horoscope.jar”），并且产生请求传送由程序包URL所标识的Jar文件210的请求消息tm28。请求消息tm 28由移动单元16发送，并且由IP服务器单元12接收。在IP服务器单元12中，产生响应消息tm 29，该响应消息tm 29包括响应于请求消息tm 28的内容的Jar文件210。响应消息tm 29由IP服务器单元12发送，并且由移动单元16接收。在移动单元16中，将Jar文件210写入固定存储器16D1中，并且完成第二Java-AP软件的安装。

当确定第二Java-AP软件不可在移动单元16中安装时，移动单元16的状态返回到开始获得ADF 209之前存在的状态。

（2-1-3）第三Java-AP软件

当用户通过操作移动单元16尝试获得说明性文件202时，开始第三Java-AP软件的安装操作。在该操作中，移动单元16获得相关的列表文件200，确定说明性文件202的位置，并且尝试获得说明性文件202。

如图18中显示的，在通过试图获得列表文件200而开始的操作中，执

行与在图17中所示操作相同的操作，直到在移动单元16接收到响应消息tm 21之后显示了例如在图9中所示的列表页201。当用户在看到列表页201之后操作移动单元16以命中列表页201内的选项201A时，在移动单元16中产生包括作为GET方法一参数的对应于选项201A的URL（“http://www.main.bbb.co.jp/ghi.html”）的请求消息tm 32。请求消息tm 32由移动单元16发送，并且由IP服务器单元13接收。在IP服务器单元13中，产生响应消息tm 33，该响应消息tm 33包括响应于请求消息tm 32的内容的说明性文件202。响应消息tm 33由IP服务器单元13发送，并且由移动单元16接收。在移动单元16中，向用户提供与说明性文件202的内容对应的UI。结果，在显示单元16C中，显示了例如在图15中所示的说明性页面203 。

当用户在看到说明性页面203之后操作移动单元16以命中说明性页面203中的锚203A时，被指定为在图14中的说明性文件202中写入的锚标记(以“<A”开始的标记)的ijam属性的值对被指定为id属性的对象标记(以“<OBJECT”开始的标记)进行识别。然后，提取被指定为所述对象标记的数据属性的URL(“http://www.aaa.co.jp/abc.sdf”)，并且执行图5中的步骤S11的判定 。在本示例中，URL的扩展名是sdf；因此，执行步骤S13及其后的过程。换句话说，按如下执行所述过程。 首先，产生用于请求传送由所述URL标识的SDF 204的请求消息tm 34。请求消息tm 34由移动单元34发送，并且由管理服务器单元18接收。在管理服务器单元18中，产生包括响应于请求消息tm 34内容的SDF 204的响应消息tm 35。响应消息tm 35由管理服务器单元18发送，并且由移动单元16经由网关服务器单元17和移动分组通信网15接收。在管理服务器单元18与网关服务器17之间的通信路径是专用线路，并且由于网关服务器单元17直接连接到确保安全的移动分组通信网15，所以直到由移动单元16接收到SDF 204(在上文，步骤S13)之前，都不能篡改SDF 204。

在移动单元16中，将SDF 204写入固定存储器16D的固定存储器16D1中。此外，在移动单元16中，从SDF 204中提取APID（“0001”）、ADF-URL（“http://www.main.bbb.co.jp/viewer.jam”）、以及公开密钥，并且

产生请求传送由ADF-URL标识的ADF 205的请求消息tm 36。请求消息tm 36由移动单元16发送，并且由IP服务器单元13接收。在IP服务器单元13中，产生包括响应于请求消息tm 36内容的ADF 205的响应消息tm 37。响应消息tm 37由IP服务器单元13发送，并且由移动单元16接收(在上文中，步骤S14)。

在移动单元16中，通过使用从SDF 204提取的公开密钥来确定ADF 205的可靠性(步骤S15)。如上所述，由于包括在SDF 204内的公开密钥与被用在ADF 205上的签名的密钥相对应，所以ADF 205被确定是可靠的，只要在IP服务器单元13内，或者在IP服务器单元13和移动单元16之间的通信路径上，ADF 205没有发生变化。

当确定ADF 205可靠时，在移动单元16中，对从SDF 204提取的APID与包括在ADF 205内的APID进行比较(步骤S 16)。如上所述，由于在IP服务器单元13中的ADF 205中写入了与SDF 204中的APID相匹配的APID，所以只要描述是正确的，从SDF 204提取的APID就与包括在ADF 205内的APID相匹配。

当APID匹配时，在移动单元16，根据ADF 205的内容确定是否可以安装第三Java-AP软件(步骤S17)。如上所述，由于移动单元16处于可以安装第三Java-AP软件的状态，所以确定可在移动单元16中安装第三Java-AP软件。

然后，在移动单元16中，将ADF 205写入固定存储器16D1。此外，在移动单元16中，提取散列值和程序包URL（“http://www.main.bbb.co.jp/viewer.jar”），并且产生请求由传送所述程序包URL标识的Jar文件206的请求消息tm 38。请求消息tm 38由移动单元16发送，并且由IP服务器单元13接收。在IP服务器单元13中，产生包括与请求消息tm 38的内容对应的Jar文件206的响应消息tm 39。响应消息tm 39由IP服务器单元13发送，并且由移动单元16接收(在上文中，步骤S18)。

在移动单元16中，通过使用Jar文件206和特定的散列函数来计算所述散列值(步骤S19)，并且对所计算出的散列值与从ADF 205提取的散列值进行比较（步骤S20）。如上所述，在ADF 205中写入对应于ADF 205的

Jar文件的散列值；因此，只要描述是正确的，这些散列值就将匹配。当这些散列值匹配时，在移动单元16中，将Jar文件206写入固定存储器16D1中，并且完成第三Java-AP软件的安装(步骤S21和S22)。

当在移动单元16中确定ADF 205不可靠时，当从SDF 204提取的APID与包括在ADF 205内的APID不相匹配时，当确定不可安装第三Java-AP软件时，或者当所计算出的散列值与从ADF 205提取的散列值不相匹配时，向用户发送失败通知（步骤S23），并且移动单元16的状态返回到开始获得SDF 204之前存在的先前的状态。

(2-2)当激活Java -AP软件时移动单元16的操作

接下来，对当激活Java-AP软件时移动单元16的操作进行说明。

(2-2-1)第一Java-AP软件

下面说明当在移动单元16中激活通过上述安装操作安装的第一Java-AP软件时移动单元16的操作，在移动单元16中，实现了JAM，并且实现了对应于所述软件(在下文中，称为第一Java-AP)的功能。

当第一Java-AP即将使用的API是不可信API时，由JAM批准API的使用。因此，第一Java-AP可以使用所述API。

另一方面，当第一Java-AP即将使用的API是可信API时，JAM检查对应于该Java-AP的SDF是否存储在固定存储器16D中。由于这样的SDF不存储在固定存储器16D中，所以JAM禁止第一Java-AP使用所述API。因此，第一Java-AP不能使用所述API。

(2-2-2)第二Java-AP软件

当在其中实现了JAM并且实现了对应于所安装的第二Java-AP软件的功能的移动单元16中激活第二Java-AP软件时，移动单元16的操作与当激活第一Java-AP软件时移动单元16的操作相同。

（2-2-3）第三Java-AP软件

下面说明当在移动单元16中激活所安装的第三Java-AP软件时，移动单元16的操作，其中在所述移动单元16中实现了JAM，并且实现了对应于所述软件(在下文中，称为第三Java-AP)的功能。

当第三Java-AP即将使用的API是不可信API时，JAM批准该API的使

用。因此，第三个Java-AP使用该API。

当第三Java-AP即将使用的API是可信API时，移动单元16的操作取决于所述API。在下文中，参照每个API来说明移动单元16的操作。

（2-2-3-1）getPhoneList()

由于“getPhoneList()”是可信API，所以由JAM根据存储在固定存储器16D中的SDF 204中的策略信息来确定所述API是否能被使用。所述策略信息的内容是图7中所示的内容；因此，JAM批准使用“getPhoneList()”。因此，第三Java-AP可以使用“getPhoneList()”。换句话说，第三Java-AP可以读出电话号码簿数据。

（2-2-3-2）getCallHistory()

由于“getCallHistory()”是可信API，所以JAM根据SDF 204中的策略信息来确定是否可使用该API。由于所述策略信息的内容是在图7中所示的内容，所以JAM禁止使用“getCallHistory()”。因此，第三Java-AP不能使用“getCallHistory()”。换句话说，第三Java-AP不能读出发送和接收的历史记录数据。

(2-3)在第三Java-AP软件被改变之后的操作

接下来，将要解释在对IP服务器单元13和IP服务器单元14进行管理的IP改变第三Java-AP软件的传送模式或内容之后的本系统的操作。然而，本改变包括为了例如改进第三Java-AP软件而进行的Jar文件206的内容的变化，以及为了例如减轻IP服务器单元13上的负荷而进行的传送方式的改变。为了实现后一改变，如图19所示，对IP服务器单元13和IP服务器单元14管理的IP将所述改变之后的Jar文件206（在下文中，称为Jar文件215）存储在IP服务器单元14的固定存储器14A中，并且根据Jar文件215通过改变ADF 205的内容来产生ADF 216。为了传送在所述改变之后的第三Java-AP软件，需要上述操作，而不需要对管理服务器单元18进行管理的通信供应商的操作。

图20中显示了在这样的改变之后的第三Java-AP软件的安装操作。当在IP服务器单元13中产生了与包含ADF 205的响应消息tm 37相对的包含ADF 216的响应消息tm 47时，图20中所示的操作开始与在图18中所示的

操作不同。响应消息tm 47对应于响应消息tm 37，响应消息tm 48对应于响应消息tm 38，而响应消息tm 49对应于响应消息tm 39。

在IP服务器单元13中产生响应消息tm 47之后的操作基本上不同于图18中所示的操作，不同之处在于ADF 216和Jar文件215是所述过程的对象；在移动单元16中产生请求消息tm 48，其请求传送由包含在ADF 216内的程序包URL（“http://www.sub.bbb.co.jp/viewer.jar”）所标识的Jar文件215；请求消息tm 48由移动单元16发送，并且由IP服务器单元14接收；在IP服务器单元14中产生包含Jar文件215的响应消息tm 49；并且响应消息tm 49由IP服务器单元14发送，并由移动单元16接收。

（3）修改

在上述传送系统中，ADF和Jar文件由IP服务器单元发送，但是这其中的一个或全部两个可以由管理服务器单元发送。

此外，在上述传送系统中，移动单元基于使用秘密密钥和公开密钥的签名数据来确认SDF的制作者与ADF的制作者的通信的可靠性，但是根据系统所需的安全等级，通过不在SDF中包括公开密钥，通过在IP服务器单元中使用秘密密钥不对ADF签名，或者通过省略移动单元中的确认过程，可以减少在移动单元和IP服务器单元中的过程的长度，或者在移动单元、管理服务器单元和IP服务器单元之间的通信量。

此外，在上述传送系统中，所述Jar文件的散列值被包括在对应于该Jar文件的ADF中；并且在移动单元中计算所述散列值；然后通过将ADF中的散列值与计算出的散列值进行比较，来确认Jar文件和ADF通信的可靠性，但是根据系统所需的安全等级，通过省略所述确认处理，在ADF中不包括散列值，可以减少移动单元和IP服务器单元中的过程长度以及在移动单元和IP服务器单元之间的通信量。

此外，在上述传送系统中，通过使用可信Java-AP固有的APID，来确定SDF与ADF（和Jar文件）的通信是否可靠，但是可以通过使用提供可信Java-AP的信息供应商固有的CID来确定SDF与ADF（和Jar文件）的通信的可靠性。此外，取决于系统所需的安全等级，可以忽略基于APID和CID进行的确定。

此外，在上述传送系统中，通过使用域名来指定所述服务器，但是还可以通过使用IP地址来指定所述服务器。

此外，在该移动单元中，通过对传送SDF的服务器单元的域名与预设的字母串进行比较，只有当域名是由可信赖的组织所管理的服务器单元的域名时，才可以确定SDF是可靠的。在此模式中，将要比较的字母串(例如，显示通信供应商域名的字母串)预存在移动单元的ROM或固定存储器中。当字母串预存在ROM中时，可以保证高安全性，因为字母串不能被重写。此外，如果字母串预存在固定存储器中，在购买移动单元之后可以存储可信赖的组织；因此，可以为用户和可信赖的组织提供极好的便利性。

此外，在上述传送系统中，通过一作为可信赖的组织的提供用于传送SDF的通信路径的通信供应商，确保了高安全级别，但是本发明的技术范围包括其中通信路径不由可信赖的组织提供的模式。例如，通过使用加密的通信路径将可信赖的组织连接到移动单元，该可信赖的组织可以通过所述加密的通信路径来传送SDF。此外，即使不保证通信路径的安全，通过在加密SDF之后再传送，并且在移动单元中解码SDF，可以以某种程度的安全来传送SDF。

在上述传送系统中，根据HTTP传送与接收文件，但是可以对系统进行修改以通过使用HTTPS来确保更高的安全性。

此外，在上述传送系统中，可信赖的组织可以是IP，换言之，管理单元可以包括IP服务器单元。

此外，在上述传送系统中，API是用于限制Java-AP的使用的对象，但是任何资源都可以是所述对象。所述资源可以是硬件资源。此外，所述资源可以是网络资源，或软件资源。硬件资源可以是移动单元可以配备的资源，例如存储器、扬声器、麦克风、红外线控制器、LED(发光二极管)，或者可以是能够与移动单元一起运行的外部硬件体，例如UIM(用户身份模块）或SIM（用户身份模块）。

接下来，解释网络资源。如上所述，移动单元执行与移动通信网的无线通信。在无线通信期间，移动单元使用无线电资源，例如移动通信

网提供的无线电信道。无线电资源是网络资源之一。而且，在比无线电资源所属的通信协议层更高的通信协议层中，移动单元使用例如分组的传送路径或连接网络的通信路径的通信资源。诸如这些的通信资源都被包括进来作为网络资源。

接下来，解释软件资源。软件资源可以是API、类、程序包等等。软件资源提供各种各样的函数，但是典型的函数可以是例如加密计算的计算过程，或与其他的应用程序（如Web浏览器）进行数据的传送或接收的函数。此外，本发明的技术范围包括限制使用上述外部硬件体所配备的软件资源的模式。

顺便提及，通常发生Java-AP通过使用软件资源而使用硬件资源或网络资源的情况。上述传送系统的移动单元也配备有软件资源以使用硬件资源或网络资源，并且通过限制此类型软件资源的使用，来间接地限制硬件资源或网络资源的使用。通过以此方式间接地进行限制，并且通过准备各种各样的软件资源，可以轻易地规定多个限制，其中如果对多个资源的限制在细节方面没有改变，该多个限制就不能实现，所述多个限制例如可以包括：给予唯一可信的Java-AP改变Java-AP授权的权利，提高对仅仅与允许为下载而访问的服务器单元进行通信的限制，或者允许访问特殊的存储区。此外，通过限制使用安装在移动单元中的软件资源来间接地限制使用上述外部硬件体的软件资源的模式包括在本发明的技术范围中。

对于表示许可的方法，可以使用对应于一个资源的标志（允许/禁止），或可以由一个表达式来表示多个资源的许可。

此外，在本发明中，许可可以表示为允许(或禁止)使用多个类型的资源。在该情况下，在移动单元中，可以实现更精确的控制。例如，由于存储器中存在双模式(读出和写入)，所以尽管不可信Java-AP仅仅使用存储器进行读出，但可信Java-AP能够使用存储器用于读出和写入。此外，例如，当激活Web浏览器等，而同时在其中多个应用程序可以共享一个分组传送路径的移动单元中激活有权使用分组传送路径的Java-AP时，可以进行控制以使得被允许“专用分组传送路径”的Java-AP可以专用分组传

送路径，尽管不被允许“专用分组传送路径”的Java-AP不能拒绝Web浏览器等共享分组传送路径。此外，通过更进一步变更以上修改，下列控制可以成为可能。换句话说，具有某种许可的Java-AP可以不经用户同意就专用分组通信路径。此外，具有另一许可的Java-AP可以不经用户同意使用所述分组通信路径，但是需要获得用户的同意以专用该分组通信路径。此外，具有另一许可的Java-AP可以不经用户同意使用分组通信路径，但是不能专用该分组通信路径。另外，具有另一许可的Java-AP仅当具有用户许可时才可使用分组通信路径。此外，具有另一许可的Java-AP甚至不能使用分组通信路径。从这些例子中很明显得出，本发明的“使用类型”还包括使用资源时的过程（获得用户同意的过程或不获得用户同意的过程）的特定类型。

此外，在上述传送系统中，为所有的移动单元提供了相同的列表页，但是可以为每个移动单元提供不同的列表页。

此外，在上述传送系统中，当执行Java-AP时，Java-AP的操作是受限制的。作为替代，通过在存储在IP服务器单元中的Jar文件中包括策略信息，并且当在移动单元中下载Jar文件时，如果在所述策略信息与SDF中的策略信息之间的比较结果为不匹配，可以禁止对应于所述Jar文件的Java-AP的激活，或者包含所述Jar文件的Java-AP软件的安装。只有对策略信息中作为匹配的结果的项目所给予的许可才是有效的。

此外，可以在由CA给予通信供应商的秘密密钥对SDF签名之后来传送SDF，并且可以由CA给予通信供应商的公开密钥在移动单元中检查SDF上的签名。通信供应商的公开密钥必须必不可少地预存在移动单元中。在通过通信传送公开密钥之后，公开密钥可被预存在固定存储器中。此外，可以在把密钥写入ROM之后售出移动单元。

此外，在上述传送系统中，将软件传送给移动单元，但是本发明的技术范围包括将软件传送给除移动单元之外的终端单元的模式。

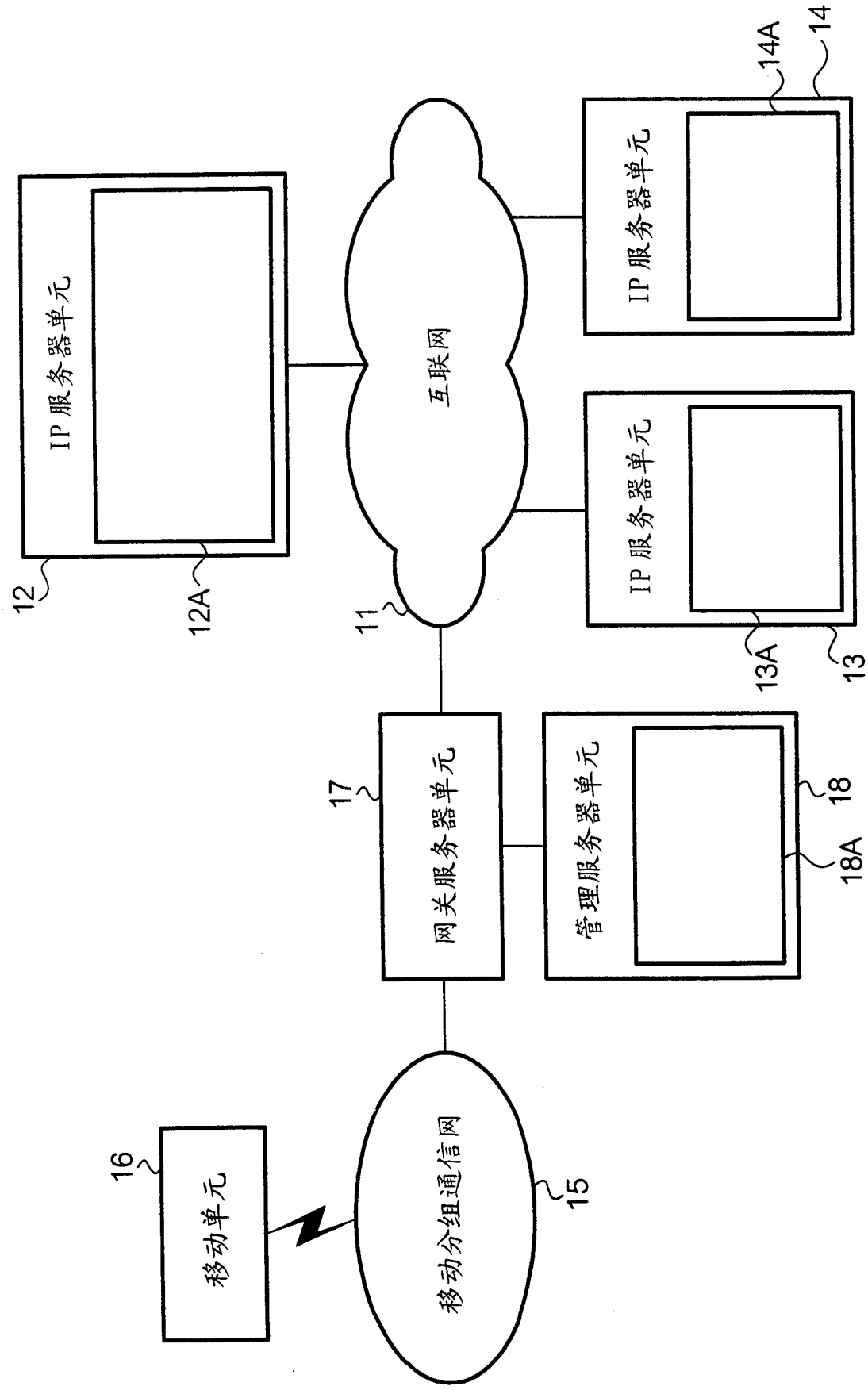

IP 服务器单元
12
12A
互联网
11
IP 服务器单元
14A
14
IP 服务器单元
13A
13
网关服务器单元
17
管理服务器单元
18
18A
移动单元
16
移动分组通信网
15

图 1

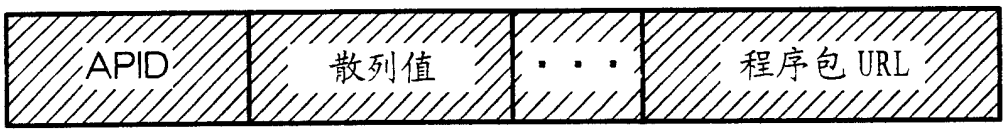

APID
散列值
· · ·
程序包 URL

图 2

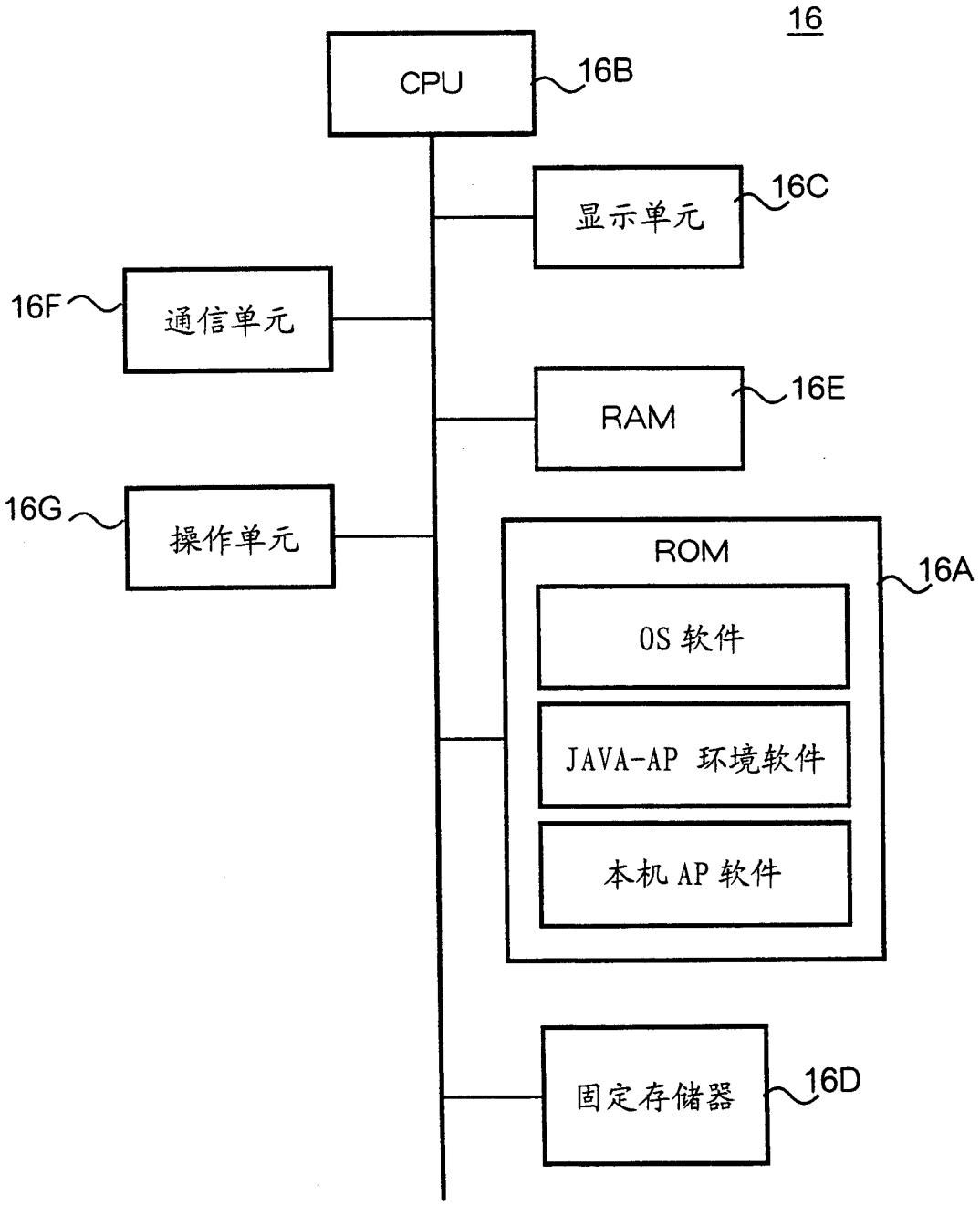

16
CPU
16B
显示单元
16C
16F
通信单元
RAM
16E
16G
操作单元
ROM
16A
OS 软件
JAVA-AP 环境软件
本机 AP 软件
固定存储器
16D

图 3

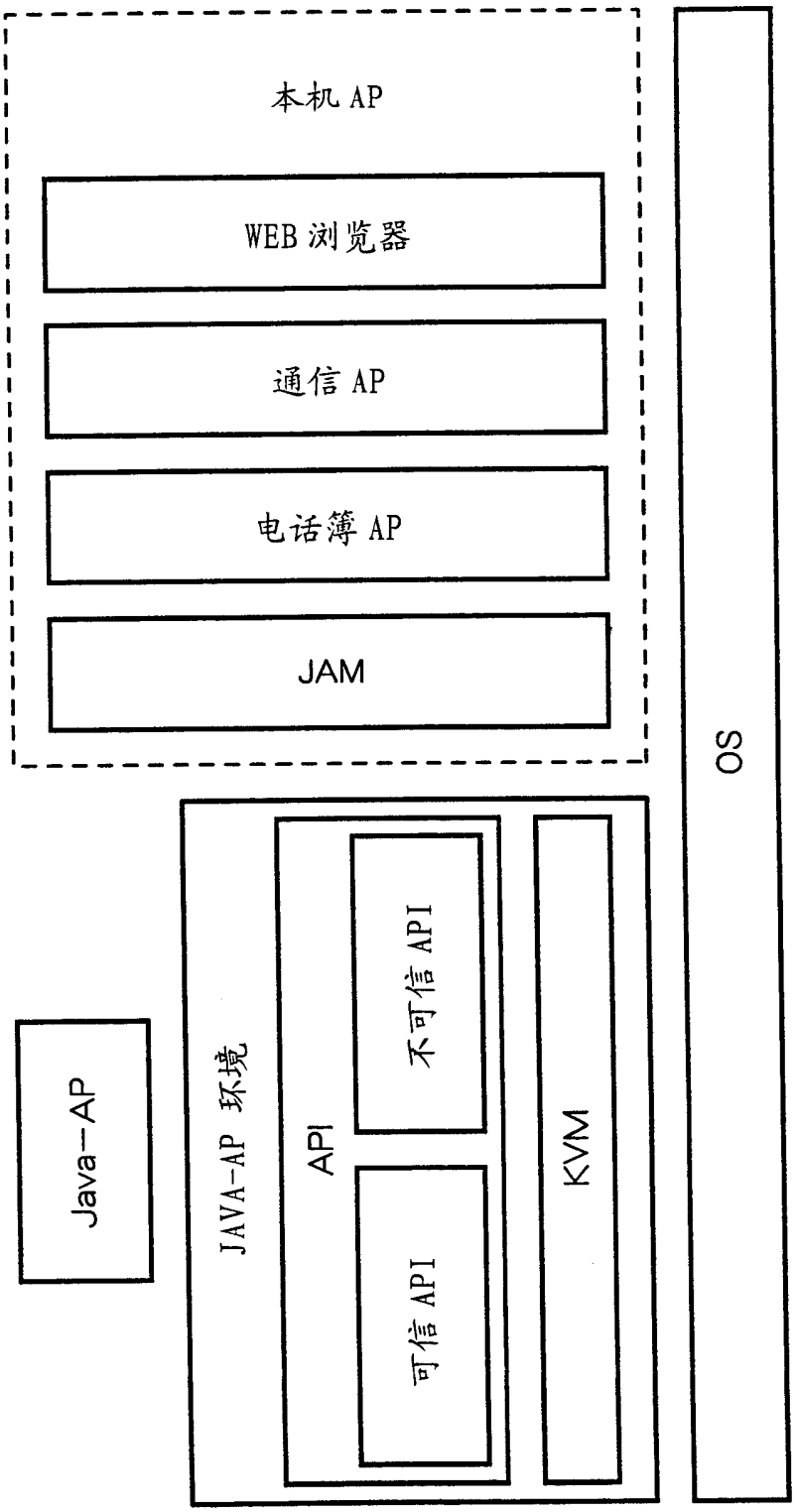

本机 AP
WEB 浏览器
通信 AP
电话簿 AP
JAM
OS
JAVA-AP 环境
API
不可信 API
可信 API
KVM
Java-AP

图 4

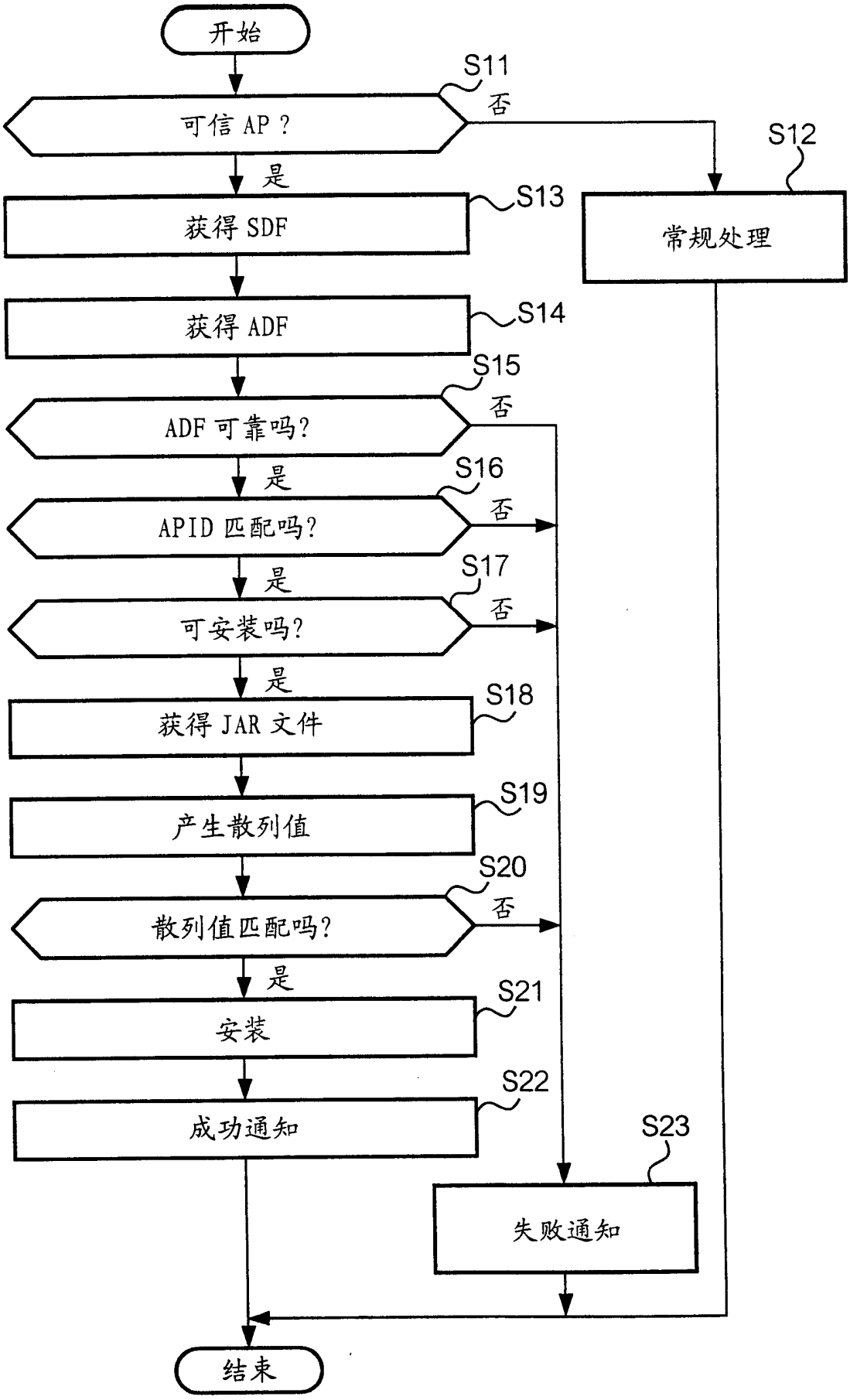

开始
S11
可信 AP ?
否
S12
是
常规处理
S13
获得 SDF
S14
获得 ADF
S15
ADF 可靠吗?
否
是
S16
APID 匹配吗?
否
是
S17
可安装吗?
否
是
S18
获得 JAR 文件
S19
产生散列值
S20
散列值匹配吗?
否
是
S21
安装
S22
成功通知
S23
失败通知
结束

图 5

APID	策略信息	ADF-URL	公开密钥

图 6

可信 API	许可
getPhoneList()	O
getCallHistory()	×
getMsStatus()	O

图 7

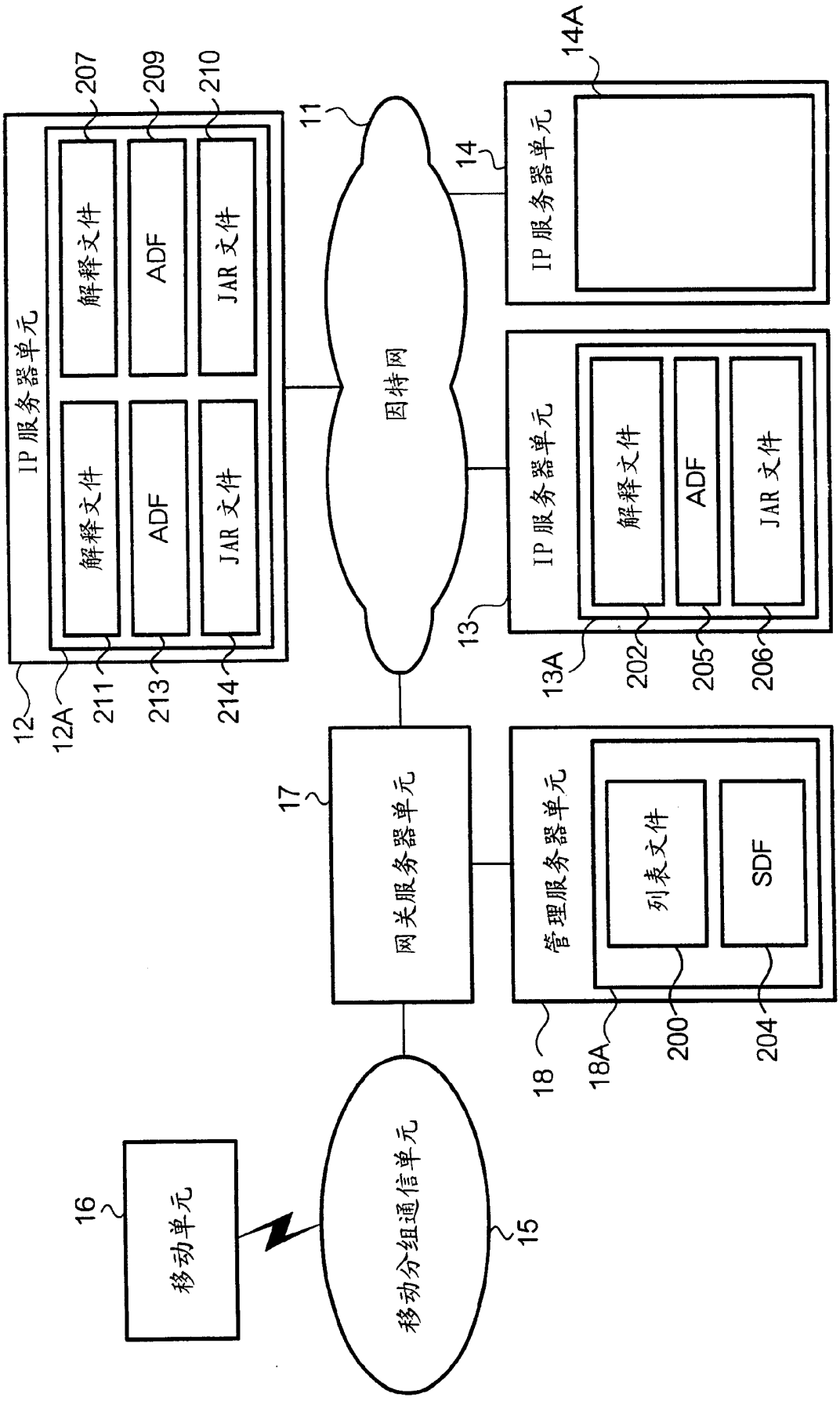

IP 服务器单元
解释文件
ADF
JAR 文件
因特网
IP 服务器单元
网关服务器单元
管理服务器单元
列表文件
SDF
移动分组通信单元
移动单元
11
12
12A
13
13A
14
14A
15
16
17
18
18A
200
202
204
205
206
207
209
210
211
213
214

图 8

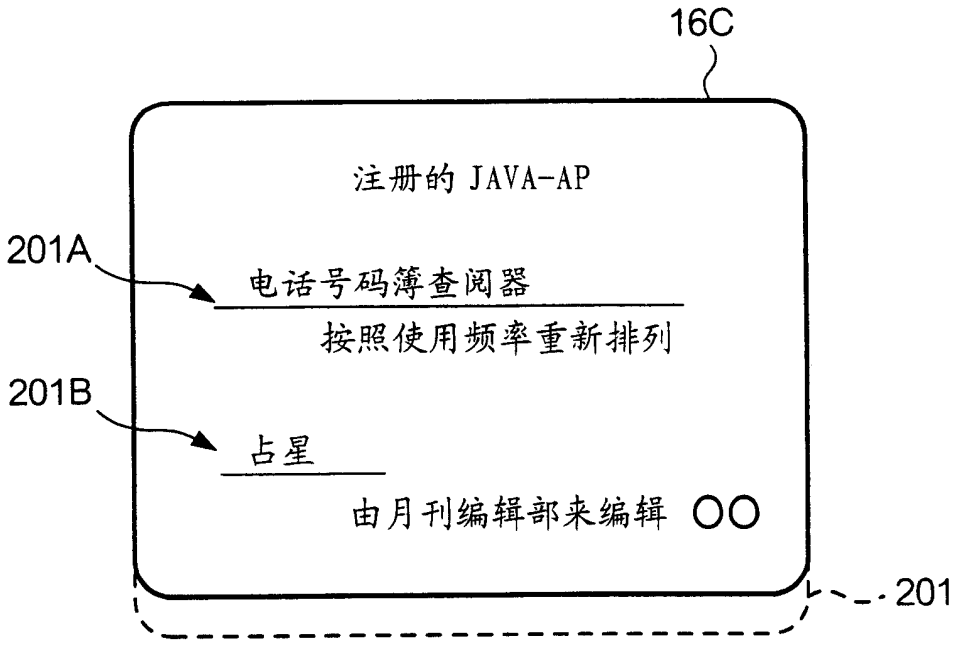


图 9

```
<OBJECT declare id="application.declaration"
data="http://www.ccc.co.jp/horoscope.jam>
TSUME-SHOGI
</OBJECT>
SOFTWARE FOR ～.CLICK
<A ijam="#application.declaration">HERE</A>
TO DOWNLOAD.
```

图 10

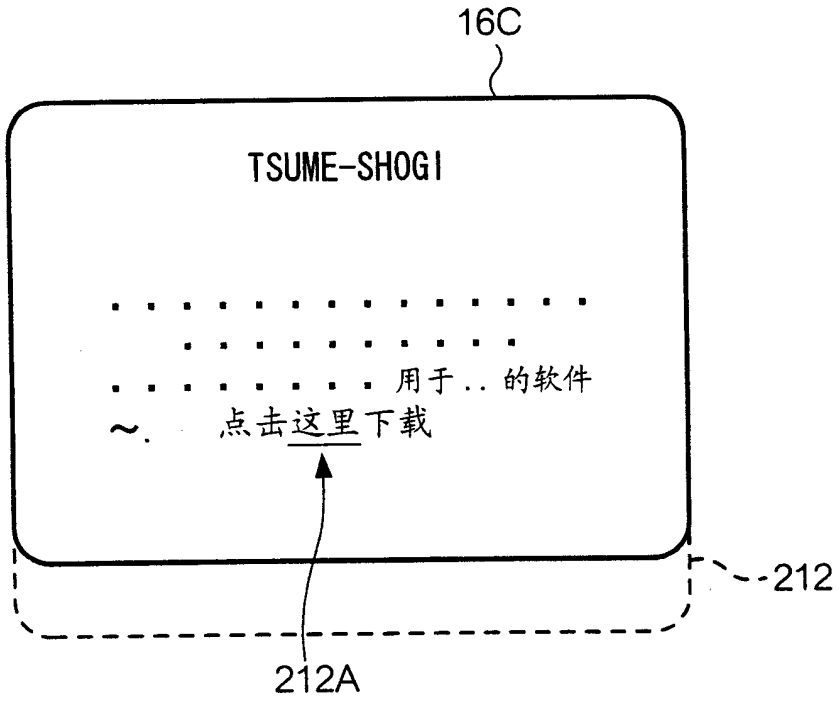


图 11

```
<OBJECT declare id="application.declaration"
data="http://www.ccc.co.jp/viewer.jam>
HOROSCOPE
</OBJECT>
SOFTWARE FOR ~. CLICK
<A ijam="#application.declaration">HERE</A>
TO DOWNLOAD.
```

图 12

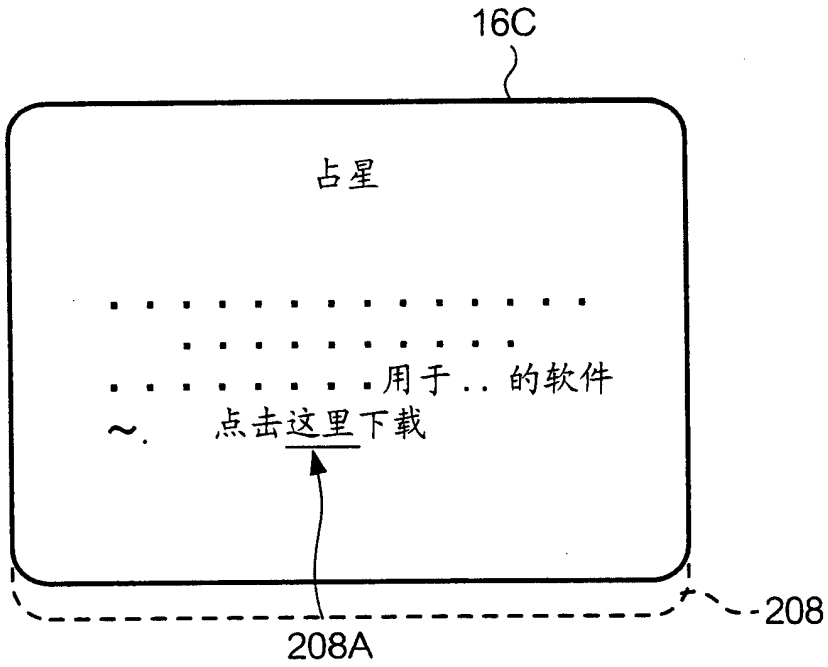


图 13

```
<OBJECT declare id="application.declaration"
data="http://www.aaa.co.jp/abc.sdf"
type="application/x-jam">
TELEPHONE DIRECTORY VIEWER
</OBJECT>
SOFTWARE FOR ~. CLICK
<A ijam="#application.declaration">HERE</A>
TO DOWNLOAD.
```

图 14

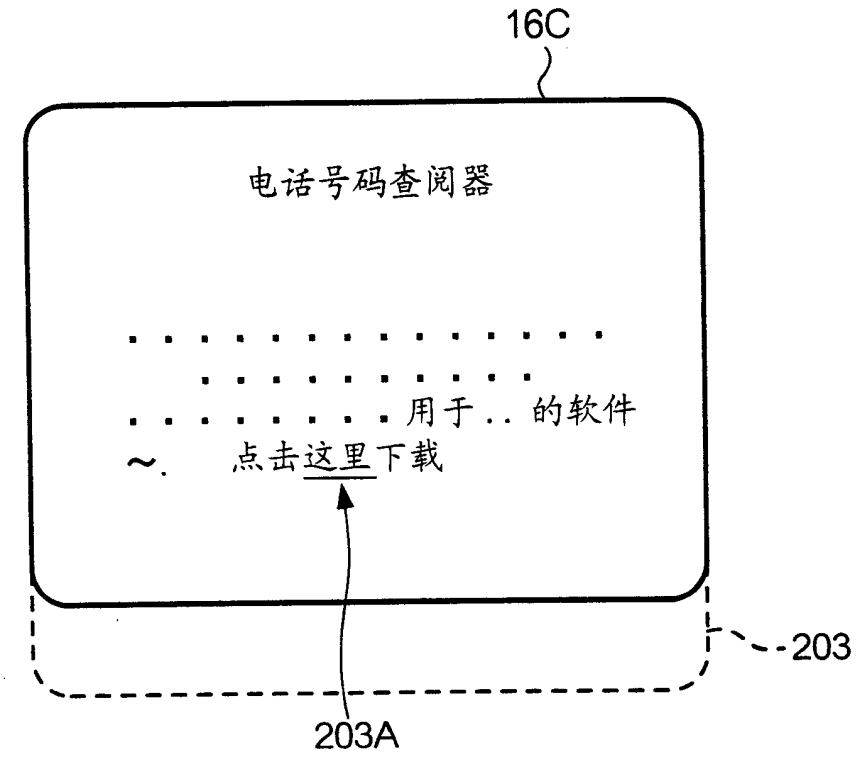


图 15

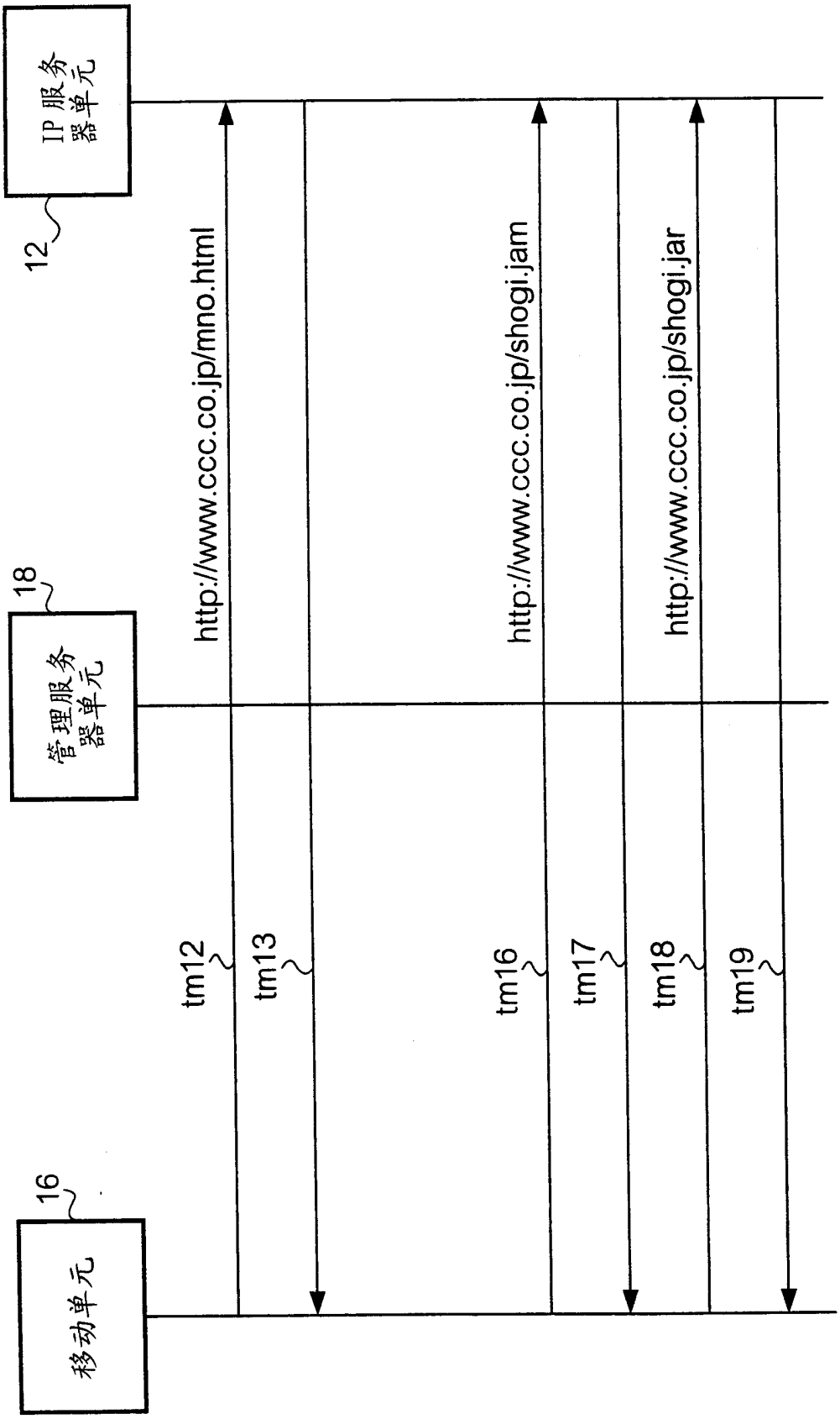

IP服务器单元
12
管理服务器单元
18
移动单元
16
http://www.ccc.co.jp/mno.html
http://www.ccc.co.jp/shogi.jam
http://www.ccc.co.jp/shogi.jar
tm12
tm13
tm16
tm17
tm18
tm19

图 16

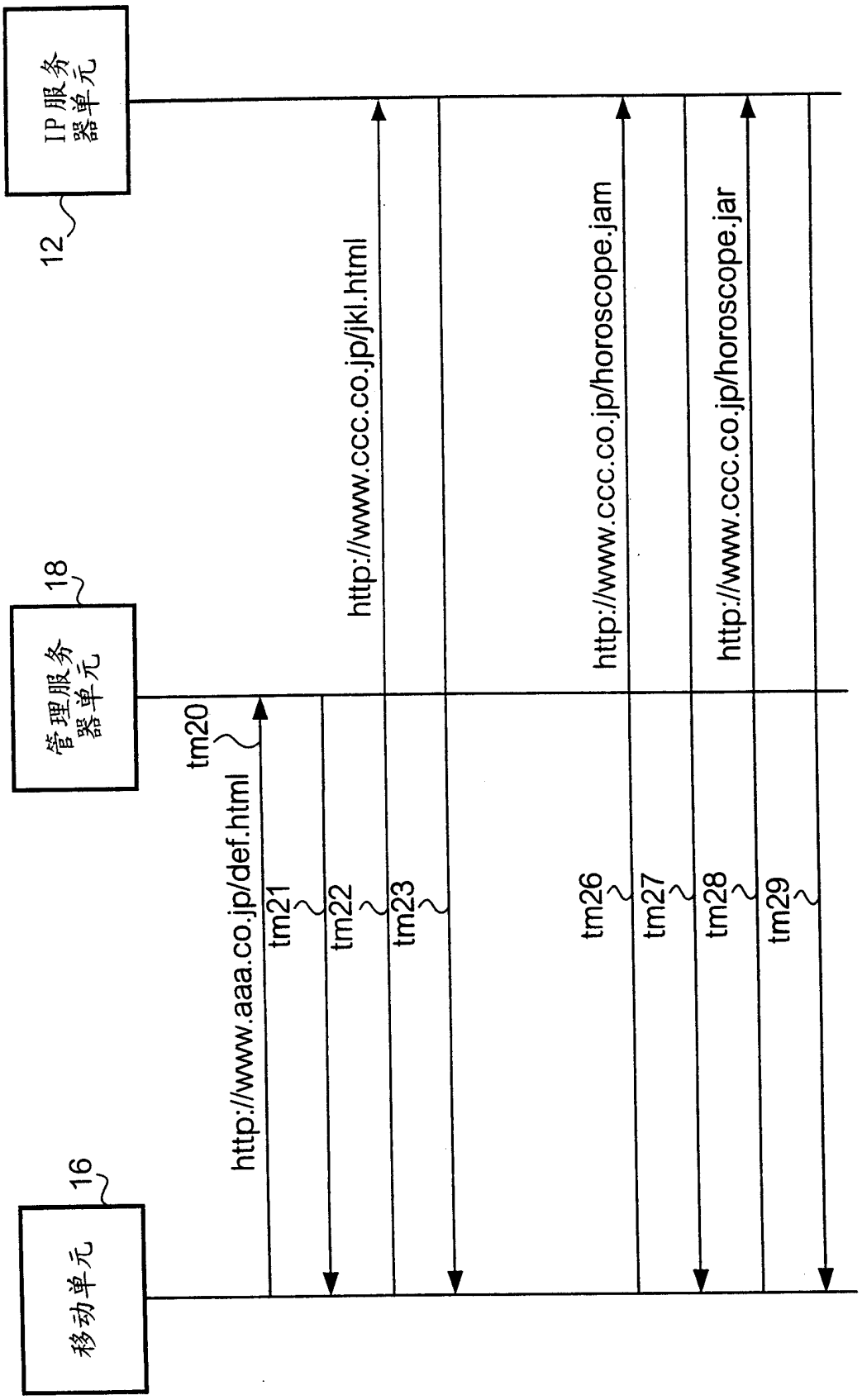

移动单元
16
管理服务器单元
18
IP服务器单元
12
http://www.aaa.co.jp/def.html
tm20
tm21
tm22
tm23
http://www.ccc.co.jp/jkl.html
tm26
tm27
tm28
tm29
http://www.ccc.co.jp/horoscope.jam
http://www.ccc.co.jp/horoscope.jar

图 17

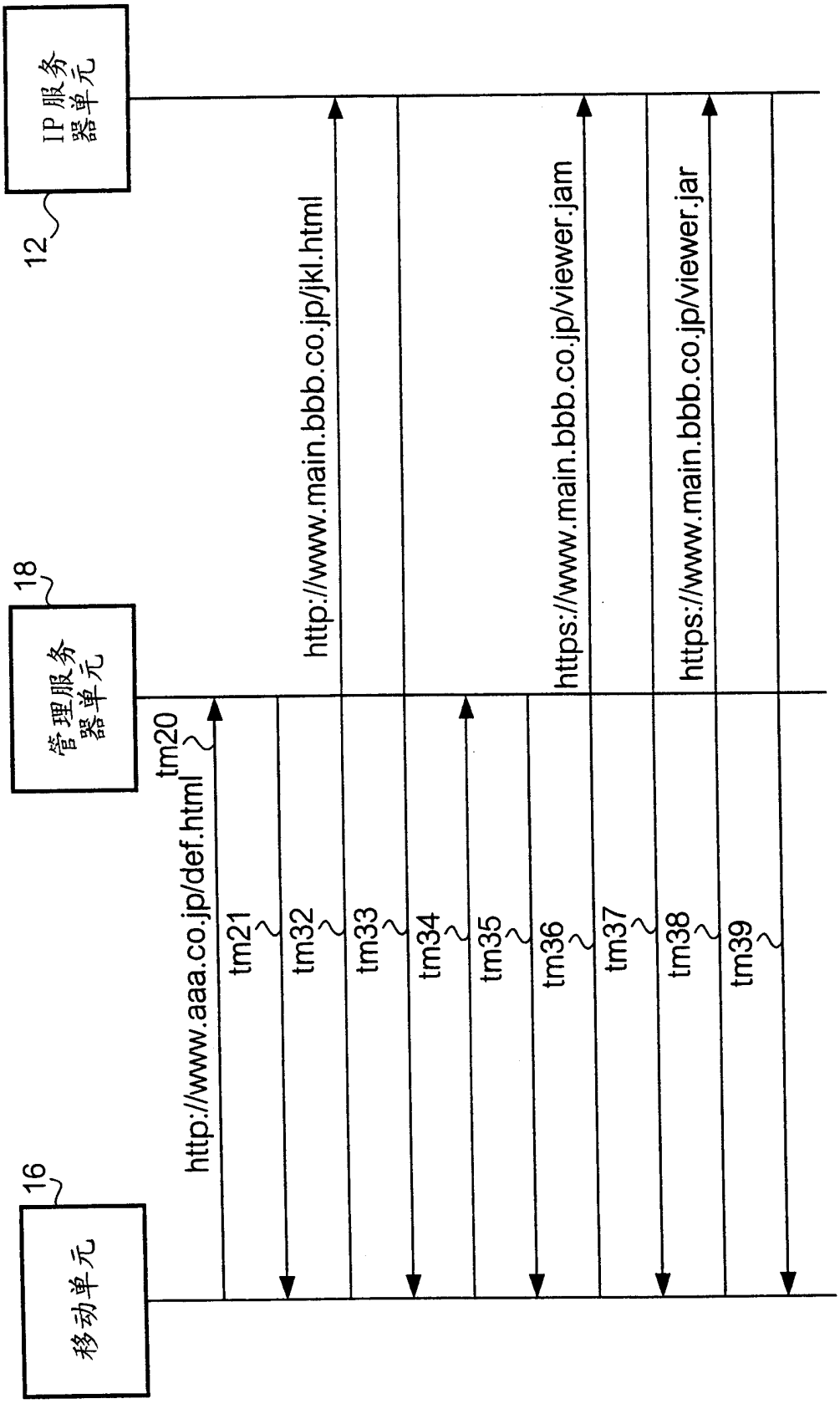

移动单元
16
管理服务器单元
18
IP服务器单元
12
http://www.aaa.co.jp/def.html
tm20
http://www.main.bbb.co.jp/jkl.html
https://www.main.bbb.co.jp/viewer.jam
https://www.main.bbb.co.jp/viewer.jar
tm21
tm32
tm33
tm34
tm35
tm36
tm37
tm38
tm39

图 18

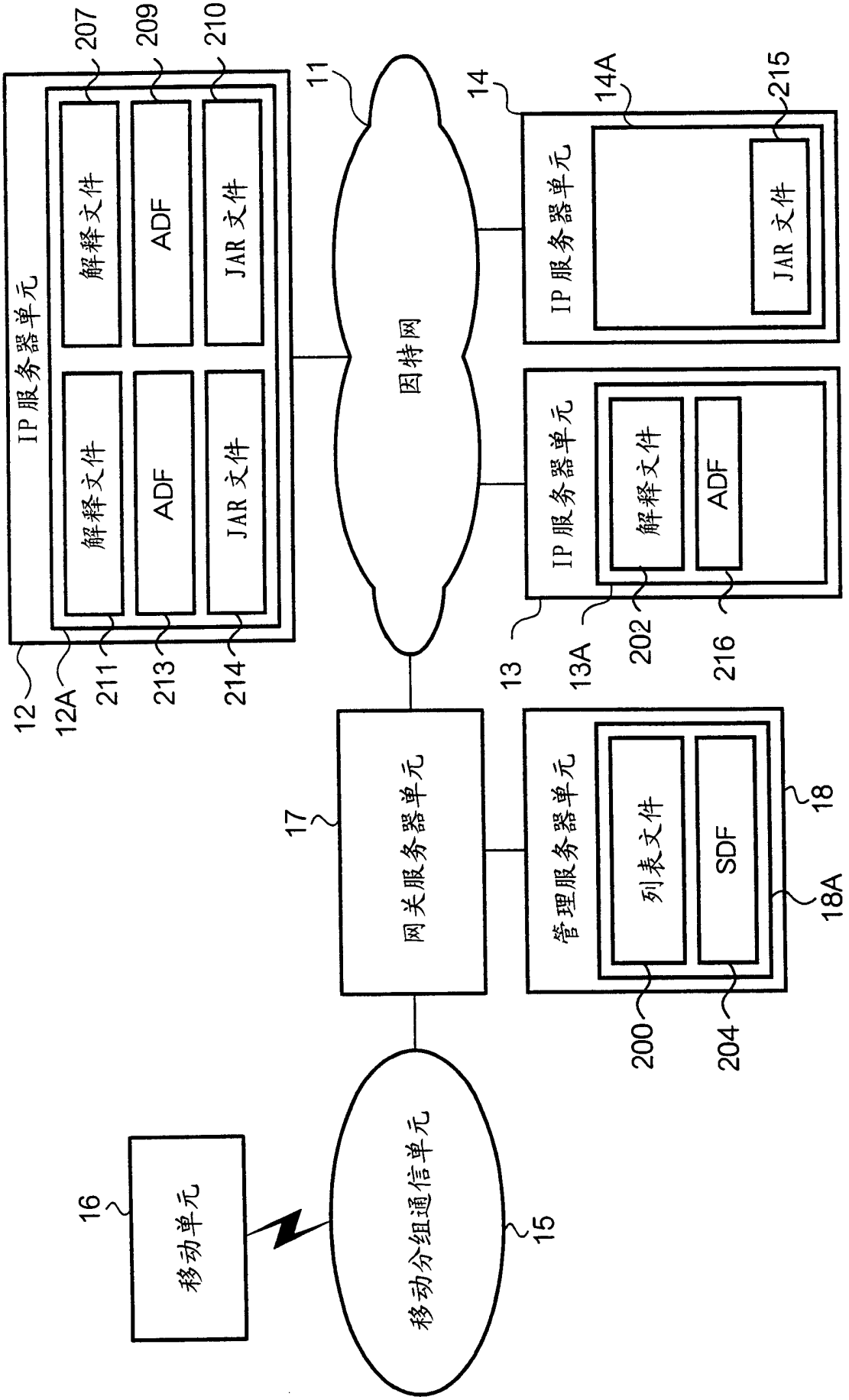

IP 服务器单元
解释文件
ADF
JAR 文件
因特网
IP 服务器单元
JAR 文件
IP 服务器单元
解释文件
ADF
网关服务器单元
管理服务器单元
列表文件
SDF
移动分组通信单元
移动单元
12
12A
211
213
214
207
209
210
11
14
14A
215
13
13A
202
216
17
18
18A
200
204
15
16

图 19

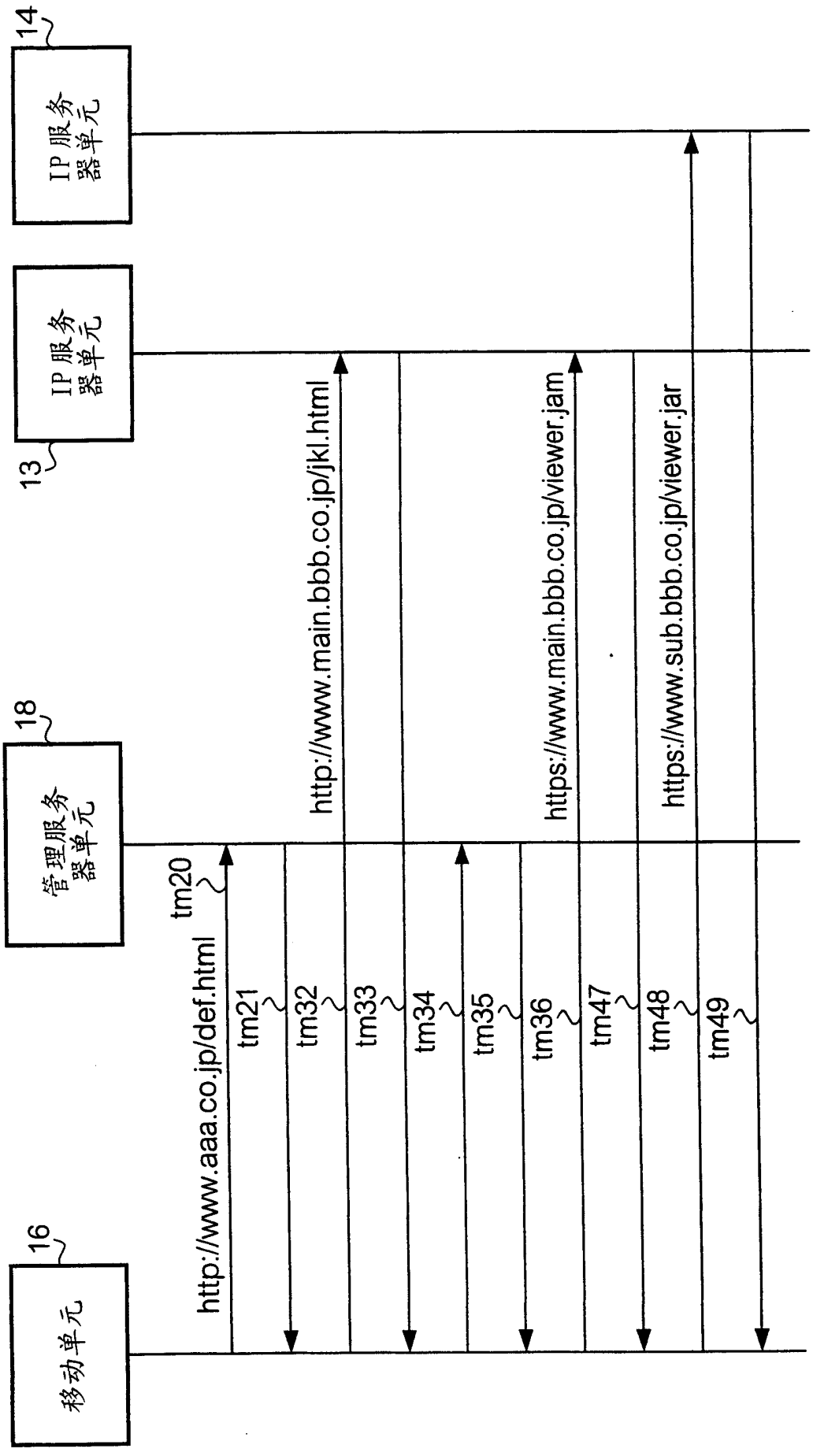

移动单元
16
管理服务器单元
18
IP服务器单元
13
IP服务器单元
14
http://www.aaa.co.jp/def.html
tm20
tm21
tm32
http://www.main.bbb.co.jp/jkl.html
tm33
tm34
tm35
https://www.main.bbb.co.jp/viewer.jam
tm36
tm47
tm48
https://www.sub.bbb.co.jp/viewer.jar
tm49

图 20