

[19] 中华人民共和国国家知识产权局

[51] Int. Cl⁷

G06F 9/06

G06F 13/00 G06F 9/445

G06F 17/60 H04L 9/10



[12] 发明专利申请公开说明书

[21] 申请号 02802387.0

[43] 公开日 2003 年 12 月 31 日

[11] 公开号 CN 1465006A

[22] 申请日 2002.5.14 [21] 申请号 02802387.0

[30] 优先权

[32] 2001.5.14 [33] JP [31] 143810/2001

[86] 国际申请 PCT/JP02/04643 2002.5.14

[87] 国际公布 WO02/093361 日 2002.11.21

[85] 进入国家阶段日期 2003.3.14

[71] 申请人 株式会社 NTT 都科摩

地址 日本东京都

[72] 发明人 夏野刚 山本正明 鹭尾谕

川端博史

[74] 专利代理机构 中国专利代理(香港)有限公司

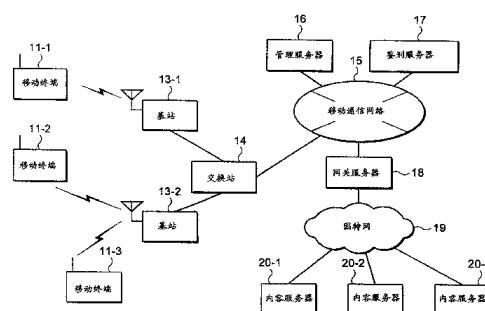
代理人 王 岳 王忠忠

权利要求书 8 页 说明书 56 页 附图 41 页

[54] 发明名称 用于管理存储在移动终端存储块中的程序的系统

[57] 摘要

管理服务器 16 通过响应移动终端 11 的请求获得来自内容服务器 20 的应用程序，并把获得的应用程序与有关应用程序可靠性的信息一起发送给移动终端 11。在移动终端 11 接收到来自管理服务器 16 的应用程序之后，通过使用有关应用程序可靠性的信息，移动终端 11 管理与其它程序的操作相协调的应用程序的操作。根据上述的多个应用程序的协调操作的管理，可以避免有关信息安全的问题，在这些问题当中，重要的信息会由于低可靠性的应用程序的操作而被泄露出去。由此，在不破坏移动终端 11 的信息安全的情况下，可以提高移动终端 11 的用户方便性。



1. 一种管理程序的方法，所述方法包括：

移动终端的程序获得步骤，获得可由所述移动终端执行的程序并把所述程序存储到所述移动终端的存储器中；

5 所述移动终端的协调信息获得步骤，通过所述程序以及与所述另一程序的数据通信，获得用于管理不是所述程序的另一程序的至少开始之一的协调信息，并把所述协调信息存储到所述移动终端的存储器中，以及；

10 所述移动终端的操作管理步骤，在存储于所述存储器中的所述程序正在执行操作时请求所述另一程序执行操作的情况下，根据响应所述程序的所述协调信息确定至少所述另一程序的开始和与所述另一程序的数据通信之一的条件。

2. 根据权利要求1的管理程序的方法，其中：

15 在所述协调信息获得步骤，所述移动终端通过通信网络从用于管理所述协调信息的管理服务器获得所述协调信息。

3. 根据权利要求1的管理程序的方法，其中：

在所述程序获得步骤，所述移动终端通过通信网络从发送程序的发送服务器获得所述程序。

4. 根据权利要求1的管理程序的方法，其中所述方法还包括：

20 通过通信网络能够与所述移动终端通信的验证服务器的验证准备步骤，准备用于验证至少所述程序和所述协调信息之一的正确性的验证信息，以及；

所述移动终端的验证信息获得步骤，通过所述通信网络获得来自所述验证服务器的所述验证信息；其中

25 所述移动终端根据所述验证信息允许或禁止所述移动终端中的所述程序的操作。

5. 根据权利要求4的管理程序的方法，其中：

所述验证信息通过使用密钥加密至少所述程序和所述协调信息之一来准备，并且；

30 在能够解密已被加密的至少所述程序和所述协调信息之一的情况下，所述移动终端允许所述程序的所述操作。

6. 根据权利要求5的管理程序的方法，其中：

所述密钥是在公共密钥系统中的密钥。

7. 根据权利要求4的管理程序的方法，其中：

所述验证信息是对至少所述程序和所述协调信息之一进行摘要的摘要信息，并且；

5 根据由所述移动终端产生的至少所述程序和所述协调信息之一的信息摘要与所述验证信息之间的验证结果，所述移动终端允许所述程序的所述操作。

8. 根据权利要求2的管理程序的方法，其中所述方法还包括：

10 所述管理服务器的存储数据准备步骤，准备有关所述移动终端中所述程序的存储状态的存储数据；

所述管理服务器的管理数据准备步骤，准备用于根据所述存储数据管理所述移动终端中的所述程序的管理数据，以及；

所述移动终端的管理数据获得步骤，从所述管理服务器获得所述管理数据；其中，

15 所述移动终端根据所述管理数据管理所述移动终端中的所述程序。

9. 根据权利要求8的管理程序的方法，其中

所述移动终端根据所述管理数据允许或禁止所述移动终端中的所述程序的操作。

20 10. 根据权利要求9的管理程序的方法，其中

在所述移动终端允许所述程序的所述操作的情况下，所述移动终端使用至少字母、图像、声音和振动之一来通知允许所述程序的所述操作。

11. 根据权利要求8的管理程序的方法，其中

25 所述移动终端根据所述管理数据删除所述移动终端中的所述程序。

12. 根据权利要求8的管理程序的方法，其中

所述通信网络包括服务费征收服务器，用于管理所述程序的服务费帐户；并且

30 所述方法还包括所述服务费征收服务器的服务费数据获得步骤，用于获得管理数据的至少一部分以作为服务费数据；其中，

所述服务费征收服务器根据所述服务费数据管理所述程序的所述

服务费帐户。

13. 根据权利要求2的管理程序的方法，其中所述方法还包括：
所述管理服务器的请求获得步骤，用于获得准备发送程序的准备请求，以及；

5 所述管理服务器的发送准备步骤，通过响应所述准备请求而准备发送所述程序至所述移动终端；其中，

在所述程序获得步骤，所述移动终端获得在所述发送准备步骤准备的所述程序。

14. 根据权利要求13的管理程序的方法，其中：

10 在所述发送准备步骤，所述管理服务器准备所述程序和位置信息中的至少之一，其中所述位置信息表示所述程序的存储位置。

15. 根据权利要求13的管理程序的方法，其中所述方法还包括：
所述管理服务器的完成通知发送步骤，当所述发送准备步骤完成时，向所述移动终端发送通知所述程序的准备发送完成的完成通知，

15 以及

所述移动终端的完成通知接收步骤，接收所述管理服务器的所述完成通知；其中，

当所述移动终端接收到所述完成通知时，所述移动终端使用字母、图像、声音和振动中的至少之一来通知所述程序准备发送。

20 16. 根据权利要求13的管理程序的方法，其中：

所述通信网络包括服务费征收服务器，用于管理所述程序的服务费帐户；

25 所述管理服务器的准备数据准备步骤，用于准备发送准备数据，该数据表示通过响应所述准备请求，向所述移动终端发送所述程序的准备已经完成，并且；

所述服务费征收服务器的服务费数据获得步骤获得所述发送准备数据的至少一部分作为服务费数据；其中，

所述服务费征收服务器根据所述服务费数据管理所述程序的所述服务费帐户。

30 17. 一种程序管理系统，所述系统包括：

一个通信网络，该通信网络包括传送服务器、管理服务器和移动终端；其中，

所述传送服务器包括用于存储程序的程序存储单元和用于把所述程序发送给所述移动终端的程序发送单元;

所述管理服务器包括协调信息存储单元和协调信息发送单元, 其中所述协调信息存储单元存储有关所述程序和不是所述程序的另一程序的协调操作控制的信息, 而所述协调信息发送单元用于把所述协调信息发送至所述移动终端, 并且;

所述移动终端包括: 程序接收单元, 用于接收来自所述传送服务器的所述程序; 协调信息接收单元, 用于接收来自所述管理服务器的所述协调信息; 程序存储单元, 用于存储所述程序; 协调信息存储单元, 用于存储所述协调信息; 以及操作管理单元, 在所述程序正在执行操作时请求所述另一程序执行操作的情况下, 根据响应所述程序的所述协调信息确定至少所述另一程序的开始和与所述另一程序的数据通信之一的条件。

18. 一种包含移动终端的通信网络的服务器, 所述服务器包括:

用于存储协调信息的协调信息存储单元, 在不是所述程序的另一程序正在执行操作时请求所述程序执行操作的情况下, 所述协调信息用于确定至少所述程序的开始以及与所述程序的数据通信之一的条件, 以及

协调信息发送单元, 用于向所述移动终端发送所述协调信息。

19. 根据权利要求 18 的服务器, 其中所述服务器还包括

准备验证信息的验证准备单元, 所述验证信息用于验证至少所述程序和所述协调信息之一的正确性, 以及;

验证发送单元, 向所述移动终端发送所述验证信息。

20. 根据权利要求 19 的服务器, 其中,

所述验证准备单元包括加密至少所述程序和所述协调信息之一的加密单元。

21. 根据权利要求 20 的服务器, 其中,

所述加密单元包括密钥存储单元, 用于存储公共密钥系统中的密钥。

22. 根据权利要求 19 的服务器, 其中

所述验证准备单元包括信息摘要准备单元, 用于准备对至少所述程序和所述协调信息之一进行摘要的摘要信息。

23. 根据权利要求 18 的服务器, 其中所述服务器还包括:

存储数据准备单元, 准备有关所述移动终端中所述程序的存储状态的存储数据;

管理数据准备单元, 准备用于根据所述存储数据管理所述移动终端中的所述程序的管理数据, 以及;

管理数据发送单元, 向所述移动终端发送所述管理数据。

24. 根据权利要求 23 的服务器, 其中所述服务器还包括:

服务费数据发送单元, 把作为服务费数据的至少所述管理数据的一部分发送到用于管理包含在所述通信网络中的服务费帐户的服务费征收服务器。

25. 根据权利要求 18 的服务器, 其中所述服务器还包括:

接收准备请求的请求接收单元, 所述请求用于请求所述程序发送单元准备发送所述程序, 以及;

发送准备单元, 通过响应所述准备请求准备向所述移动终端发送所述程序。

26. 根据权利要求 25 的服务器, 其中

所述发送准备单元包括准备信息存储单元, 用于存储至少所述程序和位置信息之一, 其中所述位置信息表示所述程序的存储位置。

27. 根据权利要求 25 的服务器, 其中所述服务器还包括:

完成通知发送单元, 当所述程序发送的准备完成时, 向所述移动终端发送通知所述程序的发送准备完成的完成通知。

28. 根据权利要求 25 的服务器, 其中所述服务器还包括:

准备数据准备单元, 用于准备发送准备数据, 该数据表示通过响应所述准备请求, 向所述移动终端发送所述程序的准备已经完成, 以及;

服务费数据发送单元, 把作为服务费数据的至少所述发送准备数据的一部分发送到用于管理包含在所述通信网络中的服务费帐户的服务费征收服务器。

29. 一种移动终端包括:

用于存储程序的程序存储单元;

协调信息存储单元, 用于存储与所述程序和不是所述程序的另一程序的协调操作控制有关的协调信息, 以及;

操作管理单元, 在所述程序正在执行操作时请求所述另一程序执行操作的情况下, 根据所述协调信息确定至少所述另一程序的开始和与所述另一程序的数据通信之一的条件。

30. 一种包含在通信网络中的移动终端, 所述通信网络包括传送程序的传送服务器和管理程序的管理服务器, 所述移动终端包括:

程序接收单元, 用于接收来自所述传送服务器的程序;

程序存储单元, 用于存储所述程序;

协调信息接收单元, 从所述管理服务器接收与所述程序与不是所述程序的另一程序的协调操作控制有关的协调信息;

10 协调信息存储单元, 用于存储所述协调信息; 以及

操作管理单元, 在所述程序正在执行操作时请求所述另一程序执行操作的情况下, 根据所述协调信息确定至少所述另一程序的开始和与所述另一程序的数据通信之一的条件。

31. 根据权利要求 30 的移动终端, 其中所述移动终端还包括:

15 用于从所述管理服务器接收验证信息的验证接收单元, 所述验证信息用于验证至少所述程序和所述协调信息之一的正确性, 以及;

操作允许单元, 根据所述验证信息允许或禁止所述程序的操作。

32. 根据权利要求 31 的移动终端, 其中

20 所述操作允许单元包括解密单元, 用于在至少所述程序和所述协调信息之一被加密的情况下解密至少所述程序和所述协调信息之一。

33. 根据权利要求 32 的移动终端, 其中

所述解密单元包括公共密钥存储单元, 用于在公共密钥系统中存储所述管理服务器的公共密钥。

34. 根据权利要求 31 的移动终端, 其中

25 所述操作允许单元包括信息摘要准备单元, 用于准备对至少所述程序和所述协调信息之一进行摘要的摘要信息。

35. 根据权利要求 30 的移动终端, 其中所述移动终端还包括:

管理数据接收单元, 用于从所述管理服务器接收管理所述程序的管理数据, 以及;

30 管理单元, 用于根据所述管理数据管理所述程序。

36. 根据权利要求 35 的移动终端, 其中所述移动终端还包括:

通知单元, 当所述管理单元允许所述程序的所述操作时, 所述单

元使用字母、图像、声音和振动中的至少之一来通知允许所述程序的所述操作。

37. 根据权利要求 30 的移动终端，其中所述移动终端还包括：

5 请示发送单元，用于向所述管理服务器发送准备发送所述程序的准备请求。

38. 根据权利要求 37 的移动终端，其中所述移动终端还包括：

完成通知接收单元，用于从所述管理服务器接收通过响应所述准备请求来通知发送准备完成的完成通知，以及；

10 通知单元，当接收到所述完成通知时，该通知单元使用字母、图像、声音和振动中的至少之一来通知所述程序准备发送。

39. 一种程序，所述程序允许用于管理包含有移动终端的通信网络中的程序的管理服务器的计算机执行如下操作：

15 把协调信息发送给所述移动终端，其中在不是所述程序的另一程序正在执行操作时请求所述程序执行操作的情况下，所述协调信息用于确定至少所述程序的开始以及与所述程序的数据通信之一的条件。

40. 根据权利要求 39 的程序，所述程序还允许所述管理服务器的所述计算机执行如下操作：

准备用于验证在所述移动终端中执行的至少一个程序的正确性的验证信息以及所述协调信息，并且；

20 发送所述验证。

41. 一种程序，所述程序允许移动终端的计算机执行如下操作：

获得有关程序协调操作控制的协调信息，以及；

25 在不是所述程序的另一程序正在执行操作时请求所述程序执行操作的情况下，确定至少所述程序的开始以及与所述程序的数据通信之一的条件。

42. 根据权利要求 41 的程序，所述程序还允许所述移动终端的所述计算机执行如下操作：

获得用于验证至少所述程序、所述另一程序和所述协调信息之一的正确性的验证信息，以及；

30 根据所述验证信息决定允许或禁止至少所述程序和所述另一程序之一的操作。

43. 一种记录介质，所述介质上包括一个程序，所述程序允许用

于管理包含有移动终端的通信网络中的程序的管理服务器的计算机执行如下操作：

把用在所述移动终端中的协调信息发送给所述移动终端，其中在不是所述程序的另一程序正在执行操作时请求所述程序执行操作的情况下，所述协调信息用于确定至少所述程序的开始以及与所述程序的数据通信之一的条件。

44. 一种记录介质，所述介质上包含如权利要求 43 所述的程序，所述程序还允许所述管理服务器的所述计算机执行如下操作：

准备用于验证在所述移动终端中执行的至少一个程序的正确性的验证信息以及所述协调信息，并且；
发送所述验证。

45. 一种记录介质，所述介质上包括一个程序，所述程序允许移动终端的计算机执行如下操作：

获得有关程序协调操作控制的协调信息，以及；
在不是所述程序的另一程序正在执行操作时请求所述程序执行操作的情况下，确定至少所述程序的开始以及与所述程序的数据通信之一的条件。

46. 一种记录介质，所述介质上包含如权利要求 45 所述的程序，所述程序还允许所述移动终端的所述计算机执行如下操作：

获得用于验证至少所述程序、所述另一程序和所述协调信息之一的正确性的验证信息，以及；

根据所述验证信息决定允许或禁止至少所述程序和所述另一程序之一的操作。

用于管理存储在移动终端存储块中的程序的系统

技术领域

- 5 本发明涉及一种用于管理在安装或连接到移动终端的存储单元中存储的程序（包括小应用程序）的系统。

背景技术

- 近年来，已经开发出了下述类型的移动终端，即它们具有较大存储能力的非易失存储器以用于存储在其用户购买移动终端时并未被存储的应用程序，并能执行这些应用程序。

上述移动终端的用户可把不必要的应用程序从非易失存储器中删除并把其它应用程序写入非易失存储器中。因此，移动终端的用户并不需要用新移动终端来替换旧移动终端就可以使用新的应用程序。

- 在上述的可把应用程序写入存储器的那些移动终端中，安装了
15 Java 虚拟机。安装了 Java 虚拟机的移动终端可通过移动通信网络下载 Java 应用程序（包括 Java applets）；把下载的 Java 应用程序写入它们的非易失存储器中；并执行这些程序。（包括 applets（小应用程序）的应用程序在下文中被称作“应用程序”）。

- 在上述移动终端的用户希望以一系列操作存取几个应用程序时，
20 使用上述移动终端并不方便。

- 下面是一个例子，它描述了已有技术的上述缺陷，在其中，移动终端的用户需要存取用于申请通过邮购来购买商品的应用程序 A 和进行付款的应用程序 B。在本例中，用户首先使用应用程序 A 申请购买某种商品。在这个阶段，用户还没有对所购商品付款，因而用户需要获取付款所需的必要信息，即汇款额、接受汇款的银行名称、进行汇款的银行帐户细目等，所有这些均被写在一张纸上，随后终止应用程序 A。接着，用户存取应用程序 B 以便汇款结帐。通过使用应用程序 B，用户可以把所需的钱数从用户的某个银行帐户汇寄到任意指定的银行帐户中。用户把付款额，银行名称、汇款的银行帐户细目等输入至执行应用程序 B 的移动终端中，同时始终参考在前面步骤中写在一张纸上的信息。随后，用户终止应用程序 B，并再次启动应用程序 A，以确
30 认汇款成功且购买商品的所有步骤均已完成。用户输入一个命令以使

执行应用程序 A 的移动终端显示表示商品购买历史的屏幕，而且，用户确认所购商品的汇款已得到销售商的确认，同时，用户得到一些其它的信息，如交货日期等。

- 5 正如上述传统技术的例子所描述的，当移动终端的用户需要使用一系列操作执行几个应用程序时，用户需要改变应用程序并人工输入必要的信息。操作因此而费时，而且用户会感到操作很烦人，并且可能会在输入信息时出错，这会在进行交易时出现问题。

本发明的公开

- 10 为了克服上述已有技术的不便之处，本申请的发明人阐述了如下的想法：在移动终端的非易失存储器中预先存储几个应用程序，使它们能够执行协调操作。但是，如果一个应用程序的功能或数据被没有限制的用于另一个应用程序，那将不能保证信息的安全。

- 15 例如，一个移动终端存储了管理移动终端用户的时间表的应用程序 C 和接发电子邮件的应用程序 D。应用程序 C 管理有关移动终端用户的时间表的信息，这些信息用户是希望保密的。但是，在用户使用应用程序 D 发送电子邮件给他/她的朋友时，如果允许应用程序 D 无限制地使用应用程序 C 的功能或数据，则会存在以下的风险，即与应用程序 C 管理的时间表有关的信息可被发送给他/她的朋友。即使是应用程序 D 中微小的操作错误或者程序错误都可能使本来要保密的信息被发送出去。因而，对于移动终端用户来说，当使用应用程序时，信息的安全得不到保证。

- 25 特别是当移动终端处理有价值的信息如个人信息和财政信息时，上述信息泄露、信息破坏以及未经许可的改写信息等都属于严重的问题。作为一种克服上述问题的方法，本申请的发明人提出了一种想法，即为了保证通信安全，首先应当保证应用程序的可靠性；为此，与每个应用程序的可靠性有关的信息要预先准备，并且彼此相关的每个应用程序的操作根据与它们的可靠性有关的信息进行管理。换言之，经过充分评估之后被判断具有高可靠性并且已知在处理重要信息时不会产生问题的应用程序可被允许使用被判断为可靠性低的应用程序的功能和数据。另一方面，不允许可靠性低的应用程序使用可靠性高的应用程序的功能和数据。因而可以防止由于低可靠性应用程序的处理而
- 30

引起的高可靠性应用程序的数据的意外泄露或破坏。

具体来说，本发明提供一种管理程序的方法，该方法包括：移动终端的程序获得步骤，获得可由该移动终端执行的程序并把该程序存储到移动终端的存储器中；移动终端的协调信息获得步骤，通过该程序以及5 与另一程序的数据通信，获得用于管理不是该程序的另一程序的至少一个开始的协调信息，并把协调信息存储到移动终端的存储器中，以及；移动终端的操作管理步骤，在存储于存储器中的该程序正在执行操作时请求另一程序执行操作的情况下，根据响应该程序的协调信息确定至少另一程序的开始以及与另一程序的数据通信之一的条件。10

本发明还提供一种程序管理系统，该系统包括：通信网络，它包括传送服务器、管理服务器和移动终端；其中，该传送服务器包括用于存储程序的程序存储单元和用于把程序发送给移动终端的程序发送单元；该管理服务器包括协调信息存储单元和协调信息发送单元，其中15 该协调信息存储单元用于存储有关该程序和不是该程序的另一程序的协调操作控制的信息，该协调信息发送单元用于把协调信息发送至移动终端，并且；该移动终端包括：程序接收单元，用于接收来自传送服务器的程序；协调信息接收单元，用于接收来自管理服务器的协调信息；程序存储单元，用于存储程序；协调信息存储单元，用于存储20 协调信息；以及操作管理单元，在该程序正在执行操作时请求另一程序执行操作的情况下，根据响应该程序的协调信息确定至少另一程序的开始以及与另一程序的数据通信之一的条件。

本发明还提供包含移动终端的通信网络的服务器，该服务器包括：用于存储协调信息的协调信息存储单元，在不是该程序的另一程序正在执行操作时请求该程序执行操作的情况下，该协调信息用于确定25 至少该程序的开始以及与该程序的数据通信之一的条件；该服务器还包括用于向移动终端发送协调信息的协调信息发送单元。

本发明还提供一种移动终端，它包括：用于存储一个程序的程序存储单元；协调信息存储单元，用于存储与该程序和不是该程序的另一程序的协调操作控制有关的协调信息；以及操作管理单元，在该程序正在执行操作时请求另一程序执行操作的情况下，根据协调信息确定30 至少另一程序的开始以及与另一程序的数据通信之一的条件。

本发明还提供一程序和包含该程序的记录介质，该程序允许用于管理包含有移动终端的通信网络中的程序的管理服务器的计算机执行如下操作：把协调信息发送给移动终端，在不是该程序的另一程序正在执行操作时请求该程序执行操作的情况下，该协调信息用于确定至少该程序的开始以及与该程序的数据通信之一的条件。

本发明还提供一程序和包含该程序的记录介质，该程序允许移动终端的计算机：获得与程序的协调操作控制有关的协调信息，并且；在不是该程序的另一程序正在执行操作时请求该程序执行操作的情况下，确定至少该程序的开始以及与该程序的数据通信之一的条件。

根据上述的程序管理方法、程序管理系统、服务器、移动终端、程序和记录介质，在一个移动终端中执行的多个程序的操作可根据基于每个程序的可靠性的协调信息来协调，因而可以防止在根据多个程序执行协调操作时由于信息泄露而破坏信息安全。

附图简述

图 1 表示根据本发明第一和第二实施例的应用程序传送系统的总配置的框图；

图 2 表示根据本发明第一和第二实施例的移动终端的外部图；

图 3 表示根据本发明第一和第二实施例的移动终端的概要的框图；

图 4 表示根据本发明第一和第二实施例的移动终端的存储器数据部分的示意图；

图 5 表示根据本发明第一和第二实施例的管理服务器配置概要的框图；

图 6 表示根据本发明第一和第二实施例的应用程序信息管理系统配置示意图；

图 7 表示由根据本发明第一和第二实施例的用户信息存储单元存储的数据实例的格式图；

图 8 表示在根据本发明第一实施例的应用程序信息存储单元的寄存应用程序区中存储的数据实例的格式图；

图 9 表示在根据本发明第一和第二实施例的应用程序信息存储单元的临时保管应用程序区中存储的数据实例的格式图；

图 10 和图 11 表示根据本发明第一和第二实施例的管理服务器执

行的应用程序存储操作的流程图；

图 12 和图 13 表示根据本发明第一和第二实施例在购买由管理服务器公布的应用程序时显示在移动终端上的屏幕图；

图 14 和图 15 表示根据本发明第一和第二实施例由管理服务器公布的应用程序的购买操作的流程图；

图 16 和图 17 表示根据本发明第一和第二实施例被判断为具有一定可靠性但不是由管理服务器公布的应用程序的购买操作的流程图；

图 18、图 19 和图 20 表示根据本发明第一和第二实施例未给定任何可靠性的应用程序的购买操作的流程图；

图 21 和图 22 表示当根据本发明第一和第二实施例下载应用程序时显示在移动终端上的屏幕图；

图 23、图 24 和图 25 表示根据本发明第一和第二实施例的应用程序下载操作的流程图；

图 26 表示当根据本发明第一和第二实施例执行应用程序启动操作时显示在移动终端上的屏幕图；

图 27、图 28、图 29、图 30 和图 31 表示根据本发明第一实施例在多个应用程序不执行协调操作的情况下显示在移动终端上的屏幕图；

图 32、图 33 和图 34 表示根据本发明第一实施例在多个应用程序执行协调操作的情况下显示在移动终端上的屏幕图；

图 35 表示根据本发明第二实施例的应用程序之间的特许信息实例的格式图；

图 36 表示根据本发明第二实施例的应用程序信息存储单元的寄存应用程序区中存储的数据实例的格式图；

图 37 表示根据本发明第三实施例的应用程序信息存储单元的寄存应用程序区中存储的数据实例的格式图；

图 38 表示根据本发明第三实施例的应用程序信息管理系统的配置图；

图 39 表示根据本发明第三实施例由用户信息存储单元存储的数据实例的格式图；

图 40、图 41 和图 42 表示根据本发明第三实施例的应用程序购买操作和应用程序下载操作的流程图。

实施本发明的最佳模式

下面的段落将解释本发明的优选实施例。

[1] 第一实施例

5 [1.1] 配置

[1.1.1] 应用程序传送系统的总配置

图 1 表示在本发明实施例中的应用程序传送系统的总配置概要的框图。

该应用程序传送系统包括：多个移动终端，即移动终端 11-1、
10 11-2...；多个基站，即基站 13-1、13-2...；多个交换站 14；移动通信网络 15；管理服务器 16；鉴别服务器 17；网关服务器 18、因特网 19 和多个内容服务器，即内容服务器 20-1、20-2...。在下文中，如果不需要将它们与其它同类型的设备进行区分时，每个移动终端均被称作
15 ‘移动终端 11’，每个基站均被称作‘基站 13’，每个内容服务器均被称作‘内容服务器 20’。

移动终端 11 是一种具有无线通信功能的信息处理装置，如移动电话和个人手持电话系统（PHS；注册商标）。移动终端 11 具有可存储应用程序的内置非易失存储器或外部非易失存储器。移动终端 11 通过
20 移动通信网络 15、交换站 14 和基站 13 从管理服务器 16 下载应用程序，并且将下载的应用程序写入其非易失存储器中。移动终端 11 的用户可在用户选择的任何时刻执行已写入移动终端 11 的非易失存储器中的应用程序。

基站 13 通过交换站 14 经通信电缆与移动通信网络 15 连接。当位于分配给基站 13 的无线电区中的移动终端 11 呼叫移动通信网络 15
25 时，或者当移动通信网络 15 呼叫移动终端 11 时，基站 13 建立与移动终端 11 的无线连接，并转播移动终端 11 和移动通信网络 15 之间的通信。通过控制信号频繁地与每个移动终端 11 进行无线电通信，基站 13 始终跟踪每个移动终端 11 在指定无线电区域中的存在，并把移动终端 11 存在的信息作为移动终端 11 的位置信息发送给移动通信网络 15。

30 交换站 14 通过通信电缆与基站 13 和移动通信网络 15 连接，并建立已经与基站 13 建立的无线连接的移动终端 11 与移动通信网络 15 之间的通信信道。而且，当已经与移动通信网络 15 建立通信连接的移动

终端 11 从交换站 14 之一管理的一个无线电区移动到同另一个交换站 14 管理的另一个无线电区时, 交换站 14 执行在交换站之间的通信连接的交换操作, 以保持所建立的通信连接。

移动通信网络 15 是一种包括交换站 14 的通信网络, 其中交换站 14 通过网关交换站 (未示出) 以通信电缆相互连接。移动通信网络 15 通过交换站 14 和基站 13 建立移动终端之间的通信信道。移动通信网络 15 还与其它通信网络 (未示出) 连接, 如固定电话网。而且, 移动通信网络 15 通过网关服务器 18 与因特网 19 连接。移动通信网络 15 配备有位置寄存存储单元 (未示出), 并且该位置寄存存储单元存储由每个基站 13 发送的移动终端 11 的位置信息。当移动通信网络 15 呼叫移动终端 11 时, 移动通信网络 15 把连接请求发送到基站 13, 这样, 通过参考由位置寄存存储单元存储的信息可建立与移动终端 11 的无线连接。

管理服务器 16 是一种通过响应来自移动终端 11 的请求把应用程序发送给移动终端 11 的服务器。管理服务器 16 接收来自作为应用程序提供者的内容服务器 20 的应用程序, 并在应用程序被发送到移动终端 11 之前把接收的应用程序存储到数据库中。

管理服务器 16 的管理实体检查内容服务器 20 提供的应用程序, 如果内容服务器 20 的管理实体请求管理服务器 16 的管理实体这样做的话; 并且管理服务器 16 的管理实体从在移动终端 11 中它们的操作安全性的角度来确定应用程序的可靠性指数。所确定的可靠性指数被记录到管理服务器 16 的数据库中。当管理服务器 16 接收到来自移动终端 11 的发送具有可靠性指数的应用程序的请求时, 管理服务器 16 将把可靠性指数与该应用程序一起发送给移动终端 11。

如果移动终端 11 使用一个应用程序, 则需要购买并下载该应用程序到移动终端 11 中并启动, 也就是说使其成为可用状态 (启动应用程序的操作在下文中被称作 '启动操作')。当管理服务器 16 接收到来自移动终端 11 的购买应用程序的请求时, 管理服务器 16 准备发送请求的应用程序。当该应用程序下载到移动终端 11 中时, 管理服务器 16 在移动终端 11 的存储器中指定一个用于存储该应用程序的区域, 并允许移动终端 11 把该应用程序存储到该区域中。而且, 管理服务器 16 命令移动终端 11 执行该应用程序的启动操作。当管理服务器 16 完成

发送应用程序的准备或者应用程序的启动操作时，管理服务器 16 把有关这些操作的信息发送到与移动通信网络 15 连接的收费管理服务器（未示出）。在收费管理服务器接收到来自管理服务器 16 的有关准备工作或者启动操作完成的信息时，收费管理服务器根据该信息计算移动终端 11 的该应用程序的使用费用。

鉴别服务器 17 是一种管理公共密钥系统中的移动终端 11、管理服务器 16、内容服务器 20 和鉴别服务器 17 的公共密钥的服务器。当鉴别服务器 17 接收来自移动终端 11、管理服务器或者内容服务器 20 中任意之一的公共密钥的请求时，鉴别服务器 17 发送所请求的公共密钥至请求该密钥的装置。

内容服务器 20 存储根据移动终端 11 的技术规格开发的一个或几个应用程序，并通过响应管理服务器 16 的应用程序的请求把应用程序发送至管理服务器 16。内容服务器 20 的管理实体可把应用程序发送给管理服务器 16 的管理实体以在必要的时候执行应用程序内容的检查，并通过管理服务器 16 的管理实体根据检查结果获得应用程序的可靠性指数。

[1.1.2] 移动终端的配置

下面以移动终端 11-1 作为移动终端 11 的一个例子来描述移动终端 11 的配置。

图 2 是移动终端 11-1 的外部图，而图 3 表示移动终端 11-1 的配置概要的框图。如图 3 所示，移动终端 11-1 包括显示单元 21、操作单元 22、天线 34A、控制单元 31、控制存储器 32、通信单元 34、存储控制器 35、存储器 12 和声音输入输出单元 36。

显示单元 21 是一个移动终端 11-1 的控制单元通过其可以向移动终端 11-1 的用户显示信息的元件。如图 2 所示，显示单元 21 显示执行应用程序的操作菜单屏幕，以及用于其它操作的菜单屏幕和用于显示从信息站点接收的信息的浏览屏幕，以及各种信息，如无线电波的强度和电话号码。

操作单元 22 是一个向控制单元 31 提供指令的元件。操作单元 22 配备有操作按钮和 appli 按钮 23，在操作按钮上还印有诸如数字这样的符号。appli 按钮 23 是一种指定简化应用程序操作的功能的操作按钮。

天线 34A 是在移动终端 11-1 执行无线通信时物理输出和输入无线电波的元件。

控制单元 31 是一个微处理器，它控制除了存储器 12 之外的移动终端 11-1 的其它所有元件。控制单元 31 根据存储在控制存储器 32 中的控制程序控制每个元件。而且，控制单元 31 通过存储控制器 35 从存储器 12 读出应用程序，并执行这些应用程序。控制单元 31 通过响应正在执行的一个控制程序或者一个应用程序的请求可使用存储在存储器 12 中的应用程序的功能或数据。在这种情况下，控制单元 31 把允许使用作出该请求的控制程序或应用程序的功能或数据以及标识信息的请求发送到存储控制器 35。存储控制器 35 使用标识信息判断是否接受该请求。控制单元 31 可在同一时间执行几个控制程序或应用程序，但控制单元 31 不允许任何数据在控制程序和应用程序之间直接传送，所有的数据均通过存储控制器 35 传送。

控制存储器 32 是一种易失存储器或非易失存储器，在其中存储了控制单元 31 的控制程序和控制程序管理的数据。控制存储器 32 还被用作控制单元 31 的工作区，以执行控制程序。控制程序包括实现移动终端 11-1 的基本功能的几个程序，如存储电话号码，这些程序在移动终端 11-1 出售时已安装。

通信单元 34 是一个通过天线 34A 利用无线电波发送和接收来自基站 13 的信号的元件。当移动终端 11-1 需要向基站 13 发送任何信息时，通信单元 34 使用在控制单元 31 的控制下发送的包括数字数据的信号调制基带信号，并通过向天线 34A 施加与调制的信号对应的电压而把无线电波信号发送给基站 13。另一方面，当通信单元 34 通过天线 34A 接收来自基站 13 的无线电波信号时，通信单元 34 解调接收的无线电波信号以检索包含在无线电波信号中的应用程序或数据。如果检索的数据是应用程序，则通信单元 34 把它们发送给存储控制器 35。如果检索的数据是数字声音数据，则通信单元 34 把它们发送给声音输入输出单元 36。否则，通信单元 34 把检索的数据发送给控制单元 31。

当移动终端 11-1 的用户与其它移动终端 11 或者固定电话等的任意一个用户交谈时，声音输入和输出单元 36 输入和输出声音数据。声音输入和输出单元 36 包括话筒（未示出）、A/D 转换器（未示出）、D/A 转换器（未示出）和扬声器（未示出）。当移动终端 11-1 的用户

交谈时,声音输入和输出单元 36 通过话筒接收作为模拟信号的移动终端 11-1 的用户的语音信息,并通过 A/D 转换器把接收的模拟信号转换为数字声音数据,并把该数据发送给通信单元 34。另一方面,当移动终端 11-1 的用户的交谈对象谈话时,声音输入和输出单元 36 通过 D/A 5 转换器把通信单元 34 提供的数字声音数据转换为模拟信号,并通过使用模拟信号由扬声器发声。

存储控制器 35 是一个微处理器,它控制存储器 12 和控制单元 31 之间以及存储器 12 和通信单元 34 之间的数据发送和接收。当通信单元 34 发送一个应用程序时,存储控制器 35 把该应用程序写入存储器 10 12 中。对于通信单元 34 发送的应用程序来说,由管理服务器 16 作出的允许把该程序写入存储器 12 的请求和表示该应用程序应当写入存储器 12 中的存储区的数据是关联的。存储控制器 35 把应用程序写入由该关联数据表示的存储区中。如果存储控制器 35 从通信单元 34 接收的应用程序给定了一个高于某个级别的可靠性指数,则存储控制器 35 15 接收该可靠性指数及应用程序。在这种情况下,存储控制器把接收的可靠性指数存储到写入该应用程序的同一个存储区中。

当存储控制器 35 接收到来自控制单元 31 的允许使用写入存储器 12 的应用程序的功能或数据的请求时,也就是接收到允许读、允许写以及允许删除一个应用程序的功能或数据的请求时,存储控制器 35 判断 20 是否接受该请求,并根据判断结果对存储器 12 执行适当的操作。由控制单元 31 作出的允许使用写入存储器 12 中的应用程序的功能或数据的请求包括请求获得允许的该程序的标识信息。当存储控制器 35 接收允许请求时,存储控制器 35 检查请求获得允许的该程序的可靠性指数。如果请求获得允许的该程序是一个管理控制单元 31 的控制程序, 25 则存储控制器 35 无条件接受该请求,并根据该请求执行对存储器 12 的操作,这是因为控制程序给定的是最高级别的可靠性指数。另一方面,如果请求获得允许的程序是从存储器 12 读出的应用程序,则存储控制器 35 根据标识信息规定该应用程序存储到存储器 12 中的存储区域,并读出给定该应用程序的可靠性指数。如果并未得到该应用程序 30 的可靠性指数,则存储控制器 35 把该应用程序看作是最低级别的可靠性指数的应用程序。随后,存储控制器 35 还从写入了请求使用的应用程序或应用程序的数据的存储区中读出可靠性指数。存储控制器

35 比较如上所述获得的可靠性指数，并且只有在作出请求的应用程序的可靠性指数等于或大于请求其功能或数据的应用程序的可靠性指数时，存储控制器 35 才会接受该请求，并在随后根据该请求对存储器 12 执行必要的操作。根据上述使用可靠性指数的允许方法的操作将在本说明书随后部分中使用具体的例子进行解释。

而且，存储控制器 35 产生移动终端 11-1 的专用密钥和公共密钥，并通过使用该专用密钥和公共密钥加密和解密数据。在控制单元 31 的控制下，存储控制器 35 根据移动终端 11 的用户输入的关键字产生一对专用密钥和公共密钥。存储控制器 35 通过通信单元 34 把公共密钥发送给鉴别服务器 17，同时，在其采取措施保护专用密钥不会从移动终端 11 泄露之后保存专用密钥。如果存储控制器 35 通过通信单元 34 从外部信号源接收使用移动终端 11-1 的公共密钥加密的数据时，移动终端 11-1 使用专用密钥解密加密的数据。当存储控制器 35 通过通信单元 34 把来自存储器 12 的数据发送给外部实体时，存储控制器 35 在必要时使用移动终端 11-1 的专用密钥加密数据。

存储器 12 是一个非易失存储器，它用于存储通过通信单元 34 从外部信号源接收的应用程序以及由这些应用程序管理的数据。图 4 表示存储器 12 的数据部分的示意图。

存储器 12 被分成多个存储区，这些区域分为管理区 40 或自由区 41。管理区 40 是由管理服务器 16 给定的高于某个级别的可靠性指数的应用程序的区域。自由区 41 是管理服务器 16 未给定高于某个级别的可靠性指数的应用程序的区域。管理区 40 由管理区 40-1, ..., 管理区 40-n (‘n’ 是一个任意的正整数) 组成，而自由区 41 是由自由区 41-1, ..., 自由区 41-m (‘m’ 是一个任意的正整数) 组成。在下面的描述中，管理区 40-1 和自由区 41-1 将分别作为管理区 40 和自由区 41 的例子。

管理区 40-1 被分成应用程序区 40A-1、数据区 40D-1 和可靠性信息区 40R-1。应用程序存储在应用程序区 40A-1 中。数据区 40D-1 中存储了由应用程序区 40A-1 中存储的应用程序所管理的数据。可靠性信息区 40R-1 中存储了给定应用程序区 40A-1 中存储的应用程序的可靠性指数。

自由区 41-1 被分成应用程序区 41A-1 和数据区 41D-1。应用程序

存储在应用程序区 41A-1 中。在数据区 41D-1 中存储了由应用程序区 41A-1 中存储的应用程序所管理的数据。

5 应用程序区 40A-1 和应用程序区 41A-1 中的应用程序的存储操作和删除操作以及可靠性信息区 40R-1 中的可靠性指数的存储操作和删除操作由存储控制器 35 根据管理服务器 16 提供的指令来执行。另一方面，应用程序区 40A-1 和应用程序区 41A-1 中的应用程序的读出操作、可靠性信息区 40R-1 中的可靠性指数的读出操作、数据区 40D-1 和数据区 41D-1 中的数据的写入操作、数据区 40D-1 和数据区 41D-1 中的数据的读出操作和数据区 40D-1 和数据区 41D-1 中的数据的删除
10 操作由存储控制器 35 通过响应控制单元 31 作出的请求来执行。

[1.1.3] 管理服务器的配置

图 5 表示管理服务器 16 的配置的示意框图。管理服务器 16 包括密钥存储单元 51、应用程序信息存储单元 52、用户信息存储单元 53 和控制单元 54。

15 密钥存储单元 51 是一个以数据库的形式存储由控制单元 54 产生的管理服务器 16 的专用密钥以及通过鉴别服务器 17 获得的每个移动终端 11 和每个内容服务器 20 的公共密钥的单元。

应用程序信息存储单元 52 是一个以数据库的形式把每个内容服务器 20 发送的应用程序以及与应用程序存储位置有关的信息与诸如应用程序名称这样的应用程序的其它信息一起进行存储的单元。
20

用户信息存储单元 53 是一个在数据库中存储信息的单元，该信息用以识别哪些应用程序被写入每个移动终端 11 的存储器 12 中以及哪些应用程序已由每个移动终端 11 的用户购买以通过响应用户的请求准备下载到存储器 12。

25 控制单元 54 是一个微处理器，它控制管理服务器 16 的每个元件。控制单元 54 控制下列操作：获得来自鉴别服务器 17 的公共密钥；获得来自内容服务器 20 的应用程序；解密被加密的应用程序；加密要被发送到移动终端 11 的应用程序；并把应用程序发送给移动终端 11。而且，通过控制单元 54 的控制操作，控制单元 54 更新密钥存储单元 51、
30 应用程序信息存储单元 52 和用户信息存储单元 53 的数据库中的数据。

管理服务器 16 的每个数据库的数据格式以及发送应用程序的操作

细节将在随后的部分中描述。

[1.1.4] 应用程序信息管理系统的配置

图 6 表示由移动终端 11、管理服务器 16 和内容服务器 20 实现的应用程序信息管理系统。

5 用户信息存储单元 53 由用户信息存储单元 53-1、用户信息存储单元 53-2, ..., 和用户信息存储单元 53-k 组成, 它们是分别对应于移动终端 11-1、移动终端 11-2, ..., 和移动终端 11-k (‘k’ 是表示移动终端 11 的数的整数) 的数据存储单元。用户信息存储单元 53-i (i=1, ..., k) 被分成下载应用程序区 53A-i 和准备下载应用程序区
10 53B-i。用户信息存储单元 53-i 的下载应用程序区 53A-i 是一个用于存储目前存储在移动终端 11-i 的存储器 12 的管理区 40 或自由区 41 中的应用程序的信息。另一方面, 用户信息存储单元 53-i 的准备下载应用程序区 53B-i 是一个用于存储未存储在移动终端 11-i 的存储器 12 中但已经由移动终端 11-i 的用户购买并准备在任意时间通过响应
15 移动终端 11 的请求传送给移动终端 11 的应用程序的信息。在下载应用程序区 53A 和准备下载应用程序区 53B 中存储了应用程序的信息, 如应用程序名、应用程序版本号、识别每个应用程序的标识号、应用程序的大小、启动操作完成和未完成的差异和应用程序存储号等。图 7 表示对应移动终端 11-1 的用户信息存储单元 53-I 所存储的数据实例
20 的格式图, 而且, 为了简化说明, 其仅仅示出了存储区、应用程序标识号、启动和存储号这几项。

根据图 7 所示的数据实例, 在移动终端 11-1 的管理区 40-1 和应用程序区 40A-1 中, 存储其标识号为 ‘AP-3568’ 的应用程序, 并且该应用程序的启动操作已经完成。存储号用于规定在应用程序信息存储
25 单元 52 的临时保管应用程序区中临时存储准备发送的应用程序的位置。已经发送到移动终端 11-1 的应用程序不需要存储号, 并且在下载应用程序区 53A 中并不给定该应用程序存储号。

根据图 7 所示的数据实例, 在移动终端 11-1 的自由区 41-1 的应用程序区 41A-1 中, 存储了其标识号为 ‘F-0325’ 的应用程序, 并且
30 该应用程序的启动操作已经完成。

另外, 根据图 7 所示的数据实例, 共有四个应用程序目前未存储到存储器 12 中, 但移动终端 11-1 的用户已经购买并且他/她可在任意

时间下载。其标识号为‘AP-4125’的应用程序是这样的一个程序，并且该程序本身被存储在由存储号‘T-7851’标识的应用程序信息存储单元52的一个区域中。另一方面，可以看到，其标识号为‘AP-3021’的应用程序目前并未存储在应用程序信息存储单元52中，这是因为一个说明‘已经删除’的符号被记录到了‘存储号’这一项中。还可以看到，其标识号为‘AP-4513’的应用程序被存储到管理服务器16的寄存应用程序区52R中，并且不需要存储号，这是因为没有数据提供给应用程序的‘存储号’这一项。当然，由于其信息存储在准备下载应用程序区53B的应用程序目前并未存储在移动终端11-1的存储器12中，因此，这些应用程序的启动操作还未被执行。至于这些应用程序，并未有数据提供给项目‘启动’。

如图6所示，应用程序信息存储单元52包括寄存应用程序区52R和临时保管应用程序区52T。在寄存应用程序区52R中，针对移动终端11开发的许多种应用程序的信息，如应用程序名称、应用程序版本号、应用程序的标识号、应用程序大小、应用程序使用费用、应用程序的功能概述等与应用程序一起存储到存储应用程序的位置上。除了它们之外，对于给定的可靠性指数高于一个特定级别的应用程序来说，诸如可靠性指数、公布和未公布的应用程序之间的区别、管理服务器16的管理实体已收取或未收取使用费用之间的差别等等这样的信息也被存储到寄存应用程序区52R中。对于未给定高于一个特定级别的可靠性指数的应用程序来说，在寄存应用程序52R中，‘可靠性指数’这一项给定为‘0’。

图8表示存储在寄存应用程序区52R中的数据实例的格式图，为了简化说明，它仅仅示出了以下诸项‘应用程序的标识号’、‘可靠性指数’、‘公布’、‘使用费的征收’和‘存储位置信息’。至于应用程序的存储位置信息，可以采用能够规定存储包含有应用程序的文件的位置的任意类型的信息。在下面的描述中，在因特网中广泛使用的统一资源定位符（URL）将被用作存储位置信息。

如图8的实例所示，根据存储在寄存应用程序区52R中的信息，可以看出，其标识号是‘AP-3568’的应用程序给定‘3’作为其可靠性指数；该应用程序在管理服务器16中公布；该应用程序的使用费的征收由管理服务器16的管理实体实施，并且应用程序本身存储在寄存

应用程序区 52R 中。另一方面，如果发现其标识号为 ‘AP-3712’ 的应用程序给定 ‘5’ 作为其可靠性指数，则该应用程序被公布但使用费的征收并不由管理服务器 16 的管理实体进行，而且应用程序本身也不存储在应用程序信息存储单元 52 中，相反，它以文件名 ‘ap-0306.exe’ 存储在由 ‘ftp://ftp.abc-software.com/application’ 所规定的位置上。而且，其标识号为 ‘F-3251’ 的应用程序并未给定可靠性指数，也没有数据提供给 ‘公布’ 和 ‘使用费征收’ 这两项。应用程序的公布和使用费的征收以及存储应用程序与存储位置信息之间的差别将在本说明书随后的部分中描述。

- 10 当移动终端 11 请求发送应用程序时，并且在应用程序被发送到移动终端 11 之前，在临时保管应用程序区 52T 中，其存储位置信息被寄存在寄存应用程序区 52R 的应用程序在管理服务器 16 接收到来自作为应用程序提供者的内容服务器 20 的应用程序之后的周期当中被临时存储。图 9 表示存储在临时保管应用程序区 52T 中的数据实例的格式图，
- 15 在临时保管应用程序区 52T 中，应用程序以及在临时保管应用程序区 52T 中指定应用程序的存储号一起被存储。

[1.2] 发送操作概述

下面解释发送应用程序的操作的概述。

[1.2.1] 购买应用程序之前的操作

- 20 [1.2.1.1] 密钥的公布

在根据本发明实施例的应用程序传送系统中，由一个管理实体管理的鉴别服务器 7 管理公共密钥系统的公共密钥，其中该管理实体独立于移动通信网络 15 的所有管理实体、管理服务器 16 的管理实体、内容服务器 20 的管理实体。

- 25 鉴别服务器 17 为其自身产生一对密钥，即鉴别服务器 17 的专用密钥（在下文中被称作 ‘鉴别服务器的专用密钥’ 或 ‘SK-AS’ ）以及鉴别服务器 17 的公共密钥（在下文中被称作 ‘鉴别服务器的公共密钥’ 或 ‘PK-AS’ ）。随后鉴别服务器 17 存储专用密钥，即 ‘SK-AS’ ，以免其泄露于外部实体，另一方面，它还发送公共密钥，即 ‘PK-AS’ 给
- 30 请求其的任何装置。根据其用户的操作，每个移动终端 11 为其自身产生一对密钥，即移动终端 11 的专用密钥（在下文中被称作 ‘移动终端的专用密钥’ 或 ‘SK-MT’ ）以及移动终端 11 的公共密钥（在下文中

被称作‘移动终端的公共密钥’或‘PK-MT’)。每个移动终端 11 的存储控制器 35 管理专用密钥,即‘SK-MT’以免其泄露于外部实体。另一方面,每个移动终端通过移动通信网络 15 向鉴别服务器 17 发送公共密钥,即‘PK-MT’。当鉴别服务器 17 接收来自移动终端 11 的

5 ‘PK-MT’时,鉴别服务器 17 把接收的公共密钥‘PK-MT’与移动终端 11 的标识号一起存储在其数据库中。与上述‘PK-AS’的情况一样,鉴别服务器 17 把公共密钥‘PK-MT’发送给请求其的任意装置。

如果需要把一个移动终端 11 的密钥与另一个移动终端 11 的密钥区别开,可在各自缩写的密钥之后增加每个移动终端 11 的下标号。例如,

10 如,移动终端 11-1 的专用密钥被称作‘SK-MT-1’。

与每个移动终端 11 的情况一样,管理服务器 16 和每个内容服务器 20 产生它们的密钥对,即专用密钥和公共密钥。随后,管理服务器 16 和每个内容服务器 20 存储它们的专用密钥以免它们泄露于外部实体,同时把它们的公共密钥发送给鉴别服务器 17。当鉴别服务器 17

15 接收来自管理服务器 16 的公共密钥时,鉴别服务器 17 把接收的公共密钥与管理服务器 16 的标识号一起存储在其数据库中。鉴别服务器 17 在其接收到内容服务器 20 的公共密钥时将针对内容服务器 20 执行相同的操作。鉴别服务器 17 把管理服务器 16 和内容服务器 20 的公共密钥发送给请求这些密钥的任意装置,这与鉴别服务器 17 和移动终端 11

20 的情况相同。在本说明书中,管理服务器 16 和内容服务器 20 的专用密钥和公共密钥将被称作:

管理服务器 16 的专用密钥: ‘管理服务器的专用密钥’或‘SK-MS’

管理服务器 16 的公共密钥: ‘管理服务器的公共密钥’或‘PK-MS’

25 MS’

内容服务器 20 的专用密钥: ‘内容服务器的专用密钥’或‘SK-CS’

内容服务器 20 的公共密钥: ‘内容服务器的公共密钥’或‘PK-CS’

与在移动终端 11 中的情况一样,如果需要把一个内容服务器 20 的密钥与另一个内容服务器 20 的密钥区别开,可在各自缩写的密钥之后增加每个内容服务器 20 的下标号。例如,内容服务器 20-1 的专用

30

密钥被称作‘SK-CS-1’。

使用密钥加密的算法和使用公共密钥的解密算法在鉴别服务器 17、在每个移动终端 11、在管理服务器 16 以及在每个内容服务器 20 中都是一样的。因此，这些装置可在它们之间交换加密数据并通过交
5 换它们的公共密钥解密数据。

[1.2.1.2] 应用程序的检查

内容服务器 20 的管理实体可向管理服务器 16 的管理实体申请其应用程序的实质检查，这样，如果该应用程序需要执行与其它任意应用程序协调的任意操作，或者如果该应用程序需要处理具有高位值的信息，那么将给定该应用程序一个高于请求的某个级别的可靠性指
10 数。

如果管理服务器 16 的管理实体接收来自内容服务器 20 的管理实体的应用程序大致检查的申请，则管理服务器 16 的管理实体将检查使用该应用程序的目的、该应用程序的操作的描述、由内容服务器 20 的管理实体操作的管理该应用程序的系统，如此等等。
15

根据检查结果，管理服务器 16 的管理实体向被检查的应用程序提供一个适当级别的可靠性指数。可靠性指数可以用许多种方式表示，但在下面的解释中，该指数系统有 6 个级别。指数‘1’、‘2’、‘3’、‘4’和‘5’被指定给通过上述检查的应用程序。指数越大，应用程序的可靠性越高。指数‘0’指定给未进行检查或未通过检查的应用程序。
20

例如，对于给定可靠性指数为‘5’的应用程序来说，管理服务器 16 的管理实体检查由内容服务器 20 的管理实体管理应用程序的系统、该应用程序的操作稳定性等，并判断检查结果是否符合要求。如果需要的
25 话，允许该应用程序使用移动终端 11 的控制程序的功能、存储在控制存储器 32 中的数据、存储在存储器 12 中的应用程序的功能和存储在存储器 12 中的数据。这些数据可包括高位值的数据，如移动终端 11 的用户个人信息、信用卡号等。

相反，指定可靠性指数为‘1’的应用程序可以是其操作目的并不是使用诸如个人信息或财政信息这样的高位值数据的应用程序，并且即使该应用程序的操作是稳定的，也不需要给定该应用程序一个高级别的可靠性指数。不过，在这种情况下，该应用程序可能被估计为具
30

有低信息安全性的应用程序，而这会引起高位值数据的泄露，原因是由于缺乏内容服务器 20 的管理实体的安全数据管理系统。可靠性指数为 ‘1’ 的应用程序可执行与可靠性指数为 ‘1’ 或 ‘0’ 的另一个应用程序的协调操作。可靠性指数为 ‘1’ 的应用程序也可将其数据或功能传送给可靠性指数为 ‘2’、‘3’、‘4’ 或 ‘5’ 的应用程序。但是，可靠性指数为 ‘1’ 的应用程序不能接收可靠性指数为 ‘2’、‘3’、‘4’ 或 ‘5’ 的应用程序的数据或者使用其功能。可靠性指数为 ‘1’ 的应用程序不能使用移动终端 11 的控制程序的任何功能，也不能使用控制存储器 32 中存储的数据。

10 如果管理服务器 16 的管理实体决定给定一个应用程序的可靠性指数为 ‘1’ 或大于 ‘1’，则其与该应用程序的标识号一起寄存在管理服务器 16 的寄存应用程序区 52R 的 ‘可靠性指数’ 这一项中。

[1.2.1.3] 对管理服务器公布应用程序的请求

内容服务器 20 的管理实体可以请求由管理服务器 16 向移动终端 11 公布可靠性指数为 ‘1’ 或大于 ‘1’ 的应用程序。对于被请求公布的应用程序来说，响应 ‘是’ 被寄存在管理服务器 16 的寄存应用区 52R 中的 ‘公布’ 这项中。如果管理服务器 16 接收来自移动终端 11 的发送可购买的应用程序的信息的请求，则管理服务器 16 向移动终端 11 发送其在寄存应用程序区 52R 的 ‘公布’ 项中的值是 ‘是’ 的应用程序的信息。根据这个信息，移动终端 11 的用户可以知道哪些应用程序被公布，并且购买公布的应用程序远远易于购买其它应用程序。

相反，如果移动终端 11 的用户想要购买管理服务器 16 未公布的应用程序，则用户直接通过因特网访问作为应用程序提供者的内容服务器 20 的主页来向内容服务器 20 的管理实体申请购买该应用程序。

25 例如，如果内容服务器 20 的管理实体希望只允许管理内容服务器 20 的管理实体设定的某些要求的移动终端 11 使用其应用程序，则对于内容服务器 20 的管理实体来说，不通过管理服务器 16 公布其应用程序会更为方便。但是，未由管理服务器 16 公布的应用程序也可以通过管理服务器 16 发送给移动终端 11，并且应用程序的信息也能够以管理服务器 16 公布应用程序的相同方式由管理服务器 16 进行管理。

[1.2.1.4] 对管理服务器征收使用费的请求

内容服务器 20 的管理实体可请求可靠性指数为 ‘1’ 或大于 ‘1’

的应用程序的使用费用征收的管理由管理服务器 16 来实施。对于其使用费用征收的管理被请求由管理服务器 16 来执行的应用程序来说，响应‘是’被寄存在管理服务器 16 的寄存应用程序区 52R 中的‘使用费征收’这一项中。

- 5 如果管理服务器 16 接收到移动终端 11 的关于购买其在寄存应用程序区 52R 的‘使用费征收’这一项的值为‘是’的应用程序的请求，则在该应用程序的信息存储和管理服务器 16 的准备下载应用程序区 53B 时，管理服务器把诸如该应用程序标识号、移动终端 11 的标识号以及该应用程序的购买日期和时间等的信息发送给与移动通信网络 15 连接的费用管理服务器。类似地，在管理服务器 16 执行其在寄存应用程序区 52R 中的‘使用费用征收’项的值为‘是’的应用程序的启动操作时，管理服务器 16 把诸如该应用程序标识号、移动终端 11 的标识号以及该应用程序的购买日期和时间等的信息发送给与移动通信网络 15 连接的费用管理服务器。正如上面所解释的，费用管理服务器根据管理服务器 16 发送的信息计算每个移动终端 11 的每个应用程序的使用费用。内容服务器 20 的管理实体和管理服务器 16 的管理实体事先同意关于每个应用程序的使用费的某些条件，也就是说，使用费是根据应用程序的购买还是根据应用程序的启动来计算；并且同意的条件作为收费信息的一部分寄存在费用管理服务器中。由费用管理服务器计算的每个应用程序的使用费连同也是由费用管理服务器计算的移动终端 11 的通信费用一起由移动通信网络 15 的管理实体向移动终端 11 的每个用户征收。移动通信网络 15 的管理实体通过征收的费用推算出某一个数额作为征收费用的手续费，并把剩余的费用汇至作为应用程序提供者的内容服务器 20 的管理实体。而且，移动通信网络 15 的管理实体把征收费用的手续费中的一部分作为获得关于征收使用费的信息的服务费提供给管理服务器 16 的管理实体。

[1.2.1.5] 对管理服务器存储应用程序的请求

- 内容服务器 20 的管理实体可请求其可靠性指数为‘1’或大于‘1’的应用程序存储到管理服务器 16 的寄存应用程序区 52R 中。如果一个应用程序被请求存储到寄存应用程序区 52R 中，则该应用程序本身被存储到寄存应用程序区 52R 的‘存储位置信息’这一项中，而不是存储关于该应用程序位置的信息。

根据管理服务器 16 和内容服务器 20 间通信的传输率以及应用程序的特性等，内容服务器 20 的管理实体可判断其应用程序本身是否应当存储在寄存应用程序区 52R 中，或者仅仅是有关应用程序存储位置的信息寄存在寄存应用程序区 52R 中。如果应用程序本身存储在寄存应用程序区 52R 中，则可在移动终端 11 请求发送该应用程序之后立即发送该应用程序给移动终端 11，因为管理服务器 16 在该请求的时间可以不必接收来自内容服务器 20 的应用程序就可以发送该应用程序。因而，对于内容服务器 20 的管理实体来说，请求其应用程序存储到寄存应用程序区 52R 是相当有益的，特别是当管理服务器 16 和内容服务器 20 间的通信的传输率比较低的时候。相反，如果一个应用程序并未存储在寄存应用程序区 52R 中，并且每次当管理服务器 16 接收到来自移动终端 11 的发送应用程序的请求时该应用程序从内容服务器 20 发送到管理服务器 16，则内容服务器 20 能够发送针对移动终端 11 的具有一些客户化的应用程序。例如，内容服务器 20 对每个移动终端 11 的相同应用程序设置不同的存取密钥，以防止未经许可的用户使用该应用程序。

下面参考图 10 和图 11 的流程图解释当内容服务器 20-1 请求管理服务器 16 存储应用程序时执行的一系列操作。首先，内容服务器 20-1 把存储应用程序的请求发送给管理服务器 16（步骤 S101）。该存储请求包含该应用程序的标识号。

当管理服务器 16 接收到存储该应用程序的请求时，管理服务器 16 使用包含于该存储请求中的标识号读出存储在寄存应用程序区 52R 中的数据，并确认该应用程序给定的可靠性指数为‘1’或大于‘1’。在确认之后，管理服务器 16 把接受存储请求的通知发送给内容服务器 20-1（步骤 S102）。

当内容服务器 20-1 接收到接受存储请求的通知时，内容服务器 20-1 向鉴别服务器 17 发送‘PK-MS’传输请求，即管理服务器 16 的公共密钥（步骤 S103）。通过响应公共密钥的传输请求，鉴别服务器 17 把‘PK-MS’发送给内容服务器 20-1（步骤 S104）。

在接收‘PK-MS’之后，内容服务器 20-1 使用‘PK-MS’加密该应用程序（步骤 S105）。当应用程序从内容服务器 20-1 发送到管理服务器 16 时，由于这个加密操作，在线路上窃取该应用程序的那些未经

许可的人将不能使用该程序。

而且，内容服务器 20-1 将使用 ‘SK-CS-1’ 即内容服务器 20-1 的专用密钥再次加密已加密的应用程序（步骤 S106）。由于该加密操作，管理服务器 16 可以确认该应用程序确实是由内容服务器 20-1 发送。这也就是说，该加密起到了一个证明的作用，它能够使管理服务器 16 确认该应用程序的发送侧。

内容服务器 20-1 把双重加密的应用程序发送给管理服务器 16（步骤 S107）。

在接收到该双重加密的应用程序之后，管理服务器 16 读出存储在管理服务器 16 的密钥存储单元 51 中的数据，以检验是否能在该数据中获得 ‘PK-CS-1’，即内容服务器 20-1 的公共密钥。如果 ‘PK-CS-1’ 并未寄存在密钥存储单元 51 中，则管理服务器 16 向鉴别服务器 17 发送 ‘PK-CS-1’ 的传输请求（步骤 S108）。通过响应公共密钥的传输请求，鉴别服务器 17 把 ‘PK-CS-1’ 发送给管理服务器 16（步骤 S109）。如果 ‘PK-CS-1’ 被寄存在密钥存储单元 51 中，管理服务器 16 将跳过步骤 S108 和步骤 S109 并前进到步骤 S110，这是因为此时并不需要获得来自外部信号源的 ‘PK-CS-1’。

随后，管理服务器 16 使用 ‘PK-CS-1’ 解密已双重加密的应用程序（步骤 S110）。如果解密应用程序失败，则表明管理服务器 16 接收的应用程序在传输期间被篡改，或者该应用程序由于另外的原因被破坏，或者该应用程序是由不是内容服务器 20-1 的一个服务器发送。因此，在这种情况下，管理服务器 16 不进行下面的操作，而是向内容服务器 20-1 发送合适的应用程序的重发请求。相反，如果使用 ‘PK-CS-1’ 解密应用程序成功，则可以确认该应用程序是没有任何问题地由内容服务器 20-1 发送。因此，管理服务器 16 使用 ‘SK-MS’ 即管理服务器 16 的专用密钥再次解密该应用程序（步骤 S111）。根据这些操作，管理服务器 16 可获得未加密的应用程序，并且管理服务器 16 的管理实体在必要时可检验内容服务器 20-1 的管理实体或者其它人是否进行了篡改。

在下文中，上面解释的从步骤 S103 至步骤 S111 的这一系列操作将被称作 ‘向管理服务器的应用程序发送操作 1’

在步骤 S111 之后，管理服务器 16 把该应用程序存储到寄存应用

程序区 52R (步骤 S112), 并向内容服务器 20-1 发送存储应用程序的操作完成的通知 (步骤 S113)。

[1.2.2] 应用程序的购买

在应用程序发送到移动终端 11 之前, 移动终端 11 的用户需要购买该应用程序。总之, 移动终端 11 的用户购买应用程序的方法有两种, 即通过管理服务器 16 购买管理服务器 16 公布的应用程序, 或者使用内容服务器 20 中的主页订立购买合同而直接从内容服务器 20 的管理实体购买应用程序。在购买合同由移动终端 11 的用户和内容服务器 20 的管理实体两者直接订立的这后一种方法中, 根据应用程序给定的可靠性指数是 '1' 或大于 '1', 或者应用程序给定的可靠性指数是 '0', 可以有两种不同的操作。下面是购买应用程序的一系列操作的例子。

[1.2.2.1] 管理服务器公布的应用程序的购买

参考图 12、图 13、图 14 和图 15, 下面的例子是在移动终端 11-1 的用户通过管理服务器 16 购买其提供者是内容服务器 20-1 的管理服务器 16 所公布的应用程序时执行的一系列操作。

首先, 移动终端 11-1 的用户按动移动终端 11-1 的 appli-按钮 23 以使其显示如屏幕 D11 所示的应用程序菜单。接着, 用户按动操作单元 22 的按钮 '1. 新的应用程序的购买' 以选择项目 '1'。当按动按钮 '1' 时, 移动终端 11-1 向管理服务器 16 发送可获得的程序的信息的传输请求 (步骤 S201)。

在接收到可获得的程序的信息的传输请求之后, 管理服务器 16 读出存储在寄存应用程序区 52R 中的数据并提取其 '公布' 项的值为 '是' 的应用程序以及未寄存在用户信息存储单元 53-1 中的那些应用程序的信息。接着, 管理服务器 16 向移动终端 11-1 发送作为与可获得的程序有关的信息的所提取的信息, 包括程序的标识号、程序的名称、程序的功能、程序的使用费用、使用费用的征收是否由管理服务器管理的信息、以及在内容服务器 20 中的主页的位置信息, 如 URL (步骤 S202)。

在接收到关于可获得的程序的信息之后, 移动终端 11-1 显示屏幕 D12。通过响应该屏幕, 移动终端 11-1 的用户按动与已经购买的程序相对应的按钮。例如, 当屏幕 D12 显示时, 如果用户按动按钮 '1', 则 '时间表管理 Ver. 2' 这一项被选择, 并且移动终端 11-

1 在显示单元 21 上显示屏幕 D13。根据移动终端 11-1 的用户作出的是
是否购买应用程序的判断，屏幕 D13 表示出有关所选应用程序的功能和
使用费用的信息。如果移动终端 11-1 的用户决定购买该应用程序并且
在显示屏幕 D13 时按动按钮 ‘9’，则移动终端 11-1 把所选应用程序
5 的标识号发送给管理服务器 16（步骤 S203）。随后，移动终端 11-1
在显示单元 21 上显示屏幕 D14。

在接收到应用程序的标识号之后，管理服务器 16 读出存储在寄存
应用程序区 52R 中的数据，并且获得该应用程序的存储位置信息（步
骤 S204）。

10 在步骤 S204，如果所选的应用程序本身并未存储在寄存应用程序
区 52 中，管理服务器 16 通过存储在寄存应用程序区 52 中的数据获得
内容服务器 20-1 中的应用程序的 URL，以作为存储位置信息。在这种
情况下，管理服务器 16 向内容服务器 20-1 发送该应用程序的传输请
求（步骤 S205）。

15 当内容服务器 20-1 接收应用程序的传输请求时，将启动与 ‘对管
理服务器的应用程序发送操作 1’ 相同的一系列操作。也就是说，管理
服务器 16、鉴别服务器 17 和内容服务器 20-1 执行如图 10 和图 11 所
示的从步骤 S103 到步骤 S111 的操作。作为执行该系列操作的结果，
管理服务器 16 获得该应用程序（步骤 S206）。

20 管理服务器 16 把一个存储号分配给所获得的应用程序，并把应用
程序与存储号一起存储到临时保管应用程序区 52T 中（步骤 S207）。
该存储号用于管理服务器 16 规定该应用程序在临时保管应用程序区
52T 中存储的位置。而且，如果存储了不同的应用程序，则向它们中的
每一个分配不同的存储号，即使它们的内容完全相同。

25 相反，如果由移动终端 11-1 选择的应用程序存储在管理服务器 16
的寄存应用程序区 52R 中，管理服务器 16 跳过从步骤 S205 到步骤 S207
的操作并且移动到步骤 S208，这是因为该应用程序已经被得到。

接着，管理服务器 16 把诸如应用程序的标识号和可靠性指数这样
的有关应用程序的信息寄存在用户信息存储单元 53-1 的准备下载应用
程序区 53B 中（步骤 S208）。在已经执行步骤 S208 的寄存操作之后，
30 移动终端 11-1 的用户能够在用户希望的任意时间把已经寄存在准备下
载应用程序区 53B 中的应用程序下载到移动终端 11-1 上。当寄存操作

完成之后，响应‘否’作为应用程序的‘启动’项的值被寄存，这是因为该应用程序还未被下载到移动终端 11-1 上，该应用程序的启动操作必然还未被执行。如果寄存的应用程序存储在临时保管应用程序区 52T 中，则该应用程序的存储号也被寄存在准备下载应用程序区 53B 中。当寄存操作完成之后，管理服务器 16 向移动终端 11-1 发送购买该应用程序的操作完成的通知（步骤 S209）。

在接收到购买该应用程序的操作完成的通知之后，移动终端 11-1 显示屏幕 D15 或屏幕 D16。屏幕 D15 表示在新购买的应用程序是一个其使用费由管理服务器 16 管理的应用程序时所显示的屏幕，并且该屏幕告知移动终端 11-1 的用户应用程序的使用费将与通信费一起征收。相反，屏幕 D16 是在该应用程序是其使用费不由管理服务器 16 管理的应用程序时所显示的屏幕，并且该屏幕告知移动终端 11-1 的用户执行用以支付应用程序的使用费的必要程序是用户的责任。当显示屏幕 D16 时，移动终端 11-1 的用户可按动按钮‘0’以显示由内容服务器 20-1 的管理实体所管理的主页，并在主页上进行支付所购应用程序使用费的必要步骤。

如果移动终端 11-1 的用户按动按钮‘9’以完成购买上述新应用程序的一系列操作，则当显示屏幕 D15 或屏幕 D16 时，移动终端 11-1 在显示单元 21 上显示屏幕 D17。屏幕 D17 类似于正常的屏幕，它在移动终端 11-1 处于备用时显示，但字母‘a’也显示在该屏幕上。字母‘a’是一个通知移动终端 11-1 的用户应用程序已准备好下载的符号。但是，也有其它的方式可以通知移动终端 11-1 的用户应用程序已准备好下载，并不限于显示字母‘a’。为了实现相同的目的，也可以采用其它的方式，如显示其它类型的符号或图像，发声或者振动移动终端 11-1。

在管理服务器 16 在步骤 S209 发送购买应用程序的操作已经完成的通知之后，管理服务器 16 向内容服务器 20-1 发送移动终端 11-1 购买应用程序的通知（步骤 S210）。而且，如果购买的应用程序是其使用费由管理服务器 16 管理的应用程序，则管理服务器 16 向费用管理服务器发送有关购买的应用程序的信息，如应用程序的标识号、移动终端 11-1 的标识号、购买应用程序的时间和日期等（步骤 S211）。

[1.2.2.2] 给定可靠性指数为‘1’或大于‘1’并且其未被公布

的应用程序的购买

参考图 16 和图 17，下面的例子是当移动终端 11-1 的用户购买并未由内容管理器 20-1 作为其提供者的管理服务器 16 公布并且给定可靠性指数为 ‘1’ 或大于 ‘1’ 的应用程序时所执行的一系列操作。

5 如果移动终端 11-1 的用户购买未由管理服务器 16 公布的应用程序，则移动终端 11-1 的用户在移动终端 11-1 上显示内容服务器 20-1 的主页，并申请购买主页中的应用程序（步骤 S301）。移动终端 11-1 的用户在必要时还负责在同样的主页上执行支付应用程序使用费的步骤。

10 在步骤 S301 中，内容服务器 20-1 检验由移动终端 11-1 发送给内容服务器 20-1 的购买请求的内容是否满足要求，并且如果购买请求的内容满足要求，则内容服务器 20-1 向移动终端 11-1 发送接受购买该应用程序的通知（步骤 S302）。接受购买该应用程序的通知包含该应用程序的标识号。当内容服务器 20-1 发送接受通知时，内容服务器
15 20-1 记录其购买应用程序的请求被接受的移动终端 11-1 的标识号。

在接收到接受购买该应用程序的通知之后，移动终端 11-1 向管理服务器 16 发送寄存购买的程序的信息的请求（步骤 S303）。寄存该信息的请求包含新购买的程序的标识号。

在接收到移动终端 11-1 的关于所购程序的信息之后，根据该
20 程序的标识号，管理服务器 16 读出存储在寄存程序区 52R 中的数据，并获得来自内容服务器 20-1 的 URL，以作为被请求寄存的程序的提供者的位置信息。随后，管理服务器 16 向内容服务器 20-1 发送允许执行程序寄存的请求，以确认对于内容服务器 20-1 来说可接受该程序被寄存以作为移动终端 11-1 使用 URL 购买的程序
25 （步骤 S304）。允许程序寄存的请求包含移动终端 11-1 的标识号。

在接收到来自管理服务器 16 的允许程序寄存的通知之后，内容服务器 20-1 检验对于其来说管理服务器 16 准备把该程序寄存为购买的程序的移动终端的标识号是否匹配对于其来说内容服务器
30 20-1 在步骤 S302 接受购买该程序的请求的移动终端的标识号。如果这些标识号匹配，则内容服务器 20-1 向管理服务器 16 发送允许程序寄存的请求（步骤 S305）。

在接收到来自内容服务器 20-1 的允许应用程序寄存的通知之后，管理服务器 16 读出存储在寄存应用程序区 52R 中的数据，并获得移动终端 11-1 请求寄存的应用程序的存储信息（步骤 S306）。

如果在步骤 S306 被请求寄存的应用程序并未存储在寄存应用程序区 52R 中，通过使用记录在寄存应用程序区 52R 中的应用程序的存储位置信息，管理服务器 16 将把发送该应用程序的请求发送至内容服务器 20-1（步骤 S307）。当内容服务器 20-1 接收到发送应用程序的请求时，则开始与‘对于管理服务器的应用程序发送操作 1’相同的一系列操作。换言之，管理服务器 16、鉴别服务器 17 和内容服务器 20-1 执行图 10 和图 11 所示的从步骤 S103 到步骤 S111 的操作。作为执行该系列操作的结果，管理服务器 16 获得该应用程序（步骤 S308）。管理服务器把一个存储号分配给所获得的应用程序，并把该应用程序与该存储号一起存储到临时保管应用程序区 52T 中（步骤 S309）。

相反，如果移动终端 11-1 请求寄存的应用程序存储到寄存应用程序区 52R 中，管理服务器 16 将跳过从步骤 S307 到步骤 S309 的操作并前进到步骤 S310。接着，管理服务器 16 在用户信息存储单元 53-1 的准备下载应用程序区 53B 中寄存移动终端 11-1 请求寄存的应用程序的信息，即该应用程序的标识号、该应用程序的可靠性指数等（步骤 S310）。对于‘启动’项来说，响应‘否’作为该项的值被寄存，这是因为该应用程序还未执行启动操作。如果该应用程序存储在临时保管应用程序区 52T 中，则该应用程序的存储号也寄存在准备下载应用程序区 53B 中。在步骤 S310 的寄存操作之后，移动终端 11-1 的用户能够在其希望的任意时间内把已经寄存在准备下载应用程序区 53B 的应用程序下载到移动终端 11-1，当寄存操作完成时，管理服务器 16 向移动终端 11-1 发送购买应用程序的操作完成的通知（步骤 S311）。

当移动终端 11-1 接收到购买应用程序的操作完成的通知时，移动终端 11-1 在显示单元 21 上显示字母‘a’，用于通知移动终端 11-1 的用户新购买的应用程序准备从管理服务器 16 下载。如果购买的应用程序是其使用费由管理服务器 16 管理的应用程序，则管理服务器 16 向费用管理服务器发送有关购买的应用程序的信息，如该应用程序的标识号、移动终端 11-1 的标识号、购买应用程序的时间和日期等（步骤 S312）。

[1.2.2.3] 给定可靠性指数为‘0’的应用程序的购买

参考图 18、图 19 和图 20，下面的例子是在移动终端 11-1 的用户购买其提供者是内容服务器 20-1 并且其可靠性指数为‘0’的应用程序时所执行的一系列操作。本例中的操作类似于从步骤 S301 开始的一系列操作，并将参考图 16 和图 17 进行解释。但是，在下面的操作中，管理服务器 16 不需要获得在普通文件中的应用程序以检验其内容，这是因为该应用程序并未被给定‘1’或者大于‘1’的可靠性指数。因此，当应用程序从内容服务器 20-1 发送到管理服务器 16 时，该应用程序并不使用管理服务器 16 的公共密钥加密，而是使用移动终端 11-1 的公共密钥加密。由于这种加密的原因，即使该应用程序在其传输期间被窃取，该应用程序也不能被移动终端 11-1 的未经许可的用户所理解。因此可以防止未经许可使用该应用程序，同时也可保证应用程序的内容的隐藏。

在这一系列操作中，移动终端 11-1 的用户首先在移动终端 11-1 上显示内容服务器 20-1 的主页，并申请购买该主页中的应用程序（步骤 S401）。移动终端 11-1 的用户还负责在同一个主页上执行支付应用程序使用费的必要步骤。

内容服务器 20-1 检验在步骤 S401 从移动终端 11-1 发送到内容服务器 20-1 的购买请求的内容是否满足要求，而且，如果购买请求的内容满足要求，则内容服务器 20-1 向移动终端 11-1 发送接受购买应用程序的通知（步骤 S402）。接受购买应用程序的通知包括该应用程序的标识号。当内容服务器 20-1 发送该接受通知时，内容服务器 20-1 记录其购买应用程序的请求已被接受的移动终端 11-1 的标识号。

在接收到接受购买应用程序的通知之后，移动终端 11-1 向管理服务器 16 发送寄存所购买应用程序的信息的请求（步骤 S403）。寄存该信息的请求包括该应用程序的标识号以及作为该应用程序的存储位置信息的内容服务器 20-1 中的 URL。

在接收到来自移动终端 11-1 的寄存该信息的请求之后，管理服务器 16 把发送该应用程序的请求发送给内容服务器 20-1（步骤 S404）。发送应用程序的请求包括移动终端 11-1 的标识号。

在接收到来自管理服务器 16 的发送应用程序的请求之后，内容服务器 20-1 检验请求发送应用程序的移动终端的标识号与内容服务器

20-1 在步骤 S402 接受其购买应用程序请求的移动终端的标识号是否匹配。如果这些标识号匹配，则内容服务器 20-1 向鉴别服务器 17 发送一个发送 ‘PK-MT-1’ 的请求，即发送移动终端 11-1 的公共密钥（步骤 S405）。通过响应发送 ‘PK-MT-1’ 的请求，鉴别服务器 17 向内容服务器 20-1 发送 ‘PK-MT-1’（步骤 S406）。

在接收到 ‘PK-MT-1’ 之后，内容服务器 20-1 使用 ‘PK-MT-1’ 加密所发送的应用程序（步骤 S407）。

而且，内容服务器 20-1 使用 ‘SK-CS-1’ 即内容服务器 20-1 的专用密钥再次加密已加密的应用程序（步骤 S408）。由于该加密操作，管理服务器 16 可确认该应用程序确实由内容服务器 20-1 发送。

内容服务器 20-1 把双重加密的应用程序发送给管理服务器 16（步骤 S409）。

在接收到双重加密的应用程序之后，管理服务器 16 读出存储在管理服务器 16 的密钥存储单元 51 中的数据以检验 ‘PK-CS-1’ 即内容服务器 20-1 的公共密钥是否可在该数据中得到。如果 ‘PK-CS-1’ 未寄存在密钥存储单元 51 中，管理服务器 16 则向鉴别服务器 17 发送 ‘PK-CS-1’ 的传输请求（步骤 S410）。通过响应该公共密钥的传输请求，鉴别服务器 17 把 ‘PK-CS-1’ 发送给管理服务器 16（步骤 S411）。如果 ‘PK-CS-1’ 寄存在密钥存储单元 51 中，管理服务器 16 跳过步骤 S410 和步骤 S411 并前进到步骤 S412，这是因为在此不需要从外部信号源获得 ‘PK-CS-1’。

随后，管理服务器 16 使用 ‘PK-CS-1’ 解密双重加密的应用程序（步骤 S412）。如果该应用程序的解密失败，则表明管理服务器 16 接收的应用程序在传输期间被篡改，或者该应用程序由于某种原因而破坏，或者该应用程序是由不是内容服务器 20-1 的服务器发送。因此，在这种情况下，管理服务器 16 不前进到下面的操作，而是向内容服务器 20-1 发送合适的应用程序的重发请求。相反，如果使用 ‘PK-CS-1’ 解密应用程序成功，则可以确认该应用程序是无任何问题地从内容服务器 20-1 发送。

上面解释的从步骤 S405 到步骤 S412 的一系列操作在下文中将被称作 ‘对于管理服务器的应用程序的发送操作 2’。

接着，管理服务器 16 把一个存储号分配给该应用程序，并把该应

用程序与该存储号一起存储到临时保管应用程序区 52T 中（步骤 S413）。在这种情况下，存储在临时保管应用程序区 52T 中的应用程序仍然使用 ‘PK-MT-1’ 即移动终端 11-1 的公共密钥加密，并且该应用程序不能由管理服务器 16 的管理实体解密。

- 5 接着，管理服务器 16 把该应用程序的标识号和作为该应用程序的存储位置信息的内容服务器 20-1 中的 URL 寄存到寄存应用程序区 52R 中（步骤 S414）。利用此寄存操作寄存的信息指的是管理服务器 16 何时需要响应发送应用程序的请求而获得来自内容服务器 20-1 的相同的应用程序。至于与寄存应用程序区 52R 中的应用程序相对应的数据，
- 10 ‘可靠性指数’ 这一项的值被设定为 ‘0’ 并且 ‘公布’ 项的值保留空白（ ‘-’ ）。

- 接着，管理服务器 16 在用户信息存储单元 53-1 的准备下载应用程序区 53B 中寄存移动终端 11-1 请求寄存的应用程序的信息，即应用程序的标识号、应用程序的存储号等（步骤 S415）。对于 ‘启动’ 项
- 15 来说，响应 ‘否’ 作为该项的值被寄存，而对于 ‘可靠性指数’ 项来说， ‘0 作为该项的值被寄存，在步骤 S415 的寄存操作之后，移动终端 11-1 的用户能够在其希望的任意时间把已经寄存在准备下载应用程序区 53B 的应用程序下载到移动终端 11-1。当寄存操作完成时，管理服务器 16 向移动终端 11-1 发送购买应用程序的操作完成的通知（步
- 20 骤 S416）。

 当移动终端 11-1 接收到购买应用程序的操作完成的通知时，移动终端 11-1 在显示单元 21 上显示字母 ‘a’，用于通知移动终端 11-1 的用户新购买的应用程序准备从管理服务器 16 下载。

[1.2.3] 向移动终端的应用程序的下载

- 25 在移动终端 11 的用户购买应用程序之后，该用户需要把购买的应用程序下载到移动终端 11-1 上。参考图 21、图 22、图 23、图 24 和图 25，下面的例子表示当移动终端 11-1 下载应用程序时所执行的一系列操作。

- 首先，移动终端 11-1 的用户按下移动终端 11-1appli 按钮 23 以
- 30 显示屏幕 D21 所示的应用程序菜单。当显示屏幕 D21 时，移动终端 11-1 的用户按动操作单元 22 的按钮 ‘2’ 以选择 ‘2. 应用程序的下载’ 这一项。当按动按钮 ‘2’ 时，移动终端 11-1 向管理服务器 16 发送关于

可下载到移动终端 11-1 的应用程序的信息的请求（步骤 S501）。

在接收到发送应用程序的信息的请求之后，管理服务器 16 向移动终端 11-1 发送寄存在用户信息存储单元 53-1 的准备下载应用程序区 53B 中的应用程序的名称、应用程序的标识号，以作为关于应用程序的信息（步骤 S502）。

在接收到关于应用程序的信息之后，移动终端 11-1 显示屏幕 D22。通过响应该屏幕，并通过按动其数字对应于屏幕上的应用程序号的按钮，移动终端 11-1 的用户可指定一个应用程序。例如，当屏幕 D22 显示时，如果用户按动按钮 ‘1’，则题为 ‘时间表管理 Ver.2’ 的应用程序被指定。当应用程序通过移动终端 11-1 的用户的操作被指定时，移动终端 11-1 向管理服务器 16 发送指定的应用程序的标识号（步骤 S503）。

在接收到所指定应用程序的标识号之后，管理服务器 16 读出存储在准备下载应用程序区 53B 中的数据，并检验所指定的应用程序的可靠性指数是否给定为 ‘1’ 或者大于 ‘1’。接着，管理服务器 16 读出存储在下载应用程序程序区 53A 中的数据并检验移动终端 11-1 的存储器 12 是否具有足够的自由空间存储所指定的应用程序（步骤 S504）。在步骤 S504，如果所指定的应用程序给定的可靠性指数为 ‘1’ 或者大于 ‘1’，则检验存储器 12 在管理区 40 中是否具有足够的自由空间。相反，在步骤 S504，如果所指定的应用程序的可靠性指数未指定为 ‘1’ 或者大于 ‘1’，则检验存储器 12 在自由区 41 中是否具有足够的自由空间。

在步骤 S504，如果移动终端 11-1 的存储器 12 没有足够的自由空间来存储所指定的应用程序，则管理服务器 16 向移动终端 11-1 发送指定要从存储器 12 中删除的应用程序的请求（步骤 S505）。指定应用程序的请求包含表示被请求下载的应用程序给定的可靠性指数是否为 ‘1’ 或者大于 ‘1’ 的信息。当移动终端 11-1 接收到指定应用程序的请求时，移动终端 11-1 通过显示单元 21 显示屏幕 D23。通过响应该屏幕，如果移动终端 11-1 的用户按动按钮 ‘9’ 以命令下面操作的执行，则移动终端 11-1 在显示单元 21 上显示屏幕 D24。如果被指定下载的应用程序是可靠性指数为 ‘1’ 或者大于 ‘1’ 的应用程序，则存储在管理区 40 中的应用程序的名称罗列在屏幕 D24 上。相反，如果

被指定下载的应用程序是未给定可靠性指数为‘1’或者大于‘1’的应用程序，则存储在自由区 41 中的应用程序的名称罗列在屏幕 D24 上。通过响应该屏幕，移动终端 11-1 的用户通过按动其数字与屏幕上的应用程序号相对应的按钮来指定用户决定从存储器 12 中删除的应用程序。移动终端 11-1 把所指定的应用程序的标识号发送给管理服务器 16（步骤 S506）。在步骤 S506 的操作之后，移动终端 11-1 在显示单元 21 上显示屏幕 D25。

相反，在步骤 S504，如果移动终端 11-1 的存储器 12 具有足够的自由空间存储指定下载的应用程序，则跳过步骤 S505 和步骤 S506 的操作，并且管理服务器 16 前进到步骤 S507 的操作。在这种情况下，移动终端 11-1 在显示单元 21 上显示屏幕 D25。

接着，管理服务器 16 读出存储在准备下载应用程序区 53B 中的数据，并检验由移动终端 11-1 指定下载的应用程序是否存储在应用程序信息存储单元 52 中（步骤 S507）。参考图 7，下面的例子表示当应用程序存储到应用程序信息存储单元 52 中所执行的操作以及当应用程序未存储到应用程序信息存储单元 52 中所执行的操作。

如果移动终端 11-1 指定下载的应用程序的标识号是‘AP-4125’，则根据图 7 所示的数据实例，相应的存储号是‘T-7851’。这意味着该应用程序存储在临时保管应用程序区 52T 中。如果移动终端 11-1 指定下载的应用程序的标识号是‘AP-4513’，则根据图 7 所示的数据实例，‘存储号’这一项并未给定数据。这表示相应的应用程序是一个被请求存储到寄存应用程序区 52R 中的应用程序。因此，所指定的应用程序被存储到寄存应用程序区 52R 中。

相反，如果移动终端 11-1 指定下载的应用程序的标识号是‘AP-3021’，则根据图 7 所示的数据实例，对应于该应用程序的‘存储号’项的值表示‘已删除’。这意味着相应的应用程序既未存储在临时保管应用程序区 52T 中，也没有存储在寄存应用程序区 52R 中。正如随后将在步骤 S523 所解释的，如果请求的应用程序是一个并未被请求存储到寄存应用程序区 52R 中的程序，那么在下载该应用程序时，该程序将从临时保管应用程序区 52T 中删除。因此，有一些应用程序是并不能在应用程序信息存储单元 52 中发现的，即使它们被寄存在准备下载应用程序区 53B 中。

在步骤 S507, 如果发现指定下载的应用程序并未存储到应用程序信息存储单元 52 中, 这与其标识号为 ‘AP-3021’ 的应用程序的情况一样, 那么管理服务器 16 将读出存储在寄存应用程序区 52R 中的数据, 并获得与该应用程序的标识号相对应的内容服务器 20-1 中的 URL, 以作为该应用程序的存储位置信息。随后, 管理服务器 16 请求内容服务器 20-1 发送该应用程序 (步骤 S508)。

如果指定下载的应用程序给定的可靠性指数为 ‘1’ 或者大于 ‘1’, 则在步骤 S508 之后, 内容服务器 20、鉴别服务器 17 和管理服务器 16 执行与 ‘针对管理服务器的应用程序发送操作 1’ 相同的一系列操作。相反, 如果指定下载的应用程序未给定可靠性指数 ‘1’ 或者大于 ‘1’, 则在步骤 S508 之后, 内容服务器 20、鉴别服务器 17 和管理服务器 16 执行与 ‘针对管理服务器的应用程序发送操作 2’ 相同的一系列操作。作为这一系列操作的结果, 管理服务器 16 获得该应用程序 (步骤 S509)。

接着, 管理服务器 16 把在步骤 S509 中获得的应用程序存储到临时保管应用程序区 52T 中 (步骤 S510)。

相反, 在步骤 S507 中, 如果发现指定下载的应用程序存储在应用程序信息存储单元 52 中, 这与其标识号为 ‘AP-4125’ 或 ‘AP-4513’ 的应用程序的情况一样, 那么管理服务器 16 将跳过从步骤 S508 到步骤 S510 的操作, 并前进到步骤 S511 的操作。

接着, 管理服务器 16 检验指定下载并存储到应用程序信息存储单元 52 中的应用程序是否加密 (步骤 S511)。如果指定下载的应用程序给定的可靠性指数为 ‘1’ 或者大于 ‘1’, 则存储在应用程序信息存储单元 52 中的应用程序未加密。如果指定下载的应用程序未给定可靠性指数为 ‘1’ 或者大于 ‘1’, 则存储在应用程序信息存储单元 52 中的应用程序使用移动终端 11-1 的公共密钥加密。

在步骤 S511, 如果存储在应用程序信息存储单元 52 中的指定应用程序未加密, 则管理服务器 16 请求鉴别服务器 17 发送 ‘PK-MT-1’, 即移动终端 11-1 的公共密钥 (步骤 S512)。通过响应发送公共密钥的请求, 鉴别服务器 17 把 ‘PK-MT-1’ 发送给管理服务器 16 (步骤 S513)。

在接收到 ‘PK-MT-1’ 之后, 管理服务器 16 联系应用程序信息,

该信息表示该应用程序存储到移动终端 11-1 的存储器 12 中的位置。而且，如果应用程序给定的可靠性指数为‘1’或者大于‘1’，那么管理服务器 16 也把该可靠性指数与该应用程序相联系。随后，管理服务器 16 使用‘PK-MT-1’加密该应用程序（步骤 S514）。如果该应用程序在从管理服务器 16 传输到移动终端 11-1 期间被窃取，那么由于此加密操作，该应用程序不会被未经许可的用户理解，并且也可防止未经许可使用该应用程序。

相反，在步骤 S511，如果存储在应用程序信息存储单元 52 中的指定应用程序被加密，则管理服务器 16 跳过从步骤 S512 到步骤 S514 的操作并移动到步骤 S515 的操作。

接着，管理服务器 16 使用‘SK-MS’即管理服务器 16 的专用密钥加密已加密的应用程序（步骤 S515）。由于该加密操作，移动终端 11-1 可确认该应用程序确实是由管理服务器 16 发送。这也就是说，这种加密起到了一个证明的作用，它能够使移动终端 11-1 确认该应用程序的发送侧。

管理服务器 16 把双重加密的应用程序发送到移动终端 11-1（步骤 S516）。

在接收到双重加密的应用程序之后，移动终端 11-1 向鉴别服务器 17 发送‘PK-MS’即管理服务器 16 的公共密钥的发送请求（步骤 S517）。通过响应该公共密钥的发送请求，鉴别服务器 17 向移动终端 11-1 发送‘PK-MS’（步骤 S518）。

在接收到‘PK-MS’之后，移动终端 11-1 使用‘PK-MS’解密双重加密的应用程序（步骤 S519）。如果该应用程序的解密失败，则意味着移动终端 11-1 接收的应用程序在传输期间被篡改，或者该应用程序由于某种原因而被破坏，或者该应用程序是由不是管理服务器 16 的服务器发送。因而，在这种情况下，移动终端 11-1 向管理服务器 16 发送合适的应用程序的重发请求。相反，如果使用‘PK-MS’的解密应用程序成功，则可以确认该应用程序是没有任何问题地从管理服务器 16 发送。因此，移动终端 11-1 使用‘SK-MT-1’即移动终端 11-1 的专用密钥再次解密该应用程序（步骤 S520）。

根据上面解释的操作，移动终端 11-1 获得未加密的应用程序和表示应用程序存储在移动终端 11-1 的存储器 12 中的位置。根据表示存

储应用程序的位置的信息，移动终端 11-1 把接收到的应用程序存储到应用程序区 41A 的应用程序区 40A 中（步骤 S521）。在步骤 S521，如果一个可靠性指数与接收的应用程序相联系，则移动终端 11-1 在该应用程序被存储时把该可靠性指数存储到相同的管理区 40 的可靠性信息区 40R 中。如果移动终端 11-1 的用户在步骤 S506 指定作为要删除的应用程序被存储在由该信息表示的区域中，则存储的应用程序被新下载的应用程序重写。随后，移动终端 11-1 向管理服务器 16 发送存储应用程序完成的通知（步骤 S522）。在步骤 S522 的操作之后，移动终端 11-1 显示屏幕 D26，它是由显示单元 21 使用的备用的常规屏幕。

10 在接收到存储应用程序完成的通知之后，管理服务器 16 按照下列方式更新用户信息存储单元 53 和应用程序信息存储单元 52 中的数据（步骤 S523）。如果通过上述操作从移动终端 11-1 的存储器 12 中删除任何应用程序，则管理服务器 16 将把寄存在下载应用程序区 53A 中的应用程序的信息移动到准备下载应用程序区 53B。管理服务器 16 把
15 新存储到存储器 12 中的应用程序的信息从准备下载应用程序区 53B 移动到下载应用程序区 53A 的相应位置上。而且，如果新存储的应用程序是一个临时存储到临时保管应用程序区 52T 中的应用程序，则管理服务器 16 从临时保管应用程序区 52T 中删除该应用程序。

[1.2.4] 应用程序的启动

20 如上所述，在移动终端 11 下载应用程序之后，在移动终端 11-1 的用户能够使用该应用程序之前，应用程序需要执行启动操作。

启动操作是管理服务器 16 允许移动终端 11-1 的存储控制器 35 使用下载应用程序的一系列操作。如果下载到移动终端 11-1 的存储器 12 的应用程序没有对其使用的限制，则应用程序的启动操作就在应用程序的下载操作之后执行。但是，如果应用程序有使用开始时间的特定
25 条件，则应用程序的启动操作并不在应用程序的下载之后立即执行，而是在开始使用时间之后执行。

例如，如果一个应用程序是在 3 月 15 日购买，移动终端 11-1 在 3 月 20 日下载，但其在某种形式的公共传输上的月票（commuter
30 ticket）的购买是在 4 月 1 日开始有效的，那么该应用程序不能在 3 月 20 日至 3 月 31 日之间使用，即使该应用程序本身存储在了移动终端 11-1 的存储器 12 中。在日期从 3 月 31 到 4 月 1 日转换的时刻，该

应用程序的启动操作被执行，并且移动终端 11-1 的用户能够使用该应用程序。

5 由于下载操作与启动操作是彼此分开的，因此从应用程序的使用有效期来说，移动终端 11-1 的用户可以无任何限制地在他/她方便的时候下载应用程序。从另一种观点来看，如果移动终端 11-1 的许多用户需要下载其使用有效期开始于同一天的应用程序并且这些用户需要
10 在同一天下载应用程序，那么因为大量的用户正试图在短时间内下载该应用程序，则在管理服务器 16、内容服务器 20 和移动终端 11-1 的任何两者之间的通信信道上很容易出现网络拥堵。但是，因为由启动操作引起的数据通信量的大小通常远小于由于应用程序的下载操作引起的数据通信量的大小，因此，如果移动终端 11 的每个用户在应用程序执行启动操作之前的任何方便的时候下载该应用程序，则可以减少在上述有效期的开始之日发生网络拥堵的可能性。下面解释启动操作的流程。

15 下面的例子是启动操作被执行的一些情况。启动操作在未限制使用有效期的应用程序下载到移动终端 11-1 时执行。启动操作还在已经下载到移动终端 11-1 的应用程序的使用有效期开始的时候执行。而且，启动操作也在应用程序的内容服务器 20 命令管理服务器 16 执行启动操作时执行。下文的例子将解释当存储在移动终端 11-1 的管理区
20 40-1 中的应用程序执行启动操作时执行的操作流程。

首先，管理服务器 16 把启动命令发送给移动终端 11-1。该启动命令包括存储器 12 中的管理区 40-1 的标识号，它将用于规定要被启动的应用程序。

25 在移动终端 11-1 的通信单元 34 接收到启动命令之后，通信单元 34 把该命令转送到存储控制器 35。直到存储控制器 35 接收到该启动命令，存储控制器 35 才会接受由移动终端 11-1 的控制单元 31 发出的允许使用应用程序区 40A-1 中的应用程序的功能或者数据区 40D-1 中的数据的请求。因此，直到接收到该启动命令，移动终端 11-1 的用户才会使用存储在管理区 40-1 中的应用程序。

30 在存储控制器 35 接收到启动命令之后，如果存储控制器 35 接收到来自控制单元 31 的允许使用应用程序区 40A-1 中的应用程序的功能或者数据区 40D-1 中的数据的请求，则存储控制器 35 读出存储在管理

区 40-1 的可靠性信息区 40R-1 中的可靠性指数。接着，存储控制器 35 把从控制单元 31 与允许使用的请求一起发送的请求程序的可靠性指数与从可靠性信息区 40R-1 读出的可靠性指数进行比较。只有当请求程序的可靠性指数大于或等于从可靠性信息区 40R-1 读出的可靠性指数时，存储控制器 35 才接受该请求并根据该允许使用的请求执行适当的操作。存储控制器 35 使用可靠性指数的这种控制操作在前面关于移动终端 11 的配置的部分中已经作出了解释。

在向移动终端 11-1 发送启动命令之后，管理服务器 16 把用户信息存储单元 53-1 的下载应用程序区 53A 中的‘启动’项的值更新为‘是’。随后，管理服务器 16 读出存储在寄存应用程序区 52R 中的数据，而且，如果与要启动的应用程序相对应的‘使用费征收’项的值为‘是’，则管理服务器 16 向费用管理服务器发送该应用程序的信息，如该应用程序的标识号、移动终端 11-1 的标识号和启动操作的日期和时间等。

同时，当移动终端 11-1 接收到启动命令时，如图 26 的屏幕 31 所示，移动终端 11-1 由显示单元 21 显示字母‘a’，用以通知移动终端 11-1 的用户现在有一个新的可用应用程序。字母‘a’可用另一个字母如‘β’替换，以便与上述的应用程序购买操作中的完成通知相区别。这个通知也可通过显示图像、发声、振动移动终端等来告知。

前面段落中解释的是启动操作。在启动操作之后，如果移动终端 11-1 的用户想要开始已经启动的操作，则移动终端 11-1 的用户按动 appli 按钮 23 以使移动终端 11-1 显示应用程序菜单（屏幕 32）。接着，移动终端 11-1 的用户按动按钮‘3’以指定‘3. 应用程序的开始’这一项，并且移动终端 11-1 显示用于从可用应用程序中选择一个应用程序的屏幕（屏幕 D33）。当选择应用程序的屏幕被显示时，如果移动终端 11-1 的用户按动按钮‘1’以选择‘1. 时间表管理器 Ver. 2’这一项，则所选应用程序变为可操作（屏幕 D34）。

[1.2.5] 应用程序的去启动

在移动终端 11-1 中的应用程序执行启动操作之后，可能会有需要中断应用程序的使用的情况。例如，如果移动终端 11-1 丢失或被盗，根据来自移动终端 11-1 的用户的请求，存储在移动终端 11-1 中的任何应用程序的使用都应当被临时中断。如果应用程序使用费的支付额

不足，或者应用程序的使用条件被移动终端 11-1 的用户破坏，那么存储在移动终端 11-1 中的特定应用程序的使用应当根据来自内容服务器 20-1 的管理实体或者管理服务器 16 的请求而临时中断。

在上述情况下，去启动操作被执行。下面的例子解释当存储在移动终端 11-1 的管理区 40-1 中的应用程序执行去启动操作时所执行的
5 操作流程。

首先，管理服务器 16 把去启动命令发送给移动终端 11-1。该去启动命令包括存储器 12 中的管理区 40-1 的标识号，它将用于规定要被去启动的应用程序。

10 在移动终端 11-1 的通信单元 34 接收到去启动命令之后，通信单元 34 把该命令转送到存储控制器 35。在存储控制器 35 接收到该去启动命令之后，存储控制器 35 拒绝由移动终端 11-1 的控制单元 31 发出的允许使用应用程序区 40A-1 中的应用程序的功能或者数据区 40D-1 中的数据的所有请求。结果，移动终端 11-1 的用户不能使用存储在管
15 理区 40-1 中的应用程序。

在向移动终端 11-1 发送去启动命令之后，管理服务器 16 把用户信息存储单元 53-1 的下载应用程序区 53A 中的‘启动’项的值更新为‘否’。随后，管理服务器 16 读出存储在寄存应用程序区 52R 中的数据，而且，如果与要被去启动的应用程序相对应的‘使用费征收’项
20 的值为‘是’，则管理服务器 16 向费用管理服务器发送有关该应用程序的信息，如该应用程序的标识号、移动终端 11-1 的标识号和去启动操作的日期和时间等。

前面段落中解释的是去启动操作。在接收到去启动命令之后，移动终端 11-1 将不在用于从可用应用程序中选择一个应用程序的屏幕上
25 显示相应的应用程序的名字。如果移动终端 11-1 的用户需要再次使用要执行去启动操作的应用程序，则该应用程序需要执行上面解释的去启动操作。例如，当丢失的移动终端 11-1 找到后或者当应用程序使用费不足的问题得到解决后，启动操作将被再次执行，但下载并存储到移动终端 11-1 的存储器 12 中的应用程序和由这些应用程序管理的数
30 据将在执行去启动操作时再次变为可用。

[1.2.6] 应用程序的删除

有一些情况需要永久停止移动终端 11-1 中的应用程序的使用。例

如，如果移动终端 11-1 的用户决定取消应用程序的购买合同，则该应用程序的使用应当永久停止。相同的情况，当一个应用程序的使用有效期到期时，或者当移动终端 11-1 的用户严重破坏了应用程序的使用条件时，应用程序的使用也应当永久停止。在这些情况下，该应用程序应当从移动终端 11-1 的存储器 12 中删除，同时，寄存在用户信息存储单元 53-1 的准备下载应用程序区 53B 中的所删除应用程序的信息也被删除。下面的例子是当存储在移动终端 11-1 的管理区 40-1 中的应用程序执行删除操作时所执行的操作流程。

首先，管理服务器 16 读出存储在用户信息存储单元 53-1 的下载应用程序区 53A 中的数据，并检验要被删除的应用程序是否存储在移动终端 11-1 的存储器 12 中。如果该应用程序存储在移动终端 11-1 的存储器 12 中，则管理服务器 16 向移动终端 11-1 发送一个删除命令。该删除命令包含管理区 40-1 的标识号，它将规定必须要删除的应用程序。在接收到删除命令之后，移动终端 11-1 的通信单元 34 将该命令传送给存储控制器 35。当存储控制器 35 接收到该删除命令时，存储控制器 35 将删除该应用程序以及由该标识号指定的管理区 40-1 中的应用程序的数据。在删除操作之后，移动终端 11-1 的存储控制器 35 把删除完成的通知发送给管理服务器 16。当管理服务器 16 接收到删除完成通知时，管理服务器 16 删除从用户信息存储单元 53-1 的下载应用程序区 53A 的关于该应用程序的信息。

相反，如果要删除的应用程序并未存储到移动终端 11-1 的存储器 12 中，管理服务器 16 将从用户信息存储单元 53-1 的准备下载应用程序区 53B 中删除关于该应用程序的信息。

接着，管理服务器 16 读出存储在寄存应用程序区 52R 中的数据，并且，如果该应用程序的‘使用费征收’项的值是‘是’，则管理服务器 16 向费用管理服务器发送关于该应用程序的信息，如该应用程序的标识号、移动终端 11-1 的标识号、删除操作的日期和时间等。

以上段落解释的是删除操作。在删除操作之后，移动终端 11-1 不在用于选择开始和下载的应用程序的屏幕上显示相应的应用程序的名称。

[1.3] 使用可靠性指数的应用程序之间的协调操作

在下面的描述中，将使用实例来解释一种使用多个应用程序的可

可靠性指数来协调它们的操作的方法。

正如已经描述的，多个应用程序被存储在移动终端 11-1 的存储器 12 中，并且存储在管理区 40 中的每个应用程序给定从整数 ‘1’ 到 ‘5’ 的一个可靠性指数。另外，可靠性指数被记录到可靠性信息区 40R 中。

5 可靠性指数的值越大，应用程序的可靠性越高。高可靠性的应用程序可使用可靠性低的应用程序的功能和数据。相反，低可靠性的应用程序不能使用高可靠性应用程序的功能或数据。由移动终端 11-1 的控制单元 31 管理并存储在控制存储器 32 中的控制程序给定的可靠性指数为 ‘5’。至于存储在自由区 41 中的应用程序，没有记录可靠性指数，

10 并且当存储在自由区 41 中的应用程序的可靠性和另一个程序的可靠性需要彼此比较时，存储在自由区 41 中的应用程序的可靠性指数采用 ‘0’，

[1.3.1] 不允许应用程序的协调操作的情况

下面的例子是较小可靠性指数的应用程序不能使用较大可靠性指数的应用程序的功能或数据的情况。图 27、图 28、图 29、图 30 和图 31 表示出了这个例子。

15

在移动终端 11-1 的管理区 40-1 的应用程序区 40A 中，存储了购买某种形式的公共交通月票的应用程序（下文中称其为 ‘通行 (pass) 应用程序’）。该通行应用程序已经执行了启动操作，并且该通行应用程序在购买时可以很容易地被使用。通过使用该通行应用程序，移动终端 11-1 的用户可以打开 ‘abc 铁路公司’ 的主页，通过该主页，用户可购买一张月票，并且获得其它相关信息，如时刻表等。如果移动终端 11-1 的用户通过上述通行应用程序购买了一张月票，那么该月票将以移动终端发送给 ‘abc 铁路公司’ 的检票机的无线电信号的形式起作用，通过响应检票口的机器发出的相应的无线电波信号，如果两个无线电信号匹配，那么移动终端的用户接近检票门时，该检票门将自动打开。也就是说，移动终端 11-1 本身起到了月票的作用。在本例中，通行应用程序的可靠性指数为 ‘3’。

20

25

在管理区 40-2 的应用程序区 40A 中，存储了可执行付费功能的应用程序（以下称作付费应用程序）。该付费应用程序已经执行了启动操作，并且该付费应用程序可以很容易地被使用。通过使用该付费应用程序，移动终端 11-1 的用户可打开 ‘xx 银行’ 的主页，在该主页中，

30

用户可以把钱从他/她的帐户汇至另一个帐户。付费应用程序的可靠性指数是‘5’。

移动终端 11-1 的用户按动 appli 按钮 23 以使移动终端 11-1 在显示单元 21 上显示应用程序菜单（屏幕 D41）。接着，当显示屏幕 D41 时，用户按动按钮‘3’以使移动终端 11-1 显示用于选择开始应用程序的屏幕（屏幕 D42）。当显示屏幕 D42 时，用户按动按钮‘1’并选择通行应用程序。移动终端 11-1 开始该通行应用程序，并且该通行应用程序打开‘abc 铁路公司’的主页（屏幕 D43）。

当显示屏幕 D43 时，用户按动按钮‘3’以选择‘3. 月票的购买’这一项，而且移动终端 11-1 显示屏幕 D44。在屏幕 D44 中，用户使用操作单元 21 输入有关所希望的月票使用区域和使用期限的数据，并且按动按钮‘9’以把购买月票的指令发送到‘abc 铁路公司’的主页。

随后，通行应用程序搜索移动终端 11-1 的存储器 12 中可如下所述支付费用的应用程序。执行通行应用程序的控制单元 31 向存储控制器 35 发送读出存储在不包含管理区 40-1 的管理区 40 和自由区 41 中的应用程序以及管理区 40-1 的标识号的请求。

当存储控制器 35 接收到控制单元 31 的读出管理区 40 和自由区 41 中的应用程序的请求时，通过使用从控制单元 31 与该请求一起接收的管理区 40-1 的标识信息，存储控制器 35 从管理区 40-1 的可靠性信息区 40R 中读出可靠性指数。在这种情况下，该可靠性指数为‘3’。这个可靠性指数在下文中将被称作‘请求应用程序的可靠性指数’。

接着，当被请求读出的应用程序存储到下面的这些区域中时，存储控制器 35 将从管理区 40-2，管理区 40-3，...，和管理区 40-n 的可靠性信息区 40R 中读出可靠性指数。但是，对于自由区 40-1，自由区 40-2，...，自由区 40-m 来说，采用可靠性指数‘0’作为这些区域中的应用程序的可靠性指数，这是因为并未向它们指定可靠性指数。通过此操作获得的可靠性指数在下文中将被称作‘被请求应用程序的可靠性指数’。

接着，存储控制器 35 把请求应用程序的可靠性指数与被请求应用程序的每个可靠性指数进行比较。如果请求应用程序的可靠性指数大于或等于被请求应用程序的可靠性指数，也就是说，如果被请求应用程序的可靠性指数是‘3’或小于‘3’，则存储控制器 35 根据该请求

读出并发送被请求的应用程序给控制单元 31。否则，存储控制器 35 将向控制单元 31 发出拒绝通知。

在本例中，可支付费用的付费应用程序存储在管理区 40-2 中，但管理区 40-2 的被请求应用程序的可靠性指数是‘5’。因此，存储控制器 35 拒绝通行应用程序读出付费应用程序的请求。结果，通行应用程序不能识别出付费应用程序的存在。因此，通行应用程序在存储器 12 中不能找到可付费的应用程序，因而移动终端 11-1 将显示屏幕 D45。在屏幕 D45 中，用户被请求自己完成汇款。用户在一张纸上写下屏幕 D45 上所显示的信息，并按动按钮‘9’退出通行应用程序。结果，显示单元 21 将显示如屏幕 D46 所示的常规屏幕。

当显示屏幕 D46 时，用户按动 appli 按钮 23 以使移动终端 11-1 显示应用程序菜单(屏幕 D47)。当显示屏幕 D47 时，用户按动按钮‘3’以使移动终端 11-1 显示用于选择开始应用程序的屏幕(屏幕 D48)。当显示屏幕 D48 时，用户按动按钮‘2’并选择付费应用程序。随后，移动终端 11-1 开始该付费应用程序，并打开‘xx 银行’的主页(屏幕 D49)。

在屏幕 D49 中，用户输入一个密码，并使移动终端 11-1 显示用于选择一个操作的屏幕(屏幕 D50)。当显示屏幕 D50 时，用户按动按钮‘3’以选择‘3. 汇款’项，并显示屏幕 D51。在屏幕 D51 中，用户输入汇款至用户写下的‘abc 铁路公司’的信息，并按动按钮‘9’以把汇单发送到‘xx 银行’的主页。‘xx 银行’通过主页接收移动终端 11-1 的汇单，并根据该汇单向‘abc 铁路公司’的指定帐户汇款。随后，移动终端 11-1 的显示单元 21 显示屏幕 D52。另一方面，‘abc 铁路公司’确认‘xx 银行’的汇款，并完成移动终端 11-1 购买月票的操作，从而更新移动终端 11-1 的购买历史信息。

当显示屏幕 D52 时，按钮‘9’被按动并且移动终端 11-1 显示如屏幕 D53 所示的备用的常规屏幕。当显示屏幕 D53 时，用户再次按动 appli 按钮 23 以使移动终端 11-1 显示应用程序菜单(屏幕 D54)。当显示屏幕 D54 时，用户按动按钮‘3’以使移动终端 11-1 显示用于选择开始应用程序的屏幕(屏幕 D55)。当显示屏幕 D55 时，用户按动按钮‘1’以开始通行应用程序(屏幕 D56)。

当显示屏幕 D56 时，如果用户按动按钮‘4’以选择‘4. 购买历史

的参考’项，则移动终端 11-1 显示屏幕 D57。当显示屏幕 D57 时，如果用户按动按钮 ‘1’，则移动终端 11-1 显示有关购买月票状态的详细信息（屏幕 D58）。在屏幕 D58 中，用户可确认购买月票的汇款已经得到 ‘abc 铁路公司’ 的确认，并且购买月票的操作已经成功完成。随后，用户按动按钮 ‘9’，而且，移动终端 11-1 在显示单元 21 上显示屏幕 D59 所示的常规屏幕。

[1.3.2] 允许应用程序协调操作的情况

下面的例子描述了较高或相同可靠性指数的应用程序可以使用较低或相同可靠性指数的应用程序的功能或数据的情况。图 32、图 33 和图 34 示出了这个例子。

移动终端 11-1 的管理区 40-1 的应用程序区 40A 中存储了可起到邮购作用的应用程序（以下称作 ‘邮购应用程序’）。该邮购应用程序已经执行了启动操作，并且该邮购应用程序现在可以被很容易地使用。通过使用邮购应用程序，移动终端 11-1 的用户可打开 ‘Cyber Shop zz’ 的主页，在该主页中，用户可购买各种类型的商品。邮购应用程序的可靠性指数是 ‘4’。

与前面例子中的情况一样，管理区 40-2 的应用程序区 40A 存储了付费应用程序。付费应用程序已经执行了启动操作，并且该付费应用程序现在备用。该付费应用程序在下文中将被称作 ‘付费应用程序 1’。付费应用程序 1 的可靠性指数是 ‘4’。

在管理区 40-3 的应用程序区 40A 中，存储了用信用卡执行付费功能的应用程序（下文称作 ‘信用卡应用程序’）。该信用卡应用程序已经执行了启动操作，并且该信用卡应用程序现在备用。通过使用该信用卡应用程序，移动终端 11-1 的用户可打开 ‘cc 信用卡公司’ 的主页，在该主页上，用户可用信用卡付费。信用卡应用程序的可靠性指数是 ‘4’。

管理区 40-4 的应用程序区 40A 存储了起到付费应用程序 1 的相同功能的应用程序。该应用程序打开 ‘kk 银行’ 而不是 ‘xx 银行’ 的主页，在该主页上，用户可以命令几个操作，如汇款。该应用程序已经执行了启动操作，并且该应用程序现在待用。在下文中，付费应用程序将被称作 ‘付费应用程序 2’。付费应用程序 1 的可靠性指数为 ‘5’。

首先，移动终端 11-1 的用户按动 appli 按钮 23 以使显示单元 21

显示应用程序菜单(屏幕 D71)。当显示屏幕 D71 时,用户按动按钮‘3’以使移动终端 11-1 显示用于选择开始应用程序的屏幕(屏幕 D72)。当显示屏幕 D72 时,用户按动按钮‘1’并选择邮购应用程序。移动终端 11-1 开始该邮购应用程序,并且邮购应用程序打开‘Cyber Shop zz’的主页(屏幕 D73)。

当显示屏幕 D73 时,如果用户按动按钮‘2’选择买牛肉,则邮购应用程序显示用于输入所订商品的发送目的地信息的屏幕(屏幕 D74)。在屏幕 D74 上,用户输入所订商品的发送目的地的信息,并按动按钮‘9’。随后,邮购应用程序在移动终端 11-1 的存储器 12 中搜索可付费的应用程序。在下面的例子中,假设用户输入‘1-1-1 Shinjyuku-ku, Tokyo’作为发送目的地。在这种情况下,搜索可付费的应用程序的操作流程与上面关于通行应用程序的操作流程相同。

在搜索可付费应用程序的操作中,读出存储器 12 中的其它应用程序的请求的请求侧的邮购应用程序的可靠性指数是‘4’。由于作为读出应用程序请求的接收侧之一的付费应用程序 1 的可靠性指数是‘4’,所以存储控制器 35 接受邮购应用程序能够读出付费应用程序 1 的请求,并把有关执行邮购应用程序的付费应用程序 1 的功能的信息发送给控制单元 31。类似地,由于信用卡应用程序的可靠性指数也是‘4’,因此存储控制器 35 把有关信用卡应用程序的功能的信息发送给控制单元 31。相反,付费应用程序 2 的可靠性指数是‘5’,它大于请求侧的邮购应用程序的可靠性指数‘4’。因此,存储控制器 35 拒绝控制单元 31 读出付费应用程序 2 的请求,并且有关付费应用程序 2 的功能的信息也不发送到邮购应用程序。结果,邮购应用程序认识到付费应用程序 1 和信用卡应用程序可被用作付费的应用程序,并显示屏幕 D75。

在屏幕 D75 上,如果用户决定使用付费应用程序 1 付费,并按动按钮‘1’,则邮购应用程序把允许读出付费应用程序的请求发送到存储控制器 35。同时,邮购应用程序向付费应用程序 1 提供一个应当由付费应用程序 1 执行的事务命令和执行该事务的必要信息。更具体来说,执行邮购应用程序的控制单元 31 请求存储控制器 35 写下要被执行的汇款操作单,以及在分配给付费应用程序 1 的管理区 40-2 的数据区 40D-2 中的汇款操作的必要信息。汇款信息包括如下信息:数额是 5,000 日元,收款人是‘Cyber Shop xx’,接收帐户是‘nn 银行’。

中帐号为‘41256378’的储蓄帐户，目的是支付1公斤牛肉的费用，而且商品发送目的地是‘1-1-1 Shinjyuku-ku, Tokyo’。

存储控制器35把读请求和写请求的请求应用程序的可靠性指数与这些请求的被请求应用程序的可靠性指数进行比较，并接受这些请求。结果，控制单元31执行付费应用程序1。

随后，通过显示屏幕D76，付费应用程序1请求移动终端11-1的用户输入鉴别个人标识的密码。在屏幕D76中，如果移动终端11-1的用户输入正确的密码，则付费应用程序1显示屏幕D77。在这个步骤中，汇款的必要信息由付费应用程序1从管理区40-2的数据区40D-2中读出，并且该信息已输入到屏幕D77中。因此，用户不需要输入此信息。

当显示屏幕D77时，用户确认汇款信息，并按动按钮‘9’。随后，付款应用程序1把汇单发送到‘xx银行’的主页。在这一步骤中，付费应用程序1还向‘xx银行’的主页发送汇款的必要信息，如所购商品的信息、所购商品的发送目的地等。

当‘xx银行’通过主页接收到来自移动终端11-1的汇单、所购商品的信息、所购商品的发送目的地等时，‘xx银行’把指定的费用与所购商品的信息、所购商品的发送目的地等一起汇至‘Cyber Shop zz’。‘Cyber Shop zz’确认‘xx银行’的汇款，并被告知1kg牛肉预订发送到‘1-1-1 Shinjyuku-ku, Tokyo’。结果，‘Cyber Shop zz’进行所购商品的发送操作，并向移动终端11-1发送购物付费的确认，以及诸如发货日期及订货号等的信息。

当由移动终端11-1的控制单元31执行的付费应用程序1接收到‘Cyber Shop zz’的付费确认信息时，付费应用程序1向存储控制器35发送执行呼叫付费应用程序1的邮购应用程序的请求，以及把诸如发货日期和订货号这样的信息写入邮购应用程序所管理的数据区40D-1中的请求。在这一步骤中，存储控制器35还把请求应用程序的可靠性指数与被请求应用程序的可靠性指数进行比较，并接受这些请求。结果，控制单元31开始邮购应用程序，该邮购应用程序在一系列操作的中间关闭，并且邮购应用程序在从数据区40D-1读出发货日期和订货号之后显示屏幕D78。当显示屏幕D78时，用户确认从‘Cyber Shop zz’发出的信息，并按动按钮‘9’。随后，移动终端11-1结束该操

作并显示屏幕 D79 所示的常规屏幕。

如上所述，给定高可靠性值的应用程序被允许从其它应用程序直接获得诸如财政信息和个人信息的高位值信息，并被允许呼叫管理高位值信息的其它应用程序的功能。而且，如果一个应用程序的可靠性指数是‘5’，则该应用程序被允许呼叫存储在控制存储器 32 中的控制应用程序，并允许使用由控制程序管理的数据。结果，用户必须执行的操作可被简化。至于已经解释的信息安全，只有经过管理服务器 16 的管理实体检查的应用程序才被给定高可靠性值，而且，管理服务器 16 的管理实体在必要时检验给定高可靠性值的应用程序是否被篡改。因此，在使用具有高位值信息的应用程序时，可以保证用户的安全。

[2] 第二实施例

正如下面将要解释的，第一和第二实施例的不同之处仅仅在于在第二实施例中，使用可靠性相关信息代替可靠性指数来用于协调操作。总的来说，第二实施例的特征与第一实施例的特征相同，因而在此只描述两个实施例的不同方面。在下面解释中，用于第一实施例中的各个部分的名称和符号将没有任何变化地用于第二实施例的所有相应的部分中。

[2.1] 特许数据的配置和功能

在第二实施例，当管理服务器 16 的管理实体被请求检查内容服务器 20 的应用程序时，根据新检查的应用程序和在过去检查的每个应用程序，管理服务器 16 的管理实体确定读取应用程序的权利、读取数据的权利、编辑数据的权利和删除数据的权利。

下面是表示新近检查其标识号为‘AP-3568’的应用程序的例子。该应用程序将被称作‘应用程序 AP-3568’，同样方式，其它应用程序也以它们的标识号来称呼。图 35 给出了表示应用程序‘AP-3568’权利的数据的例子，并且在下文中将被称作‘特许数据’。

图 35 的第一列中的数据表示被允许由应用程序‘AP-3568’读出的应用程序。例如，当应用程序‘AP-3568’正在执行时，如果控制单元 31 需要使用应用程序‘AP-3712’的任何功能，则控制单元 31 向存储控制器 35 发送允许读出应用程序‘AP-3712’的请求。应用程序‘AP-3712’被表示在应用程序‘AP-3568’的特许数据的第一列中。

根据该数据，存储控制器 35 在其接收到允许读出应用程序 ‘AP-3712’ 的请求时接受该请求。在接受该请求之后，存储控制器 35 从管理区 40 的应用程序区 40A 中读出应用程序 ‘AP-3712’，并将其发送至控制单元 31。

- 5 图 35 的第二列中的数据表示应用程序 ‘AP-3568’ 被允许读出其数据的应用程序。例如，如果控制单元 31 在应用程序 ‘AP-3568’ 正在执行时需要使用应用程序 ‘AP-8125’ 的任何数据，则控制单元 31 向存储控制器 35 发送允许读出应用程序 ‘AP-8125’ 的数据的请求。应用程序 ‘AP-8125’ 被表示在应用程序 ‘AP-3568’ 的特许数据的第
10 二列中。根据该数据，当存储控制器 35 接收到允许读出应用程序 ‘AP-8125’ 的数据的请求时接受该请求。在接受允许读出该数据的请求之后，存储控制器 35 从存储了应用程序 ‘AP-8125’ 的管理区 40 的数据区 40D 中读出被请求的数据，并将该数据发送到控制单元 31。

- 图 35 的第三列中的数据表示应用程序 ‘AP-3568’ 被允许编辑其
15 数据的应用程序，并且图 35 的第四列中的数据表示应用程序 ‘AP-3568’ 被允许删除其数据的应用程序。

- 相反，图 35 的第五列中的数据表示被允许读出应用程序 ‘AP-3568’ 的应用程序。例如，如果控制单元 31 在应用程序 ‘AP-4315’ 正在执行时需要使用应用程序 ‘AP-3568’ 的任何功能，则控制单元 31
20 向存储控制器 35 发送允许读出应用程序 ‘AP-3568’ 的请求。应用程序 ‘AP-4315’ 被表示在应用程序 ‘AP-3568’ 的特许数据的第五列中。根据该数据，当存储控制器 35 接收到允许读出应用程序 ‘AP-3568’ 的请求时接受该请求。在接受该请求之后，存储控制器 35 从管理区 40 的应用程序区 40A 中读出应用程序 ‘AP-3568’，并将其发送到控制单元
25 31。

 类似地，图 35 的第六列中的数据表示被允许读出应用程序 ‘AP-3568’ 的数据的应用程序；图 35 的第七列中的数据表示被允许编辑应用程序 ‘AP-3568’ 的数据的应用程序；并且图 35 的第八列中的数据表示被允许删除应用程序 ‘AP-3568’ 的数据的应用程序。

- 30 [2.2] 可靠性相关信息的寄存和更新

 如图 36 所示，管理服务器 16 的应用程序信息存储单元 52 的寄存应用程序区 52R 具有 ‘可靠性相关信息’ 这一项，而不是如第一实施

例的‘可靠性指数’这一项。当管理服务器 16 的管理实体完成应用程序‘AP-3568’的检查时，它把图 35 所示的特许数据输入到管理服务器 16 中。在特许数据被输入到管理服务器 16 中之后，管理服务器 16 在寄存应用程序区 52R 中产生应用程序‘AP-3568’的新记录，并
5 把特许数据的第五、第六、第七和第八列中的数据存储到新记录的‘可靠性相关信息’项中。

接着，管理服务器 16 更新与在从特许数据的第一列到第四列的任何一列中表示的应用程序相对应的‘可靠性相关信息’项中的数据。例如，由于应用程序‘AP-3712’被表示在应用程序‘AP-3568’的特
10 许数据的第一列中，所以管理服务器 16 把应用程序‘AP-3568’的标识号添加到与寄存应用程序区 52R 中的应用程序‘AP-3712’相对应的记录的‘可靠性相关信息’项中的‘读出应用程序’子项中。

接着，管理服务器 16 读出用户信息存储单元 53-1、用户信息存储单元 53-2，...，和用户信息存储单元 53-k 中的每一个的下载应用程序
15 区 53A 中的数据。随后，从应用程序‘AP-3568’的特许数据的第一列到第四列的每一列开始，管理服务器 16 列出了其‘可靠性相关信息’项的数据在上述操作中被更新的所有用户信息存储单元 53。换言之，管理服务器 16 列出了包含应用程序‘AP-3568’的特许数据中表示的应用程序标识号的所有用户信息存储单元 53。随后，管理服务器 16
20 把应用程序‘AP-3568’的标识号添加到列出的用户信息存储单元 53 的‘可靠性相关信息’项的相应子项中。随后，管理服务器 16 把应用程序‘AP-3568’的标识号被加到‘可靠性相关信息’项的通知发送到与增加了应用程序‘AP-3568’的标识号的用户信息存储单元 53 相对应的移动终端 11-1 中。例如，根据图 7 所示的用户信息存储单元 53-
25 1 的数据，移动终端 11-1 把应用程序‘AP-0123’存储到存储器 12 的管理区 40-2 的应用程序区 40A-2 中。应用程序‘AP-0123’被表示在图 35 所示的特许数据的第一列中，并且新检查的应用程序‘AP-3568’被给予了读出应用程序‘AP-0123’的权利。因此，管理服务器 16 向移动终端 11-1 发送应用程序‘AP-3568’的标识号新近进入到与用户
30 信息存储单元 53-1 中的应用程序‘AP-0123’对应的‘可靠性相关信息’项的‘读出应用程序’子项中的通知。

当移动终端 11 把经过了其内容检查的应用程序下载到存储器 12

中时，与该应用程序相对应的可靠性相关信息也与该应用程序一起下载到移动终端 11 中。移动终端 11 的存储控制器 35 把与应用程序一起下载的可靠性相关信息记录到分配给该应用程序的管理区 40 的可靠性信息区 40R 中。

- 5 正如在前面的例子中所述的，当移动终端 11-1 接收到管理服务器 16 的应用程序 ‘AP-3568’ 的标识号已经新近进入到与应用程序 ‘AP-0123’ 对应的用户信息存储单元 53-1 的 ‘可靠性相关信息’ 项的 ‘读出应用程序’ 子项中的通知时，移动终端 11-1 的存储控制器 35 包括存储在分配给应用程序 ‘AP-0123’ 的管理区 40-2 的可靠性信息区 40R-2 中的 ‘读出应用程序’ 项中的应用程序 ‘AP-3568’ 的标识号。

10 根据上述操作，存储在应用程序信息存储单元 52 的寄存应用程序区 52R 中的数据和记录在每个移动终端 11 的管理区 40 的可靠性信息区 40R 中的数据总是被更新，并且只保留新数据。

[2.3] 使用可靠性相关信息的应用程序之间的协调操作

- 15 当一个应用程序需要使用移动终端 11 中的另一个应用程序的功能或数据时，控制单元 31 向存储控制器 35 发送允许使用该应用程序或者该应用程序的数据的请求、存储被请求应用程序的存储区的标识号（下文中称作 ‘被请求应用程序的区号’）以及进行请求的应用程序的标识号。

- 20 如果由被请求应用程序区号指定的存储区是管理区 40 的存储区之一，则存储控制器 35 在接收到来自控制单元 31 的请求时将从分配给被请求应用程序的管理区 40 的可靠性信息区 40R 中读出可靠性相关信息。接着，存储控制器 35 检验请求应用程序的标识号是否包含在与可靠性相关信息中的请求内容相对应的项目中。例如，如果正在执行应用程序 ‘AP-2568’ 的控制单元 31 向存储控制器 35 发送允许读取存储在应用程序区 40A-2 中的应用程序 ‘AP-0123’ 的请求，则存储控制器 35 从可靠性信息区 40R-2 中读出可靠性相关信息，并检验应用程序 ‘AP-2568’ 的标识号是否包含在可靠性相关信息的 ‘读出应用程序’ 项中。如果请求应用程序的标识号包含在相应项中，则存储控制器 35 接受控制单元 31 的请求，并根据该请求执行操作。相反，如果请求应用程序的标识号未包含在 ‘读出应用程序’ 项中，存储控制器 35 将拒绝控制单元 31 的请求。
- 25
- 30

根据如上所述使用可靠性相关信息执行的存储控制器 35 的操作，应用程序之间的协调操作可以得到灵活地管理。

[3] 第三实施例

在第三实施例中，发送应用程序的操作流程不同于第一实施例的操作流程，但第三实施例的大部分特征与第一实施例相同。因此，以下的描述将仅仅涉及第三实施例与第一实施例的不同之处；而用于第一实施例的各部分名称和符号将会没有任何变化地应用到第三实施例中。

[3.1] 应用程序发送系统的总配置

在第三实施例中，与第一实施例中的情况一样，当内容服务器 20 的管理实体请求检查一个应用程序时，该应用程序将由管理服务器 16 的管理实体检查，并把一个可靠性指数给定该应用程序。但是，在第三实施例中，在把可靠性指数指定给应用程序之后，管理服务器 16 的管理实体将使用散列函数产生该应用程序的信息摘要。由原始数据组使用散列函数产生的数据组是不可逆的，所以应用程序不能通过该应用程序的信息摘要得到恢复。但是，通过具有不同内容的应用程序产生相同的信息摘要几乎是不可能的，这是因为每个应用程序的内容几乎必定是不同的，尽管有时候差别是细微的。因此，如果一个应用程序的内容的任何一部分发生变化，那么通过使用散列函数由原始应用程序产生的信息摘要以及使用相同的散列函数由变化后的应用程序产生的信息摘要将是不同的。由于信息摘要的尺寸通常远远小于与该信息摘要相对应的应用程序的尺寸，因此，信息摘要不需要大的存储空间并且可以快速传输。管理服务器 16 的管理实体把产生的信息摘要与该应用程序的可靠性指数一起存储到应用程序信息存储单元 52 中。图 37 表示在第三实施例中存储到应用程序信息存储单元 52 中的数据实例。但是，图 37 未示出‘公布’项，这是因为在第三实施例中，管理服务器 16 不向移动终端 11 公布有关给定可靠性指数的应用程序的信息。

而且，在第三实施例中，与第一实施例的情况一样，应用程序本身并不存储到应用程序信息存储单元 52 中，但它们存储在作为应用程序提供者的内容服务器 20 中。因此，在图 37 所示的数据格式中，在‘存储位置信息’项中未列出应用程序，而仅存储了表示每个应用程

序的存储位置的 URL。

另外，在第三实施例中，作为应用程序提供者的内容服务器 20 总是把它们的应用程序直接发送给每个移动终端 11。因此在第三实施例中，不必在管理服务器 16 的应用程序信息存储单元 52 中产生临时保管应用程序区 52T。另外，在第一实施例中具有的用于规定存储在临时保管应用程序区 52T 中的每个应用程序的罗列在管理服务器 16 的应用程序信息存储单元 52 中的‘存储号’这一项并未包含在第三实施例中，因为这也是不必要的。图 38 表示第三实施例中的应用程序信息管理系统的配置，而图 39 表示在第三实施例中存储在用户信息存储单元 53 中的数据的实例的格式图。

而且，在第三实施例中，当移动终端 11-1 的存储控制器 35 接收到来自管理服务器 16 的信息摘要时，存储控制器 35 将临时存储该信息摘要。随后，当移动终端 11-1 的存储控制器 35 通过通信单元 34 接收到给定可靠性指数为‘1’或大于‘1’应用程序时，存储控制器 35 将产生所接收应用程序的信息摘要，并通过从管理服务器 16 接收的信息摘要核实新产生的信息摘要。

[3.2] 应用程序的传送

参考图 40、图 41 和图 42 将描述在移动终端 11-1 的用户购买和下载其提供者内容为服务器 20-1 且可靠性指数为‘1’或大于‘1’的应用程序时所执行的一系列操作。在下述的操作流程中，移动终端 11-1 的显示单元 21 所显示的屏幕与用于解释第一实施例的下载操作的图 21 中的屏幕相同。因此，图 21 也被参考用于下面的解释中。

移动终端 11-1 的用户在移动终端 11-1 上显示内容服务器 20-1 的主页，并申请购买在该主页上给出的应用程序（步骤 S601）。移动终端 11-1 的用户还执行支付应用程序使用费的步骤。

内容服务器 20-1 检验购买请求的内容是否满足要求，而且，如果购买请求的内容满足要求，内容服务器 20-1 将向管理服务器 16 发送接受购买应用程序的通知（步骤 S602）。接受购买应用程序的通知包括购买该应用程序的移动终端 11-1 的标识号以及所购买的应用程序的标识号。当内容服务器 20-1 发送该接受通知时，内容服务器 20-1 记录其购买应用程序的请求被接受的移动终端 11-1 的标识号。

在接收到来自内容服务器 20-1 的接受通知后，管理服务器 16 根

据接收到的接受通知中所包含的移动终端的标识号规定购买该应用程序的移动终端。接着，管理服务器 16 把接收到的接受通知中所包含应用程序的标识号寄存在与移动终端 11-1 相对应的用户信息存储单元 53-1 的准备下载应用程序区 53 中（步骤 S603）。

5 接着，管理服务器 16 向移动终端 11-1 发送购买应用程序的操作完成的通知（步骤 S604）。当移动终端 11-1 接收到购买应用程序的操作完成的通知时，移动终端 11-1 在显示单元 21 上显示字母 ‘a’ 以向移动终端 11-1 的用户通知新购买的应用程序准备从管理服务器 16 中下载。

10 如果所购应用程序是其使用费由管理服务器 16 管理的应用程序，则管理服务器 16 向费用管理服务器发送所购应用程序的信息，如该应用程序的标识号、移动终端 11-1 的标识号、购买应用程序的日期和时间等（步骤 S605）。

15 移动终端 11-1 的用户按动移动终端 11-1 的 appli-按钮 23 以显示屏幕 D21 所示的应用程序菜单。当显示屏幕 D21 时，移动终端 11-1 的用户按动操作单元 22 的按钮 ‘2’ 以选择 ‘2. 应用程序的下载’ 项。当按动按钮 ‘2’ 时，移动终端 11-1 向管理服务器 16 请求发送可下载到移动终端 11-1 的应用程序的信息（步骤 S606）。

20 在接收到发送应用程序的信息的请求之后，管理服务器 16 向移动终端 11-1 发送寄存于用户信息存储单元 53-1 的准备下载应用程序区 53B 中的应用程序的标识号和应用程序的名称，以作为应用程序的信息（步骤 S607）。

25 在接收到应用程序的信息之后，移动终端 11-1 显示屏幕 D22。通过响应该屏幕，移动终端 11-1 的用户可指定用户通过按动其号码与屏幕上的应用程序号相对应的按钮来下载的应用程序。例如，如果用户在屏幕 D22 显示时按动按钮 ‘1’，则题为 ‘时间表管理器 Ver. 2’ 的应用程序被指定。当通过移动终端 11-1 的用户的操作指定一个应用程序时，移动终端 11-1 向管理服务器 16 发送所指定应用程序的标识号（步骤 S608）。

30 在接收到所指定应用程序的标识号之后，管理服务器 16 读出存储在下载应用程序区 53A 中的数据并检验移动终端 11-1 的存储器 12 是否具有足够的自由空间来存储所指定的应用程序（步骤 S609）。

在步骤 S609, 如果移动终端 11-1 的存储器 12 没有足够的自由空间来存储所指定的应用程序, 那么管理服务器 16 将向移动终端 11-1 发送指定从存储器 12 中删除的一个应用程序的请求 (步骤 S610)。当移动终端 11-1 接收到指定一个应用程序的请求时, 移动终端 11-1 在显示单元 21 上显示屏幕 D23。通过响应屏幕上的信息, 如果移动终端 11-1 的用户按动按钮 ‘9’ 以命令执行下面的操作, 则移动终端 11-1 在显示单元 21 上显示屏幕 D24。在屏幕 D24 上, 列出了存储在管理区 40 中的应用程序的名称。通过响应显示在屏幕上的信息, 移动终端 11-1 的用户通过按动其号码与屏幕上的应用程序的号码相对应的按钮可以指定一个从存储器 12 中删除的应用程序。移动终端 11-1 向管理服务器 16 发送所指定应用程序的标识号 (步骤 S611)。在执行步骤 S611 的操作之后, 移动终端 11-1 在显示单元 21 上显示屏幕 D25。

相反, 在步骤 S609 中, 如果移动终端 11-1 的存储器 12 具有足够的自空间存储指定下载的应用程序时, 在步骤 S610 和步骤 S611 的操作被跳过, 并且管理服务器 16 将前进到步骤 S612 的操作, 在这种情况下, 移动终端 11-1 在显示单元 21 上显示屏幕 D25。

接着, 通过使用该应用程序的标识号, 管理服务器 16 从应用程序信息存储单元 52 中读出有关所指定应用程序的信息, 即该应用程序的信息摘要、该应用程序的可靠性指数、该应用程序的存储位置信息等, 并把该信息发送给移动终端 11-1 (步骤 S612)。

当移动终端 11-1 从管理服务器 16 接收到该应用程序的信息摘要、该应用程序的可靠性指数、该应用程序的存储位置信息等时, 通过使用该应用程序的存储位置信息, 移动终端 11-1 将请求内容服务器 20-1 发送该应用程序 (步骤 S613)。发送应用程序的请求包括移动终端 11-1 的标识号和该应用程序的标识号。

在接收到发送应用程序的请求之后, 内容服务器 20-1 检验包含在发送应用程序请求中的标识号是否与在步骤 S602 内容服务器 20-1 接受的购买应用程序的请求的移动终端的标识号相匹配。如果这些标识号匹配, 则内容服务器 20-1 向鉴别服务器 17 请求发送 ‘PK-MT-1’, 即移动终端 11-1 的公共密钥 (步骤 S614)。通过响应发送 ‘PK-MT-1’ 的请求, 鉴别服务器 17 向内容服务器 20-1 发送 ‘PK-MT-1’ (步骤 S615)。

在接收到‘PK-MT-1’之后，内容服务器 20-1 使用‘PK-MT-1’加密要被发送的应用程序（步骤 S616）。

由于该加密操作，在应用程序从内容服务器 20-1 发送到移动终端 11-1 期间被窃取时，未经许可的用户不能理解该应用程序。因此可以防止未经许可使用该应用程序。

随后，内容服务器 20-1 把加密的应用程序发送给移动终端 11-1（步骤 S617）。

当移动终端 11-1 接收到加密的应用程序时，移动终端 11-1 使用‘SK-MT-1’即移动终端 11-1 的专用密钥解密该应用程序（步骤 S618）。

接着，移动终端 11-1 产生在步骤 S608 的操作之后未被加密的应用程序的信息摘要，并验证新产生的信息摘要与通过步骤 S612 的操作从管理服务器 16 接收到的信息摘要（步骤 S619）。如果来自管理服务器 16 的作为就在完成该应用程序的检查之后产生的该应用程序内容的证明的信息摘要与新产生的信息摘要相匹配，则可以确认由移动终端 11-1 从内容服务器 20-1 接收的应用程序还未被改变。另一方面，如果这些信息摘要不匹配，则该应用程序不存储到存储器 12 中，并且移动终端 11-1 将向管理服务器 16 发送接收合适的应用程序失败的通知。在步骤 S619，如果信息摘要匹配，则移动终端 11-1 把该应用程序存储到存储器 12 的管理区 40 的应用程序区 40A 之一当中（步骤 S620）。在步骤 S609，如果存储器 12 没有足够的自由空间存储该应用程序，则新接收的应用程序将被写入管理区 40 中，在管理区 40 中存储了一个在步骤 S611 被指定删除的应用程序。在步骤 S609 中，如果存储器有足够的自由空间，则接收到的应用程序被写入未存储任何应用程序的管理区 40 之一中。

在移动终端 11-1 完成存储应用程序的操作之后，移动终端 11-1 向管理服务器 16 发送存储应用程序完成的通知（步骤 S621）。在步骤 S621 的操作之后，移动终端 11-1 在显示单元 21 上显示如屏幕 D26 所示的常规屏幕。

在接收到存储应用程序完成的通知之后，管理服务器 16 按下述方式更新用户信息存储单元 53 中的数据（步骤 S622）。如果通过上述操作一个应用程序从移动终端 11-1 的存储器 12 中删除，则管理服务器

16 把寄存在下载应用程序区 53A 中的应用程序的信息移动到准备下载应用程序区 53B 中。管理服务器 16 把新近存储在存储器 12 中的应用程序的信息从准备下载应用程序区 53B 移动到下载应用程序区 53A 的相应位置中。

- 5 上述段落描述的是在移动终端 11 的用户购买和下载可靠性指数为‘1’或大于‘1’的应用程序时执行的操作流程。相反，如果移动终端 11 的用户购买和下载可靠性指数为‘0’的应用程序，则管理服务器 16 不需要向移动终端 11-1 发送应用程序的信息摘要和可靠性指数，而仅仅执行图 40 中所示的步骤 S601 到 S604，步骤 S606 到 S611，
10 步骤 S613 到 S618 以及步骤 S620 到 S622 中的操作。而且，在这种情况下，在步骤 S610 和步骤 S611 中显示的指定删除的应用程序的列表是一个存储在自由区 41 中的列表，而不是存储在管理区 40 中的应用程序的列表。

- 根据上述操作，应用程序被存储到移动终端 11-1 的存储器 12 中，
15 但该应用程序并未被启动。因此，移动终端 11-1 的用户需要执行启动操作以使新购买的应用程序可用。在第三实施例中的启动操作与第一实施例中的启动操作相同。在第三实施例中的去启动操作和删除操作也与第一实施例中的相应操作相同。

[4] 改进

20 [4.1] 第一改进

- 在第一改进中，应用程序发送系统包括多个管理服务器。多个管理服务器可以彼此同步，而且它们的数据库中的数据被频繁更新。当任何一个移动终端或内容服务器需要与管理服务器通信时，它们可选择可加快通信过程的任意一个管理服务器。根据第一改进，应用程序
25 发送系统中的事务的总速度以及管理服务器对系统故障的耐用性得到了提高，这是因为管理服务器是在分布式处理系统中执行它们的任务的。

[4.2] 第二改进

- 在第二改进中，除了移动终端的内部存储器外，移动终端的用户
30 在移动终端中有几种存储位置可以选择用来存储应用程序，如几种 IC 卡存储器，用户标识模块 (UIM) 以及可与移动终端连接的外部存储装置。根据第二改进，通过更换这些包含应用程序的记录介质，可以很

容易地在几个移动终端之间共享或移动应用程序。

[4.3] 第三改进

在第三改进中，移动终端包括输入/输出接口，通过该接口，移动终端可通过不同与移动通信网络的电缆或无线电波与其它信息终端通信。因此，移动终端可通过它们的输入/输出接口从其它信息终端获得应用程序。

[4.4] 第四改进

在第四改进中，管理服务器可以区分其内容相同但其提供者彼此不同的每个应用程序的应用程序信息存储单元中列出的标识号。而且，如果需要的话，每个应用程序给定一个彼此不同的可靠性指数。根据第四实施例，由可靠的内容提供者提供的应用程序给定高可靠性指数，而不太可靠的内容提供者提供的应用程序给定低可靠性指数。因此，不同的条件可被提供给相同内容的应用程序。

[4.5] 第五改进

在第五改进中，一个应用程序可占据移动终端的存储器中的多个存储区。因此，移动终端甚至可以处理大的应用程序。

[4.6] 第六改进

在第六改进中，用于存储其内容已被检查的应用程序的管理区和用于存储其内容未被检查的应用程序的自由区可以彼此之间进行转换。存储控制器管理有关存储区中的应用程序是否定一个可靠性指数的应用程序信息，并且它不能把管理区中的应用程序与自由区中的应用程序搞错。因此，如果管理区中的自由空间不足的话，具有自由空间的自由区可被转换为管理区。因而可以更为有效地利用存储区。

[4.7] 第七改进

在第七改进中，与管理服务器的管理实体不同的第三方实体执行应用程序的检查并提供有关应用程序可靠性的信息。由第三方实体提供的可靠性信息被发送给管理服务器，并且由管理服务器和移动终端使用。

第三方实体管理内容鉴别服务器，并且当一个应用程序从内容服务器发送到管理服务器时，内容鉴别服务器向管理服务器公布该应用程序的证明。管理服务器确认该应用程序是否由于内容服务器的篡改而发生变化。

更具体的讲，在检查一个应用程序之后，第三方实体使用散列函数产生该应用程序的信息摘要。当管理服务器接收到来自内容服务器的应用程序时，管理服务器请求内容鉴别服务器发送与该应用程序对应的信息摘要。通过响应该请求，内容鉴别服务器把信息摘要发送给管理服务器。在接收到信息摘要之后，管理服务器使用与第三方实体所使用的相同的散列函数产生应用程序的信息摘要，并验证从内容鉴别服务器接收的信息摘要和新产生的信息摘要。根据上述验证，管理服务器可确认接收的应用程序是合适的应用程序。

在第七改进中，管理服务器不需要获得未加密的应用程序，这是因为第三方实体保证其内容。因此，内容服务器通过管理服务器向移动终端发送使用移动终端的公共密钥加密的应用程序。由于管理服务器可确认应用程序的内容没发生变化，因此，管理服务器不需要检验应用程序的发射器。因此，在不使用内容服务器的专用密钥进行加密的情况下，内容服务器可以把应用程序发送给管理服务器。

15 [4.8] 第八改进

在第八改进中，可靠性相关信息用于管理一个使用另一个应用程序或控制程序的功能或数据的应用程序的请求，并且可靠性相关信息提供与用于判断请求是否被接受的各种功能或数据之间的每个关系有关的指示。

20 根据第八改进，移动终端可执行灵活的协调操作控制，其中，应用程序 A 被允许呼叫应用程序 B 的功能 1 但不允许呼叫应用程序 B 的功能 2。

[5] 本发明的效果

25 如上所述，根据本发明的方法、系统和装置，存储在移动终端的存储器中的多个应用程序可被协调执行。同时，由于存储控制器严格监督应用程序之间的数据交换并根据给定每个应用程序的可靠性信息呼叫其它应用程序的功能，因此可以减少诸如个人信息和财政数据这样的高位值数据被泄露和破坏的风险。因此，当应用程序在移动终端中执行时，既可以提高对移动终端用户的友好性，又可以维护信息安全。

30

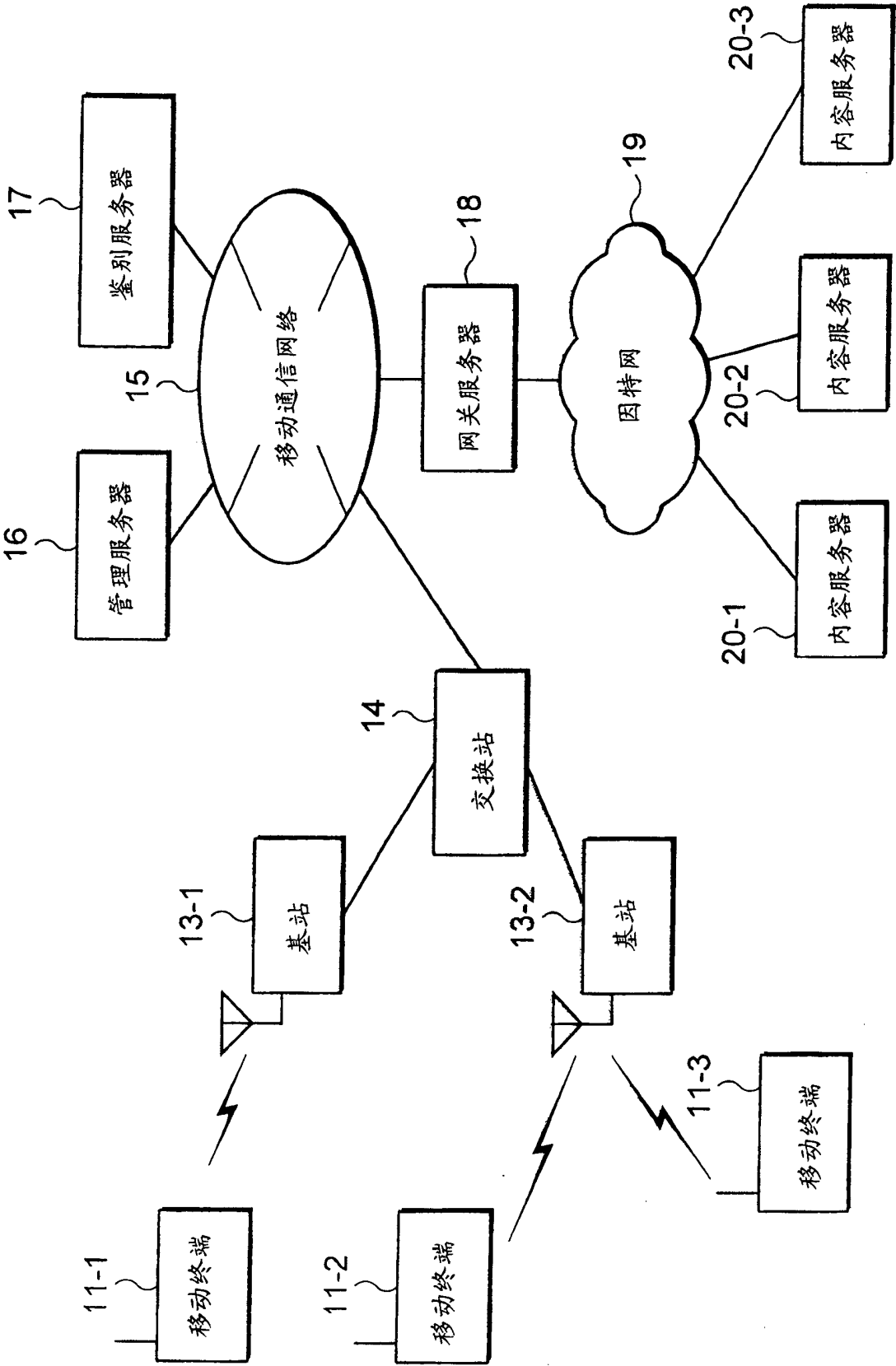


图 1

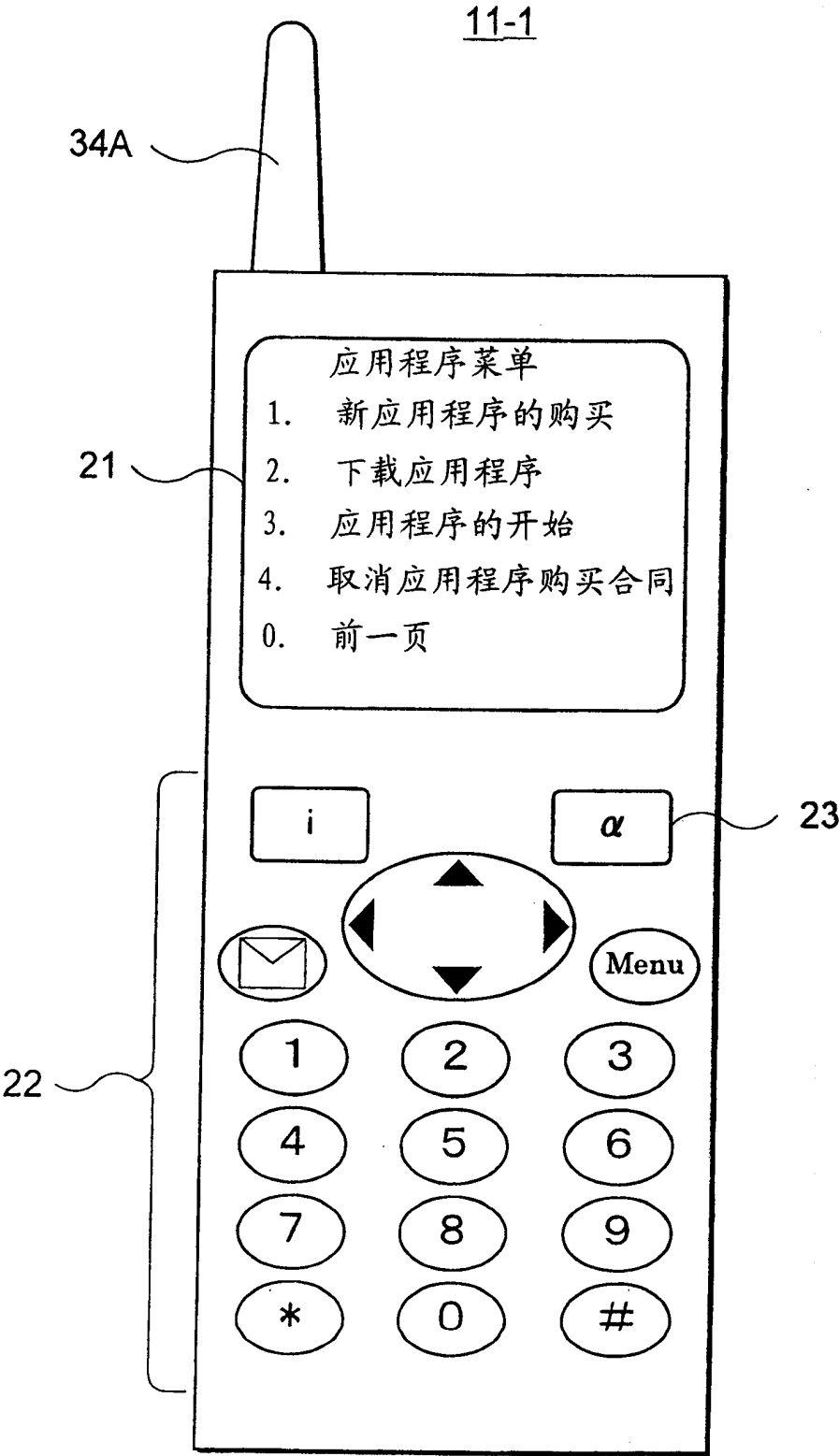


图 2

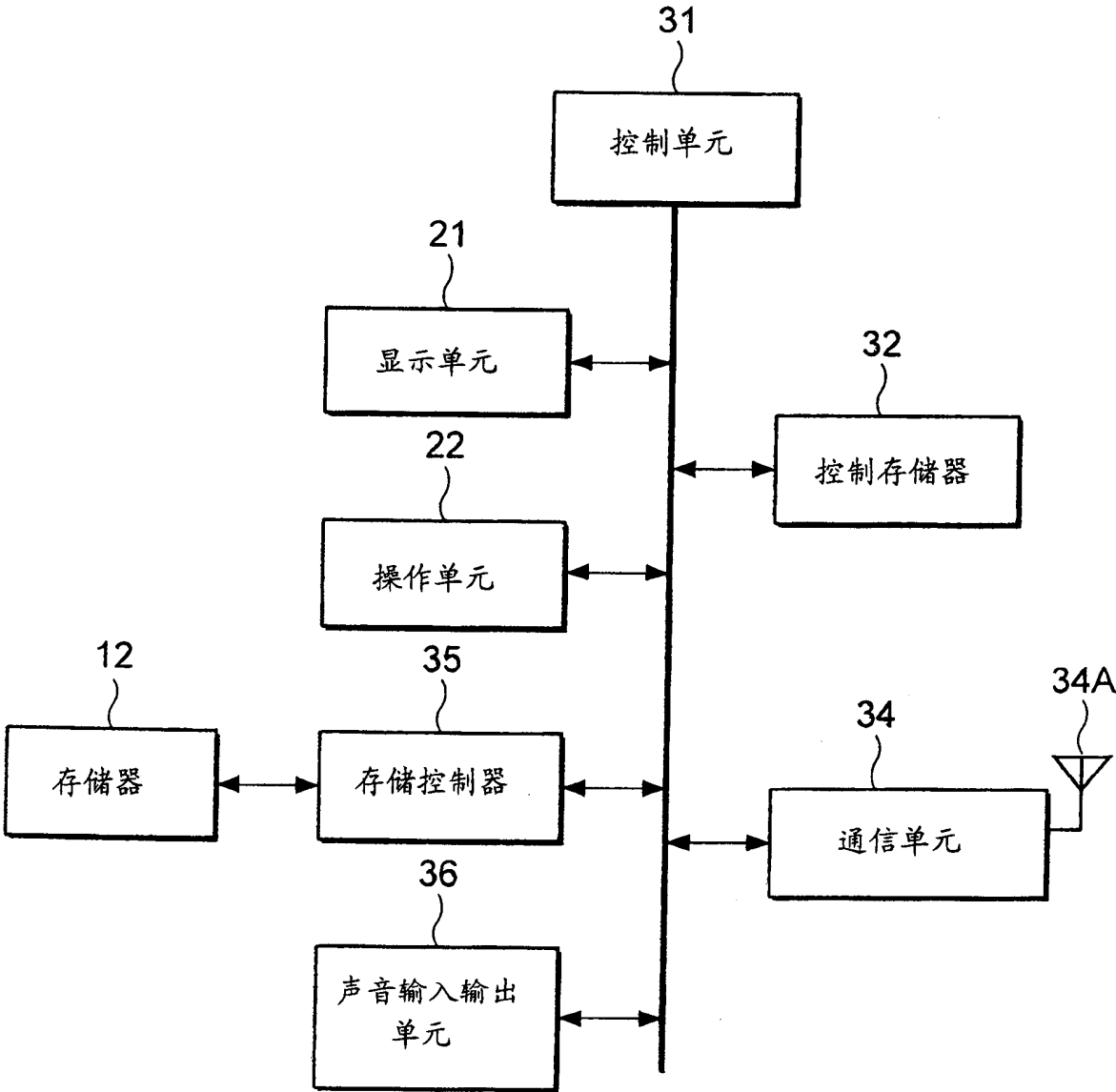


图 3

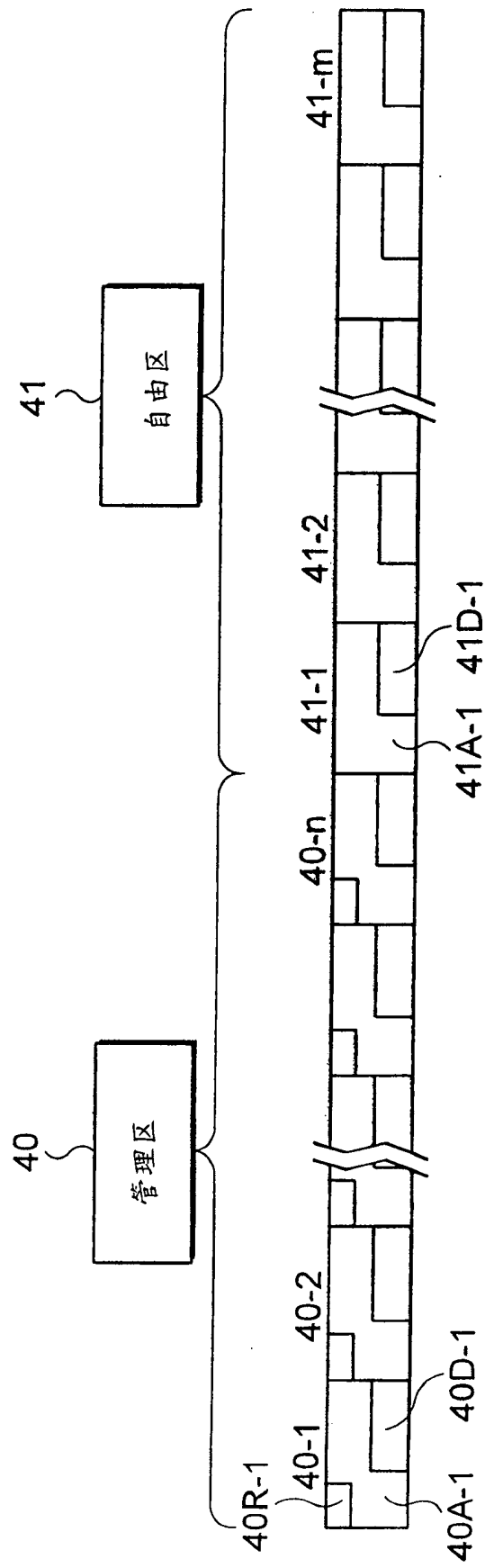


图 4

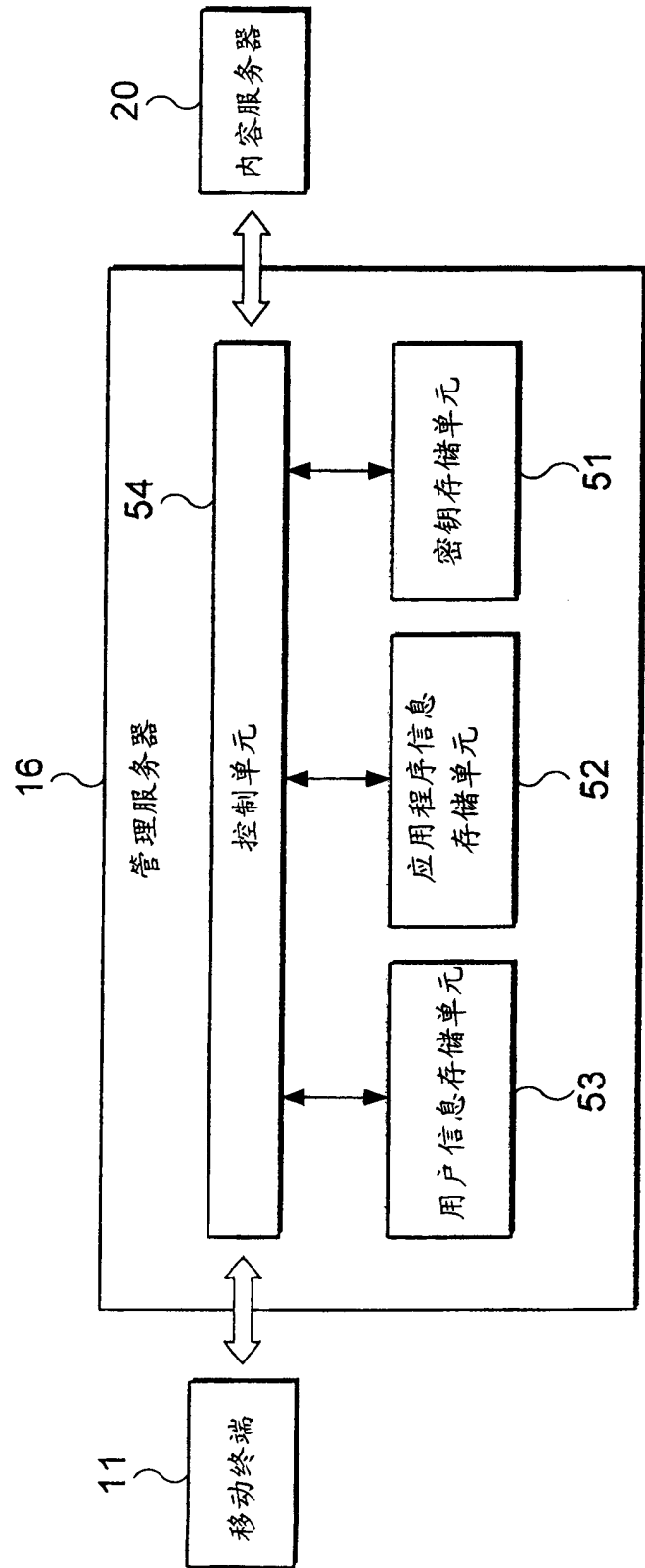


图 5

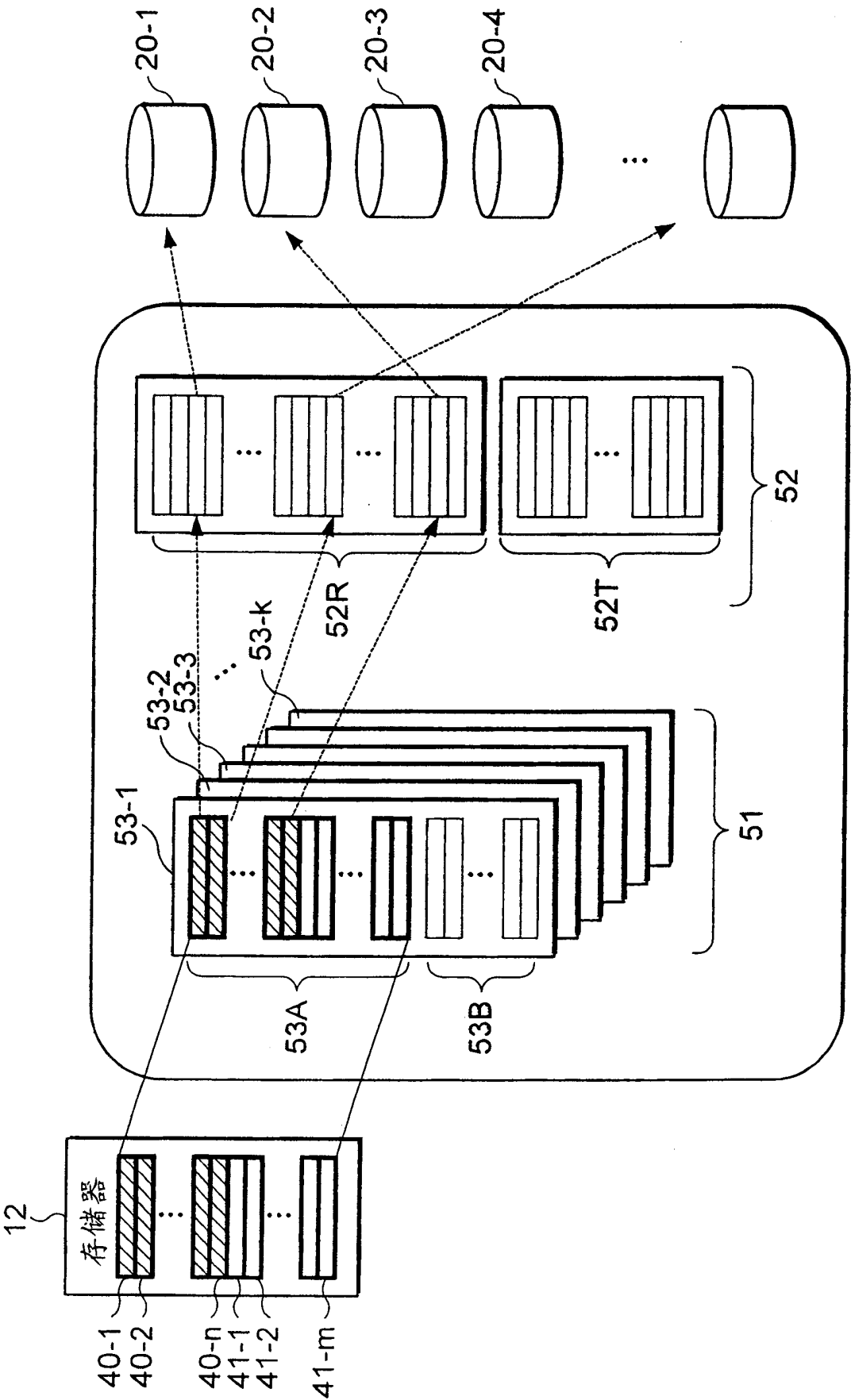


图 6

下载应用程序区	存储区		应用程序的信号	启动	存储量
	管理区	1	AP-2568	是	—
		2	AP-0123	否	—
		3	AP-1015	是	—
		⋮	⋮	⋮	⋮
		n	未使用	—	—
	自由区	1	F-0325	是	—
		2	F-7485	是	—
		3	未使用	—	—
		⋮	⋮	⋮	⋮
		m	未使用	—	—
准备下载应用程序			1	AP-4125	—
			2	F-5963	—
			3	AP-3021	—
			4	AP-4513	—
			5	未使用	—
			6	未使用	—
			7	未使用	—
			8	未使用	—
			9	未使用	—
			⋮	⋮	⋮

图 7

应用程序标识号	可靠性指数	公告	费用的 征收	存储位置信息
AP-2568	3	是	是	应用程序本身被存储
AP-3712	5	是	否	ftp://ftp.abc_software.com/application/ap_0306.exe
AP-4513	2	否	是	应用程序本身被存储
AP-3021	1	否	否	ftp://ftp.software_world.com/software/app_view.exe
F-3251	0	—	—	ftp://ftp.softpocket.com/root/app/miracle.exe
⋮	⋮	⋮	⋮	

图 8

存储号	
T-1025	应用程序本身被存储
T-7851	应用程序本身被存储
T-3639	应用程序本身被存储
T-7142	应用程序本身被存储
T-3256	应用程序本身被存储
⋮	⋮

图 9

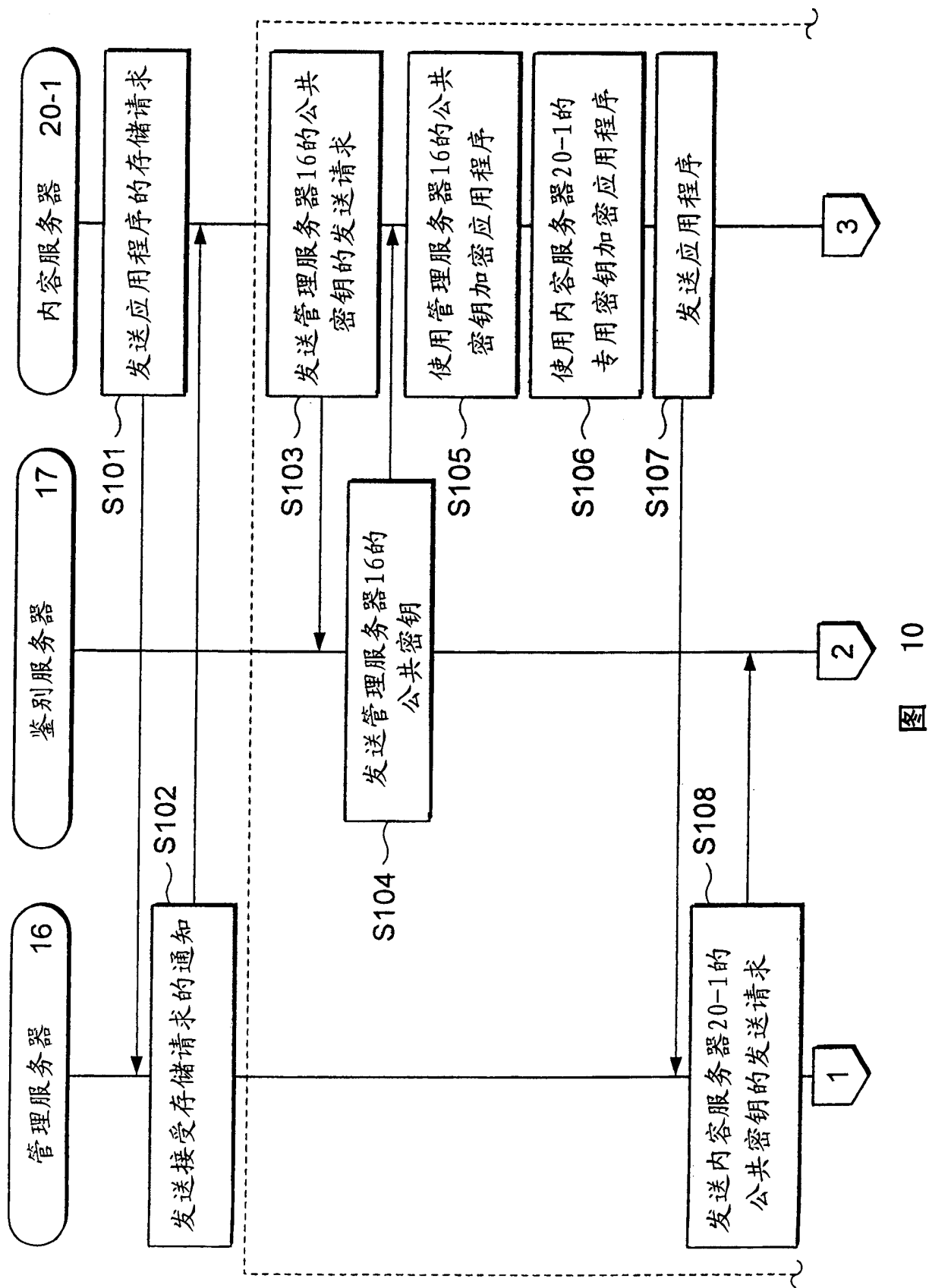


图 10

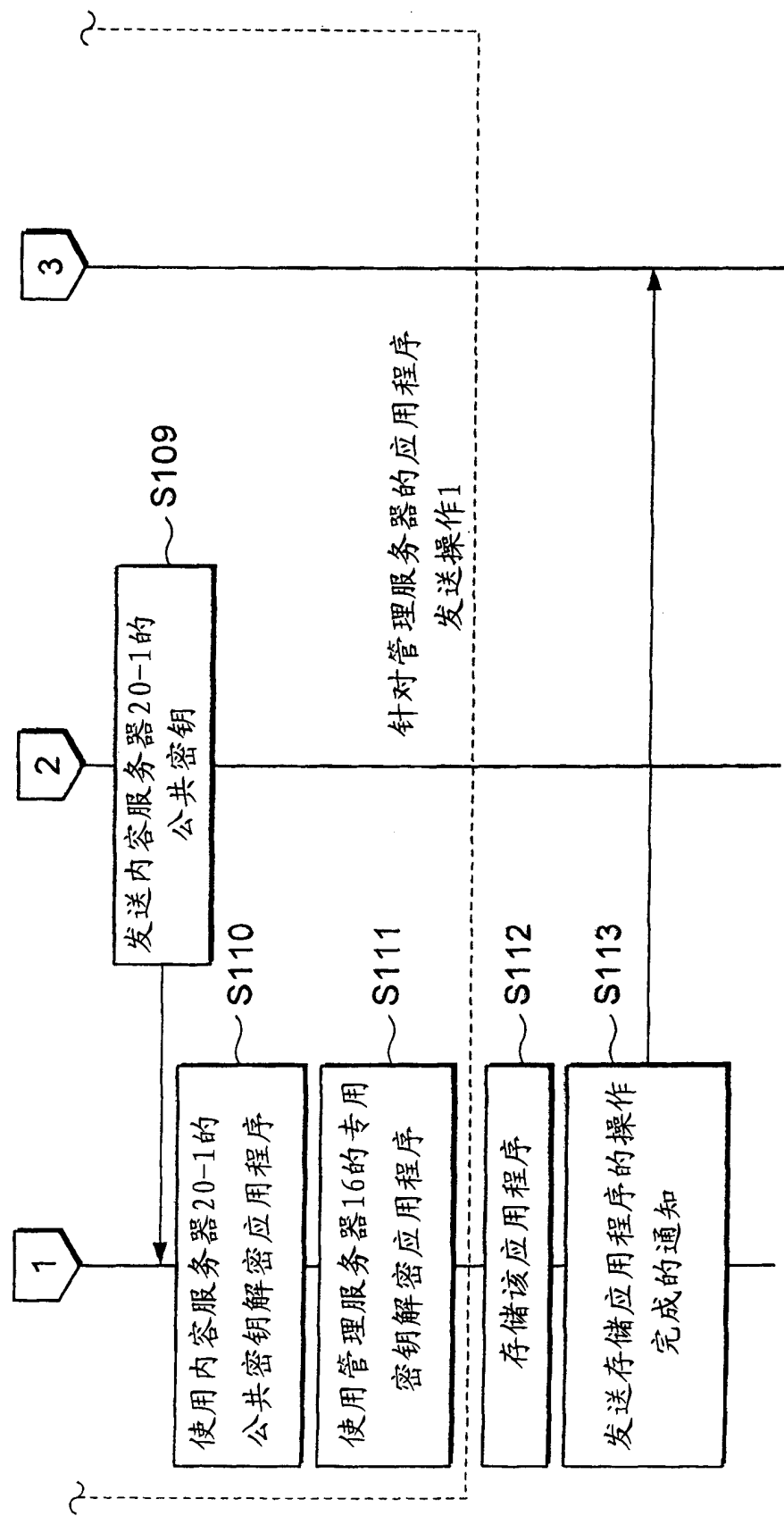


图 11

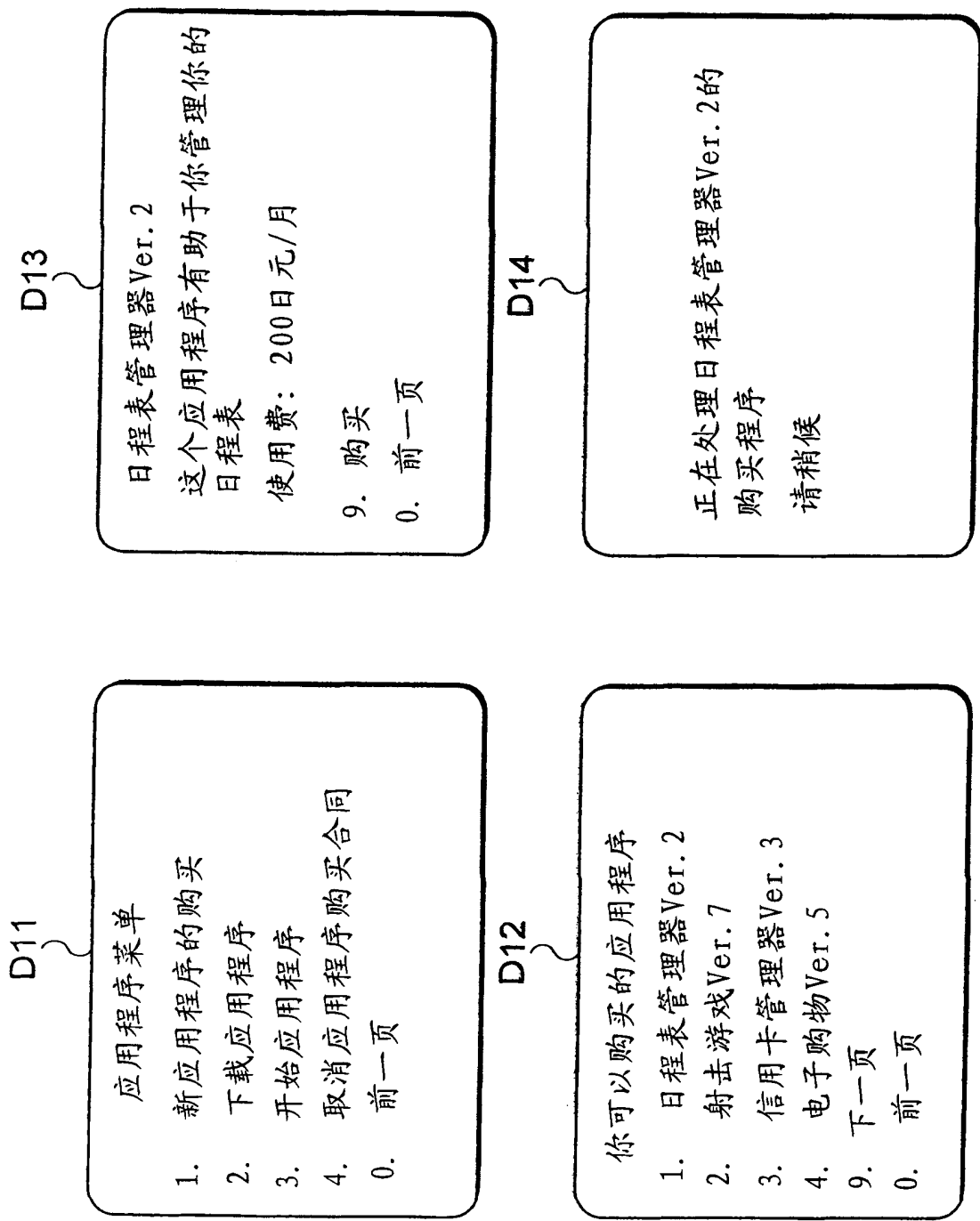


图 12

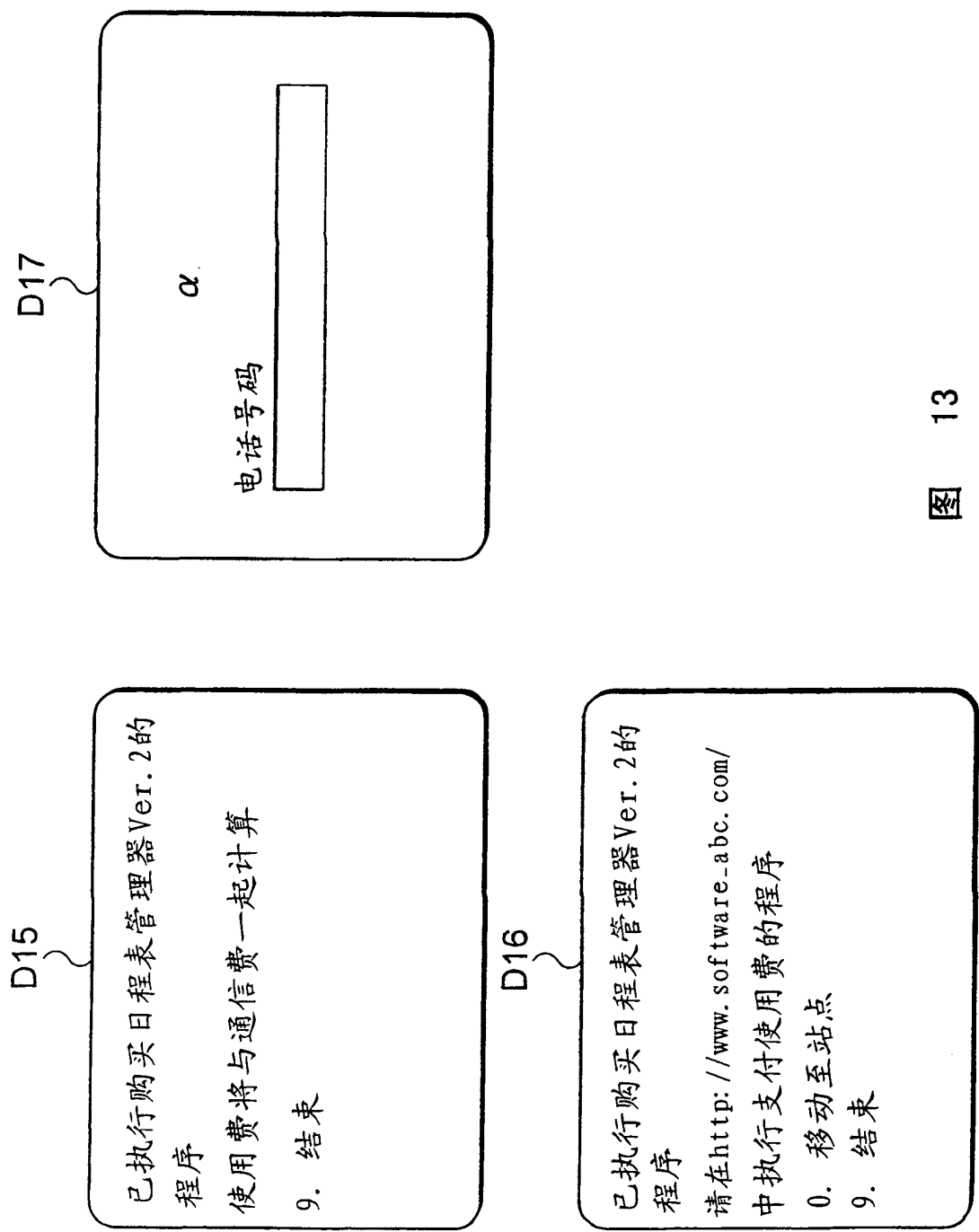


图 13

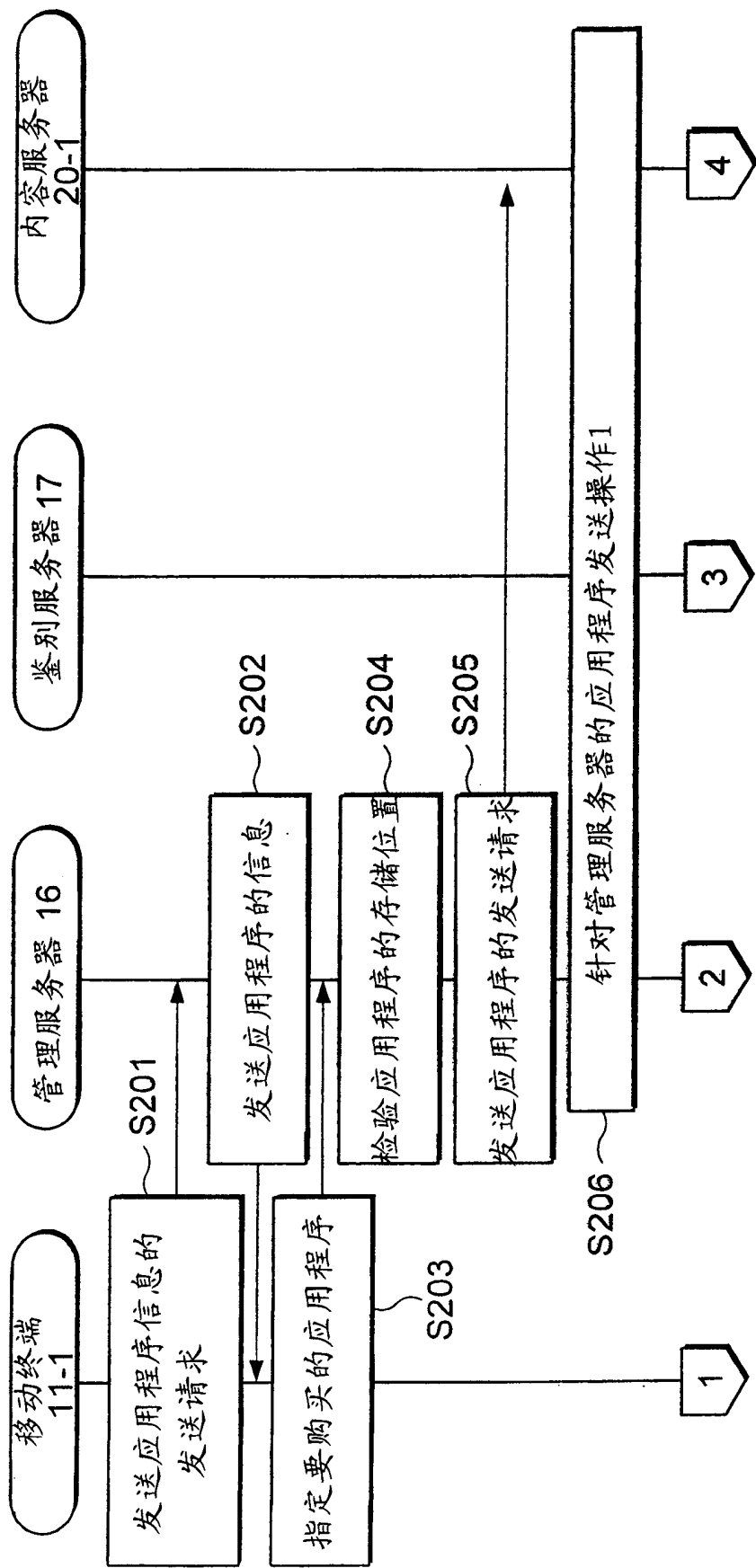


图 14

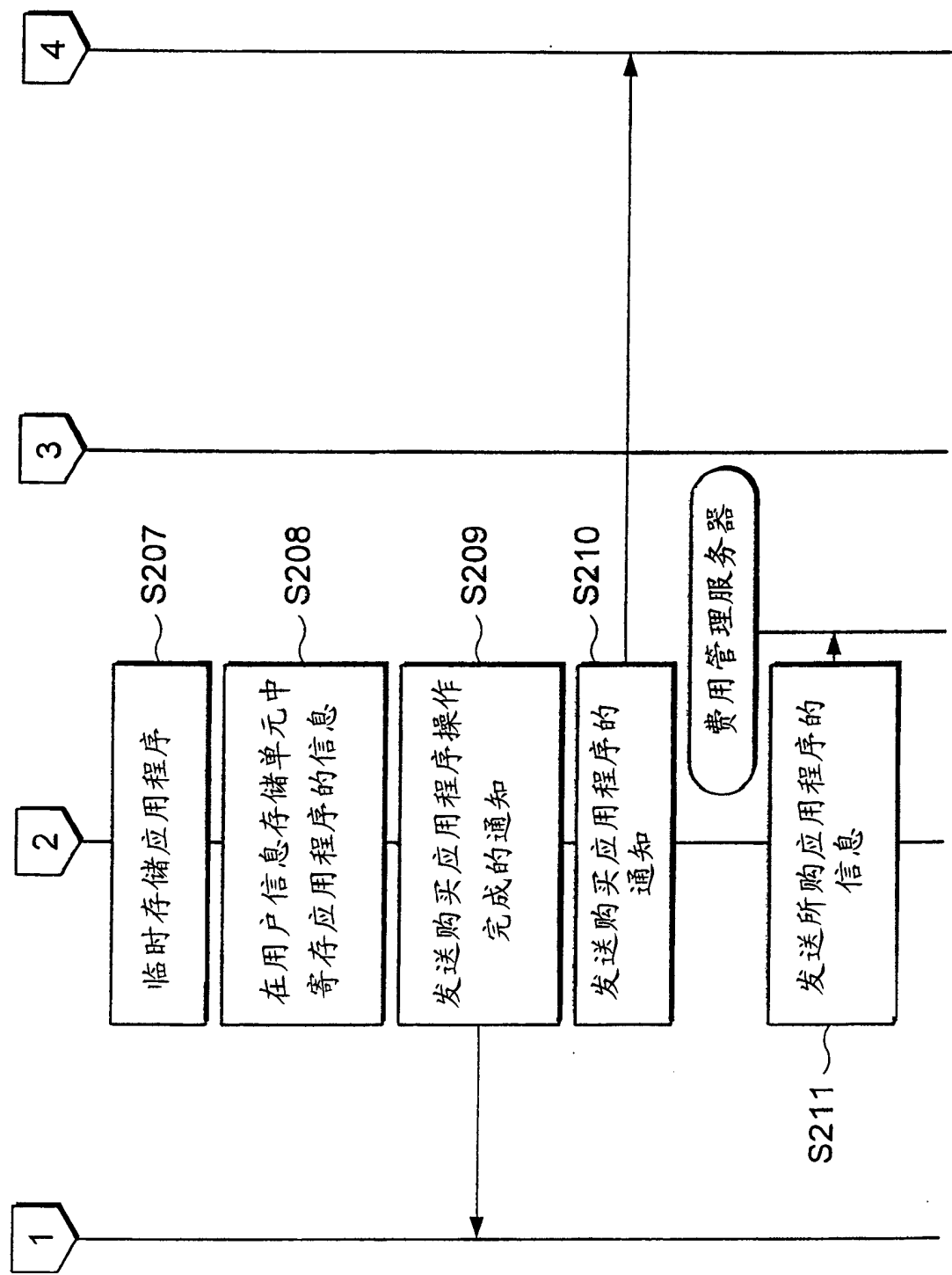
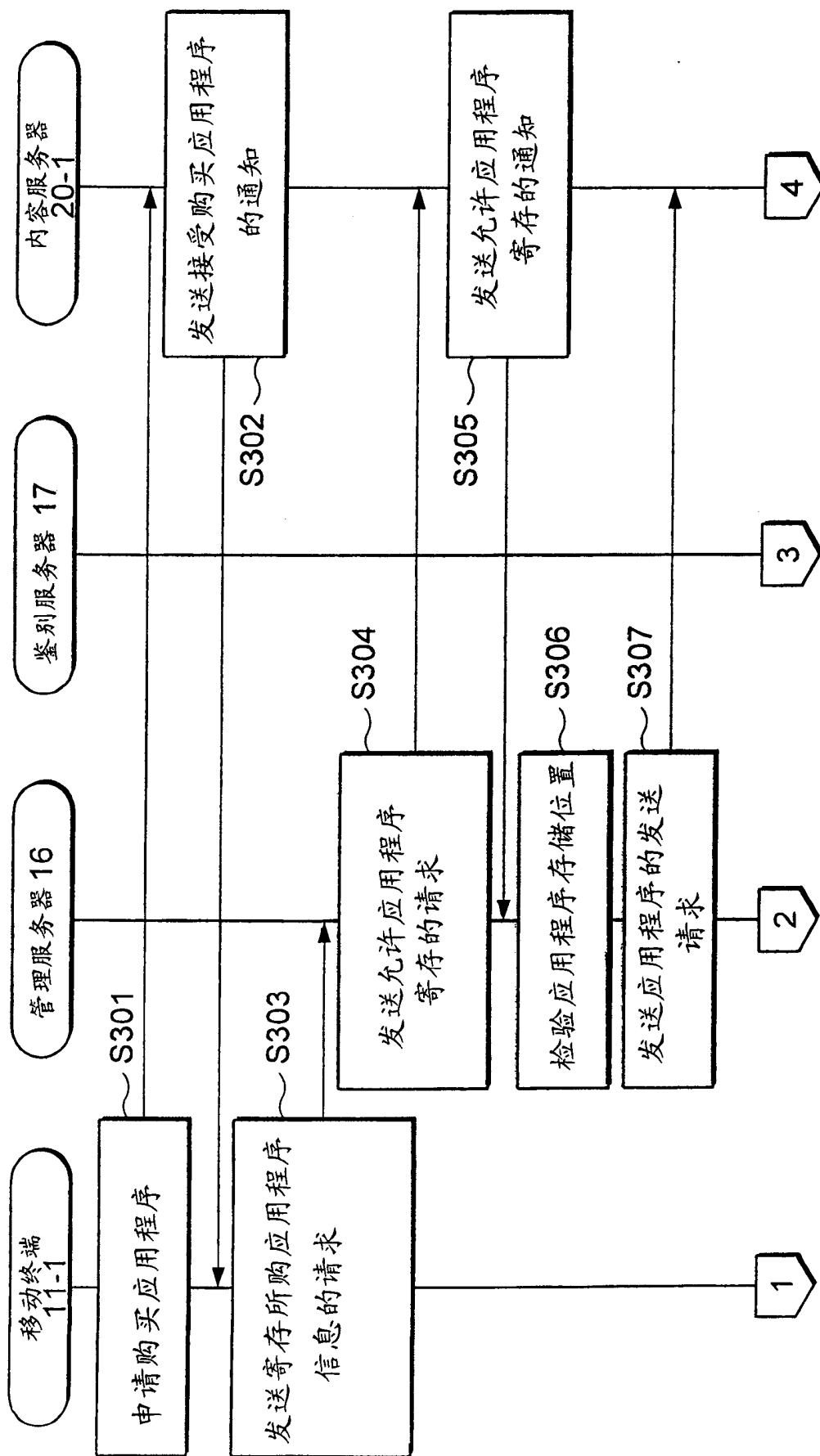


图 15



16

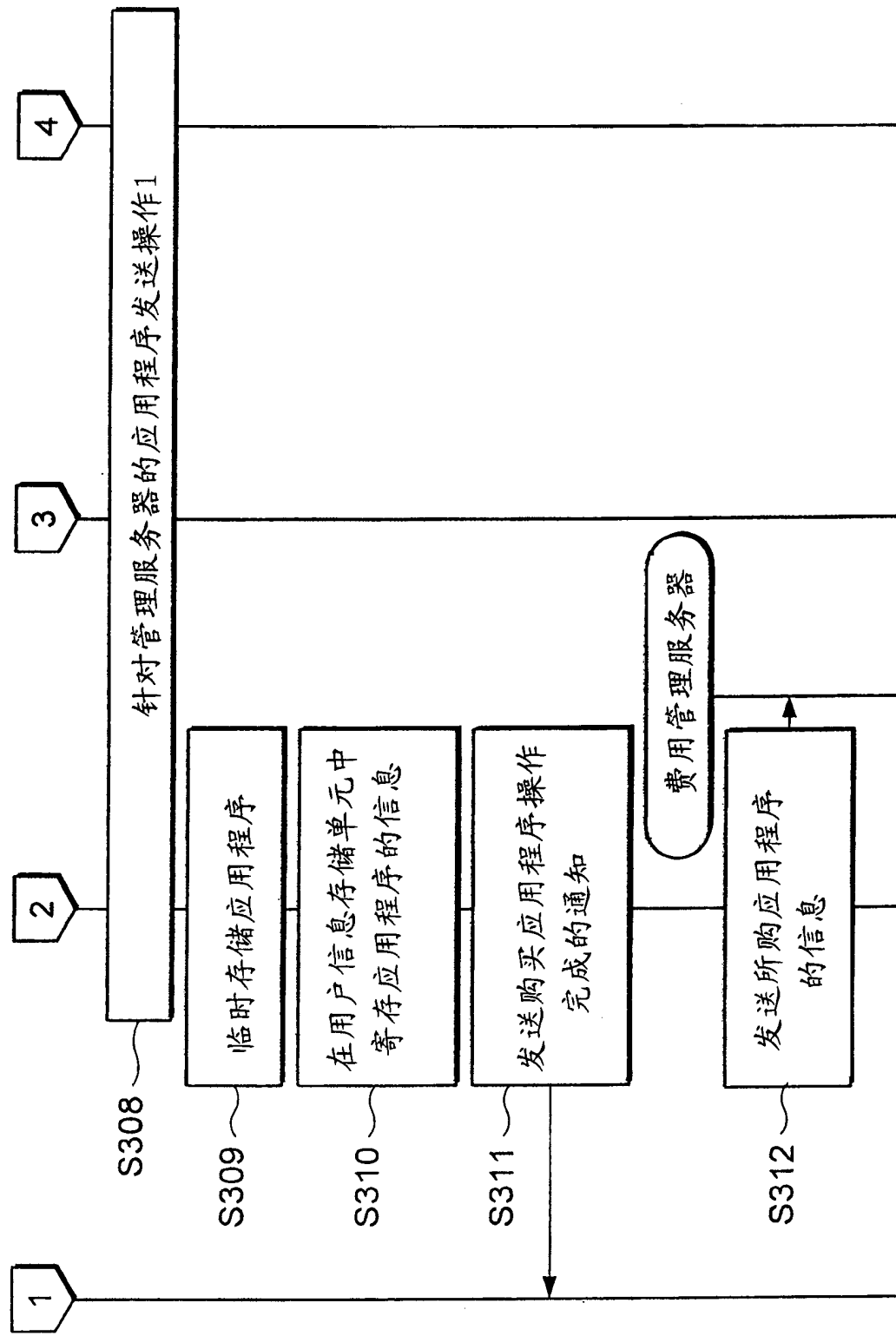


图 17

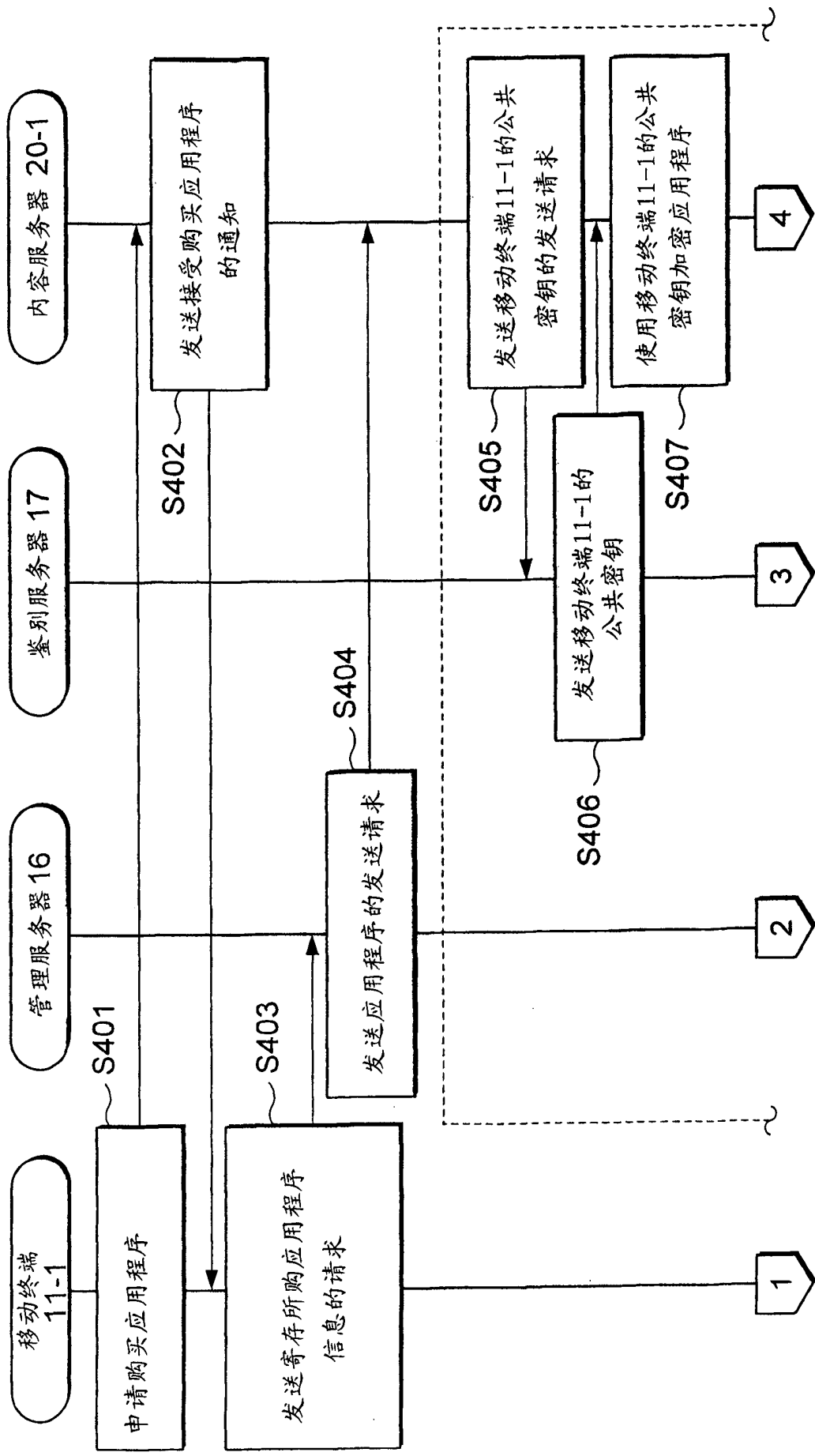


图 18

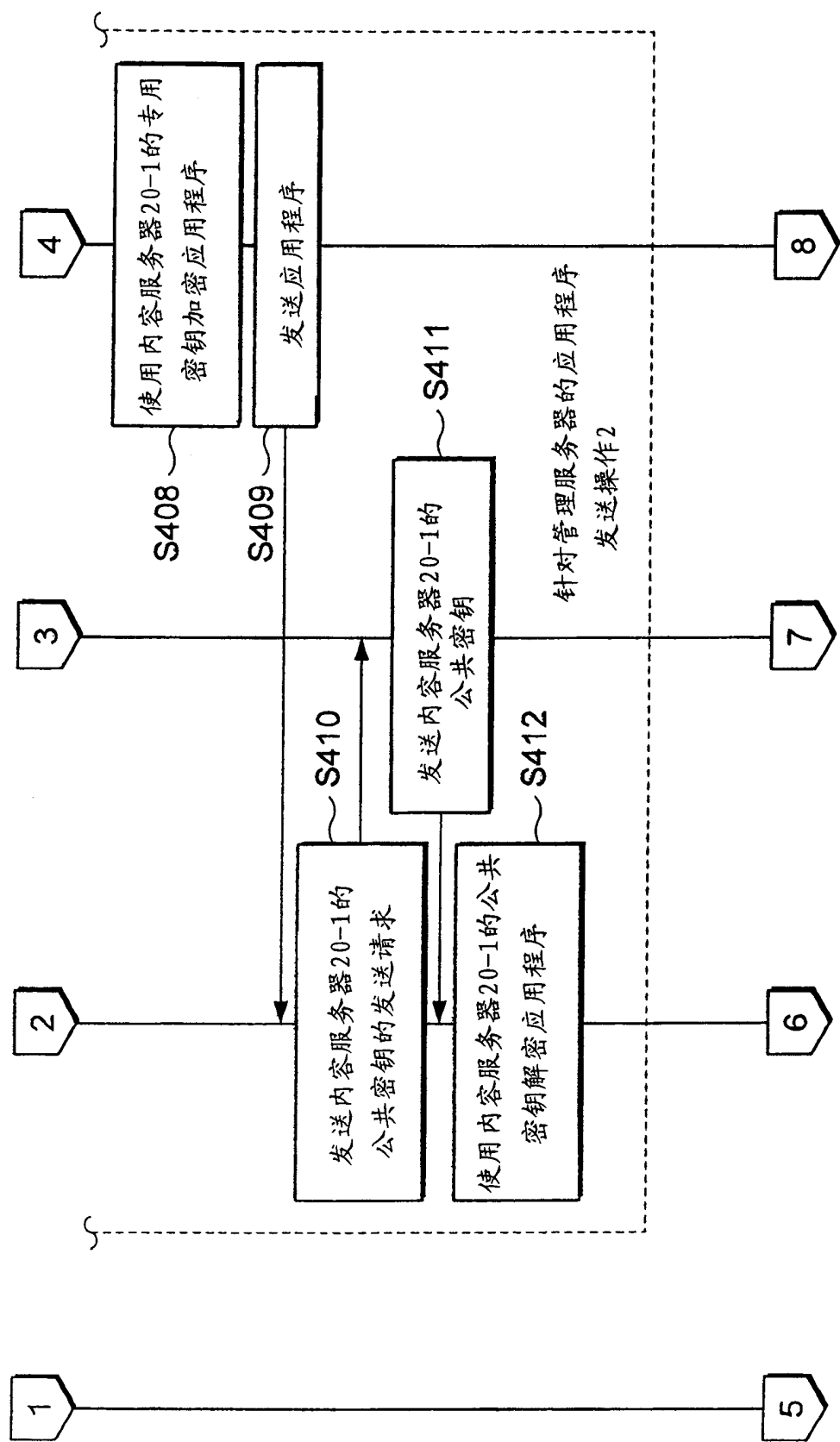


图 19

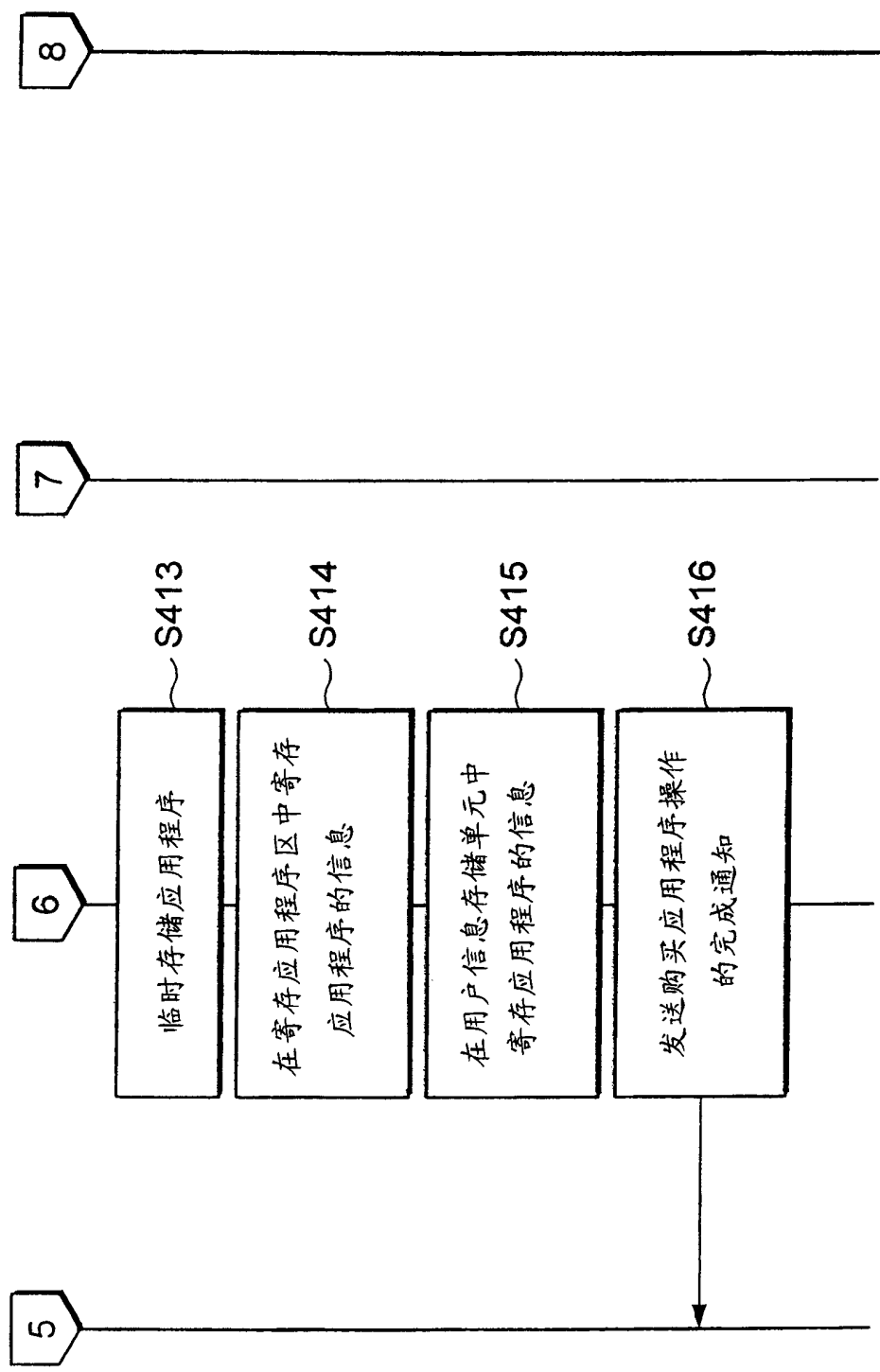


图 20

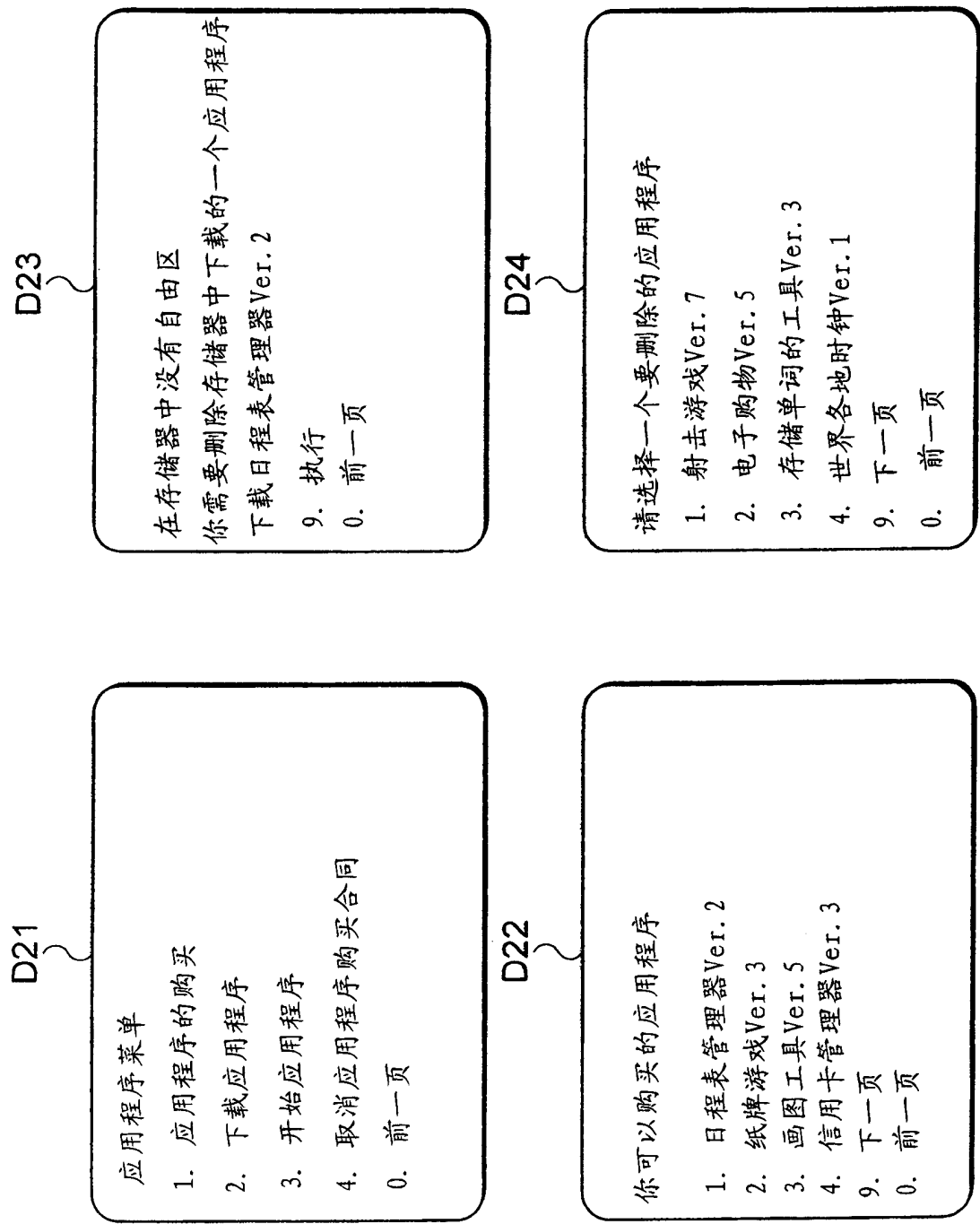


图 21

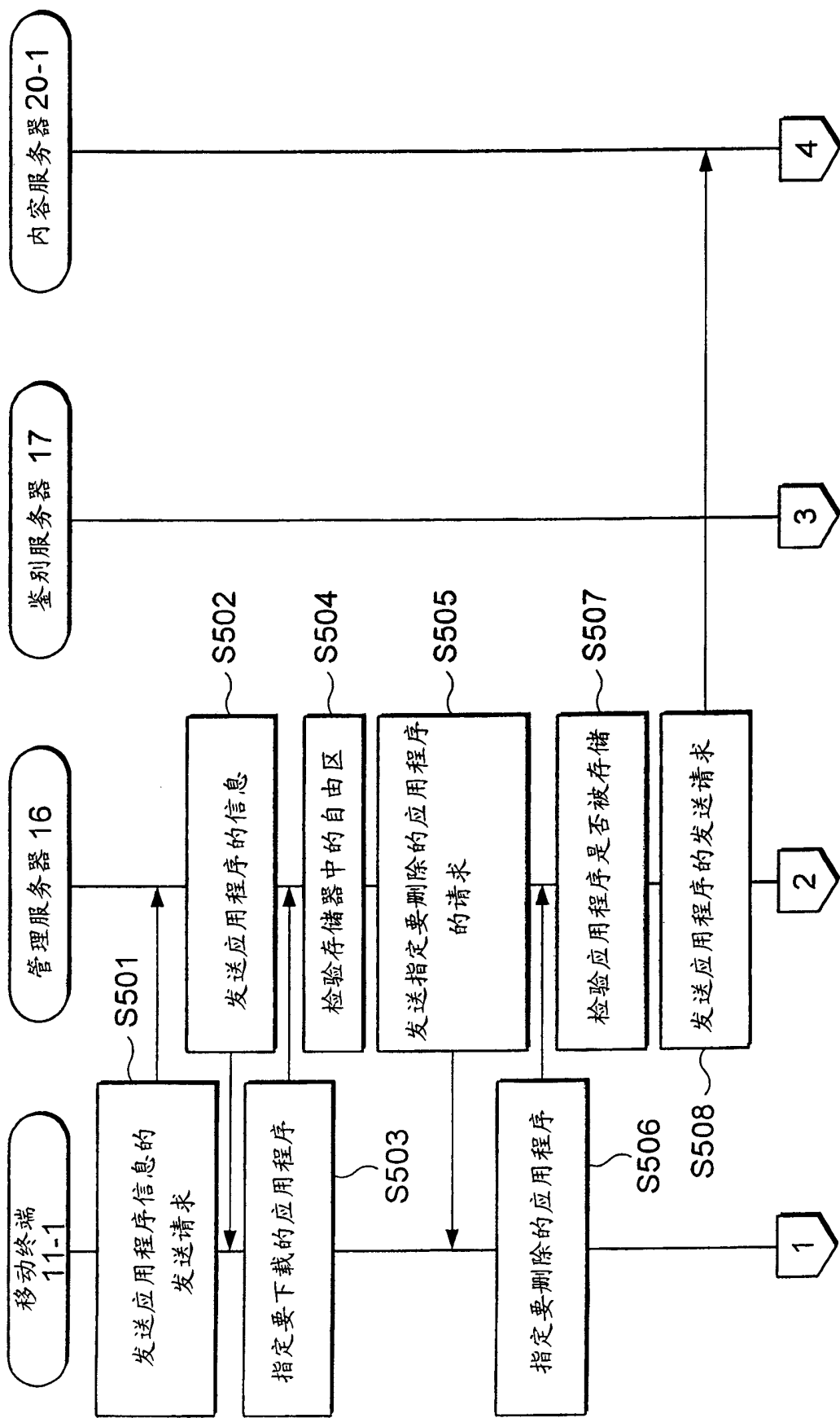


图 23

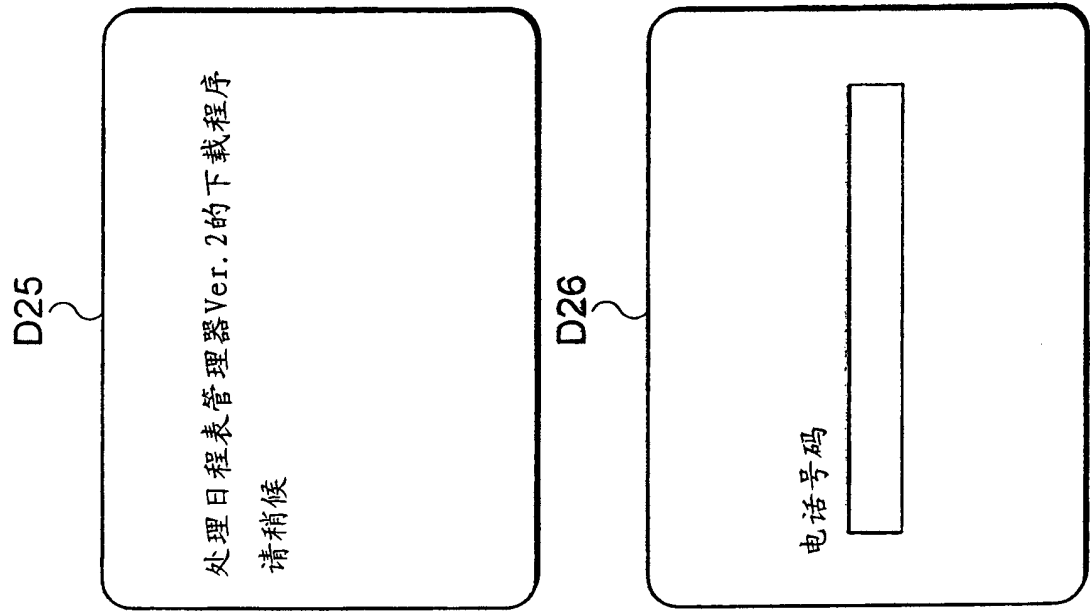


图 22

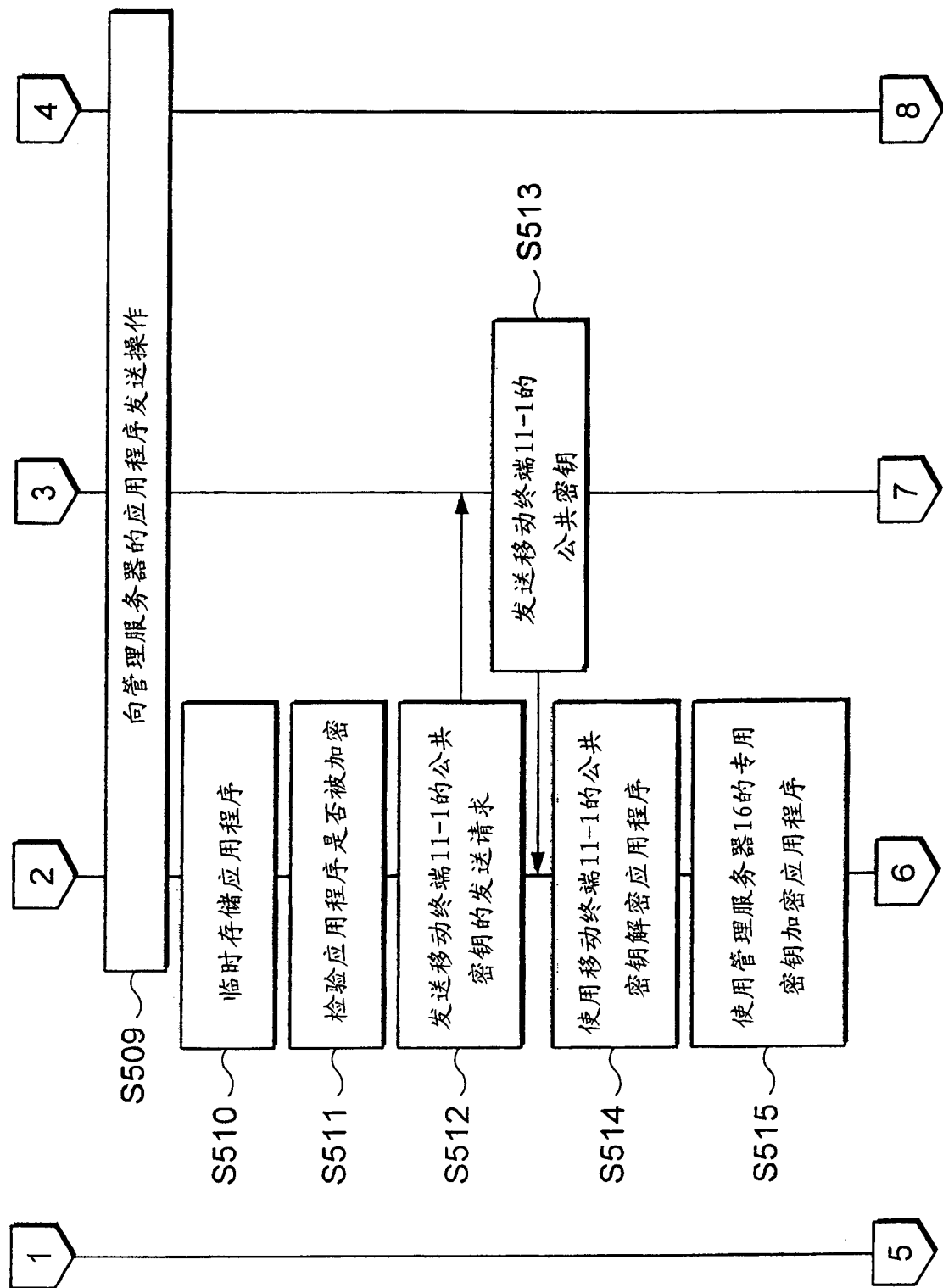


图 24

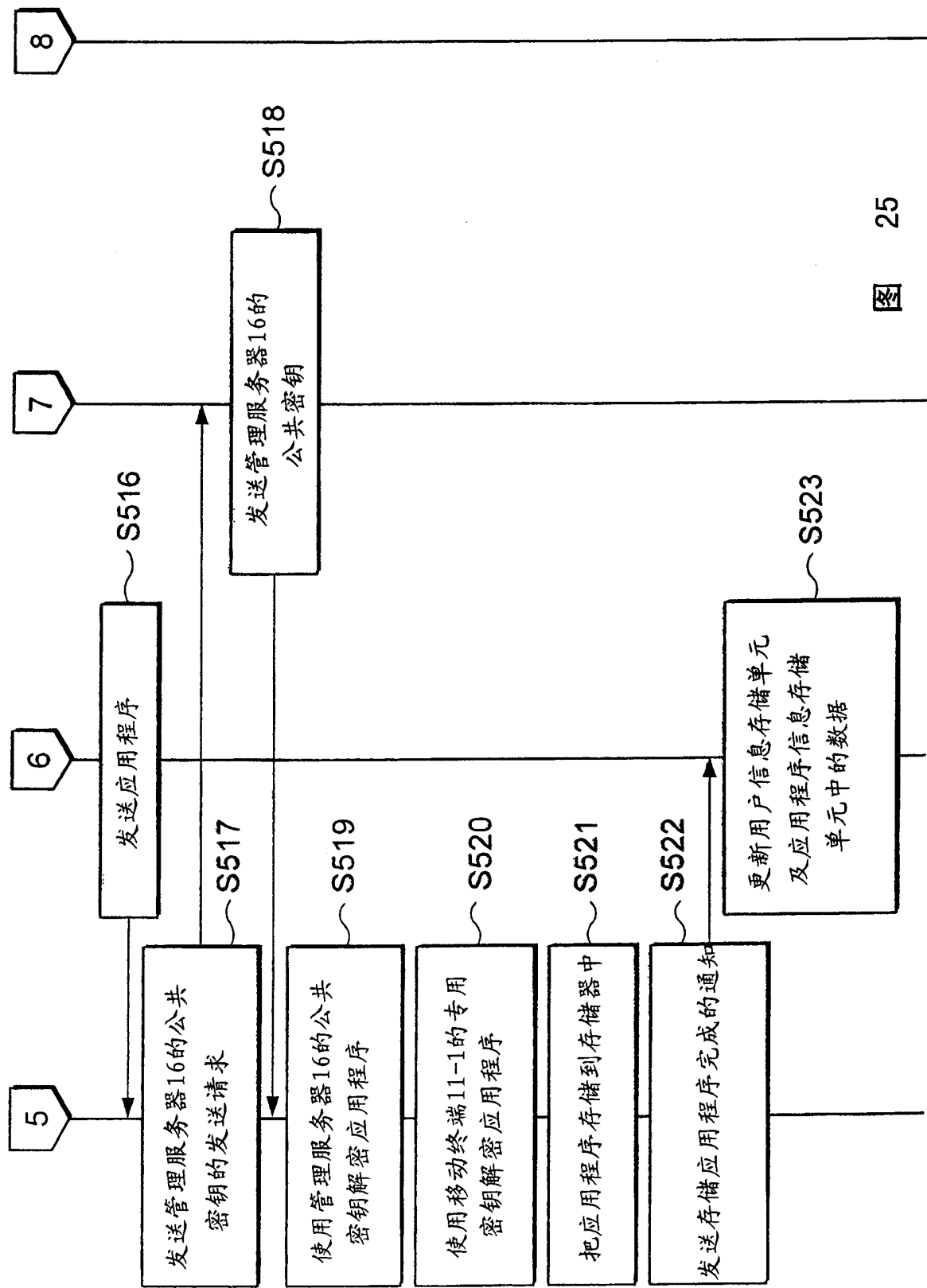


图 25

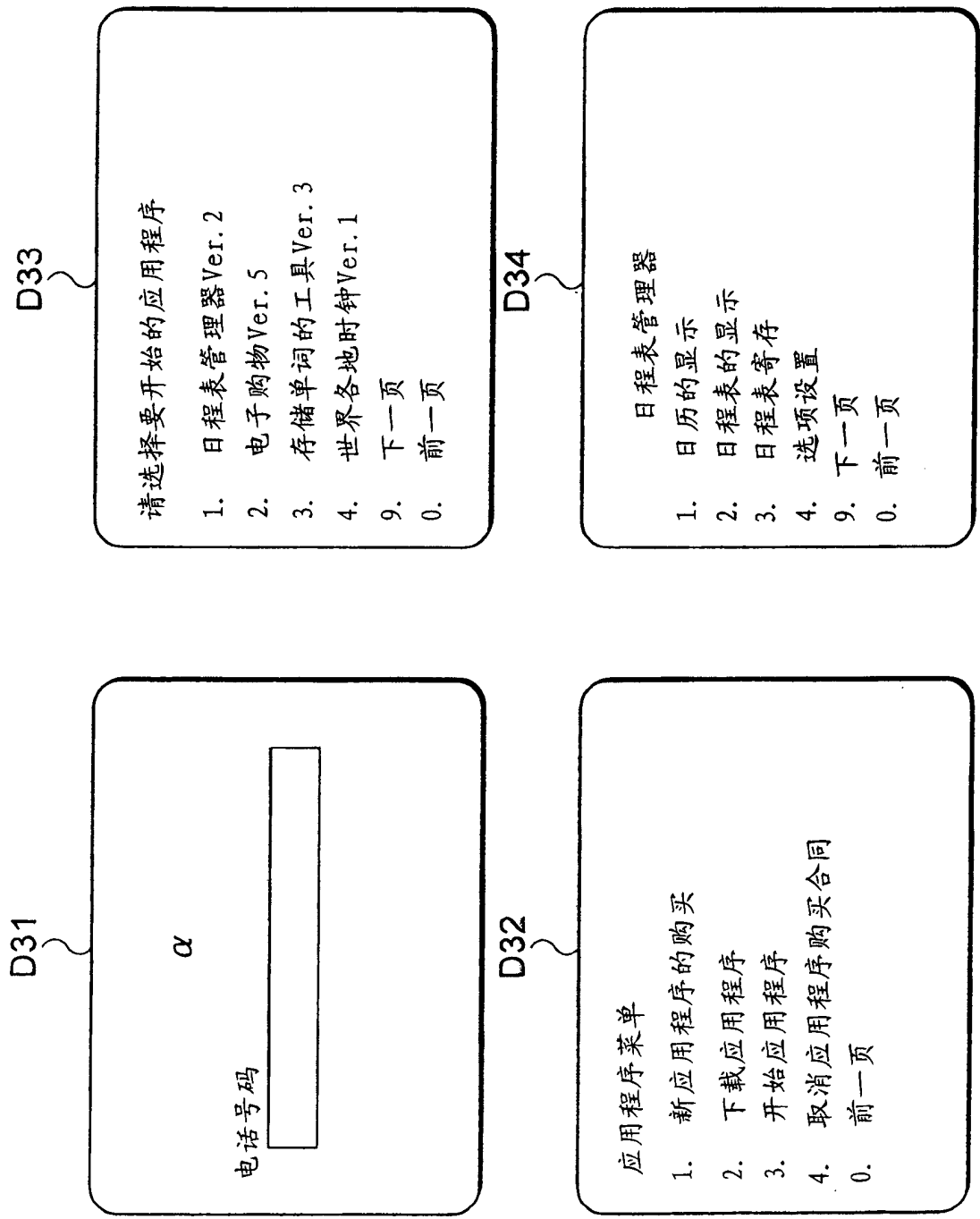


图 26

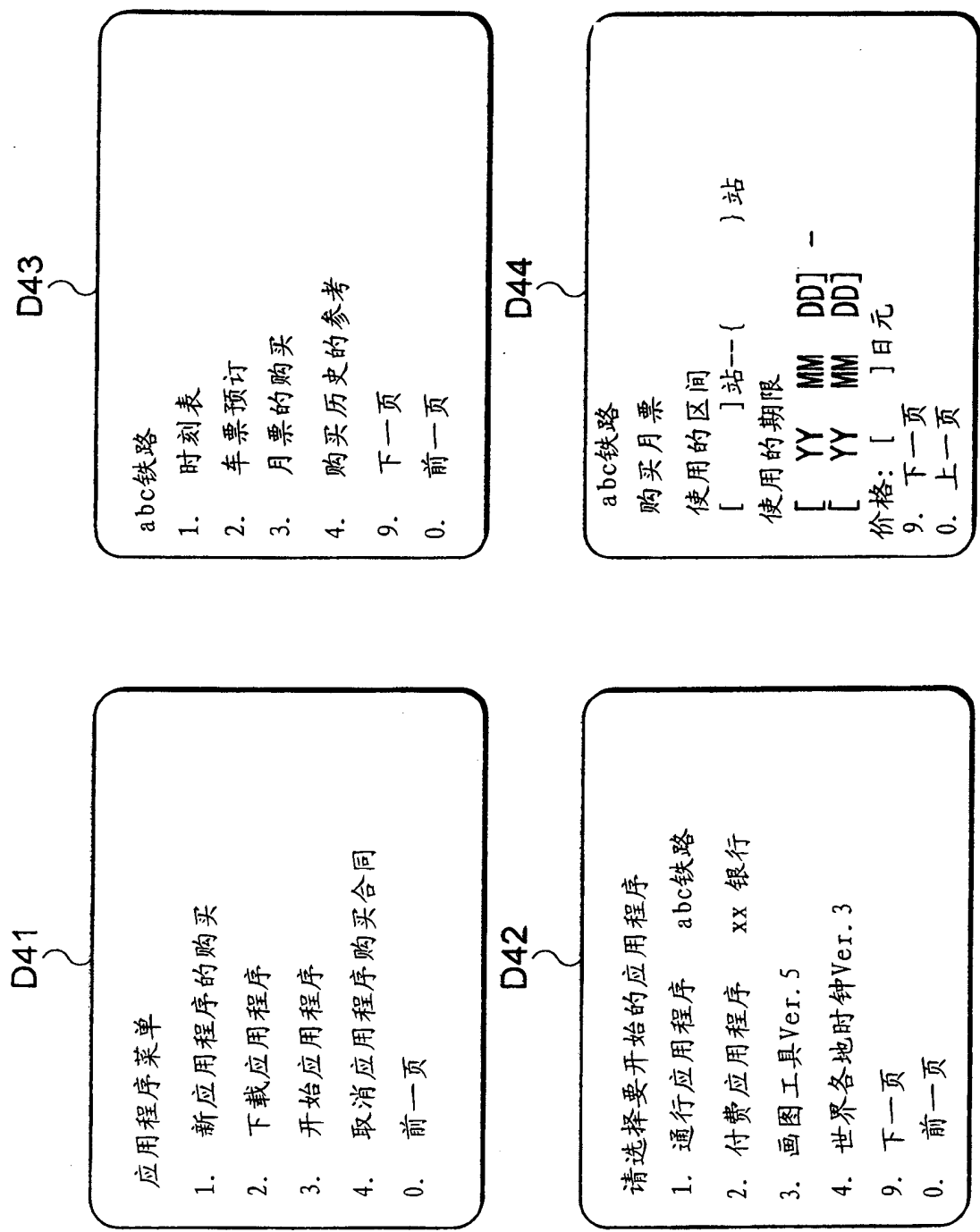


图 27

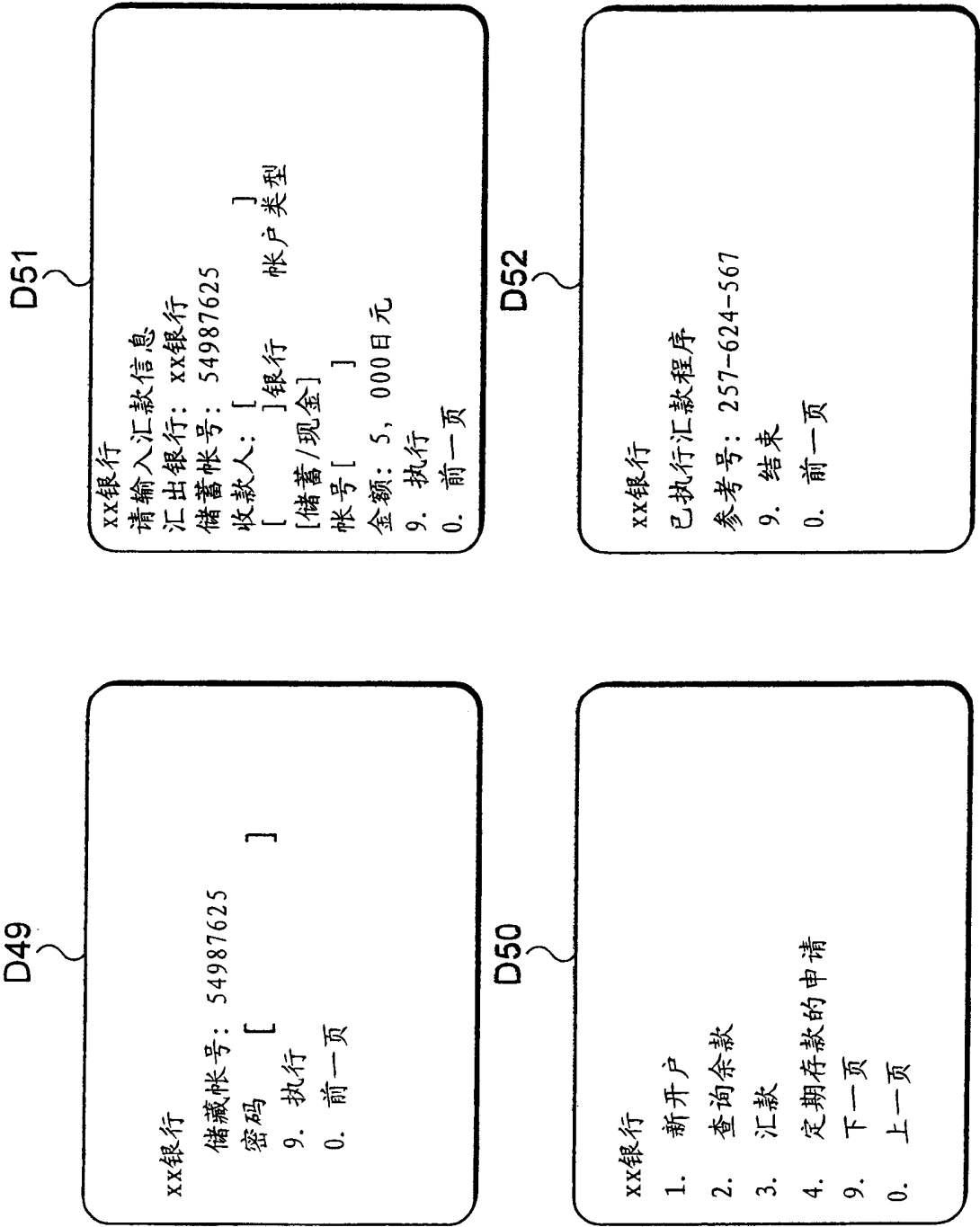


图 29

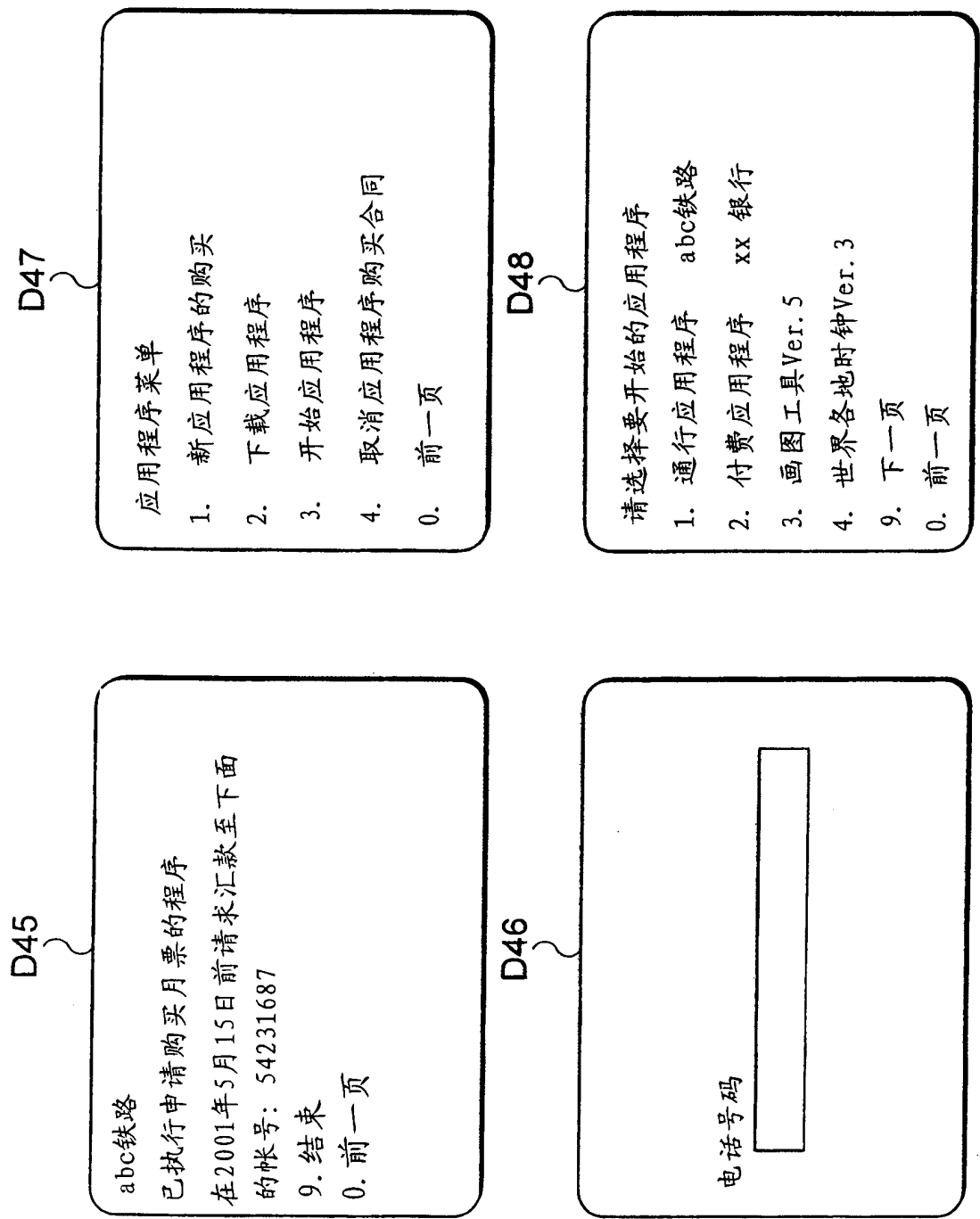


图 28

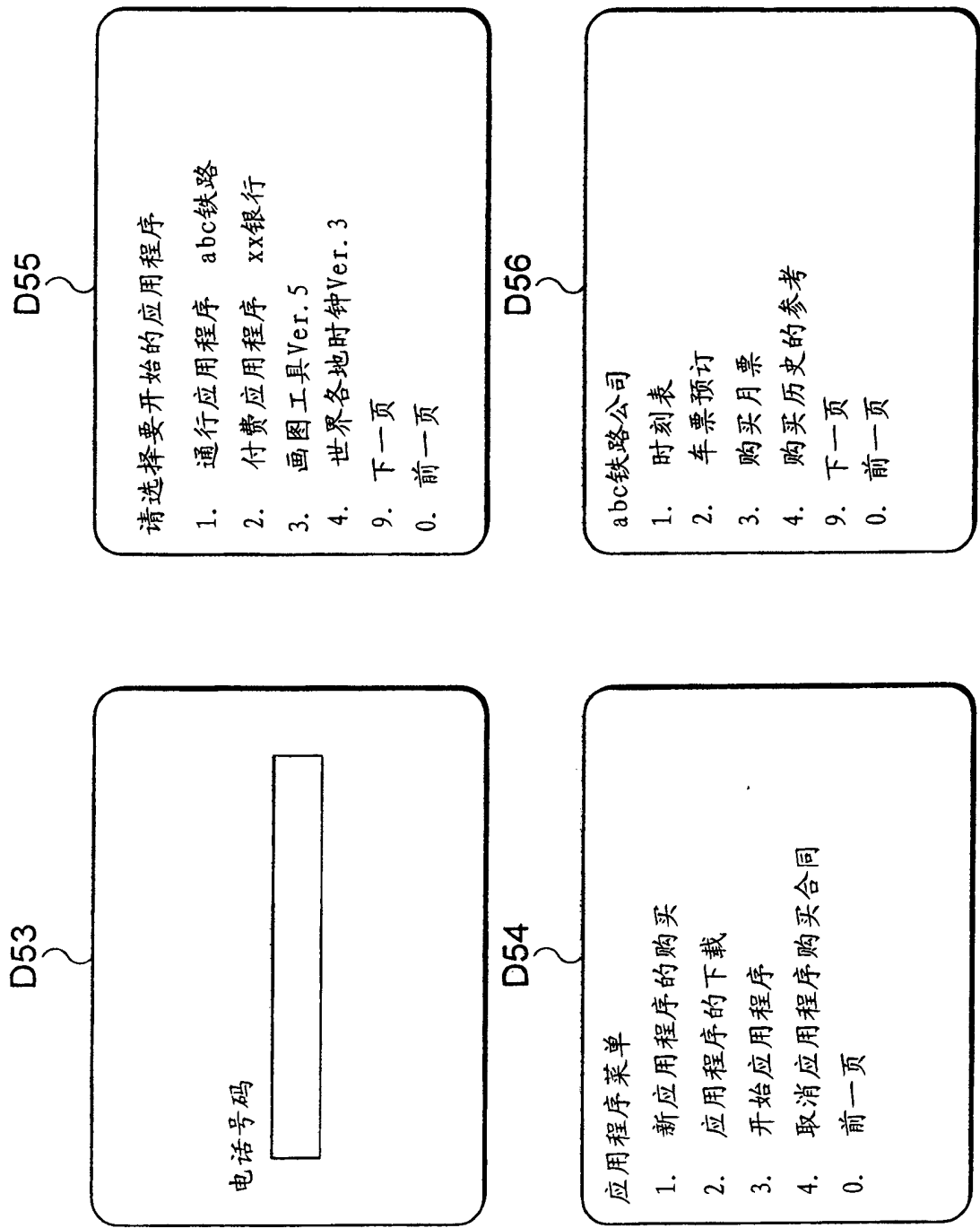


图 30

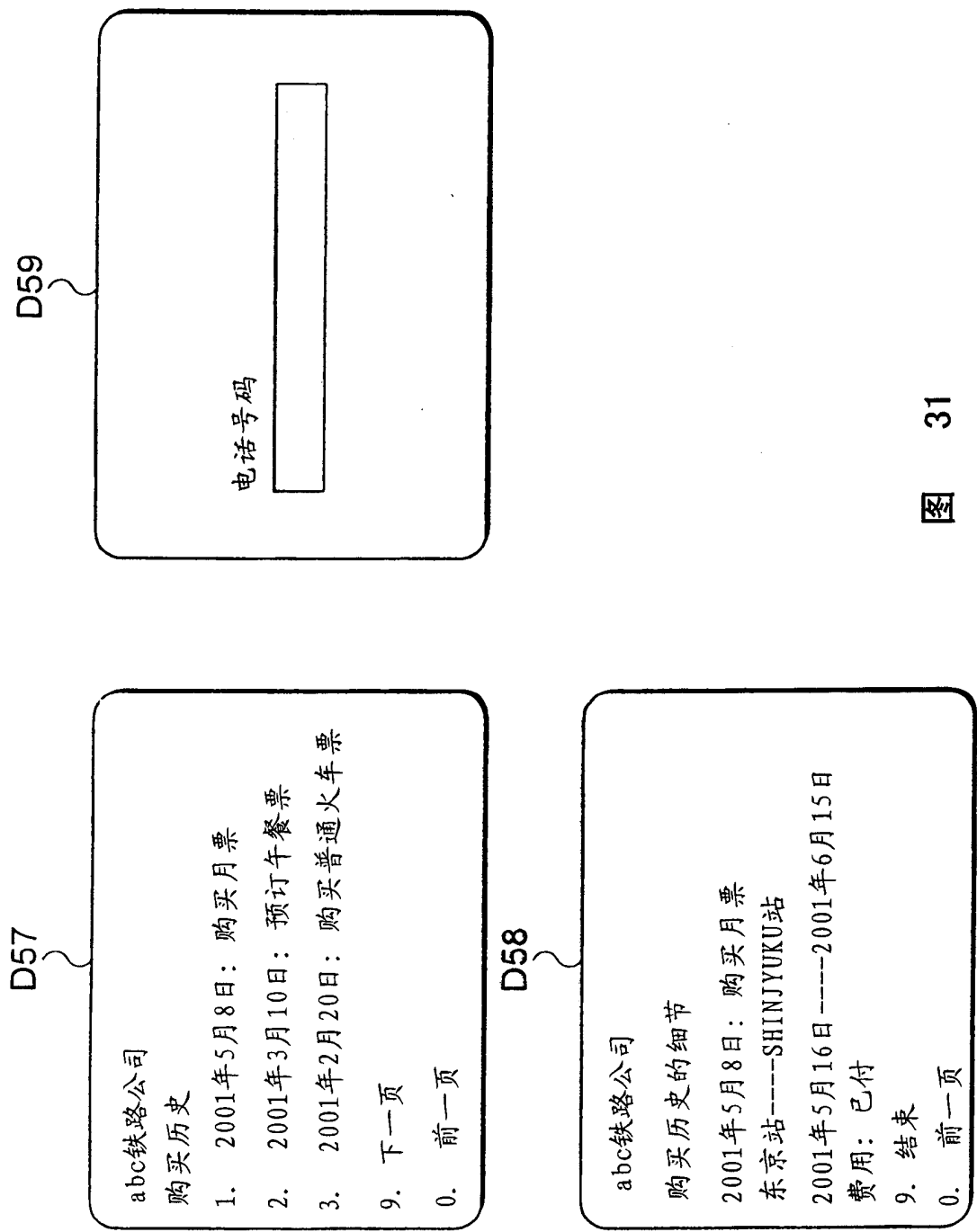


图 31

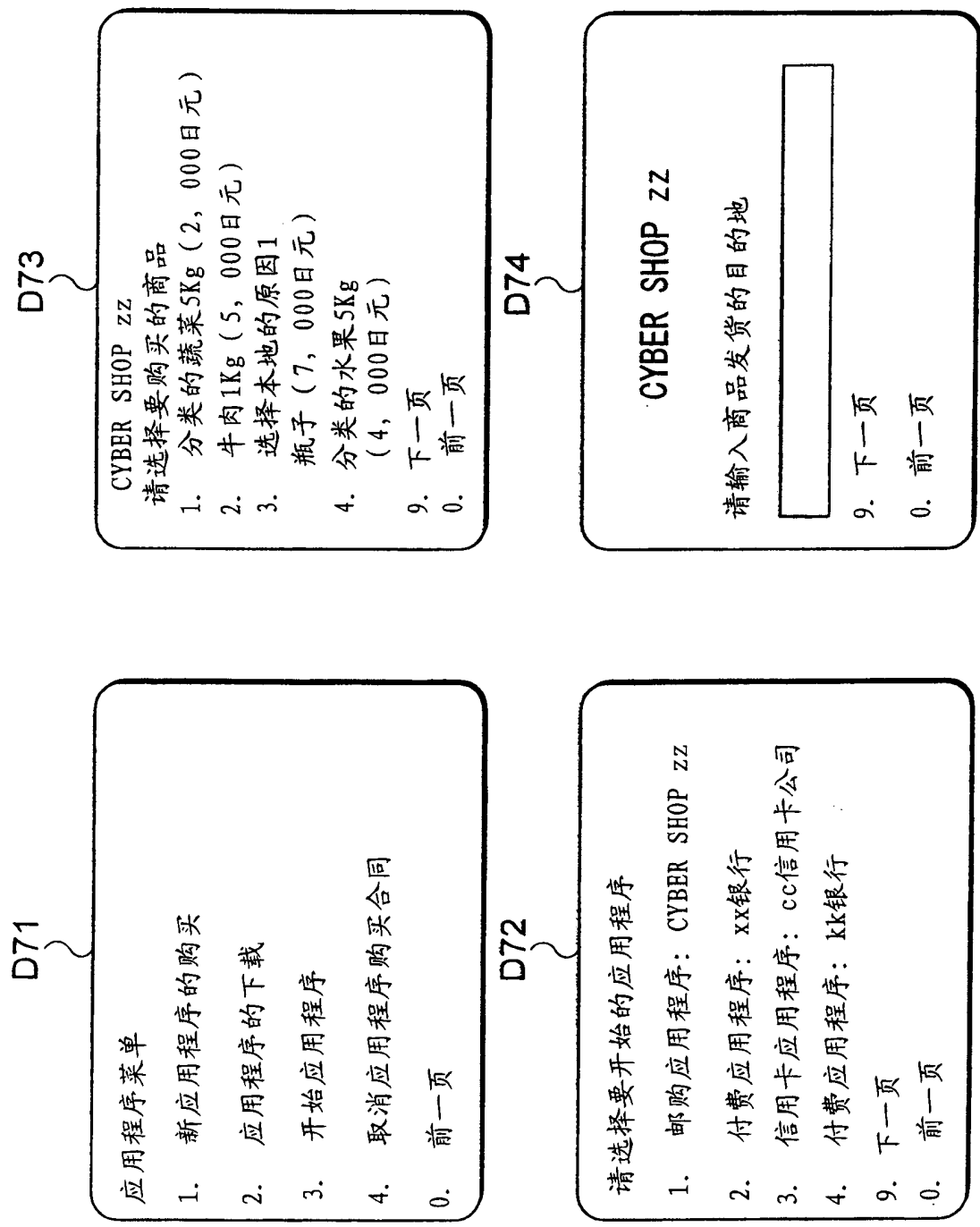


图 32

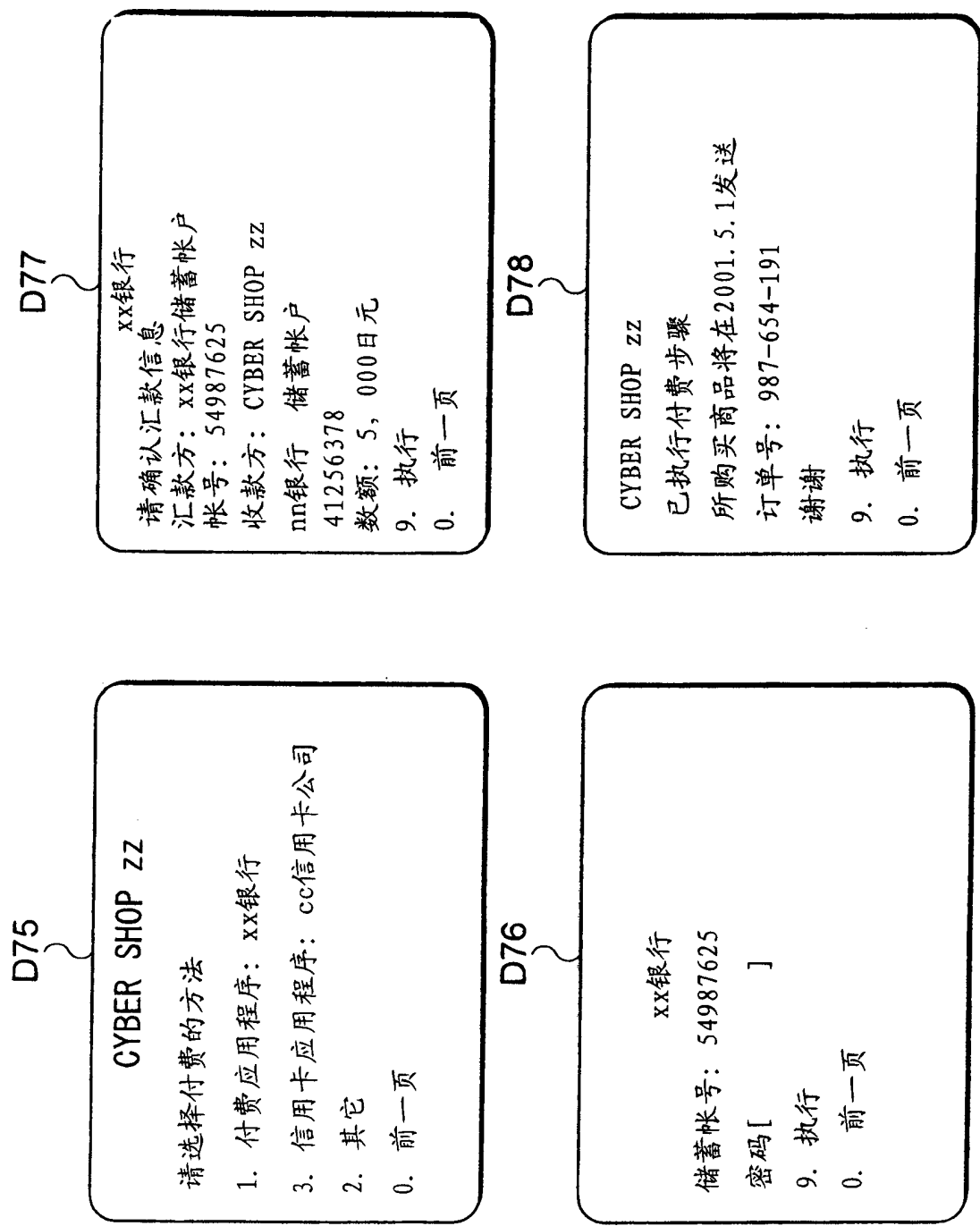


图 33

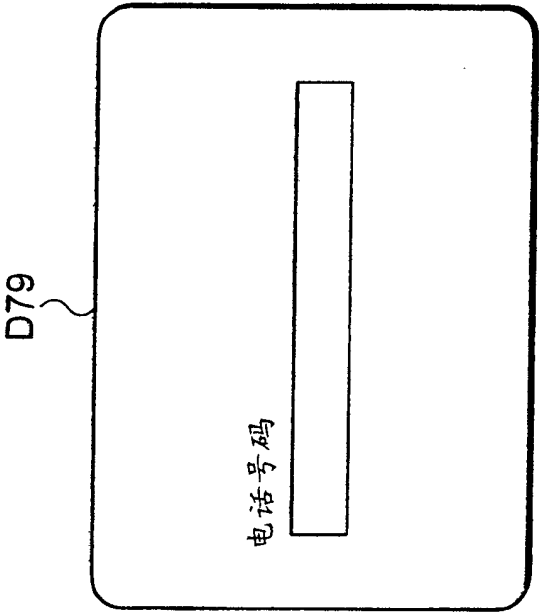


图 34

来自AP-3568的请求				至AP-3568的请求			
读出应用程序	读出数据	编辑数据	删除数据	读出应用程序	读出数据	编辑数据	删除数据
AP-3712	AP-8125	AP-1346	AP-2349	AP-4315	AP-1523	AP-2349	AP-3125
AP-0123	AP-5724	AP-2349	AP-1272	AP-2349	AP-0312	AP-8125	AP-6789
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

图 35

应用程序标识号	可靠性指数				公布	费用的征收	存储位置信息
	读出应用程序	读出数据	编辑数据	删除数据			
AP-2568	AP-4315	AP-1523	AP-2349	AP-3125	是	是	应用程序本身被存储
	AP-2349	AP-0312	AP-8125	AP-6789			
	⋮	⋮	⋮	⋮			
AP-3712	AP-2436	AP-1297	AP-2635	AP-3251	是	否	ftp://ftp.abc_software.com/application/ap_0306.exe
	AP-9870	AP-0879	AP-8187	AP-6789			
	⋮	⋮	⋮	⋮			
AP-4513	AP-9870	AP-9009	AP-7614	AP-1231	否	是	APPLICATION ITSELF IS STORED
	AP-1121	AP-0012	AP-8198	AP-6763			
	⋮	⋮	⋮	⋮			
AP-3021	AP-4121	AP-1231	AP-1213	AP-9809	否	否	ftp://ftp.software_world.com/software/app_view.exe
	AP-5454	AP-8192	AP-8125	AP-1265			
	⋮	⋮	⋮	⋮			
F-3251	—	—	—	—	—	—	ftp://ftp.softpocket.com/root/app/miracle.exe
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

图 36

应用程序标识号	可靠性指数	费用的征收	存储位置信息	
AP-2568	3	是	ftp://ftp.neonetwork.com/public/ apbinder.exe	信息摘要
AP-3712	5	否	ftp://ftp.abc_software.com/ application7ap_0306.exe	信息摘要
AP-4513	2	是	ftp://ftp.humantec.com/mobile/ application007.jar	信息摘要
AP-3021	1	否	ftp://ftp.software_world.com/ software/app_view.exe	信息摘要
F-3251	0	—	ftp://ftp.softpocket.com/root/ app/miracle.exe	信息摘要
⋮	⋮	⋮	⋮	⋮

图 37

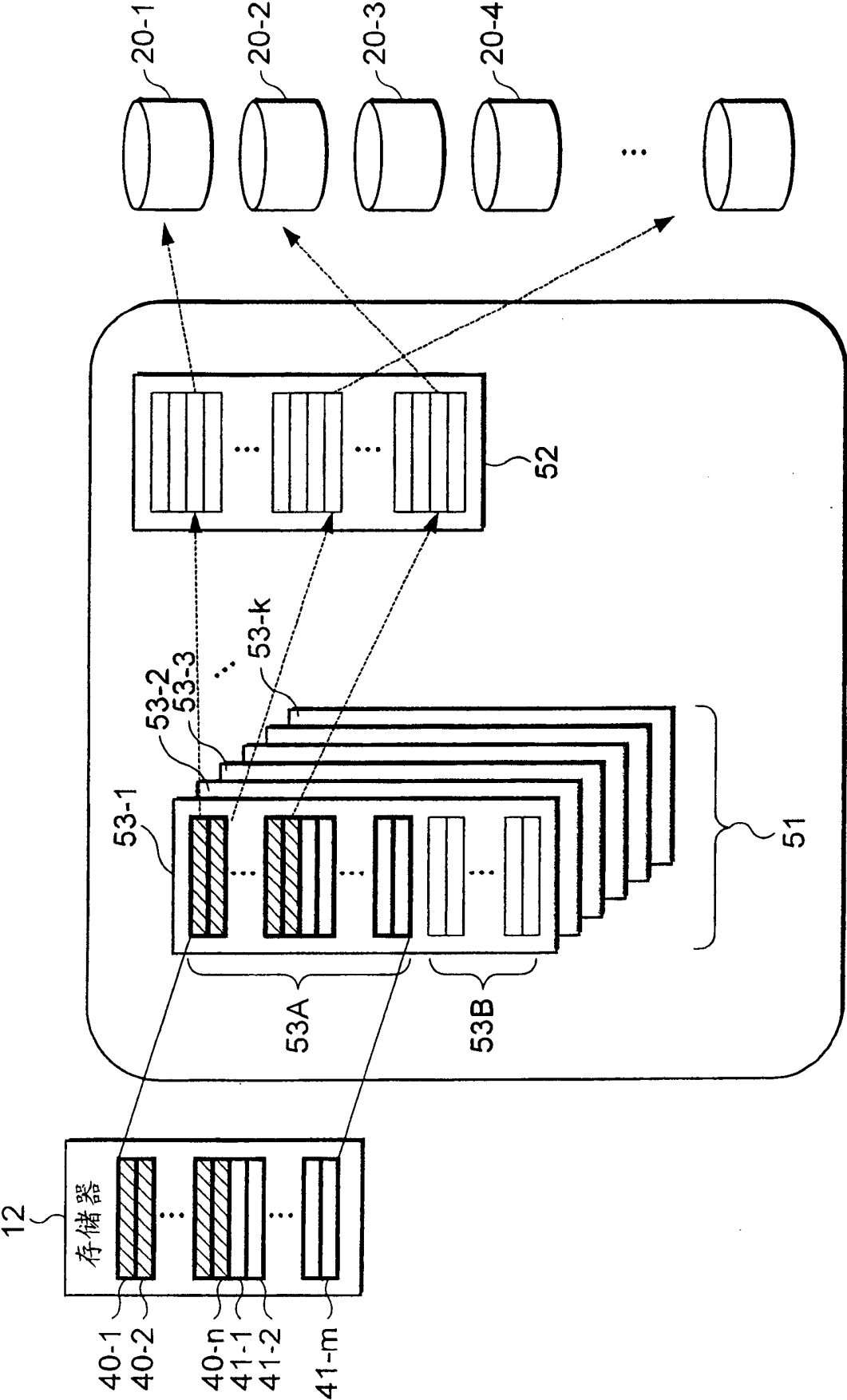


图 38

下载应用程序区	存储区		应用程序的信号	启动
	管理区	1	AP-2568	是
		2	AP-0123	否
		3	AP-1015	是
		⋮	⋮	⋮
		n	未使用	—
	自由区	1	F-0325	是
		2	F-7485	是
		3	未使用	—
		⋮	⋮	⋮
		m	未使用	—
准备下载应用程序	1	AP-4125	—	
	2	F-5963	—	
	3	AP-3021	—	
	4	AP-4513	—	
	5	未使用	—	
	6	未使用	—	
	7	未使用	—	
	8	未使用	—	
	9	未使用	—	
	⋮	⋮	⋮	

图 39

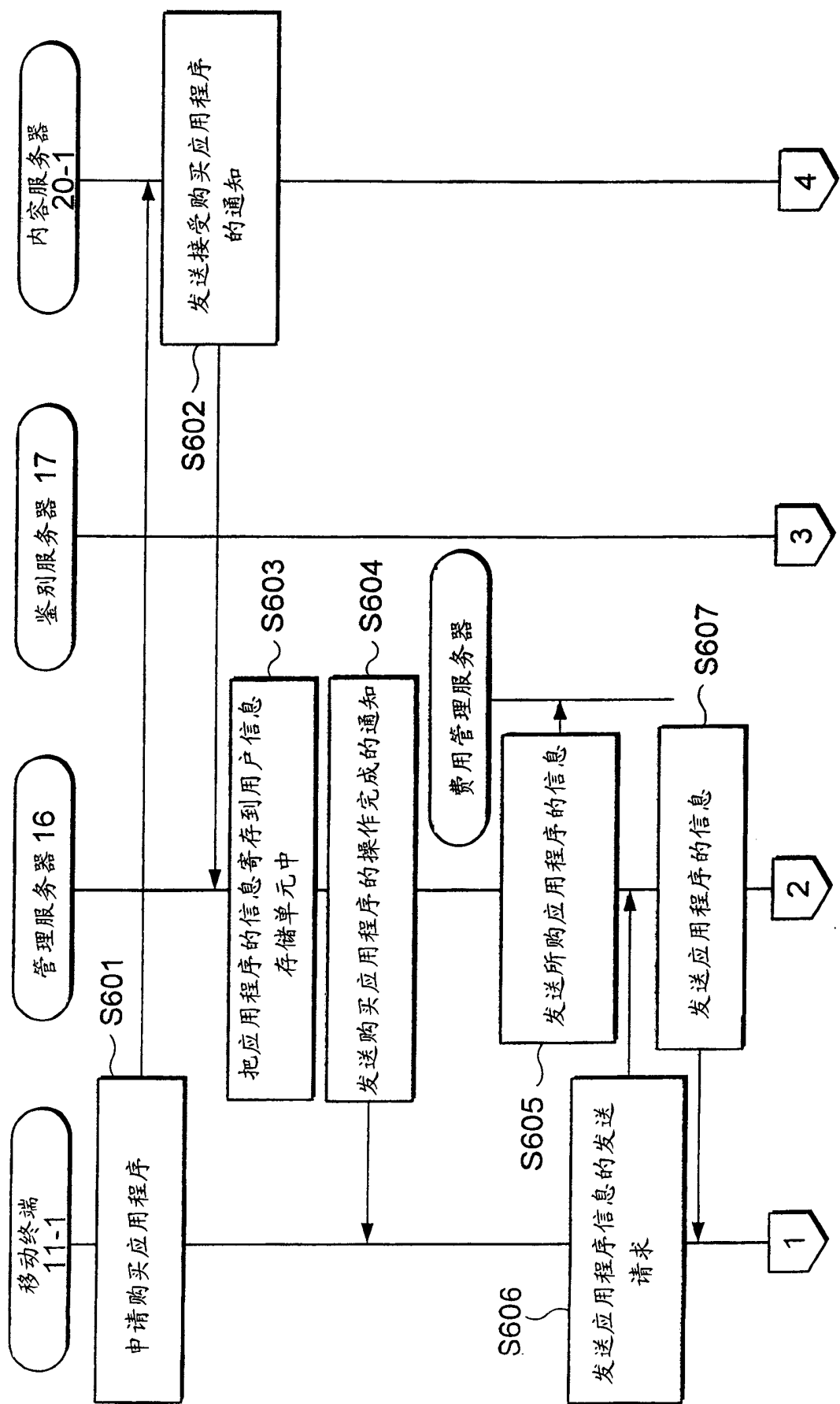


图 40

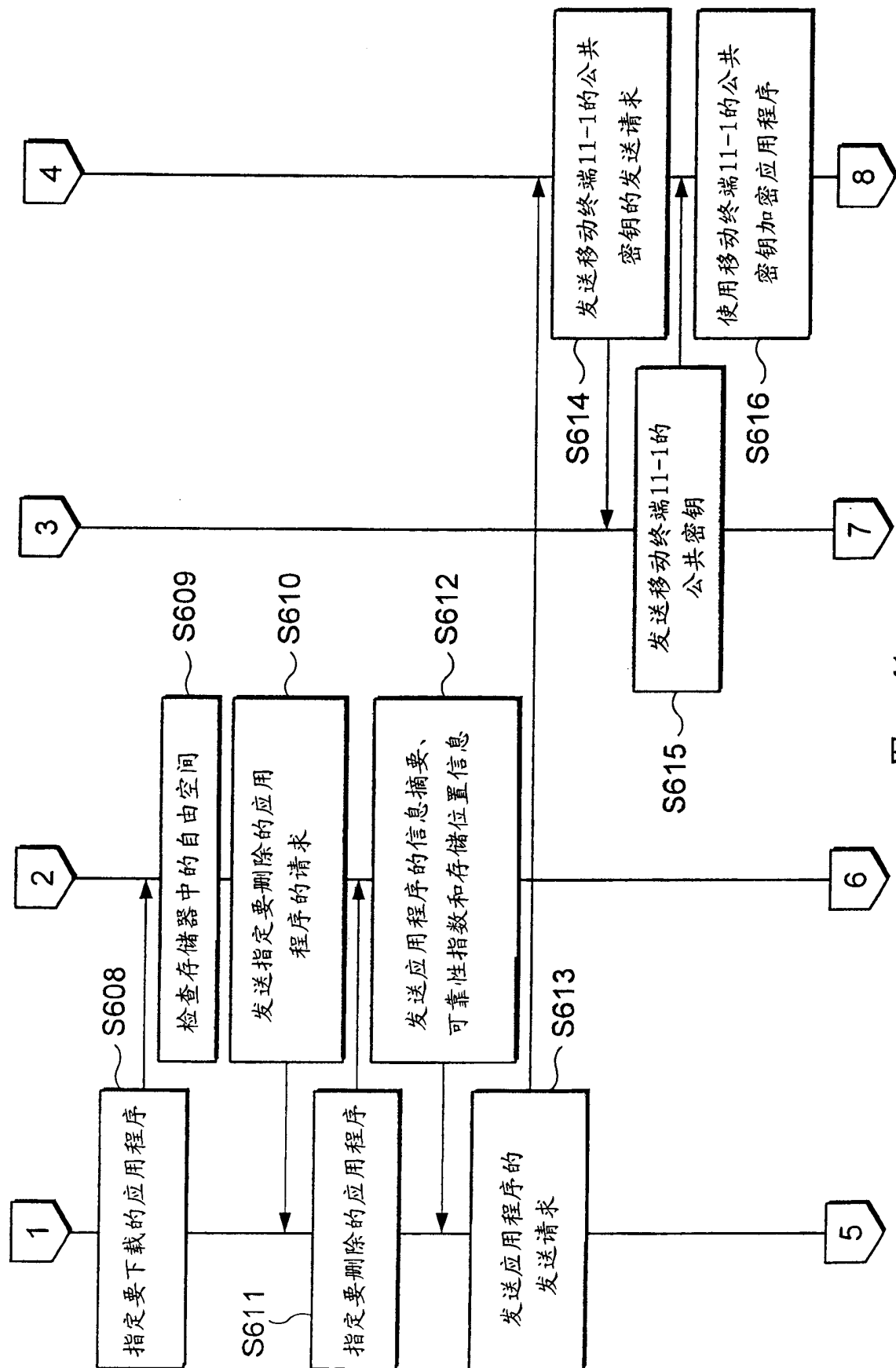


图 41

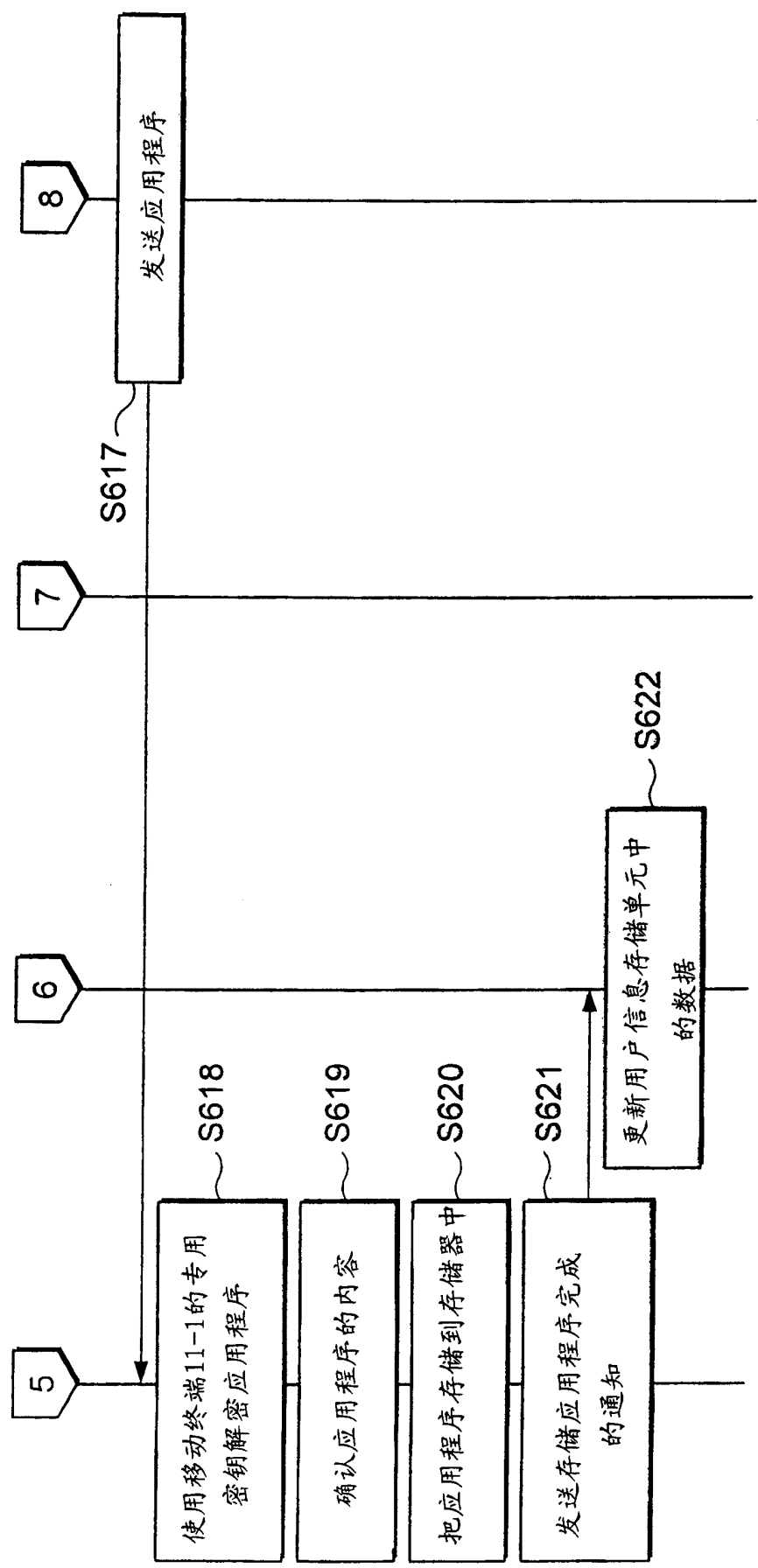


图 42