

[19] 中华人民共和国国家知识产权局



[12] 发明专利说明书

专利号 ZL 200310103074.X

[51] Int. Cl.

G06F 9/44 (2006.01)

G06F 12/14 (2006.01)

G06K 9/00 (2006.01)

H04L 9/00 (2006.01)

[45] 授权公告日 2006 年 4 月 12 日

[11] 授权公告号 CN 1251069C

[22] 申请日 2003.10.30

[21] 申请号 200310103074.X

[30] 优先权

[32] 2002.11.6 [33] JP [31] 323200/2002

[71] 专利权人 富士通株式会社

地址 日本神奈川县

[72] 发明人 小谷诚刚

审查员 胡徐兵

[74] 专利代理机构 北京东方亿思知识产权代理有限公司

代理人 杜娟 董方源

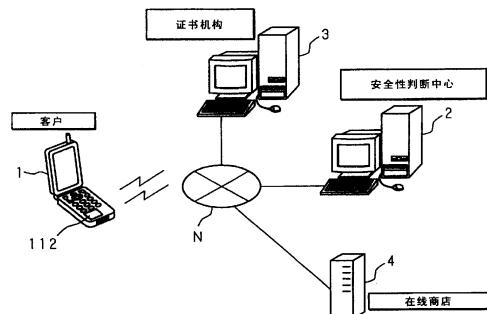
权利要求书 8 页 说明书 35 页 附图 37 页

[54] 发明名称

安全性判断方法

[57] 摘要

本发明提供安全性判断方法、系统和设备，第一认证设备，和计算机程序产品。通过进行生物信息认证和收集与信息处理设备（1）有关的环境信息，确保信息处理设备（1）的安全性。信息处理设备（1）将收集的环境信息发送到第一认证设备（2）。发送第二认证设备（3）发行的电子证书以及用第二认证设备（3）发行的秘密密钥加密的信息至第一认证设备（2）。第一认证设备获取第二认证设备（3）和信息处理设备（1）的公共密钥，解密加密信息，判断解密信息是否正确。第一认证设备（1）参考环境信息数据库和发送的信息，判断发送的环境信息是否正确。当生物信息认证、环境信息认证和电子证书认证的认证都成功时，判断信息处理设备（1）为安全的。



1. 一种安全性判断方法，用于在通过一个通信网络而被连接的信息处理设备、第一认证设备和第二认证设备当中判断所述信息处理设备的安全性，其特征在于包括如下步骤：

由所述信息处理设备接收生物信息；

由所述信息处理设备、所述第一认证设备或所述第二认证设备通过判断所接收的生物信息是否正确来认证所述生物信息；

收集包括与连接到所述信息处理设备的外围设备有关或与安装在所述信息处理设备中的软件有关的信息在内的环境信息；

将所收集的环境信息从所述信息处理设备发送到所述第一认证设备；

将由所述第二认证设备预先发行的电子证书和用由所述第二认证设备发行的秘密密钥加密的信息从所述信息处理设备发送到所述第一认证设备；

由所述第一认证设备使用一个公共密钥来解密所加密的信息并判断解密的信息是否正确来认证所述电子证书，其中所述公共密钥是通过使用从所述第二认证设备获取的公共密钥来从所发送的电子证书获取的；

由所述第一认证设备通过参考一个环境信息数据库和所发送的信息来判断所发送的环境信息是否正确来认证所述环境信息，其中所述环境信息数据库存储根据要发送和接收的信息而被划分等级的环境条件；以及

当在认证所述生物信息的步骤、认证所述环境信息的步骤和认证电子证书的步骤中所进行的所有认证都成功时，由所述第一认证设备判断所述信息处理设备是安全的。

2. 根据权利要求 1 的安全性判断方法，其特征在于还包括如下步骤：

由所述第一认证设备接收生物信息；

通过由所述信息处理设备、所述第一认证设备或所述第二认证设备判断所接收的生物信息是否正确来认证所述生物信息；

收集包括与连接到所述第一认证设备的外围设备有关或与安装在所述

第一认证设备中的软件有关的信息在内的环境信息；

用由所述第二认证设备发行的秘密密钥对在收集环境信息的所述子步骤中收集的环境信息进行加密；

将由所述第二认证设备发行的电子证书和加密的环境信息发送到所述  
5 信息处理设备；

由所述信息处理设备使用一个公共密钥来解密所加密的环境信息并判断所解密的环境信息是否正确来认证所述电子证书，其中所述公共密钥是通过使用从所述第二认证设备获取的公共密钥来从所发送的电子证书获取的；

10 由所述信息处理设备通过参考一个副环境信息数据库和所解密的环境信息来判断所发送的环境信息是否正确从而认证所述环境信息，其中所述副环境信息数据库存储根据要发送和接收的信息而被划分等级的环境条件；以及

15 当在认证所述生物信息的子步骤、认证所述环境信息的子步骤和认证电子证书的子步骤中所进行的所有认证都成功，并且在判断所述信息处理设备是安全的步骤中判断所述信息处理设备是安全的时，判断所述信息处理设备和第一认证设备是安全的。

3. 根据权利要求 1 的安全性判断方法，其特征在于还包括以下步骤：

由所述信息处理设备发送和接收与交易相关的信息；

20 由所述信息处理设备接收与交易相关的信息，所述信息包括产品信息或价格信息；

由所述信息处理设备将由所述第二认证设备发行的电子证书和用所述秘密密钥加密的与交易相关的信息发送到所述第一认证设备；

25 由所述第一认证设备根据所发送的环境信息与环境条件是否相匹配来判断所述环境条件是否正确，所述环境条件与对应于所发送的产品信息或价格信息的等级相关；以及

当所述第一认证设备判断所述信息处理设备是安全的时，将表示所述信息处理设备是安全的信息发送到所述购物计算机。

4. 根据权利要求 3 的安全性判断方法，其特征在于所述信息处理设备

包括供应主电源的主电源供应装置；以及供应用于接收所述电子证书和用所述秘密密钥加密的软件的副电源的副电源供应装置，

所述方法还包括以下步骤：当所述主电源供应装置不供应所述主电源时，通过从所述副电源供应装置供应副电源，由所述信息处理设备接收所  
5 发送的电子证书和用所述秘密密钥加密的软件。

5. 根据权利要求 4 的安全性判断方法，其特征在于还包括以下步骤：由所述信息处理设备用一个公共密钥解密所加密的软件，所述公共密钥是通过使用从所述第二认证设备获取的公共密钥来从所述电子证书获取的；以及当由所述主电源供应装置供应电源时，由所述信息处理设备判断所解  
10 密的软件是否正确。

6. 根据权利要求 5 的安全性判断方法，其特征在于所述软件是用于预安装在所述信息处理设备中的软件的补丁软件。

7. 根据权利要求 5 的安全性判断方法，其特征在于还包括以下步骤：当执行所安装的软件时，在一个预定时刻和该时刻之后删除由所述信息处  
15 理设备存储的数据。

8. 一种安全性判断方法，用于在通过一个通信网络而被连接的信息处理设备、第一认证设备和第二认证设备当中判断所述信息处理设备的安全性，其特征在于包括如下步骤：

由信息处理设备（1）接收生物信息；

20 通过由所述信息处理设备（1）、所述第一认证设备（2）或所述第二认证设备（3）判断所接收的生物信息是否正确来认证所述生物信息；

收集包括与连接到所述信息处理设备（1）的外围设备有关或与安装在所述信息处理设备（1）中的软件有关的信息在内的环境信息；

用由所述第二认证设备（3）发行的秘密密钥对所收集的环境信息进  
25 行加密；

将由所述第二认证设备（3）所预先发行的电子证书和用所述秘密密钥加密的环境信息从所述信息处理设备（1）发送到所述第一认证设备（2）；

由所述第一认证设备（2）用一个公共密钥来解密所加密的环境信息

并判断解密的环境信息是否正确来认证所述电子证书，其中所述公共密钥是通过使用从所述第二认证设备（3）获取的公共密钥来从所发送的电子证书所获取的；

由所述第一认证设备（2）通过参考一个环境信息数据库（251）和所发送的信息来判断所解密的环境信息是否正确从而认证所述环境信息，其中所述环境信息数据库（251）存储根据要发送和接收的信息而被划分等级的环境条件；以及

当在认证所述生物信息的步骤、认证所述环境信息的步骤和认证电子证书的步骤中所进行的所有认证都成功时，由所述第一认证设备（2）判断所述信息处理设备（1）是安全的。

9. 根据权利要求 8 的安全性判断方法，其特征在于还包括如下步骤：

由所述第一认证设备（2）接收生物信息；

通过由所述信息处理设备（1）、所述第一认证设备（2）或所述第二认证设备（3）判断所接收的生物信息是否正确来认证所述生物信息；

收集包括与连接到所述第一认证设备（2）的外围设备有关或与安装在所述第一认证设备（2）中的软件有关的信息在内的环境信息；

用由所述第二认证设备（3）发行的秘密密钥对在收集环境信息的所述子步骤中收集的环境信息进行加密；

将由所述第二认证设备（3）发行的电子证书和加密的环境信息发送到所述信息处理设备（1）；

由所述信息处理设备（1）使用一个公共密钥来解密所加密的环境信息并判断所解密的环境信息是否正确来认证所述电子证书，其中所述公共密钥是通过使用从所述第二认证设备（3）获取的公共密钥来从所发送的电子证书获取的；

由所述信息处理设备（1）通过参考一个副环境信息数据库（151）和所解密的环境信息来判断所发送的环境信息是否正确从而认证所述环境信息，其中所述副环境信息数据库（151）存储根据要发送和接收的信息而被划分等级的环境条件；以及

当在认证所述生物信息的子步骤、认证所述环境信息的子步骤和认证电子证书的子步骤中所进行的所有认证都成功，并且在判断所述信息处理设备（1）是安全的步骤中判断所述信息处理设备（1）是安全的时，判断所述信息处理设备（1）和第一认证设备（2）是安全的。

5 10. 根据权利要求 8 的安全性判断方法，其特征在于还包括以下步骤：

由所述信息处理设备发送和接收与交易相关的信息；

由所述信息处理设备接收与交易相关的信息，所述信息包括产品信息或价格信息；

10 由所述信息处理设备将由所述第二认证设备发行的电子证书和用所述秘密密钥加密的与交易相关的信息发送到所述第一认证设备；

由所述第一认证设备根据所发送的环境信息与环境条件是否相匹配来判断所述环境条件是否正确，所述环境条件与对应于所发送的产品信息或价格信息的等级相关；以及

15 当所述第一认证设备判断所述信息处理设备是安全的时，将表示所述信息处理设备是安全的信息发送到所述购物计算机。

11. 根据权利要求 10 的安全性判断方法，其特征在于所述信息处理设备包括供应主电源的主电源供应装置；以及供应用于接收所述电子证书和用所述秘密密钥加密的软件的副电源的副电源供应装置，

20 所述方法还包括以下步骤：当所述主电源供应装置不供应所述主电源时，通过从所述副电源供应装置供应副电源，由所述信息处理设备接收所发送的电子证书和用所述秘密密钥加密的软件。

12. 根据权利要求 11 的安全性判断方法，其特征在于还包括以下步骤：由所述信息处理设备用一个公共密钥解密所加密的软件，所述公共密钥是通过使用从所述第二认证设备获取的公共密钥来从所述电子证书获取的；以及当由所述主电源供应装置供应电源时，由所述信息处理设备判断所解密的软件是否正确。

13. 根据权利要求 12 的安全性判断方法，其特征在于所述软件是用于预安装在所述信息处理设备中的软件的补丁软件。

14. 根据权利要求 12 的安全性判断方法，其特征在于还包括以下步骤：当执行所安装的软件时，在一个预定时刻和该时刻之后删除由所述信息处理设备存储的数据。

15. 一种安全性判断方法，用于在通过一个通信网络而被连接的信息  
5 处理设备、第一认证设备和第二认证设备当中判断所述信息处理设备的安全性，其特征在于包括如下步骤：

由所述信息处理设备（1）接收生物信息；

由所述信息处理设备（1）、所述第一认证设备（2）或所述第二认证设备（3）通过判断所接收的生物信息是否正确来认证所述生物信息；

10 收集包括与连接到所述信息处理设备（1）的外围设备有关或与安装在所述信息处理设备（1）中的软件有关的信息在内的环境信息；

将所收集的环境信息从所述信息处理设备（1）发送到所述第一认证设备（2）；

15 将由所述第二认证设备（3）所预先发行的电子证书和用由所述第二认证设备（3）发行的秘密密钥所加密的信息从所述信息处理设备（1）发送到所述第一认证设备（2）；

由所述第一认证设备（2）通过参考一个环境信息数据库（251）来判断所发送的环境信息是否正确从而认证所述环境信息，其中所述环境信息数据库（251）存储根据要发送和接收的信息而被划分等级的环境条件；

20 由所述信息处理设备（1）通过使用一个公共密钥来解密所加密的软件并判断所解密的软件是否正确来认证所述电子证书，其中所述公共密钥是通过使用从所述第二认证设备（3）获取的公共密钥来从所发送的电子证书获取的；以及

25 当在认证所述生物信息的步骤、认证所述环境信息的步骤和认证所述电子证书的步骤中所进行的所有认证都成功时，在所述信息处理设备（1）中安装所解密的软件。

16. 根据权利要求 15 的安全性判断方法，其特征在于还包括以下步骤：

由所述信息处理设备发送和接收与交易相关的信息；

由所述信息处理设备接收与交易相关的信息，所述信息包括产品信息或价格信息；

由所述信息处理设备将由所述第二认证设备发行的电子证书和用所述秘密密钥加密的与交易相关的信息发送到所述第一认证设备；

5 由所述第一认证设备根据所发送的环境信息与环境条件是否相匹配来判断所述环境条件是否正确，所述环境条件与对应于所发送的产品信息或价格信息的等级相关；以及

当所述第一认证设备判断所述信息处理设备是安全的时，将表示所述信息处理设备是安全的信息发送到所述购物计算机。

10 17. 根据权利要求 16 的安全性判断方法，其特征在于所述信息处理设备包括供应主电源的主电源供应装置；以及供应用于接收所述电子证书和用所述秘密密钥加密的软件的副电源的副电源供应装置，

所述方法还包括以下步骤：当所述主电源供应装置不供应所述主电源时，通过从所述副电源供应装置供应副电源，由所述信息处理设备接收所15 发送的电子证书和用所述秘密密钥加密的软件。

18. 根据权利要求 17 的安全性判断方法，其特征在于还包括以下步骤：由所述信息处理设备用一个公共密钥解密所加密的软件，所述公共密钥是通过使用从所述第二认证设备获取的公共密钥来从所述电子证书获取的；以及当由所述主电源供应装置供应电源时，由所述信息处理设备判断20 所解密的软件是否正确。

19. 根据权利要求 18 的安全性判断方法，其特征在于所述软件是用于预安装在所述信息处理设备中的软件的补丁软件。

20. 根据权利要求 18 的安全性判断方法，其特征在于还包括以下步骤：当执行所安装的软件时，在一个预定时刻和该时刻之后删除由所述信25 息处理设备存储的数据。

21. 根据权利要求 1 到权利要求 20 中任何之一的安全性判断方法，其特征在于所述环境信息包括与所安装的软件的名称或版本，所连接的外围设备的设备名或版本，或所述信息处理设备的设备名或版本有关的信息。

22. 根据权利要求 1 到权利要求 20 中任何之一的安全性判断方法，其

---

特征在于所述生物信息是与语音、指纹、视网膜或虹膜有关的信息。

## 安全性判断方法

### 5 技术领域

本发明涉及安全性判断方法，用于在通过一个通信网络而被连接的信息处理设备、第一认证设备和第二认证设备当中判断所述信息处理设备的安全性，更具体地说，本发明涉及一种被包含到诸如移动电话、家庭电子设备以及个人计算机的信息处理设备内的安全性判断方法，以判断该信息  
10 处理设备的安全性。

### 背景技术

随着 IPv6（因特网协议第 6 版）的采用，不仅是个人计算机、服务器  
计算机和移动电话，就连家庭电子设备如冰箱、微波炉、空调、电视和  
15 DVD 设备、复印机以及其他自动化设备等，也都作为信息处理设备而被连  
接到通信网络如因特网，并发送和接收信息。随着这种连接到通信网络的  
信息处理设备在数量上的增加，安全性降低了。

具体地说，由于家庭电子设备的安全性低，就会出现从外部设备发送  
过来会妨碍家庭电子设备正常运行的程序的情况，并且人们担心家庭电子  
20 设备被用作 DDoS（分布式拒绝服务）的手段。因此，为了提高这些信息  
处理设备的安全性，人们尝试为信息处理设备配备使用指纹等的生物特征  
认证功能（例如参见日本专利申请特开 No.3-58174/1991）。

然而，有一个问题，即只通过生物特征认证难于确保高度安全性，因  
为用于认证的指纹信息可能会泄漏。具体地说，当通过使用这种信息处理  
25 设备来进行电子交易时，希望能在通过如下方式来确保安全性后才进行交  
易，即确认信息处理设备是否为适当的所有者所使用，交易是否是使用所有  
者自己的信息处理设备来进行，可能会损害安全性的设备或诸如 OS  
（操作系统）软件、浏览器和插件软件的软件是否被连接到或安装在信息  
处理设备当中等等。

而且，当为这种信息处理设备提供补丁软件或固件时，需要在发送信息的设备和所述信息处理设备之间确保足够的安全性，因为存在正在被发送的软件可能被第三人所伪造的风险。另一方面，当安全性级别被提高得太高时，会难于进行信息的顺利发送和接收。

5

## 发明内容

本发明目标在于解决上述问题，并且本发明的一个目的在于提供安全性判断方法，其能够通过将使用生物信息的认证、使用由证书机构（PKI 认证：公共密钥基础设施认证）发行的电子证书的认证以及利用信息处理设备所被使用的环境的等级的使用环境信息的认证三者结合起来，从而提高安全性，并能够在确保合适的安全性之后顺利地进行信息地发送和接收。

10

根据本发明的第一方面，提供一种安全性判断方法，用于在通过一个通信网络而被连接的信息处理设备、第一认证设备和第二认证设备当中判断所述信息处理设备的安全性，其特征在于包括如下步骤：由所述信息处理设备接收生物信息；由所述信息处理设备、第一认证设备或第二认证设备通过判断所接收的生物信息正确与否来认证所述生物信息；收集包括与连接到该信息处理设备的外围设备有关或与安装在该信息处理设备中的软件有关的信息在内的环境信息；将所收集的环境信息从所述信息处理设备发送到第一认证设备；将由第二认证设备所预先发行的电子证书和用由第二认证设备发行的秘密密钥所加密的信息从所述信息处理设备发送到第一认证设备；由第一认证设备使用一个公共密钥来解密所加密的信息并判断解密的信息是否正确来认证所述电子证书，其中所述公共密钥是通过使用从第二认证设备获取的公共密钥来从所发送的电子证书获取的；由第一认证设备通过参考一个环境信息数据库和所发送的信息来判断所发送的环境信息是否正确从而认证所述环境信息，其中所述环境信息数据库存储根据要发送和接收的信息而被划分等级的环境条件；以及当在认证所述生物信息的步骤、认证所述环境信息的步骤和认证电子证书的步骤中所进行的所有认证都成功时，由第一认证设备判断所述信息处理设备是安全的。

15

20

25

根据本发明的第二方面，提供一种安全性判断方法，用于在通过一个通信网络而被连接的信息处理设备、第一认证设备和第二认证设备当中判断所述信息处理设备的安全性，其特征在于包括如下步骤：由信息处理设备接收生物信息；通过由所述信息处理设备、第一认证设备或第二认证设备判断所接收的生物信息是否正确来认证所述生物信息；收集包括与连接到该信息处理设备的外围设备有关或与安装在该信息处理设备中的软件有关的信息在内的环境信息；用由第二认证设备发行的秘密密钥对所收集的环境信息进行加密；将由第二认证设备所预先发行的电子证书和用所述秘密密钥加密的环境信息从所述信息处理设备发送到第一认证设备；通过由第一认证设备用一个公共密钥来解密所加密的环境信息并判断解密的环境信息是否正确来认证所述电子证书，其中所述公共密钥是通过使用从第二认证设备获取的公共密钥来从所发送的电子证书所获取的；由第一认证设备通过参考一个环境信息数据库和所发送的信息来判断所解密的环境信息是否正确从而认证所述环境信息，其中所述环境信息数据库存储根据要发送和接收的信息而被划分等级的环境条件；以及当在认证所述生物信息的步骤、认证所述环境信息的步骤和认证电子证书的步骤中所进行的所有认证都成功时，由第一认证设备判断所述信息处理设备是安全的。

根据本发明的第三方面，在本发明的第一和第二方面中，所述安全性判断方法特征在于还包括如下子步骤：由第一认证设备接收生物信息；通过由所述信息处理设备、第一认证设备或第二认证设备判断所接收的生物信息是否正确来认证所述生物信息；收集包括与连接到第一认证设备的外围设备有关或与安装在第一认证设备中的软件有关的信息在内的环境信息；用由第二认证设备发行的秘密密钥对在收集所述环境信息子步骤中收集的环境信息进行加密；将由第二认证设备发行的电子证书和加密的环境信息发送到信息处理设备；由所述信息处理设备使用一个公共密钥来解密所加密的环境信息并判断解密的环境信息是否正确来认证所述电子证书，其中所述公共密钥是通过使用从第二认证设备获取的公共密钥来从所发送的电子证书获取的；由所述信息处理设备通过参考一个副环境信息数据库和所解密的环境信息来判断所发送的环境信息是否正确从而认证所述环境

信息，其中所述副环境信息数据库存储根据要发送和接收的信息而被划分等级的环境条件；以及当在认证所述生物信息的子步骤、认证所述环境信息的子步骤和认证电子证书的子步骤中所进行的所有认证都成功，并且在判断信息处理设备是安全的步骤中判断所述信息处理设备是安全的时，  
5 判断所述信息处理设备和第一认证设备是安全的。

根据本发明的第四方面，提供一种安全性判断方法，用于在通过一个通信网络而被连接的信息处理设备、第一认证设备和第二认证设备当中判断所述信息处理设备的安全性，其特征在于包括如下步骤：由所述信息处理设备接收生物信息；由所述信息处理设备、第一认证设备或第二认证设备通过判断所接收的生物信息是否正确来认证所述生物信息；收集包括与连接到该信息处理设备的外围设备有关或与安装在该信息处理设备中的软件有关的信息在内的环境信息；将所收集的环境信息从所述信息处理设备发送到第一认证设备；将由第二认证设备所预先发行的电子证书和用由第二认证设备发行的秘密密钥所加密的信息从所述信息处理设备发送到第一  
10 认证设备；由第一认证设备通过参考一个环境信息数据库来判断所发送的环境信息是否正确从而认证所述环境信息，其中所述环境信息数据库存储根据要发送和接收的信息而被划分等级的环境条件；由所述信息处理设备通过使用一个公共密钥来解密所加密的软件并判断解密的软件是否正确来  
15 认证所述电子证书，其中所述公共密钥是通过从第二认证设备获取的公共密钥来从所发送的电子证书获取的；以及当在认证所述生物信息的步骤、  
20 认证所述环境信息的步骤和认证所述电子证书的步骤中所进行的所有认证都成功时，在所述信息处理设备中安装所解密的软件。

根据本发明的第五方面，在本发明的第一、二和四方面中，所述安全性判断方法特征在于还包括以下步骤：由所述信息处理设备发送和接收与交易相关的信息；由所述信息处理设备接收与交易相关的信息，所述信息包括产品信息或价格信息；由所述信息处理设备将由所述第二认证设备发行的电子证书和用所述秘密密钥加密的与交易相关的信息发送到所述第一认证设备；由所述第一认证设备根据所发送的环境信息与环境条件是否相匹配来判断所述环境条件是否正确，所述环境条件与对应于所发送的产品  
25

信息或价格信息的等级相关；以及当所述第一认证设备判断所述信息处理设备是安全的时，将表示所述信息处理设备是安全的信息发送到所述购物计算机。

根据本发明的第六方面，在本发明的第五方面中，所述安全性判断方法特征在于所述信息处理设备包括供应主电源的主电源供应装置；以及供应用于接收所述电子证书和用所述秘密密钥加密的软件的副电源的副电源供应装置，所述方法还包括以下步骤：当所述主电源供应装置不供应所述主电源时，通过从所述副电源供应装置供应副电源，由所述信息处理设备接收所发送的电子证书和用所述秘密密钥加密的软件。

根据本发明的第七方面，在本发明的第六方面中，所述安全性判断方法特征在于还包括以下步骤：由所述信息处理设备用一个公共密钥解密所加密的软件，所述公共密钥是通过使用从所述第二认证设备获取的公共密钥来从所述电子证书获取的；以及当由所述主电源供应装置供应电源时，由所述信息处理设备判断所解密的软件是否正确。

根据本发明的第八方面，在本发明的第七方面中，所述安全性判断方法特征在于所述软件是用于预安装在所述信息处理设备中的软件的补丁软件。

根据本发明的第九方面，在本发明的第七方面中，所述安全性判断方法特征在于还包括以下步骤：当执行所安装的软件时，在一个预定时刻和该时刻之后删除由所述信息处理设备存储的数据。

根据本发明的第十方面，在本发明的第一到第九方面的任何之一中，所述环境信息包括与所安装的软件的名称或版本、所连接的外围设备的设备名或版本、或者所述信息处理设备的设备名或版本有关的信息。

根据本发明的第十一方面，在本发明的第一到第九方面的任何之一中，所述生物信息是与语音、指纹、视网膜或虹膜有关的信息。

如上所述，根据本发明，接收例如用户的指纹的生物信息，并判断所接收的生物信息正确与否。而且，收集环境信息，包括与连接到所述信息处理设备的外围设备或安装在所述信息处理设备中的软件有关的信息。更具体地说，所述信息处理设备自身的设备名和版本、连接到所述信息处理

设备的设备的名称和所安装的浏览器名称、OS 名和版本都对应于所述环境信息。信息处理设备将所收集的环境信息发送到第一认证设备。

而且，由第二认证设备如第三人所有的证书机构发行的电子证书和与交易相关的、用所述信息处理设备的秘密密钥加密的信息被发送到第一认证设备。<sup>5</sup>当第一认证设备接收到所述电子证书和所加密的信息时，它通过使用从第二认证设备（证书机构）获取的公共密钥来从所发送的电子证书中获取信息处理设备的公共密钥。然后，第一认证设备用所获取的信息处理设备的公共密钥来解密所述加密信息，并通过使用消息摘要等来判断所解密的信息是否正确。

第一认证设备参考一个环境信息数据库和所发送的信息来判断所发送的环境信息是否正确，其中所述环境信息数据库存储根据要发送和接收的信息而被划分等级的环境信息的条件。具体地说，当需要对要发送和接收的信息确保高安全性时，信息处理设备的环境信息需要满足更严格（更高等级）的环境条件。例如，在需要高的安全性的条件下（例如，股票和不低于¥50,000 的高价产品的交易），条件就是信息处理设备的 OS 必须具有最新的版本。当信息处理设备的 OS 是最新版本时，第一认证设备判断所述环境认证是成功的，然而，当信息处理设备的 OS 不是最新版本（是一个旧版本）时，第一认证设备判断所述环境认证不成功，因为这一 OS 可能有安全漏洞。<sup>10</sup>

另一方面，在低价产品的交易的情况下，由于需要确保方便性而不是安全性，因此不需要满足高等级条件。因此，即使安装了具有一些安全漏洞的旧版本的 OS，所述环境认证也被判断为成功。例如，在价格大约为¥100 的产品的交易的情况下，即使信息处理设备的 OS 是旧版本的，所述环境认证也被判断为成功。当由生物信息认证、环境信息认证和电子证书认证所进行的认证都被判断为成功时，信息处理设备被判断为安全的，<sup>15</sup>并且，例如设置一个表示信息处理设备是安全的标志，将表示信息处理设备是安全的信息发送到交易中涉及的购物计算机，并且然后在确保安全性之后进行信息在信息处理设备和购物计算机之间发送和接收。利用这一结构，可以在确保信息处理设备的安全性的同时实现信息的顺利发送和接收<sup>25</sup>

以及交易。而且，也在第一认证设备中进行生物信息认证、电子证书认证和环境认证，并且，只有当在信息处理设备中进行的生物信息认证、电子证书认证和环境认证以及第一认证设备中进行的生物信息认证、电子证书认证和环境认证都被判断为成功时，第一认证设备和信息处理设备才都被  
5 判断为正确的。因此可以确保更高的安全性。

另外，根据本发明，接收例如用户的指纹的生物信息，并且通过判断所接收的生物信息是否正确来进行个人认证。然后，如上所述，信息处理设备将所收集的环境信息发送到第一认证设备，并且在第一认证设备中进行环境信息的认证。在将补丁软件等从第一认证设备发送到信息处理设备的情况下，第一认证设备将由第二认证设备发行的电子证书和用由第二认证设备发行的秘密密钥加密的软件发送到信息处理设备。  
10

当信息处理设备接收到所述电子证书和加密的软件时，它向第二认证设备请求一个公共密钥，并通过使用这一证书机构的公共密钥来从所述电子证书获取第一认证设备的公共密钥。然后，信息处理设备用所获取公共  
15 密钥来解密所述加密的软件，并判断所解密的软件是否正确。最后，当由上述个人认证、环境认证和电子证书认证所进行的认证都被判断为成功时，在信息处理设备中安装所解密的软件。利用这样一种结构可以防止第三人的“欺骗”（spoofing），并在保持高度安全性的同时为信息处理设备提供例如补丁软件和固件的软件。

而且，根据本发明，所述信息处理设备包括主电源供应装置、副电源供应装置和被构造来从副电源供应装置接收电源供应的用于接收的通信装置。当不是由主电源供应装置供应电源即主电源不是开通（ON）的时，如果从第一认证设备发送来电子证书和用秘密密钥加密的软件，用于接收的通信装置就使用副电源供应装置来接收这些信息并存储它们。然后，当  
20 主电源供应装置供应电源时，读取所存储的电子证书和软件，判断所发送的软件是否正确，并进行个人认证和环境认证。因此可以在确保安全性之后发布大量补丁软件至客户，包括没有打开电源的客户。具体地说，对于所要提供的软件，当提供在预定时刻处和该预定时刻之后从存储单元删除  
25 所存储的数据的软件时，可以有效地防止将软件用作 DDoS 攻击的手段。

从下面的参照附图的详细说明中，本发明的上述和其他目的和特征将变得更加明显。

### 附图说明

- 5 图 1 是示出了根据本发明的安全性判断系统的概要的视图；  
图 2 是示出了一个移动电话的硬件结构的方框图；  
图 3 是示出了中心服务器的硬件结构的方框图；  
图 4 是环境信息 DB 的记录布局的说明性视图；  
图 5 是示出了在万维网服务器（Web Server）和移动电话之间的交易  
10 过程的流程图；  
图 6 是示出了一个网页的显示状态的说明性视图；  
图 7 是示出了一个安全性判断处理的过程的流程图；  
图 8 是示出了所述安全性判断处理的过程的流程图；  
图 9 是示出了所述安全性判断处理的过程的流程图；  
15 图 10 是示出了所述安全性判断处理的过程的流程图；  
图 11 是示出了所述安全性判断处理的过程的流程图；  
图 12 是示出了所述安全性判断处理的过程的流程图；  
图 13 是示出了根据实施例 2 的移动电话的硬件结构的方框图；  
图 14 是示出了根据实施例 3 的移动电话的硬件结构的方框图；  
20 图 15 是示出了根据实施例 3 的中心服务器的硬件结构的方框图；  
图 16 是示出了根据实施例 3 的安全性判断处理的过程的流程图；  
图 17 是示出了根据实施例 3 的安全性判断处理的过程的流程图；  
图 18 是示出了根据实施例 3 的安全性判断处理的过程的流程图；  
图 19 是示出了根据实施例 3 的安全性判断处理的过程的流程图；  
25 图 20 是示出了根据实施例 3 的安全性判断处理的过程的流程图；  
图 21 是示出了根据实施例 4 的移动电话的硬件结构的方框图；  
图 22 是示出了根据实施例 4 的中心服务器的硬件结构的方框图；  
图 23 是示出了根据实施例 4 的软件提供处理的过程的流程图；  
图 24 是示出了根据实施例 4 的软件提供处理的过程的流程图；

图 25 是示出了根据实施例 4 的软件提供处理的过程的流程图；  
图 26 是示出了根据实施例 4 的软件提供处理的过程的流程图；  
图 27 是示出了根据实施例 4 的软件提供处理的过程的流程图；  
图 28 是示出了根据实施例 4 的软件提供处理的过程的流程图；  
5 图 29 是示出了根据实施例 4 的软件提供处理的过程的流程图；  
图 30 是示出了所安装的删除软件的操作内容的流程图；  
图 31 是示出了根据实施例 5 的移动电话的硬件结构的方框图；  
图 32 是示出了根据实施例 6 的移动电话的硬件结构的方框图；  
图 33 是示出了根据实施例 6 的中心服务器的硬件结构的方框图；  
10 图 34 是示出了根据实施例 6 的认证处理的过程的流程图；  
图 35 是示出了根据实施例 6 的认证处理的过程的流程图；  
图 36 是示出了根据实施例 6 的认证处理的过程的流程图；并且  
图 37 是示出了根据实施例 6 的认证处理的过程的流程图。

## 15 具体实施方式

下面的说明将根据示出了优选实施例的附图来详细解释本发明。

### 实施例 1

实施例 1 示出了一种情况，其中信息处理设备是移动电话，而本发明的安全性判断系统被应用到使用移动电话的交易上。注意，所述信息处理设备不一定被限制为移动电话，而可以是个人计算机、复印机、打印机、  
20 传真机、冰箱、电视、设备、PDA（个人数字助理）、空调、微波炉、自动化设备等等。

图 1 是示出了根据本发明的安全性判断系统的概要的视图。在图 1 中，数字 1 是作为信息处理设备的移动电话，3 是作为发行电子证书的第  
25 三方的证书机构的第二认证设备（以后称为证书机构服务器），2 是中心服务器，作为是安全性判断中心的第一认证设备，用于判断移动电话 1 的安全性，而 4 是在线出售产品的在线商店的购物计算机（shop computer）（以后称为万维网服务器）。移动电话 1 通过一个移动电话网络（未示出）连接到通信网络（以后称为因特网）N，并且类似地，证书机构服务

器 3、中心服务器 2 和万维网服务器 4 被连接到因特网 N。移动电话 1 包括作为生物信息接收装置的指纹获取单元 112，并具有捕获通过将客户的指纹扫描到移动电话 1 中而获取的指纹信息的功能。

图 2 是示出了移动电话 1 的硬件结构的方框图。作为信息处理设备的 5 移动电话 1 包括移动电话引擎单元 110 和本发明的安全性判断设备 5，其中移动电话引擎单元 110 用于执行常规功能，例如通话功能和字符及图像数据的发送与接收。在实施例 1 中，安全性判断设备（以后称为安全性芯片）5 是 LSI（大规模集成电路）芯片并被安装在移动电话 1 中。

下面的说明将解释移动电话引擎单元 110 的硬件结构。如在图 2 中所示，10 RAM 12、ROM 15、天线单元 16、电源单元 113、麦克风和扬声器 111、AD/DA 转换器 20、外部连接器 19、诸如用于数据显示的液晶显示器的显示单元 14 以及输入单元 13（包括数字键、光标键以及选择与定义键）通过总线 17 连接到 CPU（中央处理单元）11。CPU 11 通过总线 17 连接到移动电话 1 的如上所述的各种硬件单元，控制这些硬件单元，并根据存储在 ROM 15 中的控制程序 15P 来执行各种软件功能。  
15

外部连接器 19 是由例如 16 根导线组成的接口，并通过 USB 电缆等连接到个人计算机或外围设备（都未示出）。RAM 12 由 SRAM（静态随机存取存储器）、快闪存储器等构成，并存储在软件执行期间创建的临时数据。ROM 15 由例如 EEPROM（电可擦可编程 ROM）构成，并存储提供 20 移动电话 1 的基本运行环境的 OS（操作系统）、控制连接到外部连接器 19 的外围设备的 BIOS（基本输入/输出系统）以及所下载或预安装的软件例如 Java®。

除了移动电话引擎单元 110 的输入单元 13 之外，在移动电话 1 的输入 25 单元 13 的旁边提供了用于获取客户的指纹信息的指纹获取单元 112。指纹获取单元 112 将通过扫描而读取的指纹信息输出到安全性芯片 5。注意，在实施例 1 中，虽然指纹被用作生物信息，但生物信息不一定局限于指纹，而可以是和语音、视网膜或虹膜有关的信息。例如在语音的情况下，通过从麦克风和扬声器 111 获取语音、用 AD/DA 转换器 20 将语音转换成数字信号、将语音输出到 CPU 11 并将语音与预先存储的客户自己的语音

数据做比较来进行认证。

下面将解释安全性芯片 5 的硬件结构。安全性芯片 5 包括微处理器（以后称为 MPU）51、RAM 52、和例如 EEPROM 的 ROM 55。MPU 51 通过总线 57 连接到 RAM 52 和 ROM 55，控制它们，并根据存储在 ROM 55 中的控制程序 55P 来执行各种软件功能。在 ROM 55 中，准备了：存储从证书机构服务器 3 接收到的电子证书的电子证书文件 553；存储移动电话 1 自身的秘密密钥的秘密密钥文件 554；预先存储客户指纹信息的指纹信息文件 552；以及存储移动电话 1 的设备名和版本、外围设备的设备名和版本以及所安装的软件的名称和版本的环境信息文件 551。注意，移动电话 1 的秘密密钥是由证书机构服务器 3 发行的，而与此秘密密钥形成一对的公共密钥由证书机构服务器 3 所管理。

安全性芯片 5 的 MPU 51 收集和移动电话 1 有关的环境信息，并将该环境信息存储在环境信息文件 551 中。MPU 51 从 ROM 15 中读取预先存储的移动电话 1 的设备名和版本，以获取移动电话 1 自身的信息。例如，当信息处理设备是移动电话时，获取设备名和版本，而当信息处理设备是微波炉时，获取制造商名称、设备名、型号等。而且，MPU 51 参考 ROM 15 的 BIOS 来获取与连接到外部连接器 19 的设备有关的信息，并将该信息作为环境信息之一存储在环境信息文件 551 中。例如，当计算机（未示出）被连接到外部连接器 19 时，获取该计算机的设备名等。另一方面，当信息处理设备是个人计算机时，如果一个 PC 卡被连接到用作外部连接器 19 的 PC 卡插槽，就获取该 PC 卡的设备名。

另外，与安装在移动电话 1 中的软件有关的信息对应于环境信息。MPU 51 参考 ROM 15 中的 OS 和软件获取所安装的软件的名称和版本。当信息处理设备是个人计算机时，举例来说，作为与所安装的软件有关的环境信息，获取 Windows® 或 Linux 作为 OS 的名称，获取“第二版”作为 OS 的版本，获取 Internet Explorer® 作为浏览器，获取“SP2”作为浏览器的版本。另外，通过因特网 N 下载的、以 Java® 编写的软件的名称对应于环境信息。因此，MPU 51 总是监控 ROM 中的 BIOS、OS 等等，并且当安装了新软件或者当新设备连接到外部连接器 19 时，MPU 51 收集与该软件

或设备有关的信息作为环境信息存储在环境信息文件 551 中。

指纹信息文件 552 被用于个人认证。例如，当客户购买移动电话 1 时，获取客户的指纹信息并在该商店将客户的指纹信息首次注册在 ROM 55 内的指纹信息文件 552 中。当从指纹获取单元 112 读取并输出指纹信息时，MPU 51 将所输出的指纹信息与存储在指纹信息文件 552 中的指纹信息做比较，以判断它是否正确。注意，在实施例 1 中，用于认证的指纹信息文件 552 存储在移动电话 1 中，但它不一定必须存储在移动电话 1 中，而是可以存储在中心服务器 2 或证书机构服务器 3 中，并用于中心服务器 2 或证书机构服务器 3 中的认证。在此情况下，将用存储在秘密密钥文件 554 中的秘密密钥加密的指纹信息和一个电子证书一起发送到中心服务器 2 或证书机构服务器 3 以用于认证。

电子证书文件 553 存储由证书机构服务器 3 发行的电子证书，并且类似地，秘密密钥文件 554 存储由证书机构服务器 3 发行的用于移动电话 1 的秘密密钥。注意，用于移动电话 1 的公共密钥存储在证书机构服务器 3 中。MPU 51 加密与交易相关的数据、环境信息和指纹信息等，这些数据和信息将与带有秘密密钥的消息摘要一起被发送和接收，并将加密的数据和电子证书通过因特网 N 发送到中心服务器 2 等。

图 3 是示出了中心服务器 2 的硬件结构的方框图。如图 3 中所示，RAM 22，例如硬盘的存储单元 25，例如网关和 LAN 卡的用于向移动电话 1、证书机构服务器 3、万维网服务器 4 等发送信息和从它们接收信息的通信单元 26，例如液晶显示器的显示单元 24，以及例如键盘和鼠标的输入单元 23 通过总线 27 连接到 CPU（中央处理单元）21。CPU 21 通过总线 27 连接到中心服务器 2 的如上所述的各种硬件单元，控制它们，并根据存储在存储单元 25 中的控制程序 25P 来执行各种软件功能。而且，在存储单元 25 中，提供了环境信息数据库（以后称为环境信息 DB）251，根据要发送和接收的信息的安全性的等级存储环境条件。

图 4 是环境信息 DB 251 的记录布局的说明性视图。如图 4 中所示，根据预设的安全性策略注册对应于安全性等级的环境条件。根据要被发送和接收的信息的安全性程度，等级字段被划分为等级 1 到等级 6，并且等

级 1 代表最高安全性级别，而等级 6 代表最低安全性级别。如在价格信息字段和产品信息字段中所示，当交易涉及小额数目如 ¥100 时，或者目标产品是例如具有旋律的通话信号（以后称为“Chakumero”）的低价产品时，必须优先考虑顺利交易而不是安全性，并且因此这一产品被划分到等 5 级 6 中。另一方面，当交易涉及不少于 ¥50,000 的高价产品时，或者当目标产品是股票证书等等，就必须确保高安全性，并且因此这样的产品被划分到等级 1 中。

在环境条件字段内的设备信息字段中，客户的移动电话 1 的设备名和版本根据其等级而被注册。例如在等级 1 中，条件规定了移动电话 1 的最新型号 S004、F004 和 N004，而当移动电话 1 不满足作为环境信息的这一条件时，此移动电话 1 就被环境认证判断为不正确。具体地说，在型号 S004 的情况下，还存在一个条件，即移动电话 1 的版本必须是 2.0 或更高版本。另一方面，在等级 6 中，当移动电话 1 的型号是 S001、S002、S003 和 S004（包括旧的型号 S001），以及 F001 到 F004 和 N001 到 N004 中的任何之一时，类似地，这一移动电话 1 被判断为正确。  
10  
15

在外围设备字段，类似地，对每一等级都注册外围设备的设备名和版本，并且它们被用于环境认证。例如，在等级 6 中，即使当外围设备 XX、YY 等被连接了，它们也被判断为正确。另一方面，在等级 1 中，由于没有存储对应的外围设备的条件，因此当有关外围设备的信息被作为环境信息从移动电话 1 发送出去时，它被判断为不正确。也就是说，在等级 20 1 中，无论连接了什么外围设备，它都被判断为不正确。注意，各个供应商提供的信息都被作为这种信息而被注册。

类似地，在软件字段，根据等级注册软件名和版本。在等级 1 中，当软件是软件 C 并且它的版本是 3.0 或更高时，这一软件被判断为正确。而在等级 6 中，当软件是软件 C 并且它的版本是 1.0 或更高，这一软件被判断为正确。通过以这种方式设置等级来判断安全性的原因在于考虑顺利交易和安全性维护之间的平衡。例如，当信息处理设备是个人计算机时，所安装的浏览器根据每个客户而不同。例如，在 Microsoft® 的 Internet Explorer® 的情况下，存在多个版本，并且版本号越高，安全性漏洞就越 25

少，即安全性越高。

当需要高安全性时，可以有一种方法，在此方法中环境信息被获取，并且，只有当所获取的环境信息属于最新版本的没有安全漏洞的浏览器时，这一环境信息才被判断为正确并允许后续交易。然而，在此情况下，  
5 由于没有安装最新版本的客户根本不能进行交易，这一方法就不合适了。因此，在不需要高安全性的低价产品的情况下，认证等级被设置成很低，并且即使具有很旧版本的浏览器在特定条件下也被判断为正确以允许交易。

参考流程图，下面的说明将解释在上述硬件结构上执行的本发明的安全性判断处理的过程。  
10 图 5 是示出了在万维网服务器 4 和移动电话 1 之间的交易的过程的流程图。首先，客户通过移动电话 1 的输入单元 13 输入作为交易的另一方的在线商店的万维网服务器 4 的 URL（统一资源定位符），并向万维网服务器 4 请求产品定单页面（步骤 S51）。作为 HTTP  
15 （超文本传输协议）服务器的万维网服务器 4 从存储单元（未示出）读取对应的 cHTML（精简超文本置标语言）文件（步骤 S52），并将所读取的 cHTML 文件发送到移动电话 1（步骤 S53）。

移动电话 1 的 CPU 11 用存储在 ROM 15 中的浏览器软件来分析所接收的 cHTML 文件，并如在图 6 中所示的那样，在显示单元 14 上显示用于交易的网页（步骤 S54）。图 6 是示出了所述网页的显示状态的说明性视图。  
20 如在图 6 中所示，与产品、数量和价格有关的信息被显示在显示单元 14 上。客户通过操作输入单元 13 来在显示单元 14 的屏幕上选择要被订购产品和数量。当选择了产品时，CPU 11 执行与所述 cHTML 文件一起发送来的 Java 脚本，并计算和显示总价格。实施例 1 中的在线商店出售计算机相关设备如个人计算机、打印机和磁盘驱动器，而图 6 示出了当客户订购一台价格为￥29,800 的喷墨式打印机的输入结果。总之，客户输入价格信息或产品信息作为与交易相关的定单信息。另外，客户可以输入地址、电话号码、姓名、ID、密码等等。  
25

当从输入单元 13 以这种方式输入定单信息时，CPU 11 接收此定单信息（步骤 S55）。然后，当选择图 6 中示出的“购买”按钮时，CPU 11 跳

转到安全性判断处理（步骤 S56）。参考流程图，下面的说明将解释作为本发明的特征的步骤 S56 的安全性判断处理的子例程。注意，后面会描述步骤 S57 之后的过程。

图 7 至图 12 是示出了安全性判断处理（步骤 S56）的子例程的过程的流程图。当输入订单信息时，安全性芯片 5 的 MPU 51 执行控制程序 55P，并在显示单元 14 上显示指纹信息获取请求（步骤 S71）。此时所显示的内容预先存储在 ROM 55 中，并且，举例来说可以读取如“将您的大拇指放在指纹获取单元上”的信息，并将其输出到显示单元 14。当从指纹获取单元 112 输入指纹信息时，安全性芯片 5 的 MPU 51 接收该指纹信息（步骤 S72），并将它临时存储在 RAM 52 中。然后，MPU 51 读取在客户购买移动电话 1 时已预先注册在 ROM 55 中的指纹信息文件 552 中的指纹信息，并比较这些指纹信息，判断所注册的信息是否与在步骤 S72 中所接收并存储在 RAM 52 中的指纹信息相匹配，即指纹信息认证是否成功（步骤 S73）。

当这些指纹信息匹配并且指纹信息认证被判断为成功（步骤 S73 中的“是”）时，MPU 51 设置指纹认证成功标志，并将所设置的指纹认证成功标志发送到中心服务器 2（步骤 S75）。另一方面，当这些指纹信息不匹配且指纹信息认证被判断为不成功（步骤 S73 中的“否”）时，MPU 51 设置指纹认证失败标志，并将所设置的指纹认证失败标志发送到中心服务器 2（步骤 S74）。中心服务器 2 的 CPU 21 将所发送的指纹认证标志（指纹认证成功标志或指纹认证失败标志）存储在存储单元 25 中（步骤 S77）。从而完成了使用指纹信息的生物认证。

注意，虽然实施例 1 采用了一种结构，在其中使用指纹信息的生物认证是在移动电话 1 中进行的，但也可以将预先收集的指纹信息注册在证书机构服务器 3 或中心服务器 2 中，并从移动电话 1 发送在步骤 S72 中所接收和存储在 RAM 52 中的指纹信息，用于在证书机构服务器 3 或中心服务器 2 中的判断。

随后，过程跳转到使用电子证书的认证。安全性芯片 5 的 MPU 51 通过使用存储在 ROM 55 中的哈希函数来为在步骤 S55 中接收的订单信息计

算消息摘要（步骤 S76）。MPU 51 从秘密密钥文件 554 读取由证书机构服务器 3 预先发行的移动电话 1 的秘密密钥，并加密订单信息和消息摘要（步骤 S81）。而且，MPU 51 从电子证书文件 553 读取由证书机构服务器 3 预先发行的电子证书，将该电子证书附加到加密的订单信息和消息摘要，并将它们发送到中心服务器 2（步骤 S82）。中心服务器 2 的 CPU 21 在 RAM 22 中存储所发送的电子证书和加密的订单信息和消息摘要。

中心服务器 2 的 CPU 21 访问在所述电子证书中描述的证书机构服务器 3，并请求获取所接收的电子证书的公共密钥（该证书机构的公共密钥）（步骤 S83）。响应于这一请求，证书机构服务器 3 将电子证书的公共密钥发送到中心服务器 2（步骤 S84）。中心服务器 2 的 CPU 21 从 RAM 22 读取所存储的电子证书，通过使用从证书机构服务器 3 发送来的证书机构的公共密钥来解密电子证书，并获取移动电话 1 的公共密钥（步骤 S85）。

中心服务器 2 的 CPU 21 通过使用从证书机构服务器 3 获取的移动电话 1 的公共密钥来解密加密的订单信息和消息摘要（步骤 S91）。而且，CPU 21 通过使用存储在中心服务器 2 的存储单元 25 中的哈希函数来为加密的订单信息计算消息摘要（步骤 S92）。中心服务器 2 的 CPU 21 判断在步骤 S91 中解密的消息摘要是否与在步骤 S92 中计算的消息摘要相匹配，即订单信息在发送期间是否没有被伪造，并还判断是否所述信息被发送到一个授权客户的移动电话 1 和从该移动电话接收到所述信息（步骤 S93）。

如果这些消息摘要不匹配（步骤 S93 中的“否”），CPU 21 判断已发生了某种伪造或“欺骗”，并为电子证书认证设置失败标志（S95）。另一方面，如果这些消息摘要相匹配（步骤 S93 中的“是”），CPU 21 判断没有发生“欺骗”或伪造，并为电子证书认证设置成功标志（步骤 S94）。然后，中心服务器 2 的 CPU 21 将电子证书认证的标志（电子证书认证成功标志或电子证书认证失败标志）存储在存储单元 25 中（步骤 S96）。从而完成使用电子证书的认证。

下面将解释环境认证。安全性芯片 5 的 MPU 51 获取与移动电话 1 有

关的环境信息（步骤 S101）。MPU 51 通过总是监控安装在移动电话 1 的 ROM 15 中的 OS、BIOS 和软件并如上所述地收集移动电话 1 的设备名、OS 的名称和版本、连接到外部连接器 19 的外围设备的设备名和版本、所安装的软件如浏览器的名称和版本来收集环境信息。所收集的环境信息被 5 存储在环境信息文件 551 中（步骤 S102）。

MPU 51 从环境信息文件 551 读取所收集的环境信息，并将它发送到中心服务器 2（步骤 S103）。中心服务器 2 的 CPU 21 在 RAM 22 中存储所发送的环境信息。中心服务器 2 的 CPU 21 参考环境信息 DB 251 读取与在步骤 S91 中解密的订单信息相对应的等级（步骤 S104）。具体地说，参考价格信息或产品信息字段，CPU 21 根据交易中将成交的订单信息中的价格或产品，从等级字段读取对应的等级。例如，当所订购的产品的价格超过¥50,000 时，就选择等级 1。  
10

中心服务器 2 的 CPU 21 从环境信息 DB 251 读取对应于所读取的等级的环境信息的条件（步骤 S105），具体地说，根据所读取的等级，从环境 15 信息 DB 251 的环境条件字段读取对应的移动电话 1 的设备名和版本、对应的软件的名称和版本以及对应的外围设备的设备名和版本。然后，CPU 21 判断存储在 RAM 22 中的所接收的环境信息是否满足从环境信息 DB 251 读取的环境信息的条件（步骤 S111）。如果该条件未被满足（步骤 S111 中的“否”）（例如，当等级是 1 并且发送了软件 C 的版本 2.0 作为环境信息，这一软件就不满足版本必须是 3.0 或更高的条件），CPU 21 就设置环境认证失败标志（步骤 S112）。另一方面，如果所述条件被满足 20 （步骤 S111 中的“是”），CPU 21 就设置环境认证成功标志（步骤 S113）。例如，当设置了等级 1 作为条件时，如果环境信息显示“对于移动电话 1 的设备名和版本是最新型号 F004 和版本 2.0，对于所安装的软件是软件 C 和版本 5.0，并且对于所连接的外围设备是没有设备”，则 CPU 21 判断该环境是正确的。中心服务器 2 的 CPU 21 在存储单元 25 中存储环境 25 认证的标志（环境认证成功标志或环境认证失败标志）（步骤 S114），从而完成环境认证。

CPU 21 读取存储在存储单元 25 中的指纹认证标志、电子证书标志和

环境认证标志，并判断指纹认证成功标志、电子证书认证成功标志和环境认证成功标志中的全部是否在与（AND）条件下都被设置（步骤 S115）。当所有成功标志都被设置时（步骤 S115 中的“是”），CPU 21 判断移动电话 1 是安全的，并设置安全标志（步骤 S121）。也就是说，只有当移动电话 1 在生物认证、电子证书认证（PKI 认证）和环境认证中的全部都被判断为正确时，移动电话 1 才被判断为正确的。在此情况下，中心服务器 2 的 CPU 21 将表示移动电话 1 是安全的安全性保证信息和订单信息发送到万维网服务器 4（步骤 122），并终止安全性判断的子例程（步骤 S56）。

另一方面，当在生物认证、电子证书认证（PKI 认证）和环境认证的至少之一中设置了失败标志时，CPU 21 就设置失败标志（步骤 S123）。在此情况下，CPU 21 将表示移动电话 1 是危险的警告信息发送到万维网服务器 4（步骤 S124），并终止安全性判断的子例程（步骤 S56）。

在图 5 中，万维网服务器 4 判断是否已从中心服务器 2 接收到与移动电话 1 有关的警告信息（步骤 S57）。如果没有接收到警告信息（步骤 S57 中的“否”），万维网服务器 4 就判断是否已收到安全性保证信息和订单信息（步骤 S58）。如果还未收到安全性保证信息和订单信息（步骤 S58 中的“否”），或者如果在步骤 57 中是“是”，万维网服务器 4 就判断移动电话 1 很可能是欺骗性的，并且然后就将取消交易的信息发送到移动电话 1（步骤 S59）。另一方面，如果已接收到安全性保证信息和订单信息（步骤 S58 中的“是”），就认为移动电话 1 的安全性得到了保证，并且万维网服务器 4 然后就正式地接收到该订单，并将表示订单已收到的订单确认信息发送到移动电话 1（步骤 S60）。这样，在实施例 1 中，通过在交易前进行个人认证、PKI 认证和环境认证，确保了足够的安全性，并且可以通过根据要成交的产品的价值来改变认证级别从而实现顺利的交易。

## 实施例 2

图 13 是示出了根据本发明的实施例 2 的移动电话 1 的硬件结构的方框

图。可以通过在移动电话 1 中如实施例 2 中的那样预安装计算机程序来提供用于执行实施例 1 的移动电话 1 的处理的计算机程序，或者使用可拆卸的记录介质如 CD-ROM、MO 和存储卡来提供。而且，也可以通过经由线路将计算机程序作为载波发送来提供所述计算机程序。具体地说，在实施 5 例 2 中，在移动电话 1 的 ROM 15 中安装了具有和安全性芯片 5 相同功能的计算机程序，而不是安装安全性芯片 5。下面将解释该程序的内容。

如在图 13 中所示，从其上记录了程序的记录介质 1a（例如 CD-ROM、MO、存储卡或 DVD-ROM）将用于认证生物信息、收集环境信息、发送环境信息、发送加密的信息并判断安全性的程序安装在移动电话 10 1 的 ROM 15 中。作为安装方法，诸如存储卡的可连接到外部连接器 19 的记录介质 1a 被连接到外部连接器 19，并安装所述程序。然而，可以从中 15 心服务器 2 下载本发明的程序。这些程序在暂时被装载到移动电话 1 的 RAM 12 中之后被执行。从而移动电话 1 就作为如上所述的本发明的实施例 1 的信息处理设备。

15

### 实施例 3

在如上所述的实施例 1 中，虽然生物信息的认证是在安全性芯片 5 中进行的，但它也可以在中心服务器 2 或证书机构服务器 3 中进行。实施例 20 3 采用了一种结构，在此结构中生物信息的认证在中心服务器 2 中进行，并且说明了一个示例，在其中本发明被应用到一个预定了安全性策略的情形中。

图 14 是示出了根据实施例 3 的移动电话 1 的硬件结构的方框图。图 15 是示出了根据实施例 3 的中心服务器 2 的硬件结构的方框图。如图 14 和图 15 所示，由于实施例 3 采用了其中生物信息认证是在中心服务器 2 中 25 进行的结构，因此用于认证的指纹信息文件 252 被存储在中心服务器 2 的存储单元 25 中，而不是在移动电话 1 内。其他的结构与在图 2 和图 3 中示出的实施例 1 的相同。注意，可以通过下述方式进行用于认证的指纹信息的初次注册：要求客户在认证前访问一个商店或服务中心，根据驾照、护照等确认个人身份，并现场读取他/她的指纹。

图 16 到图 20 示出了根据实施例 3 的安全性判断处理（图 5 中的步骤 S56 的子例程）的过程的流程图。首先，为进行一项后续通信，安全性芯片 5 的 MPU 51 向中心服务器 2 发送一个安全性确认启动信号（步骤 S161）。当中心服务器 2 的 CPU 21 接收到确认启动信号时，它就确定通信的安全性等级（步骤 S162）。在确定所述等级时，根据一个预定的安全性策略来确定所述等级。例如，当后续通信是需要高安全性的通信时，例如发行居民卡或股票交易，所述等级就被确定为等级 1，而当后续通信是不需要高安全性的通信时，例如 Chakumero 或备用显示器的图像数据，所述等级就被确定为等级 6。另外，对于公用设施收费的支付，为了确保中等级别的安全性，所述等级被确定为等级 3。

在确定了等级后，中心服务器 2 的 CPU 21 将一个对应于确认启动信号的响应信号发送到移动电话 1（步骤 S163）。当接收到该响应信号时，安全性芯片 5 的 MPU 51 执行控制程序 55P，并在显示单元 14 上显示指纹信息获取请求（步骤 S164）。此时显示的内容预先存储在 ROM 55 中，并且，举例来说，诸如“将您的大拇指放在指纹获取单元上”的信息可以被读取并输出到显示单元 14。当从指纹获取单元 112 输入指纹信息时，安全性芯片 5 的 MPU 51 接收指纹信息并将它暂时存储在 RAM 52 中（步骤 S165）。

然后，安全性芯片 5 的 MPU 51 获取与移动电话 1 有关的环境信息（步骤 S166）。如上所述，MPU 51 通过总是监控安装在移动电话 1 的 ROM 15 中的 OS、BIOS 和软件并收集移动电话 1 的设备名、OS 的名称和版本、连接到外部连接器 19 的外围设备的设备名和版本、所安装的软件如浏览器的名称和版本来收集环境信息。所收集的环境信息存储在环境信息文件 551 中（步骤 S167）。

安全性芯片 5 的 MPU 51 读取存储在 RAM 52 中的生物信息和存储在环境信息文件 551 中的环境信息（步骤 S168）。安全性芯片 5 的 MPU 51 通过使用存储在 ROM 55 中的哈希函数为所读取的生物信息和环境信息计算消息摘要（步骤 S169）。MPU 51 从秘密密钥文件 554 读取由证书机构服务器 3 预先发行的移动电话 1 的秘密密钥，并加密所述生物信息、环境

信息和消息摘要（步骤 S171）。而且，MPU 51 从电子证书文件 553 读取由证书机构服务器 3 预先发行的电子证书，将该电子证书附加到所加密的生物信息、环境信息和消息摘要，并将它们发送到中心服务器 2（步骤 S172）。中心服务器 2 的 CPU 21 将所发送的电子证书和加密的生物信息、环境信息和消息摘要存储在 RAM 22 中。注意，在实施例 3 中，尽管生物信息和环境信息都被加密和发送了，但可以只加密生物信息或只加密环境信息。

10 中心服务器 2 的 CPU 21 访问在电子证书中描述的证书机构服务器 3，并请求获取所接收到的电子证书的公共密钥（该证书机构的公共密钥）（步骤 S173）。响应于此请求，证书机构服务器 3 将该电子证书的公共密钥发送到中心服务器 2，并且中心服务器 2 接收所发送的该电子证书的公共密钥（步骤 S174）。中心服务器 2 的 CPU 21 从 RAM 22 读取所存储的电子证书，使用从证书机构服务器 3 发送来的证书机构的公共密钥来解密电子证书，并获取移动电话 1 的公共密钥（步骤 S175）。

15 中心服务器 2 的 CPU 21 用从证书机构服务器 3 获取的移动电话 1 的公共密钥来解密所加密的生物信息、环境信息和消息摘要（步骤 S181）。而且，CPU 21 通过使用存储在中心服务器 2 的存储单元 25 中的哈希函数来为解密的生物信息和环境信息计算消息摘要（步骤 S182）。中心服务器 2 的 CPU 21 判断在步骤 S181 中解密的消息摘要是否与步骤 S182 中计算出的消息摘要相匹配，即所述生物信息和环境信息是否在发送过程中没有被伪造，并且还判断是否所述信息已被发送到一个授权客户的移动电话 1 和从该移动电话 1 接收到所述信息（步骤 S183）。

20 如果这些消息摘要不匹配（步骤 S183 中的“否”），CPU 21 判断已发生了某种伪造或“欺骗”，并为电子证书认证设置失败标志（S185）。另一方面，如果这些消息摘要相匹配（步骤 S183 中的“是”），CPU 21 判断没有发生“欺骗”或伪造，并为电子证书认证设置成功标志（步骤 S184）。然后，中心服务器 2 的 CPU 21 将电子证书认证的标志（电子证书认证成功标志或电子证书认证失败标志）存储在存储单元 25 中（步骤 S186）。

随后，中心服务器 2 的 CPU 21 从 252 读取用于认证的预注册的指纹信息（步骤 S187）。CPU 21 将解密的指纹信息与用于认证的所读取的指纹信息做比较，并判断这些指纹信息是否相匹配，即指纹信息认证是否成功（步骤 S191）。

5 如果这些指纹信息匹配并且指纹信息认证被判断为成功（步骤 S191 中的“是”），CPU 21 设置指纹认证成功标志（步骤 S192）。另一方面，如果这些指纹信息不匹配且指纹信息认证被判断为不成功（步骤 S191 中的“否”），CPU 21 设置指纹认证失败标志（步骤 S193）。中心服务器 2 的 CPU 21 将指纹认证标志（指纹认证成功标志或指纹认证失败标志）存储在存储单元 25 中（步骤 S194）。

10 中心服务器 2 的 CPU 21 从环境信息 DB 251 读取对应于在步骤 S162 中所确定的等级的环境信息的条件（步骤 S195）。然后，CPU 21 判断所解密的环境信息是否满足在步骤 S195 中从环境信息 DB 251 读取的环境信息的条件（步骤 S196）。如果该条件未被满足（步骤 S196 中的“否”）  
15 CPU 21 就设置环境认证失败标志（步骤 S198）。另一方面，如果所述条件被满足（步骤 S196 中的“是”），CPU 21 就设置环境认证成功标志（步骤 S197）。中心服务器 2 的 CPU 21 在存储单元 25 中存储环境认证的标志（环境认证成功标志或环境认证失败标志）（步骤 S201）。

20 CPU 21 读取存储在存储单元 25 中的指纹认证标志、电子证书标志和环境认证标志，并判断指纹认证成功标志、电子证书认证成功标志和环境认证成功标志中的全部是否在与（AND）条件下都被设置（步骤 S202）。如果所有成功标志都被设置（步骤 S202 中的“是”），CPU 21 判断移动电话 1 是安全的，并设置安全标志（步骤 S203）。也就是说，只有当移动电话 1 在生物认证、电子证书认证（PKI 认证）和环境认证中的全部都被判断为正确时，移动电话 1 才被判断为正确。在此情况下，中心服务器 2 的 CPU 21 将指示继续通信的信号发送到移动电话 1 或万维网服务器 4（步骤 204），并终止安全性判断的子例程（步骤 S56）。

25 另一方面，如果在生物认证、电子证书认证（PKI 认证）和环境认证的至少之一中设置了失败标志，CPU 21 就设置失败标志（步骤 S205）。

在此情况下，CPU 21 将指示结束通信的信号发送到移动电话 1 或万维网服务器 4（步骤 S206），并终止安全性判断的子例程（步骤 S56）。

#### 实施例 4

5 本发明的实施例 4 涉及在提供补丁软件和固件的情形下应用的安全性判断系统。在 PDA、移动电话、冰箱、空调和打印机中，有时会在所安装的软件中发现漏洞（bug）。在此情形下，需要提供补丁软件。另外，存在一种提供具有附加功能的固件的情形。实施例 4 说明了能够在确保安全性之后提供软件的安全性判断系统。

10 图 21 是示出了根据实施例 4 的移动电话 1 的硬件结构的方框图。图 21 中的数字 114 表示主电源供应装置（以后称为主电源单元），用于向移动电话引擎单元 110 供应电源，并且此 114 使用锂电池等等。通过操作输入单元 13 的开通（ON）按钮（未示出），从主电源单元 114 向移动电话引擎单元 110 和安全性芯片 5 供应电源。另一方面，通过操作关断（OFF）按钮（未示出），就切断了从主电源单元 114 向移动电话引擎单元 110 和安全性芯片 5 的电源供应，并且移动电话 1 的电源被关闭。

但是，即使主电源单元 114 未向移动电话引擎单元 110 和安全性芯片 5 供应电源，副电源供应装置（以后称为副电源单元）115 仍然使用例如一个硬币状的锂电池并向第二 ROM 116 和副天线单元 117 供应电源，其中 116 用作存储装置，而副天线单元 117 用作接收和发送装置。在电源是由主电源单元 114 所供应，即移动电话 1 的电源是开通的情况下，那么当从中心服务器 2 发送软件过来时，此软件就由天线单元 16 所接收，并且 CPU 11 将该软件存储在 ROM 15 中。在此情形下，电源不是由副电源单元 115 所供应。

25 在电源不是由 114 所供应，即移动电话 1 的电源是关断的情况下，由副电源单元 115 向副天线单元 117 和第二 ROM 116 供应电源。然后，当从中心服务器 2 发送软件过来时，此软件就由副天线单元 117 所接收，并且所接收的软件临时存储在第二 ROM 116 中。在电源由主电源单元 114 所供应时，存储在第二 ROM 116 中的软件被写入到 ROM 15 中。注意，作

为副天线单元 117，可以使用例如已知的 FM 字符多信道广播接收模块。在此情形下，中心服务器 2 通过一个 FM 广播站发送包含软件的 FM 复用广播。当用作副天线单元 117 的 FM 字符多信道广播接收模块接收到 FM 复用广播时，由 DARC (Data Radio Channel, 数据广播信道) 标准的字符代码所描述的软件数据转换成例如由 C 语言或 Java 所描述的源代码。最后，在进行个人认证、PKI 认证和环境认证后，安全性芯片 5 的 MPU 51 在 ROM 15 中安装该软件。

图 22 是示出了根据实施例 4 的中心服务器 2 的硬件结构的方框图。如图 22 中所示，存储单元 25 存储多种由证书机构服务器 3 证明的软件，如补丁软件、固件、插件软件和防毒软件。注意，这些软件可以由软件公司 (Software House) 来提供。电子证书文件 253 存储由证书机构服务器 3 预先发行的中心服务器 2 的电子证书，而秘密密钥文件 254 存储类似地由证书机构服务器 3 发行的中心服务器 2 的秘密密钥。

参考流程图，下面的说明将解释提供已保证其安全性的软件的处理，该处理根据本发明的实施例 4 在中心服务器 2 的硬件结构上执行。图 23 到图 29 示出了根据实施例 4 的软件提供处理的过程的流程图。首先，中心服务器 2 的 CPU 21 通过呼叫移动电话 1 或其他方法来请求获取表示移动电话 1 的主电源是开通还是关断的信息 (步骤 S231)。移动电话 1 发送表示主电源是开通还是关断的信息 (步骤 S232)。中心服务器 2 判断移动电话 1 的主电源是否是开通的 (步骤 S233)。如果移动电话 1 的主电源是开通的 (步骤 S233 中的“是”)，安全性等级就以与上述的在步骤 S162 中的相同的方式确定 (步骤 S234)。管理者可以根据所提供的软件的重要性来确定安全性。例如，当该软件是补丁软件或防毒软件时，所述等级被确定为等级 1 以提高安全性，而当软件是需要低安全性的软件例如游戏软件时，所述等级就被确定为等级 6。

中心服务器 2 的 CPU 21 将认证启动信号发送到移动电话 1 (步骤 S235)。接收到所述认证启动信号的移动电话 1 的安全性芯片 5 的 MPU 51 执行控制程序 55P，并在显示单元 14 上显示指纹信息获取请求 (步骤 S236)。当从指纹获取单元 112 输入指纹信息时，安全性芯片 5 的 MPU

51 接收该指纹信息（步骤 S237），并将它暂时存储在 RAM 52 中。然后，MPU 51 读取客户购买移动电话 1 时注册在 ROM 55 中的指纹信息文件 552 中的指纹信息，并比较这些指纹信息，以判断所注册的信息是否与在步骤 S237 中所接收并存储在 RAM 52 中的指纹信息相匹配，即指纹信息认证是否成功（步骤 S241）。

10 如果这些指纹信息匹配并且指纹信息认证被判断为成功（步骤 S241 中的“是”），MPU 51 设置指纹认证成功标志（步骤 S243）。另一方面，如果这些指纹信息不匹配且指纹信息认证被判断为不成功（步骤 S241 中的“否”），MPU 51 设置指纹认证失败标志（步骤 S242）。MPU 51 将所发送的指纹认证标志（指纹认证成功标志或指纹认证失败标志）存储在存储单元 55 中（步骤 S244）。

15 然后，安全性芯片 5 的 MPU 51 获取与移动电话 1 有关的环境信息（步骤 S245）。所收集的环境信息被存储在环境信息文件 551 中（步骤 S246）。MPU 51 从环境信息文件 551 读取所收集的环境信息，并将它发送到中心服务器 2（步骤 S247）。中心服务器 2 的 CPU 21 在 RAM 22 中存储所发送的环境信息。中心服务器 2 的 CPU 21 从环境信息 DB 251 读取对应于在步骤 S162 中所确定的等级的环境信息的条件（步骤 S248）。

20 然后，CPU 21 判断存储在 RAM 22 中的所接收的环境信息是否满足从环境信息 DB 251 读取的环境信息的条件（步骤 S251）。如果条件未被满足（步骤 S251 中的“否”），CPU 21 设置环境认证失败标志（步骤 S253）。另一方面，如果条件被满足（步骤 S251 中的“是”），CPU 21 设置环境认证成功标志（步骤 S252）。中心服务器 2 的 CPU 21 在存储单元 25 中存储环境认证的标志（环境认证成功标志或环境认证失败标志）（步骤 S254），并将它发送到移动电话 1（步骤 S255）。接收到环境认证标志的安全性芯片 5 的 MPU 51 在存储单元 25 中存储环境认证标志（环境认证成功标志或环境认证失败标志）（步骤 S256）。

而且，中心服务器 2 的 CPU 21 从存储单元 25 读取要被提供的软件（步骤 S257），该软件存储在存储单元 25 中。CPU 21 通过使用存储在存储单元 25 中的哈希函数来为所读取的软件计算消息摘要（步骤 S258）。

CPU 21 从秘密密钥文件 254 读取由证书机构服务器 3 预先发行的中心服务器 2 的秘密密钥，并加密所述软件和消息摘要（步骤 S259）。而且，CPU 21 从电子证书文件 253 读取由证书机构服务器 3 预先发行的电子证书，将该电子证书附加到加密的软件和消息摘要，并将它们发送到移动电话 1 5 （步骤 S261）。安全性芯片 5 的 MPU 51 在 RAM 52 中存储所发送的电子证书以及加密的软件和消息摘要。

安全性芯片 5 的 MPU 51 访问在所述电子证书中描述的证书机构服务器 3，并请求获取所接收的电子证书的公共密钥（该证书机构的公共密钥）（步骤 S262）。响应于这一请求，证书机构服务器 3 将所述电子证书的公共密钥发送到移动电话 1，并且安全性芯片 5 的 MPU 51 接收所发送的公共密钥（步骤 S263）。MPU 51 从 RAM 52 读取所存储的电子证书，通过使用从证书机构服务器 3 发送来的证书机构的公共密钥来解密电子证书，并获取中心服务器 2 的公共密钥（步骤 S264）。

安全性芯片 5 的 MPU 51 用从证书机构服务器 3 获取的中心服务器 2 的公共密钥来解密所加密的软件和消息摘要（步骤 S265）。而且，MPU 51 通过使用存储在安全性芯片 5 的 ROM 55 中的哈希函数来为解密的软件计算消息摘要（步骤 S266）。MPU 51 判断在步骤 S265 中解密的消息摘要是否与步骤 S266 中计算出的消息摘要相匹配，即所述软件是否在发送过程中没有被伪造，并且还判断是否所述信息已被发送到一个授权中心服务器 2 和从该服务器 2 接收到所述信息（步骤 S271）。

如果这些消息摘要不匹配（步骤 S271 中的“否”），MPU 51 判断已发生了某种伪造或“欺骗”，并为电子证书认证设置失败标志（S272）。另一方面，如果这些消息摘要相匹配（步骤 S271 中的“是”），MPU 51 判断没有发生“欺骗”或伪造，并为电子证书认证设置成功标志（步骤 S273）。然后，安全性芯片 5 的 MPU 51 将电子证书认证的标志（电子证书认证成功标志或电子证书认证失败标志）存储在 ROM 55 中（步骤 S274）。

MPU 51 读取存储在 ROM 55 中的指纹认证标志、电子证书标志和环境认证标志，并判断指纹认证成功标志、电子证书认证成功标志和环境认

证成功标志中的全部是否在与（AND）条件下都被设置（步骤 S275）。如果所有成功标志被设置（步骤 S275 中的“是”），MPU 51 判断所发送的软件是安全的，并设置安全标志（步骤 S278）。安全性芯片 5 的 MPU 51 将在步骤 S265 中解密的软件安装在移动电话引擎单元 110 中的 ROM 5 15 中（步骤 S2710）。然后 MPU 51 将表示安装结束的信号发送到中心服务器 2（步骤 S2711），并终止安全性判断的子例程（步骤 S56）。

另一方面，如果在生物认证、电子证书认证（PKI 认证）和环境认证的至少之一中设置了失败标志（步骤 S275 中的“否”），MPU 51 就设置失败标志（步骤 S279）。在此情况下，MPU 51 将表示安装拒绝的信号发送到中心服务器 2（步骤 S2712），并终止安全性判断的子例程（步骤 S56）。

当在步骤 S233 中是“否”，即当移动电话 1 的主电源是关断的时，中心服务器 2 的 CPU 21 从存储单元 25 读取要提供的软件（步骤 S281），该软件存储在存储单元 25 中。CPU 21 通过使用存储在存储单元 25 中的哈希函数来为所读取的软件计算消息摘要（步骤 S282）。CPU 21 从秘密密钥文件 254 读取由证书机构服务器 3 预先发行的中心服务器 2 的秘密密钥，并加密所述软件和消息摘要（步骤 S283）。而且，CPU 21 从电子证书文件 253 读取由证书机构服务器 3 预先发行的电子证书，将该电子证书附加到加密的软件和消息摘要，并将它们发送到 FM 广播站的计算机（未示出）（步骤 S284）。

FM 广播站的计算机将电子证书和加密的软件及消息摘要根据 DARC 标准转换成广播数据，并用 FM 复用广播复用器电路（未示出）来复用 FM 音乐数据和广播数据。这些数据由 FM 调制振荡器所调频调制并被广播。移动电话 1 通过副天线单元 117 接收该 FM 复用广播（步骤 S285），并转换由 DARC 标准的字符代码描述的数据，以获取电子证书和加密的软件及消息摘要。注意，例如在日本专利申请特开 No.10-116237(1998)中公开了涉及使用 DARC 标准的 FM 复用广播的技术。

所转换的电子证书、软件和消息摘要被存储在第二 ROM 116 中（步骤 S286）。然后，当客户操作输入单元 13 以启动使用主电源单元 114 的

电源供应时（步骤 S291），以与如上所述的在步骤 S236 到 S244 中的相同的方式进行指纹认证（步骤 S292），通过在步骤 S245 到 S256 中说明的相同过程进行环境认证（步骤 S294），并且以与在步骤 S262 到 S274 中的相同的方式进行使用电子证书的认证（步骤 S293）。在进行使用电子证书的  
5 认证时，MPU 51 读取存储在第二 ROM 116 中的电子证书和加密的软件及消息摘要。简而言之，通过使用从证书机构服务器 3 获取的公共密钥来从电子证书获取所述公共密钥，用所获取的公共密钥来解密所加密的软件，并且判断所解密的软件是否正确。

MPU 51 读取存储在 ROM 55 中的指纹认证标志、电子证书标志和环境认证标志，并判断指纹认证成功标志、电子证书认证成功标志和环境认证成功标志中的全部是否在与（AND）条件下都被设置（步骤 S295）。如果所有成功标志被设置（步骤 S295 中的“是”），MPU 51 判断所发送的软件是安全的，并设置安全标志（步骤 S296）。安全性芯片 5 的 MPU 51 将在步骤 S265 中解密的软件安装在移动电话引擎单元 110 中的 ROM  
10 15 中（步骤 S298）。然后，MPU 51 将表示安装结束的信号发送到中心服务器 2（步骤 S299），并终止安全性判断的子例程（步骤 S56）。

另一方面，如果在生物认证、电子证书认证（PKI 认证）和环境认证的至少之一中设置了失败标志（步骤 S295 中的“否”），MPU 51 就设置失败标志（步骤 S297）。在此情况下，MPU 51 将表示安装拒绝的信号发  
20 25 送到中心服务器 2（步骤 S2910），并终止安全性判断的子例程（步骤 S56）。

中心服务器 2 提供的软件可以是用于删除移动电话 1 中的软件的软件或补丁软件，其中移动电话 1 是 DDoS（分布式拒绝服务）攻击的目标。例如，当出于某种原因在移动电话 1 中设置若干天后对预定万维网服务器发起攻击的软件（程序）时，提供通过本发明的认证的软件。要提供的软件存储了时间信息，并且通过安装并执行此软件来删除所有在此存储时刻和该时刻之后存储的数据。

图 30 是示出了所安装的删除软件的操作内容的流程图。在步骤 S298 中，在 ROM 15 中安装删除软件。客户通过操作输入单元 13 来使得 CPU

11 执行删除软件（步骤 S301）。CPU 11 读取 ROM 15 中的存储历史（步  
骤 S302）。更具体地说，CPU 11 读取诸如所存储的文件和所安装的软件  
的数据，并且还读取与这些数据被存储的时间有关的信息。CPU 11 从所述  
5 删 除 软件的程序读取时间信息（步骤 S303）。然后，CPU 11 参考所读取  
的存储历史，并删除所有在所读取的时刻和该时刻之后安装的数据（步骤  
S304）。因此，可以防止已被用作 DDoS 攻击的手段的移动电话 1 被用于  
所述攻击。

### 实施例 5

10 图 31 是示出了根据本发明实施例 5 的移动电话 1 的硬件结构的方框  
图。用于执行实施例 4 的移动电话 1 的处理的计算机程序可以通过在如实  
施例 5 中的移动电话 1 中安装它来提供，或者使用可拆卸的记录介质如  
CD-ROM、MO 或存储卡来提供。而且，也可以通过将该计算机程序作为  
15 载波经过线路而发送来提供它。具体地说，在实施例 5 中，在移动电话 1  
的 ROM 15 中安装了具有和安全性芯片 5 相同功能的计算机程序，而不是  
安装安全性芯片 5。下面将解释该程序的内容。

从其上记录了程序的记录介质 1a（例如 CD-ROM、MO、存储卡或  
DVD-ROM）将用于使移动电话 1 进行认证生物信息、收集环境信息、发  
送环境信息、使用电子证书进行认证并安装软件的程序安装在移动电话 1  
20 的 ROM 15 中。作为安装方法，诸如存储卡的可连接到外部连接器 19 的  
记录介质 1a 被连接到外部连接器 19，并安装程序。然而，可以从中心服  
务器 2 下载本发明的所述程序。这些程序在暂时被装载到移动电话 1 的  
RAM 12 中后被执行。从而，移动电话 1 作为如上所述的本发明的实施例  
4 的信息处理设备。

25

### 实施例 6

本发明的实施例 6 说明了一种技术，在其中，当在移动电话 1 和中心  
服务器 2 两者中，生物信息认证、环境信息认证和电子证书认证的全部都  
被判断为成功时，移动电话 1 和中心服务器 2 被判断为安全的，并且允许

随后的的信息发送和接收。

图 32 是示出了根据本发明实施例 6 的移动电话 1 的硬件结构的方框图，而图 33 是示出了根据实施例 6 的中心服务器 2 的硬件结构的方框图。如在图 32 中所示，在实施例 6 中，中心服务器 2 的环境认证也在移动电话 5 1 中进行，并且因此在移动电话 1 的 ROM 15 中准备了一个环境信息 DB 151。在此环境信息 DB 151 中，以在图 4 中说明的相同方式，根据安全性策略的等级，注册了与连接到中心服务器 2 的外部通信端口 29 的外围设备、PC 卡（未示出）和安装的 OS 及软件有关的环境信息的条件。

为了让中心服务器 2 接收由移动电话 1 进行的认证，指纹获取单元 10 212 和安全性芯片 5 通过总线 27 连接到 CPU 21。注意，由于它们的细节与在实施例 1 中所说明的那些相同，在此省略了详细说明。另外，数字 29 代表外部通信端口如 USB 端口和 RS232C 端口，并且诸如打印机、鼠标、硬盘和 MO 驱动器的外围设备被连接到外部通信端口 29。

在实施例 6 中，当在移动电话 1 和中心服务器 2 中，生物信息认证、15 环境信息认证和电子证书认证的全部都被判断为成功时，移动电话 1 和中心服务器 2 被判断为安全的，并且允许随后的的信息发送和接收。因此，当在图 11 示出的步骤 S115 中的判断结果为“是”时，即在确定移动电话 1 的安全性之后，另外还进行下面的处理。

图 34 到图 37 示出了根据实施例 6 的认证处理的过程的流程图。当步骤 20 S115 中的判断结果为“是”时，中心服务器 2 的安全性芯片 5 的 MPU 51 执行控制程序 55P，并在显示单元 14 上显示指纹信息获取请求（步骤 S341）。当从指纹获取单元 212 输入指纹信息时，安全性芯片 5 的 MPU 51 接收该指纹信息（步骤 S342），并将它暂时存储在 RAM 52 中。然后，MPU 51 读取客户购买移动电话 1 时预先注册在 ROM 55 中的指纹信息文件 552 中的指纹信息，并比较这些指纹信息，以判断所注册的信息是否与在步骤 S342 中所接收并存储在 RAM 52 中的指纹信息相匹配，即指纹信息认证是否成功（步骤 S343）。

如果这些指纹信息相匹配并且指纹信息认证被判断为成功（步骤 S343 中的“是”），MPU 51 设置指纹认证成功标志，并将所设置的指纹认证

成功标志发送到移动电话 1（步骤 S345）。另一方面，如果这些指纹信息不匹配且指纹信息认证被判断为不成功（步骤 S343 中的“否”），MPU 51 设置指纹认证失败标志，并将所设置的指纹认证失败标志发送到移动电话 1（步骤 S344）。移动电话 1 的 CPU 11 将所发送的指纹认证标志（指纹认证成功标志或指纹认证失败标志）存储在 ROM 15 中（步骤 S346）。从而完成使用指纹信息的生物认证。

注意，尽管此实施例采用了一种结构，在此结构中使用指纹信息的生物认证是在中心服务器 2 中执行的，但是可以将以前获取的指纹信息注册在证书机构服务器 3 中或移动电话 1 中，并发送从中心服务器 2 新获取的指纹信息，以用于证书机构服务器 3 或移动电话 1 中的判断。

然后，安全性芯片 5 的 MPU 51 获取与中心服务器 2 有关的环境信息（步骤 S347）。MPU 51 通过如上所述地总是监控安装在中心服务器 2 的存储单元 25 中的 OS、BIOS 和软件并收集中心服务器 2 的设备名、OS 的名称和版本、连接到外部通信端口 29 的外围设备的设备名和版本、所安装的软件如浏览器的名称和版本来收集环境信息。所收集的环境信息存储在环境信息文件 551 中（步骤 S348）。

安全性芯片 5 的 MPU 51 读取存储在 RAM 52 中的环境信息文件 551 中的环境信息（步骤 S349）。安全性芯片 5 的 MPU 51 通过使用存储在 ROM 55 中的哈希函数为所读取的环境信息计算消息摘要（步骤 S351）。MPU 51 从秘密密钥文件 554 读取由证书机构服务器 3 预先发行的中心服务器 2 的秘密密钥，并加密所述环境信息和消息摘要（步骤 S352）。而且，MPU 51 从电子证书文件 553 读取由证书机构服务器 3 预先发行的电子证书，将该电子证书附加到所加密的环境信息和消息摘要，并将它们发送到移动电话 1（步骤 S353）。移动电话 1 的 CPU 11 将所发送的电子证书和加密的环境信息及消息摘要存储在 RAM 12 中。

移动电话 1 的 CPU 11 访问在所述电子证书中书写的证书机构服务器 3，并请求获取所接收到的电子证书的公共密钥（该证书机构的公共密钥）（步骤 S354）。响应于此请求，证书机构服务器 3 将该电子证书的公共密钥发送到移动电话 1，并且移动电话 1 接收所发送的该电子证书的公

共密钥（步骤 S355）。移动电话 1 的 CPU 11 从 RAM 12 读取所存储的电子证书，使用从证书机构服务器发送来的证书机构的公共密钥来解密所述电子证书，并获取中心服务器 2 的公共密钥（步骤 S356）。

移动电话 1 的 CPU 11 用从证书机构服务器 3 获取的中心服务器 2 的公共密钥来解密所加密的环境信息和消息摘要（步骤 S361）。而且，CPU 11 通过使用存储在移动电话 1 的 ROM 55 中的哈希函数来为解密的环境信息计算消息摘要（步骤 S362）。移动电话 1 的 CPU 11 判断在步骤 S361 中解密的消息摘要是否与步骤 S362 中计算出的消息摘要相匹配，即所述环境信息是否在发送过程中没有被伪造，并且还判断是否所述信息已被发送到一个授权的中心服务器 2 和从该服务器 2 接收到所述信息（步骤 S363）。

如果这些消息摘要不匹配（步骤 S363 中的“否”），CPU 11 判断已发生了某种伪造或“欺骗”，并为电子证书认证设置失败标志（S365）。

另一方面，如果这些消息摘要相匹配（步骤 S363 中的“是”），CPU 11 判断没有发生“欺骗”或伪造，并为电子证书认证设置成功标志（步骤 S364）。然后，移动电话 1 的 CPU 11 将电子证书认证的标志（电子证书认证成功标志或电子证书认证失败标志）存储在 ROM 15 中（步骤 S366）。

移动电话 1 的 CPU 11 从环境信息 DB 151 读取对应于在步骤 S104 中所确定的等级的环境信息的条件（步骤 S371）。然后，CPU 11 判断所解密的环境信息是否满足在步骤 S371 中从环境信息 DB 151 读取的环境信息的条件（步骤 S372）。如果该条件未被满足（步骤 S372 中的“否”）CPU 11 就设置环境认证失败标志（步骤 S374）。另一方面，如果所述条件被满足（步骤 S372 中的“是”），CPU 11 就设置环境认证成功标志（步骤 S373）。移动电话 1 的 CPU 11 在 ROM 15 中存储环境认证的标志（环境认证成功标志或环境认证失败标志）（步骤 S375）。

CPU 11 读取存储在 ROM 15 中的指纹认证标志、电子证书标志和环境认证标志，并判断指纹认证成功标志、电子证书认证成功标志和环境认证成功标志中的全部是否在与（AND）条件下都被设置（步骤 S376）。如

果所有成功标志被设置（步骤 S376 中的“是”），CPU 11 判断中心服务器 2 是安全的，设置安全标志，并跳转到步骤 S121（步骤 S377）。

另一方面，如果在生物认证、电子证书认证（PKI 认证）和环境认证的至少之一中设置了失败标志，CPU 11 就设置失败标志并跳转到步骤 5 S123（步骤 S378）。因此，只有当在移动电话 1 和中心服务器 2 中，生物认证、环境认证和电子证书认证中的全部都被判断为成功时，移动电话 1 和中心服务器 2 才被判断为是安全的，并允许随后的信息发送和接收。因此可以为通信环境提供更高的安全性。

实施例 6 说明了一种技术，在其中，当移动电话 1 和中心服务器 2 中 10 所有的生物认证、环境认证和电子证书认证中都被判断为成功时，移动电话 1 和中心服务器 2 才被判断为是安全的，并允许随后的信息发送和接收。类似地，不必赘言，当在移动电话 1 和在线商店的万维网服务器 4 15 （或其他移动电话、洗衣机、或如个人计算机的信息处理设备，未示出）中，所有的生物认证、环境认证和电子证书认证中都被判断为成功时，可以判断移动电话 1 和万维网服务器 4 是安全的，并允许随后的信息发送和接收。

实施例 2 到实施例 6 具有上述多种结构。由于其他结构和功能与实施例 1 中的那些相同，因此对应的部件以相同的标号所标识，并省略了其说明。

20 如上所详叙的那样，根据本发明，接收诸如用户的指纹的生物信息，并判断所接收的生物信息是否正确。而且，收集环境信息，包括与连接到所述信息处理设备的外围设备或安装在所述信息处理设备中的软件有关的信息。信息处理设备将所收集的环境信息发送到第一认证设备。而且，信息处理设备将由第二认证设备发行的电子证书和与交易相关、用所述信息处理设备的秘密密钥加密的信息发送到第一认证设备。当第一认证设备接收到所述电子证书和所加密的信息时，它通过使用从第二认证设备（证书机构）获取的第二认证设备的公共密钥来从所发送的电子证书中获取信息处理设备的公共密钥。然后，第一认证设备用所获取的信息处理设备的公共密钥来解密所述加密信息，并判断所解密的信息是否正确。

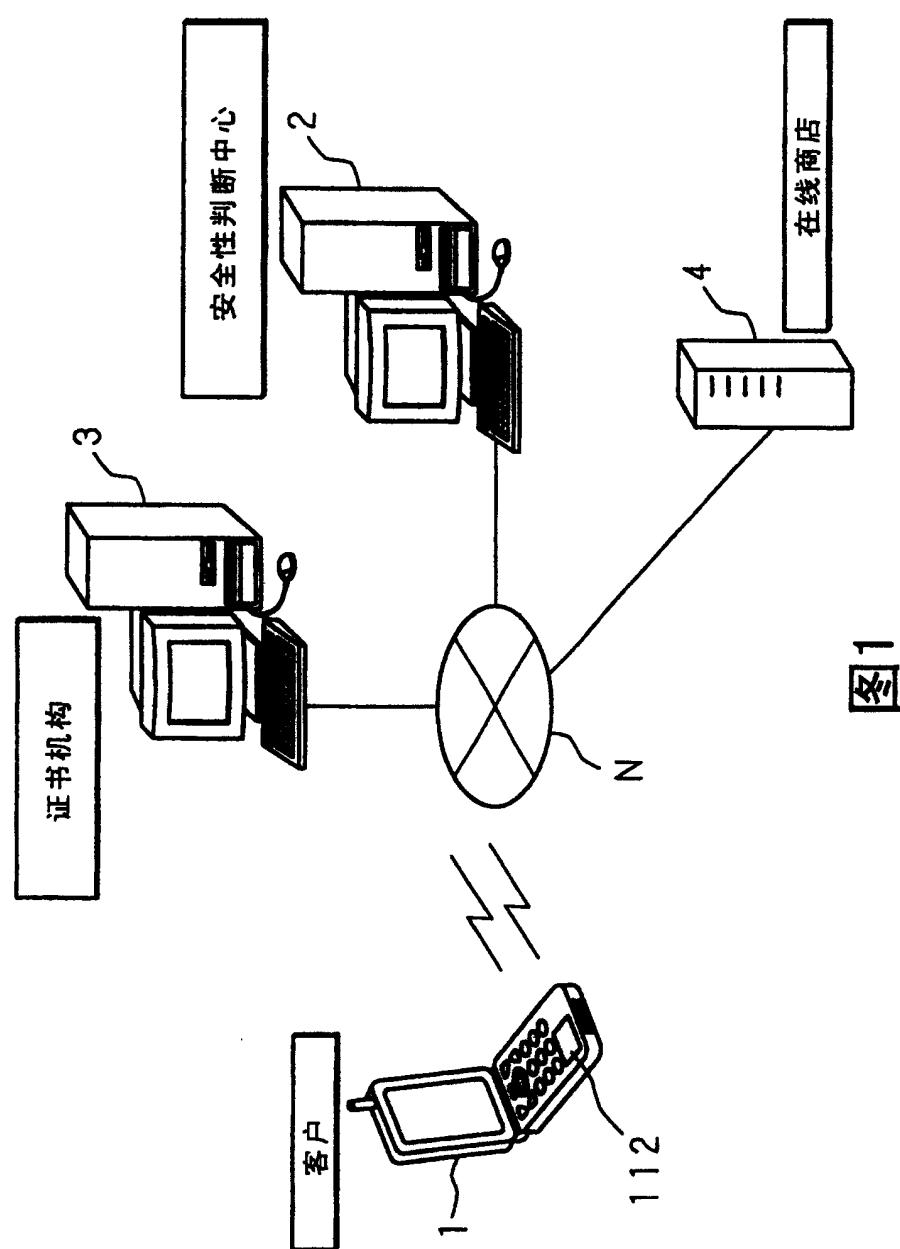
第一认证设备参考一个环境信息数据库和所发送的信息并判断所发送的环境信息是否正确，其中所述环境信息数据库存储根据要发送和接收的信息而被划分等级的环境信息的条件。当所有生物信息认证、环境信息认证和电子证书认证都被判断为成功时，第一认证设备判断信息处理设备是安全的。利用这一结构，本发明可以在确保信息处理设备的安全性的同时实现信息的顺利发送和接收以及交易。而且，也在第一认证设备中进行生物信息认证、电子证书认证和环境认证，并且，只有当在信息处理设备中进行的生物信息认证、电子证书认证和环境认证以及第一认证设备中进行的生物信息认证、电子证书认证和环境认证都被判断为成功时，第一认证设备和信息处理设备才都被判断为是正确的。因此可以确保更高的安全性。

另外，根据本发明，接收与用户有关的生物信息，并且通过判断所接收的生物信息是否正确来进行个人认证。然后，信息处理设备将所收集的环境信息发送到第一认证设备，并且在第一认证设备中进行环境信息的认证。在将补丁软件等从第一认证设备发送到信息处理设备的情况下，第一认证设备将由第二认证设备发行的电子证书和用由第二认证设备发行的秘密密钥加密的软件发送到信息处理设备。当信息处理设备接收到所述电子证书和加密的软件时，它向第二认证设备请求一个公共密钥，并通过使用这一证书机构的公共密钥来从所述电子证书获取第一认证设备的公共密钥。然后，信息处理设备用所获取公共密钥来解密所述加密的软件，并判断所解密的软件是否正确。最后，当由上述个人认证、环境认证和电子证书认证所进行的认证都被判断为成功时，在信息处理设备中安装所解密的软件。利用这样一种结构，本发明可以防止第三人的“欺骗”，并在保持高度安全性的同时为信息处理设备提供例如补丁软件和固件的软件。

而且，根据本发明，信息处理设备包括主电源供应装置、副电源供应装置和被构造来从副电源供应装置接收电源供应的用于接收的通信装置。在不是由主电源供应装置供应电源即在主电源不是开通（ON）的情况下，当从第一认证设备发送来电子证书和用秘密密钥加密的软件时，用于接收的通信装置就使用副电源供应装置来接收这些信息并将它们暂时存储

在存储器中。然后，当主电源供应装置供应电源时，读取所存储的电子证书和软件，判断所发送的软件是否正确，并进行个人认证和环境认证。利用这样一种结构，本发明可以在确保安全性之后向客户发布大量补丁软件，包括没有打开他们的信息处理设备的客户。具体地说，通过提供在预定时刻处和该时刻之后从存储单元删除所存储的数据的软件，本发明可具有若干有益效果，例如有效地防止将软件用作 DDoS 攻击的手段的效果。

在不偏离其实质特征的精神的情况下，本发明可以以若干形式实施，因而这些实施例是示例性的而不是限制性的，因为本发明的范围由权利要求而不是在其前面的说明书所限定，并且所有落入权利要求范围内的变化或此范围中的等同物因此被权利要求所覆盖。



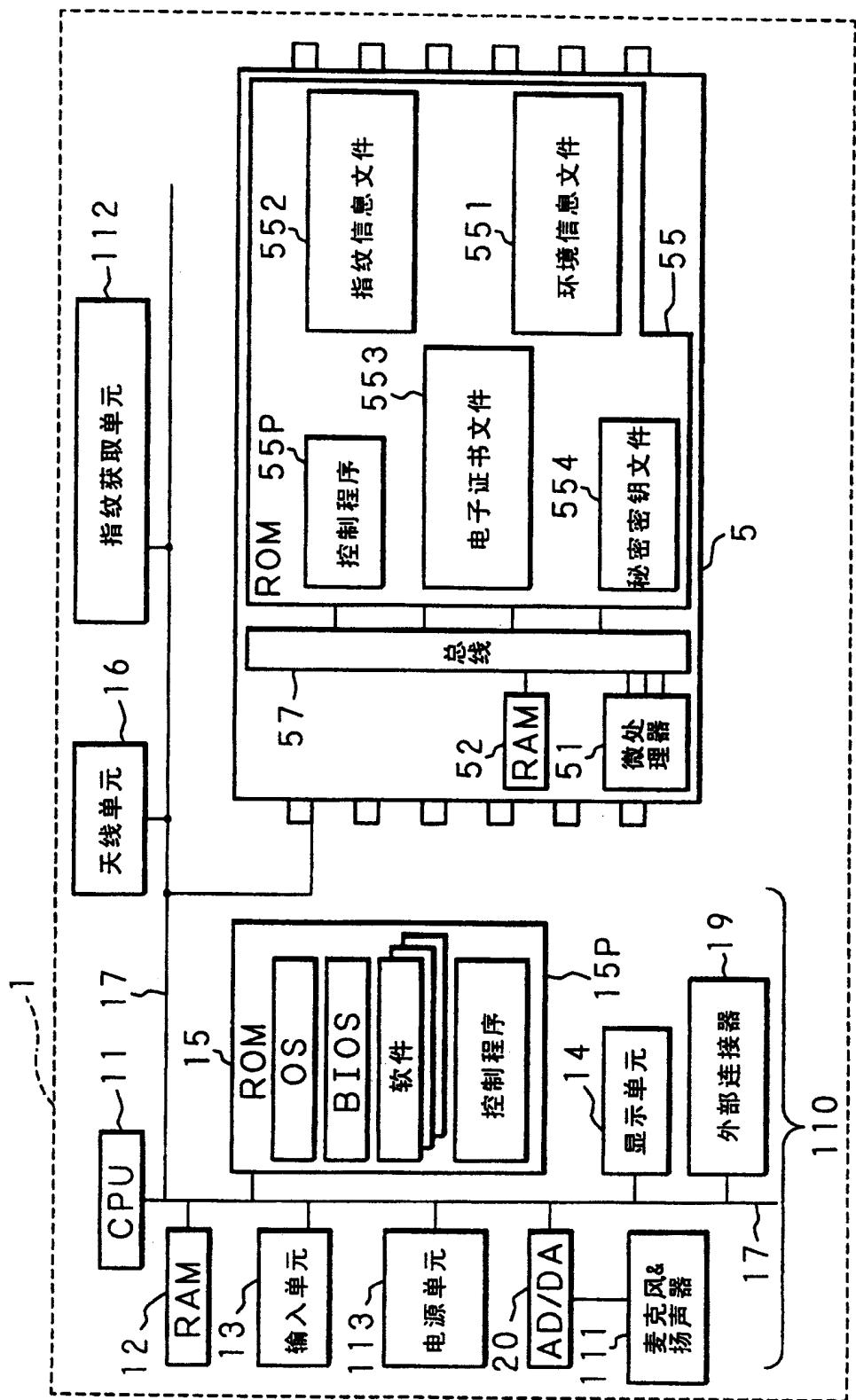


图2

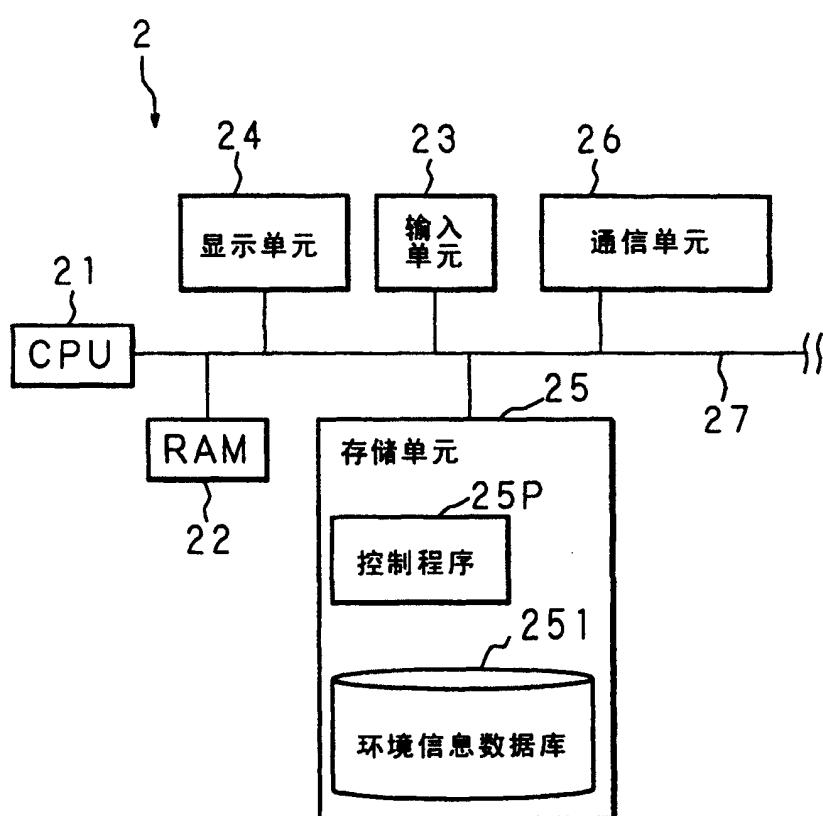


图3

## 环境信息数据库

等级	价格信息	产品信息	环境条件			
			设备名	版本	软件名	版本
6	~¥100	CHAKU-MERO 图像数据	S001~ S004 F001~ F004 N001~ N004 ⋮	1.0 或更高 1.0 或更高 — ⋮	A B C ⋮	2.0 或更高 1.0 或更高 1.0 或更高 ⋮
5	¥101~ ¥3,000	普通文档	S003. S004 F003. F004 N003. N004 ⋮	1.5 或更高 — — ⋮	B C ⋮	2.5 或更高 1.0 或更高 ⋮
⋮	⋮	⋮	⋮	⋮	⋮	⋮
1	¥50,000~	股票证书	S004 F004 N004 ⋮	2.0 或更高 — ⋮	C	3.0 或更高 — ⋮

图4

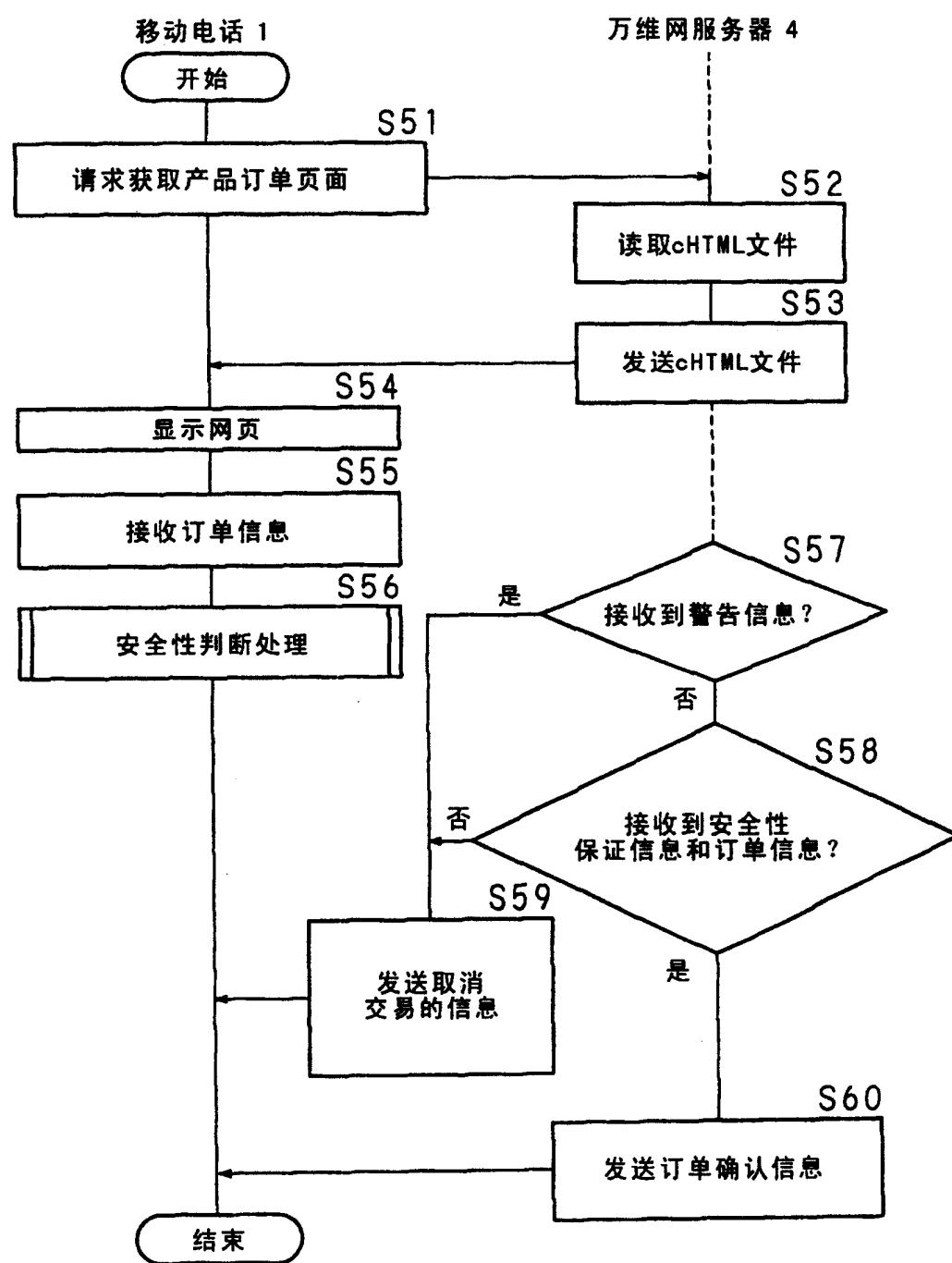


图5

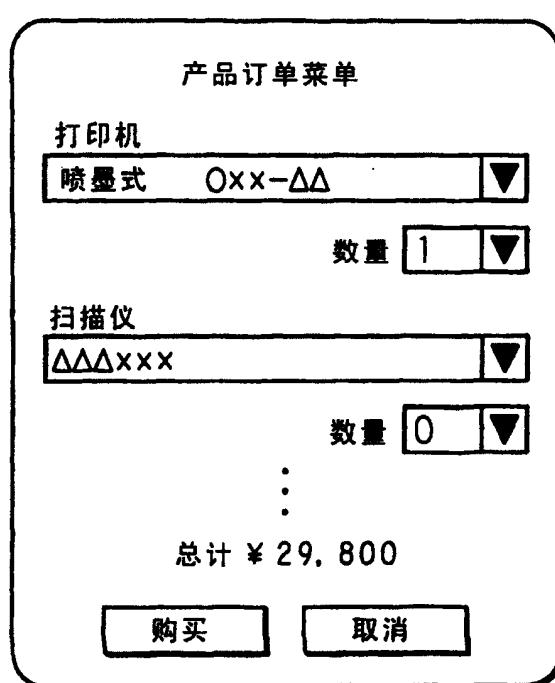


图6

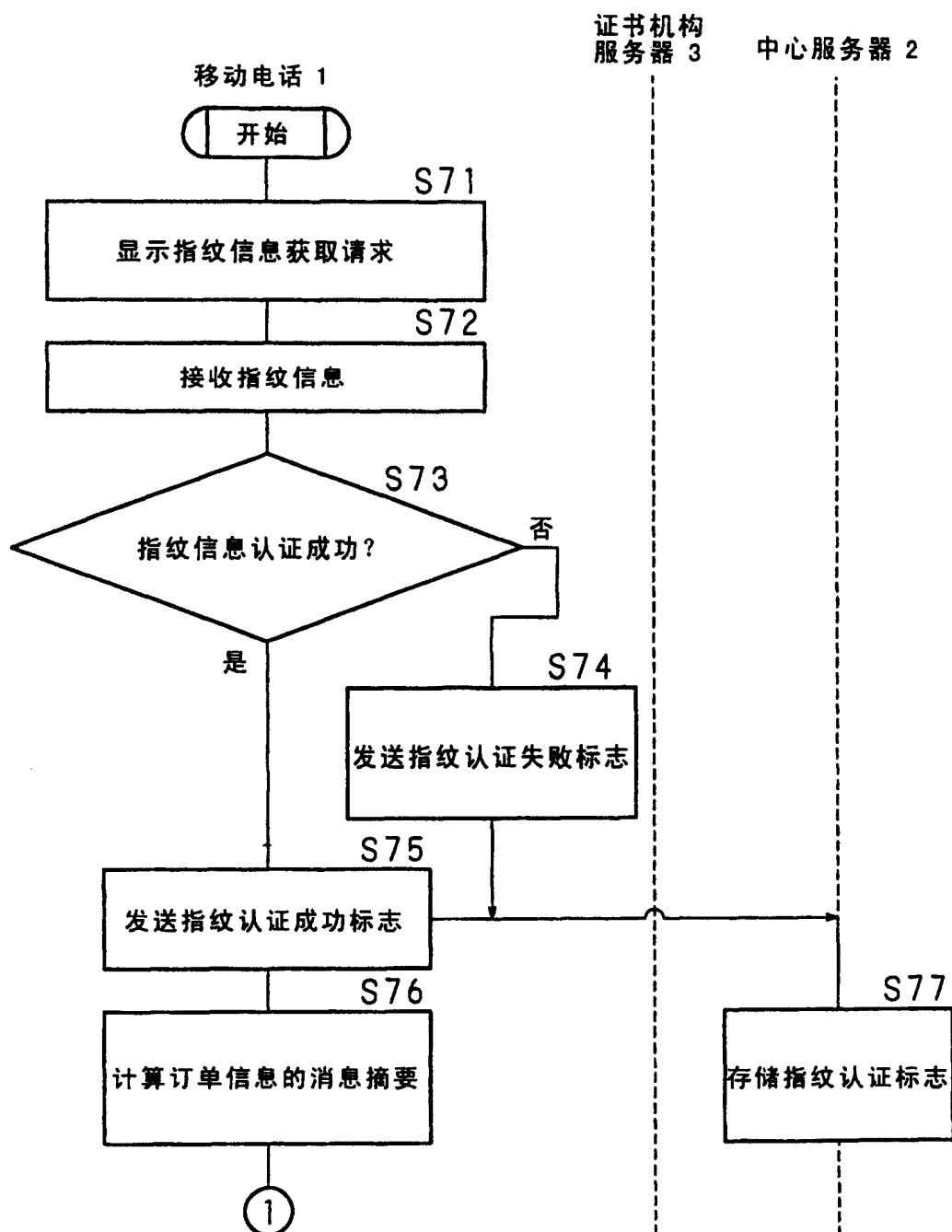


图7

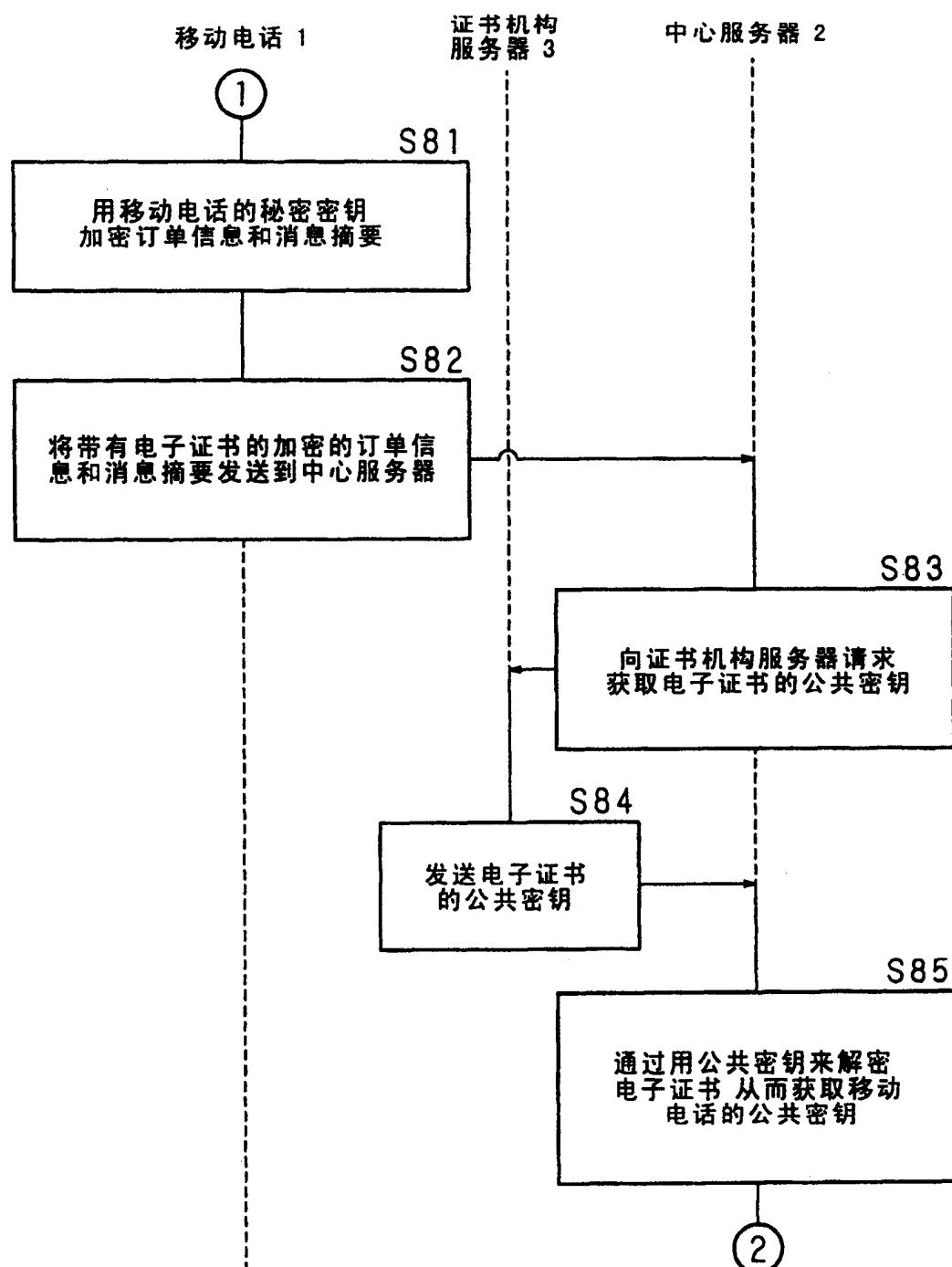


图8

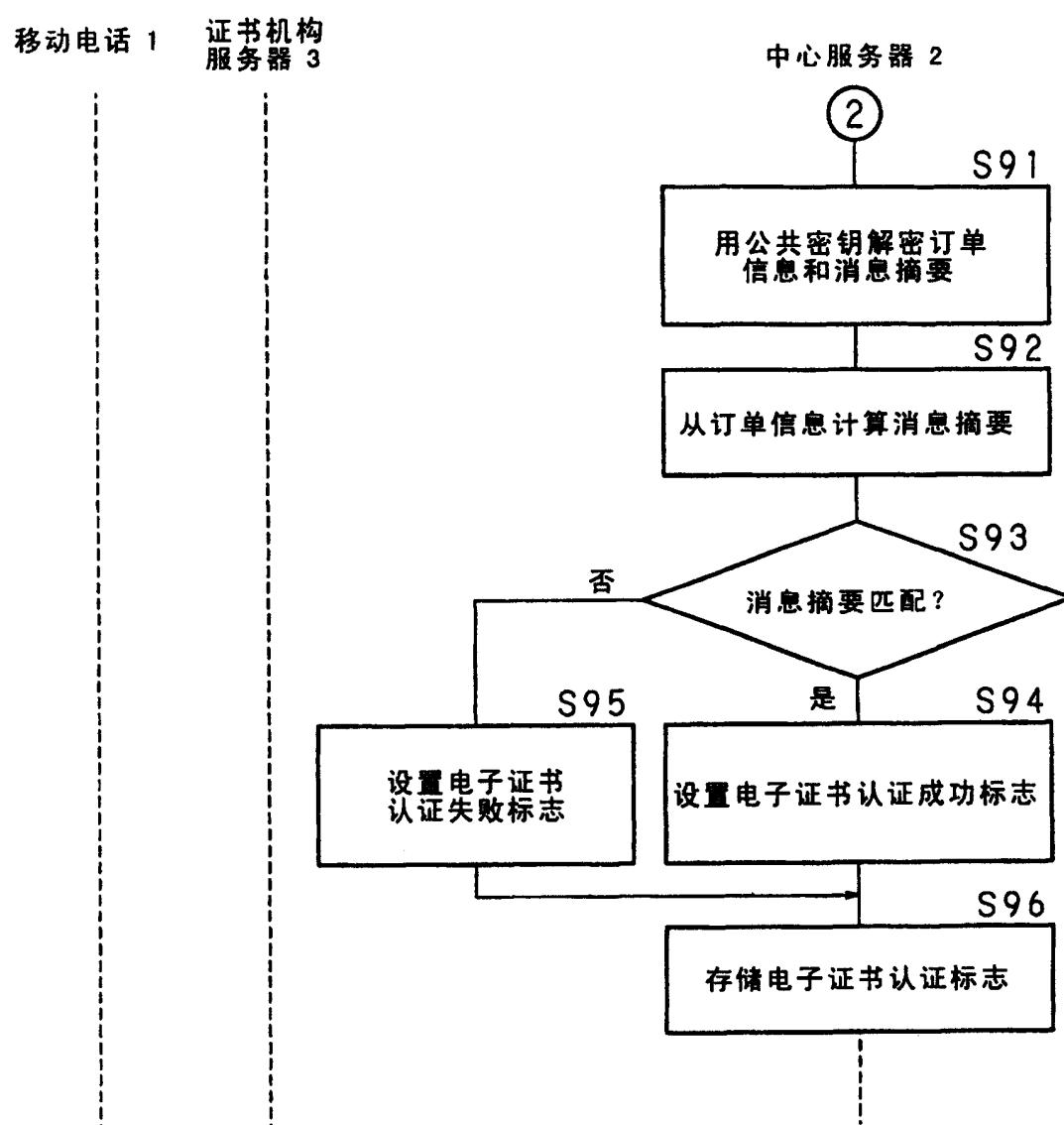


图9

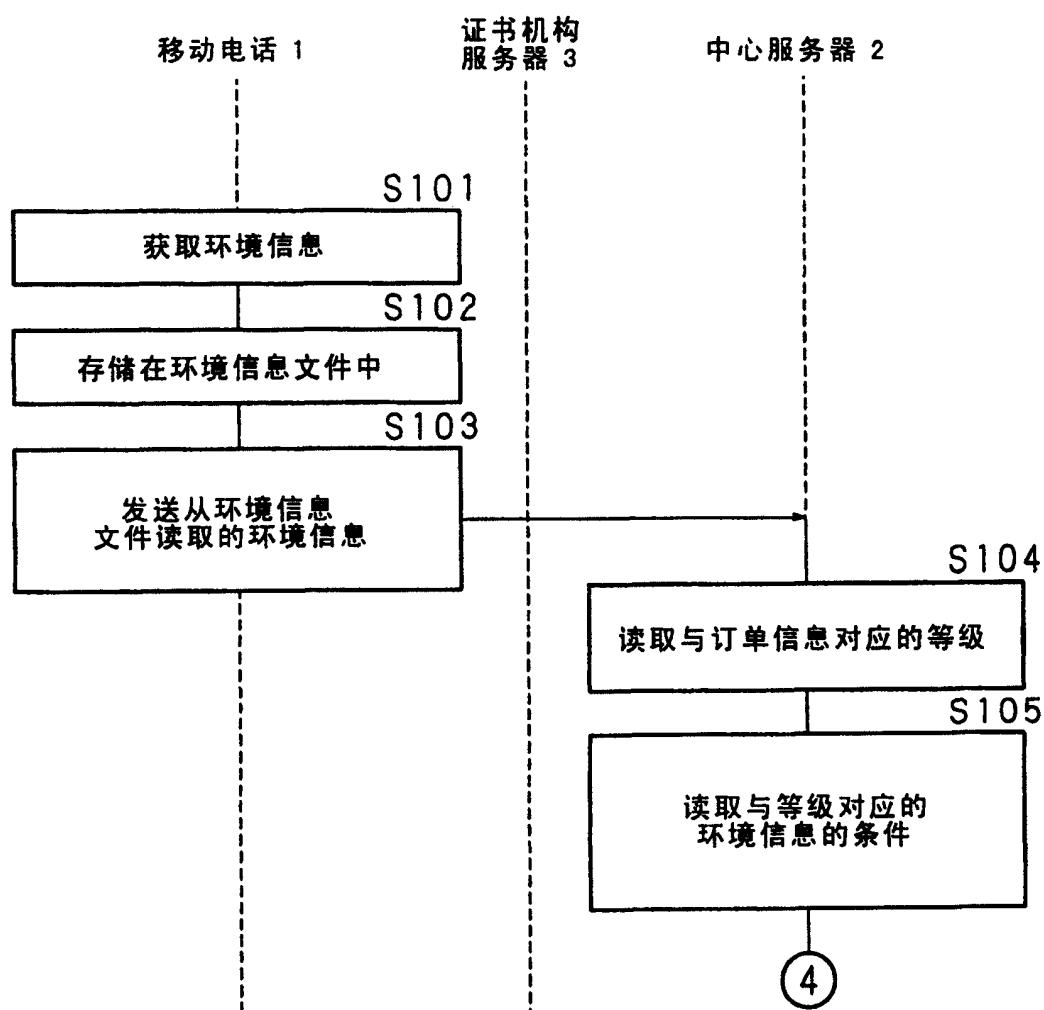


图10

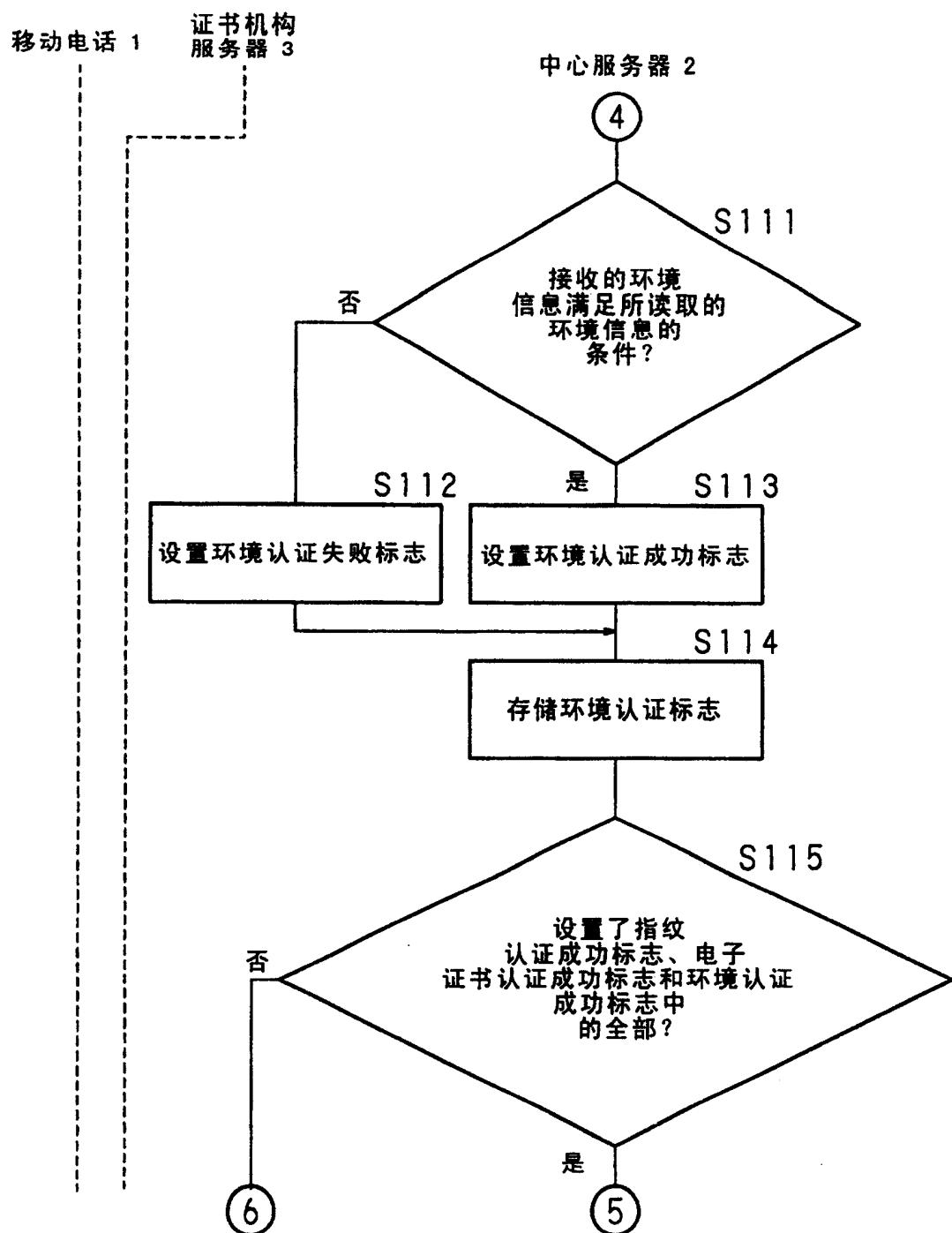


图11

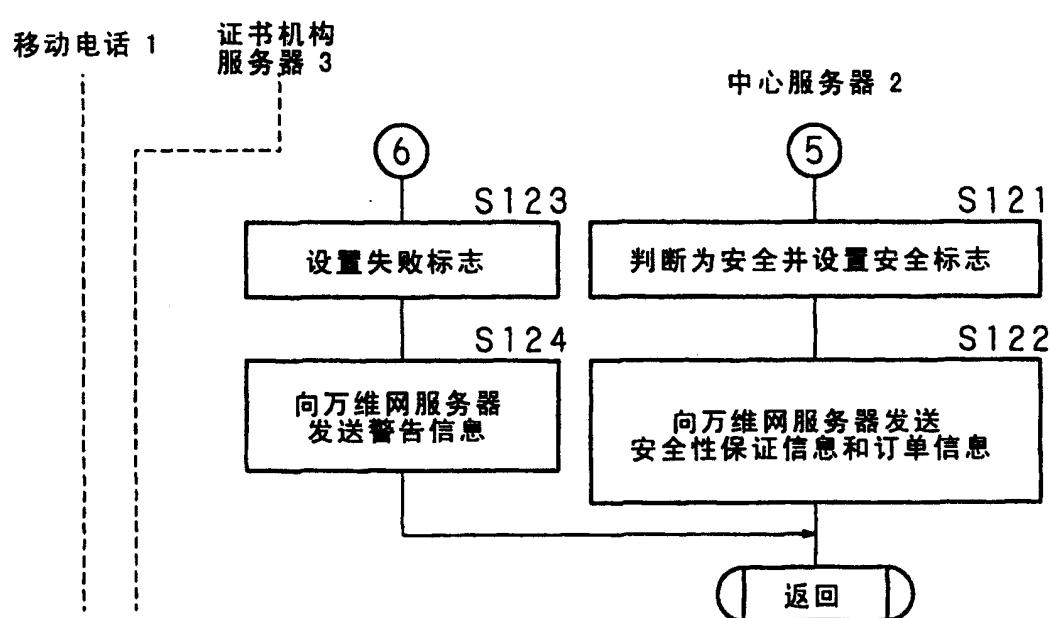


图12

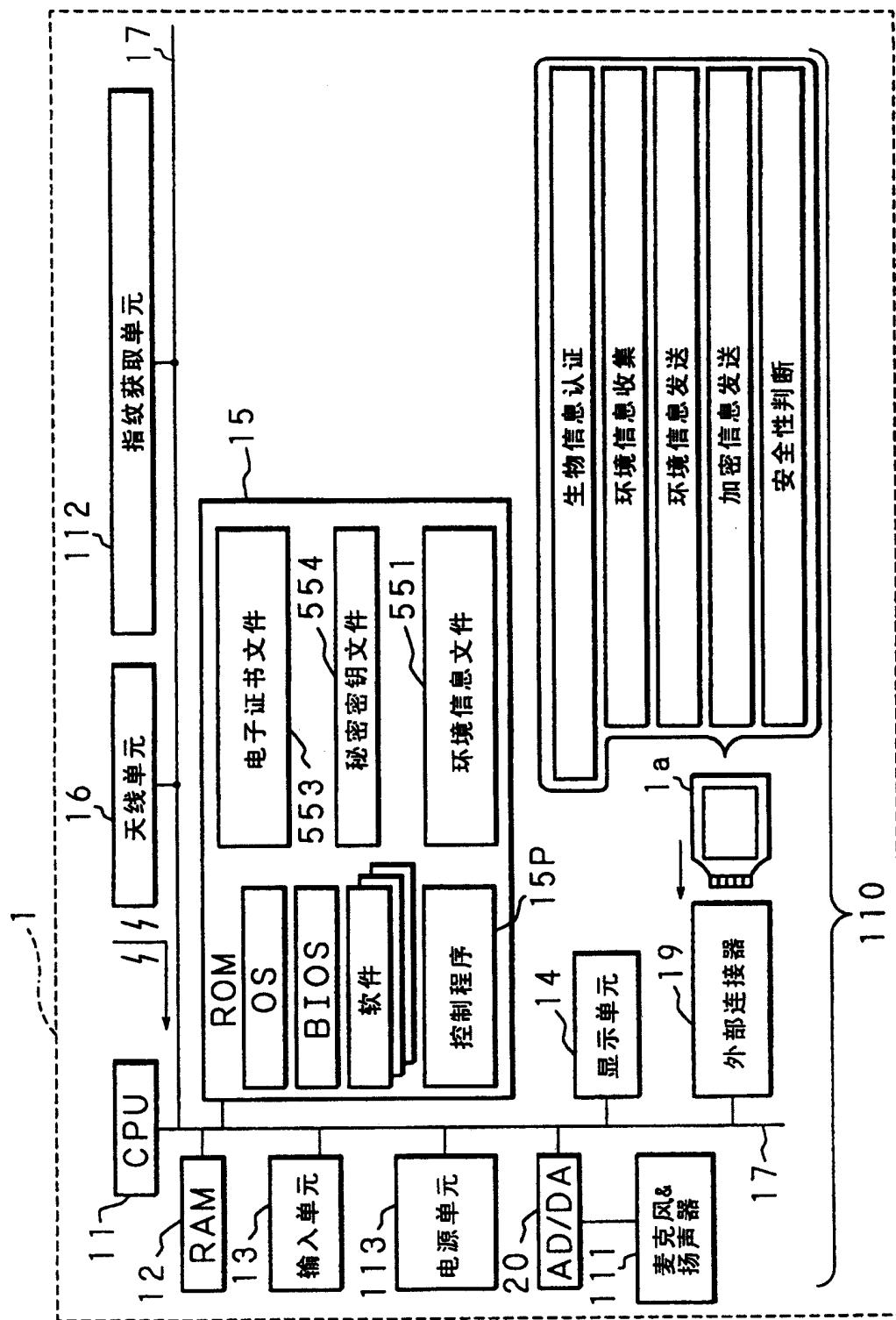


图13

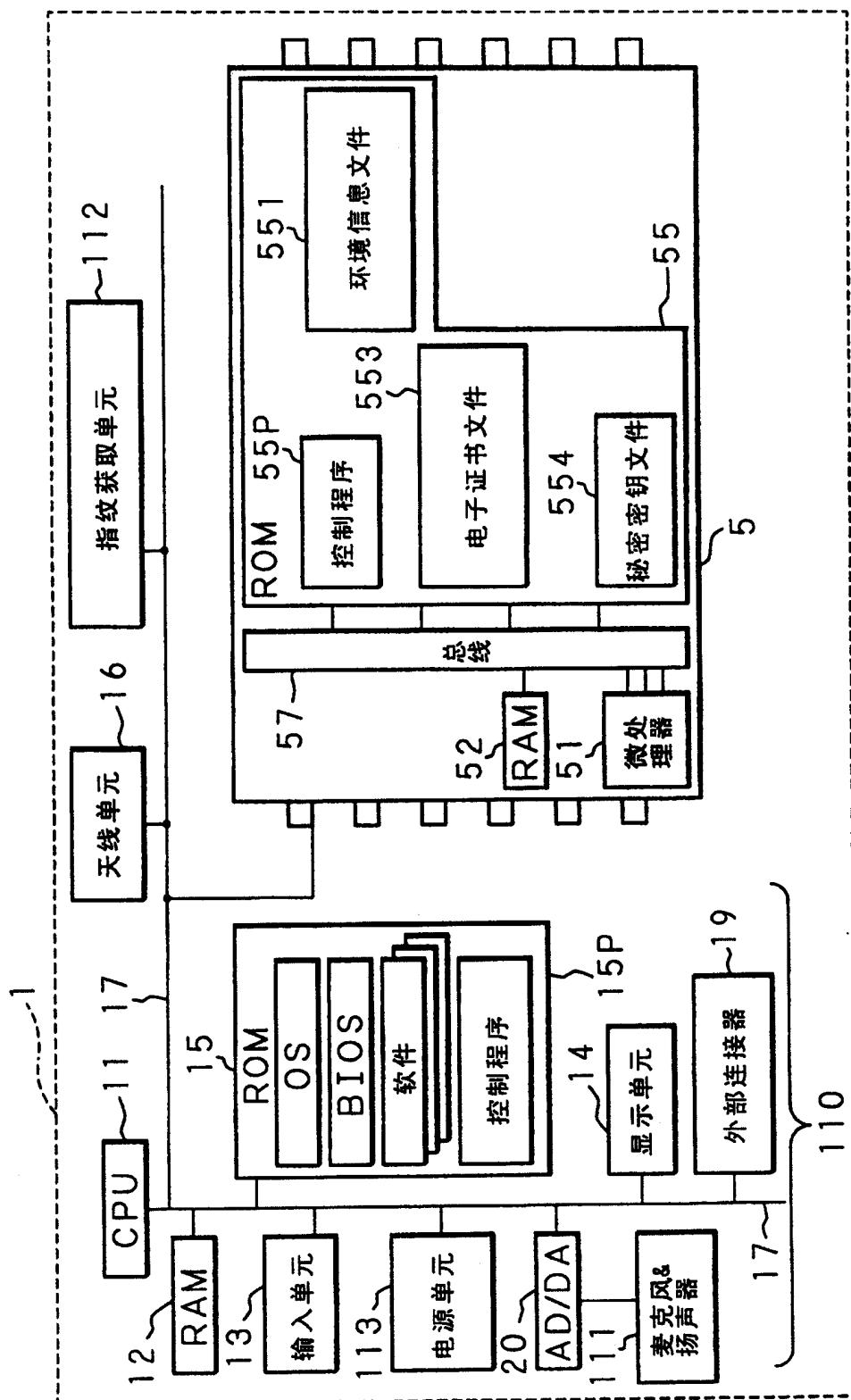


图14

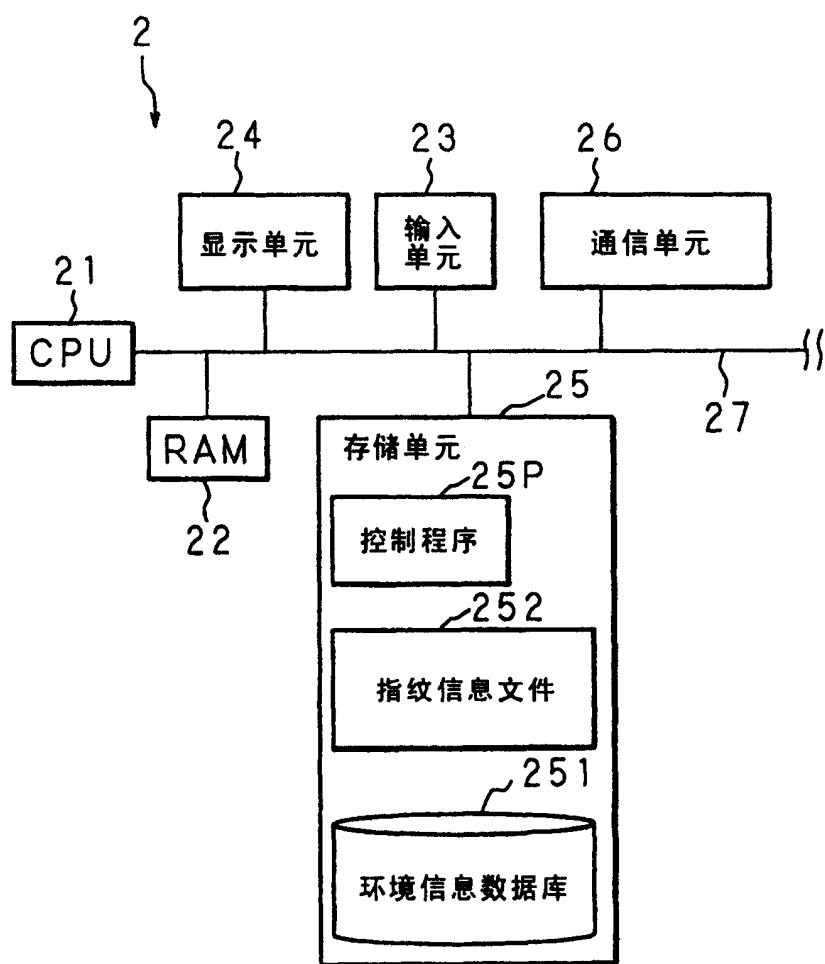
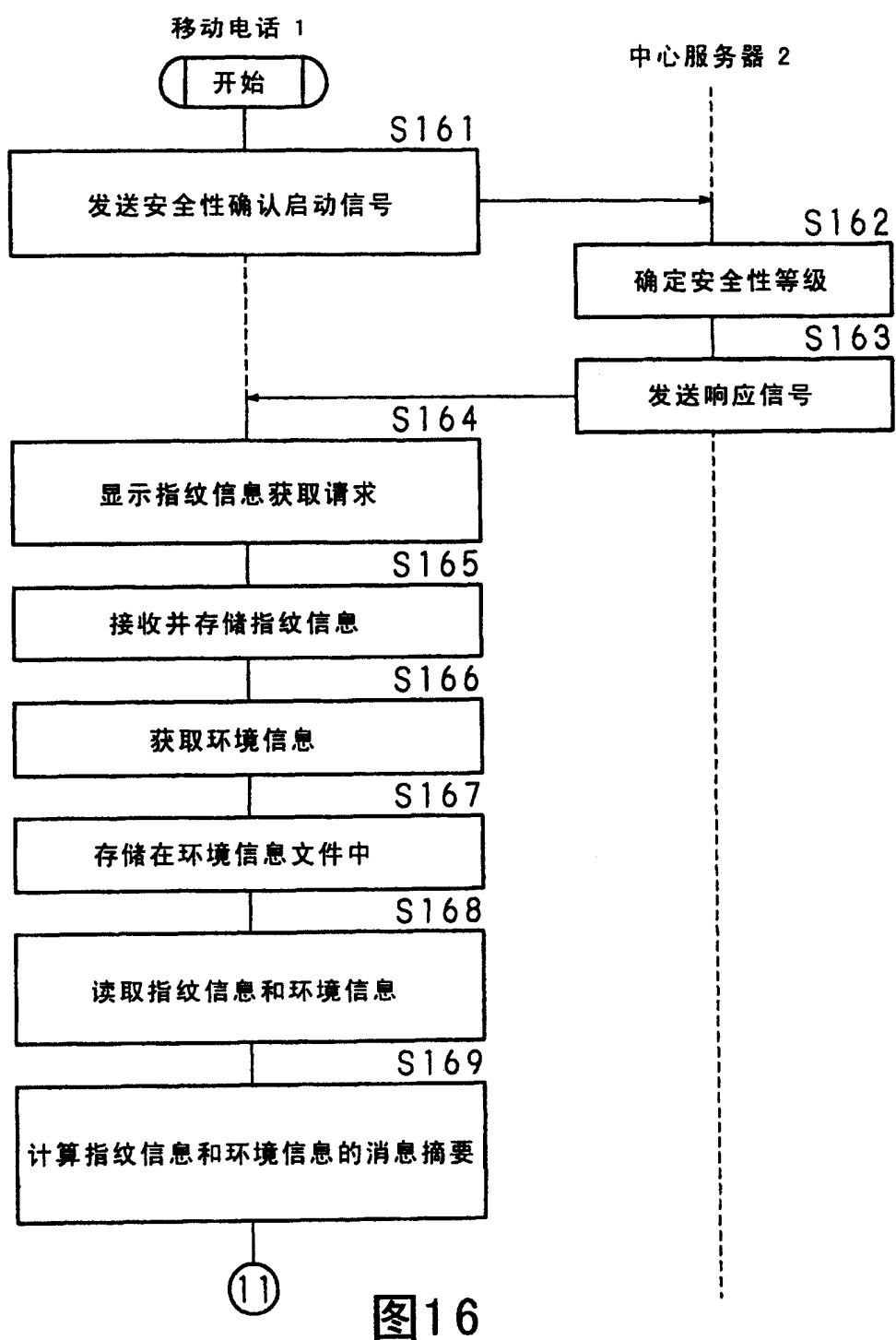


图15



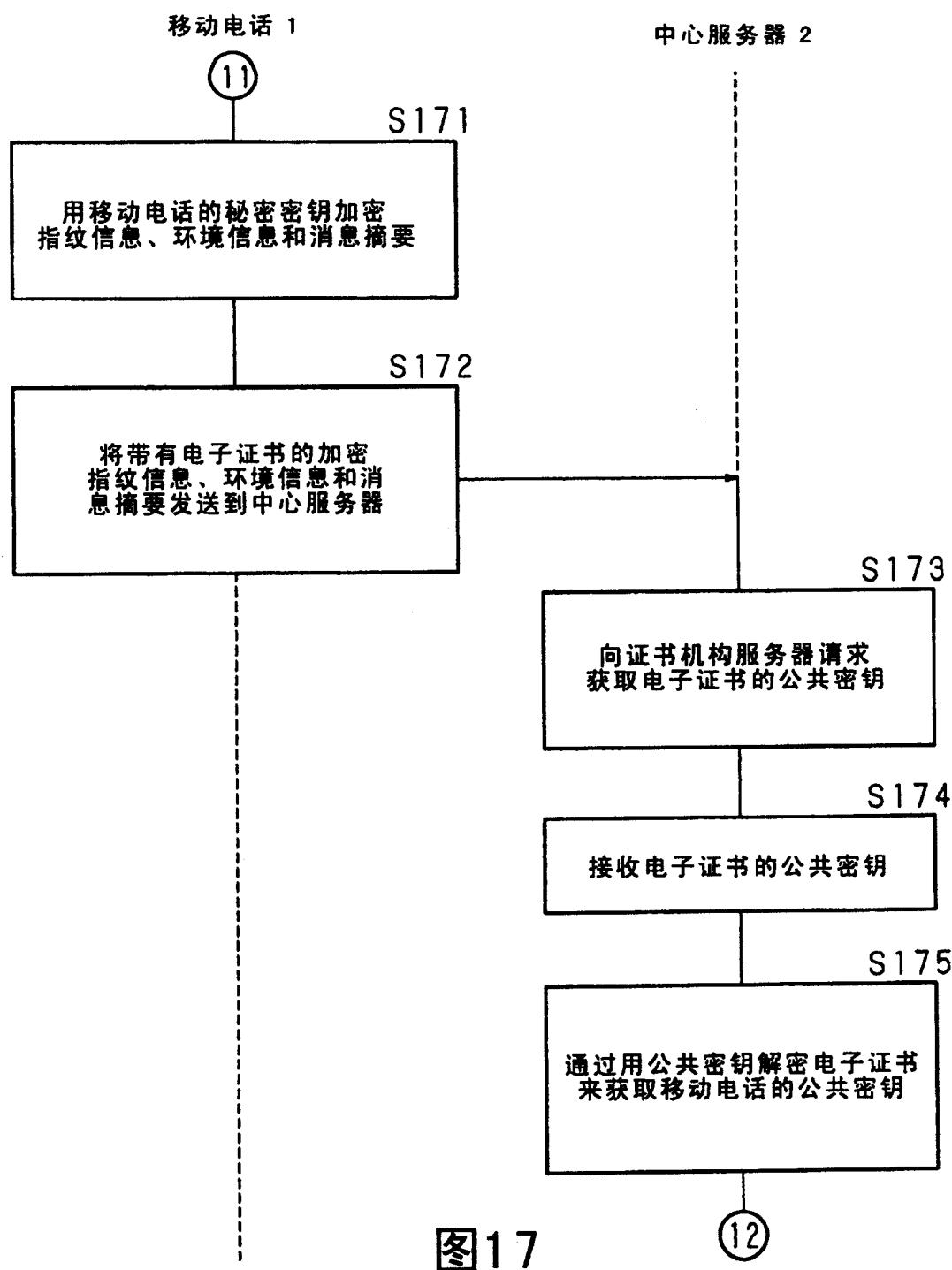


图17

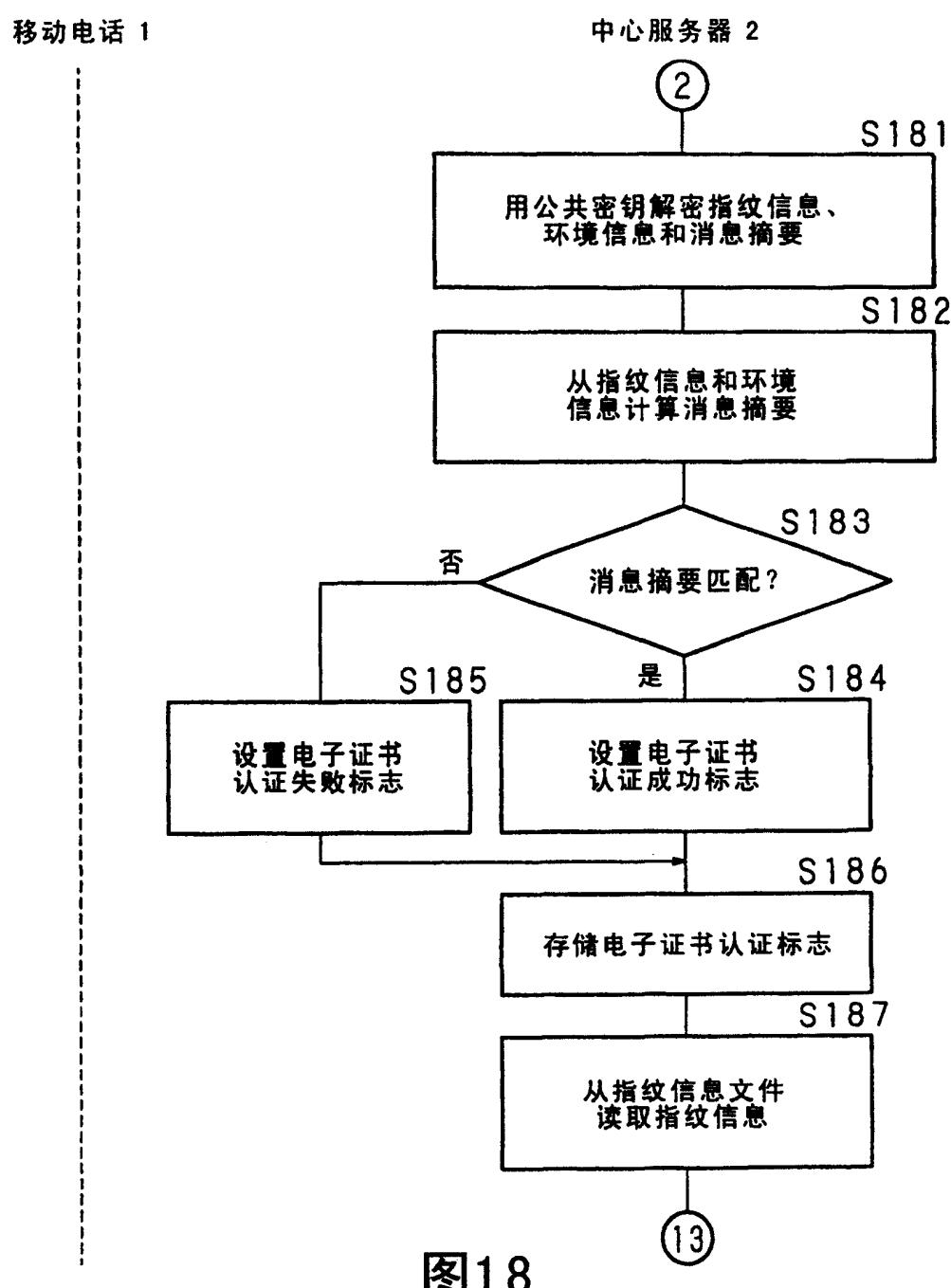


图18

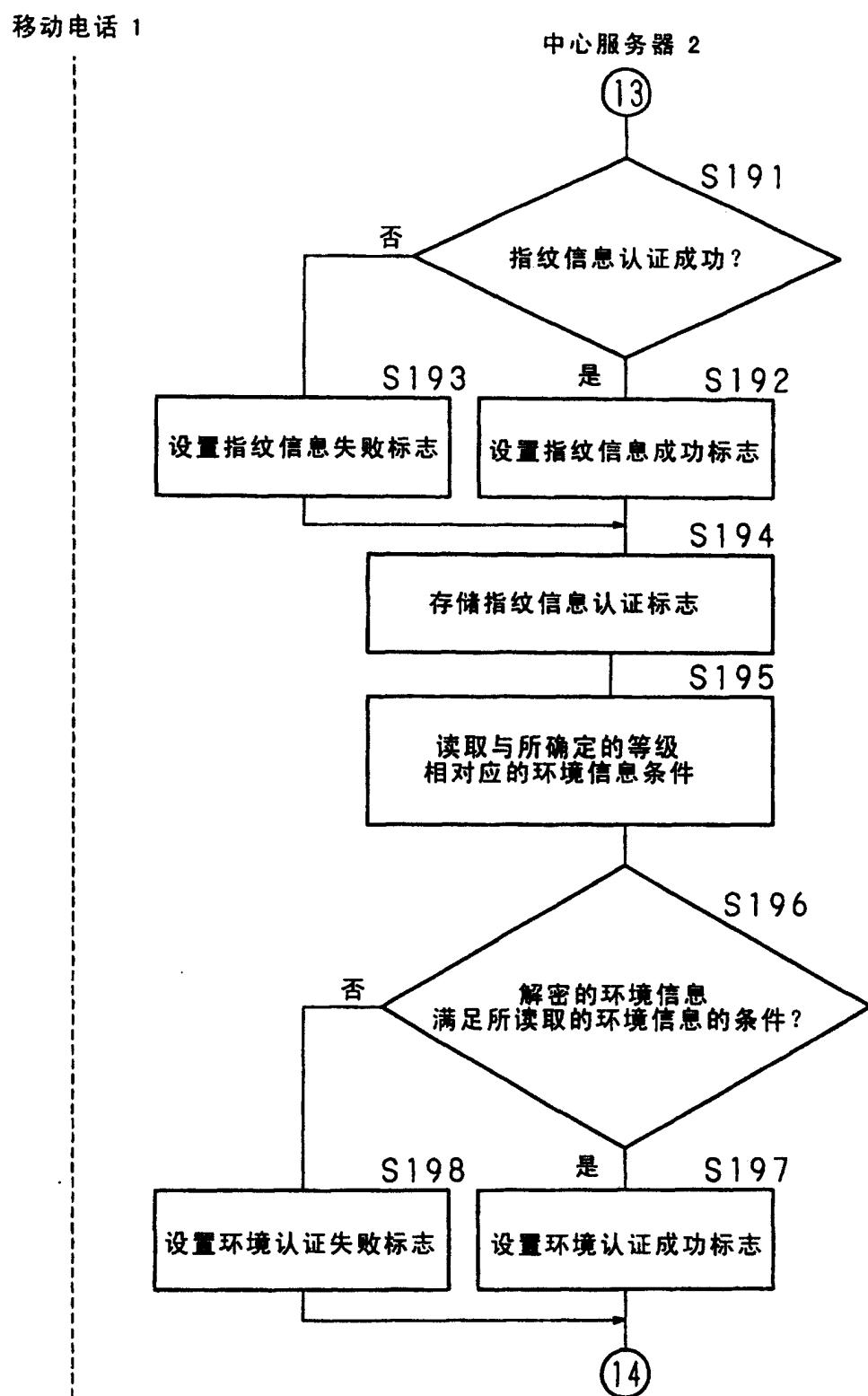


图19

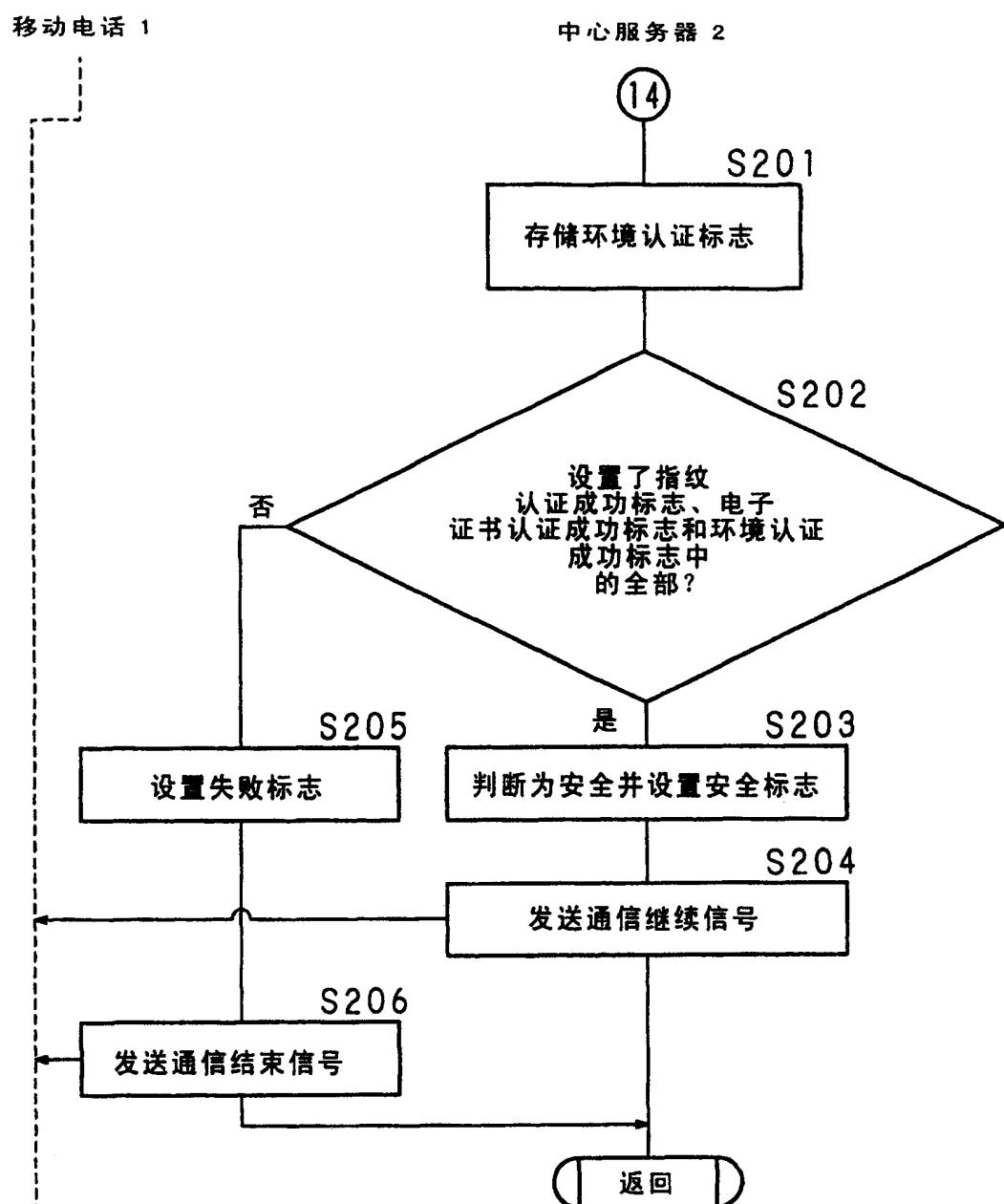


图20

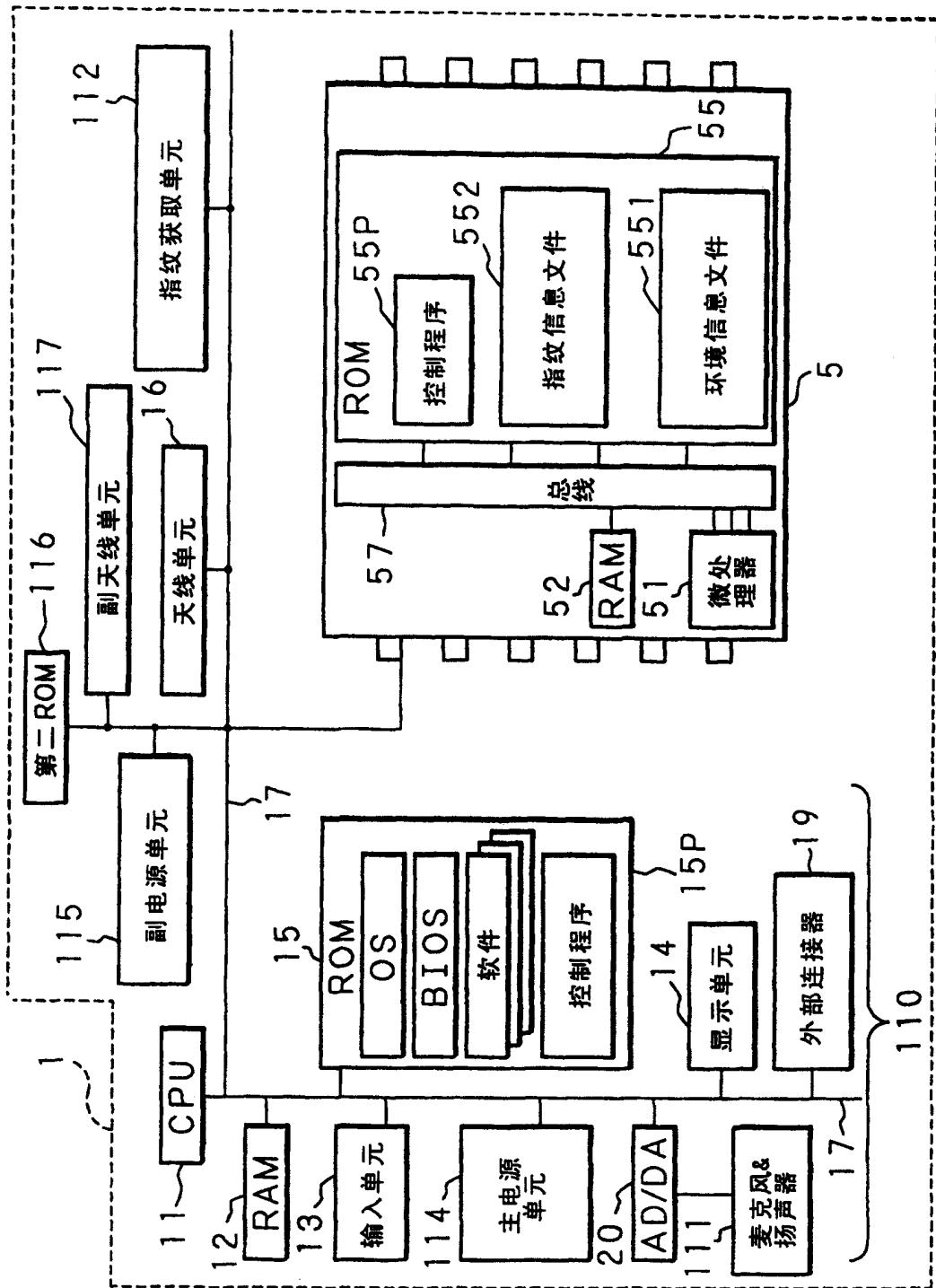


图21

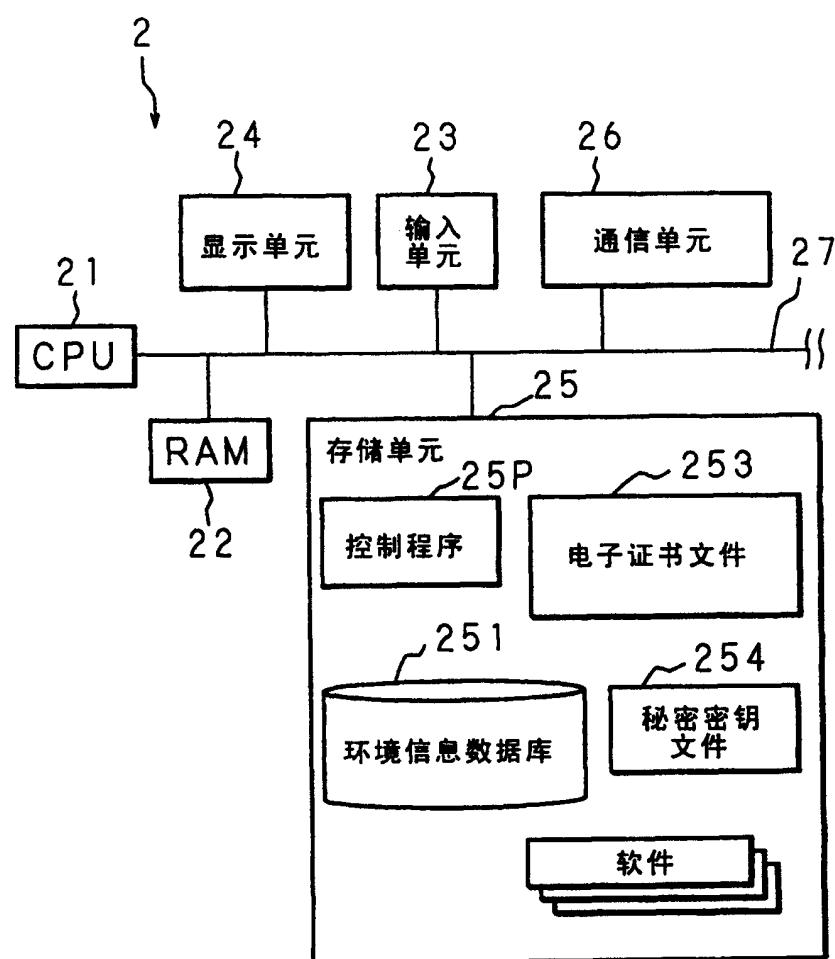


图22

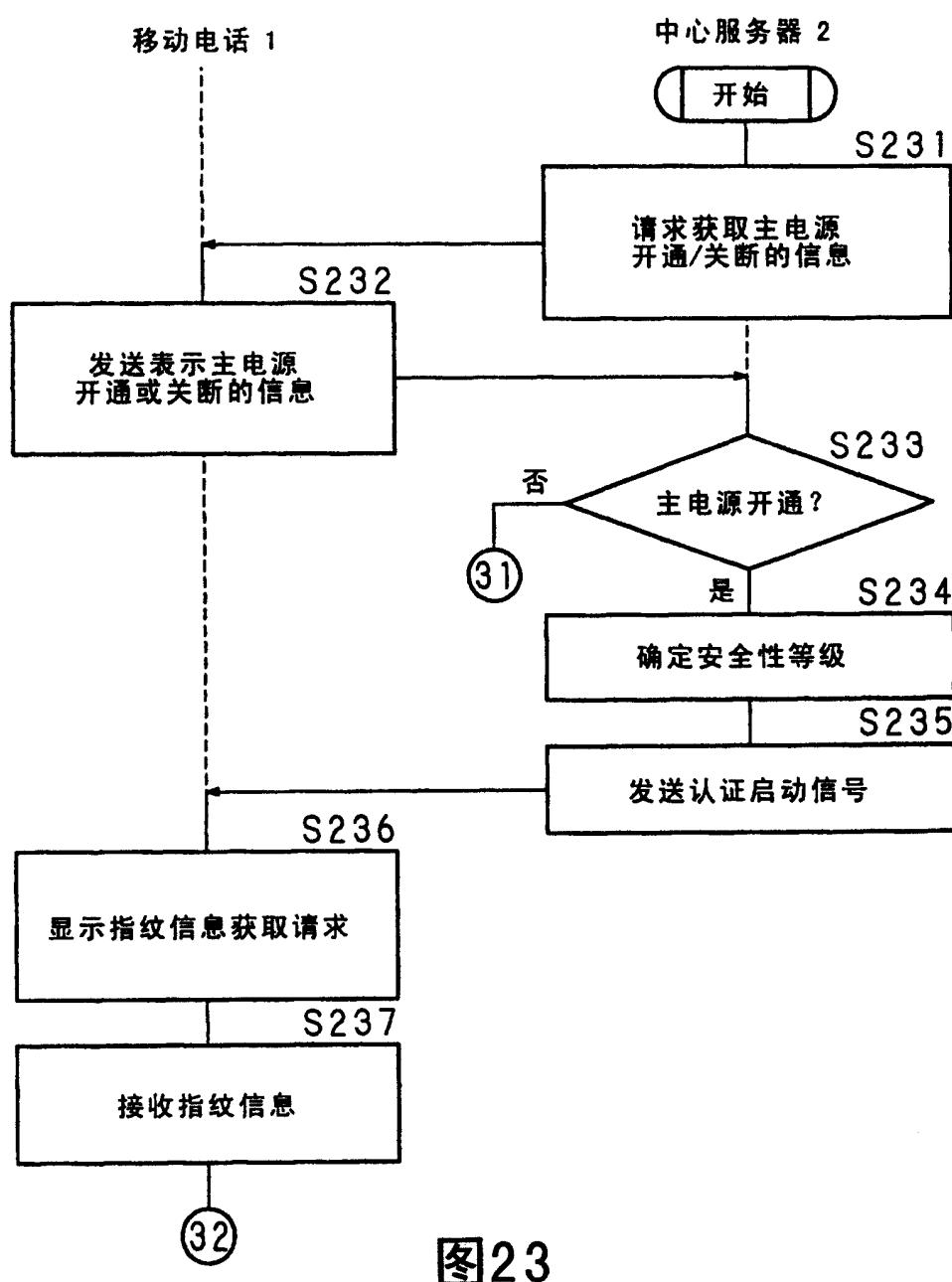
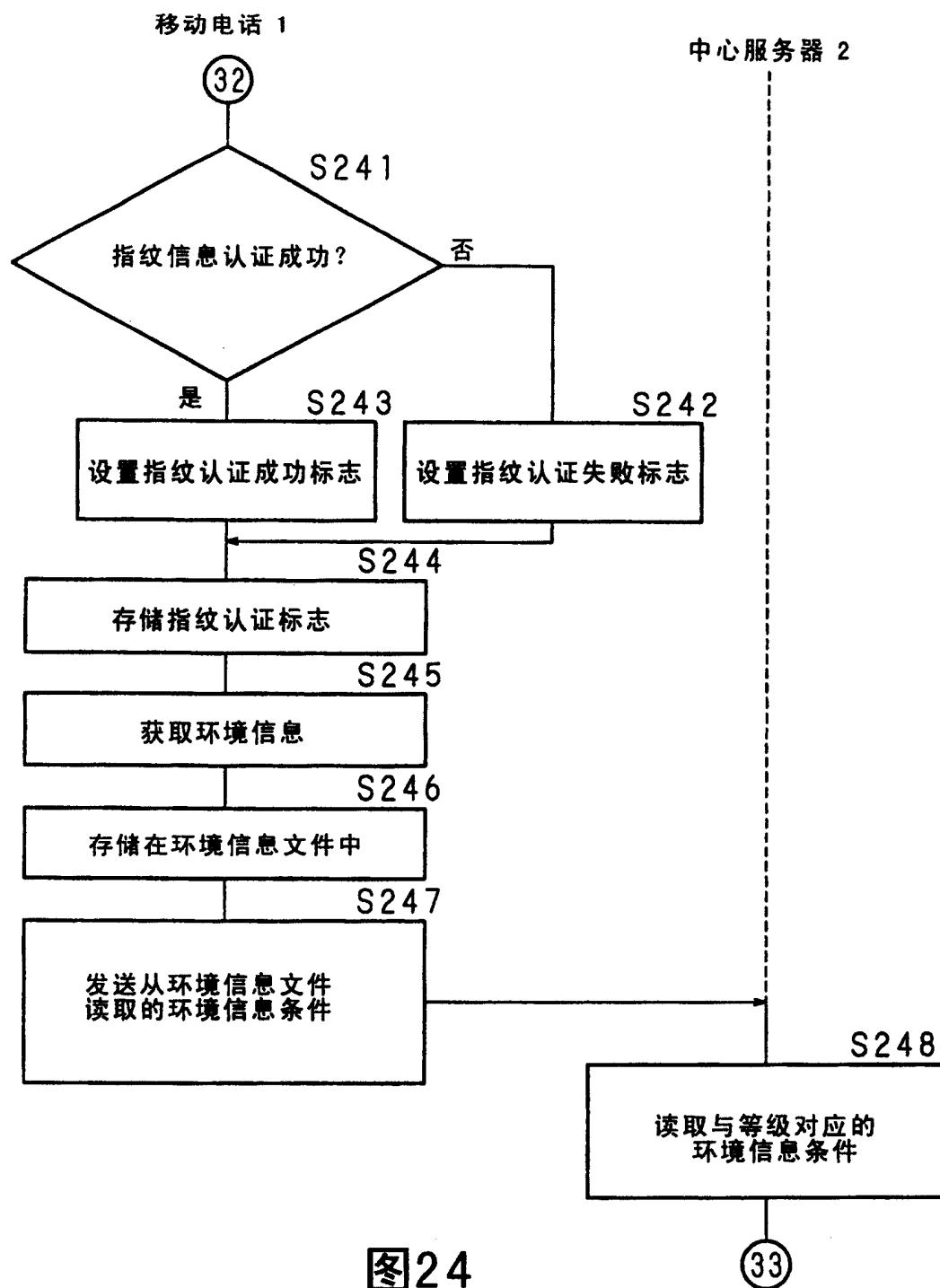


图23



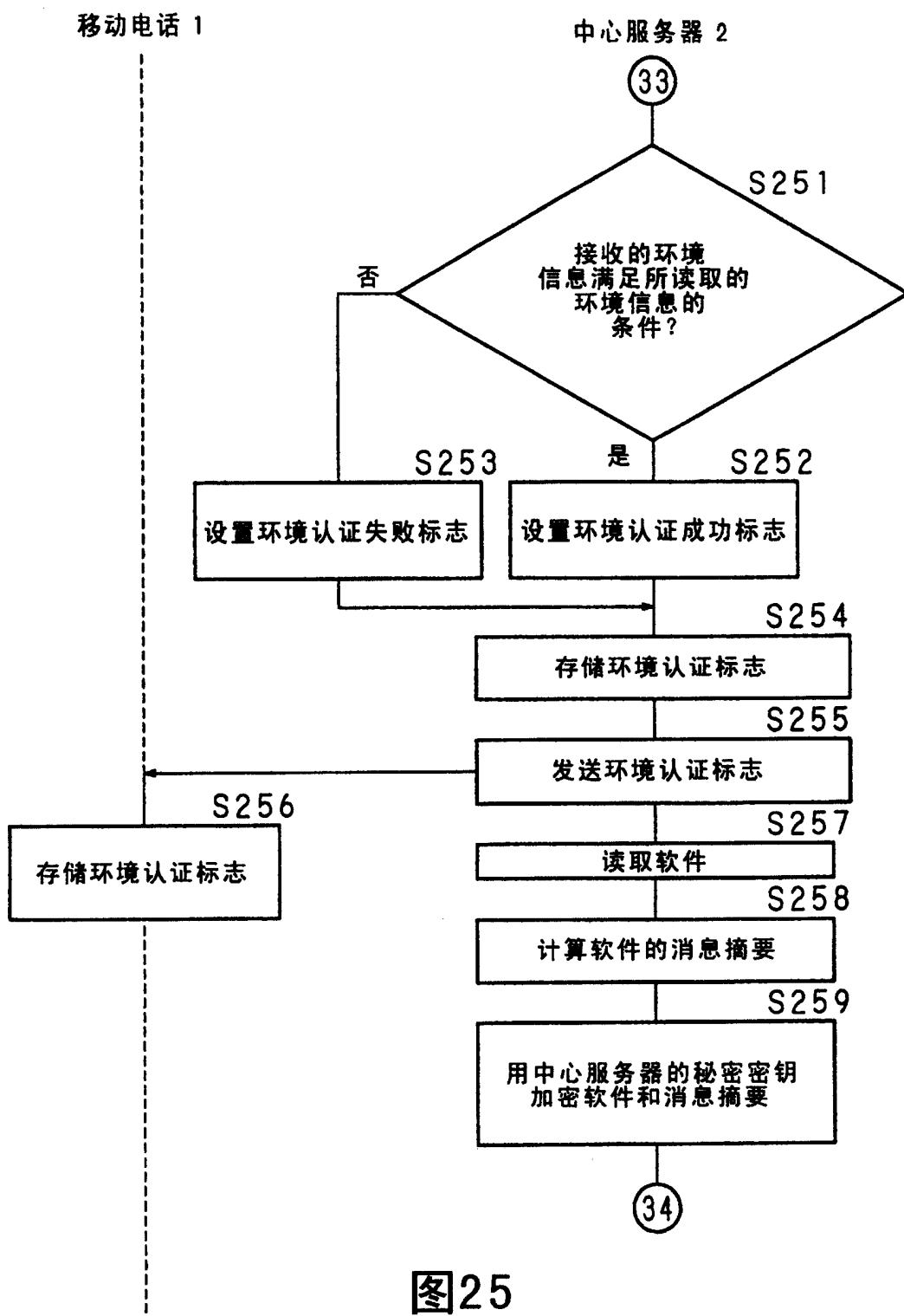


图25

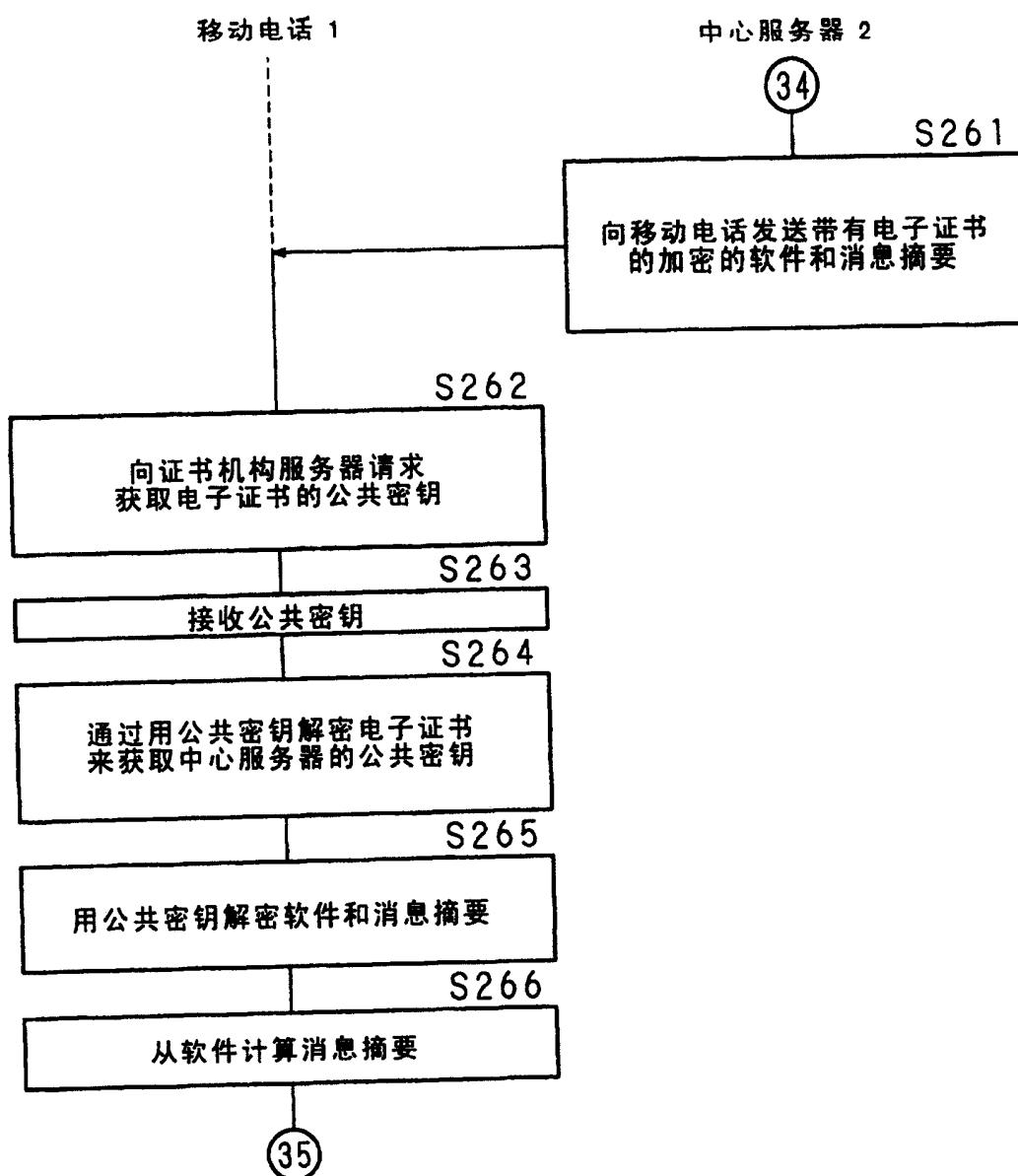


图26

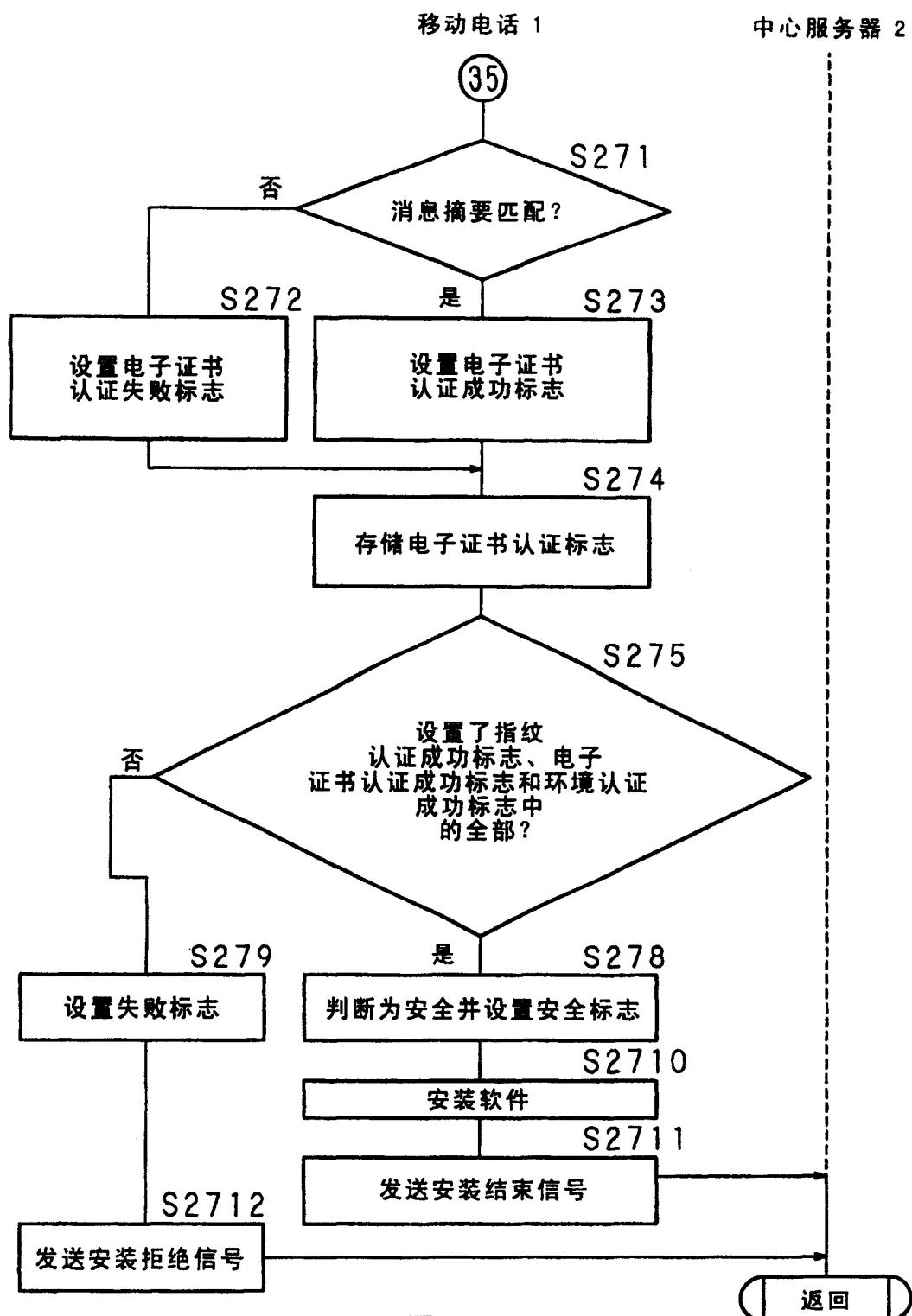


图27

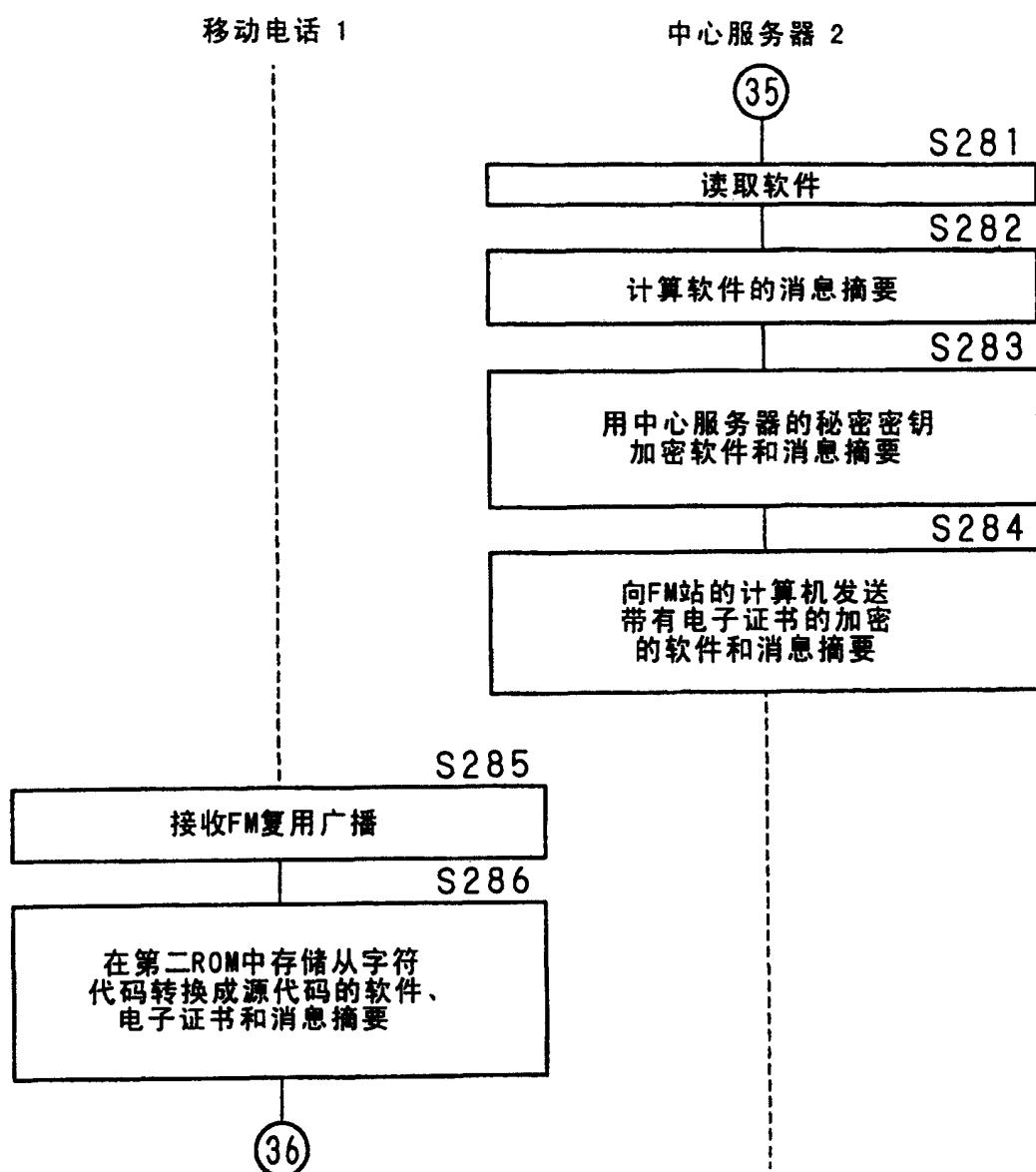


图28

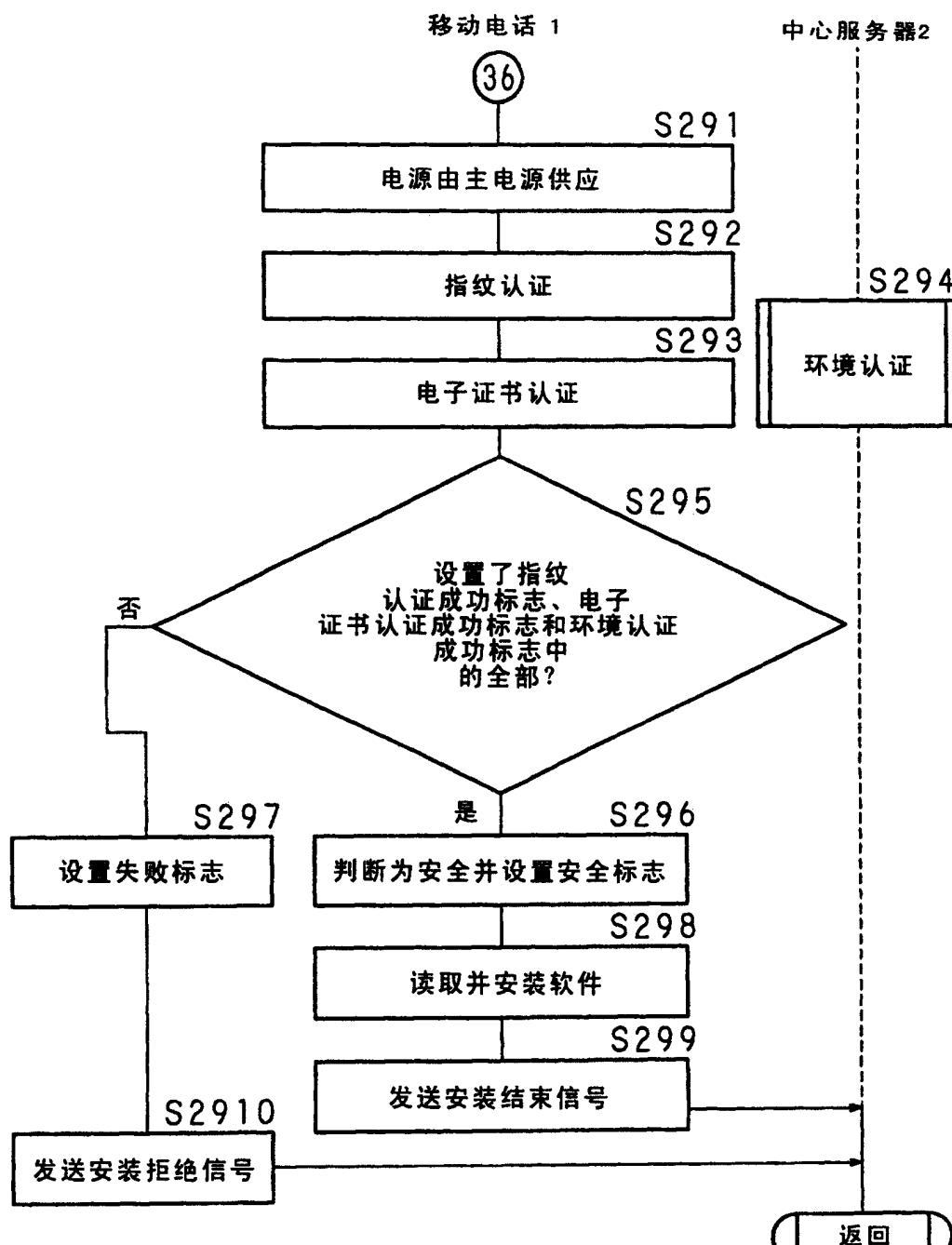


图29

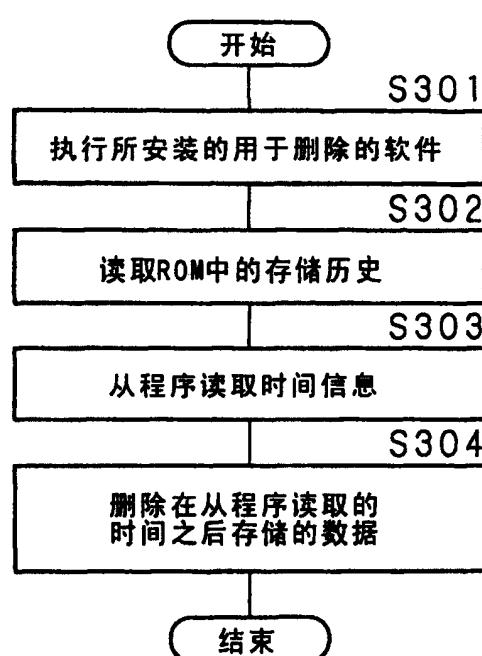


图30

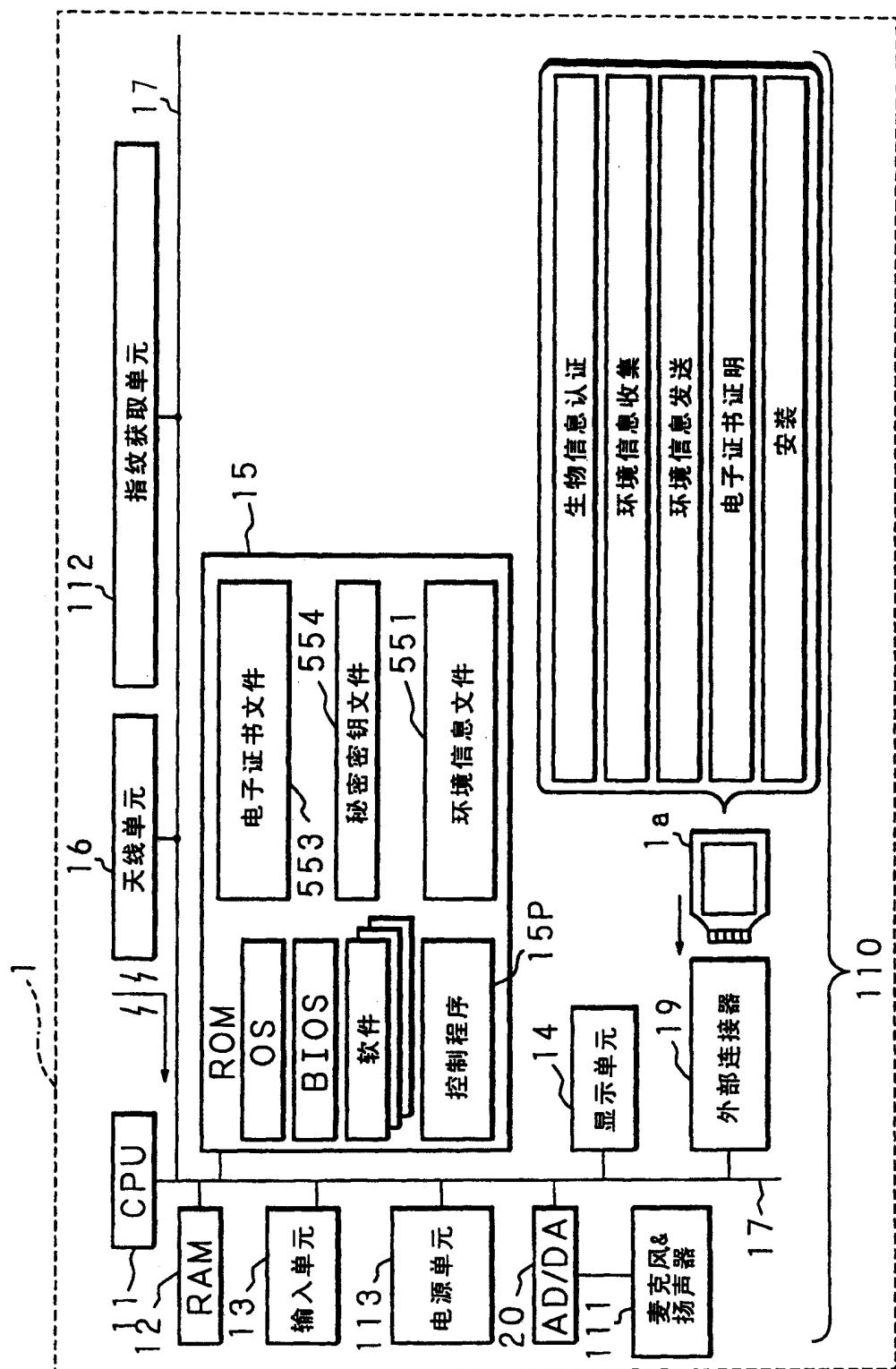


图31

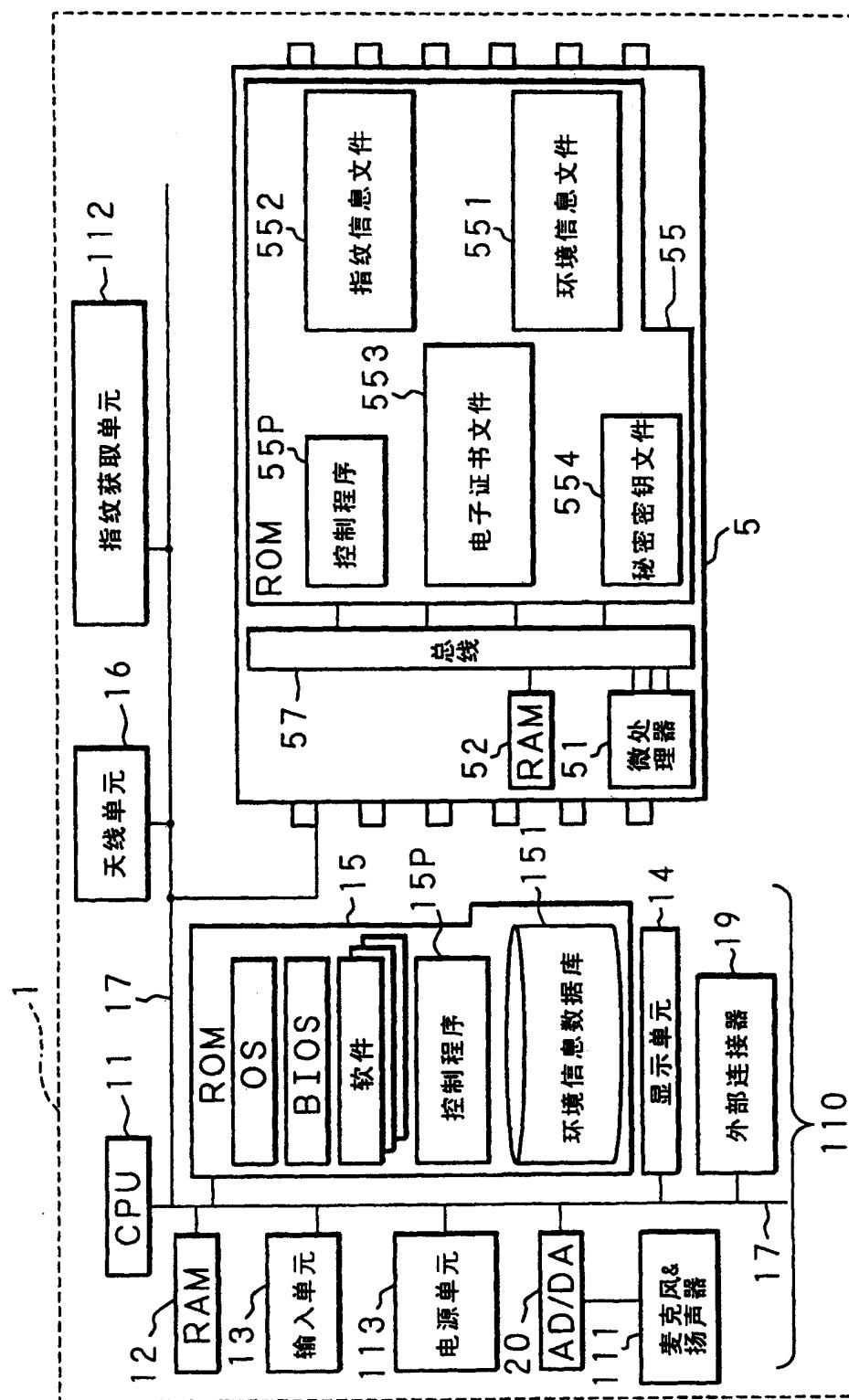


图32

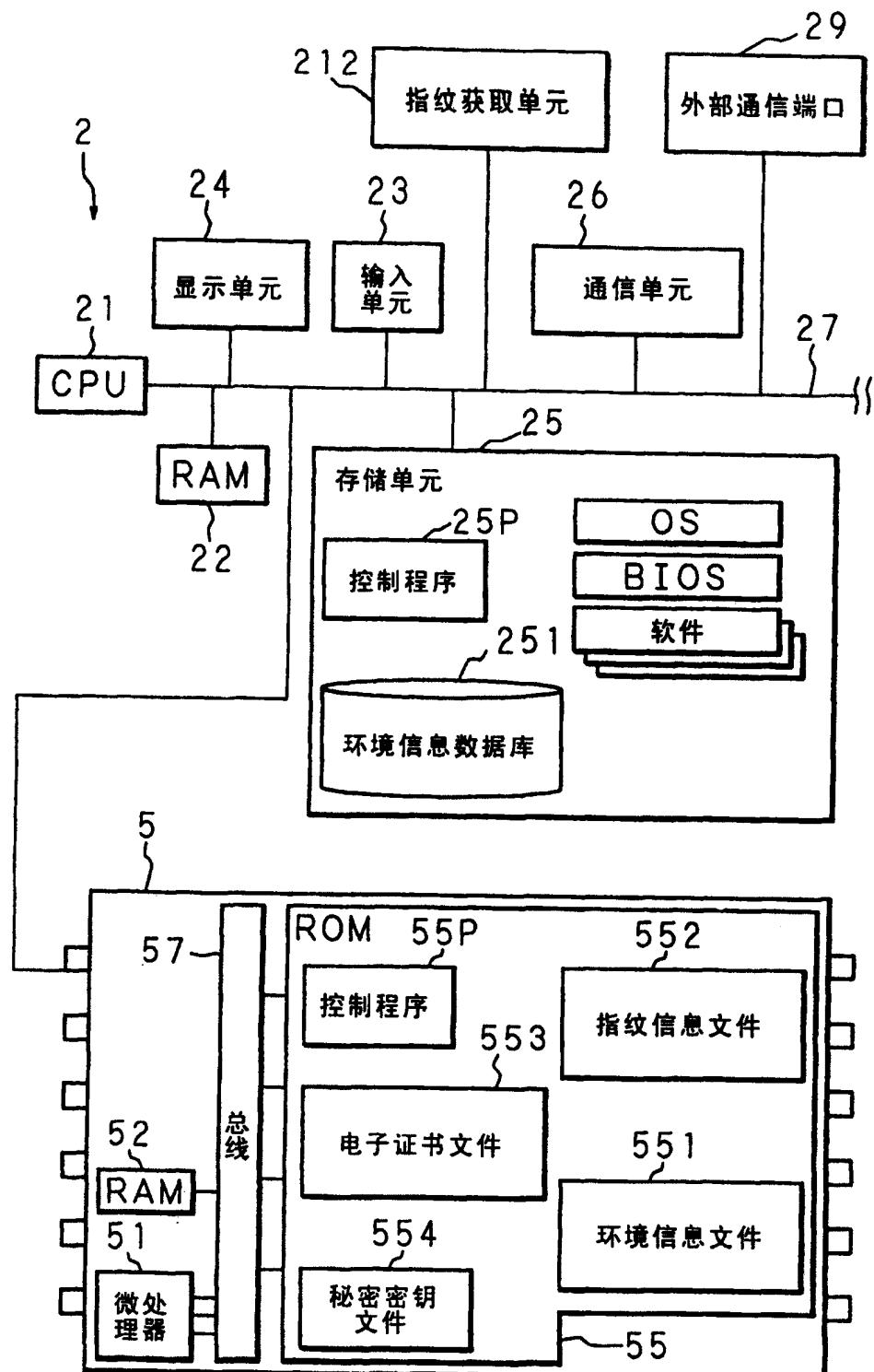


图33

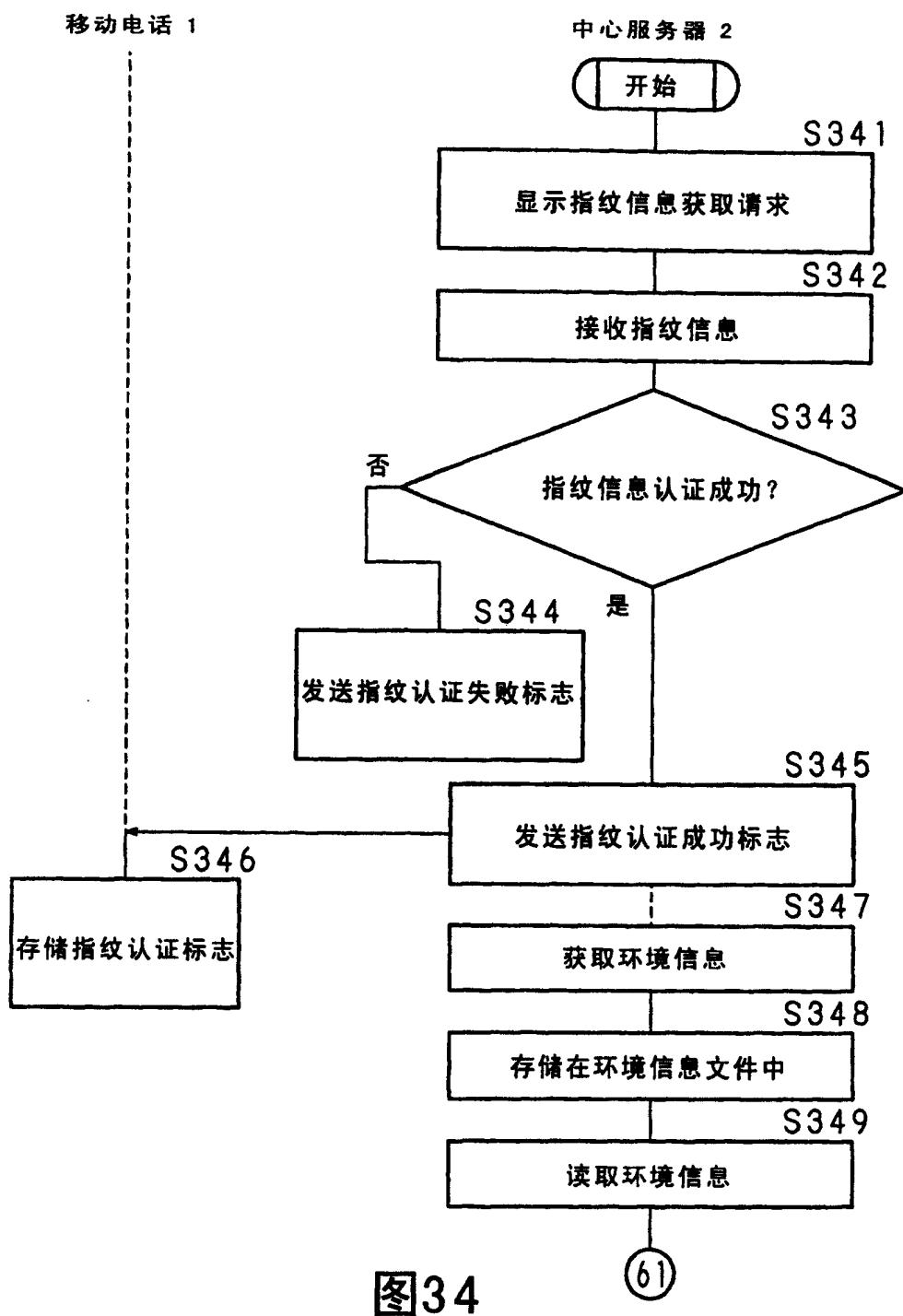


图34

(61)

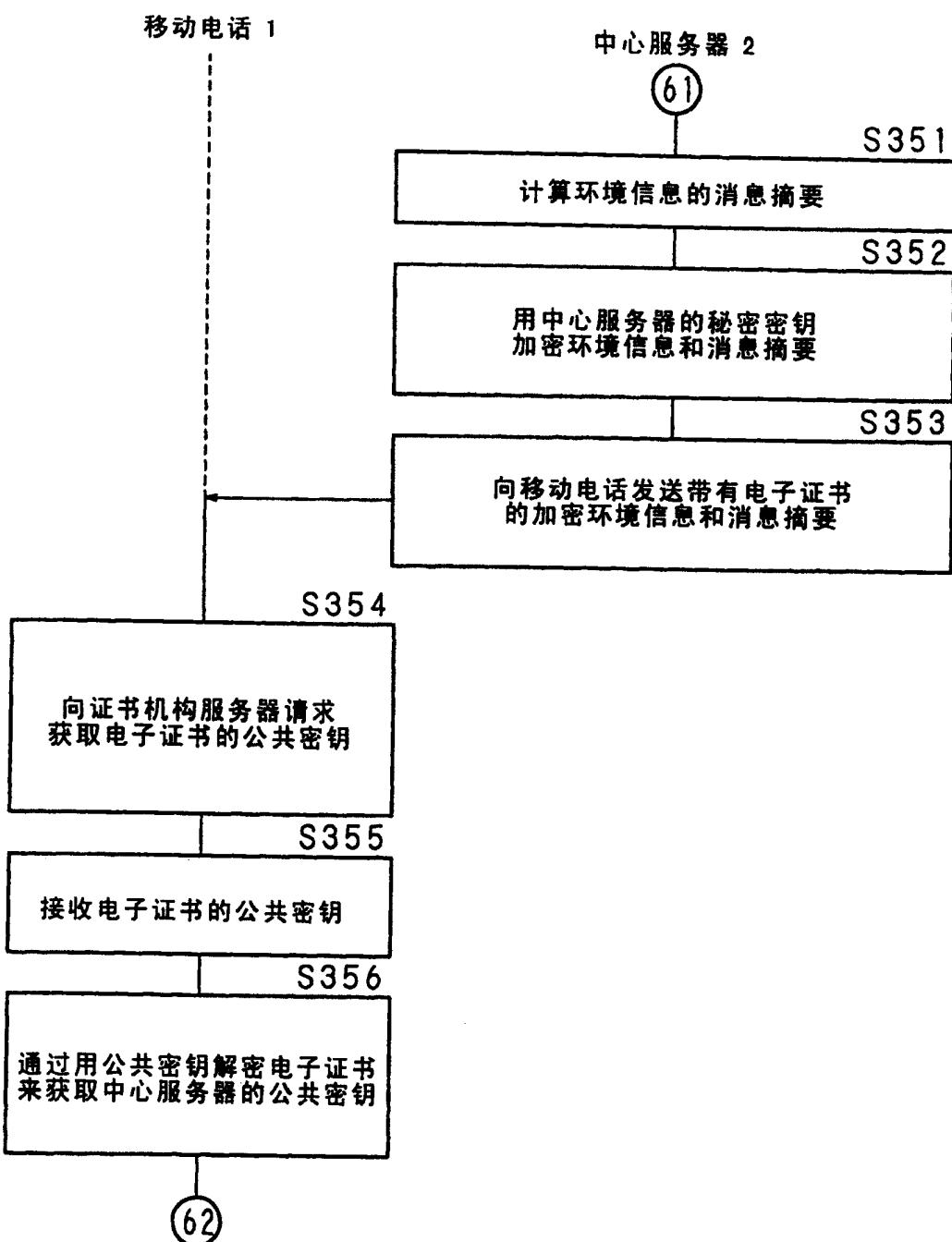


图35

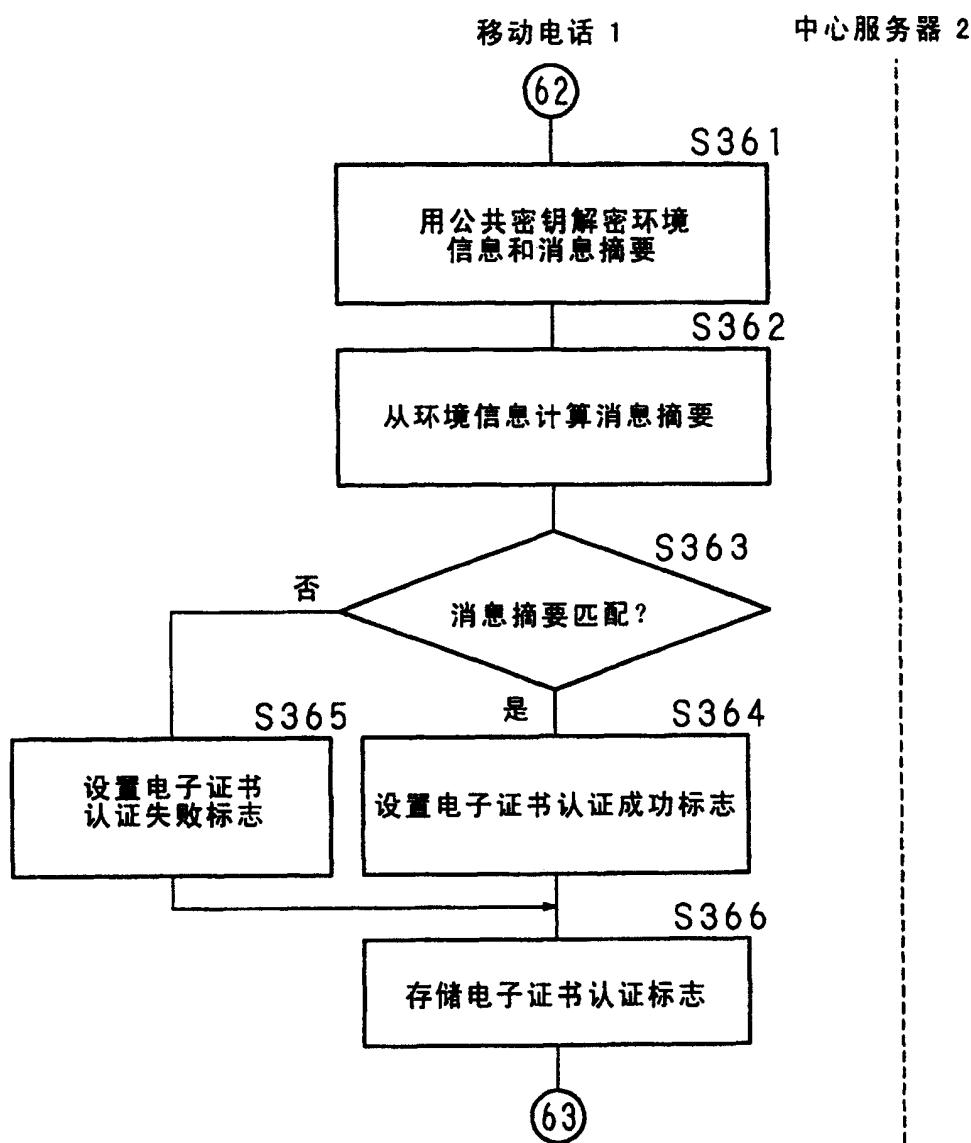


图36

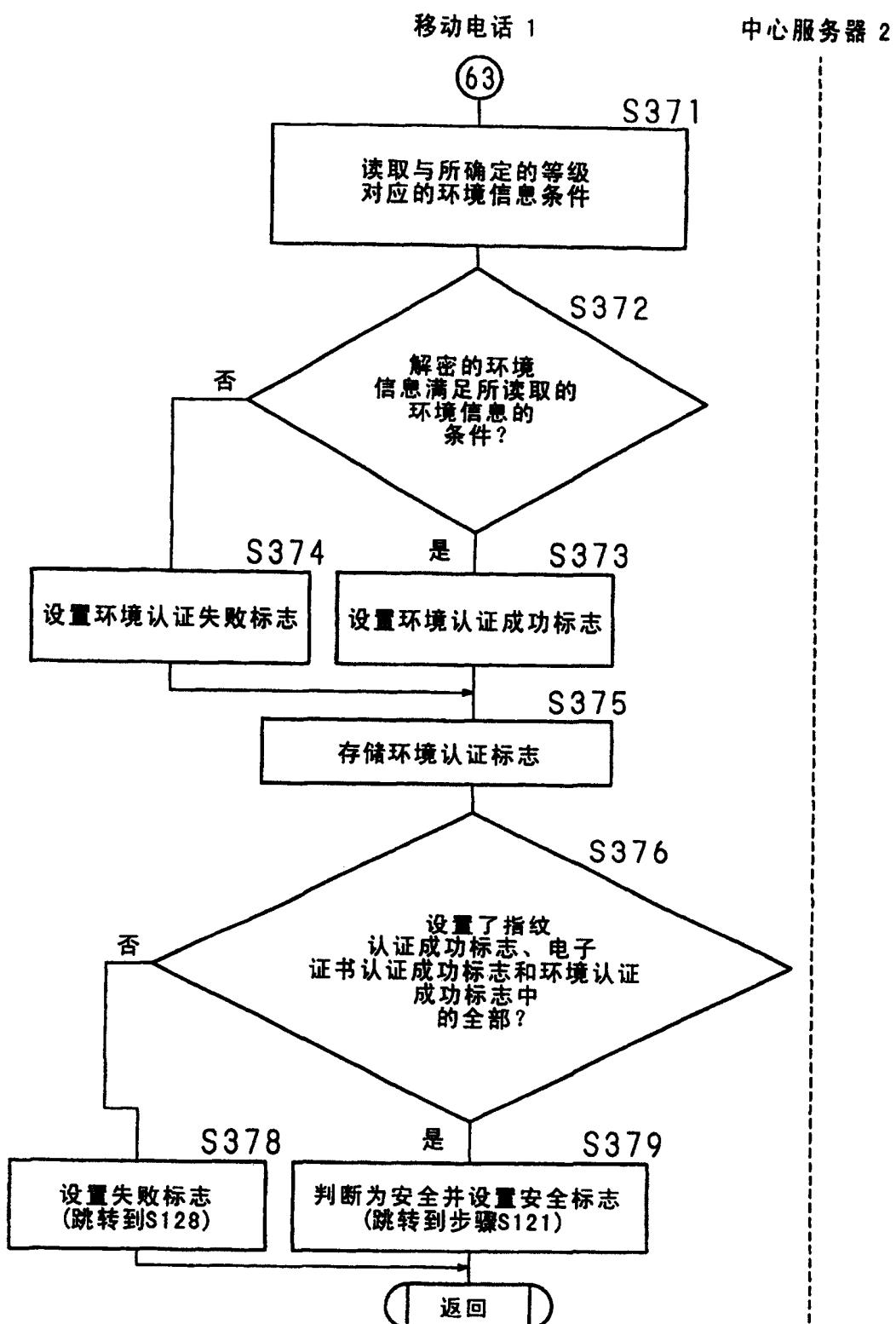


图37