



[12] 发明专利说明书

专利号 ZL 200580004092. X

[45] 授权公告日 2009 年 6 月 3 日

[11] 授权公告号 CN 100495286C

[22] 申请日 2005.2.4

审查员 李俊

[21] 申请号 200580004092. X

[74] 专利代理机构 北京三友知识产权代理有限公司

[30] 优先权

代理人 李辉

[32] 2004.2.5 [33] JP [31] 029928/2004

[86] 国际申请 PCT/JP2005/002104 2005.2.4

[87] 国际公布 WO2005/076105 英 2005.8.18

[85] 进入国家阶段日期 2006.8.4

[73] 专利权人 趋势科技股份有限公司

地址 日本东京

[72] 发明人 近藤贤志 谷田部茂

权利要求书 2 页 说明书 16 页 附图 10 页

[56] 参考文献

CN1299478A 2001.6.13

US6088801A 2000.7.11

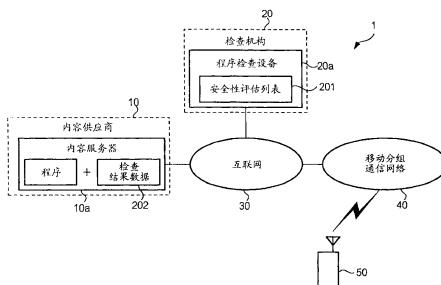
US2003/0056117A1 2003.3.20

JP2002-41170A 2002.2.8

[54] 发明名称
通过对信息设备和传输路径进行程序分析来
确保安全性

[57] 摘要

本发明提供了一种在接收设备或中继设备中，
使用简单的方法并且在短时间内，确定经由网络提
供的程序是否为导致安全性问题的程序的技术。 程
序检查设备 20a 对经由网络提供给移动电话 50 的程
序的内容进行预检查，并生成检查结果数据 202，
该检查结果数据 202 包含该程序中所包含的功能以
及与执行该程序时访问的资源有关的信息。 移动电
话 50 具有安全性管理表 507a，该安全性管理表
507a 针对各个功能登记与是否可以使用该功能有关
的信息，以及针对各个资源登记与是否可以访问该
资源有关的信息。 移动电话 50 对经由网络接收的
程序的检查结果数据 202 和安全性管理表 507a 进行
比较，由此确认该程序在执行时是否会导致安全
性问题。



1、一种接收设备，其包括：

存储装置，用于存储与是否允许使用经由网络提供的程序的功能有关的信息；

接收装置；

第一接收控制装置，用于在经由网络接收程序之前，使用所述接收装置接收表示在该程序中使用的功能的功能信息；

确定装置，用于通过对由所述第一接收控制装置接收的功能信息和由所述存储装置存储的信息进行比较，来确定是否接收该程序；

第二接收控制装置，用于在所述确定装置确定要接收该程序时使用所述接收装置经由网络接收该程序，并且在所述确定装置确定不接收该程序时取消经由网络的该程序的接收；以及

执行装置，用于执行由所述第二接收控制装置接收的程序。

2、根据权利要求 1 所述的接收设备，其中

所述确定装置还对由所述第一接收控制装置接收的功能信息和由所述存储装置存储的信息进行比较，并且如果所述功能信息中不包含不允许使用的功能，则允许所述执行装置执行该程序。

3、根据权利要求 1 所述的接收设备，其中：

所述存储装置存储与是否允许使用所接收程序的函数有关的信息；

并且

所述功能信息是与包含在要接收的程序中的函数有关的信息。

4、根据权利要求 1 所述的接收设备，其中：

所述存储装置存储与是否允许访问所接收程序的资源有关的信息；

并且

所述功能信息是与根据要接收的程序而进行访问的资源有关的信息。

5、根据权利要求 1 所述的接收设备，其中：

所述网络是无线通信网络。

6、一种接收方法，包括步骤：

第一步骤，在经由网络接收程序之前，接收表示在该程序中使用的功能的功能信息；

第二步骤，通过对在所述第一步骤中接收的功能信息和预登记在存储器中的与是否允许使用所接收程序的功能有关的信息进行比较，来确定是否接收与所述功能信息相关联的程序；

第三步骤，如果在所述第二步骤中确定要接收该程序，则经由网络接收该程序；

第四步骤，执行在所述第三步骤中接收的程序；以及

第五步骤，如果在所述第二步骤中确定不接收该程序时，取消经由网络的该程序的接收。

通过对信息设备和传输路径进行程序分析来确保安全性

技术领域

本发明涉及一种确保信息设备的安全性的技术。

背景技术

在诸如互联网的开放网络中，人们可以自由地发布信息或提供程序。因此，存在通过开放网络向例如通信终端提供恶意程序的可能性，如果执行该恶意程序，则将导致安全性漏洞，使得存储在该终端中的信息被读取并从该终端发送出去。本领域中已知用于保护通信终端免受这种程序影响的手段。例如，JP2001-117769 公开了一种程序执行设备，其中该程序执行设备中的存储器中具有表示程序的可靠的源的识别信息（例如，IP 地址或 URL）；如果该存储器中登记有表示经由网络接收的程序的源的识别信息，则允许执行该程序。

然而，在 JP2001-117769 中公开的技术中，必须登记所有可靠的程序发送源。因此，每一次添加或删除可靠程序发送源时，都必须对存储在存储器中的识别信息进行更新。此外，由于在诸如互联网的大型网络中，存在着大量的可靠程序发送源，所以实质上很难将可靠程序发送源的所有识别信息都登记在终端的存储器中。此外，即使可以将所有这种识别信息都登记在终端的存储器中，但是为了这样做，必须增大所使用的存储器的大小，特别是诸如移动电话的小型通信终端中的存储器的大小，这导致这种终端的制造成本的增加。

另一方面，如果通过例如在移动终端处对经由网络在该移动终端处接收的程序的内容进行分析来确定该程序是否为安全性威胁，以提高安全性，则该移动终端必须具有高级计算能力。此外，在移动终端处确定安全性威胁给移动终端的处理单元带来了很重的负担，并且要花费大量的时间来完成。类似地，如果在网络上的诸如服务器的中继设备处，对

经由网络接收的程序的内容进行分析，由此确定在通信终端中执行该程序是否会构成安全性威胁，则必须向该中继设备提供高级计算能力。如果该中继设备不具备足够的计算能力，则可能出现通信的延迟。

鉴于上述问题而提出本发明，并且本发明提供了一种在接收设备或中继设备处，通过使用可快速执行的简单方法来确定经由网络提供的程序是否为安全性威胁的技术。

发明内容

为了解决这些问题，本发明提供了：登记装置，用于登记与是否允许使用所接收的程序的功能有关的信息；接收装置，用于接收程序以及表示该程序中所使用的功能的功能信息；确定装置，用于通过对由所述接收装置接收的功能信息和由所述登记装置登记的信息进行比较，来确定由所述接收装置接收的程序是否包括不允许使用的功能；以及输出装置，用于输出由所述确定装置确定的结果。

本发明还提供了一种用于使计算机用作接收设备的程序，并提供了一种用于记录该程序的计算机可读存储介质。该程序可以预安装在计算机的存储器中，或者可以通过经由网络进行的通信安装在计算机中，或者可以通过存储介质进行安装。

根据本发明，接收设备通过对所接收的程序的功能信息和由所述登记装置登记的信息进行比较，来确定该程序中是否存在被禁止的功能，并输出该确定结果。

本发明还提供了一种接收设备，该接收设备包括：登记装置，用于登记与是否允许使用所接收程序的功能相关的信息；接收装置，用于接收程序以及表示在该程序中使用的功能的功能信息；确定装置，用于通过对由所述接收装置接收的功能信息和由所述登记装置登记的信息进行比较，来确定是否执行由所述接收装置接收的程序；以及执行装置，用于在所述确定装置确定要执行一程序时执行该程序。本发明还提供了一种用于使计算机用作接收设备的程序，并提供了用于记录该程序的计算机可读存储介质。

根据本发明，接收设备通过对所接收程序的功能信息和由所述登记装置登记的信息进行比较，来确定是否应该执行该程序。

本发明还提供了一种接收设备，该接收设备包括：登记装置，用于登记与是否允许使用所接收程序的功能有关的信息；第一接收装置，用于在接收程序之前，接收表示在该程序中使用的功能的功能信息；确定装置，用于通过对由所述第一接收装置接收的功能信息和由所述登记装置登记的信息进行比较，来确定是否接收程序；第二接收装置，用于在所述确定装置确定要接收一程序时接收该程序；以及执行装置，用于执行由所述第二接收装置接收的程序。本发明还提供了一种用于使计算机用作接收设备的程序，以及用于记录该程序的计算机可读存储介质。

根据本发明，接收设备通过对程序的功能信息和由所述登记装置登记的信息进行比较，来确定是否应该接收该程序。

本发明提供了一种中继设备，该中继设备包括：登记装置，用于登记与是否允许使用经由网络提供的程序的功能有关的信息；接收装置，用于接收程序、表示在该程序中使用的功能的功能信息、以及表示该程序的目的地的目的地信息；确定装置，用于通过对由所述接收装置接收的功能信息和由所述登记装置登记的信息进行比较，来确定是否对由所述接收装置接收的程序进行中继；以及发送装置，用于在所述确定装置确定要对程序进行中继时，将该程序发送至由所述接收装置所接收的目的地信息指定的目的地。

本发明还提供了一种用于使计算机用作中继设备的程序，并提供了用于记录该程序的计算机可读存储介质。该程序可以预安装在计算机的存储器中，或者可以通过经由网络进行的通信安装在计算机中，或者可以通过存储介质进行安装。

根据本发明，中继设备通过对所接收程序的功能信息和由所述登记装置登记的信息进行比较，来确定是否对该程序进行中继。

本发明还提供了一种中继设备，该中继设备包括：登记装置，用于登记与是否允许使用经由网络提供的程序的功能有关的信息；接收装置，用于接收程序、表示在该程序中使用的功能的功能信息、以及表示该程

序的目的地的目的地信息；确定装置，用于通过对由所述接收装置接收的功能信息和由所述登记装置登记的信息进行比较，来确定在由所述接收装置接收的程序中是否使用了不允许使用的功能；以及发送装置，用于在所述确定装置确定要对程序进行中继时，将所述确定装置的确定结果和该程序发送至由所述接收装置所接收的目的地信息指定的目的地。本发明还提供了一种用于使计算机用作中继设备的程序，并提供了一种用于记录该程序的计算机可读存储介质。

根据本发明，中继设备通过对所接收程序的功能信息和由登记装置登记的信息进行比较，来确定该程序中是否存在被禁止的功能，并连同该程序一起发送确定结果。

根据本发明，可以通过采用简单的方法并且在短时间内，在接收设备或中继设备处容易地确定经由网络提供的程序是否为带来安全性威胁的程序。

附图说明

图 1 是例示根据第一实施例的通信系统的结构的框图。

图 2 是例示根据第一实施例的检查结果数据 202 的数据结构的图。

图 3 是例示根据第一实施例的移动电话 50 的硬件结构的框图。

图 4 是例示根据第一实施例的安全性管理表 507a 的数据结构的图。

图 5 是例示构成根据第一实施例的通信系统 1 的各个组件的操作的时序图，这些操作在程序及其检查结果数据 202 被下载到移动电话 50 之前执行。

图 6 是例示根据第一实施例的在设定安全性级别时在移动电话 50 上显示的画面的图。

图 7 是例示用于确定是否执行经由网络接收的程序的操作的流程图，这些操作在根据第一实施例的移动电话 50 中执行。

图 8 是例示根据第一实施例的在不允许执行程序时在移动电话 50 上显示的画面的图。

图 9 是例示根据第二实施例的中继设备 60 的硬件结构的框图。

图 10 是例示确定是否执行经由网络接收的程序的操作的流程图，这些操作在根据第二实施例的中继设备 60 中执行。

图 11 是例示根据变型例（1）的通信系统 2 的结构的框图。

图 12 是例示根据变型例（2）的在移动电话中执行的操作的流程图。

图 13 是例示根据变型例（2）的显示在移动电话 50 上的画面的图。

具体实施方式

下面将参照附图来说明本发明的实施例。

[A.第一实施例]

图 1 是例示根据第一实施例的通信系统的结构的框图。在图 1 中，内容供应商 10 是向移动电话 50 提供内容的服务供应商。内容服务器 10a 经由互联网 30 和移动分组通信网络 40 与移动电话 50 进行分组通信。内容服务器 10a 存储有用于移动电话 50 的程序以及作为在检查机构（institution）20 中对该程序的检查的结果而获得的检查结果数据 202。存储在内容服务器 10a 中的程序可以是包含有在执行程序时使用的图像或音频数据的软件。

检查机构 20 是下述的机构，该机构在从内容供应商 10 接收到检查请求时，对提供给移动电话 50 的程序进行检查，并且程序检查设备 20a 存储有安全性评估列表 201。在安全性评估列表 201 中列出了诸如功能调用和系统调用的函数，这些函数在经由网络提供程序并且执行该程序时可能危及移动电话 50 的安全。安全性评估列表 201 还列出了可由移动电话 50 访问的资源，当根据经由网络提供的程序来访问这些资源时，可能危及移动电话 50 的安全。

程序检查设备 20a 参照安全性评估列表 201 对要检查的程序进行分析，并从该程序中提取安全性评估列表 201 中所列出的函数。程序检查设备 20a 还在该程序执行时所访问的资源当中，识别出在安全性评估列表 201 中列出的资源。然后，程序检查设备 20a 产生包含所提取函数的名称以及与所识别的资源有关的信息（例如，表示这些资源存储在何处的 URL 或路径，或者分配给这些资源的标识符）的检查结果数据 202。

将检查结果数据 202 返回给内容供应商 10，并连同该程序一起存储在内容服务器 10a 中。

程序检查设备 20a 可以将包含在要检查的程序中的所有函数都记录为检查结果数据 202，或者可以记录当执行要检查的程序时访问的所有资源。

移动电话 50 是由移动分组通信网络 40 提供服务的通信终端（接收设备），并且可以从内容服务器 10a 下载程序并执行该程序。

图 2 是例示检查结果数据 202 的数据结构的图。如图 2 所示，检查结果数据 202 包含所检查程序的名称、用于计算该程序的散列值（hash value）的散列算法的名称、以及所计算的散列值。检查结果数据 202 还包括包含在该程序中的函数的名称的列表以及与执行该程序时访问的资源有关的信息的列表，这些列表是作为使用安全性评估列表 201 对该程序进行分析的结果而获得的。包含在检查结果数据 202 中的散列值用于验证在由程序检查设备 20a 进行检查之后，该程序未被改动或篡改。

图 3 是例示移动电话 50 的硬件结构的框图。CPU 501 执行存储在 ROM 502 和非易失性存储器 507 中的各种程序，由此对移动电话 50 的组件进行控制。ROM 502 存储有用于控制移动电话 50 的程序。RAM 503 用作 CPU 501 的工作区。无线通信单元 504 在 CPU 501 的控制下，对与移动分组通信网络 40 的基站（未示出）的无线通信进行控制。操作输入单元 505 包括多个键，并且响应于这些键的操作而向 CPU 501 输出操作信号。液晶显示单元 506 包括液晶显示板和用于对该液晶显示板的显示进行控制的驱动电路。

非易失性存储器 507 存储有用于移动电话 50 的软件，例如操作系统和 WWW（万维网）浏览器。非易失性存储器 507 还存储有从内容服务器 10a 下载的程序，并存储有其检查结果数据 202。非易失性存储器还存储有安全管理表 507a。

如图 4 所示，安全管理表 507a 对于包含在用于移动电话 50 的程序中的函数，登记有在执行经由网络接收的程序时允许使用的函数的名称，以及在执行经由网络接收的程序时不允许使用的函数的名称。安全

性管理表 507a 还对于移动电话 50 可访问的资源，登记有与在执行经由网络接收的程序时允许访问的资源有关的信息，以及与在执行经由网络接收的程序时不允许访问的资源有关的信息。对于需要询问用户是否执行程序的函数和资源，在安全性管理表 507a 的项目“允许”栏中登记项目“用户确认”这一条件。

非易失性存储器 507 针对移动电话 50 中可用的各个安全性级别存储多个安全性管理表 507a，例如针对“级别 1”的安全性管理表 507a 或者针对“级别 2”的安全性管理表 507a。在移动电话 50 中，在确定是否执行经由网络接收的程序时，使用该多个安全性管理表 507a 当中的与移动电话 50 中当前设定的安全性级别相对应的安全性管理表 507a。该安全性级别由移动电话 50 的用户来设定。

登记在安全性管理表 507a 中的函数以及与是否允许使用这些函数有关的信息可以由移动电话 50 的用户来改变。对于登记在安全性管理表 507a 中的资源以及与是否允许访问这些资源有关的信息也是如此。

下面将说明第一实施例的操作。

图 5 是例示构成通信系统 1 的各个组件的操作的时序图，这些操作在程序以及对应的检查结果数据 202 被下载到移动电话 50 之前执行。如图 5 所示，将由内容供应商 10 编写的用于移动电话 50 的程序连同检查请求一起从内容服务器 10a 发送至程序检查设备 20a（步骤 S101）。

程序检查设备 20a 在接收到该程序和该检查请求时，对所接收的程序进行分析（步骤 S102）。程序检查设备 20a 从安全性评估列表 201 中所列出的程序函数中进行提取，并识别出执行该程序时访问的并且在安全性评估列表 201 中列出的资源。程序检查设备 20a 还使用散列算法来计算该程序的散列值。程序检查设备 20a 随后生成包含所提取函数的名称、与所识别资源有关的信息、所计算的散列值、所使用的算法的名称、以及该程序的文件名的检查结果数据 202（步骤 S103）。

然后，程序检查设备 20a 为所生成的检查结果数据 202 附加电子签名（步骤 S104）。该电子签名用于在移动电话 50 中验证该程序未被改动或篡改。此后，程序检查设备 20a 将带有电子签名的检查结果数据 202

返回给内容服务器 10a (步骤 S105)。内容服务器 10a 在接收到检查结果数据 202 时, 将检查结果数据 202 和被检查的程序存储在存储器中 (步骤 S106), 并使得该程序和检查结果数据 202 可由移动电话 50 下载。

在移动电话 50 中设定安全性级别 (步骤 S107)。在设定安全性级别时, 在液晶显示单元 506 上显示图 6 所示的画面, 用户可以使用操作输入单元 505 从“级别 0 (无)”到“级别 5”选择移动电话 50 的安全性级别。将由用户设定的安全性级别存储在非易失性存储器 507 中。

如果移动电话 50 从内容服务器 10a 下载程序, 则在移动电话 50 中启动 WWW 浏览器 (步骤 S108), 并在移动电话 50 和内容服务器 10a 之间开始分组通信。当用户使用操作输入单元 505 选择了要下载的程序时, 从移动电话 50 向内容服务器 10a 发送请求下载该程序的信号 (步骤 S109)。内容服务器 10a 从存储器中读取所请求的程序以及该程序的检查结果数据 202, 并将它们发送给移动电话 50 (步骤 S110 和 S111)。移动电话 50 在接收到该程序和检查结果数据 202 时, 将其存储在非易失性存储器 507 中 (步骤 S112)。

图 7 是示出确定是否执行经由网络接收的程序的操作的流程图, 这些操作在移动电话 50 中执行。如果在移动电话 50 中指示执行经由网络接收的程序, 则 CPU 501 执行这些操作。如图 7 所示, CPU 501 从非易失性存储器 507 中读取被指示执行的程序的检查结果数据 202 (步骤 S201)。

CPU 501 验证检查结果数据 202 的电子签名 (步骤 S202), 由此确认该检查结果数据 202 是由检查机构 20 产生的, 并且该检查结果数据 202 是未被篡改的可信的检查结果数据。如果作为电子签名的验证结果, 发现检查结果数据 202 不可信 (步骤 S203: 否), 则 CPU 501 取消该程序的执行 (步骤 S210), 并使液晶显示单元 506 显示一消息, 该消息表示由于在检查结果数据 202 中发现了篡改, 所以该程序的执行已被取消。

另一方面, 如果检查结果数据 202 被验证为可信 (步骤 S203: 是), 则 CPU 501 使用检查结果数据 202 中描述的散列算法来计算该程序的散列值。CPU 501 对所计算的散列值和在检查结果数据 202 中描述的散列

值进行比较（步骤 S204）。作为比较的结果，如果这些散列值不匹配（步骤 S205：否），则 CPU 501 取消该程序的执行（步骤 S210），并使液晶显示单元 506 显示一消息，该消息表示由于在该程序中发现了篡改，所以该程序的执行已被取消。

另一方面，如果这些散列值匹配（步骤 S205：是），则 CPU 501 识别移动电话 50 中当前设定的安全性级别的值，并从非易失性存储器 507 中读取与所识别的安全性级别的值相对应的安全性管理表 507a（步骤 S206）。CPU 501 对所读取的安全性管理表 507a 和在步骤 S201 中读取的检查结果数据 202 进行比较（步骤 S207），由此确定是否执行该程序（步骤 S208）。

为了详细说明步骤 S207 和 S208 的操作，对于检查结果数据 202 中描述的各个函数，即对于从要执行的程序中提取的各个函数，CPU 501 确定该函数是否为安全性管理表 507a 中允许使用的函数。类似地，对于检查结果数据 202 中描述的各个资源，CPU 501 确定该资源是否为安全性管理表 507a 中允许访问的资源。

结果，如果检查结果数据 202 中包含任何不允许使用的函数，或者如果检查结果数据 202 中包含任何不允许访问的资源，则 CPU 501 确定该程序违反了用户设定的安全性策略（安全性管理表 507a），因而不允许执行该程序（步骤 S208：否）。因此，CPU 501 取消该程序的执行（步骤 S210），并使液晶显示单元 506 显示如图 8 所示的消息。

例如，假设检查结果数据 202 如图 2 所示，而安全性管理表 507a 如图 4 所示，则由于检查结果数据 202 包含了根据安全性管理表 507a 不允许使用的函数“Function 1 ()”、以及根据安全性管理表 507a 不允许访问的资源“Local/UserData/AddressBook”，所以不允许在移动电话 50 中执行与检查结果数据 202 相对应的程序。

另一方面，如果检查结果数据 202 中所描述的所有函数都是根据安全性管理表 507a 允许使用的函数，并且检查结果数据 202 中所描述的所有资源都是根据安全性管理表 507a 允许访问的资源，则 CPU 501 确定该程序符合用户所设定的安全性策略，因而允许执行该程序（步骤 S208：

是)。因此，CPU 501 从非易失性存储器 507 中读取允许执行的程序，启动该程序(步骤 S209)，并根据该程序的进行操作。

如果检查结果数据 202 包含需要用户确认的资源，如图 4 的安全管理表 507a 中的资源“<http://www.xxx.co.jp>”，则 CPU 501 生成询问用户是否执行程序的消息，使液晶显示单元 506 显示该消息，并根据来自操作输入单元 505 的指令来确定该程序的执行。

如上所述，在本实施例中，程序检查设备 20a 对经由网络提供给移动电话 50 的程序的内容进行预检查，并生成检查结果数据 202，该检查结果数据 202 包含该程序中所包含的函数以及与执行该程序时访问的资源有关的信息。移动电话 50 对检查结果数据 202 和针对各个函数登记与是否可以使用该函数有关的信息和针对各个资源登记是否可以访问该资源有关的信息的安全性管理表 507a 进行比较，由此确定是否执行经由网络接收的程序。因此，移动电话 50 仅通过比较检查结果数据 202 和安全性管理表 507a，而无需分析所接收的程序，就可以确定该程序是否符合移动电话 50 中设定的安全性策略(安全性管理表 507a)。因此，可以通过使用简单的方法并且在短时间内，在移动电话 50 中完成该确定处理。

可以通过改变安全性级别而容易地改变用于确定是否执行所接收程序的安全性管理表 507a。因此，即使程序违反了安全性策略并因此被确定为不允许执行，但是如果用户确定该程序有效，则可以通过暂时降低安全性级别而在移动电话中执行该程序。如上所述，在本实施例中，可以根据用户的意愿执行与所接收程序相关的移动电话 50 的安全性级别的灵活设定。

[B.第二实施例]

下面将对本发明的第二实施例进行说明。

在本实施例中，与第一实施例共有的要素用相同的标号来表示，并省略与第一实施例共有的说明。

图 9 是例示中继设备 60 的硬件结构的框图，该中继设备 60 对内容服务器 10a 和移动电话 50 之间的分组通信进行中继。中继设备 60 可以设置在互联网 30 或者移动分组通信网络 40 上。在图 9 中，通信接口 604

在 CPU 601 的控制下，对与内容服务器 10a 或移动电话 50 的分组通信进行控制。操作输入单元 605 具有鼠标和键盘，并根据通过鼠标和键盘执行的操作向 CPU 601 输出操作信号。显示单元 606 是 LCD 或 CRT 显示器。

HD（硬盘）607 存储有第一实施例中所述的安全性管理表 507a。本实施例的中继设备 60 使用安全性管理表 507a 来确定是否对从内容服务器 10a 发送至移动电话 50 的程序进行中继。中继设备 60 从内容服务器 10a 连同该程序一起接收该程序的检查结果数据 202 以及表示该程序的目的地的目的地信息。检查结果数据 202 是由第一实施例中所述的程序检查设备 20a 生成的。地址信息是分配给移动电话 50 的通信地址，例如 IP 地址。

在本实施例中，中继设备 60 中的安全性级别是由移动分组通信网络的运营商或者中继设备 60 的管理者设定的。如第一实施例中所述，HD 607 针对各个安全性级别存储不同的安全性管理表 507a，并且根据中继设备 60 中设定的安全性级别来确定用于确定是否对程序进行中继的安全性管理表 507a。

图 10 是例示为确定是否对程序进行中继而执行的操作的流程图，这些操作是在中继设备 60 中执行的。如果中继设备 60 接收到从内容服务器 10a 发送到移动电话 50 的程序及其检查结果数据 202，则 CPU 601 执行这些操作。如图 10 所示，CPU 601 验证检查结果数据 202 的电子签名（步骤 S301）。如果在验证电子签名时，确认检查结果数据 202 不可信（步骤 S302：否），则 CPU 601 取消将该程序传送给移动电话 50（步骤 S309），并向移动电话 50 发送一消息，该消息表示由于在检查结果数据 202 中发现了篡改，所以已经取消了该程序的下载。

另一方面，如果检查结果数据被验证为可信（步骤 S302：是），则 CPU 601 使用在检查结果数据 202 中描述的散列算法来计算该程序的散列值，并对所计算的散列值和检查结果数据 202 中描述的散列值进行比较（步骤 S303）。如果作为该比较的结果，确定为这些散列值不匹配（步骤 S304：否），则 CPU 601 取消将该程序传送给移动电话 50（步骤 S309），

并向移动电话 50 发送一消息，该消息表示由于在程序中发现了篡改，所以已经取消了该程序的下载。

另一方面，如果这些散列值匹配（步骤 S304：是），则 CPU 601 识别此时中继设备 60 中设定的安全性级别，并从 HD 607 中读取与所识别的安全性值相对应的安全性管理表 507a（步骤 S305）。CPU 601 对所读取的安全性管理表 507a 和所接收的检查结果数据 202 进行比较（步骤 S306），由此确定是否将该程序中继到移动电话 50（步骤 S307）。

为了详细说明步骤 S306 和 S307 的操作，对于检查结果数据 202 中描述的各个函数，即对于从所接收程序中提取的各个函数，CPU 601 确定该函数是否为根据安全性管理表 507a 允许使用的函数。类似地，对于检查结果数据 202 中描述的各个资源，CPU 601 确定该资源是否为根据安全性管理表 507a 允许访问的资源。

结果，如果检查结果数据 202 中存在任何不允许使用的函数，或者如果检查结果数据 202 中存在任何不允许访问的资源，则 CPU 601 确定该程序违反了例如由移动分组通信网络 40 的运营商设定的安全性策略（安全性管理表 507a），因而不允许将该程序中继至移动电话 50（步骤 S307：否）。因此，CPU 601 取消该程序的传送（步骤 S309），并向移动电话 50 发送一消息，该消息表示该程序的下载已被取消。

另一方面，如果检查结果数据 202 中所描述的所有函数都是根据安全性管理表 507a 允许使用的函数，并且检查结果数据 202 中所描述的所有资源都是根据安全性管理表 507a 允许访问的资源，则 CPU 601 确定所接收程序符合由移动分组通信网络 40 的运营商设定的安全性策略，因而允许将该程序中继至移动电话 50（步骤 S307：是）。因此，CPU 601 将该程序传送至由地址信息指定的移动电话 50（步骤 S308）。

如上所述，在本实施例中，程序检查设备 20a 对经由网络提供给移动电话 50 的程序的内容进行预检查，并生成检查结果数据 202，该检查结果数据 202 包含该程序中所包含的函数以及与执行该程序时访问的资源有关的信息。中继设备 60 对检查结果数据 202 和针对各个函数登记与是否可以使用该函数有关的信息和针对各个资源登记与是否可以访问该

资源有关的信息的安全性管理表 507a 进行比较，由此确定是否将该程序中继至移动电话 50。因此，中继设备 60 仅通过比较检查结果数据 202 和安全性管理表 507a，而无需分析要中继的程序，就可以确定该程序是否符合中继设备 60 中设定的安全性策略（安全性管理表 507a）。因此，可以通过使用简单的方法并且在短时间内在中继设备 60 中完成该确定处理，从而避免了通信中的任何延迟。另外，由于取消了违反安全性策略的程序的传送，所以能够防止将这种程序提供给移动电话 50。

可以由移动分组通信网络 40 的运营商或者中继设备 60 的管理者来改变登记在安全性管理表 507a 中的函数和与可以使用哪些函数相关的信息。对于登记在安全性管理表 507a 中的资源和与可以访问哪些资源相关的信息也是如此。

[C.变型例]

(1) 在第一实施例中，连同程序一起将检查结果数据 202 发送给移动电话 50。然而，如图 11 所示，可以提供用于登记在检查机构 20 中检查的各个程序的检查结果数据 202 的检查结果登记服务器 70。在这种情况下，移动电话 50 在从内容服务器 10b 下载程序之后，从检查结果登记服务器 70 获得该程序的检查结果数据 202。对于第二实施例也是如此，即，检查结果登记服务器 70 登记各个程序的检查结果数据 202，因此如果中继设备 60 从内容服务器 10b 接收到要传送至移动电话 50 的程序，则中继设备 60 从检查结果登记服务器 70 获得该程序的检查结果数据 202。检查结果登记服务器 70 可以设置在移动分组通信网络 40 上或者检查机构 20 中。

(2) 在第一实施例中，当图 7 的步骤 S208 中的确定结果为否定时，操作可以如图 12 所示进行改变。

即，如果图 7 的步骤 S208 中的确定结果为否定，则 CPU 501 使液晶显示单元 506 显示（如图 13 所示）要执行的程序违反了安全性策略的消息、以及确认是否在可用功能受限的情况下执行该程序的消息（步骤 S401）。响应于这些消息，用户使用操作输入单元 505 指示移动电话 50 在可用功能受限的情况下执行该程序，或者取消该程序的执行。可以作

为语音消息从移动电话 50 输出这些消息。

如果通过操作输入单元 505 指示了取消该程序的执行（步骤 S402：否），则 CPU 501 取消该程序的执行（步骤 S403）。另一方面，如果通过操作输入单元 505 指示了执行该程序（步骤 S402：是），则 CPU 501 从非易失性存储器 507 中读取该程序并启动它（步骤 S404）。此后，CPU 501 确定所运行的程序是否已终止（步骤 S405），并且在所运行的程序终止之前，根据安全性管理表 507a 来限制该程序中可用的功能（步骤 S406）。用于限制可用功能的安全性管理表 507a 与此时移动电话 50 中设定的安全性级别相对应。

现详细说明步骤 S406 中的操作，如果在顺序解释并运行该程序时，CPU 501 识别到诸如功能调用和系统调用的函数，则 CPU 501 确定该函数是否为根据安全性管理表 507a 允许使用的函数。如果该函数是允许使用的函数，则 CPU 501 允许使用该函数并继续运行该程序。另一方面，如果该函数是不允许使用的函数，则 CPU 501 不允许使用该函数并中止运行该程序。

另外，CPU 501 对在顺序解释并运行该程序时出现的对资源的访问请求进行监测，并确定该访问请求的资源是否为根据安全性管理表 507a 允许访问的资源。如果该资源是允许访问的资源，则 CPU 501 允许访问该资源并继续运行该程序。另一方面，如果该资源是不允许访问的资源，则 CPU 501 不允许访问该资源并中止运行该程序。

根据上述配置，移动电话 50 通过限制该程序的可用功能，甚至可以执行违反了安全性策略的程序。

(3) 安全性管理表 507a 可以仅登记允许使用的函数和不允许使用的函数；同时，安全性管理表 507a 可以仅登记与允许访问的资源和不允许访问的资源相关的信息。此外，安全性管理表 507a 可以仅登记允许使用的函数或仅登记不允许使用的函数；同时，安全性管理表 507a 可以仅登记允许访问的资源或仅登记不允许访问的资源。

(4) 在第二实施例中，中继设备 60 的 HD 607 可以针对各个移动电话 50 登记由移动电话 50 的用户设定的安全性级别。在这种情况下，中

继设备 60 可以识别要被传送程序的移动电话 50 的安全性级别，并使用与该安全性级别相对应的安全性管理表 507a 来确定是否对该程序进行中继。

(5) 在第一实施例中，移动电话 50 的非易失性存储器 507 可以为还没有附加检查结果数据 202 的程序存储安全性管理表。另外，如果存在类似于检查机构 20 的多个检查机构，则非易失性存储器 507 可以为已经附加了在除了检查机构 20 以外的检查机构中生成的检查结果数据的程序存储安全性管理表。在第二实施例中也是如此，即，HD 607 可以为还没有附加检查结果数据 202 的程序存储安全性管理表，或者为已经附加了在除了检查机构 20 以外的检查机构中生成的检查结果数据的程序存储安全性管理表。

(6) 在第一实施例中，检查结果数据 202 还可以包含用于识别程序的供应商的供应商识别信息，例如，内容供应商的名称或者程序发送源的 URL；并且移动电话 50 的非易失性存储器 507 可以针对各个供应商识别信息存储不同的安全性管理表 507a。在这种情况下，移动电话 50 可以利用与包含在所接收的检查结果数据 202 中的供应商识别信息相对应的安全性管理表 507a，来确定是否执行所接收的程序。在第二实施例中也是如此，即，检查结果数据 202 还可以包含供应商识别信息，中继设备 60 的 HD 607 可以针对各个供应商识别信息存储不同的安全性管理表 507a；而中继设备 60 可以利用与包含在所接收的检查结果数据 202 中的供应商识别信息相对应的安全性管理表 507a，来确定是否对所接收的程序进行中继。

(7) 在第一实施例中，移动电话 50 在完成程序的下载时，可以通过对该程序的检查结果数据 202 和安全性管理表 507a 进行比较，来确定该程序是否符合安全性策略（安全性管理表 507a），并使液晶显示单元 506 显示该确定结果。该确定结果可以作为语音消息从移动电话 50 输出。另外，在用户使用操作输入单元 505 来指示检查所接收程序的安全性时，移动电话 50 可以通过对该程序的检查结果数据 202 和安全性管理表 507a 进行比较来确定该程序是否符合安全性策略，并输出该确定结果。

在其中不是确定是否应该执行程序而是确定该程序是否符合安全性策略，并且将该确定结果报告给用户的上述情况下，用户根据所报告的确定结果，从非易失性存储器 507 中删除（卸载）该程序，或者避免执行该程序，结果保持了移动电话 50 的安全性。在这种情况下，如果该程序违反了安全性策略，则可以连同确定结果一起将不允许使用的函数的名称和与不允许访问的资源相关的信息（它们包含在该程序中）报告给用户。另选地，如果该程序违反了安全性策略，则移动电话 50 可以使液晶显示单元 506 显示确认是否删除该程序的消息，并且如果通过使用操作输入单元 505 指示删除该程序，则将从非易失性存储器 507 中卸载该程序。

在第二实施例中，中继设备 60 在向移动电话 50 传送程序时，可以通过对该程序的检查结果数据 202 和安全管理表 507a 进行比较，来确定该程序是否符合安全性策略（安全管理表 507a），并连同该程序一起将确定数据发送给移动电话 50。

(8) 在第一实施例中，移动电话 50 在从内容服务器 10a 下载程序之前，可以仅从内容服务器 10a 下载该程序的检查结果数据 202。在这种情况下，移动电话 50 对所接收的检查结果数据 202 和安全管理表 507a 进行比较，由此确定要下载的程序是否符合安全性策略（安全管理表 507a）。作为该确定的结果，如果该程序符合安全性策略，则移动电话 50 从内容服务器 10a 下载该程序。另一方面，如果该程序违反了安全政策，则移动电话 50 取消该程序的下载。根据这种配置，如果要下载的程序违反了安全性策略，则阻止下载该程序，结果可以避免不必要的分组通信。

(9) 在第一和第二实施例中，可以将程序发布给移动电话 50 而不是下载。根据本发明的接收设备可应用于经由公共无线 LAN 进行通信的无线终端、或者经由互联网进行通信的个人计算机。根据本发明的中继设备可应用于网关服务器、代理服务器、或者设置在移动分组通信网络 40 中的交换中心或者基站。用于使诸如移动电话 50 或中继设备 60 的计算机执行根据本发明的处理的程序可以通过网络安装在计算机中，或者可以存储在各种计算机可读存储介质中以进行发布。

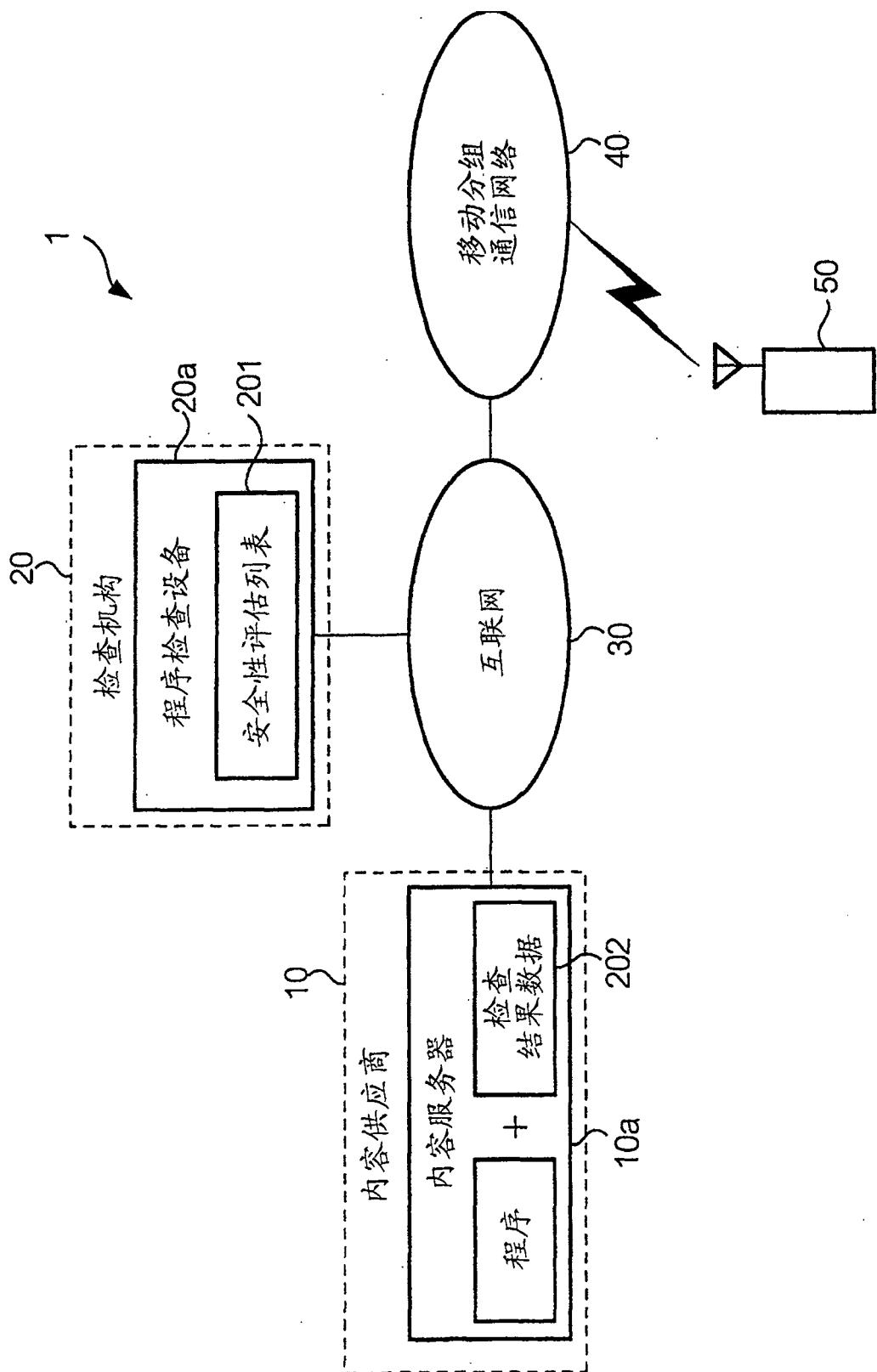


图 1

202

程序	Sample.APP
散列算法	MD5
散列算法	0D247FCB001A2BC5FED000009355FF23
	函数名称
	Function 1 ()
	Function 2 ()
函数	Function 5 ()

所访问的资源	
类型	资源
网络	http://www.XXX.co.jp
文件	Local/UserData/AddressBook

图 2

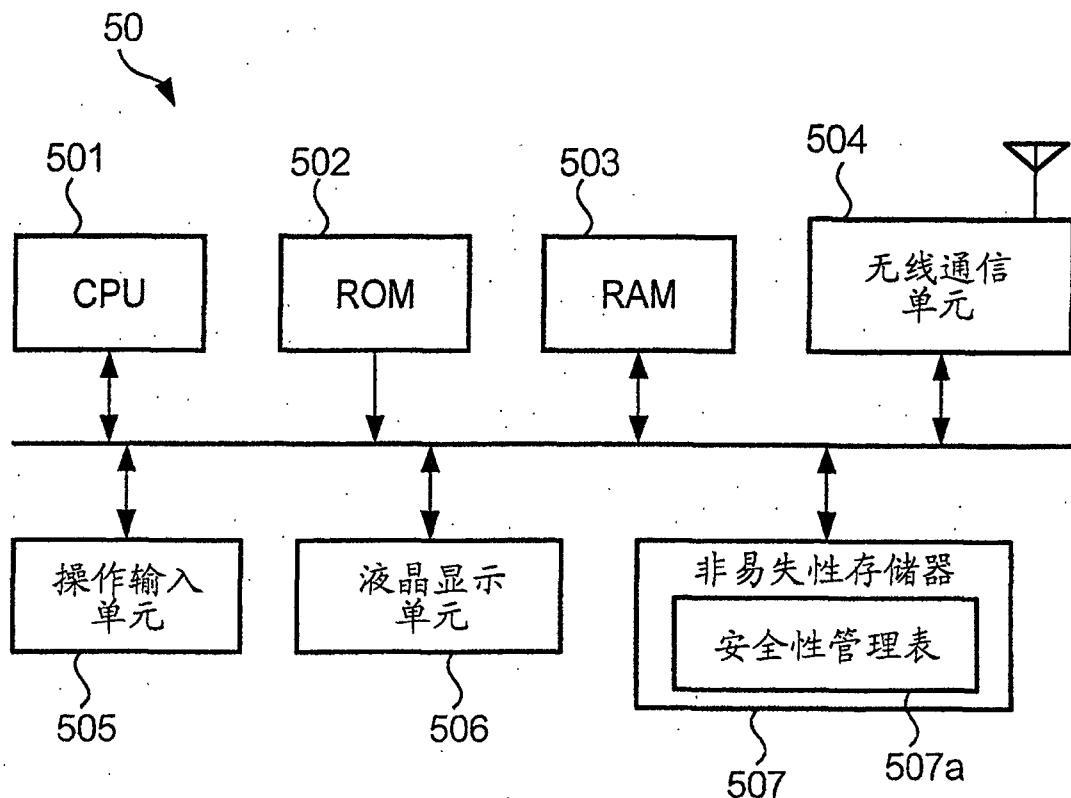


图 3

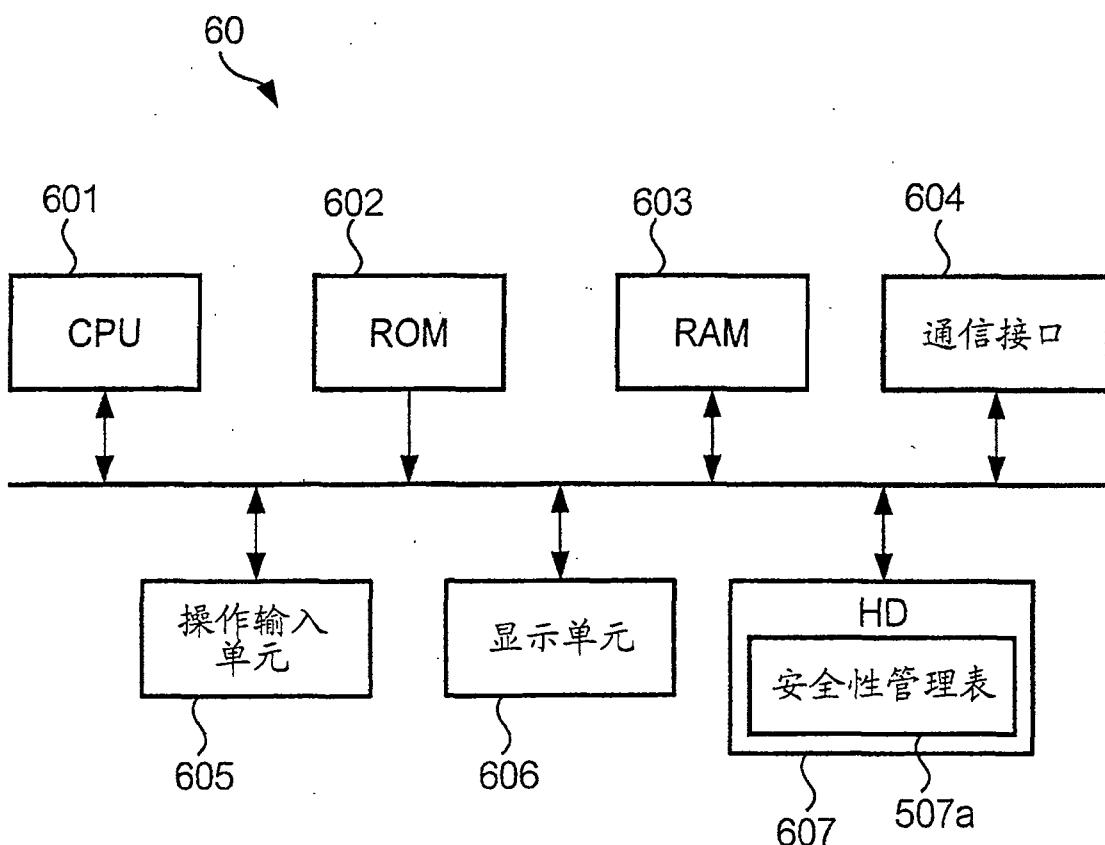


图 9

507a

安全级别	级别1	类别	函数名称	许可
函数	文件访问	函数 1()	禁止	许可
	网络访问	函数 2()	允许	
		所有函数	禁止	
			
所访问的资源	类型	资源	允许	
	网络	http://www.www.xxx.co.jp	用户确认	
	数据文件	所有数据文件	禁止	
	文件	Local/UserData/AddressBook	禁止	
			

图 4

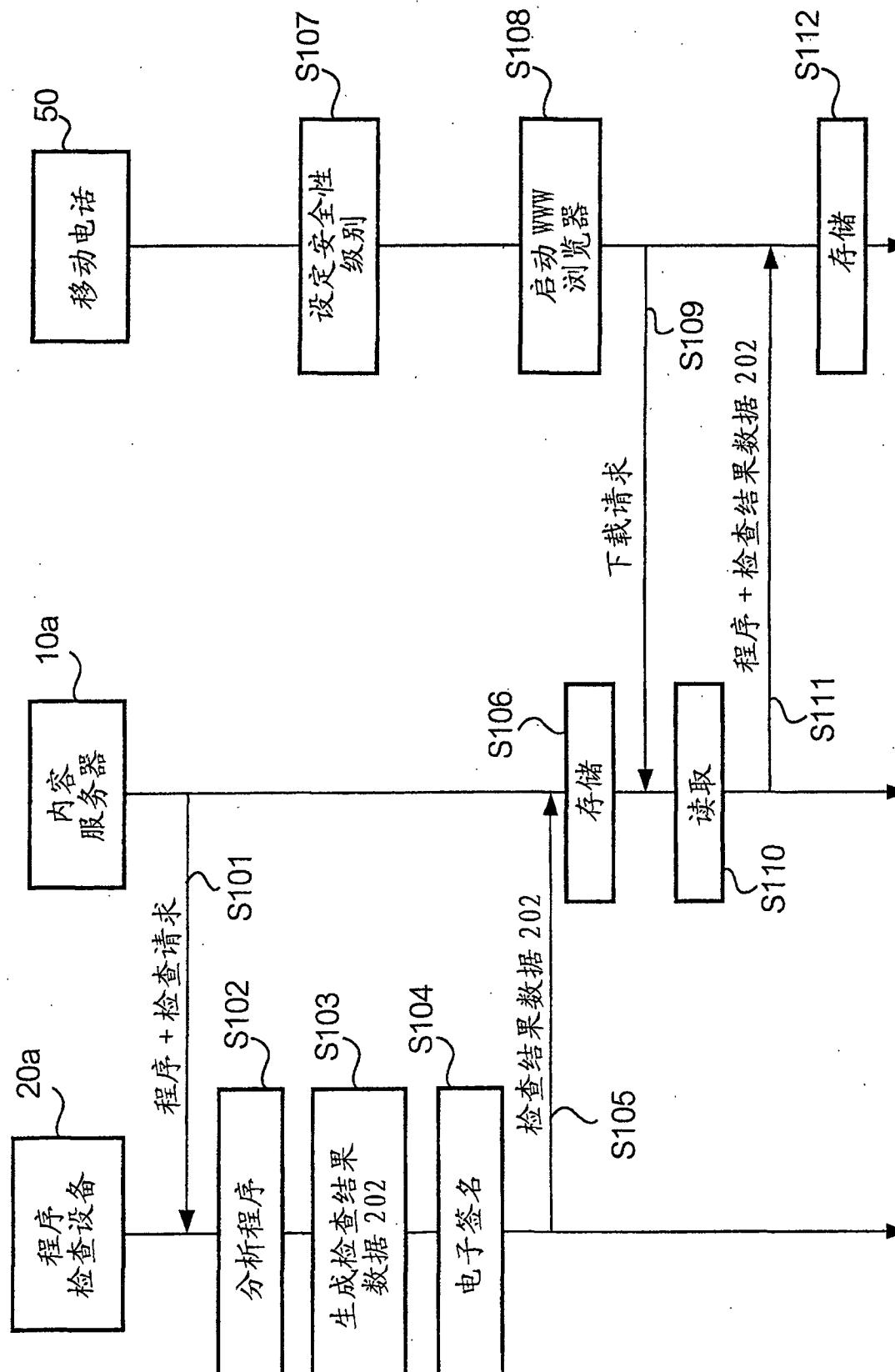


图 5

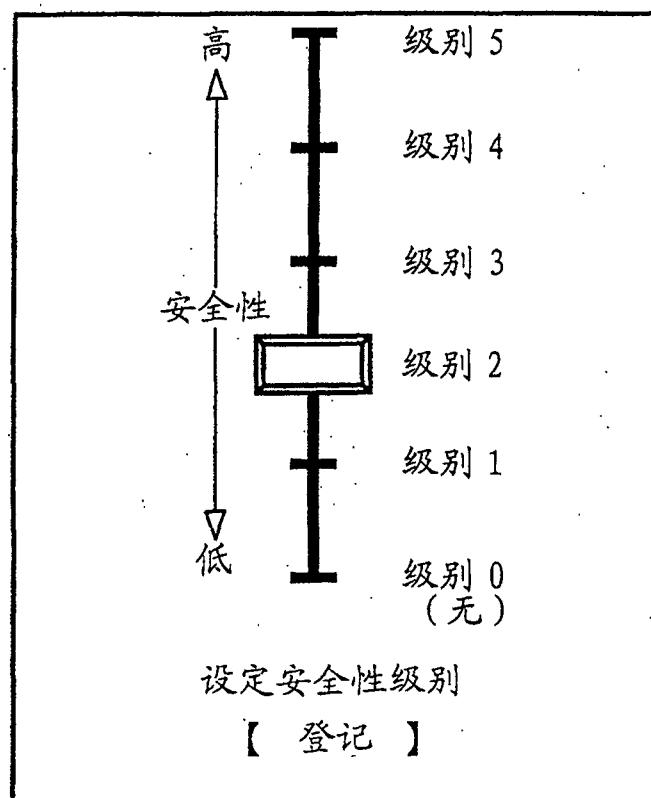


图 6

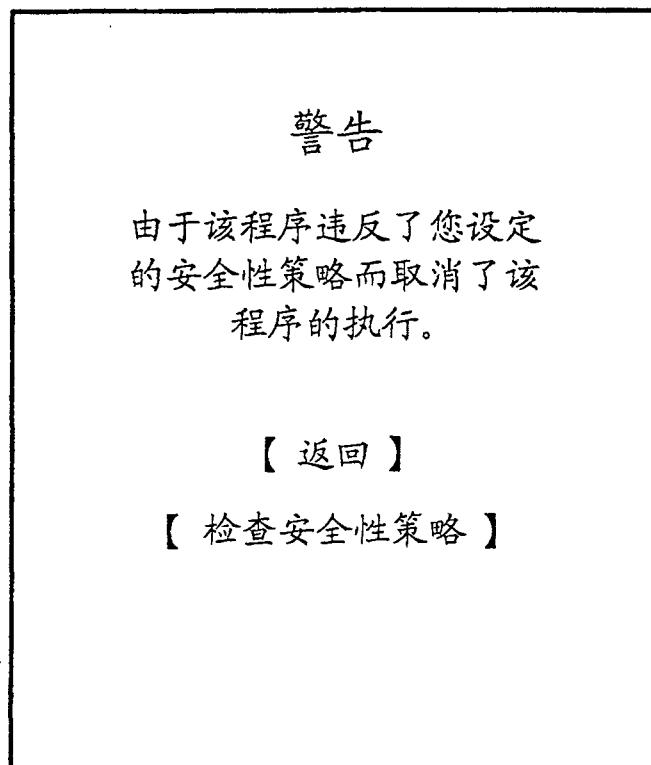


图 8

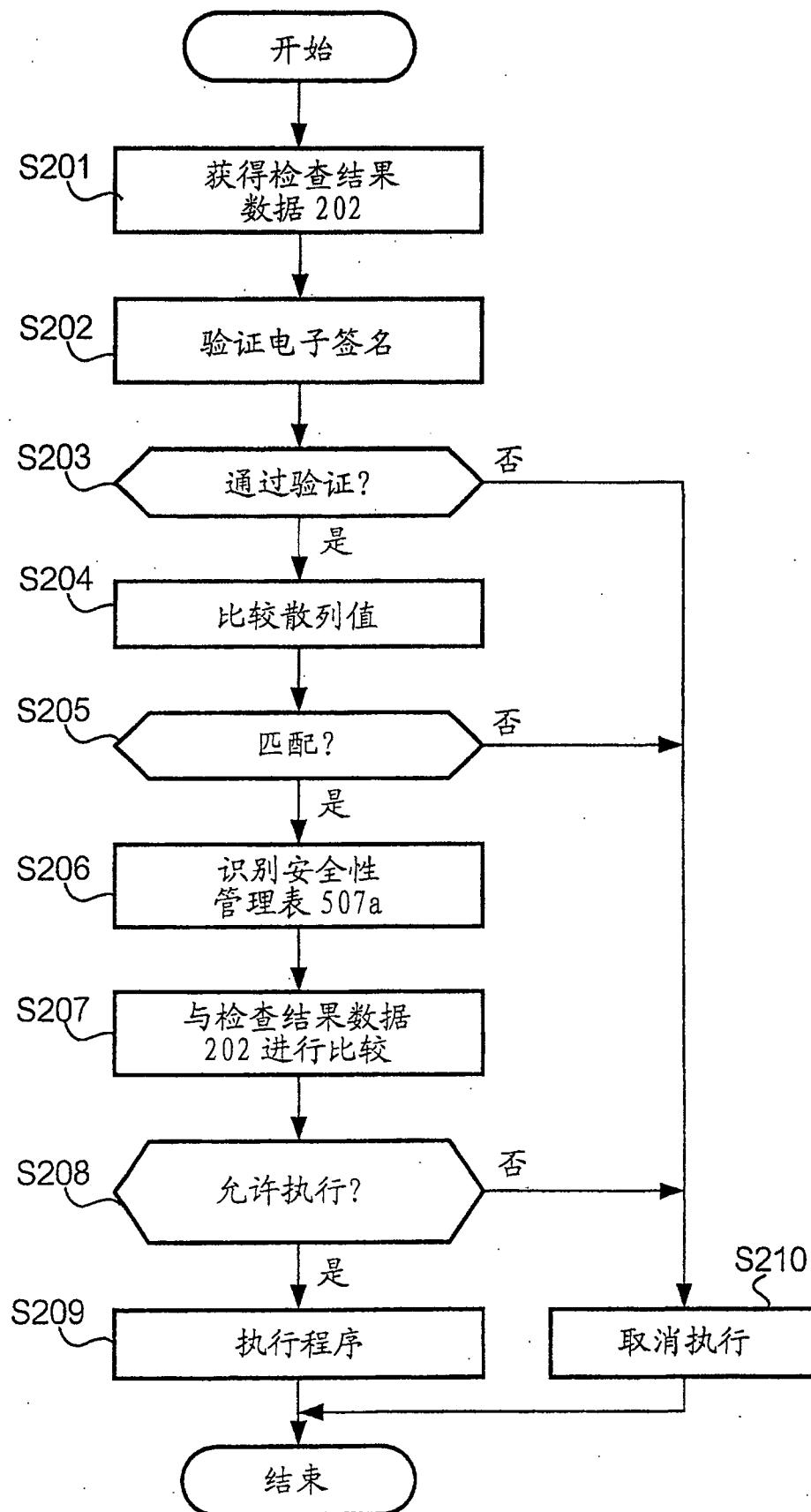


图 7

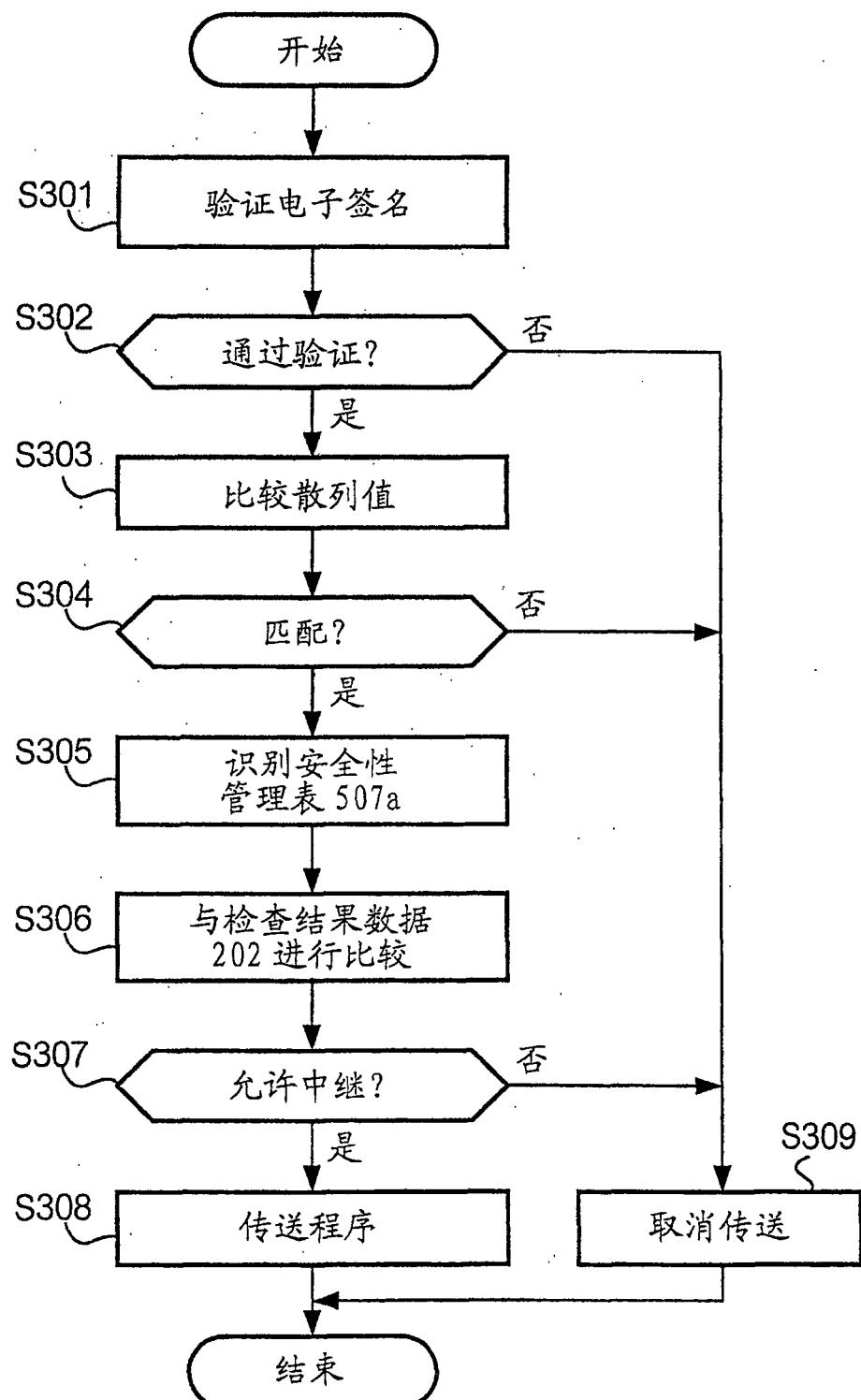


图 10

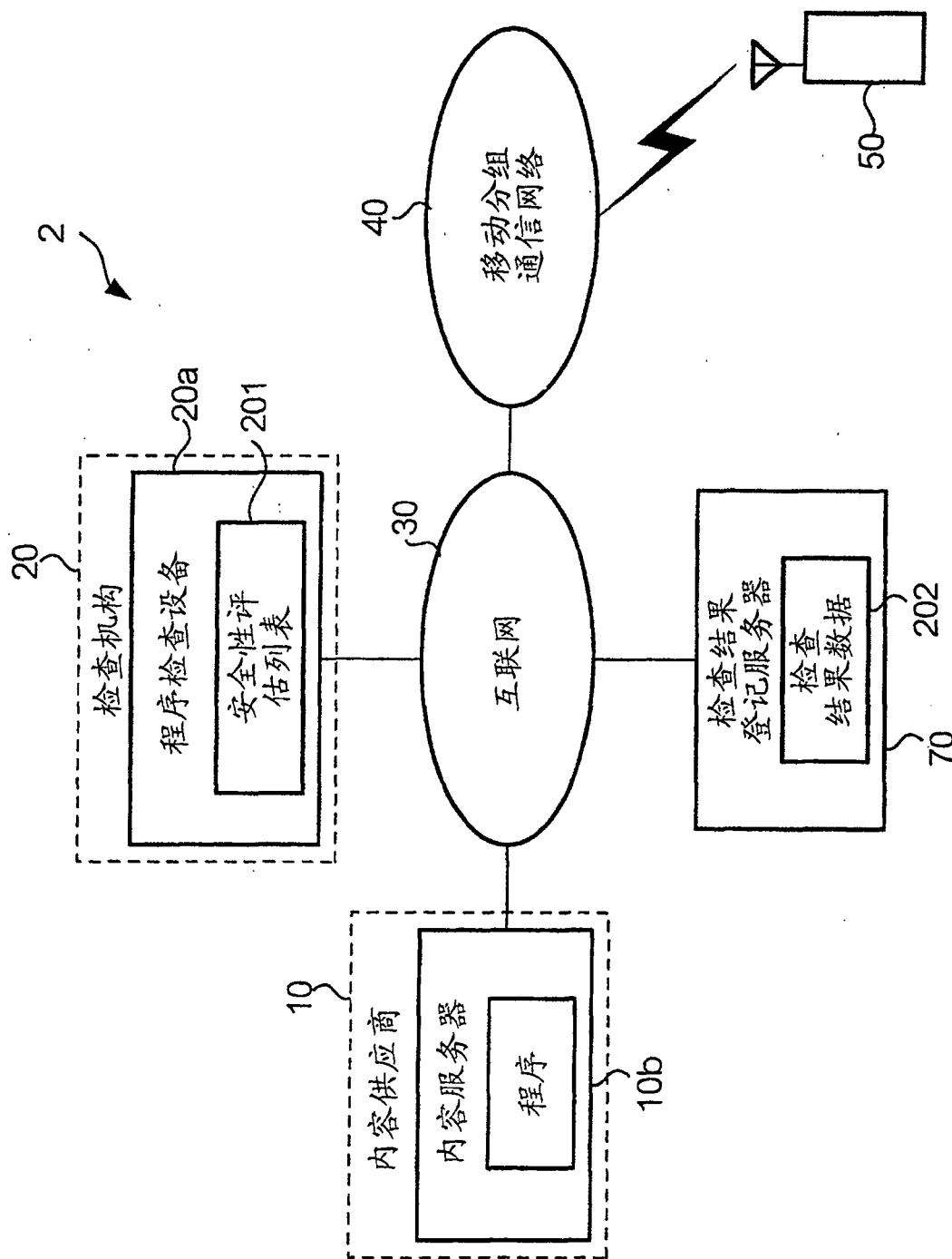


图 11

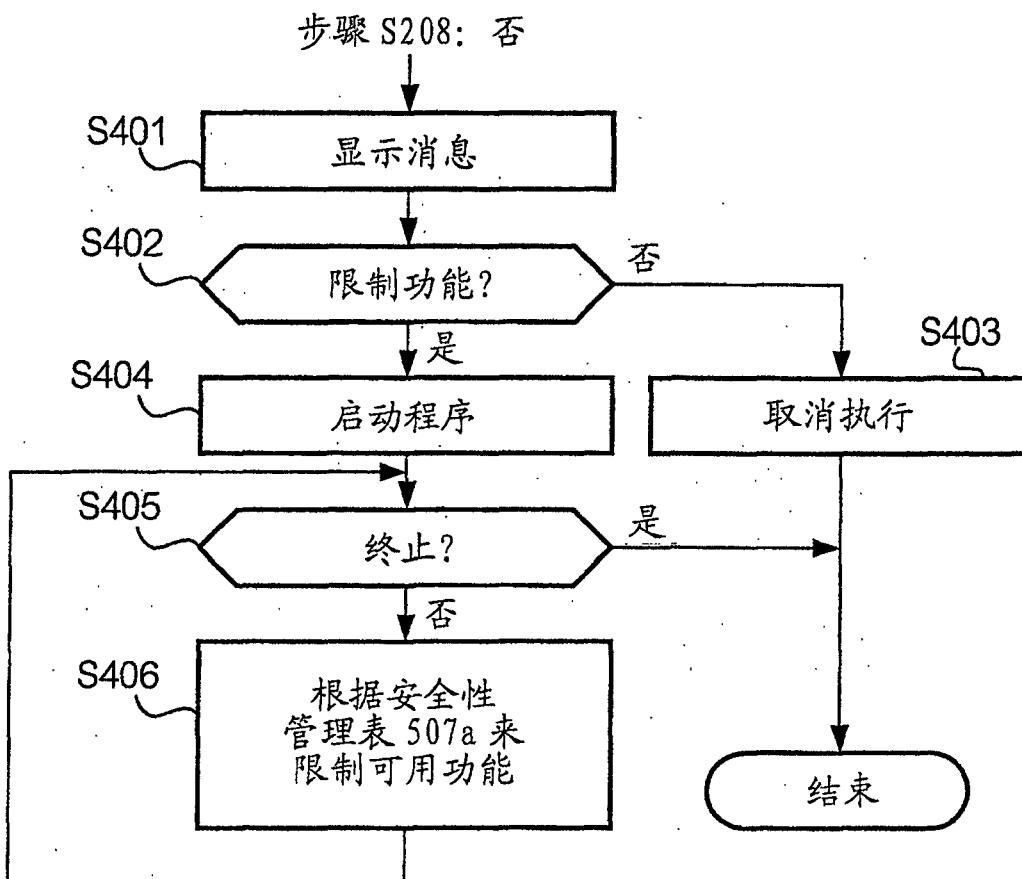


图 12

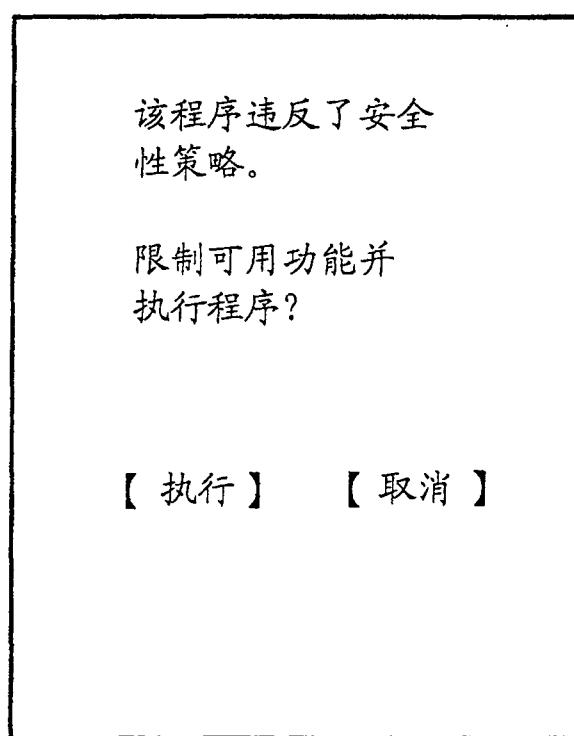


图 13