[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 21/00 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200710192736.3

[43] 公开日 2008 年 7 月 2 日

[11] 公开号 CN 101211393A

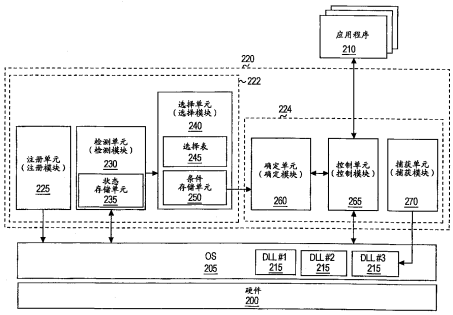
[22] 申请日 2007.11.16
[21] 申请号 200710192736.3
[30] 优先权
[32] 2006.12.27 [33] JP [31] 2006 - 351606
[71] 申请人 国际商业机器公司
地址 美国纽约阿芒克
[72] 发明人 小仓明宏 利根川聪子 古市实裕
[74] 专利代理机构 北京市金杜律师事务所
代理人 朱海波
权利要求书 3 页 说明书 17 页 附图 7 页

[54] 发明名称

用于控制应用程序对资源的访问的信息处理设备和方法

[57] 摘要

本发明提供用于基于信息处理设备的运行环境或运行状态拒绝或允许应用程序对资源的访问的技术。 该信息处理设备包括：检测单元，用于检测连接到信息处理设备的设备的连接状态或运行状态的变化；选择单元，用于作为对检测连接状态的变化的响应，基于检测到的连接状态选择要应用于信息处理设备的资源访问条件；以及条件存储单元，用于存储所选择的资源访问条件。 该信息处理设备进一步包括：捕获单元，用于捕获由应用程序向操作系统发出的针对资源访问的多个函数调用；确定单元，用于确定是否允许所捕获的函数调用；以及控制单元，用于拒绝该函数调用。 当捕获到函数调用时，基于从条件存储单元读取的资源访问条件确定是否允许所捕获的函数调用，并且作为对确定不允许该函数调用的响应而拒绝该函数调用。



1. 一种在信息处理设备中用于控制运行在所述信息处理设备上的应用程序对资源的访问的方法，所述方法包括:

检测连接到所述信息处理设备上的设备的连接状态或运行状态的变化的步骤;

作为检测所述连接状态或所述运行状态的变化的响应，参考表并选择要应用于所述信息处理设备的资源访问条件的步骤，在所述表中所述设备的所述连接状态或所述运行状态中的每个都与应当应用的资源访问条件相关联;

将所述所选择的资源访问条件存储到条件存储单元的步骤;

捕获由所述应用程序向操作系统发出的针对资源访问的函数调用的步骤;

基于从所述条件存储单元读取的所述资源访问条件确定是否允许所述捕获的函数调用的步骤; 以及

作为对确定不允许所述函数调用的响应而拒绝所述函数调用的步骤。

2. 根据权利要求 1 所述的方法，其中所述设备是网络设备、外部显示器和外部介质中的任意一个。

3. 根据权利要求 1 所述的方法，其中所述检测步骤包括检测网络设备的运行状态的变化的步骤，

其中如果无线网络设备准备就绪可以使用，则所述选择步骤包括选择比在有线网络设备准备就绪可以使用的情况下的资源访问条件更严格的资源访问条件的步骤。

4. 根据权利要求 1 所述的方法，其中所述检测步骤包括在检测到网络设备准备就绪可以使用时获取所述信息处理设备所连接到的网络的类型的步骤，所述类型表明了所述网络的安全级别，

其中如果所述网络设备准备就绪可以使用并且所述网络的所述类型并不代表安全的网络，则所述选择步骤包括选择比在所述网络设备准

备就绪可以使用并且所述网络的所述类型代表安全网络的情况下的资源访问条件更严格的资源访问条件的步骤。

5. 根据权利要求 1 所述的方法，其中所述检测步骤包括检测外部显示器的连接状态的变化的步骤，

其中如果所述外部显示器已连接，则所述选择步骤包括选择用于拒绝用以浏览预定数据的函数调用的资源访问条件的步骤。

6. 根据权利要求 1 所述的方法，其中所述检测步骤包括检测外部介质的连接状态或运行状态的变化的步骤，

其中如果所述外部介质已连接或者准备就绪可以使用，则所述选择步骤包括选择用于使得从所述外部介质调用的进程和另一个进程在不同的条件下访问资源的资源访问条件的步骤。

7. 根据权利要求 1 所述的方法，其中所述检测步骤包括在检测到外部介质已连接或准备就绪可以使用时获取所述外部介质的硬件标识信息的步骤，

其中如果所述外部介质已连接或准备就绪可以使用，则所述选择步骤包括基于所述外部介质的所述硬件标识信息选择要应用于所述信息处理设备的资源访问条件的步骤。

8. 根据权利要求 1 所述的方法，进一步包括作为对检测多个设备的所述连接状态或所述运行状态的所述变化的响应，将所述检测到的所述多个设备的连接状态或运行状态存储到状态存储单元的步骤，

其中在所述表中，所述多个设备的连接状态或运行状态的每个组合都与应当应用的资源访问条件相关联，

其中所述选择步骤包括从所述状态存储单元读取各个设备的所述当前连接状态或运行状态、参考所述表、以及选择要应用于所述信息处理设备的资源访问条件的步骤。

9. 一种用于控制应用程序对资源的访问的信息处理设备，所述信息处理设备包括：

检测单元，用于检测连接到所述信息处理设备上的设备的连接状态或运行状态的变化；

选择单元，用于作为检测所述连接状态或所述运行状态的变化的响应，参考表并选择要应用于所述信息处理设备的资源访问条件，在所述表中所述设备的所述连接状态或所述运行状态中的每个都与应当应用的资源访问条件相关联；

条件存储单元，用于存储所述所选择的资源访问条件；

捕获单元，用于捕获由所述应用程序向操作系统发出的针对资源访问的函数调用；

确定单元，用于基于从所述条件存储单元读取的所述资源访问条件确定是否允许所述捕获的函数调用；以及

控制单元，用于作为对确定不允许所述函数调用的响应而拒绝所述函数调用。

用于控制应用程序对资源的访问的信息处理设备和方法

技术领域

本发明涉及控制应用程序通过操作系统对资源的访问，并且更特别地，涉及一种用于作为对信息处理设备的运行环境或运行状态的响应而控制运行在该信息处理设备上的应用程序对资源的访问的技术。

背景技术

已经提出了一种已知技术（例如参考专利文献1），其中为了完全拒绝没有访问权限的用户所进行的信息导出，在信息处理设备中，作为对用户访问权限的响应，限制诸如文件的打印、移动和复制，在软盘中用另一个名字保存文件，以及捕获屏幕之类的功能。

在专利文献1（日本未审专利申请公开No. 2003-44297）中的技术中，首先由资源管理程序捕获对操纵由操作系统管理的诸如文件、网络、存储单元、显示器屏幕和外部附件之类的计算机资源的请求。捕获到该操纵请求的资源管理程序确定用户是否有访问在该操纵请求中指定的计算机资源的权限。然后，作为确定的结果，当用户有访问权限时，资源管理程序将操纵请求不加改变地传递给操作系统。另一方面，当用户没有访问权限时，资源管理系统拒绝操纵请求。

发明内容

但是，在前述技术中，结合用户和计算机资源的组合而定义了对计算机资源的访问许可。访问许可由例如管理员静态地定义。这样，在前述技术中，不能作为对信息处理设备的运行环境或运行状态的响应而改变访问许可。不能作为对信息处理设备的运行环境的响应而指定访问许可，该运行环境例如是如下环境，在该环境中，在诸如公司设备之类的

安全场所使用信息处理设备。而且，不能作为对信息处理设备的运行状态的响应而指定访问许可，该运行状态例如是如下状态，在该状态下，USB 连接到信息处理设备。

本发明的一个目的是提供一种用于控制应用程序通过操作系统对数据的访问的设备、方法和程序，以便为前述问题提供解决方案。

解决问题的方法

用于达到前述目的的本发明由在信息处理设备中执行的用于控制运行在该信息处理设备上的应用程序对资源的访问的以下方法来实现。在这种方法中，首先检测连接到信息处理设备上的设备的连接状态或运行状态的变化。作为对连接状态或运行状态的变化的检测的响应，选择要应用于信息处理设备的资源访问条件，参考表，在该表中设备的连接状态或运行状态中的每个都与应当应用的资源访问条件相关联。将所选择的资源访问条件存储到条件存储单元。然后，作为对捕获由应用程序向操作系统发出的针对资源访问的函数调用的响应，从条件存储单元读取资源访问条件，并且基于该资源访问条件确定是否允许所捕获的函数调用。如果确定不允许所捕获的函数调用，则拒绝该函数调用。

这里的资源表示由操作系统管理的计算机资源，诸如文件、主存储器、外部存储单元以及进程。而且，这里的针对资源访问的函数调用可以是用以浏览、创建、删除、复制和移动资源，将资源读入共享存储器，打印资源，以及激活进程的所有类型的针对数据访问的函数调用中的任意一种。

优选地，该设备可以是网络设备、外部显示器和外部介质中的任意一个。这里的外部介质包括所有被信息处理设备识别为外部驱动器的介质，例如，诸如 USB 存储器、CD-ROM、DVD-ROM、压缩闪卡及 SD 卡之类的存储介质和诸如外部硬盘驱动器和数码相机之类的外围设备。

优选地，检测步骤包括检测网络设备的运行状态的变化的步骤。如果无线网络设备准备就绪可以使用，则选择步骤包括选择比在有线网络设备准备就绪可以使用的情况下的资源访问条件更严格的资源访问条件的步骤。

优选地，检测步骤包括在检测到网络设备准备就绪可以使用时获取信息处理设备所连接到的网络的类型的步骤，该类型表明了该网络的安全级别。如果网络设备准备就绪可以使用并且所连接网络的类型并不代表安全的网络，则选择步骤包括选择比在网络设备准备就绪可以使用并且网络的类型代表安全网络的情况下的资源访问条件更严格的资源访问条件的步骤。

优选地，检测步骤包括检测外部显示器的连接状态的变化的步骤。如果外部显示器已连接，则选择步骤包括选择用于拒绝用以浏览预定数据的函数调用的资源访问条件的步骤。

优选地，检测步骤包括检测外部介质的连接状态或运行状态的变化的步骤。如果外部介质已连接或者准备就绪可以使用，则选择步骤包括选择用于使得从外部介质调用的进程和另一个进程在不同的条件下访问资源的资源访问条件的步骤。

优选地，检测步骤包括在检测到外部介质已连接或准备就绪可以使用时获取外部介质的硬件标识信息的步骤。如果外部介质已连接或准备就绪可以使用，则选择步骤包括基于外部介质的硬件标识信息选择要应用于信息处理设备的资源访问条件。使用厂商、模型号、序列号等等作为硬件标识信息。

优选地，该用于控制资源访问的方法进一步包括作为对检测多个设备的连接状态或运行状态的变化的响应，将检测到的多个设备的连接状态或运行状态存储到状态存储单元的步骤。在该表中，该多个设备的连接状态或运行状态的每个组合都与应当应用的资源访问条件相关联。选择步骤包括从状态存储单元读取各个设备的当前连接状态或运行状态、参考表、以及选择要应用于信息处理设备的资源访问条件的步骤，在该表中多个设备的连接状态或运行状态的每个组合都与应当应用的资源访问条件相关联。

虽然将本发明已经被描述为一种在信息处理设备中用于控制通过操作系统对资源的访问的方法，但是本发明可以被考虑为一种用于使信息处理设备执行这种方法的程序。而且，本发明可以被考虑为一种用于

控制通过操作系统对数据的访问的信息处理设备。

优势

根据本发明，可以基于信息处理设备的运行环境或运行状态灵活地拒绝或允许通过操作系统的资源访问。

附图说明

现在将基于附图详细描述用于执行本发明的最佳模式。以下实施例并不会对权利要求书中所要求保护的本发明构成限制。此外，实施例中所描述的特征的所有组合并不一定只能用于本发明的用于解决上述问题的方法。贯穿对实施例的描述，相同的标号被分配给相同的组件。

图 1 示出了根据本发明的一个实施例的信息处理设备 100 的硬件配置示例。

图 2 是信息处理设备 100 的功能框图，该信息处理设备 100 执行根据本发明的一个实施例的用于控制通过操作系统的数据访问的程序 220。

图 3 的（a）部分示出了表明各个设备当前连接状态或运行状态的信息的示例。（b）部分示出了分配给网络设备的两个比特的含义。（c）部分示出了分配给不同于网络设备的设备的一个比特的含义。

图 4 示出了选择表 245 的一个示例。

图 5 示出了图 4 所示的七十二个访问条件的细节的示例。

图 6 是示出驻留程序 222 的处理流程的示例的流程图。

图 7 是示出程序 224 的处理流程的示例的流程图。

具体实施方式

图 1 示出了可以在本发明的一个实施例中使用的信息处理设备的硬件配置示例。信息处理设备 100 包括 CPU 外围部分、输入输出部分和既有输入输出部分，其中 CPU 外围部分包括通过主机控制器 110 相互连接的 CPU 105、RAM 115 和图形控制器 120，显示器 125，以及外部显示器 180，输入输出部分包括通过输入输出控制器 130 连接到主机控

制器 110 的通信接口 145、硬盘驱动器 135 和 CD-ROM 驱动器 140，既有输入输出部分包括连接到输入输出控制器 130 的超级 I/O 控制器 150、闪速 ROM 160 和键盘鼠标控制器 165 以及连接到超级 I/O 控制器 150 的软盘驱动器 155。

主机控制器 110 将 CPU 105 和图形控制器 120 连接到 RAM 115，CPU 105 和图形控制器 120 以高传送速率访问 RAM 115。CPU 105 根据存储在闪速 ROM 160 和 RAM 115 中的程序运行并控制各个组件。图形控制器 120 获取在由 CPU 105 等在 RAM 115 中提供的帧缓冲器中产生的图像数据并在显示器 125 和/或外部显示器 180 上显示该图像数据。作为对这种配置的替代，图形控制器 120 可以包括存储由 CPU 105 等产生的图像数据的帧缓冲器。

输入输出控制器 130 将作为相对高速的输入输出单元的通信接口 145、硬盘驱动器 135 和 CD-ROM 驱动器 140 连接到主机控制器 110。通信接口 145 通过网络与外部设备通信。通信接口 145 是连接到 Ethernet（以太网，注册商标）的以太网适配器或通过空中接口而不是电缆连接到网络的无线 LAN（局域网）适配器。新近的信息处理设备 100 既包括以太网适配器又包括无线 LAN 适配器作为通信接口 145。当信息处理设备 100 是笔记本电脑时，输入输出控制器 130 进一步将 CardBus 控制器 190 连接到主机控制器 110。CardBus 控制器 190 控制插入到 PC 卡槽的 PC 卡，PC 卡作为例如闪存卡、硬盘、SCSI 卡、LAN 卡或无线 LAN 卡使用。

硬盘驱动器 135 存储信息处理设备 100 使用的程序和数据。CD-ROM 驱动器 140 从 CD-ROM 读取程序或数据并将这些程序或数据提供给 RAM 115 或硬盘驱动器 135。而且，在输入输出控制器 130 中提供 USB 端口。USB 端口连接到在例如信息处理设备 100 的壁面上提供的 USB 连接器 170 上。诸如 USB 存储器或 USB 外部 HDD 之类的可移动设备可以连接到 USB 连接器 170。

而且，闪速 ROM 160 以及作为相对低速输入输出单元的超级 I/O 控制器 150、键盘鼠标控制器 165 等连接到输入输出控制器 130。闪速

ROM 160 存储在信息处理设备 100 被激活时由 CPU 105 执行的引导程序、依赖于信息处理设备 100 的硬件的程序等等。软盘驱动器 155 从软盘读取程序或数据并通过 RAM 115 将这些程序或数据提供给超级 I/O 控制器 150。超级 I/O 控制器 150 通过并口、串口、键盘端口、鼠标端口等等来实现对例如打印机、软盘、键盘和鼠标之类的输入输出单元的连接。

下面描述的根据本发明的用于控制通过操作系统的资源访问的程序 220 存储在诸如软盘、CD-ROM 或 IC 卡之类的存储介质中并由用户提供。通过输入输出控制器 130 和/或超级 I/O 控制器 150 从存储介质上读取该程序并在信息处理设备 100 中安装和执行该程序。

程序 220 可以存储在外部存储介质中。除了软盘和 CD-ROM，诸如 DVD 或 PD 之类的光记录介质，诸如 MD、磁带介质之类的磁-光记录介质，诸如 IC 卡之类的半导体存储器等可以作为存储介质使用。而且，可以使用在连接到专用通信网络、因特网等的服务器系统中所提供的诸如硬盘或 RAM 之类的存储单元作为存储介质，通过网络将程序提供给信息处理设备 100。

图 2 是信息处理设备 100 的功能框图，该信息处理设备 100 执行根据本发明的一个实施例的用于控制通过操作系统的资源访问的程序 220。图 2 中示出的硬件 200 是图 1 中示出的信息处理设备 100 的硬件。信息处理设备 100 使得操作系统(以下称为 OS)205 在硬件 200 上运行。OS 205 是执行各种类型的应用 210 的通用 OS，诸如微软公司的 Windows（商标）OS，IBM 公司的 OS/2（商标），或 Linux（注册商标）OS。

一般而言，在通用 OS 上运行的应用程序 210 在该应用程序 210 访问资源时使用由 OS 205 提供的应用程序接口（以下称为 API）。例如，当应用程序 210 制作文件副本时，应用程序 210 向 OS 205 发出 API 函数调用以制作文件副本。类似地，当应用程序 210 将文件从某个介质移动到另一个介质时，应用程序 210 向 OS 205 发出 API 函数调用以移动该文件。当 OS 205 是 Windows（商标）OS 时，API 函数被提供为动态链接库（以下称为 DLL）215。说明书中描述的应用程序 210 表示所有

的运行在 OS 205 上的程序。

这样，控制各种类型的应用对资源的访问通过如下操作来实现，即监控对由 OS 205 提供的多个 API 函数中的被预设为对象的 API 函数的调用以及正在受到监控的对象中的进程，并基于适当的资源访问条件来确定是否允许检测到的 API 函数调用。根据本发明的信息处理设备 100 的一个目的是针对信息处理设备100的运行环境或运行状态动态地确定用于确定是否允许检测到的 API 函数调用的资源访问条件。根据连接到信息处理系统 100 的设备的连接状态或运行状态来估计信息处理设备 100 的运行环境或运行状态。

用于控制通过操作系统对资源的访问的程序 220 包括驻留程序 222 和程序 224，驻留程序 222 包括注册模块、检测模块和选择模块，程序 224 包括确定模块、控制模块和捕获模块。这些模块使得信息处理设备 100 用作注册单元 225、检测单元 230、选择单元 240、确定单元 260、控制单元 265 和捕获单元 270。

注册单元 225 执行用于从 OS 205 接收关于信息处理设备 100 的设备硬件配置的变化的通知的注册。一般而言，OS 205 提供用于向指定应用发送关于硬件配置变化的通知的服务。在这个实施例中，为网络设备、外部显示器和外部介质注册设备通知。

例如，在 Windows（商标）OS 中，RegisterDeviceNotification 函数可以用于注册设备通知。在 RegisterDeviceNotification 函数中，指定接收设备事件的服务或窗口的句柄和指向指定了接收通知的设备或设备类型的数据块的指针。而且，可以使用 Windows 管理工具（WMI）的 ExecNotificationQuery 函数注册更详细的设备事件通知，WMI 是管理设备驱动器的通用方法。

检测单元 230 检测连接到信息处理设备 100 的设备的连接状态或运行状态的变化。当使用 RegisterDeviceNotification 函数注册设备通知时，检测单元 230 通过从 Windows（商标）OS 接收 WM_DEVICECHANGE 消息来检测设备的连接状态或运行状态的变化。WM_DEVICECHANGE 消息包括表明发生了什么事件的参数和指向包括关于发生事件的设备

的信息的关于事件的详细信息的指针。

例如，当设备或介质被插入并准备就绪可以使用时，发送WM_DEVICECHANGE 消息，其中 DBT_DEVICEARRIVAL 作为参数被设置。而且，当网络已经准备就绪可以使用时，发送WM_DEVICECHANGE 消息，其中设置了DBT_DEVNODES_CHANGED。有必要通过单独接收关于 WMI 事件的通知来检测电缆的连接状态的变化。

而且，当检测单元 230 检测到网络设备的运行状态的变化时，检测单元 230 获取信息处理设备 100 所连接的网络的类型，该类型表明了网络的安全级别。表明了安全级别的网络类型包括可以用于确定信息处理设备 100 是否在安全环境下使用的所有网络类型，例如，建立了防火墙的内部网络或没有采取措施防止外部入侵的外部网络。例如，可以通过使用 ipconfig 命令检查分配给信息处理设备 100 的 IP 地址的网络端口值来获取网络类型。而且，当一直存在于网络中的特定设备的 IP 地址已知时，可以通过向该特定设备发出 ping 命令来获取所连接的网络的类型。例如，在特定设备是内部服务器的情况下，当获取对 ping 命令的响应时，所连接的网络是内部网络。

而且，当检测单元 230 检测到外部介质已连接或准备就绪可以使用时，检测单元 230 获取外部介质的硬件标识信息，诸如厂商、模型号和序列号。可以通过例如向设备驱动器发送 I/O 控制码（DeviceIoControl）并获取设备描述符（DeviceDescriptor）来获取这种硬件标识信息。

而且，检测单元 230 包括状态存储单元 235，其存储关于每个设备的当前连接状态或运行状态的信息并用检测到的每个设备的连接状态或运行状态更新存储在状态存储单元 235 中的信息。图 3 示出了存储在状态存储单元 235 中的信息的示例。在这个实施例中，使用一个字节存储六类设备的连接状态或运行状态，这六类设备包括有线网络设备、无线网络设备、外部显示器、外部介质#1 到#3，如图 3 的（a）部分所示。两个比特分配给每个网络设备，一个比特分配给每个其他设备。

图 3 的（b）部分示出了分配给每个网络设备的两个字节的含义。

值 00 表明对应的网络设备未被使用。值 01 和 10 都表明对应的网络设备正在被使用。值 01 表明对应的网络设备连接到内部网络，值 10 表明对应的网络设备连接到外部网络。图 3 的（c）部分示出了分配给每个其他设备的一个比特的含义。值 0 表明对应的设备未连接到信息处理设备 100，值 1 表明对应的设备连接到信息处理设备 100。

作为对检测单元 230 对连接状态或运行状态的变化的检测的响应，选择单元 240 基于检测到的连接状态或运行状态选择要应用于信息处理设备 100 的资源访问条件。更特别地，选择单元 240 包括选择表 245，该表中多个设备的连接状态或运行状态的每个组合都与应当应用于每个组合的资源访问条件相关联，并且选择单元 240 参考选择表 245 来选择与从状态存储单元 235 读取的设备的当前连接状态或运行状态的组合相关联的资源访问条件作为要应用于信息处理设备 100 的资源访问条件。选择单元 240 进一步包括条件存储单元 250 并将所选择的资源访问条件存储到条件存储单元 250。

图 4 示出了选择表 245 的示例，包括了五类设备：有线网络设备、无线网络设备、外部显示器及外部介质#1 和#2。每个网络设备处于以下三种状态中的一种：连接到内部网络、连接到外部网络、未被使用，如参考图 2 所述。每个其他设备处于以下两种状态中的一种：连接的和未连接的。这样，通过计算三（有线网络设备可能的状态数量）、三（无线网络设备可能的状态数量）、二（外部显示器可能的状态数量）、二（外部介质#1 可能的状态数量）和二（外部介质#2 可能的状态数量）的乘积，可以发现存在多个设备的连接状态或运行状态的七十二种组合，并且每个组合与应当应用于每个组合的访问条件相关联。这七十二个访问条件并非一定要相互不同，部分访问条件可以相互重合。

一般而言，多种类型的外部介质可以连接到信息处理设备 100，并且相同的资源访问条件可以应用于所有的外部介质。但是，在这个实施例中，将连接到信息处理设备 100 的外部介质分类，如图 4 所示，并且为特定的外部介质选择资源访问条件，该资源访问条件不同于其他外部介质的资源访问条件。这实现了访问控制，其中例如在有特定模型号并

由公司发给员工用于商业用途的诸如有指纹认证功能的 USB 存储器之类的可靠介质和很多非特定的不可靠介质之间进行区分。

图 5 示出了图 4 所示出的七十二个资源访问条件的细节的示例。用户或管理信息处理设备100的系统管理员可以适当地确定并设置资源访问条件。将资源访问条件 1 应用于信息处理设备 100 通过有线网络设备连接到内部网络的情况。由于信息处理设备100用电缆连接到外部网络，可以假定信息处理设备100是在基本上只有同一部门的员工可以进入的安全场所使用的，该场所诸如公司中员工的个人工作区。这样，在访问条件 1 中，允许所有类型的针对数据访问的函数调用，诸如用以浏览、创建、删除、复制和移动数据，将数据读入共享存储器，打印数据，以及激活进程的函数调用。

另一方面，将资源访问条件 6 应用于信息处理设备 100 通过无线网络设备连接到内部网络的情况。由于信息处理设备 100 通过空中接口连接到内部网络，所以可以假定信息处理系统 100 是在例如另一个部门中的员工以及参观公司的客户和商家可以进入的诸如公司的会议室或自助餐厅之类的场所使用的。这样，尽管信息处理设备 100 在公司内使用，还是需要在一定程度上考虑包括信息泄漏的风险。因此，在资源访问条件 6 中，对于诸如机密信息之类的预定数据，禁止用以复制、删除和移动数据，将数据读入共享存储器，打印数据，以及激活进程的函数调用。以这种方式，在这个实施例中，资源访问条件 6 要比资源访问条件 1 严格。当无线网络设备准备就绪可以使用时，将比在有线网络设备准备就绪可以使用的情况下更严格的资源访问条件应用于信息处理设备 100。

将资源访问条件 9 应用于信息处理设备 100 通过无线网络设备连接到外部网络的情况。由于信息处理设备 100 通过空中接口连接到外部网络，所以可以假定信息处理设备 100 是在有很多非特定的人存在的诸如机场或旅馆大厅之类的场所使用的。这样，在资源访问条件 9 中，对于诸如机密信息之类的预定数据，禁止所有类型的针对数据访问的函数调用，诸如用以浏览、复制、删除和移动数据，将数据读入共享存储器，打印数据，以及激活进程的函数调用。以这种方式，在这个实施例中，

资源访问条件 9 要比资源访问条件 6 严格。当信息处理设备 100 连接到不安全的网络时，将比在信息处理设备 100 连接到安全网络的情况下更严格的资源访问条件应用于信息处理设备 100。

将资源访问条件 12 应用于外部显示器连接到信息处理设备 100 的情况。在很多情况下，外部显示器用于进行显示，并且参与者可以通过外部显示器查看出现在信息处理设备 100 的屏幕上的信息。这样，存在由于操作信息处理设备 100 的用户的误操作而造成机密信息意外地出现在屏幕上的风险，并且内容可能泄漏。这样，在资源访问条件 12 中，对于诸如机密信息之类的预定数据，禁止用以浏览数据的函数调用。作为对禁止用以浏览数据的函数调用的替代，也可以禁止用以在屏幕上显示数据的函数调用。

将资源访问条件 19 应用于信息处理设备 100 通过有线网络设备连接到内部网络并且外部介质#1 连接到信息处理设备 100 的情况。由于外部介质#1 连接到信息处理设备 100，所以用户可以很容易地将内部网络中的信息存储到外部介质#1 中并且输出该信息。这样，在资源访问条件 19 中，禁止用以使用外部介质#1 作为存储场所来复制、创建和移动数据以及将数据读入共享存储器的函数调用。

在资源访问条件 19 中，由于外部介质#1 所连接的信息处理设备 100 连接到内部网络，当感染病毒的文件存储在外部介质#1 中时，病毒感染可能扩散到内部网络。这样，作为对资源访问条件 19 的替代或补充，对于在外部介质#1 中的数据，禁止用以复制和移动数据及将数据读入共享存储器的函数调用。

将资源访问条件 21 应用于外部介质#1 连接到信息处理设备 100 的情况。由于外部介质#1 存储不需要作为机密内容来处理的文件、程序等，所以在资源访问条件 21 中，允许所有类型的针对数据访问的函数调用，理由用以浏览、创建、删除、复制和移动数据，将数据读入共享存储器，打印数据，以及激活进程的函数调用。从资源访问条件 1、19 和 21 的对比可以明显看出，在这个实施例中，为多个设备的连接状态或运行状态的每个组合提供了适用的资源访问条件。

将资源访问条件 39 应用于外部介质#2 连接到信息处理设备 100 的情况。外部介质#2 是一种用于处理机密商业信息的特殊设备，该设备包括例如指纹认证功能和内部 VPN 访问程序，并且该外部介质#2 包括机密数据。这样，在资源访问条件 39 中，对于在外部介质#2 中由预定硬件标识信息标识的文件，禁止用以浏览、删除、复制和移动文件的函数调用，并且作为例外，只允许外部介质#2 中的特定程序浏览介质#2 中的文件。这样，在这个实施例中，将不同于外部介质#1 的资源访问条件应用于外部介质#2。

这样，根据连接到信息处理设备 100 的设备的连接状态或运行状态估计信息处理设备 100 的运行环境或运行状态，并且确定应当应用于所估计的运行环境或运行状态的资源访问条件。所确定的资源访问条件不仅存储在从驻留程序 222 和程序 224 都可以访问的例如主存储器之类的共享区域，还可以存储在例如硬盘或磁光盘之类的记录介质的共享区域。

捕获单元 270 捕获由应用程序 210 向 OS 205 发出的针对资源访问的多个函数调用。更特别地，作为对应用程序 210 开始运行的响应，捕获单元270通过将针对资源访问的多个函数调用的调用地址改变成控制模块的地址来捕获由应用程序 210 向 OS 205 发出的针对资源访问的多个函数调用，控制模块实现控制单元 265。这里针对资源访问的多个函数调用包括所有类型的针对资源访问的函数调用，例如用以浏览、复制、创建、删除和移动数据，将数据读入共享存储器，打印数据，以及激活进程的函数调用。在这个实施例中，这些功能由操作系统 205 作为 DLL#1 到#3 215 提供。

确定单元 260 基于从条件存储单元 250 读取的资源访问条件确定是否允许所捕获的函数调用。在资源访问条件中，指定函数调用的类型、数据、进程等，允许或不允许由函数调用进行的数据处理，如参考图 5 所述。这样，确定单元 260 通过将在所捕获的函数调用中调用的函数与资源访问条件中指定的函数进行比较来确定是否允许所捕获的函数调用。

当在资源访问条件中禁止对预定数据的函数调用时，确定单元 260 通过检查所捕获的函数调用的自变量所指定的数据类型来进一步确定是否允许所捕获的函数调用。例如，当禁止进行函数调用的预定数据的类型是机密数据时，确定单元 260 检查在所捕获的函数调用的自变量所指定的数据、数据名称、存储数据的文件夹的名称等等中是否包括诸如“机密”或“保密”之类的特定字符串。

当在资源访问条件中禁止指定预定数据存储场所的函数调用时，确定单元 260 通过检查所捕获的函数调用的自变量所指定的数据存储场所来进一步确定是否允许所捕获的函数调用。例如，当禁止进行函数调用的预定数据存储场所是外部介质时，确定单元 260 获取由所捕获的函数的自变量所指定的存储设备的属性并确定该设备类型是否是可移动设备。

当指定特定的外部介质作为预定数据存储场所时，确定单元 260 进一步获取存储设备的硬件标识消息并确定该硬件标识消息是否匹配于在对应的资源访问条件中指定的硬件标识符，其中该特定的外部介质由例如表明厂家的商家 ID 或产品 ID 之类的预定硬件标识信息标识。在资源访问条件中，当只允许对函数进行调用并且被从预定场所调用的进程执行函数调用时，确定单元 260 进一步获取其中存在调用进程程序模块的设备的类型、硬件标识信息等等，并确定这些信息是否匹配于资源访问条件。

当应用程序 210 已经调用了控制单元 265 时，控制单元 265 调用确定单元 260 并使得确定单元 260 确定是否允许所捕获的函数调用。当确定单元 260 确定不允许对应的数据处理时，控制单元 265 拒绝该函数调用。更特别地，当确定单元 260 确定不允许对应的数据处理时，控制单元 265 向应用程序 210 返回错误代码，而不调用 DLL #1 到#3 215 中的函数。作为替代，控制单元 265 可以仅向应用程序 210 返回空数据。当确定单元 260 确定允许对应的数据处理时，控制单元 265 指定由应用程序 210 指定的自变量，而不用改变和调用 DLL #1 到#3 215 中的函数。作为替代，控制单元 265 可以改变自变量并调用 DLL #1 到#3 215 中的

函数，或者可以在该函数调用之前和/或之后添加不同类型的函数调用。

如上所述，在根据本发明的信息处理设备 100 中，可以基于与信息处理设备100的运行环境或运行状态对应的资源访问条件拒绝或允许通过 OS 的资源访问。

现在将参考图 6 和图 7 中的流程图描述根据本发明的信息处理设备 100 的各个组件的操作。图 6 示出了由驻留程序 222 使其用作注册单元 225、检测单元 230 和选择单元 240 的信息处理设备 100 中的处理的流程示例。在执行图 6 所示出的处理之前，驻留程序 222 在信息处理设备 100 上至少执行一次并且使得信息处理设备 100 用作注册单元 225。特别地，信息处理设备 100 作为预处理而针对从 OS 205 接收到关于设备硬件配置变化的通知来执行注册。然后，在步骤 S600 中，驻留程序 222 和 OS 205 一起被激活，使得该处理开始。

当已经激活驻留程序 222 时，检测单元 230 通过从 OS 205 接收状态变化通知来检测连接到信息处理设备100的设备的连接状态或运行状态的变化（步骤 S610）。然后，检测单元 230 确定检测到的连接状态或运行状态的变化是否是网络设备或外部介质的变化（步骤 S620）。当检测到的连接状态或运行状态的变化是外部介质的变化时，检测单元 230 获取外部介质的硬件标识信息（步骤 S630）。当检测到的连接状态或运行状态的变化是网络设备的变化时，检测单元 230 获取信息处理设备所连接的网络的类型（步骤 S635）。

在步骤 S630 或 S635 之后，或在步骤 S620 的“否”的情况下，处理继续到步骤 S640，其中检测单元 230 用检测到的设备的连接状态或运行状态更新关于存储在状态存储单元235中的设备当前连接状态或运行状态的信息。该处理停留在步骤 S610 直到检测单元 230 执行了检测。

然后，作为对检测单元 230 对状态变化的检测的响应，选择单元 240 基于检测到的设备的连接状态或运行状态选择要应用于信息处理设备 100 的资源访问条件（步骤 S650）。特别地，选择单元 240 参考选择表 245，在该表中多个设备的连接状态或运行状态的每个组合都与应当应用于每个组合的资源访问条件相关联，并且选择单元 240 选择与从状态

存储单元235读取的各个设备当前连接状态或运行状态的组合对应的访问条件。然后，选择单元240将所选择的资源访问条件存储在条件存储单元250中（步骤S660）。

在步骤S660之后，处理回到步骤S610，并且重复前述的一系列步骤。这样，反映信息处理设备100的当前运行环境或运行状态的适当访问条件一直存储在条件存储单元250中。

图7示出了由程序224使其用作捕获单元270、确定单元260和控制单元265的信息处理设备100中的处理的流程示例。程序224至少需要在可以发出针对数据访问的函数调用的应用程序210被激活时运行，并且并非一定要与OS 205一起被激活，这与驻留程序222不同。在这个实施例中，程序224和可以发出针对数据访问的函数调用的应用程序210一起被激活。

为了同时激活程序224和应用程序210，将包括捕获模块、确定模块和控制模块的程序24的对象文件（例如DLL）注册为操作系统的标准DLL。例如，在Windows（商标）中，当这些程序在注册表中被作为USER32扩展DLL注册时，这些程序可以在启动链接到USER32.DLL的所有进程时被激活。

在步骤S700中，在激活程序224时，处理开始。作为对应用程序210开始运行的响应，捕获单元270通过将调用地址改变成控制模块的地址来捕获由应用程序210向OS 205发出的针对数据访问的多个函数调用，控制模块实现控制单元265（步骤S710）。

更特别地，捕获单元270在另一个区域备份DLL #1到#3 215中一些部分的首指令代码（leading instruction code），这些部分是从应用程序210调用的。然后，捕获单元270用去往控制模块的跳转指令取代这些指令代码，控制模块实现控制单元265。捕获单元270进一步使控制单元265调用备份的首指令代码，而不是从控制单元265调用DLL #1到#3 215。

当从应用程序210接收到调用时（步骤S720），控制单元265调用确定单元260并使得确定单元260确定是否允许所捕获的函数调用。作

为对来自控制单元265的调用的响应，确定单元260从条件存储单元250读取资源访问条件（步骤S730）。然后，确定单元260首先确定在资源访问条件中不允许的任意函数是否匹配于在所捕获的函数调用中调用的函数（步骤S740）。

当在资源访问条件中不允许在所捕获的函数调用中调用的函数时（步骤S740：是），确定单元260确定在资源访问条件中是否禁止针对预定数据进行的函数调用（步骤S750）。当在资源访问条件中禁止针对预定数据进行的函数调用时，确定单元260确定所捕获的函数调用的自变量指定的数据类型是否与资源访问条件中指定的预定数据对应（步骤S760）。

当所捕获的函数调用是针对资源访问条件中指定的预定数据进行的时（步骤S760：是）或在步骤S750中“否”的情况下，确定单元260进一步确定在资源访问条件中是否禁止指定预定存储场所的函数调用（步骤S770）。当在资源访问条件中禁止指定预定存储场所的函数调用时，确定单元260确定由所捕获的函数调用的自变量指定的数据存储场所是否为资源访问条件中指定的预定存储场所（步骤S775）。

当所捕获的函数调用指定在资源访问条件中指定的预定存储场所时（步骤S775：是）或在步骤S770中“否”的情况下，确定单元260进一步确定在资源访问条件中是否只允许对函数进行调用并且被从特定场所调用的进程执行函数调用（步骤S780）。当在访问条件中只允许对函数进行调用并且被从特定场所调用的进程执行函数调用时，确定单元260获取设备的类型、硬件标识信息等，并确定该设备是否为访问条件中指定的用于激活进程的特定场所，其中在该设备中进程的一个程序模块调用该函数（步骤S785）。

当调用该函数的进程进行调用的场所不是在访问条件中指定的特定场所时（步骤S785：否）或在步骤S780中“否”的情况下，确定单元260返回不允许所捕获的函数调用的确定结果到控制单元265。作为对确定单元260所得到的不允许所捕获的函数调用的确定结果的响应，控制单元265拒绝所捕获的函数调用（步骤S790）。另一方面，在步骤

S740、S760 或 S775 中“否”的情况下或在步骤 S785 中“是”的情况下，确定单元 260 返回允许所捕获的函数调用的确定结果到控制单元 265。作为对确定单元 260 所得到的允许所捕获的函数调用的确定结果的响应，控制单元 265 继续进行所捕获的函数调用（步骤 S795）。

尽管已经通过实施例对本发明进行了描述，但本发明的技术范围不限于在前述实施例中所描述的范围。本领域的普通技术人员很容易想到可以在前述实施例中进行各种改变和改进。因此，显然，经改变或改进的实施例同样被本发明的技术范围所覆盖。

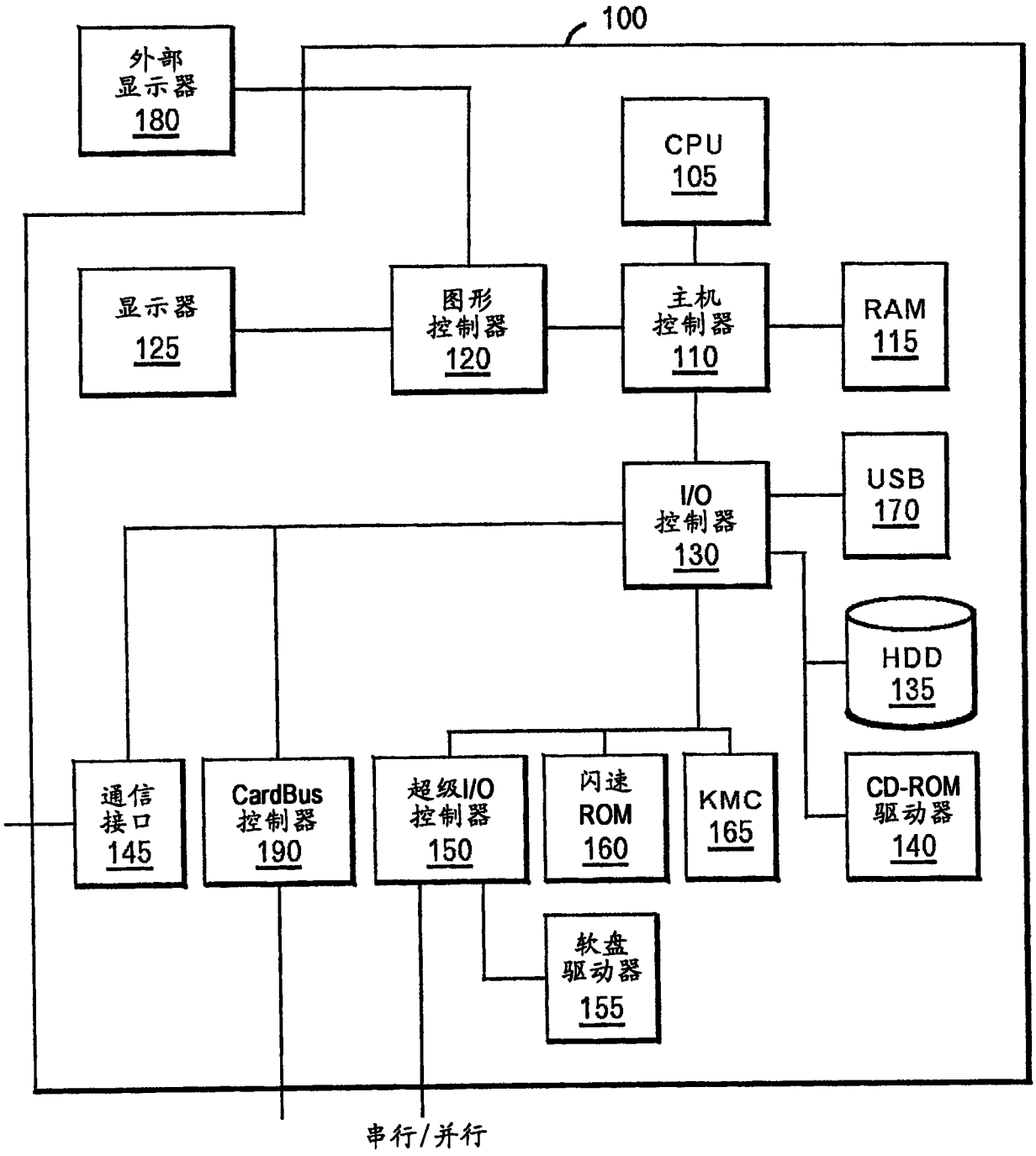

100
外部
显示器
180
CPU
105
显示器
125
图形
控制器
120
主机
控制器
110
RAM
115
USB
170
I/O
控制器
130
HDD
135
通信
接口
145
CardBus
控制器
190
超级I/O
控制器
150
闪速
ROM
160
KMC
165
CD-ROM
驱动器
140
软盘
驱动器
155
串行/并行

图1

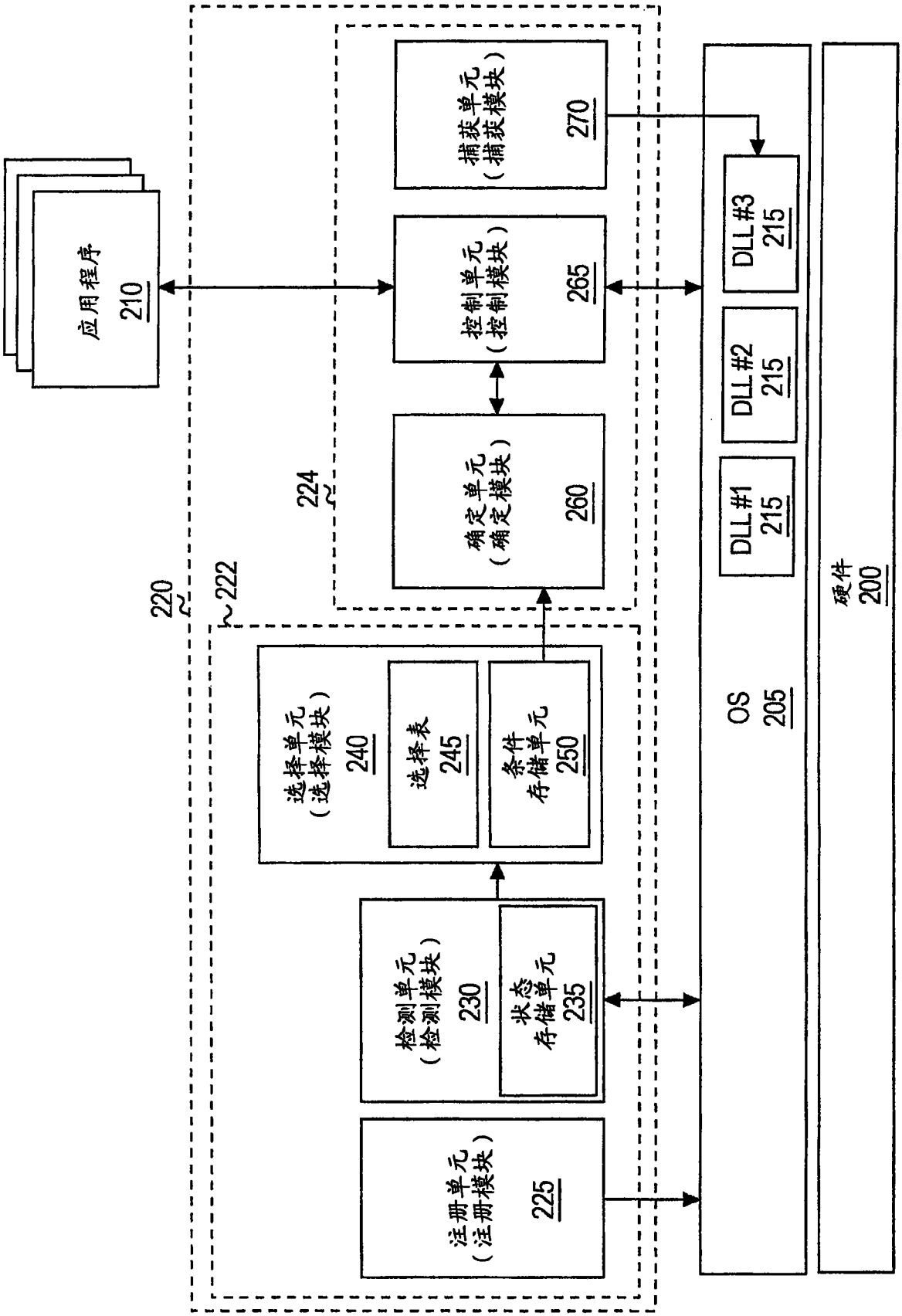

应用程序
210
220
222
224
捕获单元
(捕获模块)
270
控制单元
(控制模块)
265
确定单元
(确定模块)
260
选择单元
(选择模块)
240
选择表
245
条件
存储单元
250
检测单元
(检测模块)
230
状态
存储单元
235
注册单元
(注册模块)
225
DLL #1
215
DLL #2
215
DLL #3
215
OS
205
硬件
200

图2

a)

比特	设备
第7比特	外部介质 # 3
第6比特	外部介质 # 2
第5比特	外部介质 # 1
第4比特	外部显示器
第2和第3比特	无线网络设备
第0和第1比特	有线网络设备

b)

有线/无线网络设备		
值		含义
1	0	内部
0	1	外部
0	0	未使用

c)

其他设备	
值	含义
0	未连接
1	已连接

图 3

	条件1	条件2	条件3	条件4	...	条件71	条件72
有线网络设备	内部	外部	未使用	内部	...	外部	未使用
无线网络设备	未使用	未使用	未使用	内部	...	外部	外部
外部显示器	未连接	未连接	未连接	未连接	...	已连接	已连接
外部介质1	未连接	未连接	未连接	未连接	...	已连接	已连接
外部介质2	未连接	未连接	未连接	未连接	...	已连接	已连接

图4

资源访问条件1 （内部有线连接）	允许所有类型的针对数据访问的函数调用
...	...
资源访问条件6 （内部无线连接）	对于预定数据，禁止 用以复制、删除和移动数据，将数据读入共享 存储器，打印数据，以及激活进程的函数调用
...	...
资源访问条件9 （外部无线连接）	对于预定数据，禁止所有 类型的针对数据访问的函数调用
...	...
资源访问条件12 （外部显示器连接）	对于预定数据，禁止用以浏览数据的函数调用
...	...
资源访问条件19 （外部介质#1 连接＋内部优先级连接）	禁止用以使用外部介质#1作为 存储场所来复制、删除和移动数据以及将 数据读入共享存储器的函数调用，和/或对于 外部介质#1中的数据，禁止用以复制和移动 数据以及将数据读入共享存储器的函数调用
...	...
资源访问条件21 （外部介质#1 连接）	允许所有类型的针对数据访问的函数调用
...	...
资源访问条件39 （外部介质#2 连接）	只允许外部介质#2中的 特定程序浏览介质#2中的文件
...	...

图5

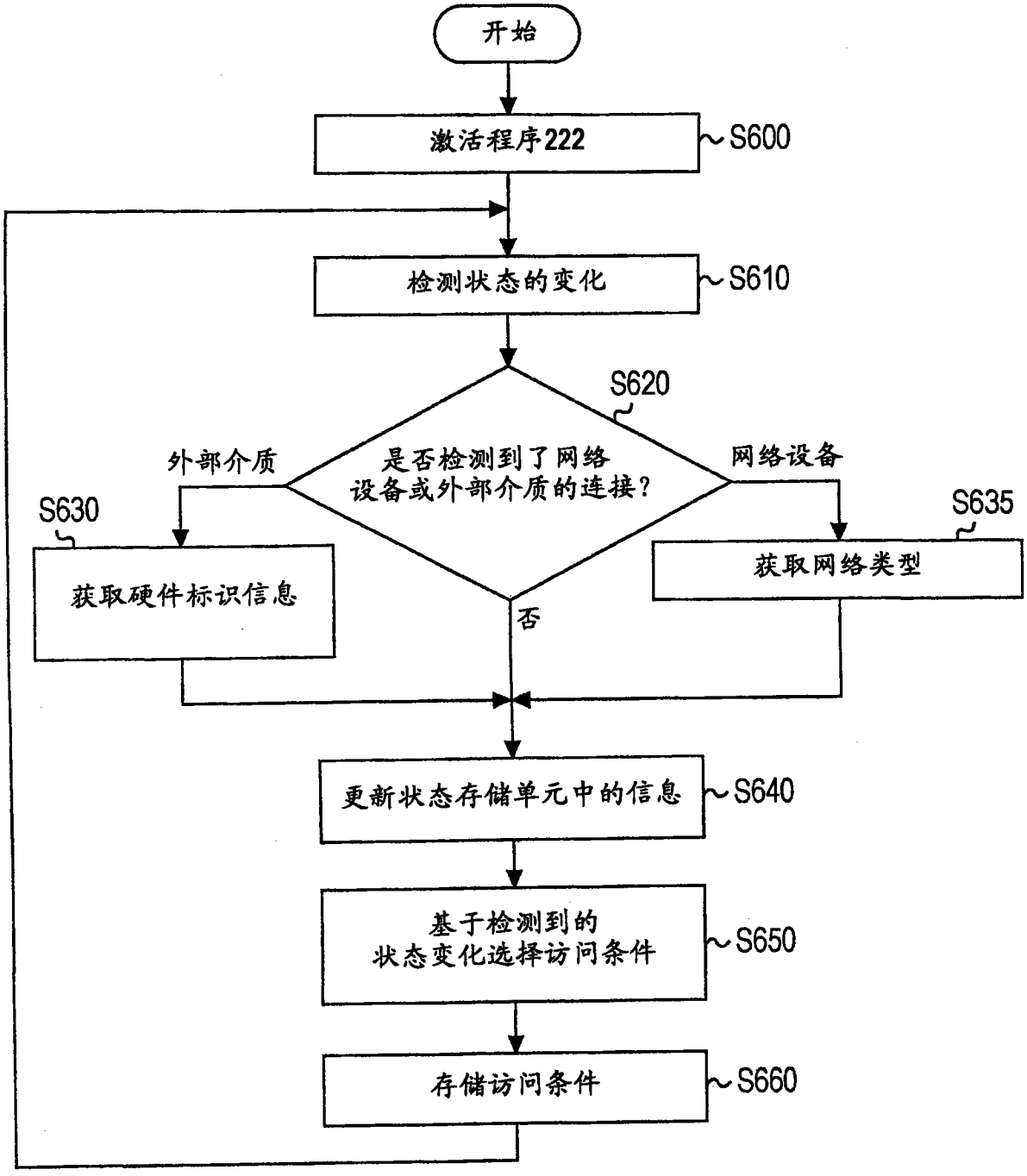

开始
激活程序222
S600
检测状态的变化
S610
S620
是否检测到了网络设备或外部介质的连接？
外部介质
网络设备
否
S630
获取硬件标识信息
S635
获取网络类型
更新状态存储单元中的信息
S640
基于检测到的状态变化选择访问条件
S650
存储访问条件
S660

图6

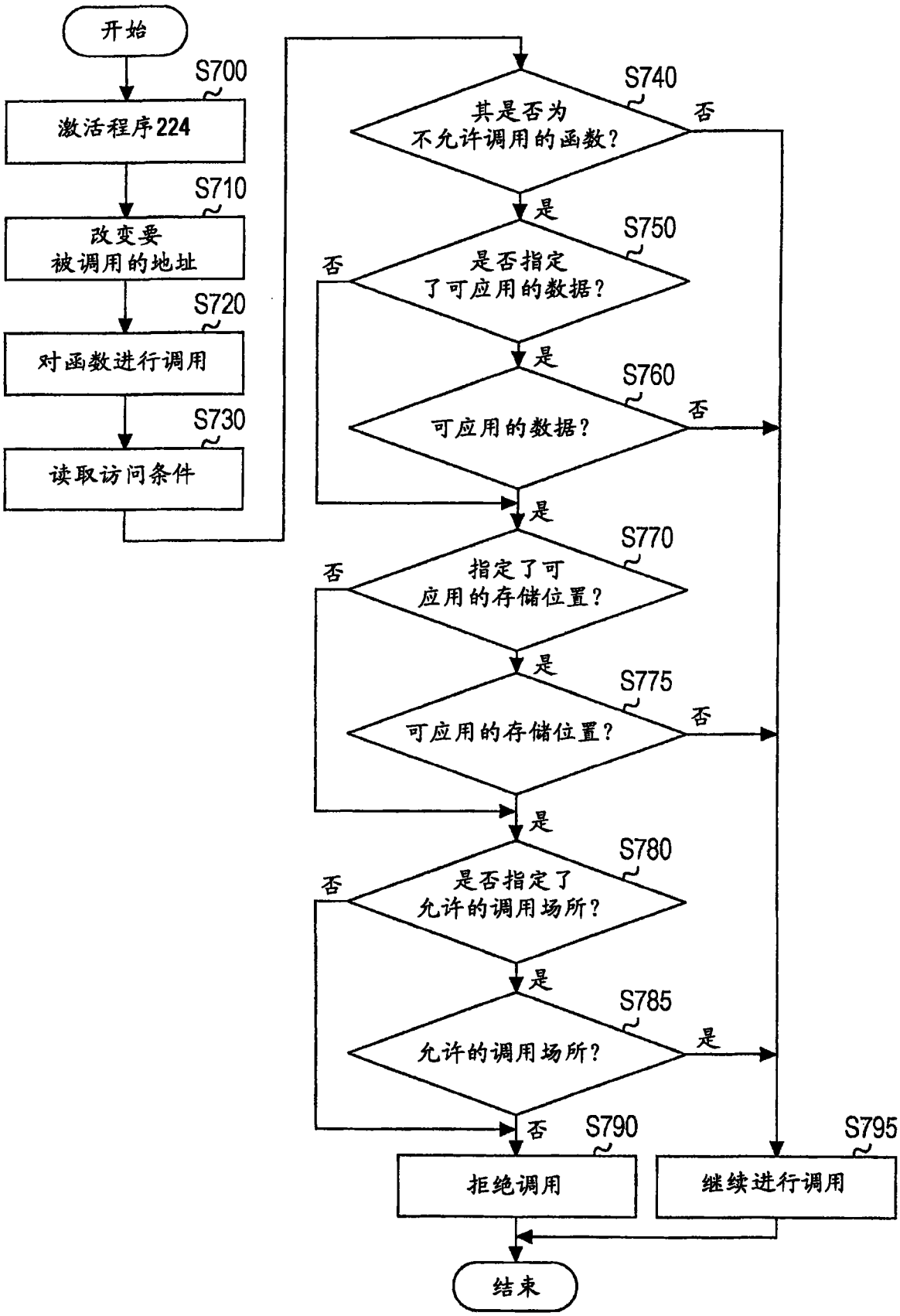

开始
S700
激活程序224
S710
改变要被调用的地址
S720
对函数进行调用
S730
读取访问条件
S740
其是否为不允许调用的函数?
否
是
S750
是否指定了可应用的数据?
否
是
S760
可应用的数据?
否
是
S770
指定了可应用的存储位置?
否
是
S775
可应用的存储位置?
否
是
S780
是否指定了允许的调用场所?
否
是
S785
允许的调用场所?
是
否
S790
拒绝调用
S795
继续进行调用
结束

图7