[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 17/30 (2006.01)
G06F 1/00 (2006.01)

[12] 发明专利说明书

专利号 ZL 200510118057.2

[45] 授权公告日 2009 年 12 月 16 日

[11] 授权公告号 CN 100570601C

[22] 申请日 2005.10.26
[21] 申请号 200510118057.2
[30] 优先权
[32] 2004.10.28 [33] JP [31] 2004 - 314070
[73] 专利权人 日本电气株式会社
地址 日本东京都
[72] 发明人 细川正广 矢野尾一男
[56] 参考文献
FR2800480A1 2001.5.4
WO03/100582A2 2003.12.4
CN1535411A 2004.10.6
US2004/0187027A1 2004.9.23
CN1307283A 2001.8.8
TW507135A 2002.10.21
CN1536807A 2004.10.13
审查员 董 刚
[74] 专利代理机构 中科专利商标代理有限责任公司
代理人 朱进桂

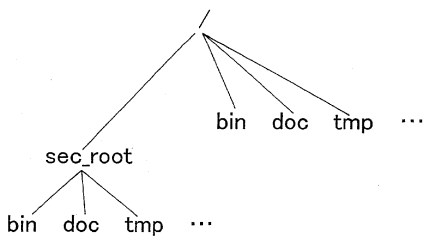
权利要求书 7 页 说明书 11 页 附图 5 页

[54] 发明名称

基于秘密模式来切换要访问的文件夹的方法及计算机系统

[57] 摘要

公开了一种根据秘密模式切换访问文件夹的方法。在该方法中，秘密根目录位于常规根目录之下。由秘密根目录之外的至少一个秘密文件夹构成的目录结构与由常规根目录之外的至少一个常规文件夹构成的目录结构相同。从应用程序接收到对盘设备的文件访问请求。如果应用程序运行为秘密模式的进程，则通过将指定文件路径名重写为与秘密根目录下的秘密文件夹相对应的文件路径名，通过内核来对秘密文件夹中的秘密文件执行文件访问。如果应用程序运行为常规模式的进程，则不允许对秘密文件夹中的秘密文件进行文件访问。



1、 一种在计算机中使用的用于基于秘密模式来切换要访问的文件夹的方法，所述计算机执行内核以及作为进程的应用程序，所述内核具有用于控制对盘设备的文件访问的文件系统，所述应用程序通过所述文件系统对盘设备执行文件访问，所述进程被启动为能够处理秘密信息的秘密模式的进程或者被启动为不能处理秘密信息的常规模式的进程，所述方法包括：

在盘设备中如下设置目录结构的步骤：

秘密根目录位于常规根目录之下；

至少一个常规文件夹按照目录结构位于所述常规根目录之下，并且被配置为存储由非秘密信息构成的常规文件；

至少一个秘密文件夹按照目录结构位于所述秘密根目录之下，并且被配置为存储由秘密信息构成的秘密文件；并且

由除了所述秘密根目录以外的所述至少一个秘密文件夹构成的目录结构与由除了所述常规根目录以外的所述至少一个常规文件夹构成的目录结构相同；

在所述计算机启动所述应用程序时，指定安全级别的步骤，其中所述安全级别表示所述应用程序应该运行为能够处理所述秘密文件的秘密模式的进程还是不能处理所述秘密文件的常规模式的进程；

当从所述应用程序接收到以指定文件路径名、对所述盘设备进行文件访问的文件访问请求时，基于所指定的安全级别，确定所述应用程序是运行为所述秘密模式的进程还是运行为所述常规模式的进程的步骤；

如果所述应用程序运行为所述秘密模式的进程，则进行重写及允许步骤：将所述指定文件路径名重写为所述秘密根目录下的所述秘密文件夹中的相应秘密文件的文件路径名，并且允许通过所述内核对由所述文件路径名指定的所述秘密文件夹中的所述秘密文件执行文件访问；以及

如果所述应用程序运行为所述常规模式的进程，则不允许对所述秘密文件夹中的所述秘密文件进行文件访问的步骤。

2、 根据权利要求 1 所述的方法，其中

所述重写及允许步骤包括

如果所述应用程序运行为所述秘密模式的进程，则通过向所述指定文件路径名的头部加入所述秘密根目录名，将所述指定文件路径名重写为所述秘密根目录下的所述秘密文件夹中的相应秘密文件的文件路径名的步骤。

3、 根据权利要求 1 所述的方法，其中

所述重写及允许步骤包括：

确定所述文件访问请求是否是写指令的步骤；

如果所述文件访问请求是写指令，则允许通过所述内核对所述秘密文件夹中的所述秘密文件执行写入的步骤；

如果所述文件访问请求不是写指令，则确定与所述文件路径名相对应的文件是否存在的步骤，其中所述文件路径名是通过向所述指定文件路径名的头部加入所述秘密根目录名写出的；

如果所述文件存在，则通过向所述指定文件路径名的头部加入所述秘密根目录名，将所述指定文件路径名重写为所述秘密根目录下的所述秘密文件夹中的相应秘密文件的所述文件路径名，并且允许通过所述内核对由所述文件路径名指定的所述秘密文件夹中的所述秘密文件执行除了写入之外的其他文件访问的步骤；以及

如果所述文件不存在，则允许通过所述内核对与所述指定文件路径名相对应的所述常规文件夹中的所述常规文件执行文件读取访问的步骤。

4、 根据权利要求 1 所述的方法，其中

所述重写及允许步骤包括：

如果所述应用程序运行为所述秘密模式的进程，则为每个应用程序维护能够输出到所述常规文件夹的例外文件的列表，并且预先将所述应用程序所特有的配置文件的路径名设置为所述列

表中维护的所述例外文件的步骤；以及

如果所述秘密文件是所述例外文件，则基于所述列表中的所述配置文件的路径名，允许通过所述内核对与所述常规文件夹中的所述例外文件相对应的所述配置文件执行文件访问的步骤。

5、 一种在计算机中使用的用于基于秘密模式来切换要访问的文件夹的方法，所述计算机执行内核以及作为进程的应用程序，所述内核具有用于控制对盘设备的文件访问的文件系统，所述应用程序通过所述文件系统对盘设备执行文件访问，所述进程被启动为能够处理秘密信息的秘密模式的进程或者被启动为不能处理秘密信息的常规模式的进程，所述方法包括：

在盘设备中如下设置目录结构的步骤：

秘密根目录位于常规根目录之下；

至少一个常规文件夹按照目录结构位于所述常规根目录之下，并且被配置为存储由非秘密信息构成的常规文件；

至少一个秘密文件夹按照目录结构位于所述秘密根目录之下，并且被配置为存储由秘密信息构成的秘密文件；并且

由除了所述秘密根目录以外的所述至少一个秘密文件夹构成的目录结构与由除了所述常规根目录以外的所述至少一个常规文件夹构成的目录结构相同；

在所述计算机启动所述应用程序时，指定安全级别的步骤，其中所述安全级别表示所述应用程序应该运行为能够处理所述秘密文件的秘密模式的进程还是不能处理所述秘密文件的常规模式的进程；

当从所述应用程序接收到以指定文件路径名、对所述盘设备进行文件访问的文件访问请求时，基于所指定的安全级别，确定所述应用程序是运行为所述秘密模式的进程还是运行为所述常规模式的进程的步骤；

如果所述应用程序运行为所述秘密模式的进程并且所述指定文件路径名是所述秘密根目录下的所述秘密文件夹中的相应秘密文件的文件路径名，则进行允许步骤：允许通过所述内核对所述秘密文件夹中的所述秘密文件执行文件访问；以及

如果所述应用程序运行为所述常规模式的进程，则不允许对所述秘密文件夹中的所述秘密文件进行文件访问的步骤。

6、 根据权利要求5所述的方法，其中

所述允许步骤包括：

如果所述应用程序运行为所述秘密模式的进程，则为每个应用程序维护能够输出到所述常规文件夹的例外文件的列表，并且预先将所述应用程序所特有的配置文件的路径名设置为所述列表中维护的所述例外文件的步骤；以及

如果所述指定文件路径名所表示的文件对应于所述例外文件，则允许通过所述内核对与所述常规文件夹中的所述例外文件相对应的所述配置文件执行文件访问的步骤。

7、 一种用于基于秘密模式来切换要访问的文件夹的计算机系统，所述计算机系统执行内核以及作为进程的应用程序，所述内核具有用于控制对盘设备的文件访问的文件系统，所述应用程序通过所述文件系统对盘设备执行文件访问，所述进程被启动为能够处理秘密信息的秘密模式的进程或者被启动为不能处理秘密信息的常规模式的进程，所述计算机系统包括：

用于在盘设备中如下设置目录结构的装置：

秘密根目录位于常规根目录之下；

至少一个常规文件夹按照目录结构位于所述常规根目录之下，并且被配置为存储由非秘密信息构成的常规文件；

至少一个秘密文件夹按照目录结构位于所述秘密根目录之下，并且被配置为存储由秘密信息构成的秘密文件；并且

由除了所述秘密根目录以外的所述至少一个秘密文件夹构成的目录结构与由除了所述常规根目录以外的所述至少一个常规文件夹构成的目录结构相同；

用于在所述计算机启动所述应用程序时，指定安全级别的装置，其中所述安全级别表示所述应用程序应该运行为能够处理所述秘密文件的秘密模式的进程还是不能处理所述秘密文件的常规模式的进程；

用于在从所述应用程序接收到以指定文件路径名、对所述盘设备

进行文件访问的文件访问请求时，基于所指定的安全级别，确定所述应用程序是运行为所述秘密模式的进程还是运行为所述常规模式的进程的装置；

重写及允许装置，用于如果所述应用程序运行为所述秘密模式的进程，将所述指定文件路径名重写为所述秘密根目录下的所述秘密文件夹中的相应秘密文件的文件路径名，并且允许通过所述内核对由所述文件路径名指定的所述秘密文件夹中的所述秘密文件执行文件访问；以及

用于如果所述应用程序运行为所述常规模式的进程，则不允许对所述秘密文件夹中的所述秘密文件进行文件访问的装置。

8、 根据权利要求 7 所述的计算机系统，其中

所述重写及允许装置包括

用于如果所述应用程序运行为所述秘密模式的进程，则通过向所述指定文件路径名的头部加入所述秘密根目录名，将所述指定文件路径名重写为所述秘密根目录下的所述秘密文件夹中的相应秘密文件的文件路径名的装置。

9、 根据权利要求 7 所述的计算机系统，其中

所述重写及允许装置包括：

用于确定所述文件访问请求是否是写指令的装置；

用于如果所述文件访问请求是写指令，则允许通过所述内核对所述秘密文件夹中的所述秘密文件执行写入的装置；

用于如果所述文件访问请求不是写指令，则确定与所述文件路径名相对应的文件是否存在的装置，其中所述文件路径名是通过向所述指定文件路径名的头部加入所述秘密根目录名写出的；

用于如果所述文件存在，则通过向所述指定文件路径名的头部加入所述秘密根目录名，将所述指定文件路径名重写为所述秘密根目录下的所述秘密文件夹中的相应秘密文件的所述文件路径名，并且允许通过所述内核对由所述文件路径名指定的所述秘密文件夹中的所述秘密文件执行除了写入之外的其他文件访问的装置；以及

用于如果所述文件不存在，则允许通过所述内核对与所述指定文件路径名相对应的所述常规文件夹中的所述常规文件执行文件读取访问的装置。

10、 根据权利要求 7 所述的计算机系统，其中

所述重写及允许装置包括：

用于如果所述应用程序运行为所述秘密模式的进程，则为每个应用程序维护能够输出到所述常规文件夹的例外文件的列表，并且预先将所述应用程序所特有的配置文件的路径名设置为所述列表中维护的所述例外文件的装置；以及

用于如果所述秘密文件是所述例外文件，则基于所述列表中的所述配置文件的路径名，允许通过所述内核对与所述常规文件夹中的所述例外文件相对应的所述配置文件执行文件访问的装置。

11、 一种用于基于秘密模式来切换要访问的文件夹的计算机系统，所述计算机系统执行内核以及作为进程的应用程序，所述内核具有用于控制对盘设备的文件访问的文件系统，所述应用程序通过所述文件系统对盘设备执行文件访问，所述进程被启动为能够处理秘密信息的秘密模式的进程或者被启动为不能处理秘密信息的常规模式的进程，所述计算机系统包括：

用于在盘设备中如下设置目录结构的装置：

秘密根目录位于常规根目录之下；

至少一个常规文件夹按照目录结构位于所述常规根目录之下，并且被配置为存储由非秘密信息构成的常规文件；

至少一个秘密文件夹按照目录结构位于所述秘密根目录之下，并且被配置为存储由秘密信息构成的秘密文件；并且

由除了所述秘密根目录以外的所述至少一个秘密文件夹构成的目录结构与由除了所述常规根目录以外的所述至少一个常规文件夹构成的目录结构相同；

用于在所述计算机启动所述应用程序时，指定安全级别的装置，其中所述安全级别表示所述应用程序应该运行为能够处理所述秘密文

件的秘密模式的进程还是不能处理所述秘密文件的常规模式的进程；

用于在从所述应用程序接收到以指定文件路径名、对所述盘设备进行文件访问的文件访问请求时，基于所指定的安全级别，确定所述应用程序是运行为所述秘密模式的进程还是运行为所述常规模式的进程的装置；

允许装置，用于如果所述应用程序运行为所述秘密模式的进程并且所述指定文件路径名是所述秘密根目录下的所述秘密文件夹中的相应秘密文件的文件路径名，则允许通过所述内核对所述秘密文件夹中的所述秘密文件执行文件访问；以及

用于如果所述应用程序运行为所述常规模式的进程，则不允许对所述秘密文件夹中的所述秘密文件进行文件访问的装置。

12、 根据权利要求 11 所述的计算机系统，其中

所述允许装置包括：

用于如果所述应用程序运行为所述秘密模式的进程，则为每个应用程序维护能够输出到所述常规文件夹的例外文件的列表，并且预先将所述应用程序所特有的配置文件的路径名设置为所述列表中维护的所述例外文件的装置；以及

用于如果所述指定文件路径名所表示的文件对应于所述例外文件，则允许通过所述内核对与所述常规文件夹中的所述例外文件相对应的所述配置文件执行文件访问的装置。

基于秘密模式来切换要访问的文件夹的方法及计算机系统

技术领域

本发明涉及用于基于秘密模式来切换要访问的文件夹的方法、程序、以及计算机系统，更具体地说，涉及一种根据安全级别的文件访问控制方案。

背景技术

在传统的文件访问控制方法中，已经知道了一种加强对计算机中文件等的访问控制的方案。在这种方案中，预先向诸如文件之类的访问对象（客体）以及诸如用户进程之类的访问主体（主体）分别分配“秘密”和“常规”的安全级别。通过比较主体和客体的安全级别，来确定从主题对客体的可访问性。这种方案通常被称作“多级安全（MLS）”。

这种 MLS 的概念作为强制访问控制（MAC）在实践中已经被引入了例如作为具有加强的安全功能的 OS（操作系统）而受到注目的各种“安全 OS”中。在这种强制访问控制之下，用户进程不能对安全级别比用户进程低的文件执行写入（这称作“NWD 原则：禁止下写原则”），并且相反，不能读取安全级别比用户进程高的文件（这称作“NRU 原则：禁止上读原则”）。以这种方式，严格防止了高安全级别的信息被传送到只有低安全级别的用户。还经常使用这样一种原则来代替 NWD 原则:用户进程只可以在与用户进程自身相同的安全级别上执行写入。结果，可以防止对无意的安全级别进行提升，但是牺牲了灵活性。

关于上述根据安全级别来实现文件访问控制的方案，存在如下两种公知的实现方案。

（第一传统技术）

在一种公知方案中，每个文件具有关于安全级别的属性信息。在

I/O（输入/输出）文件时，将属性信息与当前运行的进程的安全级别进行比较。结果，如果访问不满足 NWD 原则或 NRU 原则，则阻断对文件的访问。这使用专门创建的专用文件系统来完成。如果访问安全级别比进程的安全级别低的文件，则文件的安全级别被提升到与进程相同的安全级别。

（第二传统技术）

在 SUN MICROSYSTEM, Inc.所制造的安全 Solaris（商业名称）中实现了另一方案。在这种方案中，包括两种特殊目录，即，多级目录（MLD）和单级目录（SLD），以对应于秘密模式。MLD 是允许多个 SLD 直接位于其下的特殊目录。SLD 是与具体安全级别一一对应的特殊目录。通过组合这些特殊目录，用户可看到的目录可以与用户的安全级别相匹配。

涉及上述方案的传统技术文档包括：JP-A-2002-288030、JP-A-2004-126634、JP-A-1996-249238、以及 JP-A-1998-312335。

如上所述，通过为每个文件提供关于安全级别的属性来管理文件的技术（第一传统技术）以及对被分为多个安全级别的目录进行排列的另一技术（第二传统技术）是实施 MLS 的传统技术。这些技术中每一种都采用增强现有文件系统的方法。因此，出现了下列问题。

第一个问题是用户难以在一个应用（AP）中同时操作位于常规模式和秘密模式的进程。这是因为，在第一传统技术中，如果两个 AP 都输出相同的临时文件，则安全级别彼此冲突，因此，应用不能同时共存。这导致了对 AP 操作的限制。

第二个问题是在常规模式和秘密模式中不可避免地必须使用不同的配置文件。因此，用户被操作环境的模式之间的设置区别搞糊涂。这是因为，在第一传统技术中，如果在秘密模式中更新配置文件，则提升了该文件的安全级别，并且不能从常规级别的进程对其进行读取。另一方面，在第二传统技术中，在其中要放置配置文件的目录位于不同的单级目录中。

第三个问题是与现有文件系统不兼容。因此，难以移植基于如下假设而创建的应用：存在由现有文件系统管理的访问权限管理。这是

因为，通过为每个文件提供增强的属性信息或通过提供唯一的目录属性，增强了文件系统。

发明内容

本发明的目的是，在基于安全级别的文件访问控制方案中，对于一个应用，允许用户在同时操作处于常规模式和秘密模式的进程时工作。

本发明的另一目的是克服操作环境的模式之间的设置差别使用户造成混淆的情形。

另外，本发明的另一目的是能够在以存在由现有文件系统管理的访问权限管理的假设为基础而创建的应用中进行操作。

为了达到上述目的，在本发明中，能够处理秘密信息的进程与不能处理秘密信息的进程彼此分离。只从能够处理秘密信息的进程构建可访问的文件夹。秘密信息文件对常规进程是隐藏的。另外，从处理秘密信息的进程能够透明地访问秘密信息和非秘密信息。例如，如果从任意应用程序发出了文件访问请求，并且如果该应用程序是秘密进程，则请求访问的文件的路径被文件路径重写函数用预定秘密文件夹下的文件名代替，并将此通知给内核。否则，如果应用程序是不能处理秘密文件的常规进程，则切换访问文件夹，从而防止对秘密文件夹下的文件进行文件访问。结果，可以利用现有文件系统来强制执行与安全级别相对应的文件访问。

本发明是在上述概念的基础上完成的。

根据本发明，提供了一种在计算机中使用的用于基于秘密模式来切换要访问的文件夹的方法。计算机执行内核以及作为进程的应用程序。内核具有用于控制对盘设备的文件访问的文件系统。应用程序通过文件系统对盘设备执行文件访问。该方法包括：在盘设备中如下设置目录结构的步骤：秘密根目录位于常规根目录之下；至少一个常规文件夹分层次地位于常规根目录之下，并且被配置为存储由非秘密信息构成的常规文件；至少一个秘密文件夹分层次地位于秘密根目录之下，并且被配置为存储由秘密信息构成的秘密文件；并且由秘密根目

录之外的所述至少一个秘密文件夹构成的目录结构与由常规根目录之外的所述至少一个常规文件夹构成的目录结构相同；在计算机启动应用程序时，指定功能级别的步骤，其中所述功能级别表示应用程序应该运行为能够处理秘密文件的秘密模式的进程还是不能处理秘密文件的常规模式的进程；当从应用程序接收到以指定文件路径名、对盘设备进行文件访问的文件访问请求时，基于所指定的功能级别，确定应用程序是运行为秘密模式的进程还是运行为常规模式的进程的步骤；如果应用程序运行为秘密模式的进程，则将指定文件路径名重写为与秘密根目录下的秘密文件夹相对应的文件路径名，并且允许通过内核对由所述文件路径名指定的秘密文件夹中的秘密文件执行文件访问的步骤；以及如果应用程序运行为常规模式的进程，则不允许对秘密文件夹中的秘密文件进行文件访问的步骤。

根据本发明，提供了一种程序，用于使计算机执行用于基于秘密模式来切换要访问的文件夹的方法。计算机执行内核以及作为进程的应用程序。内核具有用于控制对盘设备的文件访问的文件系统。应用程序通过文件系统对盘设备执行文件访问。该方法包括：在盘设备中如下设置目录结构的步骤：秘密根目录位于常规根目录之下；至少一个常规文件夹分层次地位于常规根目录之下，并且被配置为存储由非秘密信息构成的常规文件；至少一个秘密文件夹分层次地位于秘密根目录之下，并且被配置为存储由秘密信息构成的秘密文件；并且由秘密根目录之外的所述至少一个秘密文件夹构成的目录结构与由常规根目录之外的所述至少一个常规文件夹构成的目录结构相同；在计算机启动应用程序时，指定功能级别的步骤，其中所述功能级别表示应用程序应该运行为能够处理秘密文件的秘密模式的进程还是不能处理秘密文件的常规模式的进程；当从应用程序接收到以指定文件路径名、对盘设备进行文件访问的文件访问请求时，基于所指定的功能级别，确定应用程序是运行为秘密模式的进程还是运行为常规模式的进程的步骤；如果应用程序运行为秘密模式的进程，则将指定文件路径名重写为与秘密根目录下的秘密文件夹相对应的文件路径名，并且允许通过内核对由所述文件路径名指定的秘密文件夹中的秘密文件执行文件

访问的步骤；以及如果应用程序运行为常规模式的进程，则不允许对秘密文件夹中的秘密文件进行文件访问的步骤。

根据本发明，提供了一种用于基于秘密模式来切换要访问的文件夹的计算机系统。计算机系统执行内核以及作为进程的应用程序。内核具有用于控制对盘设备的文件访问的文件系统。应用程序通过文件系统对盘设备执行文件访问。该计算机系统包括：装置，用于在盘设备中如下设置目录结构：秘密根目录位于常规根目录之下；至少一个常规文件夹分层次地位于常规根目录之下，并且被配置为存储由非秘密信息构成的常规文件；至少一个秘密文件夹分层次地位于秘密根目录之下，并且被配置为存储由秘密信息构成的秘密文件；并且由秘密根目录之外的所述至少一个秘密文件夹构成的目录结构与由常规根目录之外的所述至少一个常规文件夹构成的目录结构相同；装置，用于在计算机启动应用程序时，指定功能级别，其中所述功能级别表示应用程序应该运行为能够处理所述秘密文件的秘密模式的进程还是不能处理所述秘密文件的常规模式的进程；装置，用于在从应用程序接收到以指定文件路径名、对盘设备进行文件访问的文件访问请求时，基于所指定的功能级别，确定应用程序是运行为秘密模式的进程还是运行为常规模式的进程；装置，用于如果应用程序运行为秘密模式的进程，则将指定文件路径名重写为与秘密根目录下的秘密文件夹相对应的文件路径名，并且允许通过内核对由所述文件路径名指定的秘密文件夹中的秘密文件执行文件访问；以及装置，用于如果应用程序运行为常规模式的进程，则不允许对秘密文件夹中的秘密文件进行文件访问。

根据本发明，可以利用现有文件系统来强制地执行根据安全级别的文件访问。因此，用户可以在同时操作处于常规模式和秘密模式的进程时工作。另外，可以克服操作环境之间的设置差别使用户造成混淆的情形。另外，即使应用程序是在存在由现有文件系统管理的访问权限管理的前提下创建的，也可以运行而不需要改变。

附图说明

在附图中：

图 1 是示出了根据本发明第一实施例的计算机系统的整体结构的图；

图 2 是解释图 1 所示的文件路径重写函数的操作的流程图；

图 3 是解释盘设备中目录结构的树状图；

图 4 是示出了根据本发明第二实施例的计算机系统的整体结构的图；

图 5 是解释图 4 所示的文件访问强制函数的操作的流程图。

具体实施方式

现在参考附图，以最优方式来描述根据本发明的用于基于安全级别来切换要访问的文件夹的方法、程序、以及计算机系统的优选实施例。

（第一实施例）

图 1 是示出了根据本实施例的计算机系统的整体结构的图。

参考图 1，根据本实施例的计算机系统包括：CPU（中央处理单元）2，其执行预先设置的软件（程序）1 以实现软件 1 的功能；以及盘设备 103（例如硬盘驱动设备），其通过总线电连接到 CPU 2（但是在图 1 所示的示例中省略了盘设备 103 之外的其他输入/输出（I/O）设备）。

软件 1 包括：应用程序（后文简称为“应用”）101；内核 10，其具有控制对盘设备 103 的各种文件访问的文件系统 102；并且在本实施例中还具有文件路径重写函数 104 以及 AP（应用）启动检测函数 105。这里所使用的应用 101 以及具有文件系统 102 的内核 10 是由普通计算机及其 OS 提供的。因此，将省略对它们的函数的结构和细节的描述。文件路径重写函数 104 和 AP 启动检测函数 105 构成了用于切换要访问的文件夹的方法和程序的各个处理步骤的主要部分，并且构成了根据本发明的计算机系统的各个装置的主要部分。这些函数 104 和 105 以及内核 10 和应用 101 被安装为由 CPU 2 执行的控制程序。

文件路径重写函数 104 例如被实现为动态链接库（DLL）。当从应用 101 调用涉及对盘设备 103 的文件访问的系统调用时，读取该函数

104，并且该函数 104 变为能够工作。

AP 启动检测函数 105 用来监视应用 101 的启动，并且在任意应用 101 启动时，替换应用 101 的函数指针，从而在文件访问时调用文件路径重写函数 104。

接着，将参考图 1 至 3 具体描述本实施例的操作。

图 2 是示出了路径重写函数的操作的流程图。图 3 示出了盘设备 103 中的目录结构。

首先，如图 3 所示，作为盘设备 103 中的目录结构，在秘密根目录“sec_root”下预先定义去往秘密文件夹的路径，其中秘密文件夹用于写入作为秘密信息的秘密文件。秘密根目录“sec_root”位于常规根目录“/”之下。秘密根目录“sec_root”下的目录“bin”、“doc”、“tmp”等的目录结构被设置为与常规根目录下的常规文件夹“bin”、“doc”、“tmp”等的目录结构相同，其中常规文件夹用于写入作为非秘密信息的常规文件。

接着，在启动应用 101 时，用户预先指定所启动的进程是能够处理秘密信息的秘密模式的进程还是不能处理秘密信息的常规模式的进程。对安全级别的这种指定例如通过将其设置为环境变量，被传送到文件路径重写函数 104。

接着，AP 启动检测函数 105 检测到任意应用 101 的启动，并且重写应用 101 进行的文件访问中的系统调用的函数指针。这样，在访问文件时，调用与文件路径重写函数 104 相对应的函数。

接着，文件路径重写函数 104 基于从应用 101 传送来的进程的秘密模式、去往请求访问的文件的路径、以及访问请求的内容，执行下列处理（见图 2）。

如图 2 所示，文件路径重写函数 104 首先确定进程是否处于秘密模式（步骤 A1）。结果，如果进程处于秘密模式（是），则文件路径重写函数 104 确定文件访问请求是否是写指令（步骤 A2）。

结果，如果该请求是写指令（是），则重写文件路径（步骤 A4）。此时，通过向被写为完全路径的文件名的头部加入“/sec_root”，文件路径被重写为相对于被视作根目录的“/sec_root”的相对路径。例

如，如果给定的文件是“/doc/file1”的路径文件名，则在这种情形中通过重写该文件路径名，文件名被替换为“/sec_root/doc/file1”的路径名。接着，对该路径名执行写指令（步骤 A6）。

另一方面，如果在步骤 A2 中文件访问请求是写指令之外的其他指令（否），例如，如果请求是读指令，则确定在通过向给定文件路径的头部加入“/sec_root”所定义的路径处是否存在文件（步骤 A3）。结果，如果文件存在，则与写指令的情形中一样，重写文件路径名（步骤 A4）。如果不存在，则不执行重写。接着，对该路径名执行读指令（步骤 A6）。

同样，在步骤 A1 中，如果进程处于常规模式，则确认给定的文件路径是否是“/sec_root”下的文件名（步骤 A5）。结果，如果给定文件路径是“/sec_root”下的文件，则返回指示不可访问的错误（步骤 A7）。如果给定文件路径不同于“/sec_root”，则如往常一样执行文件访问指令（步骤 A6）。

因此，根据本实施例，可以获得下列优点。

第一个优点是要访问的文件夹被切换为与秘密模式相对应，并且可以防止处于常规模式的进程访问秘密文件夹中的文件以及向秘密文件夹之外的任何其他文件夹写入文件。这是因为通过重写路径，由处于秘密模式的进程所写出的每个文件位于秘密文件夹之下。这也是因为从处于常规模式的进程返回关于访问秘密文件夹之下的文件的错误。

第二个优点是可以透明地引用使用秘密模式和常规模式共有的一个相同文件名的文件。这是因为结构被布置为能够在秘密文件夹下具有与常规根目录下的所有目录结构相对应的这种目录结构。另外，因为执行路径重写，所以在秘密模式和常规模式中，应用程序可以通过指定相同的文件名来访问文件。以这种方式，在秘密模式和常规模式中具有相同名称的临时文件可以位于不同目录中，而应用程序不会察觉。因此，可以解决在同时操作处于秘密模式和常规模式的进程时临时文件的安全级别冲突的问题。

第三个优点是，即使处于秘密模式的进程读入及写出常规文件，

原始文件仍保持为常规文件，并且可以从处于常规模式的另一应用程序访问。

第四个优点是不改变现有文件系统。这是因为不是通过扩展内核中的文件系统来执行基于秘密模式的访问控制，而是通过在上层中重写文件路径来实现。因此，可以利用现有文件系统。

在本实施例中，在常规模式中禁止对秘密文件夹的读取和写入。然而，可以如此布置结构：严格应用前述 NWD 原则，从而允许对秘密文件夹进行写入。

同样，在本实施例中，从处于秘密模式的应用 101 输出的所有文件都被输出到秘密文件夹中。然而，可以如此布置结构：对于每个应用 101，文件路径重写函数 104 具有可以输出到常规文件夹的例外文件的列表。在这种情形中，可以预先将去往某个应用所特有的配置文件（不包括秘密信息）的路径作为例外文件写入例外文件列表中。那么，即使在处于秘密模式的进程中用户改变了设置，也可以向常规文件路径上的文件夹进行写入，而不会提升该配置文件的安全级别。因此，可以继续在常规模式和秘密模式中使用公共配置文件。

（第二实施例）

图 4 是示出了根据本实施例的计算机系统的整体结构的图。

在上述第一实施例中，文件路径重写函数 104（图 1）用秘密根目录“sec_root”来透明地替代秘密模式中文件的输入/输出。然而，在本实施例中，如图 4 所示，由环境变量重写函数 106 和文件访问强制函数 107 来实现与文件路径重写函数 104 相似的功能。该结构的其他方面与实施例 1 相同。因此，这里省略对它们的描述。

AP 启动检测函数 105 用来监视应用 101 的启动，并在任意应用 101 启动时，调用环境变量重写函数 106 和文件访问强制函数 107。

环境变量重写函数 106 例如被实现为动态链接库（DLL），并且在应用 101 调用系统调用时，调用该函数来获得程序的操作环境，例如环境变量、注册表等。

如果进程工作于秘密模式，则该环境变量重写函数 106 执行重写，就如同指定了临时目录的环境变量或指定了缓存文件夹的注册表值位

于“/sec_root”之下。例如，指定了临时目录的环境变量 TEMP 被设置为“/tmp”，在秘密模式中执行重写就如同该变量被设置为“/sec_root/tmp”。

例如，将文件访问强制函数 107 实现为动态链接库，并且在应用 101 调用用于文件操作的系统调用时，调用该函数。该文件访问强制函数 107 对每个应用 101 具有可以输出到常规文件夹的文件的例外文件列表（先前所述）。

接着，参考图 5 描述文件访问强制函数 107 的操作。

首先，确定进程是否处于秘密模式（步骤 B1）。如果进程处于秘密模式（是），则随后确定文件访问请求是否是写指令（步骤 B2）。结果，如果请求是写指令（是），则检查指定的路径是否表示秘密文件夹下的位置，即，检查给定的文件路径是否是“/sec_root”下的文件名（步骤 B3）。如果文件路径表示“/sec_root”下的文件，即，如果文件路径表示秘密文件夹下的位置（是），则允许写入。如果文件路径表示“/sec_root”下的文件之外的另一文件，即，如果文件路径并不表示秘密文件夹下的位置(否)，则检查该文件路径是否表示例外文件(步骤 B4)。如果文件路径表示例外文件（是），则允许对文件的访问。否则（否），返回指示不可访问的错误（步骤 B7）。

同样，在步骤 B1 中，如果进程不是处于秘密模式，即，如果进程处于常规模式(否)，则检查所指定的路径是否表示秘密文件夹下的秘密文件，即检查给定的文件路径是否是“/sec_root”下的文件名(步骤 B5)。结果，如果文件路径是“/sec_root”下的文件名（是），则返回指示不可访问的错误（步骤 B7）。否则，如果文件路径是“/sec_root”下的文件名之外的其他文件名（否），则执行正常使用的文件访问指令（步骤 B6）。

这样，在本实施例中，只能在“/sec_root”下的位置处存储秘密文件。因此，在秘密模式和常规模式之间彼此不同的文件不会被视为相同的文件。因此，普通的用户可以更容易地理解操作。另外，环境变量重写函数 106 临时写入的文件被写在秘密文件夹之下。因此，当操作于秘密模式的应用 101 要将文件写出为常规文件时，阻断该写

操作，从而防止错误操作。

在本实施例中，在常规模式中也禁止对秘密文件夹的读取和写入。然而，可以严格应用前述 NWD 原则，从而允许对秘密文件夹进行写入。

本发明适于用作防止秘密信息从通用计算机泄漏的程序。

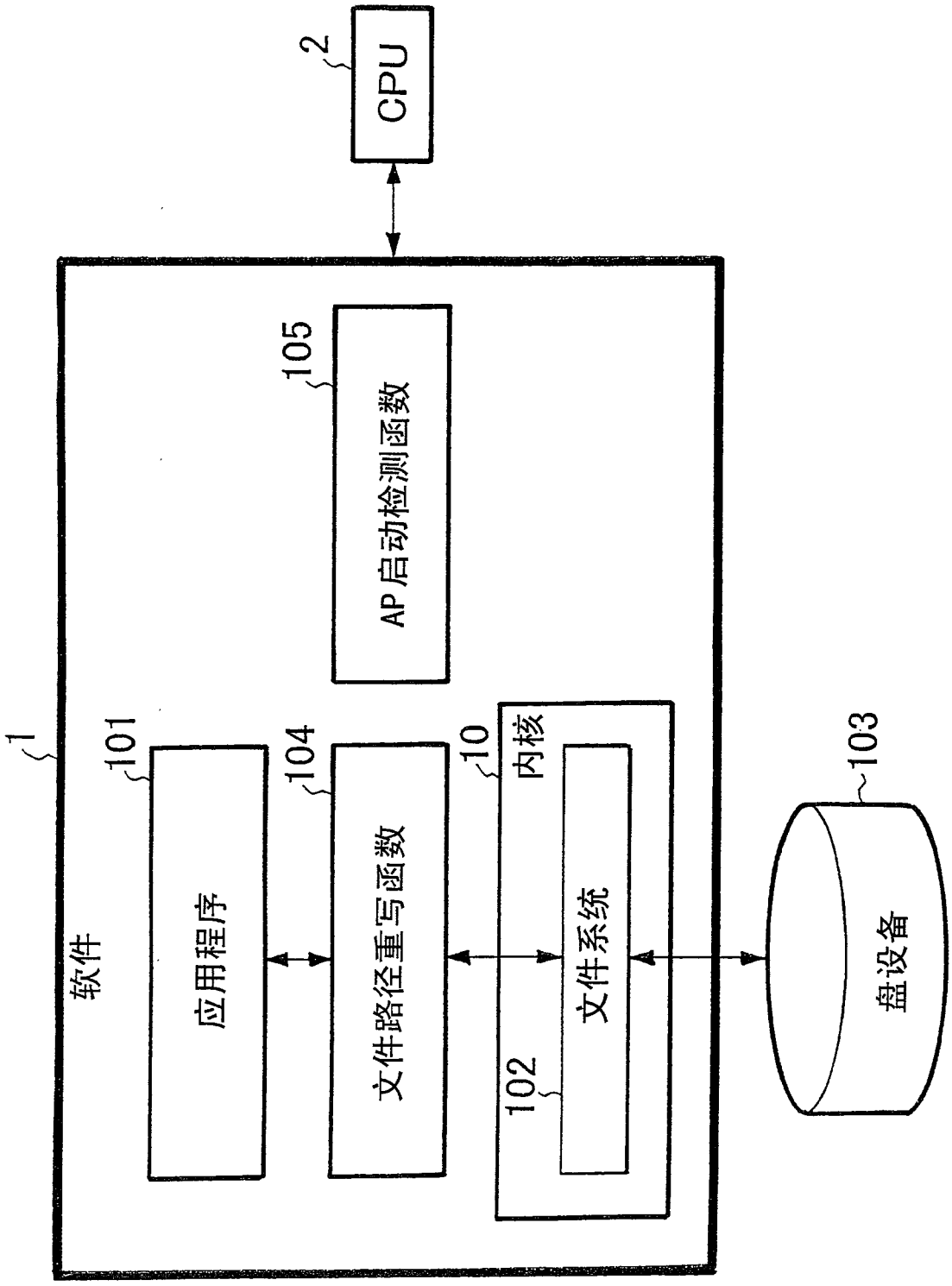

2
CPU
105
AP 启动检测函数
1
软件
101
应用程序
104
文件路径重写函数
10
内核
102
文件系统
103
盘设备

图 1

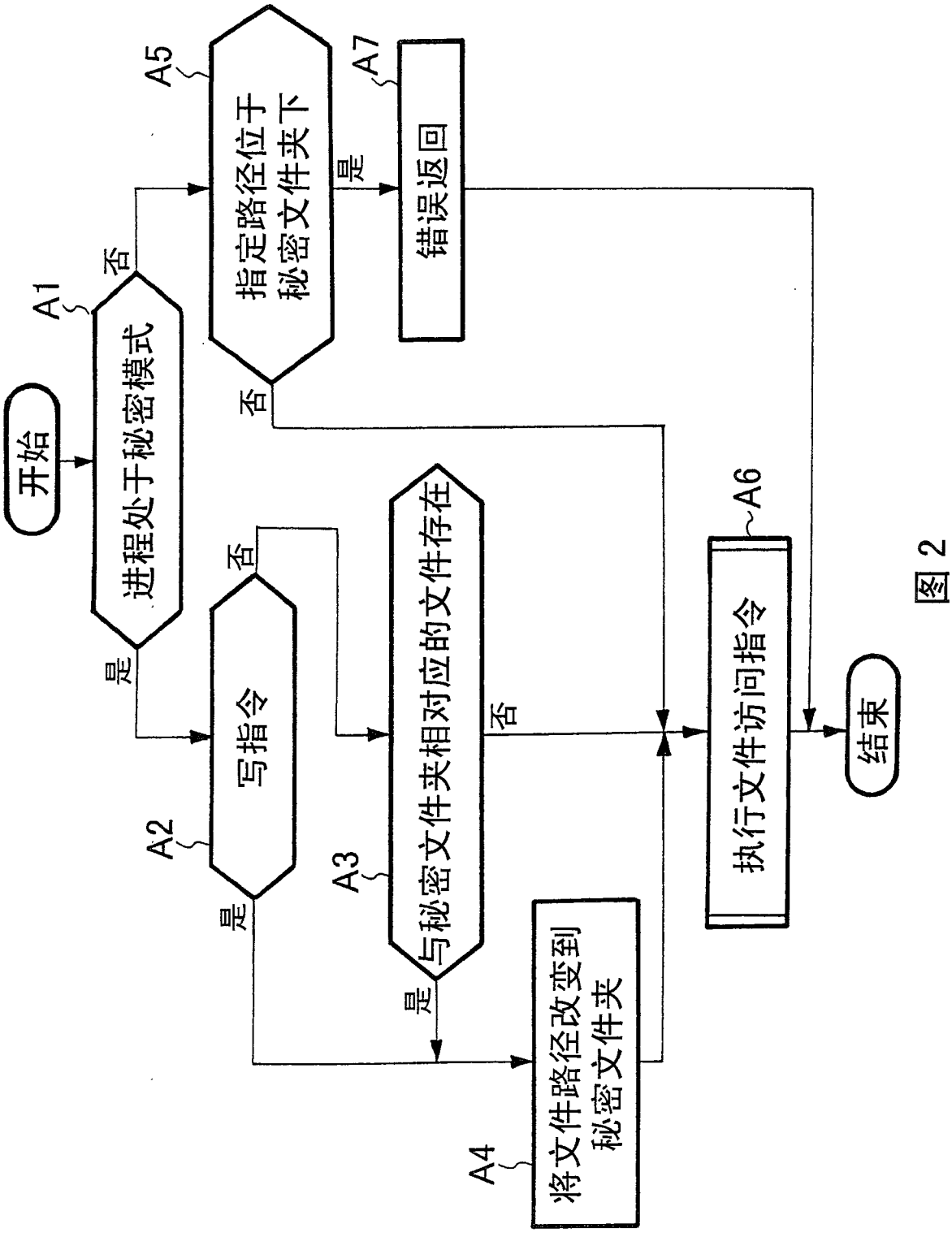

开始
进程处于秘密模式
A1
否
是
写指令
A2
否
是
与秘密文件夹相对应的文件存在
A3
否
是
指定路径位于秘密文件夹下
A5
是
否
错误返回
A7
将文件路径改变到秘密文件夹
A4
执行文件访问指令
A6
结束

图 2

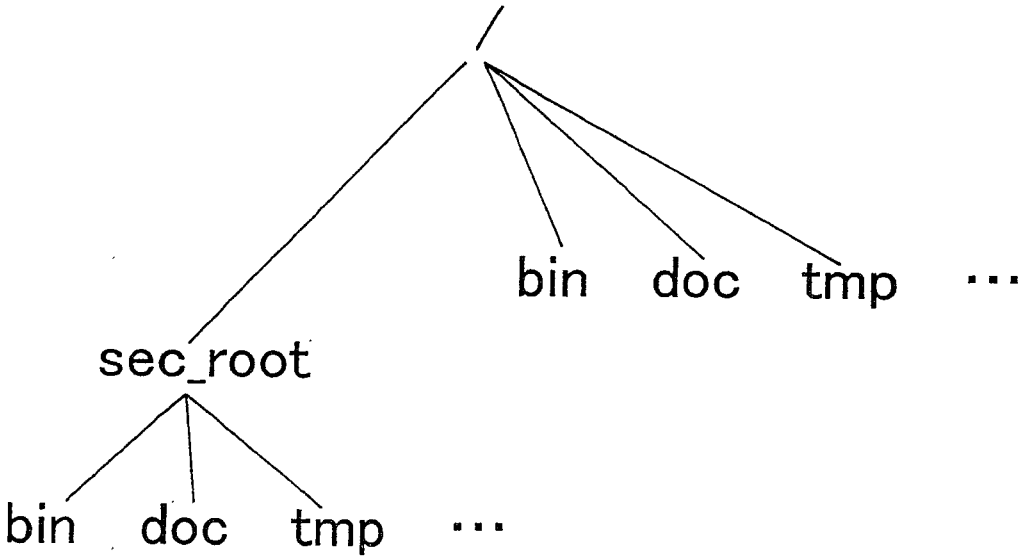


图 3

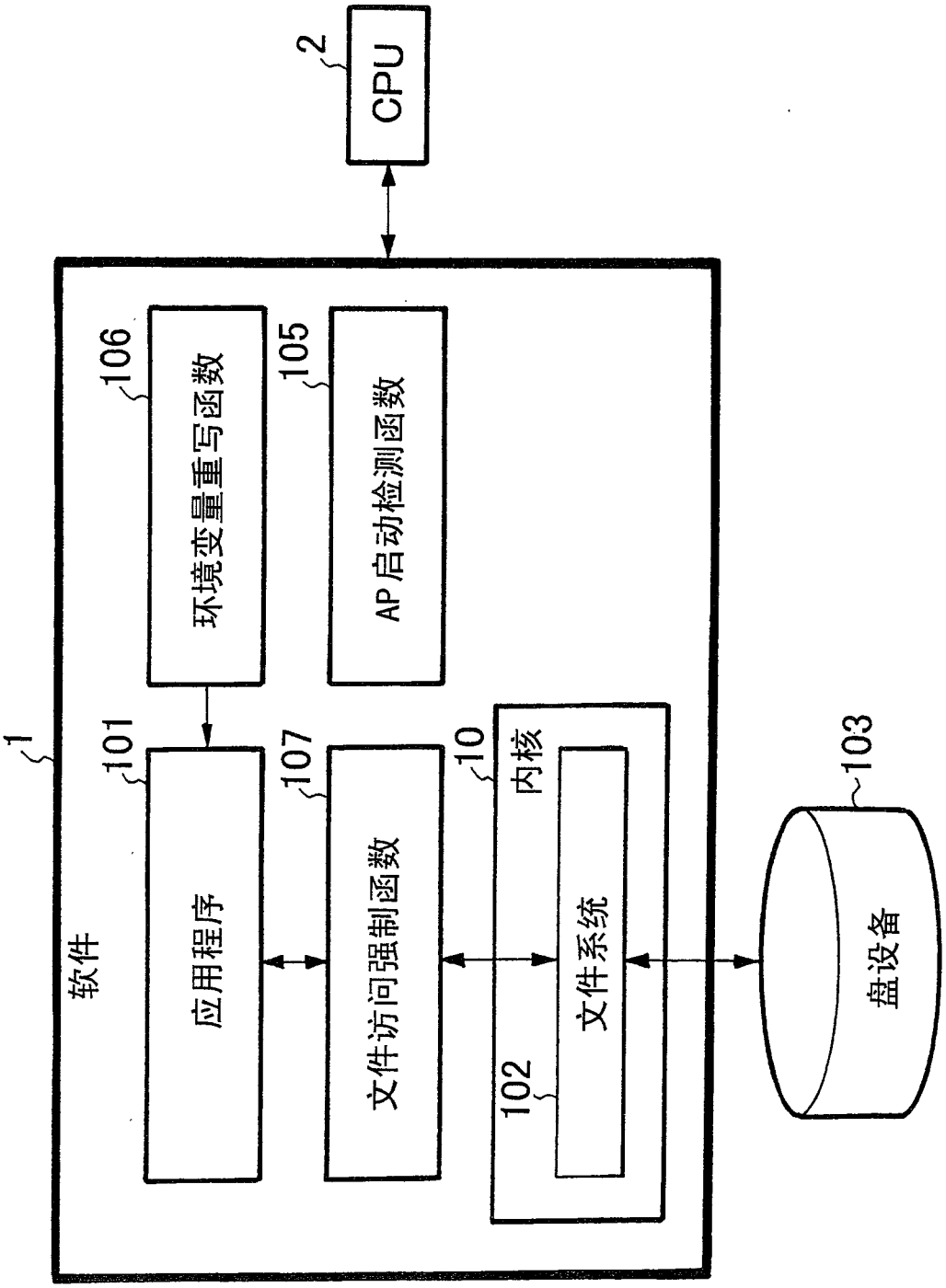

2
CPU
1
软件
106
环境变量重写函数
105
AP启动检测函数
101
应用程序
107
文件访问强制函数
10
内核
102
文件系统
103
盘设备

图 4

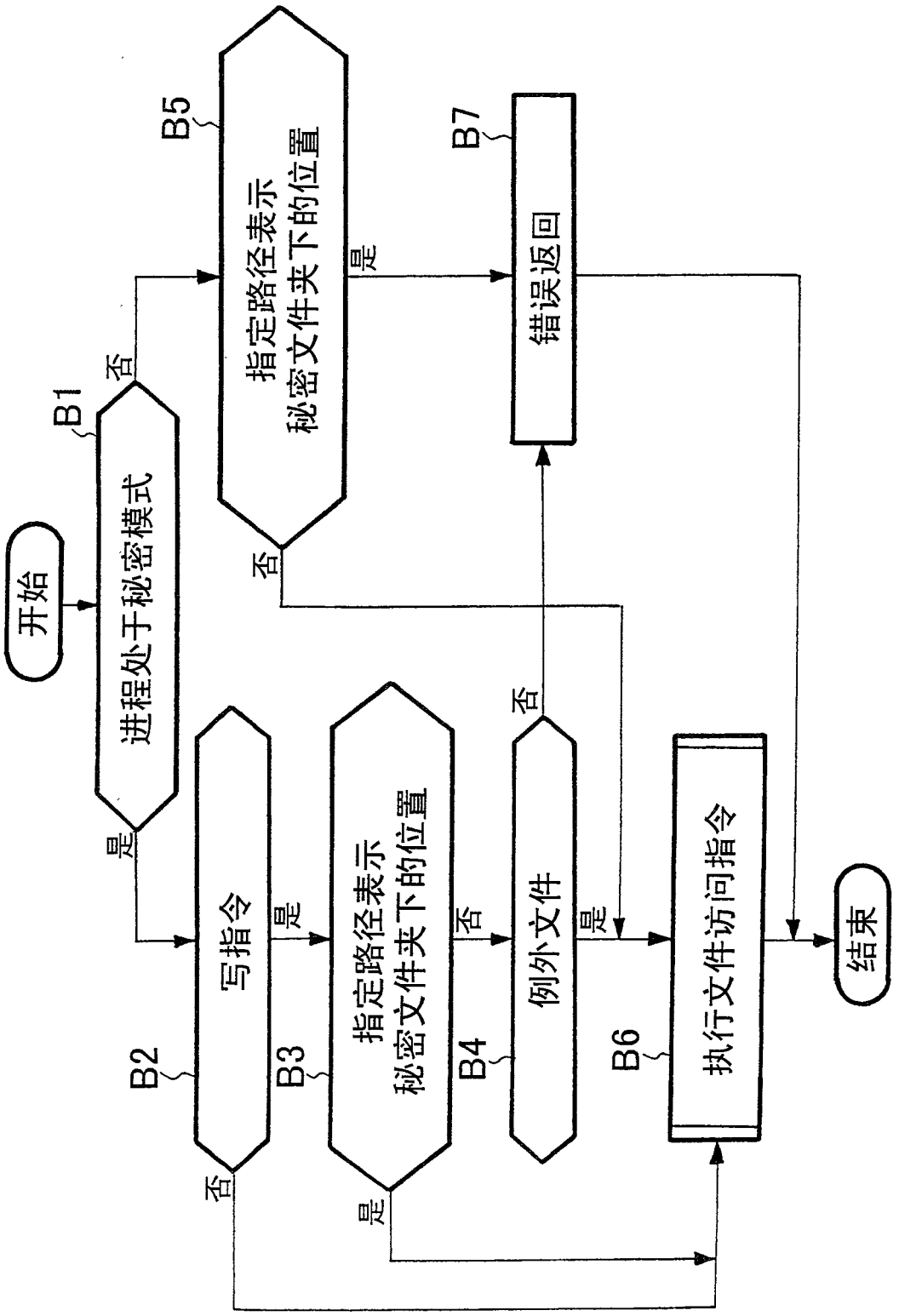

开始
进程处于秘密模式
B1
否
是
B5
指定路径表示
秘密文件夹下的位置
是
否
B7
错误返回
写指令
B2
否
是
指定路径表示
秘密文件夹下的位置
B3
是
否
例外文件
B4
否
是
执行文件访问指令
B6
结束

图 5