(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 104137114 B
(45)授权公告日 2017.03.08

(21)申请号 201280070895.5
(22)申请日 2012.12.28
(65)同一申请的已公布的文献号
申请公布号 CN 104137114 A
(43)申请公布日 2014.11.05
(30)优先权数据
61/595,021 2012.02.03 US
13/624,836 2012.09.21 US
13/624,828 2012.09.21 US
13/624,832 2012.09.21 US
(85)PCT国际申请进入国家阶段日
2014.08.29
(86)PCT国际申请的申请数据
PCT/US2012/072191 2012.12.28
(87)PCT国际申请的公布数据
WO2013/115927 EN 2013.08.08
(73)专利权人 苹果公司
地址 美国加利福尼亚
(72)发明人 P·基尔特雷伯 J·A·维德瑞恩 C·S·林 R·D·萨尔丁格 B·J·托玛斯
(74)专利代理机构 中国国际贸易促进委员会专利商标事务所 11038
代理人 陈新
(51)Int.Cl.
G06F 21/51(2006.01)
(56)对比文件
US 5917912 A,1999.06.29,
CN 101350034 A,2009.01.21,
CN 101414327 A,2009.04.22,
US 7698744 B2,2010.04.13,
CN 102016867 A,2011.04.13,
CN 101853363 A,2010.10.06,
审查员 王春圆

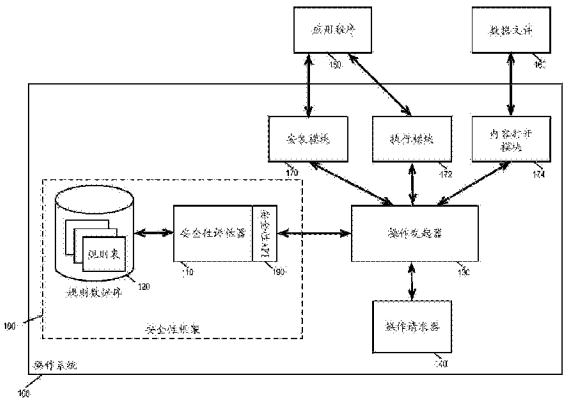
权利要求书2页 说明书28页 附图26页

(54)发明名称

集中式操作管理

(57)摘要

本发明提供一种为设备的操作系统的一部分的新型安全性框架。该框架包括安全性评估器，该安全性评估器针对需要相对于在设备上执行的应用程序而执行的不同操作来执行安全性策略评估。此类操作的实例包括安装应用程序、执行应用程序以及通过应用程序打开内容文件(如打开文档)。



CN 104137114 B

1.一种电子设备,包括:

一组处理单元;和

机器可读介质,所述机器可读介质存储操作系统,所述操作系统包括:

操作请求器,所述操作请求器用于接收打开文档以及与所述文档相关联的应用程序的命令;

操作发起器,所述操作发起器用于基于所接收的命令请求安全性评估,其中所述请求包括一组数字对象,(i)在未对所述应用程序执行安全性评估时,所述一组数字对象与所述文档和与所述应用程序相关联的多个不同操作相关联,或者(ii)当在接收到打开所述文档的命令之前对所述应用程序执行了安全性评估时,所述一组数字对象与所述文档相关联;和

安全性评估器,所述安全性评估器用于评估所述一组数字对象是否遵守安全性策略。

2.根据权利要求1所述的电子设备,其中当尚未对所述应用程序执行安全性评估时,所述一组数字对象包括与所述文档相关联的第一子组数字对象和与所述多个不同操作相关联的第二子组数字对象。

3.根据权利要求2所述的电子设备,其中在所述第一子组和第二子组遵守所述安全性策略时,所述操作发起器发起所述文档的打开并且启动所述应用程序。

4.根据权利要求1所述的电子设备,其中所述安全性评估器是用于通过使用应用编程接口(API)执行所请求的安全性评估的安全性框架的一部分。

5.根据权利要求1所述的电子设备,其中所述多个不同操作包括在执行所述操作系统的计算机中安装所述应用程序。

6.根据权利要求1所述的电子设备,其中所述安全性评估器通过检查规范要求来评估特定操作是否遵守安全性策略,所述规范要求指定与所述特定操作相关联的一子组数字对象所要求的一组特性。

7.根据权利要求6所述的电子设备,其中所述操作系统还包括存储与所述安全性策略相关联的多个指令集的数据库,其中所述安全性评估器通过从所述数据库检索匹配特定操作的指令集来确定与所述特定操作相关联的所述安全性策略。

8.根据权利要求7所述的电子设备,其中所述数据库包括权限表和高速缓存表,其中从所述数据库检索匹配所述特定操作的所述指令集包括在搜索所述权限表中的匹配条目之前搜索所述高速缓存表中的匹配条目。

9.一种在操作系统中提供安全性评估的方法,所述方法包括:

接收打开与在设备上执行的应用程序相关联的文档的命令;

请求安全性框架以(i)在所述安全性框架未对所述应用程序执行安全性评估时,对所述文档和所述应用程序执行安全性评估,或者(ii)在所述安全性框架在接收到打开所述文档的命令之前对所述应用程序执行了安全性评估时,对所述文档执行安全性评估;

基于所述安全性评估确定打开所述文档。

10.根据权利要求9所述的方法,其中所述安全性评估基于规范要求,所述规范要求指定与所述文档相关联的数字对象所要求的一组特性。

11.根据权利要求9所述的方法,其中所述方法还包括维护数据库,所述数据库存储用于执行所述安全性评估的多个指令集,其中所述安全性框架通过从所述数据库检索匹配所

述文档的指令集来确定与所述文档相关联的安全性策略。

12.根据权利要求11所述的方法，其中所述数据库包括权限表和高速缓存表，其中从所述数据库检索匹配所述文档的所述指令集包括在搜索所述权限表中的匹配条目之前搜索所述高速缓存表中的匹配条目。

13.一种由操作系统执行的评估操作的安全性的方法，所述方法包括：

接收在操作系统内执行的应用程序中打开文档的命令；

当在接收到打开所述文档的命令之前评估了所述应用程序时，通过使用应用编程接口(API)访问安全性框架来请求对所述文档而非所述应用程序进行安全性评估；

在所述应用程序先前未被评估过时，通过使用所述API来请求对所述文档和所述应用程序的安全性评估；以及

基于所请求的安全性评估确定是否执行特定操作。

14.根据权利要求13所述的方法，其中对所述文档而非所述应用程序的安全性评估是第一安全性评估，其中针对执行所述应用程序的第二安全性评估在第一安全性评估之前被请求。

15.根据权利要求13所述的方法，其中所述特定操作包括打开与所述操作系统中的执行中的应用程序相关联的所述文档。

16.根据权利要求13所述的方法，其中确定是否执行所述特定操作包括确定所述文档是否来自可信来源。

17.根据权利要求13所述的方法，其中对所述文档而非所述应用程序的安全性评估包括通过检查规范要求来评估所述文档是否遵守安全性策略，所述规范要求指定与所述文档相关联的数字对象所要求的一组特性。

18.根据权利要求17所述的方法，其中所述规范要求存储在数据库中，所述数据库存储与所述安全性策略相关联的多个指令集，其中所述数据库包括权限表和高速缓存表，其中从所述数据库检索匹配所述文档的所述指令集包括在搜索所述权限表中的匹配条目之前搜索所述高速缓存表中的匹配条目。

19.根据权利要求13所述的方法，还包括通过从数据库检索匹配所述文档的指令集来确定与所述文档相关联的安全性策略。

20.一种计算机系统，包括用于实施根据权利要求9-19中任一项所述的步骤的装置。

集中式操作管理

技术领域

[0001] 本公开一般地涉及操作系统，并且具体地涉及用于各种应用程序的操作的安全性评估的设备、系统和方法。

背景技术

[0002] 存储并运行于计算机系统上的程序的身份和安全性对于用户而言是一个根本性的安全性问题。实质上，用户希望它们所交互的程序像被宣传的程序那样执行。在用户信任特定程序，而程序以不期望的方式运行时，用户可能会遇到问题。在一些情况下，程序可能已被故意改变，或者可能存在病毒或其他安全性问题。通常，由于程序并非来自可信来源，所以程序不同于用户初始期望的那样运行，其在某个点处已被改变而使其与其他部件不兼容，或者由于某些其他原因而失效。

[0003] 因此，尝试解决这一问题的大量安全性程序在现代计算机上运行。这些应用程序中的每一个都解决计算机的一组安全性需求。它们包括防病毒应用程序、防火墙、恶意软件检测程序、签名校验机制等。这些程序中的一些是作为操作系统的一部分被提供的，一些被集成到互联网浏览器中，而其他是从第三方供应商购买或甚至下载的。

[0004] 然而，这些程序并不是用于建立身份认证的相容机制。不能依赖它们来全面检查在操作系统中运行的所有操作，即使在系统中运行的任何操作可能引入来自不可信任的来源的数据对象并且损害计算机。这些过程经常不能在操作系统中最佳地执行，并且减慢整个系统的速度。这些安全性程序的各种各样的性质使其难以或不可能为软件开发人员引入一组统一的安全性接口编程。更糟的是，安全性评估程序的这些各种各样的分类中的一些可能来自尚未被正确地认证为可信任的来源。

[0005] 需要一种用于建立身份认证的相容机制。具体地，需要一种与操作系统完全集成的安全性评估机制，以提供相容的性能、在操作系统中进行的对操作的全面检查以及统一的软件开发支持。

发明内容

[0006] 本发明的一些实施例提供了一种针对设备的新型安全性框架。在一些实施例中，该框架是设备操作系统的一部分。一些实施例的框架包括安全性评估器，该安全性评估器对不同操作执行安全性策略评估，这些不同操作需要相对于在设备上执行的应用程序来执行。此类操作的实例包括安装应用程序、执行应用程序以及通过应用程序打开内容文件(如打开文档)。

[0007] 在一些实施例中，该设备具有操作发起器，该操作发起器接收相对于应用程序的不同操作的请求。在接收到此类请求时，操作发起器指导安全性评估器基于存储在安全性策略数据存储中的安全性策略规则来检查所请求的操作的可行性。在一些实施例中，安全性策略规则用于检查下载的程序的有效性，以验证程序来源或发布者等。如果安全性策略规则允许所请求的操作，则安全性评估器通知操作发起器该操作已被批准，并且操作发起

器指导适当的操作处理程序(如安装程序、执行程序或文件打开器)执行所请求的操作。

[0008] 在一些实施例中,安全性策略体现在存储在规则数据库中的不同的规则或指令中。规则数据库中的规则规定数据对象需要什么以让数据对象(如程序代码或要打开的文档)遵守计算机的安全性策略。在一些实施例中,规则数据库包括不同的表格以便更有效地对规则数据库进行查询。权限表和高速缓存表是此类表格的两个实例。

[0009] 在一些实施例中,在安全性策略下评估数据对象的安全性需按照由其优先级阐述的顺序来检查规则数据库中的权限表的条目。对于针对在这些实施例中的数据对象的任何给定的安全性评估,较低优先级规则仅在较高优先级规则不适用时才变得适用。在较高优先级规则与较低优先级规则重叠时较高优先级规则会取代较低优先级规则。因此,对较高优先级规则的任何改变都潜在地改变了较低优先级规则的适用性。

[0010] 在一些实施例中,操作发起器针对为应用程序而请求的每个操作执行安全性评估。在其他实施例中,操作发起器仅针对为应用程序而请求的操作中的一些执行安全性评估。例如,在一些实施例中,仅针对新接收的应用程序的安装或仅针对通过应用程序新接收的文件的初次打开来执行评估。为了有利于这种方法,在将此类文件首次加载到设备上或首次打开此 类文件时(如通过网络或通过设备的外围接口首次下载),一些实施例中的设备将标记与新接收的应用程序和新接收的文件相关联。

[0011] 一些实施例的安全性评估器通过验证包含数据文件的数据结构(诸如“档案文件”)的有效性来批准或不批准一个或多个数据文件的有效性。在这样的一些实施例中,档案文件带有身份签名,该身份签名可用于安全性地认证数据文件并识别包括在那些档案文件中的数据文件的来源。更具体地,这些实施例中的操作系统包括规则数据库中的规则,该规则基于嵌入包含那些文档或数据文件的档案文件结构中的签名来批准或不批准文档或数据文件。自动批准已批准档案文件中的文档。

[0012] 上述发明内容旨在用作对本发明的一些实施例的简单介绍。其并非意味着对在本文档中公开的所有发明主题的介绍或概述。随后的具体实施方式以及在具体实施方式中被提及的附图将进一步描述发明内容中所述的实施例以及其他实施例。因此,为了理解本文档所描述的所有实施例,需要全面审查发明内容、具体实施方式和附图。此外,受权利要求书保护的主题不受限于发明内容、具体实施方式及附图中的示例性细节,而是由所附权利要求所限定,这是由于受权利要求书保护的主题能够以其他特定形式实施而不脱离本主题的实质。

附图说明

[0013] 在所附的权利要求中阐述了本发明的新颖特征。然而,出于解释的目的,在以下附图中阐述了本发明的若干实施例。

[0014] 图1示出了评估被请求执行的不同操作的安全性的计算设备的操作系统。

[0015] 图2概念性地示出了操作系统用于处理和批准所请求操作的过程。

[0016] 图3概念性地示出了基于操作系统的安全性策略对所请求的操作执行安全性评估的示例性过程。

[0017] 图4-图6示出了在使用安全性评估器和规则数据库执行安全性评估时操作系统中的数据流。

[0018] 图7概念性地示出了存储用于确定操作系统的安全性策略的规则或指令的权限表。

[0019] 图8概念性地示出了包括额外字段的权限表。

[0020] 图9概念性地示出了在每个记录或条目中仅包括一个规则字段的权限表。

[0021] 图10示出了在其中多个条目用于表达单一安全性策略的权限表。

[0022] 图11示出了用于一种示例性安全性策略的一组文氏图。

[0023] 图12示出了用于另一种示例性安全性策略的一组文氏图。

[0024] 图13概念性地示出了用于通过使用权限表来执行安全性评估的过程。

[0025] 图14示出了包括权限表和高速缓存表的规则数据库。

[0026] 图15示出了基于来自操作发起器的请求来使用权限表和高速缓存表两者以用于进行安全性评估的安全性评估器。

[0027] 图16示出了通过安全性评估器为数据对象生成并存储高速缓存表条目。

[0028] 图17概念性地示出了使用权限表和高速缓存表两者以用于执行安全性评估的过程。

[0029] 图18概念性地示出了在由用户改变规则数据库之后维护规则表的过程。

[0030] 图19示出了具有插入其自身的标识符以用于执行安全性评估的操作系统的计算机。

[0031] 图20示出了检查作为安全性评估操作的一部分的标记的操作系统。

[0032] 图21-图22示出了在使用数据对象中识别标记的操作发起器执行安全性评估时操作系统中的数据流。

[0033] 图23示出了包括具有用于处理标记位的规则的规则数据库的操作系统。

[0034] 图24示出了接收并存储包含签名的数据档案文件的计算机。

[0035] 图25示出了包括用于基于数据档案文件中的签名对数据文件或文档进行安全性评估的规则数据库中的规则的操作系统。

[0036] 图26概念性地示出了对文档打开操作执行安全性评估的过程。

[0037] 图27概念性地示出了使用其来实施本发明的一些实施例的电子系统。

具体实施方式

[0038] 在以下描述中，出于解释的目的而阐述了许多细节。然而，本领域的普通技术人员将认识到，可以不使用这些具体细节来实践本发明。在其他 情况下，以框图形式示出了熟知的结构和设备，以便不会用不必要的细节来使本发明的描述模糊。

[0039] I.具有安全性评估的操作系统

[0040] 图1示出了评估被请求执行的不同操作的安全性的计算设备的操作系统100。所请求的操作可以是执行应用程序、安装应用程序、打开文档等。由安全性评估器评估所请求操作的安全性，安全性评估器是操作系统提供的安全性框架的一部分。基于这种安全性评估，操作系统终止所请求的操作或者允许其继续进行。

[0041] 如图1所示，操作系统100包括安全性评估器110、规则数据库120、操作发起器130、操作请求器140、安装模块170、执行模块172和内容打开模块174。图1还示出了应用程序150和数据文件160，操作系统100针对其评估安全性策略。安全性评估器110和规则数据库120

是提供应用编程接口(API)190的安全性框架180的一部分。

[0042] 操作系统100是管理计算机硬件资源并为不同的软件应用程序提供通用服务的一组程序。操作系统100充当应用程序和计算机硬件之间的中介，以用于诸如输入、输出和存储器分配的功能。在一些实施例中，程序的应用程序代码由硬件执行并通过从操作系统所接收的中断或向操作系统进行的调用而与操作系统进行交互。

[0043] 应用程序150是用于对操作系统进行操作和执行功能的可执行数据对象。应用程序150的实例包括文字处理器、Web浏览器、游戏、媒体编辑应用程序等。在一些实施例中，应用程序150是安装程序，其在正在运行操作系统100的计算机上安装一个或多个可执行程序。

[0044] 在一些实施例中，应用程序150嵌入身份的一个或多个签名以允许应用程序的用户确定应用程序的真实性。嵌入到应用程序150中的签名是该应用程序的来源或发布者的安全性标识符。在通过使用仅为数据对象的签署者所知的秘密私钥，基于数据对象的内容生成签名时，“签署”数据对象(如应用程序)。因此，此类签名能够识别数据对象的签署者或来源并保护数据对象的完整性。为了认证数据对象的签名，即，为了验证签名确实是由其声称的来源/签署者从数据对象生成的，数据对象的接收人(即操作系统)使用公钥来认证签名连同数据对象的内容。已知公钥来自声称的来源/签署者，并且接收人能够独立地验证该公钥是否确实是由声称的来源/ 签署者(例如，通过查询可信证书管理机构或通过检查接收人自身的数据库)来公布的。

[0045] 在一些实施例中，从与数据对象相关联的公钥证书提取数据对象的签名。公钥证书(也称为数字证书或身份证书)是使用数字签名将公钥与身份绑定的电子文档，身份是诸如人或组织名称、它们的地址等的信息。可以使用证书来验证公钥属于个人。证书上的签名是证书签署者的证明，其证实身份信息和公钥属于一体。在认证时，基于应用程序数据对象的内容和证书中的信息两者生成或签署的签名证明应用程序数据对象的内容还未被窜改，并且证书中的信息是真实的。除了签名和来源标识符(如供应商ID和公钥)之外，证书还包括关于如何可以认证签名的信息(如用于生成签名的算法的ID)。

[0046] 在图1的实例中，操作系统100执行签名认证操作。在一些实施例中，如果操作系统未能认证应用程序的签名，则操作系统100阻止应用程序150执行或安装。在一些实施例中，操作系统100阻止甚至一个被认证的应用程序的操作继续进行，除非该应用程序来自已经根据一组安全性策略确定是可信任的来源。

[0047] 数据文件160是与能够在操作系统中执行的一个或多个应用程序相关联的数据对象。数据文件160的实例包括文本文件、文字处理器文档、电子数据表、媒体文件等。数据文件160被能够读取或打开数据文件的应用程序读取或打开。在一些实施例中，数据文件160包括不包括签名或证书的文档。也可以将数据文件放置在档案文件结构中，使得数据文件可以与签名或证书相关联。下面的图25和26描述了一些实施例的安全性评估器如何处理数据档案文件中的数据文件。

[0048] 安装模块170是监督诸如应用程序150的应用程序的安装的操作系统100内的模块。在一些实施例中，安装模块170在开始处理应用程序150以用于通过操作系统进行安装之前，等待来自操作发起器130的“继续进行”命令。在这些实施例中的一些中，安装模块向安全性评估器110传递应用程序数据对象150以用于根据一组安全性策略验证应用程序的

签名以及其符合一组要求。仅在安装模块170从操作发起器130接收到指示应用程序150被认证并且应用程序150的来源被验证的通信时，其才继续安装应用程序150。

[0049] 执行模块172是在操作系统100内启动诸如应用程序150的应用程序以用于在操作系统100中执行的模块。像安装模块170那样，在一些实施例中，执行模块172在启动应用程序150以用于通过操作系统100执行之前，等待来自操作发起器130的“继续进行”命令。在这些实施例中的一些中，执行模块向安全性评估器110传递应用程序数据对象150以用于根据一组安全性策略验证应用程序的签名并满足一组要求。仅在执行模块172在应用程序150已被认证并且应用程序150的来源被验证之后从操作发起器130接收到启动命令时才继续执行应用程序150。

[0050] 内容打开模块174是监督数据文件160的打开的操作系统100内的模块。在一些实施例中，打开内容涉及针对数据文件160中的内容识别适当应用程序并且然后将内容递送至应用程序的操作。如上所述，数据文件的内容可以伴有或不伴有签名，并可以需要或不需要被认证。对于需要被认证的文档，向安全性评估器110传递该文档，以便验证文档的签名并根据一组安全性策略满足一组要求。仅在内容打开模块174在数据文件160已经被认证并且数据文件160的来源被验证之后从操作发起器130接收到启动命令时，才继续打开文档数据文件160。

[0051] 在一些实施例中，数据文件160的打开与应用程序的执行相关联。在这些实施例中的一些中，内容打开模块174首先识别用于打开数据文件160的应用程序。如果由内容打开模块174识别的应用程序已经在操作系统中执行，则内容打开模块向要被执行的执行模块172递送数据文件。如果当前没有执行所识别的应用程序，则内容打开模块174使得执行模块172开始执行应用程序。仅在操作系统100已确定应用程序被认证并且应用程序的来源被验证之后，才执行所识别的应用程序。

[0052] 操作请求器140是请求操作系统100执行特定操作的性能的模块。此类操作可包括安装应用程序、执行应用程序、打开数据文件等。在一些实施例中，操作请求器140是接收用于打开文档或执行特定应用程序(如通过选择针对文档或应用程序的图形图标)的用户命令的用户界面(诸如GUI)。操作请求器140也可以是在操作系统内执行并向操作发起器130提出执行操作的请求的不同程序。在一些实施例中，如果操作系统100的安全性策略不允许进行该操作(如应用程序150的签名未能被认证，或如果 应用程序150的来源不受信任)，则操作请求器140还从操作发起器130接收通知。

[0053] 操作发起器130是通过允许或阻止进行特定操作而强制执行操作系统的安全性策略的模块。操作发起器130从操作请求器140接收针对特定操作的请求。基于该请求，操作发起器130获得必要的数据对象(如应用程序150或数据文件160)。操作发起器130然后请求安全性评估器110在操作系统100的安全性策略下评估所请求的操作。操作发起器还向安全性评估器传递所接收的数据对象，该操作作为所请求的安全性评估操作的一部分。

[0054] 安全性评估器110是确定操作是否遵守操作系统的安全性策略的模块。安全性评估器110从操作发起器130接收查询，请求评估关于特定操作的安全性策略。安全性评估器110通过检查与操作相关联的数据对象来确定操作是否遵守安全性策略。例如，基于安装应用程序150的操作的请求可包括要由安全性评估器检查的若干数据对象(如针对应用程序150的安装包的安装文件以及安装程序自身)。又如，用于通过应用程序150打开数据文件

160的请求可包括用于应用程序150的可执行程序和要由安全性评估器110检查的数据文件160两者的数据对象。在一些实施例中，应用程序150和数据文件160被称为安全性评估的主题。安全性评估器110然后对从操作发起器130接收的查询做出响应。例如，如果特定操作满足安全性策略的要求，则安全性评估器通知操作发起器130安全性策略已被满足。另一方面，如果特定操作未能满足安全性策略的要求，则安全性评估器向操作发起器做出特定操作未满足安全性策略的响应。

[0055] 在一些实施例中，将安全性评估器110和规则数据库120实施为对操作系统100执行安全性评估的安全性框架180中的一部分。操作系统的其他部件能够使用由安全性框架180提供的安全性API 190执行操作的安全性评估。在图1的实例中，操作发起器130是通过API 190与安全性评估器110进行通信的操作系统100的部件。

[0056] 一旦操作发起器130从安全性评估器110接收到针对查询的响应，操作发起器130就通过允许或不允许(如阻止)特定操作继续进行来强制执行安全性策略。如果允许操作继续进行，则操作发起器130使得安装模块170、执行模块172或内容打开模块174开始执行操作请求器140所请求的 操作。如果不允许该操作，则操作发起器130通知操作请求器140，操作请求器继而通知用户并终止所请求的操作。下面的图2描述了由操作发起器130执行的示例性过程。

[0057] 嵌入到数据对象中的签名在被其接收人认证时，验证该数据对象是来自特定来源。在一些实施例中，安全性评估器110认证数据对象中的签名并查明数据对象的来源。未能生成可以由安全性评估器认证的签名(如有缺陷或不完整)的数据对象可能来自不可信任的来源。在这种情况下，安全性评估器110在操作系统的安全性策略下，通知操作发起器130阻止数据对象被执行或被打开。(在一些实施例中，未能被认证的具有签名的文档或程序不能被允许继续进行。)相反地，如果安全性评估器110能够认证数据对象的签名，则安全性评估器可以通知操作发起器其可以安全地继续进行所请求的操作，假设还满足了安全性策略下的其他要求(例如，如果数据对象的来源是可信任的)。

[0058] 由一些实施例实施的安全性策略以不同方式检查不同的数据对象。对于某些类型的数据对象，除了认证签名之外，操作系统的安全性策略可能还有需要满足的其他要求。例如，安全性策略可以要求基于一系列证书认证签名，或要求数据对象的来源是特定供应商(即使代码签名成功认证)。在一些实施例中，可以由用户改变安全性策略。例如，计算机的可信管理员可以更改操作系统的安全性策略，使得安全性评估器在无需验证或认证任何签名的情况下就可接受特定数据对象。在一些实施例中，可以对安全性评估器110任意编程以实施有关由操作发起器130提交的任何数据对象的任何安全性策略。

[0059] 在一些实施例中，将用于访问数据对象的安全性策略实施为指令集，安全性评估器110执行该组指令以便确定数据对象是否遵守安全性策略。在图1的示例性操作系统中，实施安全性策略的该组指令被存储在规则数据库120中。安全性评估器110从规则数据库120检索该组指令并使用所检索的指令(i)分析数据对象(如确定数据对象的来源是否可接受)，以及(ii)基于该分析向操作发起器130发出响应。有时将存储在规则数据库中的每组一个或多个规则称为“规范要求”，由于其指定数据对象(如可执行程序代码，诸如应用程序150或数据文件160)要求什么，以便其遵守操作 系统的安全性策略。下面的图3描述了由安全性评估器110所执行的示例性过程。下面将通过参考图9和图13更详细地描述规范要求。

[0060] 规则数据库120是存储用于实施操作系统100的安全性策略的指令集的数据库。安全性评估器110从规则数据库120检索指令集，以便对通过操作发起器130进行的安全性查询做出响应。下面参考图7-图17进一步描述规则数据库。

[0061] 图2概念性地示出了用于处理和批准所请求操作的一些实施例的操作系统的过程200。具体地，该过程请求对所请求的操作进行安全性评估并启动已经被批准的操作。在一些实施例中，过程200由操作系统100内的模块诸如图1的操作发起器130来执行。

[0062] 在接收到(在210处)操作请求(如来自操作请求器140)时，过程200开始。在一些实施例中，该请求是用于打开文档或执行应用程序的用户命令。也可以通过当前执行的应用程序或系统过程来提示请求以用于执行操作系统中的特定操作。

[0063] 接着，该过程将向安全性评估器传递(在220处)请求。在图1的实例中，该请求还包括安全性评估器在安全性策略下评估请求的安全性所需的数据对象(如应用程序150或数据文件160)。例如，由用户命令发起的打开文档的操作请求可能要求向安全性评估器传递多个数据对象，由于在一些情况下，打开文档需要调用某应用程序，并且因此，传递至安全性评估器的请求将包括文档和应用程序两者的文件句柄。

[0064] 该过程接着从安全性评估器(如110)接收(在230处)响应，并确定(在240处)是否批准所请求的操作。在一些实施例中，来自安全性评估器的响应指示(如通过通知操作发起器130)请求是否已通过操作系统的安全性策略。在一些实施例中，如果响应指示该请求已通过安全性评估(如具有认证的签名并来自可允许的来源)，则过程200使所请求的操作继续进行。在一些实施例中，如果响应指示其他情况(如安全性评估器不能认证签名或数据对象并非来自允许的来源)，则过程200终止或中断所请求的操作。

[0065] 如果请求被批准，则过程200将请求传递(在250处)到能够接收请求并执行被批准的操作的操作处理程序。如图1中所示，若干操作处理程 序能够接收请求并执行操作，包括安装模块170、执行模块172和内容打开模块174。在将请求传递至操作处理程序之后，过程200结束。

[0066] 另一方面，如果过程200不批准请求，则其向操作请求器(如图1的140)返回(在260处)默认消息，操作请求器继而通知用户(未示出)。此外，在请求未被批准时，过程200不向操作处理程序传递请求。因此，在请求未被批准时，操作处理程序，诸如170、172和174都不执行所请求的操作。在向操作请求器返回默认消息之后，过程200结束。

[0067] 一些实施例执行过程200的变型。例如，过程200的特定操作可不以所示出和所描述的确切顺序执行。可不在一个连续系列的操作中执行特定操作，并且可在不同实施例中执行不同的特定操作。

[0068] 图3概念性地示出了基于操作系统的安全性策略用于对所请求的操作执行安全性评估的示例性过程300。具体地，过程300使用规则数据库用于将请求匹配到规则，该规则使得过程能够对于所请求的操作进行安全性评估。在一些实施例中，过程300是由操作系统中的模块，诸如图1的安全性评估器110来执行的。

[0069] 在从操作发起器接收到(在310处)请求时，过程300开始。该请求指示对于特定的所请求操作需要进行安全性评估。

[0070] 接着，该过程查询(在320处)规则数据库以查找匹配规则。过程300检查规则数据库中的条目以用于匹配或适用于请求的规则。不匹配请求的规则不能用于对请求进行安全

性评估。例如，用于检查具有特定名称的应用程序的规则不能用于检查具有不同名称的应用程序。如下面将要进一步论述的，规则数据库中的多个条目可能同时匹配请求，并且将仅应用具有最高优先级的规则。

[0071] 该过程然后确定(在330处)是否已在规则数据库中查找到匹配或适用的规则。如果过程300找到至少一个匹配规则，则该过程继续进行到340。否则，过程继续进行到360。

[0072] 在360处，过程向操作发起器返回默认响应以指示没有关于请求的适用的规则或指令。在一些实施例中，默认安全性策略是不允许请求用于在规则数据库中没有匹配规则的操作。在一些实施例中，默认安全性策略允许规则数据库未特别禁止的请求。在一些实施例中，默认策略要求操作系统通知用户。在返回默认响应之后，过程300结束。

[0073] 在340处，过程对于请求做出安全性评估。在一些实施例中，过程通过向与请求相关联的数据对象(如应用程序150和/或数据文件160)应用匹配规则或适用的指令集来执行安全性评估。在一些实施例中，匹配的规则集在安全性评估器中作为可执行程序而执行。在一些实施例中，匹配的规则集使得安全性评估器基于变量，诸如数据对象的来源、数据对象的身份和数据对象的类型进行安全性评估。

[0074] 一旦进行了安全性评估，过程就向操作发起器返回(在350)安全性评估以决定是否允许继续进行所请求的操作。在向操作发起器返回安全性评估之后，过程300结束。

[0075] 一些实施例执行过程300的变型。例如，过程300的特定操作可不以所示出和所描述的确切顺序执行。可不在一个连续系列的操作中执行特定操作，并且可在不同实施例中执行不同的特定操作。

[0076] 图4-图6示出了在使用安全性评估器和规则数据库执行安全性评估时操作系统100中数据流。如图1中那样，图4-图6中的操作系统100包括安全性评估器110、规则数据库120、操作发起器130、操作请求器140、安装模块170、执行模块172和内容打开模块174。

[0077] 图4示出了在所请求的操作是用于安装应用程序时操作系统100内的数据流。在操作请求器140向操作发起器130提出安装应用程序X(操作“1”)的请求时，在操作请求器140处开始操作数据流。在一些实施例中，这种请求基于用户命令以安装应用程序X。可以通过用户界面的方式接收用户命令。

[0078] 操作发起器130然后向安全性评估器110提出在操作系统的安全性策略下评估安装应用程序X的安全性的请求(操作“2”)。在一些实施例中，对安全性评估器110做出的请求包括安装应用程序X所必需的数据对象的句柄，诸如安装文件和程序包。

[0079] 在接收到请求时，安全性评估器110查询(操作“3”)用于在安全性策略下匹配安装请求的规则或指令的规则数据库120。规则数据库向安全性评估器110提供(操作“4”)在其数据库中匹配查询的规则或指令。安全性评估器110和规则数据库120之间的这一查询过程继续，直到在规则数据库中查找匹配的规则或确定在规则数据库中没有适用的规则。

[0080] 一旦找到了匹配的规则，安全性评估器110就通过向与应用程序X的安装相关的数据对象应用匹配的规则来执行安全性评估。在一些实施例中，规则采用程序指令的形式，以用于处理数据对象并确定数据对象是否遵守操作系统的安全性策略。在一些实施例中，数据对象的处理包括在数据对象内验证与应用程序X的安装相关的签名。在一些实施例中，基于签名是否被成功认证以及签名是否来自可信来源，确定是否遵守安全性策略。然后向操作发起器130发回安全性评估(操作“5”)。在图4中所示的实例中，安全性评估器指示可以安

装应用程序X。这是安全性评估，由于已经发现与应用程序X的安装相关的数据对象遵守存储在规则数据库中的安全性策略。

[0081] 在接收到可以安装应用程序X的安全性评估之后，操作发起器130命令安装模块170启动安装程序并向计算机中安装应用程序X。执行模块172和内容打开模块174周围的虚线指示这一操作不涉及那两个模块。

[0082] 图5类似于图4，不同的是，取代示出安装操作的数据流，图5示出了在所请求的操作用于执行(如启动或调用)应用程序时操作系统100内的数据流。在操作请求器140向操作发起器提出执行应用程序X(操作“1”)的请求时，在操作请求器140处开始操作数据流。在一些实施例中，这种请求是执行应用程序X的用户命令。可以通过用户界面的方式接收用户命令。

[0083] 操作发起器130然后向安全性评估器提出在操作系统的安全性策略下评估执行应用程序X的安全性的请求(操作“2”)。在一些实施例中，这一请求包括执行应用程序X所必需的数据对象的句柄，诸如应用程序X的可执行机器代码。

[0084] 在接收到请求时，安全性评估器110查询(操作“3”)用于在安全性策略下匹配执行应用程序的请求的规则或指令的规则数据库120。规则数据库向安全性评估器110提供(操作“4”)在其数据库中满足查询的规则或指令。安全性评估器110和规则数据库120之间的这一查询过程继续，直到在规则数据库中找到匹配的规则或确定规则数据库中没有适用的规则。

[0085] 一旦找到了匹配的规则，安全性评估器110就通过向与应用程序X的执行相关的数据对象应用匹配的规则来执行安全性评估。在一些实施例中，规则采用程序指令的形式，以用于处理数据对象并确定数据对象是否 遵守操作系统的安全性策略。在一些实施例中，数据对象的处理包括在数据对象内验证与应用程序X的执行相关的签名。在一些实施例中，基于签名是否被成功认证以及签名是否来自可信来源，确定是否遵守安全性策略。然后向操作发起器130发回安全性评估(操作“5”)。在图5的实例中，安全性评估器指示可以执行应用程序X。这是安全性评估，由于已经发现与应用程序X的执行相关的数据对象遵守存储在规则数据库中的安全性策略。

[0086] 在接收到可以执行应用程序X的安全性评估之后，操作发起器130命令执行模块172启动应用程序X。安装模块170和内容打开模块174周围的虚线指示这一操作不涉及那两个模块。

[0087] 图6类似于先前两个图，不同的是，图6的数据流基于打开文档的请求。在操作请求器140向操作发起器130提出打开文档数据文件X(操作“1”)的请求时时，在操作请求器140处开始数据流。在一些实施例中，这种请求是打开数据文件X的用户命令。可以通过用户界面的方式接收用户命令。

[0088] 操作发起器130然后向安全性评估器提出在操作系统的安全性策略下评估打开数据文件X的安全性的请求(操作“2”)。在一些实施例中，这一请求包括数据文件X的句柄。如果数据文件X是要由应用程序Y打开的文档，那么在一些实施例中这一请求还包括应用程序Y的可执行二进制文件的句柄。在这种情况下，文档X和应用程序Y都被视为用于打开文档X的必要数据对象。因此，对这两个数据对象都执行安全性评估。然而，在一些实施例中，打开数据文件X所必需的应用程序已正在执行(并且因此已通过了安全性评估，诸如在图5的实

例中)。因此,仅向安全性评估器传递数据文件X的句柄作为请求的一部分。

[0089] 在接收到请求时,安全性评估器110查询(操作“3”)用于在安全性策略下匹配文档打开请求的规则或指令的规则数据库120。规则数据库向安全性评估器110提供(操作“4”)在其数据库中的规则或指令。安全性评估器110和规则数据库120之间的这一查询过程继续,直到在规则数据库中找到匹配的规则或确定规则数据库中没有适用的规则。

[0090] 一旦找到了匹配规则,安全性评估器110就向与打开数据文件X(如应用程序Y)相关的数据对象应用匹配的规则。在一些实施例中,规则采 用程序指令的形式,程序指令处理数据对象并确定那些数据对象是否遵守操作系统的安全性策略。在一些实施例中,数据对象的处理包括在与数据文件X的打开相关的数据对象内验证签名。在一些实施例中,基于签名是否被成功认证以及签名是否来自可信来源来进行确定。然后向操作发起器130发回安全性评估(操作“5”)。在图6的实例中,安全性评估器指示可以打开数据文件X。这是安全性评估,由于已经发现与数据文件X的打开相关的数据对象(如数据文件X自身和应用程序Y)遵守存储在规则数据库中的安全性策略。

[0091] 在接收到可以打开数据文件X的安全性评估之后,操作发起器130命令内容打开模块174启动应用程序X。执行模块172和安装模块170周围的虚线指示这一操作不涉及那两个模块。在一些实施例中,在打开文档需要执行计算机中当前未被执行的应用程序时,操作发起器还将启动执行模块172。

[0092] II.规则数据库

[0093] 在上述实例中,根据操作系统的安全性策略来评估与所请求的操作相关联的数据对象。这些安全性策略体现在规则数据库中存储的不同规则或指令中。因此,“操作系统的安全性策略”是一组可编程规则,其控制发生于操作系统中的操作,但不是操作系统自身的程序的一部分。如将在部分II-C所论述的,可以由计算机系统的用户或供应商来更改这些“操作系统的安全性策略”。

[0094] 在一些实施例中,规则数据库包括不同的表格以便更有效地对规则数据库进行查询。下面描述两种此类表格,权限表和高速缓存表。

[0095] A.权限表

[0096] 在一些实施例中,规则数据库包括权限表。在这样的一些实施例中,权限表包含安全性评估器为了确定是否允许在操作系统中进行特定操作而检索的规则。权限表中的规则规定为了让数据对象(如程序代码或要打开的文档)遵守计算机的安全性策略,数据对象需要什么。因此,在一些实施例中将每组一个或多个这些规则称为“规范要求”。

[0097] 规范要求能够对用于签署主题的证书表达任意条件,诸如要求证书中的供应商ID和/或公钥属于特定的可信来源。规范要求还可以要求其他东西,诸如作为这些程序的一体部分的配置词典中的条目。例如,规范要求 可以声明“必须要有允许使用地址簿的权利”(权利是包括在程序中的由一些人指定的那些配置词典之一),这与其签名毫无关系。

[0098] 图7概念性地示出了存储用于确定操作系统安全性策略的规则或指令的权限表700。权限表700包括一组条目或记录,每个条目或记录都存储指定规范要求的一组一个或多个规则或指令。可以由权限表中的一个或多个条目来表达特定的安全性策略。

[0099] 如图所示,存储设备710存储权限表700,该权限表700包括若干条目或记录,记录包括记录721、722和723。记录表达若干安全性策略,策略包括策略731、732和733。每个记录

或条目还包括一组字段741-744。字段741-743被标记为“规则1”到“规则n”。字段744被标记为“动作”。

[0100] 记录的每个字段都是一组规则或指令，该一组规则或指令指示操作系统的安全性评估器执行一组逻辑或算术操作并根据该组逻辑或算术操作做出决定。例如，记录721的字段741中的“X”可以是检查安全性评估是否是用于应用程序的一组操作，记录721的字段742中的“Y”可以是检查证书的到期日期的一组操作，记录722的字段742中的“Z”可以是验证应用程序是否来自可信供应商或来源的规则，而字段741中的“W”可以是检查正被打开的文件是否是从互联网下载的文件的规则。任何条目不必所有字段都被填充。例如，条目723仅有一个填充的规则字段(741)。记录723的该字段中的指令可以是检查请求打开的文档是否是从互联网下载的。

[0101] 记录的不同字段中的不同指令集联合进行单一确定。使用这一单一确定来决定是否应当采取“动作”字段744中声明的动作。例如，如果被评估的数据对象为应用程序，具有已在X.509标准下验证的证书并来自可信供应商，则记录722的动作字段744中的“批准”会使得安全性评估器批准启动特定应用程序的请求。另一方面，如果特定内容项是从互联网下载的，则条目723的“不批准”会使得安全性评估器不批准打开特定内容项的请求。

[0102] 此类指令或要求集合构成安全性策略。在图7的实例中，记录721中的规则或指令构成安全性策略A 731，记录722中的规则或指令构成安全性策略B 732，记录723中的规则或指令构成安全性策略C 733。在一些实施例中，安全性策略是跨越权限表中的两个或更多记录的规则的集合。下面参考图10进一步论述了此类权限表。

[0103] 在一些实施例中，一些规则用于匹配，一些规则用于验证。用于匹配的规则确定特定条目是否适用于对于安全性评估的请求。用于验证的规则确定请求是否遵守由规则表的特定条目或记录体现的安全性策略。例如，拒绝来自特定供应商的一种类型的数据对象的规则是用于验证的规则，而将规则的适用性限制到游戏应用程序的规则是用于匹配的规则。

[0104] 除了规则字段和动作字段之外，一些实施例包括其他字段。图8概念性地示出了类似于权限表700的权限表800，不同的是，除了图7中所示的规则字段和动作字段之外，权限表800还包括额外的字段。权限表800还具有多个条目(821-823)，并且每个条目都具有多个字段(840-844)。这些字段包括规则字段(841-843)和动作字段(844)。然而，与权限表700不同的是，权限表800中的每个条目还包括优先级字段840。

[0105] 一些实施例的优先级字段840决定首先检查权限表中的哪个条目以用于查找匹配请求的规则。将在具有较低优先级值的条目之前检查优先级字段中具有较高优先级值的条目。如图8中所示，记录822在优先级字段840中具有优先级值1.75，而记录823具有优先级值1.25。因此将在记录823之前搜索记录822，而将在记录822和823两者之前搜索记录821(具有优先级值2.70)。可以通过其他方式表达条目的优先级(如通过使用整数，通过在链接列表中从最高优先级到最低优先级布置条目，或通过根据优先级对条目分类)。

[0106] 对于任何给定的安全性评估请求，权限表的多个条目可以匹配请求。然而，在一些实施例中，安全性评估器在找到匹配条目时停止搜索权限表。例如，对于可能具有多个匹配的搜索，安全性评估器将仅使用第一匹配条目，即最高优先级的匹配条目。因此，使用优先级字段减小了多个匹配的可能性，确保仅将单个匹配条目用于安全性评估。

[0107] 在图7和图8的实例中，权限表中的条目包括若干字段，包括若干规则字段，每个规则字段都包含指令集以用于执行一组逻辑或算术操作。然而，一些实施例将所有规则字段中的指令集表达为单一规则并在权限表中仅具有单一规则字段。权限表的记录中的单一规则字段涵盖所有必要的指令以用于在特定安全性策略下进行安全性评估。

[0108] 图9概念性地示出了在每个记录或条目中仅包括一个规则字段的一些其他实施例的权限表900。权限表900类似于权限表800，包括优先级字段 941、动作字段943和多个条目(921-923)。然而，与包括若干规则字段的权限表800不同，权限表900仅包括一个规则字段942。

[0109] 包括用于每个记录或条目的规则字段942的规范要求包括用于针对请求来执行安全性评估的所有必要指令，包括匹配和验证指令。在一些实施例中，如前所述，规范要求可以是一组一个或多个串级的规则。在这样的一些实施例中，规范要求适用于所请求的数据对象，以便验证数据对象的来源。例如，规范要求中包括用于条目921的规则字段942的指令集能够进行如下每个确定：(1)安全性评估的请求是否针对应用程序；(2)应用程序是否来自可信供应商或来源；以及(3)证书中的来源识别信息(如供应商ID、公钥等)是否确实属于可信供应商或来源。仅在三个确定中的每一个都满足其对应的规则时，才应用动作字段943中的动作。另一方面，在三个确定的一个或多个不满足其对应的规则时，将不应用记录的动作字段。因此，由动作字段规定的动作基于针对该记录的单一规则，并且会被发送到安全性评估器(如批准或不批准所请求的动作)。

[0110] 权限表可以与图7-图10所示的那些具有不同格式。例如，在一些实施例中，权限表条目可以包括称为“禁用”的字段，使得在禁用字段包含特定值时，可以跳过该条目，并且安全性评估器将不会在搜索中考虑该条目。

[0111] 如前面参考图7所述，由规则数据库中的规则和指令表达操作系统的安全性策略。在一些实施例中，权限表中的每个条目都足以表达一个特定的安全性策略(如仅允许具有来自特定供应商的有效签名的应用程序)。在一些实施例中，可以由权限表中的两个或更多条目来表达安全性策略。

[0112] 图10示出了使用多个条目表达单一安全性策略的权限表1000。将参考图11和图12来描述图10。权限表1000类似于权限表900。其具有多个条目(1021-1027)，并且每个条目都具有三个字段(优先级字段1041、规则字段1042和动作字段1043)。然而，图10还示出了由权限表的三个条目(条目1021、1024和1026)实施的示例性安全性策略1031(“安全性策略1”)。安全性策略的三个条目具有不同的优先级(P1、P5和P8)，使得仅使用具有最高匹配优先级的条目进行安全性评估。在该实例中，P1具有最高的优先级，P5的优先级低于P1的优先级，P8具有最低的优先级。

[0113] 图11示出了用于图10的示例性安全性策略1031的一组文氏图。该图示出了三个权限表条目(P1、P5和P8)之间的逻辑关系。该图还示出了通过使用优先级构造示例性安全性策略1031。

[0114] 图11包括安全性策略1031、二维文氏图1120和三维图1130。安全性策略1031包括用于优先级P1的记录(或指令集)、用于优先级P5的记录和用于优先级P8的记录。具有优先级P1的记录中的规则(即1021)将允许“具有来自公司X的有效证书的所有文字处理应用程序”。具有优先级P5的记录中的规则(即1024)将不允许“来自公司X的应用程序”。具有优先

级P8的记录中的规则(即1026)将允许打开所有应用程序。在一些实施例中，如果已经认证了证书的签名，则认为该证书是“有效的”。

[0115] 二维文氏图1120包括三个椭圆1121-1123。三维图1130以三维方式示出了同样的三个椭圆。椭圆1121代表具有优先级P1的规则，椭圆1122代表具有优先级P5的规则，而椭圆1123代表具有优先级P8的规则。

[0116] 因此，二维文氏图1120示出了三个权限表条目之间的逻辑关系。在文氏图1120内，椭圆1123涵盖椭圆1122和1121，并且椭圆1122涵盖椭圆1121。这对应于三个记录中的规则之间的逻辑关系，其中P1规则“具有来自公司X的有效证书的所有文字处理应用程序”的适用性是P5规则“来自公司X的应用程序”的适用性的子集，并且P5规则的适用性是P8规则“所有应用程序”的适用性的子集。

[0117] 三维图示出了如何使用权限表中的优先级字段决定安全性策略1031内的哪些规则应当被应用以进行安全性评估。如图所示，椭圆1121最高，并且对应于安全性策略1031中的最高优先级规则(P1)。椭圆1122是第二高的，并且对应于安全性策略1031中的次最高优先级规则(P5)。椭圆1123是最低的，并且对应于安全性策略1031中最低优先级规则(P8)。在较高优先级规则与较低优先级规则相交时会取代较低优先级规则，正像较高优先级的椭圆无论何时与较低优先级的椭圆相交时都会遮挡较低优先级的椭圆一样。较高优先级规则的适用性有效地在较低优先级规则的适用性中冲孔。

[0118] 因此，在执行安全性评估时在没有逻辑的不一致性的情况下可以使用权限表1000中的多个条目构造安全性策略1031。使用优先级字段解决在权限表中的不同条目适用于同一请求时使用哪些规则的问题。

[0119] 图12示出了用于另一示例性安全性策略1231的一组文氏图。该图示出了三个权限表条目(P1、P5和P8)之间的逻辑关系。该图还示出了通过使用优先级来构造示例性安全性策略1231。与安全性策略1031中的权限表条目不同，安全性策略1231中的权限表条目未必是彼此的子集。

[0120] 图12包括安全性策略1231、二维文氏图1220和三维图1230。安全性策略1231包括用于优先级P1的记录(或指令集)、用于优先级P5的记录和用于优先级P8的记录。具有优先级P1的记录中的规则将允许“具有有效证书的所有文字处理应用程序”。具有优先级P5的记录中的规则将不允许“来自公司X的应用程序”。具有优先级P8的记录中的规则将允许打开具有有效证书的所有应用程序。

[0121] 文氏图1220包括三个椭圆1221-1223。三维图1230以三维方式示出了同样的三个椭圆。椭圆1221代表具有优先级P1的规则，椭圆1222代表具有优先级P5的规则，并且椭圆1223代表具有优先级P8的规则。

[0122] 因此，二维文氏图示出了三个权限表条目之间的逻辑关系。在文氏图1220内，椭圆1223涵盖椭圆1221，而椭圆1222与椭圆1221和1223两者重叠。这对应于三个记录中规则之间的逻辑关系。具体地，P1规则“具有有效证书的所有文字处理应用程序”的适用性是P8规则“具有有效证书的所有应用程序”的适用性的子集。P5规则不允许“来自公司X的东西”的适用性与P1和P8记录两者都相交，但不是它们的子集或它们的超集。

[0123] 三维图1230示出了如何使用权限表中的优先级字段决定安全性策略1231内的哪些规则应当被应用以进行安全性评估。如图所示，椭圆1221最高，并且对应于安全性策略

1231中的最高优先级规则(P1)。椭圆1222是第二高的，并且对应于安全性策略1231中的次最高优先级规则(P5)。椭圆1223是最低的，并且对应于安全性策略1231中最低优先级规则(P8)。在较高优先级规则与较低优先级规则相交时会取代较低优先级规则，正像较高优先级的椭圆无论何时与较低优先级的椭圆相交时都会遮挡较低优先级的椭圆一样。

[0124] 因此，在执行安全性评估时在没有逻辑的不一致性的情况下可以使用权限表中的多个条目构造安全性策略1231。使用优先级字段解决在权限表中不同条目适用于同一请求时使用哪些规则的问题。例如，具有来自公司X的有效证书的文字处理器的请求会导致文字处理器被批准，由于规则 “具有有效证书的所有文字处理应用程序”具有比不允许“来自公司X的东西”较高的优先级。又如，具有来自公司X的有效证书的Web浏览器的请求将不会被批准，由于规则不允许“来自公司X的东西”具有比“具有有效证书的所有应用程序”较高的优先级。

[0125] 对于一些实施例而言，图13概念性地示出了通过使用权限表来执行安全性评估的过程1300。该过程接收安全性评估请求并将权限表的条目(或记录)与请求匹配。该过程然后通过验证请求的数据对象是否遵守存储在权限表中的规范要求来执行安全性评估。

[0126] 在过程1300(在1310处)接收到查询或请求以进行安全性评估时，过程1300开始。请求伴有数据对象(如应用程序代码、安装包或要打开的文档)，存储在权限表中的规范要求将应用于数据对象。

[0127] 该过程接着从数据对象提取(在1320处)代码签名。在一些实施例中，从由数据对象的来源发出的公钥证书提取签名。该过程然后确定(在1325处)所提取的签名是否被认证。在一些实施例中，安全性评估器中的独立模块执行代码签名认证(如代码签名验证器模块)。一旦已经提取了代码签名，该过程就使用代码签名验证器模块检查是否已成功认证了代码签名。如果签名被成功认证，则过程继续进行到1330。如果签名未被成功认证，则过程1300结束。

[0128] 过程接着在权限表中查找(在1330处)最高优先级条目。在一些实施例中，过程1300比较权限表中每个条目的优先级字段，以便确定哪个条目具有最高优先级。该过程然后确定(在1340处)是否已找到了条目。在一些实施例中，这是通过记录哪些条目已被检查过来完成的。如果权限表中的所有条目都已经被检查了，那么就没有更多条目要查找。如果找到了最高优先级条目，则过程继续进行到1350。如果权限表中没有更多条目要检查，则过程1300结束。

[0129] 在1350处，过程从被找到的权限表条目检索规范要求。该过程然后使用(在1360处)检索到的规范要求来验证数据对象的来源。此类验证可以包括验证用于生成签名的供应商ID和证书的到期日期。还使用检索到的规范要求来验证数据对象的其他所需属性，诸如数据对象类型、数据对象名称的属性或可能与数据对象相关联的任何其他属性。因此，例如，即使该过程能够认证来自数据对象的签名，如果数据对象不满足规范要求(例 如，如果其没有正确的类型或不是来自被认为可信任的来源)，该过程仍然可以拒绝数据对象。

[0130] 该过程然后确定(在1370处)规范要求是否匹配或适用于查询。不能基于不适用于请求的规范要求进行安全性评估。一些实施例直到过程的这一点之前都不检查规范要求的适用性，由于在过程使用规范要求处理请求的数据对象之前，有时不能确定规范要求的适用性。在一些实施例中，一旦有了充分的信息，过程就检查规范要求的适用性。如果规范要

求匹配(即适用于)查询,该过程就继续进行到1390。否则,该过程继续进行到1380。

[0131] 在1380处,为了得到次最高优先级条目该过程搜索权限表。一些实施例标记先前检查过的较高优先级条目,并且次最高优先级条目只不过是尚未标记过的最高优先级条目。该过程接着确定(在1325处)是否找到了条目。如果找到,过程返回到1330。否则,过程1300结束。

[0132] 在1390处,过程使用规范要求确定应当由操作发起器采取的动作。在一些实施例中,根据数据对象是否已满足规范要求,由匹配条目的动作字段指定这一动作(即,批准或不批准)。在对请求做出响应之后,过程1300结束。

[0133] B.高速缓存表

[0134] 在一些实施例中,使用权限表中的条目来执行安全性评估可能包括很多计算。在一些实施例中,验证嵌入到证书的信息的规则可能包括计算密集型操作。此外,跨过权限表中很多条目的遍历对完成对匹配请求的条目的搜索可能是必要的。例如,为了确保请求没有匹配条目,权限表的完整遍历可能是必要的。一些实施例通过仅对尚未评估的数据对象执行安全性评估操作而节省了安全性评估时间。换句话讲,仅在第一次启动应用程序时或仅在第一次打开数据文件时,才对权限表进行查询。

[0135] 为了进一步加快安全性评估操作,一些实施例的规则数据库除了权限表之外还纳入了高速缓存表。在一些实施例中,高速缓存表在由对于数据对象而言唯一的散列值索引的地址位置中存储该数据对象所需的动作。例如,可以为应用程序或数据文件计算唯一代码目录散列值。因此,请求对应用程序或打开档案文件(下面将参考图24和图25在部分IV中更详细地描述)的执行(或安装)进行安全性评估仅需要计算可执行应用程序、安 装文件或档案文件的散列值。然后从由散列索引值指向的高速缓存表中的地址位置检索动作(如批准或不批准)。

[0136] 与权限表的查询不同,高速缓存表的查询不需要遍历多个条目,也不需要根据规则进行冗长的计算。因此能够大大加快对涉及具有在高速缓存表中的对应条目的数据对象的操作进行评估的请求。在一些实施例中,在搜索权限表之前安全性评估的请求首先尝试在高速缓存表中查找匹配条目。高速缓存表也称为对象表,由于高速缓存表中的每个条目对应于一个数据对象(如可执行应用程序或文档)。由于用户倾向于与他们最近交互过的(并且因此在高速缓存表中具有条目)数据对象进行交互,所以使用高速缓存表显著减少了安全性评估时间。

[0137] 对于一些实施例而言,图14示出了包括权限表1410和高速缓存表1460的规则数据库1400。该图还示出了高速缓存表的示例性条目以及高速缓存表条目和权限表条目之间的关系。在一些实施例中,权限表和高速缓存表存储在独立的物理存储中,而在其他实施例中,权限表和高速缓存表存储在单一物理存储中。

[0138] 权限表1410与图9的权限表900具有相同的格式和内容,包括记录条目1421-1423、优先级字段1440、规则字段1441和动作字段1442。

[0139] 高速缓存表1460包括三个条目1471-1473。与权限表的条目不同的是,高速缓存表的条目不包括规则字段。然而,高速缓存表包括其他字段,包括散列ID字段1491、到期日期字段1492、动作字段1493和参考字段1494。

[0140] 高速缓存表1460的条目1471基于匹配权限表1410的条目1421的数据对象(数据对

象A)。高速缓存表1460的条目1472基于匹配权限表1410的条目1422的另一数据对象(数据对象B)。在一些实施例中,在基于数据对象A和B做出安全性评估请求时生成这些高速缓存表条目。条目1473基于不匹配权限表1410中任何条目的数据对象(数据对象C)。在权限表1410未能为涉及数据对象C的安全性评估请求产生匹配规则时,在高速缓存表1460中生成负条目1473。因此,在高速缓存表中存在此类负条目阻止了权限表1410的冗长的、穷举的搜索。

[0141] 由于其是从没有权限表1410中的匹配条目的对象生成的,则高速缓存表的负条目1473不会从权限表继承任何字段。在一些实施例中,负条目包 括这样的指示:这是一个负条目,并且在权限表1410中没有针对数据对象的匹配条目。在一些这样的实施例中,权限表包含“虚拟”条目,它们不被正常处理,而是为高速缓存表中的负条目充当锚以向回参照。换句话讲,由于确定没有规则适用而创建的高速缓存记录(即负条目)将参照存储在权限表中的虚拟“无权限”规则(即,虚拟条目)。这样做主要是确保数据结构中的一致性,并且不影响这些实施例的可见行为。

[0142] 高速缓存表条目中的动作字段1493记录着对数据对象实际采取的动作。此动作基于存储在权限表1410中的匹配规则的应用程序,批准或不批准数据对象。例如,高速缓存表条目1472的动作字段对对象B指示“不批准”。这指示用于对象B的匹配规则(存储在权限表条目1422中)将对象B评估为未能满足其规范要求并且不批准对象B。由基于对象B的下一个请求进行的对在高速缓存表中的该条目的检索将也不被批准。换句话讲,每个高速缓存表条目的动作字段1493存储该条目的数据对象的安全性评估。

[0143] 到期日期字段1492指示高速缓存条目何时到期。在一些实施例中,由数据对象的内容确定针对数据对象的高速缓存表条目的到期日期。一些实施例使用数据对象证书的到期日期作为高速缓存条目中的到期日期。对于数据对象,数据对象的签名从一系列证书中导出,在这些实施例中的一些中将使用最早到期的证书的到期日期。在一些实施例中,由权限表中的规则确定到期日期并在创建高速缓存表条目时插入到高速缓存表中。在一些实施例中,操作系统基于除数据对象证书之外的信息来自己指定到期日期。在一些实施例中,此类信息可以是由供应商提供的默认值、所请求的操作类型或对操作系统可用的任何其他信息。

[0144] 在一些实施例中,安全性评估器在应用条目之前检查高速缓存表条目的到期日期字段。根据到期日期已到期的高速缓存表条目将被安全性评估器忽略(并作为高速缓存缺失处理)。这阻止了安全性评估器基于高速缓存表1460中过时的条目做出不正确的安全性评估。在一些实施例中,在访问到期高速缓存表条目时清除它。一些实施例包括清除机制,该清除机制为了找到到期的条目而周期性地检查高速缓存表,并将这些到期的条目从表中移除。

[0145] 散列ID字段1491存储散列值。在一些实施例中,高速缓存表条目的散列ID字段存储与高速缓存表条目的数据对象的散列相关联的值。一些其他实施例不包括高速缓存表中的这个字段。

[0146] 在一些实施例中,参考字段1494存储返回到权限表中的条目的链接。具体地,每个高速缓存表条目的参考字段1494都存储返回到用于生成高速缓存表条目的权限表条目(即用于对与高速缓存表条目相关联的数据对象执行安全性评估的权限表条目的规则)的链

接。例如，高速缓存表条目1471的参考字段将指示高速缓存表条目1471是从权限表条目1421生成的，并且高速缓存表条目1472的参考字段将指示高速缓存表条目1472是从权限表条目1422生成的。

[0147] 一些实施例使用高速缓存表中的参考字段来清除由于权限表的变化而变得过时的高速缓存表条目。在一些实施例中，高速缓存表还包括从权限表继承的优先级字段(未示出)。一些实施例使用高速缓存表中的优先级字段来清除由于权限表的变化而变得过时的高速缓存表条目。下面将在部分II-C中并参考图18进一步描述高速缓存表条目的清除。

[0148] 在一些实施例中，高速缓存表1460包括其他字段。这些高速缓存表字段中的一些的内容是从用于创建高速缓存表条目的权限表条目继承的。在一些实施例中，高速缓存表中的条目未必是连续的，由于它们的地址是由用于产生那些条目的数据对象的散列值来确定的。在一些实施例中，通过对数据对象执行散列操作来产生数据对象的散列值。在一些实施例中，散列操作产生相对于任何其他数据对象唯一地标识该数据对象的散列值。在一些实施例中，散列操作包括递增的散列操作。例如，可以在如美国专利7,103,779中找到递增散列操作的描述，该专利据此以引用方式并入本文。

[0149] 在一些实施例中，散列操作包括代码目录散列操作。在一些实施例中，代码目录散列是引用高速缓存表中每个唯一条目的唯一值。因此，在高速缓存表中通过唯一的代码目录散列唯一地标识了具有其对应的规范要求的每个数据对象。可以在美国专利公开2008/0168553中找到代码目录的散列及其功能的描述，该专利公开据此以引用方式并入本文。

[0150] 在图14的实例中，在由对象A的散列值索引的位置处存储对象A的条目(1471)，在由对象B的散列值索引的位置处存储对象B的条目 (1472)，并且在由对象C的散列值索引的位置处存储对象C的条目(1473)。

[0151] 对于一些实施例而言，图15示出了基于来自操作发起器的请求来使用权限表和高速缓存表两者以用于进行安全性评估的安全性评估器1500。如图所示，安全性评估器1500从操作发起器1505接收请求并查询权限表1510和高速缓存表1515两者。安全性评估器1500包括用于查询权限表的查询管理器1520和用于查询高速缓存表的查询管理器1525。安全性评估器1500还包括处理器1530和高速缓存表记录生成器1540。用于查询权限表1510的查询管理器1520还包括规则引擎1550、记录选择器1560和签名验证器1570。

[0152] 操作发起器1505做出安全性评估请求并等待来自安全性评估器的处理器1530的安全性评估的结果。处理器1530从操作发起器1505接收安全性评估请求。基于这一所接收的安全性评估请求，处理器与查询管理器1520(用于权限表)和1525(用于高速缓存表)两者都进行通信，以便确定是否批准安全性评估请求。在高速缓存表1515中有高速缓存缺失时，其还使用高速缓存表记录生成器1540生成新的高速缓存条目。高速缓存表记录生成器还用于通过对作为请求的主题的数据对象(即程序代码或文档)进行散列化来生成指向高速缓存表1515的物理存储器的地址。

[0153] 用于查询高速缓存表的查询管理器1525提供了处理器1530和包含高速缓存表1515的物理存储器之间的接口。用于查询权限表的查询管理器1520提供了处理器1530和包含权限表1510的物理存储器之间的接口。查询管理器1520还使用记录选择器1560以从权限表1510选择和检索条目。然后将已检索的条目中继到规则引擎1550以进行解析并执行。在一些实施例中，查询管理器1520使用签名验证器1570来验证数据对象的代码签名。在这样

的一些实施例中，如果代码签名由于任何原因未能正确认证，则安全性评估器1500向操作发起器1505返回不批准的消息。在一些实施例中，规则引擎1550、记录选择器1560和签名验证器1570的功能是由处理器1530而非查询管理器1520执行的。

[0154] 签名验证器模块1570认证数据对象的代码签名。在一些实施例中，签名验证器模块通过使用公钥证书中的信息以及数据对象自身的内容来认证签名。签名验证器模块根据由证书标识的签名认证算法来执行签名认证操 作。在完成签名认证过程时，签名验证器模块通知安全性评估器1500是否成功认证数据对象的签名。

[0155] 图16示出了通过安全性评估器1600为数据对象生成并存储高速缓存表条目。具体地，该图示出了在基于数据对象向安全性评估器提出请求时，高速缓存表条目中不同字段的生成。图16示出了权限表1605、高速缓存表1610和针对数据对象1625向安全性评估器1600提出请求的操作发起器1620。高速缓存表包括条目1611-1613。

[0156] 安全性评估器1600包括用于权限表的查询管理器1630、散列模块1650、存储器接口1660和到期日期提取模块1670。对于一些实施例而言，查询管理器1630类似于图15中的查询管理器1520，而散列模块1650和到期日期提取模块1670的功能是由类似于图15的处理器1530的处理器执行的。安全性评估器1600还包括其他模块，诸如签名验证器模块，为了简化附图该签名验证器模块未被示出。

[0157] 操作发起器1620向安全性评估器1600提出对需要使用数据对象1625(“数据对象X”)的操作进行安全性评估的请求。将数据对象1625中继到安全性评估器1600中的若干模块，这些模块包括查询管理器1630、散列模块1650和到期日期提取模块1670。查询管理器1630从权限表1605查找匹配数据对象1625的条目。查询管理器然后应用匹配条目的规则确定用于数据对象1625的适当动作。由查询管理器采取的这一动作形成用于新高速缓存表条目1612的动作字段1642。

[0158] 散列模块1650接收数据对象1625并对所接收的数据对象执行散列操作。在一些实施例中，散列操作是递增散列操作。散列模块1650产生唯一代码目录散列值1655，其充当索引(“针对X的索引”)以用于指定为数据对象X新创建的高速缓存表条目的高速缓存表中的位置。存储器接口1660然后使用这个值作为高速缓存表的物理地址。在一些实施例中，该唯一生成的代码目录散列值将被存储在数据对象X的条目1612的散列ID字段中。

[0159] 到期日期提取模块1670也接收数据对象1625，从数据对象1625计算或提取到期日期。在一些实施例中，数据对象的到期日期由用于生成数据对象的签名的证书指定。数据对象可以从超过一个证书甚至一系列证书中导出其签名。对于此类数据对象，一些实施例使用这些证书中最早的到期 日期作为高速缓存表条目的到期。所提取的到期日期变成到期日期字段1675。在一些实施例中，到期日期提取模块1670使用其他信息作为确定到期日期的依据。在一些其他实施例中，到期日期字段1675是从权限表继承的，并非是由到期日期提取模块1670计算的。

[0160] 将动作字段1642和到期日期字段1675串级在一起以连同针对数据对象X的散列ID字段和参考字段来形成针对数据对象X的新高速缓存表条目1612。高速缓存表1610具有针对两个其他对象的两个其他条目(针对数据对象Y的条目1611和针对对象Z的条目1613)。

[0161] 在一些实施例中，可以在运行类似操作系统的不同计算机之间共享高速缓存表的内容。一台计算机能够导入由另一计算机生成的高速缓存表或由操作系统的供应商提供的

预封装高速缓存表。使用这样一种预填充的高速缓存表的计算机能够立即加快其安全性评估操作而不必生成其自身的高速缓存条目。

[0162] 对于一些实施例而言，图17概念性地示出了使用权限表和高速缓存表两者以用于执行安全性评估的过程1700。该过程首先尝试在高速缓存表中找到匹配条目。如果该过程不能在高速缓存表中找到此类条目(即高速缓存缺失)，则其将查询权限表以找到替代的匹配条目。查询权限表使在高速缓存表中获得新的条目。在一些实施例中，这个过程是由操作系统的安全性评估器执行的。

[0163] 在操作发起器提出对操作(如执行应用程序、安装应用程序或打开文档)的请求时，过程1700开始。该过程(在1710处)接收这一请求和所请求的操作所需的数据对象。

[0164] 该过程接着确定(在1720处)数据对象的散列值(即，唯一代码目录散列值)。在一些实施例中由递增的散列操作计算散列值。所计算的散列值充当索引，用于在数据对象的高速缓存表中定位条目。接着，该过程确定(在1730处)其是否能够通过使用散列值找到高速缓存表条目。在一些实施例中，这一确定基于在由散列值指向的位置处是否存储了有效的条目。在这些实施例的一些中，每个高速缓存表条目都与指示高速缓存表条目是否有效的位相关联。如果高速缓存表条目未被数据对象的高速缓存条目填充，或者如果高速缓存表条目已被清除且尚未用新的高速缓存条目进行填充，则该高速缓存表条目是无效的。如果该过程能够使用数据对象的 散列值找到有效条目(高速缓存命中)，则该过程继续进行到1740。否则(高速缓存缺失)，该过程继续进行到1750。

[0165] 在1740处，该过程基于匹配高速缓存表条目的内容确定对安全性评估请求的响应。该过程然后确定(在1780处)响应是否是批准所请求的操作。如果响应批准该操作，则过程继续进行到1790，在1790中，操作发起器向操作处理程序，诸如图1的执行模块172、安装模块170或内容打开模块174传递请求。如果响应不批准该操作，则操作发起器通过不向操作处理程序传递请求来阻止操作继续进行。在基于高速缓存表条目的内容对操作发起器做出响应之后，过程1700结束。

[0166] 在1750处，由于在高速缓存表处的高速缓存缺失，过程查询权限表。在一些实施例中，这一操作是由图13的过程1300执行的，其搜索权限表以查找匹配请求的条目。

[0167] 接着，该过程确定(在1755处)其是否能够在权限表中找到匹配条目。如果能，该过程继续进行到1760。否则，该过程继续进行到1770以为数据对象创建负高速缓存条目，后结束。如上所述，数据对象的负定高速缓存条目使得安全性评估器能够快速探知操作系统的安全性策略没有适用于特定请求的规则。

[0168] 在1760处，过程从权限表的匹配条目确定响应。该过程接着基于来自权限表的这一匹配条目在高速缓存表中创建(在1765处)新条目。过程然后继续进行到1780以确定批准还是不批准所请求的操作。在基于权限表条目的内容对操作发起器做出响应之后，过程1700结束。

[0169] C.用户覆写

[0170] 在一些实施例中，允许具有足够特权的用户通过添加、删除或修改权限表中的条目对规则数据库进行更改。例如，具有管理员特权的用户可以绕过签名认证以执行特定应用程序。用户可通过向权限表中添加取代较低先级规则的较高优先级的条目，由此允许执行特定应用程序，从而进行这种操作。

[0171] 然而，如上面的图10所示，安全性策略经常包括通过优先级链接在一起的多个表条目。因此，在安全性策略下评估数据对象需要按照由其优先级阐述的次序检查这些表条目。对于针对数据对象的任何给定安全性评 估，较低优先级规则仅在较高优先级规则不适用时才变得适用。因此，对较高优先级规则的任何改变都潜在地改变了较低优先级规则的适用性。

[0172] 由于高速缓存表存储了反映在权限表变化前的规则适用性的高速缓存条目，因此在一些实施例中，特定优先级的权限表的变化会触发高速缓存表中所有相等或较低优先级条目的清除。例如，优先级值为2.3的新权限表条目会触发清除优先级值等于或低于2.3的所有高速缓存表条目。在一些实施例中，这种清除过程使用每个高速缓存表条目中的参考字段(如图14的1494)，以得知用于创建高速缓存表条目的权限表条目的优先级。在一些其他实施例中，每个高速缓存表条目都带有为此目的而从权限表继承的优先级字段。

[0173] 在一些实施例中，假设负定高速缓存条目具有最低优先级。由于负条目是在权限表中没有匹配条目的数据对象的高速缓存表条目，因此权限表的任何变化都可能影响到负条目的数据对象(即，权限的变化可潜在地导致数据对象在权限表中具有匹配条目，从而使得负条目过时)。在这些实施例中的一些中，权限表的任何变化始终会导致负定高速缓存条目被清除。

[0174] 对于一些实施例而言，图18概念性地示出了在由管理用户改变规则数据库之后维护规则表的过程。该过程从高速缓存表清除较低优先级的条目。在特权用户(如管理员)对规则数据库做出改变时，过程1800开始。该过程从特权用户接收(在1810处)规则变化，并确定(在1820处)规则变化是否针对权限表中已经有的规则。如果规则变化针对的是权限表条目中已经有的规则，则过程继续进行到1840以更新权限表条目。如果不是，则过程继续进行到1830以在权限表中生成新的条目。

[0175] 过程接着确定(在1850处)在规则数据库中是否有优先级低于新增或更新规则的条目。如果有，该过程继续进行到1860。否则，该过程1800结束。

[0176] 在1860处，该过程删除高速缓存表中的所有较低优先级的条目。在一些实施例中，该过程检查高速缓存表中所有被占用的条目并清除优先级低于或等于新增或更新权限表条目的条目。在删除所有较低优先级高速缓存表条目(包括任何负条目)之后，过程1800结束。

[0177] III.下载内容的安全性评估

[0178] 上述实施例中的一些使用嵌入到数据对象中的证书以用于对这些数据对象进行安全性评估。在大多数情况下，这些方法依赖于由这些数据对象的来源所提供的标识符(如证书中的签名和供应商ID)。然而，这些来源提供的标识符并非始终可用或可靠。因此，作为依赖这些来源提供的标识符以用于执行安全性评估的补充或替代，一些实施例的操作系统为数据对象提供其自身的标识符。在这些实施例中的一些中，操作系统将标记与从外部来源导入的数据对象相关联，外部来源诸如是互联网、USB闪存驱动器或通过设备的任何其他外围接口。标记包括隔离位以指指出该数据对象来自外部来源。隔离位的存在进一步指出系统未对数据对象执行过安全性评估。一旦操作系统对数据对象执行了安全性评估，就更新标记(如通过移除隔离位)以指示在操作系统的安全性策略下已被评估的数据对象，并且数据对象已通过(或未通过)操作系统的安全性策略。

[0179] 图19示出了计算机1900，该计算机1900具有使用其自身的标识符以用于执行安全性评估的操作系统。具体地，计算机1900的操作系统向例如从互联网下载的内容和/或应用程序添加标记或隔离位。计算机1900包括存储设备1910、标记模块1920、当前运行于计算机1900上的应用程序1930、网络接口1940和用户界面(UI)模块1950。UI模块1950通过输入设备驱动程序1960和显示模块1970控制与用户的通信。

[0180] 网络接口1940经由网络提供计算机1900和外部世界之间的通信接口。网络允许计算机1900通过互联网1980进行通信并从其他计算机访问数据对象，诸如应用程序文件1981-1982和内容文件1983-1984。这些内容文件可以是文本文件、文字处理器文档、电子数据表、媒体文件等。应用程序文件可以包括安装和程序文件。然后可将这些应用程序和内容文件下载到计算机1900上。尽管图中未示出，但计算机1900也可从互联网之外的外部来源(诸如外部闪存驱动器)下载数据对象。

[0181] 应用程序1930是经由操作系统而当前运行于计算机1900上的程序或一组过程。应用程序1930可以是互联网浏览器、文字处理器、视频游戏、媒体编辑应用程序或能够在计算机1900上工作的任何程序。应用程序1930能够执行需要通过互联网进行通信的操作，包括经由网络接口，通过互联网从来源下载数据对象1981-1984。一旦已下载了文件，应用程序1930就 在存储设备1910中存储所下载的文件。在一些实施例中，所下载的文件在被存储之前必须要通过标记模块1920。

[0182] 标记模块1920将每个下载的文件与标记相关联。在一些实施例中，此类标记包括隔离位以指示所下载的文件来自外部来源并且未在操作系统的安全性策略下被检查。在一些实施例中，标记模块向所下载的文件上插入或附加标记。在一些实施例中，标记模块维护标记表，该标记表记录哪些文件来自互联网或其他外部来源。运行于计算机上的其他过程或模块能够访问标记表以找出将哪些文件或数据对象标记为来自诸如互联网的外部来源。在来自外部来源的文件刚被应用程序1930下载并且在文件被存储在存储设备1910中之前，一些实施例将标记与来自外部来源的文件相关联。

[0183] 存储设备1910为计算机1900存储各种数据对象。这些数据对象可包括从互联网或其他外部来源下载的内容文件和应用程序文件。在一些实施例中，将这些所下载的应用程序和内容文件与由标记模块1920提供的标记相关联。

[0184] 一旦存储并标记了所下载的文件，操作系统就能够基于考虑到数据对象是否是下载的安全性策略执行安全性评估。图20示出了操作系统2000，该操作系统2000的安全性策略要求检查标记或隔离位是否存在。具体地，操作系统2000包括用于识别在执行安全性评估操作之前数据对象是否被标记的机制。安全性评估操作类似于上面的部分I和II中描述的那些。

[0185] 如图所示，操作系统2000包括操作请求器2005、安全性评估器2020、规则数据库2030和操作发起器2010。操作发起器包括处理器2040和标记识别器模块2050。操作系统还包括安装模块2060和内容打开模块2070。

[0186] 在一些实施例中，操作系统2000类似于图1的操作系统100。具体地，像操作请求器140那样，操作请求器2005向操作发起器130提出执行操作的请求。像安装模块170和内容打开模块174那样，安装模块2060和内容打开模块2070是接收批准的请求并执行批准的操作的操作处理程序。

[0187] 安全性评估器2020和规则数据库2030执行与图1所示的安全性评估器110和规则数据库120类似的操作。安全性评估器和规则数据库的功能也在上面部分II中参考图7-图17进行了描述。例如，在一些实施例中，规则数据库2030包括权限表和高速缓存表。在一些实施例中，安全性评估器 2020基于用户输入执行对被标记对象的安全性评估。例如，在接收到对被标记对象进行安全性评估的请求时，安全性评估器2020通知用户所请求的操作涉及下载的对象并询问用户是否继续了解风险。

[0188] 像操作发起器130那样，操作发起器2010通过允许或不允许进行特定操作来强制执行操作系统的安全性策略。其从操作请求器2005接收对特定操作的请求并请求安全性评估器2020在操作系统2000的安全性策略下评估所请求的操作。然而，与图1的操作发起器130不同的是，操作发起器2010检查用于所请求的操作的数据对象是否被标记为来自互联网或任何其他外部来源。被标记为来自外部来源(如利用隔离位进行标记)的数据对象要接受安全性评估。为了避免对已被评估的数据对象进行重复安全性评估，一些实施例在安全性评估表明数据对象先前已被评估之后更新标记。一些实施例通过移除隔离位来实现这一目的。在一些实施例中，更新的标记还指示数据对象是否已通过先前的安全性评估。

[0189] 在图20的实例中，操作发起器2010内部的标记识别器模块2050检查标记并向处理器模块2040报告。在操作系统2000中，安全性评估器2020不基于标记进行其安全性评估。是操作发起器2010内的处理器2040使用标记来决定是否继续进行所请求的操作。在这些实施例的一些中，只有在与所请求的操作相关联的数据对象被标记为来自外部来源并且从未被评估过时，操作发起器2010才继续进行安全性评估。如果未如此标记过数据对象(例如，如果已经移除了隔离位或者如果已经将数据对象标记为先前已被评估过)，则操作发起器2010将不请求安全性评估器来执行安全性评估。

[0190] 图21-图22示出了在使用识别数据对象中的标记的操作发起器执行安全性评估时，操作系统2000中的数据流。如图20中那样，图21-图22中的操作系统2000包括安全性评估器2020、规则数据库2030、操作发起器2010、操作请求器2005、安装模块2060和内容打开模块2070。

[0191] 图21示出了向操作系统2000中安装应用程序的操作的数据流。在操作请求器2005向操作发起器2010提出安装应用程序X(操作“1”)的请求时，该操作在操作请求器处开始。处理器2040然后向标记识别器模块2050发送命令以询问应用程序X是否被标记(操作“2”)。如果应用程序X被标记为来自外部来源(如具有隔离位)，则标记标识符2050向处理 器2040发送确认(操作“3”)，并且处理器继而向安全性评估器2020提出执行安全性评估的请求(操作“4”)。另一方面，如果应用程序X未被标记，或者如果应用程序X被标记为先前已被评估过(或已经移除了其隔离位)，则在一些实施例中，处理器2040将不会请求安全性评估器2020执行安全性评估。在一些实施例中，如果应用程序X被标记为未通过先前的安全性评估，则处理器2040可立即结束安装过程而不涉及安全性评估器2020。相反地，如果应用程序X被标记为已通过先前的安全性评估，则在一些实施例中，处理器2040可立即允许应用程序X继续进行而不涉及安全性评估器2040。

[0192] 如果已经提出安全性评估请求，则安全性评估器2020查询规则数据库2030(操作“5”)。规则数据库2030向安全性评估器2020提供(操作“6”)其数据库中的规则或指令。安全性评估器2020和规则数据库2030之间的这一查询过程继续，直到在规则数据库中找到匹配

的规则或直到确定规则数据库中没有适用的规则。

[0193] 一旦找到了匹配的规则，安全性评估器2020就向与应用程序X的安装相关的数据对象应用匹配的规则。然后向操作发起器2010发回安全性评估(操作“7”)。在图21的实例中，从安全性评估器回到操作发起器的通信指示可以安装应用程序X，由于已经发现与应用程序X的安装相关的数据对象遵守存储在规则数据库中的安全性策略。

[0194] 在知道应用程序X已通过了安全性评估器2020执行的安全性评估时，处理器2040确定是否继续进行应用程序X的安装。除了安全性评估器进行的安全性评估之外，在一些实施例中，处理器2040考虑应用程序X是否被标记。如果处理器决定可以继续进行应用程序X的安装，则其向安装模块2060发送命令以启动应用程序X的安装(操作“8”)。内容打开模块2070周围的虚线指示其在这个操作中不被涉及。

[0195] 图22示出了在操作系统2000中打开文档的操作的数据流程图。在操作请求器2005向操作发起器2010提出打开数据文件X(操作“1”)的请求时，该操作在操作请求器2005处开始。处理器2040然后向标记识别器模块2050发送命令以询问数据文件X是否被标记(操作“2”)。如果数据文件X被标记为来自外部来源(如具有隔离位)，则标记识别器2050向处理器2040发送确认(操作“3”)，并且处理器继而向安全性评估器 2020提出执行安全性评估的请求(操作“4”)。另一方面，如果数据文件X未被标记，或者如果数据文件X被标记为先前已被评估过，则在一些实施例中，处理器2040将不会请求安全性评估器2020执行安全性评估。在一些实施例中，如果数据文件X被标记为未通过先前的安全性评估，则处理器2040可立即结束文件打开过程而不涉及安全性评估器2020。相反地，如果数据文件X被标记为已通过先前的安全性评估，则在一些实施例中，处理器2040可立即允许数据文件X的打开继续进行而不涉及安全性评估器2040。

[0196] 如果已经提出安全性评估的请求，则安全性评估器2020然后查询规则数据库2030(操作“5”)。规则数据库2030向安全性评估器2020提供(操作“6”)其数据库中的规则或指令。安全性评估器2020和规则数据库2030之间的这一查询过程继续，直到在规则数据库中找到匹配的规则或直到确定规则数据库中没有适用的规则。

[0197] 一旦找到了匹配的规则，安全性评估器2020就向与数据文件X的打开相关的数据对象应用匹配的规则。然后向操作发起器2010发回安全性评估(操作“7”)。在图22的实例中，从安全性评估器回到操作发起器的通信指示可以打开数据文件X，因为已发现数据文件X遵守存储在规则数据库中的安全性策略。

[0198] 在知道数据文件X已通过了安全性评估器2020所执行的安全性评估时，处理器2040确定是否继续进行数据文件X的打开。除了由安全性评估器进行的安全性评估之外，在一些实施例中，处理器2040还考虑数据文件X是否被标记。如果处理器决定可以继续进行数据文件X的打开，则其向内容打开模块2070发送命令以启动数据文件X的打开(操作“8”)。安装模块2060周围的虚线指示其这个操作中不被涉及。

[0199] 图20-图22示出了具有操作发起器2010的操作系统2000，操作发起器2010决定是否将数据对象标记为来自外部来源诸如互联网。操作系统2000的操作发起器2010还基于标记确定是否继续进行操作。存储在规则数据库中的规则不考虑或处理该标记。然而，在一些其他实施例中，操作系统的规则数据库包括识别标记并基于所识别的标记进行安全性评估的规则。

[0200] 对于一些实施例而言，图23示出了操作系统2300，其包括规则数据库，该规则数据库具有用于处理与下载的数据对象相关联的标记的规则。在一些这样的实施例中，操作发起器不检查与所请求的操作相关联的数据对象的标记。像操作系统2000那样，操作系统2300包括操作请求器2305、安全性评估器2320、规则数据库2330和操作发起器2310。操作系统还包括安装模块2360和内容打开模块2370。

[0201] 操作发起器2310从操作请求器2305接收对操作的请求并向安全性评估器2320提出进行安全性评估的请求。然而，与操作发起器2010不同的是，操作发起器2310不对下载的标记执行检查。

[0202] 安全性评估器2320从操作发起器2310接收对安全性评估的请求并查询规则数据库以用于查找匹配与每个安全性评估请求相关联的数据对象的规则。

[0203] 规则数据库2330存储用于执行安全性评估的规则。与规则数据库2030不同的是，规则数据库2330还包括用于分析数据对象以查看它们是否被标记的规则。如果数据对象被标记，则一些实施例然后继续应用规则数据库中的规则以对数据对象执行安全性评估并批准/不批准所请求的操作。在一些实施例中，规则数据库2330包括权限表和高速缓存表两者，如较早在部分II中描述的那样。例如，由于其隔离位而未被较早的安全性评估批准的数据对象可能具有带有不批准数据对象的动作字段的高速缓存条目。

[0204] IV.文档的安全性评估

[0205] 由于用于识别数据对象来源的签名是部分基于数据对象的内容而导出的，因此可以使用签名以测试数据对象是否已经改变。这也意味着其内容被用户频繁改变的数据对象(例如文档)不能具有其自身的签名。然而，可将数据文件置入能够承载包括签名的证书的结构(诸如档案文件)中。可使用此类签名来安全性地识别该结构中的数据文件的来源。在一些实施例中，操作系统包括规则数据库中的规则，其基于嵌入档案文件结构中的证书中的标识符，批准或不批准文档或数据文件。这些实施例中的一些将获批准档案文件中的文档也视为被批准。

[0206] 图24示出了接收并存储具有证书的数据档案文件的计算机2400。然后可由计算机2400的操作系统使用(带签名)证书来安全性地识别档案文件内的内容的来源。如图所示，计算机2400包括存储设备2410、当前运行 于计算机2400上的应用程序2430、网络接口2440和用户界面(UI)模块2450。UI模块2450通过输入设备驱动程序2460和显示模块2470来控制与用户的通信。

[0207] 网络接口2440经由网络提供计算机2400和外部世界之间的通信接口。网络允许计算机2400通过互联网进行通信并从其他计算机访问数据对象，诸如数据档案文件2481-2484。这些档案文件的内容可以是文本文件、文字处理器文档、电子数据表、媒体文件等。这些档案文件的内容也可以是可执行应用程序或应用程序安装文件。这些数据档案文件中的一些或全部具有证书，证书具有识别其来源的签名。数据档案文件可包含一条内容(诸如数据档案文件2481)或多条内容或文件(诸如数据档案文件2484)。尽管图中未示出，但计算机2400也可通过诸如外部闪存驱动器的其他数据通信装置来从其他计算机访问数据档案文件。

[0208] 应用程序2430是经由操作系统当前运行于计算机2400上的程序或一组过程。应用程序2430可以是互联网浏览器、文字处理器、视频游戏、媒体编辑应用程序或能够在计算机

2400中工作的任何程序。应用程序2430能够执行需要与互联网进行通信的操作，包括经由网络接口2440从互联网下载数据档案文件2481-2484。

[0209] 一旦下载了数据档案文件，应用程序2430就在存储设备2410中存储所下载的文件。向存储设备2410中存储数据档案文件的操作类似于较早参考图19描述的存储被标记或被隔离的数据的操作。存储设备2410存储数据档案文件。一旦存储了数据档案文件，操作系统就能够通过认证签名并检查嵌入数据档案文件中的证书来执行安全性评估。

[0210] 图25示出了包括用于基于数据档案文件的证书对数据文件或文档进行安全性评估的规则数据库中的规则的操作系统。具体地，图25示出了在操作系统2500中打开数据文件的示例性请求。数据文件嵌入数据档案文件中。

[0211] 操作系统2500包括操作请求器2505、安全性评估器2520、规则数据库2530、操作发起器2510和内容打开模块2570。操作系统2500还具有对存储设备2560的访问权限，该存储设备2560存储若干数据档案文件，包括数据档案文件2580。在一些实施例中，存储设备2560包括图24的存储装置2410，其存储从互联网或其他外部来源下载的数据档案文件。

[0212] 在一些实施例中，操作系统2500类似于图1的操作系统100。具体地，操作请求器2505，像操作请求器140那样，向操作发起器2510提出执行操作的请求。操作发起器2510从操作请求器2505接收请求并向安全性评估器2520提出进行安全性评估的请求。在图25所示的实例中，该请求用于打开嵌入数据档案文件2580中的文档或数据文件。操作发起器2510通过向安全性评估器传递数据档案文件2580来向安全性评估器2520提出请求。一旦操作发起器2510从安全性评估器2520接收到了响应，该操作发起器2510就会基于安全性评估来启动内容打开模块2570或终止所请求的操作。

[0213] 安全性评估器2520和规则数据库2530执行与安全性评估器110和规则数据库120类似的操作。在一些实施例中，规则数据库包括参考图7-图17在部分II中如上所述的权限表和高速缓存表两者。为了安全性地识别数据文件或文档的来源，安全性评估器2520在应用存储在规则数据库2530中的规则之前认证签名。

[0214] 内容打开模块2570类似于图1的内容打开模块174。一旦其从操作发起器2510接收到启动命令，内容打开模块2570就继续打开所请求的数据文件。在图25的实例中，请求打开的数据文件在数据档案文件2580中，其存储在存储设备2560中。为了打开数据文件，在一些实施例中，内容打开模块2570从档案文件结构提取数据文件并且然后打开数据文件(如通过向打开数据文件所需的应用程序发送数据文件)。

[0215] 对于一些实施例而言，图26概念性地示出了对文档打开操作执行安全性评估的过程2600。具体地，由操作系统执行的过程2600基于嵌入数据档案文件中的带签名的证书进行安全性评估确定。

[0216] 在接收到打开数据文件(或文档)的请求时，过程2600开始。该过程接收(在2610处)请求打开的文档。该过程然后确定(在2620处)文档是否是安全类型的。在一些实施例中，不论其来源如何，都允许打开被认为不可能损害计算机的各种类型的文档或文件。例如，文本文件被认为是安全的、不需要签名或其他来源标识。如果文档被视为是安全类型，则该过程继续进行到2670以向操作处理程序(诸如图25的内容打开模块2570)传递文档以用于打开文档。如果文档不被视为是安全类型，则该过程继续进行到2630。在一些实施例中，可执行的文档不被认为是安全的。在一些实施例中，特定类型的不可执行的文档也需

要来源验证，由于此类不可执行文档能够携带通过打开并使用那些文档的应用程序来损害计算机的恶意代码。

[0217] 接着，该过程确定(在2630处)文档是否在档案文件中。如上所述，一些数据文件或文档没有来源标识签名，但可以将数据文件放置在携带签名的档案文件结构中。然而，在一些实施例中，特定类型的文档能够包括其自身的签名而不在档案文件中(如很少改变的文档可能携带测试文件是否被改变的签名)。如果文档在档案文件中，则过程2600继续进行到2650。否则，过程继续进行到2640以亲自对文档执行安全性评估。

[0218] 在2640处，该过程基于文档自身的证书执行安全性评估。该操作包括认证嵌入文档证书中的文档签名以及基于证书中的其他信息额外进行安全性评估。在一些实施例中，该过程查询规则数据库以查找可用于对文档进行安全性评估的匹配规则。在一些实施例中，这种操作包括向文档应用规范要求。规范要求可包括检查嵌入文档中的证书并检查来源是否可信的指令。在执行安全性评估之后，该过程基于匹配规则确定(在2660处)是否批准用于打开的文档。如果批准，该过程向操作处理程序(诸如图25的内容打开模块2570)传递(在2670处)文档以用于打开。否则该过程结束。

[0219] 在2650处，该过程基于档案文件的证书来执行安全性评估。该操作包括认证嵌入档案文件证书中的签名以及基于证书中的其他信息额外进行安全性评估。在一些实施例中，该过程查询规则数据库以查找可用于对档案文件进行安全性评估的匹配规则。在一些实施例中，这种操作包括向档案文件应用规范要求。规范要求可包括检查档案文件中的证书并检查来源是否可信的指令。该过程然后基于匹配规则确定(在2660处)是否批准档案文件，并且因此批准档案文件中的所有文档以用于打开。如果批准，该过程向操作处理程序(诸如图25的内容打开模块2570)传递(在2670处)文档以用于打开。否则该过程结束。

[0220] V.电子系统

[0221] 上述特征和应用程序中的许多可被实施为被指定为在计算机可读存储介质(还称为计算机可读介质)上记录的指令集的软件过程。在这些指令由一个或多个计算或处理单元(如一个或多个处理器、处理器的内核或者其他处理单元)执行时，这些指令使一个或多个处理单元执行指令中所指 示的动作。计算机可读介质的实例包括但不限于CD-ROM、闪存驱动器、随机存取存储器(RAM)芯片、硬盘驱动器、可擦可编程只读存储器(EPROM)、电可擦可编程只读存储器(EEPROM)等。计算机可读介质不包括无线地或通过有线连接传递的载波和电信号。

[0222] 在本说明书中，术语“软件”旨在包括驻留在只读存储器中的固件或者可被读取到存储器中以用于由处理器进行处理的存储在磁性存储装置中的应用程序。另外，在一些实施例中，可在保留独特的软件发明的同时，将多个软件发明实施为更大程序的子部分。在一些实施例中，还可将多个软件发明实施为单独的程序。最后，共同实施本文所述的软件发明的单独程序的任何组合均在本发明的范围之内。在一些实施例中，当被安装以在一个或多个电子系统上工作时，软件程序定义执行和施行软件程序的操作的一个或多个特定机器具体实施。

[0223] 图27概念性地示出了电子系统2700，本发明的一些实施例借助该电子系统来实施。电子系统2700可为计算机(如台式计算机、个人计算机、平板电脑等)、电话、PDA或任何其他种类的电子设备。此类电子系统包括各种类型的计算机可读介质以及用于各种其他类

型的计算机可读介质的接口。电子系统2700包括总线2705、一个或多个处理单元2710、图形处理单元(GPU)2715、系统存储器2720、网络2725、只读存储器2730、永久性存储设备2735、输入设备2740及输出设备2745。

[0224] 总线2705总体地代表可通信地连接电子系统2700的许多内部设备的所有系统、外围设备及芯片组总线。例如，总线2705可通信地将一个或多个处理单元2710与只读存储器2730、GPU 2715、系统存储器2720及永久性存储设备2735连接。

[0225] 一个或多个处理单元2710从这些各种存储器单元中检索将要执行的指令以及将要处理的数据以执行本发明的过程。在不同实施例中，一个或多个处理单元可为单个处理器或者多核处理器。一些指令传递至GPU 2715并且由GPU 2715执行。GPU 2715可卸载各种计算或者补偿由一个或多个处理单元2710所提供的图像处理。在一些实施例中，可使用CoreImage的内核着色语言来提供此类功能性。

[0226] 只读存储器(ROM)2730存储一个或多个处理单元2710及电子系统的其他模块所需的静态数据和指令。另一方面，永久性存储设备2735为读 写存储器设备。该设备为即使在电子系统2700关闭时也存储指令和数据的非易失性存储器单元。本发明的一些实施例将海量存储装置(诸如磁盘或光盘及其对应的硬盘驱动器)用作永久性存储设备2735。

[0227] 其他实施例将可移除存储设备(诸如软盘、闪存存储器设备等，及其对应的磁盘驱动器)用作永久性存储设备。与永久性存储设备2735类似，系统存储器2720为读写存储器设备。然而，与存储设备2735不同，系统存储器2720为易失性读写存储器，诸如随机存取存储器。系统存储器2720存储在处理器运行时所需的指令和数据中的一些。在一些实施例中，本发明的过程存储在系统存储器2720、永久性存储设备2735和/或只读存储器2730中。例如，各种存储器单元包括用于根据一些实施例处理多媒体片段的指令。一个或多个处理单元2710从这些各种存储器单元检索将要执行的指令以及将要处理的数据以执行一些实施例的过程。

[0228] 总线2705还连接至输入设备2740和输出设备2745。输入设备2740使得用户能够将信息传送到电子系统中并且选择发送到电子系统的命令。输入设备2740包括字母数字键盘和指示设备(也称为“光标控制设备”)、摄像机(例如网络摄像机)、麦克风或用于接收语音命令的类似设备等。输出设备2745显示由电子系统生成的图像或者其他输出数据。输出设备2745包括打印机和显示设备诸如阴极射线管(CRT)或液晶显示器(LCD)，以及扬声器或类似的音频输出设备。一些实施例包括用作输入设备和输出设备两者的设备，诸如触摸屏。

[0229] 最后，如图27所示，总线2705还通过网络适配器(未示出)将电子系统2700耦接到网络2725。这样，计算机可以是计算机的网络(诸如局域网(“LAN”)、广域网(“WAN”)或内联网的一部分，或者网络的网络诸如互联网)的一部分。电子系统2700的任何或所有部件均可与本发明结合使用。

[0230] 一些实施例包括将计算机程序指令存储在机器可读或计算机可读介质(或者称为计算机可读存储介质、机器可读介质或机器可读存储介质)中的电子部件，诸如微处理器、存储装置以及存储器。此类计算机可读介质的一些实例包括RAM、ROM、只读光盘(CD-ROM)、可刻录光盘(CD-R)、可重写光盘(CD-RW)、只读数字通用光盘(如DVD-ROM、双层DVD-ROM)、各种可刻录/可重写DVD(如DVD-RAM、DVD-RW、 DVD+RW等)、闪存存储器(如SD卡，mini-SD卡、micro-SD卡等)、磁性和/或固态硬盘驱动器、只读和可刻录Blu-Ray®盘、超密度光盘、任

何其他光学或磁性介质以及软盘。计算机可读介质可存储计算机程序，该计算机程序可由至少一个处理单元执行并且包括用于执行各种操作的指令集。计算机程序或者计算机代码的实例包括机器代码，诸如由编译器产生的机器代码，以及包括可由计算机、电子部件或微处理器使用解译器来执行的较高级别代码的文件。

[0231] 虽然上述讨论主要涉及执行软件的微处理器或多核处理器，但一些实施例由诸如专用集成电路(ASIC)或现场可编程门阵列(FPGA)的一个或多个集成电路来执行。在一些实施例中，此类集成电路执行存储在电路自身上的指令。此外，一些实施例执行存储在可编程逻辑设备(PLD)、ROM或RAM设备中的软件。

[0232] 如本说明书以及本专利申请的任何权利要求中所用，术语“计算机”、“服务器”、“处理器”及“存储器”均是指电子或其他技术设备。这些术语排除人或者人的群组。出于本说明书的目的，术语显示或正在显示意指在电子设备上显示。如在本说明书以及本专利申请的任何权利要中所用，术语“计算机可读介质”(“computer readable medium,”“computer readable media)”以及“机器可读介质”完全限于以可由计算机读取的形式存储信息的可触摸的有形物体。这些术语排除任何无线信号、有线下载信号以及任何其他短暂性信号。

[0233] 虽然已参照许多特定细节描述本发明，但本领域的普通技术人员将认识到，可在不脱离本发明的实质的情况下，以其他特定形式来体现本发明。此外，附图中的至少一些(包括图2、图3、图13、图17、图18和图26)概念性地示出了各种过程。这些过程的特定操作可不以所示出和所描述的确切顺序来执行。可不在一个连续系列的操作中执行特定操作，并且可在不同实施例中执行不同的特定操作。此外，过程可使用若干子过程来实施，或者实施为更大宏过程的一部分。因此，本领域的普通技术人员将理解，本发明不受前述示例性细节限制，而是将由所附的权利要求限定。

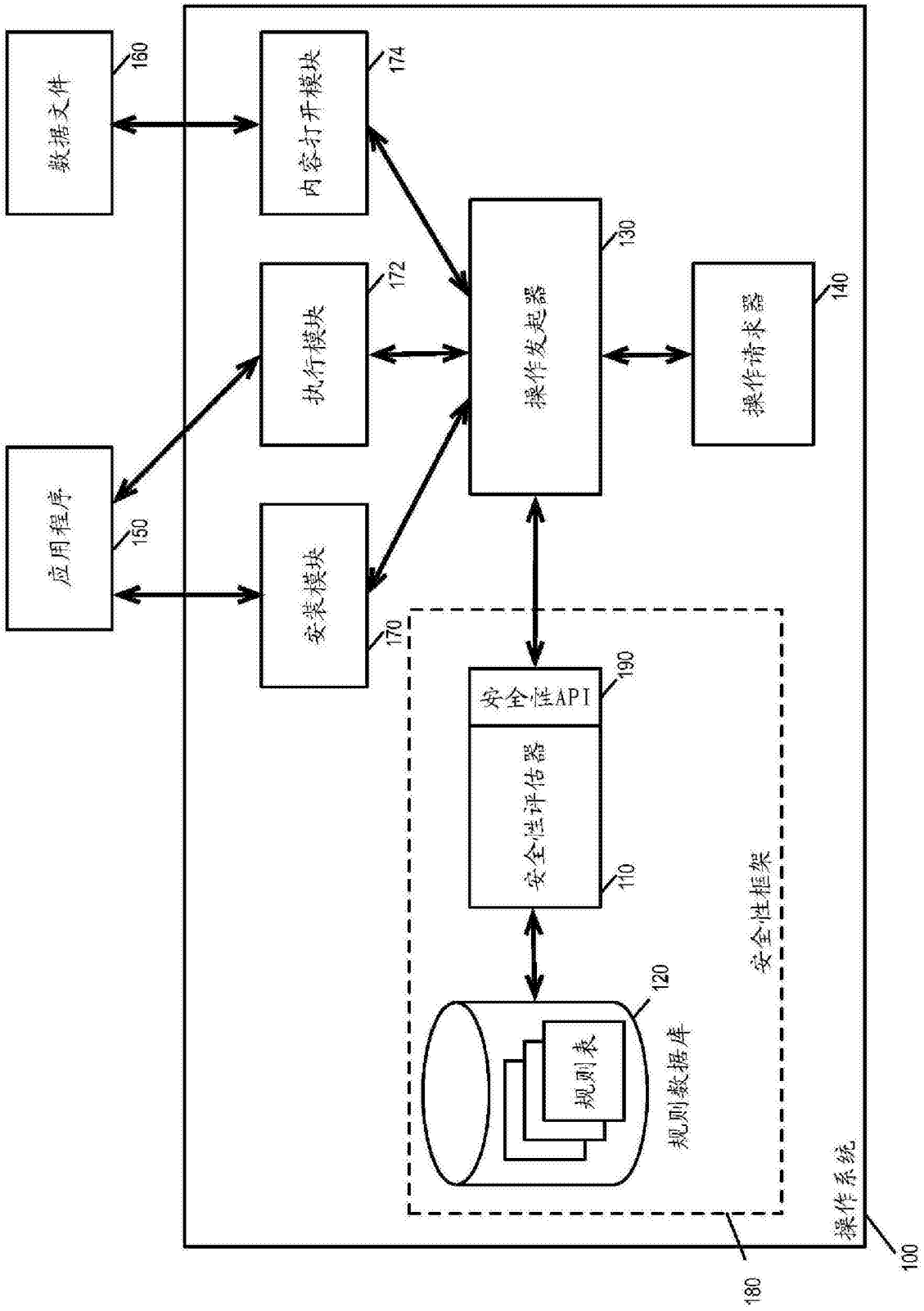

数据文件
160
内容打开模块
174
执行模块
172
操作发起器
130
操作请求器
140
应用程序
150
安装模块
170
安全性API
190
安全性评估器
110
规则表
120
规则数据库
安全性框架
180
操作系统
100

图1

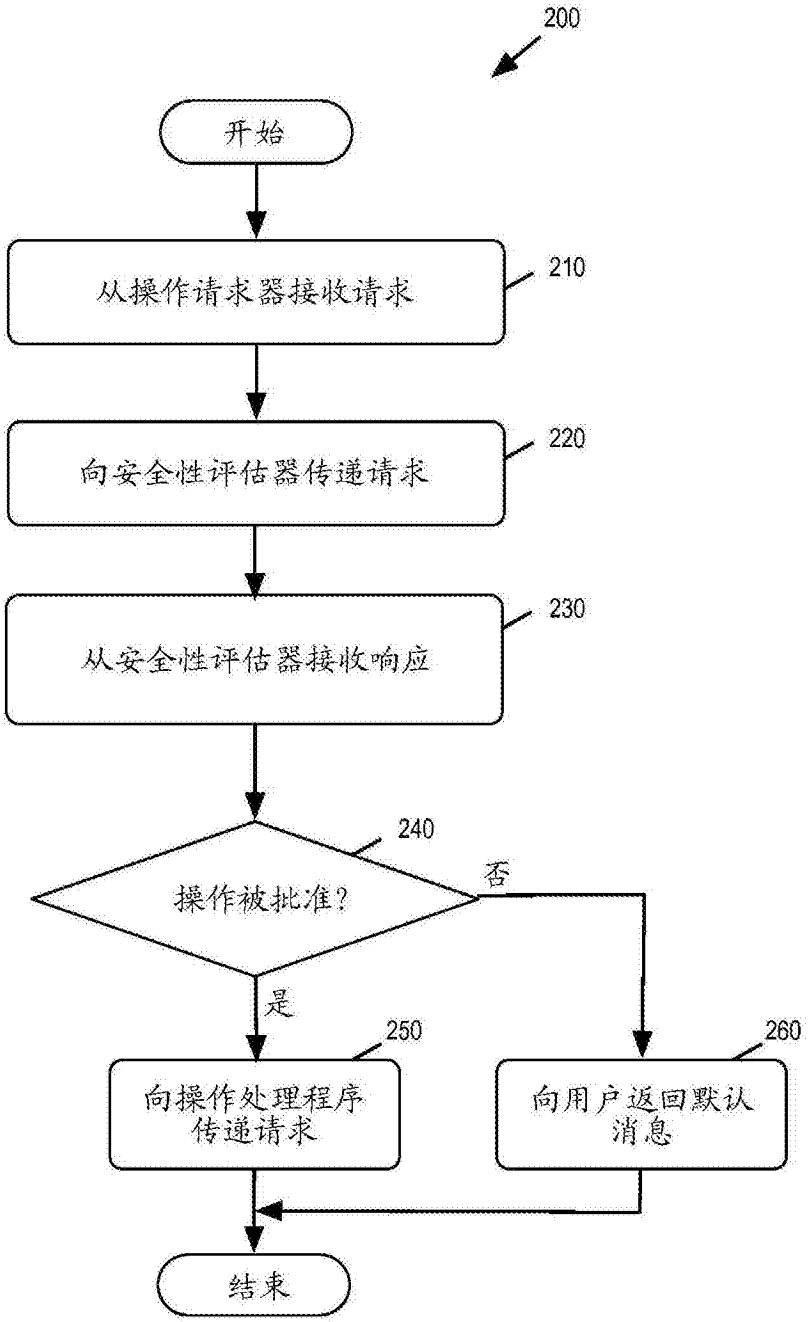

200
开始
从操作请求器接收请求
210
向安全性评估器传递请求
220
从安全性评估器接收响应
230
操作被批准?
240
否
是
向操作处理程序传递请求
250
向用户返回默认消息
260
结束

图2

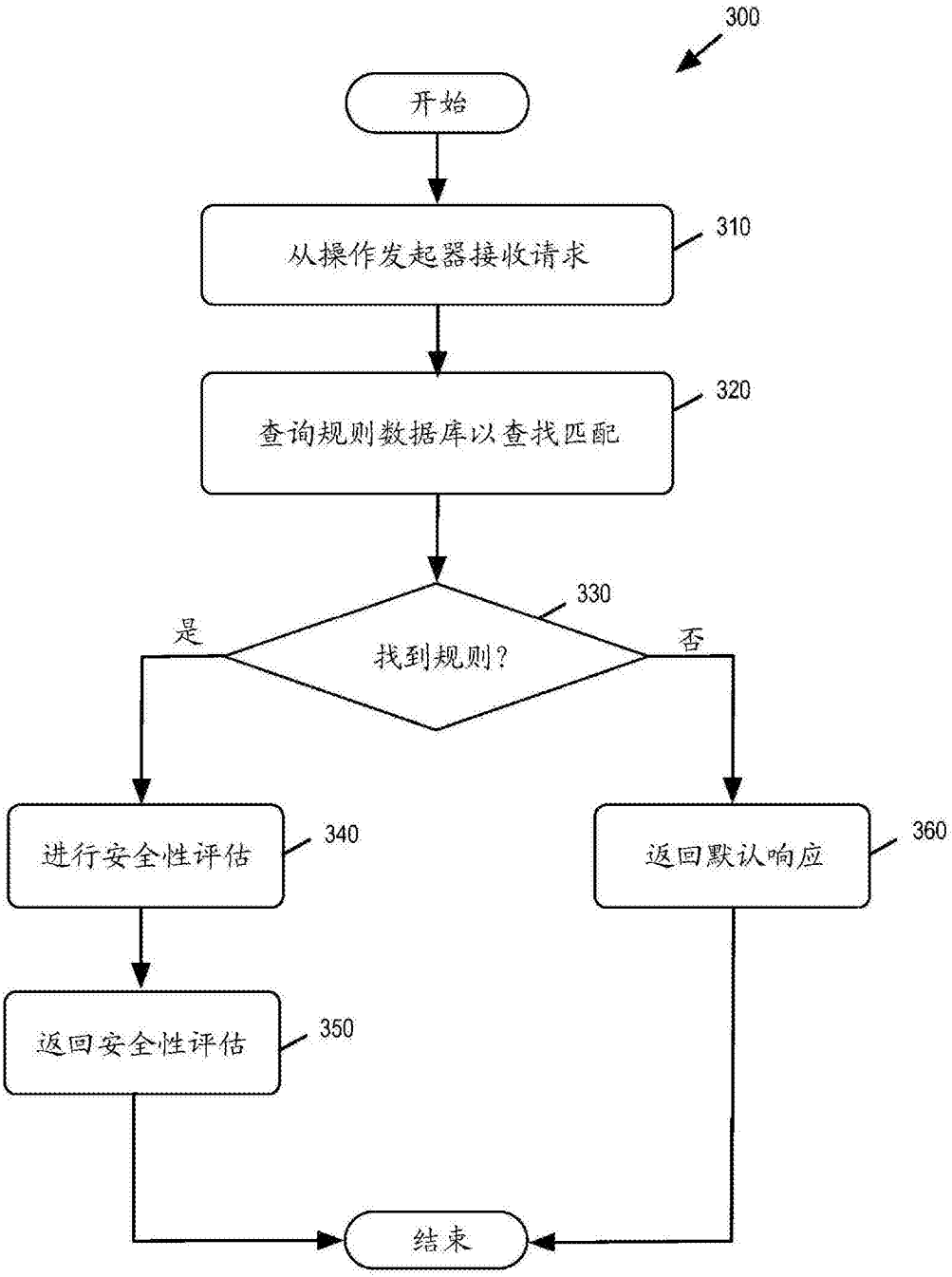

300
开始
从操作发起器接收请求
310
查询规则数据库以查找匹配
320
找到规则?
330
是
否
进行安全性评估
340
返回安全性评估
350
返回默认响应
360
结束

图3

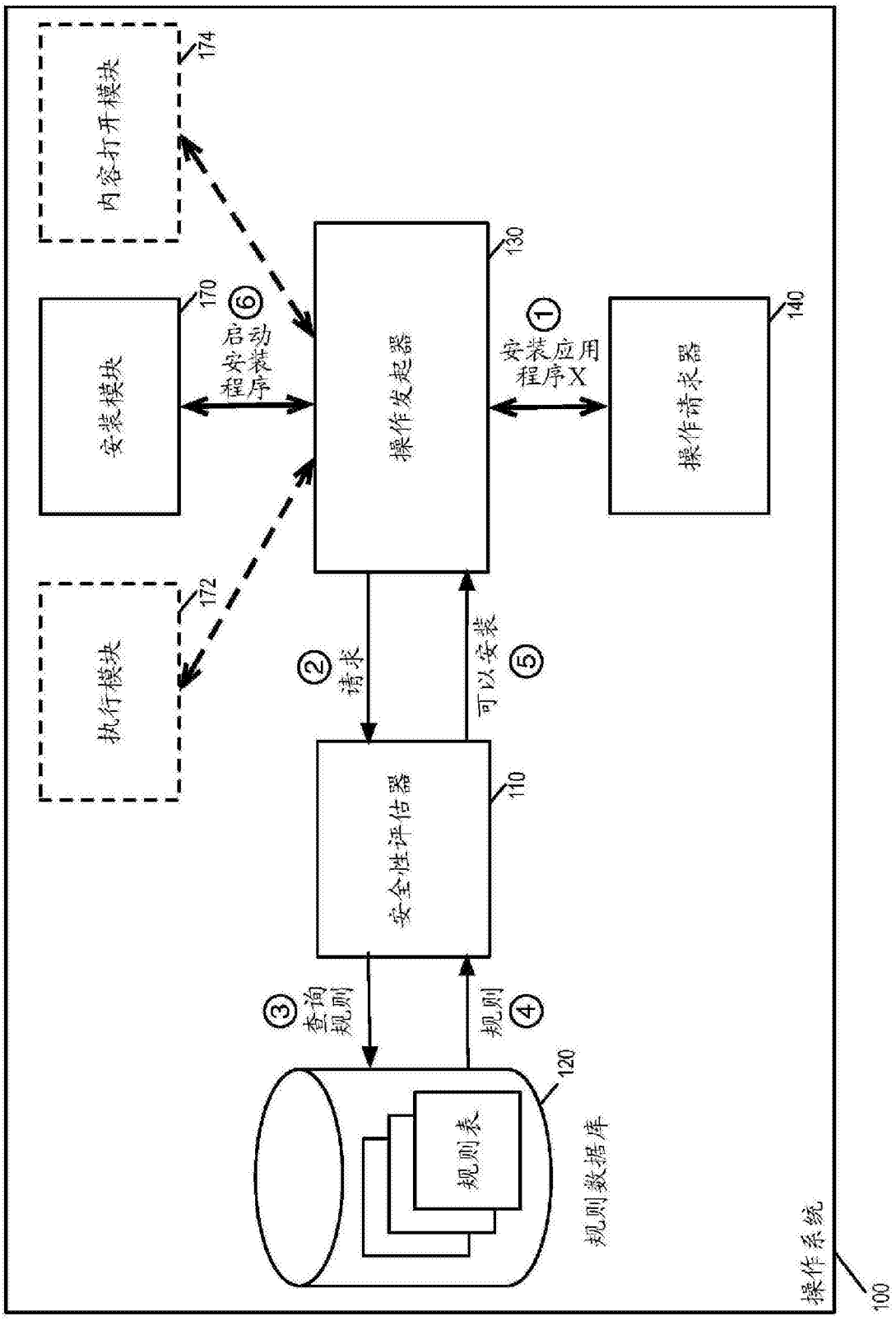

内容打开模块
174
安装模块
170
⑥
启动
安装
程序
操作发起器
130
①
安装应用
程序X
操作请求器
140
执行模块
172
②
请求
可以安装
⑤
安全性评估器
110
③
查询
规则
规则
④
120
规则表
规则数据库
操作系统
100

图4

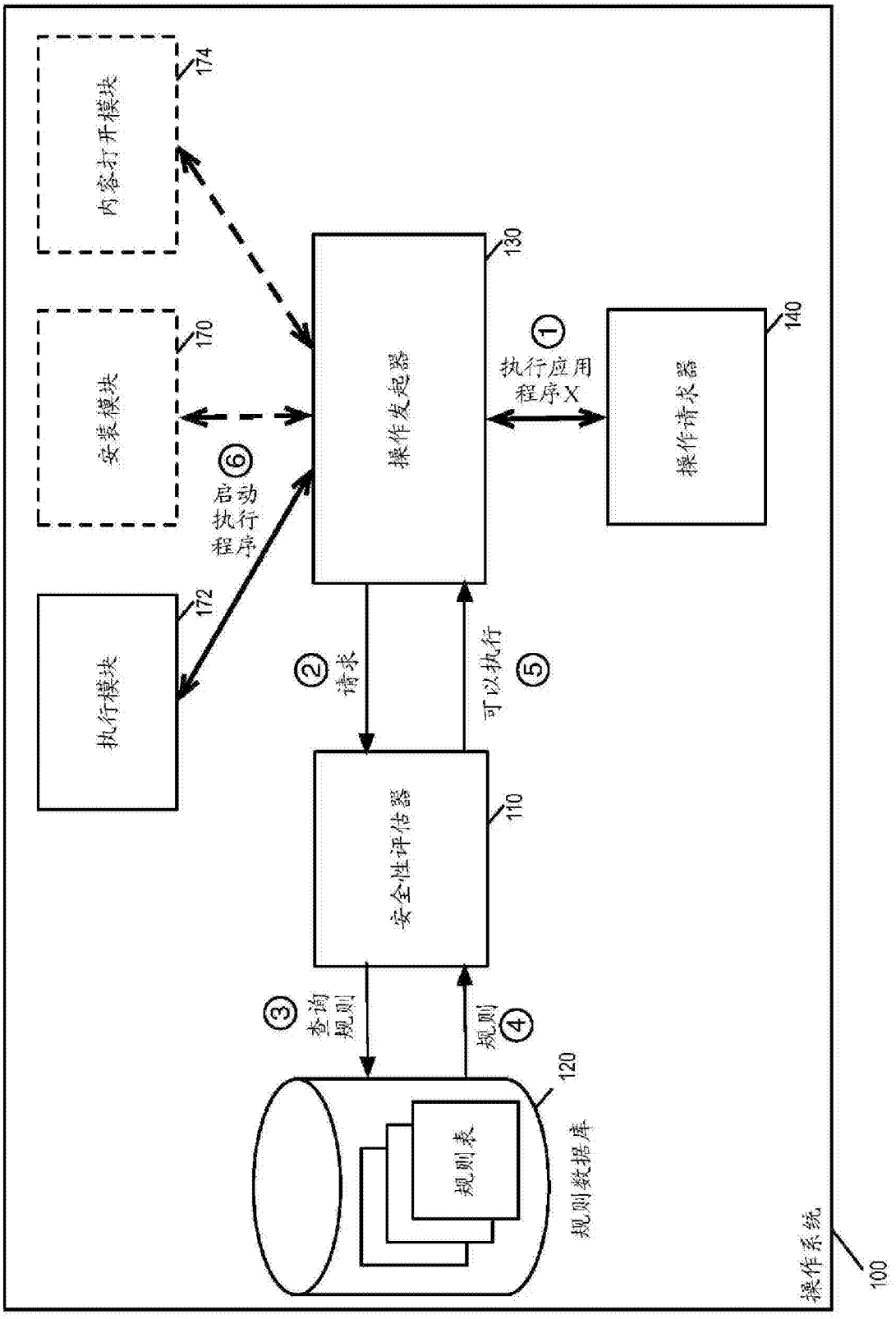

内容打开模块
174
安装模块
170
执行模块
172
操作发起器
130
操作请求器
140
①
执行应用
程序X
⑥
启动
执行
程序
②
请求
⑤
可以执行
安全性评估器
110
③
查询
规则
④
规则
120
规则表
规则数据库
操作系统
100

图5

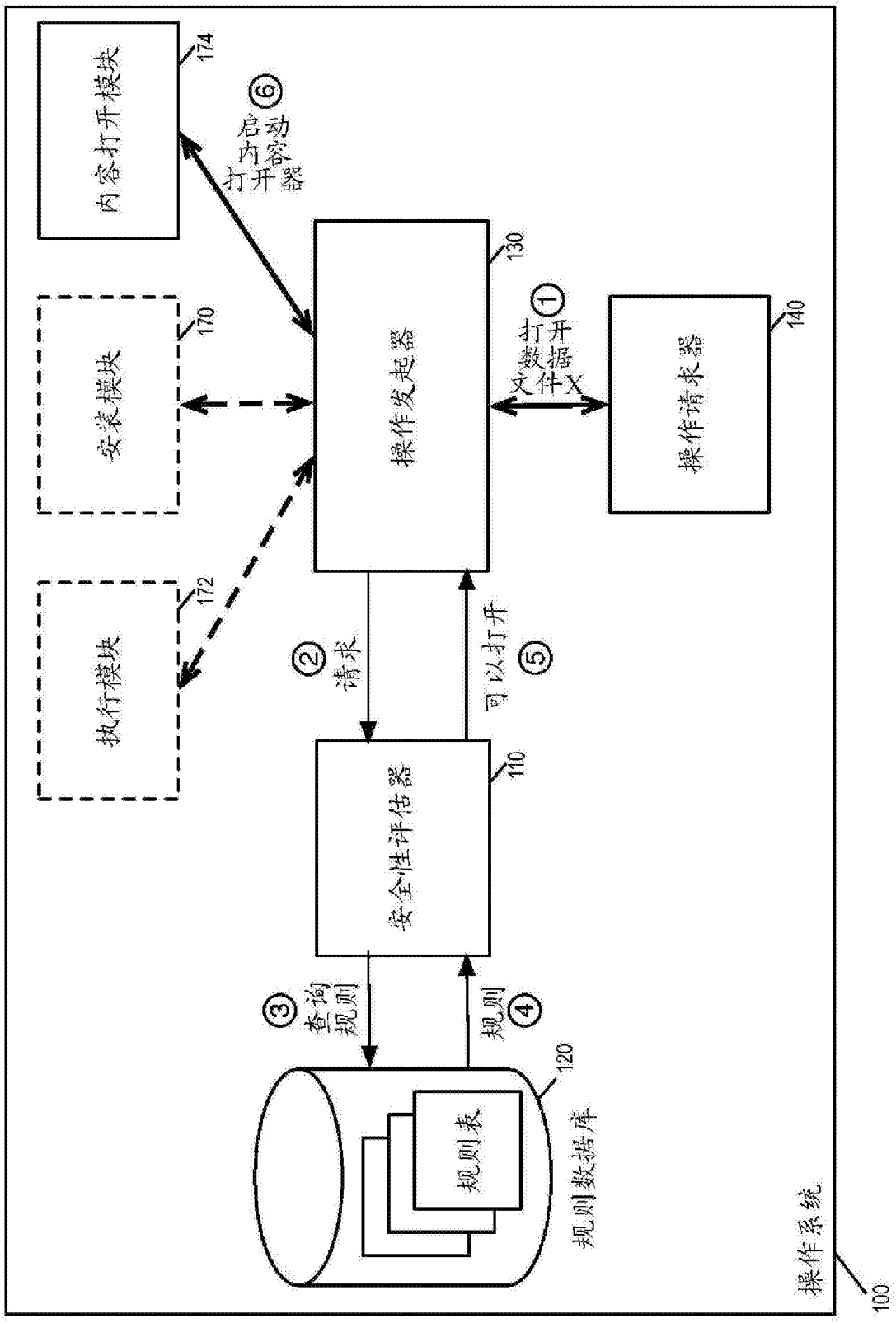

内容打开模块
174
⑥
启动
内容
打开器
安装模块
170
操作发起器
130
①
打开
数据
文件X
操作请求器
140
执行模块
172
②
请求
可以打开
⑤
安全性评估器
110
③
查询
规则
规则
④
120
规则表
规则数据库
操作系统
100

图6

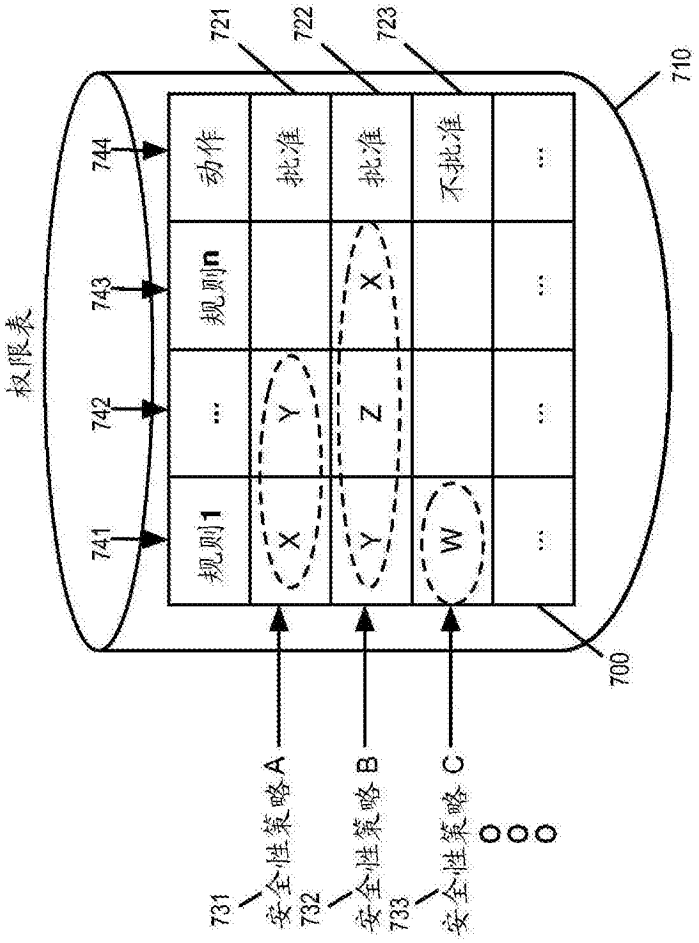

权限表
721
722
723
710
744
743
742
741
动作
批准
批准
不批准
...
规则n
X
...
...
Y
Z
...
规则1
X
Y
W
...
700
安全性策略A
安全性策略B
安全性策略C
731
732
733

图7

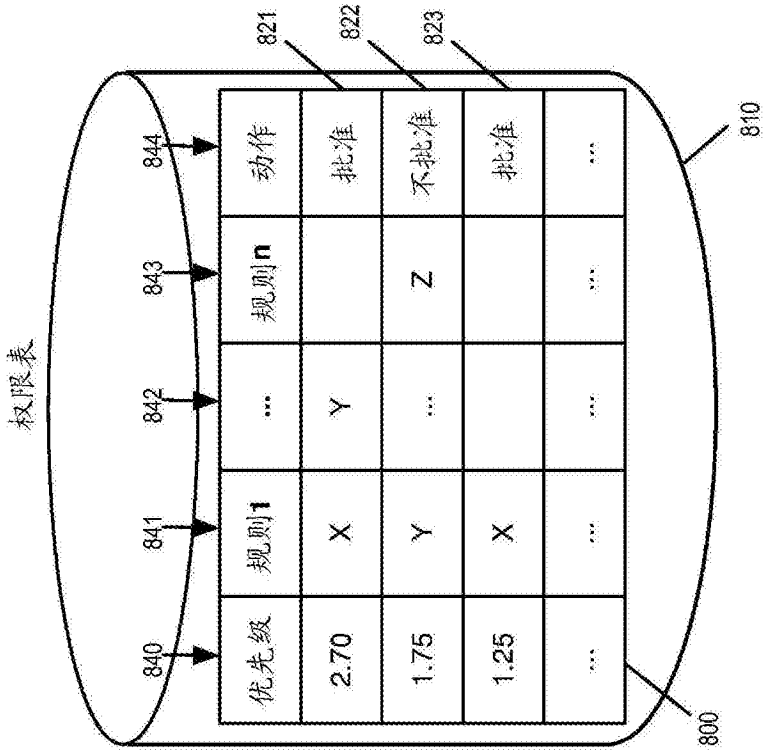

权限表
821
822
823
844
843
842
841
840
动作
批准
不批准
批准
...
规则n
Z
...
...
...
Y
...
...
规则1
X
Y
X
...
优先级
2.70
1.75
1.25
...
810
800

图8

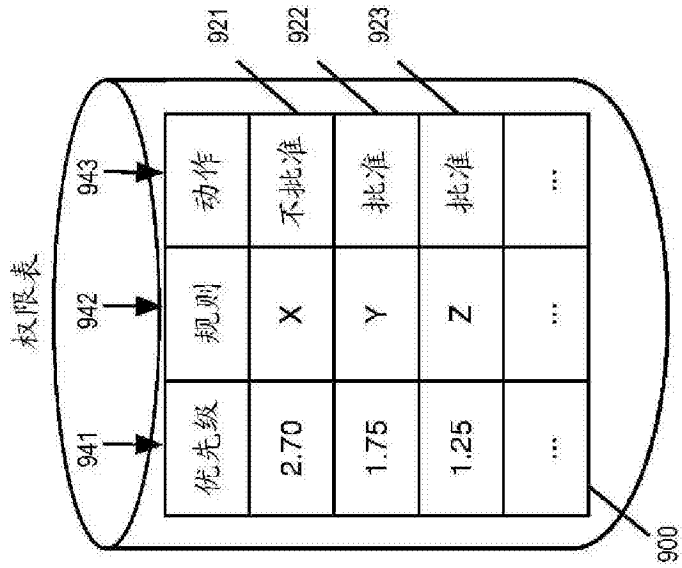

权限表
921
922
923
943
942
941
动作
不批准
批准
批准
...
规则
X
Y
Z
...
优先级
2.70
1.75
1.25
...
900

图9

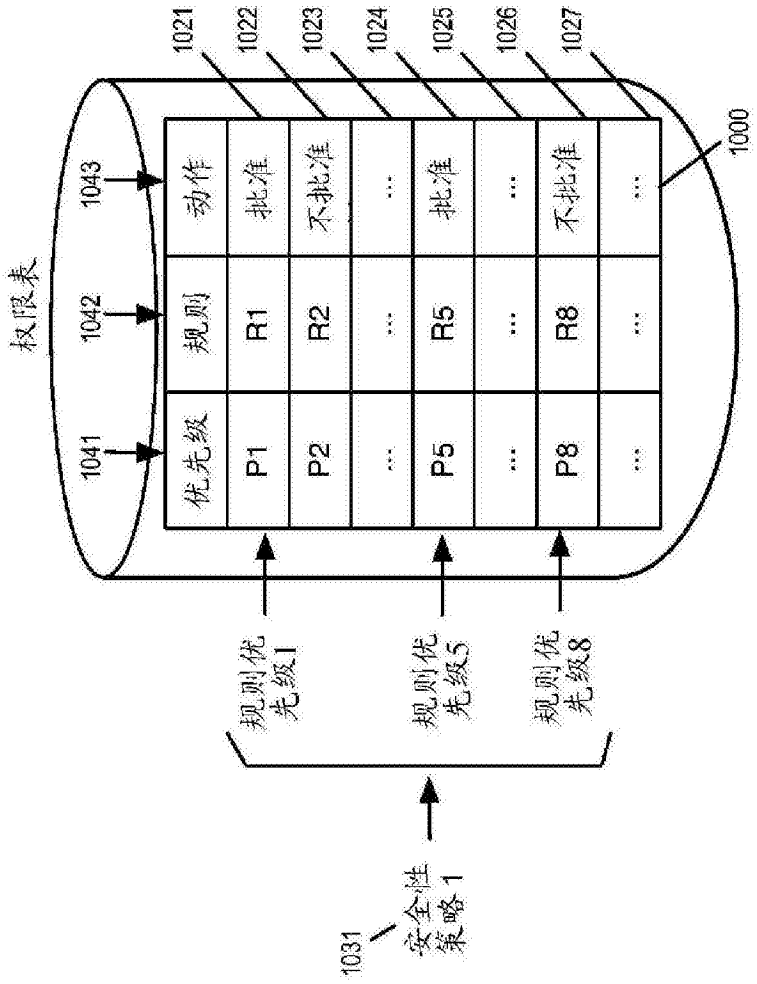

权限表
1000
1021
1022
1023
1024
1025
1026
1027
1041
1042
1043
优先级
规则
动作
P1
R1
批准
P2
R2
不批准
...
P5
R5
批准
P8
R8
不批准
规则优先级1
规则优先级5
规则优先级8
1031
安全性策略1

图10

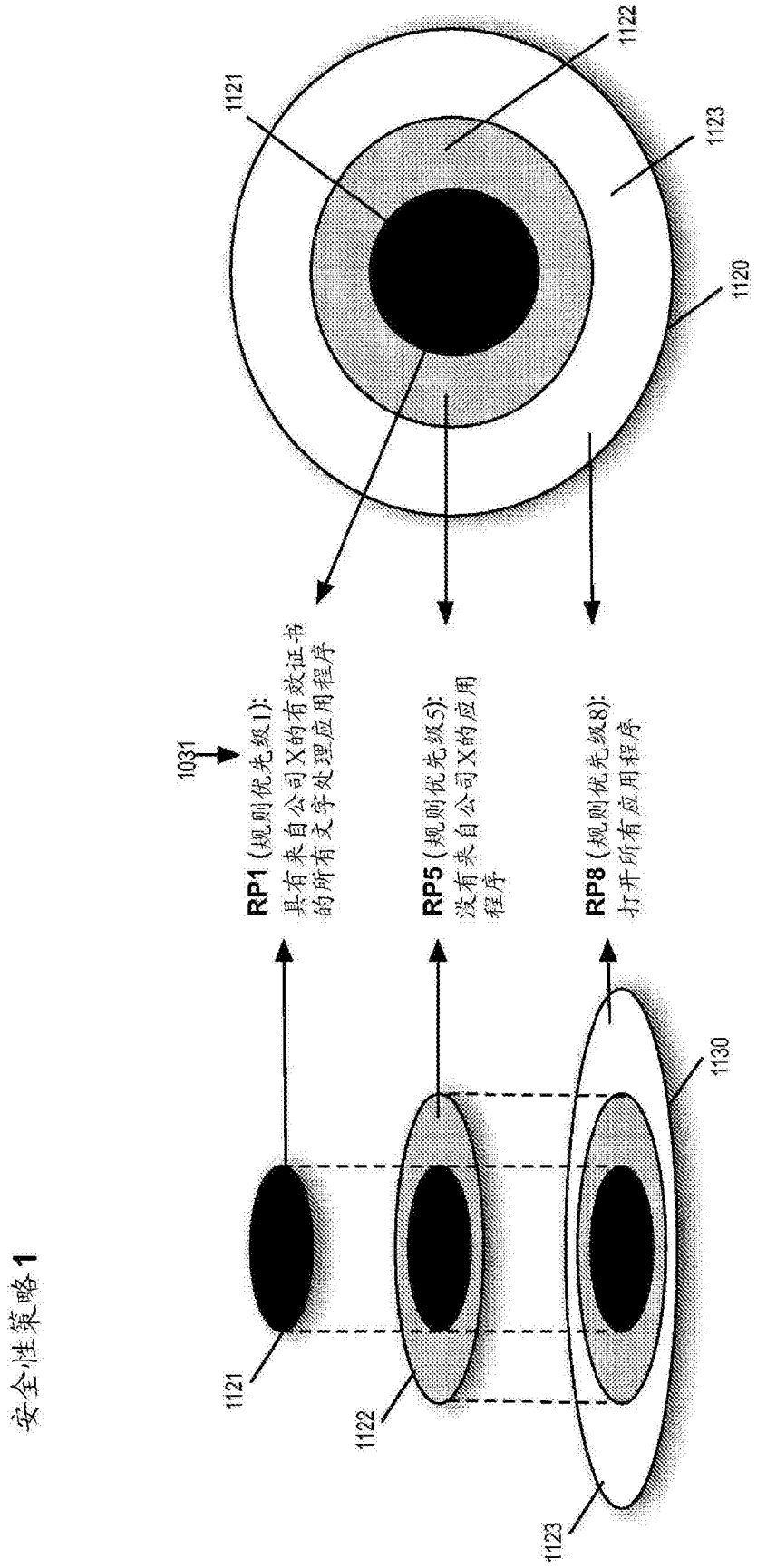

安全性策略1
1031
RP1 (规则优先级1):
具有来自公司X的有效证书的所有文字处理应用程序
RP5 (规则优先级5):
没有来自公司X的应用程序
RP8 (规则优先级8):
打开所有应用程序
1120
1121
1122
1123
1130

图11

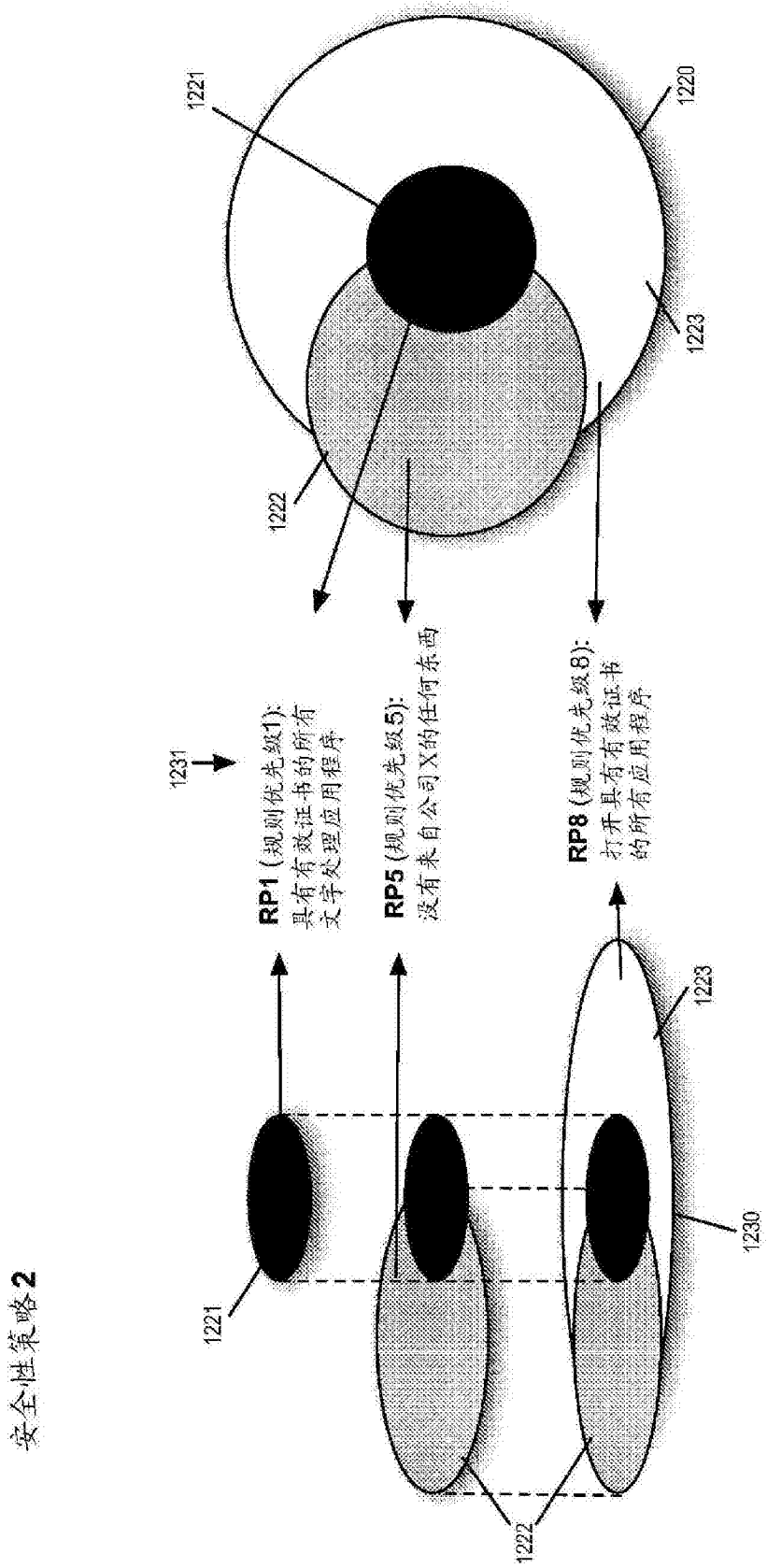

安全性策略2
1221
1220
1223
1222
1231
RP1 (规则优先级1):
具有有效证书的所有
文字处理应用程序
RP5 (规则优先级5):
没有来自公司X的任何东西
RP8 (规则优先级8):
打开具有有效证书
的所有应用程序
1223
1230
1221
1222

图12

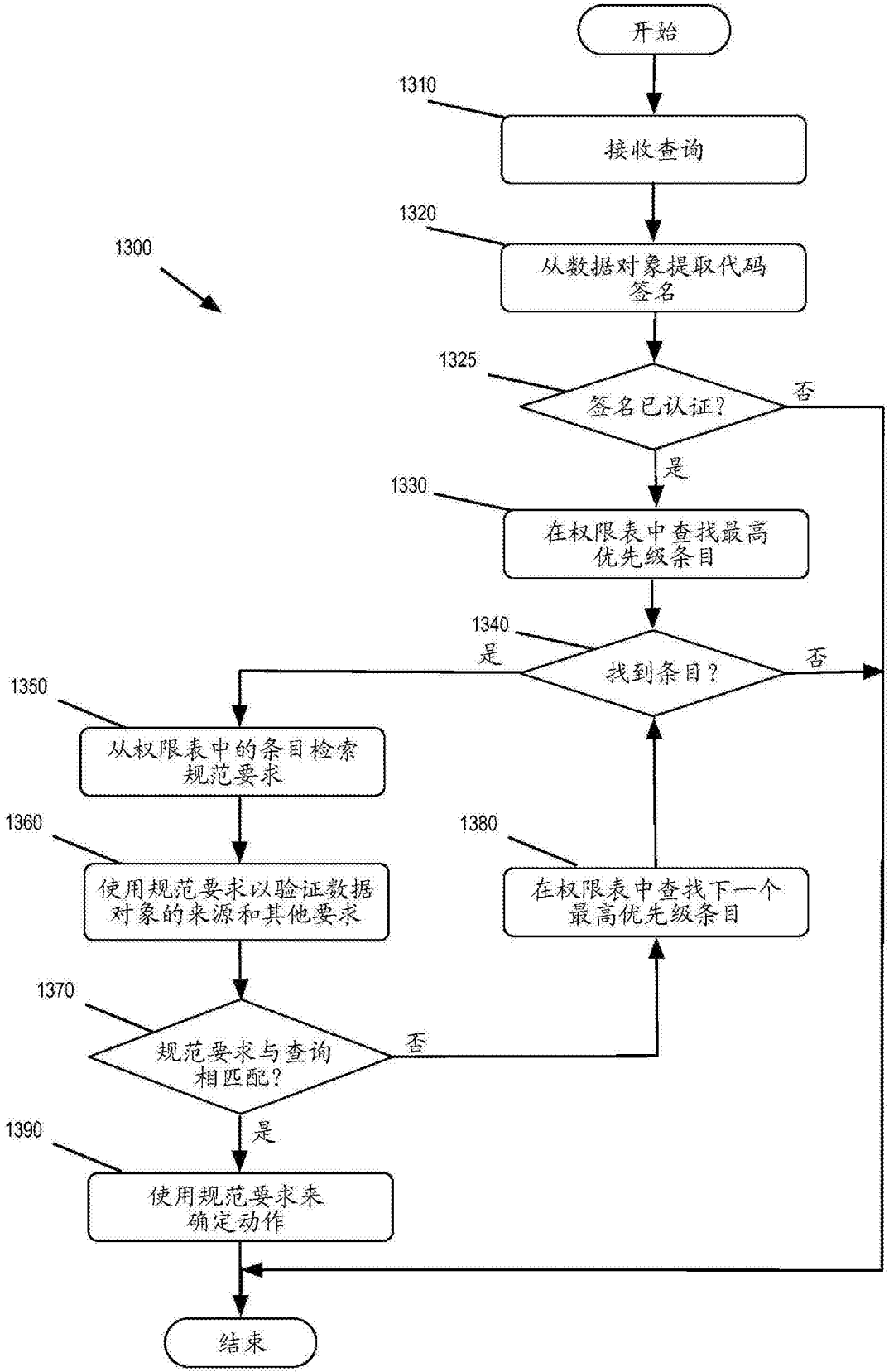

开始
1310
接收查询
1320
从数据对象提取代码签名
1300
1325
签名已认证?
否
是
1330
在权限表中查找最高优先级条目
1340
找到条目?
是
否
1350
从权限表中的条目检索规范要求
1360
使用规范要求以验证数据对象的来源和其他要求
1380
在权限表中查找下一个最高优先级条目
1370
规范要求与查询相匹配?
否
是
1390
使用规范要求来确定动作
结束

图13

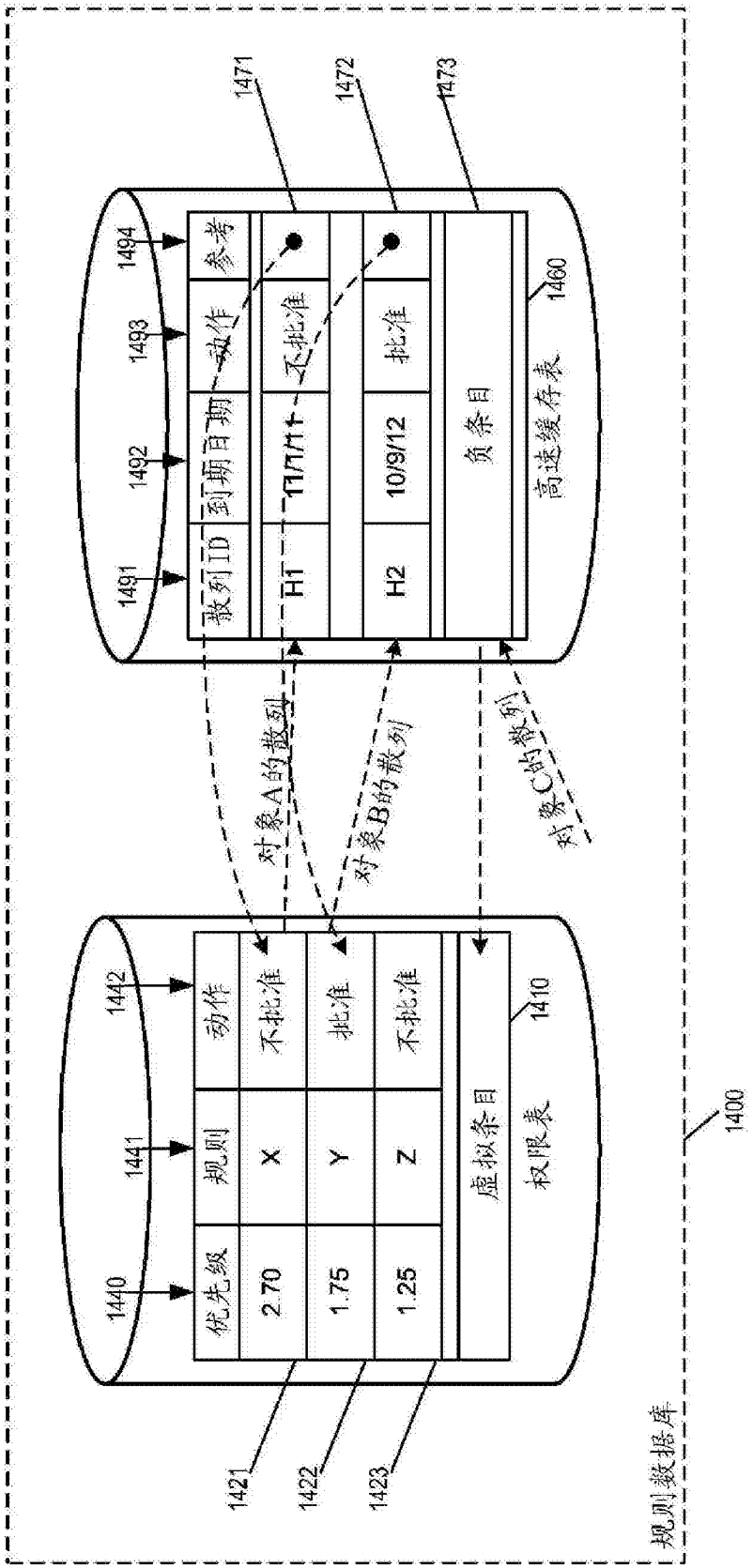

1471
1472
1473
1494
1493
1492
1491
参考
动作
到期日期
散列ID
H1
H2
11/7/11
10/9/12
不批准
批准
负条目
1460
高速缓存表
对象A的散列
对象B的散列
对象C的散列
1442
1441
1440
动作
规则
优先级
不批准
批准
不批准
X
Y
Z
2.70
1.75
1.25
虚拟条目
权限表
1410
1400
1421
1422
1423
规则数据库

图14

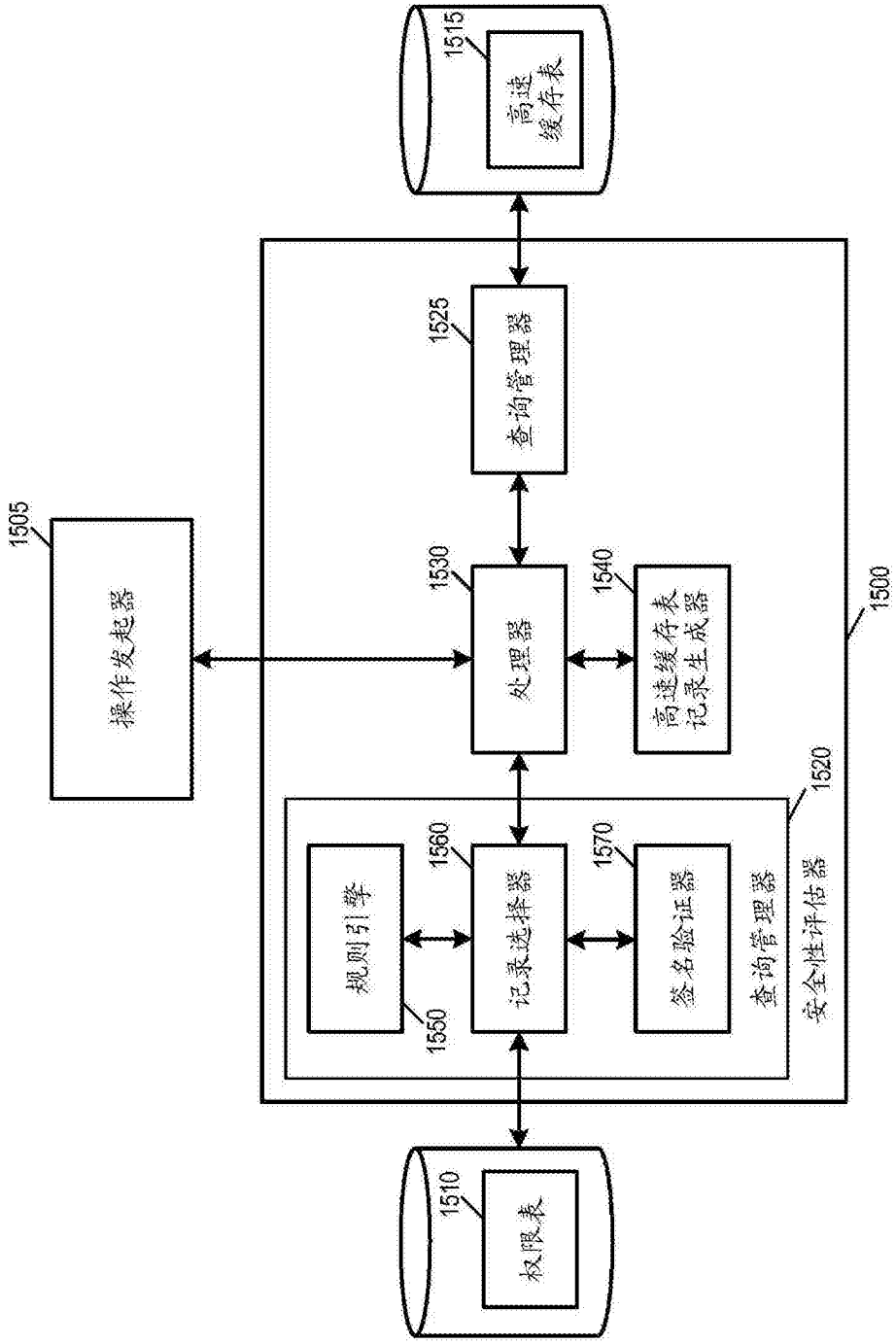

1515
高速缓存表
1525
查询管理器
1505
操作发起器
1530
处理器
1540
高速缓存表记录生成器
1500
1520
查询管理器
安全性评估器
1560
记录选择器
1570
签名验证器
规则引擎
1550
1510
权限表

图15

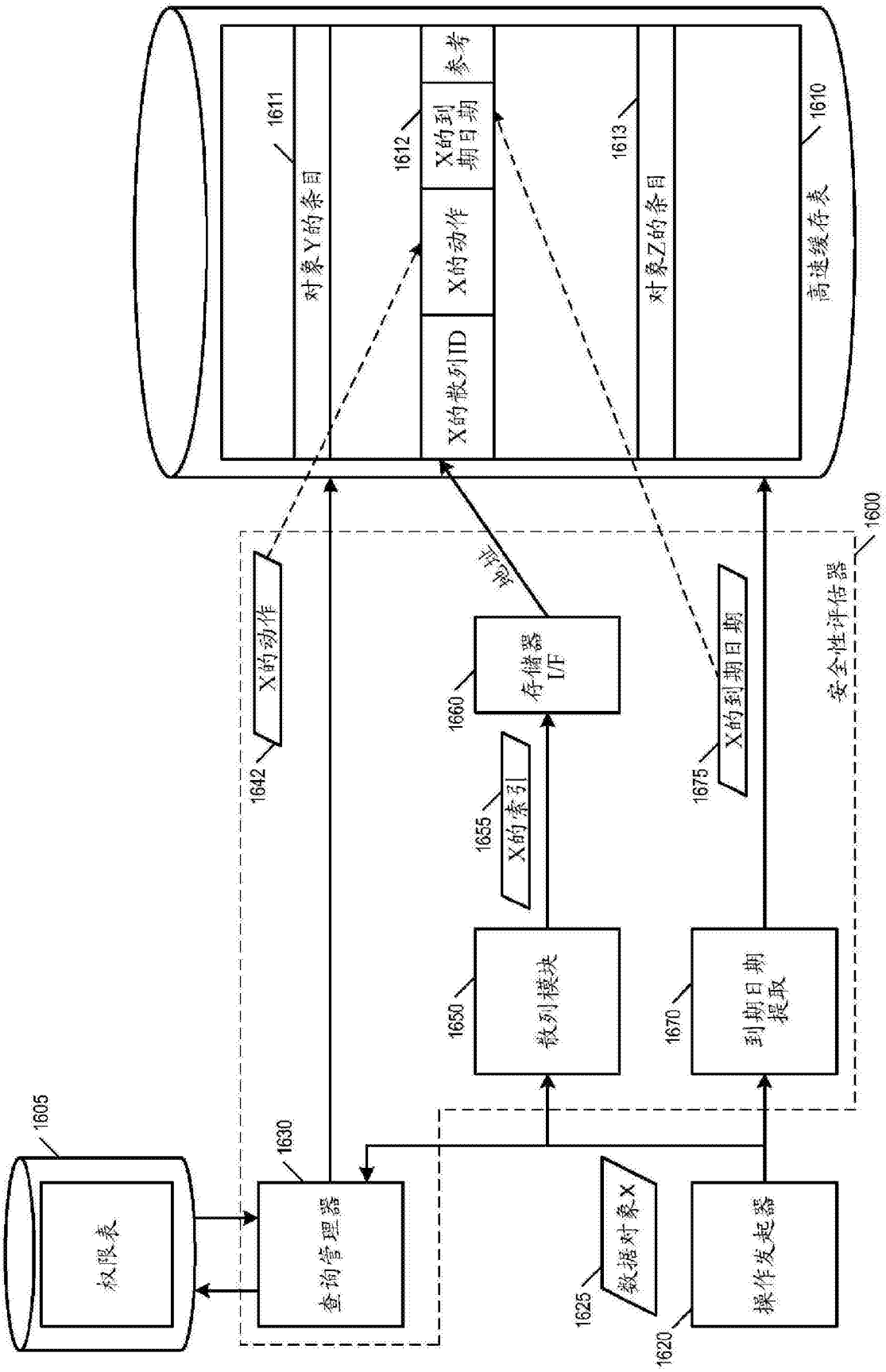

1610
高速缓存表
1611
对象Y的条目
1612
X的散列ID
X的动作
X的到期日期
参考
1613
对象Z的条目
1600
安全性评估器
1605
权限表
1630
查询管理器
1642
X的动作
1660
存储器I/F
1655
X的索引
1650
散列模块
1675
X的到期日期
1670
到期日期提取
1625
数据对象X
1620
操作发起器

图16

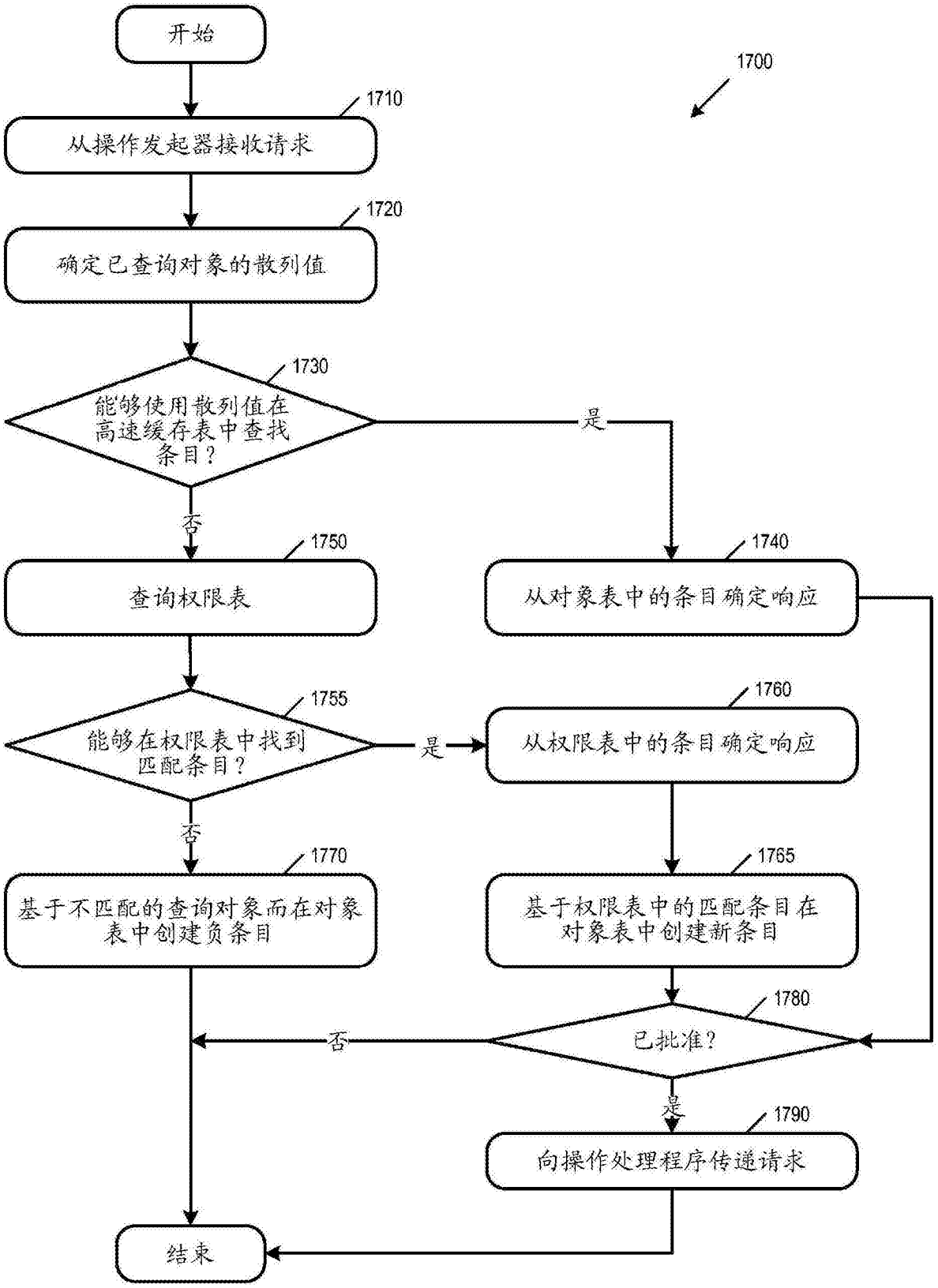

开始
1700
1710
从操作发起器接收请求
1720
确定已查询对象的散列值
1730
能够使用散列值在高速缓存表中查找条目？
是
否
1740
从对象表中的条目确定响应
1750
查询权限表
1755
能够在权限表中找到匹配条目？
是
1760
从权限表中的条目确定响应
否
1765
基于权限表中的匹配条目在对象表中创建新条目
1770
基于不匹配的查询对象而在对象表中创建负条目
1780
已批准？
否
是
1790
向操作处理程序传递请求
结束

图17

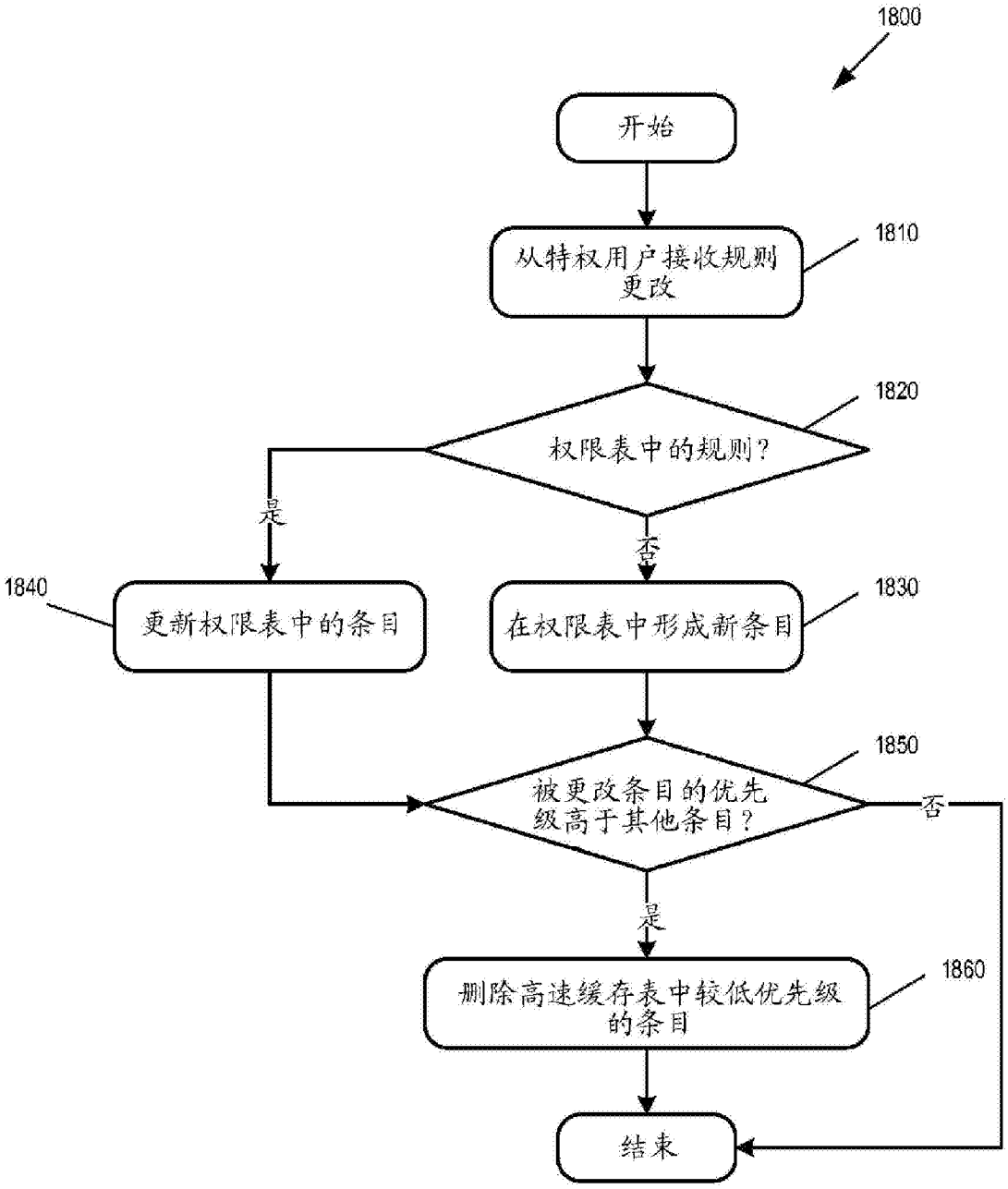

1800
开始
从特权用户接收规则更改
1810
权限表中的规则？
1820
是
否
1840
更新权限表中的条目
在权限表中形成新条目
1830
被更改条目的优先级高于其他条目？
1850
否
是
删除高速缓存表中较低优先级的条目
1860
结束

图18

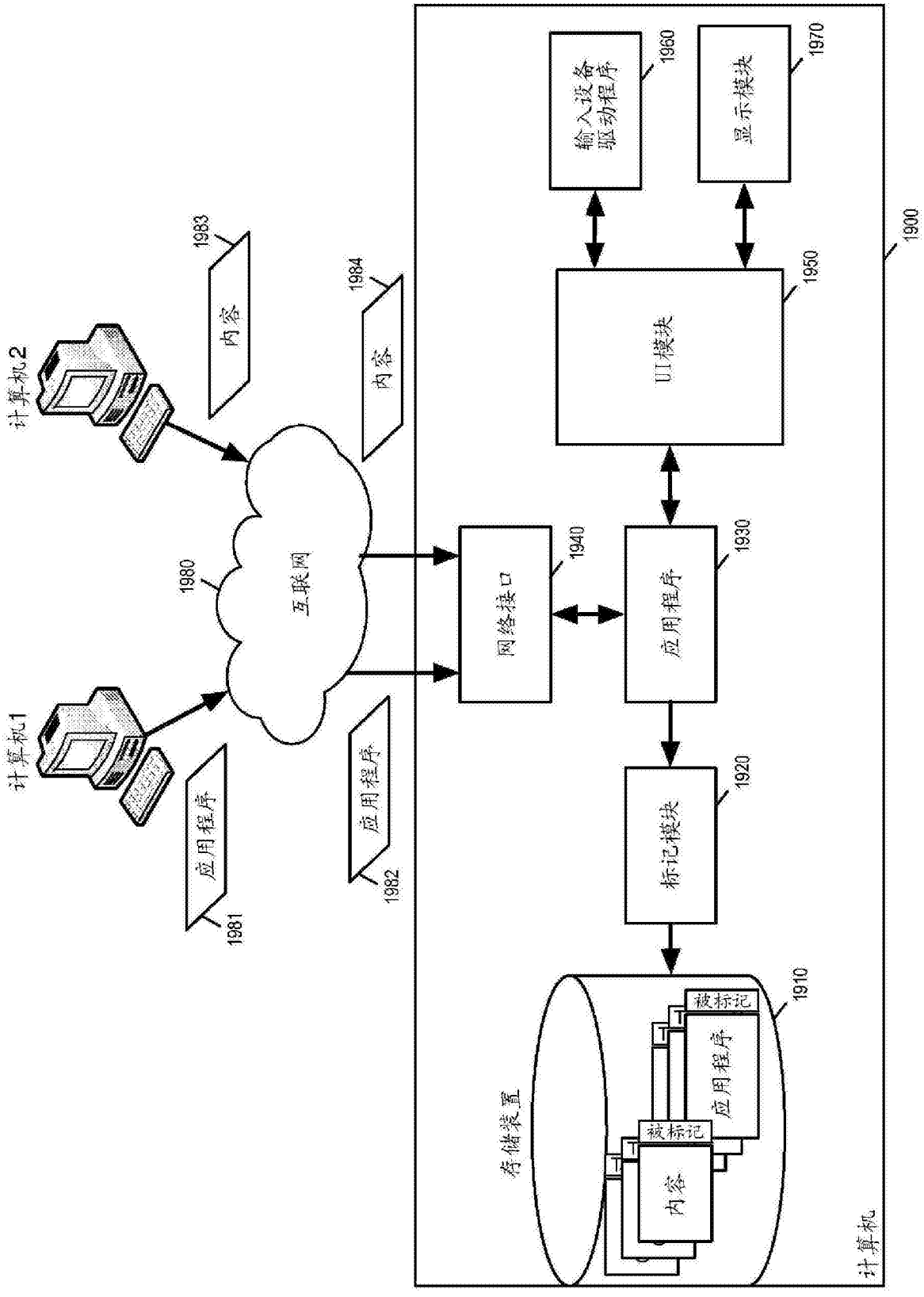

计算机2
计算机1
1983
内容
1984
内容
1980
互联网
应用程序
1981
应用程序
1982
1900
输入设备驱动程序
1960
显示模块
1970
UI模块
1950
网络接口
1940
应用程序
1930
标记模块
1920
存储装置
1910
被标记
应用程序
被标记
内容
计算机

图19

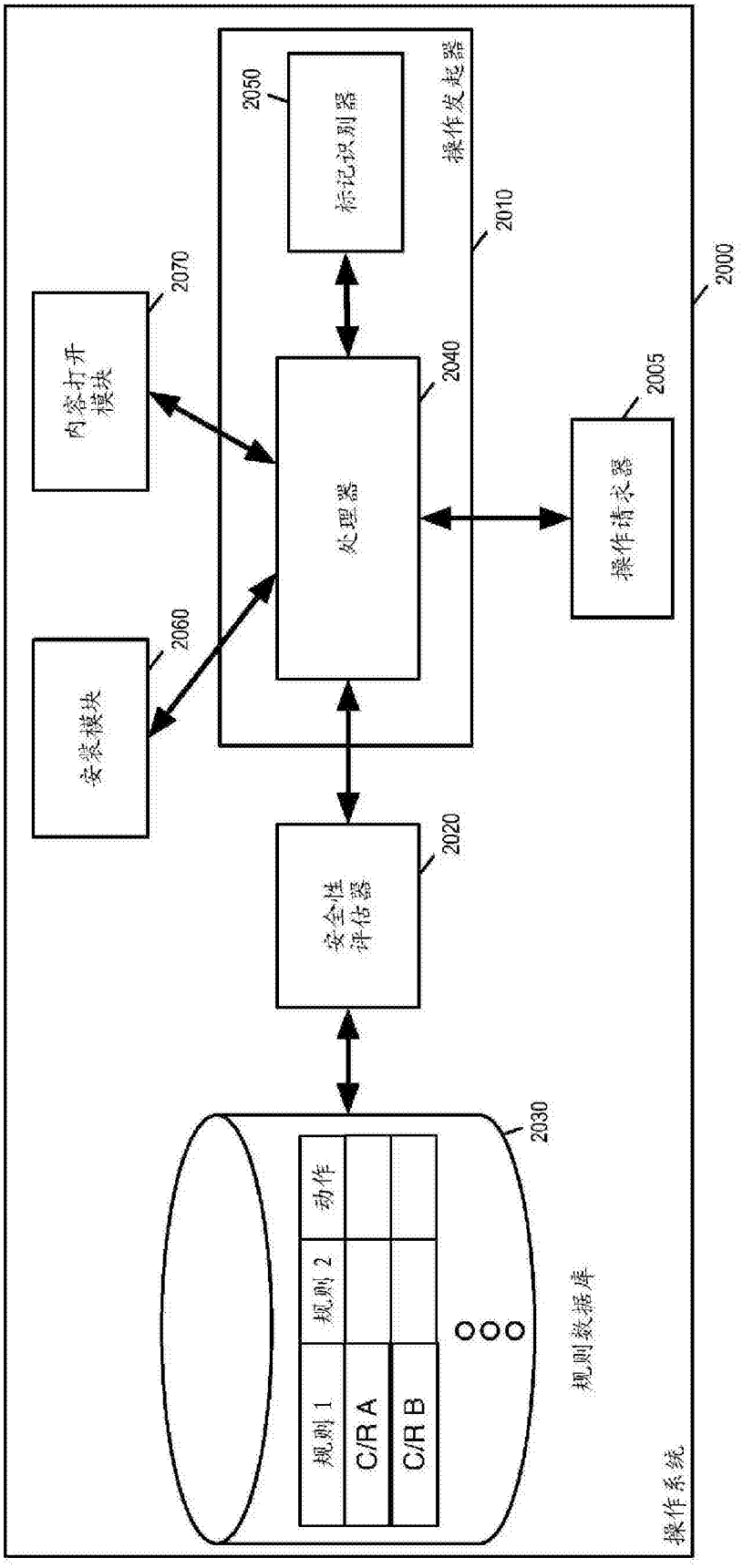

操作系统
2000
操作发起器
2010
标记识别器
2050
处理器
2040
内容打开模块
2070
安装模块
2060
安全性评估器
2020
操作请求器
2005
规则数据库
2030
规则 1
C/R A
C/R B
规则 2
动作

图20

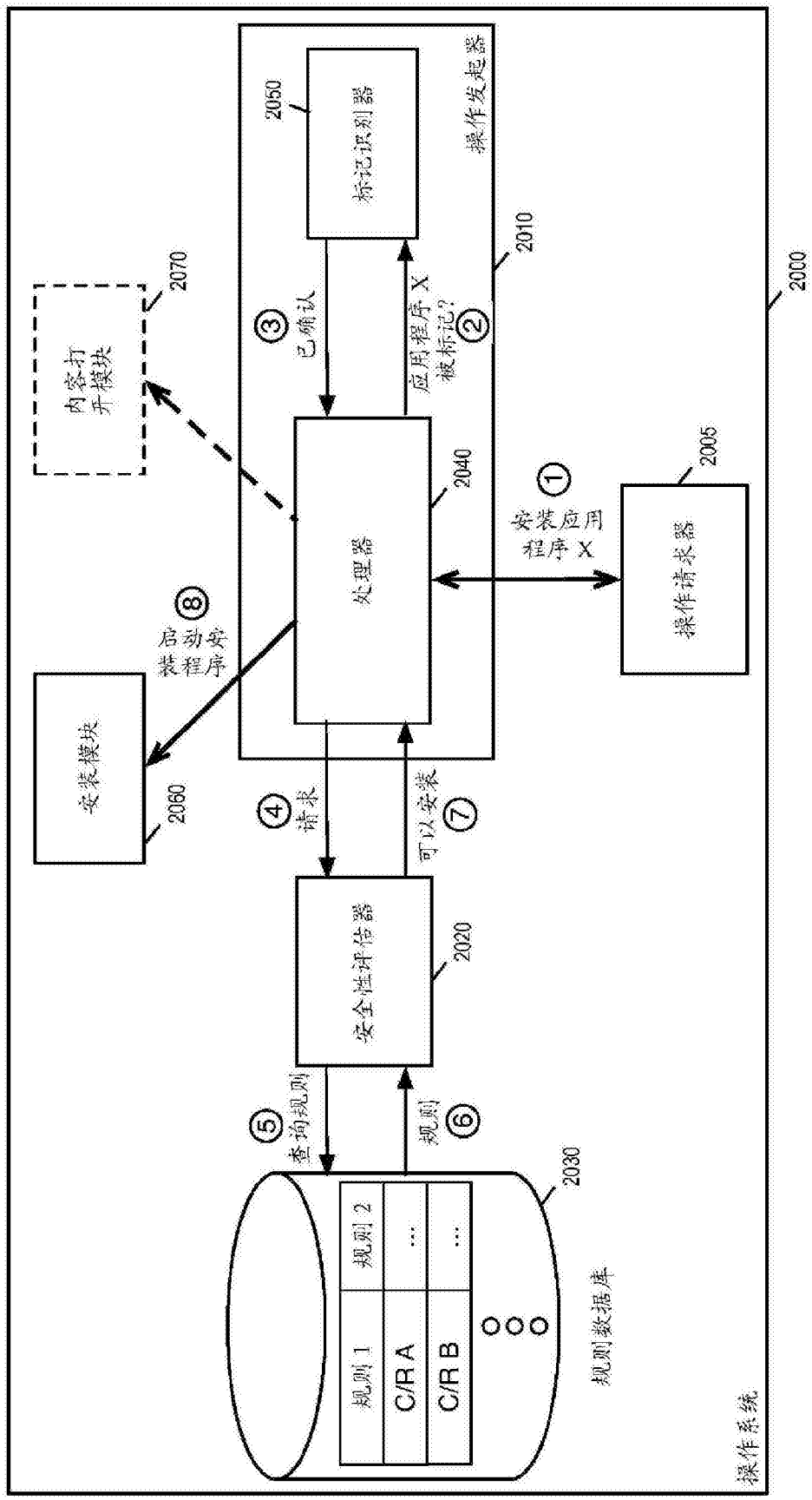

操作系统
2000
操作发起器
2010
标记识别器
2050
内容打开模块
2070
处理器
2040
操作请求器
2005
安装模块
2060
安全性评估器
2020
规则数据库
2030
规则 1
C/R A
C/R B
规则 2
...
...
①
安装应用程序 X
②
应用程序 X 被标记?
③
已确认
④
请求
⑤
查询规则
⑥
规则
⑦
可以安装
⑧
启动安装程序

图21

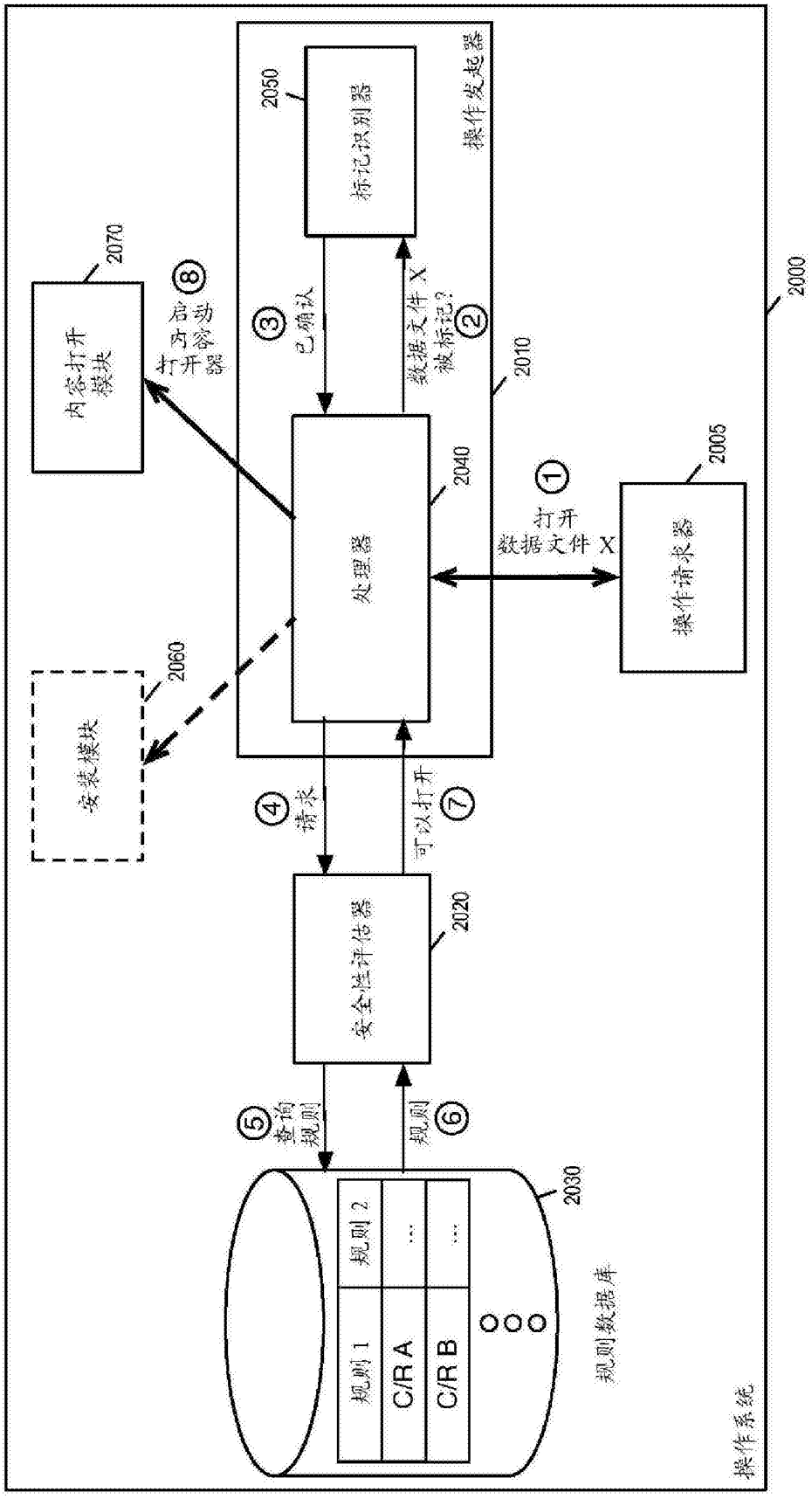
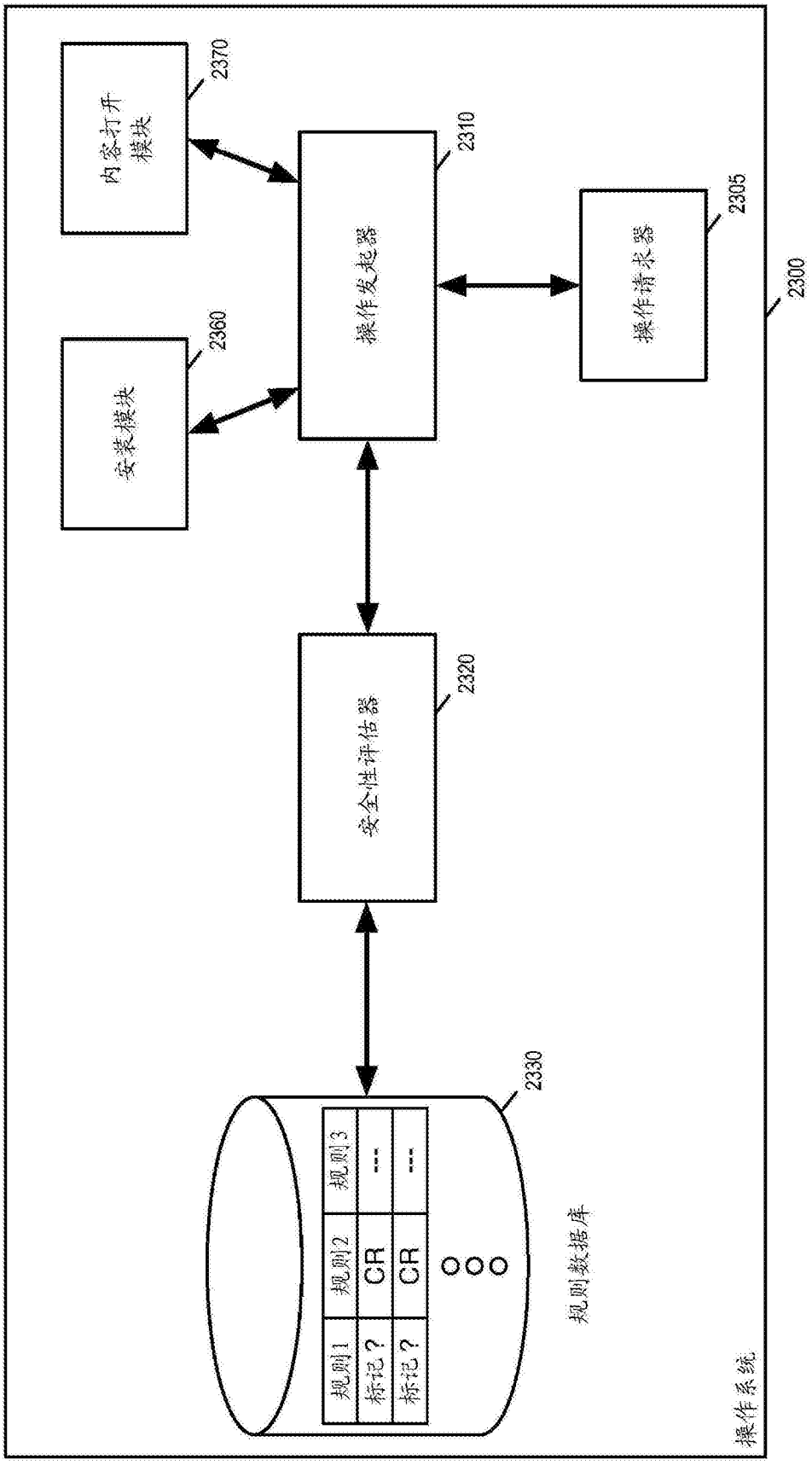

2000
操作系统
操作发起器
2050
标记识别器
2070
内容打开模块
⑧ 启动内容打开器
③ 已确认
② 数据文件 X 被标记?
2010
2040
处理器
① 打开数据文件 X
2005
操作请求器
2060
安装模块
④ 请求
⑦ 可以打开
2020
安全性评估器
⑤ 查询规则
⑥ 规则
2030
规则数据库
规则 1
规则 2
C/R A
C/R B

图22


内容打开模块
2370
安装模块
2360
操作发起器
2310
操作请求器
2305
2300
安全性评估器
2320
2330
规则1
规则2
规则3
标记？
CR

标记？
CR

规则数据库
操作系统

图23

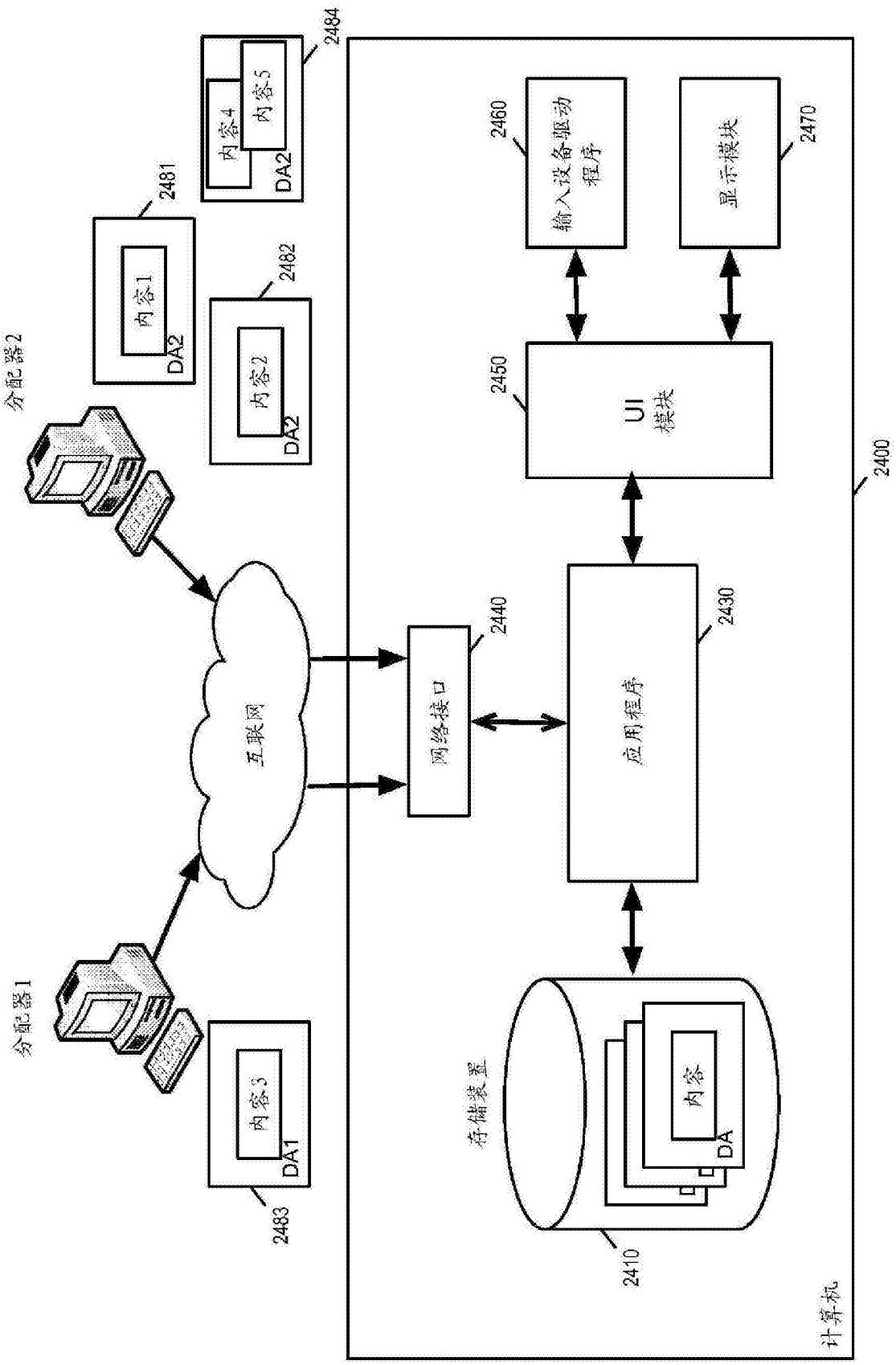

分配器2
分配器1
互联网
网络接口
2440
应用程序
2430
UI
模块
2450
输入设备驱动
程序
2460
显示模块
2470
2400
存储装置
内容
DA
2410
计算机
内容1
DA2
2481
内容2
DA2
2482
内容3
DA1
2483
内容4
内容5
DA2
2484

图24

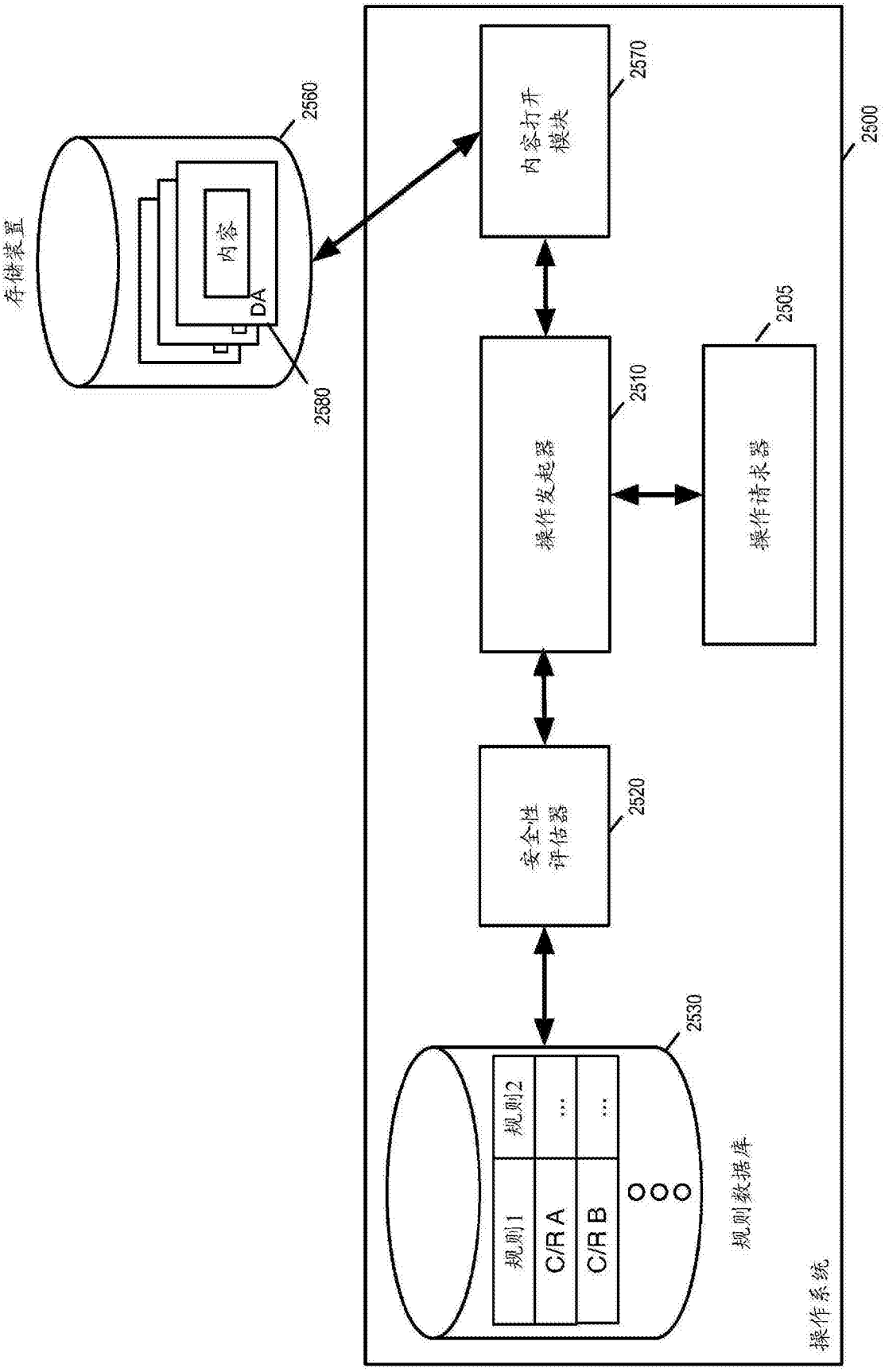

2500
2560
存储装置
内容
DA
2580
内容打开模块
2570
操作发起器
2510
操作请求器
2505
安全性评估器
2520
2530
规则1
C/R A
C/R B
规则2
...
...
规则数据库
操作系统

图25

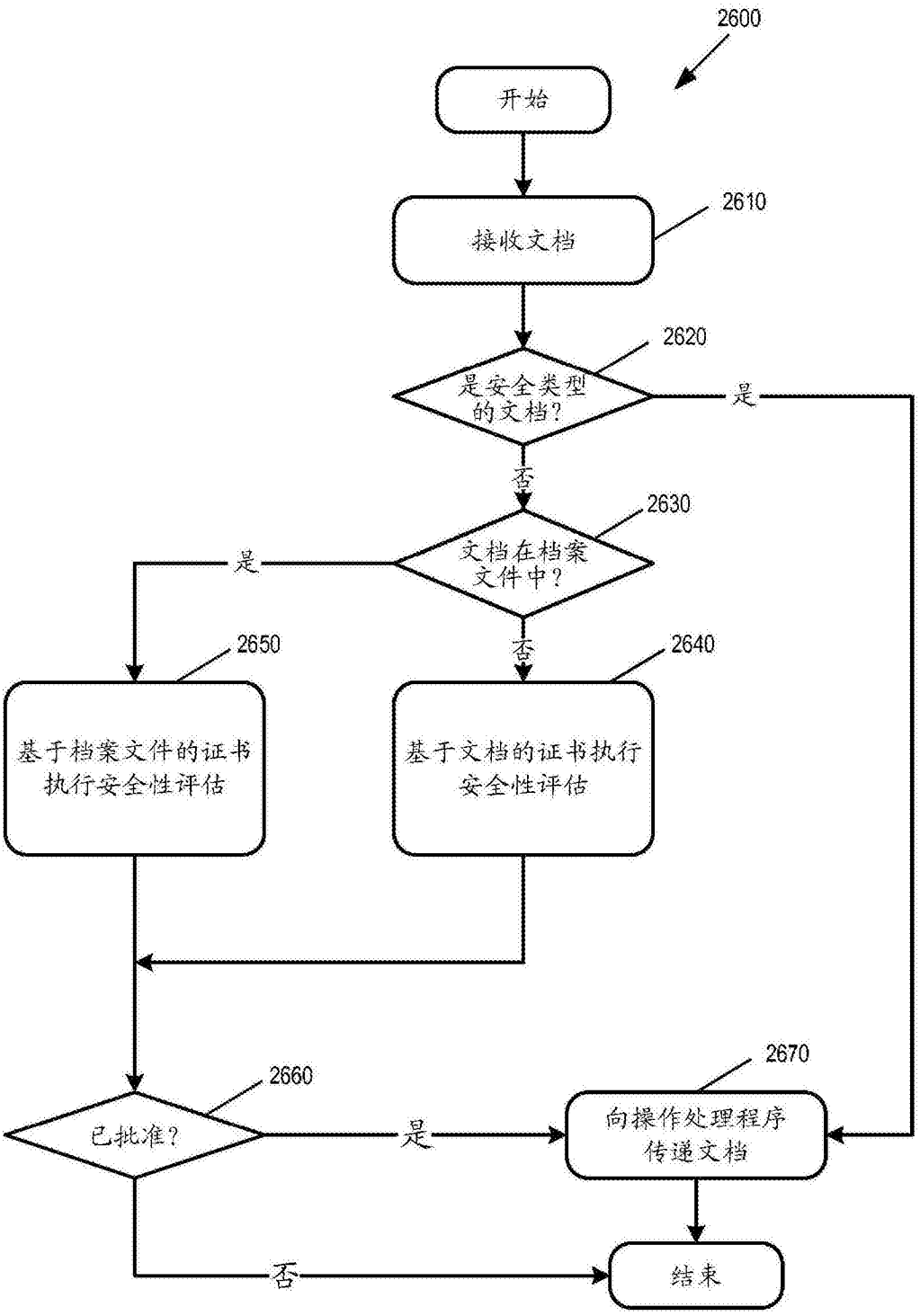

2600
开始
2610
接收文档
2620
是安全类型的文档?
是
否
2630
文档在档案文件中?
是
否
2650
基于档案文件的证书执行安全性评估
2640
基于文档的证书执行安全性评估
2660
已批准?
是
2670
向操作处理程序传递文档
否
结束

图26

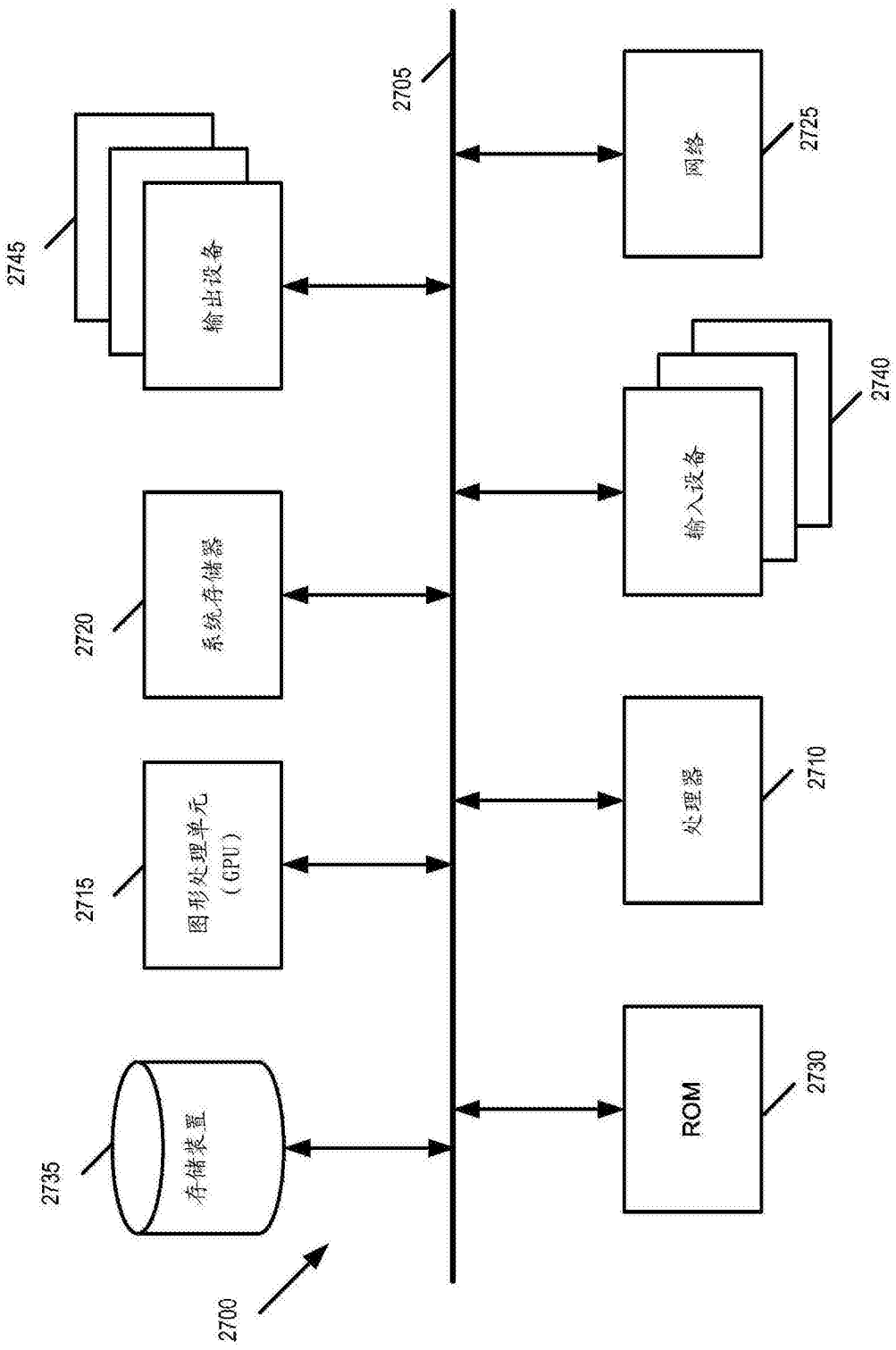

2705
网络
2725
2745
输出设备
输入设备
2740
2720
系统存储器
处理器
2710
2715
图形处理单元
(GPU)
ROM
2730
2735
存储装置
2700

图27