[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 15/16 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200780024553.9

[43] 公开日 2009 年 7 月 8 日

[11] 公开号 CN 101479716A

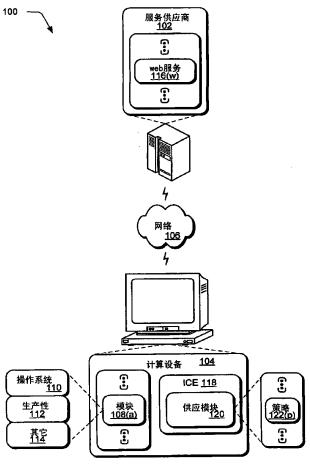
[22] 申请日 2007.6.7
[21] 申请号 200780024553.9
[30] 优先权
[32] 2006. 6.29 [33] US [31] 11/427,666
[86] 国际申请 PCT/US2007/013533 2007.6.7
[87] 国际公布 WO2008/005148 英 2008.1.10
[85] 进入国家阶段日期 2008.12.29
[71] 申请人 微软公司
地址 美国华盛顿州
[72] 发明人 J·杜弗斯 T·G·菲利普斯
A·弗兰克 W·J·威斯特瑞恩
[74] 专利代理机构 上海专利商标事务所有限公司
代理人 顾嘉运
权利要求书 3 页 说明书 21 页 附图 10 页

[54] 发明名称

独立计算环境以及计算设备功能的供应

[57] 摘要

描述了提供独立计算环境的技术。 独立计算环境至少部分包含在一或多个硬件组件的集合中，并且配置为寄宿可执行以按照各种各样因素供应计算设备的功能的供应模块。 在一个实现中，当供应模块确定在含括列表提及特定的功能时，许可计算设备访问该特定的功能。 当供应模块确定在排除列表中提及该特定的功能时，阻止计算设备访问该特定的功能。



1.一种方法，包括在独立计算环境(118)中执行供应模块(120)以将计算设备(104)的网络访问绑定于一或多个 web 服务，所述独立计算环境(118)至少部分包含在所述计算设备(104)的一或多个硬件组件中。

2.如权利要求 1 所述的方法，其特征在于，所述供应模块通过使用含括列表将所述计算设备绑定于一或多个 web 服务。

3.如权利要求 1 所述的方法，其特征在于，所述供应模块通过使用排除列表将所述计算设备绑定于一或多个 web 服务。

4.如权利要求 1 所述的方法，其特征在于：

所述计算设备被绑定，使得在不使用用户的个人可标识信息的情况下对所述一或多个 web 服务的访问可用；以及

通过使用个人可标识信息使得对另一个 web 服务的访问可用。

5.如权利要求 1 所述的方法，其特征在于，保护所述独立计算环境使包括操作系统在内的所述计算设备的其它模块不能进行未经授权的访问。

6.一种方法，包括：

提供通过使用供应模块(120)而绑定于访问服务供应商的一或多个 web 服务(116(w))的计算设备(104)，所述供应模块(120)可在至少部分包含在所述计算设备(104)的一或多个硬件组件中的独立计算环境(118)内执行；以及

资助所述计算设备(104)的至少一部分买价。

7.如权利要求 6 所述的方法，其特征在于，所述计算设备被绑定，使得在不使用用户的个人可标识信息的情况下对所述一或多个 web 服务的访问可用。

8.如权利要求 6 所述的方法，其特征在于，所述资助是由所述服务供应商执行的。

9.如权利要求 6 所述的方法，其特征在于，所述资助是通过所述服务供应商收取广告收入来执行的。

10.如权利要求 6 所述的方法，其特征在于：

所述资助是通过从所述计算设备的用户收取用于维持所述计算设备上的余额的费用来执行的；以及

所述余额由所述供应模块用来管理对所述计算设备的功能的访问。

11.如权利要求 6 所述的方法，其特征在于，所述绑定是通过使用含括列表和排除列表来执行的，所述含括列表指定许可由所述计算设备访问的 web 服务，所述排除列表指定不许可由所述计算设备访问的 web 服务。

12.一种计算设备(104)，包括：

配置维护下列各项的安全存储(214)：

提及许可经由所述计算设备访问的功能的含括列表(218)；和

提及不许可经由所述计算设备访问的功能的排除列表(220)；以及

一或多个硬件组件，被配置为提供独立计算环境(118)，其中，可执行供应模块(120)以标识功能以及通过使用所述含括列表和排除列表来确定是否许可对所标识的功能的访问。

13.如权利要求 12 所述的计算设备，其特征在于：

所述安全存储还被配置为维护条件；以及

可执行所述供应模块以在所述含括列表和所述排除列表没有提及所标识的功能时确定是否许可对所标识的功能的访问。

14.如权利要求 13 所述的计算设备，其特征在于，所述条件许可所标识的功能在所述处理器上执行指定数量的周期，在此之后阻塞执行。

15.如权利要求 13 所述的计算设备，其特征在于，保护所述独立计算环境使包括操作系统在内的所述计算设备的其它模块不能进行未经经授权的访问。

16.如权利要求 13 所述的计算设备，其特征在于，所述含括列表或者所述排除列表在预定时间量后期满，在此之后由所述供应模块实现硬件锁定模式。

17.如权利要求 13 所述的计算设备，其特征在于，所述含括列表或所述排除列表包括有关启用所述特定功能的一或多个条件。

18.如权利要求 17 所述的方法，其特征在于，所述条件中的至少一个指定：

特定时间量，在所述特定时间量期间，许可对所述特定功能的访问；或者

在启用所述特定功能之前要由服务供应商收取的付费。

19.如权利要求 17 所述的方法，其特征在于，所述条件中的至少一个指定广告消费的证据。

20.如权利要求 13 所述的计算设备，其特征在于：

使用第一技术标识所述特定功能以确定所述特定功能是否在所述含括列表中提及；

使用第二技术标识所述特定功能以确定所述特定功能是否在所述排除列表中提及；以及

所述第一技术不同于所述第二技术。

独立计算环境以及计算设备功能的供应

背景

在传统商业模型中，消费者购买计算设备和用于在计算设备上执行的软件两者。因此，传统计算设备通常配置为对软件进行“开放”且“通用”的执行以及能够对用户所需的服务且不因其本身而限于执行特定的软件和/或访问特定的服务。

例如，在这些传统商业模型中，消费者可购买具有允许执行诸如游戏、文字处理程序、电子表格等等各式各样可从各种厂商获得的应用程序的操作系统的台式个人计算机（PC）。另外，这些应用程序中的一或多个（例如浏览器）可允许访问各种各样的服务诸如网页等等。因此，台式 PC 供应商（例如制造商）一般使用允许 PC 执行尽可能多的这些不同应用程序的配置，这可对尽可能多的服务提供访问。以此方式，可用于消费者的功能且因此消费者对 PC 的需求增加。

然而，作为“通用”计算设备的配置一般将计算设备限制于这些传统的商业模型且因而限制计算设备的销售商利用其它商业模型。例如，一个销售者想要使用一种消费者“到期即付（pay as they go）”的商业模型。因此，在该示例中，计算设备的销售者可资助计算设备的初始买价以便在以后从用户收取收入，诸如通过网络向消费者销售服务和/或软件之类。然而，如果计算设备被配置用于软件的通用执行，则消费者可选择放弃对销售者的服务和/或软件的使用，从而消除了销售者资助计算设备成本的动机。

概述

描述了提供独立计算环境的技术，它可用于控制“开放”和“通用”的计算设备的功能。独立计算环境至少部分地包含在一或多个硬件组件的集合中。独立计算环境配置为寄宿可执行以按照各种各样因素供应计算设备的功能的供应模块。

在一实现中，在独立计算环境中执行供应模块。当供应模块确定在含括列表中提及特定的功能时，许可计算设备访问该特定的功能。当供应模块确定在排除列表中提及该特定的功能时，阻止计算设备访问该特定的功能。

在另一个实现中，提供通过使用供应模块绑定于访问服务供应商的一或多个 web 服务的计算设备。供应模块可在至少部分地包含在计算设备的一或多个硬件组件中的独立计算环境中执行。资助计算设备的至少一部分买价。

提供本概述以简化形式介绍在下面的详细描述中进一步描述的一些概念。本概述不是旨在标识要求保护的主题的关键特征或者必要特征，也不是旨在用于帮助确定要求保护的主题的范围。

附图简述

参考附图描述详细描述。在附图中，参考标号的最高位数字标识该参考标号首次出现的附图。在描述和附图的不同实例中使用相同的参考标号指示相似或相同的项目。

图 1 是可用于使用各种技术来提供独立计算环境的示例性实现的环境的图示。

图 2 是更详细地示出图 1 的服务供应商和计算设备的示例性实现中的系统的图示。

图 3 是包括测量在存储器中运行的主题代码（subject code）的一或多个集合的健康状况的独立计算环境的体系结构的图示。

图 4 是包括并入处理器中、测量在存储器中运行的主题代码的一或多个集合的健康状况的独立计算环境的体系结构的图示。

图 5 是示出表示可关于测量主题代码的健康状况而存在的各种时间窗口的示例性时序图的图示。

图 6 是描绘其中提供绑定于一或多个 web 服务的受资助计算设备的示例性实现中的过程的流程图。

图 7 是描绘其中模块在绑定于与特定 web 服务交互的计算设备上执行的示例性实现中的过程的流程图。

图 8 是描绘其中通过在独立计算环境中执行供应模块来使用余额管理计

算设备的功能的示例性实现中的过程的流程图。

图 9 是描绘其中使用含括列表和排除列表管理计算设备的功能的示例性实现中的过程的流程图。

图 10 是描绘其中结合相应的含括列表/排除列表使用不同的标识技术管理模块的执行的示例性实现中的过程的流程图。

详细描述

综述

传统商业模型允许消费者购买配置为执行也由消费者购买的软件的计算设备（例如台式个人计算机）。因此，该传统商业模型提供两种收入流，一是给计算设备的制造商和销售者的，而另一个是给软件的开发者和销售者的。另外，第三个收入流可由通过计算设备消费的 web 服务的销售者获得，诸如对特定网站的预付费访问。因而，传统的计算设备配置为“开放”或“通用”使用，使得消费者不因计算设备而限于执行特定软件和访问特定 web 服务。然而通过将计算设备配置为通用使用，计算设备可能不适于在其它商业模型诸如在资助计算设备的全部或部分买价以便以后从对设备的使用收取收入的模型中使用。

描述创建一种可用于保证执行特定软件的独立计算环境的技术。该特定软件例如可配置为按照指定计算设备的所需操作的策略来供应计算设备的功能。销售者例如可使用“按使用付费”模型，在该模型中销售者通过销售允许使用计算设备有限时间量、预定的次数、执行预定数量的功能等等的预付费卡来获得收入。在另一个实例中，软件供应商提供对软件的基于订阅的使用。在又一个实例中，服务供应商提供对 web 服务的收费访问。在这些实例中，策略可指定要如何管理计算设备的功能以保证计算设备用支持该模型的方式来使用。例如，可结合通过支付费用获得访问的特定 web 服务来限制用户对计算设备的使用。因此，服务供应商可资助计算设备的成本以便在用户访问服务时从用户获得收入。还设想各种其它示例。

独立计算环境可使用各种技术来管理计算设备的功能。例如，供应模块在执行时可通过含括列表和排除列表管理哪些应用程序和/或 web 服务被许可与计算设备交互。含括列表可指定许可计算设备使用哪些功能（例如应用程序、

web 服务等等）。另一方面，排除列表可通过诸如指定盗版应用程序、不信任的网站等等来指定哪些功能不被许可。因此，在标识要结合计算设备使用的 web 服务或应用程序之后，供应模块可确定是否许可该动作。此外，供应模块还可使用用于应用程序和/或 web 服务的策略，这些策略解决在含括列表或排除列表中未提及该功能的情况。管理计算设备关于特定 web 服务的使用将参考图 6-8 进一步讨论。排除与排除列表的使用将参考图 9-10 进一步讨论。

在下面的讨论中，首先描述可用于执行各种技术以提供独立执行环境的示例性环境和设备。随后描述可在示例性环境使用和/或由示例性设备实现的以及也可在其它环境中和/或由其它设备实现的示例性过程。

示例性环境

图 1 是在可用于使用各种技术来提供独立计算环境的示例性实现中的环境 100 的图示。所示环境 100 包括以通信方式经由网络 106 相互耦合的服务供应商 102 和计算设备 104。在下列讨论中，服务供应商 102 可表示一或多个实体，且因此可以指单一实体（例如服务供应商 102）或多个实体（例如服务供应商 102、多个服务供应商 102 等等）。

计算设备 104 可用各种方式来配置。例如，计算设备 104 可配置为台式计算机、移动站、娱乐设备、以通信方式耦合至显示设备的机顶盒、无线电话、游戏控制台等等。因而，计算设备 104 的范围从具有大量存储器和处理器资源的全部资源设备（例如个人计算机、游戏控制台）到具有有限存储器和/或处理资源的低资源的设备（例如，传统的机顶盒、手持式游戏控制台）。

尽管网络 106 例示为因特网，但网络可采用各种各样的配置。例如，网络 106 可包括广域网（WAN）、局域网（LAN）、无线网络、公用电话网络、内联网等等。此外，尽管示出单个网络 106，但网络 106 可配置为包括多个网络。

计算设备 104 被示为具有一或多个模块 108(a)（其中“a”可以是从一至“A”的任何整数，它在下面讨论中的实例中也被称为“代码”和“代码集合”）。模块 108(a)可用提供各种功能的各种方式来配置。例如，模块 108(a)之一可配置为其它模块 108(a)的执行提供基础的操作系统 110。其它模块 108(a)例如可配置为具有生产性应用程序 112，诸如文字处理程序、电子表格、幻灯片演示

应用程序、图形设计应用程序和笔记记录应用程序。模块 108(a)也可用各种其它方式 114 来配置，诸如配置为网络访问（例如浏览器）的游戏等等。例如，模块 108(a)在执行时可通过网络 106 与一或多个 web 服务 116(w)交互。此外，模块 108(a)可配置为添加功能至其它模块，诸如通过作为“插件”模块配置。

如前所述，在传统商业模型下，计算设备一般配置为“通用”或“开放”使用，使用户能够按需访问各种各样的模块和/或 web 服务。然而这样的“通用”和“开放”配置使计算设备无法利用其它商业模型，在这些商业模型中计算设备的成本由另一个实体诸如软件供应商、网络访问供应商、web 服务供应商等等资助的。例如，这些其它实体可向 web 服务的使用收取收入并因此资助计算设备的成本以鼓励用户使用这些 web 服务。在另一个示例中，可使用“按使用付费”模型，其中资助计算设备的初始成本并且用户以各种方式为计算设备的使用付费，诸如订阅费、为规定的时间量支付的费用、为使用规定的资源量支付的费用等等。

因此，图 1 的计算设备 104 配置为提供一种环境，其中可保证对特定软件的执行以强制按计算设备 104 的制造商/销售者所需的方式来使用计算设备 104。例如本文描述的技术的各方面针对可按实际上实时发生的常规进行方式测量任何给定软件代码以（例如，对其完整性和真实性）进行验证的技术。如本文使用的，对于软件代码而言，术语“测量”及其变化形式（例如，“经测量”、“正在测量”、“测量”等等）通常指对完整性和/或认证检查的任何抽象，其中存在若干方式来确认完整性和/或认证过程。下面描述测量的一些示例方式，然而该测量抽象不受限于这些示例，并且包括用于评估软件代码和/或其执行的未来技术。

例如可测量模块 108(a)，并且如果模块 108(a)没有被验证为“健康”例如按计算设备的销售者所愿地运行，则施加某种处罚。例如，作为处罚，计算设备 104 可在执行“不健康”模块时关机，可（至少部分地）用令正常使用不可用的某种方式来降低其性能，可强迫管理员联系软件厂商或者制造商进行修复/许可，可（例如通过捕获）停止不健康模块等等。对于访问 web 服务 116(w)，也可应用相似的技术。

一般而言且如上所述，与在开放操作系统的情形中一样，可替换或者可修

改的软件通常不是用于测量软件代码健康状况的可接受机制。然而描述了其中（例如基于处理器的）硬件辅助的机制/解决方案提供独立于操作系统 110 的外部信任根的技术。如下面也要描述的，要测量诸如二进制模块的代码集合的完整性，硬件机制可采取措施来补偿实时方法的缺乏，并且还可提供有关执行每个主题二进制模块的数据以帮助获得有关其健康状况的结论。

在一个示例实现中，硬件机制包括独立（有时可替换地称为隔离）的计算环境（或 ICE）118，它包括任何代码、微代码、逻辑、设备、另一设备的一部分、虚拟设备、建模成设备的 ICE、集成电路、电路与软件的混合结构、智能卡、上述的任意组合、执行本文所述的 ICE 功能的任何装置（与结构无关）等等，它们（例如用硬件）受到保护而不被他方篡改，包括经由操作系统 110、总线主控器等等进行的篡改。

ICE 118 允许寄宿于独立计算环境的逻辑（例如硬布线逻辑、闪存化的代码、寄宿的程序代码、微代码和/或基本上任何计算机可读指令）与操作系统 110 交互，例如让操作系统提示主题模块大概驻留的位置。多个独立计算环境是可行的。例如，监视多个不同网络地址、多个存储器区域、多个存储器区域的不同特征等等的独立计算环境可以满足需求。

例如，ICE 118 示为包括供应模块 120，它表示应用描述要如何管理计算设备 104 的功能的一或多个策略 122(p)（其中“p”可以是从一至“P”的任何整数）的逻辑。例如，通过验证供应模块 120 在计算设备 104 上的执行，可防止计算设备 104 被“黑”和用于在所设想的商业模型之外的其它目的。此外，当供应模块 120 在 ICE 118 内执行时，可测量其它模块 108(a)的“健康状况”来保证这些模块 108(a)按策略 122(p)所述地运行。

供应模块 120 例如可强制实施控制计算设备 104 能够访问哪些 web 服务 116(w)的策略。例如，供应模块 120 可监视模块 108(a)的执行以保证模块 108(a)用于访问 web 服务 116(w)的网络地址被许可。另外，提供 web 服务 116(w)的服务供应商 102 可从计算设备 104 的用户收取访问 web 服务 116(w)的费用。这些费用可用于支持“资助”商业模型，在该模型中服务供应商 102 随后可抵消计算设备 104 的部分初始购买成本以便在以后收取这些费用，这将参考图 6 进一步讨论。

在另一个示例中，可执行供应模块 120 以强制实施基于含括列表和排除列表许可访问模块 108(a)和/或 web 服务 116(w)的策略 122(p)。供应模块 120 例如可使用精确标识技术（例如密码散列）来确定模块 108(a)是否包括在可由计算设备 104 使用的“得到许可”的功能的列表中。供应模块 120 也可使用用于确定模块 108(a)和/或 web 服务 116(w)是否在排除在计算设备 104 上使用的功能列表中的标识技术（其精确性比用于含括列表的差，诸如签名测量）。此外，供应模块 120 使用的策略 122(p)也可指定在功能（例如模块 108(a)和 / 或 web 服务 116(w)）没有包括在任一这些列表中时要采取的各种各样的动作，对此的进一步讨论可关于以下附图找到。

一般而言，本文描述的任何功能可以使用软件、固件、硬件（例如固化逻辑电路系统）、人工处理或者这些实现的组合来实现。如本文使用的术语“模块”、“功能”和“逻辑”一般表示软件、固件、硬件或它们的组合。在软件实现的情形中，模块、功能或逻辑表示在处理器（例如一或多个 CPU）上执行时完成指定任务的程序代码。程序代码可以存储在一或多个计算机可读存储器设备例如存储器中。下面描述的技术的特征是平台无关的，意思是这些技术可在具有各种处理器的各种商业计算平台上实现。

图 2 例示更详细地示出图 1 的服务供应商 102 和计算设备 104 的示例性实现中的系统 200。服务供应商 102 例示为由服务器 202 实现，它可表示一或多个服务器例如服务器场。服务器 202 和计算设备 104 各自示为具有相应的处理器 204、206 和相应的存储器 208、210。

处理器不受形成它们的材料或者其中所使用的处理机制的限制。例如，处理器可由半导体和/或晶体管（例如电子集成电路（IC））组成。在这样的上下文中，处理器可执行指令可以是可用电子方式执行的指令。或者，处理器的机制或者用于处理器的机制，且因而计算设备的机制或者用于计算设备的机制可包括但不限于量子计算、光计算、机械计算（例如使用纳米技术）等等。

另外，尽管分别为服务供应商 102 和计算设备 104 示出单个存储器 208、210，但可使用各种各样类型的存储器和存储器组合，诸如随机存取存储器（RAM）、硬盘存储器、可移动介质存储器以及其它类型的计算机可读介质。例如，计算设备 104 的存储器 210 例示为包括配置为随机存取存储器（RAM）

212 的易失性存储器并且还包括例示为与 RAM 212 分开的安全存储 214。

安全存储 214 可用各种方式来配置，诸如通过系统管理随机存取存储器（SMRAM）、用于包含基本输入/输出系统（BIOS）的存储器 210 的一部分、利用可使用散列或等价物来独立地验证的加密的“智能芯片”等等。在一个实现中，安全存储 214 对于操作系统 110 和“存在于”ICE 118“之外”的其它模块 108(a)都是不可访问的（读或写访问）。然而在另一个实现中，全部或部分安全存储 214 对于“外面”的模块 108(a)可用于读访问，但不能用于写访问。

如前所述，供应模块 120 表示强制实施与计算设备 104 的功能有关的策略 122(1)-122(P)的功能，这些策略可以用各种方式来配置。例如策略 122(1)示为是“基于 web 服务”的，使得供应模块 120 可使用该策略来确定哪些 web 服务 116(w)允许使用计算设备 104 来访问。例如，供应模块 120 可使用 ICE 118 的经修改硬件中的信任根在引导时确认某些软件组件和用户界面元素存在、执行和指向所许可的网络地址（例如统一资源定位符（URL）、互联网协议（IP）地址等等）。

这些软件组件进而可通过与管理程序模块 216 交互来与服务供应商 102 的 web 服务 116(w)执行相互认证，管理程序模块 216 被示为在处理器 204 上执行并且可存储在存储器 208 中。在另一个实例中，软件组件向服务供应商 104 的管理程序模块 216 的认证是经由供应模块 120 来执行的。通过执行管理模块 216，服务供应商 104 还可接收 web 服务 116(w)被计算设备 104 消费的证明（可被签名）。因而，在该实例中策略 122(1)可提供 web 服务 116(w)的货币化并且针对资助消费者对计算设备 104 的初始买价而利用该货币化。将参考图 6-8 进一步讨论基于 web 服务的供应。

在另一个实例中，策略 122(p)示为被配置为通过使用含括列表 218、排除列表 220 和条件 222 来控制计算设备 104 的功能。例如，可执行供应模块 120 来诸如通过密码散列、对数据签名技术的使用等等来标识模块 108(a)和/或 web 服务 116(w)。供应模块 120 随后可将该标识与含括列表 218 比较以确定对该功能的访问是否被明确许可，且如果是则许可访问。例如，含括列表 218 可包括许可功能诸如来自资助计算设备 104 的初始买价的实体的模块 108(a)的网络地址和密码散列的列表。

供应模块120还可将该标识与排除列表220比较以确定对该功能的访问是否被明确限制。例如，排除列表220可包括应用程序的盗版形式的密码散列，且因此供应模块120在执行时可排除这些模块在计算设备104上执行。此外，策略122(p)可指定当模块和/或web服务不在任一列表中时要采取的动作的条件222，诸如许可有限时间量的执行直至可从服务供应商104获得对含括列表或排除列表的更新（示为包括含括列表的更新版本218'、排除列表的更新版本220'和条件的更新版本222'的列表）。将参考图9-10进一步讨论基于含括列表和排除列表的供应。

在又一实例中，策略122(P)示为基于计算设备104所维护的余额224。在例示的实现中，执行供应模块120以强制实施为计算设备104指定多个功能模式的策略122(P)，对其的强制实施基于在计算设备104本地上维护的余额224。例如，多个功能模式可包括全部功能模式，在该模式中许可计算设备104使用计算设备104的全部资源（例如处理器206、存储器210、网络和软件）来执行模块108(a)。

也可提供减少功能模式，在该模式中计算设备104的功能受到限制，诸如通过许可对应用程序模块108(a)的受限执行。例如，减少功能模式可在过了某个时间量之后阻止应用模块108(a)的执行，从而使用户能够保存和传送数据，但不许可延长与应用模块108(a)的交互。

此外，还可指定硬件锁模式，在该模式中阻止除供应模块120之外的软件的执行。例如，硬件锁定模式可完全阻止操作系统110在处理器206上的执行，并且由此阻止依赖操作系统110使用计算设备104的资源的模块108(a)的执行。

可取决于余额224进入这些不同操作模式每一个。因此，余额224的调整可引起进入不同的模式，且因此余额的调整被用于控制计算设备的功能。例如余额224可支持“按使用付费”商业模型，其中按周期性间隔减少余额224。例如，可因计算设备104的（例如由嵌入的控制器引起的）硬件中断的周期性输出而按周期性间隔执行供应模块120，从而帮助形成ICE 118。因此，供应模块120也可在这些周期性间隔时间期间执行时减少余额224，且因而随着计算设备104被使用而“降低”余额。

为“提高”余额，计算设备104可与服务供应商102的管理程序模块216

维护的特定帐户相关联。例如，诸如响应于从服务供应商 102 的人类操作员（例如客户支持人员）收到的输入、自动和在用户干预下通过与供应模块 120 交互（例如，传输用于从消费者的帐户检索记帐信息的标识符）等等，管理程序模块 216 可使供应分组通过网络 106 通信至计算设备 104。供应分组在由供应模块 120 接收时可用于“提高”余额 224 且因此重新获得/维持对计算设备 104 的功能的访问。还设想各种其它实例，其中策略用于供应计算设备 104 的功能。

计算设备 104 还示为在安全存储 214 内维护秘密 226，它可用各种方式来利用。例如，秘密 226 可配置为用于验证模块 108(a)和 web 服务(w)交互的信任根。秘密 226 例如可配置为由供应模块 120 用来验证是否应当许可对计算设备 104 上的模块 108(a)的访问的公钥/私钥对中的私钥。还可设想各种其它示例，并将参考示例性过程来进一步讨论。

图 3 和 4 表示测量代码 302 或 402（可以对应图 1 和 2 的模块 108，也可以不对应）的一或多个集合、代码模块等等的健康状况的独立（或隔离）计算环境 300 或 400 的示例。代码 302 或 402 示为包括部分“C1-CN”，它们表示在示为配置为 RAM 212 的易失性存储器但也可设想其它类型的物理存储器内的一或多个存储器区域中运行的代码的各部分的示例。

如应当显而易见的，一或多个代码集合（示为 C1-CN）在物理存储器内不必是连续的，如在图 4 所示的 RAM 212 内的不连续集合中所表示的。在另一个实现中，测量虚拟存储器中的代码，诸如通过让操作系统 110 的虚拟存储器相关代码操纵虚拟至物理的映射。在该实现中，可由可信组件和/或由本文描述的 ICE 118 控制虚拟至物理的映射来测量物理存储器空间中的内容和指令行为。

在图 3 所示的实现中，ICE 118 是独立的实体（即不是诸如处理器 206 的另一个硬件组件的一部分）。在图 3 所示的替换实现中，ICE 118 示为被并入处理器 206 中，例如作为其电路的一部分或者作为同一物理包装中的独立电路。还有另外的实现可仅依赖于软件。

图 2 和 3 的独立计算环境 118 各自包括（或者以其它方式关联于）寄宿的逻辑（示为供应模块 120）以及相应安装的策略 122(p)，它们中的任一或全部可以至少部分是硬布线的和/或在以后因改变而被（例如有可能在期满时通过闪

存方式）注入。部分或全部策略可以位于供应模块 120 内和/或与其分开，例如编码成规则。供应模块 120 和/或策略 122(p)可被签名或者以其它方式知道是有效的（例如通过硬布线），并且可被要求呈现在某个计算机或某类计算机上。此外，不同的供应模块 120 和/或策略 122(p)可应用于不同类型的计算机。如仅作为一个示例，并入处理器 206 中的图 4 的 ICE 118 的供应模块 120 和/或其相关策略 122(p)可以不同于图 3 的 ICE 118 的供应模块 120 和/或其相关策略 122(p)。

尽管未示出所有可能的实现，但应理解独立计算环境可如图 2 那样独立，或者并入基本上任何合适的硬件组件（有可能但不必是如图 4 中的处理器）中，只要独立计算环境与篡改隔离。因而，其它替换实现是可行的。例如，ICE 118 可在其它硬件诸如在存储器控制器中实现，或者可以是（例如构建在主板中的）特殊 RAM 芯片的一部分。而且，尽管供应模块 120 和/或策略 122(p)可被视为 ICE 118 的一部分，但在物理上不要求它是相同的一或多个硬件组件的一部分，并且实际上独立计算环境可以由各种物理上不同的硬件组件构成。

为了使本文简单，下面的描述将使用图 4 的标号，除非另有说明。如可容易地了解的，独立计算环境的物理位置可在诸实施例之间改变，并且因而在描述独立计算环境的许多特征时图 4 的实施例的讨论可应用于各种其它实施例，包括图 3 的实施例。

无论是任何物理实现/实施例，ICE 118 都可具有彼此相似的多个特征。例如，图 4 的 ICE 118 向供应模块 120 提供对 RAM 212 的可靠访问，RAM 中驻留有正被测量的一或多个主题的代码集合 402（例如，图 1 中正被监视/确认/认证的一或多个模块 108(a)）。在一个实现中，为访问 RAM 212，供应模块 120 不依赖于操作系统 110 侧、用于访问的代理，因为操作系统可能会被损害。被测量的代码 402 可驻留在 RAM 212 中任何位置，只要 ICE 118 能够知道其所在“位置”。例如，ICE 118 可使用偏移量和/或可具有指向 RAM 212 或其它存储器中的窗口的指令指针（或指向多个窗口的多个指针）。另一个在某种程度上较简单的选择是保证要测量的代码集合 402 驻留在相同的物理地址空间中。

包含被测量的代码集合（例如 C1-CN）的一或多个存储器段可由称为存

储器监视组件或存储器看门狗的某种机制来监控。一般而言，在试图修改存储器中的至少一个指定位置时，存储器看门狗触发异常/事件；（注意至少一个“位置”包括少至单个位置或者包括任何连续或不连续的范围、存储器块或块集合）。这与任何存储器修改有关，包括源自处理器的和源自外设的 RAM 写请求。存储器控制器 304 或 404 可配置为提供这样的事件，且因而也应当基于不会容易地被损害的硬件，然而要理解，存储器监控组件/看门狗可包括软件或硬件或者软硬件的组合。

可使用用于处理存储器看门狗异常的各种技术。例如，在一个实现中，处理器 206 可在这样的异常期间中止，直至 ICE 118 的供应模块 120 和/或策略 122(p)清除为止。可替换地，ICE 118 可改为在试图改变修改主题代码 402 的区域中的 RAM 时，以其它方式处罚系统状态（例如阻塞有问题的代码、缩减系统、使系统复位或者以其它方式激活某种强制机制）。另一个替换方案是让独立计算环境阻塞对主题代码 402 的写访问。

关于主题代码 402 的测量，供应模块 120 可使用各种技术。例如，散列/数字签名/证书和/或其它数学计算可用于认证正确的二进制代码集合是否存在于其应当在的位置，诸如基于可与策略 122(p)中的一或多个相应值进行比较的数字签名技术（例如按照 Cert X.509 和/或 Rivest、Shamir 和 Adelman(RSA)标准）。或者，如果被测量的代码相对较小，则供应模块 120 可针对策略中匹配这些指令的值简单地评估其指令或者其某个子集。还有另一种选择是对代码进行统计或类似的分析，例如诸如其执行的模式，如下所述。可使用测量技术的任何组合。

应当注意，可用于评估存储器的计算可能要花费相当大量的时间来执行。实际上，被监控的范围可以根据正在读的存储器范围（例如线性地）改变。因而，取决于策略，看门狗可在读操作期间发生任何改变时触发重读，使得在当前正在读的位置之后已经读过的存储器不能改变。策略可指定这是允许的，或者可指定再次尝试，并且如果是再次尝试，则指定间隔多久（例如最多至某个极限）等等。

因而，供应模块 120 可用各种方法获得有关主题代码 402 的健康状况数据。获得健康状况数据的一种方法是让独立计算环境在代码 402 中的感兴趣点设置

软-ICE-捕获指令。可替换地，或者在捕获技术之外，硬件（例如处理器 206）可允许 ICE 118 查询有关主题代码 402 的执行的统计。这可通过定义寄存器（306 或 406）等触发对某些二进制指令或指令范围的执行的计数来完成。注意如果有的话，这些寄存器 306 或 406 可以存在于硬件中以避免篡改，诸如例示为图 3 的独立计算环境 118 的一部分或者在图 4 的处理器 206 中。

注意，感兴趣的被测量代码可具有附随的元数据，它可以如图 3 的元数据 308(m)所示表示为被测量代码的一部分和/或如图 4 的元数据 408(m)所示存储为策略 122(p)的一部分。元数据 308(m)、408(m)可描述各种信息，诸如要收集的何种统计数字、健康状况模块应当看上去如何的描述、健康状况模块应当在“何处”执行（例如数据寄存器、存储器地址）、含括列表和/或排除列表、在模块执行期间许可访问的网络地址等等。元数据 308(m)、408(m)可由模块作者和/或计算设备供应商例如制造商或销售者提供。例如，元数据 308(m)、408(m)可指定 ICE 118 应当每秒具有十至十五次对处理器 206、306 的控制，指定主题代码 302 中的某个地址（例如 A1）处的指令每当执行某个其它地址（例如 A2）处的指令时应当执行十次，等等。

可与主题代码集合相关联对 ICE 118（它本质上在站岗以确认顺应性）描述其健康状况状态的元数据 308(m)、408(m)的其他示例包括用于完整性和/或认证检查的数字签名和/或模块在每个周期（例如秒、分或其它）获得执行的预期次数。该执行次数可以是范围，并且可概括对整个代码集合，和/或具体到指令范围或者特定指令的粒度。代替或者在执行统计数字之外，可评估代码每隔多久驻留在存储器中的统计评估，例如一个模块必须加载到存储器中某个阈限量（或百分比）的时间和/或仅可以不在存储器中指定的时间量（或者每秒、分等等的次数）。

元数据 308(m)、408(m)的又一示例包括某些指令处的某些寄存器（例如图 2 的数据寄存器 310(r)）和/或存储器地址（例如图 3 的计算设备中的 RAM 212 的地址 410(a)）的预期值。这可以称为分布，例如作为具有概率权重的各种值或者值域。另一类型的元数据 308(m)、408(m)可指定若干寄存器和存储器地址的预期值之间的关系；例如，如果一个变量小于 10（Var1<10），另一个变量必须匹配某个准则（例如变量 Var2 在百分之 50 的时间大于、在百分之 25 的

时间大于 100，以及有时可以是 399；Var2 应当从不小于零）。

元数据 308(m)、408(m)的其它示例包括基于指令的内容。可针对指令相对于其它指令执行的次数来对这些指令计数，可任选地带有用于评估好的计数相对于坏的计数的统计数字/比率，使得可以容许较小数量的偶然差异。当发生看上去可疑但并不肯定是明确的违反时，策略可改为运行一种不同的算法、改变变量、更密切或者更频繁地监控等等。

元数据 308(m)、408(m)还有一些示例包括描述存储数据的位置与方式的内容。例如，元数据 308(m)、408(m)可描述其中要存储一个模块的特定存储器地址（例如图 4 的地址 410(a)）、图 3 的处理器 206 中的特定数据寄存器 310(r)等等。以此方式，元数据 308(m)、408(m)可指定一个“泡泡(bubble)”，其中通过诸如监视控制位、指针、状态位等等来监视与数据寄存器 310(r)和/或地址 410(a)的交互的尝试以许可代码 202、302 的执行。

另外，对“泡泡”的访问也可用各种方式来提供，诸如“显式”地向其它模块（例如操作系统 110）提供读访问和“隐式”地将对泡泡的访问限制于供应模块 120 且阻止其它模块来访问（换言之，泡泡及其存在性包含在 ICE 118 的边界之内）。可提供一或多个可任选的 API 以促进操作，诸如 Ice.BeginMemoryAddessO、Ice.EndMemoryAddress()、Ice.AccessPermitted()等等。

使用元数据和/或其它技术，ICE 118 经由供应模块 120 和策略 122(p)可测量和确认任何指定的代码集合（例如 C4）的完整性和真实性。例如，可编程 ICE 118 以查找一或多个模块的某个集合，或者预期指定哪个或哪些模块要进行确认的策略。

在正常操作期间，供应模块 120 可由操作系统请求激活。例如，ICE 118 可（经由内部定时器）给予操作系统一段宽限期来启动验证测量，并且如果该时间过去，独立计算环境可认为系统破坏（不健康）并且采取某个处罚措施。

注意，关于如上所述的测量时间，一个选择是指定要测量的主题代码集合（例如 C3）要驻留在相同的物理地址空间中。在这样的情形中，ICE 118 可试图进行投机性验证，包括在随机或伪随机的时刻。

在开始测量过程之前，供应模块 120 可“锁定”部分或全部主题代码，也称为目标模块。一个实现使用上述存储器变更看门狗来保证主题代码在一或多

个被监控区域中没有改变。另一个测量技术可针对写访问锁定存储器。

为此，供应模块 120 可向操作系统提供某种接口（可以是显式的或者有可能是隐式的）以重新确定 RAM 212 的用途。显式接口允许操作系统 110 通知 ICE 118 其重新确定 RAM 用途的意图；一般而言，这可视为操作系统 110 请求 ICE 118 许可重新确定 RAM 212 的用途。可提供一或多个可选 API 来促进操作，诸如 Ice.AskPermissionToRepurposeMemory()、Ice.SetValidationPolicy()、Ice.SuggestModuleAddress()、Ice.UpdateModuleMetaInfo()等等。

隐式接口可以基于存储器-看门狗-异常，它由 ICE 118 解释为对许可 RAM 重新确定用途的请求。在这些过程中，存在 ICE 118 不关心如何重新确定存储器的用途的时候，例如当代码不是正被测量的时候。例如，元数据可指示代码集合要每秒测量十次，并且在非测量时间期间操作系统可以用它要用的任何方式来使用存储器。

在 RAM 重新确定用途请求之后，ICE 118 可隐式或者显式地准予请求。在任何情形中，ICE 118 仍站岗以保证正被测量代码的健康，如服从关联于该被测量代码的元数据。

作为示例，给出一个独立计算环境（例如分层的、基于系统的或者类似“信任根”），需要各种特征来允许模块化认证。

一般而言，ICE 118 对计算设备 104 的存储器（例如诸如 RAM 212 的易失性存储器）提供可靠的读访问。供应模块 120 假设读操作既不被虚拟化，也没有重新映射到其它存储器或 I/O 空间，也没有以另一方式过滤或修改；（目前，现在的 BIOS 可以在硬件最佳实践芯片组时利用其子集）。ICE 118 还可允许供应模块 120 在某些存储器区域上设置看门狗，它将在每次修改这些存储器区域的内容时触发一或多个信号。看门狗提供有关物理存储器空间中的任何存储器内容改变（包括源自直接存储器访问（DMA）和总线主控器的改变）的警报。注意，现有的基于 x86 的计算机系统可通过使 BIOS 寄宿一个供应模块（例如只要主题代码在特定的存储器范围内保持固定就可测量主题代码的供应模块）来将 ICE 并入其 BIOS。

ICE 118 还可允许供应模块 120 获得有关指令指针在某些存储器范围内出现的统计。例如，可使用指令指针-看门狗以每当指令指针进入或者离开所关

注的指定存储器范围时即向 ICE 118 报警。其它模型是可行的，包括上述基于寄存器的模型。

还如上所述，ICE 118 还可配置为就被测量代码的活动的种类进行观察/证明。例如，作者可以用各种方式（例如在元数据中）描述模块的特征行为，只要独立计算环境可以测量和评估该行为。只要该模块在指定的行为（例如性能）包（envelope）之内工作，就认为该模块是健康的。

作为示例，用于概述以及遵循的相对直接的特征是输入/输出（I/O）操作。为此，经认证的模块可用如果被偷（例如放在另一个操作系统的映象中），则这些模块将必须保持健康以成功通过模块化认证的方式来固定。结果，如果将这些模块放在另一个操作系统的代码中，则它们将必须在没有虚拟化（除了在硬件设备本身之中）的情况下取得控制和直接访问。

作为另一个示例，经认证的模块可具有可与该模块交互的特定的一或多个网络地址有关的指定行为。例如，供应模块 120 可监视代码 304 以保证代码 304 指向“正确”的网络地址（例如，统一资源定位符（URL）、互联网协议（IP）地址等等），诸如由元数据、策略 122(p)等等指定的那些。

如上所述，ICE 118 可连续地监视正被测量的代码 302，但取决于策略 122(p)，可改为仅在策略 122(p)认为适当的时候监视代码 302。因此，诸如按照策略没有被连续监视的代码可被交换到存储器中，其中测量或统计收集在代码被交换到存储器时的期间对代码发生。

图 5 示出一个示例时序图，其中 ICE 118 偶尔地（例如，周期性地或者在某个事件时，或者甚至随机地）测量什么代码存在和/或它是如何操作的。注意，图 5 是用于存储器的内容的时序图；采用基于统计的分析，例如代码的某些指令相对于其它指令执行了多少次，或者采用基于频率的分析例如每个时间段代码的某些指令执行了多少次，“ICE 不关心”区域可实质上跨越整个时间，只要（例如在寄存器中的）计数在每次测量时都正确即可，这可以是固定的或者是不定时的。

策略 122(p)通常将决定何时以及需要什么类型的测量。例如，图 5 例示的时序图不要求被测量的代码一直保持在存储器中。因而，在图 5 中称为“上次确认”的前一测量完成状态之后存在（除了第一次）“ICE 不关心”时间帧。

在该时间帧中，操作系统可以在一或多个相应的被测量区域中按其所想要的任何方式交换进或留下新代码，因为它们在该时间没有被测量。如果被锁定，则存储器区域在此时可被解锁。

在“ICE 感兴趣”时间，ICE 118 可开始其测量，诸如对计数器复位等等，尽管如果在该时间帧内不正确也不执行强制措施。该时间帧还可对应于给予操作系统时间以完成某事的上述宽限期，只要它在该宽限期间期满之前触发独立计算环境即可。以此方式，ICE 118 可以操作或者不操作，但没有处罚将被确定，除非和直至在以后检测到某种违反。

当独立计算环境进行测量时，在“ICE 关心”时间帧内，测量必须开始并且在示为到达“性能包”的时刻是正确的，或者将激活某种类型的强制措施。再次，策略确定该定时、测量的类型、强制措施的类型等等。

一般而言，当确认失败或者部分或全部描述策略（例如，包括供应模块 120 所使用的任何数据）不存在时，ICE 118 通过以如上一般描述的某种方式改变其状态来惩罚计算机系统。例如，当存储器内的代码不是正确的代码集合和/或在测量时间没有正确地工作时，激活强制实施机制例如中止系统。其它示例包括锁定计算机系统、减慢计算机系统、以某种方式限制存储器、减慢 I/O、通过捕获指令影响（例如杀掉）有关进程、重写进程代码（例如用无限循环指令）等等。独立计算环境可警告重叠在先的操作系统 110 以采取任何处罚错误。

应当注意，众多的定时、测量类型、强制措施类型等等的组合可在各类计算机之间甚至在相同的计算机系统本身内变化。例如，在同一计算机中，一个被评估的代码模块可能必须在物理上一直驻留在存储器内的同一位置，另一个模块可被交换进去或出来但必须在测量时间存在，还有另一个模块可在任何时间交换但必须周期地满足性能要求（指它必须被执行足够多的次数来这么做）等等。

应当注意，在检测到违反时，所采取的强制措施可变化，并且不同类型的违反可导致不同类型的强制措施。例如，改变一个（例如高度重要的）代码模块可导致系统被 ICE 关闭，而改变另一个代码模块可导致操作系统得到通知以便向用户呈现警告或发送消息至计算机系统制造商、程序厂商等等（例如一些发许可证的实体）。如另一个示例，如上所述，缺少统计可能不会导致立即处

罚，但改为将导致更仔细的监控至少一段时间，以确定是否应当采取进一步的强制措施。

示例性过程

下面的讨论描述可利用先前描述的系统和设备实现的供应技术。每个过程的诸方面可用硬件、固件或软件或者它们的组合来实现。这些过程示为一组框，它们指定由一或多个设备执行的操作且不必受限于所示的执行相应框操作的顺序。在下面讨论的各部分中，将参考图 1-4 的环境。

图 6 描绘在提供在绑定于一或多个 web 服务的受资助计算设备的示例性实现中的过程 500。提供绑定于访问服务供应商的一或多个 web 服务的计算设备（框 602）。例如，图 2 的计算设备 104 可执行供应模块 120，它通过含括列表和排除列表限制对特定 web 服务 116(w)的访问。在另一个示例中，供应模块 120 限制配置为访问特定网站而不访问其它网站的模块的执行。还设想各种其它示例。

资助计算设备的至少一部分买价（框 604）。例如，服务供应商可收取因计算设备与一或多个 web 服务交互而获得的收入（框 606），诸如因为做广告、从计算设备用户收取的与 web 服务交互的费用、从用户收取的与计算设备本身交互（例如按使用付费）的费用等等。因而，这些费用可用于补偿计算设备的买价，它鼓励消费者购买计算设备并且随后与 web 服务交互。计算设备可用各种方式绑定于 web 服务，将参考下面的附图进一步讨论。

图 7 描绘在绑定于与特定 web 服务交互的计算设备上执行模块的示例性实现中的过程 700。引导计算设备（框 702），诸如通过从用户接收“开启”输入。

使用可经由独立计算环境执行的供应模块来验证要在计算设备上加载的模块（框 704）。供应模块 120 例如可在 ICE 118 内执行并且验证模块 108(a)是真实的，诸如通过使用存储在计算设备 104 中的秘密 226（例如加密密钥）、证书等等来认证模块 108(a)的签名。如前，模块 108(a)可用各种方式来配置，诸如配置为操作系统、网络访问模块（例如浏览器）等等。

web 服务例如可由计算设备的模块之一调用（框 706），诸如浏览器在响

应从计算设备的用户接收的输入、具有网络访问功能的“智能”模块等等的时候。

web 服务质询该模块（框 708），诸如通过使用加密密钥验证该模块以确定该模块是否被授权与该 web 服务交互。web 服务也可质询独立计算环境（框 710），诸如通过与供应模块 120 交互以使用秘密 226 验证计算设备。基于这些质询，作出有关是否许可 web 服务访问的判断（判定框 712）。如果许可访问（自判定框 712 的“是”），则计算设备与 web 服务交互（714），诸如阅读电子邮件、上传照片、购买媒体（例如歌曲、电影）等等。

然而当不允许 web 服务访问（自判定框 712 的“否”）时，形成付费用户界面用于与计算设备的通信（框 716）。付费用户界面可用作配置为接收付费信息的付费实体（例如，服务供应商、第三方收费服务等等）的“前端”。当收到有效的付费信息（自判定框 718 的“是”）时，计算设备与 web 服务交互（框 714）。如果否（自判定框 718 的“否”），则仍然输出付费用户界面（框 716）。例如，付费用户界面可在硬件锁定模式期间输出，在该模式中不许可在独立计算环境“之外”的模块 108(a)执行，包括操作系统，直至收到付费信息并且计算设备被“解锁”。可使用各种不同技术来“计量”计算设备的使用，参考下面的附图作进一步的讨论。

图 8 描绘在通过执行独立计算环境中的供应模块来使用余额管理计算设备的功能的示例性环境中的过程 800。如前所述，提供至少部分包含在计算设备的一或多个硬件组件中的独立计算环境（框 802）。本例中的供应模块配置为验证要在计算设备上执行的模块。

例如，从用户收到运行媒体播放模块（例如配置为输出音频和/或视频媒体）的输入。在检测到该输入时，在独立计算环境内执行的供应模块验证媒体播放模块（框 804），诸如通过检查数字签名、证书、密码散列并与含括列表/排除列表比较等等。如果验证成功，则许可媒体播放模块在计算设备上执行。

通过媒体播放模块向服务供应商的 web 服务请求内容（框 806），诸如下载特定电影、歌曲等等的请求。响应于该请求，web 服务向供应模块查询余额（框 808），它被传递至 web 服务。例如，供应模块可从安全存储 214 读取余额 224 并且向服务供应商 104 的管理程序模块 216 出示该余额。当余额足够（自

判定框 810 的“是”）时，web 服务使供应模块减少余额（框 812），诸如通过将内容传递给供应模块 120，后者随后解锁并减少余额 224。计算设备随后可呈现内容（框 814），诸如通过执行媒体播放模块。

当余额不足（自判定框 810 的“否”）时，输出付费用户界面（框 816）。例如，付费用户界面可将用户定向到一个网站，通过该网站用户可提交付费信息，诸如用户名、口令、信用卡信息等等。当收到足够的付费时，创建要通信至计算设备的付费分组（框 818）。供应模块随后可使用该付费分组来更新余额（框 820），诸如通过使用秘密 226 解密付费分组并且基于分组内的指令更新余额 224。还可设想各种各样的其它实例来更新和使用余额以控制计算设备 104 的功能，诸如在“到期即付”商业模型中，在计算设备 104 的操作期间过一段时间就减少余额并且更新余额以继续使用计算设备 104。

图 9 描绘使用含括列表和排除列表管理计算设备的功能的示例性实现中的过程 900。监视与特定功能交互的请求（框 902）。例如可执行供应模块 120 以监视运行模块 108(a)中特定的一个、与特定的 web 服务 116(w)等等请求。

标识特定的功能（框 904）。供应模块 120 例如可通过网络地址标识 web 服务 116(w)、通过密码散列、数字签名、证书等等标识模块 108(a)。随后由可在独立计算环境中执行的供应模块作出是否许可访问该特定功能的判断（框 906）。

供应模块 120 例如可实现指定访问要通过使用含括列表 218、排除列表 220 和条件 222 来管理的策略 122(p)。供应模块确定特定的功能是否包括在含括列表 218 上（判定框 910）。如果是（自判定框 908 的“是”），则许可访问该特定功能（框 910）。

当特定的功能不在含括列表上（自判定框 908 的“否”），则作出有关该特定功能是否在排除列表上的判断（判决框 912）。如果是（自判定框 912 的“是”），则阻止对该特定功能的访问（框 914）。

当特定功能不在排除列表上（自判定框 912 的“否”）时，可应用有关访问该特定功能的一或多个条件（框 912）。例如，对在这些列表中未指定的功能的访问可被许可预定的时间量（例如，多个周期）以给予更新列表来指定解决该特定功能的策略的机会。在另一个示例中，可基于所使用的功能来应用条

件，诸如配置用于网络访问的模块可让网络访问受到限制、许可不具有该类访问的模块执行等等。还设想各种其它示例。

图 10 描绘在结合相应的含括列表/排除列表使用不同的标识技术管理模块执行的示例性实现中的过程 1000。监视运行特定模块的请求（框 1002）。

使用第一标识技术标识特定模块（框 1004）。例如，可执行有关该特定模块的密码散列。随后可作出有关所标识的模块是否在含括列表上的判断（框 1006），并且如果是，则许可对该特定功能的访问（框 1008）。因此，在该例中，使用“精确”标识技术来标识模块以限制尝试模拟含括列表中提及的这些模块的其它模块的访问，诸如防止盗版等等。

另外，含括列表、排除列表、条件和/或标识技术可在计算设备 104 的操作期间被更新（框 1010）。例如，服务供应商 102 可通信发送解决“新”功能诸如新标识的应用模块盗版副本的更新。

当模块不在含括列表上（自判定框 1006 的“否”）时，使用比第一标识技术精度较差的第二标识技术标识该特定模块（框 1012）。例如，第一标识技术可以是密码散列而第二标识技术可以是数字签名，第一技术可以是第三方验证的证书而第二技术可以是自签署的证书，等等。

随后可作出有关使用第二技术标识的模块是否在排除列表上的判断（判定框 1014）。如果是（自判定框 1014 的“是”），则阻止对特定模块的访问（框 1016）。如果否（自判定框 1014 的“否”），则可应用有关对该特定模块的访问的一或多个条件（框 1018），诸如限制哪些存储器空间可由该模块访问、限制网络访问、许可预定时间量的执行等等。尽管关于特定模块描述不同标识技术的使用，但可将不同标识技术和列表的使用应用于各种各样的其它功能，诸如 web 服务等等。

结论

尽管已经以专用于结构特征和/或方法动作的语言描述了本发明，但要理解，在所附权利要求书中定义的本发明不必受限于所述的特定特征或动作。相反，特定特征和动作是作为实现所要求的本发明的示例性形式而公开的。

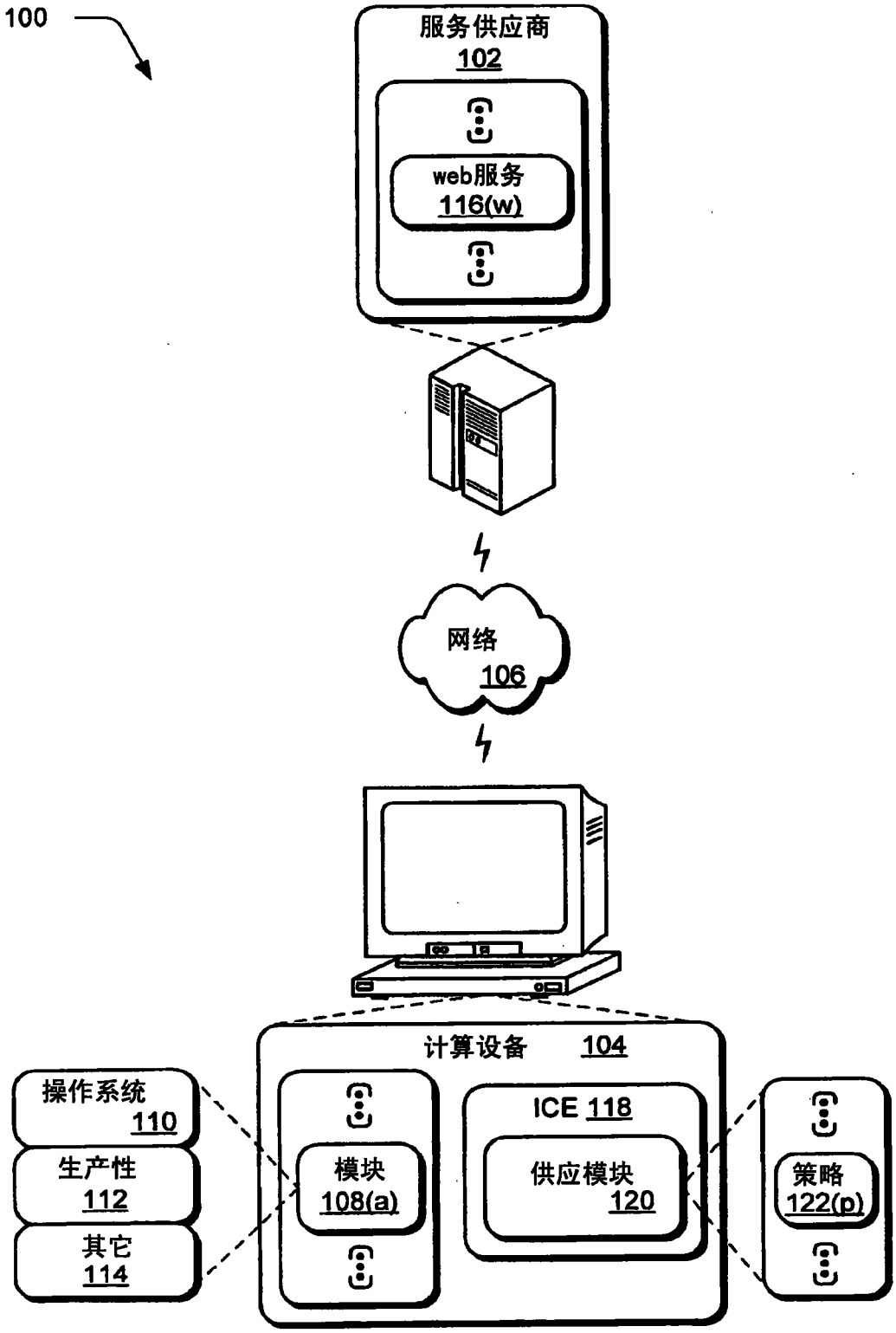

100
服务供应商
102
web服务
116(w)
网络
106
计算设备 104
操作系统
110
生产性
112
其它
114
模块
108(a)
ICE 118
供应模块
120
策略
122(p)

图 1

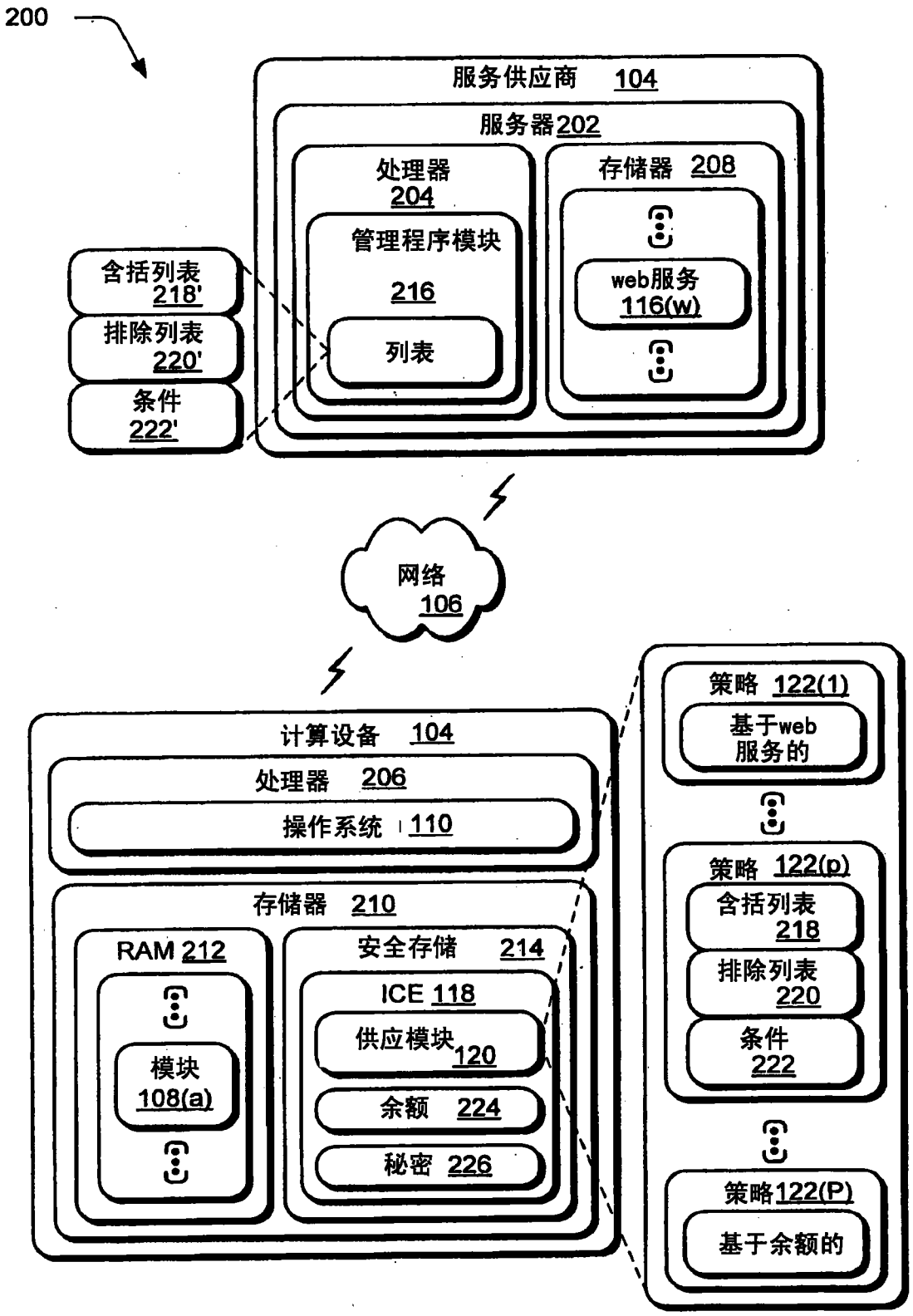

200
服务供应商 104
服务器202
处理器 204
管理程序模块 216
列表
存储器 208
web服务 116(w)
含括列表 218'
排除列表 220'
条件 222'
网络 106
计算设备 104
处理器 206
操作系统 110
存储器 210
RAM 212
模块 108(a)
安全存储 214
ICE 118
供应模块 120
余额 224
秘密 226
策略 122(1)
基于web服务的
策略 122(p)
含括列表 218
排除列表 220
条件 222
策略122(P)
基于余额的

图 2

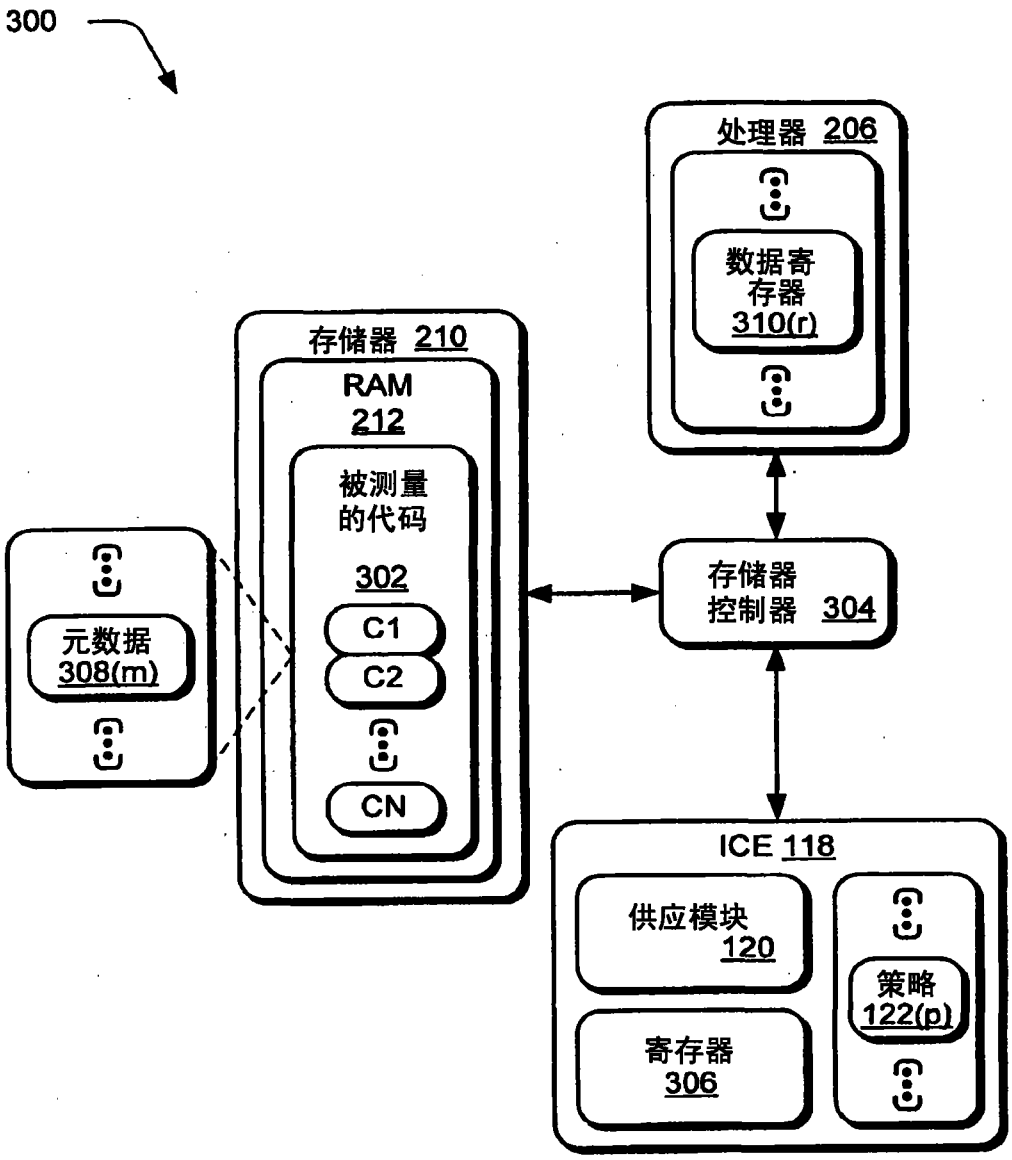

300
处理器 206
数据寄存器 310(r)
存储器 210
RAM 212
被测量的代码 302
C1
C2
CN
元数据 308(m)
存储器控制器 304
ICE 118
供应模块 120
寄存器 306
策略 122(p)

图 3

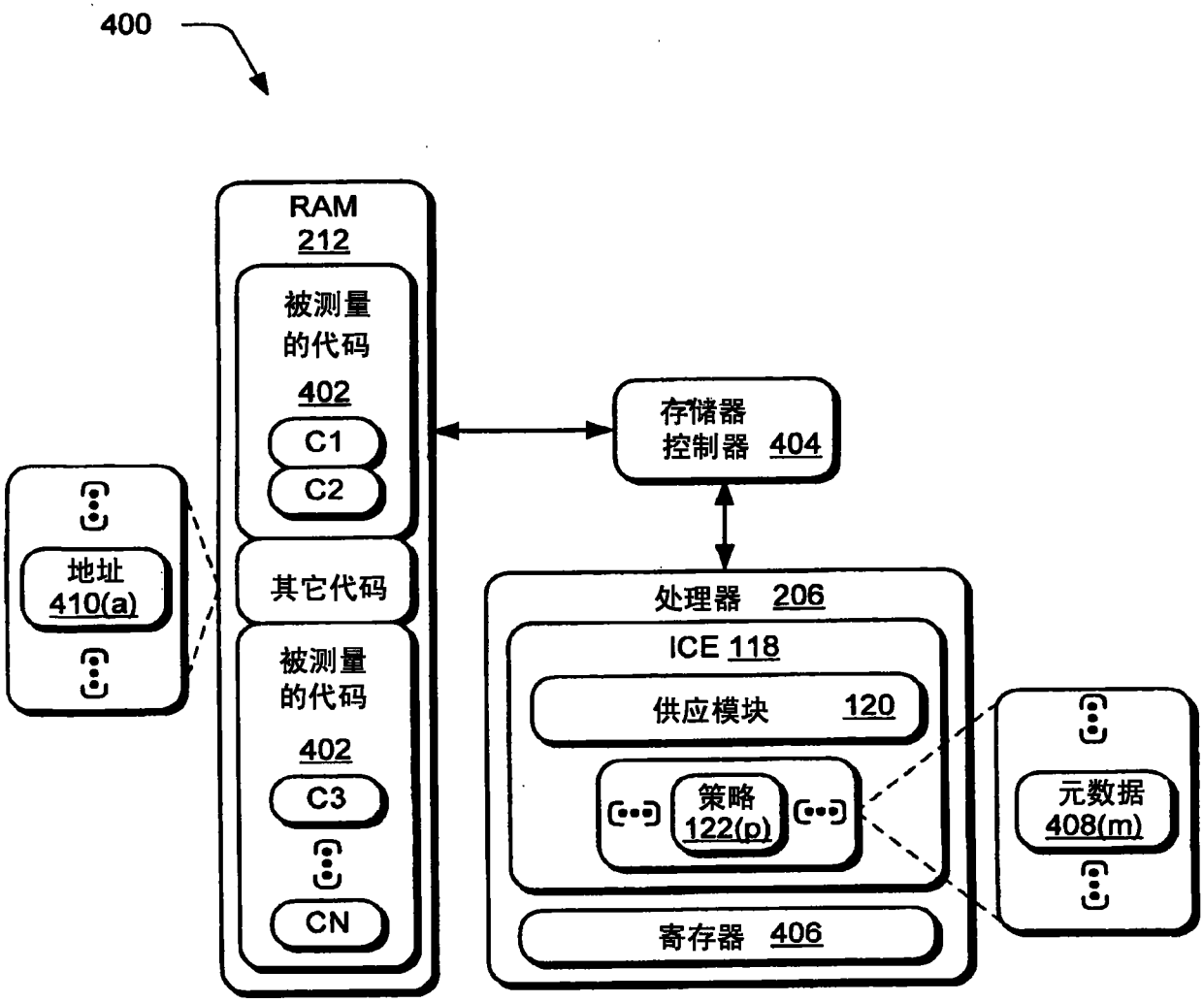

400
RAM
212
被测量
的代码
402
C1
C2
其它代码
被测量
的代码
402
C3
CN
地址
410(a)
存储器
控制器 404
处理器 206
ICE 118
供应模块 120
策略
122(p)
寄存器 406
元数据
408(m)

图 4

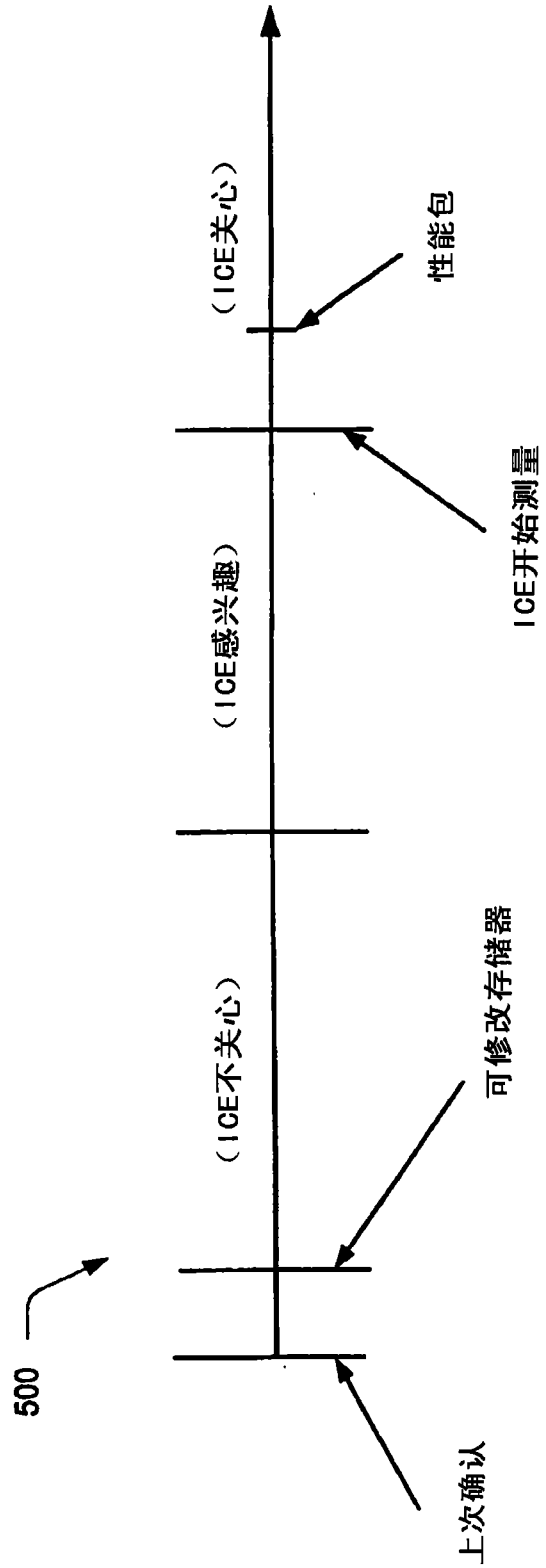


图 5

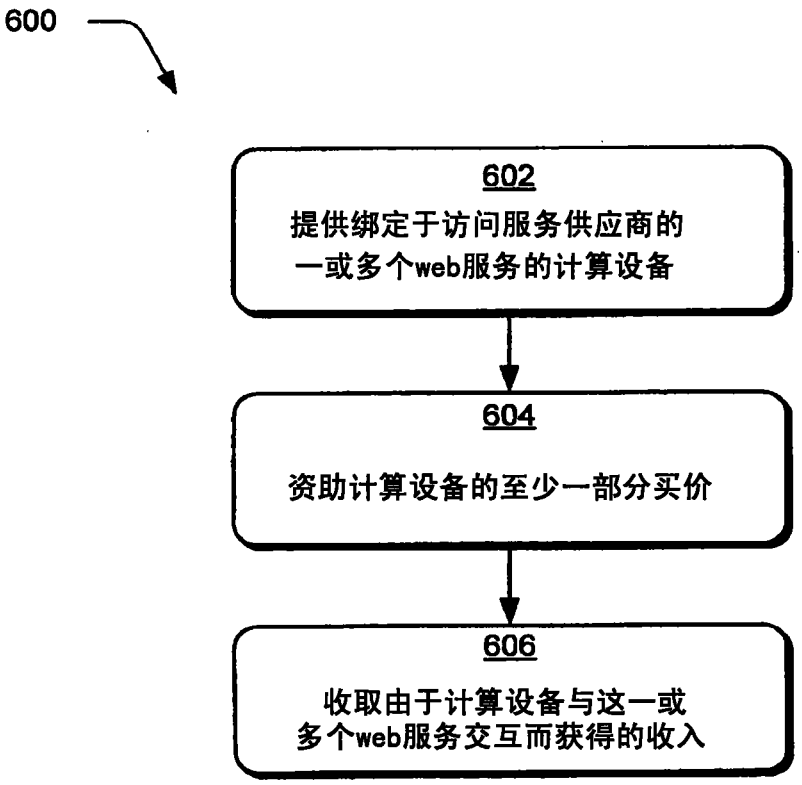

600
602
提供绑定于访问服务供应商的一或多个web服务的计算设备
604
资助计算设备的至少一部分买价
606
收取由于计算设备与这一或多个web服务交互而获得的收入

图 6

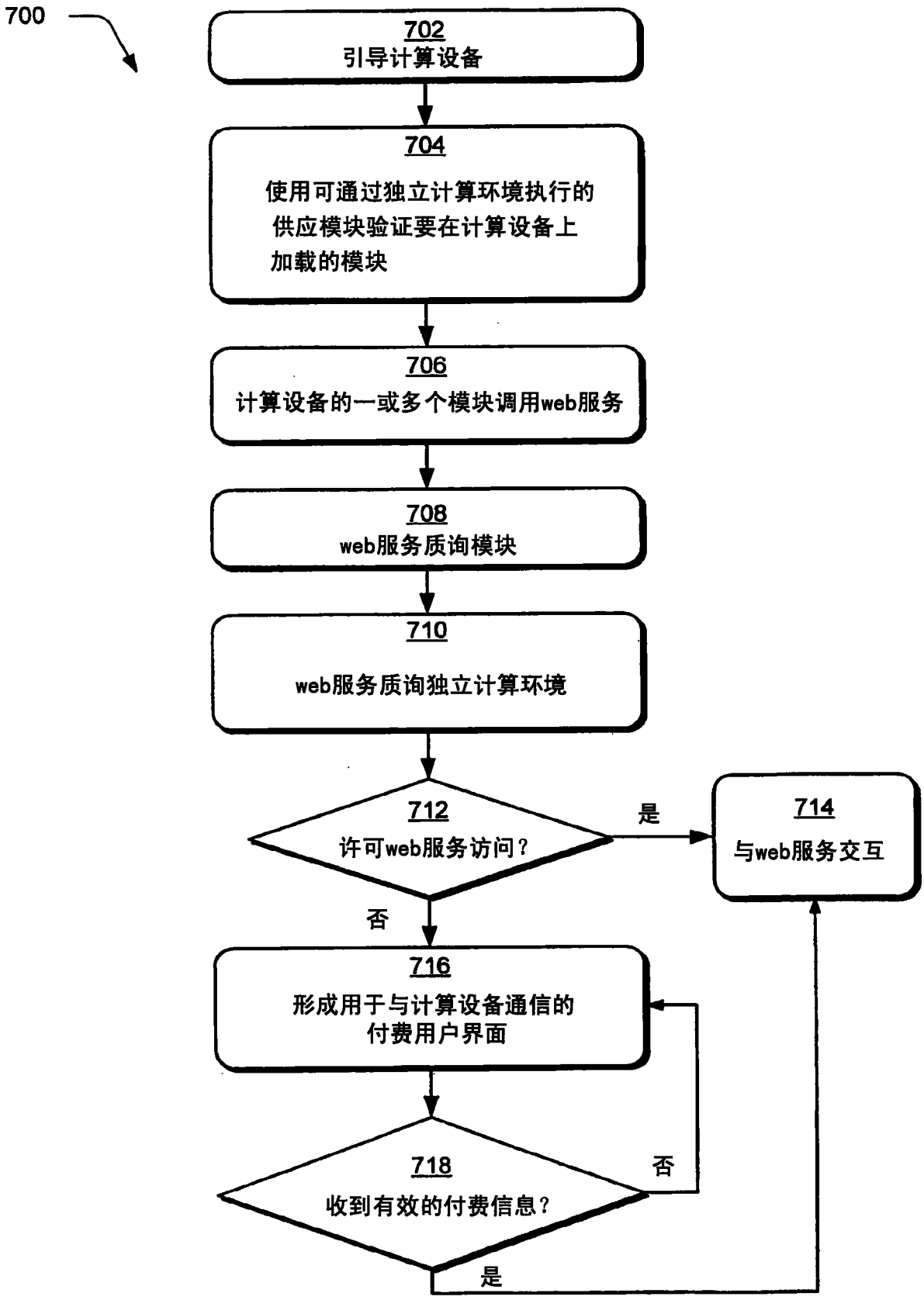

700
702
引导计算设备
704
使用可通过独立计算环境执行的供应模块验证要在计算设备上加载的模块
706
计算设备的一或多个模块调用web服务
708
web服务质询模块
710
web服务质询独立计算环境
712
许可web服务访问？
是
714
与web服务交互
否
716
形成用于与计算设备通信的付费用户界面
718
收到有效的付费信息？
否
是

图 7

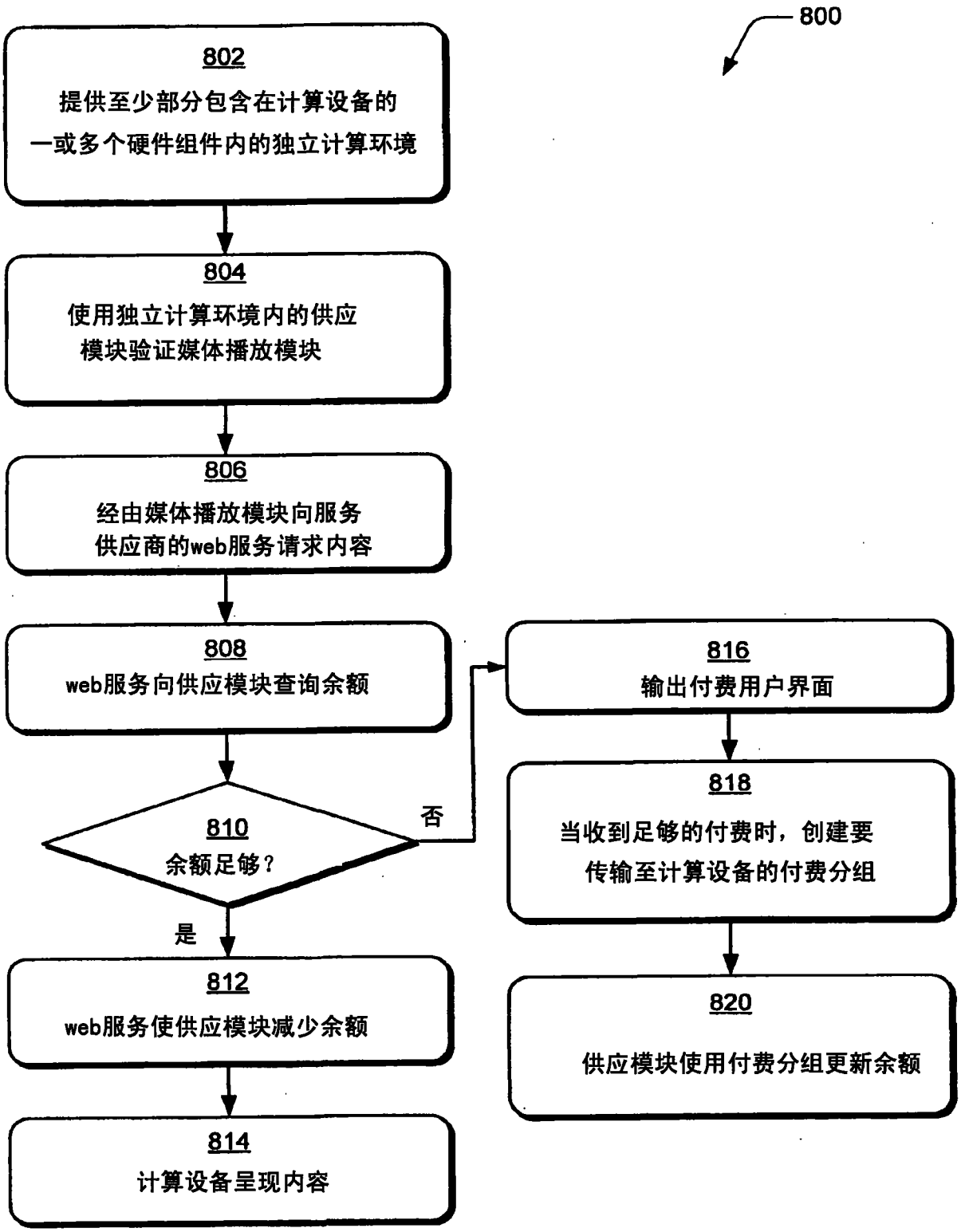

800
802
提供至少部分包含在计算设备的一或多个硬件组件内的独立计算环境
804
使用独立计算环境内的供应模块验证媒体播放模块
806
经由媒体播放模块向服务供应商的web服务请求内容
808
web服务向供应模块查询余额
810
余额足够？
否
是
812
web服务使供应模块减少余额
814
计算设备呈现内容
816
输出付费用户界面
818
当收到足够的付费时，创建要传输至计算设备的付费分组
820
供应模块使用付费分组更新余额

图 8

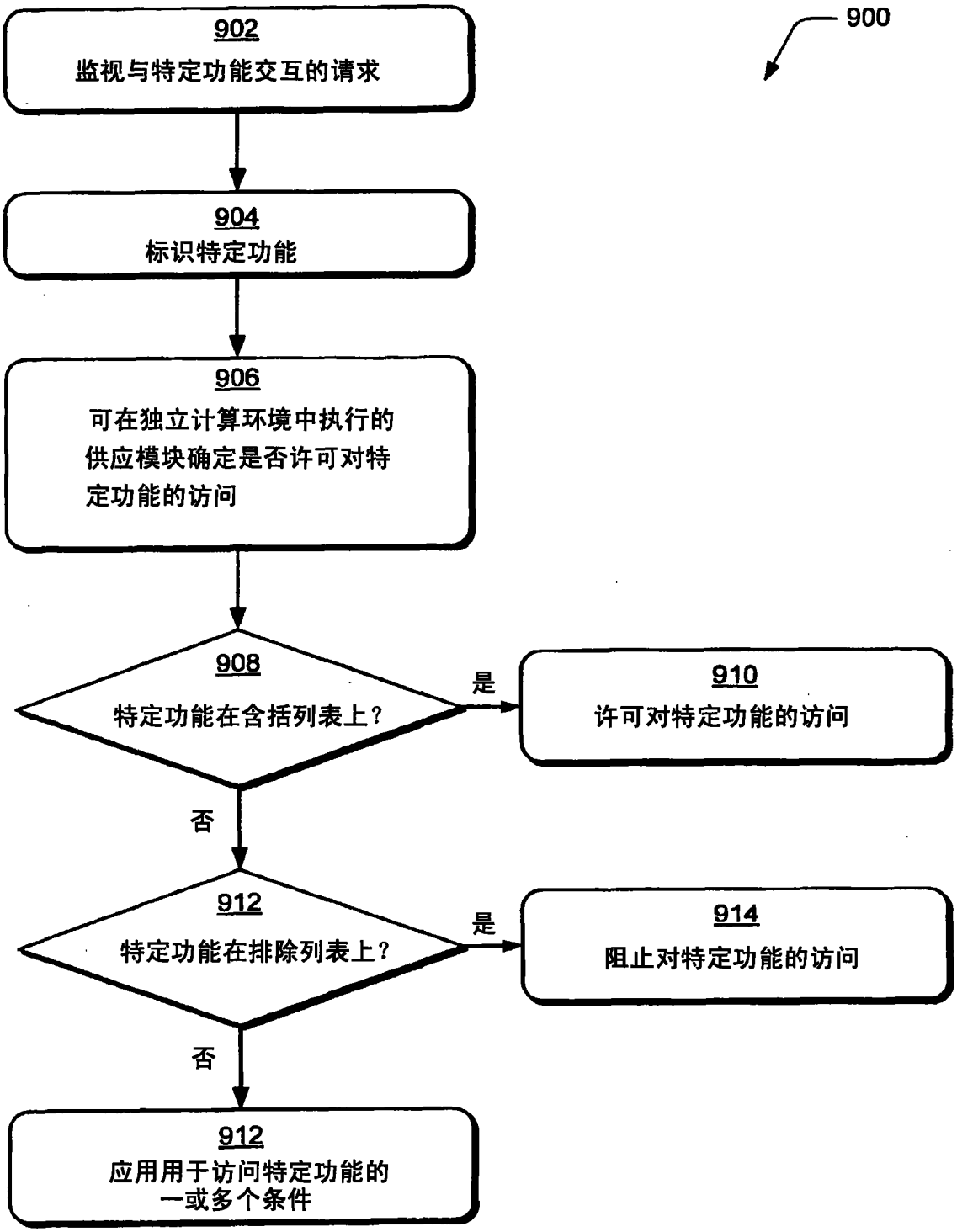

900
902
监视与特定功能交互的请求
904
标识特定功能
906
可在独立计算环境中执行的供应模块确定是否许可对特定功能的访问
908
特定功能在含括列表上？
是
910
许可对特定功能的访问
否
912
特定功能在排除列表上？
是
914
阻止对特定功能的访问
否
912
应用用于访问特定功能的一或多个条件

图 9

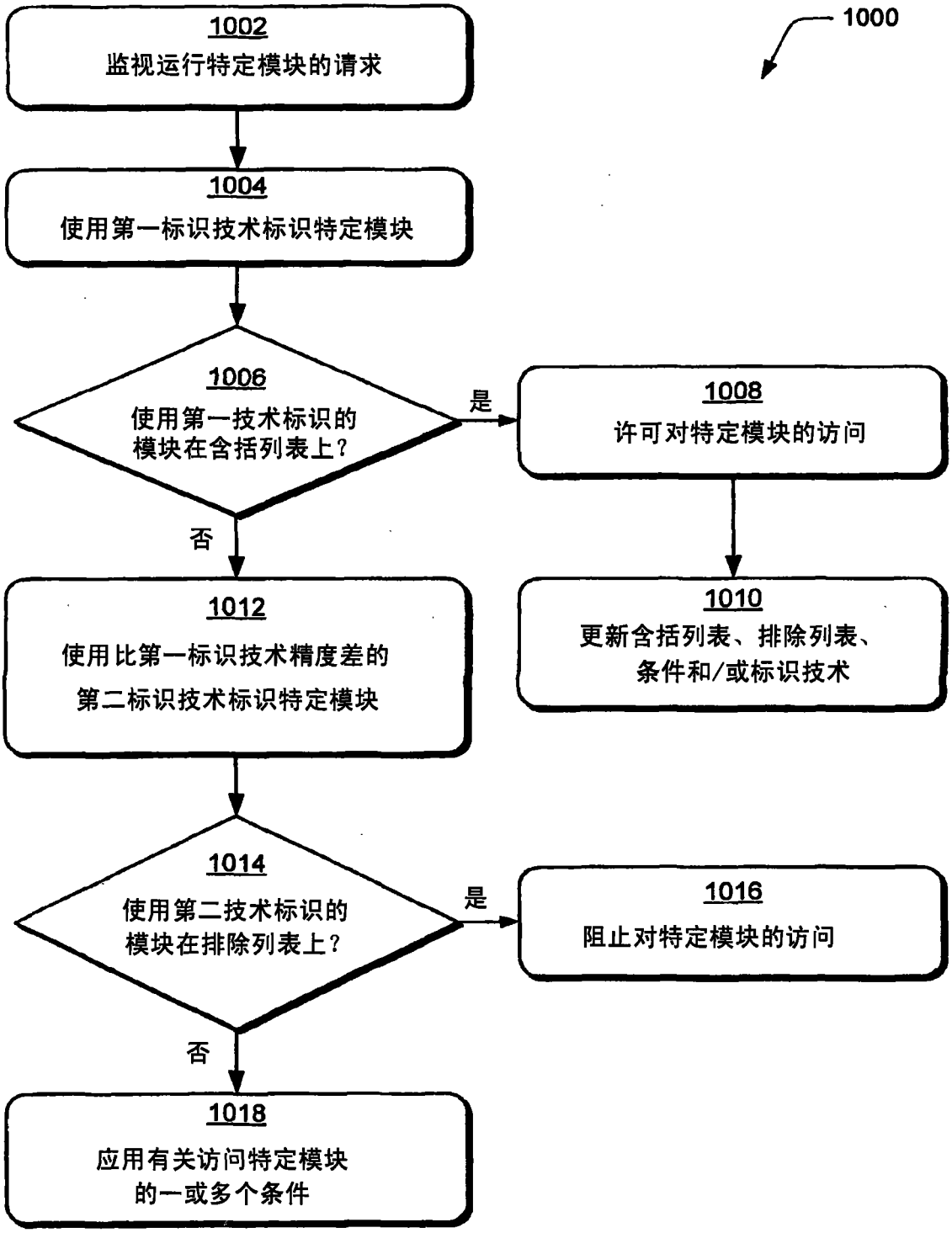

1000
1002
监视运行特定模块的请求
1004
使用第一标识技术标识特定模块
1006
使用第一技术标识的模块在含括列表上？
是
否
1008
许可对特定模块的访问
1010
更新含括列表、排除列表、条件和/或标识技术
1012
使用比第一标识技术精度差的第二标识技术标识特定模块
1014
使用第二技术标识的模块在排除列表上？
是
否
1016
阻止对特定模块的访问
1018
应用有关访问特定模块的一或多个条件

图 10