(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 103003798 B
(45)授权公告日 2017.02.22

(21)申请号 201280002021.6
(22)申请日 2012.03.30
(65)同一申请的已公布的文献号
申请公布号 CN 103003798 A
(43)申请公布日 2013.03.27
(30)优先权数据
2011-109028 2011.05.16 JP
(85)PCT国际申请进入国家阶段日
2013.01.16
(86)PCT国际申请的申请数据
PCT/JP2012/002229 2012.03.30
(87)PCT国际申请的公布数据
WO2012/157166 JA 2012.11.22

(73)专利权人 松下电器(美国)知识产权公司
地址 美国加利福尼亚州
(72)发明人 神山辉壮 天野克重 齐藤雅彦 谷川忠雄
(74)专利代理机构 中科专利商标代理有限责任公司 11021
代理人 汪惠民

(51)Int.Cl.
G06F 9/54(2006.01)
G06F 9/46(2006.01)

审查员 梁艳

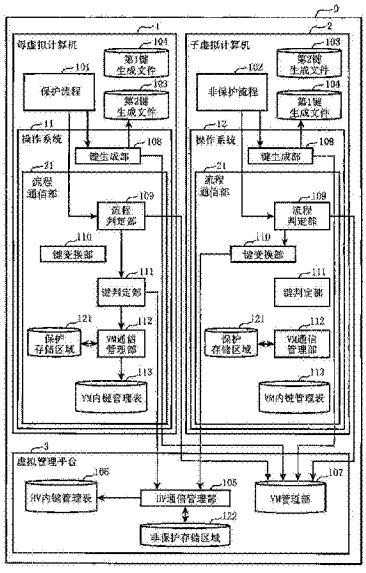
权利要求书2页 说明书17页 附图8页

(54)发明名称

虚拟计算机系统、虚拟计算机系统的控制方法

(57)摘要

当由流程判定部109判定出对象流程是保护流程101时，键判定部111基于键变换规则判定作为由键生成部108所生成的键的对象键是第1还是第2种键。当由键判定部111判定出对象键是第1种键时，VM通信管理部112将与该第1种键对应的保护存储区域121的存储ID通知给对象流程。当由流程判定部109判定出对象流程是非保护流程时，键变换部110基于键变换规则将对象键从第1种键变换为第2种键。HV通信管理部105将与第2种键对应的非保护存储区域122的存储ID通知给对象流程。



CN 103003798 B

1.一种虚拟计算机系统，具备执行保护流程的第1虚拟计算机、执行非保护流程的第2虚拟计算机以及控制所述第1、第2虚拟计算机的虚拟管理平台，其特征在于，

所述第1、第2虚拟计算机包括：

键生成部，当从与所述非保护流程通信的保护流程发出了通信请求时，生成将第1种键按指定的键变换规则变换的第2种键，当从其它的流程发出了通信请求时，生成所述第1种键；

流程判定部，判定作为发出所述通信请求的流程的对象流程是所述保护流程还是所述非保护流程；

键判定部，当由所述流程判定部判定出所述对象流程是所述保护流程时，判定作为由所述键生成部生成的键的对象键是所述第1种键还是所述第2种键；

VM通信管理部，当由所述键判定部判定出所述对象键是所述第1种键时，将与该第1种键对应的保护存储区域的存储ID通知给所述对象流程，

所述虚拟管理平台包括：

HV通信管理部，当由所述键判定部判定出所述对象键是所述第2种键时，将与该第2种键对应的非保护存储区域的存储ID通知给所述对象流程，

所述第1、第2虚拟计算机还包括：

键变换部，当由所述流程判定部判定出所述对象流程是所述非保护流程时，基于所述键变换规则，将所述对象键从所述第1种键变换为所述第2种键，其中，

所述HV通信管理部，将与由所述键变换部变换的第2种键对应的所述非保护存储区域的存储ID通知给所述对象流程。

2.根据权利要求1所述的虚拟计算机系统，其特征在于：所述键生成部，参照对各流程预先分配了键的键生成文件生成键。

3.根据权利要求2所述的虚拟计算机系统，其特征在于，所述键生成文件包括：

第1键生成文件，对各流程分配第1种键，使其值与通信对方的流程的值相同；

第2键生成文件，通过复制所述第1键生成文件，将分配给与所述非保护流程通信的保护流程的第1种键以所述键变换规则变换为第2种键而生成，其中，

所述键生成部，当从所述保护流程发出了所述通信请求时，参照所述第2键生成文件生成键，当从所述非保护流程发出了所述通信请求时，参照所述第1键生成文件生成键。

4.根据权利要求1至3中任一项所述的虚拟计算机系统，其特征在于：

所述键变换规则，是将规定值与所述第1种键相加而变换为所述第2种键的规则，

所述键判定部，在所述对象键未达到所述规定值时，判定该对象键为所述第1种键，在所述对象键为所述规定值以上时，判定该对象键为所述第2种键。

5.根据权利要求1至3中任一项所述的虚拟计算机系统，其特征在于：

所述键判定部，当判定所述对象键为所述第1种键时，将所述保护存储区域的使用请求通知给所述VM通信管理部，当判定所述对象键为所述第2种键时，将所述非保护存储区域的使用请求通知给所述HV通信管理部。

6.根据权利要求1至3中任一项所述的虚拟计算机系统，其特征在于，所述虚拟管理平台还包括：管理表示各虚拟计算机是所述第1虚拟计算机还是所述第2虚拟计算机的VM管理信息的VM管理部，其中，

所述流程判定部，基于所述VM管理信息判定执行所述对象流程的虚拟计算机相当于所述第1虚拟计算机还是所述第2虚拟计算机，当判定出相当于所述第1虚拟计算机时，判定所述对象流程为所述保护流程，当判定出相当于所述第2虚拟计算机时，判定所述对象流程为所述非保护流程。

7.根据权利要求1至3中任一项所述的虚拟计算机系统，其特征在于：

所述第1虚拟计算机为母虚拟计算机，

所述第2虚拟计算机为复制所述母虚拟计算机而生成的子虚拟计算机。

8.根据权利要求1至3中任一项所述的虚拟计算机系统，其特征在于：

所述第2虚拟计算机为母虚拟计算机，

所述第1虚拟计算机为复制所述母虚拟计算机而生成的子虚拟计算机。

9.根据权利要求1至3中任一项所述的虚拟计算机系统，其特征在于：

所述保护存储区域，在只有所述第1虚拟计算机能访问的共享存储器中生成，

所述非保护存储区域，在所述第1和第2虚拟计算机都能访问的共享存储器中生成。

10.根据权利要求1至3中任一项所述的虚拟计算机系统，其特征在于，

所述虚拟计算机系统能够通过集成电路来实现。

11.一种虚拟计算系统的控制方法，用于控制具备执行保护流程的第1虚拟计算机、执行非保护流程的第2虚拟计算机以及控制所述第1、第2虚拟计算机的虚拟管理平台的虚拟计算机系统，其特征在于包括以下步骤：

当从与所述非保护流程通信的保护流程发出了通信请求时，所述第1虚拟计算机的键生成部生成将第1种键按指定的键变换规则变换的第2种键，当从其它的流程发出了通信请求时，所述第2虚拟计算机的键生成部生成所述第1种键；

所述第1、第2虚拟计算机的流程判定部，判定作为发出所述通信请求的流程的对象流程是所述保护流程还是所述非保护流程；

当由所述流程判定部判定出所述对象流程是所述保护流程时，所述第1虚拟计算机的键判定部判定作为由所述键生成部生成的键的对象键是所述第1种键还是所述第2种键；

当由所述键判定部判定出所述对象键是所述第1种键时，所述第1虚拟计算机的VM通信管理部将与该第1种键对应的保护存储区域的存储ID通知给所述对象流程，

当由所述键判定部判定出所述对象键是所述第2种键时，所述虚拟管理平台的HV通信管理部将与该第2种键对应的非保护存储区域的存储ID通知给所述对象流程，

当由所述第2虚拟计算机的所述流程判定部判定出所述对象流程是所述非保护流程时，所述第2虚拟计算机的键变换部基于所述键变换规则将所述对象键从所述第1种键变换为所述第2种键，以及

所述HV通信管理部将与由所述键变换部变换的第2种键对应的所述非保护存储区域的存储ID通知给所述对象流程。

虚拟计算机系统、虚拟计算机系统的控制方法

技术领域

[0001] 本发明涉及一种具备多个虚拟计算机和控制虚拟计算机的虚拟管理平台的虚拟计算机系统。

背景技术

[0002] 在信息处理装置中，存在处理个人信息、金融服务的信息、著作权等的应用软件。这样的应用软件会受到来自具有恶意的其它的应用软件的访问或计算机病毒等的影响，因此必须加以保护。

[0003] 作为保护应用软件的一个手段，虚拟计算机的技术比较适用。在使用虚拟计算机的环境中，以一个物理计算机运行多个虚拟计算机。因此，让与进行一般处理的虚拟计算机不同的虚拟计算机来处理特定的需要隔离的应用软件。由此，可以在虚拟计算机层上防止需要隔离的具有恶意的应用软件对其它应用软件的影响。

[0004] 作为与本发明有关联的以往技术，例如，如下所示的专利文献1、2已为公知。专利文献1公开了让控制虚拟计算机的虚拟管理平台(hypervisor)持有共享存储器(shared memory)的键管理信息，实现虚拟计算机之间的通信的技术。

[0005] 专利文献2为了解决虚拟计算机之间的通信安全方面的问题，公开了一种技术，在虚拟管理平台内设置用于设定是否允许虚拟计算机之间进行通信的通信许可表，接收方的应用软件设定允许向该通信许可表发送的发送方的应用软件，发送方的应用软件参照该通信许可表，从而控制虚拟计算机之间的通信。

[0006] 然而，在专利文献1的技术中，只要知道了键，虚拟计算机内的流程间通信用的共享存储器就可作为虚拟计算机之间的流程间通信的共享存储器而被其它的虚拟计算机访问。因此，存在安全方面的问题。

[0007] 另外，在专利文献2的技术中，存在如果设定通信许可表的接收方的应用软件感染病毒时，则导致允许发送的发送方的应用软件也感染病毒的问题。

[0008] 以往技术文献

[0009] 专利文献

[0010] 专利文献1：日本专利公开公报特开平11-85546号。

[0011] 专利文献2：日本专利公开公报特开2010-211339号。

发明内容

[0012] 本发明的目的在于提供一种技术，在用与执行保护流程的虚拟计算机不同的其它的虚拟计算机执行非保护流程时，可以安全地进行虚拟计算机之间的通信。

[0013] 本发明的一方面所涉及的虚拟计算机系统具备执行保护流程的第1虚拟计算机、执行非保护流程的第2虚拟计算机以及控制所述第1、第2虚拟计算机的虚拟管理平台，所述第1、第2虚拟计算机包括：当从与非保护流程通信的保护流程发出了通信请求时，生成将第1种键按指定的键变换规则变换的第2种键，当从其它的流程发出了通信请求时，生成所述

第1种键的键生成部；判定作为发出所述通信请求的流程的对象流程是所述保护流程还是所述非保护流程的流程判定部；当由所述流程判定部判定出所述对象流程是所述保护流程时，判定作为由所述键生成部生成的键的对象键是所述第1种键还是所述第2种键的键判定部；当由所述键判定部判定出所述对象键是所述第1种键时，将与该第1种键对应的保护存储区域的存储ID通知给所述对象流程的VM通信管理部，所述虚拟管理平台包括：当由所述键判定部判定出所述对象键是所述第2种键时，将与该第2种键对应的非保护存储区域的存储ID通知给所述对象流程的HV通信管理部，所述第1、第2虚拟计算机还包括：当由所述流程判定部判定出所述对象流程是所述非保护流程时，基于所述键变换规则将所述对象键从所述第1种键变换为所述第2种键的键变换部，其中，所述HV通信管理部将与由所述键变换部变换的第2种键对应的所述非保护存储区域的存储ID通知给所述对象流程。

附图说明

[0014] 图1是实施例的虚拟计算机系统的功能框图。

[0015] 图2是表示本发明实施例的虚拟计算机系统的动作的流程图。

[0016] 图3(A)是本发明实施例的第1键生成文件的一个例子的示意图。(B)是本发明实施例的第2键生成文件的一个例子的示意图。

[0017] 图4是表示在本发明实施例中向VM通信管理部通知保护存储区域的使用请求时的处理的流程图。

[0018] 图5(A)是VM内键管理表的一个例子的示意图。(B)是HV内键管理表的一个例子的示意图。

[0019] 图6是表示在本发明实施例的虚拟计算机系统中，从键生成到存储ID被通知为止的处理的流程的图。

[0020] 图7是VM管理信息的一个例子的示意图。

[0021] 图8是表示本发明实施例的虚拟计算机系统硬件结构的方框图。

[0022] 图9是表示在本发明实施例中向HV通信管理部通知非保护存储区域的使用请求时的处理的流程图。

具体实施方式

[0023] (获得本发明实施例的经过)

[0024] 如背景技术所述，处理个人信息、金融服务的信息、著作权等的应用软件会受到来自具有恶意的其它的应用软件的访问或计算机病毒等的影响，因此必须加以保护。并且，在背景技术中也阐述了，为了解决该问题，让与进行一般处理的虚拟计算机不同的其它的虚拟计算机来处理特定的需要隔离的应用软件。

[0025] 其间，作为重新生成虚拟计算机的技术，提出了通过制正在运行的虚拟计算机而动态生成虚拟计算机的技术。如此，将复制虚拟计算机而动态生成的技术称为“虚拟计算机的派生(fork)”。另外，将复制源的虚拟计算机称为“母虚拟计算机”，将复制后的虚拟计算机称为“子虚拟计算机”。

[0026] 在启动需要隔离的应用软件时，执行虚拟计算机的派生而生成子虚拟计算机，在子虚拟计算上启动并处理该应用软件。由此，保护对象的应用软件得到保护，使其免受被隔

离的应用软件的恶意影响。

[0027] 相反，即使让母虚拟计算机启动危险的应用软件，让子虚拟计算机启动需要保护的应用软件，也能够保护保护对象的应用软件免受危险的应用软件的影响。并且，在子虚拟计算上应用软件的处理一结束，子虚拟计算机就消灭，被隔离的应用软件也消失。

[0028] 通过虚拟计算机的派生，当在子虚拟计算机上被隔离的应用软件的流程和在复制源的母虚拟计算机上运行的应用软件的流程进行通信时，进行虚拟计算机之间的流程间通信。

[0029] 在一般的流程间通信中使用共享存储器已为公知。在该通信中，通过由某个流程生成共享存储器，其它的流程使用该共享存储器，即，通过让流程彼此共享共享存储器，进行数据的发送和接收。在生成共享存储器时需要键，用键来识别共享存储器。相互通信的流程彼此通过出示相同的键而共享相同的共享存储器，从而可以进行通信。

[0030] 作为以往的利用共享存储器的虚拟计算机之间的通信，让控制虚拟计算机的虚拟管理平台持有共享存储器的键管理信息，来实现虚拟计算机之间的通信的技术已为公知(专利文献1)。根据专利文献1，通过让虚拟管理平台来管理以往由操作系统进行的共享存储器的键管理，实现了虚拟计算机之间的通信。

[0031] 另外，作为解决虚拟计算机之间的通信安全方面的问题的方法，在虚拟管理平台内设置用于设定是否允许虚拟计算机之间进行通信的通信许可表，接收方的应用软件设定允许向该通信许可表发送的发送方的应用软件，发送方的应用软件参照该通信许可表，从而控制虚拟计算机之间的通信的技术已为公知(专利文献2)。

[0032] 然而，在专利文献1的技术中，虚拟计算机之间的流程间通信所使用的共享存储器，与虚拟计算机内的流程间通信所使用的共享存储器没有区别。因此，只要键是一致的，虚拟计算机内的流程间通信用的共享存储器就可作为虚拟计算机之间的流程间通信的共享存储器而被其它的虚拟计算机访问。因此，在专利文献1的方法中，存在安全方面的问题，即使通过虚拟计算机的派生将危险的应用软件隔离了，但如果知道需要保护的虚拟计算机内的流程间通信所使用的共享存储器的键，则已隔离的应用软件照样可以访问该共享存储器。

[0033] 另外，在专利文献2的方法中，存在当设定通信许可表的接收方的应用软件感染病毒时，会导致许可发送的发送方的应用软件感染病毒的问题。

[0034] 而且，以往的虚拟计算机的派生只设想了让虚拟计算机内的流程彼此进行通信，并没有想到在虚拟计算机间进行通信。因此，专利文献2方法存在当应用虚拟计算机的派生，将下载应用软件与其它的虚拟计算机隔离时，下载应用软件无法与在其它的虚拟计算机上运行的应用软件进行通信的问题。

[0035] 本实施例的虚拟计算系统的目的在于提供一种技术，使在通过复制某个虚拟计算机生成其它的虚拟计算机的虚拟计算机系统中，可以安全地进行虚拟计算机之间的通信。

[0036] 以下，参照附图对本发明的实施例进行说明。

[0037] (实施例)

[0038] 图1是实施例的虚拟计算机系统0的功能框图。虚拟计算机系统0具备母虚拟计算机1、子虚拟计算机2及虚拟管理平台3。子虚拟计算机2通过复制母虚拟计算机1而生成。因此，子虚拟计算机2具备图1的各方框所示的母虚拟计算机1的全部功能。在以下的说明中，

假设母虚拟计算机1执行保护流程，子虚拟计算机2执行非保护流程。保护流程是通过执行保护应用软件而产生的流程。非保护流程是执行非保护应用软件而产生的流程。

[0039] 母虚拟计算机1具备保护流程101、操作系统11、第2键生成文件103以及第1键生成文件104。另外，在图1只记述了一个保护流程101，但根据处理也可能有多个流程动作。

[0040] 保护流程101是处理个人信息、金融信息、著作权数据、著作权管理信息等的应该保护的流程，在母虚拟计算机1内被执行。

[0041] 操作系统11在共享存储器中生成并管理保护存储区域121。在此，共享存储器是流程彼此通信时所使用的存储器。操作系统11具有键生成部108及流程通信部21。流程通信部21具有流程判定部109、键变换部110、键判定部111、VM通信管理部112、VM内键管理表113以及保护存储区域121。

[0042] 键生成部108，当从与非保护流程通信的保护流程发出了通信请求时生成按指定的键变换规则将第1种键变换的第2种键，当从其它的流程发出了通信请求时生成第1种键。在此，键生成部108参照被分配有各流程的键的键生成文件生成键。

[0043] 键生成文件中存在第1键生成文件104(参照图3(A))和第2键生成文件103(参照图3(B))。第1键生成文件104是对各流程分配了第1种键以使其值与通信对方的流程的值相同的文件。

[0044] 第2键生成文件103是通过复制第1键生成文件104，将分配给与非保护流程通信的保护流程的第1种键按照键变换规则变换为第2种键而生成的文件。第1、第2键生成文件104、103的详细内容后述。

[0045] 母虚拟计算机1的键生成部108参照第2键生成文件103生成键。另一方面，子虚拟计算机2的键生成部108参照第1键生成文件104生成键。

[0046] 流程判定部109判定作为发出通信请求的流程的对象流程是保护流程101还是非保护流程102。在此，流程判定部109根据由VM管理部107管理的VM管理信息，判定执行对象流程的虚拟计算机是母虚拟计算机1还是子虚拟计算机2，当对象流程在母虚拟计算机1上运行时，判定对象流程为保护流程101，当对象流程在子虚拟计算机2上运行时，判定对象流程为非保护流程102。

[0047] 当由流程判定部109判定对象流程为非保护流程时，键变换部110根据键变换规则将对象键从第1种键变换为第2种键。在本实施例中，键变换部110不会被母虚拟计算机1所调用。

[0048] 在由流程判定部109判定对象流程为保护流程101时，键判定部111根据键变换规则判定作为由键生成部108生成的键的对象键是第1种键还是第2种键。在此，作为键变换规则，采用将规定值与第1种键相加而变换为第2种键的规则。因此，键判定部111，当对象键小于规定值时判定为第1种键，当对象键在规定值以上时判定为第2种键。

[0049] 另外，作为键变换规则采用了将规定值与第1种键相加而变换为第2种键的规则，但并不局限于此，只要是能明确区别第1种键和第2种键的规则，采用什么样的规则都可以。例如，可以采用对第1种键赋予数值，对第2种键分配与各数值对应的符号(例如字母或字符串)的规则。具体而言，可以采用作为第1种键采用1，2，3这样的数值，将各数值变换成a，b，c这样的字母的规则。

[0050] VM通信管理部112在共享存储器中生成母虚拟计算机1内的流程间通信所使用的

保护存储区域121并加以管理。具体而言，VM通信管理部112 生成将各保护存储区域121的存储ID、键、共享存储器地址相互对应起来的VM内键管理表113(参照图5(A))，管理保护存储区域121。

[0051] 另外，当由键判定部111判定对象键为第1种键时，VM通信管理部112从VM内键管理表113确定与该第1种键相对应的保护存储区域121的存储ID，并向对象流程通知所确定的存储ID，让对象流程与其它的保护流程101进行通信。

[0052] 即，当对象流程为保护流程101、且该保护流程101是与其它保护流程101通信的流程时，VM通信管理部112使两保护流程101在母虚拟计算机1内通信。据此，保护流程101能在母虚拟计算机1内通信，从而能够防止保护流程101的信息泄漏到子虚拟计算机2或虚拟管理平台3。

[0053] VM内键管理表113由VM通信管理部112生成，是将各保护存储区域121的键、共享存储器地址以及存储ID相互对应起来的表。

[0054] 在此，如果对象键在VM内键管理表113中存在时，VM通信管理部112将与该对象键相对应的存储ID通知给对象流程。另一方面，如果对象键在VM内键管理表113中不存在时，VM通信管理部112在共享存储器中重新生成保护存储区域121，给生成的保护存储区域121赋予存储ID，将对象键、存储ID以及共享存储器地址登录在VM内键管理表113中，并向对象流程通知存储ID。

[0055] 保护存储区域121例如在母虚拟计算机1内被生成，是只有母虚拟计算机1能够访问的共享存储器。保护存储区域121在保护流程101彼此进行通信时被使用。另外，如果设定保护存储区域121只有母虚拟计算机1可以访问的限制，则保护存储区域121也可以设置在母虚拟计算机1的外部。

[0056] 子虚拟计算机2通过复制母虚拟计算机1而生成。这样的子虚拟计算机2的生成例如以非保护流程102发出非保护应用软件的启动指令为契机进行。因此，如图1所示，子虚拟计算机2除具备非保护流程102以外，其它结构与母虚拟计算机1相同。但是，在子虚拟计算机2中，不调用键判定部11、VM通信管理部112以及VM内键管理表113。

[0057] 作为非保护应用软件，例如，可以列举从互联网上下载的下载应用软件。下载应用软件中有可能含有计算机病毒或恶意软件(malware)等。于是，让子虚拟计算机2运行下载应用软件。据此，可将下载应用软件与保护流程101 隔离开来，从而能够保护保护流程101。

[0058] 子虚拟计算机2的操作系统12通过复制母虚拟计算机1的操作系统11而生成。

[0059] 虚拟管理平台3复制母虚拟计算机1生成子虚拟计算机2，控制母虚拟计算机1和子虚拟计算机2。虚拟管理平台3具备HV通信管理部105、HV内键管理表106、VM管理部107及非保护存储区域122。

[0060] HV通信管理部105在共享存储器生成非保护存储区域122并加以管理，非保护存储区域122供子虚拟计算机2内的流程间通信所使用，且供母虚拟计算机1以及子虚拟计算机2间的流程间通信所使用。具体而言，HV通信管理部105通过生成将各非保护存储区域122的存储ID、键以及共享存储器地址相互对应起来的HV内键管理表106(参照图5(B))，管理非保护存储区域122。

[0061] HV通信管理部105向对象流程通知与第2种键对应的非保护存储区域122的存储ID，使对象流程与非保护流程通信。

[0062] 即，当对象流程为保护流程101，且该保护流程101是与非保护流程102通信的流程时，HV通信管理部105使两流程利用非保护存储区域122进行通信。

[0063] 据此，保护流程101可以利用非保护存储区域122而与非保护流程102通信，可以实现虚拟计算机之间的流程通信。在保护流程101与非保护流程102之间的通信中，由于使用非保护存储区域122，因此保护存储区域121不会被非保护流程102访问，从而能够防止其它的保护流程101的信息泄漏到子虚拟计算机2。

[0064] 另外，当对象流程为非保护流程102，且该非保护流程102是与子虚拟计算机2内的其它非保护流程102或者其它的子虚拟计算机2的非保护流程102通信的流程时，HV通信管理部105使两非保护流程102利用非保护存储区域122进行通信。在非保护流程102之间的通信中，由于使用了非保护存储区域122，因此保护存储区域121不会被非保护流程102访问，从而能防止保护流程101的信息泄漏到非保护流程102。

[0065] HV内键管理表106由HV通信管理部105生成，是将键和共享存储器地址以及存储ID相互对应起来的表(参照图5(B))。

[0066] 在此，如果对象键在HV内键管理表106中存在，HV通信管理部105将与该对象键相对应的存储ID通知给对象流程。另一方面，如果对象键在HV内键管理表106中不存在，HV通信管理部105在共享存储器中重新生成非保护存储区域122，给生成的非保护存储区域122赋予存储ID，将对象键和存储ID以及共享存储器地址登录在HV内键管理表106中，并将存储ID通知给对象流程。

[0067] 非保护存储区域122例如在虚拟管理平台3内被生成，是母虚拟计算机1和子虚拟计算机2都能访问的共享存储器。而且，非保护存储区域122在非保护流程102之间进行通信时，以及保护流程101与非保护流程102进行通信时被使用。另外，非保护存储区域122也可以设置在虚拟管理平台3的外部。

[0068] VM管理部107生成用于管理各虚拟计算机是否相当于母虚拟计算机1或者子虚拟计算机2的VM管理信息并进行管理。另外，在复制母虚拟计算机1生成子虚拟计算机2时，VM管理部107将母虚拟计算机1和子虚拟计算机2的状态登录到VM管理信息中。

[0069] 图7是VM管理信息的一个例子的示意图。在VM管理信息中，对每个虚拟计算机分配一个记录，各记录具备VMID及状态的字段(field)。VMID是对各虚拟计算机分别赋予的识别信息。VMID使用能区分母虚拟计算机1和子虚拟计算机2的符号列。在图7的例子中，对母虚拟计算机1分配VM_P的符号列，对子虚拟计算机2分配VM_C1、VM_C2、.....的符号列，根据“P”和“C”可以区别是母虚拟计算机还是子虚拟计算机2。

[0070] 状态表示各虚拟计算机的状态。作为状态有“发出”和“待机”。“发出”表示虚拟计算机内的某个流程发出了通信请求的状态。待机表示虚拟计算机内的流程在等待来自其它的流程的通信的状态。

[0071] 在图7的例子中，由于VMID＝VM_P的母虚拟计算机1的保护流程101发出了通信请求，因此状态为“发出”状态。除此以外的子虚拟计算机2的非保护流程102由于没有发出通信请求，状态为“待机”状态。

[0072] 为了判定发出了通信请求的对象流程是保护流程101还是非保护流程102，键生成部108及流程判定部109参照VM管理信息。具体而言，如果对象流程发出了通信请求，键生成部108及流程判定部109参照VM管理信 息，确定状态的字段为“发出”的记录，当确定的记录

的VMID表示母虚拟计算机1时，判定该对象流程为保护流程101，当确定的记录的VMID表示子虚拟计算机2时，判定该对象流程为非保护流程102。

[0073] 图2是表示本发明实施例的虚拟计算机系统0的动作的流程图。以下，用图2说明保护流程101或者非保护流程102取得共享存储器的存储ID时的处理。

[0074] 首先，当对象流程发出通信请求键生成部108被调用时，键生成部108参照由VM管理部107管理的VM管理信息，判定对象流程是保护流程101还是非保护流程102(S2001)。

[0075] 此时，键生成部108例如确定图7所示的VM管理信息的状态的字段为“发出”的记录，如果确定的记录的VMID表示母虚拟计算机1，则判定对象流程为保护流程101，如果确定的记录的VMID表示子虚拟计算机2，则判定对象流程为非保护流程102。

[0076] 然后，键生成部108在判定对象流程为保护流程101时(在S2002为Y)，参照第2键生成文件103生成键(S2003)。另一方面，键生成部108在判定对象流程为非保护流程102时(在S2002为N)，参照第1键生成文件104生成键(S2004)。

[0077] 下面对第1、第2键生成文件104，103的详细进行说明。在本实施例中，子虚拟计算机2是通过复制母虚拟计算机1而生成的。因此，各虚拟计算机可能为母虚拟计算机1或者为子虚拟计算机2。因此，在本实施例中，不管各虚拟计算机为母虚拟计算机1还是子虚拟计算机2，在各虚拟计算机都设置了第2键生成文件103及第1键生成文件104，以使键生成部108能够生成保护流程101或者非保护流程102的键。图3(A)是本发明实施例的第1键生成文件104的一个例子的示意图。图3(B)是本发明实施例的第2键生成文件103的一个例子的示意图。

[0078] 如图3(A)所示，在第1键生成文件104中，对每个流程分配一个记录，具备储存流程名的字段3001和储存键的字段3002。另外，如图3(B)所示，第2键生成文件103具有与第1键生成文件104相同的数据结构。

[0079] 字段3001储存赋予各流程的流程名。字段3002储存用于确定各流程进行流程间通信时所使用的共享存储器的键。

[0080] 通过复制第1键生成文件104，针对与非保护流程102通信的保护流程101，按照键变换规则将键从第1种键变换为第2种键，从而生成第2键生成文件103。在此，作为键变换规则，采用将规定值与第1种键相加而将第1种键变换为第2种键的规则，作为规定值例如可采用1000。

[0081] 从图3(B)的例子可以看出，流程C以外的各流程被分配了与图3(A)的各流程相同的键，第2键生成文件103是通过复制第1键生成文件104而生成。另一方面，流程C是与非保护流程102通信的保护流程101。因此，流程C被分配了将1000加到图3(A)所示的键“21”而被变换成第2种键的键“1021”。

[0082] 另外，第1、第2键生成文件104、103由系统设计者预先制作。作为制作方法，例如，系统设计者对各流程分配第1种键以使流程采用小于1000的数值，生成第1键生成文件104。其次，系统设计者可以复制第1键生成文件104，将与非保护流程102通信的保护流程101的键加上1000，从而生成第2键生成文件103。

[0083] 返回图2，键生成部108在对象流程为保护流程101时(在S2002为Y)，根据对象流程的流程名从第2键生成文件103中确定与该流程相对应的记录，将储存在确定的记录的字段3002的键作为对象流程的键生成(S2003)。然后，键生成部108将生成的键返还给对象流程。

[0084] 另一方面，键生成部108在对象流程为非保护流程102时（在S2002为N），参照第1键生成文件104，与S2003同样生成键（S2004），并返还给对象流程。

[0085] 另外，在S2003、S2004中，键生成部108读取了第2键生成文件103、第1键生成文件104，但本实施例并不局限于此。例如，在S2003，也可以由保护流程101读取第2键生成文件103，并将其交给键生成部108。另外，在S2004，也可以由非保护流程102读取第一键生成文件104，并将其交给键生成部108。

[0086] 其次，对象流程将取得的键作为对象键，指定对象键并调用流程判定部109（S2005）。然后，流程判定部109参照VM管理部107管理的VM管理信息，判定对象流程是保护流程101还是非保护流程102（S2005）。

[0087] 此时，流程判定部109参照VM信息，确定状态的字段为“发出”的记 录，如果确定的记录的VMID表示母虚拟计算机1，则判定对象流程为保护流程101。另一方面，流程判定部109如果确定的记录的VMID表示子虚拟计算机2，则判定对象流程为非保护流程102。

[0088] 然后，当流程判定部109判定对象流程为保护流程101时（在S2006为Y），键判定部111判定对象键是第1种键还是第2种键（S2007）。

[0089] 在此，键判定部111根据上述的键变换规则判定对象键的种类。例如，在图3（B）的例子中，将1000与第1种键相加使第1种键变换成第2种键。因此，键判定部111，在对象键为1000以上时判定该对象键为第2种键，在对象键小于1000时，判定该对象键为第1种键。

[0090] 另外，键判定部111也可以利用系统设计者在键判定部111预先登录的键变换规则来判定对象键的种类。或者，键判定部111也可以读取第2键生成文件103，并解读键变换规则，利用解读的键变换规则来判定对象键的种类。作为键变换规则的解读方法，例如，在图3（B）的例子中，键判定部111可以采用确定后2位数为共同的键，如果确定的键为不同的数值，则将两个数值的差作为键变换规则的规定值来确定的手段。

[0091] 其次，键判定部111在判定对象键为第1种键时（在S2008为Y），指定对象键，并向VM通信管理部112通知保护存储区域121的使用请求（S2009）。另一方面，键判定部111在判定对象键为第2种键时（在S2008为N），指定对象键，并向HV通信管理部105通知非保护存储区域122的使用请求（S2010）。

[0092] 在S2006，当对象流程被判定为非保护流程102时（在S2006为N），键变换部110按照上述的键变换规则，将对象键从第1种键变换为第2种键（S2011）。即，键变换部110将对象键加上规定值（＝1000）而变换为第2种键。

[0093] 其次，键变换部110指定在S2011被变换为第2种键的对象键，向HV通信管理部105通知非保护存储区域122的使用请求（S2010）。

[0094] 以下是生成或共享共享存储器的处理的详细说明。在本实施例中，当对象流程为与其它的保护流程101通信的保护流程时，保护存储区域121的使用请求被通知给VM通信管理部112（S2009），当对象流程为与非保护流程102通信的保护流程101或者非保护流程102时，非保护存储区域122的使 用请求被通知给HV通信管理部105（S2010）。

[0095] 因此，首先，对向VM通信管理部112通知使用请求时的处理进行说明。图4是表示在本发明实施例中，向VM通信管理部112通知保护存储区域121的使用请求时的处理的流程图。首先，VM通信管理部112参照VM内键管理表113（S4001），判定在VM内键管理表113中对象键是否被登录（S4002）。

[0096] 图5(A)是VM内键管理表113的一个例子的示意图。如图5(A)所示，在VM内键管理表113中，对一个保护存储区域121分配一个记录，各记录具有键的字段5001、共享存储器地址字段5002、以及存储ID的字段5003。

[0097] 共享存储器地址是各保护存储区域121的开始地址。存储ID是对各保护存储区域121赋予的唯一含义的识别信息。这样，VM内键管理表113将各保护存储区域121的键、共享存储器地址、以及存储ID相互对应起来进行存储。

[0098] 因此，VM通信管理部112，当由键判定部111指定的对象键在VM内键管理表113中存在时，判定对象键被登录在VM内键管理表113(在S4002为Y)，当对象键在VM内键管理表113不存在时，判定对象键未被登录在VM内键管理表113(在S4002为N)。

[0099] 其次，VM通信管理部112使用对象键在流程通信部21内生成保护存储区域121(S4003)。接着，VM通信管理部112将生成的保护存储区域121登录在VM内键管理表113(S4004)。在这种情况下，VM通信管理部112将生成保护存储区域121时使用的对象键、生成的保护存储区域121的开始地址以及存储ID登录在VM内键管理表113中。其次，VM通信管理部112将生成的保护存储区域121的存储ID通知给保护流程101(S4005)。另一方面，当对象键已经被登录在VM内键管理表113时(在S4002为Y)，VM通信管理部112将与对象键相对应的存储ID通知给保护流程101(S4006)。

[0100] 通过以上的处理，保护存储区域121的存储ID被通知给与其它的保护流程101通信的保护流程101。

[0101] 接着，对向HV通信管理部105通知非保护存储区域122的使用请求时的处理进行说明。图9是表示在本发明实施例的虚拟计算机系统中，向VM通信管理部通知非保护存储区域122的使用请求时的处理的流程图。首先，HV通信管理部105参照HV内键管理表106(S9001)，判定对象键是否被登录在HV内键管理表106中(S9002)。

[0102] 图5(B)是HV内键管理表106的一个例子示意图。如图5(B)所示，在HV内键管理表106中，对每个非保护存储区域122分配一个记录，各记录包括键的字段5001、共享存储器地址的字段5002以及存储ID的字段5003。

[0103] 共享存储器地址是各非保护存储区域122的开始地址。存储ID是对各非保护存储区域122赋予的唯一含义的识别信息。这样，HV内键管理表106将各非保护存储区域122的键、共享存储器地址、以及存储ID相互对应起来进行存储。

[0104] 然后，当对象键未被登录在HV内键管理表106中时(在S9002为N)，HV通信管理部105使用对象键在虚拟管理平台3内生成非保护存储区域122(S9003)。

[0105] 其次，与S4004同样，HV通信管理部112将生成的非保护存储区域122登录在HV内键管理表106中(S9004)。然后，与S4005同样，HV通信管理部112将生成的非保护存储区域122的存储ID通知给发出了通信请求的保护流程101或者非保护流程102(S9005)。另一方面，当对象键未被登录在HV内键管理表106时(在S9002为Y)，HV通信管理部105将与对象键相对应的存储ID通知给发出了通信请求的保护流程101或者非保护流程102(S9006)。

[0106] 通过以上的处理，存储ID被通知给与非保护流程102通信的保护流程101以及非保护流程102。

[0107] 其次，对本发明实施例的虚拟计算系统0中的流程间通信的一个例子进行说明。图6是表示在本发明实施例的虚拟计算机系统0中，从键的生成到存储ID被通知为止的处理的

流程图。在图6中，流程A、流程B及流程C是保护流程101，流程D、流程E及流程F是非保护流程102。

[0108] 另外，图6中，作为第2键生成文件103采用了图3(B)，作为第1键生成文件104采用了图3(A)。

[0109] 另外，作为键变换规则，采用将第1种键加上1000而变换成第2种键的规则。因此，流程C的键在图3(A)的流程C的键“21”上加1000而成为 1021。

[0110] 最初，对母虚拟计算机1内的流程间通信进行说明。在此，说明根据流程A的通信请求生成保护存储区域121、流程B利用已生成的保护存储区域121与流程A通信的情况。

[0111] 首先，流程A调用键生成部108。其次，键生成部108参照第2键生成文件103将流程A的键“38”返回给流程A。在此，由于流程A是在母虚拟计算机1上运行的，键生成部108判定流程A为保护流程101。因此，键生成部108参照第2键生成文件103。

[0112] 其次，流程A指定键“38”调用流程判定部109。其次，由于流程A是在母虚拟计算机1上运行的，因此流程判定部109判定流程A为保护流程101。

[0113] 其次，由于流程A的键“38”小于1000，因此，键判定部111判定该键为第1种键。其次，由于键“38”为第1种键，键判定部111指定键“38”，将保护存储区域121的使用请求通知给VM通信管理部112。

[0114] 其次，VM通信管理部112判定键“38”是否被登录在VM内键管理表113中。在此，VM内键管理表113中键“38”还未被登录。因此，VM通信管理部112使用键“38”生成保护存储区域121。

[0115] 其次，VM通信管理部112将生成的保护存储区域121登录在VM内键管理表113，并向流程A通知该保护存储区域121的存储ID。

[0116] 其次，流程B调用键生成部108。其次，键生成部108参照第2键生成文件103，将流程B的键“38”返回给流程B。在此，由于流程B是在母虚拟计算机1上运行的，键生成部108判定流程A为保护流程101。因此，键生成部108参照第2键生成文件103。

[0117] 其次，流程B指定键“38”调用流程判定部109。其次，由于流程B是在母虚拟计算机1上运行的，因此流程判定部109判定流程B为保护流程101。

[0118] 其次，由于流程B的键“38”小于1000，键判定部111判定键“38”为第1种键。其次，由于键“38”为第1种键，键判定部111将保护存储区域121的使用请求通知给VM通信管理部112。

[0119] 其次，VM通信管理部112判定键“38”是否被登录在VM内键管理表 113中。在此，由于键“38”的保护存储区域121已被登录在VM内键管理表113中，因此将该保护存储区域121的存储ID通知给流程B。

[0120] 通过以上的处理，流程A、B可以使用键“38”所确定的保护存储区域121进行通信。

[0121] 与以上的说明相反，即使在根据流程B的通信请求生成键“38”的保护存储区域121时，也将键“38”的保护存储区域121的存储ID通知给流程A，流程A、B可以进行通信。这是因为在第2键生成文件103中流程A、B被分配了相同的键“38”，且两流程都是保护流程101，没有进行键变换。

[0122] 下面，对子虚拟计算机2内的流程间通信进行说明。在此，对根据流程E的通信请求生成非保护存储区域122，流程F利用已生成的非保护存储区域122与流程E进行通信的情况

进行说明。

[0123] 首先，流程E调用键生成部108。其次，键生成部108参照第1键生成文件104将流程E的键“57”返还给流程E。在此，由于流程E是在子虚拟计算机2上运行的，键生成部108判定流程E为非保护流程102。因此，键生成部108参照第1键生成文件104。

[0124] 其次，流程E指定键“57”调用流程判定部109。其次，由于流程E是在子虚拟计算机2上运行的，流程判定部109判定流程E为非保护流程102。

[0125] 其次，由于流程E为非保护流程102，流程判定部109指定键“57”调用键变换部110。

[0126] 其次，键变换部110在键“57”上加1000，将该键从第1种键变换为第2种键，并指定变换后的键“1057”，将非保护存储区域122的使用请求通知给HV通信管理部105。

[0127] 其次，HV通信管理部105判定键“1057”是否被登录在HV内键管理表106中。在此，HV内键管理表106中键“1057”还未被登录。因此，HV通信管理部105使用键“1057”生成非保护存储区域B。

[0128] 其次，HV通信管理部105将生成的非保护存储区域B登录在HV内键管理表106中，并将该非保护存储区域B的存储ID通知给流程E。

[0129] 其次，流程F调用键生成部108。其次，键生成部108参照第1键生成文件104将流程F的键“57”返还给流程F。在此，由于流程F是在子虚拟计算机2上运行的，键生成部108判定流程F为非保护流程102。因此，键 生成部108参照第1键生成文件104。

[0130] 其次，流程F指定键“57”调用流程判定部109，其次，流程F指定键“57”调用流程判定部109。其次，由于流程F是在子虚拟计算机2上运行的，流程判定部109判定流程F为非保护流程102。

[0131] 其次，由于流程F为非保护流程102，流程判定部109指定键“57”调用键变换部110。

[0132] 其次，键变换部110在键“57”上加1000，将该键从第1种键变换为第2种键，并指定变换后的键“1057”，将非保护存储区域122的使用请求通知给HV通信管理部105。

[0133] 其次，HV通信管理部105判定键“1057”是否被登录在HV内键管理表106中。在此，由于键“1057”的非保护存储区域B已被登录在HV内键管理表106中，因此将该非保护存储区域B的存储ID通知给流程F。

[0134] 通过以上的处理，流程E、F可以使用键“1057”所确定的非保护存储区域B进行通信。

[0135] 与以上的说明相反，即使在根据流程F的通信请求生成键“1057”的非保护存储区域B时，也将键“1057”的非保护存储区域B的存储ID通知给流程E，流程E、F可以进行通信。这是因为在第1键生成文件104中流程E、F被分配了相同的键“57”，且由于两流程都是非保护流程102，所以按相同的键变换规则都被变换成键“1057”。

[0136] 这样，当从非保护流程102发出通信请求时，键必定通过键变换部110从第1种键变换成第2种键。因此，保护存储区域121不会被非保护流程102访问，从而防止保护流程101被非保护流程102改变或参照。

[0137] 最后，对虚拟计算机之间的流程间通信进行说明。在此，根据流程D的通信请求生成非保护存储区域A，流程C利用生成的非保护存储区域A与流程D进行通信的情况进行说明。

[0138] 首先，流程D调用键生成部108。其次，键生成部108参照第1键生成文件104将流程D

的键“21”返还给流程D。在此，由于流程D是在子虚拟计算机2上运行的，键生成部108判定流程D为非保护流程102。因此，键生成部108参照第1键生成文件104。

[0139] 其次，流程D指定键“21”调用流程判定部109。其次，由于流程是在 虚拟计算机2上运行的，流程判定部109判定流程D为非保护流程102。

[0140] 其次，由于流程D为非保护流程102，流程判定部109指定键“21”调用键变换部110。

[0141] 其次，键变换部110在键“21”上加1000，将该键从第1种键变换为第2种键，并指定变换后的键“1021”，将非保护存储区域122的使用请求通知给HV通信管理部105。

[0142] 其次，HV通信管理部105判定键“1021”是否被登录在HV内键管理表106。在此，HV内键管理表106中键“1021”还未被登录。因此，HV通信管理部105使用键“1021”生成非保护存储区域A。

[0143] 其次，HV通信管理部105将生成的非保护存储区域A登录在HV内键管理表106中，并将非保护存储区域A的存储ID通知给流程D。

[0144] 其次，流程C调用键生成部108。其次，键生成部108参照第2键生成文件103将流程C的键“1021”返还给流程C。该键“1021”是按照键变换规则，预先将第1种键“21”加上1000而变换为第2种键的键。由于流程C是在母虚拟计算机1上运行的，键生成部108判定流程C为保护流程101。因此，键生成部108参照第2键生成文件103。

[0145] 其次，流程C指定键“1021”调用流程判定部109。其次，由于流程C是在母虚拟计算机1上运行的，流程判定部109判定流程C为保护流程101。

[0146] 其次，由于流程C的键“1021”不足1000，键判定部111判定为第2种键。其次，由于键“1021”为第2种键，键判定部111指定“1021”键，将非保护存储区域122的使用请求通知给HV通信管理部105。

[0147] 其次，HV通信管理部105判定键“1021”是否被登录在HV内键管理表106。在此，键“1021”已被登录在HV内键管理表106中。因此，HV通信管理部105将与键“1021”相对应的非保护存储区域A的存储ID返还给流程C。

[0148] 通过以上的处理，流程C、D可以使用键“1021”所确定的非保护存储区域A进行通信。

[0149] 与以上的说明相反，即使在根据流程C的通信请求生成键“1021”的非保护存储区域A时，也将键“1021”的非保护存储区域A的存储ID通知给流程D，流程C、D可以进行通信。

[0150] 这是因为，登录在第2键生成文件103中的流程C的键是“1021”，如果按键变换规则将流程D的键“21”变换成“1021”，则两键相一致。

[0151] 即，流程C、D进行通信时，两流程的键最终变成相同的值，相同的存储ID被通知给两流程，两流程可共享相同的非保护存储区域A进行通信。

[0152] 另外，由于流程C、D利用非保护存储区域A进行通信，因此流程D不会访问保护存储区域121，从而能防止母虚拟计算机1内的其它的流程(流程A、B)的处理信息泄漏到母虚拟计算机1的外部。

[0153] 另外，由于流程D是非保护流程102，所以必定会被变换成第2种键。因此，如果在第2键生成文件103中流程C的键没有被预先变换成第2种键，则流程D不能与流程C通信。因此，第2键生成文件103中流程C的键的变换是在系统设计者的管理下被预先进行的。

[0154] 因此，没有系统设计者的许可，流程D不能与流程C通信，从而防止作为保护流程的

流程C未经许可被作为非保护流程的流程D通信。其结果，可以防止流程C的处理信息被泄漏到系统设计者管理外的流程。

[0155] 并且，系统设计者只要在第1键生成文件104中，将与非保护流程102通信的保护流程101的键变换成第2种键而生成第2键生成文件103，就可以让保护流程101与非保护流程102通信。因此，系统设计者不改变保护应用软件或非保护应用软件，也可以实现虚拟计算机之间的流程通信。

[0156] 另外，HV通信管理部105通过将第2种键和存储ID相互对应起来管理非保护存储区域122。当从非保护流程102发出通信请求时，HV通信管理部105被通知由键变换部110变换的第2种键。另外，当与非保护流程102通信的保护流程101发出通信请求时，HV通信管理部105也被通知第2种键。

[0157] 因此，与非保护流程102通信的保护流程101及非保护流程102必然被通知非保护存储区域122的存储ID。因此，非保护流程102不能访问保护存储区域121，从而能够保护保护流程101。

[0158] 另外，VM通信管理部112通过将第1种键和存储ID相对应起来管理保护存储区域121。当与其它保护流程101通信的保护流程101发出通信请求时，VM通信管理部105被通知第1种键。

[0159] 为此，与其它的保护流程101通信的保护流程101必然被通知保护存储区域121的存储ID。因此，保护流程彼此互相通信的保护流程101只使用保 护存储区域121，可以防止保护流程101的信息泄漏到非保护流程102。

[0160] 另外，在本实施例中，让保护流程101在母虚拟计算机1中运行，让非保护流程102在子虚拟计算机2中运行，但也可以在母虚拟计算机1中运行非保护流程102，在子虚拟计算机2中运行保护流程101。

[0161] 此时，可以让子虚拟计算机2执行如图1所示的母虚拟计算机1的功能，并让母虚拟计算机1执行如图1所示的子虚拟计算机2的功能。

[0162] 另外，在本实施例中，在母虚拟计算机1生成保护存储区域121，在虚拟管理平台3生成非保护存储区域122，但也可以在虚拟管理平台3生成保护存储区域121以及非保护存储区域122。此时，如果保护存储区域121只有母虚拟计算机1可以访问，则能够保护保护流程101免受非保护流程102的影响。

[0163] 最后，对本实施例中虚拟计算系统0的硬件结构进行说明。图8是表示本发明实施例的虚拟计算系统0的硬件结构的方框图。

[0164] 虚拟计算机系统0例如由计算机构成，具备输入装置801、ROM(只读存储器)802、CPU(中央演算处理器)803、RAM(随机访问存储器)804、外部存储装置805、显示装置806、记录介质驱动装置807以及通信装置808。各方框与内部的总线连接，各种各样的数据等通过该总线而被输入输出，在CPU803的控制下，执行各种各样的处理。

[0165] 输入装置801由键盘、鼠标等构成，用于让用户输入各种各样的数据。ROM802中存储有BIOS(Basic Input/Output System、基本输入输出系统)等系统程序。外部存储装置805由硬盘驱动器等构成，存储操作系统或虚拟计算机程序等。CPU803从外部存储装置805读取操作系统或虚拟计算机程序等，控制各方框的动作。RAM804作为CPU803的工作区域等而被使用。

[0166] 显示装置806由例如液晶显示器或有机EL显示器构成，在CPU803的控制下，显示各种各样的图像。记录介质驱动装置807由CD-ROM驱动器，软盘驱动器等构成。

[0167] 另外，虚拟计算机程序被存储在CD-ROM等计算机可能读取的记录介质809中而提供给用户。用户通过让记录介质驱动装置807读该记录介质809，将虚拟计算机程序安装到计算机。另外，通过将虚拟计算机程序存储于网络 上的服务器，并从该服务器下载，也可以将虚拟计算机程序安装到计算机上。

[0168] 通信装置808例如由将计算机与互联网连接的通信装置构成，在CPU803的控制下，通过互联网在与其它的设备之间收发数据。

[0169] 另外，如图1所示的第1、第2键生成文件104、103、VM内键管理表113、HV内键管理表106、VM管理部107、保护存储区域121以及非保护存储区域122，例如由ROM802、RAM804、以及外部存储装置805等存储装置和控制存储装置的虚拟计算机程序所包含的程序模块构成。另外，如图1所示的保护流程101、键生成部108、流程判定部109、键变换部110、键判定部111、VM通信管理部112以及HV通信管理部105是虚拟计算机程序所包含的程序模块，由CPU803执行。

[0170] 如图1所示的虚拟计算系统0的各功能块，典型地作为处理器与外部存储器的协同处理的程序来实现的，但也可以通过集成电路的LSI来实现。这些功能块可以分别被单芯片化，也可以包括一部分或全部地被单芯片化。在此，虽然称为LSI，但根据集成度的不同，也可以称作IC，系统LSI，超级LSI(super LSI)或者超大级LSI(ultra LSI)。

[0171] 在用集成电路构成虚拟计算机系统0时，例如，可以将键生成部108、流程判定部109、键变换部110、键判定部111、VM通信管理部112、HV通信管理部105集成化。

[0172] 另外，集成电路化的手段不限于LSI，也可以通过专用电路或通用处理器来实现。也可以利用LSI制造后可编程的FPGA(Field Programmable Gate Array)或可再配置LSI内部的电路单元的连接或设定的可重构处理器(Reconfigurable Processor)。

[0173] 此外，如果出现了用由于半导体技术的进步或衍生的其他技术来代替LSI的集成电路化的技术，当然，也可以用该技术进行功能块的集成化。

[0174] 另外，虚拟计算系统0如果是具备处理器和时钟的计算处理装置，则可以应用于所有的计算机、电子设备、信息设备、AV设备、通信设备及家电设备，也可以应用于例如PC(个人电脑)、便携式信息终端(手机、智能手机和PDA等)、电视、硬盘录放机、使用DVD以及蓝光光盘等的各种光盘录放机、使用DVD和蓝光光盘等的各种光盘播放机、以及汽车导航系统等。

[0175] 另外，上述的说明总地来说只不过是本发明的示例而已，不是要限定其范 围的说明。不用说当然可以进行不脱离本发明范围的各种各样的改良和变形。

[0176] (本发明的实施例总结)

[0177] 本发明的实施例的虚拟计算机系统的技术特征可以归纳如下。

[0178] (1)本实施例的虚拟计算机系统具备执行保护流程的第1虚拟计算机、执行非保护流程的第2虚拟计算机以及控制所述第1、第2虚拟计算机的虚拟管理平台，所述第1、第2虚拟计算机包括：当从与非保护流程通信的保护流程发出了通信请求时，生成将第1种键按指定的键变换规则变换的第2种键，当从其它的流程发出了通信请求时，生成所述第1种键的键生成部；判定作为发出所述通信请求的流程的对象流程是所述保护流程还是所述非保护

流程的流程判定部；当由所述流程判定部判定出所述对象流程是所述保护流程时，判定作为由所述键生成部生成的键的对象键是所述第1种键还是所述第2种键的键判定部；当由所述键判定部判定出所述对象键是所述第1种键时，将与该第1种键对应的保护存储区域的存储ID通知给所述对象流程的VM通信管理部，所述虚拟管理平台包括：当由所述键判定部判定出所述对象键是所述第2种键时，将与该第2种键对应的非保护存储区域的存储ID通知给所述对象流程的HV通信管理部，所述第1、第2虚拟计算机还包括：当由所述流程判定部判定出所述对象流程是所述非保护流程时，基于所述键变换规则，将所述对象键从所述第1种键变换为所述第2种键的键变换部，其中，所述HV通信管理部，将与由所述键变换部变换的第2种键对应的所述非保护存储区域的存储ID通知给所述对象流程。

[0179] 根据此结构，当从与非保护流程通信的保护流程发出了通信请求时，由键生成部生成第2种键，当从其它的流程(保护流程之间通信的保护流程以及非保护流程)发出了通信请求时，由键生成部生成第1种键。在此，第2种键为将第1种键按指定的键变换规则变换而得到的键。

[0180] 而且，当由流程判定部判定出作为发出通信请求的流程的对象流程是保护流程时，键判定部判定作为由键生成部生成的键的对象键是第1种键还是第2种键。

[0181] 而且，当由键判定部判定出对象键是第1种键时，对象流程被判定为与其它保护流程通信的保护流程，即在第1虚拟计算机内通信的保护流程，将与第1种键对应的保护存储区域的存储ID通知给该保护流程。

[0182] 由此，在第1虚拟计算机内通信的保护流程可以访问保护存储区域并与其它的保护流程通信。

[0183] 另一方面，当由键判定部判定出对象键是第2种键时，对象流程被判定为与非保护流程通信的保护流程，即在虚拟计算机之间通信的保护流程，将与非保护存储区域对应的存储ID通知给该保护流程。

[0184] 由此，与非保护流程通信的保护流程可以访问非保护存储区域并与非保护流程通信。

[0185] 如此，在本结构中，分成保护存储区域和非保护存储区域，在非保护存储区域进行保护流程和非保护流程的通信，在保护存储区域进行保护流程之间的通信。为此，在保护保护流程免受非保护流程的影响的同时，能够实现虚拟计算机之间的通信。

[0186] 另外，当由流程判定部判定出对象流程是非保护流程时，通过键变换部将对象键从第1种键变换为第2种键。为此，非保护存储区域的存储ID被通知给非保护流程。因此，非保护流程只使用非保护存储区域进行通信，从而能够保护保护流程免受非保护流程的影响。

[0187] (2)上述的虚拟计算机系统中，例如，所述键生成部参照对各流程预先分配了键的键生成文件生成键。

[0188] 根据此结构，由于参照对各流程预先分配了键的键生成文件生成键，因此能够高速地生成键。而且，系统设计者通过设定键生成文件，能够让某流程与目的流程通信。因此，系统设计者不必变更应用软件也能管理流程。

[0189] (3)上述的虚拟计算机系统中，例如，所述键生成文件包括：对各流程分配第1种键以使其值与通信对方的流程的值相同的第1键生成文件；通过复制所述第1键生成文件，将

分配给与所述非保护流程通信的保护流程的第1种键按所述键变换规则变换为第2种键而生成的第2键生成文件；其中，所述键生成部，当从所述保护流程发出了所述通信请求时参照所述第2键生成文件生成键，当从所述非保护流程发出了所述通信请求时参照所述第1键生成文件生成键。

[0190] 根据此结构，由于在从保护流程发出了通信请求时，参照第2键生成文件生成键。在此，在第2键生成文件中，与非保护流程通信的保护流程被分配有第2种键，其它的保护流程(保护流程之间通信的保护流程以及非保护流 程)被分配有第1种键。为此，键生成部针对与非保护流程通信的保护流程生成第2种键。

[0191] 另一方面，针对与该保护流程通信的非保护流程，参照第1键生成文件生成第1种键。在此，生成的第1种键与针对通信对方的保护流程生成的第2种键的变换前的第1种键相同。

[0192] 然后，由于针对该非保护流程生成的第1种键通过键变换部按照键变换规则而被变换为第2种键，变换后的第2种键与针对通信对方的保护流程生成的第2种键相同。

[0193] 因此，非保护流程和成为通信对方的保护流程最终具备相同的第2种键，非保护存储区域的相同的存储ID被通知给该两流程。据此，两流程能够利用非保护存储区域进行通信。

[0194] 另一方面，键生成部针对与保护流程通信的保护流程，参照第2键生成文件生成第1种键。在此，在第2键生成文件中，成为通信对方的保护流程被分配有相同的第1种键。因此，保护存储区域的相同的存储ID被通知给该两保护流程。据此，两保护流程能够利用保护存储区域进行通信。

[0195] 进一步，当从非保护流程彼此之间通信的非保护流程发出了通信请求时，键生成部参照第1键生成文件针对两非保护流程生成相同的第1种键。而且，由于该第1种键由键变换部变换成第2种键，因此，两非保护流程的键最终成为相同的第2种键。因此，非保护存储区域的相同的存储ID被通知给该两非保护流程，两非保护流程能够利用非保护存储区域进行通信。

[0196] (4)上述的虚拟计算机系统中，例如，所述键变换规则是将规定值与所述第1种键相加而变换为所述第2种键的规则；所述键判定部，在所述对象键未达到所述规定值时判定其为所述第1种键，在所述对象键为所述规定值以上时判定其为所述第2种键。

[0197] 根据此结构，利用将规定值与第1种键相加而变换为第2种键的简单的规则，就能够区别第1种键和第2种键。

[0198] (5)上述的虚拟计算机系统中，例如，所述键判定部，当判定所述对象键为所述第1种键时，将所述保护存储区域的使用请求通知给所述VM通信管理部，当判定所述对象键为所述第2种键时，将所述非保护存储区域的使用请求通知给所述HV通信管理部。

[0199] 根据此结构，当由键判定部判定对象键为第1种键时，假定从与其他的保护流程通信的保护流程发出了通信请求，则将保护存储区域的使用请求通知给VM通信管理部。因此，保护存储区域的存储ID被通知给在第1虚拟计算机内通信的保护流程。

[0200] 另一方面，当由键判定部判定对象键为第2种键时，假定从与非保护流程通信的流程发出了通信请求，则将保护存储区域的使用请求通知给HV通信管理部。因此，非保护存储区域的存储ID被通知给与非保护流程通信的保护流程。

[0201] (6)上述的虚拟计算机系统中，例如，所述虚拟管理平台还包括，管理表示各虚拟计算机是所述第1虚拟计算机还是所述第2虚拟计算机的VM管理信息的VM管理部，所述流程判定部，基于所述VM管理信息判定执行所述对象流程的虚拟计算机是所述第1虚拟计算机还是所述第2虚拟计算机，当判定出相当于所述第1虚拟计算机时，判定所述对象流程为所述保护流程，当判定出相当于所述第2虚拟计算机时，判定所述对象流程为所述非保护流程。

[0202] VM管理信息表示各虚拟计算机是第1虚拟计算机还是第2虚拟计算机。另外，第1虚拟计算机执行保护流程，第2虚拟计算机执行非保护流程。因此，通过利用VM管理信息能够正确地判定对象流程是保护流程还是非保护流程。

[0203] (7)上述的虚拟计算机系统中，例如，所述第1虚拟计算机为母虚拟计算机，所述第2虚拟计算机为复制所述母虚拟计算机而生成的子虚拟计算机。

[0204] 根据此结构，若将第1虚拟计算机作为母虚拟计算机，将第2虚拟计算机作为复制母虚拟计算机而生成的子虚拟计算机，则在保护保护流程免受非保护流程的影响的同时，能够实现保护流程与非保护流程之间的通信。

[0205] (8)上述的虚拟计算机系统中，例如，所述第2虚拟计算机为母虚拟计算机，所述第1虚拟计算机为复制所述母虚拟计算机而生成的子虚拟计算机。

[0206] 根据此结构，若将第2虚拟计算机作为母虚拟计算机，将第1虚拟计算机作为子计算机，则在保护保护流程免受非保护流程的影响的同时，能够实现保护流程与非保护流程之间的通信。

[0207] (9)上述的虚拟计算机系统中，例如，所述保护存储区域在只有所述第 1虚拟计算机能访问的共享存储器中生成，所述非保护存储区域在所述第1和第2虚拟计算机能访问的共享存储器中生成。

[0208] 根据此结构，由于保护存储区域只能被第1虚拟计算机访问，因此能够防止保护存储区域的信息泄漏到第2虚拟计算机，从而保护保护流程。

[0209] 产业上的利用可能性

[0210] 本发明所涉及的虚拟计算机系统，只要是用于信息处理装置的设备在广泛的技术领域都有效。例如，不仅可应用于大型计算机或个人计算机等计算机，也可以应用在数字电视、存储再生装置等各种家电产品、手机等通信设备、工业设备、控制设备以及车载设备等。

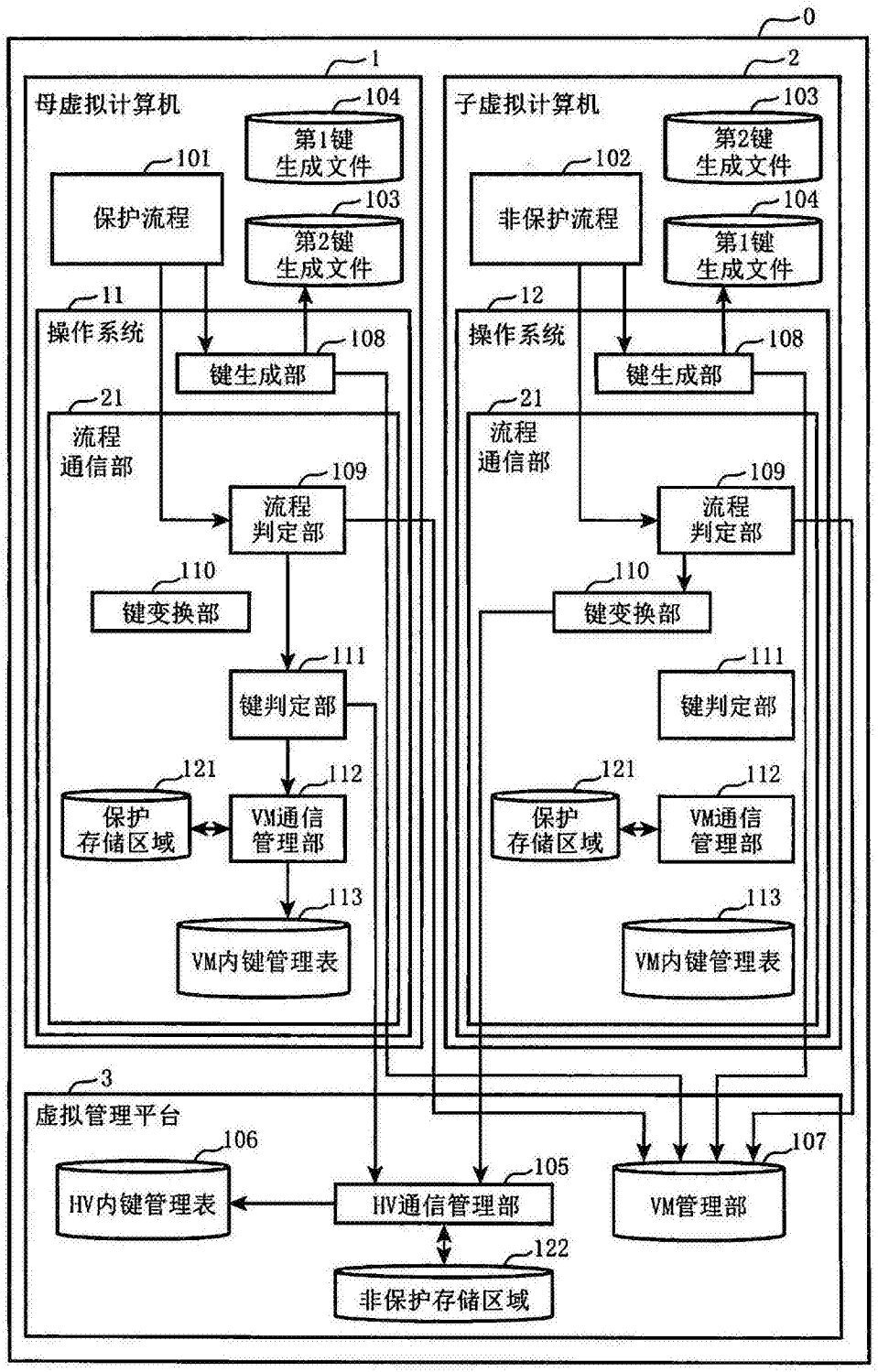

0
1
母虚拟计算机
104
第1键
生成文件
101
保护流程
103
第2键
生成文件
11
操作系统
108
键生成部
21
流程
通信部
109
流程
判定部
110
键变换部
111
键判定部
121
保护
存储区域
112
VM通信
管理部
113
VM内键管理表
2
子虚拟计算机
103
第2键
生成文件
102
非保护流程
104
第1键
生成文件
12
操作系统
108
键生成部
21
流程
通信部
109
流程
判定部
110
键变换部
111
键判定部
121
保护
存储区域
112
VM通信
管理部
113
VM内键管理表
3
虚拟管理平台
106
HV内键管理表
105
HV通信管理部
107
VM管理部
122
非保护存储区域

图1

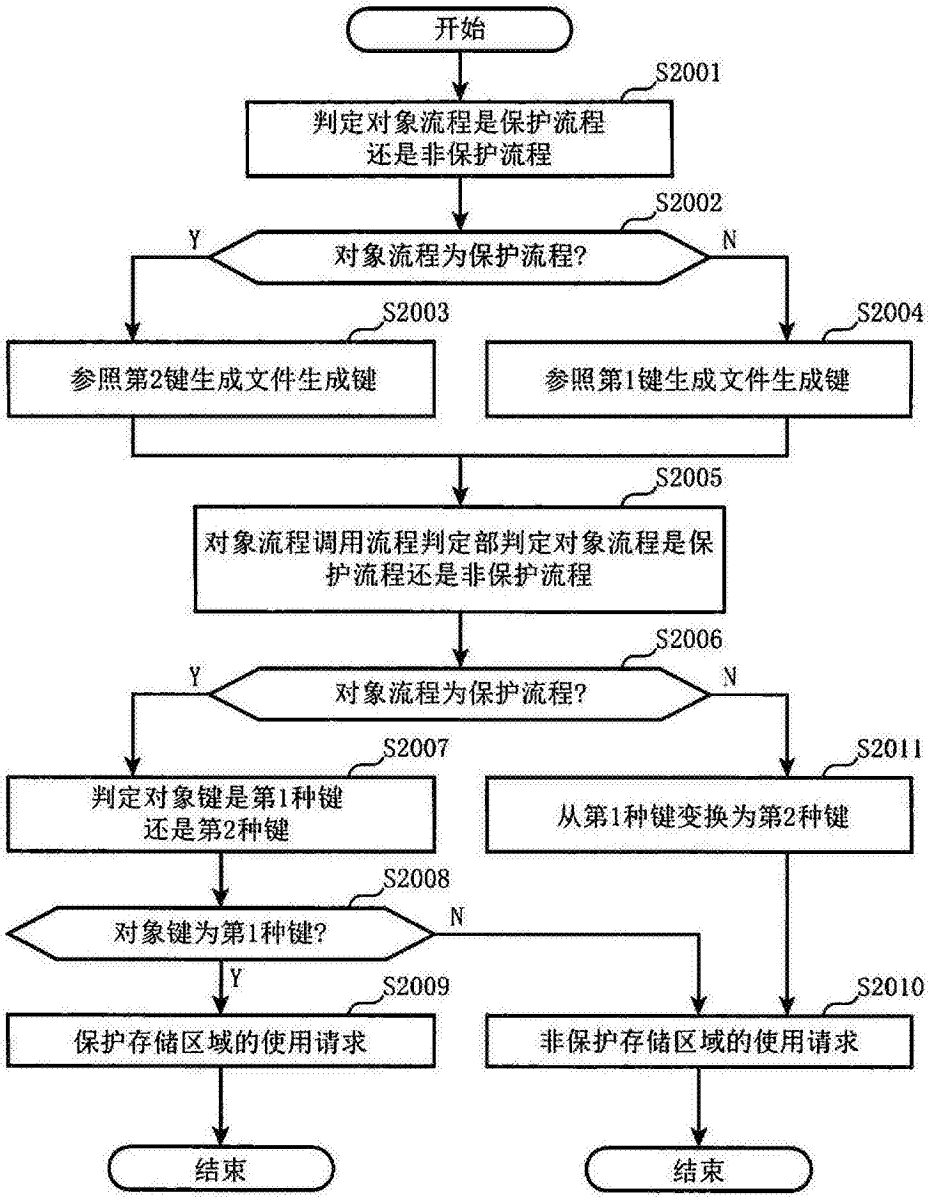

开始
S2001
判定对象流程是保护流程
还是非保护流程
S2002
Y
对象流程为保护流程?
N
S2003
参照第2键生成文件生成键
S2004
参照第1键生成文件生成键
S2005
对象流程调用流程判定部判定对象流程是保
护流程还是非保护流程
S2006
Y
对象流程为保护流程?
N
S2007
判定对象键是第1种键
还是第2种键
S2011
从第1种键变换为第2种键
S2008
对象键为第1种键?
N
Y
S2009
保护存储区域的使用请求
S2010
非保护存储区域的使用请求
结束
结束

图2

104

3001 流程名	3002 键
流程A	3 8
流程B	3 8
流程C	2 1
流程D	2 1
流程E	5 7
流程F	5 7

(A)

103

3001 流程名	3002 键
流程A	3 8
流程B	3 8
流程C	1 0 2 1
流程D	2 1
流程E	5 7
流程F	5 7

(B)

图3

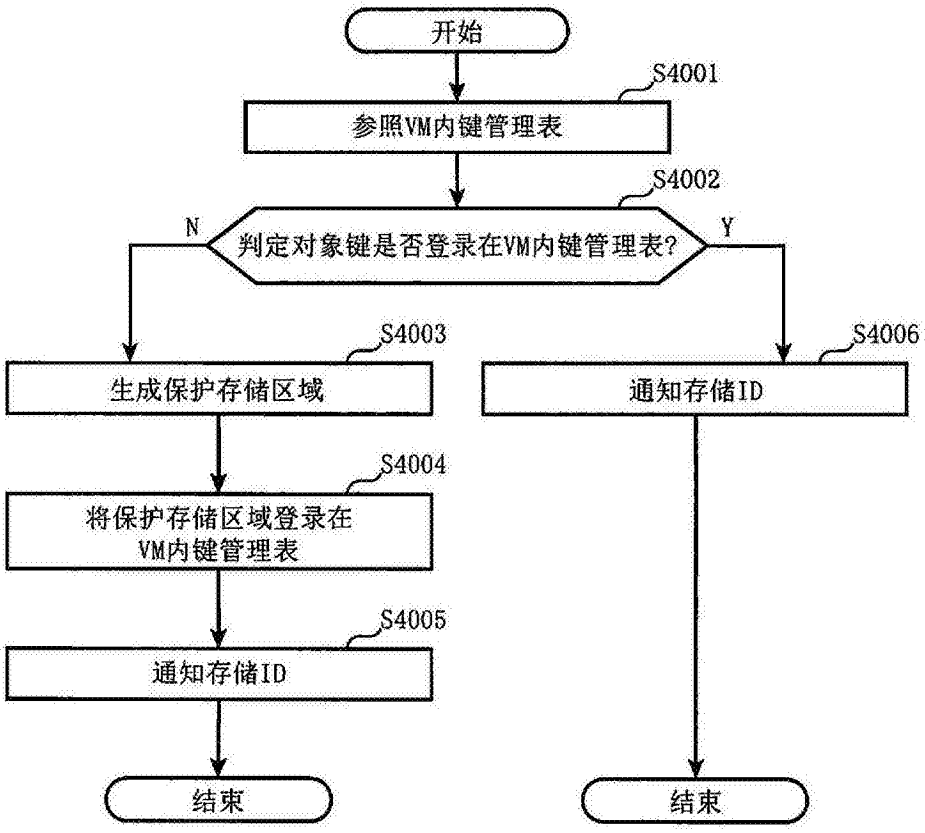

开始
S4001
参照VM内键管理表
S4002
N
判定对象键是否登录在VM内键管理表?
Y
S4003
生成保护存储区域
S4004
将保护存储区域登录在
VM内键管理表
S4005
通知存储ID
结束
S4006
通知存储ID
结束

图4

113

5001 键	5002 共享存储器地址	5003 存储ID
38	0x20004000	3313
21	0x20008000	4243
57	0x20016000	7459

(A)

106

5001 键	5002 共享存储器地址	5003 存储ID
1038	0x80004000	3891
1021	0x80008000	2998
1057	0x80012000	9701

(B)

图5

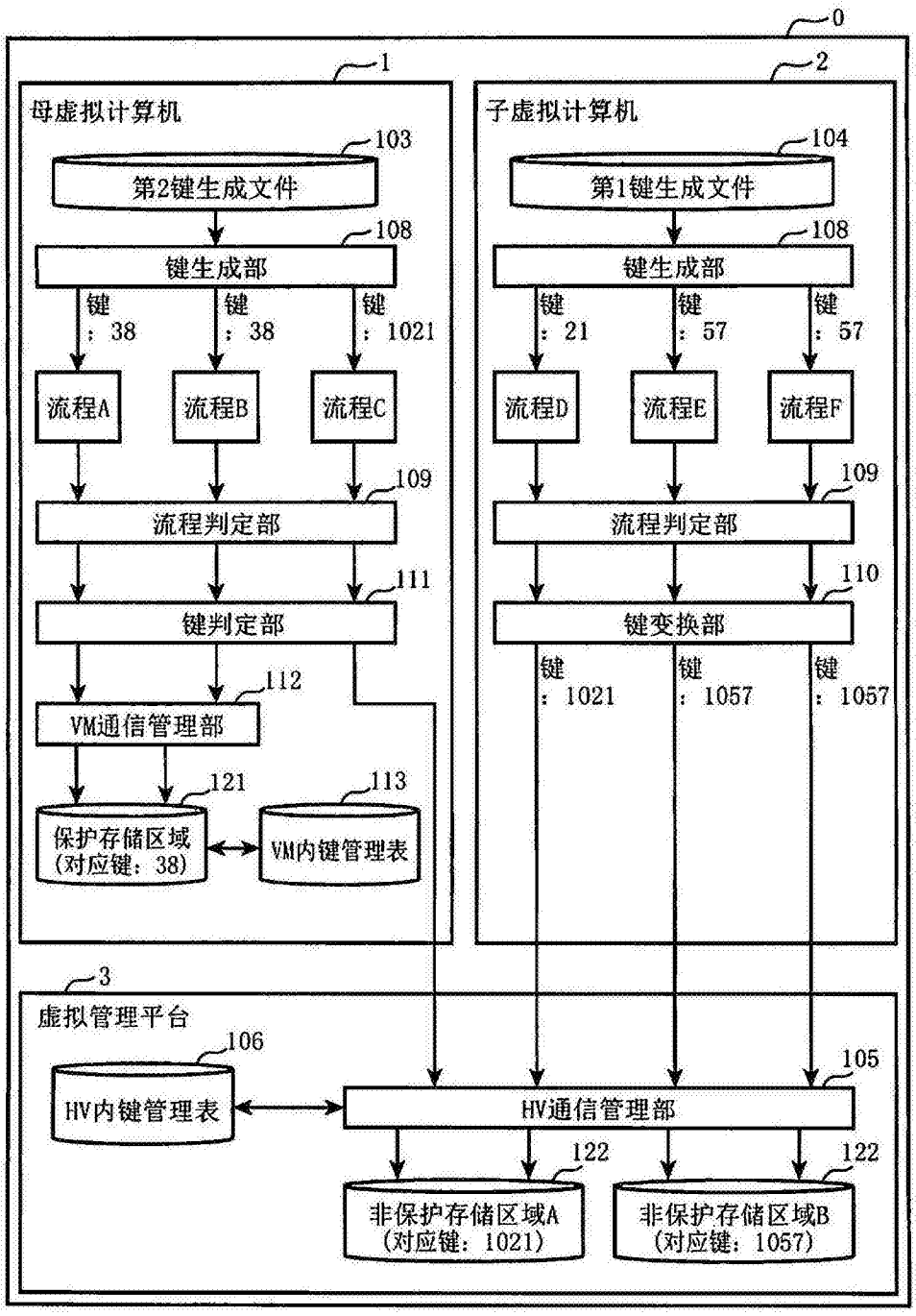

0
1
母虚拟计算机
103
第2键生成文件
108
键生成部
键：38
键：38
键：1021
流程A
流程B
流程C
109
流程判定部
111
键判定部
112
VM通信管理部
121
保护存储区域（对应键：38）
113
VM内键管理表
2
子虚拟计算机
104
第1键生成文件
108
键生成部
键：21
键：57
键：57
流程D
流程E
流程F
109
流程判定部
110
键变换部
键：1021
键：1057
键：1057
3
虚拟管理平台
106
HV内键管理表
105
HV通信管理部
122
非保护存储区域A（对应键：1021）
122
非保护存储区域B（对应键：1057）

图6

VMID	状态
VM__P	发出
VM__C1	待机
VM__C2	待机
...	...

图7

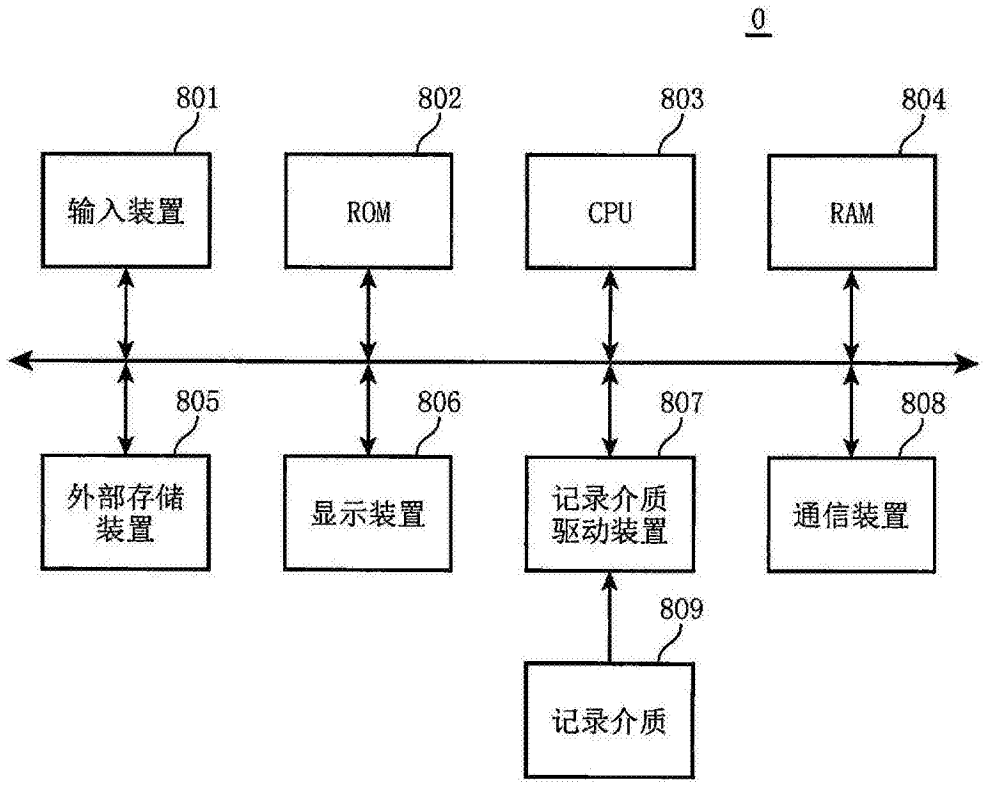


图8

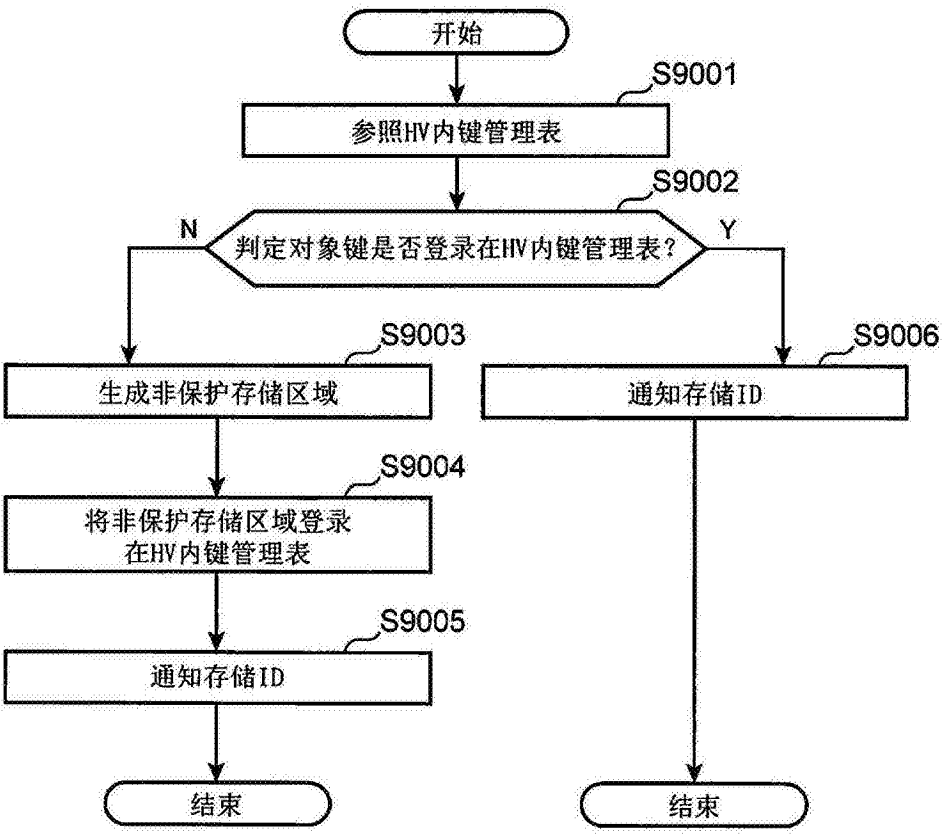

开始
S9001
参照HV内键管理表
S9002
N
判定对象键是否登录在HV内键管理表？
Y
S9003
生成非保护存储区域
S9004
将非保护存储区域登录
在HV内键管理表
S9005
通知存储ID
结束
S9006
通知存储ID
结束

图9