

(12) 发明专利

(10) 授权公告号 CN 101006433 B

(45) 授权公告日 2012. 01. 11

(21) 申请号 200580027706. 6

G06F 21/00(2006. 01)

(22) 申请日 2005. 08. 15

(56) 对比文件

(30) 优先权数据

US 5369749 A, 1994. 11. 29, 全文.

245731/2004 2004. 08. 25 JP

US 20020099952 A1, 2002. 07. 25, 说明书第 2 页 9 段, 第 3 页 26, 27 段, 第 4 页 34 段, 第 6 页 48, 52 段, 第 7 页 57 段、图 1, 4、权利要求 35.

(85) PCT 申请进入国家阶段日

2007. 02. 14

CN 1388448 A, 说明书第 1 页 23-27 行, 说明书第 2 页 1-15 行, 说明书第 8 页 19-26 行, 28-30 行, 说明书第 9 页第 1-4 行, 6-11 行, 说明书第 10 页 24-30 行, 说明书 11 页第 1 行、图 1, 3, 11, 12.

(86) PCT 申请的申请数据

PCT/JP2005/014903 2005. 08. 15

(87) PCT 申请的公布数据

W02006/022161 JA 2006. 03. 02

WO 0214987 A2, 2002. 02. 21, 说明书第 7 页 24 段 21-24 行, 第 8 页 1-2 行.

(73) 专利权人 日本电气株式会社

地址 日本东京都

审查员 田冰

(72) 发明人 井上浩明 酒井淳嗣 阿部刚

枝广正人

(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 李香兰

(51) Int. Cl.

G06F 12/14(2006. 01)

G06F 9/50(2006. 01)

G06F 9/54(2006. 01)

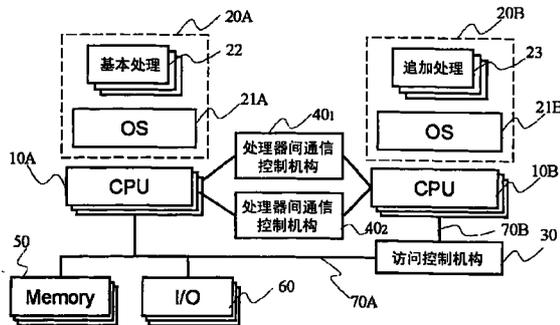
权利要求书 10 页 说明书 23 页 附图 25 页

(54) 发明名称

信息通信装置和程序执行环境控制方法

(57) 摘要

一种可以进行高速处理,在追加应用程序、驱动程序时,确保系统的安全性的装置和方法。其具备执行由基本处理(22)和OS(21A)构成的软件(20A)的第1CPU群(10A);执行由对应追加处理(23)和追加处理的OS(21B)构成的软件(20B)的第2CPU群(10B),用于第1和第2CPU(10A)、(10B)间进行通信的处理器间通信机构(40₁、40₂);控制第2CPU(10B)对存储器(50)和/或者输入输出装置(60)的访问的访问控制机构(30)。



1. 一种信息处理装置,其特征在于,
具备多个处理器,和
能够在上述多个处理器之间共用的存储器和输入输出装置;
上述多个处理器包含构成第 1 域的处理器和构成与上述第 1 域不同的第 2 域的处理器,
上述第 2 域包含处理器,该处理器执行至少 1 个以上与属于上述第 1 域的处理器执行的
处理相比可靠性低的处理,
上述信息处理装置还具备:
处理器间通信部件,其控制上述第 1 域和上述第 2 域的处理器之间的通信;
访问控制部件,其根据属于上述第 2 域的处理器所执行的处理的可靠性,限制属于上
述第 2 域的处理器对属于上述第 1 域的存储器和 / 或者输入输出装置的访问;
上述访问控制部件的设定能够由属于上述第 1 域的处理器来变更。
2. 根据权利要求 1 所述的信息处理装置,其特征在于,
上述访问控制部件具备:
存储允许访问数据的部件;和
访问允许部件,其监视来自属于上述第 2 域的处理器、对上述存储器和 / 或者上述输
入输出装置的访问,参照上述允许访问数据,判断是否允许上述访问。
3. 根据权利要求 2 所述的信息处理装置,其特征在于,上述访问控制部件具有更新上
述允许访问数据的允许访问数据更新部件。
4. 根据权利要求 2 所述的信息处理装置,其特征在于,上述访问控制部件具有:获得由
属于上述第 2 域的处理器产生的访问信息的访问监视部件,和存储上述访问信息的学习部
件。
5. 根据权利要求 1 所述的信息处理装置,其特征在于,上述处理器间通信部件具备中
断控制信息处理装置,该中断控制信息处理装置接收来自信息发送侧的处理器中断请
求,向上述信息的接收侧处理器发布中断。
6. 一种信息处理装置,其特征在于,具备:
执行事先规定的第 1 类处理的至少 1 个第 1 类处理器;
执行与上述第 1 类处理不同的第 2 类处理的至少 1 个第 2 类处理器;
能够在上述第 1 类处理器和第 2 类处理器之间共用的存储器和输入输出装置;
控制上述第 1 类和第 2 类处理器间的通信的处理器间通信部件;和
访问控制部件,其根据上述第 2 类处理的可靠性,限制由上述第 2 类处理器对上述存储
器和 / 或者上述输入输出装置的访问;
上述第 2 类处理器,执行至少 1 个以上与上述第 1 类处理器执行的上述第 1 类处理相
比可靠性低的处理;
上述访问控制部件的设定能够由上述第 1 类处理器来变更。
7. 根据权利要求 6 所述的信息处理装置,其特征在于,
具备多个上述第 1 类处理器,
具备多个上述第 2 类处理器。
8. 根据权利要求 6 所述的信息处理装置,其特征在于,

上述第 1 类处理,包含销售商提供的基本处理,

上述第 2 类处理,包含从网络或者存储介质下载的追加处理。

9. 根据权利要求 6 所述的信息通信装置,其特征在于,

上述第 2 类处理,包含上述第 2 类处理器中执行的设备驱动程序,和 / 或者应用程序。

10. 根据权利要求 6 所述的信息处理装置,其特征在于,具备:

处理器间通信部件,其进行用于从上述第 1 类处理器侧向上述第 2 类处理器传递信息的处理器间通信;

处理器间通信部件,其进行用于从上述第 2 类处理器侧向上述第 1 类处理器传递信息的处理器间通信。

11. 根据权利要求 6 所述的信息处理装置,其特征在于,

上述处理器间通信部件具备中断控制信息处理装置,该中断控制信息处理装置接收来自信息发送侧的处理器中断请求,向上述信息接收侧的处理器发布中断。

12. 根据权利要求 6 所述的信息处理装置,其特征在于,

上述处理器间通信部件,

对应中断目的地的处理器,具备中断控制信息处理装置和共享存储器,

上述中断控制信息处理装置,具备:

中断指示部,其接收来自中断请求源处理器的中断请求,向上述中断目的地处理器进行中断请求;

中断保持部,其保持上述中断指示部的中断请求;和

中断取消部,其接收来自上述中断目的地处理器的中断处理的结束通知,取消中断,

上述共享存储器,具备:

通信区域,其存储从上述中断请求源处理器向上述中断目的地处理器转送的数据;和

排他控制区域,其进行上述通信区域的排他控制。

13. 根据权利要求 6 所述的信息处理装置,其特征在于,

上述访问控制部件具备:

存储允许访问数据的部件;和

访问允许部件,其监视来自上述第 2 类处理器的、对上述存储器和 / 或者上述输入输出装置的访问,参照上述允许访问数据,判断有无上述访问的许可。

14. 根据权利要求 13 所述的信息处理装置,其特征在于,

存储上述允许访问数据的部件,与上述第 2 类处理器相关、与允许访问的处理器相对应地存储着允许访问的地址范围和对上述地址范围允许的访问种类相关的信息。

15. 根据权利要求 13 所述的信息处理装置,其特征在于,

存储上述允许访问数据的部件,与上述第 2 类处理器相关、与不允许访问的处理器相对应地,存储着不允许访问的地址范围和对上述地址范围不许可访问种类相关的信息。

16. 根据权利要求 13 所述的信息处理装置,其特征在于,

允许由上述第 1 类处理器进行的上述允许访问数据的写入和读出,

只允许从上述访问允许部件对上述允许访问数据进行读出,

不允许由上述第 2 类处理器对上述允许访问数据进行读出和写入。

17. 根据权利要求 13 所述的信息处理装置,其特征在于,上述访问控制部件具备高速

缓存存储器,该高速缓存存储器将与上述第 2 类处理器的访问地址相关的信息和与访问允许相关的信息对应地存储。

18. 根据权利要求 13 所述的信息处理装置,其特征在于,上述访问控制部件,具有进行允许访问数据更新的允许访问数据更新部件。

19. 根据权利要求 6 所述的信息处理装置,其特征在于,还具备:

执行事先规定的第 3 类处理的至少 1 个处理器即第 3 类处理器;

在上述第 2 类和第 3 类处理器间进行通信的处理器间通信部件;和

第 2 访问控制部件,其根据上述第 3 类处理的可靠性,限制由上述第 3 类处理器对与上述第 1 类处理器连接的存储器和 / 或者输入输出信息处理装置的访问。

20. 根据权利要求 6 所述的信息处理装置,其特征在于,具备:

执行事先规定的第 3 类处理的至少 1 个处理器即第 3 类处理器;和

在上述第 2 类和第 3 类处理器间进行通信的处理器间通信部件,

上述第 1 类~第 3 类处理器的每一个具备分别通过总线连接的存储器和输入输出装置,

由上述访问控制部件,根据上述第 2 类处理的可靠性,限制由上述第 2 类处理器对与上述第 1 类处理器连接的上述存储器和 / 或者上述输入输出装置的访问,被限制,

由第 2 访问控制部件,根据上述第 3 类处理的可靠性,限制由上述第 3 类处理器对与上述第 1 类处理器连接的存储器和 / 或者输入输出信息处理装置的访问,和 / 或者,对与上述第 2 类处理器连接的上述存储器和 / 或者上述输入输出装置的访问。

21. 根据权利要求 19 或者 20 所述的信息处理装置,其特征在于,

上述第 3 类处理器,执行至少 1 个以上与上述第 2 类处理器执行的上述第 2 类处理相比可靠性低的处理。

22. 根据权利要求 6 所述的信息处理装置,其特征在于,具备:

基本域,其具备基本软件环境、外部装置和 / 或者文件系统、操作系统、存储下载数据的安全信息的安全策略数据库、控制本机代码下载数据的下载的本机代码下载管理部件;

信任扩展域,其包括控制本机代码的下载程序的执行的本机代码下载执行部件、操作系统,

上述信任扩展域,执行由上述基本域的本机代码下载管理部件判断为可信任的、已下载的应用程序即信任应用程序,由上述基本域的本机代码下载管理部件,将判断为可信任的、已下载的设备驱动程序即信任驱动程序安装到上述信任扩展域的操作系统中,由上述信任驱动程序访问事先准备的、许可的外部装置,执行可信任的追加处理,

上述基本域被安装在上述第 1 类处理器中,

上述信任扩展域被安装在上述第 2 类处理器中。

23. 根据权利要求 19 或者 20 所述的信息处理装置,其特征在于,具备:

基本域,其具备基本软件环境、外部装置和 / 或者文件系统、操作系统、存储下载数据的安全信息的安全策略数据库、控制本机代码下载数据的下载的本机代码下载管理部件,

信任扩展域,其具备控制本机代码的下载程序的执行的本机代码下载执行部件、操作系统,

上述信任扩展域,执行由上述基本域本机代码下载管理部件判断能够信任的、已下载

的应用程序即信任应用程序,由上述基本域的本机代码下载管理部件,将判断为可信任的、已下载的设备驱动程序即信任驱动程序安装到上述信任扩展域的操作系统中,由上述信任驱动程序,对事先准备的、许可的外部装置进行访问,执行能够信任的追加处理,

不信任扩展域,其具备控制本机代码的下载程序的执行的本机代码下载执行部件、操作系统,

上述不信任扩展域,执行由上述基本域的本机代码下载管理部件判断为不能信任的、已下载的应用程序即不信任应用程序,由上述基本域的本机代码下载管理部件,将判断为不能信任的、已下载的设备驱动程序即无信任驱动程序安装到上述不信任扩展域的操作系统中,由上述无信任驱动程序对事先准备的、许可的外部装置进行访问,执行不信任的追加处理,

上述基本域被安装在上述第 1 类处理器中,

上述信任扩展域被安装在上述第 2 类处理器中,

上述不信任扩展域被安装在上述第 3 类处理器中。

24. 根据权利要求 23 所述的信息处理装置,其特征在于,

如果从上述基本域的外部装置输入下载数据,上述基本域的上述本机代码下载管理部件,检查上述下载数据的证书,检查结果判断为是正确的证书时,将上述下载数据发送到上述信任扩展域的上述本机代码下载执行部件,

另一方面,上述检查结果为没有证书、或者证书的内容不正确时,将上述下载数据发送到上述不信任扩展域的上述本机代码下载执行部件。

25. 根据权利要求 22 所述的信息处理装置,其特征在于,

从上述基本域的外部装置输入下载数据,将上述下载数据识别为下载应用程序时,上述基本域的上述本机代码下载管理部件,检查上述下载应用程序的证书,检查的结果判断为是正确的证书时,将上述下载应用程序,发送到上述信任扩展域的上述本机代码下载执行部件。

26. 根据权利要求 22 所述的信息处理装置,其特征在于,

从上述基本域的外部装置输入下载数据,将上述下载数据识别为下载驱动程序时,上述基本域的上述本机代码下载管理部件,检查上述下载驱动程序的证书,检查结果判断为是正确的证书时,将上述下载驱动程序发送到上述信任扩展域的上述本机代码下载执行部件中,

上述信任扩展域的上述本机代码下载执行部件,将上述下载驱动程序,安装到上述信任扩展域的操作系统中。

27. 根据权利要求 23 所述的信息处理装置,其特征在于,

从上述基本域的外部装置输入下载数据,将上述下载数据识别为下载应用程序时,上述基本域的上述本机代码下载管理部件,检查上述下载应用程序的证书,判断检查结果为没有证书或证书的内容不正确时,通过上述信任扩展域的上述本机代码下载执行部件,将上述应用程序发送到上述不信任扩展域的上述本机代码下载执行部件。

28. 根据权利要求 23 所述的信息处理装置,其特征在于,

从上述基本域的外部装置输入下载数据,将上述下载数据识别为下载驱动程序时,上述基本域的上述本机代码下载管理部件,检查上述下载驱动程序的证书,检查结果判断为

没有证书或证书的内容不正确时,通过上述信任扩展域的上述本机代码下载执行部件,将上述下载驱动程序发送到上述不信任扩展域的上述本机代码下载执行部件,

上述不信任扩展域的上述本机代码下载执行部件,将上述下载驱动程序,安装到上述不信任扩展域的操作系统中。

29. 根据权利要求 22 所述的信息处理装置,其特征在于,

上述信任扩展域具备基本功能程序库,该基本功能程序库作为程序库包含向上述基本域的基本软件环境的基本功能发布请求的处理群,

接收来自自己下载到上述信任扩展域的应用程序的请求,上述信任扩展域的上述基本功能程序库,向上述基本域的上述本机代码下载管理部件发送请求,

上述基本域的上述本机代码下载管理部件,确认由上述信任扩展域接收的请求是否合适,在请求正确时,向上述基本软件环境的基本功能请求处理。

30. 根据权利要求 29 所述的信息通信信息处理装置,其特征在于,上述基本域的上述基本功能,处理请求,向上述基本域的上述本机代码下载管理部件通知处理结束,

上述基本域的上述本机代码下载管理部件,将结束通知上述信任扩展域的基本功能程序库,由上述基本功能程序库将处理结束通知上述应用程序。

31. 根据权利要求 23 所述的信息处理装置,其特征在于,

上述信任扩展域具备基本功能程序库,该基本功能程序库作为程序库包含向上述基本域的基本软件环境的基本功能发布请求的处理群,

自下载在上述不信任扩展域的应用程序向上述信任扩展域的应用程序发送数据,

上述信任扩展域的上述应用程序,对上述基本功能程序库发布请求,该请求包含来自上述不信任扩展域的下应用程序的数据,

上述基本功能程序库,接收来自上述信任扩展域的上述应用程序的请求,对上述基本域的上述本机代码下载管理部件发送请求,

上述基本域的上述本机代码下载管理部件,确认接收的请求是否相适当,上述请求适当时,请求用户确认,上述用户的确认结果为允许时,向上述基本软件环境的基本功能请求处理,

另一方面,上述用户的确认结果为不允许时,上述基本域的上述本机代码下载管理部件,通知上述基本功能程序库不允许。

32. 根据权利要求 31 所述的信息处理装置,其特征在于,

上述用户的确认结果为允许时,上述基本功能,处理请求,通知上述基本域的上述本机代码下载管理部件处理结束,上述基本域的上述本机代码下载管理部件,将结束通知上述信任扩展域的基本功能程序库,由上述基本功能程序库向上述信任扩展域的下应用程序通知处理结束,上述信任扩展域的下应用程序,向上述不信任扩展域的上述下应用程序通知处理结束;

另一方面,上述用户的确认结果为不允许时,从基本程序库向上述不信任扩展域的下应用程序通知不允许。

33. 根据权利要求 22 所述的信息处理装置,其特征在于,上述基本域和上述信任扩展域,具备将虚拟装置映射到实际硬件装置上的虚拟机监视器,虚拟了文件系统、装置和 CPU 被虚拟化。

34. 根据权利要求 23 所述的信息通信信息处理装置,其特征在于,上述基本域、上述信任扩展域和上述不信任扩展域,具备将虚拟装置映射到实际硬件装置上的虚拟机监视器,虚拟了文件系统、装置和 CPU。

35. 根据权利要求 24 或者 25 所述的信息处理装置,其特征在于,在上述域的处理器各个群中,通过分离部件,可以分离为多个。

36. 根据权利要求 24 或者 25 所述的信息处理装置,其特征在于,上述基本域的处理器管理其他域的处理器。

37. 一种信息处理设备,具备多个权利要求 6 所述的信息处理装置,每个上述信息处理装置在不同的芯片内构成。

38. 根据权利要求 37 所述的信息处理设备,其特征在于,具有访问限制部件,其在上述芯片间形成并根据属于在上述芯片中形成的上述信息处理装置的处理的可靠性,限制对存储器/输入输出装置的访问允许。

39. 一种程序执行控制方法,其特征在于,包含:

根据执行的程序的可靠性,划分为多个域,属于不同域且能够共用存储器和输入输出装置的处理器之间,将数据或者指令,通过处理器间通信部件相互发送的步骤;和

根据至少执行 1 个以上可靠性低的程序的域的可靠性,限制属于执行至少 1 个以上可靠性低的程序的域的处理器、对属于执行可靠性高的程序的域的存储器和/或者输入输出装置的访问的步骤;

上述访问限制的设定能够由属于上述执行可靠性高的程序的域的处理器来变更。

40. 一种程序执行环境控制方法,其特征在于,

信息处理系统具备基本域和信任扩展域,

基本域具备:基本软件环境;外部装置和/或者文件系统;操作系统;存储下载数据的安全信息的安全策略数据库及控制本机代码下载数据的下载的本机代码下载管理部件;

信任扩展域具备:控制本机代码的下载程序的执行的本机代码下载执行部件;操作系统,上述信任扩展域,执行由上述基本域的本机代码下载管理部件,判断为能够信任的、已下载的应用程序即信任应用程序,由上述基本域的本机代码下载管理部件,将判断为能够信任的、已下载的设备驱动程序即信任驱动程序安装到上述信任扩展域的操作系统中,由上述信任驱动程序对事先准备的、许可的外部装置进行访问,执行能够信任的追加处理,

该程序执行环境控制方法包括:

基本域和信任扩展域间的处理器之间,通过处理器间通信部件,相互进行通信的步骤;

由访问控制部件限制属于上述信任扩展域的处理器对上述基本域的存储器和/或者输入输出装置的访问的步骤。

41. 一种程序执行环境控制方法,其特征在于,

信息处理系统具有基本域、信任扩展域和不信任扩展域

上述基本域,具备:基本软件环境;外部装置和/或者文件系统;操作系统;存储下载数据的安全信息的安全策略数据库;控制本机代码下载数据的下载的本机代码下载管理部件,

信任扩展域,具备:控制本机代码的下载程序的执行的本机代码下载执行部件;操作

系统，

上述信任扩展域，执行由上述基本域的本机代码下载管理部件判断为能够信任的、已下载的应用程序即信任应用程序，由上述基本域的本机代码下载管理部件，将判断为能够信任的、已下载的设备驱动程序即信任驱动程序安装到上述信任扩展域的操作系统中，由上述信任驱动程序，对事先准备的、许可的外部装置进行访问，执行能够信任的追加处理，

上述不信任扩展域，具备控制本机代码的下载程序的执行的本机代码下载执行部件；操作系统，

上述不信任扩展域，执行由上述基本域的本机代码下载管理部件判断为不能信任的、已下载的应用程序即不信任应用程序，由上述基本域本机代码下载管理部件，将判断为不能信任的、已下载的设备驱动程序即无信任驱动程序安装到上述不信任扩展域的操作系统中，由上述无信任驱动程序对事先准备的、已许可的外部装置进行访问，执行不信任的追加处理，

该程序执行环境控制方法包括：

上述基本域、上述信任扩展域和不信任扩展域各域的处理器之间，通过处理器间通信部件，相互通信的步骤；

由第 1 访问控制部件，限制由属于上述信任扩展域的处理器对上述基本域的存储器和 / 或者输入输出装置的访问的步骤；

由第 2 访问控制部件，限制由属于上述不信任扩展域的处理器对上述基本域的存储器和 / 或者输入输出装置的访问的步骤。

42. 根据权利要求 40 所述的程序执行环境控制方法，其特征在于，包含：

如果从上述基本域的外部装置输入下载数据，上述基本域的上述本机代码下载管理部件，检查上述下载数据的证书的步骤；

在检查的结果判断为是正确的证书时，向上述信任扩展域的上述本机代码下载执行部件发送下载数据的步骤。

43. 根据权利要求 41 所述的程序执行环境控制方法，其特征在于，包含：

如果由上述基本域的外部装置输入下载数据，上述基本域的上述本机代码下载管理部件，检查上述下载数据的证书的步骤；

在上述检查结果判断为是正确的证书时，向上述信任扩展域的上述本机代码下载执行部件发送上述下载数据的步骤；和

在上述检查结果判断为是没有证书或者证书的内容不正确时，向上述不信任扩展域的上述本机代码下载执行部件，发送上述下载数据的步骤。

44. 根据权利要求 40 或者 41 所述的程序执行环境控制方法，其特征在于，包含：

从上述基本域的外部装置输入下载数据，将上述下载数据识别为下载应用程序时，上述基本域的上述本机代码下载管理部件，检查上述下载应用程序的证书的步骤，

在上述检查结果判断为正确时，将上述下载应用程序发送到上述信任扩展域的上述本机代码下载执行部件的步骤。

45. 根据权利要求 40 或者 41 所述的程序执行环境控制方法，其特征在于，其包含：

从上述基本域的外部装置输入下载数据，将上述下载数据识别为下载驱动程序时，上述本机代码下载管理部件，检查下载驱动程序的证书的步骤；

判断上述检查结果为正确的证书时,向上述信任扩展域的上述本机代码下载执行部件发送下载驱动程序的步骤;和

上述信任扩展域的上述本机代码下载执行部件,将上述下载驱动程序安装到上述信任扩展域的操作系统中的步骤。

46. 根据权利要求 41 所述的程序执行环境控制方法,其特征在于,包含:

从上述基本域外部装置输入下载数据,将上述下载数据识别为下载应用程序时,上述基本域的上述本机代码下载管理部件,检查下载应用程序的证书的步骤;和

上述检查结果为没有证书或证书的内容不正确时,通过上述信任扩展域的上述本机代码下载执行部件,向上述不信任扩展域的上述本机代码下载执行部件,发送上述下载应用程序的步骤。

47. 根据权利要求 41 所述的程序执行环境控制方法,其特征在于,包含:

从上述基本域的外部装置输入下载数据,将上述下载数据识别为下载驱动程序时,上述基本域的上述本机代码下载管理部件,检查上述下载驱动程序的证书的步骤;

上述检查结果为没有证书或证书的内容不正确时,通过上述信任扩展域的上述本机代码下载执行部件,将上述下载驱动程序发送到上述不信任扩展域的上述本机代码下载执行部件的步骤;和

上述不信任扩展域的上述本机代码下载执行部件,将上述下载驱动程序安装到上述不信任扩展域的操作系统中的步骤。

48. 根据权利要求 40 或者 41 所述的程序执行环境控制方法,其特征在于,

在上述信任扩展域中设置有基本功能程序库,该基本功能程序库作为程序库包含向上述基本域的基本软件环境的基本功能发布请求的处理群,

上述程序执行环境控制方法,包含:

接收来自下载到上述信任扩展域中的应用程序的请求,上述基本功能程序库,对上述基本域的上述本机代码下载管理部件,发送请求的步骤;和

上述基本域的上述本机代码下载管理部件,确认由上述信任扩展域接收的请求是否适当,上述请求适当时,向上述基本软件环境的基本功能请求处理的步骤。

49. 根据权利要求 48 所述的程序执行环境控制方法,其特征在于,包含:

上述基本域的上述基本功能,处理请求,将处理结束通知上述基本域的上述本机代码下载管理部件的步骤;和

上述基本域的上述本机代码下载管理部件,将结束通知上述信任扩展域的基本功能程序库,由上述基本功能程序库通知上述应用程序处理结束的步骤。

50. 根据权利要求 41 所述的程序执行环境控制方法,其特征在于,

在上述信任扩展域中设置基本功能程序库,该基本功能程序库作为程序库包含将对上述基本域的基本软件环境的基本功能发布请求的处理群,

上述程序执行环境控制方法,包含:

由下载到上述不信任扩展域的应用程序向上述信任扩展域的应用程序发送数据的步骤;

上述信任扩展域的上述应用程序,对上述基本功能程序库发布请求的步骤,该请求包含来自上述不信任扩展域的下载应用程序的数据,和

接收来自上述信任扩展域的上述应用程序的上述请求,上述基本功能程序库,向上述基本域的上述本机代码下载管理部件发送请求的步骤;

上述基本域的上述本机代码下载管理部件,确认接收的请求是否相适当的步骤;

上述确认结果为上述请求适当时,请求用户确认,上述用户的确认结果为允许时,向上述基本软件环境的基本功能请求处理的步骤,和

另一方面,上述用户的确认结果为不允许时,上述本机代码下载管理部件,将不允许通知上述基本功能程序库的步骤。

51. 根据权利要求 50 所述的程序执行环境控制方法,其特征在于,包含:

上述用户的确认结果为允许时,上述基本功能,处理请求,将处理结束通知上述基本域的上述本机代码下载管理部件的步骤;

上述基本域的上述本机代码下载管理部件,将结束通知上述信任扩展域的基本功能程序库的步骤;

由上述基本功能程序库,将处理结束通知上述信任扩展域的下载应用程序的步骤;

上述信任扩展域的下载应用程序,将处理结束通知上述不信任扩展域的上述下载应用程序的步骤;和

另一方面,上述用户的确认结果为不允许时,从基本程序库向上述不信任扩展域的下载应用程序通知不允许的步骤。

52. 根据权利要求 40 所述的程序执行环境控制方法,其特征在于,

上述基本域和上述信任扩展域,通过将虚拟装置映射到实际硬件装置中的虚拟机监视器,虚拟了文件系统、装置和 CPU。

53. 根据权利要求 41 所述的程序执行环境控制方法,其特征在于,

上述基本域、上述信任扩展域和上述不信任扩展域,具备将虚拟装置映射到实际硬件装置中的虚拟机监视器,虚拟了文件系统、装置和 CPU。

54. 一种便携信息终端,其特征在于,

具备多个处理器,和

能够在上述多个处理器之间共用的存储器和输入输出装置;

上述多个处理器,包括:构成第 1 域的处理器和构成与上述第 1 域不同的第 2 域的处理器,

上述第 2 域包括处理器,该处理器执行至少 1 个以上比属于上述第 1 域的处理器执行的处理可靠性低的处理,

具备:

处理器间通信部件,其控制上述第 1 域和上述第 2 域处理器之间的通信;和

访问控制部件,其根据上述第 2 域中执行的处理的可靠性,限制由属于上述第 2 域的处理器对属于上述第 1 域的存储器和 / 或者输入输出装置的访问;

上述访问控制部件的设定能够由属于上述第 1 域的处理器来变更。

55. 一种信息通信装置,其特征在于,

具备多个处理器,和

能够在上述多个处理器之间共用的存储器和输入输出装置;

根据执行的处理的可靠性,上述多个处理器构成多个域,

不同域间的处理器之间,通过处理器间通信部件相互通信,

具备访问控制部件,其控制由属于执行安全相对低的处理的域的处理器对属于执行安全相对高的处理的域的存储器和 / 或者输入输出装置的访问;

上述访问控制部件的设定能够由属于上述属于执行安全相对高的处理的域的处理器来变更。

56. 一种信息通信装置,其特征在于,具备:

执行事先规定的第 1 类处理的至少 1 个第 1 类处理器;

执行与上述第 1 类处理不同的事先规定的第 2 类处理的至少 1 个第 2 类处理器;

能够在上述第 1 类处理器和第 2 类处理器之间共用的存储器和输入输出装置;

控制上述第 1 类和第 2 类处理器间通信的处理器间通信部件;和

访问控制部件,其控制由上述第 2 类处理器对上述存储器和 / 或者上述输入输出装置的访问;

上述第 2 类处理器,执行至少 1 个以上与上述第 1 类处理器执行的上述第 1 类处理相比可靠性低的处理;

上述访问控制部件的设定能够由上述第 1 类处理器来变更。

信息通信装置和程序执行环境控制方法

技术领域

[0001] 本发明涉及信息处理装置,尤其是涉及适用于确保执行从信息处理装置外部下载的追加处理时的安全的装置和方法。

背景技术

[0002] 在便携式电话机 (mobile phone) 等信息通信终端装置中,通常,用于实现该终端装置的基本功能的基本处理 (例如呼叫处理功能,访问互联网用的浏览功能,电子邮件功能,画面控制功能等),随操作系统一起事先被安装,对于与上述基本处理不同的追加处理 (程序),由用户的操作等,从网络等外部,下载到该终端装置执行并进行安装。可是,执行下载的追加处理时,操作系统和基本处理等,有可能暴露在由该追加处理产生的攻击下。

[0003] 图 21 是示意地表示执行已下载的追加处理的信息通信终端装置的典型构成的一个例子的图。图 21 由框图示意地表示了众所周知的典型装置的构成。在以下,追加处理,为由本机代码 (在提供者方面进行了编译或者汇编 (assemble) 处理的二进制代码) 提供的应用程序和设备驱动程序 (是对装置进行访问请求,执行来自装置的中断处理的软件,也称“I/O 驱动程序”) 的情况进行说明。

[0004] 在如图 21 所示的构成中,下载追加处理 23 进行执行时 (追加处理 23 为设备驱动程序时,安装到操作系统中执行时),对于基本处理 22,操作系统 (称为“OS”) 21, CPU (Central Processing Unit) 10, 存储器 50, 输入输出装置 (I/O) 60, 有可能被追加处理 23 直接攻击。其理由是由于没有安装实现安全的执行环境机构,限制来自追加处理 23 的、对基本处理 22、CPU10、OS21、存储器 50 或者输入输出装置 (I/O) 60 的攻击。即,为图 21 所示的构成时,追加处理 23 能够任意地发布对基本处理 22 的处理请求,对 OS21 的处理依赖,对 CPU10、存储器 50 和输入输出装置 60 的处理请求,也能够自由地访问硬件、软件各种资源。因此,恶意的追加处理 23 (或者,尽管不是恶意,但是感染了病毒等的追加处理),能够自由地攻击无防备的 OS21、基本处理 22 等。

[0005] 追加设备驱动程序,有时作为例如驻留 (常驻型) 驱动程序,被安装到 OS21 的内核中,该设备驱动程序的可靠性会直接对 OS21 的可靠性和性能带来影响。根据设备的特性这是很显然的,设备驱动程序包括设定对装置的处理和在来自装置的中断时被调度器起动的中断服务,中断服务的执行时间 (这期间,重新调度被禁止),根据处理性能被限制在特别短的时间 (例如毫秒以下)。即,追加设备驱动程序假定是有恶意的驱动程序时,能够容易降低信息处理装置的处理性能。其即使不是常驻型,装载驱动程序 (选择性的装载到内存,或从内存卸载的驱动程序) 时也一样。这样,通过作为追加处理安装的恶意的驱动程序进行攻击时,OS21 的内核将被直接攻击,这是致命的 (实质上将变为不能动作)。

[0006] 因此,当前提出了各种设计方式,对下载的追加处理的执行环境给予限制,保护基本处理等。以下,就几个典型例进行概述。

[0007] 图 22 是表示软件的追加处理的执行保护环境的构成的一个典型例子的图。在图 22 所示的例子中,本机代码的追加处理 23 采用在虚拟机 24 上执行的构成。作为其中的一

个例子,假定追加处理 23 是由 JAVA(注册商标)字节代码描述的,下载的 JAVA(注册商标)字节代码在形成虚拟机 24 的 JVM(JAVA(注册商标)虚拟机)上执行。

[0008] 在这样的构成中,基本处理 22 或 OS21 等,与追加处理 23 在软件上分离,确保其安全性。即,追加处理 23 只通过虚拟机 24 对 OS21、CPU10、存储器 50、I/O60 等进行访问。在虚拟机 24,通常,不赋予进行 OS21 的内核模式中的执行(例如特权性命令的执行)等的权限,因此,追加处理 23 不能直接操作 OS21。另外,由于虚拟机 24,一般,在解释的方式下执行追加处理 23 的命令代码,容易监视追加处理 23 的命令、动作是否适当,通过限制例如来自追加处理 23 的对硬件资源和软件资源的非法访问(例如将大量的数据输出到网络上或者画面上等),虚拟机 24 也能够担当软件上的保护过滤网、或者防护壁或者防护门的作用。这样,通过虚拟机 24,基本处理 22、OS21 等与追加处理 23 在软件上分离。

[0009] 可是,图 22 所示的虚拟机方式具有以下问题点。

[0010] 由下载的追加处理 23,对虚拟机 24 的漏洞(例如安全漏洞)产生攻击等时,会损害系统的安全性。

[0011] 另外,由于通常,JAVA(注册商标)虚拟机等虚拟机 24 是一条命令一条命令的解释执行 JAVA(注册商标)字节代码等的命令代码的解释方式,其执行速度慢。

[0012] 另外,虚拟机 24,在执行追加处理 23 时,通过发布系统调用(call),进行对 OS21 的处理请求,由于系统调用的开销(overhead)多,处理的执行慢。例如虚拟机 24 中,对应追加处理 23 的 1 个命令的系统调用进行 1 个或者多个发布。进行由来自用户模式的系统调用发布产生的对系统模式的上下文关联(context)/切换,OS21 的系统调用登录部中的系统调用的数据包的解码,参数等的正确性校验(错误检测处理),处理的分配(dispatch),还有,处理结束时的处理结果的提交和上下文关联(context)/切换,从内核空间向用户空间的切换等一系列的控制,开销很大。

[0013] 并且,如图 22 所示的构成的情况,作为追加处理 23,不能将设备驱动程序编入到 OS21 中。如由图 22 表明的,虚拟机 24 位于 OS21 的上层。虚拟机 24 采用,根据追加处理 23 的代码,对 OS21 进行处理请求,从 OS21 接收处理结果,根据需要返回追加处理 23 的构成,将追加处理作为设备驱动程序编入 OS21 内,控制追加处理的执行的虚拟机也需要编入 OS21 内,由于这样的构成,在如图 22 所示的虚拟机方式中,原理上是不可能的。

[0014] 作为由软件实现的其他的安全管理方式,也知道例如如图 23 所示的构成。如图 23 所示,在追加处理 23 中添加,用于证明其为可以信赖的处理的证书 25,下载到终端(信息处理装置)。在终端侧中采取,检查添加的证书 25 的内容,认证添加的证书 25 为正确的证书时,允许安装、执行下载的追加处理 23 的构成。作为证书 25 可以采用数字签名(ITU-T X. 509)。例如证书 25 中,存储着证明的组织及其公钥,CA(认证局)的数字签名(用 CA 的密钥加密证明的组织或公钥等得到的),进行证书的认证时,用 CA 的公钥解读 CA 的数字签名的部分,确认是否与证书的数据内容一致,一致时,判断可以证书的数据。或者,证书 25 既可以是证明真正的买主的证书,也可以是任意的证书。并且,设备驱动程序的签名功能(Driver Signing)也被安装在例如 Windows(注册商标)2000 等中。

[0015] 如图 23 所示的方式时,追加处理 23 能够由本机代码提供,与图 22 所示的虚拟机方式相比,可以高速执行。另外,作为追加处理 23,可以执行应用程序、设备驱动程序。可是,系统的可靠性全面依据追加处理 23 的安全性。即,有不能事先检测追加处理 23 的问题,

也有可能给系统带来致命的损坏。

[0016] 图 24 是表示由硬件进行安全管理的处理器的构成的图。参照图 24, CPU11 具有安全 (secure) 模式 12 和非安全 (unsecure) 模式 13, 下载的追加处理 23 对应该追加处理 23 的 OS21B, 主要以非安全模式 13 执行。并且, 内存管理单元 14, 将非安全模式 13 下执行的内存区域 (地址空间) 与安全模式 12 下访问的内存区域分离进行管理, 禁止从非安全模式 13 向安全模式 12 的内存区域的访问。即, 内存管理单元 14 进行来自非安全模式 13 的内存的访问控制, 进行禁止从非安全模式 13 向安全模式 12 的内存区域的访问的控制。

[0017] 这样, 在图 24 所示的构成中, 在安全模式 12 下执行基本处理 22, 假设分离成执行追加处理 23 的 CPU 和不同的 CPU, 来谋求提高安全性。

[0018] 可是, 安全模式和非安全模式, 在 CPU 中, 分时执行, 不从非安全模式返回时, 不能进行安全模式下的系统的动作。

[0019] 另外, 由于分时处理非安全模式和安全模式, 在其切换时, 需要模式转换等开销。

[0020] 此外, 将追加处理 23 作为设备驱动程序, 安装非安全模式的 OS21B 内时, 如果驱动程序有恶意, 有可能不能返回安全模式, 也有可能对系统带来致命的损坏。

[0021] 并且, 与图 24 所示的构成一样, 作为在系统内存中设置分离域, 具备正常执行模式和分离执行模式的处理器, 参照后面所述的专利文献 1 的记载。专利文献 1 所述的装置中, 正常执行模式, 是处理器在非安全环境, 即在没有由分离执行模式提供的安全功能的通常的动作模式下动作的模式, 从正常执行模式向分离域的访问被禁止, 在分离执行模式中, 采取支持规定的分离命令的执行的构成。并且, 由于这样的构成也分时处理正常执行模式和分离执行模式, 在其切换时, 需要模式转换等开销。

[0022] 另外, 公开了以下构成: 具备 2 个处理器单元和开关单元, 1 个处理器单元与公共数据通信网络相连接, 另一个处理器单元不与公共数据通信网络相连接, 起到作为数据安全用单元的功能 (参照后面的专利文献 2)。在专利文献 2 中所述的系统中, 由开关分离与公共数据通信网络连接的处理器单元和数据安全用单元, 确保了数据安全用单元的安全性。可是, 关于与公共数据通信网络连接的处理器单元, 由于执行上述的追加处理 (自网络等下载的追加处理) 而被攻击的对策, 一点也没有考虑。即使数据安全用单元是安全的, 与公共数据通信网络连接的处理器单元不具备应对由追加处理产生的攻击的有效的安全机构。因此, 对连接到公共数据通信网络的处理器单元实现安全管理时, 有必要采用上述的任意一种方式。

[0023] 此外, 在专利文献 3 中记载了以下的构成: 在将处理器中被分离的执行程序或者操作系统同时执行系统中, 由于保护非法程序的执行环境, 第 1 程序执行期间, 设定只有第 1 程序利用的内存空间, 第 1 程序和计算机的执行环境的通信, 通过包含共享存储器空间的利用、专用的中断或者专用的 I/O 端口的单一链接进行, 第 1 程序, 在被限制的执行环境中, 除了与设定的内存空间的单一链接之外, 限制访问处理器上的资源。该专利文献 3 中所述的方法, 由于第 1 程序, 除了设定的内存空间和单一链接 (共享存储器空间的利用, 专用的中断, 或者专用的 I/O 端口) 之外, 限制访问处理器上的资源, 所以不能将第 1 程序作为设备驱动程序使用, 不能应用程序到包含设备驱动程序的追加处理。

[0024] 并且, 作为公开与后面所述的本发明中使用的处理器间通信机构相关连的技术的出版物, 在后面所述的专利文献 4 公开了多处理器系统中的 CPU 间通信方式。该专利文献 4

中作为现有的技术公开了以下结构：当多处理器利用共有内存进行 CPU 间通信时，CPU2 让 CPU1 产生中断时，在对于 CPU1 的固定区域中自用的 CPU 间通信信息写入区域写入通信信息而产生中断，在 CPU1 中，如果产生中断，访问与 CPU2 对应的 CPU 间通信信息写入区域，执行中断处理，并且，发明中还记载了削减共享存储器的访问次数的技术。

[0025] 专利文献 1：特表 2004-500666 号公报

[0026] 专利文献 2：特表 2002-542537 号公报

[0027] 专利文献 3：特表 2002-533791 号公报

[0028] 专利文献 4：特开平 6-332864 号公报。

发明内容

[0029] 如上所述，在现有的装置中，其对于来自下载的、存有恶意的或者过失的追加处理的攻击实施了确保安全性的对策，但在处理性能方面，设备驱动程序的不可执行方面，在确保安全性存在问题方面等，在实用上，还有各种课题。尤其是，如图 22 和图 24 所示，关于信息处理装置，不能从装置外部下载追加设备驱动程序的设计方式（体系结构）意味着，实际上不能进行装置的追加，功能追加等，在这方面，可用性 (availability) 被限制。另一方面，如上所述，由于例如在内核模式下运行追加设备驱动程序，会给 OS、系统的可靠性带来直接影响，请求确保特别的安全性，提高可靠性。

[0030] 因此，本发明的目的在于，提供可以通过简易的构成进行高速处理，在应用程序和设备驱动程序的追加时又能确保安全性、可靠性的装置和方法。

[0031] 实现上述目的的本发明，描述其概略如下。

[0032] 本发明的 1 个方式 (aspect) 中的装置具备多个处理器，根据执行的处理的可靠性，上述多个处理器构成多个域，不同的域间的处理器之间具备访问控制机构，该访问控制机构经由处理器间通信机构相互通信，控制属于执行安全相对低的处理的域的处理器对属于执行安全相对高的处理的域的存储器和 / 或者输入输出装置的访问。

[0033] 与本发明的 1 个方式 (aspect) 相关的程序执行环境控制方法，包含：将构成信息处理装置的多个处理器，根据执行的程序的可靠性，分为多个域，不同的域的处理器之间，通过处理器间通信机构相互发送数据或者指令的步骤；和由访问控制机构检查由属于执行可靠性相对低的程序的域的处理器对属于执行可靠性相对的高的程序的域的存储器和 / 或者输入输出装置的访问，只执行许可的访问的步骤。

[0034] 本发明的另一方式的装置，具备：执行事先规定的第 1 类处理的至少 1 个处理器（称为“第 1 类处理器”）；执行与上述第 1 类处理不同的事先规定的第 2 类处理的至少 1 个处理器（称为“第 2 类处理器”）；能够在上述多个处理器之间共用的存储器和输入输出装置；控制上述第 1 类和第 2 类处理器间的通信的处理器间通信机构；和控制由上述第 2 类处理器对上述存储器和 / 或者上述输入输出装置的访问的访问控制机构，上述第 2 类处理器，执行至少 1 个以上与上述第 1 类处理器执行的上述第 1 类处理相比可靠性低的处理；上述访问控制部件的设定能够由上述第 1 类处理器来变更。

[0035] 本发明中的装置中，上述第 1 类处理包含可靠性相对高的处理，上述第 2 类处理包含可靠性相对低的处理。本发明中，上述第 1 类处理包含销售商提供的基本处理，上述第 2 类处理包含从网络或者存储介质下载的追加处理。本发明中，上述第 2 类处理也可以包含由

上述第 2 类处理器执行的设备驱动程序和 / 或者应用程序。

[0036] 在本发明中的装置中,作为上述处理器间通信机构,具备:进行从上述第 1 类处理器侧向上述第 2 类处理器传递信息的处理器间通信的处理器间通信机构;和进行从上述第 2 类处理器侧向上述第 1 类处理器传递信息的处理器间通信的处理器间通信机构。

[0037] 本发明中的装置中,上述处理器间通信机构,优先具备中断控制装置,该中断控制装置接收来自信息发送侧的处理器器的中断请求,对上述信息的接收侧处理器发布中断。本发明中,上述处理器间通信机构,优选对应中断目的地处理器,具备中断控制装置和共享存储器,上述中断控制装置,具备:中断指示部,其接收来自中断请求源处理器的中断请求,对上述中断目的地处理器进行中断请求;中断保持部,其保持上述中断指示部的中断请求;和中断取消部,其接收来自上述中断目的地处理器的中断处理的结束通知,取消中断,上述共享存储器,具备:通信区域,其存储从上述中断请求源处理器转送到上述中断目的地处理器的数据;排他控制区域,其进行上述通信区域的排他控制。

[0038] 本发明的装置中,上述访问控制机构,最好具备:存储允许访问数据的机构,其存储与来自上述第 2 类处理器的对上述存储器和 / 或者上述输入输出装置的访问相关的信息;检测上述第 2 类处理器对上述存储器和 / 或者上述输入输出装置的访问,参照上述允许访问数据,判断是否许可上述访问的访问允许机构。本发明中,存储上述允许访问数据的机构,与上述第 2 类处理器相关,并与许可访问的处理器相对应,存储着许可访问的地址范围和与上述地址范围相关的、许可访问种类相关的信息。

[0039] 本发明的另一方式的装置,还具备:执行事先规定的第 3 类处理的至少 1 个处理器(称为“第 3 类处理器”);在上述第 2 类和第 3 类处理器间进行通信的处理器间通信机构;和控制通过上述第 3 类处理器对与上述第 1 类处理器连接的存储器和 / 或者输入输出装置的访问的第 2 访问控制机构。

[0040] 本发明再另一方式的装置,具备:执行事先规定的第 3 类处理的至少 1 个处理器(称为“第 3 类处理器”);和在上述第 2 类和第 3 类处理器间进行通信的处理器间通信机构,上述第 1 类~第 3 类处理器各自具备分别通过总线连接的存储器和输入输出装置,还具备第 2 访问控制机构,由上述访问控制机构控制由上述第 2 类处理器对与上述第 1 类处理器连接的上述存储器和 / 或者上述输入输出装置的访问,由第 2 访问控制机构控制由上述第 3 类处理器对与上述第 1 类处理器连接的存储器和 / 或者输入输出装置的访问、和 / 或者对与上述第 2 类处理器连接的上述存储器和 / 或者上述输入输出装置的访问。

[0041] 本发明另一方式的装置具备:(A) 基本域,其具备基本软件环境、外部装置和 / 或者文件系统以及操作系统,以及具备存储下载数据的安全信息的安全数据库、和控制本机代码下载数据的下载的本机代码下载管理机构;(B) 信任扩展域,其具备控制本机代码下载数据的下载的本机代码下载管理机构、操作系统,并执行由上述基本域的本机代码下载管理机构判断为能够信赖的、已下载的应用程序(称为“信任应用程序”),将由上述基本域的本机代码下载管理机构判断为能够信赖的、已下载的设备驱动程序(称为“信任驱动程序”)安装到上述操作系统中,由上述信任驱动程序,访问事先准备的许可的外部装置,执行能够信赖的追加处理,(C) 不信任扩展域,其具备:控制本机代码下载数据的下载的本机代码下载管理机构、操作系统、执行由上述基本域的本机代码下载管理机构判断为不能信任的、已下载的应用程序(称为“不信任应用程序”),将由上述基本域的本机代码下载管理机

构判断不能信任、已下载的设备驱动程序（称为“无信任驱动程序”）安装到上述操作系统中，由上述设备驱动程序访问事先准备的许可的外部装置，执行不信任追加处理，上述基本域、上述信任扩展域、上述不信任扩展域分别被安装在上述第 1 类～第 3 类处理器中。

[0042] 本发明另一方式的方法，包含：自上述基本域的外部装置输入下载数据时，将上述下载数据识别为下载应用程序时，上述基本域的上述本机代码下载管理机构，检测上述下载应用程序的证书的步骤；和上述检查的结果，判断为正确的证书时，将上述下载应用程序，将下载数据发送到上述信任扩展域的上述本机代码下载执行机构的步骤。

[0043] 在本发明的方法中，自上述基本域的外部装置输入下载数据时，也可以包含：在将上述下载数据识别为下载驱动程序时，上述本机代码下载管理机构，检查下载驱动程序的证书的步骤；上述检查的结果判断为正确的证书时，将下载驱动程序发送到上述信任扩展域的上述本机代码下载管理机构的步骤；和上述信任扩展域的上述本机代码下载执行机构将上述下载驱动程序安装到上述信任扩展域的操作系统中的步骤。

[0044] 本发明的方法中，自上述基本域的外部装置输入下载数据时，也可以包含：在将上述下载数据识别为下载应用程序时，上述基本域的上述本机代码下载管理机构，检查下载应用程序的证书的步骤；上述检查结果为没有证书或证书的内容不正确时，通过上述信任扩展域的上述本机代码下载执行机构，将下载数据发送到上述不信任扩展域的上述本机代码下载执行机构中的步骤。

[0045] 本发明的方法中，自上述基本域的外部装置输入下载数据时，也可以包含：在将上述下载数据识别为下载驱动程序时，上述基本域的上述本机代码下载执行机构检查上述下载驱动程序的证书的步骤；上述检查的结果为没有证书或证书的内容不正确时，通过上述信任扩展域的上述本机代码下载执行机构，将下载驱动程序发送到上述不信任扩展域的上述本机代码下载执行机构的步骤；和上述不信任扩展域的上述本机代码下载管理机构将上述下载驱动程序安装到上述不信任扩展域的操作系统中的步骤。

[0046] 本发明的方法中，也可以包括：在上述信任扩展域中预先设置基本功能程序库，该基本功能程序库作为程序库包括对上述基本域的基本软件环境的基本功能发布请求的处理群，接收下载到上述信任扩展域的应用程序的请求，上述基本功能程序库，使用上述应用程序的证书，将请求发送到上述基本域的上述本机代码下载管理机构中的步骤；上述基本域的上述本机代码下载管理机构，确认从上述信任扩展域接收的请求是否正确（是否为与应用程序的证书相对应的程序），上述请求正确时，向上述基本软件环境的基本功能请求处理的步骤。上述基本域的上述基本功能也可以包含：处理请求，将处理结束通知上述基本域的上述本机代码下载管理机构的步骤；和上述基本域的上述本机代码下载管理机构，将结束通知给上述信任扩展域的基本功能程序库，对上述应用程序处理通知结束的步骤

[0047] 本发明中的方法中，也可以具备：在上述信任扩展域中预先设置基本功能程序库，该基本功能程序库作为程序库作为程序库包括对上述基本域的基本软件环境的基本功能发布请求的处理群，根据下载到上述不信任扩展域中的应用程序，将数据发送到上述信任扩展域的应用程序的步骤；上述信任扩展域的上述应用程序，对上述基本功能程序库，发布处理请求的步骤，该处理请求为包含来自上述不信任扩展域的下载应用程序的数据的请求的处理请求；接收来自上述信任扩展域的请求，上述基本功能程序库，将请求发送到上述基本域的上述本机代码下载管理机构的步骤；上述基本域的上述本机代码下载管理机构确认

接收的请求是否正确（是否为与应用程序的证书对应的程序）的步骤；确认的结果为上述请求正确时，请求用户确认，上述用户的确认结果为允许时，向上述基本软件环境的基本功能请求处理的步骤；另一方面，上述用户的确认结果为不允许时，上述本机代码下载管理机构，通知上述基本功能程序库不允许的步骤。

[0048] 本发明中，基本功能也可以包含：上述用户的确认结果为允许时，处理请求，将处理结束通知上述基本域的上述本机代码下载管理机构的步骤；上述基本域的上述本机代码下载管理机构将结束通知上述信任扩展域的基本功能程序库的步骤；将处理结束通知上述下载应用程序的步骤；上述下载应用程序，将处理结束通知上述不信任扩展域的上述下载应用程序的步骤，和另一方面，上述用户的确认结果为不允许时，从基本程序库向上述不信任扩展域的下载应用程序通知不允许的步骤。

[0049] 本发明中的信息处理装置具备多个处理器，上述多个处理器构成第 1 域和形成与上述第 1 域不同的第 2 域的处理器，

[0050] 上述第 2 域，由具有至少 1 以上进行比属于上述第 1 域的处理器执行的处理可靠性低的处理的处理器构成，具备：

[0051] 处理器间通信机构，其控制上述第 1 域和上述第 2 域处理器之间的通信；和

[0052] 访问控制机构，其根据上述第 2 域中执行的处理的可靠性限制由属于上述第 2 域的处理器对属于上述第 1 域的存储器和 / 或者输入输出装置的访问。

[0053] 本发明的信息处理装置中，上述访问控制机构具备：

[0054] 存储允许访问数据的机构；和

[0055] 访问允许机构，其监视属于上述第 2 域的处理器对上述存储器和 / 或者上述输入输出装置的访问，参照上述允许访问数据，判断是否允许进行上述访问。

[0056] 本发明的信息处理装置中，上述访问控制机构也可以具有更新上述允许访问数据的允许访问数据更新机构。

[0057] 本发明的信息处理装置中，上述访问控制机构也可以具有：访问监视机构，其获得属于上述第 2 域的处理器的访问信息；和存储上述访问信息的学习机构。

[0058] 本发明的信息处理装置中，上述处理器间通信机构也可以具备中断控制信息处理装置，该中断控制信息处理装置接收来自信息发送侧的处理器器的中断请求，对上述信息的接收侧的处理器发布中断。

[0059] 本发明的便携信息终端具备多个处理器，上述多个处理器构成第 1 域和形成与上述第 1 域不同的第 2 域的处理器，

[0060] 上述第 2 域由具有至少 1 个以上、进行属于上述第 1 域的处理器执行的处理可靠性低的处理的处理器构成，

[0061] 具备：处理器间通信机构，其控制上述第 1 域和上述第 2 域的处理器之间的通信；

[0062] 访问控制机构，其根据上述第 2 域中执行的处理的可靠性，限制由属于上述第 2 域的处理器对属于上述第 1 域的存储器和 / 或者输入输出装置的访问。

[0063] 通过本发明，多个处理器，构成与处理的安全对应的域，通过处理器间通信机构进行域间的处理器的通信，具备访问控制机构，其对低安全域侧的处理器对高安全域侧的存储器和输入输出装置的访问进行控制，通过下载的设备驱动程序、应用程序在低安全域侧执行，来确保安全性。

[0064] 另外,通过本发明,高安全和低安全域中的处理,由各域的处理单元进行并行处理,由此,可以实现高速处理,并且,也可以实现高安全和低安全域处理单元间的同步,协作处理。

附图说明:

- [0065] 图 1 是表示本发明的一个实施例的硬件构成的图。
- [0066] 图 2 是表示本发明的一个实施例的处理单元间通信机构构成的图。
- [0067] 图 3 是用于说明本发明的一个实施例的处理单元间通信机构动作的图。
- [0068] 图 4 是表示本发明的一个实施例的访问控制机构构成的图。
- [0069] 图 5 是表示本发明的一个实施例的访问控制机构的允许访问数据例子的图。
- [0070] 图 6 是说明本发明的一个实施例的访问控制机构动作的图。
- [0071] 图 7 是表示本发明另一实施例的硬件构成的图。
- [0072] 图 8 是表示本发明再另一实施例的硬件构成的图。
- [0073] 图 9 是表示本发明的一个实施例的软件构成的图。
- [0074] 图 10 是用于说明本发明的一个实施例的动作的图。
- [0075] 图 11 是用于说明本发明的一个实施例的动作的图。
- [0076] 图 12 是用于说明本发明的一个实施例的动作的图。
- [0077] 图 13 是用于说明本发明的一个实施例的动作的图。
- [0078] 图 14 是用于说明本发明的一个实施例的动作的图。
- [0079] 图 15 是用于说明本发明的一个实施例的动作的图。
- [0080] 图 16 是用于说明本发明的一个实施例的动作的图。
- [0081] 图 17 是用于说明本发明的一个实施例的动作的图。
- [0082] 图 18 是表示本发明其他不同的实施例的构成的图。
- [0083] 图 19 是用于说明本发明其他不同的实施例的动作的图。
- [0084] 图 20 是表示本发明的一个实施例的变形例的图。
- [0085] 图 21 是表示现有的系统构成的一个例子的图。
- [0086] 图 22 是表示现有的系统构成的不同的例子的图。
- [0087] 图 23 是表示现有的系统构成的不同的例子图。
- [0088] 图 24 是表示现有的系统构成其他不同的例子图。
- [0089] 图 25 是表示本发明的一个实施例中的可靠性的一个例子的图。
- [0090] 图 26 是表示本发明的一个实施例中的可靠性的一个例子的图。
- [0091] 图 27 是表示本发明的一个实施例中的可靠性的一个例子的图。
- [0092] 图 28 是表示本发明的一个实施例中的可靠性的一个例子的图。
- [0093] 图中:10、10A、10B、10C-CPU,11-CPU,12-安全模式,13-非安全模式,14-内存管理单元,15-分离机构,20、20A、20B、20C-软件,21,21A,21B,21C-OS,22-基本处理,23,23B、23C-追加处理,24-虚拟机,25-证书,30-访问控制机构,31-访问允许机构,32-允许访问数据,40-处理单元间通信机构,41-中断控制装置,410~41n-CPU#0~CPU#n用中断控制装置,42-共享存储器,420~42n-CPU#0~CPU#n用通信区域,50,50A,50B,50C-存储器,60,60A,60B,60C-输入输出装置(I/O),70A-基本侧总线,70B-追加侧总线,100A-基本域,100B-Trusted 扩展域,100C-Untrusted 扩展域,101A,101B,101C-OS,102A-外部装

置,102A' - 虚拟外部装置,102B,102C- 许可的外部装置,102B',102C' - 许可的虚拟外部装置,103- 专用文件系统,103' - 虚拟专用文件系统,104A- 本机代码下载管理功能,104B,104C- 本机代码下载执行功能,105- 安全策略数据库,110- 基本软件环境,111- 基本应用程序,112- 基本功能,113- 基本功能程序库,120A,120B,120C- 下载应用程序,121B,121C- 下载驱动程序,200A,200B,200C- 虚拟 CPU,210A,210B,210C- 虚拟机监视器,411- 中断指示部,412- 中断状态保持部,413- 中断取消部,421- 通信指令,422- 排他控制区域。

具体实施方式

[0094] 对本具体实施方式进行说明。本发明,在其最佳的一个实施方式中,在具备多个 CPU 的多 CPU 构成的信息处理装置中,将多个 CPU,根据执行的程序(处理)的可靠性,划分为多个域(例如基本域,信任域,不信任域等),各域包含 1 个或者多个 CPU,通过处理器间通信机构(例如图 1 的 40)进行不同的域间的 CPU 的通信的同时,属于执行追加处理等低安全处理的域的 CPU,对执行高安全处理的域的存储器和输入输出装置进行访问时,该访问请求,通过访问控制机构(例如图 1 的 30),判断访问的许可/非许可,只进行许可的访问。

[0095] 在本说明书中,“可靠性”是指,根据表示授予每个处理的安全级别的电子证书,根据某安全策略,对每个安全等级设定的。

[0096] 例如,对每个授予数字签名的处理,根据某安全策略设定安全等级。例如,图 25 所示,对

[0097] 等级 A:需要密码,

[0098] 等级 B:不进行 2 次确认,

[0099] 等级 C:对每个执行进行确认,

[0100] 等级 D:对每个访问进行确认,

[0101] 这样的情况,对适于执行的功能的域授予安全等级。

[0102] 例如,也可以

[0103] 对基本域,配置等级 A,

[0104] 对信任扩展域,配置等级 B,

[0105] 对不信任域,配置等级 C,

[0106] 对 1 个域,只配置同种的安全等级,但并不局限于这样的构成。即,也可以 1 个域包含多种安全等级。作为一个例子,图 25 所示,

[0107] 基本域,根据执行的功能的重要度,可以配置等级 A 以上,等级 B 以上,信任扩展域,也可以根据执行的功能,配置等级 B 以上,等级 C 以上这样的配置。

[0108] 既可以进行这样的设定,也可以根据什么样的证书或什么样的安全策略进行设定,可以根据执行的功能或域数目任意地设定。

[0109] 通过这样构成的本发明的一个实施方式,将下载的追加处理(包含设备驱动程序和应用程序),由与所谓高安全域硬件上不同构成的低安全域侧的 CPU 执行,确保了高安全域的安全性。

[0110] 本说明书中,“下载”,不仅是为便携式电话的载波而准备的数据通信网和一般的无线 LAN 网等,也包含以 SD 卡为代表的存储型媒体介质,经由以 USB 为代表的有线通信/介质这样的连接,向信息装置的下载。

[0111] 并且,通过本发明的一个实施方式,由不仅是由开关等分离控制高安全域和低安全域的 CPU,也可以通过相互通信的处理器间通信机构连接,一边保证了安全性,一边也可以保证高安全域和低安全域的 CPU 间的同步、协调动作。

[0112] 该处理器间通信机构(图 1 的 40),是作为从一个域的 CPU 向其他域的 CPU 进行数据(指令)交换的机构,是不对其他域的 CPU 进行直接的攻击等的结构。例如由于从低安全域侧 CPU 向高安全域的 CPU 侧大量地不断发送数据,产生高安全域的 CPU 性能劣化,缓冲溢出等,由处理器间通信机构进行抑止,该数据不会传递到高安全域的 CPU。

[0113] 另外,本发明的一个实施方式中,访问控制机构(图 1 的 30),对低安全域侧的 CPU 进行许可访问控制,只允许对事先许可的内存空间、输入输出装置等以事先许可的方式进行访问。由此,能够防止来自下载的追加处理的对高安全域的攻击。或者,访问控制机构,根据需要,通过进行范围、流量控制等,能够防止来自下载的追加处理对高安全域的各种攻击。以下,根据实施例进行说明。

[0114] 【实施例】

[0115] 图 1 是表示本发明的一个实施例构成的图。参照图 1,其具备:执行由基本处理 22 和 OS21A 构成的软件 20A 的 CPU 群 10A;执行由追加处理 23 和对应追加处理的 OS21B 构成的软件 20B 的 CPU 群 10B;在 CPU 群 10A、10B 间进行通信的处理器间通信机构 401、402;和控制由 CPU 群 10B 对存储器 50 和 / 或者输入输出装置(I/O)60 的访问的访问控制机构 30。并且,图 1,表示了 CPU 群 10A、CPU 群 10B 分别由多个(3 台)CPU 构成,当然,也可以各群都由 1 个 CPU 构成。另外,当然,CPU 群 10A、CPU 群 10B 中,各群的 CPU 的台数也可以不相等。以下将 CPU 群 10A、CPU 群 10B 只简称为 CPU10A, CPU10B。本实施例中,下载的追加处理 23 由二进制形式的本机代码构成。并且,也可以编译处理(汇编处理)下载的源程序作为二进制形式的。

[0116] 通过本实施例,分开具备执行追加处理 23 的 CPU10B,执行基本处理 22 的 CPU10A, CPU10A, 10B 是可以独立地动作的,既可以提高安全性,又可以高速执行,可以进行应用程序、设备驱动程序的执行。并且,当然也可以将执行基本处理 22 的 CPU10A 作为主导,执行追加处理 23 的 CPU10B 作为从属来构成,从属侧在主导的监督下动作的构成。此时,例如由 CPU10B 进行的追加处理 23 的执行,能够通过处理器间通信机构 402 从 CPU10A 接收指令来进行。

[0117] 处理器间通信机构 401, 402, 控制 CPU10A 和 CPU10B 间的数据的接收发送。由于 CPU10A, 10B 独立地配设,可以并行地执行各自的处理(程序),同时,也可以通过处理器间通信机构 401, 402, 进行 CPU10A 和 CPU10B 间的同步处理,协作(协调)处理。作为一个例子,是用户从显示装置的画面指示追加处理的执行时,通过处理器间通信机构 401, 从执行基本处理 22 的 CPU10A, 将追加处理 23 的起动请求发送到 CPU10B, 在 CPU10B 上执行追加处理 23, 执行结果, 通过处理器间通信机构 402, 从 CPU10B 发送到 CPU10A, 构成基本处理 22 的画面控制例行程序等, 向用户提示反映追加处理 23 的执行结果的信息的情况。

[0118] 本实施例中,由 CPU10B 执行追加处理 23 时,进行对存储器 50、输入输出装置(I/O)60 的访问请求时,由访问控制机构 30 进行与该访问相关许可的控制,只有被许可的访问请求对存储器 50、输入输出装置(I/O)60 才能执行。并且,在 CPU10B 中,在 OS21B 上执行追加处理 23,发布来自追加处理 23 的对基本处理 22 或者 OS21A 的处理请求时,该请求,通过

处理器间通信机构 401 通知 CPU10A。即,追加处理 23 不能直接操作基本处理 22。例如,有恶意的追加处理 23,即使对 CPU10A 频繁发布请求,增加负荷,使 CPU10A 侧的基本处理的执行性能显著降低,处理器间通信机构 401,通过控制以使这样的请求不传递到 CPU10A 侧,实现对来自上述攻击的防护,确保安全性。

[0119] 并且,在图 1 所示的例子中,处理器间通信机构 401 控制从 CPU10B 向 CPU10A 的信息转送,处理器间通信机构 402 控制从 CPU10A 向 CPU10B 的信息转送。或者,当然也可以由一台处理器间通信装置进行双向数据的接收。在本实施例中,在执行基本处理 22 的多个 CPU10A 之间需要进行 CPU 间的通信时,不必使用处理器间通信机构 40,而进行 CPU 间的通信。另外,对于执行追加处理 23 的多个 CPU10B 也一样。但是,如后面所述,在构成 CPU 群 10B 的多个 CPU 中的几个动态地切换作为 CPU 群 10A 的要素时,CPU 群 10B,逻辑上属于 CPU 群 10A,但 CPU 间的通信也可以通过处理器间通信机构 40 来进行。

[0120] 通过本实施例,作为追加处理 23,可以进行应用程序和设备驱动程序的下载、安装、执行。追加的设备驱动程序,被安装到 OS21B 中,在 CPU10B 上执行,对输入输出装置 60 的访问控制在访问控制机构 30 的监视下执行。

[0121] 并且,在便携式电话机, PDA 等便携型信息通信装置中,通常,图 1 中的基本处理 22, OS21A 被存储在图中没有表示的可改写的非易失性存储器 (EEPROM; Electrically Programmable and Erasable ROM), CPU10A,从 EEPROM 读取命令代码并解码执行。同样,追加处理 23、OS21B 都存储在与 CPU10A 用不同的 EEPROM 中,CPU10B 从 EEPROM 读取命令代码并解码执行。即,容纳执行基本处理 22 和追加处理 23 的各自的 OS21A、21B 的存储器,在基本处理侧和追加处理侧,硬件上被分离。并且,基本处理、OS 等命令代码,是执行存储在 EEPROM 中的代码,但是通过由 CPU10A、10B 执行的程序,初始化、参照和更新的表格等数据,是在各自的 OS 起动时等,在由 DRAM (Dynamic Random Access Memory) 构成的存储器 50 中被展开的。并且,对于 CPU10B,由访问控制机构 30 管理读 / 写内存区域,限制由 CPU10A 对参照的内存区域的访问。当然,在与便携型信息通信终端不同的一般信息处理装置中同样,也可以分别具备加载基本处理 22、OS21A 由 CPU10A 读取命令代码的存储器;和加载追加处理 23、OS21B 由 CPU10B 读取命令代码的存储器。或者,在一般的信息处理装置中,在存储器 50 中,也可以分离设置加载基本处理 22、OS21A 的区域和加载追加处理 23、OS21B 的区域,由访问控制机构 30 管理对 CPU10B 的存储器 50 的读 / 写访问。此时,对于只有 CPU10A、CPU10B 参照的代码,存储在共通的内存区域,也可以由访问控制机构 30 控制访问,以允许该 CPU10B 只读共通的内存区域。

[0122] 另外,在便携型信息处理装置中,搭载的电池余量变少时,通过强制关闭执行基本处理的 CPU 以外的 CPU 和优先关闭根据执行的处理的可靠性执行可靠性更低的处理的 CPU,可以实现电池余量的节约。这通过例如,根据由检查电池余量的机构,和通知检测结果的机构得到的与电池余量相关的信息,在进行基本处理的 CPU 上进行判断,执行关闭这样的处理能够实现。

[0123] 此外,由于便携型信息处理装置中的资源,例如与外部的通信带宽或非易失性存储器容量等被进一步限制,根据可靠性,也可以变更确保资源的相对比例。这可以通过例如,在进行基本处理的 CPU 中,进行

[0124] • 执行的处理的可靠性高时,允许优先确保资源,

[0125] • 执行的处理的可靠性低时,对资源加以限制等的判断来实现。

[0126] 图 2 是表示本发明的一个实施例中的处理器间通信机构的硬件构成的一个例子的图。参照图 2,由 1 台配置在左右两侧的 CPU(执行基本处理的 CPU 和执行追加处理的 CPU)间的中断控制装置 41 和共享存储器 42,构成图 1 的处理器间通信机构 401、402 的整体。作为中断控制装置 41,具备 CPU#0、CPU#1、... CPU#n 用的 n 个中断控制装置 410 ~ 41n,各中断控制装置,具备:中断指示部 411、中断状态保持部 412 和中断取消部 413。另外,共享存储器 42 具备:CPU#0、CPU#1、... CPU#n 用的 n 个通信区域 420 ~ 42n,各通信区域具备:指令或者缓冲发送信息(数据,信息)的通信指令 421,和进行相互排他控制的排他控制区域 422。

[0127] 例如,假设由 CPU#0 和 CPU#1 这 2 个构成,CPU#1 用的中断控制装置 411 和 CPU#1 用的通信区域 421,构成从 CPU#0 向 CPU#1 的处理器间通信机构 401,CPU#0 用的中断控制装置 410 和 CPU#0 用的通信区域 420,构成从 CPU#1 向 CPU#0 的处理器间通信机构 402。

[0128] 中断控制装置 41 和共享存储器 42 采用总线连接 CPU#0、CPU#1、... CPU#n 的构成。另外,在共享存储器 42 的通信指令 421 不仅是发送数据自身,也可以设定存储发送数据缓冲指针(例如存储器 50 上缓冲区域的地址)。

[0129] 本实施例中,共享存储器 42 中的 CPU#i 的排他控制区域 422i,是为了在某 CPU 已经占用 CPU#i 的通信区域 42i 时,其他 CPU 不能使用 CPU#i 的通信区域 42i 的相互排他控制而设置的。即,CPU#i 的排他控制区域 422i 用于 mutex 等信号、标记等同步管理信息的存储。

[0130] 通过安装在共享存储器 42 中的相互排他控制机构,保证发送 CPU 和接收 CPU 间的数据的一致性(consistency)。

[0131] 另外,通过相互排他控制机构,发送侧 CPU,在排他控制区域 422 处于锁定状态时,不能增加对接收 CPU 的中断请求,由此,能够防止从发送 CPU 向接收 CPU 的频繁的数据发送等,不正当的中断发生。

[0132] 并且,作为排他控制区域 422,也可以作对指令的连接(入队指令),来自的指令的卸载(出队指令)的锁定管理。

[0133] 图 2 中,作为通过中断控制装置 41,允许向一个接收 CPU 的多重中断的构成时,在共享存储器 42 中,各 CPU 通信区域中的通信指令 421、排他控制区域 422 被设置多重。

[0134] 没有特殊地限制,共享存储器 42 也可以将图 1 的存储器 50 的规定内存区域作为共享存储器使用,也可以在存储器 50 之外,在处理器间通信机构 40 内设置。另外,图中没有表示,来自中断控制装置 410 ~ 41n 的中断请求(Interrupt Request)线,也可以作为并行地连接在接收 CPU 上的构成(中断根数增加),或者,作为以串联方式连接的构成。

[0135] 接收 CPU,如果接收来自中断控制装置 41 的中断请求,将其通知中断控制装置 41,中断控制装置 41,将中断装置编号(中断向量信息)转送到图中没有表示的数据线,接收 CPU,根据中断装置编号生成中断向量,通过调度器,起动由接收 CPU 执行的中断服务例程,中断服务例程,根据对应的共享存储器 42 的通信指令获得数据,释放(解锁)排他控制区域的 mutex 等信号,根据中断进行返回(Return From Interrupt)这样的一系列的控制。

[0136] 图 3 是用于说明图 2 所示的本实施例的处理器间通信机构的动作步骤的图,表示从 CPU#k 向 CPU#0 发送数据时的步骤。在图 3 中,箭头线旁的数字表示步骤编号。

[0137] 步骤 1:发送 CPU#k 锁定共享存储器 42 的 CPU#0 通信区域的排他控制区域。并且,表示共享存储器 42 的 CPU#0 通信区域的排他控制区域,通过其他 CPU 被锁定时,例如直到该锁定被解除之前待机。

[0138] 步骤 2:发送 CPU#k, 锁定共享存储器 42 的 CPU#0 通信区域的排他控制区域后,在共享存储器 42 的 CPU#0 用通信区域的通信指令中写入发送到接收 CPU#0 的数据。

[0139] 步骤 3:发送 CPU#k 向中断控制装置 41 的 CPU#0 用中断控制装置的中断指示部通知中断请求。

[0140] 步骤 4:CPU#0 用中断控制装置的中断指示部,更新 CPU#0 用中断控制装置的中断状态保持部,设定为“有中断请求”。

[0141] 步骤 5:CPU#0 用中断控制装置的中断指示部对接收 CPU#0 进行中断。

[0142] 步骤 6:接收 CPU#0 受理来自 CPU#0 用中断控制装置的中断指示部的中断,根据共享存储器 42 的 CPU#0 用通信区域的通信指令,取出数据。此时,在接收 CPU#0 中,进行由上述中断服务例程产生的处理。

[0143] 步骤 7:接收 CPU#0,根据共享存储器 42 的 CPU#0 用通信区域的通信指令,获得数据后,通知 CPU#0 用中断控制装置的中断取消部中断处理结束。

[0144] 步骤 8:接收来自接收 CPU#0 的中断处理结束通知的 CPU#0 用中断控制装置的中断取消部,更新 CPU#0 用中断控制装置的中断状态保持部。

[0145] 步骤 9:接收 CPU#0 解锁共享存储器 42 的 CPU#0 通信区域的排他控制区域。

[0146] 在本实施例中,在识别对特定的接收 CPU 的中断请求存在集中时,也可以进行抑制对接收 CPU 的中断请求等的流量控制、频带控制。即,在中断控制装置 41 内也可以具备 QoS 保证功能,限制从发送 CPU 侧对接收 CPU,连续、多次地增加中断请求。例如,与对接收 CPU 提交数据无关的中断请求,不作为排他控制的对象,能够多个连续地发行。因此,在接收 CPU 侧中断处理没有结束的状态中,在进行产生来自发送 CPU 侧的中断请求,中断控制装置 41 的中断状态保持部的“有中断请求”变为规定数量以上时,也可以进行控制,禁止来自后面的发送 CPU 侧的中断请求。通过这样的构成,能够防止例如通过发送 CPU 大量产生与向接收 CPU 提交数据无关的中断请求,降低接收 CPU 性能这类攻击。

[0147] 图 4 是表示图 1 所示的本发明的一个实施例的访问控制机构 30 的构成的图。参照图 4,该访问控制机构 30,具备:通过基本侧总线 70A,与执行基本处理(图 1 的 22)的 CPU10A 连接,通过追加侧总线 70B,与执行追加处理(图 1 的 23)的 CPU10B 连接的访问允许机构 31;和存储允许访问数据 32 的存储机构。

[0148] 允许访问数据 32 可以从 CPU10A 读出、写入。只允许从访问允许机构 31 读出。并且,允许访问数据 32,从 CPU10B 读出和写入都不允许。即,在允许访问数据 32 和 CPU10B 之间不存在数据总线。

[0149] 访问允许机构 31,根据转送到追加侧总线 70B 的地址信号线、控制信号线的、对存储器 50(参照图 1)的访问地址信号和控制信号(访问指令),判断访问的种类(读/写),参照允许访问数据 32 的信息,判断该访问是否适合。判断的结果为访问非法时,访问允许机构 31,不进行向基本侧总线 70A 的访问地址、控制信号(访问指令)的发送,由此,不能进行从 CPU10B 侧向基本侧总线 70A 的访问。此时,在向追加侧总线 70B 发送访问地址的 CPU10B 侧,根据来自总线错误,或者,针对读/写访问的存储器 50 等的无响应,知该访问失

败。

[0150] 访问允许机构 31, 在输入输出装置 (I/O) 60 为存储分配 I/O 时, 监视追加侧总线 70B, 检测访问地址为对应输入输出装置的地址, 在数据总线上, 检测了 I/O 指令 (读 / 写等) 时, 参照允许访问数据 32 的信息决定该访问是否合适。输入输出装置不是存储分配 I/O 时, 也解码转送到追加侧总线 70B 的输入输出装置的装置编号、I/O 指令, 参照允许访问数据 32 的信息, 决定是否允许访问。

[0151] 并且, 本实施例中, 访问控制机构 30, 也可以具备进行控制每单位时间内数据转送量的范围制约机构。作为一个例子, 访问控制机构 30, 具备测量监视在 CPU10B 访问动作中, 从 CPU10B 转送到追加侧总线 70B 的数据量的机构, 例如转送超过每单位时间事先规定的阈值的字节数的数据时, 也可以进行中止从 CPU10B 向 CPU10A 的数据转送的控制。此时也可以, 在 CPU10B 知道向 CPU10A 的数据转送识别并重审时, 访问控制机构 30 不会进行将来自 CPU10B 的数据转送到 CPU10A。或者, 访问控制机构 30 具备缓冲器, 将从 CPU10B 向追加侧总线 70B 转送的数据蓄积到缓冲器中, 控制转送到 CPU10A 的数据的流量来构成。

[0152] 图 5 是表示本发明的一个实施例中的允许访问数据 32 的一个例子的图。参照图 5, 允许访问数据, 执行追加处理的 CPU (连接在图 4 的追加侧总线上的 CPU), 由被允许访问的范围的始点地址和终点地址构成的许可范围地址, 以及许可的访问种类 (读、读 / 写和写的种类) 以表格形式存储。并且, 许可范围地址在不同的 CPU 可以重复。图 5 所示的例子中, 第 2 行的 CPU#2, #3 的许可范围地址为 0xC000000 ~ 0xF000000, 允许进行读出 / 写入 (R/W), 第 3 行的 CPU#3 的许可范围地址为 0xE000000 ~ 0xF000000, 与第 2 行重复。地址许可数据的数量, 随着表格的条目数量, 其数量越多, 越能够细致地进行访问控制。并且, 图 5 中, 为了说明, 例示了 R (允许读出), W (允许写入), R/W (允许读出 / 写入), R (允许读出) 为只允许读出不允许写入的信息, W 为允许写入 (也允许读出) 时不需要 R/W。另外, 不允许读出 (也不允许写入) 的地址范围, 不存储在地址许可数据 32 中。图 5 所示的例子中, 作为允许访问数据, 具有对每个被允许访问的 CPU, 地址范围和访问种类, 但是在允许访问数据中, 还设置不允许访问的信息作为访问种类, 对于执行追加处理的 CPU, 也可以存储不允许访问的地址范围。

[0153] 图 4 的访问允许机构 31, 接收来自追加侧 CPU 的访问请求 (地址、读写指令), 参照允许访问数据 32 的许可范围地址、访问种类, 为许可的访问时, 允许该访问。另一方面, 为不允许时, 不允许访问。在图 5 所示的例子中, 对 CPU#4 的情况, 采用始点地址 1000 ~ 终点地址 2000 (十六进制), 访问种类为读出 (R)。CPU#2、#3 的情况, 采用始点地址 0xC000000 ~ 终点地址 0xF000000 (十六进制), 访问种类为读出和写入 (R/W)。CPU#3 的情况, 始点地址 0xE000000 ~ 终点地址 0xF000000 (十六进制) 的访问种类为写入 (W)。

[0154] 图 6 是用于说明图 4 的访问控制机构 30 的动作的一个例子的图。图 6 中, 箭头线旁的编号表示步骤编号。

[0155] 步骤 1: 执行基本处理的 CPU10A, 在访问控制机构 30 的允许访问数据 32 中, 禁止执行所有的追加处理的 CPU10B 读出某些地址范围。

[0156] 步骤 2: CPU10B, 通过追加处理 23 的执行等, 发布对读出被禁止的地址范围的读出请求。

[0157] 步骤 3: 访问允许机构 31, 读出允许访问数据 32, 检查该访问请求是否适当。

[0158] 步骤 4:访问允许机构 31 向 CPU10B 返回错误。是由于该地址范围,对于来自 CPU10B 的读出禁止。

[0159] 步骤 5:CPU10B,发布对与上述地址范围不同范围的读出请求。

[0160] 步骤 6:访问允许机构 31,读出、检查允许访问数据 32。

[0161] 步骤 7:访问允许机构 31,允许 CPU10B 读出的访问请求,向基本侧总线 70A 发出读出请求。

[0162] 并且,本实施例中,对作为访问控制机构 30 的构成,具备访问允许机构 31 和允许访问数据 32,根据访问允许信息,进行访问控制的例子进行了说明,但是本发明不仅局限于这样的构成,也可以改变(翻转)访问允许的数据,具备访问拒绝数据和访问拒绝机构。此时,访问拒绝机构,来自执行追加处理的 CPU10B 的访问地址,在访问拒绝数据与被定义访问拒绝的地址范围一致时,进行拒绝访问的控制。

[0163] 作为本实施例的变形例,访问允许机构 31 也可以具备高速缓存。此时,用于访问判定的访问地址、允许访问数据被存储在高速缓存中,在下次以后的访问控制判定中,判断符合的访问地址(地址范围)的允许访问数据是否存在于高速缓存中,命中高速缓存时,实现访问判定的高速化。高速缓存中具备对应访问地址范围的标签地址、允许访问数据,具备判断追加侧总线 70B 的访问地址是否命中高速缓存的高速缓存命中判定电路。

[0164] 此外,作为本实施例的变形例,访问控制机构,如图 26 所示,也可以具备新允许访问数据 33 和允许访问数据更新机构 34。参照图 26,访问控制机构 30,除了图 4 所示的实施例之外,还具备与基本侧总线 70A 连接的允许访问数据更新机构 34,和存储新允许访问数据 33 的存储机构。对这 2 个机构的功能的详情进行说明。

[0165] 除了新允许访问数据 33,具有图 4 的允许访问数据 32 相同的特征之外,是只允许来自允许访问数据更新机构 34 的读出的存储机构。

[0166] 允许访问数据更新机构 34,根据来自经由基本侧总线 70A 的 CPU10A 的请求,将新允许访问数据 33 的内容以最小单位(atomic)覆盖新允许访问数据 34。

[0167] 并且,在本实施例中,也可以设置并不更新允许访问数据,而进行向新允许访问数据的切换的机构。

[0168] 通过这样的构成,由于可以由 CPU 以最小单位重写允许访问数据 32 的更新,可以动态地变更应该由访问控制机构保护的区域,应该限制的区域。

[0169] 另外,图 27 是表示本发明的一个实施例的访问控制机构 30 的不同的构成的图。参照图 27,该访问控制机构 30,除了如图 4 所示的实施例之外,还具备与追加侧总线 70B 连接的访问监视机构 35 和学习机构 36。对该机构的功能的详情进行说明。

[0170] 访问监视机构 35,与访问允许机构 31 一样,获得经由追加侧总线 70B 来自 CPU10B 的访问信息。

[0171] 学习机构 36,存储由上述访问监视机构 35 提供的访问信息。并且,根据访问信息,判断此参照是否适当。例如,计数对用户保护数据的参照次数,如果超过事先指定的阈值时,认定为异常情况,向访问监视机构 35 通知此事,根据其他规定的规则动态地变更允许访问数据 32。另外,也可以根据情况,通知与基本侧总线 70A 相连的 CPU10A,起动异常时的处理。

[0172] 通过这样的构成,由于通过根据实际参照的图案,将认为可靠性低的 CPU 的动作

作为履历信息蓄积,能够自主地限制,可以进行基于实际动作中的 CPU 的动作状况的更安全的执行控制。

[0173] 另外,作为访问控制机构的构成例,除了图 4 的构成以外,也可以具备上述说明过的所有新访问控制机构、访问允许更新机构、访问监视机构和学习机构。

[0174] 图 7 是表示本发明的不同的实施例的构成的图。参照图 7,本实施例,是除了图 1 的构成之外,又追加了 1 组追加处理侧软件和 OS、CPU。即,第 2 追加处理侧的 CPU10C,通过处理器间通信机构,与第 1 追加处理用 CPU10B 相互通信。另外,第 2 追加处理侧 CPU10C,通过第 2 访问控制机构 302,与基本侧总线 70A 连接。

[0175] 各访问控制机构 301,302 的设定,由执行基本处理 22 的 CPU10A 设定。即,执行基本处理 22 的 CPU10A,起到作为主导处理器的功能。由 CPU10A 对存储器 50 和输入输出装置 (I/O)60 进行集中的管理。

[0176] 执行第 2 追加处理 23C 的 CPU10C,通过处理器间通信机构 403,对执行第 1 追加处理 23B 的 CPU10B 进行通信(数据、指令的发送),执行第 1 追加处理 23B 的 CPU10B,通过处理器间通信机构 401,对执行基本处理 22 的 CPU10A 进行通信(数据、指令的发送)。另外,执行第 2 追加处理 23C 的 CPU10C,在第 2 访问控制机构 302 的监视下,对存储器 50、输入输出装置 (I/O)60 只进行被许可的访问,执行第 1 追加处理 23B 的 CPU10B,在第 1 访问控制机构 301 的监视下,对存储器 50、输入输出装置 (I/O)60 只进行被许可的访问,第 1 访问控制机构 301、第 2 访问控制机构 302 的允许访问数据的设定全都由 CPU10A 进行。通过这样的构成,进行集中的管理,另外,由处理器间通信机构 40,进行 CPU 间的处理的收发。本实施例中,也能够回避针对执行基本处理 22 的 CPU10A 的、来自追加处理 23B、23C 的直接攻击等。即,与上述实施例一样,追加处理 23B、23C 不能直接起动基本处理 22 或呼出子程序,基本处理 22 的起动请求,例如从 CPU10C 通过 CPU10B,通过处理器间通信机构传递到 CPU10A,在接收了的 CPU10A 中,是没有授予权限的 CPU 的请求时,不受理该请求(对于其详情,在后面所述的软件的实施例中进行详细描述)。这样,除了对追加处理侧 CPU 和基本处理侧 CPU 设置权限等级之外,通过处理器间通信机构 40 和访问控制机构 30 这样的硬件机构,能够回避基本处理等直接的攻击。本实施例中的处理器间通信机构 401 ~ 404,与图 2 所示的上述实施例构成一样,由于访问控制机构 301、302,也与图 4 所示的上述实施例的构成一样,其详细构成、动作的说明省略了。

[0177] 图 8 是本发明的不同实施例的构成图。参照图 8,本实施例,与图 7 所示的构成一样,是在图 1 的构成中进一步追加了追加处理侧 CPU10C 和访问控制机构 302。本实施例,与图 7 所示的上述实施例不同,对每个各组(域)CPU 群准备存储器和输入输出装置 (I/O)。第 2 追加处理 CPU10C,能够没有访问限制自由地访问许可的存储器 50C、输入输出装置 (I/O)60C。第 1 追加处理 CPU10B 能够没有访问限制地访问许可的存储器 50B、输入输出装置 (I/O)60B。

[0178] 来自第 2 追加处理侧 CPU10C 的、对基本处理侧存储器 50A、输入输出装置 (I/O)60A 的访问,由第 2 访问控制机构 302 和第 1 访问控制机构 301 两段结构,进行访问控制。

[0179] 来自第 1 追加处理侧 CPU10B 的、对基本处理侧存储器 50A、输入输出装置 (I/O)60A 的访问,由第 1 访问控制机构 301 判断是否允许访问。

[0180] 第 1 访问控制机构 301 的允许访问数据、第 2 访问控制机构 302 的允许访问数据,

由基本处理的 CPU10A 设定。第 2 访问控制机构 302 的允许访问数据也可以由第 1 追加处理的 CPU10B 设定。通过该实施例,通过采取将存储器、输入输出装置(I/O)分离为域单位,由处理器间通信机构 40 由多段连接 CPU 间的构成,能够提高来自追加处理产生的攻击的防护功能,确保了安全性。

[0181] 图 28 是在 2 以上芯片中应用图 1 所示的本发明的一个实施例的例子。参照图 28,除了排列多个本发明的一个实施例的 CPU10A、10B、10C、10D 和访问控制机构 301 的组合之外,还由访问控制机构 303 连接每个芯片。

[0182] 通过设置某一芯片内中的一部分 CPU 作为基本处理执行用,通过一芯片内的访问控制机构既能进行访问限制,也可以设置各芯片内至少一部分 CPU 作为基本处理执行用。

[0183] 另外,通过跨不同的芯片构成域,也可以由各芯片间的访问控制机构控制执行。

[0184] 无论在哪种情况下,通过适当的访问控制机构的设定,在多个芯片间也可以进行本发明中的执行控制。

[0185] 在上述实施例中,主要对本发明的硬件构成进行了说明,以下对本发明的软件构成进行说明。

[0186] 图 9 是表示实施本发明的软件构成的一个例子的图,具备基本域、Trusted(信赖)扩展域和 Untrusted(不信任)扩展域。作为图 9 的硬件构成,能够使用具备 3 个群 CPU 的图 8 的构成等。此时,作为执行基本处理的执行环境的基本域能够与图 8 的软件 20A 和 OS21A 对应,Trusted 扩展域能够与图 8 的软件 20B 和 OS21B 对应,Untrusted 扩展域能够与图 8 的软件 20C 和 OS21 对应。

[0187] 参照图 9,基本域 100A,具备基本应用程序(称为“基本应用程序”)111;包含基本功能 112 的基本软件 110;OS101A;专用文件系统 103;和外部装置 102A,具备本机代码下载管理功能 104A 和安全策略数据库 105。不被特别地限制,但是基本功能 112,在例如,本实施例的信息通信装置为便携型信息通信终端时,是实现呼叫请求,来电处理等呼叫处理,互联网访问、画面处理等便携型信息通信终端的基本功能的处理,与图 1 的基本处理 22 相对应。基本应用程序 111,呼出基本功能 112 进行处理,基本功能 112,通过 OS 进行对文件系统、外部装置的访问。外部装置包含:无线通信接口等通信接口,显示装置的接口,键盘,指针装置等输入接口,SD(Secure Digital)存储卡接口,声音接口等。

[0188] Trusted 扩展域 100B 具备本机代码下载执行功能 104B、下载应用程序(称为“下载应用程序”)120B、基本功能程序库(ラツパー)113、OS101B 和许可的外部装置 102B。

[0189] OS101B 包含带有证书的下载驱动程序 121B。带有证书驱动程序 121B 进行许可的外部装置 102B 的输入输出控制。

[0190] Untrusted 扩展域 100C 具备本机代码下载执行功能 104C、下载应用程序 120C、OS101C 和许可的外部装置 102C。安装到 OS101C 中的下载驱动程序 121C 进行许可的外部装置 102C 的输入输出控制。

[0191] 对于由基本域 100A 外部装置 102A 输入的下载文件,本机代码下载管理功能 104A,通过参照安全策略数据库 105 的内容,将能够信任的(带有能够信任的电子证书)本机代码的应用程序,转送到 Trusted 扩展域 100B,能够进行信任的(带有能够信任的电子证书)本机代码的下载驱动程序 121B 向 OS101B 的安装。

[0192] 另外,本机代码下载管理功能 104A,将不能信任(例如没有电子证书,或证书的内

容不正确时等)应用程序,经由 Trusted 扩展域 100B,向 Untrusted 扩展域 100C 转送,进行不能信任(没有证书)下载驱动程序向 Untrusted 扩展域的 OS101C 的安装。

[0193] 由 Trusted 扩展域 100B,允许基本功能 112 的呼叫,但不允许来自 Untrusted 扩展域 100C 的基本功能 112 的呼叫。但是,Untrusted 扩展域 100C 和 Trusted 扩展域 100B 可以协调工作。

[0194] 在能够信任的域中动作的应用程序,对于来自不能信任域的数据,只在有用户的确认(OK)时,向基本功能 112 提交。没有用户的确认的来自不能信任域的数据,不向基本功能 112 提交。并且,不能从能够信任的扩展域 100B,直接地向基本域 100A 的基本功能 112,发布处理请求。

[0195] 图 10 是用于说明图 9 所示的本发明的一个实施例的动作的图,是表示基本应用程序的执行的图。在图 10 中,各箭头线带有的编号表示经该线转送信息的步骤编号。

[0196] 步骤 1:基本域 100A 的基本应用程序 111,向基本功能 112 发布处理请求(例如,地址本的追加等)。

[0197] 步骤 2:基本功能 112,使用 OS101A,处理该请求。

[0198] 步骤 3:基本功能 112,通知基本应用程序 111 请求是否成功。

[0199] 图 11 是用于说明图 9 所示的本发明的一个实施例的动作的图,是表示执行信任应用程序的下载的情况的图。图 11 中,各箭头线带有的编号表示经该线转送信息的步骤编号。

[0200] 步骤 1:下载数据从基本域 100A 上的外部装置 102A(网络或者 SD 存储卡等)送到 OS101A。

[0201] 步骤 2:下载数据,由基本功能 112,根据属性信息等信息,识别为追加应用程序(下载应用程序)。

[0202] 步骤 3:基本功能 112,将追加应用程序提交给本机代码下载管理功能 104A,本机代码下载管理功能 104A 参照安全策略数据库 105,检测追加应用程序附带的电子证书。如上所述,例如电子证书中存储着公钥或数字签名(由密钥加密被证明的机关或公钥等的信息),本机代码下载管理功能 104A 进行证书认证时,用公钥解读数字签名部分,确定与证书的数据内容是否一致,一致时,判断可以信任证书数据。此外,通过附带由应用程序的概要构成的数字签名,能够检查下载的应用程序有没有被篡改了。

[0203] 步骤 4:本机代码下载管理功能 104A,将下载信息,与电子证书同时,保存到安全策略数据库 105 中。

[0204] 步骤 5:基本域 100A 的本机代码下载管理功能 104A,电子证书的检查结果,正确时,将下载应用程序发送到 Trusted 扩展域 100B 的本机代码下载执行功能 104B,请求执行。由基本域 100A 的本机代码下载管理功能 104A,使用图 7 或者图 8 的处理器间通信机构 40 向 Trusted 扩展域 100B 的本机代码下载执行功能 104B 发送数据。

[0205] 步骤 6:Trusted 扩展域 100B 的本机代码下载执行功能 104B,控制以执行接收的下载应用程序。

[0206] 步骤 7:下载应用程序在 Trusted 扩展域上被执行。

[0207] 图 12 是用于说明图 9 所示的本发明的一个实施例的动作的图,表示信任驱动程序的下载执行的图。信任驱动程序是指,例如下载的驱动程序中附加的电子证书的对照结果

正确的驱动程序。在图 12 中,各箭头线中自带的编号,表示经该线转送信息的步骤编号。

[0208] 步骤 1:下载数据从基本域 100A 上的外部装置 102A(网络或者 SD 卡等)送到 OS101A。

[0209] 步骤 2:由基本功能 112 根据属性信息、自动安装信息等,下载数据,识别为追加设备驱动程序(下载驱动程序)。

[0210] 步骤 3:基本功能 112,将接收的驱动程序,提交给本机代码下载管理功能 104A。本机代码下载管理功能 104A,参照安全策略数据库 105,检查下载数据中附带的电子证书。

[0211] 步骤 4:本机代码下载管理功能 104A,将下载信息与电子证书一起保存到安全策略数据库 105 中。

[0212] 步骤 5:本机代码下载管理功能 104A,对 Trusted 扩展域的本机代码下载执行功能 104B,发送下载驱动程序,请求安装的执行。从基本域 100A 的本机代码下载管理功能 104A,使用图 7 或者图 8 的处理器间通信机构 40,向 Trusted 扩展域 100B 的本机代码下载执行功能 104B 发送数据。

[0213] 步骤 6:Trusted 扩展域的本机代码下载执行功能 104B,自动安装接收的下载驱动程序。没有特别的限制,在该实施例中,下载驱动程序也可以是在安装后,重新起动 CPU,安装到 OS101B 的某个区域的驻留型驱动程序。

[0214] 步骤 7:Trusted 扩展域的 OS101B,表示是否通知已经执行完成的应用程序,安装了下载驱动程序。

[0215] 步骤 8:Trusted 扩展域中,已经执行完成的应用程序 120B 参照安装的下载驱动程序 121B。

[0216] 步骤 9:被安装到 Trusted 扩展域的 OS101B 的被加载的下载驱动程序 121B 访问许可的外部装置 102B。

[0217] 步骤 10:下载驱动程序 121B,将来自外部装置 102B 的数据返回到下载应用程序 120B。

[0218] 图 13 是用于说明图 9 所示的本发明的一个实施例的动作用的图,是表示 Trusted 扩展域的信任应用程序(下载应用程序),使用基本域的基本功能情况的动作用的图。在图 13 中,各箭头线自带的编号表示经该线转送信息的步骤编号。

[0219] 步骤 1:在 Trusted 扩展域 100B 中,下载应用程序 120B,向基本功能程序库 113 请求基本域 100A 的基本功能 112 的处理。基本功能程序库 113 是收集用于执行基本域 100A 的基本功能 112 的处理的例行程序的程序库,由下载应用程序 120B 起动。

[0220] 步骤 2:Trusted 扩展域 100B 的基本功能程序库 113,使用下载应用程序 120B 保有的电子证书的密钥(公钥等),加密请求,将加密的请求向基本域 100A 的本机代码下载管理功能 104A 发送。从 Trusted 扩展域 100B 的基本功能程序库 113 向基本域 100A 的本机代码下载管理功能 104A 的请求发送,通过图 7 或者图 8 的处理器间通信机构 40 进行。

[0221] 步骤 3:基本域 100A 的本机代码下载管理功能 104A,解密接收的请求,利用电子证书,进行该请求是否符合请求发送目的地等的检查。并且,在该例子中,使用请求的加密和解密检查请求,只要是使应用程序和电子证书相对应的方法,当然可以使用任意的的方法。

[0222] 步骤 4:基本域 100A 的本机代码下载管理功能 104A,请求的检查结果如果是 OK,向基本功能 112 委托请求。

[0223] 步骤 5:基本域 100A 的基本功能 112,处理从本机代码下载管理功能 104A 接收的该请求,处理结束后,向基本域 100A 的本机代码下载管理功能 104A,通知处理结束。

[0224] 步骤 6:基本域 100A 的本机代码下载管理功能 104A,向 Trusted 扩展域 100B 的基本功能程序库 113,通知处理结束。从基本域 100A 的本机代码下载管理功能 104A,通过图 7 或者图 8 处理器间通信机构 40,向 Trusted 扩展域 100B 的基本功能程序库 113 发送通知。

[0225] 步骤 7:Trusted 扩展域的基本功能程序库 113,向下载应用程序 120B 通知处理结束,作为对请求的响应。

[0226] 图 14 是用于说明图 9 所示的本发明的一个实施例的动作用的图,是表示 Untrusted 扩展域的不信任应用程序的下载执行步骤的图。在图 14 中,各箭头线带有的编号,表示经该线转送信息的步骤编号。

[0227] 步骤 1:下载数据从基本域 100A 上的外部装置 102A(网络或者 SD 卡等)送达 OS101A。

[0228] 步骤 2:在基本域 100A 的基本功能 112 中,分析属性信息等,将下载数据识别为应用程序(下载应用程序)。

[0229] 步骤 3:基本域 100A 的基本功能 112,将下载应用程序提交给本机代码下载管理功能 104A。在本机代码下载管理功能 104A 中,判断应用程序中是否附带电子证书,或者电子证书是否正确。

[0230] 步骤 4:基本域 100A 的本机代码下载管理功能 104A,在安全策略数据库 105 中保存下载信息。

[0231] 步骤 5:基本域 100A 的本机代码下载管理功能 104A,将下载的应用程序发送到 Trusted 扩展域的本机代码下载执行功能 104B。从基本域 100A 的本机代码下载管理功能 104A 向 Trusted 扩展域的本机代码下载执行功能 104B 的应用程序的发送,通过如图 7 或者图 8 所示的处理器间通信机构 40 进行。

[0232] 步骤 6:Trusted 扩展域 100B 的本机代码下载执行功能 104B,将应用程序发送到 Untrusted 扩展域 100C 的本机代码下载执行功能 104C,请求执行。从 Trusted 扩展域 100B 的本机代码下载执行功能 104B,通过图 7 或者图 8 所示的处理器间通信机构 40,向 Untrusted 扩展域 100C 的本机代码下载执行功能 104C 发送。

[0233] 步骤 7:Untrusted 扩展域的本机代码下载执行功能 104C,进行接收的下载应用程序 120C 的起动。

[0234] 步骤 8:下载应用程序 120C,在 Untrusted 扩展域 100C 中开始动作。此时,Untrusted 扩展域的下载应用程序 120C,在 Untrusted 扩展域的 OS101C 上动作,只允许对许可的外部装置 102 进行访问。

[0235] 图 15 是用于说明图 9 所示的本发明的一个实施例的动作用的图,是表示无信任驱动程序下载执行的情况的图。在图 15 中,各箭头线带有的编号表示经该线转送信息的步骤编号。

[0236] 步骤 1:从基本域 100A 上的外部装置 102A(网络或者 SD 卡等)将下载数据送达 OS101A。

[0237] 步骤 2:基本功能 112,由下载数据的到达被起动,解析属性信息、安装信息等下载数据,识别为设备驱动程序(下载驱动程序)。

[0238] 步骤3:基本功能112将下载驱动程序提交给本机代码下载管理功能104A,本机代码下载管理功能104A判断下载驱动程序中是否带有电子证书,或者,带有电子证书,但电子证书的内容是否正确。

[0239] 步骤4:基本域100A的本机代码下载管理功能104A,只将下载信息保存在安全策略数据库105中。

[0240] 步骤5:本机代码下载管理功能104A,将下载驱动程序发送到Trusted扩展域100B的本机代码下载执行功能104B。从本机代码下载管理功能104A,通过图7或者图8所示的处理器间通信机构40,向Trusted扩展域100B的本机代码下载执行功能104B发送下载驱动程序。

[0241] 步骤6:Trusted扩展域100B的本机代码下载执行功能104B,将接收的下载驱动程序,转送到Untrusted扩展域100C的本机代码下载执行功能104C。从Trusted扩展域100B的本机代码下载执行功能104B,通过如图7或者图8所示的处理器间通信机构40,向Untrusted扩展域100C的本机代码下载执行功能104C转送下载驱动程序。

[0242] 步骤7:Untrusted扩展域100C的本机代码下载执行功能104C,安装接收的下载驱动程序121C。

[0243] 步骤8:OS101C在画面上显示向已经执行完成的应用程序120C通知驱动程序121C被安装了(通知用户)。

[0244] 步骤9:在Untrusted扩展域100C中,已经执行完成的应用程序120C,参照安装的下驱动程序121C。

[0245] 步骤10:在Untrusted扩展域100C中,安装的下驱动程序121C,通过Untrusted扩展域的OS101C,访问许可的外部装置102C。

[0246] 步骤11:在Untrusted扩展域100C中,下载驱动程序121C,向下载应用程序120C,返回从外部装置102C获得的数据。

[0247] 图16是用于说明图9所示的本发明的一个实施例的动作用的图,是表示信任应用程序和不信任应用程序协作情况的图。在图16中,各箭头线带有的编号,表示经该线转送信息的步骤编号。

[0248] 步骤1:Untrusted扩展域100C上的下载应用程序120C,向Trusted扩展域100B上的下载应用程序120B发送数据。该数据的发送,通常,由图7或者图8的处理器间通信机构40进行。

[0249] 步骤2:Trusted扩展域100B上的下载应用程序120B,进行接收的数据对应的处理,向基本功能程序库113,请求包含与Untrusted扩展域协作的信息的基本功能处理。

[0250] 步骤3:Trusted扩展域100B上的基本功能程序库113,使用应用程序保有的电子证书,加密请求,向基本域100A上的本机代码下载管理功能104A发送。该请求的发送,通常,由图7或者图8的处理器间通信机构40进行。

[0251] 步骤4:基本域100A的本机代码下载管理功能104A,解密请求,利用存储在安全策略数据库105中的电子证书检查该请求的完整性。检查结果为请求正确时,本机代码下载管理功能104A,通过基本应用程序111,请求用户确认。基本应用程序111包含画面显示、输入的应用程序。并且,在该例子中,使用请求的加密和解密,检查应用程序和电子证书的对应,只要是能够使应用程序和电子证书对应的方法,当然可以使用任意的方

- [0252] 步骤 5 :作为来自用户的确认,如果输入“NO”。
- [0253] 步骤 6 :本机代码下载管理功能 104A,向 Trusted 扩展域 100B 的基本功能程序库 113 通知不许可。该不许可的通知,通常,由图 7 或者图 8 的处理器间通信机构 40 进行。
- [0254] 步骤 7 :基本功能程序库 113,向下载应用程序 120B 通知不许可。
- [0255] 步骤 8 :Trusted 扩展域 100B 上的下载应用程序 120B,向 Untrusted 扩展域 100C 上的下载应用程序 120C 通知不许可。该不许可的通知,通常,由图 7 或者图 8 的处理器间通信机构 40 进行。
- [0256] 图 17 是用于说明图 9 所示的本发明的一个实施例的动作用的图,是表示信任应用程序和不信任应用程序协作的图。在图 17 中,各箭头线带有的编号,表示经该线转送信息的步骤编号。
- [0257] 步骤 1 :Untrusted 扩展域 100C 上的下载应用程序 120C,向 Trusted 扩展域 100B 上的下载应用程序 120B 发送数据。该数据的发送,由图 7 或者图 8 等的处理器间通信机构进行。
- [0258] 步骤 2 :Trusted 扩展域 100B 上的下载应用程序 120B,进行由接收的数据产生的处理,向基本功能程序库 113 请求包含与 Untrusted 协作的信息的基本功能处理。
- [0259] 步骤 3 :Trusted 扩展域 100B 上的基本功能程序库 113,使用应用程序 120B 保有的电子证书,加密请求,并向基本域 100A 上的本机代码下载管理功能 104A 发送。该请求,通常,由图 7 或者图 8 的处理器间通信机构 40 进行。
- [0260] 步骤 4 :基本域 100A 的本机代码下载管理功能 104A,解密请求,利用存储在安全策略数据库 105 中的电子证书检查该请求的完整性。检查结果为请求正确时,本机代码下载管理功能 104A,通过基本应用程序 111 请求用户确认。并且,在该例子中,使用请求的加密和解密,检查应用程序和电子证书的对应,只要是使应用程序和电子证书相对应的方法,当然可以使用任意的的方法。
- [0261] 步骤 5 :此时,作为用户的确认,如果输入“Yes”。
- [0262] 步骤 6 :基本域 100A 的本机代码下载管理功能 104A,向基本功能 112 委托请求。
- [0263] 步骤 7 :基本功能 112,处理请求,向本机代码下载管理功能 104A 通知处理结束。
- [0264] 步骤 8 :基本域 100A 的本机代码下载管理功能 104A,向 Trusted 扩展域 100B 的基本功能程序库 113 通知结束。该结束通知,通常,由图 7 或者图 8 的处理器间通信机构 40 进行。
- [0265] 步骤 9 :Trusted 扩展域 100B 的基本功能程序库 113,向下载应用程序 120B 通知结束。
- [0266] 步骤 10 :Trusted 扩展域 100B 的下载应用程序 120B,向 Untrusted 扩展域 100C 的下载应用程序 120C 通知结束。该结束通知,通常,由图 7 或者图 8 的处理器间通信机构 40 进行。
- [0267] 图 18 是表示本发明的其他不同的实施例构成的图。在 OS 和 CPU 间具备虚拟机监视器(设置在 OS 之间,由 CPU 执行的软件层)。由此,虚拟 CPU、I/O、存储器资源。虚拟机监视器,在 OS 和 CPU 间,将虚拟硬件(例如虚拟输入输出装置)映射到实际的硬件装置上。对于每个基本域、Trusted 扩展域和 Untrusted 扩展域,OS 进行虚拟的专用文件系统、虚拟外部装置之间的输入输出(I/O)控制,在 OS 和 CPU 间,具备虚拟 CPU200A、200B、200C 和虚

拟机监视器 210A、210B、210C,将虚拟的专用文件系统 103' 和虚拟外部装置 102A'、102B'、102C' 映射到对应的实际文件系统、实际外部装置。

[0268] 通过本实施例,与图 8 的硬件构成和图 9 的软件构成不同,在本实施例中,例如对应基本域的虚拟 CPU 不是固定的,能够将 Trusted 扩展域等的 CPU,映射作为基本域的虚拟 CPU。并且,虚拟机监视器,在其实装中,不需要现有的 OS、应用程序、CPU 等修正等。通过本实施例,各域的 CPU 个数可变,构成虚拟 CPU。作为软件构成,基本域、Trusted 扩展域和 Untrusted 扩展域的构成,装置、文件系统除了是虚拟装置、虚拟文件系统之外,与图 9 所示的构成一样。

[0269] 图 19 是表示图 18 所示的实施例的处理步骤的一个例子的图。图 19 中,各箭头线带有的编号表示步骤编号。

[0270] 步骤 1:基本域 100A 的虚拟机监视器 210A,对 Trusted 扩展域 100B 上的虚拟机监视器 210B 请求 CPU 的转移。

[0271] 步骤 2:Trusted 扩展域 100B 上的虚拟机监视器 210B,减少虚拟 CPU 资源。

[0272] 步骤 3:Trusted 扩展域 100B 上的虚拟机监视器 210B,通知基本域 100A 上的 CPU 上的虚拟机监视器 210A 可以转移的 CPU。

[0273] 步骤 4:基本域 100A 上的虚拟机监视器 210A,进行访问控制机构等设定,增加虚拟 CPU 的数量。

[0274] 通过本实施例,能够使不同群的 CPU,象基本域的 CPU 那样动作。并且,由于应用程序的下载处理,与上述实施例的处理动作(图 10~图 18)相同,省略其说明。

[0275] 作为本实施例和变形例,也可以使虚拟机监视器,在安全模式下动作。通过这样,能够进一步提高安全性。

[0276] 在上述软件各实施例中,对于各域的 CPU 群作为多处理器动作时,用于保持高速缓存一致性的总线;为了虚拟多处理器的无效化,快速擦除存储 TLB(Translation Lookaside Buffer;设置在地址管理单元内的地址变换表)的全部条目的擦除操作等,由硬件协调动作的通道,全部以能够由基本域 100A 控制的方式构成。另外,如图 20 所示,也可以将各域的 CPU 群(例如图 1 的多 CPU 构成的 CPU 群 10A、10B),通过分离机构 15,作为多个能够分离的构成。由此,例如使某个域的 CPU 转移到其他域时的控制容易,还可以应对故障多处理器的分离(graceful degrading)等。

[0277] 并且,上述各实施例子中,以从网络等装置外部下载、执行本机代码的追加处理(应用程序、设备驱动程序)的信息通信终端装置为例进行了说明,但是,本发明并不限于这样的信息通信终端装置,可以应用程序与任意的信息通信装置。以上,根据上述实施例,对本发明进行了说明,但是,本发明并不是只限于上述实施例的构成,当然也包含在本发明范围内,只要是技术人员就可以得到的各种变形、修正。

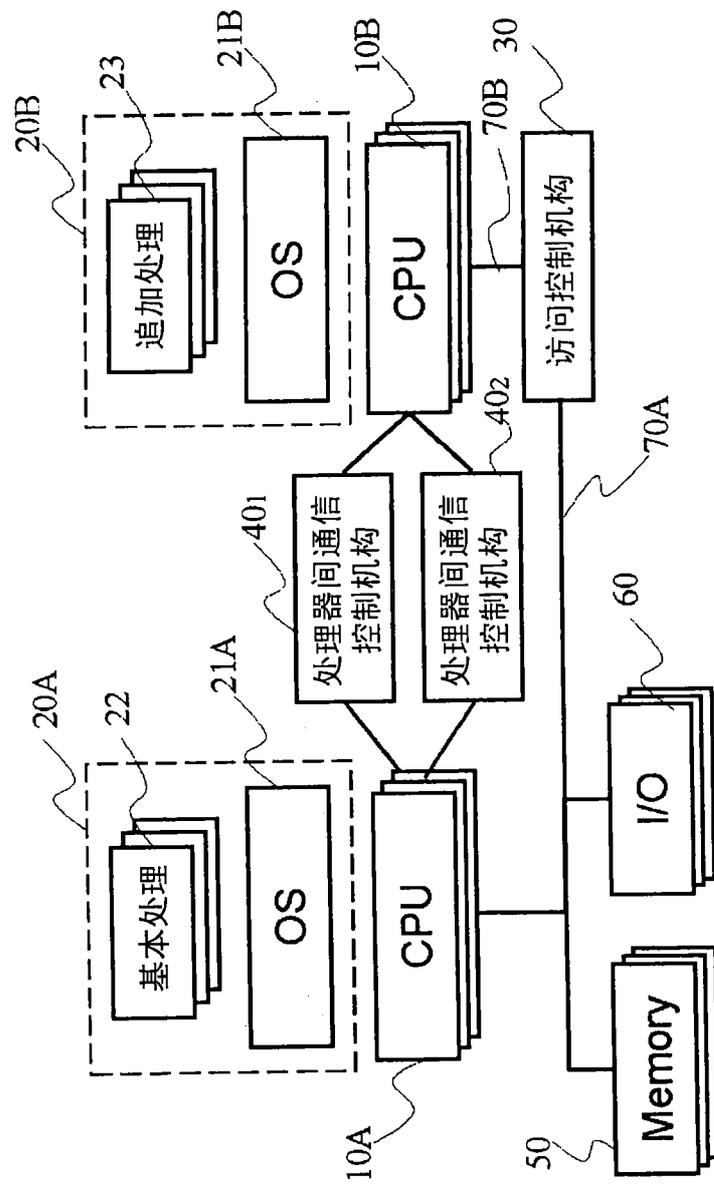


图 1

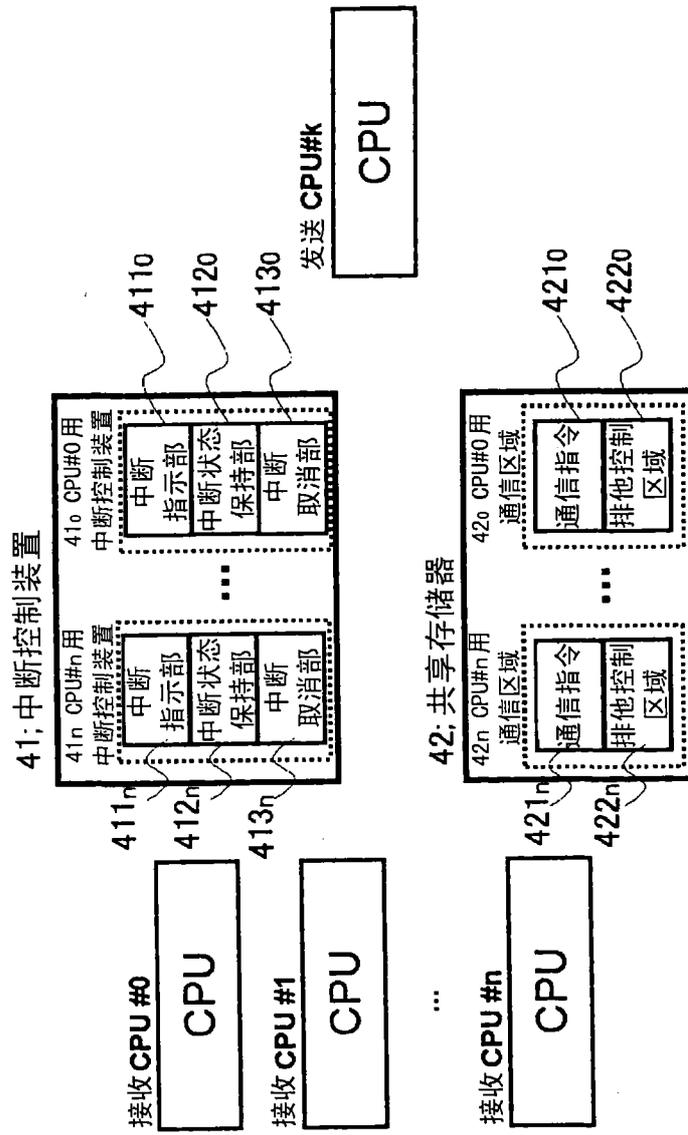


图 2

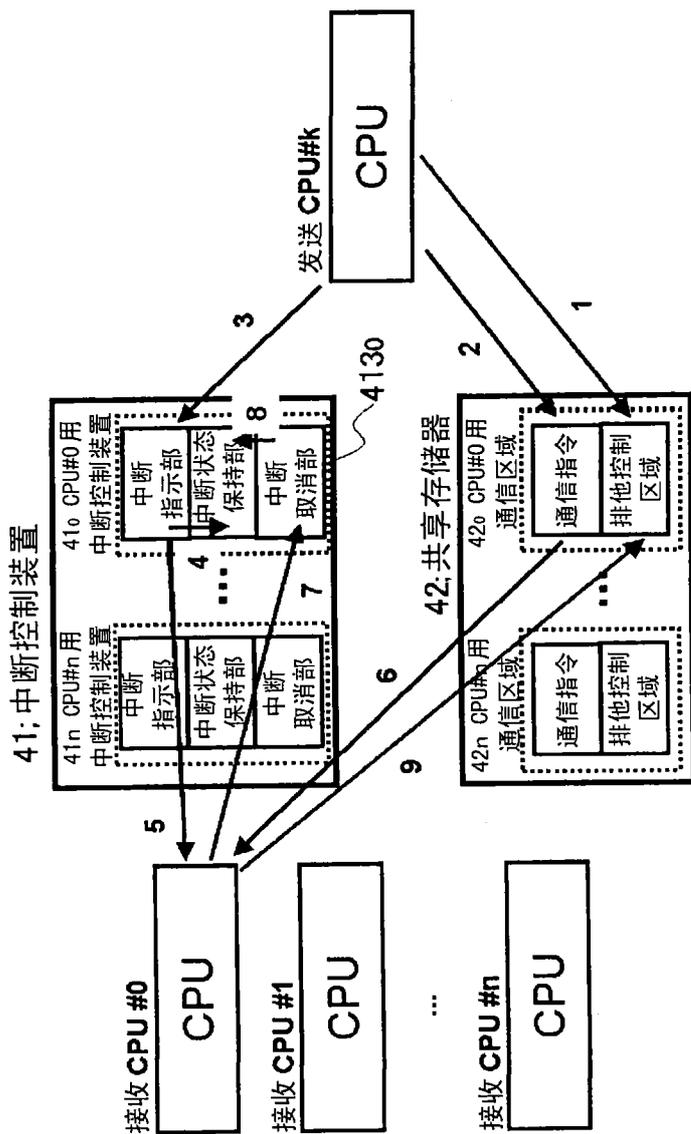


图 3

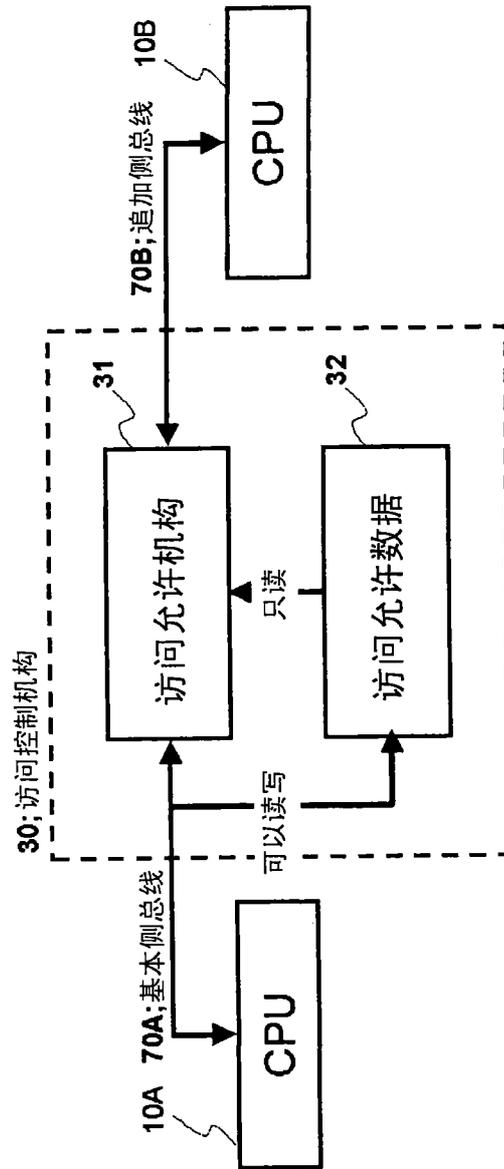


图 4

追加侧 CPU	始点地址	重点地址	访问种类
CPU#4	0x0001000	0x0002000	R
CPU#2, #3	0xC000000	0xF000000	R/W
CPU#3	0xE000000	0xF000000	W

允许范围地址 (bracketed over 始点地址 and 重点地址)

允许参照方法 (arrow pointing to 访问种类)

可以重复 (arrow pointing to 始点地址)

图 5

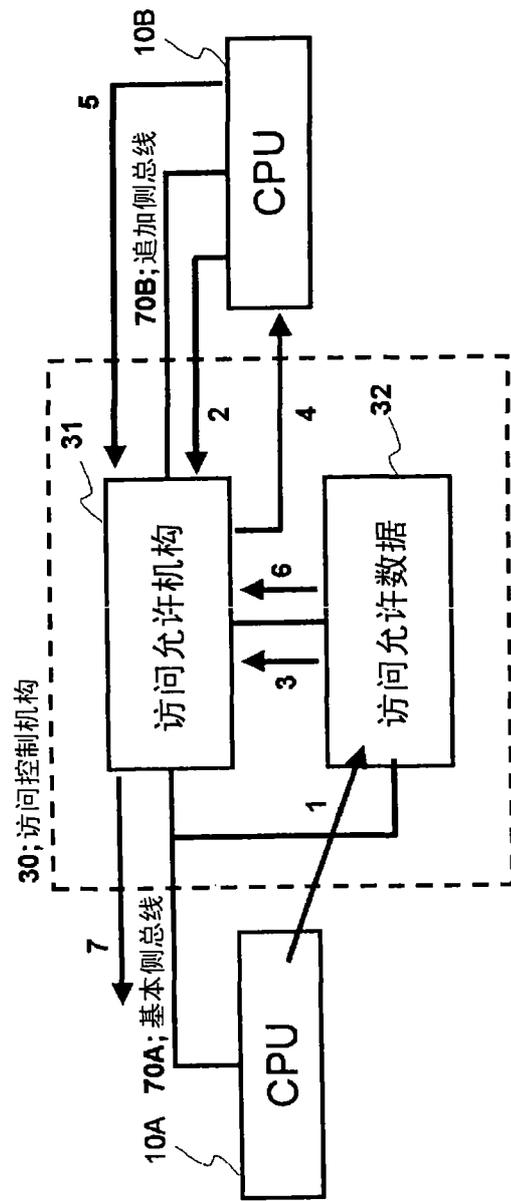


图 6

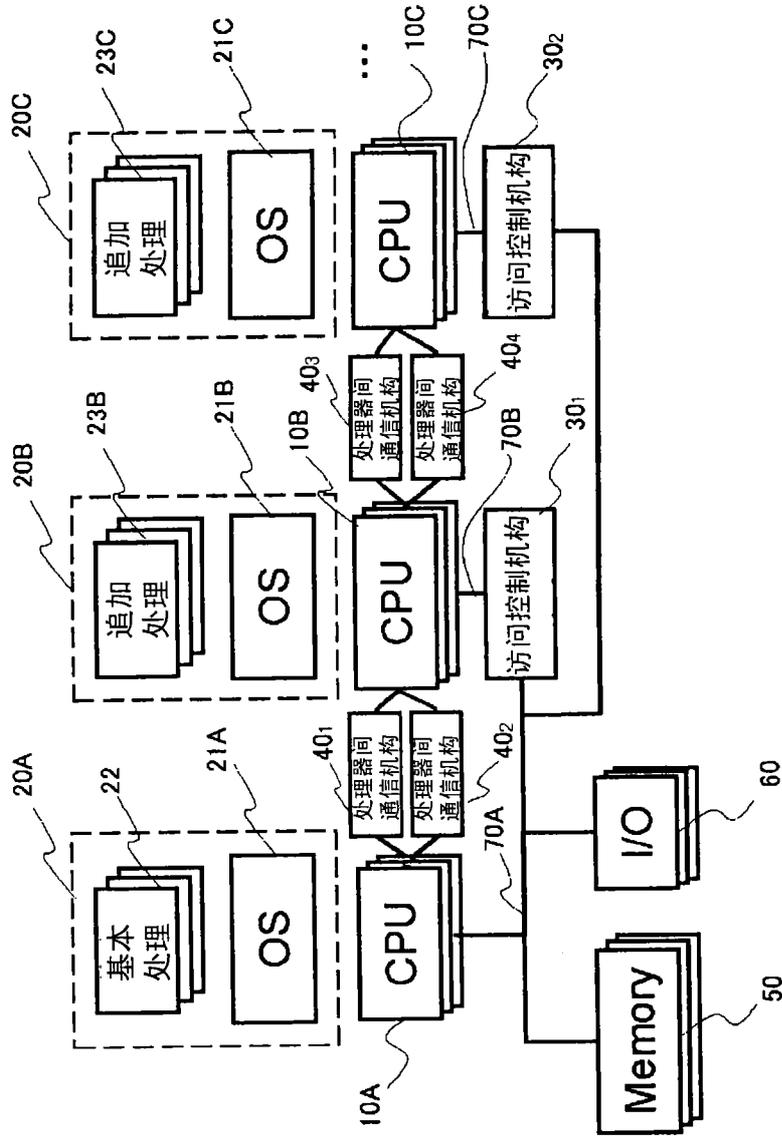


图 7

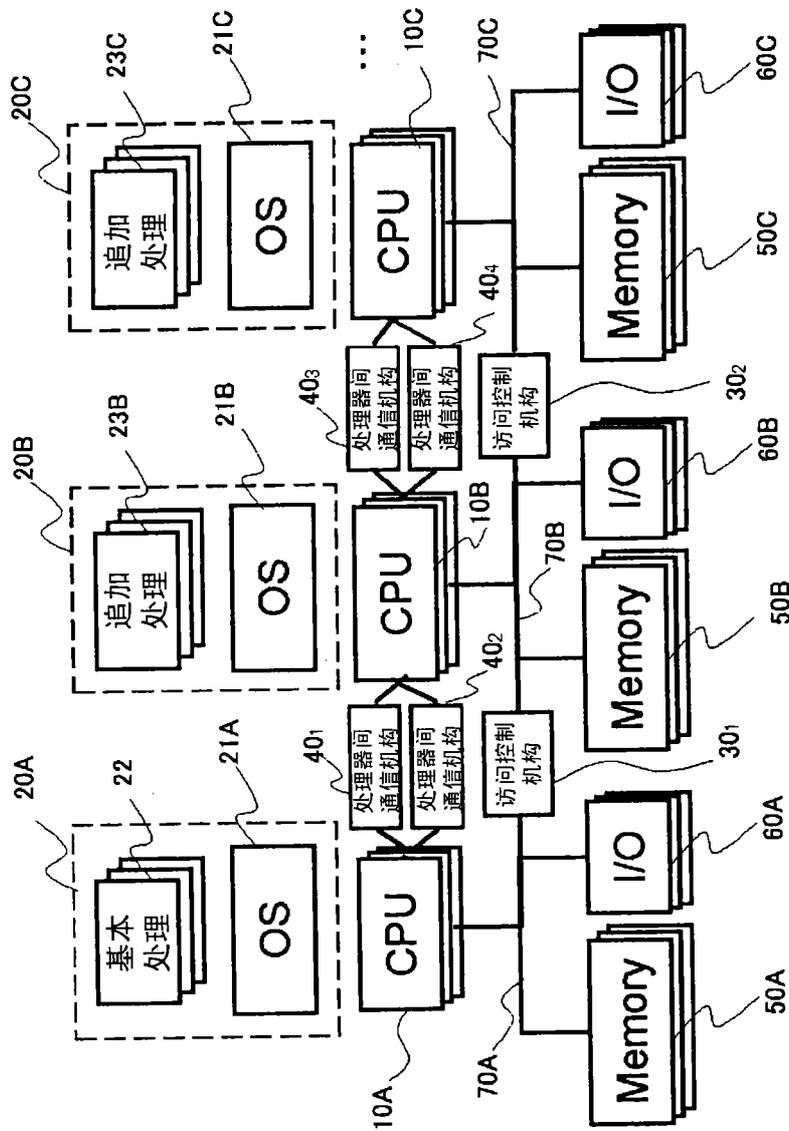


图 8

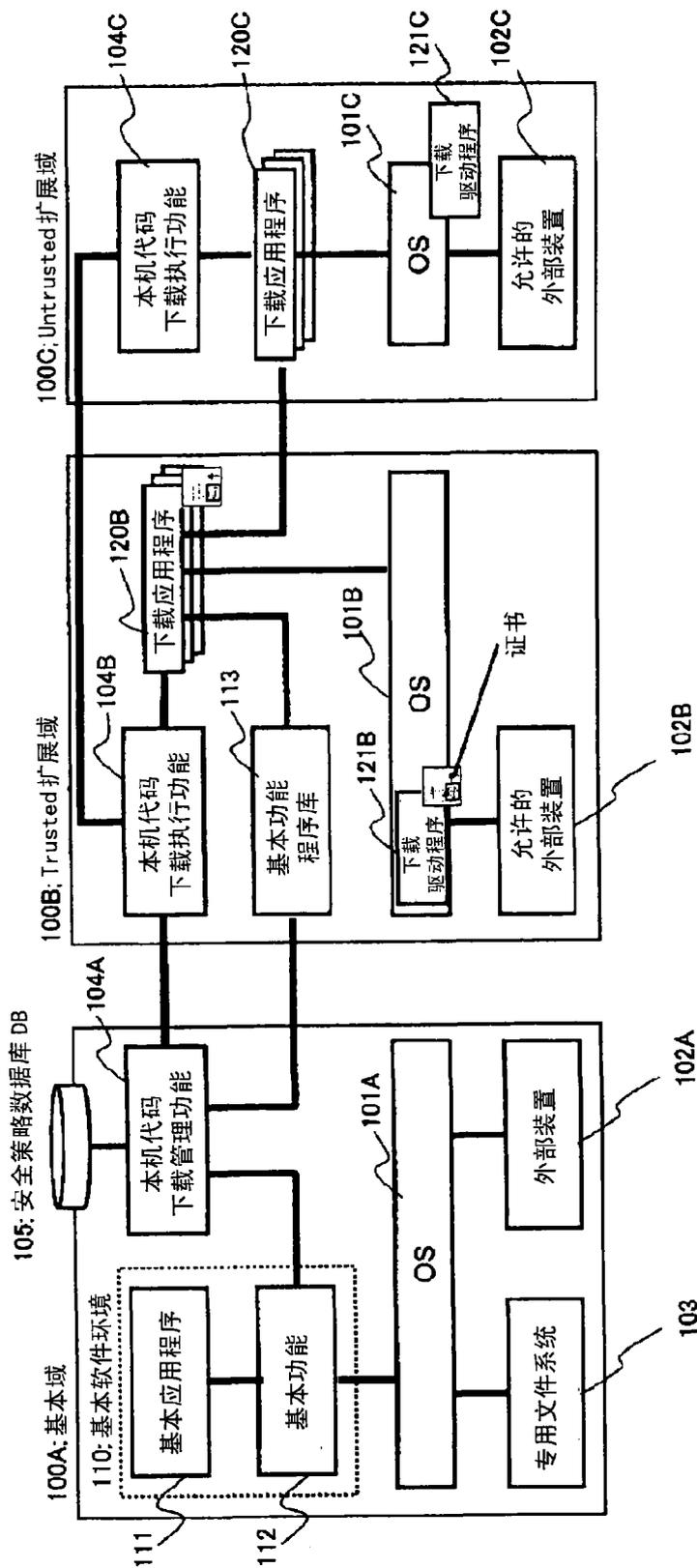


图 9

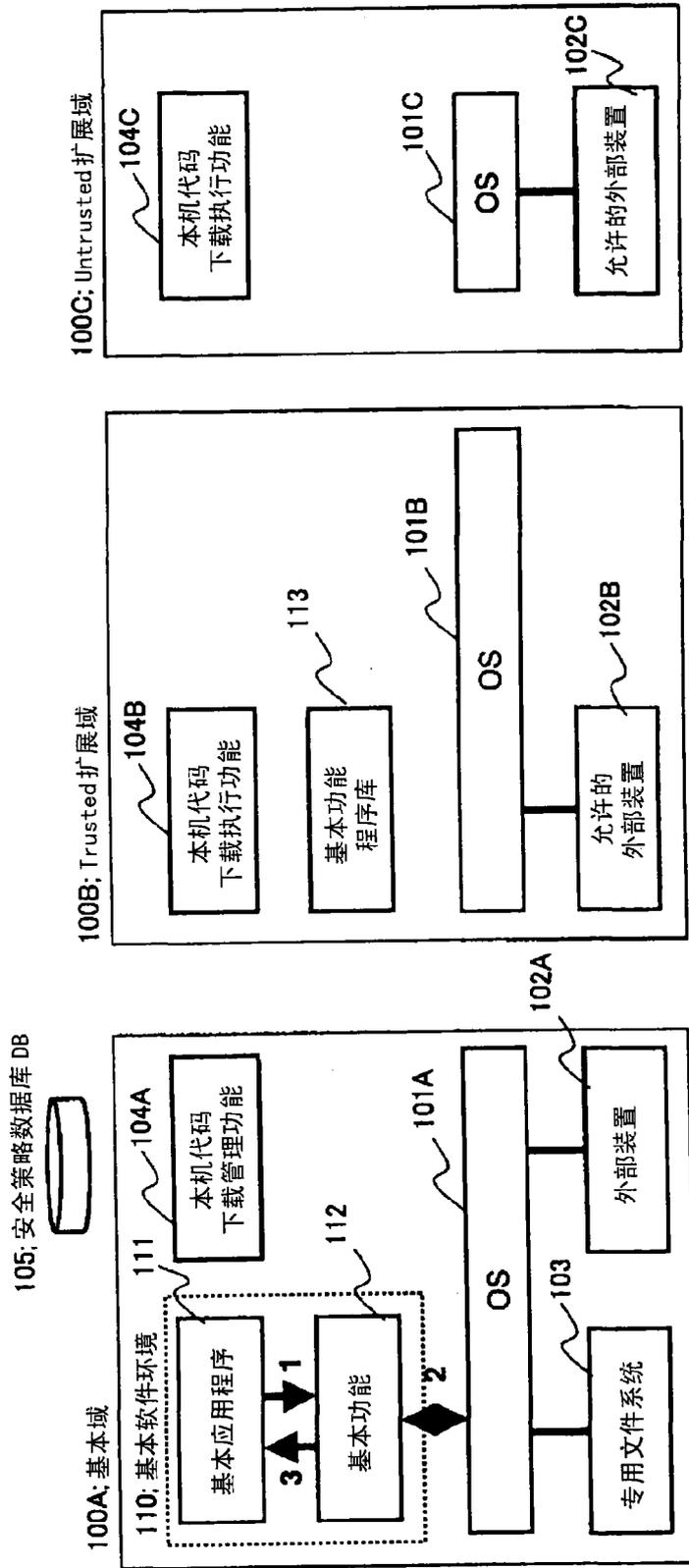


图 10

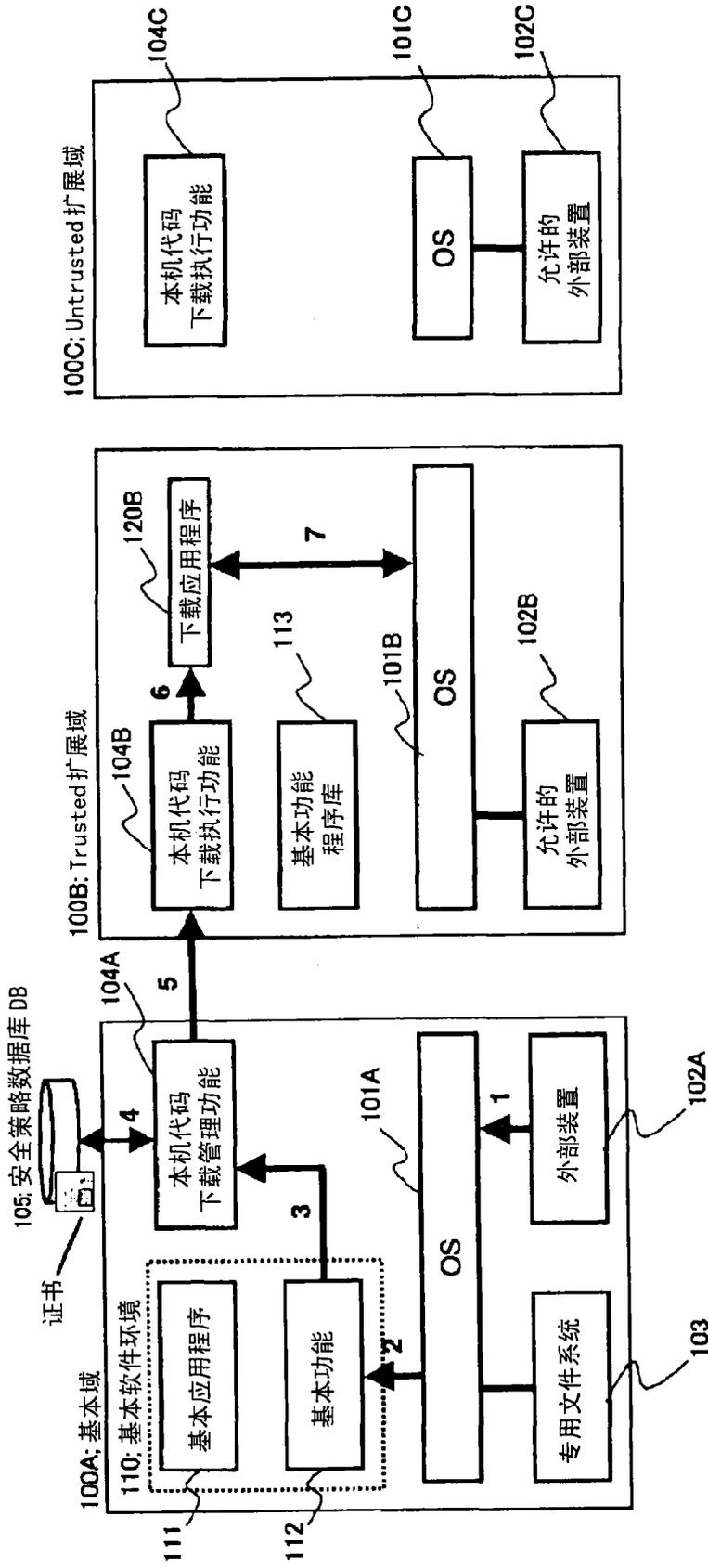


图 11

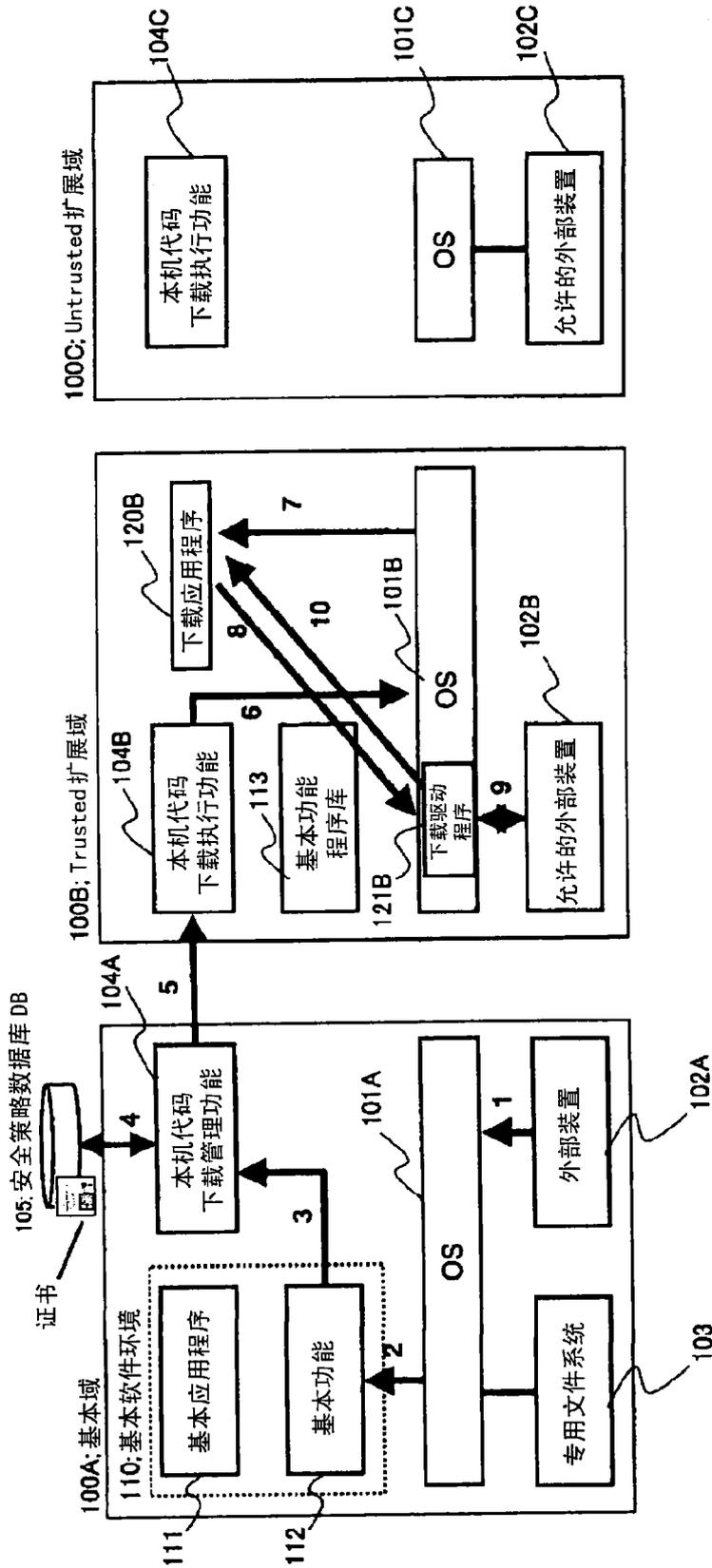


图 12

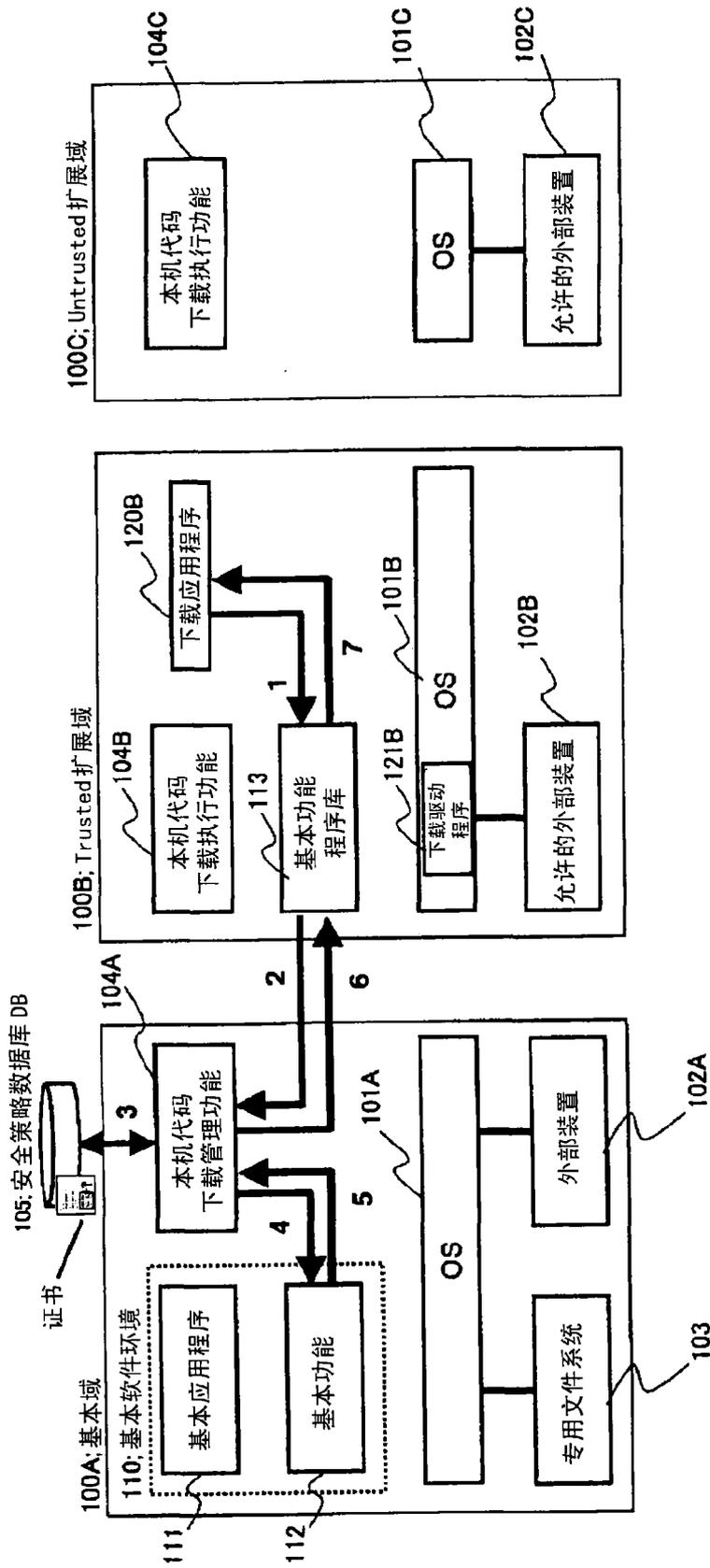


图 13

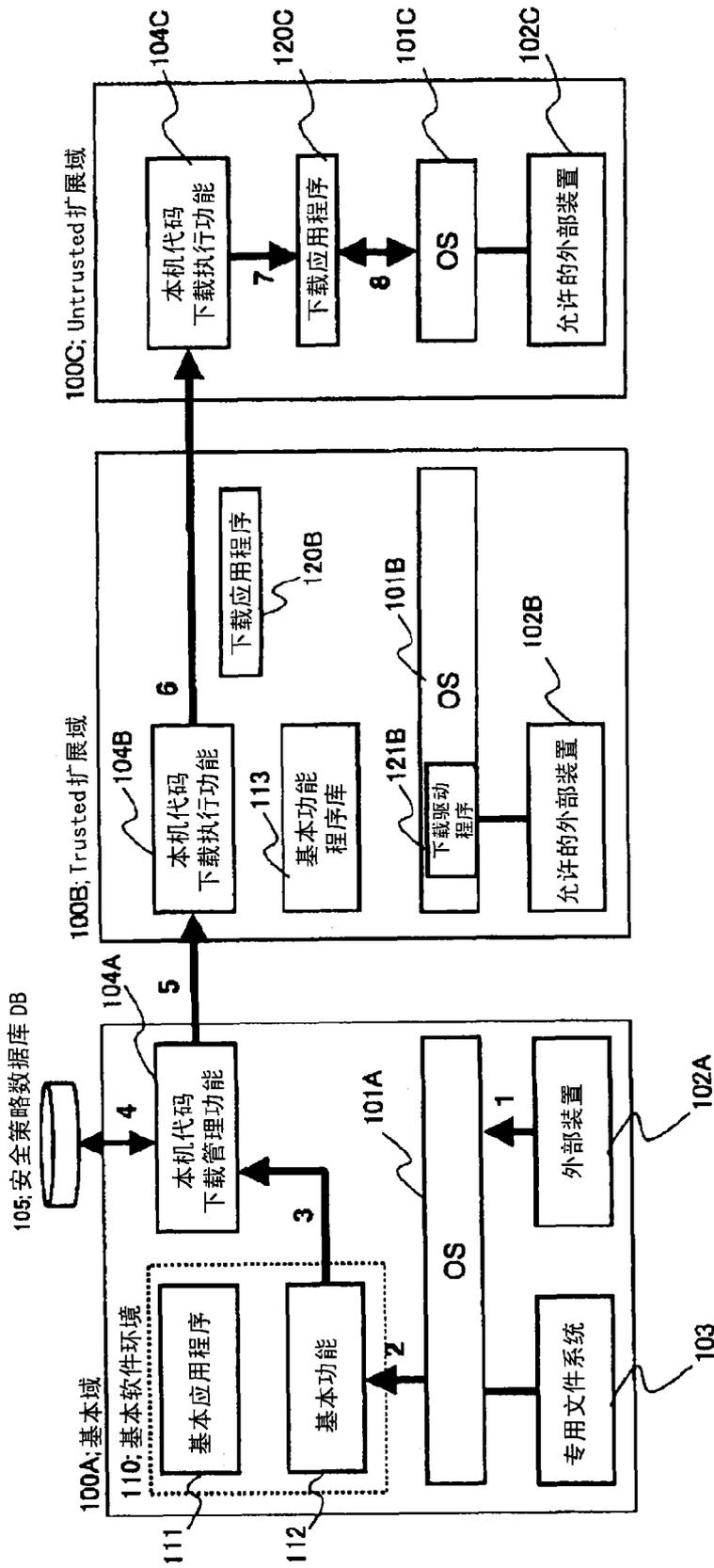


图 14

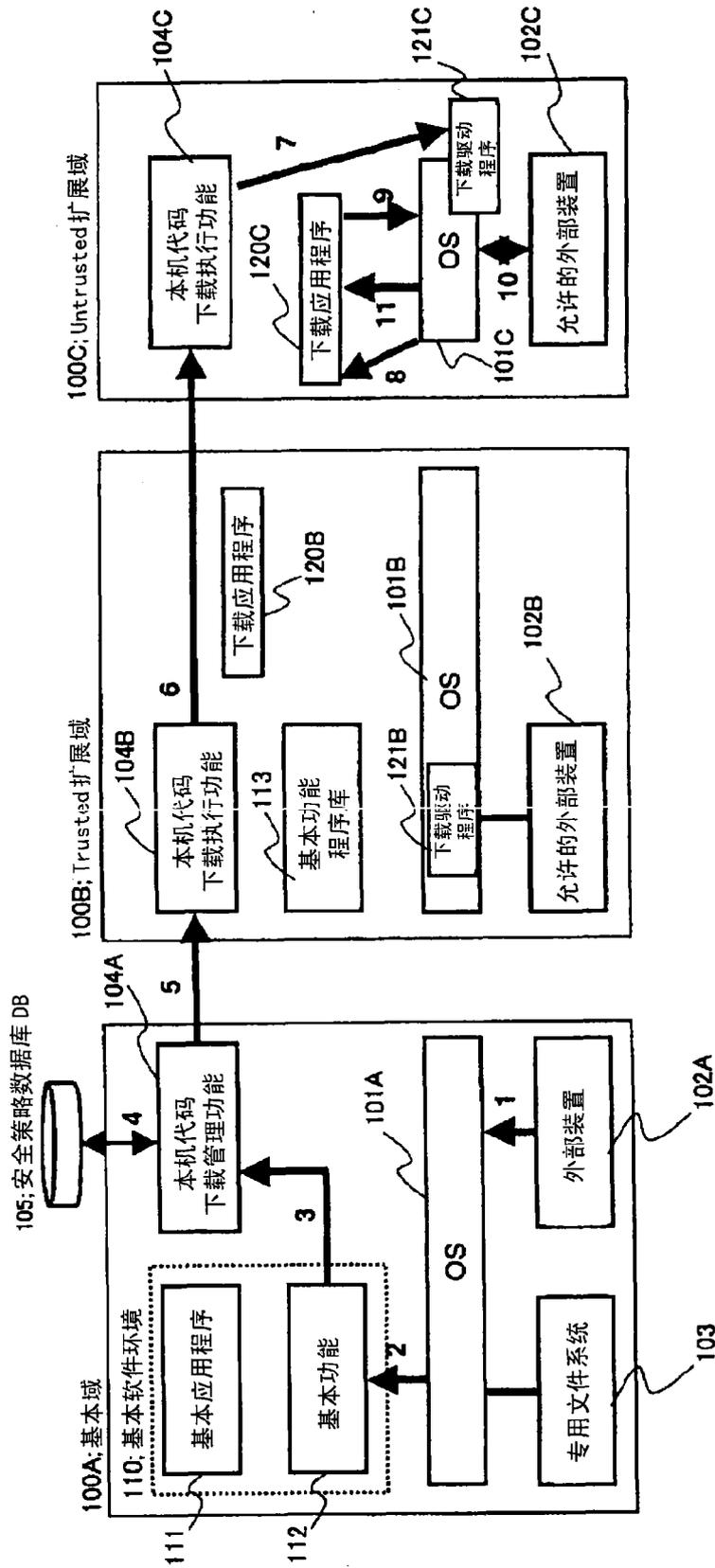


图 15

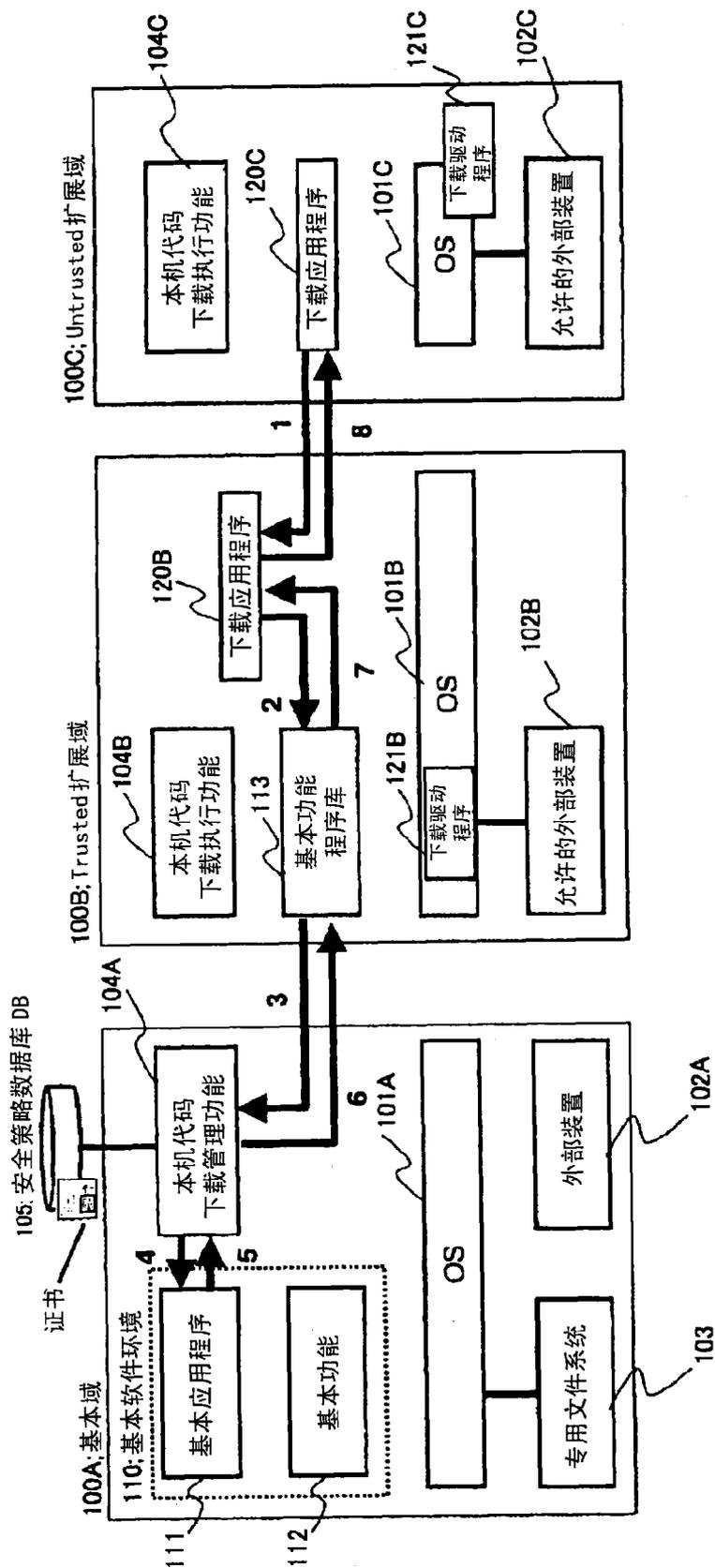


图 16

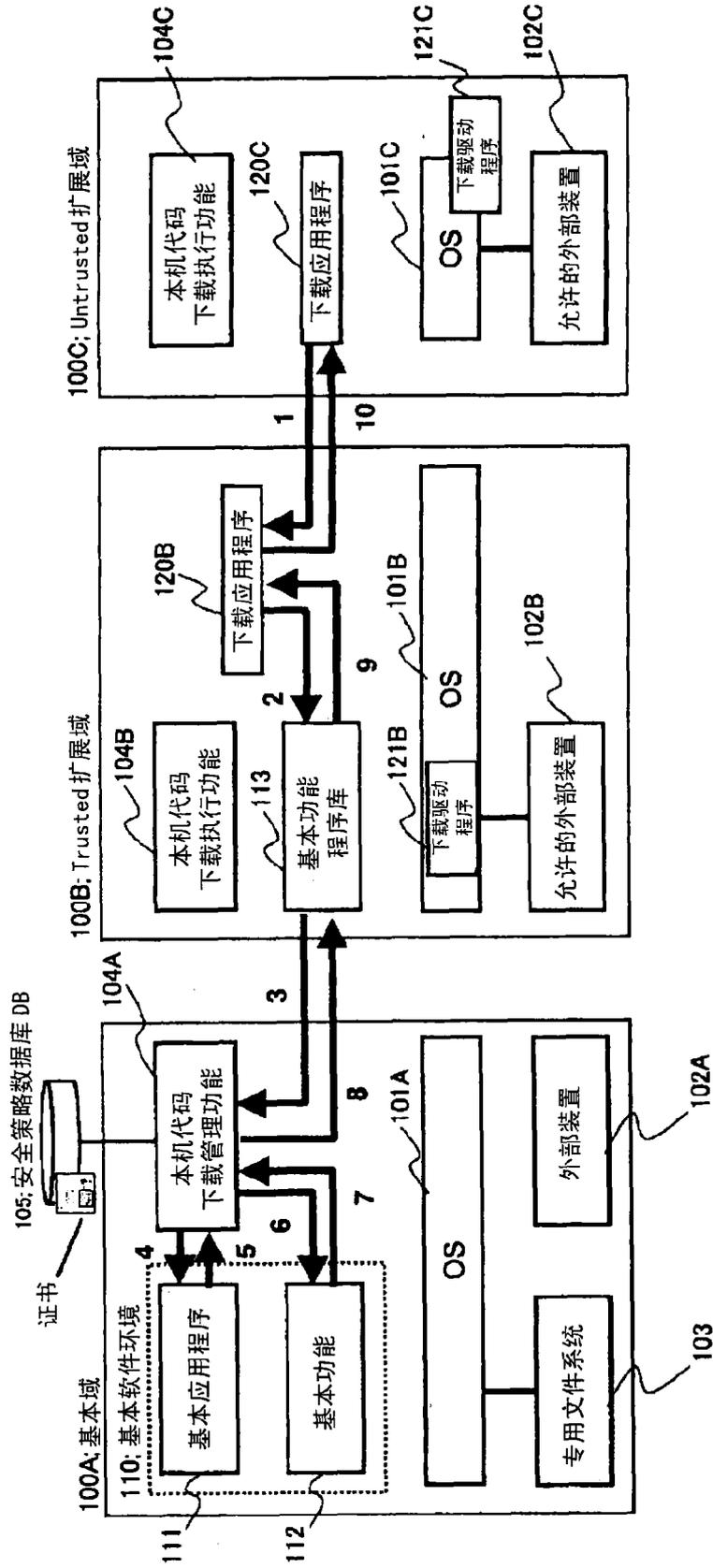


图 17

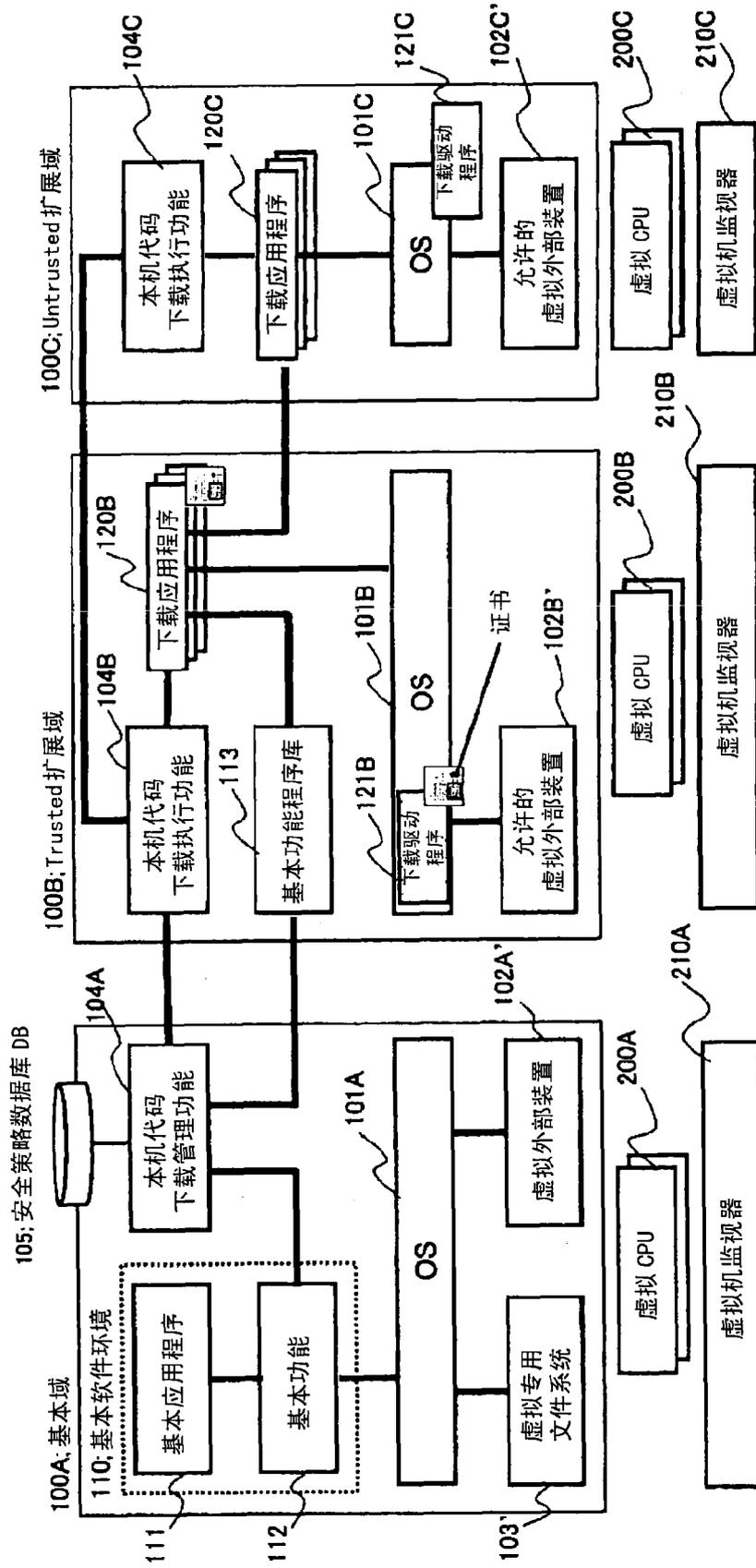


图 18

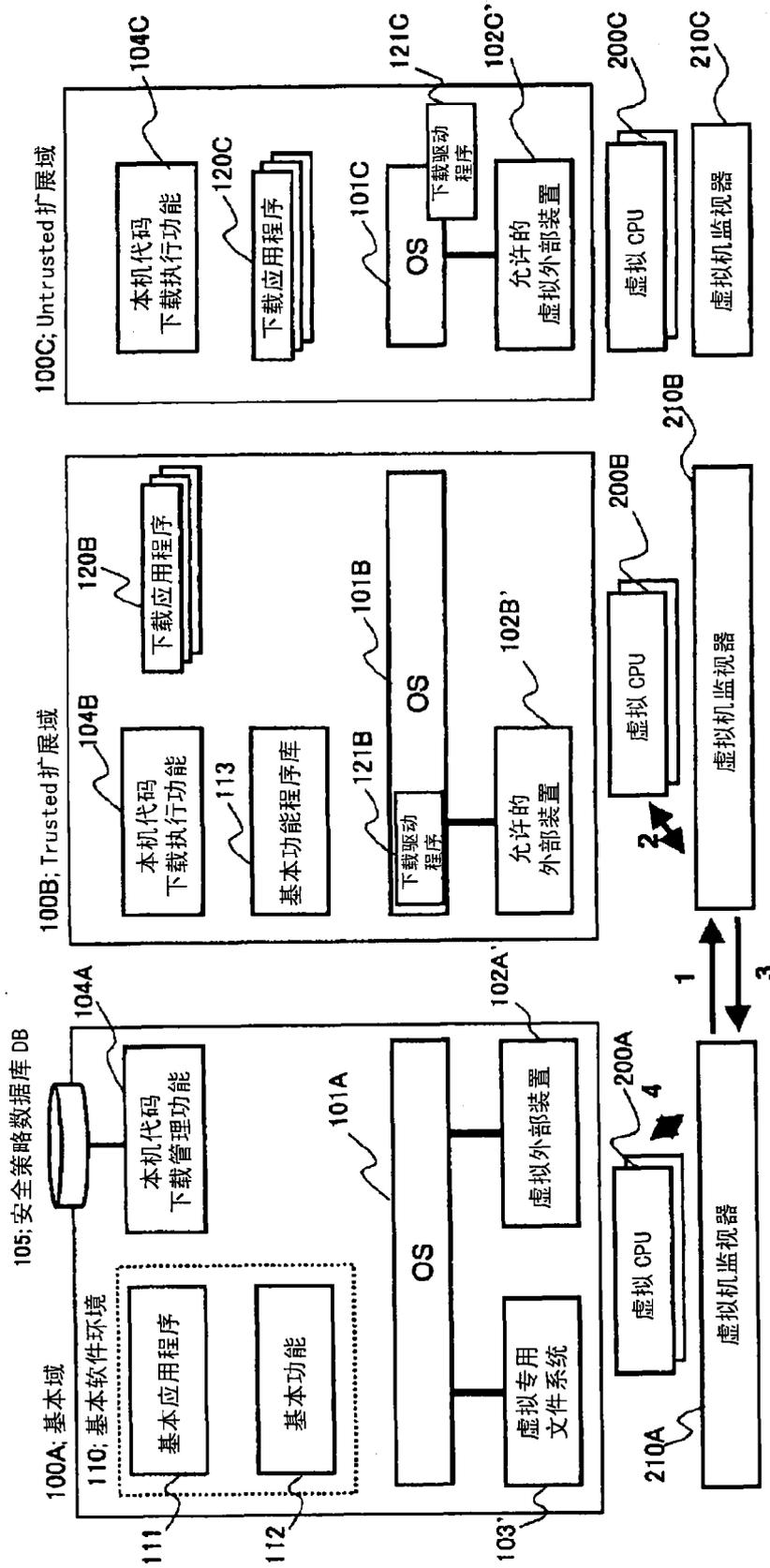


图 19

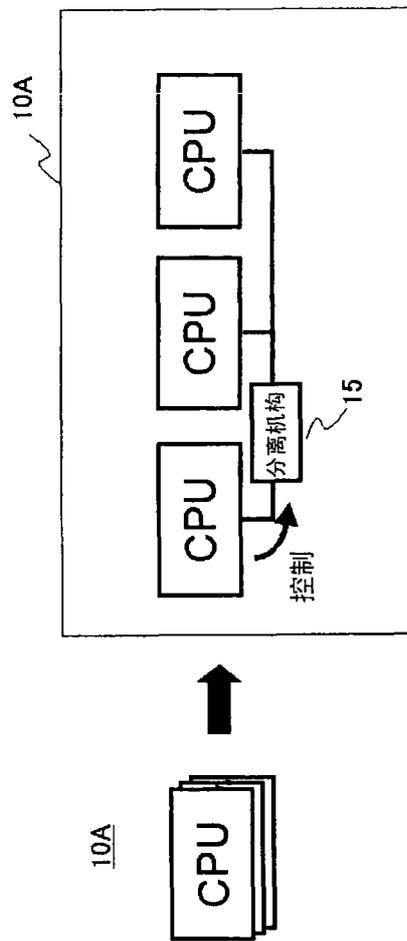


图 20

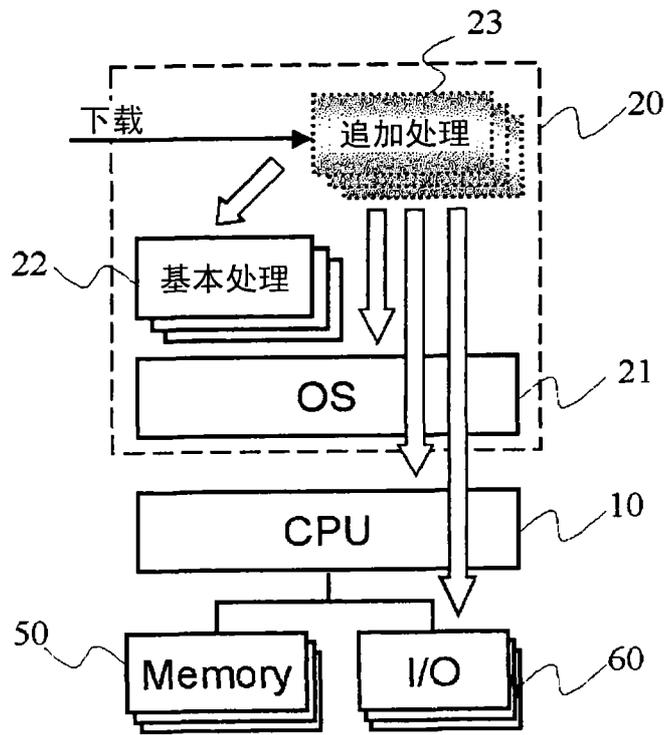


图 21

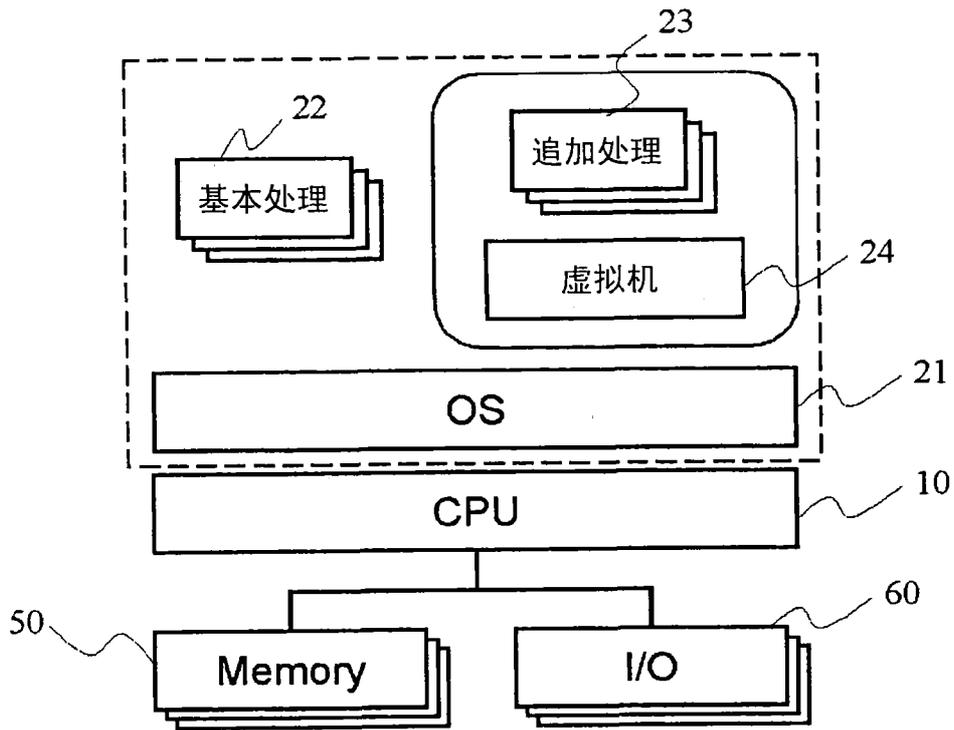


图 22

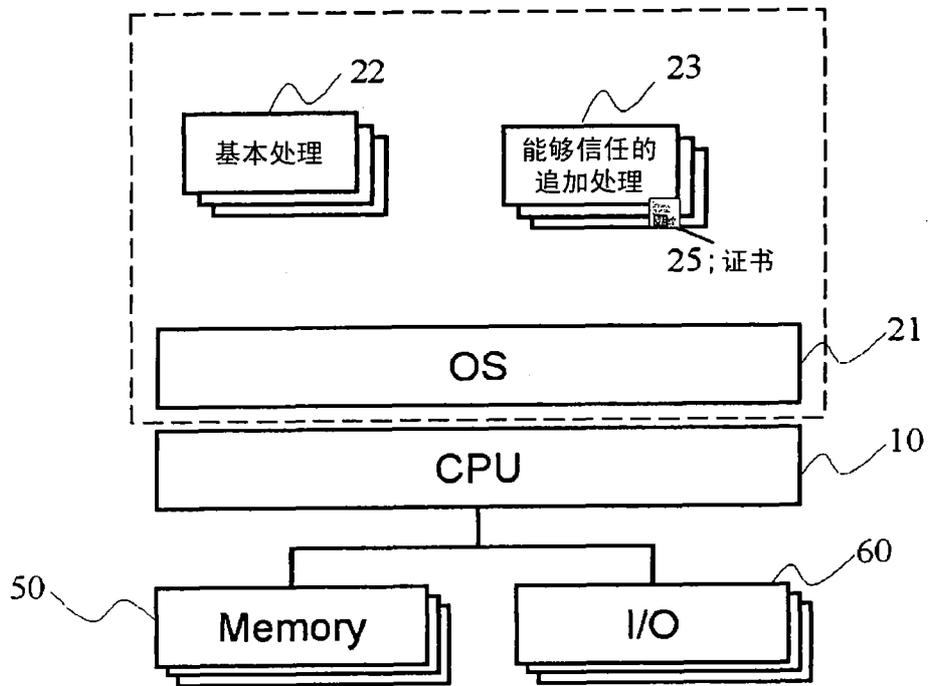


图 23

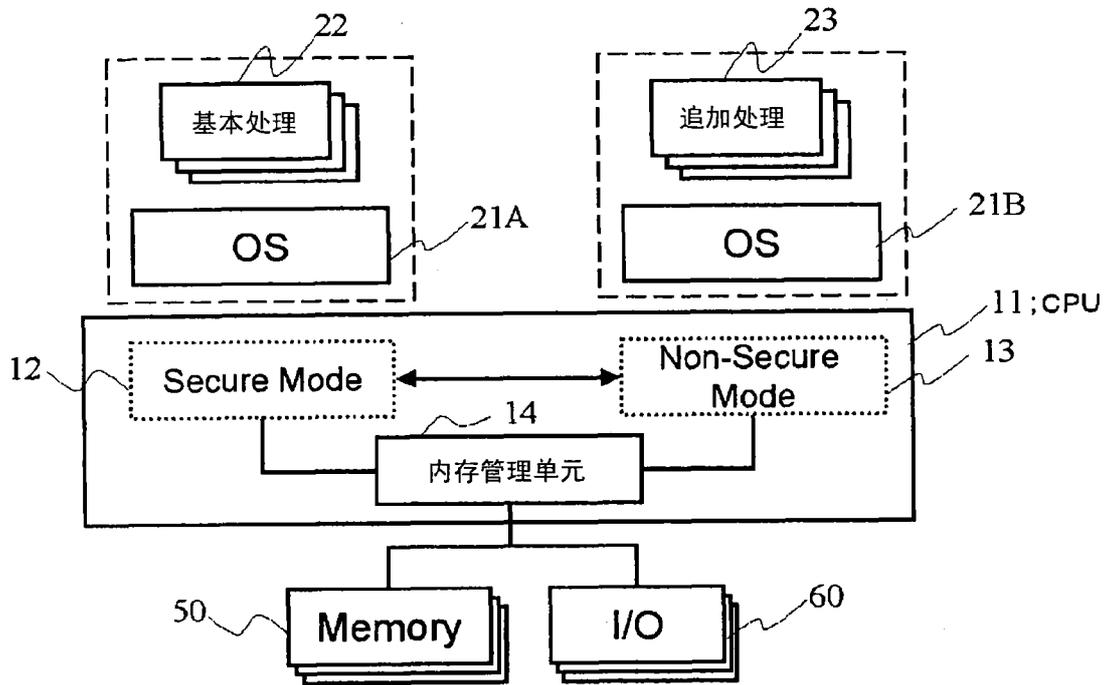


图 24

	基本域	信任扩展域	不信任扩张域
功能 1	等级 A	——	——
功能 2	等级 A	等级 B	——
功能 3	等级 A、等级 B	等级 A、等级 B	——
功能 4	等级 A、等级 B	等级 A、等级 B	等级 C
功能 5	等级 A、等级 B	等级 A、等级 B、等级 C	等级 C、等级 D

图 25

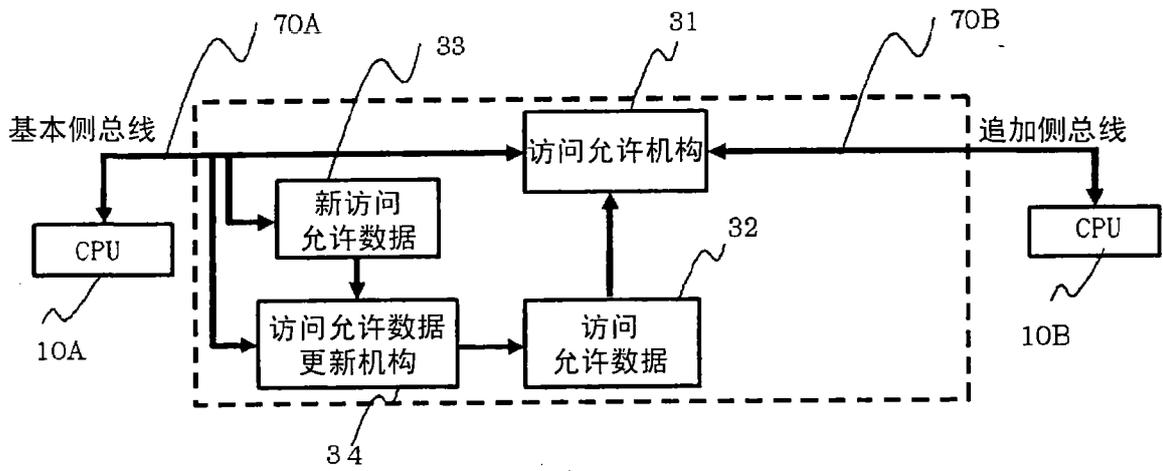


图 26

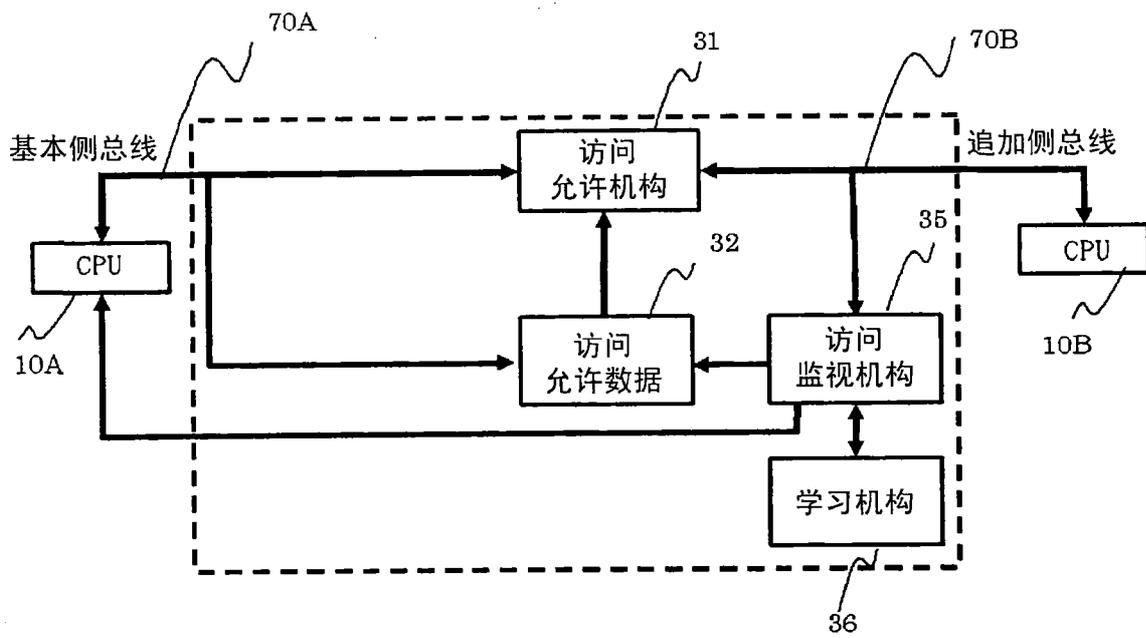


图 27

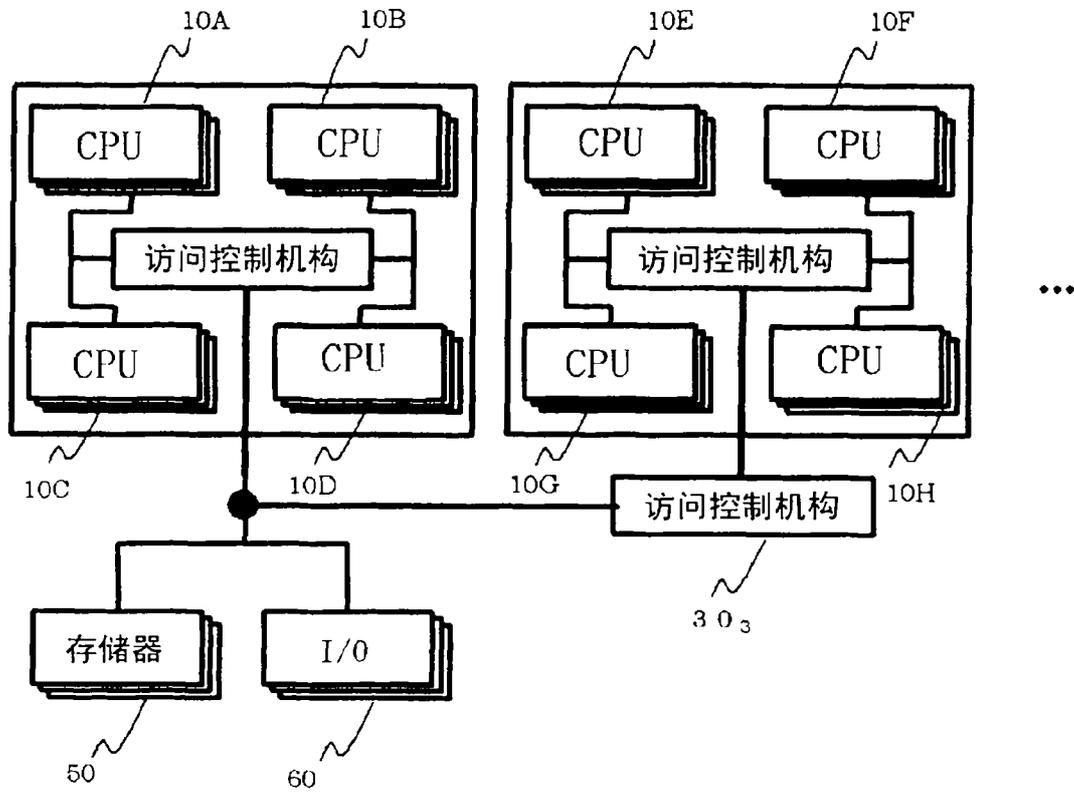


图 28