[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 1/00 (2006.01)
G06F 12/14 (2006.01)

[12] 发明专利说明书

专利号 ZL 02828752.5

[45] 授权公告日 2007 年 1 月 24 日

[11] 授权公告号 CN 1296790C

[22] 申请日 2002.6.5 [21] 申请号 02828752.5
[86] 国际申请 PCT/JP2002/005564 2002.6.5
[87] 国际公布 WO2003/104948 日 2003.12.18
[85] 进入国家阶段日期 2004.10.14
[73] 专利权人 富士通株式会社
地址 日本神奈川
[72] 发明人 蒲田顺 长谷部高行 冈田壮一 林武彦
[56] 参考文献
CN－1245925A 2000.3.1 G06F 12/00
JP－11－345117A 1999.12.14 G06F 9/06
US－5974536A 1999.10.26 G06F 9/00
CN－1204806A 1999.1.13 G06F 12/00
JP－2001－230770A 2001.8.24 H04L 9/10
JP－7－36713A 1995.2.7 G06F 9/46
审查员 毛习文
[74] 专利代理机构 中国国际贸易促进委员会专利商标事务所
代理人 吴丽丽

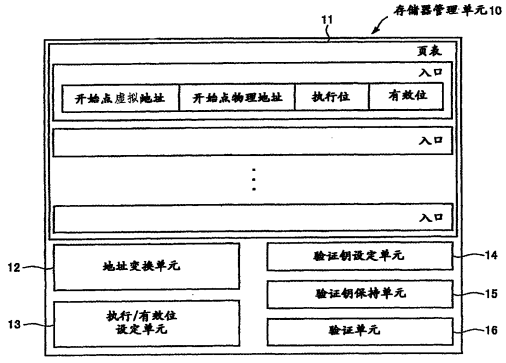
权利要求书 3 页 说明书 19 页 附图 10 页

[54] 发明名称

存储器管理单元、代码验证装置以及代码译码装置

[57] 摘要

本发明提供一种存储器管理单元、代码验证装置以及代码译码装置。管理存储代码的存储器(2)，为了用处理器(1)执行代码，进行表示存储有成为该执行对象的代码的存储器(2)是有效的设定的存储器管理单元(10)，把为了验证代码的正当性而使用的验证钥存储在验证钥保持单元(15)中。而后，当把代码存储到存储器(2)中可以由处理器(1)执行的情况下，使用被存储到验证钥保持单元(15)中的验证钥以及被赋予在代码上的验证信息，验证代码的正当性，进行控制，以便当正当性得到验证的情况下，进行表示存储器(2)是有效的设定，当正当性未得到验证的情况下，不进行表示存储器(2)是有效的设定。



1、一种存储器管理单元，是管理存储代码的存储器，为了由处理器执行上述代码，进行表示储存有成为该执行对象的代码的存储器是有效的设定的存储器管理单元，其特征在于包括:

验证钥存储装置，存储用于验证上述代码的正当性所使用的验证钥;

验证装置，当上述代码被存储在上述存储器中可以由上述处理器执行的情况下，使用由上述验证钥存储装置存储的验证钥以及在上述代码上所赋予的验证信息，来验证上述代码的正当性；以及

控制装置，进行控制，以便当由上述验证装置验证了正当性的情况下，进行表示上述存储器是有效的设定，当正当性未得到上述验证装置验证的情况下，不进行表示上述存储器是有效的设定。

2、一种存储器管理单元，是管理存储代码的存储器，为了由处理器执行上述代码，进行表示储存有成为该执行对象的代码的存储器是有效的设定的存储器管理单元，其特征在于包括:

译码钥存储装置，存储用于将被加密的代码进行译码所使用的译码钥;

译码装置，当上述被加密的代码被存储在上述存储器中的情况下，从该存储器中读出上述被加密的代码，使用由上述译码钥存储装置存储的译码钥进行译码，再存储到上述存储器中；以及

控制装置，进行表示再存储由上述译码装置译码的代码的上述存储器是有效的设定。

3、根据权利要求 1 或者 2 所述的存储器管理单元，其特征在于:

上述存储器管理单元在由上述处理器执行代码时，把从该处理器输入的虚拟地址变换为作为上述存储器上的地址的物理地址，向上述存储器输出该变换了的物理地址。

4、根据权利要求 1 或者 2 所述的存储器管理单元，其特征在于：

上述存储器管理单元在由上述处理器执行代码时，把从该处理器输入的虚拟地址作为是上述存储器上的地址的物理地址，向上述存储器输出。

5、根据权利要求 1 或者 2 所述的存储器管理单元，其特征在于：

上述代码是用机器语言表述，由作为处理器的 CPU 解释并执行的程序。

6、一种代码验证装置，是基于赋予在该代码上的验证信息验证存储在存储器中由处理器执行的代码的正当性的代码验证装置，其特征在于包括：

验证钥存储装置，为了验证上述代码的正当性，存储对应上述验证信息所使用的验证钥；

验证装置，当上述代码被存储在上述存储器中可以由上述处理器执行的情况下，使用由上述验证钥存储装置存储的验证钥以及在上述代码上所赋予的验证信息，验证上述代码的正当性；以及

当由上述验证装置验证了正当性的情况下，允许由上述处理器执行上述代码，当正当性未得到上述验证装置验证的情况下，拒绝由上述处理器执行上述代码的控制装置。

7、一种代码译码装置，是为了由处理器执行而译码被存储在存储器中的被加密代码的代码译码装置，其特征在于包括：

译码钥存储装置，存储为了译码上述被加密的代码而使用的译码钥；

译码装置，当上述被加密的代码被存储在上述存储器中的情况下，从该存储器中读出上述被加密的代码，用由上述译码钥存储装置存储的译码钥译码，再存储到上述存储器中；以及

控制装置，控制上述处理器执行由上述译码装置译码并被再存储到上述存储器中的代码。

存储器管理单元、代码验证装置以及代码译码装置

技术领域

本发明涉及被装入个人计算机和移动通信终端等的信息处理装置的存储器管理单元、代码验证装置以及代码译码装置，特别涉及不需要变更处理器和存储器的体系结构，可以简单并且可靠地保证在信息处理装置上执行的代码的正当性的存储器管理单元、代码验证装置以及代码译码装置。

背景技术

以往，在个人计算机和移动通信终端等的信息处理装置中，要求在装置上执行保证了正当性的安全代码（用机器语言记述，由 CPU 解释并执行的程序）。即，在向硬盘等的安装前或者安装后被恶意的第 3 者篡改的，在安全性上存在问题的代码必须不能存储在存储器上并在装置上执行。

并且，作为针对这种必要性的以往技术，以往一般采用以下的两种方法进行，①在信息处理装置上追加验证用软件，使用预先所赋予的验证信息，在代码执行前验证代码的正当性的方法，②在信息处理装置上追加译码用软件，通过在执行前译码预先加密的代码，担保代码的正当性的方法。

但是，上述的以往技术因为通过软件验证或者担保代码的正当性，所以验证用软件和译码用软件自身被篡改的危险性很大，存在不一定能在信息处理装置上执行保证正当性的安全代码的问题。

即，当验证用软件自身被篡改的情况下，有可能与是否得到验证没有关系地执行代码，另外，当译码用软件自身被篡改的情况下，有可能在执行已译码的代码前被篡改，其结果在上述以往技术中，不一

定能在信息处理装置上执行保证了正当性的安全代码。

为了解决由此软件引起的问题，还考虑了以下 2 种方法，①用附加在信息处理装置内的存储器上的特别的验证用的硬件，对作为处理器的存储器分配单位的每一页，验证被配置在页上的代码的方法，②用附加在信息处理装置内的处理器上的特别的译码用的硬件，译码提取的代码的方法，但存在不能简单地开发这种硬件的问题。

即，在存储器上附加特别的验证用硬件的方法，和在处理器上附加特别的译码用硬件方法，换句话说，因为是在存储器的校验部分和处理器的入口部分上追加新的智能，所以需要大幅度变更处理器和存储器的系统结构，不能简单地开发。

这样，在个人计算机和移动通信终端等的信息处理装置上，如何在装置上执行保证正当性的安全代码是极其重要的课题，希望不改变处理器和存储器的系统结构，可以简单并且可靠地解决它的硬件。

因而，本发明就是为了解决上述以往技术的问题而完成的，其目的在于提供一种不改变处理器和存储器的系统结构，就可以简单并且可靠地保证在信息处理装置上执行的代码的正当性的存储器管理单元、代码验证装置以及代码译码装置。

发明内容

本发明是管理存储代码的存储器，为了用存储器执行代码，进行表示存储有成为该执行对象的代码的存储器是有效的设定的存储器管理单元，在验证钥存储装置中存储在用于验证代码的正当性使用的验证钥。而后，当在存储器中存储代码可以由处理器执行的情况下，使用由验证钥存储装置存储的验证钥以及赋予代码的验证信息验证代码的正当性，进行控制，以便当正当性得到验证的情况下，进行表示存储器是有效的设定，当正当性未得到验证的情况下，不进行表示存储器是有效的设定。

因此，如果采用本发明，因为对于在安装前或者安装后因被恶意的第 3 者篡改而在安全性上存在问题的代码，在代码的执行前之际（即，把从虚拟页向物理页的地址变换设置为有效的时刻），用作为

对恶意的第三者来说触及不到的硬件的存储器管理单元，可靠地进行表示代码是不正当的验证，所以可以避免由处理器执行。另外，具有这样的验证功能的存储器管理单元因为不需要变更处理器和存储器的系统结构，所以与开发具有验证功能的处理器和存储器相比，可以简单地开发。因而，不变更处理器和存储器的系统结构，就可以简单并且可靠地保证在信息处理装置上执行的代码的正当性。

另外，本发明是管理存储代码的存储器，为了用处理器执行代码，进行表示存储有成为该执行对象的代码的存储器是有效的设定的存储器管理单元，在译码钥存储装置中存储为了译码经加密的代码而使用的译码钥。而后，当在存储器中存储有被加密的代码的情况下，从该存储器中读出被加密的代码，用由译码钥存储装置存储着的译码钥译码，再存储到存储器中，进而，进行表示再存储有经译码的代码的存储器是有效的设定。

因此，如果采用本发明，因为在代码的执行前之际，用作为对恶意的第三者来说触及不到的硬件的存储器管理单元，译码经加密的代码，所以对于译码后的代码，可以作为正当性被担保的代码（安装前或者安装后未被恶意的第三者篡改的代码）执行。另外，具有这样的译码功能的存储器管理单元因为不需要变更处理器和存储器的系统结构，所以和开发具有译码功能的处理器和存储器比较，可以简单地开发。因而，不变更处理器和存储器的系统结构，就可以简单并且可靠地保证在信息处理装置上执行的代码的正当性。

另外，本发明的存储器管理单元在处理器执行代码时，把从该处理器输入的虚拟地址变换为作为存储器上的地址的物理地址，对处理器输出经该变换的物理地址。

因此，如果采用本发明，则可以适用到个人计算机、工作站或者移动通信终端等，进行从虚拟地址到物理地址的地址变换的信息处理装置，可以简单并且可靠地保证在这样的信息处理装置上执行的代码的正当性。

另外，本发明的存储器管理单元在由处理器执行代码时，把从该

处理器输入的虚拟的地址作为是存储器上的地址的物理地址对存储器输出。

因此，如果采用本发明，则可以适用到 PHS 终端、便携终端或者 PDA 等，进行从虚拟地址向物理地址的地址变换的信息处理装置，可以简单地保证可以在这种信息处理装置上执行的代码的正当性。

另外，在本发明中，代码是用机器语言记述，用作为处理器的 CPU 解释并执行的程序。

因此，如果采用本发明，则对于在信息处理装置上作为基本软件执行的极其重要的代码，不需要改变处理器和存储器的系统结构就可以简单并且可靠地保证正当性。

另外，本发明是根据赋予该代码的验证信息验证被存储在存储器中由处理器执行的代码的正当性的代码验证装置，为了验证代码的正当性把与验证信息对应使用的验证钥存储在验证钥存储装置中。而后，当代码被存储在存储器中可以由处理器执行的情况下，使用由验证钥存储装置存储的验证钥和赋予代码的验证信息，验证代码的正当性，当正当性得到验证的情况下，允许由处理器执行代码，当正当性未得到验证的情况下，拒绝由处理器执行代码。

因此，如果采用本发明，则不变更处理器和存储器的系统结构，就可以简单并且可靠地保证在信息处理装置上执行的代码的正当性。

另外，本发明是为了用处理器执行而译码存储在存储器中的被加密代码的代码译码装置，把为了译码经加密的代码而使用的译码钥存储在译码钥存储装置中。而后，当把经加密的代码存储到存储器中的情况下，从该存储器中读出经加密的代码，用由译码钥存储装置存储的译码钥译码，再存储到存储器中，进而，控制处理器执行译码后再次存储到存储器中的代码。

因此，如果采用本发明，则不变更处理器和存储器的系统结构，就可以简单并且可靠地保证在信息处理装置上执行的代码的正当性。

附图说明

图 1 是展示适用于涉及本实施方式 1 的存储器管理单元系统构成的方框图。

图 2 是展示涉及本实施方式 1 的存储器管理单元构成的方框图。

图 3 是用于说明本实施方式 1 中的地址空间的图。

图 4 是用于说明本实施方式 1 中的系统处理的流程图。

图 5 是展示涉及本实施方式 2 的存储器管理单元构成的方框图。

图 6 是用于说明本实施方式 2 中的地址空间的图。

图 7 是展示适用于涉及本实施方式 3 的存储器管理单元的系统构成的方框图。

图 8 是展示涉及本实施方式 3 的存储器管理单元的构成的方框图。

图 9 是用于说明本实施方式 3 中的系统处理的流程图。

图 10 是展示涉及本实施方式 4 的存储器管理单元构成的方框图。

具体实施方式

以下，参照附图详细说明本发明的存储器管理单元、代码验证装置以及代码译码装置适宜的实施方式。进而，以下作为实施方式 1~4，在说明本发明的存储器管理单元的各种实施方式后，作为另一实施方式，说明本发明的代码验证装置以及代码译码装置及各种变形例，最后，说明本发明的效果。

（实施方式 1）

在本实施方式 1 中，说明在被安装在个人计算机、工作站或者移动通信终端等的信息处理终端上的存储器管理单元（MMU: Memory Management Unit）中追加了用于验证由处理器执行的代码的正当性的验证功能的情况。进而，在此，在说明本实施方式 1 的存储器管理单元适用的系统概要以及主要特征后，说明存储器管理单元的构成，最后，说明此系统的处理顺序。

[实施方式 1: 系统的概要以及主要特征]

首先最初，说明适用本实施方式 1 的存储器管理单元的系统概要

以及主要特征。图 1 是展示适用于本实施方式 1 的存储器管理单元的系统构成的方框图。如该图所示，此系统是个人计算机、工作站或者移动通信终端等的信息处理终端的一部分，在处理器 1、存储器 2 以及验证信息用存储器 3 之间，设置存储器管理单元 10，用地址总线 4 以及数据总线 5 连接它们而构成。

其中，处理器 1 是执行被存储在存储器 2 中的代码（用机器语言记述，由 CPU 解释执行的程序），在该执行时，读写被存储在存储器 2 中的数据的处理单元（例如，CPU 等）。另外，存储器 2 是存储处理器 1 使用的代码和数据的存储单元。另外，存储器管理单元 10 是处理单元，对存储器 2 进行管理，主要为了由处理器 1 执行代码而进行表示存储着成为该执行对象的代码的存储器 2 是有效的设定。进而，验证信息用存储器 3 是存储后述的验证信息的存储单元。

在此，如果简单地说明本系统的概略性处理的流程，则首先最初，处理器 1 经由存储器管理单元 10 对作为存储器分配单位的规定的页（例如，4Kbytes），逐页地把代码存储到存储器 2 中。接着，如果用存储器管理单元 10 进行表示存储有该代码的存储器是有效的设定，则处理器 1 把与该代码对应的虚拟地址输出到存储器管理单元 10。而后，存储器管理单元 10 把从处理器 1 输入的虚拟地址，变换为作为存储器 2 上的地址的物理地址向存储器 2 输出，由此，由处理器 1 执行与存储器 2 上对应的代码。

这样，如图 1 所示的系统大致是由处理器 1 执行被存储在存储器 2 上的代码，但在该代码上赋予了为了验证代码的正当性而使用的验证信息（例如，电子署名和电子证明书）。总之，本系统主要特征是：通过存储器管理单元 10 使用在代码上被赋予的验证信息验证代码的正当性，可以不变更处理器 1 和存储器 2 的系统结构，简单并且可靠地保证在信息处理装置上执行的代码的正当性。

如果简单地说明该主要特征，则存储器管理单元 10 预先存储用于验证代码的正当性而使用的验证钥。而后，处理器 1 当在存储器 2 中存储代码时，把赋予该代码的验证信息存储到验证信息用存储器 3

中。这样，当对于存储在存储器 2 中的代码由处理器 1 可以执行的情况下，存储器管理单元 10 使用预先存储的验证钥以及被存储在验证信息用存储器 3 中的验证信息，验证代码的正当性。而后，进行控制以使当正当性得到验证的情况下，进行表示存储器 2 是有效的设定，当正当性未得到验证的情况下，不进行表示存储器 2 是有效的设定。

因此，对于因在安装前或者安装后被恶意的第三者篡改，在安全性上存在问题的代码，在代码执行前之际（即把从虚拟页向物理页的地址变换设置为有效的时间），因为由对恶意的第三者来说触及不到的硬件的存储器管理单元 10 可靠地进行表示代码是不正当的验证，可以避免由处理器 1 的执行。另外，具有这样的验证功能的存储器管理单元 10 因为不需要变更处理器和存储器的系统结构，所以与开发具有验证功能的处理器 1 和存储器 2 相比，可以简单地开发。

因此，如果采用本实施方式 1 的存储器管理单元 10 则可以发挥不改变处理器 1 和存储器 2 的系统结构，就可以简单并且可靠地保证在信息处理装置上执行的代码的正当性的上述的主要特征。

在此，在说明存储器管理单元 10 的构成的前，简单地说明本实施方式 1 中的地址空间。图 3 是用于说明本实施方式 1 中的地址空间的图。涉及本实施方式 1 的存储器管理单元 10 在由处理器 1 执行代码时，把从处理器 1 输入的虚拟地址变换为作为存储器 2 上的地址的物理地址，对存储器 2 输出该变换后的物理地址。即，适用涉及本实施方式 1 的存储器管理单元 10 的信息处理装置是个人计算机、工作站或者移动通信终端等，从虚拟地址向物理地址进行地址变换的系统。

而后，本实施方式 1 中的地址空间例如如图 3 所示，是通过在地址变换虚拟地址空间的上位一半后，分配给存储器 2（例如，每 4Kbytes 地被分配），不变换虚拟地址空间的下位一半，而分配给验证信息用存储器 3 而形成的。但是，在同一图中，为了便于说明，把虚拟地址空间分为上位和下为的一半，另外，通常不进行地址变换省略设置在存储器 2 上的 OS（Operating System）。

另外，在图 1 所示的系统中，分别设置存储器 2 和验证信息用存

储器 3，但也可以这样构成系统，即，通过向特定的 I/O 口输出值，把存储器 2 的一部分置换为验证信息用存储器 3（即，作为存储体切换形式），另外，也可以构成为把验证用存储器 3 不是分配在存储器空间上而是分配在 I/O 空间上。

另外，在本实施方式 1 中，说明了把作为存储器 2 的分配单位的单位存储器作为 4Kbytes 固定长度的页，但也可以把此单位存储器设置为可变长，进而，也可以把存储器 2 全体设置为 1 个单位存储器。

[实施方式 1：存储器管理单元的构成]

以下说明图 1 所示的存储器管理单元的构成。图 2 是展示涉及本实施方式 1 的存储器管理单元 10 的构成的方框图。如该图所示，该存储器管理单元 10 由页表 11、地址变换单元 12、执行/有效位设定单元 13、验证钥设定单元 14、检验钥保持单元 15、验证单元 16 组成。进而，验证钥保持单元 15 与权利要求所述的“验证钥存储装置”对应，验证单元 16 与权利要求所述的“验证装置”对应，执行/有效位设定单元 13 与权利要求所述的“控制装置”对应。

其中，页表 11 是在处理器 1 存储代码时，由处理器 1 获得的多个入口组成的表。另外，该入口为在作为存储器分配单位的每 4Kbytes 页地被准备，如图 2 所示，由开始虚拟地址、开始物理地址、执行位以及有效位组成。

即，所谓入口表示把从“开始点物理地址”开始的 4Kbtes 的物理页与从“开始点虚拟地址”开始的 4Kbtes 的虚拟页对应。而后，“执行位”表示在对应的物理/虚拟页中不存储数据而存储有代码，另外，“有效位”表示对应的物理/虚拟页有效。另外，页可以不是固定长而是可变长，但在这种情况下，在入口中存储表示大小的信息。

地址变换单元 12 是按照页表 11 把虚拟地址变换为物理地址的处理单元。具体地说，在由处理器 1 执行代码时，从页表 11 中搜索与从处理器 1 输入的虚拟地址相当的入口，当相应的入口存在的情况下，变换为对应的物理地址向存储器 2 输出，另一方面，当该入口不存在的情况下，向处理器 1 通知地址变换例外。

进而，在页表 11 的相应的入口中，当执行位以及有效位被设定的情况下，只允许用于向对应的物理/虚拟页的代码（机械命令）的读取的读出，不允许用于写入、数据访问的读写的动作。

执行/有效位设定单元 13 是根据后述的验证单元 16 的验证结果，设定页表 11 对应的入口内的执行位以及有效位的处理单元。具体地说，当用验证单元 16 验证了代码的正当性的情况下，设定执行位以及有效位（进行表示存储有验证对象的代码的物理/虚拟页是有效的设定），允许处理器 1 执行代码。进而，当用验证单元 16 未验证到代码的正当性的情况下，不设定执行位以及有效位，拒绝由处理器 1 执行代码。

验证钥设定单元 14 是对验证钥保持单元 15 从存储器管理单元 10 的外部进行验证钥的输入输出的处理单元，验证钥保持单元 15 是保持在验证单元 16 的代码的验证中使用的验证钥存储单元，验证单元 16 是在把代码存储到存储器 2 中可以由处理器 1 执行的情况下，使用被存储在验证钥保持单元 15 中的验证钥以及被存储在验证信息用存储器 3 中的验证信息，验证代码的正当性的处理单元。

即，验证单元 16 如果对于页表 11 的规定入口，若从处理器 1 接收执行/有效位的设定指示，则在从验证信息用存储器 3 读出赋予存储器 2 对应的物理页上的代码的验证信息的同时，从验证钥保持单元 15 中读出与此代码对应的验证钥，用此验证信息以及验证钥验证是否是保证了正当性的安全代码。进而，对于验证方式和验证钥可以采用，例如包含在基于公开钥技术的电子署名和在证明书中的公开钥等，可以保证代码不被第三者篡改的所有的方法。

而后，验证单元 16 当进行了表示代码是正当的验证的情况下，对执行/有效位设定单元 13 指示执行/有效位的设定，另一方面，当未进行表示代码是正当的验证的情况下，对执行/有效位设定单元 13 不指示执行/有效位的设定，对处理器 1 通知例外。这样，当通知处理器 1 例外的情况下，拒绝由处理器 1 执行代码。

另外，近年的系统外表上看并行执行多个任务（程序），即大多

在多任务下工作，在这种情况下，在任务的切换时，通过验证钥设定单元 14 的控制，把存储在验证钥保持单元 15 中的验证钥更换为与任务相应的验证钥。

[实施方式 1：系统的处理顺序]

以下，说明用本实施方式 1 的系统所执行的处理的顺序。在此，作为系统的处理，说明用处理器 1 把代码存储到存储器 2，直至用存储器管理单元 10 设定执行/有效位的处理。

图 4 是用于说明本实施方式 1 的系统处理的流程图。如该图所示，首先最初，处理器 1 在从处理器管理单元 10 的页表 11 中获得未使用的入口的同时，从存储器 2 获得未使用的物理页（步骤 S401 以及 S402）。而后，处理器 1 在获得的入口中，设定开始点虚拟地址以及开始点物理地址（步骤 S403）。

接着，处理器 1 从硬盘等的数据存储单元（盘）中读入代码，在把该代码存储到在步骤 S402 中获得的物理页中的同时，把赋予该代码的验证信息存储到验证信息用存储器 3（步骤 S404 以及 S405）。而后，处理器 1 向存储器管理单元 10 指示执行/有效位的设定（步骤 S406）。

另一方面，接收到这样的设定指示的存储器管理单元 10 在从验证信息用存储器 3 中读出与设定指示相关的代码的对应的验证信息的同时，从验证钥保持单元 15 读入与该验证信息对应的验证钥（步骤 S407 以及 S408）。而后，存储器管理单元 10 的验证单元 16 用读入的验证信息以及验证钥，验证与设定指示有关的代码的正当性（步骤 S409）。

通过此验证，当进行了表示代码是正当的验证的情况下（步骤 S410 肯定），验证单元 16 对执行/有效位设定单元 13 指示执行/有效位的设定，执行/有效位设定单元 13 在与验证对象的代码有关的页表 11 内的入口中设定执行位以及有效位（步骤 S411）。由此，对于作为验证对象的代码允许由处理器 1 执行。

与此相反，当未进行表示代码是正当的验证的情况下（步骤 S410

否定），验证单元 16 对执行/有效位设定单元 13 不指示执行/有效位的设定，而对处理器 1 通知例外（步骤 S412）。因而，对于作为验证对象的代码，拒绝由处理器 1 的执行。

如上所述，如果采用本实施方式 1，则存储器管理单元 10 把为了验证代码的正当性所使用的验证钥存储到验证钥保持单元 15。而后，当代码被存储在存储器 2 中并可以由处理器 1 执行的情况下，使用被存储在验证钥保持单元 15 中的验证钥以及被附在代码上的验证信息（被存储在验证信息用存储器 3 上的验证信息）进行控制，以验证代码的正当性，当正当性得到验证的情况下，进行表示存储器 2 是有效的设定，当正当性未得到验证的情况下，不进行表示存储器 2 是有效的设定。因而，不变更处理器 1 和存储器 2 的系统结构，就可以简单并且可靠地保证在信息处理装置上执行的代码的正当性。

（实施方式 2）

在上述的实施方式 1 中，说明了把从处理器 1 输入的虚拟地址变换为物理地址向存储器 2 输出的存储器管理单元 10，但本发明并不限于此，对于不变更从处理器 1 输入的虚拟地址，作为物理地址向存储器 2 输出的存储器管理单元也同样可以适用。

即，在上述实施方式 1 中，说明了适用到个人计算机、工作站或者移动通信终端等，进行从虚拟地址到物理地址的地址变换的信息处理装置的存储器管理单元 10，但对于 PHS 终端、便携终端或者 PDA 等，进行从虚拟地址向物理地址的地址变换的信息处理装置，也可以同样适用。

因而，在本实施方式 2 中，说明关于不进行从虚拟地址到物理地址的地址变换的系统所适用的存储器管理单元。图 5 是展示涉及本实施方式 2 的存储器管理单元构成的方框图，图 6 是用于说明在本实施方式 2 中的地址空间的图。另外，在和上述实施方式 1 所示的各部分具有同样功能的部位上标注同一符号，并省略其详细说明。

涉及本实施方式 2 的存储器管理单元 20 如上所述，是不变更从处理器 1 输入的虚拟地址，作为物理地址向存储器 2 输出的单元。即，

如图 6 所示，本实施方式 2 中的地址空间与图 2 所示的实施方式 1 中的地址空间不同，虚拟地址和物理地址一致。

另外，存储器管理单元 20 如图 5 所示，不存在把虚拟地址变换为物理地址的处理单元（图 2 所示的地址变换单元 12），即使在页表 21 的各入口中，也不存在开始点虚拟地址，只存在开始点物理地址。另外，页表 21 内的入口只存在物理页的个数。

因而，此存储器管理单元 20 在处理器 1 执行代码时，把从处理器 1 输入的虚拟地址作为是存储器 2 上的地址的物理地址向存储器 2 输出。进而，此存储器管理单元 20 的验证处理和图 4 所示的存储器管理单元 10 的处理（同一图步骤 S407~S412）一样。

这样，如果采用本实施方式 2 的存储器管理单元 20，则即使对于 PHS 终端、便携终端或者 PDA 等，关于不进行从虚拟地址向物理地址的地址变换的信息处理装置，也可以不变更处理器 1 和存储器 2 的系统结构，简单并且可靠地保证在信息处理装置上执行的代码的正当性。

（实施方式 3）

在上述的实施方式 1 以及 2 中，说明了用在代码执行前验证代码的正当性的存储器管理单元 10 或者 20，简单并且可靠地保证代码的正当性的情况，但通过在执行前译码预先加密的代码，也可以和实施方式 1 以及 2 一样，简单并且可靠地保证代码的正当性。

因而，在本实施方式 3 中，说明通过在执行前译码预先加密的代码，简单并且可靠地保证代码的正当性的存储器管理单元。进而，在此，在说明了适用本实施方式 3 的存储器管理单元的系统概要以及主要特征后，说明存储器管理单元的构成，最后说明采用此系统的处理顺序。

[实施方式 3：系统的概要以及主要特征]

首先最初，说明适用于本实施方式 3 的存储器管理单元的系统概要以及主要的特征。图 7 是展示适用本实施方式 3 的存储器管理单元的系统构成的方框图。如该图所示，此系统在处理器 1、存储器 2 之

间设置存储器管理单元 30，把它们通过地址总线 4 以及数据总线 5 连接而构成。进而，在与上述实施方式 1 所示的各部分具有相同功能的部位上标注同一符号，并省略其详细声明。

图 7 所示的系统大致和图 1 所示的系统一样，是用处理器 1 执行被存储在存储器 2 中的代码的系统，但和图 1 所示的系统比较，不存在验证信息用存储器 3 这一点，和具备与同一图所示的存储器管理单元 10 功能不同的存储器管理单元 30 这一点不同。即，在本实施方式 3 中其主要特征在于：代码预先被加密，存储器管理单元 30 通过译码预先被加密的代码，不变更处理器 1 和存储器 2 的系统结构，就可以简单并且可靠地保证在信息处理装置上执行的代码的正当性。

如果简单说明此主要特征，则存储器管理单元 30 预先存储用于译码被加密的代码的译码钥，当处理器 1 在存储器 2 中存储被加密的代码的情况下，对此存储着的代码试行采用译码钥的译码。而后，在把此译码后的代码再存储在存储器 2 中的同时，通过进行表示存储器 2 是有效的设定，允许处理器 1 执行代码。进而，当被加密的代码未被译码的情况下，不进行表示存储器 2 是有效的设定，拒绝由处理器 1 的代码执行。

因此，在代码执行前之际（即，把从虚拟页向物理页的地址变换设置为有效的时间），因为用对于恶意的第三者来说是触及不到的硬件的存储器管理单元 30 将加密的代码进行译码，所以对于经译码的代码，可以作为担保了正当性的代码（在安装前或者安装后未被恶意的第三者篡改的代码）而执行。另外，具有这样译码功能的存储器管理单元 30 因为不需要变更处理器 1 和存储器 2 的系统结构，所以与开发具有译码功能的处理器 1 和存储器 2 相比，可以简单地开发。

由此，如果采用本实施方式 3 的存储器管理单元 30，则不变更处理器 1 和存储器 2 的系统结构，就可以简单并且可靠地保证在信息处理装置上执行的代码的正当性这一上述主要特征，可以和实施方式 1 以及 2 的存储器管理单元 10、20 发挥同样效果。

并且，在本实施方式 3 中，存储器管理单元 30 和实施方式 1 的

存储器管理单元 10 一样，把从处理器 1 输入的虚拟地址变换为物理地址向存储器 2 输出。即，此存储器管理单元 30 可以适用在个人计算机、工作站或者移动通信终端等，从虚拟地址向物理地址进行地址变换的信息处理装置，本实施方式 3 中的地址空间和图 3 所示的一样。

[实施方式 3：存储器管理单元的构成]

以下，说明图 7 所示的存储器管理单元 30 的构成。图 8 是展示涉及本实施方式 3 的存储器管理单元 30 构成的方框图。如该图所示，此存储器管理单元 30 由页表 31、地址变换单元 32、执行/有效位设定单元 33、译码钥设定单元 34、译码钥保持单元 35、译码单元 36 组成。并且，译码钥保持单元 35 与权利要求所述的“译码钥存储单元”对应，译码单元 36 与权利要求所述的“译码装置”对应，执行/有效位设定单元 33 与权利要求所述的“控制装置”对应。

这其中，页表 31 以及地址变换单元 32 起到和在上述实施方式 1 中说明的页表 11 以及地址变换单元 12 分别相同的效果。

执行/有效位设定单元 33 起到了和在实施方式 1 中说明的执行/有效位设定单元 33 大致同样的效果，但对应于译码单元 36 的处理，设定页表 31 对应的入口内的执行位以及有效位这一点不同。即，执行/有效位设定单元 33 用译码单元 36 译码代码，如果把译码后的代码再存储到存储器 2 中，则设定页表 31 对应的入口内的执行位以及有效位（进行表示存储有译码了的代码的物理/虚拟页是有效的设定）。

译码钥设定单元 34 对译码钥保持单元 35 来说，是从存储器管理单元 30 的外部进行译码钥的输入输出的处理单元，译码钥保持单元 35 是保持将加密的代码进行译码时所使用的译码钥的存储单元，译码单元 36 是在把加密的代码存储到存储器 2 中的情况下，使用被存储在译码钥保持单元 35 中的译码钥，将加密的代码进行译码的处理单元。

即，译码单元 36 如果对于页表 31 的规定输入，若从处理器 1 接收执行/有效位的设定指示，则在读出存储器 2 对应的物理页上的加密了的代码的同时，从译码钥保持单元 35 中读出与此代码对应的译码钥，使用译码钥译码所加密的代码。并且，对于加密以及译码的方式，

例如可以采用所谓的共用钥加密方式、公开钥加密方式等任意的方法。

而后，译码单元 36 当进行代码译码的情况下，在把译码后的代码再存储到存储器 2 中的同时，对执行/有效位设定单元 33 指示执行/有效位的设定。

另外，近年的系统在外表上看并行执行多个任务（程序），即大多在多任务下动作，在这种情况下，在任务的切换时，通过译码钥设定单元 34 的控制，把存储在译码钥保持单元 35 中的译码钥更换为与任务相应的译码钥。

[实施方式 3：系统的处理顺序]

以下，说明用本实施方式 3 的系统所执行的处理的顺序。在此，作为系统的处理，说明用处理器 1 把加密后的代码存储到存储器 2，直至用存储器管理单元 30 设定执行/有效位的处理。

图 9 是用于说明本实施方式 3 的系统处理的流程图。如该图所示，首先最初，处理器 1 在从处理器管理单元 30 的页表 31 中获得未使用的入口的同时，从存储器 2 获得未使用的物理页（步骤 S901 以及 S902）。而后，处理器 1 在获得的入口中，设定开始点虚拟地址以及开始点物理地址（步骤 S903）。

接着，处理器 1 从硬盘等的数据存储单元（盘）中读入被加密的代码，在把该加密后的代码存储到在步骤 S902 中获得的物理页中（步骤 S904）。而后，处理器 1 向存储器管理单元 30 指示执行/有效位的设定（步骤 S905）。

另一方面，接收到这样的设定指示的存储器管理单元 30 从与涉及设定指示的代码相对应的存储器 2 上的物理页中读入加密的代码的同时，从译码钥保持单元 35 读入与该代码对应的译码钥（步骤 S906 以及 S907）。而后，存储器管理单元 30 的译码单元 36 用译码钥译码加密的代码（S908）。

接着，存储器管理单元 30 的译码单元 36 把译码后的代码再存储到存储器 2 中的同时，对执行/有效位设定单元 33，指示执行/有效位的设定（步骤 S909），执行/有效位设定单元 33 在与译码对象的代码

有关的页表 31 内的入口中，设定执行位以及有效位（步骤 S910）。由此，对于作为译码对象的代码，允许由处理器 1 执行。

如上所述，如果采用本实施方式 3，则存储器管理单元 30 把为了将加密的代码进行译码所使用的译码钥存储到译码钥保持单元 35。而后，当用处理器 1 把经加密的代码存储在存储器 2 中的情况下，从存储器 2 读出经加密的代码，使用被存储在译码钥保持单元 35 中的译码钥进行译码再存储到存储器 2，进而，进行表示再存储译码了的代码的存储器 2 是有效的设定。因而，和上述的实施方式 1 以及 2 一样，不变更处理器 1 和存储器 2 的系统结构，就可以简单并且可靠地保证在信息处理装置上执行的代码的正当性。

（实施方式 4）

在上述实施方式 3 中，说明了把从处理器 1 输入的虚拟地址变换为物理地址向存储器 2 输出的存储器管理单元 30，但本发明并不限于此，不变换从处理器 1 输入的虚拟地址，对于作为物理地址向存储器 2 输出的存储器管理单元，也可以同样适用。即，和上述实施方式 2 一样，即使是 PHS 终端、便携终端或者 PDA 等，不进行从虚拟地址向物理地址的地址变换的信息处理装置，也可以同样适用。

因而，在本实施方式 4 中，说明对不进行从虚拟地址向物理地址的地址变换的系统所适用的，和上述实施方式 3 发挥一样效果的存储器管理单元。图 10 是展示涉及本实施方式 4 的存储器管理单元构成的方框图。进而，在和上述实施方式 3 所示的各部分具有同样功能的部分上标注相同的符号，并省略其详细说明。

涉及本实施方式 4 的存储器管理单元 40 如上所述，不变更从处理器 1 输入的虚拟地址，就可以作为物理地址向存储器 2 输出。即，和图 6 所示一样，本实施方式 4 的地址空间是虚拟地址和物理地址相一致的情况。

另外，存储器管理单元 40 如图 10 所示，不存在把虚拟地址变换为物理地址的处理单元（图 8 所示的地址变换单元 32），即使在页表 41 的各入口中，也是不存在开始点虚拟地址，只存在开始点物理地址。

并且，页表 41 内的入口只存在物理页的个数。

因而，该存储器管理单元 40 与上述实施方式 2 的存储器管理单元 20 一样，在处理器 1 执行代码时，把从处理器 1 输入的虚拟地址作为是存储器 2 上的地址的物理地址向存储器 2 输出。进而，该存储器管理单元 40 的译码处理和图 9 所示的存储器管理单元 30（涉及实施方式 3 的存储器管理单元 30）的处理（同一图步骤 S906~S910）一样。

这样，如果采用本实施方式 4 的存储器管理单元 40，则即使对于 PHS 终端、便携终端或者 PDA 等，不进行从虚拟地址向物理地址的地址变换的信息处理装置，也和上述实施方式 3 一样，可以不变更处理器 1 和存储器 2 的系统结构，简单并且可靠地保证在信息处理装置上执行的代码的正当性。

（其他实施方式）

至此说明了本发明的实施方式，但本发明即使在上述的实施方式以外，也可以在权利要求范围所述的技术思想的范围内以各种不同的实施方式实施。

例如，在本实施方式 1 以及 2 中，说明了在存储器管理单元 10 或者 20 上追加验证功能的情况，但本发明并不限于此，也可以只把承担验证功能的硬件（与权利要求范围所述的“代码验证装置”对应）与存储器管理单元 10 或者 20 另行设置，这种硬件和存储器管理单元 10 以及 20 的协同动作，进行代码的验证。

同样，在本实施方式 3 以及 4 中，说明了在存储器管理单元 30 或者 40 中追加了译码功能的情况，但本发明并不限于此，也可以只把承担译码功能的硬件（与权利要求范围所述的“代码译码装置”对应）与存储器管理单元 30 或者 40 另行设置，这种硬件和存储器管理单元 30 以及 40 的协同动作，进行代码的验证。

另外，在本实施方式中说明的各种处理中，可以手动地进行作为自动进行的已说明的处理的全部或者一部分，或者，也可以用公知的方法自动地进行作为手动进行的已说明的处理的全部或者一部分。此外，对于包含在上述文件中和画面中展示的处理顺序、控制顺序、具

体名称、各种数据和参数的信息，除了特定的情况外可以任意变更。同样，即使是各种输入用画面的内容，也可以任意变更。

另外，图示的各装置的各构成要素是功能概念性要素，实际上不一定如图那样构成。即，各装置的分散/综合的具体形态并不限于图示的情况，可以根据各种负荷和使用状况把其全部或者一部分，以任意单位在功能上或者物理上分散/综合构成。进而，在各装置中进行的各处理功能其全部或者任意一部分用 CPU 以及由该 CPU 解析执行的程序实现，或者可以作为采用布线逻辑的硬件实现。

如上所述，如果采用本发明，因为对于在安装前或者安装后因为被恶意的第 3 者篡改而在安全性上存在问题的代码，在代码的执行前的之际（即，把从虚拟页向物理页的地址变换设置为有效的时刻），使用作为对恶意的第三者来说触及不到的硬件的存储器管理单元，可靠地进行表示代码是不正当的验证，所以可以避免由处理器执行。另外，具有这样的验证功能的存储器管理单元因为不需要变更处理器和存储器的系统结构，所以与开发具有验证功能的处理器和存储器相比，可以简单地开发。因而，可以得到不变更处理器和存储器的系统结构，就可以简单并且可靠地保证在信息处理装置上执行的代码的正当性的效果。

另外，如果采用本发明，则在代码执行前之际，因为用对于恶意的第三者来说是触及不到的硬件的存储器管理单元将加密的代码进行译码，所以对于被译码后的代码，可以作为担保了正当性的代码（在安装前或者安装后未被恶意的第三者篡改的代码）执行。另外，具有这样的译码功能的存储器管理单元因为不需要变更处理器和存储器的系统结构，所以与开发具有译码功能的处理器和存储器相比，可以简单地开发。因而，起到了可以得到不变更处理器和存储器的系统结构，就可以简单并且可靠地保证在信息处理装置上所执行的代码的正当性的存储器管理单元的效果。

另外，如果采用本发明，则可以适用到个人计算机、工作站或者移动通信终端等，进行从虚拟地址到物理地址的地址变换的信息处理

装置，起到可以得到简单并且可靠地保证在这样的信息处理装置上执行的代码的正当性的存储器管理单元的效果。

另外，如果采用本发明，则可以适用到 PHS 终端、便携终端或者 PDA 等，进行从虚拟地址向物理地址的地址变换的信息处理装置，起到可以简单并且可靠地保证可以在这种信息处理装置上执行的代码的正当性的存储器管理单元的效果。

另外，如果采用本发明，则起到对于在信息处理装置上作为基本软件所执行的极其重要的代码，不变更处理器和存储器的系统结构，就可以简单并且可靠地保证在信息处理装置上执行的代码的正当性的代码验证装置的效果。

另外，如果采用本发明，则起到不变更处理器和存储器的系统结构，就可以简单并且可靠地保证在信息处理装置上执行的代码的正当性的代码验证装置的效果。

另外，如果采用本发明，则起到不变更处理器和存储器的系统结构，就可以简单并且可靠地保证在信息处理装置上执行的代码的正当性的代码译码装置的效果。

如上所述，本发明的存储器管理单元、代码验证装置以及代码译码装置适用于个人计算机、工作站、PSH 终端、便携终端、移动通信终端或者 PDA 等，需要保证由处理器执行的代码的正当性的信息处理装置。

图1

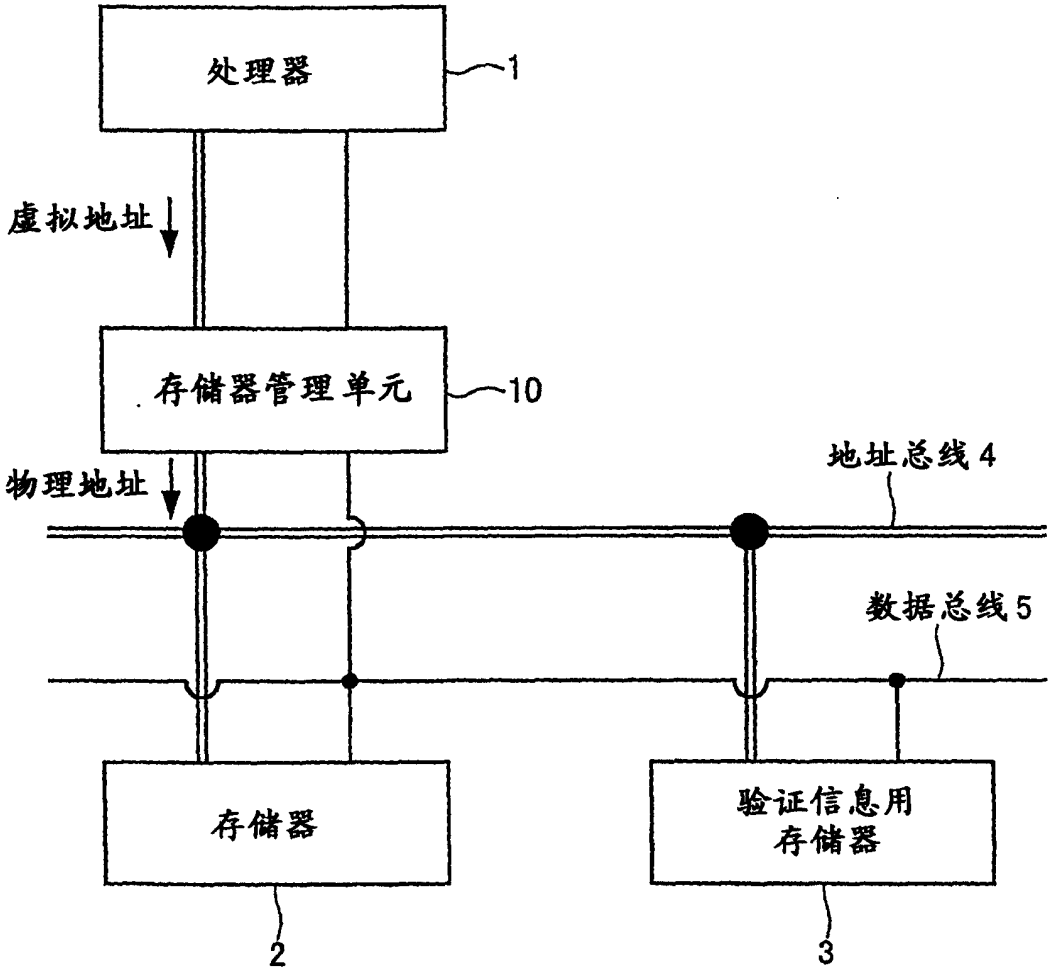


图2

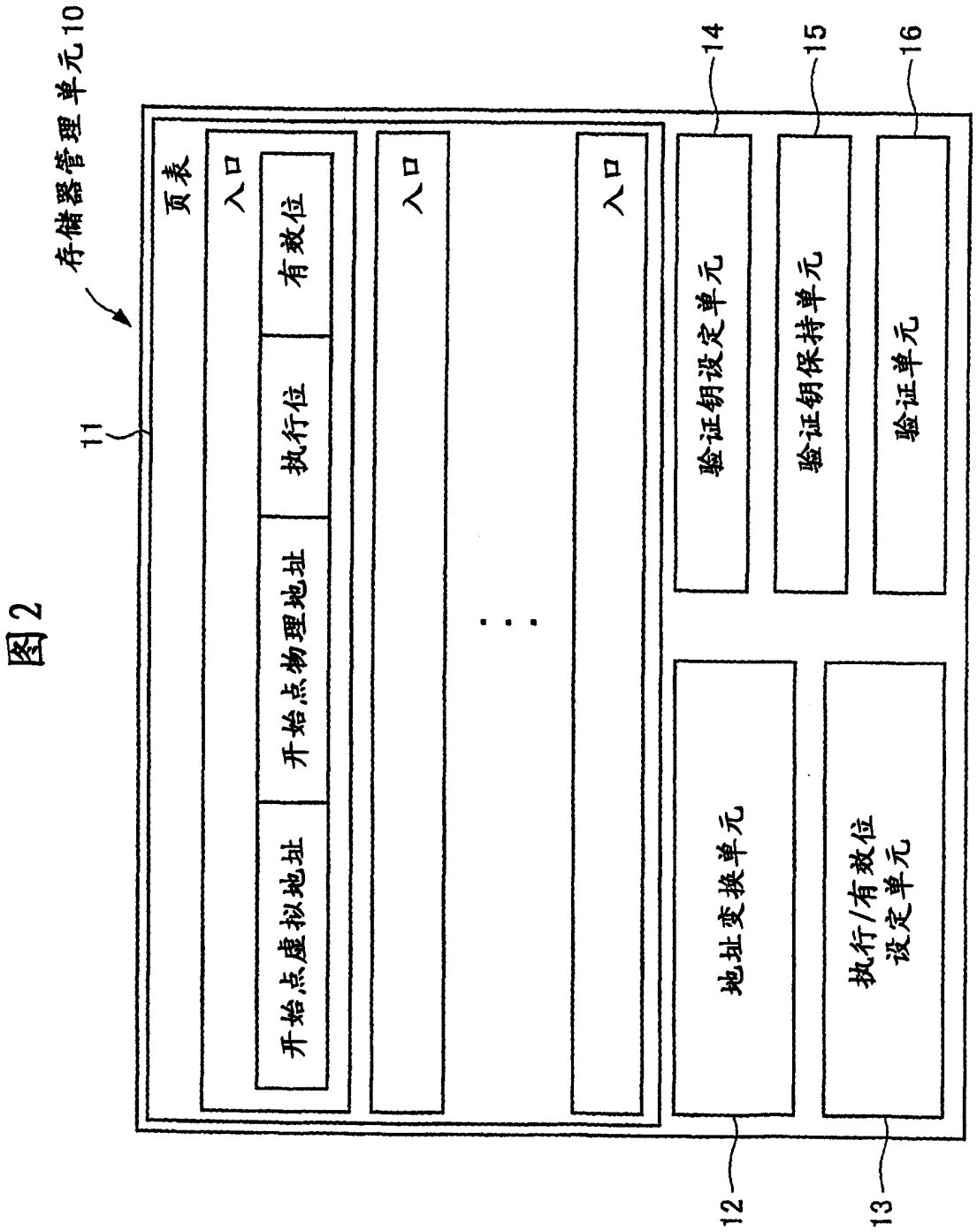

存储器管理单元10
11
页表
入口
开始点虚拟地址
开始点物理地址
执行位
有效位
入口
入口
验证钥设定单元
验证钥保持单元
验证单元
地址变换单元
执行/有效位
设定单元
12
13
14
15
16

图 3

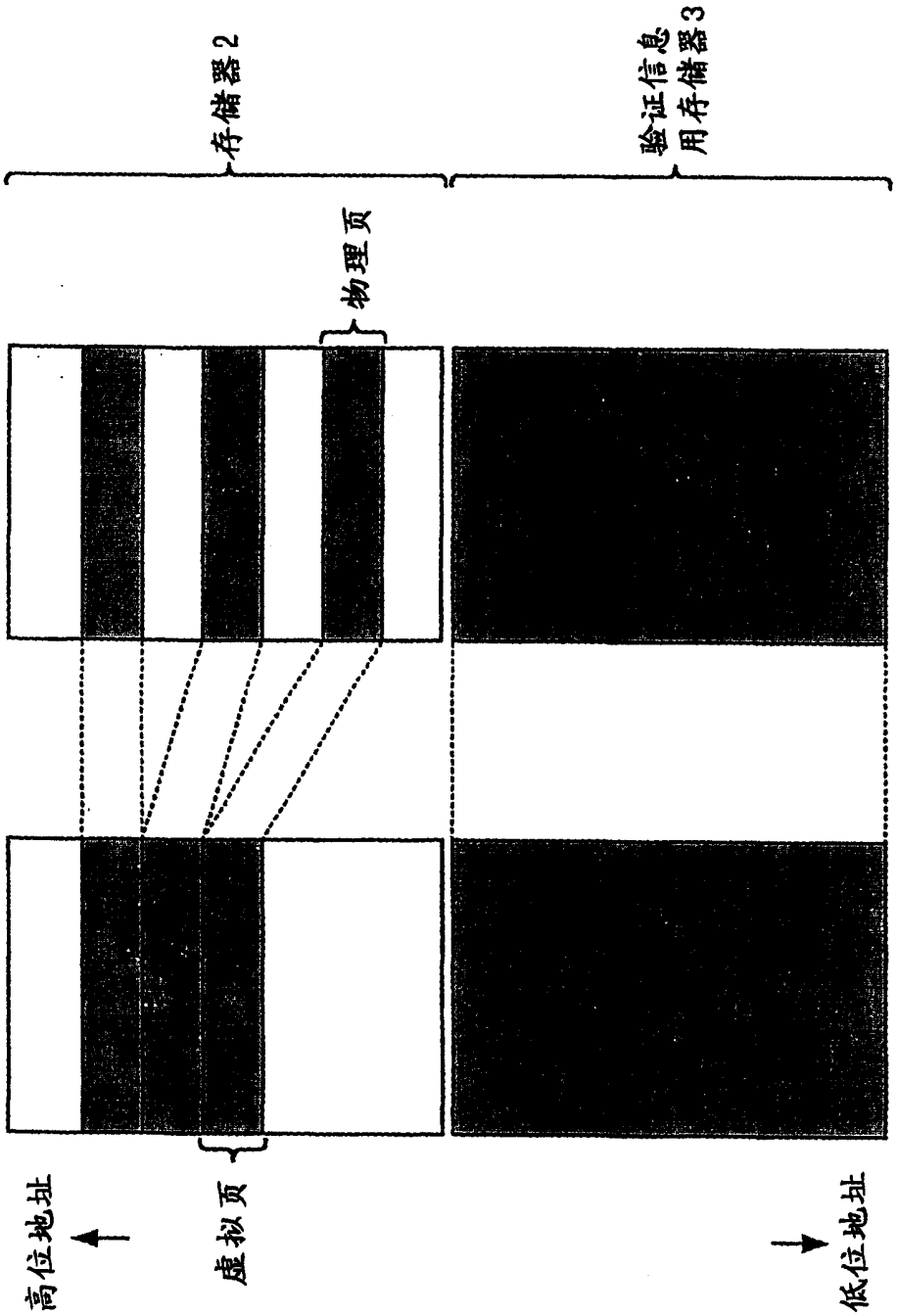


图4

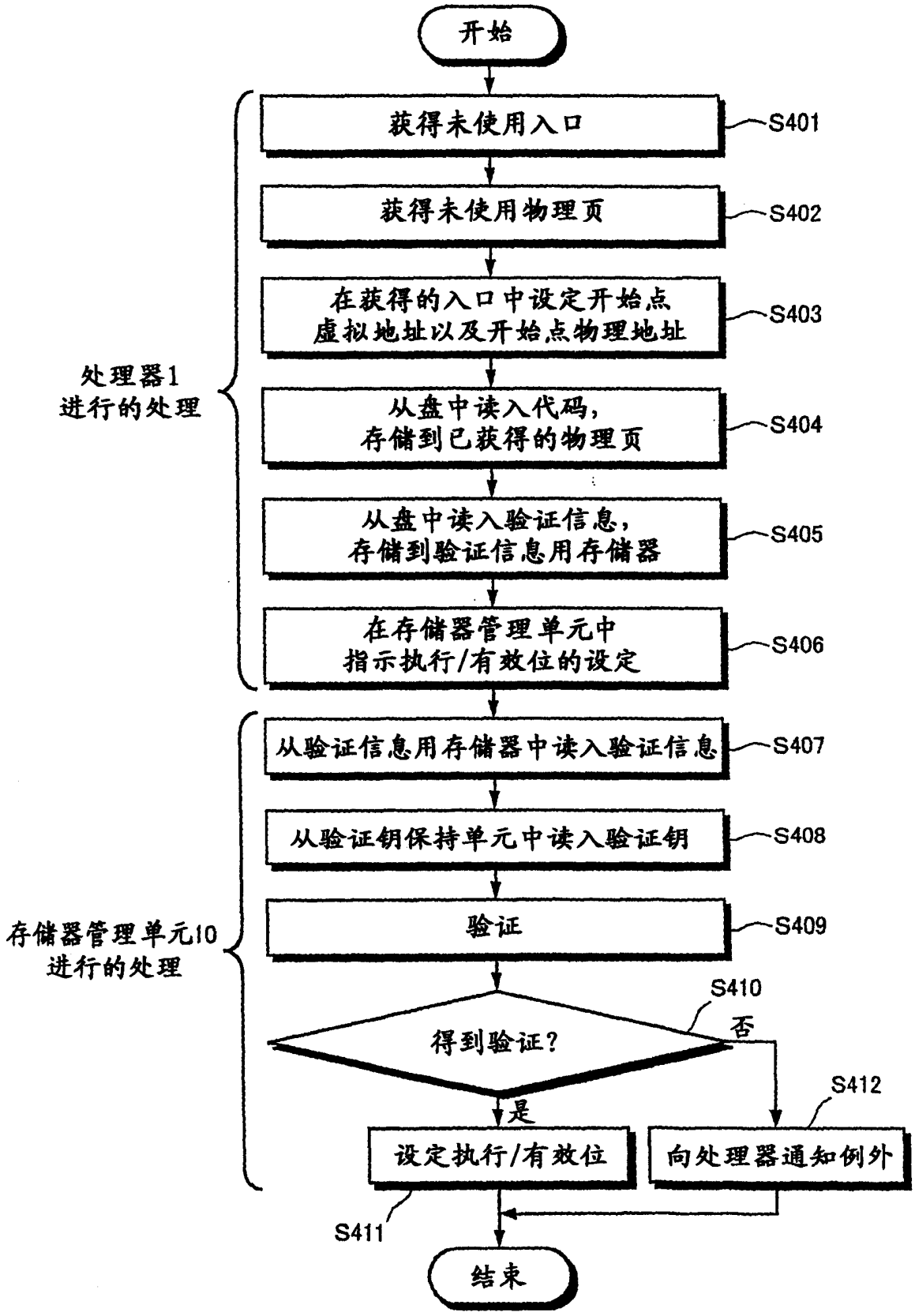

开始
获得未使用入口
S401
获得未使用物理页
S402
在获得的入口中设定开始点
虚拟地址以及开始点物理地址
S403
处理器1
进行的处理
从盘中读入代码，
存储到已获得的物理页
S404
从盘中读入验证信息，
存储到验证信息用存储器
S405
在存储器管理单元中
指示执行/有效位的设定
S406
从验证信息用存储器中读入验证信息
S407
从验证钥保持单元中读入验证钥
S408
验证
S409
存储器管理单元10
进行的处理
S410
得到验证？
否
是
S412
设定执行/有效位
向处理器通知例外
S411
结束

图 5

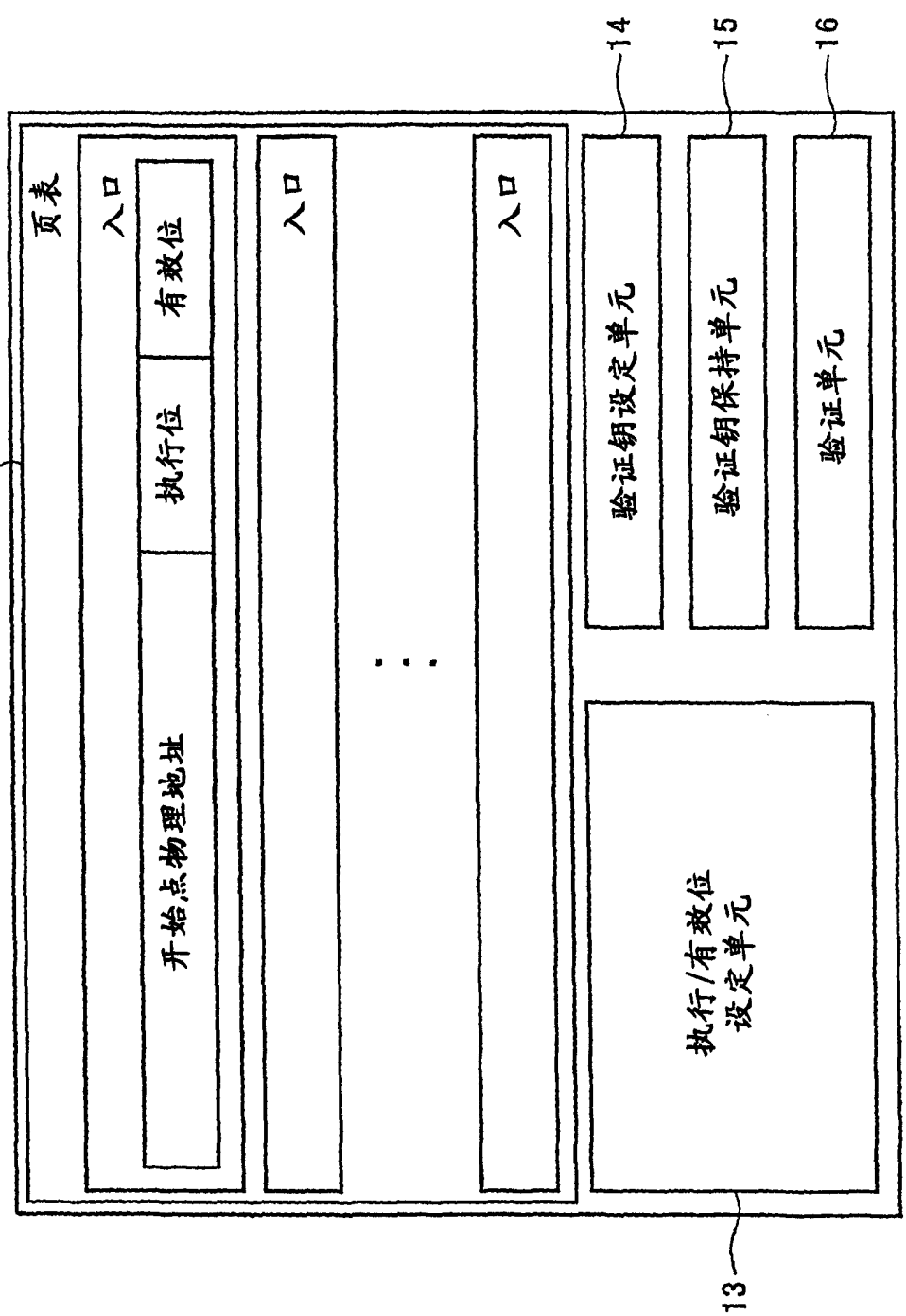

存储器管理单元 20
21
页表
入口
开始点物理地址
执行位
有效位
入口
入口
14
15
16
验证钥设定单元
验证钥保持单元
验证单元
执行/有效位
设定单元
13

图6

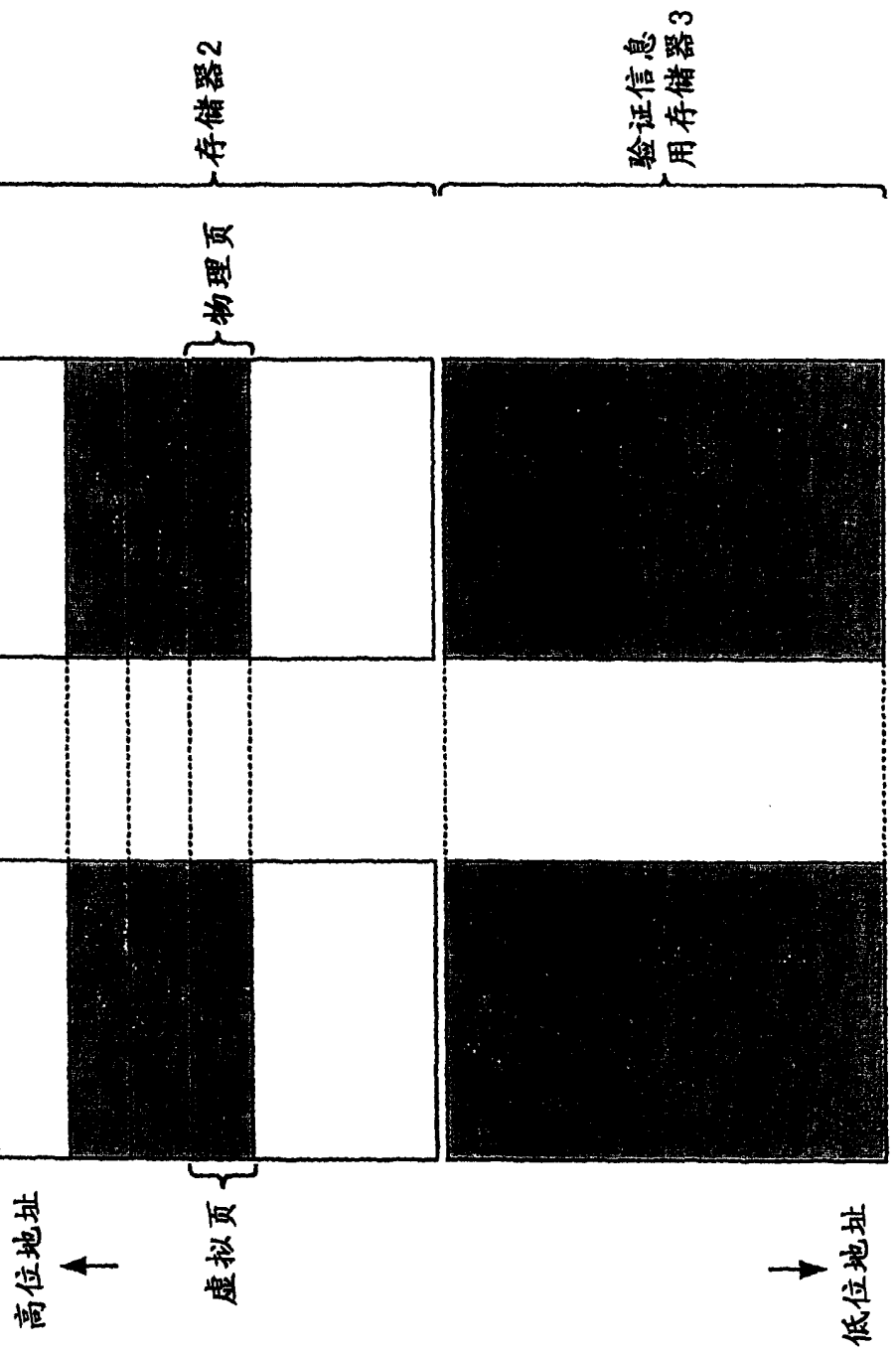


图7

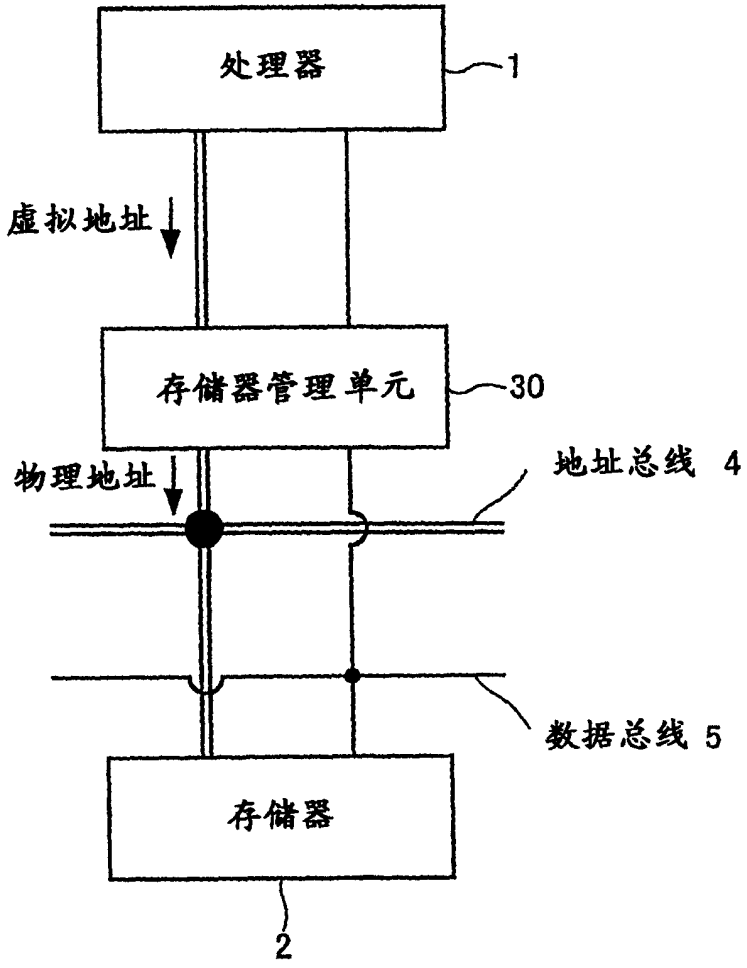


图8

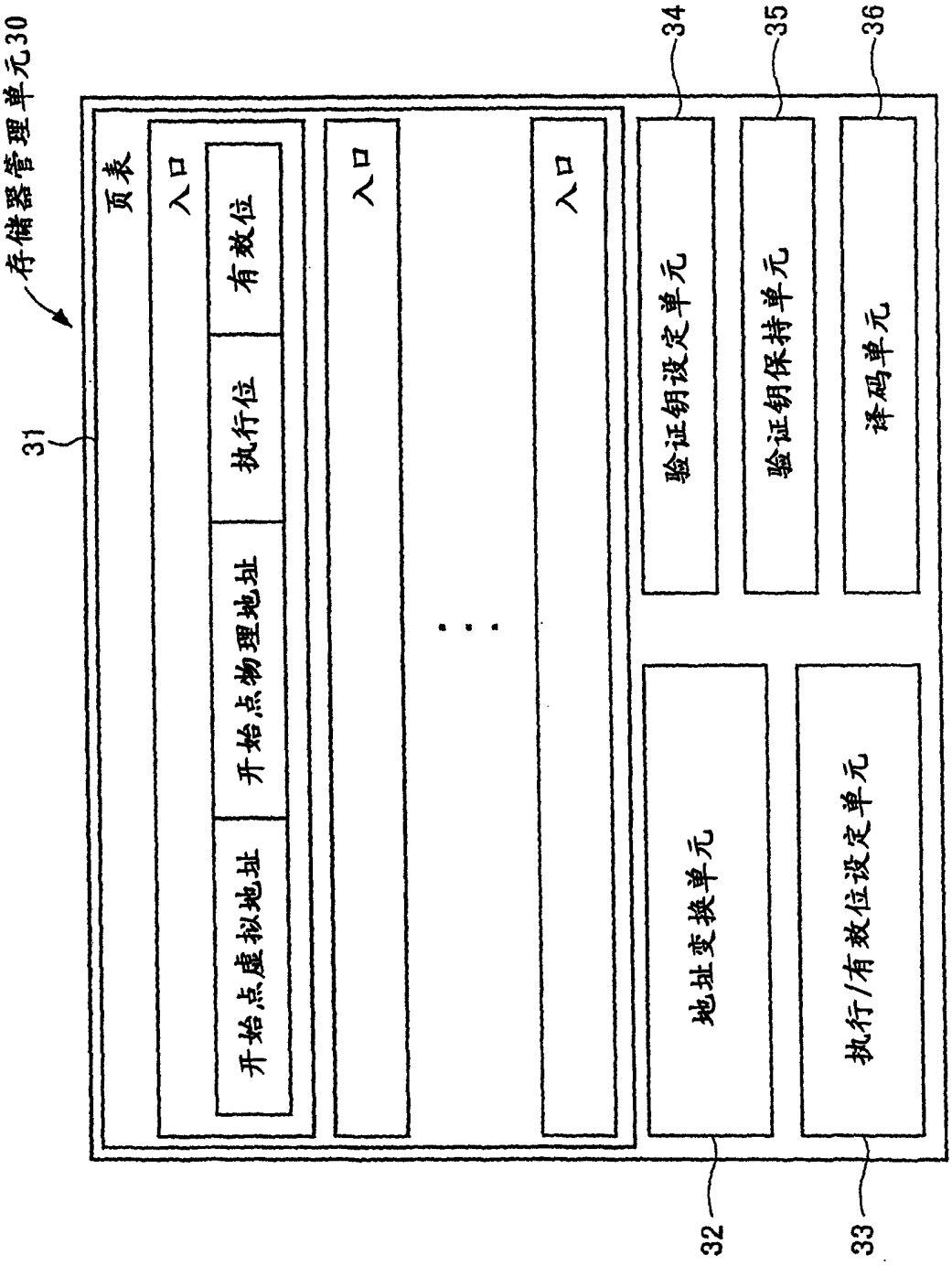

存储器管理单元30
31
页表
入口
开始点虚拟地址
开始点物理地址
执行位
有效位
入口
入口
34
35
36
验证钥设定单元
验证钥保持单元
译码单元
地址变换单元
执行/有效位设定单元
32
33

图9

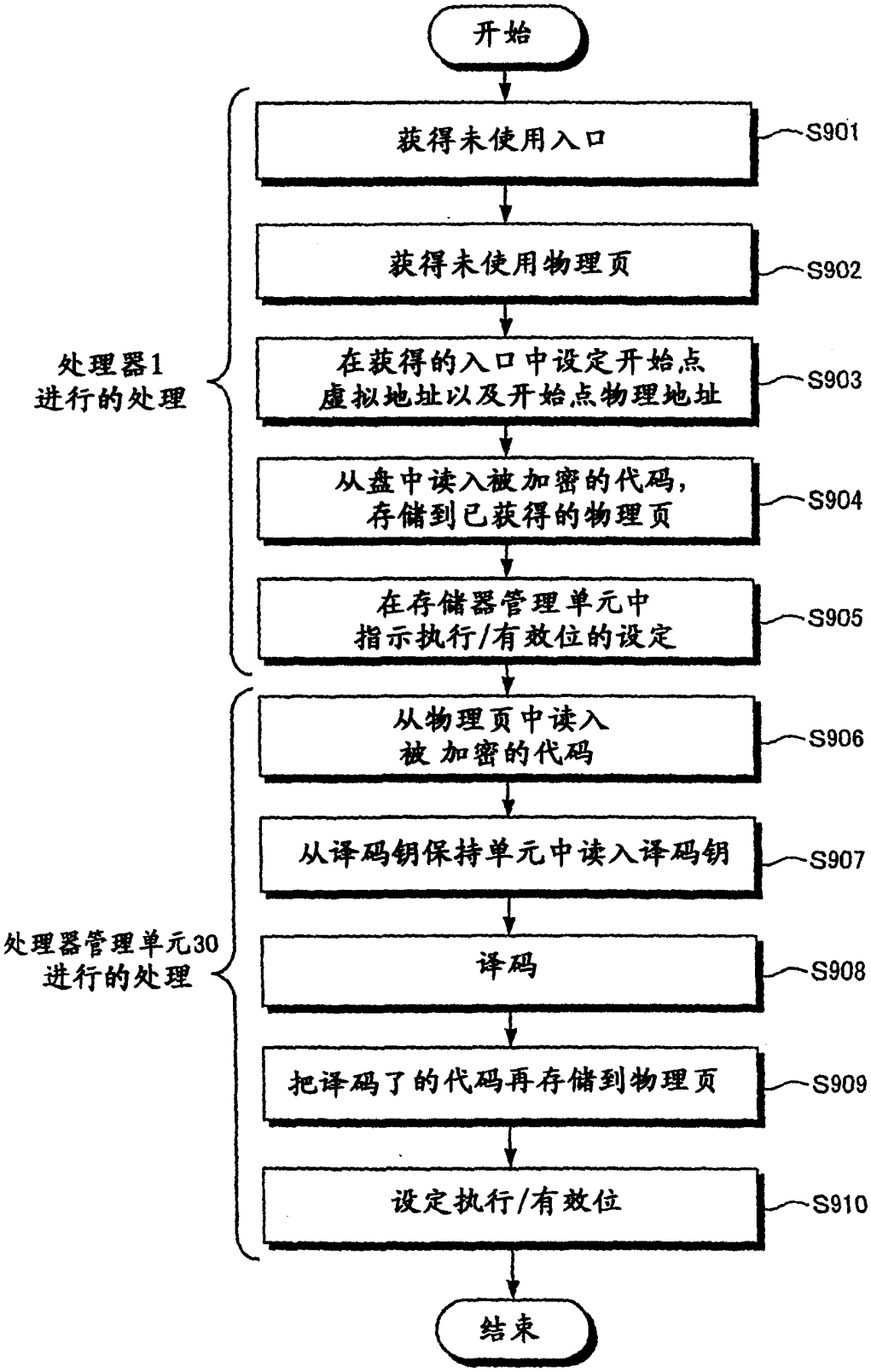
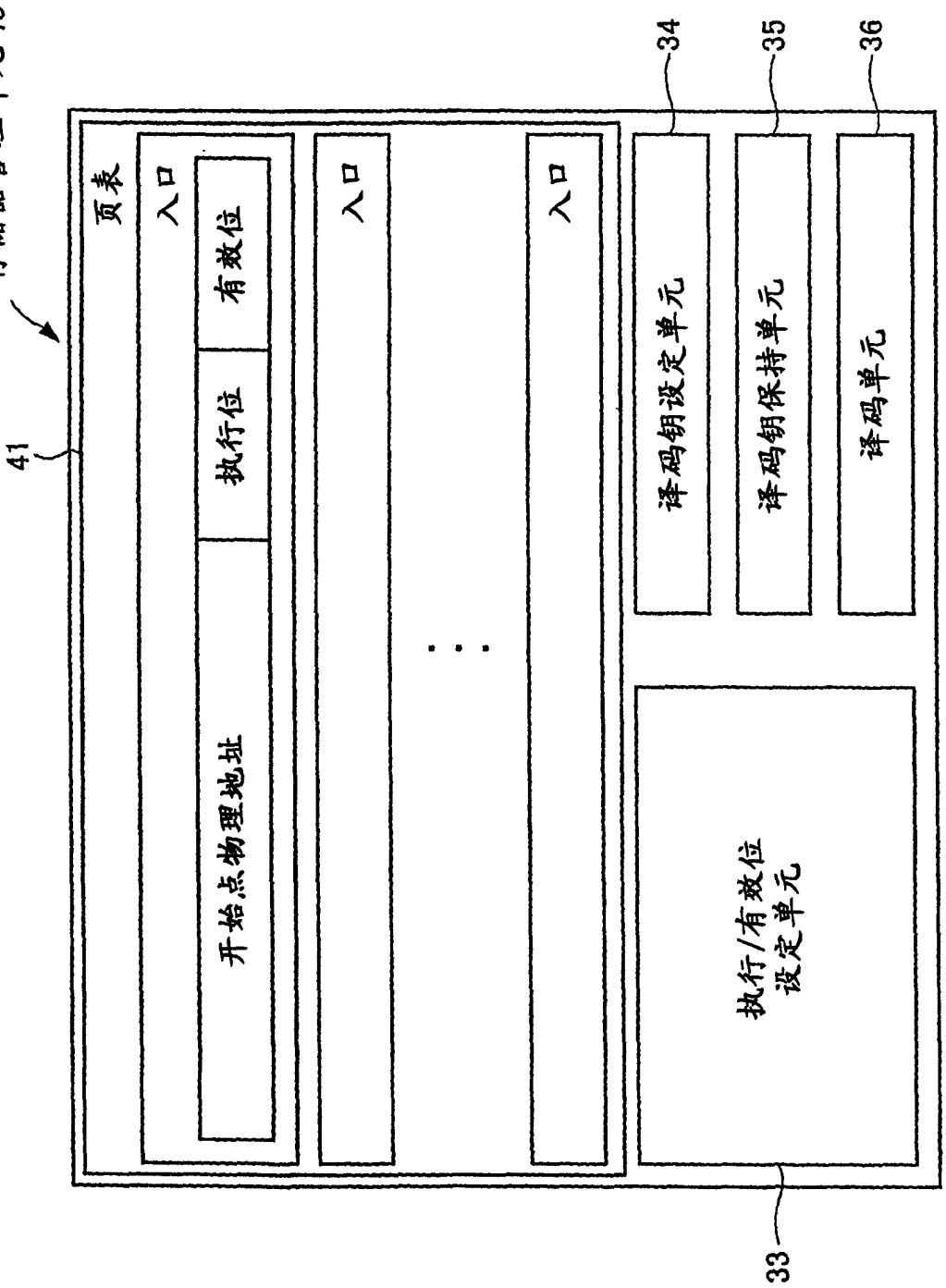

开始
获得未使用入口
S901
获得未使用物理页
S902
在获得的入口中设定开始点
虚拟地址以及开始点物理地址
S903
从盘中读入被加密的代码，
存储到已获得的物理页
S904
在存储器管理单元中
指示执行/有效位的设定
S905
处理器1
进行的处理
从物理页中读入
被 加密的代码
S906
从译码钥保持单元中读入译码钥
S907
译码
S908
把译码了的代码再存储到物理页
S909
设定执行/有效位
S910
处理器管理单元30
进行的处理
结束

图10


存储器管理单元40
41
页表
入口
开始点物理地址
执行位
有效位
入口
入口
34
35
36
译码钥设定单元
译码钥保持单元
译码单元
执行/有效位
设定单元
33