[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 3/06 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200780053273.0

[43] 公开日 2010 年 3 月 24 日

[11] 公开号 CN 101681237A

[22] 申请日 2007.6.8
[21] 申请号 200780053273.0
[86] 国际申请 PCT/JP2007/061644 2007.6.8
[87] 国际公布 WO2008/149458 日 2008.12.11
[85] 进入国家阶段日期 2009.12.8
[71] 申请人 富士通株式会社
地址 日本神奈川县
[72] 发明人 伊藤实希夫 大黑谷秀治郎
池内和彦

[74] 专利代理机构 北京三友知识产权代理有限公司
代理人 黄纶伟

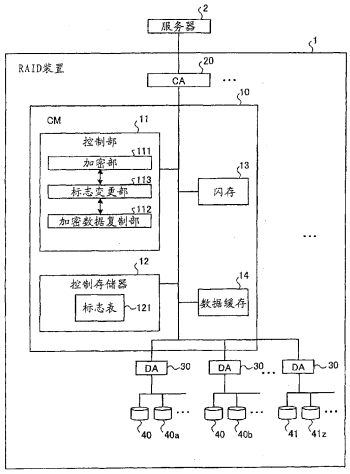
权利要求书 3 页 说明书 13 页 附图 7 页

[54] 发明名称

加密装置、加密方法以及加密程序

[57] 摘要

本发明涉及加密装置及加密方法。即使在正在加密处理时发生了故障等的情况下也可靠地重新开始加密处理。在接收加密请求后且在一个磁盘中所存储的数据的加密开始之前，标志变更部将一个磁盘的加密标志变更为正在加密，在从一个磁盘向另外的磁盘开始复制加密数据之前，标志变更部将一个磁盘的加密标志变更为加密完成，并且将其他的磁盘的加密标志变更为正在加密，在完成向其他磁盘的复制以后，标志变更部将其他磁盘的加密标志变更为加密完成。



1.一种加密装置，其对属于RAID（Redundant Array of Inexpensive Disks，独立冗余磁盘阵列）组的多个记录介质中所存储的数据进行加密，该加密装置的特征在于，

该加密装置具有：

加密单元，其对属于所述 RAID 组的多个记录介质中的一个记录介质中所存储的数据进行加密，并将其写入预定的记录介质；

变更单元，其针对每个所述记录介质而设置，对表示各个记录介质中的加密进展情况的加密变量进行变更；以及

复制单元，其将通过所述加密单元加密后的数据复制到属于所述 RAID 组的多个记录介质中的、存储有尚未加密的数据的记录介质中，

其中，所述变更单元

在所述加密单元开始所述加密之前，将与所述预定的记录介质对应的所述加密变量从表示未加密的信息变更为表示正在加密的信息，

在所述加密单元完成所述加密后，将与所述预定的记录介质对应的所述加密变量变更为表示加密完成的信息，并且将与通过所述复制单元复制有所述加密后的数据的记录介质对应的所述加密变量从表示未加密的信息变更为表示正在加密的信息，

在所述复制单元完成所述复制后，将与通过所述复制单元复制有所述加密后的数据的记录介质对应的所述加密变量变更为表示加密完成的信息。

2.根据权利要求 1 所述的加密装置，其特征在于，

所述 RAID 组是 RAID 1 级的 RAID 组，

所述预定的记录介质是所述一个记录介质。

3.根据权利要求 1 所述的加密装置，其特征在于，

所述 RAID 组是 RAID 1 级的 RAID 组，

所述预定的记录介质是被设置为备用的记录介质。

4.一种加密方法，用于对属于 RAID 组的多个记录介质中所存储的数

据进行加密，该加密方法的特征在于，

该加密方法具有：

加密步骤，对属于所述 RAID 组的多个记录介质中的一个记录介质中所存储的数据进行加密，并将其写入预定的记录介质；

变更步骤，针对每个所述记录介质而设置，对表示各个记录介质中的加密的进展情况的加密变量进行变更；以及

复制步骤，将在所述加密步骤中加密后的数据复制到属于所述 RAID 组的多个记录介质中的、存储有尚未加密的数据的记录介质中，

其中，在所述变更步骤中，

在所述加密步骤中开始所述加密之前，将与所述预定的记录介质对应的所述加密变量从表示未加密的信息变更为表示正在加密的信息，

在所述加密步骤中完成所述加密后，将与所述预定的记录介质对应的所述加密变量变更为表示加密完成的信息，并且将与在所述复制步骤中复制有所述加密后的数据的记录介质对应的所述加密变量从表示未加密的信息变更为表示正在加密的信息，

在所述复制步骤中完成所述复制后，将与在所述复制步骤中复制有所述加密后的数据的记录介质对应的所述加密变量变更为表示加密完成的信息。

5.根据权利要求 4 所述的加密方法，其特征在于，

所述 RAID 组是 RAID 1 级的 RAID 组，

所述预定的记录介质是所述一个记录介质。

6.根据权利要求 4 所述的加密方法，其特征在于，

所述 RAID 组是 RAID 1 级的 RAID 组，

所述预定的记录介质是被设置为备用的记录介质。

7.一种加密程序，其对属于 RAID 组的多个记录介质中所存储的数据进行加密，该加密程序的特征在于，使计算机执行：

加密过程，其对属于所述 RAID 组的多个记录介质中的一个记录介质中所存储的数据进行加密，并将其写入预定的记录介质；

变更过程，其针对每个所述记录介质而设定，并对表示各个记录介

质中的加密的进展情况的加密变量进行变更；以及

复制过程，其将由所述加密过程加密的数据复制到属于所述 RAID 组的多个记录介质中的、存储有尚未加密的数据的记录介质中；

其中，在由所述加密过程进行的所述加密开始之前，所述变更过程将与所述预定的记录介质对应的所述加密变量从表示未加密的信息变更为表示正在加密的信息，

在完成由所述加密过程进行的所述加密以后，所述变更过程将与所述预定的记录介质对应的所述加密变量变更为表示加密完成的信息，并且将与通过所述复制过程而复制有所述加密的数据的记录介质对应的所述加密变量从表示未加密的信息变更为表示正在加密中的信息，

在完成由所述复制过程进行的所述复制以后，所述变更过程将与通过所述复制过程而复制有所述加密的数据的记录介质对应的所述加密变量变更为表示加密完成的信息。

8.根据权利要求 7 所述的加密程序，其特征在于，

所述 RAID 组是 RAID 级 1 的 RAID 组，

所述预定的记录介质是所述一个记录介质。

9.根据权利要求 7 所述的加密程序，其特征在于，

所述 RAID 组是 RAID 级 1 的 RAID 组，

所述预定的记录介质是被设置为备用的记录介质。

加密装置、加密方法以及加密程序

技术领域

本发明涉及对进行属于RAID（Redundant Array of Inexpensive Disks，独立冗余磁盘阵列）组的多个记录介质中所存储的数据的加密有效的加密装置、加密方法以及加密程序，特别涉及即使在正在加密处理时发生了故障等的情况下也能够可靠地重新开始加密处理的加密装置、加密方法以加密程序。

背景技术

确保由计算机系统管理的信息的机密性，对持有该信息的企业等来说是非常重要的问题。作为提高信息的机密性的技术，众所周知对存储装置中所存储的信息进行加密的技术。在下面的专利文献1～3中，公开了对磁盘等的记录介质中所存储的数据进行加密的技术。另外，一般地，对记录介质中所存储的数据进行加密时，由控制加密处理的控制器来管理加密的进展状况。

专利文献1：日本特开2005-107855号公报

专利文献2：日本特开2006-302259号公报

专利文献3：日本特开2004-201038号公报

但是，正在进行加密处理时，例如，在控制器发生了故障等，对加密处理的进展状况进行管理的信息丢失的情况下，无法区分在记录介质所存储的数据中哪个数据已被加密以及哪个数据尚未加密。在这种情况下，既不能重新开始加密处理，也不能正确地对数据进行解密，导致不能恢复数据。

发明内容

本发明是为了解决上述现有技术的问题点而完成的，其目的在于提

供即使正在加密处理时发生了故障等的情况下也仍能可靠地重新开始加密处理的加密装置、加密方法以加密程序。

为了解决上述课题来达成目的，本发明的加密装置对属于 RAID 组的多个记录介质中所存储的数据进行加密，该加密装置的特征在于，该加密装置具有：加密单元，其对属于 RAID 组的多个记录介质中的一个记录介质中所存储的数据进行加密，并将其写入预定的记录介质；变更单元，其针对每个记录介质而设置，并对表示各个记录介质中的加密进展情况的加密变量进行变更；以及复制单元，其将通过加密单元加密后的数据复制到属于 RAID 组的多个记录介质中的、存储有尚未加密的数据的记录介质中，其中，在加密单元开始加密之前，上述变更单元将与预定的记录介质对应的加密变量从表示未加密的信息变更为表示正在加密的信息，在加密单元完成加密后，上述变更单元将与预定的记录介质对应的加密变量变更为表示加密完成的信息，并且将与通过复制单元复制有加密后的数据的记录介质对应的加密变量从表示未加密的信息变更为表示正在加密的信息，在复制单元完成复制后，上述变更单元将与通过复制单元复制有加密后的数据的记录介质对应的加密变量变更为表示加密完成的信息。

另外，本发明是的加密方法对属于 RAID 组的多个记录介质中所存储的数据进行加密，该加密方法的特征在于，该加密方法具有：加密步骤，对属于 RAID 组的多个记录介质中的一个记录介质中所存储的数据进行加密，并将其写入预定的记录介质；变更步骤，针对每个记录介质而设置，并对表示各个记录介质中的加密进展情况的加密变量进行变更；以及复制步骤，将在加密步骤中加密后的数据复制到属于 RAID 组的多个记录介质中的、存储有尚未加密的数据的记录介质中，其中，在加密步骤中开始加密之前，上述变更步骤将与预定的记录介质对应的加密变量从表示未加密的信息变更为表示正在加密的信息，在加密步骤中完成加密后，上述变更步骤将与预定的记录介质对应的加密变量变更为表示加密完成的信息，并且将与在复制步骤中复制有加密后的数据的记录介质对应的加密变量从表示未加密的信息变更为表示正在加密的信息，在

复制步骤中完成复制后，上述变更步骤将与在复制步骤中复制有加密后的数据的记录介质对应的加密变量变更为表示加密完成的信息。

另外，本发明是对属于 RAID 组的多个记录介质中所存储的数据进行加密的加密程序，该加密程序的特征在于，使计算机执行：加密过程，其对属于 RAID 组的多个记录介质中的一个记录介质中所存储的数据进行加密，并将其写入预定的记录介质；变更过程，其针对每个记录介质而设定，并对表示各个记录介质中的加密进展情况的加密变量进行变更；以及复制过程，其将由加密过程加密的数据复制到属于 RAID 组的多个记录介质中的、存储有尚未加密的数据的记录介质中；其中，在由加密过程进行的加密开始之前，上述变更过程将与预定的记录介质对应的加密变量从表示未加密的信息变更为表示正在加密的信息，在完成由加密过程进行的加密以后，上述变更过程将与预定的记录介质对应的加密变量变更为表示加密完成的信息，并且将与通过复制过程而复制有加密的数据的记录介质对应的加密变量从表示未加密的信息变更为表示正在加密中的信息，在完成由复制过程进行的复制以后，上述变更过程将与通过复制过程而复制有加密的数据的记录介质对应的所述加密变量变更为表示加密完成的信息。

根据这些发明，能够在存在未加密状态的磁盘或加密完成的磁盘中的任意一个的状态下执行加密处理，并根据加密处理的进展状况来变更与各磁盘对应的加密标志，因此，即使在正在加密处理时发生了故障等的情况下，也能够使用未加密状态的磁盘或加密完成的磁盘中的任意一个来重新开始加密处理。

另外，在上述发明中，本发明的加密装置的特征在于，上述 RAID 组是 RAID 级 1 的 RAID 组，上述预定的记录介质是所述一个记录介质。

另外，在上述发明中，本发明的加密装置的特征在于，上述 RAID 组是 RAID 级 1 的 RAID 组，上述预定的记录介质是被设置为备用的记录介质。

根据本发明，能够在存在未加密状态的磁盘或加密完成的磁盘中的任意一个的状态下执行加密处理，并根据加密处理的进展状况来变更与

各磁盘对应的加密标志，因此，即使在正在进行加密处理时发生了故障的情况下，也能够使用未加密状态的磁盘或加密完成的磁盘中的任意一个来重新开始加密处理。即，根据本发明，取得了这样的效果：即使在正在加密处理时发生了故障等的情况下，也能够可靠地重新开始加密处理。

附图说明

图 1 是 RAID 装置的结构图。

图 2 是标志表的数据结构图。

图 3 是表示实施例 1 的 RAID 装置中的加密处理过程的流程图

图 4 是表示正在对磁盘 b 中所存储的数据进行加密的状态的示意图。

图 5 是表示正在将磁盘 b 的加密数据复制到磁盘 a 的状态的示意图。

图 6 是表示实施例 2 的 RAID 装置中的加密处理过程的流程图。

图 7 是表示对磁盘 b 中所存储的数据进行加密，并正在将其写入磁盘 z 的状态的示意图。

图 8 是表示正在将磁盘 z 的加密数据复制到磁盘 b 的状态的示意图。

图 9 是执行加密程序的计算机的功能结构图。

符号说明

1 RAID 装置

2 服务器

10 CM

11 控制部

12 控制存储器

13 闪存

14 数据缓存

20 CA

30 DA

40 磁盘

41 备用磁盘

111 加密部

112 加密数据复制部

113 标志变更部

121 标志表

1000 计算机

1010 CPU

1020 输入装置

1030 监视器

1040 介质读取装置

1050 通信装置

1060 RAM

1061 加密处理

1070 硬盘装置

1071 加密程序

1072 加密用数据

1080 总线

具体实施方式

下面，参照附图来详细地说明本发明涉及的加密装置、加密方法以及加密程序的最佳实施方式。

实施例 1

首先，对实施例 1 中的 RAID 装置的结构进行说明。图 1 是 RAID 装置的结构图。RAID 装置 1 是对属于 RAID 1 级的 RAID 组的多个磁盘（记录介质）进行管理的存储装置，能够在对数据进行了加密的状态下存储数据。在这里，RAID 是用于管理磁盘的技术，是用于防止由磁盘故障引起的数据损失，并且提高处理性能的技术。在 RAID 中，定义有级别 RAID 0～RAID 6。在本实施例中采用的 RAID 1 是将数据同时写入 2 个磁盘中的级别，也称为镜像。

如图 1 所示，RAID 装置 1 具有：CA（Channel Adapter 信道适配器）

20，其控制与服务器 20 之间的连接；CM（Controller Module，控制器模块）10，其控制对磁盘 40 中所存储的数据的加密；DA（Device Adapter，设备适配器）30，其控制 CM 10 与磁盘 40 之间的连接；磁盘 40，其属于 RAID1 级的 RAID 组；以及备用磁盘 41，其不属于 RAID 组。CM 10 具有：控制部 11；控制存储器 12，其存储标志表 121 等的各种数据和应用程序；闪存 13；以及数据缓存 14，其临时存储作为加密处理和复制处理的对象的数据。并且，在下面需要对属于 RAID1 级的 RAID 组的 2 个磁盘进行区分来说明时，将 2 个磁盘记为磁盘 40a 以及磁盘 40b。

在这里，参照图 2 来说明标志表 121 的数据结构。图 2 是标志表的数据结构图。标志表 121 含有作为数据项目的例如磁盘 ID、加密标志、组 ID。在磁盘 ID 中存储有用于唯一确定磁盘 40 的标识码，在加密标志中，存储有表示加密处理的进展状况的加密变量，在组 ID 中，存储有用于唯一确定磁盘所属的 RAID 组的标识码。在加密标志中存储有例如由“0”、“1”、“2”表示的变量。“0”表示磁盘中所存储的数据处于未加密的状态，“1”表示磁盘中所存储的数据处于正在加密的状态，“2”表示磁盘中所存储的数据处于加密完成的状态。

另外，存储加密标志之处不限于标志表 121。例如，既可以在控制存储器 12 中所存储的对各个磁盘的结构进行管理的磁盘结构表中存储加密标志，也可以在各个磁盘 40 的存储区域中的、用户不使用的特定区域中存储加密标志。

如图 1 所示的控制部 11 具有加密部 111、加密数据复制部 112、标志变更部 113。

加密部 111 根据从服务器 2 接收的加密请求中所包含的组 ID，将与该组 ID 对应的 RAID 组确定为加密处理的对象，对属于该 RAID 组的 2 个磁盘 40a、40b 中的一个磁盘、例如磁盘 40b 中所存储的数据进行加密，并将该加密后的数据写入磁盘 40b。下面，以由加密部 111 对 2 个磁盘 40a、40b 中的磁盘 40b 中所存储的数据进行加密的情况为例进行说明。但是，这并不表示将由加密部 111 加密的磁盘限定为磁盘 40b。由加密部 111 加密的磁盘可以是磁盘 40a、40b 中的任意一个。对于选择磁盘 40a、

40b 中的哪一个作为要进行加密的磁盘，例如可以在加密请求中包含磁盘 ID，从而根据该磁盘 ID 来决定，也可以针对每个组而预先设定要进行加密的磁盘。另外，作为加密处理对象的数据的单位既可以以磁盘为单位，也可以以分区为单位，还可以以卷为单位。

加密数据复制部 112 将由加密部 111 加密的磁盘 40b 的数据复制到属于同一 RAID 组的另一个磁盘即磁盘 40a 中。

标志变更部 113 按照如下方式变更加密标志。在从接收加密请求直至磁盘 40b 中所存储的数据开始加密的期间内，标志变更部 113 将与磁盘 40b 对应的加密标志从表示未加密的“0”变更为表示正在加密的“1”。

在从完成磁盘 40b 中所存储的数据的加密直至向该磁盘 40a 开始复制该数据的期间内，标志变更部 113 将与磁盘 40b 对应的加密标志从表示正在加密的“1”变更为表示加密完成的“2”，并且将与磁盘 40a 对应的加密标志从表示未加密的“0”变更为表示正在加密的“1”。

在完成向磁盘 40a 的复制以后，标志变更部 113 将与磁盘 40a 对应的加密标志从表示正在加密的“1”变更为表示加密完成的“2”。

接下来，参照图 3 对本实施例 1 中的 RAID 装置 1 的处理过程进行说明。图 3 是表示实施例 1 的 RAID 装置中的加密处理过程的流程图。说明在该处理过程中，对属于 RAID1 级的 RAID 组的磁盘 40a 以及磁盘 40b 中所存储的数据进行加密时的过程。

首先，在接收了从服务器 2 发送的加密请求的情况下（步骤 S101），RAID 装置 1 的加密部 111 使用该加密请求中所包含的组 ID，来将与该组 ID 对应的 2 个磁盘 40a、40b 确定为加密处理的对象（步骤 S102）。

接着，RAID 装置 1 的标志变更部 113 将与磁盘 40b 对应的加密标志从表示未加密的“0”变更为表示正在加密的“1”（步骤 S103）。

接着，RAID 装置 1 的加密部 111 对磁盘 40b 中所存储的数据进行加密，并将其写入磁盘 40b（步骤 S104）。在图 4 中示出该步骤 S104 中的各磁盘 40a、40b 的状态。图 4 是表示正在对磁盘 40b 中所存储的数据进行加密的状态的示意图。

接着，完成磁盘 40b 中所存储的数据的加密时，RAID 装置 1 的标志

变更部 113 将与磁盘 40b 对应的加密标志变更为表示加密完成的“2”，并且将与磁盘 40a 对应的加密标志从表示未加密的“0”变更为表示正在加密的“1”（步骤 S105）。

接着，RAID 装置 1 的加密数据复制部 112 将在上述步骤 S104 中进行加密的磁盘 40b 的加密数据复制到磁盘 40a（步骤 S106）。在图 5 中表示该步骤 S106 中的各磁盘 40a、40b 的状态。图 5 是表示正在将磁盘 40b 的加密数据复制到磁盘 40a 的状态的示意图。

接着，完成向磁盘 40a 的复制时，RAID 装置 1 的标志变更部 113 将与磁盘 40a 对应的加密标志变更为表示加密完成的“2”（步骤 S107）。

这样，通过根据加密处理的进展状况来变更与各磁盘对应的加密标志，例如，即使在 CM 10 发生故障等、加密处理在中途停止的情况下，也能够通过参照加密标志来可靠地重新开始加密。

具体而言，在磁盘 40a 的加密标志是表示未加密的“0”、而磁盘 40b 的加密标志是表示正在加密的“1”的情况下，在将磁盘 40a 的数据复制到磁盘 40b 后，执行上述的步骤 S104 以后的步骤。并且，在该情况下，也可以无需将磁盘 40a 的数据复制到磁盘 40b，而是对磁盘 40a 中所存储的数据进行加密并将其写入磁盘 40b。

在磁盘 40a 的加密标志是表示未加密的“0”或者表示正在加密的“1”、而磁盘 40b 的加密标志是表示加密完成的“2”的情况下，执行上述的步骤 S106 以后的步骤。在磁盘 40a 以及磁盘 40b 的加密标志都是表示加密完成的“2”的情况下，结束加密处理。

如上所述，在本实施例 1 的 RAID 装置 1 中，在存在未加密状态的磁盘或加密完成的磁盘中的任意一个的状态下执行加密处理，根据加密处理的进展状况来变更与各磁盘对应的加密标志。由此，即使是在正在加密处理时发生了故障等的情况下，也能够使用未加密状态的磁盘或加密完成的磁盘中的任意一个来可靠地重新开始加密处理。

实施例 2

对实施例 2 进行说明。实施例 2 中的 RAID 装置的结构与图 1 所示的实施例 1 中的 RAID 装置的结构相同。实施例 2 与实施例 1 的不同点

在于，写入加密后的数据的磁盘不同。具体而言，不同点在于，在实施例 1 中，例如在对磁盘 40b 中所存储的数据进行加密的情况下，向同一磁盘 40b 中写入加密后的数据，与此相对，在实施例 2 中，例如在对磁盘 40b 中所存储的数据进行加密的情况下，向不属于 RAID 组的备用的磁盘 41 中写入加密后的数据。下面，以与实施例 1 的不同点为中心来说明在这样的实施例 2 中的 RAID 装置的结构以及动作。另外，与实施例 1 相同，当需要对属于 RAID 级 1 的 RAID 组的 2 个磁盘 40 进行区分来说明时，将 2 个磁盘 40 记为磁盘 40a 以及磁盘 40b。

加密部 111 根据从服务器 2 接收的加密请求中所包含的组 ID，将属于与该组 ID 对应的 RAID 组的 2 个磁盘 40a、40b 确定为加密处理的对象，并从备用的磁盘 41 中选择 1 个用于加密处理的磁盘 41z，将其添加到加密处理的对象中。加密部 111 对 2 个磁盘 40a、40b 中的一个磁盘 40b 中所存储的数据进行加密，并将该加密后的数据写入磁盘 41z。另外，由加密部 111 加密的磁盘可以是磁盘 40a、40b 中的任意一个。对于选择磁盘 40a、40b 中的哪一个作为要进行加密的磁盘，例如可以在加密请求中包含磁盘 ID，从而根据该磁盘 ID 来决定，也可以针对每个组而预先设定要进行加密的磁盘。

加密数据复制部 112 将由加密部 111 加密的磁盘 41z 的数据复制到磁盘 40a 以及磁盘 40b 中。

标志变更部 113 按照如下方式变更加密标志。从接收到加密请求直至磁盘 40b 中所存储的数据的加密开始的期间内，标志变更部 113 将与磁盘 41z 对应的加密标志从表示未加密的“0”变更为表示正在加密的“1”。

从完成磁盘 40b 中所存储的数据的加密直至向磁盘 40b 开始复制磁盘 41z 中所存储的加密数据的期间内，标志变更部 113 将与磁盘 41z 对应的加密标志从表示正在加密的“1”变更为表示加密完成的“2”，并将与磁盘 40b 对应的加密标志从表示未加密的“0”变更为表示正在加密的“1”。

从完成向磁盘 40b 的复制直至向磁盘 40a 的复制开始的期间内，标志变更部 113 将与磁盘 40b 对应的加密标志从表示正在加密的“1”变更为表示加密完成的“2”，并将与磁盘 40a 对应的加密标志从表示未加密的“0”

变更为表示正在加密的“1”。

在完成向磁盘 40a 的复制以后，标志变更部 113 将与磁盘 40a 对应的加密标志从表示正在加密的“1”变更为表示加密完成的“2”。

接下来，参照图 6 对本实施例 2 中的 RAID 装置 1 的处理过程进行说明。图 6 是表示实施例 2 的 RAID 装置中的加密的处理过程的流程图。在该加密过程中，说明对属于 RAID 级 1 的 RAID 组的磁盘 40a 以及磁盘 40b 中所存储的数据进行加密时的过程。

首先，接收到从服务器 2 发送的加密请求时（步骤 S201），RAID 装置 1 的加密部 111 使用该加密请求中所包含的组 ID 来将与该组 ID 对应的 2 个磁盘 40a、40b 确定为加密处理的对象，并从备用的磁盘 41 中选择 1 个用于加密处理的磁盘 41z，并使其包含在加密处理的对象中（步骤 S202）。

接着，RAID 装置 1 的标志变更部 113 将与磁盘 41z 对应的加密标志从表示未加密的“0”变更为表示正在加密的“1”（步骤 S203）。

接着，RAID 装置 1 的加密部 111 对磁盘 40b 中所存储的数据进行加密，并将其写入磁盘 41z（步骤 S204）。在图 7 中表示该步骤 S204 中的各磁盘 40a、40b、40z 的状态。图 7 是示出对磁盘 40b 中所存储的数据进行加密，并正在将其写入磁盘 41z 的状态的示意图。

接着，完成磁盘 40b 中所存储的数据的加密时，RAID 装置 1 的标志变更部 113 将与磁盘 41z 对应的加密标志变更为表示加密完成的“2”，并将与磁盘 40b 对应的加密标志从表示未加密的“0”变更为表示正在加密的“1”（步骤 S205）。

接着，RAID 装置 1 的加密数据复制部 112 将在上述步骤 S204 中写入的磁盘 41z 的加密数据复制到磁盘 40b 中（步骤 S206）。在图 8 中示出该步骤 S206 中的各磁盘 40a、40b、40z 的状态。图 8 是表示正在将磁盘 41z 的加密数据复制到磁盘 40b 中的状态的示意图。

接着，完成向磁盘 40b 的复制时，RAID 装置 1 的标志变更部 113 将与磁盘 40b 对应的加密标志变更为表示加密完成的“2”，并将与磁盘 40a 对应的加密标志从表示未加密的“0”变更为表示正在加密的“1”（步骤 S207）。

接着，RAID 装置 1 的加密数据复制部 112 将在上述步骤 S204 中写入的磁盘 41z 的加密数据复制到磁盘 40a（步骤 S208）。

接着，完成向磁盘 40a 的复制时，RAID 装置 1 的标志变更部 113 将与磁盘 40a 对应的加密标志变更为表示加密完成的“2”（步骤 S209）。

这样，通过根据加密处理的进展状况来变更与各磁盘对应的加密标志，例如即使在 CM 10 发生了故障等、加密处理在中途停止的情况下，也能够通过参照加密标志来可靠地重新开始加密。

具体而言，在磁盘 40a 以及磁盘 40b 的加密标志表示未加密的“0”、而磁盘 41z 的加密标志表示正在加密的“1”的情况下，执行上述步骤 S204 以后的步骤。

在磁盘 40a 的加密标志表示未加密的“0”、磁盘 40b 的加密标志表示正在加密的“1”、而磁盘 41z 加密标志表示加密完成的“2”的情况下，执行上述步骤 S206 以后的步骤。

在磁盘 40a 的加密标志表示未加密的“0”或表示正在加密的“1”、而磁盘 40b 以及磁盘 41z 的加密标志都表示加密完成的“2”的情况下，执行上述步骤 S208 以后的步骤。

在磁盘 40a、磁盘 40b 以及磁盘 41z 的加密标志都表示加密完成的“2”的情况下，结束加密处理。

如上所述，在本实施例 2 的 RAID 装置 1 中，在存在未加密状态的磁盘或加密完成的磁盘中的任意一个的状态下执行加密处理，并根据加密处理的进展状况来变更与各磁盘对应的加密标志。由此，即使在正在进行加密处理时发生了故障等的情况下，也能够使用未加密状态的磁盘或加密完成的磁盘中的任意一个来可靠地重新开始加密处理。

另外，根据本实施例 2 的 RAID 装置 1，在正在对备用磁盘 41 进行加密时发生了故障等的情况下，属于 RAID 组的磁盘 40a、40b 保持未加密状态，因此仅将备用磁盘 41 更换为其他备用磁盘，就能够容易地重新开始加密处理。

另外，在上述的实施例 2 中，对加密的多个磁盘 40 属于 RAID 1 级的 RAID 组的情况进行了说明，但是也能够适用于属于其他 RAID 级的

RAID 组的情况。例如，在适用于属于 RAID 4 级～RAID 6 级中的任一级别的 RAID 组的多个磁盘 40 的情况下，准备与属于 RAID 组的磁盘相同个数的备用磁盘 41，将属于 RAID 组的各磁盘 40 的加密数据写入与各磁盘 40 对应的备用磁盘 41，然后，将加密数据从备用磁盘 41 复制到属于 RAID 组的磁盘 40 中即可。

最后，如图 1 所示的各实施例中的 RAID 装置 1 的结构能够在不脱离本发明的主旨的范围内进行各种变更。例如，将 RAID 装置 1 的控制部 11 的功能作为软件来安装，通过由计算机执行该软件，能够实现与 RAID 装置 1 相同的功能。下面，示出执行加密程序 1071 的计算机的一个例子，在该加密程序 1071 中安装有作为软件的控制部 11 的功能。

图 9 是执行加密程序的计算机的功能结构图。该计算机 1000 通过总线 1080 连接执行各种运算处理的 CPU（Central Processing Unit，中央处理单元）1010、接受来自用户的数据输入的输入装置 1020、显示各种信息的监视器 1030、从记录介质读取程序等的介质读取装置 1040、经由网络进行与其他计算机之间的数据的交换的通信装置 1050、临时存储各种信息的 RAM（Random Access Memory，随机存取存储器）1060、硬盘装置 1070。

而且，在硬盘装置 1070 中存储有具有与图 1 所示的控制部 11 相同功能的加密程序 1071、与加密程序 1071 使用的各种程序对应的加密用数据 1072。并且，也能够适当地分散加密用数据 1072，存储在经由网络连接的其他计算机中。

而且，CPU 1010 从硬盘装置 1070 中读取加密程序 1071 来展开到 RAM 1060 中，由此加密程序 1071 作为加密处理 1061 发挥作用。而且，加密处理 1061 将从加密用数据 1072 读取的信息等适当地展开到 RAM 1060 上的分配给加密处理 1061 本身的区域中，并根据该展开的数据等执行各种数据处理。

另外，加密程序 1071 不一定必须安装在硬盘装置 1070 中，也可以是，计算机 1000 读取 CD-ROM 等的记录介质中所存储的该程序来执行。也可以是，将该程序存储在经由公共线路、因特网、LAN （Local Area

Network，局域网）、WAN（Wide Area Network，广域网）等而与计算机 1000 连接的其他计算机（或服务器）等中，计算机 1000 从这些设备读取程序来执行。

产业上的可利用性

如上所述，本发明涉及的对加密装置、加密方法以及加密程序对进行属于 RAID 组的多个记录介质中所存储的数据的加密有效，特别适用于即使在正在加密处理时发生了故障等的情况下也可靠地重新开始加密处理的情况。

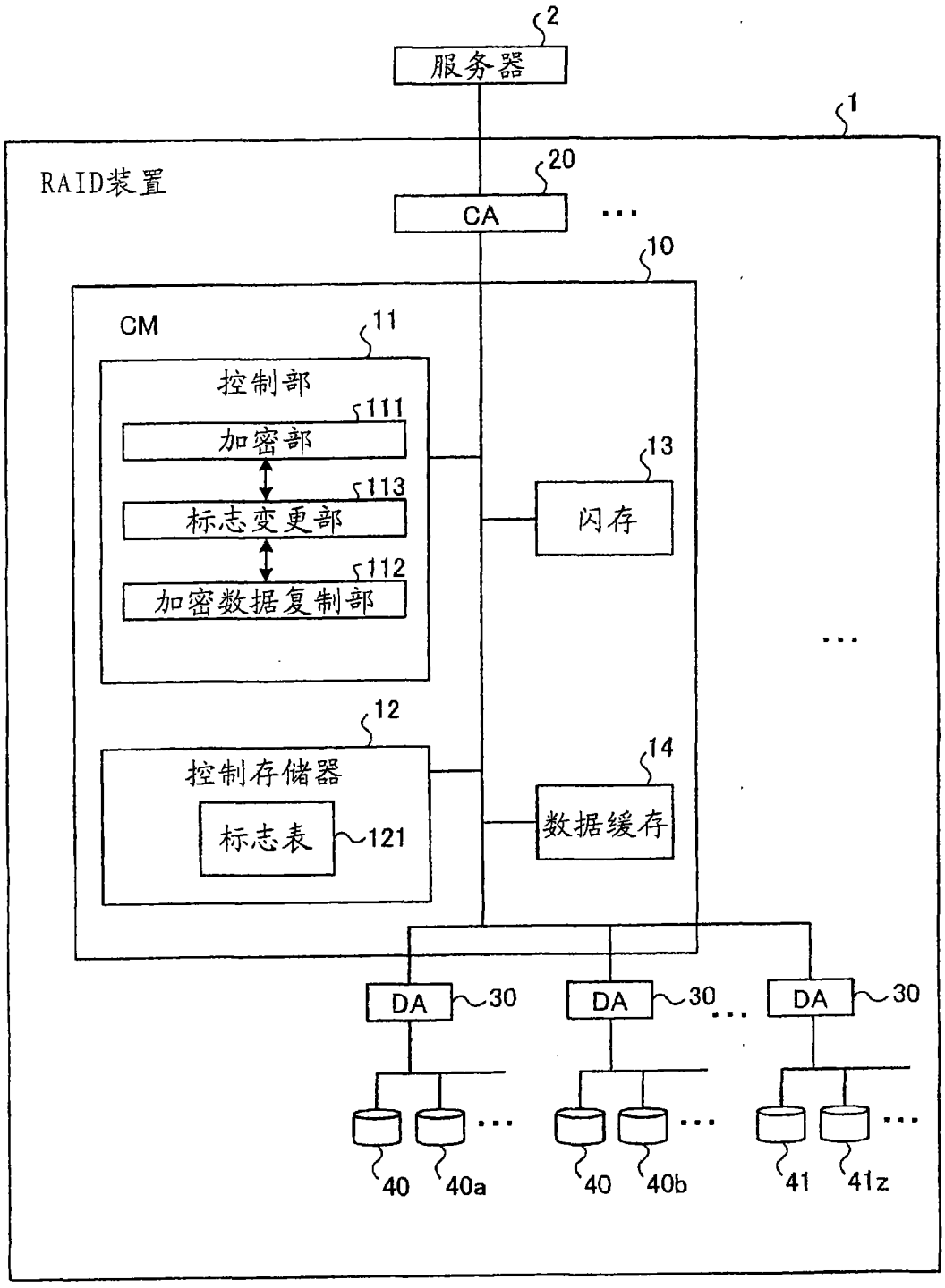

2
服务器
1
RAID装置
20
CA
10
CM
11
控制部
111
加密部
113
标志变更部
112
加密数据复制部
13
闪存
12
控制存储器
标志表
121
14
数据缓存
DA
30
DA
30
DA
30
40
40a
40
40b
41
41z

图1

磁盘ID	加密标志	组ID
001	1	01
002	0	01
003	2	02
⋮	⋮	⋮

图2

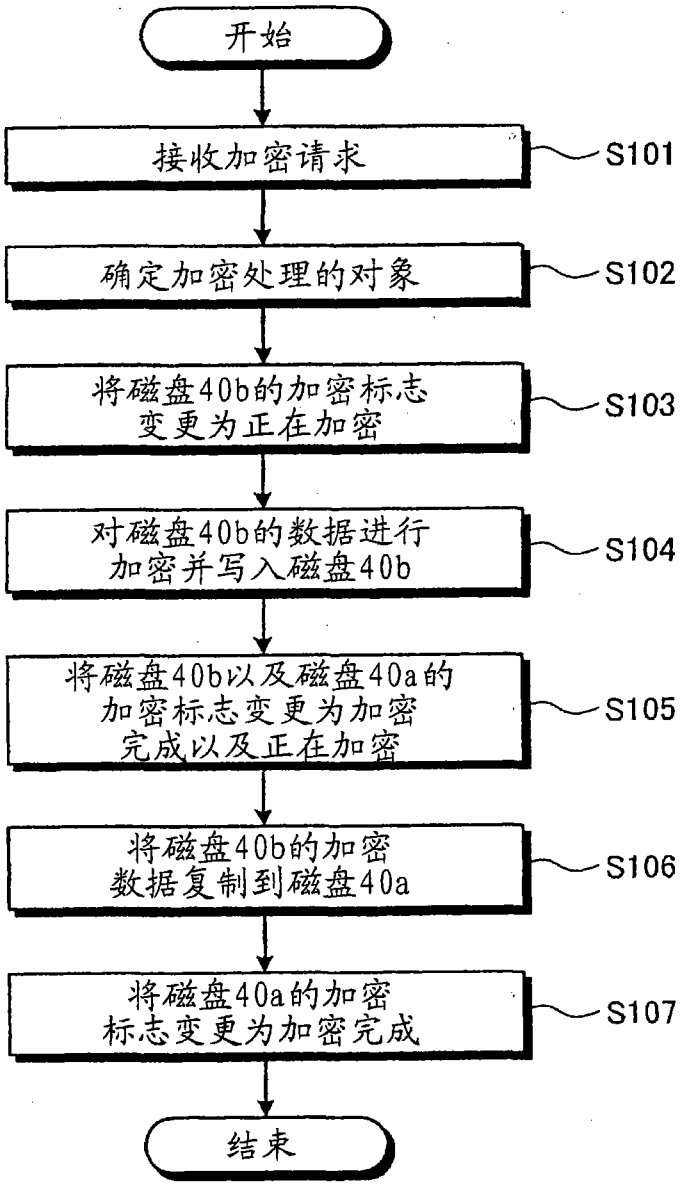

开始
接收加密请求
S101
确定加密处理的对象
S102
将磁盘40b的加密标志
变更为正在加密
S103
对磁盘40b的数据进行
加密并写入磁盘40b
S104
将磁盘40b以及磁盘40a的
加密标志变更为加密
完成以及正在加密
S105
将磁盘40b的加密
数据复制到磁盘40a
S106
将磁盘40a的加密
标志变更为加密完成
S107
结束

图3

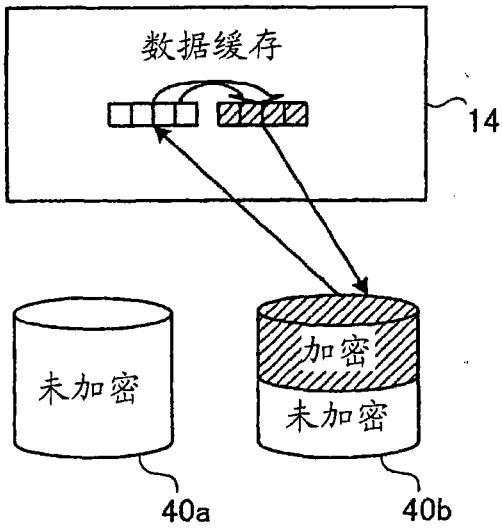


图4

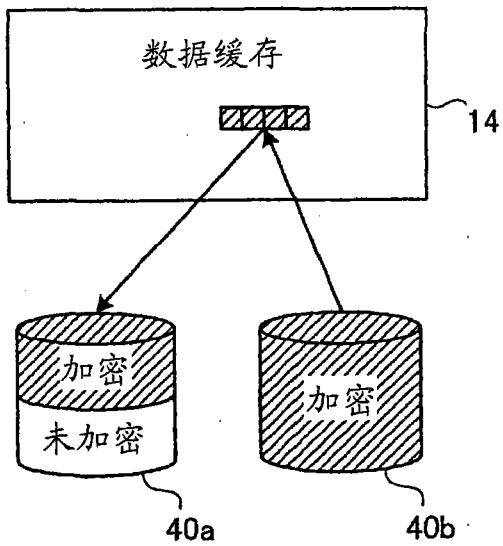


图5

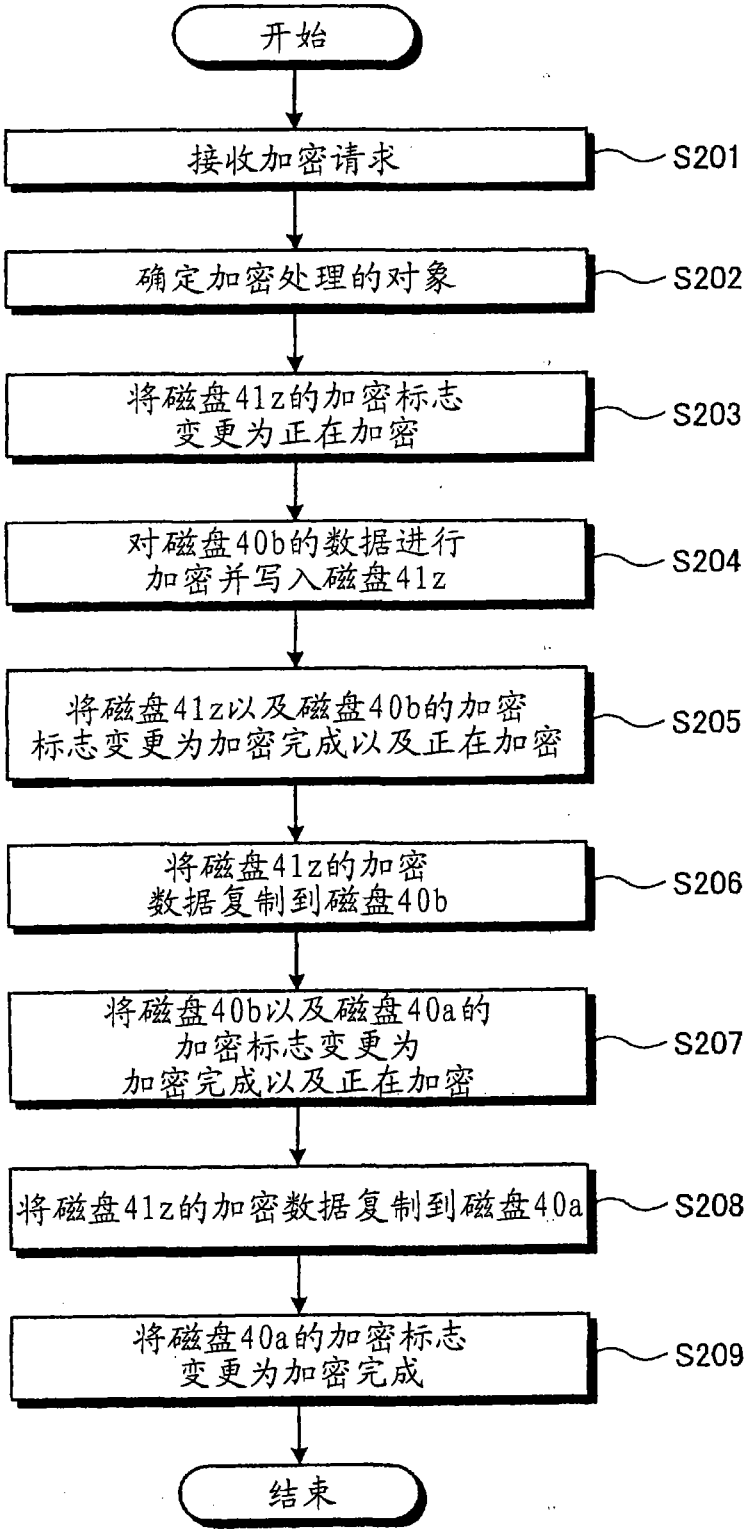

开始
接收加密请求
S201
确定加密处理的对象
S202
将磁盘41z的加密标志
变更为正在加密
S203
对磁盘40b的数据进行
加密并写入磁盘41z
S204
将磁盘41z以及磁盘40b的加密
标志变更为加密完成以及正在加密
S205
将磁盘41z的加密
数据复制到磁盘40b
S206
将磁盘40b以及磁盘40a的
加密标志变更为
加密完成以及正在加密
S207
将磁盘41z的加密数据复制到磁盘40a
S208
将磁盘40a的加密标志
变更为加密完成
S209
结束

图6

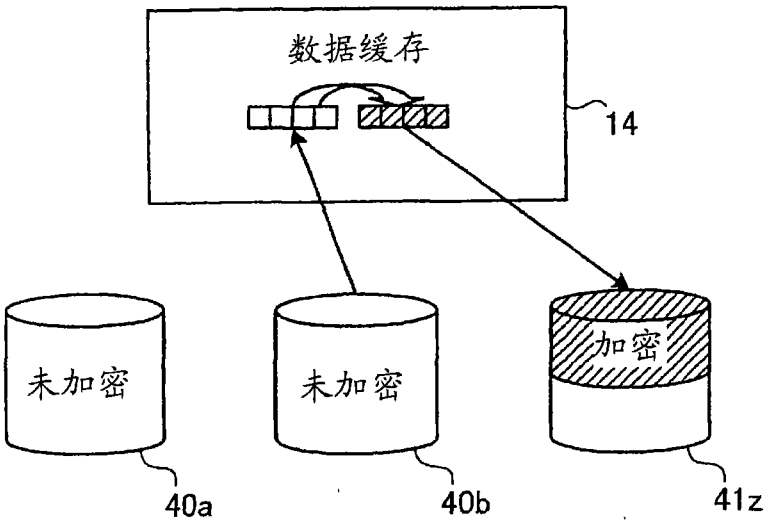


图7

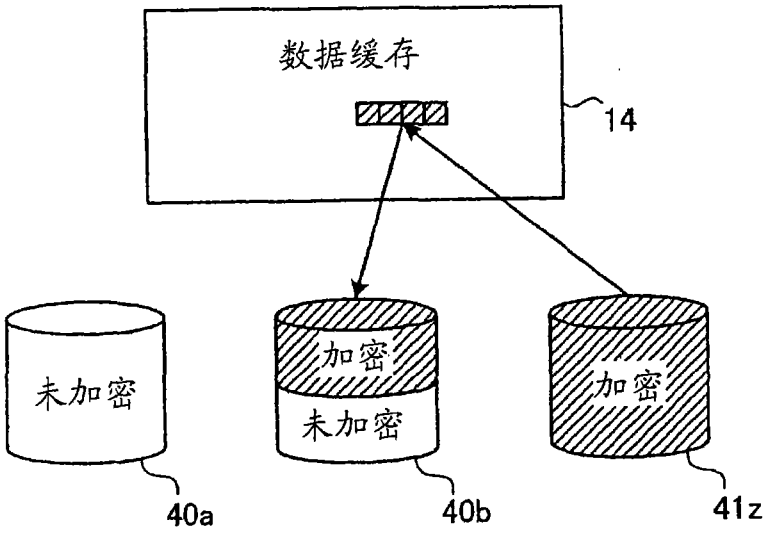


图8

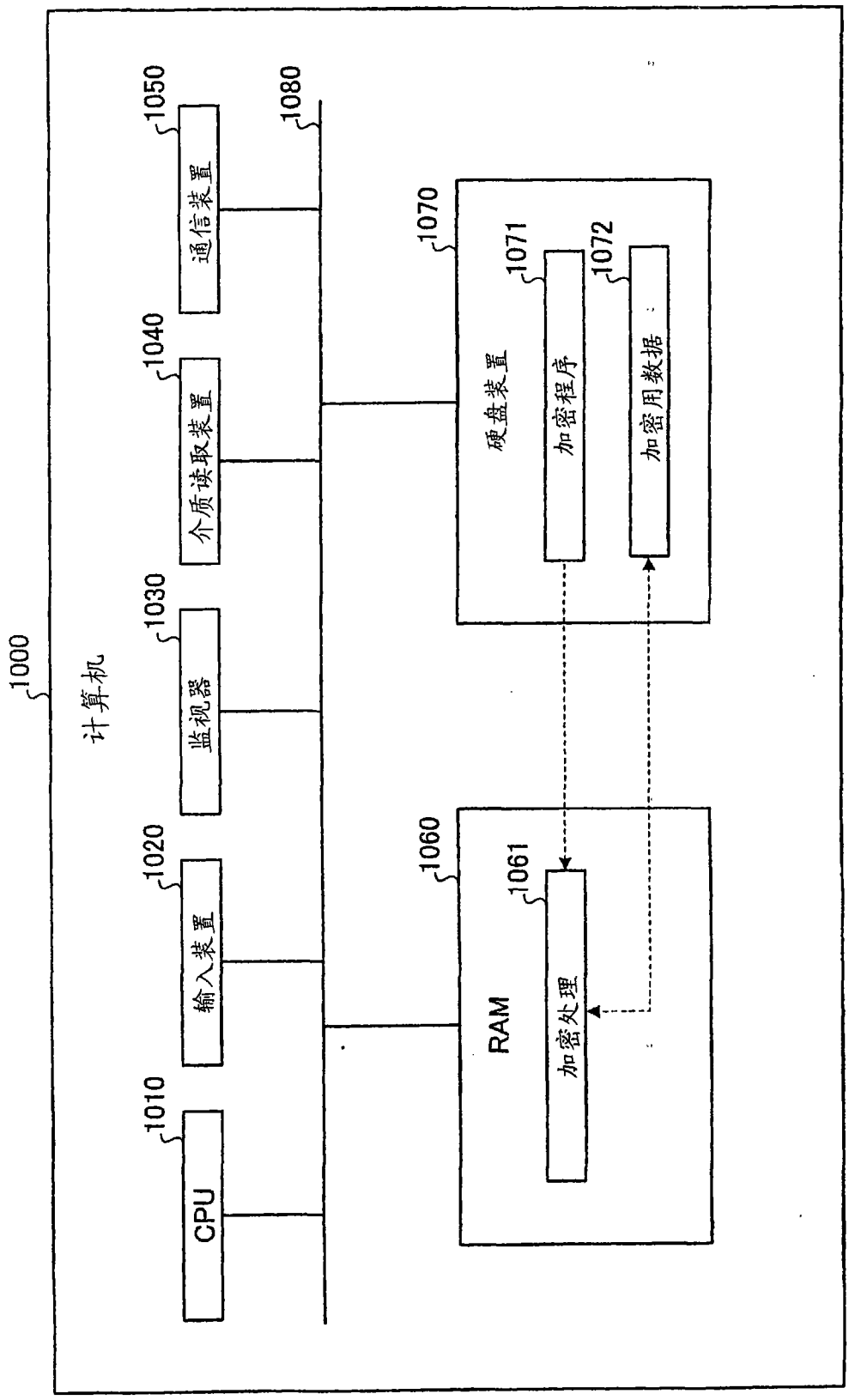

1000
计算机
1010
CPU
1020
输入装置
1030
监视器
1040
介质读取装置
1050
通信装置
1060
RAM
1061
加密处理
1070
硬盘装置
1071
加密程序
1072
加密用数据
1080

图9