(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 101930409 A
(43)申请公布日 2010.12.29

(21)申请号 201010212328.1

(22)申请日 2010.06.28

(30)优先权数据
2009-151812 2009.06.26 JP

(71)申请人 巴比禄股份有限公司
地址 日本爱知县

(72)发明人 石井俊

(74)专利代理机构 北京林达刘知识产权代理事务所(普通合伙) 11277
代理人 刘新宇

(51)Int.Cl.
G06F 12/14(2006.01)

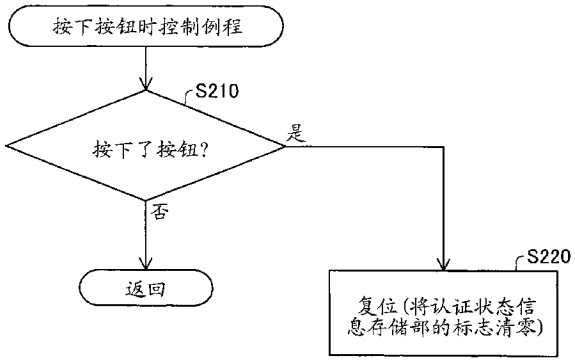
权利要求书 2 页 说明书 7 页 附图 3 页

(54)发明名称

存储装置、存储装置的控制方法以及计算机程序

(57)摘要

本发明提供一种能够提高具有认证功能的存储装置进行锁定时的便利性的存储装置、存储装置的控制方法以及计算机程序。一种与个人计算机相连接的USB硬盘，具备硬盘、访问控制器以及按钮。访问控制器具备加密/解密部(35)，作为由CPU执行的功能还具备认证部、已认证状态保持部以及解密禁止部。当按下按钮时(S210:“是”)，对访问控制器进行复位(步骤S220)。访问控制器当被复位时，再次执行启动时控制例程，通过对操作者请求进行口令认证来设为锁定状态。



CN 101930409 A

1. 一种存储装置，外置于信息处理装置，具备：

接口，其用于与上述信息处理装置进行连接；

存储介质，其用于存储处于加密状态的数据；

解密部，其对存储在上述存储介质中的、由上述信息处理装置请求读取的数据进行解密；

认证部，其认证对上述存储装置的访问是否具有合法权限；

已认证状态保持部，其在通过上述认证部进行的认证成功之后，保持已认证状态，在上述存储装置经由上述接口对上述信息处理装置进行的连接断开时，解除上述已认证状态；以及

解密禁止部，其在上述已认证状态保持部保持上述已认证状态时，允许由上述解密部进行解密，在上述已认证状态保持部解除了上述已认证状态时，禁止由上述解密部进行解密，

上述存储装置还具备：

操作指令接收部，其接收由操作者发出的规定的操作指令；以及

认证取消部，其在由上述操作指令接收部接收到上述规定的操作指令时，解除由上述已认证状态保持部保持的已认证状态。

2. 根据权利要求 1 所述的存储装置，其特征在于，

上述认证部具备：

口令请求部，其在上述存储装置与上述信息处理装置之间开始连接时，促使上述信息处理装置输入口令；以及

口令判断部，其通过判断从上述信息处理装置输入的口令是否与预先登记的口令一致，来进行上述认证，

其中，上述解密禁止部为通过禁止对上述存储装置的访问来禁止上述解密的结构，

上述认证取消部为通过对上述存储装置进行复位来解除上述已认证状态的结构。

3. 根据权利要求 1 或 2 所述的存储装置，其特征在于，

上述已认证状态保持部具备认证状态信息存储部，该认证状态信息存储部存储认证状态信息，该认证状态信息表示是处于上述已认证状态还是处于解除了上述已认证状态的状态。

4. 根据权利要求 1 ～ 3 中的任一项所述的存储装置，其特征在于，还具备：

加密部，其对写入上述存储介质的数据进行加密；以及

加密禁止部，其在上述已认证状态保持部保持上述已认证状态时，允许由上述加密部进行加密，在上述已认证状态保持部解除了上述已认证状态时，禁止由上述加密部进行加密。

5. 根据权利要求 1 ～ 4 中的任一项所述的存储装置，其特征在于，

具备操作开关，该操作开关接收由上述操作者进行的操作，以发送上述规定的操作指令。

6. 根据权利要求 1 ～ 4 中的任一项所述的存储装置，其特征在于，

上述操作指令接收部为从上述信息处理装置接收上述规定的操作指令的结构。

7. 一种外置于信息处理装置的存储装置的控制方法，包括：

认证对上述存储装置的访问是否具有合法权限，在上述认证成功之后，保持已认证状态，

在处于上述已认证状态时，允许对存储在存储介质中的、由上述信息处理装置请求读取的数据进行解密，在未处于上述已认证状态时，禁止该解密，其中，上述存储介质用于存储处于加密状态的数据，

并且，上述存储装置所具备的操作指令接收部接收由操作者发出的规定的操作指令，

在由上述操作指令接收部接收到上述规定的操作指令时，解除已认证状态的保持。

8. 一种计算机程序，用于外置于信息处理装置的存储装置，该存储装置具备：接口，其用于与上述信息处理装置进行连接；存储介质，其用于存储处于加密状态的数据；以及解密部，其对存储在上述存储介质中的、由上述信息处理装置请求读取的数据进行解密，该计算机程序用于使上述存储装置实现以下功能：

认证功能，认证对上述存储装置的访问是否具有合法权限；

已认证状态保持功能，在通过上述认证功能进行的认证成功之后，保持已认证状态，在上述存储装置经由上述接口对上述信息处理装置进行的连接断开时，解除上述已认证状态；以及

解密禁止功能，在处于上述已认证状态时，允许由上述解密部进行解密，在未处于上述已认证状态时，禁止由上述解密部进行解密，

该计算机程序还使上述存储装置实现以下功能：

操作指令接收功能，接收由操作者发出的规定的操作指令；以及

认证取消功能，在通过上述操作指令接收功能接收到上述规定的操作指令时，解除通过上述已认证状态保持功能而保持的已认证状态。

9. 一种计算机程序，用于外置于信息处理装置的存储装置，该存储装置具备：接口，其用于与上述信息处理装置进行连接；以及存储介质，其用于存储处于加密状态的数据，该计算机程序用于使上述存储装置实现以下功能：

解密功能，对存储在上述存储介质中的、由上述信息处理装置请求读取的数据进行解密；

认证功能，认证对上述存储装置的访问是否具有合法权限；

已认证状态保持功能，在通过上述认证功能进行的认证成功之后，保持已认证状态，在上述存储装置经由上述接口对上述信息处理装置进行的连接断开时，解除上述已认证状态；以及

解密禁止功能，在处于上述已认证状态时，允许通过上述解密功能进行解密，在未处于上述已认证状态时，禁止通过上述解密功能进行解密，

该计算机程序还使上述存储装置实现以下功能：

操作指令接收功能，接收由操作者发出的规定的操作指令；以及

认证取消功能，在通过上述操作指令接收功能接收到上述规定的操作指令时，解除通过上述已认证状态保持功能而保持的已认证状态。

存储装置、存储装置的控制方法以及计算机程序

技术领域

[0001] 本发明涉及一种外置于信息处理装置的存储装置、该存储装置的控制方法或用于该存储装置的计算机程序。

背景技术

[0002] 一般来说，已知一种利用 USB 等的支持热插拔的接口来与个人计算机进行连接的外置的存储装置（例如，USB 快闪存储器 (USB Flash Memory)）。以往，作为这种存储装置之一，提出了一种在与个人计算机进行连接时需要进行口令认证 (PasswordAuthentication) 的存储装置（例如，专利文献 1）。通过该结构，能够对不知道口令的人设定无法访问的状态、即锁定状态。

[0003] 专利文献 1 ：日本特开 2007-35136 号公报

发明内容

[0004] 发明要解决的问题

[0005] 然而，在上述以往的技术中，为了锁定存储装置，需要从个人计算机卸下存储装置，或者断开对存储装置的供电，从而存在进行锁定时的便利性未必很好的问题。例如，在暂时离开坐位的情况下等也需要卸下上述存储装置或断开对存储装置的供电，较为不便。

[0006] 本发明的目的在于提高具有认证功能的存储装置进行锁定时的便利性。

[0007] 用于解决问题的方案

[0008] 为了解决上述问题的至少一部分，本发明能够实现为以下的方式或应用例。

[0009] [应用例 1] 一种存储装置，外置于信息处理装置，具备 ：接口，其用于与上述信息处理装置进行连接 ；存储介质，其用于存储处于加密状态的数据 ；解密部，其对存储在上述存储介质中的、由上述信息处理装置请求读取的数据进行解密 ；认证部，其认证对上述存储装置的访问是否具有合法权限 ；已认证状态保持部，其在通过上述认证部进行的认证成功之后，保持已认证状态，在上述存储装置经由上述接口对上述信息处理装置进行的连接断开时，解除上述已认证状态 ；以及解密禁止部，其在上述已认证状态保持部保持上述已认证状态时，允许由上述解密部进行解密，在上述已认证状态保持部解除了上述已认证状态时，禁止由上述解密部进行解密，上述存储装置还具备 ：操作指令接收部，其接收由操作者发出的规定的操作指令 ；以及认证取消部，其在由上述操作指令接收部接收到上述规定的操作指令时，解除由上述已认证状态保持部保持的已认证状态。

[0010] 根据应用例 1 所涉及的存储装置，当接收到由操作者发出的规定的操作指令时，解除由已认证状态保持部保持的已认证状态。在未处于已认证状态时，禁止由解密部对数据进行解密，从而禁止从存储装置读取数据。因此，操作者只要进行发送规定的操作指令的操作就能够对存储装置进行锁定，由此，根据上述存储装置，能够提高进行锁定时的便利性。

[0011] [应用例 2] 根据应用例 1 所述的存储装置，上述认证部具备 ：口令请求部，其在上

述存储装置与上述信息处理装置之间开始连接时，促使上述信息处理装置输入口令；以及口令判断部，其通过判断从上述信息处理装置输入的口令是否与预先登记的口令一致，来进行上述认证，其中，上述解密禁止部为通过禁止对上述存储装置的访问来禁止上述解密的结构，上述认证取消部为通过对上述存储装置进行复位来解除上述已认证状态的结构。

[0012] 根据应用例 2 的结构，只要对存储装置进行复位就解除已认证状态来重新开始上述存储装置与信息处理装置之间的连接，从而能够容易地转变为需要进行口令认证的锁定状态。

[0013] [应用例 3] 根据应用例 1 或 2 所述的存储装置，上述已认证状态保持部具备认证状态信息存储部，该认证状态信息存储部存储认证状态信息，该认证状态信息表示是处于上述已认证状态还是处于解除了上述已认证状态的状态。根据该结构，能够根据认证状态信息存储部所存储的认证状态信息来容易地判断是处于已认证状态还是处于未认证状态。

[0014] [应用例 4] 根据应用例 1 ～ 3 中的任一项所述的存储装置，还具备：加密部，其对写入上述存储介质的数据进行加密；以及加密禁止部，其在上述已认证状态保持部保持上述已认证状态时，允许由上述加密部进行加密，在上述已认证状态保持部解除了上述已认证状态时，禁止由上述加密部进行加密。根据该结构，在接收到由操作者发出的规定的操作指令时，禁止从存储装置读取数据并禁止对存储装置写入数据。

[0015] [应用例 5] 根据应用例 1 ～ 4 中的任一项所述的存储装置，具备操作开关，该操作开关接收由上述操作者进行的操作，以发送上述规定的操作指令。根据该结构，能够由操作者从存储装置侧进行锁定操作。

[0016] [应用例 6] 根据应用例 1 ～ 4 中的任一项所述的存储装置，上述操作指令接收部为从上述信息处理装置接收上述规定的操作指令的结构。根据该结构，能够由操作者从信息处理装置侧进行锁定操作。

[0017] [应用例 7] 一种外置于信息处理装置的存储装置的控制方法，包括：认证对上述存储装置的访问是否具有合法权限，在上述认证成功之后，保持已认证状态，在处于上述已认证状态时，允许对存储在存储介质中的、由上述信息处理装置请求读取的数据进行解密，在未处于上述已认证状态时，禁止该解密，其中，上述存储介质用于存储处于加密状态的数据，并且，上述存储装置所具备的操作指令接收部接收由操作者发出的规定的操作指令，在由上述操作指令接收部接收到上述规定的操作指令时，解除已认证状态的保持。

[0018] [应用例 8] 一种计算机程序，用于外置于信息处理装置的存储装置，该存储装置具备：接口，其用于与上述信息处理装置进行连接；存储介质，其用于存储处于加密状态的数据；以及解密部，其对存储在上述存储介质中的、由上述信息处理装置请求读取的数据进行解密，该计算机程序用于使上述存储装置实现以下功能：认证功能，认证对上述存储装置的访问是否具有合法权限；已认证状态保持功能，在通过上述认证功能进行的认证成功之后，保持已认证状态，在上述存储装置经由上述接口对上述信息处理装置进行的连接断开时，解除上述已认证状态；以及解密禁止功能，在处于上述已认证状态时，允许由上述解密部进行解密，在未处于上述已认证状态时，禁止由上述解密部进行解密，该计算机程序还使上述存储装置实现以下功能：操作指令接收功能，接收由操作者发出的规定的操作指令；以及认证取消功能，在通过上述操作指令接收功能接收到上述规定的操作指令时，解除通过上述已认证状态保持功能而保持的已认证状态。

[0019] [应用例 9] 一种计算机程序，用于外置于信息处理装置的存储装置，该存储装置具备：接口，其用于与上述信息处理装置进行连接；以及存储介质，其用于存储处于加密状态的数据，该计算机程序用于使上述存储装置实现以下功能：解密功能，对存储在上述存储介质中的、由上述信息处理装置请求读取的数据进行解密；认证功能，认证对上述存储装置的访问是否具有合法权限；已认证状态保持功能，在通过上述认证功能进行的认证成功之后，保持已认证状态，在上述存储装置经由上述接口对上述信息处理装置进行的连接断开时，解除上述已认证状态；以及解密禁止功能，在处于上述已认证状态时，允许通过上述解密功能进行解密，在未处于上述已认证状态时，禁止通过上述解密功能进行解密，该计算机程序还使上述存储装置实现以下功能：操作指令接收功能，接收由操作者发出的规定的操作指令；以及认证取消功能，在通过上述操作指令接收功能接收到上述规定的操作指令时，解除通过上述已认证状态保持功能而保持的已认证状态。

[0020] 应用例 7 所涉及的存储装置的控制方法以及应用例 8、9 所涉及的计算机程序能够得到与应用例 1 所涉及的存储装置同样的作用效果。

[0021] 并且，本发明能够以记录上述应用例 8 或 9 所涉及的计算机程序的记录介质、包含该计算机程序并在载波内具体表现的数据信号等方式来实现。

附图说明

[0022] 图 1 是表示作为本发明的一个实施例的信息处理系统 100 的概要结构的说明图。

[0023] 图 2 是表示启动时控制例程的流程图。

[0024] 图 3 是表示口令认证画面 DB 的说明图。

[0025] 图 4 是表示按下按钮时控制例程的流程图。

[0026] 附图标志说明

[0027] 10：个人计算机 (PC)；12：USB 总线接口；14：CPU；15：RAM；16：HDD(Hard Disk Drive)；17：显示部；18：输入部；19：内部总线；20：USB 硬盘；22：USB 总线接口；30：访问控制器 (Access Controller)；31：CPU；32：ROM；33：RAM；33a：认证状态信息存储部；35：加密 / 解密部；40：硬盘单元；41：盘；42：盘控制器 (Disk Controller)；50：按钮；100：信息处理系统；DB：口令认证画面。

具体实施方式

[0028] 下面参照附图，根据实施例来说明本发明的实施方式。

[0029] 图 1 是表示作为本发明的一个实施例的信息处理系统 100 的概要结构的说明图。如图所示，信息处理系统 100 具备作为信息处理装置的个人计算机 10 以及作为存储装置的 USB 硬盘 20。

[0030] 个人计算机（以下称为“PC”）10 具备 USB 总线接口 12、CPU14、RAM 15、硬盘驱动器 (HDD)16、液晶显示器等的显示部 17 以及鼠标和键盘等的输入部 18。这些各结构部通过内部总线 19 相互连接。

[0031] USB 硬盘 20 具备 USB 总线接口 22、访问控制器 30 以及硬盘单元 40。PC 10 的 USB 总线接口 12 与 USB 硬盘 20 的 USB 总线接口 22 之间通过 USB 线缆 60 进行连接，由此能够在 PC 10 与 USB 硬盘 20 之间进行遵照 USB 标准的数据通信。

[0032] 硬盘单元 40 具备作为存储介质的盘 41 以及盘控制器 42。盘控制器 42 对盘 41 写入数据以及从盘 41 读取数据。

[0033] 访问控制器 30 具备小型微计算机以及加密 / 解密部 35，该小型微计算机具备 CPU 31 和 ROM32、RAM33 等。RAM 33 中包括认证状态信息存储部 33a。即，认证状态信息存储部 33a 是形成于 RAM 33 内的规定区域。ROM 32 中包括描述了后述的启动时控制例程和按下按钮时控制例程的计算机程序。

[0034] 访问控制器 30 对从 PC 10 经由 USB 总线接口 22 对硬盘单元 40 进行的访问进行控制。另外，访问控制器 30 还执行用于进行 USB 硬盘 20 与 PC 10 之间的 USB 连接所相关的各种设定 / 控制的通信。

[0035] 访问控制器 30 还执行认证处理，在该认证处理中认证对硬盘单元 40 的访问是否具有合法权限。将表示该认证处理的认证是否成功的状态（已认证状态或未认证状态）的信息作为认证状态信息存储到认证状态信息存储部 33a。对于该认证处理，在后面详细地进行叙述。

[0036] 加密 / 解密部 35 是用于提高 USB 硬盘 20 的安全性的硬件电路，对写入硬盘单元 40 的盘 41 的数据进行加密，并且对从盘 41 读取的数据进行解密。此外，加密 / 解密部 35 也可以不构成为硬件电路，而可以构成为如下结构 :将作为软件的加密处理程序保存在 ROM 32 中，由 CPU 31 执行加密处理程序。

[0037] 另外，USB 硬盘 20 的壳体上安装有按钮 50。按钮 50 与访问控制器 30 电连接。

[0038] 按钮 50 是用于解除处于上述已认证状态的状态的开关，由操作者对按钮 50 进行操作。即，在由操作者按下按钮 50 时，该按钮 50 对访问控制器 30 发送解除指令。访问控制器 30 在从按钮 50 接收到解除指令时，执行对访问控制器 30 进行复位的处理。在后面叙述该处理。

[0039] 接着说明包括上述认证处理的启动时控制例程。图 2 是表示由 USB 硬盘 20 的访问控制器 30 执行的启动时控制例程的流程图。访问控制器 30 所具备的 CPU 31 按照 ROM 32 所存储的规定的计算机程序来执行启动时控制例程。

[0040] 当将 PC 10 与 USB 硬盘 20 相连接（更严格地说，连接开始）时，PC 10 的 USB 总线接口 12 检测作为设备的 USB 硬盘 20 的电连接。一般来说，当由 PC 检测到与 USB 对应的设备的连接时，该设备、在此为 USB 硬盘 20 与 PC 10 之间执行 USB 的标准规格所规定的初始化处理（步骤 S110）。

[0041] 具体地说，例如执行 USB 设备请求的交换、描述符（设备类 (Device Class)、厂家 ID、产品 ID 等）的交换、对作为连接设备的 USB 硬盘 20 的地址分配等。在该初始化处理中，PC 10 对 USB 硬盘 20 进行识别，设定 USB 硬盘 20 的设备类。另外，PC 10 使与所设定的设备类相应的设备驱动器运行。此外，对于作为存储设备的 USB 硬盘 20，一般设定“大容量存储器类 (mass storageclass)”作为其设备类。

[0042] 接着，开始进行认证处理，在该认证处理中认证对 USB 硬盘 20 的访问是否具有合法权限。即，访问控制器 30 通过 PC 10 的显示部 17 来对操作者请求输入口令（步骤 S115）。

[0043] 图 3 是表示口令认证画面 DB 的说明图。如图所示，口令认证画面 DB 具备口令输入栏 PI。决定该口令认证画面 DB 的外观的认证画面用数据被预先存储在盘 41 中，访问控制器 30 的 CPU31 将该外观数据传输到 PC 10 侧，在 PC 10 侧使显示部 17 显示口令认证画

面 DB。此外，也可以构成为认证画面用数据被存储在 ROM 32 而不存储于盘 41 的结构。

[0044] 通过在显示部 17 上显示口令认证画面 DB，对操作者请求输入口令。操作者对输入部 18 进行操作来从口令输入栏 PI 输入预先登记的口令。所输入的口令从 PC 10 被发送到 USB 硬盘 20。

[0045] 返回到图 2，访问控制器 30 所具备的 CPU 31 判断是否通过 USB 总线接口 22 接收到从口令认证画面 DB 输入的口令（步骤 S120）。在此，在判断为接收到口令时（步骤 S120 ：“是”），CPU 31 参照盘 41 所存储的认证表（存储有登记口令的表），判断所接收到的上述口令是否正确、即所接收到的上述口令是否与登记口令一致（步骤 S130）。在此，在判断为口令正确时（步骤 S130 ：“是”），CPU 31 视为认证成功而在认证状态信息存储部 33a 中设置标志（步骤 S140）。

[0046] 在执行步骤 S140 之后，CPU 31 跳到“返回”，暂时结束启动时控制例程。其结果，退出显示口令认证画面 DB 的启动时控制例程，之后能够对 USB 硬盘 20 进行访问。此外，步骤 S115 ～ S130 的处理与应用例 1 中的“认证部”相当，退出该启动时控制例程而能够对 USB 硬盘 20 进行访问的结构与应用例 1 中的“已认证状态保持部”相当。

[0047] 另一方面，在步骤 S 120 中判断为没有接收到口令时（步骤 S120 ：“否”），或者在步骤 S130 中判断为口令不正确时（步骤 S130 ：“否”），CPU 31 将处理返回到步骤 S115。其结果，访问控制器 30 通过 PC 10 的显示部 17 对操作者请求重新输入口令。即，只要没有从口令认证画面 DB 输入正确的口令，在 PC 10 的显示部 17 上就继续显示口令认证画面 DB，从而无法对 USB 硬盘 20 进行之后的访问。此外，设为无法对 USB 硬盘 20 进行访问的这种结构与应用例 1 中的“解密禁止部”相当。

[0048] 执行上述结构的启动时控制例程的结果如下 ：在认证处理的认证成功之后，保持已认证状态，在认证状态信息存储部 33a 中设置表示已认证状态的标志（即，例如设置“1”）。另一方面，在认证处理的认证未成功时，不在认证状态信息存储部 33a 中设置表示已认证状态的标志，从而表示未认证状态（例如，保持“0”）。因而，访问控制器 30 通过根据需要读取认证状态信息存储部 33a 所存储的认证状态信息，能够判断是处于已认证状态还是处于未认证状态。

[0049] 图 4 是表示按下按钮时控制例程的流程图。访问控制器 30 所具备的 CPU 31 按照 ROM 32 所存储的规定的计算机程序来执行按下按钮时控制例程。每隔规定时间（例如 100msec）执行该按下按钮时控制例程。当开始处理时，CPU 31 判断是否由操作者按下了按钮 50（步骤 S210）。根据是否从按钮 50 接收到上述解除指令来进行该判断。在此，在判断为未按下该按钮 50 时（步骤 S210 ：“否”），跳到“返回”并暂时结束该按下按钮时控制例程。

[0050] 另一方面，当在步骤 S210 中判断为按下了按钮 50 时（步骤 S210 ：“是”），CPU 31 对访问控制器 30 进行复位（步骤 S220）。复位的结果如下 ：访问控制器 30 恢复为默认状态（认证状态信息存储部 33a 的标志也被清零为“0”），之后，重新启动访问控制器 30。当重新启动访问控制器 30 时，该访问控制器 30 再次执行上述的启动时控制例程，对操作者请求重新输入口令。即，通过步骤 S220 对访问控制器 30 进行复位，由此能够将认证状态从已认证状态切换为未认证状态（解除已认证状态）。该结构与应用例 1 中的“认证取消部”相当。

[0051] 此外，USB 硬盘 20 构成为如下的结构：在除了按钮 50 被按下时以外，在关闭 PC 10、切断供电时等的经由 USB 总线接口 22 对 PC 进行的连接断开时，也将认证状态从已认证状态切换为未认证状态。

[0052] 根据如上所述构成的本实施例的信息处理系统 100 所具备的 USB 硬盘 20，在由操作者按下按钮 50 时，访问控制器 30 被复位。访问控制器 30 当被复位时，如上所述那样再次执行启动时控制例程，对操作者请求进行利用口令认证画面 DB 的认证。因此，只要认证没有再次成功就无法对 USB 硬盘 20 进行之后的访问。因而，操作者仅通过按下按钮 50 就能够将 USB 硬盘 20 锁定，因此，根据本实施例的 USB 硬盘 20，能够提高进行锁定时的便利性。

[0053] • 第一变形例：

[0054] 在上述实施例中，构成为接收到来自按钮 50 的解除指令的访问控制器 30 通过复位自身来解除已认证状态，但是也可以代替该结构而构成为如下结构：通过对 USB 总线接口 22 处的连接进行软切断或者自动断开 USB 硬盘 20 的电源，来解除已认证状态。总之，只要能够解除已认证状态，就任意结构都可以。

[0055] • 第二变形例

[0056] 在上述实施例中，构成为在基于口令认证的认证不成功的未认证时，禁止包括对写入盘 41 的数据的加密以及对从盘 41 读取的数据的解密在内的整个访问，但是也能够代替该结构而构成为在未认证时仅禁止对数据进行解密。在该结构中，在由操作者按下按钮 50 时，仅禁止上述数据的解密。

[0057] • 第三变形例

[0058] 在上述实施例中，构成为由接收到来自按钮 50 的解除指令的访问控制器 30 立即复位自身，但是也可以代替该结构而构成为如下结构：在 PC 10 与 USB 硬盘 20 之间正进行数据传输的过程中，等待该数据传输结束，之后进行复位。另外，也可以在 USB 硬盘 20 中设置作为警告显示部的 LED，当在上述数据传输过程中按下按钮 50 时，不进行复位而对操作者发出表示错误的意思的警告。

[0059] • 第四变形例

[0060] 在上述实施例中，构成为将表示认证状态（已认证状态或未认证状态）的认证状态信息存储在认证状态信息存储部 33a 中，但是能够省略该认证状态信息存储部 33a。这是因为，在上述实施例中，在处于未认证状态时无法退出显示口令认证画面 DB 的状态，因此在通过了口令认证画面 DB 的情况下能够判断为处于已认证状态。

[0061] • 第五变形例

[0062] 在上述实施例中，采用了以口令对操作者进行认证的口令认证，但是也可以代替该结构而构成为如下结构：采用以 IC 卡等安全卡进行认证的卡认证等其它的认证方法。

[0063] • 第六变形例

[0064] 在上述实施例中，使用了按钮式的开关作为用于将 USB 硬盘 20 设为锁定状态的开关，但是只要是能够由操作者发送规定的操作指令的开关，就能够换成任意方式的开关。另外，按钮 50 被设置于 USB 硬盘 20，但是也可以代替该结构而构成为从 USB 硬盘 20 的外侧进行通知的结构。例如，也可以构成为如下结构：由操作者对 PC 10 进行操作，来从 PC 侧发送表示进行锁定的意思的指示。

[0065] • 第七变形例

[0066] 在上述实施例中，例示了 USB 硬盘作为存储装置，但是能够代替 USB 硬盘而换成 USB 快闪驱动器 (USB 存储器) 等其它存储装置。另外，也可以利用 SD 卡、记忆棒 (memory stick) 等介质与读卡器 (media reader) 的组合来构成存储装置。

[0067] • 第八变形例

[0068] 在上述实施例中，例示了个人计算机作为信息处理装置，但是也可以设为投影仪、传真机装置、路由器、电视装置等其它信息处理装置来代替个人计算机。

[0069] • 第九变形例

[0070] 在上述实施例中，使用了 USB 连接用的接口作为接口，但是也可以代替该结构而构成为通过 IEEE1394、eSATA 等其它接口与信息处理装置进行连接的结构。优选的是利用与热插拔对应的接口的结构。

[0071] • 第十变形例

[0072] 在上述实施例和各变形例中，也可以将利用硬件实现的结构的一部分置换为软件，相反，也可以将利用软件实现的结构的一部分置换为硬件。例如，也可以将由访问控制器 30 的 CPU31 执行的启动时控制例程和按下按钮时控制例程的一部分或全部置换为硬件。作为具体的一例，能够构成为如下结构 :以硬件电路实现原本通过由 CPU 执行的步骤 S210 来以软件方式检测按钮被按下的部分。并且，还能够构成为如下结构 :将启动时控制例程和按下按钮时控制例程的一部分或全部预先存储在盘 41 中，由盘控制器 42 来执行。

[0073] • 第十一变形例

[0074] 在上述实施例中，构成为描述了启动时控制例程和按下按钮时控制例程的计算机程序被存储在访问控制器 30 的 ROM 32，但是也可以代替该结构而构成为上述计算机程序被存储在盘 41。上述计算机程序能够存储于 CD-ROM 等各种存储介质 (计算机可读取的记录介质等) 来进行分发，或通过因特网等各种通信手段进行传送。

[0075] 此外，上述的实施例和各变形例中的结构要素中的除独立权利要求所记载的要素以外的要素是附加的要素，能够适当省略。另外，本发明并不限定于这些实施例和各变形例，在不脱离其宗旨的范围内能够以各种方式实施。

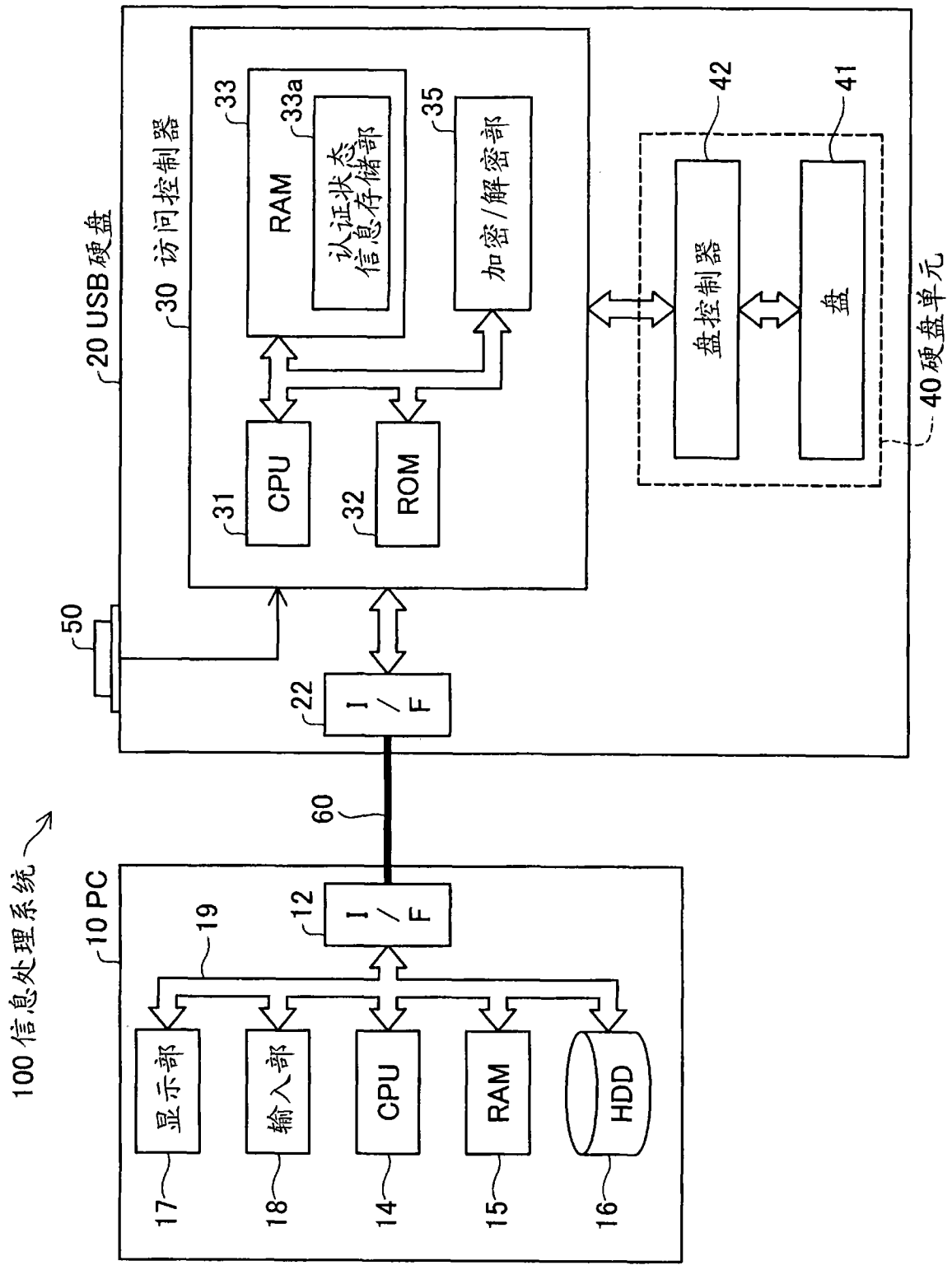

100 信息处理系统
10 PC
19
12
I/F
显示部
输入部
CPU
RAM
HDD
17
18
14
15
16
60
20 USB 硬盘
30 访问控制器
33
RAM
33a
认证状态信息存储部
35
加密/解密部
31
CPU
32
ROM
50
22
I/F
40 硬盘单元
42
盘控制器
41
盘

图 1

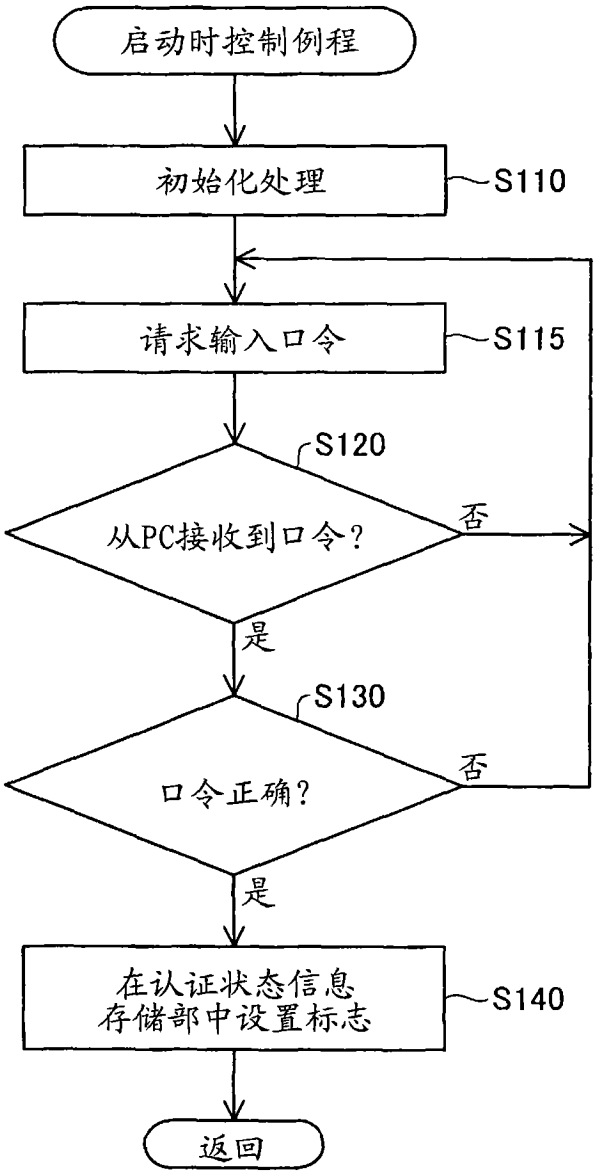

启动时控制例程
初始化处理
S110
请求输入口令
S115
S120
从PC接收到口令？
否
是
S130
口令正确？
否
是
在认证状态信息
存储部中设置标志
S140
返回

图 2

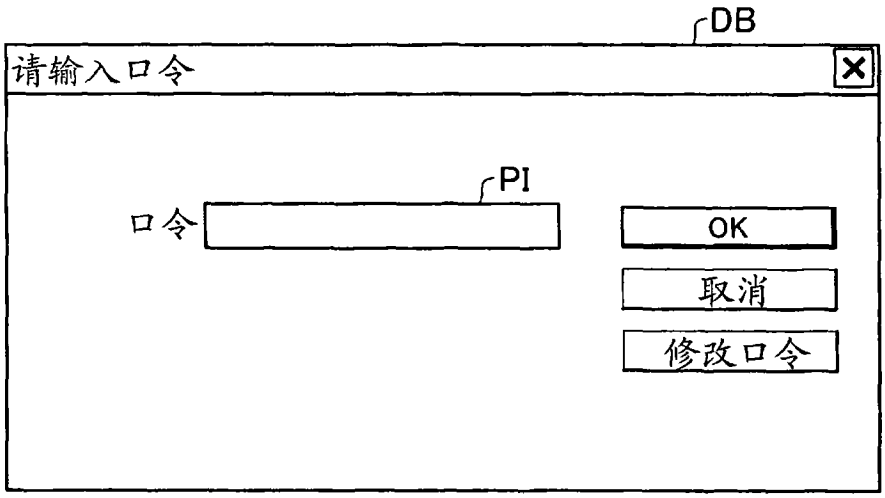

DB
请输入口令
PI
口令
OK
取消
修改口令

图 3

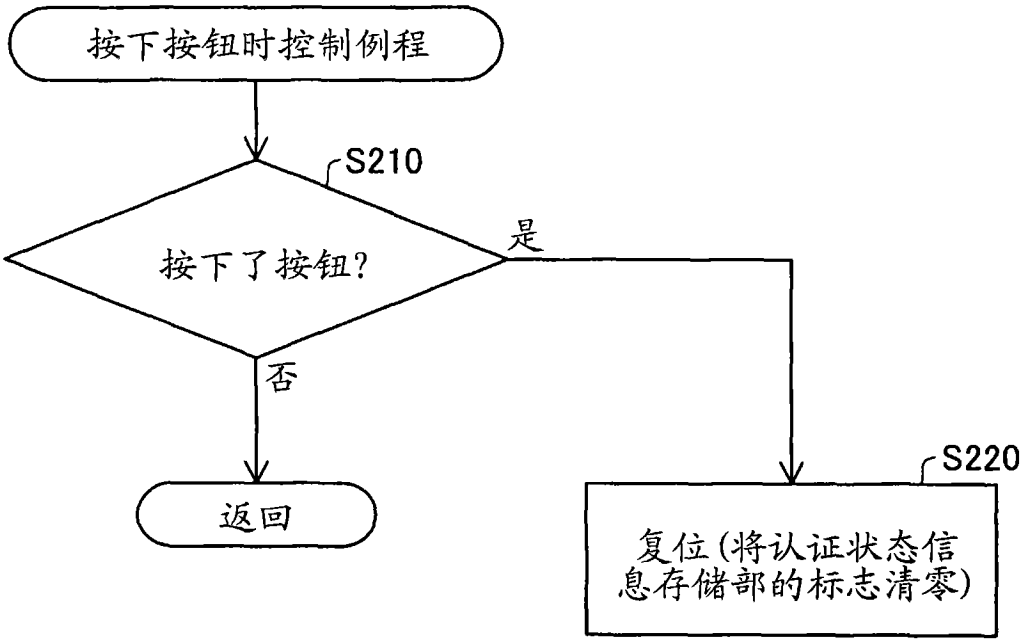

按下按钮时控制例程
S210
按下了按钮?
是
否
返回
S220
复位(将认证状态信息存储部的标志清零)

图 4