[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 12/14 (2006.01)
G06F 21/00 (2006.01)
G06K 19/00 (2006.01)
G06K 19/073 (2006.01)

[12] 发明专利说明书

专利号 ZL 200580012519.0

[45] 授权公告日 2008 年 9 月 17 日

[11] 授权公告号 CN 100419717C

[22] 申请日 2005.4.21
[21] 申请号 200580012519.0
[30] 优先权
[32] 2004. 4.21 [33] JP [31] 126046/2004
[86] 国际申请 PCT/JP2005/007642 2005.4.21
[87] 国际公布 WO2005/103911 日 2005.11.3
[85] 进入国家阶段日期 2006.10.20
[73] 专利权人 株式会社 NTT 都科摩
地址 日本东京
共同专利权人 坂村健 越塚登
[72] 发明人 坂村健 越塚登 石井一彦
寺田雅之 森谦作 本乡节之
[56] 参考文献
US4837422A 1989.6.6
CN1096040C 2002.12.11
CN2585316Y 2003.11.5
审查员 王燕_1
[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

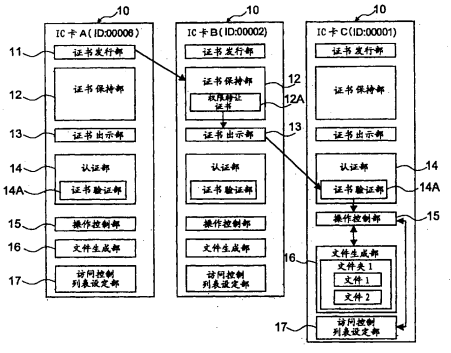
权利要求书 3 页 说明书 10 页 附图 6 页

[54] 发明名称

IC 卡以及权限转让控制方法

[57] 摘要

本发明提供一种 IC 卡以及权限转让控制方法，IC 卡(10)设置有：生成权利价值文件(以下称“文件”)的文件生成部(16)；针对所生成的文件设定访问权限的访问控制列表设定部(17)；在和权限受让方(被转让针对文件访问权限的全部或一部分的权限受让方)之间进行相互认证的同时，对由权限受让方所出示的权限转让证书数据进行验证的认证部(14)；以及通常根据上述设定的访问权限来控制对文件的操作，同时，当权限转让证书数据的验证结果为正常时，取代所设定的访问权限，根据权限转让证书数据所示的访问权限的转让内容，对权限受让方所进行的针对文件的操作进行控制的操作控制部(15)。



1. 一种 IC 卡，其特征在于，该 IC 卡具有：

文件生成单元，其按照来自通信对方的权利价值文件生成请求，以该通信对方为权利价值发行者生成权利价值文件；

文件访问权限设定单元，其按照来自权利价值发行者的访问权限设定请求，针对前述所生成的权利价值文件设定访问权限；

证书发行单元，其发行权限转让证书数据，该权限转让证书数据表示将针对所述权利价值文件所设定的访问权限的全部或一部分转让给所指定的权限受让方；

证书保持单元，其接收并保持所发行的权限转让证书数据；

证书出示单元，其在和权利价值文件保持方进行相互认证时，出示权限转让证书数据；

验证单元，其在权限转让证书数据被出示时，对所出示的权限转让证书数据进行验证；以及

操作控制单元，其在权限转让证书数据的验证结果为正常时，根据该权限转让证书数据所示的访问权限的转让内容，对由该权限转让证书数据出示方所进行的针对上述权利价值文件的操作进行控制。

2. 一种 IC 卡，其特征在于，该 IC 卡具有：

文件生成单元，其按照来自通信对方的权利价值文件生成请求，以该通信对方为权利价值发行者生成权利价值文件；

文件访问权限设定单元，其按照来自权利价值发行者的访问权限设定请求，针对前述所生成的权利价值文件设定访问权限；

证书发行单元，其发行权限转让证书数据，该权限转让证书数据表示根据作为权利价值发行者的自己的访问权限设定请求而设定的访问权限的全部或一部分转让给已指定的权限受让方；

证书保持单元，其作为权限受让方对由权利价值发行者发行的权限转让证书数据进行接收并予以保持；

证书出示单元，其在和已生成权利价值文件的权利价值生成者进行

相互认证时，作为权限受让方出示前述所保持的权限转让证书数据；

认证单元，其作为权利价值生成者，在和权限受让方之间进行相互认证的同时，对权限受让方所出示的权限转让证书数据进行验证；以及

操作控制单元，其根据前述所设定的对权利价值文件的访问权限，对针对前述权利价值文件的操作进行控制，同时，当权限转让证书数据的验证结果为正常时，取代前述访问权限，根据该权限转让证书数据所示的访问权限的转让内容，对由权限受让方进行的针对上述权利价值文件的操作进行控制。

3. 一种 IC 卡，其特征在于，该 IC 卡具有：

文件生成单元，其按照来自通信对方的权利价值文件生成请求，以该通信对方为权利价值发行者生成权利价值文件；

文件访问权限设定单元，其按照来自权利价值发行者的访问权限设定请求，针对前述所生成的权利价值文件设定访问权限；

认证单元，其在与被上述权利价值发行者转让了对上述权利价值文件的访问权限的全部或一部分的权限受让方之间进行相互认证的同时，对权限受让方所出示的权限转让证书数据进行验证，该权限转让证书数据表示将针对权利价值文件所设定的访问权限的全部或一部分转让给所指定的权限受让方；以及

操作控制单元，其根据前述所设定的对权利价值文件的访问权限，对针对前述权利价值文件的操作进行控制，同时，当权限转让证书数据的验证结果为正常时，取代前述访问权限，根据该权限转让证书数据所示的访问权限的转让内容，对由权限受让方进行的针对上述权利价值文件的操作进行控制。

4. 一种权限转让控制方法，其特征在于，该方法具有：

文件生成步骤，成为权利价值生成者的 IC 卡根据来自通信对方的权利价值文件生成请求，以该通信对方为权利价值发行者，在该 IC 卡上生成权利价值文件；

文件访问权限设定步骤，前述权利价值生成者按照来自前述权利价值发行者的访问权限设定请求，针对前述所生成的权利价值文件设定访

问权限；

证书发行步骤，发行权限转让证书数据，该权限转让证书数据表示前述权利价值发行者将根据自己的访问权限设定请求所设定的访问权限的全部或一部分转让给指定的权限受让方；

证书保持步骤，前述权限受让方对前述所发行的权限转让证书数据进行接收并予以保持；

证书出示步骤，在和前述权利价值生成者之间进行相互认证时，前述权限受让方出示前述已被保持的权限转让证书数据；

证书验证步骤，在和前述权限受让方进行相互认证时，前述权利价值生成者对前述所出示的权限转让证书数据进行验证；以及

操作控制步骤，当权限转让证书数据的验证结果为正常时，前述权利价值生成者取代前述所设定的访问权限，根据该权限转让证书数据所示的访问权限的转让内容，对由权限受让方进行的针对权利价值发行者的权利价值文件的操作进行控制。

IC 卡以及权限转让控制方法

技术领域

本发明涉及针对内部已生成的权利价值文件，可以设定向他人转让的访问权限的 IC 卡，以及该访问权限的权限转让控制方法。

背景技术

以往，提出了很多通过 IC 卡来利用电子票，电子货币、电子商品券等权利价值（也称“电子价值”）的技术方案（例如参照以下专利文献 1）。

在这些技术中，当 IC 卡和站台的检票机通信时，由于检票机在物理性质上是一台台不同的装置，因此需要以相同的访问权来操作相同发行者的权力价值。即使是卖票机也因为在物理性质上是一台台不同的装置，因此当 IC 卡和卖票机通信时，有必要发行相同发行者的权力价值。因此，为了提高与站台检票机或卖票机访问的便利性，可以考虑在站台的检票机和卖票机上使用通用的密钥。

专利文献 1：日本特开 2003-198541 号公报

然而，如果在站台的检票机和卖票机上使用通用的密钥，则因使用通用的密钥使机密性受损，恐怕很难确保系统整体的安全性。

这样，在维持安全性的同时要提高访问的便利性较为困难。

发明内容

本发明就是为了解决上述课题而提出的，其目的在于提供一种可以在维持安全性的同时，提高访问的便利性的 IC 卡及权限转让控制方法。

为实现上述目的，本发明所涉及的 IC 卡的特征在于，具有：文件生成单元，其按照来自通信对方的权利价值文件生成请求，以该通信对方为权利价值发行者生成权利价值文件；文件访问权限设定单元，其按照来自权利价值发行者的访问权限设定请求，针对前述所生成的权利价值

文件设定访问权限；证书发行单元，其发行权限转让证书数据，该权限转让证书数据表示将针对所述权利价值文件所设定的访问权限的全部或部分转让给所指定的权限受让方；证书保持单元，其接收并保持所发行的权限转让证书数据；证书出示单元，其在和权利价值文件保持方进行相互认证时，出示权限转让证书数据；验证单元，其在权限转让证书数据被出示时，对所出示的权限转让证书数据进行验证；以及操作控制单元，其在权限转让证书数据的验证结果为正常时，根据该权限转让证书数据所示的访问权限的转让内容，对由该权限转让证书数据出示方所进行的针对上述权利价值文件的操作进行控制。

上述结构的IC卡作为权利价值发行者，权利价值保持者（保持权利价值文件方），以及权限受让方可以进行本发明的特征性的动作。即，成为权利价值发行者的IC卡的证书发行单元发行表示将针对权利价值文件所设定的访问权限的全部或一部分转让给所指定的权限受让方的权限转让证书数据；以及成为权限受让方的IC卡的证书保持单元对上述所发行的权限转让证书数据进行接收并予以保持。而且，权限受让方的证书出示单元在和成为权利价值文件保持者的IC卡进行相互认证时，出示权利转让证书数据；以及权利价值保持者的认证单元对所出示的权限转让证书数据进行验证。此处，当权限转让证书数据的验证结果为正常时，权利价值保持者的操作控制单元根据该权限转让证书数据所示的访问权限的转让内容，对由出示了该权限转让证书数据方（权限受让方）所进行的针对权利价值文件的操作进行控制。

这样，根据权限转让证书数据所示的访问权限的转让内容，权限受让方可以对该权利价值文件进行操作。另外，对权利价值发行者来说，根据自己发行的权限转让证书数据所示的访问权限的转让内容， 也可以使权限受让方操作权利价值文件。

这样，通过对权利价值文件事先设定访问权限，在维持系统整体的安全性的同时，可以对权利价值文件自由地进行访问权限的权限转让，因此能够提高访问的便利性。

另外，为了实现上述目的，本发明所涉及的IC卡的特征在于，具有：

文件生成单元，其按照来自通信对方的权利价值文件生成请求，以该通信对方为权利价值发行者生成权利价值文件；文件访问权限设定单元，其按照来自权利价值发行者的访问权限设定请求，针对前述所生成的权利价值文件设定访问权限；证书发行单元，其发行权限转让证书数据，该权限转让证书数据表示根据作为权利价值发行者的自己的访问权限设定请求而设定的访问权限的全部或一部分转让给已指定的权限受让方；证书保持单元，其作为权限受让方对由权利价值发行者发行的权限转让证书数据进行接收并予以保持；证书出示单元，其在和已生成权利价值文件的权利价值生成者进行相互认证时，作为权限受让方出示前述所保持的权限转让证书数据；认证单元，其作为权利价值生成者，在和权限受让方之间进行相互认证的同时，对权限受让方所出示的权限转让证书数据进行验证；以及操作控制单元，其根据前述所设定的对权利价值文件的访问权限，对针对前述权利价值文件的操作进行控制，同时，当权限转让证书数据的验证结果为正常时，取代前述访问权限，根据该权限转让证书数据所示的访问权限的转让内容，对权限受让方针对上述权利价值文件的操作进行控制。

另外，本发明所涉及权限转让控制方法的特征在于，具有：文件生成步骤，成为权利价值生成者的 IC 卡根据来自通信对方的权利价值文件生成请求，以该通信对方为权利价值发行者，在该 IC 卡上生成权利价值文件；文件访问权限设定步骤，前述权利价值生成者按照来自前述权利价值发行者的访问权限设定请求，针对前述所生成的权利价值文件设定访问权限；证书发行步骤，发行权限转让证书数据，该权限转让证书数据表示前述权利价值发行者将根据自己的访问权限设定请求所设定的访问权限的全部或一部分转让给指定的权限受让方；证书保持步骤，前述权限受让方对前述所发行的权限转让证书数据进行接收并予以保持；证书出示步骤，在和前述权利价值生成者之间进行相互认证时，前述权限受让方出示前述已被保持的权限转让证书数据；证书验证步骤，在和前述权限受让方进行相互认证时，前述权利价值生成者对前述所出示的权限转让证书数据进行验证；以及操作控制步骤，当权限转让证书数据的

验证结果为正常时，前述权利价值生成者取代前述所设定的访问权限，根据该权限转让证书数据所示的访问权限的转让内容，对由权限受让方进行的针对权利价值发行者的权利价值文件的操作进行控制。

在如上的发明中，成为权利价值生成者的IC卡可以根据来自通信对方的权利价值文件生成请求，以该通信对方为权利价值发行者，在该IC卡上生成权利价值文件。另外，权利价值生成者可以根据来自权利价值发行者的访问权限设定请求，设定针对上述所生成的权利价值文件的访问权限。

在生成权利价值文件以及针对该权利价值文件进行设定访问权限的状态下，权利价值发行者发行表示将根据自己的访问权限设定请求所设定的访问权限的全部或一部分转让给所指定的权限受让方的权限转让证书数据时，上述权限受让方对所发行的权限转让证书数据进行接收并予以保存。接着，权限受让方在和权利价值生成者之间进行相互认证时，出示所保持的权限转让证书数据。收到出示的权利价值生成者在和权限受让方进行相互认证时，对该出示的权限转让证书数据进行验证。当权限转让证书数据的验证结果为正常时，权利价值生成者取代所设定的访问权限，根据该权限转让证书数据所示的访问权限的转让内容，对由权限受让方进行的针对权利价值发行者的权利价值文件的操作进行控制。即，并非是对权利价值文件预先设定的访问权限，而是权限受让方根据权限转让证书数据所示的访问权限的转让内容，可以对该权利价值文件进行操作。另外，对于权利价值发行者来说，根据自己发行的权限转让证书数据所示的访问权限的转让内容，也可以使权限受让方操作权利价值文件。

这样，通过对权利价值文件预先设定访问权限，可以维持系统整体的安全性，同时可以针对权利价值文件自由地进行访问权限的权限转让，由此可以提高访问的便利性。

另外，本发明所涉及的IC卡在作为权利价值生成者的结构，尤其是操作控制单元的结构上具有特征。即，本发明所涉及的IC卡的特征在于，具有：文件生成单元，其按照来自通信对方的权利价值文件生成请求，

以该通信对方为权利价值发行者生成权利价值文件；文件访问权限设定单元，其按照来自权利价值发行者的访问权限设定请求，针对前述所生成的权利价值文件设定访问权限；认证单元，其在与被上述权利价值发行者转让了对上述权利价值文件的访问权限的全部或一部分的权限受让方之间进行相互认证的同时，对权限受让方所出示的权限转让证书数据进行验证，该权限转让证书数据表示将针对权利价值文件所设定的访问权限的全部或一部分转让给所指定的权限受让方；以及操作控制单元，其根据前述所设定的对权利价值文件的访问权限，对针对前述权利价值文件的操作进行控制，同时，当权限转让证书数据的验证结果为正常时，取代前述访问权限，根据该权限转让证书数据所示的访问权限的转让内容，对由权限受让方进行的针对上述权利价值文件的操作进行控制。

通过上述的操作控制单元，通常根据所设定的针对权利价值文件的访问权限，对针对权利价值文件的操作进行控制，同时，当根据认证单元的权限转让证书数据的验证结果为正常时，取代访问权限，根据该权限转让证书数据所示的访问权限的转让内容，对由权限受让方进行的针对权利价值文件的操作进行控制。这样，通过对权利价值文件预先设定访问权限，可以维持系统整体的安全性，同时可以自由地进行针对权利价值文件的访问权限的权限转让，从而能够提高访问的便利性。

根据本发明，通过对权利价值文件预先设定访问权限，可以维持系统整体的安全性，同时可以自由地进行针对权利价值文件的访问权限的权限转让，从而能够提高访问的便利性。

附图说明

图 1 是表示发明实施方式中的 IC 卡结构的功能框图。

图 2 是表示访问控制列表设定部的结构例的图。

图 3 是表示文件夹的访问控制列表的一例的图。

图 4 是表示文件夹 1 的各个文件的访问控制列表的一例的图。

图 5 是表示权限转让证书数据的一例的图。

图 6 是用于说明有关权限转让控制的一系列处理的流程图。

符号说明

10．IC 卡；11．证书发行部；12．证书保持部；12A．权限转让证书数据；13．证书出示部；14．认证部；14A．证书验证部；15．操作控制部；16．文件生成部；17．访问控制列表设定部；17A．文件夹的访问控制列表；17B．文件的访问控制列表

具体实施方式

下面，对有关本发明所涉及的IC卡以及权限转让控制方法的实施方式进行说明。

图1是表示本实施方式中的3个IC卡10（IC卡A～C）结构的功能框图。在本实施方式中，以IC卡A为权利价值发行者，以IC卡B为权利价值受让方，以IC卡C为权利价值生成者，对各自的动作处理例进行说明，详细后叙。不过，各个IC卡都具有作为权利价值发行者，权利价值受让方以及权利价值生成者工作所需的结构。

具体而言，如图1所示，各个IC卡10构成为包含：文件生成部16，其根据来自通信对方的权利价值文件的生成请求，以该通信对方为权利价值发行者，生成权利价值文件（以下只称“文件”）并予以保持；访问控制列表设定部17，其根据来自权利价值发行者的访问权限设定请求，将对上述所生成的文件的访问权限作为后述的访问控制列表进行设定并予以保持；证书发行部11，其发行权限转让证书数据12A，该权限转让证书数据12A表示将根据作为权利价值发行者的自己的访问权限设定请求所设定的访问权限的全部或一部分，转让给已指定的权限受让方；证书保持部12，其接收由权利价值发行者发行的权限转让证书数据12A并予以保持；证书出示部13，其在和已生成了文件的权利价值生成者进行相互认证时，出示上述被保持的权限转让证书数据12A；认证部14，其包含证书验证部14A，与通信对方之间进行相互认证，该证书验证部14A对从作为权限受让方的通信对方出示的权限转让证书数据12A进行验证；操作控制部15，其根据所设定的访问权限，对针对文件的操作进行控制，同时，当权限转让证书数据12A的验证结果为正常时，取代上述

的访问权限，根据权限转让证书数据 12A 所示的访问权限的转让内容，对针对权限受让方的文件操作进行控制。

作为 IC 卡 10，存在多个相同结构的 IC 卡，不过，在各个 IC 卡 10 上预先分配有独特的识别信息（以下称“ID”）。认证部 14 保存有证明该 ID 的 ID 证书（未图示）。

在各个 IC 卡 10 上可以生成新文件。此时，在所生成的文件上，附加有是谁请求生成该文件的权利价值发行者信息（以下称“发行者 ID”）。

如上所述，在 IC 卡 10 上生成新文件的情况下，权利价值发行者可以针对来自自己以外的访问，限制对该文件的访问（这里指，复制/转让）。即，权利价值发行者可以在生成文件时设定文件的访问控制列表，用以限制自己以外的人是否可以对文件进行复制/转让。另外，在上述的访问工作中，复制相当于发行通票。除特殊情形以外，复制被设定成“不可”。

例如，如图 4 所示，在文件的访问控制列表 17B 中，保存有文件 1、文件 2 等各个文件的表示是否允许复制的信息、是否允许转让的信息、以及发行者 ID 信息。该文件的访问控制列表 17B 通过访问控制列表设定部 17 进行设定并被保持。

在图 1 的例子中，根据来自作为权利价值发行者的 IC 卡 A 的权利价值生成请求以及访问权限设定请求，IC 卡 C 作为权利价值生成者生成/保持文件 1，并对该文件 1 的访问控制列表 17B 进行设定/保持。

另外，IC 卡 C 可以限制其他的 IC 卡对该 IC 卡 C 进行文件生成/读取/转让。此时，IC 卡 C 可以设定文件夹，该文件夹含有自己保持的 1 个以上的文件，可以设定访问控制列表，用以限制针对已设定的文件夹，其他的 IC 卡是否可以生成/读取/转让该文件夹内的文件。另外，在上述的访问工作中，生成相当于例如权利价值的受让，读取相当于权利价值的查询余额。

例如，如图 3 所示，在文件夹的访问控制列表 17A 中保存有表示是否允许对文件夹 1、文件夹 2 等各个文件夹进行读取的信息、进行生成的信息以及进行转让的信息。如图 2 所示，文件夹的访问控制列表 17A 被与各个文件夹的文件的访问控制列表 17B 相关联地存储在访问控制列表

设定部 17 中。

在图 5 中，显示了权限转让证书数据 12A 的一例。如该图 5 所示，权限转让证书数据 12A 包含有权限转让方的 IC 卡 ID（此处为 IC 卡 A 的 ID“00006”），权限受让方的 IC 卡的 ID（此处为 IC 卡 B 的 ID“00002”），表示转让内容的转让访问权（此处为“读取：许可”、“复制：不可”、“转让：许可”），以及权限转让方的署名（此处为 IC 卡 A 的署名）。

下面，沿着图 6 的流程图，以 IC 卡 A 为权利价值发行者，IC 卡 B 为权利价值受让方，IC 卡 C 为权利价值生成者，对其各自工作时的具体处理流程进行说明。

首先，作为第 1 阶段，在图 6 的 S1～S4 中，对通过 IC 卡 A（权利价值发行者）请求 IC 卡 C（权利价值生成者），在 IC 卡 C 内生成文件 1 的处理进行说明。

即，在 S1 中，在 IC 卡 A、C 之间互相出示 ID 证书，按照以往所知的 PKI 的构造进行相互认证。此处，若认证成功（S2），则 IC 卡 A 对 IC 卡 C 发出文件 1 的生成请求以及对文件 1 的访问权限设定请求（S3）。IC 卡 C 收到后，根据请求，通过文件生成部 16 生成/保持文件 1，同时，通过访问控制列表设定部 17 设定文件 1 的访问控制列表。

此处，例如，假定为 IC 卡 C 已在包含现有的文件 2 的文件夹 1 中生成了文件 1。如图 3 所示，假定有关文件夹 1 的访问控制列表被设定为“读取：许可”、“生成：许可”、“转让：许可”。另外，如图 4 所示，假定有关文件 1 的访问控制列表被设定为“读取：不可”、“复制：不可”、“转让：不可”。

完成上述的文件生成以及访问控制列表的设定后，文件生成成功的意思从 IC 卡 C 通知给 IC 卡 A。

接着，作为第 2 阶段，在 S5～S9 中，对 IC 卡 B 在被 IC 卡 A 转让权限之前，要读取 IC 卡 C 内的文件 1 的情况的处理进行说明。

即，在 S5 中，在 IC 卡 B、C 之间互相出示 ID 证书，按照以往所知的 PKI 的结构进行相互认证。此处，若认证成功（S6），则 IC 卡 B 试行 IC 卡 C 内的文件 1 的读取（S7）。具体而言，向 IC 卡 C 发出读取文件 1

的请求。收到该请求的IC卡C对文件1的访问权、以及包含文件1的文件夹1的访问权进行调查（S8）。另外，文件夹1的访问权如前面所述，所有的动作都被“许可”，因此不能构成对文件1的访问限制。另一方面，在文件1的访问权中，如图4所示，由于被设定成“读取：不可”，因此S8的调查结果为“不可读取文件1”。因此，IC卡C向IC卡B通知不可读取文件1，由IC卡B进行的文件1的读取试行失败（S9）。

最后，作为第3阶段，在S10～S19中，对IC卡B被IC卡A转让了权限之后，要读取IC卡C内的文件1的情况的处理进行说明。

即，在S10中，作为权利价值（文件1）的发行者的IC卡A生成针对权限受让方的IC卡B的权限转让证书数据（S10）。这里，如图5所示，假设作为对文件1的访问权限被设定成“读取：许可”、“复制：不可”、“转让：许可”。于是，IC卡A将生成的权限转让证书数据发送给IC卡B（S11），IC卡B将权限转让证书数据保持在证书保持部12中（参照图1）。

在S12中，ID证书在IC卡B、C之间相互出示，按照以往所知的PKI的结构进行相互认证。此处，若认证成功（S13），则IC卡B向IC卡C出示权限转让证书数据（S14）。收到出示的IC卡C对该权限转让证书数据进行验证（S15）。此处，一旦验证成功（S16），则IC卡B试行读取IC卡C内的文件1（S17）。具体而言，对IC卡C发送文件1的读取请求。接收到该请求的IC卡C对权限转让证书数据中的文件1的访问权、以及包含文件1的文件夹1的访问权进行调查（S18）。此处，如前面所言，由于文件夹1的访问权所有的动作都被设成了“许可”，因此不构成对文件1的访问限制。另一方面，在权限转让证书数据中的文件1的访问权，如图5所示，被设成了“读取：许可”，因此，S18的调查结果为“允许读取文件1”。由此，IC卡C成为允许由IC卡B读取文件1，由IC卡B读取文件1的试行成功（S19）。

如上所述，根据本发明的实施方式，通常，如图6的S5～S9所示，按照对预先设定的文件1的访问权，对针对文件1的操作进行控制，当权限转让证书数据的验证结果为正常时，取代上述的访问权，根据权限

转让证书数据所示的访问权限的转让内容，控制权限受让方（IC 卡 B）对文件 1 的操作。由此，在维持系统整体安全性的同时，可以自由地进行对文件的访问权限的权限转让，从而可以提高访问文件的便利性。

产业上的可利用性

本发明针对内部已生成的权利价值文件，以可以设定能向他人转让访问权限的 IC 卡、以及该访问权限的权限转让控制方法为使用用途，在维持安全性能的同时，能够提高访问的便利性。

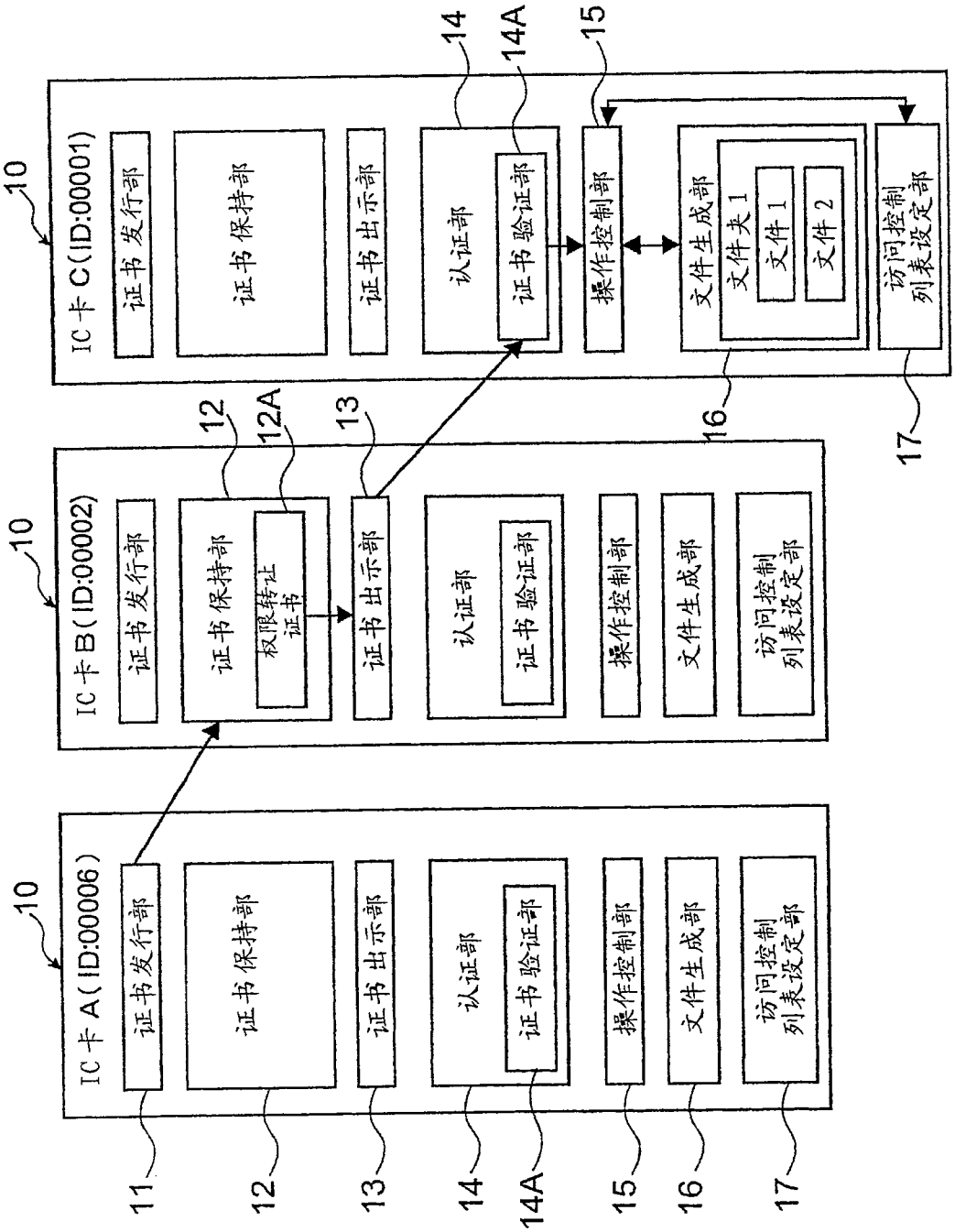

IC卡A(ID:00006)
证书发行部
证书保持部
证书出示部
认证部
证书验证部
操作控制部
文件生成部
访问控制列表设定部
IC卡B(ID:00002)
证书发行部
证书保持部
权限转让证书
证书出示部
认证部
证书验证部
操作控制部
文件生成部
访问控制列表设定部
IC卡C(ID:00001)
证书发行部
证书保持部
证书出示部
认证部
证书验证部
操作控制部
文件生成部
文件夹1
文件1
文件2
访问控制列表设定部
10
11
12
12A
13
14
14A
15
16
17

图 1

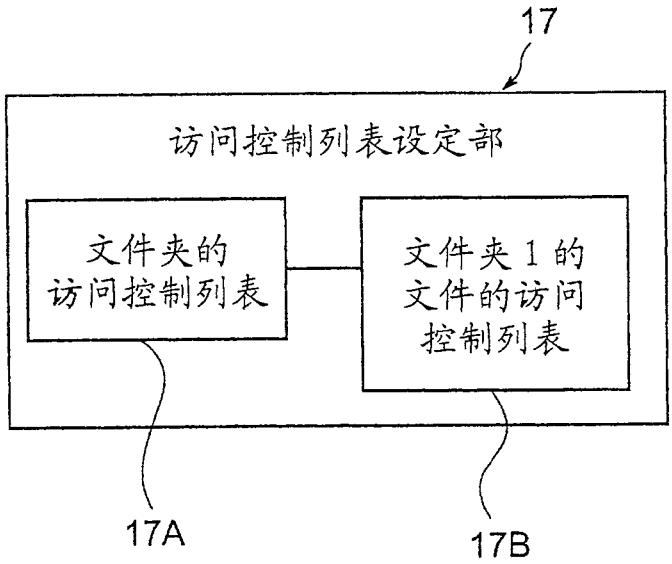


图 2

17A

	读取	生成	转让
文件夹 1	许可	许可	许可
文件夹 2	不可	许可	不可
⋮			

图 3

17B

	复制	转让	发行者 ID
文件夹 1	不可	不可	00006
文件夹 2	不可	不可	00003
⋮			

图 4

12A

权限转让方	00006
权限受让方	00002
转让访问权	读取：许可 复制：不可 转让：许可
A 的署名	

图 5

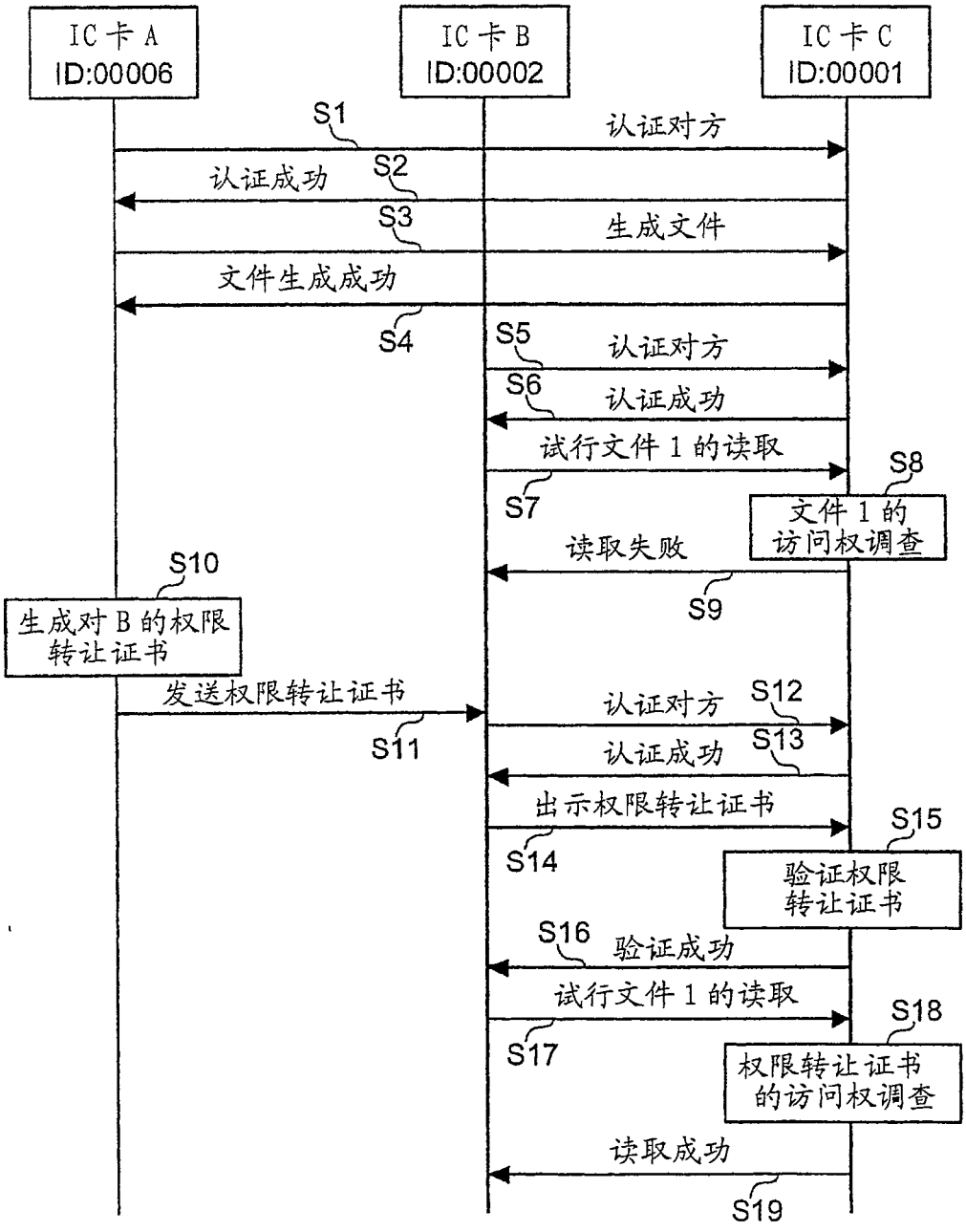

IC卡A
ID:00006
IC卡B
ID:00002
IC卡C
ID:00001
S1
认证对方
S2
认证成功
S3
生成文件
文件生成成功
S4
S5
认证对方
S6
认证成功
试行文件1的读取
S7
S8
文件1的
访问权调查
读取失败
S9
S10
生成对B的权限
转让证书
发送权限转让证书
S11
S12
认证对方
S13
认证成功
出示权限转让证书
S14
S15
验证权限
转让证书
S16
验证成功
试行文件1的读取
S17
S18
权限转让证书
的访问权调查
读取成功
S19

图 6