(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 1835456 B
(45)授权公告日 2010.05.26

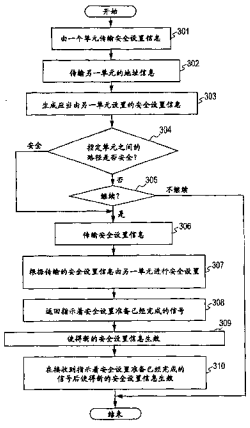
(21)申请号 200610065317.9
(22)申请日 2006.03.17
(30)优先权数据
080235/2005 2005.03.18 JP
239029/2005 2005.08.19 JP
(73)专利权人 佳能株式会社
地址 日本东京都
(72)发明人 土肥纯 丹治雅道
(74)专利代理机构 北京怡丰知识产权代理有限公司 11293
代理人 于振强
(51)Int.Cl.
H04L 12/24(2006.01)
H04L 29/06(2006.01)
(56)对比文件
CN 1411200 A,2003.04.16, 全文.
JP 2000022775 A,2000.01.21, 全文.
CN 1581777 A,2005.02.16, 全文.
审查员 张畅
权利要求书 2 页 说明书 11 页 附图 10 页

(54)发明名称

通信系统、通信设备以及通信方法

(57)摘要

在本发明的通信系统中，当第一设置信息被设置到至少两个设备的第一设备时，根据用于执行至少两个设备之间的预定处理的第一设置信息自动生成第二设置信息，其中第二设置信息为至少两个设备中的第二设备而生成。接着，该通信系统将自动生成的第二设置信息传输到第二设备。否则，该通信系统将自动生成的第二设置信息写到便携式记录介质上，使得该第二设备可以从该便携式记录介质读取第二设置信息。



CN 1835456 B

1. 一种通信系统，包括：

信息生成装置，当第一设置信息被设置到第一设备上时，所述信息生成装置根据用于执行所述第一设备和第二设备之间的预定处理的所述第一设置信息而生成第二设置信息，该第二设置信息是为了所述第二设备而生成；

信息传输装置，用于将由该信息生成装置生成的所述第二设置信息传输到该第二设备；以及

设置装置，用于将从所述信息传输装置传输的所述第二设置信息设置到所述第二设备，

其中设置所述第一设置信息和所述第二设置信息中的每一个，使得数据可以在所述第一设备和所述第二设备之间具有安全性地传送。

2. 根据权利要求 1 的通信系统，进一步包括通知装置，用于通知所述第一设备由所述设置装置设置到所述第二设备的所述第二设置信息已经生效。

3. 根据权利要求 1 的通信系统，其中从所述信息传输装置传输的所述第二设置信息包括关于由所述设置装置设置到所述第二设备的所述第二设置信息开始生效的开始时间的信息，并且其中由所述设置装置设置的所述第二设置信息根据开始时间信息而被使用。

4. 一种通信系统，包括：

信息生成装置，当第一设置信息被设置到第一设备上时，所述信息生成装置根据用于执行所述第一设备和第二设备之间的预定处理的所述第一设置信息而自动生成第二设置信息，该第二设置信息是为了所述第二设备而生成；

信息写入装置，将由所述信息生成装置生成的所述第二设置信息写到连接至所述第一设备的至少一个便携式记录介质上；

信息读出装置，当该至少一个便携式记录介质连接至所述第二设备时，该信息读出装置从该至少一个便携式记录介质读出该第二设置信息；

以及设置装置，用于将由所述信息读出装置读出的所述第二设置信息设置到所述第二设备。

5. 根据权利要求 4 的通信系统，进一步包括信息确定装置，用于确定由所述信息读出装置读出的所述第二设置信息是否包含显示所述第二设备的地址为源地址的设置信息，

其中当所述信息确定装置确定所述第二设置信息包含显示所述第二设备的地址为源地址的设置信息时，所述设置装置将由所述信息读出装置读出的所述第二设置信息设置到所述第二设备。

6. 根据权利要求 4 的通信系统，其中设置每个所述第一设置信息和所述第二设置信息，使得数据可以在所述第一设备和所述第二设备之间具有安全性地传送。

7. 一种通信设备，包括：

信息生成装置，当第一设置信息被设置到通信设备时，该信息生成装置根据用于执行在所述通信设备和外部设备之间的预定处理的所述第一设置信息生成第二设置信息，所述第二设置信息被提供给所述外部设备；以及

信息传输装置，用于将由所述信息生成装置生成的所述第二设置信息通过至少一个网络传输到所述外部设备，

其中设置所述第一设置信息和所述第二设置信息中的每一个，使得数据可以在所述通

信设备和所述外部设备之间具有安全性地传送。

8. 一种通信设备，包括：

信息生成装置，当第一设置信息被设置到通信设备时，该信息生成装置根据所述第一设置信息生成提供给外部设备的第二设置信息，使得在该通信设备和所述外部设备之间执行预定的处理；以及

信息写入装置，用于将由所述信息生成装置生成的所述第二设置信息写在插入该通信设备的至少一个便携式记录介质上。

9. 一种通信方法，包括步骤：

当第一设置信息被设置到第一设备时，根据用于执行所述第一设备和第二设备之间的预定处理的所述第一设置信息生成第二设置信息，该第二设置信息被提供给所述第二设备；

将在信息生成步骤生成的所述第二设置信息从所述第一设备传输到所述第二设备；以及

将在信息传输步骤传输的所述第二设置信息设置到所述第二设备，

其中设置所述第一设置信息和所述第二设置信息中的每一个，使得数据可以在所述第一设备和所述第二设备之间具有安全性地传送。

10. 一种通信方法，包括步骤：

当第一设置信息被设置到第一设备上时，根据用于执行所述第一设备和第二设备之间的预定处理的所述第一设置信息生成第二设置信息，该第二设置信息被提供给所述第二设备，所述第二设备与所述第一设备配对；

将在信息生成步骤生成的所述第二设置信息写到连接至所述第一设备的至少一个便携式记录介质上；

当该便携式记录介质连接至所述第二设备时，从该便携式记录介质读出在信息写入步骤写入的该第二设置信息；

将在信息读出步骤读出的所述第二设置信息设置到所述第二设备。

通信系统、通信设备以及通信方法

技术领域

[0001] 本发明涉及一种通信系统、一种通信设备以及一种通信方法，特别地涉及一种设置技术，当在两个设备之间执行预定的处理时，该设置技术适于将用于在两个设备之间执行预定处理的设置信息设置到该两个设备中的至少一个。

背景技术

[0002] 在过去，各种通信方法用于在两个设备之间通过通信网络且具有安全性地传送数据。例如，使用了利用安全套接字协议层 (SSL) 的系统，利用公共密钥和专用密钥的系统等。上述的系统在例如日本专利公开 No. 2000-22775 中被披露。

[0003] 进一步，已经使用了涉及安全性的技术，该技术适于增强安全性强度并且防止使用着至少一个该设备的普通用户知晓所进行的设置，因此保证了安全性。

[0004] 然而，根据已知的技术，尤其是根据在数据传送系统的分层的低级上所执行的涉及安全的技术，困难的是进行用于具有安全性地传送数据的设置。进一步，通常只为在两个设备之间执行的数据传送进行设置（在一对一的基础上）。在这种情况下，容易在设置中发生错误。因此，即使系统的管理员相信数据传送设置的可靠性，系统经常会因为设置中的错误而未能传送数据。

发明内容

[0005] 当用于执行数个设备之间的预定处理的设置信息被设置到数个设备中的每一个上时，本发明使得设置信息被正确而自动地设置到数个设备中的至少一个上。

[0006] 根据本发明的一个实施例的通信系统包括信息生成单元，当第一设置信息被设置到至少两个设备中的第一设备上时，所述信息生成单元配置为根据用于执行至少两个设备之间的预定处理的第一设置信息而生成第二设置信息，该第二设置信息是为了该至少两个设备的第二设备而生成；信息传输单元，配置为将由该信息生成单元生成的第二设置信息传输到该第二设备；以及设置单元，配置为将从信息传输单元传输的第二设置信息设置到第二设备，其中设置所述第一设置信息和所述第二设置信息中的每一个，使得数据可以在所述第一设备和所述第二设备之间具有安全性地传送。

[0007] 进一步，根据本发明另一个实施例的通信系统包括信息生成单元，当第一设置信息被设置到至少两个设备中的第一设备上时，所述信息生成单元配置为根据用于执行至少两个设备之间的预定处理的第一设置信息而生成第二设置信息，该第二设置信息是为了该至少两个设备的第二设备而生成，该第二设备与该第一设备配对；信息写入单元，配置为将由信息生成单元生成的第二设置信息写在至少一个插入第一设备的便携式记录介质上；信息读出单元，当该便携式记录介质插入第二设备时，该信息读出单元配置为从该便携式记录介质读出该第二设置信息；以及设置单元，用于将由信息读出单元读出的第二设置信息设置到第二设备。

[0008] 本发明的进一步特征将从以下参考附图对示例性实施例进行的描述中变得明显。

附图说明

[0009] 图 1 表示了根据本发明实施例的网络系统的示例性结构；

[0010] 图 2 示意性地表示了图 1 的多功能外围设备 (MFP) 以及个人计算机 (PC) 的示例性结构；

[0011] 图 3 为表示根据本发明第一实施例的网络系统的示例性操作的流程图；

[0012] 图 4 表示根据本发明的一个方面的用于生成设置信息的例子；

[0013] 图 5 表示了根据本发明的一个方面的用于生成设置信息的示例性指定；

[0014] 图 6 同样表示了根据本发明的一个方面的用于生成设置信息的示例性指定；

[0015] 图 7 表示根据本发明一个方面的用于生成设置信息的另一个示例；

[0016] 图 8 为表示根据本发明第二实施例的 MFP 的示例性操作的流程图；

[0017] 图 9 为表示根据第二实施例的 PC 的示例性操作的流程图；

[0018] 图 10 为表示根据本发明第三实施例的 MFP 的示例性操作的流程图；

[0019] 图 11 为表示根据第三实施例的 PC 的示例性操作的流程图；

[0020] 图 12 表示了根据本发明的一个方面的、存储根据安全设置菜单传输的设置信息的记录区域；

[0021] 图 13 表示了根据本发明的一个方面的、存储根据安全设置菜单传输的设置信息的另一个记录区域。

具体实施方式

[0022] 接下来，将参考附图对本发明的实施例进行描述。

[0023] 第一实施例

[0024] 图 1 表示使用了根据本发明任何一个实施例的通信系统的示例性网络系统的配置。如图 1 所示，上述的网络可以具有各种连接到该网络的设备，包括多功能外围设备（此后称为 MFP）101、个人计算机（此后称为 PC）102 和 103 等等。进一步，MFP101、PC102 和 103 等通过局域网（此后称为 LAN）100 彼此相连。

[0025] 在图 1 所示的网络系统中，给每个连接到 LAN100 的上述设备 (MFP 101 和 PC102 和 103) 分配一个地址。在这里，将 MFP 101、PC102 和 103 等等两两相连的网络并不限于上述的 LAN100，而是可以为任意网络。

[0026] 图 2 为示意性地表示图 1 所示的 MFP101、PC102 和 PC103 的示例性结构的框图。

[0027] 如图 2 所示，上述包括 MFP101、PC102 和 PC103 等等的设备的每一个包括中央处理单元 (CPU) 202 和作为例如 ROM 的非易失存储器而提供的只读存储器 (ROM) 203，以及作为例如 RAM 的临时存储器而提供的随机存取存储器 (RAM) 204。进一步，上述设备的每一个包括用于输入单元 (KB) 210 的输入单元控制器 (KBC) 205，以及用于显示单元 (CRT) 211 的显示单元控制器 (CRTC) 206。进一步，上述设备的每一个包括用于硬盘驱动器 (HDD) 212 和磁盘单元 (FD/ 等) 213 的磁盘单元控制器 (DKC) 207。进一步，上述设备的每一个包括用于本地接口 (USB/ 等) 214 的接口控制器 (IFC) 208 以及包括网络接口卡 (NIC) 的网络单元控制器 209。上述的功能单元通过系统总线 201 彼此相连因此功能单元可以彼此通信。

[0028] 进一步，由于 MFP101 执行例如打印的处理，MFP101 包括打印控制器 (PRC) 215 以及

打印机引擎 216，该打印机引擎配置为实际执行打印。进一步，MFP101 可以包括各种单元，包括扫描器、传真机等等，且并不对本发明的优势产生影响。

[0029] CPU202 通过执行记录在 ROM203 和 / 或 HDD212 上或是由 FD213 提供的至少一个程序而共同地控制着连接到系统总线 201 的上述功能单元。也就是说，CPU202 从 ROM203、HDD212 或 FD213 读出至少一个适于执行所需要操作的处理程序，并且执行该处理程序，其中 CPU202 执行用于执行所需要操作的控制。上述的功能单元根据传输自 CPU202 的指令或类似彼此联系地运行，从而全部的设备得以运行。

[0030] ROM203 存储 CPU202 读取的指令（程序）或类似。进一步，在 MFP101 中，用于打印的关于字体或类似的信息可以存储在 ROM203 中。RAM204 作为 CPU202 的主存储器、工作区域等等而运行。如果单元的电源关闭，存储在 RAM204 中的数据可能会丢失。

[0031] KBC205 处理从包括键盘、鼠标等等的输入单元 (KB)210 传输的信息。CRTC206 控制包括 CRT 显示单元、液晶显示单元等等的显示单元 (CRT)211。DKC207 控制固定 HDD212 和 / 或例如软盘的可移动盘单元 (FD/ 等)213。IFC208 控制包括通用串行总线 (USB)、串行端口等等的本地接口 (USB/ 等)214。NIC209 连接到图 1 所示的 LAN100 因此 NIC209 控制网络通信。

[0032] 如果在通过通信网络彼此相连的设备之间执行了要求安全的处理，则通常使用例如 IPSec 的安全性技术，因此在一对一的基础上在设备之间进行设置。在这种情况下，涉及设置的信息包括应当被机密地掌握的信息。进一步，如果仅仅是设置信息的一部分出错，执行处理都会变得困难。此外，由于进行设置比较复杂，通常需要渊博的知识和技术。因此，如果在第一实施例的网络系统的设备间执行预定的处理，执行预定处理所需要的设置就会正确且容易地完成，即使在设置复杂的情况下。接下来，对网络系统的示例性操作进行描述。

[0033] 以下详细描述根据第一实施例的网络系统的操作。图 3 是表示了上述网络系统所执行操作的流程图，其中的操作涉及设置处理。接下来，对涉及在如图 1 所示的 MFP101 和 PC102 之间执行的数据传送的一对一安全性设置进行描述。

[0034] 首先，在 MFP101 中，管理员或用户通过使用例如键盘的输入单元 210 和 / 或例如 CRT- 显示单元的显示单元，根据 MFP101 的安全设置菜单（没有显示）来指定需要的设置或是管理员或用户想要完成的设置。另一方面，在步骤 S301，MFP101 输入指示着由用户指定的设置的设置信息。

[0035] 接着，如果用户想要在 MFP101 和 PC102 之间传送数据，则用户指定 PC102 的地址 (IP 地址 :192.168.1.101)、对应于 PC102 的子网掩码以及 PC102 用来传送数据的端口号。在步骤 S302，MFP101 传输关于上述由用户指定的 IP 地址、子网掩码以及端口号的信息。在步骤 S301 和步骤 S302，传输的设置信息被存储在 RAM204 和 / 或 HDD212 中。

[0036] 图 12 和 13 的每一个表示了其上记录有根据安全设置菜单传输的设置信息的示例性记录区域。每一个上述记录区域提供在 RAM204 和 / 或 HDD212 中。

[0037] 首先，在步骤 302，传输的地址信息作为目标地址被设置到记录区域 1201。接着，在步骤 302，传输的子网掩码信息作为目标地址的子网掩码被设置到记录区域 1202 子网掩码。例如，“255.255.255.248”被设置到记录区域 1202。术语“子网掩码”指的指示着每个设备的 IP 地址的哪一位代表网络地址的数据。

[0038] 接着，由于在第一实施例中 MFP101 是信息源，所以“192.168.1.100”就作为源地

址被设置到记录区域 1203。进一步，关于对应于信息源的子网掩码的信息被写入记录区域 1204，与目标地址的子网掩码的情况一样。

[0039] 进一步，关于协议号的信息被设置到记录区域 1205，以指定用于进行了安全设置的数据传送的协议的类型。根据指定的协议号，对于用于 MFP101 和 PC102 之间的每一个数据传送协议而言安全设置会生效。

[0040] 在步骤 302，传输的端口号信息作为目标端口号被设置到记录区域 1206。关于用于数据传送的信息源所使用的端口号的信息作为源端口号被设置到记录区域 1207。进一步，关于用于执行安全处理的处理方法的信息被设置到记录区域 1208。

[0041] 指示着双向传送系统打开和 / 或指示着双向传送系统关闭的信息被设置到记录区域 1209，该信息作为当上述的安全设置生效时指示着数据可以被传送的方向的信息。当双向传送系统打开时，上述的安全设置在执行双向数据传送时（从 MFP101 传送数据到 PC102 并反之亦然）生效。当双向传送系统关闭时，上述的安全设置只有在数据从一个设备传送到另一个设备时（在本实施例中，从 MFP101 传送数据到 PC102）生效。

[0042] 图 13 表示了其上记录有涉及安全设置的详细设置信息项目的记录区域。关于密钥交换模式的信息被设置到记录区域 1301。该密钥交换模式表示了加密密钥如何在上述的设备之间进行交换。例如，如果选择了“互联网密钥交换 (IKE)”作为密钥交换模式，就可以选择主要模式和 / 或主动模式。

[0043] 关于数据传送到的另一端（第一实施例中的 PC102）的地址的信息作为另一端的地址被设置到记录区域 1302。在紧靠着数据传送实际开始之前所使用的专用密钥上的数据（也即一字节字符串）作为预共享专用密钥被设置到记录区域 1303。

[0044] 关于安全设置的更为详细的信息作为建议被设置到记录区域 1304。该建议指的是从一个设备（第一实施例中的 MFP101）传输到另一个设备（第一实施例中的 PC102）的请求。可以指定几种类型的建议使得其它的设备可以根据要求选择并使用任何一种建议。稍后将参考图 6 对上述的建议进行描述。

[0045] 现在返回图 3，在步骤 303，MFP101 自动生成设置信息，该设置信息应当根据在步骤 301 和 302 传输的信息被传送到 PC102。在步骤 303 生成的信息例如图 4 和图 5 所示。

[0046] 图 4 表示了其上记录有在步骤 303 生成的设置信息的记录区域。每一个记录区域提供在 RAM204 和 / 或 HDD212 中。由于第一实施例中目标是对于 PC102 而言的 MFP101，所以“192.168.1.100”作为目标地址被设置到记录区域 401。接着，“255.255.255.248”作为例如目标地址的子网掩码被设置到例如记录区域 402 中。

[0047] 接下来，由于第一实施例中 PC102 是对于 PC102 而言的信息源，“192.168.1.101”作为源地址被设置到记录区域 403。进一步，关于对应于信息源的子网掩码的信息作为源地址的子网掩码被写到记录区域 404 上，与目标地址的子网掩码的情况一样。

[0048] 进一步，关于协议号的信息被设置到记录区域 405，以指定用于进行了安全设置的数据传送的协议的类型。根据指定的协议号，对于用于 MFP101 和 PC102 之间的每一个数据传送协议而言，安全设置开始生效。

[0049] 用于目标设备进行数据传送的关于端口号的信息作为目标端口号被设置到记录区域 406。进一步，关于源设备用以传送数据的端口号的信息作为源端口号被设置到记录区域 407。关于用于执行安全处理的处理方法的信息被设置到记录区域 408。指示着双向

传送系统打开和/或指示着双向传送系统关闭的信息被设置到记录区域409，该信息作为当上述的安全设置生效时指示着数据可以被传送的方向的信息。当双向传送系统打开时，上述的安全设置在执行双向数据传送时（从MFP101传送数据到PC102并反之亦然）生效。当双向传送系统关闭时，上述的安全设置只有在数据从一个设备传送到另一个设备时（在第一实施例中从MFP101传送数据到PC102）生效。

[0050] 图5表示了其上记录有涉及安全设置的详细设置信息项目的记录区域。每一个上述记录区域都提供在RAM204和/或HDD212中。关于密钥交换模式的信息被设置到记录区域501。该密钥交换模式表示了加密密钥如何在上述的设备之间进行交换。例如，如果选择了“互联网密钥交换（IKE）”作为密钥交换模式，就可以选择主要模式和主动模式中的一个。

[0051] 关于数据传送到的另一端（第一实施例中的MFP101）的地址的信息作为另一端的地址被设置到记录区域502。在紧靠着数据传送实际开始之前所使用的专用密钥上的数据（也即一字节字符串）作为预共享专用密钥被设置到记录区域503。

[0052] 关于安全设置的更为详细的信息作为建议被设置到记录区域504。该建议指的是从一个设备（第一实施例中的MFP101）传输到另一个设备（第一实施例中的PC102）的请求。可以指定几种类型的建议使得其它的设备可以根据要求选择并使用任何一种建议。

[0053] 图6详细表示了建议的例子。鉴别算法字段表示了允许上述设备彼此鉴别的方法。加密算法字段表示了实际用于执行数据传送的加密方法。寿命类型字段和寿命字段表示了直到安全设置变化开始的时间期间以及数据量。从安全设置生效开始经过了预定的时间期间后，或是在预定数量的数据传送后，上述设备根据写在寿命字段中的信息取消安全设置并且用不同的新的密钥数据取代当前密钥数据。由于适于取消安全设置并且通过使用不同的新的密钥数据开始执行处理的方法对于本发明来说并非重要的，因此对该方法不作描述。

[0054] MFP101执行下面的处理，以在上述的每个PC上生成涉及安全设置的设置信息。首先，MFP101将记录在记录区域1201、1202以及1206上的信息设置到记录区域403、404以及407上。接着，MFP101将记录在记录区域1203、1204以及1207上的信息设置到记录区域401、402和406上。进一步，MFP101将记录在记录区域1205、1208以及1209上的信息设置到记录区域405、408和409上，并且将记录在记录区域1301、1302、1303以及1304上的信息设置到记录区域501、502、503和504上。这样，在步骤303，MFP101自动生成涉及安全设置的设置信息，其中生成的设置信息被传送到PC102，PC102作为将数据传送到的另一端设备（一对设备中的一个）而工作。

[0055] 参考图3，在步骤304，MFP101检查在MFP101和PC102之间传送数据所通过的通信路径（在第一实施例中为LAN100）上是否存在有安全的数据传送路径，以便传送所生成的设置信息到PC102。然而，由于MFP101检查的通信路径是已知的数据传送路径，就可能没有安全的数据传送路径。

[0056] 如果没有安全的数据传送路径，在步骤305，MFP101确认MFP101是否应当被连接到另一端的设备。也就是说，在步骤305，MFP101确认是否应当继续处理。在第一实施例中，已经作了选择当不存在安全的数据传送路径时不将MFP101连接到另一端的设备（上述的选择是提前在步骤301作出的）。否则，MFP101可以询问用户（在步骤301作出上述选

择的用户）MFP101 是否应当连接到另一端的设备。如果用户发出 MFP101 不连接到另一端的设备的指令，MFP101 可以放弃在步骤 301 传输的安全设置信息。

[0057] 如果在步骤 304 确认存在已知的安全数据传送路径，或是确认不存在安全数据传送路径并且处理应当继续时，MFP101 前进到步骤 306。接着，在步骤 306，MFP101 将在步骤 303 自动生成的设置信息传输到用作另一端设备的 PC102。

[0058] 在步骤 307，PC102 接收到涉及安全设置且在步骤 306 传输的设置信息，根据该设置信息作出安全设置，并且为使得安全设置生效而做准备。也就是说，在步骤 307，PC102 仅仅作出上述的准备而并不实际上使得安全设置生效。当使用 PC 102 时，用户可以通过使用例如键盘的输入单元和 / 或例如 CRT 显示单元的显示单元而从 PC102 的安全设置菜单指定需要的设置。然而，当 PC102 在步骤 306 进行安全设置时，从 MFP101 传输的设置信息被设置到一记录区域，在该记录区域上应当记录根据 PC102 的安全设置菜单传输的设置信息。

[0059] 在为根据所传输的设置信息生成的安全设置做好准备之后，PC102 在步骤 308 将指示着准备已完成的信号传送到 MFP101。上述的信号可以包括任何类型的数据，只要 MFP101 被通知安全设置准备已经完成。

[0060] 紧接着上述的信号被传送到 MFP101 之后，PC102 在步骤 309 使得准备的安全设置生效。另一方面，在接收到上述从 PC102 处传输的信号后，MFP101 在步骤 310 使得在步骤 301 传输的安全设置生效。

[0061] 接着，就有可能通过在由步骤 301 传输的设置信息所指定的端口和 / 或协议上使用安全设置而在上述的两个设备，也就是，MFP101 和 PC102 之间具有安全性地传送数据。

[0062] 这样，当在例如第一实施例的网络系统中的上述设备的两个设备之间传送数据需要一对一基础的设置时，用户仅为两个设备中的一个进行安全设置使得为另一设备自动生成设置信息。进一步，所生成的设置信息被传输到另一设备，从而由另一设备根据所传输的设置信息来进行安全设置。这样，如果用户仅为两个设备中的一个进行复杂的设置，对另一设备的设置信息就会自动生成。这样，就可能减少设备的管理员的工作负担并且减少由于管理员的操作错误而发生的数据传送问题。

[0063] 在第一实施例中，上述两个设备中的一个设备 (MFP101 或类似）将安全设置信息传输到另一设备 (PC102 或类似）。当另一设备根据传输给另一设备的设置信息而将指示着安全设置准备已完成的信号传输返回给上述两个设备中的一个设备时，新设置的安全设置就实际生效。然而，本发明并不限于第一实施例。也就是，如图 7 所示，关于设置生效的开始时间的数据被写入从一个设备传输给另一个设备的安全设置信息。如果两个设备中的每一个都根据开始时间数据使得安全设置生效，本发明的优势不会受到影响。每一个设备都可以从所提供的实时时钟 (RTC) 获取时间数据。

[0064] 进一步，除了安全设置信息的开始时间信息项目，关于网络时间协议 (NTP) 服务器的地址的信息可以被加进安全设置信息，如图 7 所示。两个设备的每一个都根据 NTP 服务器的地址访问 NTP 服务器，从 NTP 服务器获取时间信息，并且在对应于所写的开始时间信息的时间实际使得安全设置生效。

[0065] 因此，如在第一实施例中所描述的，两个设备的每一个都在预定的时间（也即，指定的时间）使得安全设置生效。然而，可以配置为两个设备中的每一个都进行涉及安全设置的准备并且将涉及安全设置的信息存储在非易失记录单元（例如，ROM203 和 / 或

HDD212) 上。接着，如果设备的电源关闭并且再次打开，则根据所存储的安全设置信息生成的安全设置可以得以生效。进一步，可以配置为设备被复位，因此当设备的电源关闭时，设备执行与电源再次打开时所执行的操作相同的操作，并且根据所存储的安全设置信息生成的安全设置得以生效。

[0066] 第二实施例

[0067] 接下来，描述本发明的第二示例性实施例。在第一实施例中，由两个设备中的一个自动生成的设置信息从一个设备通过网络传输给另一个设备。然而，在根据第二实施例的网络系统中，由两个设备中的一个设备自动生成的设置信息通过使用便携式记录介质传输给另一个设备。

[0068] 由于第二实施例的网络系统及其所提供的设备具有与第一实施例的相同的配置，因此对其的描述在此省略并且只按照需要提供参考着图 1 和图 2 的第二实施例网络系统的操作的描述。在以下的描述中，对用于示例的涉及在图 1 所示的 MFP101 和 PC102 之间执行的数据传送（网络通信）的一对一基础安全设置进行了说明。

[0069] 首先，描述 MFP101 根据第二实施例执行的操作。图 8 为表示了由第二实施例的 MFP101 执行的示例性操作的流程图。

[0070] 首先，网络管理员或类似通过使用例如键盘的输入单元 210 和 / 或例如 CRT 显示单元的显示单元 211 从 MFP101 的安全设置菜单（没有显示）指定执行 MFP101 和 PC102 之间的网络通信所需要的设置。接着，MFP101 在步骤 S801 输入指示着由网络管理员或类似指定的设置的信息。在步骤 S801 传输的信息被存储在 RAM204 和 / 或 HDD212 中。图 12 和图 13 的每一个表示了其上记录有根据安全设置菜单传输的设置信息的记录区域。每一个记录区域提供在 RAM204 和 HDD212 中。接着，在步骤 S802，MFP101 一直等待直到便携式记录介质被插入磁盘单元 (FD/ 等)213 和 / 或本地接口 (USB/ 等)214。这里，便携式记录介质以可移动的方式插入到上述的每个单元。该便携式记录介质可以是例如 USB 存储器。

[0071] 当便携式记录介质插入磁盘单元 (FD/ 等)213 和 / 或本地接口 (USB/ 等)214 中时，MFP101 前进到步骤 S803，从而 MFP101 根据在步骤 S801 所传输的设置信息自动生成应当被 PC102 使用的设置信息。在步骤 S803 生成的设置信息例如图 4 和图 5 所示。

[0072] 这样，在步骤 S803，MFP101 在 PC102 上自动生成涉及安全设置的设置信息，该 PC102 为来自 MFP101 的数据被传送到的另一个设备（一对设备中的一个）。接着，在步骤 S804，MFP101 将在步骤 S803 生成的设置信息写在插入磁盘单元 213 和 / 或本地接口 214 的便携式记录介质上。

[0073] 在 PC102 使用的安全设置信息被写在便携式记录介质上之后，在步骤 S805，MFP101 使得显示单元 211 产生一消息，该消息称该便携式记录介质可以被移动。当该便携式记录介质被网络管理员或类似从 MFP101 移走，该处理就终止了。

[0074] 图 9 为表示第二实施例的 PC102 所执行的示例性操作的流程图。首先，在步骤 S901，PC102 一直等待直到网络管理员将便携式记录介质插入 PC102 的磁盘单元 (FD/ 等)213 和 / 或本地接口 (USB/ 等)214。应当注意的是 PC102 所使用的安全设置信息，以及已经由 MFP101 自动生成的安全设置信息如图 8 所示地通过上述从步骤 S801 到步骤 S805 所执行的处理而被记录到便携式记录介质上。

[0075] 当便携式记录介质插入磁盘单元 (FD/ 等)213 和 / 或本地接口 (USB/ 等)214 中

时，PC102 前进到步骤 S902，从而从所插入的便携式记录介质读取其上的安全设置信息。

[0076] 接着，在步骤 S903，PC102 根据在步骤 S902 从便携式记录介质所读取的安全设置信息而进行其自身的安全设置。当使用 PC102 时，用户可以通过使用例如键盘的输入单元 210 和 / 或例如 CRT 显示单元的显示单元 211 从 PC102 的安全设置菜单指定所需要的设置。然而，当 PC102 在步骤 S903 进行安全设置时，从便携式记录介质读取的设置信息被设置到一个记录区域，在该记录区域上应当记录根据 PC102 的安全设置菜单而传输的设置信息。

[0077] 当在 PC102 上进行了安全设置之后，PC102 前进到步骤 S904，从而 PC102 使得显示单元 211 产生一消息，该消息称该便携式记录介质可以被移动。当插入到磁盘单元 213 和 / 或本地接口 214 中的该便携式记录介质被网络管理员或类似移走，该处理就终止了。

[0078] 这样，由于根据由在步骤 S801 传输的设置信息指定的端口号和 / 或协议而生成的安全设置，数据就可以在上述的两个设备，也即，MFP101 和 PC102 之间安全地传送。

[0079] 这样，根据第二实施例，就可以得到与第一实施例相同的优势。进一步，在第二实施例中，由两个设备中的一个自动生成的设置信息通过便携式记录介质从一个设备传输到另一个设备，并且另一个设备根据自动生成的设置信息进行安全设置。接着，涉及安全设置的设置信息并没有在网络上流动。因此，就可能防止设置信息被外来者看见，籍此安全设置可以安全地进行。

[0080] 第三实施例

[0081] 接下来，对本发明的第三实施例进行描述。在根据第三实施例的网络系统中，当执行两个设备之间预定的处理需要以一对一为基础设置时，由两个设备中的一个自动生成的设置信息通过使用便携式记录介质被传输到另一个设备。进一步，每一个设备确定存储在便携式记录介质上的设置信息是否是为其自身生成的设置信息或是为不同的设备生成的。

[0082] 由于第三实施例的网络系统和其所提供的设备具有与第一实施例的网络系统和设备相同的配置，因此省略对其的描述。也就是说，仅提供对第三实施例网络系统的操作的描述。在下面的描述中，涉及数据传送的以一对一为基础进行的安全设置针对每一对设备进行，例如图 1 所示的 MFP101 和 PC102，以及 MFP101 和 PC103，从而执行例如 MFP101 和 PC102 以及 MFP101 和 PC103 之间的网络通信。

[0083] 现在参考图 10 的流程图对根据第三实施例的 MFP101 的示例性操作进行描述。首先，网络管理员或类似通过使用例如键盘的输入单元 210 和 / 或例如 CRT 显示单元的显示单元 211 从 MFP101 的安全设置菜单（没有显示）指定执行 MFP101 和 PC 102 之间的网络通信所需要的设置。接着，MFP101 在步骤 S1001 输入指示着由网络管理员或类似指定的设置的信息。之后网络管理员或类似通过使用输入单元 210 和 / 或显示单元 211 从 MFP101 的安全设置菜单（没有显示）指定执行 MFP101 和 PC103 之间的网络通信所需要的设置。接着，MFP101 在步骤 S1002 传输指示着由网络管理员或类似指定的设置的信息，和步骤 S1001 的情况相同。在步骤 S1001 和步骤 S1002 传输的每一个设置信息被分别存储在 RAM204 和 / 或 HDD212 中。接着，在步骤 S1003，MFP101 一直等待直到便携式记录介质被插入到磁盘单元 (FD/ 等)213 和 / 或本地接口 (USB/ 等)214 中。这里，该便携式记录介质指的是例如 USB 存储器。

[0084] 例如，当网络管理员或类似将便携式记录介质插入磁盘单元 (FD/ 等)213 和 / 或本地接口 (USB/ 等)214 中时，MFP101 前进到步骤 S1004，从而 MFP101 根据在步骤 S1001 所

传输的设置信息自动生成应当被 PC102 使用的设置信息。在步骤 S1004 生成的设置信息例如对应于图 4 和图 5 所示的信息。

[0085] 接下来，在步骤 S1005，MFP101 根据在步骤 S1002 传输的信息自动生成应当被 PC103 使用的设置信息。在步骤 S1005 生成的设置信息对应于例如图 4 和图 5 所示的信息，与在步骤 S1004 生成的设置信息的情况相同。然而，根据在步骤 S1004 生成的设置信息，例如，显示为“192.168.1.101”的 PC102 的地址变为源地址。进一步，根据在步骤 S1005 生成的设置信息，显示为“192.168.1.102”的 PC103 的地址变为源地址。

[0086] 接着，在步骤 S1006，MFP101 将在步骤 S1004 和在步骤 S1005 生成的设置信息写在插入在例如磁盘单元 213 和 / 或本地接口 214 的便携式记录介质上。

[0087] 在 MFP101 将涉及 PC102 和 PC103 的每一个的安全设置的设置信息写在便携式记录介质上之后，MFP101 前进到步骤 S1007，从而 MFP101 使得显示单元 211 产生一消息，该消息称该便携式记录介质可以被移动。当该便携式记录介质被网络管理员或类似从 MFP101 移走，该处理就终止了。在图 10 中，MFP101 执行涉及 PC102 的处理并且执行涉及 PC103 的处理。然而，并不限于第三实施例，MFP 可以根据需要首先执行涉及 PC103 的处理。

[0088] 接着，将参考图 11 对根据第三实施例的 PC102 和 PC103 的操作进行描述，图 11 表示说明了根据第三实施例的 PC102 的操作的流程图。PC103 执行与 PC102 根据图 11 的流程图执行的操作相似的操作。首先，在步骤 S1101，PC102 一直等待直到网络管理员或类似将便携式记录介质插入 PC102 的磁盘单元 (FD/ 等)213 和 / 或本地接口 (USB/ 等)214。当便携式记录介质插入磁盘单元 (FD/ 等)213 和 / 或本地接口 (USB/ 等)214 中时，PC102 前进到步骤 S1102，从而从所插入的便携式记录介质读取安全设置信息。

[0089] 接着，在步骤 S1103，PC102 确定从便携式记录介质读取的安全设置信息是否包括显示着 PC102 的地址为源地址的设置信息。在第三实施例中，PC102 的地址显示为“192.168.1.101”。于是，PC102 确定从便携式记录介质读取的安全设置信息是否包括显示着源地址为“192.168.1.101”的设置信息。

[0090] 当在步骤 S1103 确定没有设置信息显示 PC102 的地址为源地址时，PC102 前进到步骤 S 1104，使得显示单元 (CRT)211 产生一个错误消息，该消息指示着没有用于 PC102 的设置信息。之后，PC102 没有进行安全设置，前进到步骤 S1106。在步骤 S1106，PC102 使得显示单元 211 产生一个消息，该消息指示着便携式记录介质可以被移动。当该便携式记录介质被网络管理员或类似移走，该处理就终止了。

[0091] 相反地，如果在步骤 S1103 确定有设置信息显示 PC102 的地址为源地址，则 PC102 前进到步骤 S1105，以根据上述的设置信息进行其自身的安全设置。当 PC102 在步骤 S1105 进行安全设置时，从便携式记录介质读取的设置信息被设置到一个记录区域，在该记录区域上应当记录根据 PC102 的安全设置菜单而传输的设置信息。

[0092] 在进行了安全设置之后，PC102 前进到步骤 S1106，因此 PC102 使得显示单元 211 产生一消息，该消息指示着该便携式记录介质可以被移动。当插入到磁盘单元 213 和 / 或本地接口 214 的该便携式记录介质被网络管理员或类似移走，该处理就终止了。

[0093] 接着，和对 PC102 的操作一样，参考图 11 对根据第三实施例的 PC103 的操作进行描述。首先，在步骤 S1101，PC103 一直等待直到网络管理员或类似将便携式记录介质插入 PC102 的磁盘单元 (FD/ 等)213 和 / 或本地接口 (USB/ 等)214。当便携式记录介质插入磁

盘单元 (FD/ 等)213 和 / 或本地接口 (USB/ 等)214 中时,PC103 前进到步骤 S1102,从而从所插入的便携式记录介质读取安全设置信息。

[0094] 接着,在步骤 S1103, PC103 确定在步骤 S1102 从便携式记录介质读取的安全设置信息是否包括显示着 PC103 的地址为源地址的设置信息。在第三实施例中, PC103 的地址显示为“192. 168. 1. 102”。于是,PC103 确定从便携式记录介质读取的安全设置信息是否包括显示着源地址显示为“192. 168. 1. 102”的设置信息。

[0095] 当确定没有设置信息显示 PC103 的地址为源地址时, PC103 前进到步骤 S1104,使得显示单元 (CRT)211 或类似产生一个错误消息,该消息指示着没有生成用于 PC103 的设置信息。之后,PC103 没有进行安全设置,前进到步骤 S1106。在步骤 S1106,PC103 使得显示单元 211 产生一个消息,该消息指示着便携式记录介质可以被移动。当该便携式记录介质被网络管理员或类似移走,该处理就终止了。

[0096] 相反地,如果在步骤 S1103 确定有设置信息显示 PC103 的地址为源地址,则 PC103 前进到步骤 S1105,以根据上述的设置信息进行其自身的安全设置。

[0097] 在进行了安全设置之后, PC103 前进到步骤 S1106,因此 PC103 使得显示单元 211 产生一消息,该消息指示着该便携式记录介质可以被移动。当插入到磁盘单元 213 和 / 或本地接口 214 的该便携式记录介质被网络管理员或类似移走,PC103 就终止了该处理。

[0098] 当 PC103 在步骤 S1105 进行安全设置时,从便携式记录介质读取的设置信息被设置到一记录区域,在该记录区域上应当记录根据 PC103 的安全设置菜单而传输的设置信息。

[0099] 这样,由于根据由在步骤 S1001 传输的设置信息指定的端口号和 / 或协议而生成的安全设置,数据就可以在 MFP101 和 PC102 之间安全地传送。进一步,由于根据由在步骤 S1002 传输的设置信息指定的端口号和 / 或协议而生成的安全设置,数据就可以在 MFP101 和 PC103 之间安全地传送

[0100] 如上所述,第三实施例实现了与第一和第二实施例相同的优势。进一步,每一个设备确定从便携式记录介质读取的设置信息是否被提供给其自身并且根据确定结果进行安全设置。也就是说,每一个设备可以仅根据提供给其自身的设置信息进行适当的安全设置。

[0101] 本发明的其它示例性实施例,特征以及方面

[0102] 应当可以理解的是,还可以通过将用于完成上述实施例的功能的软件的程序码提供给系统和 / 设施来实现本发明,从而该系统或设施的计算机 (CPU 和 / 或 MPU) 可以使得该系统和 / 或设施根据程序码进行操作。

[0103] 在这种情况下,程序码本身实现上述实施例的功能,并且程序码本身构成了本发明。进一步,将上述的程序码提供给计算机的设备,也就是存储上述程序码的记录介质或类似同样构成了本发明。

[0104] 存储程序码的记录介质可以是,例如,软盘,硬盘,光盘,磁光盘, CD-ROM,磁带,非易失性存储卡,ROM 等。此外,如果上述的程序码被存储在根据第二实施例和 / 或第三实施例的便携式记录介质中,同样也成为了本发明的一个实施例。

[0105] 进一步,不仅是通过执行提供的程序码的计算机,还可以通过运行在计算机上的与操作系统 (OS) 协同工作的程序码或其它的应用软件,来实现上述实施例的功能。后者同样也是本发明的一个实施例。

[0106] 在本发明的另一个实施例中，所提供的程序码可以被写入位于插入计算机的功能扩展板或连接到计算机的功能扩展设备中的存储器上。这样，在功能扩展板和 / 或功能扩展设备上提供的 CPU 或类似就可以根据程序码的指令执行部分或全部的处理。

[0107] 虽然参照上述实施例对本发明进行了描述，但是应当理解，本发明的技术范围并不限于上述的实施例。对下面的权利要求书的范围应当给与最广泛的解释从而包含了所有的修改、等同结构和功能，而没有背离本发明的技术精神和主要特征。

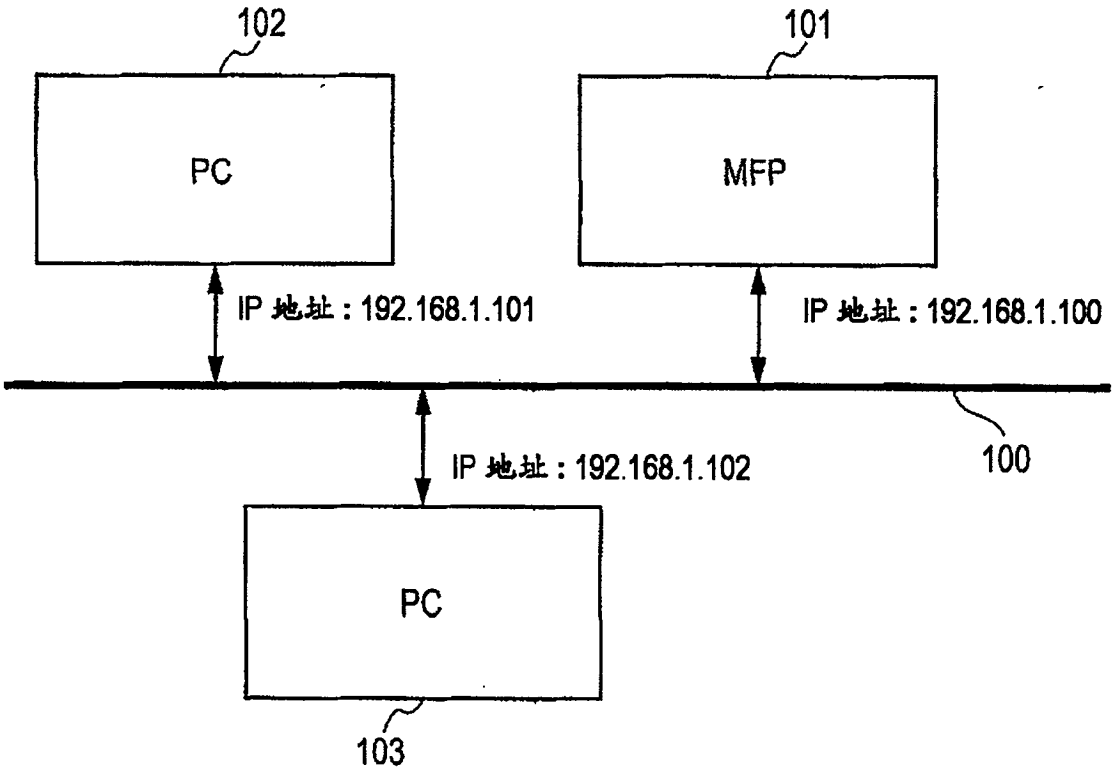

102
101
PC
MFP
IP 地址：192.168.1.101
IP 地址：192.168.1.100
100
IP 地址：192.168.1.102
PC
103

图 1

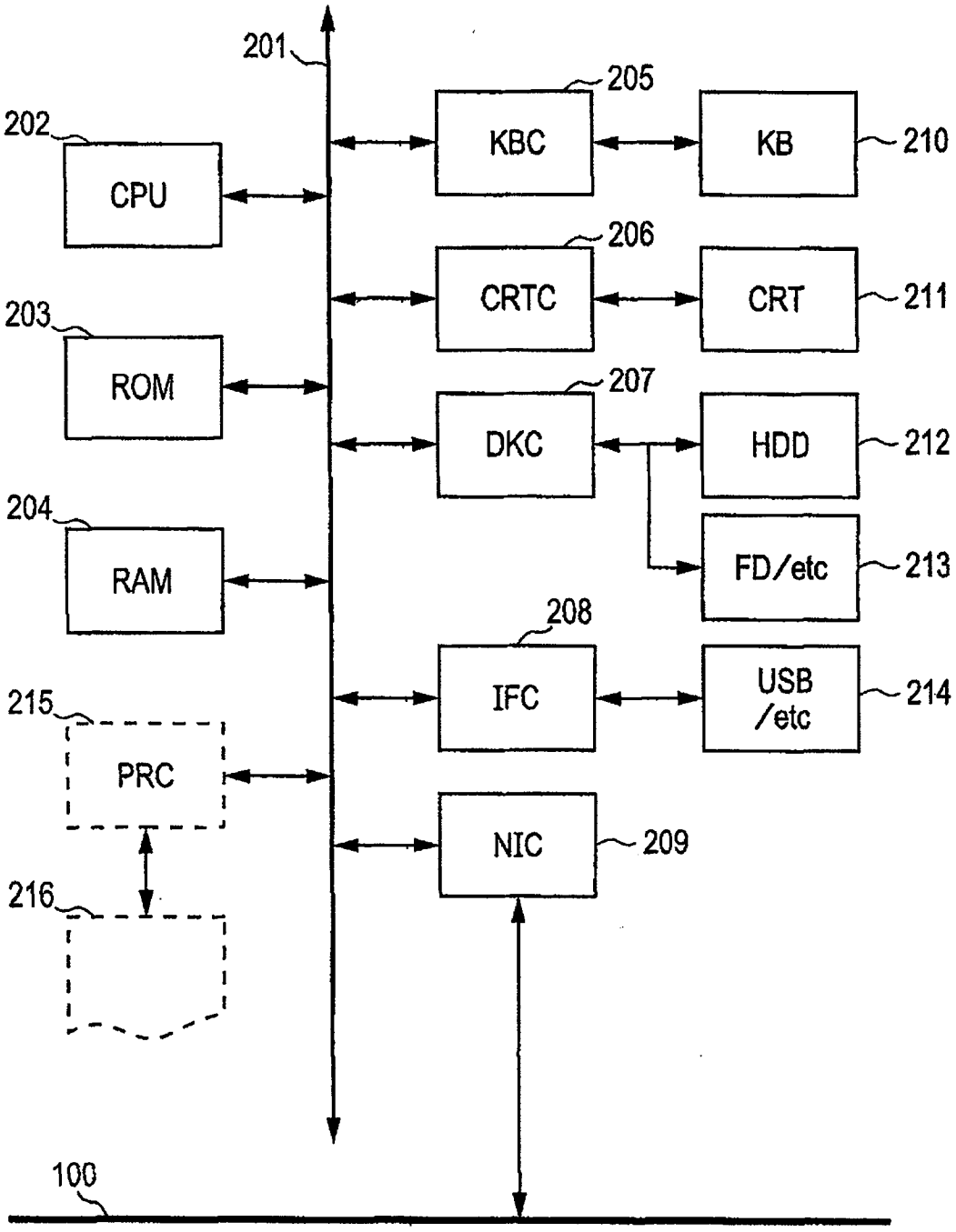

201
202
CPU
203
ROM
204
RAM
215
PRC
216
205
KBC
206
CRTC
207
DKC
208
IFC
NIC
209
KB
210
CRT
211
HDD
212
FD/etc
213
USB
/etc
214
100

图 2

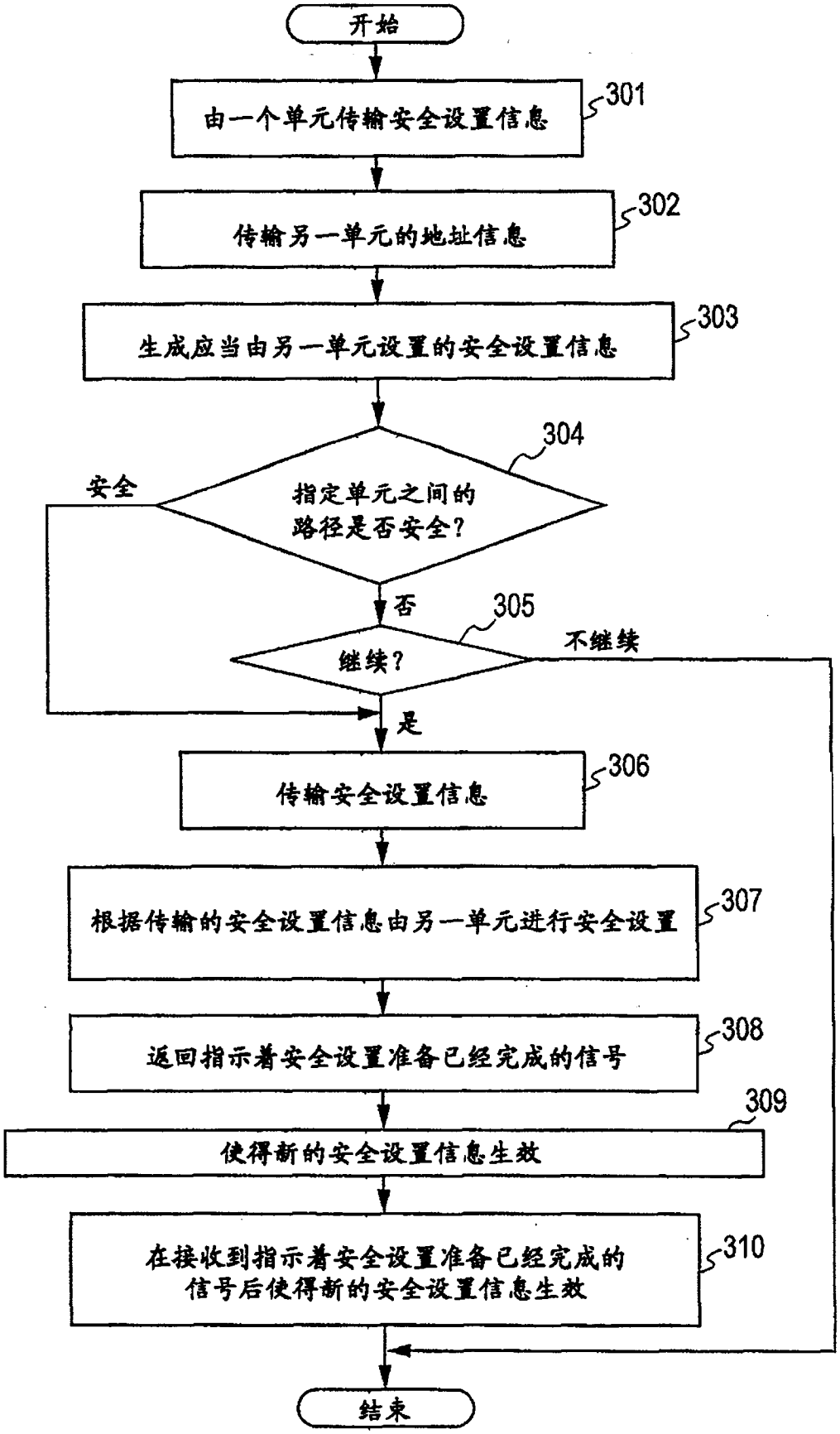

开始
由一个单元传输安全设置信息
301
传输另一单元的地址信息
302
生成应当由另一单元设置的安全设置信息
303
304
指定单元之间的
路径是否安全?
安全
否
305
继续?
不继续
是
传输安全设置信息
306
根据传输的安全设置信息由另一单元进行安全设置
307
返回指示着安全设置准备已经完成的信号
308
309
使得新的安全设置信息生效
在接收到指示着安全设置准备已经完成的
信号后使得新的安全设置信息生效
310
结束

图 3

401	目标地址	数据的目标地址
402	目标地址子网掩码	目标地址生效的位长度
403	源地址	数据的源地址
404	源地址子网掩码	源地址生效的位长度
405	协议号	数据的协议号
406	目标端口号	目标端口号
407	源端口号	源端口号
408	处理方法	数据处理方法 当执行安全处理时使用的处理方法
409	双向传输	可以设置开模式和关模式 当在开模式时，在地址和端口号上的设置自动生效，其中目标和源互换

图 4

501	密钥交换模式	指定模式
502	另一端地址	指定另一端地址
503	预共享专用密钥	一字节字符串
504	建议	指定使用的处理的细节 （可以指定两个或更多的建议）

图 5

鉴别算法	指定鉴别算法的类型
加密算法	指定加密算法的类型
寿命类型	时间或通信量
寿命	以秒或千字节指定（在寿命类型的基础上）

图 6

目标地址	数据的目标地址
目标地址子网掩码	目标地址生效的位长度
源地址	数据的源地址
源地址子网掩码	源地址生效的位长度
协议号	数据的协议号
目标端口号	目标端口号
源端口号	源端口号
处理方法	数据处理方法 执行安全处理时使用的处理方法
双向传输	可以设置开模式和关模式 当在开模式时，在地址和端口号上的设置自动生效，其中目标和源互换
开始时间	2004 年 12 月 28 日 12.23.45
NTP 服务器的地址	192.168.1.102

图 7

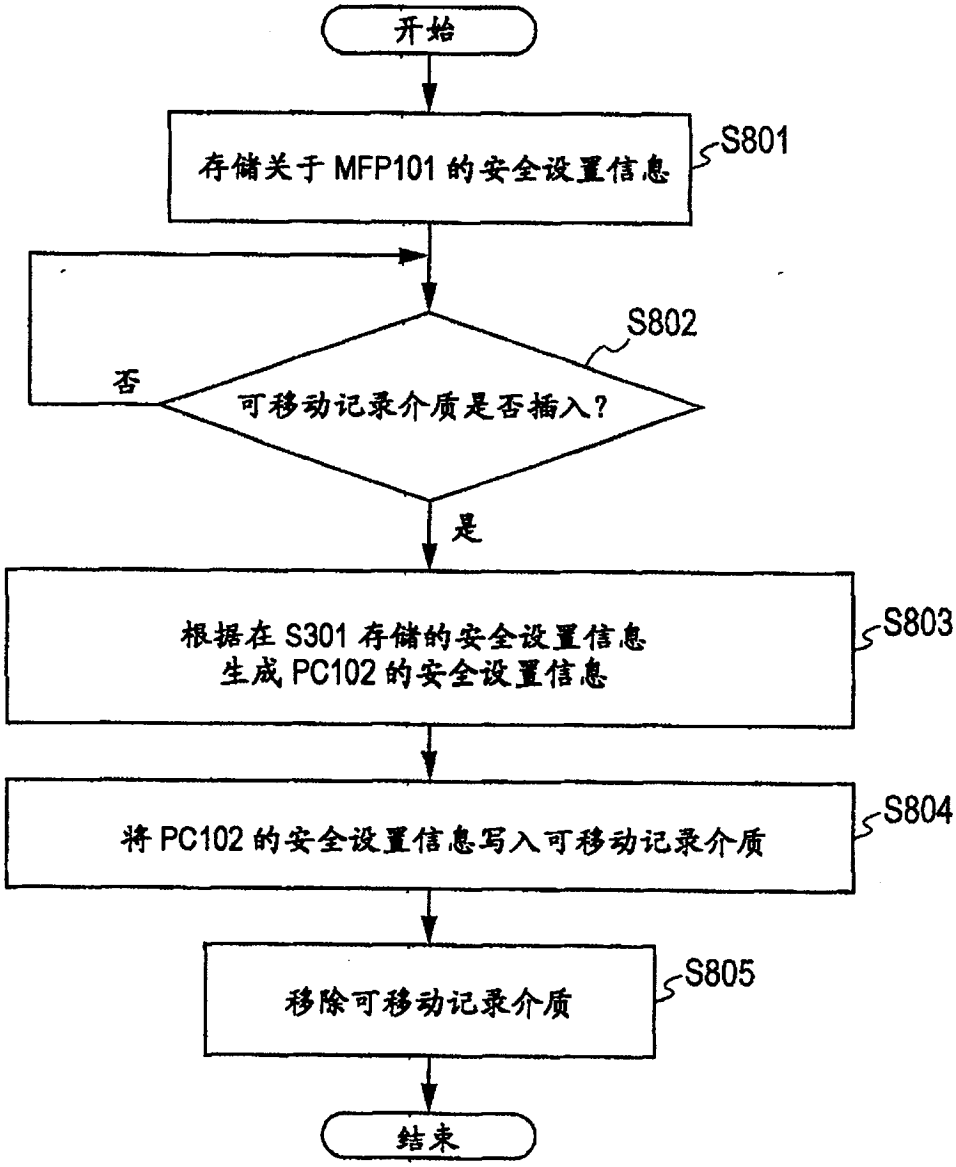

开始
存储关于 MFP101 的安全设置信息
S801
S802
否
可移动记录介质是否插入？
是
根据在 S301 存储的安全设置信息
生成 PC102 的安全设置信息
S803
将 PC102 的安全设置信息写入可移动记录介质
S804
移除可移动记录介质
S805
结束

图 8

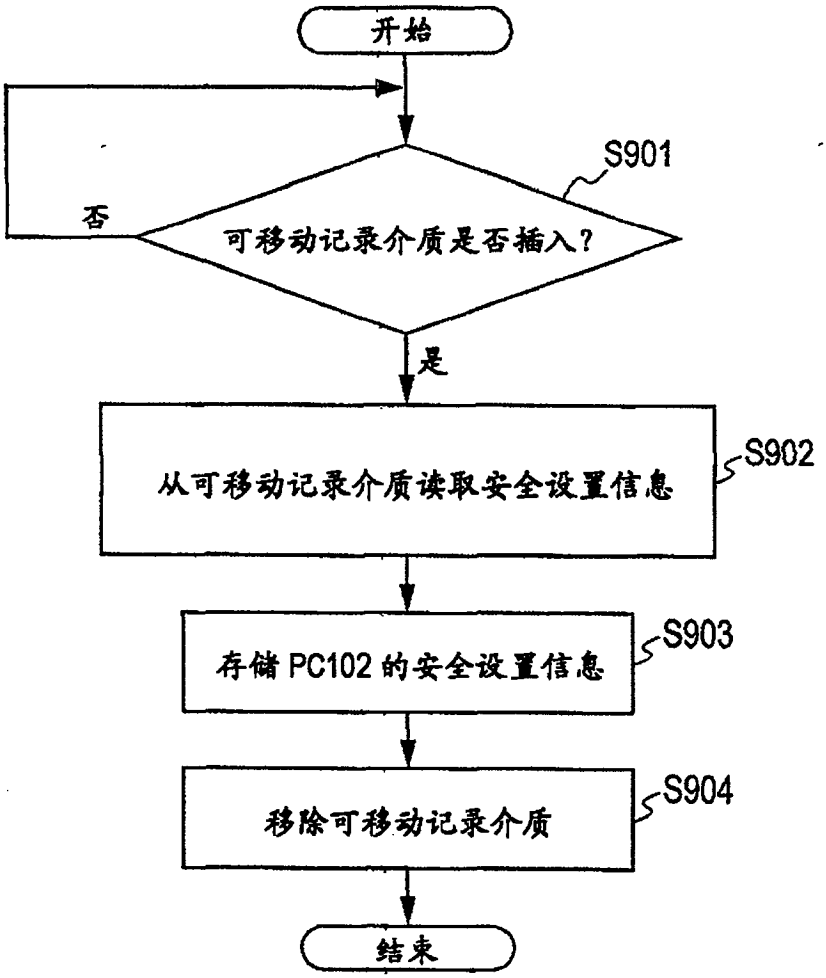

开始
S901
否
可移动记录介质是否插入?
是
从可移动记录介质读取安全设置信息
S902
存储 PC102 的安全设置信息
S903
移除可移动记录介质
S904
结束

图 9

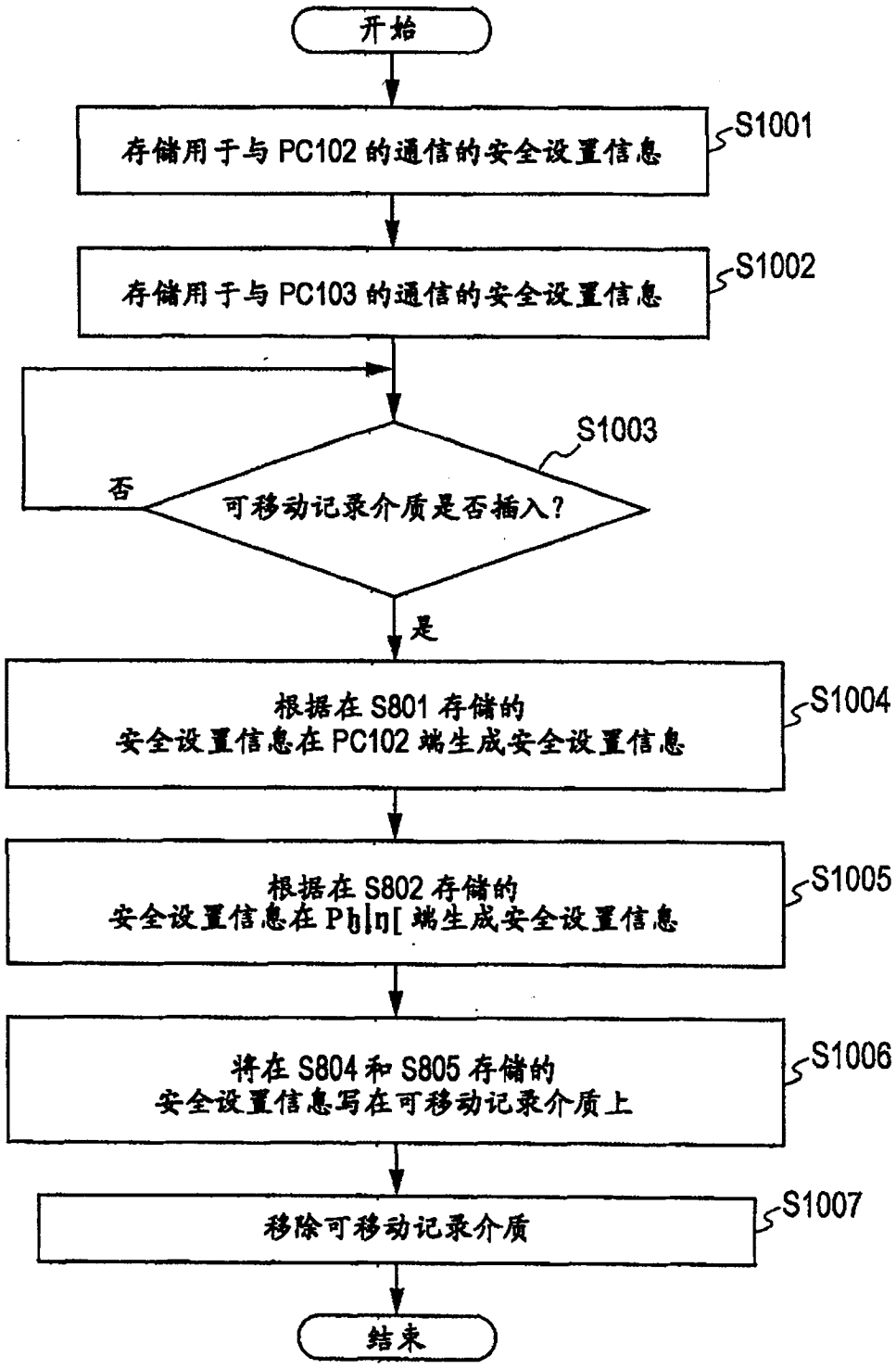

开始
存储用于与 PC102 的通信的安全设置信息
S1001
存储用于与 PC103 的通信的安全设置信息
S1002
S1003
否
可移动记录介质是否插入?
是
根据在 S801 存储的
安全设置信息在 PC102 端生成安全设置信息
S1004
根据在 S802 存储的
安全设置信息在 Pb|n[端生成安全设置信息
S1005
将在 S804 和 S805 存储的
安全设置信息写在可移动记录介质上
S1006
移除可移动记录介质
S1007
结束

图 10

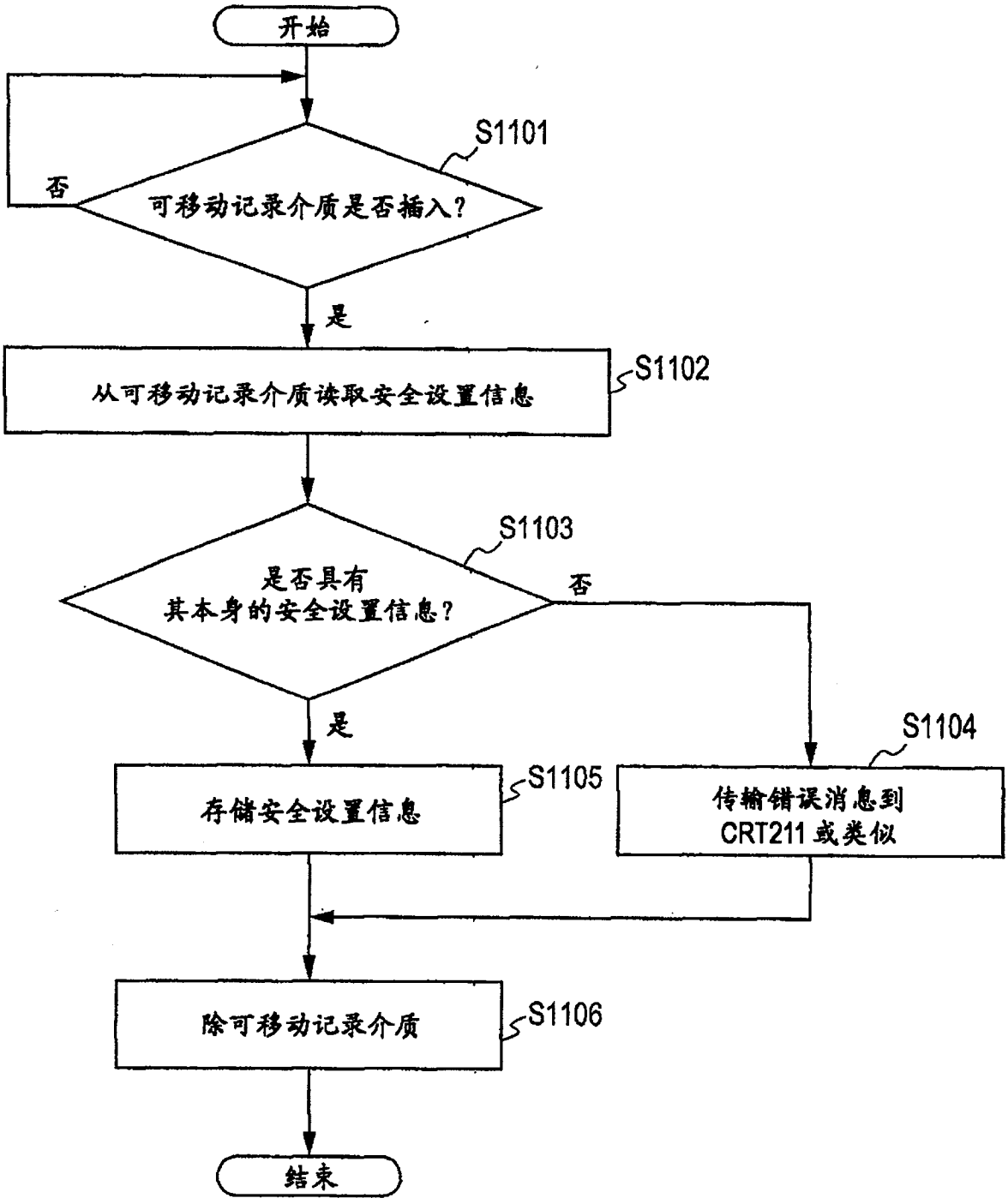

开始
S1101
可移动记录介质是否插入?
否
是
S1102
从可移动记录介质读取安全设置信息
S1103
是否具有
其本身的安全设置信息?
否
是
S1104
传输错误消息到
CRT211 或类似
S1105
存储安全设置信息
S1106
除可移动记录介质
结束

图 11

1201	目标地址	数据的目标地址
1202	目标地址子网掩码	目标地址生效的位长度
1203	源地址	数据的源地址
1204	源地址子网掩码	源地址生效的位长度
1205	协议号	数据的协议号
1206	目标端口号	目标端口号
1207	源端口号	源端口号
1208	处理方法	数据处理方法 当执行安全处理时使用的处理方法
1209	双向传输	可以设置开模式和关模式 当在开模式时，在地址和端口号上的设置自动生效，其中目标和源互换

图 12

1301	密钥交换模式	指定模式
1302	另一端地址	指定另一端地址
1303	预共享专用密钥	一字节字符串
1304	建议	指定使用的处理的细节 (可以指定两个或更多的建议)

图 13