(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 101079946 B
(45)授权公告日 2012.09.05

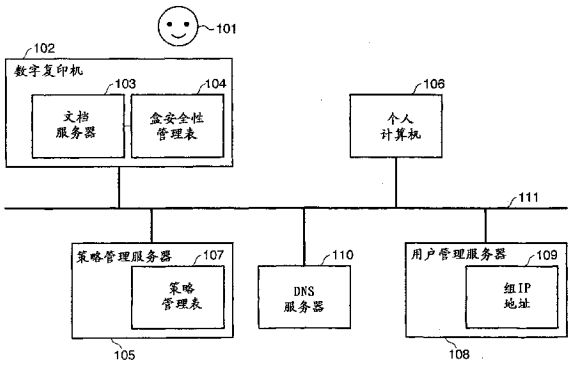
(21)申请号 200710104589.X
(22)申请日 2007.05.25
(30)优先权数据
2006-145883 2006.05.25 JP
(73)专利权人 佳能株式会社
地址 日本东京
(72)发明人 宝木洋一 村山努 深田慎一
高野润一 吉原邦男
(74)专利代理机构 中国国际贸易促进委员会专利商标事务所 11038
代理人 赵科
(51)Int.Cl.
H04N 1/21(2006.01)
H04N 1/00(2006.01)
H04N 1/32(2006.01)
G06F 21/00(2006.01)
(56)对比文件
US 20050273620 A1,2005.12.08, 说明书第0034段-0089段.
审查员 卞喜双
权利要求书 2 页 说明书 8 页 附图 12 页

(54)发明名称

信息处理装置及该装置中的数据管理方法

(57)摘要

在将存储区划分为多个盒并管理存储在每个盒中的数据的信息处理装置中,存储至少包含为每个盒所设置的编辑条件和输出条件的安全性信息。在将存储在盒中的数据传送给外部设备时,基于设置在盒中的安全性信息来设置传输目标数据的安全性信息。当设置在盒中的安全性信息被改变时,为对应于该盒的数据所设置的安全性信息也被改变。



CN 101079946 B

1. 一种信息处理设备，所述信息处理设备具有包括至少一个存储区的存储单元，并且所述信息处理设备管理存储在所述存储区中的数据，所述信息处理设备包括：

安全性存储装置，用于存储为所述存储区设置的第一安全性信息，其中所述第一安全性信息包含代表存储在所述存储区中的数据的各操作的第一权限的信息；

设置装置，用于在向传输目的地传送存储在存储区中的数据之前，基于为所述存储区设置的且存储在所述安全性存储装置中的第一安全性信息，设置要传送的数据的第二安全性信息，使得所述第二安全性信息包含代表要传送的数据的各操作的第二权限的信息，并且要传送的数据的操作的第二权限对应于存储在所述存储区中的数据的该操作的第一权限；以及

更新装置，用于在为所述存储区设置的且存储在所述安全性存储装置中的第一安全性信息被更改的情况下，更新由所述设置装置所设置的所述第二安全性信息，使得在第二安全性信息中反映改变后的第一安全性信息的内容。

2. 根据权利要求 1 所述的信息处理设备，其中所述设置装置将所述第一安全性信息发送到与信息处理设备连接并且能够管理数据的每个操作的第二权限的安全性管理服务器中，以便设置所述第二安全性信息，并且

所述更新装置将改变后的第一安全性信息发送给所述安全性管理服务器，以便更新在所述安全性管理服务器中存储的第二安全性信息。

3. 根据权利要求 1 所述的信息处理设备，还包括更改装置，用于将存储在所述存储区中的数据的所述传输目的地的电子邮件地址更改为 IP 地址。

4. 根据权利要求 1 所述的信息处理设备，其中所述第一和第二安全性信息包含至少一条代表数据改变、擦除、传送、彩色打印的允许 / 禁用和数据有效期的信息。

5. 一种信息处理设备中的数据管理方法，其中所述信息处理设备具有包括至少一个存储区的存储单元，并且所述信息处理设备管理存储在所述存储区中的数据，所述方法包括：

存储步骤，用于在所述存储单元中存储为所述存储区所设置的第一安全性信息，其中所述第一安全性信息包含代表存储在所述存储区中的数据的各操作的第一权限的信息；

设置步骤，用于在向传输目的地传送存储在存储区中的数据之前，基于为所述存储区设置的且存储在所述存储单元中的第一安全性信息，设置要传送的数据的第二安全性信息，使得所述第二安全性信息包含代表要传送的数据的各操作的第二权限的信息，并且要传送的数据的操作的第二权限对应于存储在所述存储区中的数据的该操作的第一权限；和

更新步骤，用于在为所述存储区设置的且在所述存储步骤中存储的第一安全性信息被更改的情况下，更新在所述设置步骤中所设置的所述第二安全性信息，使得在第二安全性信息中反映改变后的第一安全性信息的内容。

6. 根据权利要求 5 所述的数据管理方法，其中在所述设置步骤中，所述第一安全性信息发送到与信息处理设备连接并且能够管理数据的每个操作的第二权限的安全性管理服务器中，以便设置所述第二安全性信息，并且

在所述更新步骤中，将改变后的第一安全性信息发送给所述安全性管理服务器，以便更新在所述安全性管理服务器中存储的第二安全性信息。

7. 根据权利要求 5 所述的数据管理方法，还包括将存储在存储区中的数据的所述传输

目的地的电子邮件地址更改为 IP 地址的步骤。

8. 根据权利要求 5 所述的数据管理方法，其中所述第一和第二安全性信息包含至少一条代表数据改变、擦除、传送、彩色打印的允许 / 禁用和数据有效期的信息。

信息处理装置及该装置中的数据管理方法

技术领域

[0001] 本发明涉及一种用于管理存储在多个存储区中的每个存储区中的数据的安全策略的信息处理装置、以及该装置中的数据管理方法。

背景技术

[0002] 具有复印机、扫描仪和传真设备功能的数字多功能外设具有例如由硬盘形成的大容量存储单元来存储文档文件。这种存储单元具有多个被称为“盒”的存储区。为每个盒设置安全性（关于每个用户的存取权限和例如读、写、编辑和打印的操作权限的设置），由此保证其中文档的安全性（日本专利公开文本No.2005-346366)。该安全性设置被称为安全策略。

[0003] 作为另一种用于管理对文档文件的存取权限的方法，诸如AdobePolicy Server的系统将安全策略管理集中到服务器的操作开始了。

[0004] 但是，在上述现有技术中，服务器必须管理大量文档文件的所有安全策略。每次发出文档文件操作请求时都存取服务器，从而增加了服务器的负担。如果系统只在特定组的封闭环境中运行，则可能需要容易地基于该组的操作策略来管理安全策略。为了从特定组向该组外的设备发送数据，则安全性应当在诸如Adobe Policy Server这样的能管理每个文件的安全策略的服务器的管理下被可靠地管理。在这种情况下，还产生其他要求，以在Adobe Policy Server的管理下，根据该特定组中操作策略的变化来改变被发送到外部设备的每个文件的安全策略。

发明内容

[0005] 本发明的目的是解决现有技术中的这些问题。

[0006] 作为本发明的特性特征，可以根据特定安全策略管理特定存储区中的数据，从而容易和恰当地基于一致的安全策略管理存储区中的数据，而无需使用外部安全策略服务器。

[0007] 作为本发明的另一个特性特征，在从每个存储区向外部设备发送数据时，可以为每个要发送的数据管理和设置安全性。

[0008] 按照本发明的一个方面，提供了一种信息处理装置，其具有包括至少一个存储区的存储单元，并管理存储在每个存储区中的数据，包括：

[0009] 安全性存储装置，用于存储为至少一个存储区所设置的、并包含代表对于存储在该存储区中的数据的操作权限的信息的第一安全性信息；

[0010] 设置装置，用于将存储在该存储区中的数据传送到外部设备时，基于存储在安全性存储装置中的、为该存储区所设置的第一安全性信息，设置该数据的安全性信息；

[0011] 更新装置，用于基于为该存储区所设置的第一安全性信息改变，更新设置装置所设置的第二安全性信息。

[0012] 按照本发明的一个方面，提供了一种信息处理装置中的数据管理方法，该信息处

理装置具有包括至少一个存储区的存储单元，并管理存储在每个存储区中的数据，该方法包括：

[0013] 存储步骤，用于在存储器中存储为至少一个存储区设置的、并包含代表对于存储在该存储区中的数据的操作权限的信息的第一安全性信息；

[0014] 设置步骤，用于在向外部设备传送存储在该存储区中的数据时，基于存储在存储器中的、为该存储区所设置的第一安全性信息，设置该数据的第二安全性信息；

[0015] 更新步骤，用于基于为该存储区所设置的第一安全性信息改变，更新在设置步骤中所设置的第二安全性信息。

[0016] 作为本发明的另一特性特征，当被管理的安全策略变化时，已经被传送给外部设备的数据的安全策略也可以适当更改。

[0017] 用于解决该问题的手段没有列出本发明的所有特征。本发明的其它权利要求和特性特征的组合也可以构成本发明。

[0018] 通过下面参照附图对示例性实施例的描述，本发明的其它特征变得明显。

附图说明

[0019] 结合在说明书中并构成说明书一部分的附图示出了本发明的实施例，其与文字描述一起用于解释本发明的原理。

[0020] 图 1 是示出按照本发明一个实施例的包括服务器和数字复印机的系统的示意布置的框图；

[0021] 图 2 是用于解释按照该实施例的数字复印机的布置的框图；

[0022] 图 3 示出根据该实施例的在选择盒将图像数据存储在数字复印机中时，显示在控制台单元上的盒选择屏幕的例子；

[0023] 图 4 示出按照该实施例的盒安全性管理表的例子；

[0024] 图 5 示出按照该实施例的用户管理服务器中的组 IP 地址表的布置例子；

[0025] 图 6 示出的视图显示了按照该实施例的数字复印机的控制台单元的显示单元上所显示的文件传送指令屏幕的例子；

[0026] 图 7 示出的视图显示了按照该实施例的策略管理表的例子；

[0027] 图 8 示出的视图显示了按照该实施例的数字复印机的控制台单元的显示单元上所显示的鉴权屏幕的例子；

[0028] 图 9 示出用于解释直到该实施例的数字复印机的扫描器所读取的原始数据被存储到文档服务器的盒中之前的一系列操作的序列图；

[0029] 图 10 是用于解释向外部设备发送按照本发明的文档服务器中文件的一系列操作的序列图；

[0030] 图 11 示出解释存储从该实施例的数字复印机登记到策略管理服务器的内容的登记日志表的图；

[0031] 图 12 是用于解释改变按照该实施例的数字复印机的盒安全性管理信息的过程序列的序列图。

具体实施方式

[0032] 下面参照附图详细描述本发明的实施例。应当注意，下面的实施例不是要限制在权利要求中所提出的本发明，而且不是这些实施例中所描述的特征的所有组合都必须作为实现本发明目的的手段。

[0033] 图 1 是示出按照本发明一个实施例的作为信息处理装置的、包括服务器和数字复印机的系统的示意布置的框图。数字复印机是还用作扫描仪、打印机和传真设备的多功能外设。

[0034] 参照图 1，文档服务器 103 是将数据存储在数字复印机 102 的盒中的服务器系统。“盒”是形成在复印机 102 的硬盘 (HDD) 中的数据存储区，下面将对其详细描述。文档服务器 103 保持盒安全性管理表 104（图 4）。盒安全性管理表 104 存储关于每个盒中所存储的文件数据的安全性的信息。根据盒安全性管理表 104 的内容，一致地处理存储在每个盒中的所有数据。文档服务器 103 和盒安全性管理表 104 可以被集成在数字复印机 102 中，也可以被设置在数字复印机 102 之外。

[0035] 图 4 示出按照该实施例的盒安全性管理表 104 的例子。

[0036] 盒 ID（标识符）401 指定数字复印机 102 的盒。字段 402 存储表明盒中数据是否可以传送的数据。字段 403 存储表明盒中数据是否可以更改的数据。字段 404 存储表明盒中数据是否可擦除的数据。字段 405 存储表明盒中数据是否可彩色打印的数据。字段 406 存储表明盒中数据是否可以单色打印的数据。在字段 402 至 406 中，“OK”表示“使能”，否则设置“NG”。字段 407 存储每个盒中数据的存储时限。

[0037] 按照盒安全性管理表 104 的内容管理存储在每个盒中的数据的安全性。在图 4 的例子中，ID 为“001”的盒中的数据具有“无限制”的存储持续时间。该数据可以发送、更改和单色打印，但是禁止擦除和彩色打印该数据。

[0038] 用户管理服务器 108 保持组 IP 地址 109（图 5），其中每个组 IP 地址定义作为盒安全性管理表 104 的操作目标的、包括在组中的设备（计算机或数字复印机）。与组 IP 地址对应地保持用户名和密码。用户名和密码用于在图 8 所示的数字复印机 102 的控制台单元 213（图 2）上的用户鉴权屏幕中对用户鉴权。

[0039] 图 8 示出的视图显示了按照该实施例的数字复印机 102 的控制台单元 213（下面将参照图 2 描述）的显示单元上所显示的鉴权屏幕的例子。

[0040] 当用户 101 输入预定用户名和密码并激活“OK”按钮时，他 / 她能够操作数字复印机 102。“取消”按钮用于取消用户鉴权过程。

[0041] 策略管理服务器 105 保持策略管理表 107，以管理每个盒中每个数据的安全性。图 7 示出策略管理表 107 的例子。在向除了包括在公共组中的设备以外的个人计算机 106 发送文件时，关于安全性的文件使用限制根据盒安全性管理表 104 的内容被设置，并被存储在策略管理表 107 中。

[0042] 图 7 示出的视图显示了按照该实施例的策略管理表 107 的例子。

[0043] 文件 ID701 指定电子数据文件。字段 702 至 706 分别对应于图 4 中所示的盒安全性管理表 104 的上述字段 402 至 406。也就是说，字段 702 至 706 具有与存储该文件的盒的安全性管理表 104 的字段 402 至 406 中相同的值。IP 地址 707 指示定义作为存储该文件的盒的操作目标的、包括在组中的设备的组 IP 地址。盒 ID708 是存储该文件的盒的标识信息 (ID)。字段 709 存储表明文件是否处于有效存储持续时间中的数据。

[0044] 在图 7 所示的例子中，设置盒 ID 为“002”的盒中文件 ID 为“012...”的文件的安全性信息。在图 7 中，字段 702 至 706 的值与图 4 中相应字段 402 至 406（盒 ID “002”那一行）的值相同。

[0045] 在将文件从数字复印机 102 的盒发送到另一设备时，DNS 服务器 110 基于发送目的地的电子邮件地址或主机名称，决定相应的 IP 地址，并将所决定的 IP 地址通知给数字复印机 102。代替 DNS 服务器 110，SMTP（简单邮件传送协议）服务器（未示出）可以根据电子邮件地址决定设备的 IP 地址。

[0046] 图 6 示出的视图显示了按照该实施例的数字复印机 102 的控制台单元 213 的显示单元上所显示的文件传送指令屏幕的例子。

[0047] 参照图 6，附图标记 601 表示盒 ID 输入字段。传输目标文件在字段 602 中指定。字段 602 显示输入字段 601 中所指定的盒（在本例子中盒 ID 是 001）中所存储的文件的列表。用户 101 利用例如光标（未示出）选择传输目标文件。所选择的文件名称可以通过高亮显示来识别。用户在字段 603 中输入电子邮件地址，以指定传输目的地。DNS 服务器 110 基于在字段 603 中所输入的电子邮件地址或主机名称来决定相应的 IP 地址。

[0048] 数字复印机 102、策略管理服务器 105、个人计算机 106、用户管理服务器 108 和 DNS 服务器 110 连接到例如由**以太网®**形成的 LAN（局域网）111。

[0049] 图 2 是用于解释按照本实施例的数字复印机 102 的布置的框图。

[0050] 参照图 2，扫描仪 201 光学地读取原件，并将其转换为电信号以生成原件图像数据。扫描仪 201 生成每个像素具有 8 位亮度数据的 RGB（红、绿、蓝）数字数据。在该实施例中，扫描仪 201 在主扫描方向和副扫描方向上的读取分辨率都是 400dpi。图像处理单元 202 对从扫描仪 201 所接收的图像数据执行诸如输入掩蔽、从 RGB 数据向 CMYK（青、品红、黄、黑）数据的日志转换以及输出掩蔽的操作。打印机 203 接收被图像处理单元 202 处理的帧连续 CMYK 数据，并例如通过电子照相法打印彩色图像。

[0051] 帧缓冲器 204 由存储容量例如为 139MB 的同步 DRAM 形成。帧缓冲器 204 存储从扫描仪 201 所接收的光栅图像数据，或在 CPU 206 控制下从网络 111 所接收的图像数据。CPU 206 通过执行存储在 ROM 208 中或从 HDD 211 加载到 RAM 209 的程序来控制数字复印机 102。连接到 CPU 总线 205 的 I/O 端 ct 212 将来自 CPU 206 的控制信号输出到扫描仪 201 或打印机 203 以控制其，或者例如从传感器接收信号。ROM 208 存储在引导系统时所执行的引导程序。RAM209 是例如 117MB 的同步 DRAM。RAM 209 和帧缓冲器 204 可以形成 256MB 的同步 DRAM 存储模块，并连接到 CPU 总线 205。要由 CPU 206 执行的程序被安装在 HDD 211 中，在复印机加电时根据 ROM 208 中的引导程序被加载到 RAM 209，并在 CPU 206 的控制下被执行。

[0052] SCSI 控制器 210 连接到 CPU 总线 205。HDD 211 是连接到 SCSI 控制器 210 的硬盘驱动器。网络 I/F 207 连接到 CPU 总线 205，并连接到外部 10BaseT 或 100BaseT 以太网®，以交换数据。图 1 中所示个人计算机 106 和 DNS 服务器 110 经由网络 I/F 207 连接到数字复印机。控制台单元 213 包括显示单元，诸如 LCD、触摸屏和各种操作按钮。

[0053] 数字复印机 102 的 HDD 211 具有多个被称为“盒”的数据存储区。在一些情况下，这多个存储区整体被统称为盒。可替换地，这多个存储区中某个存储区被称为盒。文档服

务器 103 管理所有盒。盒的多个存储区中每一个都可以用盒 ID 来指定。图 4 中所示的盒安全性管理表 104 管理每个盒的操作权限和每个盒中数据的存储持续时间。

[0054] 存储在盒中的数据包括数字复印机 102 的扫描仪 201 所读取的原件的图像数据，以及通过将从个人计算机 106 所接收的打印数据光栅化而获得的图像数据。盒还可以存储由个人计算机所创建的文档数据。

[0055] 图 9 示出的序列图解释直到该实施例的数字复印机 102 的扫描仪 201 所读取的原始数据被存储在文档服务器的盒中之前的一系列操作。

[0056] 在 901 中，用户 101 从控制台单元 213 输入用户名和密码到显示在控制台单元 213 的显示单元上的用户鉴权屏幕（图 8）。数字复印机 102 向用户管理服务器 108 查询输入用户鉴权屏幕的用户名和密码，以检查所输入的用户名和密码是否可信。如果可信，则数字复印机 102 从用户管理服务器 108 接收肯定确认，从而用户 101 可以登录到数字复印机 102。如果从用户管理服务器 108 接收到否定确认，则数字复印机 102 不从用户 101 接收登录请求。在 902 中，选择用于存储扫描仪 201 所读取的图像数据的盒。

[0057] 图 3 示出的视图显示了在选择用于存储图像数据的盒时，显示在控制台单元 213 的显示单元上的盒选择屏幕的例子。

[0058] 参照图 3，显示文档服务器 103 的盒列表。用户 101 利用例如光标（未示出）从列表中选择用于存储图像数据的盒。文件名输入字段 300 用于输入要被存储在所选择的盒中的图像数据的文件名。

[0059] 在 902 中，在显示于控制台单元 213 上的盒选择屏幕中选择用于存储图像数据的盒。要被存储在盒中的图像数据的文件名被输入到输入字段 300（图 3）。在 904 中，文档服务器 103 存储所选择的盒以及要被存储在其中的文件名。

[0060] 在 903 中，数字复印机 102 向文档服务器 103 发送扫描仪 201 所读取的原件的数据文件。在 905 中，文档服务器 103 将从数字复印机 102 所发送的图像数据存储在对应于在 904 中所存储的盒名称的 HDD 211 的存储区（盒）中。

[0061] 图 10 是用于解释向外部设备（个人计算机 106）发送按照本实施例的数字复印机 102 的文档服务器 103 中的数据的一系列操作的序列图。

[0062] 在 1001 中，用户 101 通过操作控制台单元 213 的鉴权屏幕（图 8）而登录到数字复印机 102，如图 9 中 901 中那样。在 1002 中，用户 101 选择盒 ID，并通过在控制台单元 213 的文件选择屏幕（图 6）上进行操作而指定传输目标文件。用户 101 还向输入字段 603 输入诸如电子邮件地址或主机名称的信息，以指定传输目的地，从而决定传输目的地。诸如电子邮件地址的输入信息被发送到 DNS 服务器 110。在 1009 中，DNS 服务器 110 返回对应于诸如电子邮件地址的信息的 IP 地址。这使得数字复印机 102 可以指定文件的传输目的地的 IP 地址。

[0063] 在指定 IP 地址时，在 1003 中，数字复印机 102 向用户管理服务器 108 询问数据传送目的地的 IP 地址是否是特定组的 IP 地址。用户管理服务器 108 通过查询组 IP 地址 109 来确定该 IP 地址是否属于特定组。如果传送目的地的设备不属于该特定组，则执行 1005 和 1006 中的过程。如果传送目的地的设备被包括在该特定组中，则过程跳至 1007，以获得要传送的数据。在 1008 中，数字复印机 102 根据 IP 地址将数据传送到个人计算机 106。包括在该特定组中的设备的电子邮件地址可以被事先登记在发送方的数字复印机 102 中。在

这种情况下，数字复印机 102 可以确定传输目的地的电子邮件地址是否被包括在该组中，而无需询问用户管理服务器 108。

[0064] 在图 10 的 1005 中，数字复印机 102 向策略管理服务器 105 发送盒安全性管理表 104（图 4）中对应于存储被传送文件的盒的信息。通过该过程，设置策略管理服务器 105 所管理的策略管理表 107（图 7）的项“发送”、“改变”、“删除”、“彩色打印”、“单色打印”、“IP 地址”、“盒 ID”、“有效 / 无效”的值 (1010)。也就是说，策略管理服务器 105 决定文件的文件 ID，并在对应于该文件的策略管理表 107（图 7）上反映对应于该盒的盒安全性管理表 104（图 4）的内容，其中这些内容从数字复印机 102 被发送。

[0065] 图 11 示出解释存储从该实施例的数字复印机 102 登记到策略管理服务器 105 的内容的登记日志表的图。文档服务器 103 管理登记日志表。

[0066] 登记日志表存储对应于所指定的盒中的数据的文件名、指定文件的文件 ID、指定存储文件的盒的盒 ID 以及作为文件信息的传输目的地的策略管理服务器 105 的 IP 地址。在图 11 的例子中，文件 ID 为“012...”的文件具有文件名“Report_20051224”，并被存储在盒 ID 为“002”的盒中。进行设置，以将该文件发送到策略管理服务器 105 的 IP 地址“111.222.33.444”。

[0067] 在图 10 的 1006 中，数字复印机 102 向文档服务器 103 传送从策略管理服务器 105 所发送的文件 ID。在 1011 中，文档服务器 103 更新图 11 所示的登记日志表，并向数字复印机 102 发送所指定文件的安全信息。

[0068] 在 1007 中，数字复印机 102 从文档服务器 103 接收上述在 1002 中所指定的文件。在 1008 中，数字复印机 102 基于在 1002 中所获得的 IP 地址，将文件传送到目的地的个人计算机 106。

[0069] 在 1005、1010、1006 和 1011 的过程之后在 1007 中所传送的文件具有由策略管理服务器 105 所产生的文件 ID 作为属性信息，并且所产生的文件 ID 被发送到数字复印机 102。策略管理服务器 105 的 IP 地址还被添加作为所传送文件的属性信息。向文件添加由策略管理服务器 105 所产生的文件 ID 以及策略管理服务器 105 的 IP 地址信息作为属性信息就被称为向文件“添加策略”。

[0070] 在接收到具有被添加策略的文件时，个人计算机 106 执行下面的过程，以对文件执行操作（例如在应用中打开文件的操作）。个人计算机 106 通过查阅具有被添加策略的文件的属性信息，获取文件 ID 和策略管理服务器 105 的 IP 地址。文件 ID 和个人计算机 106 的 IP 地址被发送到该 IP 地址。策略管理服务器 105 通过基于所接收的文件 ID 查询图 7 所示的策略管理表 107，确认个人计算机 106 的 IP 地址被包括在图 7 的 IP 地址 707 中。策略管理服务器 105 向个人计算机 106 返回为该文件 ID 所定义的各种操作权限（例如发送、修改和擦除）的允许 / 禁止信息。如果个人计算机 106 的 IP 地址不被包括在图 7 中对应于该文件 ID 的 IP 地址 707 的字段中，则策略管理服务器 105 通知个人计算机 106 其对该文件没有操作权限。

[0071] 在从策略管理服务器 105 接收到关于操作权限的信息时，个人计算机 106 根据所接收的操作权限信息控制对该文件的各种操作的允许 / 禁止。

[0072] 通过上述方式，即使在文档服务器 103 中管理其存取权限的文件被发送给外部设备，也可以利用策略管理服务器 105 执行如在文档服务器 103 中的存取权限管理。

[0073] 图 12 是用于解释改变按照该实施例的数字复印机 102 的盒安全性管理信息的过程序列的序列图。

[0074] 在 1201 中，用户 101 通过操作控制台单元 213 的鉴权屏幕（图 8）来登录到数字复印机 102，如图 9 的 901 中那样。1202 的操作只在用户 101 具有系统管理员权限时才可能。在 1202 中，数字复印机 102 从文档服务器 103 获取盒安全性管理表 104（图 4）的信息。在 1203 中，数字复印机 102 的用户指示更改盒安全性管理信息。例如对于图 4 中的盒 ID “002”，“彩色打印”和“单色打印”都被设置为“允许”。假定发出指令以将这些设置更改为“禁止”。

[0075] 在 1204 中，文档服务器 103 根据作为更改指令的目标的盒安全性管理信息，更改盒安全性管理表 104 中的数据。在 1205 中，搜索保持在文档服务器 103 中的到策略管理服务器 105 的登记日志表（图 11），以指定对应于具有在 1203 中更改的盒安全性管理信息的盒的被登记文件 ID。

[0076] 在 1206 中，文档服务器 103 向策略管理服务器 105 通知在 1205 中所指定的文件 ID 和更改后的盒安全性管理信息。在 1207 中，策略管理服务器 105 根据从文档服务器 103 所接收的内容，更改其中的策略管理表 107（图 7）。在这个例子中，根据更改后的盒安全性管理信息，策略管理表 107 中的“彩色打印”和“单色打印”都被设置为“禁止”。

[0077] 通过该过程，文档服务器 103 中盒安全性管理表 104 的更改被反映到策略管理服务器 105 上。因此，甚至可以基于与盒安全性管理表 104 中更改的安全性管理信息相同的内容，管理对从文档服务器 103 发送到外部设备的文件的存取权限。

[0078] 如上所述，按照该实施例，可以根据特定安全策略来管理数字复印机的特定存储区（盒）中的数据，从而容易和恰当地基于一致安全策略管理盒中的数据。

[0079] 在从数字复印机的盒向外部设备发送文件数据时，可以为每个要发送的数据文件管理和设置安全性。这使得可以恰当地管理从数字复印机发送给外部设备的文件数据的安全性。

[0080] 在更改数字复印机的特定存储区（盒）的安全策略时，还可以更改关于策略管理服务器的对应信息。这使得可以将数字复印机中所管理的安全策略的改变甚至反映到已经被传送给外部设备的文件数据的安全策略的操作上。

[0081] （其它实施例）

[0082] 上面已经详细地描述了本发明的实施例。本发明可应用于包括多个设备的系统或包括单个设备的装置。

[0083] 本发明还通过直接或从远程端向该系统或装置提供实施上述实施例的功能的软件程序，并且使该系统或装置的计算机读出并执行所提供的程序来实现。在这种情况下，只有程序的功能是必需的，而形式不必总是程序。

[0084] 因此，安装在计算机中以实施本发明的功能性处理的程序代码本身也实现了本发明。也就是说，本发明的权利要求也包括用于执行本发明的功能性处理的计算机程序本身。在这种情况下，程序可以采取任何形式，诸如目标代码、由解释器执行的程序或被提供给 OS 的脚本数据，只要可以获得程序功能。

[0085] 提供程序的记录介质的例子是 **floppy®**盘、硬盘、光盘、磁光盘、MO、CD-ROM、

CD-R、CD-RW、磁带、非易失性存储卡、ROM 和 DVD(DVD-ROM 和 DVD-R)。

[0086] 为了提供程序，客户计算机可以经由浏览器连接到互联网上的主页，以从该主页下载程序到诸如硬盘的记录介质。可以下载本发明本身的计算机程序或包含自动安装功能的压缩文件。包含在本发明的程序中的程序代码可以被分为多个文件，从而用户可以从不同主页下载这些文件。也就是说，使多个用户下载用于实施本发明功能性处理的程序文件的 WWW 服务器也被包含在本发明的权利要求中。

[0087] 本发明的程序可以被加密，被存储在诸如 CD-ROM 的存储介质中，并被分发给用户。任何满足预定条件的用户都可以下载密钥信息，以解密经由互联网从主页所下载的程序。用户可以利用密钥信息将加密的程序以可执行的形式安装到计算机中。

[0088] 甚至在不使计算机执行所读出的程序的情况下，也可以实施上述实施例的功能。例如，当例如运行在计算机上的 OS 基于程序的指令部分或全部执行实际处理时，也实施上述实施例的功能。

[0089] 从记录介质所读出的程序可以被写入被插入计算机的功能扩展板或连接到计算机的功能扩展单元的存储器中。然后，功能扩展板或功能扩展单元的 CPU 基于程序指令部分或完全执行实际处理，从而实施上述实施例的功能。

[0090] 尽管已经参照示例性实施例描述了本发明，但是应当理解，本发明不限于所公开的示例性实施例。以下权利要求的范围应当与最宽泛的解释一致，从而涵盖所有这样的修改和等价结构及功能。

图 1

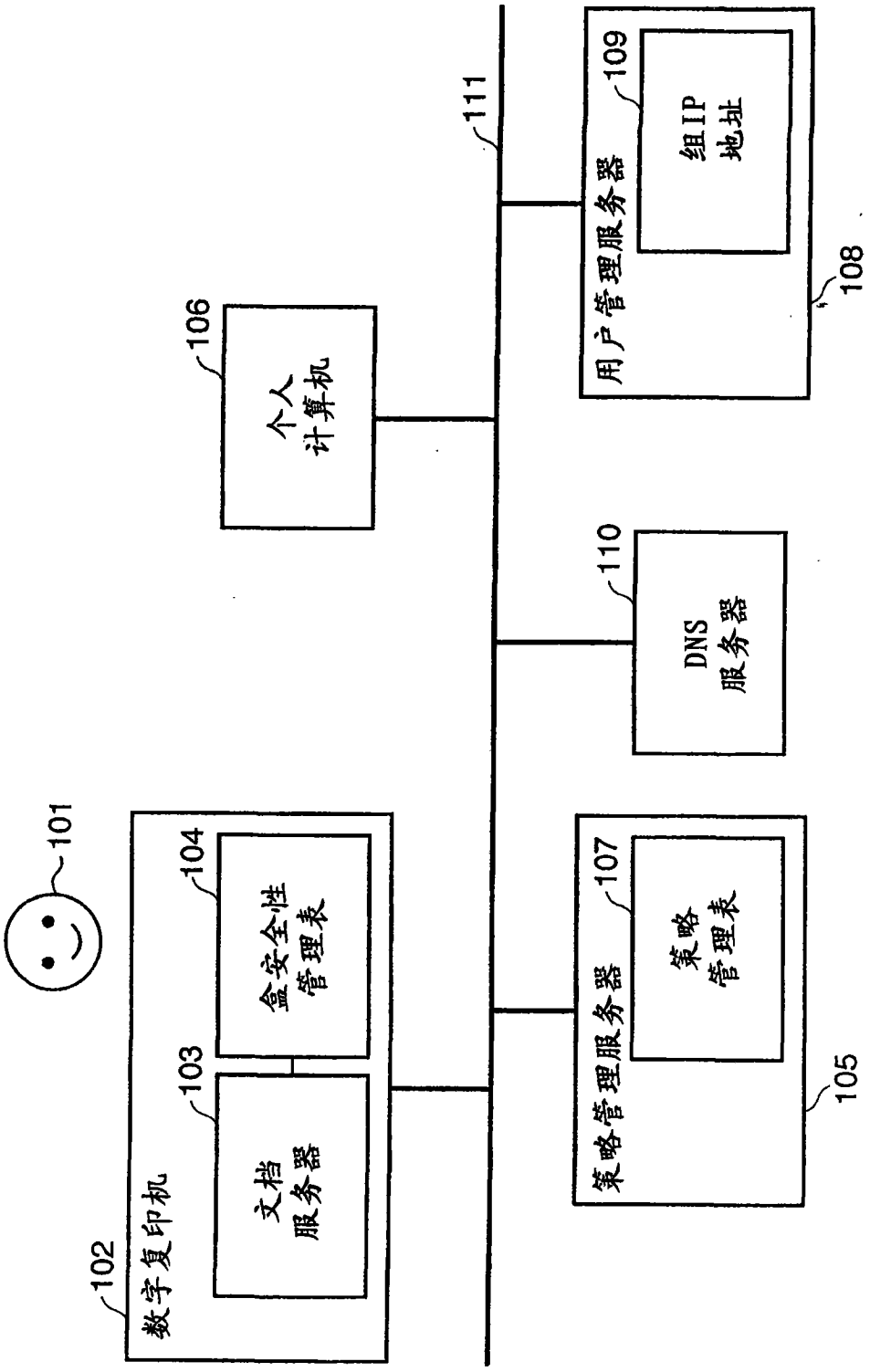
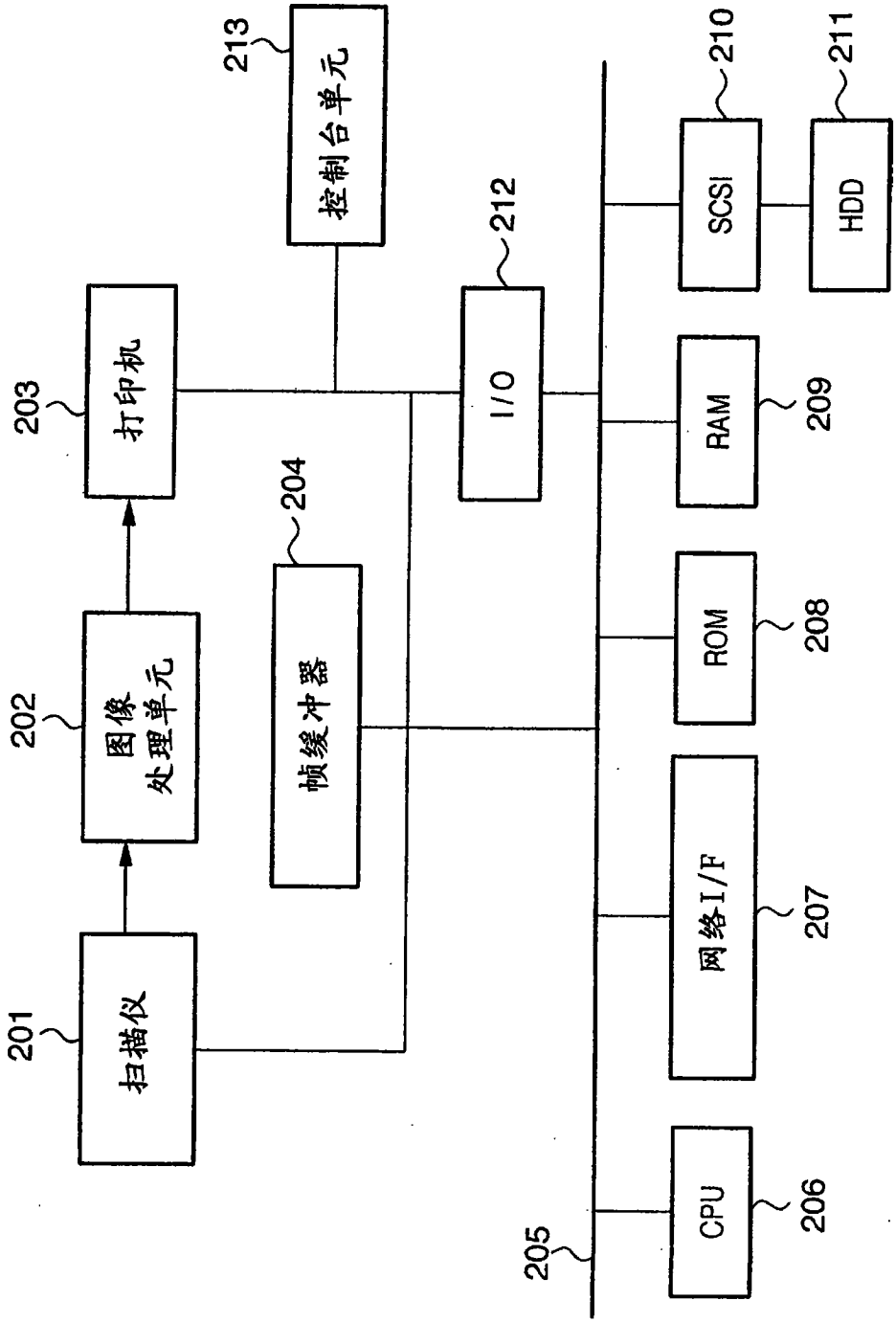

101
数字复印机
102
文档服务器
103
盒安全性管理表
104
策略管理服务器
105
策略管理表
107
DNS服务器
110
个人计算机
106
用户管理服务器
108
组IP地址
109
111

图2


213
控制台单元
210
211
SCSI
HDD
212
I/O
203
打印机
RAM
209
204
帧缓冲器
ROM
208
202
图像
处理单元
网络I/F
207
201
扫描仪
CPU
206
205

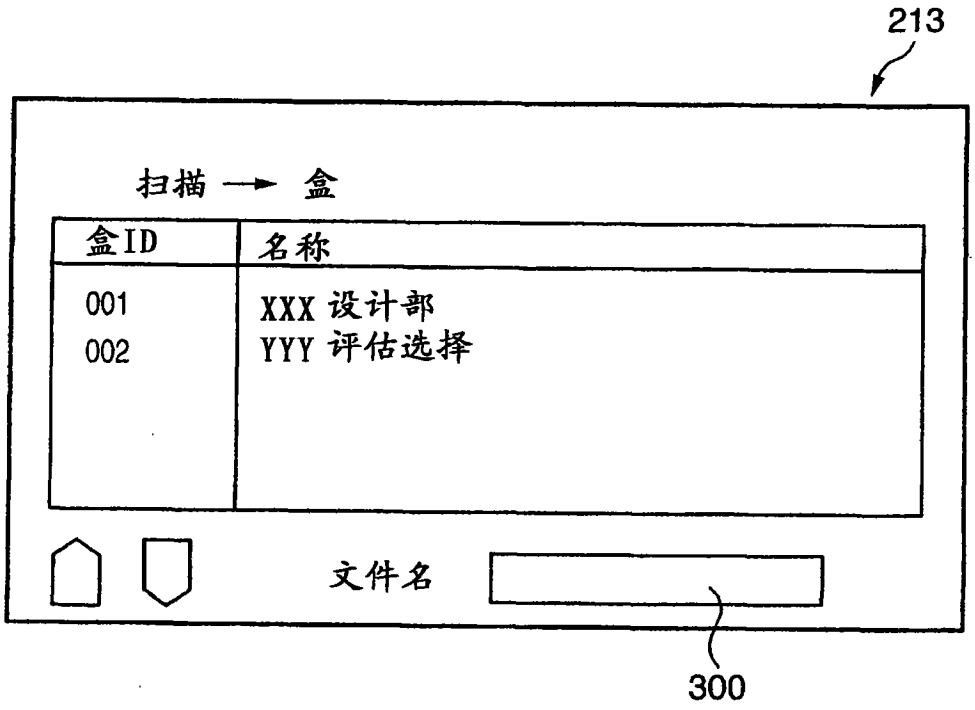


图 3

图4

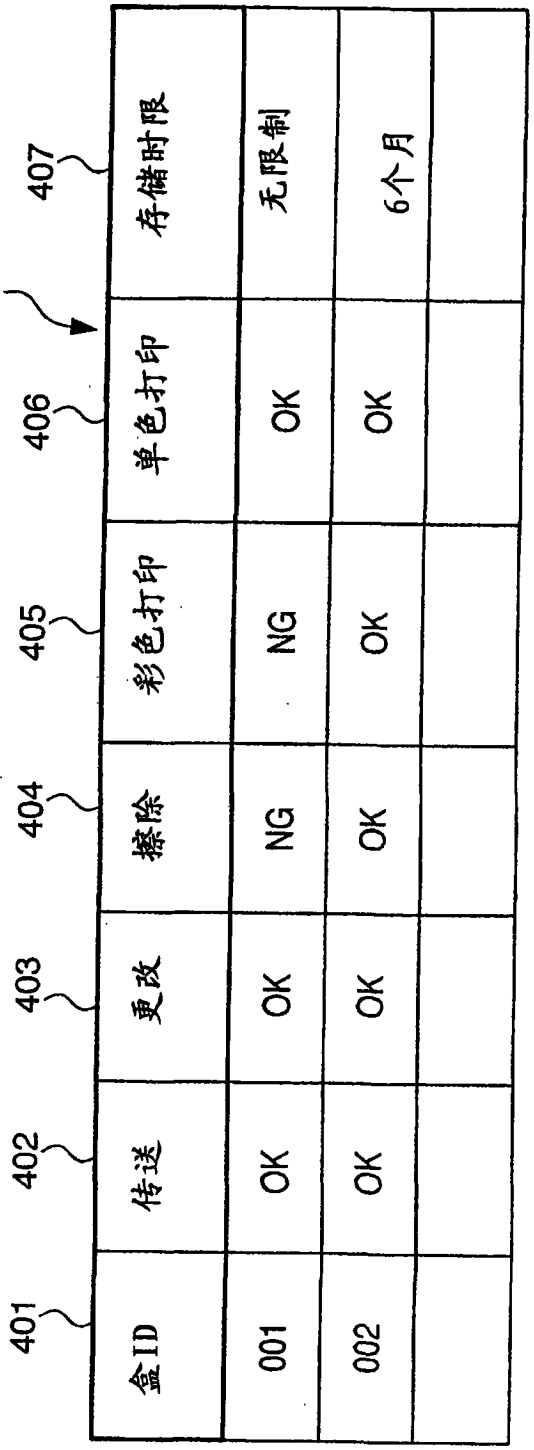

401
402
403
404
405
406
104
407
盒ID
传送
更改
擦除
彩色打印
单色打印
存储时限
001
OK
OK
NG
NG
OK
无限制
002
OK
OK
OK
OK
OK
6个月

图5

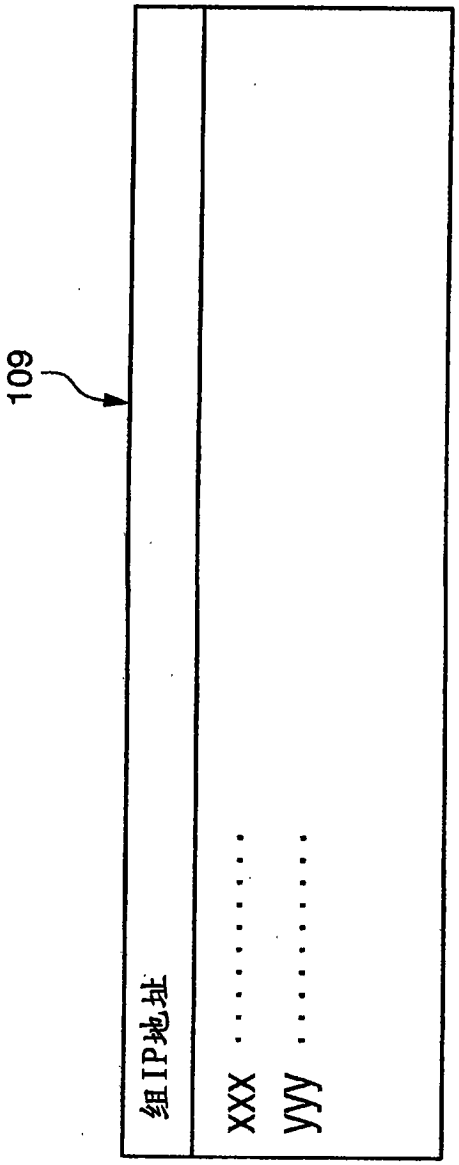


图6

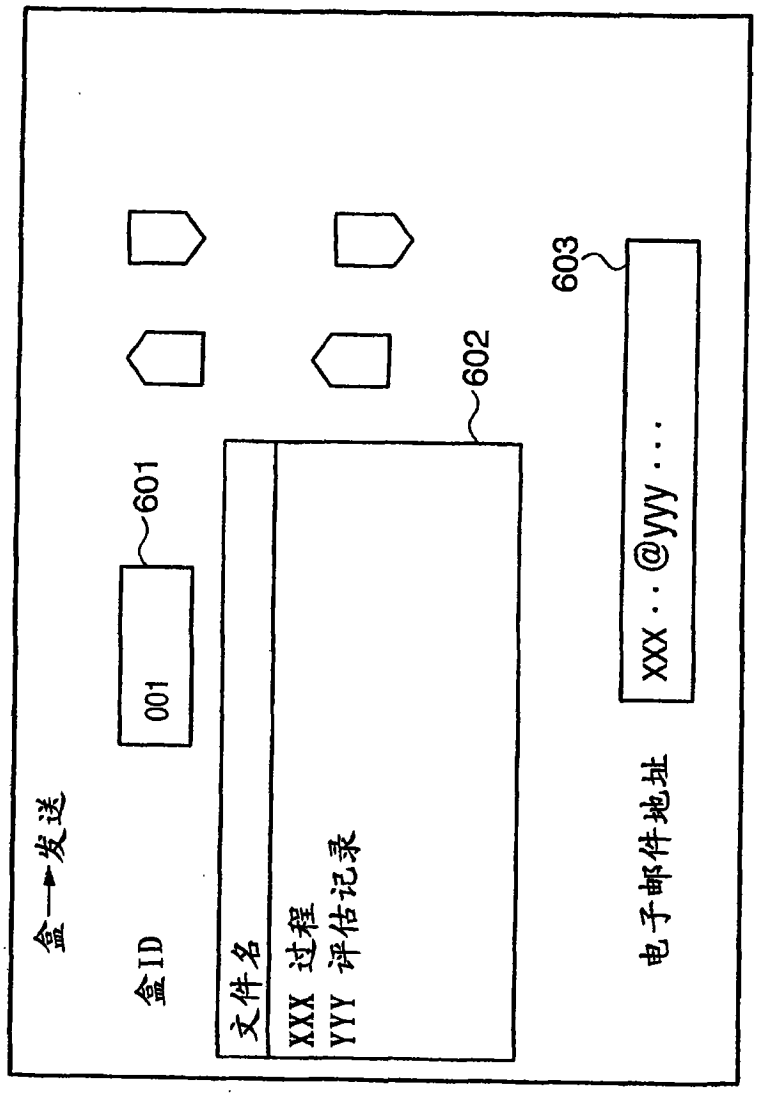
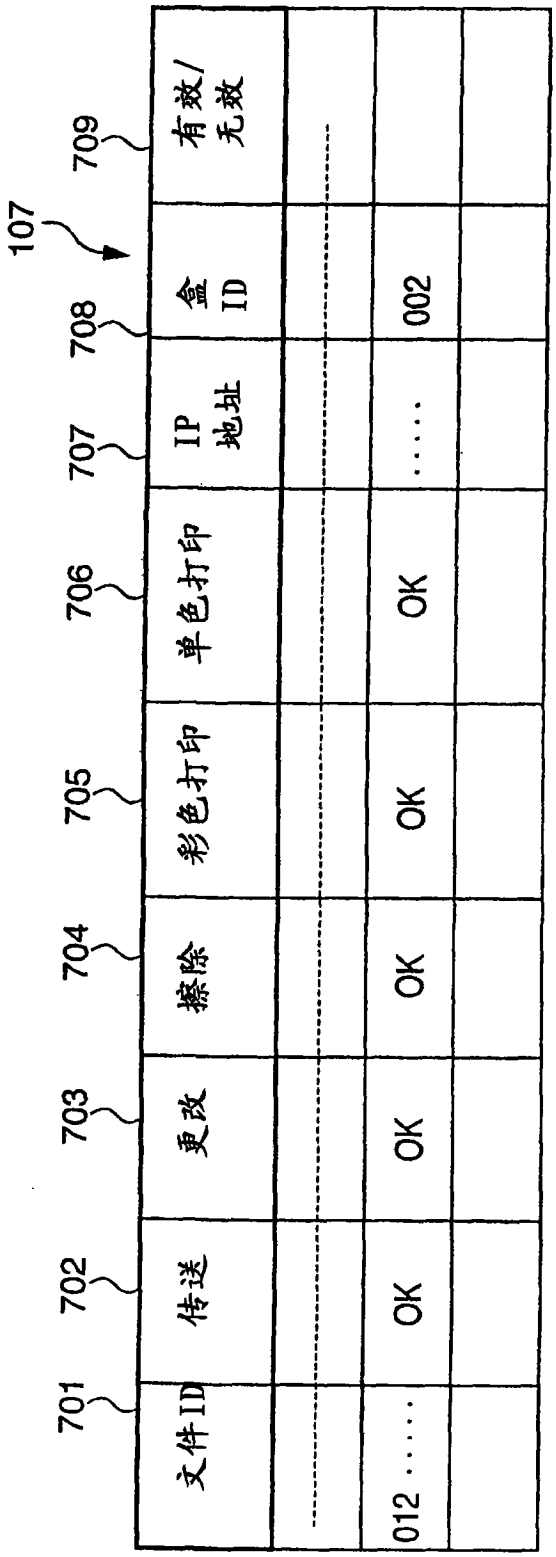


图7


107
701
文件ID
012 .....
702
传送
OK
703
更改
OK
704
擦除
OK
705
彩色打印
OK
706
单色打印
OK
707
IP 地址
.....
708
盒 ID
002
709
有效/无效

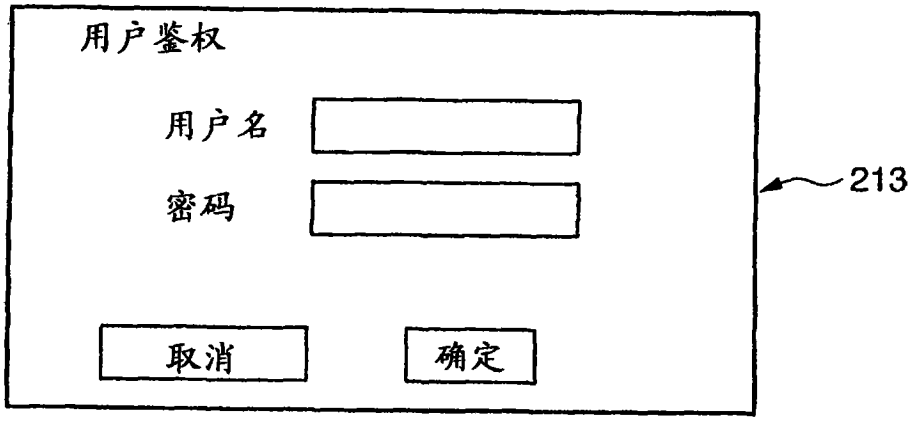
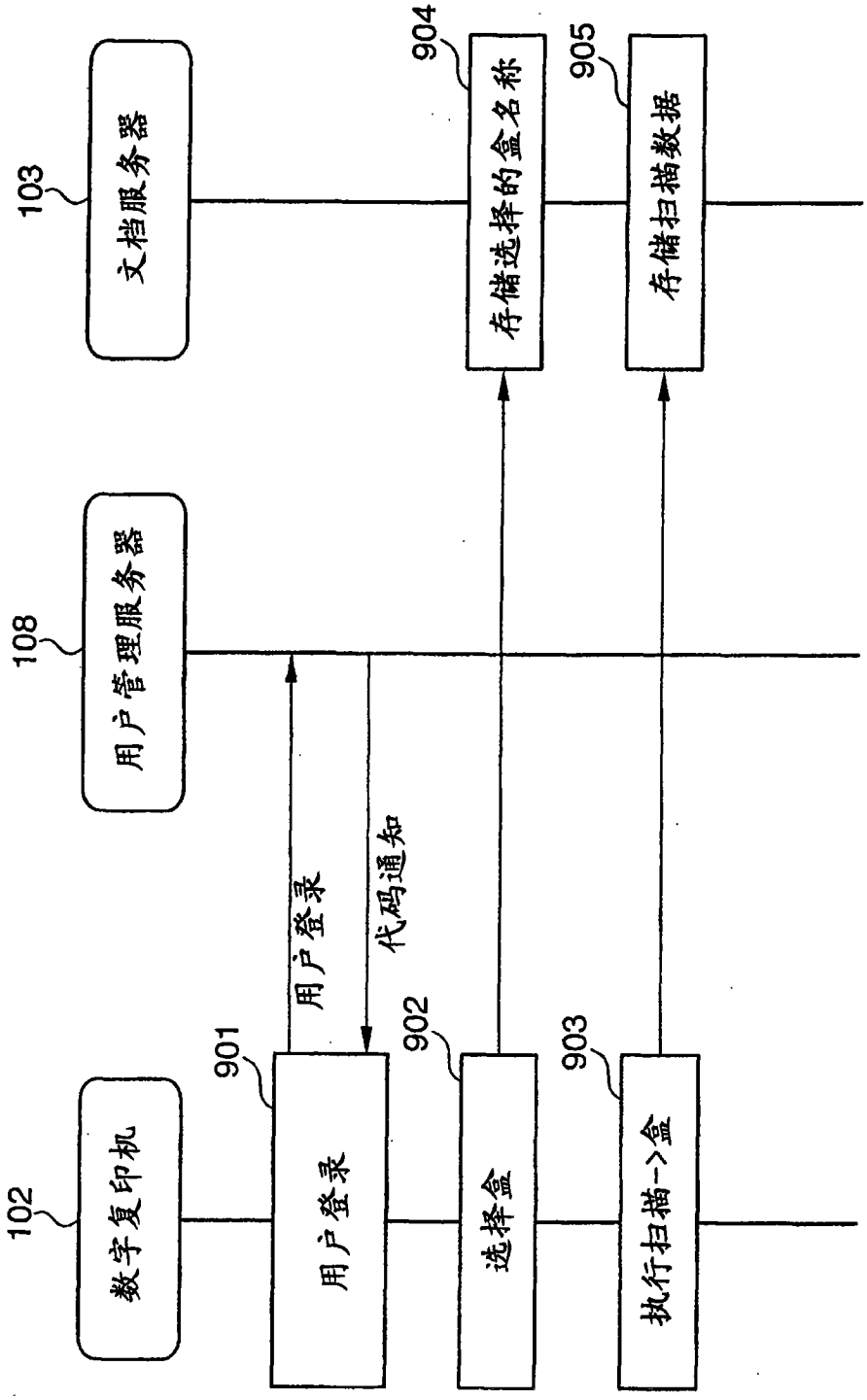


图 8

图9


数字复印机
102
用户登录
901
选择盒
902
执行扫描->盒
903
用户管理服务器
108
文档服务器
103
用户登录
代码通知
存储选择的盒名称
904
存储扫描数据
905

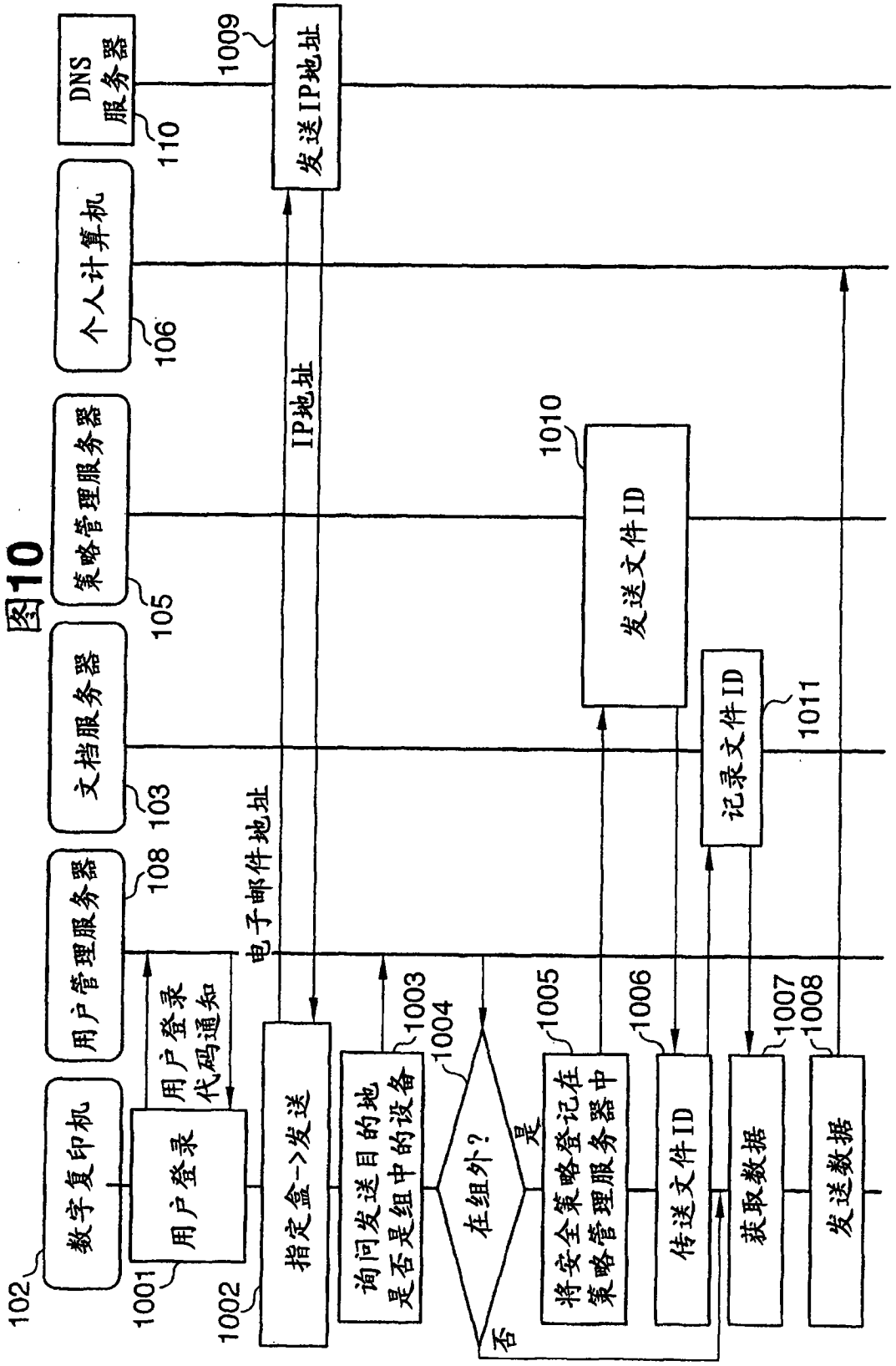
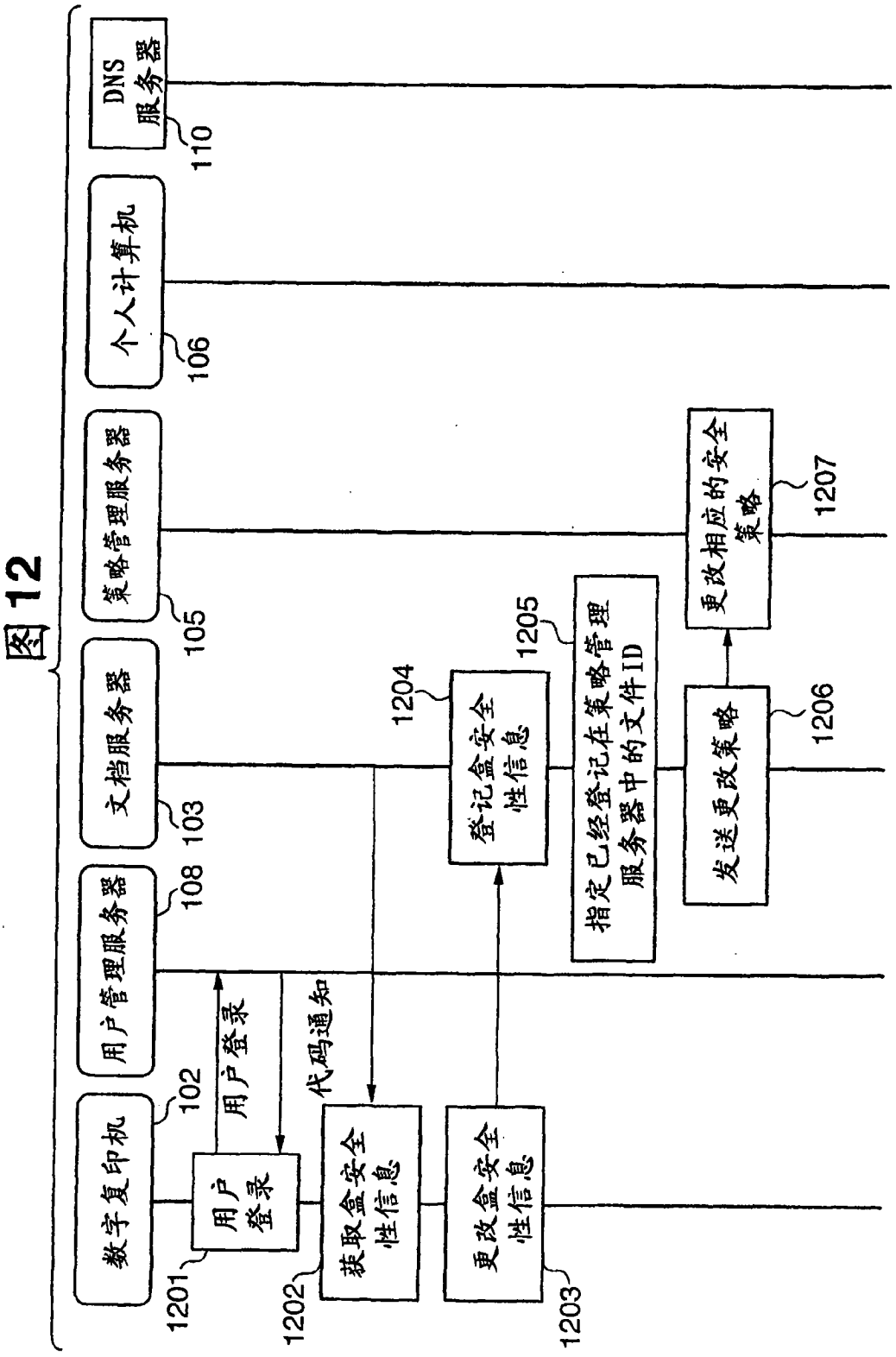

数字复印机
用户管理服务器
文档服务器
策略管理服务器
个人计算机
DNS服务器
102
108
103
105
106
110
用户登录
用户登录代码通知
电子邮件地址
IP地址
发送IP地址
1001
1002
1009
指定盒->发送
询问发送目的地是否是组中的设备
1003
在组外?
1004
是
否
将安全策略登记在策略管理服务器中
1005
发送文件ID
1010
传送文件ID
1006
记录文件ID
1011
获取数据
1007
发送数据
1008

图10

图11

文件名	文件ID	盒ID	策略管理服务器的IP地址
----------	----------	----------	----------
REPORT-20051224	012	002	111.222.33.444

图 12


数字复印机
用户管理服务器
文档服务器
策略管理服务器
个人计算机
DNS 服务器
102
108
103
105
106
110
用户登录
代码通知
用户登录
获取盒安全性信息
更改盒安全性信息
登记盒安全性信息
指定已经登记在策略管理服务器中的文件ID
发送更改策略
更改相应的安全策略
1201
1202
1203
1204
1205
1206
1207