[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 9/32 (2006.01)
H04L 29/06 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200710123322.5

[43] 公开日 2007 年 12 月 26 日

[11] 公开号 CN 101094071A

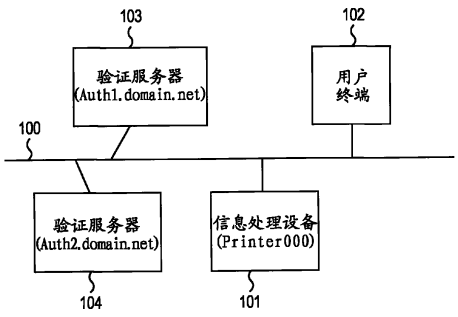
[22] 申请日 2007.6.20
[21] 申请号 200710123322.5
[30] 优先权
[32] 2006. 6.20 [33] JP [31] 2006 - 170247
[71] 申请人 佳能株式会社
地址 日本东京都大田区下丸子 3 - 30 - 2
[72] 发明人 岸本浩明
[74] 专利代理机构 北京林达刘知识产权代理事务所
代理人 刘新宇
权利要求书 2 页 说明书 15 页 附图 8 页

[54] 发明名称

能够与外部验证装置通信的信息处理设备和方法

[57] 摘要

本发明涉及一种能够与外部验证装置通信的信息处理设备和方法。 限制将在外部验证装置进行验证处理所需的验证信息未经加密而从用户终端发送到信息处理设备。 在不采用用于通信加密信息的加密通信的情况下，信息处理设备限制发送允许用户选择在外部验证装置进行验证处理的信息。



1. 一种信息处理设备，包括：

发送单元，用于在采用用来传递加密信息的加密通信的情况下，向用户终端发送允许用户选择在外部验证装置进行验证处理的信息；以及

接收单元，用于使用所述加密通信从所述用户终端接收由用户输入的在外部验证装置进行验证处理所需的验证信息；

其中，在不采用所述加密通信的情况下，所述发送单元限制向所述用户终端发送允许用户选择在外部验证装置进行验证处理的信息。

2. 根据权利要求1所述的信息处理设备，其特征在于，在采用所述加密通信的情况下，所述发送单元发送如下信息，所述信息允许Web浏览器显示允许用户输入在外部验证装置进行验证处理所需的验证信息和选择在外部验证装置进行验证处理的画面。

3. 根据权利要求1或2所述的信息处理设备，其特征在于，在不采用所述加密通信的情况下，所述发送单元发送如下信息，所述信息允许Web浏览器显示允许用户输入在所述信息处理设备进行验证处理所需的验证信息和选择在所述信息处理设备进行验证处理的画面。

4. 根据权利要求1或2所述的信息处理设备，其特征在于，还包括：

设置单元，用于允许用户选择采用或不采用所述加密通信。

5. 根据权利要求1或2所述的信息处理设备，其特征在于，还包括：

注册单元，用于允许用户注册外部验证装置；

其中，在采用所述加密通信的情况下，所述发送单元发送示出由所述注册单元注册的多个外部验证装置的列表的信息。

6. 一种信息处理方法，包括：

发送步骤，用于在采用用来传递加密信息的加密通信的情况下，向用户终端发送允许用户选择在外部验证装置进行验证处理的信息；以及

接收步骤，用于使用所述加密通信从所述用户终端接收由用户输入的在外部验证装置进行验证处理所需的验证信息；

其中，在不采用所述加密通信的情况下，限制向所述用户终端发送允许用户选择在外部验证装置进行验证处理的信息。

7. 根据权利要求6所述的信息处理方法，其特征在于，在采用所述加密通信的情况下，所述发送步骤用来发送如下信息，所述信息允许Web浏览器显示允许用户输入在外部验证装置进行验证处理所需的验证信息和选择在外部验证装置进行验证处理的画面。

8. 根据权利要求6或7所述的信息处理方法，其特征在于，在不采用所述加密通信的情况下，所述发送步骤用来发送如下信息，所述信息允许Web浏览器显示允许用户输入在所述信息处理设备进行验证处理所需的验证信息和选择在所述信息处理设备进行验证处理的画面。

9. 根据权利要求6或7所述的信息处理方法，其特征在于，还包括：

设置步骤，用于允许用户选择采用或不采用所述加密通信。

10. 根据权利要求6或7所述的信息处理方法，其特征在于，还包括：

注册步骤，用于允许用户注册外部验证装置；

其中，在采用所述加密通信的情况下，所述发送步骤用来发送示出在所述注册步骤注册的多个外部验证装置的列表的信息。

能够与外部验证装置通信的信息处理设备和方法

技术领域

本发明涉及一种能够与外部验证装置通信的信息处理设备和方法。

背景技术

包括验证功能的信息处理设备在用户通过网络操作该信息处理设备时执行验证处理。例如，当用户使用Web浏览器来指示打印设备转换到用户模式时，该打印设备请求从Web浏览器输入用户识别号，并基于由用户输入的用户识别号来执行验证处理(例如，日本特开第2002－359718号)。

当基于用户识别号的验证成功的情况下，打印设备向Web浏览器发送用户模式下的Web页。从而，用户可以从用户模式下的Web页来操作打印设备。

在具有网络环境时，在某些情况下，验证处理要采用的验证信息不是由多个信息处理设备的每一个来管理，而是由外部验证装置(下文中称为验证服务器)来整体管理。

例如，诸如用户名、密码等的验证信息被保留在验证服务器上，信息处理设备请求验证服务器基于用户输入的验证信息来执行验证处理。在用户通过网络从用户终端来操作信息处理设备的情况下，信息处理设备通过网络从用户终端接收验证信息，并请求验证服务器基于接收到的验证信息来执行验证处理。

这时，信息处理设备需要接收用户在用户终端输入的验证信息本身。在信息处理设备保持验证信息以执行验证处理的情况下，根据一些验证方法，不需要通过网络将用户输入了的验证信息本身发送到信息处理设备。另一方面，在信息处理设备

代替用户终端或作为用户终端和验证服务器之间的中介向验证服务器请求验证处理的情况下，信息处理设备需要接收由用户输入了的验证信息本身。

然而，在通过网络从用户终端向信息处理设备发送在验证服务器进行验证处理所需的验证信息的情况下，验证信息很容易遭受第三方的窃听，且很容易泄漏验证信息。

在用户终端和信息处理设备之间进行加密通信，从而防止验证信息被窃听。然而，信息处理设备不能总是执行加密处理。例如，在用户没有设定采用加密通信的情况下，信息处理设备不能执行加密通信。

使得在信息处理设备不能执行加密通信的情况下可以选择验证服务器的验证处理，这使得用户终端可以向信息处理设备发送验证信息，而不执行安全措施。

发明内容

为了该目的，本发明防止在外部验证装置进行验证处理所需的验证信息未经加密而从用户终端被发送到信息处理设备。

根据本发明的一个方面，一种信息处理设备，包括：发送单元，其用于在采用用来传递加密信息的加密通信的情况下，向用户终端发送允许用户选择在外部验证装置进行验证处理的信息；以及接收单元，其用于使用加密通信从用户终端接收由用户输入的在外部验证装置进行验证处理所需的验证信息；其中，在不采用加密通信的情况下，发送单元限制向用户终端发送允许用户选择在外部验证装置进行验证处理的信息。

此外，根据本发明的另一方面，一种信息处理方法，包括：发送步骤，用于在采用用来传递加密信息的加密通信的情况下，向用户终端发送允许用户选择在外部验证装置进行验证处理的

信息；以及接收步骤，用于使用加密通信从用户终端接收由用户输入的在外部验证装置进行验证处理所需的验证信息；其中，在不采用加密通信的情况下，限制向用户终端发送允许用户选择在外部验证装置进行验证处理的信息。

另外，根据本发明的另一方面，一种计算机可读取并可以执行的计算机程序，其使得计算机执行：发送步骤，用于在采用用来传递加密信息的加密通信的情况下，向用户终端发送允许用户选择在外部验证装置进行验证处理的信息；以及接收步骤，用于使用加密通信从用户终端接收由用户输入的在外部验证装置进行验证处理所需的验证信息；其中，在不采用加密通信的情况下，限制向用户终端发送允许用户选择在外部验证装置进行验证处理的信息。

此外，根据本发明的另一方面，一种存储计算机可读取并可以执行的计算机程序的记录介质，使得计算机执行：发送步骤，用于在采用用来传递加密信息的加密通信的情况下，向用户终端发送允许用户选择在外部验证装置进行验证处理的信息；以及接收步骤，用于使用加密通信从用户终端接收由用户输入的在外部验证装置进行验证处理所需的验证信息；其中，在不采用加密通信的情况下，限制向用户终端发送允许用户选择在外部验证装置进行验证处理的信息。

注意：该概述并不包括本发明的全部方面，权利要求书中记载的其它方面以及其特征的组合也可以包括在本发明中。

通过以下结合附图的说明，本发明的其他特征和优点将更明显，其中在全部附图中相似的附图标记指示相同或相似的部分。

附图说明

图1是示出网络系统结构的图。

图2是示出信息处理设备101和用户终端102的硬件结构的图。

图3是示出信息处理设备101执行的信息处理的流程图。

图4是示出用于允许或禁止SSL设置的管理画面的图。

图5是示出WWW浏览器显示的登录画面的图。

图6是示出信息处理设备101执行的验证处理的流程图。

图7是示出WWW浏览器显示的登录画面的图。

图8是示出用于请求验证服务器执行验证处理的信息处理的流程图。

具体实施方式

现在将参考附图详细说明本发明的实施例。应当注意：下面的实施例不限制权利要求书中所阐述的本发明，且作为达到本发明目的的手段，实施例中所述特征的全部组合不都是必不可少的。

第一实施例

下面将参考附图说明本发明的实施例。

图1是示出网络系统结构的图。使用该网络系统，信息处理设备101、用户终端102、验证服务器103、以及验证服务器104能够通过网络100互相通信。该网络可以是有线的或无线的。

验证服务器103和验证服务器104是用于基于用户名和密码执行验证处理的验证装置。信息处理设备101可以自己基于用户名和密码来执行验证处理，还可以请求验证服务器103和验证服务器104来执行验证处理。注意：验证处理所需的信息不限于用户名和密码。

对信息处理设备101、验证服务器103、和验证服务器104的每个设置名称作为识别信息。信息处理设备101的名称是“Printer000”，验证服务器103的名称是“Auth1.domain.net”，而验证服务器104的名称是“Auth2.domain.net”。

图2是示出信息处理设备101和用户终端102的硬件结构的图。现在，将打印设备作为信息处理设备101的一个例子进行说明。另外，信息处理设备101可以是扫描仪、数字多功能设备、复印机等。信息处理设备101包括：打印机单元201、中央处理单元(下文中称为CPU)202、RAM 203、网络接口单元204、I/O控制单元205、HDD 206、以及操作单元207。

CPU 202读出存储在HDD 206中的程序，并将该程序存储在RAM 203中。随后，CPU 202执行存储在RAM 203中的程序来控制整个信息处理设备101的操作。打印机单元201基于打印数据打印薄片。RAM 203存储由CPU 202执行的程序，存储执行程序所需的各种类型的变量值并/或存储打印数据。网络接口单元204通过网络100执行信息的发送/接收。I/O控制单元205控制从HDD 206的信息读取，以及对HDD 206的信息写入。HDD 206是大容量存储装置，其存储程序、打印数据、以及各种类型的信息。操作单元207包括操作面板和操作键。用户浏览显示在操作面板上的各种类型的信息，并使用操作键来输入各种类型的信息。

将个人计算机作为用户终端102的一个例子进行说明。用户终端102可以是工作站、便携终端等。用户终端102包括：中央处理单元(下文中称为CPU)210、网络接口单元211、输入/输出端口212、I/O控制单元214、HDD 215、RAM 216以及视频接口单元217。此外，将用户终端102通过输入/输出端口连

接到键盘213和鼠标219，并通过视频接口单元217连接到显示器218。

CPU 210读出存储在HDD 215的程序，并将该程序存储在RAM 216中。随后，CPU 210执行存储在RAM 216中的程序来控制整个用户终端102的操作。网络接口单元211通过网络100进行信息的发送/接收。将输入/输出端口212连接到例如键盘213、鼠标219等的输入装置，并连接到输入装置之外的外部装置(未示出)。随后，输入/输出端口212执行到/从输入装置或外部装置的信息发送/接收。用户使用键盘213或鼠标219来输入各种类型的信息。I/O控制单元214控制从HDD 215的信息读取，以及对HDD 215的信息写入。HDD 215是大容量存储装置，其存储程序和各种类型的信息。RAM 216存储由CPU 210执行的程序，还存储执行程序所需的各种类型的变量值。视频接口单元217向显示器218发送要在显示器218上显示的信息。显示器218是用于显示各种类型的信息的显示装置，用户浏览在显示单元218上显示的信息。

验证服务器103和验证服务器104的硬件结构与用户终端102的硬件结构相同。

对于用户终端102，网络浏览器(下文中称为WWW浏览器)的程序被存储在HDD 215中。WWW浏览器的程序被读出到RAM 216，并由CPU 210根据来自用户的指示来执行，从而WWW浏览器被激活。对于信息处理设备101，WWW服务器的程序被存储于HDD 206中。在信息处理设备101的电源被开启之后一会儿，WWW服务器的程序被读出到RAM 203，并由CPU 202执行，从而WWW服务器被激活。

WWW浏览器基于用户指定的地址、URL(Uniform Resource Locator，统一资源定位符)、或名称连接到WWW服

务器，并开始与WWW服务器通信。至于这时的通信协议，采用HTTP(Hyper Text Transfer Protocol，超文本传输协议)。WWW浏览器使用HTTP来访问WWW服务器，并请求从WWW服务器执行命令。WWW服务器执行命令，并向WWW浏览器发送示出其结果的文档信息。这时的文档信息用HTML(Hyper Text Markup Language，超文本标记语言)等来描述。WWW浏览器基于该文档信息绘制(render)画面，并在显示器218上显示该画面。

下面将说明根据本发明的信息处理。图3是示出信息处理设备101执行的信息处理的流程图。CPU 202执行基于图3中所示的流程图的程序，从而执行该信息处理。

信息处理设备101接收来自用户终端102的WWW浏览器的访问(步骤S301)。对此响应，信息处理设备101判断SSL(Secure Socket Layer，安全套接字层)设置是有效的还是无效的(步骤S302)。

图4是示出用于允许或禁止SSL设置的管理画面的图。当具有管理员权限的用户使用WWW浏览器访问信息处理设备101，并作为管理员验证成功时，WWW浏览器显示管理画面。此外，管理画面可以由操作单元207来显示。

在图4中，选择开关401用来允许或禁止SSL设置。在SSL设置有效的情况下，可以采用基于SSL的加密通信，在SSL设置无效的情况下，不能采用基于SSL的加密通信。该SSL是用来使用加密技术保护WWW浏览器和WWW服务器之间的HTTP通信的协议。为了执行采用SSL的加密通信，SSL设置需要在WWW服务器(这里是信息处理设备101)处是有效的，并且WWW浏览器需要执行SSL的加密通信。对于信息处理设备101的初始值，SSL设置被设定为无效。

信息处理设备101本身支持它自己的用户验证方法，从而在信息处理设备101进行验证处理所需的密码被保护，并因此，SSL的加密通信不是必须的。因此，SSL设置可以被设定为无效。

选择开关402是用来在SSL设置有效的情况下允许在验证服务器进行验证处理，或即使在SSL设置是有效的情况下也禁止在验证服务器进行验证处理的开关。

在通常情况下，对于采用SSL的加密通信，要发送/接收的信息是加密的，并且其安全性是有保障的。也就是说，即使在验证服务器进行验证处理所需的密码被从用户终端102发送到信息处理设备101的情况下，密码的安全性也是有保障的，并且只要SSL设置是有效的，密码就被保护不被窃听。然而，对于在验证服务器的验证处理所采用的验证信息被更严格管理的情况，其验证信息被防止通过网络传送，从而存在不希望允许在验证服务器执行验证处理的情况。选择开关402被用于这种情况。

区域403用来允许管理员注册验证服务器。管理员输入验证服务器的名称，借此他/她可以注册多个验证服务器。对于图4所示的例子，验证服务器103和验证服务器104被注册。

对于图4所示的例子，输入了验证服务器的名称，但也可以输入用于识别验证服务器的其它识别信息。例如，对按域管理网络的环境，对于每个域存在验证服务器。因此，可以将每个域的名称(下文中称为域名)用作识别信息来识别验证服务器。

此外，可以进行这样的设置：用户不仅输入验证服务器的名称，还自动从存在于网络上的管理服务器获取示出验证服务器列表的信息，以注册包括在列表中的验证服务器的名称。例

如，用来从存在于网络上的装置的名称中搜索装置的IP地址的DNS服务器将多个验证服务器的名称存储为SRV记录。信息处理设备101自动从DNS服务器的服务(SRV)记录中获取多个验证服务器的名称，并将它们显示在区域403中。

在步骤S302中判断为SSL设置无效的情况下，继续通信而不采用SSL。信息处理设备101仅将信息处理设备101列为登录目的地，并生成示出登录画面的文档信息(步骤S303)。随后，信息处理设备101向用户终端102发送示出登录画面的文档信息(步骤S304)。

在SSL设置无效的情况下，只允许在信息处理设备101进行验证处理。对于在验证服务器处的验证处理，信息处理设备101代理用户终端102，并请求验证服务器执行验证处理。因此，信息处理设备101需要由用户输入的密码本身，且必须将用户输入的密码本身从用户终端102发送到信息处理设备101。在执行采用SSL的加密通信的情况下，密码被加密，这保护密码不被窃听，但在不执行采用SSL的加密通信的情况下，密码很容易遭到窃听。因此，在SSL设置无效的情况下，设置不执行验证服务器的验证处理。

另一方面，对于在信息处理设备101进行的验证处理，由用户输入的密码本身不按下面的方法发送。

图5是示出基于步骤S304中发送的文档信息由WWW浏览器显示的登录画面的图。输入区域501用来允许输入用户名，输入区域502用来允许输入密码。下拉菜单503用来选择登录目的地。在登录目的地执行基于用户名和密码的验证处理。对于图5所示的登录画面，只有信息处理设备101可以被选为登录目的地。

当用户输入了用户名、密码，选择了登录目的地，并按下

了OK按钮时，用户终端102向信息处理设备101发送用于请求执行验证处理的命令(下文中称为验证请求命令)。

对于在信息处理设备101处的验证处理，不必向信息处理设备101发送用户输入的密码本身。WWW浏览器使用具有单向属性的特殊函数(例如，哈希(hash)函数)对用户输入的密码进行处理。不可能使该特殊函数生成的值逆变换为初始密码。

验证请求命令指出用户输入的用户名、由特殊函数生成的值(下文中称为第二密码)、以及用户选择的登录目的地。

信息处理设备101从用户终端102接收其验证请求命令(步骤S305)。由这里接收的验证请求命令指出的登录目的地一直是信息处理设备101。因此，执行信息处理设备101的验证处理(步骤S306a)。

图6是示出信息处理设备101执行的验证处理的流程图。CPU 202执行基于图6所示的流程图的程序，从而执行验证处理。

信息处理设备101的HDD 206保持用户数据库(下文中称为用户DB)。用户DB存储被允许登录到信息处理设备101的用户的至少一组用户名和密码。

信息处理设备101从用户DB中搜索验证请求命令指出的用户名(步骤S601)。随后，信息处理设备101基于搜索结果判断验证请求命令所指出的用户名是否存在于用户DB中(步骤S602)。

在验证请求命令所指出的用户名不存在于用户DB中的情况下，信息处理设备101向用户终端102发送说明验证失败的文档信息(步骤S603)。WWW浏览器基于该文档信息在显示器218上显示验证失败。

另一方面，在验证请求命令指出的用户名存在于用户DB

中的情况下，信息处理设备101将由验证请求命令指出的第二密码与用户DB中的密码相匹配，并判断是否一致(步骤S604)。在步骤S604中，信息处理设备101首先使用上述特殊函数对在用户DB中找到的密码进行处理以生成第二密码。随后，信息处理设备101判断验证请求命令指出的第二密码是否与从用户DB中的密码生成的第二密码相同。

在两个第二密码不相同的情况下，信息处理设备101向用户终端102发送文档信息来反映验证失败(步骤S603)。在两个第二密码相同的情况下，信息处理设备101向用户终端102发送只在验证成功的情况下才发送的文档信息(步骤S605)。例如，在步骤S605中发送图5所示的示出登录画面的文档信息、示出用于允许用户操作信息处理设备101的打印处理的操作画面的文档信息等。

不必说明这里所述基于用户名和密码的验证方法只是一个例子，可以使用其它方法来执行验证。

在图3的步骤S302中判断为SSL设置有效的情况下，信息处理设备101向用户终端102发送转向SSL的访问的指令，从而执行SSL加密通信(步骤S306b)。根据该转向指令，WWW浏览器将访问WWW服务器所采用的端口从通常HTTP通信所采用的端口切换到受SSL保护的HTTP通信所采用的端口。HTTP通信通常所采用的端口的例子是端口80，受SSL保护的HTTP通信所采用的端口的例子是端口443。随后，WWW浏览器再次使用SSL来访问端口443。

信息处理设备101接收来自用户终端102的WWW浏览器的访问(对端口443的访问)(步骤S307)。对于步骤S307中的通信，采用SSL。

接下来，信息处理设备101判断验证服务器的验证处理是

被允许还是被禁止(步骤S308)。通过管理画面的选择开关402设定验证服务器的验证处理是允许或是禁止。

即使在SSL设置有效的情况下，当禁止验证服务器的验证处理时，信息处理设备101进行到步骤S303。在这种情况下，只执行信息处理设备101的验证处理。

在允许验证服务器的验证处理的情况下，信息处理设备101判断是否存在已注册的验证服务器 (步骤S309)。在不存在已注册的验证服务器的情况下，信息处理设备101进行到步骤S303。

在存在已注册的验证服务器的情况下，信息处理设备101将已注册的验证服务器以及信息处理设备101列为登录目的地，并生成指出登录画面的文档信息(步骤S310)。随后，信息处理设备101向用户终端102发送示出该登录画面的文档信息(步骤S311)。

图7是示出基于步骤S311中发送的文档信息由WWW浏览器显示的登录画面的图。输入区域701用来允许输入用户名，且输入区域702用来允许输入密码。下拉菜单703用于选择登录目的地。对于图7所示的登录画面，不仅信息处理设备101，还有验证服务器103和验证服务器104都可以被选为登录目的地。

当用户输入了用户名和密码，选择了登录目的地，并按下OK按钮时，用户终端102向信息处理设备101发送验证请求命令。

在用户选择信息处理设备101作为登录目的地的情况下，验证请求命令指出由用户输入的用户名、从用户输入的密码生成的第二密码、以及用户选择的登录目的地。在用户选择验证服务器作为登录目的地的情况下，验证请求命令指出用户输入的用户名、用户输入的密码、以及用户选择的登录目的地。

信息处理设备101从用户终端102接收其验证请求命令(步骤S312)。接下来，信息处理设备101判断验证请求命令所指出的登录目的地是信息处理设备101还是验证服务器(步骤S313)。在登录目的地是信息处理设备101的情况下，信息处理设备101进行到步骤S306a。在这种情况下，执行信息处理设备101的验证处理。在登录目的地是验证服务器的情况下，执行该验证服务器的验证处理(步骤S314)。

图8是示出用来请求验证服务器执行验证处理的信息处理的流程图。CPU 202基于图8所示的流程图执行程序，从而执行该信息处理。

基于从用户终端102接收的验证请求命令所指出的用户名和密码，信息处理设备101请求从被选择为登录目的地的验证服务器使用预定的协议来执行验证处理(步骤S801)。预定的协议是被选为登录目的地的验证服务器支持的协议。例如，可用的协议有NTLM、Kerberos等。对于这些协议，用户名和密码不是从信息处理设备101作为它们本身传送到验证服务器的，而是根据一系列安全程序来执行验证处理。

随着验证服务器执行验证处理，信息处理设备101从验证服务器接收验证结果(步骤S802)。随后，信息处理设备101基于接收到的验证结果判断验证是否成功(步骤S803)。

在判断为验证失败的情况下，信息处理设备101向用户终端102发送指出验证失败的文档信息(步骤S804)。WWW浏览器基于该文档信息，在显示器218上显示验证失败。

在判断为验证成功的情况下，信息处理设备101向用户终端102发送仅在验证成功的情况下才发送的文档信息(步骤S805)。

其它实施例

已经对本发明的实施例进行了详细说明，但应该理解本发明不局限于上述实施例。例如，本发明可以用于由多个装置构成的系统，或可以用于由一个装置构成的设备。

注意：本发明还可以通过直接或远程地向系统或设备提供实现上述实施例的功能的软件程序，并且该系统或设备读取并执行所提供的程序来达到。在这种情况下，其形式不局限于程序，只要其具有程序的功能。

因此，为了使用计算机来实现本发明的功能处理，要安装在计算机中的程序代码本身也实现本发明。也就是说，本发明的范围还包括实现本发明的功能处理的计算机程序本身。在这种情况下，可以采用任何程序形式，例如目标代码、由解释器执行的程序、要提供给操作系统(OS)的脚本数据等，只要它包括程序的功能。

对于用于提供程序的记录介质，可以采用各种类型。例如，可以使用软盘、硬盘、光盘、磁光盘、MO、CD-ROM、CD-R、CD-RW、磁带、非易失性存储卡、ROM、DVD(DVD-ROM、DVD-R)等。

另外，对于用于提供程序的方法，可以通过使用客户计算机的浏览器访问因特网的主页、并且从主页下载程序到例如硬盘等的记录介质来提供程序。在这种情况下，可以下载根据本发明的计算机程序本身或包括自动安装功能的压缩文件。

此外，构成本发明的程序的程序代码可以被分为多个文件，从不同的主页下载每个文件，从而程序可以被提供。换句话说，允许多个用户下载用于在计算机上实现本发明的功能处理的程序文件的WWW服务器也包括在本发明的范围内。

此外，可以采这种设置：将根据本发明的程序加密，存储在例如CD－ROM等的记录介质中，并分发给用户。在这种情

况下，允许满足预定条件的用户通过因特网从主页下载用于解码加密的密钥信息，并允许通过使用该密钥信息以可执行形式来安装加密的程序。

此外，上述实施例的功能可以用不同于由计算机执行读出的程序的上述设置的另一种设置来实现。例如，运行于计算机上的操作系统等可以基于程序的指令来执行部分或全部实际的处理，上述实施例的功能由该处理来实现。

此外，可以进行这种设置：将从记录介质读出的程序写入包括在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。在这种情况下，包括在功能扩展板或功能扩展单元中的CPU等随后基于程序的指令执行部分或全部实际处理，并且通过该处理来实现上述实施例的功能。

根据本发明，在不采用用于通信加密信息的加密通信的情况下，可以防止用户选择在外部验证装置进行验证处理。

此外，在不采用加密通信的情况下，允许用户选择在信息处理设备进行验证处理，从而可以防止从用户终端向信息处理设备发送验证服务器的验证处理所需的验证信息。

尽管参考典型实施例说明了本发明，应该理解本发明不局限于所公开的典型实施例。所附权利要求书的范围符合最宽的解释，从而包括全部变形、等同结构和功能。

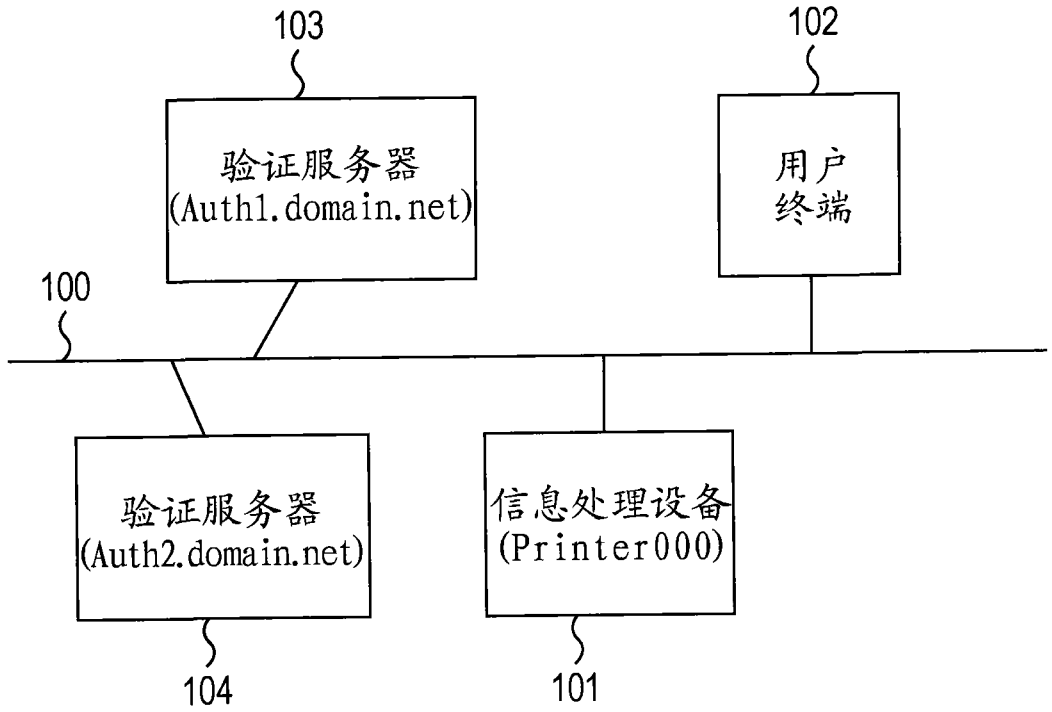

103
验证服务器
(Auth1.domain.net)
102
用户
终端
100
验证服务器
(Auth2.domain.net)
信息处理设备
(Printer000)
104
101

图 1

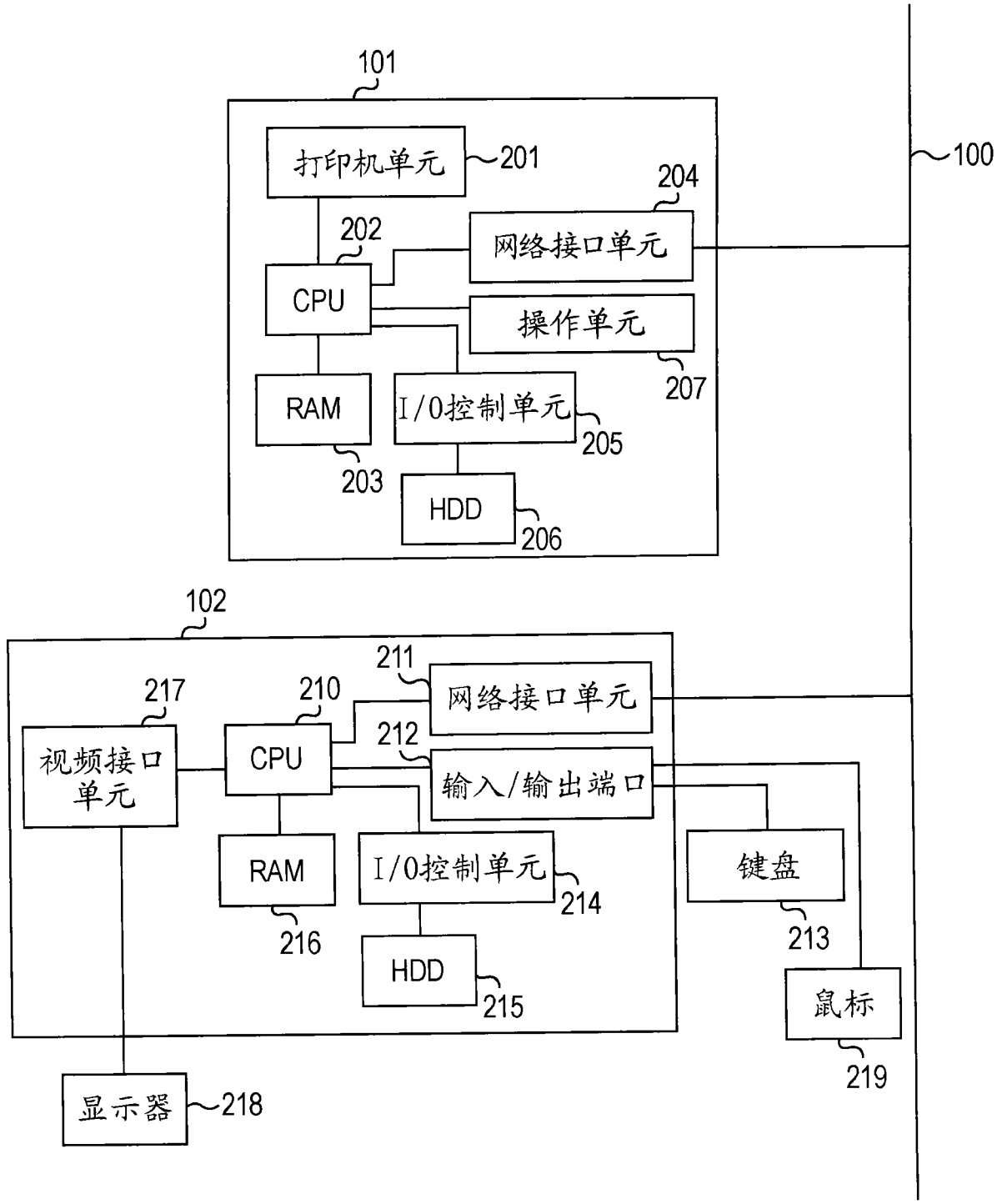

101
打印机单元
201
204
网络接口单元
202
CPU
操作单元
207
RAM
I/O控制单元
205
203
HDD
206
100
102
211
网络接口单元
217
210
视频接口单元
CPU
212
输入/输出端口
RAM
I/O控制单元
214
键盘
216
213
HDD
215
鼠标
219
显示器
218

图 2

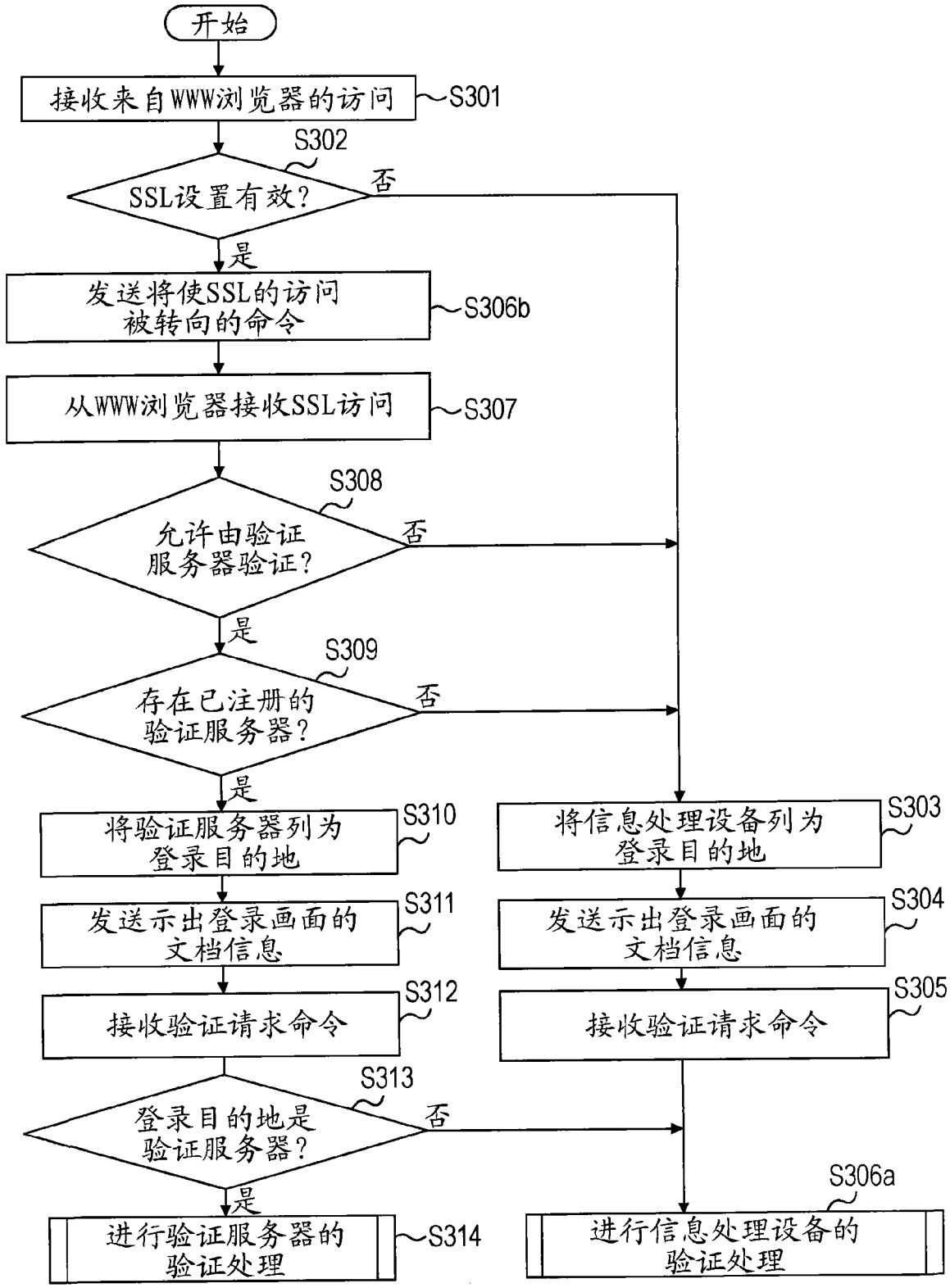

开始
接收来自WWW浏览器的访问
S301
S302
SSL设置有效?
否
是
发送将使SSL的访问被转向的命令
S306b
从WWW浏览器接收SSL访问
S307
S308
允许由验证服务器验证?
否
是
S309
存在已注册的验证服务器?
否
是
将验证服务器列为登录目的地
S310
发送示出登录画面的文档信息
S311
接收验证请求命令
S312
S313
登录目的地是验证服务器?
否
是
进行验证服务器的验证处理
S314
将信息处理设备列为登录目的地
S303
发送示出登录画面的文档信息
S304
接收验证请求命令
S305
S306a
进行信息处理设备的验证处理

图 3

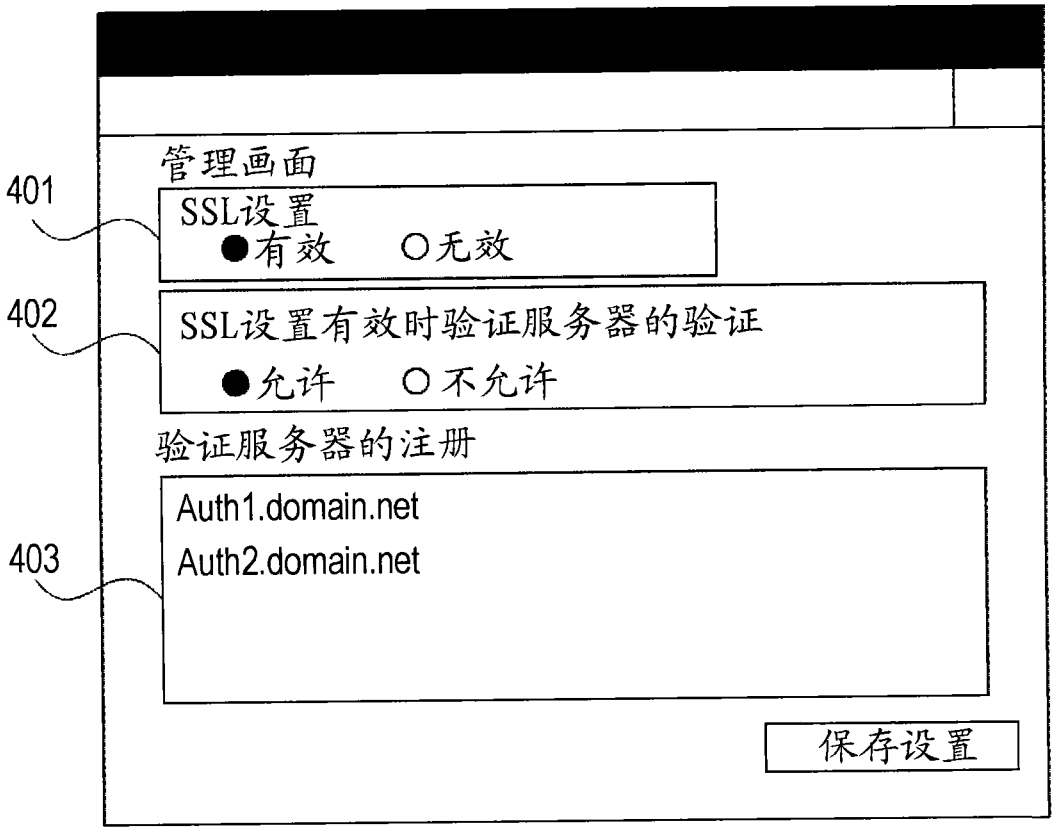

管理画面
401
SSL设置
●有效 ○无效
402
SSL设置有效时验证服务器的验证
●允许 ○不允许
验证服务器的注册
403
Auth1.domain.net
Auth2.domain.net
保存设置

图 4

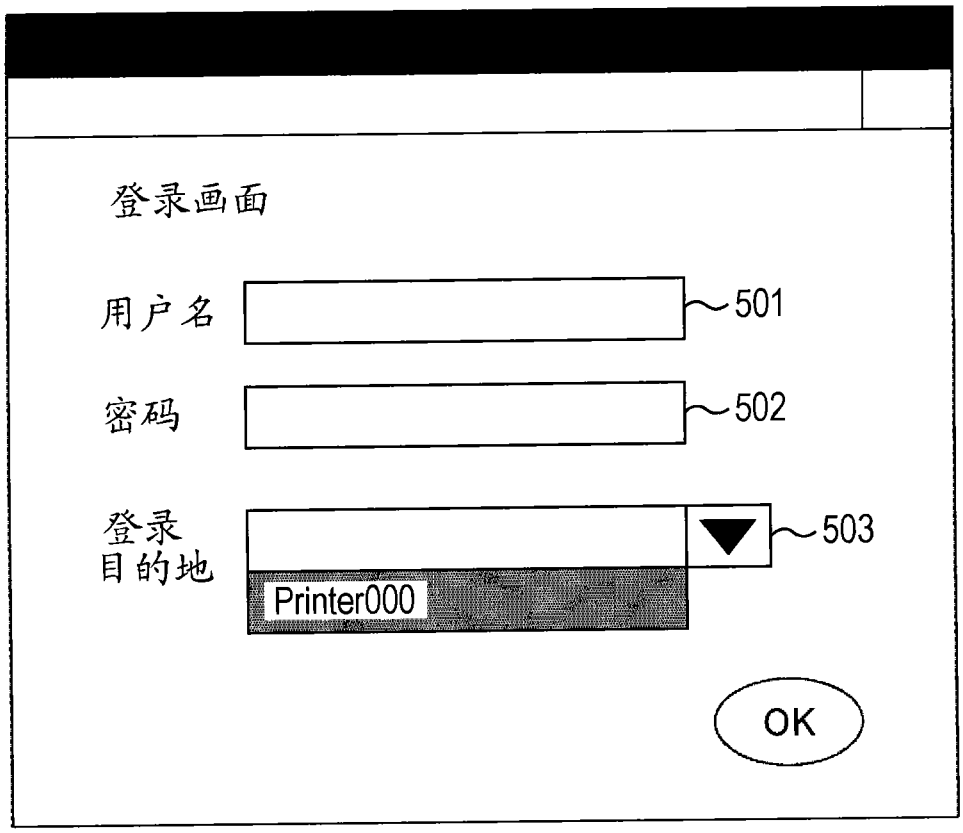


图 5

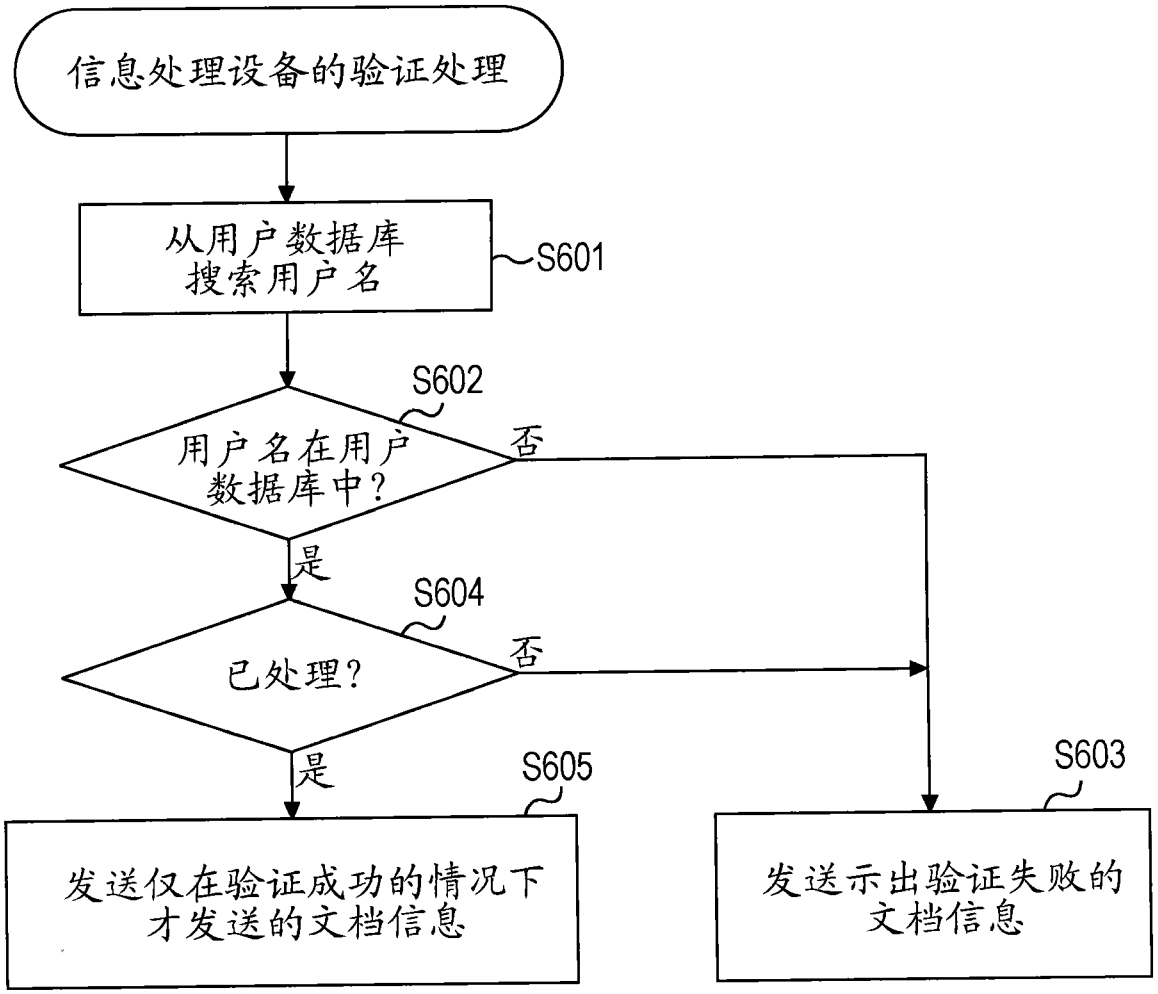

信息处理设备的验证处理
从用户数据库
搜索用户名
S601
S602
用户名在用户
数据库中？
否
是
S604
已处理？
否
是
S605
S603
发送仅在验证成功的情况下
才发送的文档信息
发送示出验证失败的
文档信息

图 6

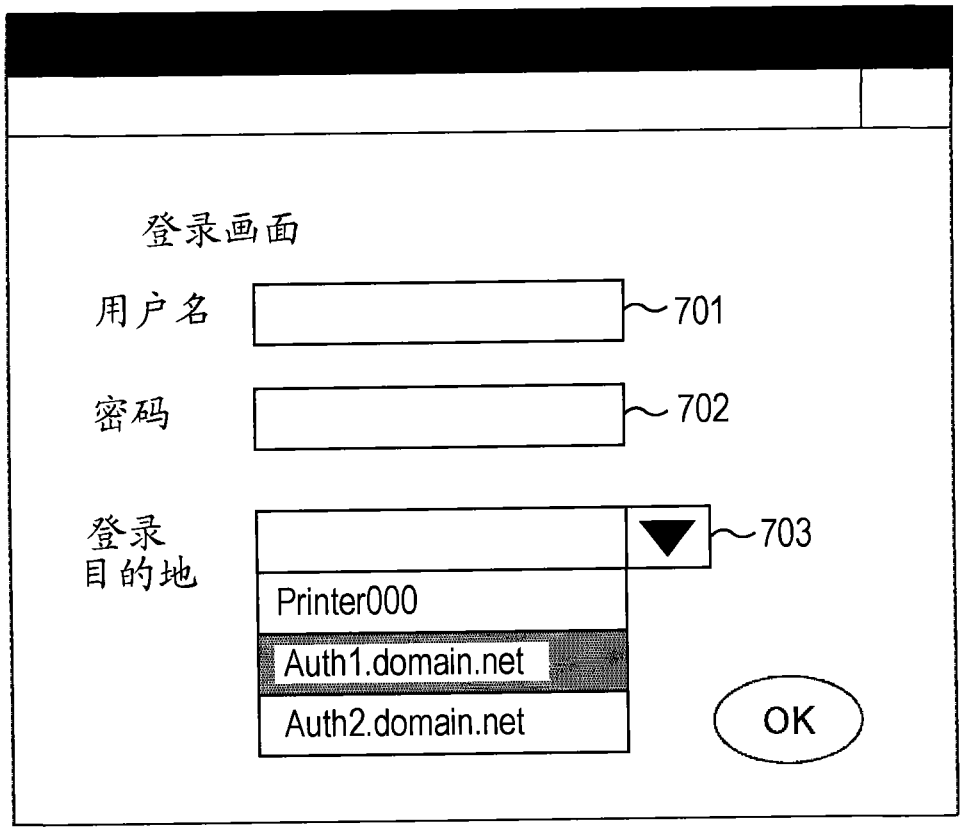

登录画面
用户名
701
密码
702
登录
目的地
703
Printer000
Auth1.domain.net
Auth2.domain.net
OK

图 7

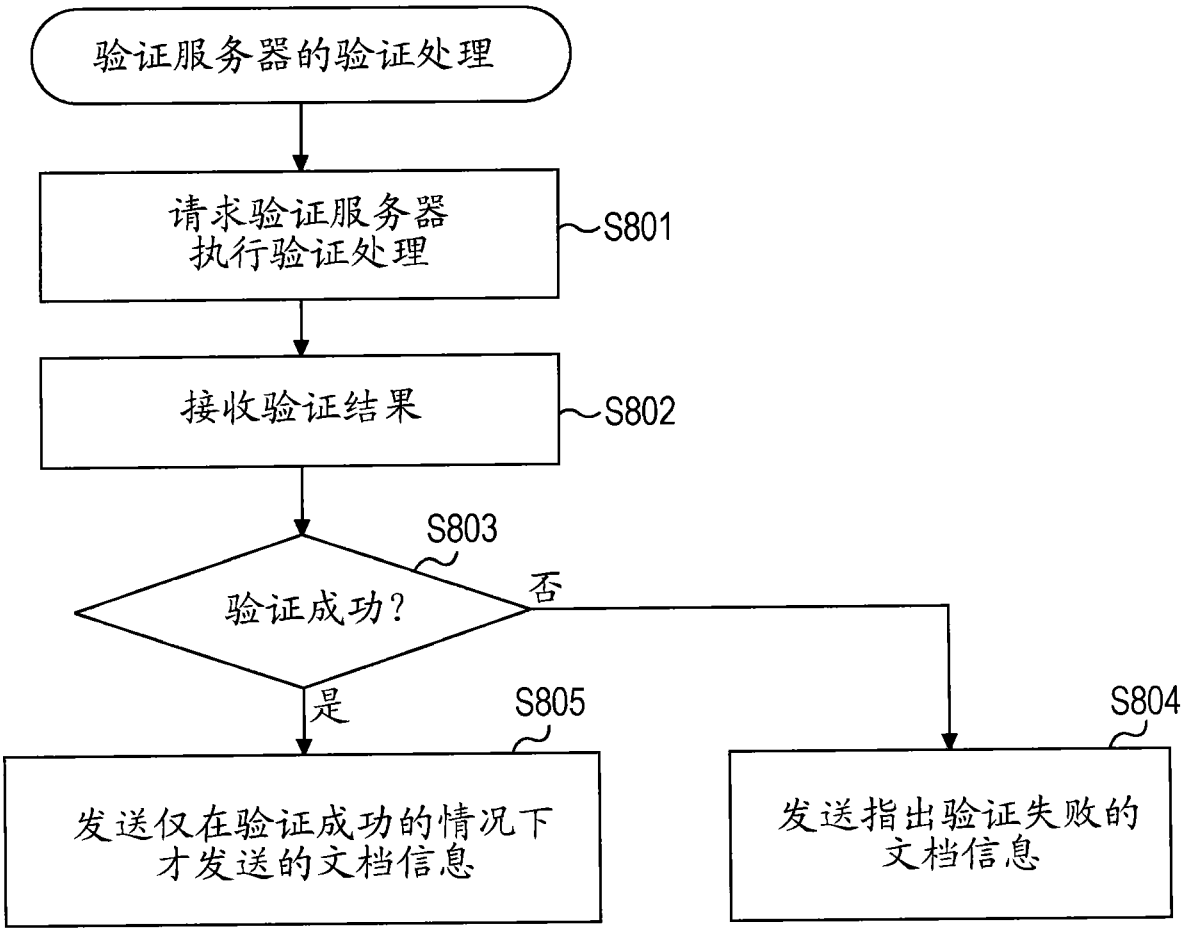

验证服务器的验证处理
请求验证服务器
执行验证处理
S801
接收验证结果
S802
S803
验证成功？
否
是
S805
发送仅在验证成功的情况下
才发送的文档信息
S804
发送指出验证失败的
文档信息

图 8