(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 104426912 B
(45)授权公告日 2017.12.29

(21)申请号 201410440836.3

(22)申请日 2014.09.01

(65)同一申请的已公布的文献号
申请公布号 CN 104426912 A

(43)申请公布日 2015.03.18

(30)优先权数据
2013-181564 2013.09.02 JP

(73)专利权人 佳能株式会社
地址 日本东京都大田区下丸子3丁目30-2

(72)发明人 细田泰弘

(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 迟军

(51)Int.Cl.
H04L 29/06(2006.01)

(56)对比文件
US 2006005044 A1,2006.01.05,
US 2006005044 A1,2006.01.05,
US 2011289571 A1,2011.11.24,
US 2006291453 A1,2006.12.28,
US 2011072322 A1,2011.03.24,
US 2008022090 A1,2008.01.24,
CN 101202668 A,2008.06.18,

审查员 李珍珍

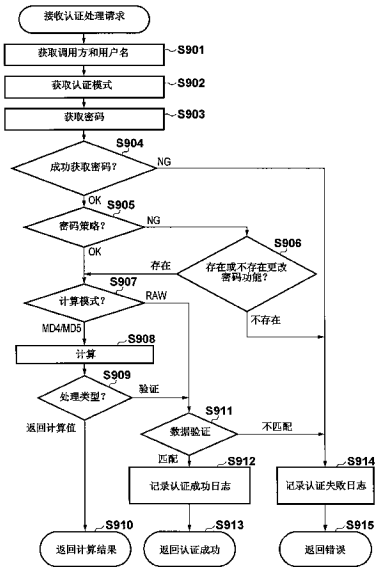
权利要求书3页 说明书10页 附图13页

(54)发明名称

信息处理装置及其控制方法

(57)摘要

本发明提供一种信息处理装置及其控制方法。所述信息处理装置能够根据多个协议中的协议来接收认证请求。所述信息处理装置存储针对各用户的用户标识和密码以及针对各协议的计算方法，并且在所述装置根据所述多个协议中的协议从远程计算机接收包括认证数据的认证请求的情况下，所述装置获得存储的与所述认证请求中包括的所述认证数据相对应的密码，获得存储的与所述协议相对应的计算方法，根据所获得的计算方法将所获得的密码转换为哈希，以及使用所述哈希来验证所述认证数据。



CN 104426912 B

1.一种信息处理装置，其能够根据多个协议中的协议来接收认证请求，所述信息处理装置包括：

存储单元，其被配置为存储针对各用户的用户标识和密码以及针对各协议的计算方法；

接收单元，其被配置为根据所述多个协议中的协议，从远程计算机接收认证请求，所述认证请求包括认证数据；

控制单元，其被配置为：

(a)提供利用HTTP与HTTP客户端通信的HTTP服务器；

(b)提供利用SNMP与SNMP客户端通信的SNMP服务器；

(c)提供认证系统，该认证系统被配置为：

(i)从所述存储单元获得与所述认证请求中包括的所述认证数据相对应的密码；

(ii)在所述接收单元利用HTTP从HTTP客户端接收到认证请求的情况下，从所述存储单元获得与HTTP相对应的计算方法；

(iii)在所述接收单元利用SNMP从SNMP客户端接收到认证请求的情况下，从所述存储单元获得与SNMP相对应的计算方法；

(iv)确定所获得的密码是否满足密码策略；

(v)在确定所获得的密码满足所述密码策略的情况下，根据所获得的计算方法，将所获得的密码转换为哈希，其中，基于所述哈希来验证所述认证数据。

2.根据权利要求1所述的信息处理装置，其中，所述控制单元基于所述验证，允许用户登录到所述信息处理装置。

3.根据权利要求1所述的信息处理装置，其中，所述协议是HTTP、SMB和SNMP中的任意一者。

4.根据权利要求1所述的信息处理装置，所述信息处理装置还包括：发送单元；

其中，所述认证系统被配置为：

在所述接收单元从HTTP客户端接收到认证请求的情况下，利用所述哈希来验证所述认证数据；

将认证结果发送给HTTP客户端；并且

在所述接收单元从SNMP客户端接收到认证请求的情况下，将所述哈希发送给SNMP服务器；以及

所述SNMP服务器被配置为：

基于从所述认证系统接收到的所述哈希来验证所述认证数据；并且，

将认证结果发送给所述认证系统。

5.根据权利要求1所述的信息处理装置，所述信息处理装置还包括：

通知单元，其被配置为在从所述存储单元获得密码失败的情况下，向所述远程计算机通知认证错误。

6.根据权利要求1所述的信息处理装置，所述信息处理装置还包括：

通知单元，其被配置为在与所述认证数据相对应的密码的有效性过期的情况下，向所述远程计算机通知认证错误。

7.根据权利要求1至6中任一项所述的信息处理装置，所述信息处理装置还包括：

控制台单元，其被配置为从用户接收认证数据，

其中，所述控制单元从所述存储单元获得与所述控制台单元接收的所述认证数据相对应的密码，并且在不将所获得的密码转换为哈希的情况下，使用所获得的密码来验证所述认证数据。

8.根据权利要求1所述的信息处理装置，所述信息处理装置还包括：

日志记录单元，其被配置为记录所述控制单元的认证结果。

9.一种信息处理装置的控制方法，所述信息处理装置能够根据多个协议中的协议来接收认证请求，所述控制方法包括：

存储步骤，将针对各用户的用户标识和密码以及针对各协议的计算方法存储到存储器中；

接收步骤，根据所述多个协议中的协议，从远程计算机接收认证请求，所述认证请求包括认证数据；

控制步骤：

(a)提供利用HTTP与HTTP客户端通信的HTTP服务器；

(b)提供利用SNMP与SNMP客户端通信的SNMP服务器；

(c)提供认证系统，该认证系统被配置为：

(i)从所述存储器获得与所述认证请求中包括的所述认证数据相对应的密码；

(ii)在所述接收步骤利用HTTP从HTTP客户端接收认证请求的情况下，从所述存储器中获得与HTTP相对应的计算方法；

(iii)在所述接收步骤利用SNMP从SNMP客户端接收认证请求的情况下，从所述存储器中获得与SNMP相对应的计算方法；

(iv)确定所获得的密码是否满足密码策略；

(v)在确定所获得的密码满足所述密码策略的情况下，根据所获得的计算方法，将所获得的密码转换为哈希，其中，基于所述哈希来验证所述认证数据。

10.一种存储程序的计算机可读存储介质，所述程序用于使处理器执行信息处理装置的控制方法，所述信息处理装置能够根据多个协议中的协议来接收认证请求，所述控制方法包括：

存储步骤，将针对各用户的用户标识和密码以及针对各协议的计算方法存储到存储器中；

接收步骤，根据所述多个协议中的协议，从远程计算机接收认证请求，所述认证请求包括认证数据；

控制步骤：

(a)提供利用HTTP与HTTP客户端通信的HTTP服务器；

(b)提供利用SNMP与SNMP客户端通信的SNMP服务器；

(c)提供认证系统，该认证系统被配置为：

(i)从所述存储器获得与所述认证请求中包括的所述认证数据相对应的密码；

(ii)在所述接收步骤利用HTTP从HTTP客户端接收认证请求的情况下，从所述存储器中获得与HTTP相对应的计算方法；

(iii)在所述接收步骤利用SNMP从SNMP客户端接收认证请求的情况下，从所述存储器

中获得与SNMP相对应的计算方法；

(iv)确定所获得的密码是否满足密码策略；

(v)在确定所获得的密码满足所述密码策略的情况下，根据所获得的计算方法，将所获得的密码转换为哈希，其中，基于所述哈希来验证所述认证数据。

信息处理装置及其控制方法

技术领域

[0001] 本发明涉及一种信息处理装置及其控制方法。

背景技术

[0002] 已知多功能外围设备(multi function peripheral,MFP)具有诸如用于扫描、打印以及通信的功能。MFP在主体上配备有操作面板,用户可以通过操作该操作面板来使用MFP的复印功能、扫描功能等。另外,近年来,MFP配备有诸如用于文件共享服务器、Web服务器等的功能,网络上的终端能够利用诸如服务器信息块(Server Message Block,SMB)、超文本传输协议(Hypertext Transfer Protocol,HTTP)等通信协议来访问MFP的服务器功能。另外,MFP配备有管理信息库(Management Information Base,MIB),网络上的终端能够利用被称为网络设备管理协议的SNMP v3(针对简单网络管理协议的第3版本(version3of the Simple Network Management Protocol,SNMP v3)的RFC3414(基于用户的安全模型(User-based Security Model,USM)))来访问MFP的MIB。

[0003] 此外,近年来,MPF配备有用于识别使用MFP的用户的用户认证机制。通常,在单个MFP配设有多种功能、通信协议等的情况下,MFP被配设有与各功能、通信协议等相对应的多种用户认证机制。例如,存在针对操作面板、针对网络服务器、针对文件共享服务器和针对SNMP v3的用户认证机制各不相同的情况。

[0004] 在单个MFP以这种方式配备有多种用户认证机制的情况下,存在下面的协调认证机制的技术。已知用于将主要用于针对操作面板的认证的用户信息与由SNMP v3的USM管理的用户信息进行关联和同步的方法(例如,日本特开第2006-195755号公报)。

[0005] 此外,近年来,认为与诸如个人计算机的网络终端类似的安全性对于MFP是必要的。为此,出现了配备有与密码策略(密码有效期、密码复杂度、锁定的设置/控制)、认证日志(认证成功/失败的日志记录)等相对应的用户认证机制的MFP。

[0006] 在多种用户认证机制存在于单个设备中的情况下,存在下面的问题。

[0007] -存在针对各用户认证机制登记了同一用户的账户,并且管理用户信息是麻烦的情况。为了使相同的账户能够用在多种用户认证机制且不会给用户带来负担,如同日本特开第2006-195755号公报中所述的发明,在用于执行用户认证的机制之间进行协作变得必要。

[0008] -从安全的角度来看,支持密码策略、认证日志等的用户认证机制与不支持密码策略、认证日志等的用户认证机制被混和在单个设备上不是优选的。为此,为了对多种用户认证机制提供等同的安全功能,存在制造设备的供应商必须承受开发成本的问题。

[0009] 在多种用户认证机制存在于单个设备中的情况下,由于上述问题,在通信协议、功能等不同的情况下,使用单个用户认证机制的配置通常是有利的。然而,各种通信协议的各用户认证方法中的规范不同,通过单个用户认证机制支持针对所有通信协议的用户认证相关的处理是困难的。例如,由于在SNMP v3的USM中定义的模式不仅利用用户的密码执行用户认证,还使用基于密码生成的密钥来执行加密处理、签名/伪造检测处理等,因此这种处

理是复杂的。

[0010] 另外，对于由RFC定义的和公知的协议，通常已公开实现该协议的软件模块或源代码。为此，实现服务器的供应商能够使用现有的软件模块或源代码等。然而，制造设备的供应商将现有软件模块和针对各协议而不同的源代码替换为对于设备的所有部分而言具有共同的用户认证的用户认证机制，将会花费非常大量的劳动和很多工时。另外，在协议中未定义关于密码策略检查、密码改变和认证日志记录的规范的情况下，现有已公布的软件模块和源代码也不具有这些功能。因此，制造设备的供应商必须在现有的软件模块和源代码中增加/实现诸如密码策略检查、密码改变和认证日志记录的功能，这存在花费非常大量的劳动和很多工时的问题。

发明内容

[0011] 本发明的一个方面在于消除使用上述传统技术的问题。

[0012] 本发明的特征在于提供一种能够使与用户认证相关的管理一体化的技术。

[0013] 本发明的第一方面提供了一种信息处理装置，其能够根据多个协议中的协议来接收认证请求，所述信息处理装置包括：存储单元，其被配置为存储针对各用户的用户标识和密码以及针对各协议的计算方法；接收单元，其被配置为根据所述多个协议中的协议从远程计算机接收认证请求，所述认证请求包括认证数据；

[0014] 控制单元，其被配置为：

[0015] (i)从所述存储单元获得与所述认证请求中包括的所述认证数据相对应的密码；

[0016] (ii)从所述存储单元获得与所述协议相对应的计算方法；

[0017] (iii)根据所获得的计算方法，将所获得的密码转换为哈希；以及

[0018] (iv)使用所述哈希来验证所述认证数据。

[0019] 本发明的第二方面提供了一种信息处理装置的控制方法，所述信息处理装置能够根据多个协议中的协议来接收认证请求，所述控制方法包括：存储步骤，将针对各用户的用户标识和密码以及针对各协议的计算方法存储到存储器中；接收步骤，根据所述多个协议中的协议，从远程计算机接收认证请求，所述认证请求包括认证数据；控制步骤：

[0020] (i)从所述存储器获得与所述认证请求中包括的所述认证数据相对应的密码；

[0021] (ii)从所述存储器中获得与所述协议相对应的计算方法；

[0022] (iii)根据所获得的计算方法，将所获得的密码转换为哈希；以及

[0023] (iv)使用所述哈希来验证所述认证数据。

[0024] 根据以下参照附图对示例性实施例的描述，本发明的其他特征将变得清楚。

附图说明

[0025] 包含在说明书中的且构成说明书一部分的附图示出了本发明的实施例，并与文字描述一起用于说明本发明的原理。

[0026] 图1描绘了示出根据本发明的第一实施例的网络配置的简化图。

[0027] 图2是用于示出根据第一实施例的MFP的硬件配置的框图。

[0028] 图3是用于说明根据第一实施例的MFP和PC的软件以及软件管理的数据的配置的框图。

[0029] 图4A至图4D描绘了用于示出根据第一实施例的在控制台单元上显示本地UI的用户界面的示例的图。

[0030] 图5A至图5F描绘了用于说明设置用户界面的图。

[0031] 图6描绘了用于示出根据第一实施例的用户数据库的数据结构的示例的图。

[0032] 图7A至图7C描绘了用于示出根据第一实施例的用户认证系统具有的API的示例的图。

[0033] 图8描绘了用于示出根据第一实施例的认证处理表的内容的示例的图。

[0034] 图9是用于描述根据第一实施例当在MFP中调用图7A的API时的用户认证系统的操作的流程图。

[0035] 图10A至图10D描绘了用于示出根据第一实施例当MFP与数据流一起执行用户认证时的软件模块的关系的图。

[0036] 图11描绘了用于示出根据本发明的第二实施例用户认证系统被构造为认证服务器的系统配置的示例的图。

[0037] 图12是用于示出根据第二实施例的MFP和认证服务器的软件配置的框图。

具体实施方式

[0038] 现在将参照附图在下文中详细描述本发明的实施例。应当理解，下面的实施例并不旨在限制本发明的权利要求的范围，针对根据下面实施例描述的方面的所有组合并不都是根据本发明的解决问题的手段所必须的。

[0039] 图1描绘了示出根据本发明第一实施例的网络的配置的简化图。

[0040] 作为根据本发明的信息处理装置的示例的MFP 101和个人计算机(PC)102连接到网络(LAN)100。MFP 101和PC 102能够经由LAN100执行相互通信。这里，MFP 101是配备有诸如用于扫描、打印和通信的多种功能的多功能外围设备。

[0041] 图2是用于示出根据第一实施例的MFP 101的硬件配置的框图。

[0042] 包括CPU 201的控制单元200控制MFP 101的整体操作。CPU 201根据ROM 202中存储的引导程序，将安装在HDD 204中的操作系统(OS)、控制程序等展开到RAM 203中，MFP 101在执行这些程序的CPU 201的控制下进行操作。RAM 203被用作CPU 201的临时存储区域(例如主存储器、工作区等)。HDD 204存储图像数据、各种程序等。控制台单元接口205连接控制台单元209和控制单元200。控制台单元209配备有作为触摸屏幕操作的显示单元。打印机接口206连接打印机单元210和控制单元200。将由打印机单元210打印的图像数据经由打印接口206从控制单元200传送到打印机单元210，并且通过打印机单元210将该图像数据打印在诸如片材的记录介质上。扫描器接口207连接扫描器单元211和控制单元200。扫描器单元211通过扫描原稿上的图像生成图像数据，并将该图像数据经由扫描器接口207提供给控制单元200。网络接口208将控制单元200(MFP 101)连接到LAN 100。网络接口208将图像数据、信息等发送到与LAN 100连接的外部装置(例如网络服务器等)，并从LAN 100上的外部装置接收各种信息。

[0043] 请注意，由于通过公知的通用计算机的硬件配置来构成PC 102，因此省略对PC 102的配置的说明。

[0044] 图3是用于说明根据第一实施例的MFP 101和PC 102的软件配置以及软件管理的

数据的配置的框图。请注意，图3的箭头符号代表在主用例中针对功能的调用方和调用目标。下面给出了针对软件功能和软件管理的数据的说明。

[0045] MFP 101的软件作为程序被存储在MFP 101的HDD 204中，通过将该程序展开到RAM 203中、CPU 201执行该程序来实现下文说明的功能。

[0046] 本地UI(用户界面)301在控制台单元209上显示用户可操作的用户界面，并向用户提供MFP 101具有的功能。

[0047] 图4A至图4D描绘了用于示出根据第一实施例的本地UI在控制台209上显示的用户界面的示例的图。

[0048] 例如，图4A描绘了用于示出用于对使用控制台单元209的用户进行认证的用户认证画面的示例的图。图4B表示用于请求在图4A的用户认证画面上认证的用户改变密码的改变密码画面的示例。图4C表示示出向使用控制台单元209的用户提供的功能的功能列表的菜单画面的示例。图4D表示用于使用MFP 101的箱(box)功能的用户界面画面的示例。例如，用户能够通过使用图4D的用户界面画面将从扫描器单元211获得的图像数据作为电子文档保存到HDD 204。或者，用户能够通过使用打印机单元210打印从HDD 204获得的电子文档。

[0049] PC 102配备有诸如Web浏览器317、文件管理工具319、MFP管理工具321等软件。

[0050] Web浏览器317配备有作为HTTP客户端318的Web浏览器317与MFP 101的HTTP服务器302通信的功能。HTTP服务器302在接收到来自Web浏览器317的请求时调用远程UI 303。远程UI 303将在超文本标记语言(HyperText Markup language，HTML)中定义的用户界面提供给操作Web浏览器317的用户。HTTP服务器302将从远程UI 303获得的HTML数据作为对来自Web浏览器317的请求的响应返回到Web浏览器317。

[0051] 文件管理工具319配备有作为SMB/CIFS客户端320的文件管理工具319与MFP 101的SMB/CIFS服务器304通信的功能。SMB/CIFS服务器304配备有用于处理NTLM(NT LAN管理器)认证协议的NTLM认证处理器305。当SMB/CIFS服务器304接收到来自文件管理工具319的诸如用于浏览文件、用于文件保存等请求时，调用文档管理服务306。文档管理服务306配备有用于执行浏览或更新HDD 204中保存的电子文档(具有诸如PDF、JPEG、PNG、DOC等文件扩展名的文件)以及用于执行新文件保存等功能。

[0052] MFP管理工具321配备有作为SNMP客户端322的功能，其用于通过访问MFP 101的SNMP服务器307来访问MFP 101配设的MIB 309。SNMP服务器307配备有用于处理由SNMP版本3的USM定义的用户认证协议的USM认证处理单元308。当SNMP服务器307接收到来自PC 102的MFP管理工具321的访问请求时，SNMP服务器307参照MIB 309中保存的数据并执行设置。

[0053] 用户认证系统310配备有用于对使用MFP 101的用户进行认证的机制。下文给出对用户认证系统310具有的功能的详情的说明。

[0054] 用户认证系统310配设有使管理MFP 101的用户执行与MFP 101的用户认证相关的设置的设置UI 311。与远程UI 303类似，设置UI 311能够被配置为以PC 102的Web浏览器317可使用的HTML中描述的用户界面。

[0055] 图5A至图5F描绘了用于说明设置UI 311的用户界面的图。

[0056] 图5A表示菜单画面的示例。当在图5A的画面上指定数字502至505表示的项目中的任一项目时，处理转换到用于指定的功能的画面。用户认证设置502是用于将MFP 101的用户认证功能设置为打开(ON)或关闭(OFF)的用户界面。当在图5A的画面上指定用户认证设

置502时，处理转换到图5B的画面。在图5B的画面上，用户能够将用户认证设置为打开或关闭，并且用户认证系统310将这里设置的内容作为认证设置312存储到HDD 204中。各软件模块能够通过访问认证设置312来参照用户认证的打开/关闭设置。在图5B的示例中，用户认证被设置为打开(用户认证是有效的)。

[0057] 通过在图5A的画面中指定用户账户管理503来显示图5C的画面。在图5C的画面中，用户能够登记并编辑用户名和用户权限。图5D的画面表示在图5C的画面中指定登记或编辑时显示的画面的示例。用户能够经由图5C和图5D所示的用户界面画面来执行用户账户的登记、编辑等。用户认证系统310通过将与利用图5D的画面登记的用户账户相关的信息存储在HDD 204的用户数据库313中来对该信息进行管理。在图5D的画面中将用户名“Alice”登记为管理员，而且登记了与该用户名相对应的密码。

[0058] 图6描绘了用于示出根据第一实施例的用户数据库313的数据结构的示例的图。

[0059] 这里，经由图5C和图5D所示的用户界面画面来登记用户名601、密码602以及权限603。密码最后更新日期/时间604表示经由图5D的画面登记或更新密码的日期和时间。

[0060] 通过在图5A的画面中指定密码策略设置504来显示图5E的画面。图5E表示用于设置与密码相关的策略的用户界面画面的示例。例如，“无有效期”、“30天”以及“90天”能够被选择作为密码有效期。另外，作为用于密码复杂度的设置，“3个字符或更多”(用于强制密码为3个字符或更多的设置)、“包含符号”(用于强制将符号包括在密码中的设置)等可以被选择是否有效/无效。用户认证系统310将经由图5E的画面而设置为密码策略设置314的项目存储在HDD 204中。

[0061] 通过在图5A的画面中指定认证日志管理505来显示图5F的画面。图5F表示用于管理认证结果的日志记录的用户界面画面。在图5F中，可以查看用户认证系统310记录到HDD 204中的认证日志316。在该画面中显示在认证日志316中登记的用户名、认证模式、执行认证的日期和时间以及认证结果(OK或NG(不好))。

[0062] 图7A至图7C描绘了用于示出根据第一实施例的用户认证系统310配设的API(应用程序界面)的示例的图。

[0063] 通过其他软件模块调用图7A的API 701，能够将请求用户认证的认证请求发送给用户认证系统310。用户认证系统310基于调用方702的信息通过参照认证处理表315来确定API 701的操作。

[0064] 图8描绘了用于示出根据第一实施例的认证处理表315的内容的示例的图。

[0065] 认证处理表315存储了调用方信息801、调用方改变密码功能的存在或不存在802、计算模式803以及认证处理类型804等的组合。在调用方信息801中，登记了作为认证请求的发送源的调用方通信协议。调用方改变密码功能的存在或不存在802表示调用方的软件模块是否包括密码改变功能。例如，由于对于控制与用户的界面的本地UI 301而言，调用方改变密码功能的存在或不存在802是“存在”，因此用于显示图4B的改变密码画面操作画面的功能也存在。

[0066] 同时，针对诸如HTTP、SMB/CIFS和SNMP v3的通信协议，还未定义用于改变密码的协议。为此，HTTP服务器302、SMB/CIFS服务器304和SNMP v3服务器307不具有用于请求密码改变的功能。计算模式803表示API 701使用以将密码转换为其他值的计算算法。“RAW”表示照原样使用密码而不对密码进行处理。“MD4”表示根据密码进行MD4(信息摘要算法4)摘要

(哈希值)的计算。“MD5”表示根据密码进行MD5(信息摘要算法5)摘要(哈希值)的计算。计算模式803不限于“MD4”、“MD5”等,可以是任何类型的计算模式,只要计算模式803是用户认证系统310能执行的已知计算模式即可。例如,公知的诸如密钥相关的哈希运算消息认证码(HMAC)(RFC 2104)、安全哈希算法(SHA)等计算算法。可以进行配置,使得用户认证系统310配设有作为计算模式的NTLM或SNMP版本3的USM的计算算法。认证处理类型804将API 701的操作分类为“验证”或“计算值返回”。“验证”表示API 701执行如下操作:根据从调用方接收到的认证数据704来验证由密码计算出的值并返回验证结果。“计算值返回”表示API 701执行如下操作:利用“计算模式”803所表示的算法根据密码计算出与密码不同的值并返回计算出的值(图7A的数字705所示的输出数据)。

[0067] 接下来,在下面给出对API 701返回的图7A中返回值706的意思的说明。

[0068] -SUCCESS

[0069] “SUCCESS”表示API 701的处理成功。在认证处理类型804是“验证”的情况下,“SUCCESS”表示用户认证处理成功。在认证处理类型804是“计算值返回”的情况下,从密码计算出的值被存储在图7A的输出数据705中并返回。

[0070] -SUCCESS_NEED_PWD_CHANGE

[0071] “SUCCESS_NEED_PWD_CHANGE”表示尽管API 701的处理成功,但由于密码不满足密码策略,因此用户必须改变密码。在有调用方密码改变功能的情况下,返回“SUCCESS_NEED_PWD_CHANGE”值。

[0072] -ERROR

[0073] “ERROR”表示暂停API 701的处理。在认证处理类型804是“验证”的情况下,“ERROR”表示用户认证处理失败。在认证处理类型804是“计算值返回”的情况下,不返回由密码计算出的值。

[0074] -ERROR_NEED_PWD_CHANGE

[0075] “ERROR_NEED_PWD_CHANGE”表示由于密码不满足密码策略,因此暂停API 701的处理。在没有调用方密码改变功能的情况下,返回“ERROR_NEED_PWD_CHANGE”值。

[0076] 对以上说明的API 701的具体描述仅为一个示例,本发明不限于该示例。例如,可以进行配置,以从API的调用方获得图8所示的认证处理表315的信息的部分或全部。在仅从调用方获得信息的部分的情况下,进行配置以从认证处理表315仅获得确定API的操作所需的信息。通过配置使认证处理表315可从外部进行编辑,使得能够灵活地支持API使用的软件模块的变更或增加。

[0077] 图7B示出了API的其他示例。图7B的API使用参数708,并使得图8所示的认证处理表315的所有信息将能够从调用方获得。这样,在进行配置以从调用方获得所有信息的情况下,用户认证系统310不必参照认证处理表315。另外,用于认证处理的API不必限于一个API,可以为预先设想的处理的各组合准备多个API。在下面的说明中,给出了使用图7A所示的API 701的说明,该API 701用作认证处理的API。

[0078] 图7C的API获得软件模块执行的用户认证的结果,并在认证日志316中记录日志。

[0079] 图9是用于描述根据第一实施例的当在MFP 101中软件模块调用图7A的API 701时的用户认证系统310的操作的流程图。请注意,执行该处理的程序在执行时被展开到RAM 203中,并在CPU 201的控制下执行。

[0080] 正在被调用的图7A所示的API 701以及接收用于与用户认证相关的处理的请求的用户认证系统310初始化该处理。首先，在步骤S901中，用户认证系统310从API 701的参数中获得调用方702的信息和用户名703(用户标识)。接下来，处理进行到步骤S902，用户认证系统310基于调用方702的信息参照认证处理表315来获得认证模式(改变密码功能存在或不存在、计算模式、认证处理类型)。接下来，处理进行到步骤S903，用户认证系统310确定在用户数据库313(图6)中是否登记了在步骤S901中获得的用户名。在登记了用户名的情况下，获得与用户名相关联登记的密码602和密码最新更新日期/时间604。同时，在在用户数据库313中未登记用户名并且在步骤S903中无法获得密码的情况下，由于用户认证系统310无法获得密码，因此在步骤S904中用户认证系统310确定认证失败，处理进行到步骤S914。在步骤S914中，用户认证系统310记录认证失败日志。然后，处理进行到步骤S915，用户认证系统310向API 701的调用方返回错误(ERROR)，并且处理结束。

[0081] 同时，在步骤S904中成功获得密码的情况下，处理进行到步骤S905，用户认证系统310参考密码策略设置314来确定获得的密码是否满足有效期、复杂度设置等。这里，在密码的有效期过期或不满足复杂度的情况下，处理进行到步骤S906，用户认证系统310还确定调用方改变密码功能的存在或不存在。这里，在存在改变密码功能的情况下，处理进行到步骤S907，并且处理继续。然而，在步骤S906中确定不存在改变密码功能的情况下，处理进行到步骤S914，记录认证失败日志，然后在步骤S915中，向API 701的调用方返回错误(ERROR_NEED_PWD_CHANGE)，并且处理结束。

[0082] 在步骤S905中，在用户认证系统310确定所获得的密码满足有效期和复杂度设置的情况下，或在步骤S906中，在确定存在调用方改变密码功能的情况下，处理进行到步骤S907。在步骤S907中，用户认证系统310参照认证处理表315来确认针对调用方设置的计算模式803。在这里的计算模式不是“RAW”的情况下(例如，“MD4”或“MD5”的情况)，处理进行到步骤S908，根据计算模式基于所获得的密码来执行计算处理。例如，这里根据MD4算法或MD5的算法来计算MD4摘要或MD5摘要。然后，处理进行到步骤S909，用户认证系统310参照认证处理表315来确认针对调用方设置的认证处理类型804。这里，在认证处理类型804是“计算值返回”的情况下，处理进行到步骤S910，用户认证系统310将计算值存储在输出数据705中，并返回处理成功(SUCCESS)，然后处理结束。另外，这里在步骤S905的密码策略检查失败的情况下，返回(SUCCESS_NEED_PWD_CHANGE)。

[0083] 同时，在步骤S909中，在用户认证系统310确定认证处理类型804是“验证”的情况下，处理进行到步骤S911，用户认证系统310根据在步骤S908中计算出的值来验证认证数据704(图7A)。在验证结果是认证数据704与计算出的值匹配的情况下，处理进行到步骤S912，用户认证系统310记录认证成功日志，处理进行到步骤S913，向API的调用方返回处理成功(SUCCESS)，并且处理结束。在此情况下，在步骤S905的密码策略检查为NG的情况下，返回(SUCCESS_NEED_PWD_CHANGE)。

[0084] 同时，在确定步骤S911中的验证结果是认证数据704并且计算值不匹配的情况下，然后确定认证失败，处理进行到步骤S914，用户认证系统310记录认证失败日志。然后，在步骤S915中，向API的调用方返回错误(ERROR)，并且处理结束。

[0085] 接下来，将给出对当MFP 101上的用户认证被设置为打开并且各种软件模块利用用户认证系统310执行用户认证时的操作示例的说明。这里，将给出对软件模块是本地UI

301、HTTP服务器302、SMB/CIFS服务器304以及SNMP服务器307的情况的说明。

[0086] 图10A至图10D描绘了用于示出根据第一实施例的当MFP 101与数据流一起执行用户认证时的软件模块的关系的图。

[0087] 图10A描绘了用于说明在本地UI 301利用用户认证系统310执行用户认证的情况的图。在图10A中，将用户认证画面显示在操作画面上，利用MFP 101为用户请求用户认证。在步骤S1001中，本地UI 301获得用户输入到图4A的用户认证画面中的用户名和密码。另外，在步骤S1002中，本地UI 301经由图7A的API 701将用户名和密码传输给用户认证系统310来作出用于认证处理的请求。这样，用户认证系统310参照认证处理表315执行密码策略检查、密码验证和认证日志记录，并在步骤S1003中利用处理结果来回复本地UI 301。

[0088] 这里，本地UI 301显示例如图4C的菜单画面，并在结果是成功(SUCCESS)的情况下允许用户使用MFP 101的功能。另一方面，在认证结果是NG(SUCCESS_NEED_PWD_CHANGE)的情况下，由于密码策略检查是NG，因此在操作画面上显示图4B的改变密码画面，用户请求改变密码。另外，在认证结果是错误(ERROR)的情况下，显示图4A的用户认证画面，请求用户重新输入认证信息。

[0089] 接下来，将参照图10B给出对MFP 101的HTTP服务器302的操作的说明。图10B描绘了用于说明HTTP服务器302利用用户认证系统310执行用户认证的情况的图。

[0090] 在步骤S1004中，HTTP服务器302从Web浏览器317接收包括HTTP摘要认证(RFC 2617)的HTML获得请求。这样，HTTP服务器302从数据包获得用户名和MD5摘要，然后，在步骤S1005中，经由API701向用户认证系统310作出用于认证处理的请求。这样，用户认证系统310参照认证处理表315执行密码策略检查、对MD5摘要计算进行验证的验证处理，执行认证日志的记录，然后在步骤S1006中，利用认证结果进行回复。在认证结果是成功(SUCCESS)的情况下，在步骤S1007中，HTTP服务器302向远程UI 303发送HTML获得请求。这样，远程UI 303从HTTP服务器302获得已认证的用户的信息，并根据用户执行HTML提供和访问控制。同时，在结果是失败(ERROR/ERROR_NEED_PWD_CHANGE)的情况下，HTTP服务器302向Web浏览器317通知错误。

[0091] 接下来，将参照图10C给出对MFP 101的SMB/CIFS服务器304的操作的说明。图10C描绘了用于说明SMB/CIFS服务器304利用用户认证系统310执行用户认证的情况的图。

[0092] 在步骤S1008中，SMB/CIFS服务器304从PC 102的文件管理工具319接收包括NTLM数据格式的认证数据的数据包。这样，SMB/CIFS服务器304从数据包中获得用户名，然后在步骤S1009中经由API 701向用户认证系统310作出用于认证处理的请求。这样，用户认证系统310参照认证处理表315执行密码策略检查和MD4摘要计算，然后在步骤S1010中连同MD4摘要一起返回处理结果。这样，在SMB/CIFS服务器304中，NTLM认证处理器305利用从用户认证系统310获得的MD4摘要和从数据包获得的NTLM认证数据执行NTLM认证处理。然后，SMB/CIFS服务器304获得由NTLM认证处理器305产生的认证结果，在步骤S1011中，经由图7C的API向用户认证系统310通知用户名和认证结果。

[0093] 这里，在用户认证成功的情况下，之后SMB/CIFS服务器304允许从PC 102的文件管理工具319到文档管理服务306的访问。在步骤S1012中，文档管理服务306从SMB/CIFS服务器304获得用户信息，并根据用户执行服务提供、访问控制等。同时，在用户认证失败的情况下，SMB/CIFS服务器304向PC 102的文件管理工具319通知错误。

[0094] 接下来，将参照图10D给出对MFP 101的SNMP服务器307的操作的说明。图10D描绘了用于说明SNMP服务器307利用用户认证系统310执行用户认证的情况的图。

[0095] 在步骤S1013中，SNMP服务器307从PC 102的MFP管理工具321接收包含根据SNMP v3的USM(RFC3414)的认证数据的数据包。然后，SNMP服务器307从该数据包获得用户名，并在步骤S1014中通过API701向用户认证系统310作出用于认证处理的请求。这样，用户认证系统310参照认证处理表315执行密码策略检查和MD5摘要计算，然后在步骤S1015中，连同MD5摘要一起返回处理结果。这样，在SNMP服务器307中，USM认证处理单元308利用从用户认证系统310获得的MD4摘要和从数据包获得的NTLM认证数据执行NTLM认证处理。然后，SNMP服务器307获得USM认证处理单元308的认证结果，并在步骤S1016中，经由图7C的API向用户认证系统310通知用户名和认证结果。在用户认证成功的情况下，在步骤S1017中，SNMP服务器307执行MFP管理工具321请求的对MIB 309的访问。SNMP服务器307根据用户执行对访问MIB 309的访问控制。同时，在用户认证失败的情况下，SNMP服务器307向PC 102的MFP管理工具321通知错误。

[0096] 通过第一实施例，如上所述，由于通过单个用户认证系统310来实现MFP 101的用户认证机制，因此，可以降低与用户认证相关的设置的管理负担和用户账户的管理负担。

[0097] 另外，通过第一实施例，由于对所有访问路径提供了密码安全策略和认证日志打印功能，因此，可以对所有访问路径适用同等的安全功能。

[0098] 另外，使用MFP 101的用户认证系统310的软件模块来支持密码安全策略、认证日志记录等并不总是必须的，因此，存在不会引起现有的软件模块或源代码的重建成本的优点。

[0099] 此外，通过第一实施例，用户认证系统310和使用用户认证系统310的软件模块可以执行与用户认证相关的分配处理。为此，存在如下效果：在最大限度使用现有的软件模块和源代码时，能够配置集成了与用户认证相关的管理的设备。

[0100] [第二实施例]

[0101] 之前描述的用户认证系统310并不必须在MFP 101的内部，可以进行配置使用户认证系统310是网络上的独立节点。

[0102] 图11描绘了用于示出根据本发明的第二实施例的用户认证系统被构造为认证服务器的系统配置的示例的图。

[0103] 这里，MFP 1101、PC 1102和认证服务器1103经由LAN 1100连接。请注意，由于MFP 1101和PC 1102的硬件配置与根据之前描述的第一实施例的MFP 101和PC 102的硬件配置相同，因此，将省略对它们的说明。

[0104] 图12是用于示出根据第二实施例的MFP 1101和认证服务器1103的软件配置的框图。由于PC 1102的配置与之前描述的第一实施例的PC 102的配置相同，因此省略说明。请注意，与之前图3描述的相同部分由相同的附图标记表示，省略对它们的说明。另外，由于由用户认证服务器1103的附图标记1211至1216所示的布置具有与之前图3描述的附图标记311至316所示的布置相同的功能，因此，省略对它们的说明。

[0105] MFP 1101配备有用于与认证服务器1103通信的代理1201。认证服务器1103配备有用户认证系统1202。MFP 1101和认证服务器1103能够通过预先交换将用于通信的加密密钥来建立信任关系。可以利用PKI技术来交换第三方发布的证书，例如客户端证书、服务器证

书等。

[0106] 代理1201配设有API(图7A或图7C中的数字701等)相当于用户认证系统1202具有的API。当从其他软件模块调用API时,代理1201经由网络上的通信,通过调用用户认证系统1202的API来获得处理结果。由于这里网络中流过的信息必须保密,因此,利用预先交换的密钥执行加密。这样,通过将用户认证系统1202配置为网络上的独立节点(认证服务器),能够提供由多个MFP可使用的用户认证系统1202。

[0107] 如上所述,通过该实施例能够获得下面的效果。

[0108] -通过将可实现的用户认证机制作为单个用户认证系统,能够降低与用户认证相关的设置的管理负担和用户账户的管理负担。

[0109] -利用该用户认证系统,可以将同一用户认证机制应用于设备的所有访问路径。

[0110] -可以重复使用现有的软件模块和源代码,并且能够配置使用相对较少的劳动和工时就能够执行用户认证的设备。

[0111] 本发明的实施例还可以通过读出并执行记录在存储介质(例如,非暂时性计算机可读存储介质)上的用于执行本发明的上述实施例的一个或更多个的功能的计算机可执行指令的系统或装置的计算机来实现,以及通过由系统或装置的计算机通过例如从存储介质读出并执行用于执行上述实施例的一个或更多个的功能的计算机可执行指令来执行的方法来实现。计算机可以包括中央处理单元(CPU)、微处理单元(MPU)、或其他电路的一个或多个,并且可以包括单独的计算机或单独的计算机处理器的网络。例如可以从网络或者存储介质向计算机提供计算机可执行指令。存储介质可以包括例如硬盘、随机存取存储器(RAM)、只读存储器(ROM)、分布式计算系统的存储器、光盘(诸如压缩光盘(CD)、数字通用光盘(DVD)、或蓝光盘(BD)™)、闪存设备、存储卡等的一个或多个。

[0112] 虽然参照示例性实施例对本发明进行了描述,但是应当理解,本发明并不限于所公开的示例性实施例。应当对所附权利要求的范围给予最宽的解释,以使其涵盖所有这些变型例以及等同的结构和功能。

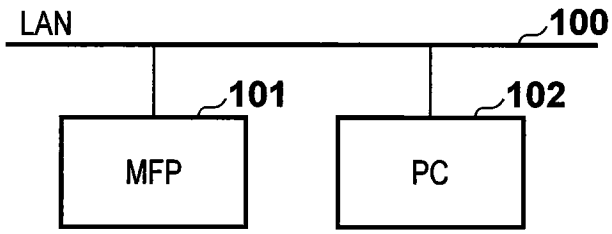

LAN
100
101
102
MFP
PC

图1

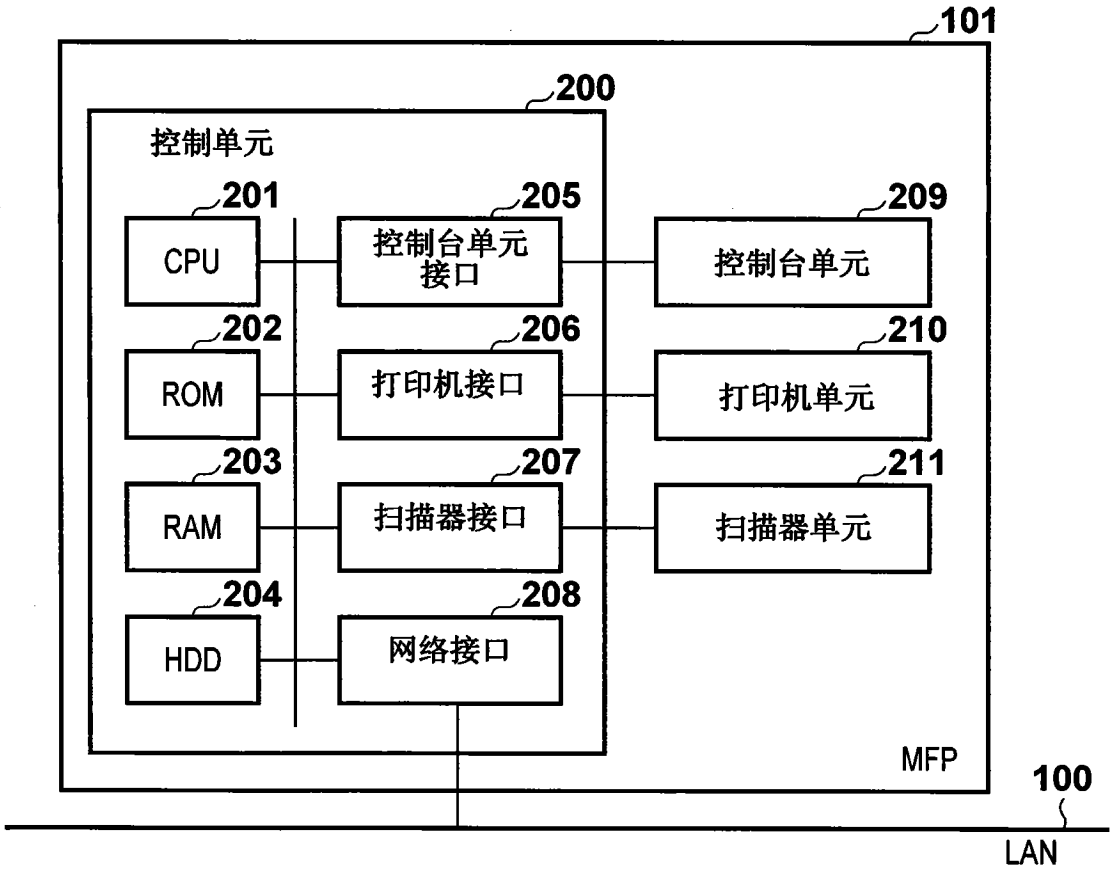

101
200
控制单元
201
CPU
205
控制台单元接口
209
控制台单元
202
ROM
206
打印机接口
210
打印机单元
203
RAM
207
扫描器接口
211
扫描器单元
204
HDD
208
网络接口
MFP
100
LAN

图2

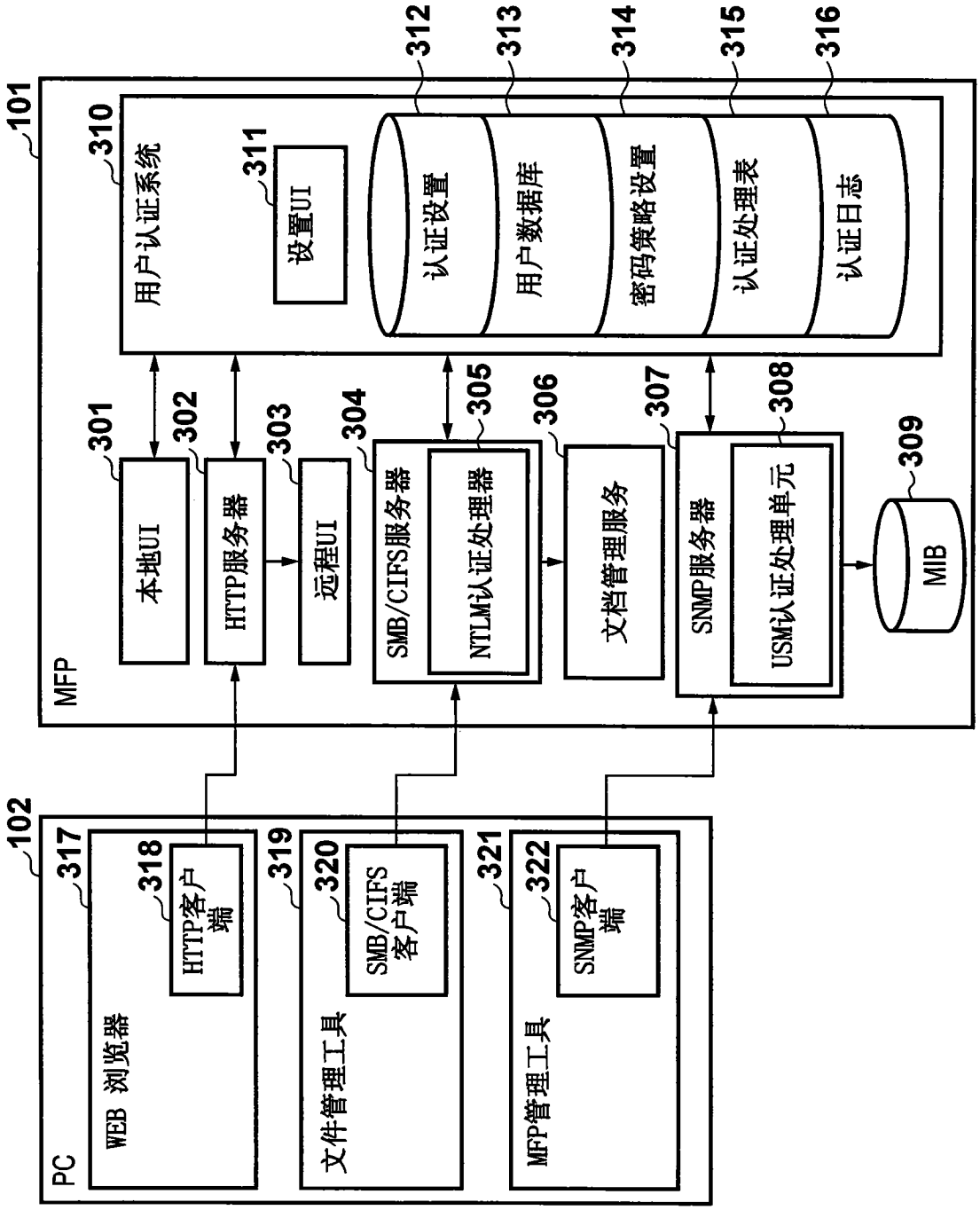

101
MFP
310
用户认证系统
311
设置UI
312
认证设置
313
用户数据库
314
密码策略设置
315
认证处理表
316
认证日志
301
本地UI
302
HTTP服务器
303
远程UI
304
SMB/CIFS服务器
305
NTLM认证处理器
306
文档管理服务
307
SNMP服务器
308
USM认证处理单元
309
MIB
102
PC
317
WEB 浏览器
318
HTTP客户端
319
文件管理工具
320
SMB/CIFS客户端
321
MFP管理工具
322
SNMP客户端

图3

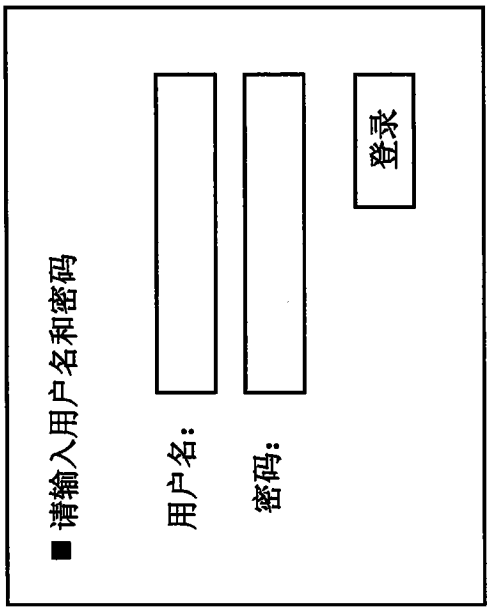


图4A

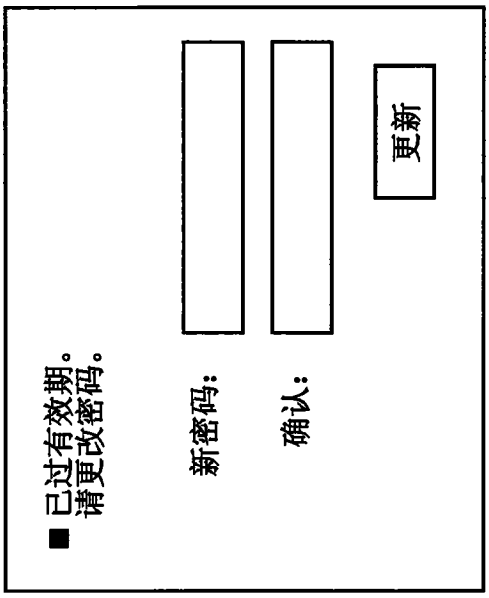


图4B

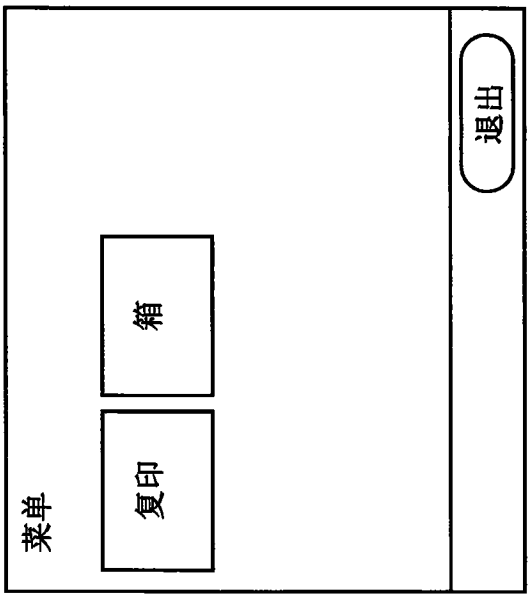


图4C

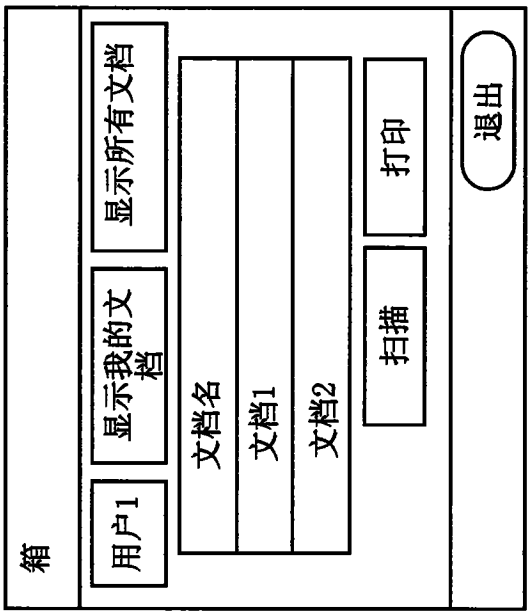


图4D

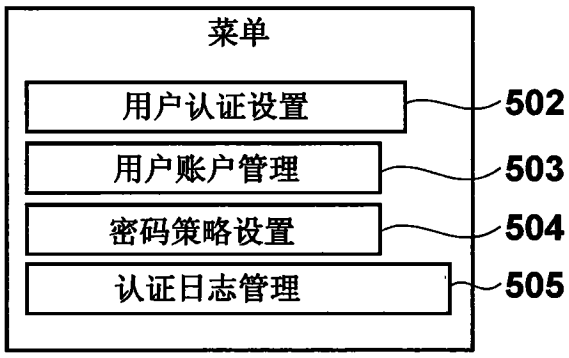

菜单
用户认证设置
502
用户账户管理
503
密码策略设置
504
认证日志管理
505

图5A

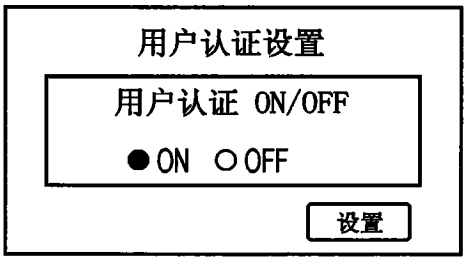

用户认证设置
用户认证 ON/OFF
● ON ○ OFF
设置

图5B

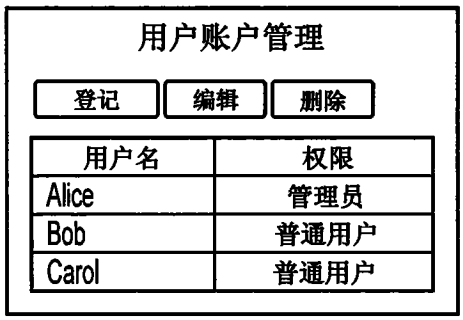

用户账户管理
登记
编辑
删除
用户名
权限
Alice
管理员
Bob
普通用户
Carol
普通用户

图5C

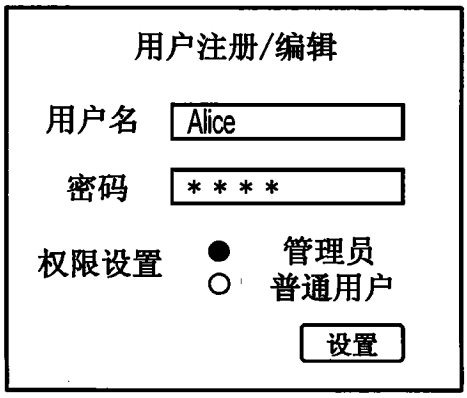


图5D

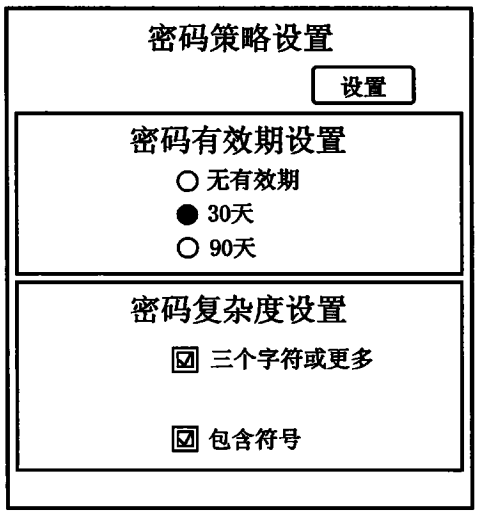
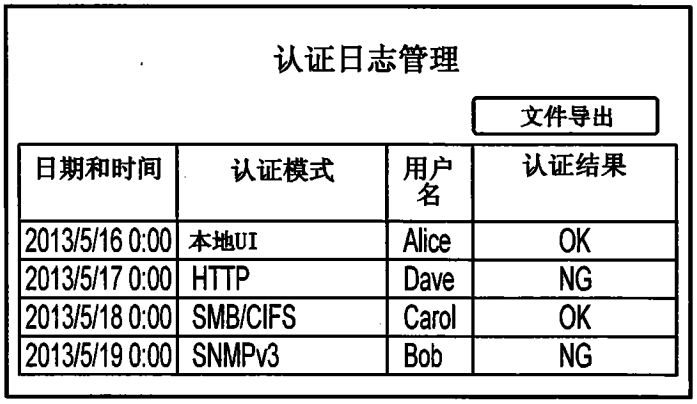


图5E



日期和时间	认证模式	用户名	认证结果
2013/5/16 0:00	本地UI	Alice	OK
2013/5/17 0:00	HTTP	Dave	NG
2013/5/18 0:00	SMB/CIFS	Carol	OK
2013/5/19 0:00	SNMPv3	Bob	NG

图5F

601 用户名	602 密码	603 权限	604 密码最新更新日期/时间
Alice	****	管理员	2013/2/1 10:00
Bob	****	普通用户	2013/2/2 10:00
Carol	****	普通用户	2013/2/3 10:00

图6

701

```
Result UserAuthProcessing(
   String Caller;          //调用方～702
   String userName,        //用户名～703
   Binary inputData,       //输入数据（认证数据）～704
   Binary outputData)      //输出数据（通过计算模式计算出的值）～705
RETURN VALUE               706
   SUCCESS                                  //成功处理
   SUCCESS_NEED_PWD_CHANGE                  //成功处理-需更改密码

   ERROR                                    //失败处理
   ERROR_NEED_PWD_CHANGE                    //失败处理-需要更改密码
```

图7A

```
Struct AuthMethod {
  String Caller;              //调用方
  String Algorithm;           //计算模式
  String ProcessingType;      //认证处理类型
  Bool PwdChangeable;         // 存在或不存在更改密码功能
}
Result UserAuthProcessingEx(
        AuthMethod authMethod,  //认证模式
        String userName,        // 用户名
        Binary inputData,       // 输入数据（认证数据）
        Binary outputData)      //输出数据（计算结果，认证结果，权限信息）等
```

708

图7B

```
void WriteAuthenticationLog(String userName,Result code);
```

图7C

801 调用方	802 存在或不存在调用方更改密码功能	803 计算模式	804 认证处理类型
本地UI	存在	RAW	验证
HTTP	不存在	MD5	验证
SMB/CIFS	不存在	MD4	返回计算值
SNMPv3	不存在	MD5	返回计算值

图8

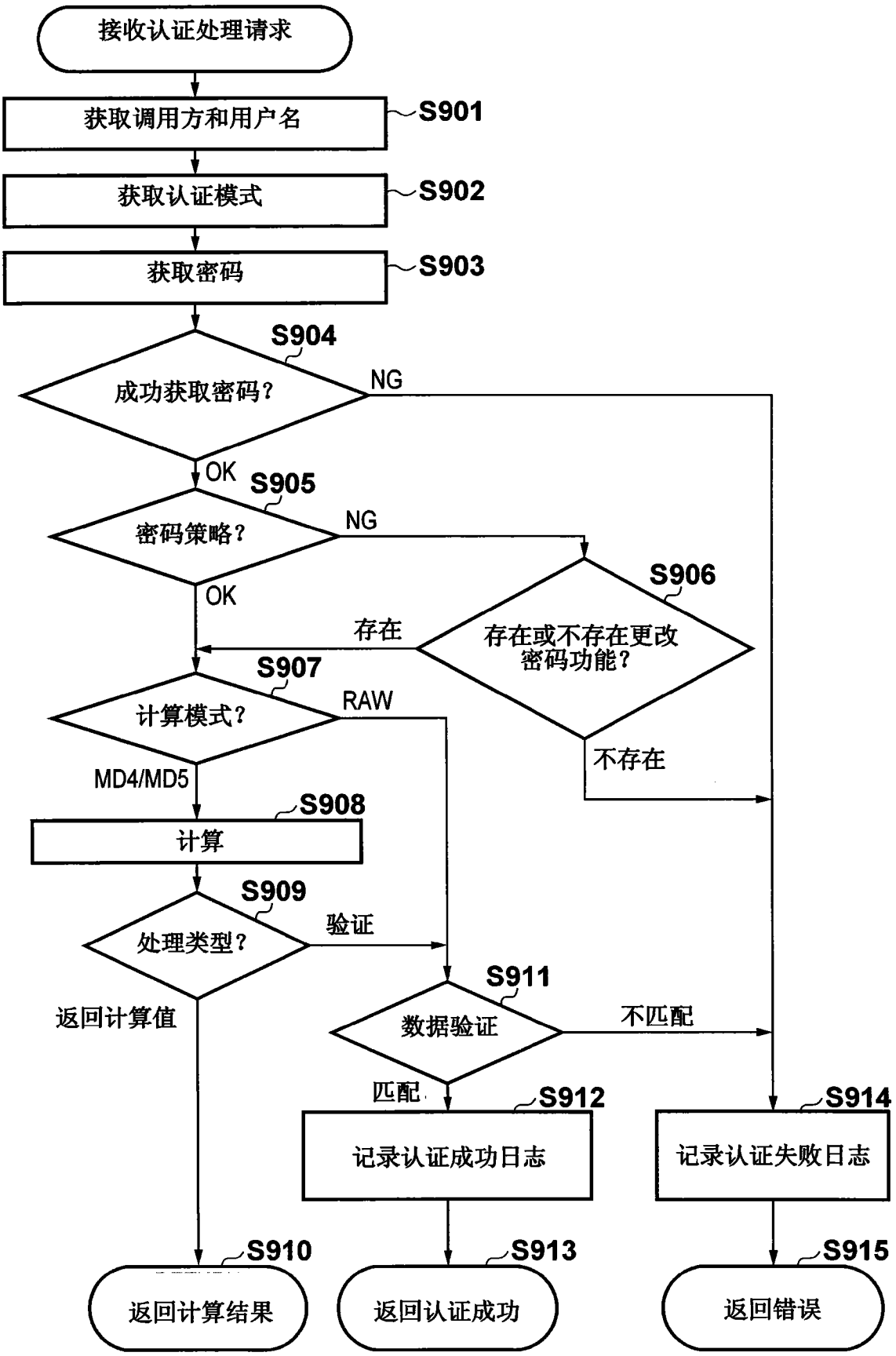

接收认证处理请求
获取调用方和用户名
S901
获取认证模式
S902
获取密码
S903
S904
成功获取密码？
NG
OK
S905
密码策略？
NG
OK
S906
存在或不存在更改密码功能？
存在
不存在
S907
计算模式？
RAW
MD4/MD5
S908
计算
S909
处理类型？
验证
返回计算值
S911
数据验证
不匹配
匹配
S912
记录认证成功日志
S914
记录认证失败日志
S910
返回计算结果
S913
返回认证成功
S915
返回错误

图9

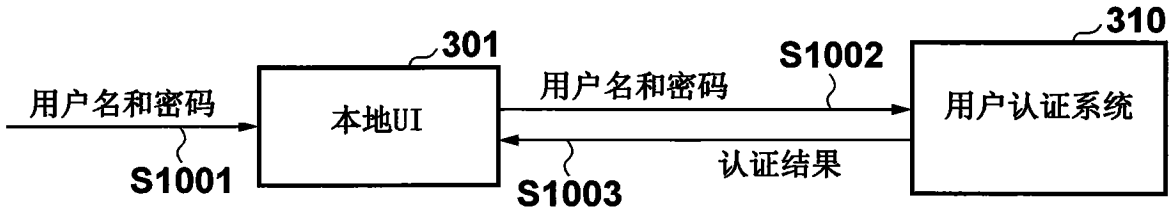


图10A

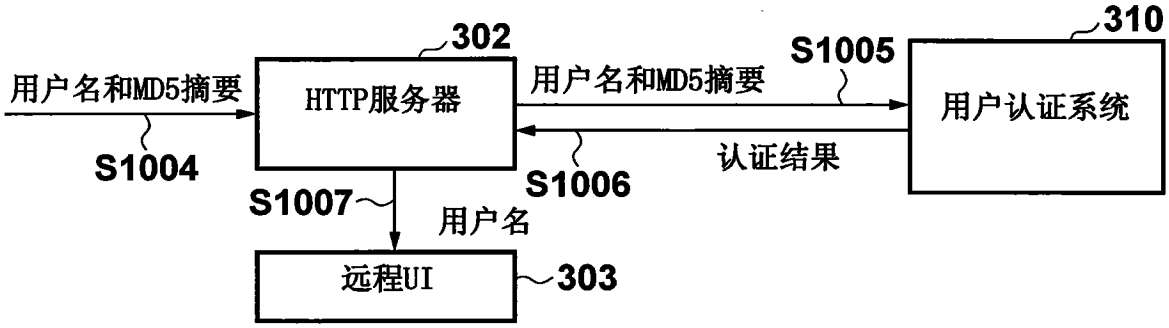


图10B

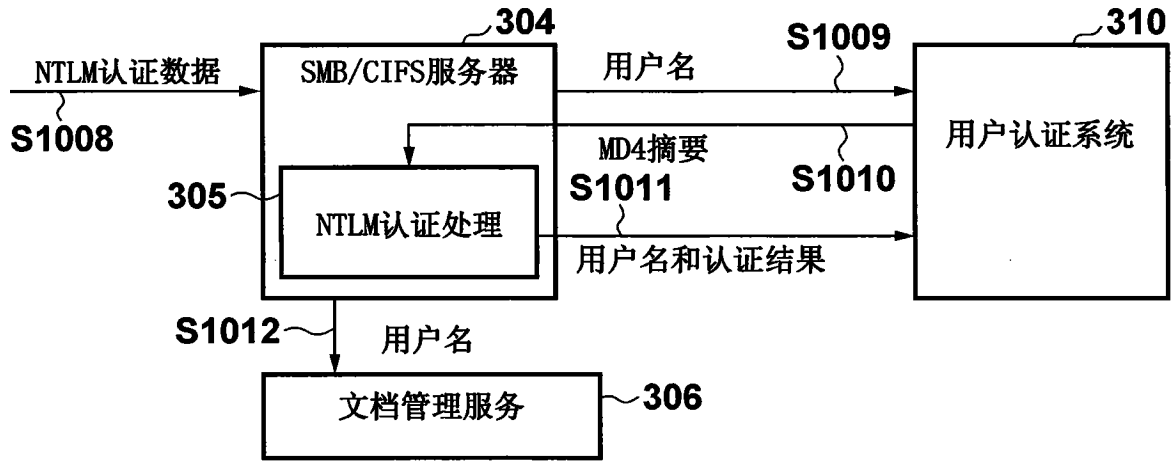


图10C

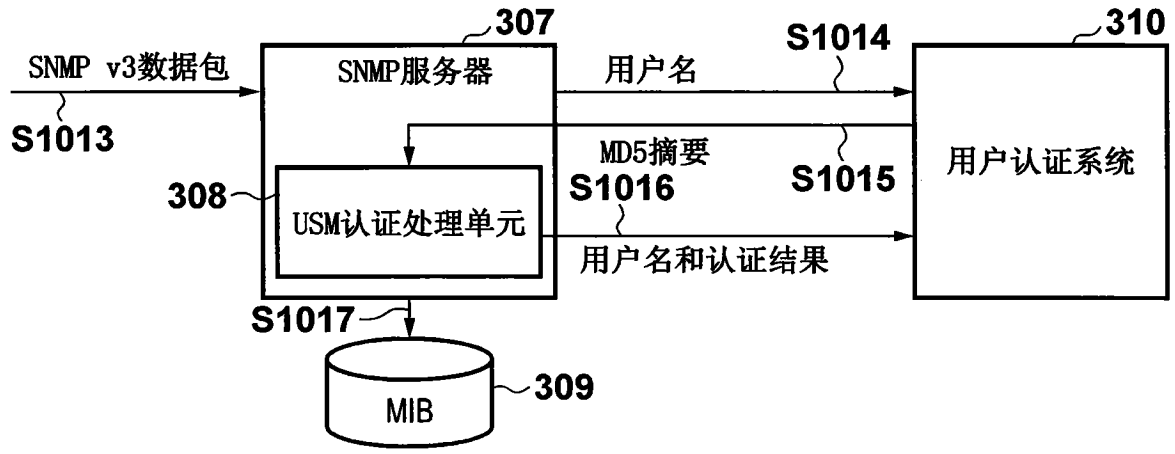

307
SNMP v3数据包
SNMP服务器
S1013
用户名
S1014
310
用户认证系统
MD5摘要
S1015
S1016
308
USM认证处理单元
用户名和认证结果
S1017
MIB
309

图10D

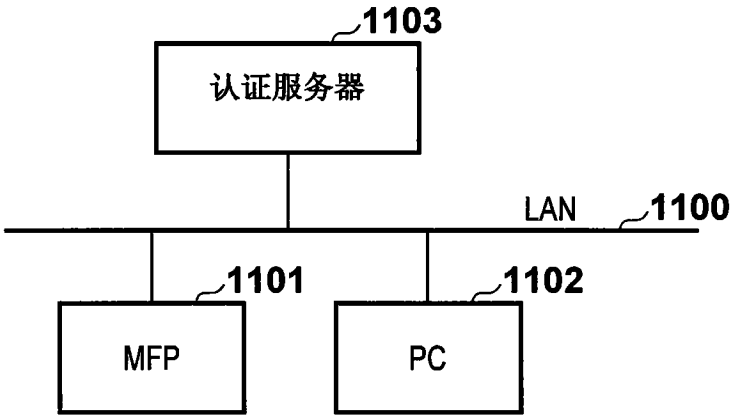

1103
认证服务器
LAN
1100
1101
1102
MFP
PC

图11

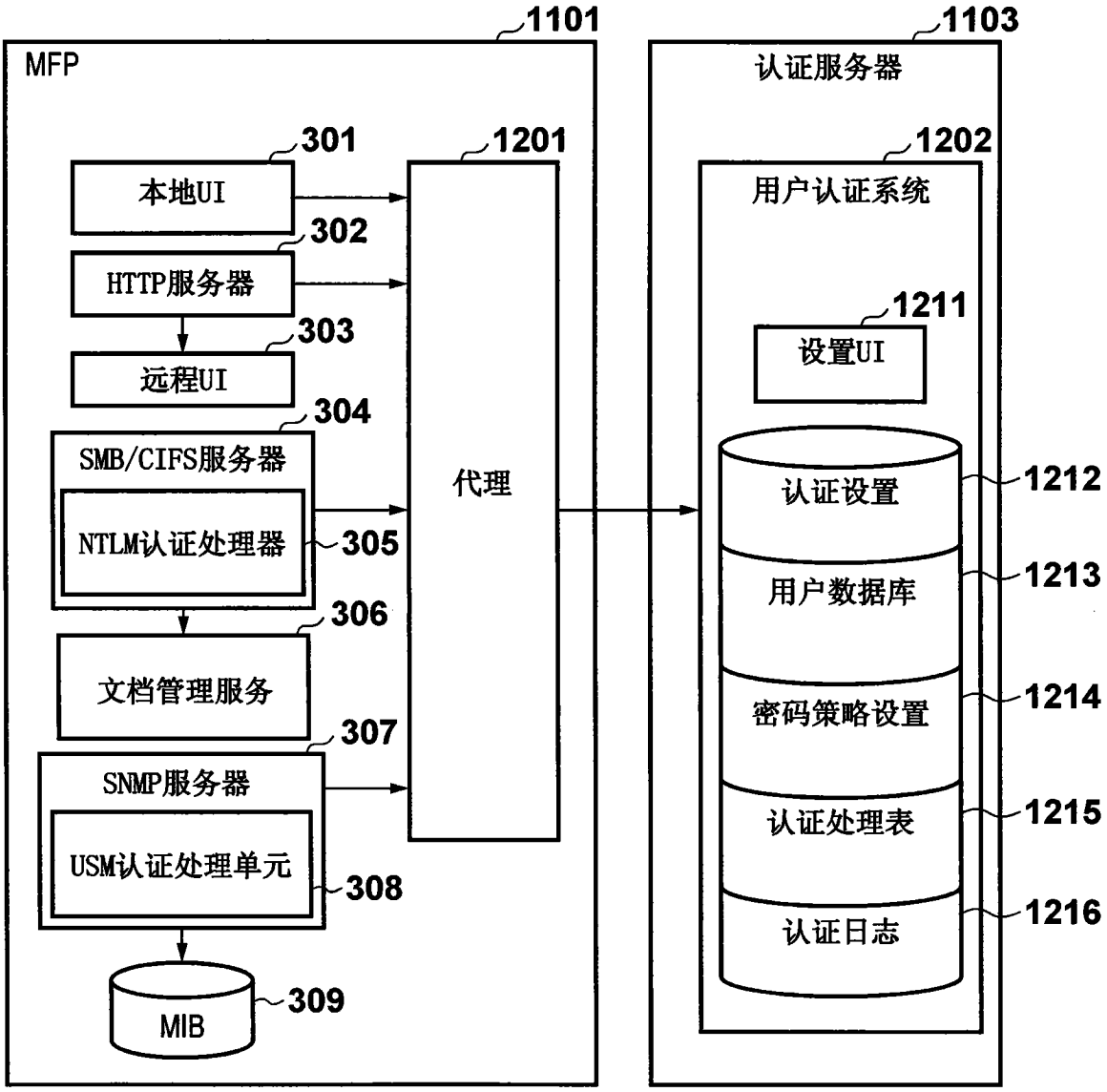

1101
MFP
301
本地UI
302
HTTP服务器
303
远程UI
304
SMB/CIFS服务器
NTLM认证处理器
305
306
文档管理服务
307
SNMP服务器
USM认证处理单元
308
MIB
309
1201
代理
1103
认证服务器
1202
用户认证系统
1211
设置UI
认证设置
1212
用户数据库
1213
密码策略设置
1214
认证处理表
1215
认证日志
1216

图12