

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.

H04L 29/06 (2006.01)



[12] 发明专利说明书

专利号 ZL 200410094735.1

[45] 授权公告日 2009 年 9 月 9 日

[11] 授权公告号 CN 100539583C

[22] 申请日 2004.11.17

[21] 申请号 200410094735.1

[30] 优先权

[32] 2003.11.17 [33] JP [31] 386985/2003

[73] 专利权人 佳能株式会社

地址 日本东京

[72] 发明人 利根川信行

[56] 参考文献

US2002/0104026A1 2002.8.1

JP11-234496A 1999.8.27

CN1430388A 2003.7.16

审查员 李 俊

[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

代理人 吴丽丽

权利要求书 3 页 说明书 20 页 附图 12 页

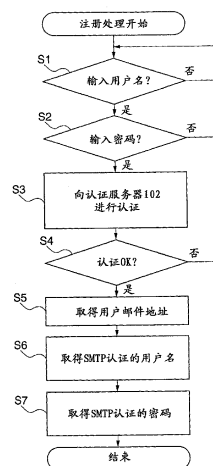
[54] 发明名称

通信装置, 电子邮件发送方法以及电子邮件
发送程序

[57] 摘要

本发明提供一种通信装置、电子邮件发送方法及电子邮件发送程序, 能够谋求提高使用发送协议将电子邮件发送给发送目的地的邮件地址时的安全性, 而不会使操作性降低。为此, MFP(100) 通过网络连接到认证服务器(102) 和邮件服务器(120), 并经由邮件服务器(120) 按照 SMTP 来发送电子邮件。用户名和密码被输入到用户名输入画面。MFP(100) 请求认证服务器(102) 对所输入的用户名和密码进行认证。在用户名和密码被认证的情况下, MFP(100) 从认证服务器(102) 取得对应于上述经过认证的用户名和密码的、遵照 SMTP 的电子邮件地址(232)、SMTP 认证用户名(233) 以及 SMTP 认证密码(234)。MFP(100) 向邮件服务器 103 要求按照 SMTP 所取得的 SMTP 认证用户名(232) 和

SMTP 认证密码(234) 的认证。在 SMTP 认证用户名(232) 和 SMTP 认证密码(234) 被认证时, MFP(100) 按照 SMTP 将电子邮件发送给邮件服务器(103)。



1. 一种通信装置，经由网络连接到认证装置和邮件分发装置，并经由上述邮件分发装置按照预定的发送协议发送电子邮件，该通信装置的特征在于包括：

输入用户信息的输入装置；

向上述认证装置请求该被输入的用户信息的认证的用户认证请求装置；

在上述用户信息被认证了的情况下，从上述认证装置取得与上述经过认证的用户信息对应的上述发送协议的认证信息的认证信息取得装置；

按照上述发送协议向上述邮件分发装置请求该所取得的认证信息的认证的发送认证请求装置；以及

在上述认证信息被认证的情况下，遵照上述发送协议将电子邮件发送给上述邮件分发装置的发送装置，

上述认证信息是对应于上述用户信息的 SMTP 认证的用户名和密码。

2. 根据权利要求 1 所述的通信装置，其特征在于：

上述认证装置具备保存与上述用户信息对应的电子邮件地址和与上述用户信息对应的上述发送协议的认证信息的保存装置，上述认证信息取得装置取得保存在上述保存装置中的电子邮件地址和上述认证信息。

3. 一种通信装置，经由网络连接到邮件分发装置，并经由上述邮件分发装置按照预定的发送协议发送电子邮件，该通信装置的特征在于包括：

保存上述发送协议的认证信息的认证信息保存装置；

输入用户信息的输入装置；

请求该被输入的用户信息的认证的用户认证请求装置；

在上述用户信息被认证了的情况下，从上述认证信息保存装置取

得与上述经过认证的用户信息对应的上述发送协议的认证信息的认证信息取得装置；

按照上述发送协议向上述邮件分发装置请求该所取得的认证信息的认证的发送认证请求装置；以及

在上述认证信息被认证的情况下，遵照上述发送协议将电子邮件发送给上述邮件分发装置的发送装置，

上述认证信息是对应于上述用户信息的 SMTP 认证的用户名和密码。

4. 根据权利要求3所述的通信装置，其特征在于：

上述认证信息保存装置保存与上述用户信息对应的电子邮件地址和与上述用户信息对应的上述发送协议的认证信息，上述认证信息取得装置取得保存在上述认证信息保存装置中的电子邮件地址和上述认证信息。

5. 一种在通信装置中执行的电子邮件发送方法，所述通信装置经由网络连接到认证装置和邮件分发装置，并按照发送协议经由上述邮件分发装置发送电子邮件，该电子邮件发送方法的特征在于包括：

输入用户信息的输入步骤；

向上述认证装置请求该被输入的用户信息的认证的用户认证请求步骤；

在上述用户信息被认证了的情况下，从上述认证装置取得与上述经过认证的用户信息对应的上述发送协议的认证信息的认证信息取得步骤；

按照上述发送协议向上述邮件分发装置请求该所取得的认证信息的认证的发送认证请求步骤；以及

在上述认证信息被认证的情况下，遵照上述发送协议将电子邮件发送给上述邮件分发装置的发送步骤，

上述认证信息是对应于上述用户信息的 SMTP 认证的用户名和密码。

6. 一种在通信装置中执行的电子邮件发送方法，所述通信装置

经由网络连接到邮件分发装置，并按照发送协议经由上述邮件分发装置发送电子邮件，该电子邮件发送方法的特征在于包括：

输入用户信息的输入步骤；

请求该被输入的用户信息的认证的用户认证请求步骤；

按每个用户保持按照上述发送协议的认证信息的保持步骤；

从在上述保持步骤中所保持的认证信息之中取得与上述经过认证了的用户信息对应的上述发送协议的认证信息的认证信息取得步骤；

按照上述发送协议向上述邮件分发装置请求该所取得的认证信息的认证的发送认证请求步骤；以及

在上述认证信息被认证了的情况下，遵照上述发送协议将电子邮件发送给上述邮件分发装置的发送步骤，

上述认证信息是对应于上述用户信息的 SMTP 认证的用户名和密码。

通信装置，电子邮件发送方法 以及电子邮件发送程序

技术领域

本发明涉及遵照预定的发送协议发送电子邮件的通信装置、电子邮件发送方法以及电子邮件发送程序。

背景技术

近年来伴随着计算机的普及以及信息的网络化，通过网络收发字符信息的电子邮件已经普及。在电子邮件中，除了作为字符信息的邮件正文以外，还可附加各种形式的文件。例如，通过在附件中添付TIFF（标签图像文件格式：Tag Image File Format）形式的文件，来进行图像收发的互联网传真已经普及。

这里，互联网FAX（下面称为IFAX）是指发送机将通过扫描器所读取的图像数据变换成TIFF形式进行发送，接收机对接收到的TIFF形式的图像数据进行打印之类的发送机和接收机间的通信技术。此时，为了使进行通信的TIFF形式的图像数据在多个设备上保持互换性，由作为对因特网技术进行标准化的组织的IETF（因特网工程任务组：Interne Engineering Task Force），在技术规范RFC（请求评论：Request for Comments）2301中详细地进行了规定。

另外，在利用简单邮件传输协议（SMTP）将电子邮件发送给发送目的地的邮件地址时，通过由邮件服务器进行用户认证后进行邮件发送，来防止非法对伪造了邮件地址的电子邮件进行转接的情况之类的、涉及SMTP认证的技术在技术规范RFC2554进行了规定。作为进行用户认证后发送电子邮件的现有技术，例如，可列举在日本专利公开特开平11-234496号公报中所记载的内容。

另外，本申请承受人已经提出了以下方法：即在发送电子邮件前

预先注册到认证服务器，在由认证服务器认证了用户名和密码的情况下，取得对应于此经过认证的用户名的电子邮件地址，将此所取得的电子邮件地址作为发送方的地址将电子邮件发送给发送目的地的邮件地址的方法（日本专利公开特开2003-066857号）。

但是，即便是上述提案的电子邮件发送方法也希望改善以下揭示的问题。

即，当在使用SMTP认证发送电子邮件时，作为在SMTP认证中所使用的用户名和密码，使用了设备（MFP等通信装置）固有的设定值（即设备固有的用户名和密码）的情况下，在该设备中作为发送日志，使注册到认证服务器的用户名的日志保留下来，但在邮件服务器中却仅保留识别固有的用户名的日志。其结果，设备保有的日志和邮件服务器保有的日志有时就不同，难以将这些日志相互对应起来。从而，确定实际的发送者是困难的。另外，还有知道设备固有的用户名和密码的人用他人的邮件地址进行发送操作的可能性。

相对于此，在使用SMTP认证发送电子邮件时，不使用设备固有的用户和密码，而每次输入在SMTP认证中所使用的用户名和密码，由此上述问题就得以回避，但在此情况下，就有操作性降低之类的新问题。

发明内容

本发明的目的是提供一种通信装置、电子邮件发送方法以及电子邮件发送程序，能够谋求提高在使用发送协议将电子邮件发送给发送目的地的邮件地址时的安全性，而不会使操作性降低。

为了达到上述目的，本发明的第1技术方案提供一种通信装置，经由网络连接到认证装置和邮件分发装置，并经由上述邮件分发装置按照预定的发送协议发送电子邮件，包括：输入用户信息的输入装置；向上述认证装置请求该被输入的用户信息的认证的用户认证请求装置；在上述用户信息被认证的情况下，从上述认证装置取得对应于上述经过认证的用户信息的上述发送协议的认证信息的认证信息取得装

置；遵照上述发送协议向上述邮件分发装置请求该所取得的认证信息的认证的发送认证请求装置；以及在上述认证信息被认证的情况下，遵照上述发送协议将电子邮件发送给上述邮件分发装置的发送装置。

根据这样的构成，向认证装置请求所输入的用户信息的认证；在用户信息被认证的情况下，从认证装置取得对应于该经过认证的用户信息的发送协议的认证信息；遵照发送协议向邮件分发装置请求该所取得的认证信息的认证；在认证信息被认证的情况下，遵照发送协议将电子邮件发送给邮件分发装置，所以能够谋求提高在使用发送协议将电子邮件发送给发送目的地的邮件地址时的安全性，而不会使操作性降低。

最好是，上述认证装置具备保存对应于上述用户信息的电子邮件地址和对应于上述用户信息的上述发送协议的认证信息的保存装置，上述认证信息取得装置取得保存在上述保存装置中的电子邮件地址和上述认证信息。

根据此优选技术方案的构成，在用户信息被认证的情况下，从认证装置取得对应于该经过认证的用户信息的电子邮件地址，防止假冒发送的电子邮件地址等非法电子邮件转接就成为可能。

最好是，上述认证信息是对应于上述用户信息的 SMTP 认证的用户名和密码。

为了达到上述目的，本发明的第 2 技术方案提供一种通信装置，经由网络连接到邮件分发装置，并经由上述邮件分发装置按照预定的发送协议发送电子邮件，包括：保存上述发送协议的认证信息的认证信息保存装置；输入用户信息的输入装置；请求该被输入的用户信息的认证的用户认证请求装置；在上述用户信息被认证的情况下，从上述认证信息保存装置取得对应于上述经过认证的用户信息的上述发送协议的认证信息的认证信息取得装置；遵照上述发送协议向上述邮件分发装置请求该所取得的认证信息的认证的发送认证请求装置；以及在上述认证信息被认证的情况下，遵照上述发送协议将电子邮件发送给上述邮件分发装置的发送装置。

根据本发明第2技术方案的构成,就取得与上述第1技术方案同样的效果。

最好是,上述认证信息保存装置保存对应于上述用户信息的电子邮件地址和对应于上述用户信息的上述发送协议的认证信息,上述认证信息取得装置取得保存在上述认证信息保存装置中的电子邮件地址和上述认证信息。

根据此优选技术方案的构成,就取得与在上述第1技术方案的最初所记述的优选技术方案同样的效果。

最好是,上述认证信息是对应于上述用户信息的SMTP认证的用户名和密码。

为了达到上述目的,本发明的第3技术方案提供一种在通信装置中执行的电子邮件发送方法,所述通信装置经由网络连接到认证装置和邮件分发装置,并按照发送协议经由上述邮件分发装置发送电子邮件,包括:输入用户信息的输入步骤;向上述认证装置请求该被输入的用户信息的认证的用户认证请求步骤;在上述用户信息被认证的情况下,从上述认证装置取得对应于上述经过认证的用户信息的上述发送协议的认证信息的认证信息取得步骤;遵照上述发送协议向上述邮件分发装置请求该所取得的认证信息的认证的发送认证请求步骤;以及在上述认证信息被认证的情况下,遵照上述发送协议将电子邮件发送给上述邮件分发装置的发送步骤。

为了达到上述目的,本发明的第4技术方案提供一种在通信装置中执行的电子邮件发送方法,所述通信装置经由网络连接到邮件分发装置,并按照发送协议经由上述邮件分发装置发送电子邮件,包括:输入用户信息的输入步骤;请求该被输入的用户信息的认证的用户认证请求步骤;按每个用户保持上述发送协议的认证信息的保持步骤;从在上述保持步骤中所保持的认证信息之中取得对应于上述经过认证的用户信息的上述发送协议的认证信息的认证信息取得步骤;遵照上述发送协议向上述邮件分发装置请求该所取得的认证信息的认证的发送认证请求步骤;以及在上述认证信息被认证的情况下,遵照上述发送协议

将电子邮件发送给上述邮件分发装置的发送步骤。

为了达到上述目的,本发明的第5技术方案提供一种在通信装置中执行的电子邮件发送程序,所述通信装置经由网络连接到认证装置和邮件分发装置,并按照发送协议经由上述邮件分发装置发送电子邮件,包括:输入用户信息的输入模块;向上述认证装置请求该被输入的用户信息的认证的用户认证请求模块;在上述用户信息被认证的情况下,从上述认证装置取得对应于上述经过认证的用户信息的上述发送协议的认证信息的认证信息取得模块;遵照上述发送协议向上述邮件分发装置请求该所取得的认证信息的认证的发送认证请求模块;以及在上述认证信息被认证的情况下,遵照上述发送协议将电子邮件发送给上述邮件分发装置的发送模块。

为了达到上述目的,本发明的第6技术方案提供一种在通信装置中执行的电子邮件发送程序,所述通信装置经由网络连接到邮件分发装置,并按照发送协议经由上述邮件分发装置发送电子邮件,包括:输入用户信息的输入模块;请求该被输入的用户信息的认证的用户认证请求模块;按每个用户保持上述发送协议的认证信息的保持模块;从在上述保持模块中所保持的认证信息之中取得对应于上述经过认证的用户信息的上述发送协议的认证信息的认证信息取得模块;遵照上述发送协议向上述邮件分发装置请求该所取得的认证信息的认证的发送认证请求模块;以及在上述认证信息被认证的情况下,遵照上述发送协议将电子邮件发送给上述邮件分发装置的发送模块。

本发明上面以及其他的目的、特征和优点,通过结合附图的以下详细说明将更为清楚。

附图说明

图1是表示涉及本发明第1实施方式的包含通信装置的电子邮件系统的整体构成图。

图2是表示图1所示的MFP (Multi Function Peripheral) 的构成的框图。

图3是表示MFP所有的网络协议层次结构的图。

图4是表示对图1所示的认证服务器中所登录的用户信息及其内容进行参照/编辑的程序的画面的图。

图5是表示取得MFP中的电子邮件地址、SMTP认证用户名以及SMTP认证密码时的注册处理的流程图。

图6是表示用户认证中的MFP和认证服务器间的具体认证过程的图。

图7是表示操作部上所显示的发送设定画面的图。

图8是表示管理发送收件方信息的地址簿的图。

图9是表示在用扫描器读取了原稿后，对各收件方发送电子邮件时的发送处理的流程图。

图10是具体地表示图9的步骤S17中的MFP和邮件服务器间的SMTP认证处理过程的图。

图11是表示对第2实施方式的认证服务器中所登录的用户信息及其内容进行参照/编辑的程序的画面的图。

图12是表示取得MFP中的电子邮件地址、SMTP认证用户名以及SMTP认证密码时的注册处理的流程图。

图13是表示操作部上所显示的发送设定画面的图。

具体实施方式

图1是表示涉及本发明第1实施方式的包含通信装置的电子邮件系统的整体构成图。此电子邮件系统，由经由遍及全世界的因特网110而连接到第1网络105以及第2网络125的多个设备构成。

在第1网络105上被分配域名“xyz. co. jp”，并连接有MFP (Multi Function Peripheral) 100、101，认证服务器102，邮件 / POP服务器103以及客户端PC104。在第2网络125上被分配域名“abc. co. jp”，并连接有邮件 / POP服务器120，PC121以及互联网传真122。

MFP100、101，搭载扫描器以及打印机，具备复制功能、传真 (FAX) 收发功能以及对由计算机所创建的数据进行打印的打印机功

能等。另外，MFP100被赋予主机名“copy1. xyz. co. jp”以及电子邮件地址“ifax @ copy1. xyz. co. jp”。MFP101被赋予主机名“copy2. xyz. co. jp”以及电子邮件地址“ifax@copy2. xyz. co, jp”。

认证服务器102，进行第1网络105的域内的用户认证，在认证服务器102上登录有多组在此域内有效的用户名、密码等。在PC104上安装有通用电子邮件软件，并赋予电子邮件地址“syain1 @ xyz. co. jp”。若接通客户端PC104的电源，则要求输入用户名和密码，若用户输入用户名和密码，则客户端PC104对认证服务器102，查询所输入的用户名和密码是否与所登录的用户名和密码一致。当在认证服务器102中作为用户已登录的情况下，PC104就成为可使用的状态。

邮件 / POP服务器103具有邮件服务器（SMTP服务器）和POP服务器双方的功能。当然，也可以设邮件服务器和POP服务器为不同的装置。另外，第2网络125的域内的邮件 / POP服务器120也具有同样的功能。例如，在从PC104向电子邮件地址“pcmail@ abc. co. jp”发送电子邮件的情况下，用PC104所创建的电子邮件数据，以SMTP（Simple Mail Transfer Protocol）协议送往邮件服务器103，进而，从邮件服务器103经由因特网110以SMTP协议送往邮件服务器120。

在PC121上安装有通用电子邮件软件。PC121使用POP3（Post Office Protocol - Version3）协议，以一定间隔监视在POP服务器120上是否有电子邮件到达，在电子邮件到达的情况下，就接收电子邮件的数据。另外，在从具有电子邮件地址“pcmail @ abc. co. jp”的PC121向具有电子邮件地址“syain1 @ xyz. co. jp”的PC104发送电子邮件的情况下，在PC121所创建的电子邮件数据，沿相反的路由，经邮件服务器120中继后被送往邮件服务器103。然后，PC104使用POP3协议，取得已达到的电子邮件数据。而且，具有对MIME等形式的电子邮件数据进行解释，并对其中所包含的图像数据进行解码后再现的功能。

在MFP100、101上，存在以将利用传真（FAX）、IFAX接收功能所接收到的图像或用扫描器所读取到的黑白 / 彩色图像送往一般的电子邮件收件方为前提进行发送的电子邮件发送模式，和以发送到遵

从IFAX规格的装置为前提的IFAX发送模式。在发送/接收的通信协议中使用SMTP、POP3, MFP100、101进行与上述利用PC的发送/接收同样的动作。

这里, 在电子邮件发送模式下, 发送JPEG文件格式的图像(简单称为JPEG图像)。例如, 若对具有电子邮件地址“syain1@xyz.co.jp”的客户端PC104发送彩色图像, 则PC104接收电子邮件, 并用通用图像观看器显示JPEG图像。在IFAX发送模式下, 则发送遵守技术规范RFC2301的TIFF形式图像。例如, 通过具有IFAX规格的MFP100、MFP101或互联网传真122来收发图像。在可处理彩色图像的设备间的情况下, 则收发TIFF形式的JPEG图像。

图2是表示MFP106的构成的框图。由于MFP100和MFP101为相同的构成, 所以在这里只对MFP100的构成进行说明。MFP100具有, CPU130、ROM131、RAM132、操作部133、扫描器134、打印机135、图像处理电路136、硬盘137、网络接口(I/F)138、格式器139以及传真部140。

CPU130作为控制系统全体的控制电路而发挥功能, 执行ROM131中所保存的程序, 并将RAM132作为工作区来使用。操作部133由启动键, 0~9数字键等硬件键以及LCD显示板构成, 在LCD显示板上作为软件键而显示按钮, 检测由用户的手指等对按钮的接触, 顺利地执行用户操作。

扫描器134, 通过光电变换将原稿图像变换成电图像数据。扫描器134具备, 放置从原稿供给装置所输送的原稿的稿台玻璃, 具有照射原稿的灯的扫描单元, 接收来自原稿的反射光的CCD图像传感器, 用于将来自原稿的反射光导入CCD图像传感器的反射镜及透镜, 以及用于将通过CCD图像传感器经过光电变换的电信号变换成数字数据的A/D变换电路。包含在扫描器134中的上述构成要素未表示在图2中。从原稿供给装置将原稿输送到稿台玻璃上, 当原稿被输送到稿台玻璃上时, 则将灯点亮, 然后使扫描单元开始移动, 对原稿进行曝光扫描。来自原稿的反射光经由反射镜和透镜被导入CCD图像传感器。当由

CDD图像传感器转换成电信号时，则通过A/D变换电路转换成数字数据。在原稿读取动作结束后，稿台玻璃上的原稿就被排出。

打印机部135，将图像数据打印在记录纸上。打印机部135具备激光发光部、感光鼓、转印部、定影部、排纸辊、以及具有多个分页格的分页器。由激光发光部发出与图像数据相应的激光。若此激光被照射到感光鼓上，则在感光鼓上形成与激光相应的潜像。在感光鼓的潜像部分上通过显影器涂敷显影剂，在与激光的照射开始以同步的定时从供纸盒供给记录纸，并输送给转印部。附着在感光鼓上的显影剂被转印在记录纸上。若转印了显影剂的记录纸被输送到定影部，则通过定影部中的热与压力，使显影剂定影在记录纸上。通过了定影部的记录纸由排纸辊所排出。被排出的记录纸，通过分页器被收放于各自的分页格，进行记录纸的分类。

图像处理电路136由大容量的图像存储器，图像旋转电路，分辨率变倍电路，以及MH、MR、MMR、JBIG、JPEG等编码/解码电路等构成，执行明暗(shading)、修整(trimming)、遮蔽(masking)等各种图像处理。硬盘137是可用SCSI、USB等接口(I/F)连接的大容量记录媒体。此外，作为记录媒体，并不限于硬盘，还可以是光磁盘(MO)等。

网络I/F138，是以10BASE-T、100BASE-T为代表的以太网(美国Xerox公司的注册商标)或者令牌环(美国IBM公司的注册商标)等，执行用于连接到网络的网络数据链路。格式器139具有遵照IEEE1284标准的并行接口、USB等PC接口(I/F)，以经由PC接口(I/F)或者网络I/F138接收到的来自个人计算机的PDL(Page Description Language)数据为基础创建图像数据。用图像处理电路136对所创建的图像数据进行图像处理，并进行用于由打印机135打印的再现(rendering)处理。

传真部140连接到电话线路，是由NCU(Network Control Unit)、MODEM(Modulator/DEModulator)等构成的传真I/F电路。此传真部140，对用扫描器134所读取的图像数据，用图像处理电路136进行

图像处理，并经由电话线路发送给其他的传真（FAX）装置，或者接收从其他的传真（FAX）装置发送的图像数据，用图像处理电路136进行图像处理，使打印机135进行打印。

扫描器134、打印机135、图像处理电路136、格式器139以及传真部140，经由与CPU130的CPU总线141不同的高速视频总线142相连接，可高速传送图像数据。从而，通过使用此高速视频总线142，对用扫描器134所读取的图像数据，用图像处理电路136进行图像处理，并通过将经过图像处理的图像数据用打印机135进行打印，来实现复制功能。

另外，在MFP100上设置有，在对用扫描器134所读取的图像数据，用图像处理电路136进行了图像处理，从网络I/F发送给网络105的发送（Send）功能，或者用图像处理电路136创建遵守技术规范RFC2301的图像数据，用电子邮件协议来发送数据的IFAX功能。

图3是表示MFP100所有的网络协议的层次结构的图。网络协议大致划分由3个层次的程序，也就是IP（Internet Protocol）层200、TCP（Transmission Control Protocol）/UDP（User Datagram Protocol）层201以及应用层202构成。

IP层200是提供从发件方主机至收件方主机，经由路由器等中继节点将消息送到的服务的互联网的协议层。而且，IP层200执行对发送数据的发件方的地址以及接收数据的收件方的地址进行管理，并对依照地址信息在网络内按怎样的路径将数据送到收件方主机进行管理的路由选择功能。

TCP/UDP层201是提供从发件应用进程将消息送到接收应用进程的服务的传输层。而且，TCP是连接式服务的协议，保证通信的高度可靠性，但UDP是无连接式的服务的协议，不进行可靠性的保证。

应用层202规定多个协议。在此层202中包含作为文件传送服务的FTP（File Transfer Protocol），作为网络管理协议的SNMP，作为打印机打印用的服务器协议的LPD，作为WWW（World Wide Web）服务器的协议HTTPd，电子邮件收发协议SMTP（Simple Mail Transfer Protocol），邮件下载协议POP3（Post Office Protocol -

Version3)等。除此以外,还搭载有在技术规范RFC1510中所规定的Kerberos认证程序。

图4是表示对在认证服务器102中所登录的用户信息及其内容进行参照/编辑的程序的画面的图。用户信息由用户名230、密码231、电子邮件地址232、SMTP认证用户名233以及SMTP认证密码234构成。用户名230表示可使用认证服务器102担当的域名为“xyz. co. jp”的域(主要的)内的计算机的用户名。在图4中,登录有“syain1”~“syain5”的用户名。在密码231中登录有对应于各用户名的密码。在这里,为了不让第三者容易地看到,各密码用“* * * * *”来进行显示。

在电子邮件地址232中登录有认证服务器102中所登录的用户可使用的电子邮件地址。用户名为“syain1”的电子邮件地址是“syain1 @ xyz. co. jp”。用户名为“syain2”的电子邮件地址是“syain2 @ xyz. co. jp”。用户名为“syain3”的电子邮件地址是“syain3 @ xyz. co. jp”。用户名为“syain4”的电子邮件地址是“syain4 @ xyz. co. jp”。用户名为“syain5”的电子邮件地址是“syain5 @ xyz. co. jp”。

SMTP认证用户名233以及SMTP认证密码234是SMTP认证(RFC2554)中所使用的用户名和密码信息,例如,在从MFP100、MFP101、PC104向邮件服务器103发送电子邮件时,在SMTP协议上进行用户认证,用于防止非法访问或冒充电子邮件的发出人名称(From地址)的邮件的非法转接。虽然在图4的设定中,用户名“syain1”~“syain5”的SMTP认证用户名为分别与用户名“syain1”~“syain5”是相同的名称,但当然也可以使用不同的名称。另外,SMTP认证密码234与密码231同样,为了不被容易地看到而使用“* * * * *”来进行显示。

追加键240是在新用户登录时所使用的键。删除键241是删除登录用户的键。属性键242是对已登录的内容进行修正的键,若按下属性键242,就显示已登录的内容。

图5是表示取得MFP100中的电子邮件地址、SMTP认证用户名以

及SMTP认证密码时的注册处理的流程图。MFP100利用此注册处理对认证服务器102请求用户认证，用所指定的用户名来使用电子邮件。此外，由于关于MFP101也同样如此，所以只对MFP100进行说明。

当MFP100的主电源被接通，存储器、I/O端口的初始化等初始化动作被执行后，在通过系统用户设定将“用户认证”设定成“执行”的情况下，此注册处理开始。在此状态下，不能执行复制等用户操作介入的处理，在操作部133上显示输入用户名的画面。

首先，显示用户名输入画面，等待由用户输入用户名（步骤S1）。若用户名被输入，则接着等待输入密码（步骤S2）。若密码被输入，则为了用认证服务器102进行认证，发送用户名和密码（步骤S3）。

然后，对认证的结果，即所输入的用户名和密码是否与认证服务器102中所登录的用户名230和密码231一致，判别从认证服务器102是否回答认证OK（步骤S4）。在所输入的用户名、密码错误情况等，没有回答认证OK而回答了认证NG的情况下，则退到步骤S1并从用户名输入画面进行反复同样的处理。另一方面，在回答了认证OK的情况下，则从认证服务器102取得在认证服务器102中所登录的、已注册的用户人的电子邮件地址232（步骤S5）。进而，从认证服务器102取得已注册的用户人的SMTP认证的用户名233和用户SMTP认证的密码234（步骤S6，S7），并结束本处理。

若此用户认证正常结束，复制、发送（SEND）等用户操作介入的处理就可执行。此外，虽然在本实施方式中，作为用户认证的方法表示了输入用户名和密码的情形，但也可以是利用指纹或眼球等的生物认证，利用非接触或接触式的控制卡的用户认证等。

图6是表示用户认证中的MFP100和认证服务器102间的具体认证顺序的图。认证服务器102的用户认证方式，是使用了作为网络应用层的协议的Kerberos的认证方式，作为技术规范RFC1510被标准化。

首先，Kerberos认证服务请求KEB-AS-REQ被从作为客户端的MFP100送往认证服务器102（T1），若进行了是否为合法用户的查询，则经过了加密的注册会话密钥和客户端认证数据就作为Kerberos

认证服务答复KEB-AS-REP从认证服务器102返回MFP100(T2)。

以此数据为基础,创建Kerberos标签认可服务请求KEB-TGS-REQ,MFP100对认证服务器102进行资格信息的请求(T3)。经过了加密的客户端认证数据作为Kerberos标签认可服务答复KEB-TGS-REP从认证服务器102返回(T4)。

以此数据为基础,创建Kerberos应用请求KEB-AP-RE,MFP100向认证服务器102请求服务利用许可(T5)。然后,若从认证服务器102返回Kerberos应用答复KEB-AP-REP(T6),则在所返回的数据正常、且答复数据内的时刻数据为规定的时间内的情况下,MFP100就认为是认证OK。

此外,虽然在本实施方式中,表示在同一认证服务器进行3种请求的情形,但根据网络构成等,也可以使用多个服务器。另外,作为认证方式,还可以是DH(Diffie-Hellman)认证等其他的认证方式。

图7是表示操作部133上所显示的发送设定画面的图。此发送设定画面,在通过图5的注册处理以用户名“syain1”进行注册正常结束,用电子邮件发送由扫描器134所读取的图像数据时,被显示在操作部133上。在读取大小300上,指定扫描器134读入的原稿大小等。作为原稿,能够指定A3、A4、A5、B4、B5、11*17、LTR、STMT等用纸大小及其方向。在图7中由于在读取大小300上设定为“自动”,故由设置在扫描器134上的原稿检测传感器所检测到的值被读入。

另外,对分辨率301可指定在扫描器134读入原稿时的分辨率。作为分辨率被指定成200*100、200*200、200*400、300*300、400*400以及600*600dpi中的某一个。在图7中,设定为缺省值200*200。另外,在详细设定302中,可对扫描时的浓度设定、原稿类型指定、双面读入、页连续打印指定,像质调整等扫描时的详细动作进行指定。

主题304和正文305分别为在将要发送的电子邮件中所附加的邮件名和邮件正文。若选择这些各设定栏,则显示软键盘,可输入字符串。收件方303是指定发送目的地的栏。

图8是表示管理发送收件方信息的地址簿的图。发送收件方的电

子邮件地址被显示于地址栏352。然后，当在选择栏350上附加标记后向收件方发送电子邮件时，所选择的地址就被记载于电子邮件的To: 字段中。在模式栏351上能够指定作为送信收件方、以送往一般的电子邮件收件方为前提进行发送的电子邮件发送模式，和以送往具有设备间的收发功能的IFAX装置为前提进行发送的IFAX发送模式中的某一个。在图8的设定中，指定了电子邮件发送模式用的两个电子邮件发送收件方（电子邮件地址“pcmail@abc.co.jp”、“syain1@xyz.co.jp”），以及IFAX发送模式用的一个IFAX发送收件方（电子邮件地址“ifax@abc.co.jp”）。

图9是表示在用扫描器134读取了原稿后，对各收件方发送电子邮件时的发送处理的流程图。此处理程序被保存于MFP100内的存储媒体（ROM131或者硬盘137），在向各收件方进行发送时，由CPU130执行。

首先，判别发送模式（模式351）是否为IFAX（步骤S11）。在是IFAX的情况下，在电子邮件的标题部的From字段上设定用户模式中所输入的设备的地址（步骤S12）。然后，在电子邮件的Sender字段上设定与注册时所设定的用户名230相对应的电子邮件地址232（步骤S13，参照图4）。在这里，由于在注册时是以用户名“syain1”进行注册的，所以在Sender地址上设定对应于用户名“syain1”的电子邮件地址“syain1@xyz.co.jp”。在设定了From字段、Sender字段后，在由扫描器所读取的图像的上端，赋予以发送设备电子邮件地址、发送收件方简称、发送时间等信息为基础作为图像数据所创建的图像标题（步骤S14）。

另一方面，在发送模式不是IFAX而是电子邮件的情况下，在From字段上设定对应于注册时所设定的用户名230的电子邮件地址232（步骤S15）。在此情况下，不创建Sender字段。

之后，以From字段、Sender字段等信息为基础，进行邮件标题的创建、MIME信息的赋予、附件的利用BASE64方式的编码等邮件数据创建处理（步骤S16）。

在将所创建的电子邮件数据发送给邮件服务器103时，使用来自认证服务器102在步骤S6中所取得的SMTP认证的用户名以及在步骤中所取得的SMTP认证的密码，执行SMTP认证（步骤S17）。然后，判别SMTP认证的结果（步骤S18）。关于此SMTP认证将在后面进行叙述。然后，在认证结束后，也就是认证结果为认证OK的情况下，通过SMTP将数据发送给邮件服务器103（步骤S19）。若发送结束，则将注册时所指定的用户名230、发送收件方信息、发送日期、发送时间、发送张数以及送信结果写入日志（步骤S20），结束本处理。另一方面，当在步骤S18中认证结果为认证NG的情况下，则不进行发送结束本处理。

由MFP100写入到日志的数据，作为通知发送结果的发送结果报告，或者每当发送件数累积到一定以上所创建的通信管理报告来进行打印。根据所打印的报告，就能够确定已发送的作业（JOB）的发送者。另外，由于在邮件服务器103中保留进行SMTP认证时的时间及认证用户名等日志，所以就能够在送信管理结果报告或者通信管理报告的内容、与邮件服务器103的日志的内容进行对照、使之对比。其结果，就能够对日志的妥当性进行验证。此外，写入到日志的数据也可列表显示在操作部133上。

图10是具体地表示步骤S17中的MFP100和邮件服务器103间的SMTP认证处理过程的图。通过此SMTP认证，就可在从MFP101向邮件服务器103发送电子邮件时，对电子邮件的发送者进行认证，并防止冒充进行发送的电子邮件地址等非法电子邮件转接。下面所示的SMTP认证处理，主要由MFP100和邮件服务器103的各CPU执行。

首先，若从MFP101向邮件服务器103进行SMTP连接（T11），则从邮件服务器103回答表示SMTP服务就绪的数字“220”和域名（T12）。从作为客户端的MFP101将扩展SMTP的表示SMTP开始的EHLO指令发送给邮件服务器103（T13），以表示所请求的指令成功的数值“250”开始的指令响应从邮件服务器103返回（T14）。进而，根据邮件服务器103所拥有的SMTP扩展功能的响应被返回（T15，

T16)。在T15的响应中，表示邮件服务器103拥有DSN(Delivery Status Notifications) 服务功能，在T16的响应中，表示支持认证功能SMTP AUTH，作为认证方式则支持CRAM - MD5以及DIGEST - MD5。

由于判断为邮件服务器103对应SMTP AUTH，所以MFP101发送表示使用SMTP AUTH进行认证，作为认证方式使用CRAM - MD5的指令（T17）。从邮件服务器103回答表示请求连续的数字“334”和作为服务器质询数据的字符串（T18）。MFP101，由所取得的服务器质询数据和密码创建以CRAM - MD5进行了加密的加密密码，并回答对用户名和密码进行了加密的字符串（T19）。

在邮件服务器103中也同样由发送的服务器质询数据和与从MFP101发送来的用户名相对的密码创建加密密码，通过对此所创建的加密密码与从MFP101发送来的加密密码的一致性进行检测，来确认密码的有效性。然后，在密码的有效性得以确认的情况下，从邮件服务器103发送以表示认证成功数字“235”开始的消息（T20），结束SMTP认证。

之后，如上述那样，通过SMTP的通常顺序，电子邮件数据得以发送。若发送结束，则邮件服务器103将接受电子邮件分发的MFP101的电子邮件地址、发送收件方的电子邮件地址、进行了SMTP认证的用户名、通信日期、时刻等信息记录到日志文件。然后，邮件服务器103的管理者，就能够参照所记录的日志文件。

这样，根据本发明的第1实施方式，由于由MFP100写入到日志的数据作为发送结果报告或者通信管理报告进行打印，所以就确定已发送的作业（JOB）的发送者。另一方面，在邮件服务器103中保留进行SMTP认证时的时间及认证用户名等日志。从而，通过使送信结果报告或者通信管理报告的内容与邮件服务器3的日志的内容进行对照并进行对比，就能够确定实际的发送者。由此，就能够谋求使用SMTP认证进行发送时的安全性的提供，而不会使操作性降低。

另外，就不需要对MFP，设定SMTP认证用户名、SMTP认证密码以及电子邮件地址，从而能够容易地进行其登录、变更等管理。而

且,如上述那样,由于在邮件服务器侧保留通过SMTP认证进行了认证的用户名的日志,所以就可与MFP的发送日志1对1进行比较,并能够谋求安全性的向上。

下面,一边参照图11~13一边对本发明的第2实施方式进行说明。

在上述第1实施方式中,SMTP认证用户名和SMTP认证密码是用认证服务器进行管理,而在本实施方式中它们是用MFP进行管理这一点上不同。也就是,将在第1实施方式中用认证服务器102所管理的SMTP认证用户名、密码保持在硬盘137上。

第2实施方式的电子邮件系统的构成与上述第1实施方式大致相同,关于与上述第1实施方式相同的构成部分,通过附加相同的标记来省略其说明。图11是表示对第2实施方式的认证服务器102中所登录的用户信息及其内容进行参照/编辑的程序的画面的图。在上述第1实施方式中,如图4所示,作为用户信息设定有SMTP认证用户名和SMTP认证密码,但在第2实施方式中,如图11所示那样它们未被设定。

这里,用户名230是认证服务器102中所登录的用户名。密码231是登录用户名的密码。电子邮件地址232是登录用户名的电子邮件地址。另外,追加键240是在新用户登录时所使用的键。删除键241是删除登录用户时所使用的键。属性键242是对已登录的内容进行修正时所使用的键。若按下属性键242,就显示已登录的内容,并可对已登录的内容进行修正。

图12是表示取得MFP100中的电子邮件地址、SMTP认证用户名以及SMTP认证密码时的注册处理的流程图。MFP100,通过此注册处理对认证服务器102请求用户认证,以可用所指定的用户名来使用电子邮件。此外,由于关于MFP101也同样如此,所以只对MFP100进行说明。

当MFP100的主电源被接通,存储器、I/O端口的初始化等初始化动作被执行后,在通过系统用户设定将“用户认证”设定成“执行”的情况下,此注册处理开始。在此状态下,不能执行复制等用户操作介入的处理,在操作部133上显示输入用户名的画面。

首先,显示用户名输入画面,等待由用户输入用户名(步骤S31)。若用户名被输入,则接着等待输入密码(步骤S32)。若密码被输入,则为了用认证服务器102进行认证,发送用户名和密码(步骤S33)。

然后,对认证的结果,即所输入的用户名和密码是否与认证服务器102中所登录的用户名230和密码231一致,判别从认证服务器102是否回答了认证OK(步骤S34)。在所输入的用户名、密码错误情况等,不回答认证OK而回答了认证NG的情况下,则退到步骤S31并从用户名输入画面开始反复同样的处理。另一方面,在回答了认证OK的情况下,则从认证服务器102取得认证服务器102中所登录的、已注册的用户电子邮件地址232(步骤S35)。

在取得电子邮件地址后,取得对MFP100、MFP101等设备的每个用户所设定的SMTP认证用户名306(步骤S36)。进而,同样地,取得对设备的每个用户所设定的SMTP认证密码307(步骤S37)。之后,结束本处理。

若此用户认证正常结束,复制、发送(SEND)等用户操作介入的处理就可执行。此外,虽然作为用户认证的方法表示了输入用户名和密码的情形,但也可以是利用指纹或眼球等的生物认证,利用非接触或接触式的控制卡的用户认证等。

图13是表示操作部133上所显示的发送设定画面的图。在用于Send操作的发送设定画面中,在用户以用户名“syain1”进行了注册的情况下,在画面左上方显示出所注册的用户名“syain1”。

在读取大小300上,指定扫描器134读入的原稿大小等。作为原稿,能够指定A3、A4、A5、B4、B5、11 * 17、LTR、STMT等用纸大小及其方向。图13中由于在读取大小300上设定为“自动”,故由设置在扫描器134上的原稿检测传感器所检测到的值被读入。

另外,在分辨率301上可指定由扫描器134读入原稿时的分辨率。作为分辨率被指定成200 * 100、200 * 200、200 * 400、300 * 300、400 * 400以及600 * 600dpi中的某一个。在图13中,设定为缺省值200 * 200。另外,在详细设定302中,可对扫描时的浓度设定、原稿类型指

定、双面读入、页连续打印指定、像质调整等扫描时的详细动作进行指定。

主题304和正文305分别为在将要发送的电子邮件中所附加的邮件名和邮件正文。若选择这些各设定栏，则显示软键盘，可输入字符串。收件方303是指定发送收件方的栏。从上述第1实施方式的地址簿（参照图8）选择收件方。

SMTP认证用户名306和SMTP认证密码307是以SMTP协议对邮件服务器103发送电子邮件数据时，分别使用的用户名和密码。这些用户名和密码是逐用户地存储在设备中的设定参数，若各用户进行注册（Login），则作为设定参数在发送设定画面上显示该SMTP认证用户名306和SMTP认证密码307。另外，此设定参数是可变更的。

由扫描器134所读入的图像数据，通过图9所示的上述第1实施方式的发送处理进行发送。然后，在步骤S17的SMTP认证处理中，使用SMTP认证用户名306和SMTP认证密码307来进行认证。

根据第2实施方式，就取得与第1实施方式相同的效果。另外，具有SMTP认证用户和SMTP认证密码的MFP，可对邮件服务器103请求SMTP认证以执行电子邮件等的发送。

另外，在以上的实施方式中针对在邮件服务器上进行SMTP认证的例子进行了说明，但并不限于此，如果SMTP服务器和POP服务器由同一装置构成，则能够采用使用在POP before SMTP中所用的POP认证用的用户名和密码等各种方式。

上面是本发明的实施方式的说明，但本发明并不限于这些实施方式的构成，只要是能够实现权利要求的范围所示的功能，或者实施方式的构成所具有的功能的构成，则怎样的构成均可适用。

例如，虽然表示了在上述第1实施方式中，SMTP认证用户名和SMTP认证密码由认证服务器进行管理，在上述第2实施方式中由MFP进行管理的情形，但也可以是对由认证服务器或者MFP中某一个来管理进行切换这样的构成。另外，虽然表示了在网络上设置认证服务器，对来自多个PC和MFP的用户信息进行认证的情形，但在MFP内部加

入认证服务器功能，也可取得与这些实施方式同样的效果。

另外无需赘言，本发明的目的也可以这样达到，即通过将记录了实现上述实施方式的功能的软件的程序代码的存储媒体提供给系统或者装置，该系统或者装置的计算机（或者 CPU 和 MPU）读出并执行保存在存储媒体中的程序代码。

在此情况下，从存储媒体读出的程序代码自身就实现上述实施方式的功能，该程序代码以及存储了该程序代码的存储媒体就构成本发明。

另外无需赘言，不仅包含通过计算机执行所读出的程序代码，上述实施方式的功能得以实现的情况，还包含根据该程序代码的指示，在计算机上运行的操作系统（OS）等进行实际处理的一部分或者全部，通过该处理上述实施方式的功能得以实现的情况。

进而无需赘言，还包含当从存储媒体读出的程序代码，被写入到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上所具备的存储器以后，根据该程序代码的指示，该功能扩展板或功能扩展单元上所具备的 CPU 等进行实际处理的一部分或者全部，通过该处理上述实施方式的功能得以实现的情况。

另外，上述程序只要能够用计算机实现上述实施方式的功能即可，其形态也可以具有目标代码、由解释程序所执行的程序、或者被提供给 OS 的脚本数据等形态。

作为供给程序的存储媒体，例如能够使用软（注册商标）盘、硬盘、光盘、磁光盘、CD-ROM、MO、CD-R、CD-RW、DVD（DVD-ROM、DVD-RAM、DVD-RW、DVD+RW）、磁带、非易失性的存储卡、ROM 等。或者，通过从连接到因特网、商用网络或者局域网等的未图示的其他计算机或数据库等进行下载来供给上述程序。

图 1

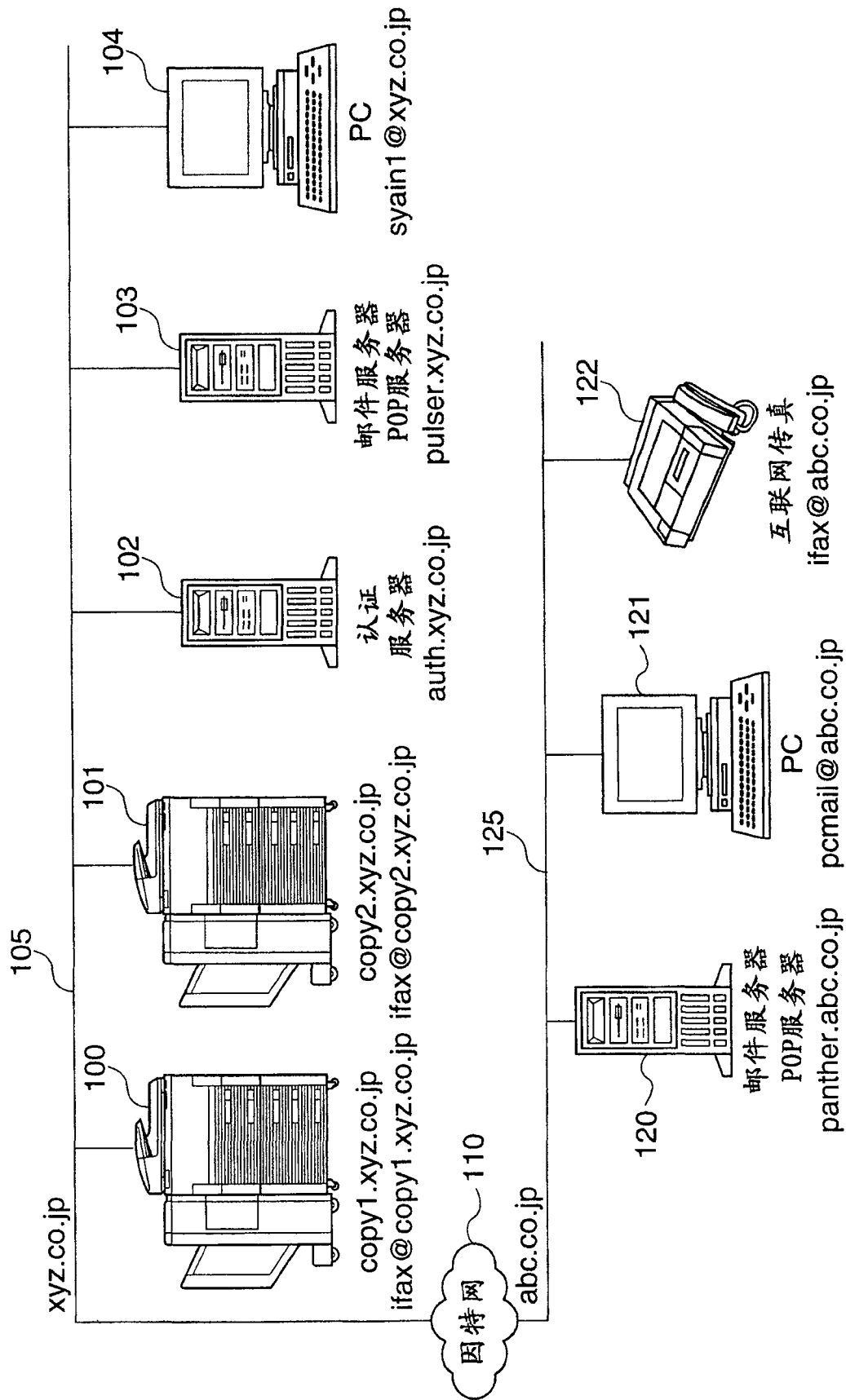


图 2

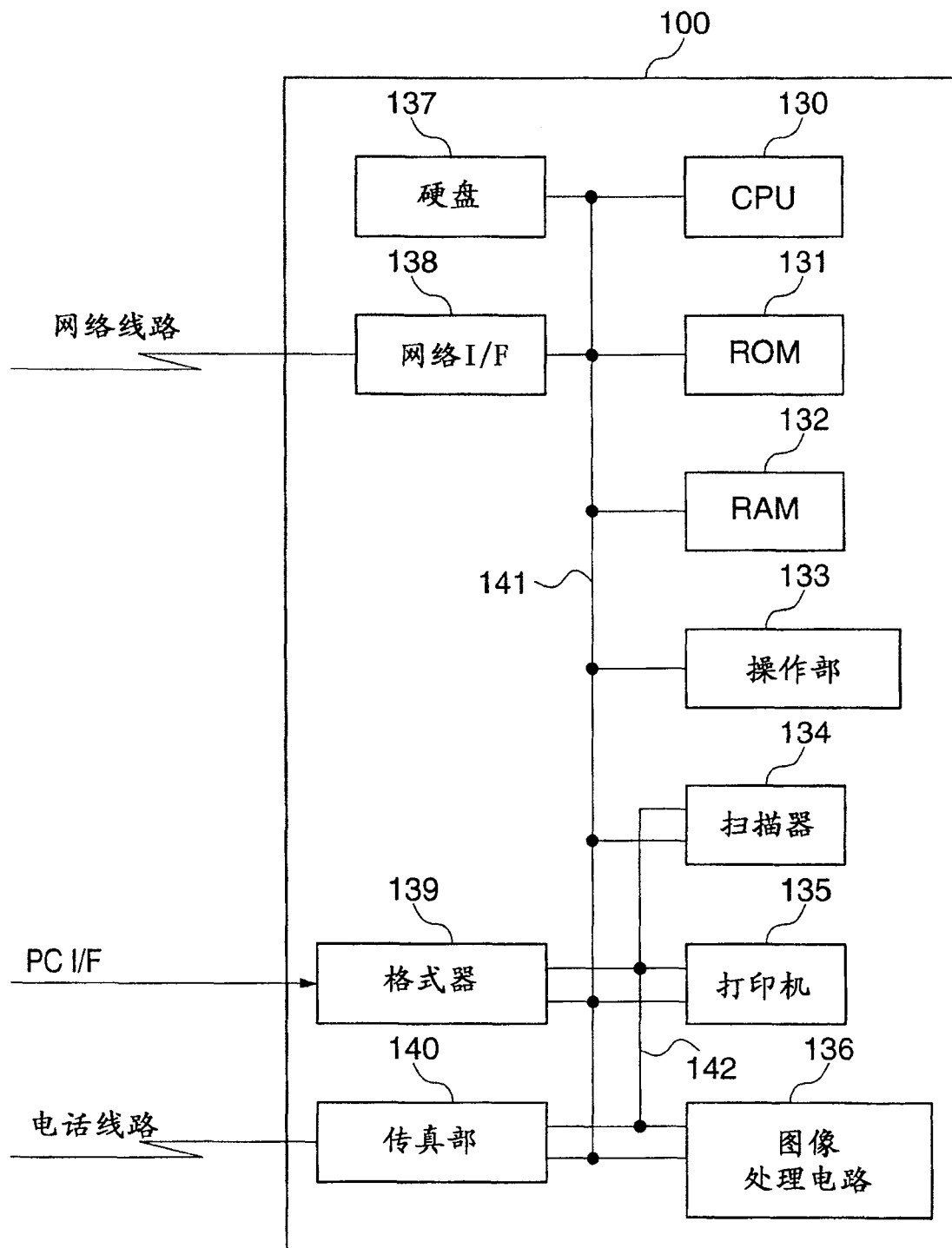


图 3

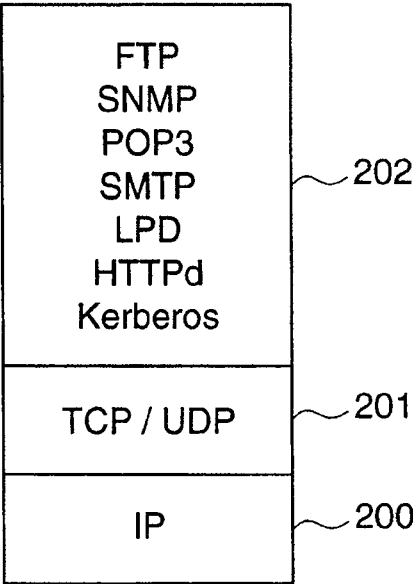


图 4

用户信息

230	231	232	233	234
用户名	密码	电子邮件地址	SMTP认证用户名	SMTP认证密码
syain1	*****	syain1@xyz.co.jp	syain1	*****
syain2	*****	syain2@xyz.co.jp	syain2	*****
syain3	*****	syain3@xyz.co.jp	syain3	*****
syain4	*****	syain4@xyz.co.jp	syain4	*****
syain5	*****	syain5@xyz.co.jp	syain5	*****

240

追加

241

删除

242

属性

图 5

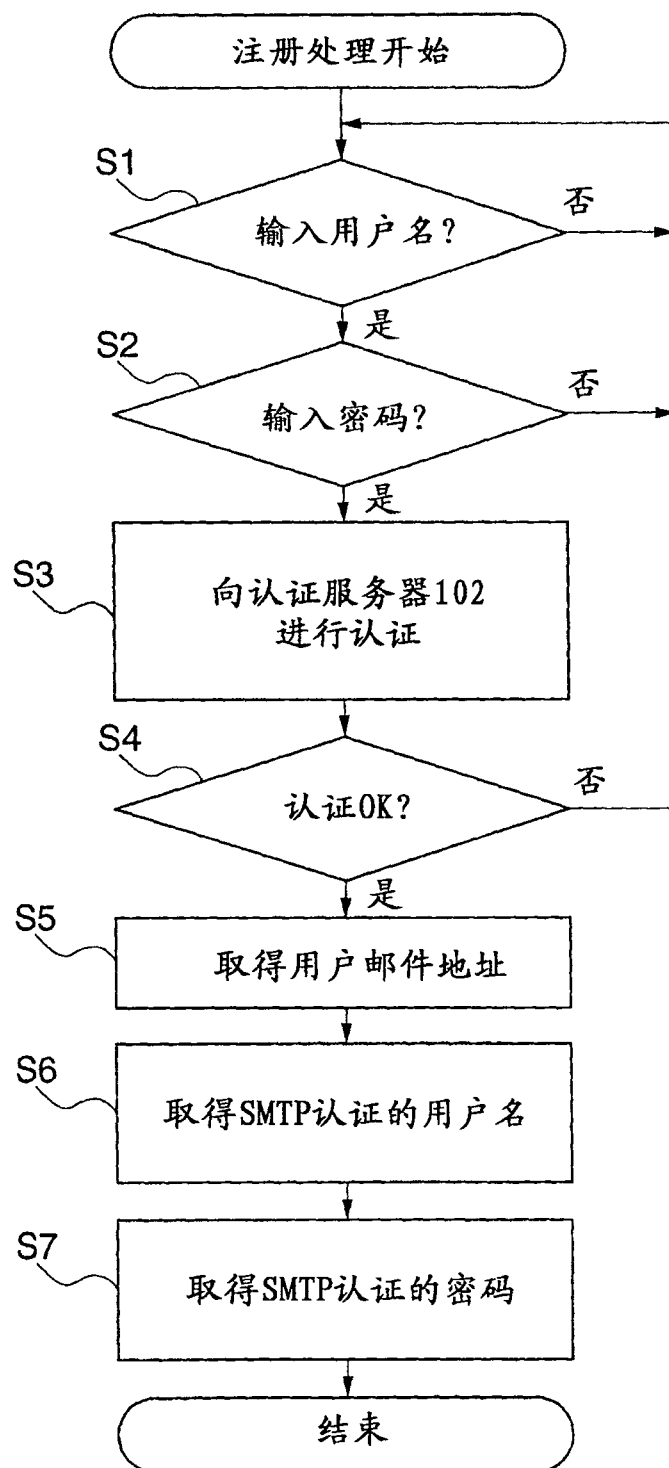


图 6

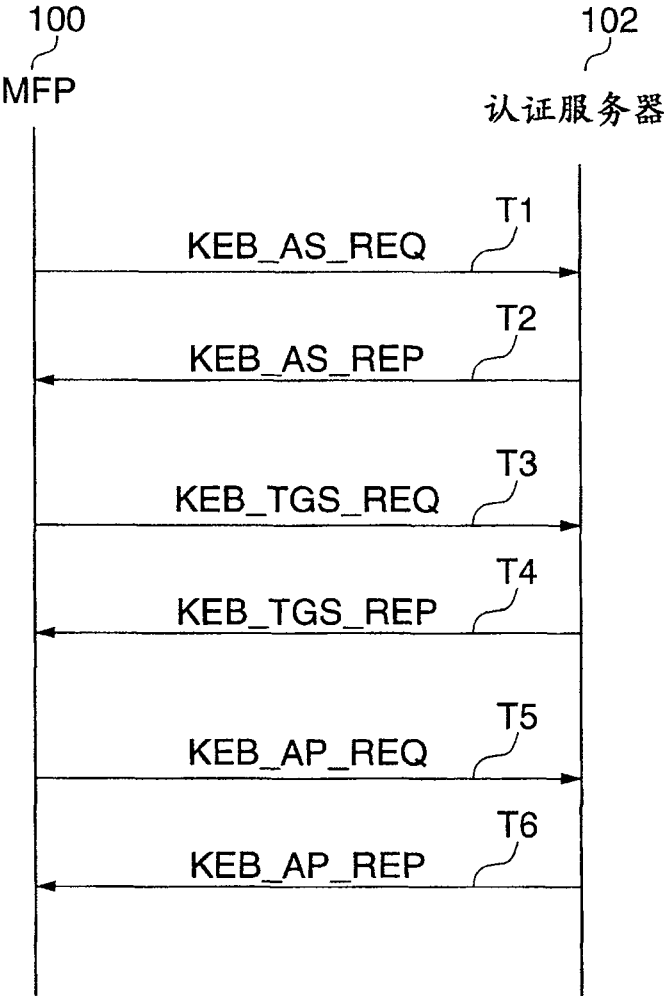


图 7

302

发送设定	
300 读取大小	自动 详细设定
301 分辨率	200×200 dpi
303 收件方	ifax@abc.co.jp
304 主题	发送报价单
305 正文	承蒙关照。 发送委托的报价单。

图 8

地址簿			
	350 选择	351 模式	352 地址
1	●	EMAIL	pcmail@abc.co.jp
2	●	IFAX	ifax@abc.co.jp
3	●	EMAIL	syain1@xyz.co.jp
4		IFAX	syain2@xyz.co.jp
5		IFAX	ifax@copy1.xyz.co.jp
6		IFAX	ifaxl@copy2.xyz.co.jp

图 9

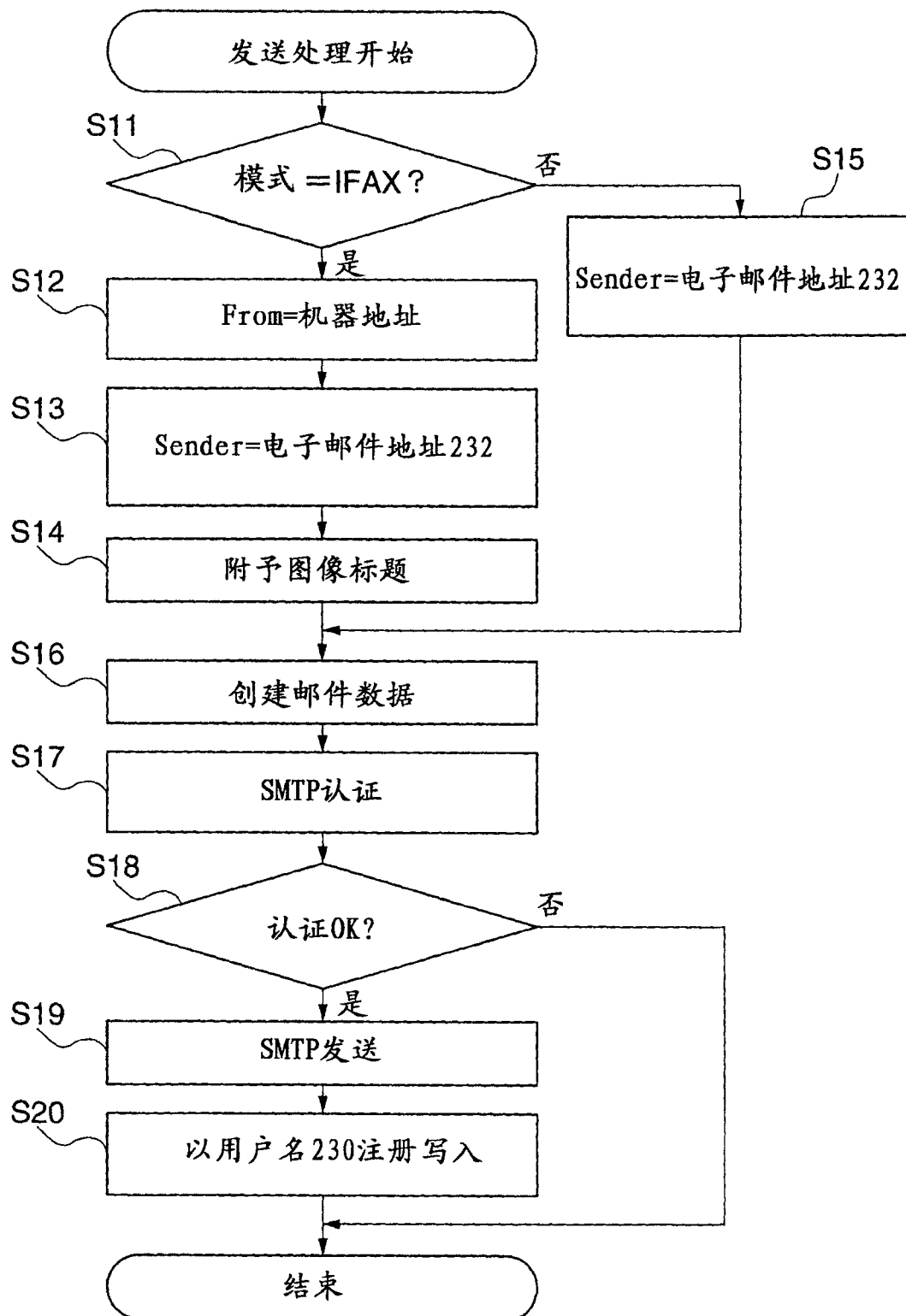


图 10

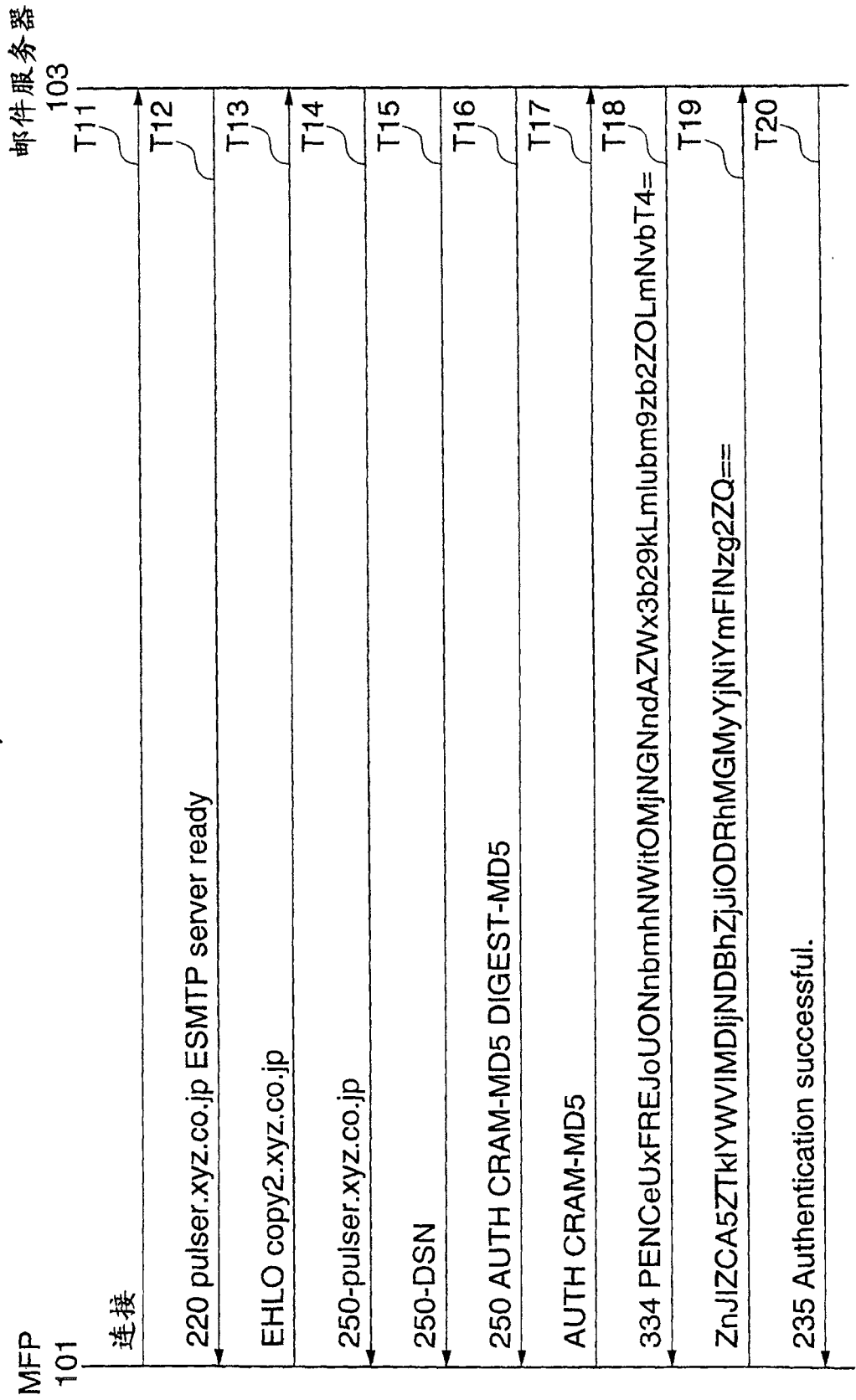


图 11

用户信息

230

231

232

用户名	密码	电子邮件地址
syain1	*****	syain1@xyz.co.jp
syain2	*****	syain2@xyz.co.jp
syain3	*****	syain3@xyz.co.jp
syain4	*****	syain4@xyz.co.jp
syain5	*****	syain5@xyz.co.jp

240

241

242

追加

删除

属性

图 12

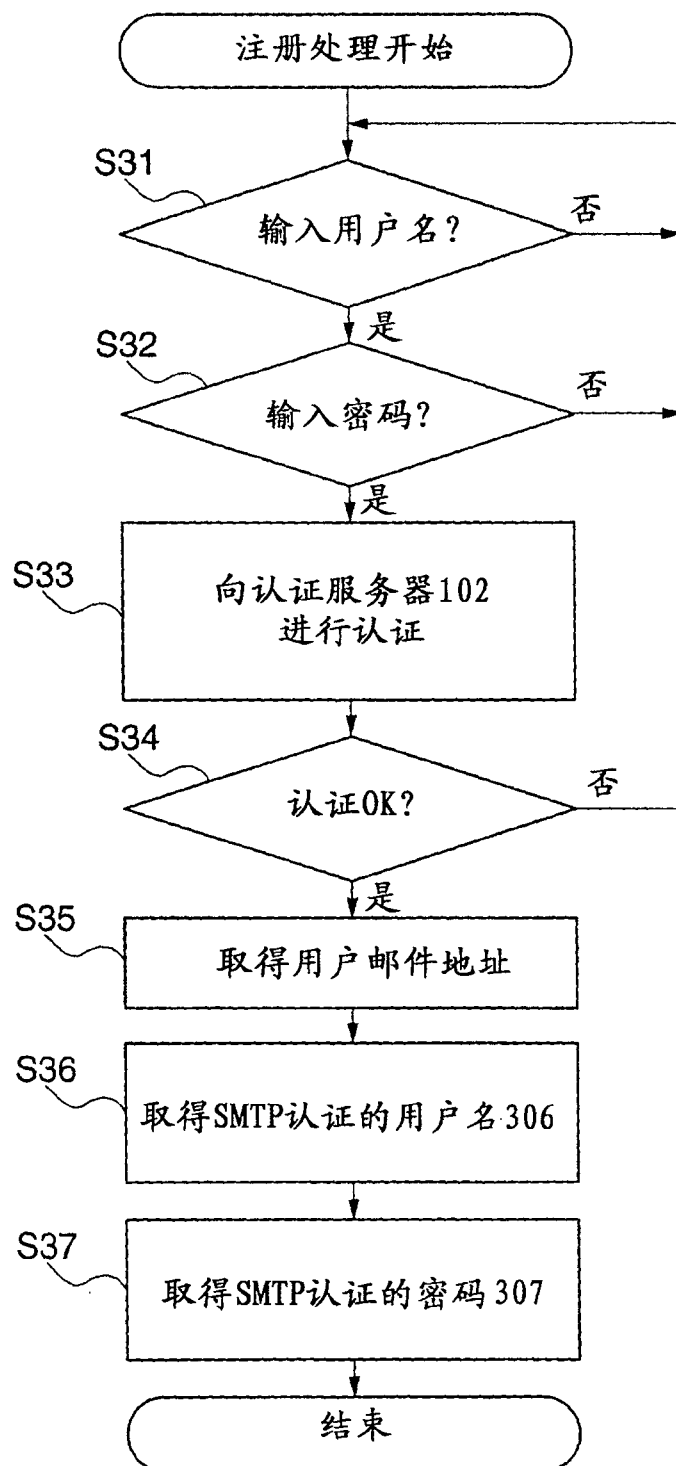


图 13

300 301 303 304 305 306 307

发送设定 [syain1]

302

自动

详细设定

200×200 dpi

308

登录

ifax@abc.co.jp

发送报价单

承蒙关照。
发送委托的报价单。

syain1

SMTP认证用户名

SMTP认证密码
