



[12] 发明专利说明书

专利号 ZL 200310121544.5

[45] 授权公告日 2009 年 8 月 5 日

[11] 授权公告号 CN 100525177C

[22] 申请日 2003.12.18

[21] 申请号 200310121544.5

[30] 优先权

[32] 2002.12.19 [33] JP [31] 367502/2002

[73] 专利权人 巴比禄股份有限公司

地址 日本爱知县

[72] 发明人 石彻白敬

[56] 参考文献

JP10070540A 1998.3.10

US5655219A 1997.8.5

审查员 刘斌

[74] 专利代理机构 北京东方亿思知识产权代理有限责任公司

代理人 杜娟

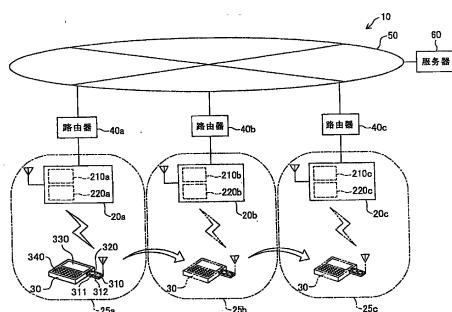
权利要求书 5 页 说明书 14 页 附图 7 页

[54] 发明名称

用于广域网的接入认证系统、设备和方法

[57] 摘要

本发明提供了接入认证技术，其能提高接入点系统在终端设备的接入认证方面的稳定性。在接入点系统 10 中，连接设备 20a 从终端设备 30 接收终端设备 30 的识别信息，注册包括与终端设备 30 相关的识别信息的认证信息，并向终端设备 30 传输连接设备 20a 的识别信息。另一个连接设备 20b 从终端设备 30 接收连接设备 20a 和终端设备 30 的识别信息，基于连接设备 20a 的识别信息来建立经由因特网到连接设备 20a 的连接，经由此连接而将终端设备 30 的识别信息传输到连接设备 20a，并基于由连接设备 20a 进行的对终端设备 30 的认证而向终端设备 30 提供接入点。



1. 一种广域网系统，包括：

多个连接设备，连接到广域网并经由所述广域网交换数据；和

多个终端设备，通过无线通信连接到所述连接设备中的任何一个，

其中所述每个单独的连接设备包括：

认证信息存档装置，基于对于所述多个终端设备中的每一个的初始认证，为该终端设备存档认证信息，其中所述初始认证是在其认证信息未被存档在所述多个连接设备中的任何一个之中的终端设备经由所述无线通信连接到所述广域网时执行的，其中所述认证信息与识别该终端设备的识别信息相关；和

认证装置，当包括在所述多个连接设备中的外部连接设备从请求连接到所述广域网的终端设备接收到识别所述请求连接的终端设备的识别信息，并且当所述外部连接设备的认证信息存档装置中没有与所述请求连接的终端设备的识别信息相关的认证信息时，所述认证装置对所述请求连接的终端设备执行接入认证，并将认证结果经由所述广域网传输到所述外部连接设备。

2. 一种接入认证系统，用于通过验证已注册的认证信息来进行接入认证，所述系统包括：

请求接入广域网的终端设备；

连接设备，用于经由无线网络来向所述终端设备提供到所述广域网的接入点；和

接入点系统，由所述连接设备组织，位于多个物理位置，

其中所述连接设备包括：

注册装置，从所述终端设备接收与所述终端设备相关的识别信息，注册包括与所述终端设备相关的识别信息的认证信息，并向所述终端设备传输与所述连接设备相关的识别信息；和

认证装置，当不同于所述连接设备的外部连接设备向已注册认证信息的所述终端设备提供接入点时，所述认证装置通过对与所述终端设备相关

的识别信息和由所述注册装置注册的认证进行交叉校验，而经由所述广域网来为所述终端设备进行接入认证，所述识别信息由所述外部连接设备经由所述广域网来传输；

其中所述终端设备包括：

终端注册装置，在还未注册认证信息的情况下，当由所述连接设备提供接入点时，所述终端注册装置将与所述终端设备相关的识别信息传输到所述连接设备，从所述连接设备接收与所述连接设备相关的识别信息，并存档所述信息；和

终端提供装置，在还未注册认证信息的情况下，当由所述外部连接设备提供接入点时，所述终端提供装置将与所述连接设备相关的存档识别信息、与所述终端设备相关的识别信息传输到所述外部连接设备；

并且其中所述外部连接设备包括：

提供装置，当向其认证信息已由所述连接设备注册的终端设备提供接入点时，所述提供装置从所述终端设备接收与所述连接设备相关的识别信息和与所述终端设备相关的识别信息，基于与所述连接设备相关的识别信息经由所述广域网建立与所述连接设备的连接，将与所述终端设备相关的识别信息经由所述连接传输到所述连接设备，并基于由所述连接设备为所述终端设备进行的接入认证而向所述终端设备提供所述接入点。

3. 一种连接设备，连接到广域网并经由所述广域网交换数据，所述连接设备包括：

无线通信装置，用于通过无线通信来和终端设备交换信息；

认证信息存档装置，用于基于对于多个所述终端设备中的每一个的初始认证，为该终端设备存档认证信息，其中所述初始认证是在其认证信息未被存档在包括所述连接设备在内的多个连接设备中的任何一个中的终端设备经由所述无线通信连接到所述广域网时执行的，其中所述认证信息与识别该终端设备的识别信息相关；和

认证装置，用于当包括在所述多个连接设备中的外部连接设备从请求连接到所述广域网的终端设备接收识别所述请求连接的终端设备的识别信息，并且当所述外部连接设备的认证信息存档装置中没有与所述请求连接

的终端设备的识别信息相关的认证信息时，对所述请求连接的终端设备执行接入认证，并将认证结果经由所述广域网传输到所述外部连接设备。

4. 一种连接设备，用于经由无线网络来向请求接入广域网的终端设备提供到所述广域网的接入点，所述连接设备包括：

注册装置，当向还未注册认证信息的终端设备提供接入点时，所述注册装置从所述终端设备接收与所述终端设备相关的识别信息，注册包括与所述终端设备相关的识别信息的认证信息，并向所述终端设备传输与所述连接设备相关的识别信息；

认证装置，当不同于所述连接设备的外部连接设备向已注册认证信息的所述终端设备提供接入点时，所述认证装置通过对与所述终端设备相关的识别信息和由所述注册装置注册的认证进行交叉校验，而经由所述广域网来为所述终端设备进行接入认证，所述识别信息由所述外部连接设备经由所述广域网来传输；和

提供装置，当向已注册认证信息的终端设备提供接入点时，所述提供装置从所述终端设备接收与注册所述认证信息的连接设备相关的识别信息和与所述终端设备相关的识别信息，基于与所述连接设备相关的识别信息经由所述广域网建立与所述连接设备的连接，将与所述终端设备相关的识别信息经由所述连接传输到所述连接设备，并基于由所述连接设备为所述终端设备进行的接入认证而向所述终端设备提供所述接入点。

5. 如权利要求 4 所述的连接设备，还包括周期注册删除装置，用于在自所述注册装置注册开始已经过去了预定时间段后删除与终端设备相关的认证信息的注册。

6. 如权利要求 4 或 5 所述的连接设备，还包括实例注册删除装置，用于当与由所述注册装置注册的终端设备相关的认证信息的实例达到预定数量时，从与先前注册的终端设备相关的认证信息中依序删除注册。

7. 如权利要求 4 或 5 所述的连接设备，还包括管理终端设备，用于管理由所述注册装置注册的与终端设备相关的认证信息。

8. 如权利要求 3 到 5 中任何一项所述的连接设备，其中与所述终端设备相关的所述识别信息是媒体接入控制地址。

9. 如权利要求 3 到 5 中任何一项所述的连接设备，其中与所述终端设备相关的所述识别信息与安装到所述终端设备上的可更换设备有关。

10. 如权利要求 3 到 5 中任何一项所述的连接设备，其中与所述连接设备相关的所述识别信息是媒体接入控制地址或广域网上的全局因特网协议地址。

11. 如权利要求 3 到 5 中任何一项所述的连接设备，其中所述广域网是因特网；而且所述无线网络是能够连接多个终端设备的无线局域网。

12. 一种终端设备，用于通过由连接设备基于接入认证经由无线网络来提供到广域网的接入点而接入所述广域网，所述接入认证是通过验证已注册的认证信息来进行的，所述终端设备包括：

 终端注册装置，在已注册认证信息的情况下，当由所述连接设备提供接入点时，所述终端注册装置将与所述终端设备相关的识别信息传输到所述连接设备，从所述连接设备接收与所述连接设备相关的识别信息，并存档所述信息；和

 终端提供装置，在已注册认证信息的情况下，当由不同于所述连接设备的外部连接设备提供接入点时，所述终端提供装置将与所述连接设备相关的存档识别信息、与所述终端设备相关的识别信息传输到所述外部连接设备。

13. 如权利要求 12 所述的终端设备，包括可更换的识别信息存储器，用于存储与所述终端设备相关的所述识别信息，用于传输到所述连接设备。

14. 一种方法，用于对经由无线通信连接到多个连接设备中任何一个的终端设备进行认证，所述连接设备连接到广域网并经由所述广域网交换数据，所述方法包括以下步骤：

 基于对于多个所述终端设备中的每一个的初始认证，为该终端设备存档认证信息，其中所述初始认证是在其认证信息未被存档在所述多个连接设备中的任何一个之中的终端设备经由所述无线通信连接到所述广域网时执行的，其中所述认证信息与识别该终端设备的识别信息相关；以及

当包括在所述多个连接设备中的外部连接设备从请求连接到所述广域网的终端设备接收到识别所述请求连接的终端设备的识别信息，并且当所述外部连接设备中没有与所述请求连接的终端设备的识别信息相关的认证信息时，对所述请求连接的终端设备执行接入认证，并将认证结果经由所述广域网传输到所述外部连接设备。

15. 一种方法，用于在接入点系统中进行接入认证，所述方法包括以下步骤：

在多个物理位置配备连接设备以经由无线网络来向终端设备提供到广域网的接入点，

为请求接入所述广域网的所述终端设备验证已注册的认证信息，

在由所述连接设备向还未注册所述认证信息的所述终端设备提供所述接入点的情况下：

从所述终端设备接收与所述终端设备相关的识别信息，

注册认证信息，所述认证信息包括与所述终端设备相关的所述识别信息，

将与所述连接设备相关的识别信息传输到所述终端设备，以及

在由不同于所述连接设备的外部连接设备向在所述连接设备中已注册认证信息的所述终端设备提供所述接入点的情况下：

从所述终端设备接收与所述连接设备相关的识别信息和与所述终端设备相关的识别信息，

基于与所述连接设备相关的识别信息经由所述广域网建立与所述外部连接设备的连接，

将与所述终端设备相关的识别信息经由所述连接从所述外部连接设备传输到所述连接设备，以及

通过对所述终端设备的识别信息和所述已注册的认证信息进行交叉校验而为所述终端设备进行接入认证，并通过所述外部连接设备来向所述终端设备提供接入点。

用于广域网的接入认证系统、设备和方法

技术领域

本发明涉及用于广域网的接入认证技术，更具体而言，涉及用于连接设备的认证技术，所述连接设备向终端设备提供经由无线网络到广域网的接入点，由此通过验证请求接入广域网的终端设备的认证信息来进行接入认证。

背景技术

在一个具有位于多个物理位置的连接设备的接入点系统中，所述连接设备向终端设备提供经由无线网络到广域网的接入点，当终端设备请求连接设备以和广域网通信时，通过验证注册终端设备的认证信息来试图避免对接入点系统的未经授权的使用。传统地，通过为接入系统中正使用的所有终端设备进行认证信息的集成管理的认证服务器来完成接入认证。

例如，日本早期公开专利公报 No.2002-124952 公开了一种由认证服务器所使用的接入认证技术，该认证服务器为接入系统中正使用的所有终端设备进行认证信息的集成管理。

但是，在接入认证依赖于对认证信息进行集成管理的认证服务器的情况下，所述系统具有这样的弱点，即，如果认证服务器因为某个原因而出故障了，那么将没有一个终端设备能够接入系统；而且，在许多接入认证集中在单个认证服务器的情况下，对认证所增加的负荷可能导致接入认证中延迟的问题。

发明内容

为了克服上述问题，本发明的一个目的是提供接入认证技术，其能提高接入点系统在终端设备的接入认证方面的稳定性。

为了解决以上问题中的至少一个，本发明提供了一种广域网系统。该

系统包括：

多个连接设备，连接到广域网并经由所述广域网交换数据；和

终端设备，通过无线通信连接到所述连接设备中的任何一个，

其中所述每个单独的连接设备包括：

认证信息存档装置，为多个所述终端设备存档认证信息，所述数据包括用于识别所述终端设备的识别数据；和

认证装置，当从请求连接到所述广域网的终端设备接收到识别所述终端的识别信息，并且当所述连接设备的认证信息存档装置中没有请求连接的所述终端设备的识别信息时，所述认证装置将所述终端设备的认证信息经由所述广域网传输到外部连接设备，并为所述终端设备进行接入认证。

用于认证本发明的广域网系统中的终端设备的方法提供了一种方法，用于对经由无线通信连接到多个连接设备中任何一个的终端设备进行认证，所述连接设备连接到广域网，并经由所述广域网交换数据，所述方法包括以下步骤：

为多个所述终端设备存档认证信息，所述认证信息包括识别所述终端设备和每个单独的连接设备的识别数据；以及

从请求连接到所述广域网的所述终端设备接收所述识别信息，搜索存档在接收到所述识别信息的连接设备中的所述认证信息，当没有请求连接的所述终端设备的识别信息时将所述终端设备的所述识别信息经由所述广域网传输到外部连接设备，并为所述终端设备进行接入认证。

根据此广域网系统及其认证方法，在一个包括连接在广域网中的多个连接设备的系统中，可由许多连接设备以分布的方式进行终端设备的认证。当用能够无线通信的大量连接设备来使得终端设备能接入广域网时，终端设备与广域网的连接并不是固定连接，在一些情况下终端将在许多连接设备之间移动的同时接入网络；在这样的系统中，与对所有终端设备的集成管理相比，这种分布管理模式减少了管理认证数据所需的资源。根据以上描述的本发明的广域网系统及其认证方法，终端设备的认证信息由多个连接设备以分布的方式管理，因此如果例如一个连接设备出现故障，就不会不能对所有的终端设备进行接入认证；并且如果一个终端设备因为认

证信息不能被验证而不能接收接入认证，则其认证信息可由不同的连接设备来重新注册，从而能够进行接入认证。此外，与整个系统中终端设备的接入认证相关的处理负荷可在多个连接设备之间分担。这在终端设备的接入认证中能提高接入点系统的稳定性。此外，可减少接入点管理的负担。还可以增加终端设备用户的方便。

对于包括终端设备识别信息的认证信息，当终端设备接触一个不同的连接设备时，由于该终端知道先前连接到哪个连接设备并由其认证，所以当所述终端设备向一个新的连接设备请求无线连接时，它将优先地通过识别连接设备的连接设备识别信息来标识自己，所述终端设备的认证信息驻留于所述连接设备中。接收到所述连接设备识别信息的连接设备可随后请求由此识别信息识别的连接设备来认证所述终端设备，所述终端设备的认证信息驻留于由此识别信息识别的连接设备中。用此布置，终端设备可容易地由一个不同连接设备来认证。

在这样一种接入认证系统及其方法中，终端设备的认证信息向一个为还未注册其认证信息的终端设备提供接入点的连接设备来注册。当一个已注册认证信息的终端设备随后由一个不同（外部）的连接设备来提供接入点，则基于向先前提供接入点的连接设备注册的认证信息来进行所述终端设备的接入认证。这样，由于终端设备的认证信息由多个连接设备以分布的方式管理，所以如果例如一个连接设备出现故障，就不会不能对所有的终端设备进行接入认证；并且如果一个终端设备因为认证信息不能被验证而不能接收接入认证，则其认证信息可由不同的连接设备来重新注册，从而能够进行接入认证。此外，与整个系统中终端设备的接入认证相关的处理负荷可在多个连接设备之间分担。这在终端设备的接入认证中能提高接入点系统的稳定性。此外，可减少接入点管理的负担。还可以增加终端设备用户的方便。

在以上描述的各种广域网系统和认证方法中采用的连接设备可采用许多可想到的实施例中的任何一种。用这样的连接设备，如果一个不同连接设备从一个特定终端设备接收到接入广域网的请求，自身已经为此终端注册了认证信息的连接设备，将替代另一个连接设备来进行接入认证。另一

方面，自身并未为一个特定终端设备注册认证信息的连接设备，如果从此终端接收到接入广域网的请求时，将基于已为此终端设备注册认证信息的不同连接设备的接入认证，来向所述终端设备提供接入点。于是，由于多个连接设备以分布的方式来注册/管理终端设备的认证信息，所以如果例如一个连接设备出现故障，就不会不能对所有的终端设备进行接入认证；并且如果一个终端设备因为认证信息不能被验证而不能接收接入认证，则其认证信息可由不同的连接设备来重新注册。此外，与整个系统中终端设备的接入认证相关的处理负荷可在多个连接设备之间分担。这在终端设备的接入认证中能提高接入点系统的稳定性。此外，可减少接入点管理的负担。

具有以上描述布置的本发明的连接设备可采用以下实施例。终端设备的识别信息可由 MAC 地址组成。用这种连接设备，连接设备通过交叉校验终端设备的 MAC 地址和其注册的认证信息来进行接入认证。这样，由于 MAC 地址是单独分配给硬件网络设备的唯一数字（即世界上仅有一个），连接设备可认为用给定终端设备硬件来接入网络的任何用户是同一个给定用户而来进行接入认证。这使得终端设备的用户能使用所述终端设备来接入广域网，而无需输入密码或其它识别数据。

与终端设备相关的识别信息可由与配备在所述终端设备上的可交换识别信息装置相关的识别信息组成。用这种终端设备，将与配备在所述终端设备上的可交换识别信息装置相关的识别信息和已注册认证信息交叉校验来进行接入认证。于是，拥有多个终端设备的用户可以将所述识别信息装置从一个已注册终端设备替换到另一个未注册终端设备中，从而允许使用此另一个终端设备来接入广域网，而无需重新注册认证信息。例如，可能的配备在个人计算机终端设备上的可交换识别信息装置包括 PC 卡、USB 密钥等等。

与连接设备相关的识别信息可至少由 MAC 地址或广域网上的全局 IP 地址组成。用这样的连接设备，当所述连接设备向已注册认证信息的终端设备提供接入点时，至少基于 MAC 地址或广域网上的全局 IP 地址建立起经由广域网到另一个已注册认证信息的连接设备的连接。这样，由于

MAC 地址是单独分配给硬件网络设备的唯一数字（即世界上仅有一个），连接设备可在广域网上识别管理终端设备的认证信息的另一个连接设备。

可配备周期注册删除装置，用于在自所述注册装置注册开始已经过去了预定时间段后删除与终端设备相关的认证信息的注册。用这种连接设备，所述连接设备检查相继注册的认证信息的多个例子并依序删除那些自注册以来已经过去了预定时间段的例子，以保证足够的存储容量来注册新的认证信息。于是，可减少存储认证信息的必要存储容量，可周期性地更新认证信息，并且可删除不再使用连接设备的终端设备的认证信息。

可配备实例注册删除装置，用于当与由所述注册装置注册的终端设备相关的认证信息的例子达到预定数量时，从与先前注册的终端设备相关的认证信息中依序删除注册。用这种连接设备，一旦相继注册的认证信息的多个例子达到特定数量，则所述连接设备按从最早开始的顺序来删除先前注册的例子，以保证足够的存储容量来注册新的认证信息。于是，可减少存储认证信息的必要存储容量，可存档认证信息直到存储容量变满，并且可删除不再使用连接设备的终端设备的认证信息。

可配备管理终端设备，用于管理与由所述注册装置注册的终端设备相关的认证信息。用这种连接设备，由连接设备注册的认证信息的部分或所有管理过程可由一个与所述连接设备分开的管理终端设备来进行。于是，可减少连接设备中管理认证信息的处理负荷，并且连接设备管理者可通过操作管理终端设备来从相对连接设备较远的位置来管理认证信息。

前述广域网可以是例如因特网，而前述无线网络可以是多个终端设备可与之连接的无线局域网。于是，通过在广阔的不同位置中安装连接设备并使多个终端设备连接到单个连接设备上，可增加向终端设备提供接入点的方便。

在与所述接入认证系统的终端设备相关的一个方面中，本发明提供了一种终端设备，通过由连接设备基于接入认证经由无线网络来向其提供到广域网的接入点来接入广域网，其中通过验证已注册的认证信息来进行接入认证，所述终端设备包括：

终端注册装置，在还未注册认证信息的情况下，当由所述连接设备提供接入点时，所述终端注册装置将与所述终端设备相关的识别信息传输到所述连接设备，从所述连接设备接收与所述连接设备相关的识别信息，并存档所述信息；和

终端提供装置，在已注册认证信息的情况下，当由不同于所述连接设备的外部连接设备提供接入点时，所述终端提供装置将与连接设备相关的存档识别信息、与所述终端设备相关的识别信息传输到所述外部连接设备。

根据此终端设备，所述终端设备在存储器中存储与连接设备相关的识别信息，已在所述连接设备中注册了终端设备的认证信息。如果终端设备随后由一个不同的连接设备提供接入点，它通过向此另一个连接设备传输与在其中注册终端设备认证信息的连接设备相关的识别信息来接受接入认证。这样，假如已经在一个特定连接设备中注册了终端设备的认证信息，则该终端设备当由一个不同的连接设备来提供接入点时，可接入广域网而无需重新注册其认证信息。

具有以上描述的布置的本发明的终端设备可采用以下实施例。可配备可交换的识别信息装置，用于存储与终端设备相关的识别信息并传输到连接设备。于是，拥有多个终端设备的用户可以将所述识别信息装置从一个已注册终端设备替换到另一个未注册终端设备中，从而允许使用此另一个终端设备来接入广域网，而无需重新注册认证信息。

附图说明

图 1 图示了本发明的一个实施例中一个完整接入点系统 10 的系统简图。

图 2 是示出在本发明的初始接入认证期间由连接设备 20a 的控制设备 210a 和终端设备 30 的控制设备 311 所执行过程的流程图。

图 3 是示出本发明中由连接设备 20b 的控制设备 210b 在接入认证例程期间所执行过程的流程图。

图 4 是示出本发明中由连接设备 20a 的控制设备 210a 在接入认证例程

期间所执行过程的流程图。

图 5 是示出本发明中由终端设备 30 的控制设备 311 在接入认证例程期间所执行过程的流程图。

图 6 图示了描述本发明中接入认证例程的序列简图。

图 7 是示出由连接设备 20a 的控制设备 210a 所执行的信息管理过程的流程图。

具体实施方式

通过以下对实施本发明的接入点系统的描述，提供了对本发明的设计和优点更充分的理解，其中将采用无线局域网（以下称为无线 LAN）的接入点系统作为其例子。

图 1 是本发明的一个实施例中一个完整接入点系统 10 的系统简图。接入点系统 10 利用广域网，即因特网 50。接入点系统 10 包括连接设备 20a、20b、20c。这些连接设备 20a、20b、20c 通过无线 LAN 连接到终端设备 30。这些无线 LAN 可以是符合 IEEE 802.11b 标准的无线 LAN。在图 1 中，未示出所有的终端设备 30；但是，在实际情况中多个终端设备 30 将连接到接入点系统 10。连接设备 20a、20b、20c 的数量并不限于三个；两个或更多中的任何数量都是可以的。

路由器 40a、40b、40c 连接到因特网 50。连接设备 20a、20b、20c 又分别连接到路由器 40a、40b、40c。路由器 40a、40b 将不同网络互连，即因特网 50 和连接设备 20a、20b、20c 的无线 LAN。这样，连接设备 20a、20b、20c 可以经由因特网 50 交换数据，而且还可以在连接设备 20a、20b、20c 之间交换数据。

响应于来自终端设备的接入请求，即接入因特网 50 的请求，连接设备 20a、20b、20c 在通过验证注册认证信息的接入认证的基础上，经由无线 LAN 向因特网 50 提供接入点。进行接入认证是为了仅仅将接入点提供给由特定个人使用的终端设备 30，该个人已被授权来使用接入点系统 10。认证信息是预注册数据，用于验证终端设备 30 是否属于被授权来使用所述系统的用户。如果对识别用户并由终端设备 30 传输的识别信息以

及所注册的认证信息的交叉校验，使得连接设备 20a、20b、20c 能够认证终端设备 30 属于被授权来使用所述系统的用户，则在终端设备 30 和服务器 60 等之间中继数据。这样，为了与连接到因特网 50 上的服务器 60 等交换数据，终端设备 30 可以经由连接设备 20a、20b、20c 而接入因特网 50。终端设备 30 接入因特网 50 的示例模式包括访问 web 内容、发送和接收电子邮件以及网络电话。

连接设备 20a、20b、20c 可以向位于无线区 25a、25b、25c 内的终端设备 30 提供接入点，所述无线区是其中可以通过各个无线 LAN 连接到终端设备 30 的范围。在图 1 中，为了示出位于无线区 25a 中的终端设备 30 随后移到无线区 25b 和 25c，该终端设备 30 在那些区中用双点划线/虚线示出。

现在描述连接设备 20a、20b、20c 的内部体系结构。连接设备 20a 包括以下：具有 CPU、ROM、RAM 等的控制单元 210a；存储设备 220a，例如硬盘驱动器（HDD）；和对因特网 50、无线 LAN 等等的接口。控制单元 210a 执行与为终端设备 30 提供接入点相关的各种过程。存储设备 220a 存储由控制单元 210a 执行的过程所产生的数据，而且还在其中存档由制造商分配给连接设备 20a 的唯一 MAC 地址。当连接设备 20a 链接到路由器 40a，控制单元 210a 在存储设备 220a 中存储路由器 40a 的全局 IP 地址（该地址使其能在因特网 50 上被识别）。当其它连接设备 20b、20c 和此连接设备 20a 交换数据时，所述 MAC 地址和 IP 地址就用作对连接设备 20a 的识别信息以使连接设备 20a 能在因特网 50 上被识别。此识别信息并不限于 MAC 地址和 IP 地址；使连接设备 20a 能在因特网 50 上被识别的任何信息都是可接受的。对连接设备 20b、20c 类似地分别提供控制设备 210b、210c 和存储设备 220b、220c，以及对因特网 50、无线 LAN 等等的接口。连接设备 20a、20b、20c 并不限于具有板载的控制设备 210a、210b、210c 和存储设备 220a、220b、220c；这些设备中的一些或全部都可通过无线或有线连接提供。

现在描述终端设备 30 的内部体系结构。终端设备 30 可以是一般的移动计算机，其包括 CPU、ROM、RAM、HDD、PCMCIA 接口 320、显示

器 330、键盘 340 等等。此终端设备 30 具有可从 PCMCIA 接口 320 移去的无线卡 310。通过配备无线卡 310，终端设备 30 可经由无线 LAN 连接到连接设备 20a、20b、20c。

配备给终端设备 30 的无线卡 310 包括以下：控制设备 311，具有 CPU、ROM、RAM 等等；存储设备 312，如 EEPROM 的非易失性存储器；无线 LAN 接口等等。控制单元 311 执行与由连接设备 20a、20b、20c 提供接入点相关的各种过程。存储设备 312 存储由控制单元 311 执行的过程所产生的数据，而且还在其中存档由制造商分配给无线卡 310 的唯一 MAC 地址。在连接设备 20a、20b、20c 进行接入认证期间，所述 MAC 地址就用作对终端设备 30 的识别信息以使终端设备 30 能被识别。此识别信息并不限于 MAC 地址；在接入认证期间使连接设备 20a、20b、20c 能识别终端设备 30 的用户的任何信息都是可接受的。终端设备 30 并不限于具有可更换无线卡 310 的设备；具有板载集成无线卡 310 功能的便携式信息终端或其它终端都是可接受的。

现在描述在对当前未注册的终端设备 30 的接入认证期间由连接设备 20a 进行的初始接入认证。图 2 是示出在本发明的初始接入认证期间由连接设备 20a 的控制设备 210a 和终端设备 30 的控制设备 311 所执行过程的流程图。在图 2 中，由连接设备 20a 的控制设备 210a 执行的过程的流程图在右边示出，而由终端设备 30 的控制设备 311 执行的过程的流程图在左边示出。

当终端设备 30 向连接设备 20a 提出接入请求以请求接入广域网时，如果终端设备 30 的控制设备 311 以前从未接受过接入认证，或者如果已收到后面描述的注册请求，那么终端设备 30 的控制设备 311 启动图 2 中左边所示的过程。当该过程开始时，执行用户识别信息输入过程来读取由终端设备 30 的用户输入的用户识别信息（步骤 S110）。在此用户识别信息输入过程中，控制设备 311 读取由终端设备 30 的用户经由键盘 340 或其它方法输入的用户识别信息。此用户识别信息是先前提供给终端设备 30 的用户的密码，该用户被授权来使用接入点系统 10。

在完成用户识别信息输入过程（步骤 S110）之后，终端设备 30 的控

制设备 311 将在用户识别信息输入过程期间读取的用户识别信息（即密码）和无线卡 310 的 MAC 地址（作为终端设备 30 的识别信息在存储设备 312 中预存档）经由连接设备 20a 的无线 LAN 传输到连接设备 20a（步骤 S120）。

当连接设备 20a 的控制设备 210a 收到从终端设备 30 传输来的用户识别信息和终端设备 30 识别信息时，它就启动在图 2 的右边示出的过程。当该过程开始时，用户识别信息和终端设备 30 识别信息就被接收和读取（步骤 S210），并执行初始认证（步骤 S220）。此初始认证包括分析用户识别信息（密码）以验证该终端设备 30 的用户被授权来使用接入点系统 10。初始认证并不限于密码认证；使终端设备 30 的用户能被识别的其它认证方法是可接受的。例如，信用卡认证就是可接受的。信用卡认证包括向信用卡发行者的验证服务器验证终端设备 30 用户的信用卡号，连接设备 20a 经由因特网 50 等等连接到该验证服务器。

当完成初始认证（步骤 S220）时，用于当前接入认证的来自终端设备 30 的认证信息作为数据在存储设备 220a 中存档，以为终端设备 30 注册认证信息（步骤 S230）。在存储器中存储与其它信息相关联的此认证信息，以及进行注册过程的日期、用户名、会员号等等，所述其它信息例如在步骤 S210 中读取的终端设备 30 识别信息。认证信息并不限于上面提到的这种信息；在管理接入认证和识别信息中使用的信息也是可接受的。随后，将在存储设备 220a 中存档的连接设备 20a 的识别信息，即连接设备 20a 的 MAC 地址和路由器 40a 的 IP 地址，经由连接设备 20a 的无线 LAN 传输到终端设备 30（步骤 S240）。然后就允许给终端设备 30 提供接入点（步骤 S250），而过程也终止了。

同时，当连接设备 20a 传输连接设备 20a 的识别信息（步骤 S240）时，终端设备 30 的控制设备 311 就接收此识别信息并读取（步骤 S130），并且将其存储在存储设备 312 中（步骤 S140）。当连接设备 20a 随后允许提供接入点（步骤 S250）时，就建立起因特网连接（步骤 S150），而且该过程结束。这样，就通过连接设备 20a 向终端设备 30 提供了接入点，使其能够和因特网 50 交换数据。

现在描述接入认证例程，连接设备 20b 通过该接入认证例程来为已经注册了认证信息的终端设备 30 进行接入认证。图 3 是示出本发明中由连接设备 20b 的控制设备 210b 在接入认证例程期间所执行过程的流程图。图 4 是示出本发明中由连接设备 20a 的控制设备 210a 在接入认证例程期间所执行过程的流程图。图 5 是示出本发明中由终端设备 30 的控制设备 311 在接入认证例程期间所执行过程的流程图。图 6 是描述本发明中接入认证例程的序列简图。

一旦终端设备 30 的控制设备 311 已经完成前述初始接入认证并接收到由连接设备 20a 提供的接入点，如果终端设备 30 随后移动到连接设备 20b 的无线区 25b 中，它就向连接设备 20b 提出接入请求。接收到此接入请求的连接设备 20b 的控制设备 210b 则请求终端设备 30 发送终端设备 30 的识别信息，以及终端设备 30 在其中注册了认证信息的连接设备的识别信息。

当终端设备 30 的控制设备 311 从连接设备 20b 接收到对于识别信息的此请求，它就启动图 5 中所示的过程。当该过程开始时，终端设备 30 的识别信息，即在存储设备 312 中预存档的无线卡 311 的 MAC 地址，以及注册了认证信息的连接设备 20a 的识别信息，即在前述初始接入认证期间在存储设备 312 中存档的连接设备 20a 识别信息，被经由连接设备 20b 的无线 LAN 而传输到连接设备 20b（步骤 S510，图 6 中所示的过程（1））。

当连接设备 20b 的控制设备 210b 从终端设备 30 接收到终端设备 30 的识别信息和连接设备 20a 的识别信息，它就启动图 3 中所示的过程。当该过程开始时，接收到并读取终端设备 30 的识别信息和连接设备 20a 的识别信息（步骤 310）。随后确定所接收到的连接设备的识别信息是否是正在接收的连接设备自己的识别信息（步骤 S320）。在本例中，终端设备 30 传输连接设备 20a 的识别信息，这意味着终端设备 30 的认证信息是向另一个设备即连接设备 20a 注册的。一旦确定认证信息由另一个设备保存（步骤 S320），则基于连接设备 20a 的识别信息在因特网 50 上识别连接设备 20a，并且建立起使其能经由因特网 50 和连接设备 20a 通信的连接（步骤

330)。终端设备 30 的识别信息在此连接上被发送到连接设备 20a，而且认证被协商(步骤 S340，图 6 中所示的过程(2))。

当连接设备 20a 的控制设备 210a 经由因特网 50 从连接设备 20b 接收到认证协商时，它就启动图 4 中所示的过程。当该过程开始时，接收并读取终端设备 30 的识别信息(步骤 S410)。随后将所读取的终端设备 30 的识别信息与在前述初始接入认证期间在存储设备 220a 中存档的认证信息进行交叉校验(步骤 S420，图 6 中所示的过程(3))。如果已经注册了认证信息而终端设备 30 可被认证(步骤 S430)，则将大意是认证成功的应答经由因特网 50 发送到连接设备 20b(步骤 S440，图 6 中所示的过程(4))，过程结束。相反，如果未注册认证信息而终端设备 30 不能被认证(步骤 S430)，则将大意是认证失败的应答经由因特网 50 发送到连接设备 20b(步骤 S450)，并且过程终止。

如果连接设备 20b 的控制设备 210b 经由因特网 50 从连接设备 20a 接收到大意是认证成功的应答(步骤 S350)，它就授权向终端设备 30 提供接入点(步骤 S360，图 6 中所示的过程(5))，并结束过程。如果相反，经由因特网 50 从连接设备 20a 接收到大意是认证失败的应答(步骤 S350)，则它就经由连接设备 20b 的无线 LAN 请求终端设备 30 向连接设备 20b 注册认证信息(步骤 390)，并结束过程。

如果终端设备 30 的控制设备 311 经由连接设备 20b 的无线 LAN 从连接设备 20b 接收到提供接入点的授权，它就建立起到因特网的连接(步骤 S530，图 6 中所示的过程(6))，并终止过程。这样，终端设备 30 接收由连接设备 20b 提供的接入点，使其能和因特网 50 交换数据。如果相反，它从连接设备 20b 接收到注册的请求，而非提供接入点的授权(步骤 S520)，则向连接设备 20b 进行前面所述在图 2 中示出的初始接入认证过程(步骤 S540)。随后过程终止。

在此例中，终端设备 30 的认证信息是向连接设备 20a 注册的，但是如果是已向例如连接设备 20b 注册，则连接设备 20b 与终端设备 30 的认证信息向连接设备 20a 注册的情况不同地来对终端设备 30 的接入认证进行接入认证例程，现在描述这个过程。在此情况下，在图 3 中所示的步骤 S310

已经完成之后，连接设备 20b 的控制设备 210b 确定认证信息是否是向自己注册的（步骤 S320），而且将所读取的终端设备 30 的识别信息与在存储设备 220b 中存档的认证信息进行交叉校验（步骤 S370）。随后，如果已经注册认证信息而终端设备 30 可被认证（步骤 S380），则授权向终端设备 30 提供接入点（步骤 S360），而且过程终止。如果相反，未注册认证信息而终端设备 30 不能被认证（步骤 S380），则连接设备 20b 经由连接设备 20b 的无线 LAN 来请求终端设备 30 向连接设备 20b 注册认证信息（步骤 S390），并终止过程。

在本例中，已经描述了已向连接设备 20a 注册的终端设备 30 移动到连接设备 20b 的情况，但是如果它随后从连接设备 20b 移动到连接设备 20c 过程将是类似的。也就是说，在此情况下连接设备 20c 将和连接设备 20a 协商认证，并确定是否向终端设备 30 提供接入点。

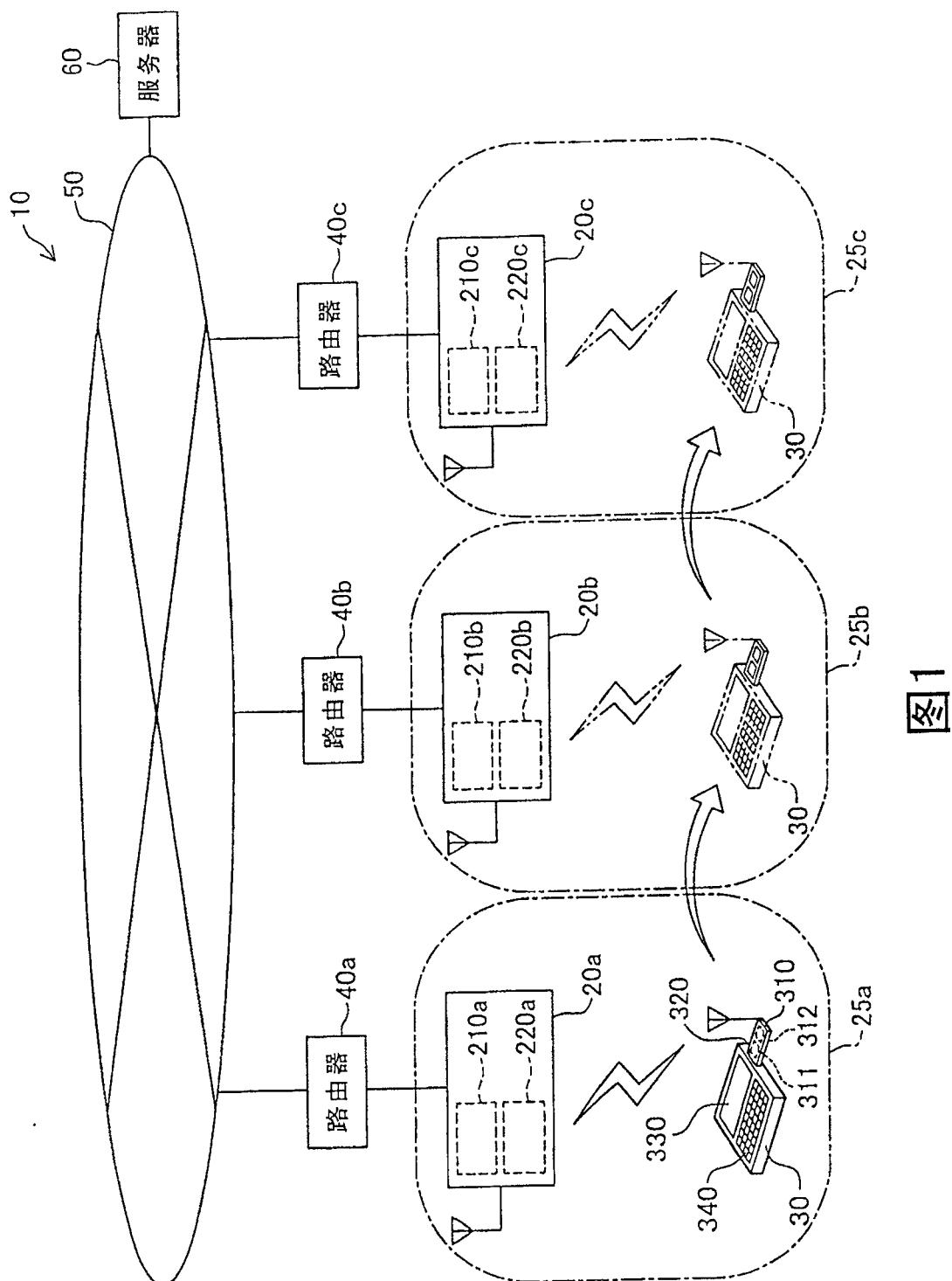
现在描述信息管理过程，连接设备 20a 的控制设备 210a 通过该过程来管理在存储设备 220a 中存档的认证信息。图 7 是示出由连接设备 20a 的控制设备 210a 执行的信息管理过程的流程图。连接设备 20a 的控制设备 210a 在预定定时下执行此信息管理过程。当图 7 中所示的过程开始时，读取进行注册过程的日期（该日期在前述初始接入认证中作为和认证信息相关的数据在存储设备 220a 中存档）（步骤 S710）。然后确定自认证信息最近被注册以来是否已经过去了预定的时间段（例如一个月）（步骤 S720）。如果自注册以来已经经过了预定时间段（步骤 S720），则从存储设备 220a 中删除所述认证信息（步骤 S730）。如果相反，自注册以来还未经过预定时间段（步骤 S720），则不删除所述认证信息。接着，如果对在存储设备 220a 中存档的所有认证信息已经完成了此过程（步骤 S740），则过程终止。另一方面，如果还没有对所有认证信息完成该过程（步骤 S740），则在步骤 S710 处开始重复此过程。在连接设备 20b、20c 的控制设备 210b、210c 中类似地进行所述信息管理过程。

可以参考各种因素，例如存储设备 220a 的存储容量、安全考虑等等，来选择自注册开始的预定时间间隔，该间隔用作删除认证信息的基准。或者，如果在信息管理过程中删除认证信息的条件是当认证信息的注册达到

预定数量的例子，则可以从最早开始依序删除与以前注册的终端设备相关的认证信息。可以通过将一个诸如一般计算机的管理终端设备通过 LAN 等等连接到连接设备 20a，而执行认证信息存档和信息管理过程。

在上述例子中，对于其认证信息由连接设备 20a 来管理的终端设备 30，当连接设备 20b 或 20c 接收到来自终端设备 30 的接入请求时，连接设备 20a 进行接入认证，而不是连接设备 20b 或 20c。另一方面，对于其认证信息不由连接设备 20b 或 20c 来管理的终端设备 30，当这些连接设备中的任一个接收到来自终端设备 30 的接入请求时，则基于由连接设备 20a 进行的接入认证而向终端设备 30 提供接入点，其中连接设备 20a 保存终端设备 30 的认证信息。这样，由于终端设备的认证信息是以在连接设备中分布的方式来管理的，所以如果连接设备中的一个出故障了，就不会不能对所有的终端设备进行接入认证；而且其认证信息由有故障的服务器管理的终端设备可通过不同的连接设备来重新注册其认证信息。此外，与整个系统中终端设备的接入认证相关的处理负荷可在连接设备间分担。这在终端设备的接入认证中能提高接入点系统的稳定性。

尽管以上已经参考某些优选实施例来示出和描述了本发明，但本发明并不限于此并可采用任何不同的其它实施例而不偏离本发明的范围和精神。例如，在以上例子中，终端设备 30 的识别信息是配备在终端设备 30 上的可交换无线卡 310 的 MAC 地址，但或者也可是终端设备 30 的 MAC 地址，或者配备在终端设备 30 上的可交换 USB 密钥或其它设备的 MAC 地址。虽然这里用 MAC 地址和 IP 地址作为连接设备 20a 和终端设备 30 的识别信息，但或者也可用使每个设备可被识别的密码或其它数据。连接设备 20a 可配备有路由器的功能并直接连接到因特网 50，而非经过路由器 40。连接设备 20a、20b、20c 接入的网络并不限于因特网 50，或者也可是其它一些广域网；由连接设备 20a、20b、20c 向终端设备 30 提供的网络并不限于无线 LAN，或者也可是其它种类的无线网络。



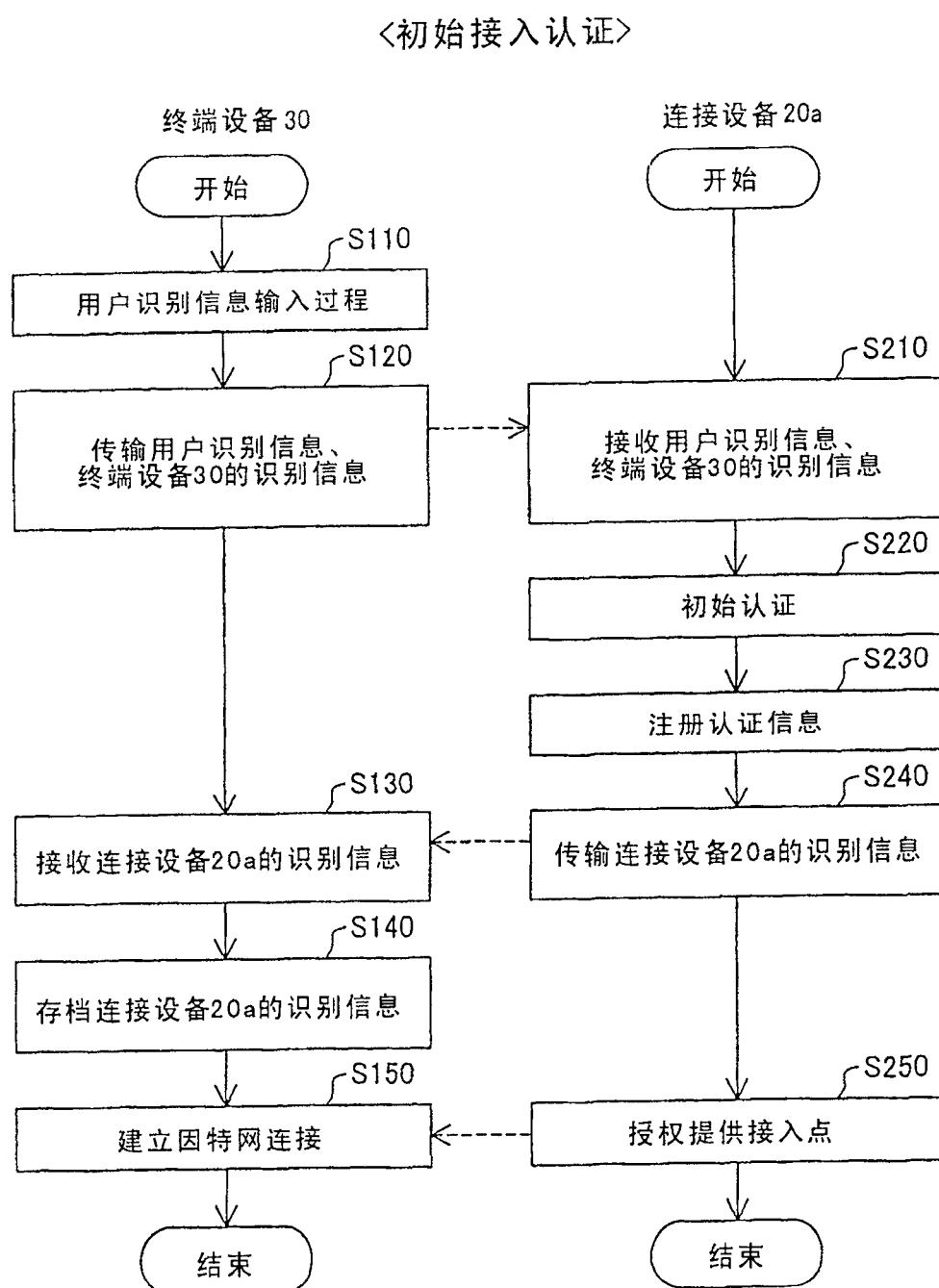


图2

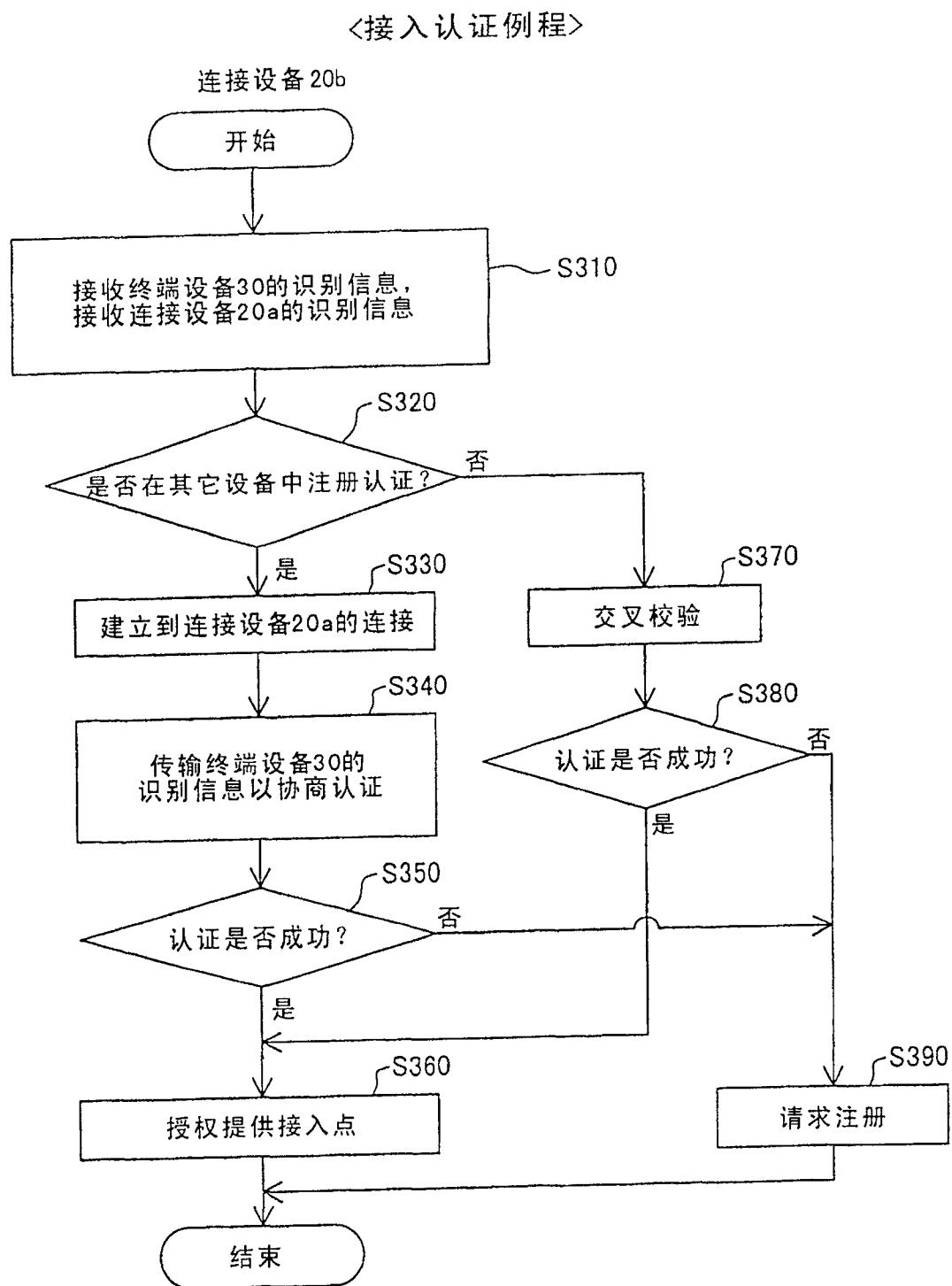


图3

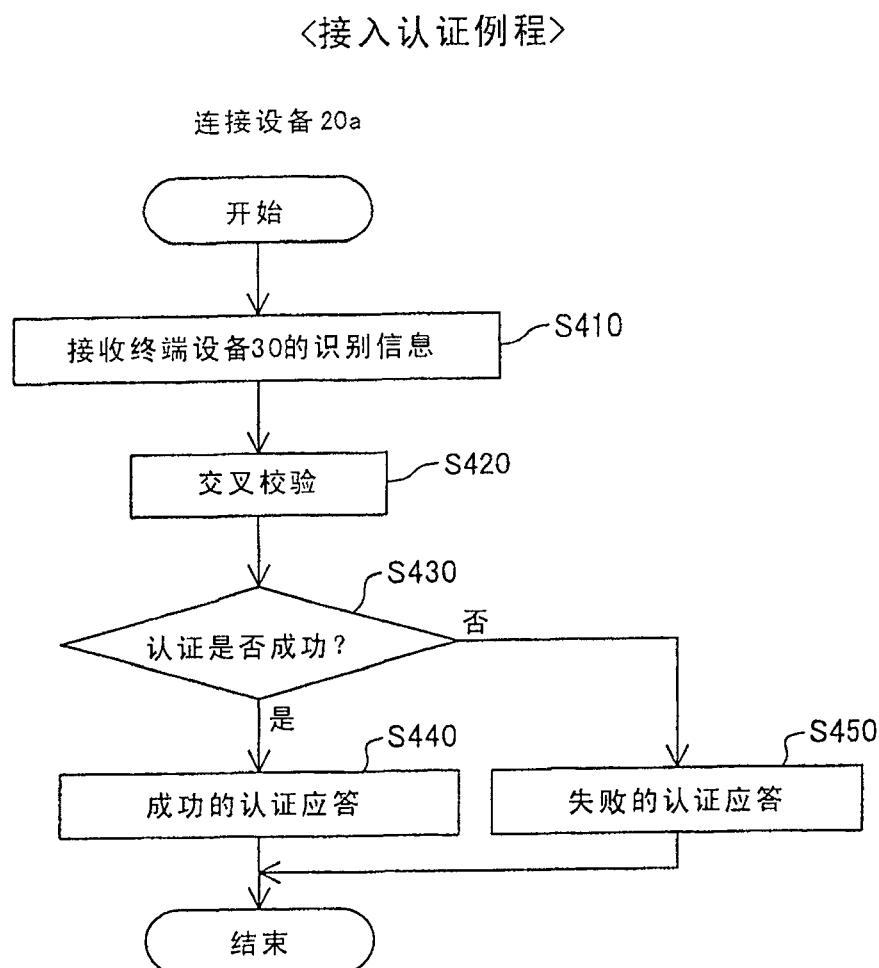


图4

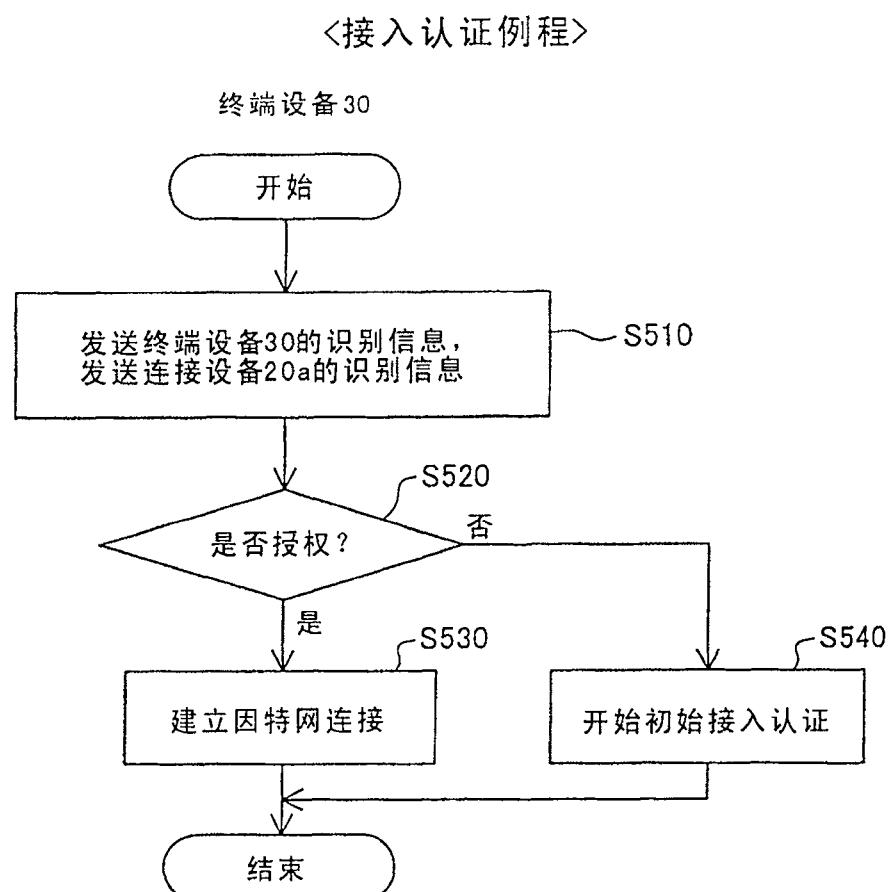


图5

<接入认证例程>

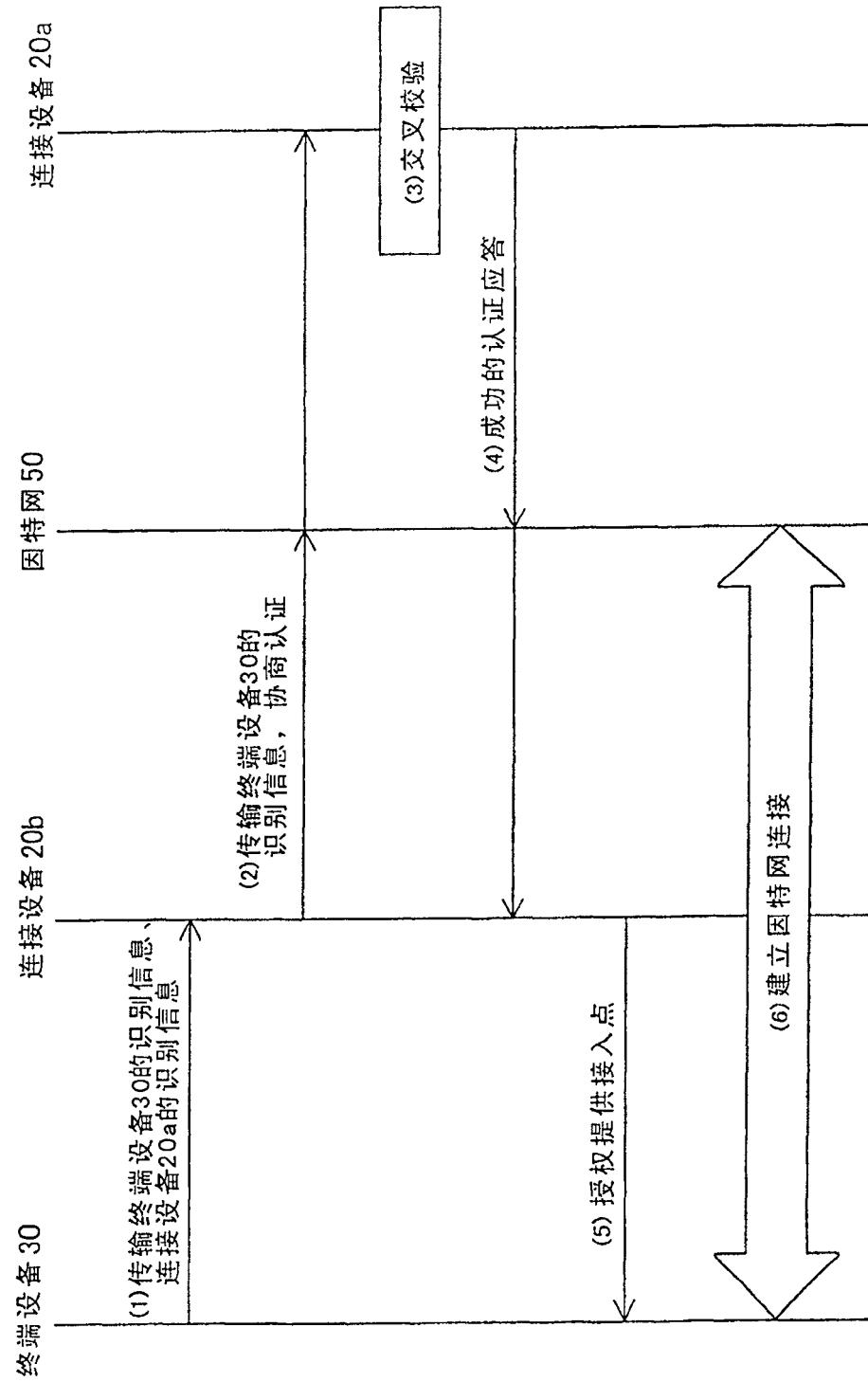


图6

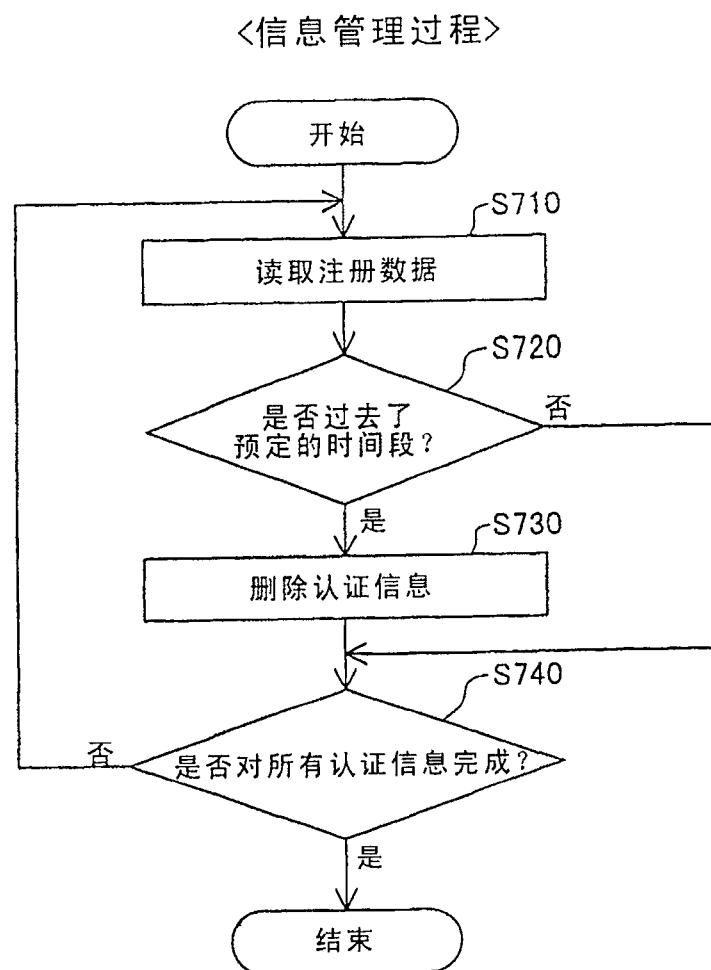


图7