(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 109561065 A
(43)申请公布日 2019.04.02

(21)申请号 201811131520.0

(22)申请日 2018.09.27

(30)优先权数据
2017-187132 2017.09.27 JP

(71)申请人 佳能株式会社
地址 日本东京都大田区下丸子3丁目30番2号

(72)发明人 小林真琴

(74)专利代理机构 北京魏启学律师事务所 11398
代理人 魏启学

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/08(2006.01)

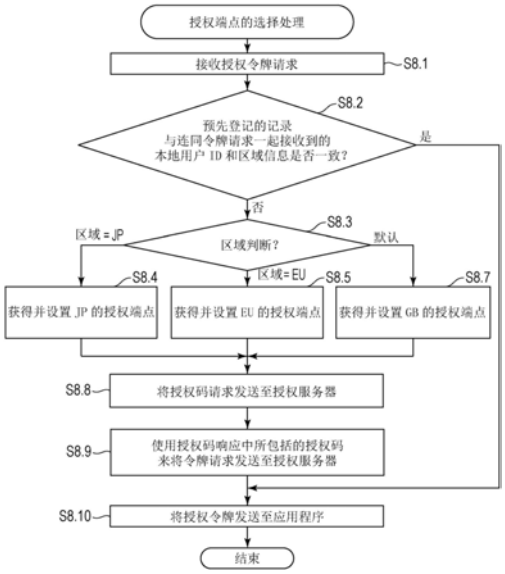
权利要求书3页 说明书12页 附图9页

(54)发明名称

信息处理装置及其控制方法和存储介质

(57)摘要

本发明提供一种信息处理装置及其控制方法和存储介质。装置基于从应用程序接收到的并且与用户相关联的区域信息来识别授权端点，将授权码请求发送至授权端点，并且从授权端点接收与授权码请求相对应的授权码响应。可选地，从装置上的预先存在的信息获得区域信息。



CN 109561065 A

1.一种信息处理装置,包括:

发送部件,用于将供授权服务器发出授权码所用的授权码请求发送至所述授权服务器,所述授权码表示用户许可了所述信息处理装置访问资源服务器;

接收部件,用于从所述授权服务器接收与所述授权码请求相对应的授权码响应;以及

令牌提供器,用于从所述信息处理装置上的应用程序获得用于识别所述授权服务器所在的区域的区域信息,并且基于所获得的区域信息来识别所述授权码请求发送至的授权端点,

其中,所述发送部件将所述授权码请求发送至所识别出的授权端点,以及

所述接收部件接收与所述发送部件所发送的授权码请求相对应的授权码响应。

2.根据权利要求1所述的信息处理装置,其中,

所述令牌提供器具有所述区域信息和所述授权端点之间的关联的关联信息,以及

基于所述关联信息来识别所述授权码请求要被发送至的授权端点。

3.根据权利要求2所述的信息处理装置,其中,

所述信息处理装置将用于发出供所述信息处理装置访问所述资源服务器所用的授权令牌的令牌请求连同所述授权码响应中接收到的授权码一起发送至所述授权服务器,以及

所述授权令牌是响应于所发送的令牌请求而从所述授权服务器获得的。

4.根据权利要求3所述的信息处理装置,其中,

所述区域信息和所述授权端点的所述关联信息包括作为所述令牌请求发送至的发送目的地的令牌端点,以及

将所述令牌请求连同所述授权码一起发送至所述令牌端点。

5.根据权利要求3所述的信息处理装置,还包括判断部件,

其中,由于执行了授权处理使得通过所述用户给出许可而使所述信息处理装置能够访问所述资源服务器,因而所述令牌提供器将作为用于识别登录到所述应用程序的本地用户的信息的本地用户ID、通过所述令牌请求所获得的所述授权令牌、以及用于识别发出了所述授权令牌的所述授权服务器所在的区域的区域信息以关联方式进行管理,

所述判断部件判断从所述应用程序接收到的区域信息和本地用户ID与所述关联信息中的区域信息和本地用户ID是否一致,

在所述判断部件判断为存在一致的情况下,使用所述关联信息所识别的授权令牌,将供所述信息处理装置使用所述资源服务器已公开的服务所用的资源请求发送至所述资源服务器,以及

在所述判断部件判断为不存在一致的情况下,使用与所述区域信息和所述授权端点有关的关联信息、以及从所述应用程序接收到的区域信息所识别的授权端点来将所述授权码请求发送至所述授权服务器。

6.根据权利要求5所述的信息处理装置,其中,

在从所述应用程序接收到的区域信息没有包括在所述关联信息中、或者从所述应用程序不能获得区域信息的情况下,使用默认设置的区域信息以及所述关联信息所识别的授权端点来将所述授权码请求发送至所述授权服务器。

7.根据权利要求1所述的信息处理装置,其中,

在具有作为独立于从所述应用程序接收到的区域信息而预先设置的区域信息的固定

区域信息的情况下，所述令牌提供器判断从所述应用程序接收到的区域信息和所述固定区域信息是否一致，

在判断为这两者一致的情况下，基于所述固定区域信息、以及所述区域信息和所述授权端点的关联信息来获得所述授权端点，并且将所述授权码请求发送至所获得的授权端点，以及

在判断为这两者不一致的情况下，将错误信息发送至所述应用程序。

8.根据权利要求7所述的信息处理装置，其中，

所述固定区域信息与用于识别所述信息处理装置所在的区域的国家代码相关联，所述国家代码是从所述信息处理装置的IP地址获得的。

9.根据权利要求7所述的信息处理装置，其中，

所述令牌提供器包括：

第二判断部件，用于判断所述令牌提供器是否具有作为用于存储固定区域信息的表的固定区域判断表，

其中，在所述第二判断部件判断为所述令牌提供器具有所述固定区域判断表的情况下，基于所述固定区域判断表中所存储的固定区域信息来识别所述授权端点，并且将所述授权码请求发送至所识别出的授权端点，以及

在所述第二判断部件判断为所述令牌提供器不具有所述固定区域判断表的情况下，基于从所述应用程序接收到的区域信息来识别所述授权端点，并且将所述授权码请求发送至所识别出的授权端点。

10.根据权利要求1所述的信息处理装置，其中，

所述区域信息是以下区域信息其中之一：

所述用户在登录到所述信息处理装置时指定的区域信息，以及

基于所述用户在所述信息处理装置上使用的语言所识别的区域信息。

11.根据权利要求1所述的信息处理装置，其中，

所述信息处理装置进行以下操作：

在本地用户登录到所述信息处理装置时生成登录上下文，

判断在所述登录上下文中是否包括所述区域信息，

在判断为在所述登录上下文中包括所述区域信息的情况下，基于所述登录上下文中所包括的所述区域信息来识别作为所述授权码请求发送至的发送目的地的授权端点，以及

在判断为在所述登录上下文中没有包括所述区域信息的情况下，提供用以向所述本地用户请求所述区域信息的输入画面。

12.一种控制方法，用于控制计算机，所述计算机包括发送部件和接收部件，所述控制方法包括：

将供授权服务器发出授权码所用的授权码请求发送至所述授权服务器，所述授权码表示用户许可了装置访问资源服务器；

从所述授权服务器接收与所述授权码请求相对应的授权码响应；

从所述装置上的应用程序获得用于识别所述授权服务器所在的区域的区域信息；

基于所获得的区域信息来识别授权端点；

使用所述发送部件将所述授权码请求发送至所识别出的授权端点；以及

使用所述接收部件接收与所述发送部件所发送的授权码请求相对应的授权码响应。

13.一种非暂时性存储介质,其存储指令,所述指令在由包括一个或多个处理器的装置执行的情况下控制以下部件:

发送部件,用于将供授权服务器发出授权码所用的授权码请求发送至所述授权服务器,所述授权码表示用户许可了所述装置访问资源服务器;以及

接收部件,用于从所述授权服务器接收与所述授权码请求相对应的授权码响应,

其中,所述装置所包括的令牌提供器从所述装置上的应用程序获得作为用于识别所述授权服务器所在的区域的信息的区域信息,

基于所获得的区域信息来识别作为所述授权码请求发送至的发送目的地的授权端点,

所述发送部件将所述授权码请求发送至所识别出的授权端点,以及

所述接收部件接收与所述发送部件所发送的授权码请求相对应的授权码响应。

信息处理装置及其控制方法和存储介质

技术领域

[0001] 本发明通常涉及通过利用授权服务器的访问授权。

背景技术

[0002] 存在如下配置:诸如多功能外围设备(MFP)等的装置具有的应用程序经由该装置具有的令牌提供器从授权服务器获得授权令牌。授权令牌是如下的令牌,该令牌许可授权用户通过授权操作将权限转移至的装置访问资源服务器已公开的应用程序编程接口(API)。使用所获得的授权令牌使得装置能够在无需移交诸如ID、密码信息或授权信息等的用户信息的情况下使用资源服务器已公开的API。如果装置例如是MFP,则该装置可以使用资源服务器提供的诸如打印服务和商业表单服务等的Web服务来显示并打印数据。

[0003] 授权令牌是通过授权服务器执行被称为OAuth 2.0的标准协议的授权流程即授权码授予(Authorization Code Grant)所发出的。具体地,授权服务器通过用户经由Web浏览器授权装置使用资源服务器的Web服务,来向已向该授权服务器发送了令牌请求的令牌提供器发出授权令牌。令牌请求是令牌提供器从授权服务器获得授权令牌的请求。

[0004] 为了使令牌提供器获得授权令牌,令牌提供器将授权码请求发送至授权服务器。

[0005] 日本特开2017-107396公开了如下的系统:装置具有的应用程序经由该装置具有的令牌提供器从授权服务器获得授权令牌。

发明内容

[0006] 一种信息处理装置,包括:发送部件,用于将供授权服务器发出授权码所用的授权码请求发送至所述授权服务器,所述授权码表示用户许可了所述信息处理装置访问资源服务器;接收部件,用于从所述授权服务器接收与所述授权码请求相对应的授权码响应;以及令牌提供器,用于从所述信息处理装置上的应用程序获得用于识别所述授权服务器所在的区域的区域信息,并且基于所获得的区域信息来识别所述授权码请求发送至的授权端点,其中,所述发送部件将所述授权码请求发送至所识别出的授权端点,以及所述接收部件接收与所述发送部件所发送的授权码请求相对应的授权码响应。

[0007] 一种控制方法,用于控制计算机,所述计算机包括发送部件和接收部件,所述控制方法包括:将供授权服务器发出授权码所用的授权码请求发送至所述授权服务器,所述授权码表示用户许可了装置访问资源服务器;从所述授权服务器接收与所述授权码请求相对应的授权码响应;从所述装置上的应用程序获得用于识别所述授权服务器所在的区域的区域信息;基于所获得的区域信息来识别授权端点;使用所述发送部件将所述授权码请求发送至所识别出的授权端点;以及使用所述接收部件接收与所述发送部件所发送的授权码请求相对应的授权码响应。

[0008] 一种非暂时性存储介质,其存储指令,所述指令在由包括一个或多个处理器的装置执行的情况下控制以下部件:发送部件,用于将供授权服务器发出授权码所用的授权码请求发送至所述授权服务器,所述授权码表示用户许可了所述装置访问资源服务器;以及

接收部件，用于从所述授权服务器接收与所述授权码请求相对应的授权码响应，其中，所述装置所包括的令牌提供器从所述装置上的应用程序获得作为用于识别所述授权服务器所在的区域的信息的区域信息，基于所获得的区域信息来识别作为所述授权码请求发送至的发送目的地的授权端点，所述发送部件将所述授权码请求发送至所识别出的授权端点，以及所述接收部件接收与所述发送部件所发送的授权码请求相对应的授权码响应。

[0009] 通过以下参考附图对典型实施例的说明，本发明的其它特征将变得明显。

附图说明

[0010] 图1示出根据本发明实施例的权限转移系统。

[0011] 图2是示出装置的硬件结构的图。

[0012] 图3是示出装置的功能的图。

[0013] 图4示出OAuth 2.0中的授权码授予的处理流程。

[0014] 图5示出令牌提供器的功能。

[0015] 图6是令牌提供器的操作的序列图。

[0016] 图7是示出第一实施例中的授权端点的选择的流程图。

[0017] 图8是示出第二实施例中的授权端点的选择的流程图。

[0018] 图9示出Web浏览器中的区域输入画面的示例。

[0019] 图10示出用于执行根据第一实施例的处理或根据第二实施例的处理的判断流程图的示例。

具体实施方式

[0020] 用户信息是在特定地理区域(以下称为“区域”)的授权服务器中管理的。在存在针对多个用户的用户信息的情况下，多个用户信息可能不是全部由同一区域的授权服务器管理。具体地，在将应用程序分发到多个区域并且在世界范围内使用的情况下，使用该应用程序的用户的用户信息由该用户信息所在的授权服务器管理。在用户信息所在的授权服务器处发出授权令牌，验证所发出的授权令牌，并且资源服务器向应用程序提供Web服务。与用户信息的位置相对应的授权服务器发出授权令牌的原因在于，存在从个人信息保护和国家安全等的角度、对区域之间的用户信息的转移和共享施加了限制的情况。

[0021] 这里将考虑在多个区域中使用应用程序的情形。在这种情况下，应用程序将与用户信息所在的区域有关的信息(以下称为“区域信息”)发送至令牌提供器。令牌提供器基于所接收到的区域信息向授权服务器发送授权码请求。因此，作为用于发送授权码请求的目的地的授权端点的选项更加广泛。

[0022] 令牌提供器需要从利用应用程序指定的区域信息中识别授权端点。授权端点是指定用于将授权码请求发送至各区域中存在的授权服务器的目的地的地址。

[0023] 已经发现，期望根据从应用程序接收到的区域信息，装置能够识别适合于发送授权码请求的授权端点统一资源定位符(URL)。

[0024] 将参考附图来说明本发明的优选实施例。注意，在以下说明中，在后面所述的授权服务器200和授权服务器201中的任一个就足够的情况下，这将被描述为“授权服务器200或201”，并且在资源服务器300和资源服务器301中的任一个就足够的情况下，这将被描述为

“资源服务器300或301”。然而，注意，在授权服务器201发出授权码或授权令牌的情况下，使用授权服务器201所发出的授权令牌来访问资源服务器301所公开的API。另一方面，在授权服务器200发出授权码或授权令牌的情况下，使用授权服务器200所发出的授权令牌来访问资源服务器300所公开的API。

[0025] 首先，将参考图1来说明根据本发明实施例的权限转移系统。权限转移系统在诸如图1所示等的网络上实现。使用万维网(WWW)系统构建广域网(WAN)100。WAN 100和各种装置200～500经由局域网(LAN)101连接。

[0026] 授权服务器200和201是用于实现OAuth 2.0或类似协议的服务器，并且进行诸如接收认证请求和发出并管理授权码等的处理。在图1中，授权服务器200和资源服务器300被例示为通过LAN 101连接，授权服务器201和资源服务器301也是如此，但可以是经由WAN 100进行连接的结构。还可以进行如下配置：授权服务器200和201经由LAN 101连接至未图示的数据库服务器，并且将授权服务器200和201为了实现它们的功能所使用的数据存储在数据库服务器中。尽管授权服务器200和资源服务器300以及授权服务器201和资源服务器301各自在图1中均被描述为单独的服务器，但也可以是如下结构：在同一服务器上实现两个服务器的功能。

[0027] 注意，资源服务器300和授权服务器200(或者资源服务器301和授权服务器201)的位置的形式不限于在相同区域中或在相同系统中。可以使用任何形式的位置，只要资源服务器300能够查询授权服务器200所发出的授权令牌即可。可选地，例如，可以使用如下形式：资源服务器300验证连同授权令牌一起接收到的签名信息。

[0028] 装置400的示例包括打印机、MFP、个人计算机(PC)和智能电话等。终端500的用户可以经由Web浏览器510使用各种装置的功能，诸如向授权服务器200或201进行用户认证请求、以及装置400的登录操作等。终端500的具体示例包括PC或智能电话等。

[0029] 装置400和终端500分别具有Web浏览器410和Web浏览器510。用户通过操作Web浏览器410或Web浏览器510执行后面说明的授权操作。装置400和终端500经由LAN 101连接。注意，在以下说明中，在可以使用Web浏览器410和Web浏览器510中的任一个执行操作的情况下，将使用表述“Web浏览器410或510”。

[0030] 接着，将参考图2来说明授权服务器200和201、资源服务器300和301、装置400以及终端500的硬件结构。注意，图2是一般信息处理装置的框图，并且一般信息处理装置的硬件结构或者作为IaaS(基础设施即服务)提供的信息处理装置的虚拟硬件结构可以应用于本实施例中的各种装置。将在图2中示例性地说明装置400，但资源服务器300和301、授权服务器200和201以及终端500也具有相同的硬件结构。

[0031] CPU 2001是从RAM 2002、ROM 2003和外部存储器2011等提取程序的单元，并且执行这些程序中的命令以控制装置400。后面所述的序列通过正在执行的程序中的这些命令来实现。CPU 2001控制连接至系统总线2004的块。

[0032] RAM 2002是CPU 2001执行命令所使用的工作存储器。将ROM 2003或外部存储器2011中所保存的操作系统(OS)、应用程序和其它这种程序加载到RAM 2002，并且CPU 2001通过顺次读出这些程序的命令来执行这些命令。ROM 2003是记录了包括应用程序和OS的嵌入程序、以及数据等的存储装置。

[0033] 键盘控制器(KBC)2005是用于控制来自键盘(KB)2009和未图示的指点装置的输入

的单元。阴极射线管控制器(CRTC)2006或具有类似功能的控制器是用于控制CRT显示器2010或类似显示单元上的显示的单元。盘控制器(DKC)2007是用于控制对外部存储器2011的数据访问的单元。网络控制器(NC)2008与经由WAN 100和LAN 101连接的其它装置执行通信控制处理。在作为IaaS提供的虚拟信息处理装置的情况下，该结构不具有KBC 2005和CRTC 2006等，并且操作经由NC 2008连接的终端所具有的键盘和CRT显示器。除非另外具体说明，否则在以下说明中，执行各种装置的功能时的硬件的主实体是CPU 2001，并且软件的主实体是安装在RAM 2002、ROM 2003和外部存储器2011等中的程序。

[0034] 接着，将参考图3来说明授权服务器200和201、资源服务器300和301、装置400以及终端500所具有的功能。注意，授权服务器201和授权服务器200以及资源服务器300和资源服务器301各自具有相同的功能，因此将在图3的说明中示例性地说明授权服务器200和资源服务器300。

[0035] 授权服务器200具有授权服务器单元210和HTTP服务器单元220。HTTP服务器单元220经由WAN 100连接至装置400和终端500，并且具有与Web浏览器410、Web浏览器510和后面所述的应用程序420进行HTTP通信的功能。HTTP服务器单元220还能够通过SSL/TLS进行通信，并且具有未图示的证书存储器。

[0036] 授权服务器单元210具有以下功能：经由HTTP服务器单元220从Web浏览器410和Web浏览器510接收请求，并且利用对所接收到的请求的结果进行响应。具体地，HTTP服务器单元220从Web浏览器410或510接收用户认证请求，生成关于与认证已成功的用户的用户信息相关联的授权令牌的信息，并且向Web浏览器410或510通知授权令牌。授权令牌是表示用户登录到授权服务器200的令牌、或者用于验证用户是否已在授权服务器200处被认证的令牌。授权服务器200可以通过使用授权令牌来识别用户。授权服务器单元210可被配置为存储用于向授权令牌提供签名信息的私钥。在这种情况下，使用该私钥将签名信息提供给授权令牌，并且将提供有签名信息的授权令牌发出至装置400。

[0037] 资源服务器300具有资源服务器单元310。资源服务器单元310是用于公开提供Web服务的API的功能。注意，可以是如下结构：与授权服务器200相同，资源服务器300具有HTTP服务器单元并且经由HTTP服务器单元执行外部接收和发送。

[0038] 装置400具有Web浏览器410、应用程序420、认证单元430和令牌提供器440。Web浏览器410是用于使用WWW的用户代理所实现的功能。Web浏览器410通过用户操作与授权服务器200和令牌提供器440进行通信。终端500具有的Web浏览器510也具有与Web浏览器410相同的功能。应用程序420经由令牌提供器440从授权服务器200获得授权令牌。所获得的授权令牌用于使用资源服务器300所公开的API。

[0039] 令牌提供器440从应用程序420接收授权令牌请求，并且通过与授权服务器200的通信获得授权令牌。用户通过使用Web浏览器410或510与授权服务器200和令牌提供器440通信来进行授权操作。

[0040] 注意，这里的授权令牌请求是应用程序420发送至令牌提供器440以获得授权令牌的请求。另一方面，令牌请求还用于描述令牌提供器440向授权服务器200或201发送以获得授权令牌的请求。这里，应当注意，根据请求的发送方和接收方是谁，以不同的方式指代用以获得授权令牌的请求。

[0041] 令牌提供器440具有由X.509标准规定的客户端证书及其私钥，以证明令牌提供器

440本身作为供应商默认凭证。通过令牌提供器440在与授权服务器200建立通信时使用客户端证书及其私钥，授权服务器200可以对令牌提供器440进行认证。

[0042] 认证单元430是用于认证用户的功能。用户在装置400处的未图示的输入画面处输入本地用户ID和本地用户密码。接收到所输入的信息的装置400通过将预先登记在认证单元430中的信息(本地用户ID和本地用户密码)与所输入的信息进行匹配来进行用户认证处理，并且生成登录上下文。注意，认证处理的形式不限于该配置，并且可以是使用集成电路(IC)卡的认证或者使用指纹的生物认证等。

[0043] 登录上下文是用于在装置400处识别本地用户的信息，并且例如由本地用户ID构成。登录上下文是在本地用户登录到装置400时在OS(未图示)处生成的，并且在注销时不再存在。通过本地用户的登录操作正在生成登录上下文，在Web浏览器410上公开登录的本地用户具有访问权限的Web页。在本地用户的注销操作之后，登录上下文不再存在，从而由于本地用户具有访问权限的Web页将不会向其它用户公开，因此确保了安全性。

[0044] 在应用程序420、认证单元430和令牌提供器440之间共享该登录上下文。注意，可以进行如下配置：登录上下文不仅包括本地用户信息，而且还包括与本地用户信息相关联的用户信息所在的区域的区域信息。在这种情况下，在装置400处生成登录上下文时，在应用程序420、认证单元430和令牌提供器440之间还共享区域信息。令牌提供器440可以基于所共享的区域信息和本地用户信息来识别作为授权码请求被发送至的目的地的授权端点。

[0045] 尽管在本实施例中说明了向装置400的登录处理通过用户直接操作装置400并且登录来进行的配置，但也可以经由Web浏览器510远程地进行登录。在这种情况下，认证单元430利用未图示的登录画面来向Web浏览器510进行响应。通过在该登录画面处输入本地用户ID和本地用户密码来对用户进行认证。如此，在应用程序420、认证单元430和令牌提供器440之间共享在认证单元430处生成的登录上下文。

[0046] 接着，将参考图4使用授权服务器200和201、资源服务器300和301、装置400以及Web浏览器510来进行装置400的令牌提供器440所提供的OAuth2.0处理。尽管在图4中示例性地使用授权服务器201来进行说明，但授权服务器200可以以相同方式应用。此外，在本实施例中将说明作为令牌提供器440提供的认证授权技术的OAuth 2.0的示例，但这可以是除OAuth 2.0以外的配置，只要发出授权令牌即可。注意，除非另外具体说明，否则在图4的以下描述中装置400是主实体的处理由令牌提供器440进行。

[0047] 作为用以执行OAuth 2.0的预备操作，向授权服务器201进行登记请求，以登记装置400(S0.0)。具体地，将装置400的登记请求发送至授权服务器201的登记端点(在图4中端点缩写为“EP”)，并且在装置400启动时、或者在开始后面所述的S1.1的授权流程时装置400未登记的情况下，开始该登记请求。用于进行登记请求的方法的示例包括装置400与授权服务器201进行自主通信的方法、以及用户经由Web浏览器510访问授权服务器201并且登记装置400的方法。

[0048] S0.0中的登记请求包括要显示在后面所述的授权确认画面中的装置名称、描述、图标图像和作为必不可少的参数的重定向URI。重定向URI是指定装置400将授权码响应发送至的发送目的地的地址。后面将说明授权码响应。从装置400接收到登记请求的授权服务器201发出用于识别装置400的装置ID、以及作为用于对装置400进行认证的机密信息的装置密钥，并且发送至装置400作为对装置400的登记响应(S0.1)。在S0.1中，授权服务器201

以关联方式存储装置ID和装置密钥、以及在S0.0中接收到的各种信息和重定向URI。以上是作为用于执行OAuth 2.0的预备操作的装置400处的登记流程。

[0049] 接着，将参考图4来说明授权服务器201处的用户认证所用的流程。用户登录到装置400(S1.0)。装置400的认证单元430生成并存储作为用于识别已登录的用户的信息的登录上下文。可以从所生成的登录上下文获得用于识别已登录的用户的信息(本地用户ID等)。通过用户经由Web浏览器510访问用于开始授权的URI来开始OAuth 2.0授权流程(S1.1)。在访问授权开始URI以开始授权流程时，装置400将授权码请求发送至授权服务器201的授权端点(S1.2)。授权码请求包括装置ID、重定向URI和状态参数。

[0050] 状态参数是用于使授权码请求和授权码响应唯一地关联的信息，并且用于防止跨站点请求伪造(CSRF)攻击和令牌替换(以下称为“授权码替换”)攻击。因此，状态参数需要是不能预测而且还不同的值。装置400所发出的状态参数由装置400以与重定向URI和登录上下文相关联的方式管理，以验证装置400在后面所述的授权码响应中接收到的状态参数与在S1.2的授权码请求中发送的状态参数的一致，并且进一步识别执行授权码请求的用户。

[0051] 在用户没有登录到授权服务器201的情况下，在S1.2中接收到授权码请求的授权服务器201在Web浏览器510上利用用户认证所用的登录画面进行响应(S1.3)。用户经由Web浏览器510输入用户ID和密码，并且向授权服务器201进行认证请求(S1.4)。接收到认证请求的授权服务器201验证在S1.4中接收到的用户ID和密码的关联信息与预先登记的关联信息是否一致，并且如果一致，则发出授权令牌。将所发出的授权令牌附加到认证cookie并返回到Web浏览器510。

[0052] 授权服务器201在Web浏览器510上利用用于确认装置400的授权的授权确认画面来向用户进行响应(S1.5)。然而，在S1.2中接收到的装置ID和重定向URI的组合与在授权服务器201中预先登记的装置ID和重定向URI的组合不一致的情况下，授权服务器201利用错误画面向Web浏览器510进行响应。因此，可以防止向未经授权URI的重定向(转移)。在登录到授权服务器201的用户以同一装置ID完成了授权操作的情况下，可以省略S1.5。

[0053] 在用户的授权操作(S1.6)之后，授权服务器201发出授权码，并且将该授权码和状态参数作为授权码响应发送至装置400(S1.7)。具体地，将授权码和状态参数作为查询参数附加到重定向URI，并且发送至Web浏览器510，使得授权码和状态参数将被重定向到利用重定向URI所指定的目的地。将S1.7中发出的授权码以与装置ID、用户ID和重定向URL相关联的方式保存在授权服务器201中。

[0054] 针对重定向URI接收到授权码响应的装置400验证该授权码响应中所包括的状态参数与装置400所管理的状态参数是否一致。在作为验证的结果、这些状态参数一致的情况下，装置400将令牌请求发送至授权服务器201的令牌端点，以获得授权令牌(S2.0)。该令牌请求包括装置ID、密钥、S1.7中所获得的授权码和S1.2中获得的重定向URI。

[0055] 在S2.0中接收到令牌请求的授权服务器201验证装置ID和密钥的组合与预先登记的组合是否一致。在作为验证的结果、配置了一致的情况下，装置400被认证。此外，授权服务器201验证S2.0中接收到的授权码是否存储在授权服务器201处，在该授权码存储在授权服务器201处的情况下验证该授权码是否未到期，并且验证与授权令牌相关联的装置ID和重定向URI与在S2.0的令牌请求中所接收到的装置ID和重定向URI是否一致。因而，授权服

务器201可以通过该验证来验证发送了S1.2中的授权码请求的装置400和发送了S2.0中的令牌请求的装置400是否一致。

[0056] 在验证成功的情况下，授权服务器201向装置400发出授权令牌，并且利用令牌响应来向装置400进行响应(S2.1)。此时，可以进行如下配置：还向装置400发出刷新令牌以更新授权令牌，并且利用令牌响应进行响应。装置400能够通过使用S2.1中接收到的授权令牌来访问资源服务器301已公开的API。在发出了授权令牌之后丢弃授权服务器201处所管理的授权码使得能够防止重放攻击。

[0057] 在S2.1的令牌响应包括刷新令牌的情况下，在装置400中以相关联的方式管理登录上下文和刷新令牌。因此，可以在下次以及后续访问API时无需执行授权处理(S1.2～S1.7)的情况下再次获得授权令牌。具体地，在接受S1.1的授权的开始时，确认在装置400处用户的登录上下文和刷新令牌是否相关联。如果不相关联，则进行上述的OAuth 2.0流程(S1.2及其后续的处理)。如果相关联，则针对授权服务器201的令牌端点进行刷新请求(S2.2)。

[0058] 刷新请求包括装置ID、密钥和刷新令牌。接收到刷新请求的授权服务器201验证装置ID和密钥的组合与在S0.1中预先登记的装置ID和密钥的组合是否一致。一旦确认为一致并且装置400被认证，则授权服务器201验证所接收到的刷新令牌是否存储在授权服务器201中，在所接收到的刷新令牌存储在授权服务器201中的情况下验证该刷新令牌是否未到期，并且验证与刷新令牌相关联的装置ID与刷新请求中的装置ID是否一致。在所有这些验证都成功的情况下，授权服务器201发出授权令牌，并将授权令牌作为令牌响应发送至装置400。此时，可以进行如下配置：再次发出刷新令牌以更新授权令牌，并且同时将该刷新令牌作为令牌响应发送至装置400。在发出新刷新令牌之后丢弃到目前为止在授权服务器201处管理的刷新令牌使得能够防止重放攻击。

[0059] 以上是OAuth 2.0中的授权码授予的处理流程。根据OAuth 2.0的处理流程使得授权服务器201能够发出授权令牌，并且使得装置400能够使用所发出的授权令牌来访问资源服务器301已公开的API，而不是授权服务器201将其管理的用户信息发送至装置400。

[0060] 第一实施例

[0061] 并非总是为如下情况：用户信息被登记在某个特定区域的授权服务器中，并且在同一区域中的授权服务器中管理多组用户信息。还存在从个人信息保护和国家安全等的角度、对不同区域之间的用户信息的转移和共享施加限制的情况。在这种情况下，令牌提供器440需要从多个授权服务器中选择与应用程序420所指定的区域相对应的授权服务器，并且将授权码请求发送至该授权服务器。在第一实施例中将说明令牌提供器440识别并选择用于管理用户信息的授权服务器的配置。

[0062] 首先，将参考图5来说明令牌提供器440具有的功能。令牌提供器440包括端点选择单元610、令牌获取单元620、令牌管理单元630和令牌分发单元640。

[0063] 端点选择单元610是在根据OAuth 2.0的授权流程中将授权码请求(图4的S1.2)发送至授权服务器200或201的授权端点的功能。此时，端点选择单元610使用端点选择单元610具有的区域信息和授权端点URL之间的相关表来选择与应用程序420所指定的区域相对应的授权端点URL。表1示出端点选择单元610具有的相关表的示例。在本实施例中将假设授权服务器200位于区域“JP”中并且授权服务器201位于区域“EU”中的情况。在图1中未图示

表1中的包括授权端点的区域“GB”的授权服务器。

[0064] 表1:端点URL数据库

[0065]

编号	区域	授权端点 URL	令牌端点 URL
1	JP	https://jp.example.com/oauth2/authorize	https://jp.example.com/oauth2/token
2	EU	https://eu.example.com/oauth2/authorize	https://eu.example.com/oauth2/token
3	GB	https://gb.example.com/oauth2/authorize	https://gb.example.com/oauth2/token

[0066] 表1具有“编号”(项目编号)、“区域”、“授权端点URL”和“令牌端点URL”的列,其中区域是主键。在本实施例中,将“JP”和“EU”登记到“区域”,并且针对各区域以相关方式登记授权端点URL和令牌端点URL。可以从外部应用程序等执行数据向表1的登记,并且可以使用任何形式的登记。

[0067] 令牌获取单元620是将令牌请求发送至令牌端点(S2.0)的功能。令牌获取单元620参考表1并且将令牌请求发送至与应用程序420所指定的区域相对应的令牌端点。

[0068] 令牌管理单元630是针对各本地用户ID管理令牌获取单元620所获得的授权令牌的功能。表2是令牌管理单元630管理的令牌数据库的示例。

[0069] 表2:令牌数据库

[0070]

编号	本地用户ID	区域	授权令牌	刷新令牌
1	Local_user1	JP	utbhtpbtrmjuevnryy0enlqe9vairx	o23Tx1T1dLRiimDq6CDDs
2	Local_user1	EU	t3geevy18czkcb9lujmtgchmuyivzg	ZTTcC8dNzTiF9FF84wF8wy
3	Local_user2	GB	t3geevy18czkcb9lujmtgchmuyivzg	ZTTcC8dNzTiF9FF84wF8wy

[0071] 表2具有“编号”、“本地用户ID”、“区域”、“授权令牌”和“刷新令牌”的列,其中本地用户ID和区域是主键。如以上已经说明的OAuth 2.0RFC6749中的“6.刷新访问令牌”那样,刷新令牌是用于再次使用相同的授权流程的新访问令牌。表2是通过已经执行的图4所示的授权流程(S1.0～S2.2)生成的,并且由令牌管理单元630管理。

[0072] 此外,在表2中,多个区域“JP”和“EU”与一个本地用户ID“Local_user1”相关联。也就是说,将与一个本地用户ID相关联的多组用户信息存储在区域“JP”的授权服务器200和区域“EU”的授权服务器201中。在这种情况下,通过用户在应用程序420处将区域切换为“JP”或“EU”来切换请求授权令牌所针对的授权服务器,并且可以将任何配置用于应用程序420。

[0073] 令牌分发单元640是基于本地用户ID和区域信息来将授权令牌发送至应用程序420的功能。具体地,从应用程序420接收到区域信息和本地用户ID。令牌分发单元640基于表2来将与所接收到的本地用户ID和区域信息相关联的授权令牌发送至应用程序420。

[0074] 在表2中不存在所接收到的本地用户ID和应用程序420所指定的区域信息的组合的情况下,认为尚未执行授权流程(图4)。然后,端点选择单元610使用所指定的区域信息和表1来识别区域的授权端点URL,从利用该授权端点URL识别的授权服务器200获得授权令牌和刷新令牌,并且将这两者连同本地用户ID和区域信息一起存储在令牌管理单元630(表2)中。以上是令牌提供器440的功能。

[0075] 接着,将参考图6来说明从应用程序420经由令牌提供器440从授权服务器200获得

授权令牌起、直到使用所获得的授权令牌来执行资源服务器300或301已公开的API为止的处理。注意，虽然在图6中将使用授权服务器200和资源服务器300进行说明，但授权服务器201和资源服务器301也执行相同的处理。将省略对以上已经说明的处理的详细说明。

[0076] 首先，应用程序420将授权令牌请求发送至令牌提供器440(S7.1)。具体地，应用程序420发送本地用户ID和区域信息作为授权令牌请求。可想到应用程序420获得区域信息所利用的多种配置。例如，可想到如下配置：在用户使用装置400的Web浏览器410输入本地用户ID和密码时，用户输入或选择区域信息。图9示出用于选择区域的画面的示例。在图9中，设置“用户ID”作为本地用户ID的输入空间，设置“密码”作为密码的输入空间，并且设置“区域”作为可以从下拉菜单中选择区域的空间。

[0077] 还可以想到如下配置：应用程序420判断在用户登录到装置400时生成的登录上下文中是否包括区域信息。在判断为包括区域信息的情况下，如上所述，基于登录上下文中所包括的区域信息来识别授权端点。在判断为没有包括区域信息的情况下，经由Web浏览器410或510提供供用户输入或选择区域所用的画面。可想到的另一配置如下：应用程序420基于预先在应用程序420或Web浏览器410等中设置的用户使用的语言的信息等，将所识别的区域信息发送至令牌提供器440。

[0078] 令牌提供器440使用令牌提供器440的令牌管理单元630所具有的令牌数据库(表2)，从S7.1中所接收到的本地用户ID和区域信息中搜索与所接收到的本地用户ID和区域信息的关联信息一致的记录。在找到与本地用户ID和区域信息的关联信息一致的记录的情况下，将与本地用户ID和区域信息相关联的授权令牌发送至应用程序420(S7.6)。

[0079] 在没有找到一致的记录的情况下，令牌提供器440根据在授权令牌请求中所接收到的区域信息以及表1来识别授权端点URL。使用所识别的授权端点URL来执行图4的S1.3～S2.1所示的处理，以从授权服务器200获得授权令牌。

[0080] 在S7.1中接收到授权令牌请求的令牌提供器440将授权码请求发送至授权服务器单元210(S7.2)。S7.2是与图4的S1.2相同的处理，因此将省略详细说明。接收到授权码请求的授权服务器单元210执行图4的S1.3～S1.6的处理，之后将授权码响应发送至令牌提供器440(S7.3)。S7.3是与图4的S1.7相同的处理，因此将省略详细说明。

[0081] S7.3中接收到授权码响应的令牌提供器440将令牌请求发送至授权服务器200的令牌端点(S7.4)。S7.4的处理与图4中的S2.0的处理等同，因此将省略详细说明。接收到令牌请求的授权服务器单元210将授权令牌和刷新令牌作为令牌响应发送至令牌提供器440(S7.5)。S7.5的处理与图4中的S2.1的处理等同，因此将省略详细说明。

[0082] 在执行S7.5之后，令牌提供器440将S7.5中所获得的授权令牌和刷新令牌以及S7.1中从应用程序420所获得的本地用户ID和区域信息登记在令牌数据库(表2)中。

[0083] 在S7.5中接收到令牌响应之后，令牌分发单元640将S7.5中所获得的授权令牌发送至应用程序420(S7.6)。获得了授权令牌的应用程序420使用授权令牌来将资源请求发送至资源服务器单元310(S7.7)。以上是从应用程序420使用令牌提供器440从授权服务器200获得授权令牌起、直到使用所获得的授权令牌执行资源服务器300或301已公开的API为止的处理。

[0084] 接着，将参考图7来说明在令牌提供器440获得授权令牌时的授权端点的选择处理。

[0085] 首先，令牌分发单元640从应用程序420接收到本地用户ID和区域信息作为授权令牌请求(S8.1)。这次将假设令牌分发单元640已接收到本地用户ID“Local_user2”和区域信息“JP”作为授权令牌请求来进行说明。

[0086] 令牌管理单元630使用令牌数据库(表2)来确认是否存在与所接收到的本地用户ID一致的记录(S8.2)。从表2可以看出，本地用户ID和区域信息的关联信息与预先存储的记录不一致。如果确认为一致的记录，则将该记录中所包括的授权令牌发送至应用程序420(S8.10)。

[0087] 如果确认为不存在记录，则端点选择单元610基于在S8.1中指定的区域来进行用以识别授权端点URL的判断(S8.3)。具体地，端点选择单元610基于端点URL数据库(表1)来获得并设置与已指定的区域“JP”匹配的授权端点(S8.4)。此次作为授权端点URL所获得的URL是来自表1的“https://jp.example.com/oauth2/authorize”。根据在S8.1的授权令牌请求中接收到的区域信息，执行S8.4～S8.7其中之一的处理。在不存在利用应用程序420的区域指定、或者在表1中没有包括已指定的区域的情况下，利用默认区域“GB”执行S8.7的处理。然而，注意，位于区域“GB”中的授权服务器是除授权服务器200和201以外的授权服务器(在图1中未图示)。

[0088] 令牌获取单元620将授权码请求发送至在S8.4～S8.7中所识别的授权端点URL(S8.8)。S8.8等同于图4的S1.2(或者图6的S7.2)。使用作为S8.8的处理的结果所获得的授权码将令牌请求发送至授权服务器200(S8.9)。S8.9等同于图4的S2.0(或者图6的S7.4)。将作为S8.9的处理的结果所获得的授权令牌发送至应用程序420(S8.10)。以上是在令牌提供器440获得授权令牌时的授权端点选择的处理。

[0089] 根据本实施例，在从应用程序420指定区域时，令牌提供器440可以选择适当的授权端点，并且可以根据所指定的区域信息来将授权码请求发送至授权服务器。

[0090] 尽管在本实施例中已经关于从应用程序420获得本地用户ID的配置进行了说明，但可以进行如下配置：在S1.0(图4)中用户登录到装置400时，从在认证单元430处生成的登录上下文中识别本地用户ID。

[0091] 第二实施例

[0092] 在第一实施例中说明了如下配置：考虑到从个人信息保护和国家安全等的角度、对不同区域之间的用户信息的转移和共享施加了限制的情况，应用程序420对令牌提供器440指定区域。然而，除应用程序420指定区域的配置外，还存在预先在令牌提供器440中设置固定区域的配置。

[0093] 在第二实施例中将说明如下配置：根据与作为授权码的获得目的地的区域是否被设置成固定有关的判断结果，来切换是将授权码请求发送至利用固定区域信息识别的授权服务器、还是执行第一实施例。注意，在第二实施例中省略了说明的部分与第一实施例相同。

[0094] 首先，将参考图8来说明令牌提供器440将授权码请求发送至授权服务器的处理。令牌分发单元640从应用程序420请求区域信息作为授权令牌请求(S9.1)。

[0095] 端点选择单元610不使用S9.1中接收到的区域信息，而是基于装置400的设置位置来识别授权端点URL。具体地，令牌提供器440从在装置400的NC2008中设置的IP地址获得国家代码(ICANN等所使用的ccTLD中的国家代码)(S9.2)。通过端点选择单元610搜索

MaxMind,Inc.提供的GeoIP数据库来执行国家代码的获得,由此可以从IP地址识别国家代码。除搜索GeoIP数据库以外的其它配置可以用于获得在装置400的区域设置信息中设置的国家信息作为国家代码。在这种情况下,将假设根据装置400的设置位置得到国家代码为“FR”。

[0096] 端点选择单元610判断在S9.2中获得的国家代码与设置到令牌提供器440的区域信息是否一致(S9.3)。这是基于端点选择单元610具有的固定区域判断表来执行的。在表3中示出固定区域判断表的示例。

[0097] 表3:固定区域判断表

[0098]

编号	固定区域	国家代码
1	JP	JP
2	EU	FR,IE,DE,ES

[0099] 表3具有“编号”(项目编号)、“固定区域”和“国家代码(ICANN等所使用的ccTLD中的国家代码)”的列。“固定区域”是令牌提供器440针对“国家代码”应当设置的区域。端点选择单元610根据固定区域判断表(表3)来判断针对在S9.2中获得的国家代码是否存在固定区域。如果不存在固定区域,则流程进入S9.8,并且从应用程序420所指定的区域获得并设置授权端点URL(S9.9～S9.12)。S9.8及其后续处理(S9.9～S9.12)与图7中的第一实施例的处理内容(S8.3～S8.7)相同,因此将省略详细说明。

[0100] 尽管在本实施例中说明了针对在S9.2中获得的国家代码、根据在表3的固定区域判断表中是否存在固定区域信息来判断是否切换为第一实施例的处理,但该判断方法并非限制性的。例如,可以想到如下配置:在令牌分发单元640从应用程序420接收到授权令牌请求之后,判断端点选择单元610是否具有固定区域判断表(图10中的S10.1)。该判断可以在S8.1(或S9.1)的处理之前执行。在S10.1中判断为存在表3的情况下,流程进入第二实施例(图8)的S9.2及其后续处理。在S10.1中判断为不存在表3的情况下,流程进入第一实施例(图7)的S8.2及其后续处理。

[0101] 在根据表3确认为针对在S9.3中获得的国家代码存在固定区域的情况下,比较固定区域信息和从应用程序420接收到的区域信息(S9.4)。如果通过比较确认为一致,则流程进入S9.6,并且如果没有确认为一致,则进入S9.5。这次在S9.2中获得的国家代码为“FR”,因此从表3可以看出存在固定区域“EU”。如果在S9.1中获得的区域信息为“FR”,则流程进入S9.6。

[0102] 另一方面,在S9.1中获得的区域信息为“CN”的情况下,这与令牌提供器440的固定区域“EU”不一致,因此流程进入S9.5。具体地,令牌提供器440将错误信息发送至应用程序420(S9.5)。错误信息可以包括意思是针对令牌提供器440设置成固定的固定区域信息和基于所获得的国家代码而识别的区域信息不一致的消息,但是任何配置对于该错误信息都是足够的。

[0103] 在S9.4中判断为存在一致的情况下,端点选择单元610使用所获得的国家代码或固定区域信息以及端点URL数据库(表1)来识别授权端点(S9.6)。

[0104] 在S9.6或者S9.9～S9.12中识别出授权端点URL之后,令牌获取单元620将授权码请求发送至所识别的授权端点URL(S9.7)。

[0105] 以上是在令牌提供器440获得授权令牌时固定授权端点的处理。

[0106] 其它实施例

[0107] 尽管区域信息已被描述为“JP”和“EU”(其中,默认区域信息为“GB”),但区域信息的类型和数量不限于上述示例。

[0108] 尽管以上已经说明了在上述流程中在利用应用程序420没有指定区域的情况下或者在表1中没有包括所指定的区域的情况下、使用默认设置的区域信息来继续处理,但是在这些情况下,可以进行发送错误信息并且结束处理的配置。

[0109] 本发明的实施例还可以通过如下的方法来实现,即,通过网络或者各种存储介质将执行上述实施例的功能的软件(程序)提供给系统或装置,该系统或装置的计算机或是中央处理单元(CPU)、微处理单元(MPU)读出并执行程序的方法。

[0110] 尽管已经参考典型实施例说明了本发明,但是应该理解,本发明不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,以包含所有这类修改、等同结构和功能。

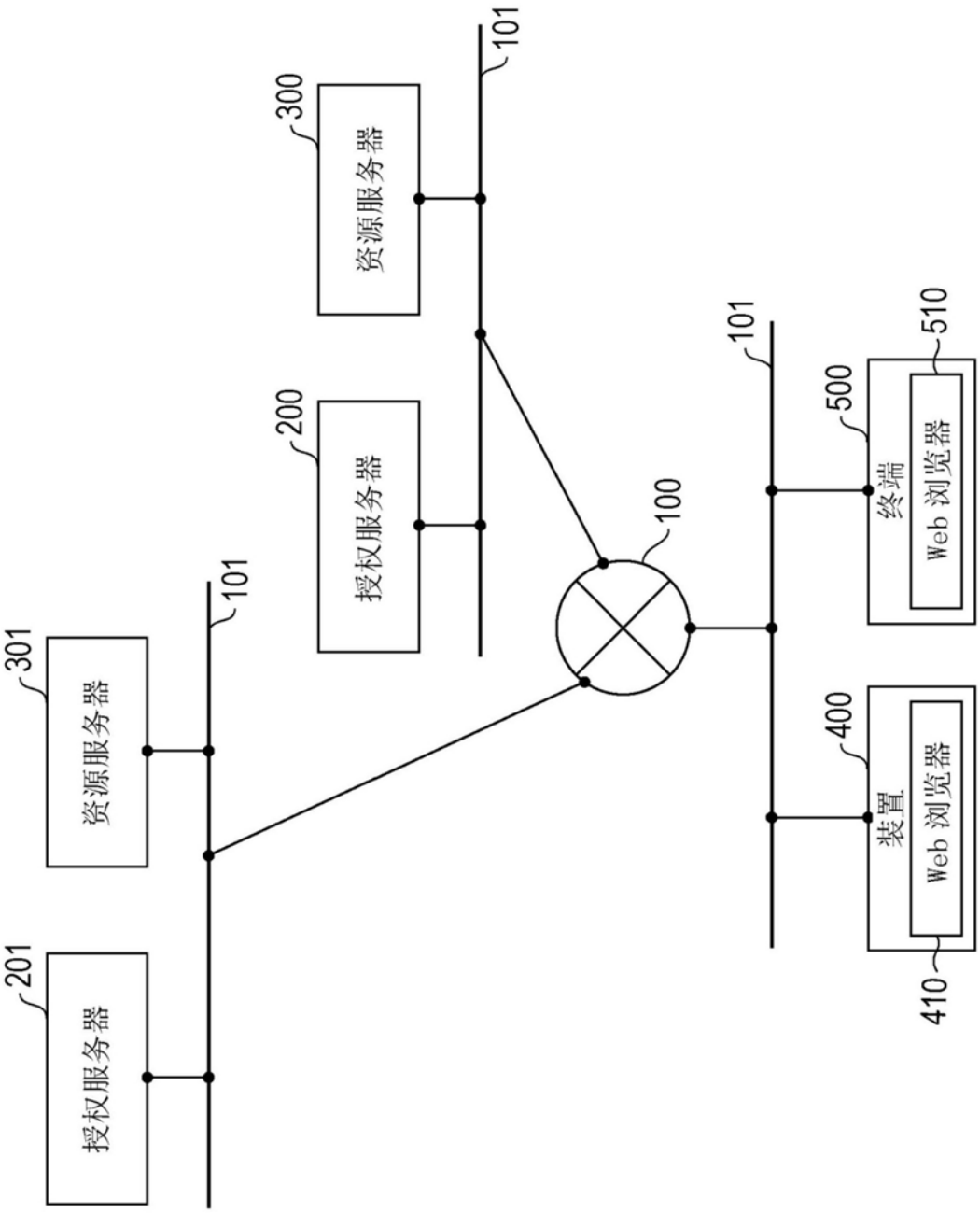

101
300
资源服务器
200
授权服务器
100
101
301
资源服务器
101
500
510
终端
Web 浏览器
201
授权服务器
400
装置
Web 浏览器
410

图1

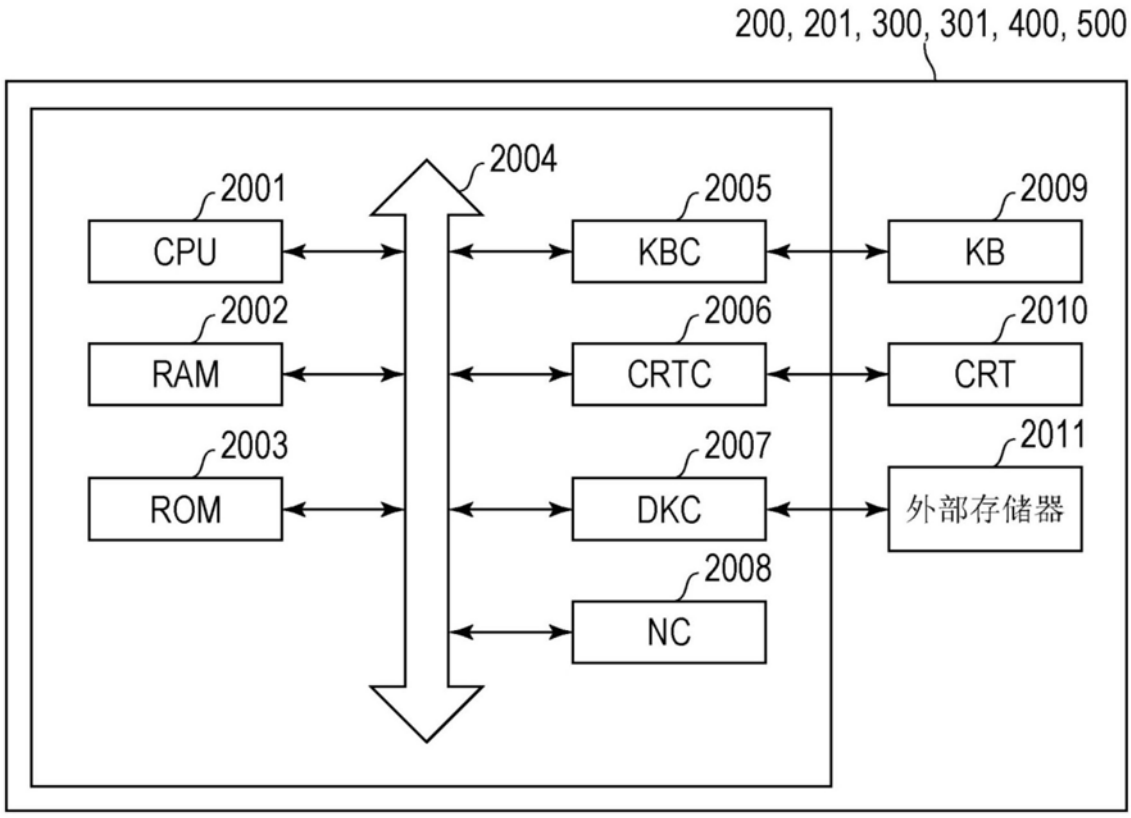

200, 201, 300, 301, 400, 500
2001
CPU
2002
RAM
2003
ROM
2004
2005
KBC
2006
CRTC
2007
DKC
2008
NC
2009
KB
2010
CRT
2011
外部存储器

图2

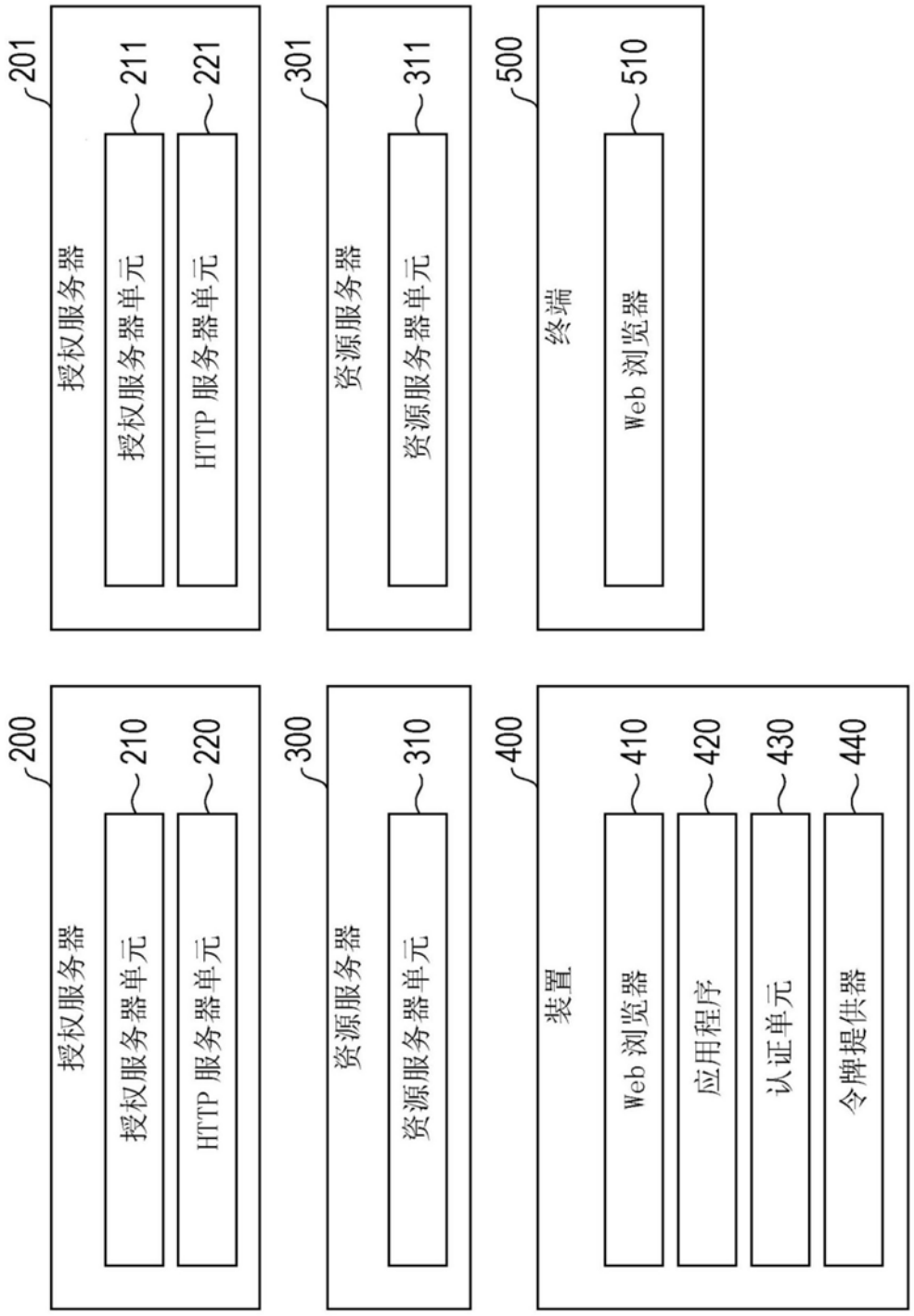

201
授权服务器
211
授权服务器单元
221
HTTP 服务器单元
301
资源服务器
311
资源服务器单元
500
终端
510
Web 浏览器
200
授权服务器
210
授权服务器单元
220
HTTP 服务器单元
300
资源服务器
310
资源服务器单元
400
装置
410
Web 浏览器
420
应用程序
430
认证单元
440
令牌提供器

图3

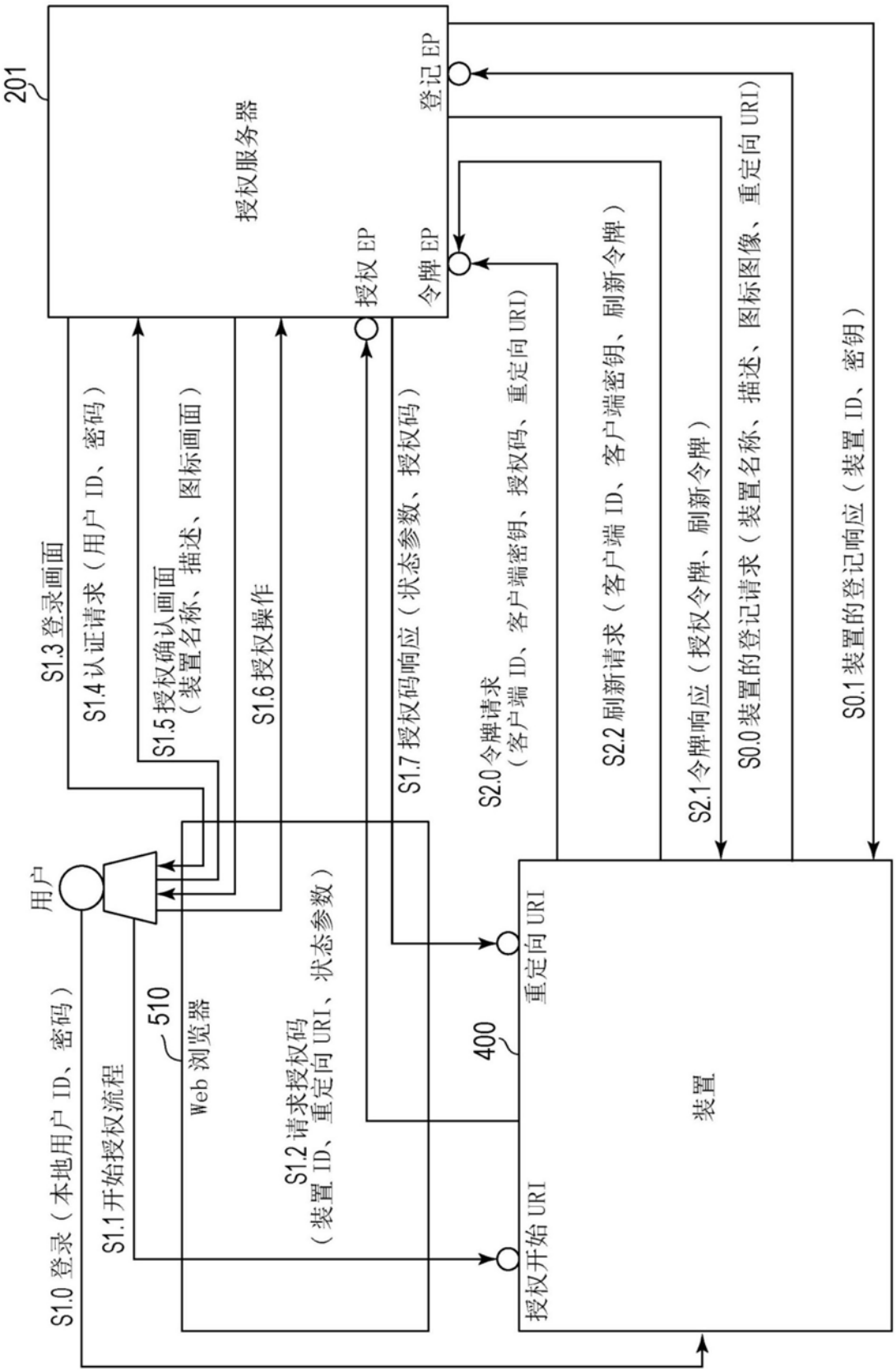

201
授权服务器
登记 EP
授权 EP
令牌 EP
S1.3 登录画面
S1.4 认证请求（用户 ID、密码）
S1.5 授权确认画面
（装置名称、描述、图标画面）
S1.6 授权操作
S1.7 授权码响应（状态参数、授权码）
S2.0 令牌请求
（客户端 ID、客户端密钥、授权码、重定向 URI）
S2.2 刷新请求（客户端 ID、客户端密钥、刷新令牌）
S2.1 令牌响应（授权令牌、刷新令牌）
S0.0 装置的登记请求（装置名称、描述、图标图像、重定向 URI）
S0.1 装置的登记响应（装置 ID、密钥）
用户
S1.0 登录（本地用户 ID、密码）
S1.1 开始授权流程
510
Web 浏览器
S1.2 请求授权码
（装置 ID、重定向 URI、状态参数）
400
重定向 URI
授权开始 URI
装置

图4

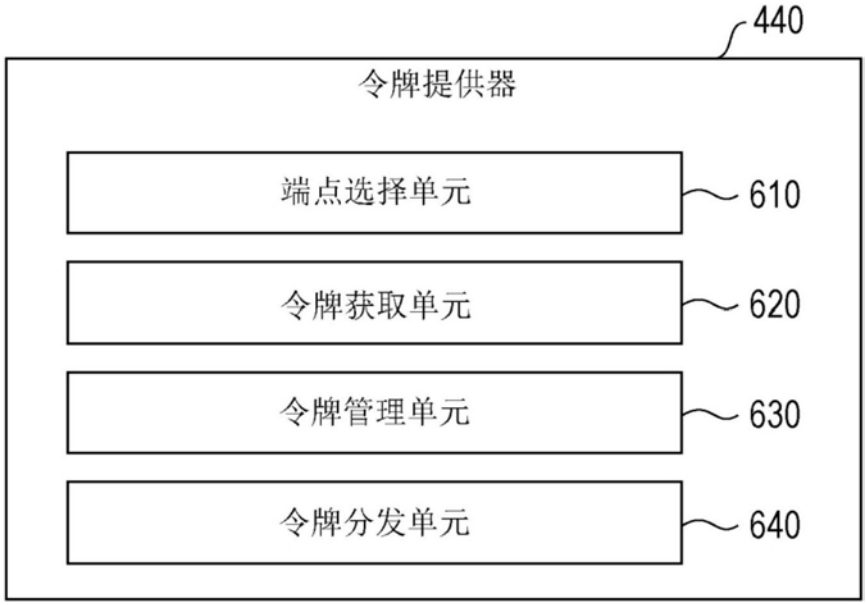


图5

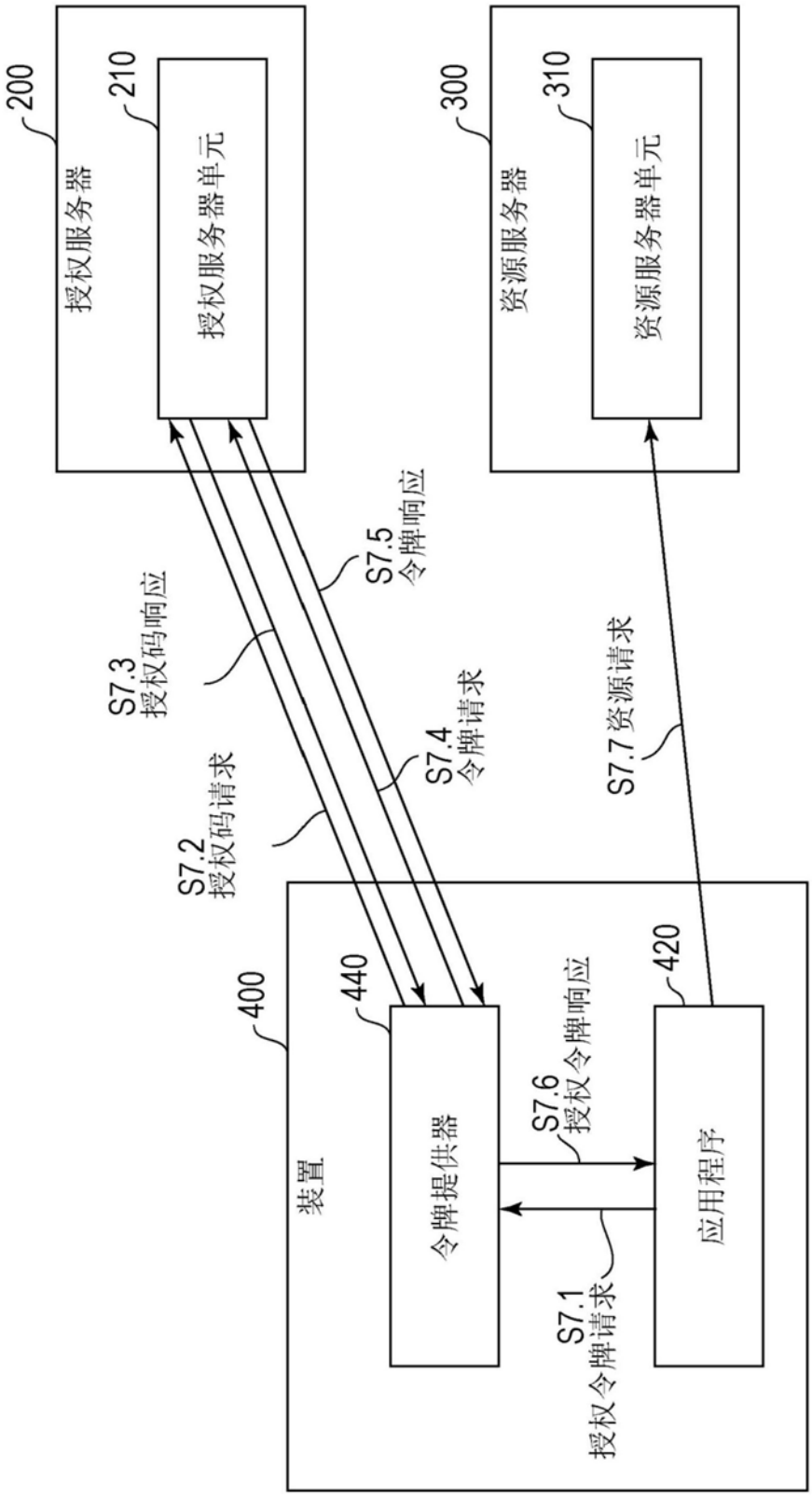

200
授权服务器
210
授权服务器单元
300
资源服务器
310
资源服务器单元
S7.3
授权码响应
S7.5
令牌响应
S7.2
授权码请求
S7.4
令牌请求
S7.7 资源请求
400
装置
440
令牌提供器
S7.6
授权令牌响应
420
应用程序
S7.1
授权令牌请求

图6

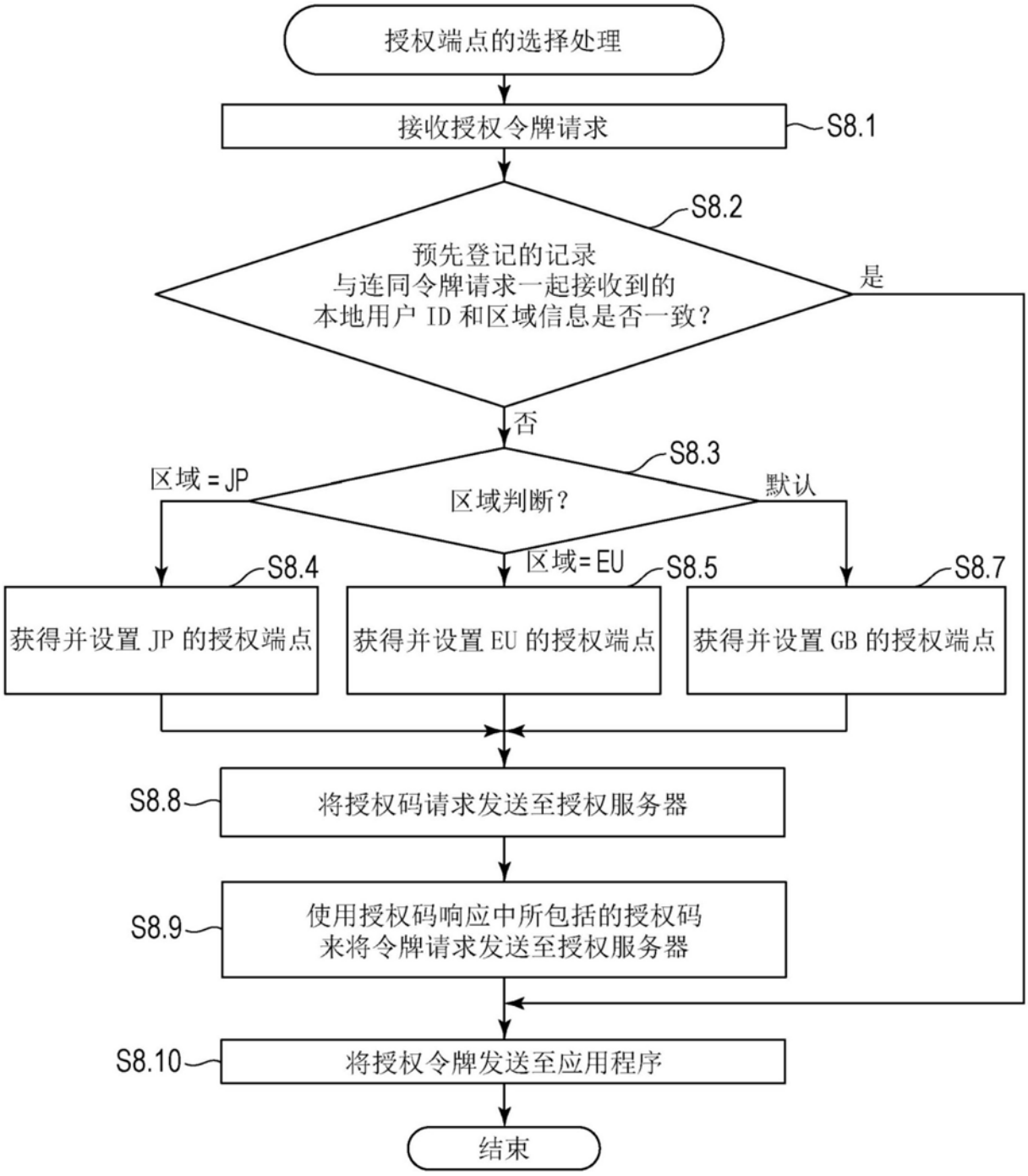

授权端点的选择处理
接收授权令牌请求
S8.1
S8.2
预先登记的记录
与连同令牌请求一起接收到的
本地用户 ID 和区域信息是否一致？
是
否
S8.3
区域判断？
区域 = JP
默认
区域= EU
S8.4
S8.5
S8.7
获得并设置 JP 的授权端点
获得并设置 EU 的授权端点
获得并设置 GB 的授权端点
S8.8
将授权码请求发送至授权服务器
S8.9
使用授权码响应中所包括的授权码
来将令牌请求发送至授权服务器
S8.10
将授权令牌发送至应用程序
结束

图7

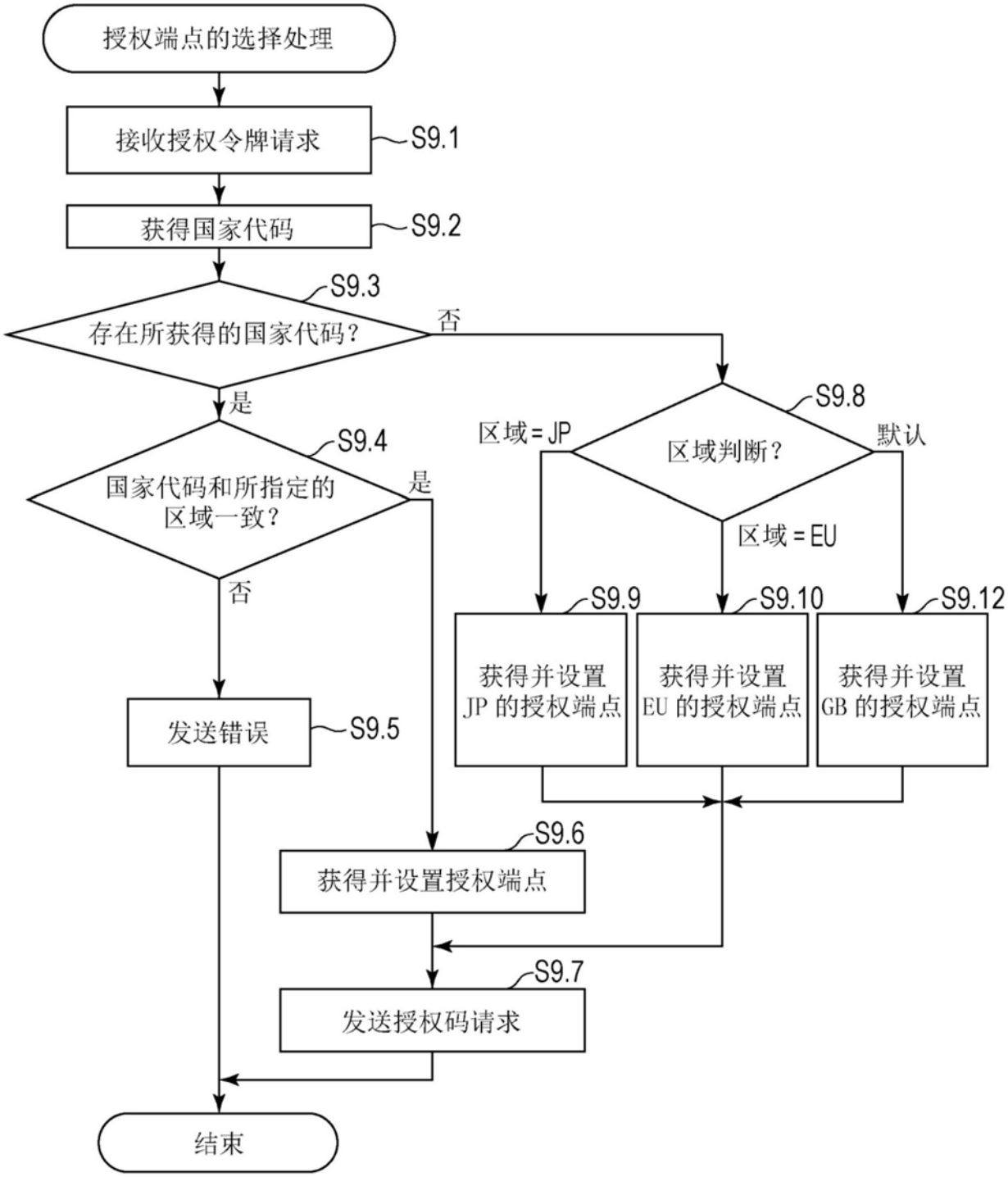

授权端点的选择处理
接收授权令牌请求
S9.1
获得国家代码
S9.2
S9.3
存在所获得的国家代码？
否
是
S9.4
国家代码和所指定的区域一致？
是
否
发送错误
S9.5
S9.8
区域判断？
区域 = JP
区域 = EU
默认
S9.9
S9.10
S9.12
获得并设置 JP 的授权端点
获得并设置 EU 的授权端点
获得并设置 GB 的授权端点
S9.6
获得并设置授权端点
S9.7
发送授权码请求
结束

图8

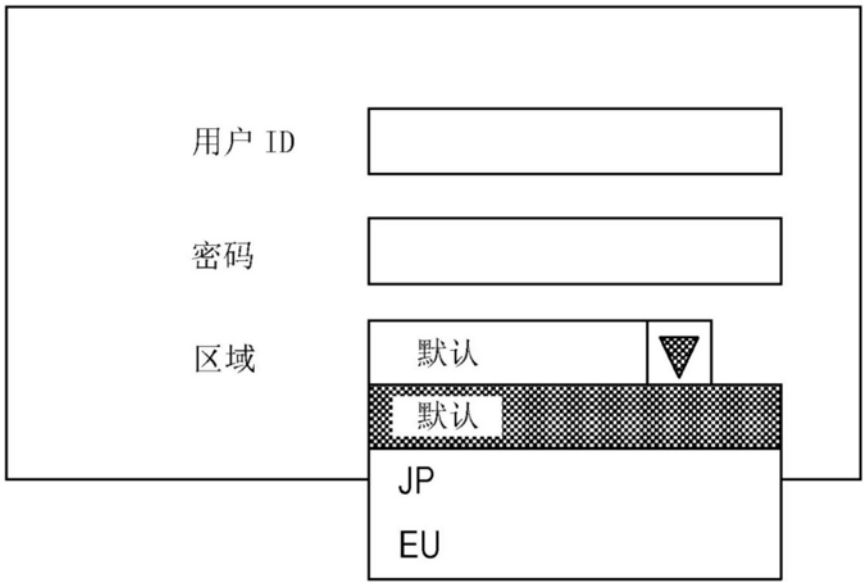

用户 ID
密码
区域
默认
默认
JP
EU

图9

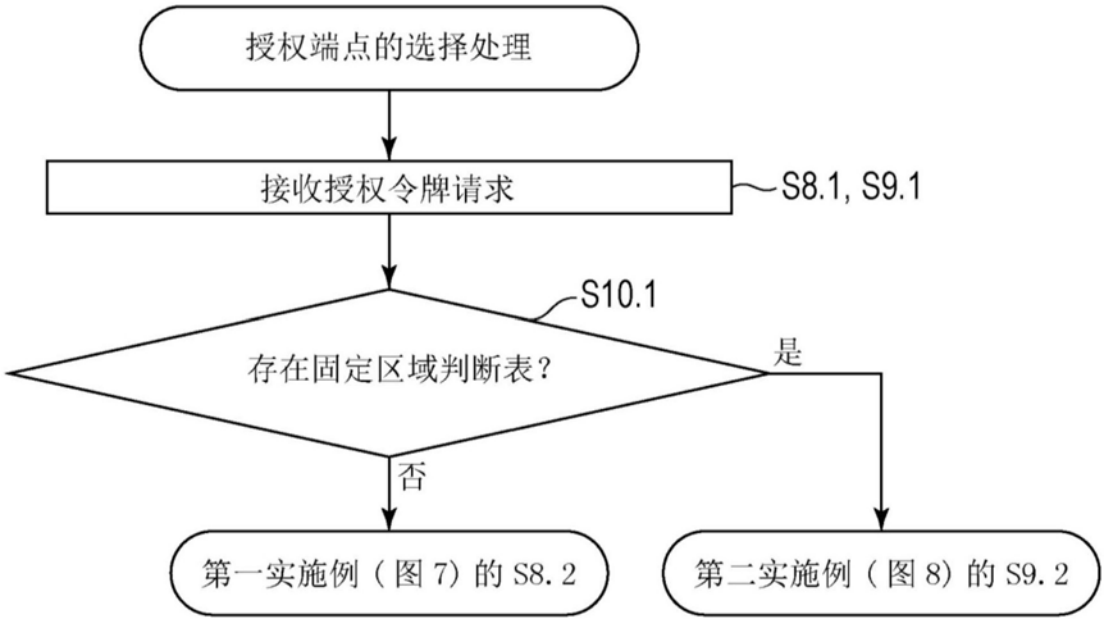

授权端点的选择处理
接收授权令牌请求
S8.1, S9.1
S10.1
存在固定区域判断表？
是
否
第一实施例（图 7）的 S8. 2
第二实施例（图 8）的 S9. 2

图10