(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 103404093 A
(43)申请公布日 2013.11.20

(21)申请号 201280009911.X
(22)申请日 2012.02.20
(30)优先权数据
2011-034407 2011.02.21 JP
(85)PCT申请进入国家阶段日
2013.08.21
(86)PCT申请的申请数据
PCT/JP2012/054013 2012.02.20
(87)PCT申请的公布数据
WO2012/115058 JA 2012.08.30
(71)申请人 日本电气株式会社
地址 日本东京都
(72)发明人 山形昌也 中江政行 森田阳一郎
下西英之 园田健太郎
(74)专利代理机构 北京市金杜律师事务所 11256
代理人 陈伟
(51)Int.Cl.
H04L 12/911(2013.01)
H04L 29/06(2006.01)

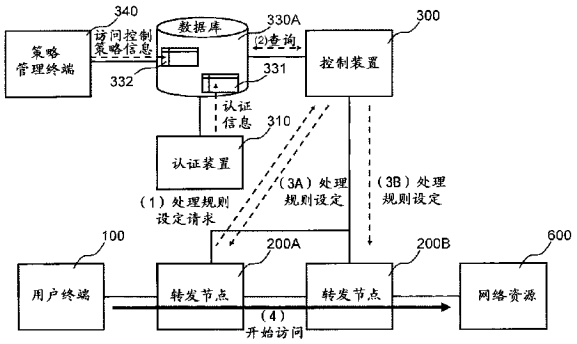
权利要求书2页 说明书12页 附图8页

(54)发明名称

通信系统、数据库、控制装置、通信方法以及程序

(57)摘要

本发明能以简单的结构来实现与赋予给各用户的访问权限相应的极细的访问控制。通信系统包括：多个转发节点，其根据处理规则处理接收数据包；数据库，其保持有用于根据与发送源有关的信息来特定相当于发送源的用户的角色的第1表和对每个角色定义了能访问或不能访问的资源的第2表，根据来自控制装置的请求，响应相当于发送源的用户能访问或不能访问的资源；和控制装置，其在从所述转发节点接收到所述处理规则的设定请求的情况下，使用与所述处理规则的设定请求所包含的发送源有关的信息，对所述数据库查询相当于所述发送源的用户能访问或不能访问的资源，基于来自所述数据库的响应，生成所述处理规则并设定到所述转发节点。



CN 103404093 A

1. 一种通信系统，包括：

多个转发节点，其根据处理规则来处理接收数据包，所述处理规则将用于特定流的匹配规则和适用于符合所述匹配规则的数据包的处理内容建立了对应；

数据库，其保持有第 1 表和第 2 表，并根据来自控制装置的请求，响应相当于发送源的用户能访问或不能访问的资源，其中，所述第 1 表用于根据与发送源有关的信息来特定相当于发送源的用户的角色，所述第 2 表按每个角色定义了能访问或不能访问的资源；和

控制装置，其在从所述转发节点接收到所述处理规则的设定请求的情况下，使用与所述处理规则的设定请求所包含的发送源有关的信息，对所述数据库查询相当于所述发送源的用户能访问或不能访问的资源，基于来自所述数据库的响应，生成所述处理规则并设定到所述转发节点。

2. 根据权利要求 1 所述的通信系统，其中，

所述第 2 表的条目使用访问控制策略信息和资源信息而生成，其中，所述访问控制策略信息按赋予给用户的每个角色定义了能访问或不能访问的资源的组，所述资源信息定义了属于所述各组的资源的详细内容。

3. 根据权利要求 2 所述的通信系统，其中，

还具有访问策略管理部，该访问策略管理部在访问控制策略信息和资源信息的至少一方被更新的情况下，更新所述第 2 表的所述被更新的位置所对应的条目。

4. 根据权利要求 1 ～ 3 中任一项所述的通信系统，其中，

在所述第 1 表中登记有认证成功的用户的条目，通过注销所述用户，从所述第 1 表中删除所述用户的条目。

5. 根据权利要求 1 ～ 4 中任一项所述的通信系统，其中，

在所述第 1 表的各条目中设定有有效期限，所述数据库从所述第 1 表中删除经过了所述有效期限的条目。

6. 根据权利要求 1 ～ 5 中任一项所述的通信系统，其中，

还包括：

进行用户认证并更新所述第 1 表的认证装置；和

受理所述第 2 表的更新内容的输入并更新所述第 2 表的策略管理终端。

7. 根据权利要求 1 ～ 6 中任一项所述的通信系统，其中，

所述控制装置基于来自所述数据库的响应，对预定的转发节点设定使从相当于所述发送源的用户发向被禁止访问的资源的数据包废弃的处理规则。

8. 根据权利要求 1 ～ 7 中任一项所述的通信系统，其中，

在来自所述数据库的响应中，包含有相当于所述发送源的用户能访问或不能访问所述资源的位置信息，

所述控制装置在从所述转发节点接收到所述处理规则的设定请求的情况下，不仅对接收到所述处理规则的设定请求的转发节点，还对与所述位置信息对应的转发节点设定访问所述资源或禁止访问所述资源的处理规则。

9. 一种数据库，与控制装置连接，所述控制装置对按照处理规则处理接收数据包的多个转发节点设定所述处理规则，所述处理规则将用于特定流的匹配规则和适用于符合所述匹配规则的数据包的处理内容建立了对应，

所述数据库保持有第 1 表和第 2 表，其中，所述第 1 表用于根据与发送源有关的信息来特定相当于发送源的用户的角色，所述第 2 表按每个角色定义了能访问或不能访问的资源，

所述数据库根据来自所述控制装置的请求，响应相当于发送源的用户能访问或不能访问的资源。

10. 一种控制装置，与多个转发节点和数据库连接，

所述多个转发节点根据处理规则处理接收数据包，所述处理规则将用于特定流的匹配规则和适用于符合所述匹配规则的数据包的处理内容建立了对应，

所述数据库保持有第 1 表和第 2 表，并根据来自控制装置的请求，响应相当于发送源的用户能访问或不能访问的资源，其中，所述第 1 表用于根据与发送源有关的信息来特定相当于发送源的用户的角色，所述第 2 表按每个角色定义了能访问或不能访问的资源，

所述控制装置在从所述转发节点接收到所述处理规则的设定请求的情况下，使用与所述处理规则的设定请求所包含的发送源有关的信息，对所述数据库查询相当于所述发送源的用户能访问或不能访问的资源，基于来自所述数据库的响应，生成所述处理规则并设定到所述转发节点。

11. 一种通信方法，是包含多个转发节点、数据库和控制装置的通信系统中的通信方法，其中，

所述多个转发节点根据处理规则来处理接收数据包，所述处理规则将用于特定流的匹配规则和适用于符合所述匹配规则的数据包的处理内容建立了对应，

所述数据库保持有第 1 表和第 2 表，并根据来自控制装置的请求，响应相当于发送源的用户能访问或不能访问的资源，所述第 1 表用于根据与发送源有关的信息来特定相当于发送源的用户的角色，所述第 2 表按每个角色定义了能访问或不能访问的资源，

所述控制装置对所述转发节点设定所述处理规则，

所述通信方法包括如下步骤 ：

所述控制装置在从所述转发节点接收到所述处理规则的设定请求的情况下，对所述数据库查询相当于所述发送源的用户能访问或不能访问的资源的步骤 ；和

所述控制装置基于来自所述数据库的响应，生成所述处理规则并设定到所述转发节点的步骤。

12. 一种程序，是由搭载于控制装置的计算机执行的程序，

所述控制装置与多个转发节点和数据库连接并对所述转发节点设定处理规则，

所述多个转发节点根据所述处理规则来处理接收数据包，所述处理规则将用于特定流的匹配规则和适用于符合所述匹配规则的数据包的处理内容建立了对应，

所述数据库保持有第 1 表和第 2 表，并根据来自控制装置的请求，响应相当于发送源的用户能访问或不能访问的资源，其中，所述第 1 表用于根据与发送源有关的信息来特定相当于发送源的用户的角色，所述第 2 表按每个角色定义了能访问或不能访问的资源，

所述程序使所述计算机执行如下处理 ：

在从所述转发节点接收到所述处理规则的设定请求的情况下，对所述数据库查询相当于所述发送源的用户能访问或不能访问的资源的处理 ；和

基于来自所述数据库的响应，生成所述处理规则并设定到所述转发节点的处理。

通信系统、数据库、控制装置、通信方法以及程序

技术领域

[0001] [关于相关申请的记载]

[0002] 本发明基于日本国专利申请:特愿2011-034407号(2011年2月21日申请)主张优先权,该申请的全部记载内容被引用并记载到本说明书中。

[0003] 本发明涉及通信系统、数据库、控制装置、通信方法以及程序,尤其涉及通过配置于网络的转发节点转发数据包来实现通信的通信系统、数据库、控制装置、通信方法以及程序。

背景技术

[0004] 近年来,提出了OpenFlow这一技术(参照专利文献1、非专利文献1、2)。OpenFlow将通信作为端对端的流而掌握,以流单位进行路径控制、障碍恢复、负载分散、最佳化。非专利文献2中被标准化的OpenFlow交换机,具有与相当于控制装置的OpenFlow控制器进行通信用的安全通道,按照从OpenFlow控制器适当指示追加或重写的流表(flow table)进行工作。在流表中,按每个流定义了与数据包报头(packet header)进行匹配的匹配规则(报头字段)、流统计信息(计数器,Counters)、和定义了处理内容的动作(Actions)的组(参照图15)。

[0005] 例如,OpenFlow交换机在接收到数据包时,从流表中检索具有符合接收数据包的报头信息的匹配规则(参照图15的报头字段)的条目(entry)。在检索的结果为找到了符合接收数据包的条目的情况下,OpenFlow交换机更新流统计信息(counter),并对接收数据包实施记载在该条目的动作字段中的处理内容(来自指定端口的数据包发送、洪泛(flooding)、废弃等)。另一方面,在所述检索的结果为没有找到符合接收数据包的条目的情况下,OpenFlow交换机经由安全通道对OpenFlow控制器转发接收数据包,委托基于接收数据包的发送源/发送目标的数据包的路径的确定,受理用于实现该路径的确定的流条目并更新流表。如此,OpenFlow交换机使用存储在流表中的条目作为处理规则来进行数据包转发。

[0006] 现有技术文献

[0007] 专利文献

[0008] 专利文献1:国际公开第2008/095010号

[0009] 非专利文献

[0010] 非专利文献1:Nick McKeown及其他7名,“OpenFlow:Enabling Innovation in Campus Networks”、[online]、[平成22(2010)年12月1日检索]、因特网<URL:http://www.openflowswitch.org//documents/openflow-wp-latest.pdf>

[0011] 非专利文献2:“OpenFlow Switch Specification”Version1.0.0.(Wire Protocol0x01)[平成22(2010)年12月1日检索]、因特网<URL:http://www.openflowswitch.org/documents/openflow-spec-v1.0.0.pdf>

发明内容

[0012] 以下的分析是由本发明提供的。

[0013] 专利文献 1 的 OpenFlow 控制器，在产生新的流时参照策略文件进行权限检查，然后，通过计算路径来进行访问控制（参照专利文献 1 的 [0052]）。因此，在专利文献 1 的结构中，存在局限于基于终端进行访问控制而无法基于用户进行访问控制这一问题。例如，在多个用户共用同一终端这种情形下，可能产生如下的不良情况：若对一个用户允许了向某网络资源的访问，则之后使用同一终端的其他用户也能够访问该网络资源。

[0014] 另外，虽然也考虑将基于已有的用户认证装置等进行的认证结果提供给 OpenFlow 控制器来进行基于用户的访问控制的方法，但在 OpenFlow 控制器中并没有掌握对该认证成功的用户授予了怎样的访问权限，因此还存在无法实现与按每个用户确定的策略等相应的极细的访问控制这样的问题。另外，假设在使 OpenFlow 控制器保持每个用户的访问权限信息的情况下，也会产生为此的资源和 / 或负载的问题、大量用户的访问权限管理问题。

[0015] 进而，当将多个 OpenFlow 控制器分担不同地域、通信量而进行集中控制的结构纳入考虑范围时，可能会产生如何将访问权限信息分布到这些 OpenFlow 控制器的问题、使 OpenFlow 控制器间的访问权限信息同步的问题。

[0016] 本发明是鉴于上述情况而完成的发明，其目的在于提供一种通信系统、控制装置、策略管理装置、通信方法以及程序，在如上述 OpenFlow 那样的控制装置集中控制转发节点的通信系统中，能够以简单的结构进行与赋予给各用户的访问权限相应的极细访问控制。

[0017] 根据本发明的第 1 观点，提供一种通信系统，包括：多个转发节点，其根据处理规则来处理接收数据包，所述处理规则将用于特定流的匹配规则和适用于符合所述匹配规则的数据包的处理内容建立了对应；数据库，其保持有用于根据与发送源有关的信息来特定相当于发送源的用户的角色的第 1 表和对每个角色定义了能访问或不能访问的资源的第 2 表，根据来自控制装置的请求，响应相当于发送源的用户能访问或不能访问的资源；和控制装置，其在从所述转发节点接收到所述处理规则的设定请求的情况下，使用与所述处理规则的设定请求所包含的发送源有关的信息，对所述数据库查询相当于所述发送源的用户能访问或不能访问的资源，基于来自所述数据库的响应，生成所述处理规则并设定到所述转发节点。

[0018] 根据本发明的第 2 观点，提供一种数据库，与控制装置连接，所述控制装置对根据处理规则来处理接收数据包的多个转发节点设定所述处理规则，所述处理规则将用于特定流的匹配规则和适用于符合所述匹配规则的数据包的处理内容建立了对应，所述数据库保持有用于根据与发送源有关的信息来特定相当于发送源的用户的角色的第 1 表和对每个角色定义了能访问或不能访问的资源的第 2 表，所述数据库根据来自所述控制装置的请求，响应相当于发送源的用户能访问或不能访问的资源。

[0019] 根据本发明的第 3 观点，提供一种控制装置，与多个转发节点和数据库连接，所述多个转发节点根据处理规则来处理接收数据包，所述处理规则将用于特定流的匹配规则和适用于符合所述匹配规则的数据包的处理内容建立了对应，所述数据库保持有用于根据与发送源有关的信息来特定相当于发送源的用户的角色的第 1 表、和对每个角色定义了能访问或不能访问的资源的第 2 表，根据来自控制装置的请求，响应相当于发送源的用户能访问或不能访问的资源，所述控制装置在从所述转发节点接收到所述处理规则的设定请求的

情况下，使用与所述处理规则的设定请求所包含的发送源有关的信息，对所述数据库查询相当于所述发送源的用户能访问或不能访问的资源，基于来自所述数据库的响应，生成所述处理规则并设定到所述转发节点。

[0020] 根据本发明的第 4 观点，提供一种通信方法，是包含多个转发节点、数据库和控制装置的通信系统中的通信方法，所述多个转发节点根据处理规则来处理接收数据包，所述处理规则将用于特定流的匹配规则和适用于符合所述匹配规则的数据包的处理内容建立了对应，所述数据库保持有用于根据与发送源有关的信息来特定相当于发送源的用户的角色的第 1 表、和对每个角色定义了能访问或不能访问的资源的第 2 表，根据来自控制装置的请求，响应相当于发送源的用户能访问或不能访问的资源，所述控制装置对所述转发节点设定所述处理规则，所述通信方法包括如下步骤：所述控制装置在从所述转发节点接收到所述处理规则的设定请求的情况下，对所述数据库查询相当于所述发送源的用户能访问或不能访问的资源的步骤；和所述控制装置基于来自所述数据库的响应，生成所述处理规则并设定到所述转发节点的步骤。本方法与对处理接收数据包的多个转发节点进行控制的控制装置这样的特定的设备结合。

[0021] 根据本发明的第 5 观点，提供一种程序，是由搭载于控制装置的计算机执行的程序，所述控制装置与多个转发节点和数据库连接并对所述转发节点设定处理规则，所述多个转发节点根据所述处理规则来处理接收数据包，所述处理规则将用于特定流的匹配规则和适用于符合所述匹配规则的数据包的处理内容建立了对应，所述数据库保持有用于根据与发送源有关的信息来特定相当于发送源的用户的角色的第 1 表和对每个角色定义了能访问或不能访问的资源的第 2 表，根据来自控制装置的请求，响应相当于发送源的用户能访问或不能访问的资源，所述程序使所述计算机执行如下处理：在从所述转发节点接收到所述处理规则的设定请求的情况下，对所述数据库查询相当于所述发送源的用户能访问或不能访问的资源的处理；和基于来自所述数据库的响应，生成所述处理规则并设定到所述转发节点的处理。该程序能够记录在计算机可读取的存储介质中。即，本发明也能够作为计算机程序产品来实现。

[0022] 发明的效果

[0023] 根据本发明，不仅能够进行基于流的路径控制，还能够进行基于赋予给各用户的角色的极细的访问控制。

附图说明

[0024] 图 1 是本发明的概要说明图。

[0025] 图 2 是表示本发明的第 1 实施方式的通信系统的结构的图。

[0026] 图 3 是表示本发明的第 1 实施方式的 IAM 的详细结构的图。

[0027] 图 4 是保存在本发明的第 1 实施方式的访问控制策略存储部中的策略信息的一例。

[0028] 图 5 是保存在本发明的第 1 实施方式的资源信息存储部中的资源信息的一例。

[0029] 图 6 是保持在本发明的第 1 实施方式的 ACL 数据库中的访问控制策略信息表的一例。

[0030] 图 7 是保持在本发明的第 1 实施方式的 ACL 数据库中的认证信息表的一例。

[0031] 图 8 是表示本发明的第 1 实施方式的控制装置的结构的框图。

[0032] 图 9 是表示本发明的第 1 实施方式的动作的顺序图。

[0033] 图 10 是表示本发明的第 1 实施方式的动作的另一顺序图。

[0034] 图 11 是用于说明由本发明的第 1 实施方式的结构进行的访问控制的一例的图。

[0035] 图 12 是用于说明由本发明的第 1 实施方式的结构进行的访问控制的另一例的图。

[0036] 图 13 是用于说明由本发明的第 1 实施方式的结构进行的访问控制的又一例的图。

[0037] 图 14 是表示本发明的第 2 实施方式的通信系统的结构的图。

[0038] 图 15 是表示非专利文献 2 所记载的流条目的结构的图。

具体实施方式

[0039] 首先参照附图对本发明的概要进行说明。如图 1 所示，本发明能够通过多个转发节点 200A、200B、数据库 330A 和控制装置 300 来实现，所述多个转发节点 200A、200B 根据处理规则来处理接收数据包，所述处理规则将用于特定流的匹配规则和适用于符合所述匹配规则的数据包的处理内容建立对应，所述数据库 330A 保持第 1、第 2 表 331、332，所述控制装置 300 对转发节点 200A、200B 设定带有效期限的处理规则。此外，该概要所标注的附图标记，是作为用于帮助理解的一例为了方便起见而标注在各要素上的，并不意图将本发明限定于图示的形态。

[0040] 在所述数据库 330A 的第 1 表 331 中，针对通过与用户进行用户认证的认证装置 310 成功完成了认证手续的用户，保存有用于根据与其发送源有关的信息来特定该用户的角色 (Role) 的条目组。此外，第 1 表 331 的条目，优选通过用户的登录或经过预定的认证手续而追加，通过用户的注销或经过一定时间而删除。

[0041] 在所述数据库 330A 的第 2 表 332 中，保存有通过受理来自网络管理者等的访问控制策略信息的输入的策略管理终端 340 对每个角色定义了能访问或不能访问的资源的条目组（访问控制策略）。

[0042] 转发节点 200A 在从用户终端 100 接收到数据包时，检索具有符合该数据包的匹配规则的处理规则。此时，在没有保持具有符合接收数据包的匹配规则的处理规则的情况下，转发节点 200A 向控制装置 300 发送处理规则的设定请求消息（参照图 1 的 (1) 处理规则设定请求）。

[0043] 控制装置 300 在从管理对象的转发节点 200A 或 200B 受理了处理规则的设定请求后，提取处理规则的设定请求所包含的 IP 地址和 / 或 MAC(Media Access Control :媒体访问控制）地址等有关发送源的信息，向数据库 330A 查询从该发送源能访问的资源或不能访问的资源的列表（参照图 1 的 (2) 查询）。

[0044] 接受所述查询的数据库 330A，首先参照第 1 表 331 来特定从控制装置 300 接受查询的相当于发送源的用户的角色。接着，数据库 330A 参照第 2 表 332 来提取所述特定的角色能访问的资源或不能访问的资源的列表，并响应给控制装置 300。

[0045] 接收了所述列表的控制装置 300，通过对所述列表与接受处理规则的设定请求的发送目标进行核对，判断是否可以生成到接受处理规则的设定请求的发送目标为止的路径。在此，例如在所述处理规则的设定请求为寻求从相当于发送源的用户向其访问权限内的发送目标（例如网络资源 600）的路径生成和用于实现该路径生成的处理规则的设定的

情况下，控制装置 300 生成相当于发送源的用户的用户终端 100 与网络资源 600 之间的路径，对该路径上的转发节点设定处理规则（图 1 的 (3A)、(3B) 处理规则设定）。另一方面，在所述处理规则的设定请求超出相当于发送源的用户的访问权限的情况下，拒绝所述处理规则的设定请求。在该情况下，控制装置 300 可以对转发节点 200A 设定将来自该用户的后续数据包废弃的处理规则。

[0046] 通过以上所述，在接收到处理规则的设定请求时，能够特定相当于其发送源的用户的角色，根据另行由策略管理终端 340 设定的访问控制策略，判别是否可以允许向网络资源 600 的访问。此外，对处理规则设置有效期限，在从设定到转发节点 200A、200B 起、或从最后接收到符合匹配规则的数据包起经过了所述有效期限的情况下，可以删除该处理规则。

[0047] 另外，在从所述数据库 330A 响应来的列表中明确有禁止从该用户访问的资源的情况下，控制装置 300 可以对转发节点 200A 和 / 或转发节点 200B 设定将来自该用户的数据包废弃的处理规则。由此，能够抑制之后的因来自该用户的数据包接收所产生的处理规则的设定请求，能够降低控制装置 300 的负载。

[0048] [第 1 实施方式]

[0049] 接着，参照附图详细说明本发明的第 1 实施方式。图 2 是表示本发明的第 1 实施方式的通信系统的结构图。参照图 2，示出了 ：多个转发节点 200A、200B、200C ；对这些转发节点设定处理规则的控制装置 300 ；根据来自控制装置 300 的查询来响应访问控制列表信息 (ACL 信息) 的 ACL 数据库 330 ；进行与用户终端 100A 的认证手续并将认证结果登记到 ACL 数据库 330 中的认证装置 310 ；对 ACL 数据库 330 提供基于角色的 ACL 信息的综合访问管理装置 (Integrated Access Manager ；以下记为“ IAM”。)320。

[0050] 转发节点 200A、200B、200C 是根据处理规则来处理接收数据包的交换机装置，所述处理规则将用于特定流的匹配规则和适用于所述匹配规则的处理内容建立对应。作为这样的转发节点 200A、200B、200C，也可以使用将图 15 所示的流条目作为处理规则进行动作的非专利文献 2 的 OpenFlow 交换机。另外，在本实施方式中，转发节点 200A 配置于东京总公司，受理从东京总公司的用户终端 100A 向业务服务器 600A、管理工具 600B 的数据包。同样，转发节点 200B 配置于大阪分公司，受理从大阪分公司的用户终端 100B 向业务服务器 600A、管理工具 600B 的数据包。

[0051] 另外，转发节点 200C 连接有业务服务器 600A 和管理工具 600B。业务服务器 600A 是提供东京总公司和 / 或大阪分公司的用户在日常业务中使用的服务的服务器。管理工具 600B 提供这些业务服务器的设定和 / 或用于更新 ACL 数据库的各表的管理工具。在以下的说明中，对业务服务器 600A 赋予 resource_group_0001 作为资源组 ID，对管理工具 600B 赋予 resource_group_0002 作为资源组 ID。

[0052] 认证装置 310 是使用密码或生物特征认证信息等与用户终端 100A、100B 进行用户认证手续的认证服务器等。认证装置 310 将表示与用户终端 100A、100B 的用户认证手续的结果的认证信息发送到 ACL 数据库 330。这样的认证装置 310 能够使用被称为 LDAP(Lightweight Directory Access Protocol ：轻量目录访问协议) 服务器或 RADIUS 认证服务器的设备来实现。

[0053] 图 3 是表示 IAM320 的详细结构的框图。参照图 3，示出了包括访问控制策略存储

部 321、资源信息存储部 322 和访问控制策略管理部 323 的结构。

[0054] 访问控制策略管理部 323 从网络管理者等操作的策略管理终端 340 受理向访问控制策略存储部 321 和 / 或资源信息存储部 322 登记的内容，并登记到访问控制策略存储部 321 或资源信息存储部 322 中。

[0055] 图 4 是保存在访问控制策略存储部 321 中的策略信息的一例。在图 4 的例子中，按以角色 ID 识别的每个角色，示出了对资源的组赋予的资源组 ID 和设定了访问权限的策略信息。例如，持有角色 ID :role_0001 的用户被允许 (allow) 向资源组 ID :resource_group_0001、resource_group_0002 双方的访问。另一方面，角色 ID :role_0002 的用户被禁止 (deny) 向资源组 ID :resource_group_0001 的访问，并被允许向 resource_group_0002 的访问。

[0056] 图 5 是保存在资源信息存储部 322 中的资源信息的一例。在图 5 的例子中，成为将上述的属于资源组 ID 的资源的资源 ID 和其详细属性相对应的内容。例如，在由资源组 ID :resource_group_0001 特定的组中，包含持有 resource_0001、resource_0002、resource_0003 的资源，能够特定各自的 IP 地址、MAC 地址和 / 或用于服务的端口号等。

[0057] 图 6 是保持在 ACL 数据库 330 中的访问控制策略信息表 332 的一例。参照图 6，示出了按每个角色 ID 保存将 IP 地址和 / 或 MAC 地址等发送目标信息、EtherType、Protocol、端口号的范围（下限值～上限值）等条件（通信条件）、访问权限、优先级建立了对应的条目的访问控制策略信息表。例如，持有角色 ID :role0001 的用户，在 EtherType ＝ 4(IPv4)、Protocol ＝ 6(TCP)、端口号＝ 80 这种条件下，被允许 (allow) 向具有 IP 地址＝ 192.168.0.1、MAC 地址＝ 00-00-00-11-22-33 的资源的访问。这样的条目能够通过将与图 4 所示的策略信息的条目的资源 ID 对应的详细数据从资源信息存储部 322 中取出来生成。此外，访问控制策略信息表 332 的优先级字段，在设定有在同一个或 2 个以上的角色 ID 间进行竞争的条目的情况下在决定向控制装置 300 侧回答的内容时使用。具体的优先级例如通过各角色的优劣和 / 或包含关系来决定即可。

[0058] 图 7 是保持在 ACL 数据库 330 中的认证信息表 331 的一例。例如，在用户 ID 为 user1 的用户的认证成功的情况下，认证装置 310 在认证信息表 331 中登记具有 user1、IP 地址 :192.168.100.1、MAC 地址 :00-00-00-44-55-66 这样的发送源信息、角色 ID :role0001、适当设定的有效期限的条目。同样，在用户 ID 为 user10 的用户的认证成功的情况下，认证装置 310 在认证信息表 331 中登记 user10、IP 地址 :192.168.100.10 这种属性、角色 ID :role_0010 这样的 user10 的条目。此外，图 7 的发送源信息的用户 ID 字段可以适当省略。另外，作为发送源信息不必需使用 IP 地址和 MAC 地址的组，也可以省略其中一方，或取代它们而使用与该用户终端 100 连接的转发节点的 ID。另外，在本实施方式中，认证信息表 331 的各条目在该用户注销时或超过在有效期限字段中设定的有效期限（过期）时被删除。

[0059] 另外，在上述的访问控制策略存储部 321 或资源信息存储部 322 的内容被更新时，访问控制策略管理部 323 从 ACL 数据库 330 的访问控制策略信息表 332（参照图 6）中提取应反映所述更新内容的条目，并进行反映该内容的处理。例如，在从持有角色 ID :role_0001 的用户能访问的资源中删除了资源组 ID :resource_group_0002 的情况下，访问控制策略管理部 323 参照资源信息存储部 322 来特定属于资源组 ID :resource_

group_0002 的资源，在图 6 的访问控制策略信息表 332 的持有角色 ID :role_0001 的条目中，删除定义了向属于资源组 ID :resource_group_0002 的资源的访问权限的条目或将该条目的访问权限变更为 deny。

[0060] 同样，例如在资源组 ID :resource_group_0002 中添加了新资源的情况下，访问控制策略管理部 323 参照访问控制策略存储部 321 来特定允许或禁止向资源组 ID :resource_group_0002 的访问的角色，在图 6 的访问控制策略信息表 332 中，作为从角色 ID :role_0001 能够访问或禁止访问的资源，添加定义了所述新资源的条目。

[0061] ACL 数据库 330 在被从控制装置 300 请求从任意的发送源能访问的资源或不能访问的资源的列表时，确认在认证信息表 331 中是否登记了相当于发送源信息的用户（是否正确地进行了认证）。在所述发送源已登记在认证信息表 331 中的情况下，将与该发送源关联的角色 ID 作为关键字，检索访问控制策略信息表 332，响应表示设定为相当于该发送源的用户能访问或不能访问的资源和其条件的列表。

[0062] 控制装置 300 在从转发节点 200A ～ 200C 接收到处理规则的设定请求时，向上述那样的 ACL 数据库 330 查询相当于所述发送源的用户能访问或不能访问的资源，基于其结果生成处理规则，并设定到转发节点 200A ～ 200C。

[0063] 图 8 是表示本实施方式的控制装置 300 的详细结构的框图。参照图 8，控制装置 300 构成为包括 :与转发节点 200A ～ 200C 进行通信的节点通信部 11、控制消息处理部 12、处理规则管理部 13、处理规则存储部 14、转发节点管理部 15、处理规则生成部 16、拓扑管理部 17、终端位置管理部 18、ACL 信息查询部 19。它们分别如下述这样进行动作。

[0064] 控制消息处理部 12 对从转发节点 200A ～ 200C 接收到的控制消息进行解析，并将控制消息信息交付给控制装置 300 内的对应的处理单元。

[0065] 处理规则管理部 13 管理对哪个转发节点设定怎样的处理规则。具体而言，将由处理规则生成部 16 生成的处理规则登记到处理规则存储部 14 中，设定到转发节点，并通过来自转发节点的处理规则删除通知等更新处理规则存储部 14 的登记信息，还应对于对转发节点设定的处理规则发生了变更的情况来更新处理规则存储部 14 的登记信息。

[0066] 转发节点管理部 15 管理由控制装置 300 控制的转发节点的能力（例如，端口的数量和 / 或种类、所支持的动作的种类等）。

[0067] 处理规则生成部 16 经由 ACL 信息查询部 19 向 ACL 数据库 330 查询与预定规则的设定请求的相当于发送源的用户的角色对应的访问控制策略信息表 332 的条目，基于其响应内容判断是否设定处理规则。在所述判断的结果是判断为能够设定处理规则的情况下，处理规则生成部 16 生成基于该内容的路径，并生成实现该路径的处理规则。

[0068] 更具体而言，处理规则生成部 16 基于由终端位置管理部 18 管理的通信终端的位置信息和由拓扑管理部 17 构筑的网络拓扑信息，计算从用户终端向有访问权的资源转发数据包的转发路径。接着，处理规则生成部 16 从转发节点管理部 15 获得所述转发路径上的转发节点的端口信息等，求出为了实现所述计算出的转发路径而使路径上的转发节点执行的动作和用于特定适用该动作的流的匹配规则。此外，所述匹配规则能够使用处理规则的设定请求所包含的发送源 IP 地址、发送目标 IP 地址、条件（选项）等来生成。

[0069] 例如，在因图 6 的持有角色 ID :role_0001 的用户发向管理工具 600B 的数据包的接收而接收到处理规则的设定请求的情况下，首先，处理规则生成部 16 基于来自 ACL 数据

库 330 的响应，确认是否允许向管理工具 600B 的访问。然后，处理规则生成部 16 生成确定使从所述用户发向管理工具 600B 的数据包从成为下一个转发点 (hop) 的转发节点 200C 或转发节点 200C 的与管理工具 600B 连接的端口转发的动作的各处理规则。

[0070] 另外，针对没有访问权的资源，处理规则生成部 16 基于由终端位置管理部 18 管理的用户终端的位置信息，对与该用户终端连接的转发节点生成制定了将从该用户终端向没有访问权的资源的数据包废弃的动作和匹配规则的处理规则。例如，由于持有角色 ID：role_0001 的用户向 IP 地址 192.168.0.3 的访问权限被设定为“deny”，所以生成并设定将发向 IP 地址 192.168.0.3 的数据包废弃的处理规则。

[0071] 拓扑管理部 17 基于经由节点通信部 11 收集到的转发节点 200A ～ 200C 的连接关系来构筑网络拓扑信息。

[0072] 终端位置管理部 18 管理用于特定与通信系统连接的用户终端的位置的信息。在本实施方式中，作为用于识别用户终端的信息而使用 IP 地址，作为用于特定用户终端的位置的信息而使用与用户终端连接的转发节点的转发节点标识符及其端口的信息来进行说明。当然也可以取代这些信息而使用例如从认证装置 310 带来的信息等来确定终端及其位置。

[0073] ACL 信息查询部 19 基于来自处理规则生成部 16 的请求，对 ACL 数据库 330 查询被设定为预定规则的设定请求的发送源所对应的用户能访问或不能访问的发送目标的列表。

[0074] 以上那样的控制装置 300，也能够通过对非专利文献 1、2 的 OpenFlow 控制器添加上述的 ACL 信息查询部 19 和基于其响应结果的处理规则（流条目）的生成功能来实现。

[0075] 另外，图 3 所示的控制装置 300 的各部（处理单元），也能够通过使用构成控制装置 300 的计算机的硬件来存储上述的各信息并使计算机执行上述的各处理的计算机程序来实现。

[0076] 接着，参照附图对本实施方式的动作进行详细说明。首先，参照图 9 说明由认证装置 310 进行的认证信息表 331 的更新处理以及由 IAM320 进行的访问控制策略信息表 332 的更新处理。

[0077] 当从用户终端 100 接收到登记请求时（图 9 的 S001），认证装置 310 与用户终端 100 进行预定的手续来进行用户认证（图 9 的 S002）。

[0078] 在此，假定为用户认证成功的情况来说明。在该情况下，认证装置 310 生成向图 6 所示的认证信息表 331 登记的条目，更新 ACL 数据库 330 的认证信息表 331（图 9 的 S003、S004）。通过以上的处理，在图 6 的认证信息表 331 中添加具有新的用户、其角色 ID 以及有效期限的条目。

[0079] 与上述用户认证手续相独立地，通过网络管理者等经由策略管理终端 340 对保持在 IAM320 的访问控制策略存储部 321 和 / 或资源信息存储部 322 中的数据进行更新（图 9 的 S005）。

[0080] 受理了所述数据的更新的 IAM320 基于更新后的内容，决定图 6 的访问控制策略信息表 332 的更新内容（图 9 的 S006）。此处的更新内容如上述那样，根据策略信息中的各角色的权限内容的变更和 / 或资源信息的详细内容的变更来决定。

[0081] 接着，IAM320 根据所述决定的内容对 ACL 数据库 330 更新访问控制策略信息表 332（图 9 的 S007、S008）。

[0082] 接着，参照图 10 对使用如上述那样更新的 ACL 数据库 330 的内容的处理规则的设定处理的流程进行详细说明。参照图 10，首先用户终端 100 在发送发向业务服务器 600A 的数据包时（图 10 的 S101），转发节点 200A 检索与该数据包对应的处理规则，并试图进行数据包处理。

[0083] 在此，由于没有对转发节点 200A 设定与该数据包对应的处理规则，所以转发节点 200A 对控制装置 300 请求处理规则的设定（图 10 的 S102）。

[0084] 接收到所述处理规则的设定请求的控制装置 300，利用所述处理规则的设定请求所包含的 IP 地址和 / 或 MAC 地址等来特定发送源（图 10 的 S103）。然后，控制装置 300 从 ACL 数据库 330 获取与相当于所述特定的发送源的用户的角色对应的访问控制策略信息表 332 的条目（图 10 的 S104）。

[0085] 控制装置 300 通过对所述访问控制策略信息表 332 的条目和接收到处理规则的设定请求的发送目标进行核对，判断是否可以生成路径。在此，在判断为可生成路径的情况下，控制装置 300 进行路径计算并生成制定各转发节点的数据包处理内容的处理规则（图 10 的 S105）。

[0086] 当控制装置 300 对路径上的转发节点设定了处理规则后（图 10 的 S106-1、S106-2），能够实现用户终端与业务服务器间的通信（图 10 的“通信开始”）。

[0087] 如上所述，由于由 IAM320 管理的内容及认证装置 310 中的认证处理的结果由 ACL 数据库来统一管理，并使控制装置 300 根据需要参照该结果来生成处理规则，所以，例如如图 11 所示，对于管理者和一般职员，仅通过管理持有角色 ID :role_0001、角色 ID :role_0002 这 2 个角色 ID 就能够进行恰当的访问控制。进而，此时，也能够根据图 6 所示的访问控制策略信息表 332 的条件字段的各项目，添加端口号的范围和 / 或协议的制限。

[0088] 另外，通过在图 6 所示的访问控制策略信息表 332 中添加允许访问的位置信息字段，除了接收到所述处理规则的设定请求的转发节点以外，也能够对与所述位置信息字段对应的转发节点设定处理规则。由此，还能够实现与位置相应的访问制限，例如如图 12 所示，在持有角色 ID :role_0001 的管理者从东京总公司进行访问的情况下，允许向业务服务器、管理工具双方的访问，而在因出差等从大阪分公司进行访问的情况下，限制向管理工具的访问等这样的与位置相应的访问制限。当然也能够全面禁止从大阪分公司的访问，这能够通过经由 IAM320 重写访问控制策略存储部 321 的数据，或经由管理工具 600B 重写访问控制策略信息表 332 来实现。

[0089] 另外，例如如图 13 所示，通过对大阪分公司的转发节点组 201 设定允许从一般职员的用户终端向业务服务器 600A 的访问的处理规则，也能够允许持有角色 ID :role_0002 的一般职员因出差等从大阪分公司进行访问。这样的控制也能够通过经由 IAM320 重写访问控制策略存储部 321 的数据，或经由管理工具 600B 重写访问控制策略信息表 332 来实现。

[0090] 另外，控制装置 300 也可以以预定的时间间隔访问 ACL 数据库 330，并确认是否需要设定处理规则或确认已有的处理规则的妥当性。如此一来，也能够实施如下这样的访问限制 :例如在某期间（例如，2011/04/01 ～ 2011/06/01）或某时间段（例如，10:00 ～ 17:30）中，允许向管理工具 600B 的访问，在此以外的期间或时间限制向管理工具 600B 的访问。另外，在这些期间中，在临时对访问权限进行了修正的情况下，也能够将其内容反映在

处理规则上。当然也能够实施组合了上述的位置、时间、期间的访问制限。

[0091] [第 2 实施方式]

[0092] 接着，参照附图对配置有多个控制装置的本发明的第 2 实施方式进行详细说明。图 14 是表示本发明的第 2 实施方式的通信系统的结构的图。以下，在本发明的第 2 实施方式中，因为能够通过与第 1 实施方式同样的构成要素来实现，所以以下以不同点为中心来说明。

[0093] 参照图 14，示出了如下结构：通过 3 台控制装置 300D ～ 300F 和按照从这些控制装置 300D ～ 300F 设定的处理规则进行动作的转发节点 200D ～ 200F 分别构成关东数据中心、北海道数据中心、冲绳数据中心，并将这三个中心彼此连接。此外，图 14 中的控制装置及转发节点的数量，是用于简单地说明本实施方式的例示，并不限定于这些数量。另外，虽然图 14 中进行了省略，但也可以在北海道数据中心和 / 或冲绳数据中心配置认证装置 310。

[0094] 认证装置 310 及 IAM320 的基本功能与上述的第 1 实施方式的认证装置及 IAM 相同。不同点在于：本实施方式的认证装置 310 与利用关东数据中心、北海道数据中心、冲绳数据中心的用户进行认证手续，将其结果登记在 ACL 数据库 330 的认证信息表 331 中。

[0095] 控制装置 300D ～ 300F 能够分别访问 ACL 数据库 330，在从下属的转发节点 200D ～ 200F 接收到处理规则的设定请求时，向 ACL 数据库 330 查询与相当于其发送源的用户对应的访问权限，并基于该结果设定处理规则。此外，在图 14 的例子中，虽然示出了控制装置 300D ～ 300F 与 ACL 数据库 330 之间直接进行查询及响应，但也可以经由转发节点 200D ～ 200F 转发控制装置 300D ～ 300F 与 ACL 数据库 330 间的查询及其响应。

[0096] 如以上的本实施方式所示，本发明也能够容易地应对转发节点、用户的增多和随之的控制装置的扩展 (scale out)。

[0097] 以上说明了本发明的各实施方式，但本发明并不限定于上述的实施方式，在不脱离本发明的基本技术思想的范围内，能够进行进一步的变形、替换、调整。例如，在上述的各实施方式中，说明了控制装置 300、认证装置 310、IAM320 分别独立地设置的结构，但也可以采用将它们适当整合的结构。

[0098] 另外，在上述的实施方式中，说明了用户终端 100A、100B 向认证装置 310 直接进行认证手续的结构，但也可以采用将认证手续涉及的认证用数据包经由转发节点转发到认证装置来实施认证手续的结构。例如，能够通过对与用户终端 100A、100B 连接的转发节点设定用于特定认证用数据包的匹配规则和制定了将该数据包转发到认证装置 310 的动作的处理规则来实现。

[0099] 最后，简要说明本发明优选的方式。

[0100] [方式 1]

[0101] 如所述第 1 观点所记载的通信系统那样。

[0102] [方式 2]

[0103] 在所述方式 1 中，优选的是，

[0104] 所述第 2 表的条目使用对赋予给用户的每个角色定义了能访问或不能访问的资源的组的访问控制策略信息和定义了属于所述各组的资源的详细内容的资源信息来生成。

[0105] [方式 3]

[0106] 在所述方式 2 中，优选的是，

[0107] 还具备访问策略管理部，该访问策略管理部在访问控制策略信息和资源信息的至少一方被更新的情况下，更新所述第 2 表的与所述被更新的位置对应的条目。

[0108] [方式 4]

[0109] 在所述方式 1 ～方式 3 的任一方式中，优选的是，

[0110] 所述第 1 表登记有认证成功的用户的条目，通过所述用户注销，从所述第 1 表中删除所述用户的条目。

[0111] [方式 5]

[0112] 在所述方式 1 ～方式 4 的任一方式中，优选的是，

[0113] 在所述第 1 表的各条目中设定有有效期限，所述数据库是将经过了所述有效期限的条目从所述第 1 表中删除的数据库。

[0114] [方式 6]

[0115] 在所述方式 1 ～方式 5 的任一方式中，优选的是，还包括 ：

[0116] 进行用户认证并更新所述第 1 表的认证装置 ；和

[0117] 受理所述第 2 表的更新内容的输入并更新所述第 2 表的策略管理终端。

[0118] [方式 7]

[0119] 在所述方式 1 ～方式 6 的任一方式中，优选的是，

[0120] 所述控制装置基于来自所述数据库的响应，对预定的转发节点设定将从相当于所述发送源的用户向被禁止访问的资源的数据包废弃的处理规则。

[0121] [方式 8]

[0122] 在所述方式 1 ～方式 7 的任一方式中，优选的是，

[0123] 在来自所述数据库的响应中，包含相当于所述发送源的用户能否访问所述资源的位置信息，

[0124] 所述控制装置在从所述转发节点接收到所述处理规则的设定请求的情况下，不仅对接收到所述处理规则的设定请求的转发节点，还对与所述位置信息对应的转发节点设定访问所述资源或禁止访问所述资源的处理规则。

[0125] [方式 9]

[0126] 如所述第 2 观点所记载的数据库那样。

[0127] [方式 10]

[0128] 如所述第 3 观点所记载的控制装置那样。

[0129] [方式 11]

[0130] 如所述第 4 观点所记载的通信方法那样。

[0131] [方式 12]

[0132] 如所述第 5 观点所记载的程序那样。

[0133] 此外，所述数据库、控制装置、通信方法以及程序，能够如方式 1 的通信系统那样，同样地展开成方式 2 ～方式 8。

[0134] 此外，将上述的专利文献及非专利文献的公开内容引用于本说明书中。在本发明的全部公开（包含权利要求书）的框架内，进而基于其基本的技术思想能够进行实施方式的变更、调整。另外，在本发明的权利要求书的框架内能够进行各种公开要素（包含各权利要求的各要素、各实施例的各要素、各附图的各要素等）的多种组合乃至选择。也就是说，

本发明当然包含本领域技术人员根据包含权利要求书在内的全部公开、技术思想所能够想到的各种变形、修正。

[0135] 附图标记说明

[0136] 11 节点通信部

[0137] 12 控制消息处理部

[0138] 13 处理规则管理部

[0139] 14 处理规则存储部

[0140] 15 转发节点管理部

[0141] 16 处理规则生成部

[0142] 17 拓扑管理部

[0143] 18 终端位置管理部

[0144] 19 ACL 信息查询部

[0145] 100、100A、100B 用户终端

[0146] 200A ～ 200F 转发节点

[0147] 201 转发节点组

[0148] 300、300D ～ 300F 控制装置

[0149] 310 认证装置

[0150] 320 综合访问管理装置 (IAM)

[0151] 321 访问控制策略存储部

[0152] 322 资源信息存储部

[0153] 323 访问控制策略管理部

[0154] 330 ACL 数据库

[0155] 330A 数据库

[0156] 331 认证信息表 (第 1 表)

[0157] 332 访问控制策略信息表 (第 2 表)

[0158] 340 策略管理终端

[0159] 600 网络资源

[0160] 600A 业务服务器

[0161] 600B 管理工具

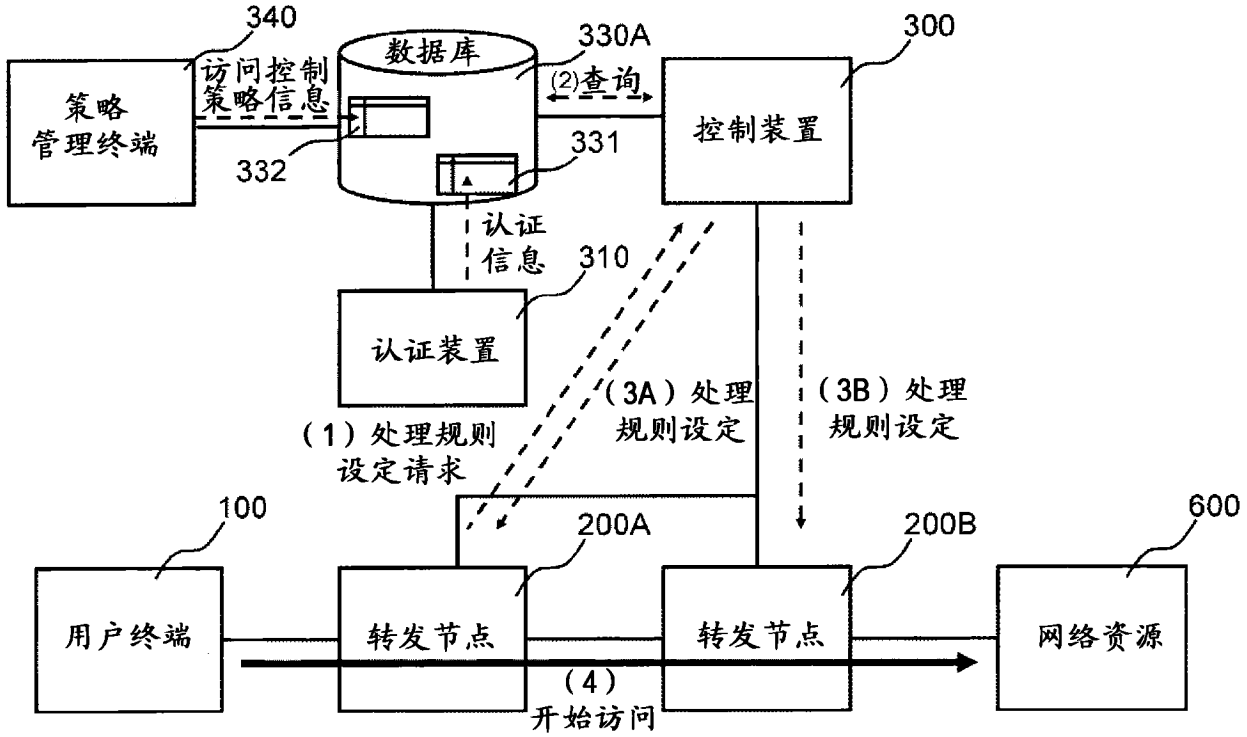

340
访问控制
策略信息
策略
管理终端
数据库
330A
(2)查询
300
控制装置
332
331
认证
信息
310
认证装置
(1)处理规则
设定请求
(3A)处理
规则设定
(3B)处理
规则设定
100
200A
200B
600
用户终端
转发节点
转发节点
网络资源
(4)
开始访问

图 1

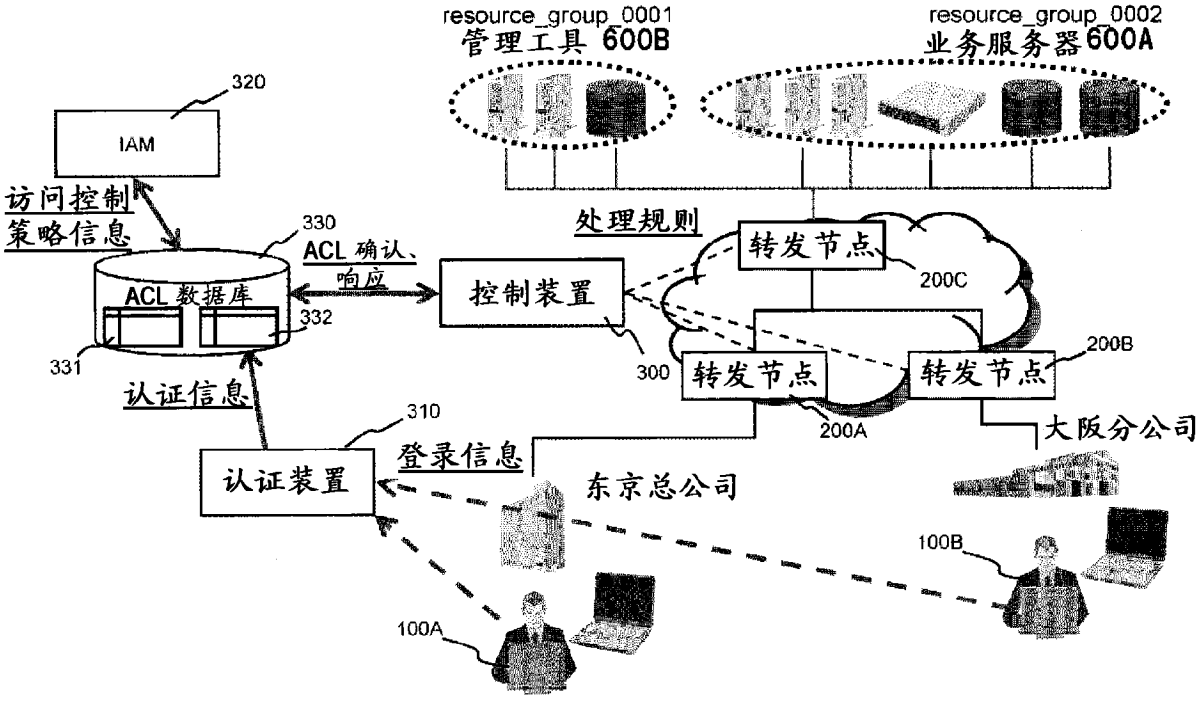

resource_group_0001
管理工具 600B
resource_group_0002
业务服务器600A
320
IAM
访问控制
策略信息
330
ACL 确认、
响应
ACL 数据库
332
331
认证信息
控制装置
300
处理规则
转发节点
200C
转发节点
转发节点
200B
200A
大阪分公司
310
认证装置
登录信息
东京总公司
100B
100A

图 2

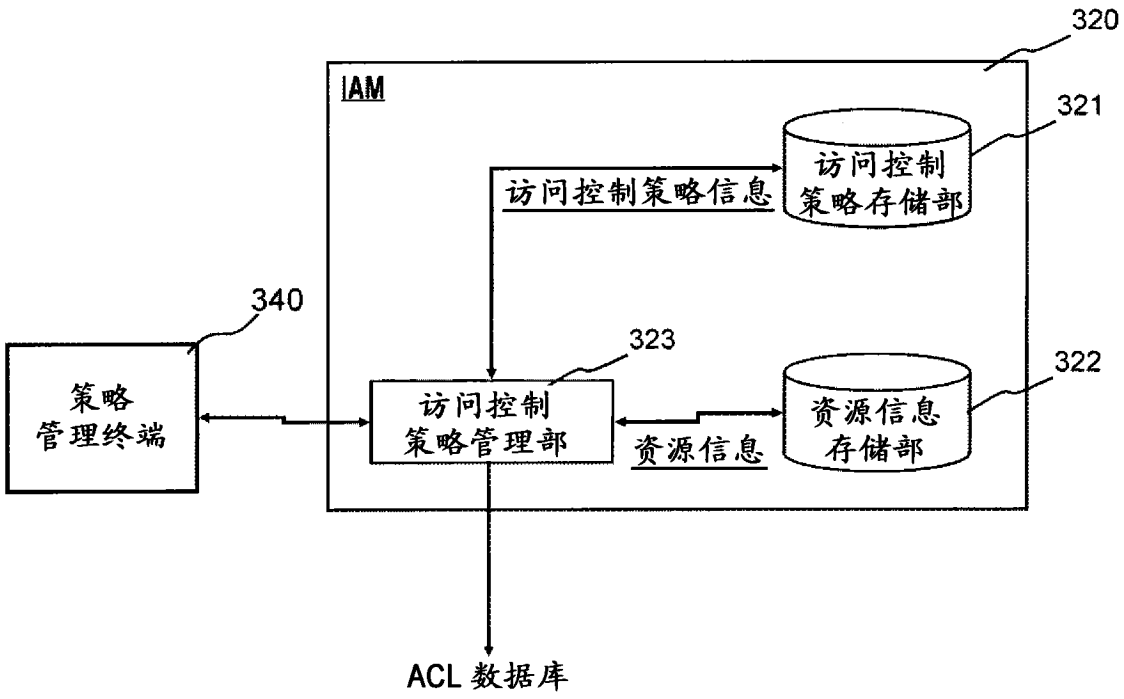


图 3

角色 ID	资源组 ID	访问权限
role_0001	resource_group_0001	allow
role_0001	resource_group_0002	allow
role_0002	resource_group_0001	deny
role_0002	resource_group_0002	allow
:	:	:

图 4

资源组 ID	资源 ID	资源属性
resource_group_0001	resource_0001	IP:192.168.0.1 MAC:00-00-00-11-22-33 SERVICE:80/tcp Ether Type:4 Priority:101 :
	resource_0002	IP:192.168.0.2 :
	resource_0010	IP:10.10.10.0/24 :
resource_group_0002	resource_000X	IP:YYY.YYY.Y.Y
	:	:
:	:	:

图 5

角色 ID	发送目标信息		条件				访问权限	优先级
	发送目标 IP 地址	MAC 地址	Ether Type	Protocol	发送目标端口号下限值	发送目标端口号上限值		
role_0001	192.168.0.1	00-00-00-11-22-33	4	6	80	80	allow	101
	192.168.0.2		4	6	0	65535	allow	102
	192.168.0.3		4	6	0	1023	deny	103
role_0002	192.168.100.0/24		4	6	3389	3389	deny	201
role_0010	10.10.10.0/24		4	6	80	80	allow	1001
	10.10.10.0/24		4	6	443	443	allow	1002
	0.0.0.0/0		4	17	53	53	allow	1003
:		:				:	:	:

图 6

用户信息（发送源信息）			角色 ID	有效期限信息
IP 地址	MAC 地址	用户 ID		
192.168.100.1	00-00-00-44-55-66	user1	role_0001	2011/11/11 11:11:11
192.168.100.10		user10	role_0010	2011/2/15 23:59:59
192.168.200.0/24		server1	role_s001	
:	:	:	:	:

图 7

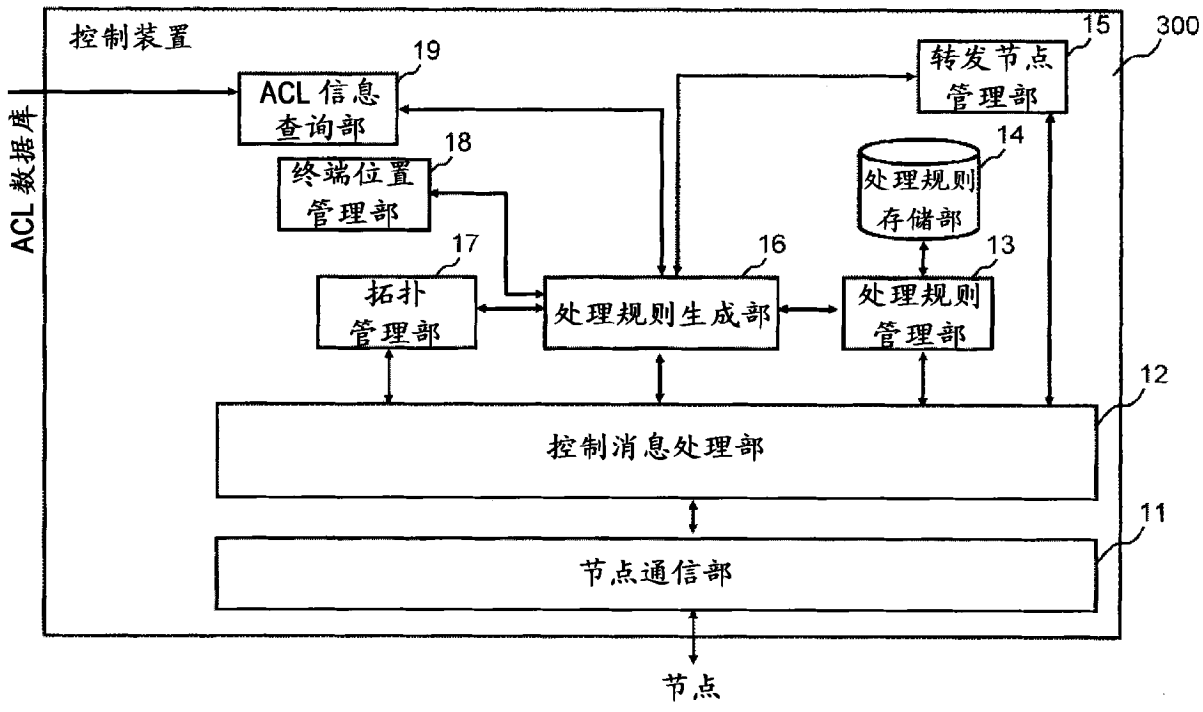


图 8

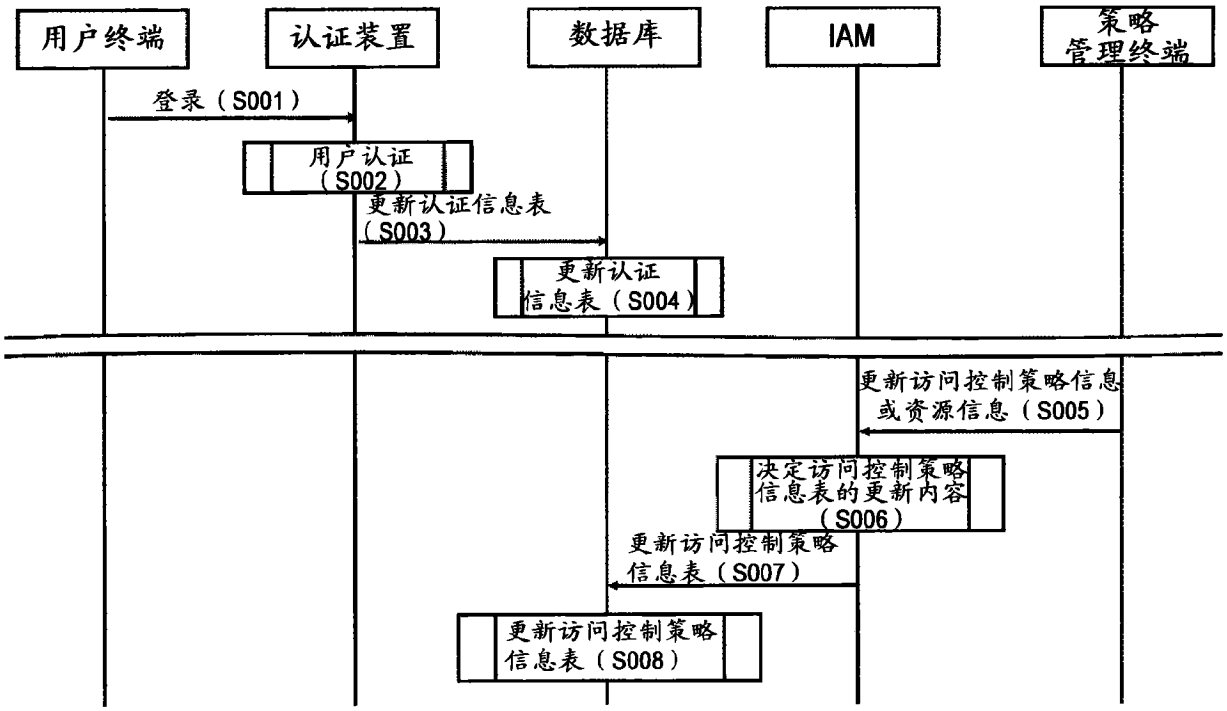

用户终端
认证装置
数据库
IAM
策略管理终端
登录（S001）
用户认证（S002）
更新认证信息表（S003）
更新认证信息表（S004）
更新访问控制策略信息或资源信息（S005）
决定访问控制策略信息表的更新内容（S006）
更新访问控制策略信息表（S007）
更新访问控制策略信息表（S008）

图 9

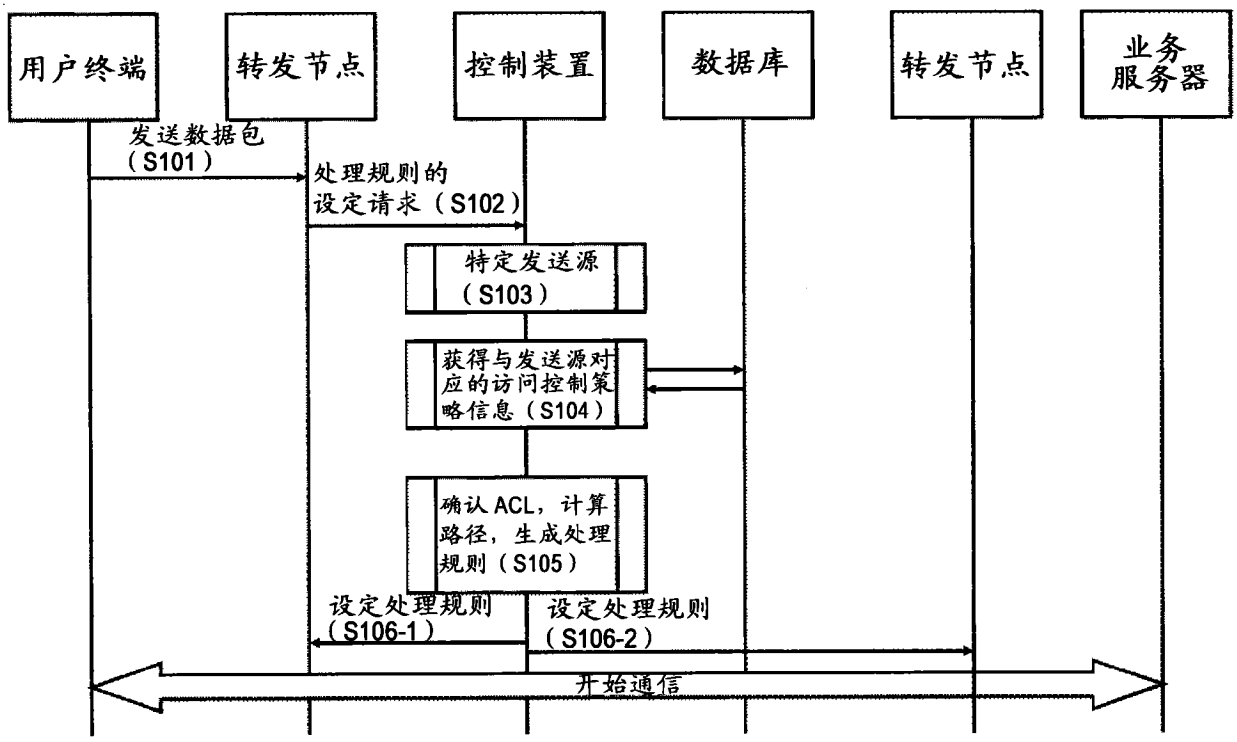

用户终端
转发节点
控制装置
数据库
转发节点
业务服务器
发送数据包（S101）
处理规则的设定请求（S102）
特定发送源（S103）
获得与发送源对应的访问控制策略信息（S104）
确认 ACL，计算路径，生成处理规则（S105）
设定处理规则（S106-1）
设定处理规则（S106-2）
开始通信

图 10

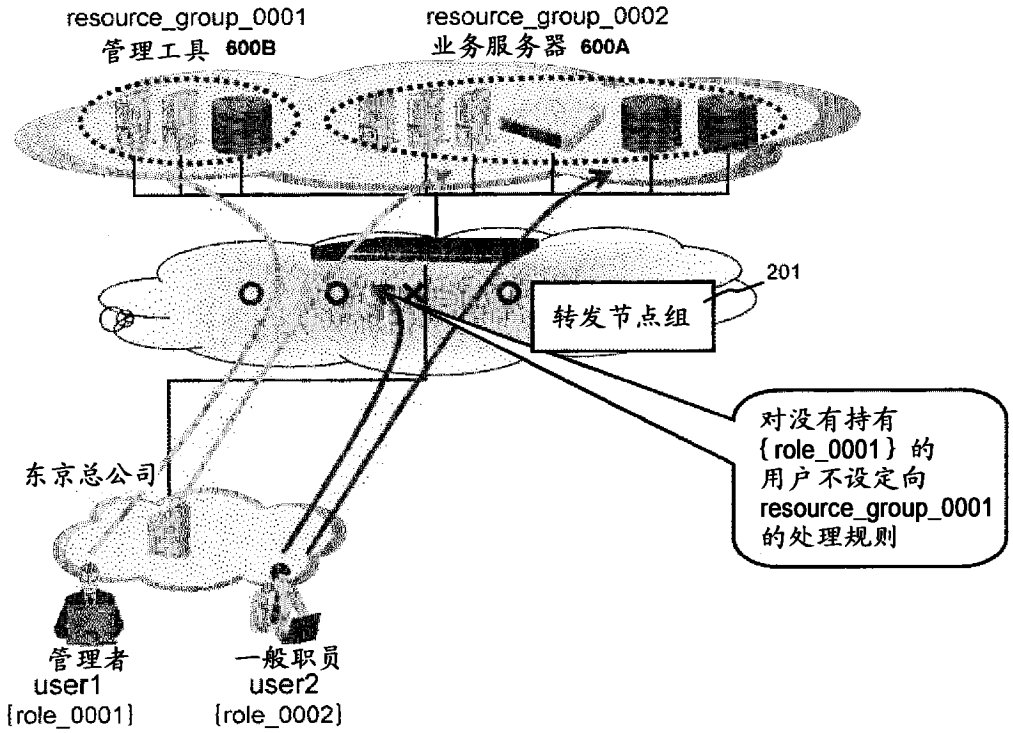

resource_group_0001
管理工具 600B
resource_group_0002
业务服务器 600A
201
转发节点组
对没有持有
{role_0001}的
用户不设定向
resource_group_0001
的处理规则
东京总公司
管理者
user1
{role_0001}
一般职员
user2
{role_0002}

图 11

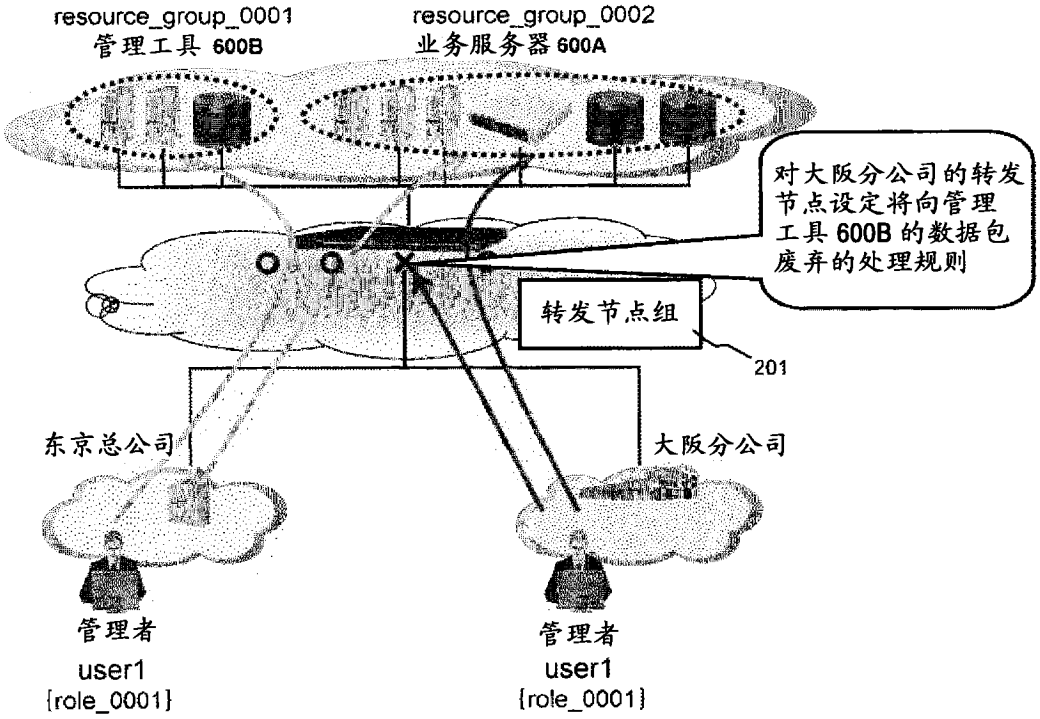

resource_group_0001
管理工具 600B
resource_group_0002
业务服务器 600A
对大阪分公司的转发
节点设定将向管理
工具 600B 的数据包
废弃的处理规则
转发节点组
201
东京总公司
大阪分公司
管理者
user1
{role_0001}
管理者
user1
{role_0001}

图 12

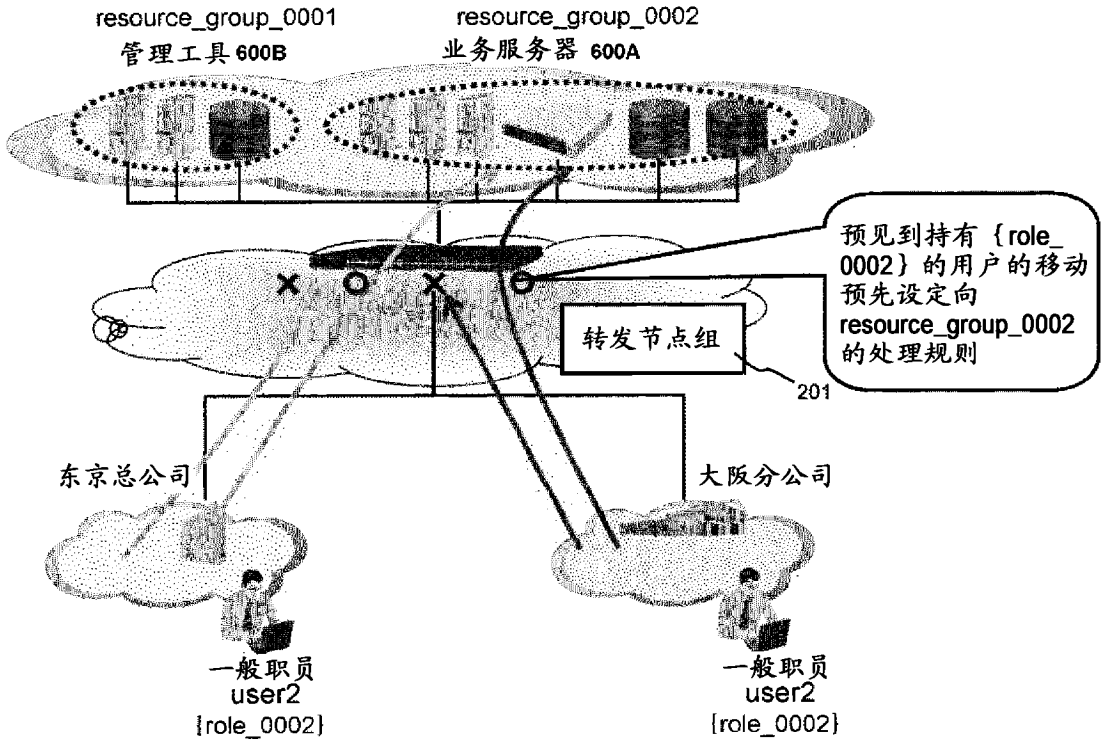

resource_group_0001
管理工具 600B
resource_group_0002
业务服务器 600A
预见到持有｛role_0002｝的用户的移动预先设定向resource_group_0002的处理规则
转发节点组
201
东京总公司
大阪分公司
一般职员
user2
{role_0002}
一般职员
user2
{role_0002}

图 13

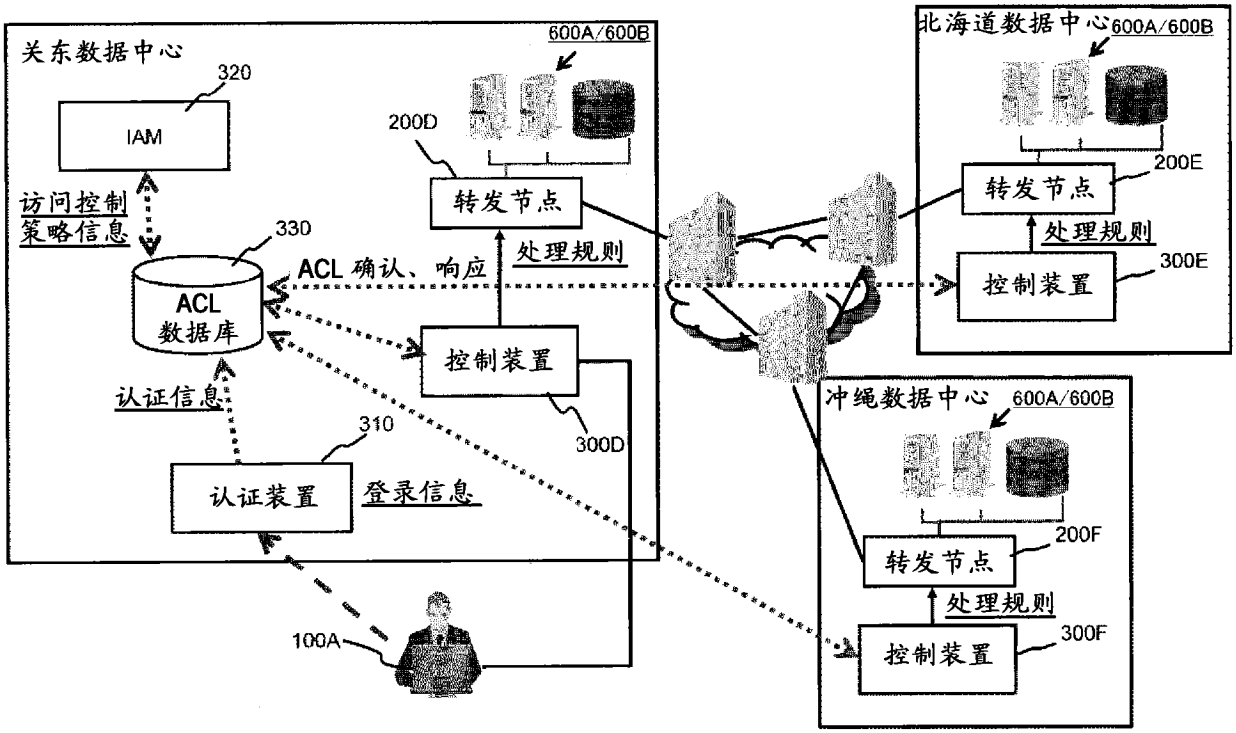

关东数据中心
600A/600B
320
IAM
访问控制策略信息
330
ACL 数据库
ACL 确认、响应
200D
转发节点
处理规则
控制装置
300D
认证信息
310
认证装置
登录信息
100A
北海道数据中心 600A/600B
200E
转发节点
处理规则
300E
控制装置
冲绳数据中心 600A/600B
200F
转发节点
处理规则
300F
控制装置

图 14

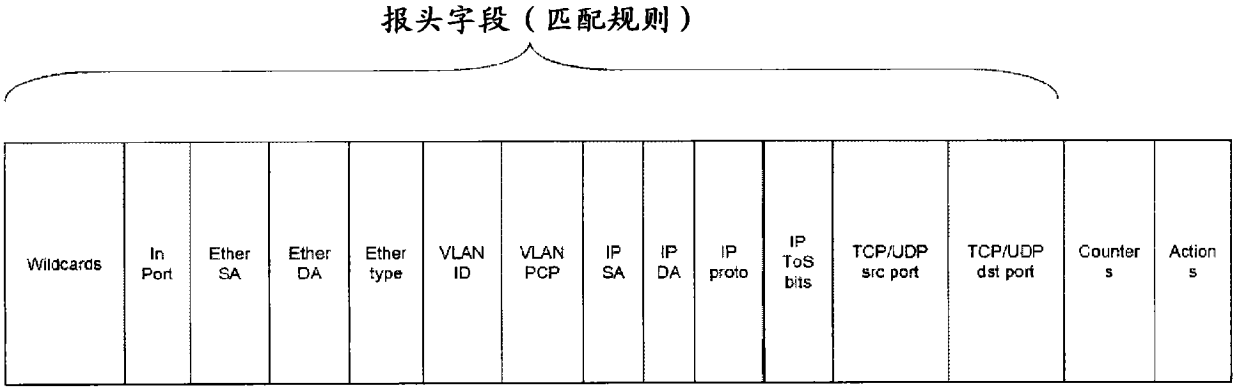

报头字段（匹配规则）
Wildcards
In Port
Ether SA
Ether DA
Ether type
VLAN ID
VLAN PCP
IP SA
IP DA
IP proto
IP ToS bits
TCP/UDP src port
TCP/UDP dst port
Counters
Actions

图 15