(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 105378648 B
(45)授权公告日 2020.04.21

(21)申请号 201480019243.8

(22)申请日 2014.03.13

(65)同一申请的已公布的文献号
申请公布号 CN 105378648 A

(43)申请公布日 2016.03.02

(30)优先权数据
13/855,543 2013.04.02 US

(85)PCT国际申请进入国家阶段日
2015.09.29

(86)PCT国际申请的申请数据
PCT/US2014/026177 2014.03.13

(87)PCT国际申请的公布数据
WO2014/165305 EN 2014.10.09

(73)专利权人 威智伦分析公司
地址 加拿大温哥华

(72)发明人 E·特里·尼利

(74)专利代理机构 北京路浩知识产权代理有限公司 11002
代理人 王莹 张晶

(51)Int.Cl.
G06F 7/04(2006.01)

(56)对比文件
WO 2012116037 A1,2012.08.30,
WO 2012116037 A1,2012.08.30,
US 2012297461 A1,2012.11.22,
US 8009013 B1,2011.08.30,
CN 1636175 A,2005.07.06,
US 2009070571 A1,2009.03.12,
US 2003200442 A1,2003.10.23,
US 2008086546 A1,2008.04.10,
CN 102664864 A,2012.09.12,
US 2013047207 A1,2013.02.21,
US 2005021661 A1,2005.01.27,

审查员 陈艳林

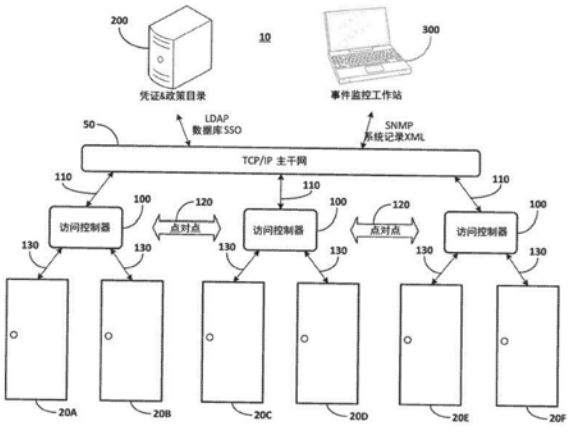
权利要求书2页 说明书11页 附图9页

(54)发明名称

自配置访问控制

(57)摘要

一种应用处理器的访问控制方法,其包括:接收凭证和政策目录信息以将访问控制器配置为通过所述访问控制器通过定期、自动查询目录允许访问控制器的自配置;从所述目录获取可能请求访问的一个或多个个人的凭证和政策信息;将所获取的凭证和政策信息存储在本地缓存中;接收访问请求以允许个人访问;将所述访问请求与所述缓存中的凭证和政策信息进行比较;以及当所述比较指示匹配时,准许所述个人访问。



CN 105378648 B

1.一种用于控制个人访问封闭区域的系统,所述系统包括:

处理器,物理地设置在所述封闭区域处,所述封闭区域包括第一门和第二门;以及

控制所述第一门的操作以及所述第二门的操作的多个访问控制器,每个访问控制器呈现在计算机可读存储介质上,所述每个访问控制器包括机器指令,所述机器指令当由所述处理器执行时至少使所述处理器:

配置第一访问控制器和第二访问控制器以:

从远程凭证和政策目录直接接收凭证和政策目录信息,

从而允许第一访问控制器通过定期、自动查询所述远程凭证和政策目录进行自配置;

从凭证和政策目录接收可能请求访问所述封闭区域的一个或多个个人的凭证和政策信息,

通过用户界面配置所述多个访问控制器之中的任何一个访问控制器,然后在所述多个访问控制器之中的所配置的访问控制器和未配置的访问控制器之间使用点对点通信,使得通过所配置的访问控制器的复制来自动地配置每个所述未配置的访问控制器;以及

将接收的所述远程凭证和政策目录的凭证和政策目录信息和所述一个或多个个人的所述凭证和政策目录的凭证和政策信息存储在可由所述处理器访问的、所述每个访问控制器的本地缓存中,

从所述凭证和政策目录信息定期地请求凭证和政策信息更新,

响应于定期请求在处理器处接收所述凭证和政策信息更新;

基于所述凭证和政策信息更新来更新所述本地缓存;

从传感装置接收访问请求以允许一个或多个个人中的个人通过所述第一门或所述第二门来访问所述封闭区域;

比较所述访问请求与所述本地缓存中的凭证和政策信息;

当所述比较指示匹配时,准许所述个人访问所述封闭区域;

配置所述每个访问控制器以监控和控制与所述第一门和所述第二门相关的事件并且监控与所述一个或多个个人相对应的进入信号和出去信号;

由所述个人尝试登录所述封闭区域内的计算机;

确定与所述个人对应的所述进入信号是否起源于所述多个访问控制器中的任何一个;以及

在没有所述进入信号的情况下,拒绝所述个人访问所述封闭区域内的任何计算机,

在所述多个访问控制器之中,在拒绝进入的访问控制器之间使用所述点对点通信来自动地更新所有其它的访问控制器,以使得所述其它的访问控制器也拒绝所述个人访问所述封闭区域和所述封闭区域内的计算机;并且

在所述多个访问控制器之中,在收集与所述第一门和所述第二门相关的事件或者所述进入信号和所述出去信号的一个访问控制器之间使用所述点对点通信来自动地更新所有其它的访问控制器,以使得所述其它的访问控制器利用所述事件或者所述进入信号和所述出去信号来更新。

2.如权利要求1所述的系统,其中,所述凭证和政策目录信息包括目录的URL,并且其中,所述远程凭证和政策目录和所述处理器使用TCP/IP协议通信。

3.如权利要求1所述的系统,其中,所述比较需要所述访问请求中的信息和所述本地缓

存中的相应的凭证和政策信息之间的准确匹配。

4.如权利要求1所述的系统，其中，为响应匹配，所述指令进一步引起所述处理器开启所述封闭区域的访问门以准许访问。

5.如权利要求1所述的系统，其中，所述指令进一步引起所述处理器配置所述每个访问控制器以根据预定义的事件定义信息监控并收集事件。

6.如权利要求5所述的系统，所述系统进一步包括：

缓冲器，以存储所收集的事件；

并且其中，所述指令进一步引起所述处理器引起所述每个访问控制器向多个事件监控器报告所收集的事件。

7.如权利要求6所述的系统，其中，所述指令进一步引起所述处理器接收多个事件监控器中的每个的地址，并且同时将所述事件发送至所述多个事件监控器中的多个。

8.如权利要求7所述的系统，其中，事件包括门打开、门关闭、门固定打开、门锁定和门解锁中的至少一个。

9.如权利要求1所述的系统，其中，所述访问请求是访问资源的请求，其中，所述资源是逻辑资源。

10.如权利要求9所述的系统，其中所述指令进一步引起所述处理器使得所述每个访问控制器基于所述个人与所述资源的位置自配置访问所述资源。

11.如权利要求1所述的系统，其中所述指令进一步引起所述处理器当所述比较指示不匹配时将所述访问请求发送至所述远程凭证和政策目录以确定匹配。

12.如权利要求1所述的系统，其中，实时地、连续地执行对于凭证和政策信息更新的请求。

13.如权利要求1所述的系统，其中，所述处理器被设置在所述封闭区域内。

自配置访问控制

背景技术

[0001] 访问控制系统可限制进入诸如建筑物、建筑物内的房间或仅允许有权限的人进入围栏内区域的封闭区域。当前的访问控制系统包括建筑物入口点(例如,门)处的访问读卡器。有权限进入建筑物的个人都配有访问控制卡,该访问控制卡可由访问读卡器读取。访问读卡器从访问卡获取信息并将该信息传达到控制面板。控制面板确定门是否应该被解锁。如果门应该被解锁(即,访问卡与有权限进入的个人有关),则控制面板发送信号至门锁定机构,引起机构解锁。

发明内容

[0002] 控制访问封闭区域的应用处理器的访问控制方法包括:由访问控制器接收凭证和政策目录信息以将访问控制器配置为通过访问控制器通过定期、自动查询目录允许访问控制器的自配置;从目录获取可能请求访问封闭区域的一个或多个个人的凭证和政策信息;将所获取的凭证和政策信息存储在本地缓存中;接收访问请求以允许个人访问封闭区域;将访问请求与缓存中的凭证和政策信息进行比较;以及当比较指示匹配时,准许该个人访问封闭区域。

[0003] 用于控制个人访问区域的系统包括处理器和呈现在计算机可读存储介质上的访问控制器,访问控制器包括机器指令,当处理器执行机器指令时,机器指令使处理器配置访问控制器以从远程目录接收凭证和政策目录信息,以通过访问控制器定期、自动地查询该目录允许访问控制器的自配置,以及从目录获取可能请求访问该区域的一个或多个个人的凭证和政策信息,将接收的获取的目录的凭证和政策信息和一个或多个个体的凭证和政策信息存储在本地缓存中,接收允许个人访问封闭区域的访问请求;比较访问请求与缓存中的凭证和政策信息;以及当比较指示匹配时,准许该个人访问封闭区域。

[0004] 用于配置访问控制器以控制个人访问资产(asset)的应用处理器的方法包括:接收凭证和政策目录地址,处理器从凭证和政策目录地址获取请求访问资产的个人的凭证和政策信息;接收凭证和政策信息的目标地址;确定获取凭证和政策信息的频率;获取请求访问资产的个人的凭证和政策信息;以及以确定的频率自动更新请求访问资产的个人的凭证和政策信息。

[0005] 自配置/自报告访问控制器包括用于存储控制访问资产的机器指令的装置和用于执行机器指令的装置。用于执行的装置包括用于自配置执行机器指令的装置、准许/拒绝访问资产的装置和报告与准许和拒绝访问资产相关的事件的装置。

附图说明

[0006] 详细说明参照下面的附图,其中相同数字指的是相同部分,并且其中:

[0007] 图1A-1C说明了示例性访问控制系统和其选择的组件;

[0008] 图2说明了与图1A-1C的系统一起使用的示例性访问控制器的元件和组件;

[0009] 图3说明了通过图2的访问控制器启用的示例性界面;

[0010] 图4说明了图2的访问控制器的示例性访问控制引擎;以及

[0011] 图5A-5C是说明图1A-1C的系统和图2的访问控制器的示例性方法的流程图。

具体实施方式

[0012] 保证只有经授权的个人访问受保护的或被保卫的区域可能是至关重要的(例如,在机场、军事设施、办公大楼等)。受保护的或被保卫的区域可由实体门(例如,人可通过其进入的门)和墙壁限定,或可以其它方式虚拟地限定。例如,受保护的区域可被限定为未被授权的进入而引起检测器发出侵入信号以及如果不提供授权可能发出警报的信号或声音的区域。

[0013] 访问控制系统可将进入建筑物、建筑物内的房间或围栏内的区域或资产及其内的资源的受保护的或被保卫的区域限制于仅具有访问准许的那些个人。

[0014] 因此,访问控制系统根本上应该识别尝试进入被保卫的区域或访问资产的个人并核实个人目前是否被授权进入或访问。在此公开的访问控制系统、装置和方法可包含任何访问技术,包括:

[0015] (1)使用可在与访问点(例如,门)相关联的键盘处输入的PIN和密码;

[0016] (2)使用可由个人通过与门相关联的专门的阅读器进入的生物特征;

[0017] (3)使用由个人通过与门相关联的专门的平板(pad)提供的传统签名;

[0018] (4)使用智能卡或非接触式卡(例如,通过专门的阅读器/接收器发送PIN至门;

[0019] (5)使用数字凭证;例如,存储在智能卡、非接触式卡或无线装置中可通过读卡器或其他接收器“与门通讯”的数字凭证;以及

[0020] (6)使用插入门锁中的物理钥匙;此类钥匙/锁机构可包括读入锁中的钥匙上的专门编码。

[0021] 上述访问技术的列表并不意味着是详尽的。此外,一些设施可使用这些技术的组合。技术可用于任何环境中,包括国有企业、私营企业、公共设施中以及个人住宅中。

[0022] 作为一些上述访问技术的进一步的说明,一些当前的访问控制系统使用装备有诸如键盘的进入装置的门,个人通过进入装置输入PIN或密码。键盘具有存储有效的PIN/密码的列表的附加的存储器或基本处理器,使得可检查PIN/密码以确定其是否仍然有效。如果PIN/密码有效,则门打开;否则门保持锁定。此类基本的访问控制机构提供最低安全。例如,离职的员工可能不再被授权通过门;然而,记得其PIN的离职的员工仍然能够打开门。因此,将有必要“消除”离职的员工的PIN。然而,此程序可能是非常繁琐和昂贵的:设施可能具有数百个门,并且无论何时员工离开或离职,消除所有这些门可能是不切实际的。

[0023] 一些当前的基于卡的访问控制系统使用射频识别(RFID)技术。访问读卡器包括RFID收发器,访问卡包括RFID标签或应答机。当卡经过RFID收发器时,RFID收发器将射频(RF)查询传输至卡。RF应答机包括硅片和天线,天线使卡能够接收和响应RF查询。响应典型地为包括预编程识别(ID)号码的RF信号。读卡器接收信号并将ID号码传输至使用有线或无线连接的控制面板。当前的读卡器在发送数据至控制面板之前可执行一些识别数据的基本的格式化,但通常不能执行更高级别的功能。

[0024] 当前的访问控制器依赖供应/取消供应凭证的私有协议和软件,提供配置信息并报告事务。一旦已经选择和安装了特定厂商的产品,这些当前的访问控制器的私有性质限

制顾客关于实施改变、添加新的特征和一般地移至其他技术方案的选择。当访问控制器移离RS232/485通信并移至TCP/IP网络通信介质上时，私有协议更不可被顾客接受。

[0025] 此外，当物理安全系统增加对组织的信息技术(IT)基础设施的信赖时，IT部门可以寻找降低成本和时间的配置选择。这需要系统遵循安装和通信标准。附加利益提供使用标准和商业成品组件产品的逻辑和物理安全系统的互操作性。

[0026] 为了克服这些和其他现有访问控制系统中的地方性问题，在此公开了自配置访问控制器和相关访问控制系统，以及它们的使用方法。在此公开的访问控制器、系统和方法可用于控制物理访问建筑物、构筑物和区域。当使用现有的信息技术(IT)基础设施时，在此公开的访问控制器、系统和方法提供分布式访问控制策略、程序和计算机网络上的凭证。

[0027] 除供应/取消供应访问诸如物理区域的资产外，在此公开的访问控制器、系统和方法还可供应具有逻辑权限的用户/凭证识别存储以提供通向诸如文档、计算资源或其他计算系统的逻辑资产或资源的访问。此外，通向逻辑资产或资源的访问可根据请求这种访问的个人的物理位置而变化。

[0028] 下面参照下面的术语描述访问控制器、控制系统和控制方法。

[0029] 访问控制器-程序化装置或程序本身，以基于识别存储供应的缓存数据做出访问决定。访问请求通过传感装置(读卡器、按钮等)做出；或者在本地或通过参照用于处理的远程识别存储来检查授权。如果访问请求被批准，则操作输出和输入装置/系统(例如，入口门)以允许访问。

[0030] 门控制器-与访问控制器通讯且物理地(例如，有线地或无线地)附着于凭证阅读器和相关的输入和输出硬件的装置。门控制器将状态变化和凭证读取发送至访问控制器，等待来自访问控制器的授权回应，以及根据授权回应命令附着的输入、输出和凭证阅读器。

[0031] 浏览器-用于访问和显示互联网网页的软件程序或固件；当前的浏览器包括IE浏览器、谷歌浏览器、火狐浏览器和苹果浏览器。

[0032] 识别存储(或目录)-包括相关的、分层的、网路的或其他包括授权和用于个人、凭证、资源和组成员资格的认证数据的架构的数据库。识别存储可驻留在由不同于拥有和/或操作保护区域的实体的实体拥有和操作的设施处。

[0033] 事件聚合-访问控制器将发生或产生在操作访问控制器的过程中的事件存储并转送至多个系统的能力。

[0034] 在实施例中，访问控制器是能够在运行的商业成品组件计算机上执行的软件应用，例如，Linux操作系统。计算机可被设计为诸如访问控制器的台式、机架可安装的、基于云的或嵌入式平台。计算机为软件应用提供必要的处理器、存储和连通性。在不需要将任何软件安装到任何其他计算机系统上的情况下，所有必需的软件都装在计算机上。

[0035] 访问控制器提供改进的方法，以维护凭证和相关的访问权限并且在不需要访问或以其它方式使用专有的通信协议的情况下使用现有的信息技术(IT)基础设施和数据库实时地传送事件。

[0036] 访问控制器作为自配置访问装置可获取和保持凭证和相关的访问权限的缓存列表；这些数据允许在不与任何其他的访问控制系统交流的情况下做出现场的、实时的访问决定。凭证和相关的访问权限的缓存可以定期地从一个或多个主系统获取，包括按预定计划、实时地或作为完整的快照(snapshot)。例如，访问控制器实际上可以连续不断地访问访

问凭证和相关访问权限的主机系统目录，以及下载所有凭证和权限中的一些。在一方面中，访问控制器下载这些数据用于个人的选择数量。为个人下载数据的该个人可被唯一地识别，由组协会识别或由指定的角色识别。

[0037] 访问控制器可用于或者按需实时地或者按预定计划地将实时的事件发送至记录和监控装置或系统。在一方面中，事件可以是访问门开锁或上锁、访问门打开或关闭信号(例如，来自限制开关或位置传感器，或基于逻辑程序)、访问门故障或不平常的操作(打开时间超过可变阈值)等。事件可以包括XML的许多格式直接地发送到记录许多远程装置或系统的设施的相关数据库或系统中。如果连通性丢失，则访问控制器可以缓冲事件并当连通性重新建立时可以继续事件传送。

[0038] 访问控制器可以包含或提供浏览器可访问的用户界面。界面为访问控制系统操作者提供配置许多访问点(例如，门)及其操作的能力以及将相关的地图提供给个人和/或团体(在个人基础、团体基础和/或确定的角色基础上)以传达访问权限。用相同的界面，操作者可以配置访问控制器以与凭证源通信，凭证源包括应用在相关数据库中或使用相关数据库的凭证源、目录或分层数据存储或诸如逗号分隔值(CSV)文件或任何普通的ASCII文件的平面文件。

[0039] 操作者用界面选择和配置数据同步类型，包括时间间隔、预定的、请求式和实时的。同步方法可包括：预约(subscription)，在预约中主机访问凭证且政策系统将信息变化“推送”至访问控制器；审查追踪，在审查追踪中访问控制器请求数据更新；或数据修改触发器，在数据修改触发器中写入主机系统的编码检测信息变化并将变化的信息发送至访问控制器。预约方法可请求主机系统和访问控制器之间持久的、不间断的连接，而其他示例的两个方法可使用短暂连接。

[0040] 访问控制器启动至源的连接并检索凭证和政策信息以建立控制器的本地缓存。每个个人可具有唯一的识别符以核对从复合源到单一记录的个人的信息。一旦被传送到本地缓存，当凭证出现在访问控制点时，信息可用于访问决定中。

[0041] 访问控制器可记录事件，记录可被配置有用户界面以建立许多装置、服务和系统作为事件接收者。访问控制器可将事件以许多格式发送至远程监控服务，所述许多格式包括例如SNMP、通过直接套接字连接(GSM、LAN、WAN、WiFi)、系统记录和通过串行端口的XML。

[0042] 访问控制器可用于分配事件优先级。事件优先级可决定哪些事件和那些事件以哪种顺序被发送至远程监控服务。

[0043] 图1A-1C说明了示例性访问控制系统及其选择组件。在图1A中，访问控制系统10包括门系统20、访问控制器100、凭证和政策目录200和事件监控工作站300，所有这些都旨在限制或控制访问区域或体积。控制器100使用例如TCP/IP主干网50将110与目录200和工作站300连通。TCP/IP主干网50可以是有线或无线的，或有线和无线的组合。主干网50可包括局域网(LAN)和广域网(WAN)的元素，包括互联网。访问控制器100和目录200之间和控制器100和工作站300之间的通信110可以是安全通信(例如，HTTPS通信)。

[0044] 图1B说明了为限制或控制个人访问封闭区域12而选择的访问系统10的组件。如所示，封闭区域12是具有入口门系统20和出口门系统20的六面结构。参照图1A和1C描述门系统20。门系统20意为用于正常人访问。可以存在其他访问点(例如，窗户)，且它们的操作可以被监控、报警和控制，但在此不再进一步描述这种访问点。

[0045] 封闭区域12包括计算平台101，在计算平台101上执行控制、监控和报告门系统20的操作的访问控制特征。计算平台101可以是固定或移动的。计算平台101被示出在封闭区域12内，但不一定这样。在执行它的控制、监控和报告功能中，具有它的范围控制特征的计算平台101可以通过具有(远程)目录200且具有(远程)事件监控工作站300的网络50将外部与封闭区域12通信。网络50可以是有线或无线的，并可提供除非安全通信和发信号之外的安全通信和发信号。

[0046] 封闭区域12可以是建筑物中的房间、建筑物本身或任何其他结构。封闭区域12并不限于六面结构。封闭区域12可以是开口结构(例如，体育场)、围栏中区域(例如，围绕跑道的区域)或具有“不可见”围栏或“虚拟壁”的区域。封闭区域12在地理上可以是固定的(例如，建筑物，建筑物中的房间)或移动的(例如，拖车、飞机、船或集装箱)。

[0047] 封闭区域12可用于控制访问政府或其中包含的商业机密文件或装置、访问其中包含的计算机系统、访问个人、访问诸如稀有画作、珠宝等的贵重物品，以及访问危险材料或系统。封闭区域12可以是银行的保险箱或金库、用于核反应堆的控制室、用于分类的、新技术的飞机的机库或机场的乘客门。

[0048] 在移动配置中，封闭区域12例如可用于野外作业以在世界上的任何地方快速建立安全设施。这种移动封闭区域12的安全性将从下列的讨论中明显。而且，如下所述，移动封闭区域可用于非常不同的操作，根据其预期用途，通过用户界面执行简单的配置变化，不同个人能够访问移动封闭区域12。因此，无论在需要访问控制的世界上的任何地方，系统10不仅提供高水平的安全、访问控制、事件监控和报告，而且提供灵活性以快速使移动封闭区域12适应任何操作或任务。

[0049] 回到图1A，访问控制器100使用点对点通信120还可以彼此间通信。例如，这种点对点通信120通过使用安全LAN可能是可行的。可选地，点对点通信120可以是无线安全通信。点对点通信120还可以遵循TCP/IP协议。

[0050] 点对点通信120允许访问控制器100将访问状态信息和事件发送至封闭区域12中使用的其他访问控制器以及从封闭区域12中使用的其他访问控制器接收访问状态信息和事件。因此，如果门系统20不起作用，则其相关的访问控制器100可以提供该信息至其他的访问控制器100。点对点通信120允许一个访问控制器100作为母(主)访问控制器，其余的访问控制器100作为子(从属的)访问控制器。在这方面，信息和配置可以存储在母访问控制器上或在母访问控制器上执行，然后可以在子访问控制器上复制。

[0051] 最后，访问控制器100可以使用有线或无线的安全通信130与门系统20通信。

[0052] 参照附图1B描述的更详细的门系统20控制正常人访问封闭区域12。在图1A的示例中，示出六个门系统20。在一方面中，六个门系统20提供三个封闭区域访问点，门系统20成对地操作；一对中的一个门系统20允许进入封闭区域12，该对中的另一个门系统20允许从封闭区域12出去。在另一方面中，单个门系统20可用于进入封闭区域12和从封闭区域12出去。

[0053] 图1A示出与单独的访问控制器100通信的每个门系统对。然而，在系统10中可以应用控制器100和门系统20的其他组合。例如，单个控制器100可以控制用于封闭区域12的所有门系统20。

[0054] 图1A所示的凭证&政策目录200可以表示一个或许多真实的目录。目录可远离封闭

区域12。目录可以由实体而不是封闭区域12的操作者操作。例如，封闭区域12可以是政府承包商的敏感隔离信息设施(SCIF)，目录200可以表示政府承包商的目录和政府机关的目录。

[0055] 目录200可包括可被允许访问封闭区域12的个人的识别信息(名字、年龄、物理特征、照片)、个人的识别凭证(PIN/密码、RFID标签、凭证)和其他信息。

[0056] 事件监控工作站300可由与封闭区域12相同的实体来实现。可选地，事件监控工作站300可由与封闭区域12的实体分开且远离封闭区域12的实体的实体实现且在与封闭区域12的实体分开且远离封闭区域12的实体的实体处实施。

[0057] 事件监控工作站300可以从访问控制器100接收事件数据。

[0058] 图1C说明可在图1A的系统中实施的示例性门系统。在图1C中，示出门系统20通过通信路径110与访问控制器100通信。门系统20包括访问门22、门锁定机构24、门控制器26和凭证阅读器28。门22可以是允许个人进入或离开封闭区域的任何门。门22可包括位置传感器(例如，限制开关-未示出)，该位置传感器当门22未完全关闭时指示。位置传感器可通过信号路径21将未完全关闭的信号发送至门控制器26。未完全关闭的信号可以被连续不断地或定期地发送，且可以直到预定时间期满后才发送。

[0059] 锁定机构包括诸如固定栓的远程操作机电锁定元件(未示出)，该远程操作机电锁定元件响应于通过信号路径21从门控制器26发送的电信号而设置(锁定或未锁定)。

[0060] 门控制器26通过信号路径29从凭证阅读器28接收凭证信息并通过信号路径130将该信息传递到访问控制器100。门控制器26通过信号路径130从访问控制器接收锁定/未锁定信号。门控制器26通过信号路径21将锁定机构锁定/未锁定信号发送至锁定机构24。

[0061] 凭证阅读器28接收个人42的凭证信息40。凭证信息40可被编码在RFID芯片中，例如，智能卡上的凭证、使用键盘输入的PIN/密码、诸如指纹和视网膜扫描数据的生物识别数据。

[0062] 门系统20基于发送至访问控制器100的访问请求信号和响应接收自访问控制器100的访问授权信号操作。门系统20可以结合在门22打开且然后关闭之后特定时间内、未锁定信号已发送至锁定机构24但门22还未打开之后或其他情况下的特定时间内激活(锁定)门22的自动锁定特征。自动锁定逻辑可在门控制器26或锁定机构24中实现。

[0063] 门系统20可通过访问控制器100将事件信号发送至事件监控系统300。这种信号包括门打开、门关闭、锁定机构锁定和锁定机构未锁定。如上所述，信号可以起源于门系统20中的限制开关。

[0064] 在一方面中，门系统20可仅用于进入，单独的门系统20可仅用于外出。

[0065] 然而，这样配置，门系统20可以基于通过分别读取个人42关于进入和出去的凭证信息40所获得的信息指示何时个人42在封闭区域12中以及何时个人42已经走出封闭区域12。例如，这些信号可用于在没有介于中间的出去的情况下防止再次进入。信号(或他们不在)还可用于防止访问封闭区域内的区域和系统。例如，在不存在起源于封闭区域12的门系统20的一个的进入信号时，个人42可能不允许登录其封闭区域12中的计算机。因此，访问控制器及其实现的安全功能可能是个人可能接触的级联的一系列的访问操作中的第一步。

[0066] 门系统20可结合诸如支撑敞开的门22、卡住的未锁定的锁定机构24和其他的缺口或故障的标志的各种警报。

[0067] 图1A-1C描述主要应用于物理访问诸如建筑物或建筑物中的房间的区域的访问控

制系统10。然而，如上所述，访问控制系统10及其选择的组件可用于控制访问组织的资产和资源，包括逻辑资源。例如，自配置访问控制器100可用于控制访问组织的计算机系统和包含在计算机系统上的文件(即，逻辑资源)。而且，访问控制器100可自配置以提供个人分期访问逻辑资源。例如，个人可被准许访问第一封闭区域中的文件1-10和访问第二和更多安全的封闭区域中的文件1-20。在该示例中，第一封闭区域可以是建筑物，第二封闭区域可以是建筑物内的SCIF。因此，自配置访问控制器100可通过个人的访问权限包括物理的和逻辑的访问建立非常精细的控制，且可基于如个人的凭证的读取所示的个人的物理位置调整逻辑访问。

[0068] 图2说明与图1A-1C的系统10一起使用的示例性访问控制器100的元件和组件。在图2中，访问控制器100被示出为在计算平台101上实现。计算平台101可以是任何计算装置，例如，包括大型机计算机、台式计算机、笔记本电脑或平板电脑和智能手机。访问控制器100可被作为软件、硬件或固件或这三者的任何组合应用。当以软件应用时，访问控制器100可存储在非暂时性计算机可读存储介质中。

[0069] 计算平台101可使用Linux操作系统。可选地，可使用其他操作系统。计算平台101包括数据存储102，其依次包括本地缓存103、非暂时性计算机可读存储介质104和事件缓冲器107，其中，本地缓存103可用于本地存储诸如个人42的个人的凭证和访问政策信息，非短暂性计算机可读存储介质104上可存储访问控制器100，事件缓冲器107可将事件传输期间暂时存储至事件监控工作站300。计算平台进一步包括浏览器105、处理器106和存储器108。处理器106可将执行程序包括访问控制器100从数据存储102装载入存储器108中。

[0070] 访问控制器100与本地缓存103通信且使用浏览器105、诸如目录200的目录和诸如事件监控工作站300的其他计算装置。然而，与目录200和工作站300的通信可通过其他手段，包括通过专用的局域网。

[0071] 访问控制器100包括界面引擎150和访问控制引擎190。如对图3的详细说明，界面引擎150为用户提供界面160(参见图3)，界面160可被访问控制系统10的操作者(人)使用以为访问控制器100建立自配置特征并且由访问控制器100建立事件报告。

[0072] 访问控制引擎190包括与目录200通信以自配置缓存103的逻辑，以基于包含在自配置缓存103中的信息来操作门系统20。访问控制引擎190包括记录事件和将该事件报告给事件监控工作站300的逻辑。逻辑能够使事件聚合，在事件聚合中访问控制器100存储事件并将事件报告至多个目的地。图4详细说明了访问控制引擎190。

[0073] 图3说明通过图2的访问控制器100可行的示例性用户界面160。用户界面160为操作者提供配置和控制许多用于封闭区域12的门系统20的操作的能力。用户界面160允许操作者创建授权的个人到组的映射以及基于组织内的个人身份、组成员关系和指定角色传达访问权限。用相同的界面160，操作者可以配置访问控制器100以与诸如目录200的凭证源或诸如CSV文件或任何常用的ASCII文件的平面文件通信，该凭证源包括任何相关数据库、目录或分层数据存储。

[0074] 如图3所示，示例性用户界面160包括用于与个人相关的信息的访问窗口170和用于与事件相关的信息的事件窗口180。个人访问窗口170包括：目录地址窗口171，操作者在目录地址窗口171中输入目录200的地址(例如，URL)；个人姓名窗口172，在个人姓名窗口172中可以输入个人的姓名或可以将个人的姓名列在下列菜单中；联系窗口173，在联系窗

口173中可以输入个人的组织;团体窗口174,在团体窗口174中可以输入个人所属的团体;任务窗口175,在任务窗口175中可以输入被分配至个人的任务或工作;标识号窗口176,标识号窗口176中出现分配的、唯一的标识;访问级别窗口177,访问级别窗口177列出个人访问的最高级别;同步窗口178,在同步窗口178中可以说明参考凭证和政策目录200更新个人的访问数据的频率。窗口171-178中的一些可以是下拉菜单的形式,诸如同步窗口178可显示一次,其选择的值适用于所有个人。窗口171-178可以一次一个的出现在操作者的显示器中。一旦数据被输入,可呈现给操作者确认页面以确认选择。不是所有的窗口都需要填写;一方面,操作者可以提供目录地址和个人姓名,其余的数据可由访问控制器从目录200检索。而且,访问控制器100可以定期参照目录200检索或更新数据,该定期可近似于实时或连续参照。可选地,例如,可以较长间隔、按计划或按需检索数据。因此,访问控制器100能够用可请求访问封闭区域12的个人的访问控制信息自配置自身。如上所述,检索数据可存储在本地缓存103中,当做访问决定时访问控制器100参考本地缓存103。

[0075] 事件窗口180提供许多数据进入窗口,事件窗口180可进一步包括下拉菜单,且系统操作者可使用事件窗口180建立访问控制器100的初始配置用于向事件监控工作站300报告事件。事件窗口180包括事件说明窗口181,在事件说明窗口181中可输入事件名称或标题、简要说明、测量参数和其他信息。例如,事件窗口180可用于说明门开启事件,提供门开启测量的装置的身份、门开启事件意味着什么以及提供门开启事件的形式。

[0076] 事件窗口180进一步包括事件优先顺序窗口182,在事件优先顺序窗口182中系统操作员能够分配事件优先顺序。优先顺序可以决定将事件从访问控制器100发送至事件监控工作站300的顺序。因此,例如,警报或故障的事件说明可具有比门开启事件更高的优先顺序。

[0077] 更进一步地,事件窗口180包括报告频率窗口183,在报告频率窗口183中系统操作者设定时间框架用于向事件监控工作站300报告事件。

[0078] 最后,事件窗口180包括报告目标窗口184,在报告目标窗口184中系统操作者输入事件监控工作站300的地址。使用窗口184,系统操作者能够指派许多不同的实体来接收事件报告。不同的实体可接收不同的报告。例如,第一事件监控工作站可以仅接收门开启和门关闭事件,而第二事件监控工作站可接收所有事件。指定的目标不需要属于相同的实体。

[0079] 图4说明访问控制器100中的访问引擎190的示例。访问引擎190包括自配置模块191、比较器195、决策模块196、事件检测器/记录器197和事件报告器198。

[0080] 在系统10包括许多访问控制器100的实施例中,一个访问控制器100可被指定为母访问控制器且其他的访问控制器可被指定为子访问控制器。主访问控制器可从目录200获取数据,然后使用点对点通信120将获取的数据复制给子访问控制器。可选地,每个访问控制器100可单独与目录200通信。

[0081] 如上所述,在此公开的访问控制系统、装置和方法的一个方面是访问控制器100自配置从凭证和政策目录200获取的访问控制信息的能力,凭证和政策目录200可远离访问控制器100且可被不同于拥有和操作访问控制器100的实体的实体拥有和操作。自配置模块191提供一些自配置功能。自配置模块191包括通信子模块192、缓存填充器193和缓存通信器194。通信子模块192确定访问控制器100应该寻址可能的多目录200中的哪个以获取和更新凭证和政策信息。然后,子模块192与选择的目录200建立安全的(加密;例如,HTTPS)通信

并获取信息。可选地，一些信息可以使用非安全的(未加密的)通信来获取。

[0082] 通信子模块192还可与事件监控工作站300建立安全的(或非安全的)通信以实时地、接近实时地(例如，在事件的几秒内)、按计划地、按事件监控工作站300的需要地或在一些其他的基础上发送事件信息。

[0083] 可通过浏览器105进行通信子模块192和目录200和事件监控工作站300之间的通信。通信子模块192可执行数据加密(用于外出请求/报告)和解密(用于从目录200接收的数据包或从事件监控工作站300接收的请求)。

[0084] 缓存填充器193从通信子模块192接收获取的信息且相应地填充本地缓存103。缓存项192可在将信息存储在缓存103中之前运行接收信息的错误检查。

[0085] 缓存通信器194可检索来自缓存103的数据用于访问控制引擎190的其他组件，诸如例如以决定是否开启门22以允许访问列在缓存103中的特定个体。缓存通信器104可包括允许系统操作者搜索缓存并接收缓存内容中的一些或全部的报告(显示)的检索/显示特征。报告可被设置在界面160上且可被打印。

[0086] 比较器195接收在门系统20处获取的凭证信息并与缓存通信器194通信以从缓存103检索适当的信息。将获取的凭证信息和检索的信息提供给决策模块196，决策模块196确定信息是否匹配(充分地)以允许个人访问封闭区域12。

[0087] 事件检测器/记录器197从门系统20接收信号，根据预定义的事件分类信号，将数据格式化为可报告的事件并将事件记录在事件缓冲器107中。然后，事件报告器198通过通信子模块192和浏览器105将记录的事件报告给事件监控工作站300。

[0088] 图5A-5C是说明图1A-1C的系统和图2-4的组件的示例性方法的流程图。

[0089] 图5A和5B说明示例性方法500，当访问控制器100接收凭证和政策目录200和事件监控工作站300信息(例如，这些装置/系统的URL)且信息用于配置访问控制器100时，示例性方法500始于框505。在具有多个访问控制器100的访问控制系统中，第一(母)访问控制器的配置可被复制给其余的(子)访问控制器。

[0090] 在框510中，目录信息用于获取可请求访问封闭区域12的一个或多个个人的凭证和政策信息。

[0091] 在框515中，因此获取的凭证和政策信息被输入每个访问控制器100的本地缓存中。

[0092] 在框520中，访问控制器100接收访问请求以允许个人42访问(离开)封闭区域12(通过特定的门22)。访问请求可基于从凭证40读取的数据。

[0093] 在框525中，来自接收的请求的信息用于访问控制器100中以检索个人42在缓存103中的凭证和政策信息，然后，检索的信息与包含在访问请求中的信息相比较。

[0094] 在框530中，访问控制器100确定比较是否指示充分匹配以允许允许个人42访问封闭区域12。例如，从缓存103中检索的每项信息可能需要恰好与从凭证40读取的信息相匹配。在框530中，如果确定匹配，则方法500移至框535。如果确定不匹配，则方法500移至框545。

[0095] 在框535中，访问控制器100向门系统20发送开启信号。在框540中，访问控制器100然后监控门系统20的操作以确定门22是否打开(以准许个人42进入，且然后关闭和锁定)。

[0096] 在框545中，如果在系统10中应用，则访问控制器100将访问请求发送至目录200，

访问控制器100使用其自身的内部处理以确定接收自凭证40的信息是否与个人42的目录200中的信息匹配。

[0097] 在框550中，访问控制器100从目录200接收指示匹配或不匹配的信号。如果指示匹配，则方法500移至框540。如果指示不匹配，则方法500移至框555且访问控制器100拒绝访问个人42。

[0098] 在框560中，框540的操作后，访问控制器100从门系统20接收事件信息、将事件信息格式化为事件并将事件发送至事件监控工作站300。

[0099] 在框555或560后，方法500移至框565并结束。

[0100] 图5C是说明图5A的框505的过程的示例性方面的流程图，特别用于配置访问控制器100。在图5C中，当系统操作者使用界面160设置目录(源)地址时，方法505始于框571，其中，访问控制器100将从目录(源)地址获取请求访问封闭区域12的个人42的凭证和政策信息。在框573中，设置目标地址(即，缓存103的地址)。在框575中，设置同步时间。在框577中，访问控制器接收特定个人42的指示，特定个人42的凭证和相关信息将被输入缓存103中。

[0101] 在框579中，访问控制器接收由访问控制器100监控的事件的定义。事件可预先定义或可由系统操作者使用例如界面160来建立和定义。在框581中，访问控制器100接收将接收事件信息的事件监控器的目标地址。在框583中，访问控制器100接收请求报告的间隔或频率。最后，在框585中，访问控制器100接收定义哪些信息将随着每个事件被提供或记录的参数。然后，方法505结束。

[0102] 附图所示的某些装置包括计算系统。计算系统包括处理器(CPU)和将包括诸如只读存储器(ROM)和随机存取存储器(RAM)的系统存储器的各种系统组件连接至处理器的系统总线。其他系统存储器也可能是有用的。计算系统可包括多于一个处理器或相互连通以提供更大处理能力的计算系统组或群。系统总线可以是任意多种类型的总线结构，包括存储器总线或存储控制器、外围总线和使用任何多种总线架构的本地总线。存储在ROM等中的基本输入/输出(BIOS)可以例如在启动过程中提供有助于在计算系统内元件间传输信息的基本程序。计算系统进一步包括数据存储，数据存储根据已知的数据库管理系统维护数据库。数据存储可以诸如硬盘驱动器、磁盘驱动器、光盘驱动器、磁带驱动器或可存储由处理器可访问的数据的诸如磁带盒、闪存卡、数字多用盘、暗盒、随机存取存储器(RAM)和只读存储器(ROM)的另一类型的计算机可读介质的多种形式呈现。数据存储可通过驱动接口连接至系统总线。数据存储提供计算机可读指令、数据结构、程序模块和其他用于计算系统的数据的非易失性存储。

[0103] 为了使人类(且在某些情况下为机器)能够用户交互作用，计算系统可包括诸如用于语音和音频的麦克风、用于手势或图形输入的触摸感应屏幕、键盘、鼠标、动作输入等的输入装置。输出装置可包括许多输出机构中的一个或多个。在某些情况下，多模式系统使用户能够提供多类型的输入以与计算系统通信。通信界面通常使计算装置系统能够使用多种通信和网络协议与一种或多种其他的计算装置通信。

[0104] 前述公开参照流程图和随附的描述以说明图5A-5C所示的实施例。公开的装置、组件和系统考虑使用或应用任何适合于执行所述步骤的技术。因此，图5A-5C仅为说明的目的，且可在任何合适的时间执行所述或相似的步骤，包括同时地、单独地或组合地。此外，流程图中的步骤可同时地和/或以与所示的和所描述的不同的顺序发生。而且，公开的系统可

使用具有附加的、较少的和/或不同的步骤的过程和方法。

[0105] 在此公开的实施例可应用于数字电子电路或计算机软件、固件或硬件，包括在此公开的结构及其等同物中。一些实施例可作为一个或多个计算机程序应用，即由一个或多个处理器加密在用于执行的计算机存储介质上的计算机程序指令的一个或多个模块应用。计算机存储介质可以是或可列入计算机可读存储装置、计算机可读存储基体或随机或串行存取存储器。计算机存储介质还可以是或可列入诸如多个CD、磁盘或其他存储装置的一个或多个单独的物理组件或介质。计算机可读存储介质不包括暂时信号。

[0106] 在此公开的方法可作为由处理器执行的操作应用在存储在一个或多个计算机可读存储装置上或接收自其他源的数据上。

[0107] 计算机程序(还被称为程序、模块、引擎、软件、软件应用、脚本或编码)可以包括编译或解释语言、说明或程序语言的任何形式的编程语言写入，且其可以包括作为独立程序或作为模块、组件、子程序、目标或适合于在计算环境中使用的其他单元的任何形式配置。计算机程序可以但不必对应于文件系统中的文件。程序可以存储在保存其他程序或数据(例如，一个或多个存储在标记语言文档中的脚本)的文件的一部分中、专门对问题中的程序的单个文件中或多个协调文件(例如，存储一个或多个模块、子程序或部分代码的文件)中。计算机程序可被配置为在一个计算机上或在位于一个位置或分布于多个位置且由通信网络连通的多个计算机上执行。

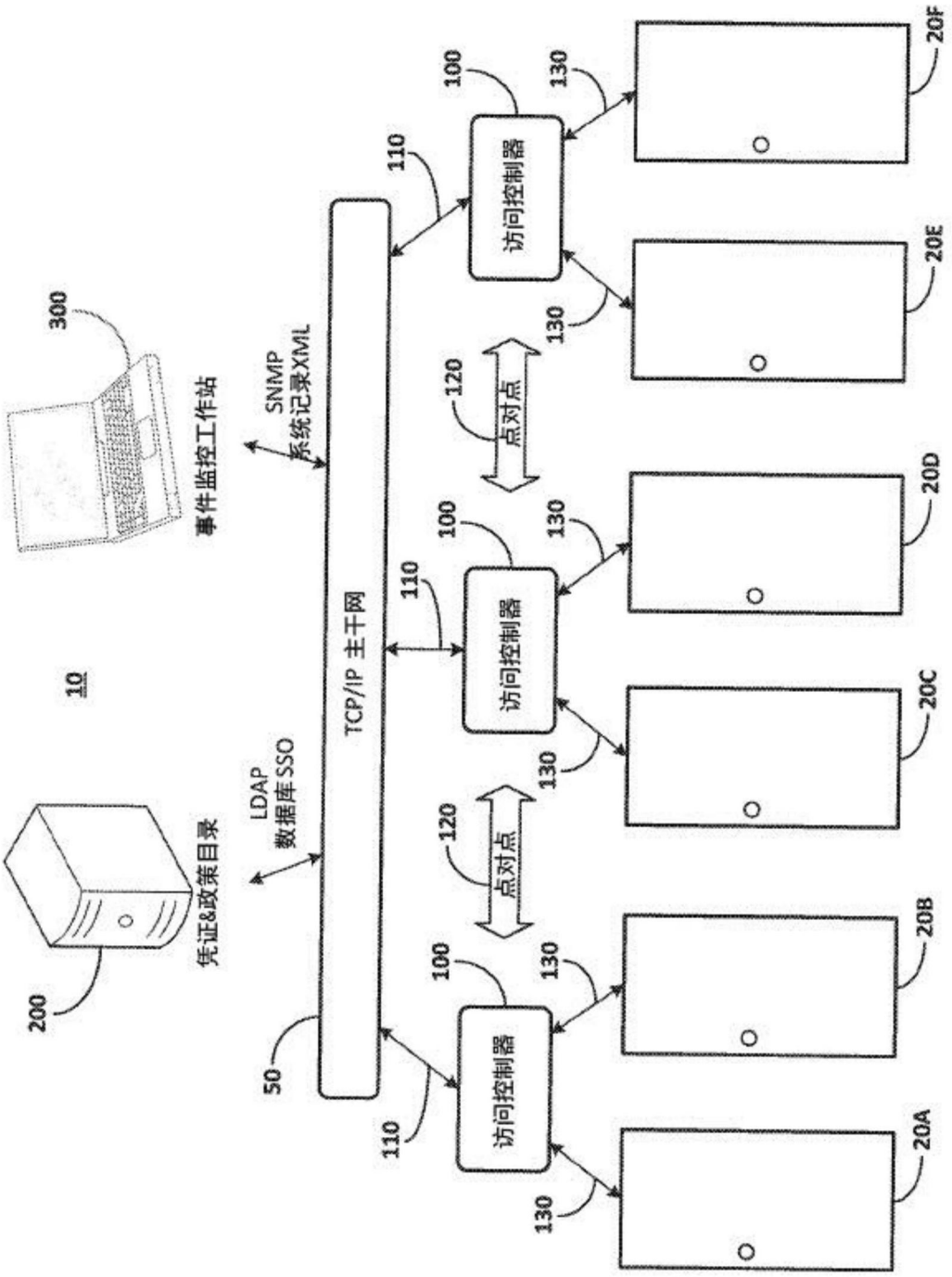

300
事件监控工作站
SNMP
系统记录XML
10
LDAP
数据库SSO
凭证&政策目录
200
50
TCP/IP 主干网
110
访问控制器
100
130
120
点对点
20A
20B
20C
20D
20E
20F

图1A

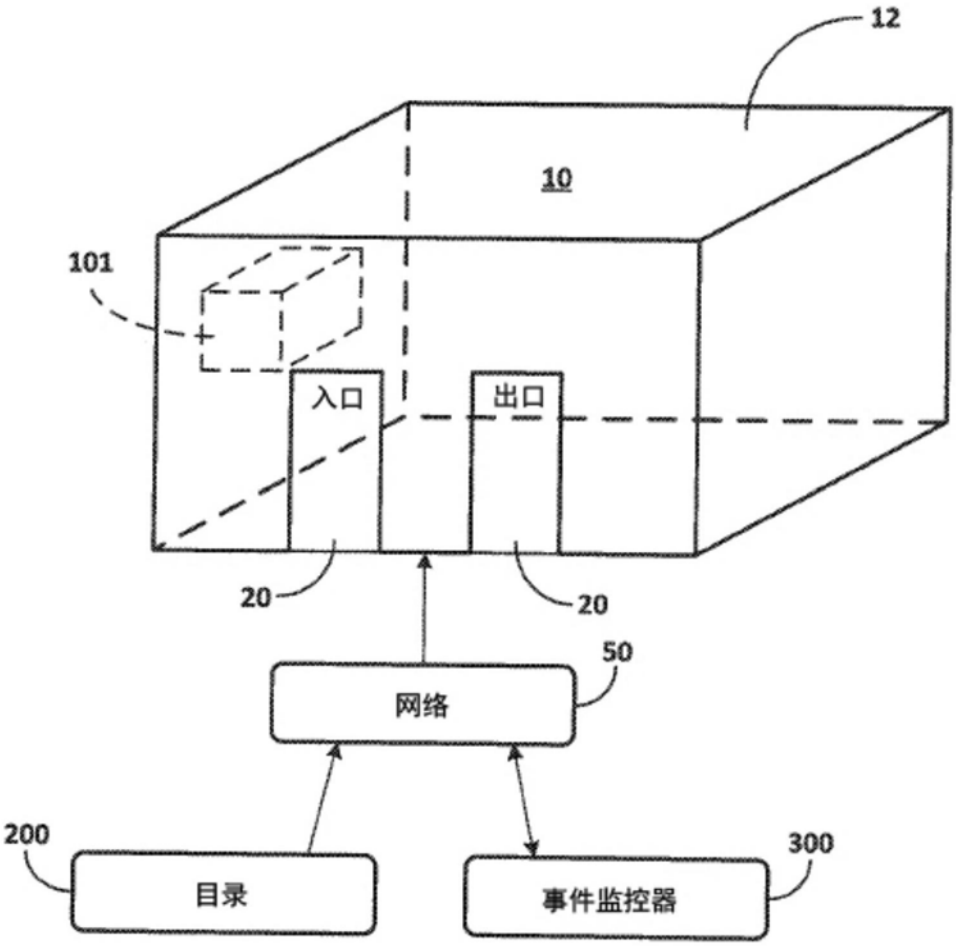


图1B

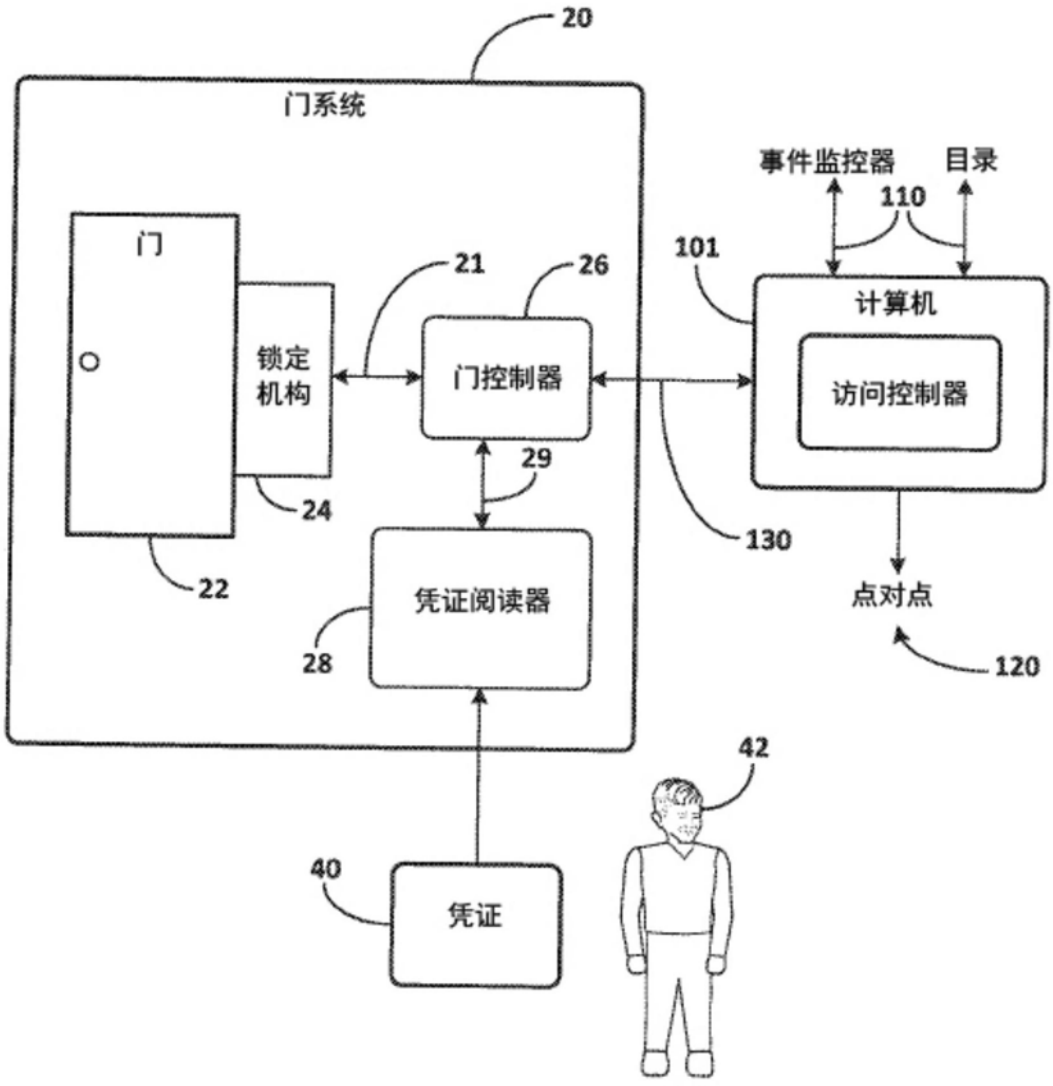

20
门系统
门
锁定
机构
21
26
门控制器
29
24
22
凭证阅读器
28
事件监控器
目录
110
101
计算机
访问控制器
130
点对点
120
42
40
凭证

图1C

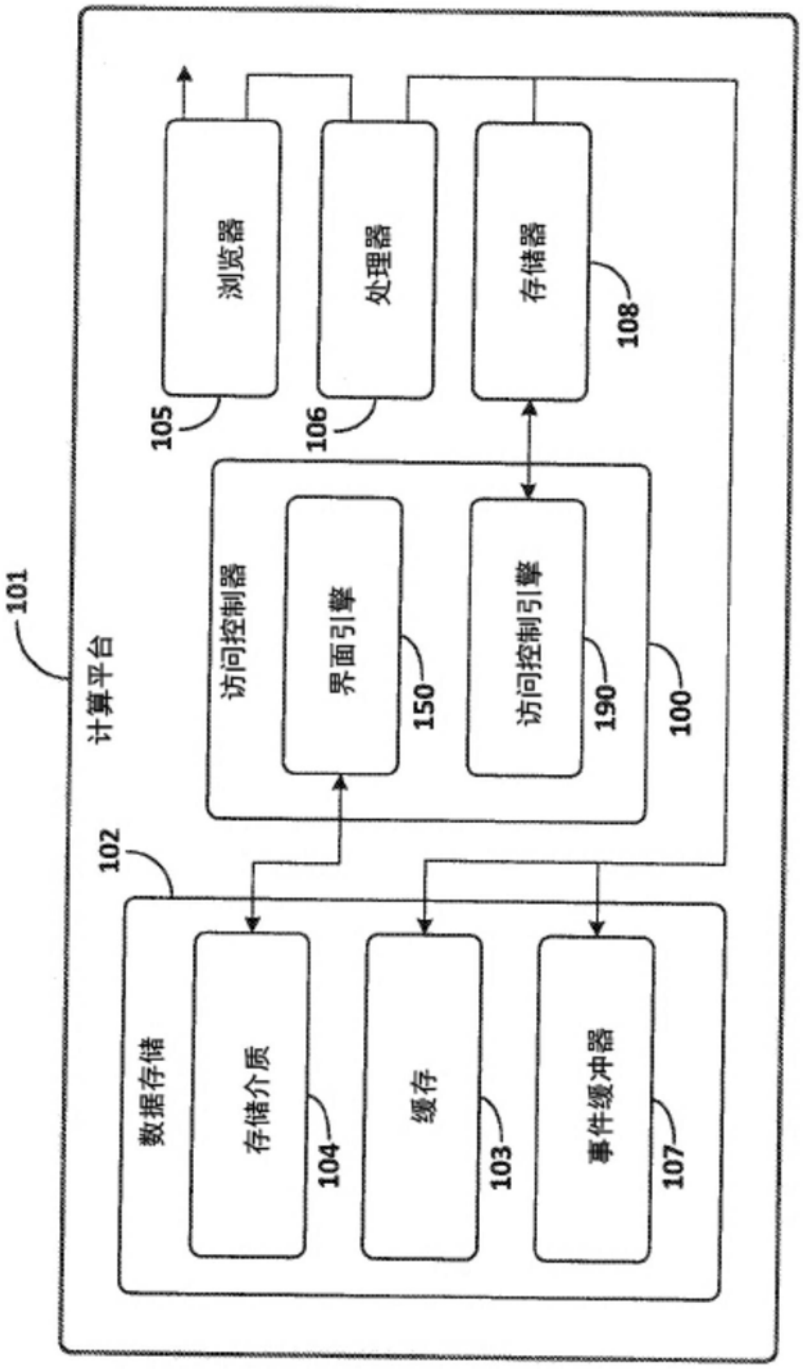

101
计算平台
102
数据存储
存储介质
104
缓存
103
事件缓冲器
107
访问控制器
界面引擎
150
访问控制引擎
190
100
浏览器
105
处理器
106
存储器
108

图2

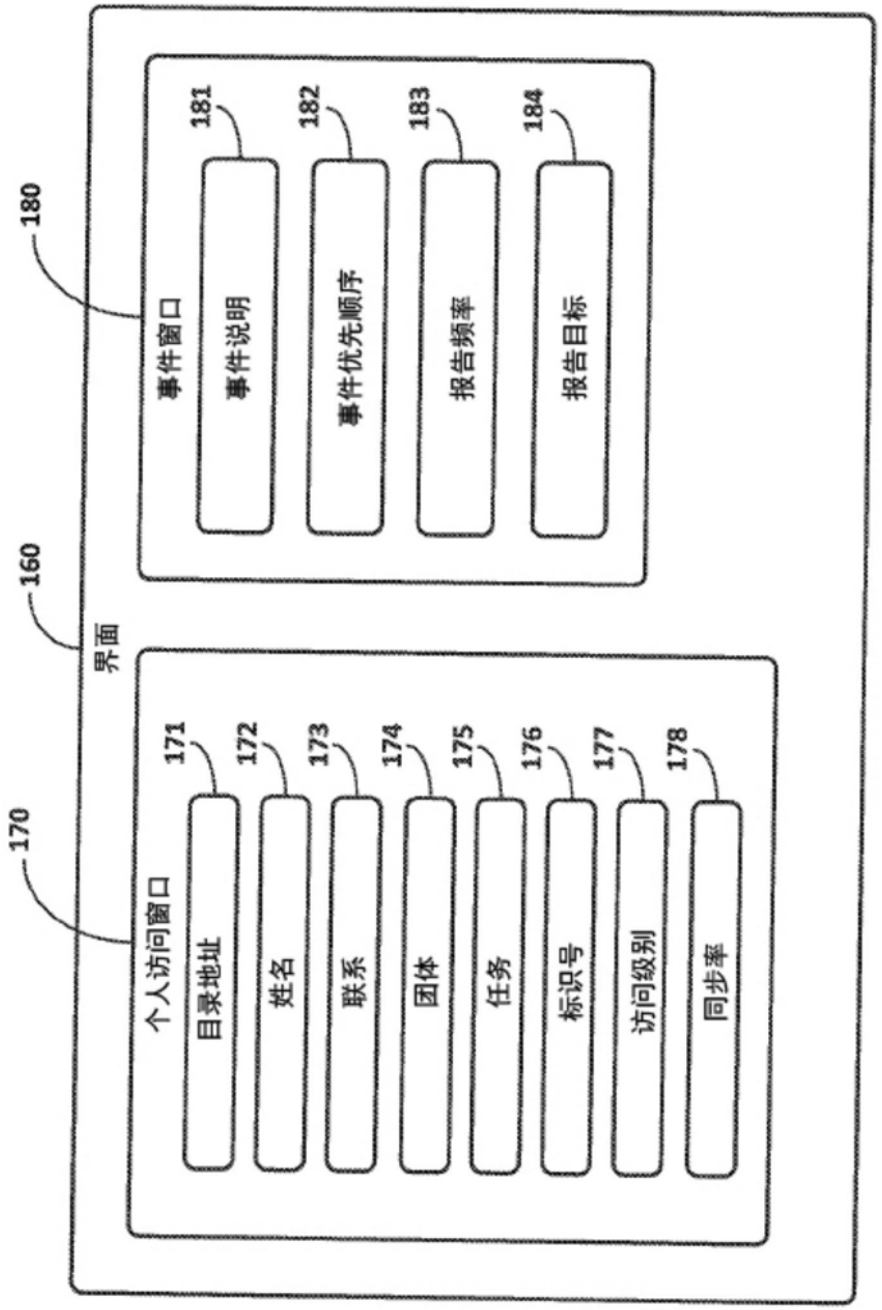

180
事件窗口
181
事件说明
182
事件优先顺序
183
报告频率
184
报告目标
160
界面
170
个人访问窗口
171
目录地址
172
姓名
173
联系
174
团体
175
任务
176
标识号
177
访问级别
178
同步率

图3

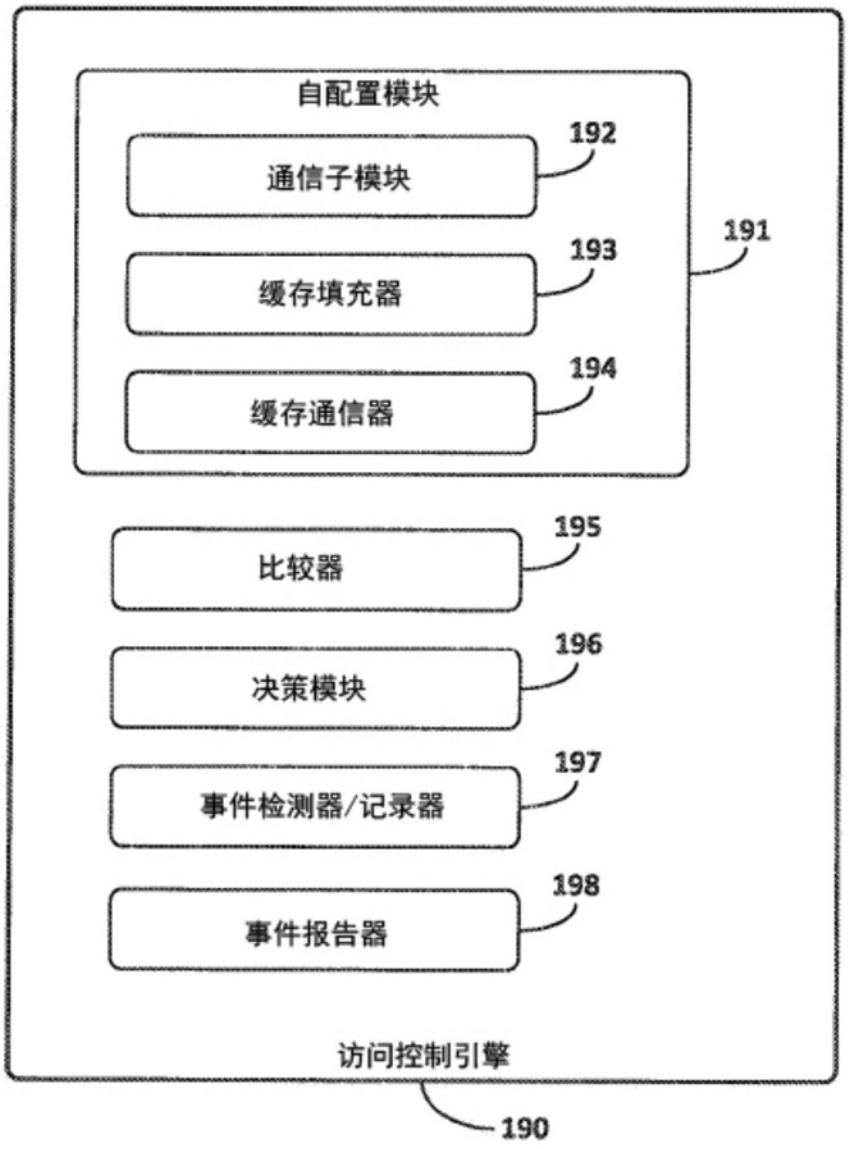

自配置模块
192
通信子模块
193
缓存填充器
194
缓存通信器
191
195
比较器
196
决策模块
197
事件检测器/记录器
198
事件报告器
访问控制引擎
190

图4

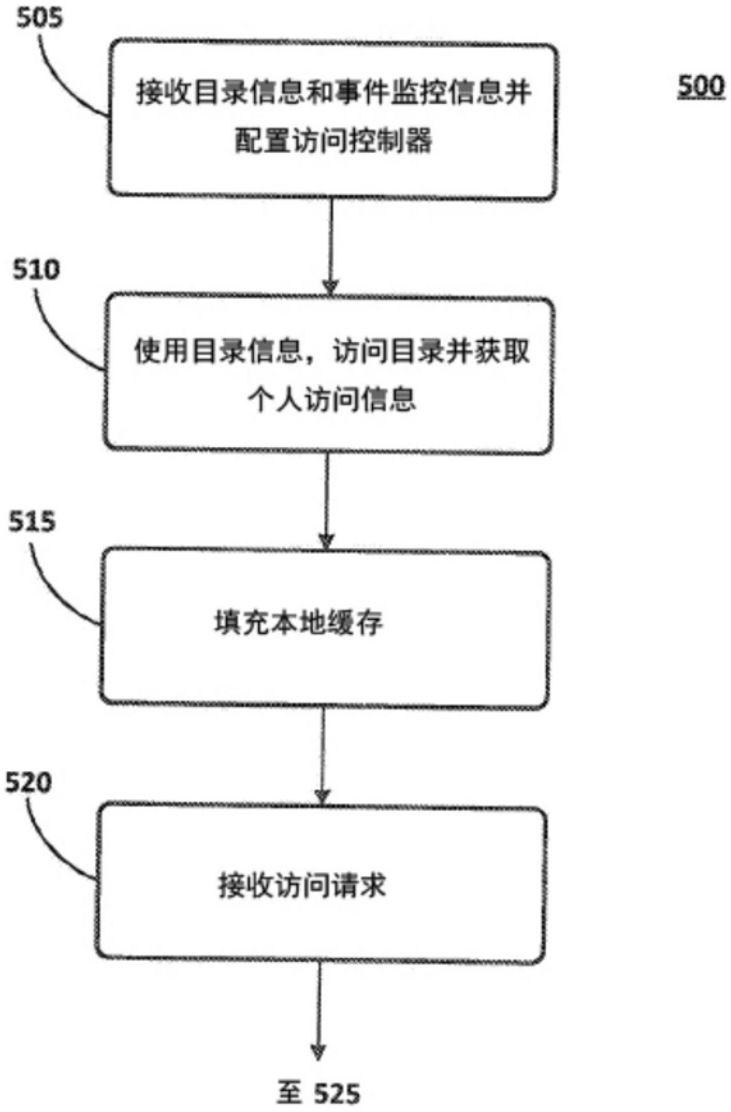

505
接收目录信息和事件监控信息并配置访问控制器
500
510
使用目录信息，访问目录并获取个人访问信息
515
填充本地缓存
520
接收访问请求
至 525

图5A

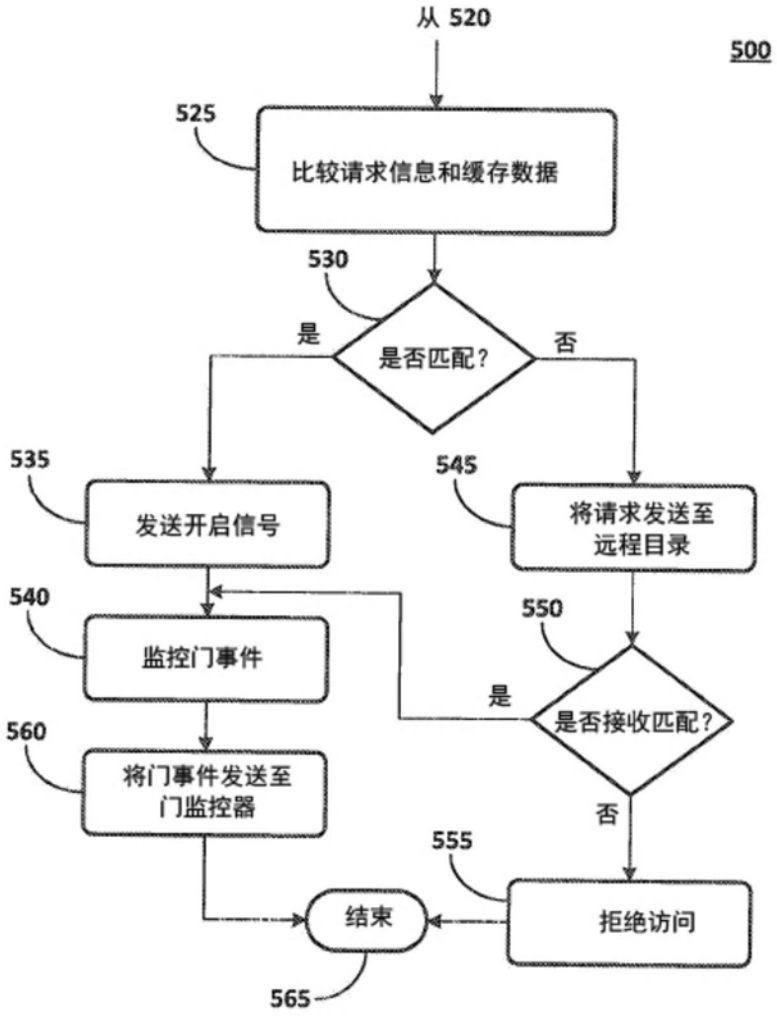

从 520
500
525
比较请求信息和缓存数据
530
是否匹配?
是
否
535
发送开启信号
545
将请求发送至
远程目录
540
监控门事件
550
是否接收匹配?
是
560
将门事件发送至
门监控器
否
555
拒绝访问
结束
565

图5B

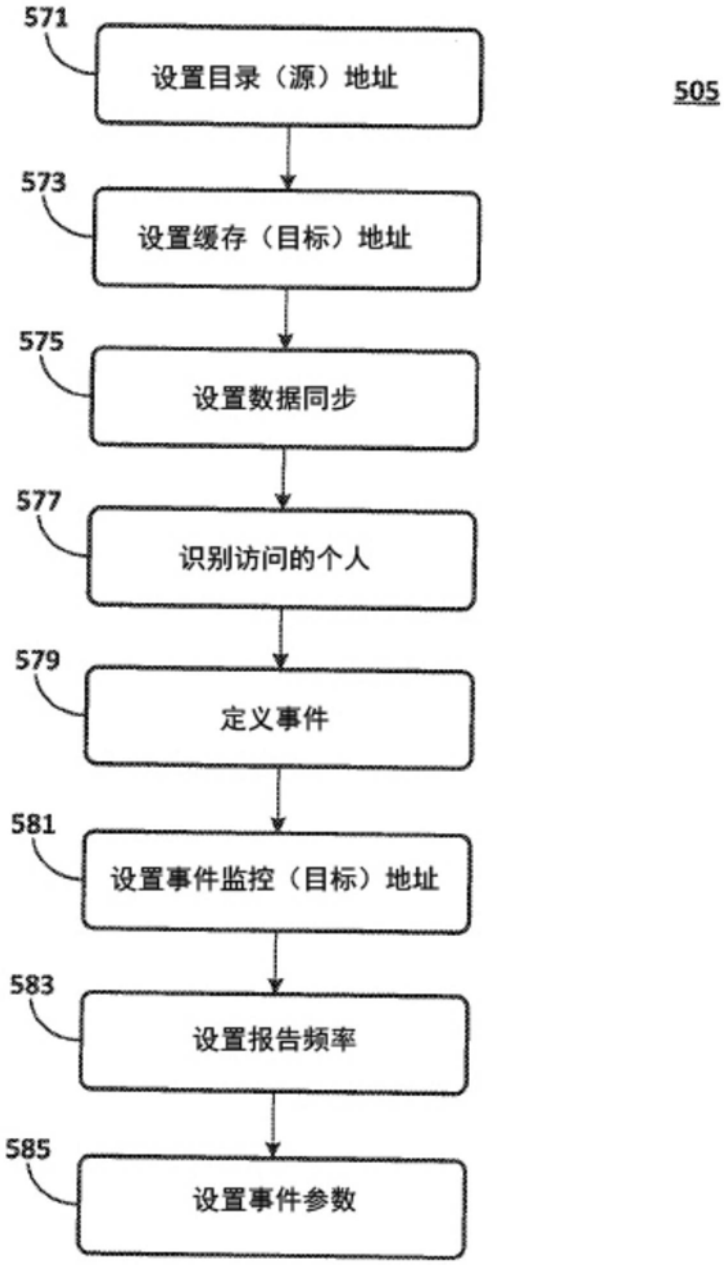

571
设置目录（源）地址
505
573
设置缓存（目标）地址
575
设置数据同步
577
识别访问的个人
579
定义事件
581
设置事件监控（目标）地址
583
设置报告频率
585
设置事件参数

图5C