(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 106104548 B
(45)授权公告日 2019.08.06

(21)申请号 201480065011.6
(22)申请日 2014.04.30
(65)同一申请的已公布的文献号
申请公布号 CN 106104548 A
(43)申请公布日 2016.11.09
(30)优先权数据
201309622-7 2013.12.26 SG
(85)PCT国际申请进入国家阶段日
2016.05.27
(86)PCT国际申请的申请数据
PCT/SG2014/000192 2014.04.30
(87)PCT国际申请的公布数据
WO2015/099607 EN 2015.07.02
(73)专利权人 策安保安有限公司
地址 新加坡新加坡市
专利权人 杨长辉
(72)发明人 杨长辉 陈宝明 叶泰山
梅拉图尔·S·钱德拉塞克兰
吕瀚政
(74)专利代理机构 北京德琦知识产权代理有限公司 11018
代理人 严芬 宋志强
(51)Int.Cl.
G06F 21/32(2013.01)
(56)对比文件
US 2008271109 A1,2008.10.30,
US 2007186106 A,2007.08.09,
US 2012042366 A,2012.02.16,
CN 101297282 A,2008.10.29,
审查员 彭明明

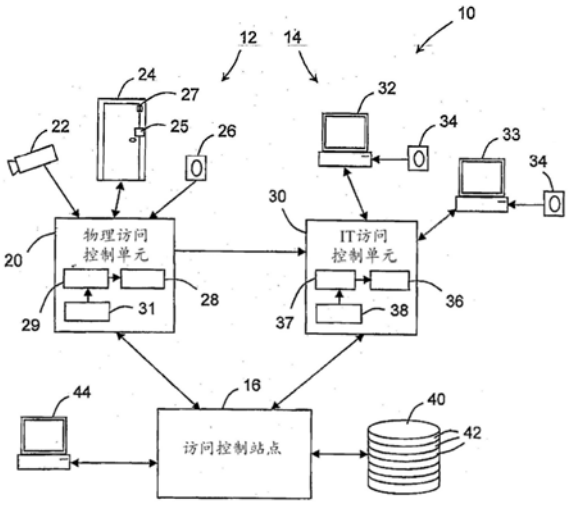
权利要求书4页 说明书8页 附图2页

(54)发明名称

集成访问控制及身份管理系统

(57)摘要

一种集成访问控制及身份管理系统包括IT访问控制单元和物理访问控制单元。IT访问控制单元包括针对与该系统相关联的每个用户定义访问权限的所存储的访问标准。IT访问控制单元被设置为基于所存储的访问标准来确定是否以及应在何种程度上准许用户进行访问。物理访问控制单元被设置为对人员物理访问区域的尝试进行监视。该集成系统被设置为将访问信息存储在访问信息存储设备中,该访问信息指示由IT访问控制单元和物理访问控制单元监视的访问尝试。所存储的访问标准被设置为使得如下标准能被定义在所存储的访问标准中:用户身份标准、访问位置标准、访问时间标准、指示用户被允许访问的IT资源的类型的类型标准、和/或访问级别标准。



CN 106104548 B

1.一种访问控制系统,包括:

IT访问控制单元,被设置为对人员访问至少一种IT资源的尝试进行监视;

物理访问控制单元,被设置为对人员物理地访问区域的尝试进行监视,并基于人员是否通过所述物理访问控制单元被肯定性识别来准许所述人员物理地访问区域;

所存储的IT访问标准,针对与所述至少一种IT资源相关联的每个用户定义访问权限;以及

访问信息存储设备,

所述IT访问控制单元被设置为基于所存储的IT访问标准,来确定是否以及应在何种程度上准许用户进行IT访问,

所述IT访问控制单元和所述物理访问控制单元中的每个能由用户直接访问,并且所述IT访问控制单元和所述物理访问控制单元彼此独立地操作,以分别准许或拒绝所述用户访问所述IT资源,或者准许或拒绝所述用户物理地访问所述区域,

所述系统被设置为将IT访问信息存储在所述访问信息存储设备中,并且将物理访问信息存储在所述访问信息存储设备中,所述IT访问信息指示由所述IT访问控制单元监视的访问尝试,所述物理访问信息指示由所述物理访问控制单元监视的访问尝试,

其中所存储的IT访问标准被设置为使得如下标准能被定义在所存储的访问标准中:身份标准,指示能够访问所述IT资源的所述用户的身份;位置标准,指示所述用户被允许访问所述IT资源时的位置;时间标准,指示所述用户被允许访问所述IT资源时的时间;类型标准,指示所述用户被允许访问的IT资源的类型;和/或访问级别标准,指示赋予所述用户的访问权限的级别;

其中所述系统被设置为将IT标记信息与所述IT访问信息相关联,将物理标记信息与所述物理访问信息相关联,并且将所述IT标记信息和所述物理标记信息存储在所述访问信息存储设备中,所述IT标记信息和所述物理标记信息包括能用来确定由所述物理访问控制单元监视的第一访问尝试是否与由所述IT访问控制单元监视的第二访问尝试相关的信息,并且所述系统便于访问被存储在所述访问信息存储设备处的所述IT标记信息和所述物理标记信息,使得所述确定能够被做出;并且

其中所述类型标准是指示所述用户被允许访问的数据的最大级别敏感性的信任级别标准。

2.根据权利要求1所述的访问控制系统,其中针对与所述系统相关联的至少一个用户,所述身份标准、所述位置标准、所述时间标准、所述类型标准以及所述访问级别标准全部被定义在所存储的访问标准中。

3.根据权利要求1或权利要求2所述的访问控制系统,其中所述IT资源包括至少一个软件应用和/或存储在至少一个数据存储设备中的数据。

4.根据权利要求1或权利要求2所述的访问控制系统,其中所述时间标准指示用户被允许访问所述IT资源时的持续时间。

5.根据权利要求1或权利要求2所述的访问控制系统,其中所述类型标准指示所述用户被允许访问的一个或多个存储位置、和/或所述用户被允许访问的一个或多个软件应用、和/或所述用户被允许访问的一个或多个数据类型。

6.根据权利要求1或权利要求2所述的访问控制系统,其中所述访问级别标准从包含管

理员、超级用户、仅查看及不可访问的组中被选择。

7.根据权利要求1或权利要求2所述的访问控制系统，其中所述用户的身份基于从所述人员处采集到的凭证来确定。

8.根据权利要求7所述的访问控制系统，其中所述凭证信息包括：与所述人员相关联的生物特征信息、从由所述人员携带的识别卡采集到的识别信息、由所述人员提供的个人识别号码、或任何其他的识别信息。

9.根据权利要求1或权利要求2所述的访问控制系统，其中所述IT标记信息和/或所述物理标记信息包括指示与所述标记信息相关联的所述访问尝试的位置的位置信息。

10.根据权利要求1或权利要求2所述的访问控制系统，其中所述IT标记信息和/或所述物理标记信息包括指示从尝试访问区域或资源的人员处采集到的至少一个凭证的凭证信息。

11.根据权利要求1或权利要求2所述的访问控制系统，其中所述IT标记信息和/或所述物理标记信息包括日期和/或时间信息。

12.根据权利要求1或权利要求2所述的访问控制系统，其中所述IT标记信息和/或所述物理标记信息以元数据的形式被添加到所述访问信息。

13.根据权利要求1或权利要求2所述的访问控制系统，其中所述访问信息存储设备从相应的IT访问控制单元和物理访问控制单元接收所述访问信息以及所述IT标记信息和所述物理标记信息，并且所述访问信息存储设备被设置为使得所述访问信息以及所述IT标记信息和所述物理标记信息能通过所述访问信息存储设备被访问。

14.根据权利要求13所述的访问控制系统，其中所述访问信息存储设备被设置为便于用户通过所述访问信息和/或所述IT标记信息和所述物理标记信息来进行搜索。

15.根据权利要求14所述的访问控制系统，其中所述访问信息存储设备能本地或远程地访问，并且能通过诸如互联网的通信网络被访问。

16.一种使用一个访问控制系统控制人员对IT资源的访问的方法，所述方法包括：

对人员访问IT资源的尝试进行监视；

存储IT访问标准，所存储的IT访问标准针对与所述系统相关联的每个用户定义访问权限；

基于所存储的IT访问标准来确定是否以及应在何种程度上准许用户进行IT访问；

对人员物理地访问区域的尝试进行监视；

基于人员是否通过一个物理访问控制单元被肯定性识别，来准许所述人员物理地访问区域；以及

将IT访问信息存储在访问信息存储设备中，并且将物理访问信息存储在所述访问信息存储设备中，所述IT访问信息指示由一个IT访问控制单元监视的访问尝试，所述物理访问信息指示由所述物理访问控制单元监视的访问尝试，

其中所述IT访问控制单元和所述物理访问控制单元中的每个能由用户直接访问，并且所述IT访问控制单元和所述物理访问控制单元彼此独立地操作，以分别准许或拒绝所述用户访问所述IT资源，或者准许或拒绝所述用户物理地访问所述区域，

其中所存储的访问标准被设置为使得如下标准能被定义在所存储的访问标准中：身份标准，指示能够访问所述IT资源的所述用户的身份；位置标准，指示所述用户被允许访问所

述IT资源时的位置;时间标准,指示所述用户被允许访问所述IT资源时的时间;类型标准,指示所述用户被允许访问的IT资源的类型;和/或访问级别标准,指示赋予所述用户的访问权限的级别;

其中所述系统被设置为将IT标记信息与所述IT访问信息相关联,将物理标记信息与所述物理访问信息相关联,并且将所述IT标记信息和所述物理标记信息存储在所述访问信息存储设备中,所述IT标记信息和所述物理标记信息包括能用来确定由所述物理访问控制单元监视的第一访问尝试是否与由所述IT访问控制单元监视的第二访问尝试相关的信息,并且所述系统便于访问被存储在所述访问信息存储设备处的所述IT标记信息和所述物理标记信息,使得所述确定能够被做出;并且

其中所述类型标准是指示所述用户被允许访问的数据的最大级别敏感性的信任级别标准。

17.根据权利要求16所述的方法,包括:针对与所述系统相关联的至少一个用户,在所存储的访问标准中定义所述身份标准、所述位置标准、所述时间标准、所述类型标准以及所述访问级别标准中的全部。

18.根据权利要求16或权利要求17所述的方法,其中所述IT资源包括至少一个软件应用和/或存储在至少一个数据存储设备中的数据。

19.根据权利要求16或权利要求17所述的方法,其中所述时间标准指示用户被允许访问所述IT资源时的持续时间。

20.根据权利要求16或权利要求17所述的方法,其中所述类型标准指示所述用户被允许访问的一个或多个存储位置、和/或所述用户被允许访问的一个或多个软件应用、和/或所述用户被允许访问的一个或多个数据类型。

21.根据权利要求16或权利要求17所述的方法,包括:从包含管理员、超级用户、仅查看以及不可访问的组中选择所述访问级别标准。

22.根据权利要求16或权利要求17所述的方法,包括:基于从所述人员处采集到的凭证来确定所述用户的身份。

23.根据权利要求22所述的方法,其中所述凭证信息包括:与所述人员相关联的生物特征信息、从由所述人员携带的识别卡中采集到的识别信息、由所述人员提供的个人识别号码、或任何其他的识别信息。

24.根据权利要求16或权利要求17所述的方法,其中所述IT标记信息和/或所述物理标记信息包括指示与所述标记信息相关联的所述访问尝试的位置的位置信息。

25.根据权利要求16或权利要求17所述的方法,其中所述IT标记信息和/或所述物理标记信息包括指示从尝试访问区域或资源的人员处采集到的至少一个凭证的凭证信息。

26.根据权利要求16或权利要求17所述的方法,其中所述IT标记信息和/或所述物理标记信息包括日期和/或时间信息。

27.根据权利要求16或权利要求17所述的方法,其中所述IT标记信息和/或所述物理标记信息以元数据的形式被添加到所述访问信息。

28.根据权利要求16或权利要求17所述的方法,包括:

在所述访问信息存储设备处接收所述访问信息以及所述IT标记信息和所述物理标记信息;以及

便于通过所述访问信息存储设备访问所述访问信息以及所述IT标记信息和所述物理标记信息。

29.根据权利要求28所述的方法，包括：便于用户通过访问信息和/或所述IT标记信息和所述物理标记信息来进行搜索。

30.根据权利要求29所述的方法，包括：便于通过通信网络本地或远程地访问所述访问信息存储设备。

31.根据权利要求16或权利要求17所述的方法，包括：使用所述访问信息和/或所述IT标记信息和所述物理标记信息来跟踪与访问尝试相关联的人员。

集成访问控制及身份管理系统

技术领域

[0001] 本发明涉及一种用于控制人员对至少一种IT资源的访问的集成访问控制系统、以及一种用于控制人员对至少一种IT资源的访问的方法。

背景技术

[0002] 已知提供一种系统，该系统用于监视并控制对区域的物理访问，以使访问仅限于授权人员。在这样一个系统中，经过多个门中任意一个门的人员的访问通过下列来控制：为每个门提供用于从人员采集诸如个人识别号码、生物特征信息、或被存储在卡上的ID号码的一个或多个凭证的凭证读取器，并对所采集的凭证与存储在后台系统中的参考凭证进行验证。

[0003] 还已知提供一种系统，该系统用于监视并控制对IT资源的访问，例如包括软件应用和数据，使得只有授权人员能够使用软件和/或访问数据。这样的IT访问控制可通过与IT资源相关联的每个用户可操作的计算设备来实现，或者可使用独立的网关设备来至少部分地实现，该网关设备操作以对访问进行控制，并根据用户的凭证来准许或拒绝访问。

[0004] 然而，这种传统的IT访问控制系统相对简单，因此无法提供有效的访问控制。

发明内容

[0005] 根据本发明的第一方面，提供了一种访问控制系统，包括：

[0006] IT访问控制单元，被设置对人员访问至少一种IT资源的尝试进行监视；

[0007] 物理访问控制单元，被设置为对人员物理地访问区域的尝试进行监视，并基于人员是否通过所述物理访问控制单元被肯定性识别来准许所述人员物理地访问区域；

[0008] 所存储的IT访问标准，针对与所述至少一种IT资源相关联的每个用户定义访问权限；以及

[0009] 访问信息存储设备，

[0010] 所述IT访问控制单元被设置为基于所存储的IT访问标准，来确定是否以及应在何种程度上准许用户进行IT访问，

[0011] 所述IT访问控制单元和所述物理访问控制单元中的每个能由用户直接访问，并且所述IT访问控制单元和所述物理访问控制单元彼此独立地操作，以分别准许或拒绝所述用户访问所述IT资源，或者准许或拒绝所述用户物理地访问所述区域，

[0012] 所述系统被设置为将IT访问信息存储在所述访问信息存储设备中，并且将物理访问信息存储在所述访问信息存储设备中，所述IT访问信息指示由所述IT访问控制单元监视的访问尝试，所述物理访问信息指示由所述物理访问控制单元监视的访问尝试，

[0013] 其中所存储的IT访问标准被设置为使得如下标准可被定义在所存储的访问标准中：身份标准，指示能够访问所述IT资源的用户的身份；位置标准，指示所述用户被允许访问所述IT资源时的位置；时间标准，指示所述用户被允许访问所述IT资源时的时间；类型标准，指示所述用户被允许访问的IT资源的类型；和/或访问级别标准，指示赋予所述用户的

访问权限的级别;并且

[0014] 其中所述系统被设置为将IT标记信息与所述IT访问信息相关联,将物理标记信息与所述物理访问信息相关联,并且将所述IT标记信息和所述物理标记信息存储在所述访问信息存储设备中,所述IT标记信息和所述物理标记信息包括能用来确定由所述物理访问控制单元监视的第一访问尝试是否与由所述IT访问控制单元监视的第二访问尝试相关的信息,并且所述系统便于访问被存储在所述访问信息存储设备处的所述IT标记信息和所述物理标记信息,使得所述确定能够被做出。

[0015] 在一个实施例中,所述系统包括访问信息存储设备,所述系统被设置为将访问信息存储在所述访问信息存储设备中,所述访问信息指示由所述IT访问控制单元和所述物理访问控制单元监视的访问尝试。

[0016] 在一个实施例中,针对与所述系统相关联的至少一个用户,所述身份标准、所述位置标准、所述时间标准、所述类型标准以及所述访问级别标准全部被定义在所存储的访问标准中。

[0017] 在一个实施例中,所述IT资源包括至少一个软件应用和/或存储在至少一个数据存储设备中的数据。

[0018] 在一个实施例中,所述时间标准指示用户被允许访问所述IT资源时的持续时间。

[0019] 在一个实施例中,所述类型标准指示所述用户被允许访问的一个或多个存储位置、和/或所述用户被允许访问的一个或多个软件应用、和/或所述用户被允许访问的一个或多个数据类型。

[0020] 在一个实施例中,所述类型标准指示所述用户被允许访问的数据的最大级别敏感性的信任级别标准。

[0021] 在一个实施例中,所述访问级别标准从包含管理员、超级用户、仅查看及不可访问的组中被选择。

[0022] 在一个实施例中,所述用户的身份基于从所述人员处采集到的凭证来确定。

[0023] 所述凭证信息可包括:与所述人员相关联的生物特征信息、从由所述人员携带的识别卡采集到的识别信息、由所述人员提供的个人识别号码、或任何其他的识别信息。

[0024] 在一个实施例中,所述标记信息包括指示与所述标记信息相关联的所述访问尝试的位置的位置信息。

[0025] 在一个实施例中,所述标记信息包括指示从尝试访问区域或资源的人员处采集到的至少一个凭证的凭证信息。

[0026] 在一个实施例中,所述标记信息包括日期和/或时间信息。

[0027] 在一个实施例中,所述标记信息以元数据的形式被添加到所述访问信息。

[0028] 在一个实施例中,所述访问信息存储设备从所述第一访问控制单元和所述第二访问控制单元接收所述访问信息和所述标记信息,并且所述访问信息存储设备被设置为使得所述访问信息和所述标记信息可通过所述访问信息控制设备被访问。

[0029] 所述访问信息控制设备可被设置为便于用户通过访问信息和/或标记信息来进行搜索。

[0030] 所述访问信息控制设备可本地或远程地被访问,并且可通过诸如互联网的通信网络被访问。

[0031] 根据本发明的第二方面，提供一种控制人员对IT资源的访问的方法，所述方法包括：

[0032] 对人员访问IT资源的尝试进行监视；以及

[0033] 存储IT访问标准，所存储的IT访问标准针对与所述系统相关联的每个用户定义访问权限；

[0034] 基于所存储的IT访问标准来确定是否以及应在何种程度上准许用户进行IT访问；

[0035] 对人员物理地访问区域的尝试进行监视；

[0036] 基于人员是否通过所述物理访问控制单元被肯定性识别，来准许所述人员物理地访问区域；以及

[0037] 将IT访问信息存储在访问信息存储设备中，并且将物理访问信息存储在所述访问信息存储设备中，所述IT访问信息指示由所述IT访问控制单元监视的访问尝试，所述物理访问信息指示由所述物理访问控制单元监视的访问尝试，

[0038] 其中所述IT访问控制单元和所述物理访问控制单元中的每个能由用户直接访问，并且所述IT访问控制单元和所述物理访问控制单元彼此独立地操作，以分别准许或拒绝所述用户访问所述IT资源，或者准许或拒绝所述用户物理地访问所述区域，

[0039] 其中所存储的访问标准被设置为使得如下标准可被定义在所存储的访问标准中：身份标准，指示能够访问所述IT资源的所述用户的身份；位置标准，指示所述用户被允许访问所述IT资源时的位置；时间标准，指示所述用户被允许访问所述IT资源时的时间；类型标准，指示所述用户被允许访问的IT资源的类型；和/或访问级别标准，指示赋予所述用户的访问权限的级别；并且

[0040] 其中所述系统被设置为将IT标记信息与所述IT访问信息相关联，将物理标记信息与所述物理访问信息相关联，并且将所述IT标记信息和所述物理标记信息存储在所述访问信息存储设备中，所述IT标记信息和所述物理标记信息包括能用来确定由所述物理访问控制单元监视的第一访问尝试是否与由所述IT访问控制单元监视的第二访问尝试相关的信息，并且所述系统便于访问被存储在所述访问信息存储设备处的所述IT标记信息和所述物理标记信息，使得所述确定能够被做出。

附图说明

[0041] 本发明现将仅通过举例并参考附图来进行描述，附图中：

[0042] 图1是根据本发明实施例的访问控制系统的图形表示；

[0043] 图2是图1所示的访问控制系统的组件的图形表示；以及

[0044] 图3示出图1和图2所示的访问控制系统的访问矩阵。

具体实施方式

[0045] 参考图1，访问控制系统10的实施例被示出，访问控制系统10被设置为控制对区域的物理访问以及对资源的IT访问。在本示例中，访问控制系统10还通过在访问信息存储设备中记录与用户相关联的历史访问事件信息并且便于由系统的操作者对该历史访问事件信息的访问，来便于对访问尝试的监视。

[0046] 在本示例中，IT资源可包括一个或多个软件应用和/或存储在一个或多个数据存

储设备中的一个或多个文件夹中的数据。

[0047] 访问事件包括:对人员的肯定性识别,由此准许该人员物理地访问区域中的至少一部分或电子地访问IT资源的应用或数据中的至少一部分;否定性识别,其中参与者尝试获得访问,但是该人员的身份未经验证,由此拒绝该人员的访问;以及另外未授权的对区域或IT资源的物理或电子访问,诸如强行进入受控入口门或从IT资源中物理断开计算设备。

[0048] 系统10包括物理访问控制装置12和IT访问控制装置14,在本示例中,物理访问控制装置12和IT访问控制装置14中的每个与访问信息存储设备通信,该访问信息存储设备采用可相对于物理访问控制装置12和IT访问控制装置14被远程放置的集成访问控制及身份管理站点16的形式,例如通过互联网与物理访问控制装置12和IT访问控制装置14通信。在本示例中,物理访问控制装置12和IT访问控制装置14被布置在相同的位置处或彼此非常接近。

[0049] 物理访问控制装置12被设置为控制对区域的物理访问,并确定是否已发生了不期望的访问事件,诸如基于所采集的用户凭证的失败的物理访问尝试、或强行获得物理访问的尝试。同样地,IT访问控制装置14被设置为控制对包括软件应用和/或数据的IT资源的访问,并确定是否已发生了不期望的访问事件,诸如基于所采集的用户凭证的失败的IT访问尝试、所定义的访问时期之外的或超过所定义的访问持续时间的访问尝试、对用户未被授权的数据的访问的尝试、来自未被授权的位置的访问尝试、或强行获得对软件或数据的访问的尝试。

[0050] 在本示例中,指示访问尝试的信息由物理访问控制装置12和IT访问控制装置14发送给集成访问控制及身份管理站点16,并且相关的标记信息通过访问控制装置12和14中的每个被添加到访问信息。标记信息包括可用于将访问事件彼此关联的信息,例如,指示位置的信息、指示所采集的用户凭证数据的信息、日期和/或时间信息等。

[0051] 因为可能彼此相关的访问控制事件能够借助于标记信息而彼此关联,所以操作者能够通过搜索特定的标记信息来容易地识别潜在相关的物理和IT访问控制事件。

[0052] 在图1所示的示例中,物理访问装置12包括物理访问控制单元20,物理访问控制单元20被设置为对物理访问控制尝试进行控制,具体是从寻求获得对区域的物理访问的用户处采集凭证,将所采集的凭证与参考凭证相比较,并基于该比较准许或拒绝访问。

[0053] 在本示例中,物理访问控制单元20被连接到至少一个被设置为从周围区域采集视频信息的摄像机22、至少一个诸如门的访问点24、以及至少一个凭证读取器26。

[0054] 每个访问点24具有相关联的门锁25,门锁25在本示例中由相应的物理访问控制单元20控制,使得可引起门锁25响应于来自物理访问控制单元20的适当信号来启用或阻止访问点24的开启。

[0055] 在使用期间,凭证读取器26从期望通过访问点24的人员处采集至少一个用户凭证,并且物理访问控制单元20将所采集的用户凭证与所存储的参考用户凭证相比较,并对是准许还是拒绝访问做出决定。如果访问被准许,则物理访问控制单元20将信号发送到门锁25,用以将门锁25置于未锁定状态,从而允许人员通过访问点24并对区域进行访问。如果访问未被准许,则物理访问控制单元20不将信号发送至门锁25,门锁25因此而保持在锁定状态下,从而防止人员通过访问点24并进入区域。是准许还是拒绝访问的决定也可以基于发生访问尝试的时间和/或日期。例如,在访问被许可时,用户可被分配有不同的日期和/或

时间，并且物理访问控制单元20被设置为允许仅在所分配的日期/时间时进行访问。

[0056] 在本示例中，凭证读取器26采用生物特征读取器的形式，该生物特征读取器被设置为从人员处采集诸如指纹数据的生物特征数据，但应当理解，也设想了其他类型的凭证读取器，诸如被设置为读取人员所携带的个人识别卡的读卡器、用于使人员能够输入个人识别号码的小键盘、或者被设置为确定人员的身份的任何其他设备。

[0057] 虽然在本示例中访问点24是门，但应当认识到，也设想了其他类型的访问点，诸如电梯门、旋转门、停车门、或任何其他的物理屏障。

[0058] 在本示例中，访问点24具有相关联的传感器27，传感器27在本示例中用于检测访问点24是打开还是关闭。也设想了用于此目的的任何适当的传感器，并且在本示例中使用磁式接近传感器。

[0059] 传感器27被连接到物理访问控制单元20，并且物理访问控制单元20监视传感器27，并在访问点24开放时生成警告信号。警告可被用于触发报警，例如在传感器27指示物理访问点24开放但是没有发生有效的凭证验证的情况下。

[0060] 访问尝试，具体是所尝试的未授权访问事件或实际的未授权访问事件，也可以使用摄像机22来确定，例如通过在物理访问控制单元20处自动分析由摄像机22拍摄的视频和/或图像。

[0061] 在本示例中，物理访问控制单元20还包括标记应用28，标记应用28被设置为将标记信息29添加到待发送给集成访问控制及身份管理站点16的访问信息。在本示例中，标记信息29包括指示物理访问控制装置12的位置的信息、访问尝试发生的日期和时间、从期望通过访问点24的人员处采集到的生物特征信息、和/或任意其他的相关信息。

[0062] 标记应用28可从如下源中获得标记信息：凭证读取器、存储在访问控制单元20处的位置和/或识别信息、从与访问控制单元20相关联的诸如IP地址的相应电子标识符得到的位置信息、或能够提供可用来将物理访问尝试与其他访问尝试相联系的标记信息的任何其他源。在本示例中，物理访问控制装置12包括定位应用31，定位应用31被设置为确定物理访问控制单元20的位置，例如使用所确定的与访问控制单元20的当前位置相关的IP地址。

[0063] 在集成访问控制及身份管理站点16处接收的指示物理访问尝试的访问信息以及关联的标记信息被存储在与集成访问控制及身份管理站点16通信的数据存储设备中，该数据存储设备在本示例中采用数据库40的形式。数据库40包括多个记录42，其中每个记录涉及访问尝试。

[0064] 标记信息被用来使操作者能够将物理访问尝试与IT访问尝试相联系。

[0065] 应当理解，物理访问控制单元20可通过计算设备来实现，例如被实现为由计算设备实现的软件应用。

[0066] IT访问控制装置14包括IT访问控制单元30，IT访问控制单元30被设置为控制对IT资源的访问尝试，从寻求获得对IT资源的访问的用户处采集凭证，将所采集的凭证与参考凭证相比较，基于该比较来准许或拒绝访问，如果访问被准许，则确定访问应在何种程度上被准许。

[0067] IT访问控制装置14能够直接从一个或多个本地布置的例如通过LAN连接到IT访问控制单元30的计算设备32接收访问尝试，或者直接从一个或多个远程放置的例如通过互联网连接到IT访问控制单元30的计算设备33接收访问尝试。

[0068] 计算设备32、33中的任何一个可被连接到凭证读取器34，凭证读取器34能够从期望获得对IT资源的访问的人员处采集到至少一个用户凭证。

[0069] 凭证读取器可包括被设置为从人员处采集诸如指纹数据的生物特征数据的生物特征读取器。然而应当理解，也设想了被设置为确定人员的身份的其他类型的认证设备，诸如被设置为读取人员所携带的个人识别卡的读卡器、用于使人员能够输入个人识别号码的小键盘、或者传统的用户名/密码装置。

[0070] 是准许还是拒绝访问的决定以及访问被准许的程度通过将所定义的IT访问标准与当前访问标准相比较来确定，当前访问标准可包括所采集的用户凭证中的任意一个或多个、访问尝试发生的时间和/或日期、访问的持续时间、尝试获得访问的人员的位置、和/或用户期望访问的数据的类型。因此，IT访问控制装置14能够基于用户是谁、用户在何处、用户何时尝试获得访问、以及用户尝试访问什么来准许、拒绝或限制对IT资源的访问，并且在这种方式下，IT访问控制装置14能够提供高度的访问控制。

[0071] 例如，在访问被许可时，用户可被分配有不同的日期和/或时间、或者所定义的访问持续时间，并且IT访问控制单元30被设置为允许仅在所分配的日期/时间进行访问和/或仅访问达所定义的持续时间。

[0072] 访问级别可基于尝试获得访问的人员的位置来确定，例如与人员相关联的计算设备是否通过本地局域网被连接到IT访问控制单元30，或者用户的计算设备是否通过互联网被连接到IT访问控制单元30。在一个实施例中，位置信息可从物理访问控制装置12(例如凭证读取器26)处得到，使得通过使用凭证读取器26获得肯定性认证，该人员的位置在物理访问控制单元处被确认。

[0073] 访问级别可基于用户身份信息来确定，该用户身份信息由从用户处采集的凭证信息得到。

[0074] 访问级别可基于用户是否已被赋予对特定类型的数据进行访问或对存储在特定位置的数据进行访问的权限来确定。例如，在组织中拥有高级职位的用户可被授权对与该组织相关联的所有数据进行访问，而在组织中拥有初级职位的用户可被授权仅对与该用户直接相关的数据进行访问，例如被存储在与用户相关联的文件夹中的数据。

[0075] 应当理解，在本实施例中，物理访问控制单元20和IT访问控制单元30彼此接合，使得由物理访问控制单元20采集到的诸如凭证信息的信息可被IT访问控制单元30使用，和/或由IT访问控制单元30采集到的信息可被物理访问控制单元20使用。

[0076] 应当理解，访问控制系统10被设置为使得上述访问标准可以被定制，以使适用于用户的访问标准可以被修改，从而应用于用户的安全性程度可以得到修改。

[0077] 在本示例中的IT访问控制单元30也被设置为将标记信息37添加到访问信息，该访问信息指示由IT监控装置14发送到集成访问控制及身份管理站点16的访问尝试。在本示例中，标记信息37包括指示IT监控装置14的位置的信息、访问尝试发生的日期和时间、诸如从期望获得对IT系统的访问的人员处采集到的生物特征信息的身份信息、和/或任何其他的相关信息。

[0078] 在本实施例中，IT访问控制单元30还包括标记应用36，标记应用36被设置为将标记信息37添加到待发送至集成访问控制及身份管理站点16的访问信息。标记应用可以从如下源中获得标记信息：凭证读取器26、34、存储在IT访问控制单元30处的位置和/或识别信

息、从与IT访问控制单元30相关联的诸如IP地址的电子标识符得到的位置信息、或能够提供可用来将IT访问尝试与其他访问尝试记录42相联系的标记信息的任何其他源。

[0079] 在本示例中，IT访问控制单元30可包括定位应用38，定位应用38被设置为对期望获得访问的计算设备32、33的位置进行确定，例如使用与计算设备32、33的当前位置相关的IP地址。基于所确定的位置，当计算设备32处于指定区域内时，访问可被准许，但是当计算设备不处于指定区域内时，访问被拒绝。类似地，访问可基于计算设备32、33的位置是否被验证来被准许或拒绝，例如基于计算设备33是否通过互联网被连接至IT访问控制单元30并且计算设备的位置是否能够被确定且该位置是否已被授权为安全。

[0080] 应当理解，IT访问控制单元30可使用计算设备来实现，例如至少部分地被实现为软件应用。

[0081] 在本示例中，在集成访问控制及身份管理站点16处接收到的指示IT访问尝试的访问信息和相关联的标记信息被存储在数据库40中的记录42中。

[0082] 在本示例中，物理访问控制装置12和IT访问控制装置14包括适当的功能组件，以能够基于用户所定义的相关标准对是否以及在什么程度上准许或拒绝人员的访问做出决定。为了这个目的，功能组件可包括被设置为实现一个或多个软件应用的处理器和存储器。在本示例中，访问标准被存储在物理访问控制装置12和IT访问控制装置14中，并且凭证被用于确定是准许还是拒绝访问。然而将理解，也设想了其他的实现方式。例如，访问标准可以被存储，并且可以远离物理访问控制装置和IT访问控制装置(例如在集成访问控制及身份管理站点16处)做出关于是准许还是拒绝访问的决定。

[0083] 标记信息可采取任何适当的形式，并且在本示例中，标记信息被添加到访问信息作为元数据。

[0084] 参考图2，IT访问控制装置14的组件被示出。在本示例中，IT访问控制单元30控制一个或多个用户计算设备32或一个或多个用户计算设备33对一个或多个软件应用50和/或存储在一个或多个存储设备54中的数据的访问，一个或多个用户计算设备32被本地布置且经由有线或无线LAN被连接到IT访问控制单元30，一个或多个用户计算设备33被远程布置且通过互联网52被连接到IT访问控制单元30。

[0085] 在本示例中，IT访问控制单元30被设置为使用被存储在访问矩阵56中的访问标准，来确定是准许还是拒绝访问以及访问应在何种程度上被准许。示例性访问矩阵56在图3中被示出，并且包括：用户信息58，指示与系统10相关联的用户；位置标准60，定义每个用户访问系统10所允许的位置；时间标准62，定义每个用户进行访问所允许的时间、日期和/或持续时间；信任级别标准64，定义用户被允许访问的数据的类型，该访问根据用户被允许访问的数据的敏感度来进行；以及访问级别标准66，定义授予每个用户的访问权限的级别。

[0086] 在本示例中，用户A被允许访问高级别敏感性的数据，仅当用户位于安全位置A或安全位置B时允许访问数据，并且仅允许在办公时间访问数据。此外，当用户A位于安全位置A时，用户被分配管理员访问级别，该管理员访问级别为用户提供高级别的访问权限。相比之下，当用户A位于安全位置B时，用户被分配超级用户访问级别，该超级用户访问级别为用户提供降低级别的访问权限。

[0087] 在本实施例中，管理员访问级别向用户提供对数据的充分且完整的访问，使得用户能够读取、写入和修改数据，并且用户能够执行所有的应用并以全系统权限来执行所有

功能。超级用户访问级别向用户提供部分权限，该部分权限取决于用户的角色以及需要该用户执行的功能。通常，超级用户仅能够读取和写入数据，并且有时能够修改数据。

[0088] 应当理解，由于用户A仅在该用户位于安全位置A或安全位置B时被允许访问IT资源，因此如果发生了访问IT资源的尝试，但用户的位置未被验证，例如通过在安全位置A或安全位置B处使用凭证读取器来确认用户凭证，则对数据的访问将被拒绝。

[0089] 同时在本示例中，用户C被分配不同的访问权限(仅查看、超级用户或不可访问)，这取决于该用户的位置是否被验证，例如通过验证与该用户相关联的计算设备的位置，并且取决于一天中的时间。

[0090] 应当理解，访问矩阵56可被设置为使得信任级别标准64可替代地或另外地根据数据的位置(例如，用户能够访问的存储设备和/或数据文件夹)对数据的类型进行具体定义。

[0091] 在本示例中，与物理和IT这两者相关的所有访问尝试被存储在与集成访问控制及身份管理站点16相关联的数据库40中，并且在这种方式下，单个的可访问源被提供有与所有访问尝试相关的信息。

[0092] 可以理解，在本示例中，对于每个访问尝试，指示用户尝试对区域或资源进行访问的信息、访问尝试发生的日期和时间、被准许访问的持续时间、用户的位置、以及用户访问的区域(多个)和/或资源(多个)被记录在数据库40中，并因此能被用于监视、跟踪和/或评估用户访问活动。例如，如果人员多次尝试从诸如网吧的特定未经验证的位置处访问IT资源，则系统10可被设置为对操作者生成警报。

[0093] 此外，系统可被设置为响应于根据存储在数据库40中的访问信息而确定的潜在访问风险状况，来修改在访问矩阵56中定义的任何一个或多个访问标准。例如在上面的示例中，其中从未验证的位置处发生多次访问尝试，系统10可被设置为将在访问矩阵56中为用户指定的信任级别64修改为诸如不可访问的较低级别。

[0094] 为了便于搜索数据库40中的记录42，系统可包括例如采用个人计算机、平板计算机或智能电话形式的终端44。为了这个目的，集成访问控制及身份管理站点16被设置为允许用户终端44基于潜在通用变量来搜索与物理和IT这两者所涉及的访问尝试有关的记录42，使得当物理访问尝试也伴随着IT访问尝试时，相关的物理和IT访问尝试都可以被识别。在本示例中，集成访问控制及身份管理站点16可例如通过互联网在线访问。

[0095] 应当理解，标记信息也允许操作者跟踪与物理或IT访问事件相关联的人员。

[0096] 应当认识到，系统使管理员能够基于用户是谁、用户在何处、用户何时尝试获得访问以及用户尝试访问什么，来控制对IT资源的访问。访问控制系统提供了高度的访问控制，并最小化假冒攻击的可能性(例如，通过受损机器或通过欺骗)。

[0097] 还应当认识到，与传统的电子访问控制系统不同，本访问控制系统提供了基于用户的位置来控制访问的能力，例如使用来自物理访问控制系统的位置。

[0098] 本集成访问控制系统可被看作是针对组织去除数据普遍性或实现数据普遍性的系统。该系统能够对需要更严格的访问控制的保密数据去除普遍性，同时能够对非保密数据实现普遍性。

[0099] 对本领域技术人员而言是显而易见的修改和变化被认为是在本发明的范围内。

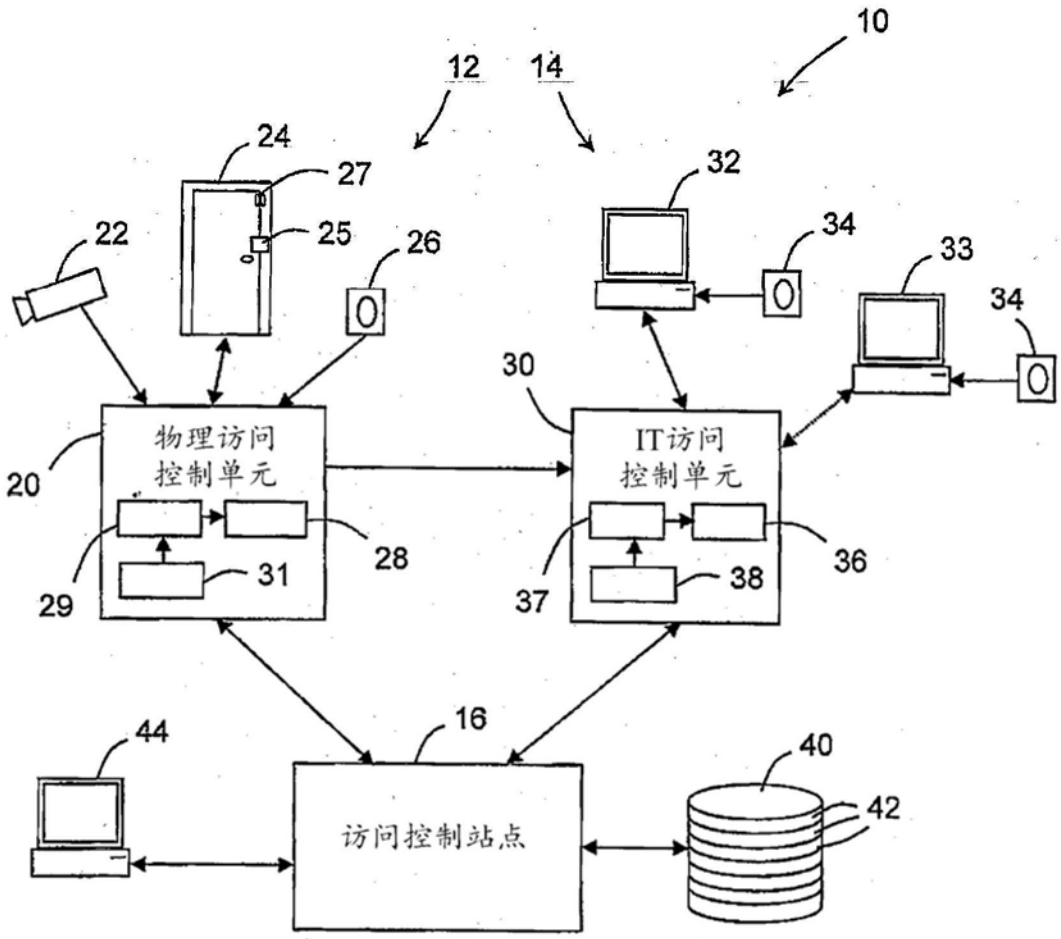

10
12
14
24
27
25
26
22
32
34
33
34
30
物理访问
控制单元
IT访问
控制单元
20
28
29
31
36
37
38
16
44
40
42
访问控制站点

图1

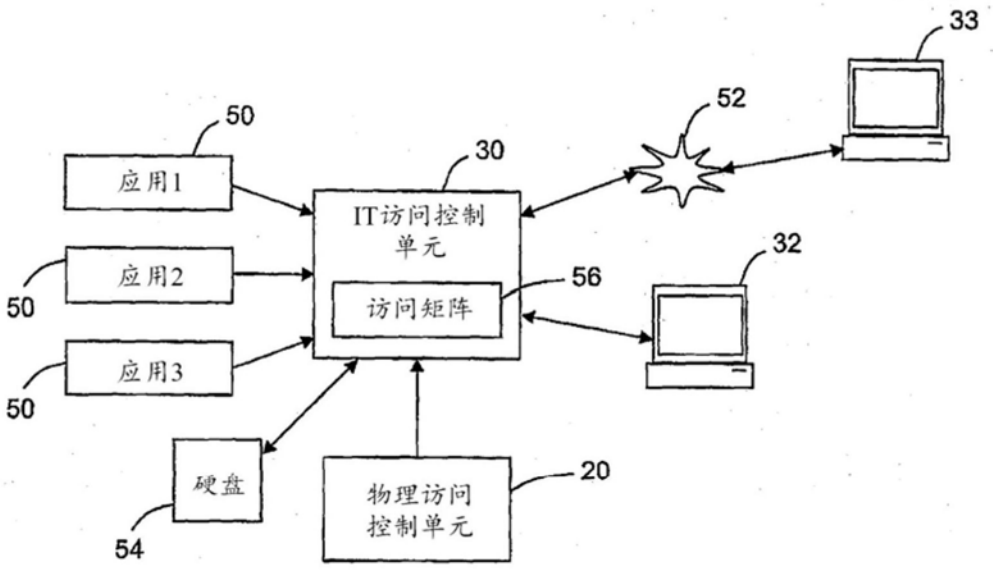
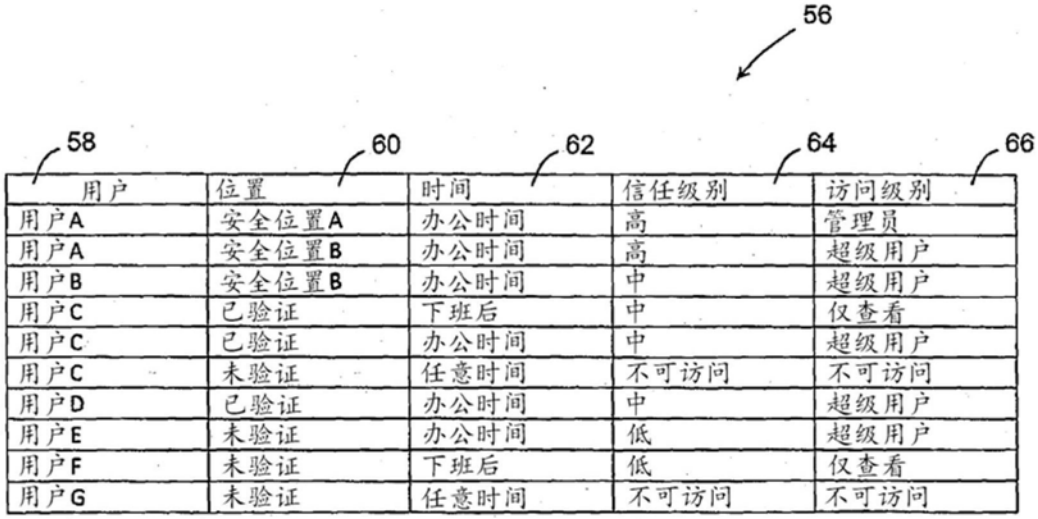

33
50
52
30
应用1
IT访问控制
单元
应用2
50
访问矩阵
56
32
应用3
50
硬盘
物理访问
控制单元
20
54

图2



用户	位置	时间	信任级别	访问级别
用户A	安全位置A	办公时间	高	管理员
用户A	安全位置B	办公时间	高	超级用户
用户B	安全位置B	办公时间	中	超级用户
用户C	已验证	下班后	中	仅查看
用户C	已验证	办公时间	中	超级用户
用户C	未验证	任意时间	不可访问	不可访问
用户D	已验证	办公时间	中	超级用户
用户E	未验证	办公时间	低	超级用户
用户F	未验证	下班后	低	仅查看
用户G	未验证	任意时间	不可访问	不可访问

图3