[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 1/00 (2006.01)
G06F 17/00 (2006.01)
G05B 23/02 (2006.01)

[12] 发明专利说明书

专利号 ZL 200510069681.8

[45] 授权公告日 2008 年 5 月 14 日

[11] 授权公告号 CN 100388155C

[22] 申请日 2005.5.8
[21] 申请号 200510069681.8
[30] 优先权
[32] 2004.5.4 [33] DE [31] 102004022215.0
[73] 专利权人 海德堡印刷机械股份公司
地址 联邦德国海德堡
[72] 发明人 汤姆·厄尔斯内尔
[56] 参考文献
CN1408082A 2003.4.2
CN1183186A 1998.5.27
WO0245378A2 2002.6.6
EP1265150A1 2002.12.11
审查员 石 岗

[74] 专利代理机构 永新专利商标代理有限公司
代理人 曾 立

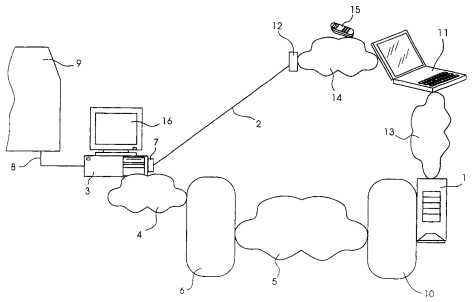
权利要求书 3 页 说明书 8 页 附图 1 页

[54] 发明名称

电子系统及方法

[57] 摘要

本发明涉及用于安全且授权地访问数据或访问至少一个第一计算机(3)的操作表面、以便由至少一个第二计算机(1，11)操作机器的一个电子系统及一种方法。 本发明的特征在于：仅可以由第二计算机(1，11)访问第一计算机(3)的数据或操作表面；第二计算机(1，11)具有一个授权装置，在该授权装置中存储用于有访问权的人员的访问数据；及在访问第一计算机(3)的数据或操作表面以前，在一个与第一计算机(3)连接的显示装置(16)上进行使第二计算机(1，11)的有访问权的及被辨认的人员可被识别的显示。



1.电子系统，具有至少一个第一计算机（3）和至少一个第二计算机（1，11），借助该电子系统可由第二计算机安全且授权地访问第一计算机的数据或操作界面，其特征在于：

第一计算机（3）被配置给一个机器，该第一计算机可通过网络与第二计算机连接；

第二计算机（1，11）具有一个授权装置，在该授权装置中存储用于有访问权的人员的访问数据；

一个显示装置（16）与第一计算机（3）连接，在该显示装置上可显示出第二计算机（1，11）的有访问权的及被辨认的人员的数据，使得该人员可被识别；

并且对于该被辨认的人员可建立在第一计算机与第二计算机之间的网络连接。

2.根据权利要求1的系统，其特征在于：该第二计算机（1，11）与该第一计算机（3）通过互联网（5）相互连接。

3.根据权利要求1或2的系统，其特征在于：该第一计算机（3）与该第二计算机（1，11）通过内联网（4，13）相互连接。

4.根据权利要求1或2的系统，其特征在于：在辨认时在第一计算机（3）的显示装置（16）上显示单一地配置给相应的被辨认人员的护照相片。

5.根据权利要求1或2的系统，其特征在于：在这些计算机（3，1，11）之间数据交换持续期间中，在这些计算机（3，1，11）的至

少一个上存在用于记录所发生的数据交换的存储可能性。

6.根据权利要求1或2的系统，该系统被设置用于与印刷机进行数据通信。

7.根据权利要求1或2的系统，其特征在于：在第一计算机（3）上设有一个操作部件，借助该操作部件可拒绝由第二计算机（1，11）访问第一计算机（3）的数据或操作界面。

8.用于安全且授权地访问至少一个第一计算机（3）的数据或操作界面、以便由至少一个第二计算机（1，11）操作机器的方法，其特征在于：仅可以由第二计算机（1，11）访问第一计算机（3）的数据或操作界面；该第二计算机（1，11）具有一个装置，该装置辨认操作人员及在访问第一计算机（3）的数据或操作界面以前在一个与第一计算机（3）连接的显示装置（16）上显示第二计算机（1，11）的有访问权的及被辨认的人员的数据，使得该人员可被识别。

9.根据权利要求8的方法，其特征在于：仅当第一计算机（3）释放访问时，才可进行第二计算机（1，11）对第一计算机（3）的数据或操作界面的访问。

10.根据以上权利要求中一项的方法，其特征在于：第二计算机（1，11）与第一计算机（3）之间的数据被编码地传输。

11.根据权利要求8或9的方法，其特征在于：操作人员的个人的、被存储的数据不能被该人员自己更改。

12.根据权利要求 11 的方法，其特征在于：操作人员的数据仅可用管理员访问权来改变。

电子系统及方法

技术领域

本发明涉及用于安全且授权地存访问数据或访问至少一个第一计算机的操作界面、以便由至少一个第二计算机操作机器的电子系统及方法。

背景技术

工业中的加工机器必需持续地被维护及检查，以便使磨损及其它缺陷引起的故障时间尽可能地小。此外在现代加工机器中，机器的控制计算机可以通过互联网及内联网与机器制造者的维护计算机连接，以便使工业机器的数据连续地被检验及可能通过互联网及内联网对加工机器进行维护工作。在该情况下维护人员不出现在工业机器运营者公司的现场，而可对机器进行所谓的远程维护及远程诊断。

这种系统已由 DE 101 52 765 A1 公知，该系统用于一个数控工业加工机器的计算机支持的操作及管理。其中加工机器具有一个在机器侧的工作计算机，该工作计算机通过数据通信连接如互联网与制造者或维护公司处的主计算机连接。主计算机能够实时地从加工机的工作计算机调用机器状态数据，将数据传送到主计算机及然后在主计算机上进行分析及评估。接着可再将数据传送回机器侧的工作计算机，以便排除可能的问题，因为由调用的机器状态数据可以实时地识别在数控的工业加工机器上出现的问题并及早地采取相应的对付措施。此外机器状态数据可被这样地评估，以便由主计算机对加工机器提供更好的机器数据。

在这种系统中维护人员的识别及授权起到一个决定性的作用，因为没有一个加工机器的运营者能够接收未被授权者访问他的加工机

器的计算机。因此必需绝对地保证，实际上仅有对加工机器负责的制造者或维护公司可访问加工机器的计算机。因为加工机器的计算机与制造者的主计算机通常通过互联网连接相互通信，因此该通信与所有的来自互联网的已知危险相联系。为了减小该危险，在现有技术中，对加工机器计算机与主计算机的连接使用编码或仅允许确定的计算机访问加工机器的计算机。

此外许多加工机器的运营者希望在其机器的制造者或维护公司那里有一个固定对话的合作人，因为他们谨慎地希望其机器仅由他们信任的确定的人员来维护。

发明内容

本发明的任务在于，避免维护人员匿名地访问加工机器计算机的数据或操作界面，以便提高用户对远程维护及远程诊断的认可程度。

根据本发明，为了解决该任务提出了一种电子系统，具有至少一个第一计算机和至少一个第二计算机，借助该电子系统可由第二计算机安全且授权地访问第一计算机的数据或操作界面，其中，第一计算机被配置给一个机器，该第一计算机可通过网络与第二计算机连接；第二计算机具有一个授权装置，在该授权装置中存储用于有访问权的人员的访问数据；一个显示装置与第一计算机连接，在该显示装置上可显示出第二计算机的有访问权的及被辨认的人员的数据，使得该人员可被识别；并且对于该被辨认的人员可建立在第一计算机与第二计算机之间的网络连接。

根据本发明，还提出了一种用于安全且授权地访问数据或访问至少一个第一计算机的操作界面、以便由至少一个第二计算机操作机器的方法，其特征在于：仅可以由第二计算机访问第一计算机的数据或操作界面；该第二计算机具有一个装置，该装置辨认操作人员及在访问第一计算机的数据或操作界面以前在一个与第一计算机连接的显示装置上显示第二计算机的有访问权的及被辨认的人员的数据，使得

该人员可被识别。

本发明的有利的构型可由下面的措施及附图中得到。在根据本发明的系统中，运营者的机器至少具有一个为该机器配置的第一计算机，该计算机通过网络连接可与制造者或维护及管理公司的至少一个第二计算机通信。一个这样的通信连接例如可通过互联网来建立，其中该连接仅当数据真正由第一计算机向第二计算机或反向地传输时才建立。基本上仅可能是，在第一计算机与第二计算机之间通过互联网建立的连接由第一计算机来激活，因为该第一计算机相对互联网被所谓防火墙保护着，一种安全软件可监视通过互联网的数据通信及尤其可防止未被授权地从外部访问第一计算机。但也可以通过在本申请的其它地方描述的特殊方法由第二计算机启动连接的建立。现在为了避免匿名地访问在机器的第一计算机上的数据，根据本发明提出：仅可以由第二计算机及不能由未被授权的第三计算机访问第一计算机的数据或操作界面；第二计算机具有一个授权装置，在该授权装置中存储用于有访问权的人员的访问数据；及在访问第一计算机的数据或操作界面以前，在一个与第一计算机连接的显示装置上进行使第二计算机的有访问权的及被辨认的人员可被识别的显示。

因此首先保证了，真正地仅可由第二计算机、即完全地由制造者或维护公司的计算机来访问第一计算机的数据，尤其是数据仅传送到这样选择的第二计算机上。因此第三者的计算机不再可以未被授权地访问第一计算机，因为没有数据被传送到它的计算机上。因此第二计算机用作访问第一计算机的过滤器，以使得仅是借助第二计算机被对此授权的人员可访问第一计算机的数据。在一个与第二计算机连接的另一计算机处的维护人员必需对此提出申请。这样一个授权装置例如要求输入一个用户名称及相应操作人员所属的密码。借助这些数据可单一地识别访问的人员及避免匿名地访问。然后这样被辨认的维护人员的数据可在显示装置、例如第一计算机的图象显示屏上被显示出

来，由此机器运营者可在图象显示屏上清楚地识别出哪个人现在真正想访问他的机器数据。

在本发明的一个构型中提出，当辨认时在第一计算机的显示装置上显示单一地配置给被辨认人员的护照相片。因此在个人数据如访问人员的名字的位置上或其附近，机器运营者还可得到访问人员的可视显示。这种显示例如可通过将护照相片作为访问数据的组成部分及被存储在第二计算机上来实现。在访问第一计算机的数据前将该相片及其它识别数据一起传送到该计算机。在第一计算机的图象显示屏上将显示相应的维护人员的名字及相片。这样的相片传送增强了机器运营者的个人对话及进一步减小了不受欢迎的匿名访问。

此外提出，操作人员的个人的、被存储的数据不能被该人员自己更改。由于机器运营者高安全性的要求，重要的是，运营者能确信，传送给他的个人数据、例如待访问的维护人员的名字及其护照相片被单一地配置给该真实的访问人员。出于该原因访问的维护人员也不能自己更改他的数据，否则将打开了作假的大门。操作人员仅可能，用自己的使用名称及其密码或通过其它识别标记在第二计算机上申请及然后进行数据访问。但维护人员不能影响他的个人数据在第一计算机的图象显示屏上的显示，由此操作人员的作假是不可能的。

在本发明的一个特别有利的构型中提出：操作人员的数据仅可用管理员访问权来改变。在一定情况下操作人员的数据必需以一定的时间间隔更新，例如当新维护人员被雇用及被委托维护相应的机器或维护人员的数据由于其它原因改变时。但该数据改变仅可由一个确定的人员，即这两个计算机的系统管理员来进行。并且由此可保证，这个改变操作人员数据的人不与操作人员本身是同一人。这种安全措施还用于：使操作人员数据的作假变难，因为仅是作为管理员的人被允许：单独地对所有维护人员的存储数据的改变负责。

此外还以有利的方式提出，在各个计算机之间数据交换持续期间

中，在至少一个计算机上存在用于记录所发生的数据交换的存储可能性。为了对可能出现的问题或机器运营者的投诉提供一个对数据交换理解的可能性，可在第一计算机上或在第二计算机上或在另一计算机上对其进行记录。因为通过根据本发明的系统还可单一地识别启动交换数据的人员，所记录的数据可单一地被分配给该人员。因此可了解：哪个人在何时刻用何机器交换了什么数据及在该数据交换时出现了什么问题及可能由谁来解决该问题。这不仅可提高机器运营者方面的安全性而且也可提高维护公司生产者方面的安全性，因为数据交换的情况可简单地被了解。

此外可有利地考虑：在第一计算机上设置一个操作部件，借助该操作部件可拒绝由第二计算机访问第一计算机的数据。当个人数据在运营者的第一计算机的图象显示屏上显示后，运营者本身能够借助一个操作部件禁止对其的计算机访问。如果该运营者譬如确定出，一个他不认识的人或一个对于维护他的机器未被授权的人想访问他的机器的第一计算机，则他可根据单一配置的名字及护照相片立即识别出来及通过操作部件拒绝维护访问。由此该人员对他的计算机数据的访问首先被一次地阻止。但该构型还可进一步扩展，即该机器的运营者将禁止被他拒绝的人员继续访问他的计算机，以使得被他拒绝的人在将来也不能再访问他的计算机。根据本发明的系统及根据本发明的方法高度地考虑到运营者的愿望，即他自己有权支配对他计算机的访问及任何时候均能识别：到底谁想访问他的计算机。尽管这样仍可作到：维护人员任何时候可起动维护访问及不被约束在固定的维护时间间隔中。

附图说明

以下将借助一个附图来详细地描述及解释本发明。

图 1 表示一个管理及诊断系统，它具有在印刷机运营者处的第一计算机及在印刷机制造者处规定用于管理的两个计算机。

具体实施方式

按照该图，根据本发明的系统用于当管理及诊断一个印刷机 9 时询问数据或访问操作界面。该印刷机 9 通过连接导线 8 与一个第一计算机 3 连接，该计算机位于印刷机 9 的运营者处。该第一计算机 3 可以同时为印刷机 9 的控制计算机及合乎目的地具有一个图象显示屏 16。根据该图，第一计算机 3 能够通过设置在印刷机 9 的运营者空间中的第一内联网 4 及互联网 5 建立一个用于向一个第二计算机 1 传输数据的连接，该第二计算机放置在印刷机制造者的空间中。该第一计算机 3 及第二计算机 1 被这样地编程，以使得第一计算机 3 的数据仅可由第二计算机 1 接收。这用于防止由未被授权者访问第一计算机 3 的数据。在印刷机制造者处的另一计算机 11 通过第二内联网 13 与第二计算机 1 相连接，维护人员可通过该计算机 11 对印刷机 9 进行远程管理。因此每个有权管理的人员在成功的识别后，可通过他们膝上型计算机 11、第二内联网连接部分 13 及第二计算机 1 访问第一计算机 3 的数据。

根据该图，此外第一内联网 4 相对互联网 5 借助一个防火墙 6 来保安，以防止未被授权者侵入印刷机 9 的运营者的第一内联网 4。因为该防火墙 6 基本上也可防止第二计算机 1 通过互联网 5 访问第一计算机 3，对第一计算机 3 的数据的访问总是由第一计算机 3 来启动。在此情况下连接的建立由第一计算机通常通过操作人员的本机输入来引起，其方式是按压一个维护按钮。在另一实施形式中由第一计算机向第二计算机 1 连接的建立可在任何时间上从远程引起，当第一计算机 3 设有一个调制解调器 7 并连接到电话网 2 上。该调制解调器 7 被这样地设计，即当收到确定的振铃信号时即引起了从第一计算机 3 向第二计算机 1 的连接建立，但无数据通过电话网 2 传输，因为在接收到振铃信号后电话连接又被中断。借助该振铃信号待访问的维护人员首先被识别为所属的维护公司。在此情况下振铃信号的发送可或由

维护人员的计算机 11 通过一个集成在计算机 11 中的调制解调器来实现，或通过任一其它的电话来实现，该电话的号码作为授权的振铃信号来释放，用于引起从第一计算机 3 向第二计算机 1 建立连接。根据该图，振铃信号也可由一个被许可的移动电话 15 通过无线电移动通信连接部分 14 及一个移动电话台 12 继续传输到电话网 2 中。也可替换地，膝上型计算机 11 可设有作为无线电移动通信调制解调器的 GSM 无线电移动通信卡及由此通过无线电移动通信连接部分 14 向计算机 3 的调制解调器 7 传送振铃信号。因此用于从第一计算机向第二计算机传输数据的连接建立仅可由管理公司的电话连接引起而不能由未被授权的第三者引起。该第二计算机 1 由另一防火墙 10 相对互联网 5 进行保护。

但在维护人员可从其计算机 11 调用数据以前，该维护人员首先必需在计算机 11 上进入一个维护入口的软件。为此该人员必需至少输入其用户名称及所配置的密码。根据本发明对该人员要求严格的认证，其特征是使用由标识卡产生的一次性口令。此外在膝上型计算机 11 上还可设有一个指纹阅读器或一个用于虹膜识别的摄象机，以便防伪地对维护人员进行辨认。在此情况下该维护人员的数据被存储在第二计算机 1 中，以致基本上可由与第二计算机 1 相连接的、及设有维护入口软件的每个计算机 11 来进行辨认及接着的数据询问或访问操作界面。

当成功地进行了人员识别及通过电话网 2 成功地启动了数据调用后，在真正的数据调用发生前，首先将待访问的维护人员的个人数据从第二计算机 1 通过互联网 5 传送给第一计算机 3。在第一计算机 3 的图象显示屏 16 上首先看到维护人员的名字，其中最好也显示维护人员的护照相片。因此印刷机 9 的运营者可毫无疑问地识别出哪个人刚才想在其计算机 3 上取数。在印刷机 9 的制造者与运营者之间的维护合同中例如可约定：仅可由确定的人员来维护该印刷机 9。如果运

营者在图象显示屏 16 上看到一个他不认识的人或他不欢迎的人，则他可通过其计算机 3 的键盘阻止对他的数据及操作界面的访问及拒绝该不受欢迎的人。根据本发明的系统或可被这样地编程，即在对不受欢迎的人的一次拒绝后还允许该人员访问第一计算机 3 的有限次数的尝试。但替换地，该维护入口也可被这样地编程，即被拒绝过一次的一个人员在以后将被禁止对第一计算机 3 的继续地访问。因此印刷机 9 的运营者始终了解哪个人刚才想访问他的计算机 3 及他可拒绝不受欢迎的人员。

参考标号表：

1. 第二计算机
2. 电话网
3. 第一计算机
4. 第一内联网
5. 互联网
6. 防火墙
7. 调制解调器
8. 连接导线
9. 印刷机
10. 另一防火墙
11. 膝上型计算机
12. 移动电话台
13. 第二内联网
14. 无线电移动通信连接部分
15. 移动电话
16. 图象显示屏

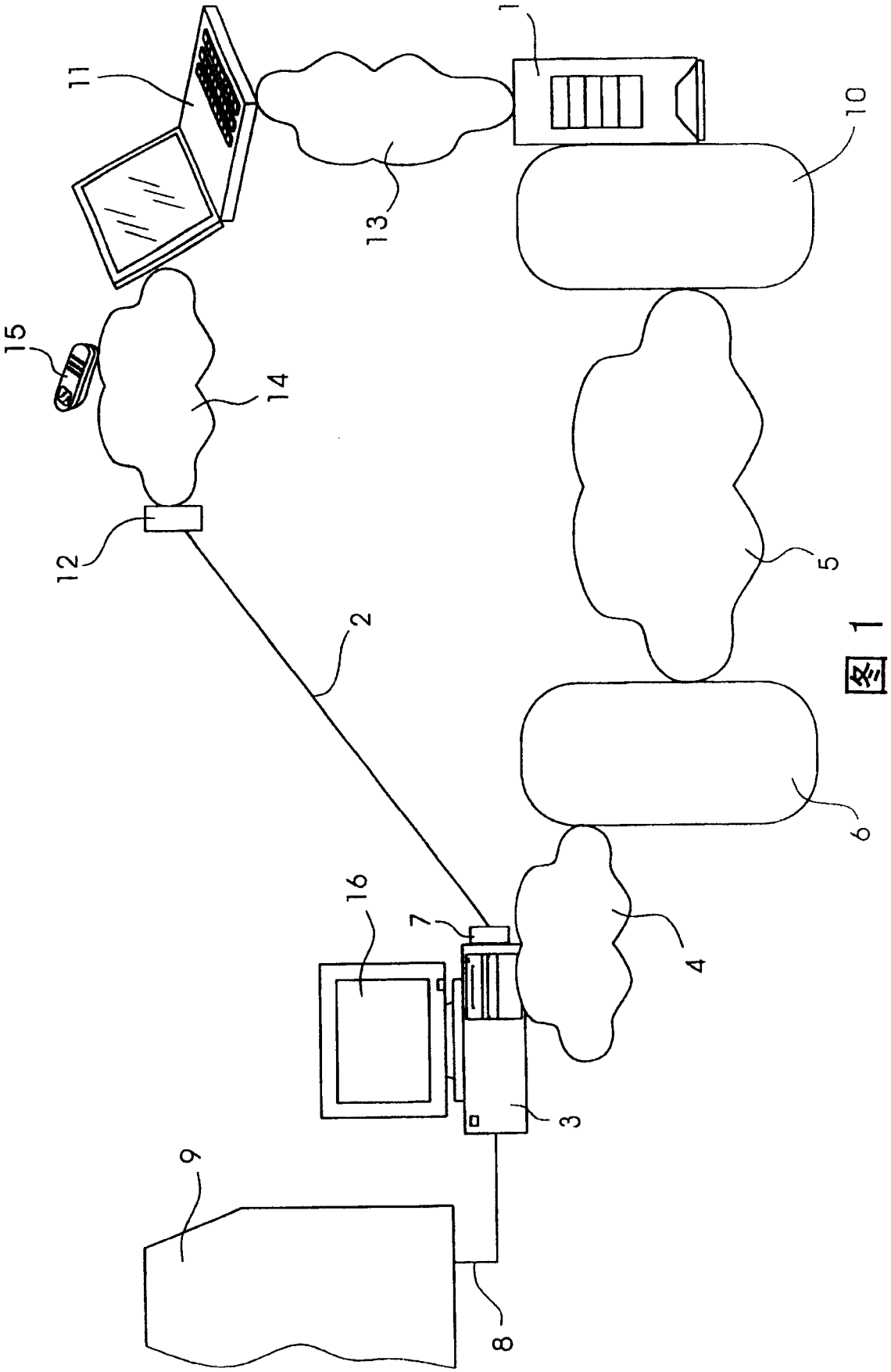


图 1