(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 103620581 B
(45)授权公告日 2017.06.06

(21)申请号 201280021230.5

(22)申请日 2012.02.29

(65)同一申请的已公布的文献号
申请公布号 CN 103620581 A

(43)申请公布日 2014.03.05

(30)优先权数据
13/038299 2011.03.01 US

(85)PCT国际申请进入国家阶段日
2013.10.31

(86)PCT国际申请的申请数据
PCT/US2012/027158 2012.02.29

(87)PCT国际申请的公布数据
WO2012/118905 EN 2012.09.07

(73)专利权人 赛门铁克公司
地址 美国加利福尼亚州

(72)发明人 P.迪科波 S.S.萨万特 S.考夫曼 A.D.加林德斯 S.贾伊斯瓦尔 A.阿加瓦尔

(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 王岳 王忠忠

(51)Int.Cl.
G06F 15/177(2006.01)

(56)对比文件

US 7480640 B1,2009.01.20,说明书第1栏第18-24行,第5栏第55-65行,第15栏第11-16行和第18栏第10-17行.

US 2009/0228499 A1,2009.09.10,说明书第[0055],[0059]-[0064]和[0067]段.

CN 101303730 A,2008.11.12,全文.

US 7480640 B1,2009.01.20,说明书第1栏第18-24行,第5栏第55-65行,第15栏第11-16行和第18栏第10-17行.

A.Al-Anazi等.A support vector machine algorithm to classify lithofacies and model permeability in heterogeneous reservoirs.《Engineering Geology》.2010,第114卷(第3-4期),第267-277页.

王德鹏等.一种Agent普适机器学习分类器在Smart-It中的应用.《电脑知识与技术》.2009,第5卷(第31期),第8761-8764页.

审查员 闫伟姣

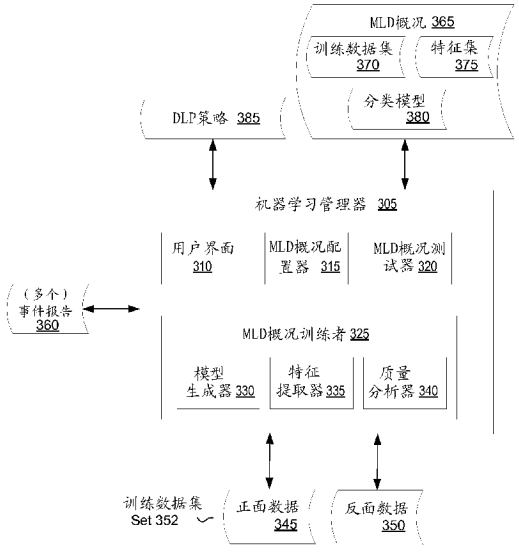
权利要求书4页 说明书12页 附图12页

(54)发明名称

用于执行机器学习的用户界面和工作流

(57)摘要

一种计算装置经由用户界面接收训练数据集,所述训练数据集包括多个敏感数据的正例和多个敏感数据的反例。计算装置通过使用机器学习来分析所述训练数据集以便训练基于机器学习的检测(MLD)的概况,MLD概况将用于将新数据分类为敏感数据或非敏感数据。计算装置在所述用户界面中显示针对所述MLD概况的质量度量。



CN 103620581 B

1.一种为数据丢失防护系统产生基于机器学习的检测概况的方法,包括:

经由用户界面接收训练数据集,所述训练数据集包括多个敏感数据的正例和多个敏感数据的反例;

经由所述用户界面接收存储器分配的用户选择;

通过使用机器学习来分析所述训练数据集以便训练基于机器学习的检测概况,所述基于机器学习的检测概况将用于将新数据分类为敏感数据或非敏感数据;以及

在所述用户界面中显示针对所述基于机器学习的检测概况的质量度量,所述质量度量包括存储器利用率,其中针对类别数据的所述存储器利用率符合所述存储器分配。

2.根据权利要求1所述的方法,其中,分析所述训练数据集包括:

在所述训练数据集上执行特征提取以生成特征集,所述特征集包括正例的特征和反例的特征;

从所述训练数据集生成分类模型;以及

计算所述质量度量,其中所述质量度量包括假正面率、假反面率或存储器利用率中的至少一种。

3.根据权利要求2所述的方法,还包括:

如果所述假正面率在假正面阈值内并且所述假反面率在假反面阈值内,就能够实现配置操作;

经由所述用户界面接收执行所述配置操作的用户请求;以及

响应于接收所述用户请求,将所述基于机器学习的检测概况添加到数据丢失防护系统的数据丢失防护策略中。

4.根据权利要求2所述的方法,还包括:

在所述用户界面中,从所述训练数据集识别引起假正面的数据和引起假反面的数据中的至少一种。

5.根据权利要求1所述的方法,还包括:

接收针对敏感数据的正例和针对敏感数据的反例的类别信息;以及

在用户界面中识别添加到训练数据集的数据类别来改进所述质量度量。

6.根据权利要求1所述的方法,还包括:

如果所述质量度量不能满足质量阈值,则响应于用户输入来修改所述训练数据集;

分析修改的训练数据集以重新训练所述基于机器学习的检测概况;以及

在所述用户界面中显示针对所述基于机器学习的检测概况的新质量度量。

7.根据权利要求1所述的方法,其中,

通过数据丢失防护系统的数据丢失防护策略收集所述训练数据集,所述多个敏感数据的反例包括由所述数据丢失防护策略错误分类为敏感文档的文档,所述方法还包括:

将所述基于机器学习的检测概况配置到所述数据丢失防护策略中。

8.根据权利要求1所述的方法,还包括:

经由所述用户界面接收针对所述基于机器学习的检测概况的敏感性阈值的选择;并且

基于所述选择控制针对所述基于机器学习的检测概况的敏感性阈值设置。

9.一种用于为数据丢失防护系统产生基于机器学习的检测概况的设备,包括:

用于经由用户界面接收训练数据集的装置,所述训练数据集包括多个敏感数据的正例

和多个敏感数据的反例；

用于经由所述用户界面接收存储器分配的用户选择的装置；

用于通过使用机器学习来分析所述训练数据集以便训练基于机器学习的检测概况的装置，基于机器学习的检测概况将用于将新数据分类为敏感数据或非敏感数据；以及

用于在所述用户界面中显示针对所述基于机器学习的检测概况的质量度量的装置，所述质量度量包括存储器利用率，其中针对类别数据的所述存储器利用率符合所述存储器分配。

10.根据权利要求9所述的设备，其中，分析所述训练数据集包括：

在所述训练数据集上执行特征提取以生成特征集，所述特征集包括正例的特征和反例的特征；

从所述训练数据集生成分类模型；以及

计算所述质量度量，其中所述质量度量包括假正面率、假反面率或存储器利用率中的至少一种。

11.根据权利要求10所述的设备，所述设备还包括：

用于如果所述假正面率在假正面阈值内并且所述假反面率在假反面阈值内，使配置操作实现的装置；

用于经由所述用户界面接收执行所述配置操作的用户请求的装置；以及

用于响应于接收所述用户请求，将所述基于机器学习的检测概况添加到数据丢失防护系统的数据丢失防护策略中的装置。

12.根据权利要求10所述的设备，所述设备还包括：

用于在所述用户界面中，从所述训练数据集识别引起假正面的数据和引起假反面的数据中的至少一种的装置。

13.根据权利要求9所述的设备，所述设备还包括：

用于接收针对敏感数据的正例和针对敏感数据的反例的类别信息的装置；以及

用于在用户界面中识别添加到训练数据集的数据类别来改进所述质量度量的装置。

14.根据权利要求9所述的设备，所述设备还包括：

用于如果所述质量度量不能满足质量阈值，则响应于用户输入来修改所述训练数据集的装置；

用于分析修改的训练数据集以重新训练所述基于机器学习的检测概况的装置；以及

用于在所述用户界面中显示针对所述基于机器学习的检测概况的新质量度量的装置。

15.根据权利要求9所述的设备，其中，

通过数据丢失防护系统的数据丢失防护策略收集所述训练数据集，所述多个敏感数据的反例包括由所述数据丢失防护策略错误分类为敏感文档的文档，所述设备还包括：

用于将所述基于机器学习的检测概况配置到所述数据丢失防护策略中的装置。

16.根据权利要求9所述的设备，所述设备还包括：

用于经由所述用户界面接收针对所述基于机器学习的检测概况的敏感性阈值的选择的装置；并且

用于基于所述选择控制针对所述基于机器学习的检测概况的敏感性阈值设置的装置。

17.一种用于为数据丢失防护系统产生基于机器学习的检测概况的系统，包括：

通信耦合到网络的一个或多个处理器;其中所述一个或多个处理器被配置成:

经由用户界面接收训练数据集,所述训练数据集包括多个敏感数据的正例和多个敏感数据的反例;

经由所述用户界面接收存储器分配的用户选择;

通过使用机器学习来分析所述训练数据集以便训练基于机器学习的检测概况,基于机器学习的检测概况将用于将新数据分类为敏感数据或非敏感数据;以及

在所述用户界面中显示针对所述基于机器学习的检测概况的质量度量,所述质量度量包括存储器利用率,其中针对类别数据的所述存储器利用率符合所述存储器分配。

18.根据权利要求17所述的系统,其中,

分析所述训练数据集包括:

在所述训练数据集上执行特征提取以生成特征集,所述特征集包括正例的特征和反例的特征;

从所述训练数据集生成分类模型;以及

计算所述质量度量,其中所述质量度量包括假正面率、假反面率或存储器利用率中的至少一种。

19.根据权利要求18所述的系统,其中所述一个或多个处理器还被配置成:

在所述用户界面中,从所述训练数据集识别引起假正面的数据和引起假反面的数据中的至少一种。

20.根据权利要求17所述的系统,其中,

通过数据丢失防护系统的数据丢失防护策略收集所述训练数据集,所述多个敏感数据的反例包括由所述数据丢失防护策略错误分类为敏感文档的文档,其中所述一个或多个处理器还被配置成:

将所述基于机器学习的检测概况配置到所述数据丢失防护策略中。

21.根据权利要求17所述的系统,其中所述一个或多个处理器还被配置成:

经由所述用户界面接收针对所述基于机器学习的检测概况的敏感性阈值的选择;并且

基于所述选择控制针对所述基于机器学习的检测概况的敏感性阈值设置。

22.一种为数据丢失防护系统产生基于机器学习的检测概况的方法,包括:

经由用户界面接收训练数据集,所述训练数据集包括多个敏感数据的正例和多个敏感数据的反例;

通过使用机器学习来分析所述训练数据集以便训练基于机器学习的检测概况,所述基于机器学习的检测概况将用于将新数据分类为敏感数据或非敏感数据;

在所述用户界面中显示针对所述基于机器学习的检测概况的质量度量;以及

如果所述质量度量不能满足质量阈值,则执行下列,包括:

响应于用户输入来修改所述训练数据集;以及

分析修改的训练数据集以重新训练所述基于机器学习的检测概况。

23.一种为数据丢失防护系统产生基于机器学习的检测概况的设备,包括:

用于经由用户界面接收训练数据集的部件,所述训练数据集包括多个敏感数据的正例和多个敏感数据的反例;

用于通过使用机器学习来分析所述训练数据集以便训练基于机器学习的检测概况的

部件，所述基于机器学习的检测概况将用于将新数据分类为敏感数据或非敏感数据；

用于在所述用户界面中显示针对所述基于机器学习的检测概况的质量度量的部件；以及

用于如果所述质量度量不能满足质量阈值则执行下列步骤的部件，所述步骤包括：

响应于用户输入来修改所述训练数据集；以及

分析修改的训练数据集以重新训练所述基于机器学习的检测概况。

24.一种计算装置，包括：

存储器，存储用于机器学习管理器的指令；以及

处理装置，执行所述指令，其中所述指令使所述处理装置：

为所述机器学习管理器提供用户界面；

经由所述用户界面接收训练数据集，所述训练数据集包括多个敏感数据的正例和多个敏感数据的反例；

通过使用机器学习来分析所述训练数据集以便训练基于机器学习的检测概况，所述基于机器学习的检测概况将用于将新数据分类为敏感数据或非敏感数据；

在所述用户界面中显示针对所述基于机器学习的检测概况的质量度量；以及

如果所述质量度量不能满足质量阈值，则执行下列，包括：

响应于用户输入来修改所述训练数据集；以及

分析修改的训练数据集以重新训练所述基于机器学习的检测概况。

用于执行机器学习的用户界面和工作流

技术领域

[0001] 本发明的实施例涉及数据丢失防护的领域，且更特别地涉及提供使用户能够生成和配置基于机器学习的检测(MLD)概况的界面的数据丢失防护(DLP)系统。

背景技术

[0002] 许多组织实施数据丢失防护(DLP)系统来识别和控制对敏感数据的访问。典型的DLP系统通过包括描述技术和指纹识别技术的深度内容检查和分析来保护敏感数据。描述技术通过识别对关键词、表达式或图案和文件类型的匹配并且通过执行其它基于签名的检测技术来保护敏感数据。指纹识别技术通过识别对整体或部分文件的确切匹配来保护敏感数据。虽然有效保护了组织的敏感数据中的许多，但是当解决大量的非结构化数据和知识产权(诸如产品配方、源代码以及销售与市场报告时，指纹识别技术和描述技术具有局限性。

[0003] 为了更精确地保护敏感的非结构化数据，一些DLP系统正在探索向量机器学习(VML，vector machine learning)技术的使用。然而，实施VML是非常复杂的。因此，使用VML的当前DLP系统需要VML专家来设计针对顾客的基于机器学习的检测(MLD)概况。装载到顾客的DLP系统则具有顾客不能够修改的预先定义的MLD概况。这种DLP系统不提供使用户能够生成他们自身MLD概况的任何用户界面或工作流。

发明内容

[0004] 在一个实施例中，计算装置经由针对机器学习(ML)的用户界面接收训练数据集，所述训练数据集包括敏感数据的正例和敏感数据的反例。计算装置通过使用机器学习来分析所述训练数据集以便训练MLD概况，所述MLD概况可以用于将新数据分类为敏感数据或非敏感数据。计算装置在所述用户界面中显示针对所述MLD概况的质量度量。在一个实施例中，所述MLD概况包括统计数据分类模型和特征集，所述特征集包括正例的统计上显著特征和反例的统计上显著特征，并且所述质量度量包括假正面率、假反面率和存储器利用率中的至少一种。在一个实施例中，所述计算装置在所述用户界面中从所述训练数据集识别引起假正面的数据和引起假反面的数据中的至少一种。

[0005] 在一个实施例中，所述计算装置在分析所述训练文档集之前，经由所述用户界面接收存储器分配的用户选择，其中针对类别数据的所述存储器利用率符合所述存储器分配。在一个实施例中，如果所述假正面率在假正面阈值内并且所述假反面率在假反面阈值内，计算装置就能够实现配置操作。响应于接收配置操作的用户请求，计算装置将所述MLD概况添加到DLP系统的数据丢失防护(DLP)策略中。

[0006] 在一个实施例中，所述计算装置接收针对敏感数据的正例和针对敏感数据的反例的类别信息。所述计算装置然后可以在用户界面中识别添加到训练数据集的数据类别来改进所述质量度量。在一个实施例中，如果所述质量度量不能满足质量阈值，则所述计算装置就响应于用户输入来修改所述训练数据集。所述计算装置然后分析修改的训练数据集以重

新训练所述MLD概况并且在所述用户界面中显示针对所述MLD概况的新质量度量。

[0007] 在一个实施例中，通过DLP系统的数据丢失防护(DLP)策略收集所述训练数据集，所述多个敏感数据的反例包括由所述DLP策略错误分类为敏感文档的文档。在该实施例中，所述计算装置然后可以将所述MLD概况配置到所述DLP策略中。

[0008] 在一个实施例中，计算机可读存储介质包括指令，所述指令将使执行指令的处理器：经由针对机器学习的用户界面来接收包括多个敏感数据的正例和多个敏感数据的反例的训练数据集。所述处理器然后通过使用机器学习来分析所述训练数据集以便训练基于机器学习的检测(MLD)概况，所述基于机器学习的检测(MLD)概况可以用于将新数据分类为敏感数据或非敏感数据并且在所述用户界面中显示针对所述MLD概况的质量度量。

[0009] 在一个实施例中，一种用于生成MLD概况的方法包括：经由针对机器学习的用户界面来接收包括多个敏感数据的正例和多个敏感数据的反例的训练数据集；通过使用机器学习来分析所述训练数据集以便训练基于机器学习的检测(MLD)概况，所述基于机器学习的检测(MLD)概况可以用于将新数据分类为敏感数据或非敏感数据；以及在所述用户界面中显示针对所述MLD概况的质量度量。

附图说明

[0010] 根据以下给出的详细说明并且根据本发明各种实施例的附图，将更充分地理解本发明。

[0011] 图1图示了根据本发明一个实施例的示例性系统架构。

[0012] 图2是根据本发明一个实施例的数据丢失防护代理的框图。

[0013] 图3是根据本发明一个实施例的机器学习管理器的框图。

[0014] 图4是图示用于生成和配置MLD概况的方法的一个实施例的流程图。

[0015] 图5至8图示了根据本发明实施例的用于生成和配置MLD概况的用户界面的各种视图。

[0016] 图9是示出根据本发明一个实施例的在MLD概况生成期间的ML管理器的不同状态的状态图。

[0017] 图10是图示用于生成MLD概况并且配置MLD概况到现存的策略中的方法的一个实施例的流程图。

[0018] 图11是图示用于通过使用包括MLD概况的DLP策略来保护计算装置免于数据丢失的方法的一个实施例的流程图。

[0019] 图12是可以执行本文描述的一个或多个操作的示例性计算机系统的框图。

具体实施方式

[0020] 描述了一种用于生成、配置和管理针对数据丢失防护(DLP)系统的基于机器学习的检测(MLD)概况的系统和方法。在本发明的实施例中，该系统和方法提供了一种使(不是向量机器学习专家的)用户能够生成MLD概况的用户界面和工作流。这减少了配置针对DLP的MLD概况的花费，并且改进了MLD概况的可配置性。此外，这使MLD概况能够通过DLP管理器连续地改进。

[0021] 在以下的说明书中，阐述了众多细节。然而，对从本公开内容受益的本领域技术人

员显而易见的是，在没有这些具体细节的情况下也可以实施本发明。在某些情况下，以框图形式示出(而不是详细示出)众所周知的结构和装置，以便避免使本发明晦涩。例如，以下的说明书提供了针对在端点DLP系统中使用MLD概况的细节。然而，对本领域技术人员而言清晰的是，本发明的实施例还适用于使DLP系统联网并且发现了DLP系统(可以扫描存储装置以识别和/或分类敏感数据的DLP系统)。例如，在本发明的实施例中，可以生成MLD概况用于检测通过企业网络移动的敏感数据。

[0022] 根据对计算机存储器内数据位操作的算法和符号表示，呈现了以下的详细说明的一些部分。这些算法说明和表示是数据处理领域的普通技术人员使用的手段，以便最有效地将他们工作的实质传达给本领域的其它技术人员。算法在本文中且一般地构思为导致期望结果的自我一致的步骤序列。这些步骤是需要物理量的物理操控的步骤。通常，尽管不是必要的，但是这些量采用能够存储、转移、组合、比较以及以其它方式操控的电信号或磁信号的形式。主要出于通常使用的原因，已经多次证明将这些信号称为位、值、元素、符号、字符、术语、数字等等是方便的。

[0023] 然而，应该考虑到所有这些术语与类似术语都与适当的物理量相关联，并且仅是适用于这些量的方便的标签。除非根据以下讨论明显另有特别说明，否则应该领会的是，贯穿通篇说明书，利用诸如“接收”、“分析”、“显示”、“启动”、“识别”、“修改”等术语的讨论指的是计算机系统或类似电子计算装置的动作和过程，所述计算机系统和类似电子计算装置操控如计算机系统的寄存器和存储器内的物理(例如，电子)量表示的数据，并且将如计算机系统的寄存器和存储器内的物理(例如，电子)量表示的数据变换为类似表示为计算机系统存储器或寄存器或其它这种信息存储、传输或显示装置内的物理量的其它数据。

[0024] 本发明还涉及用于执行本文操作的设备。该设备可以针对需要的目的而特殊地构造，或者该设备可以包括由存储在计算机中的计算机程序选择性激活或重新配置的通用计算机。这种计算机程序可以存储在计算机可读存储介质中，诸如但不限于，包括软盘、光盘、CD-COM和磁光盘中任何类型的盘、只读存储器(ROM)、随机存取存储器(RAM)、EPROM、EEPROM、磁卡或光卡、或适于存储电子指令的任何类型的介质。

[0025] 图1图示了根据本发明一个实施例的示例性系统架构100。该系统构架100包括联网到端点服务器115的多个端点装置102A至102C，从而依次联网到强制执行服务器(enforcement server)120。

[0026] 每个端点装置都可以是个人计算机(PC)、膝上型计算机、移动电话、平板计算机或者可以由用户访问的任何其它计算装置。每个端点装置102A至102C具有多个不同的数据丢失向量。每个数据丢失向量都是通过其数据可以从端点装置转移出的路径。数据丢失向量的示例包括烧录(burning)文件到光盘、复制数据到便携式驱动器(例如，便携式通用串行总线(USB)驱动器)、打印数据到打印机、通过传真机发送数据、发送电子邮件、发送即时消息、执行打印屏幕操作等等。

[0027] 端点装置102A至102C中的每个都运行管理端点装置的硬件和软件的操作系统(OS)。OS可以例如是Microsoft® Window®、Linux®、Symbian®、Apple®的OS X®、Solaris®等等。一种或多种应用运行在OS上，并且各种操作，所述各种操作包括访问、移动、或以其它方式操控存在于数据存储器(包括在端点装置中、直接附接到端点装置上或联网到端点装置)中的数据。例如，应用可以包括CD或DVD烧录应用、电子邮件应用、网页浏览器、

即时消息应用、打印应用、打印屏幕功能等等。在一个实施例中，响应于接收用户指令，应用执行操作。

[0028] 每个端点装置102A至102C都可以连接到可以是硬盘驱动器、磁带备份、光驱动器、易失性存储器(例如，随机存取存储器(RAM))或其它存储装置的数据存储器135A至135C上。数据存储器135A至135C可以在端点装置102A至102C内部或端点装置102A至102C外部。在一个实施例中，数据存储器135A至135C可以组合到诸如存储区域网络(SAN)或网络附接存储器(NAS)等网络存储器中。在一个实施例中，数据存储器135A至135C可以组合到诸如关系数据库(relational database)之类的网络数据库中。数据存储器135A至135C可以包含包括敏感信息的数据。数据可以包括文件(例如，文档)、表格或其它数据格式。敏感信息的示例包括源代码、患者健康信息、保险索赔、产品配方、法律文档、并购文档、销售与市场报告、社会保险号码、信用卡号码等等。

[0029] 每个端点装置102A至102C都包括监控数据丢失向量的DLP代理106以确保敏感(例如，机密)信息不离开端点装置用于非法目的。当DLP代理106通过数据丢失向量移动时，和/或当接收到通过数据丢失向量发送数据的请求时，DLP代理106可以扫描数据。当DLP代理106检测到通过数据丢失向量移动的数据或通过数据丢失向量移动数据的请求时，DLP代理106实施DLP策略110以确定数据是否是敏感数据(包括敏感信息)。DLP策略110可以规定待监控的内容类型(例如，消息、显示的数据、存储的文档，等等)，怎样识别敏感数据和/或当检测到敏感数据时待执行的动作。在一个实施例中，DLP策略110包括MLD概况112。DLP代理106包括通过使用MLD概况112来处理数据的机器学习(ML)模块108。通过使用MLD概况112来处理数据，ML模块108确定数据是否是敏感数据。

[0030] 对于一些类型的DLP检测技术而言，DLP代理106将数据发送到端点服务器115，并且包括在端点服务器115中的全局DLP检测引擎122确定是否数据包括敏感信息。一旦全局DLP检测引擎122确定文件还是其它数据包含敏感信息，端点服务器115就将消息发送回DLP代理106，从而陈述是否数据是敏感数据。如果数据包含机密信息，则DLP代理106可以执行一个或多个动作以强制执行DLP策略110。在一个实施例中，全局DLP检测引擎122包括ML模块108和DLP策略126(包括MLD概况128)。DLP策略128和MLD概况128可以不同于DLP策略110和MLD概况112。

[0031] 在一个实施例中，端点服务器115充当关于违反DLP策略的数据聚合器(例如，事件报告的聚合器)。端点服务器115可以从每个端点装置102A至102C收集这种数据，并且将收集的数据报告给强制执行服务器120以用于分析。

[0032] 强制执行服务器120管理DLP策略。这可以包括生成并且修改DLP策略(例如，基于管理员输入)。强制执行服务器120然后可以将DLP策略传播到端点服务器115和/或端点装置102A 至 102C 。此外，强制执行服务器120可以生成DLP应答规则，该DLP应答规则还可以传播到端点服务器115和/或端点装置102A 至 102C 。DLP应答规则指明当违反DLP策略时端点装置102A 至 102C 和/或端点服务器115采取的动作。端点装置可以采取的动作的示例包括：将通知发送到管理员、防止数据通过数据丢失向量退出端点装置102A至102C、将端点装置锁定使得没有数据可以通过任何数据丢失向量移动出端点装置、当数据移动出端点装置时对数据进行加密等等。

[0033] 在一个实施例中，强制执行服务器120包括机器学习(ML)管理器130。ML管理器130

提供针对用户的用户界面和工作流，以生成并配置MLD概况。参照附图3在下文中更详细地描述ML管理器130。

[0034] 图2是根据本发明一个实施例的数据丢失防护代理205的框图。DLP代理205可以监控不同的数据丢失向量、应用、数据，等等，以便检测尝试使数据移动出端点装置的操作。用户发起的操作可以包括例如：保存或访问端点装置的任何存储装置上的受限数据库数据、使用应用中的受限数据库数据、打印机密数据、使用网络通信协议中的机密数据。

[0035] DLP代理205可以包括一个或多个策略违反检测器，每个策略违反检测器都可以处理不同的DLP策略250和/或DLP策略250内的不同概况255、260、265以识别并且保护敏感数据。DLP策略250可以包括可以指示增加的数据丢失风险的标准。如果满足包括在DLP策略250中的一个或多个标准，则违反DLP策略250。标准的示例包括：用户状态(例如，是否用户具有对文件的访问特权)、文件位置(例如，待复制文件是否存储在机密数据库中)、文件内容(例如，是否文件包括敏感信息)、时间(例如，是否在正常营业时间期间请求操作)、数据丢失向量、尝试操作的申请等等。

[0036] DLP策略250可以包括一个或多个概况255、260、265。每个概况都可以用于识别敏感数据。在一个实施例中，DLP策略250包括描述内容匹配(DCM)概况255。DCM概况255定义一个或多个关键词和/或待搜索的正则表达式(regular expression)。例如，通过使用正则表达式，DCM概况255可以定义社会保险号码。通过使用DCM策略255，DLP代理205确定是否包括在已扫描数据中的任何信息与关键词和/或正则表达式匹配。如果发现匹配，则可以确定数据包括敏感信息。

[0037] 在一个实施例中，DLP策略250包括确切数据匹配(EDM)概况和/或索引文档匹配(IDM)概况260。确切数据匹配(EDM)可以用于保护诸如数据库记录之类的典型结构化格式的数据。索引文档匹配(IDM)可以用于保护诸如Microsoft®Word或PowerPoint®文档或CAD制图之类的非结构化数据。对于EDM和IDM而言，敏感数据首先由希望保护数据的组织识别，并且然后采集指纹以用于精确、不间断的检测。在一个实施例中，采集指纹过程包括：访问并提取文本和数据、使文本和数据正规化，并且通过使用不可逆散列来保护文本和数据。当扫描文件或其它数据时，指纹(例如，散列)根据该文件或该文件的内容生成，并且与存储的指纹进行比较。如果发现匹配，则扫描的文件识别为包含敏感数据。

[0038] 在一个实施例中，DLP策略250包括基于机器学习-学习的检测(MLD)的概况265。向量机器学习和其它类型的机器学习可以用于保护诸如Microsoft®Word或PowerPoint®文档或CAD制图之类的非结构化数据。MLD概况265可以包括训练数据集270、分类模型275和特征集280。训练数据集270是敏感数据的正例(positive example)和敏感数据的反例(negative example)的集合。训练数据集270由ML管理器处理，以生成分类模型275和特征集280。分类模型275是包括支持向量(表示边界特征)映射的针对数据分类的统计模型。特征集280是诸如包括从训练数据集270提取的多个特征的列表或表格之类的数据结构。在一个实施例中，每个特征都是包括在来自训练数据集270的数据中的词。

[0039] 策略违反检测器的一个示例是机器学习模块225。ML模块225包括将MLD概况265和未分类数据(例如，文件235)采取为输入并且将针对数据的分类采取为输出的ML引擎230。通过使用分类模型275和特征集280，ML引擎230处理输入数据。因此，ML模块225可以使用MLD概况265以便在敏感数据与非敏感数据之间进行区分。

[0040] 当检测到DLP策略违反时，策略违反应答器220应用一种或多种DLP应答规则245。每个DLP应答规则245都可以与一种或多种DLP策略250相关联。每个DLP应答规则245都包括一个或多个动作，策略违反应答器220采取所述一个或多个动作以便响应于相关联DLP策略250的违反。一旦发现违反DLP策略250，策略违反应答器220就可以确定哪个DLP应答规则与违反的DLP策略250相关联。然后可以执行包括在应答规则245中的一个或多个动作。执行的动作的示例包括：将通知发送到管理员、防止数据通过数据丢失向量退出端点装置、锁定计算机使得没有数据可以通过任何数据丢失向量移动出端点装置、当数据移动出端点装置时对数据进行加密等等。

[0041] 事件报告生成器215可以生成记录违反DLP策略250的事件报告240和围绕违反DLP策略250的环境。事件报告生成器215保持已经在端点装置上发生和/或已经由特定用户尝试的一些或全部策略违反的事件报告240的记录。可以例如基于用户登录识别用户。除了识别违反的DLP策略之外，每份事件报告240还可以指示策略违反的环境。例如，事件报告240可以识别与策略违反相关联的应用、用户、数据丢失向量、敏感数据类型(例如，社会保险号码、信用卡号码等等)等等。事件报告生成器215还可以包括示出策略违反何时发生的时间戳(time stamp)。

[0042] 图3是根据本发明一个实施例的机器学习(ML)管理器305的框图。ML管理器305包括MLD概况训练器325、MLD概况测试器320和MLD概况配置器315。在一个实施例中，ML管理器305还包括用户界面310。注意到，在可替换的实施例中，MLD概况训练器325、MLD概况测试器320中的一个或多个或者MLR概况训练器325可以组合为单一模块或划分为多个模块。

[0043] MLD概况训练器325基于训练数据集352来训练MLD概况365。MLD概况训练是在其中从训练数据集提取内容并且对内容执行统计分析以生成分类模型和特征集(这都在下文中更详细地描述)的过程。用户(例如，DLP管理员)可以规定数据以在训练数据集中使用。在一个实施例中，用户选择敏感数据的正例(正面数据345)和敏感数据的反例(反面数据350)，并且将这些示例添加到训练数据集352。这可以经由用户界面310来完成。可替换地，用户可以经由标准文件系统界面(例如，Microsoft® Explorer®)将文件添加到正面数据文件夹和反面数据文件夹。数据可以作为谨慎文件(例如，文档)或单一压缩文件(例如，zip文件)的组成部分而添加到训练数据集。

[0044] 在一个实施例中，从事件报告360提取针对训练数据集352的数据。事件报告360可以在DLP策略385的强制执行期间针对现存的DLP策略而已经生成。事件报告360可以识别操作被执行或请求以对敏感数据执行的实例。事件报告可以包括敏感数据的真正实例，并且还可以包括在其中非敏感数据被分类为敏感数据的假正面(false positive)。其它可以或不可以与事件报告相关联的历史数据也可以用于训练数据集。历史数据可以包括敏感数据的真正实例、误报、非敏感数据的真正实例和/或假负面(false negative)。

[0045] 在一个实施例中，MLD概况训练器325执行针对现存的MLD概况的增值(incremental)训练。利用增值训练，基于自MLD概况最近训练以来已经生成的事件报告，MLD概况训练器325将新的正面数据和/或反面数据添加到训练数据集。MLD概况训练器325可以自动或响应于用户输入执行增值训练。在一个实施例中，根据预定时间表执行增值训练。例如，MLD概况训练器325可以定期地(诸如每天、每周、每月之类)执行对MLD概况的训练。

[0046] 在一个实施例中，MLD概况训练器325直到阈值数目的文档已经添加到训练数据集才生成针对训练数据集352的MLD概况325。在一个实施例中，应该添加正面数据345的阈值量和反面数据350的阈值量。阈值例如可以是50个正面文档和50个反面文档。在一个实施例中，最大文档大小(例如，15MB、30MB，等等)由ML管理器305强制执行。可以拒绝任何大于最大文档大小的文档用作训练数据。最大文档大小可以是用户可选择的。

[0047] 在一个实施例中，MLD概况训练器325包括模型生成器330、特征提取器335和质量分析器340。特征提取器335分析训练数据集352中的敏感数据的正例和敏感数据的反例，并且在正面数据和反面数据中确定特征(例如，词)的出现频率。特征提取器335然后基于例如出现频率而将正面特征和反面特征进行排序。在一个实施例中，特征提取器335过滤掉诸如“这”、“它”、“和”等常用词。特征提取器335然后选择针对特征集375的最高排序的特征。

[0048] 在一个实施例中，特征提取器335根据针对诸如中文字符(日本汉字)等基于字符的字母表的字符生成特征。特征提取器335针对每个字符生成特征，并且附加地创建针对每对相邻字符的特征。例如，对于字符Ξλ而言，特征提取器将生成针对Ξ、λ和Ξλ的特征。

[0049] 添加到特征集375的特征数目可以基于存储器分配，该存储器分配可以由MLD概况训练器325自动地选择或可以由用户选择。随着存储器分配增加，包括在特征集375中的特征数目也增加，这可以增加MLD概况的精确度。存储器分配可以例如在大约30MB与大约100MB之间变化。在一个实施例中，存储器分配可选择为高、中或低。可替换地，可以选择特定存储器分配(例如，43MB)。最终得到的MLD概况365的大小与训练文档的数目和存储器分配设置成比例。在一个实施例中，较低存储器分配用于将由DLP代理实施的MLD概况365，并且较高存储器分配用于将由全局DLP检测引擎实施的MLD概况365。

[0050] 在一个实施例中，特征提取器335使用词频-逆向文档频率(TF-IDF，term frequency-inverse document frequency)算法以选择特征集375。可替换地，特征提取器335可以使用诸如段组词频-逆向段组频率(STF-ISSF，segment-set term frequency-inverse segment-set frequency)、段组词频-逆文档频率(STF-IDF，segment-set term frequency-inverse document frequency)之类的其它特征提取算法。在一个实施例中，特征提取器335使用的特征选择算法是用户可选择的。此外，特征提取器335可以多次执行特征提取，每次都使用不同的特征提取算法。使用不同算法生成的特征集每个都可以用于生成不同的分类模型，并且可以由质量分析器340测试。然后可以保存具有最佳质量度量(quality metrics)的特征集，并且可以丢弃其它特征集。

[0051] 在特征提取器335已经生成特征集375之后，模型生成器330基于特征集375和训练数据集352生成分类模型380。分类模型380是针对包括支持向量映射(表示边界特征)的数据分类的统计模型。边界特征可以从特征集375选择，并且可以表示特征集375中的最高排序特征。

[0052] 一旦特征提取器335生成特征集375并且模型生成器330生成分类模型380，则MLD概况365就是完整的。MLD概况365可以包括特征集375、分类模型380和/或训练数据集370。MLD概况365还可以包括用户定义设置。在一个实施例中，用户定义设置包括敏感性阈值(还称为置信水平阈值)。敏感性阈值可以设置为例如75％、90％等等。当ML引擎使用MLD概况365以便将文档分类为敏感或不敏感时，ML引擎可以将置信值分配给分类。如果针对文档的置信值是100％，则更可能的是，文档为敏感(或不敏感)的决定比置信值是否是例如50％更

精确。如果置信值小于敏感性阈值，则即使文档分类为敏感文档，则也可能不生成事件。该特征可以有助于用户进一步控制并且减少假正面和/或假反面。如果ML引擎试图将训练从未被看到的类型的文档分类，则其具有非常低的文档置信为正面和/或反面。在这种情况下，敏感性阈值可以用于减少假正面的发生。在一个实施例中，MLD概况训练器325基于训练自动地选择针对MLD概况365的敏感性阈值。

[0053] 在一个实施例中，质量分析器340分析MLD概况365的质量并且生成针对MLD概况365的一个或多个质量度量。质量度量可以包括假正面率(由MLD概况365错误分类为敏感数据的敏感数据的反例)、假反面率(由MLD概况365错误分类为非敏感数据的敏感数据的正例)和/或存储器利用率(由MLD概况365使用的存储器的量)。质量分析器340可以将质量度量与一个或多个质量阈值进行比较。这些可以包括假正面阈值、假反面阈值和/或存储器利用阈值。在一个实施例中，假正面阈值是5％并且假反面阈值是5％。可替换地，可以使用其它假正面阈值和/或假反面阈值。如果假正面率超过假正面阈值，则假反面率就超过了假反面阈值，或者如果存储器利用率超过存储器利用阈值，则MLD概况365可能没有准备好配置。如果一个或多个质量阈值已经由MLD概况365超过，则ML管理器305可以不允许MLD概况365被配置。

[0054] 通过改变训练数据集352并且验算特征集375和分类模型380，可以修改MLD概况365。通过添加新的正面数据345、添加新的反面数据350、移除正面数据345的实例和/或移除反面数据350的实例，可以修改训练数据集352。在一个实施例中，质量分析器340从引起假正面的反面数据350识别特定的文件、文档等等，并且从引起假反面的正面数据345识别特定的文件、文档等等。用户可以检查该信息以确定添加到训练数据集的附加数据。在训练数据集352中可能已经非充分表示了某类别的文档。例如，用户可以希望保护源代码，并且产品文档可能已经由MLD概况365交叉分类为源代码。用户可以通过将产品文档的附加示例添加到反面数据集来校正这一点。可以认出并分类为敏感或非敏感的数据类别的示例包括源代码、处方(recipes)、法律文档、产品文档、病历文档、保险文档、产品配方、患者健康信息等等。

[0055] 在一个实施例中，用户能够规定针对用户添加到训练数据集的每个文件(例如，文档)的类别。质量分析器340然后可以识别引起大多数假正面和/或大多数假反面的文档类别。在一个实施例中，质量分析器340针对用户建议添加特定的文档类别，以改进MLD概况365的质量。

[0056] 在一个实施例中，ML管理器305保持包括对于之前生成的MLD概况进行改变的改变报告。改变报告还可以包括之前生成的MLD概况与最近修改的MLD概况之间的质量度量区别。改变报告可以显示给用户以便使用户能够接受改变或重新运行(roll back)改变以使之前的MLD概况恢复原状。

[0057] 一旦MLD概况365准备好配置(例如，质量度量在质量阈值内)，MLD概况配置器315就配置MLD概况315。在一个实施例中，MLD概况配置器315将MLD概况添加到现存的DLP策略385。可替换地，MLD概况配置器315可以生成新的DLP策略并且将MLD概况365添加到新的DLP策略385。

[0058] 在一个实施例中，ML管理器305包括VML测试器320。VML测试器测试关于附加数据的MLD概况。在一个实施例中，MLD概况测试器执行对预定测试数据集的反面测试。该预定测

试数据集可以包括已知不包括任何敏感信息的大量数据(例如,10,000个文档)。MLD概况测试器320还可以测试关于用户选择数据的MLD概况,该用户选择数据的MLD概况可以包括附加的正面数据和/或反面数据。

[0059] 图4是图示用于生成并配置MLD概况的方法400的一个实施例的流程图。该方法400通过可以包括硬件(电路、专用逻辑,等等)、软件(诸如运行在通用计算机系统或专用机器上)或硬件与软件组合的处理逻辑来执行。方法400可以通过诸如运行在图1的强制执行服务器120上的ML管理器130之类的ML管理器来执行。虽然方法400在下文中描述为由ML管理器执行,但是方法400还可以由其它处理逻辑执行。

[0060] 参照图4,在方框405中,ML管理器生成针对新MLD概况或待修改的现存的MLD概况的临时工作空间。在一个实施例中,针对可能已经使诸如IDM或EDM概况之类的其它概况运行的现存的DLP策略生成空的MLD概况。在另一个实施例中,针对仍然待配置的新DLP策略生成空的MLD概况。可替换地,在临时工作空间中打开现存的MLD概况。在一个实施例中,临时工作空间响应于用户请求而生成,以便创建新的MLD概况或经由用于机器学习的用户界面修改现存的MLD概况。在一个实施例中,新的MLD概况用于保护数据的特定类别。例如,MLD概况可以用于保护源代码、用于保护患者信息、用于保护销售数据等等。

[0061] 图5图示了示出根据本发明一个实施例的空的临时工作空间的用于机器学习的用户界面的第一视图500。如所示,临时工作空间包括用于上载正面文档的“正面”按钮505和用于上载反面文档的“反面”按钮510。响应于用户选择“正面”按钮505或“反面”按钮510,ML管理器可以打开文件浏览器窗口。用户然后可以导航文件浏览器窗口以选择用于上载的一个文档或多个文档。

[0062] 在一个实施例中,用户界面包括存储器分配按钮515。响应于用户选择存储器分配按钮515,ML管理器打开窗口,所述窗口向用户呈现存储器分配的选项。在一个实施例中,用户能够在高、中与低存储器分配之间选择。每个存储器分配可以与特定存储器利用阈值相关联。可替换地,用户可以能够选择特定存储器分配(例如,12MB、54MB,等等)。在一个实施例中,用户界面包括当选择时打开窗口(在其中用户可以在概况名和/或概况描述中打字)的附加按钮515。

[0063] 返回图4,在方法400的方框410中,ML管理器接收训练数据集。在一个实施例中,用户经由用户界面选择针对训练数据集的数据。训练数据集包括敏感数据的正例和敏感数据的反例。训练数据集可以包括多个文档。在一个实施例中,用户针对每个文档规定类别(例如,源代码、销售数据、病历等等)。在一个实施例中,ML管理器检查训练数据集中每个文档的文档大小。ML管理器可以拒绝超过最大文档大小的那些ML文档。

[0064] 图6图示了示出根据本发明一个实施例的训练数据集的图5的用户界面的第二视图600。训练数据集中的每个文档可以连同文档的多个属性一起显示。在一个实施例中,显示的文档属性包括文档类型605(即,文档是正面文档还是反面文档)、文档名610、文档日期615(即,上载文档的日期)和文档作者620。每个文档还可以包括移除按钮625。通过选择移除按钮625,用户可以从训练数据集移除特定文档。在一个实施例中,还显示文档类别。用户可以为每个文档分配文档类别。在一个实施例中,点击临时工作空间选项卡(tab)上呈现的叉形按钮使已经对概况进行的全部改变重新运行。概况然后继续保持为最近已知的功能状态。

[0065] 一旦正面文档和反面文档的阈值数目已经添加到训练数据集(例如,每个类型20个文档、每个类型50个文档等等),训练概况操作就变得可用的。在一个实施例中,当正面文档和反面文档的阈值数目已经添加时,“训练概况”按钮630就变得有效。用户可以选择“训练概况”按钮630以便训练MLD概况(例如,针对MLD概况生成特征集和分类模型)。

[0066] 返回到图4,在方法400的方框415中,ML管理器接收存储器分配的选择。在方框420中,ML管理器通过使用机器学习(例如,向量机器学习)来分析训练数据集以便训练MLD概况。在一个实施例中,ML管理器在训练期间执行对MLD概况的写入锁定。在一个实施例中,训练MLD概况包括执行特征提取(方框421)、生成分类模型(方框422)以及确定分类模型和特征集的质量(方框423)。在方框425中,ML管理器在用户界面中显示分析结果。结果可以包括诸如假正面率、假反面率、存储器利用率、提取失败的正面文档和提取失败的反面文档等一个或多个质量度量。在一个实施例中,用户可以点击提取失败信息以发现哪个文档提取失败。

[0067] 图7图示示出了训练的MLD概况的图5的用户界面的第三视图700。在一个实施例中,用户界面示出MLD概况训练的每个步骤,包括特征提取、精确度计算、模型创建和最终处理。可以突出MLD概况训练的当前步骤以示出ML管理器在MLD概况生成中的位置。在一个实施例中,当训练概况时,锁定临时工作空间。此外,当训练概况时,可以不调节存储器分配。这确保产生精确的训练结果。在一个实施例中,用户可以在训练期间的任何时候选择取消训练选项以停止训练。

[0068] 图8图示了示出MLD概况训练结果的图5的用户界面的第四视图800。在一个实施例中,MLD概况结果包括正面文档计数805、反面文档计数810和总文档计数815。在一个实施例中,ML管理器显示在特征集中的特征(例如,词)列表。训练结果还包括一个或多个针对MLD概况的质量度量。在一个实施例中,质量度量包括假正面率820、假反面率825和存储器利用率830。用户可以选择假正面率820以观察诸如引起假正面的特定文档之类的附加假正面率信息。此外,用户可以选择假反面率825以观察诸如引起假反面的特定文档之类的附加假反面率信息。如果质量度量在质量阈值内,则“配置训练”按钮835可以是有效的。用户可以选择“配置训练”按钮835以便配置MLD概况。用户还可以选择“拒绝训练”按钮840以拒绝MLD概况。

[0069] 返回图4,在方框430中,ML管理器确定分析结果是否示出MLD概况满足一个或多个配置标准。如果结果满足配置标准,则方法行进到方框435。否则,方法持续到方框440。

[0070] 在方框435中,ML管理器能够实现MLD概况配置操作。在方框450中,ML管理器接收配置命令(例如,基于用户在用户界面中按压配置按钮)。如果MLD概况与策略相关联,则配置命令就导致使概况配置到检测服务器。如果DLP策略是有效的DLP策略,则MLD概况变为有效并且可以立即用于策略文档。注意到,如果MLD概况具有之前配置版本,则该版本保持配置直到配置了该MLD概况的新版本。配置较新的版本的MLD概况可以替代较旧版本。

[0071] 在方框440中,ML管理器建议用户对训练数据集进行修改。如果用户在训练数据集中标示了文档的类别,则ML管理器可以识别应该添加到训练数据集的文档类别。例如,如果特定的文档类别引起更大数目的假正面,则ML管理器可以建议用户将该类别的更多文档添加到训练数据集中的反面文档上。

[0072] 在方框445中,ML管理器确定是否对训练数据集或存储器分配选择进行任何修改。

如果对训练数据集或存储器分配进行改变，则方法返回到方框420。否则方法结束。可以在配置的概况页面上示出配置概况。该页面提供给用户当前配置概况的视图。

[0073] 图9是示出根据本发明一个实施例的MLD概况生成/修改期间的ML管理器的不同状态的状态图900。当用户输入命令以生成新的MLD概况时，ML管理器就进入“新”状态905，其使ML管理器生成临时工作空间和空的MLD概况。根据“新”状态905，ML管理器可以进入“管理概况”状态910。根据“管理概况”状态910，ML管理器可以基于用户输入将文档添加到训练数据集。ML管理器还可以使MLD概况重新运行到之前的状况，并且返回到“新”状态905或行进到“训练”状态915。如果修改之前生成的MLD概况，则ML管理器还可以从“管理概况”状态910过渡到“已接受”状态930。

[0074] 当在“训练”状态915中时，ML管理器训练MLD概况。如果训练被取消或以其它方式失败，则ML管理器过渡到“训练失败/取消”的状态920。在用户确认之后，ML管理器使“管理概况”状态910恢复原状。如果训练成功，则ML管理器过渡到“已训练”状态925。用户然后可以拒绝MLD概况，从而使ML管理器返回到“管理概况”状态910，或者接受MLD概况，从而使ML管理器过渡到“已接受”状态930。根据“已接受”状态，则ML管理器可以配置MLD概况。

[0075] 图10是图示针对生成MLD概况并且将MLD概况配置到现存的DLP策略的方法1000的一个实施例的流程图。方法1000通过处理逻辑来执行，所述处理逻辑可以包括硬件(电路、专用逻辑等等)、软件(诸如运行在通用计算机系统或专用机器上)或硬件与软件组合。方法1000可以通过诸如运行在图1的强制执行服务器120上的ML管理器130之类的ML管理器来执行。

[0076] 参考图10，在方框1005中，ML管理器收集由DLP策略生成的事件报告和/或历史数据。事件报告可以包括错误分类为非敏感文档的文档和/或错误分类为敏感文档的文档。此外，事件报告可以包括正确分类为敏感文档的文档和/或正确分类为非敏感文档的文档。

[0077] 在方框1010中，ML管理器将来自事件报告/历史数据的文档添加到针对MLD概况的训练数据集。在方框1015中，ML管理器通过使用机器学习来分析训练数据集以训练MLD概况。这可以包括生成特征集、生成分类模型和生成一个或多个针对MLD概况的质量度量。在方框1020中，ML管理器将MLD概况添加到DLP策略。

[0078] 方法1000示出来自现存的DLP策略的事件可以怎样用于生成MLD概况。因此，ML管理器可以执行方法1000以改进现存的DLP策略，从而使得它能够将文档分类为敏感或非敏感(之前其在分类上不成功)。

[0079] 图11是图示通过使用包括DLP概况的DLP策略来保护计算装置免于数据丢失的方法1100的一个实施例的流程图。方法1100通过处理逻辑来执行，所述处理逻辑可以包括硬件(电路、专用逻辑等等)、软件(诸如运行在通用计算机系统或专用机器上)或硬件与软件组合。方法1100可以通过诸如运行在图1的端点装置102A上的DLP代理106之类的DLP代理来执行。方法1100还可以通过诸如运行在图1的端点服务器115上的全局DLP检测引擎122之类的全局DLP检测引擎来执行。

[0080] 参考图11，在方框1105中，处理逻辑接收在文档上执行操作的请求。在方框1110中，ML模块通过使用MLD概况来分析文档以便将文档分类。在方框1125中，处理逻辑确定文档分类为敏感还是非敏感。如果文档分类为敏感，则方法持续到方框1130，且执行通过DLP响应规则规定的动作，并且生成事件报告。这可以包括防止操作、生成事件响应报告等等。

如果文档分类为非敏感，则方法行进到方框1135，并且执行操作。

[0081] 图12图示了以在其内部可以执行指令集(用于使机器执行在本文中讨论的任何一个或多个方法)的计算机系统1200的示例形式的机器的图解表示。在可替换的实施例中，机器可以在LAN、内联网、外联网或因特网中连接(例如，联网)到其它机器。机器可以在客户-服务器网络环境下操以服务器或者客户机的资格操作，或者在点对点(或分布式)网络环境下操作为对等机器。机器可以是个人计算机(PC)、平板PC、机顶盒(STB)、个人数字助理(PDA)、蜂窝电话、网络器具、服务器、网络路由器、交换机或桥接器或能够执行规定了待由该机器采取动作的指令集(顺序或非顺序的)的任何机器。而且，虽然仅图示单个机器，但是术语“机器”还应该理解为包括单独或共同执行一个或多个指令集以便执行本文中讨论的一个或多个方法中的任何一个的任何机器集合。

[0082] 示例性计算机系统1200包括处理装置(处理器)1202、主存储器1204(例如，只读存储器(ROM)、闪存、诸如同步DRAM(SDRAM)或Rambus DRAM(RDRAM)等等之类的动态随机存取存储器(DRAM)、静态存储器1206(例如，闪存、静态随机存取存储器(SRAM)等等)和经由总线1208彼此通信的数据存储装置1218。

[0083] 处理器1202表示诸如微处理器、中央处理单元等之类的一个或多个通用处理装置。更特别地，处理器1202可以是复杂指令集计算(CISC)微处理器、精简指令集计算(RISC)微处理器、超长指令字(VLIW)微处理器或实施其它指令集的处理器或实施指令集组合的多个处理器。处理器1202还可以是诸如专用集成电路(ASIC)、现场可编程门阵列(FPGA)、数字信号处理器(DSP)、网络处理器等之类的一个或多个专用处理装置。处理器1202配置成执行指令1226以用于执行在本文中讨论的操作和步骤。

[0084] 计算机系统1200还可以包括网络接口装置1222。计算机系统1200还可以包括视频显示单元1210(例如，液晶显示器(LCD)或阴极射线管(CRT))、字母数字输入装置1212(例如，键盘)、光标控制装置1214(例如，鼠标)和信号生成装置1220(例如，扬声器)。

[0085] 数据存储装置1218可以包括在其上存储体现在本文中描述的任何一个或多个方法或功能的一个或多个指令集1226(例如，软件)的计算机可读存储介质1224。在由计算机系统1200关于其的执行期间，指令1226还可以完全或至少部分地居于主存储器1204内和/或处理器1202内，主存储器1204和处理器1202还构成计算机可读存储介质。指令1226可以进一步经由网络接口装置1222通过网络1274发射或接收。

[0086] 在一个实施例中，指令1226包括针对诸如图2的ML管理器205之类的ML管理器的指令，和/或包含调用ML管理器的方法的软件库。虽然在示例性实施例中计算机可读存储介质1224示出为单个介质，但是术语“计算机可读存储介质”应该理解为包括存储一个或多个指令集的单个介质或多个介质(例如，集中式或分布式数据库和/或相关联的缓存和服务器)。术语“计算机可读存储介质”还应该理解为包括任何介质，所述任何介质能够存储、编码或承载用于由机器执行的指令集并且使机器执行本发明的一个或多个方法中的任何一个。术语“计算机可读存储介质”因此应该理解为包括但不限于固态存储器、光介质和磁介质。

[0087] 应该理解以上说明书意图是说明性的，而非限制性的。通过阅读并理解以上说明书，许多其它实施例对本领域技术人员将是显而易见的。因此，应该参照所附权利要求连同使这种权利要求有权的全部范围的等同物来确定本发明的范围。

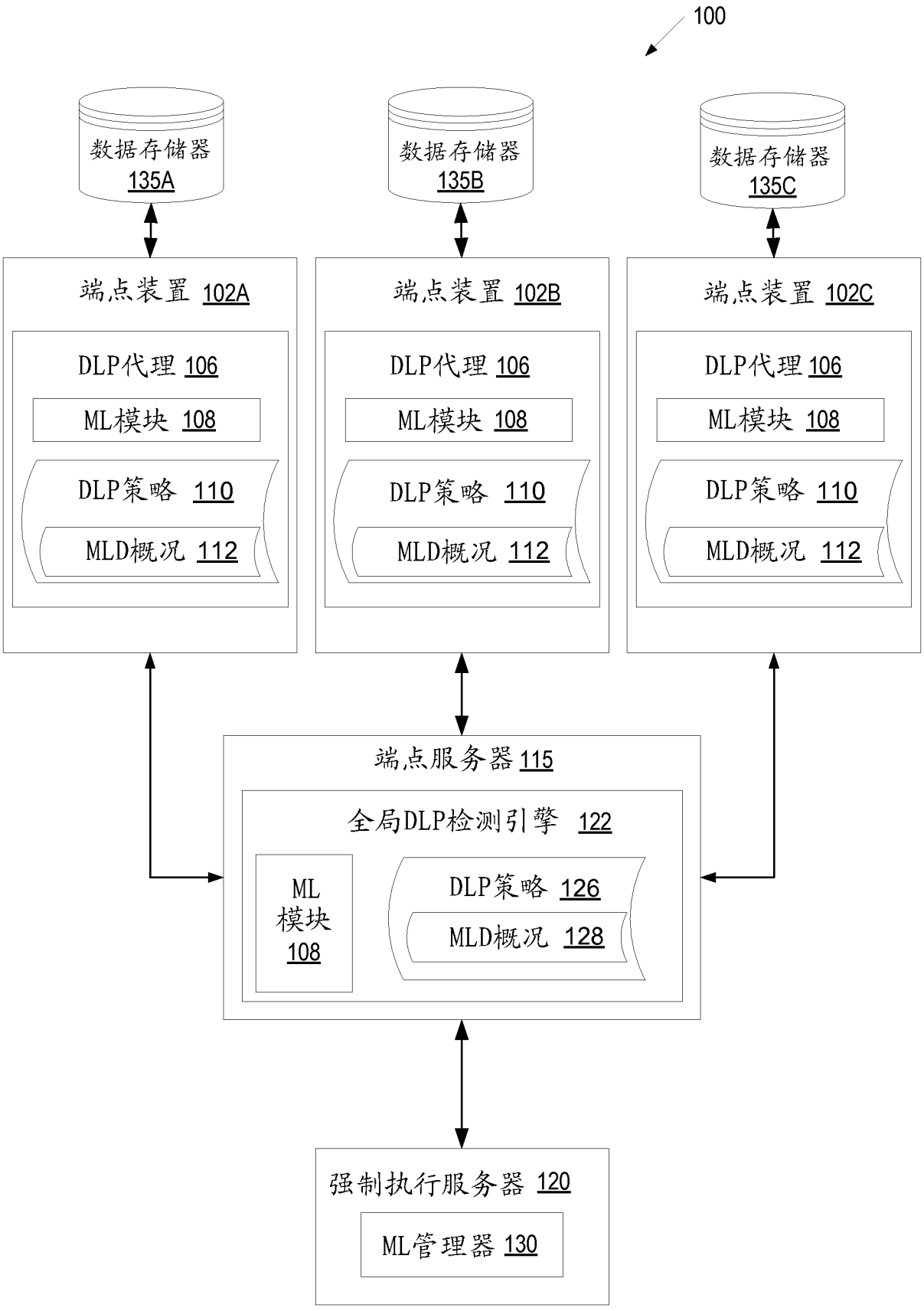

100
数据存储器 135A
数据存储器 135B
数据存储器 135C
端点装置 102A
DLP代理 106
ML模块 108
DLP策略 110
MLD概况 112
端点装置 102B
DLP代理 106
ML模块 108
DLP策略 110
MLD概况 112
端点装置 102C
DLP代理 106
ML模块 108
DLP策略 110
MLD概况 112
端点服务器 115
全局DLP检测引擎 122
ML 模块 108
DLP策略 126
MLD概况 128
强制执行服务器 120
ML管理器 130

图 1

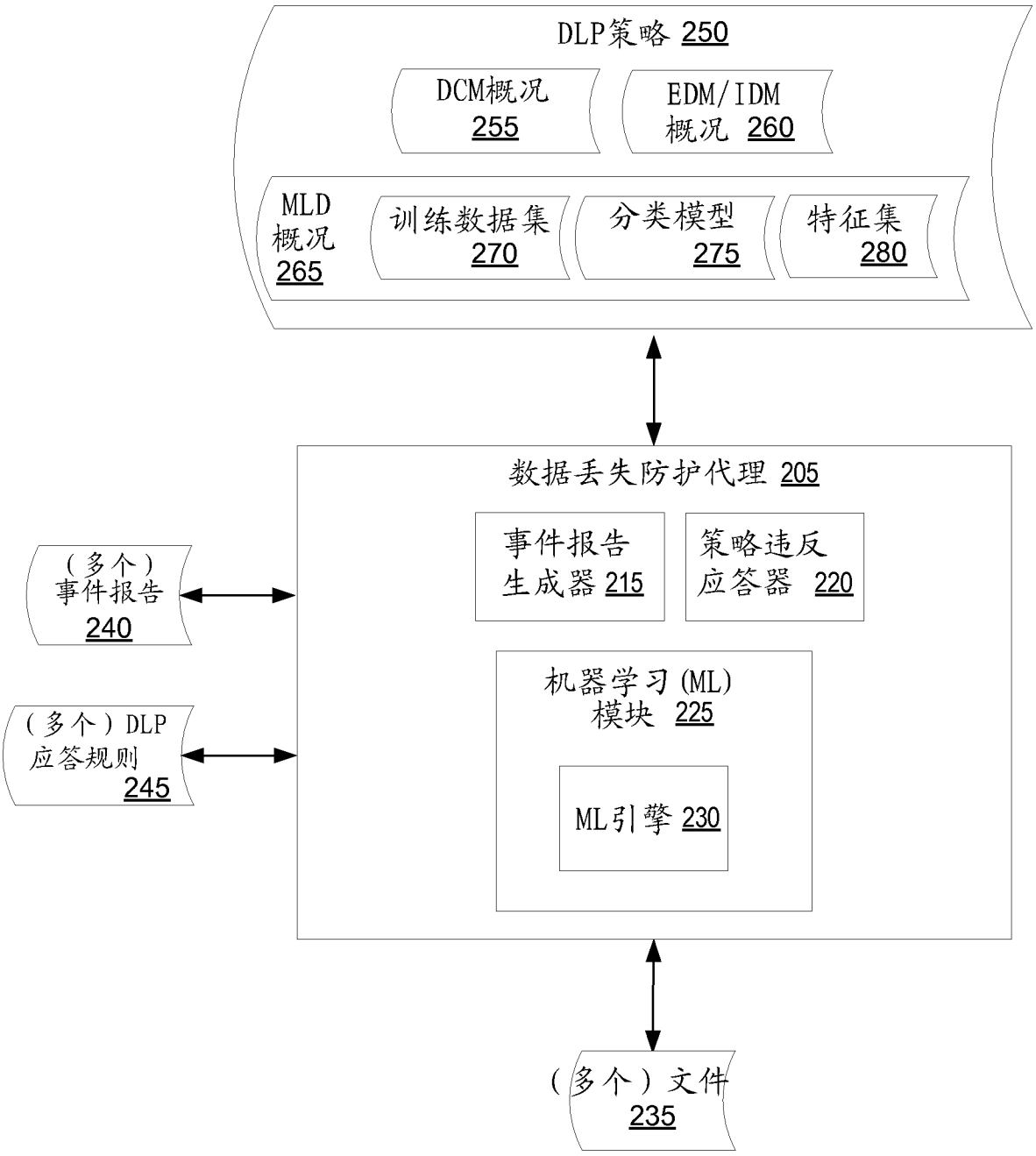

DLP策略 250
DCM概况 255
EDM/IDM 概况 260
MLD 概况 265
训练数据集 270
分类模型 275
特征集 280
数据丢失防护代理 205
事件报告 生成器 215
策略违反 应答器 220
机器学习(ML) 模块 225
ML引擎 230
(多个) 事件报告 240
(多个) DLP 应答规则 245
(多个) 文件 235

图 2

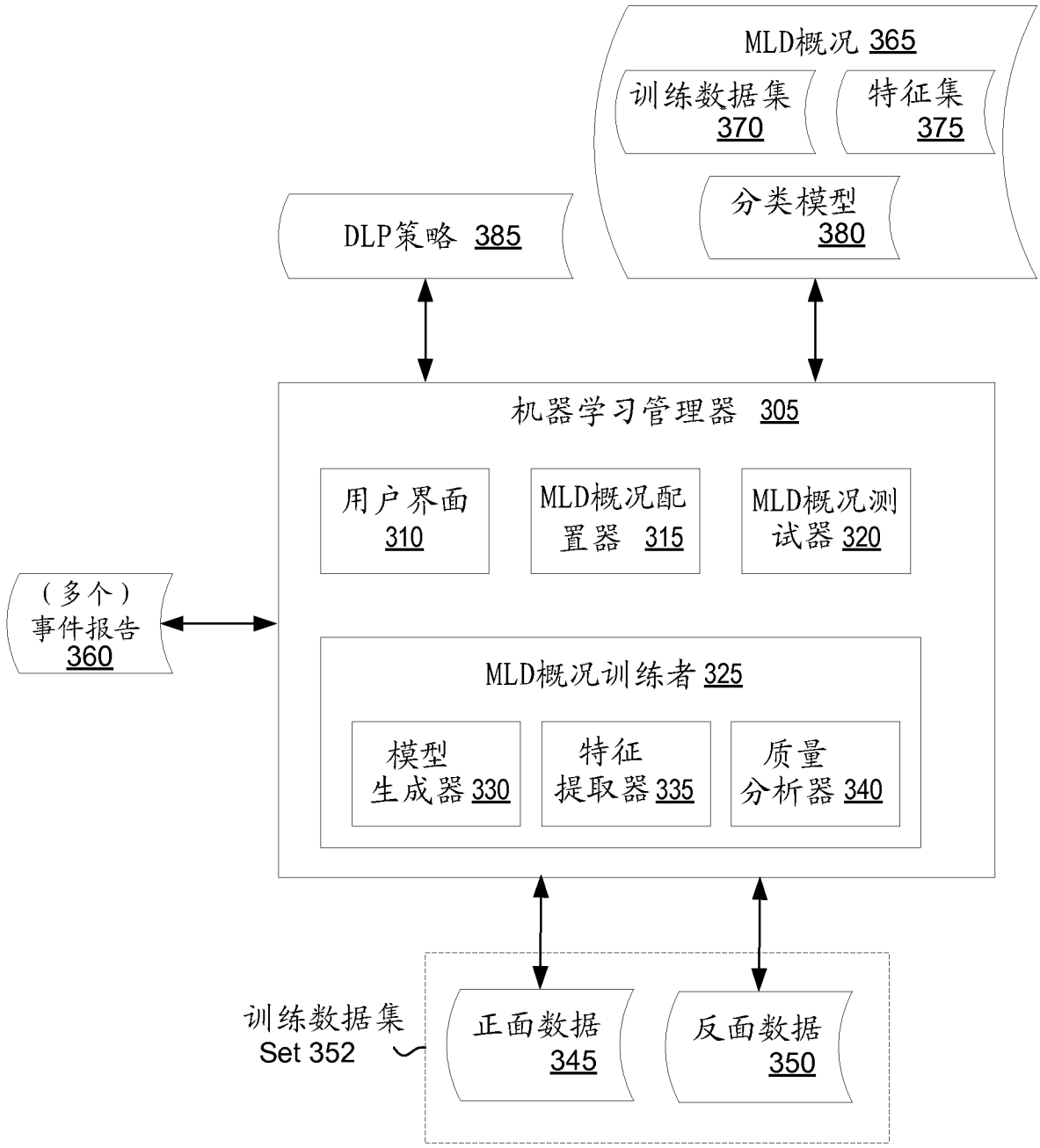

MLD概况 365
训练数据集 370
特征集 375
分类模型 380
DLP策略 385
机器学习管理器 305
用户界面 310
MLD概况配置器 315
MLD概况测试器 320
（多个）事件报告 360
MLD概况训练者 325
模型生成器 330
特征提取器 335
质量分析器 340
训练数据集 Set 352
正面数据 345
反面数据 350

图 3

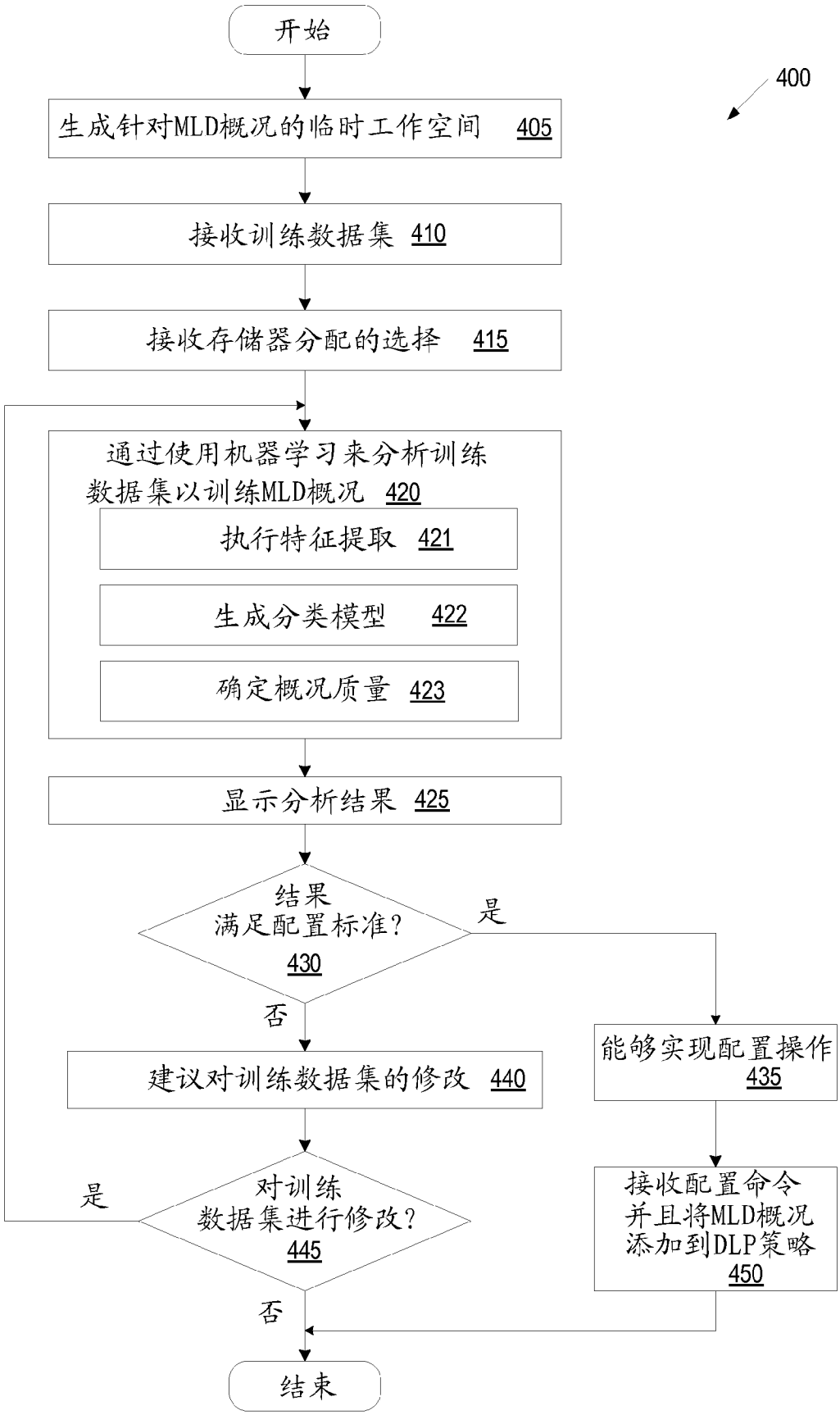

开始
400
生成针对MLD概况的临时工作空间 405
接收训练数据集 410
接收存储器分配的选择 415
通过使用机器学习来分析训练数据集以训练MLD概况 420
执行特征提取 421
生成分类模型 422
确定概况质量 423
显示分析结果 425
结果满足配置标准? 430
是
否
能够实现配置操作 435
建议对训练数据集的修改 440
对训练数据集进行修改? 445
是
否
接收配置命令并且将MLD概况添加到DLP策略 450
结束

图 4

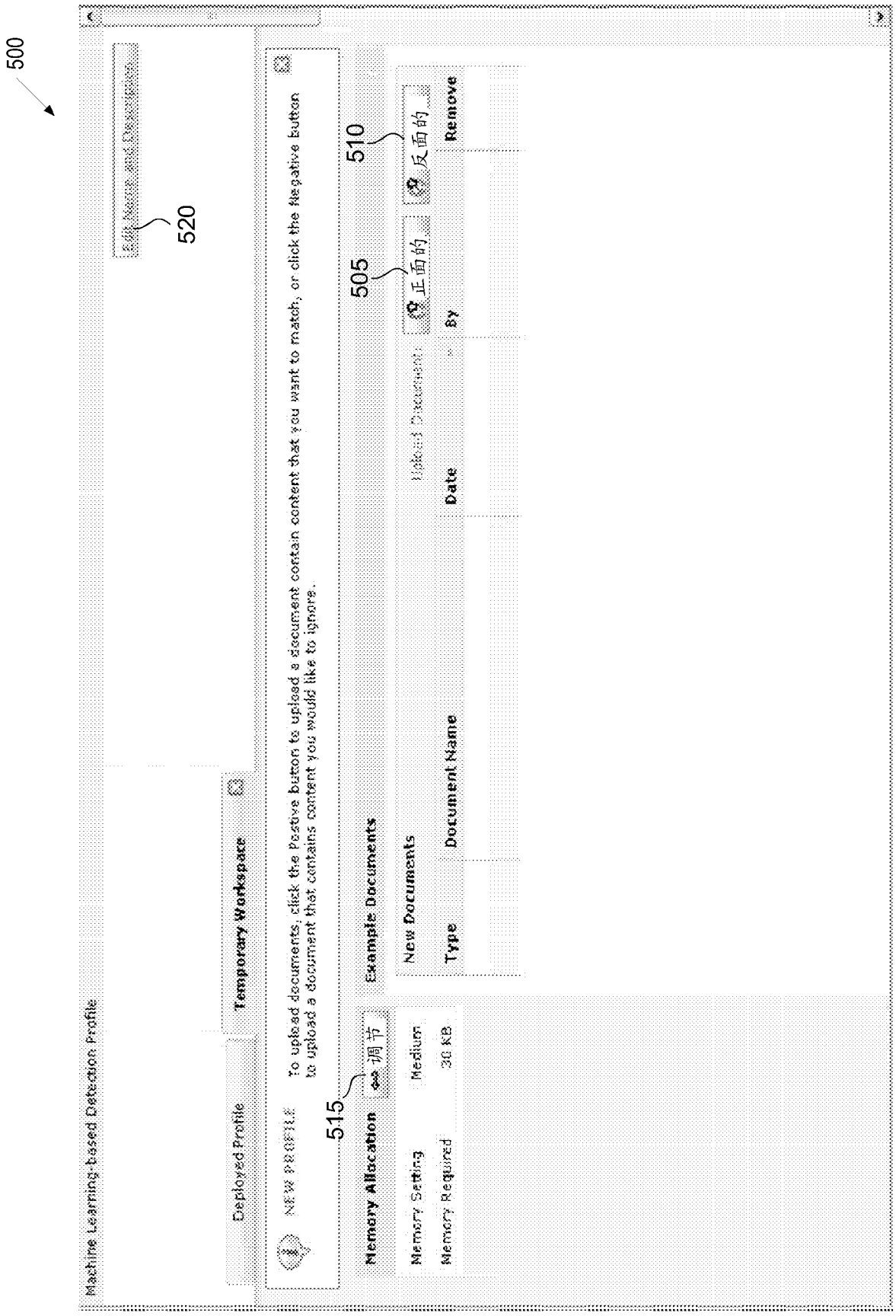

500
520
510
505
515
Machine Learning-based Detection Profile
Edit Name and Description
Deployed Profile
Temporary Workspace
To upload documents, click the Postive button to upload a document contain content that you want to match, or click the Negative button to upload a document that contains content you would like to ignore.
Example Documents
New Documents
Upload Document:
正面的
反面的
Type
Document Name
Date
By
Remove
Memory Allocation
调节
Memory Setting
Medium
Memory Required
30 KB

图 5

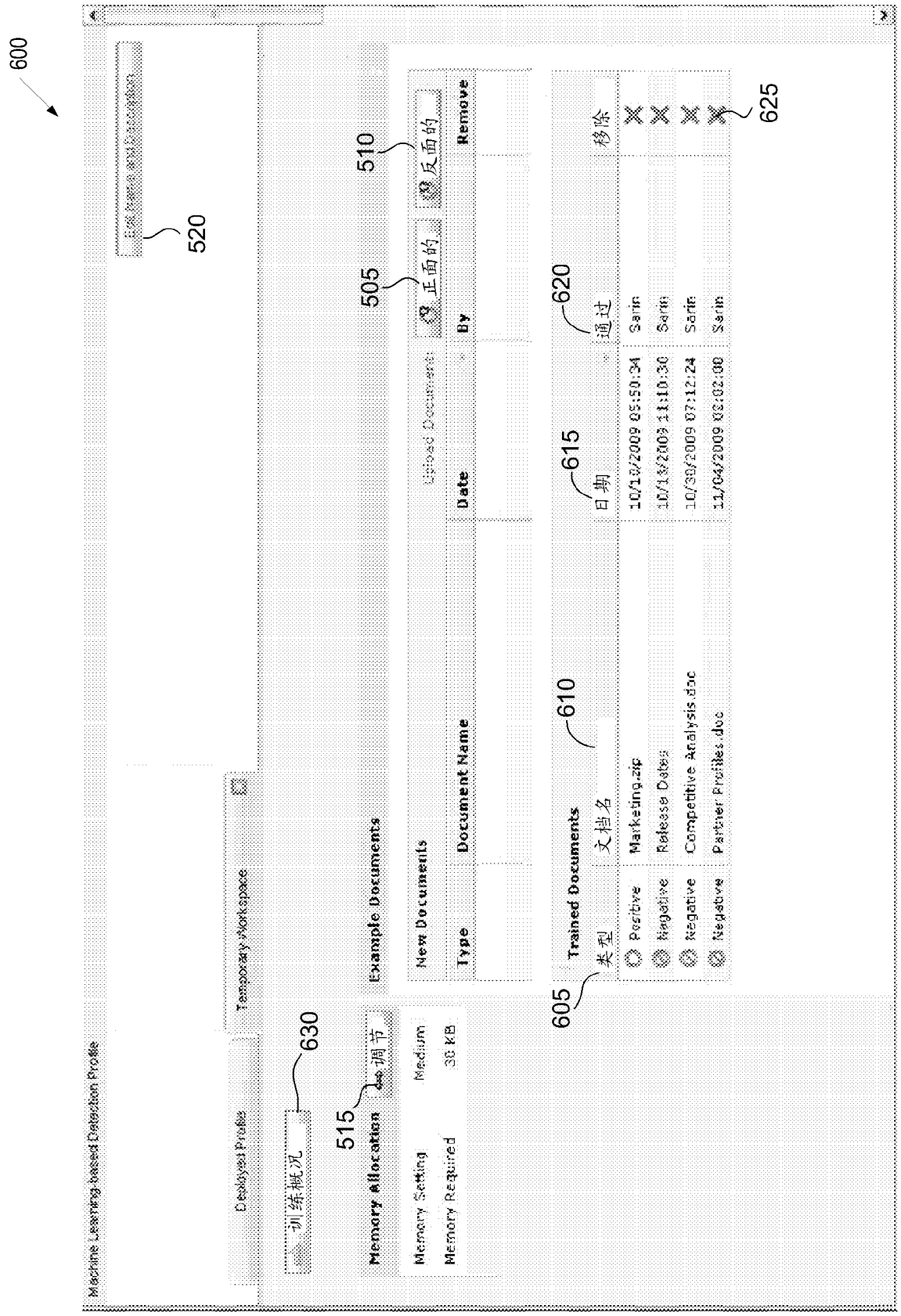

600
Machine Learning-based Detection Profile
Temporary Workspace
Deployed Profile
训练概况
630
515
Memory Allocation
调节
Memory Setting
Medium
Memory Required
38 KB
Example Documents
New Documents
Upload Documents
正面的
反面的
510
505
Type
Document Name
Date
By
Remove
Existing Examples
520
605
Trained Documents
类型
文档名
610
日期
615
通过
620
移除
Positive
Marketing.zip
10/15/2009 05:50:34
Sarin
Negative
Release Dates
10/13/2009 11:10:30
Sarin
Negative
Competitive Analysis.doc
10/30/2009 07:12:24
Sarin
Negative
Partner Profiles.doc
11/04/2009 03:02:00
Sarin
625

图 6

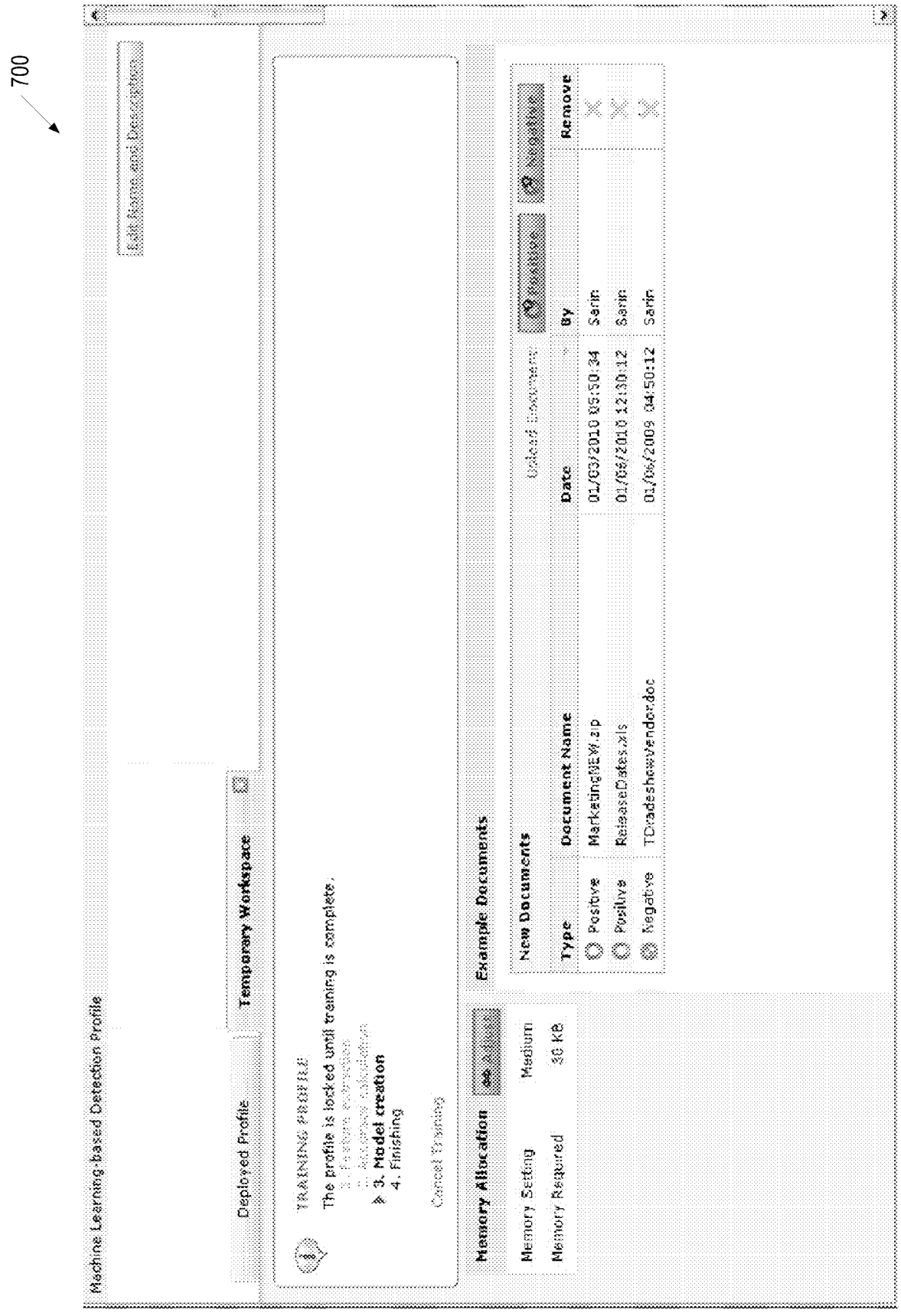

700
Machine Learning-based Detection Profile
Deployed Profile
Temporary Workspace
Edit Name and Description
TRAINING PROFILE
The profile is locked until training is complete.
3. Model creation
4. Finishing
Cancel Training
Memory Allocation
Example Documents
Memory Setting Medium
Memory Required 30 KB
New Documents
Upload Documents
Remove
Type
Document Name
Date
By
Positive MarketingNEW.zip 01/03/2010 05:50:34 Sarin
Positive ReleaseDates.xls 01/06/2010 12:00:12 Sarin
Negative TDtradeshowVendor.doc 01/06/2009 04:50:12 Sarin

图 7

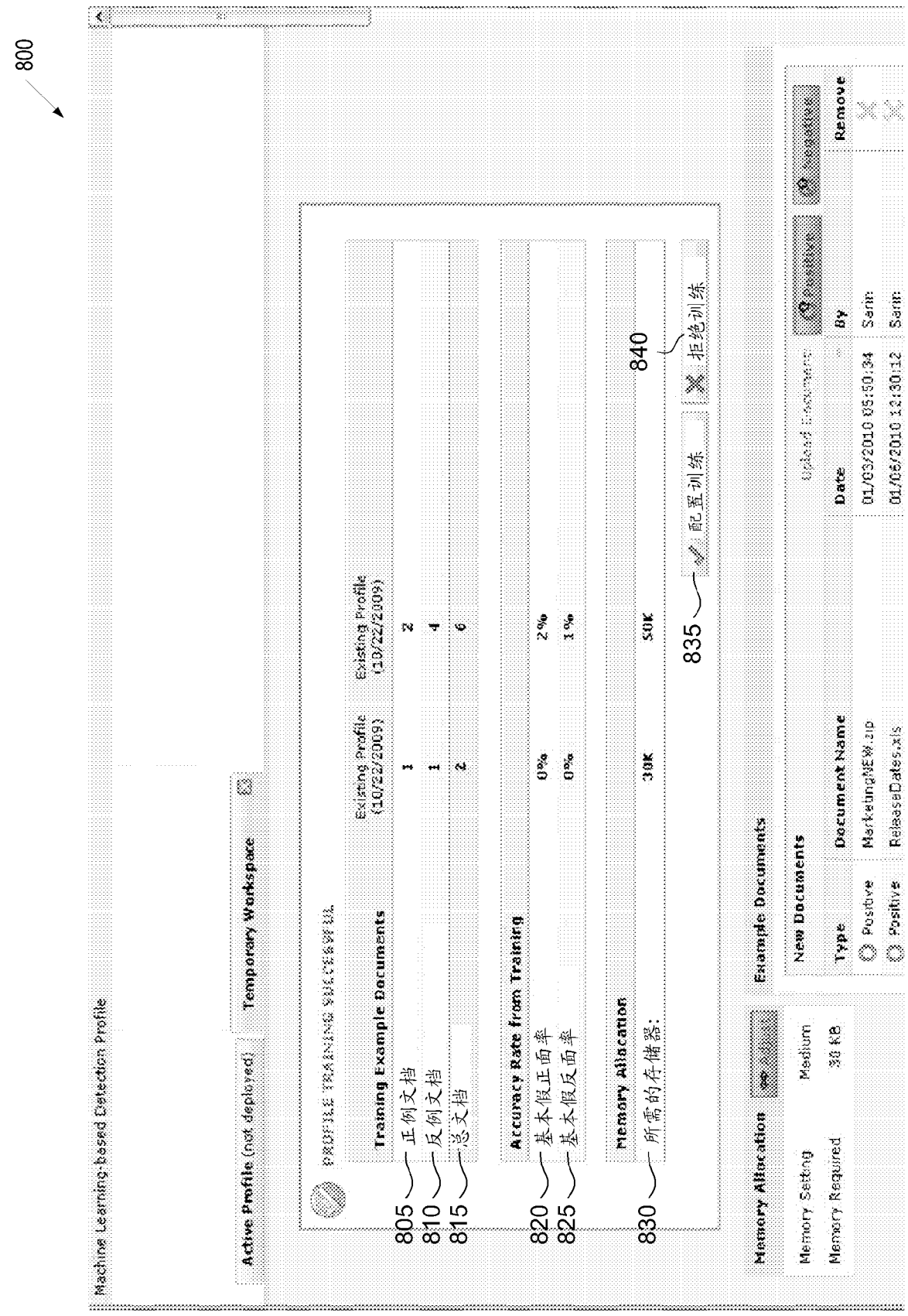

800
Machine Learning-based Detection Profile
Active Profile (not deployed)
Temporary Workspace
PROFILE TRAINING SUCCESSFUL
Training Example Documents
Existing Profile (10/22/2009)
Existing Profile (10/22/2009)
正例文档
反例文档
总文档
1
1
2
2
4
6
805
810
815
Accuracy Rate from Training
基本假正面率
基本假反面率
0%
0%
2%
1%
820
825
Memory Allocation
所需的存储器:
30K
50K
830
835
配置训练
拒绝训练
840
Memory Allocation
Medium
Memory Setting
Memory Required
New Documents
Example Documents
Upload Documents
Positive
Positive
Type
Document Name
MarketingNEW.zip
ReleaseDates.xls
Date
01/03/2010 05:50:34
01/05/2010 12:30:12
By
Sam
Sam
Remove

图 8

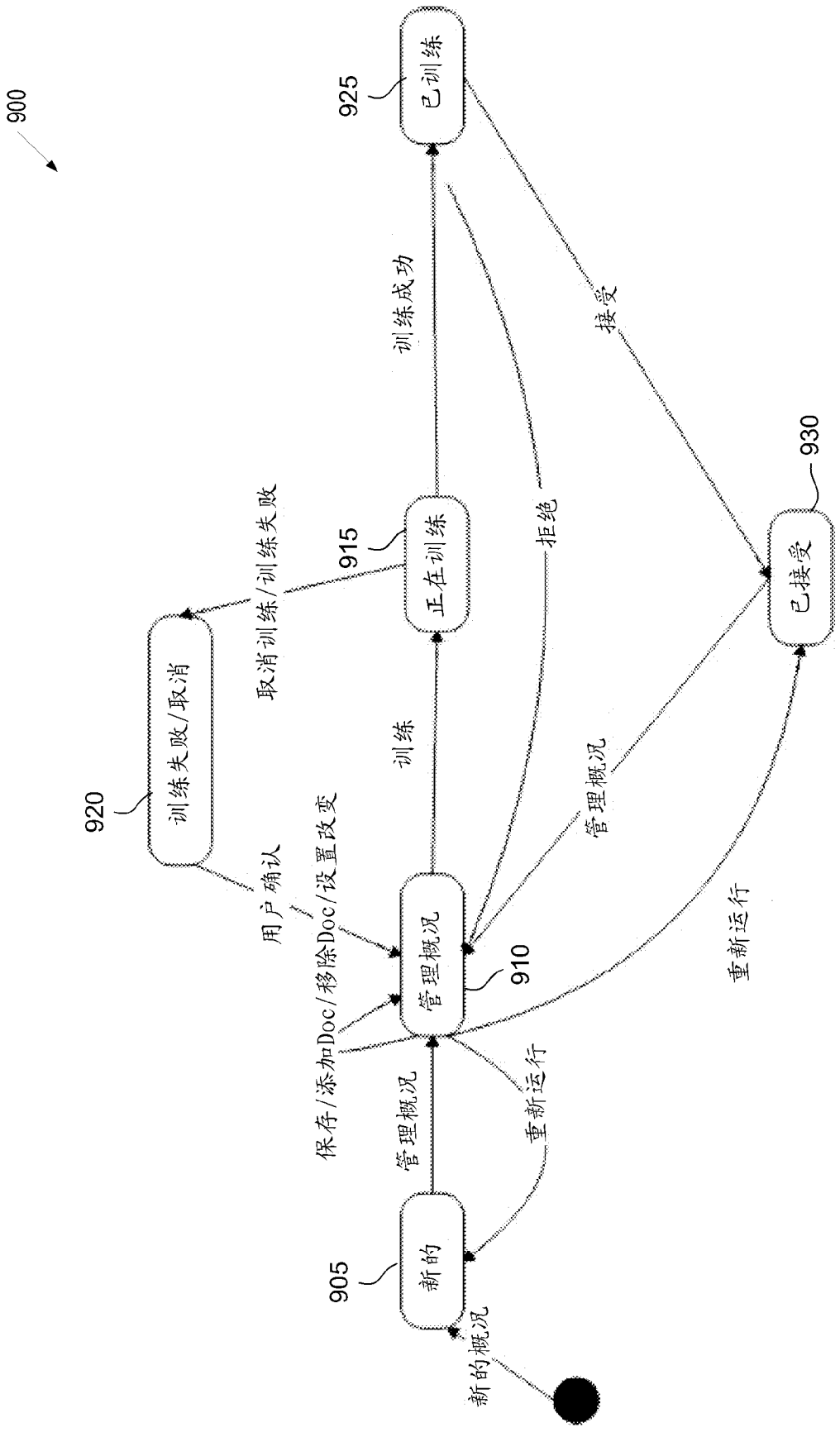

900
905
新的
910
管理概况
915
正在训练
920
训练失败/取消
925
已训练
930
已接受
新的概况
管理概况
保存/添加Doc/移除Doc/设置改变
重新运行
用户确认
取消训练/训练失败
训练
训练成功
拒绝
管理概况
接受
重新运行

图 9

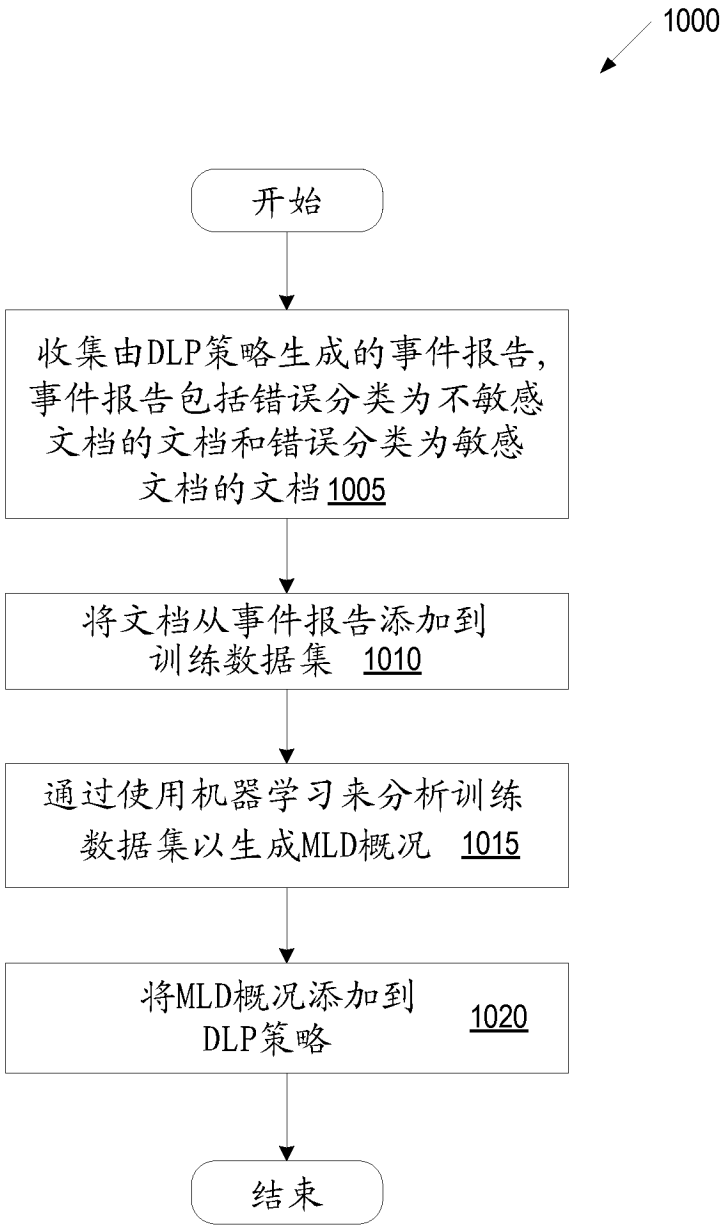

1000
开始
收集由DLP策略生成的事件报告，事件报告包括错误分类为不敏感文档的文档和错误分类为敏感文档的文档 1005
将文档从事件报告添加到训练数据集 1010
通过使用机器学习来分析训练数据集以生成MLD概况 1015
将MLD概况添加到DLP策略 1020
结束

图 10

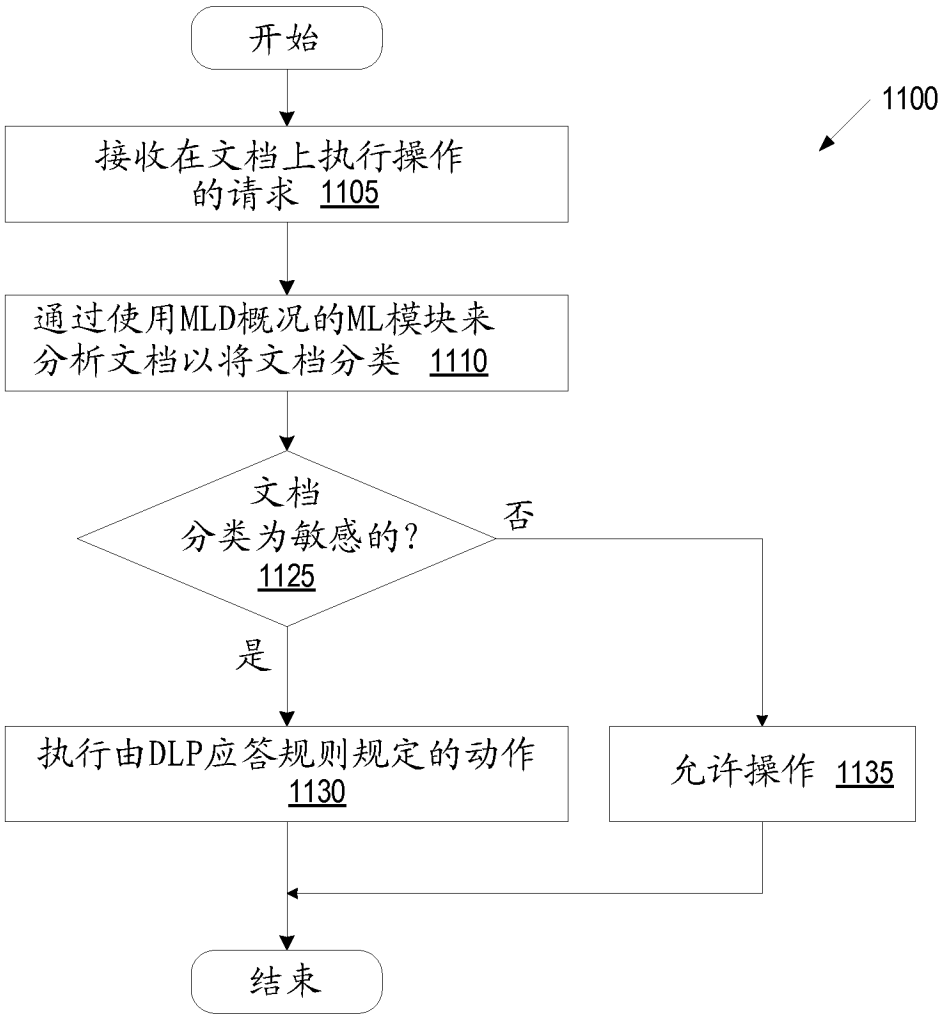

开始
1100
接收在文档上执行操作的请求 1105
通过使用MLD概况的ML模块来分析文档以将文档分类 1110
文档分类为敏感的? 1125
否
是
执行由DLP应答规则规定的动作 1130
允许操作 1135
结束

图 11

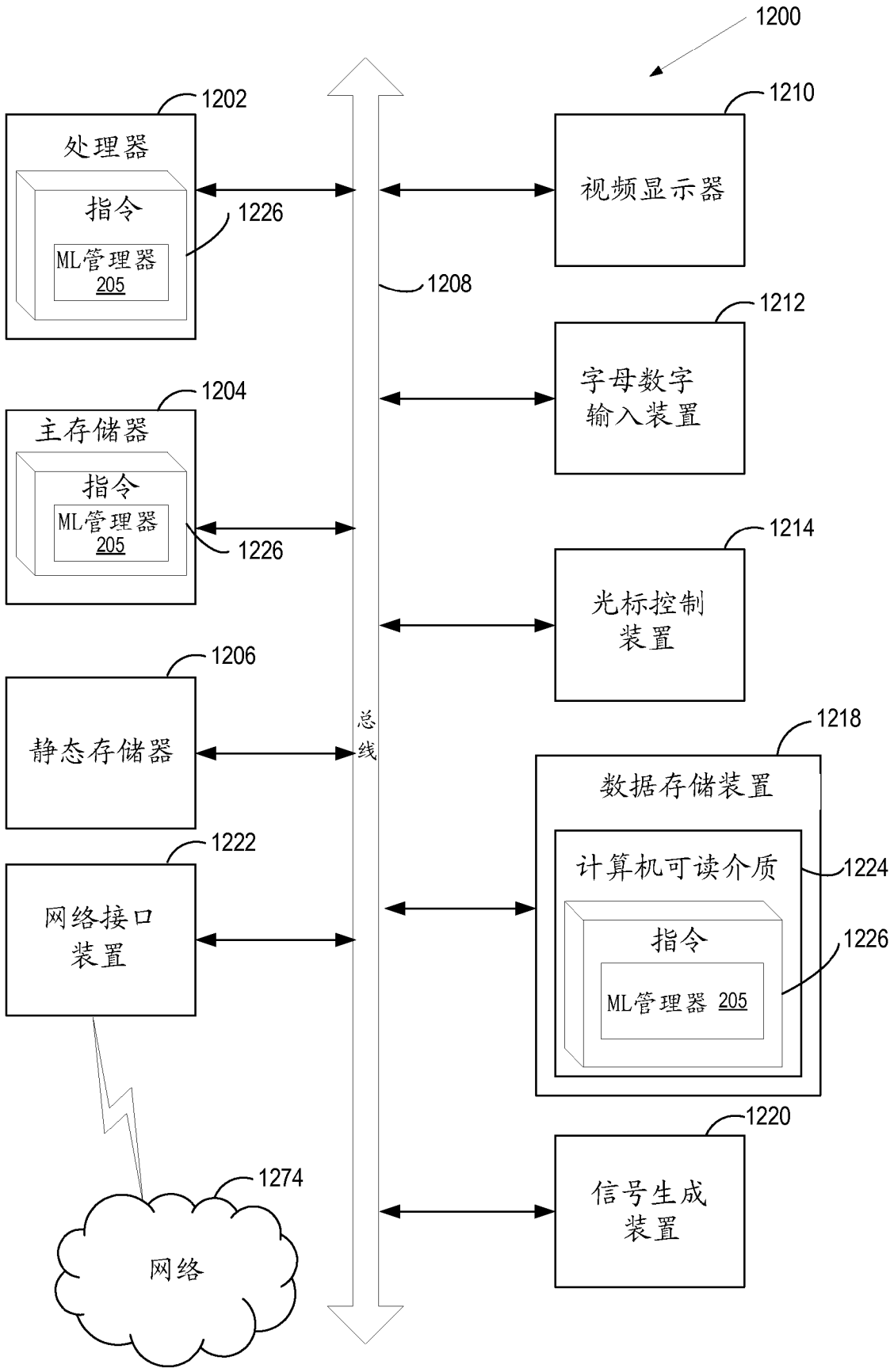

1200
1202
处理器
指令
ML管理器 205
1226
1210
视频显示器
1208
1212
字母数字输入装置
1204
主存储器
指令
ML管理器 205
1226
1214
光标控制装置
1206
静态存储器
总线
1218
数据存储装置
计算机可读介质
1224
指令
ML管理器 205
1226
1222
网络接口装置
1220
信号生成装置
1274
网络

图 12