[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
*G06F 17/30 (2006.01)*

[12] 发明专利说明书

专利号 ZL 00817894.1

[45] 授权公告日 2008 年 2 月 13 日

[11] 授权公告号 CN 100369037C

[22] 申请日 2000.11.28 [21] 申请号 00817894.1

[30] 优先权

[32] 1999.12.31 [33] KR [31] 1999/68606

[32] 2000. 3. 7 [33] KR [31] 2000/11282

[86] 国际申请 PCT/KR2000/001374 2000.11.28

[87] 国际公布 WO2001/050344 英 2001.7.12

[85] 进入国家阶段日期 2002.6.27

[73] 专利权人 INCA 网络有限公司

地址 韩国首尔

[72] 发明人 郑连燮

[56] 参考文献

US6006034A 1999.12.21

审查员 韩燕_2

[74] 专利代理机构 北京三友知识产权代理有限公司

代理人 李 辉

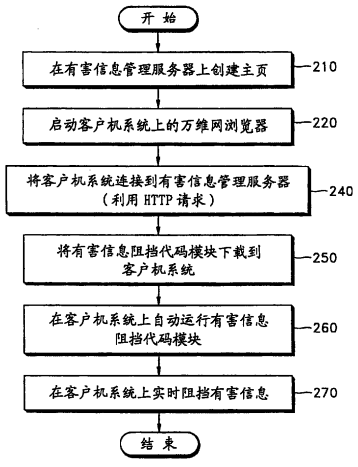
权利要求书 4 页 说明书 11 页 附图 6 页

[54] 发明名称

# 在线阻挡有害信息的系统和方法

[57] 摘要

本发明披露了一种通过将客户机与万维网服务器互相链接在一起的计算机网络对包括计算机病毒在内的有害信息进行在线诊断、排除和阻挡的系统和方法。 该方法包括：在将万维网服务器与客户机系统互相链接在一起的计算机网络上，万维网服务器通过计算机网络从客户机系统接收一个连接请求。 然后，万维网服务器将有害信息阻挡代码模块发送到客户机系统。 一旦完成发送有害信息阻挡代码模块，有害信息阻挡代码模块就自动在客户机系统上运行以实时阻挡包括计算机病毒在内的有害信息。 仅通过在线连接到有害信息管理服务器，可以将有害信息阻挡代码模块自动发送到并安装到客户机系统内，因此可以实时地主动阻挡客户机系统上检测到的有害信息，而无需手动安装过程。



1. 一种用于阻挡要被实时执行的文件中的有害信息的方法，该方法包括步骤：

（a）在将万维网服务器与客户机系统互相链接在一起的计算机网络上，万维网服务器通过计算机网络从客户机系统接收一个连接请求；

（b）万维网服务器将有害信息阻挡代码模块发送到客户机系统；以及

（c）一旦完成有害信息阻挡代码模块的发送，有害信息阻挡代码模块就自动在客户机系统上运行以实时阻挡包括计算机病毒在内的有害信息，

其中步骤（c）包括以下步骤：

（c1）通过跟踪文件 I/O 例程来检查客户机系统上的文件输入/输出（I/O）；

（c2）确定与在步骤（c1）检查的文件输入/输出对应的所述要被执行的文件是否有害；以及

（c3）对在步骤（c2）中被确定为有害的文件进行处理，并且如果所述文件可以被处理，则执行所述文件，而如果所述文件不能被处理，则终止执行所述文件。

2. 根据权利要求 1 所述的方法，其中在步骤（c3），如果不能对在步骤（c2）确定有害的文件进行处理，则将该文件发送到万维网服务器。

3. 根据权利要求 1 所述的方法，其中步骤（c3）包括请求客户机系统用户授权执行步骤（c3）的步骤。

4. 根据权利要求 1 所述的方法，其中步骤（c）还包括步骤：

（c4）检查客户机系统上的网络分组输入/输出（I/O）；

（c5）确定步骤（c4）检查的分组是否有害；以及

（c6）如果确定任何分组有害，则阻挡对该分组 I/O 分配的通信端口。

5. 根据权利要求 1 所述的方法，其中在步骤（c）执行的有害信息阻挡代码模块检验在客户机系统上运行的当前进程是否有害。

6. 根据权利要求 1 所述的方法，其中在步骤（c）执行的有害信息阻挡代

码模块将其运行状态显示在单独窗口内，并且在关闭该单独窗口时，终止执行此有害信息阻挡代码模块。

7. 根据权利要求 1 所述的方法，其中即使客户机系统访问另一个万维网服务器，仍可以在客户机系统上继续运行在步骤（c）执行的有害信息阻挡代码模块。

8. 一种用于阻挡要被实时执行的文件中的有害信息的方法，该方法包括步骤:

（a）在一个将第一万维网服务器、第二万维网服务器以及客户机系统互相链接在一起的计算机网络上，客户机系统通过计算机网络连接到第二万维网服务器;

（b）根据第二万维网服务器提供到客户机系统的信息，客户机系统通过计算机网络连接到第一万维网服务器;

（c）第一万维网服务器将有害信息阻挡代码模块发送到客户机系统；以及

（d）一旦完成有害信息阻挡代码模块的发送，就在客户机系统上自动运行有害信息阻挡代码模块以实时阻挡包括计算机病毒在内的有害信息，

其中步骤（d）包括以下步骤:

（d1）通过跟踪文件 I/O 例程来检查客户机系统上的文件输入/输出（I/O）;

（d2）确定与在步骤（d1）检查的文件输入/输出对应的所述要被执行的文件是否有害；以及

（d3）对在步骤（d2）中被确定为有害的文件进行处理，并且如果所述文件可以被处理，则执行所述文件，而如果所述文件不能被处理，则终止执行所述文件。

9. 根据权利要求 8 所述的方法，其中即使客户机系统访问另一个万维网服务器，仍在客户机系统上继续运行在步骤（d）执行的有害信息阻挡代码模块。

10. 一种用于阻挡要被实时执行的文件中的有害信息的在线业务提供方法，该方法包括步骤:

（a）通过一个将第一万维网服务器和客户机系统互相链接在一起的计算机网络，在第一万维网服务器上创建在线业务主页；

（b）通过计算机网络，第一万维网服务器从客户机系统接收一个连接请求；以及

（c）一旦第一万维网服务器将有害信息阻挡代码模块发送到客户机系统，在客户机系统上自动运行有害信息阻挡代码模块以实时阻挡包括计算机病毒在内的有害信息，

其中步骤（c）包括以下步骤：

（c1）通过跟踪文件 I/O 例程来检查客户机系统上的文件输入/输出（I/O）；

（c2）确定与在步骤（c1）检查的文件输入/输出对应的所述要被执行的文件是否有害；以及

（c3）对在步骤（c2）中被确定为有害的文件进行处理，并且如果所述文件可以被处理，则执行所述文件，而如果所述文件不能被处理，则终止执行所述文件。

11. 根据权利要求 10 所述的方法，其中在将客户机系统连接到与第一万维网服务器分离的第二万维网服务器后，根据第二万维网服务器提供的信息，客户机系统发出第一万维网服务器在步骤（b）接收的连接请求。

12. 根据权利要求 10 所述的方法，其中即使客户机系统访问另一个万维网服务器，仍在客户机系统上继续运行在步骤（c）发送的有害信息阻挡代码模块。

13. 一种用于阻挡要被实时执行的文件中的有害信息的系统，该系统包括：

第一万维网服务器，通过计算机网络提供在线业务；以及

客户计算机，通过计算机网络与第一万维网服务器链接，

其中在第一万维网服务器从客户机系统接收到连接请求时，第一万维网服务器将有害信息阻挡代码模块发送到客户计算机，并且在客户计算机上自动运行该有害信息阻挡代码模块以实时阻挡包括计算机病毒在内的有害信息，

并且其中有害信息阻挡模块通过跟踪文件 I/O 例程来检查客户机系统上的

文件输入/输出（I/O），以及

确定与检查的文件输入/输出对应的所述要被执行的文件是否有害；以及

对被确定为有害的文件进行处理，并且如果所述文件可以被处理，则执行所述文件，而如果所述文件不能被处理，则终止执行所述文件。

14. 根据权利要求13所述的系统，其中有害信息阻挡代码模块将其运行状态显示在单独窗口内，并且在关闭该单独窗口时，终止执行此有害信息阻挡代码模块。

15. 根据权利要求13所述的系统，该系统进一步包括通过计算机网络与客户计算机链接以通过计算机网络提供在线业务的第二万维网服务器，以及

其中在客户计算机通过计算机网络与第二万维网服务器相连时，第二万维网服务器将用于访问第一万维网服务器的超级链接信息提供到客户计算机。

16. 根据权利要求13所述的系统，其中即使客户计算机访问另一个万维网服务器，仍在客户计算机上继续运行有害信息阻挡代码模块。

# 在线阻挡有害信息的系统和方法

## 技术领域

本发明涉及计算机安全系统，更具体地说，本发明涉及通过一个把客户机链接到万维网服务器的计算机网络对包括计算机病毒在内的有害信息进行在线诊断、排除和阻挡的系统和方法。

## 背景技术

随着计算机网络技术，特别是万维网（“Web”）技术的发展，计算机网络的用户数量，特别是因特网用户数量在急剧增加。现在，因特网不再属于虚拟空间内的新技术和业务领域，而是正在走入人们的现实生活中。因特网上出现的商业数量在不断增长，例如，购物、拍卖、银行业务、以及广告业务。现在，计算机用户通常通过因特网访问各种信息，并进行各种经济活动。

因特网在许多方面方便了计算机用户。另一方面，由于与计算机和因特网有关的技术在不断增长，所以对通过计算机网络非法获取个人信息的高度可能性或由各种计算机病毒引起的损失的关注也在迅速提高。由诸如计算机病毒的有害信息引起的损失会很严重。根据报道，在 1999 年的上半年，在世界范围内，由计算机病毒引起的的损失比 1998 年的 25 亿美元增长了 3 倍，已经达到 76 亿美元。

例如，Chernobyl（CIH）病毒是一种高危险计算机病毒，它可以破坏硬盘内的所有数据，并且在包括韩国在内的世界范围内，引起严重损失。最近，在因特网上新出现了诸如 Back Orifice 病毒或 School Bus 病毒的有害信息，这种病毒将可以遥控一个计算机的“间谍”文件与其它计算机病毒一起嵌入计算机从而从计算机上非法获取个人信息。

防护各种有害信息的现有对抗方案基于先损失/后维修策略。在计算机系统已经受到未识别的有害信息破坏之后，再采取措施（例如，适当抗病毒程序的跟踪开发），因此这种防护对抗方案处于被动位置。该防护策略的另一个缺陷在于，需要将防止有害信息的各种抗病毒程序手动安装到单独个人计算机上，这是一种低效过程，使得计算机用户增加了安装抗病毒程序的过重负担。此外，由于各种有害信息总是通过因特网快速创建和传播，所以难于始终为计算机配备最新版抗病毒程序。

因此，如果新型有害信息（例如还没有开发出相应的适当抗病毒程序的新计算机病毒种类）侵入用户计算机，显然这种新型计算机病毒会破坏此计算机系统，或者从计算机系统内非法获取个人信息。此外，每当发现未识别的计算机病毒时，用户还必须访问有害信息相关业务提供商或在线通信公司以获得最新版抗病毒程序。此外，下载最新版抗病毒程序后还要进行手动安装，这是一种劳动强度高的不必要完成的任务。

防止用户计算机受到有害信息破坏的现有对抗方案没有提供将有害信息的出现或由有害信息引起的损失有效地报告有害信息相关业务提供商的通信渠道，因此有害信息相关业务提供商不能获得关于有害信息的分布和由有害信息引起的损失的统计数据及其系统数据分析。

## 发明内容

为了解决上述问题，本发明的第一个目的是提供一种在线阻挡有害信息的系统和方法，利用在通过一个计算机网络接入万维网服务器后自动发送和安装在客户机系统中的有害信息阻挡程序，可以使客户机系统主动阻挡有害信息，并且可以实时检查客户机系统上的文件输入/输出（I/O）或网络分组I/O。

本发明的第二个目的是提供一种利用一个计算机网络的万维网服务器提供在线阻断有害信息的业务的方法。

本发明的第三个目的是提供一种用于存储有害信息阻挡程序的计算机可读

介质。

根据本发明的一个方面，提供一种用于阻挡要被实时执行的文件中的有害信息的方法，该方法包括步骤：

（a）在将万维网服务器与客户机系统互相链接在一起的计算机网络上，万维网服务器通过计算机网络从客户机系统接收一个连接请求；

（b）万维网服务器将有害信息阻挡代码模块发送到客户机系统；以及

（c）一旦完成有害信息阻挡代码模块的发送，有害信息阻挡代码模块就自动在客户机系统上运行以实时阻挡包括计算机病毒在内的有害信息，

其中步骤（c）包括以下步骤：

（c1）通过跟踪文件 I/O 例程来检查客户机系统上的文件输入/输出（I/O）；

（c2）确定与在步骤（c1）检查的文件输入/输出对应的所述要被执行的文件是否有害；以及

（c3）对在步骤（c2）中被确定为有害的文件进行处理，并且如果所述文件可以被处理，则执行所述文件，而如果所述文件不能被处理，则终止执行所述文件。

根据本发明的另一个方面，提供一种用于阻挡要被实时执行的文件中的有害信息的方法，该方法包括步骤：

（a）在一个将第一万维网服务器、第二万维网服务器以及客户机系统互相链接在一起的计算机网络上，客户机系统通过计算机网络连接到第二万维网服务器；

（b）根据第二万维网服务器提供到客户机系统的信息，客户机系统通过计算机网络连接到第一万维网服务器；

（c）第一万维网服务器将有害信息阻挡代码模块发送到客户机系统；以及

（d）一旦完成有害信息阻挡代码模块的发送，就在客户机系统上自动运行有害信息阻挡代码模块以实时阻挡包括计算机病毒在内的有害信息，

其中步骤（d）包括以下步骤：

（d1）通过跟踪文件 I/O 例程来检查客户机系统上的文件输入/输出（I/O）；

（d2）确定与在步骤（d1）检查的文件输入/输出对应的所述要被执行的文件是否有害；以及

（d3）对在步骤（d2）中被确定为有害的文件进行处理，并且如果所述文件可以被处理，则执行所述文件，而如果所述文件不能被处理，则终止执行所述文件。

根据本发明另一个方面，提供一种用于阻挡要被实时执行的文件中的有害信息的在线业务提供方法，该方法包括步骤：

（a）通过一个将第一万维网服务器和客户机系统互相链接在一起的计算机网络，在第一万维网服务器上创建在线业务主页；

（b）通过计算机网络，第一万维网服务器从客户机系统接收一个连接请求；以及

（c）一旦第一万维网服务器将有害信息阻挡代码模块发送到客户机系统，在客户机系统上自动运行有害信息阻挡代码模块以实时阻挡包括计算机病毒在内的有害信息，

其中步骤（c）包括以下步骤：

（c1）通过跟踪文件 I/O 例程来检查客户机系统上的文件输入/输出（I/O）；

（c2）确定与在步骤（c1）检查的文件输入/输出对应的所述要被执行的文件是否有害；以及

（c3）对在步骤（c2）中被确定为有害的文件进行处理，并且如果所述文件可以被处理，则执行所述文件，而如果所述文件不能被处理，则终止执行所述文件。

根据本发明另一个方面，提供一种用于阻挡要被实时执行的文件中的有害信息的系统，该系统包括：

第一万维网服务器，通过计算机网络提供在线业务；以及

客户计算机，通过计算机网络与第一万维网服务器链接，

其中在第一万维网服务器从客户机系统接收到连接请求时，第一万维网服务器将有害信息阻挡代码模块发送到客户计算机，并且在客户计算机上自动运行该有害信息阻挡代码模块以实时阻挡包括计算机病毒在内的有害信息，

并且其中有害信息阻挡模块通过跟踪文件 I/O 例程来检查客户机系统上的文件输入/输出（I/O），以及

确定与检查的文件输入/输出对应的所述要被执行的文件是否有害；以及

对被确定为有害的文件进行处理，并且如果所述文件可以被处理，则执行所述文件，而如果所述文件不能被处理，则终止执行所述文件。

## 附图说明

图 1A 和图 1B 示出用于实现本发明的各系统的原理图；

图 2A 和图 2B 示出根据本发明用于在线阻挡有害信息的方法的优选实施例的流程图；

图 3 示出本发明采用的有害信息阻挡代码模块的实例配置原理图；以及

图 4 示出图 3 所示的有害信息阻挡代码模块运行过程的流程图。

## 实现本发明的最佳方式

如图 1A 所示，图 1A 示出可以实现本发明优选实施例的系统，有害信息管理服务器 110 是一个万维网服务器，它具有主页，并通过诸如因特网的计算机网络与客户计算机 130 相连。

有害信息管理服务器 110 提供在线业务，以将能够实时阻挡有害信息的有害信息阻挡代码模块提供到客户计算机 130。术语“有害信息”是对计算机系统和/或计算机网络产生不利影响的令人讨厌的对象或行为的总称，包括：计算机病毒、因特网上的令人讨厌的黄色网站以及非法获取个人信息的行为。

图 2A 示出图 1A 所示系统的运行过程。现在，参考图 2A 说明根据本发明在线阻挡有害信息的方法的第一实施例。

该方法从在有害信息管理服务器 110 上创建在线业务主页开始(步骤 210)。计算机用户启动客户计算机(以下简称“客户机”)130 上的万维网浏览器(步骤 220)。在客户机 130 与有害信息管理服务器 110 相连时(步骤 240),有害信息管理服务器 110 将有害信息阻挡代码模块发送到客户机 130(步骤 250)。

对于这种情况,利用超文本传输协议格式化的请求(HTTP 请求)实现客户机 130 与有害信息管理服务器 110 之间的连接,并利用 HTTP 响应,将有害信息阻挡代码模块从有害信息管理服务器 110 发送到客户机 130。通常,通过键入有害信息管理服务器 110 的统一资源定位符(URL)或者点击万维网浏览器上与该 URL 有关的超级链接,执行该 HTTP 请求。

有害信息阻挡代码模块优选是运行在客户机 130 上的可执行应用程序。例如,有 Microsoft Corporation 开发的、应用于 Window 环境下的 ActiveX™控件,以及 Java™小应用程序和 JavaScrip™,万维网浏览器可以执行它们。另选地,还可以将利用高级语言设计的目标编码程序链接到万维网浏览器来运行。

优选与一个为用户界面提供的独立窗口一起执行有害信息阻挡代码模块,并在独立窗口内显示有害信息阻挡代码模块的状态报告。以此方式,在将客户机 130 链接到有害信息管理服务器 110 上后,有害信息管理服务器 110 首先提供一个使得能够创建一独立窗口的 HTTP 响应,然后,根据客户机 130 发送的 HTTP 请求,提供有害信息阻挡代码模块作为 HTTP 响应。在关闭窗口时,终止执行有害信息阻挡代码模块。除了显示有害信息阻挡代码模块的运行状态之外,为用户界面提供的独立窗口可以应用于多种目的。例如,在独立窗口内可以显示各种新闻或标题广告。

在完成有害信息阻挡代码模块的传输时,在客户机 130 上自动执行有害信息阻挡代码模块(步骤 260)并实时阻挡包括计算机病毒在内的有害信息(步骤 270)。由于在客户机 130 上实时运行有害信息阻挡代码模块,所以除非关闭状态显示窗口,否则即使在客户机 130 试图链接到另一个万维网服务器上时,客户机 130 仍将继续运行有害信息阻挡代码模块。因此,通过到有害信息管理服

务器 110 的单个连接，可以为客户机 130 提供有害信息阻挡业务从而实现安全。

在说明有害信息阻挡代码模块的原理之前，先说明参考图 1A 说明的实施例的变换例（以下简称“第二实施例）。图 1B 示出应用于根据本发明第二实施例的系统配置，图 2B 示出根据本发明在线阻挡有害信息的方法的第二实施例的流程图。

如图 1B 所示，除了有害信息管理服务器 110 之外，该系统进一步包括万维网服务器 120（以下简称“第二万维网服务器”）用于通过网络提供在线业务。第二万维网服务器 120 是通过诸如因特网的计算机网络与客户机系统链接的通用万维网服务器。

在本实施例中，参考图 2B，以参考图 2A 说明的第一实施例的同样方式执行步骤 210 和步骤 220。接着，客户机 130 首先访问第二万维网服务器 120（步骤 230）。

由于第二万维网服务器 120 将用于访问有害信息管理服务器 110 的超级链接信息以及与在线业务有关的信息提供到客户机 130（步骤 235），所以超级链接信息优选不是有害信息管理服务器 110 标题主页的链接信息，而是直接使客户机 130 通过单独窗口从有害信息管理服务器 110 接收有害信息阻挡代码模块的链接信息。

接着，根据第二万维网服务器 120 提供的超级链接信息，客户机 130 对有害信息管理服务器 110 进行 HTTP 请求（步骤 245）。根据客户机 130 发出的 HTTP 请求，有害信息管理服务器 110 发送有害信息阻挡代码模块作为 HTTP 响应（步骤 255）。

与在第一实施例中相同，在完成有害信息阻挡代码模块的传输时，在客户机 130 上自动执行有害信息阻挡代码模块（步骤 260），并实时阻挡诸如计算机病毒的有害信息（步骤 270）。

现在将更详细说明有害信息阻挡代码模块。图 3 示出本发明采用的有害信息阻挡代码模块的实例配置，图 4 示出图 3 所示有害信息阻挡代码模块运行过

程的流程图。

如图 3 所示，有害信息阻挡代码模块包括：输入/输出管理单元 310、有害信息阻挡单元 320 以及信息传输单元 330。如上所述，有害信息阻挡代码模块涉及在用于显示其运行状态的单独窗口 340，并且在关闭单独窗口 340 后，终止执行有害信息阻挡代码模块。

输入/输出管理单元 310 检查客户机 130 上的文件输入/输出（I/O）。该文件 I/O 检查是指通过跟踪文件 I/O 例程来获得文件信息。输入/输出管理单元 310 还优选检查客户机 130 上的网络分组 I/O，从而阻挡来自网络的有害信息。通过检验文件 I/O 或如下所述的检验进程可以阻挡非法获取个人信息的计算机病毒，例如 Back Orifice 病毒。输入/输出管理单元 310 优选进一步具有监视客户机 130 试图访问的任何因特网地址的功能，这样可以防止计算机用户访问令人讨厌的黄色网站。

有害信息阻挡单元 320 诊断文件或分组是否有害，并且如果文件或分组有害，则采取适当排除行动。信息传输单元 330 将确定有害的文件或分组的信息通知有害信息管理服务器 110。

在有害信息阻挡代码模块的运行过程中，参考图 4，在客户机 130 上自动执行的有害信息阻挡代码模块首先检查客户机 130 上当前运行的进程是否有害（步骤 410）。这是因为存储器内的当前进程会影响所有未来进程。其另一个原因是，能够从系统非法获取个人信息的 Back Orifice 病毒以进程的形式运行，并且可以使外部计算机系统远程控制一个用户计算机。

检验进程是否有害的方法包括对载入存储器内的正在进行的进程列表，并检验对应于每个进程的文件是否有害。如果确定文件有害，则确定相应进程为有害进程并终止此进程。显然，还可以对相应有害文件进行适当处理。在检测到有害信息之后并且在进行适当处理之前，有害信息阻挡代码模块最好通知用户出现了有害信息，并请求用户授权采取排除行动。

接着，有害信息阻挡代码模块检查客户机 140 上的每个文件 I/O（步骤 420）。

如上所述，通过跟踪文件 I/O 例程，执行文件 I/O 检查。例如，可以跟踪 VxD（在 Windows 环境下运行的 I/O 例程）来进行检查。

在步骤 420，可以检查网络分组 I/O 以及文件 I/O 以阻挡由网络侵入的有害信息，这在前面也已经描述。通过跟踪套接字 I/O 例程（例如：Windows 环境下的所谓“Winsock 模块”），执行网络分组 I/O 检查。

此外，如上所述，在步骤 420，进一步对客户机 130 要访问的任何因特网地址进行监视，这样可以防止访问令人讨厌的黄色网站。通过检验 HTTP 请求消息或域命名服务（DNS）查看消息的首部，可以实现这种用于防止令人讨厌的访问的监视。

换句话说，步骤 420 可以包括对客户机 130 上可能存在的有害信息进行检验的附加功能。现在，将参考文件 I/O 检查，说明有害信息阻挡代码模块的后续操作，然而，仅以文件 I/O 检查作为一个例子，对本发明范围没有限制意义。

接着，确定在步骤 420 监视的文件是否有害（步骤 430）。根据有害信息的类型或应用的必要性，可以利用各种方法实现此确定过程。例如，为了实现此确定过程，可以进行与已知有害信息（例如：被识别的计算机病毒）的模式比较过程。总之，因为计算机病毒在预定模式下运行，所以可以将模式比较技术作为识别新型病毒的工具。

在步骤 430，最好对网络分组是否有害，或者客户机 130 是否试图访问令人讨厌的黄色网站进行确定。

如果确定监视的信息安全，有害信息阻挡代码模块不对该文件进行规定的处理。因此，允许用户在客户机 130 上继续他或她的工作，而不考虑有害信息阻挡代码模块。

如果确定监视的信息有害，则进一步确定监视的信息是否与文件 I/O 或分组 I/O 有关以对有害文件或有害分组进行适当处理。尽管在图 4 中未示出，但是对于阻挡访问令人讨厌的黄色网站的过程，可以对一个 HTTP 请求消息进行重组以将客户机 130 引导到对用户有益的希望网站。

在监视的信息与文件 I/O 有关的情况下，确定是否可以对有害文件进行适当处理（步骤 450）。如果可以进行处理，则对有关文件进行处理（步骤 454）。如果不可能进行处理，则仅终止执行相应文件（步骤 452）。在步骤 454，最好通知用户检测到有害信息，并且请求授权对该有害信息进行处理。

最后，如果从客户机 130 在线检测到指示有害信息的信息，则最好利用有害信息阻挡代码模块通知有害信息管理服务器 110（步骤 470）。如果检测到的信息是新型有害信息并且因此不能进行处理，则最好将与未识别的有害信息有关的整个文件发送到有害信息管理服务器 110。当然，最好得到向有害信息管理服务器 110 通知检测到有害信息和/或将未识别有害信息文件发送到有害信息管理服务器 110 的预先授权。

换句话说，本实施例提供自动将在客户机 130 检测到有害信息的信息提供到有害信息管理服务器 110 的功能。因此，可以使有害信息管理服务器 110 获得有害信息的统计数据，并且例如通过开发有效抗病毒程序，可以立即对抗出现的未识别计算机病毒。以此方式，有害信息管理服务器 110 对来自客户机 130 的未识别有害信息进行分析以开发适当处理程序，并利用最新版有害信息阻挡代码模块提供适当安全服务以阻挡有害信息攻击客户机 130。因此，本发明可以防止运行于公开网络环境中的用户计算机被各种有害信息破坏。

在本实施例中，有害信息阻挡代码模块将有害信息自动发送到有害信息管理服务器 110 所使用的通信信道，可以利用因特网邮件传输协议（例如：简单邮件传输协议（SMTP），或文件传输协议（FTP））实现。更优选地，设置专门用于传输有害信息的指定通信信道。

与此同时，如果在步骤 440 确定有害信息与分组 I/O 有关，则阻挡对分组 I/O 分配的通信端口（步骤 460）。如果正在执行通过通信信道支持网络分组 I/O 的内部进程，则最好终止这些进程。

接着，与对与文件 I/O 有关的有害信息进行处理的类似方式，对通过通信端口侵入的有害信息进行适当处理（步骤 462）。在步骤 470，通知有害信息管

理服务器 110 从网络分组 I/O 检测到了有害信息。

可以将本实施例作为计算机可读程序码来实现。通过运行计算机可读介质内的程序，可以将本发明在通用数字计算机中实施，计算机可读介质包括但并不局限于磁性存储介质（例如：ROM、软盘、硬盘等）、光可读介质（例如：CD-ROM、DVD 等）以及载波（例如：通过因特网传输）。

尽管参考本发明的优选实施例对本发明进行了说明和描述，但是，显然，在所附权利要求所述的本发明实质范围内，本技术领域内的熟练技术人员可以在形式和细节方面对其进行变更。应该将这些实施例理解为是对本发明的解释，而非对本发明范围的限定。因此，不是由上述说明，而是由所附权利要求限定本发明范围。

**工业应用**

如上所述，根据本发明，仅通过在线连接到有害信息管理服务器，可以将有害信息阻挡代码模块自动提供到并安装到客户机系统内，因此可以实时地主动阻挡客户机系统上检测到的有害信息，而无需手动安装过程。

有害信息阻挡代码模块具有将指示在客户机系统内检测到未识别计算机病毒的信息通知有害信息管理服务器的功能。因此，有害信息管理服务器可以获得与有害信息有关的实用统计数据，并保持最新版的有害信息阻挡代码模块，这样可以对用户计算机提供最新安全服务。

此外，有害信息阻挡代码模块还可以检查网络分组 I/O，这样可以保证通过因特网实现安全电子商务。具体地说，对于私营企业或政府机构，本发明可以主动有效地防止商业信息，或与国家安全有关的机要信息免受各种有害信息的破坏。本发明在安全和效率方面均可行。

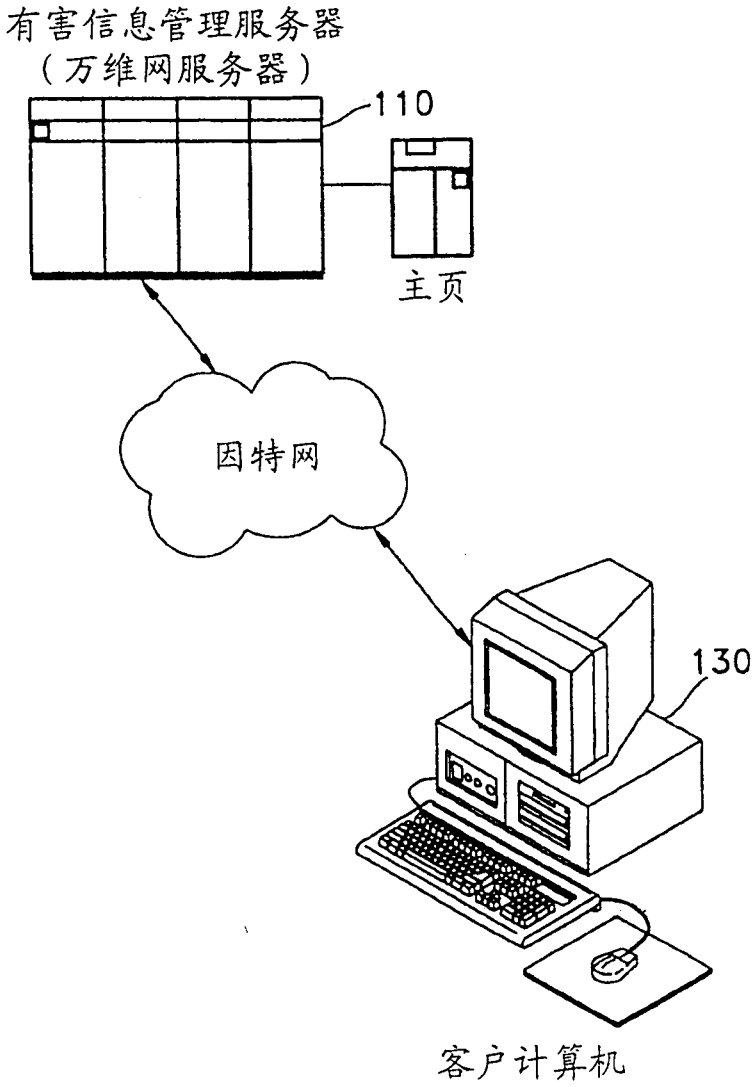



图 1A

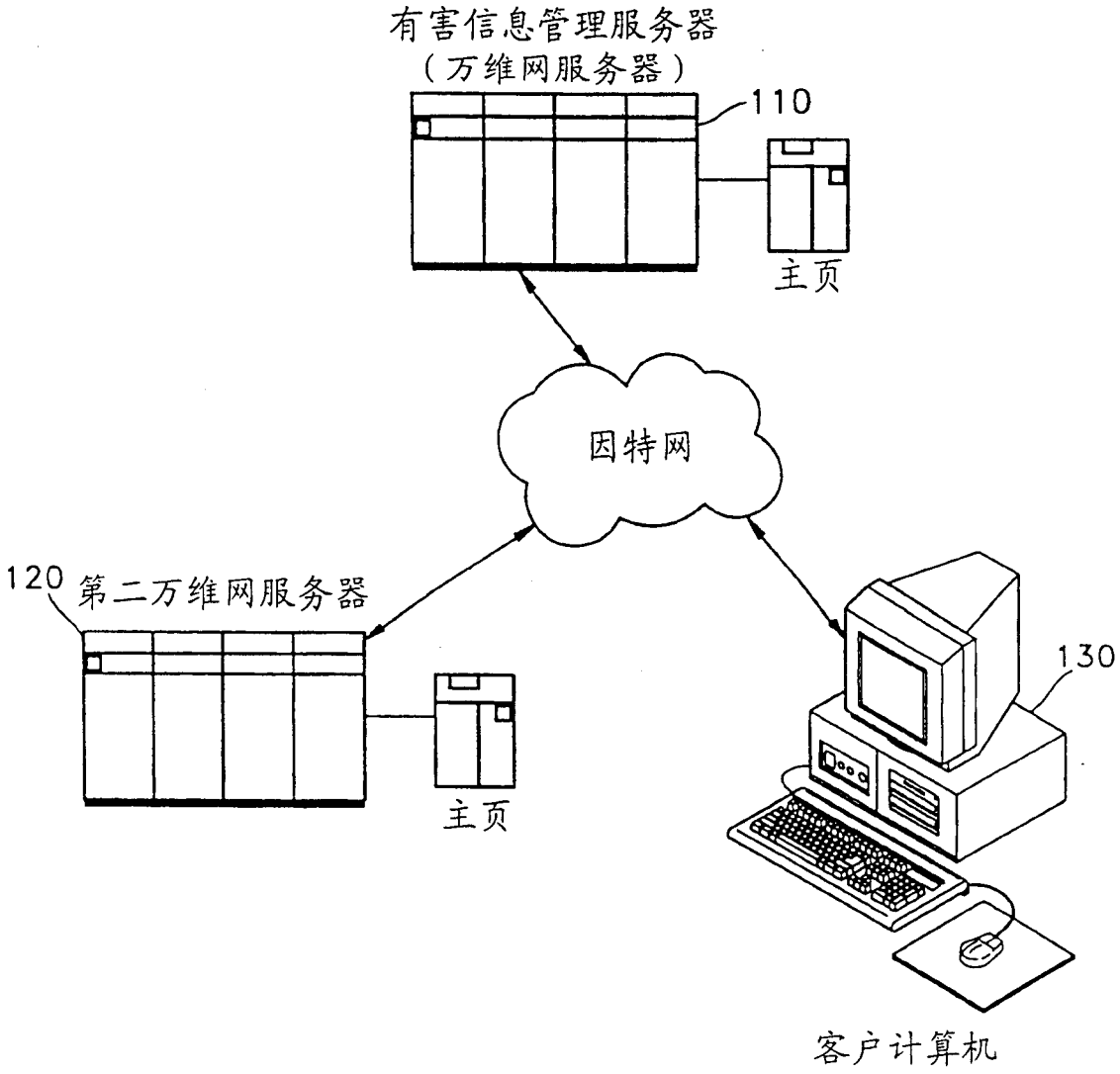



图 1B

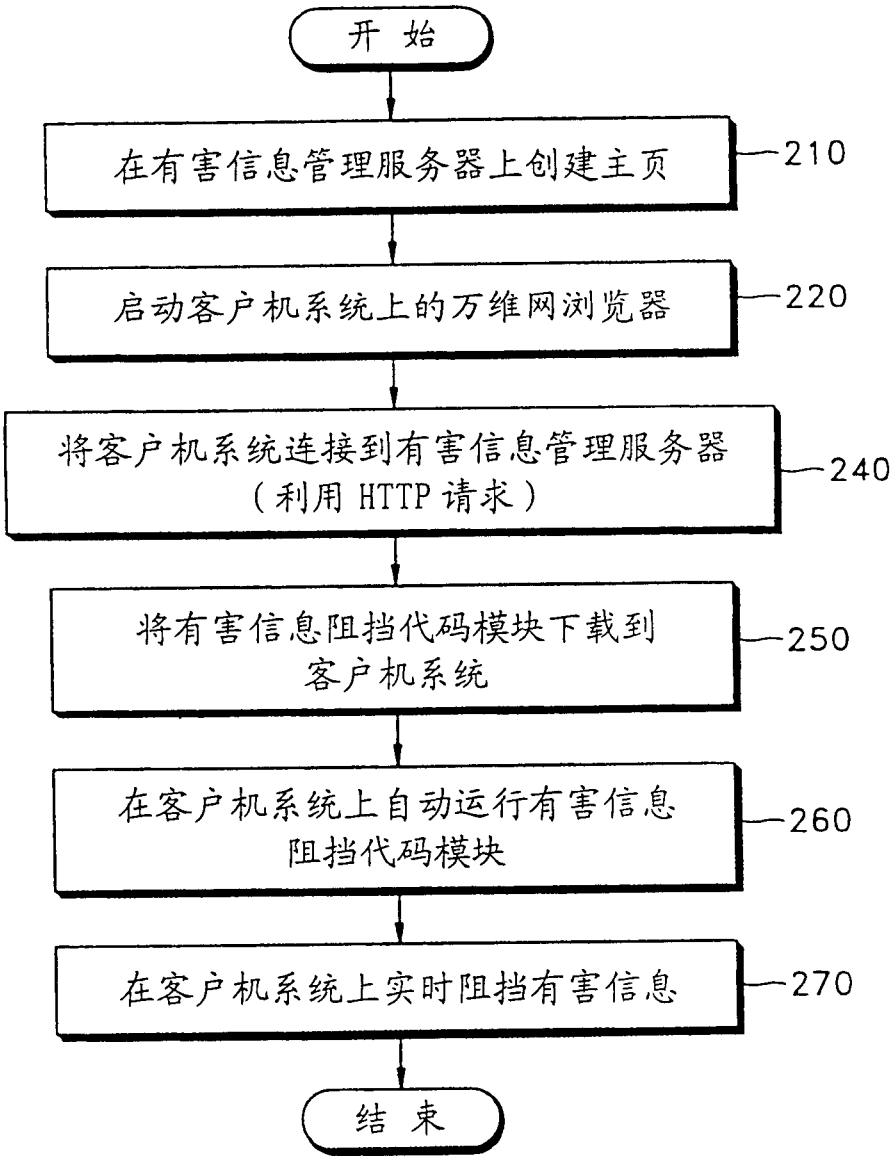

开 始
在有害信息管理服务器上创建主页
210
启动客户机系统上的万维网浏览器
220
将客户机系统连接到有害信息管理服务器
（利用 HTTP 请求）
240
将有害信息阻挡代码模块下载到
客户机系统
250
在客户机系统上自动运行有害信息
阻挡代码模块
260
在客户机系统上实时阻挡有害信息
270
结 束

图 2A

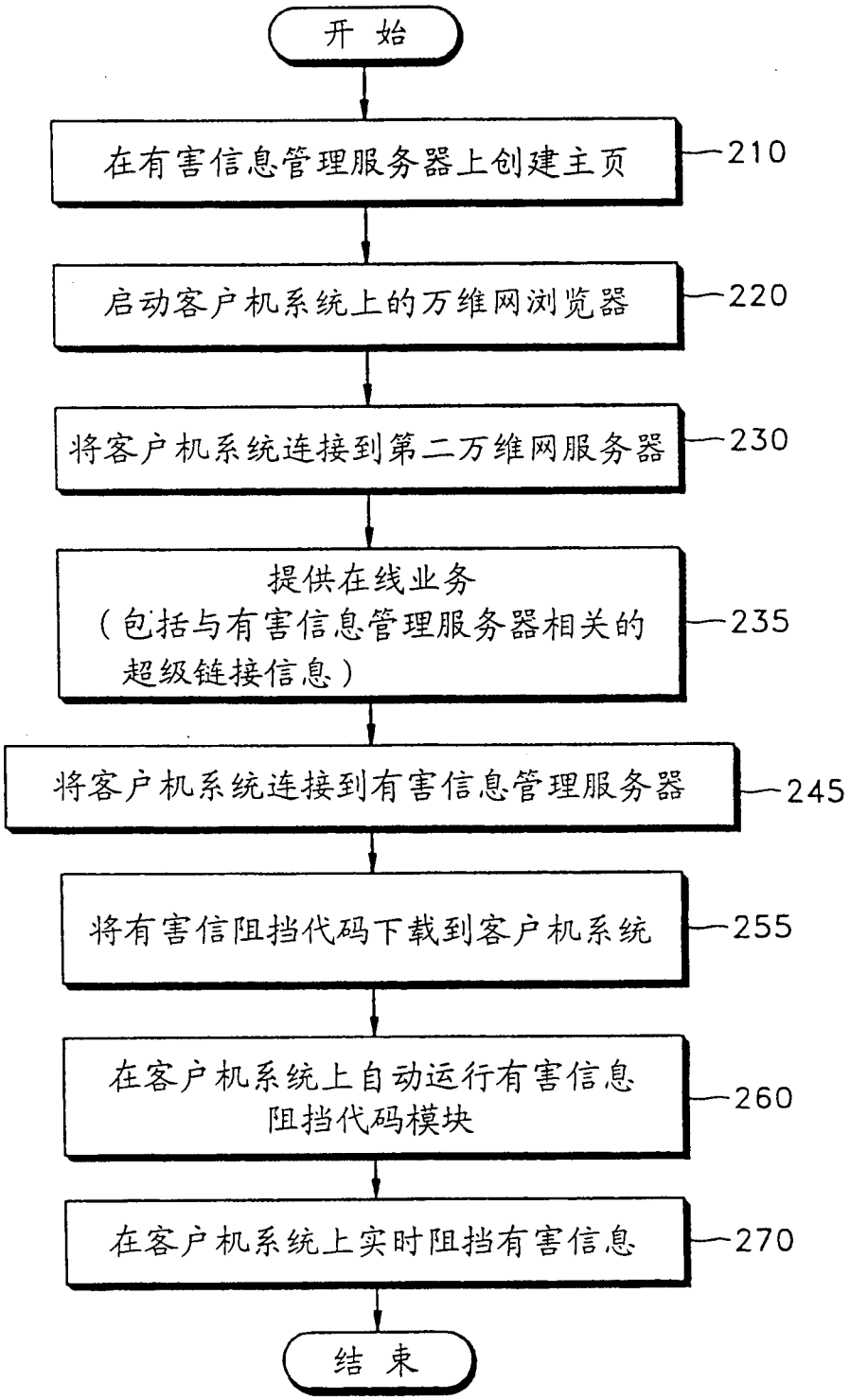

开 始
在有害信息管理服务器上创建主页
210
启动客户机系统上的万维网浏览器
220
将客户机系统连接到第二万维网服务器
230
提供在线业务
（包括与有害信息管理服务器相关的
超级链接信息）
235
将客户机系统连接到有害信息管理服务器
245
将有害信阻挡代码下载到客户机系统
255
在客户机系统上自动运行有害信息
阻挡代码模块
260
在客户机系统上实时阻挡有害信息
270
结 束

图 2B

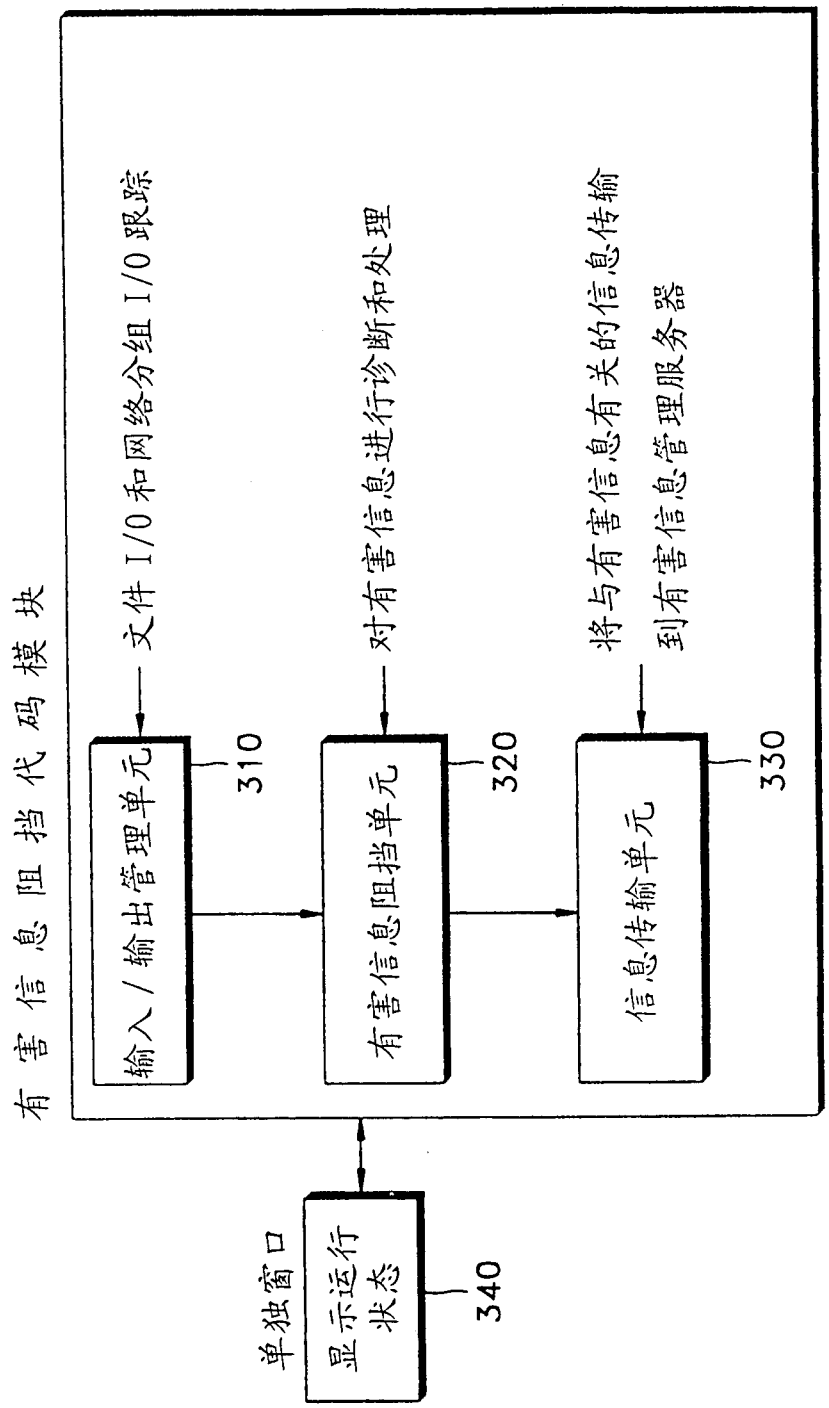

有害信息阻挡代码模块
输入/输出管理单元
310
文件I/O和网络分组I/O跟踪
有害信息阻挡单元
320
对有害信息进行诊断和处理
信息传输单元
330
将与有害信息有关的信息传输到有害信息管理服务器
单独窗口
显示运行状态
340

图 3

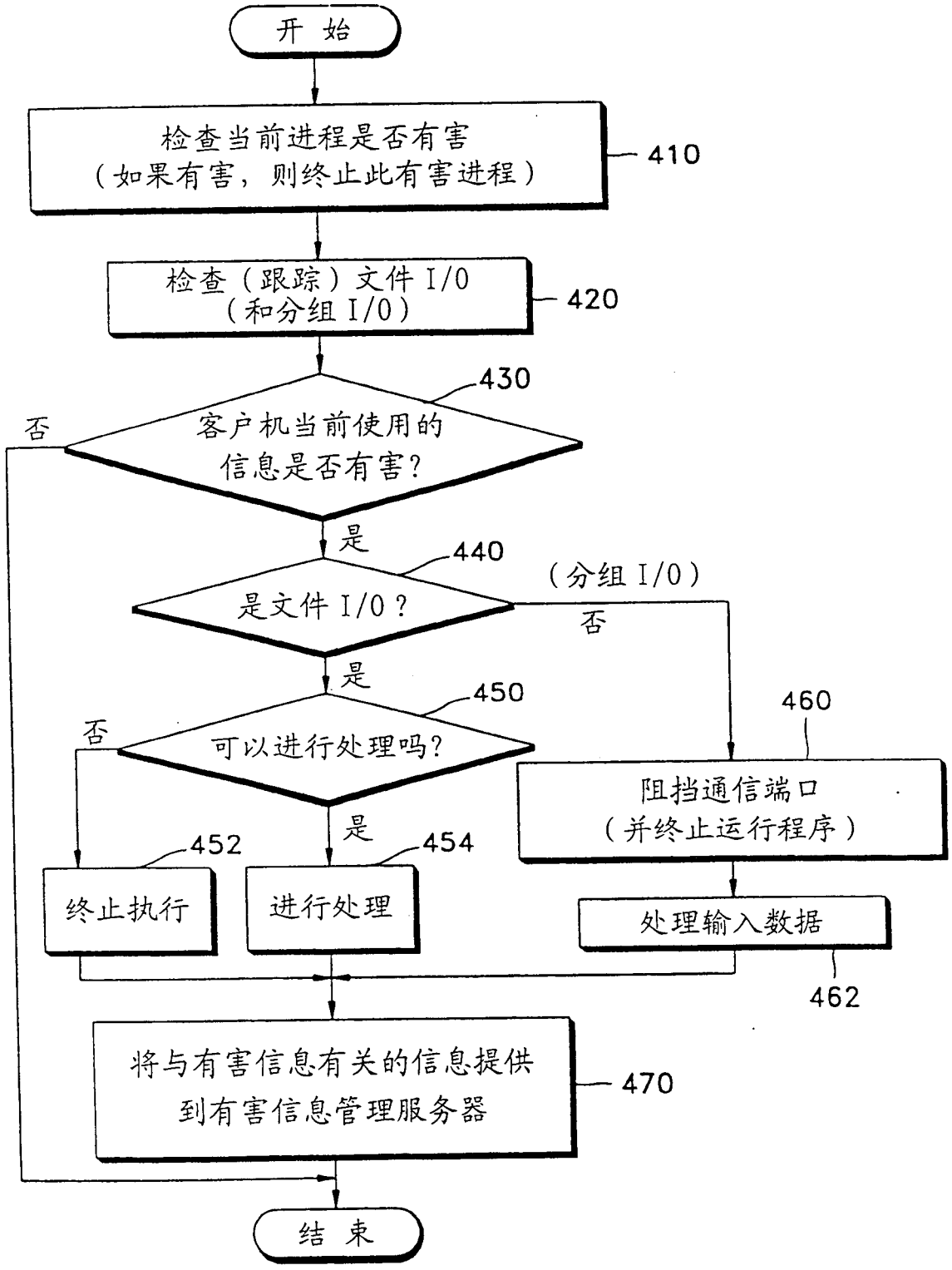

开 始
检查当前进程是否有害
（如果有害，则终止此有害进程）
410
检查（跟踪）文件 I/O
（和分组 I/O）
420
430
客户机当前使用的
信息是否有害？
否
是
440
是文件 I/O？
（分组 I/O）
否
是
450
可以进行处理吗？
否
460
阻挡通信端口
（并终止运行程序）
是
452
454
终止执行
进行处理
处理输入数据
462
将与有害信息有关的信息提供
到有害信息管理服务器
470
结 束

图 4