(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 101558398 B
(45)授权公告日 2012.11.28

(21)申请号 200680019483.3
(22)申请日 2006.05.05
(30)优先权数据
60/678,391 2005.05.05 US
(85)PCT申请进入国家阶段日
2007.11.30
(86)PCT申请的申请数据
PCT/US2006/017782 2006.05.05
(87)PCT申请的公布数据
WO2006/119508 EN 2006.11.09
(73)专利权人 思科埃恩波特系统有限公司
地址 美国加利福尼亚州
(72)发明人 丹尼尔·昆兰 詹森·克尔
杰弗里·韦斯科特
(74)专利代理机构 北京东方亿思知识产权代理有限责任公司 11258
代理人 王怡
(51)Int.Cl.
G06F 15/16(2006.01)
(56)对比文件
US 2005/0081059 A1,2005.04.14, 全文.
CN 1573784 A,2005.02.02, 全文.
审查员 赵婷

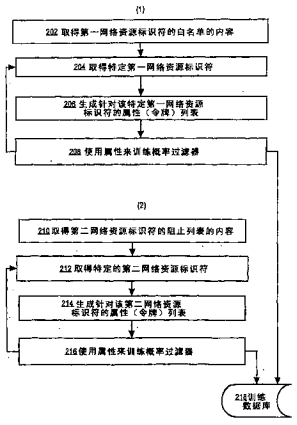
权利要求书 4 页 说明书 16 页 附图 6 页

(54)发明名称

基于被引用资源的概率分析检测不想要的电子邮件消息

(57)摘要

在一个实施例中,基于被引用资源的概率分析检测不想要的电子邮件消息包括:接收白名单和阻止列表,其各自包括多个已经出现在在先消息中的网络资源标识符;取得特定的网络资源标识符;生成针对该特定网络资源标识符的属性列表;使用属性训练概率过滤器;以及针对白名单和阻止列表中的所有网络资源标识符重复上述取得、生成和训练步骤。随后,当接收到电子邮件消息并且其包含URL或其他网络资源标识符时,可以通过利用经训练的概率过滤器测试网络资源标识符的属性来生成针对该消息的垃圾邮件得分或威胁得分。



CN 101558398 B

1. 一种用于基于对被引用资源的概率分析来检测不想要的电子邮件消息的方法，包括：

取得包含多个已被包括在过去的电子邮件消息中的第一网络资源标识符的白名单；

从所述白名单取得特定第一网络资源标识符；

生成针对所述特定第一网络资源标识符的第一属性列表；

使用所述第一属性列表中的属性来训练概率过滤器；

针对所述白名单中的所有第一网络资源标识符重复所述取得、生成和训练步骤；

取得包含多个已被包括在与垃圾邮件或威胁相关联的过去的电子邮件消息中的第二网络资源标识符的阻止列表；

从所述阻止列表取得特定第二网络资源标识符；

生成针对所述特定第二网络资源标识符的第二属性列表；

使用所述第二属性列表中的属性来训练所述概率过滤器；

针对所述阻止列表中的所有第二网络资源标识符重复所述取得、生成和训练步骤，

其中，所述第一属性列表中的属性和所述第二属性列表中的属性包括以下各项中的任何一个：基于所述特定第一或第二网络资源标识符从 DNS 查询获得的信息，包括名称、IP 地址和服务器中的任何一种；网页；所述特定第一或第二网络资源标识符使用的服务器软件；基于针对包含在所述特定第一或第二网络资源标识符中的域名的域名拥有者和网络块拥有者两者从“whois”查询获得的信息；以及从所述特定第一或第二网络资源标识符提取出的单词。

2. 如权利要求 1 所述的方法，还包括：

接收第三网络资源标识符；

使用所述经训练的概率过滤器来测试所述第三网络资源标识符，并且接收指示所述第三网络资源标识符与垃圾邮件或威胁相关联的概率的概率输出；

当所述概率输出大于第一指定阈值时，将所述第三网络资源标识符添加到黑名单。

3. 如权利要求 1 所述的方法，其中生成所述第二属性列表包括：

提取所述第二网络资源标识符的域部分；

从域名系统取得与所述提取出的域部分相关联的一个或多个邮件交换记录；

从所述域名系统取得针对在所述邮件交换记录中标识的每个邮件服务器的每个地址记录；

取得与每个所述地址记录的网络地址相关联的声誉得分值；

当平均声誉得分值小于指定阈值时，将所述网络资源标识符添加到所述黑名单。

4. 如权利要求 1 所述的方法，其中所述网络资源标识符是统一资源定位符 (URL)。

5. 如权利要求 1 所述的方法，其中生成所述第二属性列表包括：

提取所述第二网络资源标识符的域部分；

从域名系统取得与所述提取出的域部分相关联的一个或多个名称服务器记录；

从所述域名系统取得针对在所述名称服务器记录中标识的每个邮件服务器的每个地址记录；

取得与每个所述地址记录的网络地址相关联的声誉得分值；

当平均声誉得分值小于指定阈值时，将所述网络资源标识符添加到所述黑名单。

6. 如权利要求 3 所述的方法，还包括将所述黑名单发送到耦合到所述网络的多个消息传递网关设备。

7. 如权利要求 3 所述的方法，其中所述黑名单与所述阻止列表相分离。

8. 如权利要求 3 所述的方法，还包括：

在消息传递网关处接收所述黑名单的拷贝；

在所述消息传递网关处，接收包含统一资源定位符 (URL) 的电子邮件消息；

提取所述统一资源定位符并判定所述统一资源定位符是否在所述黑名单的拷贝中；

当所述统一资源定位符在所述黑名单的拷贝中时，修改与所述电子邮件消息相关联的威胁得分值。

9. 如权利要求 1 所述的方法，其中所述威胁包括病毒、网络钓鱼攻击和网址嫁接攻击中的任何一种。

10. 如权利要求 5 所述的方法，还包括将所述黑名单发送到耦合到所述网络的多个消息传递网关设备。

11. 如权利要求 5 所述的方法，其中所述黑名单与所述阻止列表相分离。

12. 如权利要求 5 所述的方法，还包括：

在消息传递网关处接收所述黑名单的拷贝；

在所述消息传递网关处，接收包含统一资源定位符 (URL) 的电子邮件消息；

提取所述统一资源定位符并判定所述统一资源定位符是否在所述黑名单的拷贝中；

当所述统一资源定位符在所述黑名单的拷贝中时，修改与所述电子邮件消息相关联的威胁得分值。

13. 一种用于基于对被引用资源的概率分析来检测不想要的电子邮件消息的装置，包括：

用于取得包含多个已被包括在过去的电子邮件消息中的第一网络资源标识符的白名单的装置；

用于从所述白名单取得特定第一网络资源标识符的装置；

用于生成针对所述特定第一网络资源标识符的第一属性列表的装置；

用于使用所述第一属性列表中的属性来训练概率过滤器的装置；

用于针对所述白名单中的所有第一网络资源标识符重复所述取得、生成和训练装置的执行的装置；

用于取得包含多个已被包括在与垃圾邮件或威胁相关联的过去的电子邮件消息中的第二网络资源标识符的阻止列表的装置；

用于从所述阻止列表取得特定第二网络资源标识符的装置；

用于生成针对所述特定第二网络资源标识符的第二属性列表的装置；

用于使用所述第二属性列表中的属性来训练所述概率过滤器的装置；

用于针对所述阻止列表中的所有第二网络资源标识符重复所述取得、生成和训练装置的执行的装置，

其中，所述第一属性列表中的属性和所述第二属性列表中的属性包括以下各项中的任何一个：基于所述特定第一或第二网络资源标识符从 DNS 查询获得的信息，包括名称、IP 地址和服务器中的任何一种；网页；所述特定第一或第二网络资源标识符使用的服务器软

件；基于针对包含在所述特定第一或第二网络资源标识符中的域名的域名拥有者和网络块拥有者两者从“whois”查询获得的信息；以及从所述特定第一或第二网络资源标识符提取出的单词。

14. 如权利要求 13 所述的装置，还包括：

用于接收第三网络资源标识符的装置；

用于使用所述经训练的概率过滤器来测试所述第三网络资源标识符，并且用于接收指示所述第三网络资源标识符与垃圾邮件或威胁相关联的概率的概率输出的装置；

用于当所述概率输出大于第一指定阈值时，将所述第三网络资源标识符添加到黑名单的装置。

15. 如权利要求 13 所述的装置，其中生成所述第二属性列表包括：

用于提取所述第二网络资源标识符的域部分的装置；

用于从域名系统取得与所述提取出的域部分相关联的一个或多个邮件交换记录的装置；

用于从所述域名系统取得针对在所述邮件交换记录中标识的每个邮件服务器的每个地址记录的装置；

用于取得与每个所述地址记录的网络地址相关联的声誉得分值的装置；

用于当平均声誉得分值小于指定阈值时，将所述网络资源标识符添加到所述黑名单的装置。

16. 如权利要求 13 所述的装置，其中所述网络资源标识符是统一资源定位符 (URL)。

17. 如权利要求 13 所述的装置，其中生成所述第二属性列表包括：

提取所述第二网络资源标识符的域部分；

从域名系统取得与所述提取出的域部分相关联的一个或多个名称服务器记录；

从所述域名系统取得针对在所述名称服务器记录中标识的每个邮件服务器的每个地址记录；

取得与每个所述地址记录的网络地址相关联的声誉得分值；

当平均声誉得分值小于指定阈值时，将所述网络资源标识符添加到所述黑名单。

18. 如权利要求 15 所述的装置，还包括用于将所述黑名单发送到耦合到所述网络的多个消息传递网关设备的装置。

19. 如权利要求 15 所述的装置，其中所述黑名单与所述阻止列表相分离。

20. 如权利要求 15 所述的装置，还包括：

用于在消息传递网关处接收所述黑名单的拷贝的装置；

用于在所述消息传递网关处，接收包含统一资源定位符 (URL) 的电子邮件消息的装置；

用于提取所述统一资源定位符并判定所述统一资源定位符是否在所述黑名单的拷贝中的装置；

用于当所述统一资源定位符在所述黑名单的拷贝中时，修改与所述电子邮件消息相关联的威胁得分值的装置。

21. 如权利要求 13 所述的装置，其中所述威胁包括病毒、网络钓鱼攻击和网址嫁接攻击中的任何一种。

22. 如权利要求 17 所述的装置，还包括用于将所述黑名单发送到耦合到所述网络的多个消息传递网关设备的装置。

23. 如权利要求 17 所述的装置，其中所述黑名单与所述阻止列表相分离。

24. 如权利要求 17 所述的装置，还包括：

用于在消息传递网关处接收所述黑名单的拷贝的装置；

用于在所述消息传递网关处，接收包含统一资源定位符 (URL) 的电子邮件消息的装置；

用于提取所述统一资源定位符并判定所述统一资源定位符是否在所述黑名单的拷贝中的装置；

用于当所述统一资源定位符在所述黑名单的拷贝中时，修改与所述电子邮件消息相关联的威胁得分值的装置。

基于被引用资源的概率分析检测不想要的电子邮件消息

技术领域

[0001] 本发明一般地涉及网络数据通信。更具体而言，本发明涉及对不想要的电子邮件消息或与垃圾邮件 (spam)、病毒 (virus) 或其他威胁 (threat) 相关的电子邮件消息的处理。

背景技术

[0002] 在本部分中描述的方法可以是已经实现的，但不一定是先前已经设想到或实现的方法。因此，除非另外指示，否则本部分中描述的方法不是针对本申请权利要求的现有技术，并且不因包括在本部分中而被承认是现有技术。

[0003] 作为不想要的或者不请自来的电子邮件消息（“垃圾邮件”）或者包含病毒或诸如“网络钓鱼 (phishing)”攻击之类的其他威胁的电子邮件消息的发送者通常使用某些手段来掩盖该消息是不想要的或不请自来的或包含病毒或其他威胁的事实。消息可以具有主题行、发送者名称（“From：”值），以及看起来合法的其他元素。另外，消息可能设法使电子系统难以确定消息的意图。但是，消息可以包含超级链接、统一资源指示符 (URI)、统一资源定位符 (URL) 或与垃圾邮件、病毒或其他威胁相关联的其他网络资源标识符。当用户选择（“点击”）这种消息中的超级链接时，用户的浏览器将用户定向到递送病毒、广告软件或间谍软件的有害的或不合需要的网页，或者尝试引导用户公开个人信息或金融信息，或者导向到不合需要的内容，例如广告或色情内容。

[0004] 其他时间，URL 访问向垃圾邮件引擎回报垃圾邮件消息“成功”递送的可执行代码或脚本。再另外的时间，URL 旨在用于垃圾邮件所涉及的任何商品的点入式营销 (click-through marketing)。

[0005] 因此，当消息被接收时，基于对消息内容的典型分析，威胁检测系统和其他分析工具通常无法判定消息是否是垃圾邮件或者与威胁相关联。

附图说明

[0006] 本发明在附图中以示例方式而非限制方式示出，在附图中，相似标号指示相似元件，其中：

[0007] 图 1 是示出可被用于实现实施例的示例性网络布置的框图；

[0008] 图 2A 是示出基于接收到的消息中的网络资源标识符来训练概率过滤器 (probabilistic filter) 的一个实施例的高级概况的流程图；

[0009] 图 2B 是示出测试接收到的消息是否是垃圾邮件或与威胁相关联的一个实施例的高级概况的流程图；

[0010] 图 2C 是示出判定是否将网络资源标识符添加到阻止列表 (block list) 的一个实施例的高级概况的流程图；

[0011] 图 2D 是示出将阻止列表传送到消息传递网关并使用阻止列表来过滤消息的一个实施例的高级概况的流程图；

[0012] 图 3 是示出域名系统 (DNS) 服务器中的记录的框图 ;以及

[0013] 图 4 是示出可以在其上实现实施例的计算机系统的框图。

具体实施方式

[0014] 用于基于对被引用资源的概率分析来检测不合需要的电子邮件消息的方法和装置被描述。在以下描述中,出于说明的目的而提出多个特定细节,以便对本发明提供全面理解。但是,本领域技术人员显而易见,本发明在没有这些特定细节的情况下也可以实现。在其他实例中,公知的结构和设备以框图形式示出,以免不必要地模糊本发明。

[0015] 这里根据以下大纲来描述实施例 :

[0016] 1.0 总体概述

[0017] 2.0 结构和功能概述

[0018] 2.1 示例性结构布置

[0019] 2.2 功能概述

[0020] 3.0 实现机制——硬件概述

[0021] 4.0 扩展和替代

[0022] 1.0 总体概述

[0023] 在前面“背景技术”中提及的需求以及将从以下描述中显现出来的其他需求和目的被本发明所实现,在一个方面中,本发明包括通过下述操作来基于对被引用资源的概率分析检测不想要的电子邮件消息的方法 :取得白名单,该白名单包括已被包括在过去的电子邮件消息中的多个第一网络资源标识符 ;从白名单取得特定的第一网络资源标识符 ;生成针对该特定第一网络资源标识符的第一属性列表 ;使用所述属性来训练概率过滤器 ;针对白名单中的所有第一网络资源标识符重复提取、取得和训练操作 ;取得阻止列表,该阻止列表包括已被包括在与垃圾邮件或威胁相关联的过去的电子邮件消息中的多个第二网络资源标识符 ;从阻止列表取得特定的第二网络资源标识符 ;生成针对该特定的第二网络资源标识符的第二属性列表 ;使用所述属性来训练概率过滤器 ;针对阻止列表中的所有第二网络资源标识符重复提取、取得和训练操作。

[0024] 在一个特征中,该方法还包括接收第三网络资源标识符 ;使用经训练的概率过滤器来测试第三网络资源标识符并接收指示第三网络资源标识符与垃圾邮件或威胁相关联的概率的概率输出 ;当概率输出大于第一指定阈值时,将第三网络资源标识符添加到黑名单。

[0025] 在另一特征中,生成第二属性列表的操作包括 :提取出第二网络资源标识符的域部分 ;从域名系统取得与提取出的域部分相关联的一个或多个邮件交换记录 ;从域名系统取得在邮件交换记录中标识的每个邮件服务器的每个地址记录 ;取得与每个地址记录的网络地址相关联的声誉得分值 ;当平均声誉得分值小于指定阈值时,将该网络资源标识符添加到黑名单。

[0026] 在又一特征中,网络资源标识符是统一资源定位符 (URL)。

[0027] 在又一特征中,生成第二属性列表的操作包括 :提取出第二网络资源标识符的域部分 ;从域名系统取得与提取出的域部分相关联的一个或多个名称服务器记录 ;从域名系统取得在名称服务器记录中标识的每个邮件服务器的每个地址记录 ;取得与每个地址记录

的网络地址相关联的声誉得分值；当平均声誉得分值小于指定阈值时，将该网络资源标识符添加到黑名单。

[0028] 在又一特征中，该方法还包括将黑名单发送到耦合到网络的多个消息传递网关设备。

[0029] 在另一特征中，黑名单与先前识别出的阻止列表相分离。

[0030] 在又一特征中，该方法还包括在消息传递网关处接收黑名单的拷贝；在消息传递网关处，接收包含统一资源定位符 (URL) 的电子邮件消息；提取出 URL 并判定该 URL 是否在黑名单的拷贝中；当 URL 在黑名单的拷贝中时，修改与该电子邮件消息相关联的威胁得分值。

[0031] 在本描述中，威胁可以包括病毒、网络钓鱼攻击和网址嫁接 (pharming) 攻击中的任何一种。在此上下文中，“网络钓鱼攻击”指的是由以下行为表征的犯罪行为形式：通过在明显官方的电子通信（例如电子邮件）中化妆成值得信任的人或企业来企图骗取敏感信息，例如密码或信用卡细节。该术语是由于使用越来越先进的诱饵来“钓取”用户的金融信息和密码而得名的。“网址嫁接”指的是非法利用 DNS 服务器软件的脆弱性，所述 DNS 服务器软件允许计算机用户获取站点的域名或将例如该网站的流量重定向到另一网站。

[0032] 在其他方面中，本发明包括被配置用于执行上述步骤的电子邮件服务器、其他计算机装置和计算机可读介质。

[0033] 2.0 结构和功能概述

[0034] 2.1 示例性结构布置

[0035] 图 1 是可被用来实现实施例的示例性网络布置的框图。出于说明清晰示例的目的，这里的部分描述提到了垃圾邮件消息。但是，其他实施例可以用于包含任何形式的消息承载的威胁或问题或与这样的威胁或问题相关的消息，例如垃圾邮件或不请自来的消息、包含“网络钓鱼”攻击或其他欺骗性或有害内容的消息。因此，这里的宽泛方法不局限于对垃圾邮件起作用的系统。此外，实施例可以测试“正常邮件 (ham)”消息并提供指示这些消息不是垃圾邮件或不与威胁相关联的输出。

[0036] 现在参考图 1，威胁发送者 100 的身份和位置通常是未知的，该威胁发送者 100 被直接或间接耦合到公共网络 102，并通常在电子消息或电子邮件中将消息发送到公共网络。消息被寻址到多个接收者或目的地，例如私有网络 110 中的计算机 120A、120B、120C 的用户的账户、威胁信息源 104 和威胁陷阱 (trap)106。消息包括垃圾邮件，其包含诸如病毒之类的威胁，或包含呈现垃圾邮件内容或恶毒或有害的网络资源的网络标识符。

[0037] 威胁信息源 104 包括消息签名的网络可访问源、黑名单、白名单或标识作为垃圾邮件或有害的消息或其发送者的其他信息。作为附加或替换，威胁信息源 104 可以包括在万维网上的域“spamcop.net”可访问的 SpamCop 信息服务，或 SpamCop 服务的用户。SpamCop 包括用于跟踪与垃圾邮件、正常邮件和概率得分相关联的 URL、主机名和 IP 地址的数据库。

[0038] 威胁信息源 104 可以包括由一个或多个因特网服务提供商或其他大量邮件接收者拥有、操作或管理的服务或数据库。

[0039] 在另一替换实施例中，作为对这里的自动方法的补充，威胁信息源 104 可以包括对由信息服务顾问或分析员或外部源获得的数据的手动审查。例如，在大多数情况下，监视来自防垃圾邮件供应商、防病毒供应商、第三方供应商、防垃圾邮件列表或防病毒邮件列

表、垃圾邮件陷阱 (spamtrap) 或威胁陷阱数据和其他源的警告的人类管理员可以在对防垃圾邮件软件或处理规则的更新被发布之前检测到垃圾邮件。

[0040] 威胁陷阱 106 是专用于收集关于包含垃圾邮件或与威胁相关的电子邮件消息的信息的电子邮件地址、账户或邮箱。为了说明简单示例，图 1 仅以威胁信息源 104 和威胁陷阱 106 的形式示出两个目的地，但是在实际实施例中，可能存在任何数目的这样的垃圾邮件信息源。

[0041] 威胁发送者 100 可以获得来自公共来源、购买的电子邮件地址列表、在线张贴等的威胁陷阱 106 和计算机 120A、120B、120C 的网络地址。

[0042] 威胁信息处理器 108 可通信地耦合到公共网络 102，并且可以从威胁信息源 104 和威胁陷阱 106 接收信息。威胁信息处理器 108 实现这里进一步描述的某些功能，包括从威胁信息源 104 和威胁陷阱 106 收集垃圾邮件和威胁信息、生成垃圾邮件和威胁发作信息，并且将发作信息存储在数据库 112 中。

[0043] 网络资源 150 和网站 152 被耦合到公共网络 102。网络资源 150 可以包括网络可访问的可执行计算机程序代码、脚本或其他软件元件。网络资源 150 还可以包括网站 152、文件服务器或任何其他网络可访问的信息资源。在各种实施例中，可能存在任何数目的耦合到网络 1 02 的网络资源 150 和网站 152。在本描述中，术语“网络资源标识符”泛指标识任何种类的网络资源的任何数据；因此，“网络资源标识符”可以是 URL、URI、超级链接、域名、主机名等等。

[0044] 一个或多个域名服务 (DNS) 服务器 160 被耦合到公共网络 102。每个 DNS 服务器 160 存储 DNS 记录，所述 DNS 记录可被用于将域名解析成网络地址，例如 IP 地址、与域名相关联的邮件交换 (MX) 服务器的名称、名称服务器记录等等。

[0045] 现有的公共 URI 阻止列表 140 被耦合到公共网络 102。阻止列表 140 一般包括已经在垃圾邮件消息中广告的统一资源定位符 (URI) 的列表。在实施例中，阻止列表 140 包括其他都针对在垃圾邮件消息中找到的域的阻止列表的集合。在阻止列表 140 中的信息可以使用 DNS 查找来访问，所述 DNS 查找需要连通因特网并且需要相对较长的等待时间才能获得结果。在实施例中，因为阻止列表 140 包括列表的集合，因此来自阻止列表 140 的每个输出条目被标注以一个位掩码，其标识该域出现在哪个或哪些列表上。

[0046] 消息传递网关 107 被直接或通过防火墙 111 或其他网络元件间接耦合在公共网络 102 和私有网络 110 之间，所述私有网络 110 包括多个末端站 120A、120B、120C。消息传递网关 107 可以与邮件传送代理 109 集成在一起，该邮件传送代理 109 处理针对私有网络 110 的邮件，或者该邮件传送代理可以被单独部署。例如，诸如商业上可从加州 San Bruno 的 IronPort Systems 公司获得的 C60、C30、C10、X1000 型等等的 IronPort 消息传递网关设备 (MGA) 可以实现邮件传送代理 109、防火墙 111 和这里针对消息传递网关 107 描述的功能。

[0047] 在实施例中，消息传递网关 107 包括病毒信息逻辑 114，其用于获得来自威胁信息处理器 108 的病毒发作信息，并根据在消息传递网关处设置的策略来处理以末端站 120A、120B、120C 为目的地的消息。这种病毒信息逻辑可以与消息传递网关 107 的内容过滤功能集成在一起。

[0048] 消息传递网关 107 还可以包括防病毒检查器 116（例如 ClamAV）、内容过滤器 118 和防垃圾邮件逻辑 119（例如 SpamAssassin 模块）。防病毒检查器 116 可以例如包括 Sophos

防病毒软件。内容过滤器 118 提供用于限制在消息主题或消息主体中包含根据与私有网络 110 相关联的策略不可接受的内容的消息的递送或接受。防垃圾邮件逻辑 119 扫描进入消息以根据邮件接受策略（例如进入消息是否是不请自来的商业邮件）来判定它们是否是不想要的消息，并且防垃圾邮件逻辑 119 应用策略来限制对任何不想要的消息的递送，重定向或拒绝接受不想要的消息。防垃圾邮件逻辑可以与本地黑名单通信，所述本地黑名单标识已经在垃圾邮件消息中广告的网络资源（例如网络资源 150、网站 152）的标识符或被禁止的发送者。

[0049] 这里使用的术语“邮件服务器”包括消息传递网关 107、邮件传送代理、邮件交换和接收并转发电子邮件消息的任何其他数据处理单元、服务器、软件或系统。

[0050] 私有网络 110 可以是与商业企业相关联的企业网络或需要增强安全性或保护的任何其他形式的网络。公共网络 102 和私有网络 110 可以使用开放标准协议（例如 TCP/IP）进行通信。

[0051] 威胁信息源 104 可以包括消息传递网关 107 的另一实例，其介于公共网络 102 和另一私有网络（为了清晰而未示出）之间以保护该另一私有网络。在一个实施例中，威胁信息源 104 是 IronPort MGA。

[0052] 威胁陷阱 106 与一个或多个电子邮件地址或电子邮件邮箱相关联，这一个或多个电子邮件地址或电子邮件邮箱与一个或多个域相关联。威胁陷阱 106 被建立以用于接收不请自来的电子邮件消息或“垃圾邮件”以供分析或报告，并且威胁陷阱 106 通常不用于传统的电子邮件通信。例如，垃圾邮件陷阱可以是诸如 dummyaccountforspam@mycompany.com 之类的电子邮件地址，或者垃圾邮件陷阱可以是被组成 MX 型 DNS 记录（接收到的电子邮件信息被提供给该记录）的电子邮件地址的集合。邮件传送代理 109 或另一 IronPort MGA 的邮件传送代理可以容宿威胁陷阱 106。

[0053] 在实施例中，威胁信息源 104 生成并提供信息到威胁信息处理器 108 以用于管理计算机病毒发作，并且威胁信息处理器 108 可以从威胁陷阱 106 获得信息以用于相同目的。例如，威胁信息源 104 生成接收到的具有可疑附件的消息的计数，并将该计数提供到威胁信息处理器 108，或者允许外部进程取得该计数并将它们存储在专门数据库中。消息传递网关 107 也可以通过以下操作来充当病毒信息源：检测具有与病毒相关或在其他方面可疑的指示的消息；创建在特定时间段内接收的可疑消息的计数；并且周期性地将该计数提供到威胁信息处理器 108。

[0054] 作为特定示例，这里描述的功能可被实现为全面消息数据收集部件或报告设施（例如来自 IronPort Systems 公司的 SenderBase 服务）的一部分。在本实施例中，威胁信息处理器 108 可以从威胁信息源 104 和威胁陷阱 106 取得或接收信息，生成针对由防垃圾邮件逻辑 119 确定为垃圾邮件或具有可疑附件或被防病毒检查器 116 指示为具有病毒指示符的消息的发送者的声誉得分，并利用声誉得分更新数据库 112，以供消息传递网关 107 的防垃圾邮件逻辑 119 和病毒信息逻辑 114 以后取得和使用。

[0055] 威胁信息处理器 108 包括一个或多个分析消息并生成信息的服务器、系统或服务，所述信息可以被消息传递网关 107 和部署在私有网络中或耦合到公共网络 102 的其他消息传递网关所使用。威胁信息处理器 108 可以包括或可通信地耦合到威胁操作中心 (TOC)、接收病毒得分 (RVS) 处理器或其两者。TOC 和 RVS 处理器可以与威胁信息处理器 108

分离开，但被可通信地耦合到数据库 112 和公共网络 102。TOC 可以实现为每日 24 小时、每周 7 日都有人员可用的职员中心，用于监视威胁信息处理器 108 收集的被存储在数据库 112 中的信息。操作 TOC 的人员可以采取手工动作，例如分析来自威胁信息源 104 的新信息、审查在威胁陷阱 106 处接收的消息、创建防垃圾邮件规则、创建防病毒规则、发布病毒发作警告、更新存储在数据库 112 中的信息、公布病毒发作信息，从而消息传递网关 107 可以访问病毒发作信息，并手动发起病毒发作信息到该消息传递网关和其他消息传递网关的发送。

[0056] 在实施例中，威胁信息处理器 108 包括网络标识符分析逻辑 130，其包括实现这里结合图 2A- 图 3 描述的功能的一个或多个计算机程序或其它软件元件。

[0057] 在实施例中，威胁信息处理器 108 包括或从一个或多个受信黑名单接收信息，所述受信黑名单编辑了已知包含垃圾邮件或已知承载威胁的消息的拷贝或属性。威胁信息处理器 108 可以容宿黑名单、查询外部黑名单，或通过消息传递协议获得黑名单信息。

[0058] 在某些实施例中，数据库 112 被称作“全集 (corpus)”，并且包括威胁信息处理器 108 的一个数据库，该数据库包含已被明确归类为垃圾邮件与否、包含病毒与否或以其他方式针对其他特定威胁分类的消息。因此，全集代表可被用于确定指示未来消息是否是垃圾邮件或包含威胁的规则或其他标准的历史消息信息的受信库。消息从自动源 (例如威胁陷阱 106) 和从来自消息传递网关 107 的报告进入全集。消息还从人类分类系统进入 ;因此，分析员可以接收消息或 URL 并确定该消息或 URL 应该被添加到数据库 112 中的白名单还是黑名单。全集还可以使用“化身 (avatar)”进入公共网络 102 并获得用于分类的消息。

[0059] 在实施例中，数据库 112 可以存储消息的以下属性值 :

[0060]

属性	源	注释
源	头部	
日期	头部	
发送者	头部	
来自	头部	
接收者 / 去往	头部	
抄送 (cc)	头部	
回复到	头部	
主题	头部	
内容类型	头部	
消息 id	头部	消息 ID 头部的值

邮件代理	头部	
附件	头部 / 主体	
sbrs 得分	经查询	用于连接 IP 地址的 SBRS 得分是在使用连接 IP 地址进行消息插入期间被查询的。
sbrs 得分	经计算	在为获取得分而查询 SBRS 时设置
时间戳		
sbrs 规则集	经计算	哪些 SBRS 规则（从位掩码反向生成）对声誉得分有贡献
连接 ip	经计算	从 X-Spam-Untrusted-Relays 头部获得。该头部是通过回看“跳”直到遇到网络边界而计算出的。如果这样不起作用，则使用接收到的头部中的第一“不受信”IP 地址。
校验和	经计算	用于唯一性确定。利用 SHA1 从消息主体的前 N 字节计算出，其中 N = min(1024，消息主体长度 /2)
连接 ip 国家	经查询	从 X-Spam-RBL 头部获得。该头部从 TXT 记录查询直接获得。
疑似类别	经计算	使用 X-Spam-Status 和 X-ClamAV-Status 头部计算出。如果 ClamAV 报告消息为病毒，则它是“病毒”。如果 SpamAssassin 得分小于针对给定源配置的疑似正常邮件阈值，则该消息是“正常邮件”（不被看作垃圾邮件的消息，但不一定完全受信）。如果 Spam Assassin 得分大于针对给定源配置的疑似垃圾邮件阈值，则它是“垃圾邮件”。如果对于给定源不存在特定阈值，则使用默认阈值。否则，它是“未知的”。
类别	设置 / 经计算	如果消息与一个类别一起手工提交，则该类别被使用。否则，使用与疑似类别相同的算法来计算，但是使用可配置的针对“正常邮件”和“垃圾邮件”的阈值，而非“疑似正常邮件”和“疑似垃圾邮件”阈值
后压 (blowback)	设置	全集管理员必须手工设置该属性。其默认为假 (False)。

弹回 (bounce)	设置	全集管理员必须手工设置该属性。其默认为假。
网络钓鱼	设置 / 经计算	如果 X-ClamAV-Status 头部确定消息是网络钓鱼攻击，则其为真 (True)。否则，全集管理员可手工设置该值。其默认为假。
病毒重扫描	经计算	如果消息的病毒状态为未知，则设置为真。否则，设置为假。
病毒得分	经计算	使用 ClamAV 来计算。
病毒得分 时间戳	经计算	在每次使用 ClamAV(重) 扫描消息时计算。
病毒规则集	经计算	哪些病毒被找到。
垃圾邮件重扫描	经计算	如果消息的垃圾邮件状态为未知或者如果其他关键属性所需的任何 X-Spam 头部在上次扫描期间没有出
		现，则设置为真。
垃圾邮件得分	经计算	使用 stock SpamAssassin 来计算。
垃圾邮件得分 时间戳	经计算	在每次使用 ClamAV(重) 扫描消息时计算。
垃圾邮件规则集	经计算	哪些垃圾邮件规则对“垃圾邮件性 (spaminess)”得分有贡献
语言	经计算	使用 Spam Assassin 语言检测功能来计算
审计	经计算	每次任何消息属性改变时设置。跟踪什么属性改变，何时改变以及谁对此负责。

[0061] 在实施例中，威胁信息处理器 108 包括阻止列表 142。在一个实施例中，阻止列表 142 可以是本地管理的拷贝或者是公共发送者 URI 阻止列表 140 的镜像。对阻止列表 140 执行镜像确保了威胁信息处理器 108 即使在阻止列表 140 经历网络中断 (outage) 或故障时也能够连续获得 URI 阻止列表信息。在实施例中，阻止列表 142 可被集成到数据库 112 中。

[0062] 在实施例中，威胁信息处理器 108 包括 HTTP 服务 132，其可以发布 HTTP 请求以获得网络资源 150 的拷贝、来自网站 152 的信息或存储在 HTTP 服务器中的其他网络可访问信息。

[0063] 在实施例中，威胁信息处理器 108 包括声誉得分服务 136，其可以确定存储在数据库 112 中的消息的声誉得分值，并在接收到新消息时利用得分值动态更新数据库。声誉得

分值代表基于已知某发送者已经发送的过去的消息或者基于包含某消息元素的过去的消息，该消息发送者或消息元素是否与垃圾邮件消息或包含威胁的消息相关联。在一个实施例中，声誉得分值的范围从 (-10) 到 (+10)，其中 (-10) 指示差声誉或者频繁或一贯发送垃圾邮件或带有威胁的消息，而 (+10) 指示好声誉。

[0064] 在实施例中，威胁信息处理器 108 包括以软件组件实现的一个或多个训练数据库或概率过滤器 134。作为附加或替换，网络标识符分析逻辑 130 和概率过滤器 134 可被实现为消息传递网关 107 中的防垃圾邮件逻辑 119 的一部分，或以消息传递网关的防垃圾邮件逻辑的插件 (plug-in) 软件组件的形式实现。概率过滤器 134 可以是贝叶斯过滤器。概率过滤器 134 的使用在以下部分进一步描述。

[0065] 2.2 功能概述

[0066] 一般地，处理电子消息的方法的一个实施例包括接收消息，识别消息中的一个或多个网络资源标识符，建立到网络资源标识符所引用的资源的网络连接，取得被引用的资源，评价被引用的资源，并且基于被引用的资源判定消息是否包含威胁或代表垃圾邮件。

[0067] 在一个实施例中，对资源进行概率分析（例如贝叶斯分析）以判定它们是否与垃圾邮件发送者相关联。一般而言，贝叶斯分析是一种统计程序，其致力于基于观察到的分布来评估潜在分布的参数。分析开始于“先验分布”，其可以基于任何相关数据，包括对参数的相对似然 (likelihood) 或非贝叶斯观察的结果的评价。实践中，常见的做法是假设适当范围的值上的统一分布作为先验分布。

[0068] 给定先验分布，进程收集数据以获得观察分布。然后，该进程计算观察分布作为参数值的函数的似然，将该似然函数乘以先验分布，并归一化结果以获得所有可能值上的单位概率（称之为后验分布）。分布的模式于是成为参数估计，并且“概率间隔”（对信任间隔的贝叶斯模拟）可以使用标准程序来计算出。在贝叶斯分析中，结果的有效性取决于先验分布的有效性，该先验分布的有效性无法从统计上评估。

[0069] 在另一方法中，利用例如 DNS 查找将电子邮件消息中的主机名引用解析为 IP 地址。这些方法都可被用于识别应该被添加到在数据库 12 中维护的黑名单或者被更新到阻止列表 142 中的网络地址（例如 IP 地址）。

[0070] 在另一方法中，从消息主体中的 URL 中提取出的主机名被映射到 IP 地址（例如使用 DNS)。所产生的 IP 地址在一个或多个黑名单中被查找。同时，声誉得分被生成，并且低声誉得分与表明 IP 地址在黑名单中的指示的组合被用于判定相关 URL 是否也应该被放入黑名单。

[0071] 该方法可被应用于全集中的所有消息，无论该消息是否先前已经被确定为垃圾邮件。

[0072] 在这里的另一方法中，消息被接收并存储在全集中。消息被手工审查并被标记为正常邮件或垃圾邮件。在消息中引用的一个或多个 URL 被识别并且一个或多个主机名被从 URL 中提取出。代理取得针对消息主体中的 URL 的网页。代理可以针对域查找域名寄存器“whois”记录，并且可以取得在提取出的域名处的根网页。可以采取预防措施 (precaution) 以避免经常取得相同网页，这可以告知 web 服务器的拥有者或操作者它正在被防垃圾邮件服务所调查。

[0073] 取得的数据被加注令牌 (token)，令牌用于训练概率垃圾邮件检测引擎或过滤器。

作为结果，概率过滤器接受训练以基于某些令牌的存在而识别哪些消息代表垃圾邮件。例如，垃圾邮件发送者可能在重复的垃圾邮件活动中使用类似的出现的域名，或者网页取得操作将产生 HTTP 404 错误（网页未找到），这可以发生在垃圾邮件发送者发送假 URL 或尚未在指示的 URL 处建立网页时，或者网页中的内容可能正在尝试广告已知与垃圾邮件源相关联的产品。

[0074] 在训练阶段之后，新接收的消息被概率过滤器处理，并且与产生高概率得分的那些消息相关联的 IP 地址被放入黑名单。

[0075] 在一个实施例中，消息传递网关 107 周期性地查询威胁信息处理器 108 以请求用于防垃圾邮件逻辑 119 中的防垃圾邮件更新。威胁信息处理器 108 创建 URL 黑名单，该 URL 黑名单是从阻止列表 142 形成的，并且作为在数据库 112 中管理的内部白名单和黑名单。所产生的 URL 黑名单被单独或与针对消息传递网关的其他元件的其他更新一起发送到消息传递网关 107。

[0076] 在一个实施例中，URL 黑名单被发送到消息传递网关 107，作为包含（主机名、位掩码）形式的元组 (tuple) 列表的 Perl SDBM 文件。该列表包含尚未被放入白名单的主机名。在使用中，任何作为针对其他列表条目的“通配符”白名单条目的列表条目将胜过该条目。例如，假设 foo.bar.com 被放入黑名单，而“*.bar.com”被放入白名单。结果，foo.bar.com 将不会出现在发送到消息传递网关 107 的最终黑名单中。如果只有“bar.com”被放入白名单，也发生同样的结果。

[0077] 现在参考图 2A、图 2B、图 2C 和图 2D 来描述功能示例。图 2A 是示出基于接收到的消息中的网络资源标识符来训练概率过滤器的一个实施例的高级概况的流程图；图 2B 是示出测试接收到的消息是否是垃圾邮件或与威胁相关联的一个实施例的高级概况的流程图；图 2C 是示出判定是否将网络资源标识符添加到阻止列表的一个实施例的高级概况的流程图；并且图 2D 是示出将阻止列表传送到消息传递网关并使用阻止列表来过滤消息的一个实施例的高级概况的流程图。

[0078] 首先参考图 2A，部分 (1)，在步骤 202 中，第一网络资源标识符的白名单的内容被取得。在实施例中，威胁信息处理器 108 创建并管理 URI 白名单。可替换地，公共 URI 白名单可以被使用。步骤 202 的白名单以及随后将描述的步骤 210 的阻止列表可以由机器生成或者由人为生成。为了正确地执行随后的过滤操作，白名单和黑名单应该高度准确。在此上下文中，“白名单”指的是一般尚未与垃圾邮件或威胁相关联的网络地址、IP 地址、域名或其他网络资源标识符的列表。

[0079] 在步骤 204 中，从白名单取得特定第一网络资源标识符。

[0080] 在步骤 206 中，用于取得的第一网络资源标识符的属性或令牌列表被生成。在此上下文中，网络资源标识符的“属性”示例可以包括：基于网络资源标识符从 DNS 查询获得的信息，例如名称、IP 地址、服务器等等；网页；网络资源标识符正在使用的服务器软件；基于包含在网络资源标识符中的域名的域名拥有者和网络块拥有者两者而从“whois”查询获得信息；以及从 URI 和 / 或域名提取出的单词（例如针对域名“bluepillorders.com”，提取出的单词可以包括“blue”、“pill”和“orders”）。

[0081] 在实施例中，步骤 206 包括取得由特定网络资源标识符标识的网页或其他网络资源的拷贝。例如，威胁信息处理器 108 的 HTTP 服务 132 创建和发布 HTTP GET 请求以下载

上述提取出的URL处的资源。假设提取出的URL标识活动的在线网站152或其他网络资源150，则响应于HTTPGET请求接收网页或其他资源的拷贝。

[0082] 与网络资源标识符相关联的属性被转换成令牌表或流，其中每个令牌是一个单独的属性部分。例如，令牌可以包含字符串、单词、文本块、图形图像、URL、框或其他页面元素。将拷贝转换成令牌可以包括扫描存储的拷贝以及标识各种类型的定界符(delimiter)。

[0083] 在步骤208中，利用令牌来训练由训练数据库218代表的概率过滤器。例如，概率过滤器134被提供以令牌和指示令牌与“已知好的”网络资源标识符相关联的信息。在训练期间，威胁信息处理器的管理员或其他受信用户指示概率过滤器134关于特定网络资源和属性是否实际上与垃圾邮件或消息威胁相关联。可替换地，步骤208可以包括训练概率过滤器，该概率过滤器仅被用于生成一组其他网络资源标识符属性指示“好的”或者不与垃圾邮件或消息威胁相关联的网络资源标识符的概率。

[0084] 图2A的部分(2)中示出的步骤210到216(包括步骤216)对应于步骤202到208，但是步骤210到216基于出现在第二网络资源标识符的阻止列表中的网络资源标识符来训练概率过滤器(例如训练数据库218)。例如，出现在阻止列表140中的URI可被用于在步骤210到216中的训练。图2A的部分(1)和(2)可以独立运行，但是两者通常训练同样的训练数据库或概率过滤器。结果，概率过滤器被训练以准确地生成随后获得的另一网络资源标识符可能与垃圾邮件或消息威胁相关联的概率。

[0085] 因此，不同于现有方法，概率过滤器在出现在阻止列表和白名单中并且可以在消息中引用的网络资源的内容上被训练，而不是在出现在消息头部或主体中的单词上被训练。结果，概率过滤器134获取存储的以下信息：该信息指示出现在网络资源中的特定文本、图像、图形或其他文档元素在包含或递送基于计算机的威胁的垃圾邮件消息或网络资源中被引用的概率。

[0086] 因此，当新消息随后被接收但是包含指向已用来训练过概率过滤器的类似内容的不同URL时，概率过滤器将正确地识别新消息为垃圾邮件或与威胁相关联。该方法十分有用，因为垃圾邮件的发送者可能快速改变它们的域名，但是它们的域递送的内容不会改变。因此，这里提出的对内容的概率分析允许系统确定没有列入黑名单的URL与垃圾邮件或威胁相关联的可能性。

[0087] 在另一实施例中，在概率过滤器内，概率值被与网络资源标识符以及标识在消息中引用的网络资源的令牌或其他内容元素的信息两者相关联地存储。在该方法中，随后的测试或过滤可以包括仅将网络资源标识符呈现给概率过滤器，以及接收指示网络资源标识符是否与垃圾邮件或威胁相关联的相应概率值。结果，每个随后的测试或过滤不一定需要取得网络资源的另一拷贝。

[0088] 此外，由于概率过滤器134是基于在消息中引用的网络资源的内容而非消息本身被训练的，因此概率过滤器不太可能在过滤具有无害的文本但是包含嵌入的递送“网络钓鱼”攻击或威胁的超级链接的消息时失败。

[0089] 步骤202-208可以针对出现在白名单中的任何数目的网络资源标识符被重复。类似地，步骤210-216可以针对出现在阻止列表中的任何数目的网络资源标识符被重复。

[0090] 现在参考图2B，在步骤210中，关于第三网络资源标识符的信息被接收。在实施例中，在步骤210中，威胁信息处理器108从消息传递网关107接收指示消息传递网关接收到

包含特定网络资源标识符的一个或多个消息的通信。例如，该通信可能通过对在威胁信息处理器 108 中维护的服务器的 DNS 查询而发生。作为附加或替换，威胁信息处理器 108 在“SenderBase 网络参与”协议下被链接到消息传递网关 107，通过所述“SenderBase 网络参与”协议，消息传递网关可以周期性地报告消息传递网关处理的数据。

[0091] 可替换地，步骤 210 可以包括实际上接收包含一个或多个网络资源标识符的消息。出于说明清晰示例的目的，假设接收到的消息的主体包含表 1 所示文本。

[0092] 表 1- 示例性接收消息

[0093] 为了向您提供可能的最好服务，我们 Online Payment Services 需要您与我们核实您的账户信息。如果您不核实您的账户信息，我们则将禁用您的账户。为了提供您的账户细节，请点击 :http://onlinepayment.phishingscam.com，谢谢！

[0094] 不管消息的外观怎样，该消息没有被 Online Payment Services 授权，并且消息中的 URL(http://onlinepayment.phishingscam.com) 访问出于欺骗或恶毒目的而收集用户账户数据的服务器。出于说明清晰示例的目的，表 1 的消息包括一个 URL，但是各自包含任何数目的 URL 或其他网络资源标识符的任何数目的消息可以在这里描述的方法中被使用。

[0095] 步骤 210 通常在概率过滤器 134 被训练之后的某一时刻被执行。因此，图 2B 假设概率过滤器已经用在消息中引用的网络资源内容是垃圾邮件或与威胁相关联的概率训练过。

[0096] 在步骤 211 中，针对第三网络资源标识符生成属性列表。基于以上针对步骤 206 描述的相同类型的信息，属性可以包含令牌。

[0097] 在步骤 212 中，第三网络资源标识符的属性利用训练的概率过滤器被测试，并且在步骤 214 中，概率输出值被接收。

[0098] 在步骤 216 中，概率值被测试以判定其是否大于指示垃圾邮件或威胁的阈值。如果接收的概率大于阈值，则在步骤 218 中，第三网络资源标识符被添加到阻止列表。在实施例中，为了防止“反馈循环”效应，步骤 218 包括将网络资源标识符添加到阻止列表但不是在图 2A 的步骤 210-216 中用于训练的阻止列表。单独的本地阻止列表、阻止列表 142 或数据库 112 中的私有黑名单中的任何一个可以被使用。随后，当阻止列表被发送到消息传递网关 107 时，消息传递网关可以阻止包含相同网络资源标识符的消息的递送，如下面针对图 2D 将进一步描述的。

[0099] 步骤 218 可以包括向外部信息服务（例如威胁信息源 104 或阻止列表 140）报告网络资源标识符与垃圾邮件或威胁相关联。

[0100] 在图 2A、图 2B 中处理的属性可以包括基于声誉的信息。现在参考图 2C，在一种方法中，当第三网络资源标识符在步骤 217 处被接收时，第三网络资源标识符的域名部分在步骤 219 处被提取出。如果网络资源标识符是“http://onlinepayment.phishingscam.com”，则在步骤 219 中，域名部分“phishingscam.com”被提取出。

[0101] 在步骤 220 中，用于域名的 MX 或 NS 记录被从 DNS 系统取得。例如，威胁信息处理器 108 的网络标识符分析逻辑 130 向 DNS 服务器 160 发布 DNS 查询以获得用于提取出的域名的 MX 记录。如图 3 所示，DNS 服务器 160 存储 MX 记录集合 162、NS 记录集合 164 和 A 记录集合 166。特定域名可以在零、一种、两种或所有三种记录中找到。所有有效的注册的域名具有至少一个映射关联的 IP 地址的 A 记录。管理邮件交换或邮件服务器的域将具有 MX

记录。管理名称服务器的域将具有 NS 记录。

[0102] DNS 服务器 160 返回 MX 记录的拷贝或指示没有找到 MX 记录的响应。如果没有找到 MX 记录，则用于域名的 A（地址）记录被请求。可替换地，名称服务器 (NS) 记录被请求。

[0103] 接收的 MX 记录和 NS 记录标识服务器名称。在步骤 222 处，对于每个接收的记录，地址记录被取得。例如，另一 DNS 查询被发布以针对在每个 MX 记录或 NS 记录中给定的名称获得一个 A 记录。结果，威胁信息处理器 108 获取与提取出的域名部分相关联的网络地址（例如 IP 地址）。

[0104] 在步骤 224 中，与地址记录中的每个地址相关联的声誉得分或阻止列表被确定。在实施例中，包含来自地址记录的 IP 地址的查询被发布到声誉得分服务 136，其回复以与该 IP 地址相关联的声誉得分值。针对与域相关联的多个 IP 地址的多个查询可以被发送。针对与在同一消息中被引用的多个域中的所有域相关联的多个 IP 地址的多个查询可以被发送。所产生的声誉得分值可以例如通过计算平均值来组合。可替换地，步骤 224 包括对照阻止列表检查地址。

[0105] 如果平均声誉得分低于特定阈值，或者如果在步骤 226 处测试出地址被阻止，则在步骤 228 中，网络资源标识符被添加到阻止列表。对于步骤 219，可以使用单独的阻止列表来防止反馈效应。可替换地，控制返回步骤 230 以进行其他消息处理或动作。

[0106] 因此，图 2C 的方法使得能够集成从声誉服务获得的信息以基于与在消息中找到的网络资源标识符相关联的声誉值来判定特定消息是否可能是垃圾邮件或与威胁相关联。

[0107] 基于引用的网络资源标识符，消息传递网关 107 或邮件服务器可以使用在前述方法中开发的信息来过滤、阻止或应用策略到垃圾邮件或与威胁相关的消息。现在参考图 2D，在步骤 240 中，从消息传递网关接收对于更新的阻止列表的查询。因此，在一个实施例中，消息传递网关 107 周期性地查询威胁信息处理器 108 关于是否可获得更新的阻止列表。在步骤 242 中，更新的阻止列表被发送到消息传递网关。步骤 242 可以包括基于数据库 112 和 / 或阻止列表 142 的内容创建阻止列表。

[0108] 在步骤 244 中，更新的阻止列表在本地存储。例如，消息传递网关 107 基于接收到的更新的阻止列表来存储本地黑名单 117。

[0109] 在步骤 246 中，包含网络资源标识符的新电子邮件消息例如在消息传递网关 107 处被接收。该消息被提供到防垃圾邮件逻辑 119。在步骤 248 处，从消息中提取出一个或多个网络资源标识符。防垃圾邮件逻辑 119 可以执行提取。在步骤 250 处，执行测试以判定提取出的网络资源标识符是否在阻止列表中被找到。

[0110] 如果是，则在步骤 252 中，消息传递网关 107 基于测试 250 的真实结果来修改威胁得分值。因此，当图 2D 在防垃圾邮件扫描的上下文中被实现时，步骤 252 可以包括增大垃圾邮件得分值以指示步骤 246 中的消息可能是“垃圾邮件”。

[0111] 如果提取出的网络资源标识符没有在阻止列表中找到，则在步骤 254 中，消息传递网关 107 可以执行其他消息处理，例如防病毒扫描、内容过滤、策略增强等等。

[0112] 2.3 插件实施例

[0113] 在一个实施例中，这里的方法被实现在用于消息传递网关 107 的防垃圾邮件逻辑 119 的软件插件中。一般而言，这样的本地 URI 阻止列表插件使用利用防垃圾邮件逻辑 119 从消息中提取出的数据来找到消息中的网络资源标识符并对照 URI 阻止列表来测试它们。

[0114] 在实施例中，插件通过在消息主体中搜索网络资源标识符而为每个消息返回一个肯定结果。作为附加或替换，肯定和否定结果值可以针对在消息中找到的所有网络资源标识符来创建。

[0115] 在一个实施例中，插件支持写入规则以指定应该为肯定的源列表以及它们的得分权重。规则使得管理员或消息传递网关 107 的其他用户能够指定引用一个或多个列表的位掩码以对照其进行测试。利用这种方法，可以在已知尤其可靠或不可靠的特定列表或源上设置额外的得分权重。

[0116] 测试可以对照阻止列表 140、阻止列表 142 或本地存储在消息传递网关 107 中的另一阻止列表来执行。因此，出于图 1 的目的，本地黑名单 117 可以代表这样的本地阻止列表。阻止列表可以存储在本地数据库或文件中，以允许 Perl 脚本和 Python 程序连接到该文件并将该文件视为包含散列值。在一个实施例中，本地数据库或文件中的条目包含（关键字→值）组合，其中每个关键字是一个域值，每个相关的值是一个源位掩码。例如，一个条目可以包括 (foo.bar ＝＞ 0.0.68)，其中“0.0.68”是代表 IronPort、第三方阻止列表等等的位掩码。

[0117] 4.0 实现机制——硬件概述

[0118] 图 4 是示出可以在其上实现本发明的实施例的计算机系统 400 的框图。优选实施例是使用运行在诸如路由器设备之类网络元件上的一个或多个计算机程序来实现的。因此，在该实施例中，计算机系统 400 是路由器。

[0119] 计算机系统 400 包括用于传输信息的总线 402 或其他通信机制，以及与总线 402 耦合以用于处理信息的处理器 404。计算机系统 400 还包括耦合到总线 402 的用于存储信息和将被处理器 404 执行的指令的主存储器 406，例如随机访问存储器 (RAM)、闪存或其他动态存储设备。主存储器 406 还可以用于在执行将被处理器 404 执行的指令期间存储临时变量或其他中间信息。计算机系统 400 还包括耦合到总线 402 的只读存储器 (ROM) 408 或其他静态存储设备，用于存储用于处理器 404 的静态信息和指令。存储设备 410（例如磁盘、闪存或光盘）被提供并耦合到总线 402，以用于存储信息和指令。

[0120] 通信接口 418 可被耦合到总线 402，用于向处理器 404 传输信息和命令选择。接口 418 是传统的串行接口，例如 RS-232 或 RS-422 接口。外部终端 412 或其他计算机系统连接到计算机系统 400 并使用接口 414 向其提供命令。运行在计算机系统 400 中的固件或软件提供终端接口或基于字符的命令接口，以使得外部命令可以被提供到该计算机系统。

[0121] 交换系统 416 被耦合到总线 402 并且具有到一个或多个外部网络元件的输入接口 414 和输出接口 419。外部网络元件可以包括耦合到一个或多个主机 424 的本地网络 422 或具有一个或多个服务器 430 的全球网络（例如因特网 428）。交换系统 416 根据预先确定的公知的协议和规范将到达输入接口 414 的信息流量交换到输出接口 419。例如，交换系统 416 与处理器 404 合作可以确定到达输入接口 414 的数据分组的目的地并利用输出接口 419 将其发送到正确的目的地。目的地可以包括在本地网络 422 或因特网 428 中的主机 424、服务器 430、其他末端站或其他路由和交换设备。

[0122] 本发明涉及用于基于对引用资源的概率分析来检测不想要的电子邮件消息的计算机系统 400 的使用。根据本发明一个实施例，基于对引用资源的概率分析来检测不想要的电子邮件消息是由计算机系统 400 响应于处理器 404 执行包含在主存储器 406 中的一个

或多个指令的一个或多个序列而提供的。这些指令可以从另一计算机可读介质（例如存储设备 410）读入到主存储器 406 中。包含在主存储器 406 中的指令序列的执行使得处理器 404 执行这里描述的进程步骤。在多处理布置中的一个或多个处理器也可以被采用以执行包含在主存储器 406 中的指令序列。在替换实施例中，可以使用硬连线电路来取代软件指令或与软件指令相结合来实现本发明。因此，本发明的实施例不局限于硬件电路和软件的任何特定组合。

[0123] 这里使用的术语“计算机可读介质”指的是参与提供指令到处理器 404 以供执行的任何介质。这种介质可以采取很多形式，包括但不局限于，非易失性介质、易失性介质和传输介质。非易失性介质例如包括光盘或磁盘，例如存储设备 410。易失性介质包括动态存储器，例如主存储器 406。传输介质包括同轴线缆、铜线和光纤，包括包含总线 402 在内的电线。传输介质还可以采取声波或光波的形式，例如在无线电波和红外数据通信期间生成的那些。

[0124] 计算机可读介质的常见形式例如包括软盘、柔性盘、硬盘、磁带或任何其他磁介质、CD-ROM、任何其他光介质、打孔卡、纸带、任何其他具有孔状图样的物理介质、RAM、PROM 和 EPROM、FLASH-EPROM、任何其他存储器芯片或卡带、下文将描述的载波或者计算机可以读取的任何其他介质。

[0125] 在运载一个或多个指令的一个或多个序列到处理器 404 以供执行时可以涉及各种形式的计算机可读介质。例如，指令最初可以在远程计算机的磁盘上运载。远程计算机可以将指令加载到其动态存储器中并利用调制解调器通过电话线将指令发送出去。位于计算机系统 400 本地的调制解调器可以在电话线上接收数据并使用红外发射器将数据转换成红外信号。耦合到总线 402 的红外检测器可以接收在红外信号中运载的数据并将数据放在总线 402 上。总线 402 将数据运载到主存储器 406，处理器 404 从主存储器 406 取得并执行指令。由主存储器 406 接收的指令可以在被处理器 404 执行之前或之后被可选地存储在存储设备 410 上。

[0126] 通信接口 418 还提供到网络链路 420 的双向数据通信耦合，所述网络链路 420 连接到本地网络 422。例如，通信接口 418 可以是综合服务数字网络（ISDN）卡或调制解调器，以提供到相应类型的电话线的数据通信连接。作为另一示例，通信接口 418 可以是本地局域网（LAN）卡，以提供到可兼容的 LAN 的数据通信连接。无线链路也可以被实现。在任何这样的实现方式中，通信接口 418 发送和接收运载代表各种信息的数字数据流的电信号、电磁信号或光信号。

[0127] 网络链路 420 通常通过一个或多个网络向其他数据设备提供数据通信。例如，网络链路 420 可以通过本地网络 422 提供到主机计算机 424 或到由因特网服务提供商（ISP）426 操作的数据设备的连接。ISP 426 进而通过全球分组数据通信网络（现在一般称之为“因特网”）428 提供数据通信服务。本地网络 422 和因特网 428 都使用运载数字数据流的电、磁或光信号。运载数字数据到计算机系统 400 并且从计算机系统 400 接收数字数据的通过各种网络的信号和在网络链路 420 上并且通过通信接口 418 的信号具有示例性的传输信息的载波形式。

[0128] 计算机系统 400 可以通过网络、网络链路 420 和通信接口 418 来发送消息和接收数据，包括程序代码。在因特网示例中，服务器 430 可能通过因特网 428、ISP 426、本地网

络 422 和通信接口 418 来发送针对应用程序请求的代码。根据本发明，如这里所述，一个这样的下载的应用用于基于对引用的资源的概率分析来检测不想要的电子邮件消息。

[0129] 接收的代码可以在其被接收时被处理器 404 执行和 / 或被存储在存储设备 410 或其他非易失性存储设备中以供随后执行。以这种方式，计算机系统 400 可以获得载波形式的应用代码。

[0130] 5.0 扩展和替代

[0131] 在以上说明书中，已经参考本发明的特定实施例描述了本发明。但是，显而易见，在不脱离本发明的更广阔精神和范围的情况下，可以对其进行各种修改和改变。因此，说明书和附图被视为示例性的而非限制性的。

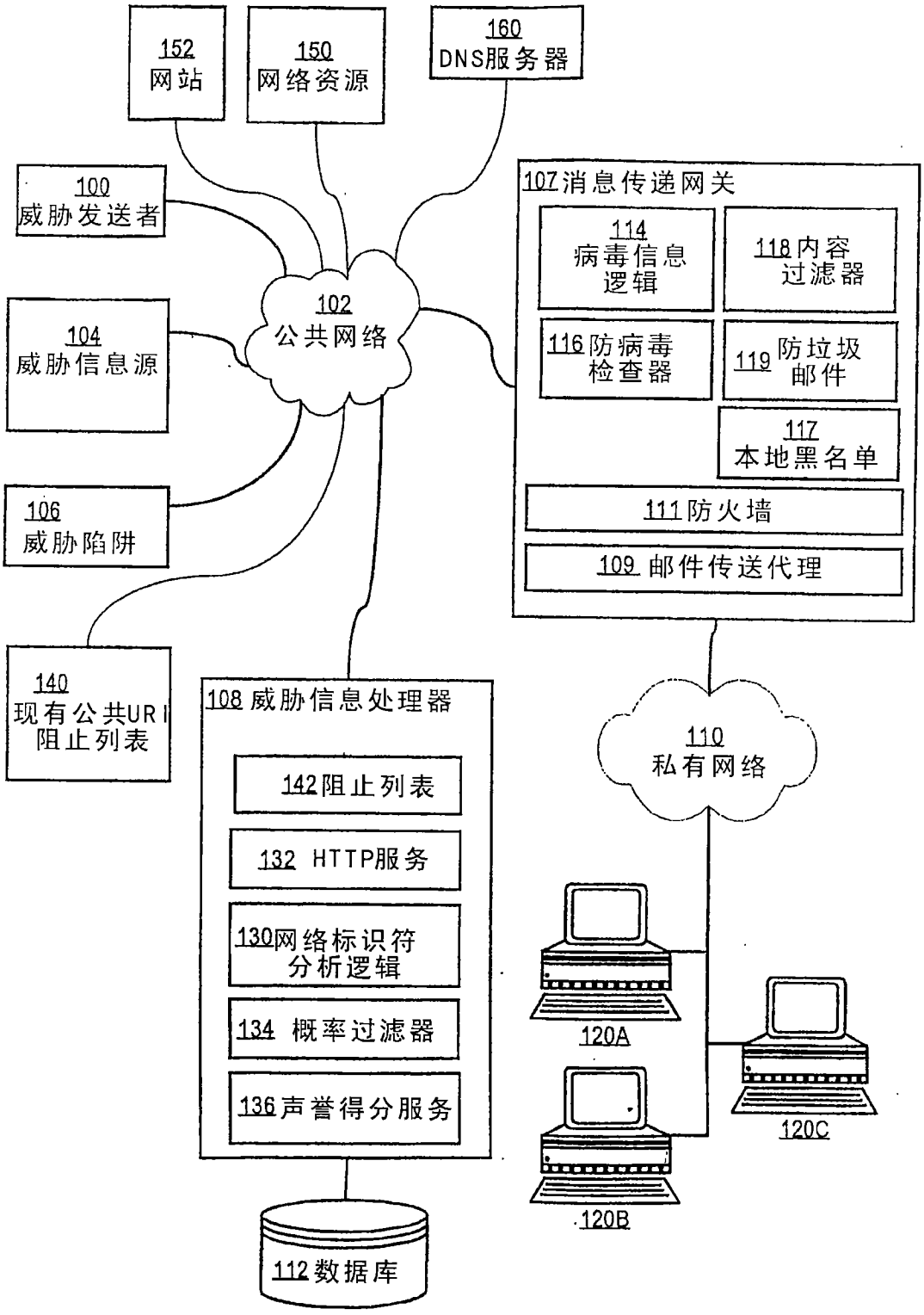

152
网站
150
网络资源
160
DNS服务器
100
威胁发送者
102
公共网络
104
威胁信息源
106
威胁陷阱
140
现有公共URI
阻止列表
107消息传递网关
114
病毒信息
逻辑
118内容
过滤器
116防病毒
检查器
119防垃圾
邮件
117
本地黑名单
111防火墙
109 邮件传送代理
108威胁信息处理器
142阻止列表
132 HTTP服务
130网络标识符
分析逻辑
134 概率过滤器
136声誉得分服务
112数据库
110
私有网络
120A
120C
120B

图1

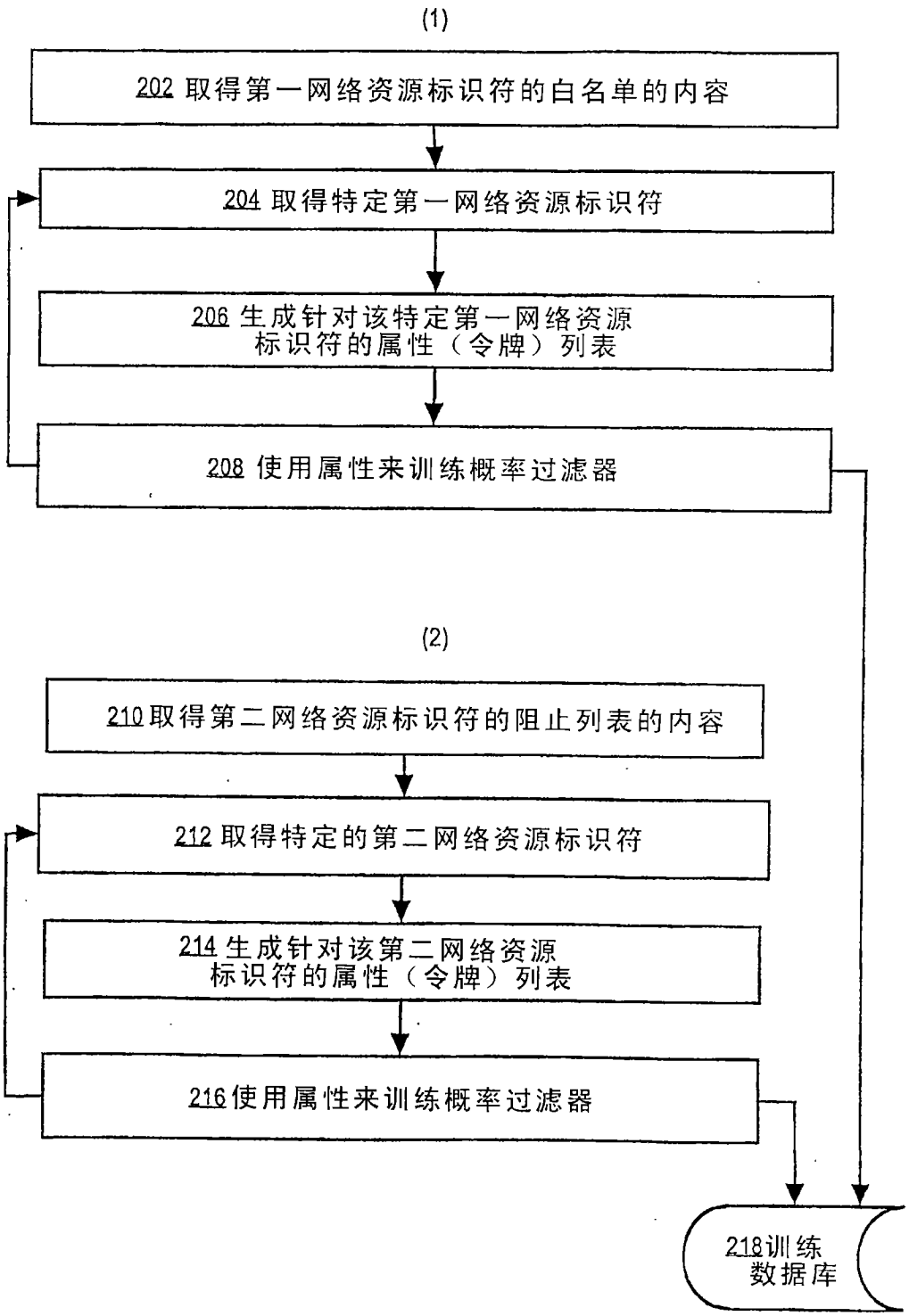

(1)
202 取得第一网络资源标识符的白名单的内容
204 取得特定第一网络资源标识符
206 生成针对该特定第一网络资源标识符的属性（令牌）列表
208 使用属性来训练概率过滤器
(2)
210 取得第二网络资源标识符的阻止列表的内容
212 取得特定的第二网络资源标识符
214 生成针对该第二网络资源标识符的属性（令牌）列表
216 使用属性来训练概率过滤器
218 训练数据库

图2A

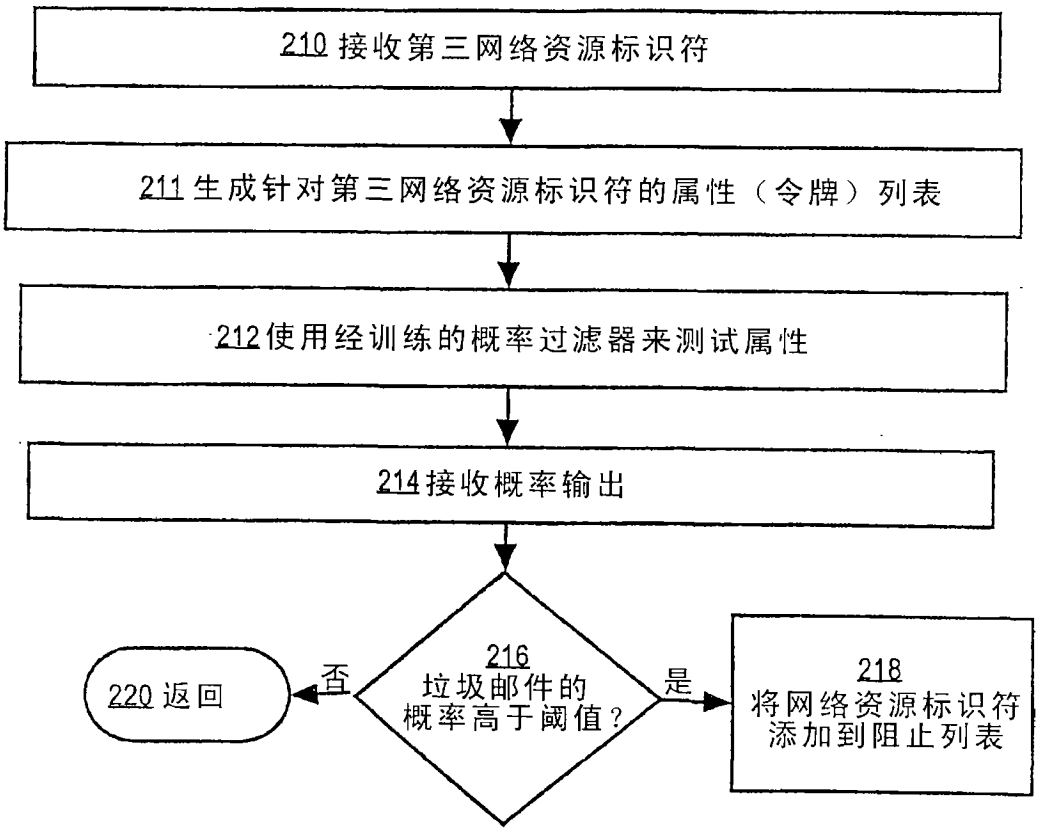

210 接收第三网络资源标识符
211 生成针对第三网络资源标识符的属性（令牌）列表
212 使用经训练的概率过滤器来测试属性
214 接收概率输出
216
垃圾邮件的概率高于阈值？
否
是
220 返回
218
将网络资源标识符添加到阻止列表

图2B

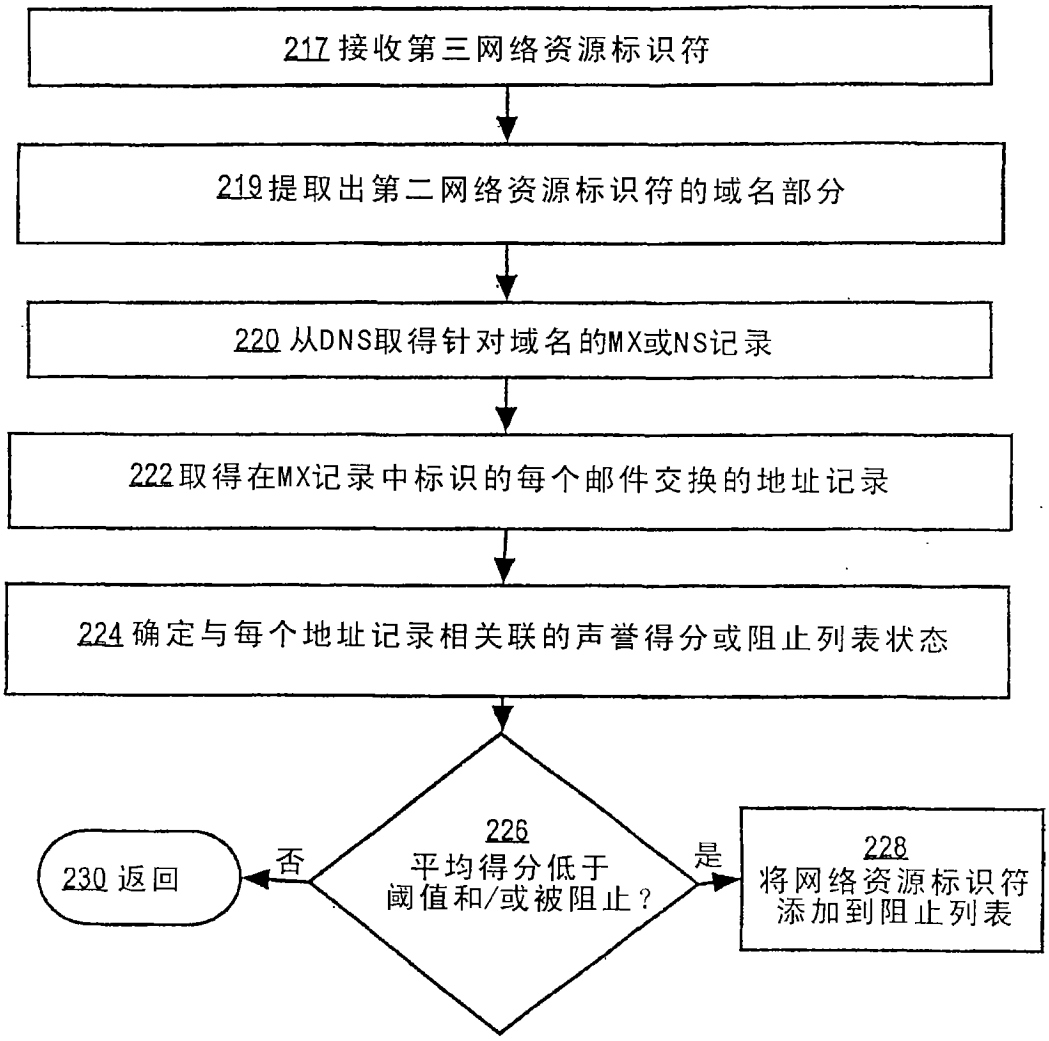

217 接收第三网络资源标识符
219 提取出第二网络资源标识符的域名部分
220 从DNS取得针对域名的MX或NS记录
222 取得在MX记录中标识的每个邮件交换的地址记录
224 确定与每个地址记录相关联的声誉得分或阻止列表状态
226
平均得分低于阈值和/或被阻止？
否
是
230 返回
228
将网络资源标识符添加到阻止列表

图2C

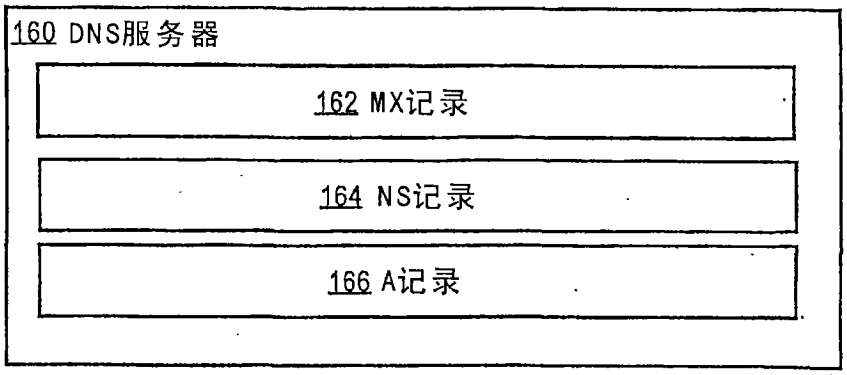

160 DNS服务器
162 MX记录
164 NS记录
166 A记录

图3

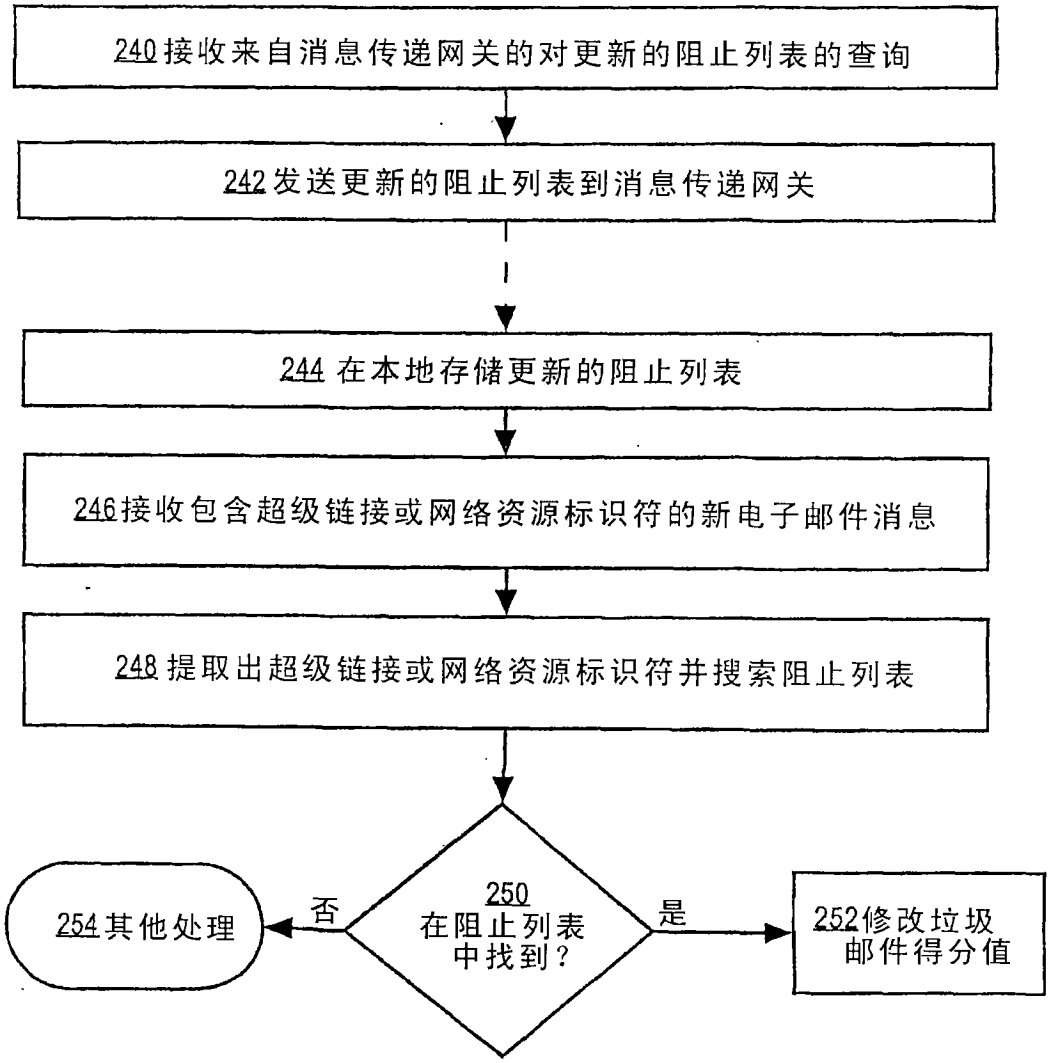

240 接收来自消息传递网关的对更新的阻止列表的查询
242 发送更新的阻止列表到消息传递网关
244 在本地存储更新的阻止列表
246 接收包含超级链接或网络资源标识符的新电子邮件消息
248 提取出超级链接或网络资源标识符并搜索阻止列表
250 在阻止列表中找到？
否
是
254 其他处理
252 修改垃圾邮件得分值

图2D

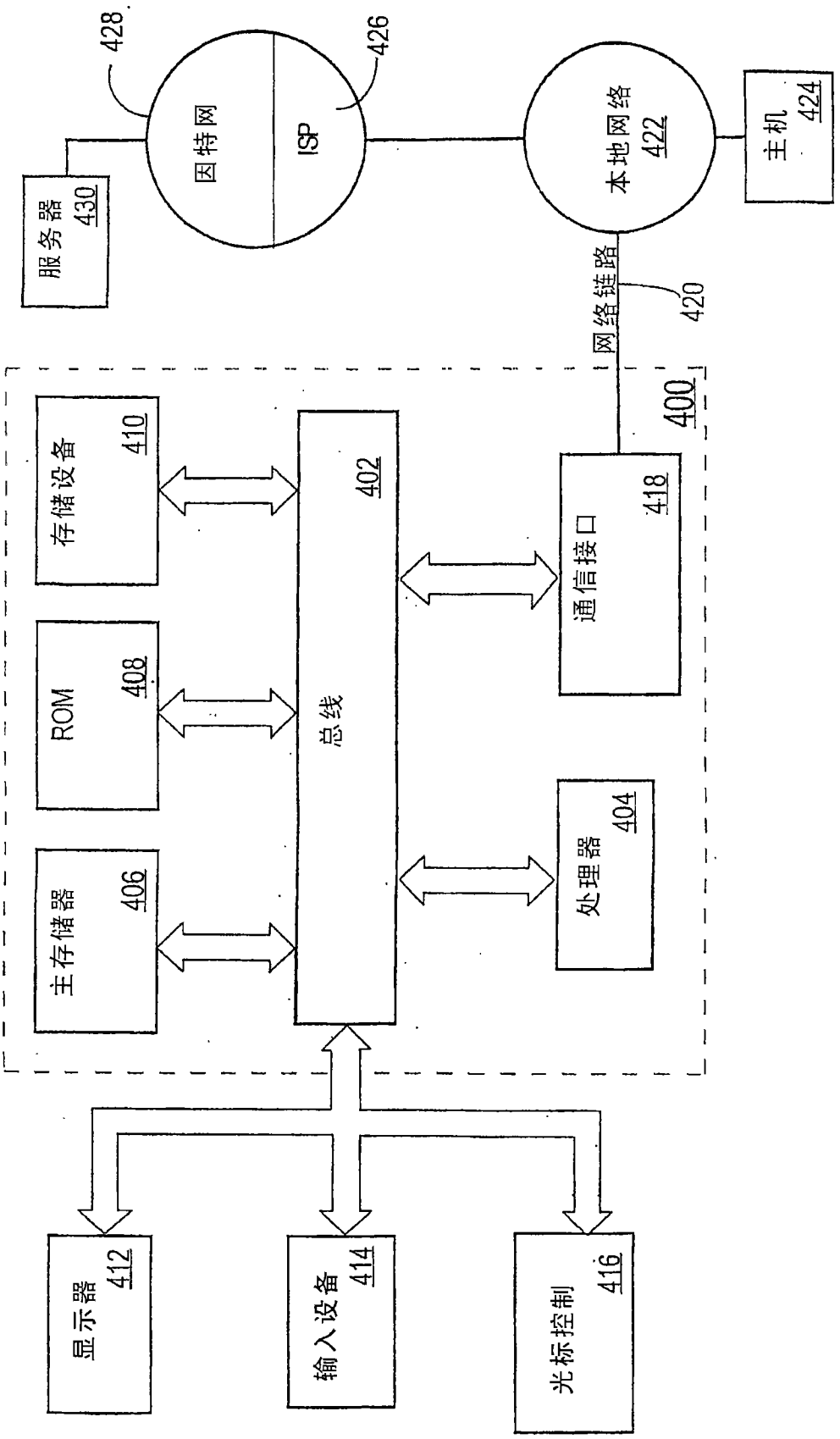

428
因特网
ISP
426
服务器
430
本地网络
422
主机
424
网络链路
420
400
存储设备
410
402
通信接口
418
ROM
408
总线
主存储器
406
处理器
404
显示器
412
输入设备
414
光标控制
416

图4