(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 102918810 B
(45)授权公告日 2016.05.11

(21)申请号 201180025046.3
(22)申请日 2011.05.02
(30)优先权数据
12/785,348 2010.05.21 US
(85)PCT国际申请进入国家阶段日
2012.11.20
(86)PCT国际申请的申请数据
PCT/US2011/034800 2011.05.02
(87)PCT国际申请的公布数据
WO2011/146232 EN 2011.11.24
(73)专利权人 微软技术许可有限责任公司
地址 美国华盛顿州
(72)发明人 G·古雷维奇 V·W·H·博克特 W·德 格拉夫
(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 范玮
(51)Int.Cl.
H04L 12/58(2006.01)

(56)对比文件
US 2007162394 A1,2007.07.12,
US 2006048210 A1,2006.03.02,
US 2006121880 A1,2006.06.08,
US 2005210272 A1,2005.09.22,
US 2004203589 A1,2004.10.14,

审查员 李红玲

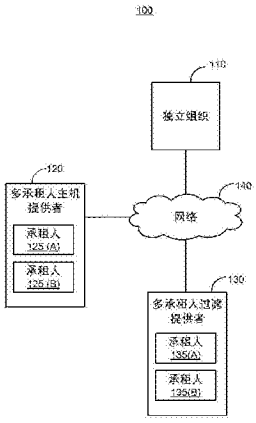
权利要求书2页 说明书8页 附图4页

(54)发明名称

用于多承租人环境中的可信电子邮件通信的方法和系统

(57)摘要

可以提供可信电子邮件通信。可以验证消息源组织。当从经确认的消息源组织接收到发送给接收者组织的消息时,可以做出关于该接收者组织是否支持归属数据扩展的判断。如果是,则可以将该消息和与消息源组织相关联的归属元素一起传送给接收者组织。



CN 102918810 B

1. 一种用于提供可信电子邮件通信的方法，所述方法包括：

从消息源组织接收送往接收者组织的消息；

标识所述消息源组织；

判断所述接收者组织是否支持归属数据扩展，包括判断所述接收者组织是否响应于经由简单邮件传输协议（SMTP）传送的 EHLO 命令来通告对所述归属数据扩展的支持；以及

响应于判断所述接收者组织支持所述归属数据扩展，将所述消息和与所述消息源组织相关联的归属元素一起传送给所述接收者组织。

2. 如权利要求 1 所述的方法，其特征在于，进一步包括在所述消息源组织和所述接收者组织之间建立安全通信信道，其中，所述消息源组织包括独立组织且所述接收者组织包括多承租人电子邮件服务提供者。

3. 如权利要求 1 所述的方法，其特征在于，将所述消息和与所述消息源组织相关联的归属数据一起传送给所述接收者组织进一步包括在将所述消息传送给所述接收者组织之前将所述归属元素添加到所述消息。

4. 如权利要求 1 所述的方法，其特征在于，判断所述接收者组织是否支持所述归属数据扩展包括响应于经由所述简单邮件传输协议（SMTP）传送的 EHLO 命令判断所述接收者组织是否通告对所述归属数据扩展的支持。

5. 如权利要求 1 所述的方法，其特征在于，进一步包括：

执行所述消息源组织的域所有者确认。

6. 一种用于提供可信电子邮件通信的方法，包括：

与多承租人电子邮件提供者建立信任关系；

告知所述多承租人电子邮件提供者归属元素受到支持，包括响应于经由简单邮件传输协议（SMTP）传送的 EHLO 命令通告对归属数据扩展的支持；

从所述多承租人电子邮件提供者的客户端接收电子邮件消息；

判断所述电子邮件消息是否与归属元素相关联；

响应于判断所述电子邮件消息与所述归属元素相关联，判断所述归属元素是否将所述客户端标识为可信发送者；以及

响应于判断所述归属元素将所述客户端标识为可信发送者，应用与从可信发送者接收的电子邮件消息相关联的电子邮件处理规则。

7. 如权利要求 6 所述的方法，其特征在于，所述归属元素进一步作为下列各项中的至少一项而被接收到：与所述电子邮件消息相关联的首部、所述电子邮件消息的正文的子集、以及与所述电子邮件消息相关联的附件。

8. 如权利要求 6 所述的方法，其特征在于，应用与从可信发送者接收的电子邮件消息相关联的电子邮件处理规则包括绕开被应用到不是从可信发送者接收的电子邮件消息的至少一个消息分析器。

9. 如权利要求 6 所述的方法，其特征在于，应用与从可信发送者接收的电子邮件消息相关联的电子邮件处理规则包括允许比对于不是从可信发送者接收的电子邮件消息所允许的更大的附件大小。

10. 如权利要求 6 所述的方法，其特征在于，进一步包括：

响应于判断所述归属元素不将所述客户端标识为可信发送者：

接受所述消息以供传递，以及

应用与不是从可信发送者接收的电子邮件消息相关联的第二电子邮件处理规则。

11. 如权利要求 6 所述的方法，其特征在于，进一步包括 ：

响应于判断所述归属元素不将所述客户端标识为可信发送者，拒绝所述消息。

12. 如权利要求 6 所述的方法，其特征在于，进一步包括 ：

响应于判断所述归属元素不将所述客户端标识为可信发送者 ：

向管理员告知来自非可信客户端的所述电子邮件消息，以及

临时拒绝所述消息直到接收到是否投递所述电子邮件消息的决定。

13. 一种用于提供可信电子邮件通信的方法，所述方法包括 ：

创建与源组织的经确认的通信信道，其中，用于创建所述经确认的通信信道包括用于执行基于传输层安全 (TLS) 协议证书的认证，

从所述源组织接收电子邮件消息，其中，所述源组织包括多承租人电子邮件服务提供者，

判断所述电子邮件消息是否与包括在之前接收到的简单邮件传输协议 (SMTP) 命令中的归属数据元素相关联，

响应于判断所述电子邮件消息与归属数据元素相关联，判断所述归属数据元素是否标识可信源组织，

响应于判断所述归属数据元素标识可信源组织，在投递所述电子邮件消息之前应用至少一个第一消息处理规则，以及

响应于判断所述归属数据元素不标识可信源组织，在投递所述电子邮件消息之前应用至少一个第二消息处理规则。

14. 一种用于提供可信电子邮件通信的系统，所述系统包括 ：

用于从消息源组织接收送往接收者组织的消息的装置 ；

用于标识所述消息源组织的装置 ；

用于判断所述接收者组织是否支持归属数据扩展的装置，包括用于判断所述接收者组织是否响应于经由简单邮件传输协议 (SMTP) 传送的 EHLO 命令来通告对所述归属数据扩展的支持的装置 ；以及

用于响应于判断所述接收者组织支持所述归属数据扩展，将所述消息和与所述消息源组织相关联的归属元素一起传送给所述接收者组织的装置。

用于多承租人环境中的可信电子邮件通信的方法和系统

技术领域

[0001] 本申请涉及可信电子邮件通信，尤其涉及多承租人环境中的可信电子邮件通信。

背景技术

[0002] 多承租人环境中的可信电子邮件通信是用于认证从多承租人系统接收的消息的过程。在一些情形中，一个组织可以从多个其他组织接收电子邮件。该组织可能希望将某些消息处理规则应用到被认证为来自特定的其他组织的消息，但使得其他消息遵守不同的规则。常规的电子邮件系统可以采用基于证书的认证和 / 或基于 IP 地址的认证来与另一组织的电子邮件系统建立可信通信信道。然而，这些技术，可能仅在可信信道的双方都在其本地主控它们自己的电子邮件系统时是有用的。当任一方（或双方）使用由服务提供者主控的电子邮件服务时，提供者的证书和 IP 地址可以在该服务提供者的所有客户之间共享，且可能不足以与服务提供者的特定客户（又称为承租人）建立可信通信信道。

[0003] 概述

[0004] 提供本概述以便以简化形式介绍下面在详细描述中进一步描述的概念的选集。本概述不旨在标识所要求保护的本主题的关键特征或必要特征。本概述也不预期用来限制所要求保护的本主题的范围。

[0005] 可以提供可信电子邮件通信。可以确认消息源组织。当从经确认的消息源组织接收到发送给接收者组织的消息时，可以做出关于该接收者组织是否支持归属数据扩展的判断。如果是，则可以将该消息和与消息源组织相关联的归属元素一起传送给接收者组织。

[0006] 以上一般描述和下列详细描述两者提供示例且仅是解释性的。因此，以上一般描述和下列详细描述不应被认为是限制。进一步，可以提供除了在此陈述的那些特征或变更的之外的特征或变更。例如，各实施例可以涉及详细描述中所描述的各种特征组合和子组合。

[0007] 附图简述

[0008] 附图合并在本公开内容中且构成本公开内容的一部分，附图阐释了本发明的各种实施例。附图中：

[0009] 图 1 是操作环境的框图；

[0010] 图 2 是用于提供消息源确认和归属的方法的流程图；

[0011] 图 3 是用于提供可信电子邮件通信的方法的流程图；以及

[0012] 图 4 是包括计算设备的系统的框图。

[0013] 详细描述

[0014] 下列详细描述参考了附图。在可能之处，各图和下列描述中使用的相同的参考数字指代相同的或相似的元素。尽管可以描述本发明的各实施例，但修改、改编和其他实现是可能的。例如，可以对附图中所阐述的元素进行替换、添加或修改，且可以同替代、重排所公开的方法或向其添加步骤来修改在此描述的方法。因此，下列详细描述不限制本发明。相反，本发明的正确范围由所附权利要求界定。

[0015] 可以提供多承租人环境中的可信电子邮件通信。根据本发明的各实施例，从多承租人电子邮件系统接收电子邮件消息的电子邮件系统可以将所接收的消息归结为多承租人系统的特定承租人。这种归属可以允许接收系统执行与为非归属消息而执行的不同的消息处理规则。例如，可以将额外能力、显示选项和 / 或绕开过滤步骤的能力授权给与特定承租人相关联的消息。术语“独立系统”可以是指部署在第一方本地的电子邮件系统。术语“多承租人系统”可以是指由电子邮件服务提供者主控且由第二方使用的电子邮件系统和 / 或服务。术语“承租人”可以是指多承租人系统中的第二方的表示。

[0016] 图 1 是用于提供可信电子邮件通信的操作环境 100 的框图。操作环境可以包括独立组织 110、包括多个电子邮件主控承租人 125(A)-(B) 的多承租人电子邮件主控提供者 120、以及包括多个电子邮件过滤承租人 135(A)-(B) 的多承租人电子邮件过滤提供者 130。独立组织 110、多承租人电子邮件主控提供者 120 和 / 或多承租人电子邮件过滤提供者 130 中的每一个都可以包括至少一个消息传输代理（未示出）。独立组织 110、多承租人电子邮件主控提供者 120 和 / 或多承租人电子邮件过滤提供者 130 可以经由诸如局域网、蜂窝式数据网络和 / 或公共网络（例如因特网）等的网络 140 相互通信。多承租人电子邮件主控提供者 120 可以包括用于提供电子邮件发送 / 接收功能性以及用于存储与多个电子邮件主控承租人 125(A)-(B) 相关联的电子邮件的存储器存储两者的服务提供者。多承租人电子邮件过滤提供者 130 可以包括用于从多个电子邮件过滤承租人 135(A)-(B) 接收电子邮件消息和 / 或在根据至少一个消息处理规则处理电子邮件消息之后向多个电子邮件过滤承租人 135(A)-(B) 发送电子邮件消息的邮件中继。例如，多承租人电子邮件过滤提供者 130 可以对所中继的电子邮件消息执行防病毒扫描和 / 或垃圾邮件过滤。多承租人电子邮件主控提供者 120 和 / 或多承租人电子邮件过滤提供者 130 在全文中可以被称为“多承租人系统”，且电子邮件主控承租人 125(A)-(B) 和 / 或电子邮件过滤承租人 125(A)-(B) 在全文中可以被称为“承租人”。电子邮件过滤承租人 125(A)-(B) 可以用于提供由独立组织 110 使用的一些邮件处理功能性，例如接收、发送和向与电子邮件过滤承租人 125(A)-(B) 的订阅组织相关联的接收者投递消息。例如，电子邮件过滤承租人 125(A) 的订阅组织可以用于发送、接收和存储消息而不需要来自多承租人电子邮件过滤提供者 130 的辅助，但可以选择通过多承租人电子邮件过滤提供者 130 中继传入和 / 或传出消息，以便接收对诸如防病毒扫描等的附加服务的访问。

[0017] 消息传输代理 (MTA) 可以包括可以在单跳和 / 或多跳应用级事务中将电子邮件消息（电子邮件）从一个计算机传递到另一计算机的计算机进程和 / 或软件代理。MTA 可以实现简单邮件传输协议 (SMTP) 的客户端（发送）和服务器（接收）部分两者。SMTP 是用于诸如网络 140 等的跨因特网协议 (IP) 网络的电子邮件传输的因特网标准。SMTP 在 RFC RFC 5321(2008) 中界定，RFC RFC 5321(2008) 包括了扩展 SMTP(ESMTP) 附加部分。操作环境 100 的组件可以使用与 SMTP 相关联的命令来通信。例如，在交换电子邮件消息之前，多承租人主控提供者 120 可以经由 SMTP 向独立组织 110 发送“EHLO”命令。独立组织 110 可以用诸如“DSN”、“STARTTLS”和 / 或“SIZE”等的受支持的 SMTP 扩展的列表应答。根据本发明的各实施例，独立组织 110 可以在应答中指示它支持归属数据元素扩展，例如通过在受支持的扩展的列表中包括扩展名称“XOORG”。

[0018] 在独立组织 110、多承租人电子邮件主控提供者 120 和 / 或多承租人电子邮件过滤

提供者 130 之中可以期望到特定承租人的安全通信信道。例如，独立组织 110 可能需要与电子邮件主控承租人 125(A) 安全地通信。独立组织 110 可能需要即使电子邮件主控承租人 125(B) 通过欺骗封装和 / 或消息内容属性来尝试假扮电子邮件主控承租人 125(A) 也能够将从电子邮件主控承租人 125(A) 到来的消息与从电子邮件主控承租人 125(B) 到来的消息区分开来。在类似的示例中，电子邮件过滤承租人 135(A) 可能需要与电子邮件主控承租人 125(A) 安全地通信，在这种情况中，通信的双方可能必须是承租人特定的。

[0019] 通过建立到特定承租人的安全通信信道，可以应用一些政策，和 / 或可以绕开强加在不通过该信道接收的消息上的一些限制。例如，可以绕开防垃圾邮件过滤，电子邮件客户端程序中的独特的格式化 / 呈现可以基于某些消息属性（例如基于具体的消息首部看上去是内部邮件的跨场所邮件），可以准许向可以被配置为不接受来自因特网的邮件的收件人和收件组发送电子邮件的能力，消息和 / 或附件大小限制可以是不严格的，可以允许不同的附件类型等等。

[0020] 图 2 是陈述根据本发明的各实施例的用于提供消息源确认和归属的方法 200 中涉及的一般步骤的流程图。可以使用如下面相对于图 4 更详细地描述的计算设备 400 实现方法 200。下面将更详细地描述实现方法 200 的各步骤的方式。方法 200 可以从开始框 205 开始并进行到步骤 210，步骤 210 中，计算设备 400 可以从源组织接收消息。例如，多承租人主控提供者 120 可以从主控承租人 125(A) 接收送往在独立系统 110 处的接收者的消息。

[0021] 然后，方法 200 可以进行到步骤 220，步骤 220 中，计算设备 400 可以识别源组织。例如，多承租人主控提供者 120 可以判断消息是不是从经确认的承租人接收到。根据本发明的各实施例，多承租人主控提供者 120 也可以验证首部与正确标识源组织的消息相关联。根据本发明的各实施例，多承租人系统可以确认主控承租人（例如，主控承租人 125(A)-B) 和 / 或过滤承租人 135(A)-(B)），例如，通过要求由在与多承租人主控提供者 120 处设法主控与给定域相关联的其电子邮件通信的组织对域所有者记录做出可验证的改变，以及 / 或者利用由多承租人电子邮件过滤提供者 130 提供的服务。

[0022] 在多承租人系统首次与新承租人通信时，该系统可以执行新承租人的域确认。这可以在新承租人签约服务时进行一次。可以对每一所接收到的消息执行与所接收到的供传递的消息相关联的承租人的标识。可以例如通过消息发送者的用户名 / 密码认证完成标识。一旦发送者的承租人被标识，域（在签订时确认）可以被用作该消息的归属数据。

[0023] 然后，方法 200 可以进行到步骤 225，步骤 225 中，计算设备 400 可以与接收者组织建立安全通信信道。例如，多承租人主控提供者 120 执行与独立组织 110 的认证。在独立组织 110 和多承租人主控提供者 120 之间的认证可以使用传输层安全 (TLS) 和基于证书的相互认证来实现。也可以使用诸如物理安全专用线路等的其他实现。

[0024] 传输层安全 (TLS) 包括为在诸如因特网等的网络上的通信提供安全的密码协议。TLS 在传输层端对端地加密网络连接的各部分。TLS 协议可以允许客户端 / 服务器应用跨越网络以被设计为防止窃听和篡改的方式通信。在根据本发明的各实施例的双边连接模式中，TLS 可以被用来执行相互认证。相互认证要求通信的每一方都包括定义所要求的字段和数据格式的诸如 X.509 证书等的证书。

[0025] 从步骤 225，方法 200 可以进行到步骤 230，步骤 230 中，计算设备 400 可以判断接收者是否支持归属数据。例如，可以由接收者系统作为 EHLO 命令响应的一部分通告被称

为 XOORG 的 SMTP 扩展。这可以响应于在 STARTTLS 命令之后的 EHLO 命令和 / 或响应于第一 EHLO 命令而完成。XOORG 通告可以包括给发送方的信号 :“MAIL FROM:”命令 (也被称为 XOORG) 的新参数可以用来发送代表其发送消息的组织的身份。该身份可以包括完全合格域名。例如,独立系统 110 可以用在多承租人主控提供者 120 发送 EHLO SMTP 命令时用 XOORG 扩展作出响应。然后,多承租人主控提供者 120 可以判断独立系统 110 支持归属数据。

[0026] 如果接收者不支持归属数据,则方法 200 可以进行到步骤 260,步骤 260 中计算设备 400 可以传送没有归属数据的消息。例如,多承租人主控提供者 120 可以使用 SMTP 在网络 140 上将消息传送给独立系统 110。然后,在步骤 265,方法 200 可以结束。

[0027] 如果,在步骤 230,判断接收者支持归属数据,则方法 200 可以进行到步骤 240,步骤 240 中,计算设备 400 可以判断源组织是否受到接收组织的信任。接收组织可以用于给发送组织提供它想要从中接收归属数据的组织的列表。例如,独立系统 110 可以告知多承租人主控提供者 120,它信任主控承租人 125(A) 但不信任承租人 125(B)。如果源不可信,则方法 200 可以进行到步骤 260,步骤 260 中,如上所述,计算设备 400 可以传送消息。

[0028] 如果从受到接收者信任的源接收到消息,则方法 200 可以进行到步骤 250,步骤 250 中计算设备 400 可以传送与源相关联的归属数据。每一承租人的身份可以由多承租人系统在服务提供过程期间可靠地确认。因而,多承租人系统可以具有将由其任何承租人产生的任何消息归结于产生该消息的实际承租人的可靠方式,且可以能够将从独立系统 110 接收到的消息归结于其各自的组织。

[0029] 根据本发明的各实施例,多承租人系统也可以用于标识由多承租人系统接收的消息的发送者以供传递给其承租人中的一个。例如,多承租人系统可以具有足以标识独立系统 110 的数据 (例如消息源组织的证书中的完全合格域名 (FQDN)) 且可以基于安全地认证的通信信道可靠地将传入消息归结于第一方。

[0030] 为了将与发送者相关联的归属数据提供给接收者,例如,计算设备 400 可以使用 SMTP 协议扩展。XOORG 命令可以在 SMTP 框架内实现和 / 或 XOORG 参数可以被包括在 SMTP 标准框架内的现有“MAIL FROM:”命令中。分开的 XOORG 命令可以被用来传送与在单个 SMTP 会话期间从给定的源组织 (例如,来自多承租人系统的具体承租人) 传送的多个消息相关联的归属数据,而对每一消息,“MAIL FROM:”命令的 XOORG 参数可以变化。协议扩展可以允许接收系统在接收到所有收件人和实际消息数据之前决定消息是否可信。

[0031] 作为另一示例,归属数据可以被添加导消息本身并在诸如“X-Originator Organization(X- 发起者组织)”等的首部中传送。至于 SMTP 扩展,首部的值可以包括代表其发送消息的组织的身份,且可以包括完全合格域名。SMTP 扩展和首部不互斥,且两者都可被提供。协议参数中提供的数据可以优先于首部值。如果接收 MTA 检测到差异,它可以对首部重新加戳以便匹配协议参数值。

[0032] 从步骤 250,方法 200 可以进行到步骤 260,步骤 260 中,计算设备 400 可以如上所述传送消息。根据本发明的各实施例,归属数据和消息可以被一起传送,只要归属数据被包括在被相对于步骤 250 描述的消息首部中。然后,在步骤 265,方法 200 可以结束。

[0033] 图 3 是陈述根据本发明的各实施例的用于提供可信电子邮件通信的方法 300 中所涉及的一般步骤的流程图。可以使用如下面相对于图 4 更详细地描述计算设备 400 实现方法 300。下面将更详细地描述实现方法 300 的各步骤的方式。方法 300 可以从开始框 305

开始并进行到步骤310，步骤310中，计算设备400可以与另一组织建立信任关系。例如，独立系统110可以被配置为接受来自诸如多承租人主控提供者120等的给定的多承租人系统的归属数据。根据本发明的各实施例，归属数据可以仅从可信的组织接受，且不可以从尝试建立安全信道的任何人接收。

[0034] 然后，方法300可以进行到步骤320，步骤320中，计算设备400可以告知消息提供者它支持归属数据。例如，响应于来自多承租人主控提供者120的SMTP EHLO命令，如果多承租人主控提供者120被配置成可信系统，则独立系统110可以传送它支持“XOORG”扩展的指示符。

[0035] 从步骤320，方法300可以进行到步骤330，步骤330中，计算设备400可以从可信消息提供者接收消息。例如，多承租人主控提供者120可以将电子邮件消息从主控承租人125(A)传送到独立系统110。

[0036] 从步骤330，方法300可以进行到步骤340，步骤340中，计算设备400可以判断电子邮件消息是否与归属数据相关联。例如，独立系统110可以判断XOORG数据是否如以上相对于方法200的步骤240所描述的是作为SMTP通信的一部分和/或作为消息首部的一部分而被接收到的。

[0037] 在步骤340，如果计算设备400判断消息与归属数据相关联，方法300可以进行到步骤350，步骤350中，计算设备400可以判断归属数据是否标识可信源组织。例如，独立系统110可以信任主控承租人125(A)但不信任主控承租人125(B)。独立系统110可以检查归属数据（例如，使用多承租人主控系统120的源组织的完全合格域名）并将该数据与内部存储的可信组织的域的列表相比较。

[0038] 在步骤350，如果计算设备400判断归属数据与可信源相关联，则方法300可以进行到步骤360，步骤360中，计算设备400可以应用与来自可信源的消息相关联的消息处理规则。例如，来自可信源的消息可以绕开垃圾邮件过滤过程，可以被允许更大的附件尺寸和/或不同的附件类型，和/或可以使外观格式化被应用。根据本发明的各实施例，不同的可信源可以与不同的消息处理规则相关联。例如，来自主控承租人125(A)和主控承租人125(B)的消息两者都可以受到信任，但是仅可以准许来自主控承租人125(A)的消息发送大于10MB的附件，同时允许两者都绕开垃圾邮件过滤。然后，在步骤375，方法300可以结束。

[0039] 如果在步骤340判断消息不具有归属数据和/或在步骤350判断归属数据不与可信源相关联，方法300可以进行到步骤370，步骤370中，可以应用不可信任的和/或默认的消息处理规则。例如，这样的消息可以由垃圾邮件过滤处理且可以受到与可信消息不同的附件限制。然后，方法300可以在步骤375结束。

[0040] 当接收者（例如，独立系统110）接收到归属数据参数时，它可以检查它是否被配置为信任所标识的承租人。如果承租人是可信的，则独立系统110可以允许消息绕开其适用的匿名消息政策中的一些。如果承租人不被配置成可信的，则独立系统110可以例如以三种方式中的一种起作用：1）接受消息并将其看作是从非可信方到来的任何消息，2）用4XX响应临时拒绝消息，或3）用5XX响应永久拒绝消息。4XX和5xx响应可以包括根据SMTP标准的错误/告知消息。临时拒绝可以导致来自非可信“发起者组织”的消息排队一段时间，这给双方的管理员提供了解决配置问题和/或审阅消息并投递排队消息而不影响最终

用户的机会。

[0041] 依照本发明的一个实施例可以包括用于提供可信电子邮件通信的系统。该系统可以包括存储器存储和被耦合到存储器存储的处理单元。处理单元可以用于确认消息源组织，从经确认的消息源组织接收送往接收者组织的消息，判断接收者组织是否支持归属数据扩展，并且如果是，则将该消息传送给带有与消息源组织相关联的归属元素的接收者组织。归属元素可以被添加到消息，例如在消息首部、消息正文中和 / 或作为附件，而不考虑是否判断了接收者组织支持归属数据扩展。然后，接收者组织可以判断是否接受、拒绝、忽略和 / 或利用所添加的归属数据。

[0042] 依照本发明的另一实施例可以包括用于提供可信电子邮件通信的系统。该系统可以包括被耦合到存储器存储的存储器存储和处理单元。处理单元可以用于与多承租人电子邮件提供者建立信任关系，告知多承租人电子邮件提供者归属元素受到支持，从多承租人电子邮件提供者的客户端承租人接收电子邮件消息，并判断电子邮件消息是否与归属元素相关联。如果电子邮件消息与归属元素相关联，则处理单元可以用于判断归属元素是否将客户端承租人标识为可信发送者，且如果是，则应用与从可信发送者接收的电子邮件消息相关联的电子邮件处理规则。

[0043] 依照本发明的又一实施例可以包括用于提供可信电子邮件通信的系统。该系统可以包括存储器存储和被耦合到存储器存储的处理单元。处理单元可以用于与源组织创建经确认的通信信道，从源组织接收电子邮件消息，判断电子邮件消息是否与归属数据元素相关联，且如果是，则判断归属数据元素是否标识可信源组织。如果归属数据元素标识可信源组织，则处理单元可以用于在投递电子邮件消息之前应用至少一个第一消息处理规则。如果归属数据元素不标识可信源组织，则处理单元可以用于在投递电子邮件消息之前应用至少一个第二消息处理规则。

[0044] 图 4 是包括计算设备 400 的系统的框图。根据本发明的一个实施例，前述的存储器存储和处理单元可以在，诸如图 4 的计算设备 400 等的计算设备中实现。硬件、软件或固件的任何合适的组合可以被用来实现存储器存储和处理单元。例如，可以借助于计算设备 400 或与计算设备 400 组合的任何其他计算设备 418 实现存储器存储和处理单元。根据本发明的各实施例，前述的系统、设备和处理器是示例，且其他系统、设备和处理器可以包括前述的存储器存储和处理单元。此外，计算设备 400 可以包括如上所述的系统 100 的操作环境。系统 100 可以在其他环境中操作且不限于计算设备 400。

[0045] 参考图 4，依照本发明的一个实施例的系统可以包括诸如计算设备 400 等的计算设备。在基本配置中，计算设备 400 可以包括至少一个处理单元 402 和系统存储器 404。取决于计算设备的配置和类型，系统存储器 404 可以包括但不限于易失性 (例如随机存取存储器 (RAM))、非易失性 (例如只读存储器 (ROM))、闪速存储器或任何组合。系统存储器 404 可以包括操作系统 405、一个或多个编程模块 406，且可以包括消息传输代理 (MTA)407。例如，操作系统 405 可以适用于控制计算设备 400 的操作。本发明的各实施例可以与图形库、其他操作系统或任何其他应用程序联合操作，且不限于任何特定的应用或系统。图 4 中，这种基本配置由虚线 408 内的那些组件阐释。

[0046] 计算设备 400 可以具有附加的特征或功能性。例如，计算设备 400 也可以包括附加的数据存储设备 (可移动和 / 或不可移动)，诸如例如磁盘、光盘或带。图 4 中，这样的附

加存储由可移动存储 409 和不可移动存储 410 阐释。计算设备 400 也可以包含可以允许设备 400 例如在分布式计算环境中的网络例如内联网或因特网上与其他计算设备 418 通信的通信连接 416。通信连接 416 是通信介质的一个示例。

[0047] 在此所使用的术语计算机可读介质可以包括计算机存储介质。计算机存储介质可以包括以用于存储诸如计算机可读指令、数据结构、程序模块或其他数据等的信息的任何方法或技术实现的易失性介质和非易失性介质、可移动介质和不可移动介质。系统存储器 404、可移动存储 409 和不可移动存储 410 都是计算机存储介质示例（即存储器存储）。计算机存储介质可以包括但不限于 RAM、ROM、电可擦除只读存储器 (EEPROM)、闪速存储器或其他存储器技术、CD-ROM、数字多用盘 (DVD) 或其他光存储、磁带盒、磁带、磁盘存储或其他磁存储设备、或可以被用来存储信息且可由计算设备 400 访问的任何其他介质。任何这样的计算机存储介质都可以是设备 400 的一部分。计算设备 400 也可以具有诸如键盘、鼠标、笔、声音输入设备、触摸输入设备等等的输入设备 412，也可以包括诸如显示器、扬声器、打印机等等的输出设备 414。前述的设备是示例，且可以使用其他设备。

[0048] 在此所使用的术语计算机可读介质也可以包括通信介质。通信介质可以由计算机可读指令、数据结构、程序模块、或诸如载波或其他传输机制等的经调制的数据信号中的其他数据实现，且包括任何信息传输介质。术语“经调制的数据信号”可以描述以编码信号中的信息的方式设定或改变一个或多个特性的信号。作为示例而非限制，通信介质可以包括诸如有线网络或直接有线连接等的有线介质，以及诸如声学、射频 (RF)、红外和其他无线介质等的无线介质。

[0049] 如上面所说明的，包括操作系统 405 的许多程序模块和数据文件可以被存储在系统存储器 404 中。尽管在处理单元 402 上执行，但编程模块 406（例如 MTA 407）可以执行包括例如如上所述的方法 200 的步骤和 / 或方法 300 的步骤中的一个或多个的进程。前述的进程是示例，且处理单元 402 可以执行其他进程。根据本发明的各实施例可以使用的其他编程模块可以包括电子邮件和联系人应用、字处理应用、电子表格应用、数据库应用、幻灯演示应用、绘图或计算机辅助应用等等。

[0050] 一般地，根据本发明的各实施例，程序模块可以包括可以执行特定的任务或可以实现特定的抽象数据类型的例程、程序、组件、数据结构和其他类型的结构。此外，本发明的各实施例可以与包括手持式设备、多处理器系统、基于微处理器的或可编程的消费性电子设备、小型计算机、大型计算机等等的其他计算机系统配置一起实践。本发明的各实施例也可以在分布式计算环境中实践，分布式计算环境中，任务由通过通信网络链接的远程处理设备执行。在分布式计算环境中，程序模块可以位于本地存储器存储设备和远程存储器存储设备两者。

[0051] 此外，本发明的各实施例可以在包括分立电子元件的电路中、在包含逻辑门的封装或集成电子芯片中、在利用微处理器的电路中或在包含电子元件或微处理器的单个芯片的电路上实践。本发明的各实施例也可以使用能够执行诸如例如与、非、或的逻辑操作的包括但不限于机械、光学、流体和量子技术的其他技术实践。另外，本发明的各实施例可以在通用计算机内或在任何其他电路或系统中实践。

[0052] 本发明的各实施例，例如，可以被实现为计算机进程（方法）、计算系统或产品，例如计算机程序产品或计算机可读介质。计算机程序产品可以是可由计算机系统读取且编码

用于执行计算机进程的指令的计算机程序的计算机存储介质。计算机程序产品也可以是可由计算系统读取并编码用于执行计算机进程的指令的计算机程序的载波上传播的传播信号。因此，本发明可以被具体化在硬件或软件（包括固件、驻留软件、微代码等等）中。换句话说，本发明的各实施例可以采用具有在介质中具体化的供指令执行系统使用或结合其使用的计算机可用的或计算机可读的程序代码的计算机可用的或计算机可读的存储介质上的计算机程序产品的形式。计算机可用的或计算机可读的介质可以是可以包含、存储、通信、传播、或传输供指令执行系统、装置或设备使用或结合其使用的程序的任何介质。

[0053] 计算机可用的或计算机可读的介质可以是例如但不限于电、磁、光、电磁、红外或半导体系统、装置、设备或传播介质。作为更具体的计算机可读介质示例（非详尽列表），计算机可读介质可以包括以下：具有一个或多个线的电连接、便携式计算机磁盘、随机存取存储器（RAM）、只读存储器（ROM）、可擦除可编程的只读存储器（EPROM或闪速存储器）、光纤和便携式光盘只读存储器（CD-ROM）。注意，计算机可用的或计算机可读的介质甚至可以是在其上打印程序的纸或另一合适的介质，这是由于可以经由例如纸或其他介质的光学扫描电捕捉程序，然后编译、解释、或如果有必要的话以另外方式以合适的方式处理程序，且然后将其存储在计算机存储器中。

[0054] 例如，以上参考根据本发明的各实施例的方法、系统和计算机程序产品的附图和操作阐释描述了本发明的各实施例。各框中可见的功能/动作可以脱离在任何流程图中所示出的次序而发生。例如，被示出为连续的两个框事实上可以基本平行地执行，或者有时各框可以以相反次序执行，这所涉及的功能性/动作。

[0055] 尽管已经描述了本发明的特定实施例，但可以存在其他实施例。此外，尽管本发明的各实施例已经被描述为与被存储在存储器和其他存储介质中的数据相关联的，但数据也可以被存储在诸如辅助存储设备（例如硬盘、软盘或CD-ROM）、来自因特网的载波、或其他形式的RAM或ROM等的其他类型的计算机可读介质上或从中读取。进一步，在不偏离本发明的前提下，可以以包括通过重新排序步骤和/或插入或删除步骤的任何方式修改所公开的方法的步骤。

[0056] 包括在此所包含的代码的版权在内的所有权利属于申请人的财产。申请人拥有并保留在此包含的代码的所有权利，且只授权在结合经授权的专利的复制时复制材料，且不用于其他目的。

[0057] 尽管本说明书包括示例，但本发明的范围由下列的权利要求指定。此外，尽管已经用对结构特征和/或方法论动作来说特异的语言描述了说明书，但权利要求不限于以上所描述的特征或动作。相反，以上所描述的具体的特征和动作是作为本发明的各实施例而公开的。

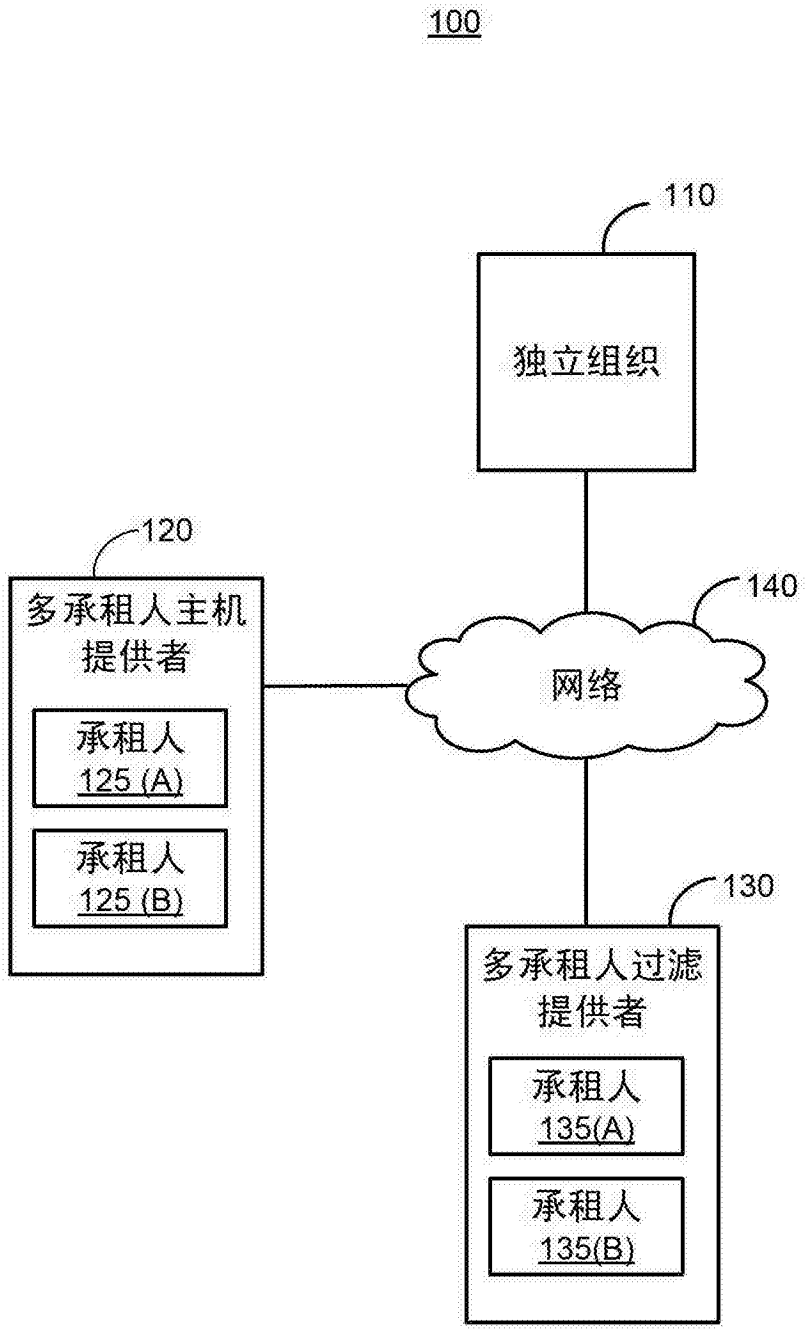

100
110
独立组织
120
多承租人主机提供者
承租人 125 (A)
承租人 125 (B)
140
网络
130
多承租人过滤提供者
承租人 135(A)
承租人 135(B)

图 1

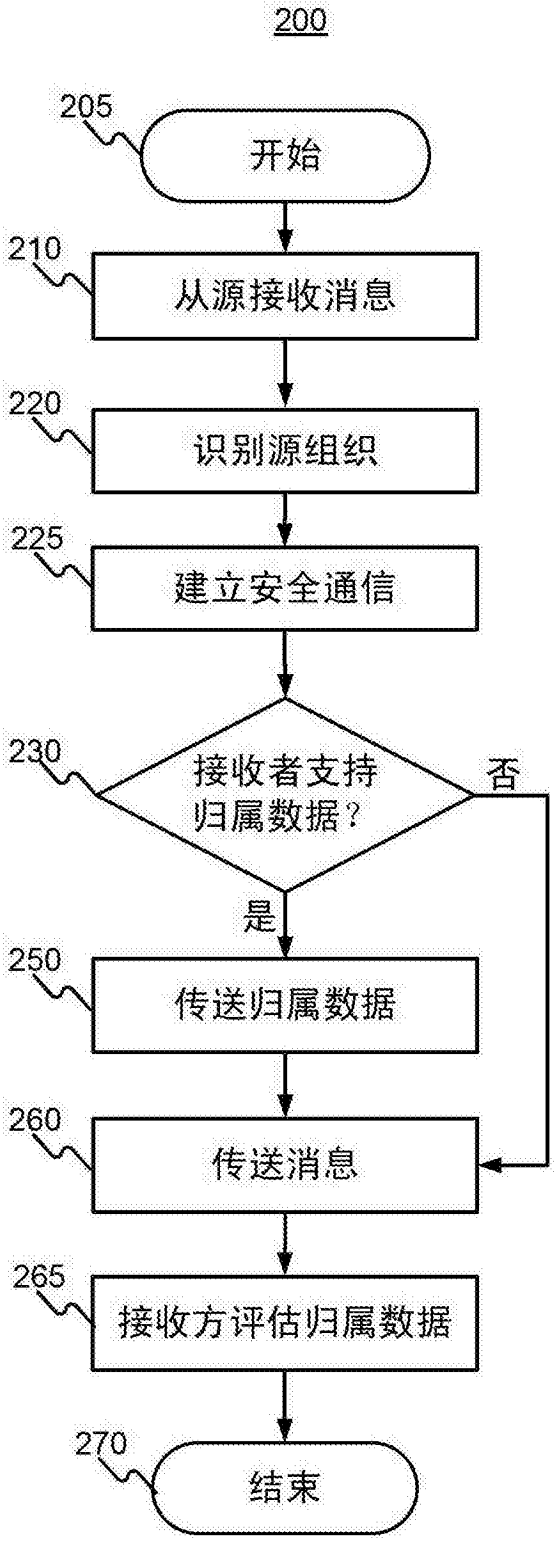

200
205
开始
210
从源接收消息
220
识别源组织
225
建立安全通信
230
接收者支持归属数据？
否
是
250
传送归属数据
260
传送消息
265
接收方评估归属数据
270
结束

图 2

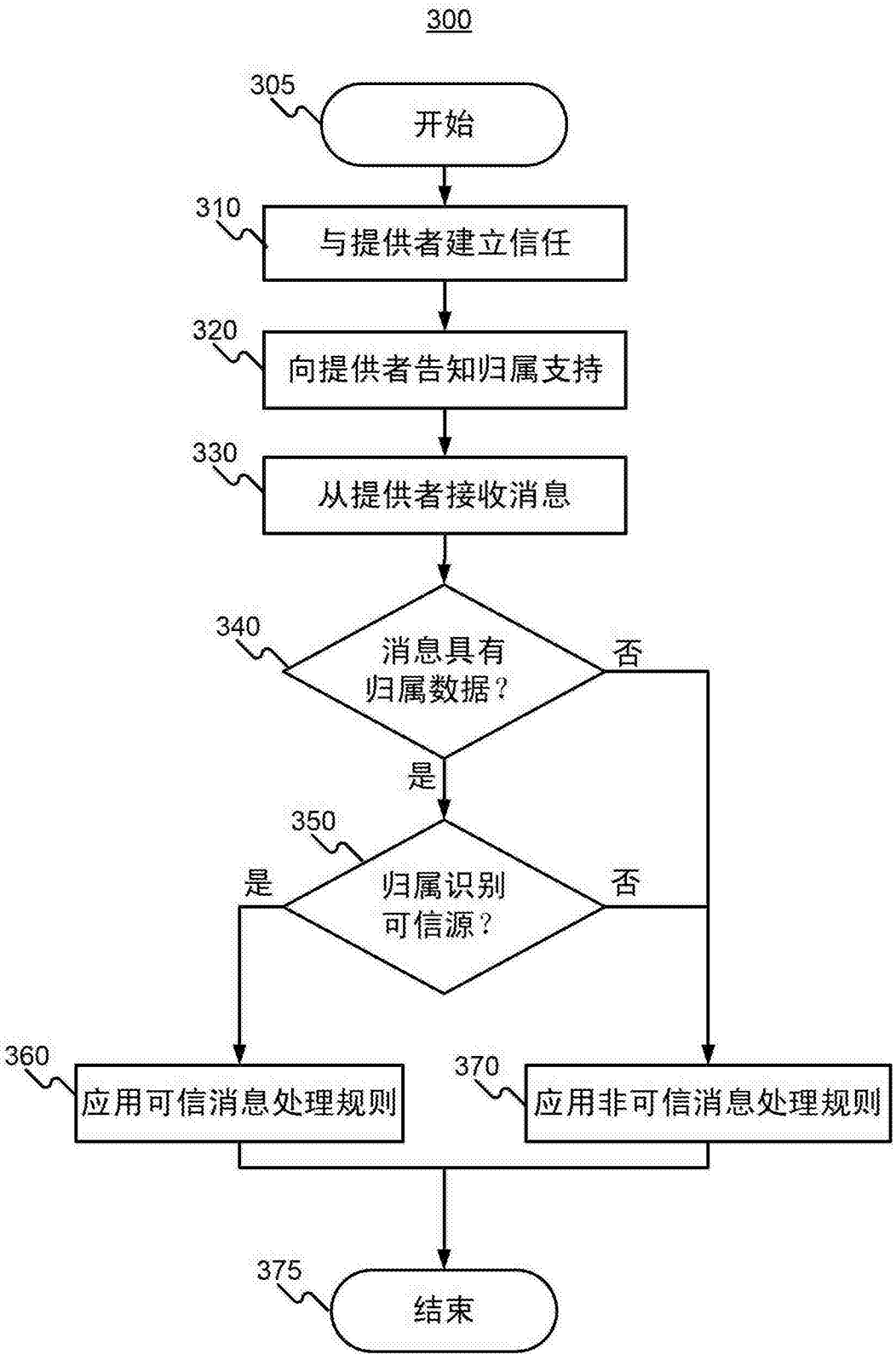

300
305
开始
310
与提供者建立信任
320
向提供者告知归属支持
330
从提供者接收消息
340
消息具有归属数据？
否
是
350
归属识别可信源？
是
否
360
应用可信消息处理规则
370
应用非可信消息处理规则
375
结束

图 3

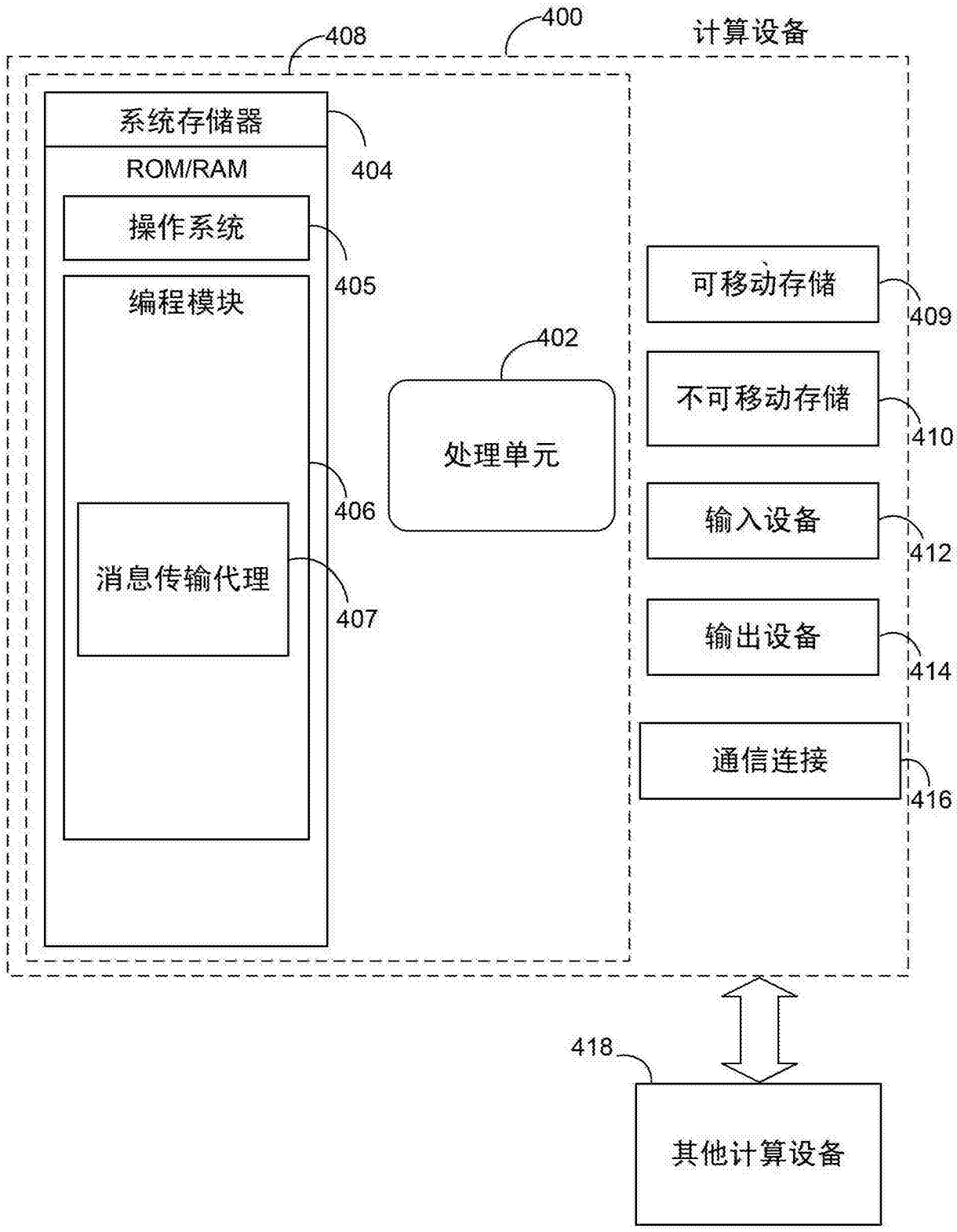

400
计算设备
408
系统存储器
ROM/RAM
404
操作系统
405
编程模块
406
消息传输代理
407
402
处理单元
可移动存储
409
不可移动存储
410
输入设备
412
输出设备
414
通信连接
416
418
其他计算设备

图 4