

(12) 发明专利申请

(10) 申请公布号 CN 102710537 A

(43) 申请公布日 2012. 10. 03

(21) 申请号 201210077642. 2

(22) 申请日 2012. 03. 22

(30) 优先权数据

13/053, 431 2011. 03. 22 US

(71) 申请人 微软公司

地址 美国华盛顿州

(72) 发明人 I. 奥西科夫

(74) 专利代理机构 中国专利代理(香港)有限公司 72001

代理人 董宁 刘鹏

(51) Int. Cl.

H04L 12/58(2006. 01)

H04L 29/06(2006. 01)

G06F 21/00(2006. 01)

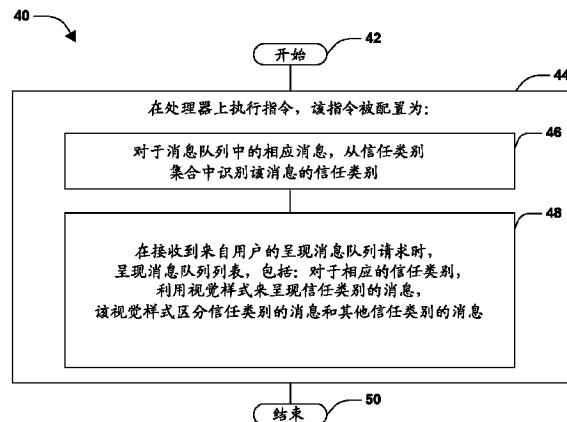
权利要求书 3 页 说明书 13 页 附图 9 页

(54) 发明名称

用于消息的信任类别的视觉样式

(57) 摘要

消息队列(例如，电子邮件邮箱)可以包括从各种源接收的并且包括各种类型内容的消息。对于相应的消息，信任类别可以被识别，例如，包括从已知源接收的消息的受信任消息类别、包括从未经验证的源接收的消息的不受信任消息类别、和包含潜在有害的附件或潜在不想要的内容的消息的可疑消息类别。可以用每个具有视觉样式的信任类别的消息将信息队列呈现给用户，该视觉样式可视地区分信任类别；例如，受信任消息可以在视觉上被强调，而可疑消息可以在视觉上不被强调。这样区别消息的方式可以使得用户能够对消息队列的消息进行分类，并可以缓解信任级别识别中误报的缺点(与将可疑消息移动到不同文件夹相比)。



1. 一种将消息(12)的消息队列(16)呈现给用户(14)的方法(40),该方法(40)在具有处理器(64)的设备(62)上执行并且包括：

在所述处理器(64)上执行(44)指令(86),该指令(86)被配置为：

对于所述消息队列(16)中的相应消息(12),从信任类别集识别(16)所述消息(12)的信任类别(32);以及

在接收到来自所述用户(14)的呈现所述消息队列(16)的请求时,呈现(48)消息队列列表(24),其中对于相应的信任类别(32),所述消息队列列表(24)包含利用视觉样式呈现的所述信任类别(32)的消息(12),所述视觉样式将该信任类别(32)的消息(12)与所述信任类别集合的其他信任类别(32)的消息(12)区别开来。

2. 如权利要求1所述的方法,识别相应消息的信任类别包括:将从信任启发法集合中选择出的至少一个信任启发法应用到所述消息,所述信任启发法集合包括：

消息发送者信任启发法；

消息接收者信任启发法；

消息递送信道信任启发法;以及

信息内容信任启发法。

3. 如权利要求1所述的方法：

所述设备包括信任规则集合,所述信任规则集合包括至少一个信任规则,所述信任规则包括：

至少一个信任规则标准,以及

满足所述至少一个信任规则标准的消息的信任类别;以及

识别消息的信任类别,其包括：

识别包括与所述消息相匹配的信任规则标准的至少一个信任规则,以及
为所述消息选择所述信任规则的信任类别。

4. 如权利要求3所述的方法,从信任规则源接收至少一个信任规则。

5. 如权利要求3所述的方法,所述指令被配置为:在从所述用户接收到指定至少一个信任规则标准和信任类别的定制信任规则时,将所述定制信任规则添加到所述信任规则集合。

6. 如权利要求3所述的方法,所述指令被配置为：

以所述消息队列的消息监控所述用户的用户行为；

根据所述用户的所述用户行为,推断包括至少一个信任规则标准和信任类别的至少一个推断的信任规则;以及

将所述推断的信任规则添加到所述信任规则集合。

7. 如权利要求1所述的方法：

至少一个信任规则包括可疑消息类别；

所述消息队列包括所述可疑消息类别中的至少一个可疑消息;以及

所述指令被配置为:在所述用户未能与呈现在所述消息队列列表中的可疑消息进行交互时,从所述消息队列去除所述可疑消息。

8. 如权利要求1所述的方法,从视觉样式集合中选择出至少一个视觉样式,所述视觉样式集合包括：

字体；
字体粗细；
字体大小；
颜色；
图标；以及
布局。

9. 如权利要求 1 所述的方法，所述指令被配置为：在从所述用户接收到针对信任类别的所选视觉样式时，将所选视觉样式应用到所述消息队列列表中所述信任类别的消息。

10. 如权利要求 1 所述的方法：

所述信任类别集合的信任类别代表信任梯度；以及
所述信任类别集合的相应信任类别具有指示所述信任类别在所述信任梯度中的位置的视觉样式。

11. 如权利要求 1 所述的方法，所述指令被配置为：在从所述用户接收信任类别的信任子类别时，

为所述信任子类别选择视觉样式，以及
将所述信任子类别添加到所述信任类别集合。

12. 如权利要求 1 所述的方法，为所述信任子类别选择视觉样式包括：为所述信任子类别选择所述信任类别的视觉样式中的视觉子样式。

13. 如权利要求 1 所述的方法：

所述消息队列列表具有排序顺序；以及

呈现所述消息队列列表，包括：

对于相应的消息，根据所述排序顺序识别所述消息队列中消息的位置；以及
根据所述消息的位置对所述消息队列列表进行排序。

14. 如权利要求 13 所述的方法：

至少一个信任类别包括可疑消息类别；

所述消息队列包括所述可疑消息类别中的至少一个可疑消息；以及

所述指令被配置为：

在所述用户未能与呈现在所述消息队列列表中的可疑消息进行交互时，定期地降低所述可疑消息的位置；以及

在所述可疑消息的位置降低到去除位置时，从所述消息队列中去除所述可疑消息。

15. 一种被配置为将包括至少一个消息(12)的消息队列(16)呈现给具有显示器(66)的设备(62)的用户(14)的系统(68)，所述系统(68)包括：

消息存储部分(70)，其被配置为存储所述消息队列(16)的所述消息(12)；

消息信任类别识别组件(72)，其被配置为针对相应的消息(12)，识别从信任类别集合中选择出的信任类别(32)；以及

消息队列呈现组件(74)，其被配置为：在接收到来自所述用户(14)的呈现所述消息队列(16)的请求时，

生成消息队列列表(24)，对于相应的信任类别(32)，其包括利用视觉样式呈现的所述信任类别(32)的消息(12)，所述视觉样式将该信任类别(32)的消息(12)与所述信任类别

集合的其他信任类别(32)的消息(12)区别开来；以及
将所述消息队列列表(24)呈现在所述设备(62)的所述显示器(66)上。

用于消息的信任类别的视觉样式

背景技术

[0001] 在计算领域中,很多场景涉及消息队列中的消息(例如邮件客户端中呈现的电子邮件消息的集合、网络论坛中发送给用户的私有消息的集合、或者聊天环境中各种其他用户接收到的聊天消息的集合)的呈现。在这样的场景中,一些消息可能会呈现不期望的内容,例如大量非请求的消息(“垃圾邮件”);违法、虚假或只是与用户不相关的商品或服务的广告;有异议的素材;恶意内容,例如对于恶意编写的软件的附接或链接;以及冒充受信任的个人以便利用用户的信任的“钓鱼”尝试。

[0002] 可以利用各种技术来评估消息以便识别这些消息是期望的还是不期望的,例如消息的发送者的验证、消息的内容的语义评估、恶意内容的消息中包括的任意链接或软件的评估。识别为不想要的消息会被自动删除、划分(例如,将这样的消息移到“垃圾邮件”文件夹)或者被过滤到消息队列以外。这样的过滤技术被仔细地构想以减少真实的消息被不正确地识别为不想要的消息并被过滤到消息队列以外的误报的发生率,从而导致丢失了用户可能原先期望在消息队列中包括的消息。

发明内容

[0003] 提供此发明内容来以简要形式介绍以下在具体实施方式中进一步描述的概念的选择。此发明内容不旨在识别所要求保护主题的关键因素或必要特征,也不旨在用以限制所要求保护主题的范围。

[0004] 随着不想要的消息的越发盛行(例如,附着或链接到恶意编写的软件的消息和“垃圾邮件”的激增),用以识别并滤除不想要消息的消息的评估相比于未经过滤的消息队列呈现出显著优势。然而,虽然这样的识别技术的准确性持续提高,考虑到用户可能期望接收的消息中可以包括各种内容并且误报的结果可能代表着对于用户的明显损害,无差错过滤技术的开发是不可能的。

[0005] 将消息呈现给用户还是从消息队列中排除消息的决定代表了此评估技术中的粗粒度,尤其对于难以高置信度地取得确定的临界消息。然而,可能期望包括这些消息的中间过滤选项,从而消息以消息队列的方式呈现给用户,但是相对于其他消息是去强调的。相反,对于识别为用户想要的消息(并且尤其是对于用户具有可验证的期望度和 / 或高优先级的消息),可能期望的是,在将消息队列呈现给用户时,相对于其他消息强调这些消息。

[0006] 鉴于这些考虑,在此呈现的技术涉及将包括待递送给用户的消息集合的消息队列呈现给用户。根据这些技术,可以定义信任类别集合,包括代表用户希望接收消息的置信度的信任类别集合。例如,信任类别集合可以包括受信任消息类别、可疑消息类别和不受信任消息类别,其中,受信任消息类别代表具有用户对于期望性的高置信度的消息(例如,从包括在用户的地址簿中的发送者接收的消息、从用户已与其开展业务的经验证的零售商接收的消息、或包括用户很感兴趣的关键词的消息);可疑消息类别代表可能是用户不想要的消息(例如,看起来是对于产品或服务或诈骗的大量非请求要约的消息);不受信任消息类别代表用户可能希望或可能不希望接收的消息。可以评估并用这些信任类别中的一个来标识

消息队列的消息。此外,可以为每个信任类别选择视觉样式,其在视觉上将信任类别的消息与消息队列中的其他消息相区别,并且可以利用根据相关联的信任类别的视觉样式呈现的相应消息来将消息队列呈现给用户。例如,可以用更大或更重粗细的字体或吸引注意的字体颜色或阴影来在视觉上强调受信任消息类别中标识的消息,同时可以用更小或更细的字体或用排斥注意的字体颜色或阴影来在视觉上去强调可疑消息类别中标识的消息。以这种方式,消息的视觉样式可以允许用户以快速并容易理解的方式对消息队列的消息进行分类。

[0007] 这样的呈现是有益的,这是因为消息队列可包括具有宽范围信任级别的消息(包括可能但不一定不想要的可疑消息),从而减少不正确地排除期望的消息的发生率,同时还使得用户能够以快速并易于理解的方式对消息队列的消息进行分类。此外,有区别的视觉样式的使用可以与其他技术相结合,包括从消息队列中排除一定不想要的消息(例如,一定不想要的消息被自动移动到“垃圾邮件”文件夹,但是,可能但并非一定不想要的消息包括在消息队列中,但在视觉上以去强调的方式呈现)以便将更细、更复杂的粒度提供给消息队列的过滤。

[0008] 为了实现之前的和相关的目的,以下描述和附图阐述了特定的说明性方面和实施方案。这些包含可以采用一个或多个方面的各种方式,然而是各种方式中的少许。当结合附图考虑时,本公开的其他方面、优点和新颖的特征将根据以下的详细描述而变得明显。

附图说明

- [0009] 图 1 是以将消息队列呈现给用户为特征的示例性场景的说明。
- [0010] 图 2 是以根据在此呈现的技术将消息队列呈现给用户为特征的示例性场景的说明。
- [0011] 图 3 是说明将消息队列呈现给用户的示例性方法的流程图。
- [0012] 图 4 是说明用于将消息队列呈现给用户的示例性系统的组件框图。
- [0013] 图 5 是包括被配置为体体现此阐述一个或多个供给部分(provision)的处理器可执行指令的示例性计算机可读介质的说明。
- [0014] 图 6 是以信任规则集合到消息队列的消息的应用为特征的示例性场景的说明。
- [0015] 图 7 是以将视觉子样式应用到相应的信任类别的信任子类别为特征的示例性场景的说明。
- [0016] 图 8 是以从消息队列中自动去除可疑消息为特征的示例性场景的说明。
- [0017] 图 9 说明可以实现在此阐述的一个或多个供给部分的示例性计算环境。

具体实施方式

[0018] 现参照附图描述要求保护的主题,在附图中,相同的附图标记始终用来指代相同的要素。在以下描述中,为了解释起见,阐述了众多具体细节以便提供对要求保护主题的彻底理解。然而,可能明显的是,可以在没有这些具体细节的情况下实施所要求保护的主题。在其他实例中,以框图形式示出结构和设备以便于方便描述所要求保护的主题。

[0019] 在计算领域中,许多场景涉及将消息队列中的消息呈现给用户。作为第一示例,用户可以接收与用户的电子邮件地址相关联的邮箱中的电子邮件消息,并且可以通过电子邮

件客户端或网络浏览器来请求邮箱的呈现。作为第二示例，用户可以在网络论坛或其他讨论场景中接收公开或私有消息，并且可以希望查看针对于该用户的所有消息的集合。作为第三示例，用户可以具有诸如即时消息传递客户端或因特网中继聊天(IRC)室的聊天环境中的身份，并且可以从其他用户接收并请求查看聊天消息的集合。

[0020] 在这些场景中，发送给用户的一些消息可能是不想要的。作为第一示例，经常大容量地生成和发送涉及产品和服务的要约的大量非请求的电子邮件消息(“垃圾邮件”电子邮件消息)，这对电子邮件服务的用户和管理员都提出了重要的挑战。作为第二示例，一些消息可以为非法的商品或服务(例如，处方药物或假冒商品)、虚假的商品或服务(例如，没有像所广告的那样起作用的产品)或只是与用户不相关的商品或服务呈现广告。作为第三示例，一些消息可以呈现有异议的素材，诸如包括在呈现给年轻用户的电子邮件消息中的成人内容。作为第四示例，一些消息可附于或链接到可能损害用户操作的设备的恶意编写的软件之类的恶意内容。作为第五示例，一些消息可能试图冒充受信任的发送者，例如该用户认识的个人或者由该用户资助的金融或学术机构，以便利用用户的信任并提取敏感的信息，例如受保护账户的密码和银行账户信息。

[0021] 于是，已经设想了很多技术来评估消息的内容以便区分不想要的消息和期望的消息。作为第一示例，已经设想了很多垃圾邮件过滤技术，其评估消息的内容以便识别频繁使用的内容的语义模式(例如，经常在大量非请求的电子邮件消息中使用的关键词，如流行处方药的名称)，以便确定用户可能认为特定消息是期望的还是不想要的。作为第二示例，可以利用各种形式的白名单(其标识受信任的和可验证的发送者)和 / 或黑名单(其标识不想要消息的信誉不好的发送者)以根据发送者的身份区分消息。作为第三示例，可以利用很多认证技术来确定声称由已知的发送者(例如，众所周知的金融机构)发送的特定消息是由此真实地发出还是已被假冒者伪造。作为第四示例，很多安全软件套件被配置为检查与消息相关联的内容，例如可以在线检索的对象的附件和超级链接，以便识别并隔离引用危险内容的消息。作为第五示例，内容控制技术可以识别在各种消息中呈现的成人内容(例如，基于淫秽或建议性的词语)，并可以审查对于个人而言不适当的消息。这些技术的很多复杂特征可能是可用的(例如，根据用户行为的推断过滤规则、开发并应用代表个人的兴趣和可预见行为的启发法的自适应算法)。

[0022] 可以将这些和其他评估技术应用到消息队列以便根据其中的内容对消息进行划分。例如，当用户操作的设备接收消息时，在该设备上执行的自动处理可以应用这些技术以确定消息是期望的还是不想要的，并且可以从消息队列中排除不想要的消息(例如，通过删除消息、将消息移动到垃圾邮件消息的集合、或隔离消息以便阻断对于恶意内容的访问)。看起来并非是不想要的消息可以例如作为消息队列列表呈现给用户，所述消息队列列表包括用于相应消息的行的集合和标识消息的相应属性(例如，消息发送者的名称、消息发送的日期和消息的标题)的列的集合。在一些场景中，可以允许用户检查分离分区(例如，分离“垃圾邮件”文件夹)中的排除消息，并可以挽救已被不正确地标识为不想要的消息。

[0023] 图1呈现以将包括消息队列的消息12的集合呈现给用户28为特征的示例性场景10的说明。在此示例性场景10中，用户28操作具有显示器20和消息队列16的设备22，该消息队列16被配置为存储由各个发送者14发送的消息12的集合。受用户28的请求，设备22可以在显示器20上呈现消息队列列表24，其包括消息12及其属性(例如，消息12

的发送者、标题和接收时间)。此外,在此示例性场景 10 中,利用各种评估技术来区分期望的消息 12 和不想要的消息 12,并且该后者消息 12 可以被自动过滤到不同的文件夹 18,例如:第一文件夹 18,其代表用户 28 可能希望查看的消息 12 的收件箱;第二文件夹 18,其包括被识别为不想要的消息 12。用户 28 可以请求设备 22 为所选择的文件夹 18 显示消息队列列表 24,并且设备 22 可以在显示器 20 上呈现包括所选文件夹 18 中的消息 12 的消息队列列表 24。此外,用户 28 可以请求为特定类别的邮件(例如,从在用户 28 的地址簿中具有条目的个人接收到的邮件)创建新文件夹 18;可以配置设备 22 将待递送的特定消息 12 插入到特定文件夹 18 中;以及可以人工地将特定消息 12 从第一文件夹 18 移动到第二文件夹 18。设备可以通过满足这些请求来响应,从而使得用户 28 能够以期望的方式管理消息队列 16。

[0024] 虽然图 1 的示例性场景 10 呈现出一些优点,但是一些缺点也可能会源自这些技术到消息队列 16 的消息 12 的应用。作为第一示例,不可能是用户 28 期望的但并非一定不想要的临界消息(borderline message)的过滤可能会给诸如图 1 的示例性场景 10 的过滤技术提出挑战。例如,这些评估技术可能不正确地将消息 12 标识为不想要的,例如:包含冒犯某些个人但没有冒犯用户 28 的语言的消息 12、包含用户 28 已经请求或希望购买的产品或服务的要约的消息 12、来自真实地引用流行处方药物的名称的用户 28 的医疗提供商的消息 12。这些消息 12 从消息队列 16 中的排除可能给用户 28 带来明显的不利,并且尽管语义评估技术已经随着正在进行的开发而变得稳步地更加复杂,但是这些技术不可能实现无差错的评估。相反,传统的过滤方法可能将不一定不想要的任意消息 12 递送到用户 28 的消息队列 16,但是因为这样的消息 18 以与真实消息 12 等同的方式予以呈现,因此用户 28 可能不能够区分消息 12 并可能暴露至不想要的消息 12。作为第二示例,被该技术识别为用户 28 一定期望的消息 12(例如,从在用户 28 的地址簿中识别出的经验证的发送者 14 发送的消息 12、包含用户 28 很感兴趣的关键词的消息 12)以与用户具有较少或不确定兴趣的不受信任消息 12 相似的方式予以呈现。虽然用户 28 可以建立用以对这些消息 12 进行分类的规则(例如,指示要将由用户 28 之前已经把消息 12 发送到的发送者 14 所发送的所有消息 12 移到“受信任邮件”文件夹 18 的规则),但是用户在形成这些规则时的参与以及这种消息 12 在单独文件夹 18 的单独消息队列列表 24 中的呈现可能不期望地涉及用户 28 的注意和/或交互。

[0025] 可以观察到的是,在图 1 的示例性场景 10 中利用的技术中,将消息 12 呈现给用户 28 还是从消息队列 16 中排除消息 12 的决定代表相对粗粒度(coarse — granularity)的决定,并且该粒度的粗度可能尤其与临界期望度的消息相关,其中该临界期望度的消息或者是完全授权的真实状态并且以与中度甚至高度期望的消息 12 等同的方式予以呈现,或者完全从消息队列 16 中排除。可以通过提供没有完全从消息队列 16 排除临界消息 12 而是降低临界消息 12 相对于其他消息 12 的可见性的中间选项来改进这些选项的粗粒度。例如,边界消息 12 可以相对于其他消息 12 在视觉上去强调的方式(例如,更小或更细的字体;不引起注意力的字体、字体颜色或阴影;或者消息队列列表 24 中更小的条目)予以呈现。相反,用户 28 可能很感兴趣的消息 12(例如,来自用户 28 的家庭成员和亲密关系的消息 12)可以相对于其他消息 12 在视觉上强调的方式(例如,更大或更粗的字体;吸引注意力的字体、字体颜色或阴影;或者消息队列列表 24 中的更大条目)予以呈现。以这样的方

式,消息队列列表 24 中的消息 12 可以在视觉上区别于其他消息 12,并且用户 28 可以轻易地根据与之关联的信任类别 32 来识别和分类消息 12。例如,在消息队列 16 中利用消息 12 的有区别的视觉样式,用户 28 可以选择仅关注受信任的消息 12,或者可以在视觉上扫描消息队列列表 24 以识别已经不经意地识别为可疑的消息 12。这些技术还可以和用于过滤消息队列 16 的其他技术(例如,可以将一定不想要的消息 12 自动地过滤到消息队列 16 以外并且过滤到“垃圾邮件”文件夹,同时,仅仅可疑的消息 12 可以保持在消息队列 16 中,但是可以在视觉上去强调的方式呈现在消息队列列表 24 中)进行组合。

[0026] 在此呈现的技术使得能够以可以减少用于将消息队列 16 呈现给用户 28 的其他技术的这些和其他缺点的方式把消息队列 16 呈现给用户 28。根据在此呈现的技术,消息队列 16 中的消息 12 可以标识为属于信任类别集合中的若干信任分类 32 中的一个。例如,信任类别集合可以包括受信任消息类别、可疑消息类别和不受信任消息类别,其中,受信任消息类别包括有可能受用户 28 信任的消息 12,例如从用户 28 的地址簿中识别出的发送者 14 发送的消息 12、从用户 28 之前已经联系的发送者 14 发送的消息 12、或者包括用户感兴趣的一个或多个关键词的消息 12;可疑消息类别包括用户 28 可能不想要的消息 12,例如包括经常在大量非请求消息中使用的关键词(例如,流行药物的名称)但是可能真实地应对这种主题的消息 12、包括对于某些用户 28 可能有争议但是可能对该用户 28 没有争议的内容的消息 12;不受信任消息类别包括既不受信任也不可疑的消息队列 16 的消息 12(例如,由未知或未识别的发送者 14 发送的明显无害的消息)。此外,可以为每个信任类别 32 的消息 12 选择视觉样式;例如,可以为受信任消息类别选择相对大的、粗体的和亮色的视觉样式,并且可以为可疑消息选择相对小的、细体的和中性着色的视觉样式;并且可以为不受信任消息选择中间的视觉样式。当接收请求以将消息队列 16 呈现给用户 28 时,消息队列列表 24 可以被生成并呈现给用户 28,其中每个消息 12 根据消息 12 的信任类别 32 的有区分视觉样式来呈现。以此方式,消息队列列表 24 的视觉呈现可以便于用户查看消息队列 16 并根据其信任类别 32 分类对于相应消息 12 的注意力。

[0027] 图 2 呈现以应用在此呈现的技术以便将消息队列 16 呈现给设备 22 的用户 28 为特征的示例性场景 30 的说明。在该示例性场景 30 中,消息 12 从各个发送者 14 发送到用户 28 的消息队列 16,并根据各种技术(例如,验证发送者 14 的身份、语义评估消息 12 的内容、扫描附着和 / 或链接的资源、和 / 或应用规则)被评估,以便识别消息 12 的期望或不想要的性质。根据在此呈现的技术,可以为每个消息 12 标识信任类别 32 以指示评估技术的结果。当用户 28 请求消息队列 16 的呈现时,这些技术的实施可以生成标识消息队列 16 中的消息 12 的消息队列列表 24 并呈现给用户 28(例如,以便要再现(render)在用户 28 的设备 22 的显示器 20 上)。此外,对于呈现在消息队列列表 24 中的相应消息 12,与消息 12 的信任类别 32 相关联的视觉样式 34 可以应用到消息队列列表 24 中消息 12 的条目。例如,应用到受信任消息类别的消息 12 的第一视觉样式 34 包括用于消息队列列表 14 中的消息 12 的大字体、加粗的边框和更高的条目;应用到可疑消息类别的消息的第二视觉样式 38 可以包括消息队列列表 24 中的小字体和短的并且可能是模糊的条目;并且第三视觉样式 38 可以应用到不受信任消息类别的消息,该样式可以包括在消息队列列表 24 中字体和条目的选择中的中性外观,其既不吸引也不排斥用户 28 的注意。以这样的方式,在将消息队列列表 24 呈现给用户 28 时使用视觉样式 34 可以便于用户根据在此呈现的技术在视觉上对

消息队列 16 的内容进行分类。

[0028] 图 3 呈现这些技术的第一实施方式,其被示出为将消息 12 的消息队列 16 呈现给用户 28 的示例性方法 40。该示例性方法可以例如实现为存储在设备的存储器组件(例如,存储器电路、硬盘驱动器的底板、固态存储设备、或者磁或光盘)中的指令,该指令在设备的处理器上运行时使得设备应用在此呈现的技术。示例性方法 40 开始于 42,并包括在设备的处理器上执行 44 指令。具体地,该指令包括对于消息队列 16 中的相应消息 12 从信任类别集合识别 46 消息 12 的信任类别 32。指令还被配置为:在从用户 28 接收呈现消息队列 16 的请求时,呈现 48 消息队列列表 24,其中对于相应信任类别 32,该消息队列列表 24 包括以视觉样式 34 呈现的信任类别 32 的消息 12,所述视觉样式 34 将信任类别 32 的消息 12 和信任类别集合的其他信任类别 32 的消息 12 区分开来。以这样的方式,示例性方法 40 根据在此呈现的技术实现消息队列 16 的呈现,并因此在 50 处结束。

[0029] 图 4 呈现了这些技术的第二实施方式,其被示出为以配置成将消息队列 16 的消息 12 呈现给用户 28 的示例性系统 68 为特征的示例性场景 60。示例性系统 68 可以在具有处理器 64 和显示器 66 的设备 62 中操作,并且可以例如实现为互操作来利用设备 62 的资源以便将消息队列 16 呈现给用户 28 的组件集合。示例性系统 68 例如可以实现为软件架构,其包括组件集合,该组件集合分别包括存储在设备的存储器组件(例如,存储器电路、硬盘驱动器的底板、固态存储设备、或磁或光盘)中的指令,该指令在设备的处理器上运行时执行各种任务和 / 或与其他组件进行互操作以便应用在此呈现的技术。示例性系统 68 包括消息存储部分 70,其被配置为存储消息队列 16 的消息 12。示例性系统 68 还包括消息信任类别识别组件 72,其被配置为针对相应的消息 12 识别从信任类别集合中选择出的信任类别 32。示例性系统 68 还包括消息队列呈现组件 74,其被配置为在接收来自用户 28 的呈现消息队列 16 的请求时生成消息队列列表 24,该消息队列列表 24 对于相应的信任类别 32 包括以视觉样式 34 呈现的信任类别 32 的消息 12,该视觉样式 34 区别信任类别 32 的消息 12 和其他信任类别 34 的消息 12,并且消息队列呈现组件 74 被配置为将消息队列列表 24 在设备 22 的显示器 20 上呈现给用户 28。以这样的方式,示例性系统 68 的组件相互操作以使得设备 62 根据在此呈现的技术呈现消息队列 16。

[0030] 又一实施方式涉及计算机可读介质,其包括被配置为应用在此呈现的技术的处理器可执行指令。这样的计算机可读介质例如可以包括计算机可读存储介质,其包括诸如存储器半导体(如,利用静态随机存取存储器(SRAM)、动态随机存取存储器(DRAM)和 / 或同步动态随机存取存储器(SDRAM)技术的半导体)之类的有形器件、硬盘驱动器的底板、闪存器件、或磁或光盘(如 CD-R、DVD-R 或软盘),该计算机可读存储介质对计算机可读指令的集合进行编码,该计算机可读指令在由设备的处理器执行时使得设备实现在此呈现的技术。这样的计算机可读介质可以还包括(作为区别于计算机可读存储介质的技术的一分类)各种类型的通信介质,例如这样的信号:该信号可以通过各种物理现象传播(例如,电磁信号、声波信号或光学信号)并且可以在各种有线场景(例如,经由以太网或光纤线缆)和 / 或无线场景(例如,诸如 WiFi 的无线局域网(WLAN)、诸如蓝牙的个人区域网(PAN)、或者蜂窝或无线电网络)中传播,并且其对计算机可读指令进行编码,所述计算机可读指令在由设备的处理器来执行时使得设备实现在此呈现的技术。

[0031] 图 5 中示出了以这些方式设想的示例性计算机可读介质,其中实施方案 80 包括编

码有计算机可读数据 84 的计算机可读介质 82 (例如, CD-R、DVD-R 或硬盘驱动器的底板)。这样的计算机可读数据 84 进而包括计算机指令 86 的集合, 其配置为根据在此阐述的原理进行工作。在一个这样的实施方式中, 处理器可执行指令 86 可以被配置为执行将消息队列呈现给用户的方法, 例如图 3 的示例性方法 40。在另一这样的实施方式中, 处理器可执行指令 86 可以被配置为实现用于将消息队列呈现给用户的系统, 例如图 4 的示例性系统 68。这样的计算机可读介质的一些实施方式可以包括被配置为存储以此方式配置的处理器可执行指令的非瞬时性计算机可读存储介质(例如, 硬盘驱动器、光盘或闪存器件)。本领域技术人员可以设想出被配置为根据在此呈现的技术进行工作的很多这样的计算机可读介质。

[0032] 可以在很多方面有变型地设想在此讨论的技术, 并且一些变型可以相对于这些和其他技术的其他变型呈现另外的优点和 / 或减少的缺点。此外, 可以组合地实现一些变型, 并且一些组合可以通过协同合作而以另外的优点和 / 或减少的缺点为特色。变型可以并入到各种实施方式(例如, 图 3 的示例性方法 40 和图 4 的示例性系统 68) 以对这些实施方式给予单个和 / 或协同的优点。

[0033] 在这些技术的实施方式之中可以改变的第一方面涉及可利用这些技术的场景。作为第一示例, 这些技术可用以呈现各种类型的消息队列 16 和消息 12(其包括存储在电子邮件邮箱中的电子邮件消息; 网络论坛中引导至用户 28 的公开和 / 或私有消息 12; 聊天环境中由其他用户 28 引导至用户 28 的聊天消息 12)。作为第二示例, 这些技术可以在用户 28 操作的设备 22 上实现, 例如在用户 28 的计算机上执行的电子邮件客户端中, 其将消息队列 16 呈现在连接到设备 22 的显示器 20 上, 和 / 或在提供针对由用户 28 操作的设备 22 的服务的设备 22 上实现, 例如电子邮件服务, 该电子邮件服务再现并发送网页至用户 28 的设备 22 以便在设备 22 的显示器 20 上的浏览器内再现。本领域技术人员可以设想可利用在此呈现的技术的很多场景。

[0034] 可以在这些技术的实施方式中变化的第二方面涉及识别消息队列 16 的相应消息 12 的信任类别 32 的方式。作为第一示例, 这些技术的实施方式可以在接收消息 12 时识别信任类别 32; 可以定期地检查消息队列 16 以识别消息 12 的信任类别 32; 和 / 或可以在准备消息队列列表 24 的呈现时执行信任类别 32 的“恰好及时”的识别。另外, 消息 12 的信任类别 32 的识别可以被存储(例如, 在作为相应消息 12 的元数据的消息队列 16 中), 在后续更新涉及识别信任类别 32 的逻辑的情况下可选地具有重新检查, 和 / 或消息 12 的信任类别 32 的识别可以对包括在消息队列列表 24 的呈现中的每个消息 12 进行重新识别。

[0035] 作为该第二方面的第二示例, 这些技术的实施方式可以利用包括其组合的很多评估技术来识别相应消息 12 的信任类别 32。作为第一变型, 一实施方式可以通过应用一个或多个信任启发法来识别消息 12 的信任类别 32。这些信任启发法可以从信任启发法集合中选择出, 所述信任启发法集合包括消息发送者信任启发法(例如, 自动将源自特定发送者 14 的消息 12 与特定信任类别 32 相关联); 消息接收者信任启发法(例如, 自动将寄往特定接收者的消息 12 (例如, 发送到很多接收者的大量消息相对于仅向用户 28 发送的消息) 与特定的信任类别 32 相关联); 消息递送信道信任启发法(例如, 自动将从已知为可靠和 / 或不可靠的电子邮件服务器发送的消息 12 与特定信任类别 32 相关联); 以及消息内容信任启发法(例如, 自动将包括表明更高级别的信任和 / 或怀疑的特定关键词的消息 12 与特定的信任类别 32 相关联)。可以以静态的方式和 / 或以自适应的方式设想这些技术, 例如, 自适应地

改善用以识别消息 12 的信任类别 32 的逻辑的神经网络或遗传算法之类的学习算法。

[0036] 作为该第二方面的该第二示例的第二变型,相应消息 12 的信任类别 32 的识别可以包括信任规则集合,所述信任规则集合包括指定这种识别的逻辑的一个或多个信任规则。例如,每个信任规则可以指定一个或多个信任规则标准(例如,应用到要根据信任规则归类的消息 12 的条件布尔值集合)以及为满足信任规则标准的消息 12 识别出的信任类别。这些技术的实施方式可以通过识别具有与消息 12 相匹配的信任规则标准的信任规则并选择信任规则的信任类别 32 来识别消息 12 的信任类别 32。这些信任规则可以从许多源得到。例如,可以通过消息队列 16 的管理员、用户 28 操作的设备 22(例如,安装在设备 22 上的电子邮件客户端)和 / 或提供给设备 22 的服务(例如,设备 22 访问的电子邮件服务)来定义一个或多个信任规则;可以从信任规则源(例如,标识受信任发送者 14 的白名单和 / 或标识可疑发送者 14 的黑名单的提供者)接收一个或多个信任规则。还可以从用户 28 指定定制的信任规则(例如,指定为一个或多个信任规则标准和信任类别)并将其添加到信任规则集合。

[0037] 图 6 呈现以信任规则集合 92 为特征的示例性场景 90 的说明,包括分别具有至少一个信任规则标准 96 和信任类别 98 的信任规则 92 的集合。例如,第一信任规则 94 可以指定信任规则标准 96,其指示消息 12 的发送者 14 标识在用户 28 的地址簿中,并且指示满足该信任规则标准 96 的消息 12 将被分配给受信任的消息类别,而第二信任规则 94 可以指定信任规则标准 96,其指示消息 12 附着可执行文件,并指示满足该信任规则标准 96 的消息 12 将被分配给可疑消息类别。在从发送者 14 接收消息 12 时,这些技术的一实施方式可以将相应的信任规则标准 96 与消息 12 的对应属性进行比较,并且,在识别所有信任规则标准 96 都与消息 12 相匹配的信任规则 94 时,该实施方式可以用信任规则 94 识别出的信任类别 32 来标识消息队列 16 中的消息 12。

[0038] 作为该第二方面的第三示例,这些技术的一实施方式可以监控和评估用户 28 的用户行为以便确定识别相应消息 12 的信任类别 32 的逻辑。作为第一这样的示例,可以通过利用消息队列 16 的消息 12(例如,用户 28 读取的、用户回复的和 / 或用户 28 移动到消息队列 16 中的文件夹 18 的消息 12 的类型)监控各种用户行为以自动地生成一个或多个推断的信任规则并将其添加到信任集合。作为第二这样的示例,用户 28 的不作为和 / 或不注意也可以用作用来识别相应消息 12 的信任类别 32 和 / 或过滤消息 12 的逻辑的指示器。例如,消息队列 16 可以包括标识为属于可疑消息类别的消息 12。消息 12 可以因而根据去强调可疑消息 12 的视觉样式而呈现在消息队列列表 24 中。如果用户 28 随后未能与可疑消息 12 进行交互(例如,如果用户 28 没有在特定时间段内或者响应于消息队列列表 24 中可疑信息 12 的若干呈现来选择读取可疑信息 12),则可以隐含地确认消息 12 的可疑性质,并且可以从消息队列 16 中去除可疑消息 12。本领域普通技术人员可以设想并利用根据在此呈现的技术识别消息 12 的信任类别 32 的很多方式。

[0039] 在这些技术的实施方式中可以变化的第三方面包括多种类型的视觉样式 34,其可以在将消息队列列表 24 呈现给用户 28 时应用到相应信任类别 32 的消息 12。作为第一示例,视觉样式可以包括很多视觉方面,用以在呈现时区分相应信任类别 32 的消息 12。例如,视觉样式集合可以包括每个视觉样式的很多这样的视觉方面,例如有区别的字体、有区别的字体粗细、有区别的字体大小、有区别的字体颜色、消息队列列表 24 中消息 12 的条目的

有区别的阴影颜色或样式、用来描绘消息队列列表 24 中的消息 12 的有区别的图标、消息队列列表 24 中的消息 12 的有区别的边框、和 / 或有区别的布局(例如,消息队列列表 24 中消息 12 的水平或垂直定位)。作为该第三方面的第二示例,用户 28 可以选择所选定的视觉样式来标识并区分特定信任类别 32 的消息 12,并且可以在将消息队列列表 24 呈现给用户 28 时利用所选定的视觉样式。作为该第三方面的第三示例,信任类别集合可以包括受信任的消息类别 32,其具有强调受信任消息类别 32 的消息 12 的视觉样式 34(例如,利用较大的字体、较深的边框、和 / 或更亮或更醒目的字体颜色),和 / 或可疑消息类别 32,其具有去强调可疑消息类别 32 的消息 12 的视觉样式(例如,利用较小的字体、较细或不可见的边框、和 / 或更中性或更不明显的字体颜色)。可替换地,信任类别 32 可以是代表信任梯度的信任类别集合(例如,代表很多信任等级的信任类别的范围)中的,并且相应的信任类别 32 可以具有指示信任梯度中信任类别的位置的视觉样式 34(例如,递增地更加明亮的明亮颜色和 / 或更大的字体,其指示代表递增地更高的信任级别的信任类别 32 中的消息 12 的包含)。

[0040] 作为该第三方面的第四示例,用户 28 可以定制信任类别 32,并且分配给它的视觉样式 34 可以被相应地调节。作为第一这样的示例,用户 28 可以指定信任类别 32 的信任子类别(例如,在具有共享属性的信任类别 32 中识别的消息 12 的子集),并且这些技术的一实施方式可以将信任子类别添加到具有特定视觉样式 34 的信任子类别集合。此外,为信任子类别选择的视觉样式 34 可以包括分配给信任类别 32 的视觉样式 34 的视觉子样式。例如,视觉特性的第一集合可以应用到特定信任类别 32 中所有消息 12 的呈现,但是可以另外应用视觉特性的第二集合来进一步区分信任类别 32 中信任子类别的消息 12 和信任类别 32 的其他消息 12。

[0041] 图 7 呈现了以为相应的信任类别 32 中的相应信任子类别 102 选择视觉子样式为特征的示例性场景 100 的说明。在该示例性场景 100 中,信任类别集合 102 包括 3 个信任类别 32,包括受信任消息类别、不受信任消息类别和可疑消息类别。在每个信任类别 32 中,定义了两个信任子类别 102,其进一步标识分配给它的消息 12 的信任级别;例如,受信任消息类别包括第一信任子类别 102,其用于来自朋友的消息 12;以及第二信任子类别 102,其用于来自用户 28 经常与之进行交易的经验证业务的消息。每个信任类别 32 根据区别的视觉样式 34 来描绘;例如,受信任消息类别的视觉样式 34 包括消息队列列表 24 中更大的字体和更高的条目,同时可疑消息类别的视觉样式 34 包括消息队列列表 24 中较小的字体和较短的条目。此外,每个信任类别 32 中的视觉类别 102 还包括视觉样式的视觉特性,而且包括应用另外视觉特性的视觉子样式。例如,除了根据第一视觉样式的大字体和高条目,还可以利用包括条目的第一区别阴影的第一视觉子样式来呈现第一信任类别 32 的第一信任子类别 102 中的消息 12,同时可以利用包括条目的第二区别阴影的第二视觉子样式来呈现第一信任类别 32 的第二信任子类别 102 的消息 12。以对信任类别 32 的视觉样式 34 的补充方式来应用信任子类别 102 的视觉子样式可以使得用户 28 能够通过对于消息队列列表 24 的粗略视觉检测来识别相应消息 12 的信任类别 32 和信任子类别 102。本领域普通技术人员可以设想很多类型的视觉样式 34 来根据在此呈现的技术区分在消息队列列表 24 的呈现中相应消息 12 的信任类别 32。

[0042] 在这些技术的实施方式中可以改变的第四方面涉及消息队列列表 24 的呈现。作为第一示例,消息队列列表可以包括一个或多个消息队列列表视图,其以多种方式来调整

消息队列 24 的呈现,例如仅呈现与特定过滤标准(例如,“仅显示上个星期内发送的消息”和“仅显示具有附件的消息”)相匹配的消息队列 24 的消息 12 的过滤器。当用户 28 选择特定消息队列列表视图时,这些技术的一实施方式可以将所选择的消息队列列表视图应用到消息队列列表 24。作为该第四方面的第二示例,各种类型的分组可以应用到消息队列列表 24 的消息 14;例如消息可以根据信任类别 102 或其他属性(例如发送者、日期、或标题、或附件状态)来进行分组。作为该第四方面的第三示例,消息队列列表 24 可以包括用于将各种类型的消息行为应用到消息队列列表 24 的一个或多个消息 12 的选项(例如,“将所有选择的消息标记为已读”,或者“将所有可疑的消息移动到垃圾邮件文件夹”),并且一实施方式可以在从用户 28 接收到消息行为的选择时,将所选择的消息行为应用到消息队列列表 24 的所选消息 12。

[0043] 作为该第四方面的第四示例,消息队列列表 24 可以用根据特定排序顺序所排序的消息 12 来呈现,例如按发送或接收的日期、发送者 14 的名称、消息 12 的主题或长度、或指示用户 28 以之看待消息 12 的所预测兴趣级别和 / 或紧急性的大致优先级得分,以升序或降序进行排序。例如可以通过根据排序顺序识别相应消息 12 在消息队列 16 中的位置并随后根据消息 12 的位置对消息队列列表 24 进行排序,来取得该排序顺序。还可以利用排序顺序来改进消息队列列表 24 的呈现。作为一个示例,可疑消息 12 根据排序顺序可以初始呈现在特定的位置,但是如果用户 28 没有与可疑消息 12 进行交互,消息队列列表 24 中可疑消息 12 的位置可随着时间而下降,直到从消息队列列表 24 中去除该可疑消息 12 为止。例如,这些技术的一实施方式可以定期地降低可疑消息 12 的位置(例如,使得可疑消息 12 在消息队列列表 24 的连续呈现中看起来递增地降低),并且当可疑消息达到可去除位置(例如,消息队列列表 24 中的最低条目)时,实施方式可以从消息队列 16 去除可疑消息 12。以这样的方式,消息队列 16 可以展现出自清理的特性,以使得可疑消息 12 在初始呈现给用户 12 (从而减少误报的发生率),但是稳步地被去除而不涉及用户 12 的注意或交互。

[0044] 图 8 呈现了以不涉及用户 28 的交互的消息队列列表 24 的增量自清理为特征的示例性场景的说明。在该示例性场景中,呈现了消息队列列表 24,其包括用视觉样式呈现的各种消息 12,该视觉样式区分用各种信任类别 32 标识的消息 12。消息队列列表 24 还应用涉及消息 12 接收的下降日期的排序顺序。在该示例性场景中,并且如在第一时间点 110 处所示,顶部的消息 12 被标识为可疑消息(根据第二视觉样式 38 来描绘,所述第二视觉样式 38 包括小字体、缩小的边框和消息队列列表 24 中短的条目),并且在初始根据其按照排序顺序的位置被排序到消息队列列表 24 中。但是,到第二时间点 112 为止,用户 28 还没有与该可疑消息 12 进行交互,并且可疑消息 12 的位置在消息队列列表 24 中下降,并且可疑消息 12 现在出现在其按照排序顺序的位置的下面。随着用户继续没有与可疑消息 12 进行交互,它在消息队列列表 24 中的位置可以在第三时间点 114 处进一步下降;并且在第四时间点 116 处,可疑消息 12 的位置可能如此远远地降低(例如,在消息队列列表 24 的多页呈现时,不再出现在消息 12 的第一页中)以致可疑消息 12 从消息队列 16 被去除,并且代之放置在用于不想要的消息的文件夹 18 中。以这样的方式,消息队列列表 24 可以呈现自清理特征,其中可疑消息 12 是临时呈现的(从而减少了由于评估技术的误报而导致的消息 12 的去除),但是可以从消息队列 16 中去除而没有用户 28 的介入。本领域普通技术人员可以设想根据在此呈现的技术呈现消息队列列表 24 的很多方式。

[0045] 虽然以对于结构特征和 / 或方法学上的行为而言特定的语言描述了本主题,但是要理解的是,所附权利要求中限定的主题不必限于以上所描述的特定特征或行为。而是,将以上所描述的特定特征和行为公开为实现权利要求的示例形式。

[0046] 如在本申请中所使用的,术语“组件”、“模块”、“系统”、“接口”等通常意在指代计算机相关的实体,或者是硬件、硬件和软件的组合、软件、或者是运行中的软件。例如,组件可以但不限于是运行在处理器上的进程、处理器、对象、可执行程序、执行的线程、程序和 / 或计算机。通过说明的方式,运行在控制器上的应用程序和控制器都可以是组件。一个或多个组件可以驻留在执行的进程和 / 或线程中,并且组件可以位于一个计算机上和 / 或分布在两个或更多个计算机之间。

[0047] 此外,要求保护的主题可以实现为这样的方法、装置或制品:其使用标准的编程和 / 或工程技术来生产软件、固件、硬件或其任意组合以控制计算机实现所公开的主题。在此使用的术语“制品”旨在包括从任意计算机可读设备、载体或介质可得到的计算机程序。当然,本领域技术人员将认识到,可以在不脱离所要求保护主题的范围或精神的情况下对该配置进行很多的修改。

[0048] 图 9 和以下讨论提供用以实现此阐述的一个或多个供给部分的实施方式的合适计算环境的简要、一般描述。图 9 的操作环境仅是合适操作环境的一个示例,而不旨在表明对操作环境的使用范围或功能的任何限制。示例计算设备包括但不限于个人计算机、服务器计算机、手持设备或膝上型设备、移动设备(例如移动电话、个人数字助理(PDA)、媒体播放器等)、多处理器系统、消费电子设备、迷你计算机、大型机计算机、包括任意以上系统或设备的分布式计算环境等。

[0049] 虽然没有要求,但是在通过一个或多个计算设备执行“计算机可读指令”的上下文中描述了各实施方式。可以经由计算机可读介质(下面讨论)分布计算机可读指令。计算机可读指令可以实现为执行特定的任务或者实现特定的抽象数据类型的程序模块(如功能、对象、应用编程接口(API)、数据结构等)。通常,计算机可读指令的功能可以在多种环境中根据期望来组合或分布。

[0050] 图 9 示出包括计算设备 122 的系统 120 的示例,该计算设备 122 被配置为实现在此提供的一个或多个实施方式。在一个配置中,计算设备 122 包括至少一个处理单元 126 和存储器 128。根据计算设备的实际配置和类型,存储器 128 可以是易失性的(例如 RAM)、非易失性的(例如 ROM、闪存等)或二者的某种组合。在图 9 中通过虚线 124 示出了该配置。

[0051] 在其他实施方式中,设备 122 可以包括另外的特征和 / 或功能。例如,设备 122 还可以包括另外的存储部分(例如,可拆卸和 / 或不可拆卸),包括但不限于磁存储部分、光学存储部分等。这些另外的存储部分通过存储部分 130 在图 9 中示出。在一个实施方式中,用以实现在此提供的一个或多个实施方式的计算机可读指令可以在存储部分 130 中。存储部分 130 还可以存储其他计算机可读指令来实现操作系统、应用程序等。例如,计算机可读指令可以加载在存储器 128 中以供处理单元 126 执行。

[0052] 在此使用的术语“计算机可读介质”包括计算机存储介质。计算机存储介质包括以用于信息(诸如计算机可读指令或其他数据)存储的任意方法或技术实现的易失性和非易失性、可拆卸和不可拆卸介质。存储器 128 和存储部分 130 是计算机存储介质的示例。计算机存储介质包括但不限于 RAM、ROM、EEPROM、闪存或其他存储器技术、CD-ROM、数字多功能

盘(DVD)或其他光学存储部分、磁盒、磁带、磁盘存储部分或其他磁存储设备、或者可以用来存储期望的信息并可以由设备 122 访问的任意其他介质。任意这样的计算机存储介质都可以是设备 122 的一部分。

[0053] 设备 122 还可以包括允许设备 122 与其他设备进行通信的一个或多个通信连接部分 136。一个或多个通信连接部分 136 可以包括但不限于调制解调器、网络接口卡(NIC)、集成网络接口、射频发射机 / 接收机、红外端口、USB 连接部分、或用于将计算设备 122 连接到其他计算设备的其他接口。一个或多个通信连接部分 136 可以包括有线连接部分或无线连接部分。一个或多个通信连接部分 136 可以发送和 / 或接收通信媒体。

[0054] 术语“计算机可读介质”可以包括通信介质。通信介质通常以“经调制的数据信号”(诸如载波)或者其他传输机制体现计算机可读指令或者其他数据，并且包括任意信息递送介质。术语“经调制的数据信号”可以包括这样的信号：该信号以对该信号中的信息进行编码的方式使得其特征中的一个或多个被设置或改变。

[0055] 设备 122 可以包括一个或多个输入设备 134，例如键盘、鼠标、语音输入设备、触摸输入设备、红外相机、视频输入设备和 / 或任意其他输入设备。一个或多个输出设备 132(如，一个或多个显示器、扬声器、打印机和 / 或任意其他的输出设备)也可以包括在设备 122 中。一个或多个输入设备 134 和一个或多个输出设备 132 可以经由有线连接、无线连接或其任意组合来连接到设备 122。在一个实施方式中，来自另一计算设备的输入设备或输出设备可以用作计算设备 122 的一个或多个输入设备 134 或者一个或多个输出设备 132。

[0056] 计算设备 122 的组件可以通过诸如总线的各种互连来连接。这样的互连可以包括外设组件互连(PCI)，例如 PCI Express、通用串行总线(USB)、FireWire (IEEE 1394)、光学总线结构等。在另一实施方式中，计算设备 122 的组件可以通过网络互连。例如，存储器 128 可以包括位于通过网络互连的不同物理位置的多个物理存储器单元。

[0057] 本领域技术人员将认识到，用来存储计算机可读指令的存储设备可以跨网络分布。例如，可经由网络 138 访问的计算设备 140 可以存储计算机可读指令来实现在此提供的一个或多个实施方式。计算设备 122 可以访问计算设备 140 并下载部分或全部供执行的计算机可读指令。可替换地，计算设备 122 可以根据需要下载多条计算机可读指令，或者一些指令可以在计算设备 122 处执行，而一些指令在计算设备 140 处执行。

[0058] 在此提供了实施方式的各种操作。在一个实施方式中，所描述的操作中的一个或多个可构成存储在一个或多个计算机可读介质上的计算机可读指令，其在由计算设备运行的情况下使得计算设备执行所描述的操作。描述这些操作的一些或全部的顺序不应被理解为暗示这些操作一定是依赖顺序的。得益于此描述的本领域技术人员将会意识到可替换的排序。此外，将会理解的是，不是所有的操作都一定存在于在此提供的每个实施方式中。

[0059] 此外，在此使用词语“示例性”以意味着用作示例、实例或说明。在此作为“示例性”描述的任意方面或设计都不一定被理解为优于其他方面或设计。而是，词语示例性的使用旨在以具体的方式呈现概念。如在本申请中使用的，术语“或者”旨在意味着包含性的“或者”而不是排他的“或者”。即，除非另有指定或者根据上下文是清楚的，否则“X 采用 A 或 B”旨在意味着任意自然的包含性置换。即，如果“X 采用 A”；“X 采用 B”；或者“X 采用 A 和 B 两者”，则在任意前述实例下都满足“X 采用 A 或 B”。另外，本申请和所附权利要求中使用的冠词“一”通常可以理解为意味着“一个或多个”，除非另有指定或者根据上下文清楚地被

指引为单数形式。

[0060] 此外,虽然已经针对一个或多个实施方式示出并描述了本公开,但是本领域技术人员基于对此说明书和所附的附图的阅读和理解将会想到等同的替换和修改。本公开包括所有这些修改和替换,并且仅受限于所附权利要求的范围。尤其对于通过上述组件(例如,元素、资源等)执行的各种功能,除非另外指示,否则用来描述这些组件的术语旨在对应于执行所描述组件的指定功能的任意组件(例如,在功能上等同),即使在结构上与执行在此示出的本公开示例性实施方案中的功能的所公开结构不等同。另外,虽然可能已经仅针对若干实施方案中的一个公开了本公开的特定特征,但是可以将这样的特征与可能对于任何给定或特定的应用所期望和有益的其他实施方案的一个或多个其他特征相组合。此外,就具体实施方式或权利要求书中使用的术语“包含”、“具有”、“含有”、“带有”或其变型而言,以类似于术语“包括”的方式,这些术语旨在是包含性的。

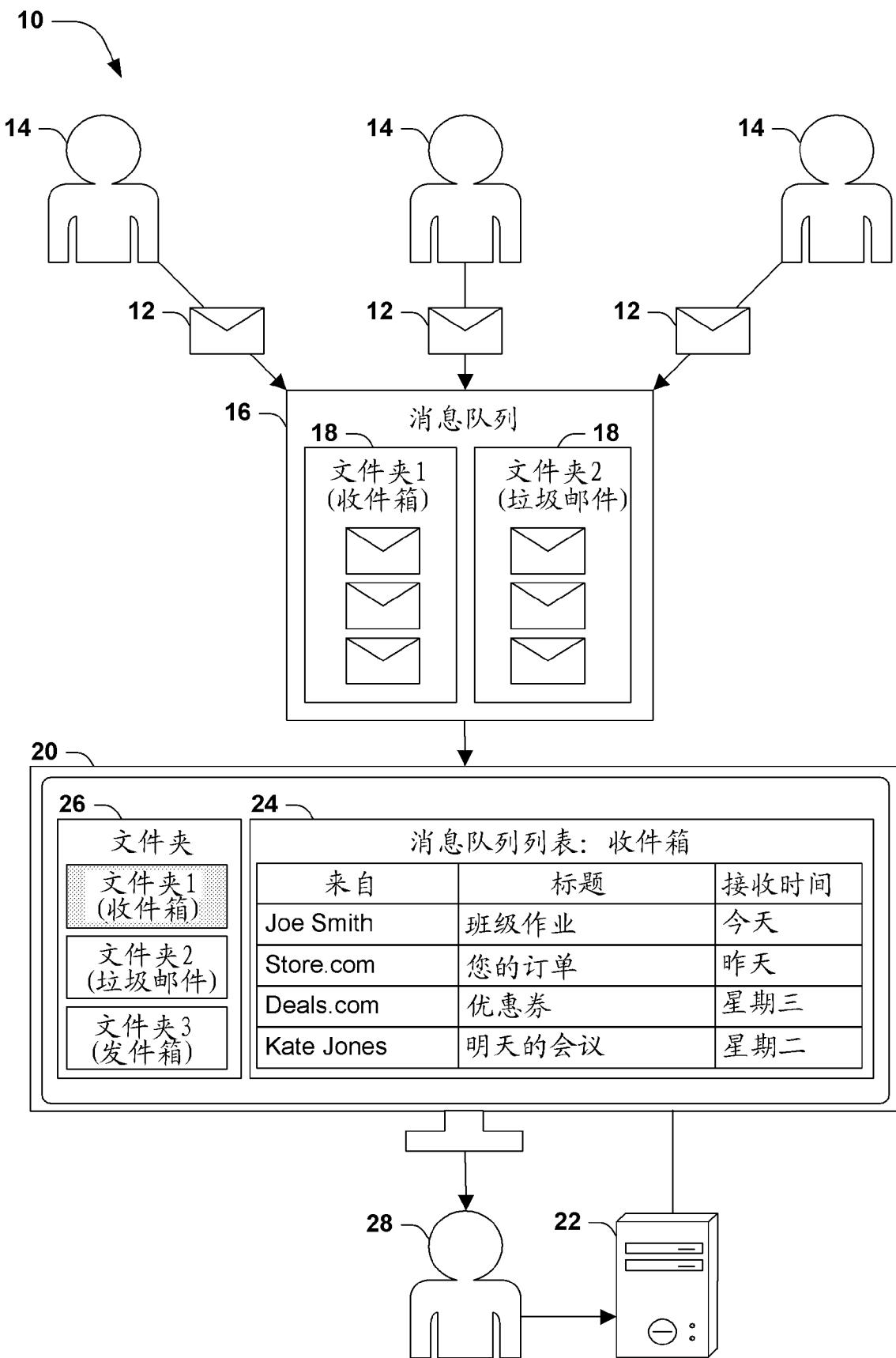


图 1

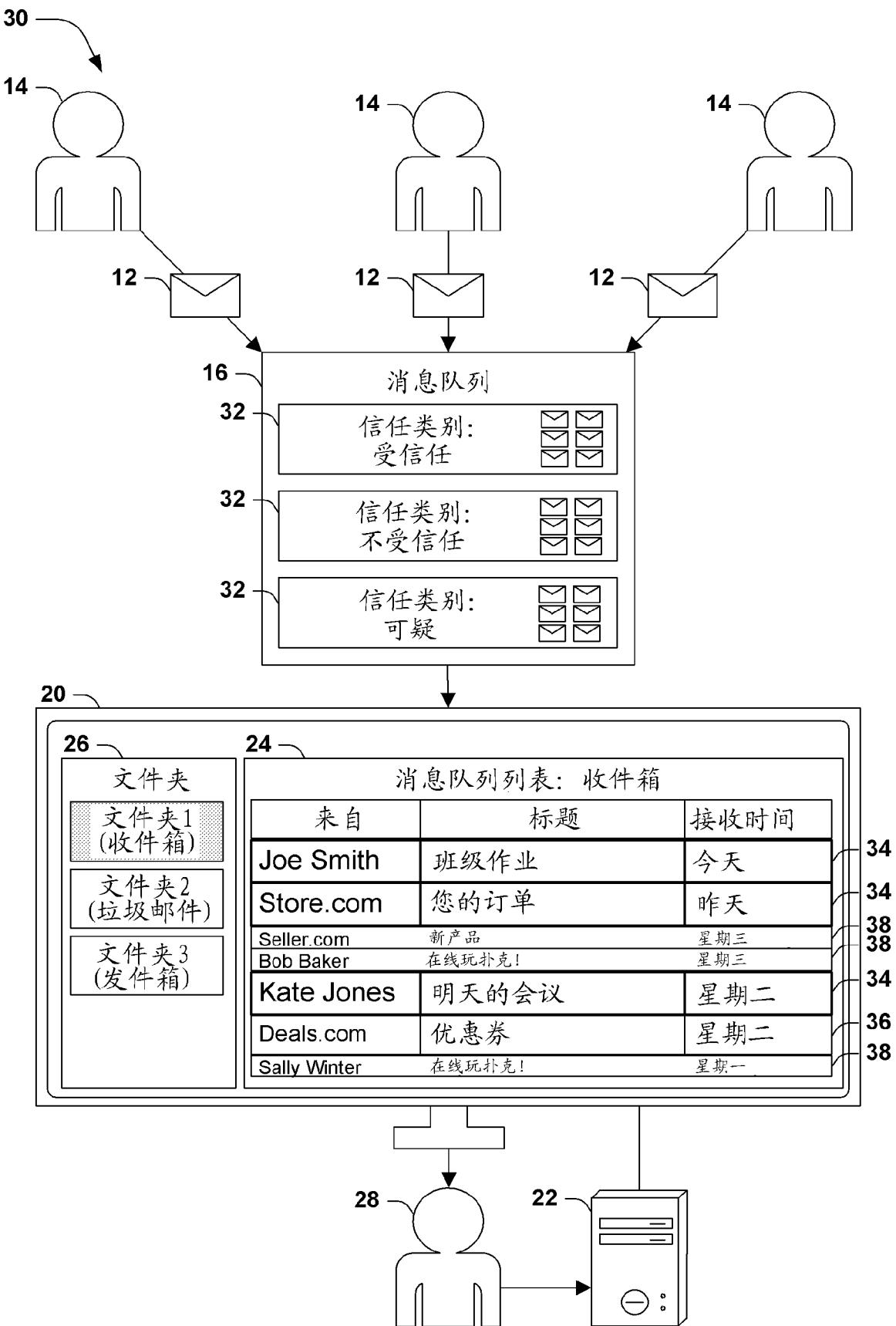


图 2

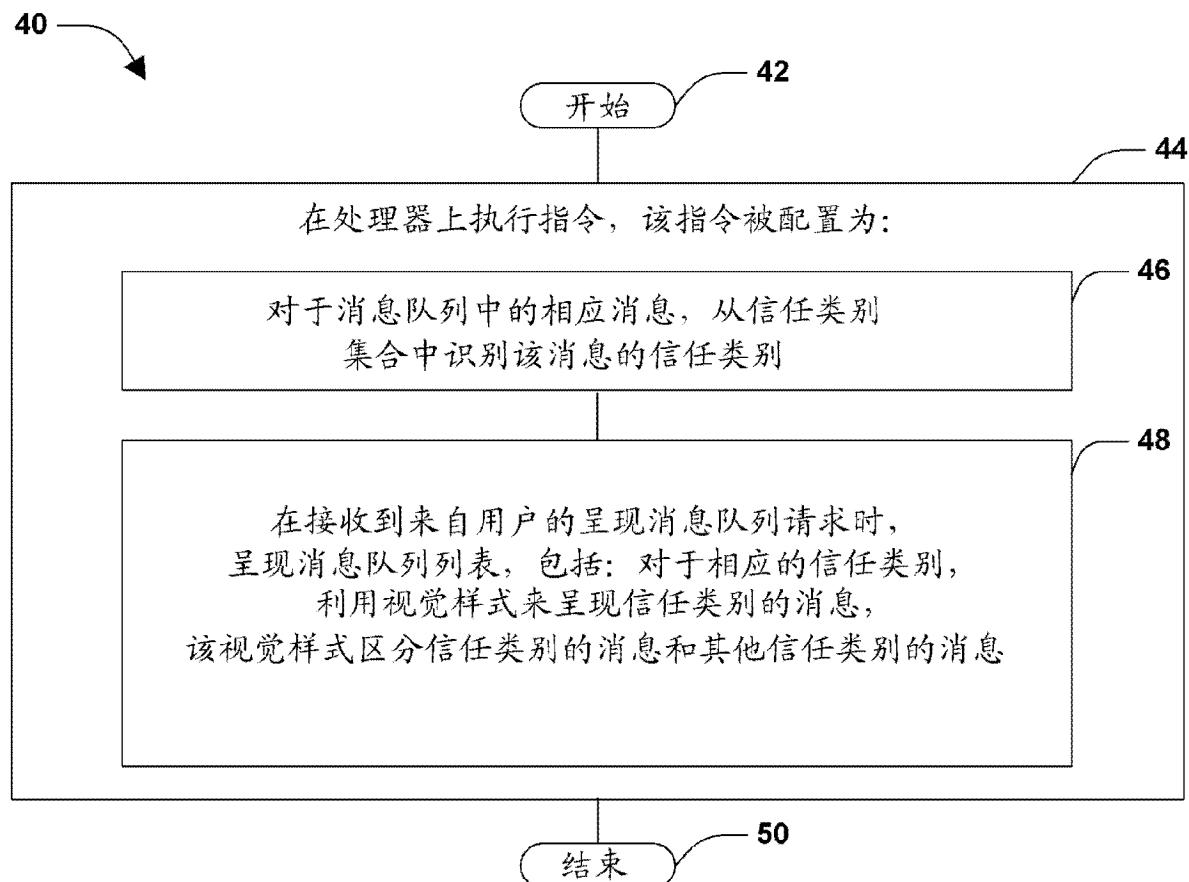


图 3

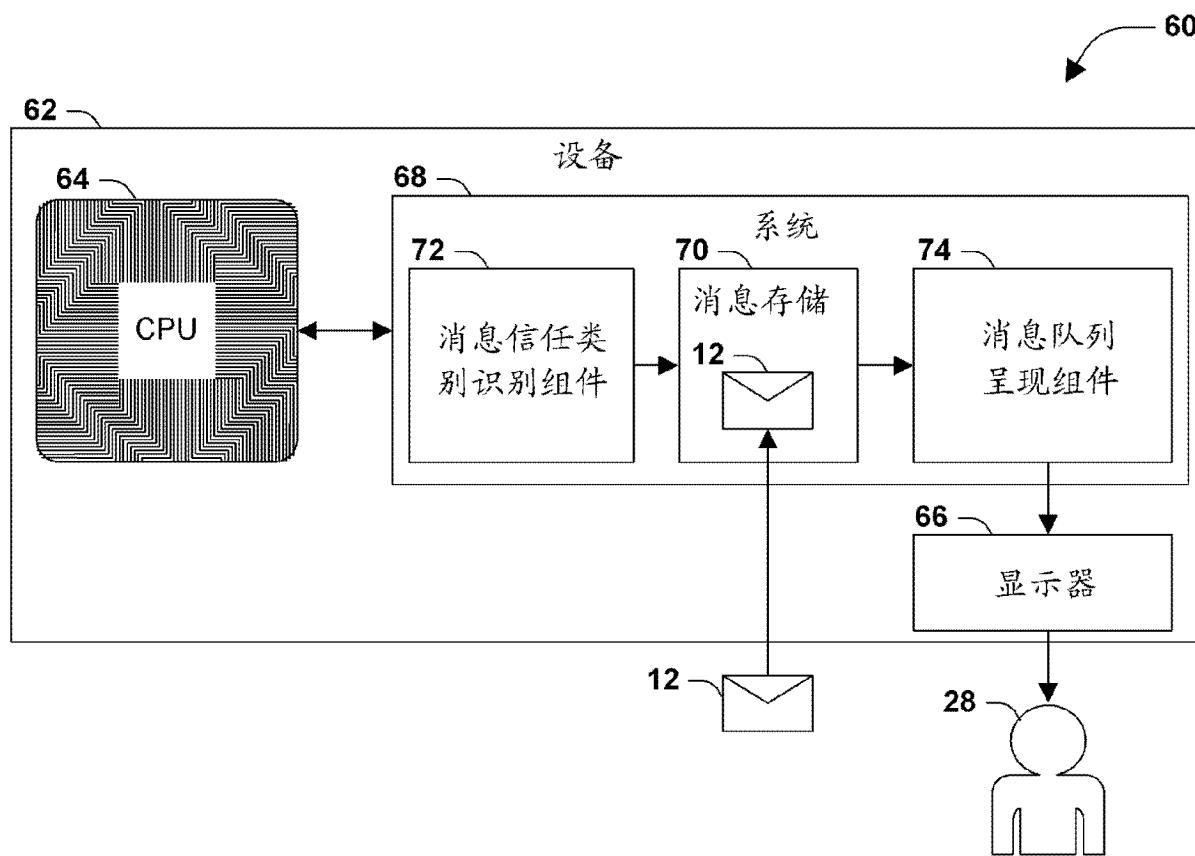


图 4

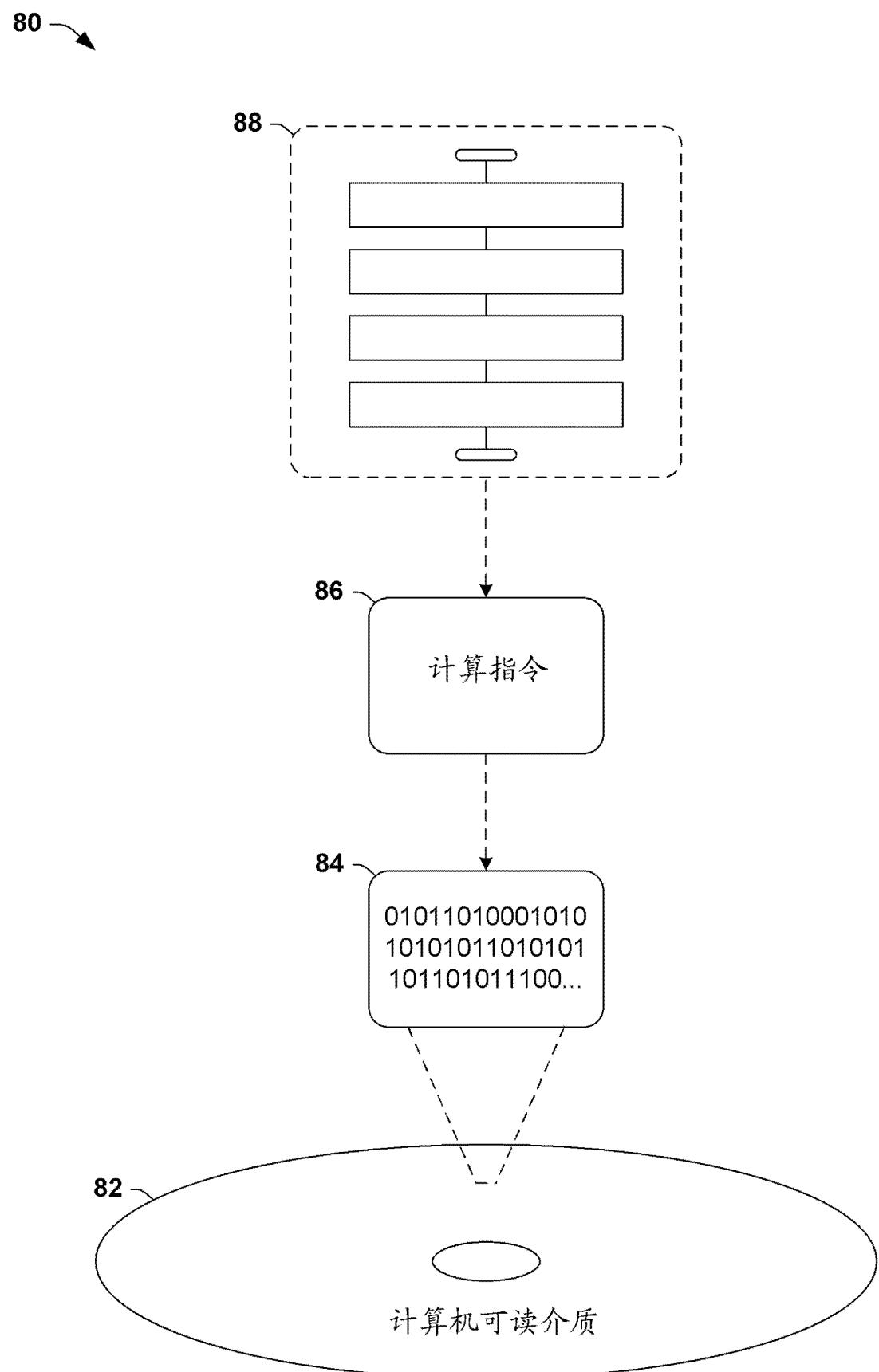


图 5

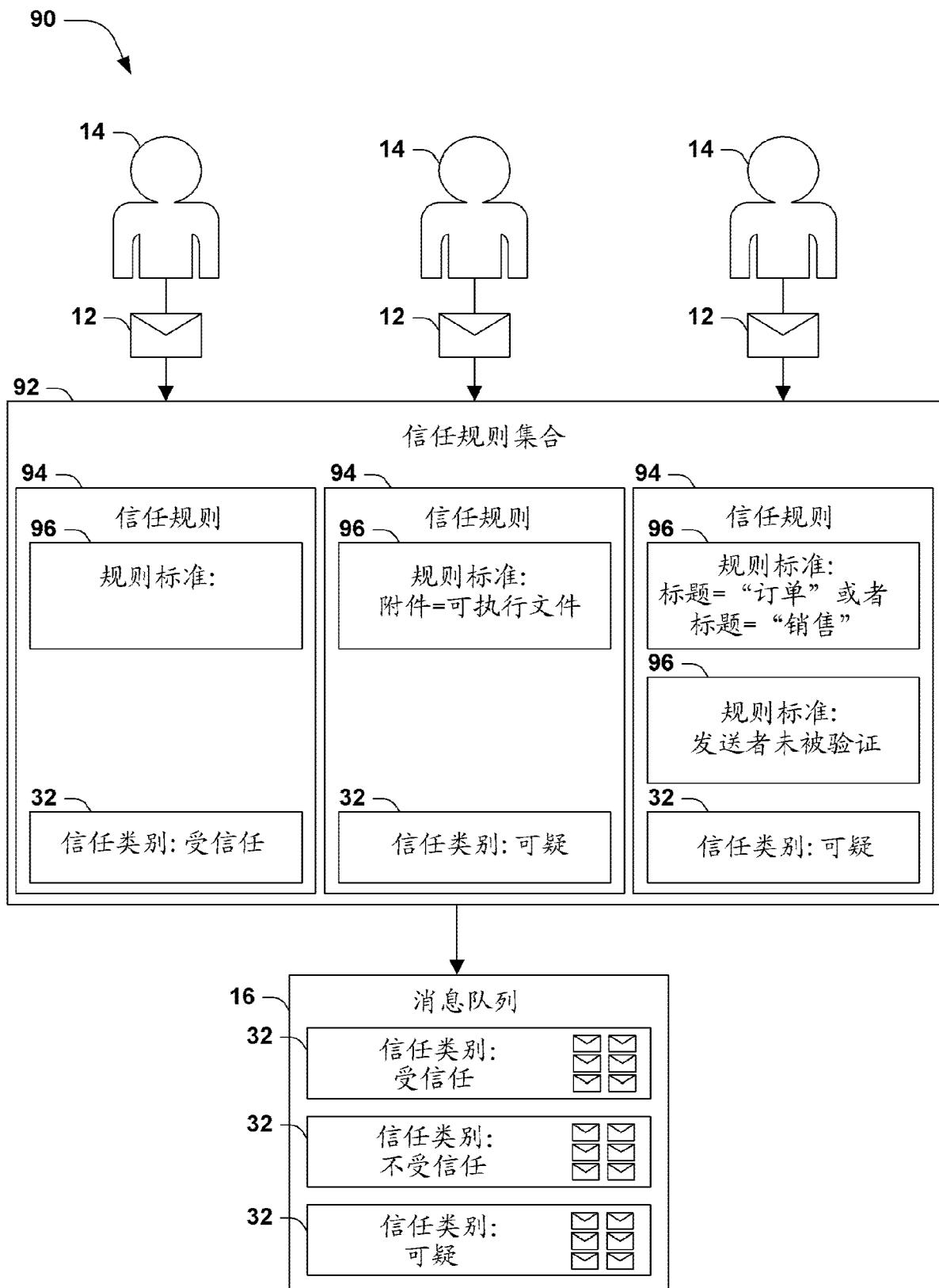


图 6

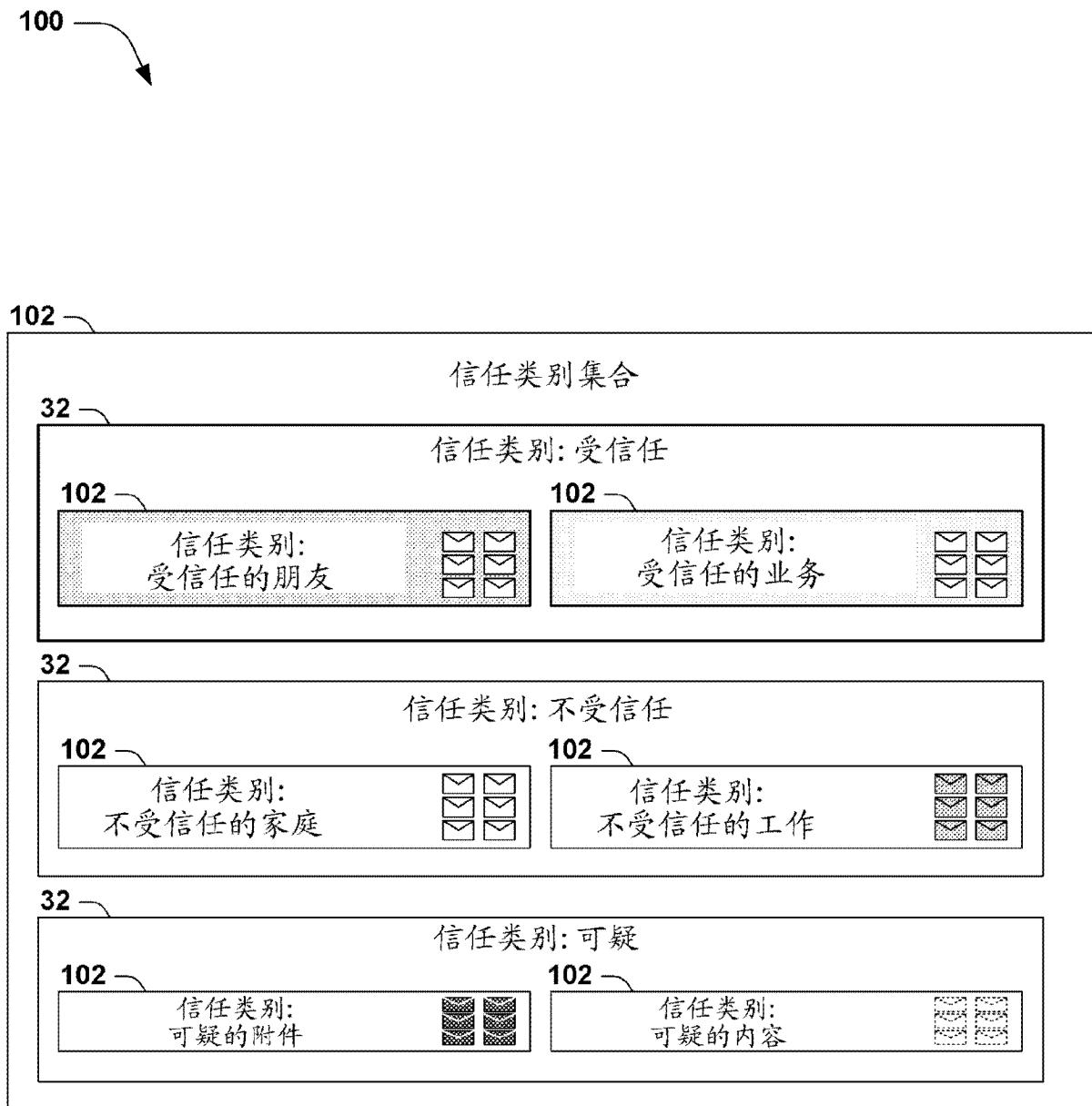


图 7

24 → 110

消息队列列表: 收件箱			
来自	标题	接收时间	
Seller.com	新产品	今天	38
Joe Smith	班级作业	今天	34
Store.com	您的订单	昨天	34
Kate Jones	明天的会议	星期二	34
Deals.com	优惠券	星期二	36

12 → 24 → 112

消息队列列表: 收件箱			
来自	标题	接收时间	
Joe Smith	班级作业	今天	34
Store.com	您的订单	昨天	34
Seller.com	新产品	今天	38
Kate Jones	明天的会议	星期二	34
Deals.com	优惠券	星期二	36

12 → 24 → 114

消息队列列表: 收件箱			
来自	标题	接收时间	
Joe Smith	班级作业	今天	34
Store.com	您的订单	昨天	34
Kate Jones	明天的会议	星期二	34
Deals.com	优惠券	星期二	36
Seller.com	新产品	今天	38

24 → 116

消息队列列表: 收件箱			
来自	标题	接收时间	
Joe Smith	班级作业	今天	34
Store.com	您的订单	昨天	34
Kate Jones	明天的会议	星期二	34
Deals.com	优惠券	星期二	36

18 →
 文件夹2
 (垃圾)
 12 →



图 8

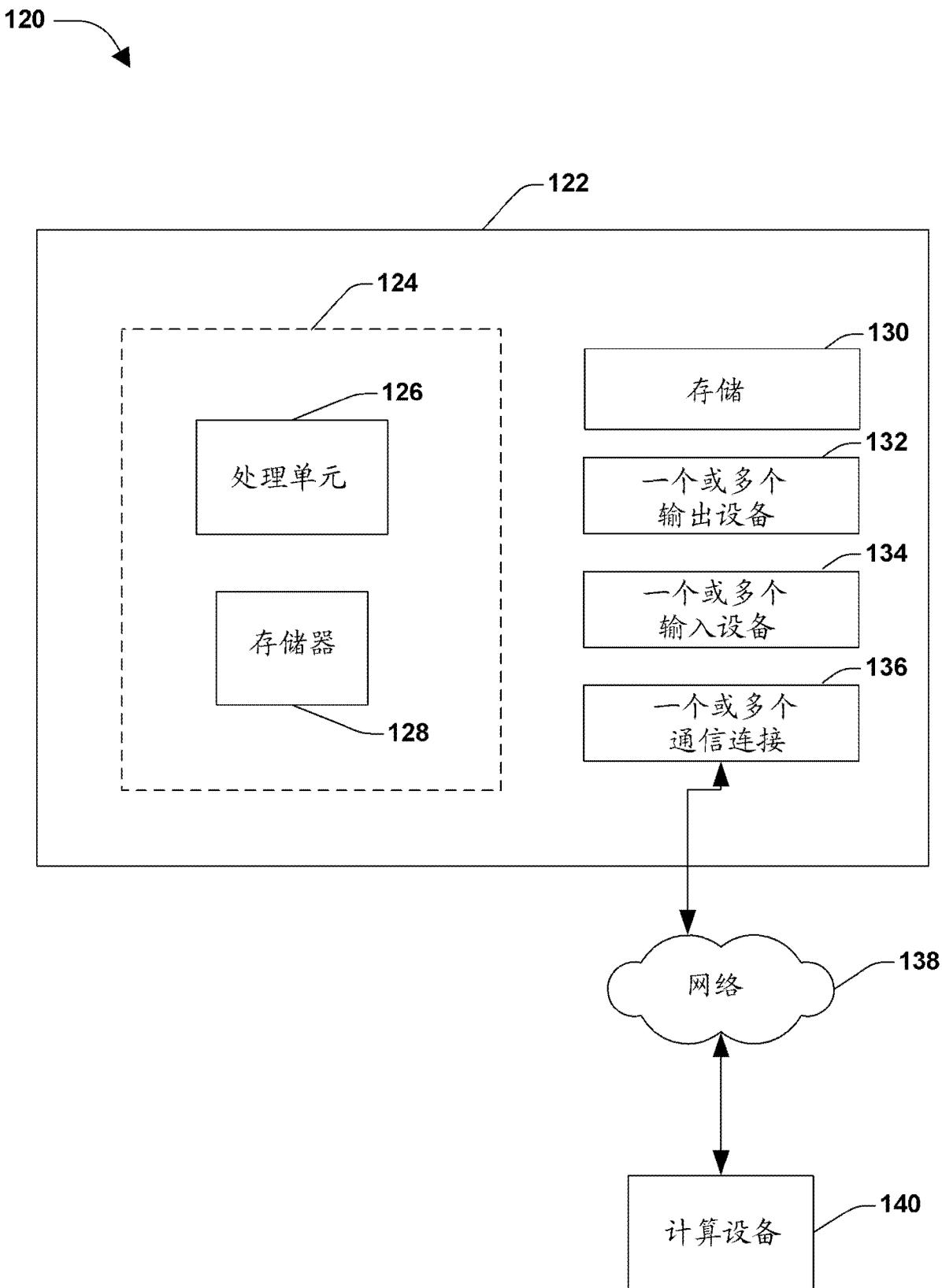


图 9