(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2016 年 11 月 17 日 (17.11.2016)

WIPO | PCT

(10) 国际公布号
WO 2016/180134 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01)

(21) 国际申请号: PCT/CN2016/078990

(22) 国际申请日: 2016 年 4 月 11 日 (11.04.2016)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201510236503.3 2015 年 5 月 11 日 (11.05.2015) CN

(71) 申请人: **中兴通讯股份有限公司 (ZTE CORPORATION)** [CN/CN]; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。

(72) 发明人: **滕志猛 (TENG, Zhimeng)**; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦中兴通讯股份有限公司转交, Guangdong 518057 (CN)。 **蒋璐峥 (JIANG, Luzheng)**; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦中兴通讯股份有限公司转交, Guangdong 518057 (CN)。 **沈岷 (SHEN, Min)**; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦中兴通讯股份有限公司转交, Guangdong 518057 (CN)。 **严为 (YAN, Wei)**; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦中兴通讯股份有限公司转交, Guangdong 518057 (CN)。 **周娜 (ZHOU, Na)**; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦中兴通讯股份有限公司转交, Guangdong 518057 (CN)。 **霍玉臻 (HUO, Yuzhen)**; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦中兴通讯股份有限公司转交, Guangdong 518057 (CN)。

(74) 代理人: **北京安信方达知识产权代理有限公司 (AFD CHINA INTELLECTUAL PROPERTY LAW OFFICE)**; 中国北京市海淀区学清路 8 号 B 座 1601A, Beijing 100192 (CN)。

(81) 指定国 (除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR,

[见续页]

(54) **Title**: METHOD AND APPARATUS FOR MANAGING INFORMATION SECURITY SPECIFICATION LIBRARY

(54) **发明名称** : 管理信息安全规范库的方法和装置

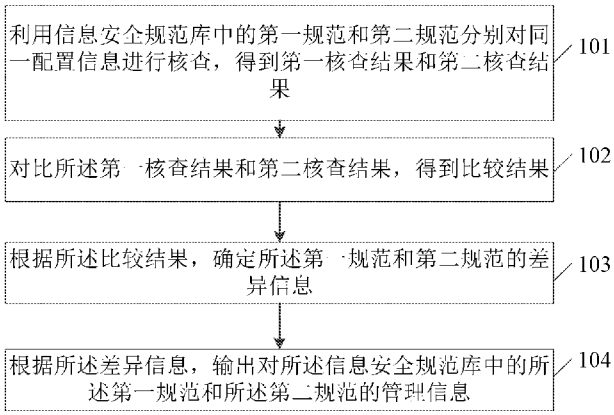

图 1

101 Respectively check same configuration information by using a first specification and a second specification in an information security specification library, so as to obtain a first check result and a second check result

102 Compare the first check result and the second check result to obtain the comparison result

103 Determine difference information between the first specification and the second specification according to the comparison result

104 Output management information of the first specification and the second specification in the information security specification library according to the difference information

(57) **Abstract**: A method for managing an information security specification library comprises: respectively checking same configuration information by using a first specification and a second specification in an information security specification library, so as to obtain a first check result and a second check result; comparing the first check result and the second check result to obtain the comparison result; determining difference information between the first specification and the second specification according to the comparison result; and outputting management information of the first specification and the second specification in the information security specification library according to the difference information.

(57) **摘要**: 一种管理信息安全规范库的方法，包括：利用信息安全规范库中的第一规范和第二规范分别对同一配置信息进行核查，得到第一核查结果和第二核查结果；对比所述第一核查结果和第二核查结果，得到比较结果；根据所述比较结果，确定所述第一规范和第二规范的差异信息；根据所述差异信息，输出对所述信息安全规范库中的所述第一规范和所述第二规范的管理信息。

WO 2016/180134 A1

CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) **指定国** (除另有指明，要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

根据细则 4.17 的声明:

— 关于申请人有权申请并被授予专利(细则 4.17(ii))

— 发明人资格(细则 4.17(iv))

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

管理信息安全规范库的方法和装置

技术领域

本文涉及但不限于通信领域，涉及一种管理信息安全规范库的方法和装置。

背景技术

目前，网络安全性正受到越来越普遍的关注，一方面因为网络入侵事件经常发生，另一方面由于网络安全性技术的大量涌现。如何利用网络安全性技术保护企业网络系统的安全成为大家所关心的问题。网络的安全性不是单纯的技术问题，它和系统的管理维护制度等方面密切相关。整个网络系统的安全性不仅依赖于安全可靠的网络操作、应用系统和网络设备的安全性，还依赖制定完整的安全策略。

完整的网络系统安全策略涵盖的内容很多，例如反病毒、备份、内容过滤、防火墙、端点加密、反恶意软件工具等技术控制手段应当在安全策略中涉及到对这些技术的控制，并应当描述如何实施这些控制来保护单位的资源。问题是一些企业存在对安全管理不重视或者网络安全管理员自身安全领域相关知识匮乏，导致整个企业安全策略不完善，存在可能被黑客利用的漏洞，严重威胁到企业网络安全。

相关技术多为对配置的核查与改进，缺乏对策略规范库的管理，因此如何管理相关安全策略规范库是亟待解决的问题。

发明内容

以下是对本文详细描述的主题的概述。本概述并非是为了限制权利要求的保护范围。

本发明实施例提供一种管理信息安全规范库的方法和装置，实现了对信息安全规范库的管理。

本发明实施例提供了一种管理信息安全规范库的方法，包括：利用信息

安全规范库中的第一规范和第二规范对同一配置信息进行核查，得到第一核查结果和第二核查结果；对比所述第一核查结果和第二核查结果，得到比较结果；根据所述比较结果，确定所述第一规范和第二规范的差异信息；根据所述差异信息，输出对所述信息安全规范库中的所述第一规范和所述第二规范的管理信息。

可选地，所述根据所述比较结果，确定所述第一规范和第二规范的差异信息，包括:

根据所述比较结果，获取所述配置信息分别在所述第一规范和第二规范中不遵从的核查条目；

根据得到的核查条目，得到所述第一规范和第二规范的差异信息。

可选地，所述根据得到的核查条目，得到所述第一规范和第二规范的差异信息之后，所述方法还包括:

利用预先存储的评估模板，对所述核查条目进行评估，确定所述配置信息对不遵从所述核查条目时造成不同遵从程度的原因；

根据得到的原因，查找所述原因对应的建议信息；

输出所述建议信息。

可选地，根据所述比较结果，确定所述第一规范和第二规范的差异信息之后，所述方法还包括:

通知将接收到的核查条目更新到所述信息安全规范库的模板中；或者，

通知对所述信息安全规范库的模板中已有的核查条目进行删除操作；或者，

通知对所述信息安全规范库中已有的核查条目进行修改操作。

可选地，所述配置信息为预先存储的配置信息或者随机采集得到的配置信息。

本发明实施例提供一种管理信息安全规范库的装置，包括：核查模块，设置为利用信息安全规范库中的第一规范和第二规范对同一配置信息进行核查，得到第一核查结果和第二核查结果；对比模块，设置为对比所述第一核

查结果和第二核查结果，得到比较结果；第一确定模块，设置为根据所述比较结果，确定所述第一规范和第二规范的差异信息；第一输出模块，设置为根据所述差异信息，输出对所述信息安全规范库中的所述第一规范和所述第二规范的管理信息。

可选地，所述第一确定模块包括:

获取单元，设置为根据所述比较结果，获取所述配置信息分别在所述第一规范和第二规范中不遵从的核查条目；

确定单元，设置为根据得到的核查条目，得到所述第一规范和第二规范的差异信息。

可选地，所述装置还包括:

第二确定模块，设置为利用预先存储的评估模板，对所述核查条目进行评估，确定所述配置信息对不遵从所述核查条目时造成不同遵从程度的原因；

查找模块，设置为根据得到的原因，查找所述原因对应的建议信息；

第二输出模块，设置为：输出所述建议信息。

可选地，所述装置还包括:

通知模块，设置为通知将接收到的核查条目更新到所述信息安全规范库的模板中；或者，通知对所述信息安全规范库的模板中已有的核查条目进行删除操作；或者，通知对所述信息安全规范库中已有的核查条目进行修改操作。

可选地，所述配置信息为预先存储的配置信息或者随机采集得到的配置信息。

此外，本发明实施例还提供一种计算机可读存储介质，所述计算机可读存储介质中存储有计算机可执行指令，所述计算机可执行指令被执行时实现所述管理信息安全规范库的方法。

在本发明实施例中，利用第一规范和第二规范对同一配置信息进行核查，得到第一核查结果和第二核查结果，并对比第一核查结果和第二核查结果，得到比较结果，再根据所述比较结果，确定所述第一规范和第二规范的差异信息，根据所述差异信息，输出对所述信息安全规范库中的所述第一规范和

所述第二规范的管理信息，方便用户获知规范之间的差异，为日后进一步完善规范提供了依据。

在阅读并理解了附图和详细描述后，可以明白其它方面。

附图说明

图 1 为本发明实施例一提供的管理信息安全规范库的方法的流程图;

图 2 为本发明实施例二提供的管理信息安全规范库的方法的流程图;

图 3 为本发明实施例三提供的管理信息安全规范库的方法的流程图;

图 4 为本发明实施例四提供的管理信息安全规范库的方法的流程图;

图 5 为本发明实施例五提供的管理信息安全规范库的装置的结构图;

图 6 为本发明实施例五提供的管理信息安全规范库的装置的另一结构图。

具体实施方式

下面将结合附图及具体实施例对本发明实施例的技术方案作进一步的详细描述。需要说明的是，在不冲突的情况下，本申请中的实施例及实施例中的特征可以相互任意组合。

实施例一

图 1 为本发明实施例一提供的管理信息安全规范库的方法的流程图。图 1 所示方法包括:

步骤 101、利用信息安全规范库中的第一规范和第二规范分别对同一配置信息进行核查，得到第一核查结果和第二核查结果;

步骤 102、对比所述第一核查结果和第二核查结果，得到比较结果;

步骤 103、根据所述比较结果，确定所述第一规范和第二规范的差异信息;

步骤 104、根据所述差异信息，输出对所述信息安全规范库中的所述第一规范和所述第二规范的管理信息。

本实施例提供的方法，利用第一规范和第二规范分别对同一配置信息进行核查，得到第一核查结果和第二核查结果，并对比第一核查结果和第二核查结果，得到比较结果，再根据所述比较结果，确定所述第一规范和第二规范的差异信息，根据所述差异信息，输出对所述信息安全规范库中的所述第一规范和所述第二规范的管理信息，方便用户获知规范之间的差异，为日后进一步完善信息安全规范库提供了依据。

在实际应用中，信息安全规范包含各种丰富的知识规范库，既包含标准规范库，例如各种风险库、合规库、基线库等，也包含用户自定义的规范库，例如安全管理策略库等，这些核查库和核查条目可以从不同维度为设备、装置或系统提供不同需求的核查。

上文所说的配置信息包括设备、装置或系统的配置信息。配置信息可以通过例如配置命令远程采集设备、装置或系统获取，或者从设备、装置或系统的维护管理设备上获取，或者本地构建或生成设备、装置或系统的配置信息文件。

可以为配置信息选择多个不同的信息安全规范库，进行配置核查。例如，为配置信息选择两种不同的规范进行配置核查。将配置信息根据规范 1 中的配置核查条目进行核查，依据配置核查条目检测相关配置信息的遵从程度，生成配置核查结果。同样，将该配置信息根据规范 2 中的配置核查条目进行核查，依据配置核查条目检测相关配置信息的遵从程度，生成另一个配置核查结果。

将上述两个配置核查结果进行对比，比较同一配置信息针对两种不同规范的遵从程度。不同规范包含的配置核查条目可能会不同，因此同一配置信息对不同规范的核查有不同的遵从程度，安全策略管控设备可以分析造成不同遵从程度的原因，找出不同规范间的差异，例如，不遵从条目间是否存在范围太宽、某些条目对应内容是否有更高风险、是否存在更大漏洞等，展示给用户参考决策。可选地，支持根据实际网络安全需求将核查条目更新到规范库模版中，这里的规范库模版可以包括标准规范模版，也可以包括自定义的规范模版，从而完善规范库功能。

实施例二

下面对本发明实施例提供的方法作进一步说明:

图 2 为本发明实施例二提供的管理信息安全规范库的方法的流程图。在此实施例中，安全策略管控设备不仅可以对核查对比分析给出合理建议，同时还支持配置的变更，如图 2 所示:

步骤 201、配置信息选择多个不同的知识库，进行配置核查;

例如，为配置选择两种不同的规范进行配置核查，这里选择核查用的规范模版既可以包含需要改进更新的模版，也可以不包含。将配置信息，根据规范 1 中的配置核查条目进行核查，依据配置核查条目检测相关配置信息的遵从程度，生成配置核查结果。同样，将配置信息，根据规范 2 中的配置核查条目进行核查，依据配置核查条目检测相关配置信息的遵从程度，生成另一个配置核查结果。

步骤 202、对比上述配置核查结果，比较同一配置信息针对两种不同规范的遵从程度;

步骤 202 可以包括: 根据所述比较结果，获取所述配置信息分别在所述第一规范和第二规范中不遵从的核查条目；根据得到的核查条目，得到所述第一规范和第二规范的差异信息。例如，不同规范包含的配置核查条目可能会不同，因此同一配置信息对不同规范的核查会有不同的遵从程度，可以将不遵从条目整理展示。安全策略管控设备评估分析功能是根据评估模版对不遵从条目分析造成不同遵从程度的原因，找出不同规范间的差异，例如，不遵从条目间是否存在范围太宽，某些条目对应内容是否有更高风险、是否存在更大漏洞等，展示给用户参考决策。

步骤 203、利用预先存储的评估模板，对所述核查条目进行评估;

对所述核查条目进行评估从而确定所述配置信息对不遵从所述核查条目时造成不同遵从程度的原因；根据得到的原因，查找所述原因对应的建议信息；输出所述建议信息。

其中，建议信息可以是预先存储的，在确定原因后，通过查找对应建议信息，并将查找到的建议信息输出给用户，为用户进一步完善信息安全规范库提供了帮助。

步骤 204、向本地给安全策略管控设备发送更新规范库请求；

例如，要添加核查条目到规范库中，可以给安全策略管控设备发送一个添加信息安全规范库条目的请求，请求内容包含：添加操作码+要操作的规范库 ID+添加条目序号+添加的具体条目内容；要修改原规范库中核查条目，可以给安全策略管控设备发送一个修改信息安全规范库条目的请求，请求内容包含：修改操作码+要操作的规范库 ID +修改的条目序号+修改的具体条目内容；同样要删除原规范库中核查条目，可以给安全策略管控设备发送一个删除信息安全规范库条目的请求，请求内容包含：删除操作码+要操作的规范库 ID +删除的条目序号（该序号为唯一标识号）。

步骤 205、安全策略管控设备接收并响应更新规范库请求。

例如，安全策略管控设备对收到的请求进行解析，如果得到内容是需要添加条目到任一信息安全规范库中，则安全策略管控设备会调用该信息安全规范库并执行添加操作。这里需要改进的规范库模版既可以是标准规范模版，也可以是自定义的规范模版。

可选地，本实施例支持信息安全规范库的改进。例如，可以根据实际网络安全需求，将上述存在更高风险的核查条目更新到信息安全规范库模版中，或者删除规范库模版中不必要的核查条目，当然还可以对信息安全规范库模块中核查条目进行变更。支持配置信息变更功能。例如，对于上述核查结果为不遵从的配置项，安全策略管控设备根据核查结果中的建议，支持对配置信息的变更，可以是添加、修改、删除配置信息等。还支持将变更后的配置信息下发。例如可以本地构建配置文件下发到设备、装置或系统上，也可以直接远程设备、装置或系统，下发配置命令，使其变更为符合核查条目的配置信息。

本发明实施例二提供的方法，利用第一规范和第二规范分别对同一配置信息进行核查，得到第一核查结果和第二核查结果，并对比第一核查结果和第二核查结果，得到比较结果，再根据所述比较结果，确定所述第一规范和第二规范的差异信息，根据所述差异信息，输出对所述信息安全规范库中的所述第一规范和所述第二规范的管理信息，方便用户获知规范之间的差异，为日后进一步完善规范提供了依据；通过确定第一规范和第二规范之间的差

异，根据该差异提出建议信息，方便用户进一步完善规范，另外，通过对配置信息的变更，可以有效提高配置信息的准确性。

实施例三

图 3 为本发明实施例三提供的管理信息安全规范库的方法的流程图。如图 3 所示，所述方法包括:

步骤 301、为配置选择多个不同的知识库，进行配置核查;

例如，为配置信息选择两种不同的规范进行配置核查，这里选择核查用的规范模版既可以包含需要改进更新的模版，也可以不包含。将配置信息，根据规范 1 中的配置核查条目进行核查，依据配置核查条目检测相关配置信息的遵从程度，生成配置核查结果。同样，将配置信息，根据规范 2 中的配置核查条目进行核查，依据配置核查条目检测相关配置信息的遵从程度，生成另一配置核查结果。

在本实施例中，安全策略管控设备可以支持通过采集的配置信息进行核查对比分析的方法，采集的配置信息包括设备、装置或系统的配置信息。例如，可以通过配置命令远程登录设备、装置或系统采集获取，或者从设备、装置或系统的维护管理设备上获取。

步骤 302、对比上述两个配置核查结果，比较同一配置信息针对两种不同规范的遵从程度;

例如，不同规范包含的配置核查条目可能会不同，因此同一配置信息对不同规范的核查会有不同的遵从程度，可以将不遵从条目整理展示。

步骤 303、评估分析;

安全策略管控设备评估分析功能是根据评估模版对不遵从条目分析造成不同遵从程度的原因，找出不同规范间的差异，例如，不遵从条目间是否存在范围太宽，某些条目对应内容是否有更高风险、是否存在更大漏洞等，展示给用户参考决策。

步骤 304、给安全策略管控设备发送更新规范库请求;

例如，要添加核查条目到信息安全规范库中，可以给安全策略管控设备发送一个添加信息安全规范库条目的请求，请求内容包含: 添加操作码+要操

作的规范库 ID+添加条目序号+添加的具体条目内容；要修改原规范中条目，可以给安全策略管控设备发送一个修改信息安全规范库条目的请求，请求内容包含：修改操作码+要操作的规范库 ID +修改的条目序号+修改的具体条目内容；同样要删除原规范中条目，可以给安全策略管控设备发送一个删除信息安全规范库条目的请求，请求内容包含：删除操作码+要操作的规范库 ID + 删除的条目序号（该序号为唯一标识号）。

步骤 305、接收并响应变更请求。

例如，安全策略管控设备对收到的请求进行解析，得到内容是需要添加条目到某规范库中，安全策略管控设备会调用该规范库并执行添加操作。这里需要改进的规范库模版既可以是标准规范模版，也可以是自定义的规范模版。

可选地，本实施例支持信息安全规范库的改进。例如，可以根据实际网络安全需求，将上述存在更高风险的核查条目更新到信息安全规范库模版中，或者删除规范库模版中不必要的核查条目，当然还可以对信息安全规范库模块中核查条目进行变更。

本发明实施例三提供的方法，利用第一规范和第二规范对同一配置信息进行核查，得到第一核查结果和第二核查结果，并对比第一核查结果和第二核查结果，得到比较结果，再根据所述比较结果，确定所述第一规范和第二规范的差异信息，根据所述差异信息，输出对所述信息安全规范库中的所述第一规范和所述第二规范的管理信息，方便用户获知规范之间的差异，为日后进一步完善规范提供了依据；通过确定第一规范和第二规范之间的差异，根据该差异提出建议信息，方便用户进一步完善规范，另外，通过对配置信息的变更，可以有效提高配置信息的准确性；利用采集得到的配置信息进行核查，提高了数据的随机性，为后续获取管理数据提供了帮助。

实施例四

图 4 为本发明实施例四提供的管理信息安全规范库的方法的流程图。如图 4 所示，所述方法包括：

步骤 401、为配置信息选择多个不同的知识库，进行配置核查；

例如，为配置选择两种不同的规范进行配置核查，这里选择核查用的规范模版既可以包含需要改进更新的模版，也可以不包含。将配置信息，根据规范 1 中的配置核查条目进行核查，依据配置核查条目检测相关配置信息的遵从程度，生成配置核查结果。同样，将配置信息，根据规范 2 中的配置核查条目进行核查，依据配置核查条目检测相关配置信息的遵从程度，生成另一个配置核查结果。

在此实施例中，安全策略管控设备可以支持通过计划配置进行核查对比分析，从而增强安全策略规范的方法，配置信息为设备、装置或系统的配置信息文件。例如，可以通过本地构建或生成设备、装置或系统的计划配置信息文件。

步骤 402、将上述两个配置核查结果进行对比，比较同一配置信息针对两种不同规范的遵从程度;

例如，不同规范包含的配置核查条目可能会不同，因此同一配置信息对不同规范的核查会有不同的遵从程度，可以将不遵从条目整理展示。

步骤 403、评估分析;

安全策略管控设备评估分析功能是根据评估模版对不遵从条目分析造成不同遵从程度的原因，找出不同规范间的差异，例如，不遵从条目间是否存在范围太宽，某些条目对应内容是否有更高风险、是否存在更大漏洞等，展示给用户参考决策。

步骤 404、给安全策略管控设备发送更新规范库请求;

例如，要添加核查条目到信息安全规范库中，可以给安全策略管控设备发送一个添加信息安全规范库条目的请求，请求内容包含：添加操作码+要操作的规范库 ID+添加条目序号+添加的具体条目内容；要修改原规范中条目，可以给安全策略管控设备发送一个修改信息安全规范库条目的请求，请求内容包含：修改操作码+要操作的规范库 ID +修改的条目序号+修改的具体条目内容；同样要删除原规范中条目，可以给安全策略管控设备发送一个删除信息安全规范库条目的请求，请求内容包含：删除操作码+要操作的规范库 ID + 删除的条目序号（该序号为唯一标识号）。

步骤 405、安全策略管控设备接收并响应变更请求。

例如，安全策略管控设备对收到的请求进行解析，得到内容是需要添加条目到任一规范库中，安全策略管控设备会调用该信息安全规范库并执行添加操作。这里需要改进的信息安全规范库模版既可以是标准规范模版，也可以是自定义的规范模版。

可选地，本实施例支持信息安全规范库的改进。例如，可以根据实际网络安全需求，将上述存在更高风险的核查条目更新到信息安全规范库模版中，或者删除信息安全规范库模版中不必要的核查条目，当然还可以对信息安全规范库模块中核查条目进行变更。步骤可以如下:

本发明实施例四提供的方法，利用第一规范和第二规范分别对同一配置信息进行核查，得到第一核查结果和第二核查结果，并对比第一核查结果和第二核查结果，得到比较结果，再根据所述比较结果，确定所述第一规范和第二规范的差异信息，根据所述差异信息，输出对所述信息安全规范库中的所述第一规范和所述第二规范的管理信息，方便用户获知规范之间的差异，为日后进一步完善规范提供了依据；通过确定第一规范和第二规范之间的差异，根据该差异提出建议信息，方便用户进一步完善规范，另外，通过对配置信息的变更，可以有效提高配置信息的准确性；通过预先存储的配置信息进行检测，减少了配置数据的采集流程，减少了前期的准备时间，提高了处理速度。

实施例五

图 5 为本发明实施例提供的管理信息安全规范库的装置的结构图。图 5 所示装置包括:

核查模块 501，设置为利用信息安全规范库中的第一规范和第二规范分别对同一配置信息进行核查，得到第一核查结果和第二核查结果;

对比模块 502，设置为对比所述第一核查结果和第二核查结果，得到比较结果;

第一确定模块 503，设置为根据所述比较结果，确定所述第一规范和第二规范的差异信息；

第一输出模块 504，设置为根据所述差异信息，输出对所述信息安全规范库中的所述第一规范和所述第二规范的管理信息。

可选地，如图 6 所示，所述第一确定模块包括：

获取单元 5031，设置为根据所述比较结果，获取所述配置信息分别在所述第一规范和第二规范中不遵从的核查条目；

确定单元 5032，设置为根据得到的核查条目，得到所述第一规范和第二规范的差异信息。

可选的，所述装置还包括：

第二确定模块 505，设置为利用预先存储的评估模板，对所述核查条件进行评估，确定所述配置信息对不遵从所述核查条目时造成不同遵从程度的原因；

查找模块 506，设置为根据得到的原因，查找所述原因对应的建议信息；

第二输出模块 507，设置为：输出所述建议信息。

可选的，所述装置还包括：

通知模块 508，设置为通知将接收到的核查条目更新到所述信息安全规范库的模板中；或者，通知对所述信息安全规范库的模板中已有的核查条目进行删除操作；或者，通知对所述信息安全规范库中已有的核查条目进行修改操作。

可选的，所述配置信息为预先存储的配置信息或者随机采集得到的配置信息。

本发明实施例提供的管理信息安全规范库的装置，利用第一规范和第二规范对同一配置信息进行核查，得到第一核查结果和第二核查结果，并对比第一核查结果和第二核查结果，得到比较结果，再根据所述比较结果，确定所述第一规范和第二规范的差异信息，根据所述差异信息，输出对所述信息安全规范库中的所述第一规范和所述第二规范的管理信息，方便用户获知规范之间的差异，为日后进一步完善规范提供了依据。

此外，本发明实施例还提供一种计算机可读存储介质，所述计算机可读存储介质中存储有计算机可执行指令，所述计算机可执行指令被执行时实现所述管理信息安全规范库的方法。

本领域普通技术人员可以理解上述实施例的全部或部分步骤可以使用计算机程序流程来实现，所述计算机程序可以存储于一计算机可读存储介质中，所述计算机程序在相应的硬件平台上（如系统、设备、装置、器件等）执行，在执行时，包括方法实施例的步骤之一或其组合。

可选地，上述实施例的全部或部分步骤也可以使用集成电路来实现，这些步骤可以被分别制作成一个个集成电路模块，或者将它们中的多个模块或步骤制作成单个集成电路模块来实现。这样，本申请不限制于任何特定的硬件和软件结合。

上述实施例中的各装置/功能模块/功能单元可以采用通用的计算装置来实现，它们可以集中在单个的计算装置上，也可以分布在多个计算装置所组成的网络上。

上述实施例中的各装置/功能模块/功能单元以软件功能模块的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。上述提到的计算机可读取存储介质可以是只读存储器，磁盘或光盘等。

以上所述，仅为本发明的具体实施方式，但本发明的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本发明揭露的技术范围内，可轻易想到变化或替换，都应涵盖在本发明的保护范围之内。因此，本发明的保护范围应以权利要求所述的保护范围为准。

工业实用性

上述技术方案可以方便用户获知规范之间的差异，为日后进一步完善规范提供了依据；同时可以有效提高配置信息的准确性，减少配置数据的采集流程，减少前期的准备时间，提高处理速度。

权 利 要 求 书

1、一种管理信息安全规范库的方法，包括:

利用信息安全规范库中的第一规范和第二规范分别对同一配置信息进行核查，得到第一核查结果和第二核查结果;

对比所述第一核查结果和第二核查结果，得到比较结果;

根据所述比较结果，确定所述第一规范和第二规范的差异信息;

根据所述差异信息，输出对所述信息安全规范库中的所述第一规范和所述第二规范的管理信息。

2、根据权利要求 1 所述的方法，其中，所述根据所述比较结果，确定所述第一规范和第二规范的差异信息，包括:

根据所述比较结果，获取所述配置信息分别在所述第一规范和第二规范中不遵从的核查条目;

根据得到的核查条目，得到所述第一规范和第二规范的差异信息。

3、根据权利要求 2 所述的方法，所述根据得到的核查条目，得到所述第一规范和第二规范的差异信息之后，所述方法还包括:

利用预先存储的评估模板，对所述核查条目进行评估，确定所述配置信息对不遵从所述核查条目时造成不同遵从程度的原因;

根据得到的原因，查找所述原因对应的建议信息;

输出所述建议信息。

4、根据权利要求 2 所述的方法，根据所述比较结果，确定所述第一规范和第二规范的差异信息之后，所述方法还包括:

通知将得到的核查条目更新到所述信息安全规范库的模板中；或者，

通知对所述信息安全规范库的模板中已有的核查条目进行删除操作；或者，

通知对所述信息安全规范库中已有的核查条目进行修改操作。

5、根据权利要求 1 所述的方法，其中，所述配置信息为预先存储的配置

信息或者随机采集得到的配置信息。

6、一种管理信息安全规范库的装置，包括:

核查模块，设置为利用信息安全规范库中的第一规范和第二规范分别对同一配置信息进行核查，得到第一核查结果和第二核查结果;

对比模块，设置为对比所述第一核查结果和第二核查结果，得到比较结果;

第一确定模块，设置为根据所述比较结果，确定所述第一规范和第二规范的差异信息;

第一输出模块，设置为根据所述差异信息，输出对所述信息安全规范库中的所述第一规范和所述第二规范的管理信息。

7、根据权利要求 6 所述的装置，其中，所述第一确定模块包括:

获取单元，设置为根据所述比较结果，获取所述配置信息分别在所述第一规范和第二规范中不遵从的核查条目;

确定单元，设置为根据得到的核查条目，得到所述第一规范和第二规范的差异信息。

8、根据权利要求 7 所述的装置，所述装置还包括:

第二确定模块，设置为利用预先存储的评估模板，对所述核查条目进行评估，确定所述配置信息对不遵从所述核查条目时造成不同遵从程度的原因;

查找模块，设置为根据得到的原因，查找所述原因对应的建议信息;

第二输出模块，设置为：输出所述建议信息。

9、根据权利要求 6 所述的装置，所述装置还包括:

通知模块，设置为通知将得到的核查条目更新到所述信息安全规范库的模板中；或者，通知对所述信息安全规范库的模板中已有的核查条目进行删除操作；或者，通知对所述信息安全规范库中已有的核查条目进行修改操作。

10、根据权利要求 6 所述的装置，其中，所述配置信息为预先存储的配置信息或者随机采集得到的配置信息。

11、一种计算机可读存储介质，所述计算机可读存储介质中存储有计算

机可执行指令，所述计算机可执行指令被执行时实现权利要求 1~5 任一项所述的方法；

规范库中的所述第一规范和所述第二规范的管理信息。

5

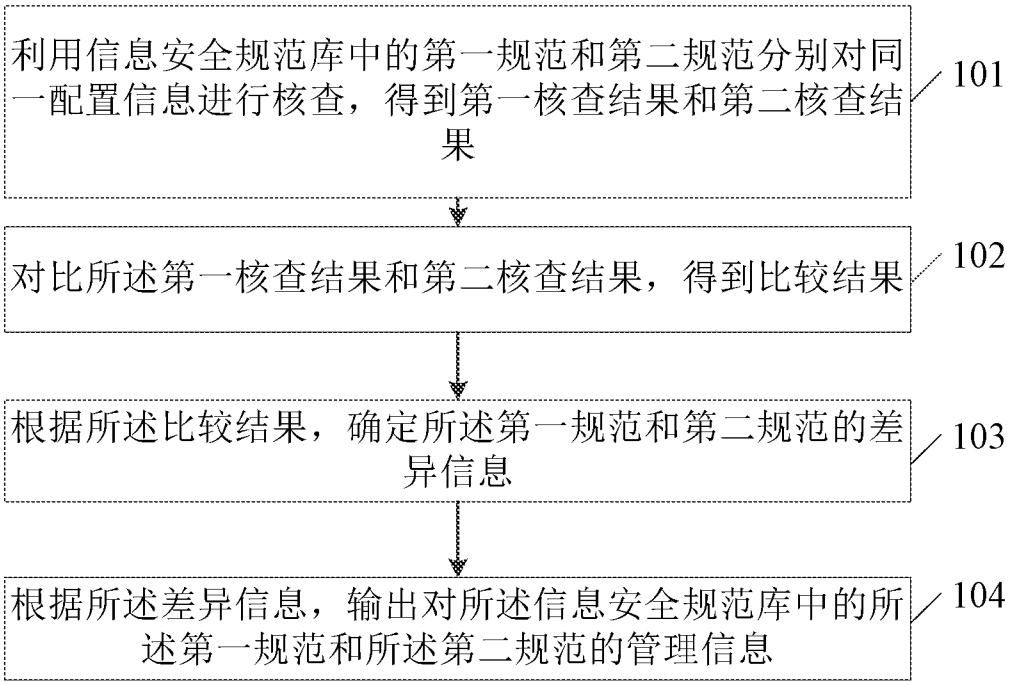
利用信息安全规范库中的第一规范和第二规范分别对同一配置信息进行核查，得到第一核查结果和第二核查结果
101
对比所述第一核查结果和第二核查结果，得到比较结果
102
根据所述比较结果，确定所述第一规范和第二规范的差异信息
103
根据所述差异信息，输出对所述信息安全规范库中的所述第一规范和所述第二规范的管理信息
104

图 1

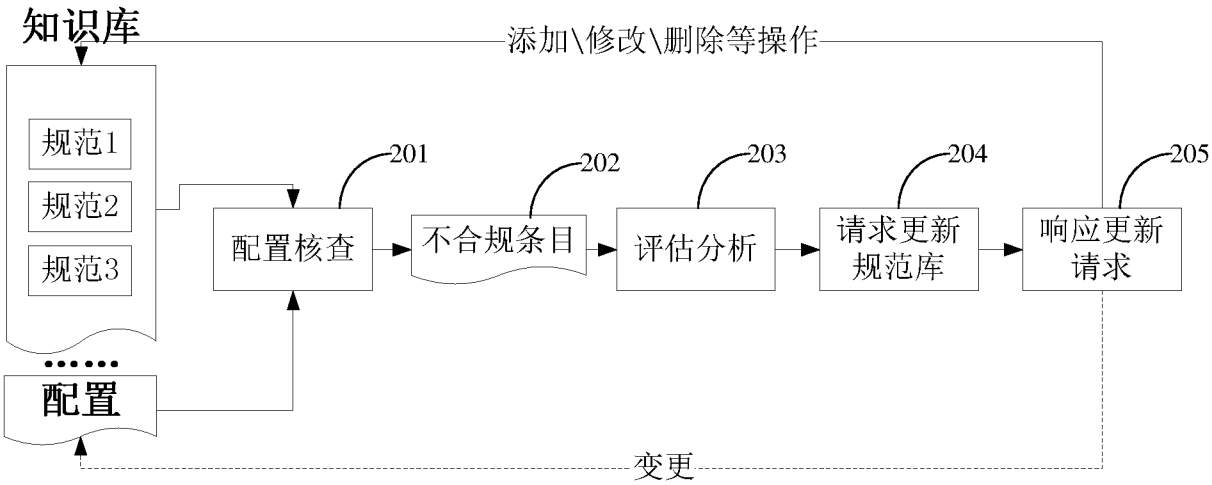
知识库
添加\修改\删除等操作
规范1
规范2
规范3
配置
201
202
203
204
205
配置核查
不合规条目
评估分析
请求更新规范库
响应更新请求
变更

图 2

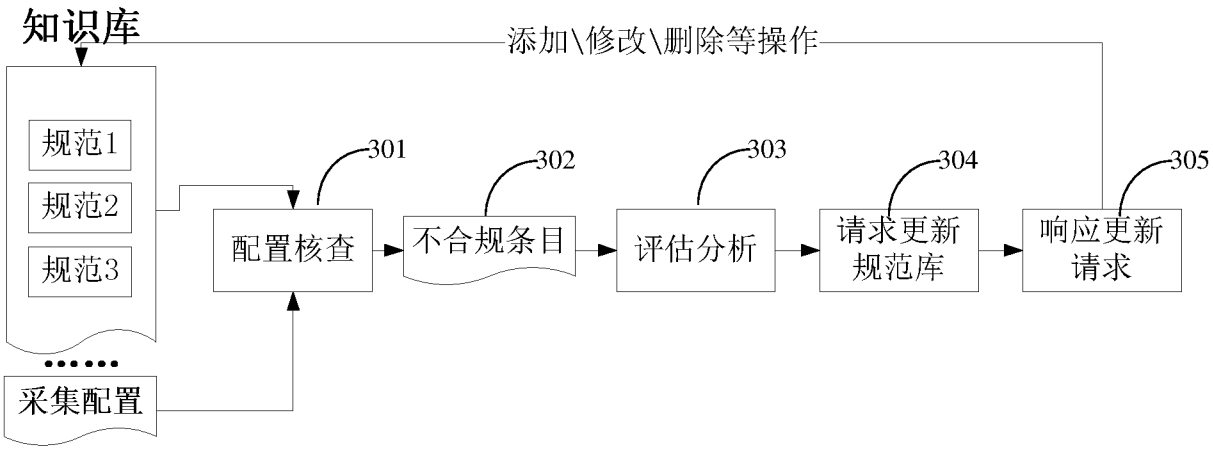
知识库
添加\修改\删除等操作
规范1
规范2
规范3
.....
采集配置
301
配置核查
302
不合规条目
303
评估分析
304
请求更新规范库
305
响应更新请求

图 3

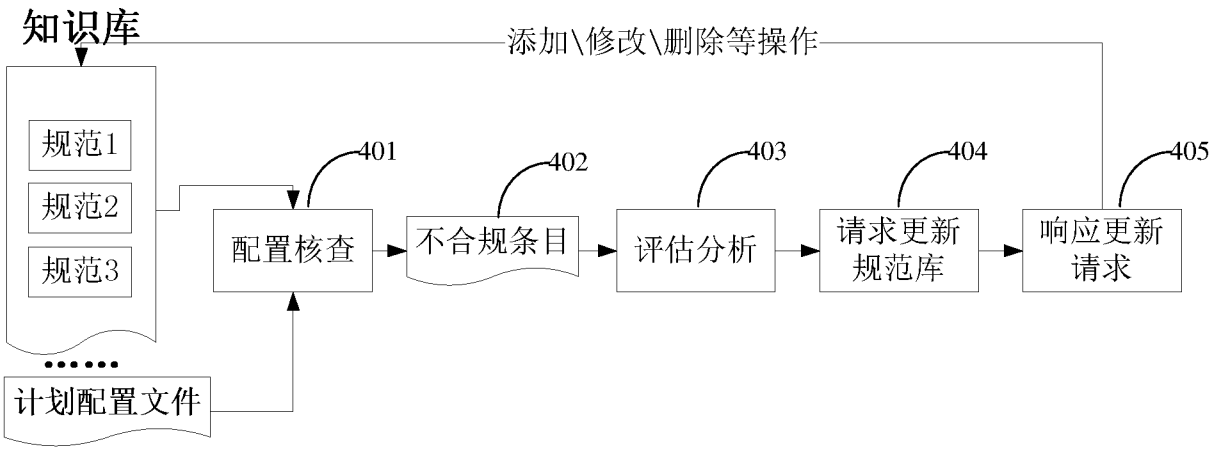
知识库
添加\修改\删除等操作
规范1
规范2
规范3
.....
计划配置文件
401
配置核查
402
不合规条目
403
评估分析
404
请求更新规范库
405
响应更新请求

图 4

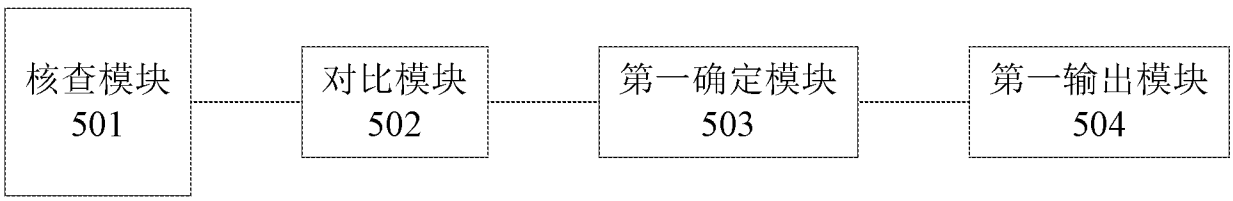
核查模块 501
对比模块 502
第一确定模块 503
第一输出模块 504

图 5

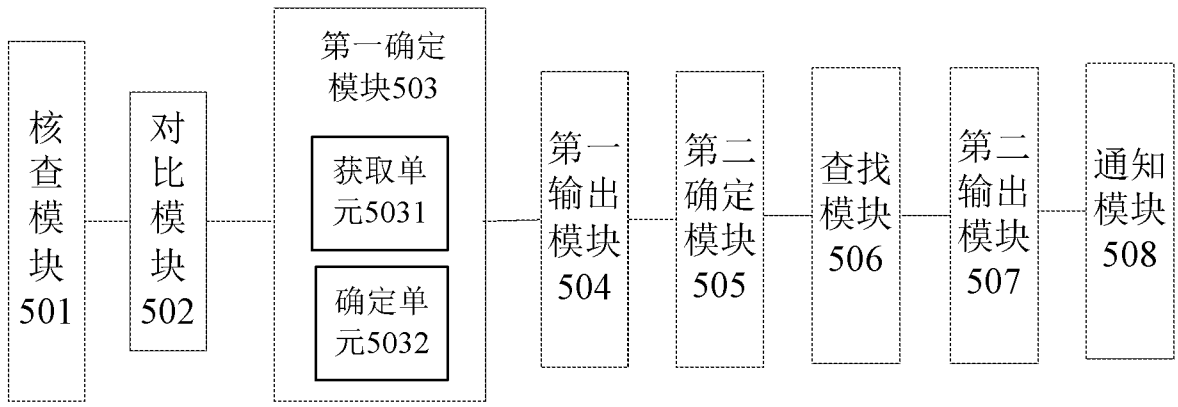
核查模块 501
对比模块 502
第一确定模块503
获取单元5031
确定单元5032
第一输出模块 504
第二确定模块 505
查找模块 506
第二输出模块 507
通知模块 508

图 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2016/078990

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNABS; CNTXT; CNKI; VEN: rule, difference, disagree, disobey, conflict+, reason, suggestion, perfect, analyz+, updat+, modif+, delet+, add+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 2819346 A1 (KASPERSKY LAB ZAO), 31 December 2014 (31.12.2014), description, paragraphs 3, 7-13, 17-18, 38-48 and 58, and figures 1-5	1-2, 4-7, 9-11
A	EP 2819346 A1 (KASPERSKY LAB ZAO), 31 December 2014 (31.12.2014), description, paragraphs3, 7-13, 17-18, 38-48 and 58, and figures 1-5	3, 8
A	CN 102341808 A (ROYAL DUTCH PHILIPS ELECTRONICS LTD.), 01 February 2012 (01.02.2012), the whole document	1-11
A	WO 2015040456 A1 (ERICSSON TELEFON AB L M), 26 March 2015 (26.03.2015), the whole document	1-11

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
31 May 2016 (31.05.2016)	**21 June 2016 (21.06.2016)**
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer **REN, Ling** Telephone No.: (86-10) **62088423**

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2016/078990

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
EP 2819346 A1	31 December 2014	RU 2013129544 A	10 January 2015
		US 2015007252 A1	01 January 2015
		US 8943547 B2	27 January 2015
CN 102341808 A	01 February 2012	WO 2010100590 A1	10 September 2010
		EP 2404259 A1	11 January 2012
		US 2011321122 A1	29 December 2011
		JP 2012519893 A	30 August 2012
		IN 201106738 P4	16 November 2012
WO 2015040456 A1	26 March 2015	None	

国际检索报告

国际申请号
PCT/CN2016/078990

A. 主题的分类

H04L 29/06(2006.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用）)

CNABS;CNTXT;CNKI;VEN:规则，rule，差异，不一致，冲突，不遵从，conflict+，原因，分析，建议，更新，修改，完善，删除，添加，analyz+，updat+，modif+，delet+，add+

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
X	EP 2819346 A1 (KASPERSKY LAB ZAO) 2014年 12月 31日 (2014-12-31) 说明书第3、7-13、17-18、38-48、58段，图1-5	1-2，4-7，9-11
A	EP 2819346 A1 (KASPERSKY LAB ZAO) 2014年 12月 31日 (2014-12-31) 说明书第3、7-13、17-18、38-48、58段，图1-5	3，8
A	CN 102341808 A (皇家飞利浦电子股份有限公司) 2012年 2月 1日 (2012-02-01) 全文	1-11
A	WO 2015040456 A1 (ERICSSON TELEFON AB L M) 2015年 3月 26日 (2015-03-26) 全文	1-11

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2016年 5月 31日	2016年 6月 21日

ISA/CN的名称和邮寄地址	受权官员
中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088	任玲
传真号 (86-10)62019451	电话号码 (86-10)62088423

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2016/078990

检索报告引用的专利文件			公布日（年/月/日）	同族专利			公布日（年/月/日）
EP	2819346	A1	2014年 12月 31日	RU	2013129544	A	2015年 1月 10日
				US	2015007252	A1	2015年 1月 1日
				US	8943547	B2	2015年 1月 27日
CN	102341808	A	2012年 2月 1日	WO	2010100590	A1	2010年 9月 10日
				EP	2404259	A1	2012年 1月 11日
				US	2011321122	A1	2011年 12月 29日
				JP	2012519893	A	2012年 8月 30日
				IN	201106738	P4	2012年 11月 16日
WO	2015040456	A1	2015年 3月 26日		无		