OPENCHAIN

OpenChain 规范

1.2 版

内容

This is an official translation from the OpenChain Project. It has been translated from the original English text. In the event there is confusion between this translation and the English version, The English text shall take precedence.

本文档为 OpenChain 项目的官方翻译，从原始的英文版本翻译而来。如果本文档跟英文版本有不一致的地方，以英文版本为准。

1) 介绍

OpenChain 促进会始于 2013 年，当时一群开源软件供应链的从业者注意到两种新出现的情况：1) 开源合规方案管理比较成熟的组织间的重要流程是基本相似的；2) 仍然有大量的组织采用不太成熟的方案来进行软件的交换。后者会导致对所交换软件的合规管理在一致性和质量上缺乏信任。因此，在软件供应链的每一层，下游组织经常重复上游组织已经执行过的合规工作。

一个研究团队开始成立，目标是创建一份标准规范，以用于 i) 促进提高整个工业界内共享的开源信息的高质量和一致性；ii) 降低由于开源合规工作中的重复劳动而产生的高交易成本。该研究团队发展成为一个工作组，并于 2016 年 4 月，正式成为 Linux 基金会旗下的协作项目。

OpenChain 促进会的愿景和使命如下：

- **愿景**: 一个传递开源软件（FOSS）时附随可信和一致性合规信息的软件供应链。

- **使命**: 为软件供应链从业者建立有效管理开源软件的要求，并使得来自软件供应链的厂商，开源社区，学术界的代表们，能够开放并协力的完善本要求和相关文档。

根据愿景和使命，本规范定义了一系列的要求，尽管不能确保满足所有规范要求的方案完全合规；但如果满足这些要求，将大大提高该开源合规方案达到足够高质量，一致性和完整性水平的可能性。这些要求定义了被认为满足 OpenChain 合规要求的基础等级（最小）要求的一个方案。本规范聚焦于开源合规方案的“是什么”和“为什么”，而不是考虑“如何”和“何时”。这将确保实际操作的灵活度，使得不同的组织能够定制跟他们目标最符合的政策和流程。

第二章节介绍了整个规范所使用的关键术语的定义。第三章节提供了规范要求，每个要求都有一个或多个核查材料的列表。它们代表了满足某项要求所必须存在的证据。如果一个给定方案满足了所有要求，它将被认为是遵循 OpenChain 规范 1.2 版的规范。核查材料并不被指定公开，但是可以根据保密协议或者 OpenChain 组织的私下请求来提供，以核查合规性。

有关如何解释规范的更多说明，可以查看 FAQ：
https://www.openchainproject.org/specification-faq

2) 定义

合规材料 - 对于一个向第三方提供的软件版本进行开源软件管理所输出的所有材料的集合，该集合可包括（但不限于）以下一项或者多项：源代码，归属通知，版权声明，许可证副本，修改通知，书面报价，开源组件清单，SPDX 文档等。

开源软件 (自由开源软件) - 使用一个或者多个许可证的软件，这些许可证符合 OSI（opensource.org）组织发布的开源软件定义或者自由软件定义（由自由软件基金会发布）或类似条款。

开源软件联系人 - 被指派接受外部开源软件垂询的人员。

已经确认的许可证 - 遵循软件供应管理的适当方法而确认的一组开源许可证。

OpenChain 合规方案 - 满足本规范所有要求的方案。

软件工作人员 - 定义，贡献或负责准备软件供应的任何员工或者承包商。根据组织的不同，这可能包括（但不限于）软件开发人员，发布工程师，质量工程师，产品营销和产品管理人员。

SPDX or Software Package Data Exchange - SPDX 工作组为交换给定软件包的许可证和版权信息而创建的格式标准。SPDX 规范的描述可以在 www.spdx.org 找到。

提供的软件 - 一个组织提供给第三方（例如其他组织或者个人）的软件。

核查材料 - 为了使某一个特定要求被确认符合而必须存在的证据。

3) 要求

目标 1: 了解你的开源责任

1.1 **存在一份书面的开源软件政策，该政策用于管理所提供开源软件分发的合规性。该政策必须在内部传达。**

核查材料:

- ☐ 1.1.1 存在一份有记录的开源管理政策文档。
- ☐ 1.1.2 存在一份有记录的流程，用于让软件员工知晓该开源管理政策（例如培训，内部 Wiki 或者其他实际可行的传达方式）。

理由:

确保采取步骤来制定和记录政策，并使得软件工作人员认识到该开源管理政策的存在。虽然此处没有对政策中包含的内容提出任何要求，但是其他章节可能会对内容提出要求。

1.2 **对公司内所有软件工作人员进行强制性的开源管理培训:**

- **培训至少涵盖如下主题:**
  - **开源管理政策及从哪里找到副本;**
  - **关于开源和开源软件许可证的知识产权法基础知识;**
  - **开源软件许可证的概念（包括宽松的和 Copyleft 许可证）**
  - **开源软件项目的许可证模式**
  - **软件工作人员在遵守开源政策方面的具体角色和职责，和开源软件的一般性政策**
  - **用于在所提供的软件中识别，记录和/或跟踪开源组件的流程**
- **软件工作人员必须在过去 24 个月内完成开源管理培训，才能被视为最新培训（“最新受训”）。可以使用测试软件使软件工作人员满足培训要求。**

核查材料:

- ☐ 1.2.1 开源培训材料必须涵盖如上主题（例如幻灯片、线上课程或者其他培训资料）。
- ☐ 1.2.2 跟踪软件工作人员完成培训的有记录的方法。
- ☐ 1.2.3 根据如上定义，至少 85%的软件工作人员接受过最新培训。85%不一定指整个组织，而是指涉及到 OpenChain 开源合规工作的员工。

理由:

确保软件工作人员参加了最新的开源软件培训，并确保该培训内容涵盖一套相关的开源软件核心主题。这样做的目的是为了确保涵盖一套核心基础级别的主题，但是典型的培训计划可能比这里要求的更全面。

1.3 **存在一个检查已确认的软件许可证的流程，以确定每个开源许可证所授予的义务，限制和权利。**

核查材料:

- 1.3.1 存在一份有记录的流程，用于检查和存档每一个被确认的开源许可证授予的义务，限制和权利

理由:

确保在已经确认的软件许可证的各种使用案例中，存在一个流程，用于审查和确认每个软件许可证的义务。

目标 2: 合规的责任分配

2.1 确认开源软件联系人的职责

- **指派负责接受外部开源软件垂询的联系人；**
- **该开源软件联系人必须做出商业上合理的努力，酌情答复开源软件合规的垂询；并且**
- **公示他人可联络到该开源软件联系人的联络方式**

核查材料：

- ☐ 2.1.1 开源软件联系人的身份对外公示（例如通过公开的邮件地址，或者 Linux 基金会的开放合规名录）
- ☐ 2.1.2 一份内部文件流程，分配接收开源软件合规垂询的责任

理由：

确保第三方有适当方式就开源软件合规垂询与该组织联系，并确保该责任已经被有效分配。

2.2. 确认内部合规角色

- **指派个人负责管理内部开源软件合规。开源合规角色和开源软件联系人可以是同一个人。**
- **开源软件合规管理活动资源充足**
  - **分配了履行该职责的时间并且**
  - **分配了商业上合理的预算**
- **分配开发和维护开源合规政策和流程的责任**
- **跟开源合规相关的法律专家，可为开源软件合规角色提供支持（例如：内部或者外部专家）；和**
- **存在一个解决开源合规问题的流程**

核查材料：

- ☐ 2.2.1 内部确定开源合规角色中的人员，团体或者职能的名称
- ☐ 2.2.2 确定开源合规可利用的内部或外部法律专家
- ☐ 2.2.3 存在一份有记录的流程，用于开源合规分配内部责任
- ☐ 2.2.4 存在一份有记录的流程，用于处理不合规案例的审查和补救

理由：

确保内部开源合规职责已经被有效的分配。

目标 3:审查及批准开源软件内容

3.1 存在一个流程用于创建和管理开源组件清单，该清单包括所提供软件中的每个开源组件（和它已确认的许可证）

核查材料

- 3.1.1 A 一个有记录的流程，用于识别，跟踪和归档所提供软件中的开源组件集合的信息
- 3.1.2 每个所提供软件的版本都有开源组件记录，以证明该流程被正确的执行

理由：

确保存在一个流程，用于创建和管理该软件包含的开源组件清单。该清单用于支持对每个组件的许可证条款进行系统审查，以了解适用于所提供软件分发的义务和限制内容。

3.2. 开源管理方案必须能够处理软件工作人员在提供软件时一般会碰到的通用的许可证使用案例，其中可能包括如下案例（请注意，该列表并非详尽无遗，也可能不适用于所有案例）

- **以二进制形式进行发布；**
- **以源码形式进行分发；**
- **以其他可能触发 CopyLeft 义务要求的开源软件集成；**
- **包含修改过的开源软件；**
- **包含与该软件许可证不兼容的开源和/或其他软件；**
- **包含归属标示要求的开源软件**

核查材料：

- 3.2.1 一份有记录的流程，用于处理该软件中常见的开源许可证使用案例

理由：

确保该方案能够充分处理一个组织中常见的开源许可证案例。存在一个支持这个活动的流程，并被执行。

目标 4: 发布开源内容文档和相关资料

4.1 存在为每个提供的软件版本创建一组合规性材料的流程

核查材料：

- 4.1.1. 一个有记录的流程，确保按照确认许可证的要求进行准备和分发的合规性材料随该软件一并分发

- 4.1.2 已提供软件版本的合规性材料的副本将存档并易于检索，并且计划至少在提供的软件期间或已确定许可证要求的期间(以时间较长者为准) 存在存档

理由：

确保按照“已识别的软件”的要求，完整的收集合规性材料和在开源软件审查过程中创建的其他报告。

目标 5: 理解开源社区的参与

5.1 有一项书面政策来管理该组织对开源软件项目的贡献，该政策必须在内部传达。

核查材料：

- 5.1.1 一份有记录的开源贡献政策；
- 5.1.2 一份有记录的流程，使得所有软件工作人员都知道开源软件贡献政策的存在（例如，通过培训，内部 Wiki 或者其他实用的沟通方式）

理由：

确保一个组织合理考虑制定一项关于公开贡献开源的政策。该开源贡献政策可以是该组织整个开源政策的一部分，也可以是独立的政策。在贡献被限制或者不允许的情况下，应该制定明确立场的政策。

5.2. 如果一个组织允许开源贡献，那么就有一个流程来执行第 5.1 节概述的开源贡献政策

核查材料：

- 5.2.1 如果开源贡献政策允许贡献，则需要有一个有记录的流程用于管理开源贡献

理由：

确保组织有一个有记录的流程，来了解组织如何进行开源贡献。可能存在一种政策，即不允许贡献，在这种情况下，可以理解的是，不存在任何流程，但仍然满足这一要求。

目标 6: 根据 OpenChain 要求进行认证

6.1 为了使组织获得 OpenChain 的认证，它必须确认其有一个开源管理方案，该方案符合 OpenChain 规范 1.2 版中描述的要求

核查材料：

- 6.1.1 确认存在一个开源软件管理方案，满足 OpenChain 规范 1.2 版中所有的要求

理由：

确保如果某组织申明其有一个遵守 OpenChain 标准的方案，那么该方案已满足该规范的所有要求。仅仅满足这些要求的一部分是不够的。

6.2. 符合此版本规范将从完成一致性验证之日起持续 18 个月。一致性验证的要求可以在 OpenChain 项目的网站上找到。

核查材料：

- 6.2.1 在实现一致性验证的 18 个月内，该组织确认存在一个开源管理方案，该方案满足 OpenChain 规范 1.2 版的所有要求。

理由：

如果一个组织希望持续宣称与 OpenChain 方案一致，那么该组保持与规范的同步是十分必要的。如果他们想持续宣称与此规范具一致性，此要求确保该方案的支持流程和控制不会慢慢弱化。

附录：其他语言版本

为了促进全球采用, 我们欢迎将该规范翻译为多种语言的努力。由于 OpenChain 是一个开源项目，翻译是由那些愿意贡献自己的时间和专业知识，并根据 CC-BY 4.0 许可证和该项目的翻译政策进行翻译的人推动的。 该政策和现有翻译的详细信息可在 OpenChain 项目规范网页上找到.