OPENCHAIN

OpenChain Specification

Version 1.1

コメントの追加 [N1]: 「Conformance」が削除された。各ページのヘッダおよびフッタの表記も変更。

Contents

Disclaimer

本文書は、The Linux Foundation における OpenChain プロジェクトの英文ドキュメントから翻訳された公式翻訳版です。翻訳版と英語版との間で何らかの意味の違いがあった場合には、英語版が優先されます。

また、OpenChain は世界中のメンバー企業が参加するプロジェクトではありますが、資料の細部では必ずしも各国の法令を検討していない可能性もあります。本翻訳資料を日本で活用する際には、各企業の法務部門を加えた検討が不可欠です。

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 a translation and the English version, The English text shall take precedence.

Copyright and License

コメントの追加 [N2]: 「specification」から修正

コメントの追加 [N3]: 追記された

1) Introduction

The OpenChain Initiative began in 2013 when a group of software supply chain open source practitioners observed two emerging patterns: 1) significant process similarities existed among organizations with mature open source compliance programs; and 2) there still remained a large number of organizations exchanging software with less developed programs. The latter observation resulted in a lack of trust in the consistency and quality of the compliance artifacts accompanying the software being exchanged. As a consequence, at each tier of the supply chain, downstream organizations were frequently redoing the compliance work already performed by other upstream organizations.

A study group was formed to consider whether a standard program specification could be created that would: i) facilitate greater quality and consistency of open source compliance information being shared across the industry; and ii) decrease the high transaction costs associated with open source resulting from compliance rework. The study group evolved into a work group, and in April 2016, formally organized as a Linux Foundation collaborative project.

The Vision and Mission of the OpenChain Initiative are as follows:

- **Vision**: A software supply chain where free/open source software (FOSS) is delivered with trustworthy and consistent compliance information.
- **Mission**: Establish requirements to achieve effective management of free/open source software (FOSS) for software supply chain participants, such that the requirements and associated collateral are developed collaboratively and openly by representatives from the software supply chain, open source community, and academia.

In accordance with the Vision and Mission, this specification defines a set of requirements that if met, would significantly increases the probability that an open source compliance program had achieved a sufficient level of quality, consistency and completeness; although a program that satisfies all the specification requirements does not guarantee full compliance. The requirements represent a base level (minimum) set of requirements a program must satisfy to be considered OpenChain Conforming. The specification focuses on the “what” and “why” qualities of a compliance program as opposed to the “how” and “when” considerations. This ensures a practical level of flexibility that enables different organizations to tailor their policies and processes to best fit their objectives.

Section 2 introduces definitions of key terms used throughout the specification. Section 3 presents the specification requirements where each one has a list of one or more Verification Artifacts. They represent the evidence that must exist in order for a given requirement to be considered satisfied. If all the requirements have been met for a given program, it would be considered OpenChain Conforming in accordance with version 1.1 of the specification. Verification Artifacts are not intended to be public, but could be provided under NDA or upon private request from the OpenChain organization to validate conformance.

コメントの追加 [N4]: 「trusted」から変更

コメントの追加 [N5]: 「1.0」から変更

コメントの追加 [N6]: 新規に追加

2) Definitions

FOSS (Free and Open Source Software) - software subject to one or more licenses that meet the Open Source Definition published by the Open Source Initiative (OpenSource.org) or the Free Software Definition (published by the Free Software Foundation) or similar license.

FOSS Liaison - a designated person who is assigned to receive external FOSS inquires.

Identified Licenses - a set of FOSS licenses identified as a result of following an appropriate method of identifying such licenses.

OpenChain Conforming - a program that satisfies all the requirements of this specification.

Software Staff - any employee or contractor that defines, contributes to or has responsibility for preparing Supplied Software. Depending on the organization, that may include (but is not limited to) software developers, release engineers, quality engineers, product marketing and product management.

SPDX or Software Package Data Exchange - the format standard created by the SPDX Working Group for exchanging license and copyright information for a given software package. A description of the SPDX specification can be found at www.spdx.org.

Supplied Software - software that an organization delivers to third parties (e.g., other organizations or individuals).

Verification Artifacts - evidence that must exist in order for a given requirement to be considered satisfied.

コメントの追加 [N7]: 文言は Specv1.0 から変化なし。ただし、用語の順番が変わっている。

コメントの追加 [N8]: Spec v1.0 では「ww.spdx.org」(wが二つだけ)だったところが修正された。

3) Requirements

G1: Know Your FOSS Responsibilities

1.1 **A written FOSS policy exists that governs FOSS license compliance of the Supplied Software distribution.** The policy must be internally communicated.

Verification Artifact(s):

1.1.1 A documented FOSS policy exists.

1.1.2 A documented procedure exists that makes all Software Staff aware of the existence of the FOSS policy (e.g., via training, internal wiki, or other practical communication method).

Rationale:

Ensure steps were taken to create, record and make Software Staff aware of the existence of a FOSS policy. Although no requirements are provided here on what should be included in the policy, other sections may impose requirements on the policy.

1.2 **Mandatory FOSS training for all Software Staff exists such that:**

- **The training, at a minimum, covers the following topics:**
  - **The FOSS policy and where to find a copy;**
  - **Basics of Intellectual Property law pertaining to FOSS and FOSS licenses;**
  - **FOSS licensing concepts (including the concepts of permissive and copyleft licenses);**
  - **FOSS project licensing models;**
  - **Software Staff roles and responsibilities pertaining to FOSS compliance specifically and the FOSS policy in general; and**
  - **Process for identifying, recording and/or tracking of FOSS components contained in Supplied Software.**
- **Software Staff must have completed FOSS training within the last 24 months (to be considered current). A test may be used to allow Software Staff to satisfy the training requirement.**

Verification Artifact(s):

1.2.1 FOSS training materials covering the above topics exists (e.g., slide decks, online course, or other training materials).

1.2.2 Method of tracking the completion of the training for all Software Staff.

1.2.3 At least 85% of the Software Staff are current, as per the definition in above section.

Rationale:

Ensure the Software Staff have recently attended FOSS training and that a core set of relevant FOSS topics are covered. The intent is to ensure a core base level set of topics are covered but a typical training program would likely be more comprehensive than what is required here.

1.3 **A process exists for reviewing the Identified Licenses to determine the obligations, restrictions and rights granted by each license.**

Verification Artifact(s):

1.3.1 A documented procedure exists to review and document the obligations, restrictions and rights granted by each Identified License governing the Supplied Software.

Rationale:

コメントの追加 [N9]: 「as a minimum, it must be…」から変更

コメントの追加 [N10]: 表現が変更されている。以前は「other requirements in other sections may.」だった。

コメントの追加 [N11]: 「as」から変更

コメントの追加 [N12]: 「IP」（略号）から変更

To ensure a process exists for reviewing and identifying the license obligations for each Identified License for the various use cases.

コメントの追加 [N13]: 1.3 節全部が新たに追加された。

G2: Assign Responsibility for Achieving Compliance

2.1 Identify FOSS Liaison Function ("FOSS Liaison").

- **Assign individual(s) responsible for receiving external FOSS inquiries;**
- **FOSS Liaison must make commercially reasonable efforts to respond to FOSS compliance inquiries as appropriate; and**
- **Publicly identify a means by which one can contact the FOSS Liaison.**

Verification Artifact(s):

2.1.1 FOSS Liaison function is publicly identified (e.g., via a published contact email address, or the Linux Foundation's Open Compliance Directory).

2.1.2 An internal documented procedure exists that assigns responsibility for receiving FOSS compliance inquiries.

Rationale:

Ensure there is a reasonable way for third parties to contact the organization with regard to FOSS compliance inquiries and that this responsibility has been effectively assigned.

2.2 Identify Internal FOSS Compliance Role(s).

- **Assign individual(s) responsible for managing internal FOSS compliance. The FOSS Compliance role and the FOSS Liaison may be the same individual.**
- **FOSS compliance management activity is sufficiently resourced:**
  - **Time to perform the role has been allocated; and**
  - **Commercially reasonable budget has been allocated.**
- **Assign responsibilities to develop and maintain FOSS compliance policy and processes;**
- **Legal expertise pertaining to FOSS compliance is accessible to the FOSS Compliance role (e.g., could be internal or external); and**
- **A process exists for the resolution of FOSS compliance issues.**

Verification Artifact(s):

2.2.1 Name of persons, group or function in FOSS Compliance role(s) internally identified.

2.2.2 Identify source of legal expertise available to FOSS Compliance role(s) which could be internal or external.

2.2.3 A documented procedure exists that assigns internal responsibilities for FOSS compliance.

2.2.4 A documented procedure exists for handling the review and remediation of non-compliant cases.

Rationale:

Ensure certain FOSS responsibilities have been effectively assigned.

コメントの追加 [N14]: 表現が変更。Spec v1.0 では「means of contacting the FOSS Liaison by way of electronic communication.」

コメントの追加 [N15]: 「and/or」から修正された

コメントの追加 [N16]: 追加された

コメントの追加 [N17]: 「and」以降が追加された

コメントの追加 [N18]: インデントが下がった

コメントの追加 [N19]: インデントが下がった

コメントの追加 [N20]: 文面変更 v1.0 では「Escalation path is available for resolution of FOSS compliance issues.」

コメントの追加 [N21]: 追加された

コメントの追加 [N22]: 文面が変更。V1.0 は「exists that identifies an escalation path for issue resolution.」

G3: Review and Approve FOSS Content

3.1 A process exists for creating and managing a FOSS component bill of materials which includes each component (and its Identified Licenses) in a Supplied Software release.

Verification Artifact(s):

3.1.1 A documented procedure exists for identifying, tracking and archiving information about the collection of FOSS components from which a Supplied Software release is comprised.

3.1.2 FOSS component records exist for each Supplied Software release which demonstrates the documented procedure was properly followed.

Rationale:

To ensure a process exists for creating and managing a FOSS component bill of materials used to construct the Supplied Software. A bill of materials is needed to support the systematic review of each component's license terms to understand the obligations and restrictions as it applies to the distribution of the Supplied Software.

3.2 The FOSS management program must be capable of handling common FOSS license use cases encountered by Software Staff for Supplied Software, which may include the following use cases (note that the list is neither exhaustive, nor may all of the use cases apply):

- **distributed in binary form;**
- **distributed in source form;**
- **integrated with other FOSS such that it may trigger copyleft obligations;**
- **contains modified FOSS;**
- **contains FOSS or other software under an incompatible license interacting with other components within the Supplied Software; and/or**
- **contains FOSS with attribution requirements.**[1]

Verification Artifact(s):

3.2.1 A procedure has been implemented that handles the common FOSS license use cases for the FOSS components of each Supplied Software release.

Rationale:

To ensure the program is sufficiently robust to handle an organization's common FOSS license use cases. That a procedure exists to support this activity and that the procedure is followed.

コメントの追加 [N23]: 大幅文面変更。Spec v1.0 では「A process exists for identifying, tracking and archiving a list of all FOSS components (and their respective Identified Licenses) from which Supplied Software is comprised.」

コメントの追加 [N24]: 全面変更。Spec v1.0 では「A documented procedure exists used to identify, track, and archive a list of FOSS components and their Identified Licenses from which the Supplied Software is comprised.」

コメントの追加 [N25]: 本節は新たに追加。

コメントの追加 [N26]: 全面変更。Sec v1.0 では「To ensure a process exists for identifying and listing all FOSS components used to construct the Supplied Software. This inventory must exist to support the systematic review of each component's license terms to understand their respective distribution obligations and restrictions applicable to the Supplied Software. The recorded inventory also serves as evidence that the process was followed.」

コメントの追加 [N27]: 追加された。

コメントの追加 [N28]: 「typical」から変更された。

コメントの追加 [N29]: 表現変更。Spec v1.0 では「nor may all of the below use cases apply depending on the organization」

コメントの追加 [N30]: 「are distributed」から変更。

コメントの追加 [N31]: 「are distributed」から変更。

コメントの追加 [N32]: 「are integrated」から変更。

コメントの追加 [N33]: 追加された。

コメントの追加 [N34]: 表現が変更された。Spec v1.0 では「implemented that is capable of addressing the typical FOSS use cases encountered by Software Staff for Supplied Software.」

コメントの追加 [N35]: 変更。Spec v1.0 では「To cause the FOSS program」

コメントの追加 [N36]: 変更。Spec v1.0 では「address」

コメントの追加 [N37]: 変更された。Spec v1.0 では「typical use cases as a result of that organization's business practices.」

コメントの追加 [N38]: 一文まるごと新規追加された。

[1] （Wikipedia「帰属」より引用）「ある著作物（works）を利用（use）する場合、その著作物の著作者への謝辞（acknowledge）やクレジットの掲載を要求することを指す用語である。または別の著作物に表示すること（appear in works）自体を指す。」

G4: Deliver FOSS Content Documentation and Artifacts

4.1 **Prepare the set of artifacts which represent the output of the FOSS management program for each Supplied Software release. This set is referred to as the Compliance Artifacts which may include (but are not limited to) one or more of the following: source code, attribution notices, copyright notices, copy of licenses, modification notifications, written offers[2], SPDX documents and so forth.**

Verification Artifact(s):

4.1.1 A documented procedure exists that ensures the Compliance Artifacts are prepared and distributed with Supplied Software release as required by the Identified Licenses.

4.1.2 Copies of the Compliance Artifacts of the Supplied Software release are archived and easily retrievable, and the archive is planned to exist for at least as long as the Supplied Software is offered or as required by the Identified Licenses (whichever is longer)

Rationale:

Ensure the complete collection of Compliance Artifacts accompany the Supplied Software as required by the Identified Licenses that govern the Supplied Software along with other reports created as part of the FOSS review process.

コメントの追加 [N39]: Spec v1.0 から構造が大きく変更されている。

コメントの追加 [N40]: 文面大幅変更。Specv1.0 では、以下のような構造。

4.1 . Prepare the following Distributed Compliance Artifacts to accompany the Supplied Software as required by the corresponding Identified Licenses which might include (but is not limited to) the required:

- . copyright notices
- . copies of Identified Licenses
- . modification notifications
- . attribution notices
- . prominent notices
- . source code
- . required build instructions and scripts
- . written offers

コメントの追加 [N41]: 変更。Spec v1.0 では「exists describing a process that ensures the Distributed Compliance Artifacts be distributed with」

コメントの追加 [N42]: 変更あり。Spec v1.0 では「Distributed Compliance Artifacts」

コメントの追加 [N43]: この後のカッコ書きが削除された。Spec v1.0 では「retrievable (e.g., legal notices, source code, SPDX documents)」

コメントの追加 [N44]: 固有名詞化（語頭を大文字で表現）。Spec v1.0 では「compliance artifacts」

コメントの追加 [N45]: 新たに追加。

[2] 「書面による申し出（Written Offer）」について、GPL ライセンスを例に gnu.org の記述を参照（以下引用）。「GPL には、バイナリをソースコード抜きで商業的に配布する場合、あなたが後にソースコードを配布する旨が書かれた**書面による申し出**を提供しなければならないとあります。ユーザがあなたから受け取ったバイナリを非商業的に再配布するときには、この書面による申し出の複製を一緒に渡さなければなりません。これは、バイナリを直接あなたから入手しなかった人々も、書面による申し出に則してソースコードの複製を受け取ることができるということを意味します。」

G5: Understand FOSS Community Engagement

5.1 A written policy exists that governs contributions to FOSS projects by the organization. The policy must be internally communicated.

Verification Artifact(s):

5.1.1 A documented FOSS contribution policy exists;

5.1.2 A documented procedure exists that makes all Software Staff aware of the existence of the FOSS contribution policy (e.g., via training, internal wiki, or other practical communication method).

Rationale:

Ensure an organization has given reasonable consideration to developing a policy with respect to publicly contributing to FOSS. The FOSS contribution policy can be made a part of the overall FOSS policy of an organization or be its own separate policy. In the situation where contributions are not permitted at all, a policy should exist making that position clear.

5.2 If an organization permits contributions to FOSS projects then a process must exist that implements the FOSS contribution policy outlined in Section 5.1.

Verification Artifact(s):

5.2.1 Provided the FOSS contribution policy permits contributions, a documented procedure exists that governs FOSS contributions.

Rationale:

Ensure an organization has a documented process for how the organization publicly contributes FOSS. A policy may exist such that contributions are not permitted at all. In that situation it is understood that no procedure may exist and this requirement would nevertheless be met.

コメントの追加 [N46]: 文面が大幅に簡素化。Spec v1.0 では以下。

5.2 。Provided the FOSS contribution policy permits such contributions, a process exists for confirming contributions adhere to the FOSS contribution policy, which might include (but is not limited to) the following considerations:
・ 。legal approval for license considerations
・ 。business rationale or approval
・ 。technical review of code to be contributed
・ 。community engagement and interaction, including a project's Code of Conduct or equivalent
・ 。adherence to project-specific contribution requirements

コメントの追加 [N47]: 表現変更。Spec 1.0 では「exists that describes the FOSS contribution process.」

コメントの追加 [N48]: Spec v1.0 では「specific situation」だった。

G6: Certify Adherence to OpenChain Requirements

6.1 In order for an organization to be OpenChain certified, it must affirm that it has a FOSS management program that meets the criteria described in this OpenChain Specification version 1.1.

Verification Artifact(s):

6.1.1 The organization affirms that a FOSS management program exists that meets all the requirements of this OpenChain Specification version 1.1.

Rationale:

To ensure that if an organization declares that it has a program that is OpenChain Conforming, that such program has met all the requirements of this specification. The mere meeting of a subset of these requirements would not be considered sufficient to warrant a program be OpenChain certified.

6.2 Conformance with this version of the specification will last 18 months from the date conformance validation was achieved. Conformance validation requirements can be found on the OpenChain project's website.

Verification Artifact(s):

6.2.1 The organization affirms that a FOSS management program exists that meets all the requirements of this OpenChain Specification version 1.1 within the past 18 months of achieving conformance validation.

Rationale:

It is important for the organization to remains current with the specification if they want to assert program conformance overtime. This requirement ensures that the program's supporting processes and controls do not erode if they want to continue to assert conformance with the specification overtime.

コメントの追加 [N49]: 追加された。

コメントの追加 [N50]: Spec v1.0 では「OpenChain Conformance Specification」だった。

コメントの追加 [N51]: 「version 1.0」からアップデート。

コメントの追加 [N52]: 新たに追加。

コメントの追加 [N53]: Spec v1.0 では「OpenChain Conformance Specification」だった。

コメントの追加 [N54]: 「version 1.0」からアップデート

コメントの追加 [N55]: 本節が新たに追加された。

Appendix I: Language Translations

To facilitate global adoption we welcome efforts to translate the specification into multiple languages. Because OpenChain functions as an open source project translations are driven by those willing to contribute their time and expertise to perform translations under the terms of the CC-BY 4.0 license and the project's translation policy. The details of the policy and available translations can be found on the OpenChain project specification webpage.

コメントの追加 [N56]: 新たに新設。（Appendix 全部）