

**OpenChain Specification**

Version 1.1

**目次**

[免責事項（Disclaimer） 3](#_Toc480816633)

[著作権、ライセンス 3](#_Toc480816634)

[はじめに 4](#_Toc480816635)

[用語の定義 5](#_Toc480816636)

[満たすべき要件 6](#_Toc480816637)

[G1: FOSSに関わる責任の理解 6](#_Toc480816638)

[G2: コンプライアンスを履行するための責任者のアサイン 7](#_Toc480816639)

[G3: FOSSコンテンツのレビューと承認 8](#_Toc480816640)

[G4: FOSSコンテンツ ドキュメントとコンプライアンス関連資料の頒布 9](#_Toc480816641)

[G5: FOSSコミュニティへの（積極的な）関わり方の理解 10](#_Toc480816642)

[G6: OpenChain要件適合の認定 11](#_Toc480816643)

# 免責事項（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.

# 著作権、ライセンス

Copyright © 2016-2017 Linux Foundation. This document is licensed under the Creative Commons Attribution 4.0 International (CC-BY 4.0) license. A copy of the license can be found at <https://creativecommons.org/licenses/by/4.0/> .

# 1)はじめに

OpenChain イニシアチブは2013年に開始されました。当時ソフトウェア サプライチェーンでオープンソースを活用していた実務者グループは、オープンソース コンプライアンスに関して2つのパターンを見出していました。それは、1）成熟したオープンソース コンプライアンス プログラムを持つ組織のプロセスには顕著な類似性があること、および、2）いまだに多くの組織が遅れたコンプライアンス プログラムでソフトウェアをやりとりしていること、です。後者の実態は、やりとりするソフトウェアに付随したコンプライアンス関連資料の一貫性や品質に対する信頼を喪失させました。そしてその結果、サプライチェーンの各段階で、上流側組織が既に実行したコンプライアンス業務を下流側組織が頻繁に再実行していました。

こうした背景から、標準的なコンプライアンス プログラムの仕様書を整備できるかどうかを検討する研究グループが形成されました。この仕様書は、i）業界全体で共有されるオープンソース コンプライアンス関連情報の品質と一貫性の向上促進、および、ii）コンプライアンス作業の再実施に起因するオープンソース関連の作業コストの低減、を実現するものです。本グループはワーキング グループへと発展し、その後2016年4月に正式にLinux Foundation協業プロジェクトとして組織されました。こうした背景から、標準的なコンプライアンス プログラムの仕様書を整備できるかどうかを検討する研究グループが形成されました。この仕様書は、i）業界全体で共有されるオープンソース コンプライアンス関連情報の品質と一貫性の向上促進、および、ii）コンプライアンス作業の再実施に起因するオープンソース関連の作業コストの低減、を実現するものです。本グループはワーキング グループへと発展し、その後2016年4月に正式にLinux Foundation協業プロジェクトとして組織されました。

OpenChainイニシアチブのビジョンとミッションは以下のとおりです。

* **Vision**: A software supply chain where free/open source software (FOSS) is delivered with trustworthy and consistent compliance information.
* **ミッション：FOSSの効果的マネジメントを実現するための要件をソフトウェア サプライチェーンに参加する人々のために確立すること。このような要件やそれらに関連する付帯事項については、ソフトウェア サプライチェーン、オープンソース コミュニティ、および学術研究機関の代表者らがオープンに協働しながら開発を進める。**

上記のビジョンとミッションに則り、本仕様書では一連の要件を定義しています。これらを満たすことで、オープンソース コンプライアンス プログラムの品質、一貫性、および完全性が十分なレベルに到達する可能性が大きく高まります。ただし、本要件のすべてを満たしても、そのプログラムが全面的にコンプライアンスを履行していることを保証するものではありません。本要件は、そのコンプライアンス プログラムがOpenChainに適合しているとみなされるために満足しなければならない基本レベル（最低限）の要件一式を提示するものです。本仕様書は、コンプライアンス プログラムの「何（What）」や「なぜ（Why）」の属性に焦点をあてており、「どのように（How）」や「いつ（When）」といった考慮点には言及していません。このため実用的レベルで柔軟性があり、さまざまな組織が自社の目的に最適なポリシーやプロセスを作成することができます。

第2節では、本資料全般で用いられる重要用語について定義します。第3節では、仕様としての要件を示します。それぞれに1つ以上の「 検証すべき証跡（Verification Artifact）」があります。これらは示された要件が満たされているかどうかを確認するために存在しなくてはならない確証としての役割を果たしています。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.

# 2)用語の定義

**FOSS（フリー／オープンソース ソフトウェア）－Open Source Initiative（OpenSource.org）によって公開されているオープンソースの定義や（Free Software Foundationによって公開されている） フリー ソフトウェアの定義に該当または類似したライセンスの1つもしくはそれ以上に従うソフトウェアのこと。**

**FOSS 窓口（FOSS Liaison）－FOSSに関し、外部からの問い合わせに対応するためにアサインされた担当者のこと。**

**確認ライセンス（Identified License）－適切なライセンス確認手順の結果として存在の確認ができた一連のFOSSライセンスのこと。**

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

**ソフトウェア スタッフ－供給ソフトウェアについて、定義し、コントリビュートし、もしくは使えるよう準備する責任を持つ従業員や契約者のこと。組織によって異なるが、ソフトウェア開発者、リリース エンジニア、品質管理技術者、プロダクト マーケティング担当者、プロダクト管理者などが含まれる（ただし、この限りではない）。**

**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).

**検証すべき証跡（Verification Artifact）－与えられた要件を満足しているとみなされるために存在しなければならない確証のこと。**

# 3)満たすべき要件

## G1: FOSSに関わる責任の理解

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

#### 検証すべき証跡：

* 1. 文書化されたFOSS ポリシーが存在する。
  2. すべてのソフトウェア スタッフが（トレーニングや社内wiki、その他実践的なコミュニケーションを通じて）FOSSポリシーの存在を知ることのできる文書化された手続きが存在する。

#### 論拠:

FOSSポリシーを作成・記録するステップが取られ、ソフトウェア スタッフにFOSSポリシーの存在を知らせることを確かなものにします。Although no requirements are provided here on what should be included in the policy, other sections may impose requirements on the policy.

### すべてのソフトウェア スタッフに対して、受講必須のトレーニングが存在すること。

* **The training, at a minimum, covers the following topics:**
* **FOSSポリシーおよびそれがどこで見つけられるか**
* **Basics of Intellectual Property law pertaining to FOSS and FOSS licenses;**
* **FOSSライセンスの概念（コピーレフト ライセンスやパーミッシブなライセンスの概念など）**
* **FOSSプロジェクトのライセンス供与のモデル**
* **FOSSコンプライアンスに具体的に関係し、FOSSポリシー全般に関係するソフトウェア スタッフの役割と責任**
* **供給ソフトウェアのFOSSコンポーネントを特定、記録、および追跡するためのプロセス**
* **ソフトウェア スタッフは、FOSSトレーニングを過去24か月以内に（最新の状況に即すとみなされるよう）修了していること。ソフトウェア スタッフがトレーニング要件を満たしていることを認めるために試験を実施する場合もある。**

#### 検証すべき証跡：

* + - 1. FOSS training materials covering the above topics exists (e.g., slide decks, online course, or other training materials).
      2. Method of tracking the completion of the training for all Software Staff.
      3. At least 85% of the Software Staff are current, as per the definition in above section.

#### 論拠:

ソフトウェア スタッフが最新のFOSSトレーニングに参加したこと、およびそのトレーニングでFOSS関連の適切なトピックが取り扱われていることを確かなものにします。ここで意図しているのは、一連の中核的な基本レベルのトピックがカバーされることですが、通常実施されているトレーニング プログラムでは、ここで求められる内容より包括的なものになると考えられます。

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

#### 検証すべき証跡：

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

#### 論拠:

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

## G2: コンプライアンスを履行するための責任者のアサイン

### FOSSに関する窓口機能を明確にすること（「FOSS窓口」）。

* **FOSSに関する外部からの問い合わせに対応する責任者をアサインすること。**
* **FOSS窓口はFOSSコンプライアンスの問い合わせに対し、商業的に合理的な努力を払い適切に対応すること。**
* **Publicly identify a means by which one can contact the FOSS Liaison.**

#### 検証すべき証跡：

* + - 1. FOSS Liaison function is publicly identified (e.g., via a published contact email address, or the Linux Foundation's Open Compliance Directory).
      2. An internal documented procedure exists that assigns responsibility for receiving FOSS compliance inquiries.

#### 論拠:

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.

### 組織内部におけるFOSSコンプライアンスを履行する役割を明確にすること。

* **組織内部のFOSSコンプライアンスを管理する責任者をアサインすること。The FOSS Compliance role and the FOSS Liaison may be the same individual.**
* **FOSSコンプライアンス管理に十分な活動資源が提供されていること。** 
  + **職務を遂行するための時間が割り当てられている。**
  + **商業的に合理的な予算が配分されている。**
* **FOSSコンプライアンスのポリシーとプロセスを策定および維持するための責任者をアサインすること。**
* **FOSSコンプライアンスの履行担当者がFOSSコンプライアンスに関する法的な専門知識を（その組織内もしくは組織外で）獲得できること。**
* **A process exists for the resolution of FOSS compliance issues.**

#### 検証すべき証跡：

1. Name of persons, group or function in FOSS Compliance role(s) internally identified.
2. Identify source of legal expertise available to FOSS Compliance role(s) which could be internal or external.
3. A documented procedure exists that assigns internal responsibilities for FOSS compliance.
4. A documented procedure exists for handling the review and remediation of non-compliant cases.

#### 論拠:

適切なFOSS責任者が効果的にアサインされたことを確かなものにします。

## G3: FOSSコンテンツのレビューと承認

### 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.

#### 検証すべき証跡：

* + - 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.
      2. FOSS component records exist for each Supplied Software release which demonstrates the documented procedure was properly followed.

#### 論拠:

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.

### 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]](#footnote-1)

#### 検証すべき証跡：

* + - 1. A procedure has been implemented that handles the common FOSS license use cases for the FOSS components of each Supplied Software release.

#### 論拠:

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.

## G4: FOSSコンテンツ ドキュメントとコンプライアンス関連資料の頒布

### 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]](#footnote-2), SPDX documents and so forth.

#### 検証すべき証跡：

* + - 1. A documented procedure exists that ensures the Compliance Artifacts are prepared and distributed with Supplied Software release as required by the Identified Licenses.
      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)

#### 論拠:

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.

## G5: FOSSコミュニティへの（積極的な）関わり方の理解

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

#### 検証すべき証跡：

1. FOSSコントリビューション ポリシーが文書化されている。
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).

#### 論拠:

FOSSへの公的なコントリビューションに関するポリシーの作成について、組織が十分に検討していることを確かなものとします。FOSSコントリビューション ポリシーは、組織全体のFOSSポリシーの一部として策定することも、独立したポリシーとして策定することも可能です。コントリビューションがまったく許容されていない状況の場合は、その立場を明確に示すポリシーの存在が必要です。

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

#### 検証すべき証跡：

* + - 1. Provided the FOSS contribution policy permits contributions, a documented procedure exists that governs FOSS contributions.

#### 論拠:

組織が公的にFOSSにコントリビュートする方法について文書化されたプロセスを有することを確かなものにします。コントリビューションが許容されてない場合においても、ポリシーは存在した方がよいでしょう。In that situation it is understood that no procedure may exist and this requirement would nevertheless be met.

## G6: OpenChain要件適合の認定

### 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.

#### 検証すべき証跡：

* + - 1. The organization affirms that a FOSS management program exists that meets all the requirements of this OpenChain Specification version 1.1.

#### 論拠:

組織がOpenChainに適合したコンプライアンス プログラムを有していると宣言した場合、当該プログラムが本仕様書のすべての要件を満たしていることを確かなものにします。これらの要件に部分的に準拠しているだけではOpenChain適合認定を保証するに十分なものとはみなされません。

### 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.

#### 検証すべき証跡：

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.

#### 論拠:

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.

# 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](https://wiki.linuxfoundation.org/openchain/spec-translations).

1. （Wikipedia「[帰属](https://ja.wikipedia.org/wiki/%E5%B8%B0%E5%B1%9E_(%E8%91%97%E4%BD%9C%E6%A8%A9))」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。」 [↑](#footnote-ref-1)
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](https://www.gnu.org/licenses/gpl-faq.ja.html#WhatDoesWrittenOfferValid)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。」 [↑](#footnote-ref-2)