**Openchain 適合仕様書**  
Version 1.0

**Contents**

[**はじめに** 3](#_Toc476563264)

[**用語の定義** 4](#_Toc476563265)

[**満たすべき要件** 5](#_Toc476563266)

[G1: FOSSに係る責任を理解している 5](#_Toc476563267)

[G2: コンプライアンス実現のための責任者のアサインしている 6](#_Toc476563268)

[G3: FOSSコンテンツをレビューし承認する 7](#_Toc476563269)

[G4: FOSSドキュメント類や生成物をデリバリする 8](#_Toc476563270)

[G5: Understand FOSS Community Engagement 9](#_Toc476563271)

[G6: Certify Adherence to OpenChain Requirements 10](#_Toc476563272)

# はじめに

OpenChain イニシアチブがスタートした2013年、この年ソフトウェア・サプライチェーンでオープンソースを活用していた実践者たちは、表面化してきている2つのパターンを観測していた：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では、そのプロセスに意味ありげな類似性があったが； 2)一方でいまだ多くの組織においてソフトウェアのやり取りするためのプログラムは非先進的なものだった。後者では、ソフトウェアのやり取りに付随する、コンプライアンス関連生成物の一貫性や品質について信頼を喪失させる事態を引き起こし、. 結果として、サプライチェーンのそれぞれの段階において、上流側組織で既に実施したコンプライアンス業務を下流組織で再び実施されていた。

こういった背景から、標準的なプログラムの仕様というものを整備することができるかどうか検討する研究グループが形成された。これは、 i) 産業横断的に共有されるオープンソース・コンプライアンスに係る情報の品質と一貫性を促進し; ii)コンプライアンス作業の再実施に起因する、オープンソースに関連するトランザクションコストの低減することを見据えている。本研究グループは、ワーキンググループへと発展、のち2016年4月 、正式にThe Linux Foundationのコラボレーティブ・プロジェクトとして組織されることとなった。

OpenChain イニシアチブは以下のビジョンとミッションを有する：

* **ビジョン： フリー/オープンソース・ソフトウェア(FOSS)が、信頼でき一貫性のあるコンプライアンス情報とともに提供されるソフトウェア・サプライチェーンを実現すること**
* **ミッション: フリー/オープンソース・ソフトウェア(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・サプライチェーンの参加者のために確立すること。こういった要件や関連する付随事項は、オープンに、ソフトウェア・サプライチェーン、オープンソース ・コミュニティやアカデミア（学術研究機関）の関係者それぞれがオープンに協働しながら開発を進めていく**

上記ビジョンとミッションに則り、本仕様書ではこれに適合するならばそのオープンソース・コンプライアンスプログラムは十分なレベルでの品質、一貫性と完全性を獲得している、その可能性を著しく高めてくれるであろう要件の一式を定義する。ただし、本要件のすべてを満たしていたとしてもそれが完全なコンプライアンスプログラムであることを保証するものではない。本要件は、そのプログラムがOpenChain に適合しているとみなすために満足していなければならない、ベースレベル（最低限）の要件セットを示したものである。本仕様書は、「どうやって(How）」や「いつ(When)」といった考慮ではなく、コンプライアンスプログラムの「何(What)」、「なぜ(Why)」の属性に焦点をあてている。また本仕様書は、さまざまな組織が自身のポリシーやプロセスが目的にベストフィットするよう仕立て上げられるよう、実用的なレベルでの柔軟性を確保している。

第2節では、仕様として全般で用いられる重要用語について定義していく。第3節では、仕様としての要件を示していく。それぞれに 一つ以上の「検証物件」が存在する。これらは提示された要件が満たされているかどうかを検討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担っている。すべての要件をそのプログラムが満たしている場合、それは仕様書1.0版における「 OpenChain 準拠(OpenChain Conforming)」とみなされる。

# 用語の定義

**頒布・配布コンプライアンス生成物 －供給されたソフトウェアとともに特定されたライセンスが提供されることが求められる生成物一式であり以下を含んむもの：著作権表示（Copyright notice）、ライセンスのコピー、修正箇所の通知、帰属情報の通知、ソースコード、書面による提案など**

**FOSS (フリー/オープンソース・ソフトウェア) －オープンソース・イニシアティブ(OpenSource.org)によって発行されているオープンソース定義、もしくはフリーソフトウェア・ファンデーションによって発行されているフリーソフトウェア定義に当てはまるライセンス、もしくはそれに類似した1つ以上のライセンスに従うソフトウェアのこと**

**FOSS 窓口担当－外部からのFOSSに係る問合せを受け付ける、指名された人のこと確認済みライセンス－適切な方法に則り確認ができたFOSSライセンスのこと**

**OpenChain準拠 －本仕様書のすべての要件を満たすプログラムのこと**

ソフトウェアスタッフ－提供されるソフトウェアを作り出し、コントリビュートし、もしくはそれを使えるようにするために責任を有しているあらゆる従業員や契約者のこと。組織によっては、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やプロダクト管理者が含まれる場合があるが、この限りではない。

**SPDX もしくはSoftware Package Data Exchange－ SPDXワーキンググループによって作られた、ライセンスや著作権情報をやり取りすることを目的としたフォーマット標準のこと。SPDXについてはww.spdx.orgにその仕様が記載されている。**

**供給されるソフトウェア －組織が第三者に対し提供するソフトウェアのこと**

**検証物件 - 与えられた要件が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**

# 満たすべき要件

## G1: FOSSに係る責任を理解している

**1.1供給されるソフトウェアの配布についてFOSSライセンスコンプライアンスを統制するFOSSポリシーが書面として存在し、それが最低でも組織内で伝えられていなければならない**

**確証として必要となるもの:**

* 1.1.1文書化されたFOSS ポリシー
* 1.1.2FOSSポリシーの存在をすべてのソフトウェアスタッフがを知ることができる、文書化された手続き

**論理的根拠:**

これにより作成・記録するステップを確実なものとし、加えてソフトウェアスタッフへFOSSポリシーの存在を周知することができる。ポリシーとして記載されるべき内容についての要件についてはここでは扱わず、他節にて記載する。.

**1.2ソフトウェアスタッフ向けの受講必須のトレーニングが存在していること**

* **トレーニングとして最低でも以下に示すトピックを含んでいる：**
* **FOSSポリシーおよびその入手先；**
* **知的財産権関連法令の基礎；**
* **FOSSライセンス供与の概念（コピーレフトおよびパーミッシブなライセンスの概念を含む）;**
* **FOSSプロジェクトのライセンス供与のモデル；**
* **ソフトウェアスタッフの役割、全体としてのFOSSポリシーや具体的なFOSSコンプライアンスに付随する責任および；**
* **提供されるソフトウェアのFOSSコンポーネントを特定し、記録し、もしくは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（現状に即すとみなされるよう）少なくとも直近24ヶ月以内に修了していなければならない。ソフトウェアスタッフが本トレーニング要件を満足させるために試験を実施してもよい

**確証として必要となるもの:**

* 1.2.1上記のトピックを含んだFOSS教材（例：スライド資料、オンラインコースもしくはその他トレーニング用資料）
* 1.2.2ソフトウェアスタッフ全員がコースを修了していることを確認する方法
* 1.2.3全ソフトウェアスタッフのうち少なくとも85%が本節上記定義で、現行に即した状態であること

**論理的根拠:**

ソフトウェアスタッフが直近でFOSSトレーニングに参加したということと併せ、そのトレーニングが今日的に意味のあるFOSSに係る一連のトピックがカバーされていることを確かなものとする。ここで意図しているのは、中核的な基本レベルにおいて一連のトピックがカバーされることであるが、典型的なトレーニングプログラムにおいては、ここで求めるものよりも包括的になることがふさわしいだろう。

## G2: コンプライアンス実現のための責任者のアサインしている

**2.1FOSS窓口機能を明確化すること（FOSS窓口）**

* **FOSSに係る外部からの問合せ受け付けに責任をもつ要員をアサインする；**
* **FOSS窓口はFOSSコンプライアンスの問合せに対し適切に対応すべく、商業的に理にかなった活動を行ない、**
* **電子的通信を通じFOSS窓口にコンタクトする手段を公衆に対し明らかにしなければならない**

**確証として必要となるもの:**

* 2.1.1公衆に対し明示されたFOSS窓口機能の存在（例：電子メールアドレス、あるいはLinux Foundationのオープンコンプライアンスディレクトリの情報など）
* 2.1.2FOSSコンプライアンスに係る問合せを受けつける責任者をアサインするための文書化された手続きが存在

**論理的根拠:**

FOSSコンプライアンスに関する問合せについて第三者がその組織にコンタクトできる、合理的な手段があることを確かなものに関して、についてする。

**2.2内部でFOSSコンプライアンスを遂行する役職を明確にすること**

* **内部のFOSSコンプライアンス管理に対し責任者をアサインするFOSSコンプライアンスを担う役職はFOSS窓口担当者を兼ねることができる**
* **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：**
* **役割を遂行する時間が割り当てられており、**
* **商業的に理にかなった形で予算が配分されている**
* **FOSSコンプライアンスポリシーとプロセスを開発・維持する責任者をアサインする；**
* **FOSSコンプライアンスを担う役職がFOSSコンプライアンスに係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、；**
* **FOSSコンプライアンスに係る諸問題の解決のためにエスカレーションパスが有効となっている**

**確証として必要となるもの:**

* 2.2.1FOSSコンプライアンスにおける機能名称、グループ名もしくは個人名
* 2.2.2FOSSコンプライアンスを担う役職にとって使用可能で、その源泉が特定できる法的専門知識
* 2.2.3FOSSコンプライアンスの責任者をアサインする、文書化された手続きの存在
* 2.2.4問題の解決のためのエスカレーションパスを明確にした、文書化された手続きの存在

**論理的根拠:**

ここで定められたFOSS責任者が有効性をもってアサインされたことを確かなものとするOpenChain Conformance Specification 1.0

## G3: FOSSコンテンツをレビューし承認する

**3.1供給されたソフトウェアに含まれる全てのFOSSコンポーネント（およびそれらそれぞれの確認済みライセンス）を特定し、追跡し、リストとして保管するプロセスが存在すること**

**確証として必要となるもの:**

* 3.1.1供給されたソフトウェアに含まれるすべてのFOSSコンポーネントおよびそれらの確認済みライセンスを特定し、追跡し、リストして保管するために使われる文書化された手続きの存在

**論理的根拠:**

供給されたソフトウェアを構成するために用いられる全てのFOSSコンポーネントを特定し、リスト化するためのプロセスが存在することを確かなものとする。個々のコンポーネントの頒布に関する義務や制約を理解するべく、ライセンス条項のシステマチックなレビューを支援するよう、本目録は存在していなければならない。記録としての本目録は、そのプロセスにもどいている証拠として機能することになる

**3.2FOSSプログラムは供給されたソフトウェアについて、ソフトウェアスタッフが直面する典型的なFOSSユースケースに対処できなければならない。以下のようなユースケースが含まれることがある－供給ソフトウェアのパーツが：（以下のリストは網羅的でなく、組織によっては下のユースケースが当てはまらないこともありうる点は注意）**

* **バイナリ形態で頒布されている**
* **ソースコード形態で頒布されている**
* **コピーレフトの義務を生じうる他のFOSSと統合されている**
* **修正されたFOSSを含んでいる**
* **供給されたソフトウェア内で他コンポーネントと連動するが、お互いに互換性のないライセンスの下にあるFOSS、その他ソフトウェア**
* **帰属要求のあるFOSSを含んでいる**

**確証として必要となるもの:**

* 3.2.1供給されたソフトウェアについてソフトウェアスタッフが直面する典型的なFOSSのユースケースに取り組むために整備されたプロセス

**論理的根拠:**

FOSSプログラムを、組織のビジネスを実践する上で生じる典型的なユースケースに取り組むことに耐えうるものにする

## G4: FOSSドキュメント類や生成物をデリバリする

**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**

**確証として必要となるもの:**

* 4.1.1 A documented procedure exists describing a process that ensures the Distributed Compliance Artifacts be distributed with Supplied Software as required by the Identified Licenses.
* 4.1.2 Copies of the Distributed Compliance Artifacts of the Supplied Software are archived and easily retrievable (e.g., legal notices, source code, SPDX documents), 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).

**論理的根拠:**

Ensure the complete collection of compliance artifacts accompany the Supplied Software as required by the Identified Licenses that govern the Supplied Software.

## G5: Understand FOSS Community Engagement

**5.1 A written policy exists that governs contributions to publicly accessible FOSS projects by employees on behalf of the organization where, as a minimum, it must be internally communicated.**

**確証として必要となるもの:**

* 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).

**論理的根拠:**

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 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

**確証として必要となるもの:**

* 5.2.1 Provided the FOSS contribution policy permits contributions, a documented procedure exists that describes the FOSS contribution process.

**論理的根拠:**

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 specific situation it is understood that no process may exist and this requirement would nevertheless be met.

## 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 program that meets the criteria described in this OpenChain Conformance Specification version 1.0.**

**確証として必要となるもの:**

* 6.1.1 The organization affirms that a program exists that meets all the requirements of this OpenChain Conformance Specification version 1.0.

**論理的根拠:**

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.