

**Openchain 適合仕様書**

第1.0版

**目次**

[はじめに 3](#_bookmark0)

[用語の定義 4](#_bookmark1)

[満たすべき要件 5](#_bookmark2)

[G1: FOSSに関わる責任の理解 5](#_bookmark3)

[G2: コンプライアンス到達のための責任者のアサインしている 6](#_bookmark4)

[G3: FOSSコンテンツをレビューし承認する 7](#_bookmark5)

[G4: FOSSドキュメントや生成物をデリバリする 8](#_bookmark6)

[G5: FOSSコミュニティとの（積極的な）関わり方を理解している 9](#_bookmark7)

[G6: OpenChainの要件を遵守していることを認定する 10](#_bookmark8)

# 免責事項（Disclaimer）

本文書は、The Linux FoundationにおけるOpenChainプロジェクトの本家英文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 Linux Foundation. 本仕様書の利用は、Creative Commons Attribution License 4.0ライセンスにもとづき許諾されます。ライセンスの写しはこちらで入手できます。： CC-BY-4.0

# 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ました：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において、そのプロセスに意味ありげな類似性があったこと； 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が非先進的なものだったこと。後者の観測では、ソフトウェアのやり取りで付随する、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、その結果、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が下流組織で再び実施されていました。

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調査グループが形成されました。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向上を促進し； 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を低減することを見据えています。本研究グループは、ワーキンググループへと発展し、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りました。

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：

* **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。**
* **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」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。すべての要件をそのコンプライアンス プログラムが満たしている場合には、仕様書第1.0版における「OpenChain適合（OpenChain Conforming）」とみなされます。

# 用語の定義

**頒布コンプライアンス関連資料－確認済みライセンスによって供給ソフトウェアとともに提供を求められる生成物一式のこと。著作権表示（Copyright notice）、ライセンスのコピー、改変告知、帰属告知、ソースコード、書面による申し出などを含む。**

**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もしくはそれに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－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適合（Open Chain Conforming）－本仕様書のすべての要件を満たすコンプライアンス プログラムのこと。**

**ソフトウェア スタッフ－供給ソフトウェアについて、創り出し、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も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 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、ライセンスや著作権情報をやりと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。**

**供給ソフトウェア－組織が第三者（他組織または個人）に対して提供するソフトウェアのこと。**

**検証すべき証跡－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。**

# 満たすべき要件

## G1: FOSSに関わる責任の理解

### 供給ソフトウェアの頒布について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、少なくともそれが組織内に周知されていること。

#### 検証すべき証跡：

* + - 1.1.1文書化されたFOSS ポリシーが存在する。
    - 1.1.2すべてのソフトウェアスタッフに（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手法を通じ）FOSSポリシーの存在を知らせる、文書化された手続きの存在

#### 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 スタッフへFOSSポリシーの存在を周知することを確実にします。FOSSポリシーに含まれるべき内容についてはここで提示されませんが、他の要件で提示されることがあります。

### ソフトウェア スタッフ向けの受講必須の最低でも以下に示すトピックを含んだトレーニングが存在し：

* **そのトレーニングが最低でも以下に示すトピックを含んでいること：**
  + **FOSSポリシーおよびその写しがどこで見つけられるか；**
  + **FOSSおよびFOSSライセンスに付随する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コンポーネントを確認、記録、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に）少なくとも直近24ヶ月以内に修了していなければなりません。 そのトレーニング要件を満足させるために、ソフトウェアスタッフに対して試験を実施することができます。**

#### 検証すべき証跡：

* + - 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手段
    - 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、現行に即した状態にあること

#### 論拠:

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、そのトレーニングでFOSS関連として今日的に意味のある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、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すが、典型的なトレーニング プログラムでは、ここで求められる内容はより広範囲で包括的なものになってくると考えられます。

## G2: コンプライアンス到達のための責任者のアサインしている

### FOSS窓口機能を明確にすること（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し；**
* **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りません。**

#### 検証すべき証跡：

* 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）
* 2.1.2 FOSSコンプライアンスの問合せを受け付ける責任者をアサインする、文書化された手続きの存在

#### 論拠:

FOSSコンプライアンスの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します。

### 組織内部におけるFOSSコンプライアンスを遂行する役職を明確にすること

* **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。 本FOSSコンプライアンスを担う役職はFOSS窓口担当を兼ねることができます。**
* **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：**
* **役割を遂行するために割り当てられた時間；**
* **商業的に理にかなった形で配分された予算**
* **FOSSコンプライアンスポリシーとプロセスを策定し・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こと**

#### 検証すべき証跡：

* 2.2.1 FOSSコンプライアンスの役割おける特定の個人名、グループ名もしくは機能名
* 2.2.2 FOSSコンプライアンスの役職が利用可能な法的専門知識の情報源
* 2.2.3 FOSS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にします。

## G3: FOSSコンテンツをレビューし承認する

### 供給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

#### 検証すべき証跡：

* + - 3.1.1 供給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にします。 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ために、ライセンス条項の体系的なレビューを支援するよう、本目録が存在していなければなりません。 記録された本目録は、そのプロセスにもとづいていることを示す確証として機能します。

### FOSSプログラムは供給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ユースケースに対応できること。以下のようなユースケースが含まれる場合がある－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、組織によっては以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を含んでいる**
* **帰属要求のあるFOSSを含んでいる**

#### 検証すべき証跡：

* + - 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

#### 論拠:

FOSSプログラムが組織のビジネスを実践する際の典型的なユースケースに十分耐えられるものにします。

## G4: FOSSドキュメントや生成物をデリバリする

### 提供ソフトウェアが伴う確認済みライセンスに応じ要求される、以下の頒布・配布コンプライアンス生成物が用意されていること：

* **著作権表示**
* **確認されるライセンスの写し**
* **改修内容の通知**
* **帰属表示**
* **重要な通知**
* **ソースコード**
* **ビルドに必要な手順とスクリプト**
* **書面による申し入れ**

#### 検証すべき証跡：

* 4.1.1 確認済みライセンスが要求するとおり供給ソフトウェアとともにコンプライアンス生成物が、頒布・配布されていることを確実にするためのプロセスを記載する、文書化された手続きの存在
* 4.1.2 供給ソフトウェアに係る頒布・配布コンプライアンス生成物の、保管され、容易に検索可能な写し（例：法的な通知、ソースコードやSPDXドキュメント）および本保管物が少なくとも当該提供ソフトウェアが申し出ている期間、もしくは確認済みライセンスが要求する期間（のうちいずれか長い方の期間）存在するために立てられた計画

#### 論拠:

供給ソフトウェアを統制している確認済みライセンスが要求するとおりにコンプライアンス関連生成物がすべて集められてそれが添付されていることを確かなものとします。

## G5: FOSSコミュニティとの（積極的な）関わり方を理解している

### 公衆が広くアクセスできるFOSSプロジェクトへ従業員がその企業を代表してコントリビューションすることを統制する文書化されたポリシーが存在し、そのポリシーが最低限組織内に行き渡っていること

#### 検証すべき証跡：

* + - 5.1.1 文書化されたコントリビューションポリシーの存在
    - 5.1.2 FOSSコントリビューション ポリシーがあることをすべてのソフトウェア スタッフに認知させる手続きの存在（例：トレーニング実施、社内Wikiもしくはその他実践的な伝達策）

#### 論拠:

公の場でのFOSSコントリビューションに関し方針を立てることについて理にかなった検討を行なった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、組織における全体としてのFOSSポリシーの一部として、もしくは独立したポリシーとして、どちらの形でも策定可能です。 コントリビューションが全く許容されていない状況においても、その立場を明確に示すポリシーが存在しているのが望ましいでしょう。

### FOSSコントリビューション ポリシーがここでいうコントリビューションを許容するものである場合、コントリビューションがFOSSコントリビューション ポリシーに忠実に従っていることを確認するためのプロセスが存在していること。それらには、以下のような点が考慮されることがあります（ただしこの限りではありません）：

* **ライセンスに関する検討結果への法務面での承認**
* **ビジネス面での合理的根拠もしくは承認**
* **コントリビューション対象となるコードの技術的レビュー**
* **コミュニティに係る積極的関与と相互交流、およびプロジェクトの行動規範（Code of Conduct ）もしくはそれに同等のものを含む**
* **プロジェクト固有のコントリビューション要求の遵守**

#### 検証すべき証跡：

* + - 5.2.1 FOSSコントリビューション ポリシーがコントリビューションを許容するものである場合の、FOSSコントリビューションのプロセスを記載した文書化された手続きの存在

#### 論拠:

公にされているFOSSへコントリビュートするやり方について文書化されたプロセスを有していることを確かなものとします。 ポリシーはここでいう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存在する場合があります。そのような特有の状況でプロセスが存在しないと理解される場合には、上記に関わらず本要件は満たされないものとなります。

## G6: OpenChainの要件を遵守していることを認定する

### 組織がOpenChainに認定されるためには、本Openchain適合仕様書第1.0版に記載された基準を満たすFOSSプログラムを有していることを確認しなければなりません。

#### 検証すべき証跡：

* + - 6.1.1 その組織が確認できている、本OpenChain適合仕様書第1.0版の要件を満たしたプログラムの存在

#### 論拠:

組織がOpenChainに適合した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。 これら要件の単なる部分的な対応では、プログラムがOpenChain認定を保証するために十分なものとみなすことはできません。