**Openchain 適合仕様書**  
第1.0版

**目次**

[**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: コンプライアンス到達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ドキュメントや生成物をデリバリする 8](#_Toc476563270)

[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](#_Toc476563271)

[G6: OpenChainの要件を遵守していることを認定する 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研究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
* **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 サプライチェーンに参加する人たち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きます**

上記ビジョンとミッションに則り、本仕様書ではオープンソース コンプライアンス プログラムがこれに適合した場合、品質や一貫性や完全性が十分なレベルに到達する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しています；ただし本仕様書は、本要件のすべてを満たしていたとしてもそのプログラムが全面的に準拠していることを保証するものではありまえせん。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、基準レベル（最低限）の要件を一式として提示するものです。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ます。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うまく合う形で仕立て上げられるように、実用的レベルでの柔軟性を確保しています。

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きます。第3節では、仕様としての要件を示していきます。それぞれに 一つ以上の「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ます。すべての要件をそのプログラムが満たしている場合には、仕様書第1.0版において「 OpenChain 準拠(OpenChain Conforming)」とみなされます。

# 用語の定義

**頒布・配布コンプライアンス関連生成物 －供給ソフトウェアとともに確認済みライセンスの提供が求められる生成物一式のことであり、以下を含むもの：著作権表示（Copyright notice）、ライセンスのコピー、修正内容の通知、帰属情報の通知、ソースコード、書面による申し入れなど**

**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の定義、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の定義に該当するライセンス、もしくはそれに類似する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－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もつ、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りますが、この限りではありません。

**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ます。**

**供給ソフトウェア －組織が第三者に対し提供するソフトウェアのこと**

**証跡 - 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、それが最低でも組織内に周知されていること**

**証跡：**

* 1.1.1文書化されたFOSS ポリシーの存在
* 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の存在

**論拠:**

本要件により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。このFOSSポリシーに含まれるべき内容について、ここでの要件としては提示されていませんが、他の節では提示されている場合があります。

**1.2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。

**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

**2.1FOSS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。**

**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）
* 2.1.2FOSS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。

**2.2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**

**証跡：**

* 2.2.1FOSS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
* 2.2.2FOSS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
* 2.2.3FOSS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。OpenChain 適合仕様書 第1.0版

## G3: FOSSコンテンツをレビューし承認する

**3.1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**

**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。

**3.2FOSS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**

**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

**4.1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確認済みライセンス意されていること：**

* **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**

**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

**5.1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**

**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
* 5.1.2FOSS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。

**5.2FOSS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

**証跡：**

* 5.2.1FOSS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

**6.1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。**

**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。