OpenChain仕様書

第2.0版

ソフトウェアソリューションを構成する

**オープンソース**への信頼を確立するために

目次

[免責事項（Disclaimer） 5](#_Toc19594962)

[著作権、ライセンス 5](#_Toc19594963)

[はじめに 6](#_Toc19594964)

[用語の定義 7](#_Toc19594965)

[具体的要求事項 9](#_Toc19594975)

[1.0 プログラムの基盤確立 9](#_Toc19594976)

[2.0 関連タスクの定義と実行支援 12](#_Toc19594982)

[3.0 オープンソースコンテンツのレビューと承認 14](#_Toc19594985)

[4.0 コンプライアンス関連資料の作成と配布 16](#_Toc19594988)

[5.0 オープンソースコミュニティ活動への理解 17](#_Toc19594990)

[6.0 仕様に規定する要求事項の遵守 18](#_Toc19594992)

[付録 I: 本文書の翻訳について 20](#_Toc19594995)

# 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。ただし、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© 2016-2019 Linux Foundation®.

本仕様書の利用は、Creative Commons Attribution 4.0 International (CC-BY 4.0)ライセンスの下で許諾されます。ライセンスの写しは <https://creativecommons.org/licenses/by/4.0/> で確認できます。

# はじめに

この仕様書は、オープンソースライセンスに対する質の高いコンプライアンスプログラム（以下では、プログラムと略します）の主要な要求事項を定義しています。これにより、オープンソースソフトウェアで構成されたソフトウェアソリューションを相互に取り交わす組織（主として、企業として運営される組織を想定しています）の間での信頼構築に至る基準を提供することを目的としています。組織のライセンスコンプライアンス活動を管理するプログラムが本仕様書に適合していることで、個別のソフトウェアソリューションにそれぞれについて、必要とされるコンプライアンス関連資料（すなわち、法的通知、ソースコードなどの資料）が確実に生成されることが保証されます。OpenChainの仕様書によるプログラムの要求事項の定義は、「どのようなやり方で（How）」や「どのような時に（When）」という側面ではなく、「何を対象に（What）」と「どのような理由で（Why）」という側面に焦点を当てています。この柔軟性により、さまざまな市場に存在するさまざまな規模の組織それぞれが、この仕様書に基づき、規模、目標、統制範囲に合ったポリシーとプロセスを選択できます。例えば、OpenChain適合プログラムは、組織の単一の製品ラインを対象とすることも、あるいは、組織全体を対象とすることもできます。

このセクション（セクション１：はじめに）ではすべてのOpenChainユーザに向けて、仕様書の背景を提供しています。セクション２（用語の定義）では、本仕様書全体で使用される主要な用語を定義しています。セクション３（具体的要求事項）では、本仕様書に適合するためにプログラムが満たすべき要求事項を定義しています。各要件は、当該要求事項を満たすために生成される必要のある１または複数の証跡となる資料（すなわち、記録として残される書類）で構成されています。証跡となる資料を一般に公開する必要はありませんが、仮に他者に提供することとなる場合は、機密保持契約（NDA）の下での開示となるでしょう。

この仕様書は、オープンイニシアティブとして開発され、150人以上の貢献者からフィードバックが寄せられています。開発履歴の詳細は仕様書用の[メーリングリスト](https://lists.linuxfoundation.org/mailman/listinfo/openchain-spec)、および、[Frequently Asked Questions (FAQ)](https://wiki.linuxfoundation.org/openchain/specification-questions-and-answers)でご覧いただけます。

# 用語の定義

原文における英語のアルファベット順。本文中では、太字で表記しています。

****コンプライアンス関連資料（Compliance Artifact）****

供給ソフトウェアに対応してプログラムが生成する資料の集合。たとえば、ソースコード、帰属告知[[1]](#footnote-1)、著作権表示、ライセンスの写し、改変告知、書面による申し出、オープンソースコンポーネント部品表、SPDXドキュメントなど。（以上は例示であり、これらに限定されるものではない）

****確認ライセンス（Identified License）****

供給ソフトウェアを構成するオープンソースコンポーネントに、適切なライセンス確認手法を用いることにより存在が確認されたオープンソースライセンスの一式。

****OpenChain適合（OpenChain Conformant）****

本仕様書のすべての要求事項を満たすプログラム。

****オープンソース（Open Source）****

Open Source Initiative（OpenSource.org）が策定したOpen Source Definitionや、Free Software Foundationが策定したFree Software Definitionに準拠した、1または複数のライセンス、または同等のライセンスに従うソフトウェア。

****プログラム（Program）****

組織のライセンスコンプライアンス活動を管理するポリシー、プロセス、および要員の一式。

****ソフトウェアスタッフ（Software Staff）****[[2]](#footnote-2)

供給ソフトウェアを定義する、供給ソフトウェアに貢献する、あるいは、供給ソフトウェアを使えるように準備する責任を持つ、組織の従業員または業務請負者のすべて。該当する者は組織によって異なるが、たとえば、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挙げられる（以上は例示であり、これらに限定されるものではない）。

****SPDX****

Linux FoundationのSPDX（Software Data Package Exchange）ワーキンググループによって作られ、ソフトウェアパッケージのライセンスおよび著作権情報を交換することを目的としたフォーマット標準。SPDX仕様の詳細はwww.spdx.orgを参照のこと。

****供給ソフトウェア（Supplied Software）****

組織が第三者（たとえば、他の組織や個人）に対して提供するソフトウェア。

****証跡となる資料（Verification Material）****

与えられた要求事項を満たすことを実証する資料。

# 具体的要求事項

## 1.0 ****プログラム****の基盤確立

### 1.1 ポリシー

供給ソフトウェアに対するオープンソースライセンスコンプライアンスを統制する、オープンソースポリシーが書面にまとめられ存在していること。また、このポリシーが組織内で周知されていること。

#### ****証跡となる資料****

1.1.1 文書化したオープンソースポリシー。

1.1.2 ソフトウェアスタッフにオープンソースポリシーの存在を認識させるための文書化した手順（例えば、トレーニング、社内wiki、またはその他の実効的な伝達方法による）。

#### 論拠

オープンソースポリシーを作成し、記録し、ソフトウェアスタッフにその存在を認識させる、各段階が実行されているかを確認するため。なお、この項では、ポリシーに含めるべき内容に関する要求事項は規定していない。ポリシーに関する具体的要求事項については、他の項で説明されるでしょう。

### 1.2 能力

組織は以下の各項目を実行する必要がある：

* プログラムの遂行結果および有効性に影響を与える、役割および役割に対応する責任を特定する
* 特定された役割それぞれを果たすために必要な、担当者の能力を決定する
* 担当者が十分な能力を持っていることを、適切な教育やトレーニングの受講や当該担当者の経験に基づいて確認する
* 担当者に必要な能力が欠落している場合に、当該担当者に必要な能力を獲得するための措置を講じる
* 能力があることのエビデンスとして、文書化した適切な情報を保持する

#### 証跡となる資料

1.2.1 プログラムに参加する立場の異なる参加者それぞれの、役割と対応する責任を文書化したリスト。

1.2.2 それぞれの役割に要求される能力を特定する文書。

1.2.3 それぞれのプログラム参加者の能力評価についての、文書化したエビデンス。

#### 論拠:

プログラムの役割を実行する、特定された参加者が、それぞれの役割と責任について十分な水準の能力を獲得していることを確認するため。

### 1.3 認識

組織はプログラム参加者[[3]](#footnote-3)が、以下を認識していることを確認する必要がある：

1. オープンソースポリシー
2. 関連するオープンソースの目的[[4]](#footnote-4)
3. プログラムの有効性に対する、参加者の寄与
4. プログラムの要求事項を守らないことの意味

#### ****証跡となる資料****

1.3.1 プログラムの目的、プログラムにおける参加者の寄与、プログラムの不適合の意味を含む、プログラム要員それぞれの認識度を評価した文書化したエビデンス。

#### 論拠:

プログラム要員が、プログラムにおけるそれぞれの役割と責任に対する、十分な認識レベルを獲得していることを確認するため。

### 1.4 プログラムの統制範囲

プログラムの統制範囲は、プログラムごとにレベルが異なる運用となり得る。例えば、プログラムが統制範囲は、特定の製品ライン、特定の部署全体、あるいは、特定の組織全体となり得る。プログラムそれぞれについて、対象として指定した統制範囲を明記する必要がある。

#### ****証跡となる資料****

1.4.1 プログラムの統制範囲と境界について、明確に定義する文書。

#### 論拠:

組織のニーズに合った統制範囲に、最も適したプログラムを構築するための柔軟性を与えるため。たとえば、組織は、特定の製品ラインを対象としたプログラムを確立することを選択してもよいし、組織全体についての供給ソフトウェアを統制するプログラムを導入してもよい。

### 1.5 ライセンス義務

確認ライセンスをレビューし、それぞれのライセンスに従うことで生じる義務、制約、および、権利の内容を判断する、プロセスが存在すること。

#### ****証跡となる資料****

1.5.1. それぞれの確認ライセンスに従うことで生じる義務、制約、および、権利の内容を、レビューし、レビュー結果を文書として記録する、文書化した手順。

#### 論拠

組織が直面する可能性のあるさまざまなユースケースにおいて、確認ライセンスそれぞれに従うことで生じる義務を特定およびレビューする、プロセスが存在することを確認する。ユースケースについては、3.2において定義している。

## 2.0 関連タスクの定義と実行支援

### 2.1 アクセス

外部からのオープンソースに関する問い合わせに効果的に対応するプロセスを維持すること。また、第三者がオープンソースのコンプライアンスに関する問い合わせを行うことができる手段を、一般に公開された形で明示すること。

#### ****証跡となる資料****

2.1.1 一般に公開され可視化された、第三者がオープンソースのライセンスコンプライアンスに関する問い合わせを行うことができる方法。（例えば、連絡先メールアドレスを公開する、または、Linux Foundation のオープンコンプライアンスディレクトリに掲載する。）

2.1.2 第三者からのオープンソースのライセンスコンプライアンスに関する問い合わせへの対応についての、文書化した手順。

#### 論拠

オープンソースのコンプライアンスに関する問い合わせに関し、第三者が組織にコンタクトする合理的な方法があること、および、組織が有効な回答を行う準備ができていることを、確認するため。

### 2.2 十分なリソース割当

プログラムの関連タスクを特定し、リソースを割り当てること：

* プログラムの関連タスクが確実に実行されるように、担当責任を決定すること。
* プログラムの関連タスクは十分なリソースが割り当てられていること：
  + 関連タスクを実行する時間の割り当て
  + 十分な予算の割り当て
* ポリシー、および、関連タスクについて、レビューとアップデートのプロセスが存在すること。
* オープンソースのライセンスコンプライアンスについて法的な支援が必要な者に対し、法的な専門家に相談可能な状態であること。
* オープンソースのライセンスコンプライアンスに関する問題が発生したときに、それを解決するプロセスが存在すること。

#### ****証跡となる資料****

2.2.1 プログラムの役割それぞれに対し、担当者、グループ、または、部署の名称を特定したドキュメント。

2.2.2 プログラムの特定された役割それぞれに、適切に要員配置がなされ、十分な予算割当が行われていること。

2.2.3 組織内外で発生するライセンスコンプライアンスに関連した事項について、支援依頼可能な法務の専門家が特定されていること。

2.2.4 オープンソースコンプライアンスに関する組織内の責任者を割り当てる、文書化した手順。

2.2.5 コンプライアンス違反の事例に対して、レビューや是正措置を行うための、文書化した手順。

#### 論拠

(i)プログラムにおける責任に対し、有効な支援および十分なリソース割り当てが行われていることの確認のため、および、(ii)オープンソースコンプライアンスに関するベストプラクティスが変化していくことに対応して、ポリシーおよび支援プロセスが定期的に更新されることの確認のため。

## 3.0 オープンソースコンテンツのレビューと承認

### 3.1部品表（Bill of Materials）

供給ソフトウェアを構成するオープンソースコンポーネント（および、確認ライセンス）を含む部品表を作成し、管理するプロセスが存在すること。

#### ****証跡となる資料****

3.1.1 供給ソフトウェアを構成するオープンソースコンポーネントの集合を、特定し、追跡し、レビューし、承認し、情報保管する、文書化した手順。

3.1.2 供給ソフトウェアに対し、文書化した手順が適切に運用されたことを示す、オープンソースコンポーネントの記録。

#### 論拠

供給ソフトウェアを構成するオープンソースコンポーネントについての部品表を作成し、管理するプロセスが存在することを確認する。部品表は、それぞれのコンポーネントのライセンス条項を体系的にレビューし、承認する手順をサポートするために必要となる。そのようなレビューおよび承認によって、供給ソフトウェアを配布する際に適用される義務や制限が理解される。

### 3.2 ライセンスコンプライアンス

プログラムは、供給ソフトウェアに対応するソフトウェアスタッフが遭遇する可能性のある、よく用いられるオープンソースライセンスのユースケースに対応できる必要がある。ユースケースとして以下を例示する（ただし、下記リストはすべてを網羅したものではなく、また、すべてのユースケースにあてはまるものではない）

* バイナリ形態での配布
* ソースコード形態での配布
* コピーレフトの義務に従うこととなる他オープンソースとの統合
* 改変されたオープンソースを含む状況
* 供給ソフトウェア内のコンポーネントと相互作用するオープンソース、ないしは、他のソフトウェアを含んでおり、それらが両立性のないライセンス下にある状況
* 帰属要求**[[5]](#footnote-5)**のあるオープンソースを含む状況

#### ****証跡となる資料****

3.2.1 供給ソフトウェア内のオープンソースコンポーネントについて、よく用いられるオープンソースライセンスのユースケースの対応に関する、文書化した手続き。

#### 論拠

プログラムが、組織内のよく用いられるオープンソースライセンスのユースケースを取り扱ううえで十分対応できる状況であることを確認する。また、このような活動をサポートする手続きが存在し、かつ、手続が守られていることを確認する。

## 4.0 コンプライアンス関連資料の作成と配布

### 4.1 コンプライアンス関連資料

供給ソフトウェアのコンプライアンス関連資料一式を作成するプロセスが存在すること。

#### ****証跡となる資料****

4.1.1 確認ライセンスの要求に従って供給ソフトウェアに応じたコンプライアンス関連資料を準備し、配布するプロセスを記述する、文書化された手順。

4.1.2 供給ソフトウェアのコンプライアンス関連資料のコピーを保管する、文書化された手順。保管された資料は、供給ソフトウェアの最終提供以降、適切な期間[[6]](#footnote-6)、あるいは、確認ライセンスの要求事項として定められた期間（どちらか長い方）保持することが計画されている必要がある。また、手順が適切に守られていることを示す記録が存在する必要がある。

#### 論拠

確認ライセンスの要求事項に従い、供給ソフトウェアに付随するコンプライアンス関連資料の準備に商業的に妥当な努力が払われることを、確認するため。

## 5.0 オープンソースコミュニティ活動への理解

### 5.1 オープンソースへの貢献

組織がオープンソースプロジェクトへの貢献を許容する場合、以下を行う必要がある：

* オープンソースプロジェクトへの貢献を統制する文書化されたポリシーの存在
* ポリシーが組織の内部で周知されていること
* ポリシーを実行に移すプロセスがあること

#### ****証跡となる資料****

組織がオープンソースプロジェクトへの貢献を許容する場合、以下の資料が必要である：

5.1.1 文書化したオープンソース貢献ポリシー。

5.1.2 オープンソース貢献を統制する文書化した手続き。

5.1.3 すべてのソフトウェアスタッフがオープンソース貢献ポリシーの存在を認識する文書化した手続き（例えば、トレーニング、内部wiki、その他の実効的な伝達手段を通じて）。

#### 論拠

組織がオープンソースへの貢献を許可する場合、貢献ポリシーの策定と適用に向けて十分に考慮されていることを確認するため。オープンソース**貢献**ポリシーは、オープンソースポリシー全体の一部としてもよいし、あるいは、独立したポリシーとして作成されてもよい。

## 6.0 仕様に規定する要求事項の遵守

### 6.1 適合

当該プログラムがOpenChain適合とみなされるためには、この仕様書の提示する要求事項をプログラムが満たしていることを組織として明確に宣言する必要がある。

#### **証跡となる資料**

6.1.1 1.4で指定したプログラムがこの仕様書のすべての要求事項を満たしていることを明確に宣言する文書。

#### 論拠

組織がOpenChain適合であるプログラムを有していることを宣言するとき、そのプログラムが、この仕様書のすべての要求事項を満たしていることを確認するため。要求事項の一部のみを満たしていることは十分であるとはみなされない。

### 6.2 継続期間

本仕様書のこのバージョンに対応したOpenChain適合のプログラムは、適合認証の取得日から18ヶ月間、OpenChain適合の状態を継続する。適合認証の登録手順はOpenChainプロジェクトのWebサイトを参照のこと。

#### ****証跡となる資料****

6.2.1 当該プログラムが本仕様書（第2.0版）のすべての要求事項を満たすことを明確に宣言する、過去18ヶ月以内に適合取得を示す文書[[7]](#footnote-7)。

#### 論拠

組織が継続してプログラムの適合性を主張しようとする場合、最新の仕様書に準拠した状態を保つことが大切である。この要求事項は組織が継続してプログラム適合性を主張する際に、プログラムの支援プロセスや制御が損なわれることを防いでいる。

# 付録 I: 本文書の翻訳について

本仕様書がグローバルに採用されることを促進するために、私たちは本仕様書を多言語に翻訳する取り組みを歓迎します。OpenChainはオープンソース プロジェクトとして機能するため、各種翻訳は時間と専門的知見を以て貢献することに前向きな方々によって、CC-BY-4.0ライセンスとプロジェクトの翻訳ポリシーの下で推進されます。そのポリシーおよび現在入手可能な翻訳版の詳細については、OpenChainプロジェクトの[仕様書Webページ](https://wiki.linuxfoundation.org/openchain/spec-translations)でご確認ください。

1. 帰属告知(attribution notice)と、3.2の規定で用いられている帰属要求(attribution requirements)の使い分けについては、ISO化に向けた検討版（Specification 2.1）において検討されている。 [↑](#footnote-ref-1)
2. （訳注）Specification 2.0においては、「ソフトウェアスタッフ」（”software staff”・定義用語）と、「プログラム参加者（”program participants”・ 1.3 「認識」における規定で使用）の双方が用いられているが、同じ意味であるため、ISO化に向けた検討版（Specification 2.1）では 「プログラム参加者」へと統一された。 [↑](#footnote-ref-2)
3. （訳注）脚注1にて説明したように、ISO化に向けた検討版（Specification 2.1）では定義用語の「ソフトウェアスタッフ」（”software staff”）は、本項目で用いられている 「プログラム参加者」へ同じ意味であるとして統一されている。 [↑](#footnote-ref-3)
4. （訳注） b)では「オープンソースの目的」、1.3.1では「プログラムの目的」となっているが、「プログラムの目的」が正しいとのこと [↑](#footnote-ref-4)
5. （訳注）：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-5)
6. 原注：製品ドメイン、地域や国による制度の違い、あるいは、顧客との契約によって決まる。 [↑](#footnote-ref-6)
7. （訳注）適合取得が18ヶ月以内であることを明確に宣言する文書であれば（たとえば、宣言日付が18ヶ月以内である6.1の宣言文書であれば）、6.2の「証跡となる資料」に該当する、という説明形式。 [↑](#footnote-ref-7)