

OpenChain 適合仕様書

第 1.0 版

目次

免責事項（Disclaimer）	3
著作権、ライセンス	3
はじめに	4
用語の定義	6
満たすべき要件	7
G1: FOSS に関わる責任の理解	7
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	8
G3: FOSS コンテンツのレビューと承認	9
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	10
G5: FOSS コミュニティへの（積極的な）関わり方の理解	11
G6: OpenChain 要件適合の認定	12

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 Linux Foundation. 本仕様書の利用は、Creative Commons Attribution License 4.0 ライセンスに基づき許諾されます。ライセンスの写しはこちらで入手できます。 : [CC-BY-4.0](https://creativecommons.org/licenses/by/4.0/)

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。

こういった背景から、標準的なコンプライアンス プログラムの仕様書を整備することが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 The Linux Foundation の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。

- **ビジョン**： フリー/オープンソース ソフトウェア (FOSS) が、信頼性と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**： 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。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（Modification notification）、帰属告知（Attribution notice）、ソースコード、書面による申し出（Written offer）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（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 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、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 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 www.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。

検証すべき証拠（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。

満たすべき要件

G1: FOSS に関わる責任の理解

- 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、少なくともそれが組織内に周知されていること。

検証すべき証拠：

- └ 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。**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。

- 1.2 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。
- トレーニングは少なくとも以下に示すトピックを含んでいること。
 - **FOSS** ポリシーおよびそれ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。

検証すべき証拠：

- └ 1.2.1 上記のトピックを含んだ **FOSS** 教材（たとえばスライドやオンライン コースなどのトレーニング用資料）が存在する。
- └ 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がある。
- └ 1.2.3 全ソフトウェア スタッフのうち少なくとも 85%が、本節上記で定義したような最新の状況に即した状態にある。

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。

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

2.1 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。
- 電子的通信を通じて FOSS 窓口にコンタクトする手段を公的に明らかにすること。

検証すべき証拠：

- └ 2.1.1FOSS に関する窓口機能が（たとえば電子メールアドレスや Linux Foundation オープン コンプライアンス ディレクトリを通じて）公的に明示されている。
- └ 2.1.2FOSS コンプライアンスの問い合わせに対応する責任者をアサインするための手続きが文書化されている。

論拠:

FOSS コンプライアンスの問い合わせについて、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。本 FOSS コンプライアンスを履行する役割と FOSS 窓口は同じ担当者が兼務することができます。
- 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。
- 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。
- FOSS コンプライアンスに関わる諸問題を解決するためにエスカレーションパスが有効となっていること。

検証すべき証拠：

- └ 2.2.1FOSS コンプライアンスの履行担当者名、グループ名または役割名称が特定できる。
- └ 2.2.2FOSS コンプライアンスの履行担当者が利用可能な法的専門知識の情報源が特定されている。
- └ 2.2.3FOSS コンプライアンスの責任者をアサインする手続きが文書化されている。
- └ 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手続きが文書化されている。

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

- 3.1 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（およびそれぞれの確認ライセンス）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。

検証すべき証拠：

」 3.1.1 供給ソフトウェアに含まれるすべての **FOSS** コンポーネントとそれらの確認ライセンスを特定し、追跡し、リストとして保管するための手続きが文書化されている。

論拠：

供給ソフトウェアを構成するために用いられるすべての **FOSS** コンポーネントを特定およびリスト化するためのプロセスが存在することを確認可能なものにします。この一覧表は、供給ソフトウェアに適用される頒布上の義務や制約を理解し、各コンポーネントのライセンス条項の体系的レビューをサポートする上で必須となります。一覧表の記録は、そのプロセスが実行されたことを示す確証として機能します。

- 3.2 **FOSS** コンプライアンス プログラムは、ソフトウェア スタッフが扱う供給ソフトウェアの代表的な **FOSS** ユースケースに対応できること。代表的ユースケースでは、供給ソフトウェアの一部が以下のように扱われている（ただしこれらのリストは網羅的ではない。また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る）。
- 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る他の **FOSS** と統合されている
 - 改変された **FOSS** を含んでいる
 - 供給ソフトウェア内の他のコンポーネントとやりとりする、両立性のないライセンス下の **FOSS** やその他のソフトウェアを含んでいる
 - 帰属要求（**Attribution requirement**）のある **FOSS** を含んでいる¹

検証すべき証拠：

」 3.2.1 ソフトウェア スタッフが扱う供給ソフトウェアの代表的な **FOSS** ユースケースに対応するためのプロセスが整備されている。

論拠：

その **FOSS** プログラムが組織の業務遂行上生じる代表的なユースケースに対応できるよう十分堅固なものにします。

¹ (Wikipedia「[帰属](#)」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。”

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

4.1 供給ソフトウェアの確認ライセンスに応じて要求される、以下の頒布コンプライアンス関連資料が用意されていること（ただし、この限りではない）。

- 著作権表示（Copyright notice）
- 確認ライセンスの写し
- 改変告知（Modification notification）
- 帰属告知（Attribution notice）
- 重要事項の告知（Prominent notice）
- ソースコード
- 必要なビルド手順とスクリプト
- 書面による申し出（Written offer）²

検証すべき証拠：

- └ 4.1.1 確認ライセンスの要求に基づいて、頒布コンプライアンス関連資料が供給ソフトウェアとともに頒布されることを確実にするプロセスを説明した手続きが文書化されている。
- └ 4.1.2 供給ソフトウェアに関する頒布コンプライアンス関連資料のコピーが保管され、容易に取り出すことができる（法的告知、ソースコード、SPDX ドキュメントなど）。また、少なくとも当該供給ソフトウェアが提供され続けている期間、または確認ライセンスが要求する期間（いずれか長い方の期間）は、本保管物が存在するように立案されている。

論拠：

供給ソフトウェアを統制する 確認ライセンスの要求に基づいて、コンプライアンス関連資料が完備され、供給ソフトウェアに添付されることを確かなものにします。

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-3.0-ja.html)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と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。”

G5: FOSS コミュニティへの（積極的な）関わり方の理解

- 5.1 公的にアクセス可能な **FOSS** プロジェクトに対し、従業員がその企業を代表してコントリビュートすることを統制するポリシーが文書化されており、最低限、それが組織内に周知されていること。

検証すべき証拠：

- └ 5.1.1FOSS コントリビューション ポリシーが文書化されている。
- └ 5.1.2FOSS コントリビューション ポリシーの存在を（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）すべてのソフトウェア スタッフに認知させる手続きが文書化されている。

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。

- 5.2 **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、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に、以下の検討事項を含むプロセスが存在していること（ただし、この限りではない）。
- ライセンスに関する検討結果に対する法務面での承認
 - ビジネス観点での合理的根拠、もしくは承認
 - コントリビューションの対象となるコードの技術的レビュー
 - コミュニティへの積極的参加および関わり方。たとえばプロジェクトの行動規範（Code of Conduct）もしくはそれと同等のものなど
 - プロジェクト固有のコントリビューション要件の遵守

検証すべき証拠：

- └ 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、FOSS コントリビューションのプロセスを記載した手続きが文書化されている。

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い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。そのような状況においては、具体的な行動のプロセスは存在しないと理解され、本要件が満たされたこととなります。

G6: OpenChain 要件適合の認定

- 6.1 組織が OpenChain に適合していると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 コンプライアンス プログラムを有していることを確認する必要がある。

検証すべき証拠：

- 」 6.1.1 その組織に本 OpenChain 適合仕様書第 1.0 版の要件を満たしたコンプライアンス プログラムが存在することを確認する。

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。