OPENCHAIN

OpenChain 仕様書

第 1.1 版

目次

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

1)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。

こうした背景から、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 Linux Foundation 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 1.1 版における「OpenChain 適合（OpenChain Conforming）」とみなされます。「 検証すべき証跡（Verification Artifact）」は、公開を意図したものではありませんが、

OpenChain 適合を認定する機関による非公開の要請や守秘義務契約（NDA）のもとで提供されることがあります。

2)用語の定義

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または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 Liaison）－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（OpenChain 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（Supplied Software）－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（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。

3)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ていること。またそのポリシーは組織内に周知されていなければならない。**

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、他の節でポリシー上の要件として課される場合があります。

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。**

検証すべき証跡：

1.2.1 上記のトピックを含んだ FOSS トレーニング教材（たとえばスライドやオンライン コース、その他のトレーニング用資料）が存在する。

1.2.2 ソフトウェア スタッフ全員について、トレーニングの修了を追跡する手段がある。

1.2.3 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。

1.3 供与される義務、制約および権利を判断するための確認ライセンスをレビューするプロセスが存在すること。

検証すべき証跡：

1.3.1 供給ソフトウェアを統制している確認ライセンスそれぞれが供与する義務、制約および権利についてレビューし、記録するための手続きが文書化されている。

論拠：

確認ライセンスそれぞれについてレビューし、さまざまなユースケースに対するライセンスの義務を明確化するプロセスが存在することを確かなものにします。

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。**
- **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。**

検証すべき証跡：

2.1.1 OSS 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。

2.1.2 FOSS 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内部文書化されている。

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り、責任者が効果的にアサインされていることを確かなものとします。

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のプロセスが存在していること。**

検証すべき証跡：

2.2.1 FOSS コンプライアンスの役割を有する履行担当者名、グループまたは機能の名称が内部で特定できる。

2.2.2 FOSS コンプライアンスの履行担当者が利用可能な、内部・外部の法的専門知識の情報源が特定されている。

2.2.3 FOSS コンプライアンスの内部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 遵守されていない状況での調査や改善を取り扱うための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 リリースされた供給ソフトウェアについて、各 FOSS コンポーネント（およびその確認ライセンス）を含む部品表（Bill of material[1]）を作り、管理するためのプロセスが存在すること。

検証すべき証跡：

3.1.1 リリースされた供給ソフトウェアを構成する FOSS コンポーネント集について情報を特定し、追跡し、保管するための手続きが文書化されている。

3.1.2 供給ソフトウェアの各リリースに対し、FOSS コンポーネントの記録が存在し、文書化された手続きに適切に従っていることを示している。

論拠：

供給ソフトウェアを構成するために使用される FOSS コンポーネントの部品表（Bill of material）を作り、管理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。部品表は、各コンポーネントについて供給ソフトウェアを頒布する際に適用される義務、制約が書かれたライセンス条件を体系的に（システマチックに）レビューする上で必要となります。

3.2 FOSS のマネジメント 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共通的な FOSS ユースケースに対応できること。共通的ユースケースとして以下のようなものがある（ただしこのリストは網羅的ではなく、組織によっては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うる他の 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**
- **もしくは、帰属要求（Attribution requirement）のある FOSS を含んでいる[2]**

検証すべき証跡：

3.2.1 供給ソフトウェアそれぞれのリリースの FOSS コンポーネントに対し、共通的な FOSS ライセンスのユースケースを取り扱うプロセスが整備されている。

論拠：

そのプログラムが組織における共通的な FOSS ライセンスの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。そしてその活動を支援する手続きが存在し、その手続きに従っていることを確かなものにします。

[1] （Wikipedia「部品表（Bill of Material）」）https://ja.wikipedia.org/wiki/BOM_(部品表)

[2] （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各リリースに対し、FOSS のマネジメント プログラムによる生成物一式が用意されていること。この生成物一式はコンプライアンス関連資料として次の一つ、もしくは複数のもの（ただし、この限りではない）：ソースコード、帰属告知（Attribution notice）、著作権表示（Copyright notice）、ライセンスの写し、改変告知（Modification notification）、書面による申し出（Written offer）[3]、SPDX ドキュメントなど

検証すべき証跡：

4.1.1　コンプライアンス関連資料が用意され、それらが確認ライセンスの要求するとおりに供給ソフトウェアのリリースと併せ頒布されることを確かにする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コンプライアンス関連資料の写しが保管され、容易に取り出すことができる。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（のいずれか長い方の期間）は、本保管物が存在するように計画されている。

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、その他 FOSS レビュープロセスで生成されたレポートと併せて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。

[3] 「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を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 **FOSS プロジェクトに対し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いること。またそのポリシーは組織内に周知されていなければならない。**

検証すべき証跡：

5.1.1 FOSS コントリビューション ポリシーが文書化されている。

5.1.2 FOSS 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ている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 プロジェクトへのコントリビューションを組織が許容する場合、5.1 節に挙げたコントリビューション ポリシーを実践するプロセスが整備されていること。**

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、FOSS コントリビューションを統制する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プロセスが存在しないと理解され、本要件が満たされたことになります。

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 仕様書第 1.1 版に記載された基準を満たす FOSS マネジメント プログラムを有していることを確認する必要がある。

検証すべき証跡：

6.1.1 その組織に本 OpenChain 仕様書第 1.1 版のすべての要件を満たした FOSS マネジメント 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。

6.2 本版の仕様書への適合は、適合が認定された日から 18 か月間持続する。適合認定のための要件は OpenChain プロジェクトの Web サイトで確認できる。

検証すべき証跡：

6.2.1 本 OpenChain 仕様書第 1.1 版の要件すべてを満たし、過去 18 ヶ月以内に適合認定を達成した FOSS マネジメント プログラムがその組織に存在することを確認する。

論拠：

その組織が一定期間を超えてプログラムの適合を主張する場合、本仕様書に即している状態を保つことが重要となります。本要件は、組織が本仕様書への適合を一定期間超えて主張し続けたい場合においてそのプログラムが支えているプロセスや統制機能が損なわれていないことを確かなものにします。

付録 I：言語翻訳について

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コントリビュート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入手可能な翻訳版の詳細については、OpenChain 仕様の Web ページでご確認ください。