

OPENCHAIN 仕様書

第 2.1 版



この仕様書は下記と機能的に同一である。

- OPENCHAIN 仕様書 第 2.0 版
- ISO/IEC PRF 5230

詳細はこちら：www.openchainproject.org

目次

はじめに	iii
1 適用範囲	1
2 用語と定義	1
3 要求事項	2
3.1 プログラムの基盤	2
3.1.1 ポリシー	2
3.1.2 力量	3
3.1.3 認識	3
3.1.4 プログラムの適用範囲	3
3.1.5 ライセンス義務	4
3.2 関連業務の定義と支援	4
3.2.1 アクセス	4
3.2.2 十分なリソース配分	4
3.3 オープンソースコンテンツの見直しと承認	5
3.3.1 部品表 (Bill of Materials)	5
3.3.2 ライセンスコンプライアンス	5
3.4 コンプライアンス関連資料の作成と配布	6
3.4.1 コンプライアンス関連資料	6
3.5 オープンソースコミュニティ活動への理解	6
3.5.1 コントリビューション	6
3.6 仕様要求事項の遵守	7
3.6.1 適合	7
3.6.2 期間	7
附属書 A (参考) 本仕様書の言語翻訳	8

はじめに

本文書は、質の高いオープンソースライセンス準拠プログラムの主要要求事項を定義する。その目的は、オープンソースソフトウェアで構成されるソフトウェアソリューションをやり取りする組織間の信頼を構築するベンチマークを提供することである。仕様適合とは、各ソフトウェアソリューションに必要なコンプライアンス関連資料（法的通知、ソースコードなど）を生成するようにプログラムが設計されていることを保証するものである。本文書は、「いつ」「どのように」ではなく、プログラムの「何」「なぜ」という側面に焦点を当てている。それにより、市場規模の異なるさまざまな組織が、その規模、目標、範囲に合った特定のポリシーとプロセスの内容を選択できる柔軟性が確保される。例えば、OpenChain 適合プログラムは、単一の製品ラインを対象としている場合もあれば、組織全体を対象としている場合もある。

本序章は仕様の背景をすべての OpenChain ユーザに向けて説明している。第 2 箇条は、本仕様書全体で使用される主要な用語を定義する。第 3 箇条は、適合を達成するためにプログラムが満たすべき要求事項を定義する。要求事項はそれを満たすために生成されなければならない 1 つ以上の検証資料（例えば、記録として残される書類）で構成される。検証資料の公開は必須ではないが、機密保持契約（NDA）の下で、組織は他者への提供を選択することが可能である。23

本文書は、200 人以上の貢献者からのフィードバックを受け、オープンな取り組みとして作成されたものである。開発履歴の詳細は仕様書用メーリングリストおよび Frequently Asked Questions (FAQ) で閲覧可能である。

情報技術 - OpenChain 仕様

1 適用範囲

本文書は、オープンソースソフトウェアで構成されるソフトウェアソリューションをやり取りする組織間の信頼関係を構築するためのベンチマークを提供するために、質の高いオープンソースライセンスコンプライアンスプログラムの主要な要求事項を規定している。

2 用語と定義

この文書では、以下の用語と定義が適用される。

2.11

コンプライアンス関連資料

コンプライアンスプログラムの成果物を表し、供給ソフトウェアに付属する資料の一群。

注：この資料には下記を1つ以上含むが、これらに限定されるものではない：ソースコード、帰属告知、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、およびSPDXドキュメント。

2.22

確認ライセンス

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を特定する適切な手法に従った結果として特定された一連のオープンソースライセンスソフトウェアライセンス。

2.33

OpenChain 適合

本文書のすべての要求事項を満たすプログラム

2.44

オープンソース

Open Source Initiative (OpenSource.org) によって公開されている Open Source Definition (opensource.org/osd 参照)、または Free Software Foundation によって公開されている Free Software Definition ([gnu.org/philosophy/free-sw.html](https://www.gnu.org/philosophy/free-sw.html) 参照)、または同様のライセンスを満たす1つ以上のライセンスの対象となるソフトウェア。

2.55

プログラム

組織のオープンソースライセンスコンプライアンス活動を構成する一連のポリシー、プロセス、および要員。

2.66

プログラム参加者

供給ソフトウェアについて、定義、コントリビュート、または準備する責任を持つ組織の従業員または契約者のこと。

注：組織によって、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（が、必ずしも限定されない）。

2.77

SPDX

Linux Foundation の SPDX (Software Package Data Exchange) Working Group が作成したフォーマット標準。関連するライセンスや著作権情報を含むソフトウェアパッケージの BOM（部品表）のやり取りに使用される（spdx.org 参照）。

2.88

供給ソフトウェア

組織が第三者（他の法人または個人）に対して配布するソフトウェア。

2.99

検証資料

既定の仕様要件が満たされていることを示す資料

ISO と IEC は、下記サイトにおいて標準化で使用する用語のデータベースを管理している。

- ISO Online browsing platform: <https://www.iso.org/obp> にて入手可能
- IEC Electropedia: <http://www.electropedia.org/> にて入手可能

3 要求事項

3.1 プログラムの基盤

3.1.1 ポリシー

供給ソフトウェアに対するオープンソースのライセンスコンプライアンスを管理する文書化されたオープンソースポリシーが存在していること。ポリシーが組織の内部で周知されること。

検証資料：

- ☐ 3.1.1.1 文書化されたオープンソースポリシー。
- ☐ 3.1.1.2 プログラム参加者にオープンソースポリシーの存在を（例えば、トレーニング、社内 wiki、またはその他の実践的なコミュニケーション手法を通じて）認識させる文書化された手順。

理由：

オープンソースポリシーを作成、記録、またプログラム参加者にオープンソースポリシーの存在を認識させるための手順が取られていることを確実にするため。ポリシーにどんな内容を含めるべきかの要求事項がここに提示されていないが、他のセクションでポリシーに関する要求事項が課せられる場合がある。

3.1.2 力量

組織は以下を行うこと。

- 当該プログラムの遂行とその効果に影響を及ぼす役割、および、その役割に対応した責任の特定；
- 各役割を果たすプログラム参加者の必要な力量の決定
- プログラム参加者が適切な教育、トレーニング、および／または経験に基づいて十分な力量を持っていることの確認
- 状況に応じて、必要な力量を獲得するための措置を実施
- 文書化された記録を力量のエビデンスとして保持

検証資料：

- ☐ 3.1.2.1 プログラム参加者の役割とその責任の文書化されたリスト。
- ☐ 3.1.2.2 各役割の力量を特定する文書。
- ☐ 3.1.2.3 各プログラム参加者の力量の評価を文書化した証拠。

理由：

プログラム参加者がプログラムにおけるそれぞれの役割と責任を果たす十分なレベルの力量を有していることを確認するため。

3.1.3 認識

組織はこのプログラム参加者が以下を認識していることを確認すること。

- オープンソースポリシー；
- 関連するオープンソースの目標；
- プログラムの有効性に対する参加者の貢献；
- プログラムの要求事項を遵守しないことの意味

検証資料：

- ☐ 3.1.3.1 プログラムの目的、プログラムにおける参加者の貢献、プログラムの不適合の影響を含む、プログラム参加者の意識を評価した証拠の文書。

理由：

プログラム参加者がプログラムにおけるそれぞれの役割と責任を果たす十分なレベルの認識度を有していることを確認するため。

3.1.4 プログラムの適用範囲

さまざまなプログラムは異なったレベルの適用範囲で管理することができる。例えば、単一の製品ライン、部署全体、あるいは、組織全体をプログラムが管理することが可能である。それぞれのプログラムに対する適用範囲の指定が明記されること。

検証資料：

- ☐ 3.1.4.1 プログラムの適用範囲と限界を明確に定義する文書。

理由：

組織のニーズの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提供するため。特定の製品ラインのためのプログラムを維持することを選択する組織もあれば、組織全体で提供されるソフトウェアを管理するためのプログラムを実施する組織もある。

3.1.5 ライセンス義務

各ライセンスによって付与される義務、制約および権利を決定するために、確認ライセンスを見直すプロセスが存在すること。

検証資料：

- 3.1.5.1 各確認ライセンスによって付与される義務、制約および権利を見直し、文書化するための手順書。

理由：

組織が直面する可能性のあるさまざまな使用事例（§ 3.3.2 で定義）について、各確認ライセンスに対するライセンス義務を見直し、特定するためのプロセスが存在することを確認するため。3.3.2

3.2 関連業務の定義と支援

3.2.1 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保持すること。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ができる手段を公開すること。

検証資料：

- 3.2.1.1 第三者がオープンソース ライセンスのコンプライアンスに関する問い合わせができる公開された方法（公開された連絡先メールアドレス、Linux Foundation のオープン コンプライアンス ディレクトリなど）。
- 3.2.1.2 第三者による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に対応するための内部手順書。

理由：

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い、組織が効果的に対応できる合理的な方法があることを確実にするため。

3.2.2 十分なリソース配分

プログラムタスクを特定し、リソースを確保すること。

- プログラムタスクを確実に実行するための役割を決定する。
- プログラムタスクに十分なリソースを配分する：
 - タスクを実行する時間が割り当てられている；および
 - 十分な予算が割り当てられている。
- ポリシーおよび支援タスクを見直し、更新するプロセスが存在する。
- 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法的専門知識が、そのような指導を必要とする人に利用可能である。
- オープンソースのライセンスコンプライアンスの問題を解決するためのプロセスが存在する。

検証資料：

- ☐ 3.2.2.1 当該プログラムの役割に携わる担当者、グループおよび部署の名称を記載した文書。
- ☐ 3.2.2.2 特定されたプログラムの役割に適切な人員配置がされ、十分な予算が確保されている。
- ☐ 3.2.2.3 オープンソースライセンスコンプライアンスに関する内部、および外部問題に対応するために利用可能な法的専門知識の特定。
- ☐ 3.2.2.4 オープンソースコンプライアンスに関する内部責任を割り当てた手順書。
- ☐ 3.2.2.5 不適合の見直しおよび是正処置を取り扱う手順書。

理由：

i) プログラムの責任が効果的にサポートされ、リソースが確保されていること、および ii) オープンソースコンプライアンスのベストプラクティスの変更に対応するために、ポリシーと支援プロセスが定期的に更新されることを確実にするため。

3.3 オープンソースコンテンツの見直しと承認

3.3.1 部品表 (Bill of Materials)

提供されるソフトウェアを構成する各オープンソースコンポーネント（およびその確認ライセンス）を含む部品表の作成および管理のプロセスが存在するものとする。

検証資料：

- ☐ 3.3.1.1 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特定、追跡、見直し、承認および情報保管のための手順書。
- ☐ 3.3.1.2 手順書が適切に遵守されていることを示す、供給ソフトウェアに対するオープンソースコンポーネントの記録。

理由：

供給ソフトウェアを構築するために使用されたオープンソースコンポーネントの部品表を作成、管理するためのプロセスが存在することを確実にするため。部品表は、供給ソフトウェアの配布に適用されるので、義務および制限を理解するために各コンポーネントのライセンス条項の体系的な見直しおよび承認をサポートするために必要とされる。

3.3.2 ライセンスコンプライアンス

プログラムは、プログラム参加者が供給ソフトウェアに関して遭遇する一般的なオープンソースライセンスの使用事例を管理できるものであること。これには、次のような場合が含まれる（リストはすべてを網羅しているわけではなく、またすべての使用事例が適用されるわけでもないことに注意すること）：

- バイナリ形式での配布；
- ソースコード形式での配布；
- 他のオープンソースと統合されており、追加のライセンス義務が発生する；
- 改変されたオープンソースを含む；

OpenChain 2.1 - オープンソースライセンス準拠の業界標準

- オープンソースまたは供給されたソフトウェア内で他のコンポーネントと相互作用する互換性のないライセンスの下での他のソフトウェアを含む；および／または
- 帰属要件のあるオープンソースを含む。

検証資料：

- 3.3.2.1 供給されたソフトウェアのオープンソースコンポーネントの一般的なオープンソースライセンスの使用事例の取り扱い手順書。

理由：

組織の一般的なオープンソースライセンスの使用事例に対処するためにプログラムが十分にロバストであることを確実にするため。この活動をサポートするための手順が存在し、その手順が守られていること。

3.4 コンプライアンス関連資料の作成と配布

3.4.1 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の作成プロセスが存在するものとする。

検証資料：

- 3.4.1.1 確認ライセンスの要求事項に従い、コンプライアンス関連資料が作成され、供給ソフトウェアとともに配布されるプロセスを記述した手順書。
- 3.4.1.2 提供された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ための手順書。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¹、あるいは確認ライセンスの要求事項によって定められた期間（どちらか長い方）保持されること。手順が適切に守られていることを示す記録が存在する。

理由：

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作成に商業的に妥当な努力が払われたことを確実にするため。

3.5 オープンソースコミュニティ活動への理解

3.5.1 コントリビューション

組織がオープンソースプロジェクトへのコントリビューションを検討する場合、以下を実施するものとする。

- オープンソースプロジェクトへのコントリビューションを管理する文書化されたポリシーが存在すること。
- ポリシーが組織の内部で周知されること。
- ポリシーを実行するプロセスがあること。

¹ ドメイン、法的管轄権、および／または顧客契約によって決定される。

検証資料：

組織がオープンソースプロジェクトへの貢献を許可している場合、以下のものが存在するものとする：

- ☐ 3.5.1.1 文書化されたオープンソースコントリビューションポリシー。
- ☐ 3.5.1.2 オープンソースコントリビューションを管理する手順書。
- ☐ 3.5.1.3 すべてのプログラム参加者に（例えば、トレーニング、社内 wiki、またはその他の実践的なコミュニケーション手法を通じて）オープンソースポリシーの存在を認識させる手順書。

理由：

組織がオープンソースのコントリビューションを許可する場合、コントリビューションポリシーの開発と実施に向けて十分に検討が行われることを意図する。オープンソースコントリビューションポリシーは、オープンソースポリシー全体の一部としても、あるいは、独自のポリシーとしても作成可能である。

3.6 仕様要求事項の遵守

3.6.1 適合

プログラムが OpenChain に適合しているとみなされるために、組織は、当該プログラムがこの文書に示された要求事項を満たしていることを確認するものとする。

検証資料：

- ☐ 3.6.1.13.1.4 で規定されたプログラムが本文書のすべての要求事項を満たしていることを確認する文書。3.1.4

理由：

組織が OpenChain に準拠したプログラムがあること宣言した場合、そのプログラムが本文書のすべての要求事項を満たしていることを確実にするため。それら要求事項のサブセットを満たしているだけでは不十分である。

3.6.2 期間

仕様書の本版に対応した OpenChain 適合のプログラムは、適合認証の取得日から 18 ヶ月間有効であるものとする。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。

検証資料：

- ☐ 3.6.2.1 プログラムが、適合認証取得から過去 18 ヶ月以内に、本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文書。

理由：

組織が長期的に適合性を主張したい場合、プログラムが最新の仕様書に準拠した状態を保つことが重要である。本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場合に、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ぐ。

Annex A

(参考)

本仕様書の言語翻訳について

世界的な採用を促進するために、仕様を異なる言語への翻訳を推奨しています。OpenChain はオープンソースプロジェクトとして機能しているため、翻訳のために時間と専門知識を提供してくれる人によって翻訳は行われています。翻訳は、i) CC-BY-4.0 ライセンスの条件の下で提供され、ii) プロジェクトの翻訳ポリシーと一致しています。ポリシーの詳細と利用可能な翻訳は OpenChain プロジェクトの wiki でご覧いただけます。