OPENCHAIN 仕様書

第 2.0 版

書式を変更: 蛍光ペン（なし）

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） **3**
著作権、ライセンス **3**
1)　はじめに **4**
2)　用語の定義 **5**
3)　満たすべき要件 **6**
1.0 プログラムの基盤 6
2.0 関連業務の定義と支援 8
3.0 オープンソースコンテンツのレビューと承認 9
4.0 コンプライアンス関連資料の作成と頒布 10
5.0 オープンソースコミュニティ活動への理解 11
6.0 仕様要件の遵守 12
付録 I: 本文書の翻訳について **13**

変更されたフィールド コード
変更されたフィールド コード
変更されたフィールド コード
変更されたフィールド コード
変更されたフィールド コード
変更されたフィールド コード
変更されたフィールド コード
変更されたフィールド コード
変更されたフィールド コード
変更されたフィールド コード
変更されたフィールド コード
変更されたフィールド コード

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

コメントの追加 [FH(1]: 原文は The がついていない。

変更されたフィールド コード

変更されたフィールド コード

変更されたフィールド コード

1) 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）の基幹要件を定義しており、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）の間に信頼構築の基礎を提供することを目的としています。組織の *プログラム*が本仕様に適合することにより、一つ一つのソフトウェアソリューションに必要とされる*コンプライアンス関連資料*（法的通知、ソースコードなど）を確実に生成するように *プログラム*が設計されていることを保証します。OpenChain の仕様は *プログラム*の「どのように」や「どのような時に」ではなく、「何」と「なぜ」の側面に焦点を当てています。これは、さまざまな市場に存在するさまざまな規模の組織において、規模、目標、スコープに合ったポリシーとプロセスを具体化できるような柔軟性をもたらすためです。例えば、*OpenChain 適合プログラム*は、組織の単一の製品ラインに対して適用することも、あるいは、組織全体に対して適用することもできます。

このセクションはすべての OpenChain ユーザに向けて仕様の背景を提供しています。セクション 2 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 は、適合を達成するために *プログラム*が満たすべき要件を定義しています。各要件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*証跡となる資料*（例えば、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*を公開する必要はありませんが、機密保持契約 (NDA) の下で、他者に提供することを選択することはできます。

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 以上のコントリビュータ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、および、Frequently Asked Questions (FAQ)でご覧いただけます。

変更されたフィールド コード
変更されたフィールド コード

2) 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、斜字体で表記しています。

***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。以下を 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。

***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適用することにより存在が確認された*オープンソース*ライセンスの一覧 。

***OpenChain 適合*（OpenChain Conformant）** – 本仕様書のすべての要件を満たす *プログラム*のこと。

***オープンソース*（Open Source）** – Open Source Initiative（OpenSource.org）によって公開されている Open Source Definition や Free Software Definition （Free Software Foundation によって公開）、または同様のライセンスの 1 つ以上のライセンスに従うソフトウェアのこと。

***プログラム*（Program）** – 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管理するポリシー、プロセス、および要員の集合。

***ソフトウェアスタッフ*（Software Staff）** – *供給ソフトウェア*について、定義、コントリビュート、または使えるように準備する責任を持つ組織の従業員または契約者のこと。組織にも依存するが、スタッフには（必ずしも限定されないが）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。

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のこと。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）** –o 組織が第三者 （他の法人または個人）に対して提供するソフトウェアのこと。

***証跡となる資料*（Verification Material）** – 与えられた要件を満足することを示す確証のこと。

コメントの追加 [FH(2]: 日本語フォントが MS ゴシックと MS 明朝が混ざっていますが、今後揃えられますか？
イタリックになっているのも今後戻されますか？

ひとまず、以下ではフォントは訂正していません。

書式を変更： 蛍光ペン（なし）

3) 満たすべき要件

1.0 プログラムの基盤

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。このポリシーは組織内で周知されていなければならない。**

証跡となる資料

- ☐ 1.1.1 文書化された*オープンソース*ポリシー。
- ☐ 1.1.2 *ソフトウェアスタッフ*が*オープンソース*ポリシーの存在を認識する文書化された手続き（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）。

論拠

*オープンソース*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*がその存在を認識することを確かなものにします。ポリシーに含めるべき内容についての要件はここで提示されませんが、他のセクションではポリシーに関する要件が課される場合があります。

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を特定する**
- **それぞれの役割を果たす担当者の必要な力量を決定する**
- **これらの担当者が適切な教育、トレーニング、経験に基づいて十分な力量を持っていることを確認する**
- **状況に応じて、必要な力量を獲得するための措置を講じる**
- **文書化された記録を力量のエビデンスとして保持する**

証跡となる資料

- ☐ 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。
- ☐ 1.2.2 各役割の力量を特定する文書。
- ☐ 1.2.3 それぞれの *プログラム*参加者の力量の評価を文書化したエビデンス。

論拠:

このような *プログラム*を担う参加者が各々の役割とその責任を果たす十分な力量を有していることを確かなものとするためです。

コメントの追加 **[FH(3]:** ISO9001 では、「力量」としている。

コメントの追加 **[FH(4]:** ISO9001 では、「役割」となっている。

1.3 認識

組織はこの *プログラム*への参加者が以下を認識していることを確認すること。

a) ***オープンソースポリシー***
b) **関連する*オープンソースの目標***
c) ***プログラム*の有効性に対する参加者の貢献**
d) ***プログラム*要件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*における参加者の貢献、*プログラム*の不適合の意味を含む各*プログラム要員*の認識度を評価したエビデンスとしての文書。

コメントの追加 [FH(5]: もとに戻しました。

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を果たす十分な認識レベルを有していることを確認するためです。

1.4 *プログラム*のスコープ

いろいろな *プログラム*は異なったレベルのスコープによって運用される。例えば、*プログラム*が、単一の製品ライン、部署全体、あるいは、組織全体を統制する可能性がある。それぞれの *プログラム*に対してスコープの指定を明記する必要がある。

コメントの追加 [工内6]: 論拠の説明から見ても、企業の中に複数のプログラムが併存するような想定は無理ではないか。

書式を変更: 蛍光ペン（なし）

証跡となる資料

☐ 1.4.1 *プログラム*のスコープと境界を明確に定義する文書。

論拠:
組織に必要なスコープに最適な *プログラム*を構築するための柔軟性をもたらすためです。ある組織は、特定の製品ラインのための *プログラム*を整備することを選択するかもしれません。一方、他の組織は組織全体の *供給ソフトウェア*を管理する *プログラム*を導入するかもしれません。

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が付与する義務、制約、および、権利を判断するプロセスが存在すること。**

証跡となる資料

☐ 1.51. それぞれの確認ライセンスが付与する義務、制約、および、権利をレビューし、文書として記録するための手続き文書。

論拠
組織が利用する可能性のあるさまざまなユースケースに合わせて *確認ライセンス*の義務をレビューし、特定するためのプロセスが存在することを確かなものとします。ユースケースの要件は、3.2 にて定義しています。

2.0 関連業務の定義と支援

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を行うことができる手段を公開すること。

証跡となる資料

- ☐ 2.1.1 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を可能とする公開された方法。（例えば、公開された連絡先メールアドレス、または Linux Foundation のオープンコンプライアンスディレクトリを通じて。）
- ☐ 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応答するための内部手続き文書。

論拠

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、組織が効果的に応答できる合理的な方法があることを確かなものとします。

2.2 十分なリソース配分

***プログラム*の関連業務を確認し、リソースを確保すること。**

- ***プログラム*の関連業務の確実な実行のために役割を決定すること。**
- ***プログラム*の関連業務に十分なリソースを配分すること。**
  - **業務を実行する時間**
  - **十分な予算を確保**
- **ポリシー、および、支援業務に関し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務的な指導が必要な時に専門家にアクセスできること。**
- ***オープンソース*のライセンスコンプライアンスの問題が発生したときに、それを解決するためのプロセスが存在していること。**

証跡となる資料

- ☐ 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ドキュメントが存在する。
- ☐ 2.2.2 *プログラム*の役割に適切な要員配置と十分な予算確保が行われている。
- ☐ 2.2.3 内部、および、外部で発生するライセンスコンプライアン問題に対応するための法務の専門家が特定できる。
- ☐ 2.2.4 コンプライアンスの組織内責任者をアサインする手続き文書が存在する。
- ☐ 2.2.5 コンプライアンスに違反する状況の調査や是正措置を行うための手続き文書が存在する。

論拠

(i) *プログラム*の遂行責任者が十分に支援され、リソース配分が行われること、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を確かなものとします。

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*コンポーネントの特定、追跡調査、レビュー、承認、および、情報保管のための手続き文書が存在する。
- ☐ 3.1.2 *供給ソフトウェア*に対して手続き文書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が存在する。

論拠

*供給ソフトウェア*を構成する*オープンソース*部品表を作成、管理するプロセスが存在することを確かなものとします。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、承認するために必要となります。そのようなレビューによって、*供給ソフトウェア*の頒布のさいに適用される義務や制約を理解することができます。

3.2 ライセンスコンプライアンス

当該 *プログラム*は、*供給ソフトウェアの ソフトウェアスタッフ*が利用する可能性のあるさまざまな*オープンソース*ライセンスのユースケースに対応することが求められる。ユースケースとしては、以下が含まれる（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ことに注意。）

- **バイナリ形態での頒布**
- **ソースコード形態での頒布**
- **コピーレフトの義務が発生する可能性のある他*オープンソース*との統合**
- **改変された*オープンソース*を含んでいる**
- ***供給ソフトウェア*内のコンポーネントとやりとりする*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**
- **帰属要求[1]のある*オープンソース*を含んでいる**

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*コンポーネントに応じ、さまざまな*オープンソース*ライセンスのユースケースを取り扱うための文書化された手続き。

論拠

当該 *プログラム*が組織内のさまざまな*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頑強であり、さらに、このような活動をサポートする手続きが存在し、かつ、それに従っていることを確かなものとします。

[1] 訳注：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。」

コメントの追加 [FH(7)]: 翻訳する側から見るとかっこいい言葉なので好きなのですが、一般的な読む立場の人にはわかりにくいので、共通的とかはいかがでしょうか。

コメントの追加 [工内8]: 1．5節では various となっている

書式を変更: 蛍光ペン（なし）

4.0 コンプライアンス関連資料の作成と頒布

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*の要件に従って*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、また、頒布するプロセスを記述した手続き文書。

- ☐ 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ための手続き文書。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[2]、あるいは、*確認ライセンス*の要件として定められた期間（どちらか長い方）保持することを計画。手続きが適切に守られていることを示す記録の存在。

論拠

*確認ライセンス*の要件に従い、*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かなものとします。

[2] 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。

5.0 オープンソースコミュニティ活動への理解

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考慮する場合、以下を行うこと。

- **_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ポリシー文書が存在する**
- **ポリシーが組織の内部で周知される**
- **ポリシーを実装するプロセスがある**

証跡となる資料

- ☐ 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。
- ☐ 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続き文書。
- ☐ 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*コントリビューションポリシーの存在を認識する文書化された手続き （例えば、トレーニング、内部 wiki、その他の実践的なコミュニケーション方法を通じて）。

論拠

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装に向けて十分に検討することが望まれます。*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できます。

6.0 仕様要件の遵守

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件を *プログラム*が満足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 要件 1.4 で指定した *プログラム*がこの仕様書のすべての要件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、それはこの仕様書のすべての要件を満たしていることを確かなもとするためです。要件のサブセットのみを満たしていることは十分とはいえません。

6.2 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。

証跡となる資料

- 6.2.1 当該 *プログラム*が、過去 18 ヶ月以内に適合認証を取得し、本仕様書の第 2 版のすべての要件を満たしていることを明確に宣言する文書。

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なら、最新の仕様書に準拠した状態を保つことが大切です。この要件は組織が継続して *プログラム*適合性を主張するさいに、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ぎます。

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 ページでご確認ください。

変更されたフィールド コード