OpenChain 仕様書詳細解説

– OpenChain Specification version 2.0 –

目次

はじめに

本書の目的

本書は、OpenChain 仕様について理解し、適合認証を目指す方のための、OpenChain 仕様書の解説書です。2020 年 10 月時点の最新版である OpenChain 仕様(バージョン 2.0)をもとに、仕様の原文、日本語訳、解説および参考資料について記載しています。また、より詳しい理解のため、OpenChain 仕様の各要求事項と共に、適合認証の際の questionnaire(質問)を掲載していますので、参考にしてください。

OpenChain 仕様について詳しく知りたいと思われている方、適合認証を目指して OSS コンプライアンス活動を推進されているすべての方々の一助になれば幸いです。

免責事項(Disclaimer)

日本語訳に関して、本書作成時点では、バージョン 2.0 の公式日本語訳が正式リリースされていないため、本書における日本語訳は、バージョン 1.2 の公式日本語訳を参考にしながら、筆者が翻訳したものです。OpenChain 仕様(バージョン 2.0)と本書との間で何らかの意味の違いがあった場合には、OpenChain 仕様(バージョン 2.0)が優先されます。

著作権、ライセンス

著者プロフィール

氏名	: 渡邊　歩(AYUMI Watanabe)
所属	: OpenChain Japan WG Planning SWG
連絡先(質問など)	: ayumi.waatnabe.ze@hitachi-solutions.com

謝辞

The author is grateful to Mark Gisi for his support. I also thank Nobuo Imada for advice and comments.

OPENCHAIN SPECIFICATION （OpenChain 仕様）

Version 2.0 （バージョン 2.0）

Establishing trust in the Open Source from which Software Solutions are built

（ソフトウェアソリューションの根源であるオープンソースへの信頼の確立）

1. Introduction （イントロダクション）

【オリジナル】

This specification defines the key requirements of a quality Open Source license compliance program. The objective is to provide a benchmark that builds trust between organizations exchanging software solutions comprised of Open Source software. Specification conformance provides assurance that a Program has been designed to produce the required Compliance Artifacts (i.e., legal notices, source code and so forth) for each software solution. The OpenChain Specification focuses on the "what" and "why" aspects of a Program rather than the "how" and "when". This ensures flexibility for different organizations of different sizes in different markets to choose specific policy and process content that fits their size, goals and scope. For instance, an OpenChain Conformant Program may address a single product line or the entire organization.

This introduction provides the context for all potential users. Section 2 defines key terms used throughout the Specification. Section 3 defines the requirements that a Program must satisfy to achieve conformance. A requirement consists of one or more Verification Materials (i.e., records) that must be produced to satisfy the requirement. Verification Materials are not required to be made public, though an organization may choose to provide them to others, potentially under a Non-Disclosure Agreement (NDA).

The Specification is developed as an open initiative with feedback received from over 150 contributors. Insight into its historical development can be obtained by reviewing the Specification mailing list and Frequently Asked Questions (FAQs).

【日本語訳】

本仕様書は、良質な OSS 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定義しています。その目的は、OSS 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とりする組織間における信頼関係を構築するためのベンチマークを提供することにあります。仕様に適合しているということは、各ソフトウェアソリューションに関して、*Program* が、要求される *Compliance Artifacts*(例：法的な告知、ソースコード等)を作成するようにできていることを保証します。OpenChain 仕様は、「どのように(how)」や「いつ(when))」よりも、*Program* の「何(what)」や「なぜ(why)」の側面に焦点を当てています。これにより、様々な市場の様々な規模の様々な組織が、特定のポリシーを選択し、その規模、目標、および範囲に適したコンテンツを実行できる柔軟性が保証されています。

本イントロダクションでは、すべての潜在ユーザ向けに背景(コンテキスト)を述べます。2 章では、本仕様書全体を通して使用される主要な用語を定義します。3 章では、適合認証を達成するため *Program* が満たすべき要求事項を定義します。要求事項は、要求を満たすために作成するべき1つないしは複数の *Verification Materials*(例：記録)により構成されています。*Verification Materials* は必ずしも組織外へ公開する必要はありませんが、組織は、守秘義務契約(NDA)に基づいて、他者に提供することを選択する場合があります。

本仕様書は、150 名を超える寄稿者からのフィードバックによる公開的な構想として作成されました。作成における過去の議論や詳細は、Specification のメーリングリストと Frequently Asked Questions (FAQs)で知ることができます。

【解説】

イントロダクションでは、OpenChain 仕様の目的と概要の説明、および本仕様書の構成について述べられています。

OpenChain は、The Linux Foundation 傘下のプロジェクトのひとつで、組織が OSS のライセンスコンプライアンスプログラムを構築するための指針を整備することを目的として活動しており、その活動のアウトプットとして、OSS コンプライアンスのために組織が満たすべき要件を示す OpenChain 仕様、チェックリスト、トレーニング資料や参考資料、認証プログラ

ムなどがあります。

ソフトウェアがより高度に、複雑になってきた昨今、ソフトウェアのサプライチェーンもまた複雑化しています。製品やサービスという形で世の中に対してリリースされるソフトウェアには、最終頒布者である組織の単一の開発チームにより開発されたソフトウェアだけではなく、開発委託先からの納入ソフトウェアやサードパーティーから購入した商用ソフトウェア、開発コミュニティから入手した OSS なども多数含まれ、「それらのソフトウェアすべてに含まれるすべての OSS に関して」、ライセンスを遵守した形で頒布することが求められます。このように複雑なサプライチェーンにより開発された製品やサービスにおいて確実にライセンスコンプライアンスを遵守するには、サプライチェーンを構成する企業・団体・組織がそれぞれの責任において、自身が頒布するソフトウェアに関して OSS ライセンスコンプライアンス上の「なすべきこと」を確実に実施し、ソフトウェアに含まれる OSS に関する必要な情報を提供することが必要です。

OpenChain 仕様は、組織が OSS ライセンスコンプライアンスを適切に実行するための要件を定義したものであり、この仕様に適合している組織は、OSS を適切に取り扱うことのできる組織として、信頼に値すると言えます。OpenChain 仕様の大きな特徴として、「あらゆる規模の組織、あらゆる市場に対応できること」を目的として作られているという点があります。このため、本仕様書には具体的な実施項目や粒度については規定されておらず、それは時として具体性に欠けると思われるかもしれません。この点について、本書では、できる限り参考情報としての具体例を提示し、読者に理解しやすい解説をすることを心がけています。

自身の組織が OpenChain 仕様を満たしているかどうかを知りたい場合は、Self-Certify(自己認証)にチャレンジしてみることをお勧めします。自己認証は、認証取得自体を目的としている必要はなく、自組織のプロセスの最適化に向けた課題抽出のためやヘルスチェックのためなどの目的で活用することもできます。認証適合を公にアナウンスしている企業・組織は Example Conformant Programs として OpenChain の Web サイトに掲載されています。

【参考】

- 「OpenChain Specification」(作成者：The OpenChain Project)
  https://wiki.linuxfoundation.org/_media/openchain/openchainspec-2.0.pdf
- 「OpenChain Conformance」(作成者：The OpenChain Project)
  https://www.openchainproject.org/get-started/conformance
- 「Example Conformant Programs」(作成者：The OpenChain Project)
  https://www.openchainproject.org/

2. Definitions （定義）

本仕様書で使用する特別な用語の定義について説明します。本書の以下の部分においては、特別な用語は *Compliance Artifacts* のようにイタリック体で表記しますが、「OSS」という用語は例外的に、通常の文章と同じ書式で記載しています。

本章の定義およびその日本語訳は、下記の記載ルールに基づいて記載されています。

（記載例）

“定義される用語” … 定義される用語の日本語訳	
OpenChain 仕様書における定義	OpenChain 仕様書における定義の日本語訳

下記は、本仕様書において定義されている特別な用語の定義とその日本語訳です。

“Compliance Artifacts” … コンプライアンス関連資料	
a collection of artifacts that represent the output of the Program for the Supplied Software. The collection may include (but is not limited to) one or more of the following: source code, attribution notices, copyright notices, copy of licenses, modification notifications, written offers, Open Source component bill of materials, and SPDX documents.	*Supplied Software* の *Program* のアウトプットを示す関連資料一式。一式には、ソースコード、帰属告知、著作権表示、ライセンスのコピー、改変告知、書面による申し出、OSS コンポーネント部品表、*SPDX* ドキュメントなどの資料の一つ、ないしは複数が含まれる（ただしこれに限らない）。

“Identified Licenses” … 確認されたライセンス	
a set of Open Source Software licenses identified as a result of following an appropriate method of identifying Open Source components from which the Supplied Software is comprised.	*Supplied Software* を構成する OSS コンポーネントを検出する適切な確認手法により存在が確認された、OSS ライセンス一式。

“OpenChain Conformant” … OpenChain 認証適合	
a program that satisfies all the requirements of this specification.	本仕様書のすべての要求事項を満たすプログラム。

“Open Source” … OSS	
software subject to one or more licenses that meet the Open Source Definition published by the Open Source Initiative (OpenSource.org) or the Free Software Definition (published by the Free Software Foundation) or similar license.	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。

“Program” … OSS プログラム	
the set of policies, processes and personnel that manage an organization’s Open Source license compliance activities.	組織の OSS 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、および人員の総称。

“Software Staff” … ソフトウェアスタッフ	
any organization employee or contractor that defines, contributes to or has responsibility for preparing Supplied Software. Depending on the organization, that may include (but is not limited to) software developers, release engineers, quality engineers, product marketing and product management.	*Supplied Software* 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（ただしこれに限らない）。

“SPDX” … Software Package Data Exchange / SPDX	
the format standard created by the Linux Foundation’s SPDX (Software Package Data Exchange) Working Group for exchanging license and copyright information for a given software package. A description of the SPDX specification can be found at www.spdx.org.	Linux Foundation の *SPDX* ワーキンググループによって作られた、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。

“Supplied Software” … 提供ソフトウェア	
software that an organization distributes to third parties (e.g., other organizations or individuals).	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。

“Verification Materials” … 証跡となる資料	
materials that demonstrate that a given requirement is satisfied.	与えられた要件が満たされていることを示す資料。

3. Requirements (要求事項)

【オリジナル】

1.0 Program Foundation

1.1 Policy

A written Open Source policy exists that governs Open Source license compliance of the Supplied Software. The policy must be internally communicated.

Verification Material(s):

- ☐ 1.1.1 A documented Open Source policy.
- ☐ 1.1.2 A documented procedure that makes Software Staff aware of the existence of the Open Source policy (e.g., via training, internal wiki, or other practical communication method).

Rationale:

To ensure steps are taken to create, record and make Software Staff aware of the existence of an Open Source policy. Although no requirements are provided here on what should be included in the policy, other sections may impose requirements on the policy.

【日本語訳】

1.0 *Program* の基本事項

1.1 ポリシー

***Supplied Software* の頒布について OSS ライセンスコンプライアンスを統制する OSS ポリシーが書面として存在していること。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。**

証跡となる資料(群):

- ☐ 1.1.1 文書化された OSS ポリシー
- ☐ 1.1.2 すべての *Software Staff* 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)OSS 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

論拠:

OSS ポリシーを作成・記録するステップが取られ、*Software Staff* に OSS ポリシーの存在を知らせることを確かなものにします。OSS ポリシーに含まれるべき内容についてこの要件はここで提示されませんが、他の節でポリシーに関する要件が課される場合があります。

【解説】

本項目は、組織における OSS ポリシーの作成および周知の方法について定義されています。

ポイントとなるのは下記の 2 点です。

(1) ポリシーは「文書化されたもの」であること

OSS コンプライアンスをチーム内の共通認識によりルーチンワーク的に行われる不確かなもののままにしておくのではなく、明文化された OSS ポリシー策定のため、企業理念や経営戦略を鑑みて、OSS によって実現したいことを組織内で議論した結果を反映させ、組織内で合意形成するプロセスを大切にしてください。

また、OSS ポリシーは実用的な文書であり、すべての *Software Staff* が簡単にアクセスでき、リファレンスとして活用できるものであることが必要なため、解りやすさや具体性が求められます。しかしながら、ポリシーがすべての詳細な OSS コンプライアンス業務を定義している必要はなく、例として、ポリシーを抽象的な概念や指針の記載に留め、具体的なオペレーションは「ガイドライン」として別途纏めることも、実例として良く実施されている方法です。

（2） 組織内で周知する手続きが文書化されていること

「文書化された、OSS 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」については、組織の OSS ポリシーが存在することおよびその場所(Wiki やドキュメントの URL など)が関係者の間で周知されていることが求められ、それらの情報が例えば、新規にプロジェクトに参画するメンバー向けの導入トレーニング等において共有されることが必要です。

「はじめに」で述べた通り、OpenChain 仕様書では、備えておくべき OSS ポリシーの内容や粒度についての規定はなく、「ある」か「ない」か、だけを対象としています。組織は、自分たちの目的や範囲、OSS の使い方などに合わせて独自の OSS ポリシーを作成し、活用できていれば良いと言えます。

【参考】

本項目で述べられている OSS ポリシーについて、ポリシーに含まれるべき内容についてここでは述べられていないため、具体的なイメージを掴んでいただくべく、以下に参考となるものを挙げておきます。

- 「Linux Foundation Compliance Program : Generic FOSS Policy」(作成者：The OpenChain Project)
  https://github.com/todogroup/policies/blob/master/linuxfoundation/lf_compliance_generic_policy.pdf
- 「The OpenChain Open Source Policy Template」(作成者：The OpenChain Project)
  https://github.com/OpenChain-Project/Reference-Material/tree/master/Policy-Templates/Official
- 「オープンソースビジネスに取り組む SI 企業のための企業ポリシー策定ガイドライン」(作成者：一般社団法人情報サービス産業協会（JISA））
  https://www.jisa.or.jp/Portals/0/report/16-J013.pdf
- 「企業のためのオープンソースガイド・オープンソース戦略の策定」(作成者：The Linux Foundation、TODO グループ)
  https://www.linuxfoundation.jp/resources/open-source-guides/setting-an-open-source-strategy/

===== 認証時の関連質問項目 (Conformance in Questions) ==========

【質問 1.a】(Spec Ref 1.1, 1.1.1)

Do you have a documented policy that governs open source license compliance of the Supplied Software distribution (e.g., via training, internal wiki, or other practical communication method)?

(訳)

Supplied Software の頒布について OSS ライセンスコンプライアンスを統制する文書化された OSS ポリシーがありますか？(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)

【質問 1.b】(Spec Ref 1.1.2)

Do you have a documented procedure that communicates the existence of the open source policy to all Software Staff?

(訳)

すべての *Software Staff* が OSS 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ありますか？

==========

【オリジナル】

1.2 Compliance

The organization shall:

- **Identify the roles and the corresponding responsibilities of those roles that affects the performance and effectiveness of the Program;**
- **Determine the necessary competence of person(s) fulfilling each role**
- **Ensure that these persons are competent on the basis of appropriate education, training, and/or experience;**
- **Where applicable, take actions to acquire the necessary competence; and**
- **Retain appropriate documented information as evidence of competence.**

Verification Material(s):

- ☐ 1.2.1 A documented list of roles with corresponding responsibilities for the different participants in the Program.
- ☐ 1.2.2 A document that identifies the competencies for each role.
- ☐ 1.2.3 Documented evidence of assessed competence for each Program participant.

Rationale:

To ensure that the identified participants fulfilling Program roles have obtained a sufficient level of competence for their respective roles and responsibilities.

【日本語訳】

1.2 コンプライアンス

組織において、以下の要件が満たされていること。

- ☐ ***Program* のパフォーマンス(実績)と有効性を主導する人員の役割とそれらの役割に対応する責任を定義すること**
- ☐ **各役割を担当する人員に求められる適性を決定すること**
- ☐ **適切な教育、トレーニング、および/または経験に基づいて、その役割に求められる適性を有している人員をアサインすること**
- ☐ **該当する場合は、求められる適性を得るための措置を講じること**
- ☐ **適性の証拠となる文書化された情報を保存すること**

証跡となる資料(群):

- ☐ 1.2.1 *Program* における人員の役割とそれに対応する責任に関する、文書化されたリスト
- ☐ 1.2.2 各役割に求められる適性を定義した文書
- ☐ 1.2.3 *Program* における人員に関する、適性評価結果の文書化されたエビデンス

論拠:

Program における役割を担当する人員が、各役割と責任に対して十分なレベルの適性を有していることを確かなものにします。

【解説】

本項目は、*Program* において必要となる役割とその責任を定義し、それらの各役割に対して求められる適性を定義した上で、各担当者がその適性を満たしているかどうかを評価することについて定義されています。役割だけでなくその適性を定義し、例として教育・トレーニングおよび/または経験という具体的な項目を挙げ、その適性を有する人員をアサインすること、としています。

以前のバージョン(Version 1.2)では、教育・トレーニングに関する内容は 1.2 項に規定されており、すべての *Software Staff* が受講必須なトレーニングについて、含まれるべきトピックや修了条件(期間および最新教育の修了者の割合の規定)が存在していましたが、それらの要求事項は『Prescriptive(規定的)』であり、トレーニングの実施方法にはもっと柔軟性を持たせたほうが良いという議論があり、本バージョン(Version 2.0)では削除されています。

ここでは、*Program* において必要となる役割について具体的な要求はありませんが、「Linux Foundation Compliance Program : Generic FOSS Policy」では例として、FOSS Steering Committee, FOSS Compliance Officer, FOSS Program Office 等、8 種類の役割が定義されています。役割に付随する責任の定義は、Open Source Review Board(OSRB)の例として、「OSS の適切に利活用するため、プロダクトデザインとライセンス義務について調査し、製品における OSS 利用の申請をレビューし承認する。OSBR は製品チームと連携し、調査に必要な情報を入手する。このことにより、製品チームがライセンス義務についてきちんと理解し、義務を履行することが保証される。」のように定められており、粒度や内容の参考にすることができます。

===== 認証時の関連質問項目 (Conformance in Questions) ==========

【質問 1.c】(Spec Ref 1.2.1)

Have you identified the roles and the corresponding responsibilities that affect the performance and effectiveness of the Program?

(訳)

Program のパフォーマンス(実績)と有効性を主導する役割とそれらの役割に対応する責任の定義がありますか？

【質問 1.d】(Spec Ref 1.2, 1.2.2)

Have you identified and documented the competencies required for each role?

(訳)

各役割に求められる適性を定義し、文書化していますか？

【質問 1.e】(Spec Ref 1.2, 1.2.3)

Have you documented evidence of assessed competence for each Program participant?

(訳)

各 *Program* 関係者に関する適性評価結果の文書化されたエビデンスがありますか？

==========

【オリジナル】

1.3 Awareness

The organization shall ensure that Program participants are aware of:

a) The Open Source policy;

b) Relevant Open Source objectives;

c) Their contribution to the effectiveness of the Program; and

d) The implications of not following the Program's requirements.

Verification Material(s):

☐ 1.3.1 Documented evidence of assessed awareness for each Program participants including the Program's objectives, ones contribution within the Program, and implications of Program non-conformance.

Rationale:

To ensure Program participants have obtained a sufficient level of awareness for their respective roles and responsibilities within the Program.

【日本語訳】

1.3 認識

***Program* の関係者が下記の内容を認識していること。**

a) OSS ポリシー

b) OSS 利活用の目的

c) *Program* の有効性に対する彼らの貢献

d) *Program* の要件に従わないことによる影響

証跡となる資料(群):

☐ 1.3.1 *Program* 関係者が、*Program* の目的、*Program* 内の貢献、および *Program* の要件に従わないことによる影響を認識していることを確認したことの、文書化されたエビデンス

論拠:

Program 関係者が、*Program* におけるそれぞれの役割と責任について十分なレベルの認識を有していること。

【解説】

本項目は、OSS ポリシーそのものおよび目的や貢献、ポリシーに従わないことによる影響について、*Program* 関係者が理解しており、意識して活動しているかどうかについて述べられています。以前のバージョン(Version 1.2)の 1.2 項で定義されていた教育・トレーニングに関する内容が、形を変えて本項目になったと解されます。

c)の *Program* の有効性に対する貢献については、「The OpenChain Open Source Policy Template」においてサンプルとして述べられている事柄として、ポリシーの背景としてある根本的な事項を理解すること、例としてメーリングリストやニュースなどからビジネス・ソフトウェア開発に関する最新動向を入手したり、トレーニングを受けたりすることで、*Program* の有効性に対して貢献することができる、とされています。

d)の不適合の場合の影響については、例として、不適切な形で OSS を利用した場合に著作権者から訴訟を起こされることや自分たちの独自プログラムを外部に開示しなければならなくなるリスク、関連して発生する組織の評判の失墜や金銭的なダメージ、サプライヤや顧客との間の契約不履行などが挙げられます。この d)をきちんと認識させることは、ライセンス違反等による *Program* への不適合を抑止する大きな力になります。

トレーニングの内容に関する具体的な要求事項はありませんが、OpenChain 仕様に準拠したトレーニングスライドのリファレンスとして OpenChain Curriculum が作成・公開されています。

【参考】

- 「OpenChain Curriculum」(作成者：The OpenChain Project)
  https://github.com/OpenChain-Project/Curriculum/blob/master/slides/openchain-curriculum-for-2-0.pdf
- 「FOSS トレーニング リファレンス スライド OpenChain 仕様書 2.0 版対応」(作成者：The OpenChain Project)
  https://github.com/OpenChain-Project/OpenChain-JWG/blob/master/Education_Material/Training/Training-FOSS-compl-process-jp.pptx

===== 認証時の関連質問項目 (Conformance in Questions) ==========

【質問 1.f (1.f.i- 1.f.iv)】(Spec Ref 1.3, 1.3.1)

Do you have evidence documenting the awareness of your personnel of the following topics?

- The open source policy and where to find it,
- The relevant open source objectives,
- The contributions expected to ensure the effectiveness of the Program,
- The implications of failing to follow the Program requirements,

(訳)

以下の項目について、担当者の認識を文書化したエビデンスはありますか？

- OSS ポリシーとその場所
- OSS 利活用の目的
- *Program* の有効性を確保するために期待される貢献
- *Program* の要件に従わなかった場合の影響

==========

【オリジナル】

1.4 Program Scope

Different Programs may be governed by different levels of scope. For example, a Program could govern a single product line, an entire department or an entire organization. The scope designation needs to be declared for each Program.

Verification Material(s):

- 1.4.1 A written statement that clearly defines the scope and limits of the Program.

Rationale:

To provide the flexibility to construct a Program that best fits the scope of an organization's needs. Some organizations could choose to maintain a Program for a specific product line while others could implement a Program to govern the Supplied Software of the entire organization.

【日本語訳】

1.4 *Program* の対象範囲

スコープの異なる *Program* が複数存在することができる。例として、*Program* は一つのプロダクトラインを対象としても良いし、部門全体や組織全体を対象としても良い。各 *Program* はそれぞれ、対象範囲が定められていること。

証跡となる資料(群):

- 1.4.1 *Program* の対象範囲と制限を明確に定義した文書

論拠:

組織の求める範囲に最適な *Program* を構築するため柔軟性が担保されていること。組織は、特定のプロダクトラインに合わせて *Program* をメンテナンスすることもできるし、一つの *Program* を組織全体の *Supplied Software* に適用することもできる。

【解説】

本項目は、*Program* の対象範囲に関する柔軟性の確保について定義されています。一般的に、組織においては様々な種類のソフトウェアが開発されており、プロジェクトにより OSS 利活用の目的や活用方法は様々です。このような状況において、*Program* は必ずしも組織において唯一のものである必要はなく、プロジェクト特性や目的、活用方法に応じて複数作成することが許容されており、本項目により各 *Program* の適用範囲を定めることで、柔軟性が担保されています。

範囲(Scope)については、「社外に対して頒布するすべての製品」や「社外に対するサービス提供においてサーバサイドで動作するプログラム」のように定義します。制限(limits)については、例として組織が複数のプロダクトラインを持っている場合に、「このコンプライアンスプログラムはプロダクトライン A にのみ適用されます(その他の製品には適用されません)。」という様に、Program の適用範囲を設定することを意味しています。

===== 認証時の関連質問項目 (Conformance in Questions) ==========

【質問 1.g】(Spec Ref 1.4)

Do you have a process for determining the scope of your Program?

(訳)*Program* の適用範囲を決めるプロセスがありますか？

【質問 1.h】(Spec Ref 1.4.1)

Do you have a written statement that clearly defines the scope and limits of the Program?

(訳)*Program* の適用範囲と制限を明示的に定義し、文書により宣言されていますか？

==========

【オリジナル】

1.5 License Obligations

A process exists for reviewing the Identified Licenses to determine the obligations, restrictions and rights granted by each license.

Verification Material(s):

- 1.5.1 A documented procedure to review and document the obligations, restrictions and rights granted by each Identified License.

Rationale:

To ensure a process exists for reviewing and identifying the license obligations for each Identified License for the various use cases an organization may encounter (as defined in requirement 3.2).

【日本語訳】

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、および権利を判断できるように、*Identified Licenses* をレビューするプロセスが存在すること。

証跡となる資料(群):

- 1.5.1 *Identified Licenses* それぞれが付与する義務、制約、および権利についてレビューし、文書として記録するための手続き文書

論拠:

Identified Licenses それぞれについて、組織が実施する可能性のあるさまざまなユースケース(要件 3.2 で定義されます)に対応したライセンスの義務をレビューおよび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。

【解説】

本項目は、OSS ライセンスの解釈のためのレビュープロセスについて定義されています。

以前のバージョン(Version 1.2)からの変更点として、「～for the various use cases an organization may encounter (as defined in requirement 3.2).」のように、3.2 項で定義されているユースケースとの関連性が明確に記されることになったことが挙げられます。ライセンス義務のレビューを行うべき役割について、ここでは記載がありませんが、例として、Open Source Review Board(OSRB)や Open Source Compliance Lead が第一段階的な評価を行い、疑問がある場合は知財・法務部門や組織外の法律専門家に相談する、というプロセスが一般的です。また、議論や検討の過程および決定した事柄を記録しておくことも必要です。この結果として、組織におけるライセンス毎の利用可否を定めたホワイトリスト/ブラックリストを作成することもあります。

OSS ライセンスの義務、制約、および権利はその OSS の使い方により異なるため、本項目では要件 3.2 で定義されているユースケース毎にそれらを整理しておくと便利です。日立製作所は、ライセンス毎に、ライセンス上許可されているユースケースとそれに伴う義務、制約および権利を構造化して整理したデータである OSS License Open Data を、OSS として公開しており、誰でも自由に入手して利用することができます。

【参考】

- 「OSS License Open Data」(作成者:Hitachi, Ltd.)
  https://github.com/Hitachi/open-license

===== 認証時の関連質問項目 (Conformance in Questions) ==========

【質問 1.i】(Spec Ref 1.5)

Do you have a process for reviewing open source license obligations, restrictions and rights?

(訳)

OSS ライセンスの義務、制約、および権利についてレビューするプロセスがありますか？

【質問 1.j】(Spec Ref 1.5.1)

Do you have a documented procedure to review and document the obligations, restrictions and rights?

(訳)

OSS ライセンスの義務、制約、および権利についてレビューし、文書として記録するための手続き文書がありますか？

==========

【オリジナル】

2.0 Relevant Tasks Defined and Supported

2.1 Access

Maintain a process to effectively respond to external Open Source inquiries. Publicly identify a means by which a third party can make an Open Source compliance inquiry.

Verification Material(s):

- 2.1.1 Publicly visible method that allows any third party to make an Open Source license compliance inquiry (e.g., via a published contact email address, or the Linux Foundation's Open Compliance Directory).
- 2.1.2 An internal documented procedure for responding to third party Open Source license compliance inquiries.

Rationale:

To ensure there is a reasonable way for third parties to contact the organization with regard to Open Source compliance inquiries and that the organization is prepared to effectively respond.

【日本語訳】

2.0 関連タスクの定義とサポート

2.1 アクセス

外部からの OSS ライセンスコンプライアンスに関する問い合わせにきちんと対応するプロセスをもつこと。第三者が OSS 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方法が公に示されていること。

証跡となる資料(群):

- 2.1.1 第三者が OSS 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ための公に示された方法(たとえば公開された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)。
- 2.1.2 OSS ライセンスコンプライアンスに関する第三者からの問い合わせへの対応に関する内部手続き文書

論拠:

OSS ライセンスコンプライアンスに関する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、またその組織が当該問合せに対してきちんと対応するように準備がされていること。

【解説】

本項目は、組織外の第三者からの OSS ライセンスコンプライアンスに関する問い合わせを受領する窓口と方法、および問い合わせに対して適切に対応するための準備について定義されています。組織外の第三者からの問い合わせは、例として、使用している OSS に関するコンプライアンス関連の質問や GPL 系のライセンス義務に基づくソースコードの請求など、多岐にわたり、それらに対してきちんと対応できるようになっていることが求められています。

第三者からの問い合わせを受領する窓口については、例にあるように、問い合わせ受領用の電子メールアドレスを社外向け Web サイトに掲載しておくことなどが求められています。しかしながら、このような問い合わせは必ずしも窓口に寄せられるわけではなく、営業担当やカスタマーサービス、開発エンジニアなどに対して直接問い合わせが来る可能性もあります。そのような場合において、各個人が自己判断で不適切な対応をすることが無いよう、関連するすべての人が、このような問い合わせを受けた場合の適切な対応方法を理解し実行することができるようにしておくことが重要です。

===== 認証時の関連質問項目 (Conformance in Questions) ==========

【質問 2.a】(Spec Ref 2.1, 2.2.1)

Have you assigned individual(s) responsible for receiving external open source compliance inquiries ("Open Source Liaison")?

(訳)

組織外部からの OSS コンプライアンス関連の問い合わせを受領する担当者("Open Source Liaison")がアサインされていますか？

【質問 2.b】(Spec Ref 2.1.1)

Is the Open Source Liaison function publicly identified (e.g. via an email address and/or the Linux Foundation's Open Compliance Directory)?

(訳)

Open Source Liaison について公に示されていますか（たとえば公開された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）？

【質問 2.c】(Spec Ref 2.1.2)

Do you have a documented procedure that assigns responsibility for receiving and responding to open source compliance inquiries?

(訳)

OSS ライセンスコンプライアンスに関する問い合わせの受領および対応に関する手続き文書がありますか？

==========

【オリジナル】

2.2 Effectively Resourced

Identify and Resource Program Task(s):

- **Assign accountability to ensure the successful execution of Program tasks.**
- **Program tasks are sufficiently resourced:**
  - **Time to perform the tasks have been allocated; and**
  - **Adequate funding has been allocated.**
- **A process exists for reviewing and updating the policy and supporting tasks;**
- **Legal expertise pertaining to Open Source license compliance is accessible to those who may need such guidance; and**
- **A process exists for the resolution of Open Source license compliance issues.**

Verification Material(s):

- 2.2.1 Document with name of persons, group or function in Program role(s) identified.
- 2.2.2 The identified Program roles have been properly staffed and adequate funding provided.
- 2.2.3 Identification of legal expertise available to address Open Source license compliance matters which could be internal or external.
- 2.2.4 A documented procedure that assigns internal responsibilities for Open Source compliance.
- 2.2.5 A documented procedure for handling the review and remediation of non-compliant cases.

Rationale:

To ensure: i) Program responsibilities are effectively supported and resourced and ii) policies and supporting processes are regularly updated to accommodate changes in Open Source compliance best practices.

【日本語訳】

2.2 効果的なリソース

***Program* 関連タスクを定義し、活動資源を提供する。**

- ***Program* 関連業務を確実に実行するための責任者をアサインする**
- ***Program* 関連業務に十分な活動資源が提供されていること。**
  - **業務を遂行するための時間が割り当てられている**
  - **適切な予算が割り当てられている**
- **ポリシーおよびサポート業務に対するレビューおよび更新するプロセスがあること**
- **必要とする人が、OSS ライセンスコンプライアンスに関する法律的な専門知識を利用できること**
- **OSS ライセンスコンプライアンスに関する懸案事項を解決するためのプロセスがあること**

証跡となる資料(群):

- 2.2.1 *Program* 関連の役割を担当する個人、グループまたは職務の名前が記載された文書
- 2.2.2 *Program* 関連の役割に対して人員が適切に配置され、適切な予算が割り当てられていること
- 2.2.3 組織内部または外部の OSS ライセンスコンプライアンスに関する問題に取り組むための法律的な専門知識が提供されていること
- 2.2.4 OSS コンプライアンスの内部責任者をアサインするための手続き文書
- 2.2.5 コンプライアンスに反する状況の調査や救済策を実施するための手続き文書

論拠:

i) *Program* 責任者が効果的にサポートされ活動資源が提供されていること、ii) OSS コンプライアンスのベストプラクティスにおける変化に追従するため、ポリシーおよびサポート業務が定期的に更新されていること。

【解説】

本項目は、*Program* を確実に遂行するためのリソースについて定義されています。

まず基本となるのは 1.2.1 項で述べられた *Program* における各役割であり、本項目ではそれらの役割に対して責任者(個人、グループまたは職務)をアサインし、かつそこに適切な人員配置、十分な活動資源(工数的および予算的リソース)が割り当てられていることを求めています。

また、2.2.3 項においては、法律的な専門知識を得ることができるようにすることが求められています。具体的には、懸案事項がある場合に専門家(例として、社内の法務部門や社外の法律事務所)に相談できるような仕組みを整えてあり、各担当者はまず Open Source Compliance Officer に懸案事項について相談し、Open Source Compliance Officer が外部有識者のアドバイスを受けるかどうかを決め、必要な場合は専門家に相談する、などのようなプロセスが想定されます。

2.2.5 項においては、コンプライアンスに関する懸案事項を解決するためのプロセスについて規定されており、これは例として、問い合わせを受けた場合、問い合わせ受領の連絡と解決までに要する時間の通知、インシデントの重要度に基づく優先度付け、解決に向けた対応の実施、履歴の記録などを行う手順などが定義され文書化されていることを求めています。

また、ベストプラクティスの変化に追従するため、定期的な更新を求めていることも特徴と言えます。

===== 認証時の関連質問項目 (Conformance in Questions) ==========

【質問 2.d】(Spec Ref 2.2.1)

Have you documented the persons, group or function supporting the Program role(s) identified?

(訳)

Program における各役割を担当する個人、グループまたは職務を記した文書がありますか？

【質問 2.e】(Spec Ref 2.2.2)

Have the identified Program roles been properly staffed and has adequate funding provided.?

(訳)

Program における各役割には、適切な人員が配置されており、適切な予算が割り当てられていますか？

【質問 2.f】(Spec Ref 2.2.3)

Is legal expertise pertaining to internal and external open source compliance identified?

(訳)

組織内部および外部の OSS コンプライアンスに関する法律的な専門知識(を得る方法)が定義されていますか？

【質問 2.g】(Spec Ref 2.2.4)

Do you have a documented procedure assigning internal responsibilities for Open Source compliance?

(訳)

OSS コンプライアンスの内部責任者をアサインするための手続き文書がありますか？

【質問 2.h】(Spec Ref 2.2.5)

Do you have a documented procedure for handling review and remediation of non-compliant cases?

(訳)

コンプライアンスに反する状況の調査や救済策を実施するための手続き文書がありますか？

==========

【オリジナル】

3.0 Open Source Content Review and Approval

3.1 Bill of Materials

A process exists for creating and managing a bill of materials that includes each Open Source component (and its Identified Licenses) from which the Supplied Software is comprised.

Verification Material(s):

- 3.1.1 A documented procedure for identifying, tracking, reviewing, approving, and archiving information about the collection of Open Source components from which the Supplied Software is comprised.
- 3.1.2 Open Source component records for the Supplied Software that demonstrates the documented procedure was properly followed.

Rationale:

To ensure a process exists for creating and managing an Open Source component bill of materials used to construct the Supplied Software. A bill of materials is needed to support the systematic review and approval of each component's license terms to understand the obligations and restrictions as it applies to the distribution of the Supplied Software.

【日本語訳】

3.0 OSS コンテンツのレビューと承認

3.1 OSS コンポーネント部品表(Bill of Materials / BoM)

OSS コンポーネント部品表を作成および管理するためのプロセスが存在すること。この OSS コンポーネント部品表には、*Supplied Software* を構成する各 OSS コンポーネント(およびその *Identified Licenses*)が含まれる。

証跡となる資料(群):

- 3.1.1 *Supplied Software* を構成する OSS コンポーネントについて情報を特定し、追跡し、レビューし、承認し、保管するための手続き文書
- 3.1.2 *Supplied Software* に対し、文書化された手続きが適正に実施されていることを示す OSS コンポーネントの記録

論拠:

Supplied Software に使用される OSS コンポーネントの部品表を作成および管理するためのプロセスが存在すること。部品表は、各コンポーネントのライセンス条件に対する体系的レビューと承認を手助けする上で必要となります。そのようなレビューによって、*Supplied Software* を頒布する際に適用される義務、制約が理解されます。

【解説】

本項目は、OSS コンプライアンス遵守のために必要な OSS コンポーネント部品表の作成について定義しています。頒布するソフトウェアに含まれるすべての OSS コンポーネントについて、コンポーネント情報および付帯情報を一覧化したリストを OSS コンポーネント部品表といいます。OSS コンポーネント部品表の必須構成要素として、本項目では OSS コンポーネントおよびその *Identified Licenses* と定義されていますが、それ以外にも、頒布時に適用される義務や制約を理解するため、ユースケースや改変の有無などが一緒に管理されているとより便利です。さらに、取得元情報や依存関係のリスト、使用方法など、詳細な管理のために管理しておいたほうが良い情報は多数ありますが、一方でこれらの情報を漏れなく収集し管理するには非常に多くの工数がかかります。開発現場に大く収集し管理するには非常に多くの工数がかかります。開発現場に大きな負担を強いることのない様、収集する情報の種類を最小限に抑えたり、ツールなどを使っ

て自動化したりする工夫を検討してください。

また、OSS コンポーネント部品表は、組織間のソフトウェア授受に伴う関連情報のやりとりの方法としても期待されているため、*SPDX* のフォーマットで作成している企業もあります。*SPDX* は記載するべき情報が多く作成が困難な場合は、*SPDX* の項目の中でもより必須なものだけを選択した *SPDX Lite* のフォーマットを使用することも検討してください。

【参考】

- 「A Template for Approval Request Form For The Use of Free and Open Source Software」(作成者：The Linux Foundation Open Compliance Program)
  https://github.com/todogroup/policies/blob/master/linuxfoundation/lf_compliance_approval.pdf
- 「The Software Package Data Exchange® (SPDX®)」(作成者：SPDX Workgroup a Linux Foundation Project)
  https://spdx.dev/
- 「SPDX-Lite」(作成者：OpenChain Japan WG License Info Exchange SWG)
  https://github.com/OpenChain-Project/Japan-WG-General/tree/master/License-Info-Exchange

===== 認証時の関連質問項目 (Conformance in Questions) ==========

【質問 3.a】(Spec Ref 3.1.1)

Do you have a documented procedure for identifying, tracking and archiving information about the collection of open source components from which a Supplied Software release is comprised?

(訳)

Supplied Software を構成する OSS コンポーネントについて情報を特定し、追跡し、レビューし、承認し、保管するための手続き文書がありますか？

【質問 3.b】(Spec Ref 3.1.2)

Do you have open source component records for each Supplied Software release which demonstrates the documented procedure was properly followed?

(訳)

Supplied Software リリースに対し、文書化された手続きが適正に実施されていることを示す OSS コンポーネントの記録がありますか？

==========

【オリジナル】

3.2 License Compliance

The Program must be capable of managing common Open Source license use cases encountered by Software Staff for Supplied Software, which may include the following use cases (note that the list is neither exhaustive, nor may all of the use cases apply):

- **distributed in binary form;**
- **distributed in source form;**
- **integrated with other Open Source such that it may trigger copyleft obligations;**
- **contains modified Open Source;**
- **contains Open Source or other software under an incompatible license interacting with other components within the Supplied Software; and/or**
- **contains Open Source with attribution requirements.**

Verification Material(s):

- 3.2.1 A documented procedure for handling the common Open Source license use cases for the Open Source components of the Supplied Software.

Rationale:

To ensure the program is sufficiently robust to handle an organization's common Open Source license use cases. That a procedure exists to support this activity and that the procedure is followed.

【日本語訳】

3.2 ライセンスコンプライアンス

***Program* は、ソフトウェアスタッフが扱う *Supplied Software* の共通的な OSS ライセンスのユースケースに対応できること。共通的ライセンスの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）**

- **バイナリ形式での頒布**
- **ソースコード形式での頒布**
- **コピーレフトの義務を生じうる他の OSS と統合されている**
- **改変された OSS を含んでいる**
- ***Supplied Software* 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 OSS 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 OSS を含んでいる**

証跡となる資料(群):

- 3.2.1 *Supplied Software* の各リリースの OSS コンポーネントに対し、共通的な OSS ライセンスのユースケースを取り扱うための手続き

論拠:

その ***Program*** が組織における共通的 OSS ライセンス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。

【解説】

本項目は、各ユースケースにおける OSS ライセンスの対応に関する手続きについて定義されています。共通的なユースケースとしてバイナリ形式での頒布、ソースコード形式での頒布など 6 種類が列挙されていますが、「このリストは網羅

的ではない」と明言されている通り、この他にも組織において実施する可能性のあるユースケースがあれば、それについても検討する必要がありますし、逆に、例示された中に実施する可能性がないユースケースがあれば、それは検討の対象外として差し支えありません。

===== 認証時の関連質問項目 (Conformance in Questions) ==========

【質問 3.c (3.c.i – 3.c.vi)】(Spec Ref 3.2, 3.2.1)

Have you implemented a procedure that handles at least the following common open source license use cases for the open source components of each Supplied Software release?

- distributed in binary form;
- distributed in source form;
- integrated with other open source such that it may trigger copyleft obligations;
- contains modified open source;
- contains open source or other software under an incompatible license interacting with other components within the Supplied Software;
- contains open source with attribution requirements.

(訳)

各 *Supplied Software* のリリースにおいて、少なくとも以下のような共通的な OSS ライセンスのユースケースを取り扱うための手続きがありますか？

- バイナリ形式での頒布
- ソースコード形式での頒布
- コピーレフトの義務を生じうる他の OSS と統合されている
- 改変された OSS 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 OSS やその他のソフトウェアを含んでいる**
- **帰属要求のある OSS を含んでいる**

==========

【オリジナル】

4.0 Compliance Artifact Creation and Delivery

4.1 Compliance Artifacts

A process exists for creating the set of Compliance Artifacts for the Supplied Software.

Verification Material(s):

- 4.1.1 A documented procedure that describes the process under which the Compliance Artifacts are prepared and distributed with the Supplied Software as required by the Identified Licenses.
- 4.1.2 A documented procedure for archiving copies of the Compliance Artifacts of the Supplied Software – where the archive is planned to exist for a reasonable period of time1 since the last offer of the Supplied Software; or as required by the Identified Licenses (whichever is longer). Records exist that demonstrate the procedure has been properly followed.

Rationale:

To ensure reasonable commercial efforts have been instituted in the preparation of the Compliance Artifacts that accompanies the Supplied Software, as required by the Identified Licenses.

【日本語訳】

4.0 *Compliance Artifacts* の作成と提供

4.1 *Compliance Artifacts*

***Supplied Software* に対し、*Compliance Artifacts* 一式を作成するプロセスがあること。**

証跡となる資料(群):

- 4.1.1 *Identified Licenses* の要求に基づいて *Compliance Artifacts* を用意し *Supplied Software* とともに頒布するプロセスに関する文書化された手続き文書
- 4.1.2 *Supplied Software* の *Compliance Artifacts* の複製を保管するための文書化された手続き文書、ここで、保管されたものは *Supplied Software* が提供されている間、または *Identified Licenses* が要求する期間(のいずれか長いほうの期間)において保持されるものとする(領域や法的管轄、顧客との契約による)。手続きが適切に実施されている記録をとること。

論拠:

Identified Licenses の要求に基づいて *Compliance Artifacts* を準備するために合理的な商業的努力がなされていること

【解説】

本項目は、*Compliance Artifacts* の作成および頒布に関して定義されています。ソースコードや帰属告知、著作権表示等の必要なすべての情報・ドキュメントが、*Supplied Software* と共に頒布されるためのプロセスについて定義されていることを求めています。

「合理的な商業的努力」という言葉は法律文書や契約書等でよく使われる言葉ですが、これは「商業上、またはその業界において、合理的または相当と考えられる手段を講ずる」ことを要求しており、結果としての 100%完璧な正解を求めているものではないと解されます。これは、OSS コンプライアンスに関する課題が、例として OSS のソースコードに必要なライセンス情報のすべてが含まれていない場合など、必ずしも自身の努力によって解決することができる課題ばかりではないことを考慮し、OpenChain 仕様上の要求事項としては、それらに対して合理的な範囲で手段を講じることのみとしています。一見、救済措置のようにも見えますが、一方で、例として顧客による監査などにおいては組織が合理的な努力をしたかどうかを、業界における標準的なレベルをもとに判断されるため、業界動向や周囲のレベルに追随しておく必

要があり、高い目標を目指す必要があることも忘れてはなりません。

Compliance Artifacts の保管期間については、「*Supplied Software* が提供されている間、または *Identified Licenses* が要求する期間の、いずれか長いほうの期間」としており、さらに注釈で「領域や法的管轄、顧客との契約による」と補足されています。「*Identified Licenses* が要求する期間」については、例として GNU General Public License version 3 の「最低 3 年間または当該モデルの補修用部品またはカスタマーサポートを提供している間のいずれか長い方の期間」が挙げられますが、注釈にある通り、顧客との契約がそれ以上の期間の保管を求めている場合などはそれに従う必要があります。また、以前のバージョン(Version 1.2)では「(*Compliance Artifacts* の写しが)容易に取り出すことができる」という規定があり、本バージョン(Version 2.0)では削除されたものの、第三者からの要求に応じていつでも提供できることは引き続き必要であると解されます。

===== 認証時の関連質問項目 (Conformance in Questions) ==========

【質問 4.a】(Spec Ref 4.1.1)

Do you have a documented procedure that describes a process that ensures the Compliance Artifacts are distributed with Supplied Software as required by the Identified Licenses?

(訳)

Identified Licenses の要求に基づいて *Compliance Artifacts* を *Supplied Software* とともに頒布するプロセスに関する文書化された手続き文書がありますか？

【質問 4.b】(Spec Ref 4.1.2)

Do you archive copies of the Compliance Artifacts of the Supplied Software?

(訳)

Supplied Software の *Compliance Artifacts* の複製を保管していますか？

【質問 4.c】(Spec Ref 4.1.2)

Are the copies of the Compliance Artifacts archived for at least as long as the Supplied Software is offered or as required by the Identified Licenses (whichever is longer)?

(訳)

Compliance Artifacts の複製は、少なくとも、*Supplied Software* が提供されている間または *Identified Licenses* が要求する期間(のいずれか長いほうの期間)において保管されていますか？

==========

【オリジナル】

5.0 Understanding Open Source Community Engagements

5.1 Contributions

If an organization considers contributions to Open Source projects then

- **a written policy exists that governs contributions to Open Source projects;**
- **the policy must be internally communicated; and**
- **a process exists that implements the policy**

Verification Material(s):

If an organization permits contributions to Open Source projects then the following must exist:

- 5.1.1 a documented Open Source contribution policy;
- 5.1.2 a documented procedure that governs Open Source contributions; and
- 5.1.3 a documented procedure that makes all Software Staff aware of the existence of the Open Source contribution policy (e.g., via training, internal wiki, or other practical communication method).

Rationale:

When an organization permits Open Source contributions we want to ensure the organization has given reasonable consideration to developing and implementing a contribution policy. The Open Source contribution policy can be made a part of the overall Open Source policy or be its own separate policy.

【日本語訳】

5.0 OSS コミュニティへの(積極的な)関わり方の理解

5.1 コントリビューション

組織が OSS 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、

- **OSS プロジェクトに対するコントリビューションを統制する文書化されたポリシーがあること**
- **そのポリシーが組織内に周知されていること**
- **そのポリシーを遂行するプロセスがあること**

証跡となる資料(群):

OSS 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、以下が存在すること。

- 5.1.1 文書化された OSS コントリビューションポリシー
- 5.1.2 OSS へのコントリビューションを統制する文書化された手続き文書
- 5.1.3 すべての *Software Staff* に OSS コントリビューションポリシーの存在を認識させるための文書化された手続き文書(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)

論拠:

組織が OSS へのコントリビューションを容認する際は、組織がコントリビューションポリシーの策定と遂行に対して適正な検討を行うことを求める。OSS コントリビューションポリシーは包括的な OSS ポリシーの一部として作成しても良いし、分離された別個のポリシーとしても良い。

【解説】

本項目は、OSS コミュニティへのコントリビューション(貢献)について定義されています。ここでいうコントリビューションとは、会社としてのプログラム(ソースコードやパッチなど)の提供およびコミュニティに対するエンジニアの時間と労力での貢献の両方を意味しています。会社としてのコントリビューションの場合、そのコントリビューションが自社の利益を損なわないこと、自社の知的財産権を侵害しないこと、などについて注意が必要であり、それらのリスクを事前に検討するた

め、コントリビューションの計画を立案し、検討するためのプロセスを定義しておくと良いでしょう。また、エンジニアがコントリビューションポリシーの存在を知らず、独自の判断においてコントリビューションを実施することが無いよう、すべての *Software Staff* にその存在を周知しておく必要があります。

===== 認証時の関連質問項目 (Conformance in Questions) ==========

【質問 5.a】(Spec Ref 5.1)

Do you have a policy that governs contributions to open source projects on behalf of the organization?

(訳)

組織として OSS プロジェクトへのコントリビューションを行うことを統制するポリシーがありますか？

【質問 5.b】(Spec Ref 5.1.2)

Do you have a documented procedure that governs Open Source contributions?

(訳)

OSS へのコントリビューションを統制する文書化された手続き文書がありますか？

【質問 5.c】(Spec Ref 5.1.3)

Do you have a documented procedure that makes all Software Staff aware of the existence of the Open Source contribution policy?

(訳)

すべての *Software Staff* に OSS コントリビューションポリシーの存在を認識させるための文書化された手続き文書がありますか？

==========

【オリジナル】

6.0 Adherence to the Specification Requirements

6.1 Conformance

In order for a Program to be deemed OpenChain Conformant, the organization must affirm that the program satisfies the requirements presented in this specification.

Verification Material(s):

- 6.1.1 A document affirming the Program specified in requirement 1.4 satisfies all the requirements of this specification.

Rationale:

To ensure that if an organization declares that it has a program that is OpenChain Conforming, that such program has met all the requirements of this specification. The mere meeting of a subset of these requirements would not be considered sufficient.

【日本語訳】

6.0 OpenChain 要求事項への適合

6.1 適合

組織が OpenChain に適合していると認定されるためには、本 OpenChain 仕様書に記載された基準を満たす *Program* を有していることを確認する必要がある。

証跡となる資料(群):

- 6.1.1 本仕様書 1.4 項で定義された *Program* が、本 OpenChain 仕様書のすべての要求事項を満たしていることを示す文書

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十分とはみなされません。

【解説】

本項目は、OpenChain 仕様への適合について定義されています。組織が OpenChain 仕様に適合しているということは、本仕様書の要求事項すべてを満たしていることを意味し、そのうちの一部だけを満たしていても、適合しているとは言えません。

===== 認証時の関連質問項目 (Conformance in Questions) ==========

【質問 6.a】(Spec Ref 6.1.1)

Do you have documentation confirming that your Program meets all the requirements of this specification?

(訳)

Program が本仕様書のすべての要求事項を満たしていることを示す文書がありますか？

==========

【オリジナル】

6.2 Duration

A Program that is OpenChain Conformant with this version of the specification will last 18 months from the date conformance validation was obtained. The conformance validation registration procedure can be found on the OpenChain project's website.

Verification Material(s):

- 6.2.1 A document affirming the Program meets all the requirements of this version of the specification (version 2.0), within the past 18 months of obtaining conformance validation.

Rationale:

It is important for the organization to remain current with the specification if that organization wants to assert program conformance over time. This requirement ensures that the program's supporting processes and controls do not erode if an organization continues to assert program conformance over time.

【日本語訳】

6.2 持続期間

***Program* の本バージョンの要求事項への適合は、認証が取得された日から 18 か月の間持続する。適合認証登録の手続きは OpenChain プロジェクトの Web サイトで参照できる。**

証跡となる資料(群):

- 6.2.1 ***Program*** が本バージョン(Version 2.0)の要求事項のすべてを満たし、18 か月以内に適合認証を取得したことを示したドキュメント

論拠:

その組織が一定期間を越えて ***Program*** の適合を主張したい場合、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、適合している組織が適合を一定期間越えて主張する場合にその ***Program*** が支えるプロセスや統制機能が損なわれないことを確かなものにします。

【解説】

本項目は、OpenChain 仕様の適合認証の持続期間について定義されています。OpenChain 仕様の適合認証の有効期間は認証取得時から 18 か月であり、その期間を過ぎると認証は失効し、組織が認証の維持を希望する場合は、再度認証取得しなければなりません。本要求事項の目的は、組織の ***Program*** が長期間にわたって要件を満たし続けていることを定期的にチェックすることにあります。時間の経過に伴う外的環境の変化や組織そのものの変化により、***Program*** が認証適合しなくなる可能性があるためです。

一度取得した認証の有効期間の間に次のバージョンの OpenChain 仕様がリリースされたとしても、上位互換が保証されていないため、あくまで前のバージョンでの認証適合として扱われ、更新の際にはその時の最新バージョンでの認証適合を目指すことになります(ただし、取得時の最新バージョン以外の認証を取得することも実務上可能です)。

【参考】

OpenChain 仕様の適合認証に関する情報は下記から参照できます。

- OpenChain 仕様に関するよくある質問
  https://www.openchainproject.org/resources/faq
- OpenChain 仕様適合認証(自己認証)
  https://certification.openchainproject.org

- OpenChain 仕様適合認証適合認証を受けた組織の一覧
  https://certification.openchainproject.org/certified.html?locale=en

===== 認証時の関連質問項目（Conformance in Questions）=====

【質問　6.b】（Spec Ref 6.2.1）

Do you have documentation confirming that your Program conformance was reviewed within the last 18 months?

（訳）

Program の適合性が 18 か月以内にレビューされたことを示す文書がありますか？

==========

--- 以上 ---

OpenChain Japan WG について

- Web ページ

  https://openchain-project.github.io/OpenChain-JWG/

- メーリングリストの参加方法

各メーリングリストに参加するには、それぞれ下記のアドレスにメールを送信してください。本文の記載は不要です。

- ✓ OpenChain Japan WG ML: japan-wg+subscribe@lists.openchainproject.org
- ✓ FAQ SG ML: japan-sg-faq+subscribe@lists.openchainproject.org
- ✓ ライセンス情報 SWG ML: japan-sg-licensing+subscribe@lists.openchainproject.org
- ✓ Planning SWG ML: japan-sg-planning+subscribe@lists.openchainproject.org
- ✓ Tooling SWG ML: japan-sg-tooling+subscribe@lists.openchainproject.org

- Slack

  https://openchain-japanwg.slack.com/