OpenChain Japan WG　第３回オンライン会合

OpenChain仕様解説

2020/10/15

OpenChain Japan WG Planning SWG
渡邊 歩

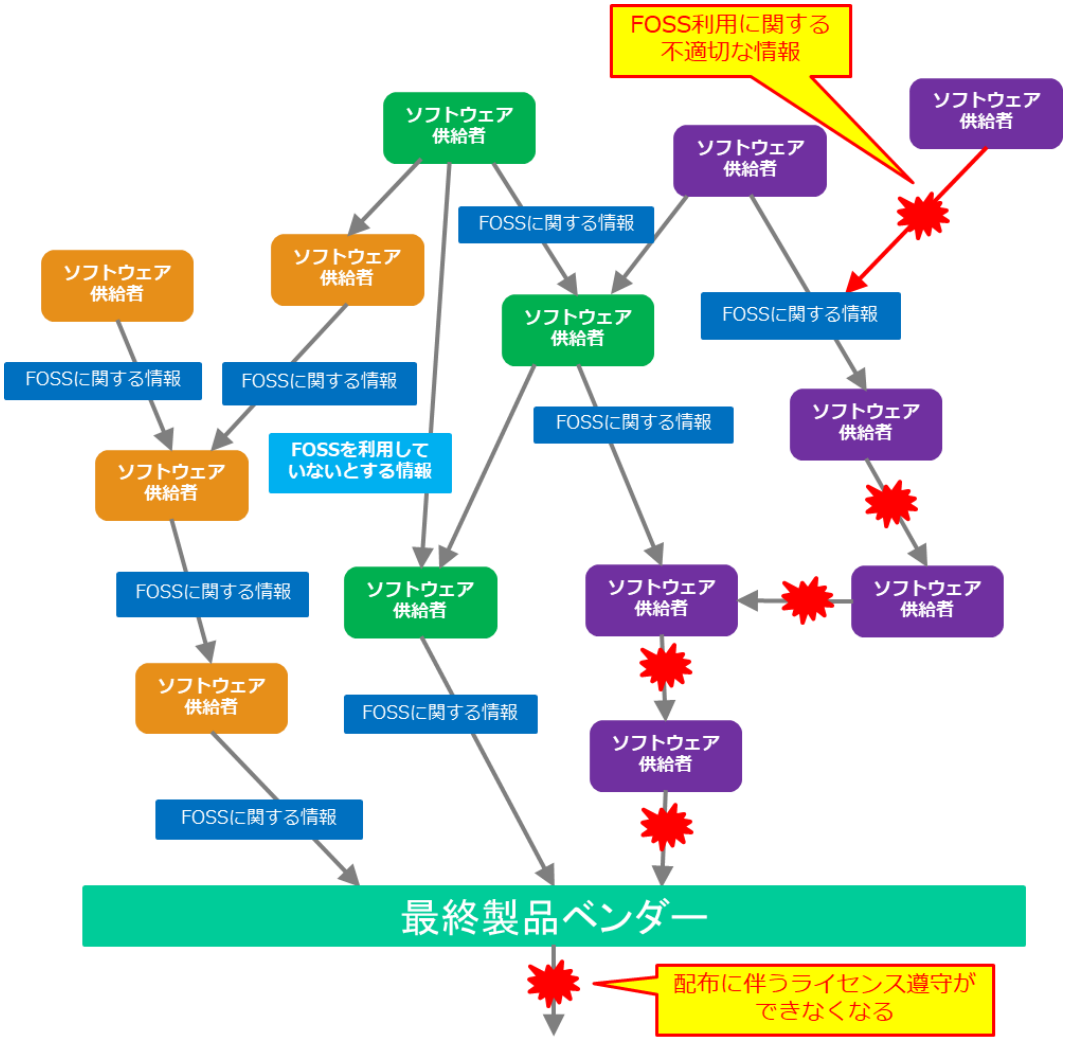
Contents

OpenChainおよびOpenChain仕様について、策定の背景や基礎となる内容について説明します。

1．OpenChain仕様概要

1-1 背景

■ ソフトウェアのサプライチェーンの抱える課題



サプライチェーンにおいて
- OSSの不適切な利用
- ライセンス情報の不足

があると、
最終製品を作り上げる段階で大きな問題に

- ✓ 最終製品が出荷できなくなる事態
- ✓ 第三者やOSSの著作権者からの指摘

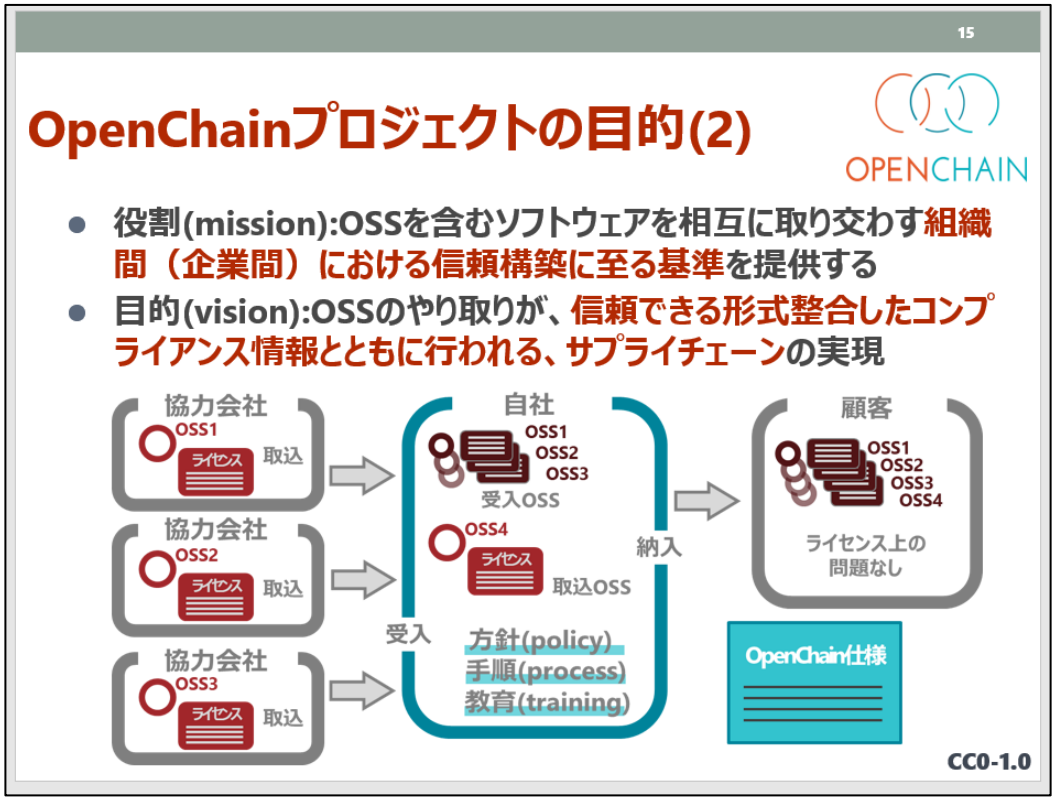
- サプライチェーンの上流段階で問題を把握して対策を講じることが重要
- サプライチェーンを構成する企業・団体それぞれがすべきことを的確に実施し、相互に**信頼関係を構築**し、互いに**適切な情報や必要な素材**（たとえばソースコードなど）**の受け渡し**をしっかりと行う事が重要

1 - 2 OpenChainとは①

■ OpenChainとは

【OpenChainとは】

- Linux Foundation傘下のプロジェクトのひとつ(2016年～)
- 組織が「OSS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いる



1 - 2 OpenChainとは②

OPENCHAIN

■ ビジョンとミッション (https://www.openchainproject.org/about)

- Vision(ビジョン/目的)
  OSS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
- Mission(ミッション/役割)
  OSS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

OpenChainの3本の柱

Specification(仕様)	Conformance(適合)	Curriculum(教育)
組織内に確立すべきコンプライアンスプログラムの要件を定義したもの	組織がSpecificationの要件を満たしていることを認証するしくみ	仕様の要求事項のひとつである教育プログラムに活用できる資料

↑本日お話しする内容

1 - 3 OpenChain仕様

■ OpenChain仕様

- OpenChain仕様の定義
  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(基本レベル/最低限の要件一式)

- 2020年10月現在の最新バージョンは、2019年4月にリリースされたVersion 2.0

- 最新のOpenChain仕様は、下記のURLから参照
  https://wiki.linuxfoundation.org/_media/openchain/openchainspec-2.0.pdf

- 2020年末までにISO標準化が予定されている

OpenChain仕様の改訂履歴	
1.0	2016年10月
1.1	2017年4月
1.2	2018年4月
2.0	2019年4月

※ 用語の定義
- OSSライセンスコンプライアンスプログラム(*Program*)
  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、人員などの総称。簡単に言うと、「組織がOSSを適切に取り扱うためのしくみ」のこと。

1 - 4 OpenChain仕様適合認証

■ OpenChain仕様適合認証

- OpenChain仕様に適合しているかどうかの確認は、
  自己認証(OpenChain Self Certification)
  第三者認証(Third-Party Certification)
  のいずれかの方法で実施できます。

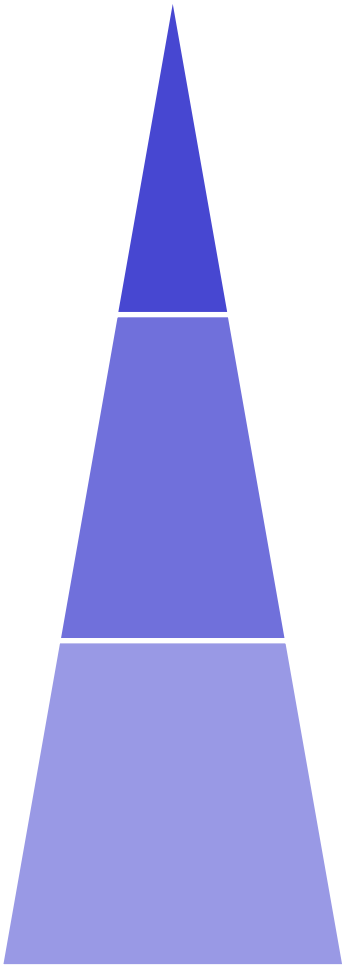
- 自己認証は、下記のURLから自由に実施できます。
  https://certification.openchainproject.org/

- 適合認証を受けた組織の一覧は、下記のURLから参照できます。
  https://certification.openchainproject.org/certified.html?locale=en

- 10月10日時点で60社が適合認証を表明しています
- 「会社全体」を対象とする必要はなく、組織やチームの単位で適合認証することができます

1 - 5 OpenChain適合にチャレンジする意義

■ OpenChain適合にチャレンジする意義



① OpenChainに適合した組織であることを示すことにより、社外からの「OSSコンプライアンスに適切に対応できる組織である」という信頼を得ることができる

② OpenChain仕様に対して、現状とのFit＆Gapを知ることで、より良いコンプライアンスプログラムにしていくためのヒントを得ることができる

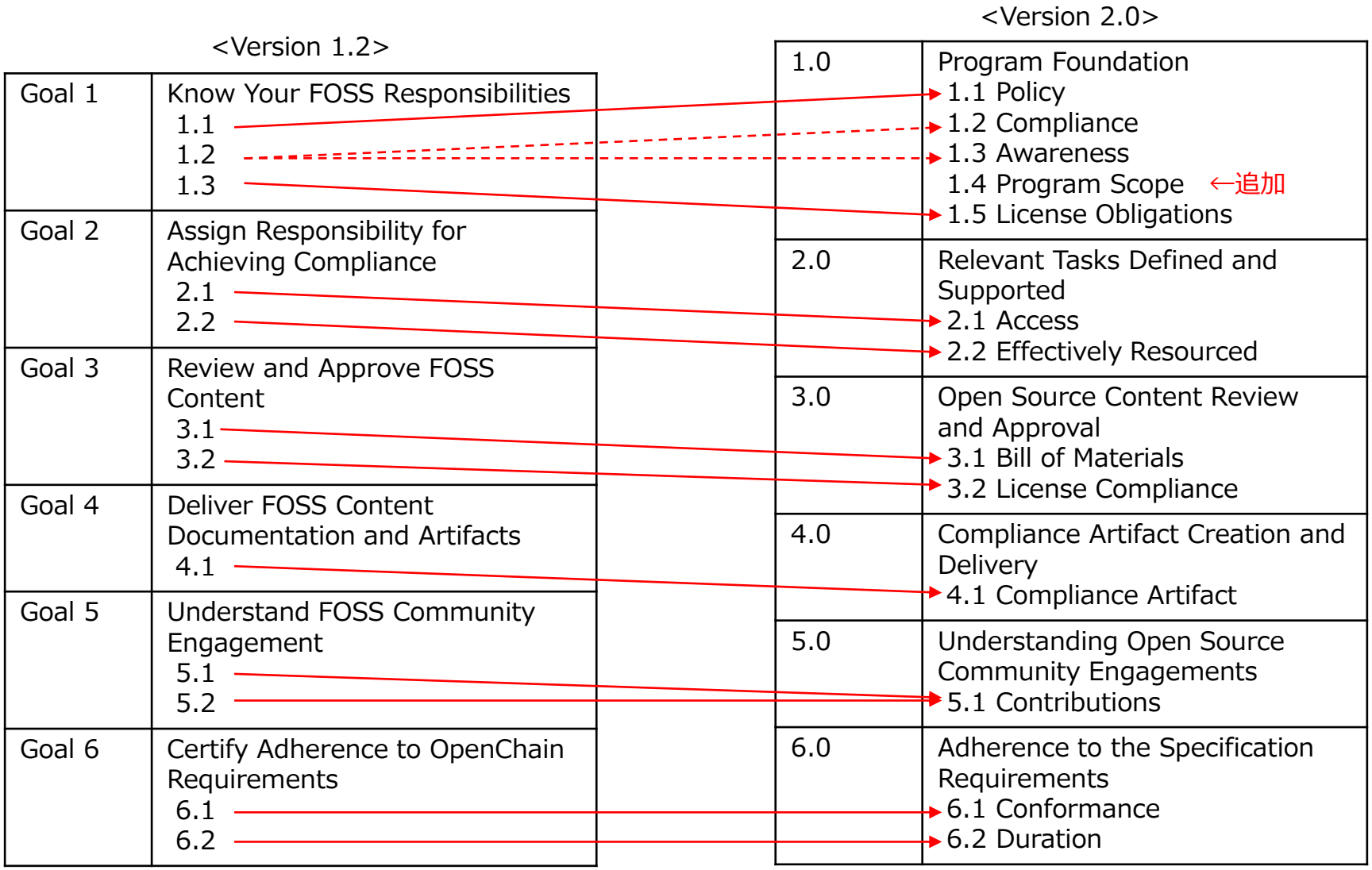
③ OpenChain仕様について学び、理解することで、**「OSSコンプライアンスを遵守するにあたって必要なこと」を体系的に理解することができる**

今回取り上げるVersion 2.0に関して、前バージョンVersion 1.2からの変更点について説明します

2. 変更点

2-1 前バージョンからの変更点(構成)

■ 前バージョンからの変更点(構成)



2-2 前バージョンからの変更点(詳細)

OPENCHAIN

■ 前バージョンからの変更点(詳細)

- 「FOSS」→「OSS」への用語の変更
  - ✓ 広く一般的に使われている用語を使用することにした

- トレーニングに関する規定の一部削除(Version 1.2 #1.2)
  - ✓ トレーニングに含まれるべきトピック(知的財産権関連法令の基礎、ライセンスの概念など)の定義の削除
  - ✓ トレーニング修了条件(24か月以内にSoftware Staffの85%が修了済であること)の規定の削除
  - ✓ トレーニングに柔軟性を持たせるための変更

- OSSコンプライアンスプログラムの範囲の規定の追加(Version 2.0 #1.4)
  - ✓ 対象範囲の柔軟性に関する規定の追加
    →組織の求める範囲に合わせてOSSコンプライアンスプログラムを構築できることがより明確に規定された

OpenChain仕様の各要求事項に関して説明します

3．OpenChain仕様詳細解説

3 - 1 全体構成

OPENCHAIN

■ 全体構成

- OpenChain Specification version 2.0 -

1) Introduction

2) Definitions

3) Requirements
   - 1.0 Program Foundation
   - 2.0 Relevant Tasks Defined and Supported
   - 3.0 Open Source Content Review and Approval
   - 4.0 Compliance Artifact Creation and Delivery
   - 5.0 Understanding Open Source Community Engagements
   - 6.0 Adherence to the Specification Requirements

Appendix I : Language Translations

3-2 参考資料

■ 参考資料

- 「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
- 「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/
- 「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

■ 用語の定義

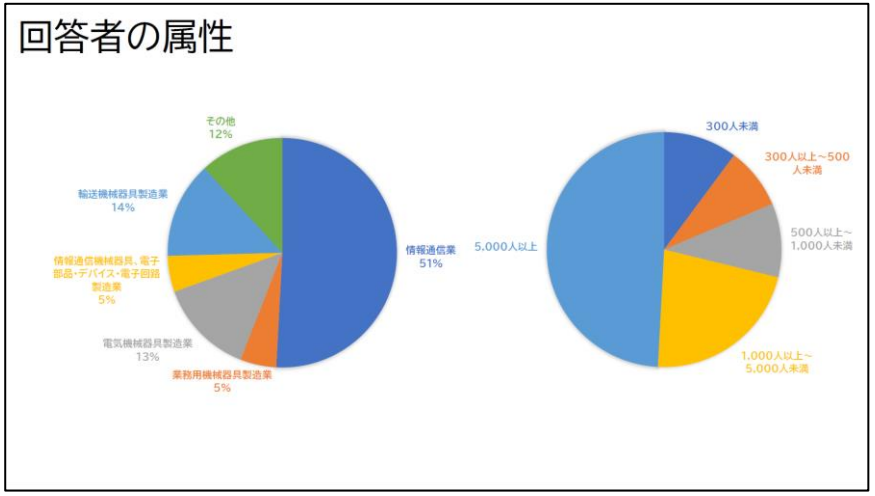
※理解しやすい様に簡単な表現にしています。
正式な日本語訳は「OpenChain仕様書詳細解説」を参照してください。

- Compliance Artifacts…「コンプライアンス関連資料」
  頒布するソフトウェアに関連して提供するべき情報・ドキュメントの一式
- Identified Licenses…「確認されたライセンス」
  頒布するソフトウェアを構成するOSSコンポーネントのライセンス(群)
- Program …「ライセンスコンプライアンスプログラム」
  組織がOSSを適切に取り扱うためのしくみ
- Software Staff…「ソフトウェアスタッフ」
  頒布するソフトウェアの関係者
- SPDX(Software Package Data Exchange)
  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
- Supplied Software…「提供ソフトウェア」
  組織が第三者(他組織または他人)に対して頒布するソフトウェア
- Verification Materials…「証跡となる資料」
  与えられた要件が満たされていることを示す資料

3-4 企業におけるコンプライアンス業務実態

■ 「企業におけるOSSコンプライアンス業務実態調査」について

2020年7月にOpenChain JapanWG Promotion Sub Group OSSスキル標準検討チームにより各企業におけるOSSコンプライアンス業務実態に関するアンケート調査が実施され、国内外約60社からの回答を頂戴しました。
本資料では、得られた結果の中から、OpenChain仕様に関連する内容を抽出し、参考情報として掲載します。



■ イントロダクション

サマリ：
　仕様書の内容、目的、背景等に関する説明

【ポイント】

- 本仕様書は、高度なOSS 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たもの
- 目的は、ソフトウェア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の提供
- ベストプラクティスを提供するものではなく、「組織のOSSコンプライアンスプログラムが、ベースラインレベルの品質と一貫性を有しているかを確認する方法」を提供している
- 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ある

■ 要求事項 #1.1- Policy

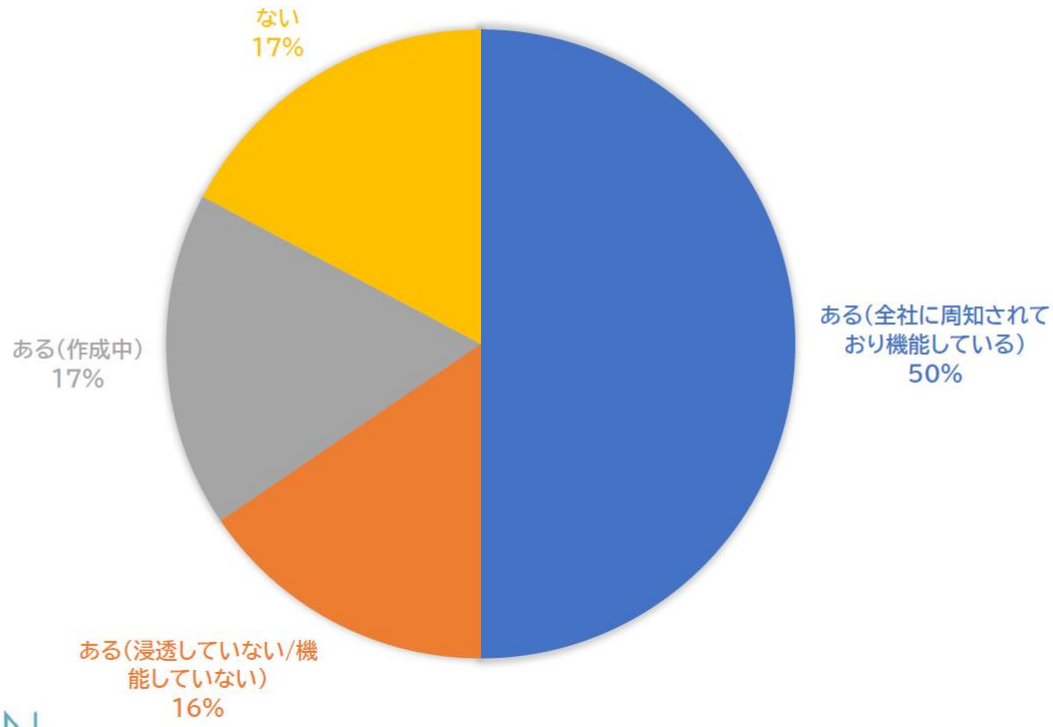
サマリ：
文書化されたOSSポリシーがあり、すべての*Software Staff*がOSSポリシーの存在を知ることができるようになっていること

【ポイント】

- OSSポリシーが文書化されていること：
  - ✓ 単なる共通認識やルーチンワーク等の不確かなものではない
  - ✓ 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、組織内で議論した結果を反映して合意形成するプロセスを大切にしてほしい
- トレーニングや社内Wiki、その他の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が存在すること：
  - ✓ アクセス方法やトレーニング教材などが、プロジェクトの新規参入者向けの導入トレーニング等で漏れなく共有されるようになっていることが必要

■ 「企業におけるOSSコンプライアンス業務実態調査」より

4-1:貴社には、オープンソースに関する会社のポリシーはありますか？
(cf. OpenChain Spec2.0 Sec1.1)



■ 要求事項 #1.2 - Compliance

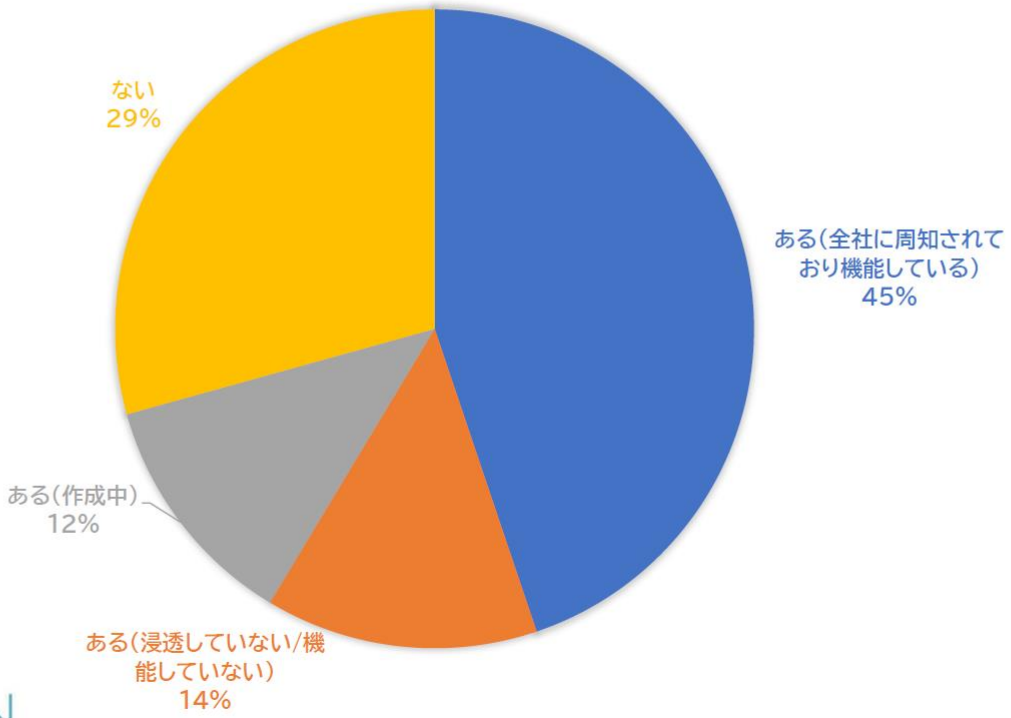
サマリ：
OSSコンプライアンスプログラムを実現する人員の役割と責任および適性を定義し、その適性評価の結果を保管する

【ポイント】

- OSSコンプライアンスプログラムを実現する役割と責任の定義：
  - ✓ 「どのような役割を定義するべきか」という規定はなく、組織の状況や課題によって独自に決定することができる
  - ✓ 責任については、例として「Open Source Review Board：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。」のような粒度で良い
  - ✓ 適性については、教育やトレーニングの履修状況、経験などに基づいて定義する
- 適性評価の証拠となる文書化された情報を保管する

■ 「企業におけるOSSコンプライアンス業務実態調査」より

4-3:貴社には、ライセンスコンプライアンスに関わる各部門及び従業員の社内での役割及び責任を定義したものはありますか？(cf. OpenChain Spec2.0 Sec1.2)



■ 要求事項 #1.3 - Awareness

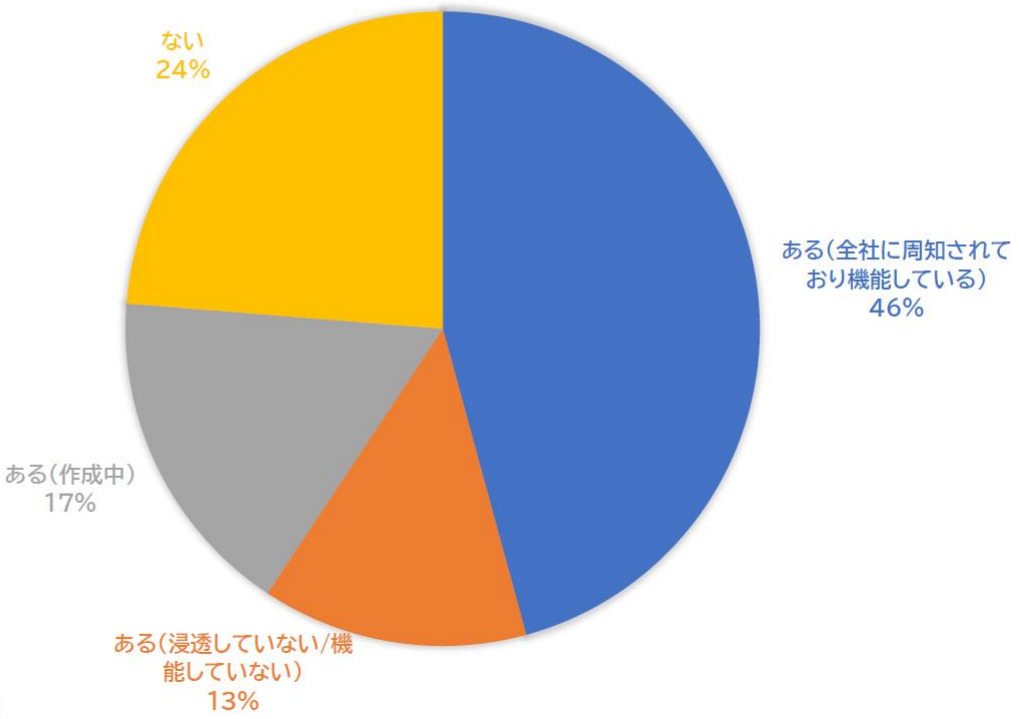
サマリ：
OSSコンプライアンスプログラム関係者が、OSSポリシー、OSS利活用の目的、貢献、不遵守の場合の影響について認識していること

【ポイント】

- 認識しておくべき事柄(トレーニング等により共有し、関係者に周知徹底させる)：
  - ✓ OSSポリシーとその場所(URLなど)
  - ✓ 組織がOSSを利活用する目的
  - ✓ OSSポリシーの背景としてある根本的な事項、OSSコンプライアンスプログラムに対して行うべき貢献(トレーニングの適切な受講やソフトウェア開発における最新動向の理解など)
  - ✓ コンプライアンスプログラムの要件に従わなかった場合の影響(ライセンス違反による訴訟リスクや組織の評判の失墜など)
  - OpenChainのCurriculumを活用可能 https://github.com/OpenChain-Project/Reference-Material/tree/master/Training-Slides

■ 「企業におけるOSSコンプライアンス業務実態調査」より

5-1:貴社には、オープンソースに関する教育プログラムはありますか？
(cf. OpenChain Spec2.0 1.2 Sec1.3)



■ 要求事項 #1.4 - Program Scope

サマリ：
OSSコンプライアンスプログラムは、組織に合わせて対象範囲を決めることができる

【ポイント】

- 組織の求める範囲に合わせてOSSコンプライアンスプログラムを構築することができる：
  - ✓ 特定のプロダクトラインのみを対象とする
  - ✓ 組織全体のソフトウェア開発全体を対象とする　など

■ 要求事項 #1.5 - License Obligations

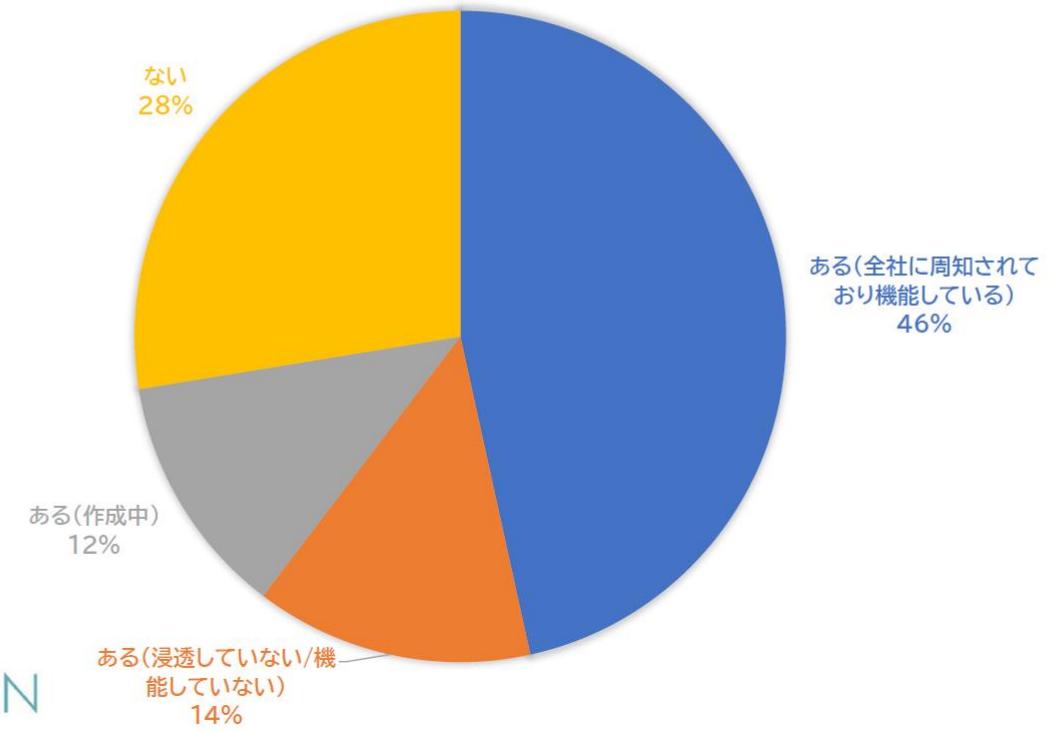
サマリ：
ユースケースに応じてOSSライセンスの義務、制約、および権利についてレビューし、文書として記録するプロセスが存在すること

【ポイント】

- ユースケースに応じて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：
  - ✓ Open Source Compliance LeadやOpen Source Review Boardがレビューを行い、疑問がある場合は組織内の知財・法務担当者や組織外の法律の専門家に相談する　など
  - ✓ ユースケースは#3.2で例示されている

■ 「企業におけるOSSコンプライアンス業務実態調査」より

6-1：貴社には、OSS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、権利を判断する文書化されたプロセスがありますか？
（cf. OpenChain Spec2.0 Sec1.5）



■ 要求事項 #2.1 - Access

サマリ：
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に適切に対応できること

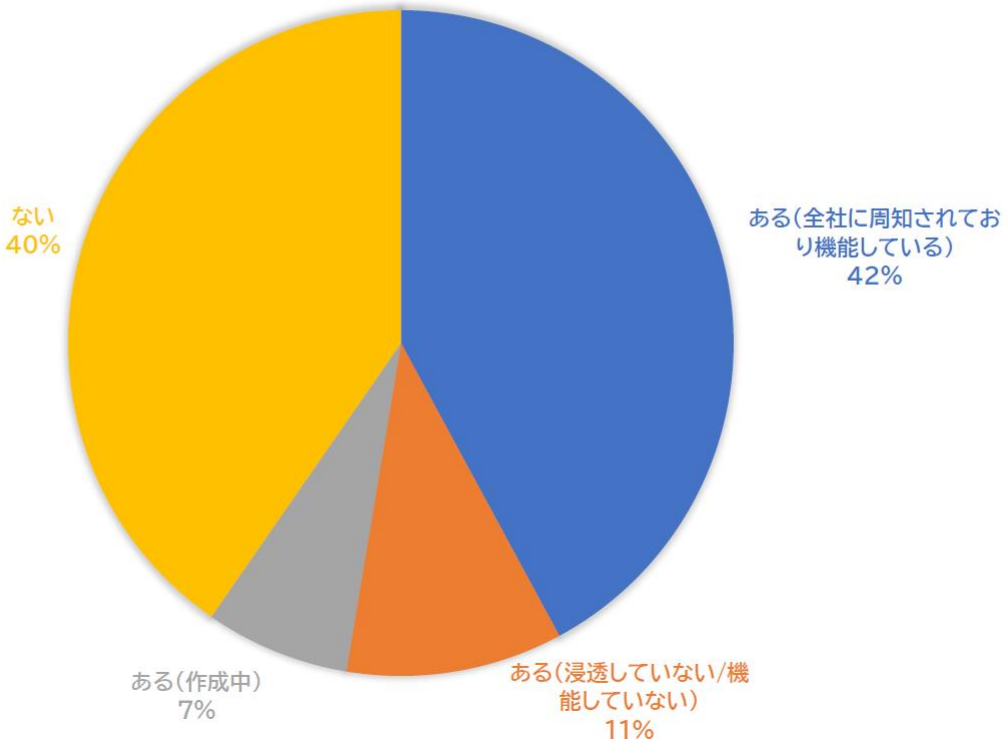
【ポイント】

- 第三者からの問い合わせを受け付ける窓口を用意する：
  - ✓ 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、第三者が問い合わせできるようになっていること
- 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があること：
  - ✓ 問い合わせを受けた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、可能性のあるすべての人が、適切な対応方法を理解し実行できるようになっていること

3 - 5 OpenChain仕様詳細解説

■ 「企業におけるOSSコンプライアンス業務実態調査」より

6-2:貴社には、オープンソースに関する情報公開や外部から問い合わせに対応に関する手段がありますか？(cf. OpenChain Spec2.0 Sec2.0)



■ 要求事項 #2.2 - Effectively Resourced

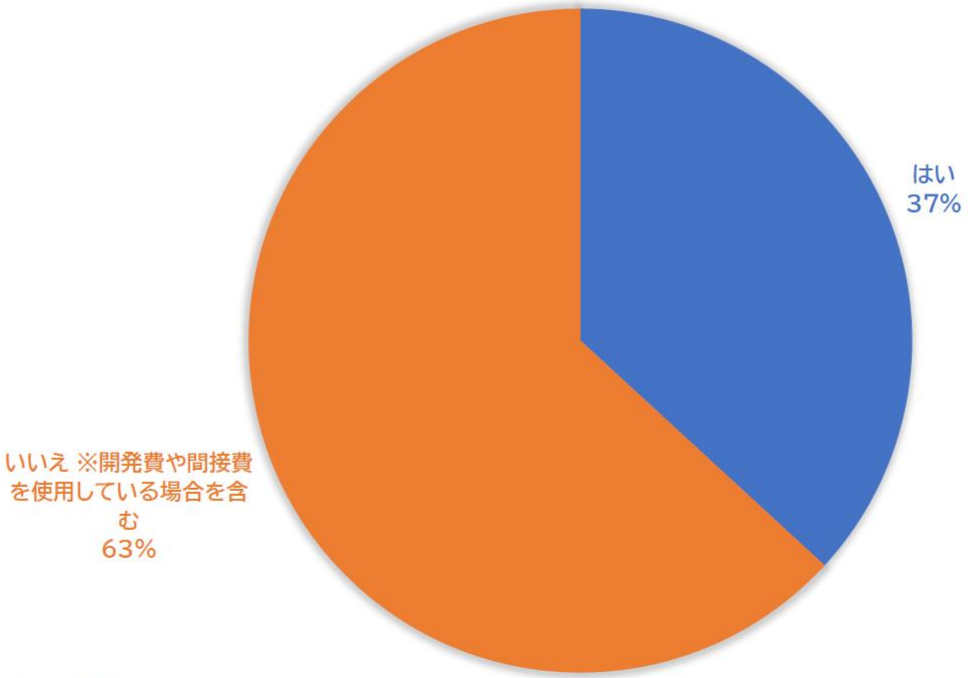
サマリ：
コンプライアンスプログラム関連役割への適切な人員・十分な活動資源の割り当て、法律専門家のアサイン、懸案事項解決プロセスの整備

【ポイント】

- OSSコンプライアンスプログラム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：
  - ✓ 適切な人員と十分な活動資源(業務遂行のための時間及び適切な予算)の割り当て
- 必要な場合に、法律的な専門知識を利用できること
- 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ること：
  - ✓ インシデントの重要性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

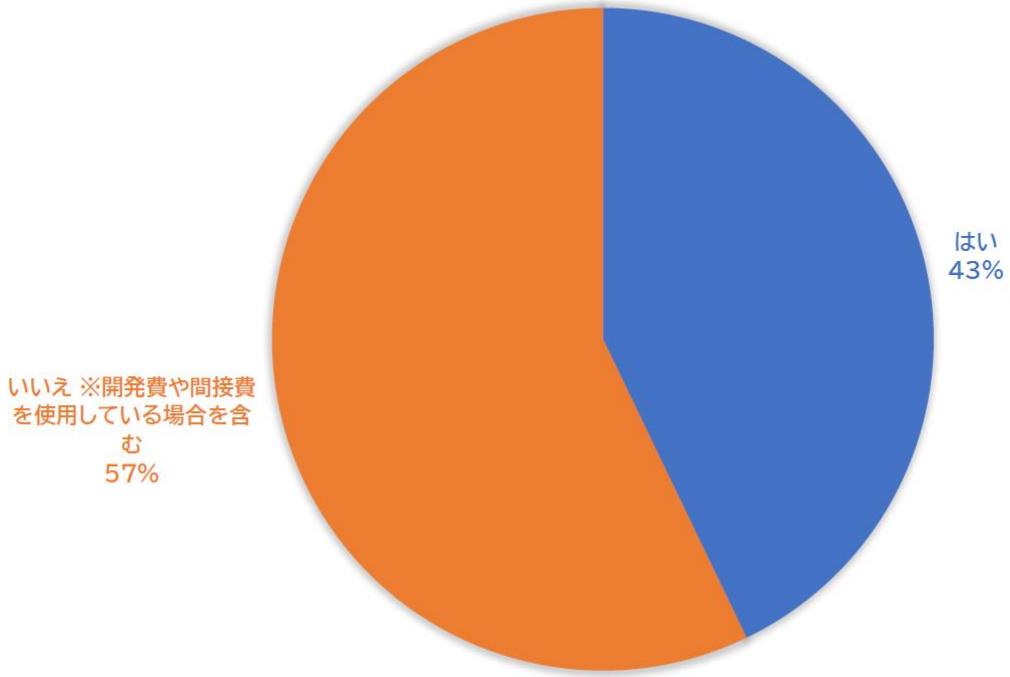
■ 「企業におけるOSSコンプライアンス業務実態調査」より

6-4：貴社は、OSSライセンスコンプライアンスに関する独立した予算を確保していますか？（cf. OpenChain Spec2.0 Sec2.2）



■ 「企業におけるOSSコンプライアンス業務実態調査」より

6-5:貴社は、OSSライセンスコンプライアンスに関する専属の人材を確保していますか？(cf. OpenChain Spec2.0 Sec2.2)



■ 要求事項 #3.1 - Bill of Materials

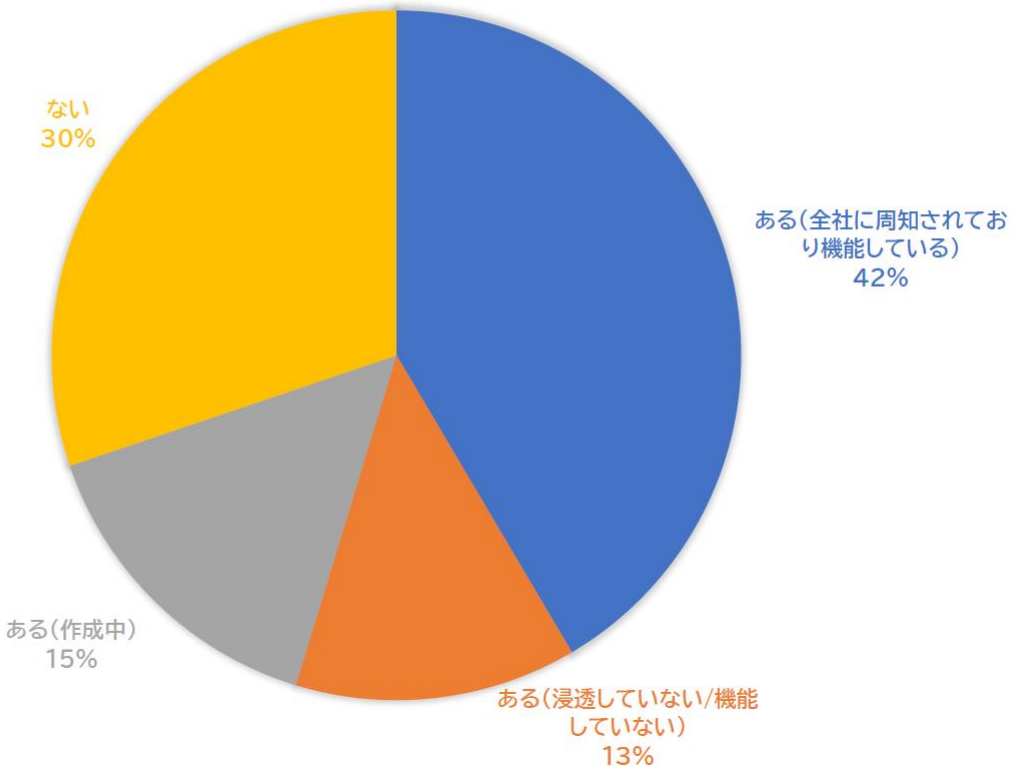
サマリ：
OSSコンポーネントの部品表を作成および管理するためのプロセスが存在すること

【ポイント】

- 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
- OSSコンポーネント部品表(Bill of Materials / BoM)：
  - ✓ *Supplied Software*を構成するOSSコンポーネント(必須)
  - ✓ *Identified Licenses* (必須)
  - ✓ ユースケース(任意)
  - ✓ 改変の有無(任意)
- 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：
  - ✓ *SPDX*や*SPDX-Lite*のフォーマットを使用しても良い

■ 「企業におけるOSSコンプライアンス業務実態調査」より

6-9:貴社は、利用もしくは作成したソフトウェアに含まれるOSSコンポーネントの部品表(SBOM)を作成し、管理する文書化されたプロセスをお持ちですか？
(cf. OpenChain Spec2.0 Sec3.1)



■ 要求事項 #3.2 - License Compliance

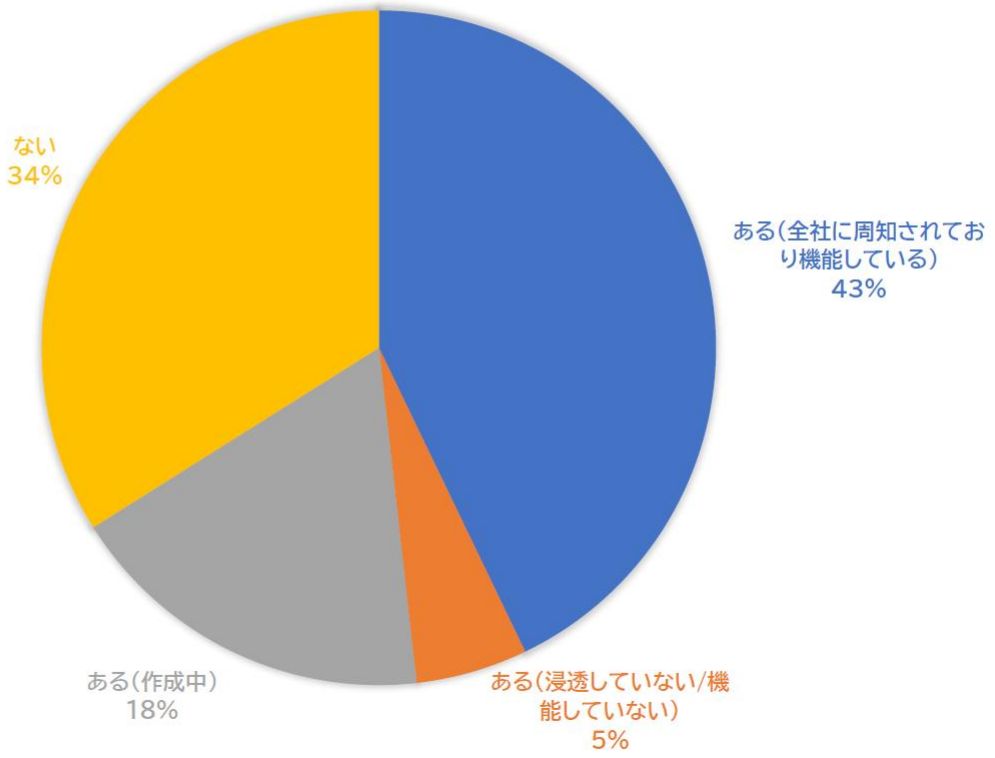
サマリ：
OSSの共通的なユースケースとそれらを取り扱うための手続きが存在すること

【ポイント】

- OSSの共通的なユースケース(ただし網羅的な列挙ではなく、組織ごとに追加・除外の可能性あり)：
  - ✓ 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

■ 「企業におけるOSSコンプライアンス業務実態調査」より

6-13：貴社は、ユースケース毎（社内利用、組込機器に利用、SI利用等）にOSSライセンスを適切に遵守するための文書化されたプロセスをお持ちですか？
（cf. OpenChain Spec2.0 Sec3.2）



■ 要求事項 #4.1 - Compliance Artifacts

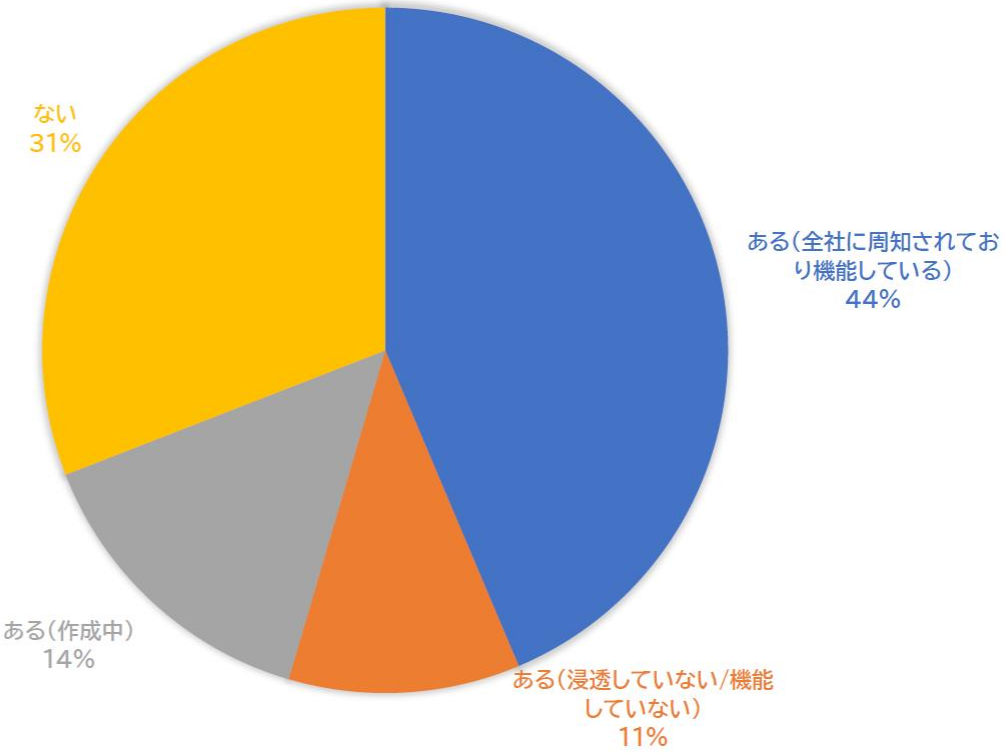
サマリ：
*Compliance Artifacts*の作成、提供、複製の保管

【ポイント】

- *Compliance Artifacts*とは、*Supplied Software*と共に提供するべき関連資料一式：
  - ✓ ソースコード、ライセンスのコピー
  - ✓ 帰属告知、著作権表示、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
- *Identified Licenses*の要求に基づいて、*Compliance Artifacts*を*Supplied Software*とともに頒布する(合理的な商業的努力)
- *Compliance Artifacts*の複製を、*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する

■ 「企業におけるOSSコンプライアンス業務実態調査」より

6-14：貴社は、ソフトウェアを第三者に配布する場合にライセンスに応じた著作権表示・ソースコード開示等のコンプライアンス関連資料を準備し、頒布するために文書化したプロセスをお持ちですか？（cf. OpenChain Spec2.0 Sec4.1）



■ 要求事項 #5.1 - Contributions

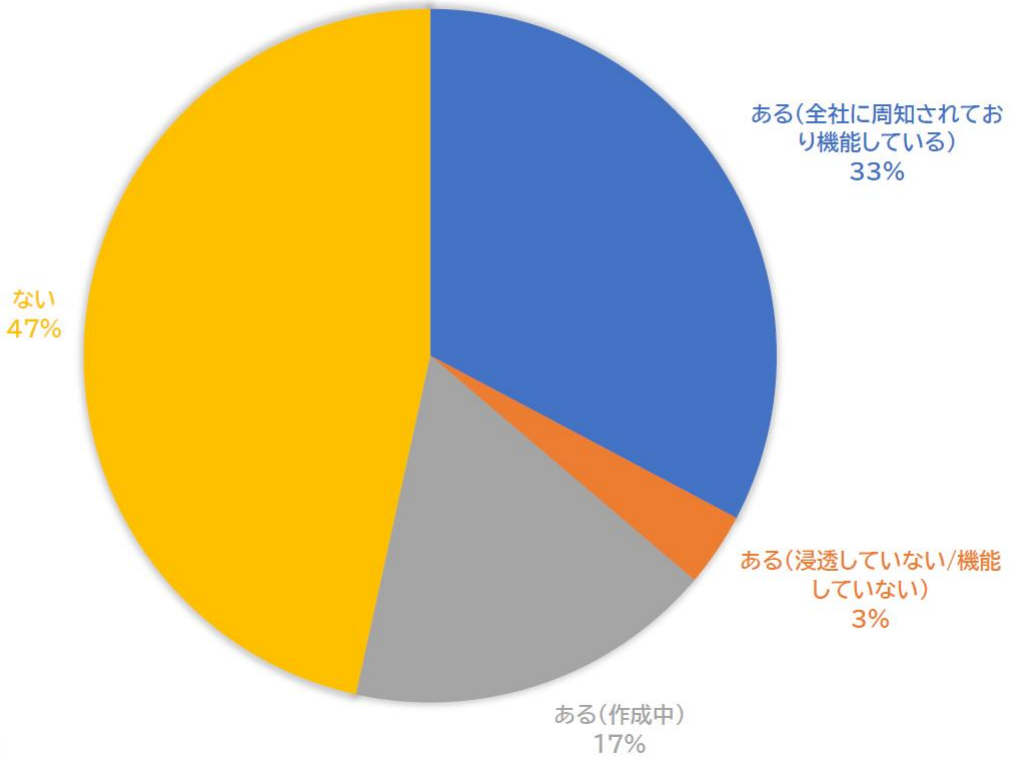
サマリ：
OSSへのコントリビューションを容認する際は、組織がコントリビューションポリシーの策定と遂行に対して適正な検討を行うこと

【ポイント】

- 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：
  - ✓ 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

■ 「企業におけるOSSコンプライアンス業務実態調査」より

9-1:貴社は、OSSコミュニティへのコントリビューションを行うための文書化されたプロセスをお持ちですか？(cf. OpenChain Spec2.0 Sec5.1)



■ 要求事項 #6.1, 6.2 – Conformance, Duration

サマリ：
組織がOpenChainに適合していると認定されるためには、本仕様の要求すべてを満たすOSSマネジメントプログラムを有していること

【ポイント】

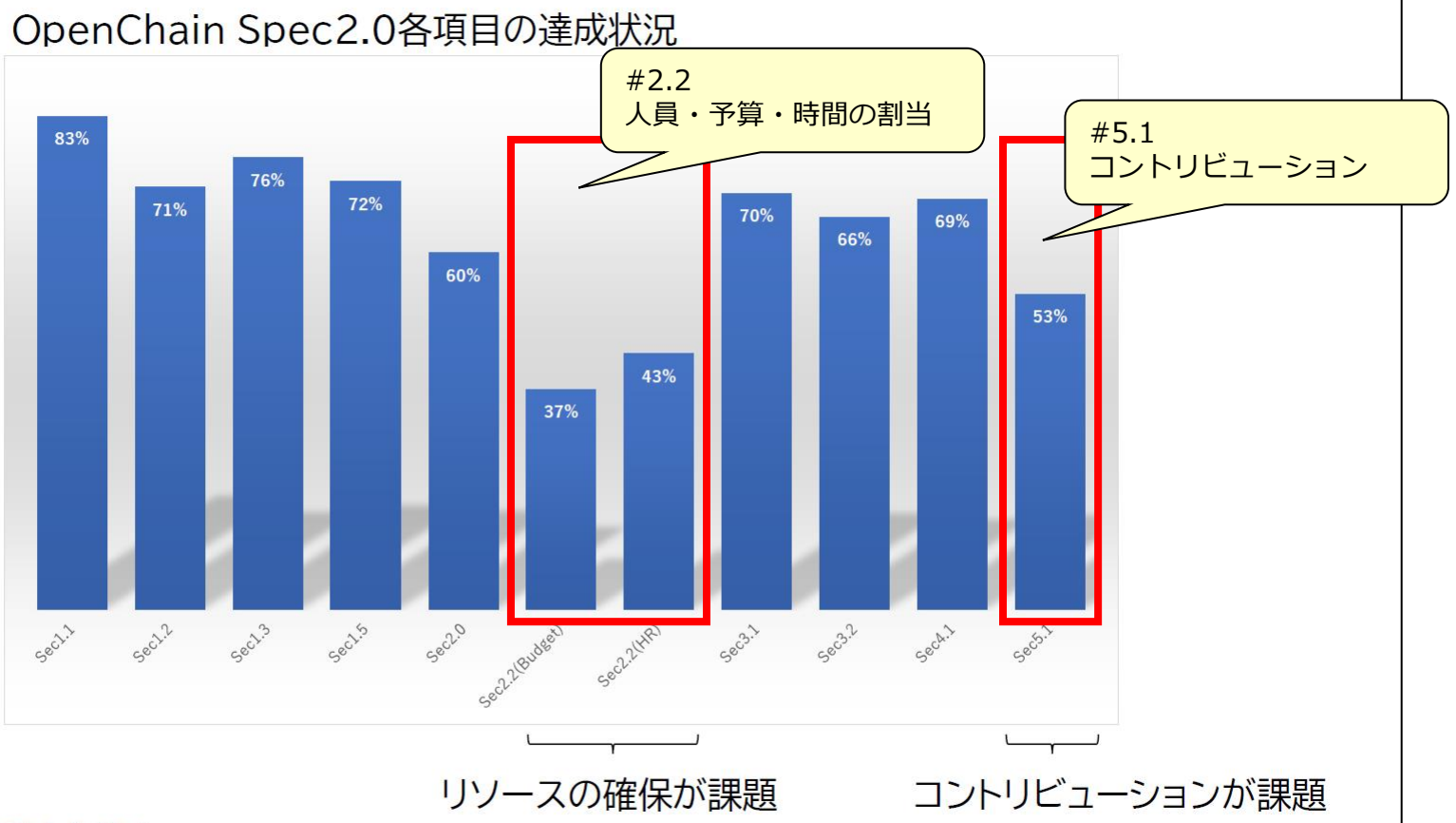
- 本仕様の要求すべてを満たさないと、OpenChain適合とはいえない
- 部分的に準拠しているだけでは不十分
- 適合認証の有効期限は18か月(時間の経過による焦点のずれを定期的にチェックするため)

４．まとめ

4-1 まとめ①

■ 「企業におけるOSSコンプライアンス業務実態調査」より

まとめ



4-2 まとめ②

■ まとめ

- 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」
- 必ずしも適合認証のためのものではなく、自組織のポリシーやプロセスを改善するための指標として活用できる
- 柔軟性を持たせているが故に理解しづらい内容もあり、その場合は公開・共有されている具体例を参考にすると良い
- OpenChain仕様は、現在でも業界内のデファクトスタンダードであるが、ISO標準化されることにより、正式な国際標準となるため、今後は適合認証の重要性が増していくと予想される

END

★ 発表者プロフィール ★

氏名：
渡邊歩　(Watanabe AYUMI)
所属：
株式会社日立ソリューションズ
連絡先：
ayumi.watanabe.ze@hitachi-solutions.com