» オープン コンプライアンス プログラム

自己診断チェックリスト

Version 1.0

2010 年 11 月

The Linux Foundation
http://www.linuxfoundation.org

日付	バージョン	説明
2010 年 11 月 1 日	1.0	自己診断チェックリスト初版

序文

自己診断チェックリストは、2010 年 8 月 10 日に発表された The Linux Foundation オープン コンプライアンス プログラムの重要な要素です。このプログラムには、コンプライアンスの精査に役立つ無料ツール、無償の教育資料、専門家による包括的なトレーニング、コンプライアンスのベスト プラクティス (効率的業務プロセス) に関する情報を交換するためのオンライン コンプライアンス コミュニティ (FOSSBazaar)、オープン ソースの構成表 (Bill of Material: BoM) を記入するための SPDX™ (Software Package Data eXchange) 標準、および企業やオープン ソー:ス開発者がコンプライアンスの問題について連絡を取り合うためのコンプライアンス緊急対応ディレクトリなどが含まれています。

背景

The Linux Foundation は、業界の優れた各種コンプライアンス プログラムを分析し、この詳細なコンプライアンス プラクティス チェックリストを編成しました。企業は、このチェックリストを社内ツールとして使用することにより、厳格なコンプライアンス プロセス実装の進捗状況を評価でき、プロセス改善活動の優先順位を決定しやすくなります。この自己診断チェックリストは、確立されたプロセス成熟度モデルの少なくとも 2 つの概念を採用しています。すなわち、Software Engineering Institute の能力成熟度モデル (Capability Maturity Model: CMM) の次の概念です。

- プロセスの導入は、初期のプロセスの定義から、制度化を経て、制御されたプロセス管理の状態へと進行すること。
  コンプライアンス プロセスを使用する目的は、他のプロセスと同様、一貫性のある期待どおりのビジネス成果を達成することです。企業は、推奨されるプラクティスのチェックリストを使用することにより、コンプライアンス活動をどの程度組織化したか、そして、求めていたビジネス成果はコンプライアンス活動によってどの程度達成されたかを自己評価することができます。
- プロセスの目的と、その目的を達成するために実行するプラクティスとを区別する必要があること。
  コンプライアンス チェックリストは、1 つの目的を達成するために利用できる複数の有効な代替手段を明確に評価します。

チェックリストに含まれているコンプライアンス プラクティスは、コンプライアンス プログラムの効率性を高め、プラクティスにかかるコストよりはるかに有益なメリットをもたらします。コンプライアンス プロセスの失敗パターンと、そのような失敗を防ぐためのプラクティスを特定するために、プロセス失敗モード影響解析 (failure modes effects analysis: FMEA) アプローチを使用しています。

OPEN COMPLIANCE PROGRAM
1796 18th Street, Suite C
San Francisco, CA 94107
+1 415 723 9709
http://www.linuxfoundation.org
compliance@linuxfoundation.org
THE LINUX FOUNDATION

なぜ「自己診断」と呼ぶのか

このチェックリストは、企業がサード パーティの助けを借りず、また社内のコンプライアンス プラクティスを公表せずに、社内で使用できるため、自己診断チェックリストと名づけました。このチェックリストを使用するには、コンプライアンス プログラムの十分に機能しているところと不十分なところを、包み隠さず評価することが必要です。評価については、その事業体の製品開発プロセス、製品ロードマップ、製品アーキテクチャ、企業カルチャーなどを熟知した組織メンバーが行うのが理想的です。チェックリストには法的資格や拘束力はありません。使用するかどうかは、完全に任意です。このチェックリストの唯一の目的は、解決しなければコンプライアンス問題に発展するようなプロセスの欠落を明確にすることです。

利用者、および、意図された目的

このチェックリストは、組織においてオープン ソース コンプライアンス プログラムの定義、実装、および改善を担当するチームが使用するように開発されました。コンプライアンス プログラムの履行を開始して間もない場合は、このチェックリストを使用するだけでなく、The Linux Foundation のオープン ソース コンプライアンス トレーニング コースも受講するとよいでしょう。このチェックリストに含まれているプラクティスは、そのトレーニング コースで詳細に説明されます。コースの説明については、下記のページを参照してください。

http://www.linuxfoundation.org/programs/legal/compliance/training-and-education

コンプライアンス プログラムについて経験を積んでいる企業は、このチェックリストを使用して、効果的なコンプライアンス プロセス実装の進捗を評価し、プロセス改善の優先順位づけに役立てることができます。チェックリストによって追加作業の必要性が明らかになった場合は、効果的であることが実証されているプラクティスを取り入れるべく、トレーニングやベンチマーキング、さらには他社とのコミュニケーションを試みることにより、効果が得られるでしょう。オープン コンプライアンス プログラムは、このような試みに対応できるよう作成されています。

自己診断チェックリストは、OSS のライセンス義務を順守しつつ、オープン ソースの使用奨励に取り組んだ多くの企業の経験をもとに、推奨される一連のプラクティスを紹介しています。すべての組織がすべてのプラクティスを実行する必要はないでしょう。また、異なるプラクティスや実行方法でコンプライアンス プログラムの目的を達成する組織もあるでしょう。各組織は、それぞれが使用するオープン ソースの性質や量、それらのオープン ソースに適用される各ライセンス、および製品そのものの設計に応じて、コンプライアンス アプローチを適切に適合させてください。

チェックリストの使用方法

この自己診断チェックリストは、コンプライアンス プログラムの厳格さや効果について議論を促したい場合や、最も改善が必要な領域に注目を集めたい場合に使用できます。チェックリストの質問から生まれた議論によって、実施すべき活動に関する合意が得られたり、改善の見通しがついたりする可能性があります。

また、このチェックリストは、組織がサプライヤーを選定する際に、サプライヤーのコンプライアンス プロセスを評価したり、サプライヤーのオープン ソース開示の信頼性などを判断したりする際にも使用できます。

OPEN COMPLIANCE PROGRAM
1796 18th Street, Suite C
San Francisco, CA 94107
+1 415 723 9709
http://www.linuxfoundation.org
compliance@linuxfoundation.org
THE LINUX FOUNDATION

今回発表される最初のバージョンのチェックリストは、採点方式にはなっていません。
組織は、以下のように各コンプライアンス プラクティスを評価することができます。

- Yes / No / Not Applicable
  (はい/いいえ/あてはまらない)
- Frequently Performed / Occasionally Performed / Rarely Performed
  (頻繁に実行されている/時々実行されている/あまり実行されていない)
- Strong / Satisfactory / Weak / Not Done
  (強い/ふつう/弱い/していない)
- Fully Satisfied / Partly Satisfied / Not Satisfied
  (充分満たしている/ある程度満たしている/満たしていない)
- Green (Good) / Yellow (Marginal) / Red (Unacceptable)
  (緑 (良好) / 黄 (要注意) /赤 (容認できない))

また、個々のプラクティスの評価を集約し、全体的なコンプライアンス活動の展望を明らかにする方法を知ることが必要な組織もあるでしょう。たとえば、サポート プラクティスの満足度は、コア コンプライアンス プロセス (検出、レビューと承認、義務の履行、コミュニティへの貢献) の目的が果たされているかどうかを (Software Engineering Institute の能力成熟度モデル方式で) 評価する際に使用できます。また (ISO 9000の 認定評価のように)、サマリ レポートに、大小の逸脱が認められることがあります。(ISO 9000 の用語では、小さな逸脱や非準拠は、重要であり、正しい対処が必要ですが、大量に検出されることもあり、それでもそれらが認定の障害にはなりません。しかし、大きな逸脱は、たとえ 1 つでも、認定を阻む可能性があります。)
Software Engineering Institute (SEI) の評価プログラムもそうですが、チェックリストの利用者は、書類上の定義としてのプラクティスと、コンプライアンスを履行するために日常的に使用し、依拠しているプラクティスとを区別する必要があります。つまり、プラクティスを「実行可能なものとして整備」して、「自社流」にしてください。オリジナルの SEI トレーニングでは、組織がその活動目的を果たしているかどうかを決定するために、鑑定士は、次のような諸点を評価するように指導されています。

- 履行の強い意志 (ポリシーや文書化されたプロセス要件によって証明される)
- 履行能力 (スキルある人材、リソース、資金)
- 作業 (使用される主なプラクティス)
- 測定と分析 (プロセスの実行を監視するために使用する手段と基準)
- 検証 (正しい作業の完了を確認するための監査と評価)

自己診断チェックリストを使用する際、組織は同様の分析を適用し、効果的なオープン コンプライアンス プログラムが確立されているかどうかを判断できます。

フィードバックと今後の改訂

自己診断チェックリストの改善案や、チェックリストの使用方法に関するフィードバックをぜひお送りください。

宛先は compliance@linuxfoundation.org (英語) です。Linux Foundation に提出されたフィードバックは、組織間でコンプライアンスに関する意見やチェックリストの利用に関する意見を共有する際に、共通の資料として役立てられます。

OPEN COMPLIANCE PROGRAM
1796 18th Street, Suite C
San Francisco, CA 94107
+1 415 723 9709
http://www.linuxfoundation.org
compliance@linuxfoundation.org
THE LINUX FOUNDATION

その他の資料

The Linux Foundation では、以下のようなオープン コンプライアンス トレーニング コースを提供しています。

- **LF281 オープン ソース コンプライアンスのエグゼクティブ レビュー**
  役員レベルの管理者層のための半日トレーニング。コンプライアンスの重要性、およびオープン ソース ライセンス義務を果たすために行うべきことに焦点を絞っています。
- **LF384 オープン ソース コンプライアンスの詳細プロセス概要**
  コンプライアンス プロセスに関する 1 日コースの総合レビュー。行うべきプロセスの説明、およびコンプライアンス プロセスのインスタンス化への取り組みの勧め。
- **LF488 オープン ソース コンプライアンスの実装と管理**
  コンプライアンス プロセスを包括的に説明する 2 日間のコース。コンプライアンス作業を各組織のニーズにどう適応させるかというテーマで、コンプライアンス チームとワーキング セッションも行います。

The Linux Foundation から、コンプライアンスに関するホワイト ペーパーも提供されています。
下記のサイトから入手できます。
http://www.linuxfoundation.org/programs/legal/compliance/training-and-education（英語）
http://www.linuxfoundation.jp/programs/legal/compliance/training-and-education（日本語）
たとえば、以下のようなホワイト ペーパーがあります。

- “Free and Open Source Software Compliance: The Basics You Must Know”
  『フリー & オープン ソース ソフトウェア コンプライアンス: 基本概念』
- “Establishing Free and Open Source Software Compliance Programs: Challenges and Solutions”
  『フリー & オープン ソース ソフトウェア コンプライアンス プログラムの確立: 課題と解決策』
- “Free and Open Source Software Compliance: Who Does What”
  『フリー & オープン ソース ソフトウェア コンプライアンス: 誰が何をするか』
- “Managing FOSS Compliance in the Enterprise”
- “FOSS Compliance: A Glimpse into Operational Best Known Practices”

また、Linux Foundation では、企業による精査作業を支援する各種ツールを開発しました。これらのツールは、
下記のサイトからダウンロードできます。
http://www.linuxfoundation.org/programs/legal/compliance/tools
また、同じ URL から入手できる以下のホワイトペーパーで、ツールについて説明しています。

- “Dependency Checker Tool: Overview and Discussion”
- “Code Janitor Tool: Overview and Discussion”

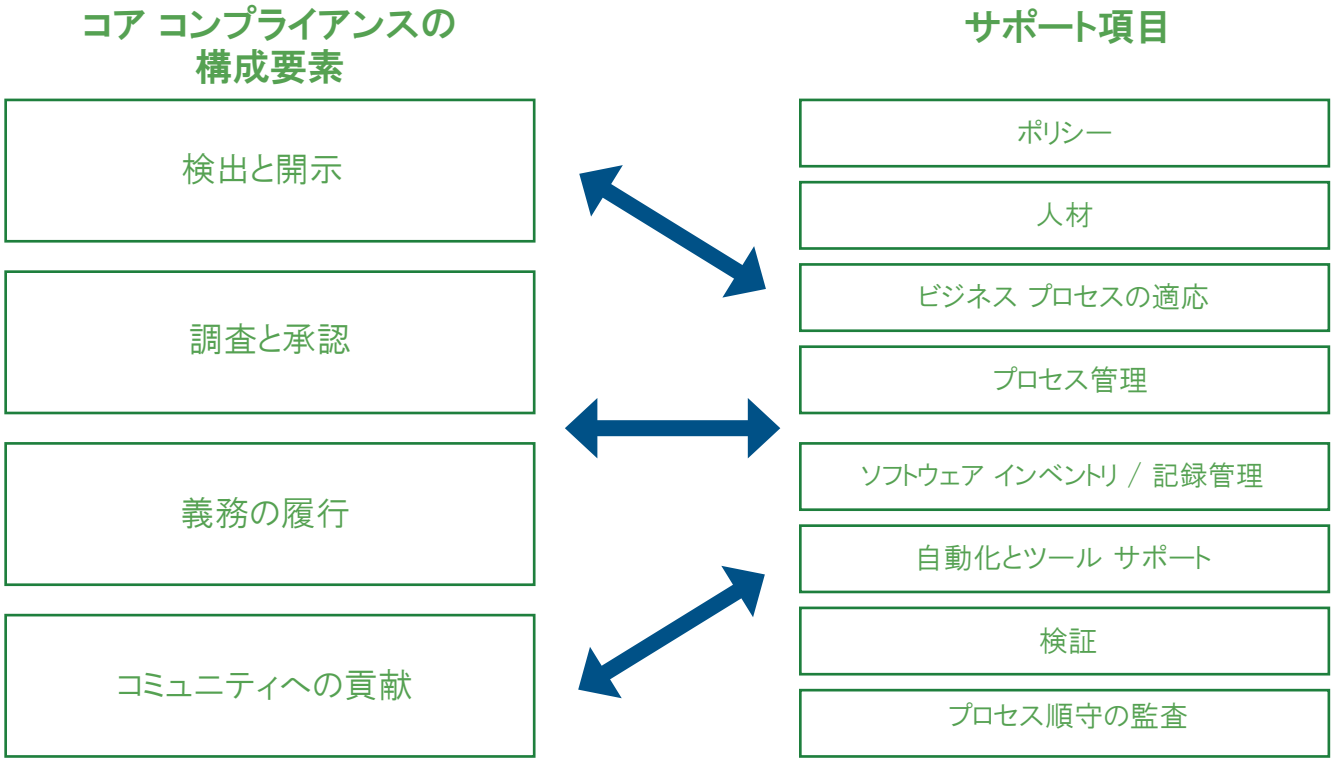
使用している略語

FMEA	Failure Mode Effects Analysis（失敗モード影響解析）
IT	Information Technology（情報技術）
OSRB	Open Source Review Board（オープンソース調査委員会）
OSS	Open Source Software（オープン ソース ソフトウェア）

OPEN COMPLIANCE PROGRAM
1796 18th Street, Suite C
San Francisco, CA 94107
+1 415 723 9709
http://www.linuxfoundation.org
compliance@linuxfoundation.org
THE LINUX FOUNDATION

はじめに

この自己診断チェックリストに掲載されているプラクティスは、下図のような、コア コンプライアンス プロセスとサポート項目という概念に従って編成および提案されています。（まず、コア プロセスが上から順に、続いてサポート項目が上から順に現れます。）サポート項目というのは、組織がコア コンプライアンス プロセスの目的を果たせるように支援するプラクティスです。



OPEN COMPLIANCE PROGRAM
1796 18th Street, Suite C
San Francisco, CA 94107
+1 415 723 9709
http://www.linuxfoundation.org
compliance@linuxfoundation.org
THE LINUX FOUNDATION

検出

「検出」は、出荷予定の製品に含まれているサードパーティ ライセンス ソフトウェア（オープン ソース ソフトウェアを含む）の識別に関わるプロセスです。この分野の主なプラクティスと機能には、次のようなものがあります。

メモ:

1. 製品開発サイクルの早期段階で OSS 検出を行うこと。 ☐
2. 製品担当チームは、コンプライアンス分析を行うべきすべてのソフトウェア、およびその他の要素を体系的に識別すること。 ☐
3. サード パーティ サプライヤーは、提供品に含まれているすべての OSS を開示すること。 ☐
   a) 開示用に定義されている書式を使用すること。
   b) OSS コンプライアンス チームは、利用可能なすべてのツールを用いて、開示の正確性と完全性を調査すること。
4. 組織は、サプライヤー選定プロセスの一環として、サードパーティ サプライヤーが利用している OSS と、その OSS のコンプライアンス プラクティスを調査すること。 ☐
   a) 組織は、サードパーティ サプライヤーのコンプライアンスおよびサプライ チェーン管理プラクティスを調査し、サードパーティの妥当性を評価すること。
   b) 組織は、定義されたガイドラインを使用して、サプライヤーの開示に関して、追加的な自動スキャニングやその他の確認が必要かどうかを決定すること。
   c) ソフトウェア ライセンス同意書に、OSS に関する適切な契約条件が含まれていること。
   d) サプライヤーとやりとりするサプライ チェーン スタッフやその他の担当者は、OSS 問題の教育を受けており、サードパーティ サプライヤーとの議論に OSS の事項を含めていること。
5. 組織は定期的に OSS 利用の監査を実施すること。 ☐
   a) 組織は、合意された頻度で、社内で使用されている OSS の監査と目録作成を実施し、その結果を記録すること。
   b) 組織は、出荷する製品に含まれる OSS の監査と目録作成を行うこと。
   c) 組織は、製品のソース コードを改めて監査する必要のある条件やイベント、あるいは、OSS コンプライアンスが検証されているコードベースにさらに変更を加える必要のある条件やイベントを特定すること。
6. 各製品リリースのオープン ソース コンテンツを反映する BoM（構成表）を用意していること。 ☐
   a) ソース コードを利用可能な場合には、コード スキャンを使用して BoM を用意すること。
   b) ソース コードを利用できない場合には、サプライヤーの開示を使用すること。
7. 組織は、コード ベースラインの変更を識別し、かつ変更に伴ってさらに必要となるコンプライアンスを効率的に履行するための体系的な方法を考案すること。 ☐
8. 組織は、検出活動によって生じる問題を体系的に解決すること。 ☐
   a) 組織は、未解決の問題を体系的に追跡すること。
   b) 組織は、合理的な期間内で解決するために、適切なリソースを割り当てること。
9. 組織は、商用ツールおよびオープン ソース ツールを定期的に調査し、それらをコード ベースラインの OSS 検出に使用する際のコストとメリットを評価すること。 ☐

OPEN COMPLIANCE PROGRAM
1796 18th Street, Suite C
San Francisco, CA 94107
+1 415 723 9709
http://www.linuxfoundation.org
compliance@linuxfoundation.org
THE LINUX FOUNDATION

調査と承認

「調査と承認」プロセスでは、社外に提供する自社製品のオープン ソース使用計画について調査します。また、企業ポリシーによって義務付けられる場合は、社内プロジェクトについても調査を実施します。

メモ:

1. 組織は、製品内のすべてのオープン ソース使用に調査を義務付け、さらに、OSS 使用に関してどのような変更があると再承認処理が必要になるかを定義すること。 ☐

2. 組織は、特定の OSS パッケージおよびバージョンの使用に関する問題点を検討すること。たとえば、コミュニティが後続バージョンに施したバグ修正、特定のパッケージ バージョンに確認されたセキュリティ脆弱性、パッケージに組み込まれ、輸出管理規制の対象となる可能性のあるテクノロジなど。 ☐

3. オープン ソース調査委員会は、配布予定の製品における OSS の使用計画を調査および承認すること。 ☐
   a) OSRB (オープン ソース調査委員会) は、適切なスキルと知識を持つ人々で構成されていること。
   b) OSS ライセンスの解釈や、履行する義務の定義について、適切なリソースを利用できること。
   c) 製品開発サイクルに合致した短いサブミッション応答時間を実現できるよう、OSRB に充分な要員が提供されていること。
   d) OSRB の手続き (調査のための入力、参加者、調査手順、分析手順、結論、上訴、および棄却など) が定義され、文書化されていること。
   e) OSRB は、出荷製品に OSS を含める際のアーキテクチャ ガイドラインや要件を検討および提供すること。
   f) OSRB は、チームから OSS 使用の承認要求が提出されたら、独立した分析メソッドを使用して、チームから提出された OSS の内容を確認すること。
   g) 今後の審議での使用に備えて、OSRB 審議記録 (事例、状況、過去の決定、製品担当チームに課せられた要件など) を維持管理すること。
   h) OSRB は、提出された OSS の使用を承認するかどうか決定し、履行すべき義務があれば特定し、満たすべき条件があれば特定した上で、最後に製品の出荷を承認すること。

4. 組織は、OSS 使用の承認を求めて OSRB に提出するべき情報の定義と例を提供すること。 ☐
   a) OSS の使用案には、各 OSS コンポーネントとシステム全体との間のアーキテクチャ インタフェース、および依存性の説明が含まれること。

5. OSRB はあらゆる事業体と見解をやりとりし、ライセンス義務と調査プラクティスに関する解釈の一貫性を図ること。 ☐

OPEN COMPLIANCE PROGRAM
1796 18th Street, Suite C
San Francisco, CA 94107
+1 415 723 9709
http://www.linuxfoundation.org
compliance@linuxfoundation.org
THE LINUX FOUNDATION

義務の履行

「義務の履行」には、OSS ライセンス義務を履行するために必要なコンプライアンス プラクティスが含まれます。

メモ:

1. 組織は、サードパーティ製品の入手時に、サードパーティ サプライヤーが OSS 義務の履行に必要なすべての情報（著作権告知、帰属告知、ライセンス文書、公開するべき対応ソースコードなど）を提供していることを保証すること。 ☐

2. 組織は、ライセンス義務を発生させる外部ソフトウェアの譲渡方法を定義し、そのように受け入れたすべてのソフトウェアが、コンプライアンス要件を満たしていることを保証すること。 ☐

3. 組織は、一貫した規律ある方法で義務を履行すること。 ☐
   a) 組織は、ライセンス文書と義務要件のリポジトリを利用可能にし、一貫した解釈とコンプライアンス作業ができるようにすること。
   b) 組織は、明確な義務履行方法の例を提供すること。
   c) スキルと知識を持つ担当者が、製品ドキュメントの OSS 関連のセクションを記述し、果たすべきその他のライセンス義務を履行すること。

4. 組織は、任意の製品リリースに使用されている各 OSS パッケージに厳密に対応した完全なソース コードをソフトウェア リポジトリに保存すること。 ☐
   a) チームは、ライセンス条件に定められている場合は、完全なソース コードを提供すること。これには、関連するすべてのインタフェース定義ファイル、およびコンパイルと実行ファイルのインストールを制御するために使用されるスクリプトなども含まれる場合があること。
   b) 調査対象の OSS に対応するソース コードを組織のビルド環境以外で構築できること、およびその OSS パッケージの成果物であるバイナリと製品バイナリが一致することを保証するために、検証作業を行うこと。
   c) 配布予定のソース コードからすべての不適切なコメントが削除されていることを保証するために、検証作業を行うこと。
   d) 配布予定のすべての OSS パッケージが OSRB によって承認されていることを保証するために、検証作業を行うこと。

5. ソース コード調査プロセスを開発段階で実行し、著作権、帰属、ライセンス、変更記録情報などの必要不可欠かつ適切な文書が OSS パッケージに含まれるよう保証すること。 ☐

6. OSS ライセンス義務を評価および履行する作業を計画し、プロジェクト スケジュールの予定に組み込み、製品リリースまでに義務が履行されるよう保証すること。 ☐

7. ソースコード配布リクエストに対応するために、定義されたコード配布メカニズムを用意すること。 ☐
   a) 組織は、特定の OSS ライセンスの要件を満たすコード配布メカニズムを定義すること。
   b) コミュニティ向けに Web ポータルなどの窓口を作成し、自社製品で使用されているソース コードへのオンライン アクセスを提供すること。
   c) ポータルの管理責任者が割り当てられ、適切な人材が配置されること。

OPEN COMPLIANCE PROGRAM

1796 18th Street, Suite C
San Francisco, CA 94107
+1 415 723 9709
http://www.linuxfoundation.org
compliance@linuxfoundation.org

THE LINUX FOUNDATION

メモ:

d) 正確かつ完全な OSS のバージョンの掲載を保証するための手順が確立されていること。
e) 利用者が、製品のライセンス情報や、場合によってはソース コードに簡単にアクセス できるような、わかりやすく有用なポータルを提供すること。

8. ドキュメンテーションやローカリゼーションの担当者、あるいは、チームは、確実に義務を履行するために必要な作業を行うこと。 ☐
a) サポート チーム (サプライチェーン、ドキュメンテーション、IT など) は、OSS の基礎知識について教育を受けていること。
b) サポートチームの行うべきことをタイムリーに計画し、スケジュールを組み、実行すること。

9. 組織は、外部からのあらゆるコンプライアンス リクエストにタイムリーに応答すること。 ☐
a) 定型のリクエストに対応するためのコンプライアンス履行プロセスが存在すること。
b) メトリクスが定期的に収集され、応答時間が報告されること。
c) コンプライアンス照会対応プロセスが存在すること。
i) 応答作業には、高い優先順位がつけられ、問題は適切な管理者層に報告されること。
ii) コンプライアンスに関する適切な監督、調査、および承認作業が実施されていること。
iii) コンプライアンス問題の再発を防止するために、組織が定めたコンプライアンス プロセスに対して、適宜、変更が行われること。
d) コンプライアンス リクエストは、終結するまで追跡されること。
e) 必要と判断した場合は、定義された手順に従い、著作権のあるコードを プロプライエタリ ソフトウェアとしてクリーンルーム方式で修正する試みが実行されること。

OPEN COMPLIANCE PROGRAM
1796 18th Street, Suite C
San Francisco, CA 94107
+1 415 723 9709
http://www.linuxfoundation.org
compliance@linuxfoundation.org
THE LINUX FOUNDATION

コミュニティへの貢献

「コミュニティへの貢献」プロセスは、従業員によるコミュニティ プロジェクトへの貢献、および企業による
コミュニティ プロジェクトへのコードやその他リソースの貢献について、調査および承認します。

メモ:

1. 定義されたプロセスに従って、コミュニティへの貢献が調査され、承認されること。 ☐
2. 確立されたガイドラインに基づいて、従業員による貢献が業務上のものか、あるいは非業務上のものかを見極めること。 ☐
   a) 調査と承認プロセスの権限によって出された結論の適用範囲を定めること。
3. コミュニティ貢献者用のライセンス契約が、OSRB および企業の法務部門によって調査されること。 ☐
4. 提案された貢献に異論を唱えている組織内事業体があるかどうかを確認するメカニズムを用意すること。 ☐
5. 計画されている貢献の著作権のオーナーシップを明確にすること。 ☐
6. コミュニティ プロジェクトに対して、企業による財政支援、労働力、コード、あるいはその他の知的財産の貢献を行うメカニズムを用意すること。 ☐
7. オープン ソース コミュニティへの企業貢献を追跡すること (バグ修正のような個人の貢献と、企業が支援するプロジェクトの両方が対象)。 ☐

OPEN COMPLIANCE PROGRAM
1796 18th Street, Suite C
San Francisco, CA 94107
+1 415 723 9709
http://www.linuxfoundation.org
compliance@linuxfoundation.org
THE LINUX FOUNDATION

ポリシー

「ポリシー」の領域は、事業利益を確保すると同時に、OSS の利用を促進するよう、企業の方針を検討します。

メモ:

1. 組織のポリシーにより、自社製品に OSS を組み込んで利用することが認められること。そのポリシーは、役員レベルの管理者によって署名され、全従業員に周知されること。 ☐
2. 少なくとも、組織のポリシーは、コンプライアンス作業に関する役割と責任、OSS 利用に関する調査と承認プロセス、コミュニティ プロジェクトへの貢献に関するガイドライン、貢献に関する調査と承認プロセス、および自社製品内の OSS 利用を管理するために実行すべきコア プロセスについて取り上げていること。 ☐
3. 管理チームは、ポリシーを支持し、オープン ソースに関わるすべての従業員にそのポリシーを確実に理解させること。 ☐

OPEN COMPLIANCE PROGRAM
1796 18th Street, Suite C
San Francisco, CA 94107
+1 415 723 9709
http://www.linuxfoundation.org
compliance@linuxfoundation.org
THE LINUX FOUNDATION

コンプライアンス要員の適正配置

「コンプライアンス要員の適正配置」は、コンプライアンス プログラムの履行に必要なスキルを持つ人材を集めることに焦点を当てます。

メモ:

1. スキルと知識を持つ人材が、コンプライアンス活動への貢献に参加可能であること。 ☐
2. コンプライアンスの職務に専任者を配置することにより、継続的な関与と専門知識の蓄積を行うこと。 ☐
3. 職務説明書により、コンプライアンスを適正に履行するために必要なスキルと見識を特定すること。 ☐
4. 組織は、コンプライアンスの任務に関わるために必要なスキル、見識、および関心を持つ人材を特定すること。 ☐
5. 必要に応じ、クロスファンクショナルな部門からコンプライアンス作業貢献者を選出すること。 ☐
6. 一連の必要なスキルを習得するためのトレーニングや、経験学習の機会が提供されていること。 ☐
   a) 異なる事業体でコンプライアンスの任務を実行している関係者は、専門知識や見識を相互に交換・共有して、一貫性のあるコンプライアンス アプローチを実現するよう奨励されていること。
7. 必要に応じて外部のコンサルタントを採用し、社内のコンプライアンス活動を強化すること。 ☐
8. 組織のコンプライアンス要件に対応するために要するコンプライアンス活動の量と期間に関する推定値を用意しておくこと。 ☐
9. 単発の作業や間接作業の見積もりを算定し、追跡すること。 ☐
10. 組織のコンプライアンス チームと製品担当チームの両方の観点から、製品関連のコンプライアンス作業の見積もりを算定し、追跡すること。 ☐
11. 製品リリース サイクルに合致した応答性レベルとサイクル タイムを提供できるように、要員配置計画を用意すること。 ☐
12. 組織のコンプライアンス計画と、製品担当チームのコンプライアンス計画に対して、進行状況を追跡すること。また、コンプライアンスの目的を達成するために、必要に応じて人材を追加すること。 ☐

OPEN COMPLIANCE PROGRAM
1796 18th Street, Suite C
San Francisco, CA 94107
+1 415 723 9709
http://www.linuxfoundation.org
compliance@linuxfoundation.org
THE LINUX FOUNDATION

ビジネス プロセスの適応

「ビジネス プロセスの適応」は、既存のビジネス プロセスの文脈に OSS コンプライアンスの諸事項をうまく組み込むことに焦点を当てます。

メモ:

1. 既存のビジネス プロセスを修正し、OSS コンプライアンス作業と検討事項を組み込むこと。 ☐
   a) コンプライアンス作業を製品開発プロセスに対応付け、レバレッジ ポイントを特定すること。
   b) プロセス失敗モード影響解析 (failure modes effects analysis: FMEA) を実行し、コンプライアンスの失敗の発生パターンや、そのような失敗を防ぐために変更するべきビジネス プロセスを特定すること。
2. サプライ チェーンのサプライヤー選定手続きを手直しし、サプライヤーの精査を実行する際に、必ず OSS コンプライアンス要件が検討されるようにすること。 ☐
3. プロセス管理者は、OSS コンプライアンス作業を製品開発サイクルの早期段階に組み入れ、組織が製品のリリース タイムラインを守れるよう保証すること。 ☐
4. 後期検証 (Late-cycle verification steps) を実施して、外部に配布される前に、すべてのコンプライアンス要件が満たされるよう保証すること。 ☐
5. ビジネス プロセス管理の責任者は、OSS コンプライアンス要件に関する教育を受けており、OSS コンプライアンスの検討事項について充分配慮すること。 ☐

OPEN COMPLIANCE PROGRAM
1796 18th Street, Suite C
San Francisco, CA 94107
+1 415 723 9709
http://www.linuxfoundation.org
compliance@linuxfoundation.org
THE LINUX FOUNDATION

トレーニング

「トレーニング」は、OSS コンプライアンスを履行するために行うべきことを、企業全体が確実に理解するために必要な活動を担当します。

メモ:

1. 組織の OSS ポリシー、および OSS 利用のメリットに関する基本的トレーニングを、OSS に関わるすべての人々、あるいは顧客やサプライヤーとの対話や製品配布業務に関わるすべての人々に提供すること。 ☐
   a) 組織は、トレーニングを受けるべき要員を定義すること。
   b) トレーニングの記録を保持すること。
      i) トレーニングの目的を設定すること。
      ii) 計画されたトレーニングの完了を確認するための追跡作業を行うこと。
   c) OSS トレーニングは、組織のトレーニング カリキュラムに統合され、組織および個人の達成目標の一部とすること。
   d) OSS トレーニングを新入社員のオリエンテーションに組み込んで提供すること。
2. 基本カリキュラムを補足するために、マネージャーおよびマネージャー以外の社員の両方に、OSS に関する追加的なトレーニングを提供すること。たとえば、組織の手続き、ツール、OSS ライセンス、ソフトウェアの設計ガイドラインなどがこれに含まれる。 ☐
3. 社内の OSS 利用者コミュニティの成長を奨励することにより、組織全体が OSS を正しく利用することの重要性を認識するようにすること。 ☐
4. OSS コンプライアンスに関する再教育を定期的に実施すること。 ☐

OPEN COMPLIANCE PROGRAM
1796 18th Street, Suite C
San Francisco, CA 94107
+1 415 723 9709
http://www.linuxfoundation.org
compliance@linuxfoundation.org
THE LINUX FOUNDATION

コンプライアンス プロセス管理

「コンプライアンス プロセス管理」は、OSS コンプライアンスを履行するためのプロセス機能の確立、保守、および改善に焦点を当てます。

メモ:

1. 組織全体にわたり、OSS コンプライアンスを履行するすべての責任について、明確に指定すること。 ☐
   a) 指定されたコンプライアンス オフィサーは、組織の役員レベルの管理層に対し、コンプライアンス問題を随時報告できること。
   b) コンプライアンス サポート チームは、コンプライアンス作業を指導または実行するため、OSRB、ドキュメンテーション、IT などの業務専門家にアクセスできること。
   c) 社外の OSS コミュニティと、コンプライアンス関連のコミュニケーションをとるために、組織の連絡先窓口として、個人またはチームが指定されていること。
   d) 各従業員が意見や質問を発する機会や手段を持てるように、オンブズマンを設置していること。
2. コンプライアンス作業を調整することに責任を負うチームが、製品開発や製品リリースの計画や作業を知ることができ、製品担当チームと効果的に連絡を取り合えること。 ☐
3. プロジェクト管理の基本が、コンプライアンス プロジェクトやコンプライアンス チームの作業の管理に適用されていること。 ☐
   a) コンプライアンスの達成目標が設定されていること。
   b) コンプライアンス プロジェクトの優先順位が設定されていること。
   c) コンプライアンス活動の見積もりが行われていること。
   d) コンプライアンス要員が割り当てられていること。
   e) コンプライアンス プロジェクトが計画およびスケジューリングされ、進捗が追跡され、必要に応じて問題が報告されていること。
4. 組織の OSS 利用の効果、および OSS コンプライアンス作業を評価するために、メトリクスが定義され、収集されていること。 ☐
   a) プロセスの不備に対処するための是正措置が取られること。
   b) コンプライアンス プロセスに対するプロセス改善計画が確立されていること。
5. 組織は、コンプライアンス プロセスに対する改善の可能性を見出すために、社外にフォーカスしたベンチマーキング活動に携わっていること。 ☐
6. 組織は、OSS コンプライアンスに関わるサプライ チェーンの問題に対応するために、常にコミュニティの動きに着目していること。 ☐

OPEN COMPLIANCE PROGRAM
1796 18th Street, Suite C
San Francisco, CA 94107
+1 415 723 9709
http://www.linuxfoundation.org
compliance@linuxfoundation.org
THE LINUX FOUNDATION

OSS インベントリ / 記録管理

「OSS インベントリ / 記録管理」は、組織のニーズに沿って、OSS コンテンツと OSS コンプライアンス作業の正確な記録を保持することにより、コンプライアンス照会に対する応答や、コンプライアンス環境の変化に対応します。

メモ:

1. 組織は、リリース準備中の製品について、コンプライアンス作業の進捗を追跡すること。 ☐

   a) 組織は、OSS 検出プロセスおよび製品コードスキャンと監査の進捗を追跡すること。

   b) 組織は、検出プロセスで確認された OSS 問題の解決を体系的に追跡すること。

   c) 組織は、OSS 事例の調査と承認プロセスの進捗を追跡すること。

   d) 組織は、リリース準備中の製品について、義務履行の進捗を追跡すること。

2. 組織は、定義されている手順に従って、自社製品内の OSS コンテンツ、および
   それが使用されている状況について、完全かつ正確な記録を保持すること。 ☐

   a) 定義されている書式を使用して、含まれている OSS の情報を記録すること。

   b) OSRB は、その調査と調査結果に関する正確な記録を保持すること。
   たとえば、状況によっては異なる結果になりうる承認の制約や条件なども含めること。

   c) 組織は、承認を求められた新しい OSS 使用事例を調査する際、参考として、
   過去の OSS の調査と承認の記録を使用すること。

3. 組織は、ツール、運用システム、プロトタイプ開発などの目的で社内で使用される
   OSS について、完全かつ正確な記録を保持すること。 ☐

   a) 組織は、OSS の社内利用の記録を定期的に調査し、コスト削減、パフォーマンス向上、
   および運用シナジー達成のチャンスを見極めること。

OPEN COMPLIANCE PROGRAM
1796 18th Street, Suite C
San Francisco, CA 94107
+1 415 723 9709
http://www.linuxfoundation.org
compliance@linuxfoundation.org
THE LINUX FOUNDATION

自動化 / ツール サポート

「自動化 / ツール サポート」は、コンプライアンス作業を支援するために、組織によるツールの利用や考慮点について分析します。

メモ:

1. 組織は、コンプライアンス プロセスを評定し、自動化とツール サポートの機会を見極め、優先順位付けしていること。 ☐
2. 組織は、コンプライアンス作業に役立つ可能性のある商用ツールや OSS ツールを定期的に調査していること。 ☐
   a) 体系的なツール評価手段を採用していること。
      i) ツール要件が文書化されていること。
      ii) ツール評価計画が確立され、実行されていること。
      iii) 使用事例とパイロット プロジェクトが定義されていること。
      iv) 評価ライセンスを取得している、あるいは、ツールを試すための別のメカニズムを使用していること。
3. ツール開発・導入のために定義された手続きに従って、ツール入手プロジェクト、またはツール開発プロジェクトが計画および実行されていること。 ☐
4. 組織は、コンプライアンス ツールに関連のあるユーザー グループ会議やコミュニティ フォーラムに参加していること。 ☐
5. コンプライアンス分析を行う必要のある製品の OSS コンテンツやファイルを特定するために、一定のメカニズムが使用されていること。 ☐
6. OSS 問題をクローズまで追跡するために、ツールが使用されていること。 ☐
7. 配布製品のバージョン間に存在するソフトウェア コンテンツの差異を確認するために、一定のメカニズムが使用されていること。 ☐
8. 製品の最初のコンプライアンス ベースラインを構築するのに、その利用が有益である場合は、常にスキャニング ツールを活用していること。 ☐
9. OSS パッケージのリポジトリが保守され、組織がそれを利用できるようになっていること。 ☐

OPEN COMPLIANCE PROGRAM
1796 18th Street, Suite C
San Francisco, CA 94107
+1 415 723 9709
http://www.linuxfoundation.org
compliance@linuxfoundation.org
THE LINUX FOUNDATION

検証

「検証」は、OSS に関する義務が正しく履行されていることを確認するために、OSS コンプライアンス チームによって実行される独立した保証措置です。

メモ:

1. コンプライアンス チームは、定義された手続きに従って、検証作業を実行すること。 ☐
2. コンプライアンス チームは、製品のリリース準備が整うまでに、ソース コード ライセンス義務が履行されていることを検証すること。 ☐
   a) コンプライアンス チームは、ソース コードとして必要なすべての提供物が含まれていることを検証すること。
   b) コンプライアンス チームは、リリース準備段階の製品に含まれている各 OSS パッケージの配布用ステージング領域にソース コードが配置されていること、および、公開の必要があるすべてのソース コードに対して、充分な配布メカニズムが存在することを検証すること。
   c) コンプライアンス チームは、公開されるソース コードが、製品内のバイナリと正しく対応していることを検証すること。
   d) コンプライアンス チームは、ソース コードが組織のビルド環境以外でもビルドできることを検証すること。
3. コンプライアンス チームは、著作権告知、帰属告知、ライセンス文書、およびすべての変更記録が正確に含まれていることを検証すること。 ☐
4. コンプライアンス チームは、リリース製品内のすべての OSS パッケージについて、OSRB の承認が得られていることを検証すること。 ☐
5. コンプライアンス チームは、サードパーティ サプライヤーが、彼らの提供物に含まれているオープン ソースをすべて正確に開示していること、および、これらのサプライヤーが、OSS ライセンスの下で彼らの義務を履行していることを検証すること。 ☐
6. コンプライアンス チームは、オープン ソースを定義された配布メカニズムで取得できること、および、取得したそのソース コードを独立した環境でビルドできることを検証すること。 ☐

OPEN COMPLIANCE PROGRAM
1796 18th Street, Suite C
San Francisco, CA 94107
+1 415 723 9709
http://www.linuxfoundation.org
compliance@linuxfoundation.org
THE LINUX FOUNDATION

プロセス順守の監査

「プロセス順守の監査」は、組織がチェックした項目を参照し、定義されたコンプライアンス プロセスを利用しているか、および、その利用により、期待した結果が得られているかを確認します。

メモ:

1. 「プロセス順守の監査」は、組織が定義されたコンプライアンス プロセスに従っているかどうかを確認すること。 ☐
   a) 監査は、基準外の手法を使用している事例を識別すること。
2. 監査は、コンプライアンス プロセスの実行により、どの程度期待通りのコンプライアンス結果が得られるかを算定すること。 ☐
3. 監査は、その製品の OSS コンテンツと、組織が実行するコンプライアンス作業について、組織が正確な記録を保持しているかどうかを確認すること。 ☐

--- **チェックリスト終了** ---

OPEN COMPLIANCE PROGRAM
1796 18th Street, Suite C
San Francisco, CA 94107
+1 415 723 9709
http://www.linuxfoundation.org
compliance@linuxfoundation.org
THE LINUX FOUNDATION

オープン コンプライアンス プログラムについて

The Linux Foundation のオープン コンプライアンス プログラムは、業界唯一の中立かつ包括的なソフトウェア コンプライアンス戦略です。コンプライアンス コミュニティのメンバーやリーダーのリソースを整理することにより、The Linux Foundation ではオープン ソース ソフトウェアを広く普及させるために必要な個人、企業、法務的要素を結集すると同時に、法務関連のコストおよび FUD（不安や懸念）を低減します。オープン コンプライアンス プログラムは、包括的なトレーニングや情報資料、オープン ソース ツール、オンライン コミュニティ（FOSSBazaar）、ベストプラクティス チェックリスト、企業のコンプライアンス オフィサーの緊急警報ディレクトリ、製品で使用しているソフトウェアを一様に認識およびレポートするための標準などを提供します。オープン コンプライアンス プログラムは、コンプライアンス分野の専門家による主導のもと、Adobe, AMD, ARM Limited, Cisco Systems, Google, HP, IBM, Intel, Motorola, NEC, Nokia, Novell, Samsung, Software Freedom Law Center, Sony Electronics などの企業により支えられています。詳細は、下記のページをご覧ください。

http://www.linuxfoundation.org/programs/legal/compliance

http://www.linuxfoundation.jp/programs/legal/compliance（日本語）

OPEN COMPLIANCE PROGRAM

1796 18th Street, Suite C
San Francisco, CA 94107
+1 415 723 9709
http://www.linuxfoundation.org
compliance@linuxfoundation.org

THE LINUX FOUNDATION

The Linux Foundation は、Linux の普及促進、保護、ならびに
標準化に取り組み、Linux がクローズドなプラットフォームに対抗するのに
必要とされる統合されたリソースとサービスを提供します。

The Linux Foundation、オープン コンプライアンス プログラム、
およびその他の活動については、
http://www.linuxfoundation.jp/ を参照してください。