» オープン コンプライアンス プログラム

FOSS コンプライアンス管理プロセスにおける推奨プラクティスの紹介

パート I

By Ibrahim Haddad (Ph.D.), The Linux Foundation

A White Paper By The Linux Foundation
http://www.linuxfoundation.org

このホワイトペーパーの構成と背景

このホワイトペーパーは、FOSS (フリー&オープン ソース ソフトウェア) コンプライアンスのトピックを取り上げたシリーズの 1 つで、The Linux Foundation がオープン コンプライアンス プログラムのもとで公開している無償の教育資料です。今回は、自社製品に FOSS を組み込む際に履行するべきプラクティスや、考慮事項について取り上げます。次の 2 つの部分で構成されています。

- パート I では、FOSS コンプライアンス管理プロセスの各段階で履行するべきプラクティスについて説明します。
- パート II では、ソースコードの改変、告知、配布、ソフトウェア設計、利用、リンク、コード混合などに関する FOSS コンプライアンスの考慮事項に重点をおいて説明します。また、FOSS コンプライアンス プログラムのさまざまな構成要素に関する推奨プラクティスについても取り上げます。「FOSS コンプライアンス プログラムの構成要素」については、下記のホワイトペーパーを参照してください。
  「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」
  (http://www.linuxfoundation.jp/whitepapers/apply1)

The Linux Foundation では、このような教育用資料のほかに、『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』も公開しています。これは、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て作成された、詳細なコンプライアンス プラクティス チェックリストです。そのようなわけで、このホワイトペーパーのタイトルには「紹介」という語を使用しています。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、コンプライアンス プロセス実装の進捗状況を評価したり、プロセス改善活動の優先順位を決定したりすることができます。このチェックリストの入手方法については、巻末を参照してください。

はじめに

以前公開したホワイトペーパー (http://www.linuxfoundation.org/publications (英語)、および http://linuxfoundation.jp/whitepapers (日本語) からダウンロード可能) でも、FOSS コンプライアンスの詳細な管理プロセスについて取り上げました。そこでの説明の繰り返しになりますが、図 1 は、あるソフトウェア コンポーネントを自社製品のソフトウェア スタックに組み込む際の承認手続きを示しています。このプロセスは、まず、製品のビルド システムにて統合される各種のソフトウェア コンポーネントを識別することから始まり、最終的なライセンス義務のリストを作成して終了となります。以下のセクションでは、FOSS 利用要求に対応するための推奨プラクティスをいくつか紹介します。推奨プラクティスは、このコンプライアンス プロセスの図で説明している各ステップに対応しています。

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

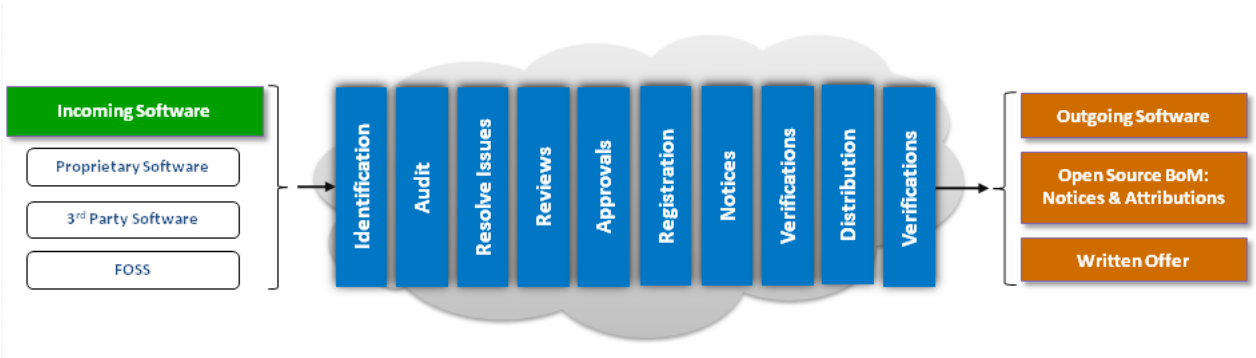

図 1. コンプライアンス管理プロセスの詳細

識別

コンプライアンス プロセスの「識別」ステップでは、製品のビルド システムに入るすべての構成要素、それらの出自、およびライセンス情報を識別します。ソース コードの出自は、大きく分けて 3 種類あります。

- 1 つ目はプロプライエタリ ソフトウェアです。これは、自社の開発者によって作成されたもので、FOSS の断片が含まれている場合があります。また、多くの場合、FOSS に依存あるいはリンクしています。
- 2 つ目はサード パーティ商用ソフトウェアです。サード パーティのソフトウェア提供者やコンサルタントによって開発され、商用ライセンスや FOSS ライセンスのもとで入手されたものです。このソフトウェア カテゴリにも、FOSS の断片が含まれている場合があります。また、多くの場合、FOSS に依存あるいはリンクしています。
- 3 つ目は FOSS ソフトウェアです。FOSS コミュニティのメンバーによって開発されたものです。

コア チームやオープンソース調査委員会 (OSRB) からの指示に基づいて、利用するソフトウェア コンポーネントをすべて識別し、それらをすべてソース コード監査のステップに渡すことをお勧めします。

ソース コード監査

ソース コードの監査やスキャンに関する推奨プラクティスは、4 つあります。

- **全ソース コードをスキャンする:** 製品に組み込まれているすべてのソース コードをスキャンしてください。開発チームが、プロプライエタリ ソース コードやサード パーティ ソース コードの中で FOSS を利用している可能性があります。また、開発チームが FOSS に変更を加えることで、さらなる精査や義務履行の必要が生じている可能性もあります。したがって、製品に組み込まれているすべてのソース コードを識別し、監査することが必須です。
- **既承認パッケージの新バージョンをスキャンする:** 以前承認されたパッケージが、(時には承認された状況とは異なる状況で) 改変されて利用される場合、あるいは、そのまま、または改変されて別の製品に利用される場合、さらには、新しいバージョンがダウンロードされて製品のソフトウェア スタックに適用される場合があります。コンプライアンスというのは、製品ごとに履行されることが原則であるため、ある製品で FOSS の利用が承認されたからといって、別の製品で承認されるとは限りません。つまり、開発者が既承認コンポーネントを改変する場合や、別の製品に使用する場合は、そのコンポーネントのソース コードを

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

スキャンし直し、もう一度承認プロセスまでの手続きを踏む必要があります。

- **FOSS コンポーネントの各新バージョンを確実にレビューおよび承認する:** 開発者が FOSS パッケージのバージョンをアップグレードした時は、新バージョンのライセンスと前回使用したバージョンのライセンスが同じであることを確認してください。バージョンのアップグレードで、ライセンスの変更が発生する場合もあります。したがって、同じコンポーネント (古いバージョン) が過去に承認されていても、もう一度承認プロセスまでの手続きを踏むことをお勧めします。
- **早期かつ頻繁にスキャンする:** 「早期かつ頻繁にリリースする」というのは、FOSS 開発モデルの基本とも言えるオープン ソース開発メソッドです。ソース コードを早期かつ頻繁にリリースすることで、継続的な品質保証活動の一環として、ユーザーがテストし、バグを報告することができるというものです。「早期かつ頻繁なスキャン」もこれと同じ考えで、開発プロセスの早い段階でソース コードをスキャンし、定期的に繰り返すことにより、コンプライアンス活動が開発活動より遅れることなく、並行して進行するようにします。また、スキャン処理が必要なタイミングの条件をリストにすることで、プロセスをさらに効率化することもできます。「早期かつ頻繁にスキャンする」ことにより、次のようなメリットがあります。
  - コンプライアンス問題を即時に発見できる。
  - 発見された問題の解決策を受容可能な時間内に提供できる。
  - 前回のスキャンとの差分が最小限に抑えられる。
  - インクリメンタル スキャンで効率を上げることができる。

問題の解決

ソース コードがスキャンされ、コンプライアンス問題が警告または発見された場合、さまざまな解決方法が考えられます。いくつか例をあげてみましょう。

- スキャン結果に疑問がある場合は、技術担当者と検討します (対象となるソフトウェア コンポーネントの開発者に尋ねる)。
- スキャンツールの警告により、当該ソースコードが予想外の開発元で作成されていることがわかった場合、それぞれのファイルやソースコードの断片を調査し、問題を解決します。
- FOSS に対するソース コードの改変をすべて特定します。コードの改変に関して、技術者の記憶を頼るべきではないでしょう。ビルドツールなどを利用して、コードの改変を識別し、誰が、いつ改変したかを特定してください。
- ソース コード スキャン ツールを実行した結果、たとえば、プロプライエタリ コンポーネントで (そのコンポーネントはプロプライエタリとして維持するものとして)、GPL ライセンスのソース コードが不正に使用されていることがわかった場合は、これを修正リクエストとともに技術担当者に報告します。技術担当者が問題を解決したら、ソース コードを再スキャンし、技術担当者が GPL ソース コードを削除したこと、およびプロプライエタリ ソース コードで置換したことを必ず確認してください。
- 法務検査に備えて、スキャン ツールが生成したソース コード監査レポートだけでなく、そのコンポーネントのライセンスに関する全情報を弁護士に提供することをお勧めします。
  - FOSS コンポーネントの場合には、COPYING、README、または LICENSE ファイルを提供します。

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

- サード パーティ ソフトウェア プロバイダーから受け取ったソフトウェア コンポーネントの場合には、ライセンス契約書も提供します。

レビュー (調査)

コンプライアンス プロセスの一環として、各種のレビューが行われます。ここでは、アーキテクチャ レビューとリンク解析レビューについて説明します。アーキテクチャ レビューとは、FOSS とプロプライエタリやサード パーティのソフトウェア コンポーネントとの間の相互関係を解析することです。通常、アーキテクチャ レビューには、対象製品の担当アーキテクトと、重要なソフトウェア コンポーネントの開発担当者を参加させます。
このレビューの目的は、次の項目を明らかにすることです。

- (そのまま使用されている、あるいは改変されている) FOSS コンポーネント
- プロプライエタリなコンポーネント
- 商用ライセンスのもとでライセンスされているサード パーティのコンポーネント
- コンポーネントの依存状態
- 通信プロトコル
- 動的リンクか、静的リンクか (次のセクションを参照)
- カーネル スペースにあるコンポーネントとユーザー スペースにあるコンポーネント
- 共有ヘッダー ファイルを使用するコンポーネント
- 当該ソフトウェア コンポーネントが相互作用する、または依存する他の FOSS。
  特にそれが異なる FOSS ライセンスによって管理されている場合。

アーキテクチャ レビューの結果により、FOSS からプロプライエタリ コンポーネントやサード パーティ コンポーネントにライセンス義務が拡張する可能性があるかどうかが解析されます。

アーキテクチャ レビューの延長がリンク解析レビューです。その目的は、問題発生の可能性のあるコードの組み合わせを静的および動的リンクレベルで検出することです。推奨プラクティスは、ビルド システム内の全バイナリに対する動的および静的リンク解析の実行です。これにより、プロプライエタリ ソフトウェア コンポーネントやサード パーティ ソフトウェア コンポーネントに、何らかの FOSS 義務が及んでいるかどうかがわかります。

このようなレビューや解析は、自動ツールによって簡単に実行できます。自動ツールは、ビルド システムをくまなく探し、事前定義されたルールやポリシーに基づいて、リンクの矛盾の可能性を警告します。リンク問題が見つかった場合は、問題の説明と解決案を添えて、技術担当者あてにバグ チケットを発行します。
技術担当者は、問題の解決を確認後、リンク解析を再実行し、自身が行ったコード変更が、実際に新たな問題を起こすことなくリンク問題を解決したことを必ず確認してください。

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

依存状態チェッカー ツール (Dependency Checker Tool)

依存状態チェッカー ツールは、企業や個人のコンプライアンス精査を支援するために、The Linux Foundation により、オープン コンプライアンス プログラムの一環としてリリースされました。他のオープン ソース プロジェクトと同様に、このプロジェクトもオープンであり (オープンなメーリング リスト、オープンな git リポジトリ、オープンなバグ登録システムである bugzilla などを使用)、オープン ソース開発プロセスによって管理されています。このツールの目的は、動的および静的リンク レベルで、問題発生の可能性のあるコードの組み合わせを警告することです。このツールは、ツールの使用者が事前に定義したライセンス ポリシーに基づいて、バイナリとライブラリー間のリンクの矛盾を識別します。このツールには、さまざまな機能があるため、コンプライアンスの容易な履行を実現するプラットフォームとして利用できます。

リソース

- git でソース コードにアクセス: http://git.linuxfoundation.org/?p=dep-checker.git
- メーリングリストに登録: https://lists.linux-foundation.org/mailman/listinfo/dep-checker-dev
- bugzilla でバグを報告または機能をリクエスト: http://bugs.linuxfoundation.org ("Compliance" プロジェクトを選択してから、"Dependency Checker Tool" コンポーネントを選択)
- 依存状態チェッカー ツールに関するホワイトペーパーをダウンロード: http://www.linuxfoundation.org/sites/main/files/publications/lf_foss_compliance_dct.pdf

承認

コンプライアンス プロセスの承認ステップには、2 つの主要な推奨プラクティスがあります。

- コンプライアンス チケットを承認する前に、そのコンプライアンス チケットに関するすべてのサブタスクが完了し、クローズされていることを確認します。サブタスクを忘れたり、問題をペンディング状態で残すことはありがちですが、オープン イシューを残したまま、コンプライアンス チケットをクローズしてはいけません。
- 承認または否認に至った検討の概要を記録します。コンプライアンスの照会を受けた場合、対象のコンポーネントがどのような理由で承認されたのか、およびどのように問題が解決されたかを追跡できるため、大変有効です。

告知

自社製品に FOSS を使用している企業は、以下の作業を行う必要があります。

- 完全な著作権告知および帰属告知を提供し、FOSS を使用していることを表明します。製品のエンドユーザーに、対応する FOSS ソース コードのコピーの入手方法を通知します (たとえば GPL や LGPL など、ソース コードの提供が必要な場合)。
- 製品に組み込まれている FOSS コードのライセンス契約書の全文を転載します。

ここでの推奨プラクティスには、次のようなものがあります。

- FOSS を製品に組み込むことが承認されたら、帰属告知とライセンス告知を収集します。こうすることに

OPEN COMPLIANCE PROGRAM

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

THE LINUX FOUNDATION

より、企業が公開する必要のある告知ファイルは、常に最新で、すべての FOSS のリスト、ライセンス情報、著作権告知、および帰属告知を含むようになります。

- 書面によるオファー (written offer) にはわかりやすい表現を使用し、製品に組み込まれているすべての FOSS を含めます。
- 製品自体、または製品のドキュメント (ユーザー マニュアルや CD-ROM) と Web サイトのいずれかまたは両方で、この情報の入手方法について、製品のエンド ユーザーに確実に知らせてください。

検証

検証にはいくつもの作業が含まれているため、コンプライアンス チームが行うすべての検証作業のチェックリストを作成し、随時改訂して、一貫性を保ち、検証作業の見落としを防ぐことが大切です。

配布前の検証ステップには、以下のような作業が含まれます。

- 配布予定のすべての FOSS パッケージが識別および承認されていることの検証。
- ソース コード パッケージから不適切なコメントが削除されていることの検証。
- ソース コード パッケージ (改変も含む) が、製品内のバイナリに対応していることが確認されていることの検証。
- すべての適切な告知が製品ドキュメントに含まれていることの検証、および必要に応じ、製品内の FOSS のソース コードの要求権についてエンド ユーザーに通知する「書面によるオファー」が有効であることの検証。

FOSS パッケージをディストリビューション Web サイトにアップロードしたら、以下のような「配布後検証」作業を行ってください。

- パッケージが正常にアップロードされていることの検証。
- 外部コンピューターで、パッケージをエラーなくダウンロードおよび解凍できることの検証。
- パッケージが適切にコンパイルできることの検証。

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

コード管理ツール (Code Janitor Tool)

ソース コードを公開する前に、企業は通常、言語チェックを行い、開発者がソース コード内に将来の製品コード、製品名、競合に関する言及などの不適切なコメントを残していないか確認します。コード管理ツールは、The Linux Foundation がオープン ソース プロジェクトとして手がけたもので、ユーザーが不適切な文言やキーワードのデータベースを作成すると、ツールはそのデータベースを使用して、コードのブルート フォース スキャン (総当たりスキャン) を行います。スキャンの結果として、問題のある「キーワード」を含むファイルの一覧が出力されます。

リソース

- git でソース コードにアクセス: http://git.linuxfoundation.org/janitor.git
- bugzilla でバグを報告または機能をリクエスト: http://bugs.linuxfoundation.org ("Compliance" プロジェクトを選択してから、"Janitor Checker Tool" コンポーネントを選択)
- メーリングリストに登録: https://lists.linux-foundation.org/mailman/listinfo/code-janitor-dev
- コード管理ツールに関するホワイトペーパーをダウンロード: http://www.linuxfoundation.org/sites/main/files/publications/lf_foss_compliance_cjt.pdf

まとめ

このホワイトペーパーでは、FOSS コンプライアンス管理プロセスの各ステップで利用するべきプラクティスについて説明しました。パート II では、ソースコードの改変、告知、配布、ソフトウェア設計、利用、リンク、コード混合などに関する FOSS コンプライアンスの考慮事項について取り上げます。

Linux Foundation リソース

- **オープン コンプライアンス プログラム:** http://www.linuxfoundation.jp/programs/legal/compliance
- **専門的/包括的コンプライアンストレーニング:** The Linux Foundation では、オープン ソース ライセンス準拠を履行する必要があり、オープン ソース コンプライアンス プログラムを確立する必要がある人々や企業向けに、あるいはコンプライアンスについて詳しく学習したい方のために、コンプライアンスの専門家による実践的なトレーニングを提供しています。インストラクターが指導するライブ リモート トレーニングに加え、ライブ オンサイト トレーニングも提供されています。 http://www.linuxfoundation.jp/programs/legal/compliance/training-and-education
- **コンプライアンス関連のホワイトペーパー:** http://www.linuxfoundation.jp/whitepapers
- **オープン コンプライアンス ディレクトリと緊急警報システム:** http://www.linuxfoundation.jp/programs/legal/compliance/directory
- **コンプライアンス ツール:** http://www.linuxfoundation.jp/programs/legal/compliance/tools
- **ソフトウェア パッケージ データ交換 (Software Package Data Exchange™):** SPDX™ 仕様とは、ソフトウェア パッケージに関連するコンポーネント、ライセンス、および著作権情報をやりとりするための標準フォーマットです。http://www.spdx.org/

OPEN COMPLIANCE PROGRAM

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

THE LINUX FOUNDATION

- **FOSSBazaar:** 企業におけるフリー & オープン ソース ソフトウェア導入を促進するために協力し合う技術/業界リーダーのオープン コミュニティです。http://fossbazaar.org/

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

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、コンプライアンス プロセス実装の進捗状況を評価したり、プロセス改善活動の優先順位をしたりすることができます。このチェックリストは、2010 年 11 月 1 日より The Linux Foundation の Web サイトで公開されています。こちらから、コピーをダウンロードできます。
http://www.linuxfoundation.jp/whitepapers/apply4

謝辞

このホワイトペーパーの作成にあたっては、Karen Copenhaver 氏 (The Linux Foundation のリーガル ディレクター兼 Choate, Hall & Stewart LLP 社 Business & Technology practice 所属のパートナー)、ならびに Philip Koltun 氏 (The Linux Foundtion の Open Compliance Program ディレクター) から、貴重なレビューやアドバイスをいただきました。ありがとうございました。

作者について

Ibrahim Haddad は The Linux Foundation のモバイル Linux 戦略を管理しており、次世代モバイル コンピューター機器向けの Linux プラットフォームを進化させるために、コミュニティと協力し、ベンダー中立な環境を推進しています。

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 コンプライアンス構想です。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集結させることにより、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、および法務などの要素を結集すると同時に、法務関連のコストや 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。詳細については、下記のページをご覧ください。
http://www.linuxfoundation.jp/programs/legal/compliance

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

The Linux Foundation は、
Linux の普及促進、保護、ならびに発展に取り組み、
Linux/OSS 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。