OPEN SOURCE COMPLIANCE IN THE ENTERPRISE

Ibrahim Haddad, PhD

This page intentionally left blank.

Ibrahim Haddad, Ph.D.

The Linux Foundation

2016

Open Source Compliance in the Enterprise

4

Copyright c 2016 The Linux Foundation

All rights reserved

5

Contents

Chapter 1 INTRODUCTION TO OPEN SOURCE COMPLIANCE 16

A CHANGING BUSINESS ENVIRONMENT 16

ENTER OPEN SOURCE COMPLIANCE 19

Benefits of Ensuring Open Source Compliance 20

FAILURE TO COMPLY 21

Intellectual Property Failures 22

License Compliance Problems 24

Process Failures 26

LESSONS LEARNED 28

Ensure Compliance Prior to Product Shipment/Service Launch 28

Non-Compliance is Expensive 29

Relationships Matter 30

Training is Important 30

Chapter 2 ESTABLISHING AN OPEN SOURCE MANAGEMENT PROGRAM 31

OPEN SOURCE COMPLIANCE PROGRAM 31

Compliance Strategy 32

Inquiry Response Strategy 32

Policies and Processes 32

Compliance Teams 33

Tools 34

Web Presence 35

Education 36

Automation 37

Messaging 37

COMPLIANCE CHALLENGES AND SOLUTIONS 37

Long-Term Goals versus Short-Term Execution 39

Communicating Compliance 40

Establishing a Clean Software Baseline 41

Maintaining Compliance 42

Institutionalization and Sustainability 43

Chapter 3 ACHIEVING COMPLIANCE: ROLES AND RESPONSIBILITIES 46

OPEN SOURCE REVIEW BOARD (OSRB) 50

LEGAL 53

ENGINEERING AND PRODUCT TEAMS 55

COMPLIANCE OFFICER 57

OPEN SOURCE EXECUTIVE COMMITTEE 58

DOCUMENTATION 58

LOCALIZATION 59

SUPPLY CHAIN 59

IT 60

CORPORATE DEVELOPMENT 60

Chapter 4 OPEN SOURCE COMPLIANCE PROCESS 62

EFFECTIVE COMPLIANCE 63

ELEMENTS OF AN END-TO-END COMPLIANCE PROCESS 64

ステップ1Identification of Open Source 65

ステップ 2 . Auditing Source Code 67

ステップ3Resolving Issues 70

ステップ4Reviews 70

ステップ5Approvals 72

ステップ6Registration 73

ステップ7Notices 74

ステップ8. Pre-Distribution Verifications 75

ステップ9Distribution 76

ステップ10Final Verifications 76

Chapter 5 COMPLIANCE PROCESSES AND POLICIES 78

POLICY 78

PROCESS 79

Source Code Scan 79

Identification and Resolution 81

Legal Review 81

Architecture Review 82

Final Review 83

PROCESS STAGES’ INPUTS AND OUTPUTS 83

Source Code Scan Phase 84

Identification and Resolution Phase 85

Legal Review Phase 85

Architecture Review Phase 87

Final Approval Phase 87

DETAILED USAGE PROCESS 88

INCREMENTAL COMPLIANCE PROCESS 93

OSRB USAGE FORM 95

Rules Governing the OSRB Usage Form 99

AUDITING 99

SOURCE CODE DISTRIBUTION 100

Distribution Incentives 100

Distribution Policy and Process 101

Distribution Methods and Modes 103

Distribution Checklists 104

Pre-Distribution Checklist 105

Post-Publication Checklist 107

Written Offer 107

Chapter 6 RECOMMENDED PRACTICES FOR COMPLIANCE PROCESS MANAGEMENT 109

COMPLIANCE PROCESS 109

Identification Phase 109

Source Code Auditing 111

Resolving Issues 112

Reviews 113

Approvals 114

Notices 115

Verifications 115

TOOLS AND AUTOMATION 116

Source Code Identification Tools 117

Project Management Tools 118

Software Bill of Material (BOM) Difference Tools 118

Linkage Analysis Tool 119

CHAPTER 7 MANAGING COMPLIANCE INQUIRIES 121

RESPONDING TO COMPLIANCE INQUIRIES 122

Acknowledge 122

Inform 123

Investigate 123

Report 123

Close Inquiry 124

Rectify 124

Improve 124

General Considerations 124

CHAPTER 8 OTHER COMPLIANCE-RELATED PRACTICES 125

EMPLOYEE APPRAISAL 125

WEB PORTALS 126

MESSAGING 126

TRAINING 127

Informal Training 127

Formal Training 128

SOURCE CODE MODIFICATION CONSIDERATIONS 128

NOTICES CONSIDERATIONS 128

DISTRIBUTION CONSIDERATIONS 129

USAGE CONSIDERATIONS 130

ATTRIBUTION CONSIDERATIONS 132

Attribution Types 132

Presentation of Attributions 133

SPECIFIC LICENSE OBLIGATIONS 133

GENERAL GUIDELINES 135

Chapter 9 SCALING OPEN SOURCE LEGAL SUPPORT 137

PRACTICAL LEGAL ADVICE 137

LICENSE PLAYBOOKS 138

LICENSE COMPATIBILITY MATRIX 139

LICENSE CLASSIFICATION 141

SOFTWARE INTERACTION METHODS 143

CHECKLISTS 145

CONCLUSION 146

PREFACE

My involvement with open source compliance started early in my career as a software developer, and has been a part of my job directly or indirectly for two decades now. Throughout my journey working with open source software, it was difficult to find practical references on open source compliance. My interest grew in making my own experiences available so that others could possibly learn from them, and then publish their experiences, so that as an industry we can all strive towards better ways to achieve open source compliance while minimizing impact on engineering resources and product delivery timelines.

This handbook summarizes my experience driving open source compliance activities in the enterprise, and focuses on practical aspects of creating and maintaining an open source compliance program. Since most of my experience was focused in the embedded space (with C and C++ being the dominant programming languages), this emphasis comes across throughout this handbook.

I hope you find it useful in your day-to-day drive to achieve open source compliance.

Foreword

Open source has expanded not only from an idealistic movement led by individuals around software and intellectual property but from one where organizations (e.g., governments, companies, and universities) realize that open source is a key part of their IT strategy and want to participate in its development. Early success in Linux and other open source technologies has spread to all areas of technology.

More traditional organizations are also taking notice; they are making open source software a priority and using the software for strategic advantage in their operations.

Use of open source in enterprise IT has doubled since 2010.

78% of surveyed companies run their businesses on open source.

64% currently participate in open source projects.

39% plan to launch their own open source projects.

North Bridge & Black Duck

“The 2015 Future of Open Source Survey”

“Open Source First: Simply put, any solution developed using taxpayer dollars should be in the taxpayer’s domain (open source). At GSA, we believe that all code we developed should be shared under an open license so others may benefit from it. In addition, we will give priority to using open source software as we design now solutions.”

Office of the CIO, U.S. General Services Administration (U.S. agency that oversees $66 billion of procurement annually)

“The development of Blockchain technology has the potential to redefine the operations and economics of the financial services industry. It emerges at an important time, as the industry strives to be leaner, more efficient, and more digital. Open source development will accelerate the innovation and help drive the scalability of this technology, and we are proud

to support the Hyperledger Project.”

Richard Lumb, Chief Executive, Financial Services, Accenture

“From increasing member investments to a growing, vibrant developer community, the Dronecode Project’s first year has been extremely exciting. By bringing efforts together to establish a common platform and utilizing open source best practices, we’re able to build the foundation for a new era of drone applications that extend from the camera to the cloud. The Dronecode ‘full-stack’ platform approach, combined with the hardware and software innovations of its members, will bring about a new generation of drones that are autonomous, aware of their environments, and continuously connected . an airborne Internet of Things.”

Chris Anderson, CEO, 3DR

(Former Editor in Chief of Wired magazine and author of “The Long Tail”)

“Open source is essential to our development process. It’s a powerful approach that lets people work together to build great solutions while realizing shared benefits.”

Rob Alexander, CIO, Capital One

Organizations are looking for guidance on how best to participate appropriately in open source communities and to do so in a legal and responsible way. Participants want to share their code and IP, and they need a trusted neutral home for IP assets (trademark, copyright, patents). They also need a framework to pool resources (financial, technical, etc.).

Participants need expertise to train them how to collaborate with their competitors in an effective manner. To that end, this book is geared to creating a shared understanding on the best ways to create shared value and innovation while adhering to the spirit and legal particulars of open source licensing.

第1章

オープン ソース コンプライアンス導入

変わりゆくビジネス環境

従来、プラットフォームやソフトウェアスタックはプロプラエタリなソフトウェアを使って実装され、内部開発されたソフトや交渉の結果であるライセンス条件によるサードパーティのソフトから成る様々なソフトウェアのブロックから構成されていました。ビジネス環境は予測可能で、企業は潜在的なリスクをソフトウェアベンダーとのライセンス交渉や契約交渉を通じて軽減していました。全てのソフトウェアコンポーネントについて誰が提供者であるかを知るのは大変容易でした。図１は従来のハードウェア、ソフトウェアのプラットフォームについて主なブロックを示したものです。

図1プロプラエタリなソフトウェアのブロックに依る従来のソフトウェアプラットフォームの単純化したアーキテクチャ

時と共に企業はOSSを自社のプラットフォームやソフトウェアスタックに組み込み、その恩恵に預かるようになってきました。その理由は製品ごとに様々ですが、様々な業界で共通するのは、オープンソースのコンポーネントには即座に使える卓越した特徴があったこと、分散的な開発による市場投入への時間短縮により経済的に有意の利益があったこと、そしてソースコードをカスタマイズするという新しく出来ることを提供したこと、です。その結果、複数のソースによる新たな開発モデルが登場しました。その結果、複数のソースによる新たな開発モデルが登場しました。

この新たなモデルでは、製品は下記の任意の組み合わせとなります。

. プロプラエタリなコード、その製品やサービスを作る企業が開発したものプロプラエタリなコード、元々はその企業によりオープンソースのライセンス下でオープンソースのコンポーネントを統合したり適用したりすることで開発されたが、上流のオープンソースプロジェクトに寄付されず戻されなかったものサードパーティの商用コード、サードパーティのソフトウェアプロバイダにより開発され、製品やサービスを作る企業が商用ライセンスの下で受領したものオープンソースのコード、オープンソースのコミュニティにより開発され、製品やサービスを作る企業がオープンソースライセンスの下で受領したもの

図２（次ページ）に複数のソースによる開発モデル、および入ってくるソースコードの様々な組み合わせを示します。

この開発モデルでは、ソフトウェアコンポーネントは任意の数の出所から来た、様々なライセンス下でライセンスされたソースコードから構成され得ます。たとえば、ソフトウェアコンポーネントAはサードパーティのプロプラエタリのコードに加えプロプラエタリなコードも含んでおり、ソフトウェアコンポーネントBはオープンソースプロジェクトからのソースコードに加えプロプラエタリなコードを含む、などです。

図 2 マルチソース開発モデル

かつては明らかにプロプラエタリなソフトウェアスタックだったものの中にオープンソースのソフトウェアのコンポーネントが増えていくに従い、ビジネス環境は慣れ親しんだ領域、企業が好む環境から離れていきます。

図３（次ページ）はあるプラットフォームやソフトウェアスタックにおいて、様々な階層でオープンソースソフトウェアを受けいれる様子を示したものです。

プロプラエタリな開発モデルと、マルチソースによる開発モデルとの大きな違いの一つは、オープンソースソフトウェアのライセンスは交渉するものではないことです。ソフトウェアの提供者（すなわちオープンソースの開発者やプロジェクト）と調印する契約はありません。そうではなく、オープンソースプロジェクトを開始した人々が所定のライセンスを選びます。そしてプロジェクトがある規模に達すると、変更は事実上不可能となります。マルチソースの開発モデルを使うとは、数十の相異なるライセンス（とライセンスの組み合わせ）に基づく数百人、時には数千人のライセンス提供者やコントリビューター（著作権者）と関わること、を企業は理解しなければなりません。その結果、かつては企業対企業のライセンスや合意に至る交渉を通じて管理されていたリスクは、強固なコンプライアンスプログラムと、注意深いエンジニアリングの実施によって管理されることになります。

図3A simplified view of the architecture of a modern software platform, showing the proliferation of open source inside each of the software building blocks.

オープンソースコンプライアンス手始め

オープンソースのイニシアチブやプロジェクトを使う事で、企業や組織はオープンソースソフトウェアの開発者を代表する数百、時に数千のコミュニティと協力し、イノベーションを加速できるようになります。しかしながら、オープンソースのコミュニティと組むには責任が伴います。オープンソースのライセンスに伴う義務を順守することを保証しなければなりません。

オープンソースのコンプライアンスとは、オープンソースのユーザー、インテグレーター、開発者が著作権表示をきちんと見て、自らに関わるオープンソースのソフトウェアコンポーネントのライセンス上の義務を満たすプロセスです。適切に規定されたオープンソースのコンプライアンスのプロセスは、ライセンス条項の順守を保証すると同時に、企業自身、あるいはサードパーティのサプライヤの知的財産が意図せず公開されたり、その他不適当な結果を招いたりしないように設計されるべきです。

オープンソースのコンプライアンスは3つの主要な目的の達成に役立ちます。

. ライセンス上の義務に従う

. オープンソースが商用製品で効果的に使われることを助ける. サードパーティとの契約上の義務に従う

オープンソースのコンプライアンスを保証する利点

オープンソースのコンプライアンスを達成する事にはいくつかの利点があります。確固たるコンプライアンスプログラムを持つ企業は技術的にも利益を得ることが多いです。規定に従っているソフトウェア群の資産はサービスし、試験し、アップグレードし、保守することが容易だからです。更に、コンプライアンスの活動は、様々な製品や部門で使われていてカギとなる、組織にとって高度に戦略的で利益をもたらすオープンソースソフトウェアの洗い出しにつながります。また逆に、レビューを繰り返すことを通じてコンプライアンスは、オープンソースのコンポーネントの利用に伴うコストやリスクを示すことにもなります。

健全なコンプライアンスのプログラムは外部コミュニティと協業する上でも大いに有用です。コンプライアンス上の問題が生じた時、そうしたプログラムは会社が善意であることを示すことができます。

最後に、頻度は下がるが強固なコンプライアンスのプログラムがもたらす利益として、例えば、会社の買収や売却、新製品や新サービスのリリースのためより良い準備となる、が挙げられます。オープンソースへのコンプライアンスの保証はそうした業務が完了する前に終了させることが必須だからです。更には、OEMや下流のベンダーとの取引においてコンプライアンスが検証できることは付加的な優位となります。

コンプライアンスの失敗

ソフトウェア開発の全工程において、コンプライアンスプログラム上のエラーや不十分さはコンプライアンス上の失敗に繋がることがあります。下記はこうした失敗の例です。

. 不適切な帰属表示 (attribution notice)帰属表示は通常、テキストファイルとしてオープンソースのコンポーネントと共に提供され、オープンソースコンポーネントへのコントリビューターが提供したことを示します。

. ライセンス表示提供を怠るライセンス表示とは、製品やスタックに含まれるオープンソースのライセンス文書を含んだファイルで、多くの場合、製品の文書と共に、あるいは製品やアプリケーションのUIと共に提供されます。

. 著作権表示の省略著作権表示は、ソフトウェアのコピーにつけられる識別情報で、著作権者を示します。

. 変更表示の付け忘れ変更表示とは、ソースコードに対する変更をチェンジログ内で表示する、GPLやLGPLで必要になるものです。一例を下記に示します。

/\* \* Date Author Comment \* 10/15/2015 Ibrahim Haddad Fixed memory leak in nextlst() \*/

. 不十分な、あるいは誤解を招く主張

. ソースコード提供の失敗ソースコードを利用可能とすること（変更を含む）はGPL/LGPLライセンスファミリーの要求の一つです。

. GPL/LGPL等のライセンスのソースコードを使う際に書面で告知しない書面での告知は、その製品のエンドユーザーに対してその製品に含まれるオープンソースソフトウェアの情報、そして頒布されるべきソースコードをダウンロードする方法を開示します。It is usually provided as part of the product documentation and also accessible from the product’s user interface. 書面告知の基本的な例は下記のようになります。

Foobarの本製品の中で使われているソフトウェアに関連する、FooBar社が公開しているソースコードのコピーを得るには、http://opensource.foobar.com にアクセスするか、opensource@foobar.com にメールでリクエストを送るか、またはリクエストを通常の郵便で

Foobar株式会社

オープンソースプログラム室

住所、郵便番号

City, State, Postal Code

国名

. ビルド用スクリプトを提供しない　コンパイルに必要なもの（GPLやLGPLファミリのライセンス毎に）。

知的財産権上の失敗

表1 (次ページ) はソフトウェア開発の過程においてプロプラエタリな知財とオープンソースの知財を誤って混ぜてしまい、ライセンスコンプライアンス問題となるありがちな例を示したものです。もっともありがちなのは、異なる、または両立しないライセンス（例：プロプラエタリ、サードパーティやオープンソース）下のソースコードを混ぜてしまう、ことです。そうして混ぜてしまうと企業はプロプラエタリなソースコードをオープンソースライセンスで開示することを強制され、（おそらくは）高い価値を持つ知財の制御を失い、市場における差別化が弱くなってしまいます。

知財上の失敗は下記を招く。

. 差し止め命令によりコンプライアンス上の懸念が解決されるまで製品が出荷できない問題のバイナリコードに関わるプロプラエタリなソースコードを（ケースに応じた）オープンソースライセンスで配布するよう要求されますコンプライアンス上の懸念を解消するため多大な工数が費やされます顧客、ディストリビュータ、サードパーティのソフトウェア供給者、そしてオープンソースコミュニティを困惑させます

表１知財上の失敗の例

問題の類型

発見する方法

回避方法

オープンソースのコードをサードパーティのコードに挿入

開発プロセスの中で開発者がオープンソースのコード (いわゆるスニペット) をプロプラエタリやサードパーティのコードに挿入して発生

オープンソースのコードとの一致の可能性を求めてソースコードをスキャン

コンプライアンスやオープンソースライセンス、プロプラエタリやサードパーティのコードにオープンソースのコードを含めることの意味について認識するためのトレーニングを提供

予期されないライセンスやコードのスニペットのため、定期的にプロジェクトの全ソースコードをスキャン

オープンソースソフトウェアを使う際には製品のレポジトリにコミットする前に承認を必要とするようにします

問題の類型

発見する方法

回避方法

オープンソースのソフトウェアをプロプラエタリなソースコードのソフトウェアにリンク (またはその逆。C/C++特有の問題) specific to C/

C++ source code)

衝突(conflict)する、または互換性のない(incompatible)[03] ライセンスのソフトウェアコンポーネントをリンクした結果発生

異なるソフトウェアコンポーネント間のリンクを検出できる依存性追跡ツールを利用; 企業のオープンソースポリシーで許容されているかを識別

企業のコンプライアンスポリシーに基づくリンクのシナリオについての訓練を提供

定期的に依存性追跡ツールを動作させ、全てのリンク関係を検証; 企業のポリシーで許容されていないあらゆる事柄にフラグを立てます

オープンソースのコンポーネントにプロプラエタリなコードを含めます

開発者がプロプラエタリなソースコードをオープンソースソフトウェアにコピー/ペーストして発生

ソースコードをスキャンする。ツールでオープンソースのコンポーネント由来ではないソースコードは識別できるので、監査のため各種のフラグをつけます

スタッフを訓練

ソースコードを定期的に検査

プロプラエタリなソースコードをオープンソースのコンポーネントに含めるには承認を必要とするようにします

ライセンスコンプライアンス問題

ライセンスコンプライアンス問題は知財上の問題に比べ一般に損害は小さいです。自社のプロプラエタリなコードをオープンソースライセンスで開示するといった副作用がないからです。

ライセンスコンプライアンス上の失敗は下記のいずれか（か、その組み合わせ）を招き得ます。

. ソースコードが開示されるまで製品出荷を差し止める命令

. バージョンのミスマッチによりカスタマーサポート・カスタマーサービス上の問題となる（サポートホットラインに電話やemailでソースコード開示について問い合わせがくる結果）

. 顧客やオープンソースコミュニティにおいて困惑や悪い評判を招く

表２にソフトウェア開発プロセスでの最も一般的なライセンスコンプライアンス問題の例、および回避方法を示します。

表2Examples of license compliance problems and how to avoid them

問題の類型

回避方法

ライセンス上の義務の一環としてソースコードのパッケージを出版[05] (publish)したり利用可能としたりし損ねる

詳細なコンプライアンスチェックリストに従い、製品やアプリケーション、ソフトウェアスタックの出荷時には全てのコンプライアンス上のアクションアイテムが完了したことを確認

出荷されたバイナリと異なるバージョンのソースコードを提供

検証作業をコンプライアンスプロセスに追加し、提供するソースコードのバージョンが、出荷される バイナリのバージョンと確かに正確に対応することを確認

出荷製品に組み込まれたオープンソースソフトウェアへの変更をリリース忘れ

部品表 (bill of material, BOM) 差分検出ツールを使いリリース毎のソフトウェアコンポーネント変更を特定

コンプライアンスプロセスにおいて、より新しいバージョンのソフトウェアコンポーネントを再導入

「diffの計算」を変更された(オープンソースとするにふさわしい) ソースコードのチェックリストに加え 、製品に使われたオープンソースのリリース前に行う

問題の類型

回避方法

変更されたオープンソースのコードにマークを付け忘れる、変更の記述を入れ忘れる

ソースコードへのマーク付けをソースコードのリリース前のチェックリストに加え、ダウンロードしたオリジナルのコピーとの差分すべてに確実にマーク

ソースコードのリリース前に検査

変更されたソースコードが適切にマークされていることを、コンプライアンスプロセス上のマイルストーンとする

ソースコードの変更履歴をアップデートすることを、開発プロセスの一部とするようスタッフを教育

コンプライアンスプロセス上の失敗

コンプライアンスプロセス上の失敗は、オープンソースのライセンス条件の侵害、例えばライセンス上の義務を満たさない、に繋がる。表３にソフトウェア開発で起きる最も一般的なコンプライアンスプロセス上の失敗のリスト 、および回避方法を示します。

表3Sample process compliance failures

失敗

回避方法

開発者が企業内のオープンソース委員会 (時にオープンソース評価委員会と呼ばれる) オープンソースソフトウェアの利用申請をしない、期限までに行わない

コンプライアンスポリシーとプロセスについての教育

Conduct periodic full scans of software platform to detect any OS not corresponding to a given approval form. 定期的にソフトウェアプラットフォーム の全スキャンを行い、承認された型に該当しないオープンソースを検出。もしビルドされたシステムに該当するコンプライアンスチケットがないオープンソースコンポーネントが検出されたら、自動で新チケットを発行（企業がBugzillaのようなツールに埋め込まれているワークフローを使ってソフトウェアコンポーネントを追跡していると仮定）

業績評価にコンプライアンスを含める。例えばコンプライアンスポリシーに従わなかったらボーナス査定に直結

開発者がオープンソースの利用申請を早期に、オープンソースのコード の利用を決める前でも行うよう命令

オープンソースの訓練を受けない

オープンソースの訓練は従業員のキャリア開発計画の一部であり、業績評価プロセスの一部としてモニタされていることを念押し

ソースコードの監査を行わない

コンプライアンスのスタッフを適切に訓練

ソースコードを定期的にスキャン

繰り返される開発プロセスのマイルストーンに監査を確かに入れ込む

適切なレベルのスタッフを揃え、監査がスケジュール遅れとならないようにする

監査で発見された問題を解決しない

監査レポートが完結しない限りコンプライアンスチケットをクローズ させない。チケットのクローズは、関連するサブのタスクが存在しない時のみとする

得た教訓

この数年で明るみに出たコンプライアンス違反が数件ありました。そうしたコンプライアンス違反の法的な決着を通じて、オープンソースのプロフェッショナル達は次のような教訓を学びつつあります。lessons that we will explore in following subsections.

製品出荷やサービス立ち上げに先立ちコンプライアンスを確実に行う

コンプライアンス違反事件の最も重要な教訓は、関係した企業は最終的には問題のライセンス条項に従わなければならなかった、のであり、この事実を踏まえた問題解決のコストは基本的なコンプライアンスのコストを圧倒的に上回っていた、のです。従って、製品出荷やサービス立ち上げに先立ってコンプライアンスを確実に行うのが賢いやり方です。

コンプライアンスは法務部門の業務に留まるものではない、と認識することは重要です。全部門が関わって適切なコンプライアンス、正しいオープンソースの利用、必要に応じた再配布、を確実に行う必要があります。この関わりには首尾一貫したコンプライアンスポリシーや手続きの確立と維持管理、利用中（プロプラエタリ、サードパーティ、オープンソース）の全ソフトウェアコンポーネントのライセンスが共存し得ることを製品出荷やサービス立ち上げ前に確認すること、が含まれます。そのためには企業はオープンソースを管理するインフラを末端まで構築し下記を行う必要があります。

. 製品の中で、サービスが開示している、あるいは内部で利用されている全てのオープンソースを識別アーキテクチャを評価し、オープンソースのライセンス上の義務がプロプラ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まで拡大していないか、拡大しているならばどのように、を検証適用可能なオープンソースライセンスを収集し、法務部門が評価

. オープンソースの利用および配布のポリシーと手続きを定めますアーキテクチャ設計と製造の実務においてリスクを低減

コンプライアンス違反は高くつく

コンプライアンス違反が公となった事件の多くはGPLのソースコードが関わっています。これらの紛争解決の合意では下記の一つないし一つ以上 の条項が含まれています。

. コンプライアンスを満たすよう必要なアクションを取る

. コンプライアンスオフィサーを置きコンプライアンスをモニタし確認させます

. 製品を受け取った過去の顧客に、製品はオープンソースソフトウェアを含んでいること、そのソフトウェアについての権利、を通知

. ライセンス告知を企業のウェブサイトに掲載

. 製品説明に告知を追加

. ソースコードをすべての改変と共に利用可能 に（GPL/LGPLファミリのライセンスに限る）

. 問題となっているオープンソースソフトウェアのバイナリの配布を、関連のソースコードが開示されるまで、あるいはコンプライアンス違反で影響を受けた特定顧客が利用可能となるまで差し止め. いくつかの事件では、原告に対し非開示の額の金銭的対価

更に、コンプライアンス異議申し立てを受け、それが成功すると下記のコストを負うことになりました。

. コンプライアンスの照会への対応として申し立てに応じた調査、問題のソースコードのデューデリジェンス、のためのディスカバリとデューデリジェンスのコスト

. 外部・内部のリーガルコストブランドや評判、信頼性へのダメージ

ほぼすべての事件において、オープンソースライセンス上の義務違反は面目の失墜、否定的な記事、オープンソースコミュニティとの関係悪化を招いています。

関係は大事

オープンソースソフトウェアを自社製品で利用する企業は、利用しているコードを開発し維持七得るオープンソースコミュニティと良い関係を持ち、維持することが望ましいです。オープンソースプロジェクトのコミュニティは企業が自社製品に含まれるオープンソースソフトウェアのライセンスを尊重すると期待しています。その方向に動き、オープンかつ正直な関係を気づくことは大いに価値があります。

訓練は重要

訓練はコンプライアンスプログラムにおいて必須の構成要素であり、オープンソースソフトウェアの利用を律するポリシーを従業員がよく理解する礎となります。ソフトウェアに関わる全職員が企業のポリシーとプロセスを理解する必要があります。企業はそうした教育を公式・非公式の教育で提供することが多いです。

第2章

オープンソース管理プログラムの確立

オープンソース管理プログラムはオープンソースソフトウェアの全ての側面、その選択、承認、利用、配布、監査、インベントリ、訓練、コミュニティとの関わり、広報等々の体系を定めます。本賞はオープンソース管理プログラムの様々な構成要素を概観し、新しいコンプライアンスプログラム策定における難しさを概説し、そうした難しさを克服する方法を述べます。

オープンソースコンプライアンスプログラム

最初に、成功するオープンソースコンプライアンスプログラムでコアとなる構成要素を概観します。本章と図4にこれら構成要素の概観を示すします。

図4オープンソース 管理プログラムの必須構成要素

コンプライアンス戦略

オープンソースコンプライアンス戦略は、ポリシーやプロセスの実装 の主たる側面について、ビジネスに立脚してコンセンサスを推し進めるものです。こうしたハイレベルなコンセンサスに基づかずにポリシーやプロセス の実装の細部について社内合意しようとすると、不可能とは言わないまでも非常な困難に直面します。コンプライアンス戦略はコンプライアンスを確保するために行うべきことを定め、職員のオープンソースソフトウェアの扱いを統べる原則を与えます。オープンソースの承認、取得 (acquisition) , 利用、オープンソースライセンスを含むかオープンソースラインセンスに基づいてライセンスされたソフトウェアをリリースする方法、の正式なプロセスも本戦略に含まれます。

照会応答戦略

照会応答戦略は、コンプライアンスが問われた時に行うべきことを定めます。企業は時として悪評（場合によっては正式な申し立て）を、コンプライアンスについての追加情報提供の要請を無視したり、コンプライアンスの照会を扱う方法を知らなかったり、オープンソースコンプライアンスプログラムが欠落していたり不十分だったり、単に照会者と協力しなかったために、受けてきました。こうしたアプローチは関係者のだれにとっても実りや利益を生みません。従って企業は照会を受けとり、受領したことを応答し、照会者に検討することを伝え、現実的なフォローアップの日程を通知する方法を定めるべきです。後ろの章で、オープンソースコンプライアンスに対する照会を扱うシンプルなプロセスについて述べます。

ポリシーとプロセス

オープンソースコンプライアンスポリシーとは、オープンソースソフトウェアの管理（利用と寄付の双方）を取り仕切るルール群です。プロセスとは、日々の業務にこれらルール群を実装するかを詳細に列挙したものです。コンプライアンスポリシーとプロセスがオープンソースソフトウェアの様々な側面、利用、寄付、監査、配布を取り仕切ります。図５（次ページ）はコンプライアンスプロセスの例を図示したもので、個々のソフトウェアコンポーネントがデューデリジェンスの一環として通るべき様々なステップを示しています。このプロセスの詳細は後ろの章で述べます。

図5コンプライアンスデューデリジェンスプロセスの例

コンプライアンスチーム

オープンソースコンプライアンスチームとは、オープンソースコンプライアンスを確実に行うため様々な分野の人々を集めたチームです。コアとなるのはオープンソース評価委員会 (Open Source Review Board, OSRB) と呼ばれることが多い委員会で、エンジニアリング、製品のチームの代表者たち、一人以上の法務顧問、そしてコンプライアンスオフィサーから構成されます。拡大チームは様々な部門からコンプライアンス活動のため随時加わる人々で、文書作成、サプライチェーン、全社開発、IT、ローカル化、オープンソース幹部会議 (Open Source Executive Committee, OSEC)らが含まれます。ただし拡大チームのメンバはコアチームと違い、OSRBから仕事を委任された時だけ活動します。コンプライアンスに常時携わるわけではないです。第３章ではオープンソースコンプライアンスを達成するための個々の人間の役割と責任について詳述します。

図６（次ページ）はコンプライアンス達成のためのこれら二つ、コアチームと拡大チーム、を図示しています。

図6オープンソースコンプライアンスを確かなものとする個人とチーム

ツール

オープンソースコンプライアンスチームはツールを使うことでソースコードの監査、オープンソースコードとそのライセンスの発見、が自動化され楽になります。こうしたツールには

. コンプライアンスプロジェクト管理ツール、コンプライアンスプロジェクトを管理し、タスクやリソースを追跡

. ソフトウェアインベントリツール、個々のソフトウェアコンポーネント、バージョン、それを使用している製品、関連情報を継続的に追跡

. ソースコードとライセンスの識別ツール、ビルドするシステムに含まれるソースコードの由来とライセンスを特定. リンク解析ツール、問題となるC/C++ソフトウェアコンポーネントと、製品に含まれる他のソフトウェアコンポーネントとの関係を特定。本ツールを使うことで、企業のポリシーを満たさないソースコードパッケージとのリンクを発見できます。この目標は、プロプラ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にオープンソース上の義務が何ら及んでいないことの確定です。もしリンクが発見されたら、製造部門に対しバグチケットを発行し、問題と解決方法を記述します。. ソースコードのピアレビュー（査読）ツール、ライセンス上の義務を満たすための開示に先立ちオリジナルソースコードに対する変更をレビュー。

. 部品表 (bill of material, BOM) 差分ツール、二つの異なるビルドでの部品表の違いを特定。本ツールはコンプライアンス準拠作業を積み上げで行う場合に非常に有用です。

ウェブ上のプレゼンス

企業はポータルを２方向で使います。：一つは内向きに、企業内へ。もう一つは外向きに、社会とオープンソースコミュニティへの窓として。内部向けのポータルはコンプライアンスポリシー、ガイドライン、各種文書、訓練、通知、メーリングリストへのアクセスを提供します。外部向けのポータルは社会とオープンソースコミュニティに向けて公開のプラットフォームとなり、またオープンソースのパッケージのソースコードや受領通知ほかの情報開示を投稿する場としてライセンス上の義務を履行します。

教育

教育はコンプライアンスプログラムにおいて必須の構成要素で、オープンソースソフトウェアの利用を取り仕切るポリシーを従業員がよく理解する基礎となります。オープンソースとコンプライアンスの教育の目標は、公式非公式を問わず、オープンソースのポリシーや戦略、オープンソースのライセンスや、製品やソフトウェアポートフォリオにオープンソースソフトウェアに組み入れることのビジネス的、法的リスクについて共通理解を作り上げ、注意喚起することです。またトレーニング は、企業内でコンプライアンスポリシーを広め推進し実施し、コンプライアンスの文化を育てる場となります。

公式トレーニング

企業の規模やオープンソースの営利活動への浸透度合いに応じて、企業はオープンソースに携わる従業員に公式の講師によるトレーニングコースを命じることができます。実例でのトレーニングがその頂点となりえます。

非公式トレーニング

非公式のトレーニングは下記のいずれか、あるいは全部を含む。

. ブラウンバッグセミナー（茶色鞄のセミナー）：ブラウンバッグセミナーとは一般に、昼食時に従業員や招待者が行うプレゼンテーションです。こうしたセミナーの目標は、商用の製品や企業のソフトウェアポートフォリオの中にオープンソースを組み込むことの様々な側面について講演し、議論を起こすことです。これらのセッションは、企業のコンプライアンス プログラム、ポリシー、そしてプロセスに関する議論も含みます。. 新人研修：時にはコンプライアンスオフィサーが企業のコンプライアンスの努力、規則、ポリシー、プロセスを新人に対して研修の一部として講演し、必要となるオープンソースの管理上の情報（聞くべき人、訪れるべき内部のウェブサイト、オープンソースとコンプライアンスのトレーニングへの参加方法等々）を提供します。

自動化

オープンソースソフトウェアを使いたい、寄付したい開発者はオンラインで申請し、適切な承認を得る必要です。これは自動化されたオンラインシステム、通常はオープンソースコンプライアンスの管理を特に組み込んだワークフローに従うバグ追跡システムで行うのがベストです。

メッセージの発信

メッセージの発信は内部向け、外部向けともコンプライアンスプログラムの必須の構成要素です。ここで最も重要なのは明確で首尾一貫していることで、内部的に従業員に対してオープンソース関連の会社の目標や懸念事項を伝える場合も、外部に向け自社製品やソフトウェアスタックが利用しているオープンソースプロジェクトの開発者コミュニティに伝える場合も同様です。

コンプライアンスの難しさと解決策

企業でのコンプライアンスプログラムの確立では、ほぼ確実に困難に直面します。以下の説では最もありふれた困難を取り上げ、克服する方法を示唆します。

コンプライアンスプログラムの作成

最初の難しさは、コンプライアンスプログラムやそれを支える（既存の）内部手続きのためのインフラと、製品出荷やサービス開始の〆切とのバランスを取ることです。こうした難しさを和らげ解決し、開発活動にとって重荷とは見做されない能率的なプログラム確立を助ける様々な手段があります。

解決策

役員のサポート

役員レベルでのオープンソース管理プログラムへのコミットは、その成功と継続のために重要です。

ポリシーとプロセスの負荷の軽さ

プロセスとポリシー は重要である。だが開発プロセスにとって重荷に過ぎると開発チームが見做さないよう軽く効果的でなければなりません。

能率的なオープンソース管理は二つの基盤の上に成り立つ。：簡単で明確なコンプライアンスポリシーと、軽いコンプライアンスプロセスです。

基本ルールを強制

コンプライアンスプログラムを実施する一環として、誰でも従わねばならない幾つかのシンプルな規則を定める必要があります。

. 開発者がオープンソースソフトウェアを製品やソフトウェアスタックに組み入れを計画するときは申請します。

. サードパーティのソフトウェアサプライヤに、提供物に含まれるオープンソースソフトウェアの情報を開示させます。あなたのサプライヤがオープンソースコンプライアンスを見事に実践しているとは限りません。オープンソースの開示に関わる文言を入れるよう、契約を見直すべきです。. アーキテクチャのレビューとコードの検査を指示し、オープンソース評価委員会 (OSRB) がソフトウェアコンポーネント間の関係を理解し、オープンソースからプロプラエタリなソフトウェアへとライセンス上の義務が派生していることを見つけられるようにします。大規模に行うには適切なツールが必要となります。

. サードパーティのソフトウェアプロバイダから受領するすべてのソフトウェアをスキャンし、オープンソースに関する開示が正しく、完全であることを確認します。

コンプライアンスを開発プロセスに統合

コンプライアンス確立の最善の方法は、コンプライアンスプロセスやポリシー、チェックポイント、活動を既存のソフトウェア開発プロセスに組み込むことです。

長期的な目標と短期的な実行

図4はコンプライアンスプログラムの成功に必須の構成要素を示しています。プログラムのすべてを実装するのに必要な作業の多さに圧倒される関係者もいるかもしれません。実際にはそこまで難しいものではありません。すべての要素を同時に実装しなければならない訳ではないからです。すべての組織において優先されるのは、製品やサービスを期限通りに出荷し、と同時に内部的なオープンソースコンプライアンスのインフラストラクチャー を構築し拡大することです。従って、企業なりのコンプライアンスのインフラストラクチャーを状況の進展に合わせて構築すべきと考えればよく、その際には将来の活動や製品をふまえ拡張性を考えるべきです。カギとなるのは思慮深く現実的な計画です。

解決策

. 長期的な目標に合致する、十全なコンプライアンスのインフラストラクチャーを計画し、短期的な実行の必要性に合わせ、要素を一つずつ実装します。たとえば、もしオープンソースを含む製品開発やサービス提供を始めたばかりであり、すでに動いているコンプライアンスのインフラストラクチャーが何もないならば、最も差し迫った懸念はコンプライアンスチームを作ることであり、プロセスとポリシー、ツールと自動化を確立することであり、従業員を訓練することです。これらの活動を（この順番で）開始し、システム構築を（コンプライアンスの観点から）適切に制御しつつ開始したならば、プログラムの他の要素に進むことができます。

. ポリシーとプロセスを確立

. 開発プロセスの一部としてコンプライアンスを組み込み

コンプライアンスについての対話

コンプライアンス活動の成功を確かなものとするには、対話は必須です。2種類の対話、あなたの組織内での内部的なもの、あなたの製品で使われているオープンソースのプロジェクトの開発者コミュニティとの外部に向けたもの、を考えることが重要です。

内部的な対話

企業はコンプライアンスについての対話が内部的に必要となります。オープンソースを商業ソフトウェアのポートフォリオへの組み入れが何をもたらすのか従業員が理解していることを確実にするためであり、企業のコンプライアンスポリシー、プロセス、ガイドラインについて教育を受けていることを確かなものとするためです。内部的な対話は下記のいずれでも可能です。

. オープンソースコンプライアンス活動を幹部がサポート する電子メールでの対話オープンソースソフトウェア関連業務に携わる全従業員に対する正式な訓練命令オープンソースとコンプライアンスについてのブラウンバッグセミナーによりコンプライアンスについて更に注意喚起し、活発な議論を奨励内部的なポータルを作り、企業のコンプライアンスポリシーやプロセス、オープンソースに関係した出版物やプレゼンテーション、メーリングリスト、オープンソースとコンプライアンスに関係する討論フォーラムをホスト企業全体に向けたオープンソースのニュースレター。一般に隔月か四半期ごとに、オープンソースのコンプライアンスについて注意喚起

外部との対話

企業は外部とのコンプライアンスについての対話が必要となります。自社が製品で使うオープンソースソフトウェアについてライセンス上の義務を果たす努力をしていることを、オープンソースのコミュニティに確かに認識させるためです。

外部との対話は下記のいずれでも可能です。

. コンプライアンス遵守のためにオープンソースを配布するためのウェブサイト. オープンソースの組織への参加 やサポート。こうした活動は企業がオープンソースの組織との関係を確立し、そうした組織の役割を理解し、有意義な貢献をするのを助けます。オープンソースのイベントや会議への参加。参加には様々なレベルがある。イベントのスポンサーから講演や出版物への寄与、あるいは単に開発者を参加させオープンソースの開発者たちと知り合いオープンソースコミュニティのメンバと新たな関係を育成します。

クリーンなソフトウェア起点 の確立

コンプライアンスプログラムの開始当初の困難の一つは、使われているオープンソースソフトウェアとそのライセンスを正確に把握することです。この初期の監査プロセスは、製品やソフトウェアポートフォリオのクリーンなソフトウェア起点の確立、と呼ばれることが多いです。これは数か月かかることもある重い活動で、開発と並行してどの程度早期に作業を開始するかに掛かっています。

解決策

組織は初期のコンプライアンスを以下の活動を通じて達成します。

. オープンソースの利用申請の早めの提出と評価

. 自動化されたソースコードのスキャン を継続的に、事前設定した時間間隔で全ソースコードに対して 実行

. ソースコードのベースを継続的にスキャン。これにはサードパーティのソフトウェアプロバイダから受領したものを含めます。該当するコンプライアンスチケットなしにコードベースにチェックインしたソースコードを捕まえるためです。こうしたソースコードのスキャンはたとえば毎月行います。. 設計とアーキテクチャの評価をソースコードの検査に加えて強制します。これはオープンソース、プロプラエタリ、そしてサードパーティのソフトウェアコンポーネントのコードの関係を解析するためです。これを強制するのは、そうした関係がライセンス上のコンプライアンスの義務に関わるときのみでよいです。

もし企業がコンプライアンスの起点構築に失敗すると、その製品の将来の改訂版（またはおなじ起点を使った異なる製品）がコンプライアンス問題で苦しむことはほぼ確定となります。

そうしたシナリオを防ぐため、企業は下記を考慮すべきです。

. シンプルだが確実に行われるポリシーと軽量なプロセスを提供

. コンプライアンス上のチェックポイントをソフトウェアの開発プロセスに含め、コンセプトが出荷される製品やソフトウェアスタックとなる時に行います。理想的にはすべての開発上のマイルストーンにおいて対応するコンプライアンス上のマイルストーンを組み込み、ビルドに使われる全ソフトウェアコンポーネントが対応する、承認されたコンプライアンスチケットを確実に持つようにします。

. 専任のコンプライアンスチームを確保します。この点は後ろの章で文章を割きます。

. コンプライアンスチケットを効率的に処理するためツールや自動化を利用します。この点は後ろの章で論じます。

コンプライアンスの維持

オープンソースのコンプライアンスを維持するには、コンプライアンスの起点確立と同様、いくつかの困難があります。実際には踏むべきステップの多くは同じで、ただし規模は小さく、積み増しとなります。コンプライアンスの維持は継続的な努力であり、規律、そして既存の製造およびビジネスのプロセスへのコンプライアンス活動組み込みのコミットメントによります。

図7に積み上げのコンプライアンスの概念を示します。ここでは初期のコンプライアンスの起点と現在のバージョンとの間で起きたソースコードの変更が何であれ、コンプライアンスを確実に満たすことが必要となります。

図7積み上げのコンプライアンスの例

解決策

企業は以下の活動を通じてコンプライアンスを維持することができます。

. 企業のコンプライアンスポリシーとプロセス、加えてあらゆるガイドラインの厳守コードベースに統合されたすべてのソースコードについて、出所を問わず継続的に監査コンプライアンスや自動化に使われるツールを継続的に改善し、コンプライアンスプログラムにおいて可能な限り多くのプロセスを高い効率で実行

内面化と末永い実行

オープンソースのコンプライアンス活動を維持するのは組織 が成長し、オープンソースを使った更なる製品やサービス出荷に伴う進行中の挑戦です。企業は開発のカルチャーの中へとコンプライアンスを内面化し、末永く実行するためにいくつかの段階を踏むとよいです。

解決策

後援者

役員レベルのコミットメントがコンプライアンス活動を持続させる上で必須です。進行中のコンプライアンスのリーダーとなり、オープンソースの管理機能を企業としてサポートする役員がいなければなりません。

一貫性

企業全体で一貫性を保つことは複数のビジネスユニットや子会社を持つ大企業では重要です。部門間での一貫したアプローチは、記録の保持、グループ間でのコードの共有促進と並び有用です。

計測と分析

コンプライアンス活動やプロセス、手続きのインパクトや効率性を計測し分析すべきです。パフォーマンスを調べ、コンプライアンスプログラムを改善するためです。計測の尺度は、コンプライアンスプログラムを推進する場合にプログラムの個々の構成要素から得られる生産性向上について対話をする助けとなります。

コンプライアンスプロセスの改善

組織がオープンソースを利用する範囲や目的 は変化します。製品や技術、企業の吸収や合併、海外への委託、その他多くの要因によって動きます。従って、今ぷらインすポリシーとプロセスを絶えず評価し、改善する必要があります。

更に、オープンソースラインセンスの解釈や法的リスクも進化します。こうしたダイナミックな環境の中で、コンプライアンスプログラムも進化する必要があります。

守らせること

コンプライアンスプログラムは、守られなければ無意味です。効果を持たせるため、コンプライアンスプログラムにはプログラム厳守を監視し、ポリシーやプロセスやガイドラインを全社的に守らせる メカニズムを含めるべきです。コンプライアンスプログラムを守らせる方法の一つは、ソフトウェア開発プロセスと統合し、従業員の業績査定の幾分かをコンプライアンスプログラム活動へのコミットメントと実行とすることです。

スタッフ割り当て

スタッフがコンプライアンスの職務のために割り当てられ、十分なコンプライアンスの訓練が組織の全従業員に確実に施されていなければなりません。大きな組織ではコンプライアンスオフィサー、および関連する職務はフルタイムの仕事となり得ます。小さい組織では分担したり、時間の一部を割くべき活動となる可能性が高いです。

第3章

コンプライアンス達成に向けて：役割と責任

一人の個人では、どれほどの達人であろうとも、オープンソースコンプライアンスを組織全体に実装することはできません。図8はオープンソースコンプライアンスの達成に責任がある様々な部門を書き下したものです。コンプライアンス達成には二つのチームが必要となる。コアチームと拡大チームです。後者は通常、前者を包括するものとなります。

図8オープンソースコンプライアンスを確かなものとする個人とチーム

コアチームはオープンソース評価委員会 (Open Source Review Board, OSRB) と呼ばれることも多いです。エンジニアリングと製品のチームの代表者たち、一人以上の法務顧問、そしてコンプライアンスオフィサーから構成されます。表４に個々の参加者のコアチームにおける役割と責任を示します。

拡大チームは表5 (49ページ) に示す通り、様々な部門からコンプライアンス活動のため随時加わる人々で、文書作成、サプライチェーン、全社開発 、IT、ローカル化、オープンソース幹部会議 (Open Source Executive Committee, OSEC)らが含まれます。ただし拡大チームのメンバは（実体をもつ組織である）コアチームと違い、OSRBから仕事を委任された時だけ活動します。

表4コンプライアンスコアチーム (OSRB) の主な役割と責任

参加者

主な役割と責任

法務の代表者

代表者はその時の作業に応じ、法律顧問から弁護士補助職員まで変化します

OSRBとOSECへ参加

オープンソースソフトウェアの利用、改変、配布をレビューし承認

ライセンスについてのガイドラインの提供

トレーニングの提供と承認

オープンソースコンプライアンスプログラム改善への貢献

オープンソースのポータルの内容をレビューし承認

ライセンス上満たすべき義務一覧のレビューと承認

オープンソースに関する告知の承認

参加者

主な役割と責任

エンジニアリングおよび製品チームの代表

企業によってはエンジニアリングと製品のチームは分かれていない

OSRBとOSECへ参加

コンプライアンスポリシーとプロセスの遵守

コンプライアンスの実践を開発プロセスの中に統合

コンプライアンスプログラムの改善に貢献

技術的なコンプライアンスプログラムの遵守

あらゆる質問への迅速な回答

設計、アーキテクチャ、コードのレビューの実施

配布のためのソフトウェアパッケージ準備

コンプライアンスオフィサー

オープンソースコンプライアンスオフィサーは必ずしも専任である必要はないです。大抵の場合、オープンソース部門の部長や所長が役割を果たします

全てのコンプライアンス活動を推進

ソースコードのスキャンと監査を調整

ソースコードパッケージの配布を調整

OSRBとOSECへ参加

コンプライアンスとオープンソースのトレーニングに寄与

コンプライアンスプログラムの改善に寄与

OSECにコンプライアンス活動について報告

自動化や、開発環境の中にオープンソースのコードを見つける新たなツール作成に寄与

表5コンプライアンス拡大チームの役割と責任

参加者

主な役割と責任

オープンソースの戦略を決定するオープンソース幹部会議 (Open Source Executive Committee, OSEC)

知財のリリース提案 をレビューし承認

プロプラエタリなコードをオープンソースライセンス下でリリースする提案をレビューし承認これはそのソースコードはオープンソースにする前提で開発されたならば不要です。

文書作成

オープンソースライセンスの情報と告知を製品の文書の中に含めます

ローカル化

製品やソフトウェアスタックに関わるオープンソースについて、基本的情報をターゲットとなる言語に翻訳

サプライチェーン

サードパーティプロバイダからライセンスされた、または購入したソフトウェアコンポーネントに含まれるオープンソースの情報の開示をサードパーティプロバイダに指示

オープンソースソフトウェアが含まれている、またはバンドルされているサードパーティのソフトウェアの納入を手助け

IT (情報技術)

コンプライアンスプログラムで利用されるツールと自動化のインフラをサポートし整備

OSRBの要請に応じ、新しいツールを作成、入手

参加者

主な役割と責任

Corporate Development

Request open source compliance be completed before a merger or acquisition

Request open source compliance be completed when receiving source code from outsourced development centers or third-party software vendors

オープンソース評価委員会 (Open Source Review Board, OSRB)

OSRBは下記に責任を持ちます。

. サードパーティのソフトウェアとオープンソースのソフトウェアライセンスとが相互にコンプライアンスを確かに満たすようにします. オープンソースソフトウェアの効果的な利用、およびオープンソースソフトウェアへの寄与を促進

. プロプラエタリな知財（引いては製品の差異化）を、オープンソースのライセンスがプロプラエタリな、またはサードパーティのソフトウェアに確かに及ばないようにすることで防御

日々の活動としては、OSDBのメンバーは下記に従事します。

. エンドツーエンド（端から端まで）のコンプライアンスプロセスの確立します。OSRBはエンドツーエンドのコンプライアンスプロセス、すなわち利用、監査、開発、関与、保障、コンプライアンス管理に責任を持ちます。エンドツーエンドのコンプライアンスプログラムについては4章で概観します。

. コンプライアンスプログラムで使われるコンプライアンスポリシー、プロセス、ガイドライン、テンプレート、フォームを作成し保守

. オープンソースの利用、改変、配布の申請をレビューする。OSRBはエンジニアリングや製品部門からのオープンソース利用申請 をレビューし承認します。利用のプロセスは6章で論じます。. Perform software audits: The OSRB performs audits on all software included in a product, which involves the following tasks:

. ソフトウェアベースに対しソースコードをスキャンするツールを適用Analyze the results provided by the scanning tool

. スキャンのツールで発見されたコード合致 、潜在的な合致、ライセンスの衝突を識別 . スキャンのツールで特定されたすべての問題が解決することを監督

. Create a final audit report and ensure that all identified issues have been closed

監査はOSRBか独立した監査チームかが組織の規模に応じて責任を持ち、コンプライアンスオフィサーに報告します。Chapter 6 provides a discussion of the auditing process.

. アーキテクチャのレビュー実行。承認過程の一つとして、OSRBはエンジニアリング部門の代表と共にアーキテクチャをレビューし、オープンソースのソースコード、プロプラエタリのコード 、サードパーティのソースコードの関係を解析します。本レビューの目的は、アーキテクチャのガイドラインが尊重され、オープンソース、プロプラエタリ、サードパーティのソフトウェアの関係が、現場が受け入れ可能な法的ガイドラインの範囲内に収まっていることを確認することです。. リンク解析をレビュー。OSRBはAPI呼び出し等によるリンク関係により、何らかのオープンソースのライセンス上の義務がプロプラエタリやサードパーティのソフトウェアに広がっていないかの確認のためリンク解析を行います。

. オープンソースを含む製品のリリースやサービスの開始を取りやめる決定を検証. 社内のスタッフやエンジニアから寄せられるオープンソースに関する質問に対しガイダンスを提供

. 配布前の検証作業の一環としてコードの検査を実施。オープンソースライセンスのテキストや著作権表示が完全な形となっており、ソースコードに対して施された変更を反映するようエンジニアたちが変更ログ をアップデートしていることを確認

. 問題となっているオープンソースソフトウェアで満たすべきライセンス上の義務の一覧を作り、満たすよう関係部門に展開：OSRBがオープンソースを製品に利用することを承認したら、承認プロセスの一部としてOSDBは義務一覧を作り、関係する様々な個人やチームに展開して確実に満たすようにします。配布前のプロセスの一部としてOSDBは製品やサービスのリリース前に最終チェックを行いますが、義務を満たしていることの検証もここに含みます。

. オープンソースとコンプライアンスの訓練を開発し提供。OSRBはオープンソースとコンプライアンスの訓練の開発を主導し、従業員が企業のオープンソースのポリシーやコンプライアンスのプロセスについて良く理解するようにします。更に、OSRBは最も広く利用されるいくつかのオープンソースのライセンス、商用でのオープンソース利用に関わる話題についても教育すべきです。この訓練はオープンソースを使ったソフトウェアの開発や管理に関わる従業員全員が受けなければなりません。. 企業のオープンソースのウェブサイトをホストし維持。：従業員向けの内部のウェブサイトはオープンソースのプロセスやポリシー 、ガイドライン、訓練、告知が主となります。外部向けのサイトは通常、ソースコードのパッケージを利用可能とし、特定のコンプライアンス上の義務を満たすことが第一の目的となります。

. コンプライアンスの質問を取扱う。OSRBは企業に送付されたオープンソースのコンプライアンスに関わるあらゆる質問に答える責任があります。第9章でコンプライアンスの質問を扱うプロセスを述べます。. Maintain records of compliance: OSRB is responsible for ensuring that all compliance records for any given open source software component are up to date.

. Review end-user documentation to ensure that appropriate copyright, attribution, and license notices are given to consumers regarding open source included in the product or the software stack. In addition, specific to the GPL/LGPL family of licenses, provide a written offer on how to obtain the source code, when applicable.

. Recommend new tools to be used as part of the compliance infrastructure that will contribute to making the compliance work more efficient through automation.

. Sign off on product distribution from an open source compliance perspective. . Develop community involvement policy, process, procedures, and guidelines. This responsibility is not compliance-related; however, it is listed here for completion of the list of responsibilities.

LEGAL

The Legal Counsel is a core member of the OSRB, the committee that ensures compliance with open source licenses. The Legal Counsel focuses on four essential duties:

1. Provide approval regarding the use of open source in products or services

The approval of the Legal Counsel is required when using open source in a commercial product. Typically, the Legal Counsel reviews the compliance ticket in the online tracking system (for instance, JIRA or Bugzilla), the resulting report from the source code scanning tool, and the license

information provided with the source code package. They then evaluate risk factors based on feedback provided by both engineering and the open source compliance officer. As part of this exercise, the Legal Counsel also decides on incoming and outgoing licenses of the software component in question. The incoming licenses are the licenses of all source code included in a given body of code; the outgoing licenses are the licenses under which the source code and/or object files are being made available to its recipients.

2. Advise on open source licensing

. Offer guidance about open source license obligations. . Advise on licensing conflicts arising from incompatible or conflicting licenses primarily based on company policy, which is some cases rely on external factors such as legal opinions of relevant open source organizations.

. Advise on IP issues associated with the use of open source. This is especially the case when the company is about to release previously proprietary source code under open source license(s).

. Provide recommendations and guidance to engineering teams on open source questions and concerns.

3. Review and approve updates to end-user documentation

This form of legal support is related to ensuring that appropriate open source notices (copyright, attributions, and license notices) are provided to consumers in relation to any open source included in the product. In addition, if there is source code licensed under one of the GPL/LGPL family of licenses, a written offer needs to be provided along with information on how to obtain the source code.

4. Contribute to the startup and ongoing management of the open source compliance program

. Establish and maintain the open source policy and process. . Handle inquiries sent to the company in relation to open source compliance.

. Provide training around open source licenses, company policies, and guidelines.

ENGINEERING AND PRODUCT TEAMS

Engineering and product teams may have one or more representatives who participates in the OSRB, tracks down all compliance-related tasks assigned to engineering, and ensures proper resolution. In parallel, engineering and product teams have several responsibilities with respect to open source compliance:

. Submit requests to use open source software: Engineering and product teams decide what external software to bring into the product baseline, including third-party and open source. Their primary responsibility from a compliance perspective is to submit a usage form for any open source that is planned for inclusion in a product or service. The form describes the intended use of the open source in question and helps construct and maintain a good record of software origin and provenance. . Follow technical compliance guidelines: Engineering and product teams should follow OSRB technical guidelines to architect, design, integrate, and implement source code. The OSRB guidelines typically cover:

. Common mistakes and how to avoid them

. Rules to follow when integrating libraries and other middleware to avoid linkage issues that might arise

. Development in kernel space versus user space (on Linux), especially with whole-platform development in embedded environments

. Specific engineering situations that are applicable to open source compliance

. Conduct design reviews: Engineering teams should continuously conduct design reviews to discover and remedy any compliance issues in a timely manner. The Compliance Officer drives the design reviews and invites different engineering participants depending on the software component in question.

. Cooperate with OSRB: Engineering teams must respond promptly to questions asked by the OSRB and cooperate in resolving compliance tickets.

. Track changes: Maintain a change log for each modified open source component: As part of meeting the open source license obligations and depending on the open source license in questions, some licenses (such as the GPL/LGPL family of licenses) mandate that modified files carry prominent notices stating that you changed the files and the date of the change(s).

. Prepare source code packages for distribution: Engineering teams prepare the source code packages that will be made available on a public website as part of meeting open source license obligations (other source code distribution methods are discussed in a later chapter). . Integrate compliance milestones as part of the development process: This exercise takes place in collaboration with the OSRB and the Compliance Officer. . Undergo open source training: All engineers must take the available open source training. . Monitor the open source projects to determine whether any bug fixes or security patches have become available, and take responsibility for updating the open source component used in the product. The individual package owner within the organization usually performs this specific task.

COMPLIANCE OFFICER

The Compliance Officer, also called OSRB Chair or Manager/Director of Open Source, chairs the OSRB and manages the compliance program.

Ideally, the compliance officer must possess as many as possible of the following:

. Solid understanding of common open source licenses and obligations to discuss with legal counsel Knowledge of industry practices

. Knowledge and experience in establishing corporate-wide policies and processes . Technical knowledge related to the company’s products . Historical perspective on open source . Knowledge of community consensus and practices

. Contacts in the key open source project communities . Contacts in the open source organizations such as the Linux Foundation, Apache Foundation, Mozilla Foundation, Software Freedom Law Center, etc.

In addition to the responsibilities pertaining to the OSRB, the Compliance Officer carries the following duties:

. Drive the compliance due diligence end-to-end process and act as the compliance program manager, ensuring all compliance-related tasks are addressed and there are no compliance issues blocking products from shipping

. Coordinate source code scans and drive all auditing issues to closure

. Participate in engineering design reviews, code inspections, and distribution readiness assessments to assure that the engineering and product teams follow all compliance processes and policies and conform to the approved OSRB usage form

. Coordinate source code distribution of open source packages (when stipulated by licenses) with engineering and product teams, including preparing and verifying a distribution checklist for each open source package

. Act as liaison between OSEC and OSRB

. Escalate compliance issues to OSEC . Act as liaison between the engineering and product team and the OSRB and OSEC in regard to usage plan approval processes

. Report on compliance activities to the OSEC, including flagging issues that prevent shipping a product or service

OPEN SOURCE EXECUTIVE COMMITTEE

The Open Source Executive Committee (OSEC) consists of engineering, legal, and product marketing executives in addition to the Compliance Officer. The OSEC is responsible for setting open source strategy, reviewing and approving release of IP, and providing approvals to release previously proprietary source code under a specific open source license.

DOCUMENTATION

The documentation team is responsible for including written offers and any appropriate open source notices in the product documentation. Figure 9, on the next page, provides an illustration of how such notices are prepared and approved. The process starts with the compliance officer, who prepares the draft of the written offer and the notices that are to be made available once the product ships. Next, the legal counsel reviews the draft proposed by the compliance officer, edits it, and pushes a final version to the documentation team. The last step of the process is including the final text in the product documentation.

Figure 9. The role of the documentation team in updating the product documentation, reflecting the presence of open source in the product

LOCALIZATION

The localization team is responsible for translating basic language that informs users of the availability of open source software in the product and directs them to the proper notices made available in English.

SUPPLY CHAIN

Supply chain (software procurement) procedures must be updated to address the acquisition and use of open source. It is highly recommended that you examine software supplied to you by third-party software providers. Supply Chain personnel are usually involved in moving software from the suppliers to your company. Supply Chain can support open source compliance activities by mandating that third-party software (and hardware) providers disclose any open source that is being delivered with their wares, and by assisting with licensing-in third-party software that is bundled with and/or integrates open source packages.

A best practice in this area is to mandate that third-party software providers disclose any open source used in their offering, along with a statement on how they plan to meet the applicable open source license obligations. If third-party software includes open source, Supply Chain must ensure that open source license obligations are satisfied, since, after initial ingress, those obligations become your responsibility as distributor of a product or service that includes open source. It is not acceptable to point “upstream” to a supplier and to inform recipients of your code that meeting license obligations was the responsibility of the supplier instead of your own.

IT

IT provides support and maintenance for the tools and automation infrastructure employed by a compliance program. This responsibility spans the servers hosting the various tools, the tools, mailing lists, and web portals. In addition, IT may receive requests from the OSRB to develop and/

or acquire tools that will be used to improve effectiveness the compliance activities.

CORPORATE DEVELOPMENT

Corporate Development is involved with open source compliance in two major scenarios: mergers and acquisitions transactions, and outsourced development.

Mergers and Acquisitions

If a company is considering a merger or is the target of an acquisition, it should structure its compliance program to offer a level of disclosure and provide representations. Company policies regarding merger and acquisition transactions need to be updated to account for open source. Corporate Development must mandate that source code be evaluated from a compliance perspective prior to any merger or acquisition to avoid surprises that might derail discussions or affect the company’s valuation. For the acquiring company, comprehensive code evaluation assures accurate valuation of software assets and mitigates the risk of unanticipated licensing issues undermining future value. In addition, the acquiring company may include provisions in the purchase agreement requiring the disclosure of open source that is subject to the transaction. Diligence practices should be updated to require open source disclosure and include guidance regarding the review of any disclosed open source and licenses.

Outsourced Development

Agreements relating to outsourced development of software should also be updated to reflect compliance procedures and to ensure that other provisions of these agreements (such as representations and warranties) are broad enough to cover the risks posed by open source. Corporate Development must mandate that all source code received from outsourced development centers must go through the compliance process to discover all open source being used and to ensure proper actions to fulfill license obligations.

Other Corporate Transactions

Corporate Development is also involved with compliance in transactions such as spin-offs and joint ventures. In some cases, the compliance due diligence may result in a decision not to proceed with the transaction, if that the compliance situation proves far from ideal.

第4章

オープン ソース コンプライアンス プロセス

オープン ソース コンプライアンス プロセスの実現は、コンプライアンスを組み込む必要がある開発プロセス、コードのサイズと数、関連する製品とサービスの数、外部から導入されたコード量、組織のサイズや体制など、多くの要因に基づいて、組織ごとに変化します。しかし、コンプライアンスの中心的要素は、通常同じです：コード中のオープン ソースを特定し、レビューし、利用を許可し、義務を順守することです。この章では、コンプライアンス プロセスの中心的要素に焦点を当てます。コンプライアンス精査の結果は、外部出荷を意図した製品において使われる全てのフリー オープン ソース ソフトウェアの特定と、それに付随するライセンス義務を遵守するための計画です。図10は、一貫したコンプライアンス プロセスの高水準の概要図の一例を提示しており、外部出荷される製品やサービスへの統合許可を受ける前にフリー オープン ソース ソフトウェアを含むコンポーネントが通過する様々なコンプライアンス ステップやフェーズを図示しています。

図10一貫したコンプライアンス プロセスの簡略図

図10に示されているのは一例であり、同じ目的を達成するためにコンプライアンス プロセスを作る方法は多くあります。この章を通じて、これらの様々なフェーズ、各フェーズのインプットとアウトプット、そしてコンプライアンス プロセスによってソフトウエア利用をどのように管理するかを確認していきます。

効果的なコンプライアンス

精査（due diligence）という用語は、ソース コード検査、ソース コード監視、品質義務やシステム監査の実行などを含む多くの概念を指しています。オープン ソース コンプライアンスのこのケースでは、精査は、以下の項目の確認を要求されるものとします；

. 製品で利用されるオープン ソース ソフトウェアは、特定され、レビューされ、承認されている。製品実装は、承認されたオープン ソース コンポーネントとライセンスのみを含む。

. ライセンスされたものの利用に関する全ての義務は、特定されている。適切な通知は、帰属表記や著作権表記を含む文書で提示されている。変更（適用可能な場合）を含むソース コードは準備されて、製品出荷の時点で入手可能になっている。プロセス中の全段階の検証

簡潔で、組織内で十分に理解されている一貫したコンプライアンス プロセスを持つことには大きな利点があります。そのようなプロセスは：

. 組織に義務を履行させつつ、一方で組織がオープン ソースから恩恵を得られるようにします。オープン ソース利用を一時的なものから標準プロセスへと移行させます。オープン ソース コンポーネント入手の管理を助けます。従業員が、責任ある方法でオープン ソースとどのように取り組めばよいか理解するのを助けます。組織で利用している様々なオープン ソース プロジェクトの開発者との関係を改善します。

. ソース コード変更の共有を行うことで、統合コードのプロジェクト コミュニティとの間で、情報やアイディアの交換が加速されます。組織は安全にオープン ソース コンポーネントを採用して、新しいサービスや製品の立ち上げに必須のものとして利用できるので、イノベーションを加速できます。

一貫したコンプライアンス プロセスの要素

一貫したコンプライアンス プロセスの10ステップ

1. 入るソース コードの特定

2. ソース コードの監査

3. 監査で検出された課題の解決

4. 適切なレビューの完了

5. オープン ソース利用の承認受領

6. ソフトウェア リストへのオープン ソースの登録

7. オープン ソース利用を反映した製品文書の更新

8. 頒布前の上記全段階の検証

9. ソース コード パッケージの頒布

10. 頒布に関連した最終検証の実施

図11一貫したコンプライアンス プロセス

この章の残りの部分では、これらの10ステップについて詳しく説明します。

ステップ1オープン ソースの特定

この最初のステップの目的は、標準パッケージや、サード パーティか自社開発ソフトウェアに組み込まれた形で、オープン ソースがソフトウェア ポートフォリオに入り込んだり統合されたりすることを監視することです。製品に利用されるオープン ソースを特定するいくつかの方法があります。

. オープン ソース利用の要求：これは、製品中のオープン ソース利用を特定する最も普通の方法です。技術担当か製品マネージャは、OSRB（3章で説明）かコンプライアンス チームに特定製品やプラットフォーム リリースに特定のオープン ソースを利用したい旨を通知することが求められています。申請者は、レビューと承認の対象であるオープン ソース パッケージの計画した利用に関して情報を提供します。. コンプライアンス基盤として確立するために、全プラットフォームや製品コード ベースを監査し、その上で、後続のリリースで変更されたコード モジュールを監査する。

. サード パーティ ソフトウェア プロバイダー精査：これは、オープン ソース コンプライアンス チームによる開示内容のレビューを伴う、サード パーティ供給者によって提供された製品中にあるオープン ソース コンポーネントの全開示を要求します。あるケースでは、精査の追加として、供給コードの監査結果をサード パーティ ソフトウェア ベンダーに要求することも意味があります。これは、製品へ入るオープン ソースの管理を確実にします。. プロプライエタリ（自社開発の） ソフトウェア コンポーネントの監査：例として、技術者が、オープン ソース コンポーネントにあるソース コードをコピー／ペーストして、プロプライエタリ ソフトウェアに加えるかもしれません。それゆえに、製品出荷日前に発見されなければコンプライアンス違反に陥るようなオープン ソース コードを含んでいるかもしれませんので、自社開発ソフトウェア コンポーネントを監査することは重要です。

. 組織のソース コード リポジトリに入る、オープン ソースの利用要求に対応していない全オープン ソース コンポーネントの検査：オープン ソース利用の意図のフォームへの記載を技術者に頼るのは、全ての入るオープン ソース ソフトウェアを説明するには必ずしも確実な方法とはいえません。それゆえに、バックアップとして、オープン ソース用の分離したフォルダーを持つソース コード管理システムの準備と、このフォルダーにチェックインがされた時の警告を検討して下さい。オープン ソースと自社開発プロプライエタリ ソフトウェアとサード パーティ ソフトウェアをビルド システムで別のフォルダーに分離しておくのは常に奨励されるプラクティスですから、新しいコードが提出された時に警告が出るようにすることはできます。既存の利用（オープン ソース要求）フォームに対応しない新しいコンポーネントが提出されたら、それは新しいコンポーネントであり、新しいフォームに記入する必要があります。

特定フェーズの前提条件

以下条件の一つが満たされる：

. 特定のオープン ソース利用を要求する入るOSRBフォームプラットフォーム スキャンによって（適切な承認なしに）利用されているオープン ソースの発覚

. サード パーティ ソフトウェアの一部として利用されているオープン ソースの発覚

特定フェーズの結果

. コンプライアンス記録は、オープン ソースに対して生成（更新）されます。ソース コードをスキャンするように、監査が要求されます。

ステップ 2 . ソース コードの監査

コンプライアンス精査の2番目のステップは、既知のオープン ソース プロジェクトとの一致を検出する自動解析ツールを使ったスキャンで構成されます。

監査担当者は、リリースに含まれているものは様々な適用可能なオープン ソース ライセンスに適合している証拠を、リリースごとに反復して、ソースコードスキャンを実施します。

監査の目的は：

. 最後のスキャンからの間に、加えられた（削除された）オープン ソースを説明するリリースBOMを更新します。オープン ソースの由来も含めて、ソース コードの由来を確認します。全ての依存関係、コード一致、ライセンス矛盾にフラグを付けます。

監査フェーズの前提条件

適切なコンプライアンス記録（チケットとも呼ばれます）は、特定のオープン ソース利用に関する全ての必要な情報を補足し、内部ビルドシステム内のソース コードの場所を提供するように、作成されます。ある場合には、特にプラットフォームのフル スキャンが実施される時、適切なコンプライアンス報告が作成される前に、オープン ソース コンポーネントはスキャンされることもあります。この場合には、オープン ソース コンポーネントが発見された時に、記録が作成されます。

監査フェーズの結果

. ソース コードの出自とライセンスを特定する監査報告. 変更要求チケットは、適切な技術チームに対して、監査中に特定された解決すべき課題について記載されます。

いくつかの活動が、ソフトウェア コンポーネントの発見と監査の契機となります。（図12、次ページ）

. 開発者からのオープン ソース コンポーネント利用の要求. 全ソフトウェア スタックのソース コード スキャン以前に承認されたコンポーネントでのソース コード変更サード パーティ ベンダーから受け取ったオープン ソースウェブからダウンロードされたソース コード（著者やライセンスが不明）ソース コード リポジトリへ提出されるプロプライエタリ ソフトウェアコード リポジトリへ追加された、利用申請フォームに対応していないオープン ソース以前、異なる製品で承認を受けたオープン ソースの利用

図12入るオープン ソースの特定と監査の方法

ステップ3課題解決

コンプライアンス精査のこのステップでは、監査ステップで特定された全ての課題が解決されます。OSRBチェアは、監査ステップで技術者に割り当てられたチケットのクローズを監視します。技術者が特定された課題を解決した時には、OSRBチェアは、解決された課題がもはや存在しないことを確認するために監査を要求するべきです。

課題解決フェーズの前提条件

ソース コード スキャンが完了し、ソース コードの出自とライセンスを特定した監査報告が生成される。報告は、特定されていないソース コード ファイルや、異なるライセンスで結合されるソース コードによって生じるライセンス矛盾にフラグを付けます。コンプライアンス オフィサーは、これらの課題解決を推進します。

課題解決フェーズの結果

報告にあるフラグ付きのファイルの解決と、フラグ付きのライセンス矛盾の解決

ステップ4レビュー

監査が完了し、以前に特定された全ての課題が解決されたら、特定のソフトウェア コンポーネントに対するコンプライアンス チケットは、レビュー ステップへ移動します。図13（次ページ）に示すように、様々なレビューが実施され、特定された全ての課題は解決していなければなりません。レビュアーは、ソフトウェアの利用、変更、頒布を支配するライセンスを理解し、様々なライセンスの義務を特定する必要があります。与えられたソフトウェア コンポーネントに対する、コンプライアンス チケットのレビュアーは、

. 社内パッケージ所有者（特定のソース コード コンポーネントの開発者）ソース コード スキャンか監査の担当者

. OSRBチェア、法務担当、およびOSRB技術代表からなるOSRB (オープン ソース レビュー ボード)OSEC （オープン ソース エグゼクティブ ボード）

図13コンプライアンス チケットのレビュアーとその役割

コンプライアンス精査のこのステップの一部として、2つの重要なレビューがあります：アーキテクチャー レビュー、リンク解析レビュー

アーキテクチャー レビュー

アーキテクチャー レビューの目的は、オープン ソース、サード パーティ、プロプライエタリ コード間の相互作用を解析することです。アーキテクチャー レビューの結果は、オープン ソース コンポーネントからプロプライエタリ コンポーネントへ（その逆も）影響を与えるライセンス義務の解析です。社内パッケージ所有者、OSRB技術代表、そしてオープン ソース エキスパートが、アーキテクチャ レビューを行います。もしライセンスの矛盾になるような依存関係を発見した場合、コンプライアンス オフィサーは、ソース コードの再作業によって依存関係問を題解決するためにチケットを技術担当に発行する。

リンク解析レビュー

リンク解析の目的は、動的および静的リンク レベルで、GPL ライブラリをプロプライエタリ ソース コード コンポーネントにリンクしているなど、問題発生の可能性のあるコードの組み合わせ を検出することです。OSRB チェアは、自動ツールを使用してこの調査を行います。リンク問題は、解決するように技術担当に報告されます。

レビュー フェーズの前提条件

監査されたソース コード、解決されている全ての課題。

レビュー フェーズの結果

OSRBメンバーは、特定のコンポーネントに対してアーキテクチャ レビューとリンク解析を実施し、もし課題が発見されなければ、次のステップ（つまり承認）への準備が整っているという印をつけます。

ステップ5承認

全てのレビューが完了したら、ソフトウェア コンポーネントのコンプライアンス チケットは、製品に利用して良いかを決定する承認ステップへ移動します。承認はOSRBが行います。（前の章で説明したように、法務担当、技術代表、オープン ソース エキスパートが含まれます）

ほとんどのソフトウェア コンポーネントに対して、チケットがコンプライアンス プロセスのこの点まで進めば、承認が与えられます。OSRBがオープン ソース コンポーネントの利用を承認したら、OSRBは製品チームに承認を伝えますので、製品チームは責任を理解し、ライセンス義務履行の準備を始めます。OSRBがオープン ソース コンポーネントの利用を却下する場合、OSRBは却下の理由を要求者に伝え、この情報はコンプライアンス チケットの一部として記録されます。要求者はOSRBに再考を促すことは可能ですが、結果としては、オープン ソース コンポーネントは製品に使用できません。

承認フェーズの前提条件

全てのOSRBメンバーはコンプライアンス チケットをレビューし、OSRBはアーキテクチャー レビューとリンク解析を完了している。

承認フェーズの結果

特定コンポーネントの利用の承認または却下

ステップ6登録

ソフトウェア コンポーネントが製品やサービスへの利用を承認されたら、コンプライアンス チケットは、承認を反映するように更新されます。ソフトウェア コンポーネントは、オープン ソース利用とユースケースを記録したソフトウェア一覧表に加えられます。

保守的なアプローチの後にコンプライアンス プラクティスを進めるならば、特定のバージョンと、特定の製品やサービスバージョンでの利用に対して、オープン ソース ソフトウェアを承認します。このオープン ソース ソフトウェアの新しいバージョンが入手可能になったら、利用形態とライセンスが内部ポリシーと整合していることを確認するために新しい承認依頼を出します。

登録フェーズの前提条件

OSRBはコンポーネントの製品への利用を承認している。

登録フェーズの結果

コンポーネントは、コンポーネント名、バージョン、内部所有者、および製品名、バージョン、リリース番号等のコンポーネントが利用される場所の詳細などと共に、ソフトウェア一覧表に登録されます。

ステップ7通知

オープン ソースを利用する際の重要な責務の一つは、ドキュメント記載の義務、または通知義務ともいわれるものです。外部に提供する製品やサービスにオープン ソースを利用している企業は以下を行う必要があります：

. エンド ユーザーに、ライセンス義務を満たした結果として入手可能になっているソース コードのコピーをどのおうに入手できるかを通知します（必要に応じて）必要な著作権や帰属を通知することで、オープン ソースを利用していることを知らせます。. 製品に含まれているオープン ソース コードに対応するライセンスの全文を提示します。

オープン ソース ライセンス義務を順守しない企業は、ライセンスを取得できず、著作権を侵害したとして、著作権所有者に法的行動をさらされる可能性があります。また、対象となるソフトウェアを使用および配布する権利を失う可能性があります。ドキュメント記載義務を履行するには、製品に適切な通知を含める必要があります。コンプライアンス精査の中のこのステップでは、OSRB チェアが通知文を準備し、それを各担当部署に手渡します 。

通知フェーズの前提条件

ソフトウェア コンポーネントについて、使用が承認され、ソフトウェア一覧表への登録が完了している。

通知フェーズの結果

対象のコンポーネントのライセンス、著作権、および帰属通知が準備され、製品の資料に含めるべく担当部署に手渡される。

ステップ8. 頒布前検証

コンプライアンス精査の次のステップは、頒布の方法とモード、頒布するパッケージのタイプ、および頒布メカニズムを決定することです。

頒布前検証の目的は、以下を確実にすることです：

. 頒布されることになっているオープン ソース パッケージは、特定され、承認されている。. ソース コード パッケージ（変更を含む）は、製品として出荷されるバイナリと一致することが確認されている。適切な通知が、製品文書に含まれていて、エンド ユーザーに特定のオープン ソースのソース コードを要求する権利があることを知らせている。全てのソース コード コメントはレビューされ、不適切な内容は取り除かれている。これは厳密にはコンプライアンスの課題ではないですが、しかしながら、ある場合には、コードが受け取られた場所に関する無邪気なコメントが大きなコンプライアンスに関する問い合わせを生むきっかけになる可能性があります。

頒布前検証フェーズの前提条件

コンポーネントは利用が承認され、ソフトウェア一覧表に登録され、全ての通知が収集され義務履行のために送付されている。

頒布前検証フェーズの結果

. 頒布方法と様式を決定します

. 全ての頒布前検証が問題なく完了していることを確実にします。

ステップ9頒布

頒布前検証が全て完了したら、対応する製品とバージョンをラベル付けして（このシナリオは、ソース コードを入手可能になることを想定しています。他の方法は後続の章で議論します。）、オープン ソース パッケージを頒布用ウェブサイトにアップロードします。この作業は、コードのダウンロードを希望する人には役に立ちますが、これ自体でライセンス義務を満たしていることにはなりません。更に、推奨プラクティスでは、コンプライアンスやオープン ソースに関係する問い合わせの受付に関する、電子メールや住所などの情報を提供します。

頒布フェーズの前提条件

全ての頒布前検証がチェックされ、問題が発見されていない。

頒布フェーズの結果

対象のコンポーネントのソース コードは、頒布用のウェブサイトにアップロードされる。（そういう頒布方法が選択された場合）

ステップ10最終検証

オープン ソース パッケージを頒布用のウェブサイトにアップロードしたら、パッケージが正しくアップロードされ、ダウンロードでき、エラー無しに外部コンピューターで解凍できることを確認します。もし、パッチを提供する時には、それが容易に適用できること、アップストリーム コンポーネントの適切なバージョンを特定していることを確認します。

最終検証フェーズの前提条件

ソース コードはウェブサイト上で公開される。

最終検証の結果

ソース コードは正しくアップロードされ、ダウンロード可能で、承認されたものと同じバージョンに対応しているという確認結果を受けます。

第5章

コンプライアンス プロセスとポリシー

本書の目的から、ここでの議論の焦点は、商用製品におけるオープン ソースとプロプライエタリやサード パーティ ソースコードとの統合や利用に当てます。ここでの議論では、テストや評価目的など組織内だけで利用されるオープン ソースのためのポリシーやプロセスは除外されますこの章では、基本コンプライアンス プロセスとインクリメンタル コンプライアンス プロセスや、インクリメンタル コンプライアンスを達成するためのガイドラインに加えて、利用ポリシーや利用プロセスも議論します。

ポリシー

利用ポリシーは、コンプライアンス プログラムの不可欠要素です。このポリシーは、長文や複雑なものである必要はありません。単純なポリシーでも、以下の項目を要求するものであれば、複雑なポリシーと同じように効果的であることができます。

. 技術者は、いかなるオープン ソースであっても製品に統合する前には、OSRBから承認を得ることが必要です。. サード パーティ企業から受け取るソフトウェアは、含まれているオープン ソースを全て特定しなければなりません。このことは、製品出荷前までにライセンス義務を実施することを確実にしてくれます。

. 全てのソフトウェアは、監査とレビューを受ける必要があります。これにはプロプライエタリ ソフトウェア、サード パーティ プロバイダーから受け取ったソフトウェア、そしてオープン ソース ソフトウェアを含みます。

. 製品は、顧客が受け取る前に、オープン ソース ライセンス義務を実施しておく必要があります。

. 一つの製品に対する承認は、たとえ同じオープン ソース コンポーネントを利用していても、別の製品への承認とはなりません。

. 全ての変更されたコンポーネントは、承認プロセスを通過しなければなりません。

これらの規則は、いずれのソフトウェア（プロプライエタリ、サード パーティ、オープン ソース）も製品基盤へ導入されるまでに監査され、レビューされ、承認されることを確実にします。さらに、それは、顧客が製品を受け取る前に、様々なソフトウェア コンポーネント利用に起因するライセンス義務を実行する計画を、企業が持つことを確実にします。

プロセス

コンプライアンス利用プロセスは、問題となるソフトウェア パッケージのソースコードのスキャン、発見された課題の特定と解決、法務レビューおよびアーキテクチャー レビューの実施、そのソフトウェア パッケージに対する利用許可に関する判断を含みます。

図14は、コンプライアンス利用プロセスの簡略化された図を示しています。この図は、プロセスの反復的な性質は示していません。より詳しい図は、図17（90ページ）に示します。.

図14. コンプライアンス利用プロセスの例

ソース コード スキャン

ソース コード スキャン フェーズで、全てのソース コードはソース コード スキャン ツールを使用してスキャンされます。図15（82ページ）は、ソース コード スキャンを開始する要因を示しています。それらは、

. 通常、技術スタッフによって記入されるOSRB利用フォームの到着。これは、技術者や開発者が、問題となるソース コードについての基本情報を提供するために記入する簡単なオンラインのフォームです。フォームの提出によって、（JIRAやBugzillaなどのシステムで）コンプライアンス チケットが自動的に生成され、ソース コード スキャン要求が監査スタッフへ送られます。. 定期的に計画された全プラットフォーム スキャン：こうしたスキャンは、ソフトウェア プラットフォームにOSRBフォーム無しで忍び込んでいるかもしれないオープン ソースを明らかにするのに非常に役に立ちます。. 前に承認されたソフトウェア コンポーネントに対する変更：多くの場合、技術スタッフは特定のバージョンのOSS コンポーネントを評価やテストして、新しいバージョンが利用可能になった時にそのコンポーネントを採用します。

. オープン ソースを開示しているか不明なサード パーティ ソフトウェア プロバイダーから受け取ったソース コード。作者やライセンスが不明であり、オープン ソースが含まれているかもしれないウェブからダウンロードしたソース コード。技術者がオープン ソース コードを模倣しているかもしれないし、プロプライエタリ ソフトウェアにオープン ソース コード使っているかもしれないようなビルドシステムに、入ってくる新しいプロプライエタリ ソフトウェア コンポーネント。

図15. ソース コード スキャンを開始するイベント

法務レビューへの準備中に、ソース コード スキャンを実施する担当者は、著作権や帰属を表記しているファイルに加えて、COPYING, README, LICENSEファイルなど、パッケージで見つかった全てのライセンス情報をコンプライアンス チケットに付けておくべきです。

特定と解決

特定と解決フェーズで、監査チームは、スキャン ツールでフラグをつけられたファイルやコード断片を検査し解決します。

法務レビュー

法務レビュー フェーズでは、法務担当（OSRBメンバー）は、スキャン ツールによって生成された報告や、ソフトウェア コンポーネントのライセンス情報や、技術者やOSRBメンバーによってコンプライアンス チケットに記載されたコメントをレビューします。ライセンスに問題が無いならば、法務担当は、ソフトウェア コンポーネントに関して、入るライセンスと出るライセンスを決定し、コンプライアンス アーキテクチャー レビュー フェーズへコンプライアンス チケットを進めます。例えば両立しないライセンスをもつソース コードを組み合わせるなど、ライセンスに課題が発見されたときには、法務担当はこれらの課題にフラグをつけて、コードの再作業のためにコンプライアンス チケットを技術担当へ再割り当てします。ライセンス情報が不明確である、ライセンス情報が入手できない等、いくつかの場合には、法務担当は、不明瞭な点を明確にするとともに特定のソフトウェアに付与されているライセンスの確認をするために、プロジェクトのメインテナーやオープン ソース開発者にコンタクトします。

アーキテクチャー レビュー

アーキテクチャー レビューの中では、コンプライアンス オフィサーとOSRB技術代表は、オープン ソースとプロプライエタリ、およびサード パーティ コードの間の相互関係を解析します。これは特定されたアーキテクチャー図を検査することで実行されます。

. オープン ソース コンポーネント (そのままで利用、又は変更して利用) . プロプライエタリ コンポーネントサード パーティ ソフトウェア プロバイダー由来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特に、異なるオープン ソース ライセンスによって許諾されているような場合で、特定のソフトウェア コンポーネントが相互作用するか、または依存するような、他のオープン ソース パッケージ。

アーキテクチャー レビューの結果は、オープン ソースからプロプライエタリやサード パーティ ソフトウェア コンポーネントへ（同様にオープン ソース コンポーネント間で）影響を与えるようなライセンス義務の分析となります。コンプライアンス オフィサーは、例えば、プロプライエタリ ソフトウェア コンポーネントとGPLで許諾されたコンポーネントがリンクされるような課題を見つけたら、解決のためにコンプライアンス チケットを技術担当へ送ります。課題が無いならば、コンプライアンス オフィサーは、チケットを承認プロセスの最終段階へ送ります。

最終レビュー

最終レビューは、通常はOSRBメンバが対面する会議で行い、OSRBは利用の許可または却下を決めます。ほとんどのケースでは、ソフトウェア コンポーネントが最終レビューの段階まで到達したら、（そのソフトウェア コンポーネントがもう使われていないなどの）何かの条件が現れない限り、そのコンポーネントは承認されます。承認されたら、コンプライアンス オフィサーは、承認されたソフトウェア コンポーネントのライセンス義務リストを準備し、義務実施のために適切な部署へ送ります。

プロセスの各ステージにおけるインプットとアウトプット

この節では、図16で示されるOSRB利用プロセスの5つのフェーズにおけるインプットとアウトプットについて議論します。これらのフェーズは、説明目的のものであって、実際のシナリオとは正確には一致しないかもしれません。

図16利用プロセスのインプットとアウトプット

ソース コード スキャン段階

インプット

スキャン フェーズへのインプットは、技術者がオンラインで記入して提出するOSRB利用フォームとなります。表6 (98ページ)はフォームの詳細です。フォームは、ソース コード リポジトリ システムの中でのソース コードの位置も含めて、問題となっているオープン ソース コンポーネントに関する全ての情報を含んでいます。定期的な全プラットフォーム スキャンは、対応するOSRBフォーム無しにプラットフォームへソフトウェア コンポーネントが入らないことを確実にするために、数週間に1回程度実施されるべきです。

アウトプット

スキャン フェーズのアウトプットは、ソース コード スキャン ツールによって生成される報告です。これには、次のような情報が書かれます。

. 利用されている既知のソフトウェア コンポーネント、ソフトウェア構成リスト（BoM）として知られているもの影響があるライセンス、ライセンス文、義務の要約法務担当によって検証されるべきライセンス矛盾ファイル一覧表特定されたファイル依存関係コード一致特定保留中のファイル特定保留中のソース コード一致

特定と解決フェーズ

インプット

このフェーズへのインプットは、前フェーズでスキャン ツールによって生成された報告書になります。この報告書は、矛盾を起こしているライセンスや両立しないライセンスのような課題にフラグを付けています。課題がないならば、コンプライアンス オフィサーは、コンプライアンス チケットを法務レビュー フェーズへと進めます。. 解決すべき課題がある時には、コンプライアンス オフィサーは、コンプライアンス チケットにサブタスクを設定し、解決のために適切な技術者に担当を割り当てます。ある場合にはコードの再作業が必要となりますし、別の場合には単に状況を明確にするだけで解決することもあります。サブタスクは、課題の説明、技術担当によって実施されるべき解決提案、そして完了までの具体的な日程を含んでいるべきです。

アウトプット

このフェーズでは、サブタスクはクローズされた上で、全課題の解決がアウトプットとなります。コンプライアンス オフィサーは、ソース コードの再スキャンを依頼してスキャン報告書を作成し、前に上がった課題が解決済みになっていることを確認するかもしれません。コンプライアンス オフィサーは、レビューと承認を受けるために、コンプライアンス チケットを法務代表へ送ります。

法務レビュー

インプット

コンプライアンス チケットが法務レビュー フェーズへ届いた時には、コンプライアンス チケットは以下を含んでいます。

. ソース コード スキャン報告、スキャン フェーズで発見された課題が全て解決済みであることの確認

. チケットに付けられたライセンス情報のコピー：通常、コンプライアンス オフィサーは、ソース コード パッケージに含まれているREADME, COPYING, AUTHORSなどのファイルをコンプライアンス チケットに付与します。通常COPYING, LICENSEファイルに含まれているOSSコンポーネントに関するライセンス情報以外にも、著作権や帰属情報を入手することが必要です。この情報は、製品ドキュメントに適切に入れられます。. コンプライアンス チケットに関するコンプライアンス オフィサーからの（懸念点や追加の質問などの）フィードバック

. OSRBの技術代表や、内部的にこのパッケージを担当／保守する技術者（パッケージのオーナー）からのフィードバック

アウトプット

このフェーズのアウトプットは、コンプライアンスに関する法務の意見、問題となっているソフトウェア コンポーネントについての入るライセンスと出るライセンスに対する決定となりまソフトウェア コンポーネントは、異なるライセンスによって許諾されるソース コードを含むことがあるので、入るライセンスと出るライセンスは、複数のフォーム入ることがあります。

入るライセンス、出るライセンス

入るライセンスは、受け取ったソフトウェア パッケージに対するライセンスです。出るライセンスは、使用許諾するソフトウェア パッケージに対するライセンスです。あるケースでは、入るライセンスが（BSDのように）再許諾を許すような許容型ライセンスである場合には、企業はそのソフトウェアをプロプライエタリ ライセンスで再許諾します。より複雑な例としては、プロプライエタリ ソース コード、ライセンスAで許諾されているがライセンスBでも許諾可能なソース コード、ライセンスCで許諾されたソース コードが含まれるものがあります。法務レビュー期間に、法務担当は出るライセンスと入るライセンスを決める必要があります。

入るライセンス = プロプライエタリ ライセンス + ライセンスA + ライセンスB + ライセンス

出るライセンス = ?

アーキテクチャー レビュー

アーキテクチャー レビューの目的は、オープン ソース コードとサード パーティ、プロプライエタリ コードの間の相互作用を解析することです。アーキテクチャー レビューの結果は、オープン ソース コンポーネントがプロプライエタリ コンポーネントへ影響を与えるかもしれないライセンス義務の分析です。企業内のパッケージ オーナー、OSRB技術代表とコンプライアンス オフィサーが、通常アーキテクチャー レビューを実施します。もしライセンスの矛盾になるような依存関係を発見した場合、コンプライアンス オフィサーは、ソース コードの再作業によって依存関係問を題解決するためにチケットを技術担当に発行する。

インプット

監査されたソース コード、解決されている全ての課題。

アウトプット

OSRBメンバは、特定のコンポーネントに対してアーキテクチャ レビューを実施し、次のステップ（つまり最終承認）への準備が整っているという印をつけます。

最終承認フェーズ

インプット

このフェーズへのインプットは、ソフトウェア コンポーネントに関する全てのコンプライアンス記録です。それには以下が含まれます。

. スキャン ツールによって生成されたソース コード スキャン報告発見された課題、課題が解決された経緯に関する情報、課題が解決されたことを確認した人アーキテクチャー図、ソフトウェア コンポーネントが他のソフトウェア コンポーネントとどのように相互作用するかの情報

. コンプライアンスに関する法務の意見、入るライセンスと出るライセンスに関する決定組み込み環境（C/C++）で適用可能であれば、動的リンクと静的リンクの解析

アウトプット

このフェーズのアウトプットは、ソフトウェア コンポーネントの利用に関する、承認または却下の判断です。

詳細な利用プロセス

勿論、コンプライアンス手順に影響を与える多くの事情があります。図17（次ページ）は、いくつかの可能なシナリオと、コンプライアンス プロセスにおいて、一つのステップから別のステップへどのように状態遷移するかについて、詳細なプロセスを示しています。8つの可能なプロセスを議論します。これらのシナリオは、相互に排他的ではありませんし、唯一の可能なプロセスでもありません。これらは、図示と議論の目的のために提示します。

シナリオ1：スキャンされたソース コードは100%プロプライエタリである

シナリオ2：スキャンされたソース コードは両立しないライセンスを含むコードを含んでいる

シナリオ3：リンクに関する課題がアーキテクチャー レビューの最中に特定される

シナリオ4：ソース コード パッケージはもはや使われていない

シナリオ5：精査でライセンス義務を満足する形でリリースするべきIPが特定される

シナリオ6：検証ステップで解決すべき課題が特定される

シナリオ7：ソース コードは利用が承認される

シナリオ8：ソース コードは利用が却下される

図17コンプライアンス シナリオの一例

シナリオ1：スキャンされたソース コードは、100%プロプライエタリである

スキャンされたソフトウェア コンポーネントは、100%プロプライエタリ コードだけを含んでいて、オープン ソース コードは申告も特定もされていない。このケースでは、迅速な処理を想定し、特定のコンポーネントのコンプライアンス チケットは、法務レビューに進められます。法務担当は、ライセンスをこのプロプライエタリ コンポーネントに付与し、アーキテクチャー解析とリンク解析の実施のためにコンプライアンス オフィサーへ送ります。

シナリオ2：両立性のないライセンス（の組み合わせ）

スキャンされたソフトウェア コンポーネントは、両立性のないライセンスが付けられた複数のソース コードに由来するソース コードを含んでいることがあります。他の例としては、プロプライエタリ ソース コードとGPLで許諾されたソース コードとが組み合わされたものがあります。このシナリオでは、コンプライアンス チケットにスキャン報告が付けられ、プロプライエタリ ソフトウェア コンポーネントからGPLソース コードを取り去るという作業要求と共に、企業内でそのソフトウェア コンポーネントを管理している開発者に作業が割り当てられます。いったん開発者がコードの再作業を行った後は、そのソフトウェア コンポーネントは、法務レビューへ進む前に、GPLコードが取り除かれたことを確認するために、再スキャンされます。

シナリオ3：リンクに関する課題が特定される

このシナリオでは、コンプライアンス チケットは、法務レビューをパスして、アーキテクチャー レビューとリンク レビューに進みます。コンプライアンス オフィサーは、リンクに関する課題を見つけます。このケースでは、コンプライアンス オフィサーは、コンプライアンス チケットを解決フェーズに送り、リンクに関する課題を解決するように開発者に割り当てます。

シナリオ4：ソース コードは、もはや使われない

このシナリオでは、技術担当は、コンプライアンス プロセスの処理中に、そのソフトウェア コンポーネントが製品に混入しないようにします。結果として、そのコンプライアンス チケットは（却下として）クローズされます。当該コンポーネントが次に利用される場合には、そのコンポーネントが製品に組み込まれるか、ソース コード リポジトリに入る前に、コンプライアンス プロセスに再入力して承認を得なければなりません。

シナリオ5：開示要求のリスクがあるIP

このシナリオは、法務レビューが、非開示になっている知的財産とオープン ソース コード パッケージとが組み合わされていることを明らかにしたものです。法務担当は、この件にフラグを付けて、オープン ソース コンポーネントからプロプライエタリ ソース コードを取り除くために、コンプライアンス チケットを技術担当に割り当てます。技術担当がオープン ソース コンポーネント中にプロプライエタリ ソース コードを保持し続けることを固辞した場合には、OSECはプロプライエタリ ソース コードをオープン ソース ライセンスの下でリリースする決定をしなければならなくなるでしょう。

シナリオ6：未解決の課題が見つかる

OSRBメンバーがソフトウェア コンポーネント中にコンプライアンスに関する課題を発見したような全てのケースは、コンポーネントは同じライフ サイクルを進みます。

. 技術担当は、特定された課題を解決します。

. 監査チームは、ソフトウェア コンポーネントを再スキャンし、新しいスキャン報告を提出します。

. 法務担当は、新しい監査報告を確認します。. コンプライアンス オフィサーは、アーキテクチャー解析、リンク解析において未解決の課題がないことを確認します。

シナリオ7：ソースコードは、承認される

ソフトウェア コンポーネントが、監査、法務レビュー、コンプライアンス承認を全て受けたら、OSRB会議でその結果をレビューします。もし、状況に何も変更が無いならば、つまり、まだ使用されており、同じバージョンであり、利用形態が同じであること（次ページの図18）コンプライアンス オフィサーは、

. あるOSSソフトウェア コンポーネントのバージョンXは、製品YのバージョンZでの使用が承認されたことをソフトウェア一覧表に反映させます。

. 製品に付属する文書中のエンド ユーザーへの通知を更新して、製品やサービスにオープン ソースが使用されていることを反映させるため、文書チームへチケットが発行されます。

. 製品出荷前に、頒布プロセスを開始させます。

図18OSRB承認後に実施されるステップ

シナリオ8：ソース コードは利用が却下される

このシナリオでは、OSRBは、特定のソフトウェア利用の却下を決定します。そういう却下につながるような理由がいくつかあります。

. そのソフトウェア コンポーネントは、もはや使われない。

. 容易に解決できないリンクに関する課題がある。このケースの結論は、開発を中止し、より良いソリューションを設計しなおすというものです。

. 容易に解決できない両立しないライセンスがある。このケースの結論は、開発を中止し、より良いソリューションを設計し直すというものです。

. 特定のコンポーネントの利用やリリースを阻害する知的財産に関する課題がある。

. その他の理由：それぞれのケースは、問題となっているソフトウェア コンポーネントの個別条件や、最終製品やサービスでの利用形態に依存します。

インクリメンタル コンプライアンス プロセス

インクリメンタル コンプライアンスは、すでに初期コンプライアンスが完了しているベースライン版に製品フィーチャーを追加する時に、コンプライアンスを維持するために実施されるプロセスです。（ベースライン コンプライアンスとも呼ばれる、初期コンプライアンスは、開発が開始された時に発生し、製品の初期版が出荷されるまで継続します。）インクリメンタル コンプライアンスは、ベースライン コンプライアンスを確立するために必要とする努力と比べると小さな努力ですみます。

図19は、製品開発とインクリメンタル コンプライアンスを示しています。

図19インクリメンタル コンプライアンス

この例では、コンプライアンス チームは、ソフトウェア ベースライン（ここでは仮にV 1.0と呼びます）に含まれる全てのオープン ソースを特定し、オープン ソース コンポーネント全てが、コンプライアンス プロセス全体を通るようにします。製品が出荷されたら、追加機能や不具合修正などを含む開発は、新しいブランチで行われます。この例では、V 1.1です。

インクリメンタル コンプライアンスに関しては、解決すべきいくつかの課題が発生します。特に、V1.0とV1.1の間で変更されたソース コードを正確に把握し、リリースの間の変化点についてコンプライアンスを検証します。

. 新しいソフトウェア コンポーネントが、導入されているかもしれません。. 既存のソフトウェア コンポーネントが、既に使用中止になっているかもしれません。. 既存のソフトウェア コンポーネントが、新しいバージョンに更新されているかもしれません。. ソフトウェア コンポーネントのライセンスが、バージョンの間で変更されているかもしれません。

. 既存のソフトウェア コンポーネントが、不具合修正を含むコード変更や、機能やアーキテクチャーに対する変更を含んでいるかもしれません。

あるべき質問は、「どうすれば全ての変更を追跡できるだろうか？」というものです。

答えは単純です。：第7章で議論しますが、BoM比較ツールです。ここでの議論のために簡単に言うと、そのツールは、同じ製品やサービスに使う2つのBOMの差分を与えてくれます。製品V1.1のBOMと製品V1.0のBOMがあると、その差分を計算します。ツールの出力は以下のようなものです。

. V1.1で追加された新しいソフトウェア コンポーネントの名前更新されているソフトウェア コンポーネントの名前使用されなくなったソフトウェア コンポーネントの名前

この情報を知ることで、インクリメンタル コンプライアンスの達成は、比較的容易なタスクになります。

. 新しいソフトウェア コンポーネントをコンプライアンス プロセスに入力します。

. 変更されたソフトウェア コンポーネントのソース コードの差異を計測し、再度ソース コードをスキャンするか、あるいは前のスキャンは信頼に足るものかを、決定します。

. もはや使われなくなったソフトウェア コンポーネントをソフトウエア管理表から除いて更新します。

図20（次ページ）は、インクリメンタル コンプライアンス プロセスの全体像を示しています。それぞれの製品リリースに対するBOMファイルは、ビルド サーバーに保存されます。BOM差分ツールは、異なる製品リリースに対応する2つのBOMファイルを入力として受け取り、前に議論したように、変更リストを生成します。この時点で、コンプライアンス オフィサーは、リリースに含まれる全ての新しいソフトウェア コンポーネントに対して新しいチケットを発行し、ソース コードが変更されている部分はコンプライアンス チケットを更新した上で、できればプロセスを再実行し、使用中止になったソフトウェア コンポーネントを承認リストから削除して、ソフトウェア管理表を更新します。

OSRB利用フォーム

OSRB利用フォーム（要求フォームとも呼ばれます）を記入することは、オープン ソース ソフトウェアを企業へ導入する際の最も重要なステップの一つです。ですから、真剣に取り扱うべきものです。開発者は、該当するオープン ソース コンポーネントの利用の承認を要求するオンライン フォームを記入します。そのフォームは、提案されているオープン ソース コンポーネントの利用をOSRBが承認または却下することを決めるのに必要な情報を与えるような、いくつかの質問から構成されています。図6（97ページ）は、OSRB利用フォームで要求されている情報を示しています。通常、これらの値は、データ入力を効率的に行うために、プルダウン メニューで選べるようにします。

図20インクリメンタル コンプライアンス プロセスの例

ダウンロードされたオープン ソース パッケージに対する注意

ウェブからダウンロードしたオープン ソース パッケージをオリジナル形式で保管しておくことは不可欠なことです。これらのパッケージは、後の段階で（頒布の前に）、オリジナル パッケージと変更されたパッケージの差異を計算することによって、ソース コードに加えられた全ての変更を検証し追跡するために、使用されます。もし、サード パーティ ソフトウェア プロバイダーがオープン ソース コードを使っていれば、そのコードを製品に統合する製品チームは、OSRB利用フォームに、利用するオープン ソースを記載して提出しなければなりません。もし、サード パーティ ソフトウェア プロバイダーが、ソースコード無しにバイナリだけを提供している場合には、製品チームと、そのサード パーティ ソフトウェア プロバイダーと連絡を取っているソフトウェア供給マネージャは、両方、またはどちらかが、（例えばスキャン報告などによって）提供されたソフトウェアにオープン ソースが含まれていないことを確認しなければなりません。

表6OSRB利用フォームの一部として要求される情報

区分

説明

提出者情報

フォームを提出する社員の社員ID（社員名、電話、Eメール、管理者、職務場所、チームなどを社員管理表から受け取ります）

OSSコードの情報

パッケージ名とバージョン

ソフトウェア区分：オープンソース、内製、サード パーティ パッケージ

ウェブサイトURL

説明

ライセンス名とバージョン

ライセンス ウェブサイトURL

ソフトウェア カテゴリ：OS/kernel, driver, middleware, library, utility, other (explain), etc.

OSSコンポーネントを利用する利点

コンポーネントやパッケージとは別の手段

ソフトウェアを利用しないことによって発生すること

SCMSでのソフトウェアの位置

ユースケース

内部利用（ツール、IT等）

製品の一部として出荷

外部向けサービスを可能にする

変更

変更されているか (Y/N)?

会社IPは含まれるか?

IPを開示するか?

アーキテクチャー図に対する注意

アーキテクチャー図は、あるプラットフォーム上での様々なソフトウェア コンポーネント間の相互作用を示します。図21は、アーキテクチャー図の一例です。この図では、以下を示します。

. モジュールの依存関係プロプライエタリ コンポーネントオープン ソース コンポーネント（変更後とオリジナル）動的リンクと静的リンクカーネル空間とユーザー空間共有されているヘッダ ファイル通信プロトコル課題となっているソフトウェア コンポーネントが、相互作用する、または依存関係にあるような、他のオープン ソース コンポーネント。特に、別のオープン ソース ライセンスによって許諾されている場合。

図21（CやC++に依存するような組み込み環境へ適用する）アーキテクチャー図のテンプレート

OSRB利用フォームに影響する規則

OSRB利用フォームに影響するいくつかの規則があります。ここにいくつか挙げます。

. フォームは、特定の利用状況における、特定の製品でのオープン ソースの利用に対して適用します。それは、全製品の全ユースケースに対するそのオープン ソース コンポーネントの全般的な承認ではありません。

. フォームは、監査活動の基礎となり、OSRBが、フォームで表現された利用計画と、監査やアーキテクチャー レビューの結果とに矛盾が無いかを確認するための情報を提供します。. フォームは、該当するオープン ソース コンポーネントの利用計画が変更になった場合には、更新して再提出されなければなりません。

. 技術担当がそのオープン ソースを製品ビルドに統合する前に、OSRBがフォームを承認しなければなりません。

. ライセンスが特許許諾条項や非係争条項を要求している時には、OSECがオープン ソース利用の承認をしなければなりません。

監査

良い監査プラクティスは、製品やサービスの一部として採用される全てのソフトウェアの由来を完全に把握することを確実にします。このことを理解することによって、オープン ソース ソフトウェアライセンス義務を果たす組織能力が出来上がります。監査ポリシーは、単純でわかりやすいものです：ポートフォリオ／スタックに含まれる全てのソース コードは、監査され、コンプライアンス チケットに監査報告がつけられなければなりません。監査プロセスは、技術担当が特定のソフトウェア コンポーネントに対するOSRB利用フォームを提出した後に、続いて実行されるワークフローから構成されます。

監査プロセスは、次のフェーズで構成されます。（図22）

監査すべきソース コードの場所を含む、OSRB利用フォームを受け取ります。

. ソース コードのスキャンを実施します。. スキャン ツールでフラグがつけられたコンポーネントの分析を実施します。

. 最終監査報告を作成します。

図22：基本監査プロセス

ソース コード頒布

ソース コード頒布プロセスとポリシーの目的は、以下を確実にすることです。

. オープン ソース ソフトウェアを含む製品を購入する顧客やサービスを利用するユーザは、適用可能な場合に、ソース コードを受け取る権利があることを通知される。頒布したソース コードは、頒布サイトに転送されるソフトウェアのバイナリ バージョンと照らし合わせて正しいバージョンであり、また、適切にラベル付けされている。

頒布の動機

オープン ソース コードを頒布することには主に3つのビジネス上の動機があります。ライセンス義務の遵守、オープン ソース プロジェクトの価値を高めるための貢献、新しいオープン ソース プロジェクトに対するコードの貢献です。

ライセンス義務の順守

この例では、組織は、オープン ソースを製品やサービスに組み込んでおり、オープン ソース コンポーネントライセンスにより、ソース コードに加えた変更を含めて、ソース コードの開示義務を持っています。コミュニティとの相互関係が双方向であるのに対して、このことは一方向頒布と略式に考えられます。

既存のオープン ソース プロジェクトへの修正の貢献

あるケースでは、オープン ソース ライセンスは、ライセンス コンプライアンスの目的からすると、修正を開示する義務を含んでいません。しかしながら、技術的な負荷、言い換えればこれらの修正を保守するコストを抑えるために、修正をリリースし、可能なアップストリームに載せます。

新しいオープン ソース プロジェクトの設立

組織は、ビジネス的な必要性から、新しいオープン ソース プロジェクトを設立し、ソース コードの貢献をするかもしれません。このケースは、既存のオープン ソース プロジェクトへ、（不具合修正や新規機能追加の形で）ソース コードの貢献をすることとは異なります。

頒布プロセスとポリシー

頒布ポリシーの目的は、ソース プロジェクト コード（＊＊＊）の供給プロセスに強い影響を与え、オープン ソース コードの入手性に関するオープン ソース ラインセンス義務の遵守するために、様々な流通[ロジスティックス]に対するガイドラインを提供することです。この頒布ポリシーは、ライセンスがソース コードの再頒布を要求するようなソフトウェア パッケージに適用されます。公開プロセス、公開方法、モード、チェックリストなどをカバーします。

プロセスを開始させる前に、ソース提供の方法と様式を決めなければなりません。プロセスは、外部へ頒布するソース コードの準備をもって始まり、頒布前チェックリストの確認、ソース コード パッケージの入手性の確認、そして、頒布後チェックリストの確認と続きます。

図23は、頒布プロセスの例を示します。以下を含みます。

. ソース コード提供方法を決めます。頒布様式を決めます。外部頒布のためにソース コード パッケージの準備をします。前に置かれた全ステップが問題なく完了していることと、外部頒布に向けてソース コード パッケージの準備が整っていることを確実にするために、頒布前チェックリストを全て確認します。. 頒布を実行します。頒布プロセスの一部で発生するかもしれない誤りを把握するために、頒布後のチェックリストを確認します。

図23公開プロセスの例

頒布方法と様式

ソース コード パッケージを入手可能な状態にする、3つの主な頒布方法があります。

即時コンプライアンス方法

この頒布方法に従い、製品やソフトウェア スタックの出荷時または直後にコードを提供し、一般的にはウェブサイトからダウンロードによって、コードを欲しい人は誰でも入手できるようにします。開発者は、入手資格を確認されることなく（つまりソース コードの入手資格を得るために製品を購入する必要なく）、直接ソースコードにアクセスが許されますので、このやり方は通常開発者にとって頒布の好ましい方法となります。あるケースでは、即時コンプライアンス方法は、メディアのディレクトリproduct/deviceにソース コードを含めることで、達成することができます。

この頒布方法には2つの不利な点があります。まず第1に、全てのソース コードをパッケージ化し、製品出荷の準備を整える出荷日までに、ウェブサイト上でソース コードを入手可能にするという多大な努力が必要です。第2に、将来のソース コード頒布でも同じ方法が取られるだろうという期待を築いてしまいます。これは、毎回満足させるべきとても高い期待となります。

オンライン供給方法

この頒布方法によれば、ソース コードを入手する資格を持っている顧客だけが、排他的にアクセス権を与えられます。この方法は、アクセスしてソース コード パッケージをダウンロードするための認証を必要とするセキュアなウェブサイトにより最もよく管理されます。

オン デマンド コンプライアンス

この頒布方法は、オンライン供給方法の変形で、書面による通知(GPL/LGPL系のライセンスの場合)を利用して、どのようにすればソース コードを要求したりアクセスしたりできるかを顧客に伝えます。ある組織は、企業窓口emailや郵便アドレス(書面による通知に書かれている)に対して書面で要求が送られるのを好みます。結果として、顧客は、入手資格を確認された後で、ソース コードのコピーを受け取ります。このコンプライアンス方法は、製品出荷後に、ソース コード パッケージ化終了のための追加の予備時間を組織に与えてくれます。しかしながら、一般的に言って、ソース コードへのアクセスを要求してくる人たちの入手資格を確認するのにかかるオーバーヘッドや、要求を満たすために必要となる資源を考えると、好ましい頒布方法とは言えません。加えて、GPL/LGPL系のライセンスに特有のケースとして、書面による通知は3年間有効でなければなりません。それゆえ、製品を最後に出荷した日から少なくとも3年間は、コード頒布を管理しなければなりません。CD-ROMでのソース コード頒布を選んだ場合には、追加のコストがかかりますし、ソース コード パッケージを格納したCD-ROMを生成するプロセスを確認する追加の検証ステップも必要になります。

頒布チェックリスト

顧客や一般向けのウェブサイトで公開する前に、オープン ソース パッケージの正当性を確認するための多くのチェックポイントがあります。更に、追加の正当性確認は、一般に入手可能になった後にも必要になります。以下では、頒布前、頒布後のプロセスについて概要を示します。

頒布の前提条件

以下は、ソース コード パッケージが頒布可能になる前に、適合しておくべき条件リストです。（頒布の衛生とも呼ばれます）

. オープン ソース パッケージは、利用フォームで宣言された範囲で、その利用をOSRBによって承認されています。. オープン ソース パッケージを含む製品は、出荷可能か、すでに出荷されています。

. もし、GPL/LGPLで許諾されたコードを開示するのであれば、自分たちが加えた変更について、コードと文書を提供することを確実にします。. リンギスティック レビューを実施しています。このことはコンプライアンス関連ではないですが、将来使用予定の製品コード名、下品または粗野な言葉づかい、個人やemailアドレスやURLへの参照などがコードに残されたままであったというような課題が過去にありました。

頒布前チェックリスト

以下は、ソース コードの一般公開や頒布の前に行うチェックリスト例です。

. オープン ソース パッケージに加えられた変更は、文書化されて、オープン ソースのリリース ノートに変更履歴として含まれていることを検証します。変更されたソース コード ファイルは、著作権表記や免責事項の記載や一般的な変更履歴への記載を含んでいることを確認します。

. ソース コード パッケージに含まれている全ての内容物は、技術担当によってレビューされ、OSRBによって確認されていることを、確認します。. オープン ソース パッケージは、企業のものでないマシンでコンパイルできることを確認します。企業で初期設定したマシン上でパッケージをコンパイルする時に、環境やコンパイラが全て事前に構成されたり設定されているということがよくあります。しかしながら、別のシステムでパッケージをコンパイルしようとする場合には、コンパイラの設定や、Makefileのオプションや、Include path等が適切でないかもしれません。このステップの目的は、頒布しようとしているオープン ソース パッケージが、平凡なエンド ユーザー システム上でコンパイルできることを確実にすることです。. 製品マニュアルを更新します。：製品がオープン ソース ソフトウェアを含むことを言及します。

. 製品に含まれる異なるオープン ソース ソフトウェアに対応する全てのライセンスのリストを含めます。

. 適切な著作権と帰属に関する通知を提供します。

. オープン ソース パッケージのコードへのアクセス方法（書面による申し出）、ウェブページからのダウンロードや、製品マニュアルで提供される特定のアドレス宛てのemailや郵便による問い合わせなどを提示します。

. 書面による申出が、そういう通知を必要とするソース コード（基本的に、GPL/LGPL系ライセンスで許諾されたコード）全てを包含しているかを検証します。

. ソース コードに不適切なコメントが残っていないことを確実にするために、リンギスティック レビューを実施します。ある企業では、リンギスティック レビューを通すことを忘れてしまい、製品がハックされた時に、ソース コード中に残っていた不適切なコメントが発覚し、困惑しました。リンギスティック レビューを実施する他の重要な理由は、ソース コードやコメントが、将来使用する開発コード名や機能を言及していないことを確実にすることです。. 既存のライセンス表記、著作権表記、帰属表記に手が入っていないことを確実にします。. 製品に搭載されて出荷されるバイナリに対応したソース コードであること、そのソース コードが製品とともに出荷されるライブラリを構成していること、ビルド手順がソース頒布（派生するバイナリは、タイム スタンプを除いて通常同一のものになります）に含まれていること、を検証します。

. パッケージが、OSRB利用フォームで定義されたリンク関係や相互作用を守っていることを検証します。例えば、開発者がコンポーネントをLGPLで許諾されたライブラリと動的にリンクすると宣言したならば、その通りになっていて、代わりに静的リンクを使っていないことを検証する必要があります。これは、リンク依存関係マッピング ツールを使って検証されます。

. もし、まだ入っていなければ、オープン ソース パッケージのソース コード ルート フォルダにあるLICENSEファイルに、ライセンス文のコピーを追加します。

. もし、ソース コード パッケージが、特別なビルド ツールや環境を必要とするならば、READMEファイル等にその詳細を記載します。

一般公開後のチェックリスト

以下は、ソース コードを一般公開した後に、ソース コード パッケージが入手可能になっているかを検証するチェックリストの例です。

. ソース コード パッケージは、ウェブサイトに問題なくアップロードされ、外部コンピュータからダウンロード可能になっています。

. ソース コード パッケージは、外部コンピュータでエラー無しに圧縮解凍できます。

. ソース コード パッケージは、外部コンピュータでエラー無しにコンパイルとビルドができます。

書面による申出

以下は、ソース コードを提供するための書面による申出の例です。

このFooBar製品で使用されているソフトウェアに関連して、FooBar社(“FooBar”) によって一般に開示されているソース コードのコピーを入手するためには、書面で要求を以下に出すことが必要です。

Foobar株式会社

Attention: Open Source Compliance Inquiries

Street Address

City, State, Postal Code

Country

FooBarは、妥当な遅延の範囲で、http://opensource.foobar.com (“Website”)にてソース コードが入手可能になるように可能な全ての努力をいたします。書面による要求を出される前に、ソース コードが既に公開されているか、このウェブサイトを確認して下さい。

代替手段として、郵便ではなくemailにて要求を受けたいならば、書面による通知の文言を少し変更します。

このFooBar製品で使用されているソフトウェアに関連して、FooBar社(“FooBar”) によって一般に開示されているソース コードのコピーを入手するためには、書面で要求をopensourcecompliance@foobar.comに出す必要があります。

FooBarは、妥当な遅延の範囲で、http://opensource.foobar.com (“Website”)にてソース コードが入手可能になるように可能な全ての努力をいたします。書面による要求を出される前に、ソース コードが既に公開されているか、このウェブサイトを確認して下さい。

第6章

コンプライアンス プロセス管理の推奨プラクティス

この章では、オープン ソースを商用製品に統合する際の、推奨プラクティスや様々な考察を扱います。3つの部分に分かれます。

. 推奨プラクティスは、オープン ソース コンプライアンス管理の一貫プロセスの中の様々なステップに配置されます。. ソース コード改変、告知、頒布、ソフトウェア設計、利用、リンク、コード結合など関連したコンプライアンスについての考察。. 推奨プラクティスは、オープン ソース コンプライアンス プログラムの中の様々な不可欠要素に関連します。

コンプライアンス プロセス

コンプライアンス管理プロセスは、製品ソフトウェア スタックへの組み込みが承認される前に、ソフトウェア コンポーネントが通過する様々なステップを含んでいます。プロセスは、製品ビルド システムへ統合する様々なソフトウェア コンポーネントを特定することで始まり、結果として発生するライセンス義務をリスト化することで終わります。

以下の節では、コンプライアンス要求を処理するための推奨プラクティスを示します。推奨プラクティスは、図24（次ページ）に示したコンプライアンス プロセスの中のステップに直接配置されます。

特定フェーズ

コンプライアンス プロセスの特定フェーズでは、組織は、ビルド システムへ入る全てのコンポーネント、その由来、ライセンス情報を特定します。入るソース コードには、主に3つの由来があります。

. 内部開発者によって作られたプロプライエタリ ソフトウェア。オープン ソースのコード断片を含んでいるかもしれません。コンポーネント レベルでオープン ソース コードと依存関係を持ったり、リンクされたりして、オープン ソースと統合されているかもしれません。独立プロバイダやコンサルタントによって開発され、商用ライセンスやオープン ソース ライセンスで許諾されたサード パーティ ソフトウェア。このソフトウェア カテゴリは上と同様にコード断片や依存関係を含んでいるかもしれません。

. オープン ソース プロジェクトのメンバーによって開発されたオープン ソース ソフトウェア。

図24コンプライアンス一貫管理プロセス

入るソフトウェア コンポーネントは、全て特定され、コンプライアンス プロセスを通されることが推奨されます。

ソース コード監査

ソース コード監査やスキャンに関して、3つの推奨プラクティスがあります。

全ソース コードスキャン

開発チームがオープン ソースをプロプライエタリ ソース コードやサード パーティ ソースコードに使用しているかもしれないので、製品やサービスに統合される全てのソース コードをスキャンします。更に、開発チームは、オープン ソース コンポーネントに変更を入れているかもしれませんが、これは、追加の精査を必要とするかもしれませんし、潜在的に追加義務を負うかもしれません。従って、製品に組み込まれている全てのソース コードを監査し、特定することが重要です。

前に承認されているパッケージの新しいバージョンのスキャン

ある場合には、前に承認されているパッケージが変更されて（同じ条件や異なる条件で）再利用されたり、そのまま再利用されたり、変更されて異なる製品やサービスに再利用されたり、新しいバージョンがダウンロードされてソフトウェア スタックに使用されたりします。コンプライアンスは、製品ごと、サービスごとに確認されますので、一つのケースでの利用承認は、必ずしも全てのケースに適用されることにはなりません。

規則として、開発者が前に承認されたコンポーネントを変更する時や、別の条件で前に承認されたコンポーネントの利用を計画する時には、その都度、ソース コードは再スキャンし直し、コンポーネントは再度承認プロセスを通過するべきです。

オープン ソース コンポーネントの各新しいバージョンが、レビューされ、承認されることを確実にします。

バージョン更新の間に、ライセンス変更が起きる可能性があります。開発者がオープン ソース パッケージのバージョンを更新するときには、新しいバージョンに適用されているライセンスが、古いバージョンに適用されていたものと同じであることを確認します。

「早めのリリース、頻繁なリリース“release early and release often.”」というオープン ソースに関する格言があります。

オープン ソース開発モデルは、プロジェクト初日に始める頻繁なリリースを推奨しています。これによってユーザーに評価実験や不具合報告の機会を与えます。その目的は、品質保証活動が開発プロセスの定常的な一部となることです。

「早めに、そして頻繁にスキャン“Scan early and often”」は、同じ精神に従っています。開発プロセスにおいて早期にソースコードスキャンを行い、それを定常的に継続することは、コンプライアンスの取り組みが開発の取り組みに後れを取らないようにします。組織は、プロセスがより効率的になるように、新しいスキャンが必要とされる時を定義した条件リストを作成すべきです。

「早めに、そして頻繁にスキャン“scan early and often”」というアプローチには、いくつかの有利な点があります。

. それは、プロセスの早い段階でのコンプライアンス課題の発見を助けます。

. それは、出荷スケジュールへ深刻な問題を与えないような許容できる期間で、発見された問題へ解決をもたらすことを促進します。. それは前に実行したソース コード スキャンの中でスキャンが必要なソース コード差分を減らすので、インクリメンタル スキャンの実行効率を改善します。

課題解決

ソースコードがスキャンされて、コンプライアンス課題が発見され、フラグがつけられた時、課題解決にはいくつもの方法があります。

. 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。（問題となっているソフトウェア コンポーネントの担当開発者にインタビューします。）. スキャン ツールでフラグを付けられた各ファイルやコード断片を精査し、解決します。驚くような由来のソース コードと一致することがあります。

. オープン ソースに施された変更を特定します。理想的には、コード変更をしたかどうか、（ドキュメントはいうに及ばず、）技術者の記録に依存するべきではありません。誰が、いつ、コード変更を行ったかを特定するには、ビルド ツール(SCM, build automation, etc.)に頼るべきです。

. 例えば、ソース コード スキャン ツールが、プロプライエタリ コンポーネントの中に未承認のGPL許諾されたソース コード（コード断片）の利用を発見したならば、このことについて、技術担当に訂正要求を提出します。技術担当が課題を解決した後、問題のソース コードが削除され、適切で同等のコードによって置き換えられていることを確認するために、ソース コードを再スキャンすることを推奨します。

. 法務レビューの準備としては、特定のコンポーネントに対して発見されたライセンス情報の全てを、法務担当に提供するのが最も良い方法です。スキャン ツールによって生成されたソース コード監査報告

. オープン ソース コンポーネントに対するCOPYING, README, LICENSE ファイルサード パーティ ソフトウェア プロバイダから受け取るソフトウェア コンポーネントに対するライセンス契約

レビュー

コンプライアンス プロセスの一部として行われる、異なるタイプのレビューがあります。この節では、アーキテクチャー レビューとリンク解析レビューを議論します。

アーキテクチャー レビューは、オープン ソースとプロプライエタリやサード パーティ ソフトウェア コンポーネントとの相互作用に関する解析です。企業は、しばしば、問題となっている製品に責任を持つアーキテクトと、様々な重要ソフトウェア コンポーネントに責任を持つ開発者を参加させて、アーキテクチャー レビューを実施します。

このレビューの目的は、特定することです。

. オープン ソース コンポーネント（そのまま利用、または変更利用）プロプライエタリ コンポーネント商用ライセンスで許諾されたサード パーティ コンポーネントコンポーネントの依存状態コンポーネントとサブシステム間の通信プロトコル動的リンクと静的リンク（以下の節で議論されます）

. カーネル空間実行（ドライバ等）とユーザー空間実行（ライブラリ、ミドルウェア、アプリケーション）. 共有されたヘッダファイルを使用するコンポーネント特に別のオープン ソース ライセンスで許諾されているような場合、特定のソフトウェア コンポーネントと相互作用する、または依存関係にある、別のオープン ソース

アーキテクチャー レビューの結果は、オープン ソース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 コンポーネントへ影響するかもしれないライセンス義務の分析です。

承認

コンプライアンス プロセスの承認段階の一部として、2つの推奨プラクティスがあります。

. コンプライアンス チケットに関連する全てのサブタスクは、コンプライアンス チケットを承認する前に、完了し、クローズされていることを検証します。サブタスクや保留中の小課題は簡単に忘れてしまいますが、そうすると、未解決の課題が残っている時でさえもコンプライアンス チケットをクローズするような未熟なプロセスに陥ってしまいます。

. 承認や却下の判断を下した議論の概要を記録します。そうした文書は、該当するコンポーネントに提示された承認の基礎が何であったのか、課題はどのように解決されたのか、を特定するときに非常に役に立ちます。

通知

製品やサービスにオープン ソースを利用している組織は、以下が必要となります。

. 著作権や帰属を全て通知することで、オープン ソースを利用していることを知らせます。. （例えば、GPL, LGPLで許諾されたソース コードのように、適用可能な場合には）エンド ユーザーにオープン ソース コードのコピーの入手方法を伝えます。

. 製品に含まれているオープン ソース コードに対応するライセンスの全文を提示します。

この分野のいくつかの推奨プラクティスには以下のものがあります。

. オープン ソースの利用が承認されるその都度、帰属とライセンス文を追加的に集めます。この方法に従いますと、要求される通知ファイルは、常に最新に更新され、全てのオープン ソースのリスト、ライセンス情報、著作権、帰属通知を含むことになります。

. 書面による申出には、明快な言葉を使い、製品に使われている全てのオープン ソースが含まれるようにします。

. 製品のエンド ユーザーが、この情報が、製品そのものの中、製品文書（ユーザーマニュアルまたはCD-ROM）の中、かつ／またはウェブサイトなど、どこに置かれているかを知ることができるようにします。

検証

コンプライアンス チームが、一貫性を確認して、検証ステップが見落とされていないかを確認する時に従うチェックリストを、作成し維持し発展させるのは大変有益で効率的なことです。頒布前検証の例としては以下があります。

. 頒布されることになっているオープン ソース パッケージは、特定され、承認されている。. 不適切なコメントは、ソース コード パッケージから取り除かれている。（厳密には、これはコンプライアンス課題ではありません。しかしながら、コメントは、見えていないコンプライアンス課題を明らかにするかもしれません。）ソース コード パッケージ（変更分も含めて）は、製品やソフトウェア スタックに入って出荷されるバイナリと一致するものが、入手可能にされる。エンド ユーザーにオープン ソースのソース コードを要求する権利を伝える文書通知に加えて、適切な通知が、製品文書に入れられる。

オープン ソース パッケージが頒布用ウェブサイト（かつ／または、同等のメディアに格納）にアップロードされたとしても、作業は完了していません。以下を検証する必要があります。

. パッケージは、正しくアップロードされている。パッケージは、外部コンピュータでエラー無しにダウンロードして圧縮解凍できる。含まれるパッケージは、適切にコンパイル、ビルドできる。. 開発者は、将来の製品、製品開発コード名、競合他社への言及、その他不適切なコメントを残していない。

ツールと自動化

ツールは、組織がコンプライアンス活動を効率的で正確に実行するのを助ける、コンプライアンス プログラムの中の不可欠要素です。多くのツールは、オープン ソース コンプライアンス プログラムの中で、とても有用であることを証明しています。

. ソース コード スキャンとライセンス特定ツール. プロジェクト管理ツールBoM比較ツールリンク解析ツール

以下の小節では、ツールに関する情報と、ツール利用がコンプライアンス活動にどのように活用できるかを示します。市場では、以下で記述するような様々な機能を提供する、複数の商用、プロプライエタリ、オープン ソースのツールがあります。

ソース コード特定ツール

ソース コードとライセンスを特定するツールは、ユーザーがオープン ソース ソフトウェア コンポーネントに関連するソース コードとライセンスの由来を特定するのを助けるような、検出と解析の機能を提供します。

. Antelink Reporter: http://www.antelink.com/

. Black Duck Protex: https://www.blackducksoftware.com/products/

protex

. The Black Duck Hub: https://www.blackducksoftware.com/

products/hub

. FOSSology: http://www.fossology.org/projects/fossology . nexB DejaCode: http://www.nexb.com/products.html

. Open Logic Exchange: http://www.openlogic.com/products-

services/openlogic-exchange

. Palamida Enterprise: http://www.palamida.com/products/enterprise . Protecode Enterprise: http://www.protecode.com/our-products/ . WhiteSource: http://www.whitesourcesoftware.com

Project Management Tools

プロジェクト管理ツールは、コンプライアンス活動を管理し追跡するのに不可欠なものです。いくつかの企業では、カスタマイズしたコンプライアンス ワークフローと共にバグ追跡ツールをすでに実際に利用しています。他の企業では、特定のプロジェクト管理ツールや自社開発ツールを利用しています。どちらにしても、ツールは、プロセスのある段階から別の段階へコンプライアンス チケットを移し、タスクやリソースの管理、時間追跡、email通知、プロジェクト統計、報告機能などを提供して、コンプライアンス プロセスのワークフローを反映させるべきです。

コンプライアンスで広く利用される不具合追跡ツールの例

. Bugzilla: https://www.bugzilla.org/ . IBM Rationale ClearQuest: http://www.ibm.com/software/products/

en/clearquest/

. JIRA: https://www.atlassian.com/software/jira . Redmine: http://www.redmine.org/ . Bugzilla: https://www.bugzilla.org/

ソフトウェアBOM差分ツール

ソフトウェアBOM差分ツールの目的は、二つのBOMの差分を計算し、変更リストを生成することです。このようなツールは、（例えば、リリース1.1から1.2へ移行するなど）既存のベース コードの新しいバージョンを扱う時、インクリメンタル コンプライアンスを効率的に実施するのを可能にします。BOM差分ツールへの入力は、製品やサービスのコード ベースの二つのバージョンのコンポーネント リストを示す二つのBOMファイルです。BOM差分ツールの出力は、新しいコンポーネント、使わなくなったコンポーネント、および変更されたコンポーネントのリストです。

BOM管理ツールは、物理的な製造の世界には多くのものがありますが、オープン ソース ソフトウェアの管理用途のものは少ないです。著者の経験では、オープン ソース管理プロセスを支援するBOM差分ツールは、

通常、自社内製であるか、かつ／または、既存ツールや機能をより集めて作られたものです。BOMのフォーマットにも依存しますが、ウェブベースでBOMバージョン比較を作成するために、コマンドラインのdiffツールや、生産性ツール(spreadsheets等)や、ディレクトリ比較ツール、ビルドや連続統合ツールからの報告に加えて、これらを結合するスクリプトを利用することが可能です。図25は、図での説明目的のために作られてものですが、自社内製のBOM差分ツールのサンプル出力を示しています。

図25BOM差分報告の例

リンク解析ツール

依存関係解析ツールの目的は、CやC++言語に特有の話題ですが、動的リンク、静的リンクのレベルで問題のあるコードの組み合わせにフラグを付けることです。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のライセンス間のリンクの矛盾を特定します。

上記のソース コード特定ツール、多くの静的解析ツール、ビルドや統合の報告ツール、自社内製のコード解析ツールなど、依存関係を解析するために一緒に利用されるツールが多くあります。依存関係マッピングに対する主な要求事項は、以下の機能です。

. バイナリとライブラリ間のリンクを特定します。バイナリとライブラリのライセンスを特定します。

. ライセンス スキャン ツールと接続します。または、出力を使います。. （GPLで許諾されたコードとのリンクなど）方針から逸脱しているリンクにフラグを付け、企業方針と合うように構成します。

著者の経験では、依存関係マッピング ツールは、BOMツールとよく似ていますが、通常、自社内製であるか、かつ／または、既存ツールや機能をより集めて作られたものです。

このタイプのオープン ソースの既存ツールとしては、Linux FoundationのDep-Checkerがあります。 (http://git.linuxfoundation.org/dep-checker.git/).

第7章

コンプライアンスに関する照会の管理

この章は、コンプライアンスに関する照会を扱うガイドラインについて示します。これらのガイドラインは、申し立てを調査している間に申立人に対して肯定的で協力的な態度を維持することと、ライセンス違反が実際に起きた時には適切な行動を取ることを、確実にします。

コンプライアンス情報の提供要求を無視した後に、否定的な評判を受けたり、かつ／または、法的手続きを受けた組織、コンプライアンスに関する照会をどう扱えばよいかわからなかった組織、コンプライアンス プログラムを持っていなかったり整備していない組織、ライセンスが強制的でないと（誤って）考えて協力を単に拒む組織があります。今日、ベスト プラクティスは、これらのアプローチがいずれの関係者の利益にもならないことを教えてくれます。従って、企業は、コンプライアンスに関する照会を無視するべきではありません。むしろ、照会を受け取ったことを知らせ、照会者に回答を保留していることを伝え、回答予定日を知らせるべきです。

コンプライアンスに関する照会は、以下の要求も含まれます。

. GPL, LGPLやその他のライセンスで許諾されたソース コードを提供するという文書通知に従って行われる、ソース コードへのアクセス製品内にあることがわかったが、開示されていないコンポーネントに関するソース コードへのアクセス特定のオープン ソース コンポーネントが製品やサービスで利用されているかどうかの確認無効となった帰属や著作権の通知に対する更新ライセンス義務の一環として入手可能になっているオープン ソース パッケージにおいて、抜けているファイルの提供

企業は、通常、コンプライアンスに関する照会を、書面による申出やオープン ソース通知の一部として案内している専用emailアドレス経由で受け取ります。

コンプライアンスに関する照会への対応

この節では、コンプライアンスに関する照会への対応方法について紹介します。図26は、照会を受け取ってからクローズするまでの各段階を説明する、コンプライアンスに関する照会への対応プロセス例を提示します。

図26コンプライアンスに関する照会へ対応するプロセス

確認

コンプライアンスに関する照会を受け取ったら、照会を受け取ったことを伝え、期日を定めて調査を約束するなどの応答をすぐに行うべきです。

照会者の身元と動機を理解し、主張が正当で正確なものでその時点で意味のあるものかを確認するのは重要です。照会者がライセンスを十分に理解しておらず、誤った仮定で照会を提出することがしばしばあることを理解します。照会が情報を欠いている時には、追加で次のような確認を要求します。

. 影響のある製品やサービスや、該当するコードの名前違反があると信じる理由プロジェクト コードと違反状態にあるライセンスの名前プロジェクト サイトへのリンク

通知

照会者との率直な対話を維持することが推奨されます。常に、自分たちのオープン ソース コンプライアンス プラクティスを示し、コンプライアンスに対する長年の誠実な取り組みを行動によって示します。照会者に自社のコンプライアンス手続きとプラクティスを伝え、照会された事項を調査することを確約します。提示可能になったところで、内部調査に関する最新情報を伝えることは良いことです。

調査

この段階では、報告済みの申し立て案件を調査して、問題となっているコンポーネントに関するコンプライアンス記録を参照し、レビューし、コンプライアンス記録と照会とを比較するべきです。

報告

許容できる期間内で内部調査の結論を出して発見された事項を内部記録に残した後、照会者に結果を伝える必要があります。

照会のクローズ

コンプライアンスに関する照会が誤った警告であった場合には、（照会者に結論を伝える以外には）特に何もしないでコンプライアンス チケットをクローズすることができます。

矯正

調査がコンプライアンス課題を明らかにした場合には、照会者に対し、製品やサービスをコンプライアンス遵守の状態に戻すために必要な手順を全て実行することと、これらの作業を完了するのに予想される日程を明確にして、事実を伝えるべきです。協力的で誠意をもって照会者と一緒に課題を解決するのが、担当者の責任です。適用されているライセンスに基づく義務を理解していることを示し、いつまでにどのようにして義務を満足するかを伝える必要があります。and when . you will meet the obligations.

問題を解決したら、紹介者にすぐに伝え、解決策を検証するために来てもらうべきです。

改善

コンプライアンス課題があった場合には、OSRBを招集して、事例を議論し、どのようにしてこのコンプライアンス違反が生じたかを学び、そのような誤りが再び生じないように、既存のプロセスとプラクティスを改善するべきです。

一般的な考察

. 全ての照会は、正式な照会として扱います。照会者とのやりとりの中で開示する情報は、一般に開示する可能性があるという前提で作業をします。

. オープン ソース コンプライアンスに対して努力することは、ライセンス強制を受けた時にいかに役立ち、自社プロセスをいかに改善するかを考えてみて下さい。

第8章

その他のコンプライアンス関連プラクティス

この章は、実際のコンプライアンス プロセスの範囲外ではありますが、コンプライアンスのベスト プラクティスや様々な考察に光を当てます。

従業員の評価

技術面やコンプライアンス強制に関連して、全ての企業が直面する4つの挑戦があります。

. 技術者が利用したいオープン ソース コンポーネント毎に一貫して要求フォームを確実に記入するようにします。コンプライアンス チケットに対して適時に応答するように、技術者に要求します。OSRBによって定められたガイドラインに従って技術者が行動していることを検証します。

. 組織内のオープン ソース コンプライアンスに関するトレーニングを技術者が受けるように義務付けます。

これらの4つの挑戦に直面した企業をサポートするのに効果的であったプラクティスは、従業員の実績評価の一部としてオープン ソースとコンプライアンス評価項目を含めることです。結果として、従業員のボーナスの一部は、コンプライアンス ポリシーと手順に彼らが従った程度によって決まります。レビューは、従業員が以下の項目を実行したかを評価します。

. 利用するオープン ソース コンポーネント毎にOSRBフォームを記入する。大きな遅延なしにコンプライアンス チケットに応答する。マネージャによって設定された期限内にオープン ソースとコンプライアンスに関するトレーニングを修了する。OSRBが制定したガイドラインの範囲内でオープン ソースを利用し、コンプライアンス違反を起こさない。

逆に、コンプライアンスを従業員の実績評価として利用するためには、OSRBは各担当者の以下の点を追跡しなければなりません。

. ソフトウェアBOMに含まれているが、承認を受けていないコンポーネントコンプライアンス チケットへの応答時間トレーニングコース修了経営チームへ報告されたコンプライアンス違反

ウェブ ポータル

いくつかの企業は、社内向け、社外向けのオープン ソース ウェブ ポータルを運営しています。社内向けポータルは、コンプライアンス ポリシーやガイドライン、トレーニング教材、通知、関連するメーリング リストなどを提供しています。社外向けポータルは、ライセンス義務を履行する形で、利用しているオープン ソース パッケージのソース コードを一貫した方法で提供します。

意思伝達

意思の伝達に関する最も重要で唯一の推奨事項は、社内にオープンソースに関連する企業目標や懸念事項を説明するか、社外のコミュニティ参加者に対するかに関わらず、明確で一貫性を持つことです。explaining company goals and concerns around open source, or externally . facing community participants. コミュニティとの接点となるサイトを持つことは、コンプライアンスに関する照会に応答する時に特に重要になります。

トレーニング

オープン ソースとコンプライアンスに関するトレーニングの目標は、オープン ソース ポリシーと戦略についての意識を高め、オープン ソース ライセンスの課題と事実について共通理解を形成することです。トレーニングは、製品にオープン ソースを統合することによるビジネスリスク、法的リスクも扱います。また、組織のコンプライアンス ポリシーやプロセスを広めて推進し、コンプライアンス文化を促進する手段でもあります。

公式と非公式のトレーニング方法があります。公式の方法は、修了するために従業員は試験に合格する必要がある、インストラクターが担当するトレーニングコースを含みます。非公式の方法は、ウェブでのトレーニング、ブラウン バッグ セミナー、新規雇用従業員へのオリエンテーションの一部としての説明などを含みます。

非公式トレーニング

ブラウン バッグ セミナー

ブラウン バッグ セミナーは、企業従業員（法務担当者、オープン ソース エキスパート、コンプライアンス オフィサー等）や招待スピーカ（広く行われているのは著名なオープン ソース開発者）による、昼食時の講演会です。これらのセミナーの目標は、製品やソフトウェア スタックに統合されているオープン ソースの様々な面に関して説明して議論を引き出すことです。これらのセッションは、企業のコンプライアンス プログラム、ポリシー、そしてプロセスに関する議論も含みます。

新規従業員へのオリエンテーション

いくつかの例では、コンプライアンス オフィサーが、企業のコンプライアンスに関する努力や規則、ポリシー、そしてプロセスをオリエンテーションの一部として新規従業員に説明します。初日に、新規従業員は、オープン ソースとコンプライアンスに関する30分のトレーニングを受けます。結果として、新規従業員は、社内で誰がその内容のエキスパートであるか、どういう社内イントラネットがあるか、オープン ソースとコンプライアンスに関するトレーニングがどのように登録されるかなど、必要な情報を受け取ります。

公式トレーニング

組織の規模や、オープン ソースが商品に使われている範囲にもよりますが、組織は、オープン ソースに携わる従業員が公式な講師の教えるコースを受講し、その領域での習熟度のテストを受けるように命じることができます。

ソース コード変更に関する考察

既存のソース コードを変更する基本ルールを確立するために、平易で法務用語を使わない言葉で表現した、内部利用目的のガイドラインを発行することを強く勧めます。例

. プロプライエタリを残すソース コード変更は、特に派生物への義務を持つような（GPL, LGPL等の）オープン ソース パッケージ内で行っていはいけません。. プロプライエタリ ソース コードは、派生物への義務を持つようなオープン ソース ライブラリにリンクしてはいけません。企業では、通常、それらを実行するには正式なOSRB承認を必要とします。. ソース コードに加えられるいかなる変更も、オープン ソース ライセンスに適合して頒布前に文書化されることを確実にします。. オープン ソース モジュールへの全ての変更は、モジュールの修正履歴（変更ログファイル）で把握されるようにします。

通知に関する考察

オープン ソースを使う時に重要な義務の一つは、著作権、帰属、ライセンス情報、そして書面による申出（GPL/LGPLで許諾されたソース コード）などの明確で正確な文書作成を確実にすることです。これらの文書化の義務の全体は、しばしばオープン ソース通知と呼ばれます。

提供物にオープン ソースを利用している企業は、著作権の帰属を全て表示し、ほとんどの場合、製品やサービスに含まれているオープン ソース ソフトウェアのライセンス全文を記載することで、オープン ソース利用を知らせなければなりません。従って、企業は、出荷する全ての製品や提供する全てのサービスの文書に、著作権、帰属、そしてライセンス通知を記載することで、文書化の義務を満たさなければなりません。

文書化義務の要求を満たす2つの主要な選択肢があります。

. 製品自体にオープン ソース通知を表示します。これは、ユーザーと対話してライセンス情報を引き出すか、ライセンス情報を表示するかできるユーザー インタフェースを製品が持っている場合には、実行可能な選択肢です。この選択肢の例は、携帯電話やタブレットです。. 製品マニュアルや、製品に付属する文書に、オープン ソース通知を含めます。

いくつかの企業は、ウェブサイト（一つの選択肢ではありますが、頻繁に採用され、維持にも手がかかりません。基本的にはウェブサイト上に通知ファイルを置くだけです。）上で通知を維持しながら、可能な時には両方の選択肢を選びます。basically just hosting the notices file on the website). 通知に関する考察から得られる重要なことは、製品出荷やサービス開始前に、全てのオープン ソース通知に対する要求が満たされることを、確実にしなければならないということです。

頒布に関する考察

一般的に言って、企業は、製品出荷前にオープン ソース頒布に関する義務を果たした状態にできることを望みます。コンプライアンス プラクティスを開発サイクルで徹底的に実施することによって、頒布に関する考察はとても単純で簡素なものになります。

利用に関する考察

以下の節では、完全にコンプライアンスに適合したオープン ソース利用についての、考察と警告を示します。

BoMをクリーンにします。

入るソフトウェアが、利用宣言されていないオープン ソースを含んでいないことを確実にします。供給者から受け取る時に、いつもソースコードを監査します。代わりの方法としては、ソフトウェア供給者が供給するコードの監査報告を必ず提供しなければならないという企業ポリシーを制定します。

それぞれのオープン ソース コンポーネントに対するOSRBフォーム

利用するそれぞれのオープン ソース コンポーネントに対してOSRB利用要求フォームを記入します。明白なOSRB許可がないオープン ソースを利用するのは避けます。

M&Aによるリスクの理解

利用されているオープン ソース コードと関連する事項は、企業間の取引に先立って実施される資産監査対象の一部であることを理解します。

使用しなくなったオープン ソース パッケージ

承認済みのオープン ソース パッケージが利用されなくなったならば、技術者はOSRBに連絡してオープン ソースリストを更新するように通知しなければなりません。さもなければ、OSRBが、BOM差分ツールを実行する際にもはや使われなくなっているパッケージを見つけるでしょう。

大きなソース コード変更

承認済みのパッケージが大きな変更を受けた時には、OSRBにソースコードを再スキャンするように通知します。さもなければ、OSRBがBOM差分ツールを実行する際にパッケージが変更されていることを発見するでしょう。設計や実装での大きな変更は、アーキテクチャー、API、ユースケースにインパクトを与えますし、ある場合にはコンプライアンス面でもインパクトがあります。

参考オリジナル ソース コード

ダウンロードしたパッケージを保存するのに加えて、オープン ソース パッケージをダウンロードしたURLも文書化します。

オープン ソースの新しいバージョンへの更新

同じオープン ソース コンポーネントの新しいバージョンがレビューされ承認されることを確実にします。バージョン更新の間でライセンス変更が起きることがありますので、オープン ソース パッケージのバージョンを更新する時には、新しいバージョンのライセンスが前のバージョンから変更されていないことを確認します。もしライセンスが変わっていたら、コンプライアンス記録を更新して、新しいライセンスが問題を起こさないように、OSRBに相談します。

コンプライアンス 検証の黄金律

コンプライアンスは製品ごとサービスごとに検証されます。というのは、オープン ソース パッケージは、ある条件での利用を承認されたのであり、2次利用について承認されたわけではないからです。

コピー／ペースト

事前のOSRB承認なしでの、ソース コード断片の利用や、オープン ソース コードをプロプライエタリやサード パーティ ソースコードへ（その逆も）コピー／ペーストすることを避けます。これらの行動は、コンプライアンスに深く関わります。

ソース コードの異なるライセンスとの結合

多くのオープン ソース ライセンスは互いに両立性を持っていないので、派生物に異なるオープン ソース ライセンスを結合することを避けます。このトピックに関して、法務担当からのサポートを受けることを強く勧めます。

ソース コード コメント

ソース コードに不適切なコメントを残さないようにします。（個人的なコメント、商品コード名、競合他社名等）

既存ライセンス情報

既存の著作権やライセンスの情報をオープン ソース コンポーネントから削除あるいは変更しないようにします。全ての著作権やライセンスの情報は、ライセンスが変更を許していると完全に確信できるとき以外は、オープン ソース コンポーネントでそのままの状態にしておきます。

帰属についての考察

製品にオープン ソースを組み込んでいる企業は、エンド ユーザーに帰属情報を提供する必要があります。この節では、オープン ソースの帰属に関する義務をどのように達成するかについてのガイドラインを示します。

帰属タイプ

オープン ソースの帰属要求は、ライセンスによって異なりますが、一般的に4つのカテゴリに分けられます。

ライセンス全文

ライセンス全文の逐語的コピーが、ほとんど全てのオープン ソース ライセンスで要求されます。

著作権表記

著作権表記の逐語的コピーが、多くのオープン ソース ライセンスで要求されます。

謝辞表記

いくつかのオープン ソース ライセンスは、明示的に著者の帰属を要求します。ほとんどの場合、オープン ソース プロジェクトは、貢献者のリストを含むAUTHORSと呼ばれるファイルを含んでいますので、帰属表記の一部としてこの情報を使うことができます。

ソース コード入手についての情報

ソース コード再頒布義務を持つほとんどのライセンスは、製品に付随するソース コード提供か、ソース コードの入手方法を記述した書面による申出かを要求します。GPL と LGPL は、このカテゴリーのライセンスの例です。

帰属の提示

オープン ソースを含むあるいは利用している製品やサービスに関していうと、帰属は、（製品マニュアル等の）印刷されたユーザー文書や、CDまたはウェブサイトからのダウンロードなど、印刷または電子形式で頒布されなくてはなりません。もし、製品やサービスがグラフィカル ユーザー インターフェイスやコマンド ライン インターフェイスを持っているならば、帰属をそのUI経由で表示することも選択肢の一つです。携帯電話での通信での（OTA）製品アップデートに関していうと、製品アップデートが新しいあるいは更新されたオープン ソース コンポーネントを含むのであれば、帰属は、更新されなければなりません。

特定のライセンス義務

「エンド ユーザーが利用可能な文書にライセンスのコピーを入れなければならない」

問題となっているオープン ソース コンポーネントのライセンスは、このオープン ソースを利用する全ての製品のユーザー文書に含まれていなければなりません。

推奨事項

. 携帯電話やタブレットなど、いくつかの例では、製造会社は、ウェブ ブラウザやPDFビューアを使って（ライセンス文は、HTMLやPDF形式で機器上で利用可能です）、実際の機器上で通知を提示することができます。. ユーザーがアクセス可能なファイルシステムを有する製品では、ライセンスは、意味が分かるようするために、また、オープン ソースのライセンスファイル名と同じようにするために、LICENSEというファイル名でファイルシステムに含まれていることを推奨します。

. 製品アップデートに関して、ライセンス情報もまたアップデートされなければなりません。例えば、新しいソフトウェア リリースが入手可能になった時、アップデートされたリリースは、新しいリリースで導入されたオープン ソースの全ての変更を反映している、アップデートされたライセンス情報ファイルを含んでいなければなりません。変更は、以下を含むかもしれません：新しいオープン ソース評価が下がった／使われなくなったオープン ソース新しいバージョンにアップグレードされたオープン ソース。帰属／著作権表記の更新を必要とするかもしれません。まれにライセンスの更新を必要とすることもあります。

「エンド ユーザーが利用可能な文書に著作権表記を入れなければならない」

問題となっているオープン ソース コンポーネントのライセンスは、エンド ユーザーが利用可能な製品文書中に著作権表記を必要とするかもしれません。

推奨事項

. 全ての製品に関して、著作権情報は、（ユーザーマニュアルのような）印刷物に含まれていなければなりません。

. グラフィカル ユーザー インタフェースを有する場合には、エンド ユーザーは「製品について」や「ライセンス」の画面から著作権情報を参照することができるようにすべきです。. 製品が、ユーザーが利用可能なファイル システムを有している場合には、著作権情報は、例えば製品で利用されている全オープン ソースに対する全著作権表記は、ファイル システムに含まれているべきです。

. 製品アップデートに関して、著作権情報もまたアップデートされなければなりません。

「広告資料は、特別な謝辞が必要になるかもしれません。」

オリジナルのBSDライセンスに由来する広告文は、以下のように書かれています。

All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed by the University of California, Berkeley and its contributors.

適用可能ならば、全てのマーケティングや広告の資料（ウェブや雑誌、新聞、チラシ等）は謝辞を表示しなければなりません。

一般的なガイドライン

オープン ソース プロジェクト名を推奨に利用しない、自分たちが行ったソース コード変更に印をつける、オリジナルのライセンス、著作権、帰属情報を保持する、などオープン ソース ライセンスを応用するガイドラインのいくつかについては既に良く知っているかもしれません。以下の節では、これらのガイドラインの細かな議論を発展させます。

推奨や推進に利用しない

オープン ソース プロジェクト、著者、貢献者などの名前を、事前に文書による許諾を受けないで、マーケティング、広告や文書（紙媒体、電子媒体、ウェブなど）に利用することはできません。

ソース コード変更の印

変更したオープン ソース コードを再頒布するとき、既存の著作権行をそのまま保持しながら、自分の変更箇所へは、著作権行（会社、年）によって印をつける必要があります。

ある会社は別のアプローチを取りました。オリジナルのオープン ソース コードと共に、そのコードに適用させる自社の貢献修正ファイルを提供しました。このアプローチに従えば、会社の修正は、オリジナル ソース コードと明らかに分離されます。

オリジナルのライセンス、著作権、帰属情報を維持する

オープン ソース コードを再頒布する時にはいつでも、変更が伴っても伴わなくても、オリジナルのライセンス情報、著作権行、やその他の帰属情報を維持しなければいけません。

ソース コード コメント

個人的なコメント、製品コード名、競合社への言及など、不適切なコメントをソース コードに残してはいけません。

既存ライセンス情報

既存のオープン ソースライセンス著作権や他のライセンス情報を、利用するオープン ソース コンポーネントから取り除いたり、他のいかなる方法でも手を入れてはいけません。全ての著作権とライセンス情報は、全てのオープン ソース コンポーネントの中で触らずそのまま残しておく必要があります。

第9章

オープン ソース法務サポートを拡大させる

オープン ソース コンプライアンスは、しばしば、法務的な問題というよりも運用や物流的な問題です。コンプライアンスを達成するためには、適切なポリシーやプロセス、トレーニング、ツール、著作権者の著作権を尊重し、ライセンス義務を遵守し、組織や顧客や供給者の知的財産を守りながら、オープン ソースを効果的に利用しオープン ソース プロジェクトやコミュニティに貢献する体制が構築できる適切な担当者の配置などが必要です。

しかしながら、法務担当は、オープン ソース コンプライアンス プログラムや適切なコンプライアンスを確実にするもっとも重要なコアチームをサポートする不可欠な役割を果たします。この章では、オープン ソース コンプライアンスを確実にする法務担当の役割を詳細に見て、法務担当がソフトウェア開発チームに与えることができる実際的なアドバイスを提供します。そういう実際的なアドバイスは、ソフトウェア開発者が、法務担当に頼らなくてもできる、細かな問題に対する毎日の判断を可能にします。

実際的な法務アドバイス

法務担当からソフトウェア開発者に向けた実際的なアドバイスは、以下を含むかもしれません

. ライセンス プレーブック：ソフトウェア開発者を意図して書かれた、オープン ソース ライセンスについての簡単に読める要約形式のまとめライセンス両立性マトリックス：ライセンスAがライセンスBと両立性があるか判断するのを助ける表ソフトウェア開発者は、異なるプロジェクトの異なるライセンスにあるコードをマージする際に、そのようなマトリックスを使うことができます。

. ライセンス クラス：異なるライセンスと、これらのライセンスで許諾されたソース コードを利用する際に必要な行動を理解する簡単な方法

. ソフトウェア相互作用法：異なるライセンスで利用可能なソフトウェア コンポーネントがどのように相互作用するか、相互作用の方法は企業のコンプライアンス ポリシーで許可されているかを理解するガイドチェックリスト：開発やコンプライアンスのプロセスの全てのポイントで必要なことは何かを覚えておくための、一貫性のある、極めて簡単な方法

以下の節では、これらの5つのアドバイスを確認し、例を示し、これらによって開発者がオープン ソースに関わる時にどのように助けになるかを議論します。

ライセンス プレーブック

ライセンス プレーブックは、広く使われているオープン ソースについての要約です。ライセンスの許諾、制約、義務、特許への影響、その他、このライセンスに関する簡単に理解できる情報が書かれています。ライセンス プレーブックは、法務担当へ来る基本的な質問の数を最小化し、これらのライセンスに関する法務的な情報を即座に開発者に提供します。

図27（次ページ）は、GPL v2に関するライセンス プレーブックの例を示します。このプレーブックは、説明目的で書かれたものであり、その中身は確実と考えないように注意して下さい

図27GPL v2 ライセンス プレーブック例（説明目的のみに使用）

ライセンス両立性マトリックス

ライセンス両立性とは、ソフトウェア コンポーネントとそのライセンスが一つ以上の他のコンポーネントとそのライセンスと両立できるかどうか（ライセンスが矛盾を起こさないか）を決めることです。両立性は、また、

二つやそれ以上のライセンス（結合されたアウトライセンス）を結合した作成物に対する適切なライセンスについても言及します。

ライセンス両立性に関する取り組みは、両立しない条件の下に頒布されている様々なオープン ソース ソフトウェア コンポーネントを、ソースやオブジェクト形式で結合する際に、生じます。そのような結合は、純粋に法的な理由から再頒布できないようなソフトウェア コンポーネントの集合、つまり、ライセンス キメラを作り出します。

両立しないライセンスの例は、Apache version 2ライセンスで頒布されたコードをGNU GPL version 2の（古いGPLライセンスには存在していなかった特許終了と免責に関する事項によって）ソフトウェアと結合しようとするときに見られます。ライセンス両立性の例は、明らかにGPL version 2と両立できる、X11ライセンスのコードを結合する時に見られます。

図28は、異なるライセンスで許諾された複数のソースからなる一つのソース コンポーネントを生成する例を示します。このシナリオでは、ソースは矛盾を抱えることなしにバイナリやオブジェクトファイルに結合できるような両立性のあるライセンス条件を持つことを確認しなければなりません。

図28異なるライセンスで許諾されたソースを一つのバイナリへ結合する

ライセンス両立性は、開発チームが法務担当からの詳細なガイドラインを必要とするもので、自分たちだけで結論を出すべきではない分野です。そのようなガイドラインは、一般的なほとんどのライセンスをカバーするライセンス両立性マトリックスによって得られます。マトリックスの例を、表7に示します。

表7ライセンス両立性マトリックスの例（説明目的のみに使用）

License-A

License-B

License-C

License-D

License-E

License-F

License-G

License-A

a

a

a

License-B

a

License-C

a

License-D

a

a

a

License-E

a

License-F

a

License-G

a

a

開発チームは、異なるライセンスで許諾されたコードを結合する必要がある時には、問題となっている結合したソフトウェア コンポーネントがライセンス的な矛盾を発生させるかを確認するために、このマトリックスを参照できます。マトリックスに含まれていない新しいライセンスに出会った時には、そのライセンスは法務担当によって分析されなければなりません。法務担当は、分析結果に基づいて表の更新をするべきです。

ライセンス分類

法務担当が受ける質問数を減らし、ライセンスとコンプライアンス プロセス教育を増やすために、いくつかの会社では製品に使用する最もよく利用するライセンスをいくつかのカテゴリに分類しています。図29（次ページ）は、最もよく使用するライセンスを4つのカテゴリに分類している、ライセンス分類の例です。

事前承認ライセンス

許容型オープン ソース ライセンスは、しばしばこのカテゴリに分類されます。これらのライセンスで許諾されたソース コードは、開発者が、マネージャや法務担当への承認プロセスを通すことなく、利用が事前承認されています。そのような事前承認は、開発者に、全ての通知を抜き取って、文書チームへ送付するように要求します。

マネージャ承認を必要とするライセンス

通知に関する義務（ライセンス文、帰属通知、著作権通知などの表記）に加えて、ソース コード変更を開示する義務があるので、これらのライセンスで許諾されたコンポーネントでは、マネージャによる承認が要求されます。

図29ライセンスカテゴリの例（説明目的にのみ使用）

法務担当による承認を必要とするライセンス

これらのライセンスで許諾されたソース コードは、法務によるレビューを承認を必要とします。これは、通常、特許に関する条項を含むライセンスに適用されます。

禁止されたライセンス

いくつかの企業では、特定のライセンスには「不許可」のフラグを付けます。企業ポリシーによって利用が許可されていません。

ライセンス分類はいかに役に立つか？

上記のライセンス カテゴリは、これらのライセンスで許諾されたコードを統合する際に、開発者が適切な一連の行動を簡単に知ることができるように分類する一つの方法です。更に、ライセンスとなすべき行動との関連付けを簡単に作成することができます。表8は、開発者が様々なライセンスに関連した適切な行動を思い出すのに簡単な一つの方法です。

表8ライセンス分類のための簡単なハウツー

どのライセンス

行動

License A

問題なく利用

License E

マネージャの承認をもらう

License I

法務に相談する

License M

このソース コードは使えない

Other

一連の行動についてはマネージャに質問する

これらの異なるシナリオは、説明目的のみに提示されています。自分の組織ポリシーやガイドラインに従って、異なる行動を割り当てるような異なる分類モデルを作成することも可能です。

ソフトウェア相互作用法

コンプライアンス プロセスの一部として、通常、アーキテクチャー レビューがあります。その目的は、得的のソフトウェア コンポーネントが他のソフトウェア コンポーネントとどのように相互作用するかと、相互作用の方法を理解することです。アーキテクチャー レビューは、以下を特定します。

. （そのまま、または変更して利用される）オープン ソースからなるコンポーネントプロプライエタリ コンポーネント

. サード パーティ プロバイダから提供されたものに由来するコンポーネント

. コンポーネントの依存状態共有ヘッダ ファイルの利用コンポーネントの実行時のコンテキスト(Kernel/dirver/modules, middleware, libraries, applications, etc.)

. APIを超えたコンポーネント間依存関係(s/w buses, IPCs, web APIs, etc.). 言語間の結合

表9と10（次ページ）は、法務担当がソフトウェア開発者に提供できる追加情報を示します。この表は、どのライセンスが、企業ポリシーを考慮した上で、他のライセンスと動的静的にリンク可能であるかを示します。

表9動的リンク マトリックス例

動的リンクできるか

License-A

License-B

License-C

License-D

License-A

a

a

a

a

License-B

a

a

License-C

a

a

License-D

a

「事前承認必要」

a

例えば、表9で、ライセンスBで許諾されたソース コードは、ライセンスDで許諾されたソース コードと動的にリンクすることが可能です。しかしながら、ライセンスCで許諾されたソース コードは、ライセンスBで許諾されたソース コードと動的にリンクすることはできません。また、リンクは、ライセンス間で常に相互に成り立つとは限らないに注意して下さい。

同様に、表10で、ライセンスAで許諾されたソース コードは、ライセンスCで許諾されたソース コードに静的にリンク可能です。しかしながら、ライセンスAで許諾されたソース コードは、ライセンスBで許諾されたソース コードに静的にリンクすることはできません。いくつかのリンクの組み合わせは、ケース バイ ケースで許可されます。そのため、「事前承認必要」と注意が書かれています。

表10静的リンク マトリックスの例

静的リンクできるか

License-A

License-B

License-C

License-D

License-A

a

a

License-B

a

「事前承認必要」

License-C

a

a

License-D

「事前承認必要」

a

アーキテクチャー レビューによってリンクに関する課題（リンク マトリックスで示される企業ポリシーに従わない動的リンク静的リンクなど）が発見されたとき、アーキテクチャー レビューを推進した責任者（通常はコンプライアンス オフィサー）は、ソフトウェア コンポーネントに責任を持つソフトウェア開発者に通知して、改善を要求します。

チェックリスト

ほとんどの企業は、開発プロセスの全てのメジャーなマイルストンで利用するチェックリストを確立しています。オープン ソース コンプライアンスで利用する時には、いくつかのチェックリストを作り上げ、製品のソース コード リポジトリへ外部の新しいオープン ソース コードを入れる前にチェックリストを使います。一つの例が、外部向けウェブサイトにソース コードを置く前に利用される、以下のチェックリストです。

. 全てのソース コード コンポーネントは、対応するコンプライアンス チケットを持っています。

. 全てのコンプライアンス チケットは、技術担当と法務担当に承認されています。

. 全てのコンプライアンス チケットは、付属している未解決サブタスクがクリアされています。

. 全てのソフトウェア コンポーネントの通知は、文書チームへ送付され、製品文書に含まれています。

. 法務担当は、書面による申出とコンプライアンス文書全体を承認しています。

. ソース コード パッケージは、準備され、標準開発マシン上でコンパイルできるかテストされます。

. 提供されるソース コードは、完結しており、製品に搭載されるバイナリと一致します。

そのようなチェックリストは、誤る確率を最小化し、オープン ソース管理に携わる全ての人がプロセスの次の段階へ進む前に何をすべきかを気づくようにさせます。

結論

ソフトウェア開発者は、統合し利用する様々なオープン ソース コンポーネントのライセンスに関しての教育を受ける必要があります。法務担当が実際的な方法で教育を実施するようにすることは、とても役に立ちます。ソフトウェア開発者が、法務に関連する日々の質問に答えてくれる文書化された実際的なアドバイスに、アクセスできるからです。この実際的なアドバイスは、通常以下の点を中心に展開します。

. オープン ソース コンポーネントをプロプライエタリやサード パーティ ソース コードへの挿入、またはその逆。オープン ソース コンポーネントをプロプライエタリやサード パーティ ソース コードにリンク、またはその逆。. 様々なソフトウェア コンポーネント間（プロプライエタリ、サード パーティ、オープン ソース）の相互作用法オープン ソース コンポーネントを利用する際に満足しなければならないライセンス義務

オープン ソース コンプライアンスは、コンプライアンス プログラムを確立し、コンプライアンス ポリシーとプロセスを作成し、実行する担当者を確立し、コンプライアンスの自動化の面で助けとなるツールをチームが使えるようにすれば、容易に達成できます。

著者について

イブラヒム ハダッド（Ph.D.） は、Samsung Electronics Co. Ltd.（韓国）のR&Dに関する100%子会社であるSamsung Research AmericaのR&D担当副社長で、オープン ソース グループ長です。彼は、Samsungのオープン ソース戦略立案と実行、社内外との共同R&Dプロジェクト、重要オープン ソース開発プロジェクトへの参画に責任を持っており、様々なオープン ソース財団とオープン標準組織でSamsungの代表を務めています。Samsungに加わる前、ハダッドはLinux Foundationの経営チームにおいて技術と法務コンプライアンス プロジェクトとイニシアティブの責任者でした。ハダッドは、キャリアをEricsson Researchで始めました。そこで彼は、5年間ワイヤレスIPネットワークに関する先端研究と、通信業品質環境へのLinuxとオープン ソース ソフトウェアの導入に携わりました。その後、彼はMotorolaにオープン ソース技術グループの技術担当役員として加わり、Motorolaのオープン ソースでのイニシアティブに貢献しました。Motorolaを離れた後、彼は、Palmにおいて、webOS オープン ソース戦略とコンプライアンスに責任を持つオープン ソース担当役員としてオープン ソース部門を指揮しました。後に彼は、webOSをオープン ソース化したopen webOSプロジェクトで、コンサルティングとして、Hewlett Packardを支援しました。

ハダッドは、優秀な成績で計算機科学の博士号をConcordia University (Montreal, Canada)から授与されました。彼は、学士と修士（ともに計算機科学）をLebanese American Universityで取得しています。彼は、Linux Journalの寄稿編集者の一人で、Red Hat LinuxとFedoraに関する2つの本の共著者であり、Linux System Administration、Fedora Linux、Ubuntu Linuxに関する4つの本の技術監修者です。彼は、オープン ソース法務コンプライアンスから、ビジネス戦略や共同開発やイノベーションを推進するR&Dツールとしてのオープン ソース利用に至る話題についての著書と講演で知られています。

ハダッドは、アラビア語、英語、フランス語が堪能です。

Twitter: @IbrahimAtLinux

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/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 およびその他の活動については、http://www.linuxfoundation.org/ を参照してください。