



» オープン コンプライアンス プログラム

Software Package Data Exchange™ 標準フォーマット: 誰にとって必要か

.....
Phil Ocence, VP, Black Duck Software
Kate Stewart, Release Manager, Canonical

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

ソフトウェア コミュニティにおけるオープンソースの役割の増大についての議論は終わりました。2009年5月28日付のエコノミスト紙は、「オープンソースは議論に勝った。将来はプロプライエタリとオープンソースソフトウェアが混じり合った世界になるということを人々は認めている。」と報じています。

成長を続ける大きなアプリケーションの一群は、オープンソースライセンスのもとで利用することができますが、現在開発されているほとんどの商用アプリケーションのコンポーネントにも、オープンソースのコードが使われています。車からハンドセットや発電所に至るまで、ありとあらゆる製品がソフトウェアを使用していることを考えると、オープンソースコードは、ほとんどの産業の無数のサプライチェーンに行き渡っています。

サプライチェーンのどの位置にある企業も、サードパーティコードと同じようにオープンソースを扱う必要性を自覚しつつあります。企業は、さまざまな理由で利用したり配布したりしている製品やソフトウェアに含まれているコンポーネントを認識し、文書化する必要がありますが、その中でもとりわけ、法的義務を確実に理解することが重要です。このため、ソフトウェアパッケージや関連コンテンツの情報を共有するための共通のアプローチを求める声が高まっています。また、情報集約の方法についても、現在、作業が進められています。幸い、新しいワーキンググループが、ソフトウェアパッケージの情報共有に関する最も難しい問題の1つに取り組み始めました。すなわち、「ソフトウェアパッケージとその関連コンテンツ(ライセンスなど)に関する情報の検出と共有」のための協力です。

正しい行動をとる

ソフトウェアライセンスの種類は急増しており、インターネットで自由に使用できるソフトウェアには、約2,000種類のソフトウェアライセンスが存在します。これは、ソフトウェアコンポーネントを再利用して開発の効率化を狙うソフトウェア開発組織や、製品にソフトウェアパッケージを組み込んで再配布する企業にとって、大きな頭痛の種です。Free Beer(無料)ライセンスから、GPL系ライセンス、あるいはApacheやEclipseのようなプラットフォーム別のライセンスまで、膨大な数と種類のライセンスがあるため、企業が自社の製品やアプリケーションに含まれているソフトウェアコンポーネントについて、「正しい行動をとる」ことが難しくなっています。

各ライセンスは、そのソフトウェアの利用および再利用に関する作成者固有の定義を含んでいます。BSDやMITのような寛容なライセンスの場合は簡単です。ソフトウェアを再配布でき、開発者は、コードを改変しても、その改変を一般に公開する必要はありません。一方、再利用や再配布について、さまざまな制約が課されたライセンスもあります。ライセンスの制約の問題を理解しないまま、単純なWeb検索でコードを取得する開発者が存在するのは、本当に困ったことです。

ライセンスコンプライアンス - 正しい行動の第一ステップ

多くの企業は、コードコンポーネントを再利用する際、ライセンスコンプライアンスに関して正しい行動をとろうとしますが、明確なソフトウェアパッケージデータ交換(SPDX™: software package data exchange™)の標準規格がないため、問題が複雑化しています。手作りのスプレッドシートから、FOSSologyのようなフリーソフトウェアオプション、あるいはBlack Duck Suiteのようなエンタープライズクラスのアプリケーションまで、ライセンスコンプライアンスを確実に履行するためのアプローチは数多くありますが、ソフトウェアパッケージ

データ交換の包括的な標準規格は見当たりません。サプライヤーがすべてのデータを列挙しているとしても、彼ら独自のフォーマットや表記法を使用しています。利用者側の企業でも、こうした情報を求める声が高まっていますが、求める側にもその企業の数と同じくらいのさまざまな形式があります。

しかし状況は変化しています。The Linux Foundation の FOSSBazaar Software Package Data Exchange (SPDX™) ワーキンググループがこの活動に取り組みました。この草の根の取り組みにあたり、ソフトウェアベンダー、システムベンダー、ツールベンダー、さまざまな標準化組織・財団、システムインテグレーターなど20を超える団体から、SPDX™ フォーマット作成への賛同が得られました。

SPDX™ フォーマットに関心があるのは、誰でしょうか？

それは、ソフトウェアライセンスコンプライアンスへの標準的アプローチに関心があるソフトウェア開発マネージャーや、法律家だけではありません。ソフトウェアパッケージを使用したり、配布したりするすべての企業が、その成果に関心を持っています。IT マネージャーも、開発者が記述したコードに何が入っているかを知りたいソフトウェア開発マネージャーも、ソフトウェアパッケージを購入している企業の上層部も、みな関心を持っています。また、ソフトウェアを開発している組織、特に、世界中に分散している開発チームが協力し合い、ライセンスや義務の視認性を必要としているような組織も関心を持っています。関心が高まっている理由の1つに、サプライヤーに部品構成表 (BoM) の提供を求める企業が増えていることが挙げられます。BoM は、パッケージにどのようなソフトウェアコンポーネントが含まれているか、どのようなライセンスが適用されているかを明確に示します。つまり、企業は、正しい行動をとるだけでは不十分なのです。経験豊かなユーザーは、ライセンス違反のリスクを低減するための証明を求めています。サプライヤーは、独自のフォーマットを使用する各メーカーの要求に応えるより、オープンソース開示用の標準フォーマットを使える方がよいでしょう。

影響を受ける関係者が多いため、SPDX™ ワーキンググループは、次のような簡単なチャーターを作成しました。

企業や組織が、ソフトウェアパッケージと関連コンテンツのライセンスやコンポーネント情報 (メタデータ) を共有できるように、一連のデータ交換標準規格を作成することにより、ライセンスやその他のポリシーのコンプライアンスを促進する。

このように「ソフトウェアパッケージと関連コンテンツに関する情報を簡単に検出、収集、および共有するために、共通の SPDX™ フォーマットを作成する」ことで、時間の短縮、ライセンスデータ収集の精度の向上、およびソフトウェアライセンス順守の簡略化が約束されます。



問題のスコープ

多くの企業は、確立されたプラクティスによって、ソフトウェアのリリースと配布を管理しています。しかしソフトウェアの再利用は、新たな問題を招いています。プロダクト マネージャー、開発マネージャー、上級管理者層などが把握することなく、開発されているソフトウェア製品にさまざまな開発元を持つコードが混在し、ソフトウェアのサプライチェーンが複雑化しているのです。

コンポーネント単位で考えることで、問題のスコープがはっきりします。

- ソフトウェア群を配布する前に、組み込まれる各パッケージの内容をレビューして、再配布されるコードのすべてのライセンスを確実に順守する必要があります。
- 製品のサプライチェーンは、開発者が「ソフトウェアの血統書」を作成し、これに誤用防止とリスク低減のための情報を含めることを要求する。
- ソフトウェア パッケージで宣言されているライセンスは、パッケージ内の個々のファイルのライセンスと常に一致するわけではない。
- 実際に、典型的なソフトウェア パッケージでも、異なるライセンスを持つ何千ものファイルで構成されているものがある。
- コードを再利用すると、両立性のない各種のライセンスでカバーされたコードの断片やコンポーネントが取り込まれることがある。

このため、業界は、ソフトウェア パッケージの法的順守の目的にかなった BoM を参照する共通の方法を必要としています。ソフトウェア パッケージに含まれるライセンス情報を、効率的かつ正確に交換するための標準的方法が必要です。

この問題の緊急性に加えて、複数のバージョンを持つソフトウェア パッケージには、複雑な相互依存関係があることも考慮する必要があります。ソフトウェアが時間とともに進化するにつれ、異なるライセンスを持つ複数の新しいコード コンポーネントが、ともすればあらゆるソフトウェア レベルで組み込まれる可能性があります。コードの再利用は、開発を高速化するための優れた方法ですが、時が経つうちにライセンスの矛盾を招く恐れがあります。とにかく、約 2,000 種類のライセンスが存在する中で、すべてのライセンスに両立性があるわけではないことは明らかです。

事実だけが重要

通常、ソフトウェア ライセンスは開発者の意図を伝えるものですが、SPDX™ 活動は事実を伝えることに重点を置いています。SPDX™ の活動は、「すべてのソフトウェア パッケージに、定義されたフォーマットのファイルを添付する」ことにより、問題を解決しようとするものです。ライセンス情報を企業間で簡単に交換するために、3つの区分域を設けています。それは、識別のための区分、概要情報を提供する区分、およびソフトウェア パッケージのファイル別情報を提供する区分です。それぞれの区分は、当該ソフトウェア パッケージの実情を反映します。SPDX™ ワーキング グループは、個々のライセンスを、たとえば「BSD ライクな」ライセンスなどと分類することによって、法的判断を適用しようというわけではありません。

SPDX™ 標準規格のバージョン 1 では、まずパッケージを識別するための区分のフォーマットを、続いて、パッケージの内容を表すための区分のフォーマットを、そして最後にパッケージを構成するファイルについて説明する区分のフォーマットを提供しています。

SPDX™ の仕様書では、ソフトウェア パッケージの識別情報 (メタデータ) に対応するものとして、次のようなものを挙げています。

- 使用している SPDX™ 仕様書のバージョン
- 一意の識別子
- そのソフトウェア パッケージに関連付けられた一意の識別子を生成する暗号ハッシュ アルゴリズム
- その情報がどのように生成されたか
- SPDX™ 仕様書は、手動による、あるいは視覚的なレビュー (誰が、いつ) の実績を表現する方法を定義しています
- ライセンス情報抽出のために使用したツール (ID、バージョン、いつ)
- 独立監査の実績
- 複数の人物による「サインオフ/レビュー」プロセスの可能性

また、SPDX™ 仕様書では、ソフトウェア パッケージの内容に関する概要情報として、次のようなものを挙げています。

- 正式名
- パッケージ名
- ダウンロード場所
- 宣言されているライセンス
- 著作権情報と日付

最後に、SPDX™ 仕様書では、ソフトウェア パッケージのファイル別プロパティに関する情報として、次のようなものを挙げています。

- ファイル名 (サブディレクトリも)
- ファイル タイプ (ソースかバイナリか)
- 各ファイルに適用されるライセンス (ファイルから抽出)
- 著作権所有者 (掲載があれば)
- 著作権発生日 (掲載があれば)

同ワーキング グループは、この仕様書のライセンス指向性を高めるために、標準化されたライセンス リファレンスの提供に取り組んでいます。正しいライセンスの正しい版を正確に参照することは、想像以上に難しいものです。仕様には、以下のものが含まれます。

- ライセンス名
- 共通のオープンソース ライセンスに対応する一意の識別子
- 非標準ライセンスを取り扱うためのメカニズム

SPDX™ は今どこにあるか？

一連のソフトウェア パッケージ データ交換 (software package data exchange™) 標準規格を作成し、ソフトウェア開発組織や、システム/ツール ベンダーや、オープンソース プロジェクトのために、曖昧さを排除する必要があるのは明らかです。そしてそれは、ベストプラクティス、使用事例、プロトタイプ ツールなどによって裏付けられ、さまざまな組織で使用できる必要があります。

当初より、SPDX™ ワーキング グループは、2010 年の第 4 四半期までに、ライセンス情報のファイルに関するフォーマットを定義する、という大きな目標を掲げていました。作業は、直接ミーティング、プロジェクトの Wiki、および <http://spdx.org> サイトで進行しています。The Linux Foundation は、LinuxCon から開始されたこの取り組みを当初から支援してきましたが、The Linux Foundation のオープンソース コンプライアンス プログラムにより、さらに連携が深まりました。実際に SPDX™ は、このプログラムの大きな柱の 1 つになりました。このため、このオープンソース コンプライアンス プログラムの発表に合わせて、バージョン 1.0 のベータ版を公開しました。

今後の予定

バージョン 1.0 のベータ版は、開始点にすぎません。実地試験は行いましたが、まだ一般利用されていません。このため、同ワーキンググループは実用化を推し進め、重要なフィードバックを改訂版に反映させて行きます。次のステップは、ワーキンググループが、SPDX™ レポート作成の対象となる重要プロジェクトのリストを作成し、考えられるあらゆる手法を用いてそれらを実行することです。まずは、当グループが、このライブテストを始めますが、私たちは、グループ以外の人々にも関わってもらうよう働きかけます。SPDX™ データの文法チェックや読み出しツールなどの開発支援ツールも必要でしょう。

このテストによって、仕様の曖昧さや欠陥がわかり、リリースに反映されて、バージョン 2.0 の基本方針が決定します。現在の私たちには、公に働きかける勢い、構造、基盤がそろっています。バージョン 1.0 は、この活動の参加者全員に公開されましたが、正確には、一般公開されたとは言えません。現在運営中の Web サイトには、匿名の閲覧者から熱心な参加者まで、だれでも、またどのようなレベルにも簡単に関わることができます。エコシステム全体に SPDX™ を浸透させるのは大変なことです。主な Linux ディストリビューターやパッケージメンテナー、(商用およびオープンソースの) ツール開発者、さらにはパッケージの利用者側の組織による参加と支援が必要です。既にこれらの全カテゴリの主要な組織や人々が参加していたため、私たちには自信がありました。The Linux Foundation のさらなる支援を得たことで、より一層自信を持つことができました。

参加者募集

SPDX™ ワーキンググループへの参加にご興味のある方は、下記のチェアパーソンの一人に電子メールをお送りくださるか、<http://spdx.org> サイトをご覧ください。

著者について

Kate Stewart は、Ubuntu のリリース マネージャーとして Canonical に入社しました。Canonical 入社前の10年間は、Freecale Semiconductor 社において、Power アーキテクチャのためのオープンソースを開発するチームを指揮していました。その際、Linux ボード サポート パッケージと、新しいシリコン向けの必要機能の開発を担当しました。そのために、ソフトウェアを配布したり、Linux コミュニティ、GNU コンパイラー、U-Boot プロジェクトへのコード コントリビューションを行ったりし、オープンソース ライセンスを理解し、さらに世界中の開発者、企業の法務部門、シニア マネージャー、およびサードパーティ パートナーと一緒にオープンソースのポリシーを開拓する必要がありました。彼女は、カナダのマニトバ大学でコンピューターサイエンスの BS を、ウォータールー大学でコンピューターサイエンスの MM を取得しています。

Phil Oden 氏は、Black Duck Software のビジネス開発担当バイス プレジデントです。同社は、オープンソースに関わる管理、コンプライアンス、およびセキュリティ問題を処理する企業アプリケーション開発ツールを提供しています。マルチソース開発、リーガル、およびオープンソースエコシステムのパートナーシップを発展させることにより、同社の対象領域、イメージ、製品の幅を拡大する責任を負っています。同社に入社する前は、Empirix、High Performance Systems、および Teradyne 社のシニア マーケティング、セールス、およびビジネス開発を担当していました。彼は、ダートマス カレッジにおいて、エンジニアリングサイエンスの AB、およびシステムシミュレーションの MS を取得しています。



オープンコンプライアンスプログラムについて

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

<http://www.linuxfoundation.org/programs/legal/compliance> (英語)

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



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

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

