FOSSA

HITACHI
Inspire the Next

JS Foundation

オープンソースライセンスの認証における信頼性と自律性の確立

顧客名: Kris Borchers（エグゼクティブディレクター）

本ケーススタディーはFOSSAの事例（https://fossa.com/customers/js-foundation）を日本語に翻訳・再構成したものです。

JS Foundationは、ESLint、lodash、jQuery、mocha、webpackなど28のプロジェクトを擁していますが、これらは世界のトップ100万のWebサイトのうち75%で利用されており、重要なインフラを支えています。JS Foundationの使命は、オープンソースのJavaScriptエコシステムの中心となることで、主要なJavaScriptソリューションや関連技術の幅広い採用と継続的な開発を促進することです。

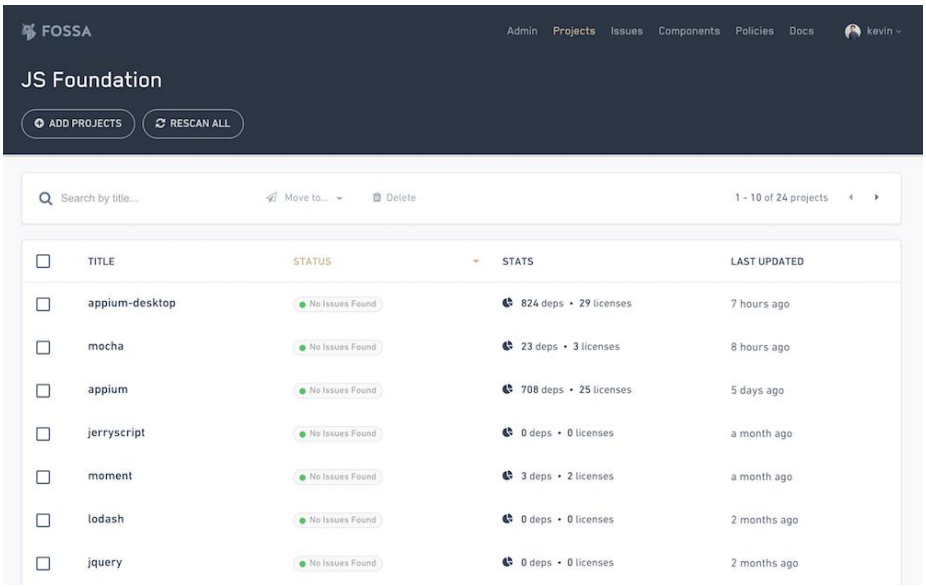
課題

JavaScriptエコシステムのユニークな特徴は、コード共有の自由な文化です。小さなJavaScriptプロジェクトでさえ、何千ものサードパーティの依存関係があることで知られています。

> “JavaScriptの依存関係を手作業で把握するのは不可能です。オープンソースソフトウェアは今やビジネスの大部分を占めています”

JS Foundationが提供する主なサービスのひとつに、プロジェクトの法的監督があります。ほとんどすべてのウェブビジネスがオープンソースのJavaScriptライブラリに依存しているので、JS Foundationはこのインフラが安全であることを保証しなければなりません。 Kris氏は「私たちは法的な観点から、プロジェクトを確実に保護したいと考えています。28のプロジェクトは言うまでもなく、1つのプロジェクト内だけでもレビューする依存関係が非常に多くあります。すべてのプロジェクトの依存関係を一つ一つ確認するために、弁護士にお金を払う余裕はありません。」と述べています。

コンプライアンス遵守は非常に重要です。 Kris氏は「プロジェクトのユーザーが安全であることを保証するために法的確認を行っていなければ、大きなビジネスリスクが発生する可能性があります。」と述べています。もし問題が起きてしまえば、何百万人ものユーザーに影響を与える可能性があります。JS FoundationはWebの重要なサプライチェーンを担っており、JavaScriptのエコシステムの長期的な持続可能性はJS Foundationの成功にかかっています。



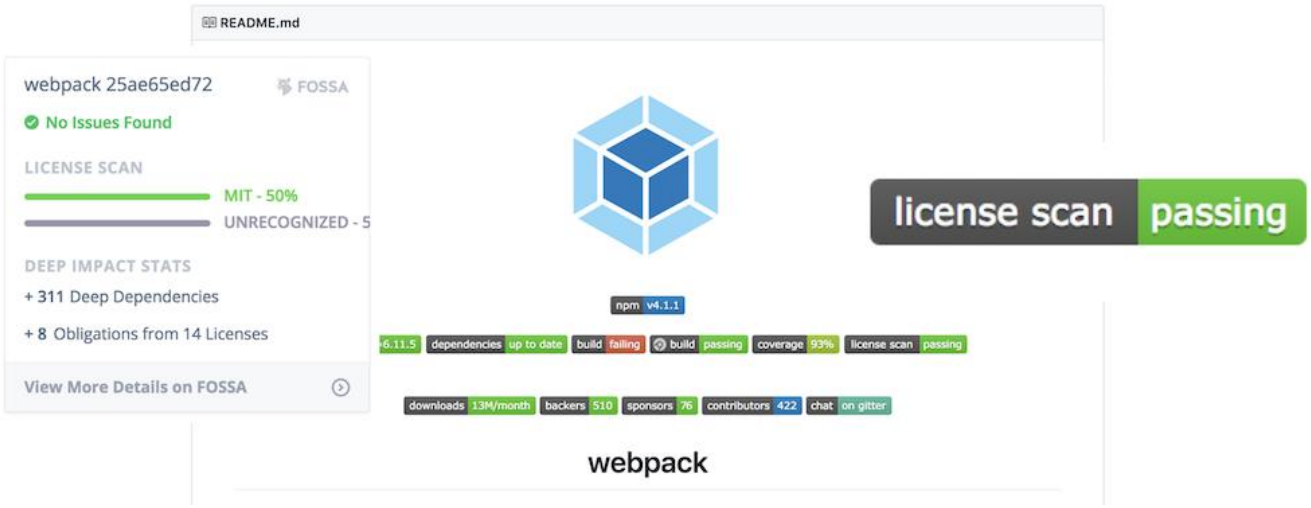
ソリューション

JS Foundationは、各プロジェクトの自律性を維持しながら、主要プロジェクトのライセンスコンプライアンスと依存関係の追跡を監視、管理、維持するための、信頼性の高い自動化された方法を必要としていました。

FOSSAは継続的に動作し、プロジェクト内のすべてのソースファイルと依存関係をスキャンしてライセンス違反を検出します。FOSSAは開発ワークフローと完全に統合されており、Slackで問題を通知したり、互換性のないライセンスの依存関係をプルリクエストでブロックしたり、著作権ヘッダーを含む帰属レポートを生成したりすることで、リリースがコンプライアンス基準を満たしていることを証明します。このように、FOSSAは開発チームのために、コンプライアンス遵守の自動化および省力化を実現します。

最初の評価時、わずか数分でリアルな検出結果が得られました。これによって早い段階で信頼が確立され、これが選定の際の重要なポイントとなりました。また開発ワークフローにシームレスに統合できることもFOSSAを選択する際の決め手となりました。 Kris氏は「開発者がツールチェーンの一部として選択し、自然に適合できるのは素晴らしいことです。我々は簡単にポリシーを設定することができ、すべてのプロジェクトの可視性を高めることができます。」と述べています。

Kris氏はFOSSA導入の指揮を執り、まずは主要プロジェクトのリポジトリ群に対する基本的なライセンスチェックを行うことにしました。最初のステップは、FOSSAアカウントをセットアップするために、各プロジェクトのメンテナを特定することでした。アカウントの設定に続いて、各プロジェクトのメンテナには、コミットごとのスキャン、CIツールとの統合、さらにはプルリクエストコメントを有効にしてライセンス標準に対してコントリビューションを実行する権限が与えられました。最初のデプロイメントは数分で開始され、完全なデプロイメントは1週間以内に有機的に展開されました。



FOSSA適用の概要

- 24のプロジェクトとチームにおけるライセンスコンプライアンス遵守
- 2000以上のコンポーネントの継続的な追跡、スキャン、分析
- 公開されているホームページやドキュメントでバッジおよび認証を掲載

“FOSSAを導入してすぐに成果が出ました。ある例では、GPLコードのように見える誤解を招くようなメタデータを見つけました。FOSSAが問題にフラグを立ててくれたので、問題を先取りすることができました”

導入の結果

FOSSAの導入で、自動化されたライセンスコンプライアンスの継続的なスキャンにより、法務チームとエンジニアリングチームの両方で手作業による調査の負担が軽減されました。さらに重要なのは、FOSSAの認証が監査レベルの詳細さで実行されていることが証明されたことで、問題が常に追跡、監視、フラグ付けされているという信頼感が浸透したことです。

“FOSSAが我々のプロジェクトを保護していると知っていることが、我々にとって最大の価値でした。そうでなければ、すべてのプロジェクトの依存関係を調べるのに、何百時間もかかってしまうでしょう”

JS Foundationは、新しいプロジェクトやプロジェクトリーダーが加わるたびに、ライセンスコンプライアンスと依存関係の追跡にFOSSAを推奨していきます。Kris氏は「すべてのオープンソース組織は、ライセンスと依存関係の追跡を導入すべきです。これまでの経験から、大規模なプロジェクトや進行中のプロジェクトがたくさんある組織にはFOSSAをお勧めします。また、JavaScriptを使用している場合は特にお勧めです。」と述べています。

“もし私がビジネスでFOSSAのバッジを見たら、それはライセンスコンプライアンス遵守の面で大きなプラスになります”

株式会社 日立ソリューションズ
www.hitachi-solutions.co.jp