SYNOPSYS®

自動化で効率はこうも変わる
「3時間から数分に」作業工程を短縮 日立製作所が導入したOSS利用の仕組み

開発のスピードアップやコスト削減のために、オープンソースソフトウェア（OSS）は欠かせない存在になった。ただし OSS を活用するにはライセンスの順守が大前提であり、担当者の頭を悩ます問題でもある。

HITACHI
Inspire the Next


日立製作所の金子真也氏


日立製作所の小出大亮氏


日立製作所の石川晃久氏

コストを抑制しつつ、迅速に製品やサービスをリリースするために、オープンソースソフトウェア（OSS）の力が必要になっている。OSS の利用は IT システムをはじめ、家電、IoT（モノのインターネット）、自動車など業界を問わず当然のように利用されている。

ただし OSS の利用にはリスクが伴う。「無償で使えるから」と安易に利用して OSS のライセンスを侵害してしまうケースが後を立たない。ライセンス違反として批判を受けたり、使用差し止め、さらには損害賠償を求められたりするケースもある。OSS も商用ソフトウェアのように、利用、改変、再配布に当たって権利と義務を定めたそのライセンスを守らなければならない。

OSS のライセンスを順守するためには適切な管理が必要だが、ライセンスの複雑さが担当者の悩みの種になっている。こうした課題に直面していた日立製作所は、OSS のライセンス確認作業を自動化し、劇的にその作業工程を効率化した。日立製作所はどのようにしてその仕組みを導入したのか紹介しよう。

負担が大きかったOSSライセンスの確認作業

日立製作所は「Linux」「PostgreSQL」「OpenStack」「Hyperledger」など、さまざまな OSS を活用している。Linux Foundation をはじめとするコミュニティーにも参加し、OSS の利用促進に貢献してきた企業だ。同社の OSS 活用を推進しているのが 2015 年設立の「OSS ソリューションセンタ」。各社内カンパニーに散在していた OSS の利用に関するノウハウを集約し、IT から組み込み、制御に至るまで幅広い分野で OSS の活用を支援している。

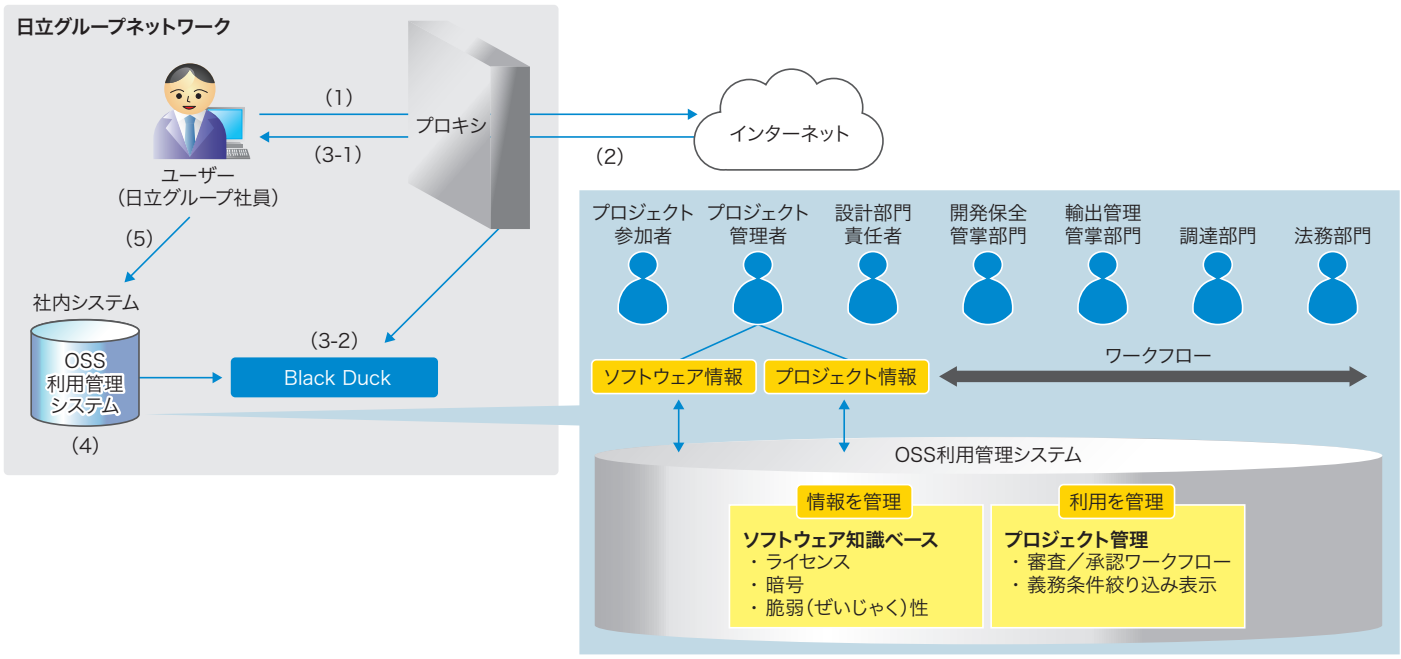
OSS の活用を進める上で、日立製作所には大きな課題があった。利用する OSS のライセンス確認作業の負担が大きい点だ。同社は OSS の利用に関する社内の情報を一元管理するためのプロセスを導入していた。コンプライアンスの観点から「OSS をダウンロードして利用する際には、ライセンスを確認すること」という社内ルールを定め、その上で OSS のライセンスや機能、暗号アルゴリズムなどを整理した「構成要素管理データベース」を作成。新たな OSS をダウンロードした際は、その担当者が手作業でライセンスを確認し、データベースに登録して情報を共有してきた。

問題は、基本的には手作業でライセンスを確認することだ。煩雑な作業になるため、特に急ぎのプロジェクトの場合は担当者にかかる負担が大きくなってしまう。OSS ソリューションセンタで技師を務める金子真也氏は「ダウンロードするたびに担当者がツールでスキャンしていたが、一つの OSS ライブラリの中に、芋づる式に何百、何千もの OSS が含まれていることもあり、ある OSS を調査するのに 1 カ月もの時間を要することもあった」と振り返る。

OSS の場合、ライセンスをどこに明記するかはルール化されておらず、その分作業は煩雑になる。「OSS のライセンスは必ずしも『LICENSE.txt』に書かれているとは限らず、ソースコードのコメントに含まれていたり、公式サイトや『GitHub』をはじめとするソースコード共有サービスに記されていたりと、複数の場所を探し回ってライセンスを確認する必要があった。しかも基本的には英文で書かれており、それもまた負担だった」。OSS ソリューションセンタの小出大亮氏はこう語る。こうした煩雑な作業のため、これまで 1 つの OSS のライセンス確認作業に平均 3 時間ほどかかっていたという。

一方で利用する OSS の数は増加していた。OSS ソリューションセンタの石川晃久氏によれば「この 1 年は月当たり 700 件程度の OSS を審査する必要があった」という。「この先もさらに増加することが予想されるため、手作業ではとても間に合わない、何か手を打つ必要があると判断した」（石川氏）

システムの全体像



日立製作所が導入したOSSのライセンスをスキャンし、登録する仕組み(注)

※注 ： 図中の記号の意味は次の通り。(1):OSSダウンロードリクエスト、(2):ファイルレスポンス、(3-1):ファイルレスポンス、(3-2):ファイルをBlack Duckにアップロード、(4):OSS名、バージョン、ライセンス情報を取得、(5):取得したOSSのライセンス確認。

Black Duckを採用、APIを活用して確認プロセスを自動化

こうした状況で日立製作所が採用したのが日本シノプシスの「Black Duck」だった。日立製作所はソースコード中のコピー＆ペースト部分の発見などを目的に同社製品を利用しており、同社製品への信頼があったことが導入に当たっての一つの理由になった。それに加え、「業界で広く利用されているだけでなく、実際にテストしてみたところ、ライセンスをスキャンするスピードが満足できるレベルだった」（石川氏）こともあり、Black Duck の採用を決定した。日立製作所は、Black Duck をそのまま導入するのではなく、API を活用して既存のプロセスの中に組み入れ、作業を自動化した。

日立製作所は、業務で OSS をダウンロードする際はプロキシを経由させる仕組みを構築している。このプロセスにおいて API を介し、OSS のダウンロードと同時にバックエンドで Black Duck を連動させてライセンス情報をスキャンし、自動的にデータベースに登録するシステムを開発した。担当者はコマンドラインや Web インタフェースで、このプロセスの結果をチェックできる。

ライセンス確認作業が1件当たり数分単位に短縮

ライセンス確認作業は数分単位で済むまでに作業負担が軽減し、結果として月に約 8000 件もの OSS のライセンスをチェックし、データベースに追加できるようになった。製品の開発、リリース後にライセンス違反が判明すれば、その事態に対処するためのコストが膨らんでしまう。Black Duck を中核としたライセンスチェックの仕組みを整備したことで、開発工程の早い段階でそのリスクを排除できるようになった。

「従業員はライセンス違反のリスクから保護されるとともに、ライセンスのチェックや登録の作業に工数をかけることなく、価値を生み出す作業に力を注げるようになった」と石川氏は評価する。OSS が必要な開発者は利用したい OSS を単にダウンロードするだけでよく、パッケージのあちらこちらを目視で確認しなくても、コンプライアンスに違反しない形で OSS を利用できる環境が整ったのだ。

OSSに潜む脆弱性の課題解消にも期待

日立製作所は、Black Duck のさらなる活用を計画している。その一つが OSS の利用で懸念されるセキュリティの脆弱（ぜいじゃく）性への対処だ。

SSL ／ TLS ライブラリの脆弱性「Heartbleed」や Web アプリケーションフレームワーク「Apache Struts 2」の脆弱性が判明した際、自社で利用しているシステムがその影響を受けるのかどうか、受けるならどのような対処が必要になるかを確認、検討するため、対処に追われた技術者は少なくないだろう。

開発、出荷時には当然のことだが、リリース後も製品やサービスに含まれる OSS の脆弱性をトレースすることが必要になっている。日立製作所はこうした脆弱性への対処についても、Black Duck が役立つと期待している。他社の脅威情報も組み合わせて検証しつつ、安全な製品、サービス作りに生かす。

現在、OSS は価値創造に不可欠な存在になった。ただし利用に当たってはライセンスの順守と脆弱性への対処が必要だ。こうした点が欠けてしまうと、思わぬ批判を受けたり、顧客に迷惑を掛けたりする可能性がある。

日立製作所は Black Duck を利用して自動化された仕組みを作り、OSS の利用に潜むリスクを抑えつつ、価値創造の最大化に取り組んでいる。これに並行して、Linux Foundation の OSS ライセンス順守に関するプロジェクト「OpenChain」にも参加し、OSS ライセンスの標準化に取り組んでいる。目標とするのは OSS ライセンスを情報交換するための標準規格「Software Package Data Exchange」（SPDX）のような形で、開発者、利用者双方のメリットになる体制を整備することだ。こうした OSS のサプライチェーン構築への貢献を掲げる日立製作所にとって、Black Duck は大きな力になるはずだ。

SYNOPSYS®
https://www.synopsys.com/jp/software
日本シノプシス合同会社 営業本部 ソフトウェア インテグリティグループ
〒158-0094 東京都世田谷区玉川2-21-1二子玉川ライズオフィス
TEL: 03-6746-3600 Email: sig-japan@synopsys.com