OSSとの「上手な付き合い方」【第2回】:

OSSの“謎”現象「入れた覚えがないのに大量利用」はこうして起こる

https://techtarget.itmedia.co.jp/tt/news/2208/10/news06.html

企業はOSSを知らないうちに自社のシステムに組み込んでいる現実がある。使用しているOSSを検出し、OSSに含まれる脆弱性によるリスクを減らすには、どうすればよいのか。

2022年08月08日 05時00分 更新

[藤原洋平, ベリサーブ]

関連キーワード

OSS | 脆弱性対策 | セキュリティ

近年、企業が自社システムにOSS(オープンソースソフトウェア)を組み込むことは特別なことではなく、当たり前となってきている。フルスクラッチ(完全の自前開発)でプログラムを書き上げる方が珍しくなった。しかし自社システムに利用するOSSを適切に把握・管理できている企業は少数派だと、筆者は感じている。

中には、OSSのことを何も気にせず利用してきた企業もあると考えられる。もしそうであれば、今からでもOSSの管理に取り組めばよい。厄介なのは、「利用しているOSSは開発者が表計算ソフトウェアのシートに記録している」「OSSの利用は申請制にしているため、勝手に使われることはない」といったように、OSSを管理した“つもり”になっている企業だ。

だから気付きにくい　OSSが自社製品に組み込まれる「さまざまな経路」とは

併せて読みたいお薦め記事

連載:OSSとの「上手な付き合い方」

- 第1回:知らないと危険な「OSSのリスク」　“脆弱性祭り”への対処法とは?

OSSの知識を深めるには

- いまさら聞けない「OSS」はなぜ魅力的で、なぜ手を出しにくいのか?
- 開発力のある企業はなぜ「OSSのサービスメッシュ」を選択するのか?

OSSが自社システムに組み込まれる経路は、開発者が意図したものだけとは限らない。OSSはあらゆるところからやって来る。経路として考えられるのは、大きく次の3つだ。

- パッケージ管理システム(注)
  - 開発においてソフトウェアの自動取得を可能にするパッケージ管理システムが、OSS群をダウンロードし、ビルド(組み立て)することがある。
- 市販ソフトウェア
  - 市販ソフトウェアを購入して組み込む場合、その中にOSSが含まれていることがある。
- 委託開発
  - ソフトウェアの開発を委託する場合、委託先の会社がOSSを利用していることがある。

※注:例えばC言語(開発実行環境として「.NET Framework」を利用する場合)であれば「NuGet」、JavaScriptであれば「npm」(Node Package Manager)など。

このように、OSSが自社システムに組み込まれる経路は単一ではない。そのためOSSを管理している企業はいま一度、管理の観点に抜け漏れがないかどうかを確認することが重要だ。OSSが組み込まれる経路別に、まずは次の点を確認するとよい。

- パッケージ管理システム
  - 設定ファイルを確認する。
- 市販ソフトウェア
  - 購入元にOSSの利用有無を確認する。
- 委託開発
  - 委託先との契約内容にOSSに関する取り決めを盛り込む。

OSSを管理する上では、以上の内容を確認しただけでは完璧とは言えない。意図しないOSSの利用（本稿では「OSSの混入」と呼ぶ）があるからだ。

OSSの混入はなぜ起きるのか

企業は意図的なのかどうかを問わず、自社システムにOSSが組み込まれているのであれば、脆弱（ぜいじゃく）性のリスクにさらされる可能性がある。OSSライセンスの利用条件を守らなければ、コンプライアンスの面でも問題になる。

OSSの混入はなぜ起きるのか――。理由はさまざまだ。まず考えられるのは、前述したパッケージ管理システムの使用だ。それ以外にも市販ソフトウェアの購入、開発の委託などが原因となってOSSが混入することもある。企業は「OSSが含まれているかもしれない」という意識を持たなければ、気が付かないうちに自社システムにOSSが組み込まれてしまう。

開発者がOSSのソースコードをコピー＆ペーストし、自社のソースコードに組み込んでしまう場合は、非常に厄介なことになる。自社のソースコードに組み込まれてしまったOSSのソースコードは、人手による目視レビューで検出することがほぼ不可能だからだ。

自社で開発したソースコードも、OSSのソースコードも、「単なる文字列」であるという点では違いはない。そのため大量のソースコードがある中、あるソースコードが自社で開発されたものなのか、OSSとして公開されているものなのかを人が見分けることは極めて難しい。

混入したOSSを検出する

目視では見つけられないOSSの検出には「OSS検出ツール」が有効になる。OSS検出ツールは名前の通り、OSSを検出するためのツールだ。OSS検出ツールには、Synopsysの「Black Duck」など複数の選択肢がある。

各種OSS検出ツールは世界中のOSSの情報を蓄積したデータベースを保持している。簡単に言えばソースコードをスキャンし、データベースの情報と突合することでOSSの有無が分かる。

ではOSS検出ツールを導入すれば、OSSの把握と管理の問題が全て解決するかというと、必ずしもそうではない。OSS検出ツールは、目視では気付くことのできないOSSの流用の可能性を指摘するが、最終的には人手による確認が必要となる。データベースの情報が誤っていたり、ノイズとなる情報が混ざっていたりするからだ。

OSS検出ツールの結果の確認には、一定の知識やスキルが要る。本当はOSSを利用していないのに、OSS検出ツールがOSS流用の可能性を指摘することもある。利用しているOSSとは違うOSSを提示することも想定しなければならない。ユーザー企業は、OSS検出ツールが提示する結果の中から、正しい情報を取捨選択する必要があるのだ。

意図しないOSSの混入を検出するには、OSS検出ツールの使用が有効であることをお伝えした。しかしOSSに関する知識やノウハウがない、あるいはOSSの確認をするためのリソースがない、といった問題を抱える企業もある。

そのような企業にとっての選択肢として「OSS混入検査サービス」がある。ベンダーが対象のソースコードをOSS検出ツールでスキャンし、OSSの正しい情報を収集するサービスだ。ベンダーは収集した結果をレポートにまとめ、ユーザー企業に報告する。OSSに関する知見を持った専門家がスキャンや分析を実施するので、ユーザー企業は高精度なレポートを受け取れる。

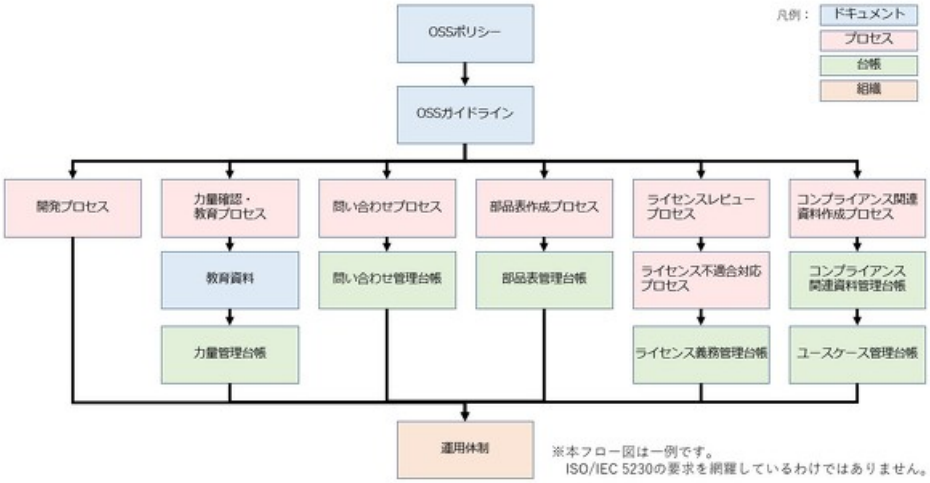
意図しない「OSSの混入」の予防

上記で説明した通り、OSSはさまざまな経路からやって来る可能性がある。従ってそれぞれの経路について、OSSの使用状況を把握可能な開発プロセスを策定しておくことが重要だ。開発プロセスの策定に当たっては、2020年12月に発行されたOSS管理の国際標準「ISO/IEC 5230:2020」を参考にすることを推奨する。

ISO/IEC 5230:2020には、幾つかの要求事項がある。詳細は割愛するが、例えば

- OSSポリシーを策定し、文書化する。
- OSS管理に関わる役割（メンバー）ごとに、OSS管理に関する力量を定義する。
- 策定したOSSポリシーの存在を、OSS管理に関わる組織に周知する。

といったことが記載されている。これらはどれも、意図しないOSSの混入を防ぐための重要な要素だ。



ISO/IEC 5230に対応したプロセスの一例（出典：ベリサーブの資料）《クリックで拡大》

少なくとも、OSSポリシーと開発プロセスの策定と、開発者の教育は必須だと筆者は考えている。その上でOSS混入検査サービスを利用することが、OSSのリスク対策の第一歩となる。

第3回は、把握したOSSをどのように管理すればよいのかを説明する。

著者紹介

藤原洋平（ふじわら・ようへい） ベリサーブ

2010年からベンチャー系開発企業で組み込み系ブラウザエンジンの品質保証業務に従事。2016年、ベリサーブ現職入社。OSSのリスク管理サービスを担当している。他にも、セキュリティに関するコンサルティングや脅威分析、脆弱性診断に携わる。社外では、ソフトウェアテストのワークショップを開催する若手コミュニティー「WACATE」の実行委員として活動中。