


## OSSライセンス管理「FOSSA」の 試用結果および所感

2020/06/23

株式会社 日立ソリューションズ  
森下 大輔

- 
1. はじめに
  2. 概要
  3. 使い方
  4. 詳細（仕組みなど）



## 1. はじめに

## 【所属】

ITプラットフォーム事業部 デジタルシフト開発支援本部  
プロセスコンサルティング部 OSS利活用グループ  
森下 大輔

## 【経歴】

2014年～ WEBアプリ開発（Java/JS）、OSS検証（BlackDuck）  
2017年～ 大手Web系企業様 出向 OSS管理部門支援  
2020年～ OSS管理プロダクト担当

## 【使ったことのあるOSS管理ツール】

FOSSology、SW360、BlackDuck、FOSSA、WhiteSource、等

## 【その他の活動】

日立グループSNS「OSS全般情報共有部屋」管理人  
Qiita (<https://qiita.com/d-morishita>)  
MS Teamsコンサルタント（自称）

## ■ FOSSA(フォッサ)?



<https://www.linuxfoundation.jp/resources/open-source-guides/tools-managing-open-source-programs/>

## ■ Qiita書きました。

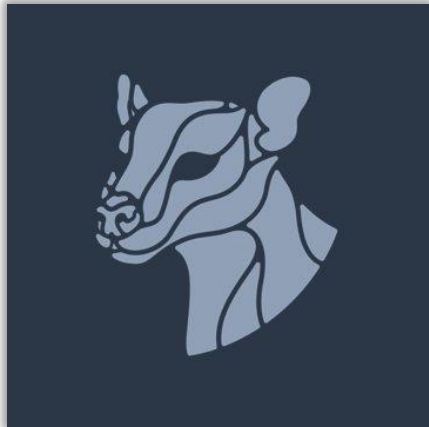
OSSライブラリのライセンス管理の決定版「FOSSA」を使ってみよう

<https://qiita.com/d-morishita/items/7ee9242652975fc21b72>



## 2.概要

## ■ OSSライセンス管理のためのSaaS型のツール

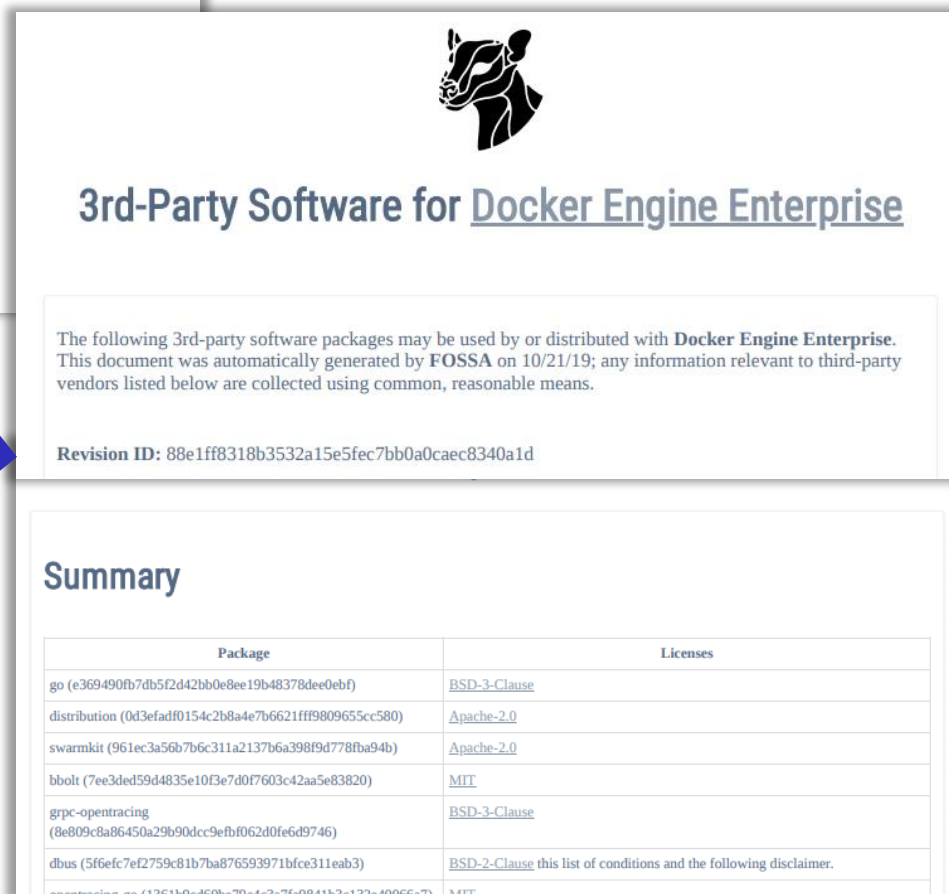
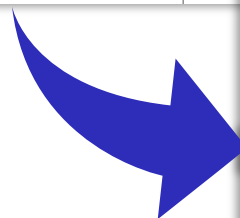
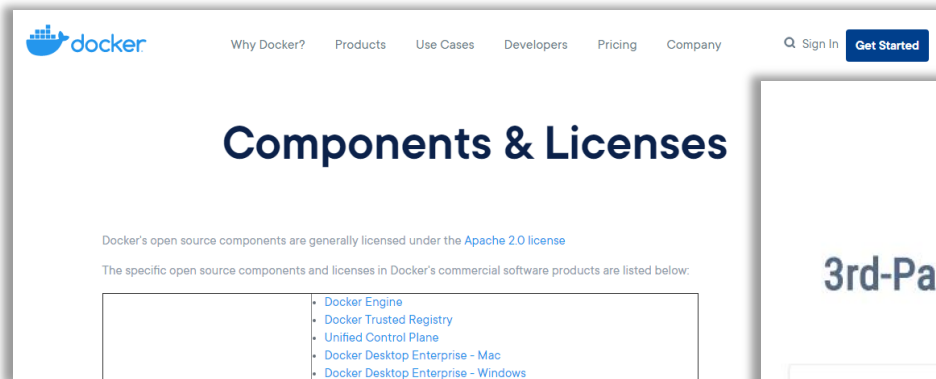


<https://fossa.com>

- プロジェクトの依存OSSをチェック  
※使い方は後述
- OSSのライセンス & 責務を明示
- ライセンスに関する問題発生時にアラート発行
- 個人での利用は無料

## ■ 例：Dockerのレポート

<https://www.docker.com/legal/components-licenses>





## ■ 例：WebpackのReadme

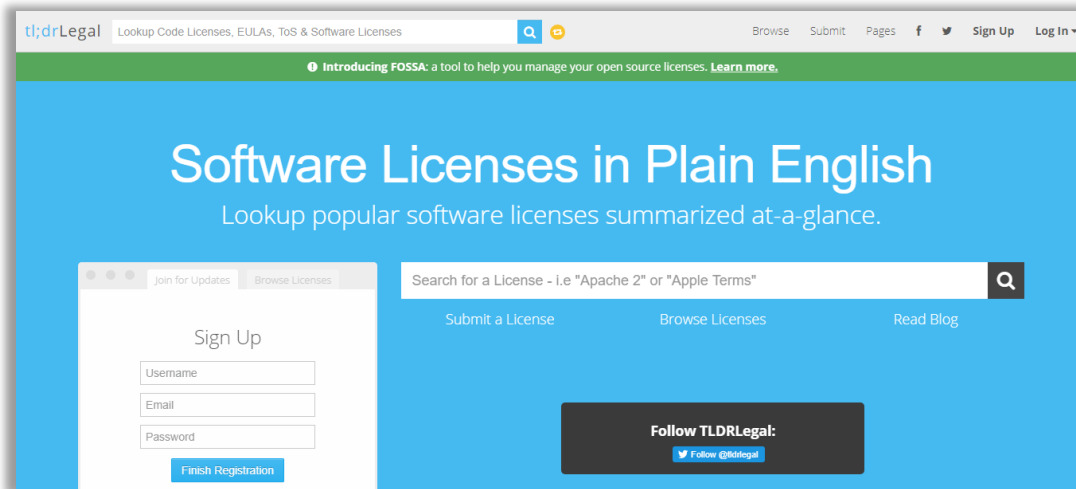
The screenshot displays the webpack project page on the FOSSA platform. On the left, a sidebar shows the project name 'webpack 25ae65ed72' and a 'FOSSA' logo. Below this, it states 'No Issues Found' and provides a 'LICENSE SCAN' progress bar showing 'MIT - 50%' and 'UNRECOGNIZED - 5'. Further down, 'DEEP IMPACT STATS' are listed: '+ 311 Deep Dependencies' and '+ 8 Obligations from 14 Licenses'. A button 'View More Details on FOSSA' is at the bottom of the sidebar. The main content area features the webpack logo, the version 'npm v4.1.1', and a series of status bars: '6.11.5', 'dependencies up to date', 'build failing', 'build passing', 'coverage 93%', and 'license scan passing'. At the bottom, a row of statistics is shown: 'downloads 13M/month', 'backers 510', 'sponsors 76', 'contributors 422', and 'chat on github'. A large green speech bubble on the left points to the sidebar with the text 'FOSSA/バッジ (Large)'. Another green speech bubble on the right points to the 'license scan passing' status with the text 'FOSSA/バッジ'.

<https://fossa.com/customers/js-foundation/>

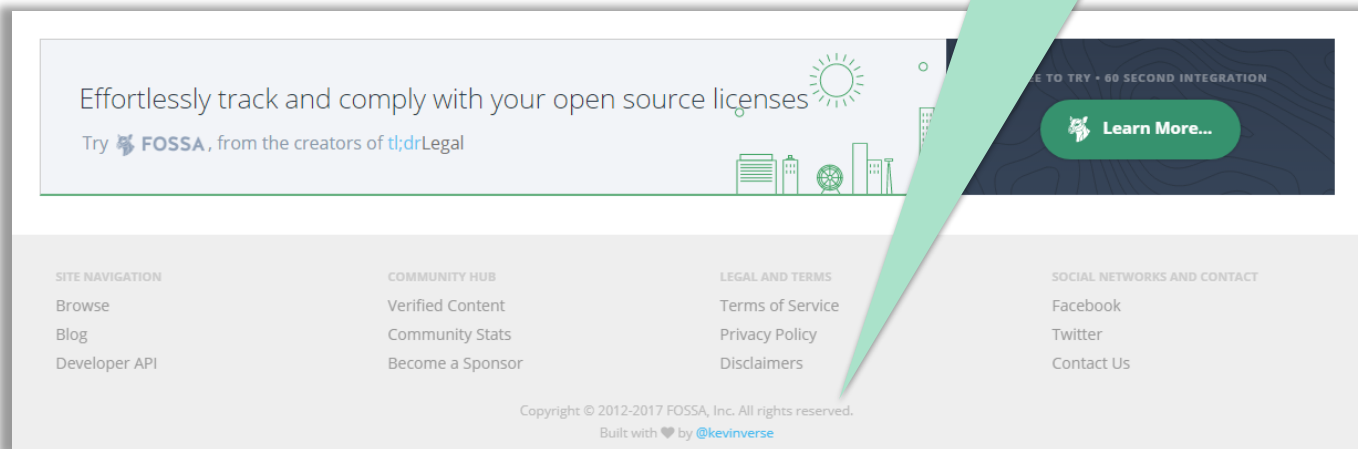
決定版では!?



## ■ FOSSA, Inc.は tl;dr Legal を運営



FOSSA, Inc. All rights reserved.



<https://tldrlegal.com/>

---

## 3. 使い方

## ■ サインアップ

<https://fossa.com>

A screenshot of the FOSSA sign-up form. The form is titled 'Sign up for FOSSA' with a sub-note 'Get started free-no credit card required.' It offers four social login options: Google, Github, Bitbucket, and Gitlab. Below these is an 'OR' separator. To the right of the social logins are input fields for 'Username:', 'Email:', and 'Password:'. A note below the password field states: 'Passwords must be 8-128 characters long and contain at least 3 of the following character types: lowercase letters, uppercase letters, digits, and symbols.' At the bottom right are two buttons: 'Sign Up' and 'Login to Existing Account'.

## ■ スキャナをインストール



※ スキャナはオープンソースで公開されています。  
<https://github.com/fossas/fossa-cli>

## ■ スキャン

### 2. Run & Upload Build Analysis

Navigate into your code directory and run the following command.

```
fossa init  
FOSSA_API_KEY=5561724e878a44f209a0c7a89400dd6a fossa analyze
```

The screenshot displays the FOSSA web application interface. At the top, the navigation bar includes links for Projects, Issues, Components, Policies, Docs, Support, and a Demo button. The main header shows the project name 'express-sample' and the branch 'master'. Below this, a summary card indicates that all checks passed for the master branch, with a 'Rescan' button. To the right, two summary boxes show '50' dependencies and '8' licenses. A central message states: 'FOSSA ran license checks across 50 dependencies. No issues were found.' Below this message are buttons for 'Generate Report' and 'Share'. On the right side, an 'ACTIONS' section provides links to 'Generate Compliance Report', 'Generate Vulnerability Report', and 'Visit API Endpoint'.

## ■ DEPENDENCIES

The screenshot shows the FOSSA web interface for a project named 'express-sample'. The top navigation bar includes links for Projects, Issues, Components, Policies, Docs, Support, and a Demo button. Below the project name, there's a commit hash '1617c7' and a timestamp 'Jun 12th 2020, 11:12 am'. The main navigation bar has tabs for SUMMARY, ISSUES (0), DEPENDENCIES (50), LICENSES (8), and REPORTS. The DEPENDENCIES tab is active, showing a list of 50 dependencies. The interface includes filters for license and source, a 'Flagged' checkbox, an 'Export' button, and a search bar. The dependencies are categorized into DIRECT (1) and DEEP (49). Three dependencies are visible: 'express' (4.17.1), 'accepts' (1.3.7), and 'array-flatten' (1.1.1), all with MIT licenses.

**FOSSA** Projects Issues Components Policies Docs Support Demo

**express-sample** master

1617c7 : Jun 12th 2020, 11:12 am

SUMMARY ISSUES 0 DEPENDENCIES 50 LICENSES 8 REPORTS ACTIVITY SETTINGS

50 Dependencies ✓

Filter license... Filter source... ☐ Flagged Export Search by Title...

▼ DIRECT DEPENDENCIES (1) + ADD

✓ **express** (4.17.1) npm  
Fast, unopinionated, minimalist web framework  
LICENSES: MIT

▼ DEEP DEPENDENCIES (49)

✓ **accepts** (1.3.7) npm  
Higher-level content negotiation  
LICENSES: MIT

✓ **array-flatten** (1.1.1) npm  
Flatten nested arrays  
LICENSES: MIT

## ■ LICENSES

The screenshot displays the FOSSA web interface for a project named 'express-sample'. The top navigation bar includes links for Projects, Issues, Components, Policies, Docs, Support, and a Demo button. Below the navigation bar, the project name 'express-sample' is shown with a lock icon and a branch selector set to 'master'. A commit hash '1617c7' and timestamp 'Jun 12th 2020, 11:12 am' are visible. The main navigation tabs are SUMMARY, ISSUES (0), DEPENDENCIES (50), LICENSES (8), and REPORTS. The 'LICENSES' tab is currently selected, showing a list of 8 licenses found. The licenses are categorized by their depth in the dependency tree: DIRECTLY IN CODE, STARTING IN DIRECT DEPENDENCIES, STARTING FROM 2-LEVEL DEEP DEPENDENCIES, and STARTING FROM 4-LEVEL DEEP DEPENDENCIES. The licenses listed are MIT License, ISC License, BSD 2-Clause "Simplified" License, BSD 3-Clause "New" or "Revised" License, and Apache License 2.0. To the right of the license list, a section titled '7 Obligations Found' provides details on the license obligations, including a quote: "You must include the license notice in all copies or substantial uses of the work." and a list of licenses: ISC, BSD-2-CLAUSE, APACHE-2.0, CPL-1.0, MIT-CMU, and SPL-1.0. Below this, the obligations are further detailed for specific dependencies: 'inherits (2.0.3)' and 'mime-db (1.44.0)', both showing they are depended on in multiple ways.

**FOSSA** Projects Issues Components Policies Docs Support Demo

express-sample master

1617c7 : Jun 12th 2020, 11:12 am

SUMMARY ISSUES 0 DEPENDENCIES 50 LICENSES 8 REPORTS ACTIVITY SETTINGS

### 8 Licenses Found

DIRECTLY IN CODE + ADD

STARTING IN DIRECT DEPENDENCIES

MIT License

STARTING FROM 2-LEVEL DEEP DEPENDENCIES

ISC License

BSD 2-Clause "Simplified" License

BSD 3-Clause "New" or "Revised" License

STARTING FROM 4-LEVEL DEEP DEPENDENCIES

Apache License 2.0

### 7 Obligations Found

▼ Include License for projects

"You must **include** the **license** notice in all copies or substantial uses of the work."

MIT

49 Projects...

"**Including** the full text of **license** in modified software."

ISC & BSD-2-CLAUSE & APACHE-2.0 & CPL-1.0 & MIT-CMU & SPL-1.0

inherits (2.0.3) Depended on in 6 ways

mime-db (1.44.0) Depended on in 5 ways



## ■ REPORTS

The screenshot displays the FOSSA web application interface. At the top, the navigation bar includes the FOSSA logo, a search bar, and links for Projects, Issues, Components, Policies, Docs, Support, and a Demo button. Below the navigation bar, the project name 'express-sample' is shown with a lock icon and a dropdown menu set to 'none'. A timestamp '1617c7 : Jun 12th 2020, 11:12 am' is visible. The main navigation tabs are SUMMARY, ISSUES (0), DEPENDENCIES (50), LICENSES (8), and REPORTS (active), followed by ACTIVITY and SETTINGS. The REPORTS section features a 'Compliance Report' card with a description of FOSSA's compliance report and a 'Switch to Vulnerability Report' button. Below this, a sidebar on the left offers export format options: HTML, MARKDOWN, PDF, CSV, and PLAIN TEXT, with a '2. CUSTOMIZE REPORT INFORMATION' section below. A dark blue banner states: 'Previews show a limited number of dependencies and licenses. Please download for a complete report.' The main content area shows a preview of a report titled '3rd-Party Software for express-sample', which includes a Hitachi logo, a description of the report's purpose, and a revision ID: 1617c784a50967c0.

FOSSA

Projects Issues Components Policies Docs Support Demo

express-sample none

1617c7 : Jun 12th 2020, 11:12 am

SUMMARY ISSUES 0 DEPENDENCIES 50 LICENSES 8 REPORTS ACTIVITY SETTINGS

**Compliance Report**

FOSSA's compliance report provides a comprehensive listing of this project's licensing and compliance information. This is the most used report type from FOSSA.

[Switch to Vulnerability Report](#)

1. SELECT EXPORT FORMAT

- HTML
- MARKDOWN
- PDF
- CSV
- PLAIN TEXT

2. CUSTOMIZE REPORT INFORMATION

Previews show a limited number of dependencies and licenses. Please download for a complete report.

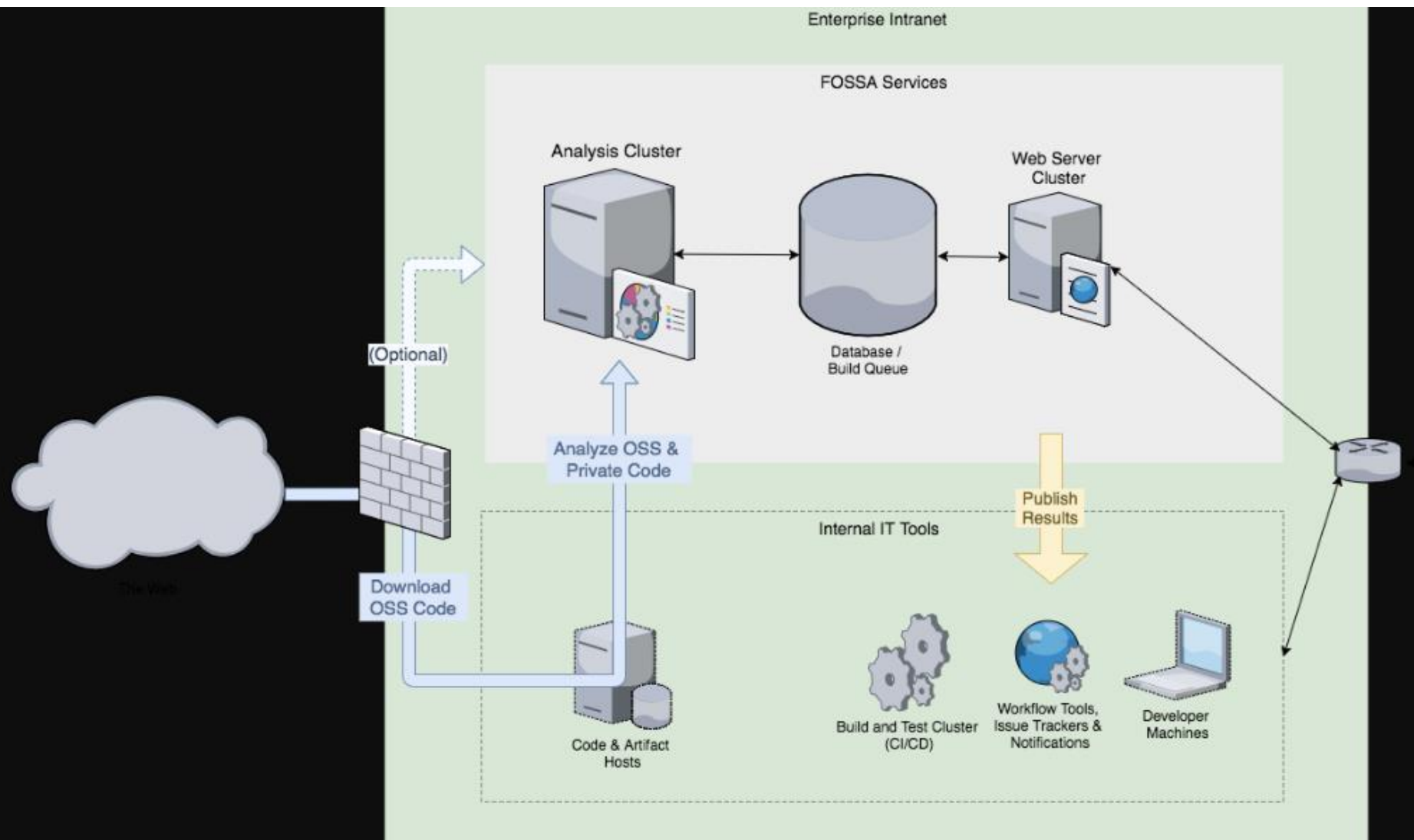
**3rd-Party Software for express-sample**

The following 3rd-party software packages may be used by or distributed with **express-sample**. This document was automatically generated by FOSSA on 06/16/20; any information relevant to third-party vendors listed below are collected using common, reasonable means.

Revision ID: 1617c784a50967c0

---

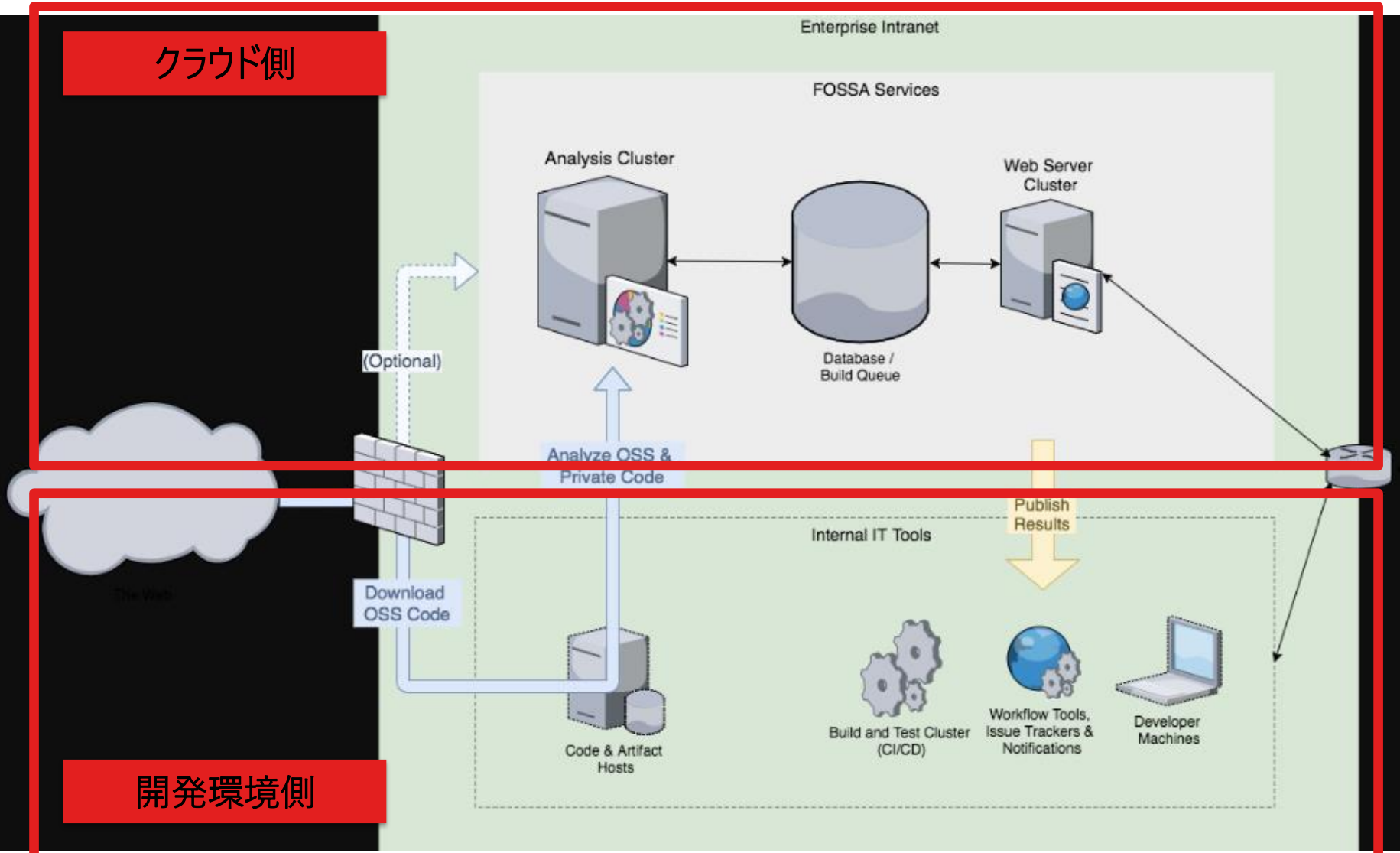
## 4. 詳細（仕組みなど）



※ オンプレミス版の構成

<https://docs.fossa.com/docs/architecture-overview>

クラウド側



<https://docs.fossa.com/docs/architecture-overview>

# 構成（スキャンの流れ）

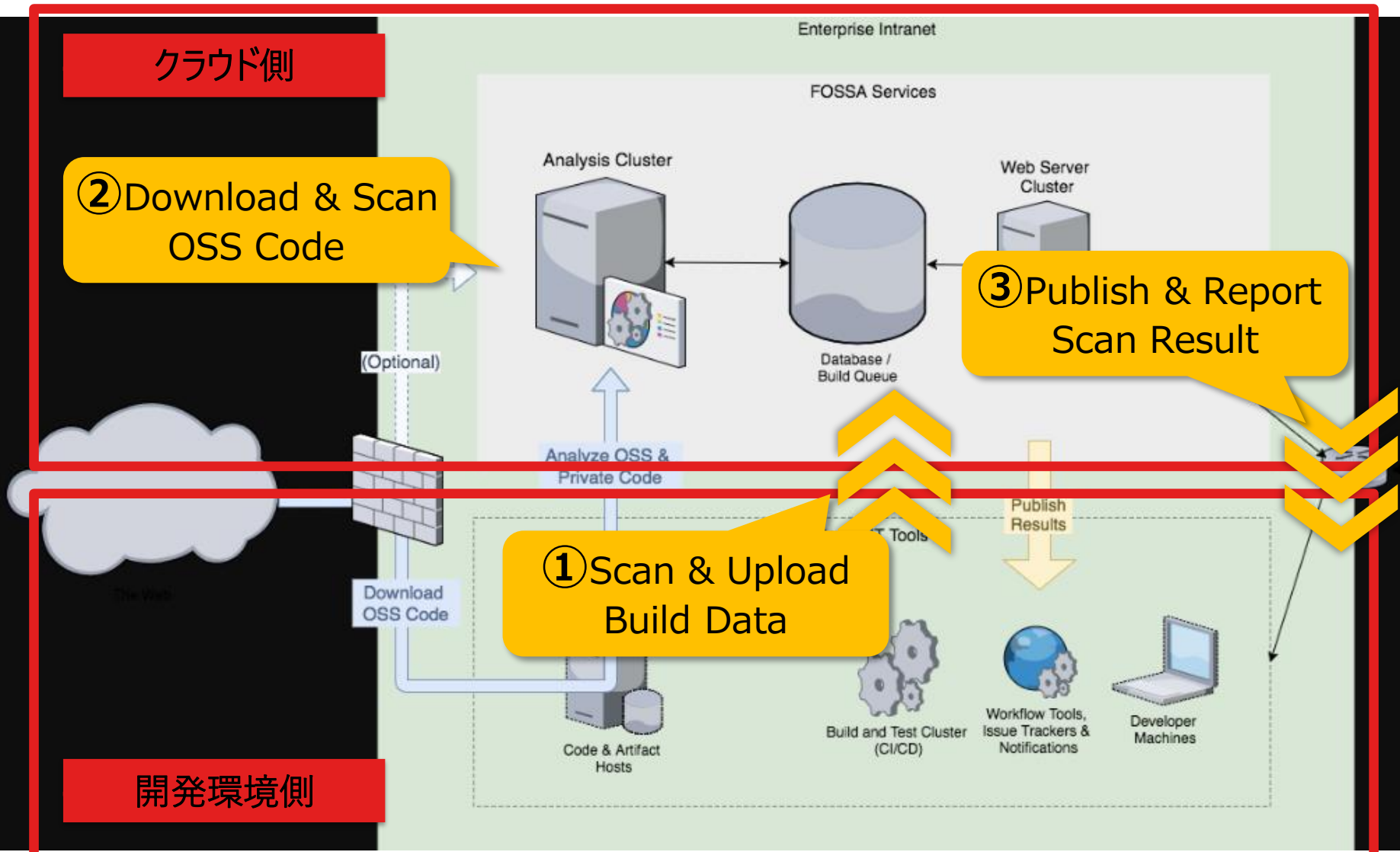
クラウド側

② Download & Scan  
OSS Code

③ Publish & Report  
Scan Result

① Scan & Upload  
Build Data

開発環境側



<https://docs.fossa.com/docs/architecture-overview>

## ■ スキャナの詳細

<https://github.com/fossas/fossa-cli>

`fossa -o` コマンドで、スキャン結果をjson出力

```
"Imports": [
  "npm+express$4.17.1"
],
"Dependencies": [
  {
    "locator": "npm+bytes$3.1.0"
  },
  {
    "locator": "npm+toidentifier$1.0.0"
  },
  {
    "locator": "npm+content-disposition$0.5.3",
    "imports": [
      "npm+safe-buffer$5.1.2"
    ]
  },
  {
    "locator": "npm+proxy-addr$2.0.6",
    "imports": [
      "npm+forwarded$0.1.2",
      "npm+ipaddr.js$1.9.1"
    ]
  }
],
```

- Npmプロジェクトのスキャン結果（Expressのみ依存した場合のスキャン）
- locatorおよびimportsによって推移的依存まで検出されているのが分かる
- ソースコードの実体は解析をしない

Environment	Package Managers
Android	Gradle
Clojure	Leiningen
Debian	Dpkg
Golang	Dep, Gomodules, Vndr, GDM, Glide, Godep, Govendor
Groovy	Gradle
Haskell	Cabal and Stack
Java	Gradle, Maven, Ant
Javascript	nodejs & npm
Kotlin	Gradle
Monorepo tooling	okbuck, Buck
.NET	NuGet, Paket
Objective-C	Cocoapods, Carthage
PHP	Composer
Python	Pip, Pipenv, requirements.txt
Ruby	Bundler
Rust	Cargo
Scala	SBT
Swift	Cocoapods, Carthage
C, C++	Archive Uploader

- スキャン可能な環境一覧
- 概ね有名どころのパッケージ管理ツールはカバーしている

情報源 : <https://github.com/fossas/fossa-cli>



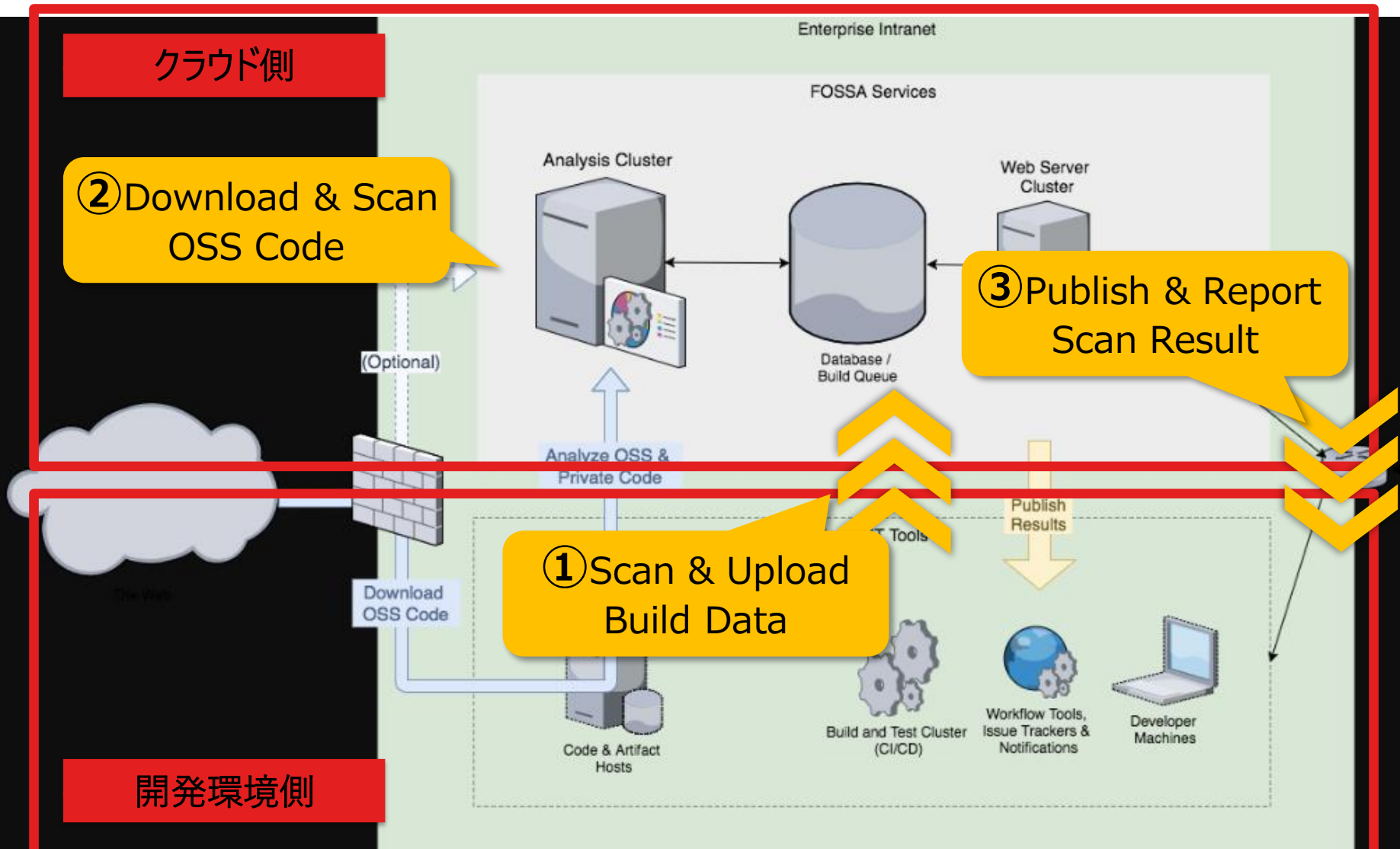
クラウド側

② Download & Scan  
OSS Code

③ Publish & Report  
Scan Result

① Scan & Upload  
Build Data

開発環境側

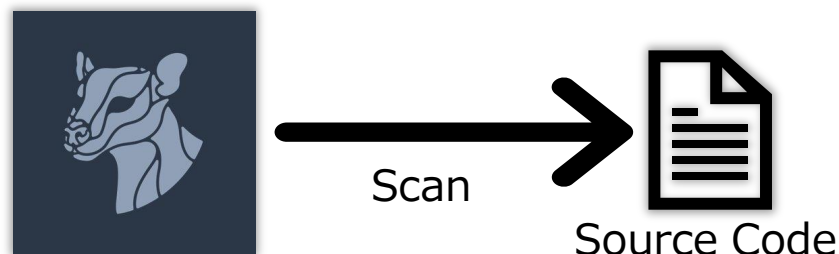




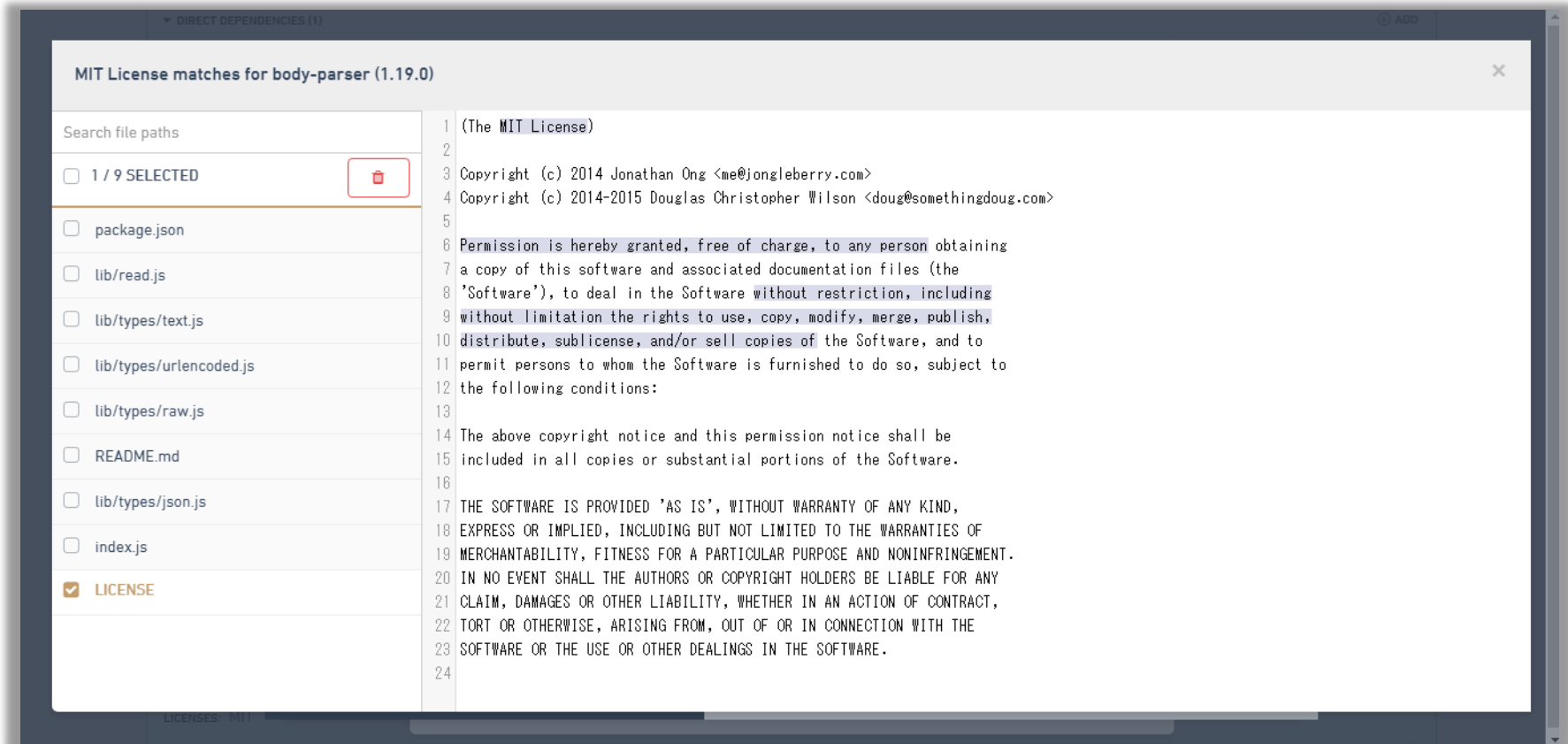
1. アップロードされたJSONに含まれるライブラリの識別子を基にOSSライブラリに対応するソースコードを取得する。



2. 取得したソースコードに対して、ライセンススキャンを行う。



## ■ 画面



<補足> FOSSA側でのライセンススキャン(OSSコードからのライセンス情報の抽出処理)については、ツールの仕様上ユーザ側での設定変更は不可と思われる。

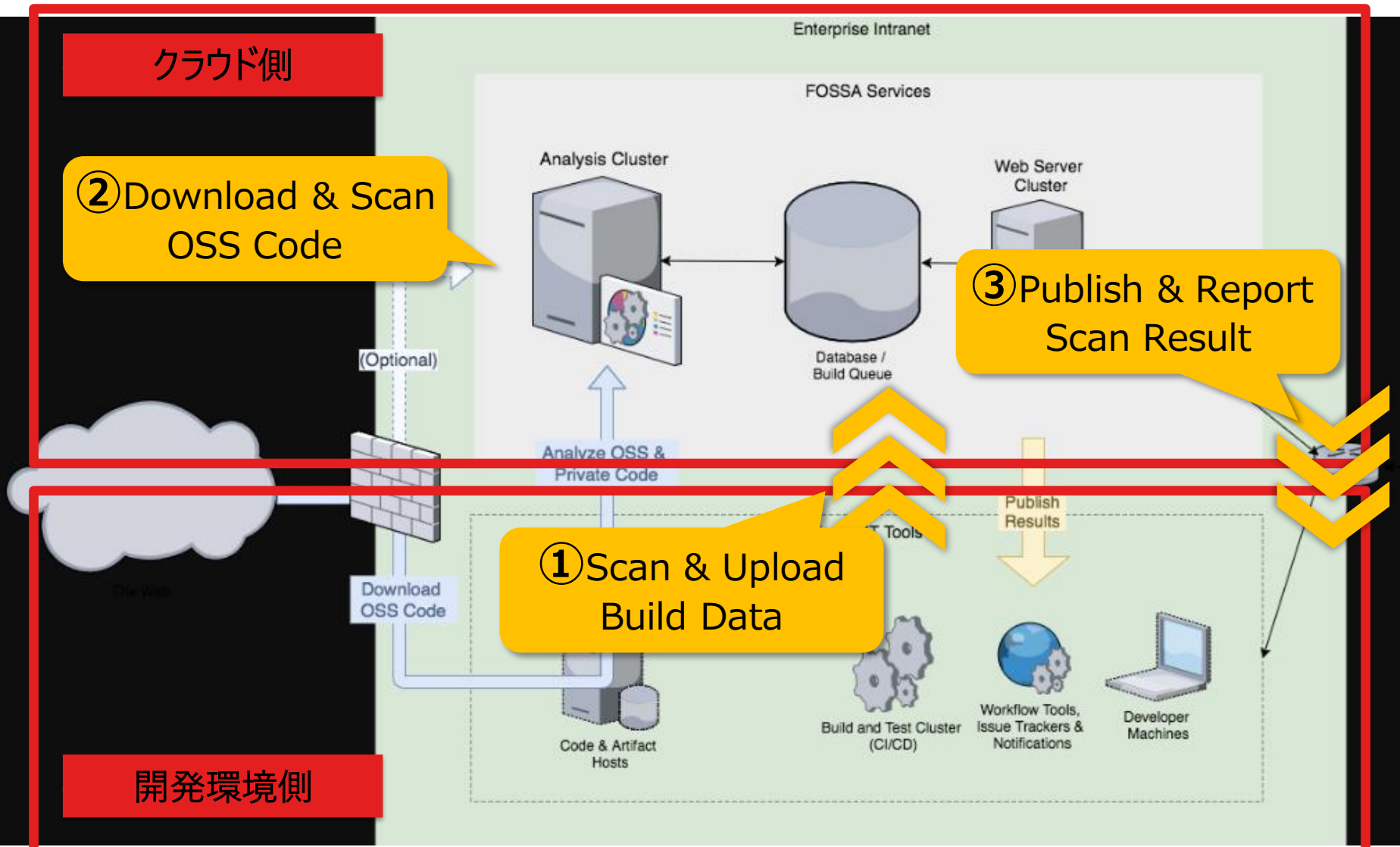
クラウド側

② Download & Scan  
OSS Code

③ Publish & Report  
Scan Result

① Scan & Upload  
Build Data

開発環境側



<https://docs.fossa.com/docs/architecture-overview>

## ■ アラート①

Issueタブでは、ポリシーに違反するライセンスが検出された際のアラートを確認することができます。

The screenshot shows the FOSSA web application interface. At the top, the navigation bar includes links for Projects, Issues (selected), Components, Policies, Docs, Support, and a Demo button. The main header displays the project name 'MvnJava' with a lock icon and a dropdown menu set to 'none'. Below this, a timestamp '161900 : Jun 16th 2020, 10:44 am' is shown. The main content area has tabs for SUMMARY, ISSUES (0), DEPENDENCIES (9), LICENSES (15), REPORTS, ACTIVITY, and SETTINGS. Under the ISSUES tab, there are filters for 'All Licensing Issues' (2), 'Flagged by Policy' (1), 'Denied by Policy' (0), and 'Unlicensed Dependencies' (1). The left sidebar shows a list of issues with columns for 'Active' (2), 'Exported' (0), and 'Resolved' (0). The first issue is 'No license found in Batik Parser' (2 minutes ago), and the second is 'Flagged: AGPL-3.0-only in iText' (14 minutes ago). The right sidebar contains a section titled 'Triaging Licensing Issues' with instructions on how to use the view.

FOSSA

Projects Issues Components Policies Docs Support Demo

MvnJava none

161900 : Jun 16th 2020, 10:44 am

SUMMARY ISSUES 0 DEPENDENCIES 9 LICENSES 15 REPORTS ACTIVITY SETTINGS

All Licensing Issues 2 Flagged by Policy 1 Denied by Policy 0 Unlicensed Dependencies 1 Options

Active 2 Exported 0 Resolved 0

Order issues by...

Search issues by package name

2 minutes ago  
**No license found in Batik Parser**  
Used by MvnJava

14 minutes ago  
**Flagged: AGPL-3.0-only in iText**  
Used by MvnJava

**Triaging Licensing Issues**

In this view, you can triage multiple issues across your organization at once. Similar issues are grouped together for easy viewing and bulk resolution.

To get started, select an **Issue Thread** on the left.

Open source management powered by FOSSA, Inc. © 2020  
vers: 2.15.8 - revid: e340ac123b

## ■ アラート②

GPL系のライセンスはアラートが出る

The screenshot displays a software licensing management interface. At the top, there are tabs for 'All Licensing Issues' (2), 'Flagged by Policy' (1), 'Denied by Policy' (0), and 'Unlicensed Dependencies' (1). The 'Flagged by Policy' tab is active, showing a list of issues. One issue is highlighted: 'Flagged: AGPL-3.0-only in iText', which occurred '26 minutes ago' and was 'Used by MvnJava'. A 'Resolve' button is visible next to the issue. A modal window titled 'Deep Scan Match: AGPL-3.0-only' is open, showing a list of affected dependencies (all are 'com/itextpdf/text/pdf/...') and a detailed view of the license text. The license text includes the GNU Affero General Public License version 3. Below the license text, there is a 'Licenses' section with three buttons: 'AGPL-3.0-ONLY' (499 Matches), 'APACHE-2.0' (53 Matches), and 'BSD-4-CLAUSE' (44 Matches). The 'AGPL-3.0-ONLY' button is highlighted with a red border.

All Licensing Issues 2 | Flagged by Policy 1 | Denied by Policy 0 | Unlicensed Dependencies 1 | Options ▾

Active 1 | Exported 0 | Resolved 0

Order issues by... ▾

Search issues by package name

26 minutes ago  
**Flagged: AGPL-3.0-only in iText**  
Used by MvnJava

Resolve ▾

**Deep Scan Match: AGPL-3.0-only**

Affected Dependencies

- com/itextpdf/text/pdf/...
- com/itextpdf/text/pdf/...
- com/itextpdf/text/pdf/...
- com/itextpdf/text/pdf/...
- com/itextpdf/text/pdf/...
- com/itextpdf/text/pdf/...
- com/itextpdf/text/pdf/...

iText (mvn)  
Homepage

A Free Java-PDF Library

Deep Scan Match

```
1 /*
2 *
3 * This file is part of the iText (R) project.
4 * Copyright (c) 1998-2017 iText Group NV
5 * Authors: Bruno Lowagie, Paulo Soares, et al.
6 *
7 * This program is free software; you can redistribute it and/or modify
8 * it under the terms of the GNU Affero General Public License version 3
9 * as published by the Free Software Foundation with the addition of the
10 * following permission added to Section 15 as permitted in Section 7(a):
11 * FOR ANY PART OF THE COVERED WORK IN WHICH THE COPYRIGHT IS OWNED BY
12 *
```

Licenses

- ☒ AGPL-3.0-ONLY 499 Matches
- ☐ APACHE-2.0 53 Matches
- ☐ BSD-4-CLAUSE 44 Matches

## ■ アラート③

ライセンスがないOSSは「Unlicensed Dependencies」としてアラートが出る

The screenshot displays the Hitachi Licensing Issues dashboard. At the top, there are tabs for 'All Licensing Issues' (2), 'Flagged by Policy' (1), 'Denied by Policy' (0), and 'Unlicensed Dependencies' (1). The 'Unlicensed Dependencies' tab is selected. On the left sidebar, there are filters for 'Active' (1), 'Exported' (0), and 'Resolved' (0). Below these are search and sorting options. The main content area shows a red alert icon with a question mark and the text 'No license found in Batik Parser'. Below this, a message states: 'These dependencies contain unlicensed code, which by default is copyrighted to the original author. You may not use these dependencies without first obtaining a license.' There are two buttons: 'Resolve' and 'Setup Issue Tracker'. Below the alert, there is a section titled 'Affected Dependency' with a button 'Edit Package'. It shows 'Batik Parser' with a 'mvn' tag and 'VERSION USED: 1.6'. Below this, there is a 'Licenses' section with a button 'Add a License' and the text 'No License Found'.

All Licensing Issues 2 | Flagged by Policy 1 | Denied by Policy 0 | Unlicensed Dependencies 1 Options ▾

Active 1 | Exported 0 | Resolved 0

Order issues by... ▾

Search issues by package name

10 minutes ago  
**No license found** in Batik Parser  
Used by MvnJava

**No license found in Batik Parser**

These dependencies contain unlicensed code, which by default is copyrighted to the original author. You **may not** use these dependencies without first obtaining a license.

✓ Resolve ▾ | ⚙ Setup Issue Tracker

📦 Affected Dependency Edit Package

**Batik Parser** mvn

Search the Web 🔍

Batik Parser

📁 Licenses

No License Found | + Add a License

## ■ アラート④

ポリシーに違反するライセンスが検出された場合は、以下のようなメールが届く



### 1 New Issues

found in [MvnJava \(1619004cef3ea6d1\)](#)

Issue Scan - June 16th 2020 @ 10:46am

[View Report in FOSSA »](#)

### 1 Flagged Projects (+1 New)

For more details and to resolve these issues, go to the [Project Overview](#) page.

To change notification settings, [click here](#).

FOSSA, Inc. © Copyright 2019

## ■ レポート

1. SELECT EXPORT FORMAT

HTML

MARKDOWN

PDF

CSV

PLAIN TEXT

2. CUSTOMIZE REPORT INFORMATION

☐ Project Declared Licenses ?

☐ License Summary ?

☒ Direct Dependencies ?

☒ Deep Dependencies ?

! Previews show a limited number of dependencies and licenses. Please download for a complete report.

Direct Dependencies

Package	Declared License(s)	Discovered License(s)
<a href="https://github.com/expressjs/express">express (4.17.1)</a> <small>(https://github.com/expressjs/express)</small>	<ul style="list-style-type: none"><li>MIT</li></ul> <div>Attribution Notice:  (The MIT License)  Copyright (c) 2009-2014 TJ Hol Copyright (c) 2013-2014 Roman Copyright (c) 2014-2015 Dougla  Permission is hereby granted, a copy of this software and as 'Software'), to deal in the So without limitation the right</div>	



- Good or 他ツールにない特徴
  - 依存OSSのライセンスをコードレベルで確認するSaaS
  - tl;dr Legalのライセンス責務をうまく統合
- 惜しいポイント
  - 自製コードのスニペットスキャンなどはなさそう
  - 有償機能がチラホラ
    - ポリシーのカスタマイズ etc.
- どんなプロジェクトで有効か？
  - パッケージマネージャでビルド
  - CI/CD
  - 基本OSS利用はAS-IS
  - 要ライセンス遵守（頒布有）

⇒ スマホアプリの開発は適しているのではないか？

⇒ WEBアプリのAGPLチェックにも良いか



**END**



※本文に記載の会社名、商品名は各社の商標、または登録商標です。