



エンジニアのためのOSSライセンス管理

～OSS管理ツールの池の水ぜんぶ抜く～

株式会社 日立ソリューションズ
OSSコンサルティンググループ
森下 大輔

本日のアジェンダ

はじめに
OSS管理ツールの池の水ぜんぶ抜く
クラウドサービスFOSSAについて



はじめに

森下 大輔

@OSSコンサルティンググループ

HITACHI
Inspire the Next

🌐 株式会社 日立ソリューションズ



Qiitaやっています
<https://qiita.com/d-morishita>

- MIT、Apache-2.0、GPL、AGPL、など
- OSI (Open Source Initiative) が定義

- 使っているOSSをすべて把握すること
- OSSライセンスを正しく把握すること
- ライセンスのルールに従うこと（責務を全うすること）

- 手間がかかる
 - ライセンスの確認には手間と時間がかかる
 - 開発スピードを落としたくない
- よく分からない
 - ライセンスは英語でよく分からない
 - 日本語にしても法律関連の文章で意味不明

- 手間がかかる
 - ライセンスの確認には手間と時間がかかる
 - 開発スピードを落としたくない
- よく分からない
 - ライセンスは英語でよく分からない
 - 日本語にしても法律関連の文章で意味不明

←ツール

←解釈共有

- さまざまなツール
 - 無償（フリー/OSS）
 - FOSSology
 - scancode-toolkit
 - LicenseFinder
 - など
 - 有償
 - Black Duck
 - WhiteSource
 - FlexNet Code Insight
 - など

1. TLDRLegal

- FOSSA社が公開しているOSSライセンスの要約を解りやすい形式で提供するWebサイト

2. OSADL License obligations checklist

- Open Source Automation Development Lab (OSADL) が公開しているライセンス義務条件データ

3. OSS License Open Data

- 日立が公開しているライセンス解釈データ

1. <https://tldrlegal.com/>

2. <https://www.osadl.org/Access-to-raw-data.oss-compliance-raw-data-access.0.html>

3. <https://github.com/Hitachi/open-license>

今日はここを深掘り

- 手間がかかる
 - ライセンスの確認には手間と時間がかかる
 - 開発スピードを落としたくない
- よく分からない
 - ライセンスは英語でよく分からない
 - 日本語にしても法律関連の文章で意味不明

←ツール

←解釈共有

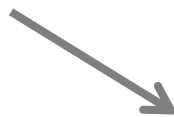
OSS管理ツールの池の水ぜんぶ抜く

- 今日の話
 - OSSライセンス管理のためのツールはどんなものがあるか
 - それらはどんなことができるか
 - どう使えば良いか

どんなツールがあるのか

オープンソースが世の中に広まっていく中でさまざまなツールが誕生
→ 全容が分かり辛くなっている（まるで公園の池のように…）

2004年に旧BlackDuck社が
OSSスキャンソリューションを発表



無償・有償問わず
多数のツールが誕生



まるで新種のように…

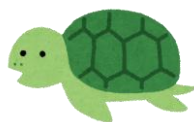


多数の機能を持ったツールも存在



まるで巨大魚のように…

ツールによっては珍しい
機能を持ったツールも



希少種のように…



たくさんあるね





開始10分ですが、
さっそく水を抜きます

FOSSology

licensee

LicenseFinder

AboutLibraries
(android)

scancode-toolkit

ninka

licensed

LicensePlist(iOS)

askalono

licenseclassifier

license-
checker(npm)

pip-licenses(pip)

lc

LiD

license maven
plugin(Maven)

php-legal-
licenses(composer)

go-license-detector

ORT

license gradle
plugin(Gradle)

go-licenses(Go)

BlackDuck

Insignary Clarity

Veracode SCA

Nexus

WhiteSource

FOSSA

WhiteHat SCA

Contrast OSS

FlexNet Code
Insight

Snyk

GitLab

CAST Highlight

FOSSID

JFrog Xray

yamory

CxSCA

~~全ツールについて詳細を解説~~
整理した上で全体像（何が出来るか）を解説

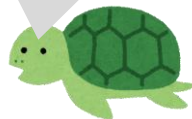
1. OSSとライセンスのスキャン
 - 依存関係（メタデータ）のスキャン
 - ライセンス文字列のスキャン
 - コードパターンのスキャン
2. ポリシーの設定とアラートの通知
 - GPL/AGPLの検出でメール送付するなど
3. ライセンスファイルの生成
 - 利用OSSすべてのライセンステキストまとめを生成

※ツールによって持っている機能が異なります

1 だけできます



1 と 2 できます



全部 できます



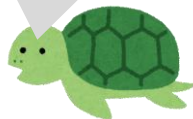
1. OSSとライセンスのスキャン
 - 依存関係（メタデータ）のスキャン
 - ライセンス文字列のスキャン
 - コードパターンのスキャン
2. ポリシーの設定とアラートの通知
 - GPL/AGPLの検出でメール送付するなど
3. ライセンスファイルの生成
 - 利用OSSすべてのライセンステキストまとめを生成

※ツールによって持っている機能が異なります

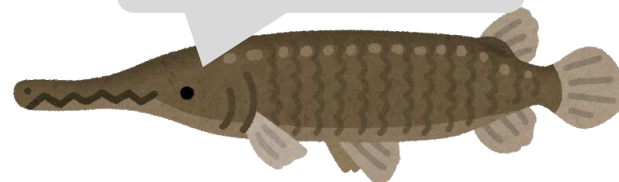
1 だけできます



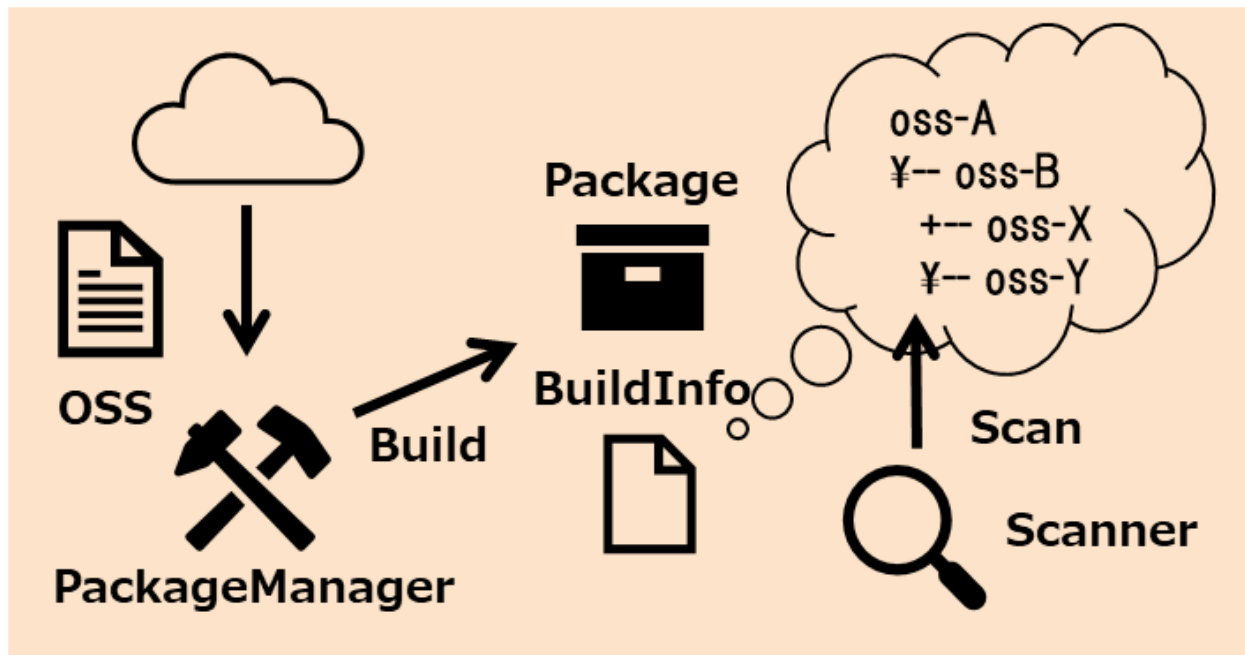
1 と 2 できます



全部 できます



- パッケージマネージャなどで依存モジュールとして設定したOSSライブラリの検出
- 無償・有償含め、本機能を持っているツールは多数存在

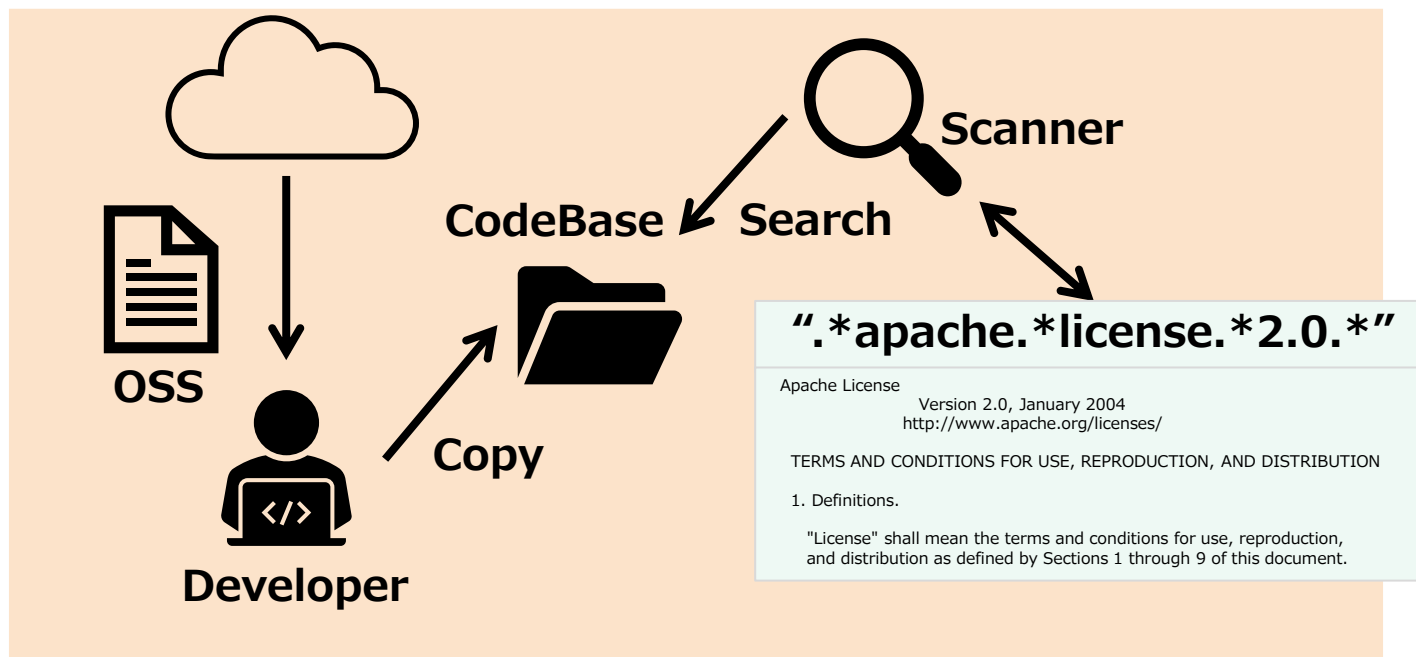


～パッケージマネージャの例～

Maven
Npm
Gradle
nuget
CocoaPods
...

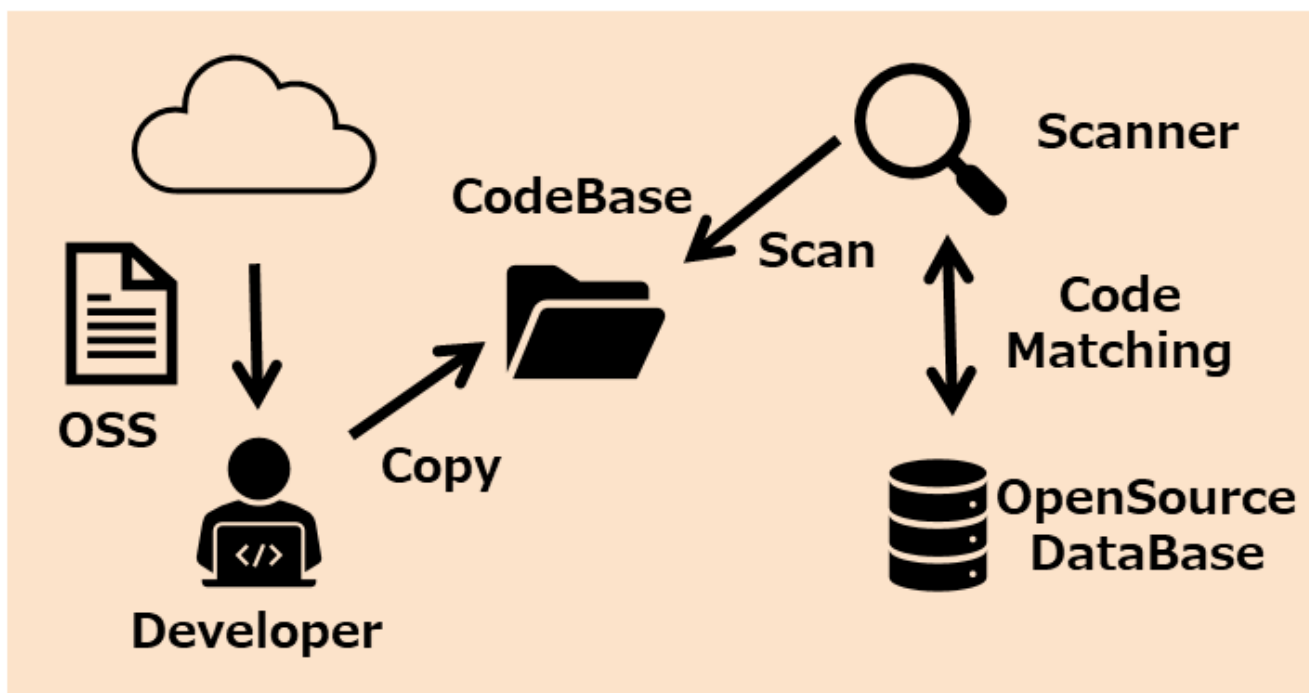
- ツールの例
 - 特定環境特化型
 - 特定の言語や環境に特化してOSSライセンスを調べるツール
 - ツールの例
 - license-checker(npm)
 - LicenseToolsPlugin(android)
 - など
 - 環境横断型
 - 複数言語（パッケージマネージャ）に対応したツール
 - ツールの例
 - LicenseFinder(pivotal)
 - Licensed(github)
 - など
- ツールによる違い
 - 検出対象
 - アプリケーションのパッケージ（npm、maven、…）
 - OSのパッケージ（rpm、deb、…）
 - ライセンスの判断材料
 - パッケージのメタデータ
 - 「LICENSE」や「README」などのファイル
 - ソースファイル（ライセンスヘッダ等）

- OSSライセンスと思われるテキスト（文字列）の検出
- 無償、有償含め、多数のツールが存在



- ツールの例
 - FOSSology
 - scancode-toolkit
 - Licensee
 - askalono
 - など
- ツールによる違い
 - 検出手段
 - 正規表現
 - テキスト類似度
 - 正確さを優先するもの、指摘漏れの回避を優先するものなど、さまざま
 - 著作権表示（コピーライト）、Email、URLなどを検出するものもある

- ソースファイルの内容をOSSデータベースと照合（マッチング）させて検出
- 基本的に有償ツールでのみ実施可能（OSSデータベース要）



- ツールの例 ※有償なので実際は色々なスキャンが可能です
 - BlackDuck
 - WhiteSource
 - FlexNet Code Insight
 - FOSSID
 - Insignary Clarity
- ツールによる違い
 - 検出の対象
 - ソースコード
 - 独自バイナリ
 - 検出の粒度
 - ファイル
 - スニペット（コードの一部であっても検出する）
 - OSS特定のレベル
 - OSSの特定は行わない（候補を出すのみ）
 - OSSの特定まで行う（OSSを一意に決定する）

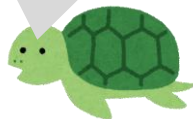
1. OSSとライセンスのスキャン
 - 依存関係（メタデータ）のスキャン
 - ライセンス文字列のスキャン
 - コードパターンのスキャン
2. ポリシーの設定とアラートの通知
 - GPL/AGPLの検出でメール送付するなど
3. ライセンスファイルの生成
 - 利用OSSすべてのライセンステキストまとめを生成

※ツールによって持っている機能が異なります

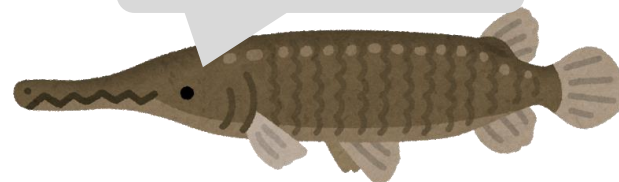
1 だけできます



1 と 2 できます



全部 できます



1. OSSとライセンスのスキャン


- 依存関係（メタデータ）のスキャン
- ライセンス文字列のスキャン
- コードパターンのスキャン

2. ポリシーの設定とアラートの通知

- GPL/AGPLの検出でメール送付するなど

3. ライセンスファイルの生成

- 利用OSSすべてのライセンステキストまとめを生成



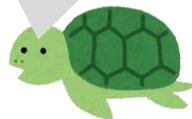
結局、何を
どうすべき？

※ツールによって持っている機能が異なります

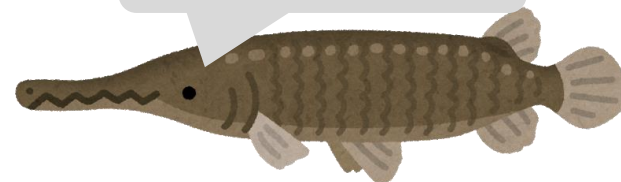
1 だけできます



1 と 2 できます



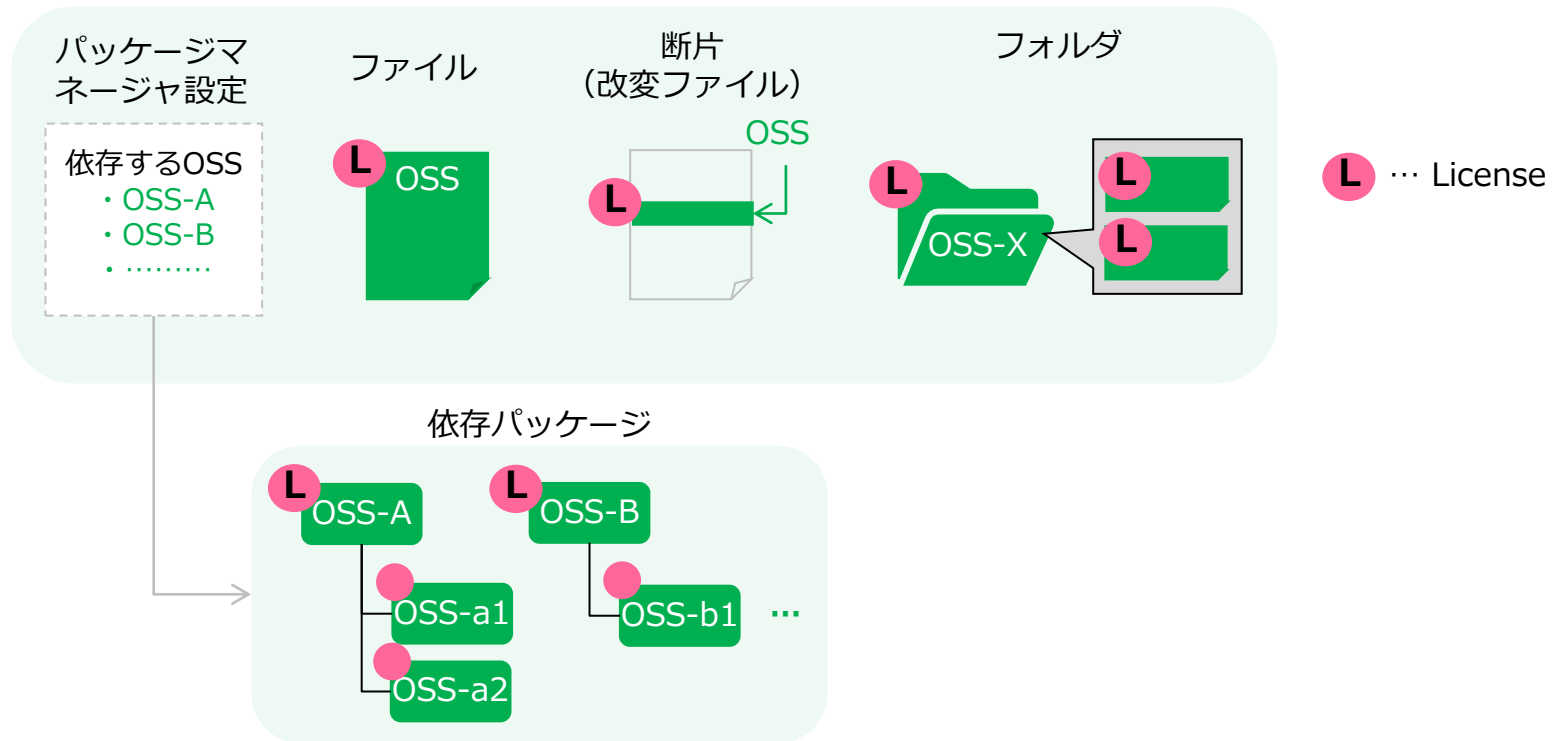
全部 できます



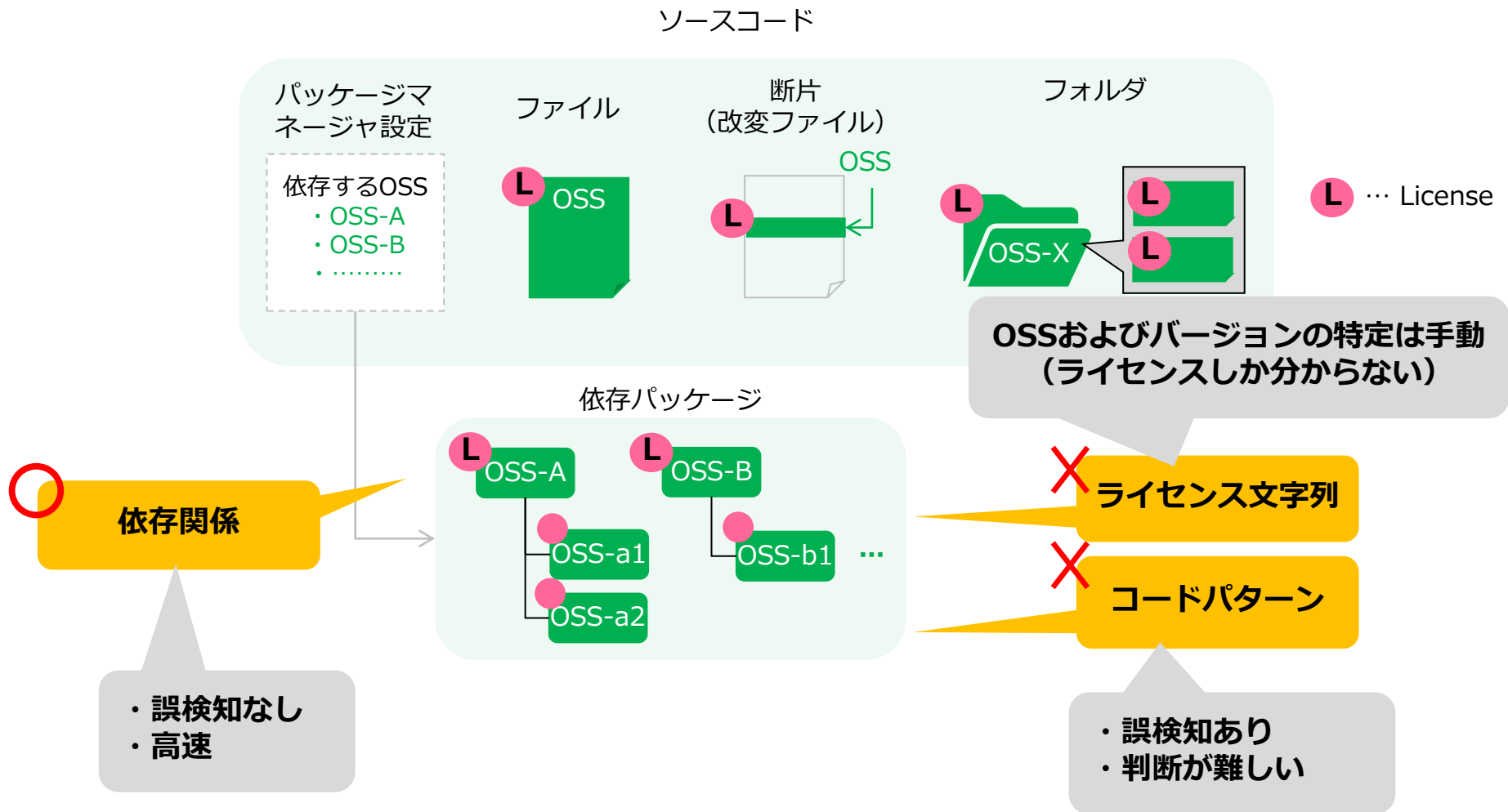
エンジニアのためのOSSライセンス管理戦略

以下のようなプロジェクトで考える

ソースコード

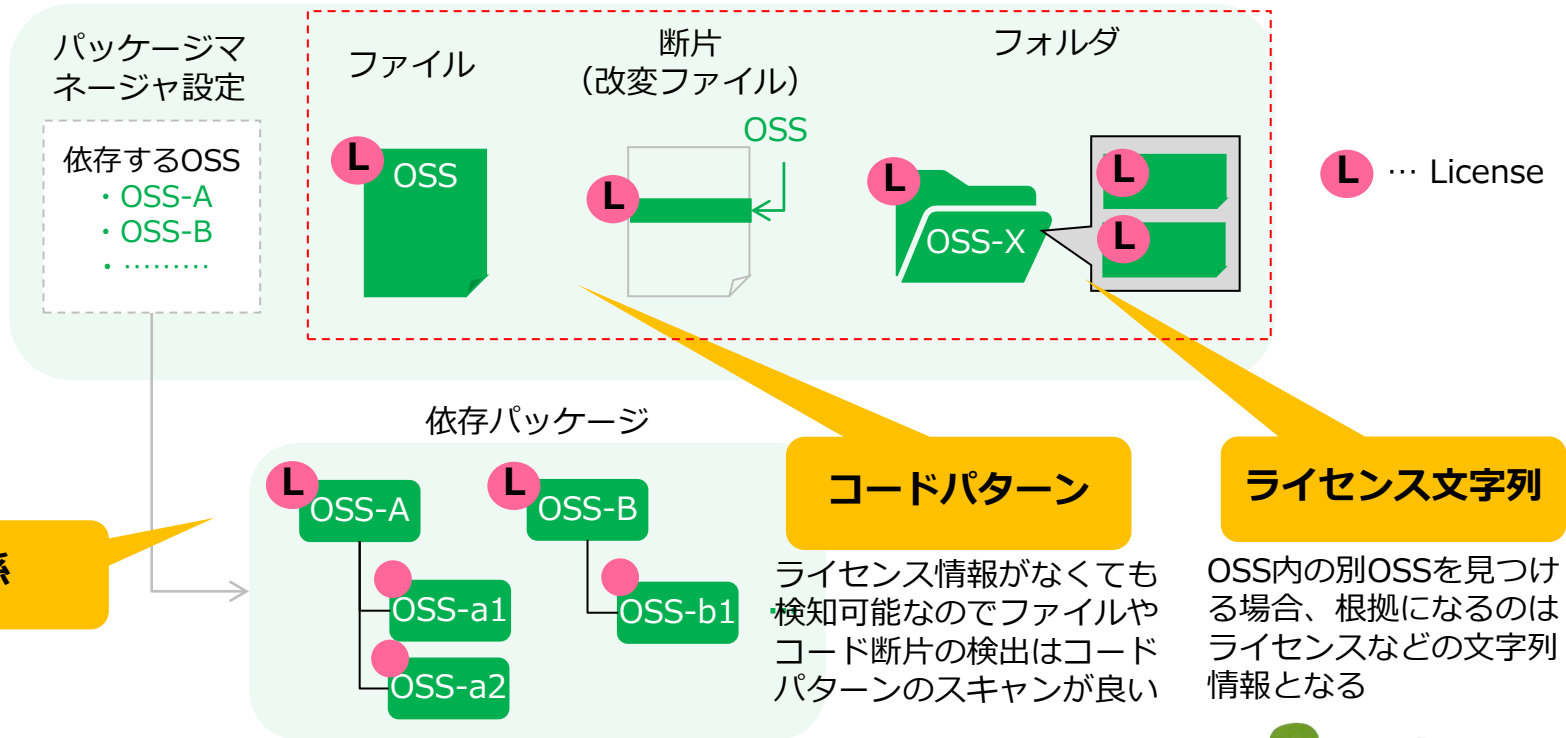


依存パッケージは依存関係（メタデータ）のスキャンで対応



残りの部分はどのようなアプローチでスキャンすべきか？

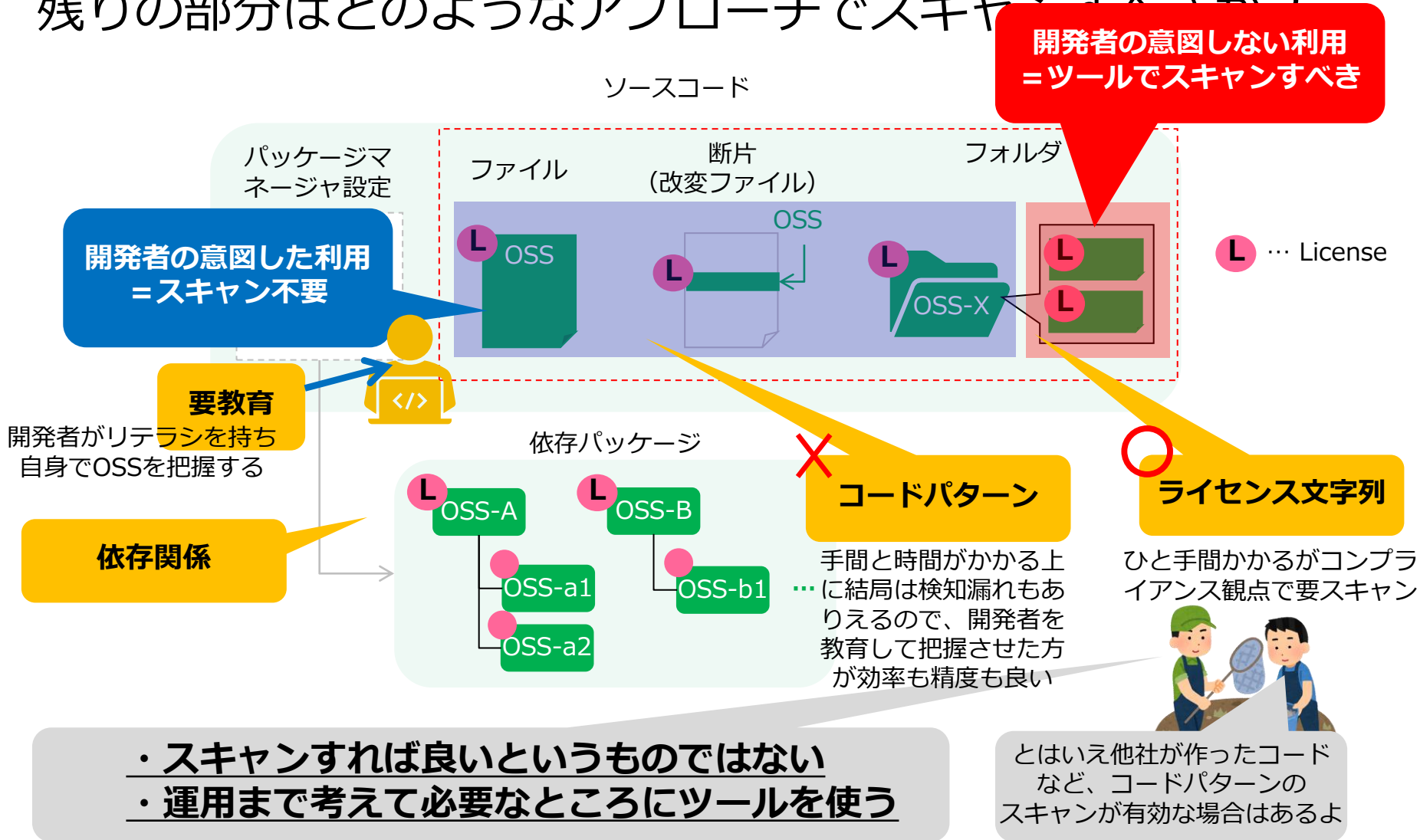
ソースコード



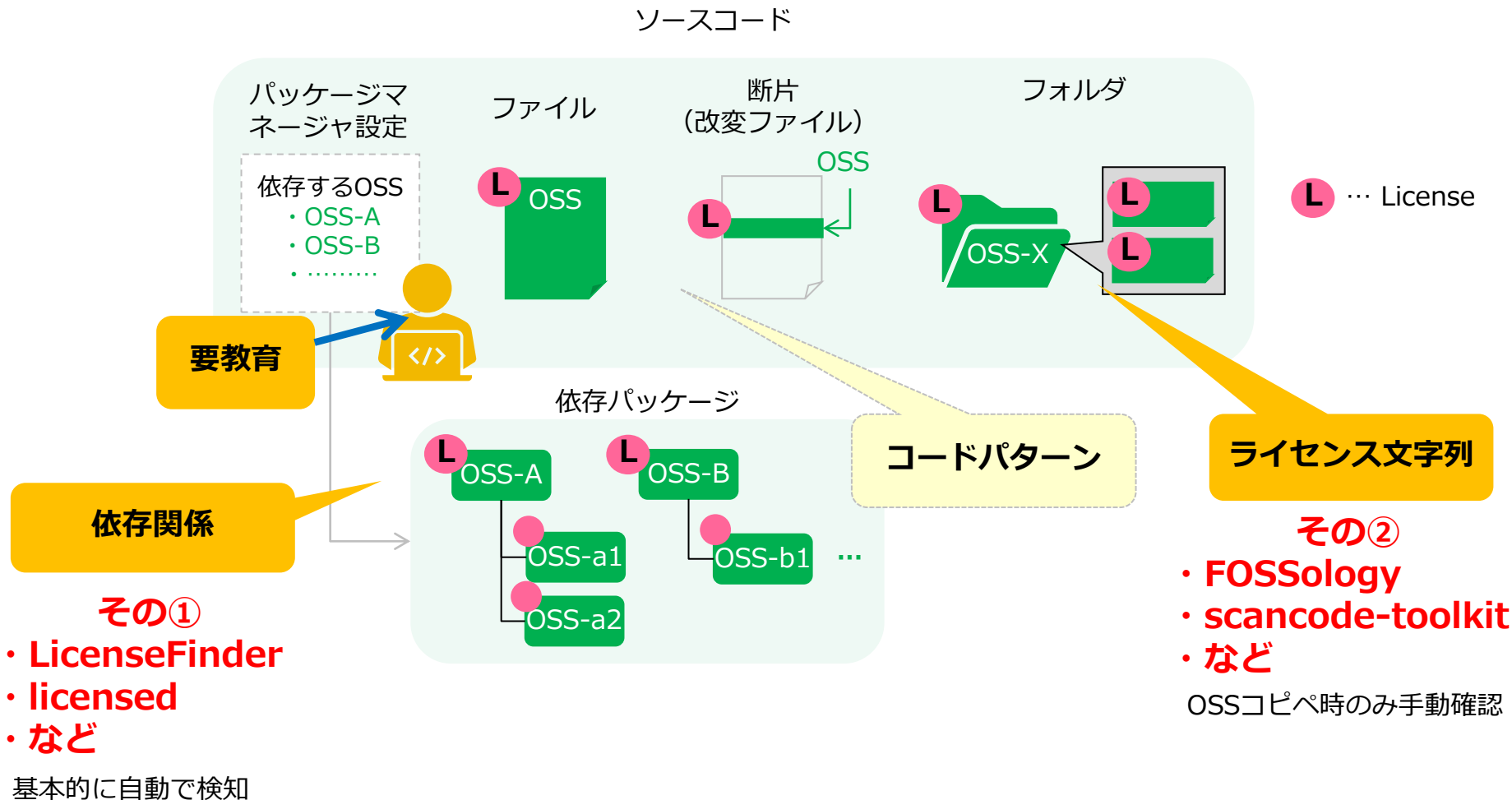
でもさ、そもそもスキャンってやる必要がある？



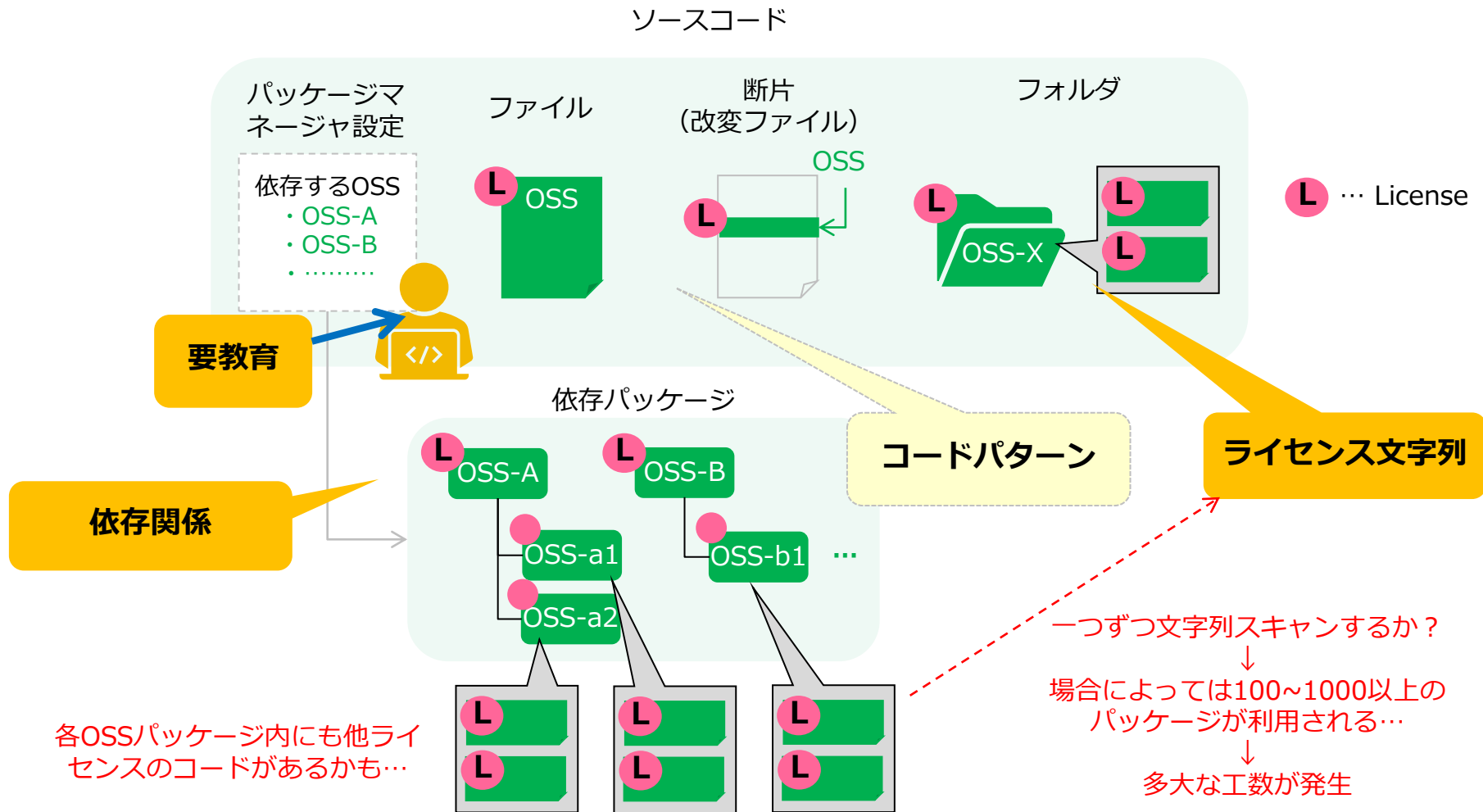
残りの部分はどうのようなアプローチでスキャンすべきか？



2パターンのスキャンアプローチが準備できていればOK

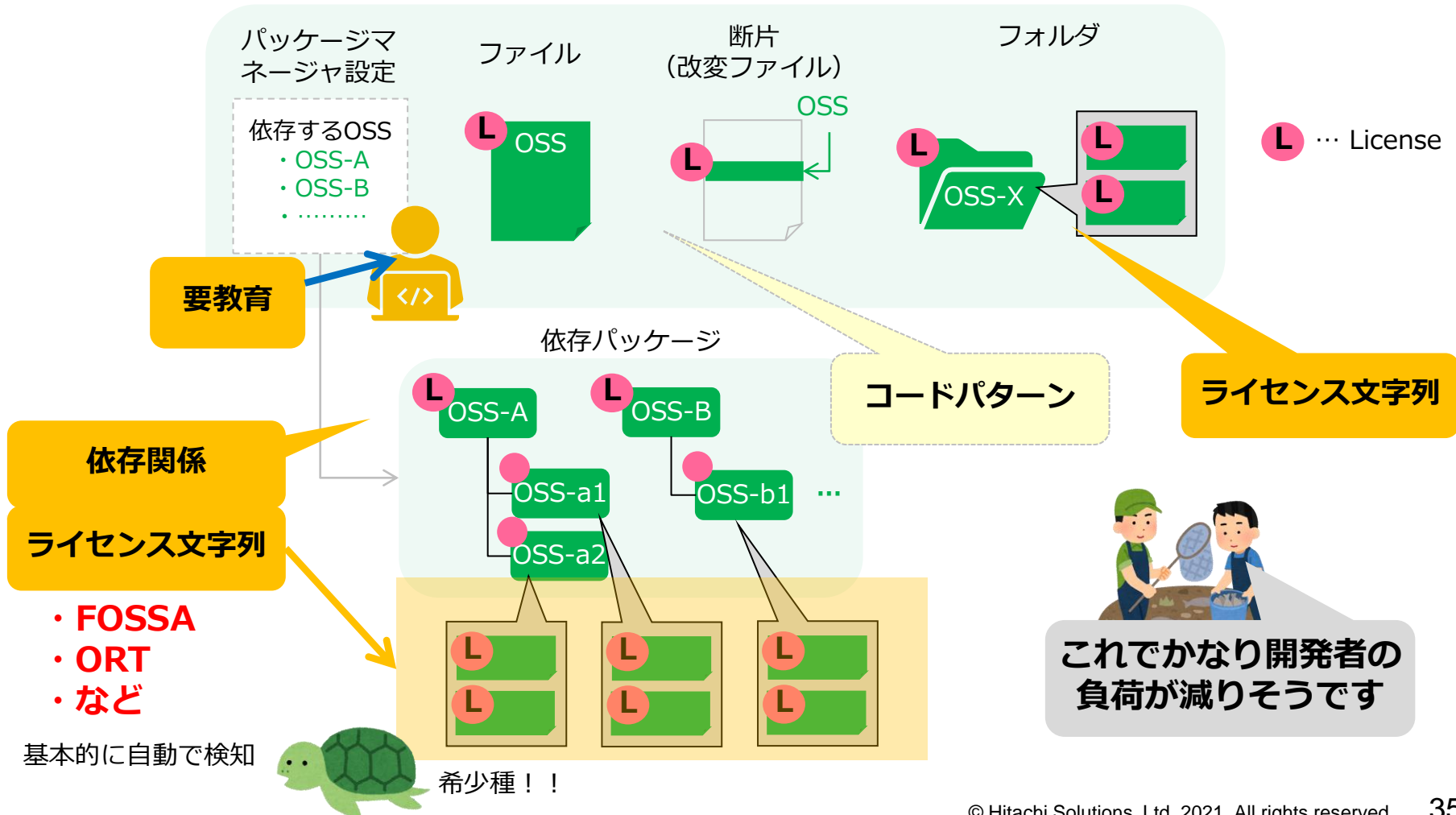


依存パッケージ内のOSSライセンスは大丈夫か？



依存チェックと同時に文字列スキャンしてくれるツールを使う

ソースコード



クラウドサービスFOSSAについて

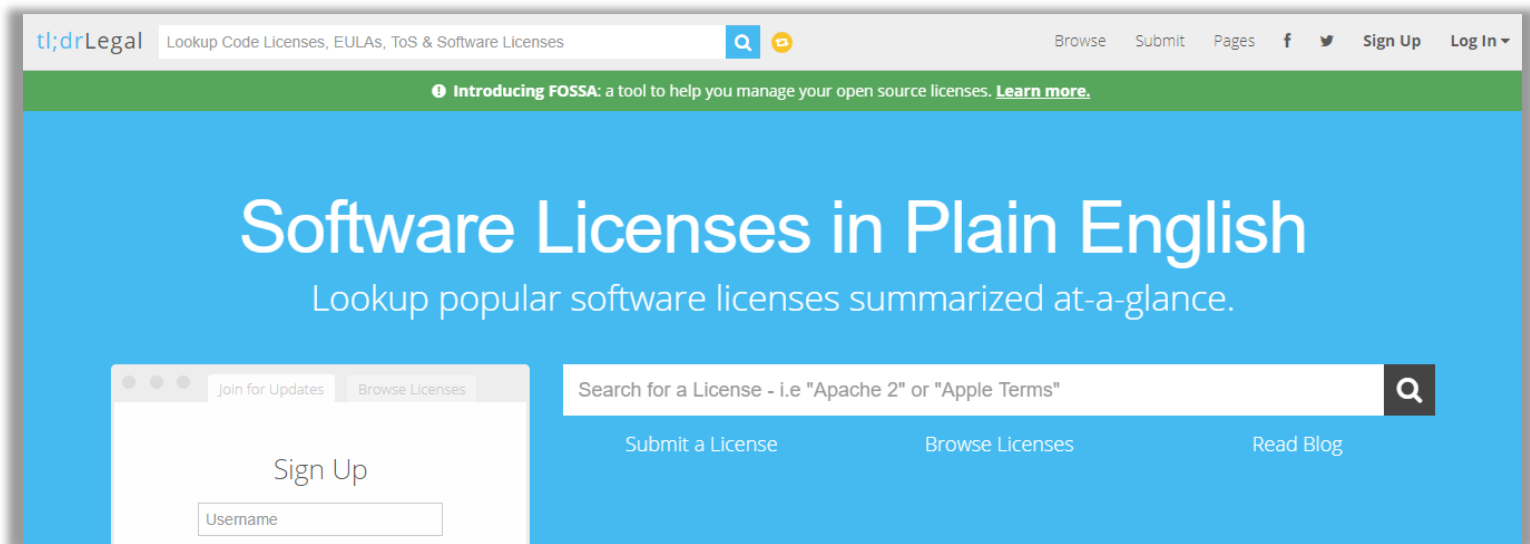
FOSSA

- OSSライセンス管理のためのクラウドサービス
- 個人利用は無料（制限つき）
- 「license scan」 バッジを提供



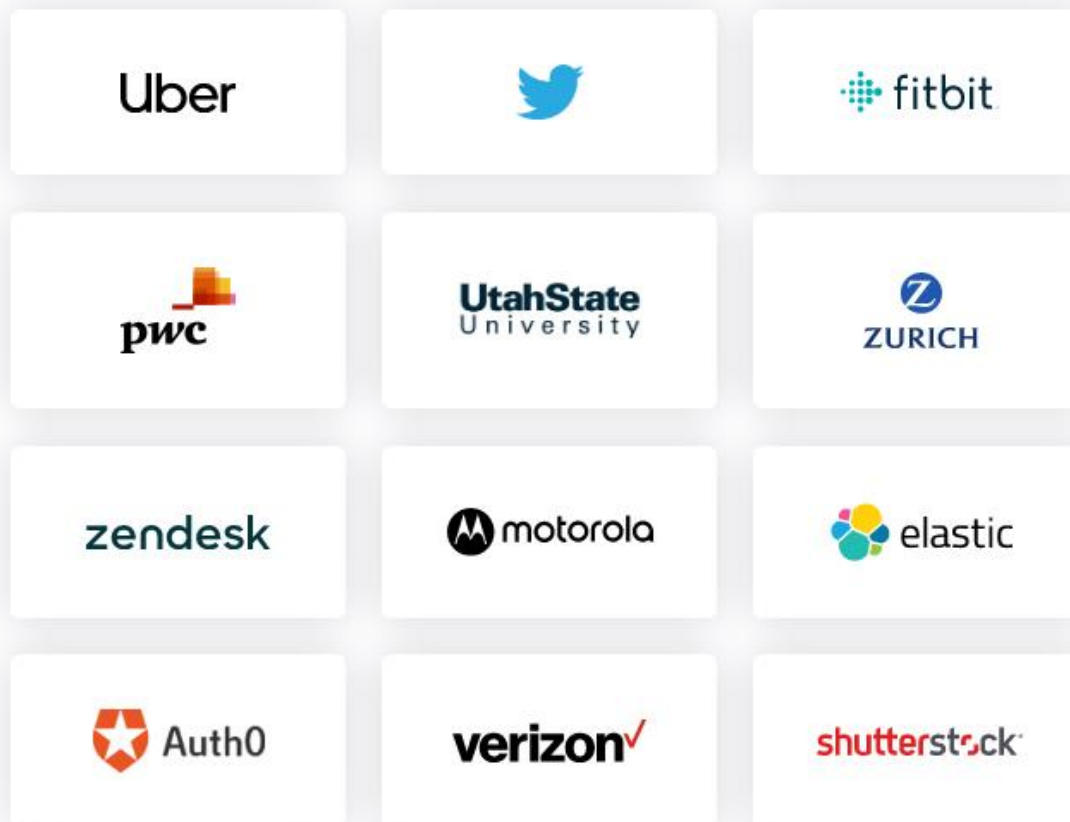
引用 : <https://fossa.com/customers/js-foundation>

- TLDRLegalを提供
- 業界の専門家と協力体制を構築
 - OSSライセンスの世界で著名な米国弁護士であるHeather Meeker氏がアドバイザーとして参画
 - Cloud Native Computing Foundation (CNCF)のCTOであるChris Aniszczyk氏がアドバイザーとして参画



<https://tldrlegal.com/>

- 全世界16000チームが採用



引用 : <https://fossa.com/customers>

- 機能
 - OSSとライセンスのスキャン
 - 依存関係（メタデータ）のスキャン
 - ライセンス文字列のスキャン
 - ポリシー・アラート
 - ライセンスファイルの生成

- 機能
 - OSSとライセンスのスキャン
 - 依存関係（メタデータ）のスキャン
 - ライセンス文字列のスキャン
 - ポリシー・アラート
 - ライセンスファイルの生成

- クイックインポート
- スキャナ連携（CI/CD連携） ※ベンダ推奨

- GitHub、GitLab、Bitbucketのアカウントと連携
- 自身が管理するリポジトリを指定してFOSSAにインポート

Quick Import
Automatically analyze from code host for easy initial results

← Go Back

GitHub Bitbucket.org

Gitlab Bitbucket Server

Upload Archive

GITHUB XIZHAO Search by Name IMPORT ALL **IMPORT 3**

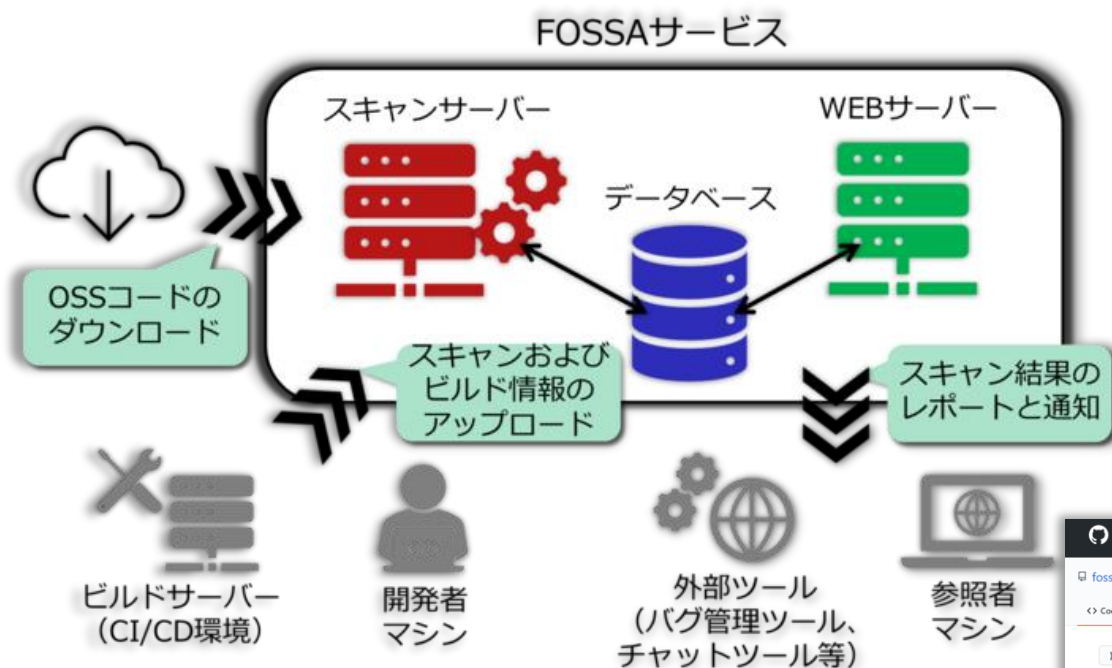
If you don't see your org listed, you may need to grant FOSSA access to it in Github's settings. Disconnect from Github

Submit badge PRs after import (public Github READMEs only)

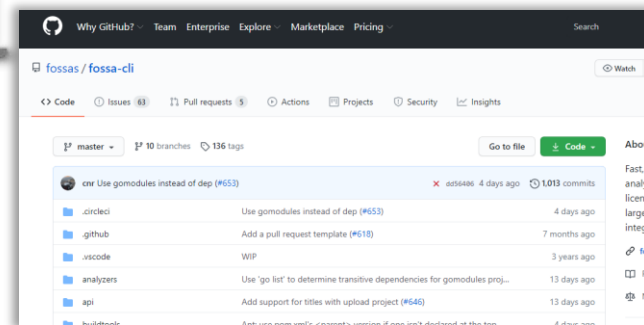
TITLE	BRANCH	LAST UPDATED
<input checked="" type="checkbox"/> fossa-installer	Imported: 2 years ago	
<input type="checkbox"/> altus-sdk-java	master	
<input checked="" type="checkbox"/> docsify	master	
<input checked="" type="checkbox"/> kaybinwang.github.io	master	
<input checked="" type="checkbox"/> node-sourcegraph	master	
<input type="checkbox"/> react-playground-vscode	master	
<input type="checkbox"/> transactional-email-templates	master	
<input type="checkbox"/> vitess	master	

引用 : <https://docs.fossa.com/docs/quick-import>

- 開発環境 (開発PC、CI環境など) でスキャナを実行
- スキャナがスキャン結果をサーバに送信



スキャナはOSSです。

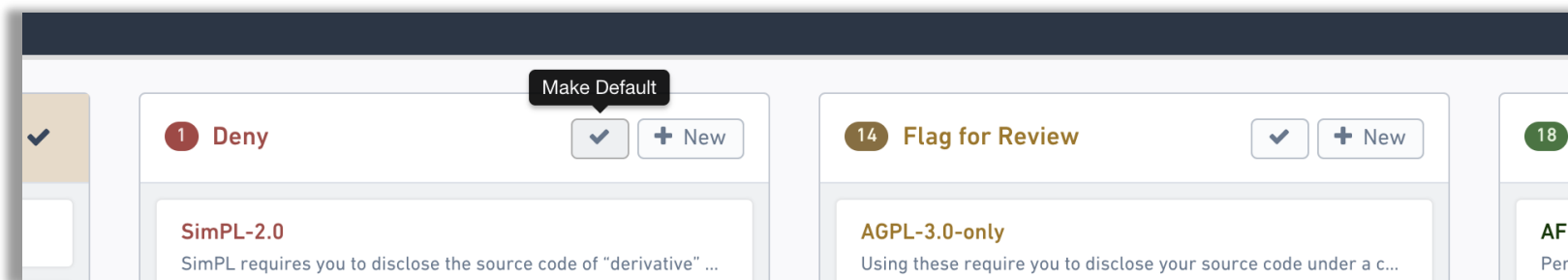


<https://github.com/fossas/fossa-cli>

- 機能
 - OSSとライセンスのスキャン
 - 依存関係（メタデータ）のスキャン
 - ライセンス文字列のスキャン
 - **ポリシー・アラート**
 - ライセンスファイルの生成

- FOSSAのポリシーおよびスキャン結果の確認
 - Policies画面
 - Issue画面

- ポリシーを利用してコンプライアンス違反の可能性を検出可能
- 専門家が監修した3種類のポリシーがプリセットされている
 - Standard Bundle Distribution
 - Single-Binary Distribution
 - Website/Hosted Service
- ポリシーはカスタマイズも可能



引用 : <https://docs.fossa.com/docs/configuring-default-policy-rules>

- ポリシーに違反している事象の列挙
- 問題に関わる情報の提供
- Jiraへのチケット作成機能

The screenshot displays a software issue tracking interface. On the left, a sidebar shows a list of issues with filters for 'Active 3', 'Exported 0', and 'Resolved 0'. The issues listed are:

- 6 days ago: **No license found in Batik Parser**, Used by MvnJava
- an hour ago: **Flagged: AGPL-3.0-or-later in JPMMML evalua...**, Used by MvnJava
- an hour ago: **Flagged: AGPL-3.0-only in JPMMML evaluator**, Used by MvnJava

The main panel shows a detailed view of the issue: **Flagged: AGPL-3.0-or-later in JPMMML evaluator**. The description states: "These packages contain code files that may require you to disclose your source code under a compatible license, unless they're distributed and run as completely separate processes & packages. AGPL also contains provisions requiring delivery of installation information for consumer devices (which may be inconsistent with use in closed systems)." Below the description are buttons for 'Resolve' and 'Setup Issue Tracker'. A 'Deep Scan Match: AGPL-3.0-or-later' section shows a code snippet with a license notice highlighted in yellow:

```
1 /*
2  * Copyright (c) 2013 Villu Ruusmann
3  *
4  * This file is part of JPMMML-Evaluator
5  *
6  * JPMMML-Evaluator is free software: you can redistribute it and/or modify
7  * it under the terms of the GNU Affero General Public License as published
8  * by the Free Software Foundation, either version 3 of the License, or
9  * (at your option) any later version.
10 *
11 * JPMMML-Evaluator is distributed in the hope that it will be useful,
```

- 機能
 - OSSとライセンスのスキャン
 - 依存関係（メタデータ）のスキャン
 - ライセンス文字列のスキャン
 - ポリシー・アラート
 - ライセンスファイルの生成

- カスタマイズ性が高く実用性に優れたレポートを生成可能

The image shows a workflow from a source page to a generated report. On the left is a screenshot of the Docker website's 'Components & Licenses' page. A yellow arrow points from this page to a larger screenshot of a FOSSA-generated report titled '3rd-Party Software for Docker Engine Enterprise'. The report includes a summary table of third-party software packages and their licenses.

Docker社の例

3rd-Party Software for Docker Engine Enterprise

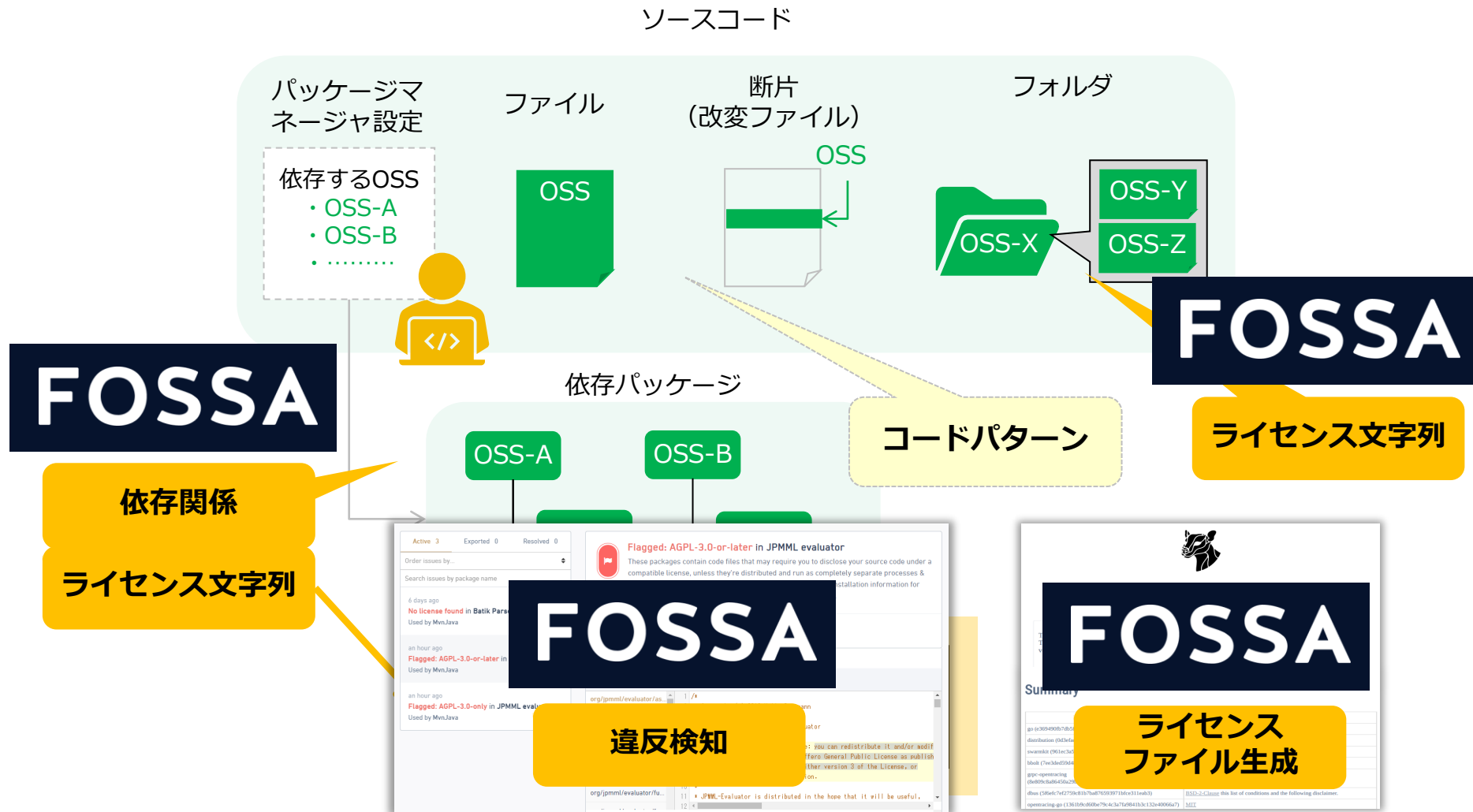
The following 3rd-party software packages may be used by or distributed with **Docker Engine Enterprise**. This document was automatically generated by FOSSA on 10/21/19; any information relevant to third-party vendors listed below are collected using common, reasonable means.

Summary

Package	Licenses
go (e369490fb7db5f2d42bb0e8ee19b48378dee0ebf)	BSD-3-Clause
distribution (0d3efadf0154c2b8a4e7b6621fff9809655cc580)	Apache-2.0
swarmkit (961ec3a56b7b6c311a2137b6a398f9d778fba94b)	Apache-2.0
bbolt (7ee3ded59d4835e10f3e7d0f7603c42aa5e83820)	MIT
grpc-opentracing (8e809c8a86450a29b90dcc9efbf062d0fe6d9746)	BSD-3-Clause
dbus (5f6efc7ef2759c81b7ba876593971bfce311eab3)	BSD-2-Clause this list of conditions and the following disclaimer.
opentracing-go (1361b9cd60be79c4c3a7fa9841b3c132e40066a7)	MIT

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

FOSSAなら全体のスキャン→違反検知→ライセンスファイル生成まで一気通貫



- 主要な言語/パッケージマネージャをサポート
 - npm、Maven、Gradle、pip、Nuget、CocoaPods、など
- 主要な外部ツールとの統合をサポート
 - GitHub、GitLab、Bitbucket、Jira、Slack、など
- 有償版はOSS脆弱性管理の機能もサポート

詳細はFOSSAのドキュメントを参照ください：<https://docs.fossa.com/docs>

- OSS管理ツールは整理する以下の機能に分解される
 - OSSとライセンスのスキャン
 - 依存関係（メタデータ）のスキャン
 - ライセンス文字列のスキャン
 - コードパターンのスキャン
 - ポリシー設定とアラート通知
 - ライセンスファイルの生成
- 管理の戦略
 - スキャンすれば良いというものではない
 - 適材適所のスキャンアプローチ
 - 違反の検知やライセンス生成はツールで自動化
- 具体的な管理施策（例）
 - FOSSAでプロジェクトを管理

END



※本資料に記載の会社名、商品名、ロゴ等は各社の商標または登録登録です。