HITACHI
Inspire the Next

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

HITACHI
Inspire the Next

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

HITACHI
Inspire the Next

はじめに

自己紹介

HITACHI
Inspire the Next

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やってます
https://qiita.com/d-morishita

（念のため）OSSライセンスとは

HITACHI
Inspire the Next

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

OSSライセンス”管理”とは

- 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）

エンジニアにとってのOSSライセンス管理

HITACHI
Inspire the Next

- 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

エンジニアにとってのOSSライセンス管理

HITACHI
Inspire the Next

- 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ライセンス管理のためのツール

HITACHI
Inspire the Next

- 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

OSSライセンスの解釈共有サービス・ツール

HITACHI
Inspire the Next

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

エンジニアにとってのOSSライセンス管理

HITACHI
Inspire the Next

今日はここを深堀り

- 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

←ツール

- 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

←解釈共有

HITACHI
Inspire the Next

OSS管理ツールの池の水ぜんぶ抜く

OSS管理ツールの池の水ぜんぶ抜く

HITACHI
Inspire the Next

- 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

HITACHI
Inspire the Next

どんなツールがあるのか

OSSライセンス管理のためのツール

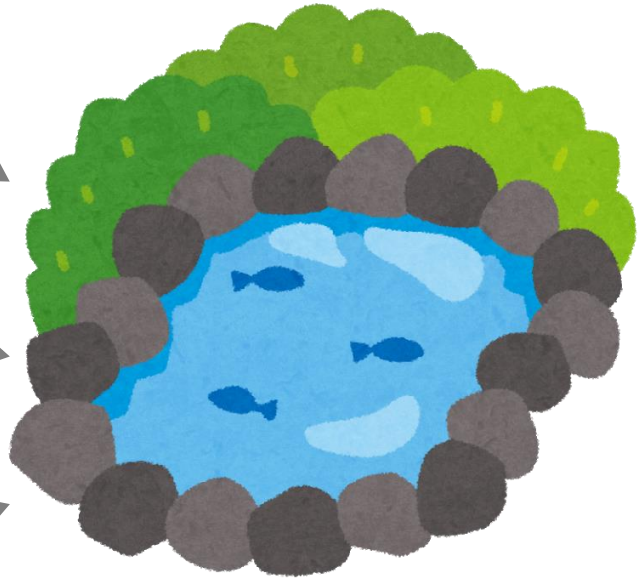
HITACHI
Inspire the Next

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

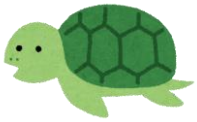
まるで新種のように…



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…

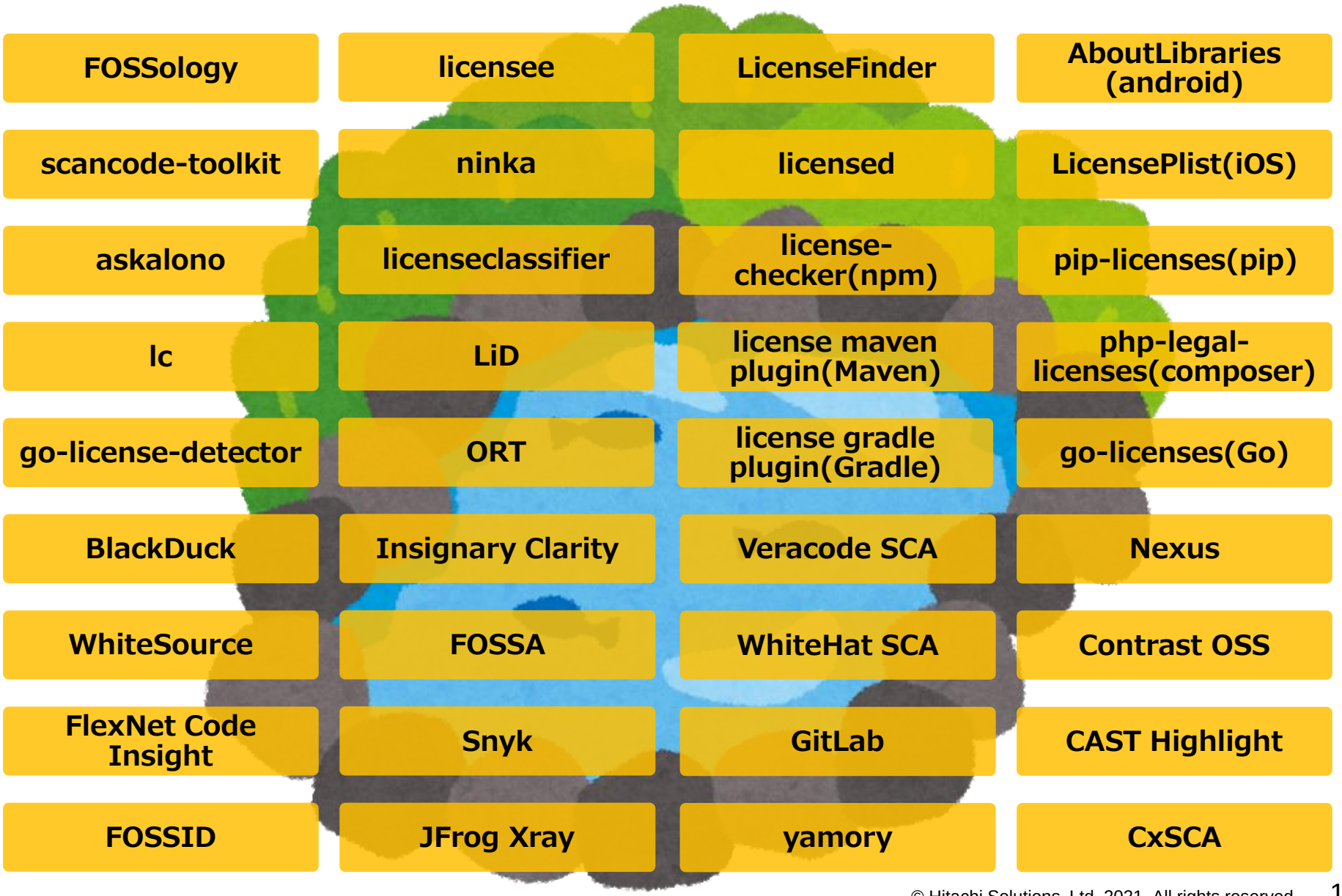
ツールによっては珍しい
機能を持ったツールも



希少種の
ように…

池の水ぜんぶ抜いてみた

HITACHI
Inspire the Next



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

何ができるのか？（ライセンス関連）

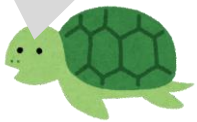
HITACHI
Inspire the Next

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

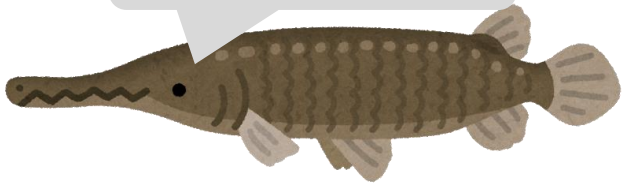
※ツールによって持っている機能が異なります

１だけできます

１と２できます



全部できます



何ができるのか？（ライセンス関連）

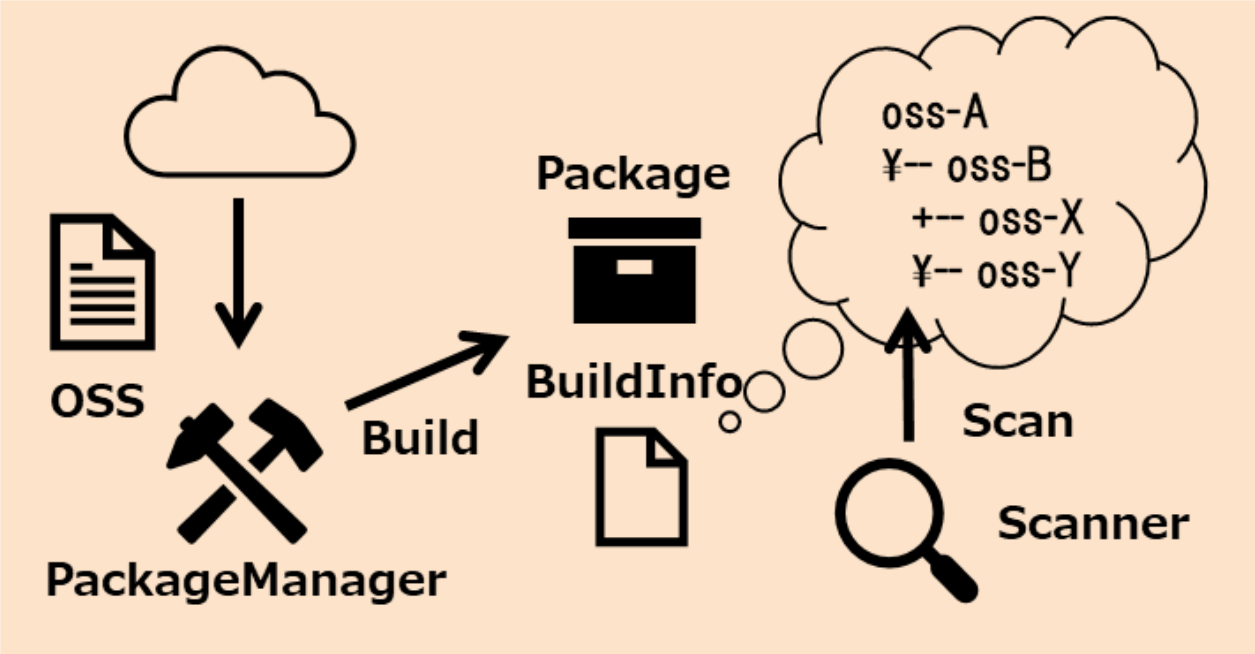
HITACHI
Inspire the Next

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

依存関係（メタデータ）のスキャンとは

- 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の例～

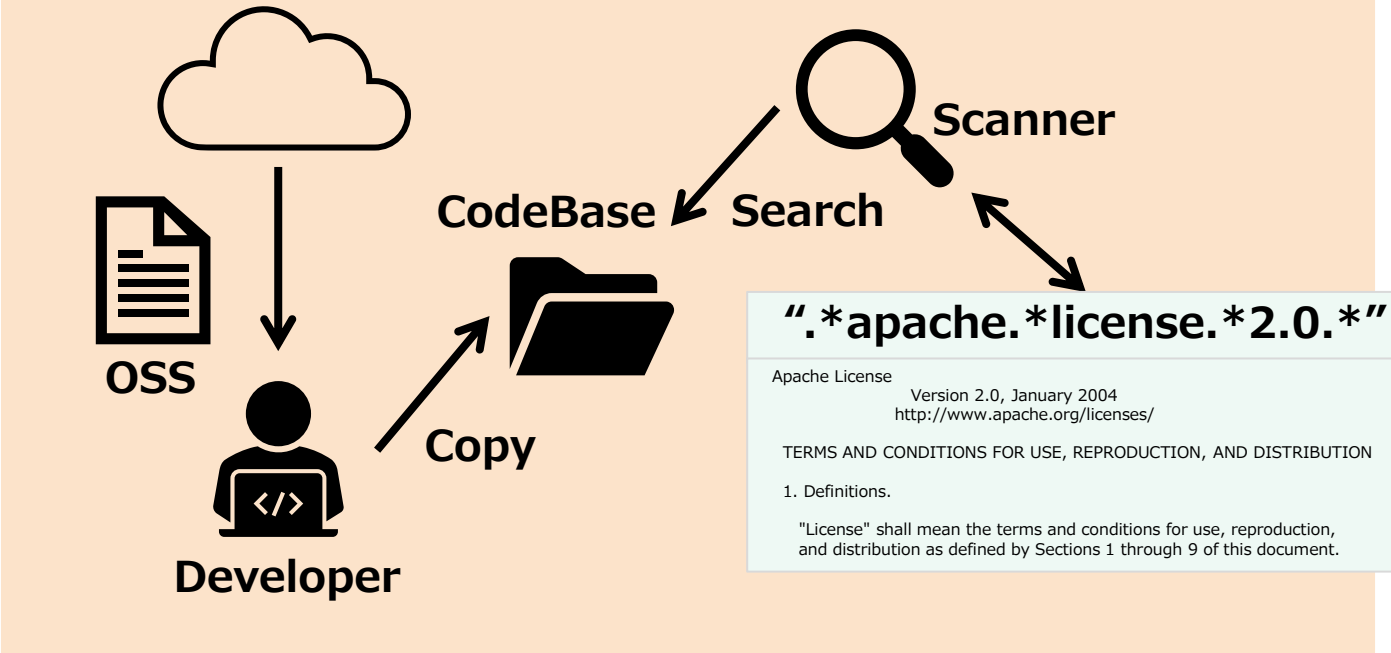
Maven
Npm
Gradle
nuget
CocoaPods
…

依存関係（メタデータ）のスキャン 補足

- 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）

ライセンス文字列のスキャンとは

- 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



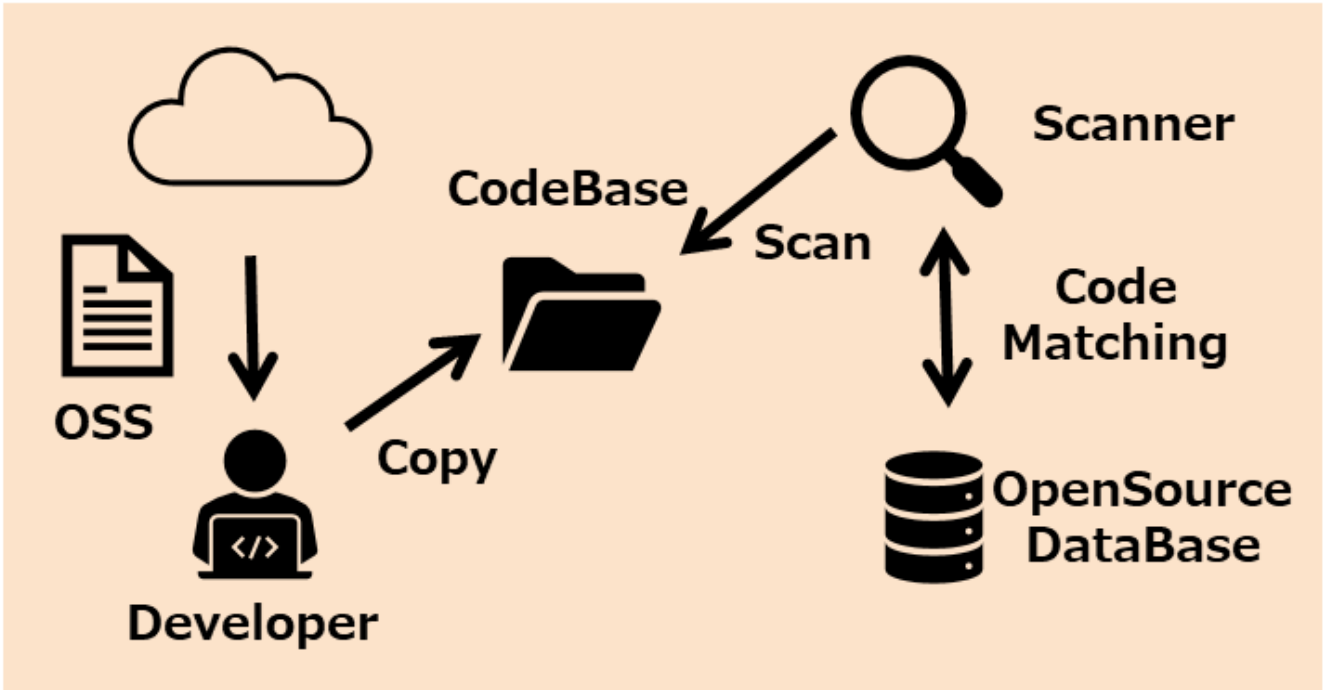
ライセンス文字列のスキャン 補足

HITACHI
Inspire the Next

- 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

コードパターンのスキャンとは

- 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）



コードパターンのスキャン 補足

- 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（コードの一部分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）

何ができるのか？（ライセンス関連）

HITACHI
Inspire the Next

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

何ができるのか？（ライセンス関連）

HITACHI
Inspire the Next

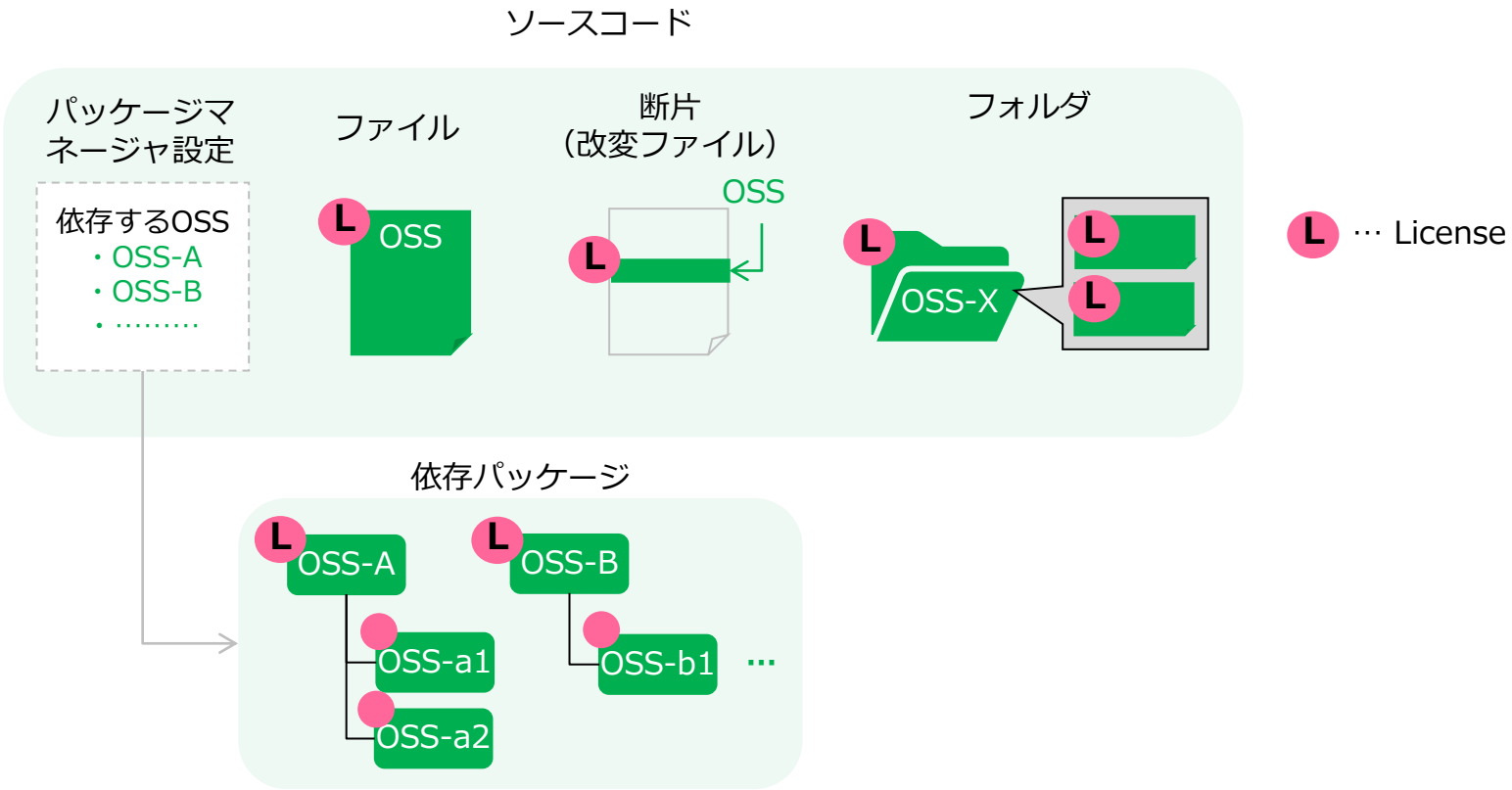
1. OSSとライセンスのスキャン
   - 依存関係（メタデータ）のスキャン
   - ライセンス文字列のスキャン
   - コードパターンのスキャン
2. ポリシーの設定とアラートの通知
   - GPL/AGPLの検出でメール送付するなど
3. ライセンスファイルの生成
   - 利用OSSすべてのライセンステキストまとめを生成

※ツールによって持っている機能が異なります

HITACHI
Inspire the Next

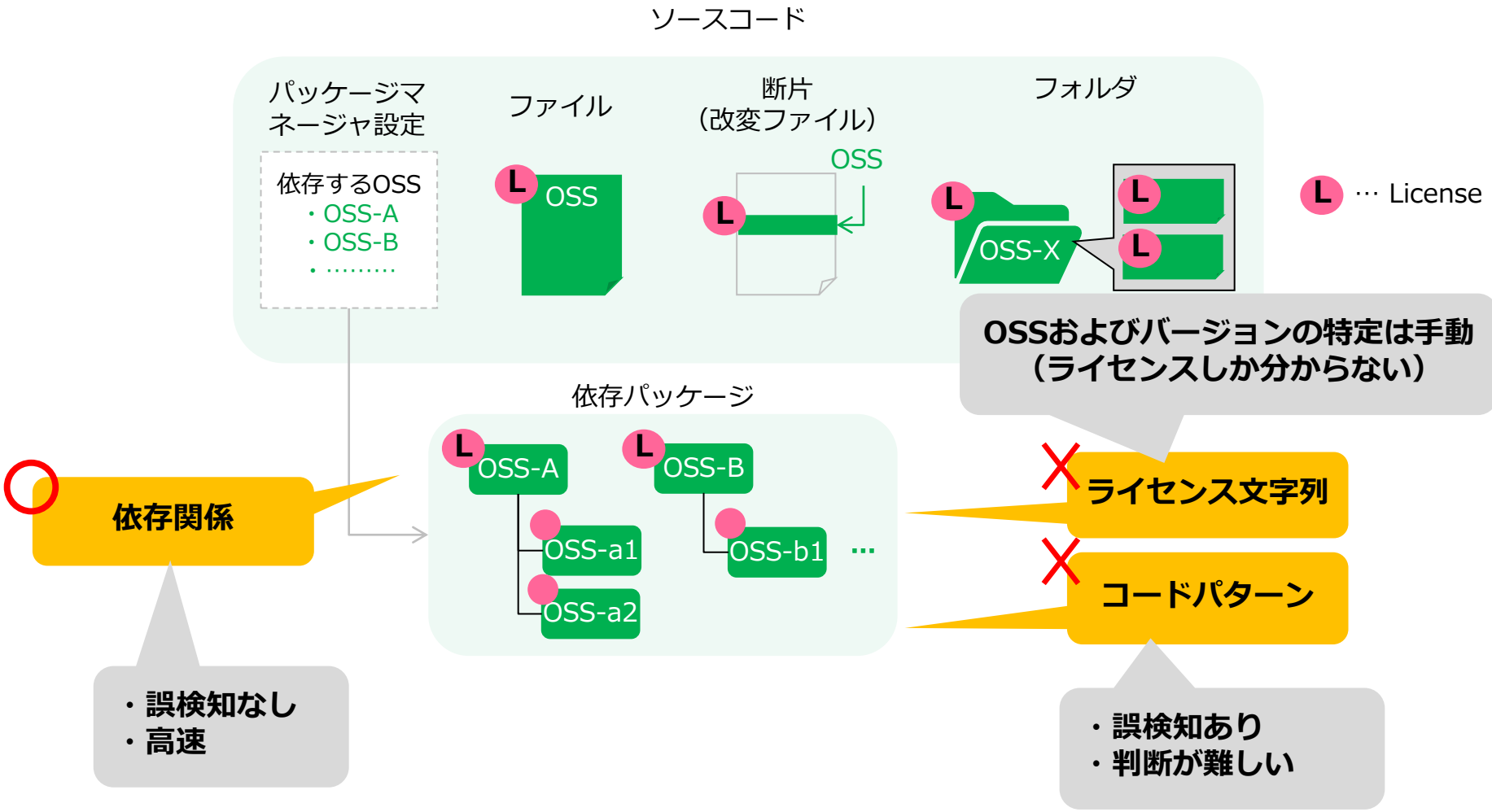
エンジニアのためのOSSライセンス管理戦略

以下のようなプロジェクトで考える



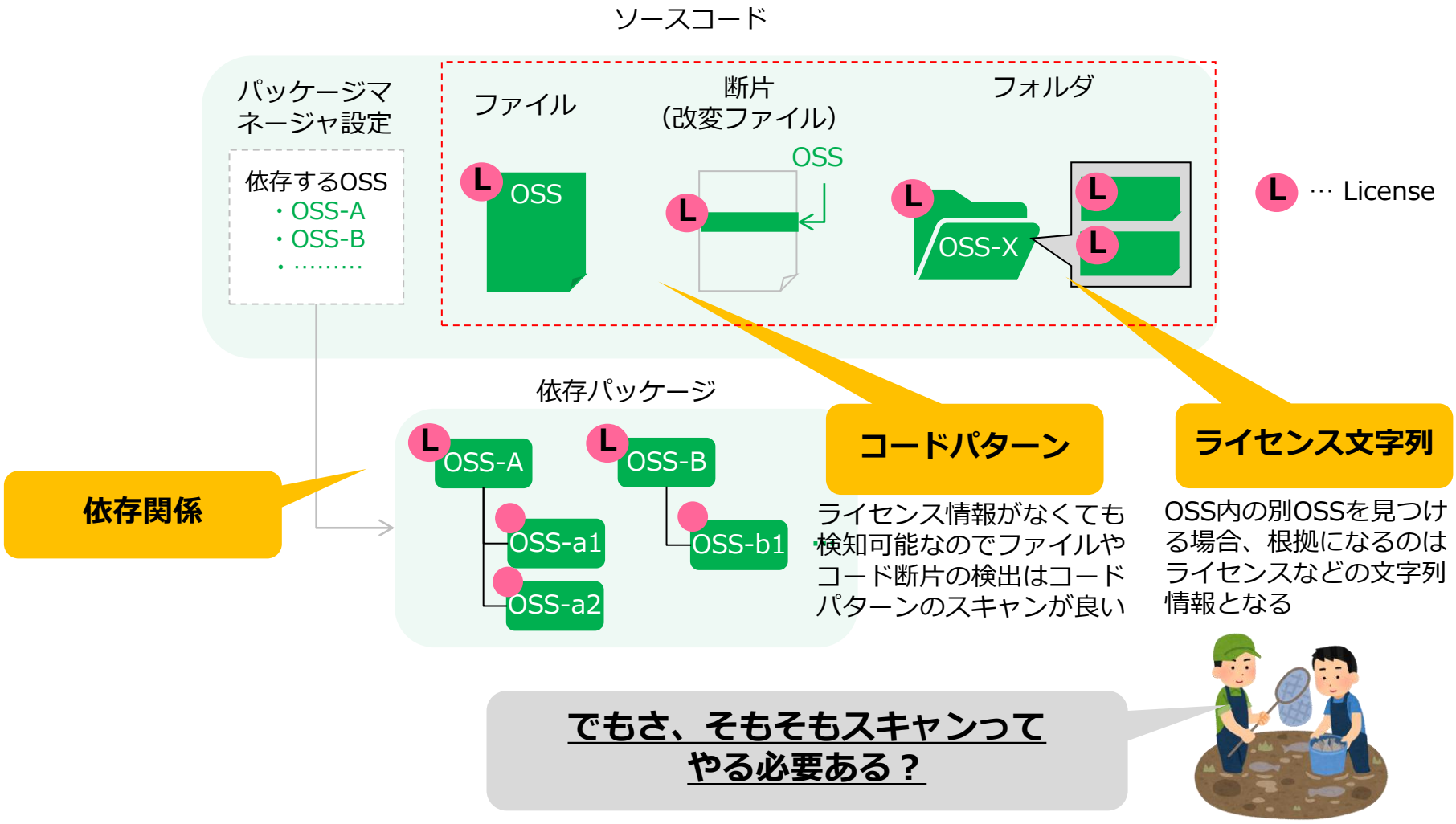
OSSの管理戦略①

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



OSSの管理戦略②

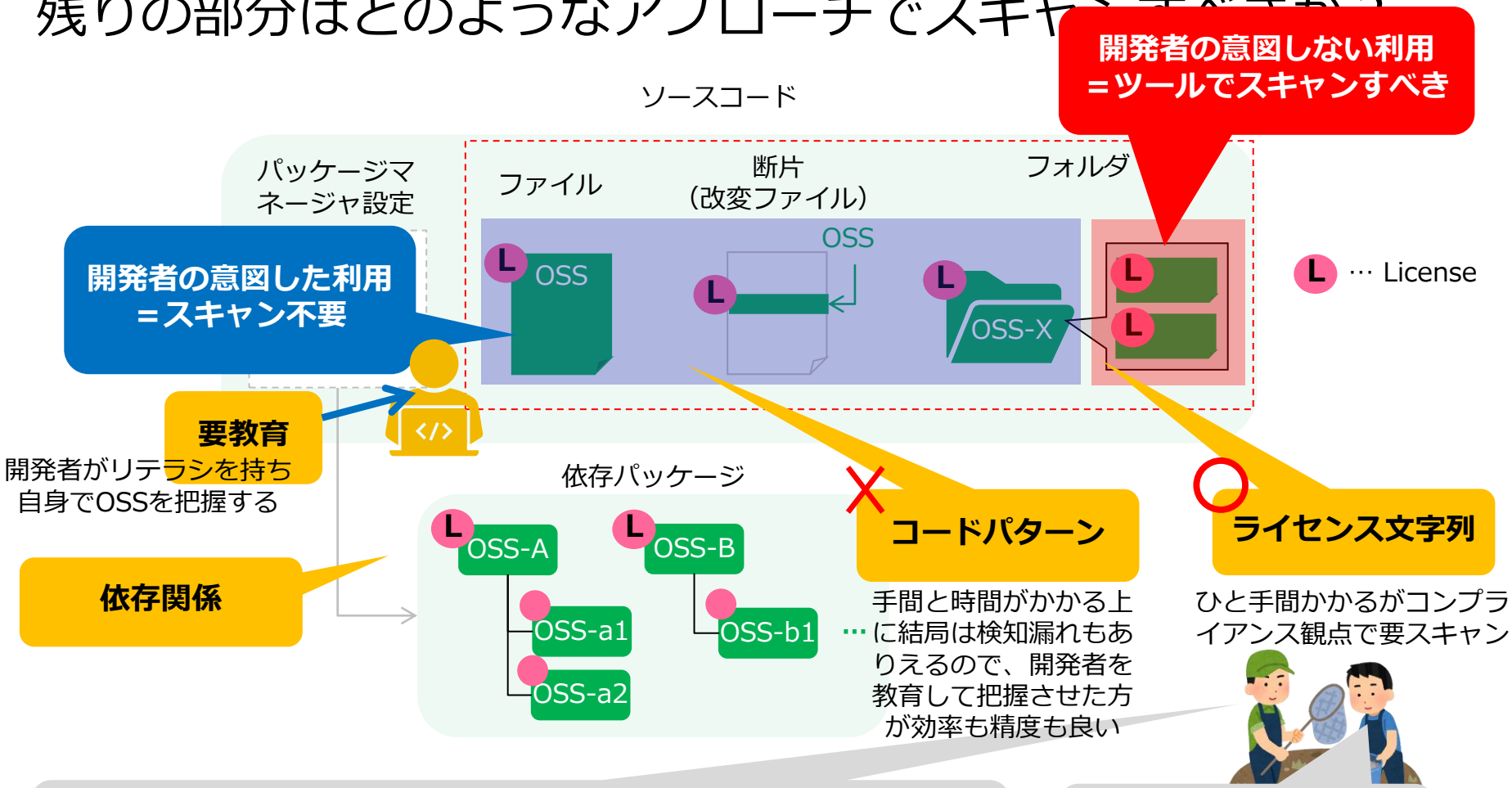
残りの部分はどのようなアプローチでスキャンすべきか？



OSSの管理戦略③

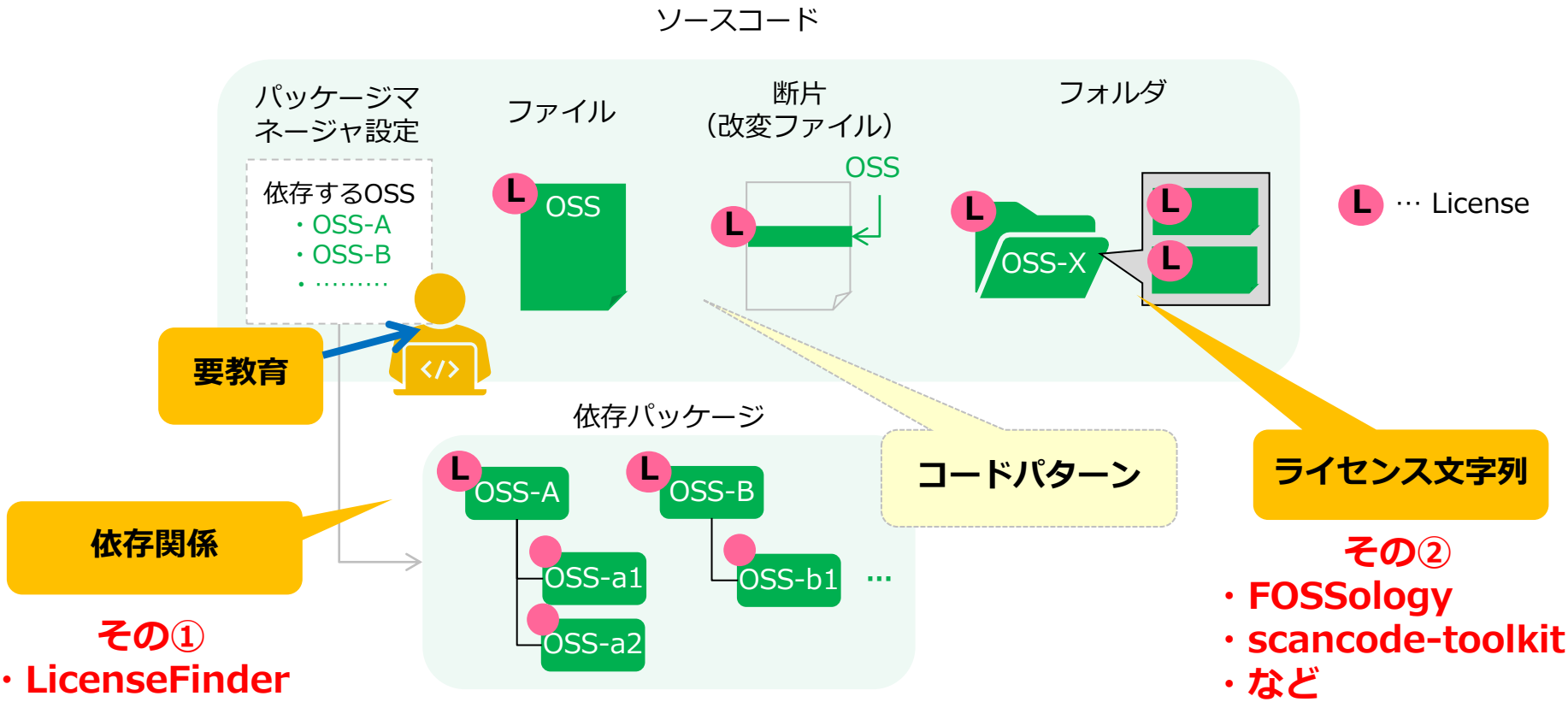
HITACHI
Inspire the Next

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？



OSSの管理戦略④

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



その①
- **LicenseFinder**
- **licensed**
- **など**

基本的に自動で検知

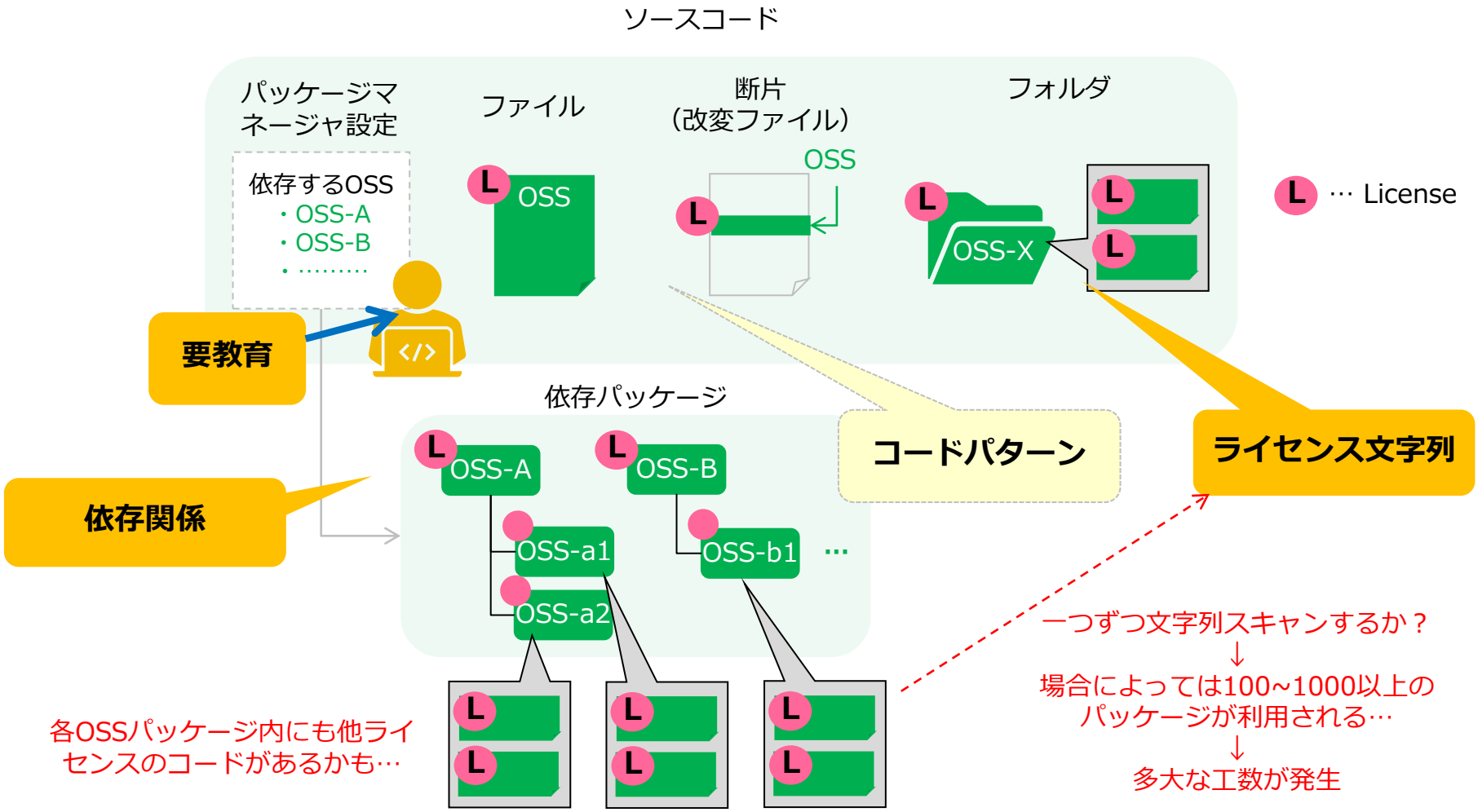
その②
- **FOSSology**
- **scancode-toolkit**
- **など**

OSSコピペ時のみ手動確認

OSSの管理戦略⑤

HITACHI
Inspire the Next

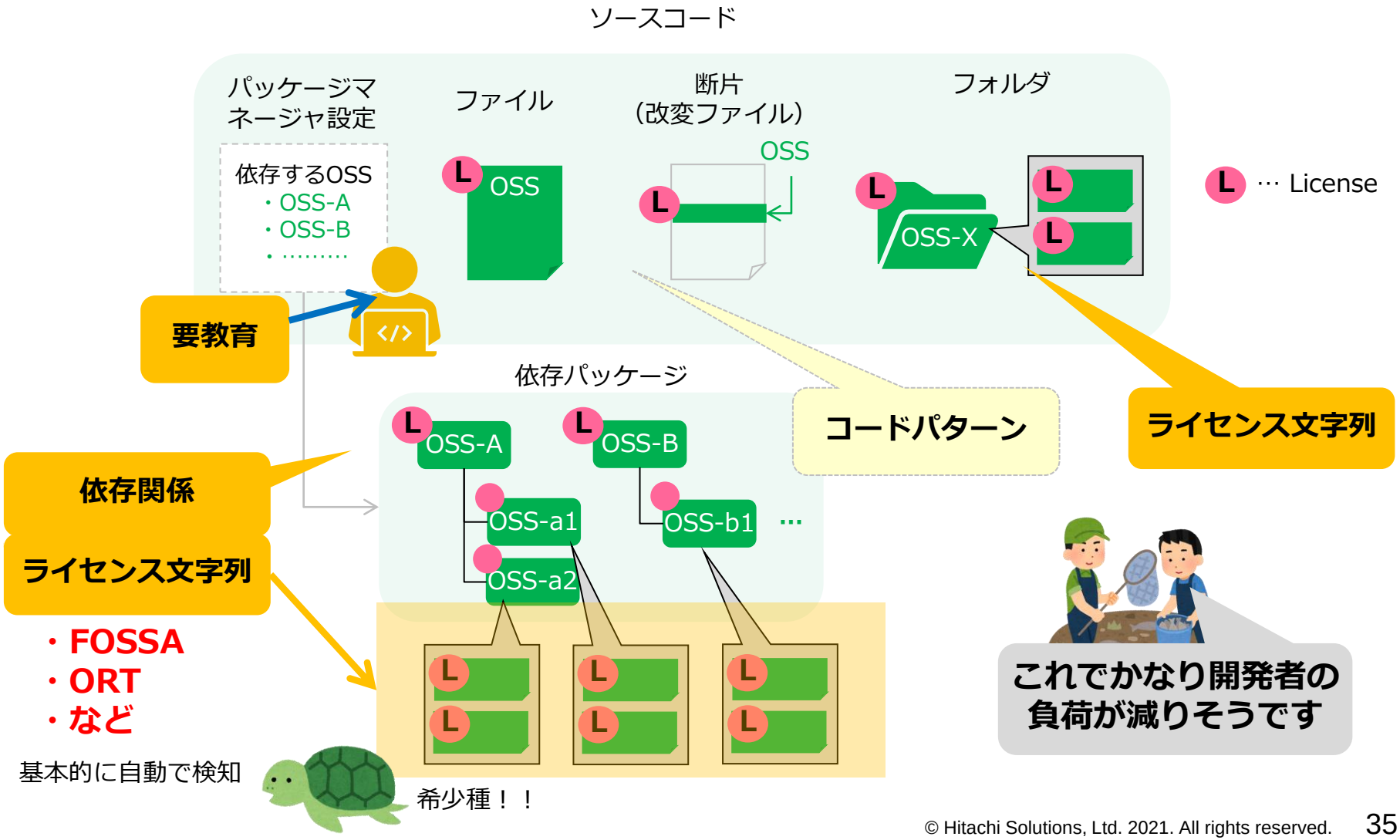
依存パッケージ内のOSSライセンスは大丈夫か？



OSSの管理戦略⑥

HITACHI
Inspire the Next

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



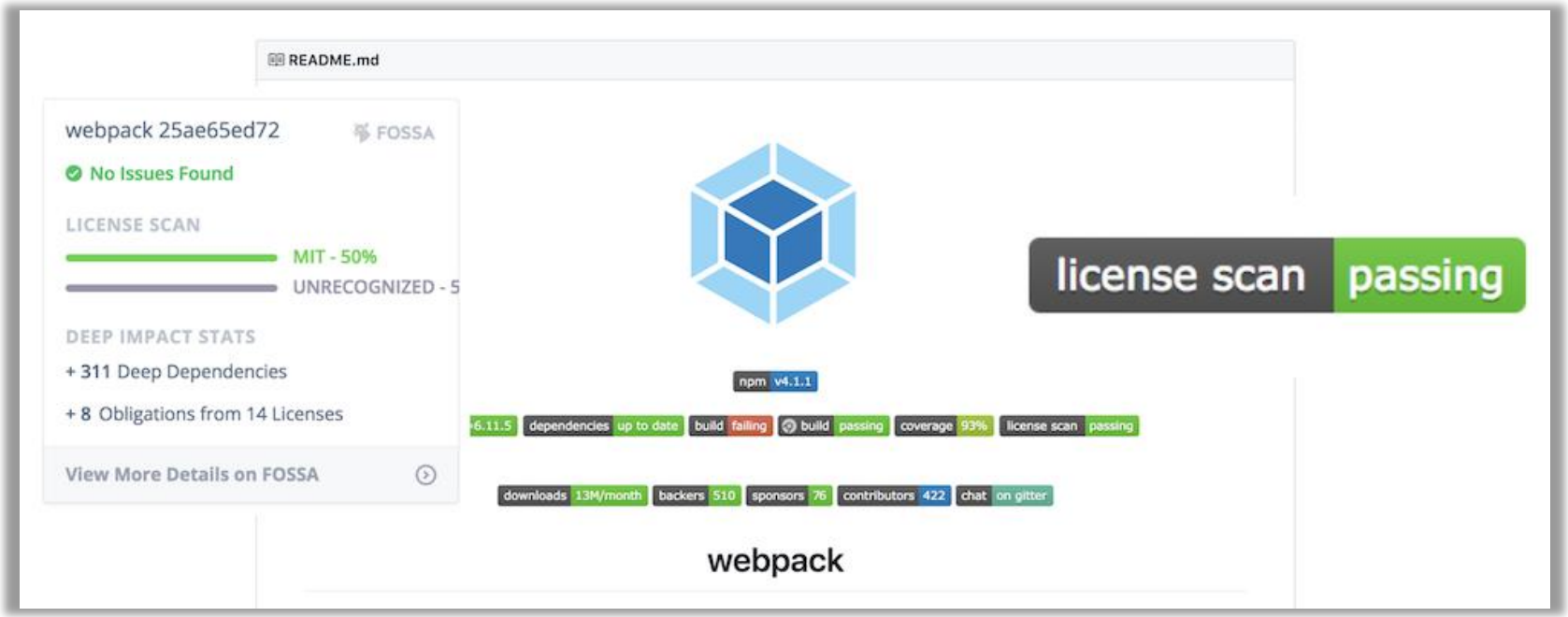
HITACHI
Inspire the Next

クラウドサービスFOSSAについて

FOSSA

FOSSAとは

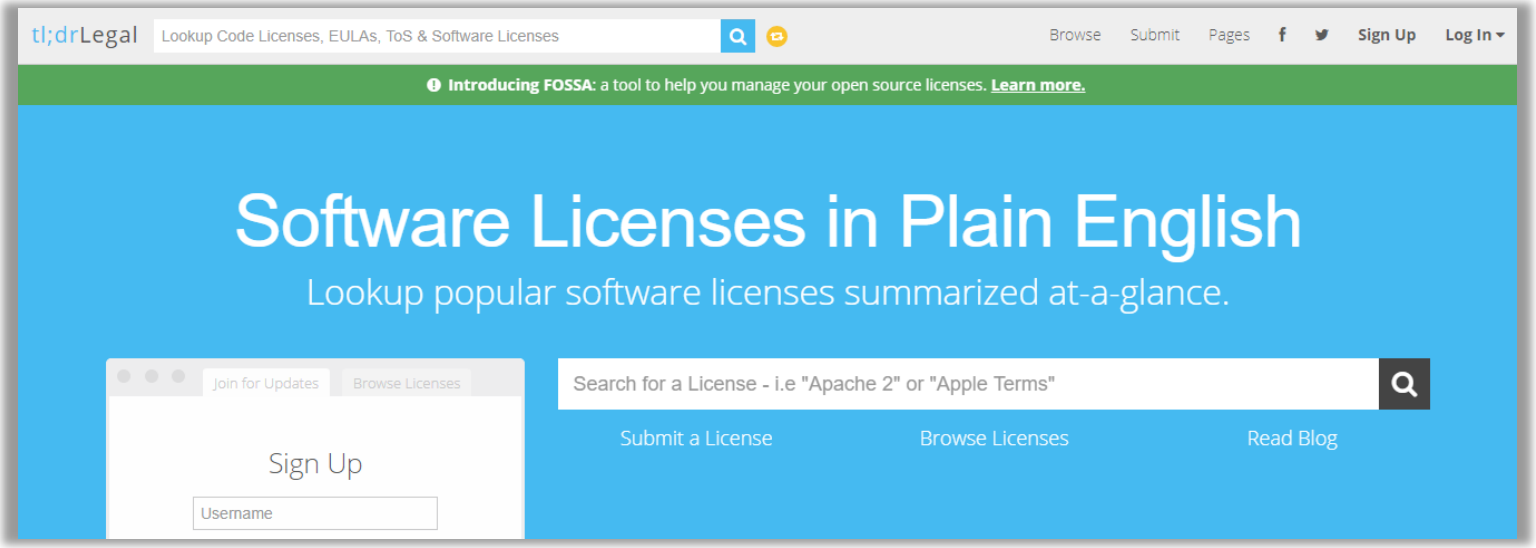
- OSSライセンス管理のためのクラウドサービス
- 個人利用は無料（制限つき）
- 「license scan」バッジを提供



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

FOSSA社について

- 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

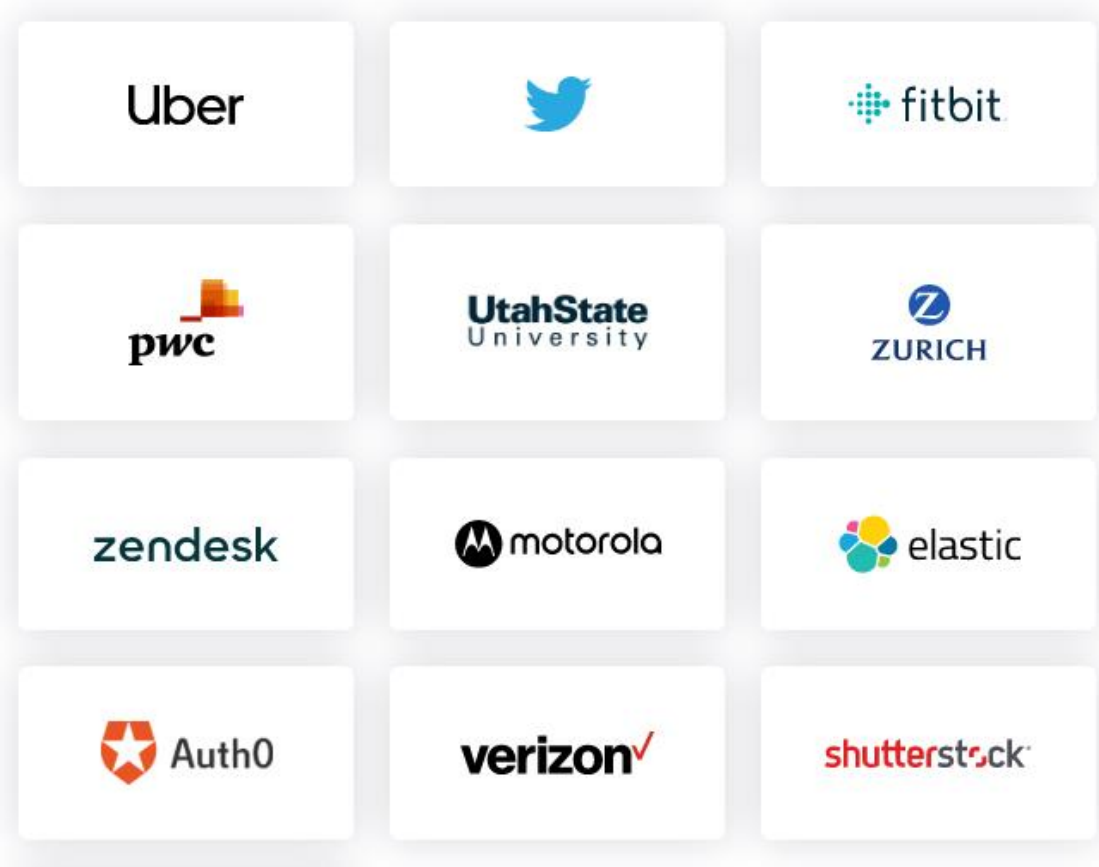


https://tldrlegal.com/

FOSSA導入実績

HITACHI
Inspire the Next

- 全世界16000チームが採用



引用：https://fossa.com/customers

FOSSAの概要

HITACHI
Inspire the Next

- 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の概要

HITACHI
Inspire the Next

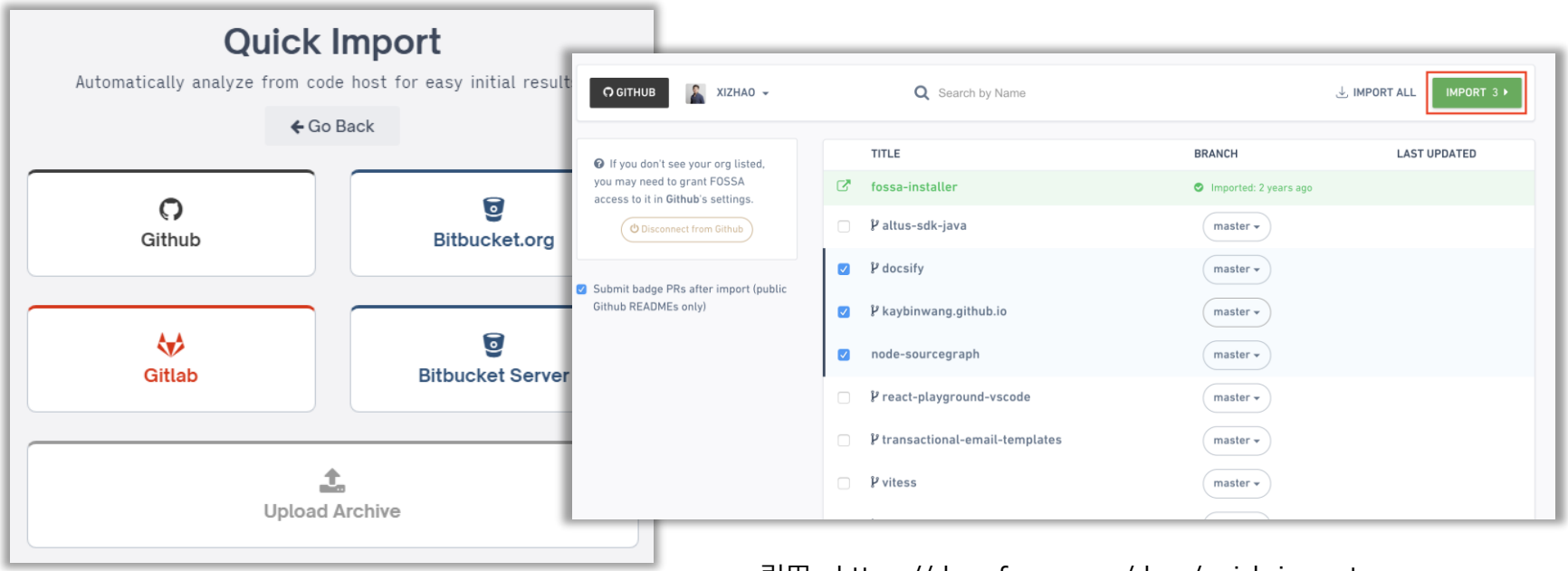
- 機能
  - OSSとライセンスのスキャン
    - 依存関係（メタデータ）のスキャン
    - ライセンス文字列のスキャン
  - ポリシー・アラート
  - ライセンスファイルの生成

FOSSAの機能（OSSとライセンスのスキャン）

- クイックインポート
- スキャナ連携（CI/CD連携）※ベンダ推奨

クイックインポート

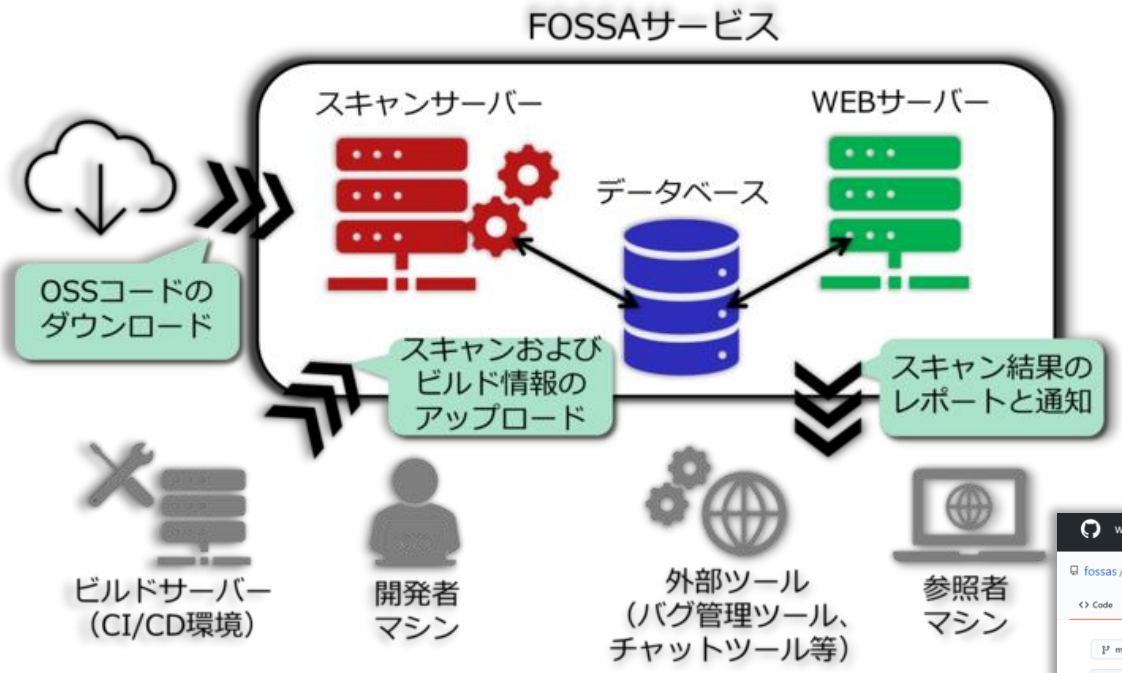
- GitHub、GitLab、Bitbucketのアカウントと連携
- 自身が管理するリポジトリを指定してFOSSAにインポート

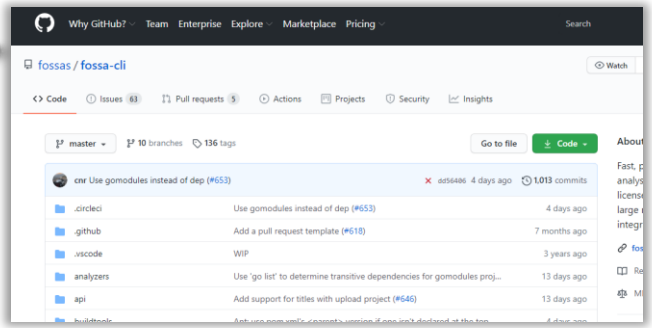


引用：https://docs.fossa.com/docs/quick-import

スキャナ連携（CI/CD連携）

- 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





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

FOSSAの概要

HITACHI
Inspire the Next

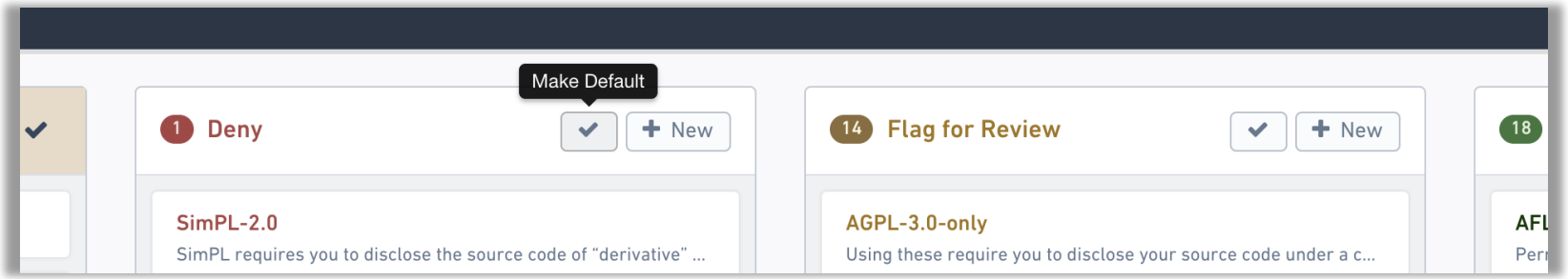
- 機能
  - OSSとライセンスのスキャン
    - 依存関係（メタデータ）のスキャン
    - ライセンス文字列のスキャン
  - ポリシー・アラート
  - ライセンスファイルの生成

FOSSAの機能（ポリシー・アラート）

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

Policies画面

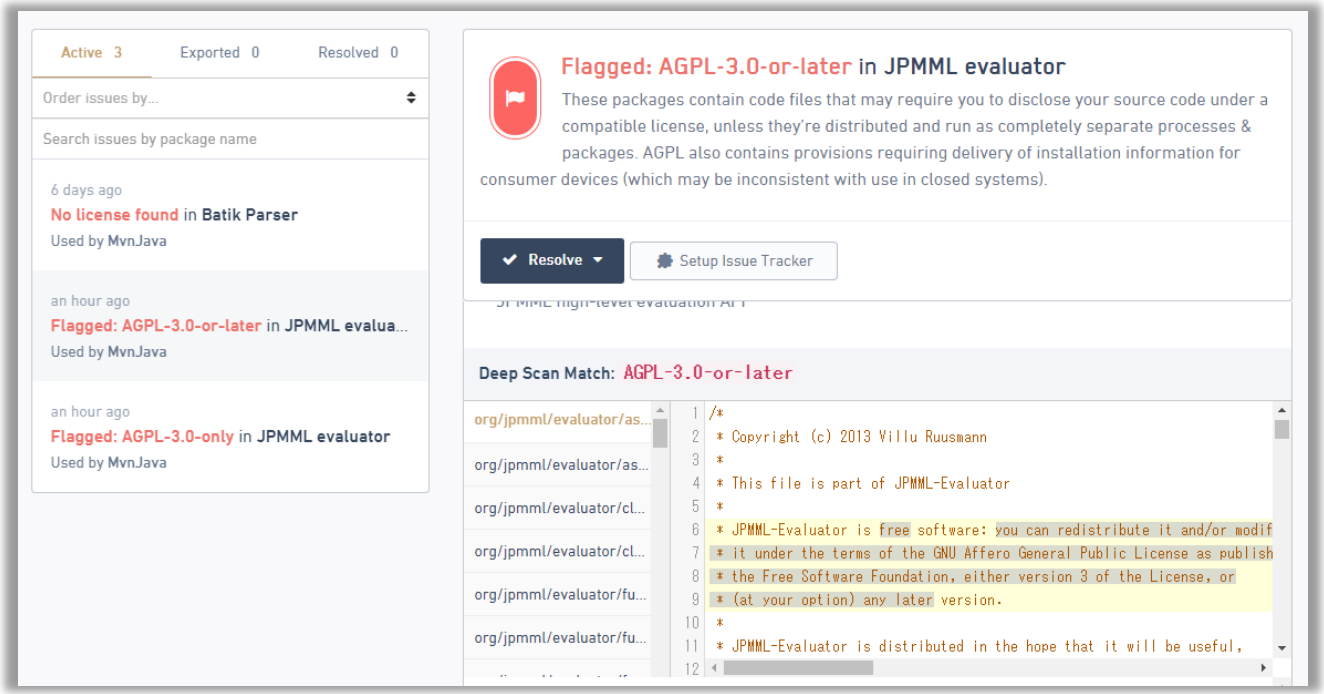
- ポリシーを利用してコンプライアンス違反の可能性を検出可能
- 専門家が監修した3種類のポリシーがプリセットされている
  - Standard Bundle Distribution
  - Single-Binary Distribution
  - Website/Hosted Service
- ポリシーはカスタマイズも可能



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

Issue画面

- 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



FOSSAの概要

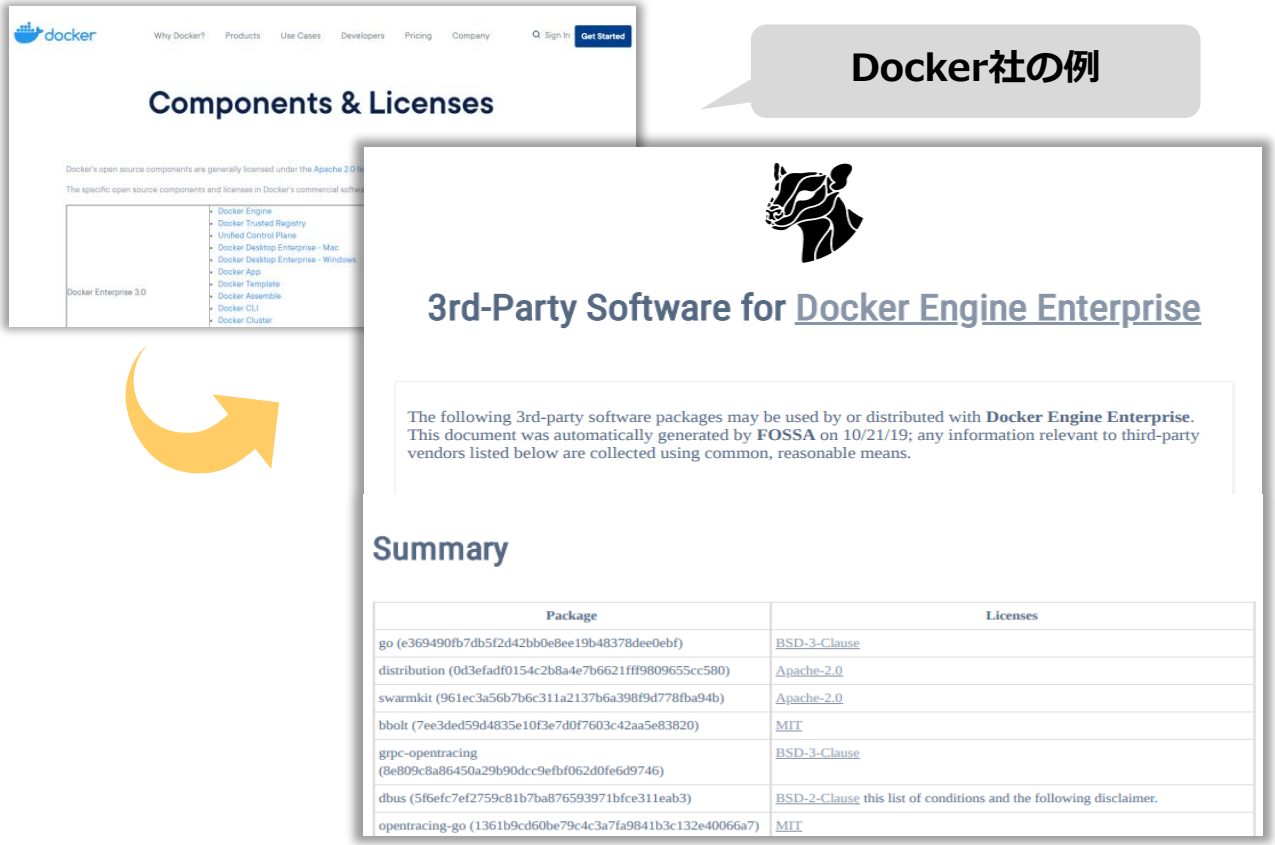
HITACHI
Inspire the Next

- 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の機能（ライセンスファイルの生成）

HITACHI
Inspire the Next

- 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

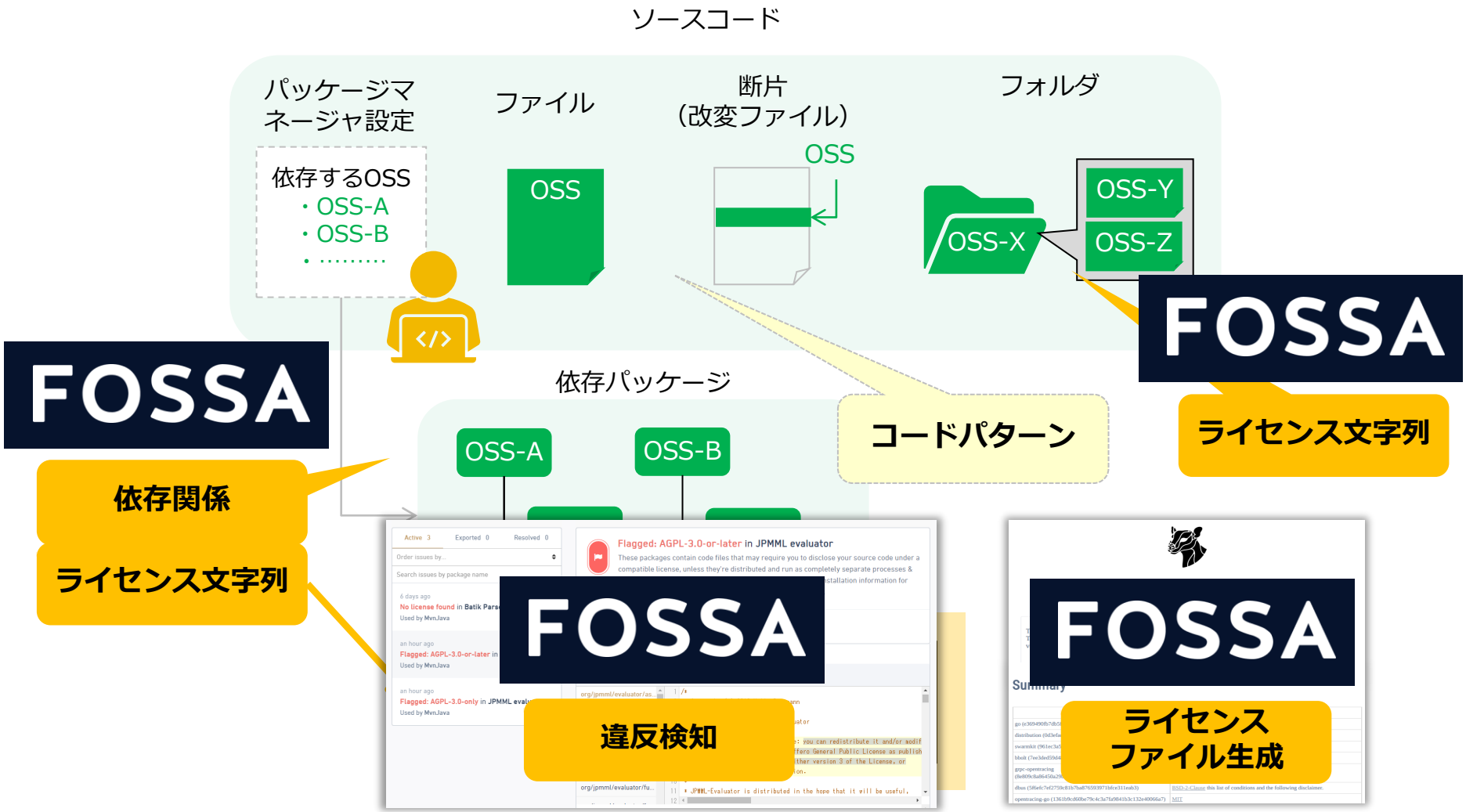


引用：https://www.docker.com/legal/components-licenses

FOSSAまとめ

HITACHI
Inspire the Next

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



補足：サポート範囲

- 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

全体まとめ

HITACHI
Inspire the Next

- 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

HITACHI
Inspire the Next

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。