生成AIコードに潜むライセンスリスクを乗り越えるDevOps自動化

サイオステクノロジー
佐々木寛太

SIOS

自己紹介

佐々木寛太

サイオステクノロジー PS/SL

技術領域

- Web Application (API, Front)
- Blockchain (Ethereum, Hyperledger)
- SBOM (ツール調査, 技術検証)

個別連絡

email: ka-sasaki@sios.com

X (旧twitter): @kanta_sasaki_

Facebook: 佐々木寛太

アジェンダ

1. OSSライセンス概要
2. 生成AIとライセンスリスクについて
3. SBOMとは
4. SCANOSSについての紹介
5. SCANOSS × DevOpsによる安全な開発環境構築

OSSライセンスの概要

OSSライセンスの概要

パーミッシブライセンス

特徴:

- ソースコードの公開義務がない
- ソフトウェアに組み込み可能
- ライセンスの変更が可能
- 商用利用に制限がない

コピーレフトライセンス

特徴:

- 派生作品も同じライセンスで公開する必要がある
- ソースコードの公開義務がある
- プロプライエタリ化を防ぐ仕組み

パーミッシブライセンス

MIT

- 著作権表示
- ライセンス条文表示
- 生成AIで再現されても比較的リスクは低い

Apache License 2.0

- 著作権と特許権表示
- ライセンス条文表示
- 変更箇所の明記が必要

BSD License

- 著作権表示
- ライセンス条文表示
- 宣伝・販促制限ありも

コピーレフトライセンス

GPL

- **強いコピーレフト**
- 派生物もGPLで配布が必要
- 第三者頒布時にソースコード開示義務
- AI由来のコードに含まれていると重大なリスクに

AGPL

- GPLよりもさらに厳しい
- SaaS提供時でもソースコードの開示が必要
- **クラウドサービス開発で特に注意が必要**

LGPL

- ライブラリ自体の変更時にソースコードを開示
- 動的リンクの場合には比較的安全

ライセンス違反事例①

プロジェクト概要

フランス政府と契約し行政手続きポータルサイトの開発

技術的詳細

使用ライブラリ: Lasso（Entr'ouvert製）

機能: シングルサインオン（SSO）を実現するIDプロバイダー認証プロトコル

ライセンス: GPL または 商用ライセンス（デュアルライセンス）

問題: Orangeは商用ライセンスを取得せず、GPLの義務も履行しなかった

最終判決結果

GLPライセンス違反による著作権侵害等により 65万ユーロ(1億600万)の損害賠償

ライセンス違反事例②

プロジェクト概要

メディアプレーヤーファームウェアの配布

技術的詳細

使用ライブラリ: GPL Lv2ライセンスのOSS複数

機能: メディアプレーヤーファームウェア機能

ライセンス: GPL Lv2

問題: 開示したソースコードに該当 OSSが含まれず製品とバージョンも異なる
一方製品の開発・提供は別の中国サプライヤーであるためGPL違反の責任はサプライヤーにあると主張

最終判決結果

弁護士費用、適切なソースコードの開示義務、サプライヤーに責任はなくすべて製品配布企業が責任を負う

生成AIとライセンスリスクについて

生成AIとライセンス違反について

生成結果に関する懸念点

既存コードの複製

- 学習データの特定のコードスニペットをそのまま出力する恐れ
- GPL等のコピーレフトのライセンスコードの断片を含む出力により、利用者の製品全体がGPLの適用対象となる可能性

ライセンス情報の欠如

- 生成されたコードにライセンス情報や帰属情報が含まれない
- 利用者が知らずにライセンス違反を犯すリスク

ライセンス違反の影響

1 金銭リスク

著作権侵害による損害賠償は数百万円から数十億円規模に及びます。GPL 違反の対応として、侵害コードの除去やリライト、追加制裁金や追加ライセンス購入などのコストも発生します。

2 法的リスク

裁判所から差し止め命令が出されると製品販売やサービス提供が即座に停止されます。継続的な弁護士費用や訴訟費用が発生し、国際展開時は各国で個別訴訟リスクもあります。経営陣が個人的な法的責任を追及される可能性もあります。

3 ビジネスへの影響

製品・サービスの緊急停止により売上が完全にストップし、開発スケジュールが数ヶ月から数年遅延します。最悪の場合は主力製品の市場撤退を余儀なくされます。顧客との契約解除や新規顧客獲得困難により事業基盤が揺らぐ可能性もあります。

ライセンス違反の影響

4 企業価値・組織への長期影響

訴訟発表時の株価急落により企業価値が毀損し、IPO準備企業では上場延期リスクなどが考えられます。投資家から信頼低下により資金調達条件が悪化し、優秀な人材が流出します。さらに企業ブランドの毀損により市場地位が著しく低下する恐れがあります。

5 業界・競合への影響

業界団体からの信頼を失い標準化活動から排除され、業界内での影響力が低下します。サプライチェーン排除や官公庁入札での減点リスクがあります。競合他社の攻撃材料となり、営業活動で圧倒的に不利な立場に置かれます。

6 生成AI時代特有のリスク増大要因

生成AIにより大量ライセンス違反が同時発生する可能性があり、検出困難なため発覚が遅れ被害が拡大します。このリスクを恐れ企業が生成AI利用を制限すると開発生産性が大幅に低下し、積極活用する競合他社との開発競争に敗れ市場での競争優位性を失います。

生成AIとライセンス違反対策

SIOS

SBOMを利用した適切なライセンス管理の必要性

- プロジェクトで使用しているソフトウェアのライセンス管理
- 生成AIが提案またはStack Overflow等からコピペしてきたコード(コードスニペット)のライセンス情報確認
- 開発段階での自動ライセンスチェック体制の確立

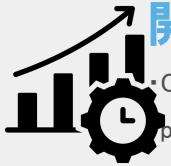
生成AIとライセンス違反対策例

プロジェクトで使用しているソフトウエアのライセンス管理

・パッケージ管理ツール等から使用しているソフトウエアを確認しコピーレフトライセンスを持っている場合通知する
・プロジェクト内で許可したパッケージのみ利用を可能にする制約を入れる

コードスニペットのライセンス違反チェック

・コピペや生成AIが提案したソースコードがGPLライセンスの断片ではないかチェックを行う製品の導入
・コードスニペット情報のマッチングを提供しているサービスを利用したチェック



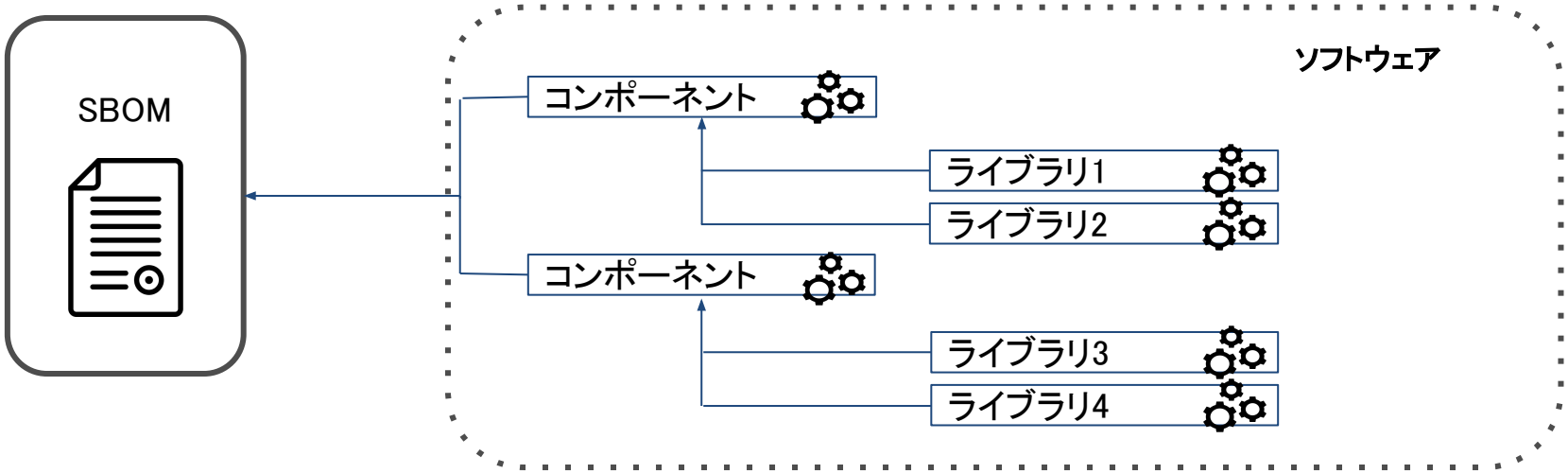
開発段階で自動ライセンスチェック体制の確立

・CI/CDパイプラインの構築
・pre-commitの利用によりローカル開発環境でチェック

SBOMとは

SBOM(Software Bill of Materials)

- ソフトウエアの構成部品（コンポーネント）をまとめたもの



SBOMの目的

- ソフトウエアの透明性とセキュリティの向上
- 脆弱性やライセンスリスクの管理を容易にする

SBOMの背景

- **サプライチェーンを利用した攻撃の増加**
  - IPA情報セキュリティ10大脅威に6年連続6回の選出
  - 2024年度は2位

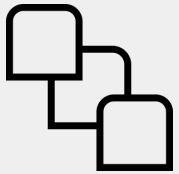
- **サプライチェーンの弱点を悪用した攻撃とは**
  - サプライチェーンの脆弱な部分から標的に対して攻撃を行う(Apach Log4j)
  - ソフトウエアの製造過程やアップデートプログラムにマルウエアを埋め込んで感染させる(XZ utils)

- **対策**
  - 納品物に組み込まれているソフトウエアの把握と脆弱性対策の実施(**SBOMの導入**)

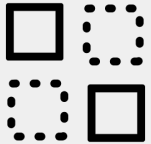
SBOMに含まれる情報

SIOS

SBOMに含まれる「最小要素」Data Fileds



依存関係



コンポーネント名

コンポーネントバージョン

識別子

サプライヤー名

SBOM作成者

タイムスタンプ

ライセンス情報

SBOMに必要な構成要素

カテゴリー名	概要	定義
Data Fields	各コンポーネントに関する基本情報を明確化すること	ひとつ前のスライドに記載されている項目
Automation Support	SBOM自動生成、可読性の自動化サポート	機械判読可能かつ相互運用可能なフォーマットにより運用 ・SPDX ・CycloneDX ・SWIDタグ
Practice and Process	SBOMの要求、生成、利用に関する運用方法の定義をする	・SBOM作成の頻度 ・SBOMの深さ ・SBOMの共有 ・アクセス管理 ・誤りの許容

SBOM導入のメリット

脆弱性管理

ソフトウエアの脆弱性管理が効率化され、影響の即時認識や迅速な対応が可能

また手動管理に比べ管理工数が70%削減されサプライチェーン全体のセキュリティが向上し、さらに
製品価値や企業価値の向上に起用することが期待

ライセンス管理

ソフトウェアに含まれるコンポーネントのライセンスを識別し、ライセンス違反のリスクを低減し管理コストを削減

ライセンス違反による販売停止や罰金のリスクを回避するために、SBOMによる正確なライセンス管理が重要

生産性向上

ソフトウェア開発ライフサイクルの改善により生産性向上が期待

SBOMを利用することで既知の脆弱性やライセンス問題を早期に特定・対応でき、開発遅延や対応コストを削減

社内で承認されたコンポーネント情報を管理により、次回以降の開発での調査、承認が不要になり工数削減を期待

CycloneDX vs SPDX

観点	CycloneDX	SPDX
開発元	OWASP Foundation	Linux Foundation
定義	セキュリティ目的のソフトウェア部品表	オープンソースライセンスの管理のための標準
目的	セキュリティと脆弱性	ライセンスコンプライアンスと法的リスクの管理
フォーマット	XML, JSON	JSON, YAML, Tag, Spredseheet
適用分野	セキュリティ、脆弱性、コンプライアンス	ライセンスコンプライアンス、法的リスク管理

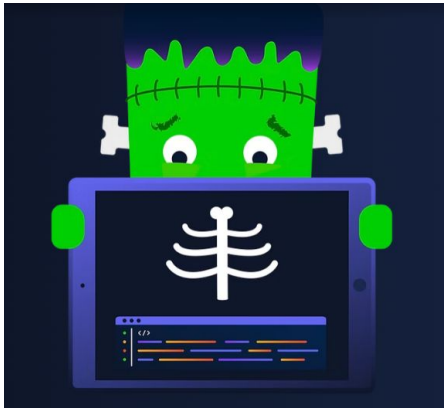
SBOMツール紹介
SCAN OSSについて

SCANOSS – 会社概要 –

SCANOSS

Scan Open Source Solutions S.L.

・SCANOSSは2020年に設立されたスペイン マドリードに本社を置くソフトウェア企業
・メンバーとしてはOSSライセンス＆セキュリティ管理ツールとして有名なBluck Duckの元CROやFOSSIDの共同創業者を始めとした10年以上のSCA経験を持つエンジニア集団



■SCANOSS Introduction – Our Vision

SCANOSSは、セキュリティの脆弱性、暗号化、ライセンス、コードの出所などに関する洞察を提供する、実用的なオープンソースソフトウェア（OSS）インテリジェンスの最も包括的な知識ベースを構築しました。

私たちの目標は、より良いソフトウェアサプライチェーンガバナンスを可能にするOSSインテリジェンスの事実上の情報源となることです。

私たちは、組織がより迅速で情報に基づいた決定を下し、ポリシーを自動化し、サプライチェーンやCI/CDパイプラインにおけるOSS関連の摩擦を減少させるためのワークフローを合理化するお手伝いをします。

OSSを超えて、私たちのビジョンは、独自のコードを含むすべてのコードに対するソフトウェアインテリジェンスを提供することに及びます。

SCANOSS の特長①

■SCANOSS製品の特長

・**ソフトウェアとアルゴリズムは100% OSS**
コスト削減、柔軟性、適応性、透明性、ベンダーロックインの回避

・**宣言された依存関係だけでなく、完全なSBOM（ソフトウェア部品表）を生成**
コードスニペットのような生成AIのサジェストコードやStack Overflowのようなエンジニア QAサイトからのコードコピペにも対応

・**監査人向けではなく、DevSecOpsチームのために設計**
CI/CD統合を前提とした設計

宣言型

- 著作権表示
- ライセンスファイル
- ヘッダー
- パッケージファイル
- マニフェストファイル

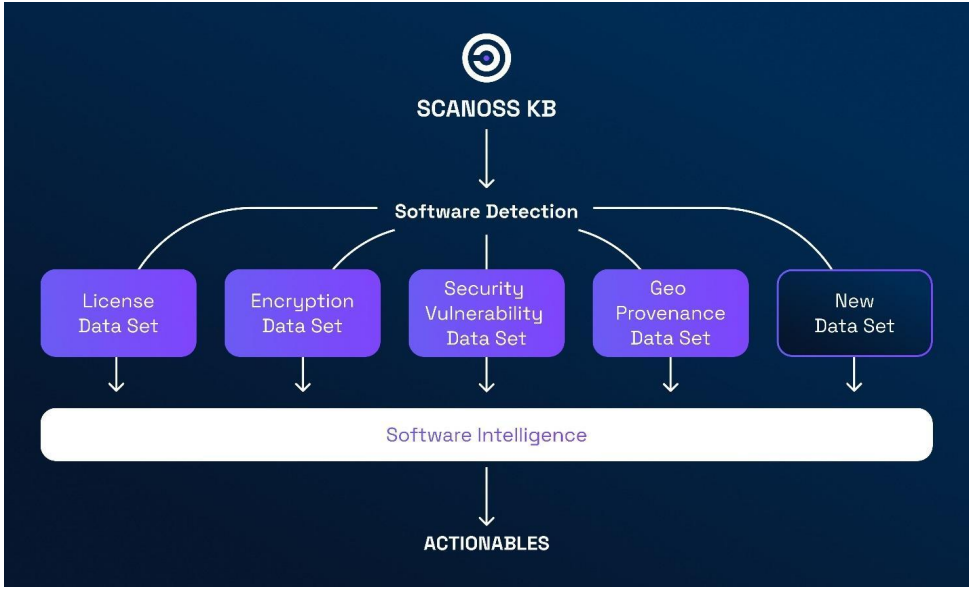
非宣言型

- ライセンスヘッダー無しファイル
- 組み込み依存関係
- コピペコード
- AI生成コード
- スニペット

SCANOSS Knowledge Baseの特長①

■SCANOSS製品の特長①

・『SCANOSS Knowledge Base』はAPIを介して提供され、4つの異なるデータセットを活用してOSSを可視化



・ライセンスデータセット

ライセンス義務、ライセンスの互換性、著作権表示、帰属などの実用的な情報を提供します。あらゆるプログラミング言語をサポートするSCANOSSは、開発元が特定されたオープンソースと未特定のもの、およびコード内の依存関係を検出します。また、完全な構成要素からオープンソースのファイルやスニペット[*1]まで、全てを明らかにすることで、ライセンス義務の遵守が可能となります。

・暗号化データセット

オープンソースおよびプロプライエタリコード [*2]の暗号アルゴリズムの完全な一覧表を提供します。アルゴリズムの種類と強度を把握することで、輸出規制への準拠、量子コンピューターによる攻撃に備えた強いセキュリティ計画が可能になります。

・セキュリティ脆弱性データセット

National Vulnerability Database（NVD）、OSV、GitHub Advisoriesなどの信頼できるソースから必要不可欠な情報を把握することができます。これにより、新たな脅威に関する情報を常に入手し、潜在的な不正プログラムを評価し、アップデートの計画を確実に行えます。

・Geo Provenance データセット

オープンソースソフトウェアの開発者の出所、地理的な出所を含むコードの所有権に関する詳細な情報を提供します。これにより、ライブラリーや依存関係の信頼性を検証することができます。透明性を維持し、ソフトウェアのサプライチェーンを強化し、安全で追跡可能なコードベースで信頼を築くことができます。

SCANOSS Knowledge Baseの特長②

■SCANOSS製品の特長②
“DevSecOps実現のためのサービスです”

🧩 100% FOSSのソフトウェア構成

- ソフトウェアはすべて **フリー＆オープンソース（ FOSS）**
- 提供価値は **高品質なデータサブスクリプション**

🔗 APIファースト設計

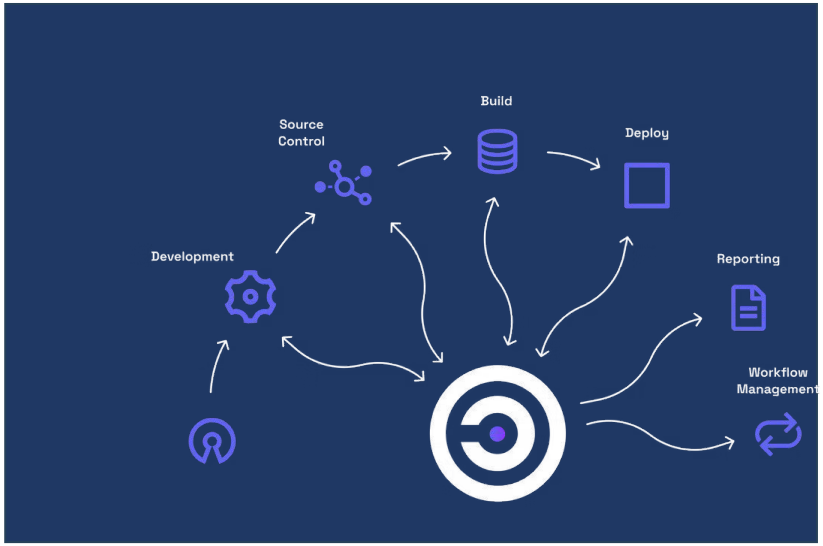
- OSS検出・SBOM生成・リスク分析を **APIで統合**
- **IDE～デプロイまで** 依存関係を継続的にトラッキング

📊 リアルタイムでリスク可視化

- SCANOSS APIにより**開発フローを止めずに**
  セキュリティ・コンプライアンスを強化

✅ DevSecOpsに自然にフィット

- 開発スピードと安全性の両立を実現！



SCANOSS Knowledge Base　導入事例①

●ソニー・インタラクティブ・エンタテイメント
「AI生成コードの管理」

課題:

・法務チームは、著作権のリスクと所有権に関する懸念から、AI支援のコーディングを禁止しました。

・AIの結果におけるOSSの断片を検出する方法がありません。

影響:

・開発者の生産性が最適でない

・ローンチの遅延と技術的リスクの増大の懸念

解決方法:

・AIの結果における変更されていないOSSコードと変更されたOSSコードの両方を識別するために
SCANOSSを採用しました。

・SCANOSSのビジュアルインターフェースをgitと統合することで、開発者はコード行を比較し、
宣言されたコードまたは独自のコードとして登録することができました。

結果:

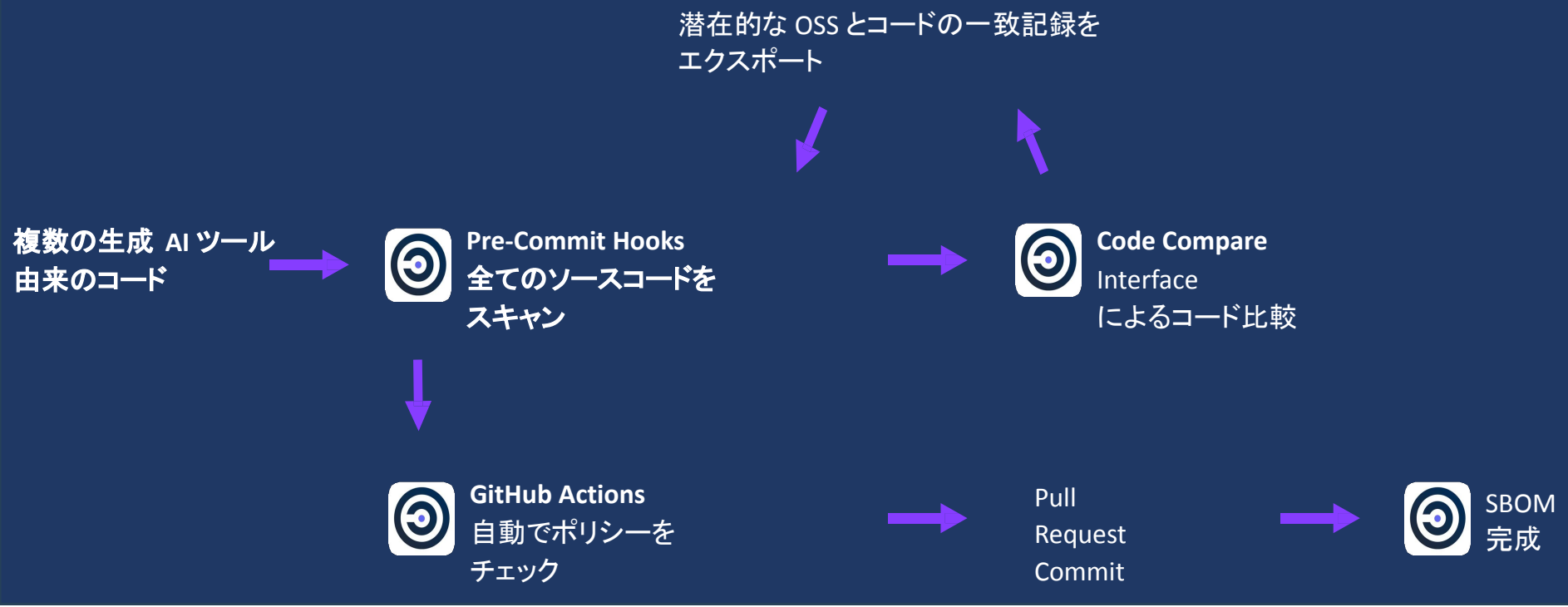
・1ヶ月以内に禁止が解除され、AI支援のコーディングを安全に使用できるようになりました

・開発者の生産性が向上しました。

・法的コンプライアンスを維持しました。

SCANOSS 導入イメージ

課題解決イメージ



SCANOSS – ユースケース –

🧩 既存のインフラに自動ライセンススキャンを組み込みモニタリングがしたい場合

- ベンダーロックをしないため既存の構成を保ったまま導入が可能
- 既存の開発フローを保ったまま自動でスキャン、モニタリングをすることが可能

🔗 OSSライセンスのコンプライアンスを確保しながら生成　AIを活用したい場合

- 開発ツールに依存しない形でCI/CDやエディタにシームレスに導入、スキャンすることが可能
- ライセンス管理の自動化により煩雑な手作業が削減

📊 自分たちの要件に合わせたコンプライアンスポリシーをカスタマイズして運用したい場合

- 許可したライブラリのみを使用させたい、特定のライセンスチェックを除外するといった柔軟なカスタマイズ
- 30000人規模の開発までスケールさせることが可能
- ライセンス違反の潜在的なリスクを開発のサイクルの中で早期発見が可能

SCANOSS×DevOpsによる
安全な開発環境構築

SIOS

SCANOSSで検知したい課題

1. 依存ライブラリのライセンス違反
2. 生成AIが生成したコードスニペットのライセンス違反
3. Stack Overflowなどからのコピペコードのライセンス違反
4. レガシー暗号化ロジック

解決アプローチ

CI/CDパイプラインへの組み込み

- プルリクエスト時の自動スキャン
- ビルド前のライセンスチェック
- デプロイ前の最終検証

段階的チェック体制

- 開発者ローカル環境での事前チェック
- ステージング環境での詳細スキャン
- 本番リリース前の包括的監査

実装パターン

SIOS

課題解決
イメージ

検出されたOSSライセンスの内容を開発者が確認・比較

ローカル環境でスキャン

開発者への即時FB

複数の生成 AI ツール由来のコード

Pre-Commit Hooks
全てのソースコードをスキャン

Code Compare
Interface
によるコード比較

ポリシーチェック
チーム共通のライセンス基準
最終的な品質ゲート

GitHub Actions
自動でポリシーをチェック

Pull
Request
Commit

SBOM
完成

SCANOSS統合のメリット

1. 既存の開発ワークフローの中にシームレスに導入
2. 手動では検出できない精度でライセンス違反を検出
3. CI/CDの利用により継続的に利用可能
4. PR段階でポリシー違反している場合のマージを防止
5. 開発者にはポリシー違反が見つかった場合即時FB

デモ

デモの流れ

CI/CDパイプライン

- コピーレフトライセンスを持つコードスニペットの検出
- 依存ライブラリのライセンス違反リスク検出

https://github.com/SIOS-Technology-Inc/excel-rag-frontend


SIOS