TechMatrix

SBOM

テクマトリックス

SBOMソリューション

SBOM導入でソフトウェアサプライチェーンの
セキュリティ・コンプライアンスリスクを低減

- SBOM 環境構築・体制整備
- SBOM 作成・共有
- SBOM 管理・運用
- SCAツール

SBOMツール導入における環境構築、SBOM作成・管理

テクマトリックス SBOMソリューション

テクマトリックスは、SBOM導入から運用まで、
お客様の状況に応じたソリューションを提供します。

SBOMを導入することで、最終的な製品を構成する
要素が明確化され、OSSの脆弱性対策やライセンス
コンプライアンス対応が行えるようになります。

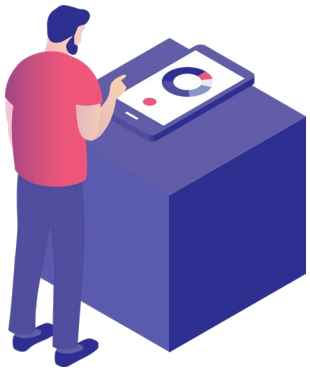
SBOM導入でサプライチェーンのセキュリティとライセンスのリスクを低減

ソフトウェアに含まれるOSSの脆弱性・ライセンスを管理するSBOMツールに加え、パートナー各社の幅広い支援サービスを組み合わせることで、SBOM対応における包括的なソリューションを提供します。

「環境構築・体制整備」、「作成・共有」、「管理・運用」の3つの段階的フェーズから、SBOMの作成や管理、SBOM導入に向けての組織体制づくりなど、フェーズごとに各種サービスやツールを提供します。

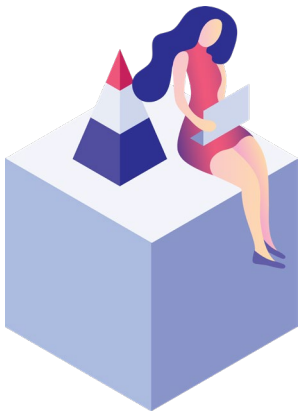
※SBOMとは、Software Bill of Materials（ソフトウェアの部品表）の略語で、ソフトウェアを構成するコンポーネントに関する詳細とサプライチェーン関係を記載した記録です。

1 環境構築・体制整備



- **SBOM運用範囲の明確化**
- **SBOMツール選定**
- **SBOMツール導入・設定**

2 SBOM 作成・共有



- **コンポーネント解析**
- **SBOMの作成**
- **SBOMの共有**

3 SBOM 管理・運用

- **脆弱性・ライセンス管理、対応**
- **SBOM情報の管理**

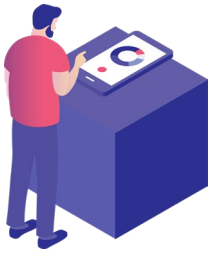
SBOM導入に向けた体制づくり（プロセスやルール設計など）や、SBOMツールの選定・導入の支援、CI環境構築による自動化など、幅広いサービスを用意しています。また、SBOMの導入支援だけでなく、EUサイバーレジリエンス法（CRA）、ISO/SAE 21434などの各法規・規格対応に向けたSBOM作成支援などのサービスも提供しています。

SBOM作成や管理、SBOM導入に向けての体制、プロセスの構築を支援します！

SBOM支援サービス
無償・有償サービス

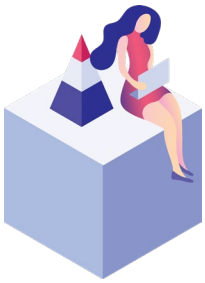
無償サービス　有償サービス

1. 環境構築・体制整備フェーズ



SBOM簡易説明会	SBOMが求められている背景、導入することにより得られるメリット、関連する規格などについて説明します。
SBOM無料相談会	SBOMに関連するお客様の状況、お困りごと、疑問点などをヒアリングし、取り組むべきことを討議の上、お客様にとって最適なソリューションを提案します。
簡易レポートサービス	お客様の製品において、利用されている可能性のあるOSSを検出し、ライセンス、脆弱性の情報を含むレポートを提供します。自社製品がライセンスに違反していないか、脆弱性を含んでいないかを確認することができます。
SBOMレポーティングサービス	お客様の製品において、利用されている可能性のあるOSSを検出し、ライセンス、脆弱性の情報を含むレポートを提供します。ツールが出力した結果を有識者が分析し、精度の高いSBOM、分析レポートを提供します。
SBOM導入支援サービス	お客様におけるSBOM導入に向け、国内外のSBOM関連法規・事例を踏まえた要件整理やツール選定、導入計画の策定を支援します。
OSS審査プロセス構築サービス	OSSそのものや、OSS利用の方法、留意点に関する基礎教育を実施します。OSS利用時のプロセス・ルール・成果物・運用体制を含めたOSS利用規定、OSSライセンスポリシーの策定を支援します。
OSSガイドライン構築サービス	お客様におけるソフトウェア開発プロセスでのOSS脆弱性、ライセンスリスク管理の適切な運用に向けて、OSSガイドライン構築を支援します。

2. 作成・共有フェーズ



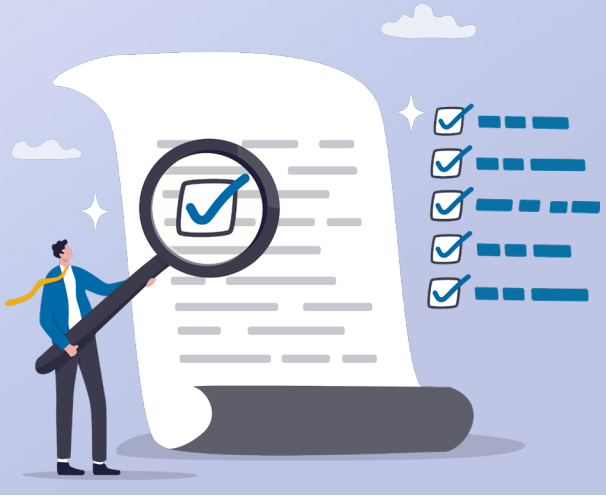
ツール簡易勉強会	FossIDの基本操作、効率的な識別作業のポイントを中心に説明します。動画の案内となりますが、内容に関する質問は弊社サポートにて対応します。
ツール勉強会	FossIDの基本操作、効率的な識別作業のポイントを中心に説明します。有識者によるリアルタイムの勉強会です。質疑応答も勉強会の中で実施いたします。また、ご要望に応じて内容のカスタマイズが可能です。
FossID環境構築サービス	新規にFossIDを実行可能な環境を構築します。
識別作業支援サービス	FossID上で行う識別作業を請け負います。特に作業工数を必要とする、初回の識別作業を請け負い、貴社の識別作業の負担を軽減します。
SBOM運用設計サービス	SBOMツール導入後、本来実施したい運用プロセスのあるべき姿を設計します。現状の運用プロセスを分析し、あるべき姿とのギャップを整理した上で、新たな運用ルール・体制・プロセスを設計します。現場への導入支援も実施します。
各種法規・規格向けSBOM作成支援サービス	EU CRA、ISO/SAE 21434、ISO/IEC 5230など各種法規・規格に必要な取り組み内容を整理してレクチャーします。SBOMツールを活用することで対応可能な内容、SBOMツールだけでは対応できない法規・規格対応のための実務について対策案を整理します。

3. 管理・運用フェーズ

SBOM運用支援サービス	SBOMを作成したものの、脆弱性にどう対応すればよいか分からない、ライセンスポリシーに違反している場合の対処方法が分からないなど、SBOM作成後のお困りごと、疑問点をヒアリングし、適切な対処方法を提案します。
OSSサポートサービス	OSSガバナンス、マネジメントのエキスパートによるOSSサポートサービスパッケージです。ライセンスの解釈、OSSの組み込み方など、さまざまなOSSに関する疑問に対して、タイムリーにアドバイスを提供します。
CI環境構築サービス	お客様のご要望をヒアリングし、FossIDを自動実行するための環境構築を行います。今後の拡張も考慮し、メンテナンス性の高いCI環境のベストプラクティスを提供します。

OSSライセンス＆セキュリティ管理ツール　FossID

コードスニペットレベルで検出 OSS脆弱性・SBOM管理

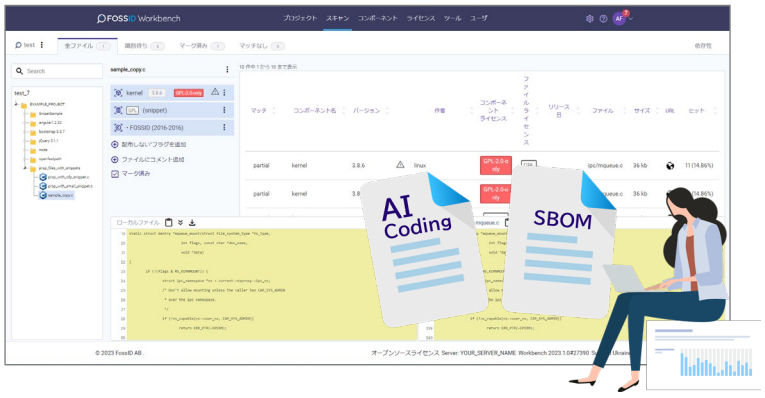


FossIDは、最新鋭のスキャニングエンジンと、膨大なオープンソース情報ナレッジベースに支えられた新しいOSSライセンス＆セキュリティ管理ツールです。

さまざまなプログラミング言語のソースコードに対し、独自のコード検索アルゴリズムで高速にスキャンを行い、コードの派生元であるオープンソースを特定します。

ソフトウェア開発のリスク管理・SBOM作成／生成AIコードのOSS検出

FossIDは、OSSの依存関係の分析や脆弱性の検出などによって、OSSの脆弱性やライセンス違反のリスクを低減することができます。また、AIコーディングアシスタントの利用において、OSSのスニペット検出機能を備えたFossIDがセキュリティ確保に役立ちます。独自のExcel形式のレポートに加え、 SPDX、SPDX Lite、CycloneDX形式に対応したSBOMを生成します。



<FossIDの特長>

- ✓ **最大規模のナレッジベースにOSSの情報を蓄積**
- ✓ **高速スキャンと高精度の解析**
- ✓ **コードスニペットレベルでOSSを検出**
- ✓ **SBOMを作成し、SPDX、CycloneDX形式などのレポートを出力**
- ✓ **コンポーネントに含まれる脆弱性情報をCVEごとに表示**
- ✓ **脆弱性の原因となるコードスニペットを検出**
- ✓ **直感的でわかりやすいUI**

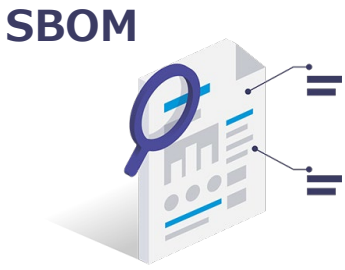
OSSスキャン

OSSから部分的にコピー&ペーストしたソースのライセンス情報が確認できるコードスニペット検出にも対応しているため、より正確で広範囲な情報を可視化します。

セキュリティ対策

NIST（アメリカ国立標準技術研究所）で公開されるCVE情報に基づく、OSSの脆弱性情報を表示し、早期にOSSのセキュリティ対策が行えます。

SBOM作成



FossIDはSBOMを作成し、SPDX/SPDX Lite、CycloneDX、Excelレポートなど用途に合わせたレポートを出力できます。SPDX, CycloneDXをインポートすることも可能です。

※CVE(Common Vulnerabilities and Exposures：共通脆弱性識別子)

FossIDは、あらゆる言語のソースコードに対応、SBOM作成を支援します。

業界最大規模のデータベース

FossIDのナレッジベースには、オープンソースプロジェクト、ソースファイルが格納されており、常に追加・拡大、および最適化をしています。

2億 件	2500 個	20万 件
プロジェクト	ライセンス	脆弱なプロジェクト

高速スキャンと高精度の解析でヒューマンエラーを低減

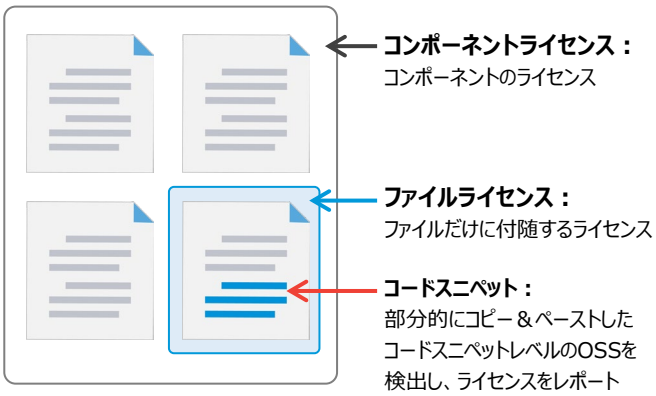
高速度スキャン：
独自のデータベースエンジンにより、非常に高速なスキャニングを実現しました。

高速度の解析：
FossIDのスキャニングアルゴリズムは誤検出を低減し、より精度の高いスキャニング結果を提供します。スキャニング結果を手動でふるい分けする時間とコスト、さらには、ヒューマンエラーを低減できます。

コードスニペットレベルでOSSを検出

ユーザーのソースコードに含まれているOSSをコンポーネント、ファイル、コードスニペットのレベルで検出し、そのライセンス情報とセキュリティ脆弱性情報を提供します。

ライセンス情報を提供：
検出したOSSのコンポーネントやファイルに付属するライセンス情報を提供します。

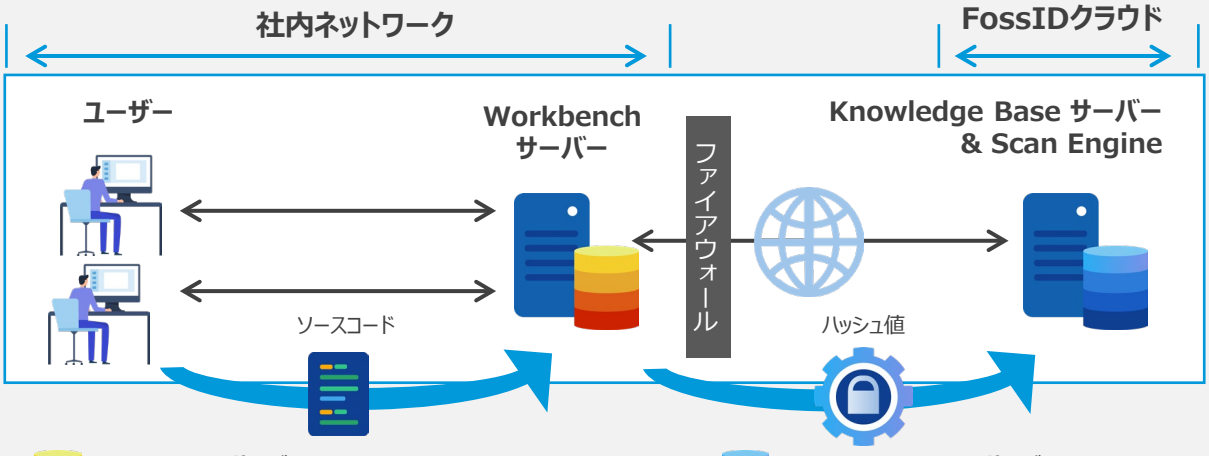


セキュリティ脆弱性（CVE）を検出：
OSSコンポーネントとそれに紐づく既知の脆弱性（CVE）を検出します。さらにオプションのVulnSnippetFinderを用いることで、脆弱性の原因となるコード行（スニペット）を検出し、自社コードや派生物に埋め込まれた個別の脆弱性を検出することができます。

FossIDのしくみ

Wordbenchサーバーにソースコードをアップロードし、ハッシュ値を作成するため、クラウドベースのスキャン実行時に、**FossIDサーバーにソースコード（ファイル名を含む）が送信されることはありません。**ナレッジベースの照会には、ソースコードから生成されたハッシュ値だけが使用されます。

Step 1	Step 2	Step 3
Workbenchサーバにソースコードをアップロードし、ハッシュ値を作成	ハッシュ値を使い、Knowledge Baseに OSSの情報を問い合わせ	解析結果を Workbenchサーバに返却、見やすい形式で表示



Workbenchサーバー
アップロードされたコードとプロジェクト/スキャン/ユーザー情報を含むデータベース

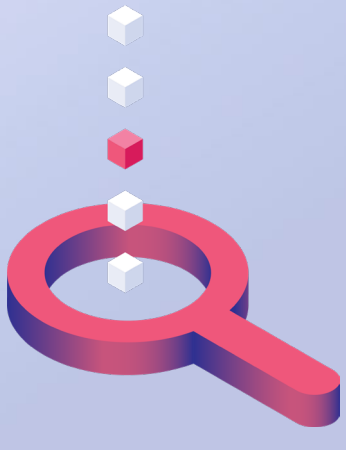
Knowledge Base サーバー & Scan Engine
2億件のプロジェクトが登録されたOSSデーターベース

バイナリ解析OSS管理ツール　Clarity

バイナリからSBOMを生成
OSS脆弱性・ライセンス管理

Insignary Clarityは、バイナリファイルからOSSを抽出し、OSSの脆弱性、ライセンスを特定するバイナリ解析OSS管理ツールです。

バイナリを対象にOSSの混入チェックを行うことができるため、ソースコードが入手できない対象についても、脆弱性・ライセンスコンプライアンス問題の有無を確認することができます。



バイナリファイル内のOSSを自動的に識別し、OSSの問題を効果的に発見

Clarityは、許取得済みのディープフィンガープリンティングおよびマッチングアルゴリズムを使用して、バイナリからOSSコンポーネントを抽出し、OSSの脆弱性およびライセンスを特定することができます。また、独自のExcel形式のレポートに加え、SPDX、CycloneDX形式に対応したSBOMを生成します。

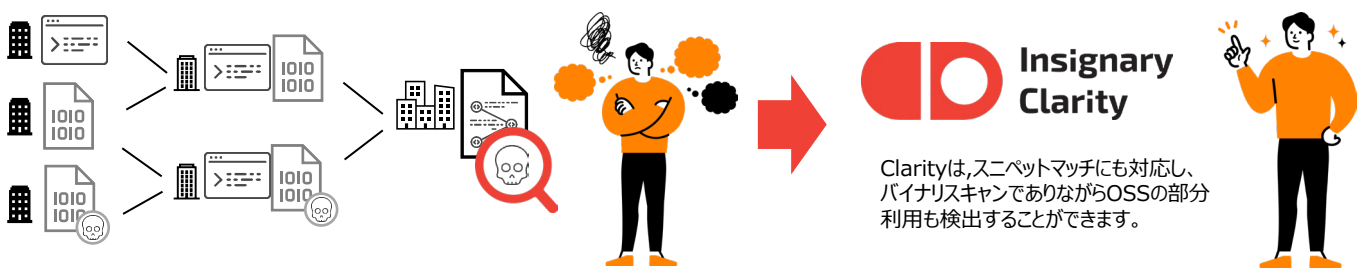
<Insignary Clarityの特長>

- ✓ **リバースエンジニアリングを行わずに、バイナリからOSSを検出**
- ✓ **単一のバイナリ内の複数のOSSコンポーネントとバージョンを検出**
- ✓ **LITIGATORトロールに関連するOSSコンポーネントをハイライト**
- ✓ **包括的なSBOM（ソフトウェア部品表）を提供**
- ✓ **クラウドベースまたはオンプレミスの導入をサポート**
- ✓ **独自のExcel形式のレポートに加え、SPDX、CycloneDX形式に対応**

フィンガープリントマッチングによりバイナリからOSSの脆弱性・ライセンスを特定

ソフトウェアサプライチェーンでは、ソースコードが提供されずバイナリでのみ提供されるケースも少なくありません。使用されているOSSの把握が難しく、潜在的なセキュリティ問題やライセンスコンプライアンス遵守における課題が多くあります。
そこで、Clarityをおすすめします。Clarityの技術は、バイナリに残るソースコード情報の断片を基にOSSを探索するため、「バイナリコンポーネント用のリポジトリがない」「ハッシュベースのマッチングが難しい」といったケースにも対応できます。

複雑化・不透明化が進むサプライチェーンにおけるOSS管理の課題を、Clarityで解決！



Clarityは、バイナリ・ソースコードに対応、SBOM作成を支援します。

バイナリファイルからOSSを検出

Clarityは、バイナリに含まれるOSSを検出します。
OSSのライセンス、脆弱性の情報を確認することができます。

バイナリスキャン：
ソースコードが入手できない状況でも
OSSの混入をチェック

OSSのスニペット利用も検出

特許取得済み技術「ディープフィンガープリンティング」がバイナリスキャンでのスニペットマッチを実現します。

バイナリスキャンのスニペットマッチ：
OSSのコードをコピーペーストして部分利用しているような場合でも、その部分利用したソースコードの断片からOSSを特定

特許取得済みの技術が支える精度

コンパイルプロセスで変更されずに残るソースコードの要素から派生したフィンガープリントを利用します。バイナリコンポーネント用のリポジトリがなく、ハッシュベースのマッチングが難しいケースにも対応できます。

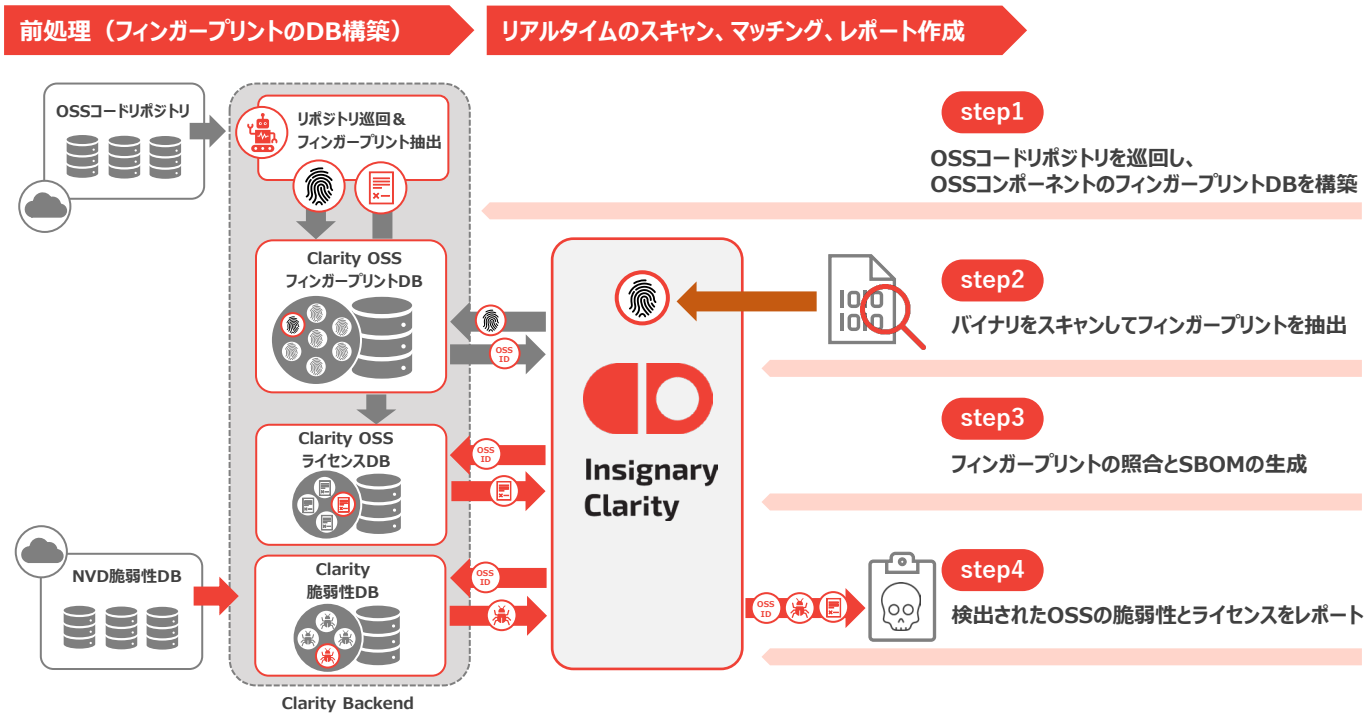
ソースコードからのOSSを検出

ソースコードも対象にスキャンすることが可能です。ソースコード全てを見てテキスト比較を行うのではなく、バイナリスキャンと同様に識別子の情報からマッチするOSSの探索をします。

識別子の情報をもとにOSSとのマッチ：
Clarityは、委託先などからもらったバイナリスキャンの目的で使うツールですが、自社のソースコードを対象にしてOSSの混入をチェックすることも可能

Clarityのしくみ

Clarityは、ターゲットバイナリをスキャンして「フィンガープリント」を抽出し、多数のOSSコードリポジトリから収集されたフィンガープリントと比較する特許取得済み技術ディープフィンガープリンティングを用いています。



1. OSSコンポーネントのフィンガープリントのデータベースを構築
2. ターゲットバイナリから文字列、関数、変数名などを基にフィンガープリントを抽出
3. ターゲットバイナリから抽出したフィンガープリントを、OSSのフィンガープリントデータベースと照合し、OSSの脆弱性とライセンスを適切に管理するためのSBOMを生成
4. 利用されているOSSに含まれる脆弱性とライセンスをレポート

SBOM

お問い合わせはこちら

課題やご要望がありましたら、お気軽にお問い合わせください。

SBOM支援サービス
無償・有償サービス

SBOM作成や管理、SBOM導入に向けての体制、プロセスの構築を支援します。

テクマトリックスSBOMソリューション

SBOM

詳細はこちら

FossID
あらゆる言語のソースコードに対応

OSSライセンス＆セキュリティ管理ツール

FOSSID

詳細はこちら

Insignary Clarity
バイナリ、ソースコードに対応

バイナリ解析OSS管理ツール

Insignary Clarity

詳細はこちら

【お問い合わせ先】

テクマトリックス株式会社

ソフトウェアエンジニアリング事業部
〒108-8588　東京都港区港南1丁目2番70号 品川シーズンテラス 24F
TEL：03-4405-7853
URL：https://www.techmatrix.co.jp/product/sbom/
E-MAIL：se-info@techmatrix.co.jp

TechMatrix