Parasoft C/C++test

導入後も安心してお使いいただける サポート体制

C/C++test導入時のサポートから、運用支援、問題発生時のQ&A対応など、導入後も安心してお使いいただけるサポート体制でお客様をバックアップいたします。

稼動環境

C/C++testの稼動環境は、Webをご確認ください。
https://www.techmatrix.co.jp/product/ctest/requirement.html

稼動環境はこちら

C/C++test体験版

C/C++testを体験版にてお試しください。
最新バージョンのC/C++testをお客様のマシンで、14日間お試しいただけます。

体験版の申し込みはこちら

ハンズオン/オンラインセミナー

C/C++testでは、無料ハンズオンセミナー・オンラインセミナーを実施しています。静的解析、単体テストの機能を知りたいという方は、ぜひご参加ください。

セミナーの詳細はこちら

【開発元】

PARASOFT

TMX202406

【総販売代理店】

TechMatrix
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1-2-70 品川シーズンテラス 24F
TEL：03-4405-7853
URL：https://www.techmatrix.co.jp/
E-MAIL：parasoft-info@techmatrix.co.jp

PARASOFT

for IEC 61508
for ISO 26262
for IEC 62304

Parasoft C/C++test

C言語/C++言語対応 静的解析・単体テストツール C/C++test

ソフトウェアの品質向上と効率的な開発の実現をサポート

- コーディング規約チェック
- フロー解析
- メトリクス計測
- 単体テスト
- カバレッジ計測
- カバレッジアドバイザー
- アプリケーションモニタリング
- 組み込みソフトウェア開発での利用
- CI/CDプラットフォーム連携
- Docker連携
- GoogleTest連携
- レポート生成
- 機能安全認証取得
- コンプライアンスパック

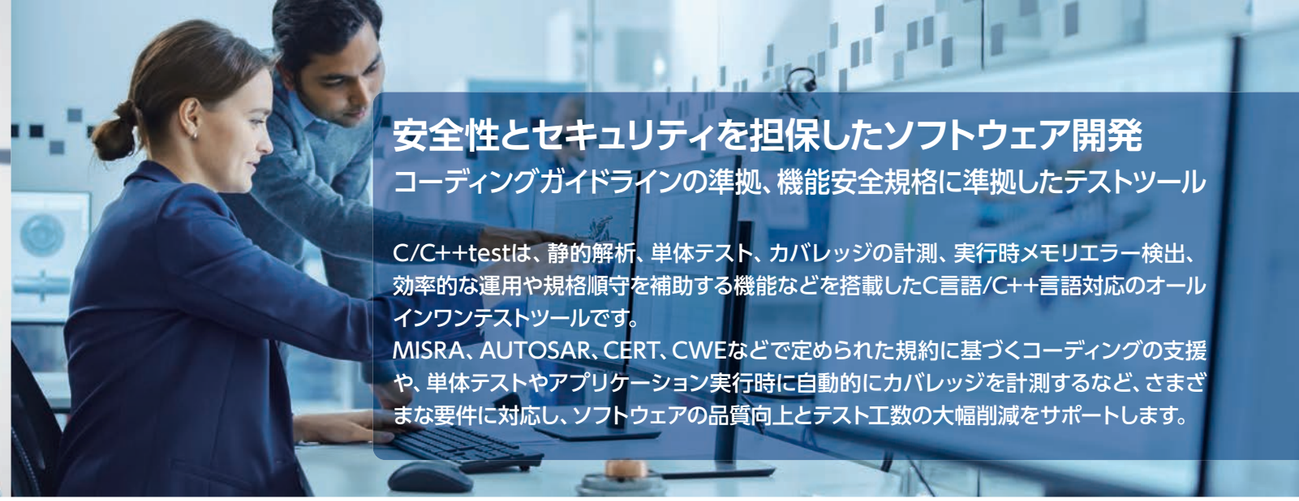
製品情報はこちらから

TechMatrix

C言語/C++言語対応 静的解析・単体テストツール

Parasoft C/C++test

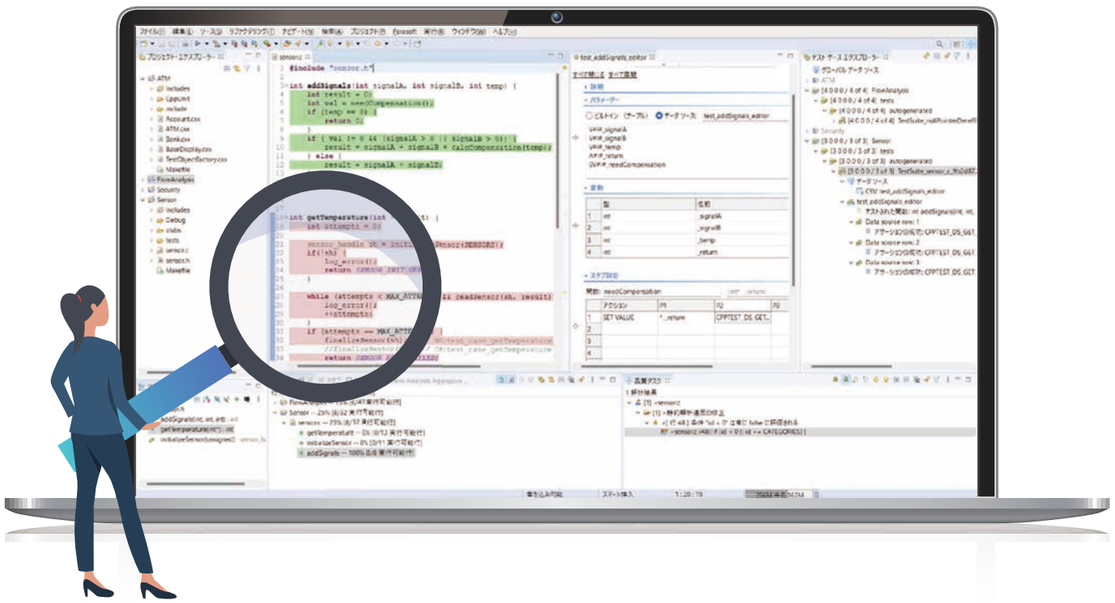
MISRA、AUTOSAR、CERT、CWEなどのコーディング規約チェック、
単体テスト、カバレッジの計測などさまざまな要件に対応



安全性とセキュリティを担保したソフトウェア開発

コーディングガイドラインの準拠、機能安全規格に準拠したテストツール

C/C++testは、静的解析、単体テスト、カバレッジの計測、実行時メモリエラー検出、効率的な運用や規格順守を補助する機能などを搭載したC言語/C++言語対応のオールインワンテストツールです。
MISRA、AUTOSAR、CERT、CWEなどで定められた規約に基づくコーディングの支援や、単体テストやアプリケーション実行時に自動的にカバレッジを計測するなど、さまざまな要件に対応し、ソフトウェアの品質向上とテスト工数の大幅削減をサポートします。



01. 静的解析

**静的解析でバグを早期発見、
保守性や再利用の指標となるメトリクスを計測**

コーディング規約チェック機能およびプログラムのあらゆるパスをシミュレートするフロー解析でバグを早期に発見します。
また、複雑度が高くバグが入り込みやすいコードを検出できます。早期にリファクタリングすることで、バグの未然防止とテストしやすいソースコードの実装が可能です。

- コーディング規約チェック
- フロー解析
- メトリクス計測

02. 動的解析

**テストドライバー・スタブ・テストケースの生成、
カバレッジアドバイザー機能で、単体テストを効率化**

GUI操作で「テストケース」の作成や「スタブ」の生成、スタブの振る舞いの設定ができます。
カバレッジを計測して単体テストの網羅性を視覚的にレポートします。また、効率的にカバレッジを向上させるためのテストデータ作成を支援します。

- 単体テスト
- カバレッジ計測
- カバレッジアドバイザー
- アプリケーションモニタリング
- 組み込みソフトウェア開発での利用

03. 補助機能

**効率的な運用や
規格遵守を補助する機能を搭載**

C/C++testは、効率的な運用を補助する各機能を搭載。
第三者認証機関であるTÜV SÜD社よりIEC 61508およびISO 26262、IEC 62304に準拠したテストツールとして認証を取得済みです。また、CI/CDプラットフォーム連携、Docker連携、GoogleTest連携、レポート生成など各種機能を搭載しています。

- CI/CDプラットフォーム連携
- Docker連携
- GoogleTest連携
- レポート生成
- 機能安全認証取得

04. コンプライアンスパック

**MISRA C:2023/MISRA C++:2023の
ルールに完全対応**

MISRA、AUTOSAR、CERT、CWEなどの遵守状況をリアルタイムに表示するダッシュボード画面の提供、コーディングガイドラインに則った遵守サマリーレポートや逸脱のレポートを自動生成します。

対応規格を一部抜粋

- MISRA C:2023 (MISRA C:2012)
- MISRA C++:2023
- AUTOSAR C++14コーディングガイドライン
- SEI CERT C コーディングスタンダード
- SEI CERT C++ コーディングスタンダード
- CWE TOP 25

01 . 静的解析

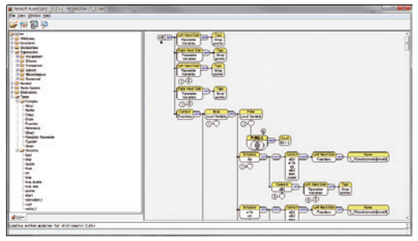
コーディング規約チェック

バグの作り込みを抑制、ソースコードの可読性と保守性を強化

- MISRA・AUTOSARなどのコーディングガイドライン対応ルールを搭載
- SEI CERT C/C++、CWE TOP 25などセキュリティルールを搭載
- 独自コーディングルールの作成、新規ルールセットの追加
- 重複コード検出機能を装備

高い信頼性と安全性を実現するためのソフトウェア設計標準規格「MISRA」「AUTOSAR」に対応、セキュリティ対策に有効な「CERT」「CWE TOP 25」にも対応しています。
バグの作り込みを防止し、ソースコードの可読性と保守性、拡張性に優れた高品質で寿命の長いソースコードの実装を支援します。また、ユーザー定義コーディングルールを作成する「RuleWizard」を搭載しています。社内やプロジェクトのコーディング規約に合わせて、独自のコーディングルールに修正したり、新規にルールセットを作成できます。他にも、重複コード検出機能を備えています。

●独自のコーディングルールの作成



●コーディングルールセット（抜粋）

- MISRA C:1998
- MISRA C:2004
- MISRA C:2023（MISRA C:2012）
- MISRA C++:2008
- MISRA C++:2023
- AUTOSAR C++14
- HISソースコードメトリクスチェックルール
- FDA C/C++ 推奨ルール
- SEI CERT C
- SEI CERT C++
- CWE TOP 25
- OWASP TOP 10
- DISA ASD STIG
- PCI DSS
- UL2900
- IPA/SEC コーディング作法ガイド

フロー解析

プログラムのあらゆるパスをシミュレートし、バグを早期に発見

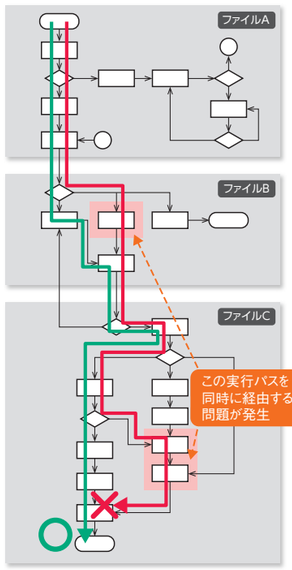
- ソースコードを解析し、関数・ファイルにまたがるバグを自動的に検出
- バグ発生までのデータフローを可視化

フロー解析は、プログラムを静的に解析して、プログラム実行時に発生し得る問題を検出します。複雑なアプリケーションでも、複数のファイル、メソッドにまたがるパスを自動的にトレースし、NULLポインターの間接参照やバッファオーバーフローなどプログラムの動作に致命的な影響をもたらすバグを早期に発見します。また、Parasoft DTPと連携することにより、フロー解析におけるデータフローのシミュレート結果をより詳しく表示できます。

●検出可能な項目（抜粋）

- メモリリーク/リソースリーク
- バッファオーバーフロー
- NULLポインターの参照
- 未初期化変数の参照
- 整数オーバーフロー
- ゼロ除算
- 配列の境界外アクセス
- イテレーター範囲外アクセス
- セキュリティ脆弱性
- デッドロック
- 不適切な排他制御

●ファイルをまたがる問題を検出（イメージ図）



メトリクス計測

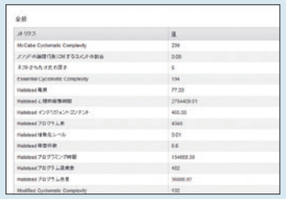
ソフトウェアの品質を定量的に評価

- コードの保守性や再利用性の指標となるメトリクスを計測
- 複雑度が高くバグが入り込みやすいコードを検出

オブジェクト間の結合や継承の深さなど、コードの保守性や再利用性の指標となるメトリクスを計測し、一覧データとして確認が行えます。それぞれのメトリクスのしきい値を任意の値に変更できるため、プロジェクトの基準に違反しているコードを瞬時に特定できます。

●計測できるメトリクスの例

- オブジェクト間の結合
- McCabe Cyclomatic Complexity
- コメントの割合/行数
- ファンアウト
- Halstead complexity
- クラスの継承の深さ
- 凝集性の欠如
- 保守性インデックス
- ネストの深さ
- コード行数
- メソッドのパラメータ数
- クラス数
- ファイル数
- 空白行数



02 . 動的解析

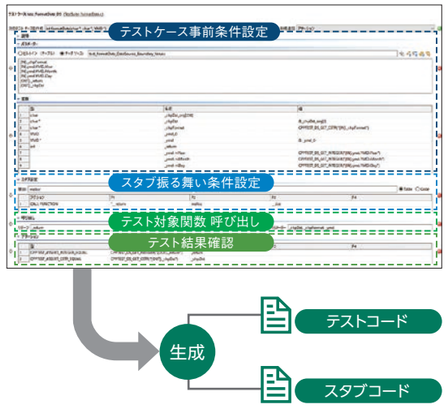
単体テスト

GUI操作でテストケースとスタブを生成。テストの実行と回帰テストを自動化

- テストドライバー、スタブ、テストケースを生成し、ソフトウェアの単体テストを自動化
- Excelで管理しているテストデータ、CppUnitのテストケースを活用

単体テスト時の課題であった「テストのためのコーディング」を行う必要はありません。C/C++testはGUI操作のみで「テストケース」の作成や「スタブ」の生成、さらにスタブの複雑な振る舞いの設定も可能です。また、テストケースとスタブを1つの画面でコントロールできるため、管理、メンテナンスを容易に行うことができます。
テストケース、スタブを作成するための工数およびこれらを管理、メンテナンスするための工数を大幅に削減します。また、外部テストデータの取り込みや、既存のテスト資産の再利用が可能です。

●テストケース・スタブを1画面でコントロール



カバレッジ計測

9種類のカバレッジを計測。単体テストの網羅性を視覚的にレポート

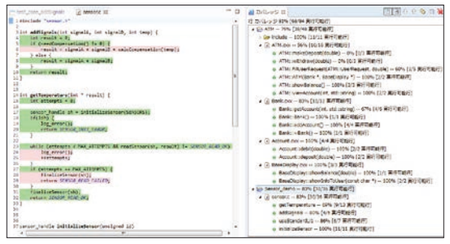
- プロジェクト、ファイル、関数単位でカバレッジの計測が可能
- 実行/未実行の箇所をハイライト表示

単体テスト実行時に自動的に9種類のカバレッジを計測します。複数のカバレッジを同時に計測することもできます。画面上で実行/未実行の箇所を分かりやすくハイライト表示するため、視覚的に確認することができます。

●C/C++testがレポートするカバレッジ

- ステートメントカバレッジ（C0:命令網羅率）
- 判断文カバレッジ（C1:分岐網羅率）
- 単純条件カバレッジ（C2:条件網羅率）
- MC/DC（Modified Condition/Decision Coverage）
- 関数カバレッジ
- コールカバレッジ
- 行カバレッジ
- 基本ブロックカバレッジ
- パスカバレッジ

●9種類のカバレッジを自動的に計測（行カバレッジの計測結果の例）



カバレッジアドバイザー

カバレッジアドバイザーで、単体テストを効率化

- 効率的にカバレッジを向上させるためのテストデータ作成を支援
- 実行できていない行をエディタで確認
- 複雑な条件分岐も瞬時に計算

カバレッジアドバイザーは、単体テストにおいて誰もが抱える「中身が複雑なコードのカバレッジを満たすのが大変」、「テストケース作成に必要なパラメータ、事前条件が多くて洗い出すのが大変」といった悩みの解決へアプローチします。
ソースコードの任意の行に対するワンステップの操作で、その行のカバレッジを満たすのに必要なテストのパラメータや事前条件を把握できます。事前条件を即座に把握できるため、ユーザーのテストに掛かる時間や労力を大幅に削減できます。

●カバレッジアドバイザーの実行結果イメージ

02. 動的解析

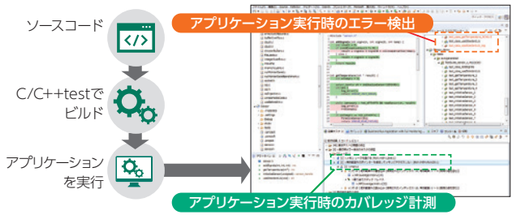
アプリケーションモニタリング

アプリケーション実行時に、メモリ関連エラーの検出とカバレッジを計測

●アプリケーション実行時のカバレッジを計測
●アプリケーション実行時に発生したエラーを自動検出

C/C++testは、システムテストを実施しながらカバレッジを計測することで、テストの抜け漏れを効率的に確認できます。また、不正メモリアクセス・メモリ破壊・メモリリーク・未初期化メモリの参照・NULLポインター参照などを検出し、スタックトレースと併せて問題をレポートします。また、システムテストに限らず、他のユニットテストフレームワークや独自のユニットテストフレームワークでのテスト実行時のカバレッジを計測できます。

●アプリケーション実行時のカバレッジ計測イメージ



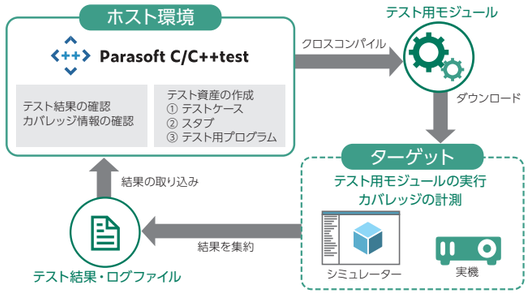
組み込みソフトウェア開発での利用

実機やシミュレーターで、単体テスト・カバレッジ計測が可能

●ホスト、シミュレーター、ターゲット環境で実行可能

C/C++testをインストールしたホストマシンだけでなく、実機（ターゲット機）や開発環境などに付属するシミュレーター上でも、単体テスト、カバレッジ計測（単体テスト時とアプリケーション実行時）および実行時メモリエラー検出を実行できます。
C/C++testは、さまざまな組み込みソフトウェアのクロス開発環境をサポートしています。

●組み込みソフトウェアでの単体テスト実行イメージ



03. 補助機能

CI/CDプラットフォーム連携

モダン開発ワークフローにおけるテスト自動化手法に対応

●Jenkins, GitHub, GitLab, Azure DevOpsへ簡単に統合可能
●CI/CDプラットフォーム上での解析結果確認

開発ワークフローにC/C++testを組み込むことで、テストの実施漏れを防ぎ、エラーや欠陥のフィードバックサイクルを早めることができます。自動化により開発者に負担をかけず、品質の高いソフトウェア開発をサポートします。

Docker連携

Dockerコンテナでの作業をサポート

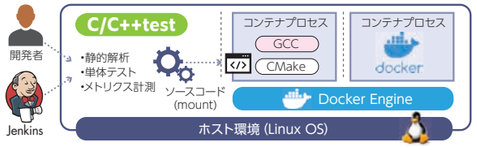
●Dockerコンテナ上のビルド環境を利用したテストが可能

ホスト環境上にインストールされたC/C++testから、Dockerコンテナ上に存在するビルド環境を利用し、静的解析および単体テストを実行することができます。
Jenkinsからも実行可能なため、CI環境にも組み込むことができます。

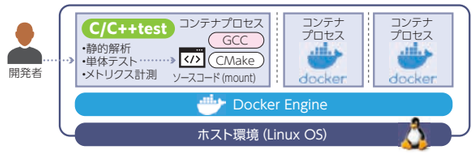
●Dockerイメージの配布で、テスト環境構築作業が不要に

C/C++testは、仮想環境上でも動作可能であるため、C/C++testを組み込んだ「Dockerイメージ」を開発者に配布することができます。これにより、ビルド環境だけでなく、C/C++testのテスト環境の構築作業もゼロにすることができます。

●「C/C++test」からDockerコンテナ内の環境を利用するイメージ図



●「C/C++test」をDockerコンテナ内で利用するイメージ図



GoogleTest連携

●GoogleTestでのテスト実行時のカバレッジ計測

GoogleTestで作成した既存のテストケースをそのままテスト資産として活用することができます。C/C++testのアプリケーションモニタリング機能を使用し、GoogleTestのテスト用プログラムをC/C++testを経由してビルドすることで、「C2カバレッジ」、「MC/DCカバレッジ」など9種類のカバレッジを取得することが可能となります。

レポート生成

●豊富な情報を見やすいレイアウトでレポート出力

テスト結果をHTML、PDF、XML、CSV、SARIF形式でレポート出力できます。レポートは、コーディング規約が守られていることを証明する場合などに利用できます。テスト実行に関する詳細な追加情報を出力することも可能です。

CSV　XML
PDF　HTML
SARIF

機能安全認証取得

●IEC 61508 / ISO 26262 / IEC 62304準拠

C/C++testは、第三者認証機関であるTÜV SÜD社よりIEC 61508およびISO 26262、IEC 62304に準拠したテストツールとして認証を取得済みです。

《機能安全規格準拠に役立つルールセット》
・HISソースコードメトリクス チェックルール
・MISRA C:1998、MISRA C:2004、MISRA C++:2008、MISRA C:2023（MISRA C:2012）、MISRA C++:2023 規約チェックルール

《医療機器ソフトウェア安全規格対応ルールセット》
・FDA C/C++（米国食品医薬品局）に関するルール

for IEC 61508
for ISO 26262
for IEC 62304

04. コンプライアンスパック

品質状況をリアルタイムに表示、レポートを自動生成

●MISRA C:2023/MISRA C++:2023のルールに完全対応、コンプライアンスレポート作成をサポート
●MISRA、AUTOSAR、CERT、CWEなどの遵守状況をリアルタイムに表示

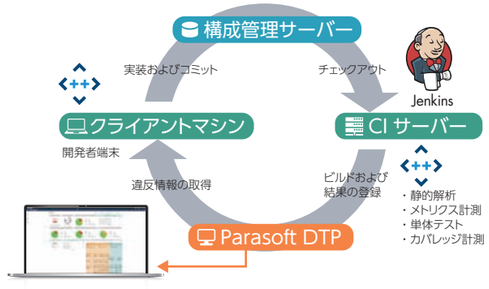
コンプライアンスパックは、MISRA、AUTOSAR、CERT、CWEなどの遵守状況をリアルタイムに表示するダッシュボード機能を提供します。また、コーディングガイドラインに則った遵守サマリーレポートや逸脱のレポートを自動生成します。
コーディングガイドラインの遵守状況の説明責任を果たすことが容易になるだけでなく、未遵守箇所を早期に特定し必要な措置を講ずることにより、欠陥のあるソフトウェアに関連するビジネスリスクを排除することが可能になります。

●MISRA 遵守用ダッシュボード／レポート出力

●Parasoft DTP（ダッシュボード）と連携したCI環境

Parasoft DTPは、C/C++testで行った静的解析/単体テストの結果、カバレッジなどの情報を自動的に収集・集約し、プロジェクトの状況をレポーティング、分析するためのツールです。
コーディング規約の遵守状況やプロジェクトの品質状況などをリアルタイムに表示します。CIに組み込むことで、常に最新のプロジェクト状況を確認することができます。開発者がレポーティングの作業をすることなく、管理者は各プロジェクトの状況を俯瞰して確認することができます。

●Parasoft DTPと連携したCI環境のイメージ図



最新の開発トレンド対応！言語規格・開発スタイルをサポート

C/C++testは、軽量なエディタであるVisual Studio Codeへのプラグインや、Dockerコンテナやクラウド環境での利用、Modern C++（C++17やC++20対応）をサポートしています。分散型SCMであるGitベースの開発ワークフローにシームレスに統合して利用することもできます。車載ソフトウェアを始めとして、組み込みソフトウェアでも採用が増えている開発スタイルにも適用できます。

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

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ご提供します。

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、幅広いサービスをご用意しています。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、お困り事、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作成後のお困り事、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

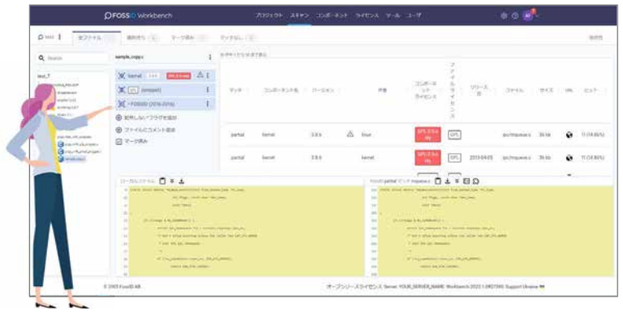
コードスニペットレベルで検出 OSS脆弱性・SBOM管理

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。

ソフトウェアサプライチェーンのリスク管理・SBOM作成

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、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

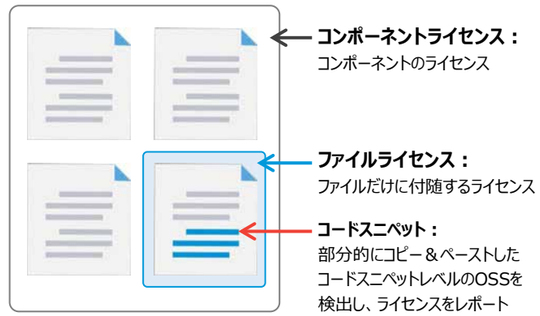
高速度スキャン：
独自のデータベースエンジンにより、非常に高速なスキャニングを実現しました。

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。

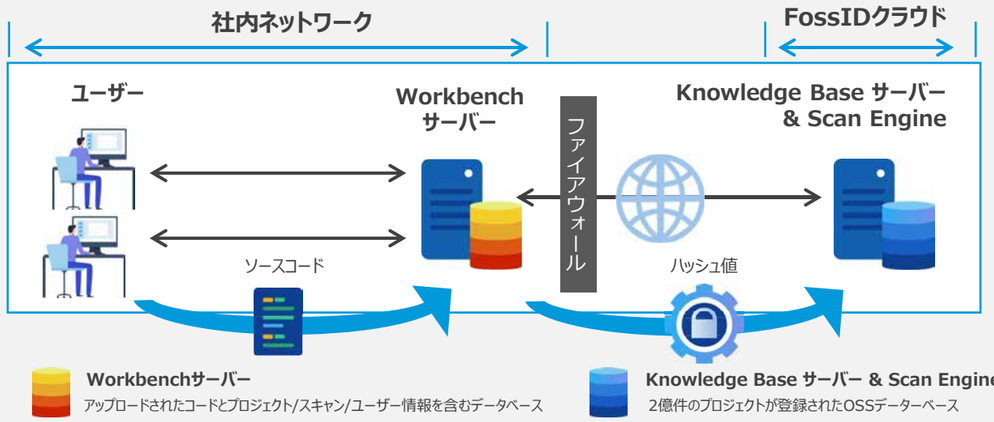


セキュリティ脆弱性（CVE）を検出：
OSSのコンポーネントとそれに関する既知の脆弱性（CVE）を識別するだけでなく、コンポーネントの中でも外でも、あるいは変更されたソースコードであっても、深く埋め込まれた個別のセキュリティ脆弱性を検出します。

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



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。

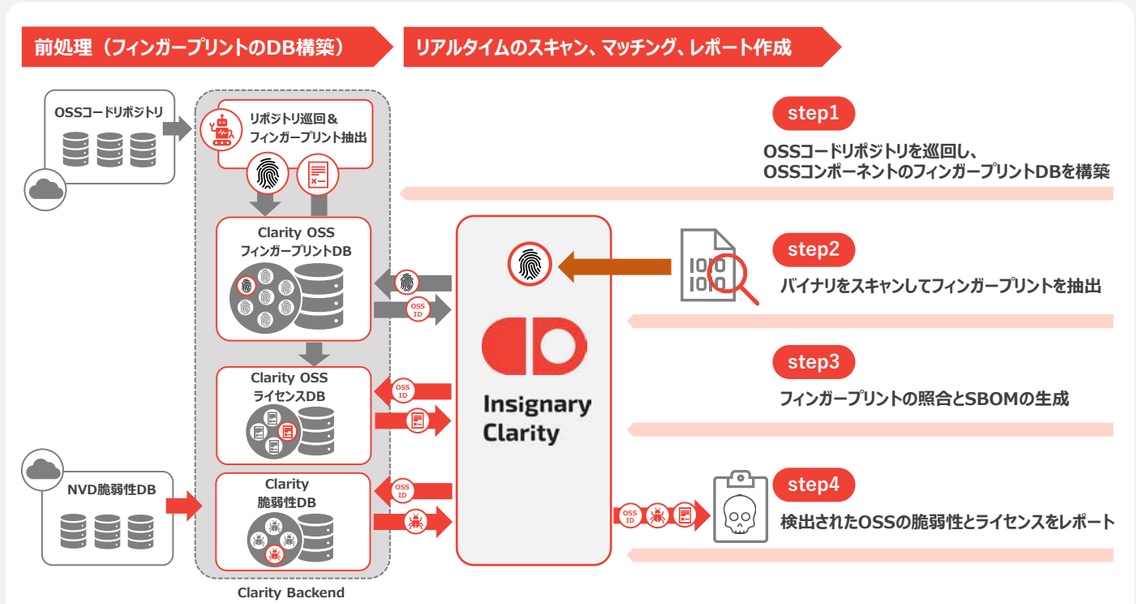
ソースコードからのOSSを検出

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