SYNOPSYS®

Coverity

静的解析

コーディング中に
セキュリティと品質の
重大な問題をすばやく
見つけて修正できます。

利点

- **セキュリティ・リスクの可視性が向上：**クラス最高の各種 AppSec ツールからのレポートが一箇所に集約されるため、プロジェクトのリスクを全体的な視点から網羅的に把握できます。
- **柔軟な導入：**どのプロジェクトにアプリケーション・セキュリティ・テストを実施するかによって、オンプレミスまたはクラウドでの導入を選べます。
- **セキュリティ・テストのシフト・レフト：**コーディング中に高精度な増分解析の結果が即座に提示されるため、ビルド / テスト工程に進む前に問題を修正できます。
- **開発者をサポート：**問題の修正方法を理解する上で必要なコンテキスト、詳細情報、アドバイスがすべて提示されるため、ソフトウェアの不具合を簡単かつ適切に修正できます。
- **コンテキストに応じた e ラーニング（別途 e ラーニング契約が必要）：**開発者が作成したコードに問題が見つかった場合、該当する CWE に関するセキュリティ・トレーニングを即座に受けることができ、事前にセキュリティの専門知識がなくても安心して開発できます。

概要

Coverity® はスピード、使いやすさ、精度、業界標準規格への適合、スケーラビリティを兼ね備え、高品質でセキュアなアプリケーションの開発を支援します。Coverity では開発プロセス早期のコーディング時に重大な品質上の不具合およびセキュリティ脆弱性を特定できるため、修正の手間とコストが最小に抑えられます。正確かつ具体的な修正アドバイス、およびコンテキストに応じた e ラーニングにより、セキュリティの専門知識がない開発者でも優先度の高い問題の修正方法をすばやく理解できます。Coverity は自動セキュリティ・テストを CI/CD パイプラインにシームレスに統合し、既存の開発ツールおよびワークフローをサポートします。また、Coverity は開発の場所とスタイルに応じてオンプレミスだけでなく、スケーラブルなアプリケーション・セキュリティ・プラットフォームを SaaS モデルとして提供するクラウド・ベースの Polaris ソフトウェア・インテグリティ・プラットフォームとしても導入できます。Coverity は 22 の言語および 70 を超えるフレームワークとテンプレートをサポートしています。

Coverity には、web およびモバイル・アプリケーション、マイクロサービス、IaC（Infrastructure-as-Code）構成を高速にスキャンできる軽量の静的解析エンジン Rapid Scan が搭載されています。Coverity でスキャンを実行すると、特別な設定をしなくても毎回自動で Rapid Scan が動作します。また、完全な CI ビルドの一環として、従来と同じスキャン時間をかけて Rapid Scan を実行することもできます。Rapid Scan は Code Sight™またはコマンドライン・インターフェイス、あるいは自動ビルド・パイプラインで単体のスキャン・エンジンとしても利用できます。このスタンドアロン・ユース・ケースでは、ほとんどのプロジェクトで実践的な早期解析結果を即座に得ることができます。セットアップは不要で、任意のディレクトリまたは Git リポジトリをポイントするだけで簡単に利用できます。各種プラットフォームおよびファイル・フォーマットを幅広くサポートしているため、IaC の構成ファイルを容易にスキャンできます。API および構成チェッカーにより、設定ファイルにおける API の誤使用や脆弱な構成を特定できます。Rapid Scan はコーディング中、およびコード・コミットごとに解析結果のフィードバックを即座に受け取りたいという開発者ニーズに最適です。複数の解析出力フォーマット（SARIF、JSON、コンソール）、および GitHub Actions と GitLab CI をサポートしているため、パイプライン・スキャンの自動化および課題管理をサポートできます。GitHub Actions は、プルリクエストにコード・レビューのフィードバックを統合します。Rapid Scan には、ポリシー・ファイルに課題を割り当てて自動的にビルドを中断する機能もあります。

主な特徴

高速かつ高精度な解析

- Code Sight™ IDE（統合開発環境）プラグインにより、開発者は IDE 環境でコーディングしながら即座に正確な解析結果を取得できます。Coverity は、特定された問題の修正に必要なすべての情報（詳細説明、カテゴリ、深刻度、CWE データ、不具合の位置、詳細な修正ガイダンス、データフローのトレースなど）と、IDE 上の課題のトリアージと管理機能を開発者に提供します。
- Coverity Point and Scan デスクトップ・アプリケーションは、ユーザーがソースコードをポイントするだけでアプリケーションをオンボードすることができます（IaC ビルド・キャプチャ機能を含む）。コマンドライン・インターフェイスを好む開発チームには、Coverity CLI 機能が同様の機能を提供します。

包括的なレポートおよびコンプライアンスの可視化

Coverity on Polaris はソフトウェア開発ライフサイクル（SDLC）の各ステージでアプリケーションのリスク状況を全体的な視点から捉えることができます。

- セキュリティ・チームは、アプリケーション・ポートフォリオ全体のリスク・プロファイルを一箇所にまとめて取得できます。解析結果は、API 経由で他のリスク・レポート・ツールにインポートできます。
- 特定した脆弱性のカテゴリごとに表示するフィルタ機能、トレンド・レポートの表示、脆弱性の重大度に基づく修正の優先付け、チームおよびプロジェクトの垣根を越えたセキュリティ・ポリシーへの適合管理（OWASP Top 10、CWE Top 25、PCI DSS など）を実行できます。
- タイムフレームを切り替えて重大度を確認できる時系列の問題レポートにより、プロジェクトのセキュリティ態勢を一目で把握できます。このレポートを PDF 形式でダウンロードしておくと、監査用の詳細なコンプライアンス記録として利用できます。

また、Coverity は C/C++ コードの品質問題の特定に関してクラス最高の精度を達成している他、安全、セキュリティ、信頼性に関する標準規格（MISRA®、CERT C/C++、CERT Java、DISA STIG、ISO 26262、ISO/IEC TS 17961、AUTOSAR® など）や NVIDIA 社の CUDA C++ ガイドラインに記載されている品質上の問題も包括的にサポートしています。Coverity Qualification Kit(Q-Kit) は、Coverity がセーフティ・クリティカルなプロジェクトに適切に設定され、業界の安全基準を満たしていることを保証します。

エンタープライズ環境に適したスケーラビリティとアジリティ

- Polaris プラットフォームの Coverity は、オンプレミスで高価な機材を導入・維持する必要がなく、ビジネス・ニーズの成長に合わせてアプリケーション・セキュリティ・テストを弾力的に拡張できます。
- Polaris のセットアップは簡単。専用の URL にログインし、コマンドライン・インターフェイス（CLI）をダウンロードしてインストールするか、CI ワークフローから実行するだけでソースコードの解析を開始できます。
- Polaris プラットフォームの Coverity は、可用性の高いクラウド・プラットフォーム上で解析エンジンが動作するため、開発者やプロジェクトの数が数千に達しても容易に対応でき、優れた性能とアップタイムを維持しながら数百万件もの問題を管理できます。

ソフトウェア開発ライフサイクル（SDLC）との統合

- Code Sight プラグインは Visual Studio、Eclipse、IntelliJ、WebStorm、PyCharm、PhpStorm、RubyMine のマーケットプレイス Web サイトからダウンロードでき、面倒な設定なしで利用できます。
- Coverity は各種 IDE（Visual Studio、Visual Studio Code、Eclipse、IntelliJ、RubyMine、Wind River Workbench および Android Studio など）用のレガシーなネイティブ統合機能も備えており、ソースコード・マネージメント（SCM）ソリューション、バグ追跡システム（Jira、Bugzilla など）、CI ビルド・ツール（Jenkins、Azure DevOps など）、アプリケーション・ライフサイクル・マネージメント（ALM）ソリューションとネイティブに統合します。
- 解析結果は、REST API 経由でその他のビルド自動化ソリューション、および他のエンタープライズまたはカスタム・ツールにインポートできます。
- Polaris プラットフォームの Coverity には、開発ステージおよびデプロイ前ステージでのクラウド・ベースの自動セキュリティ・テストをサポートするプラグインおよび統合機能もあります。
- 解析結果は、REST API 経由でセキュリティ / リスク・レポート・ツールにインポートできます。詳細は、Polaris のデータシートをご参照ください。

ダッシュボードによる問題の一元管理

- 開発マネージャーは、全体的なセキュリティ・リスクや業界標準規格（OWASP Top 10、CWE Top 25 など）への適合状況、および優先課題に対する個々の開発者やプロジェクト・チーム全体の進捗状況を時系列で示したトレンドライン・チャートを作成できます。
- 業界で認知されている優先リスト、上位 5 つの問題タイプ、テクニカル・リスク指標などのレポートをダッシュボードで簡単に確認できるため、それぞれの組織にとって最も重要な問題から優先的に対策をとることができます。
- CWE、標準規格の分類、優先リスト、リスク指標、パス、開発者（オーナー）ごとに問題を絞り込み / グループ化できる定義済みフィルタが用意されています。

標準準拠と脆弱性検知を拡張

Coverity Extend は、開発者が固有の欠陥タイプを検出できるようにする、使いやすいソフトウェア開発キット（SDK）です。SDK は、カスタムまたはドメイン固有の欠陥を特定するためのプログラムアナライザーまたはチェッカーを作成するためのフレームワークです。Coverity CodeXM は、開発者が独自のカスタムチェッカーを簡単に開発できるようにするドメイン固有の関数型プログラミング言語です。これらのカスタマイズされたチェッカーは、企業のセキュリティ要件および業界標準またはガイドラインへの準拠をサポートします。

Coverity 静的解析 | 技術スペック

対応言語とプラットフォーム

- Apex
- C/C++*
- C#*
- CUDA
- Java*#
- JavaScript*#
- PHP*#
- Python*
- .NET Core
- ASP.NET
- Objective-C/C++*
- Go
- JSP
- Ruby*
- Swift*#
- Fortran
- Scala
- VB.NET
- iOS
- Android
- TypeScript*#
- Kotlin

* これらの言語は現在、Coverity の Point and Scan デスクトップ・アプリケーションと Coverity CLI 機能でサポートされています。
# これらの言語は Rapid Scan によるソースコードの脆弱性スキャンでサポートされます。

対応 IaC プラットフォームとファイル・フォーマット

プラットフォーム

- Terraform
- AWS CloudFormation
- Kubernetes
- Helm
- ELK

ファイル・フォーマット

- JSON
- YAML
- HCL (Terraform)
- HTML
- XML
- plist
- TOML
- Properties
- Vue テンプレート
- JSX
- TSX

対応クラウド・デプロイメント

- Coverity Connect は AWS、Azure および GCP パブリック・クラウドのコンテナ内で実行できます。
- 対応クラウド・ネイティブ・テクノロジー：Docker、Kubernetes

対応フレームワーク

Coverity は Java、JavaScript、C# などに対応する 70 種類以上のフレームワークに対応しています。Coverity は、AWS サービス（EC2、S3、DynamoDB、IAM）および Google Cloud Storage API（GCP）とやり取りするクラウドネイティブの JavaScript アプリケーション用の主要なクラウドプロバイダー API フレームワークのセキュリティモデリングもサポートしています。

Java

- Android SDK
- Apache Shiro
- Axis
- DWR
- Enterprise Java Beans (EJBs)
- GWT
- Hibernate
- iBatis
- Java フレームワーク
- Java Persistence API (JPA)
- Javax.websocket
- JAX RS
- JAX WS
- JEE
- JSF/Facelets
- JSP and JSP Standard Tag Library (JSTL)
- ReactiveX (RxJava, Reactor)
- Restlet
- Spring Boot
- Spring Framework
- Struts
- Terasoluna
- Tiles
- Vert.x
- WS XML-RPC

C#

- ASP.NET Core MVC/ASP.NET MVC
- ASP.NET Core Web API
- ASP.NET ASMX Web Services
- ASP.NET Web Forms
- Identity Server
- MassTransit
- Razor templates
- WCF Services

JavaScript/TypeScript

クライアント側

- Angular
- Angular JS
- Apache Cordova
- Backbone
- Bootstrap
- Ember
- HTML5 DOM APIs/Ajax
- jQuery
- Mithril
- React/ Preact
- React Native
- Socket.IO
- Swig
- Vue

サーバー側

- Angular server-side rendering (Express and Hapi engines)
- Express
- Fastify
- Hapi
- Koa
- Mean.io
- Node
- Passport
- React server-side rendering (Next.js)
- Restify
- SAP XS Classic and Advanced
- Socket.IO
- Vue server-side rendering

テンプレートエンジン

- Consolidate
- doT.js
- EJS
- Handlebars
- Hogan
- Jade
- koa-views
- Lodash (templating)
- Marko
- Mustache
- Nunjucks
- Pug
- Swig
- Twig
- Underscore (templating)
- Vision

主要なライブラリ

- Axios
- Google Cloud APIs (Storage)
- Mongoose / MongoDB
- Request
- Sequelize
- Sqlx
- Swashbuckle
- Underscore / Lodash

GO

- Echo

PHP

- Symfony

Python

- Flask
- Django

Ruby

- Ruby on Rails

Rapid Scan IaC フレームワーク

- Android
- Apache Cordova
- Apache Kafka
- Apache Struts
- Apache Zookeeper
- Apollo GraphQL
- AWS CloudFormation
- Consul
- Express
- Grails® フレームワーク
- GraphQL
- Istio
- Jakarta Server Faces
- Java/Jakarta EE
- Kubernetes
- MyBatis
- Node.js
- OpenAPI
- Postman
- RabbitMQ
- React
- Socket.IO
- Spring
- Terraform
- Vue.js

対応プラットフォーム

- Windows
- Linux
- Mac OS X
- Solaris
- AIX
- FreeBSD

SDLC ネイティブ統合

SCM

- AccuRev
- Apache Subversion (SVN)
- CVS
- Git
- Mercurial (Hg)
- Perforce Helix
- Team Foundation Server SCM

レガシー IDE

- IBM Rational Team Concert
- QNX Momentics
- Wind River Workbench

CI ビルドサーバー

- Azure DevOps Server
- Bazel
- Jenkins

Code Sight 対応の IDE†

- Visual Studio for VB.NET, C#, C/C++, JavaScript, PHP, Python, Ruby, TypeScript
- Visual Studio Code for C# (.NET Core), C/C++, Java, JavaScript, PHP, Python, Ruby, TypeScript
- Visual Studio Code (Rapid Scan) for Java, JavaScript, and TypeScript
- Eclipse for Java, JavaScript, C/C++, PHP, Python, Ruby, TypeScript
- IntelliJ for Java, JavaScript, PHP, Python, Ruby, TypeScript
- WebStorm for JavaScript, TypeScript
- PyCharm for Python
- PhpStorm for PHP
- RubyMine for Ruby

バグ追跡システム

- Jira
- Bugzilla

対応コンパイラ

- Analog Devices Blackfin
- Analog Devices SHARC
- Analog Devices TigerSHARC
- ARM C/C++
- Borland C++
- CEVA BXx
- CEVA XC16
- CEVA-X2
- CEVA-XC4500
- Clang
- Cosmic C
- Freescale CodeWarrior
- GNU GCC/G++
- GHS PowerPC on Windows
- Green Hills C/C++/EC++
- HI-TECH PICC
- IAR C/C++
- IBM AIX
- IBM XLC
- Intel C++ for Windows
- JDK for Mac OS X
- Keil compilers
- Marvell MSA
- MPLAB XC8
- Nvidia CUDA Compiler (NVCC)
- OpenJDK
- QNX C/C++
- Renesas C/C++
- SNC C/C++
- SNC GNU C/C++
- SONY PS4 SDK
- STMicroelectronics GNU C/C++
- STMicroelectronics ST Micro C/C++
- Sun (Oracle) CC
- Sun/Oracle JDK
- Synopsys MetaWare C and C++
- Tasking for ARM Cortex and TriCore
- TI Code Composer
- Visual Studio
- Wind River C/C++

他

クリティカルチェッカー

- API 使用エラー
- コーディング・エラーのベストプラクティス
- バッファ・オーバーフロー
- ビルド・システムの問題
- クラス階層の不一致
- コードのメンテナンス性の問題
- 同時データアクセス違反
- 制御フローの問題
- クロスサイト・リクエスト・フォージェリ (CSRF)
- クロスサイト・スクリプティング (XSS)
- デッドロック
- エラー処理の問題
- ハードコードされた証明書
- 不正な式
- セキュアでないデータ処理
- 整数の取り扱いの問題
- 整数オーバーフロー
- メモリー：破損
- メモリー：不正アクセス
- NULL ポインタの参照先取得エラー
- パス操作
- 非効率なパフォーマンス
- プログラムのハング
- 競合状態
- リソースリーク
- コーディングルール違反
- セキュリティ・ベストプラクティスの違反
- セキュリティ設定ミス
- SQL インジェクション
- メンバーの未初期化

† 最新の CodeSight と対応する IDE のバージョンについては、こちらをご参照ください。https://dev.sig-docs.synopsys.com/codesight/topics/support_matrix/r_codesight_support_matrix.html

Rapid Scan 解析エンジンに関する最新の発表内容およびリリース・アップデート (スタンドアロン・ユース・ケース) はこちらをご覧ください。

このデータシートは、Coverity 2023.6.0 以降のバージョンに適用されます。

シノプシスの特色

シノプシスがご提供する統合型ソリューションは、ソフトウェア開発とデリバリのあり方を根底から変革し、ビジネス・リスクに対処しながらイノベーションを加速することを可能にします。シノプシスのソリューションにより、開発者はスピードを落とすことなくセキュアなコードを作成することができます。開発および DevSecOps チームはスピードを犠牲にすることなく、開発パイプライン内でテストを自動化できます。セキュリティ・チームは先手を打ったリスク管理が可能となり、組織にとって最も重要な問題の修正に集中できます。シノプシスは業界随一のノウハウを活かし、最適なセキュリティ・イニシアティブの立案と実行をご支援します。信頼性の高いソフトウェアの構築に必要なものをワンストップでご提供できるのは、シノプシスだけです。

詳しくは、www.synopsys.com/jp/software をご覧ください。

日本シノプシス合同会社 ソフトウェア インテグリティ グループ
〒 158-0094 東京都世田谷区玉川
2-21-1 二子玉川ライズオフィス

TEL: 03-6746-3600
Email: sig-japan@synopsys.com
www.synopsys.com/jp/software