SYNOPSYS®

Coverity 静的解析

Coverityは、ソースコードに潜む重大な不具合やセキュリティ脆弱性をコーディング中に高精度で検出する正確で包括的な静的解析およびSAST（静的アプリケーション・セキュリティ・テスト）のプラットフォームです。

概要

Coverity静的解析は数々の特許解析技術、10年間にわたる研究開発、そしてオープンソースを含む数兆行ものコード解析に基づき、品質上の重大な不具合や潜在的なセキュリティ脆弱性を開発段階で洗い出し、信頼性の高い実践的な修正ガイダンスを提示することにより、リスク軽減とプロジェクト全体のコスト削減に貢献します。

主な特徴

解析の深さと精度

- Coverity静的解析はソースコードおよび基盤のフレームワークを詳細に把握することで高精度かつ実行可能な解析結果を提供します。このため、大量の誤検出で開発者の時間を無駄にすることがなく、アジャイルなCI/CDワークフローのスピードで開発ライフサイクルにセキュリティを効率よく組み込むことができます。
- Coverity静的解析はフルパス・カバレッジをサポートしており、すべてのコード行およびすべての潜在的な実行パスを確実にテストします。複数の特許技術により、深く正確な解析が可能です。
- Coverity静的解析はお使いのビルド・システムと統合し、ソースコードの正確な表現と挙動を生成します。
- 開発チームはCoverityにプロジェクトのソースコードを指定するだけで、ビルドを実行することなく、多くの言語を分析できます。

解析のスピードとスケール

Coverityはどのような既存のワークフローにも統合できるようにゼロから設計されています。主な特長は以下のとおりです。

- Coverityは最大16コアを利用した並列解析が可能で、シリアル解析に比べ最大で10倍のパフォーマンスを発揮します。
- 高速デスクトップ解析と増分解析はコードベース全体ではなく変更のあったコードまたは変更の影響を受けるコードのみを再解析するため、解析時間が短縮します。ファイル・システム・キャプチャは未コンパイルのコードも解析可能なため、最初に完全なビルドを実行する必要がありません。
- Coverityは優れたスケーラビリティを備えており、広域分散環境における数千人規模の開発者をサポートできます。プロジェクトのコードが1億行を超えても容易に解析できます。

ソース段階でのセキュリティ対策

- 重大な不具合のトラブルシューティングと修正を短時間で効率よく進められるよう、開発者に必要な情報を提示します。
- 品質とセキュリティを開発フローに組み込むことにより、開発サイクル終盤に不具合が見つかった場合に生じる手戻りのコストを軽減し、製品リリースの遅れを防ぎます。
- 量産開始後または製品発売後にソフトウェア不具合やセキュリティ脆弱性が見つかった場合の多大なコストとブランド失墜を防ぎます。

ソフトウェア開発ライフサイクル（SDLC）との統合

- Coverityは、バージョン管理システム、ビルドおよび継続的インテグレーション（CI）、バグ・トラッキング、アプリケーション・ライフサイクル・マネジメント（ALM）ソリューションや統合開発環境（IDE）など、開発プロセスをサポートする重要なツールやシステムと短時間で統合できます。
- オープンなプラットフォームであるため、サードパーティの解析結果をワークフローにインポートして、ソフトウェア不具合やリスクと同じビューで一元的に表示することで、あらゆる種類の不具合を、同様に管理できます。

問題の効率的な管理と修正

- このプラットフォームでは、共同問題管理インターフェイスのCoverity Connect から具体的な情報と的確な修正ガイダンスが開発者に提示されるため、セキュリティに関する深い知識がなくても指示されたコード行を指示された方法で修正するだけで不具合を解消できます。
- Coverity Connectには不具合へのパスを正確に指摘するソースコード・ナビゲーション機能があり、共有コード全体で出現するすべての不具合を自動的に洗い出します。
- 検出された不具合は解決に最も適した開発者に自動的にアサインされます。セキュリティ、OWASP Top 10、CWE、PCI DSSに関する問題や、同様に品質、MISRA、CERT C/C++、およびAUTOSARに関する問題はすぐに確認できます。

基準への適合と脆弱性の検出を拡張

Coverity Extendは、検出可能な不具合の種類を開発者が独自に拡張できる使いやすいソフトウェア開発キット（SDK）です。このSDKをフレームワークとして利用してプログラム・アナライザ（チェッカー）を記述すると、カスタムまたは特定分野の不具合を検出できます。Coverity CodeXMは特定分野向けの関数型プログラミング言語で、開発者が独自のカスタム・チェッカーを容易に記述できます。これらのカスタム・チェッカーにより、企業ごとのセキュリティ要件や業界標準規格およびガイドラインへの準拠をサポートします。

受け入れを促進し、リスクを軽減

Coverity Policy Managerを使用することで、コード・セキュリティおよび品質、テストに関して開発チームの垣根を越えた一貫性のある基準を定義し、これら基準への適合を図ることができます。チーム単位、プロジェクト単位、コンポーネント単位でこれらの基準への適合状況が可視化され、不具合やテストに関して事前に定義した指標に基づいて定量的にステージ節目での合否を判断できます。このビューはカスタマイズ可能なため、組込み、エンタープライズ、モバイルなど各種アプリケーションの目的に応じた開発指標およびしきい値を選択できます。

SYNOPSYS®

Coverity 静的解析
技術スペック

対応言語

- C/C++
- C#
- Java
- JavaScript
- PHP
- Python
- .NET Core
- ASP.NET
- Objective-C
- JSP
- Node.js
- Ruby
- Android
- Swift
- Fortran
- Scala
- VB.NET
- iOS
- TypeScript

対応フレームワーク

CoverityはJava、JavaScript、C#などに対応する50種類以上のフレームワークに対応しています。

Java

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

C#

- ASP.NET MVC
- ASP.NET ASMX Web Services
- ASP.NET Web API
- ASP.NET Web Forms
- ASP.NET Core
- ASP.NET Core MVC
- WCF services
- Razor templates

JavaScript/TypeScript

クライアント側

- HTML5 DOM APIs / Ajax
- jQuery
- AngularJS
- Angular
- Vue
- React / Preact
- Backbone
- Socket.IO
- Bootstrap
- Mithril

サーバー側

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

テンプレートエンジン

- Nunjucks
- Consolidate
- Haml
- Marko
- Hogan
- Vision
- Koa-views

JSテンプレートDAをサポートするテンプレートエンジン

- EJS
- Handlebars
- Swig
- Pug
- Jade

主要なライブラリ

- Underscore / Lodash
- Axios
- Sequelize
- Request
- Mongoose / MongoDB

PHP

- Symfony

Python

- Flask
- Django

Ruby

- Ruby on Rails

対応プラットフォーム

- Windows
- Linux
- Mac OS X
- Solaris
- AIX
- HP-UX
- NetBSD
- FreeBSD

SDLC統合

SCM

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

IDE/CI

- Android Studio
- Eclipse
- IBM Rational Team Concert
- IntelliJ IDEA, WebStorm, RubyMine, PhpStorm, PyCharm
- MS Visual Studio
- QNX Momentics
- Team Foundation Server
- Wind River Workbench
- Jenkins

バグ・トラッキング

- Jira
- Bugzilla

対応コンパイラ

- ARM C/C++
- Borland C++
- CEVA-XC4500
- Clang
- Cosmic C
- Freescale CodeWarrior
- GNU GCC/G++
- Green Hills C/C++/EC++
- HI-TECH PICC
- HP aCC
- IAR C/C++
- IBM AIX
- IBM XLC
- Intel C++
- JDK for Mac OS X
- Keil compilers
- Marvell MSA
- MPLAB XC8
- OpenJDK
- QNX C/C++
- Renesas C/C++
- SNC C/C++
- SNC GNU C/C++
- Sony ORBIS SDK
- Sony PS4
- STMicroelectronics GNU C/C++
- STMicroelectronics ST Micro C/C++
- Sun (Oracle) CC
- Sun/Oracle JDK
- Synopsys MetaWare C and C++
- TASKING for ARM Cortex
- TI Code Composer
- Visual Studio
- VisualDSP++
- 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
- ビルド・システムの問題
- バッファ・オーバーフロー
- 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・スクリプティング（XSS）
- クロスサイト・リクエスト・フォージェリ（CSRF）
- 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
- 整数の取り扱いの問題
- 整数オーバーフロー
- セキュアでないデータ処理
- 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

シノプシスの特色

シノプシスのソフトウェア インテグリティ グループは、企業が安全で高品質のソフトウェアを構築し、リスクを最小限に抑えながらスピードと生産性の最大化に貢献します。シノプシスは、アプリケーション・セキュリティのリーダーであり、静的解析、ソフトウェア・コンポジション解析、動的解析ソリューションを提供しており、独自のコード、オープンソース・コンポーネント、およびアプリケーションの動作における脆弱性や欠陥を迅速に見つけて修正します。業界をリードするツール、サービス、専門知識を組み合わせることで、シノプシスはDevSecOpsにおけるセキュリティと品質を最大化し、ソフトウェア開発のライフサイクル全体にわたって組織を支援します。

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