SYNOPSYS®

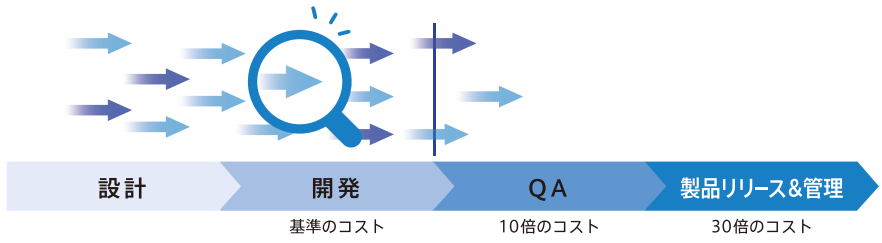
SRA GROUP

静的コード解析 Coverity

開発上流工程での品質向上・脆弱性対策

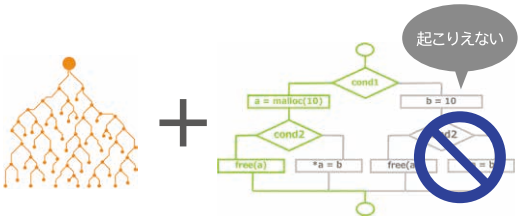
開発早期に、ソースコードからバグや脆弱性を検出
Coverityで、高品質・セキュア開発のシフトレフトが可能です。

開発段階でバグ、脆弱性を自動的に検知。修正の十分な時間を確保。



高リスクな不具合の検知（誤検知率：低）

クラス・関数・ファイルを跨ぐ全ての分析パターンを網羅する「フルパス解析」で、抜け・漏れなく修正すべき箇所を指摘。



わかりやすい指摘、修正ガイダンス

修正すべき箇所や修正方法がわかりやすく、開発者は容易に対応可能。

言語、セキュリティガイドライン、標準準拠、開発プロセス対応

JS, Scala, Microsoft ASP.net, Fortran, php, Microsoft VB.net, Kotlin, GO, TS, python, node, .NET Core, NVIDIA CUDA, C C++ Objective C, Java

OWASP, CWE, CWE and SANS Institute TOP 25 MOST DANGEROUS SOFTWARE ERRORS, OWASP Open Web Application Security Project

CERT, ISO 26262, FDA, PCI, MISRA, JSF++, AUTOSAR

Android Studio, IntelliJIDEA, Atlassian JIRA, Bugzilla, Jenkins, eclipse, Visual Studio, git

実行時エラーにつながる不具合を検出　検出可能な不具合例

並列処理の問題
・デッドロック
・競合状態
・ブロック呼び出しの誤用

パフォーマンスの低下
・メモリリーク
・スタックの使用度合い

クラッシュの原因
・Nullポインタの間接参照
・ポインタの解放後のメモリ使用
・二重解放

セキュリティ上の脆弱性
・バッファ・オーバーフロー
・外部入力値の不適切な利用

APIなどの不適切な使用
・APIエラー処理

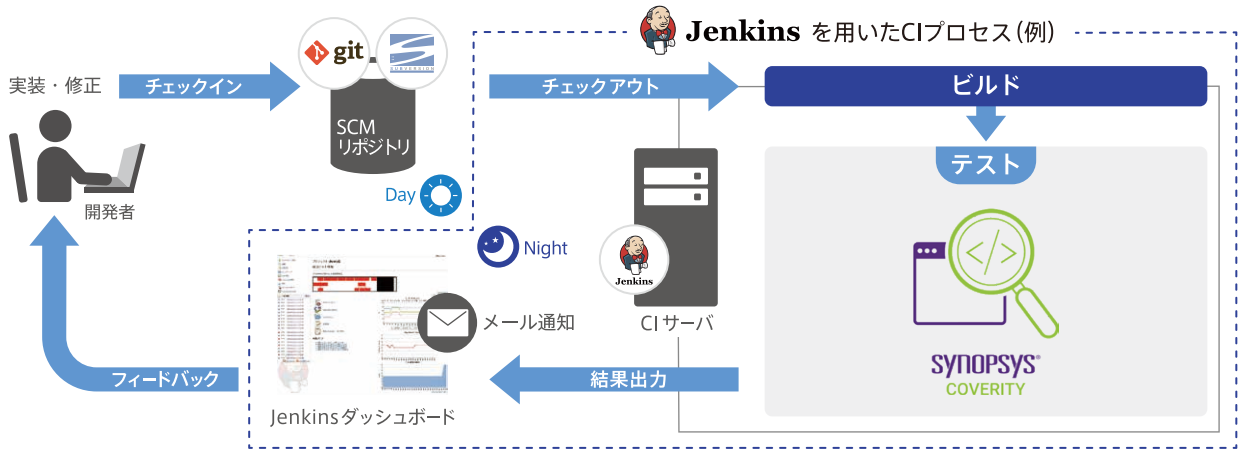
プログラムの不正な動作
・デッドコード
・未初期化変数
・コピー＆ペーストのミス

導入メリット

- テスト工程以降で発見される不具合や脆弱性を最小化
- 予期せぬ不具合によるリリース遅延リスクの回避
- 市場で不具合が発生する事による顧客満足度・ブランドイメージの低下を阻止
- テスト工程での工数削減による、開発トータルコスト低減
- 不具合の指摘により開発者の問題意識と対応スキルが向上

Coverityの効率的な活用方法

CI（継続的インテグレーション）プロセスへの組込みによる自動化



【お問い合わせ】　株式会社 SRA　関西事業部
TEL：06-4704-2611　E-Mail：kb-sales@sra.co.jp　URL：https://www.sra.co.jp/coverity