

テストケース生成からテスト実行までをワンクリックで自動実行。
セキュアなアプリケーションの開発やフレームワークアプリケーションのテスト、
Google Androidアプリケーションの静的検証など、
対応範囲がさらに進化したJava対応自動テストツール、Jtest



- ◎単体テストプロセスを自動化
- ◎充実したコーディングルールによる静的解析
- ◎Google Androidや組み込みJavaソースコードを静的に検証
- ◎セキュアコーディングチェック機能を標準装備
- ◎リソースリークや配列を超えたアクセスなどを静的に検証するバグ探偵機能を搭載

テストケース生成から単体テスト実行までを自動化。さらに静的解析も自動実行。 効率的なテスト環境を提供し、アプリケーションの品質と生産性を向上させます。

動的解析

単体テスト

テストケース、テストスタブを自動生成し、単体テストを自動実行します。テスト実行時にコードカバレッジを測定。テストの妥当性を確認できます。

実行時エラー検出

単体テスト時、アプリケーション実行時にアプリケーションを監視し、スレッドに関するデッドロックの問題やクラッシュ、セキュリティに関する問題を検出します。

静的解析

コーディング規約チェック

セキュリティやGoogle Androidなどを含む1,000個のコーディングルールで、ソースコードを検証。問題を引き起こす可能性のあるコードを検出します。

処理フロー解析 (バグ探偵)

実行パスを検証し、リソースリーク、配列を超えたアクセス、セキュリティ脆弱性の可能性のあるコードを検出します。
※バグ探偵は、Server EditionまたはJtest Securityに含まれる機能です。

動的解析

単体テスト

テストケース、テストスタブを自動生成

テスト対象クラスを解析し、キャッチされない実行時例外を発生させるテストケースやコードの広範囲をカバーするテストケースを自動生成します。利用できない外部リソースを参照している場合には、テストスタブを自動生成するので、スタートボタンをクリックするだけでテストを開始することができます。

テストカバレッジ情報をレポート

テスト実行時に行カバレッジと判断文カバレッジを計測。テストカバレッジ情報をプロジェクト、ファイル、メソッド単位でレポートします。テストカバレッジを確認しながらテストを実施することで、信頼性の高いテストが実施できます。

サーバーサイドコンポーネントのテストを自動化

Cactusを使用したテストケースを自動的に生成し、サーバーサイドコードのテストを自動化します。デブロイ後や実環境以外では実行することが難しいサーバーサイドコンポーネントのテストを開発者のデスクトップ上で実施することが可能です。開発の後期で実施することが多いEJBやサーブレット、StrutsActionクラス、Springクラスなどのテストを開発の早期に実施できるので、デバッグ作業の大幅な軽減が期待できます。

実行時エラー検出

単体テストレベルでは検出が難しいスレッドに関するデッドロックの問題やアプリケーションのクラッシュに繋がる問題、セキュリティに関する問題を単体テスト時またはアプリケーション実行時に自動的に検出します。運用後に発生する可能性のある重大なエラーをリリース前に発見、修正できます。また、アプリケーション実行時のカバレッジも計測するので、テスト漏れを確認できます。

検出するエラーの種類

- 競合条件
- セキュリティ攻撃の脆弱性
- 例外
- リソースリーク

単体テストモード

単体テストモードでは、単体テスト時に実行時エラーを検出、レポートします。単体テストという開発早期に実施する工程で、実行時エラーの有無を確認することにより、結合テスト以降で発見される場合に比べて、はるかに少ない工数でエラーの修正が行えます。また、実際のアプリケーションでは実行することが困難な例外処理のパターンについても、単体テストモードを利用して容易に検証が行えます。

※動的解析機能はJtest Securityには含まれません。

アプリケーションモード

実際にアプリケーションを動作させる環境で、アプリケーションを実行し、実行時エラーを検出できます。アプリケーションの完成に近い段階で実行時エラーを検証することで、運用後に発生する可能性のある重大なエラーをリリース前に発見、修正できます。

テストケースの作成からテストの実行までの自動処理を実現させたJava対応自動テストツール>Jtest。効率的なテスト環境を提供し、製品品質を向上させます。

自動生成されるテストケースは、ホワイトボックステストやブラックボックステスト、回帰テストに適用され、コードを徹底的にテストします。また、ソース

コードの静的解析についても、あらかじめ搭載されている約1,000種類のコーディングルールを自由に利用できます。これにより、開発サイクルにあわせた適切なルールを適用でき、従来にないスムーズでスピーディなテスト環境の構築が可能です。

静的解析

静的解析

Jtestは、Javaエキスパートたちが推奨する約1,000種類のコーディングルールに従ってソースコードを静的に解析し、違反している箇所をレポートするほか、約70種類のメトリクスルールに従ってコードを計測します。多くのルールにはカスタマイズ可能なパラメータがあり、ニーズに合わせて詳細な条件を指定できます。また、RuleWizard[®]によって、グラフィカルなインターフェースを使用してユーザー独自のルールを追加することも可能です。

Jtestのコーディングルールカテゴリ

- 重複コードの検出
- Enterprise JavaBeans
- 例外
- ガーベージコレクション
- Hibernate フレームワーク
- Java データベース接続
- Java Server Pages
- 最適化
- バグの可能性
- プロパティファイル
- セキュリティ
- サーブレット
- Struts フレームワーク
- スレッド同期化
- XML 開発
- Google Android
- 組込みデバイス など

※バグ探偵に含まれるセキュリティルールは、Server EditionおよびJtest Securityにのみ含まれます。

コードメトリクスの計測

メソッド数、オブジェクトの結合度、サイクロマティック複雑度など約70種類のメトリクスをレポートします。GUIのテーブル形式のビューにメトリクス情報を表示したり、XML形式またはHTML形式のレポートを出力したりできます。また、メトリクスが指定された許容範囲を超える場合に、違反としてレポートすることもできます。

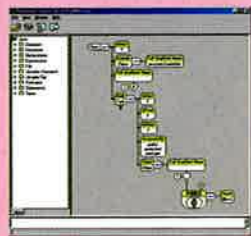
※XML形式のレポート出力機能は、Server Editionにのみ含まれます。

コーディングルール作成ツール

RuleWizard

ユーザー定義コーディングルールを作成する「RuleWizard」が搭載されています。

RuleWizardでは、視覚的にコーディングルールを作成したり、サンプルソースからコーディングルールを自動生成することが可能です。



処理フロー解析 (バグ探偵)

リソースリークや配列を超えたアクセスを静的に検出するバグ探偵機能

バグ探偵は実行パスを検証し、処理フローや渡された値によって発生する問題点を指摘します。処理フローが複数のクラスやパッケージに渡った複雑なパスも検証できるので、クラス単位で実行する静的解析や単体テストでは発見することが難しい実行パスとデータの組み合わせによって発生するリソースリークやNullPointerExceptionといった検出困難な問題点を検出します。バグ探偵は静的に検証するので、人手によるテストに比べて、網羅性の高い検証が可能です。さらに、問題の起点から発生までの処理フローをレポートするので、デバッグ作業が容易になります。

※バグ探偵は、Server EditionおよびJtest Securityにのみ含まれます。



バグ探偵が検出する問題

- NullPointerException
- 配列を超えたアクセス
- nullチェックの前の間接参照
- セキュリティの脆弱性
- リソースリーク

ソースコードセキュリティ検証

バグ探偵(フロー解析)と静的解析(コーディングルールを使用したパターンマッチング解析)の機能を使って、OWASP (Open Web Application Security Project) やPCI DSS (Payment Card Industry Data Security Standard) に掲載されている脆弱性を有するソースコードを検出します。また、Parasoft社が独自に選択した脆弱性を検出するルールセットも搭載されています。Jtestはバグ探偵と静的解析でソースコードの脆弱性をコーディング時に検出することによって、セキュアなアプリケーションの開発を強力にサポートします。

セキュリティ・ルールセット

- OWASP (Open Web Application Security Project) Top 10ルールセット
- PCI DSS (Payment Card Industry Data Security Standard) ルールセット
- Security Assessment ルールセット

セキュリティ・ルール

- クロス サイト スクリプティング (XSS)
- 安全ではないオブジェクトの直接参照
- 不適切な認証とセッション管理
- URLアクセスの制限の不備
- インジェクションの欠陥
- クロス サイト リクエスト フォージェリ
- 安全ではない暗号の保存
- 悪意のあるファイルの実行
- 情報の漏洩と不適切なエラー処理
- 安全ではない通信方法

※バグ探偵に含まれるセキュリティルールは、Server EditionおよびJtest Securityにのみ含まれます。

Google Android や組込みJavaソースコードの静的解析

Google 社が提供する携帯端末の実行環境である「Google Android」や組込みJava ソースコードに有効な静的解析ルールセットを使用して、ソースコードを静的に検証します。



●ワンクリックで実施するテストは4種類

静的解析 → **【Javaコーディングルールに反するソースコードを検出】**

フロー解析 → **【処理フローを静的に解析してエラーを検出】**

単体テスト → **【単体テストを自動実行、実行時例外を検出】**

実行時エラー検証 → **【アプリケーション実行時にエラーを検出】**

○多彩な機能を搭載

- JUnit形式のテストケース、テストスタブの自動生成
- ワンクリックでテストを自動実行
- キャッチされない実行時例外を検出
- テストケースの修正・追加・削除が可能
- 外部ファイルからのテストデータのインポートが可能
- 仕様と異なるコードを検出
- サーバーサイドコンポーネントのテストを自動化するインコンテナテスト機能を搭載
- アプリケーション実行時に発生するエラーを検出
- 実行中のアプリケーションの動作をモニタし、JUnitテストケースを自動生成するJtest Tracer機能を搭載 (オプション)
- テストカバレッジの計測が可能
- コーディングルールに反するコードを検出
- コーディングルールの修正・追加が可能
- セキュリティの脆弱性を有するソースコードを検出
- リソースリークや配列を超えたアクセスを検出
- 即時修正機能を利用したコードの自動修正
- PDF、HTML、XML形式でレポートを出力
- 効率的・生産的なレビューを支援

○導入によるメリット

- アプリケーションの品質が向上
- コードレビューとデバッグに要する時間を削減
- 開発プロセスを効率化し、開発期間の短縮を実現
- 開発コストを削減
- サポートコストを削減
- コードの再利用性が向上
- 開発者の生産性が向上

○稼動環境

Windows (32bit/64bit)

- Windows 2000
- Windows XP
- Windows Server 2003
- Windows Vista
- Windows 7
- Sun Microsystems JRE 1.3以上
- CPU: Pentium III 1.0 互換 1.0GHz以上
- Intel Pentium IV Single Core 3.0 GHz 以上
- メモリ: 1GB以上 (推奨: 2GB以上)
- モニタ: SVGA (800x600) 以上 (推奨 1024 x 768)
- マウスまたはマウスに代替するポインティングデバイス

Linux (32bit/64bit)

- Red Hat Enterprise Linux 3, 4, 5 (glibc バージョン 2.3.2 以上, compat-libstdc++-33 パッケージのインストール)
- Windowing システム: Motif xServer または GTK
- Sun Microsystems JRE 1.3以上
- CPU: Intel Pentium III 1.0 GHz 以上, Intel Core 2 Duo 2.0 GHz 以上
- メモリ: 1GB以上 (推奨: 2GB以上)
- モニタ: SVGA (800x600) 以上 (推奨 1024 x 768)
- マウスまたはマウスに代替するポインティングデバイス

統合可能な開発環境

- Eclipse 3.2~3.6
- Rad7.0, 7.5

○Edition の紹介

Jtest Professional Edition

- テストケースの自動生成
- テストの自動実行
- 静的解析の自動実行
- セキュリティルールの使用
- テストカバレッジ情報のレポート
- 即時修正機能を使用したソースコードの自動修正
- PDF、HTML形式のレポート出力
- コードレビュー機能^{※2}
- Team Configuration Manager^{※3}との連携
- Concerto (別売り)との連携

Jtest Architect Edition

- Jtest Professional Editionの機能
- 静的解析コーディングルールの生成/編集
- 実行時エラー検出機能

Jtest Server Edition

- Jtest Architect Editionの機能
- バグ探偵
- バグ探偵に含まれるセキュリティルール
- コマンドラインインターフェース
- XML形式のレポート出力
- Team Configuration Manager

Jtest Security

- Jtestの豊富な機能のうち、とくに開発初期段階からのセキュリティ検証に有効な機能を搭載した製品です。
- 単体テスト機能、実行時エラー検出機能、コマンドラインインターフェース、XML形式のレポート出力を除くJtest Server Editionの機能

【開 発 元】

PARASOFT[®]
We make software work.

Jtestの情報は

<http://www.techmatrix.co.jp/quality/jtest/>

※1: RuleWizardは、Jtest Professional Editionには含まれません。

※2: コードレビュー機能を使用するには、最低でもチーム内にServer Editionが1ライセンス必要です。

※3: Team Configuration ManagerはJtest Server EditionおよびJtest Securityに含まれています。

● 掲載されているあらゆる製品名は、各社の商標あるいは登録商標です。

【総販売代理店】

TechMatrix
テクマトリックス株式会社

システムエンジニアリング事業部

ソフトウェアエンジニアリング営業部

本社: 〒108-8588 東京都港区高輪 4-10-8 京急第7ビル

TEL.03(5792)8606 FAX.03(5792)8706

大阪営業所: 〒541-0054 大阪市中央区南本町 2-6-12

サンマリオンNBFタワービル

TEL.06(6243)3801 FAX.06(6243)3803

[U R L] <http://www.techmatrix.co.jp>

[E-mail] parasoft-info@techmatrix.co.jp