Press Release

2024 年 8 月 28 日

報道関係者各位

テクマトリックス株式会社
（東証プライム /証券コード：3762）

Java 対応テスト自動化ツール「Jtest 2024.1」の販売を開始

OpenAI および Azure OpenAI との連携機能により、静的解析違反コードの解説と修正方法の確認、テストケースの改善を生成 AI に依頼することが可能に。

テクマトリックス株式会社（本社：東京都港区、代表取締役社長：矢井隆晴、以下「テクマトリックス」）は、米国 Parasoft Corporation（本社：米国カリフォルニア州、最高経営責任者：Elizabeth Kolawa、以下「Parasoft 社」）が開発した Java 対応テスト自動化ツール「Jtest 2024.1」の販売を 2024 年 8 月 28 日より開始します。

「Jtest」は、静的解析と単体テスト支援によって、Java ソースコードの品質可視化と単体テストの効率化を強力にサポートする Java 対応テスト自動化ツールです。静的解析では、コーディングルール解析とフロー解析という 2 種類の解析方法で、ソースコードに潜む問題点を指摘します。コーディングルール解析では、4,000 個超のルールでソースコードを検証し、プログラム中の問題の未然防止や保守性の向上を支援します。フロー解析では、クラスやパッケージを横断する膨大な数の処理フローの中から、リソースリーク、セキュリティ脆弱性などのバグの可能性が潜む特定のフローを検出します。単体テスト支援では、Java 単体テスト用オープンソースフレームワークである JUnit で利用可能なテストテンプレートやモックを自動作成し、単体テストにかかる工数を削減します。さらに、Web ブラウザー上でダッシュボード表示によるさまざまな情報提供が可能なレポーティング機能も装備しており、リモートワーク業務下においてもプロジェクトメンバー間で効率的なソースコードの品質レビューが行える環境を提供します。

このたびのバージョンアップでは、OpenAI および Azure OpenAI との連携機能が搭載されました。静的解析では、検出された違反に対する修正方法を生成 AI に問い合わせて、実コードに合わせた具体的な解説や修正方法を確認できるようになりました。同様に、単体テストでも、既存のテストコードをパラメータライズテストに変換、エラーケースの追加といったテストケースの改善に生成 AI を活用できようになりました。OpenAI および Azure OpenAI との連携機能により、効率的な開発と単体テストの妥当性の向上に貢献します。また、静的解析機能では、CWE（Common Weakness Enumeration）の ver.4.14 や OWASP API Security Top 10-2023 といったセキュアな Java プログラムを作成するためのコーディングルールが追加され、18 種類のセキュリティコンプライアンスに対応しました。さらに、Jtest に付属するレポーティングツールの Parasoft DTP では、機械学習で、類似の違反の修正・抑制履歴に基づいた推奨事項が提示されるようになりました。加えて、OpenAI および Azure OpenAI との連携機能を利用した CVE マッチ機能が搭載され、違反を含むメソッドのソースコードと既知のセキュリティ脆弱性を持つソースコードとの類似性を定量的に可視化することができるようになりました。

テクマトリックスは、Parasoft 社製品の国内総販売代理店として、Java ソフトウェア開発に携わるすべてのお客様の課題解決に最適なツールとして、Jtest の販売、マーケティング、ユーザーサポートなどの活動を強化してまいります。

【Jtest 2024.1 の新機能・改善点】

・ **OpenAI および Azure OpenAI との連携機能を搭載**

静的解析や単体テストの結果に対し、具体的な解説や修正方法の提示を依頼できるようになりました。

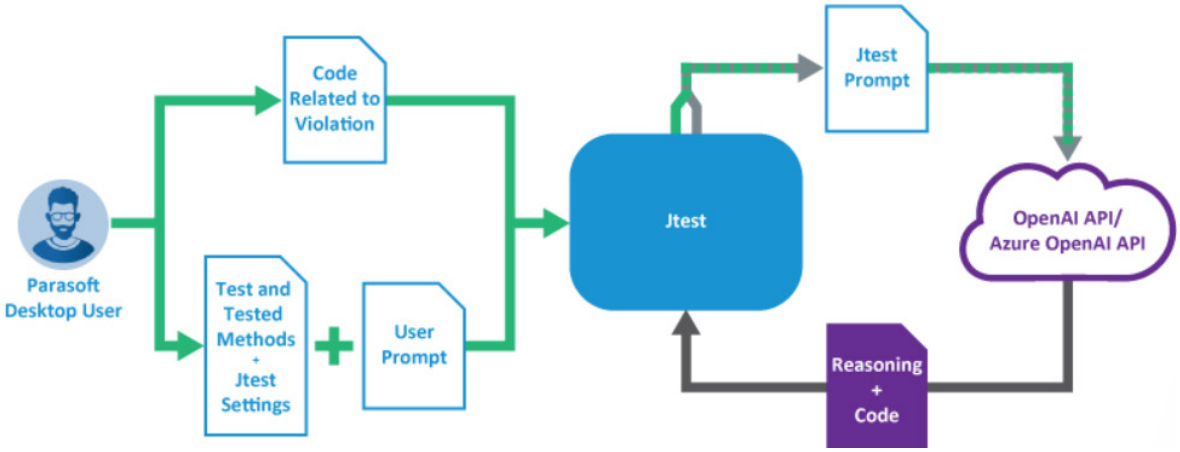

図 1：生成 AI との連携機能のイメージ

・ **静的解析違反の推奨する修正案を生成**

生成 AI に修正方法を問い合わせることで、なぜ違反が検出されたのか、コードの何が悪いのか、について、実コードに合わせた具体的な解説を参照できるようになりました。どうするべきか、実際のコードを使って修正方法が解説されるため、違反を防ぐだけではなく開発者の理解を助け、技術力の向上にもつながります。従来の静的解析ツールの課題である「違反の修正に時間がかかる」、「違反の具体的な修正方法がわからない」といった問題を解決し、違反の修正プロセスを加速することができます。

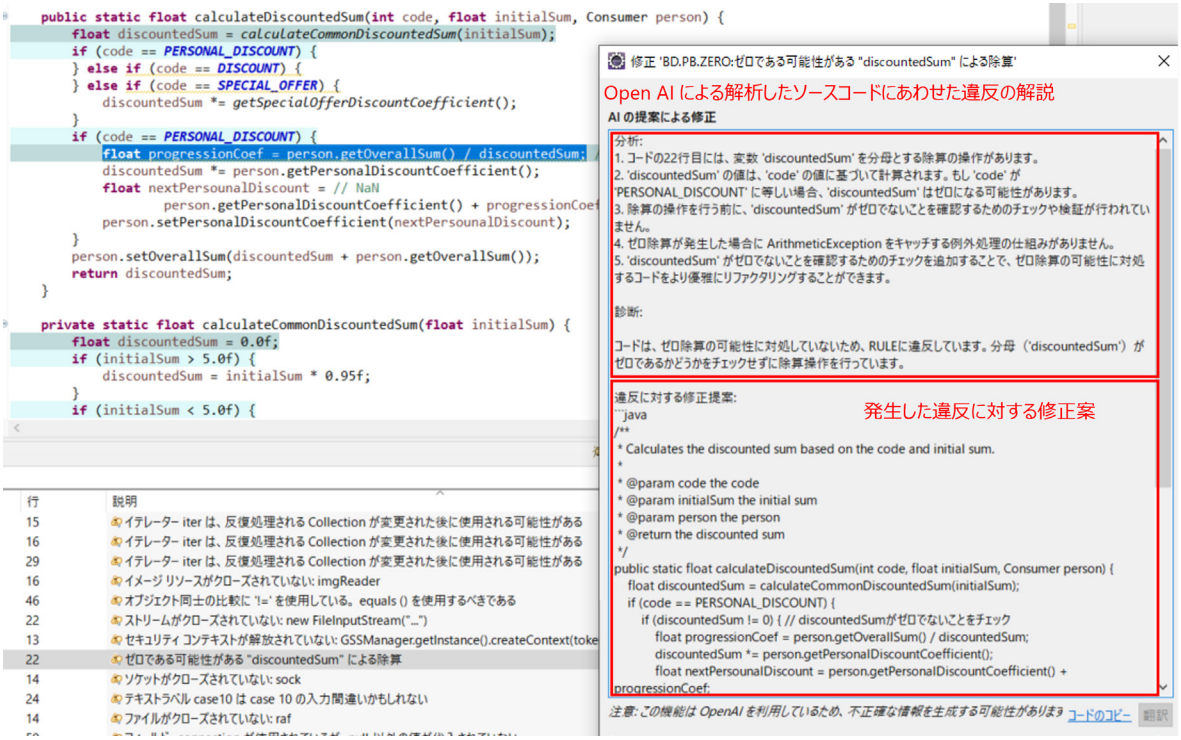

図 2：生成 AI との連携機能を活用した違反修正のイメージ

・**単体テストケースの改善案の生成**

既存テストコードのパラメータライズテストへの変換、エラーケースや境界値の追加などが生成 AI との連携により簡単な操作で可能になりました。また、プロンプトを編集してテストケースの改善を実施することも可能です。 これにより、カバレッジ計測の効率化やカバレッジの向上、さらに開発プロセスの品質と効率性を向上させることができます。

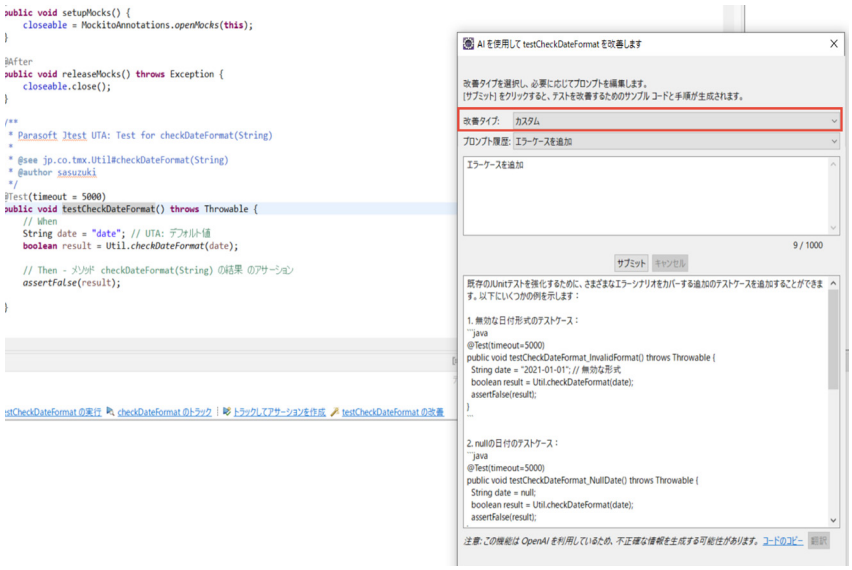

図 3：生成 AI との連携機能を活用した単体テストケース改善のイメージ

※ 生成 AI との連携機能には OpenAI および Azure OpenAI の利用契約は含まれておりません。利用者が個別に契約する必要があります。

・**単体テスト運用のための改善**

単体テストテンプレート機能とテスト影響分析機能が追加されました。

・**単体テストテンプレート機能**

単体テストアシスタント機能が生成する JUnit のテストクラスやテストメソッドのテンプレートを定義するための単体テストテンプレート機能のサポートを開始しました。共通のベースクラスを実装させたり、決まった setup メソッドを追加したりといった共通の処理をテンプレート化することが可能になりました。

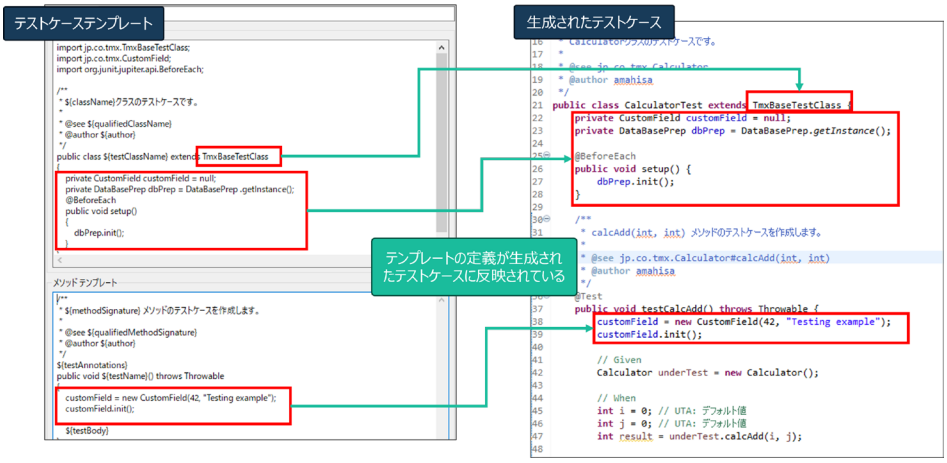

図 4：単体テストテンプレート作成のイメージ

・**テスト影響分析機能**
テスト影響分析は、必要なテストだけを実行可能にする機能です。Jtest がソースコードを監視してコード修正によって影響を受けるテストケースだけを自動的に選択して実行したり、カバレッジを計測したりすることができます。また、メソッドを修正した場合はメソッドレベルで関連するテストケースを検出して、必要なテストケースだけを実行します。これにより、テスト実行時間とテスト実行漏れの削減に貢献します。

- **CWE4.14 や OWASP API Security Top 10-2023 といったセキュリティコンプライアンスルールを追加**
ソフトウェアの脆弱性を識別するための共通脆弱性タイプ一覧である CWE（Common Weakness Enumeration）の ver.4.14 やOWASP API Security Top 10-2023といった 18 種類のセキュリティコンプライアンスに対応しました。

【Jtest のセキュリティコンプライアンス】

- CERT for Java
- CERT for Java Guidelines
- CWE 4.14
- CWE Top 25 2023
- CWE Top 25 2022
- CWE Top 25 + On the Cusp 2023
- CWE Top 25 + On the Cusp 2022
- DISA-ASD-STIG
- HIPAA
- OWASP API Security Top 10-2019
- OWASP API Security Top 10-2023
- OWASP ASVS 4.0.3
- OWASP Top 10-2021
- OWASP Top 10-2017
- PCI DSS 4.0
- PCI DSS 3.2
- UL 2900
- VVSG 2.0

※ セキュリティコンプライアンスルールによる解析には、セキュリティコンプライアンスパックオプション（別売）が必要です。

- **Android Kotlin のサポート**
Android Kotlin プロジェクトのテストの実行および、カバレッジ計測のサポートを開始しました。テストをサポートすることで、Android Kotlin プロジェクトのアプリケーションの信頼性向上と開発効率の向上に寄与します。

【Parasoft DTP 2024.1（レポーティング機能）の新機能・改善点】

- **コンプライアンスの遵守を促進するパッケージを更新**
CWE Compliance アーティファクトで CWE 4.14 がサポートされました。さらに、API 固有のセキュリ脆弱性を定義している OWASP API Security Top 10 の 2023 も追加されました。Jtest による静的解析の結果から CWE 4.14 や CWE Top 25 2023、OWASP API Security Top 10 2023 に則ったレポートをいつでも確認できます。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、セキュリティ上の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。

※ 本機能を利用するには、セキュリティコンプライアンスパックオプション（別売）が必要です。

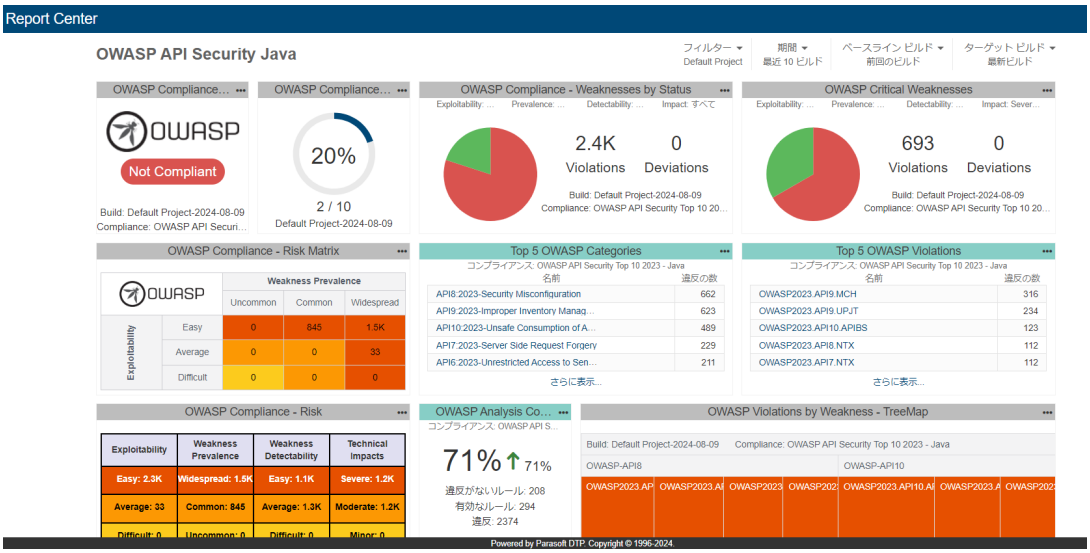

図 5：OWASP API Security Top 10 2023 用ダッシュボード

- **DTP 機能を強化**
  機械学習機能により、類似の違反が修正、抑制されたかどうかの履歴に基づいて推奨事項の取得が可能になりました。さらに生成 AI との連携機能を利用した CVE マッチ機能では、違反を含むメソッドのソースコードと既知のセキュリティ脆弱性を持つソースコードとの類似性を定量的に計測します。

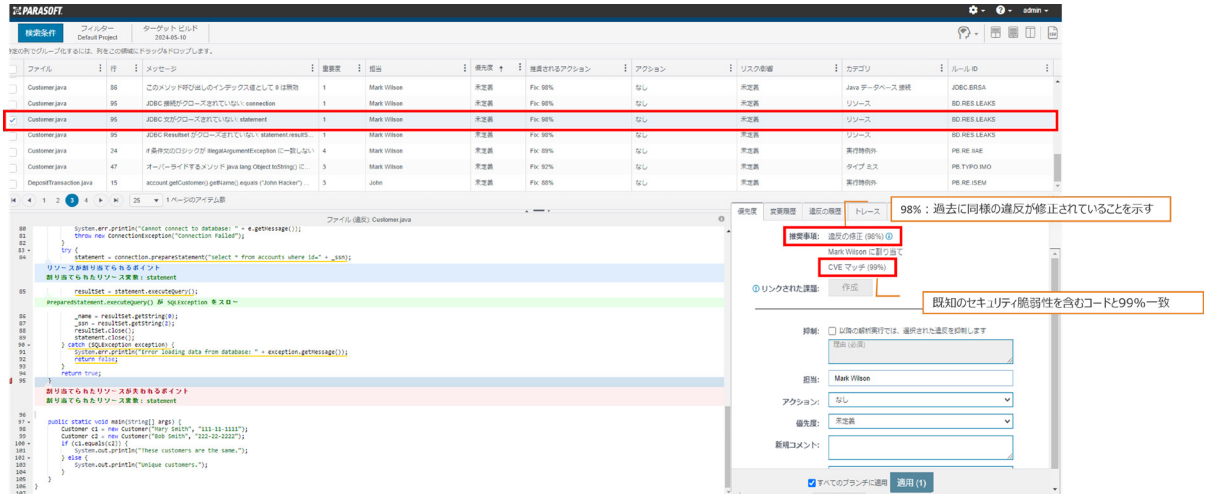

図 6：違反エクスプローラーイメージ

【稼動環境】

- Windows 64bit
  Windows 10、Windows 11、Windows Server 2022

- Linux 64bit
  Linux glibc 2.12 以上

- プラグインできる統合開発環境
  Eclipse 4.23～4.31、IntelliJ 2022.1～2024.1

- プラグインできるビルドツール
  Apache Maven 3.0.3～3.9.x、Gradle 3.3～8.7、Apache Ant 1.7～1.9.14

- 解析対象の Java のサポート
  Java 1.3～Java 21

製品の詳細は Web ページ https://www.techmatrix.co.jp/product/jtest/ をご確認ください。

- **販売開始日**
  2024 年 8 月 28 日

- **出荷開始予定日**
  2024 年 8 月 28 日

2024 年 8 月 28 日において、保守サービスをご契約いただいている Jtest のユーザー様には、「Jtest 2024.1」バージョンアップ製品を無償でご提供します。

■テクマトリックス株式会社について

テクマトリックス（東証プライム：3762）は、お客様のニーズに沿った最適な IT インフラと IT ライフサイクルをワンストップで提供する「情報基盤事業」、蓄積された業務ノウハウを実装したアプリケーションの提供により顧客の課題解決を実現する「アプリケーション・サービス事業」、“医療情報をみんなの手に。そして、未来へ。”をテーマに健康な社会を支える医療情報インフラの構築に取り組む「医療システム事業」の 3 事業を展開し、顧客企業のビジネスモデル変革と競争力の強化をサポートしています。
詳細は Web サイト： https://www.techmatrix.co.jp/ をご参照ください。

■Parasoft Corporation について

Parasoft 社は、30 年以上にわたり、ソフトウェアのバグがアプリケーションに混入する原因と仕組みを研究し、数々のソリューションを提供してきました。Parasoft 社のソリューションは、ソフトウェア開発ライフサイクルにおける継続可能なプロセスとして、品質改善活動を支援し、頑強なソースコードの実装、無駄がなく機能性の高いシステムの構築、安定したビジネスプロセスの実現を可能とします。数々の賞を受賞した Parasoft 社製品は、長年の研究成果と経験から得られたノウハウを自動化し、エンタープライズシステムから組み込みソフトウェアまで、どのようなタイプのソフトウェア開発においても、生産性向上と品質改善を実現します。Parasoft 社のコンサルティングサービスは、ツールでは解決できない問題の解決や開発プロセスの改善など、Parasoft 社の 30 年以上の経験を直接お客様に提供し、お客様の改善活動を支援します。
詳細は Web サイト： https://www.parasoft.com/ をご参照ください。

＜本件に関するお問い合わせ先＞
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 Jtest 担当
E-mail：parasoft-info@techmatrix.co.jp
TEL：03-4405-7853