

平成 21 年 8 月 4 日

報道関係者各位

テクマトリックス株式会社
Parasoft Japan 株式会社

テクマトリックス(株)が『Jtest Security』の販売を開始 ～PCI DSS や OWASP TOP10、CWE/SANS Top 25 で紹介されている ソースコードに潜む脆弱性を自動検出。 高セキュリティなアプリケーションの開発を支援します。～

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：由利 孝）は、米国 Parasoft Corporation（本社：米国カリフォルニア州、最高経営責任者：Adam Kolawa）が開発した高セキュリティな Java アプリケーションの開発をサポートする「**Jtest Security**」の販売を開始しました。「**Jtest Security**」は、アプリケーションのソースコードを検証し、PCI DSS(要件 6)や OWASP TOP10、CWE/SANS Top 25 など で発表されているセキュリティ上脆弱なソースコードを指摘し、セキュリティを向上させます。テクマトリックス(株)は、国内総販売代理店として、「**Jtest Security**」の日本国内での販売、マーケティング、日本語化、ユーザサポート、高セキュリティなアプリケーションの開発をサポートするさまざまなサービスを展開してまいります。

Parasoft の「**Jtest Security**」は、静的解析とフロー解析でソースコードを検証し、クロスサイトスクリプティングや SQL インジェクション、HTTP レスポンス分割といった、PCI DSS(要件 6)や、OWASP TOP10、CWE/SANS Top 25 など で発表されているセキュリティ上の脆弱性を、ピンポイントで検出します。「**Jtest Security**」には、約 200 種類のセキュリティ脆弱性に関するコーディングルールが搭載されており、それらを使用してソースコードと処理フローを解析し、情報漏えいや情報の改ざん、なりすましなどに利用される危険なコードを検出します。コーディングルールの多くは、パラメータの変更が可能で、自社やプロジェクトの基準に沿ったルールに修正することが可能です。また、セキュリティ関連以外にも 800 種類のコーディングルールが搭載されており、不定・不良データへのアクセスといったアプリケーションの品質に影響するようなコードやアプリケーションの致命的なバグに繋がる可能性を含むコードの検出、またメトリクスの計測、重複コードの検出などの静的解析機能も備えています。「**Jtest Security**」でソースコードを検証することにより、脆弱で危険なソースコードを一掃し、セキュリティ攻撃にも耐えうるアプリケーションの開発が可能になります。

【「Jtest Security」の特長】

「**Jtest Security**」は、1997 年より販売している Java 対応自動テストツール「**Parasoft Jtest®**（以降、**Jtest** と記す）」において、多くのユーザー様にご利用いただいているバグ探偵(処理フローを検証して問題点を検出)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)の機能を利用して、セキュリティ上、脆弱で危険なコードをピンポイントで指摘するソースコードセキュリティ検証ツールです。「**Jtest Security**」が指摘するセキュリティ上の脆弱性には、クロスサイトスクリプティングや SQL インジェクション、HTTP レスポンス分割といった代表的な攻撃手法と、OWASP TOP10 や CWE/SANS Top 25、PCI DSS(要件 6)などで発表されている脆弱性が含まれています。さらに、リソースリークや不定・不良データへのアクセス、バ

グの可能性、パフォーマンスの劣化といったアプリケーションの品質に影響するようなコードの検出も可能です。

◆SQL インジェクションやクロスサイトスクリプティング(XSS)などの脆弱性を検出

情報漏えいや情報の改ざん、なりすましなどに利用される、インジェクションやクロスサイトスクリプティング(XSS)、HTTP レスポンス分割などのセキュリティ関連の問題(脆弱性)を、ソースコードと処理フローから検出します。

【Jtest Security が検出するセキュリティ上の脆弱性(抜粋)】

- SQL インジェクション、コマンドインジェクション、XML インジェクションなどのインジェクション
- クロスサイトスクリプティング
- HTTP レスポンス分割
- 機密データの公開を防止
- 機密データの公開防止
- 暗号化および保存の方法
- 数値エラーによるバグの可能性
- パスワードの長さや保存方法
- リソースリーク
- ゼロ除算

など

◆OWASP TOP 10※1 や PCI DSS※2、CWE/SANS 最も危険なプログラミングエラーTOP 25※3 といった権威ある団体が発表している Web アプリケーションの安全性に関する基準で取り上げられているセキュリティ脆弱性を含むコードを検出

「Jtest Security」には、OWASP TOP 10※1 や PCI DSS※2、CWE/SANS 最も危険なプログラミングエラーTOP 25※3 といった権威ある団体が発表している Web アプリケーションの安全性を脅かすセキュリティ脆弱性を検出するためのコーディングルールセットが用意されています。それらのコーディングルールセットで、クロスサイトスクリプティングやインジェクション、安全でない直接オブジェクト参照、安全でない暗号化保存、クロスサイトリクエスト偽造といった攻撃手法に対して脆弱なコードを検出します。

※1 OWASP (Open Web Application Security Project、<http://www.owasp.org>)は、安全な Web アプリケーションを実現するためのセキュリティ向上を推進する非営利団体で、OWASP TOP10 (http://www.owasp.org/index.php/Top_10_2007)は、2007 年に公開された脆弱性トップ 10 です。

※2 PCI DSS(https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml)は、Visa、MasterCard、American Express、Discover、JCB International が共同で創設した PCI Security Standards Council によって、クレジットカード会員情報を取り扱う上で、カード情報と IT システムを安全に保護するための基準で、12 の要件が定義されています。今日では、クレジットカード業界のグローバルセキュリティ基準となっており、クレジットカード業界以外でも、セキュリティの基準に採用する企業が増えています。

※3 CWE/SANS 最も危険なプログラミングエラーTOP 25(<http://www.sans.org/top25errors/>)は、SANS Institute と CWE (Common Weakness Enumeration、統一的なソフトウェアの欠陥の一覧を定めるプロジェクト)が 2009 年 1 月に発表したもので、世界各国の 30 の情報セキュリティ機関・団体から選ばれたエキスパートによって、情報漏えいやサイバー犯罪につながる危険なプログラムエラーの上位 25 が選定されています。

◆コーディング時から運用後まで、アプリケーションライフサイクル全般で使用可能

ソースコードがあれば検証が可能なので、コーディング工程でも、アプリケーションのリリース前でも、運用後の追加開発でも、あらゆる工程でセキュリティ脆弱性を検証できます。特に、コーディング工程において検証を実施する場合、開発工程後半に実施するのに比べて、手戻り作業が少ないため、開発スケジュールへの影響を最小限にとどめることができます。また、リリース後のアプリケーションの修正時にも、「Jtest Security」でソースコードを検証することにより、常にソースコードをセキュアなものに維持できます。

◆ユーザ独自のセキュリティポリシーに基づくルールの追加やルールセットの作成も可能

「Jtest Security」の静的解析で使用するコーディングルールは、ルールの新規作成と追加、またパラメータの変更によるカスタマイズが可能です。このカスタマイズ機能を使用して、自社のセキュリティポリシーに基づくルールを作成し、「Jtest Security」で検証すれば、これまで目視でチェックしていたセキュリティポリシーの推進を、ツールで確認することが可能になり、ポリシー遵守の徹底と目視でのチェック工数を削減できるようになります。

◆性能や品質に関わるコーディングルールも利用可能

「Jtest Security」は、セキュリティに関わる問題点の検出に加えて、800種類のコーディングルールを備えています。不定・不良データへのアクセス、バグの可能性やパフォーマンスの劣化といったアプリケーションの性能や品質に影響するようなコードの検出やメトリクスの計測、重複コードの検出などの静的解析機能も備えています。セキュリティ上の脆弱性の検証に加えて、これらの性能や品質に関わるコーディングルールでの検証を実施することにより、アプリケーションの品質向上も図ることができます。

◆納品ソースコードの受入れ検査や品質保証部門によるソースコード検査時にも効果を発揮

「Jtest Security」は、複数の開発会社に関わるアプリケーション開発において、成果物としての納品ソースコードの受入れ検査や、品質保証部門等におけるソースコードの品質チェックの際にも、ソースコード中に潜むセキュリティ上の脆弱性確認が行え、様々な場面でその効果を発揮します。

=====

「Jtest Security」のサポートプラットフォームは、Windows 2000、Windows XP、Windows 2003 server、Windows Vista、Red Hat Enterprise Linux 3/4/5、Solaris 8/9/10。プラグイン可能な統合開発環境は、Eclipse3.0~3.4、RAD6.0/7.0/7.5、JBuilder2007。

本日から2009年12月31日まで、発売記念キャンペーンとして、定価「Jtest Security」1,200,000円(消費税別)のところ、998,000円(消費税別)で販売します。なお、製品には1年間の保守サービスが含まれています。

■テクマトリックス株式会社(JASDAQ:3762)について

テクマトリックス株式会社は、IT 分野において、最先端の製品とソリューションを提供する総合的なソリューション プロバイダーです。ソフトウェア品質管理、ネットワーク、インターネット、セキュリティ、データベース等の分野の製品を海外より輸入し、日本国内に提供するためのローカライゼーション、コンサルティング、技術サポート、教育など様々な付加価値を付けてご提供します。また、これらの技術を駆使し、金融分野、通信分野、エレクトロニック・コマース分野において、お客様のニーズに適合したソリューションの提供、インテグレーション、システムの受託開発などのサービス提供、さらには、コールセンターシステム、医用画像システム等の自社製品の開発も行っています。

テクマトリックス株式会社

東京都港区高輪 4-10-8 京急第 7 ビル

TEL 03-5792-8600 FAX 03-5792-8700

E-MAIL mg-planer@techmatrix.co.jp

URL <http://www.techmatrix.co.jp>

■Parasoft Corporation および Parasoft Japan 株式会社について

Parasoft は、20 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 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、無駄が無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 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 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 の 20 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: <http://www.parasoft.co.jp> をご参照ください。

Parasoft Japan 株式会社

東京都新宿区西新宿 1-26-2 新宿野村ビル 32F

TEL 03-5322-1315 FAX 03-5322-2929

E-MAIL info-japan@parasoft.com

URL <http://www.parasoft.co.jp>

【この発表に関するお問合せ先】

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

TEL 03-5792-8606 FAX 03-5792-8706

E-MAIL: parasoft-info@techmatrix.co.jp

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