

2011年12月5日

報道関係者各位

No.60102

株式会社東陽テクニカ

“バグ検出”と“セキュリティの脆弱性検出”向けの 新アプローチを導入した静的解析ツール QA・C8.0J 販売開始

QA・C 8.0J は組込みソフトウェアにおける複雑な状況下でのバグを検出可能

株式会社東陽テクニカ(本社:東京都中央区・社長:五味勝)は、取扱い製品である英国 Programming Research 社(以下、PRQA 社)製品ソースコード静的解析ツールの新バージョン QA・C 8.0J の出荷を2012年1月から開始を予定していることを発表しました。

QA・C 8.0J は、ディープフロー解析およびデータフロー解析を実現する洗練された技術を備えた製品で、制御フロー、変数の状態、ライブラリの使用方法に関する深刻なコーディング上の問題を検出します。

*ディープフロー解析: プログラムを実行したときに通る可能性のある経路(制御フロー)をプログラムの詳細な意味解析をしながら解析する手法

*データフロー解析: プログラム内の変数や式が取りうる値の集合に関する情報を収集しながら解析する手法

“C/C++言語の利用率が高い組込みソフトウェア業界は、私たちが提供する新しいデータフロー解析の能力を歓迎して下さると思います。”と PRQA 社の最高技術責任者 Fergus Bolger 氏は語ります。

“QA・C 8.0J は、要約したデータを抽象化し、プログラムのインタフェースレイヤで解析する手法ではなく、プログラムの詳細な意味解析を行う手法を採用しているため、多くの既存の静的解析ツールが抱える機能限界を克服しています。QA・C 8.0J は、ビット列とバイト列をプログラムの記述通りに読み取りながら、精密かつ詳細に関数解析を行います。”

この新しいデータフロー解析技術には、ディープフロー静的解析ツールに初めて導入される、業界で実績のある先進的な市販の SMT ソルバーが含まれます。

この「SMT ソルバー技術」と「制御フロー解析と言語の意味解析に関する PRQA 社の専門知識」が融合することによって、C 言語コードの静的解析は、新たなレベルに達するでしょう。

PRQA 社が提供するソリューションの強みは、QA・C で利用できるチェック項目にあります。

QA・C 8.0J のチェック機能は、既知のすべての C 言語の脆弱性に加えて、次のような演算処理をカバーします。

- ・ 無効なポインタ演算: ヌルポインタの間接参照と算術演算、無効なポインタ値の計算と間接参照(例: バッファアンダーランとバッファオーバーラン)、無関係なポインタ同士のポインタ演算

- 危険な算術演算: ゼロ除算、オーバーフローまたはラップアラウンドを発生させる算術演算、負の値から符号なし型への変換やその他の変換に関する問題、符号ビットの消失や無効な値を発生させるビットシフト演算
- 異常な制御フロー: 冗長な初期化または代入、不変な論理演算や制御式、到達不能なコード、無限ループ、未設定変数の使用箇所、返却値の不一致

データフロー解析能力を備えた QA-C 8.0J は、標準ライブラリ API 呼び出しの解析(例えば、対になるポインタのチェック)も含むため、セキュリティの脆弱性も検出します。

コーディング上の問題を検出した際には、補助メッセージを用いてパスと値の追跡情報を提供します。

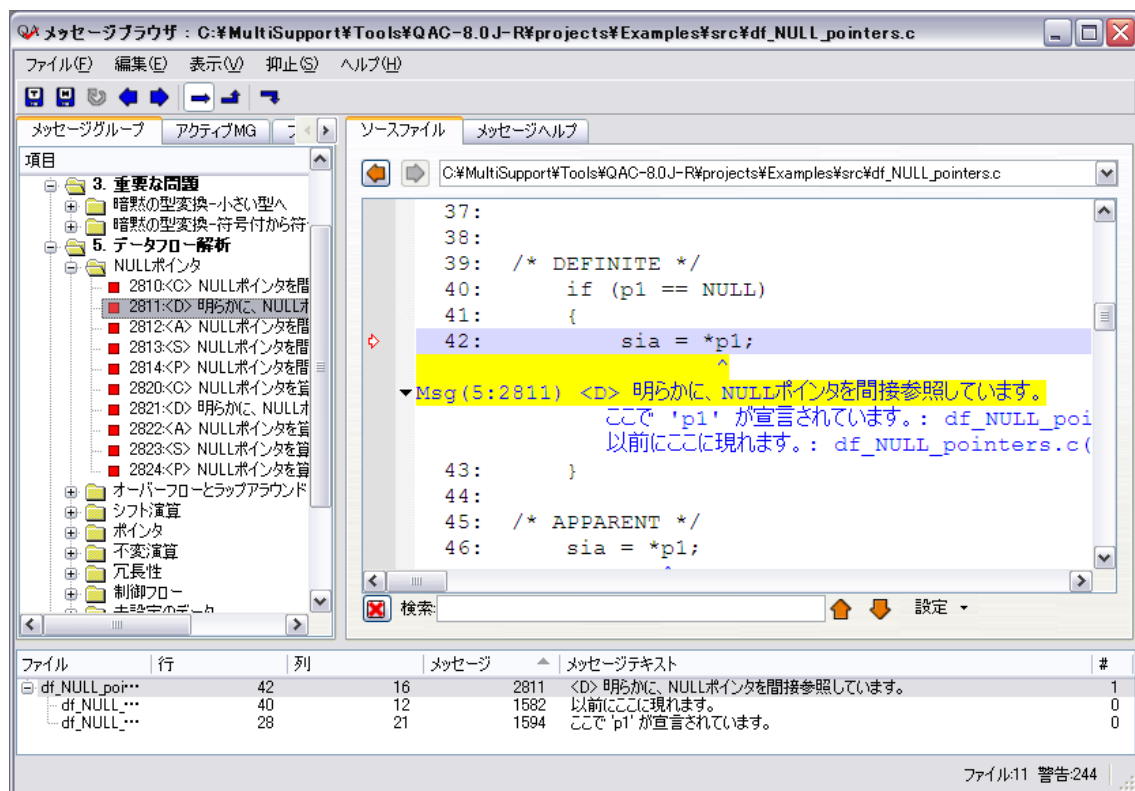


図: チェック結果の確認画面、図中ではヌルポインタの間接参照を指摘

QA-C 8.0J は、市販製品として鍛えられた SMT ソルバーの長所を活かして、次の点でデータフロー解析を洗練させています。

- 代入演算内の情報と条件式の判定内の情報を用いて、変数の相互依存関係を追跡可能にしています。
- 変数の使用箇所よりも前に現れる条件式だけでなく、後に現れる条件式も用いて、疑わしい変数の使用箇所を検出するという双方向のアプローチを採用しています。
- ループの増分数が 1 以外の場合、ループ制御変数が複数個存在する場合、ループが入れ子になっている場合を含む形で、ループ文のデータフローを正確に表現しています。
- すべての型の正確なサイズを表現することによって、共用体とビットフィールドの演算をコンパイラの処理と同等の方法で追跡可能にしています。

QA・C 8.0J は、これらのディープフロー解析に基づく先進的なデータフロー解析機能に加え、118 の新しい指摘項目を搭載しています。

また、IEC61508 および ISO26262 に基づいた安全関連ソフトウェアの開発ツールとして、TÜV SÜD 社により認証されています。

ソフトウェアエンジニアは、「コーディング規約準拠によるバグの未然防止」と「正確かつ精密なバグ検出」の両方の観点でコード品質に注意を払う必要があります。数多くの改善点を実装された QA・C 8.0J は、この重要なニーズに応えることができます。

製品に関するより詳細な情報は東陽テクニカソフトウェア・ソリューションにお問い合わせ下さい。

[英国 Programming Research 社について]

PRQA は 1986 年に創立され、業界内で「コーディング規約の専門家」として認識されています。PRQA はコーディング規約検証ツールを初めて開発し、現在ではその専門技術を、業界随一のソフトウェア検証および規格準拠検証のテクノロジーを通して、世界中に普及させています。PRQA の事業所は英国、米国、インド、アイルランド、およびオランダにあり、その他世界中に流通ネットワークが構築されています。

PRQA の業界トップツールである QA・C および QA・C++は、C と C++のコードを可能な限り厳密に検証します。両製品は、高品質な言語の解析と理解を提供する、強力かつ固有の構文解析エンジンを含みます。これらのツールは、言語の用法が危険であるか、過度に複雑であるか、移植性がないか、保守が困難であるために生じる問題を特定します。さらに、コーディング規約への準拠に必要な基本ビルドブロックが含まれています。

英国 Programming Research 社に関する詳細は www.programmingresearch.com をご覧下さい。

[株式会社東陽テクニカについて]

東陽テクニカは昭和 28 年の設立より「技術と情報」をキーワードに、最先端の「測るツール」を内外の電子計測器メーカーより輸入し、日本の技術発展に寄与することを使命として、日本の研究者・開発者に提供してきました。「電子技術センター」における修理、校正、技術サポートや自社製品の開発、「テクノロジーインターフェースセンター」で行うお客様向けの各種セミナー・トレーニングなどの取組みは、400 人を超える全従業員の 8 割を占めるエンジニアの技術力に裏付けられています。東陽テクニカはこれからも、「テクノロジーインターフェース」の使命を果たすべく努力してまいります。東陽テクニカの詳細は、www.toyo.co.jp をご覧下さい。

英国 Programming Research 社製製品に関するお問い合わせは下記までお願いします。

株式会社東陽テクニカ ソフトウェア・ソリューション

Tel:03-3279-0771 Fax:03-3246-0645 E-mail: ss_sales@toyo.co.jp

また、当社に関するご質問は下記までお願いします。

株式会社東陽テクニカ 経営企画室

Tel:03-3279-0771 Fax:03-3246-0645 E-mail: kikaku@toyo.co.jp