〈ソリューション紹介〉

Embedded Solution

組込みソフト開発の目視レビューの負荷を軽減するソースコード変数異常値診断サービスを提供

高信頼性が求められる組込みソフトウェア開発でのソースコードのチェックは、市販の静的解析ツールや目視レビューだけではカバーできない面があります。当社は、変数の設計上の値範囲を考慮したチェックを行いランタイムエラー発生の可能性を検出する「ソースコード変数異常値診断サービス」を開始しました。お客様の開発効率向上と稼働後の品質リスク低減を図ります。

従来のレビュー、テスト手法の限界

ADAS(先進運転支援システム) 時代を迎えた車載ソフトウェアの開発においては、高い安全性・信頼性が要求されるとともに厳しいコスト条件とも相まって、従来のレビュー、テスト手法では限界が見られています。

ADASや車載ECUのソフトウェア開発では、ソースコードで使用されている各変数の取り得る値の範囲まで設計され、その仕様上取り得る値の範囲内で入力変数が変動することによって変数が設計上の値範囲外となるケースが発生し、その結果、オーバーフローやアンダーフロー、ゼロ除算、範囲外アクセスなどが発生することがないかをチェックしています**(図-1)**。

コンパイル時には判明しないものの、演算した結果オーバーフローが発生するといった不具合は稀にしか発生しないため再現性に乏しく、テストでの発見が困難なケースが多いのが実情です。出荷後の製品でこのような不具合が発生した場合は、製品回収など大きな問題につながる恐れがあります。

そのため、人の手によるコードレビューがどうしても必要となりますが、目視によってソースコードを1ステップずつ確認する作業となるため、コスト・期間の大幅な増加はもとより、見落としなど人的ミスの発生、特定の要員への依存、レビュー品質のばらつきといった品質への懸念、というさまざまな問題が浮き彫りになっています。

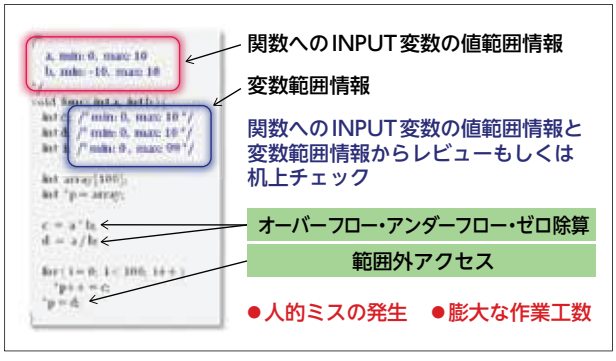

図-1　変数異常値のコードレビューと問題点

変数の値範囲を考慮した変数異常値を検出

こうした現状の課題を解決するため、当社では目視によるコードレビューを支援するための解析ツール「ソースコード変数異常値診断ツール」の開発を進めてきました。

このツールは以下の3つの特徴を備えています。

(1) プログラム実行時の状態をシミュレーションして、各変数が取り得る値範囲を自動で算出しリスト化

(2) 各変数に設定された「設計上の値範囲」からの逸脱を検出して警告を出力

(3) 各変数の「設計上の値範囲」を考慮したランタイムエラー検出

呼び出し最上位関数の引数および外部変数(グローバル／スタティック) に値範囲を設定するだけで、内部変数および関数の戻り値の値範囲を自動で算出して、その値範囲に基づいて変数異常値を検出し、それに起因して発生するランタイムエラーを検出するため、他の静的解析ツールと比較して、対象を変数の値範囲に関するものだけに特化した分、深くチェック・解析ができる点がメリットとなっています**(図-2)**。

しかし、市販の静的解析ツールが抱えている問題、例えば、ツールの運用プロセスが煩雑、教育など初期コストがかかる、欠陥の誤検知や些細な欠陥の報告が多いといった問題

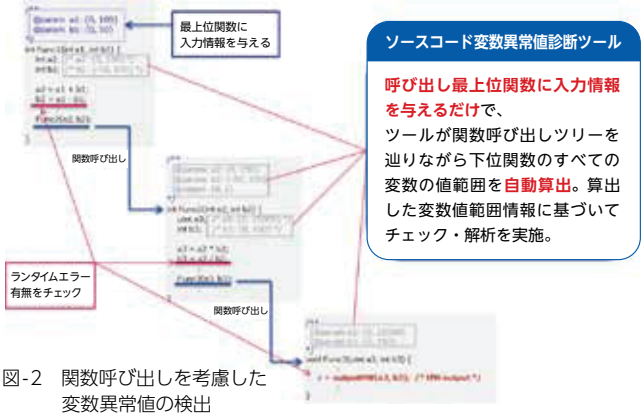

図-2　関数呼び出しを考慮した変数異常値の検出

は、当社ツールにおいても共通の問題であり、単に当社ツールを提供するだけではお客様の問題は解決しません。そこで、お客様のソースコードを当社ツールで分析した結果をフィードバックする、「ソースコード変数異常値診断サービス」として提供することにしました。自動車や航空機やプラントなど、絶対に止めてはならない、運行や運用に関わるような分野向けのサービスを想定しています。

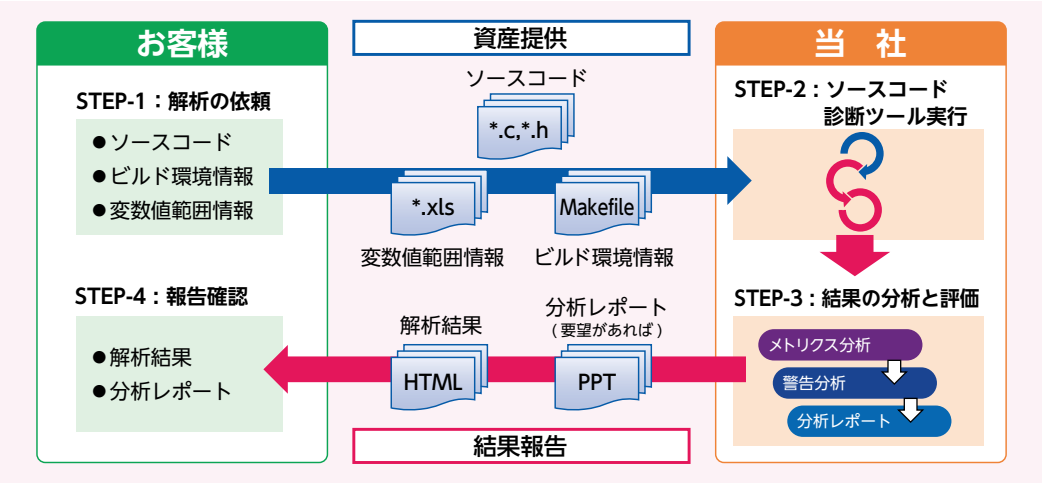

図-3　ソースコード変数異常値診断サービスの概要

ソースファイル、およびソースに含まれる変数の値範囲の情報をお客様から預かり、当社がソースコード変数異常値診断ツールを実行して、変数の値範囲により発生する可能性がある問題点を報告します**(図-3)**。

また、診断結果について個別の問題解決の依頼をいただいた場合は、当社エンジニアによる分析を行い、解決策を提案します。

このサービスは、各変数の「設計上の値範囲」を考慮した変数異常値（変数が設計上の値範囲外となるケース）の検出にフォーカスした点を最大の特徴としています。変数異常値の検出ができることで、オーバーフロー／アンダーフロー、ゼロ除算、配列の範囲外アクセス、不正なポインタへのアクセス、初期化前の変数へのアクセス、デッドコード（到達不能コード）、必ず真または偽となるコードといった、ランタイムエラーの高精度な検出を可能とします。

お客様の開発効率化と製品出荷後の品質リスク低減を

ソースコード変数異常値診断サービスは、お客様に次のようなメリットを提供します。

(1) ツール導入／教育、解析環境立ち上げ、解析／利用ノウハウ蓄積といった手間が不要

(2) 専門技術者チームが警告を診断、重要度が高く改善効果が高い問題を効率的に抽出

これらにより、お客様はレビュー工数や見落としの発生を削減でき、開発作業の効率化と稼働後の品質リスクの低減を実現します**(図-4)**。

すでに特定のお客様向けにサービスを開始しており、今後、今以上にお客様にとって価値のあるサービス品質の向上に努め、前述したような極めて高い信頼性が要求されるソフトウェア開発分野に広く提供していきたいと考えています。

また現在は、このツールの診断に基づく警告を人の手によって分析していますが、いずれはこの部分にAIを活用していけば、これらのプロセスがすべて自動化できるようになり、さらに、インタフェースもクラウド化されれば、お客様の使い勝手の向上を図ることができるでしょう。今後、より一層お客様の深いニーズを発掘していけるよう、サービスの拡充に努めていきます。

（エンベデッドシステム事業部　山中　明）

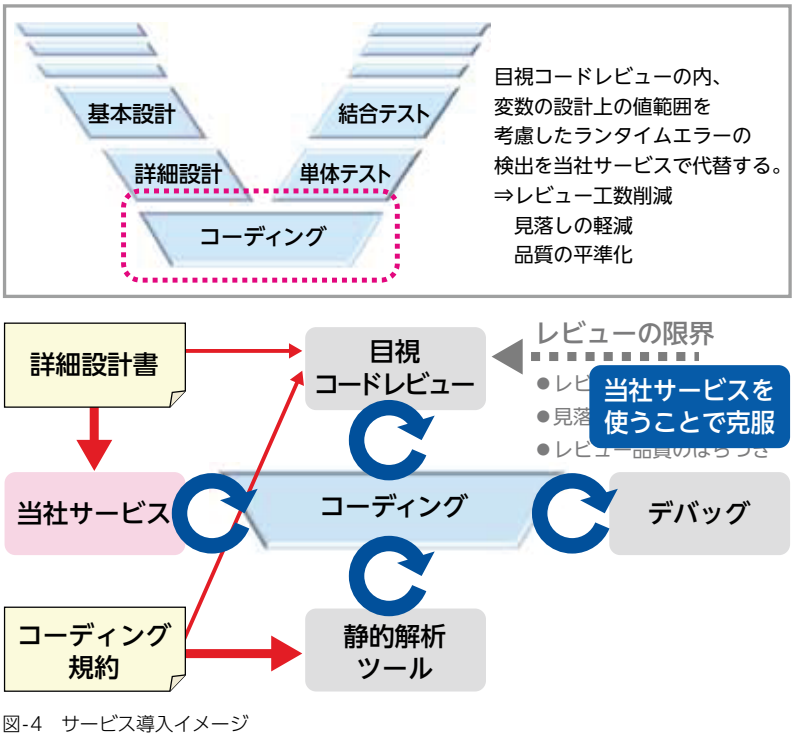

図-4　サービス導入イメージ