コンパイラ:ツール認定の新常識

ユーザーがコンパイラをテストして信頼性を確保する

コンパイラにもバグは必ず存在する。それゆえコンパイラが正しく動作することの証明は
アプリケーションの信頼性にとって非常に重要であり、機能安全規格ではツール認定が求められる。

コンパイラツールの認定について

コンパイラが生成するコードはアプリケーションの一部となり、生成コード上のエラーがセーフティクリティカルな事象につながる。そのため、コンパイラがエラーを出さないという要求は根源的なものであり、ISO 26262などの機能安全規格では「生成されたコードでどんなエラーも発見できる強力なアプリケーションテスト手順を作成する」か、「認定によってコンパイラが十分信頼できる」かの選択を行うことが要請されている。

「生成されたコードでどんなエラーも発見できる強力なアプリケーションテスト手順を作成する」には、コンパイラの不具合とそれに起因する誤った出力が防止または検知されることを確信できることが必要になる。これにはアプリケーションのテストをターゲット上で実行して、オブジェクトコードレベルのカバレッジ解析で十分性を証明する必要がある。しかしながら最適化が行われると、生成されるオブジェクトにはソースコードになかった分岐やパスを含むため、多大な工数と費用を費やすことになる。また高度な最適化で追加される多数の条件分岐の中には冗長なものが含まれるため、完全なカバレッジは不可能に近い。そのため、一般に現実的なソリューションとは言えない。最適化を全く利用しないアプリケーションで、潤沢な予算と工期が与えられるプロジェクトに限定した考え方と言える。

一方、「認定によってコンパイラが十分信頼できる」は、コンパイラの正しさに十分な確信を得るために機能安全規格に記載されているプロセスであり、言語標準規格への準拠、正確性、堅牢性を厳密にテストすることが必要である。これはコンパイラの仕組みを熟知したうえで念入りに開発することが必要で、莫大な工数を要するプロジェクトになり、テストプログラム数も膨大になる。ただ幸いなことに、市販されるテストスイートなら、極めて低いコストで導入することができる。

Solid Sands 社の SuperTest は、コンパイラ品質への信頼を得るためのテストスイートであり、コンパイラによる解析、変換、最適化を評価・検証する業界最大クラスのテストが提供されている。(2019年5月版で、コアテストケース6万件超、ターゲット依存算術演算、最適化、ストレステストを含め200万件超)既に多くのコンパイラメーカーが自社製品のテストやツール事前認定を目的にSuperTestを利用している。

コンパイラがテストスイートにより認定された場合、それは欠陥がないということではなく、その欠陥がアプリケーション開発者に分かっており避けられ得るということを意味する。そして認定されたコンパイラを用いることで、アプリケーションへの関心とコンパイラに対する関心を分離できる。そのため、派生製品の開発時にアプリケーションを再利用して複数のターゲットに展開することがより容易、かつ効率的にでき、その結果として費用対効果が高くなる。

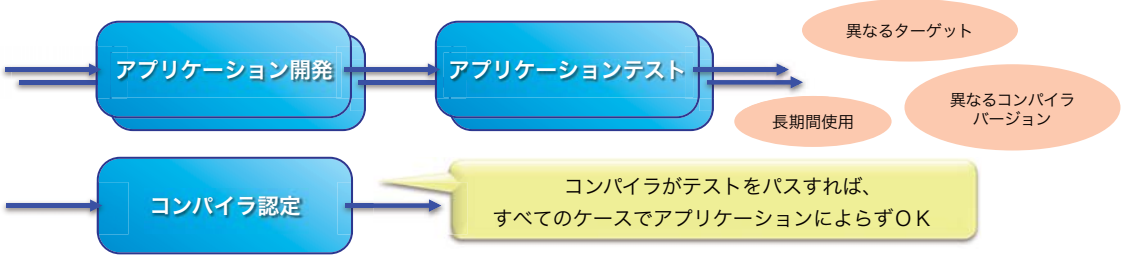
ユーザーによるコンパイラテスト

ただ課題もある。最適化やデバイスのバリアント指定などの各種オプションによる、コンパイラユーザー固有のユースケースに対しては、コンパイラメーカーによる認定は十分ではない。実際、全てのユースケースでテストをすることは事実上不可能であり、事前ツール認定されたコンパイラを利用する場合は、特定のユースケースに従う必要がある。

これに対して、近年、コンパイラユーザーもSuperTestを、機能安全規格の要件を満たすことや間違ったコードの生成を防ぐために活用し始めている。固有のユースケースでコンパイラを事前にテストすることで、早期段階で問題を明らかにして、後工程あるいは出荷後にコンパイラのバグで多大な痛手をこうむるといった問題を回避できるためである。

コンパイラ認定なしの場合：

コンパイラ認定ありの場合：



CASECARD DENSO

車載システムの機能安全のリスクを軽減するSuperTest

実はコンパイラを検証する必要があるのは、コンパイラ開発者だけではない。コンパイラによってアプリケーションコードに不測のエラーが混入されることがないように、ソフトウエア開発者であってもコンパイラの品質を意識する必要がある。特にセーフティクリティカルな製品では、その傾向が顕著になる。

株式会社デンソー（最先端のオートモーティブテクノロジー、システムおよびコンポーネントのサプライヤー）も、この問題を解決するコンパイラテストと検証用のパッケージとして、Solid Sands 社の SuperTest を支持している。

コンパイラで実績済みのソースコードを再利用することは、ソフトウエアや製品の品質を維持する最善策のひとつである。しかしながら新たに製品系列を展開する場合に、新しく生成されるソースコードが、コンパイラの欠陥を表面化させる可能性がある。さらにソフトウエア開発担当者ごとで異なる様々なコードスタイルによって、コンパイラの欠陥が浮き彫りにされることもある。また一方、コンパイラに潜在する問題が露呈するのは、新規のソースコードをコンパイルする場合に限らない。

“新しいバージョンのコンパイラを入手するたびに、コンパイルされたコードが旧バージョンと一致することをチェックする必要があります。以前はアセンブラレベルでの手動比較や、機能テストを実施していましたが、いずれも膨大な時間と労力を必要とし、また再現性のない結果が出ることもありました。また同じことは C 言語の規格や CPU 種別を切り替える際にも起こり得ます。”
ー 株式会社デンソー 基盤ソフト技術部 谷 充弘 氏

SuperTest は、コンパイラのバージョン間の違いの評価や、言語規格や CPU の違いに対する検証のプロセスを自動化することに加えて、独自のテスト要件を取り込む柔軟性も備えている。

コンパイラメーカはテストスイートを用いて正当性の確認をするものの、それは代表的な設定で行われるのであって、全てのコンパイラオプションの組み合わせがカバーされるわけではない。SuperTest が有れば、実際の製品開発に採用するオプション設定でテストができるうえに、社内で蓄積された知見を活用して、各アプリケーションの評価に重要なテストケースの追加が行なえる。

また SuperTest は定期的にアップデートされるので、ライブラリコードを採用する際に必要となる検証にも有効である。例えば SuperTest で検出される欠陥には、数学関数の C 言語規格との不一致動作や、異なるコンパイラバージョン、メーカ間でのライブラリのふるまいの違いなどがある。

“コンパイラに潜む問題点が、製品開発途中や製品出荷後に見つかり手戻りが発生する可能性があったことを考えると、コンパイラ入手時に検出できる SuperTest の採用は、大きな投資対効果があったと言えます。”
ー 株式会社デンソー 基盤ソフト技術部 中里 弘樹 氏

SuperTest に提供される相当な規模のテストスイートを自前で開発することや、様々なコンパイラの問題を検出するコードサンプルを入手することを考えると、SuperTest への投資効果は非常に高い。大規模なテストから、欠陥の検出と特定に必要なテストを素早く効果的に選別できるし、コンパイラが C 言語標準に準拠することのチェックは自動実行で 1～2 日で済むので、多くの工数と費用を削減できる。

車載システムの機能安全規格に準拠して、顧客からの高い信用を維持するには、コンパイラの品質は常に問題になる。コンパイラが十分な信頼水準であることの判断に活用できる SuperTest は、今や必須のソフトウエア開発ツールとして位置づけられる。

FUJI SETSUBI
富士設備工業株式会社 電子機器事業部
〒591-8025 大阪府堺市北区長曽根町1928-1 TEL.072-252-2128
www.fuji-setsu.co.jp