Formal Methods
形式検証

AdaCore

形式検証ツール
SPARK Pro

SPARK Proは形式検証と静的検証が統合されたツール・スイート
定理証明を用いて プログラムエラーを最小化

□ SPARKに備わっている機能

■ **データフロー解析**
非初期化変数参照等、不確実性や不正な動作の原因となるエラー検出

■ **インフォメーションフロー解析**
プログラムを解析して指定されたデータの依存関係を検証

■ **実行時例外の検出**
ゼロ除算、数値オーバーフロー、バッファオーバーフロー、配列の範囲外インデックスなどの実行時例外を検出

■ **プロパティチェック**
セーフティやセキュリティプロパティをcontract（事前、事後条件）で記述し検証

■ レベル別検証
- **ストーン（Stone）**
SPARK言語の制約事項により、安全なプログラムを記述
- **ブロンズ（Bronze）**
データフロー解析とインフォメーションフロー解析を使用して、非初期化変数の参照等の広範なエラーを排除
- **シルバー（Silver）**
実行時エラーがないことを検証
- **ゴールド（Gold）**
証明（Proof）を使用して、ソフトウェアの重要なプロパティを検証
- **プラチナ（Platinum）**
クリティカルなコードが機能仕様を満たしていることを証明

SPARK Proは形式検証後GNAT Proコンパイラでコード生成対応

◆ **SPARK Proは、MITREのCommon Weakness Enumeration（CWE）互換性および有効性プログラムによりCWE互換として指定されており、CWEの上位25に含まれる非安全なソフトウェアエラーやコードの弱点を検出**

● **CWEの一例**

CWE weakness	Description
CWE 120, 123, 124, 125, 126, 127, 129, 130, 131	Buffer overflow/underflow
CWE 136, 137	Variant record field violation, Use of incorrect type in inheritance hierarchy

AdaCore社の製品は、民間航空機の電子システム、軍事防衛システム、航空管制・制御、鉄道システム、宇宙システム、自動車、医療機器、金融サービス分野の主要な民間企業や政府機関を含む世界中のお客様が使用されています。各プロジェクトの概要に関しては、www.adacore.com/ industries/をご覧ください。

2021.10

AdaCore www.adacore.com ✉ info@adacore.com
代理店：アイティアクセス株式会社 https://www.itaccess.co.jp/service/adv/adacore/ ✉ info@itaccess.co.jp