



静的解析ツール C-STAT

静的解析によるコード品質の確保

静的解析は、ソースコードレベルで解析を行うことで、プログラムをメイク/実行することなく、コードの潜在的な問題を見つけるのに役立ちます。静的コード解析ツールC-STATは、IAR Embedded Workbench IDE に完全に統合されています。また、アプリケーションがMISRAによって定義されたコーディング標準や、CWE や CERT から派生した何百もの他のチェックに準拠していることを簡単に確認することができます。

主な特徴

- CおよびC++コードの解析
- MISRA C:2012、MISRA C++:2008、MISRA C:2004で定義されたルールに準拠した、合計約700のチェック
- CWEがカバーする課題に対応する250以上のチェック
- 安全なコーディングのためのコーディング標準 CERT C に準拠したチェック
- IAR Embedded Workbench IDEと完全統合
- 包括的で詳細なエラー情報
- 迅速な実行
- ほとんどのIAR Embedded Workbench製品で利用可能

C-STATは、業界標準MISRA、CWEおよびCERT C/C++へのコードの準拠をチェックします。

C-STAT は、CERT C/C++ Secure Coding Standards によって定義されたMISRAルールセットおよびルールに準拠しているかどうか、また以下のような多くの弱点について、CWEで定義されている通り、多くのセキュリティチェックを実行します。コンプライアンス・タスクをさらに簡素化するために、C-STATはCWE/CERT/MISRAにおけるルール名を使った出力を提供します。

MISRA (Motor Industry Software Reliability Association) のルールは世界中のさまざまな業界セグメントで使用されており、さらに、組み込み業界で最も広く使用されているC/C++言語のコーディングガイドラインです。

MISRA-C:2012には、143のルールと16の指令と呼ばれるルールが含まれています。

ルールは、必須、必須、勧告に分類され、整数サイズのようなコンパイラの違いによる移植性に問題がある記述の回避、コーディングで失敗しやすい関数や構造体の使用の回避、コードの複雑さの制限、命名規則やコメントの使用などによるコードの保守性の確保などの分野をカバーしています。

CWE (The Common Weakness Enumeration : 共通脆弱性タイプ一覧) は脆弱性の種類を分類し、弱点とその潜在的な影響の説明、潜在的な緩和策、コードサンプル、分類法、参考文献が掲載されています。コミュニティプロジェクトにより保守されており、ソフトウェアの弱点をよりよく理解し、管理すること、また、これらの弱点を見つけることができるソフトウェアセキュリティツールやサービスをより効果的に選択し、使用できるようにすることを目的としています。

CERT は、C++やCでの安全なコーディングのためのルールセットを提供しています。各ガイドラインは、タイトル、説明、非準拠のコード例、および準拠した解決策の例で構成されています。標準には、コーディングエラーや実装エラー、低レベルの設計エラーを回避するための指針が含まれています。規格の目的は、悪用可能な脆弱性につながる安全でないコーディング手法や未定義の動作を排除することです。

