ISO/IEC9126 & MISRA-C:2004ベース ソースコード品質診断

～ MISRA-C:2004ベース品質診断のご紹介 ～

株式会社 東陽テクニカ
ソフトウェア・ソリューション

MISRAとは

- **Motor Industry Software Reliability Associationの略**
- **ヨーロッパ自動車技術会（MIRA)の下部組織**

  MIRA: Motor Industry Research Association

- **研究成果に基づく各種MISRAドキュメントを発行**
  - Development guideline for vehicle based software (ISO/DTR 15497)
    自動車用ソフトウェアの開発ガイドライン（自動車技術会　TP-01001）
  - Guidelines for the use of the C language in vehicle based software
    自動車用C言語利用のガイドライン（自動車技術会　TP-01002）
  - Guidelines for the Use of the C Language in Critical Systems
    自動車用C言語利用のガイドライン（第2版）（自動車技術会　TP-01002）

MISRA-C:1998
&
MISRA-C:2004

その他にも…
Safety Analysis
Auto Code
C++ に関する活動を実施

東陽テクニカ

MISRA-Cとは

- ECU(電子制御ユニット)の品質向上を目指して、MISRAが研究開発した組込みC言語用プログラミングガイドライン
- 品質サブシステムの解説と具体的なプログラミング標準から構成されている
  - MISRA-C:1998では127個のルールを規定
  - MISRA-C:2004では141個のルールを規定
- 各ルールの検証手段を定めることが要求されている
- 自動車業界の各企業が牽引しているので、自動車用の側面が強いが、C言語による組込みソフト開発全般に適用可能
  - 自動車業界以外の業界でも広く利用されている
- 自動車業界では世界的なデファクト・スタンダード
  - プログラミング標準の適用は機能安全(IEC61508)の要件の一つ

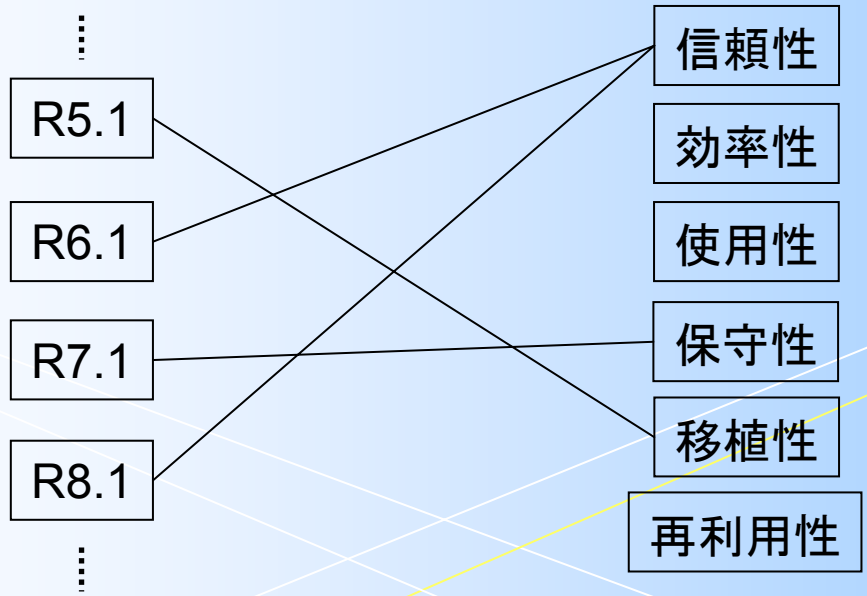
MISRA-Cのルール例

- 信頼性・保守性・移植性に関わるルールが多い

5.2	外部スコープの識別子が隠蔽されることになるため，内部スコープの識別子には，外部スコープの識別子と同じ名前を用いてはならない。
6.1	単なるchar 型は，文字データの格納及び使用に限って用いなければならない。
6.5	signed int 型のビットフィールドの幅は，2ビット長以上でなければならない。
7.1	（0以外の）8進定数及び8進拡張表記は，用いてはならない。
8.1	関数は，常にプロトタイプ宣言をもち，プロトタイプ宣言は，関数定義及び関数呼出しの両方から参照されなければならない。
9.1	すべての自動変数は，用いる前に値を代入しなければならない。

MISRA-C:2004ベース品質診断とは(1/2)

- MISRA-C:2004のルールを品質特性にマッピング
  - MISRA-Cへの適合度評価を行う
  - MISRA-Cの観点も含めた品質特性評価を行う

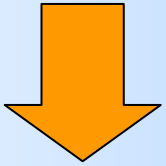


東陽テクニカ

MISRA-C:2004ベース品質診断とは(2/2)

- **MISRA-Cを手がかりにした品質向上への取り組みを支援**

ISO/IEC9126の品質特性に基づく品質向上アプローチ

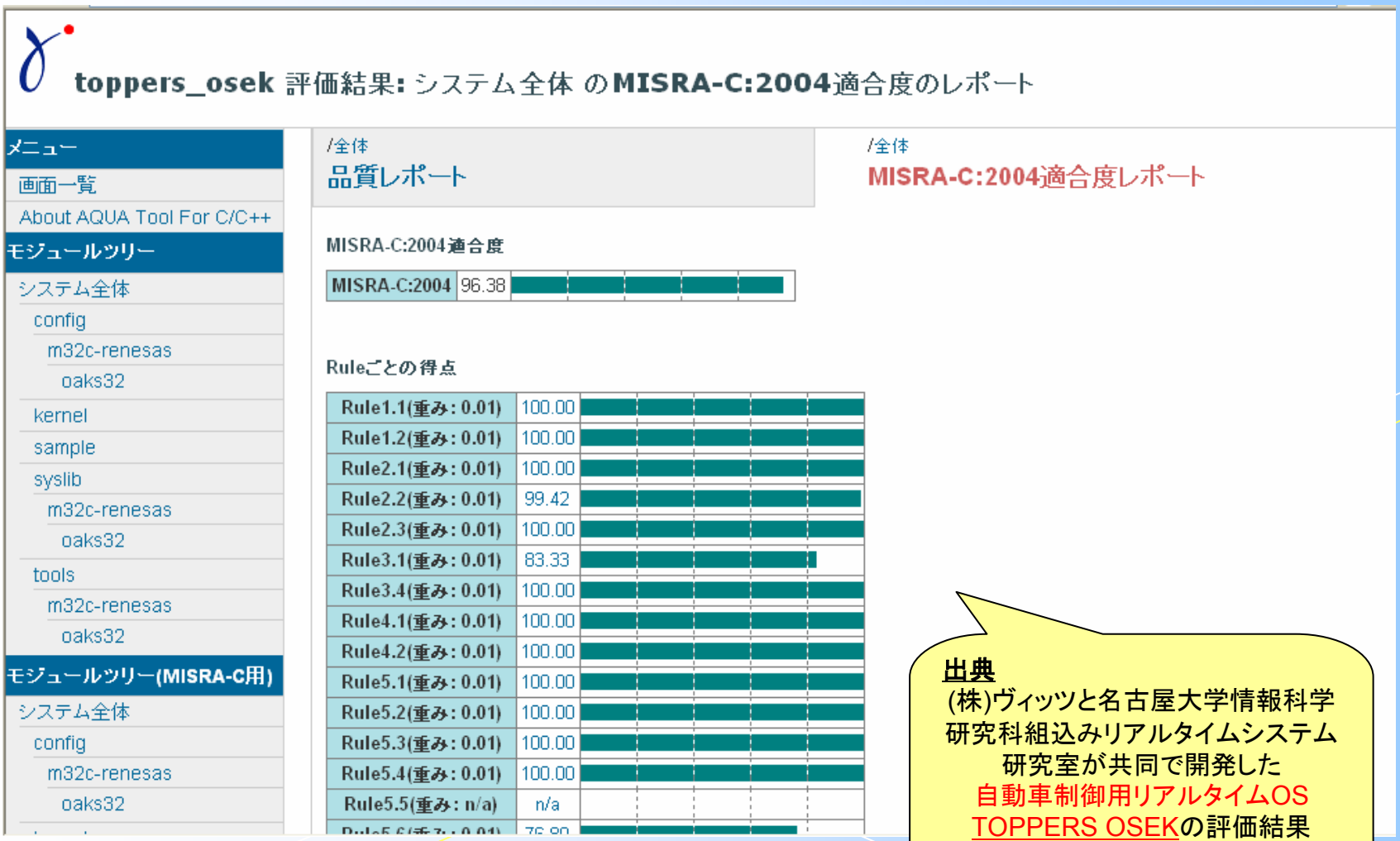


ソフトウェアの品質を総合的に向上

MISRA-C:2004への取り組みに基づく品質向上アプローチ

東陽テクニカ

品質診断例(MISRA-C適合度評価)



toppers_osek 評価結果: システム全体 のMISRA-C:2004適合度のレポート

メニュー
画面一覧
About AQUA Tool For C/C++
モジュールツリー
システム全体
config
m32c-renesas
oaks32
kernel
sample
syslib
m32c-renesas
oaks32
tools
m32c-renesas
oaks32
モジュールツリー(MISRA-C用)
システム全体
config
m32c-renesas
oaks32

/全体
品質レポート

/全体
MISRA-C:2004適合度レポート

MISRA-C:2004適合度

MISRA-C:2004	96.38

Ruleごとの得点

Rule1.1(重み: 0.01)	100.00
Rule1.2(重み: 0.01)	100.00
Rule2.1(重み: 0.01)	100.00
Rule2.2(重み: 0.01)	99.42
Rule2.3(重み: 0.01)	100.00
Rule3.1(重み: 0.01)	83.33
Rule3.4(重み: 0.01)	100.00
Rule4.1(重み: 0.01)	100.00
Rule4.2(重み: 0.01)	100.00
Rule5.1(重み: 0.01)	100.00
Rule5.2(重み: 0.01)	100.00
Rule5.3(重み: 0.01)	100.00
Rule5.4(重み: 0.01)	100.00
Rule5.5(重み: n/a)	n/a

出典
(株)ヴィッツと名古屋大学情報科学研究科組込みリアルタイムシステム研究室が共同で開発した
自動車制御用リアルタイムOS
TOPPERS OSEKの評価結果
(MISRA-C対応済みコード)

東陽テクニカ

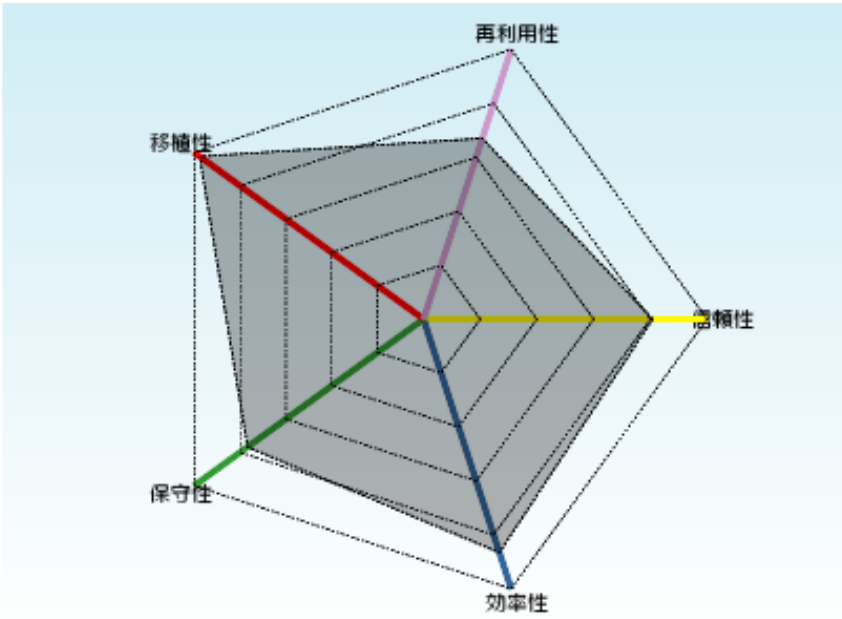
品質診断例(品質特性評価[MISRA-C含む])

モジュールツリー(MISRA-C用)

- システム全体
  - config
    - m32c-renesas
      - oaks32
  - kernel
  - sample
  - syslib
    - m32c-renesas
      - oaks32
  - tools
    - m32c-renesas
      - oaks32

特性の得点

性能(エンドユーザ視点)	信頼性(重み: 0.50)	80.82
	効率性(重み: 0.50)	86.58
品質(開発者視点)	保守性(重み: 0.33)	76.71
	移植性(重み: 0.33)	97.59
	再利用性(重み: 0.33)	67.02



東陽テクニカ

MISRA-C:2004ベース品質診断の適用(1/3)

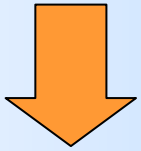
- 現状把握

  適用対象:

  MISRA-Cへの対応を検討中のProject

  適用目的:

  最新ソースのMISRA-C適合度の把握



MISRA-Cを適用するためには運用方法の検討を含めて相応の工数が必要になります。

品質診断の適用により、現状を把握し、スタートラインを定めることができます。

MISRA-C:2004ベース品質診断の適用(2/3)

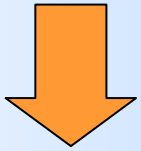
- 品質改善

  適用対象:

  MISRA-C対応中のProject

  適用目的:

  過去ソースと最新ソースのMISRA-C適合度の比較



MISRA-Cの適用は継続的に実施する必要があります。

品質診断の継続的な適用により、MISRA-Cに適合させる上でボトルネックになっている箇所を見出すことができます。

MISRA-C:2004ベース品質診断の適用(3/3)

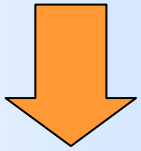
- 品質維持

  適用対象:

  MISRA-C対応中のProjectとは別の新規Project

  適用目的:

  異なるProject間でのMISRA-C適合度の比較



MISRA-Cは製品単位で適用する必要があります。

品質診断の適用により、MISRA-Cベースの品質向上活動が新規Projectにも引き継がれ、品質水準が向上しているのかを評価することができます。

東陽テクニカ

MISRA-C:2004ベース品質診断のポイント

- MISRA-C:2004への適合度をモジュール単位、ファイル単位で評価
  → モジュール別の特徴、ファイル別の特徴を把握できる
- MISRA-C:2004への適合度をルール単位に評価
  → ルール別の特徴を把握できる
- MISRA-C:2004への適合度をProject全体の総点として評価
  → 異なるProject同士が比較しやすくなる
- MISRA-C:2004の観点を含めた品質特性を評価
  → MISRA-Cの適用効果を品質特性の増減で把握できる

コーディング標準への取り組みをより明確に
品質向上のための活動として位置づけることができる

東陽テクニカ

品質診断に関する注意点

- MISRA-C:2004にはドキュメントの作成を要求するルールがあります。これらのルールは得点化の対象外(n/a表示)になります。
- MISRA-C:2004にはコードがルールに適合しているかどうかを判断しにくいルールがあります。これらのルールの全てまたは一部は得点化の対象外(n/a表示)になります。
- MISRA-C:2004ではルールに適合していないコードが見つかった場合、「コードの修正」または「非適合理由を記載したドキュメントの作成(Deviation)」を行うことになっています。後者の対応をした場合、コードが修正されないので、該当ルールの評点は100点になりません。
- MISRA-C:2004の品質診断は、企業内での品質改善活動の支援を想定したサービスになります。

東陽テクニカ

MISRA-Cに関する東陽テクニカの取り組み

- MISRA-C研究会(SESSAME[*1] Working Group 3)の設立・運営に寄与し、研究会メンバーの一員として活動[*2]
- 欧州MISRA委員会との技術交流を実施
- MISRA-C適合度評価モジュール(QA MISRA)の販売
  - QA MISRAの開発元である英国Programming Researchは、ISO C、欧州MISRA委員会のメンバーとして活動
  - QA MISRAは弊社および英国Programming Researchの研究活動を反映した正確なルール解釈に基づいている

※ *1 SESSAME: 組込みソフトウェア管理者・技術者育成研究会

※ *2 日本規格協会より次の書籍を出版済み

MISRA-C研究会編「組込み開発者におくるMISRA-C」

MISRA-C研究会編「組込み開発者におくるMISRA-C:2004」

東陽テクニカ

ご清聴ありがとうございました。

東陽テクニカ

