R20TS0378JJ0100
Rev.1.00
2018.12.16 号

【お知らせ】

スタック領域の破壊を動的にチェックして品質と安全性向上！ ルネサス製コンパイラ professional 版 スタック破壊検出機能のご紹介

概要

ルネサス製コンパイラ（CC-RL/CC-RX/CC-RH）professional 版の機能のひとつ、スタック破壊検出機能についてご紹介します。

本機能を使用することにより、プログラム実行中にスタック領域が破壊されていないかチェックすることが可能です。これによりプログラムのバグやセキュリティアタックによるスタック領域破壊時の暴走や誤動作を未然に防ぐことが可能になります。

1. 特長

1.1 プログラムの品質と安全性確保に貢献

スタック破壊検出機能では、スタック領域が破壊された場合にはエラー処理を実行します。これによりプログラムの暴走や誤動作を未然に防ぐことが可能になり、**プログラムの品質や安全性向上に寄与します。**

スタック破壊検出機能は、関数本体を実行する前にスタック領域に特定の値を埋め込み、実行後にこの値をチェックすることで、スタック領域が破壊されていないか検出する仕組みです。これにより暴走や誤動作を防止します。

図 1、図 2 にスタック破壊検出機能がない場合とある場合の処理フローを示します。

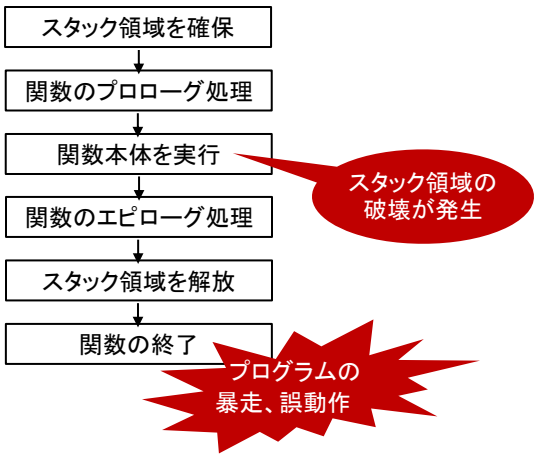

図 1 通常時の処理

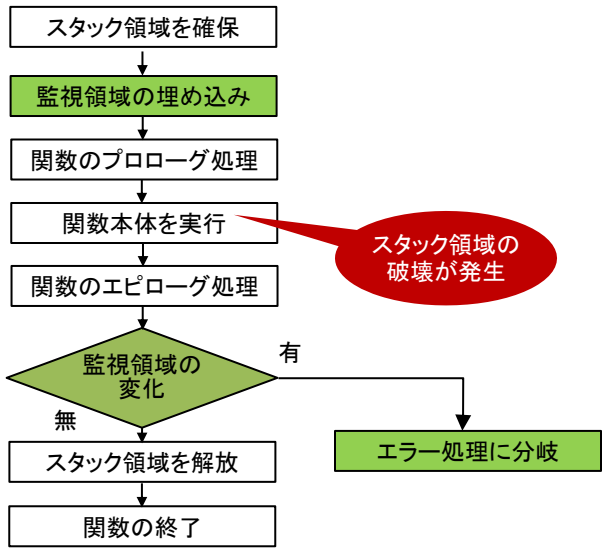

図 2 スタック破壊検出機能有効時の処理

関数が使用するスタック領域は、関数の入り口で確保します。その際に監視領域と呼ばれる領域（CC-RL の場合 2 バイト、CC-RX/CC-RH の場合 4 バイト）をローカル変数領域の直前に確保し、特定の値を埋め込みます（図 3）。監視領域は通常の関数実行によって変化することはありませんが、何らかの理由でスタック領域が破壊されると、監視領域内の値も変化します（図 4）。

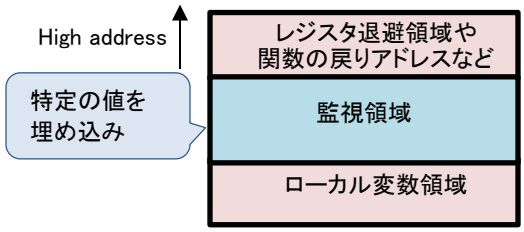

図 3 【関数本体処理前】監視領域

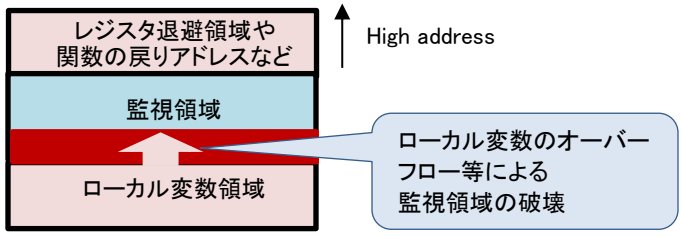

図 4 【関数本体処理中】スタック破壊

関数本体の処理を実行後に、監視領域に埋め込まれた値が変化していないかチェックを行います。値が変化している場合には、スタック領域が破壊されたと判断し、エラー処理を行います（図 5）。
エラー処理の内容についてはユーザが任意に記述可能です。

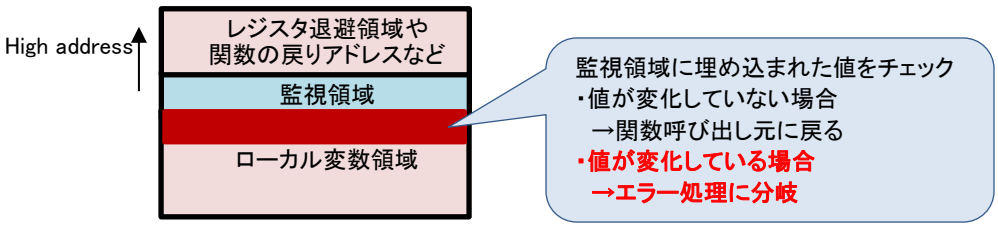

図 5【関数本体処理後】監視領域チェック

このように、スタック領域が破壊された場合にはエラー処理を指定して、プログラムの暴走や誤動作を未然に防ぐことが可能になり、プログラムの品質や安全性向上に寄与します。

1.2 実行例

スタック破壊検出機能を使用するために、以下の 2 種類の方法から選択できます。

（1）統合開発環境(CS+または e² studio) のプロパティでスタック破壊検出を行う設定を有効にする。

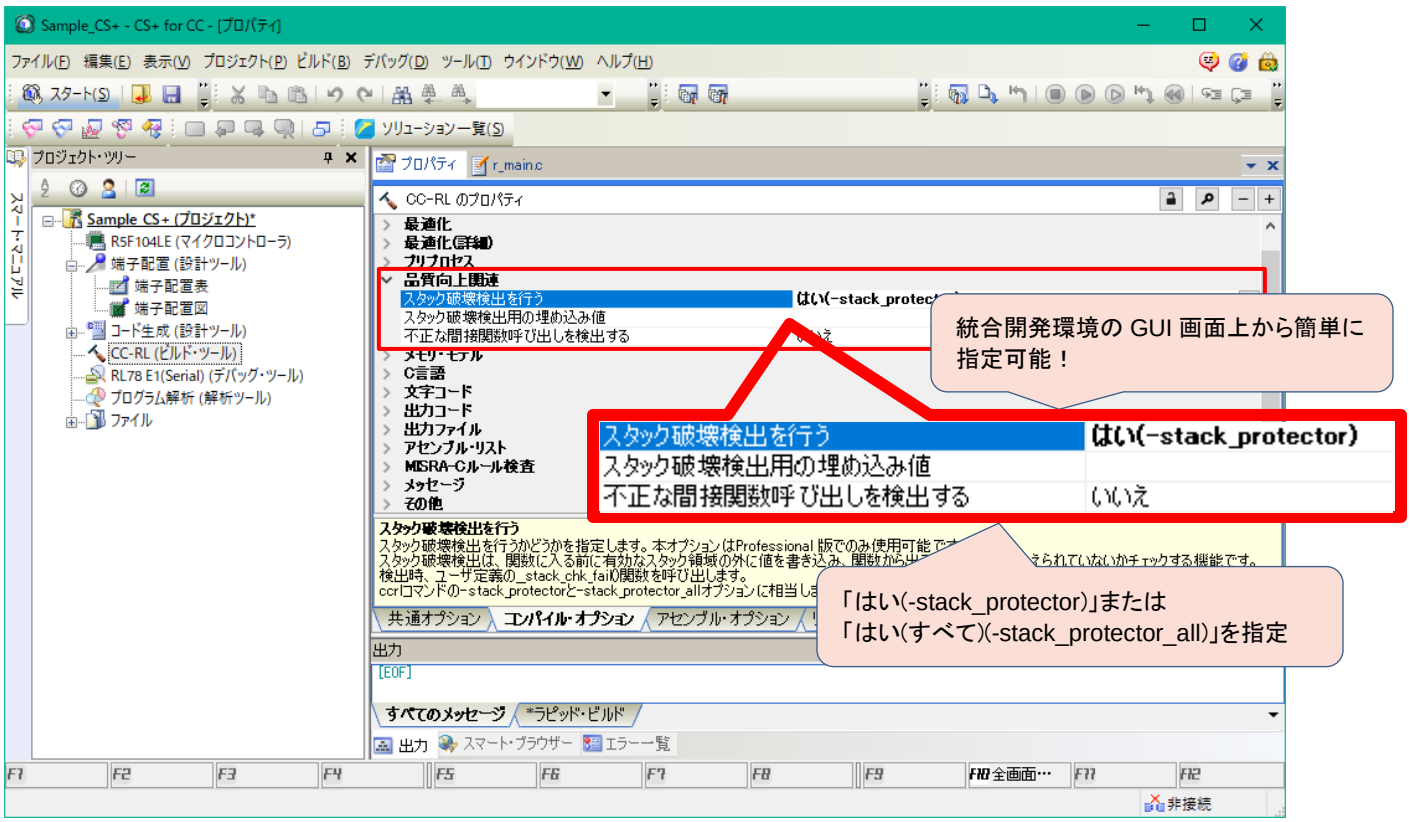

図 6 CS+の設定方法(CC-RL の場合)

（2）拡張言語 #pragma 指令を使用して、対象の関数を指定する。

”#pragma stack_protector”を使用すると、指定した関数がスタック破壊検出の対象関数となります。

```
#pragma stack_protector 関数名 (num=数値)
```

指定した数値を監視領域に埋め込みます。「(num=数値)」を省略するとコンパイラが自動的に数値を指定して監視領域に埋め込みます。

次にエラー処理の関数を記述します。

スタック破壊を検出するとエラー処理として__stack_chk_fail 関数が呼ばれます。
__stack_chk_fail 関数の処理内容はユーザが任意に記述可能です。

```
void __stack_chk_fail(void) {
// エラー処理内容を記述
}
```

2. その他の professional 版の機能のご紹介

- MISRA-C ルールチェック機能

本機能について、以下のツールニュースでご紹介しています。

コンパイルとの同時実行で「プログラム開発の工数削減と品質向上」を実現する本機能を、ぜひご確認ください。

https://www.renesas.com/search/keyword-search.html#genre=document&q= r20ts0342
【お知らせ】
MISRA-C ルールチェックとコンパイルの同時実行でプログラム開発の工数削減と品質向上！
ルネサス製コンパイラ professional 版 MISRA-C ルールチェック機能のご紹介

- 制御レジスタ更新時の同期化機能

本機能について、以下のツールニュースでご紹介しています。

同期化処理の自動挿入で「RH850 ファミリの開発工数を削減する」本機能を、ぜひご確認ください。

https://www.renesas.com/search/keyword-search.html#genre=document&q= r20ts0347
【お知らせ】
同期化処理の自動挿入で RH850 ファミリの開発工数の削減！
ルネサス製コンパイラ professional 版 制御レジスタ更新時の同期化機能のご紹介

- その他の便利な機能

ルネサス製コンパイラ professional 版には様々な機能（*）があります。

*：不正な間接関数呼び出し検出機能、動的メモリ管理関数のセーフティ向上機能、
半精度浮動小数点数 など

詳細は、以下のリーフレットをご参照ください。

https://www.renesas.com/search/keyword-search.html#genre=document&q=r20pf0024

ルネサス製コンパイラ professional 版

ルネサス製コンパイラ professional 版 の機能の詳細については、以下のアプリケーションノートをご参照ください。お客様のプログラムの品質向上と開発期間短縮に貢献する機能を掲載しています。また、コピー&ペーストですぐに試せる C ソース例も掲載しています。

https://www.renesas.com/search/keyword-search.html#genre=document&q=r20ut4026
ルネサス製コンパイラ professional 版コンパイラ編

3. 購入方法

ご注文の際には、最寄りの弊社営業または特約店までご連絡ください。

standard 版ノードロック・ライセンスをすでにお持ちのお客様は「アップグレード(エディション)ライセンス」を追加でご購入いただくことで、standard 版から professional 版へアップグレードすることができます。製品型名は以下コンパイラパッケージの web ページをご参照ください。

CC-RL： https://www.renesas.com/rl78_c

CC-RX： https://www.renesas.com/rx_c

CC-RH： https://www.renesas.com/rh850_c

以上

改訂記録

Rev.	発行日	改訂内容	
		ページ	ポイント
1.00	2018.12.16	-	新規発行

ルネサスエレクトロニクス株式会社
〒135-0061　東京都江東区豊洲 3-2-24（豊洲フォレシア）

■総合お問い合わせ先
https://www.renesas.com/contact/

TS Colophon 2.1