コーディング作法ガイド(ESCR※1)整備の取り組み

SEC調査役 三原 幸博　SEC調査役 十山 圭介

1 コーディング作法ガイドの改訂

IPA/SECでは組込みソフトウェアのソースコード品質の向上を目的に、ESCRとして、コーディングの際に注意すべき事柄やノウハウを取りまとめ、公開している。ESCRでは、コーディングにおける基本的な考え方(作法)と、作法を対象言語に合わせて具体化した個々のルールとを、ソフトウェア品質特性の観点で整理している。組織でコーディング規約を決める際や、コーディング時の参考、また個人のプログラミング学習のために、書籍やPDF版など、これまで3万部を超えて多くの方々にESCRを利用いただいている。

● ESCR[C++言語版]の改訂

ESCRにはC言語とC++言語に向けた2種があり、それぞれ言語規格の更新に追随して改訂を行っているが、2016年度はC++言語の新しい標準規格C++11及びC++14に準拠し、C言語版との整合性も確保したESCR[C++言語版]の改訂作業を終え、2016年10月にVer.2.0として発行した※2。

この改訂について、方針を図1に、変更個所のまとめを図2に示す。また、今回、パブリックコメントを実施すると共に、中田育男先生(筑波大学名誉教授)にご監修をいただいて表現の分かりやすさと正確性の向上を図った。

● セキュアコーディングに向けたESCR[C言語版]の改訂

セキュリティに配慮したコーディングの重要性が高まっており、ESCR[C言語版]を対象としてセキュアコーディング対応の検討を開始した。

これまでのESCRの改訂では、セキュリティ品質特性に対する説明の追加と脆弱性やCERT※3 Cとの対応付けの追加にとどめていたが、以降CERT Cルールの一部やIPAセキュリティセンターからの提案を、新規ルールの追加や解説の拡充といった形でESCRの中に取り込む改訂作業を進めている。

2 コーディング作法ガイドに関する海外連携

MISRA CとMISRA C++はMISRA※4が策定しているコーディングガイドラインで、安全で信頼性あるソフトウェアの開発のため、自動車業界を中心に広範に運用され標準技法としての地位を築いている。IPA/SECでは、ESCRとMISRA Cとで相互引用や、改訂時のレビューを行うなど、MISRAと連携して活動している。

今回のESCR[C++言語版]の改訂では、日本語版と英語版を同時に発行したので、MISRAに英語版を送付し、MISRA WGのメンバから多くのコメントをいただいた。それらへの対応も実施中である。

また、コーディングルールに関して2014年よりNIST※5、CMUとも意見交換を行っているが、今年度は2017年1月にCMU/SEI※6を訪問し、IPAからは、ESCRの改訂状況、及びESCRのルールとCERT Cルールとの対応表の現状について説明した。

(1)セキュリティへの対応
- JIS X 25010で追加された品質特性に対応する説明を追加

品質特性	品質副特性		コードの品質
セキュリティ	機密性	製品またはシステムが、アクセスすることを認められたデータだけにアクセスすることができることを確実にする度合い。	アクセスが認められたデータだけにアクセスすることができることを確実にする度合い。
	インテグリティ	コンピュータープログラムまたはデータに権限を持たないでアクセスすることまたは修正することを、システム、製品または構成要素が防止する度合い。	プログラムまたはデータ領域に権限を持たないでアクセスすることまたは修正することを防止する度合い。
	否認防止性 ・・・		

(2)作法・ルールの改訂方針
- 新機能について、C++11を中心にコーディングの決まりとしてある程度成熟していると思われるルールを取り込む

図1　ESCR C++改訂の方針

ESCR C++ Ver. 1.0 からの作法・ルールの修正数

		Ver.1.0	Ver.2.0	追加	修正	削除
信頼性	作法詳細	21	23	2		
	ルール	60	65	5	19	
保守性	作法詳細	29	30	1	1	
	ルール	82	82	2	27	2
移植性	作法詳細	6	7	1		
	ルール	15	16	1	7	
効率性	作法詳細	1	←			
	ルール	10	←		2	
合計	作法詳細	57	61	4	1	—
	ルール	167	173	8	55	2

※軽微な変更は「修正」としてカウントせず　※重複カウントあり

- 追加ルール
  - ✓C++11対応　5
  - ✓ESCR C 整合　2
  - ✓他(改善)　1
- 修正ルール
  - ✓C++11対応　24
  - ✓ESCR C 整合　25
  - ✓他(改善)　9
- 削除ルール
  - ✓不要と判断(ESCR C 整合)　2

図2　作法・ルール変更個所のまとめ

脚注

※1 ESCR：Embedded System development Coding Reference
※2 http://www.ipa.go.jp/sec/reports/20161018.html
※3 CERT：Computer Emergency Response Team
※4 MISRA：The Motor Industry Software Reliability Association
※5 NIST：National Institute of Standards and Technology
※6 CMU/SEI：Carnegie Mellon University / Software Engineering Institute