コーディング作法ガイド(ESCR※1)の整備について

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(ESCR C++)の改訂状況

IPA/SECでは組込みソフトウェアのソースコード品質をより良いものとすることを目的に、コーディングの際に注意すべき事柄やノウハウを作法ガイド：ESCRとして公開している。

ESCRは、コーディングにおける基本的な考え方(作法)と、作法を対象の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たものである。組織やプロジェクトでコーディングルールを決める際や実際のコーディング時の参考のため、また個々人のプログラミング学習のためとして、書籍やPDFなどこれまで3万部を超えて多くの方々に利用いただいている。

ESCRはC言語とC++言語に対応しており、近年広く使用されるようになってきているC++言語向けでは2003年版の言語規格(C++03)に準拠したESCR［C++言語版］Ver. 1.0を2010年に発行している。

今回、この［C++言語版］について、言語の新しい標準規格C++11及びC++14に準拠し、また2013年度に改訂したESCR［C言語版］との整合性を確保するべく改訂作業を進めている。改訂作業は、コード記述のレベルを基本にライブラリ関数やテンプレートに関しては含めないというVer. 1.0と同じ方針で、2014年度からコーディング作法ガイド改訂WGにおいて開始しており、2015年度は、C++11及びC++14での改訂項目に対応した変更点とESCR［C言語版］の改訂に関連する変更点を整理しつつ、原稿作成を行った。改訂版は、2016年10月発行の予定である。

2 コーディング作法ガイドにおける海外連携

MISRA CとMISRA C++は英国MISRA※2が策定しているコーディングガイドラインであり、安全で信頼性の高い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では設立時から、ESCRとMISRA Cとで相互に記述の引用や、改訂時のレビューを行うなど、MISRAと連携して活動を実施している。

2015年10月14日に、MISRAからCとC++ WGの議長であるA. Banks氏とC. Tapp氏を招聘し、「ソフトウェア品質向上のためのコーディング技法と標準」と題するセミナー※3を、名古屋国際会議場においてIPA主催、ASIF・JASA・SESSAME共催で開催した。

本セミナーでは日本における安全で高信頼なソフトウェア開発の実践を目的に、ガイド適用時の効果や制限まで含めてMISRA C及びC++とESCR、セキュアコーディングのためのCERT C※4を関連付けると共に、これら技法の標準化に向けた日欧での活動についての紹介と議論を行った。MISRA側からはC、C++のガイドライン策定活動やスケジュール、安全性とセキュリティに関する活動を、日本側からはESCRの状況とSESSAME※5を中心とする日本での有志によるMISRA C適用に向けた活動を、それぞれ紹介した。

また、2014年よりESCRのセキュリティ対応に関してSECで作成しているESCRのルールとCWE※6の対応付けについて、米国NIST※7と意見交換を行っている。昨年度は、3月にNISTを訪問し、対応表の現状を説明した。

【脚注】

※1 ESCR：Embedded System development Coding Reference
※2 MISRA：The Motor Industry Software Reliability Association（欧州の自動車業界団体）
※3 http://sec.ipa.go.jp/seminar/20151014.html
※4 CERT C：C言語を使ってセキュアコーディングを行うためのルール等をまとめたコーディング規約
※5 SESSAME：NPO法人組込みソフトウェア管理者・技術者育成研究会
※6 CWE：Common Weakness Enumeration（ソフトウェアの脆弱性の種類や関連する情報について列挙したもの）
※7 NIST：National Institute of Standards and Technology（米国国立標準技術研究所）