システム構築能力の強化

SEC システムグループリーダー　山下 博之

IT の利用拡大と IT システムの複雑化・大規模化が進展し、IT システムの信頼性・安全性は一層重要となっている。しかしながら、システム構築プロジェクトの失敗はなくならないばかりか、深刻さを増すセキュリティ上の課題に新たな対応を迫られている。こうした背景から、IPA/SEC では、システム構築能力の強化に取り組み、過去 5 年間に次の活動を行った：要件定義などシステム構築上流工程の強化、システム理論に基づく安全性解析手法の普及展開、制御システム向けのセーフティ・セキュリティ対策の検討、コーディング作法ガイドの整備。

システム構築能力の強化

上流工程の課題解決に向けて

SEC 研究員　山本 英明　SEC 研究員　村岡 恭昭　SEC システムグループリーダー　山下 博之

システム構築上流工程の作業不備による開発プロジェクトの失敗や運用後のシステムトラブルがなくならないという背景から、要件定義と再構築の 2 つの課題に取り組んだ成果をまとめガイドブックと小冊子を発行した。また、非機能要求の考慮漏れによる手戻りをなくすために、非機能要求グレードを 8 年ぶりに改訂した。

1 背景

当初、業務支援であった IT システムは、その技術自身の進展と時代の要請から、その利用が質、量共に拡大してきた。新たなビジネス価値を創出するための攻めの分野と、基幹業務を確実に遂行する守りの分野を区別し、それぞれに強化することが経営に直結する課題となった。

攻めの分野では、要求のすべてが開発初期に分からず、IT システムのサービス開始後に徐々に明らかになる要求への対応が常に求められる課題がある。また、攻めの分野を推進するためには守りの分野を着実に整備／更新し、適切に連携する必要がある。守りの分野では、長年保守開発を続けたシステムの再構築に「特有の難しさ」があり、下流工程のリスクであるにもかかわらず把握が難しい課題がある。実際、再構築プロジェクトの失敗事例報告は少なくない。

また、公開済の非機能要求に関しては、新たなセキュリティ脅威の台頭や、システム基盤技術の進展など、社会や技術の変化により、非機能要求グレード※1 初版公開時から非機能要求に変化が生じていることが課題である。

以上の上流工程に関する課題を解決するために、「要件定義」「システム再構築」「非機能要求」をテーマとした取り組みを行った。

2 要件定義

要件定義は、立場が異なる人とのコミュニケーションが最も多く、抜けや漏れが発生しやすい。図 1-1 に示す通り、5 つのリスクに対する対策が求められる。

「ユーザのための要件定義ガイド～要求を明確にするための勘どころ～」（以下、要件定義ガイド）を 2016 年度に出版※2 し、主にユーザ企業で IT システムの要件定義を実施する方を対象に、要件定義において発生する抜け、漏れなどの問題と、その解決方法をまとめた（図 1-2）。

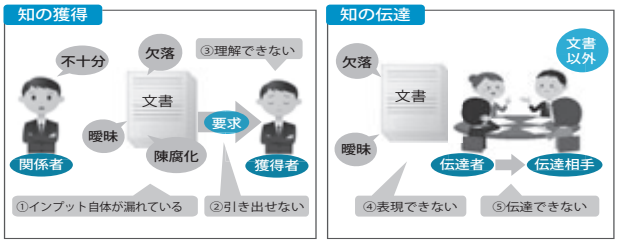

図 1-1　コミュニケーションギャップを生む 5 つのリスク

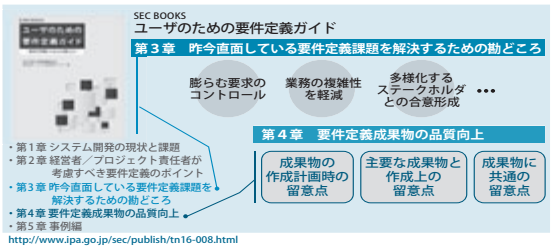

図 1-2　要件定義ガイドの構成

3 システム再構築

「システム再構築を成功に導くユーザガイド　第２版　～ユーザとベンダで共有する再構築のリスクと対策～」（以下、再構築ガイド）を 2017 年度に出版※3 し、ユーザ企業がシステム再構築の企画／計画工程で留意すべきポイントを、実践に即した形式で紹介した（図 1-3）。

とくに、品質保証における最も重要なテーマである「業務継続性の担保」については、読者の実践につながるような具体的な内容を示した（図 1-4）。

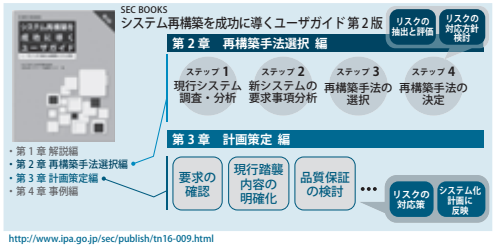

図 1-3　再構築ガイドの構成

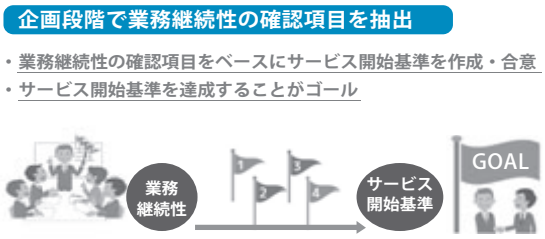

図 1-4　業務継続性を上流工程から明確化するイメージ

4 非機能要求

非機能要求グレードの初版を 2010 年度に公開したが、非機能要求の変化に伴う定義漏れを防止するため、非機能要求グレードのスコープは維持したまま、「非機能要求グレード 2018」を 2018 年 4 月に公開した。主な改訂対象は、「セキュリティ」と「仮想化」に関する要求である。

なお、主要な改訂は、図 1-5 に示す通り「非機能要求グレード本体」である。本体のうちの利用ガイド（解説編、利用編）、及び周辺資料の利用ガイド（活用編）や小冊子、各種研修教材は、メトリクスの総数など、改訂内容と整合させる必要がある部分のみを更新した。

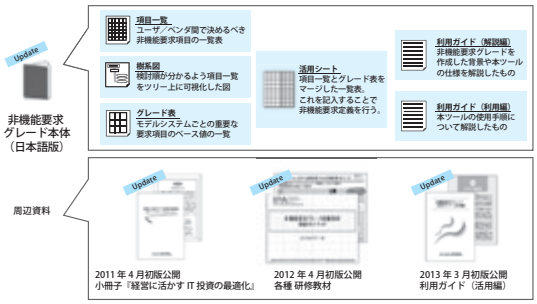

図 1-5　改訂した「非機能要求グレード」の成果物一覧

5 今後の予定

ガイドブックや非機能要求グレードの更なる普及のため、セミナーやイベントでの発信を行う。とくに、作成した小冊子を用いて、経営層など企業の上位層や、経験が浅い読者層にも内容をご理解いただきたい。

なお、要件定義ガイドは第２版や中小企業向けを作成する。第２版では、要件定義工程のより前半における課題解決の勘どころを充実させる。中小企業向けでは、比較的小さな規模に適用する際の勘どころをまとめる。

※1　URL: https://www.ipa.go.jp/sec/reports/20180425.html
※2　URL: https://www.ipa.go.jp/sec/publish/tn16-008.html
※3　URL: https://www.ipa.go.jp/sec/publish/tn16-009.html

システム構築能力の強化

システム理論に基づく安全性解析手法 STAMP/STPA の普及促進

SEC 調査役　石井 正悟　SEC 調査役　三原 幸博
SEC 調査役　十山 圭介　SEC 研究員　金子 朋子　SEC 研究員　向山 輝

STAMP/STPA は、現代の複雑システムに適した新しい安全性解析手法としてマサチューセッツ工科大学（MIT）が 2012 年に提唱した手法であり、欧米において活用が進展している。IPA/SEC では 2015 年度から、国内での STAMP/STPA の普及活動を行っており、この分野の有識者などが参加する「IoT システム安全性向上技術 WG」での検討を通し、これまでにガイドブックの発行、STAMP 支援ツールの開発・公開、ワークショップの開催を行ってきた。

1 はじめてのSTAMP/STPA（活用編）

IPA/SEC では、2015 年度に入門書として「はじめての STAMP/STPA」を発行し、2016 年度には、実際に適用する際のヒントやコツを解説した「実践編」を発行した。

2017 年度は、「理解する」「やってみる」と段階を踏んできたシリーズの第 3 弾として、「当たり前に実施する」ことを目指し、「はじめての STAMP/STPA（活用編）」を公開した（図 2-1）。

図 2-1　「はじめての STAMP/STPA」シリーズ

活用編では、鉄道、ロボット、自動車、電力網の分野の 4 つの具体例で、人と機械の協調による安全制御の分析や安全とセキュリティの統合分析などへの適用を解説した。いずれも、産業界において STAMP/STPA を役立てる際に参考となる先進的な事例である。

(1)　鉄道踏切の分析例

既存の鉄道踏切制御システムの課題を整理した上で、その解決方法として列車と踏切制御装置が情報交換を行いながら制御を行う「クローズドループ型」の安全性を STAMP を用いて評価した事例を解説した（図 2-2）。

(2)　二輪倒立ロボットの分析例

人と機械（ロボット）の協調によって転倒や衝突を避ける安全制御に対して、指示の競合などによる事故要因を STAMP を用いて分析した事例を解説した。

(3)　自動車の電動パーキングブレーキ（EPB）の分析例

一般社団法人 JASPAR（Japan Automotive Software Platform and Architecture）が仮想的な EPB を取り上げて STAMP/STPA 分析を実施した例を紹介した（図 2-3）。ISO 26262（自動車向け機能安全の国際規格）に規定される安全分析に STAMP/STPA を適用するための工夫や留意点が示されている。自動車分野以外の産業分野における安全規格や既存開発プロセスとの整合を考える上でも参考となる事例である。

(4)　電力網のセキュリティ分析への応用例

米国における広域送電網とローカル送電網の接続に関して、安全性とセキュリティを統合して分析するための STPA 拡張手法である "STPA-SafeSec" を適用した分析事例に関する文献を紹介した。

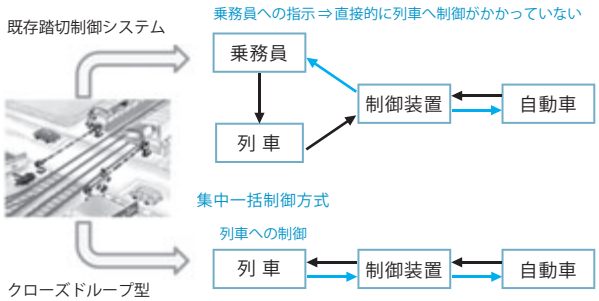

図 2-2　クローズドループ型踏切の STAMP モデル

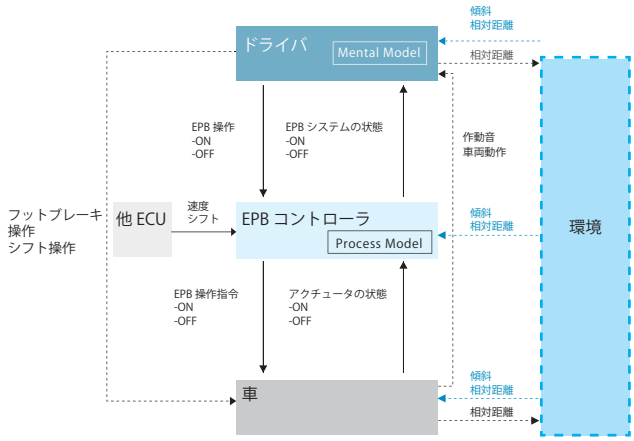

図 2-3　電動パーキングブレーキの STAMP モデル

2 STAMP Workbench

STAMP の導入を容易にするモデリングツール STAMP Workbench を 2018 年 3 月に無償で公開した。

STPA は分析において自由な発想を引き出すことを意図した手法であることから、分析の途中で新たな気づきを得て前の Step に立ち戻ることが少なくない。そうすることによって、分析の質が向上するので、新たな気づきを得ることは喜ばしいことである。しかし、喜ばしいとは言っても手戻りであることに違いはない。既に作成した図表を修正するのは、面倒な上に、修正ミスを犯しやすい作業である。更に、図表修正作業のために分析のための思考が中断されることが困る。こういうときに有効なのがモデリングツールである。しかし、STPA 分析という目的に合ったモデリングツールは海外に 2,3 あるものの、いずれも研究目的に開発されており、分析作業を支援するツールとしては物足りなかった。そこで、「産業界で STAMP を実適用する多くの人の役に立つ機能」を備えたツール STAMP Workbench を IPA/SEC が開発し、広く普及するよう、OSS として公開した。同ツールの開発思想は次の通り。

■手順を誘導する。しかし、使い方を限定しない

■専門用語、表記法を知らなくても解析できる

■可能な限り自動化し、分析者が思考に専念できる

STAMP　Workbench の画面例を図 2-4 に示す。

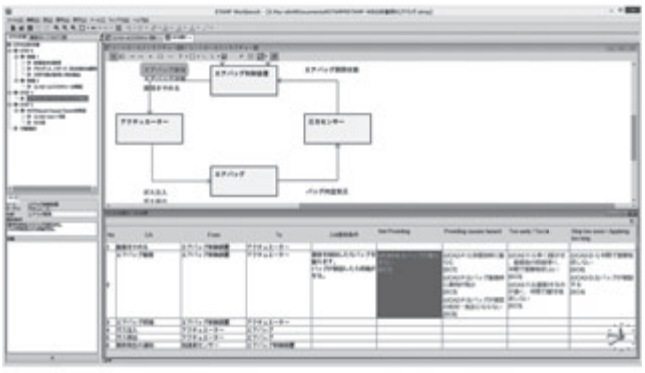

図 2-4　STAMP　Workbench の画面例

3 STAMPワークショップ in Japan

2016年に福岡市で開催した第1回に引き続き、第2回STAMPワークショップ in Japanを、2017年11月27日から3日間にわたって慶応義塾大学で開催した。

4カ国から延べ181名（第1回は117名）の参加者が集まり、初日に米国MITからの基調講演／チュートリアル、欧州STAMPワークショップ（ESW）からの招待講演が順に行われ、その後、一般講演として産業界から13件、学術界から11件、合計24件（第1回は16件）の発表が行われた（表2-1）。

表2-1　STAMPワークショップ（第2回）のスケジュール

開催日	プログラム
11/27（月）	チュートリアル・招待講演・一般講演（Overseas & Tools Session）：3件・STAMPツールデモ
11/28（火）	一般講演：16件
11/29（水）	一般講演：5件

併せてポスター展示を2件（第1回は0件）行い、2017年度に開発中であったSTAMP支援ツールSTAMP Workbenchを紹介し、期間中、デモ展示した。また、講演資料をIPA/SEC Webサイトに掲載した。（https://www.ipa.go.jp/sec/events/20171127.html）

一般講演の内容を分析した結果、以下の傾向が読み取れた。

①学術界からの発表は、手法解説に偏っているが、産業界からはどの種別にもほぼ同じ件数の発表がある

②試行事例の発表件数は産業界と学術界でほぼ同じである。産業界は、開発済みの制御システムを題材としているが、学術界は、制御システム以外にも目を向けている

③活用事例と手法改善は、産業界から多く発表されており、開発中又は今後のシステムに適用してみようという産業界の意欲が感じられる

④産業界から手法改善の発表が多かったのは、適用プロセスの標準化を目指して、手法の定型化を求めていることによると考えられる

4 今後の取り組み

今後は、これまでの活動の積み上げを生かし、STAMPを適用した効果をより多くの方に実感いただき、複雑化するシステムの安全解析の手法として広く有効活用されていくことを目指していく。

システム構築能力の強化

制御システム向けのセーフティ及びセキュリティ対策

SEC 調査役 石田 茂　SEC 調査役 久野 倫義
SEC 研究員 細目 紀子　SEC 専門委員 中谷 博司

クローズした環境で運用されてきた重要インフラを担う制御システムに対し、IoT化の進展や事業系システムとの連携など相互接続が進む中、セキュリティ対策が急務となっている。このような状況に対応するため、「制御システムセーフティ・セキュリティ要件検討ガイド」を発行し、セーフティとセキュリティのそれぞれの要件を連携させるための基本的な考え方と手順を示した。

1 背景

プラント、鉄道、電力など社会の重要インフラを担う制御システムは、稼働の連続性と共に、安全性や環境への影響などにも配慮を要することから、その多くは独自システムによるクローズした環境で運用されてきた。しかし近年では、IoT化の進展や制御系システムの事業系システムとの連携など、制御システムの稼働環境にも大きな変化が生じてきた。こうした相互接続が進む中、重要インフラを狙ったサイバー攻撃の増加は大きな問題となっており、セキュリティ対策が急務となっている。

一方、開発・運用に携わる現場には「セーフティ※1とセキュリティ双方に精通した技術者が極めて少ない」「安全性を確保しながらセキュリティ検討をどのように進めたら良いのか分からない」「情報セキュリティ技術者は、機密漏えいやシステムに対する改ざん・攻撃が、健康や安全性、環境に重大な影響を及ぼすなど、制御システム特有の被害イメージをつかみにくい」などの課題がある。

そこでIPAでは、2015年より関係企業や大学機関の方々から成る制御システムセーフティ・セキュリティ検討WGを設置し、これらの課題の解決に向けた検討を進めてきた。その成果を「制御システム セーフティ・セキュリティ要件検討ガイド」として取りまとめ、2018年3月に公開した。

2 本ガイドの目的と特徴

2.1 目的

システム障害発生時、人命や環境など社会活動に影響を及ぼすような制御システムを想定し、既存のセーフティシステム※2に対し、セーフティとセキュリティのそれぞれの要件を連携させるための基本的な考え方と手順を示すことを目的としている。

2.2 特徴

本ガイドの特徴を以下に示す。

【セーフティファースト】

セーフティシステムを含む制御システムによって稼働中の工場、プラントがあり、安全性の確保を実現済のシステムにセキュリティ対応を行うケースを想定。

【グローバル対応と国際規格】

事業のグローバル化の実情に鑑み、セーフティ・セキュリティの国際規格・標準を参照。

セーフティ：IEC 61508※3, Functional safety of electrical/electronic/programmable electronic safety-related systems

セキュリティ：IEC 62443※4, Industrial Automation and Control Systems Security

【二編構成による解説】

基本編では基本となる考え方と検討手順を示し、より理解を深めることができるよう、ケーススタディ編で抽象化されたシステムによる詳細を解説。また、脅威分析を実施する際の分析シートテンプレートも添付。

3 ガイドの構成

3.1 基本編

基本編ではセーフティとセキュリティの検討を進める際の考え方と検討プロセスについて図表を用いながら説明している。この際、記述内容に関連のある情報やトピックスをコラムとして要所に掲載した。

セーフティファーストの考え方に基づき、セキュリティ検討を行う際の検討プロセス概要は図 3-1 の通りである。

セーフティは構築済という前提なので、Step0 として過去に行われた安全設計経緯の確認から開始し、事業者が実施するセキュリティ検討とその結果を受けてインテグレータが実施するセキュリティ検討という手順として示した。

※1 「セーフティ」：安全
※2 「セーフティシステム」：国際機能安全規格などに適合した安全関連システム
※3 IEC 61508: IEC（国際電気標準会議）が制定した基本安全規格。プロセス産業における電気・電子・プログラマブル電子（E/E/PE）機能安全に関する国際規格
※4 IEC 62443: 制御システムセキュリティの事業者、インテグレータ、装置ベンダを対象とした汎用的な国際標準規格。

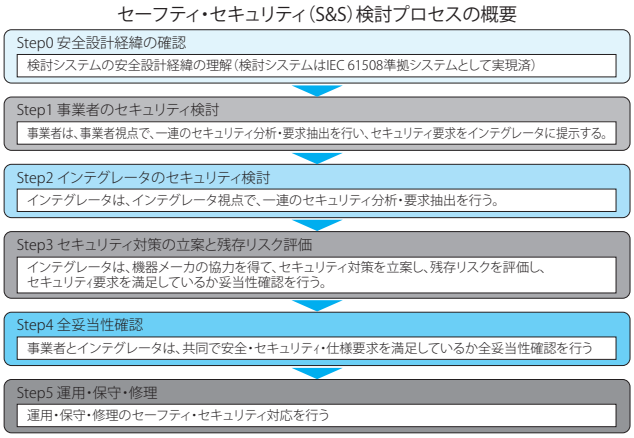

図 3-1　検討プロセス

3.2 ケーススタディ編

ケーススタディ編では、基本編の内容を具体的に示し、理解を促進できるよう、現実のシステムを抽象化した「検討システム」を用いて解説した。この「検討システム」は産業用ロボットを含む FA（ファクトリーオートメーション）システムで、実在するものではなく、あくまでも解説用のものである。

ケーススタディ編ではこの検討システムに対して、基本編で示したプロセス手順に従って、検討が進む一連のストーリーとして記述した。図 3-2 に検討例を示す。

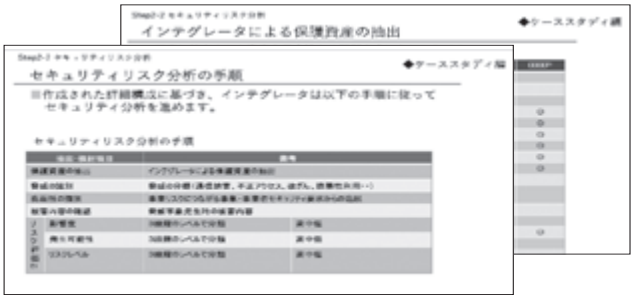

図 3-2　ケーススタディの検討例

3.3 脅威分析シート

本ガイドでは、手順に従って系統的に脅威分析を行うために、図 3-3 に示す「脅威分析シート」を用いている。

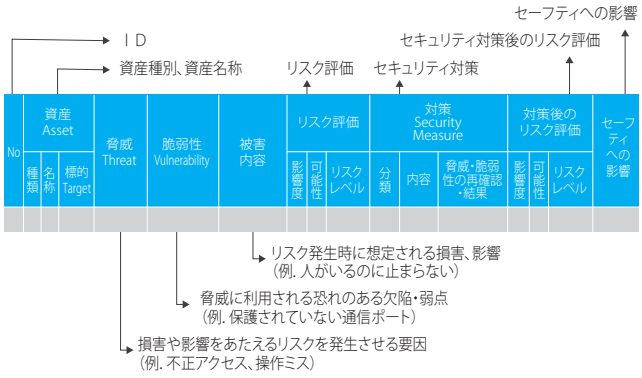

図 3-3　脅威分析シートの構成

コーディング作法ガイド（ESCR※1）の整備

SEC 調査役 十山 圭介　SEC 調査役 三原 幸博　SEC 調査役 久野 倫義

ESCR は 2006 年の C 言語版 Ver. 1.0 発行以来、言語規格の更新などに追随して改訂を行っている。2015 ～ 2016 年度には、C++ 言語版の改訂（Ver. 2.0）を実施し、2017 年度には、セキュアコーディングに向けた C 言語版の改訂に取り組み、C 言語版 Ver. 3.0 を公開し、2018 年 6 月 20 日に書籍化し発行した。

1 コーディング作法ガイドの改訂

SEC ではコーディング作法ガイド改訂 WG において、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）と対象言語に合わせて作法を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。2017 年度は以下の改訂を行い、その結果を公開した。

● セキュアコーディングに向けた ESCR の改訂

この改訂では、CERT C※2 ルールの一部や IPA セキュリセンター（ISEC）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 の中に取り込む作業を進めた。CERT C ルールと ISEC 提案ルール 6 個をリストアップし、それらに対応する ESCR ルールがあるか、ない場合に新規作成するか、解説を追加するかといった点を検討して ESCR [C 言語版] の改訂版（Ver. 3.0）を作成した。

● ESCR ルールと CERT ルール対応表の改訂

「現状の ESCR のルールにはセキュリティの観点から重要なものが含まれており、それらと CERT C ルールとの対応付けを行ってコーディング規約の作成段階からセキュリティを念頭に置く」（図 4-1）ことが重要であるとの認識から、暫定版ではあるが 2016 年 6 月から ESCR C ルールと CERT C ルールの対応表を公開している。

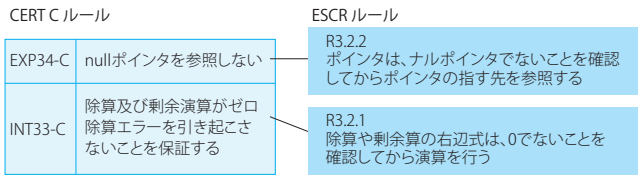

図 4-1　ESCR と CERT の典型的なルール対応関係

2017 年度には、ルールや解説の ESCR 本編への追加に加え、この対応表を改訂・拡張して C++ 言語のルール対応も含めたものとして更新した。表 4-1 に対応表の一部を示す。

表 4-1　ESCR と CERT などのルール対応（一部）

ESCR ルール	MISRA ルールとの関係			CERT C	CERT C++	CWE
	C:2004	C:2012	C++:2008			
［信頼性 1］R1 領域は初期化し、大きさに気を付けて使用する。						
R1.1.1	9.1	R9.1	8-5-1	EXP33-C	EXP53-CPP	CWE-119 CWE-456 CWE665
R1.1.2						CWE-456
R1.2.1				ARR02-C STR11-C STR31-C		ARR02-C STR11-C STR31-C
R1.2.2	9.3	R8.12	8-5-3	INT09-C		CWE-665
R1.3.1	17.1	R18.1	5-0-15 5-0-16	ARR30-C ARR37-C ARR39-C	ARR30-C ARR37-C ARR39-C	CWE-119 CWE-122 CWE-129 CWE-468 CWE469 CWE-788
	17.4	R18.4				

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※3 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。 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。

MISRA からは、MISRA C++ の改訂スケジュールとその適用プロジェクトに関する情報を得ている。また、SEC の WG では 2016 年度の ESCR［C++ 言語版］改訂に対する MISRA WG のメンバからのコメントに対応し、C 言語版にも適用される項目については、その Ver. 3.0 に反映した。

※1　ESCR：Embedded System development Coding Reference
※2　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を定めたもの（カーネギーメロン大学ソフトウェア工学研究所による）
※3　MISRA：The Motor Industry Software Reliability Association