

統合システムの安全・安心に向けた 2012年度の取組み

SEC 統合系プロジェクト リーダー
中村 雄三

SEC 統合系プロジェクト 研究員
三毛 功子

SEC 統合系プロジェクト 研究員
細目 紀子

1 はじめに

現代の社会では、重要インフラをはじめとして、身の回りの製品・システムが高機能・複雑化しており、それを構成するIT技術の重要性が一層高まっている。さらに、このような情報システムや組込み製品・システム等が相互接続されることによる新たなシステム（System of Systems、統合システム）が構成されつつある。経済産業省で推進するIT融合6分野^{*1}は、まさに統合システムであり、例えばスマートコミュニティにおけるスマートハウスでは、従来単独で動作してきた家電、自動車等も相互接続され家庭のエネルギー効率化のため連携して動作するようになる。また、交通システムとしての自動車や都市交通等の連携も今後、進展すると考えられている。

従来、日本の製品・サービスは、その重要なコンポーネントであるソフトウェアも含め、高い品質である、と言われてきた。それぞれの製品・システムに対して、設計・製造工程での品質を意識した開発プロセスの確立や、利用者の利用形態までを含め、様々な観点での品質作りこみが行われてきており、その努力によって安全・安心が確保されてきた。統合システム化等により、想定とは異なった新たな利用形態、異なる動作環境、さらには新たな製品・システムとの接続が行われることで、想定外の新たな障害が生じる可能性がある。同時に、システム間の相互接続により、いったん障害が発生してしまった場合の影響範囲の拡大を防止するなど、利用者の安全・安心に対応する信頼性の確保が重要な課題になっている。

発足後3年となる統合系プロジェクトでは、安全・安心なIT社会の実現を目指し、統合システムに特有、或いは統合システムを構成する情報システムと組込み製品・システムに共通する課題の解決に向けた取組みを進めてきた。ここでは、2012年度の統合系プロジェクトの活動を概説する。

2 2012年度の統合系プロジェクトの活動

2012年度に統合系プロジェクトは、大きく「品質説明力

強化」と「上流品質技術強化」の2つの柱となるテーマに取り組んだ。さらにそれらと関連した「組織的取組み強化」として、信頼性自己診断ツールの提供と海外での障害状況調査等を推進した。ここではその概略を示す。

(1) 1つめの柱：品質説明力強化

「品質説明力強化」では、製品・サービスの品質に関して第三者が検証し、利用者に分かりやすく提示する公正な制度を、それぞれの障害時の影響度やニーズ等に合わせて分野毎に構築できるようにするため、「ソフトウェア品質説明のための制度ガイドライン」を策定した。供給者とは別の第三者が、ある分野の専門家の立場で利用者側の観点から製品・システムを検証することは、供給者のみが品質の確かさを主張することに比べ、利用者の安心のためには大きな前進になると考えられる。また供給者にとっても、品質に関する自らの主張を第三者の検証により確認できること、また場合によっては検証に向けて供給者側で開発プロセスやドキュメント整備等を見直す事によるソフトウェア品質向上の効果も考えられる。詳しくは、この後の記事を参照していただきたい。

(2) 2つめの柱：上流品質技術強化

品質説明力強化の技術的な基盤整備の一環として、「上流品質技術強化」に取り組んだ。上流工程での品質向上を目指して、数学的基盤を持つ形式手法の普及に取り組み、「曖昧性や矛盾のない厳密な仕様を記述すること」、同時に「そのような事のできる人材育成」、のための教材を作成・公開した。また、コンシューマデバイスのディペンダビリティ保証に向けた取組みを進めた。さらに、多様な要求を満足すると同時に、その要求が変化するような統合システムを高信頼で効率的に開発するための手法であるMBSE（Model Based Systems Engineering）の啓発のため、プロジェクト

【脚注】

※1 IT融合6分野 <http://www.meti.go.jp/press/2011/08/20110811002/20110811002.html>

表1 諸外国における政府機関の業種別 IT 障害等に対する対応状況

<諸外国における政府機関の業種別 IT 障害等に対する対応状況について報告書から抜粋>

区分	業種分野	障害情報収集組織	障害に関する公開情報	公開情報例	関連する準拠法、規定
重要 インフラ	情報通信 ・放送	シンガポール 情報通信開発庁 (IDA)	シンガポール (IDA) ・通信障害情報や品質 (QoS) 情報を公開	シンガポール (IDA) ・携帯電話の通信障害に 対し、サービスレジリ エンシ法に基づき、事 業者に罰金 (2012 年)	シンガポール (IDA) ・サービスレジリエンシ 法、通信法
	金融	米 証券取引委員会 (SEC) 連邦準備制度理事会 (FRB) NY 証券取引所 (NYSE) 金融取引業規制機構 (FINRA)	米 (SEC) (FRB) ・障害情報、復旧に関す る情報、調査状況、原 因等を公開 ・証券監督者国際機構 (IO SCO)、バーゼル銀行監 督委員会 (BCBS) へ報 告	米 (NYSE) (SEC) ・証券自動売買障害に 対し、拡大防止策、リ スク管理規定違反調査 (2012 年)	米 (NYSE) (SEC) ・米国証券取引法 ・market-access rule (Rule 15c3-5- Risk Management Controls for Brokers or Dealers with Market Access) ・NYSE Euronext 証券シ ステムの障害に関連す る補償 - 規則 18
	業種横断 (製品安全)	欧州 EU 緊急警告システム (RAPEX) EU 市場監視制度 (ICSMS)	EU (RAPEX) (ICSMS) ・EU 加盟国と中国の消費 製品の障害情報を公開 ※ Software 起因関連は 自動車系が多い	EU (RAPEX) ・ Software に起因する障 害 18 件報告 (2005 年～)	EU ・ EU 一般製品安全指令 (GPSD)

の手法選択や予算決定権のある方を対象とした手引きを作成した。詳しくは、このあとの記事を参照していただきたい。

(3) 海外障害事例調査

システムの信頼性向上のためには、様々な障害事例やその対策等の情報を収集し、共有する事が有効と考えられる。そこで SEC は、海外の障害事例に関する状況把握のため、「海外における IT 障害の影響及び対応策に関する事例調査」を実施した。重要インフラ 10 分野（情報通信・放送、金融、航空、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流）における、2000 年以降に発生した海外障害事例約 300 件に関して、障害の概要、原因、事業者の対策、政府機関等における対応策（障害情報収集・公開・調査方法、法律・規定等の整備状況）等について整理し、調査報告書と障害事例集にまとめ、2013 年 4 月に公開した^{※2}。その一例として、「情報通信・放送」、「金融」業種の政府機関等の障害対応状況について、シンガポール、米国の例を抜粋して紹介する。また業種横断の「製品安全」にかかわる対応例として欧州の EU 緊急警告システム (RAPEX) をとりあげた (表 1)。調査結果の詳細は報告書と事例集を参照していただきたい。

(4) 信頼性自己診断ツール

情報システムの信頼性確保のためには、システム自体の信頼性はもとより、そのシステムの開発・運用に関わるユーザ・ベンダの組織的な取り組みが重要である。経済産業省が 2009 年 3 月 24 日に発行した「情報システムの信頼性向

上に関する評価指標 (第 1 版)」に準拠して、SEC ではユーザ・ベンダの信頼性・安全性の担保となる作業度合を診断する「信頼性自己診断ツール」を提供してきた。本年度は、中核となる診断機能に特化して選択肢を改善し、診断精度の向上を計り、改変可・営利目的で利用可能な形態^{※3}の「スタンドアロン型信頼性自己診断ツール」として 3 月に公開した^{※4}。本ツールを前述の評価指標と共に活用することにより、情報システムのユーザ・ベンダそれぞれが実施すべき事項、協力すべき事項、合意すべき事項等を明確化して、信頼性向上に取り組むことができる。ぜひ、ご活用いただきたい。

3 おわりに

ここでは 2012 年度の統合系プロジェクトの主な活動に関して概説した。2012 年度をもって IPA の第二期中期計画は終了したが、第三期中期計画でも、国民生活の安全・安心のため、SEC として複雑・多様化する情報処理システムの信頼性の見える化に対する取り組みを推進していく。

【脚注】

- ※ 2 「海外における IT 障害の影響及び対応策に関する事例調査」
<http://sec.ipa.go.jp/reports/20130430.html>
- ※ 3 クリエイティブコモンズ表示 - 継承 2.1 日本ライセンス
<http://creativecommons.org/licenses/by-sa/2.1/jp>
- ※ 4 「スタンドアロン型信頼性自己診断ツール」
<http://sec.ipa.go.jp/tool/dependability.html>