

ソフトウェア品質説明力強化に向けた実験
報告書

2013年2月



独立行政法人 情報処理推進機構
Information-technology Promotion Agency, Japan

更新履歴

日付	内容
2013.3.8	<p>以下の実験名を修正しました。</p> <p>実験 4</p> <p>旧：製品利用情報を分類する際に係るコスト評価 新：製品利用者情報を分類する際に係るコスト評価</p> <p>実験 12</p> <p>旧：JIS-X-25051（ISO/IEC25051）準拠レベルでのパッケージソフトウェア製品認定仮想実験 新：JIS-X-25051（ISO/IEC 25051）準拠レベルでのパッケージソフトウェア製品認証仮想実験</p>

はじめに

IPA/SEC では、ソフトウェア品質説明力を強化すべく様々な観点からの検討を実施してきました。本報告書はソフトウェア品質を説明するための手法等について具体的な実施方法、そのための作業量、実施にあたっての課題等を整理し、実際にソフトウェア品質を説明する際の参考とできるように行った実験結果をまとめたものです。

本実験は、「2011 年度 システムエンジニアリング実践拠点事業」として、次ページに記載の委託先にそれぞれの実験を委託し実施しました。

報告内容は 2012 年度時点の内容であり、掲載されている個々の情報に関しての著作権及び商標はそれぞれの権利者に帰属するものです。

「ソフトウェア品質説明力強化に向けた実験」

【報告書】

独立行政法人情報処理推進機構

Copyright© Information Technology Promotion Agency, Japan. All Rights Reserved 2013

表 1 委託先一覧

実験番号	実験テーマ名	委託先
1	IC カードを用いた社会情報基盤システムにおける、安全性とセキュリティの同時認証に関する実証実験	株式会社シーエーブイテクノロジーズ
2	既製システムを ISO 26262 に適合させる場合のセーフティケースの利用とその評価	株式会社ベリサーブ
3	独立検証機関による形式手法を用いた第三者検証のコスト評価	株式会社フォーマルテック
4	製品利用者情報を分類する際に係るコスト評価	キャッツ株式会社
5	車載システム開発時に使用するソフトウェアツールを ISO 26262 の要求事項に準拠させるための作業項目の抽出と考察	日本ノーベル株式会社
6	CO2無線測定センサーを対象とした監査レベル別コスト評価	一般社団法人 IT 検証産業協会
7	製品マニュアルと製品テスト結果のトレーサビリティ確保に係るコスト評価	キャッツ株式会社
8	トレーサビリティ確保におけるソフト開発データからの効果検証	東芝情報システム株式会社
9	カーナビゲーションシステムにおける利用品質（安全性）に対する監査内容の提案とコスト算出	株式会社ヴェス
10	ソフトウェア品質説明力の強化に伴い発生する開発工程負荷の評価・分析	株式会社ベリサーブ
11	モデルベース開発ツールを活用した際のコストの効果検証	東芝情報システム株式会社
12	JIS-X-25051 (ISO/IEC 25051) 準拠レベルでのパッケージソフトウェア製品認証仮想実験	一般社団法人コンピュータソフトウェア協会

目次

1. 実験の背景・目的	1
2. 事業概要	2
3. 報告書の構成	4
4. 実験結果	5
5. まとめ	9
6. 参考としたい情報、キーワードと各実験の対応	9

1. 実験の背景・目的

システムの大規模・複雑化やシステム同士の連携によるさらなる大規模システム化等によりシステムの品質の確保が大きな課題となっている。

システムの利用者の安全・安心のためには品質の確保とともに品質についての何らかの根拠ある説明が必須となっている状況である。またシステムを提供する側にとっても万一の場合、品質がどのように達成できているかについて客観性を担保しつつ説明できる状況にしておくことはますます重要となっている。

IPA/SEC ではシステムの機能を実現しているソフトウェアについてその品質説明力を強化することを目的に検討を重ねている。現在までに整理できているソフトウェア品質説明力強化のポイントを下記にまとめる。

1. 製品の品質が合理的に説明されていること

- ① 品質目標が妥当かつ明確であること
- ② 品質目標を達成するために何をしたらよいか(ロジック)が明確化されていること
- ③ ロジックを実施した証拠が存在すること
- ④ 品質目標、ロジック、証拠が相互にトレースできること

2. 製品が適切な基準を満たしていること

- ① 国際規格に適合していること
- ② その他の業界標準等一般に認められている基準に適合していること

3. 製品が適切な手法や管理に基づいて開発されていること

あるシステムの品質を漏れなく完全に説明するという事は現在のところ不可能と言っても過言ではない。したがって、品質とは何かを定義した上でその品質の達成度がどうであることを示すことが現実的である。ソフトウェアをよりよい製品にするためにソフトウェアの特性を考慮しながら工学的な取り組みが行われてきており、その成果は ISO を代表とするような技術標準としてまとめられている。品質を説明する場合もこのように一定の評価を得ている標準等をできるだけ活用していくことが根拠や客観性

を示すうえで有効である。

上記した品質説明力強化のポイントはこれまでの産業全体の取り組み、知見を参考に検討を加え品質を説明するとはどういうことかを現段階における合理的な考え方としてまとめたものである。それぞれを適切にあるいは適宜に実施することによりその対象とする範囲に対し一定の水準で品質を説明できるものと考えている。

今回の実験はこれらのソフトウェア品質を説明する方法について実証的な評価を実施することにより、各方法による説明の実施容易性の評価、工数等負荷の評価、有効とされている技術の評価、課題の抽出等を行い、今後のソフトウェア品質の説明力強化に資することを目的としている。

2. 事業概要

1. 実験の背景・目的でも述べたように対象となるソフトウェアに対し説明したいソフトウェア品質が定まっていることが前提となる。そのうえでどのような方法と根拠で説明していくかを選定し実験を実施することが必要となる。また選定した方法に関しどのような課題が想定され実施によりどのような結果が得られたかを明らかにできなければならない。実在するソフトウェアを対象としなければ実験たり得ないため、前述の趣旨を明確にして公募により複数の実験を採択することで、できるだけ多くのパターンが得られるよう考慮した。

表 2 に各実験テーマとその概要、説明する品質、実験目的、前述したソフトウェア品質説明力のポイントとの対応を一覧としてまとめた。ソフトウェア品質説明力のポイントとの対応部の●は強く関連、○は参考として関連していることを示す。

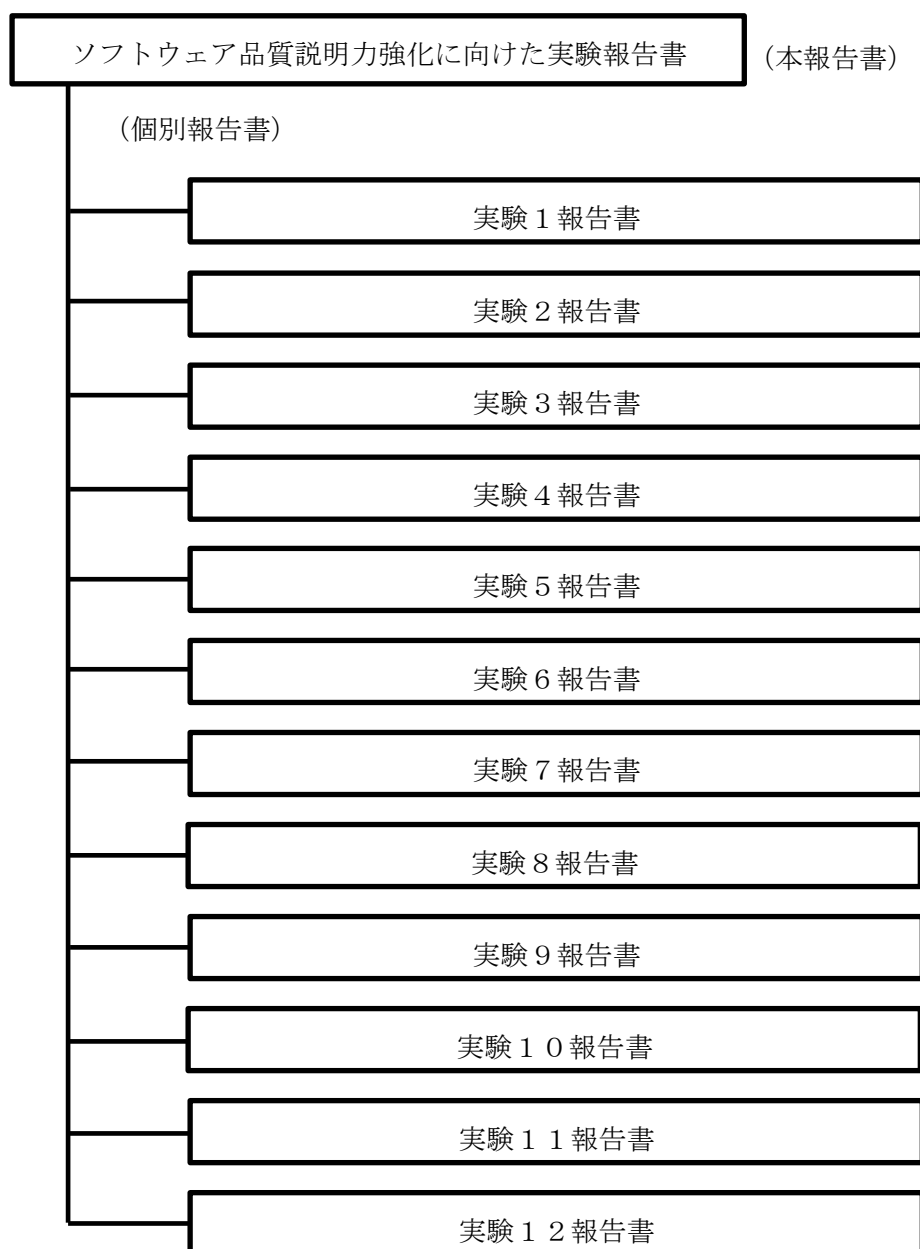
表 2 実験内容一覧

実験番号	実験テーマ名	委託先	概要	説明する品質	実験目的	3. 製品が適切な手法や管理に基づいて開発されていること				
						②その他の業界標準等一般に認められている基準に適合していること	①国際規格に適合していること	2. 製品が適切な基準を満たしていること	1. 製品の品質が合理的に説明されていること	
1	IC カードを用いた社会情報基盤システムにおける、安全性とセキュリティの同時認証に関する実証実験	株式会社シーエーブイテック/ロジック	機能安全とセキュリティ規格の同時認証を先進的な技術で実施。コスト削減効果を測定。	入退室管理システムの安全性とセキュリティ IEC61508 と Common Criteria	二種類の品質を別々に分析する場合に対するコスト削減効果	●	●	●	●	●
2	既製システムをISO26262に適合させる場合のセーフティケースの利用とその評価	株式会社ベリサーブ	ISO26262適合に必要な品質説明のためのエビデンス文書作成とコスト評価	自動車の集中ドアロックシステムの安全性 (ISO26262への適合性の証明)	既成システム (既に開発を完了している製品) を、後から ISO26262への適合性を証明するのに要するコスト	●	●	○	●	●
3	独立検証機関による形式手法を用いた第三者検証のコスト評価	株式会社フォーマルテック	配電自動化システムが安全性を満たしていることを、第三者による形式手法を用いた検証で確認。作業工数を計測し実施容易性を評価。	配電自動化システムの設計上の安全性	形式手法適用による安全性の保証。第三者による形式手法を用いた検証にかかる工数。	●	●	○	○	●
4	製品利用者情報を分類する際に係るコスト評価	キャッツ	製品やサービスの企画立案に用いられる利用者情報の収集や分類にかかるコスト評価。	POSシステム、AV家電システム、スマートフォンの利用品質 (利用者情報が活用されていること)	利用者情報の分類を手作業とツール使用により行った場合の工数差の測定、およびそれぞれのメリット・デメリットの整理	●	●			●
5	車載システム開発時に使用するソフトウェアツールをISO 26262の要求事項に準拠させるための作業項目の抽出と考察	日本ノーベル株式会社	車載システム開発で使用するツール (コンパイラ) についてISO26262の安全要求項目を満たすのに必要な作業の洗い出しと一般的なソフトウェア開発の品質確認項目と差分分析	車載システム開発で使用するツール (コンパイラ) の安全性 (ISO26262への適合性)	ISO26262に適合させるための品質作業項目抽出。および一般的なソフトウェア品質確認項目との差分分析。	●	●		●	
6	CO2無線測定センサーを対象とした監査レベル別コスト評価	一般社団法人 IT検証産業協会	複数社による一定の設計情報からのテストケース抽出と作業見積り。	CO2無線測定センサーの安全性	第三者による検証 (テスト) の実施容易性を判断するための複数社による実施データ (抽出テストケース、工数) 取得。	○	●	○		○
7	製品マニュアルと製品テスト結果のトレーサビリティ確保に係るコスト評価	キャッツ	マニュアル記載事項とテスト結果の間のトレーサビリティ確保に係るコスト評価	① 携帯オーディオプレーヤー ② POSシステムのテスト品質	専用ツールを使用する場合と手作業で行う場合の、トレーサビリティ管理 (トレーサ情報の作成と、利用の両面) に必要なコスト (工数)。				●	●
8	トレーサビリティ確保におけるソフト開発データからの効果検証	東芝情報システム株式会社	ツール導入による、トレーサビリティ確保に必要なコストの増加、減少効果の洗い出し	通信ソフトウェアについて適切な開発管理によって実現されていることの説明	トレーサビリティ管理を行うことによる開発コスト削減効果および不具合対応の工数削減				●	●
9	カーナビゲーションシステムにおける利用品質 (安全性) に対する監査内容の提案とコスト算出	株式会社ヴェス	カーナビの利用における安全性に焦点をあてた監査項目の抽出と監査実施にかかるコスト評価。	カーナビゲーションシステムの利用品質 (安全性)	審査項目と、その策定に要する工数並びにその基準に従った審査に必要な工数				○	●
10	ソフトウェア品質説明力の強化に伴い発生する開発工程負荷の評価・分析	株式会社ベリサーブ	ISO26262を想定しトレーサビリティ管理と設計段階のシミュレーションを導入した場合の工数を測定。	自動車の集中ドアロックシステムの安全性 (ISO26262)	モデルベース適用工数とそのフロントローディング効果による削減効果測定。トレーサビリティ管理コストと変更管理の削減効果測定。				○	●
11	モデルベース開発ツールを活用した際のコストの効果検証	東芝情報システム株式会社	モデルベース技術適用に際して増加や減少が見込まれるコストの洗い出し	半導体製造装置の高信頼性	モデルベース開発を行うことでの開発コスト削減効果					●
12	JIS-X-25051 (ISO/IEC25051) 準拠レベルでのパッケージソフトウェア製品認証仮想実験	一般社団法人コンピュータソフトウェア協会	パッケージソフトウェアの利用者文書において製品品質を説明するための仕組みづくりと審査の実施	パッケージソフトウェアの製品説明品質	審査基準の具体化 審査工数の把握				●	●

3. 報告書の構成

実験の概要を本報告書に「ソフトウェア品質説明力強化に向けた実験報告書」としてまとめている。

各実験の詳細は個別の報告書としてまとめている。



4. 実験結果

表 3 に各実験の結果、得られた成果を簡単にまとめた。また使用した代表的な手法・技法について記述している。

表 4 には実験により明らかとなり今後ソフトウェア品質説明力を強化していくために解決しなければならない課題および課題解決に向けた提案、その他提案について簡単にまとめた。

表 5 には各実験結果がどのような場面で参考とできるか代表的な例を記述した。

表 3 実験結果・成果

実験番号	実験テーマ名	概要	説明する品質	手法・技術	実験目的	実験結果・成果				
						●	○	●	○	
						3. 製品が適切な手法や管理に基づいて開発されていること ②その他の業界標準等一般に認められている基準に適合していること ①国際規格に適合していること 2. 製品が適切な基準を満たしていること ④品質目標、ロジック、証拠が相互にトレースできること ③ロジックを実施した証拠が存在すること ②品質目標を達成するために何をしたらよいか(ロジック)が明確化されていること ①品質目標が妥当かつ明確であること 1. 製品の品質が合理的に説明されていること				
1	IC カードを用いた社会情報基盤システムにおける、安全性とセキュリティの同時認証に関する実証実験	機能安全とセキュリティ規格の同時認証を先進的な技術で実施。コスト削減効果を測定。	入退室管理システムの安全性とセキュリティ IEC61508 と Common Criteria	SafSec (Safeecをベースとした安全性、セキュリティの同時分析手法)	二種類の品質を別々に分析する場合に対するコスト削減効果	●	●	●	●	●
2	既製システムをISO26262に適合させるためのセーフティケースの利用とその評価	ISO26262適合に必要な品質説明のためのエビデンス文書作成とコスト評価	自動車の集中ドアロックシステムの安全性 (ISO26262への適合性の証明)	GSNIによるセーフティケースの作成	既成システム(既に開発を完了している製品)を、後からISO26262への適合性を証明するのに要するコスト	●	●	○	●	●
3	独立検証機関による形式手法を用いた第三者検証のコスト評価	配電自動化システムが安全性を満たしていることを、第三者による形式手法を用いた検証で確認。作業工数を計測し実施容易性を評価。	配電自動化システムの設計上の安全性	形式手法 (準形式手法: モデル検査 [NuSMV])	形式手法適用による安全性の保証。第三者による形式手法を用いた検証にかかる工数。	●	●	○	○	●
4	製品利用者情報を分類する際に係るコスト評価	製品やサービスの企画立案に用いられる利用者情報の収集や分類にかかるコスト評価。	POSシステム、AV家電システム、スマートフォンの利用品質 (利用者情報が活用されていること)	製品利用情報の分類 (テキスト分類ツール)	利用者情報の分類を手作業とツール使用により行った場合の工数差の測定。およびそれぞれのメリット・デメリットが大幅に減少してしまう。	●	●	●	●	●
5	車載システム開発時に使用するソフトウェアツールをISO 26262の要求事項に準拠させるための作業項目の抽出と考察	車載システム開発で使用するツール(コンパイラ)についてISO26262の安全要求項目を満たすのに必要な作業の洗い出しと一般的なソフトウェア開発の品質確認項目と差分分析	車載システム開発で使用するツール(コンパイラ)の安全性 (ISO26262への適合性)	ISO26262 Automotive SPIICE	ISO26262に適合させるための品質作業項目抽出。および一般的なソフトウェア品質確認項目との差分分析。	●	●	●	●	●
6	CO2無線測定センサーを対象とした監査レベル別コスト評価	複数社による一定の設計情報からのテストケース抽出と作業見積り。	CO2無線測定センサーの安全性	業界団体で作成した作業標準	第三者による検証(テスト)の実施容易性を判断するための複数社による実施データ(抽出テストケース、工数)取得。	○	●	○		○
7	製品マニュアルと製品テスト結果のトレーサビリティ確保に係るコスト評価	マニュアル記載事項とテスト結果の間のトレーサビリティ確保に係るコスト評価	① 携帯オーディオプレーヤー ② POSシステムのテスト品質	トレーサビリティ管理 (手作業と、ツール: TERAS TRAを使用した場合)	専用ツールを使用する場合と手作業で行う場合の、トレーサビリティ管理(トレーサビリティ情報の作成と、利用の両面)に必要なコスト(工数)。	●			●	●
8	トレーサビリティ確保におけるソフト開発データからの効果検証	ツール導入による、トレーサビリティ確保に必要なコストの増加、減少効果の洗い出し	通信ソフトウェアについて適切な開発管理によって実現されていることの説明	トレーサビリティ管理	トレーサビリティ管理を行うことによる開発コスト削減効果 および不具合対応の工数削減	●			●	●
9	カーナビゲーションシステムにおける利用品質(安全性)に対する監査内容の提案とコスト算出	カーナビの利用における安全性に焦点をあてた監査項目の抽出と監査実施にかかるコスト評価。	カーナビゲーションシステムの利用品質(安全性)	既存の安全基準「画像表示装置の取り扱いについて 改訂第3.0版」一般社団法人日本自動車工業会	審査項目と、その策定に要する工数並びにその基準に従った審査に必要な工数				○	●
10	ソフトウェア品質説明力の強化に伴い発生する開発工程負荷の評価・分析	ISO26262を想定しトレーサビリティ管理と設計段階のシミュレーションを導入した場合の工数を測定。	自動車の集中ドアロックシステムの安全性 (ISO26262)	● モデルベース開発 (OpenModelica) のシミュレーション ● トレーサビリティ管理 (TERAS)	モデルベース適用工数とそのフロントローディング効果による削減効果測定。トレーサビリティ管理コストと変更管理の削減効果測定。				○	●
11	モデルベース開発ツールを活用した際のコストの効果検証	モデルベース技術適用に際して増加や減少が見込まれるコストの洗い出し	半導体製造装置の高信頼性	モデルベース開発 MATLAB/Simulink	モデルベース開発を行うことでの開発コスト削減効果					●
12	JIS-X-25051 (ISO/IEC25051) 準拠レベルでのパッケージソフトウェア製品認証依頼実験	パッケージソフトウェアの利用者文書において製品品質を説明するための仕組みづくりと審査の実施	パッケージソフトウェアの製品説明品質	JIS-X-25051 (ISO/IEC25051) パッケージソフトウェア品質 (PSQ) 認証制度	審査基準の具体化 審査工数の把握	●			●	●

表 4 実験から得られた課題・提案

実験番号	実験テーマ名	概要	説明する品質	手法・技術	実験目的	実験結果から得られた課題・提案															
						1. 製品の品質が合理的に説明されていること	2. 製品が適切な基準を満たしていること	3. 製品が適切な手法や管理に基づいて開発されていること	4	5	6	7	8	9	10	11	12				
						<p>3. 製品が適切な手法や管理に基づいて開発されていること</p> <p>②その他の業界標準等一般に認められている基準に適合していること</p> <p>①国際規格に適合していること</p> <p>2. 製品が適切な基準を満たしていること</p> <p>④品質目標、ロジック、証拠が相互にトレースできること</p> <p>③ロジックを実施した証拠が存在すること</p> <p>②品質目標を達成するために何をしたらよいか(ロジック)が明確化されていること</p> <p>①品質目標が妥当かつ明確であること</p> <p>1. 製品の品質が合理的に説明されていること</p>															
1	IC カードを用いた社会情報基盤システムにおける、安全性とセキュリティの同時認証に関する実証実験	機能安全とセキュリティ規格の同時認証を先進的な技術で実施。コスト削減効果を測定。	入退室管理システムの安全性とセキュリティ IEC61508 と Common Criteria	SafSec (Safsecをベースとした安全性、セキュリティの同時分析手法)	二種類の品質を別々に分析する場合に対するコスト削減効果	今回実施したリスク分析以外の特に下記の実証が必要。 1) ディベンダビリティ仕様分析、獲得 2) ディベンダビリティ仕様ロスに対して十分対抗していることの議論の構築 3) システムモジュールと、妥当性の議論モジュールとの連携 4) 安全性とセキュリティの認証に関するディベンダビリティケース	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
2	既製システムをISO26262に適合させる場合のセーフティケースの利用とその評価	ISO26262適合に必要な品質説明のためのエビデンス文書作成とコスト評価	自動車集中ドアロックシステムの安全性 (ISO26262への適合性の証明)	GSNIによるセーフティケースの作成	既成システム(既に開発を完了している製品)を、後からISO26262への適合性を証明するのに要するコスト	モデルベース開発仕様書の活用 ・マネジメントプロセスの確立	●	●	○	●	●	●	●	●	●	●	●	●	●	●	
3	独立検証機関による形式手法を用いた第三者検証のコスト評価	配電自動化システムが安全性を満たしていることを、第三者による形式手法を用いた検証で確認。作業工数を計測し実施容易性を評価。	配電自動化システムの設計上の安全性	形式手法 (準形式手法: モデル検査 [NuSMV])	形式手法適用による安全性の保証。第三者による形式手法を用いた検証にかかる工数。	実際の検証作業に入るための準備段階(対象のシステム、設計書の理解や設計情報の吸い上げ等)に多くの工数を要する。特に第三者が検証を実施する場合、検証対象の設計情報を適切に用意しておくことが重要であり、検証実施者においては対象の理解、検証への入力となる設計情報の整理・吸い上げ等の高い能力が求められる。	●	●	○	○	●	●	●	●	●	●	●	●	●	●	
4	製品利用者情報を分類する際に係るコスト評価	製品やサービスの企画立案に用いられる利用者情報の収集や分類にかかるコスト評価。	POSシステム、AV家電システム、スマートフォンの利用品質(利用者情報が活用されていること)	製品利用情報の分類(テキスト分類ツール)	利用者情報の分類を手作業とツール使用により行った場合の工数差の測定、およびそれぞれのメリット・デメリットの整理	利用者情報を効率よく分類するためには手作業、ツール利用にかかわらず入力情報を分類方式に合わせた整理を行う必要がある。ツールを使用する際のコストを正確に知るためには、分類精度向上や辞書の管理などツールのメンテナンスに要するコストなどを評価する必要がある。	●	●	●	●	●	●	●	●	●	●	●	●	●	●	
5	車載システム開発時に使用するソフトウェアツールをISO 26262の要求事項に準拠させるための作業項目の抽出と考察	車載システム開発で使用するツール(コンパイラ)についてISO26262の安全要求項目を満たすのに必要な作業の洗い出しと一般的なソフトウェア開発の品質確認項目と差分分析	車載システム開発で使用するツール(コンパイラ)の安全性 (ISO26262への適合性)	ISO26262 Automotive SPICE	ISO26262に適合させるための品質作業項目抽出。 および一般的なソフトウェア品質確認項目との差分分析。	規格認定作業を支援するためのガイドラインや支援ツールが整備されていない。 監査レベルによっては対応コストが許容コストを超過する場合もある。その場合の現実的な解(業界での考え方の含意等含む)が必要。	●	●	●	●	●	●	●	●	●	●	●	●	●	●	
6	CO2無線測定センサーを対象とした監査レベル別コスト評価	複数社による一定の設計情報からのテストケース抽出と作業見積り。	CO2無線測定センサーの安全性	業界団体で作成した作業標準	第三者による検証(テスト)の実施容易性を判断するための複数社による実施データ(抽出テストケース、工数)取得。	バラつきを抑えられる、適切な検証基準の標準化の必要性	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○
7	製品マニュアルと製品テスト結果のトレーサビリティ確保に係るコスト評価	マニュアル記載事項とテスト結果の間のトレーサビリティ確保に係るコスト評価	① 携帯オーディオプレーヤー ② POSシステム のテスト品質	トレーサビリティ管理 (手作業と、ツール: TERAS TRA を使用した場合)	専用ツールを使用する場合と手作業で行う場合の、トレーサビリティ管理(トレーサビリティ情報の作成と、利用の両面)に必要なコスト(工数)。	ツールを選択する場合は、トレーサビリティ情報の編集機能(TERAS TRAではリンクエディタと呼称)の機能が重要である。	●	●	●	●	●	●	●	●	●	●	●	●	●	●	
8	トレーサビリティ確保におけるソフト開発データからの効果検証	ツール導入による、トレーサビリティ確保に必要なコストの増加、減少効果の洗い出し	通信ソフトウェアについて適切な開発管理によって実現されていることの説明	トレーサビリティ管理	トレーサビリティ管理を行うことによる開発コスト削減効果 および不具合対応の工数削減	トレーサビリティ管理の有効性を向上させるためには対象ドキュメント等の体系を統一することが望ましい。	●	●	●	●	●	●	●	●	●	●	●	●	●	●	
9	カーナビゲーションシステムにおける利用品質(安全性)に対する監査内容の提案とコスト算出	カーナビの利用における安全性に焦点をあてた監査項目の抽出と監査実施にかかるコスト評価。	カーナビゲーションシステムの利用品質(安全性)	既存の安全基準「画像表示装置の取り扱いはについて」改訂第3.0版)一般社団法人日本自動車工業会	審査項目と、その策定に要する工数並にその基準に従った審査に必要な工数	審査項目のまとめ方において、審査を実施する手順を考慮したグルーピングなどを行うことで審査コスト削減をはかれる。 業界依存な項目と非依存な項目を分けてまとめることで審査項目のメンテナンス効率を上げることができる。	○	●	○	○	○	○	○	○	○	○	○	○	○	○	
10	ソフトウェア品質説明力の強化に伴い発生する開発工程負荷の評価・分析	ISO26262を想定しトレーサビリティ管理と設計段階のシミュレーションを導入した場合の工数を測定。	自動車集中ドアロックシステムの安全性 (ISO26262)	・モデルベース開発 (OpenModelica)のシミュレーション ・トレーサビリティ管理 (TERAS)	モデルベース適用工数とそのフロントローディング効果による削減効果測定。 トレーサビリティ管理コストと変更管理の削減効果測定。	モデルベース開発(シミュレーション)はシミュレーションを反復しながら開発するようなプロジェクトに適する。 プロジェクトによっては、導入コストが効果を上回る可能性があるのが注意が必要。 トレーサビリティ管理は、管理方針を事前に定める必要がある。	○	●	○	○	○	○	○	○	○	○	○	○	○	○	
11	モデルベース開発ツールを活用した際のコストの効果検証	モデルベース技術適用に際して増加や減少が見込まれるコストの洗い出し	半導体製造装置の高信頼性	モデルベース開発 MATLAB/Simulink	モデルベース開発を行うことでの開発コスト削減効果	モデルベース開発の有効性は認められた為適用範囲を拡大することにより、工数削減効果や品質向上が期待できる。	●	●	●	●	●	●	●	●	●	●	●	●	●	●	
12	JIS-X-25051 (ISO/IEC25051)準拠レベルでのパッケージソフトウェア製品認証仮想実験	パッケージソフトウェアの利用者文書において製品品質を説明するための仕組みづくりと審査の実施	パッケージソフトウェアの製品説明品質	JIS-X-25051 (ISO/IEC25051) パッケージソフトウェア品質(PSQ) 認証制度	審査基準の具体化 審査工数の把握	費用対効果を勘案した制度、審査の必要性	●	●	●	●	●	●	●	●	●	●	●	●	●	●	

表 5 実験結果の利活用場面

実験番号	実験テーマ名	概要	説明する品質	手法・技術	実験結果の利活用場面								
					1.製品の品質が合理的に説明されていること	2.製品が適切な基準を満たしていること	3.製品が適切な手法や管理に基づいて開発されていること	4.品質目標、ロジック、証拠が相互にトレースできること	5.品質目標を達成するために何をしたらよいか(ロジック)が明確化されていること	6.国際規格に適合していること	7.国際規格に適合していること	8.国際規格に適合していること	9.国際規格に適合していること
1	ICカードを用いた社会情報基盤システムにおける、安全性とセキュリティの同時認証に関する実証実験	機能安全とセキュリティ規格の同時認証を先進的な技術で実施。コスト削減効果測定。	入退室管理システムの安全性とセキュリティ IEC61508 と Common Criteria	SafSec (Safsecをベースとした安全性、セキュリティの同時解析手法)	複数の規格についての検証を同時に実施する場合の効率よい実施方法を知りたい。 ・FTAやFMEAなどのリスク分析、ハザード分析の実例を知りたい。	●	●	●	●	●	●	●	●
2	既製システムをISO26262に適合させる場合のセーフティケースの利用とその評価	ISO26262適合に必要な品質説明のためのエビデンス文書作成とコスト評価	自動車集約ロックシステムの安全性 (ISO26262への適合性の証明)	GSNIによるセーフティケースの作成	既に開発を完了している製品を認証する場合の手段やコストの目安を知りたい。 客観的な証明手段としてのセーフティケースの作成の例を知りたい。	●	●	○	●	●	●	●	●
3	独立検証機関による形式手法を用いた第三者検証のコスト評価	配電自動化システムが安全性を満たしていることを、第三者による形式手法を用いた検証で確認。作業工数を計測し実施容易性を評価。	配電自動化システムの設計上の安全性	形式手法 (準形式手法: モデル検査[NuSMV])	形式手法を用いた検証について作業項目と工数の目安を得たい。 ・モデル検査に要するコストの目安やその内訳の参考資料が欲しい場合に、本実験の作業別工数が見える。 ・モデル検査の概要を知りたい場合に、本実験の作業の構成を参考資料として使うことができる。	●	●	○	○	●	●	●	●
4	製品利用者情報を分類する際に係るコスト評価	製品やサービスの企画立案に用いられる利用者情報の収集や分類にかかるコスト評価。	POSシステム、AV家電システム、スマートフォンの利用品質 (利用者情報が活用されていること)	製品利用情報の分類 (テキスト分類ツール)	利用者情報を製品品質向上へ活用することを検討している場合、その作業例、本実験の手順 (作業の組み立て)、コストを知りたい。 テキスト分類ツールを使用した利用者情報の分類作業の例を知りたい。	●	●	●	●	●	●	●	●
5	車載システム開発時に使用するソフトウェアツール名ISO 26262の要求事項に準拠させるための作業項目の抽出と考察	車載システム開発で使用するツール (コンパイラ) についてISO26262の安全要求項目を満たすのに必要な作業の洗い出しと一般的なソフトウェア開発の品質確認項目と差分分析	車載システム開発で使用するツール (コンパイラ) の安全性 (ISO26262への適合性)	ISO26262 Automotive SPICE	・開発するソフトウェアをISO26262に対応させたい。 ・安全に関する検証項目はどのようなものか知りたい。	●	●	●	●	●	●	●	●
6	CO2無線測定センサーを対象とした監査レベル別コスト評価	複数社による一定の設計情報からのテストケース抽出と作業見積もり。	CO2無線測定センサーの安全性	業界団体で作成した作業標準	第三者検証 (テスト) を活用する場合に考慮しておくべき事項を知りたい。 具体的には、依頼する企業による抽出テストケース数、作業工数のバラつきの可能性。およびそれを抑制するヒントを知りたい。	○	●	○	○	○	○	○	○
7	製品マニュアルと製品テスト結果のトレーサビリティ確保に係るコスト評価	マニュアル記載事項とテスト結果の間のトレーサビリティ確保に係るコスト評価	① 携帯オーディオプレーヤー ② POSシステム のテスト品質	トレーサビリティ管理 (手作業と、ツール: TERAS TRAを使用した場合)	トレーサビリティ管理の導入事例を知りたい。 トレーサビリティ管理の実際の構成例と、それに要するコストの増加に影響を与える要因などを知りたい。 ツールを使わない場合のトレーサビリティ管理の方法を知りたい。	●	●	●	●	●	●	●	●
8	トレーサビリティ確保におけるソフト開発データからの効果検証	ツール導入による、トレーサビリティ確保に必要なコストの増加、減少効果の洗い出し	通信ソフトウェアについて適切な開発管理によって実現されていることの説明	トレーサビリティ管理	トレーサビリティ管理による効果を知りたい。 トレーサビリティ管理により開発時の不具合を減らしたい。	●	●	●	●	●	●	●	●
9	カーナビゲーションシステムにおける利用品質 (安全性) に対する監査内容の提案とコスト算出	カーナビの利用における安全性に焦点をあてた監査項目の抽出と監査実施にかかるコスト評価。	カーナビゲーションシステムの利用品質 (安全性)	既存の安全基準 「画像表示装置の取り扱いについて改訂第3.0版」一般社団法人日本自動車工業会	審査項目をどのように作れば良いか知りたい。 その策定の手順や、策定要するコスト、審査実施に要するコスト (の見積もり) の参考情報を知りたい。	○	●	○	○	○	○	○	○
10	ソフトウェア品質説明力の強化に伴い発生する開発工程負荷の評価・分析	ISO26262を想定しトレーサビリティ管理と設計段階のシミュレーションを導入した場合の工数を測定。	自動車集約ロックシステムの安全性 (ISO26262)	・モデルベース開発 (OpenModelica) のシミュレーション ・トレーサビリティ管理 (TERAS)	モデルベース・シミュレーションを組み込んだ開発プロセスをどう構成するかの事例・概要を知りたい。 トレーサビリティ管理の導入例、概要を知りたい。	○	○	○	○	○	○	○	○
11	モデルベース開発ツールを活用した際のコストの効果検証	モデルベース技術適用に際して増加や減少が見込まれるコストの洗い出し	半導体製造装置の高信頼性	モデルベース開発 MATLAB/ Simulink	モデルベース開発を導入するにあたりモデルベース開発の効果を示す定量的な情報が欲しい。	●	●	●	●	●	●	●	●
12	JIS-X-25051 (ISO/IEC25051) 準拠レベルでのパッケージソフトウェア製品認証仮想実験	パッケージソフトウェアの利用者文書において製品品質を説明するための仕組みづくりと審査の実施	パッケージソフトウェアの製品説明品質	JIS-X-25051 (ISO/IEC25051) パッケージソフトウェア品質 (PSQ) 認証制度	・国際規格に準拠した認証制度の設計をしたい。 ・認証にかかわる審査の工数を事例として知りたい。	●	●	●	●	●	●	●	●

5. まとめ

今回の実験はソフトウェア品質を説明するにあたり様々な説明したい品質、説明のための手法・技法を実施した場合の工数負荷、その他課題等を広く収集する目的で実施した。ごく短い期間（各 3 か月程度）で実施したこともあり全体として更に分析・検証が必要とされる部分もあるが所期の目的は一定レベルで達せられたと評価している。各報告にある詳細部のデータ、手法・技法については実験というかたちで収集できたものであり実用度も高いものとなっている。

IPA/SEC ではこのような評価データ等も有効に活用しつつ、ソフトウェア品質説明力の強化に向けた基盤整備などの取り組みを継続する。

6. 参考としたい情報、キーワードと各実験の対応

【表 5 の「実験結果の利活用場面」から参考とできる実験との対応を下記にまとめる。】

「複数の規格についての検証を同時に実施する場合の効率よい実施方法を知りたい。」

「FTA や FMEA などのリスク分析、ハザード分析の実例を知りたい。」

実験 1：IC カードを用いた社会情報基盤システムにおける、安全性とセキュリティの同時認証に関する実証実験

「既に開発を完了している製品を認証する場合の手段やコストの目安を知りたい。」

「客観的な証明手段としてのセーフティケースの作成の例を知りたい。」

実験 2：既製システムを ISO 26262 に適合させる場合のセーフティケースの利用とその評価

「形式手法を用いた検証について作業項目と工数の目安を得たい。」

「モデル検査に要するコストの目安やその内訳の参考資料が欲しい。」

実験 3：独立検証機関による形式手法を用いた第三者検証のコスト評価

「利用者情報を製品品質向上へ活用することを検討している場合、その作業例、本実験の手順（作業の組み立て）、コストを知りたい。」

「テキスト分類ツールを使用した利用者情報の分類作業の例を知りたい。」

実験 4：製品利用者情報を分類する際に係るコスト評価

「開発するソフトウェアを ISO 26262 に対応させたい。」

「安全に関する検証項目とはどのようなものか知りたい。」

実験 5：車載システム開発時に使用するソフトウェアツールを ISO 26262 の要求事項に準拠させるための作業項目の抽出と考察

「第三者検証（テスト）を活用する場合に考慮しておくべき事項を知りたい。」

「第三者検証を依頼する企業による抽出テストケース数、作業工数のバラツキの可能性。およびそれを抑制するヒントを知りたい。」

実験 6：CO₂無線測定センサーを対象とした監査レベル別コスト評価

「トレーサビリティ管理の導入事例を知りたい。」

「トレーサビリティ管理の実際の構成例と、それに要するコストの増加に影響を与える要因などを知りたい。」

「ツールを使わない場合のトレーサビリティ管理の方法を知りたい。」

実験 7：製品マニュアルと製品テスト結果のトレーサビリティ確保に係るコスト評価

「トレーサビリティ管理による効果を知りたい。」

「トレーサビリティ管理により開発時の不具合を減らしたい。」

実験 8：トレーサビリティ確保におけるソフト開発データからの効果検証

「審査項目をどのように作れば良いか知りたい。」

「審査項目の策定の手順や、策定要するコスト、審査実施に要するコスト（の見積もり）の参考情報を知りたい。」

実験 9：カーナビゲーションシステムにおける利用品質（安全性）に対する監査内容の提案とコスト算出

「モデルベース・シミュレーションを組み込んだ開発プロセスをどう構成するかの事例・概要を知りたい。」

「トレーサビリティ管理の導入例、概要を知りたい。」

実験 10：ソフトウェア品質説明力の強化に伴い発生する開発工程負荷の評価・分析

「モデルベース開発を導入するにあたりモデルベース開発の効果を示す定量的な情報が欲しい。」

実験 11：モデルベース開発ツールを活用した際のコストの効果検証

「国際規格に準拠した認証制度の設計をしたい。」

「認証にかかわる審査の工数を事例として知りたい。」

実験 12：JIS-X-25051（ISO/IEC 25051）準拠レベルでのパッケージソフトウェア製品認証仮想実験

【キーワードから参考とできる実験との対応を下記にまとめる】

「複数規格の同時検証」

実験 1：IC カードを用いた社会情報基盤システムにおける、安全性とセキュリティの同時認証に関する実証実験

「Safsec」

実験 1：IC カードを用いた社会情報基盤システムにおける、安全性とセキュリティの同時認証に関する実証実験

「FTA」

実験 1：IC カードを用いた社会情報基盤システムにおける、安全性とセキュリティの同時認証に関する実証実験

「FMEA」

実験 1：IC カードを用いた社会情報基盤システムにおける、安全性とセキュリティの同時認証に関する実証実験

「GSN」

実験 2：既製システムを ISO 26262 に適合させる場合のセーフティケースの利用とその評価

「(準)形式手法、モデル検査 (工数)」

実験 3：独立検証機関による形式手法を用いた第三者検証のコスト評価

「利用者情報」

実験 4：製品利用者情報を分類する際に係るコスト評価

「テキスト分類ツール」

実験 4：製品利用者情報を分類する際に係るコスト評価

「クレームポートフォリオツール」

実験 4：製品利用者情報を分類する際に係るコスト評価

「Automotive SPICE」

実験 5：車載システム開発時に使用するソフトウェアツールを ISO 26262 の要求事項に準拠させるための作業項目の抽出と考察

「トレーサビリティ」

実験 7：製品マニュアルと製品テスト結果のトレーサビリティ確保に係るコスト評価

実験 8：トレーサビリティ確保におけるソフト開発データからの効果検証

実験 10：ソフトウェア品質説明力の強化に伴い発生する開発工程負荷の評価・分析

「TERAS TRA」

実験 7：製品マニュアルと製品テスト結果のトレーサビリティ確保に係るコスト評価

「不具合情報管理」

実験 8：トレーサビリティ確保におけるソフト開発データからの効果検証

「“画像表示装置の取り扱いについて 改訂第 3.0 版” 一般社団法人日本自動車工業会」

実験 9：カーナビゲーションシステムにおける利用品質（安全性）に対する監査内容の提案とコスト算出

「リスク分析」

実験 9：カーナビゲーションシステムにおける利用品質（安全性）に対する監査内容の提案とコスト算出

「モデルベース開発」

実験 10：ソフトウェア品質説明力の強化に伴い発生する開発工程負荷の評価・分析

実験 11：モデルベース開発ツールを活用した際のコストの効果検証

「MATLAB/Simulink」

実験 11：モデルベース開発ツールを活用した際のコストの効果検証

「パッケージソフトウェア品質(PSQ)認証制度」

実験 12：JIS-X-25051（ISO/IEC 25051）準拠レベルでのパッケージソフトウェア製品認証仮想実験

「第三者検証」

実験 3：独立検証機関による形式手法を用いた第三者検証のコスト評価

実験 6：CO₂無線測定センサーを対象とした監査レベル別コスト評価

「ISO 9126」

実験 9：カーナビゲーションシステムにおける利用品質（安全性）に対する監査内容の提案とコスト算出

「IEC 61508」

実験 3：独立検証機関による形式手法を用いた第三者検証のコスト評価

「ISO 26262」

実験 2：既製システムを ISO 26262 に適合させる場合のセーフティケースの利用とその評価

実験 5：車載システム開発時に使用するソフトウェアツールを ISO 26262 の要求事項に準拠させるための作業項目の抽出と考察

実験 9：カーナビゲーションシステムにおける利用品質（安全性）に対する監査内容の提案とコスト算出

実験 10：ソフトウェア品質説明力の強化に伴い発生する開発工程負荷の評価・分析

「JIS-X-25051 (ISO/IEC 25051)」

実験 12 : JIS-X-25051 (ISO/IEC 25051) 準拠レベルでのパッケージソフトウェア製品認証仮想実験