

「組込みシステムの第三者検証に関する調査」
調査報告書

2012年3月15日

はじめに

IPA/SEC では、「国内産業の第三者検証に対する要求」「海外における第三者検証の現状」「第三者検証に関わる国際規格」等の調査を実施し、結果を報告書としてとりまとめました。

本調査は、「2010 年度 システムエンジニアリング実践拠点事業」として、ガートナー・ジャパン株式会社に委託し実施しました。

報告内容は 2010 年度時点の内容であり、掲載されている個々の情報に関する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。

組込みシステムの第三者検証に関する調査
【調査報告書】

独立行政法人情報処理推進機構

Copyright© Information-Technology Promotion Agency, Japan. All Rights Reserved 2012

1. 背景.....	4
2. 調査結果	5
2.1. 調査スコープについて	5
2.2. 第三者機関に求められる独立性・中立性.....	5
2.3. 第三者検証の現状（航空機業界）	6
2.3.1. 概要	6
2.3.2. 法律・法令.....	6
2.3.3. 認定機関（認証機関を認定する機関）	7
2.3.4. 認証機関	8
2.3.5. 認証サービス企業.....	9
2.3.6. 国際規格について.....	11
2.3.7. アメリカ連邦航空局（FAA）の DER 制度について.....	12
2.3.8. 日本における型式証明の手続き（参考）	19
2.3.9. 相互認証（参考）	20
2.3.10. 第三者検証のユーザ	21
2.4. 第三者検証の現状（医療機器業界）	22
2.4.1. 概要	22
2.4.2. 法律・法令.....	22
2.4.3. 認定機関（認証機関を認定する機関）	24
2.4.4. 認証機関	25
2.4.5. 国際規格	26
2.4.6. 第三者検証の方法.....	27
2.5. ソフトウェア品質監査制度(仮称)に参考となる公認会計士制度について.....	33
2.5.1. 専門性と独立性	33
2.5.2. 監査法人	34
2.5.3. 会計基準と監査基準.....	35
2.5.4. 公認会計士協会	36
2.5.5. 公認会計士認定制度.....	37
2.5.6. 監査方法とリスクの関係.....	38
2.6. 海外企業、大学へのインタビュー.....	40
2.6.1. HighRely.....	40
2.6.2. Safeware Engineering Corporation.....	42
2.6.3. Boston Atlantic Technology,INC./Software Quality Consulting,Inc.	43
2.6.4. Massachusetts 工科大学.....	44
2.6.5. NTS Inc.	45
2.7. 第三者検証取り組み状況調査.....	46
2.7.1. 第三者検証取り組み状況に関するアンケート項目	46
2.7.2. アンケート調査結果.....	47
3. 調査結果まとめ.....	53
3.1. 第三者検証の現状について.....	53
3.2. アンケート調査について	53

1. 背景

これまで組込みシステム製品の信頼性・安全性は、企業独自の品質管理により確保されてきた。一方、組込みシステムの高機能化・高性能化により、これらを実現するための技術が高度化・複雑化し、組込みソフトウェアで実現される領域は飛躍的に拡大した。この変化に伴い、組込みシステム製品の信頼性・安全性を確保する考え方や担保する考え方にも変化が現れてきている。

世界における組込みシステム製品の信頼性・安全性に対する考え方は、欧州では従来と同様に国際標準化と国際標準に基づく認証を軸とした考え方である。一方、米国では国際標準に加えてそれらでカバーされない領域についても第三者による検証が求められるようになってきている。さらに中国では、第三者による検証を可能とするためのソースコードの開示義務等に見られるように、欧米とは異なる考え方での仕組みづくりを目指していると考えられる。

我が国の組込みシステム産業はこのような状況の中、欧州が求める国際標準に基づく認証取得については対応できているものの、米国が求める第三者による検証については、国内の第三者検証に係る産業が未成熟であるため、迅速・的確な対応が困難な状況になっており、米国さらには中国市場におけるわが国組込みシステム製品の競争力低下や市場参入の機会損失等が懸念される状況にあると考えられる。

本調査は米国・中国等海外諸国から認知される形で国内に第三者検証産業を構築し、わが国組込み産業の国際競争力の低下を防止し、維持・強化していくことを目的に、「国内産業の第三者検証に対する要求」「海外における第三者検証の現状」「第三者検証に関わる国際規格」等を調査・分析するものである。

2. 調査結果

2.1. 調査スコープについて

調査対象業界として、第三者検証の仕組みがあり、第三者検証事業を行う企業、市場が存在する航空機業界と医療機器業界に注目し調査を実施した。

また、第三者検証の仕組みの参考として、公認会計士の制度に着目した。

2.2. 第三者機関に求められる独立性・中立性

第三者検証機関の要件を考える場合、独立性と中立性が重要な案件となる。以下はそれを示す例である。

・ ISO/IEC 17021:2006. Conformity assessment – Requirements for bodies providing audit and certification of management systems

適合性評価-マネジメントシステムの審査及び認証を提供する機関に対する要求事項では、公平性についての記述がある。

・ 公認会計士法では、公認会計士の独立性、公平性、専門性について定義している。

(公認会計士の使命)

第一条 公認会計士は、監査及び会計の専門家として、独立した立場において、財務書類その他の財務に関する情報の信頼性を確保することにより、会社等の公正な事業活動、投資者及び債権者の保護を図り、もって国民経済の健全な発展に寄与することを使命とする。

公認会計士法抜粋

・ 公益社団法人 日本適合性認定協会は、2009年8月にマネジメントシステム規格認証制度の信頼性確保に向けたアクションプランを公表した。「MS 信頼性ガイドライン対応委員会報告書」において、マネジメントシステム規格認証機関の信頼性・独立性・公平性等の評価・比較に資する情報として19項目が定めている。

(<http://www.jab.or.jp/news/2009/09081800.html> 「MS 信頼性ガイドライン対応委員会 報告書」 「資料3 認証機関の情報公開」 参照)

2.3. 第三者検証の現状（航空機業界）

2.3.1. 概要

航空機業界における第三者検証に関連する事項を米国、欧州、日本で比較した。

表 2-1 航空機業界の第三者検証への対応比較(米・欧・日)

対象業界		航空業界		
対象地域		米国	欧州	日本
対象製品		航空機、サブシステム、部品		
法律・法令		14 CFR part 21	EASA Part 21	航空法
第三者検証組織・企業	認定機関 (Notifying Authority) 認証機関(certifying body)	FAA(Federal Aviation Administration: 連邦航空局)	EASA(European Aviation Safety Agency: 欧州航空安全局)	JCAB(Japan Civil Aviation Bureau: 国土交通省航空局)
	公認-認証機関 (Notified Body)、認証者	Company DER、Consultant DER	—	—
	認証サービス企業、ツールベンダ	HighRely、Paragon Transportation、Certification Services等	Esterel(フランス)、LDRA(イギリス)、ENEAS(スウェーデン)	ITK、兼松エアロスペース
認証方式		型式証明	型式証明	型式証明
国際規格	システム安全規格	ARP-4754: システム認証規格 ARP-4761: システム安全評価規格 DO-254: ハードウェア認証規格	ARP-4754、ARP-4761相当 DO-254相当	不明
	ソフトウェア安全規格	DO-178B: ソフトウェア認証規格	DO-178B、ED-12相当	不明
第三者検証の方法		DER方式(DER制度の概要については後述)による検証	EASA職員による検証	国土交通省交通局への申請
第三者検証ユーザ企業の例		Boeing、Rockwell Collins	Airbus、EADS	HondaJet、MRJ、IHI

「法律・法令」、「認定機関」、「認証機関」、「国際規格」について各項で個別に説明する。

また、第三者検証の方法としてアメリカ連邦航空局（FAA）の DER（Designated Engineering Representative）制度が参考となることから、これに対し詳細な調査を実施した。

2.3.2. 法律・法令

航空機業界の部品認証について法律・法令を調査した。

(1). 米国における法令

連邦航空局が定める航空機と部品の認証手続きとして“14 CFR Part 21”がある。

“14” “CFR” “Part21” はそれぞれ下記の意味である。

[14 : Title 14]

連邦航空局によって管理される連邦航空規則（Federal Aviation Regulations)のタイトル

[CFR : Code of Federal Regulations]

アメリカ合衆国の連邦政府により連邦官報の中で公布される連邦規則集

[PART 21—CERTIFICATION PROCEDURES FOR PRODUCTS AND PARTS]

米国運輸省連邦航空局が定める航空機の製品や部品の認定手順を定める

(2). 欧州における法令

EASA（欧州航空安全局）が定める、航空機、航空機部品の開発組織や製造組織を認証する要件と手続き（型式証明）として“EASA Part 21”がある。

(3). 日本における法令

日本では航空法において型式証明として定められている。

(型式証明)

第十二条 国土交通大臣は、申請により、航空機の型式の設計について型式証明を行う。

- 2 国土交通大臣は、前項の申請があつたときは、その申請に係る型式の航空機が第十条第四項の基準に適合すると認めるときは、前項の型式証明をしなければならない。
- 3 型式証明は、申請者に型式証明書を交付することによつて行う。
- 4 国土交通大臣は、第一項の型式証明をするときは、あらかじめ経済産業大臣の意見をきかなければならない。

航空法第十二条抜粋

2.3.3. 認定機関（認証機関を認定する機関）

(1). 米国の認定機関

[名称]

アメリカ連邦航空局（FAA：Federal Aviation Administration）

[設立]

1958年

[拠点]

ワシントン

[概要]

アメリカ運輸省の下部組織で航空輸送の安全維持を担当する部局。米国内での航空機の全て（開発、製造、修理、運航）の承認を行う。

[主な業務]

航空管制業務

航空機の設計

乗員の訓練

機体の整備計画等を含む、民間航空機の安全性の向上

民間航空技術の開発支援、民間及び国家宇宙航空に関する技術開発

など

(2). 欧州の認定機関

[名称]

欧州航空安全局（EASA：European Aviation Safety Agency）

[設立]

2002年7月15日

[拠点]

ケルン（ドイツ）

[概要]

2008年にJAA（Joint Aviation Authorities：合同航空当局）の機能を引き継ぎ、本格的に始動

[主な業務]

EU（欧州連合）の民間航空機産業における、安全に関する分野での規制やその管理

加盟国の状況監査を含む、安全ルールの実装および監視

航空機「型式証明」の承認と、その構成要素である設計、製造、保守への関与

非EUである第三国の技術（者）の審査・承認

航空機の安全性の分析・研究等、技術開発

など

(3). 日本の認定機関

[名称]

国土交通省航空局 (JCAB : Japan Civil Aviation Bureau)

[設立]

—

[拠点]

東京

[概要]

航空関連事業を所管

[主な業務]

航空運送事業に係る許認可

航空機の登録

航空機騒音・環境対策

パイロットなど航空従事者の資格証明および養成、航空管制

航空機／エンジンの型式証明

2.3.4. 認証機関

(1). 米国の公認認証機関

公認の認証機関はないが、DER (Designated Engineering Representative) 資格の人間が FAA (連邦航空局) の ACO (Aircraft Certification Office) により任命され、航空機、航空機のサブシステム、部品の検証を行う制度がある (詳細は後述)。

(2). 欧州の公認認証機関

EASA の職員が認証を行うため公認認証機関はない。

EASA の型式認証の申請先

Type certificates

[Applications](#) for new type certification must be sent to :

European Aviation Safety Agency (EASA)

Programmes Department

Applications and Certifications Manager

Postfach 10 12 53 **(for letters only**)**

D-50452 Köln

Germany

Fax: +49 221 89990 9505

Email: tc@easa.europa.eu

出典:EASA Web ページ

(3). 日本の公認認証機関

国土交通省航空局が認証を行うため公認認証機関はない。
航空局の型式認証の申請先

1. 案内情報	
① 手続名	: 航空機の型式証明
② 手続根拠	: 航空法第 12 条第 1 項
③ 手続対象者	: 航空機の製造者
④ 提出時期	: 航空法施行規則第 17 条第 2 項による。
⑤ 提出方法	: 型式証明申請書を作成し、添付書類とともに、国土交通省航空局技術部航空機安全課に提出してください。
⑥ 手数料	: 航空法関係手数料令第 2 条及び第 8 条による。
⑦ 添付書類・部数	: 航空法施行規則第 17 条第 2 項による。
⑧ 申請書様式	: 型式証明申請書（航空法施行規則第 9 号様式）
⑨ 記載要領・記載例	: 提出先にお問い合わせ下さい。
2. 窓口情報	
① 提出先	: 国土交通省航空局技術部航空機安全課
② 受付時間	: 提出先にお問い合わせ下さい。
③ 相談窓口	: 上記提出先と同

国土交通省・航空局の Web ページより

2.3.5. 認証サービス企業

(1). 米国の認証サービス企業

Highrely

[所在地] Phoenix, Arizona, USA
[概要] 従業員数は、約 30 人。DER が 8 人(うち 2 人はパートタイム)

Paragon Transportation

[所在地] Phoenix, Arizona, USA
[概要] Paragon の DER の領域 Type Certificates (TC) Supplemental Type Certificates (STC) Type Inspection Authorization (TIA) Major Repair and Alteration (Form 337) Technical Standard Order (TSO) Parts Manufacturer Approval (PMA) Standard Airworthiness Certificate Inspections (8100-2) 日本の株式会社 itk(ITK Corporation)がパートナー企業となっている。

Certification Services

[所在地]

Eastsound, WA 98245 USA

[概要]

DO-178 FAA DER

DO-254 FAA DER

FAA 航空機型式証明取得

FAA/EASA 認証関連コンサルティング

日本の兼松エアロスペース株式会社が代理店となっている。

(2). 欧州の認証サービス企業

Esterel Technologies

[所在地]

Elancourt France

[概要]

DO-178B 関連製品とサービス

DO-178 Reference Center

DO-178B Methodological Handbooks

DO-178B - Qualified Code Generation

Optimized DO-178B Code Generation for Embedded Displays

DO-178B Design Process Consulting

(3). 日本の認証サービス企業

株式会社 itk(ITK Corporation)

[所在地]

東京都

[概要]

半導体組込み制御システム開発

半導体組込み制御システム開発プロセスに関するコンサルテーション

コンピュータソフトウェアの開発、輸入、販売、組込み及びサポートサービス

半導体、半導体素子及び熱電変換素子並びにこれらの半導体、素子が組み込まれた部分品の設計、製造、販売及び輸出入

認証サポート

航空機搭載ソフトウェアにおける工学設計並びに認証サポートを、プロダクトライフサイクルの終始に渡り提供

パートナー企業 Paragon Transportation LLC 他

2.3.6. 国際規格について

航空関係の国際規格について調査を実施した。

(1). DO-178B

航空システムと機器認証でのソフトウェアに関する考慮事項。

主に、開発プロセスに関する規格、多くの裏づけ書類や記録の提示が必要となる。認証レベルは、A-E に分類される。必要な書類の量は、認証レベルによって異なる。ソフトウェアの不具合によって起こる結果は、壊滅的、非常に危険、メジャー、マイナーあるいは影響なしと類別される。

レベル	障害の条件	検証項目目標値
レベル A	壊滅的	66
レベル B	非常に危険	65
レベル C	メジャー	58
レベル D	マイナー	28
レベル E	影響なし	0

DO-178B の認証書類例

- Plan for Software Aspects of Certification (DO-178B, 11.1)
- Software Development Plan (DO-178B, 11.2)
- Software Verification Plan (DO-178B, 11.3)
- Software Configuration Management Plan (DO-178B, 11.4)
- Software Quality Assurance Plan (DO-178B, 11.5)
- Software Requirements Standards (DO-178B, 11.6)
- Software Design Standards (DO-178B, 11.7)
- Software Code Standards (DO-178B, 11.8)
- Software Requirements Document (DO-178B, 11.9)
- Software Design Description (DO-178B, 11.10)
- Software Verification Cases and Procedures (DO-178B, 11.13)
- Structural Coverage Analysis Results (DO-178B Section 6)
- Software Environment Configuration Index (DO-178B, 11.15)
- Software Configuration Index (DO-178B, 11.16)
- Software Accomplishment Summary (DO-178B, 11.20)

(2). RTCA 規格 DO-254

航空システムと機器認証でのハードウェアに関する考慮事項

RTCA : Radio Technical Commission for Aeronautics / アメリカ航空無線技術委員会

DO-254 の認証書類例

- Plan For Hardware Aspects of Certification (DO-254, 10.1.1)
- Hardware Design Plan (DO-254, 10.1.2)
- Hardware Validation Plan (DO-254, 10.1.3)
- Hardware Verification Plan (DO-254, 10.1.4)
- Hardware Configuration Management Plan (DO-254, 10.1.5)
- Hardware Process Assurance Plan (DO-254, 10.1.6)
- Hardware Requirements Standards (DO-254, 10.2.1)
- Hardware Design Standards (DO-254, 10.2.2)
- Validation and Verification Standards (DO-254, 10.2.3)
- Hardware Archive Standards (DO-254, 10.2.4)
- Hardware Requirements (DO-254, 10.3.1)
- Hardware Design Data (DO-254, 10.3.2)
- Hardware Test Procedures (DO-254, 10.4.4)

Hardware Lifecycle Environment Configuration Index (CAST 27)
Hardware Configuration Index (CAST 27)
Hardware Accomplishment Summary (DO-254, 10.9)

(3). EUROCAE ED-12B

DO-178B と同等 (EUROCAE が RTCA と共同で発行)

EUROCAE : European Organization for Civil Aviation Equipment

(4). EUROCAE ED-80

DO-254 と同等 (EUROCAE が RTCA と共同で発行)

(5). ARP4761

SAE が開発した安全評価ガイドライン、“14 CFR 25.1309” (耐空性基準) への適合証明に利用されている

SAE : Society of Automotive Engineers / 自動車技術者協会

(6). ARP4754A

SAE が開発した、航空機およびシステムの開発プロセスのガイドライン、“14 CFR 25.1309” (耐空性基準) への適合証明に利用されている

2.3.7. アメリカ連邦航空局 (FAA) の DER 制度について

(1). 航空システムと機器認証の関係

連邦航空規定、“14 CFR Part 21” で定める「型式認証プロセス/連邦航空局が定める航空機と部品の認証手続き」では、DO-178B や DO-254 の安全規格に沿って、航空機や部品の認証が行われる。

認証者は、FAA (アメリカ連邦航空局) となるが、実際の認証作業は、FAA が委任する DER (Designated Engineering Representative) により行われる。

型式認証では、ソフトウェアやハードウェアが、その要求仕様に沿って開発されていることを認証するものであり、概念設計/要求仕様定義フェーズに対する評価は行っていない。

FAA では、型式証明とは別に、連邦航空法 “14 CFR 25.1309” (耐空性基準) への適合を要求している。

製造者は、ARP4761 に則り、安全評価解析の結果を審査する。

ARP4761 は、“14 CFR 25.1309” への適合証明のために民間 (SAE) が開発した安全評価ガイドラインである。

ARP4754A は、航空機およびシステムの開発プロセスのガイドラインである。詳細は別の文書 (DO-178B 等) に記載されている。

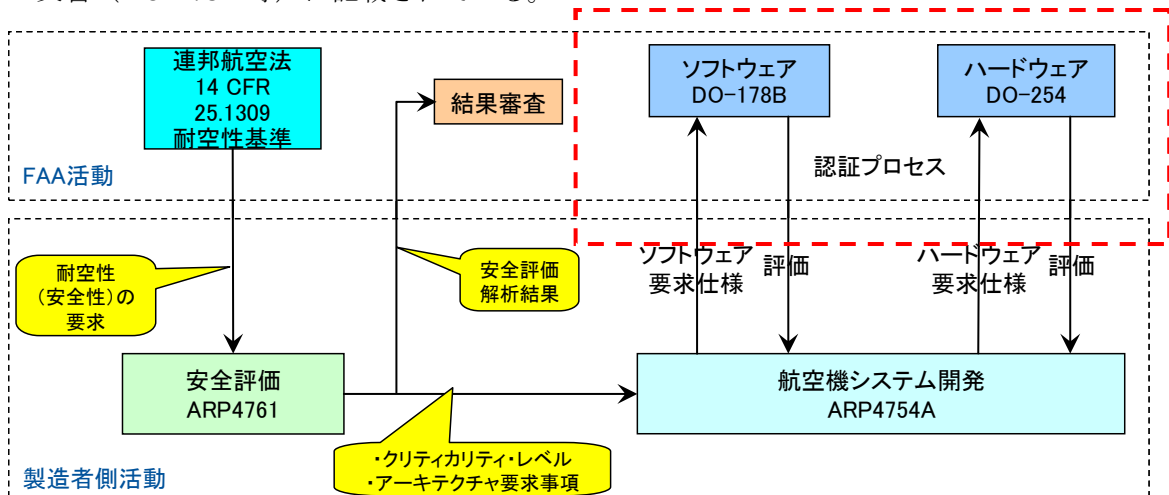


図 2-1 航空システムと機器認証の関係

(2). DER (Designated Engineering Representative) の業務について

DER は、FAA が型式認証の作業を委任する指名代理人であり、型式認証プロセスで下記の業務を代行する技術専門家である。

- ①エンジニアリング技術データの検証
 - ②FAA が要求するテストの立会い
 - ③FAA が要求する監査の実行
- (②と③は FAA (ACO) のさらなる委任が必要)

FAA は型式認証の実質的な作業の全てを DER に委任しているわけではない。

FAA は、全ての作業を自ら行なう権限をリザーブしている。

DER が代行できず、FAA による検証を必要とする項目もある。

(3). カンパニーDER とコンサルタント DER について

・カンパニーDER (Company DER)

- ・所属(雇用)企業が申請して任命される DER
- ・企業がその従業員を申請(推薦)して DER に任命されるもので、DER がその企業を離れる場合は DER の任命も終了する。
- ・カンパニーDER は個人が獲得する公的資格というよりは、社内における役割という性格が強い。

・コンサルタント DER(Consultant DER)

- ・自ら申請する自営 (self-employed) する DER
- ・コンサルタント DER は、認証サービスを提供する企業によって雇用されることが多い。

同一人がカンパニーDER とコンサルタント DER の両方を兼ねることもできるが、別々の申請が必要となる。

(4). DER の委任機能と権限領域例

DER が権限を委任される範囲は、下記の 9 つの技術分野である。各分野で、詳細な権限領域を定めており、各権限領域でさらに委任機能が細分化されている。(図 2-2 システム及び機器(電気機器)DER 代行範囲 参照)

技術分野 (9 分野)

騒音、エンジン、飛行解析、飛行テスト・パイロット、動力装置、プロペラ、無線、機構、システム及び機器 (機械、電気)

権限領域

技術分野ごとに、権限領域が定められる。

- 例： 電気機能／システム
電子機能／システム 等

委任機能

各権限領域には、さらに細分化された委任領域がある。

DER は、委任機能ごとに権限の委任を受ける。例えば、ソフトウェアは委任機能の 1 つであり、ソフトウェア DER には、各権限領域のソフトウェア機能の検証が委任される。

FAA から特別に委任されて(権限領域=Special)、プロジェクト管理的な業務を行なう DER もある。あるいは、通常は FAA が行なう作業を特別に委任するケースもある。

■ : 対象外

委任機能	権限領域											
	電気機器/システム	電子機器/システム	通信システム/アンテナ	自動飛行制御/拡張機能	計装	航行システム/アンテナ	大気データ/ピトー静圧データ	警報システム	内装/外装照明	飛行データ/音声記録	乗客対応/エンターテインメント	指定項目
1 詳細設計及び実装	○	○	○	○	○	○	○	○	○	○	○	○
2 機器品質テスト	○	○	○	○	○	○	○	○	○	○	○	○
3 ソフトウェア	○	○	○	○	○	○	○	○	○	○	○	○
4 サービスドキュメント	○	○	○	○	○	○	○	○	○	○	○	○
5 電気負可解析	○	○	○	○	○	○	○	○	○	○	○	○
6 安全解析	○	○	○	○	○	○	○	○	○	○	○	○
7 落雷/高放射電磁界保護	○	○	○	○	○	○	○	○	○	○	○	○

出典:FAA 規定 8100.37C DESIGNATED ENGINEERING REPRESENTATIVE (DER) GUIDANCE HANDBOOK

図 2-2 システム及び機器(電気機器)DER 代行範囲

(5). DER になる要件

DER 委任の申請には、少なくとも次の a~h の 8つ(a., b.は排他なので実質 7つ)の一般要件を満たす必要がある。

- a. カンパニーDER
技術コンサルティング企業、製造業者、航空会社、または認証された修理ステーションに雇用され、かつその推薦を受けること。また、所属企業の中で、適切な認証を執行できる地位にあること
- b. コンサルタント DER
DER に指名されるために自営であること。航空産業に限らず、他の企業に雇用されていてもよい
- c. 認証の実務知識があること
- d. 指名を受けようとする業務の責任を果たす能力があること
- e. 誠実で健全な判断ができ、協力的な態度のとれる人物であること
- f. 会話及び文書の両方で、英語に堪能であること
- g. 8 年以上の、漸次責任を増す、航空・機械・土木・電気及び一般工学の技術経験、指名を受けようとするのに適切な分野の組合せの経験を必要とする。8 年以上の技術経験には、工学の学位の履修単位を 4 年分まで充てることができる
- h. ACO(FAA)と直接関係する業務の経験があること。指名を受けようとする FAA 認証業務に関する技術データの処理に関わる経験であること

(6). 特殊な権限の DER の要件

前述の要件以外に、特殊な権限の DER についてはそれごとに追加の特殊要件が指定されている。特殊要件が追加される特別な DER は次の a.~f.の 6 種類。

- a. Administrative DER
- b. Management DER
- c. Flight test pilot DER’ s
- d. DER ‘s with a delegation of Software Approval(ソフトウェア DER)
- e. Structural DER’ s with a delegated function of Damage Tolerance Evaluation
- f. Structural DER’ s with a delegated function of Fatigue Analysis

(7). ソフトウェア DER の要件

1. DO-178 に精通していること
2. システム安全検証プロセス、特に software criticality levels について知っていること
3. ソフトウェア開発プロセスの知識
4. ソフトウェア開発ライフサイクルへの参加経験
5. DO-178 で挙げられたソフトウェアの開発及びテストのプロセスの全てのフェーズへの関与の経験
6. 少なくとも1つの高級言語及びアセンブラへの熟練
7. ソフトウェア異常の原因と各テスト手法の相対的特長に関する知識
8. リアルタイム航空システム特有の計算に関する知識
9. ソフトウェアのシステムアーキテクチャ、異種ソフトウェア、パーティションなどのレベルを削減するためのテクニックの理解
10. ハードウェアの知識
11. DER が認証するソフトウェアの認証レベルが決定され、関連するドキュメントに記述される
12. 各レベルの認証をするために、最低限 DER に必要な経験が決まっている。例えばレベル A ソフトウェアの認証権限を得るためには、最低1年間のレベル A データ提出レビューの経験が必要となる

(8). DER の任命申請方法

- ・ 任命申請を、ACO(Aircraft Certification Office)に提出 (ACO は 10 数ヶ所ある)
- ・ FAA Advisor と FAA Evaluator を含む 2 人以上の Evaluation Panel が、要件に照らして DER を任命判定する。
- ・ 任命判定は面接を含む手段によって行なわれる。面接を行なわない場合は、Evaluation Panel はその理由を文書化しなければならない。
- ・ Evaluation Panel は ACO Manager に従属し、更新拒絶等の重要なケースに関しては、Evaluation Panel は ACO Manager に相談しなくてはならない。

(9). DER の更新方法

- ・ 年に 1 回以上、Form 8110-29 を FAA に提出しなければならない。
- ・ 年に 1 度、FAA の Advisor/Evaluator が、DER の業績評価を行ない、DER PERFORMANCE EVALUATION FORM 8110-30 を作成する
- ・ 評価は、DER の activity と FAA との interaction 及び Form 8110-29 の 8 つの key interaction に関して DER から提出された回答に基づいて行なう。
- ・ Advisor は、DER の方法や実績に問題がないか判定し、問題があれば是正措置をとる。例えば、追加の教育やカウンセリングを行なう。次の年次評価の際に follow-up session を行い、是正措置の結果が容認可能か判定する。
- ・ DER の業績がまだ不十分な場合、Advisor は ACO Manager と資格停止の可能性について議論する。
- ・ 更新申請は電子的に可能。

(10). DER になるには

- ・ FAA との業務経験を積むこと。
型式認証の実務経験が要求されるが、これは、FAA が認めた、DER に準じたあるいは DER を補佐する役割で働かないと獲得できない。
他の要件を満たし、これのみが欠けている申請者は、まず DER Candidate と認められ、その資格で DER 指名に必要な FAA との業務経験を積むことになる。
- ・ 申請者の技術的専門性(d、g.)を証明してくれる保証人が 3 人必要。人物(e.)保証人も必要で、技術保証人が人物保証人を兼ねてもよい。

(11). DER の地位

- ・ DER の任命は、ACO が必要と認め、DER を管理するリソースが ACO にある場合に限り行なわれる。この点は、試験や所定の教育により一定の能力・要件を満たすと認められた人には例外なく認定されるいわゆる「資格」とは異なる。
- ・ DER がその肩書きを使用できるのは、委任された権限の行使、すなわち、型式認証に必要な技術データの認証に限られる。それ以外の場面（例えば名刺）で、FAA との雇用・代理関係を類推させるようなロゴや DER ID 番号の使用は禁止されている。
- ・ DER への任命が ACO によって一方的に停止・解除されることを認めた上で、DER に就くことになっている。
- ・ DER は資格といっても技術的な知識と FAA の解釈に関する知識を有するという能力の認定にすぎず、何らかの法的権利が付与されるという意味での資格ではない。

(12). DER への委任の停止

FAA (ACO) は、次の理由によって、DER への委任を停止できる。

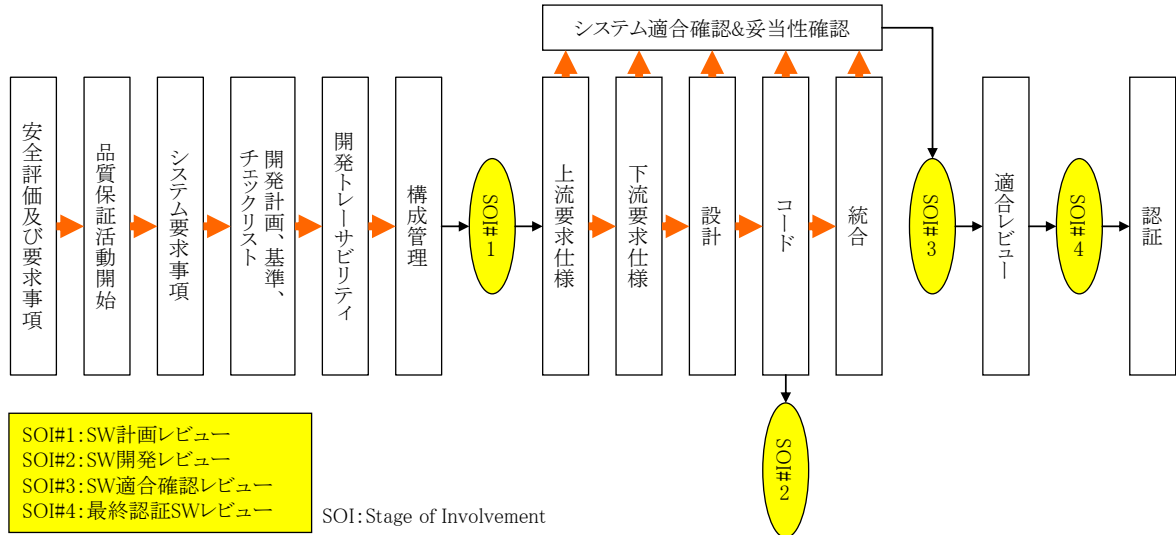
- ・ DER の死亡
- ・ DER として勤務している会社からの退職
- ・ DER または DER の所属企業(任命を申請した)からの申出
- ・ DER として勤務している会社からの転職
- ・ 活動不十分
- ・ 資格要件の錯誤
- ・ 委任に必要な資格の停止
- ・ 注意力、判断力、誠実さの欠如
- ・ FAA (ACO) からみた必要性の欠如、FAA (ACO) の管理リソースの不足
(DMIR/DAR の停止条件)
- ・ 更新申請の欠如
- ・ 活動内容が不正だったり、達成が不十分
- ・ 管理者が適当と認める、その他の理由

FAA (ACO) が必要な仕事量に対して DER リソースが過剰と判断したり、FAA (ACO) 自体に DER を管理する人的リソースが不足すると判断したときは、任意に DER への委任を停止できるようになっている。

(13). DER による監査とレビューのタイミング

DER の主要業務は、アセスメントのための公式レビューと、監査 (Audit) のための机上レビューを行うことにある。公式レビューは以下に示した「DO-178B ソフトウェア認証プロセス」の SOI#1、SOI#2、SOI#3、SOI#4 のタイミングで実施される。

机上レビューは以下のプロセスの⇒のタイミングで実施



HighRelly 資料より作成

図 2-3 DO-178B ソフトウェア認証プロセス

(14). 航空分野のプロセス

航空機分野 製品認証／開発／運用プロセス図を示す。

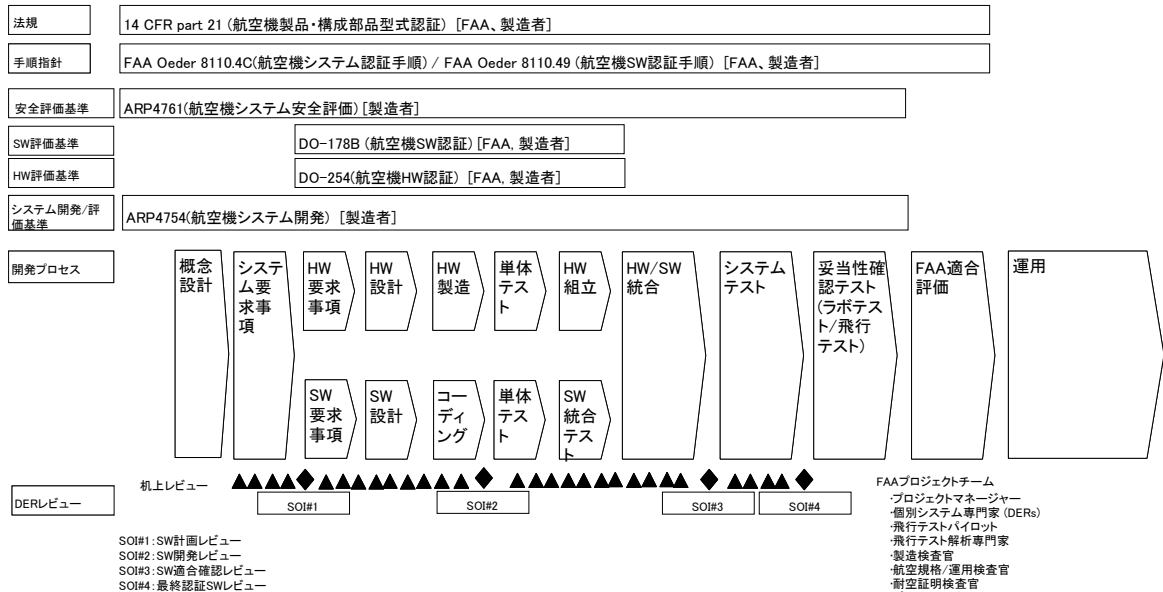


図 2-4 航空機分野 製品認証／開発／運用プロセス図

(15). 航空分野の製品認証ドキュメント体系

航空分野の製品認証ドキュメント体系を示す。

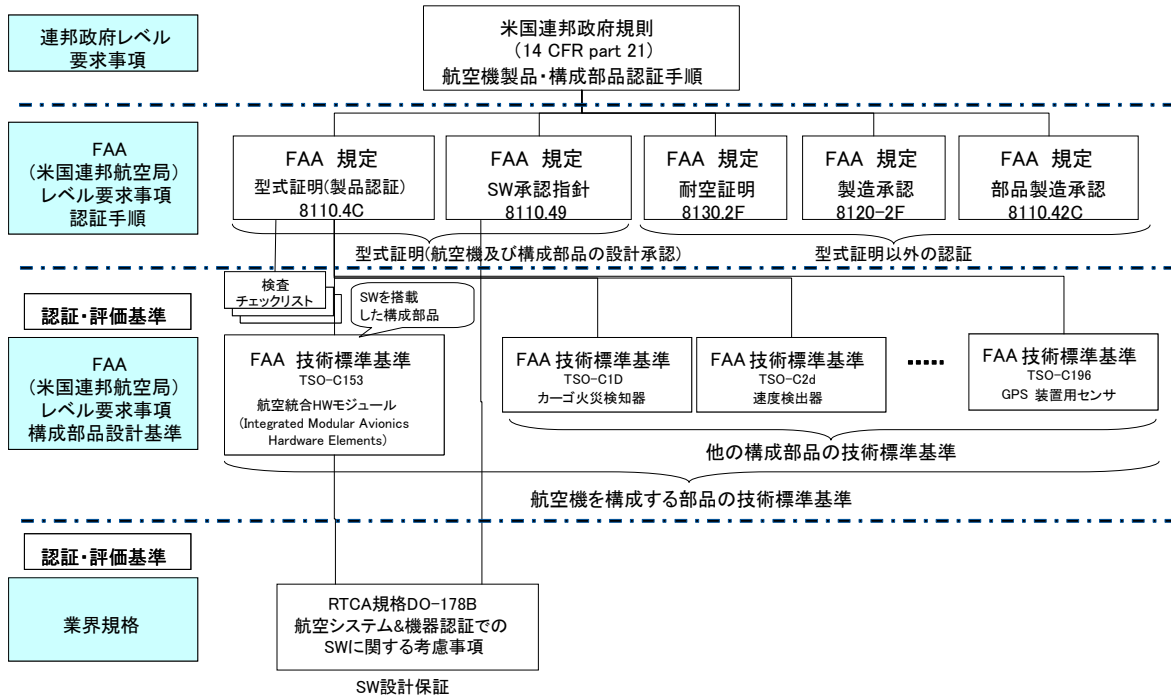


図 2-5 航空分野の製品認証ドキュメント体系

(16). DER によるソフトウェア認証のコスト

DER による認証コストの目安を一表にした。

表 2-2 DER による認証コストの目安

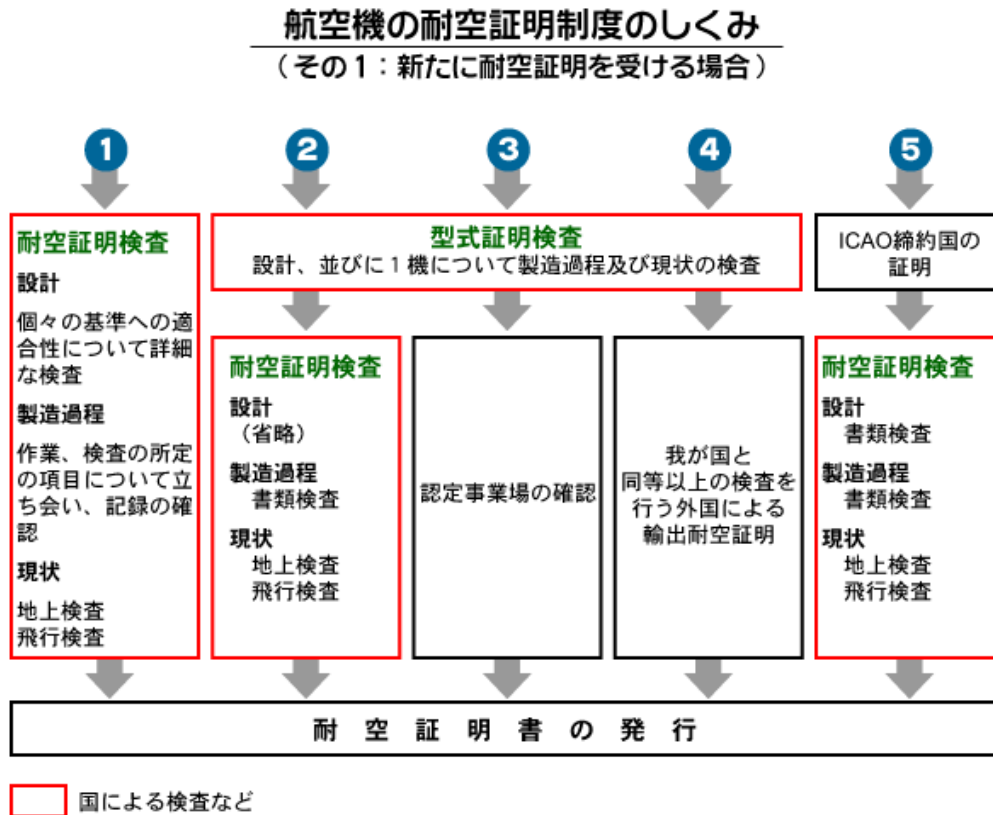
コストの種類	説明	コストの目安
D178 B教育コスト	開発プロジェクトのメンバー及びマネージャは、DO-178Bに関する教育を受ける必要がある	非公開(顧客別)トレーニングの講師料は、\$8-12K程度
ギャップ分析コスト	自社の開発プロセスが、DO-178Bの開発プロセスと乖離しているかを分析し、何が再利用できて、何を再履行しなければならないかを決定する	訓練と経験のあるDERによるギャップ分析のコストは、\$20-30K、所要期間は2-4週間。
DO-178B 計画書類、及びチェックリストの購入・作成コスト	ドキュメントは、DO-178Bの豊富な経験と時間があれば、自分で作成することも可能	document packageの購入コストは、\$10K - 20K程度。
DERのコンサルティング費用	時間制の他に、パック料金のような形態もある	時間制のDER料金は、時間あたり \$120 - \$400
認証コスト	経験によれば、コード1行あたりの認証コストは、コードサイズや開発組織の経験や賃金水準によって\$50～300の範囲	100,000行のコードの認証に数百万\$かかることもありうる。(Safe Software Consulting)

総コストに関する通説

- DO-178Bの検証作業は、1つのエンジニアリングチームがコード1行の検証に1～4時間かかるほど労力を要する
- DO-178Bの検証作業にかかる追加コストは、50～200%になると考えられている (HighRelY)
- 始めから高信頼ソフトウェア工学の原理が使用されれば、DO-178Bの追加コストは25～40%のはず (HighRelY)
- DO-178B、および、DO-254が効率的に実行されれば、開発コストの増加はずっと少なく、長期的にはコスト効率がよくなる (HighRelY)
- コストを下げるためにツール(による自動化)を採用する場合は、ツールの認証 (Qualification)が必要

2.3.8. 日本における型式証明の手続き（参考）

国土交通省国土交通省・航空局が定める滞空証明、型式証明の制度を示す。



出典：国土交通省・航空局

図 2-6 航空機の耐空証明制度のしくみ

国土交通省・航空局の資料によると、日本国内で航空機を新たに製造、または輸入した場合、耐空証明を受けるまでには前記のように①～⑤のプロセスがある。

① 設計、製造過程、現状の全てを詳細に検査する

国があらかじめ「型式証明」を発行して設計の検査を終了している場合は、

② 設計検査を省略、製造過程を書類で行い、現状の検査（実際の機体による検査）を行う

③ 国があらかじめ認定した航空機製造者（航空機製造検査認定事業場という）が航空機の完成後の現状まで確認した場合、国は実際の検査を行わない。

④ 日本と同等以上の検査を実施する外国の航空当局が、輸出耐空証明書を発行していれば、我が国は実際の検査を行わない。

ICAO 条約締結国が輸出耐空証明書を発行している場合は、

⑤設計、製造過程は書類にて検査し、現状の検査を実機を使用して行うこととされている

ICAO 条約：国際民間航空機関（ICAO）が作成する条約

2.3.9. 相互認証（参考）

二国間取極（BASA: Bilateral Aviation Safety Agreement）と呼ばれ、国土交通省は、米国との間での締結を目指している。

以下、国土交通省・航空局の資料より抜粋。

米国との航空安全に関する二国間取極(BASA)の締結の推進

米国との BASA の締結の意義

○航空安全に関する二国間取極（BASA: Bilateral Aviation Safety Agreement）は、我が国と同等以上の制度を有する相手国の証明、評価結果等を基に、一部検査を省略して自国の証明等を行う相互承認のための協定であり、現在米国との間でその締結に向けた交渉を行っている。BASA に基づき航空分野の各分野毎の実施取決め（IP: Implementation Procedures）を当局間で作成することにより、安全を確保しつつ、一層の検査効率を図ることが可能となる。

○現時点では航空機の安全性（耐空性）等の分野を優先して協議を行っており、BASA が締結されれば、いずれか一方の国の証明を受けることにより相手国の証明のための検査を大幅に省略することが可能となり、航空機メーカー、航空会社等の大幅な負担軽減になる。特に、我が国企業が開発し昨年10月に型式証明の申請がされた国産ジェット機について、米国 FAA の証明を効率的に取得することが可能となる。

○また、BASA を締結することにより、航空安全分野における包括的な相互承認を行うための基盤が整備され、今後、整備施設、乗員ライセンス、シミュレータ等に関する IP を追加することにより、ライセンスの切替えにおける試験、認定事業場、シミュレータ等の認定・維持における検査の省略が期待できる。

今後の措置

○米国との間で航空機及び装備品の耐空性に関する相互承認を推進するため、BASA 及びこれに基づく耐空性に関する実施取決め（IP）の早期締結を目指す。

○米国との間で相互承認分野の拡大を図るため、耐空性に関する実施取決め（IP）が締結された後速やかに、整備施設、乗員ライセンス、シミュレータ等の分野における実施取決め（IP）の協議を推進する。

2.3.10. 第三者検証のユーザ

第三者検証のユーザは、航空機メーカー、航空機のサブシステムメーカー、部品メーカーとなる。日本の例では、HondaJet、MRJなどが挙げられる。

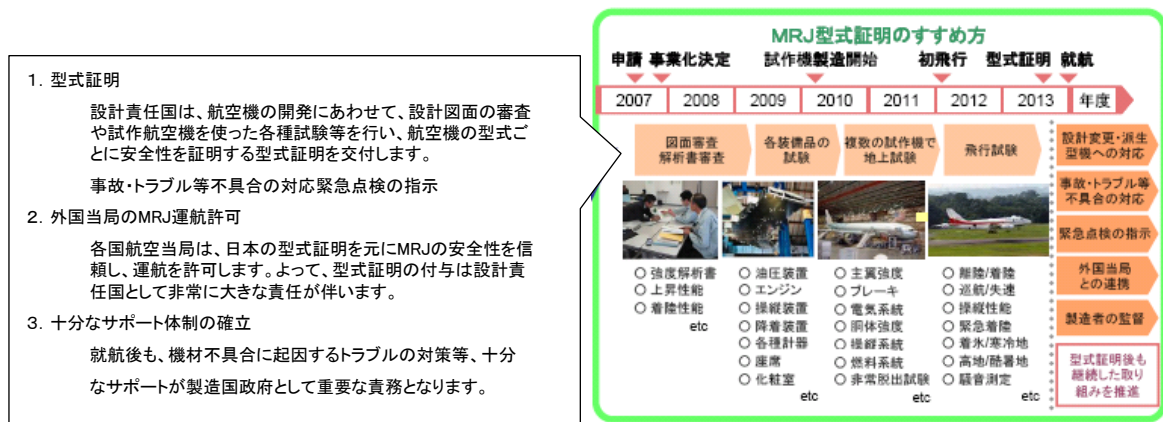
(1). HondaJet の例

2012年のFAAおよび欧州航空安全局（EASA）の型式認定取得を目指す。機体引き渡しは2012年後半を予定とされている。

米国で、DERによりFAAの型式認証を取得している。

(2). MRJ（Mitsubishi Regional Jet）の例

MRJは、国土交通省・航空局による型式認証の取得を進めている。米国、欧州については、相互認証による認証取得を考えていると思われる。



国土交通省資料より

図 2-7 MRJ の型式証明のすすめ方

2.4. 第三者検証の現状（医療機器業界）

2.4.1. 概要

医療機器業界における第三者検証に関連する事項を米国、欧州、日本で比較した。法律・法令、認定機関、国際規格、第三者検証の方法については以降の項で個別に説明する。

表 2-3 医療機器業界の第三者検証への対応比較(米・欧・日)

対象業界		医療機器業界		
対象地域		米国	欧州	日本
対象製品		医療機器、サブシステム、部品		
法律・法令		FD&CA(医薬品及び化粧品法)	MDD(欧州医療機器指令)	薬事法
第三者検証組織・企業	認定機関 (Notifying Authority) 認定機関(certifying body)	FDA(食品医薬品局)のCDRH(医療機器・放射線保健センター)	EU各国に、認定機関(Notifying Authority)がある	厚生労働省 医薬品医療機器総合機構
	公認-認証機関 (Notified Body)、認証者	REGULATORY TECHNOLOGY SERVICES、TUV RHEINLAND OF NORTH AMERICA等11の認証機関	TUV Rhenland、Bureau Veritas等 74の認証機関	都道府県、テフズードジャパン、UL Japan等 14の認証機関
	認証サービス企業	Boston Atlantic Emergo Group	-	テクマトリックス
認証方式		PMA (510(k))	CEマーキング	QMS省令
国際規格	システム安全規格	IEC60601-1(EMC規制) GSR(Quality System Regulation)	IEC60601-1(EMC規制) ISO13485	IEC60601-1(EMC規制) ISO13485
	ソフトウェア安全規格	IEC62304	IEC62304	IEC62304
第三者検証の方法		FDAの第三者検証方式については後述	CEマーキングの第三者検証方式については後述	QMSの第三者検証方式については後述
第三者検証ユーザ企業の例		GE Healthcare、Boston Scientific	Philips	オリンパス

2.4.2. 法律・法令

(1). 米国における法令

FD&C Act（医薬品及び化粧品法）（Federal Food, Drug, and Cosmetic Act）

SEC. 515. [21 USC § 360e] Premarket Approval; General Requirement

PMA：市販前審査に関する条項、クラス III 機器の市販前審査（公認認証機関による第三者検証）を義務付ける

SEC. 510. [21 USC § 360] Registration of Producers of Drugs and Devices

510(k)：市販前届けに関する条項、クラス II 機器の製造業者による届出を義務付ける

クラス分類

医療機器を、1,700種に分け、これらを16の専門分野ごとに分類、患者や使用者に影響を及ぼす可能性のあるリスクの程度によってクラス I、II、IIIのクラスに分類

- I 本来の使用に際してまずリスクがないと考えられるもの
- II リスクはあるが、その安全性／有効性の審査を受けて市場化された事例 (predicate) が存在するもの
- III 体内に永久的に埋込まれたり、本来の使用に際してのリスクが高いもの、及び、リスクがあつて、その安全性／有効性を審査して市場化された事例がない、あるいは不十分なもの

認証、届出の方法

クラス I：市販前届を免除

クラス II：多くは市販前届が必要 (510(k))

クラスⅢ：市販前承認が必要（PMA）

* 新医療機器を除く

クラスⅢの市販前承認（PMA）で公認認証機関が関与する

市販前届（510(k)）では、FDA が認定する第三者機関によるレビューによる申請をすることもできる

(2). 欧州における法令

欧州：MDD（欧州医療機器指令）（Medical Device Directive 93/42/EEC）

欧州で販売する医療機器には、CE マークを貼付する義務を定める。

要求事項違反をすると、罰金を科せられる強制事項。

クラスⅢ 高リスクでは、認定機関による第三者認証、臨床試験が必須となる。

クラス分類

クラス分類を決める規則として、18 のルールがある

規則 1-4：非侵襲性(※)機器

規則 5-8：侵襲性機器

規則 9-12：能動医療機器

規則 13-18：特別規則

ルールに基づき、リスク別に 4 つのクラスにクラス分け

I 低リスク

IIa 中リスク

IIb 中リスク

III 高リスク

認証、届出の方法

クラスごとに決められた評価手順（ANNEX II、III、IV、V、VI、VII、VIII の組み合わせ）で、認証、届出を実施

クラス I：自己宣言

クラス I の一部とクラス IIa 以上で、公認認証機関が関与

(3). 日本における法令

薬事法 QMS 省令

クラスⅡ以上の医療機器及びクラスⅠ医療機器一部のものの設計開発、製造にあたって、QMS 省令(平成 16 年厚生労働省令第 169 号「医療機器及び体外診断用医薬品の製造管理及び品質管理の基準に関する省令」)に適合している必要がある。

承認もしくは認証の申請にあたって、医薬品医療機器総合機構、認証機関（注：第三者認証制度）もしくは都道府県により省令への適合性調査を受審する。また、受審は定期的に必要である。

クラス分類

I 一般医療機器

II 管理医療機器

III 高度管理医療機器

IV 高度管理医療機器

認証、届出の方法

管理医療機器(クラスⅡ)のうち厚生労働大臣が基準を定めて指定した管理医療機器（指定管理医療機器）について、厚生労働大臣による承認制度に代えて登録された第三者機関による認証制度がある

- クラス I : 製造販売届け
医薬品医療機器総合機構による承認
- クラス II : 第三者機関による認証
都道府県による承認
- クラス III : 都道府県による承認
医薬品医療機器総合機構による承認
- クラス IV : 医薬品医療機器総合機構による承認

2.4.3. 認定機関（認証機関を認定する機関）

(1). 米国の認定機関

[名称]

アメリカ食品医薬品局（FDA : Food and Drug Administration）

[設立]

1927年に、農務省化学局から食品・医薬品・農薬局と改称・昇格し、1930年にはFDAと改称した。

[拠点]

メリーランド州

[概要]

医薬品および動物用医薬品、生物学的製剤、医療機器、国内の食糧供給、化粧品、そして電磁波を放出するような製品の安全性と有効性を保証することによって国民の健康を守ることを責務としている。FDAの組織のひとつである、医療機器・放射線保健センター（CDRH : Center for Devices and Radiological Health）は、新規の医療機器が市場に参入する前にそれが安全で有効であることを確認する。

(2). 欧州の認定機関

欧州委員会の各国に認証機関を認定する認定機関がある。

英国医薬品・医療製品規制庁(MHRA)
(Medicines and Healthcare products Regulatory Agency)

ドイツ連邦労働安全衛生研究所 (BAuA)
(Bundesanstalt für Arbeitsschutz und Arbeitsmedizin, Gruppe 2.1
“Produktbeschaffenheit, Grundsatzfragen)

フランス医薬品医療機器安全庁 (Afssaps)
(Agence Française de Sécurité Sanitaire des Produits de Santé - Direction de l'Evaluation des Dispositifs Médicaux)

(3). 日本の認定機関

[名称]

厚生労働省 独立行政法人医薬品医療機器総合機構

[主な業務]

- 承認審査業務
- 安全対策業務
- 健康被害救済業務

[承認審査業務の概要]

- 対面助言業務
- 信頼性保証業務
- 医薬品等承認審査業務
- 医療機器承認審査業務
- GMP/QMS 適合性調査業務

2.4.4. 認証機関

(1). 米国の認証機関

アメリカの他、イギリス、オランダ、ノルウェー台湾に、合計 11 の公認の認証機関がある

REGULATORY TECHNOLOGY SERVICES, LLC (アメリカ)
TÜV RHEINLAND OF NORTH AMERICA, INC. (アメリカ)
TUV SUD AMERICA, INC. (アメリカ)
UNDERWRITERS LABORATORIES, INC. (アメリカ)
CITECH (アメリカ)
INTERTEK TESTING SERVICES (アメリカ)
BRITISH STANDARDS INSTITUTION (イギリス)
CENTER FOR MEASUREMENT STANDARDS OF INDUSTRIAL (台湾)
CHEIROON BV (オランダ)
KEMA QUALITY B.V. (オランダ)
NIOM - NORDIC INSTITUTE OF DENTAL MATERIALS (ノルウェー)

(2). 欧州の認証機関

74 の認証機関がある

VTT (フィンランド)
TÜV Rheinland (ドイツ)
TÜV SÜD (ドイツ)
TÜV NORD Group(ドイツ)
BUREAU VERITAS (フランス)
BSI:British Standards Institution (イギリス)
DQS GmbH (ドイツ)
KEMA (オランダ)
Intertek (イギリス)
LGA InterCert GmbH (ドイツ)
LNE/G-MED(フランス)
NSAI:National Standards Authority of Ireland (アイルランド)
SGS (イギリス)
UL (イギリス)
他

(3). 日本の認証機関

財団法人 医療機器センター
SGS ジャパン株式会社
キーマ・クオリティ・ジャパン株式会社
株式会社コスモス・コーポレーション
ナノテックシュピンドラー株式会社
テュフズードジャパン株式会社
テュフ ラインランド ジャパン株式会社
一般財団法人 電気安全環境研究所
日本化学キューエイ株式会社
一般財団法人 日本品質保証機構
BSI グループジャパン株式会社
フジファルマ株式会社
株式会社 UL Japan

2.4.5. 国際規格

(1). ISO 13485 の概要

ISO 13485:2003 Medical devices -- Quality management systems -- Requirements for regulatory purposes ISO9001 をベースに作られた医療機器製造、品質管理のための規格であり、製品・サービスの品質の良否を決める規格ではない。顧客が求める機能を持ち、安全性の高い一定の品質の製品・サービスが常に提供されるような仕組みを作る規格である。(JIS規格は、「JIS Q 13485:2005 医療機器-品質マネジメントシステム-規制目的のための要求事項」が対応している。)

既に ISO9001 は商取引のグローバル化を背景に、工業生産を行う全世界に浸透している。医療機器については、製造・販売のグローバル化を背景に、日本でも厚生労働省から ISO13485 に準拠した、医療機器 QMS 省令(医療機器製造の GMP:Good Manufacturing Practice を含む)が出ている。ISO13485 を取り入れることにより、顧客が要求する一定品質の製品・サービスを提供するための製造管理、品質管理の仕組みが実現する。

目的

- (a) 国際標準化機構(ISO)が定めた 23 項目の要求事項(しなければならないこと)からなる医療機器の製造管理、品質管理に関する世界標準システム。
- (b) 製品そのものの規格を定めたものではなく、管理システム(管理の仕組み)のモデルを示したものの。
- (c) 医療機器用に人体への危害リスク、安全性管理の必要性を加味して、ISO9001 の要求事項の一部を変更、追加したもの。システムは ISO9001 とほぼ同様。

審査機関(認証機関)

- (a) 国際標準化機構(ISO)ー日本では相互認証している公益財団法人日本適合性認定協会(JAB)より認定を受けた機関が、企業のこの規格の構築、運用状況を審査し合格すれば認証を与える。ただし、この認証取得は、JAB が独自に行うもので、医療機器の品目承認・認証(厚労省管轄)には効果がない。
- (b) 厚労省が医療機器の承認・認証の第三者機関として認定した機関でかつ JAB より認定を受けた機関が、企業のこの規格の構築、運用状況を審査し合格すれば認証を与える。この認証は、第三者機関が行う医療機器の承認・認証の際に有効である。

要求事項

ISO 13485 では、プロセスごとに要求事項が定義されている。下記は、各プロセスの一覧(標準の目次)である。要求事項に沿って、実施方針を決め、実行し記録する(標準化→文書化→実行→記録)。その通りできているかをチェックし改善する(計画→実行→チェック→改善)。

表 2-4 ISO 13485 の要求事項(目次)

1	適用範囲	5.6.2	マネジメントレビューへのインプット	7.4.1	購買プロセス	7.5.4	顧客の所有物
1.1	一般	5.6.3	マネジメントレビューからのアウトプット	7.4.2	購買情報	7.5.5	製品の保存
1.2	適用	6	資源の運用管理	7.4.3	購買製品の検証	7.6	監視機器及び測定機器の管理
2	引用規格	6.1	資源の提供	7.5	製造及びサービス提供	8	測定、分析及び改善
3	定義	6.2	人的資源	7.5.1	製造及びサービス提供の管理	8.1	一般
4	品質マネジメントシステム	6.2.1	一般	7.5.1.1	一般要求事項	8.2	監視及び測定
4.1	一般要求事項	6.2.2	力量、認識及び教育・訓練	7.5.1.2	製品及びサービス提供の管理-固有要求事項	8.2.1	フィードバック
4.2	文書化に関する要求事項	6.3	インフラストラクチャー	7.5.1.2.1	製品の清浄性及び汚染管理	8.2.2	内部監査
4.2.1	一般	6.4	作業環境	7.5.1.2.2	届け活動	8.2.3	プロセスの監視及び測定
4.2.2	品質マニュアル	7	製品実現	7.5.1.2.3	付帯サービス活動	8.2.4	製品の監視及び測定
4.2.3	文書管理	7.1	製品実現の計画	7.5.1.3	滅菌医療機器に対する特別要求事項	8.2.4.1	一般要求事項
4.2.4	記録の管理	7.2	顧客関連のプロセス	7.5.2	製造及びサービス提供に関するプロセスの妥当性確認	8.2.4.2	能動埋め込み機器及び埋め込み機器固有の要求事項
5	経営者の責任	7.2.1	製品に関連する要求事項の明確化	7.5.2.1	一般要求事項	8.3	不適合製品の管理
5.1	経営者のコミットメント	7.2.2	製品に関連する要求事項のレビュー	7.5.2.2	滅菌医療機器に対する固有の要求事項	8.4	データの分析
5.2	顧客重視	7.2.3	顧客とのコミュニケーション	7.5.2.1	一般要求事項	8.5	改善
5.3	品質方針	7.3	設計・開発	7.5.2.2	滅菌医療機器に対する固有の要求事項	8.5.1	一般
5.4	計画	7.3.1	設計・開発の計画	7.5.3	識別及びトレーサビリティ	8.5.2	是正処置
5.4.1	品質目標	7.3.2	設計・開発へのインプット	7.5.3.1	識別	8.5.3	予防処置
5.4.2	品質マネジメントシステムの計画	7.3.3	設計・開発からのアウトプット	7.5.3.2	トレーサビリティ		
5.5	責任、権限及びコミュニケーション	7.3.4	設計・開発のレビュー	7.5.3.2.1	一般		
5.5.1	責任及び権限	7.3.5	設計・開発の検証	7.5.3.2.2	能動埋め込み医療機器及び埋め込み医療機器固有の要求事項		
5.5.2	管理責任者	7.3.6	設計・開発の妥当性確認	7.5.3.3	状態の識別		
5.5.3	内部コミュニケーション	7.3.7	設計・開発の変更管理				
5.6	マネジメントレビュー	7.4	購買				
5.6.1	一般						

JIS Q 13485:2005 医療機器-品質マネジメントシステム-規制目的のための要求事項より引用

(2). IEC 62304 の概要

IEC 62304:2006 Medical device software -- Software life cycle processes は、医療機器ソフトウェア ソフトウェアライフサイクルプロセスの国際規格である。メーカーがソフトウェアに起因する危害が患者など人に及ぼす影響に応じて、下記のようにソフトウェアの安全クラスに分類することとしている。

クラス	安全区分
クラス A	負傷または健康障害の可能性がない
クラス B	重傷の可能性はない
クラス C	死亡または重傷の可能性がある

(3). IEC 62366 の概要

IEC 62366:2007 Medical devices -- Application of usability engineering to medical devices は、医療機器のユーザビリティに関する規格である。ISO との JWG(合同作業部会)で 2007 年 10 月に国際規格として発行された。

(4). IEC 60601-1-9 の概要

IEC 60601-1-9 ed1.0 Medical electrical equipment - Part 1-9: General requirements for basic safety and essential performance - Collateral Standard: Requirements for environmentally conscious design

2007 年 7 月に IEC 60601-1-9 (医用電気機器—第 1-9 部：基礎安全及び基本性能に関する一般要求事項—副通則：環境配慮設計の要求事項) が国際規格として発行された。

2.4.6. 第三者検証の方法

(1). 米国

医療機器をクラス I、クラス II、クラス III に分類する。

クラス I：市販前届を免除

クラス II：多くは市販前届が必要 (Premarket Notification：510(k))

クラス III：市販前承認が必要 (Premarket Approval：PMA)

*新医療機器を除く

クラス II の機器では、市販前届 (許可) が必要であり、一般的に 510(k) 申請と呼ばれる。

クラス III の機器では、市販前承認が必要であり、一般的に PMA 申請と呼ばれる。

510(k) 申請と PMA 申請の主な相違を下表に示す。

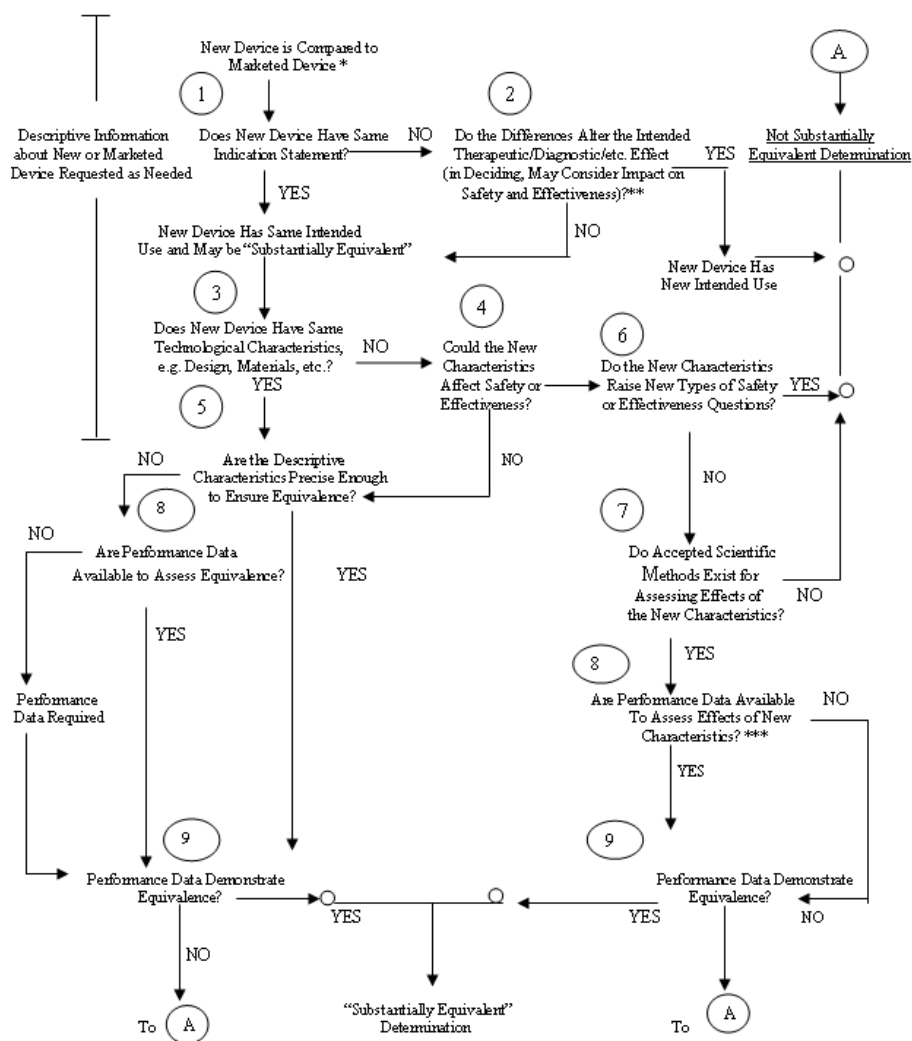
表 2-5 510(k) 申請と PMA 申請の主な相違

510(K) 申請	PMA 申請
主にクラス II の機器	主にクラス III の機器
クラス I あるいはクラス II の改正前機器、あるいは法的に市販後の同等機器が存在する	クラス I あるいはクラス II の改正前機器、あるいは法的に市販後の同等機器が存在しない
第三者レビューの利用が選択できる、臨床データは要求されない	生命を維持するあるいは／または患者へのリスクをもたらす可能性のある機器
既存の機器に対する本質的同等性を証明する書類を必要とする	機器の安全性と効果を示す書類を必要とする

出典：FDA Web ページ

510(k)申請では、開発プロセスに関わる一定レベルのドキュメントの提出を求められるが、内容の審査は行なわない。レビューのプロセスを第三者に任せることも出来る。PMA 申請では、市販前承認のために公認認証機関（第三者認証）が関与する。

FDA の 510(k)では、開発プロセスに関わる一定レベルのドキュメントの提出を求められるが、内容の審査は行なわない。そのかわり、開発プロセスのガイドラインや標準（IEC 62304 等）を示して、その遵守を推奨する。なお、510(k)レビューでは、既に市場化された類似製品との本質的同等性のみが評価され、提出された個々のドキュメントの内容の正当性は審査されない。本質的同等性の評価の手順を下記に示す。



出典：FDA Web ページ

図 2-8 本質的同等性の評価の手順

FDA は第三者機関に、510(k)のレビューを委任し、第三者機関は、予め指名して FDA の教育を受けさせた従業員をレビューに従事させることができる。

申請された 510(k)に最終的に許可 (clearance) を与えるのは FDA であるが、信任された第三者機関は、FAA が行なうのと全く同じレビューを行なって推奨 (recommendation) を与える。レビューのガイドラインはマニュアル化されており、レビュー実施者は FDA の教育を受けることが義務付けられている。

信任において重視される要件は組織の独立性で、機関及びレビュー実施者が業界といかなる利害関係も持ってはならない。

510(k)レビュー実施者の第三者委任は、EU との情報交換の促進や、他の標準との重複審査の負担の軽減も目的としている。信任の申請はだれでもできるが、望ましい委任先の候補は、当初から適格審査機関 (CAB) の中である程度絞り込まれていると考えられる。

一般的に、510(k)申請で提出する書類は、次のことがらを示す必要がある。

- ・ 機器の設計 (design) の記述 (要求仕様・機能設計)
- ・ 設計がどのように実装されたかの記録 (実装設計)
- ・ 設計・実装によって作り出された device がどのようにテストされたかの説明 (テスト)
- ・ ハザードが適切に認識され、リスクが効果的に管理されていることの説明 (ハザード解析)
- ・ 設計・実装・テスト・リスク管理を相互にリンクするトレーサビリティの提供 (トレーサビリティ)

ソフトウェアの重要性のレベルは、マイナー、モデレート、メジャーの 3 レベルがあり、FDA がそれぞれのレベルで 510(k)の提出書類として推奨する書類の種類と程度・範囲は、次表のようになっている。

表 2-6 510(k)申請書類

ドキュメントの種類	ソフトウェアの重要性のレベル		
	マイナー	モデレート	メジャー
重要性のレベル	重要性のレベルの表明と、その判断理由の記述		
ソフトウェアの記述	特徴とソフトウェア動作環境の要約・概観		
device/ハザード解析	厳しさの査定と緩和策を含むハードウェア及びソフトウェアのハザードの表		
ソフトウェア要求仕様 (SRS)	機能要件の SRS からの抜粋	完全な SRSドキュメント	
アーキテクチャ設計チャート	提出不要	機能ユニットとソフトウェアモジュールの詳細な記述	
		フローチャート及び状態図 (state diagram) を含んでもよい	
ソフトウェア設計仕様 (SDS)	提出不要	ソフトウェア設計仕様書	
トレーサビリティ解析	要件、仕様、ハザード及び緩和策、V&Vテストの間のトレーサビリティ		
ソフトウェア開発環境の記述	提出不要	ソフトウェアライフサイクル開発計画の要約	ソフトウェアライフサイクル開発計画の要約
		構成管理及びメンテナンス活動の要約を含む	
Verification&Validation関連	ソフトウェア機能テスト計画	単体・結合・システムの各レベルでの V&V活動の記述	
ドキュメント	pass/failの基準及び結果	システムレベルのテスト手順	開発プロセス中に生成された制御ドキュメントの注釈付きリスト
		pass/failの基準及び結果を含む	
リビジョンレベル履歴	リビジョン履歴ログ リリースバージョン番号と日付を含む		
未解決異常 (バグまたは欠点)	提出不要	ソフトウェア異常の残件のリスト	
		オペレータの使用方法和ヒューマンファクタを含む、安全性または効果に対する影響の説明の注釈付き	

出典：FDA Web ページ

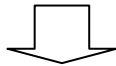
(2). 欧州

医療機器は、18 のルールに基づき、クラス I、クラス I*、クラス IIa、クラス IIb、クラス III に分類される。

表 2-7 クラス分けの 18 のルール

製品特徴	適用ルール
・非侵襲性医療機器 侵襲性：体表もしくは開口部を通じ一部または全部が体内に貫通するような機器	ルール 1：患者との接触がないもしくは皮膚を介しての接触があるのみ ルール 2：血液、体液、体組織およびガスの処理及び保管 ルール 3：血液、体液、その他液体の組成の改善 ルール 4：創傷部に対する接触（機械的保護、滲出物吸収）
・侵襲性医療機器	ルール5：体の開口部に対し適用（外科的方法でなく） ルール6：侵襲性機器で一過的（60分以下）な使用 ルール7：侵襲性機器で短期的（60日以下）な使用 ルール8：侵襲性機器で長期的（60日以上）な使用または埋込型機器
・能動医療機器 握力・重力以外の動力源及び電気的エネルギー源の変換によって作用する機器 □	ルール9：エネルギーの変換もしくはエネルギーを使用する治療用機器 ルール10：診断用機器 ルール11：薬液の投与／注入 或いは 体内より物質を取り出す機器 ルール12：その他の能動医療機器
・その他特別ルール	ルール13：薬剤を伴い補助的に作用する機器 ルール14：性病の予防を目的とした機器 ルール15：医療機器の洗浄を目的とした機器 ルール16：診断用X線フィルム ルール17：動物由来の機器 ルール18：血液パック

出典：JETRO 自己宣言のための CE マーキング適合対策実務ガイドブック



クラス I 低リスク
クラス II a 中リスク
クラス II b 中リスク
クラス III 高リスク

クラス分類により、付則（Annex II～VII）に従い、認証が実施される。

表 2-8 クラス分けと適合宣言の種類

付則 (Annex)	適合宣言の種類	認証方法	第三者認証機関の関与	医療機器の対応クラス				
				クラス I	クラス I*	クラス IIa	クラス IIb	クラス III
II	品質システムによる適合宣言	設計から最終検査まで全体 (ISO13485 に準拠した品質管理体制の確立・維持)	第三者認証機関による審査			○	○	○
III	型式試験による適合宣言	製造業者によって規定された製造工程で製造された代表サンプルについて、欧州整合規格等を用いて、製品が基本要件を満たしているかを評価する。	第三者認証機関による評価				○	○
IV	製品検証による適合宣言	製品毎もしくは製品バッチからサンプルした最終製品を試験し、製品毎もしくはロット毎に認証書を発行する。	第三者検証機関による試験		○	○	○	○
V	品質システムによる適合宣言	製造と最終検査 (ISO13485 に準拠した品質管理体制の確立・維持)	第三者認証機関による審査		○	○	○	○
VI	品質システムによる適合宣言	最終検査 (ISO13485 に準拠した品質管理体制の確立・維持)	第三者認証機関による審査		○	○	○	
VII	製造業者による適合宣言	比較的リスクの低い製品に適用される。基本要件への適合性は製造業者の責任で行われる。	基本要件への適合性は製造業者の責任で行われる。クラス I の場合は認証機関の関与なしに自己宣言できる	○	○	○		

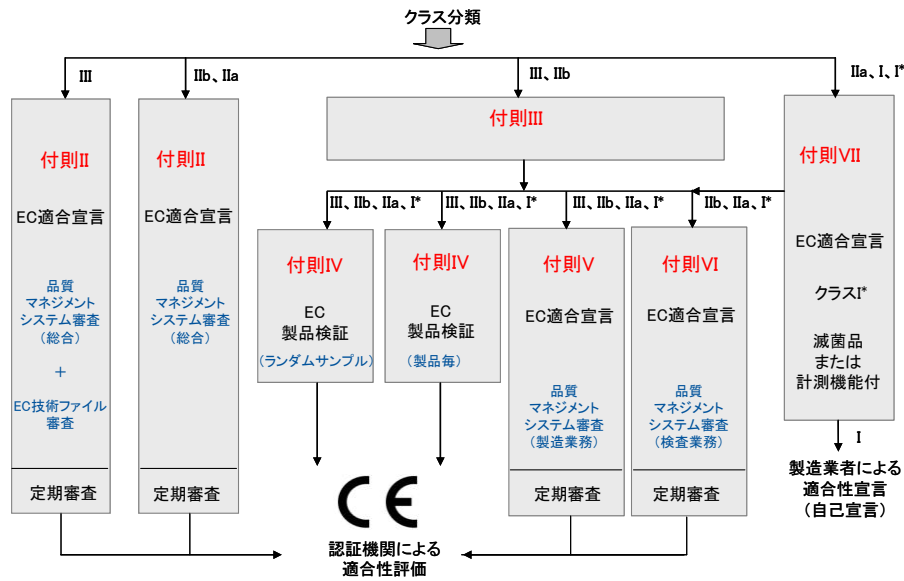


図 2-9 クラス分類と適合性評価

(3). 日本

医療機器は、クラス I ~ IV に分類され、それぞれの機関、方法で承認を得る。

- クラス I : 製造販売届け
医薬品医療機器総合機構による承認
- クラス II : 第三者機関による認証
都道府県による承認
- クラス III : 都道府県による承認
医薬品医療機器総合機構による承認
- クラス IV : 医薬品医療機器総合機構による承認

各クラス別の承認取得方法を「表 2-9 クラス別承認取得方法」に示す。

表 2-9 クラス別承認取得方法

医療機器の区分		高度管理医療機器		管理医療機器		一般医療機器
クラス		細胞組織機器等 *1、クラス4	クラス3	クラス2		クラス1
承認/認証/届出		承認	承認	承認	認証(指定管理) *4	製造販売届
承認・認証不要品目 (通常査察)		-	-	-		都道府県
既承認・認証品目 (通常査察)		-	都道府県	都道府県※2	第三者認証機関	-
承認申請品目	新医療機器	Pmda※2	Pmda*2(政令で定める期間経過後は、都道府県)	Pmda*2(期間経過後に都道府県)*3	-	Pmda*2(政令で定める期間経過後は、都道府県)
	上記以外の医療機器	-	都道府県	都道府県※2	第三者認証機関	-

*1 新医療機器、特定生物由来製品、細胞組織医療機器
 *2 Pmda：独立行政法人 医薬品医療機器総合機構
 *3 第三者認証機関に直ちに移行しないものについては、クラス 3 と同様の扱い。
 *4 第三者認証機関の調査対象は、指定管理医療機器（厚生労働省告示第 112 号等）のみ

出典：大阪府 医療機器 Qms 適合性調査申請を基に作成

適合性調査申請に必要な書類を示す。

表 2-10 適合性調査申請に必要な書類

提出書類	必須	省略条件
1.経過表	○	
2.医療機器適合性調査申請書(施行規則様式第25(2)) 又は 輸出用医療機器適合性調査申請書(施行規則様式第113(2))	○	
3.提出用申請データ出力書面	△	書面申請のとき
4.適合性調査結果通知書又は調査結果報告書の写し →当該適合性調査申請の日から過去2年間に実施されたGmp/Qms調査に係るもの。(他の適合性調査権者等が実施した調査を含む。)	△	調査が実施されていない場合
5.構造設備の概要の一覧表(製造設備器具及び試験検査設備器具の一覧)	○	
6.平面図及び建物の配置図	△	*1
7-A.他の機関等の利用概要	△	利用しないとき
7-B.他の機関の施設の図面	△	*1、2又は、利用しないとき
7-C.他の機関の試験検査設備及び器具の一覧表	△	*2又は、利用しないとき
7-D.利用する他の試験検査機関等の利用関係証明書(写し)	△	*1又は、利用しないとき
14.申請品目の製造販売承認申請書の写し (輸出用医療機器等の製造届に基づく場合は、その届出書)	○	
15.電子申請ソフトによって提出用出力したFD又はCD-R	△	書面申請のとき
16.その他、適合性調査権者が必要とする資料 →大阪府では、以下の書類の事前提出をお願いしております。 ・ 製造方法のフロー図 ・ 品質管理監督基準書(品質マニュアル)の写し ・ Qms組織図(品質管理監督システムの組織体制の説明資料) ・ 文書管理図 ・ 製造工程におけるバリデーションの実施状況(滅菌工程等)	□	

*1 既に同一の書類を大阪府健康医療部薬務課に提出している場合は、省略可。省略する場合は、省略する書類名、それらが添付されている申請書等の種類と提出年月日、業許可番号を備考欄に記載して下さい。

*2 厚生労働大臣の登録を受けた試験検査機関、又は大阪府下で医薬品、医薬部外品、化粧品又は医療機器製造業許可を受けた施設を利用する場合。

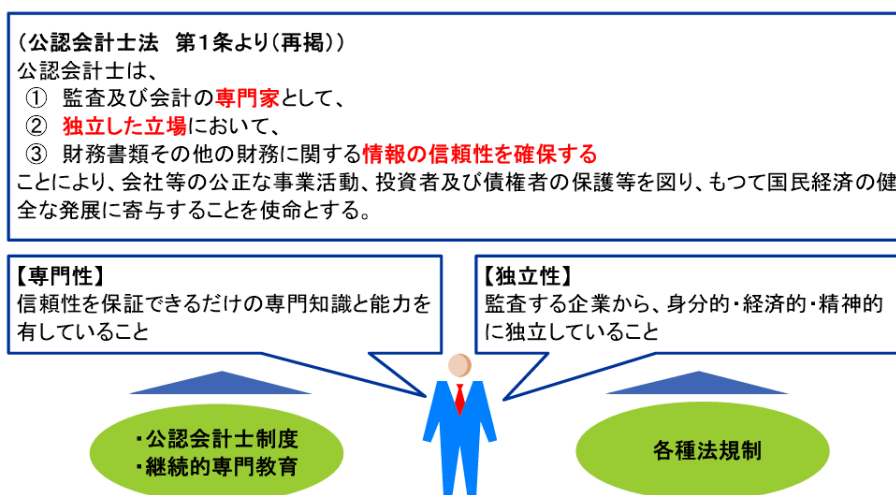
出典：大阪府 医療機器 Qms 適合性調査申請を基に作成

2.5. ソフトウェア品質監査制度(仮称)に参考となる公認会計士制度について

ソフトウェア品質監査制度(仮称)の参考事例として公認会計士制度がある。
公認会計士制度から、第三者検証の参考となる部分について抜粋してまとめた。

2.5.1. 専門性と独立性

検証制度での公認審査官の専門性・独立性の確立に公認会計士制度は参考となる。



有限責任監査法人 トーマツ 「財務諸表監査の概論」より抜粋

図 2-10 公認会計士の専門性・独立性

公認会計士の専門性は信頼性を保証できるだけの専門知識と能力を有している。

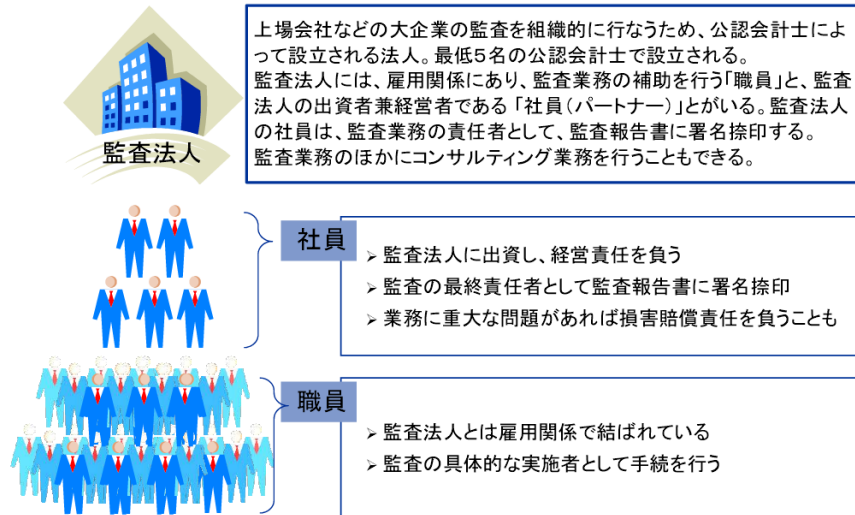
専門知識の判断としては「公認会計士」資格認定や継続的な専門教育を実施する制度で行う。

独立性としては監査する企業から身分的・経済的・精神的に独立していることを、各種法規制により定められている。

ソフトウェア品質監査制度(仮称)においても公認会計士同様の専門性・独立性を維持するために、同様の仕組みを構築する必要があると考える。

2.5.2. 監査法人

検証制度での監査機関にと同様な機能が監査法人である。



有限責任監査法人 トーマツ 「財務諸表監査の概論」より抜粋

図 2-11 監査法人

監査法人とは上場会社などの大企業の監査を組織的に行うため、公認会計士によって設立される法人をさす。法人の設立には最低5名の公認会計士が必要となる。

監査法人には、雇用関係にあり、監査業務の補助を行う「職員」と監査法人の出資者経営者である「社員(パートナー)」とがいる。監査法人の社員は監査業務の責任者として、監査報告書に署名捺印する。

監査業務のほかにコンサルティング業務を行うこともある。

社員の定義

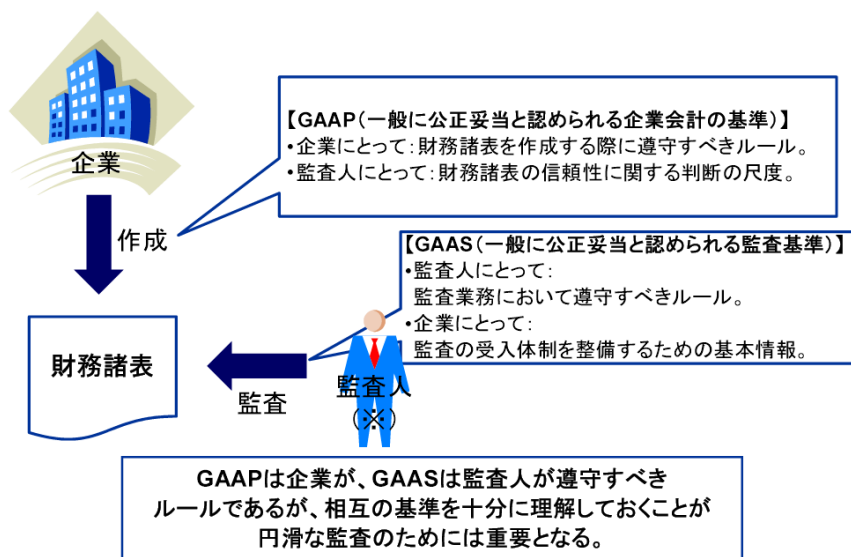
- ・ 監査法人に出資し、経営責任を負う
- ・ 監査の最終責任者として監査報告書に署名・捺印する。
- ・ 業務に重大な問題があれば損害賠償責任を負う場合もある。

職員の定義

- ・ 監査法人とは雇用関係で結ばれている。
- ・ 監査の具体的な実施者として手続を行う。

2.5.3. 会計基準と監査基準

検証制度における審査基準・監査基準のモデルとなるのが会計基準・監査基準である。



有限責任監査法人 トーマツ 「財務諸表監査の概論」より抜粋

図 2-12 会計基準と監査基準

会計基準：GAAP（一般に構成妥当と認められる企業会計の基準）について

- ・ 企業にとっての基準
財務諸表を作成する際に遵守すべきルール
- ・ 監査人にとっての基準
財務諸表の信頼性に関する判断の尺度

監査基準：GAAS(一般に構成妥当と認められる監査基準)

- ・ 監査人にとっての基準
監査業務において遵守すべきルール
- ・ 企業にとって
監査の受け入れ体制を整備するための基本情報

GAAP は企業が、GAAS は監査人が遵守すべきルールであるが、相互の基準を十分に理解しておくことが円滑な監査のために必要となる。

2.5.4. 公認会計士協会

公認審査官協会のモデルとなるのが日本公認会計士協会である。

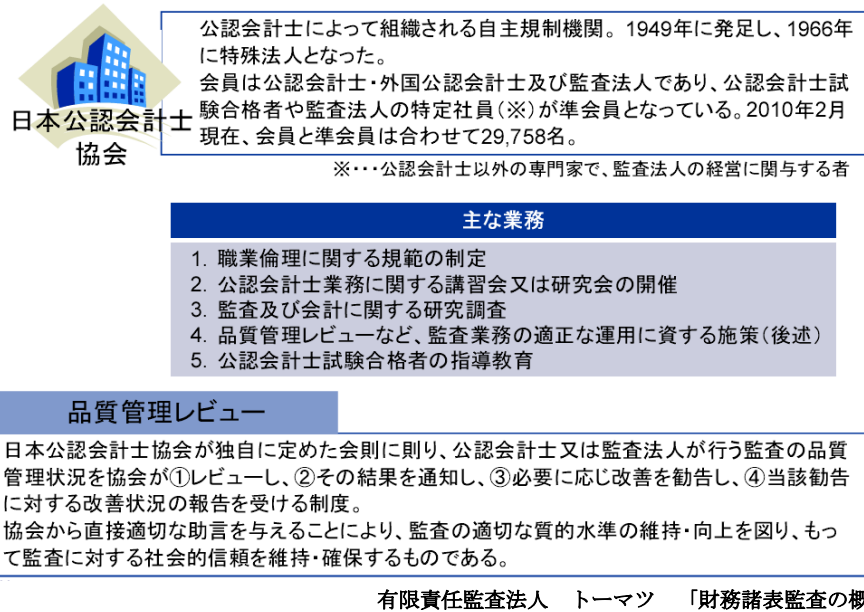


図 2-13 日本公認会計士協会

日本公認会計士協会は公認会計士によって組織される自主規制機関。

1949年に発足し、1966年に特殊法人となった。

会員は公認会計士・外国公認会計士及び監査法人であり、公認会計士試験合格者や監査法人の特定社員(※)が準会員となっている。2010年2月現在、会員・準会員合わせて29,758名

※公認会計士以外の専門家で、監査法人の経営に関与する者

日本公認会計士協会の主な業務

- 1) 職業倫理に関する規範の制定
- 2) 公認会計士業務に関する講習会または研究会の開催
- 3) 監査及び会計に関する研究調査
- 4) 品質管理レビューなど、監査業務の適正な運用に資する施策
- 5) 公認会計士試験合格者の指導教育

品質管理レビュー

日本公認会計士協会が独自に定めた会則に則り、公認会計士又は監査法人が行う監査の品質管理状況を協会が①レビューし、②その規則を通知し③必要に応じ改善を勧告し、④当該勧告に対する改善状況の報告を受ける制度。

協会から直接適切な助言を与えることにより、監査の適切な質的水準の維持・向上を図り、もって監査に対する社会的信頼性を維持・確保するものである。

2.5.5. 公認会計士認定制度

公認審査官の認定制度のモデルとなる。

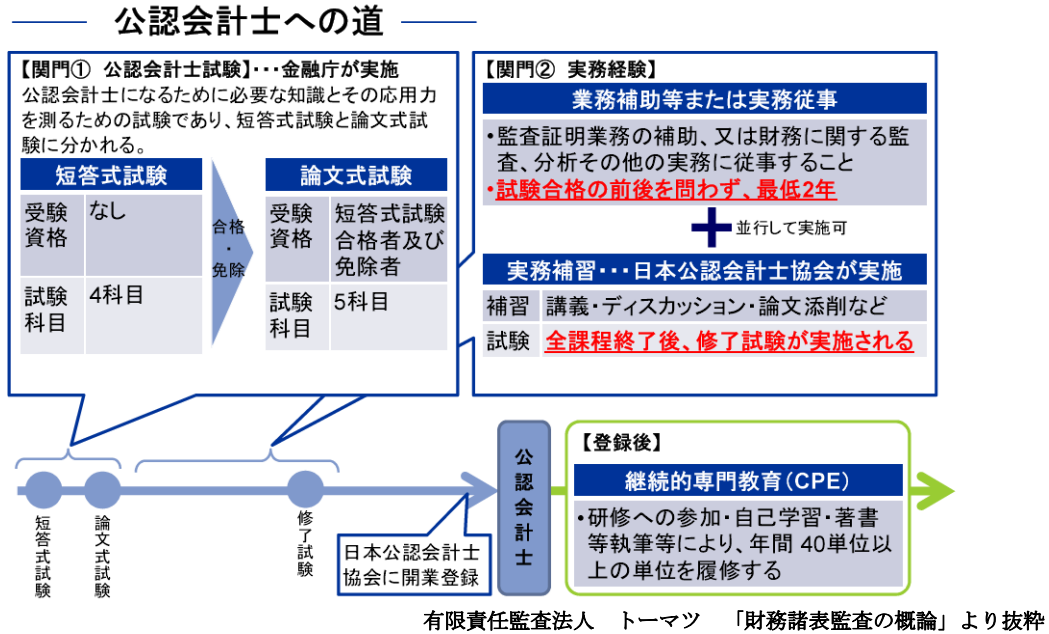


図 2-14 公認会計士認定制度

公認会計士になるためには

関門① 公認会計士試験

公認会計士になるために必要な知識と、その応用力を測るための試験であり、短答式試験と論文式試験に分かれる。

関門② 実務経験

試験合格の前後を問わず、最低2年間は監査証明業務の補助、または、財務に関する監査・分析その他実務に従事すること。

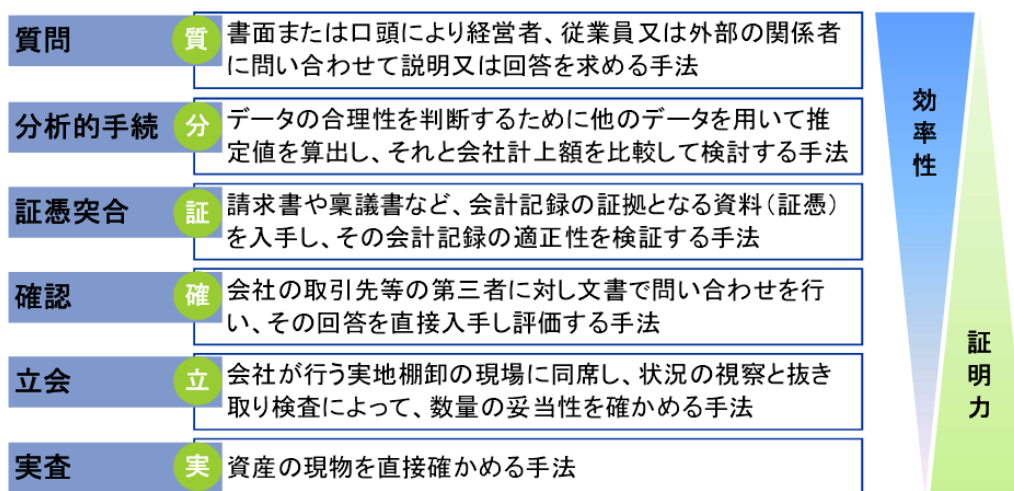
実務補習として講義・ディスカッション・論文添削等の補習を行い、全課程終了後、修了試験が行われる。

関門①、②を通過し公認会計士に登録された後、継続的専門教育(CPE)を毎年行わなければならない。

継続的専門教育は研修への参加・自己学習・著書等執筆により、年間40単位以上の単位を履修することを定められている。

2.5.6. 監査方法とリスクの関係

公認会計士における監査方法を下記に示す。



有限責任監査法人 トーマツ 「財務諸表監査の概論」より抜粋

図 2-15 監査方法

監査方法について

質問： 書面または口頭により経営者、従業員または外部の関係者に問い合わせして説明または回答を求める手法。

分析的手続： データの合理性を判断するために、他のデータを用いて推定値を算出し、それと会社計上額を比較して検討する手法。

証憑突合： 請求書や稟議書など、会計記録の証拠となる資料（証憑）を入手し、その会計記録の適正性を検証する手法

確認： 会社の取引先等の第三者に対して文章で問い合わせを行い、その回答を直接入手し評価する手法。

立会： 会社が行う実施棚卸の減座に同席し、状況の視察と抜き取り検査によって数量の妥当性を確かめる手法

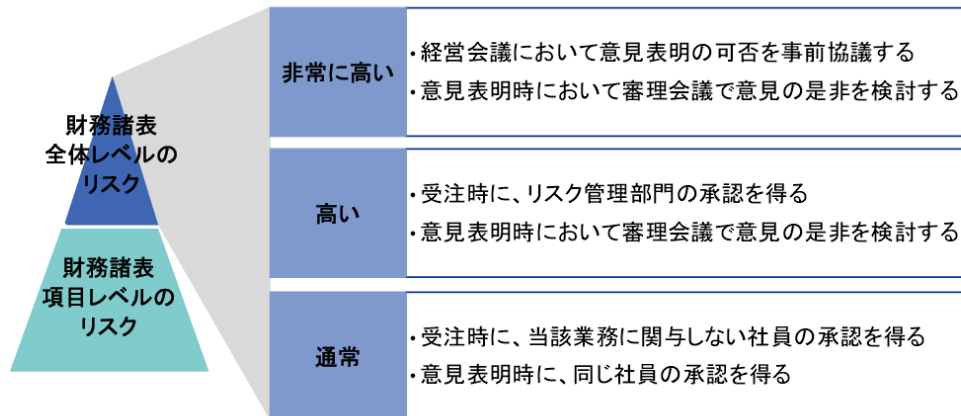
実査： 資産の現物を直接確かめる手法

効率性と証明力のバランスでどの監査方法で監査するかを決定する。

財務諸表監査で監査を行う場合におけるリスク管理をまとめたものが下記である。

- ・「財務諸表全体レベル」のリスクは、監査業務のリスク管理を伴う概念である。

—— リスク管理手法の例 ——



有限責任監査法人 トーマツ 「財務諸表監査の概論」より抜粋

図 2-16 財務諸表監査でのリスク管理の例監査方法のリスク

リスクが非常に高い場合におけるリスク管理

- ・経営会議において意見表明の可否を事前協議する。
- ・意見表明時において審理会議での意見を是非を検討する。

リスクが高い場合におけるリスク管理

- ・受注時にリスク管理部門の承認を得る。
- ・意見表明時において審理会議で意見の是非を検討する。

リスクが通常の場合におけるリスク管理

- ・受注時に、当該業務に関与しない社員の承認を得る
- ・意見表明時に同じ社員の承認を得る

2.6. 海外企業、大学へのインタビュー

2.6.1. HighRely

(1). HighRely の概要

所在地は、Phoenix Arizona。従業員数は、約 30 人。DER は 8 人。

コンサルタント DER の業務、トレーニング、製品開発のコンサルティング、戦略的ソリューションの開発、受託開発、ツールの販売等を行う。トレーニングメニューとして、JumpCert™があり、今までに 11,000 人以上が受講している。

ツール

チェックリストツール、プロジェクト管理ツール、トレーサビリティツール、アドオンツール等

業界別売上比率

航空宇宙：50%

医療機器：20

産業用制御機器：20%

その他：10%（原子力、通信、軍事等）

パートナー企業

Esterel Technologies、Green Hills Software、Vector Software、Telelogic、PolySpace、ALDEC、axosoft 他

(2). インタビュー概要

Phoenix について

HighRely によると、Phoenix には、1 万人近くのセーフティクリチカルエンジニアがいるという。Honeywell、General Dynamics、Rockwell Automation などの航空機関連の企業があり、航空機エンジン、航空機情報システム、航空機関連製品、航空管理システムなどの製品が開発されている。10~20 社の検証企業があり、そのほとんどは従業員 5 名程度の小規模企業だという。

Phoenix の空港はまた、US Airway と Southwest の 2 つの航空会社のハブ空港となっており、3.5 時間で全米の主要都市へアクセス可能。

DER について

以前は、政府が業界の審査をしていたことがある。政府のソフトウェアの知識がない審査員が審査をしていた。しかし、審査員が複数の企業の情報にアクセスできることから情報漏れが起こった。このような背景もあり、産業界の FAA への信頼性が揺らいだ。そこで考えられたのが DER の制度である。DER は、産業界が自分自身で製品を監査する制度と言える。

DER はメーカー（審査を受ける企業）に雇用されるが、報告をする相手は、FAA となる。FAA が DER の業務を厳しく管理することで DER の信頼性を担保している。また、DER が審査をした審査書類のすべて（ソースコード等）が、FAA に渡ることではないため、審査対象企業や製品の機密事項が漏れることはない（FAA は審査をするがすべての書類を得るわけではない）。

FAA の「Aircraft Certification Office」(ACO) の職員が個々の DER を管理する。ACO は、Los Angeles、Seattle、Chicago、Kansas、Oklahoma、New York、Phoenix、Fort-worth、Boston、Miami、Dallas など 12 ヶ所にある。

DER は個人が持つ資格であり、その取得には数年を要する。資格は毎年更新する必要がある。更新時にクラスを受講する必要がある。FAA は DER のレポートを監査し、問題が有る場合資格を剥奪する。約 300 人の DER が登録されている。

欧州には DER の制度はない。EASA には約 100 人の検査官がいて、検査官が審査をする。一般的な話として、米国は、産業界が強いが、欧州は政府が強い。

DO-178B について

DO-178B は、プロセスベースの検証であると同時に、製品ベースの検証であると言える。これに対し、CMMI 等はプロセスのみの認証であり、製品に関する認証ではない。DO-178B では、開発製品の開発プロセスが詳細に定義されており、DO-178B の開発プロセスと開発製品の開発プロセスの間のギャップ分析がなされ、その差異が修正される。ギャップ分析には、少なくとも 2~3 週間を要し、その修正にはさらに数ヶ月を必要とする。

一方、ソフトウェアのすべてのコードで、1 行ごとに、各コードが存在する理由、バックワードトレーサビリティなどの検証が要求される。

DO-178B では、Level A の場合、初回は 40~50%コスト増となる（評価項目を減らせば、10%程度のコスト増で抑えることも可能）である。2 回目からは、保守費用が減ることや再利用性が増すことで、コストは下がる。

DO-178B の改訂版となる DO-178C は現在策定中であり、2011 年にリリースの予定。欧州の ED-12B は DO-178B と 99%同じもの。

FDA について

FDA の規模は FAA に比べて小さい。フォーカスをしているのは、医療機器というよりも、医薬品（ドラッグ）である。40~50 年の歴史のある組織であり、いわば、聴診器の時代の組織とも言え、医療機器は、シンプルなものという認識がまだあるように思える。

しかし、実際には、インフュージョンポンプなどは、10 万行以上のソフトウェアで制御される複雑なシステムとなっている。HighRelly では、Baxter、CardinalHealth、Hospira などが開発する機器のソフトウェアを開発した実績がある。

FDA には、FAA の DER のような制度はない。審査員の数も多くなく、ソフトウェアにも精通していないため、検証業務はメーカー依存となっている。FDA の 510(k)は DO-178A の簡略版と言える。

検証システムの相違について

FDA は監査するだけであり、開発の詳細に関与することは好まない。メーカーが策定したプロセスに従い、検証をすれば良いという立場。

FDA は、「Innocent until prove you guilty」（有罪が証明されるまでは無罪）の立場をとる。

IEC の企画（61508 など）の厳格さは、FDA と FAA の中間にあり、プロセスを規格として提示するが、フレームワークとしての提示であり、変更が許される。DO-178B と IEC 61508 は、カバー範囲がほぼ同じだが、要求度合が異なると言える。

FAA の規格（DO-178B）は、厳格であり、740 のクライテリア（Criteria）と 66 の目的（Objective）を絶対守らないといけない。

それ故、航空機は安全と言えるが、それでもソフトウェアに 100%はない。検証をしていれば、例え、不具合が起こった場合でも、原因を発見して、リスクを軽減することはできる。

FAA は、「Guilty until proven innocent」（無罪が証明されるまでは有罪）の立場をとる。

NASA の IV&V は DO-178 に似ているが、20%程度の相違がある。特にテストのプロセスが異なる。DO-178B の方が強力と思う。

その他

DO-178B は、仕様どおりに製品が開発されているかを確認する（製品仕様検証）ものであり、要求仕様の妥当性を検証（妥当性検証）するものではない。

仕様の正しさ（妥当性検証）は、システムの規格であり、ARP-4754 の守備範囲となる。DO-178B や DO-254 と組み合わせることで、システム全体の妥当性と仕様の検証が可能となる。

DO-178 や DO-254 のインダストリグループがあり、情報交換の機会提供、セミナーやコンファレンスの開催、ホワイトペーパーの提供などがされている。

<http://www.do178site.com>
<http://www.do178blog.com>
<http://www.do254site.com>
<http://www.do254blog.com>

2.6.2. Safeware Engineering Corporation

(1). Safeware Engineering Corporation の概要

所在地は、Seattle Washington。1992 年創業。現在の人数は 8 人。航空、宇宙(NASA、JAXA)、軍、自動車、医療、鉄道、化学などが顧客。

(2). インタビュー概要

DO-178 は、必ずしも安全を考慮したものとは言えない。ソフトウェアの設計仕様を検証するものであり、システムの仕様や要求仕様を検証するものではない。

要求仕様 (Requirement Specification) と設計仕様 (Design Specification) の相違を理解することが必要となる。システム要求仕様は、システムに求められる要求を記述するものであり、システム要求仕様の検証では、求められる仕様の妥当性を検証 (Validation) することとなる。

設計仕様の検証は、仕様どおりに作られているかを検証することであり、安全を考慮した妥当性を検証することではない。

航空機と自動車は製品の特性が元々違う。航空機で事故が起こらないのは、設計の変更が少ないこと、同じロジックを再利用することにある。航空機の設計は保守的であり、安全を犠牲にして、新技术を積極的に採用することはしない。これに比べ、軍事技術は、新たな技術を多く採用し、複雑化している。この結果、安全性が保持できず、悪循環に陥っている。このための対策として、「System Safety」の考え方を進めている。MIL-STD-882 はそのための規格である。新規機能を追加する車やロボット等には MIL-STD-882 の方が向いているのではないかと思う。

車載システムも新技术採用により、複雑性が増し、安全性の確保が困難になっているように思える。コンポーネント間のインタラクションで言えば今や車の方が複雑とも言える。

ここでいう、複雑性とは、コンポーネント間のインタラクション (相互作用) の複雑さの度合いを意味する。ソフトウェアの観点で言えば、ソフトウェアの中身ではなく、ソフトウェアの入出力に注目することが、「System Safety」のアプローチでは重要になる。

安全を阻害する原因の多くは、ソフトウェアのエラーではなく、システム要求仕様の問題であることが多い。このため、安全はシステムエンジニアの領域に依るところが大きいと言える。この意味でも DO-178 は安全のための規格とは言えない。システムレベルの検証をする規格には ARP-4754 があるが、古い方法であり、一つ一つのコンポーネントを見ているが、コンポーネント間のインタラクションは見えていない。このため、ARP-4754 では、ファンダメンタルな問題は解決できない。

セーフティーケースは、「なぜ安全なのか」の議論 (Argument) に焦点を当てているのが問題だ。なぜ安全なのかを議論しても、事故は起こる。「なぜ安全でないのか」という視点で議論しないと安全には役に立たない。

コンポーネント間のインタラクションに注目してシステムを解析する手法に、STAMP (Systems-Theoretic Accident Modeling and Processes) と STPA (STAMP based hazard analysis) がある。

FTA (Fault Tree Analysis) や FMEA (Failure Modes and Effect Analysis)、HAZOP (Hazard and Operability Study) は 50 年代から使われている古い手法でハードウェアの分析には使えるがソフトウェアの分析には向いていない。STAMP と SPTA は、1990 年に開発された新しい手法である。

JAXA (独立行政法人宇宙航空研究開発機構) の「こうのとりのとり」(HTV) や「きぼう」(JEM)

の開発でも使われた。HTV の開発では、FTA の解析を完了していたが、STAMP による分析で新たな問題点が発見された。MDA (アメリカミサイル防衛局) の迎撃ミサイルの開発において、誤発射の可能性の有る問題を多数発見したことがある。

分析ツールとしては、SpecTRM がある。TCAS II (航空機の衝突防止システム) の仕様書作成を FAA から依頼された際に、開発した記述ツールが SpecTRM の原型となっている。要求仕様の妥当性を分析するツールである。

SpecTRM はモデルベースの開発システムであり、モデル (コンポーネント) 間のインタラクション (やりとり) を分析する。分析は、要求仕様を元に行うため、コンポーネントレベルの設計仕様は必要ない。コンポーネントレベルの入出力に注目し、システムの要求仕様の妥当性を分析する。

分析は要求仕様を元に行う。要求仕様を得るために関係者からの聞き取りを行う場合もある。また、要求仕様がない場合は設計仕様からリバースエンジニアリングをし、要求仕様を作成することもある。SpecTRM にはモデリングのためのツールと半自動で分析をする機能が備わっている。

SpecTRM (Specification Tools and Requirements Methodology) の概要

安全システムとソフトウェアの仕様作成を支援するツールセット

- ・開発の早い段階でエラーを発見する。
- ・低コストで、システム設計への影響が少ない修正を可能にする。
- ・システム設計とドキュメンテーションにより、要求仕様をトレースし、論拠を得る。(安全制約を含む)
- ・要求仕様の設計仕様への組み込みを、開発の初期段階から行う。開発の後半では効果的な対応は難しく費用もかかる。

人間をシステムの 1 つとして捉える研究もある。この場合、人間 (ユーザ/オペレータ) は、コマンドを発するモデルの 1 つとなる。人間のモデル (行動) は、ワーストケースシナリオ (人間のふるまいが引き起こす最悪のシナリオ) を元にモデル化される。

Socio-technical system と呼ばれる研究があり、ハードウェア、ソフトウェア、ヒューマンファクタ、組織を考慮してシステムを分析する。例えば、航空機がオーバーランをした原因を調査するには、航空機のシステムだけでなく、ヒューマンファクタや組織の意志決定などのプロセスを考慮して分析する必要がある。

2.6.3. Boston Atlantic Technology,INC./Software Quality Consulting,Inc.

(1). Boston Atlantic Technology の概要

Boston Atlantic Technology は Boston 郊外にある従業員 5 人の企業。

医療系 SW の開発、検証サービス。現在は医療系にフォーカスしているが原子力、航空のセーフティクリティカルな SW の開発経験もある。米国に参入する企業支援を行う。

Software Quality Consulting について

Boston Atlantic Technology のパートナー企業、日本の医療機器メーカーのコンサルティングを実施中。NASA で IV&V の専門家以外に対する入門コース (Software V&V for Mission critical system) を受託して実施している。

(2). インタビュー概要

FDA の認証はプロセス認証で、製品認証ではない。開発のプロセスが正しければ、開発された製品の品質も高いはずだという考え方に依っている。これに対し、FAA の航空機やそのシステム、部品の認証では、すべてのコードがテストされる製品認証となっている。医療機器の認証は、自己宣言であり、第三者検証を必要としない場合が多い。

医療機器は多種多様なのでシステムチェックなアプローチによる規制が難しい。また、FDA にはソフトウェアの専門家がいなかったため書類形式の審査になっていることは問題である。

FDA の審査は、プロセスを重視し、提出された書類が「Reasonable」（もっともらしい）であることが求められる。

そもそも、1970 年頃までは、医療機器ではソフトウェアを必要としなかった。その後、医療機器にもソフトウェアが使われるようになり、1980 年前半に、事故が散見されるようになった。これを機に、FDA でも医療機器のソフトウェアの安全性に眼を向けるようになった。

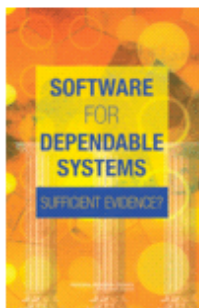
最近の出来事として、インシュリンポンプの故障の問題を機に、FDA はセーフティーケースの提出を求める事にした（2010 年 7 月から）。今後は、セーフティーケースが別領域に適用される可能性がある。米国ではセーフティーケースは比較的新しい手法である。セーフティーケースは欧州において多く採用されているが、米国においては、原子力のシステム以外にはほとんど採用されていない。

FDA のガイドラインでは、使用したツールやソフトウェアの検証が求められる（コンパイラ、リンカは対象外）。バグトラッキングツールやスプレッドシートにも検証の必要がある。その要求度合いは、使用したツールやソフトウェアのリスクにより異なる。スプレッドシートなどのソフトウェアのリスクは低く、フラッシュ書込みツールなどのリスクは高くなる。

2.6.4. Massachusetts 工科大学

(1). Massachusetts 工科大学 Daniel Jackson 教授の概要

米国科学アカデミー（NAS : National Academy of Sciences）が助成(数 M\$程度、3~4 年)したプロジェクト「Software for Dependable Systems: Sufficient Evidence?」のチェアを努めた。



Software for Dependable Systems: Sufficient Evidence?

Daniel Jackson, Martyn Thomas, and Lynette I. Millett,
Editors, Committee on Certifiably Dependable Software
Systems, National Research Council

ISBN: 0-309-66738-0, 148 pages, 6 x 9, (2007)

This free PDF was downloaded from:
<http://www.nap.edu/catalog/11923.html>

米国の複数の規制当局が、認証取得コストに見合う有効性があるか疑問を抱いた。商業飛行、航空、エネルギー、公共輸送、医療機器などの分野での認証取得に膨大な仕事量とコストがかかっているが、品質やディペンダビリティの向上に役立っているか疑問が有った。どのような証拠があれば、このシステムがディペンダブルだと言えるかというのがこの研究である。

Jackson 教授によると、研究結果で提案したアプローチの発表後、業界はゆっくりとではあるが変わりつつあると感じるといふ。

Jackson 教授は、形式手法、Alloy の提唱者でもある。

(2). インタビュー概要

第三者検証が、製品の検証なのか、プロセスの検証なのかで考え方が変わってくる。プロセスの検証の場合は、多くの場合、規格などに基づく、プロセス認証取得になる（CMMI、ISO や IEC の規格等）。これにはそれなりの価値がある。一方、製品の第三者検証では、何を、どのレベルで検証するかが課題となる。何か怪しい（Smell Bad）というレベル（モジュールのアイソレーションなど必要な対策がとられているかなどで判断できる）か、自信がある（Confidence）レベルまでなのかでは、その意味がまったく違う。

次に、何のためにソフトウェアのテストを行うかを考える際、2 つの目的が挙げられる。1 つはテストにより、バグを発見すること、いま 1 つは、バグを発見できなかったことを証

明することであり、後者はエビデンスとなる。このためのテストは、ユーザプロファイル（利用環境）からテストケースを作成し、テストを行い、統計的に妥当な主張（Plausible Claim）に到達する必要がある。高い信頼レベルを得るためには、あまりにも多くのテストが必要となり実用的でない。

例えば、90%の信頼レベルを得るには、5倍から6倍のテストが必要となる（1000回に1度のエラー率を90%の信頼レベルで得るには、5000回から6000回のテストが必要）。高信頼性のシステムでは、 10^6 ~ 10^7 回のテストが必要となる。

ましてや、第三者による検証では、第三者が開発者より深い製品知識を持つことは難しく、中立性を求める必要があるとは言え、第三者による検証（テスト）は、時間と費用がかかり過ぎ実用的でない（Economically Feasible or not?）。そのため、少しコストはかかるが、証明（proof）という方法を採用することが考えられる。テキスト（コード）を分析し、すべての可能なシナリオでの検証をする。これは可能である。しかし、この場合でも課題となるのは、完成した複雑なシステム（ソフトウェア）を第三者検証者に渡しても、そのシステムが、最初から検証を考慮した設計をしていない限り、第三者による検証は難しいことだ。

ソフトウェアが最初から検証を考慮した設計になっていない限りは、開発者より開発対象となるソフトウェアの情報をもたない第三者検証者が検証をするのは、現実的でない。

セーフティーケース（デペンダビリティケース）のアプローチでは、開発当初から開発者が検証者と係わりながらセーフティーケースを作成していくので、製品検証が可能なアプローチと言える。

プロセスアセスメントではサンプリングによる検証に意味があるが、製品のアセスメントでは、サンプリングの検証はあまり意味がない。

航空・宇宙はかなり品質が良い。NASAの作っているものは良い。医療機器のシステムで小さい会社の作っているものについては、品質が悪いという印象。小規模の企業が開発する医療機器は単独で小規模なものが多く、システムに組込まれて動作するという概念がしっかりしていないのではないかと思われる。

2.6.5. NTS Inc.

(1). NTS Inc.概要

Los Angeles 郊外 Culver Cityにある製品のテストサービスを行う会社。テストサービスには、製品の動作環境(温度、湿度、気圧、振動、音響)試験、EMC/EMI等の試験、標準への適合試験、加速寿命試験等がある。

顧客の要求に合わせてテスト Lab を作るサービス。テスト Lab を運営するサービスもある。例えば HP ヒューストンで 100 人規模の Lab を作ってサービスを提供している。

(2). インタビュー概要

自動車関係は標準に協調性がない。航空、軍事、宇宙、医療は標準に協調性があるが、自動車は各社バラバラだ。

航空のソフトウェアに関連するテストサービスはあまりやっていない。システムテストではソフトウェアに関連する事もある程度。

航空の場合、テスト仕様はユーザが提供する

Logo プログラムを立上げるサービスをしている。ゲーム機器の周辺機器の認定ロゴプログラム等。同社が試験を行っているが、最終的な認証はメーカーから出る。(合格した物の一つは残していくような仕組みにしないと、後で廉価変更版ができた時等の認証が難しくなる)

ツールは、主に 3rd Party のツールを使う。

標準への適合試験ツールを作成し、認定機関に認証してもらい、ユーザに認証前に使う自己確認ツールとして売ることがある。

2.7. 第三者検証取り組み状況調査

第三者検証検討部会(ソフトウェア品質監査制度部会の2010年度時点の旧名称)委員所属企業等にアンケートによる第三者検証についての取り組み状況について調査を実施した。

アンケート調査は第三者検証を受ける企業10社(ユーザ企業と略す)、第三者検証を行う企業6社(検証サービス企業と略す)について調査を実施した。

※本アンケート調査は2011年1月11日に第三回第三者検証検討部会にて依頼。

2.7.1. 第三者検証取り組み状況に関するアンケート項目

下記項目についてアンケート調査を実施した。

1. プロファイル情報 (製品ドメイン、総開発費、総プロジェクト数、技術者数等)
2. 第三者検証を理解していますか
3. 既に第三者検証を実施している場合の具体例
4. 第三者検証のニーズがありますか、またその理由は
5. 第三者検証をしておけばよかったと思うことはありますか
6. 第三者検証が必要な国と製品は
7. 第三者検証で重要な検証項目は何ですか
8. 第三者検証にどの程度コストをかけてよいと考えますか
9. 第三者検証に関する社内制度・規定・研修等があれば教えてください
10. 第三者検証を実施する場合の課題は何ですか(人、モノ、金)
11. 上記の課題解決に向けた取り組みはありますか
12. 第三者検証に関わるどのようなツールがあると効率的になるとおもいますか
13. 第三者検証サービス事業者が国内に在る必要性を感じていますか
14. 国内にある第三者検証サービス事業者にとって重要な要件はなんだと考えますか(独立性、ドメイン知識・経験、海外での認知度等)
15. 国内にある第三者検証サービス事業者にはどの程度の仕事を出すことになりませんか(製品ドメイン、プロジェクト数)
16. 機能安全やプロセスで認証が要求されるような製品がありますか(製品ドメイン)
17. 機能安全やプロセス認証を行っているサービス事業者にはどの程度の仕事を出していますか(プロジェクト数)

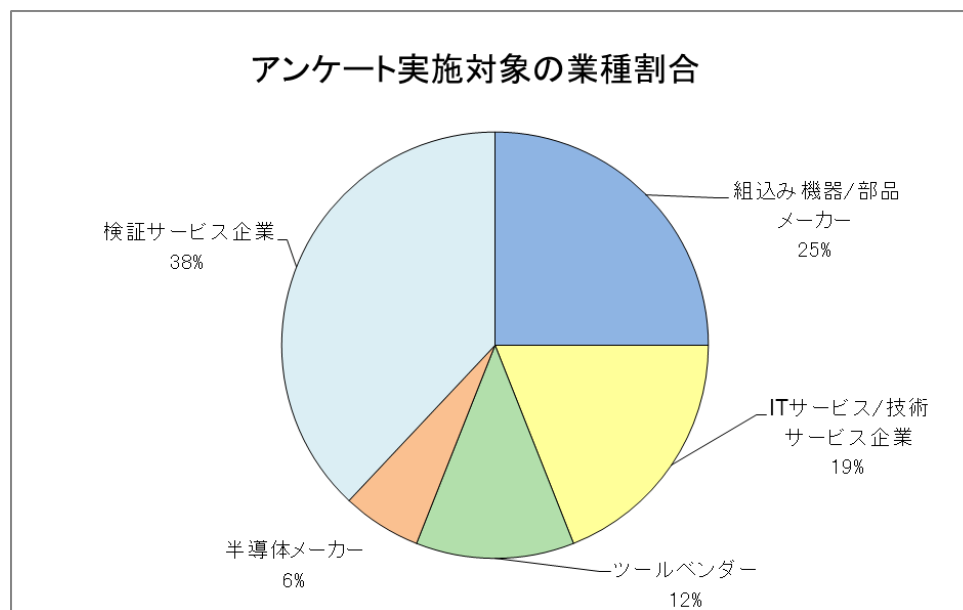
2.7.2. アンケート調査結果

アンケート調査結果を設問毎に分析したものを記載する。

(1). アンケート実施の業種について

今回アンケート実施した企業の業種の割合を下図に示す。

対象の約6割が第三者検証を利用するユーザ企業であり、4割が検証サービスを実施する側の企業である。



組込み機器/部品メーカー	4社
ITサービス/技術サービス企業	3社
ツールベンダー	2社
半導体メーカー	1社
検証サービス企業	6社

(2). 設問2：「第三者検証を理解していますか」について

第三者検証の理解については、ほぼ100%の企業が理解しているとの回答であった。

理解している	16社
理解していない	0社

第三者検証については全ての企業において理解しているとの回答であり、第三者検証に関して意識の高さが伺える。

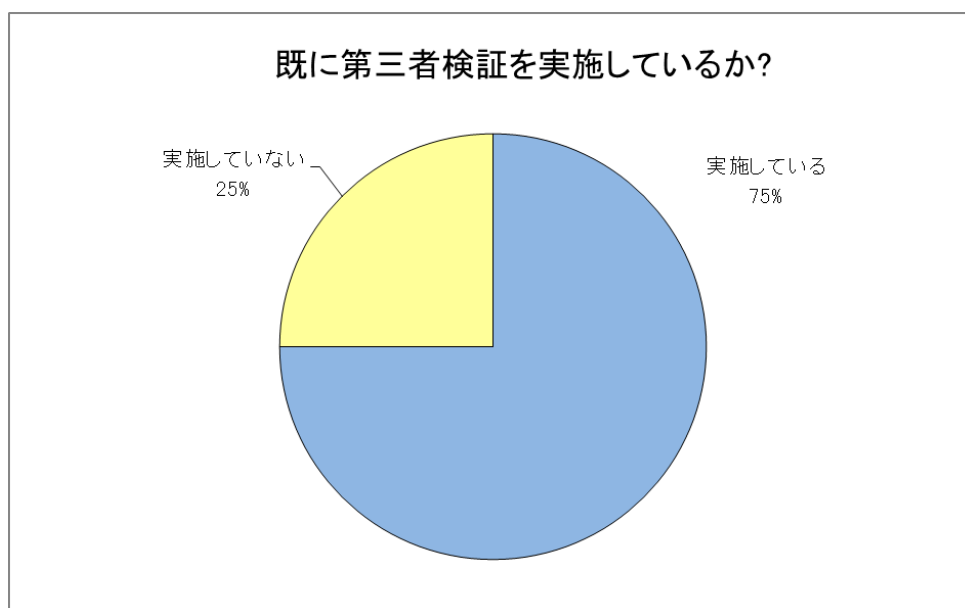
第三者としてのキーワードとして「独立性」「IV&V」「妥当性」「品質保証」「妥当性(Validation)」などが挙げられた。

アンケートの詳細を確認すると、業種毎に第三者検証に関する認識は多少異なっている。

大まかに分類すると、検査工程を外部で行うものと、妥当性確認、監査などの意見があった。

(3). 既に第三者検証を実施しているかについて

「設問 3: 既に第三者検証を実施している場合の具体例」の回答から、既に第三者検証を実施しているかについて下図に示す。



実施している : 12 社
実施していない : 4 社

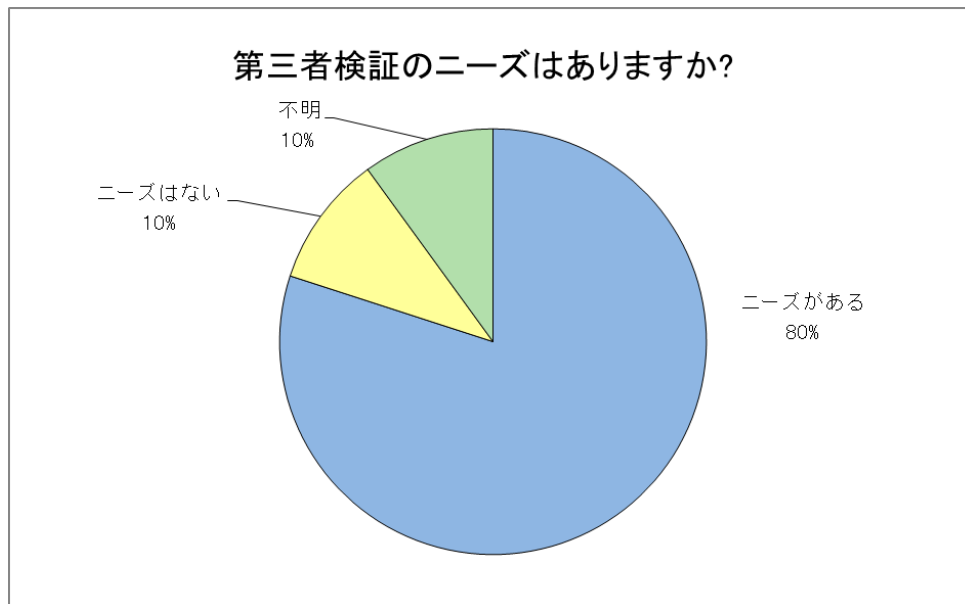
実施対象製品として、自動車制御、プリンタ・複合機、医療機器、IT 製品、航空、防衛、流通、通信が挙げられた。

実施例としては、「IV&V」、「CMMI によるプロセス管理」、「社内独自組織による検証」が挙げられた。

ユーザ企業で「第三者検証を実施している」との回答があった 6 社中 3 社は自社内で検証を実施している。

(4). 設問 4 : 「第三者検証ニーズがありますか、またその理由は」について
第三者検証のニーズについてユーザ企業・検証サービス企業に分けて下図に示す。

・ ユーザ企業 (10 社結果)



ニーズがある :	8 社
ニーズはない	1 社
不明	1 社

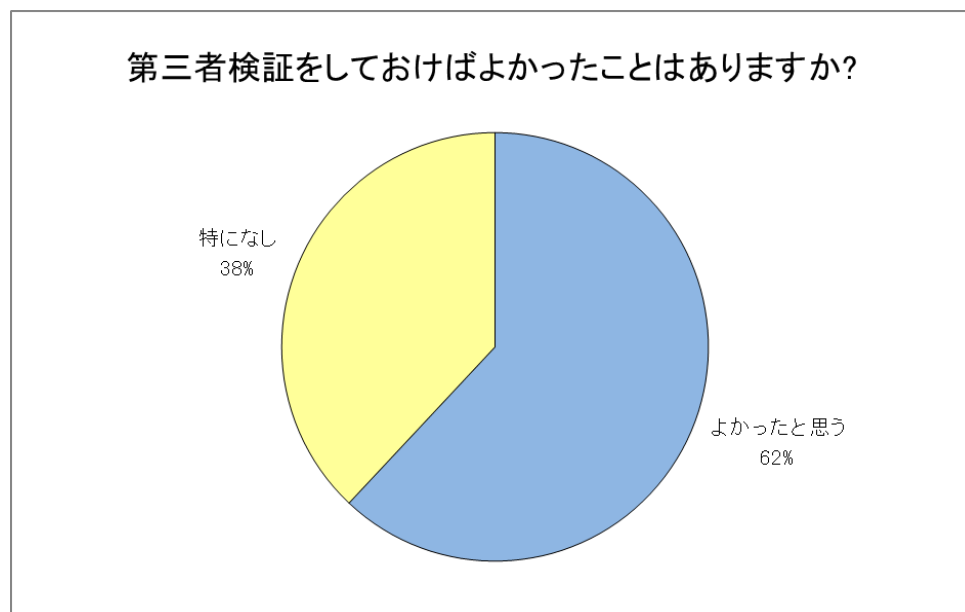
・ 検証サービス企業

ニーズがある	6 社
ニーズはない	0 社

主な理由については「顧客に対しての品質の説明」「自社品質の向上」などが挙げられた。

(5). 設問 5 : 「第三者検証をしておけばよかったと思うことはありますか」について

第三者検証を実施してよかったことがあるかとの設問で、約 6 割が第三者検証をしておいて良かったと回答をしている。



よかったと思う	10 社
特になし	6 社

主な理由としては

「顧客に対する信頼性」「テスト技術が不足しているプロジェクトの技術力向上」「統合したシステムでの不具合での責任区分の明確化」「輸出の認証取得」などが挙げられた。

(6). 設問 6 : 「第三者検証が必要な国と製品は」について

対象国としては 「自社製品輸出対象国」「ヨーロッパ」「米国」「中国」が挙げられた。対象製品としては「自動車」「安全が求められる製品」「顧客より高い品質を求められている製品」「人命に関わるシステム」「インフラ等の社会基盤」「機能安全対象の製品」等が挙げられた。

(7). 設問 7 : 「第三者検証で重要な検証項目は何ですか」について

業種により回答のばらつきはあるが、「安全規格」関連についての回答が多かった。検証項目としては「安全規格(自動車であれば ISO 26262)等の規格で定められた項目」「製品開発部門では検証しにくい項目」「専門的な知識を必要とする項目」「IV&Vに関する項目」「対象の妥当性確認」等が挙げられた。

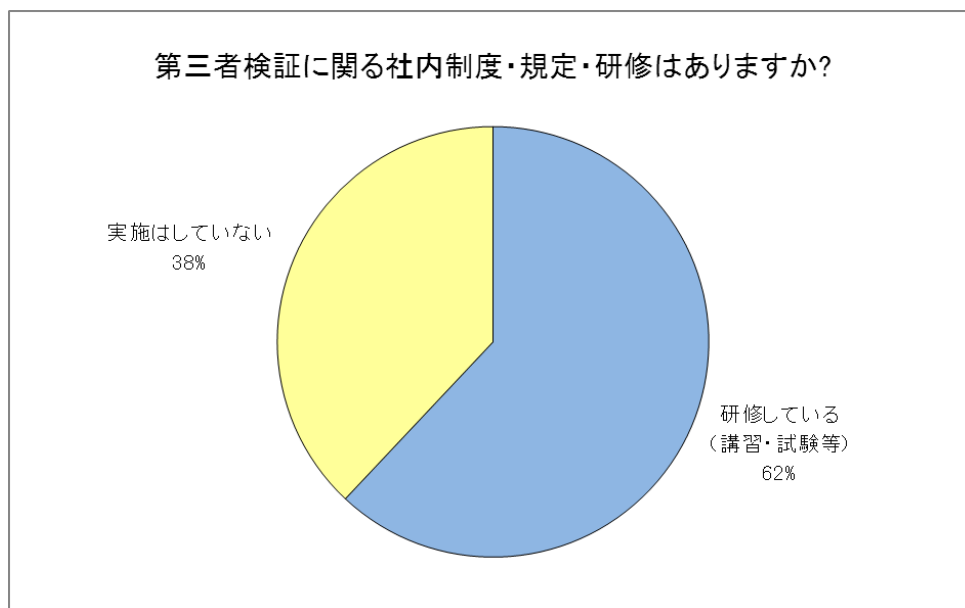
(8). 設問 8 : 「三者検証にどの程度コストをかけてよいと考えますか」について

製品によりコストは異なるとの回答が多く挙げられ、製品ドメイン(どこで使われる製品か)によりコストは変わるとの回答が多かった。

あえて、数値を上げると開発コストの 10%程度との回答が 3 件挙げられた。

(9). 設問 9 : 「第三者検証に関する社内制度・規定・研修等があれば教えてください」について

現在第三者検証に関わる制度・規定・研修を実施している企業は全体の 6 割程度となった。



研修をしている(講習・試験等)	10 社
実施はしていない	6 社

主な研修では「品質管理部門による講習」「社内資格試験」「新人教育カリキュラム」「IV&V教育」が挙げられた。

(10). 設問 10：「第三者検証を実施する場合の課題は何ですか (人、モノ、金)」について
第三者検証の枠組みに関する意見が多く見受けられた。また、「人材育成」「費用」などが挙げられた。また、検証を行うためにツールの必要性も挙げられた。

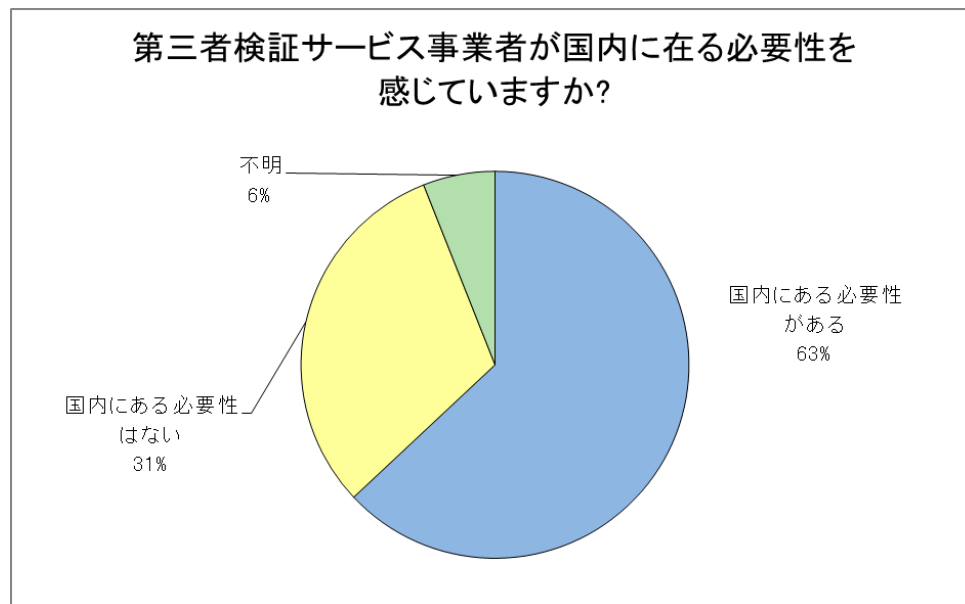
(11). 設問 11：「上記の課題解決に向けた取組みはありますか」について
主な取り組みとしては「IPA の活動に参加」「社内検証技術力の強化」「IV&V プロセスの明確化」「社内に第三者検証チームを作っている」などが挙げられた。

(12). 設問 12：「第三者検証に関わるどのようなツールがあると効率的になるとお考えですか」について
「テスト管理」「プロセス管理」「品質解析」が挙げられており、テスト作業 (テストの自動化、コードの自動チェック等) の効率化するツールとプロセスを管理するツールの要望が多く挙げられた。

(13). 設問 13 : 「第三者検証サービス事業者が国内に在る必要性を感じていますか」について

第三者検証サービス事業者は国内に在る必要性があるとの回答が6割強となった。

国内に在る必要性の理由として「迅速な対応」「言語・習慣」「国際競争力維持」が挙げられた。なお、国内に在る必要はないとの回答には上記に挙げた必要性がクリアされていればとの条件付きである場合が挙げられた。



国内にある必要性がある	10社
国内にある必要性はない	5社
不明	1社

(14). 設問 14 : 「国内にある第三者検証サービス事業者にとって重要な要件はなんだと考えますか」について

「ドメイン」「国際的な認知度（権威）」「技術力」などが挙げられている。

特に、ドメインを挙げている意見が多いことから、製品要件の重要性が伺える。また、国際的に通じる仕組みであることが求められている。

(15). 設問 15 : 「国内にある第三者検証サービス事業者にはどの程度の仕事を出すことになりますか」について

現状では判断不可能との回答であった。

(16). 設問 16 : 「機能安全やプロセスで認証が要求されるような製品がありますか」について

「自動車」「安全制御機器」「交通」「金融系システム」「組込み OS」「官公向け組込みシステム」などが挙げられた。

(17). 設問 17 : 「機能安全やプロセス認証を行っているサービス事業者にはどの程度の仕事を出していますか（プロジェクト数）」について

未回答

3. 調査結果まとめ

3.1. 第三者検証の現状について

組込みシステムの海外における第三者検証の現状については、第三者検証が義務付けられている米国連邦航空局(FAA)の航空機分野、米国食品医療局(FDA)の医療機器分野を中心に、制度の概要、認証プロセス、関係する技術基準や法律・法令、検証に係るコストなどについて調査した。

調査結果として、FAA の制度では、企業の機密情報の秘匿性を担保しつつ独立性を確保する仕組みとして、DER(Designated Engineering Representative)制度が運用されていることなど、企業や産業界の要求に応じて制度に工夫がされていることが把握できた。

第三者検証に関しては様々な国際規格が規定されていることが把握できた。

- ・航空機分野：「DO-178B」、「DO-254」「ED-12B」「ED-80」「ARP4761」「ARP4754A」
- ・医療機器分野：「ISO 13485」「IEC 62304」「IEC 62366」「IEC 60601-1-9」

国内他分野における第三者検証事例としては、制度の目的、要求される独立性や専門性、国際的な相互運用性の観点で類似性の高い財務諸表監査制度(会計監査制度)について整理した。

3.2. アンケート調査について

組込みシステムの国内産業の第三者検証に関する要求について、第三者検証ユーザー企業 10 社、検証事業組織・企業 6 社についてアンケート調査を行い、「第三者検証が要求される国と製品」「第三者検証で重要な検証項目」「第三者検証のために許容できるコスト」など、17 の観点で整理した。

アンケート調査では第三者検証に関する関心の高さを示す結果が得られた。

第三者検証が求められる製品としては「自動車」「安全が求められる機器」「インフラ等の社会基盤」等々障害が発生した場合の影響が大きい機器が挙げられた。

第三者検証が求められる輸出国としては、「アメリカ」「欧州」「中国」など日本の主要輸出国が挙げられている。

第三者検証にかけられるコストについては、推定が困難との回答が多かったが、あえて割合を算出した場合、開発コストの 10%程度との意見が挙げられた。