AMED ロボット介護機器開発・標準化事業　安全化設計手法の開発
研究成果報告

これから機能安全に取り組む開発者のための

ロボット介護機器の安全制御回路開発ガイダンス

（初版）

はじめに

本事業[1]では，被介護者の自立支援のための，ロボット技術を実装した機器の開発を促進することを目的としている。自律的に動作するロボット介護機器の場合，介護者の関わりの程度が軽減し，機器の制御回路への高い安全性が期待される。しかし，我が国の介護機器の JIS 規格では制御回路の安全性の程度に関わる要求は，ほとんど言及されておらず，安全なロボット介護機器を開発する上で課題になると考えられる。一方で国際標準化では，ISO TC173 にて，ロボット技術を含む介護機器の全般的な安全規格が開発中である。（2021 年 1 月現在，DIS 段階）この国際規格は，制御回路の安全性に関しては医療機器の規格群を引用する方針で開発が進められている。また，日本国内の介護機器は，法令上，医療機器とは見なされない事情から，医療機器規格に馴染みのないロボット介護機器開発者は多いと推測する。したがって，医療機器規格に馴染みのない，国内のロボット介護機器の開発事業者にとっては，このギャップは今後の海外展開を狙う際の障害になり得る。

我が国の課題に対し，このガイダンスでは，ロボット介護機器の開発の規格適用の要件と流れを示し，続いて，適用する各医療機器規格の制御安全に関する要求とその考え方について解説を行うことで，導入の一助となることを目的とする。ロボット介護機器を想定した具体例や参考情報などを盛り込むことにより，初めて医療機器系規格の制御安全に取り組む，ロボット介護機器の開発者にも分かりやすいよう配慮する。

---

[1] AMED **ロボット**介護機器開発・標準化事業

◇ 想定する読者とこのガイダンスの活用方法

このガイダンスは，医療機器規格に馴染みのない開発者が，海外展開を前提としたロボット介護機器の安全制御回路を開発するケースをメインに想定する。したがって，基本的には，一般の生活支援ロボットに適用する機能安全については理解済みであることを前提としている。ただし，機能安全の基礎的なイメージがつかめるよう，平易な表現と具体的な事例を多用している。

このガイダンスは，医療機器規格と，機能安全の理解度に応じて，下表のように読み進めることができる。

	機能安全開発に馴染みがある。	機能安全開発には馴染みがない。
医療機器規格に馴染みがある。	× **このガイダンス文書の読解は不要と考える。**	△ **部分的に参考になる場合がある。** 読み方 目次から必要な分野を検索して読む。
医療機器規格には馴染みがない。	◎ **まさに想定読者である。** 読み方 第1章から第6章まで、順番に読み進める。	○ **想定読者に含まれる。** 読み方 第1章から第6章まで、順番に読み進める。但し，リスクアセスメントの基礎は，本安全ハンドブック『2-1 リスクアセスメントの基礎とRAシートひな形説明』を先に理解する。

※国内仕向けのロボット介護機器の制御安全に対応する場合，本ガイダンスの適用規格とは要求が異なるため、JIS 規格など国内の適用規格の要求を確認する。ただし，本ガイダンスの開発アプローチは国際的に主流になりつつあり，様々な制御回路の開発で参考になる。

◇ このガイダンスの用語について

このガイダンスで用いる専門用語は，医療機器規格（ISO 21856, ISO 14971, IEC 60601-1, IEC62304）の定義をなるべく用いている。これらの医療機器規格に適切な定義がない場合，機械安全及び機能安全規格の定義を用いる。専門用語は，**ボールド体**で記載し，付録 C の専門用語リストに定義・説明を記載する。

尚，医療機器規格では，厳密には“機能安全”という用語を用いていない。したがって，このガイダンスでは，ロボット介護機器の規格要求の言い回しは，例えば「ロボット介護機器の”安全制御回路開発”のため要求される。」などの言い回しを通常用いている。ただし，他産業分野も含めた機能安全共通の内容を表す場合には，「“機能安全”的なアプローチである。」などの言い回しをする場合もある。

◇ このガイダンスの章番号と規格の箇条番号の表記について

このガイダンスでは，章毎に異なるテーマで解説をしている。また，ガイダンスの他の箇所や規格への引用・参照を多く用いている。対象箇所を区別するため以下の通りの表記を用いる。

・このガイダンスの見出し番号は“章”を用いる。（例えば「5.1 章を参照」など。）

・規格の見出し番号は“箇条”を用いる。（例えば「箇条 5.1 を参照」など。）

◇ このガイダンスの構成について

このガイダンスでは，まず第 1 章にて，ロボット介護機器の安全性と電子制御の関係について概要に触れる。続く，第 2 章では，現在開発中の国際規格 ISO 21856 草案[2]「Assistive products — General requirements and test methods」が要求する機能安全のフレームワークを概説し，詳細を言及している各医療系規格との関係を説明する。

このガイダンスの第 3 章から第 5 章は，ロボット介護機器の機能安全に適用する各医療系規格の要求を解説する。第 3 章は，医療機器の機能安全プロセスの前半となるリスクマネジメントプロセスについて，ISO 14971[3]「Medical devices -- Application of risk management to medical devices」の規格要求から，特に機械のリスクアセスメントとの差分を中心に，医療機器リスクマネジメント規格の特徴を説明している。尚，機械のリスクアセスメントについては，本書を読む前に安全ハンドブック『2-1 リスクアセスメントの基礎と RA シートひな形説明』を参照されたい。

第 4 章は，医療機器の電子制御回路の開発要求について，IEC 60601-1[4]「Medical electrical equipment -- Part 1: General requirements for basic safety and essential performance」規格の安全要求をロボット介護機器に適用できるよう解説する。PEMS 開発要求とは，リスク分析を行った結果，電子制御回路の故障により受容できないリスクが生じる場合，又は，リスク低減に制御を用いる場合の電子制御システムに適用される。いわゆる安全関連の電子制御システムの開発プロセスへの要求やハードウェアの不具合に対して，どのような取り組みをするのか，開発経験者の事例を含め，具体的に解説している。第 5 章は，医療機器のソフトウェア開発・保守プロセスの要求について，IEC 62304[5]「Medical device software－Software life cycle processes」の規格要求に従い解説する。ここではソフトウェアの安全性についての考え方や，規格が要求するソフトウェア開発プロセスについて，なぜ開発プロセス要求をするのか，かみ砕いた解説を行う。

第 6 章は，ロボット介護機器の一つのモデルをベースに，リスクマネジメント，PEMS 開発，ソフトウェア開発と一連の開発の流れを開発経験者への取材をもとにしたスタディケースを説明する。

付録では，本文の理解を助ける情報を記載する。医療機器と非医療機器の分野にまたがるロボット介

---

[2] ガイダンス作成時点(2021 年 1 月)の最新バージョン：ISO DIS 21856 に対応している。

[3] 第 3 章作成時点(2019 年 1 月)の最新バージョン：ISO 14971:2007 に対応している。

[4] ISO DIS 21856 の引用バージョン：IEC 60601-1/A1:2012 に対応している。

[5] 第 3 章作成時点(2019 年 1 月)の最新バージョン：IEC 62304/A1:2015 に対応している。

護機器について，区分を確認するための情報（付録 A），機能安全の具体的な技法（付録 B），このガイダンスで使用される専門用語集（付録 C），参考となる規格の一覧表（付録 D）を記載する。医療機器規格の言及内容は比較的に抽象度が高く，機能安全自体に馴染みがない開発者にとって基礎を理解するために参考になると考える。

このガイダンスは ISO/IEC などの国際規格，JIS などの国内規格からの内容を含むが，ロボット介護機器の機能安全の理解に役立つ情報を，なるべく簡単に解説することを目的とするため，規格の要求とは差異が存在する場合が考えられる。また，解説のため記載した規格の要求内容は，あくまで参考和訳であるため，この点にも注意が必要である。実際の開発業務で使用する場合など，正確な情報が必要な場合には規格原文を必ずご確認頂きたい。

1 目次

ロボット介護機器の安全制御回路 開発ガイダンス 1
はじめに 2
1 ロボット介護機器の電子制御回路への安全要求 9
1.1 ロボット介護機器に求められる安全機能 9
1.2 制御回路の安全性 13
1.3 ロボット介護機器の国際規格 16
1.4 医療機器と見なされるロボット介護機器 17
2 規格要求の適用ガイド 20
2.1 開発フェーズ【１】製品安全規格の選定 22
2.2 開発フェーズ【２】製品安全規格の要求遵守（ISO 21856） 24
2.3 開発フェーズ【３】リスクマネジメントの実施（ISO 14971） 25
2.4 開発フェーズ【４】リスクコントロール 30
2.5 開発フェーズ【５】PEMS 安全要求適合（IEC 60601-1） 35
2.6 開発フェーズ【６】ソフトウェアのライフサイクル要求（IEC 62304） 46
2.7 PEMS 開発の品質管理 50
3 リスクマネジメント実施ガイド（ISO 14971） 52
3.1 ISO 14971 規格の全体像 53
3.2 ISO 14971 附属書の解説 55
3.3 リスクマネジメントの説明 58
3.4 ロボット介護機器のリスクマネジメントのポイント 60
3.4.1 ポイント① リスクマネジメントの一般要求 62
3.4.2 ポイント② 機械安全要素のリスク特定 72
3.4.3 ポイント③ PEMS 開発中のリスクマネジメント 76
3.4.4 ポイント④ 製造及び製造後のリスク低減の有効性を監視 81
4 PEMS のためのシステム開発実施ガイド（IEC 60601-1） 84
4.1 PEMS 開発ライフサイクルの実施ガイド （IEC 60601-1 箇条 14） 86
4.1.1 故障の考え方 86
4.1.2 設計管理 88
4.1.3 設計プロセス 97
4.1.4 PEMS 内外の通信 （IEC 60601-1 箇条 14.13） 102
4.1.5 変更管理 （IEC 60601-1 箇条 14.12） 104
4.1.6 ハードウェアの系統的な故障への対応策 104
4.2 単一故障安全の実施ガイド （箇条 4.7，箇条 13.1 及び 13.2） 106

4.2.1 単一故障安全 107
4.2.2 ハードウェア偶発故障への対応策 119
4.2.5 単一故障状態試験のためのガイダンス 125
4.2.6 CPU/MPU 関連の故障への対応 130
4.3 電磁ノイズ耐性の要求（IEC 60601-1-2） 138
4.3.1 EMC 設計と開発 140
4.3.2 EMC 試験の方法 145
4.3.3 電磁妨害に関するリスクマネジメント 148
5 ソフトウェア開発実施ガイド（IEC 62304） 150
5.1 IEC 62304 規格の目的と要求の概要 152
5.1.1 ソフトウェアの安全性を向上する 3 大原則 152
5.1.2 他の規格との関係性 153
5.1.3 ソフトウェアの安全性 154
5.1.4 IEC 62304 規格の要求概要 159
5.1.5 ソフトウェア開発モデルとその管理について 165
5.1.6 この規格への適合を依頼する場合のマネジメント 168
5.2 IEC 62304 の一般要求事項（箇条 4） 170
5.2.1 品質マネジメントシステム（箇条 4.1） 170
5.2.2 リスクマネジメント（箇条 4.2） 170
5.2.3 ソフトウェア安全クラス分類（箇条 4.3） 171
5.2.4 レガシーソフトウェア（箇条 4.4） 175
5.3 ソフトウェアライフサイクルの実施方法（IEC 62304 箇条 5～9） 180
5.3.1 ソフトウェア開発プロセス （箇条 5） 181
5.3.2 ソフトウェア保守プロセス （箇条 6） 223
5.3.3 ソフトウェアリスクマネジメントプロセス （箇条 7） 227
5.3.4 ソフトウェア構成管理プロセス （箇条 8） 235
5.3.5 ソフトウェア問題解決プロセス （箇条 9） 238
5.3.6 システム開発側との調整事項 244
5.4 ソフトウェアに関する情報 245
6 開発の具体例：装着型歩行支援機器での開発事例 246
付録 A 主要国における医療機器への該当を調査する方法 264
(ア) 日本での扱われ方 265
(イ) 欧州での扱われ方 266
✧ 医療機器指令 93/42/EEC の医療機器の定義 266
✧ 欧州委員会発行のガイダンス文書 267
✧ 欧州 医療機器指令整合規格リスト 269

(ウ) 米国の場合 271
(エ) 開発する医療機器を海外で販売したい時の相談窓口 271
付録 B 機能安全で用いられる技法 272
(ア) ハザードの特定で用いる技法 272
(イ) リスク分析で用いる技法 299
(ウ) リスク評価で用いる技法 308
(エ) 機能安全で用いる技法 310
付録 C 関連用語集 314
(ア) ロボットおよびロボティクスデバイスに関する用語（ISO 8373 Robots and robotic devices — Vocabulary） 314
(イ) リスクマネジメント・リスクアセスメントに関連する用語（ISO 14971, ISO 12100） 316
(ウ) 医用電気機器（プログラマブル電気医用システム：PEMS を含む）に関連する用語（IEC 60601-1） 327
(エ) 医療機器のソフトウェアライフサイクルプロセスに関連する用語（IEC 62304） 334
(オ) 機能安全に関する用語（IEC 61508 シリーズなど） 340
付録 D 関連・参考規格リスト 358
(ア) 安全原則に関するガイド 358
(イ) 福祉機器関連規格(ISO TC173) 359
(ウ) リスクマネジメント・リスクアセスメント関連の規格 368
(エ) 医療機器(医用電気機器) 関連の規格 370
(オ) システム・ソフトウェア関連の規格 373
(カ) 品質マネジメントシステム関連の規格 374
(キ) ロボット関連の規格 375
(ク) 機械安全に関する規格 (ISO TC199) 377
(ケ) 機能安全に関する規格 379

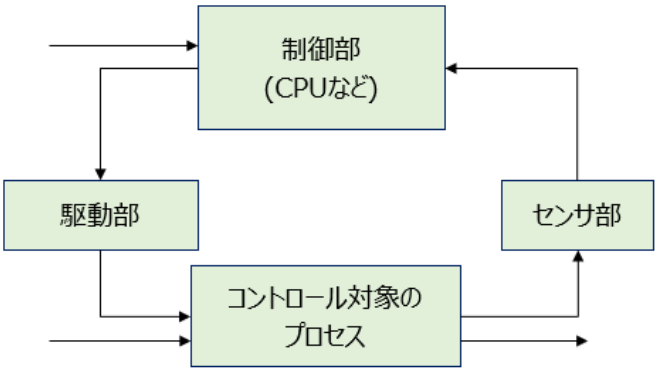
1　ロボット介護機器の電子制御回路への安全要求

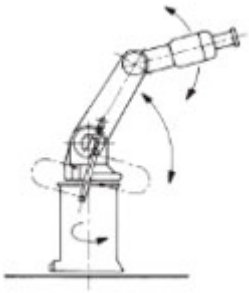
1.1　ロボット介護機器に求められる安全機能

ロボットとは，意図された**タスク**の実行のため，一定の**自律性**を持ち，環境内を移動し，複数の軸から成るプログラム可能な作動機構と ISO 規格で定義される。そのために，一般的には以下の基本要素から構成されている。

◆構成要素

① センサ系（情報を感知し）
② 知能・制御系（判断し）
③ 駆動系（動作する）





イラスト出展：ISO 8373

本事業におけるロボット介護機器とは，このようなロボット技術の要素を用いて，使用者の自立支援や介護者の負担の軽減に役立つ福祉機器である。

ロボット介護機器は障がい者や高齢者の身体的なハンディキャップを補完する医療機器的な側面を持つ場合があったり，介護現場で動力機器として介護者の力作業を代行する役割を果たしたり，高齢者の生活の質（QOL）を上げるために，外出時に歩行をアシストしたり，その果たす役割は多様である。使用者をアシストするために，使用者からの入力（操作，命令など），又は環境からの入力（センシングした情報など）を感知し，**タスク**を判断し，適切なエネルギを，出力する。**自律性**を伴うことで，従来の福祉機器には無かった更なる利便性や安全性の提供が期待される。

しかし，ハンディキャップや重労働をアシストするための大きな力やエネルギを機器に蓄える場合もあり，その上で，人間（使用者および周辺に存在する人）と同じ活動エリア(近距離，もしくは接触状態など)で協働作業を果たす必要がある。このためロボット介護機器は，誤操作，装置の**故障**又は誤作動を起こした場合，近接した使用者や周辺の人による回避・抑制行動は通常より困難なことが多く，重篤な

危害を及ぼす恐れもある。

ロボットは，国際規格 ISO 8373「ロボットとロボティックデバイス－用語」において，**産業用ロボット**とそれ以外のいわゆる**サービスロボット**とに大別され，ロボット介護機器は**サービスロボット**に類別される。（図 1-1 に示す。）**産業用ロボット**とロボット介護機器では双方の**安全**対策の種類には実際違いが生じる場合が多い。従来型の**産業用ロボット**を含む機械製品の安全対策は“隔離”と“停止”が基本と言われ，人間と**ロボット**の間に防護柵を設けて物理的に隔離するなど，物理的な安全対策を行うことが優先的に検討される。図の例では，工場稼働中に**ロボット**が動作している間は，人間は柵の外におり，トラブル及びメンテナンス時のみ，ドアを開けることで柵のインタロックが解除され，**ロボット**の動力が遮断され，停止状態が維持され，それから共同作業エリアに人間が侵入して作業を行う。**ロボット**と人間は稼働を時分割で協調作業していると考える。一方で，人間と同じ活動エリア，同じ時間でエネルギを発揮することが要求されるロボット介護機器については，**産業用ロボット**のような物理的な安全対策を行うことは実用性を損なう面から，難しいケースも多い。まず，危険なエネルギの使用を無くす，それが無理ならば必要最低限にエネルギを減らすことを検討することが大事だが，この安全対策は，本来の機能性を損なうこともあり，制御による安全対策に頼らざるを得ないケースがしばしば発生する。

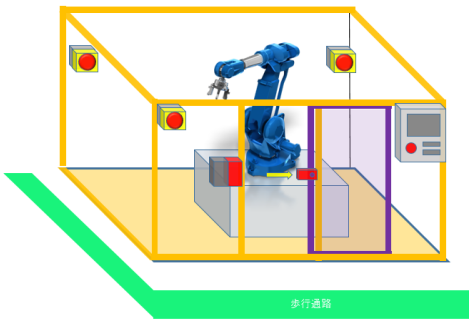
１．**産業用ロボット**	２．ロボット介護機器（**サービスロボット**の一つ）
人と**ロボット**が異なるエリア，又は異なる時間（で交代）にて作業を行う。➡”協調作業”と呼ばれる	人と**ロボット**が同じエリアで同時に作業を行う ➡”協働作業”と呼ばれる
	
・堅牢な柵で囲う。（場所を区分する。） ・インタロックを設ける。（稼働時間を区分する。）	・**危険状態・危険事象**を頻繁に監視する。 ・安全状態に直ちに移行する。 （停止や通報など）

図 1-1 産業用ロボットとロボット介護機器の特質と安全対策のイメージ

ここでは制御による安全対策のいくつかの例を，図 1-2 に示す。ロボット介護機器の一つで，使用者に装着して使用する装着型移動支援ロボットにおいては、使用環境内の危険な物体を検出したり、アシスト制御機能の**故障**を検出した場合に、アシストを停止するなど、制御によって様々な機能を設計・実装することで安全性の向上が期待できる。制御（厳密には電子制御以外のハードウェアなどの**リスク**軽減措置も含む）を用いた機能によって安全な状態（以降，**安全状態**と呼ぶ）を達成又は維持するものを**安全機能**という。

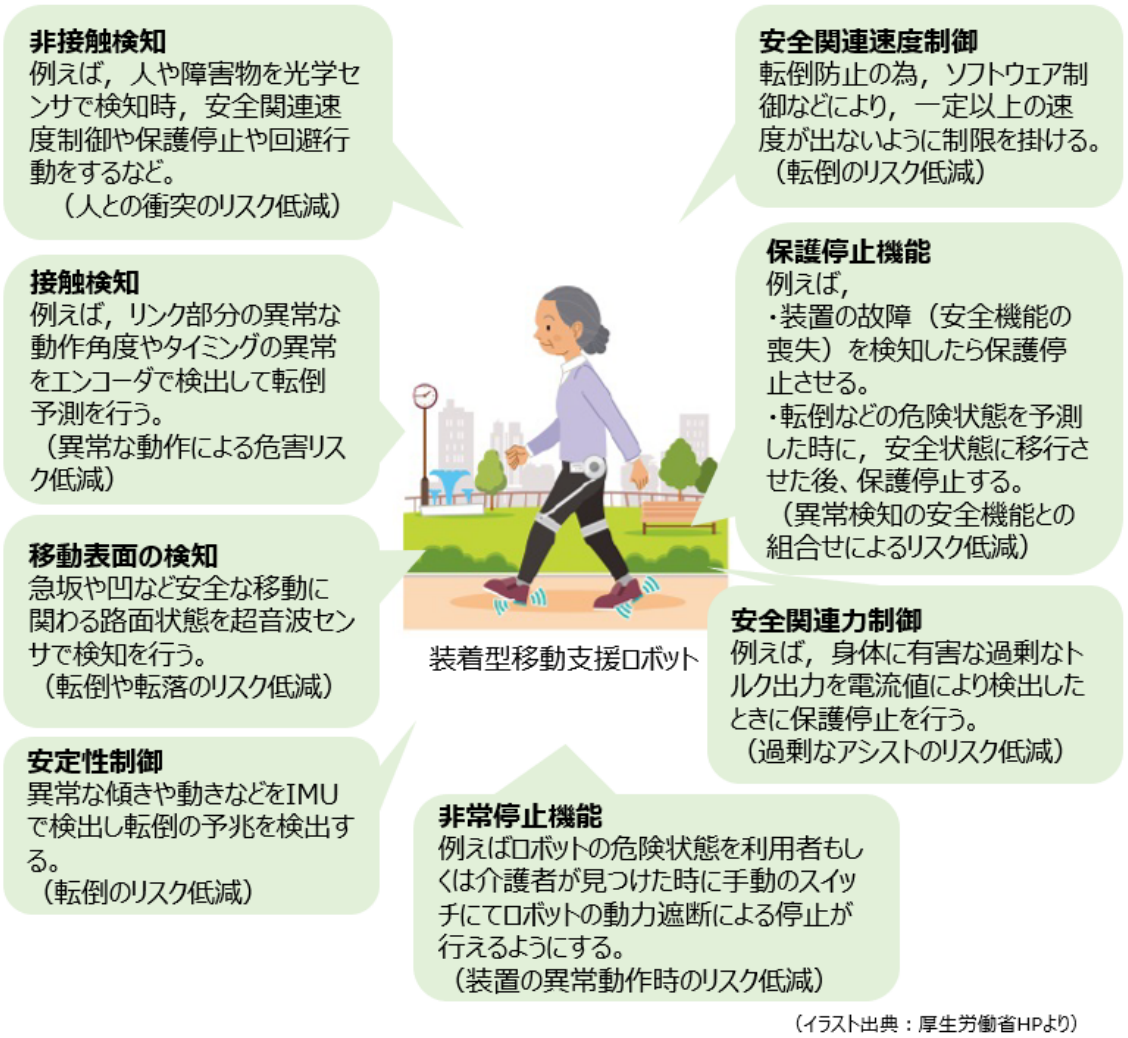
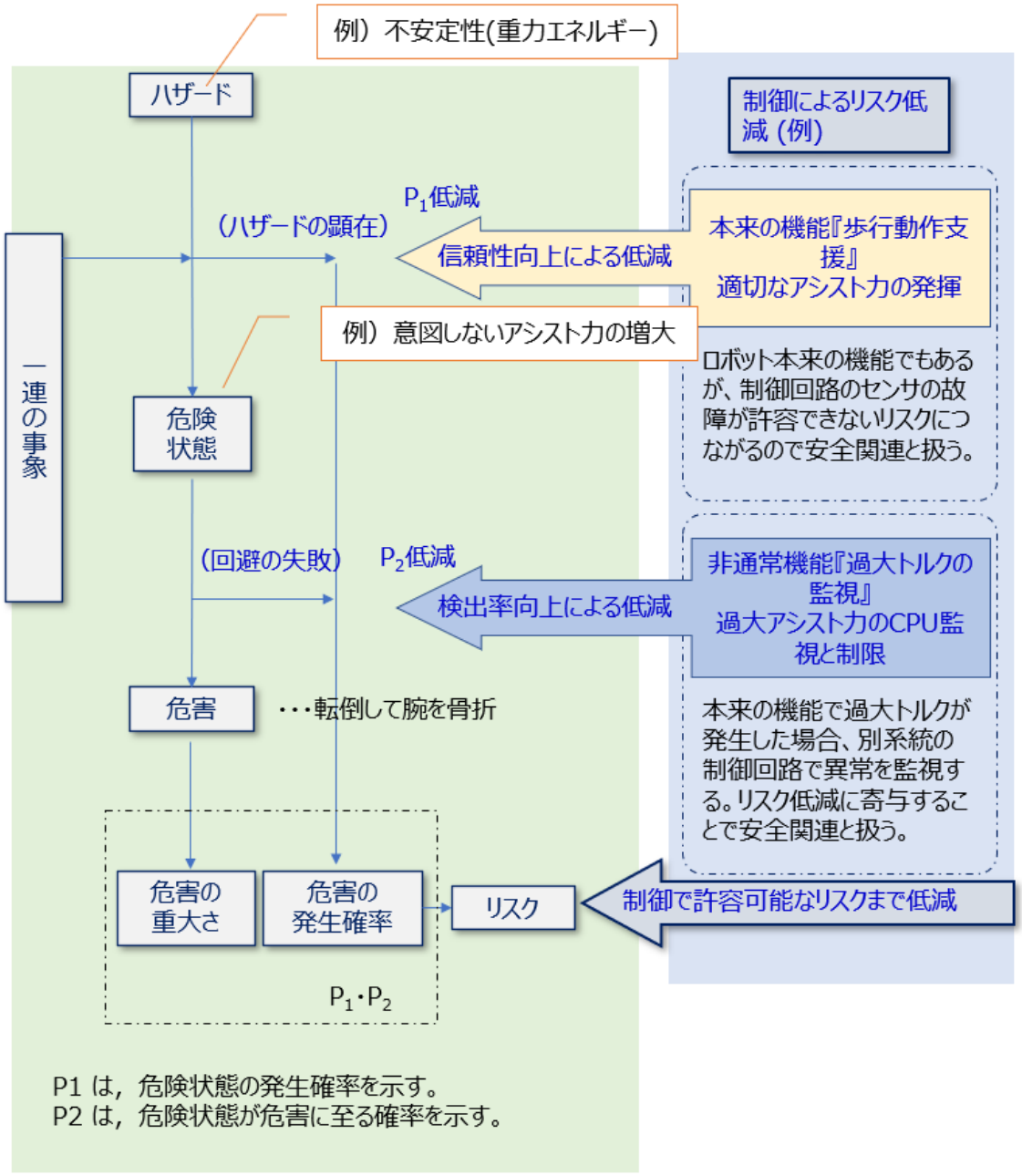


図 1-2 装着型移動支援ロボットの安全機能の例

この図の例のように，ロボット介護機器に内在する様々な**ハザード**（例えば衝突や不安定さ）を制御による工夫を用いて，**危険状態**に遷移しづらくしたり，**危険状態**から**危害**に至るのを防いだりできることは，工学的且つ合理的な安全対策を具現化し，製品の安全性を確保する上で大変有効な手段となる。ここでは、**安全機能**とそれによって達成される安全性の関係について説明する。

国際規格である ISO 規格及び IEC 規格への安全概念の指針を示した規格作成ガイド ISO/IEC Guide 51「Safety aspects - Guidelines for their inclusion in standards」では「**安全**とは，

受容できない**リスク**がないこと。」と定義される。また，ロボット介護機器で適用する、**医療機器**への**リスクマネジメント**の適用方法を扱う国際規格 ISO 14971「医療機器－医療機器へのリスクマネジメントの適用」では，潜在的な**ハザード**が**リスク**に至るまでのプロセスを図 1-3 の左側のフローのように示す。この中で**リスク**の大きさとは，**危害**の**重大さ**と発生確率の組み合わせで決定するとなっているので，制御を使った**安全機能**を用いることで，**危害**の発生確率が低減していることを右側の矢印で示す。**安全機能**の採用の結果として，受容可能なレベルまで**リスク**が低減でき，**安全**であることを示すことができる。



(ISO 14971 の図E.1を解説を付与するなど編集)

図 1-3 ハザード，一連の事象，危険状態及び危害の関係の図式

ここでは，脚の位置に応じ，適切なトルクアシストを行う，装着型歩行動作支援ロボットを例に挙げて説明する。**異常**なアシスト力の発生により，バランスを崩して転倒し，骨折をしてしまう**リスク**から，**リスク**を低減するため，**リスク**の大きさに寄与する２つの要素である「P1：**危険状態**の発生確率」と「P2：**危険状態**が**危害**に至る確率」を下げる**安全機能**を説明する。

まず（**リスクアセスメント**では，後述する**本質的安全設計方策**を考慮するが，ここでは省略する），「P1：**危険状態**の発生確率」を下げるには，通常の歩行アシスト機能を制御するセンサなどの電子制御回路の**信頼性**を向上させることで、過大アシストトルクを発生（**危険状態**）させるような**故障**モードの確率を下げることが可能である。次に，「P2 **危険状態**が**危害**に至る確率」を下げるには，通常の歩行アシスト機能の電子制御回路の**異常**を安全機構が監視し，もし**異常**が発生した場合には，動力源を遮断して停止できれば（場合によっては、徐々に縮退する複雑な制御が必要かもしれないが、ここでは省略），**危害**に至るプロセスを断ち切ることが可能である。

ここでは，通常のアシスト機能の**信頼性**が**リスク**に影響する。また，**危険状態**が起こった場合でも，別の電子制御回路を用いた**安全機能**を実装することで，**リスク**を低減できること（一例）を説明した。次章では，具体的な構造レベルで，**安全機能**と**安全**性確保の手段について説明する。（尚，本章の**安全**や**リスクマネジメント**に関連する用語は付録 C の関連用語集に説明を記載する。）

1.2 制御回路の安全性

この章では，制御を用いた機能が**信頼性**高く作動する，又は，**故障**しても結果的に人への**危害**は無いように振る舞うなど，**リスク**に関連する制御回路の安全性について解説する。

図 1-4 は電子制御回路の構造を単純化したものであり，ここでは，センサ部，制御部，駆動部の 3 ブロックで表現した。これらの各ブロックが，情報を感知し（センサ部），判断し（制御部），動作する（駆動部）ことで意図した機能を実現する。この時，各ブロックが要求仕様通りに機能し，かつ，センサから取り込んだデータを，制御部・駆動部と要求通りのインターフェースで伝達すれば，**安全機能**は要求通りに動作し，**危害**に至るプロセスを想定した通りに断ち切ることが出来る。よって，電子制御回路は，扱う**リスク**の大きさに応じた**信頼性**を有し，動作するように設計することが必要である。具体的には，意図した環境・使われ方にて，製品寿命を十分に超える期間，正常動作し続ける**信頼性**の高いセンサが採用されたり（一般にはアベイラビリティが高いと呼ぶ），偶発的にセンサ部～制御部間のインターフェース部品の一つが**故障**を起こしても，二重系統にしていた他の部品がカバーして，信号が電子制御回路全体としては機能不全無く伝達されたり（**フォールトトレラント**），もしくは正常に機能はしなくとも，CPU が**故障**を判断して安全にシャットダウンさせるなど，安全方向に働く信号が伝達されたり（フェールセーフ），いくつかの安全工学に基づいた**保護方策**がある。電子制御回路の安全要求に応じた適切な方策を選択し，安全性を有することが求められる。

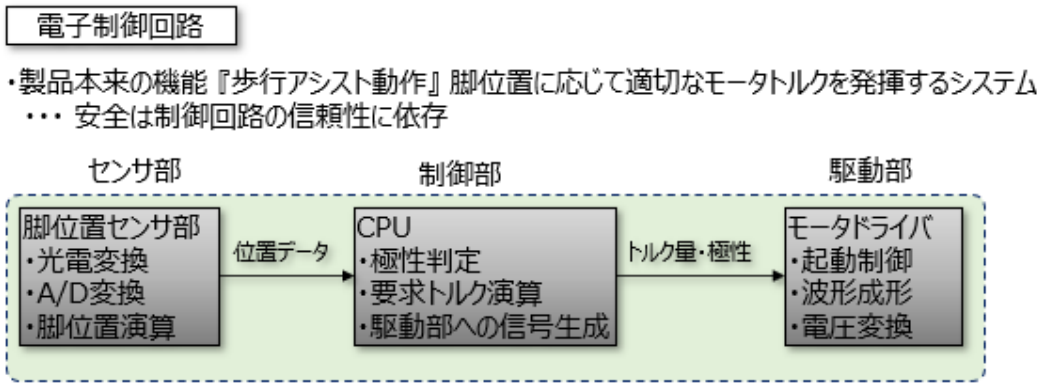


図 1-4 適切なアシストカを発揮して使用者の歩行を支援するシステム

図 1-5 の電子制御回路では，脚の位置に応じて適切なモータトルクを発揮するという製品通常の機能を実現するため，各ブロックが必要な機能を持つ。各ブロック内のすべての構成部品の**故障率**が十分に低く，製品寿命期間中の動作**信頼性**が高ければ**危険状態**への移行確率（前章の P1 を指す）は低いと言える。しかし，実際に**信頼性**部品のみで安全性を満足することは，部品選定・コストなどの面でも容易では無い。**機能安全**の規格では，ハードウェア部品はいつかは**故障**し，ソフトウェアバグをゼロにすることは困難である。そこで，個々の部品の**信頼性**だけに依存しない方策を**機能安全**では考える。この**システム**の構成部品のどこかが**故障**をして，制御信号の**エラー**によって，歩行バランスを崩すほどの**異常**なトルクが発生し（**危険状態**），**危害**に至ることを懸念する場合，**異常**なトルク（過大なモータ電流）を CPU が監視し，**危害**に至る前に，モータドライバに保護停止命令を送出するといった。通常の機能に**異常**があったときに備える**安全機構**を追加実装することが一つの現実的な**保護方策**となる。図 1-5 は**安全機構**としての制御**サブシステム**を追加したものである。このように，電子制御回路による**安全**では，個々の部品の**故障率**よりも，**システム**全体として適切な**アーキテクチャ**が**安全**に寄与する場合が多い。制御回路の安全性を考慮するときには，**リスク**の大きさに応じた**アーキテクチャ**，次いで，**安全機能**として定義した制御回路の振る舞いを侵害する故障確率を考慮する。

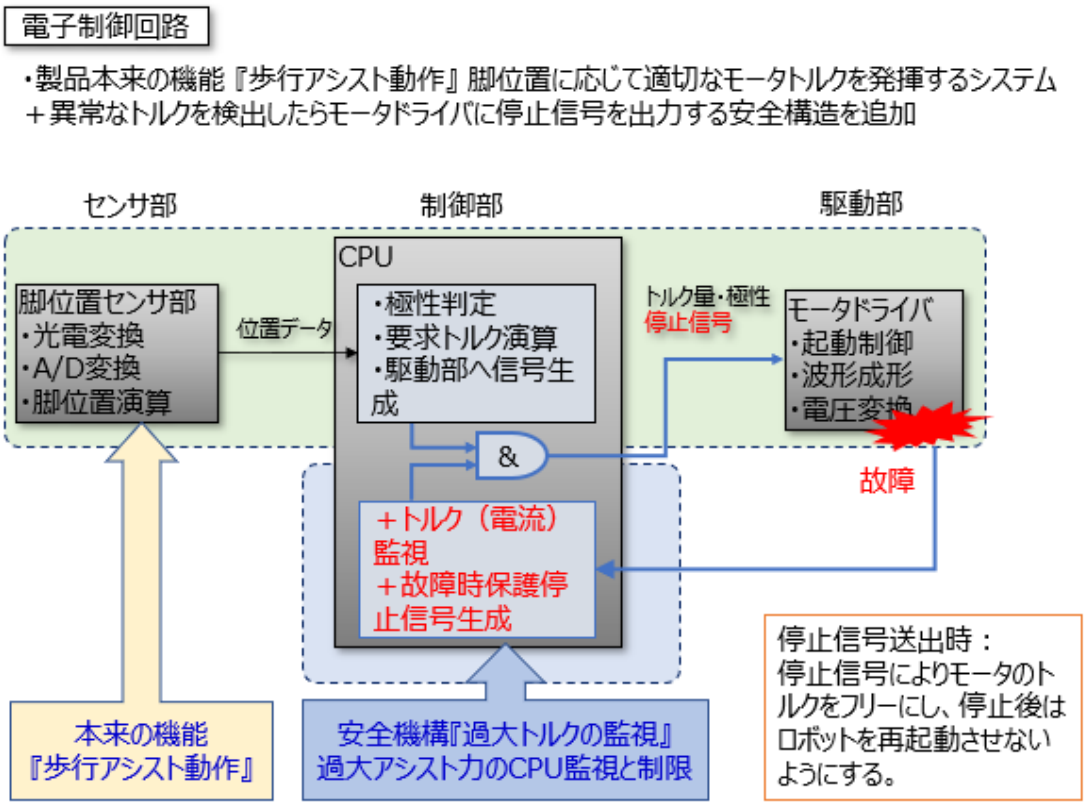


図 1-5 部品故障した場合，故障検出して安全に停止させる構造を追加したシステム

このように電子制御回路の安全性を確保する開発は，大半の開発事業者であれば従来から検討している活動にすぎない。2000 年に国際電気標準会議 （IEC: International Electrotechnical Commission） が安全性の確保を必要とする広範囲の電気・電子・プログラマブル電子機器に適用できる基本安全規格（Basic safety publication）として，IEC 61508 シリーズ（-1 から-4）「電気・電子・プログラマブル電子**安全関連系**の**機能安全**」を発行した。この規格が制定されたことにより，制御による**安全機能**を**リスク**に応じた安全度にするための体系的な取り組みが示され，それまでは各開発事業者が独自で取り組んでいた制御安全の考慮事項が，IEC 61508 をベースに国際的に一本化された。近年ではそれに加え，鉄道，プラント，医療機器，産業機械製品，生活支援ロボットなどの各分野で，その産業の事情に合わせた要求が見直された**機能安全**規格も存在する世の中になっている。それらは産業分野別**機能安全**規格と呼ばれ，IEC 61508 をベースとした本質的なコンセプトを踏襲しつつも，規格間で具体的な要求は差異があり，この部分に留意して進めることが重要である。（図 1-6 は，IEC 61508 シリーズのコンセプトをいくらか引き継いだ産業別規格の一例である。）

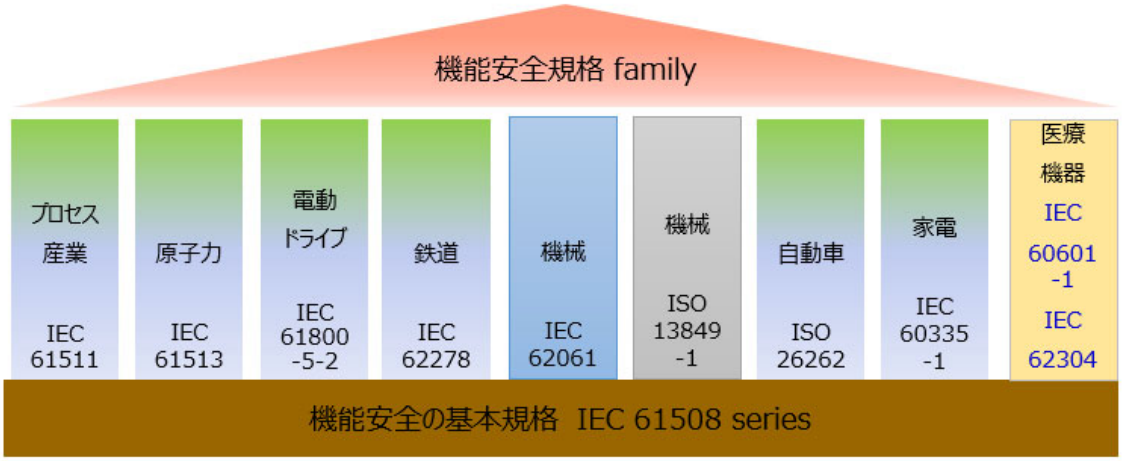


図 1-6 機能安全に関連する規格の例

1.3 ロボット介護機器の国際規格

福祉機器に電子化，動力化が求められる背景のもと，国際標準化活動として，福祉機器にロボット技術を導入する場合の**機能安全**要求を明確にする規格の策定が進められており，福祉機器が持つ医療的な側面と，福祉機器に要求されるべき安全性が考慮された規格となるべく，現在検討・開発作業が進められている。

現在，ISO/TC173-WG12 では，福祉機器の通則 ISO 21856「Assistive products－General Requirements and test methods」を開発中であり，この規格は，基本的には**医療機器**と見なされる福祉機器に適用される。（図 1-7 規格の Scope を参照。）ロボット介護機器を含む福祉機器の**機能安全**は正に検討段階となっている。(2021 年 1 月) 現時点では医用電気機器の規格 IEC 60601-1 が要求する”**単一故障安全**”および”**プログラマブル電気医用システム**（**PEMS** ）”と同様の要求が妥当であるとの意見が主流であり，**医療機器**関連の規格（群）を引用する方向で議論が行われている。

この方向で，参加各国の間でコンセンサスが形成されつつあるため，本ガイダンスでは ISO/TC173-WG12 最新の国際標準化の動向に沿った要求体系をベースに，国内のロボット開発事業者がロボット介護機器の**機能安全**開発をスムーズに理解・導入できるよう，注意点と提案を含めて解説をする。

1．Scope This document specifies general requirements and test methods for assistive products, considered to be medical devices, intended for use to alleviate or compensate for a disability. Assistive products are medical devices in some jurisdictions but not in others. This document does not apply to assistive products which achieve their intended purpose by administering pharmaceutical substances to the user. (参考和訳)

１．適用範囲 この規格では，**障害**の軽減又は補完に使用するための，**医療機器**と見なされる支援機器の一般的な要件と試験方法を規定している。支援機器は，一部の地域では**医療機器**と見なされ，他の区域では見なされない。この規格は，医薬品を利用者に投与することにより，目的を達成する支援機器には適用しない。

図 1-7 ISO 21856 原案の箇条 1 Scope より抜粋

尚，**医療機器**の規格の中では，電子制御回路で**安全**を担保する**システム**に”**機能安全**”という用語は使用しない。そこでこのガイダンスでロボット介護機器など福祉機器の分野の**機能安全**については”安全制御回路の開発”という用語を使用する。

1.4 医療機器と見なされるロボット介護機器

ロボット介護機器は，医学的な効果効能を製造事業者が言及するか（**意図する使用**において医療行為を行うか）や，その仕向け国における法令・規制によって，**医療機器**に該当する場合と非**医療機器**の扱いになる場合があり，ボーダーに位置する製品もある。新たにロボット介護機器を開発する事業者は，開発する**ロボット**が**医療機器**に該当するか，否かを，初めに明確にすることが賢明である。なぜならば，**医療機器**としてのロボット介護機器に求められる電子制御回路への安全要求体系は，非医療機器の生活支援ロボットの**機能安全**の規格要求体系とは異なり，加えて，適用規格の書きぶりも異なるので，両方を習得し導入するまでには，多くの労力・工数を割く必要があると考えるからである。この章では，**医療機器**の電子制御回路への安全性を扱う規格群を明確にし，非医療機器の生活支援ロボットとの違いについて解説をする。

医療機器系の規格の中では，電子制御回路を ”**プログラマブル電気医用システム**（略称：**PEMS**）” という専門の用語を用い，一般的な生活支援**ロボット**で言う **SRP/CS**（ISO 13849-1 の用語）など，いわゆる”**機能安全**”の**システム**という言い方は用いることなく，混同することを避けている。また，双方への要求コンセプトは共通部分が多くありながら，規格要求の説明方法にはギャップがある。**医療機器**系の規格では，構造要求や技法などの技術的な要求はあまり言及していない傾向にあり，開発工程への要求が主に言及されている。一方，非医療機器の生活支援ロボットの**機能安全**規格では，適用範囲において「**医療機器**は扱わない」と明確にスコープから除外している。（例えば以下の２つの規格[6]）また，要求の説明方法も開発工程への要求もあるが，技術レベルでの達成手段が比較的多く説明され，要求の意図が比較的つかみやすい。これは過去の機械・ロボット製品で実績があり熟成された技術や技法を導入する事で，所与の**安全**性が達成できる。という考え方によるものである。

---

[6] ISO 13482：2014 の適用範囲において 医療機器としてのロボットには、適用しない。としている。
IEC 61508-1:2010 の適用範囲において IEC 60601 シリーズに適合する医療機器には、適用しない。としている。

このように，一括りに**機能安全**の関連規格と言っても産業セクターによって，その書きぶりは異なる。一般の生活支援ロボットの開発者が，海外展開の**ロボット**介護機器を開発する際に，初めて**医療機器**規格を適用する場合には，考え方の切り替えをしないと読解に苦労することを述べておきたい。

医療機器規格体系の新規導入に際する主な課題を以下にまとめる。

① 同じコンセプトの要求を求めているにも拘らず，**医療機器**と生活支援ロボットでは，用語や説明方法が異なり，規格要求もお互いを容認していない状況（互換性は無い）であること。

② **医療機器**系規格は，医療業界独特の表現が用いられており，また，**医療機器**に要求される規制や品質**システム**を前提に作成しているため，業界の予備知識に馴染みが薄い機械設計者の理解を困難にする。

③ 多様な機能・構造の**医療機器**を扱うため，規格には具体的な技術の解説は少ない。具体的な技術に関する内容が読み取れるのは，副通則規格，機器毎の個別規格，**医療機器**分野毎の開発指南書などを読み渡る必要があり，ロボット介護機器の具体的技術に関する情報源はまだ非常に少ない。

以上の課題から，**医療機器**に該当するロボット介護機器分野に新規参入する一般の生活支援ロボットの開発者にとっては規格解釈に疑問が存在し，導入に負担が大きい状況であると考えている。そこで，無駄な取り組みを行わないために，開発事業者は自社のロボット介護機器が**医療機器**に該当するか，否かを慎重に調査し，適用規格を決定するところから着手されたい。

① 自社で製造販売する製品を**医療機器**に該当する機器か，否か明確に絞る。場合によっては，非医療機器のみの開発に絞り，比較的開発がしやすい一般生活支援ロボットの**機能安全**規格体系を適用する。

注記　付録 A に主要国での**医療機器**に該当するかを調査するいくつかの情報と手段を記入する。

② **医療機器**扱いのロボット介護機器の**機能安全**開発を決定した場合，一般の生活支援ロボットの規格要求との共通／差分を把握し，既存の開発資産を有効活用できるように開発活動をテーラリングする。このガイダンスで差分として示す情報を有効に活用することができる。

医療機器扱いのロボット介護機器への要求は ISO 21856 原案で扱っており，一般生活支援**ロボット**で適用すべき規格は明確に区分される。図 1-8 は ISO 21856 が引用する**機能安全**に関連する規格群になるが，一般の生活支援ロボットの**機能安全**規格群とは異なり，また基本的には互換性がないため（※注記），開発者は新たな規格を理解することになる。また**機能安全**の様々な要件を満たすために ISO 21856 原案のみでは無く，他にも複数の規格が引用されていることが分かる。

※注記　開発中の ISO (FDIS) 21856:2020 では，ISO 13849 の**機能安全**設計について，「使用しても良い」，とあるが，**医療機器**前提の規格要求の中で，この一文は奇異な記述であり，今後見直される懸念がある。

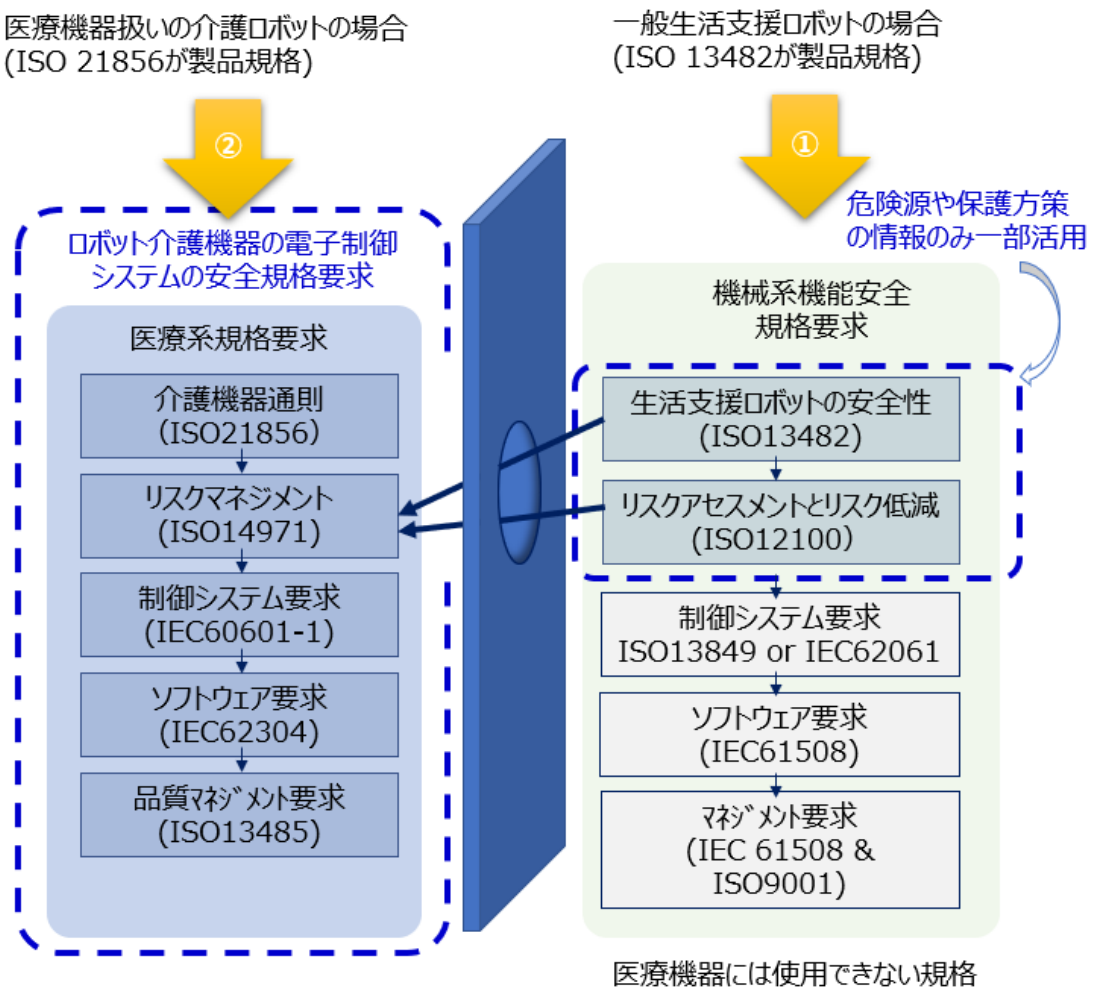


図 1-8 一般用途ロボットと医療機器ロボットの機能安全関連規格の相違

注記： 双方の規格の要求構造は異なるため，単純比較はできないことに注意が必要

このガイダンスでは，一般（非医療の）生活支援ロボットの開発事業者が既存の知識を活かし，新たな規格の開発を効率的に実現するポイントと流れを示すため，**医療機器**系規格と生活支援ロボット系規格との**機能安全**関連における差分を中心に，各医療系規格を解説していく構成となっている。

2　規格要求の適用ガイド

この章では，国際規格 ISO 21856 原案の求める，国際潮流に基づいたロボット介護機器の**安全**に関わる制御回路の開発の流れを，要求のコンセプトも含めて，分かりやすく説明する。ロボット介護機器の開発者は，この規格の要求体系を把握し，多様な要求があることを，理解したい。自社製品の効果効能や仕向け地などの販売戦略を考慮の上で，**安全制御回路開発**への対応準備に活用してほしい。

適用規格とその要求の全体像を，「**安全制御回路開発**のための規格要求マップ（図 2-1）に示し，次に，このマップの流れに沿って開発工程を説明していく。ここでは開発の流れをわかりやすくするため，「開発フェーズ〇：〇〇〇〇〇〇」と呼んで順番に説明をするが，規格にはこのような概念は無い。
注記：　このガイダンスは ISO 21856 原案の要求事項に沿うように作成するが，すべての要求を網羅するものでは無い。また，ISO 21856 は現在も協議中であるため，なるべく最新の情報を反映するが，正式発行規格とは相違がある場合がある。

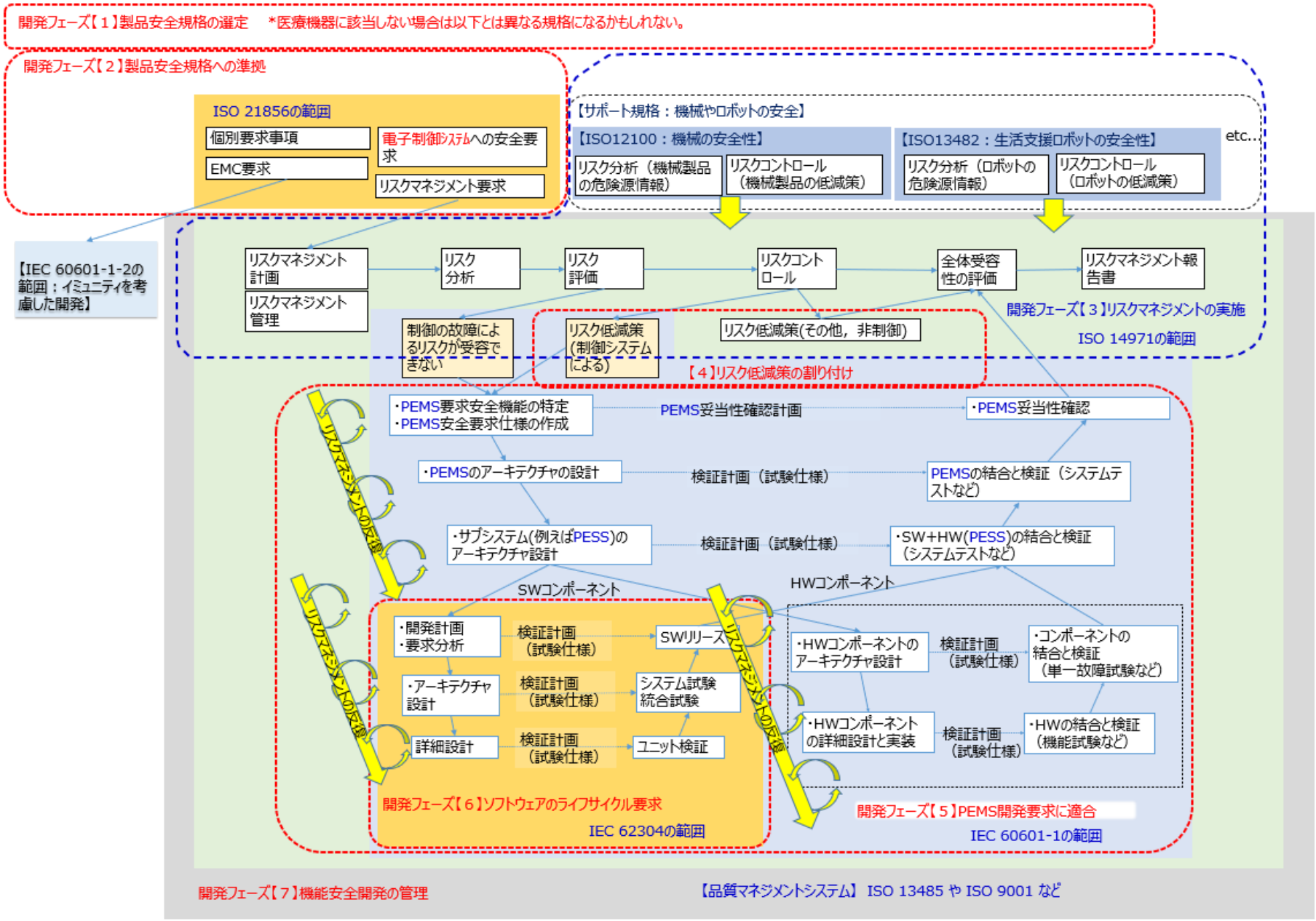


図 2-1 安全制御回路開発のための規格要求マップ

2.1 開発フェーズ【１】製品安全規格の選定

最初に，自社で開発するロボット介護機器に適用する主たる製品**安全**規格の選定を行う。
（電子制御回路の**安全**に限った**プロセス**では無いが，製品安全を考える最初の**プロセス**であり，関連情報として説明する。）
仕向け国における強制の法規制が無い場合には，一般的な製造者責任法を鑑みて，最も適切に機器の安全性をカバーする規格を選定する。
仕向地によっては法規制への適合が求められる。例えば，欧州の場合には，CE マーキングが要求され，該当する Directive（指令）もしくは Regulation（規則）を選択し，一般的には，各 Directive もしくは Regulation の要求事項への適合を推定するための（give presumption of conformity with the essential requirements）欧州整合規格(EN 規格)リストから製品安全規格を選定する。（回りくどい言い方だが，要するにリストから選んだ EN 規格（群）要求に適合することで，その Directive もしくは Regulation へ適合したとみなすことになる。）
このように，法規制，顧客要求もしくは製造者責任などの観点から，適切な一つもしくは複数の規格を選定する。昨今の ISO/IEC などの国際規格の場合，規格体系は階層的になっていることが多い。対象製品固有の種別に適用する個別製品規格がある場合には，まずは個別製品規格を選定する。個別製品規格が無い場合には，グループ規格，基本規格という優先順位で規格を適用する。 図 2-2 は ISO 規格の階層化構造を表すが，ISO TC199 が開発する機械の安全性の規格群はタイプ A～C 規格に識別され，タイプ A 規格：ISO 12100 は，**リスクアセスメント**及び**リスク**低減の方法を示し，タイプ B 規格：グループ安全規格は，広範囲な機械に共通して適用できる**保護方策**を示し，タイプ C 規格：製品**安全**規格は個別の種類の機械に適用できる**保護方策**を示す。ISO/TC173-WG12 が開発する福祉機器の製品安全規格群はそのような階層化構造とは明言してはいないが，コンセプトは同じである。例えば，非装着移動支援ロボットの場合，製品安**全**規格として ISO 11199 の Walking aids manipulated by both arms -- Requirements and test methods が存在するので，まずは最優先として規格要求に従う。しかし，その規格内には**安全制御回路開発**への要求事項が十分ではない場合，上位のグループ安全規格の位置付けとなる ISO 21856 原案の要求に従う， ISO 21856 原案 Assistive products— General requirements and test methods はある程度の範囲の福祉機器グループを対象としており，ISO 11199 に無い要求を補完できる役割となっている。ちなみに ISO 11199 は現在の国際標準化でロボット技術も組み込む方向で改訂作業がなされており，非装着移動支援機器特有の**安全機能**を扱う予定である。その他の電子制御回路への安全要求については，ISO 21856 原案の関連条項を引用する関係性で規格開発が進められている。**図 2-3** は ISO 21856 の箇条 1 の抜粋だが，優先順位の記載がある。

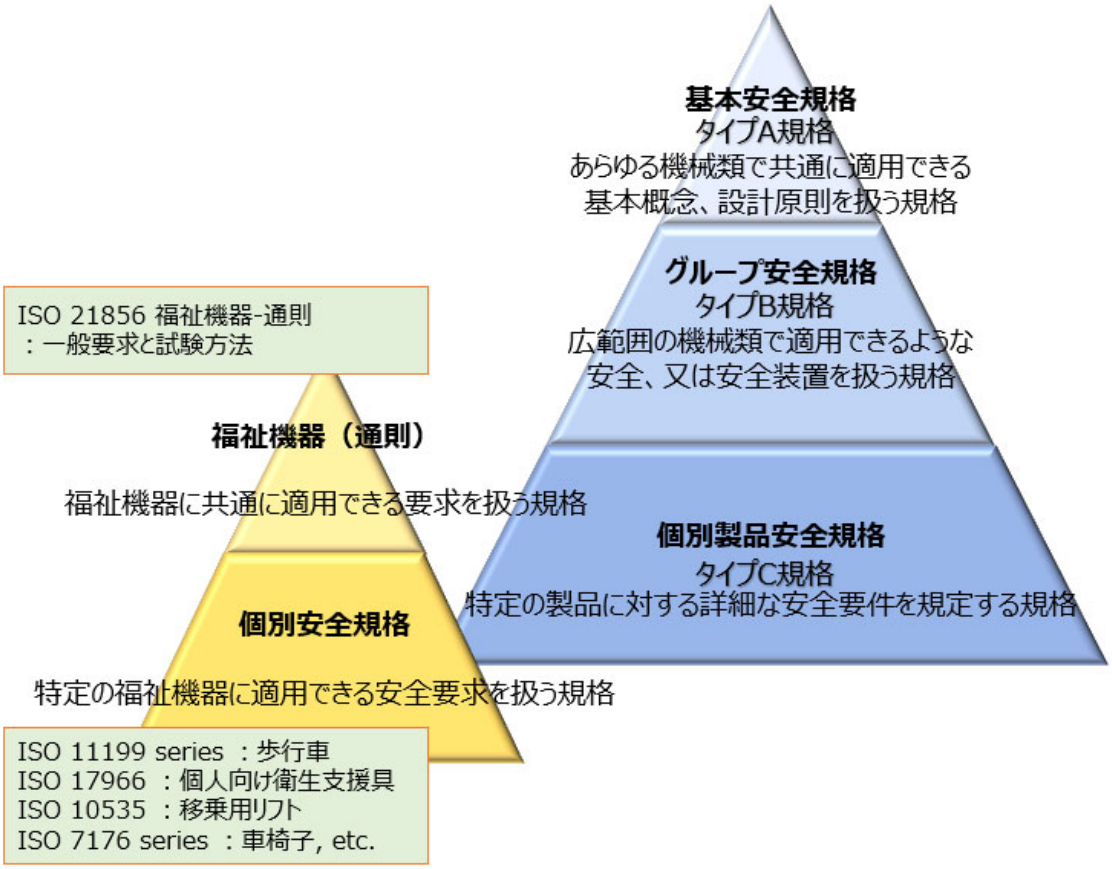


図 2-2 ISO 規格の階層化構造の例（機械安全の場合）

適用規格を選定する際，ISO 規格の箇条 1 Scope(適用範囲)にて，その規格が扱う機器や適用範囲を確認する。**図 2-3** に規格の抜粋と参考和訳を記載した。この規格は基本的には，**医療機器**と見なされる福祉機器に適用されることを認識しないといけないわけだが，“NOTE”を見ると，非医療機器と見なされる機器に使用されることを排除しない記述が見て取れる。

1 Scope This document specifies general requirements and test methods for assistive products, considered to be medical devices, intended for use to alleviate or compensate for a disability. Assistive products are considered to be medical devices in some jurisdictions but not in others. This document does not apply to assistive products which achieve their intended purpose by administering pharmaceutical substances to the user. Where other International Standards exist for particular types of assistive products then those standards apply. Where requirements in this document are not covered in a particular standard, this document can be used as a supplement. NOTE Not all the items listed in ISO 9999 are medical devices. Contracting parties

might wish to consider if this standard or parts of the standard can be used for assistive products which are not medical devices.

(参考和訳)
１．適用範囲
この規格では，**障害**の軽減又は補完に使用するための，**医療機器**と見なされる支援機器の一般的な要求と試験方法を規定している。支援機器は，一部の地域では**医療機器**と見なされ，他の区域では見なされない。この規格は，医薬品を利用者に投与することにより，目的を達成する支援機器には適用しない。
特定のタイプの支援機器に向けた他の国際規格が存在する場合，それらの規格が適用される。それらの規格の要求でカバーされていない要求がこの規格にある場合，この規格は補足するために使用するだろう。
注記：ISO 9999 に記載されているアイテムのすべてが**医療機器**では無い。この規格の使用者は，**医療機器**ではない支援機器に，この規格ないしはこの規格の要求の一部を使用できるかどうかを検討したい場合があるだろう。

図 2-3 ISO 21856 原案の箇条 1 Scope を抜粋

2.2 開発フェーズ【２】製品安全規格の要求遵守（ISO 21856)

このフェーズでは，選定した製品**安全**規格から，対象製品（ロボット介護機器）に適用する要求事項に適合するよう開発を行う。このガイダンスでは，ISO 21856 原案を製品安全規格として選定した場合の電子制御回路の安全関連要求事項を説明する。
ISO 21856 原案は，広範囲な福祉機器の**ハザード**とその安全要求を取り扱うので，電気安全，機械安全，化学物質や放射に対する**安全**など，多様な個別要求事項が有り，これに適合する必要がある。加えて，対象製品には，個別要求事項では具体的に言及されていない**ハザード**も存在する場合がある。規格が広範囲な福祉機器のすべての**ハザード**と要求事項を規定する事は困難であることから，ISO 21856 原案では製品安全の汎用的な手法である**リスクマネジメントプロセス**が要求される。図 3-4 に示すように，医療系**リスクマネジメント**規格 ISO 14971，及び(and)関連するならば(if relevant)，機械系**リスクアセスメント**規格 ISO 12100 を引用して，**リスク**をアセスメントとすることが要求されている（2021 年 1 月末現在）。しかし，その具体的な使い分けや細かな引用方法は製造事業者に一任される。解説は次章に譲る。

2.3 開発フェーズ【3】リスクマネジメントの実施（ISO 14971）

このフェーズでは，**リスクマネジメント**を実施する。

ISO 21856 原案では，図 2-4 に示すように，医療系**リスクマネジメント**規格 ISO 14971，及び(and)関連するならば(if relevant)，機械系**リスクアセスメント**規格 ISO 12100 を引用している。

4 General requirements

4.1 Risk analysis and management

The safety of an assistive product shall be assessed by identifying hazards and estimating the risks associated with them using the procedures specified in ISO 14971 and, if relevant, ISO 12100.

When an assistive product is intended by the manufacturer to be used in combination with a device that is not a medical device, the resulting combination of the assistive product and device shall behave in a safe way as a system.

An assistive product may only be used as specified by the manufacturer in the intended use.

Risk management shall include all involved persons.

NOTE 1 In the case of certain disabilities, there can be a need for higher levels of safety for equipment used to offset the effects of that disability.

NOTE 2 Conformity with the requirements of this standard can be used to claim compliance with the requirements of ISO 14971 for those hazards and risks identified in this standard.

(参考和訳)

4 一般要求事項

4.1 **リスク分析**と**リスクマネジメント**

支援機器の**安全**性は，ISO 14971 及び関連する場合は ISO 12100 で規定された**手順**を用いて，**ハザード**を特定し，それらに関連する**リスク**を推定することによってアセスメントされる。

医療機器ではない装置と組み合わせて使用することが製造事業者によって意図されている支援機器の場合，支援機器と装置の組み合わせた**システム**として**安全**に動作しなければならない。

支援機器は，製造元が指定した用途でのみ使用されるだろう。

リスクマネジメントには，すべての関係者を含めなければならない。

注 1 特定の**障害**の場合，その**障害**の影響を相殺するために使用される機器の**安全**性の高いレベルが必要になる可能性があります。

注 2 この規格の要件に適合すると，この規格で特定された**ハザード**及び**リスク**に関する ISO 14971 への要求に遵守していることの主張ができる。

図 2-4 ISO 21856 原案の箇条 4.1 Risk analysis and management を抜粋

「ISO 14971 **医療機器**への**リスクマネジメント**の適用」は，正しくは，**リスクアセスメント**ではなく，医療用機器の**リスクマネジメント**の**プロセス**を示す規格である，**医療機器**としての**ロボット**介護機器については，原則，この規格をメインに**リスクマネジメント**を実施する。「ISO 12100 機械類の**安全**性一設計の一般原則一**リスクアセスメント**及び**リスク**低減」は，関連する機械類の**安全**性のために**リスクアセスメント**の方法と**リスク**低減策を示す。図 2-5 に示すように，双方の規格には共通する**プロセス**が多くあり，また，管理面の要求や製造後の監視の有無など，相違点もある。ISO 21856 原案では，2 つの規格の使い方について，具体的に示しておらず，このガイダンスでは，基本的には非医療の**ロボット**介護機器の開発者向けとするので，ISO 12100 の**プロセス**をベースに ISO 14971 の差分取り組みを追加し，効率的な活動となるようテーラリングすることを提案する。具体的な方法は第 3 章 **リスクマネジメント**実施ガイド（ISO 14971）にて説明する。

注記： ISO 12100 （JIS B 9700） の**リスクアセスメント**に馴染みがなく，ロボット介護機器に適した**リスクアセスメント**基礎から習得する場合は，本**安全**ハンドブック『2-1 **リスクアセスメント**の基礎と RA シートひな形説明』を参照することをお勧めする。

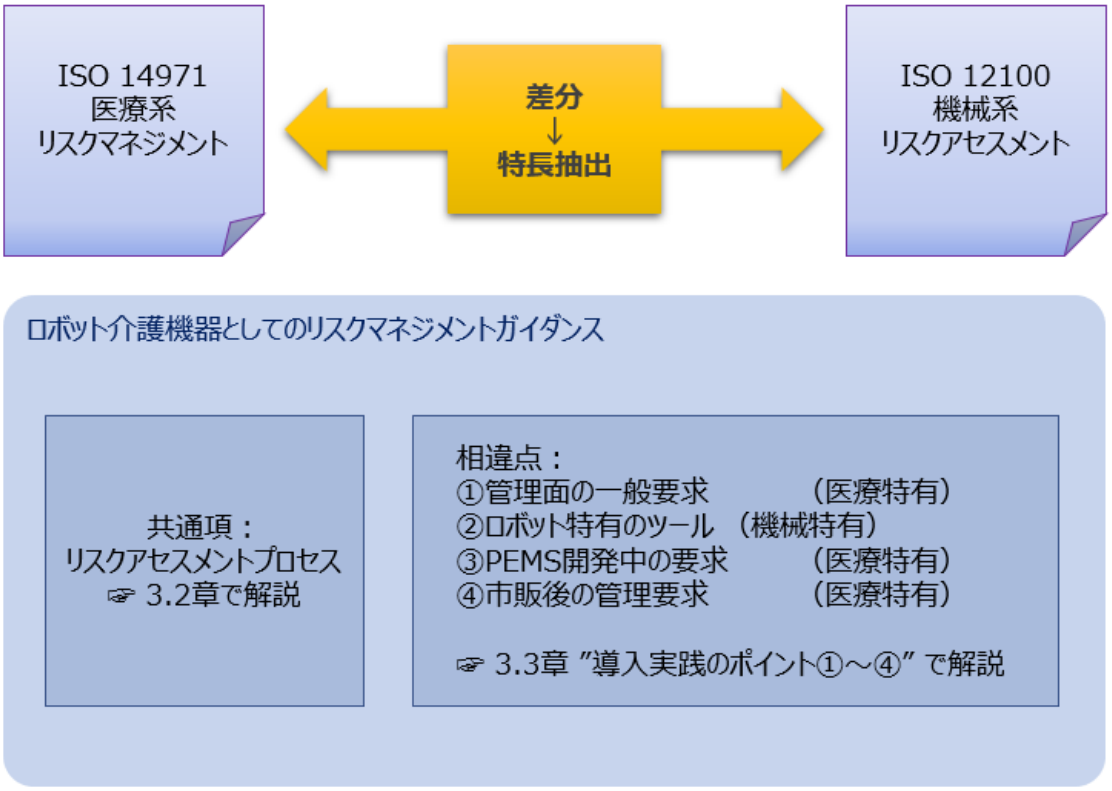


図 2-5 リスクマネジメント規格の違いとテーラリング

リスクマネジメントは，**医療機器**や福祉機器などの**安全**性確保において幅広く用いられている一般的な手法である。**医療機器**の**リスクマネジメント**の**プロセス**を概略図にしたものを図 2-6 に示す。最初に機器の特性を把握した上で，**ハザード**を特定し，**リスク**を分析し，**リスク**の大きさを**評価**し，（必要な場

合）受容可能なレベルまで**リスク低減**を行う。**残留リスク**の受容可能性を**評価**し，満足していれば**リスクマネジメント**報告書に文書化を行うが，不足していれば反復して**リスク分析プロセス**まで遡る。

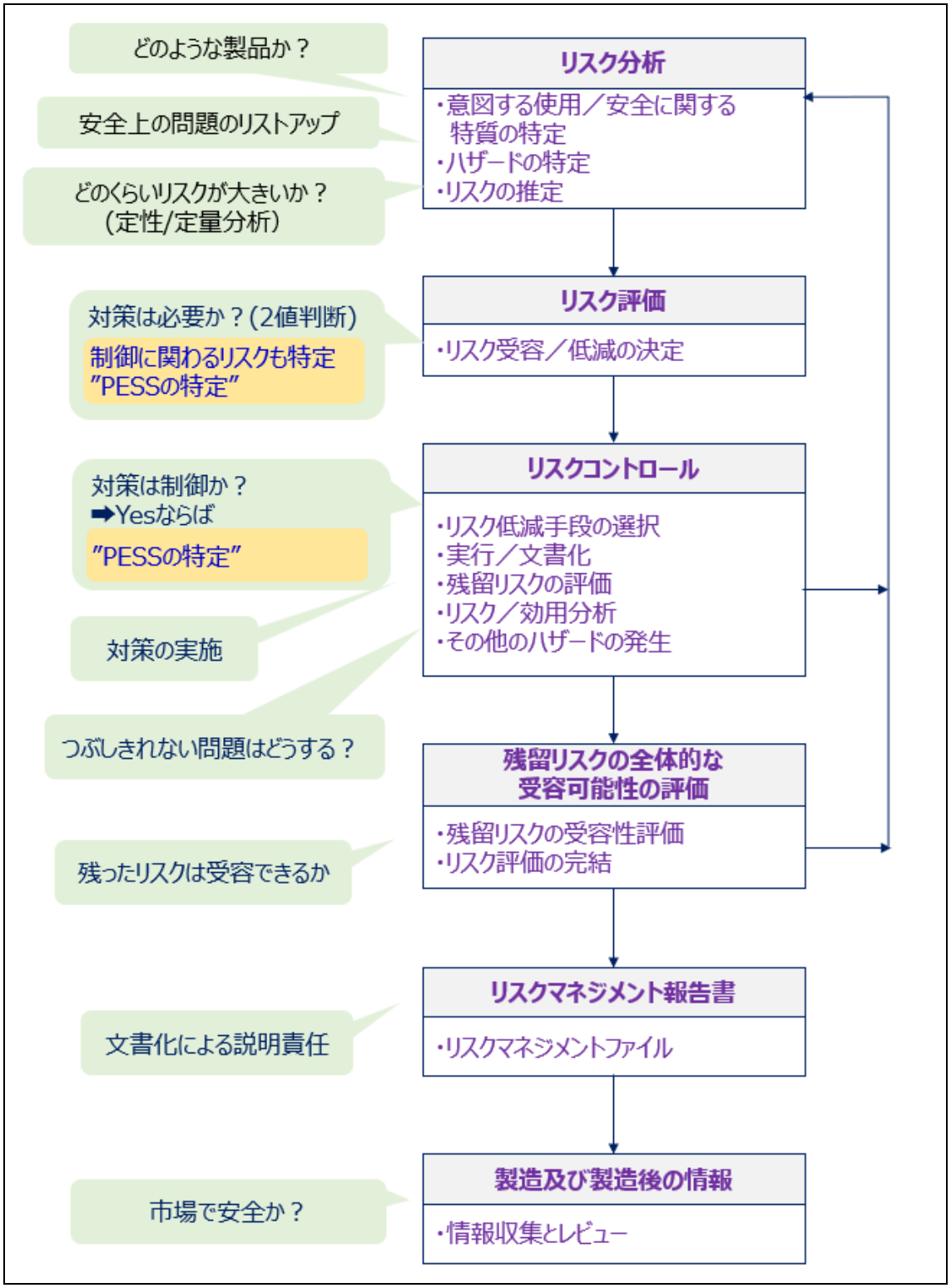


図 2-6 リスクマネジメントの基本的なプロセス

リスクマネジメントでは，図 2-6 の**リスク分析プロセス**内の，“**ハザード**の特定”で，その**ロボット**タイプに応じた機械的，電気的，熱的など多様な**ハザード**の考慮が必要になる。**自律性**の高いロボット介護機器の場合，**ロボット**特有の技術や**安全**要求を考慮することも，効果的であるが，そのような観点から，ISO 14971 だけでは，情報不足かもしれない。その点，ISO 12100 や，ISO 13482 などの機械製品および及び生活支援**ロボット**の**ハザード**情報や安全要求で補完するなど，有効に活用したい。
自律性を有するロボット介護機器の**リスク**では，特に電子制御回路部分が要求仕様に対して不正確，不適切な振る舞いを起こす**ハザード**を特定すべきである。ISO 21856 では，図 2-8 の一つ目のセンテンスで言及されるように，電気的に操作される支援機器（規格の性質から，電力供給される，又は電気的に制御される機器も含まれると考える。）には IEC 60601-1 の要求を満たすよう記述がある。例えば，**安全機能**を実現する電子制御回路を構成する電子部品に**故障**，劣化や単体不良により，不安全事象が発生するかも知れない。また，図 2-8 の三つ目のセンテンスで言及されるように，ソフトウェア制御を用いる場合は，仕様の考慮漏れ，設計ミスやコーディング**エラー**により，不安全事象が発生するかも知れない。そのような**ハザード**の**リスク**を考慮するとき，IEC 60601-1 の箇条 14 の電子制御に対する要求を満たすこととなる。このガイドの 4.1 章 **PEMS 開発ライフサイクル**の実施ガイド（IEC 60601-1）にて説明する。

8 Electrical safety

8.1 General

An electrically operated assistive product shall conform to IEC 60601-1:2005 + A1:2012 regarding electrical safety unless requirements are covered by this document. For electrical safety covered by both IEC 60601-1:2005 + A1:2012 and this document, the requirements of this document prevail over the ones given in IEC 60601-1:2005 + A1:2012.

For assistive products intended to be used in a home care environment, IEC 60601-1-11 shall be applied.

When software is used to control the motion of the assistive product, the requirements specified in IEC 60601-1:2005 + A1:2012, Clause 14 shall apply.

In addition, clauses 8.2, 8.3, 8.4 and 8.5 shall apply.

For robotic assistive products, functional safety design as stipulated in IEC 61508 and ISO 13849 may be used.

(参考和訳)

8 電気**安全**

8.1 一般

電気的に操作される支援機器は，この規格で要求を扱わない場合，電気**安全**に関する IEC 60601-1:2005 + A1:2012 に準拠するものとする。IEC 60601-1:2005 + A1:2012 及びこの規格の両方でカバーされる電気的**安全**については，この規格の要求が，IEC 60601-1:2005 + A1:2012 より

も優先される。 ホームケア環境で使用することを目的とした支援機器については，IEC 60601-1-11 を適用する。 支援機器の動作を制御するためにソフトウェアを使用する場合，IEC 60601-1:2005 + A1:2012 の要求が適用される。 また，ISO 21856 の箇条 8.2，8.3，8.4 及び 8.5 も適用される。 ロボット支援製品の場合，IEC 61508，及び ISO 13849 に規定されている**機能安全**設計が使用されても良い。

図 2-8　ISO 21856 原案の箇条 8.1 Electrical safety, General を抜粋

ISO 21856 原案は， EMC 要求があり，電子制御回路の**安全**に関わる部分が，機器が設置される環境下における電磁妨害で正常に作動することも重要な要件である。ISO 21856 の電磁両立性に関する記載は，図 2-9 のように，**医療機器**の EMC 規格 IEC 60601-1-2 を引用している。ロボット介護機器が医療施設にて使用される場合，他の**医療機器**や通信機器などから発生する電磁ノイズが**ロボット**の**安全機能**を侵害する**リスク**がある。この規格では，この**リスク**を**評価**し，対処するための開発及び**妥当性確認**を行うことを求める。このガイドの 4.3 章 電磁ノイズ耐性の要求（IEC 60601-1-2）にて説明する。

7　　Electromagnetic compatibility Assistive products containing electrical or electronic devices/components shall comply with the requirements of IEC 60601-1-2. NOTE For guidance, see A.7. (参考和訳) 電気機器又は電子装置/コンポーネントを含む支援機器は，IEC 60601-1-2 の要求に準拠しなければならない。 注記：ガイダンスについては，A.7 を参照。

図 2-9 ISO 21856 原案の箇条 7 Electromagnetic compatibility の関連部分抜粋

ISO 14971 では，広い範囲の**医療機器**の**ハザード**を扱っており，電子制御回路に関する**ハザード**や要求についての具体的な記述は少ないが，**安全機能**が**リスク**を低減したり，電子制御回路に関する**ハザード**が潜在したりする場合，**リスクマネジメント**で考慮する必要がある。このガイダンスの第 3 章では ISO 14971 をベースに**ロボット**介護機器に適した**リスクマネジメント**について解説する。
注記： ISO 12100 （JIS B 9700） の**リスクアセスメント**基礎から習得する場合は，安全ハンドブック『2-1 リスクアセスメントの基礎と RA シートひな形説明』を参照されたい。

2.4 開発フェーズ【４】リスクコントロール

図 2-6 の**リスク評価**の結果，**リスク**が受容できない場合，**保護方策**を選択し，設計・開発することが求められる。ロボット介護機器の場合，**危害**を受ける人間が１人程度となることが一般的で，適切な**リスク評価**を行うことで，後工程で合理的な設計・開発を行うことが出来る。

電子制御回路に受容できない**リスク**がある場合，非制御の**リスク**低減策を選択したり，電子制御回路に安全機構を追加したりすることで**リスク**を低減することが出来る。一方で，電子制御回路を用いた**安全機能**が**リスク**低減になる。

保護方策はスリーステップメソッドという優先順位を考慮して選択する。（詳しい説明は安全ハンドブック『2-1 **リスクアセスメント**の基礎と RA シートひな形説明』を参照されたい。）また，一つの**リスク**に対し，受容可能なレベルまで低減を達成するためには，複数の**保護方策**を組み合わせることも実際には多い。この場合，物理的な**保護方策**，電子制御回路による**保護方策**，マニュアルやラベルなど，使用の情報提供の**保護方策**に配分され，協調して**リスク**を低減する。これらの協調した**保護方策**については，ISO 14971 の**リスク評価プロセス**で再評価され，**リスク**低減が実施されているか**検証**される。一方，電子制御回路による**リスク低減**を用いる場合については，ISO 21856 原案では IEC 60601-1 で述べられる **PEMS** の開発要求を満足するよう言及されている。

(1) PESS と PEMS とは

IEC 60601-1 では，電子制御回路（**医療機器**の規格では**プログラマブル電子サブシステム，PESS** という。）の**故障**が受容できない**リスク**を生じる場合，又は **PESS** が，**安全**（**医療機器**の規格では，**基礎安全**又は**基本性能**という）に必要な**保護方策**を提供する場合，電子制御回路部分（**PESS**）を含む**ロボット介**護機器は IEC 60601-1 の **PEMS （プログラマブル電気医用システム， Programmable Electrical Medical Systems という)**への安全要求事項に従うこと，となっている。PESS と **PEMS** の例を図 2-10 にて説明する。

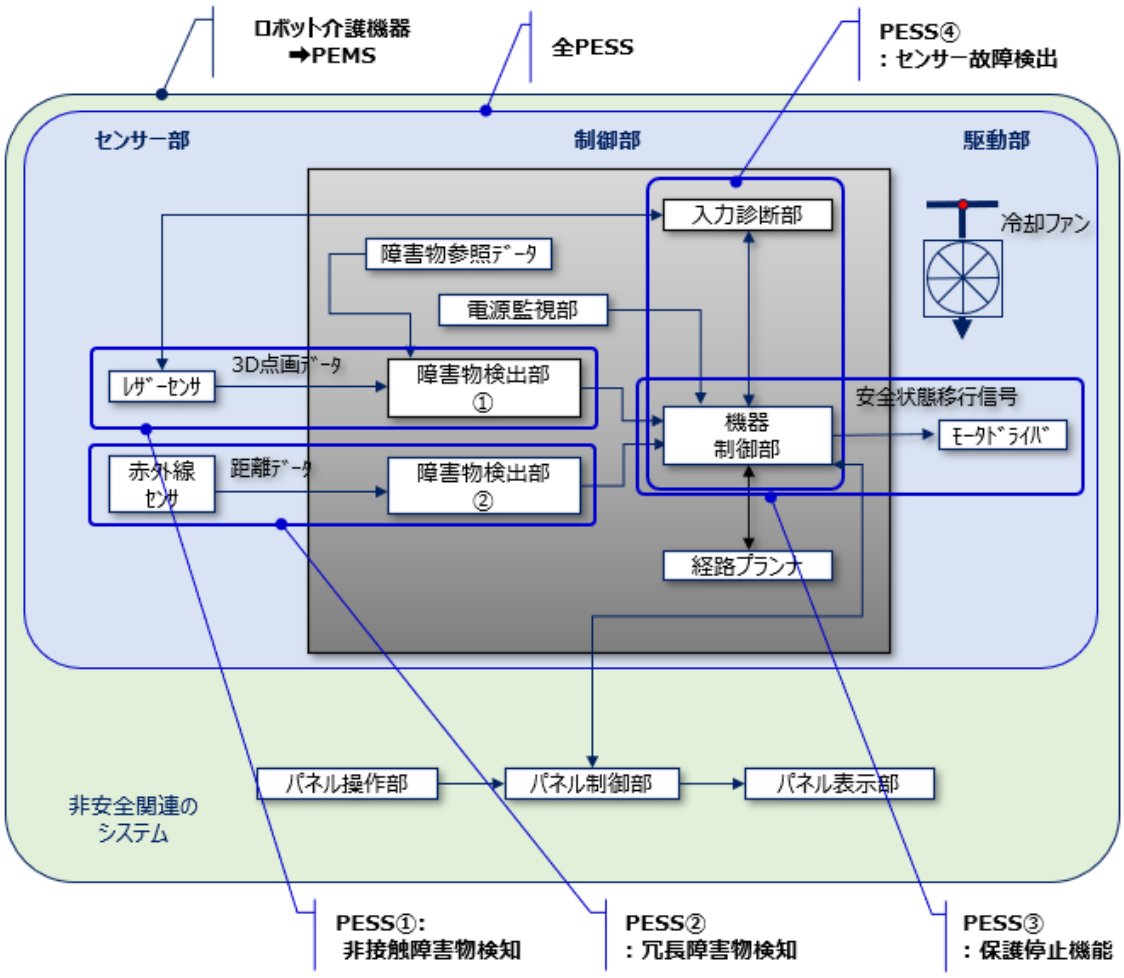


図 2-10　IEC 60601-1 で定義される PESS と PEMS

ロボット介護機器の**リスク**低減を**安全機能**で実現する場合，電子制御回路はソフトウェア及びハードウェアで構成され，CPU を中心として機能を実現することが一般的である。この図では，内蔵するいくつかの制御**サブシステム** PESS①： 非接触障害物検知， PESS③： 保護停止機能 など，を記す。PESS①： 非接触**障害**物検知は，半径 5m 以内に設定した安全防護区域内に侵入した障害物体（人など）をレーザーセンサで検知して，CPU に信号を与える。PESS③： 保護停止機能は，CPU

からの信号により，モータドライバの回転制御とブレーキにより**ロボット**を規定制動距離内で停止させる**保護方策**を実現する例を示す。ここで **PEMS** とは，いくつかの PESS に加え，ブレーキなどの，その他の**サブシステム**も含んだ**システム**全体，つまりロボット介護機器の事を指している。

(2) リスク低減手段（保護方策）の選択

リスクコントロールでは，特定した各**ハザード**に対し，合理的に機能する**保護方策**が選択されることが肝要である。合理的に機能する**保護方策**を選択するため，一般的には，過去から十分に吟味された実績のある方法をまず検討する。一般的には，国際規格や欧州整合(EN)規格などで言及されている**保護方策**をまず選択することが良い。例えば，図 2-11 のように，電気的エネルギによる火災に対しては， IEC 60601-1 の箇条 11 過度の温度及び他の**ハザード**に関する保護 の**保護方策**と安全基準が引用される、動作時の温度上昇を閾値以下に制限したり，**異常**時の過昇な温度上昇を，IEC 部品規格適合品の不可逆的な過昇温度トリップ装置（例えば温度ヒューズなど）で遮断したりする。加えて，規定の難燃性材料を使用した防火エンクロージャを設ける。これらの**保護方策**は，国際規格で古くから使用された安全基準として実績があり，対象の**リスク**シナリオとマッチすることを条件に，合理的な**保護方策**であるとみなされる。同様に，ロボット介護機器の**リスク**を低減するために，制御の振る舞い自体の**信頼性**を高く設計したり，**監視**回路を加えたりすることで，**リスク**低減につながる場合があり，これらは，IEC 60601-1 の箇条 14 の **PESS** とみなされる。この **PESS** が，**ロボット**の動作環境や使われ方において，要求した通りに機能しないなど，**リスク**を増大させるのは困るため，箇条 14 の **PEMS** への**安全**要求が存在する。箇条 14 の要求は“機能する**安全**”と，**リスク**に応じた“機能の**安全**性”を実現するための開発方法を規定しており，「**PEMS 開発ライフサイクル**」と呼ばれる。

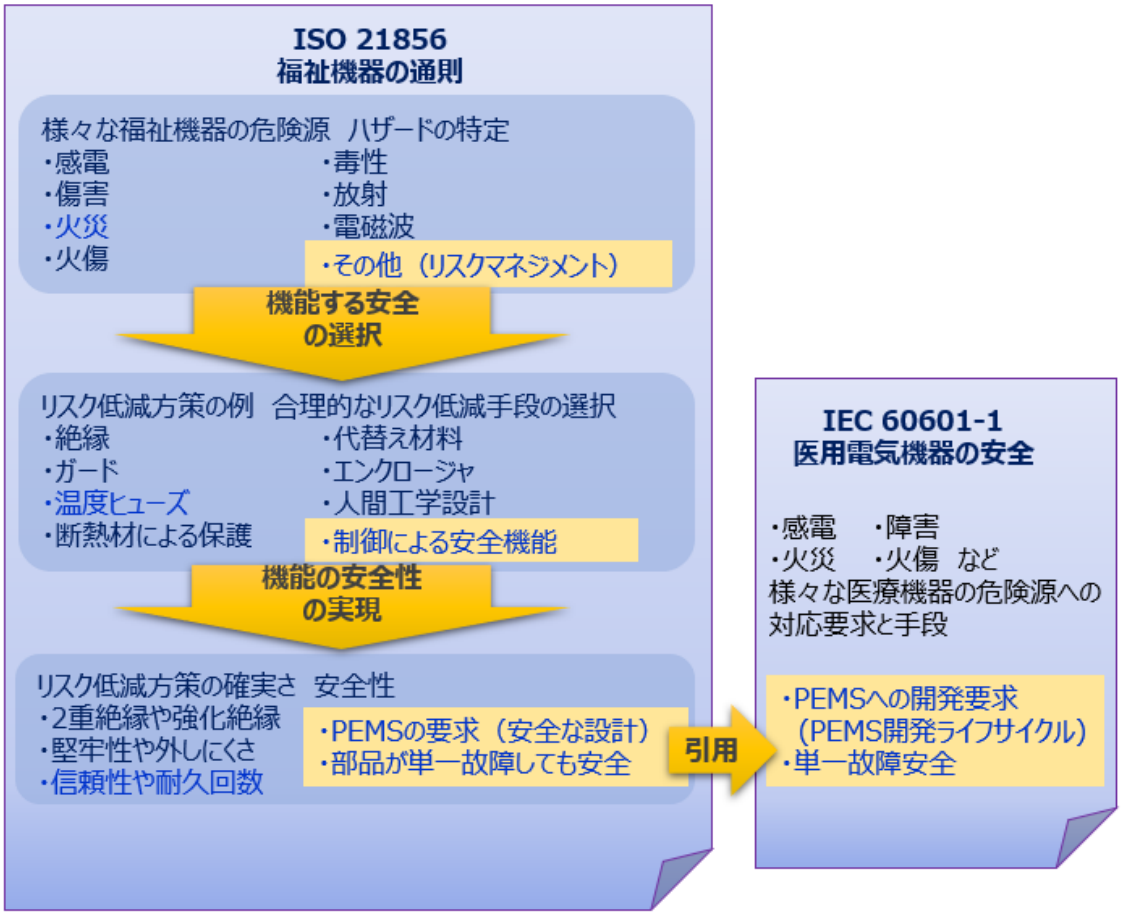


図 2-11 リスク低減手段（保護方策）の選択

図 2-11 に示す火災**ハザード**に対する**保護方策**として，温度ヒューズなどのハードウェアコンポーネントによる**保護方策**，または，サーミスタを含む電子制御回路による**安全機能**と選択肢がある。**保護方策**の選択の際には，想定した**ハザード**から保護できる機能があること（機能する**安全**），及び，**保護方策**が設置された環境・寿命期間中に確実に作動すること（機能の**安全**性）を考慮することが重要である。「想定した**ハザード**から保護できる機能であること（機能する**安全**）。」とは，製品に内在する**ハザード**から，製品の**危険状態**により生じる**危害**までの各段階で誘因となる状態を適切に検出して，**危害**への連鎖を断ち切るような工学的な技術を適切に選択することである。図 2-12 ではサーミスタと CPU の過昇温度検知回路により，基板の温度上昇を検出して，基板が発火する前に，電力供給を遮断する。同様の目的で，温度ヒューズを用いる**保護方策**の例を示しており，どちらも**ハザード**から製品の**危険状態**により生じる**危害**への連鎖を合理的に断ち切ることが出来得る機能を選択しているといえる。

「**保護方策**が確実に作動すること（機能の**安全**性）」の重要性は言うまでもないが，具体的な説明は２．５章の **PEMS 安全**要求適合（IEC 60601-1）要求に譲る。

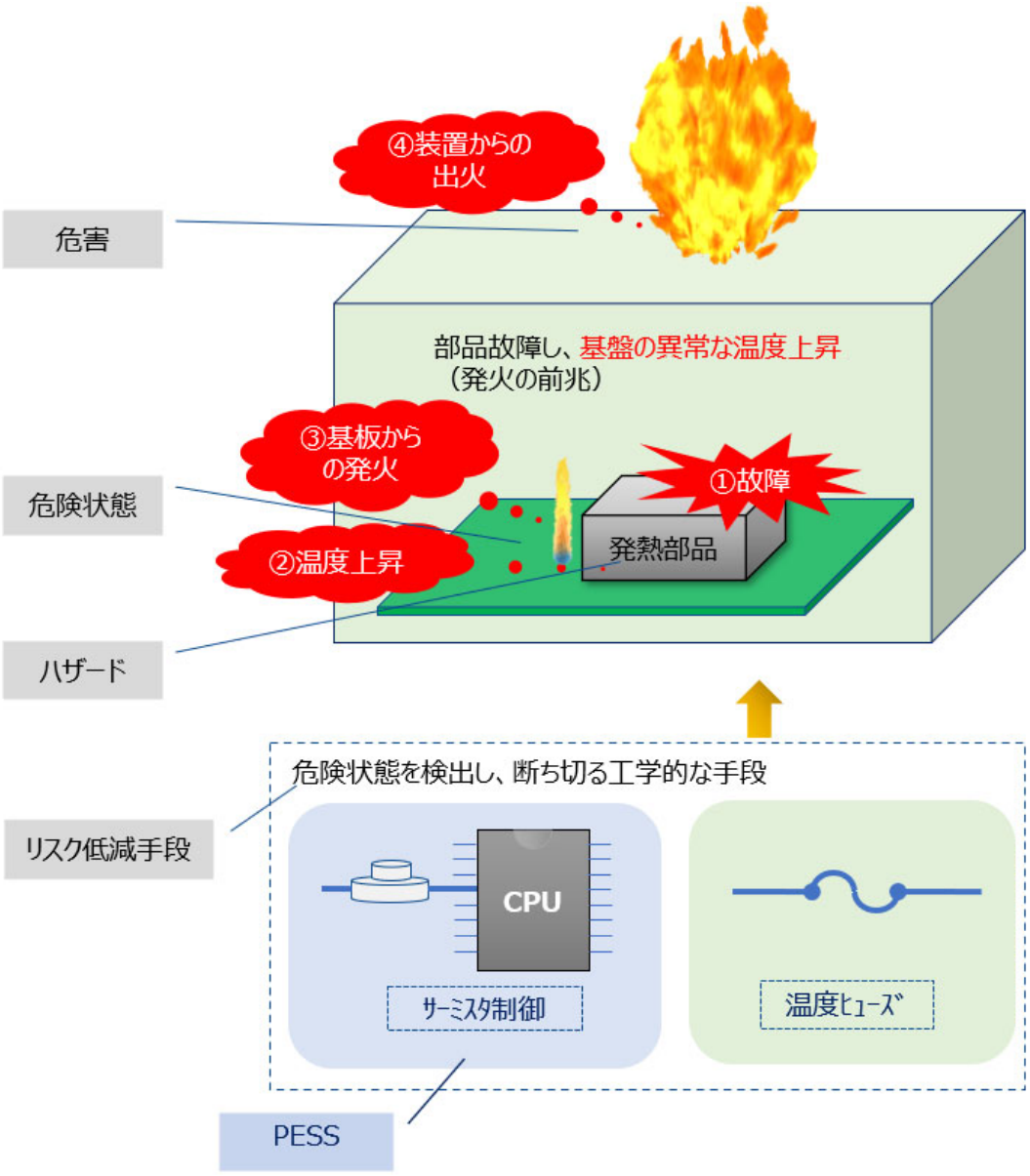


図 2-12 ハザードから危害までの連鎖とその保護方策(PESS を含む)の選択

2.5 開発フェーズ【５】PEMS 安全要求適合（IEC 60601-1）

このフェーズでは，IEC 60601-1 規格の **PEMS** に要求される設計を実施する。
ISO 21856 草案にて，電子制御回路への要求を担う IEC 60601-1 は，さぞかし電子制御回路に関する安全要求や，その対策のための工学的な技法が具体的に示されているものと期待したくなるが，実際には具体的な情報は多くない。IEC 60601-1 規格は医療電気機器の**安全**性に関する一般要求事項扱う規格であり，その中身は感電，火災，火傷，メカニカルな傷害，毒性など，様々な**ハザード**を総合的に考慮した内容になっており，**安全制御回路**に特化した規格書では無いからである。
ISO 21856 草案では具体的に IEC 60601-1 のどこの細分箇条を引用するか示していないため，初読者は規格全体を読解する必要があり，効率性に欠ける。そこで，この章では，電子制御回路の**安全**性を考慮するポイントと，IEC 60601-1 規格のどの箇条に **PEMS** への要求があるかを説明する。
IEC 60601-1 規格が **PEMS** に要求する内容は，主に以下のポイントである。

① 属人的なミスや，設計考慮不足による**故障**やソフトウェアバグなど（**系統的な故障**と呼ぶ）を回避・抑制するため， IEC 60601-1 の箇条 14.2-14.12 の **PEMS** 開発要求に従い，電子制御回路の**安全**性を反復して考慮しながら開発を行うこと。
② ハードウェアの外的ストレスや寿命などによる**故障**（**偶発的な故障**と呼ぶ）時の，ロボット介護機器の**リスク**増加を抑制するため，IEC 60601-1 の箇条 4.7， 13.1-2 の**単一故障安全**を満足すること。
③ **ロボット**が活動する電磁環境下でも**安全機能**が適切に動作すること。これは電磁環境へのイミュニティ要求と呼び IEC 60601-1-2 にて規定される。

(1) 安全機能の確実な作動

ロボット介護機器全体を捉えて確実に**安全機能**が作動するかを考慮する時，PESS の不具合を考慮する。
図 2-13 は発熱部品の通常機能における制御を実現する“コントロール対象の**プロセス**”に対して，サーミスタと CPU による過昇温度検知回路，及び CPU から電力リレーによる電力遮断制御の**安全機能**を実現する部分示したもので，PESS と見なされる。**図 2-13** のように“サーミスタ”，“コントローラ”，“アクチュエータ”の各コンポーネントからなる PESS は以下のようなケースでの**障害**が考**え**られるだろう。

① サーミスタが寿命による**故障**で，**異常**な温度を検出できず，過少温度上昇が継続してしまい基盤発火してしまうかもしれない。
② **異常**な温度を検出した時，本来はリレーを遮断すべきところ，停止信号が外来の電磁ノイズ干渉により打ち消されて，過少温度上昇が継続してしまい基盤発火してしまうかもしれない。
③ **異常**な温度を検出した時，本来は 100ms 以内にリレーを遮断すべきところ，CPU の割り込み処理による遅れで，停止信号送出が遅延して，基盤発火してしまうかもしれない。
④ 操作者が煩わしさから**安全機能**を無効化してしまう不適切行動の可能性。

などが考**えら**れ，これらは電子制御回路に起因する**リスク**の増大である。

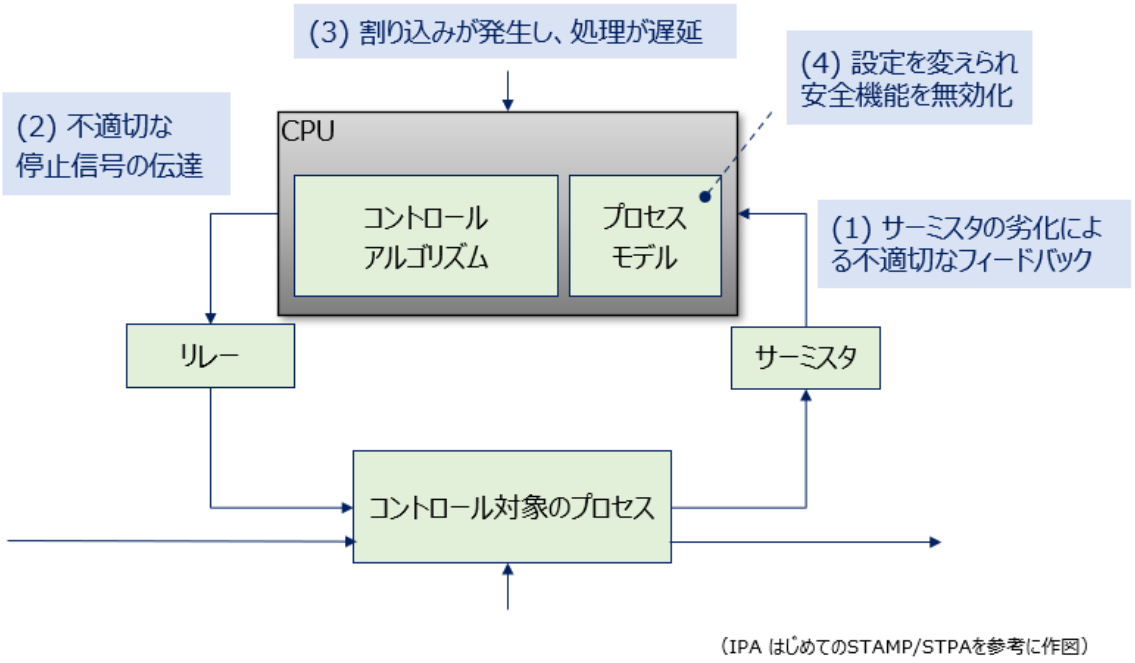


図 2-13 電子制御回路に起因するリスクの増大

このように，**リスク**の増大は，使用環境に対して脆弱なコンポーネント，電子制御回路の構造・アルゴリズム・インターフェースなどの不適切な設計などによるが，**機能安全**の考え方では，物理的現象から人の設計に起因する望ましくない事象まで，これらすべて”**故障**”として捉える。**リスク**に作用する PESS が正常に動作しないと，**PEMS**（**ロボット**介護機器）の**リスク**が増大するわけだが，この“**故障**”の発生を回避，及び抑制し，**リスク**を受容可能なレベルに維持しながら，開発を進めるのが，**PEMS** 開発における**リスクマネジメント**と考える。

箇条 14.8 では，「**アーキテクチャ**の仕様は，**リスク**を受容可能なレベルに低減するため，次の一つ以上を使用する。」とある。

a) **高信頼性部品**
b) フェールセーフ機能
c) **冗長性**
d) **多様性**
e) 機能の分割
f) 防御設計 例えば，利用可能な出力を制限にすることよって，又はアクチュエータの動きを制限する手段の導入によって，潜在的に危険な影響を抑制する。

図 2-14 は，PESS になんらかの望ましくない事象（**故障**）が発生し，PESS に与**えら**れた能力が喪失した**障害**状態を示す。この時，この**障害**状態を検出・回復できれば良いのだが，PESS の**障害**状態が上位**サブシステム**の**故障**になる場合がある。この**サブシステム**が**障害**状態のときに**安全機能**の作動要求が発生すると，**PEMS** における**リスク**増大を引き起こす。このような事象を回避・抑制するために，**リ**

スクマネジメントを反復して実施しながら開発することが要求され、**PEMS 開発ライフサイクル**と呼ばれる 。

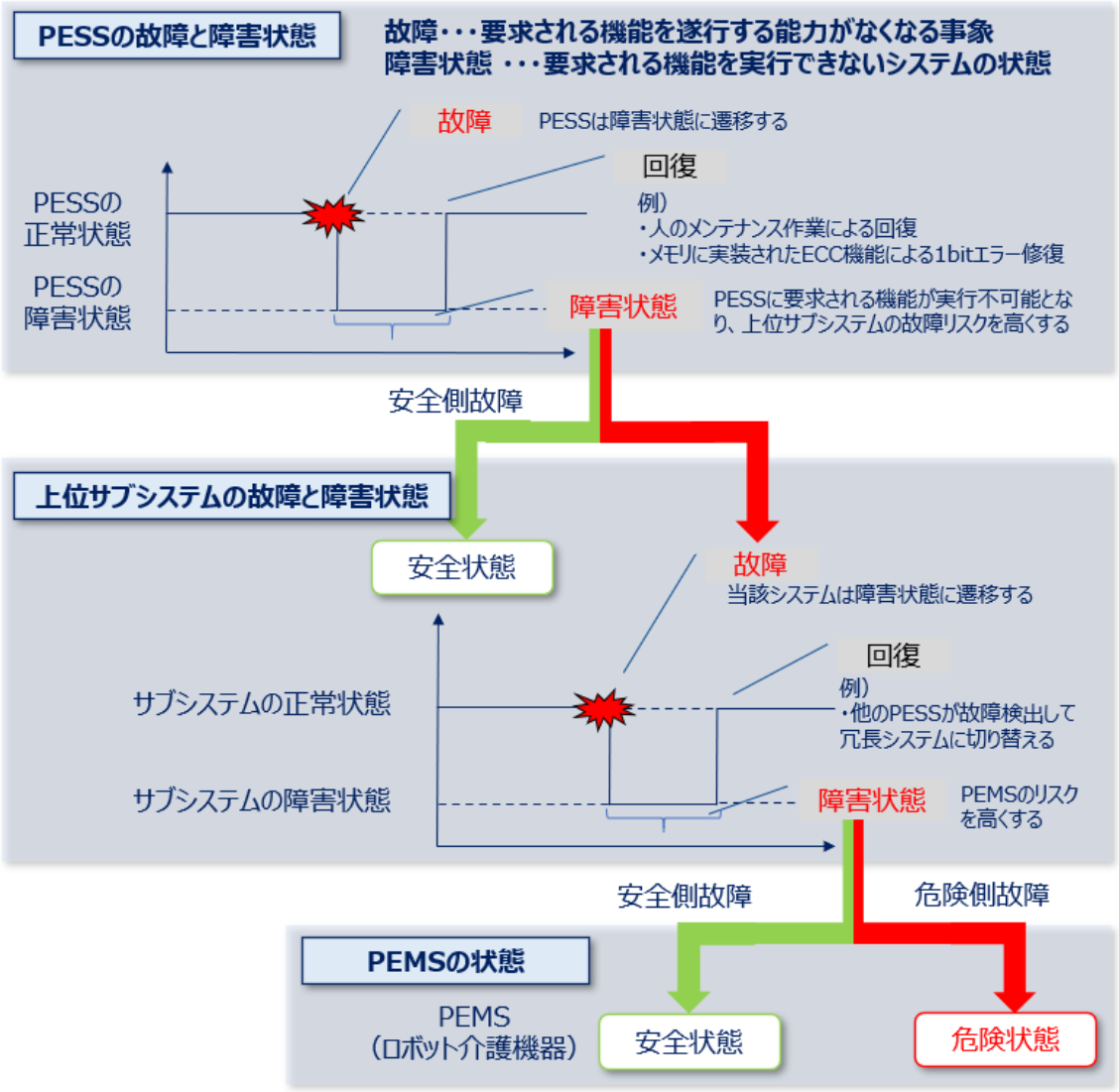


図 2-14 故障と障害状態と PEMS の危険状態

安全機能が，いざという時にきちんと作動するため，PESS の正常な状態を保全する必要がある。ここでは，PESS が**障害**状態になり得る（ならない場合もある）２種類の“**故障**”について解説する。１つは，「（ハードウェアの）**偶発的な故障**」，もう１つは「**系統的な故障**」である。

(2) 故障１．ハードウェアの偶発的な故障

偶発的な故障とは，**安全機能**を実現する電子制御回路を構成する電子・電気部品など，ハードウェアコンポーネントに発生する劣化や単体不良などの**偶発的な故障**を指す。

ある程度の確率では発生するだろうとは推測するものの，「どこで（どの部品で），いつ発生するのか」が確定できない**故障**である。なぜなら，ハードウェアは同じ仕様・条件で製造されても，一定の品質ばらつきは避けられない。また，製造環境，動作時の周囲環境，使用の頻度など，様々な要因により多様なメカニズムのもとで摩耗・劣化する。**図 2-15** にハードウェア故障のバスタブカーブを記す。バスタブカーブは，初期故障期，偶発故障期，磨耗故障期と三つの期間に分けられる。初期故障期の不良を回避するための一般的な手段は，製造工程でのパイロットランニングや部品検査を厳格に行うことである。摩耗故障期の不良を回避するためには，摩耗故障期間に入る前の部品交換など，使われ方を考慮した合理的な周期・方法でメンテナンスを行う。

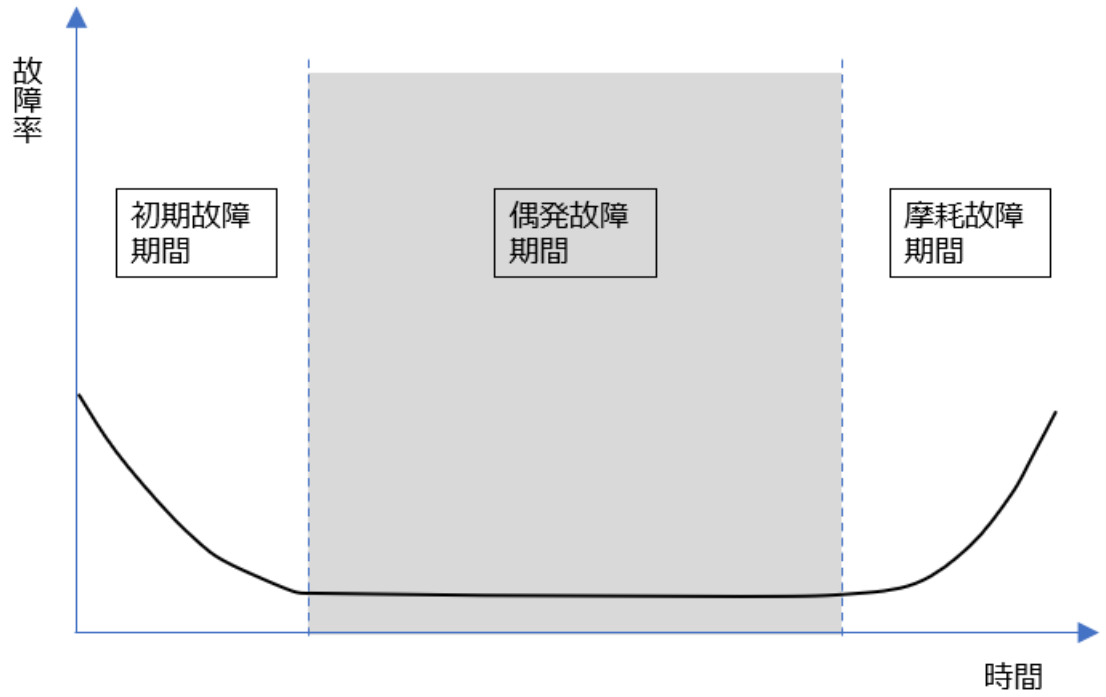


図 2-15 故障率のバスタブ曲線

偶発**故障**期を考慮するため，**予測耐用期間**の間に**障害**に至らない程度に、高い**信頼性**の部品を使用する**保護方策**がある。一方で， IEC 60601-1 では，“**単一故障安全を満たすこと**“が要求される。**単一故障安全**とは，「一つの**故障**が偶発的に起こる可能性はあるが、2 つ同時に**故障**する確率は無視できるほど低いと考え、一つの**故障**で **PEMS** が**安全**側に**故障**することや、一つ目の**故障**を検出することで**故障**の累積を防止し、**危害**に至る**プロセス**を断ち切るという考えである。図 2-16 に IEC 60601-1 の定義を示す。

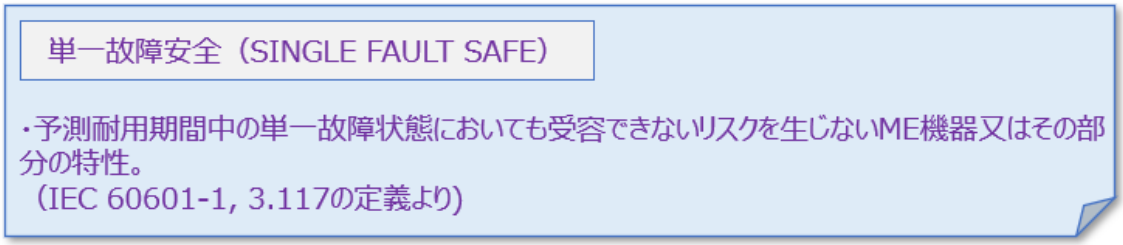


図 2-16 単一故障安全の IEC 規格の定義

単一故障安全の**検証**では **PEMS** の設計解析を行い，予見できる**故障**状態については実際の基板を使って模擬試験も取り入れる。図 2-17 にあるようにハードウェア部品の短絡・開放故障に加え，部品の種類によっては性能がドリフトする現象も考慮される。

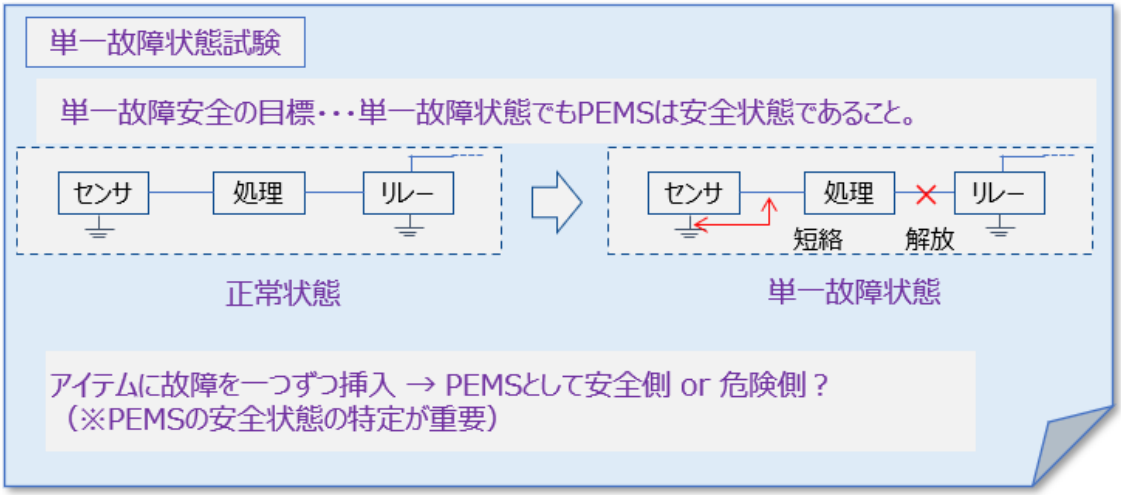


図 2-17 単一故障試験の検証

IEC 60601-1 では**偶発的な故障**の回避・抑制を考慮するため，**単一故障安全**の要求の関連箇条 4.7 **医用機器の単一故障状態** と 箇条 13.1～13.2 **医用機器の危険状態及び故障状態** にて言及する。箇条 4.7 は**単一故障安全**の要求を示し，箇条 13.1～13.2 は具体的に考慮すべき**危険状態**と**故障**状態を挙げている。

まず箇条 4.7 では，医療電気機器は，**単一故障安全**を確保できるように設計し製造するか，又は**リスクマネジメント**を適用して決定したように**リスク**が受容できる状態にすることが求められ，ISO 21856 原案でもこの要求を引用する。**機能安全**では，『部品とは，いつかは壊れる。』という考え方をしており，この規格でも，**ロボット**の**予測耐用期間**の間に，ハードウェアの偶発的**故障**は，ある程度の確率では発生するが，恐らくは**ロボット**の**危険側故障**には至らない程度になるよう，『せめて単一**故障**でも**安全**』を考慮して設計すること。を要求している。

箇条 13.1～13.2 は次の点に注意して読解する必要がある。箇条 13.1～13.2 は電気エネルギによる感電や発火など（例えば，過大な電流が流れて発火しないことなど），制御に関わらない**ハザード**を中心に視点で記載されている。しかし，**安全**関連の **PEMS** についてはこれに加え，単一故障によって

一つの機能が喪失した時に，周りの回路へ影響し，ひいては製品として不安全事象を引き起こすことが無いか，ハードウェアの設計を分析・**検証**することが求められる。具体的には，**故障**挿入試験と呼ばれる**故障**のシミュレーションを行い，**ロボット**介護機器が危険な状態にならないことを確認する。すべての**故障**シミュレーションは，特に端子数が多いマイコンなど，多大な時間を要するため，回路図を読んで**FMEA** などの**故障**解析を行い実際の**故障**シミュレーション試験を省略する場合もある。ただし，どの部分の試験を省略するかは製造事業者の判断(自己責任)に委ねられる。省略する場合には，妥当性のある理由を残さねばならない。
このガイダンスでは第 4 章に「**単一故障安全**の実施ガイド」として詳しく説明を記す。

(3) 故障２．系統的な故障

一方の**系統的な故障**は，とても広い概念である。ソフトウェアのいわゆるバグが**系統的な故障**の典型的な例である。また，ハードウェアでも，例えば CPU のポート処理の不適切さにより，不定なハイインピーダンスポートに隣接する信号線の干渉が生じ，誤動作を起こせば，それは**系統的な故障**になる。それ以外も，ノイズ干渉の考慮が不足した脆弱なプリント基板設計や，ソフトウェアとのインターフェースに係る仕様設定の欠落や連絡ミスや，取扱説明書へのメンテナンス作業指示間違いなども**系統的な故障**と考える。**系統的な故障**は，確率的に発生するのではなく，その間違いに関係する局面になれば，必ず顕在化するのが特徴である。多くの設計者が介在する **PEMS 開発ライフサイクル**において，とても広い局面で要因を仕込んでしまう厄介な**故障**であるが，重要なことは，対処すべき開発**アクティビティ**を計画して，それを確実に実行するために，**検証**をして，文書化して，**トレーサビリティ**を維持し，管理を行うことである。このような開発における欠陥を**故障**として捉えることは馴染みが薄く，理解しづらいかもしれないが，**機能安全**に取り組む場合は必要な考え方である。
「**系統的な故障**の発生を防ぐよう適切に開発すること」の実現方法として，**PEMS 開発ライフサイクル**のモデルの一部を**図 2-18** に示す。**PEMS システム**開発では，ロボット介護機器（製品）の**リスク**低減手段から割り当てられた電子制御回路としての**リスク**低減手段が，要求仕様レベル，機能要求レベル，部品要求レベルと製品化に向けて細分化されて行っても，機能の振る舞いや安全度などの安全要求が引き継がれ，**リスクマネジメント**の視点で繰り返し**検証**を行いながら，組織的に開発を厳しく管理することが求められる。
そのための要求として，IEC 60601-1 では箇条 14 にて **PEMS 開発ライフサイクル**と呼ばれる開発**プロセス**モデルを示している。**PEMS 開発ライフサイクル**を**図 2-19** の**プロセス**モデルで説明する。

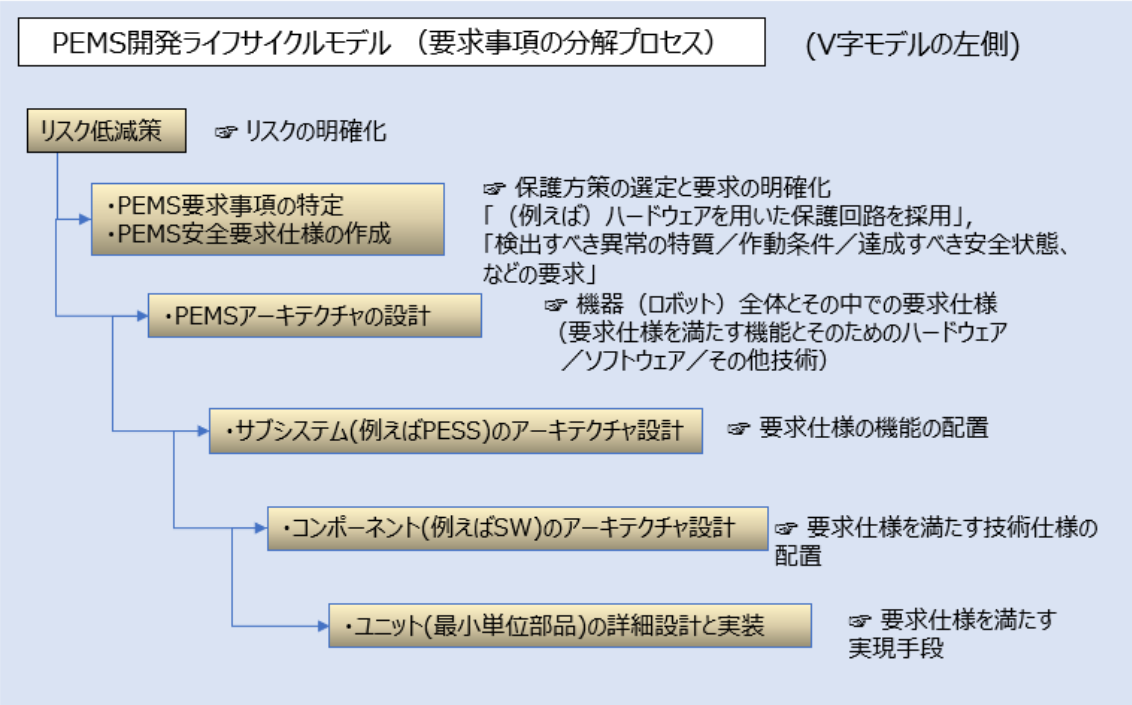


図 2-18 系統的な故障の回避／抑制のためのプロセスモデル

PEMS に要求される**リスク**低減策を入力のトップとし，これを満足するために階層化設計を実施していく。ここで重要な要求は要求仕様の作成，**アーキテクチャ**設計，**サブシステム**設計，コンポーネント設計と製品化に向けて細分化されて行っても，上位**プロセス**で作成した要求仕様を満足するように，下位**プロセス**では設計されることである。また，その各**プロセス**の中では各設計**成果物**に対して ISO 14971 ベースの**リスク分析**が繰り返し行われる。例えば，**PEMS アーキテクチャ**の設計書に対する HAZOP や **FMEA** などの**リスク分析**を行い，機能ブロックに**障害**状態が発生した場合，別系統に切り替えるなどの**保護方策**が検討されるなど，電子制御回路に予想される**故障**への**リスクマネジメント**を行っていく。この活動をＶ字の左側で細分化を行い，最小単位の“ユニット”まで作成する。ここまでの設計**プロセス**が分解**プロセス**と呼ばれる。Ｖ字の右側は逆に結合**プロセス**と呼ばれ，ユニット，コンポーネントから**サブシステム**へと，仕様通りに作られているかを，左側の開発**プロセス**で作成した設計仕様書をベースにユニット試験，結合試験，**システム**試験など，**検証**をしながら，順に結合して行き，**PEMS** を完成させる。

PEMS として完成した後は，**PEMS 妥当性確認**を行い，**リスク**低減策として要求した通りに **PEMS**（ロボット介護機器）が作られているかを確認する。

規格の箇条 14 が「**プログラマブル電気医用システム（PEMS）**」となっているように，電子制御回路への要求としては，PESS ではなくあくまで **PEMS**（ロボット介護機器完成品）を対象としていることである。なぜなら，完成品に実装された多数の**サブシステム**の相互作用を含めた振る舞いの**評価**や，一つの PESS のハードウェア部品が**故障**した時に従動的に他の PESS へも**故障**を波及させないことの**評価**

や，電磁ノイズなどの外的な環境による**安全機能**への影響の**評価**は，完成品でないとできないことにある。

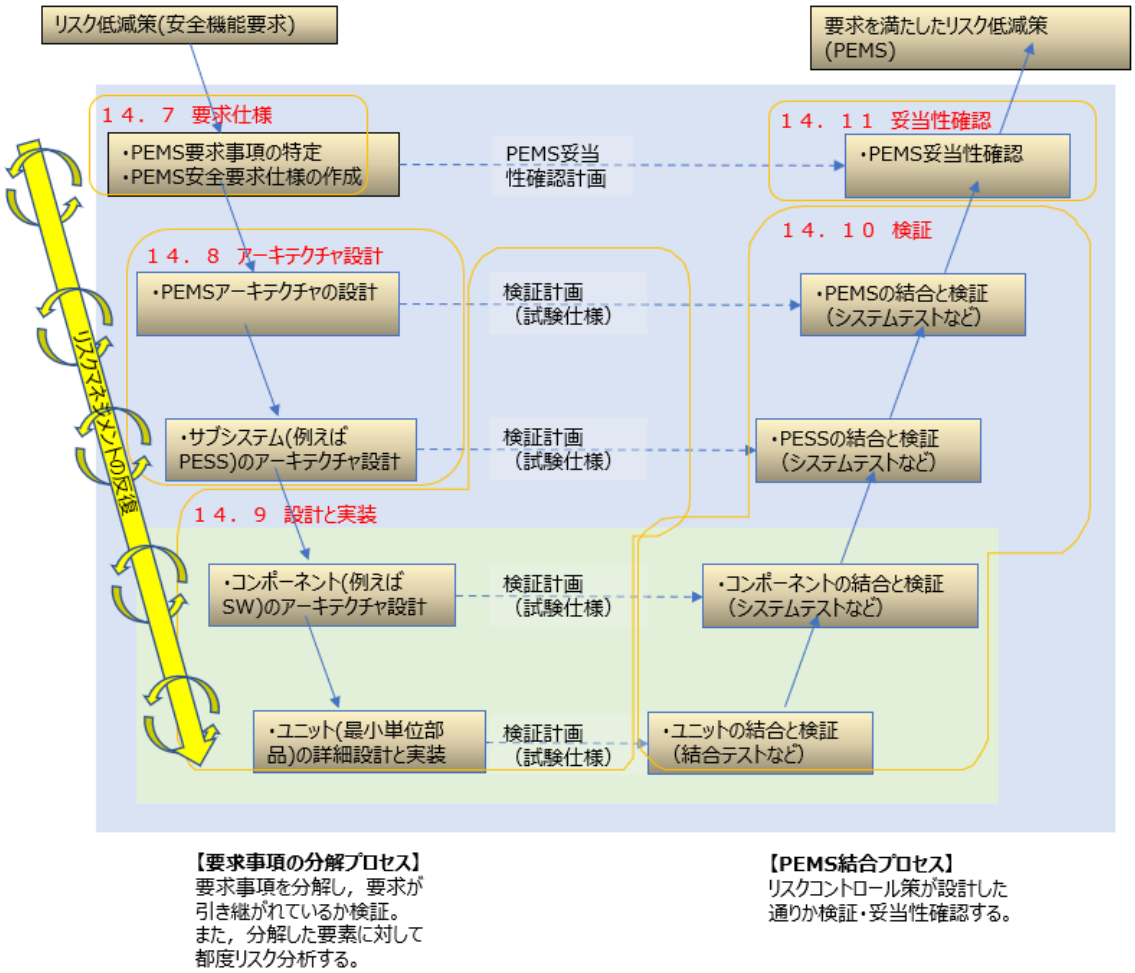


図 2-19　PEMS 開発ライフサイクルの概念図

このガイダンスでは，第 4 章に「**PEMS 開発ライフサイクル**実施ガイド」として詳しく説明を記す。また，**機能安全**の開発工程で活用できる技法の例を付録 B で説明するので参考にされたい。
尚，IEC 60601-1 の箇条 14.1 では，ソフトウェアを含む場合，各 PESS のソフトウェアの開発又は変更管理に対して，IEC 62304 の箇条 4.3，箇条 5 及び箇条 7～箇条 9 への適用が要求されている。ISO 21856 は IEC 62304 を直接言及していないが，対象の箇条には適合する必要があるだろう。ソフトウェアの開発又は変更管理の説明はガイダンスの第 5 章に譲る。

電子制御回路は，電磁環境下で，電子制御回路がノイズ干渉による不作動を起こして，仕様通りの動作を侵害するケースをも**系統的な故障**の一つである。

この**系統的な故障**を回避・抑制するためには，電子制御回路の誤動作による**リスク**の増加に着目したEMC 設計が求められる。ノイズ源の特性や侵入ルートに応じた対応策と一定以上の耐性を持つことが求められる。これをイミュニティ（電磁ノイズ耐性）の確保と言い，考慮された設計と適切な**妥当性確認**試験が求められる。**検証**は最終機器を用い実際を模擬したノイズ環境下で試験をすることを基本とする。適切な設計考慮や実装のミスは電子回路の不作動にもつながるため，**機能安全**では電磁ノイズからの影響により**安全機能**が侵害されることも**系統的な故障**の一つに分類される。ISO 21856 は IEC 60601-1-2 を引用することによってこのイミュニティ耐性に関する要求を求めている。

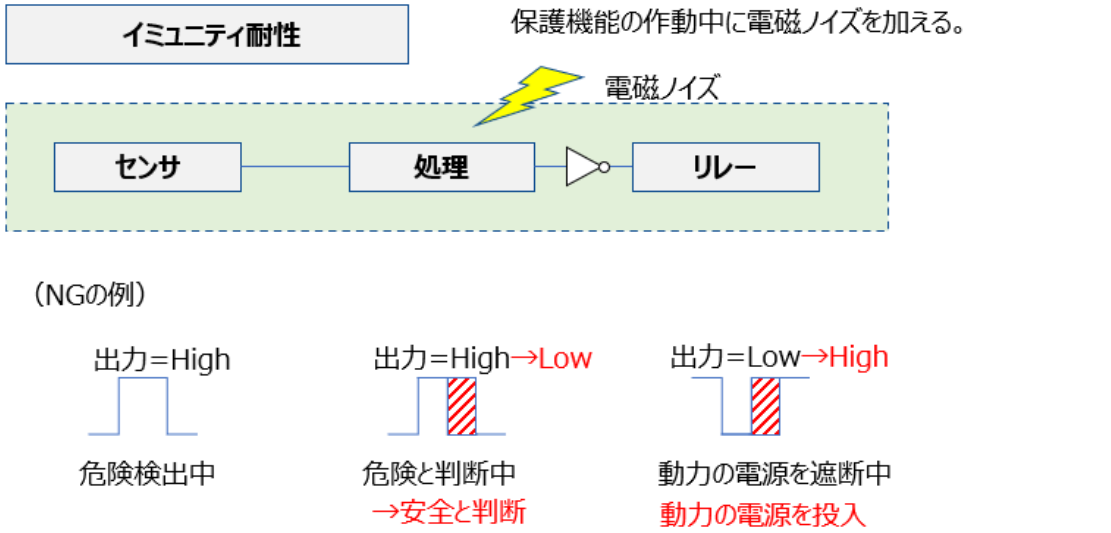


図 2-20 安全機能の作動中に電磁ノイズが加わる

医療機器の規格 IEC 60601-1-2 では，**PEMS** が**安全**を達成するために，単純にイミュニティ試験レベルで試験すればよいと考えてはならないことに注意する必要がある。**図 2-21** は，**リスクマネジメントプロセス**をベースとした EMC 設計の中で，IEC 60601-1-2 規格をどのように引用すればよいか，対象となる箇条と情報源を示している。

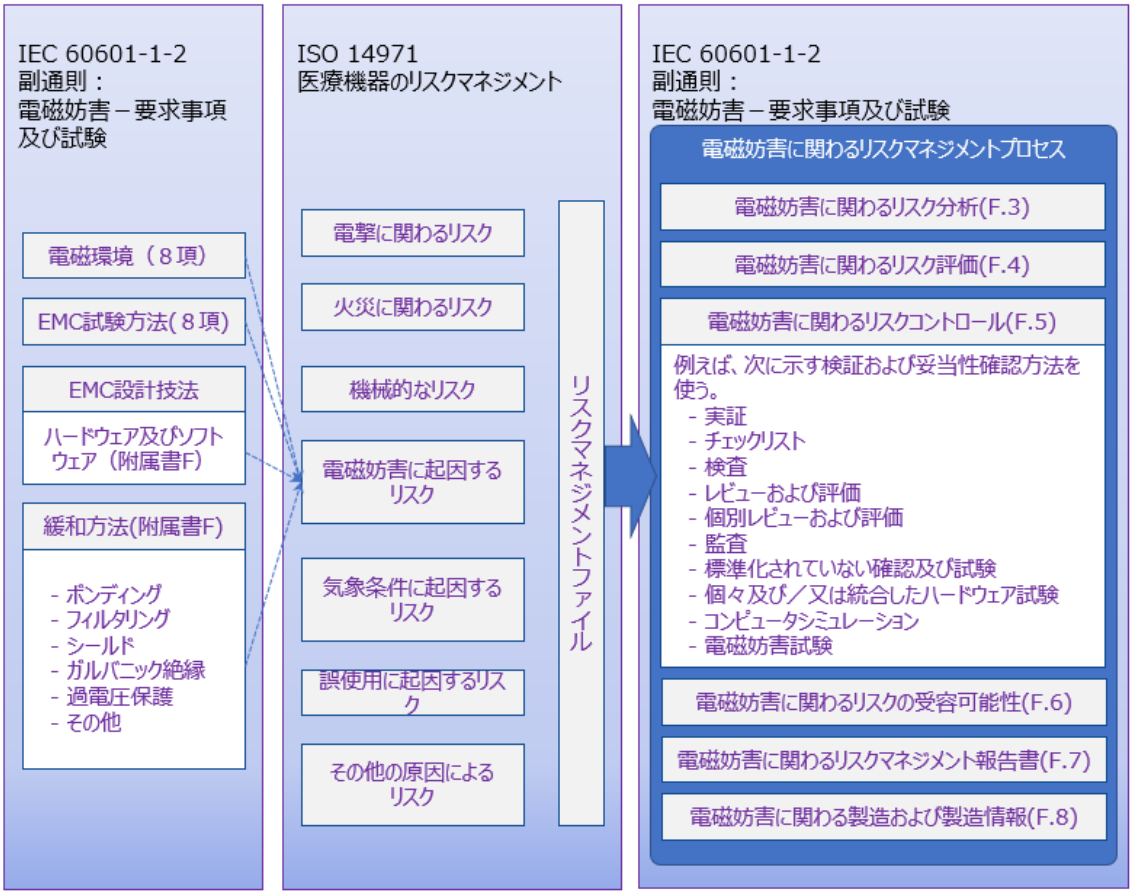


図 2-21 リスクマネジメントプロセスにおける IEC 60601-1-2

このように，**PEMS** への要求は多岐にわたり，細かな設計・管理要求が存在する。したがって，**PESS** はなるべく小規模で，ロボット介護機器のそれ以外の**安全**には関係ない電子制御回路からは物理的もしくは論理的に分離されることが開発効率の向上につながる。このガイダンスでは第 4.3 章に「電磁ノイズ耐性の要求」として説明する。

ここまで，開発フェーズ【５】電子制御回路の **PEMS** 要求適合の要件について説明してきた。図 2-22 は，ISO 21856 が要求する電子制御回路への **PEMS** 要求の規格体系を図にまとめたものである。ISO 21856 が電子制御回路へ直接要求する部分は少ないが，実は複数の引用規格に引き継がれており，該当する箇条も入り組んでおり，初めて取り組む開発者にとっては導入準備が必要となるだろう。

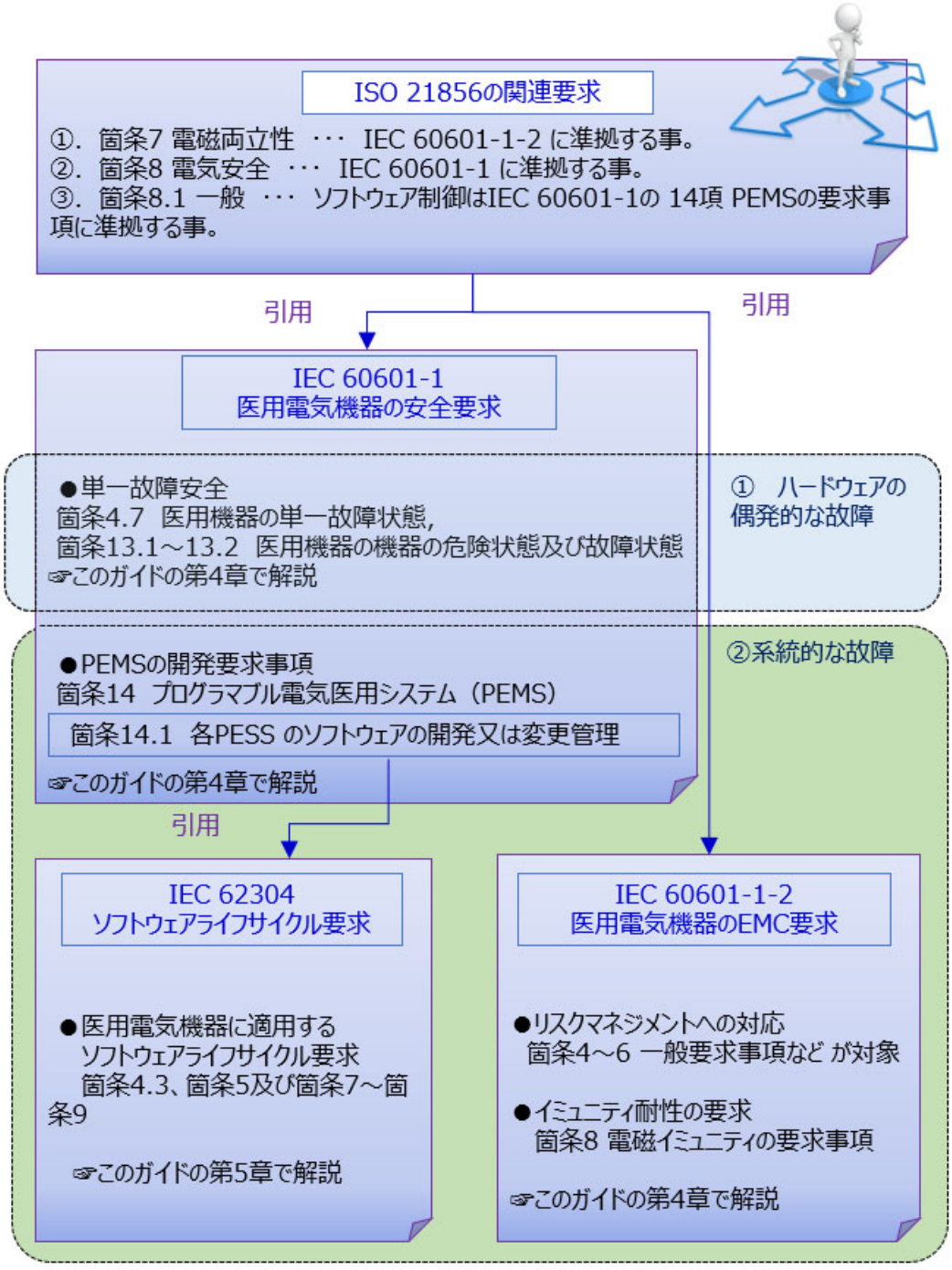


図 2-22　ISO 21856 の安全制御回路開発要求

2.6 開発フェーズ【６】ソフトウェアのライフサイクル要求（IEC 62304）

このフェーズでは，IEC 62304 規格の**ソフトウェアライフサイクル**で要求される設計を実施する。
図 2-23 に示す通り，**PEMS 開発ライフサイクル**のＶ字左側，分解**プロセス**で**要素**分解され，そのうちソフトウェアコンポーネントに関する部分については IEC 62304 の**ソフトウェアライフサイクル**要求に準拠することが求められる。

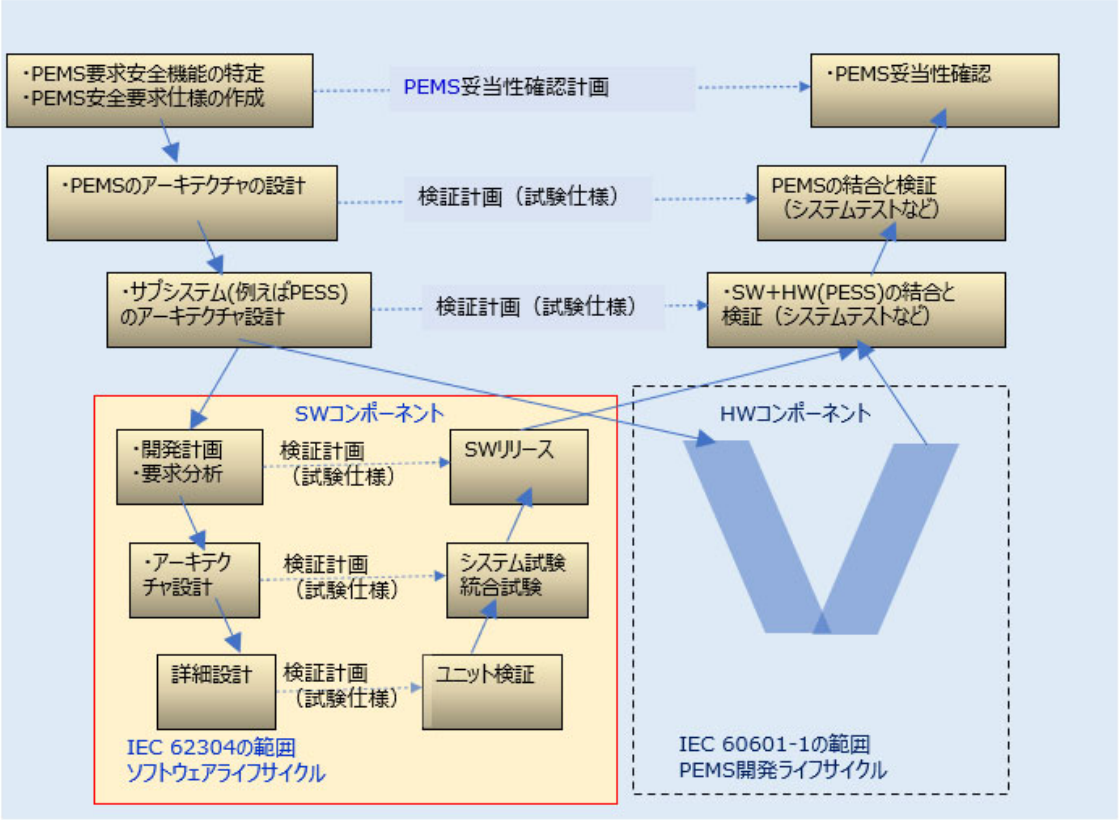


図 2-23 IEC 62304 の範囲：ソフトウェアライフサイクル

ロボットを含む福祉機器の国際規格 ISO 21856 は，この規格自体にソフトウェア開発について具体的な要求を言及せず，細かな要求は，専用の規格 IEC 62304 を引用する構成になっている。この規格は，多種多様な医療電気機器の**システム**に対応するため，それらすべてに汎用的に適用できるような**プロセス**要求がメインになっている。そのため，ソフトウェア品質管理に馴染みがない製造事業者においては，自社の開発にどう適用すれば良いのかイメージしづらいという問題がある。そこで，この規格の主要な要求とその考え方を理解するために，IEC 62304 の対象箇条とその概要を説明する。
ISO 21856 草案では，**ロボット**介護機器の動作制御のためにソフトウェアを用いている場合は，IEC 60601-1 の箇条 14 の適合を要求する（ISO 21856 草案，箇条 8.1），IEC 60601-1 の箇条 14 では，次のようなケースに **PEMS 開発ライフサイクル**の要求が示される。

【PEMS 開発ライフサイクルの特別な要求を適用するケース】

① **プログラマブル電子サブシステム**（PESS）が，**基礎安全**又は**基本性能**に必要な機能を提供する場合。

② 箇条 4.2 に従った**リスクマネジメント**の適用によって，PESS の**故障**が受容できない**リスク**を生じないことを立証できない場合。

この **PEMS 開発ライフサイクル**の要求を適用する場合は，各 PESS のソフトウェアの開発又は変更管理に対しては IEC 62304 の細分箇条 4.3，箇条 5，及び箇条 7～箇条 9 の要求事項も適用することが要求される（IEC 60601-1，箇条 14.1）。ここで，このソフトウェア要求の概要を説明する。

① 細分箇条 1.4 適合性

この規格は**安全**なソフトウェアを生産できる**プロセス**を考慮し，その最低限実施すべき**アクティビティ**及び**タスク**を特定して，要求事項とする。**リスク**に基づき**ソフトウェアアイテム**の**安全**性クラスを明確化し，そのソフトウェア**安全**性クラスに従って，この規格に明示されたすべての**プロセス**，**アクティビティ**，及び**タスク**を実施し，それらの要求事項を満たせば，そのソフトウェアはこの規格に適合するといえる。適合性の**評価**は，規格が文書化を要求する内容を記述した文書，及びその他の**記録**を調査することにより判定する。文書や**記録**の様式について規定は無いため，適切と考える様式を用いる。

② 細分箇条 4.3 ソフトウェア**安全**クラス分類

ソフトウェアシステムに起因する**危険状態**がもたらす**危害**の**リスク**に応じて，各**ソフトウェアシステム**をソフトウェア**安全**クラス（A，B 又は C）に分類する。これは，**プロセス**を**リスク**に基づいた厳格さで実施するためである。製造事業者は，要求**安全**仕様の中で，ソフトウェアを使用する**システム**が誘発する**ハザード**の結果として，被介護者，介護者，又はその他の人に与える影響に応じて，ソフトウェア**安全**性クラスを，次のような**重大さ**に基づいて指定しなければならない：

クラス A： 傷害又は健康被害の可能性なし

クラス B： 重大でない傷害の可能性あり

クラス C： 死亡又は重大な傷害の可能性あり

次に，この規格でソフトウェア**安全**クラス毎に，要求されている**プロセス**，**アクティビティ**及び**タスク**を実施することが要求される（つまり，**安全**クラス C の方が多くの要求がある。）。

プロセスとは規格本文の箇条 5 から箇条 9 で示される以下の**プロセス**を対象にする。

5 ソフトウェア開発**プロセス**

6 ソフトウェア保守**プロセス**

7 ソフトウェア**リスクマネジメントプロセス**

8 ソフトウェア**構成管理プロセス**

9 ソフトウェア問題解決**プロセス**

アクティビティとは，**プロセス**の内の活動であり，**タスク**とは，**アクティビティ**内の活動であり，規格の細分箇条が対応する。

例えば，図 2-24 に示すように，ソフトウェア開発**プロセス**の要求は，規格の箇条 5 にて言及される。**プロセス**の中にはいくつかの**アクティビティ**があり，そのうちの一つが"ソフトウェア**アーキテクチャ**開発**アクティビティ**"であり，規格の細分箇条 5.3 にて要求されている。更に，**アクティビティ**内にはいくつかの**タスク**があり，ソフトウェア要求事項を**アーキテクチャ**に変換する**タスク**があり，これは規格の細分箇条 5.3.1 にて言及される要求に従って開発を進めることが求められる。

図 2-24 ソフトウェアライフサイクルでのプロセス，アクティビティ，タスクの関係

③ 箇条 5 ソフトウェア開発**プロセス**
開発**プロセス**で要求されるアクティビティや**タスク**を規定する。アイテムに割り当てられたソフトウェア**安全**クラスに基づき，要求されるアクティビティや**タスク**を計画及び実行する。

④ 箇条 7 ソフトウェア**リスクマネジメントプロセス**
IEC 62304 では，ソフトウェアを有する機器においては，**製造業者**はソフトウェアが引き起こす**危険状態**を分析し，**リスクコントロール**を行うことが求められる。この規格は ISO 14971 を引用しており，適合する**リスクマネジメントプロセス**を使用しながら，この箇条では，それに付加してソフトウェア**リスクマネジメントプロセス**を独自に要求する。

この規格 IEC 62304 は，高品質で**安全**な**医療機器ソフトウェア**を，常に製造することを目的としている。この目的を達成するために，この規格では，**信頼性**の高い**安全**なソフトウェアを生産できる方法で**ソフトウェアライフサイクル**と呼ぶ開発エンジニアリング活動を要求する。図 2-25 は**ソフトウェアライフサイクル**の活動概念図だが，考え方は **PEMS 開発ライフサイクル**と同様である。ソフトウェア要求仕様の決定からソフトウェア**アーキテクチャ**設計，詳細設計，実装（コーディング），各**評価**と続く開発**プロセス**の**リスクマネジメント**を反復して行うことを規格では求めている。また，結合**プロセス**では，仕様を満足した各アイテムが適切に組み付けられ，分割**プロセス**で設定された要求仕様を満足することがを**検証**され

記録される。尚，この規格には具体的な情報は記載がないが，各開発**プロセス**で”**機能安全**”で実績のある**安全**技法を用いることが，個々の**ロボット**の**リスク**に応じた対策のポイントと考える。

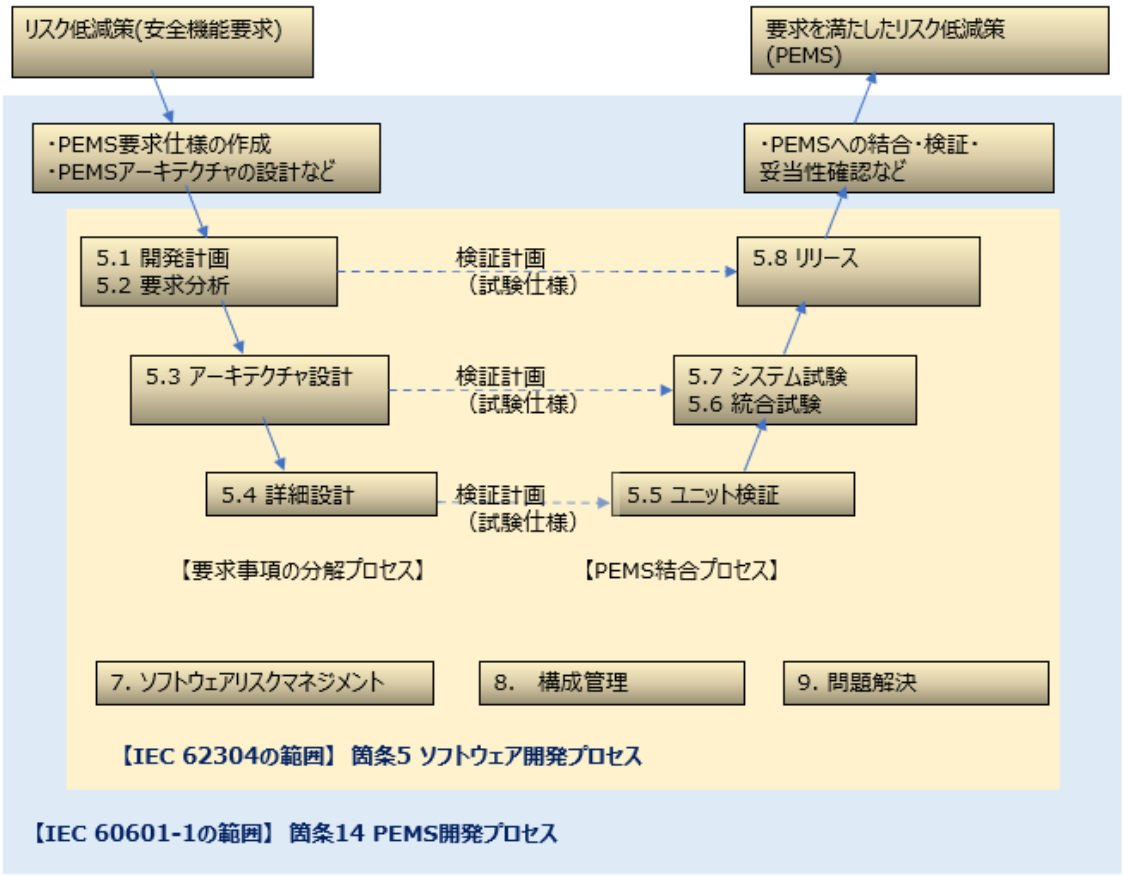


図 2-25 ソフトウェアライフサイクルの概念図

⑤ 箇条 8 ソフトウェア**構成管理プロセス**

IEC 62304 では，**ソフトウェアライフサイクル**全般にわたって管理**手順**及び技術的**手順**を規定し，適用するソフトウェア**構成管理プロセス**を要求する。この**プロセス**では文書を含む**システム**における**構成アイテム**（COTS や OSS を含む**ソフトウェアアイテム**，設計文書，構成ファイル及びインストール用スクリプト，ソフトウェア**リリース**生成に使用するコンパイラ，オペレーティング**システム**及び開発ツール，試験結果**記録**などの**成果物**のこと）の識別及び定義，アイテムの修正及び**リリース**の管理，アイテム及び変更要求の状況の文書化や報告を行う。

⑥ 箇条 9 ソフトウェア問題解決**プロセス**

IEC 62304 では，開発及び保守を含む**ソフトウェアライフサイクル**において，問題又は不適合が発生した時に，**製造業者**がソフトウェア問題解決**プロセス**を使用することを要求する。この**プロセス**の**アクティビティ**では，発見された問題と**安全**性の関係性について分析，**評価**，

解決する上で，通知，認識及び文書化などを行う。

以上，IEC 60601-1 で指定した IEC 62304 の対象箇条の概要を説明した。ここで，「対象外の箇条はまったく考慮をする必要がないのか」，疑問が湧く。結論としては， **PEMS** の開発**プロセス**のみを扱う IEC 60601-1 の適用範囲に含まれる箇条の該当を言及しており，たとえ対象外の箇条でも**安全**なソフトウェア製品を市場に投入し，維持するための，重要となる情報を含んでいる。この点も含め，ソフトウェア**開発ライフサイクル**の推奨される取り組みについて，このガイダンスでは，第 5 章「**ソフトウェアライフサイクル**の実施ガイド」として説明を記す。

2.7 PEMS 開発の品質管理

電子制御回路の開発では，開発者の属人的なミスが**ロボット**介護機器の**安全**な開発を阻害する可能性がある。これを防止するために設計管理の要求がある。設計管理要求を満たして開発を行うことを確実にするためには，品質マネジメント**システム**をベースにした体系的な開発管理が推奨される。
品質マネジメント**システム**の規格（例えば ISO 13485）では，**システム**の有効性を維持・改善するために，**プロセス**アプローチが推奨される。この**プロセス**アプローチとは，組織内で用いられる**プロセス**及び，その**プロセス**間の相互作用を体系的に明確にし，運営管理することである。
プロセスとは，”インプットをアウトプットに変換する，相互に関連する又は相互に作用する一連の活動（ISO 9001）”と定義される。この**プロセス**の考えのもと**安全**要求仕様作成**プロセス**に関連するインプット事項として機器の要求仕様，**リスク分析**結果，類似機種に関する事故事例などのインプットされるべき文書を明確にし，**安全**要求仕様書，**安全検証**仕様書，レビュー結果**記録**などの定められた文書がアウトプットできるような仕組み・ルールを決めておく。
そのために必要な**プロセス**として，**安全**要求仕様に関するレビュー**プロセス**を設ける。対象の検討情報をインプットとして，レビュー報告書，申し送り事項への依頼書などをアウトプットにするなど適切なレビューが可能な**プロセス**を設け，十分なリソースを用意し，漏れの無いよう**検証**項目を定めておくなどレビューの**プロセス**も明確にしておくことが重要である。
このように**プロセス**及びその相互関係を明確にすることで，品質に関する問題が発生した時に，品質マネジメントの有効性を損なう原因となる**プロセス**を特定して改善しやすいというメリットを持つ。このような**プロセス**構築はプロジェクト単位よりも，むしろ開発組織単位で行われる。
厳密に言えば，ISO 21856 原案に基づく一連の電子制御回路の**安全**要求には品質マネジメント**システム**の要求は言及されていない。また，PESS ソフトウェアでは，IEC 60601-1 が IEC62304 の細分箇条”4.1 品質マネジメント**システム**”を除外しているように，**PEMS** の開発にあたって品質マネジメント**システム**を要求はしていない。しかしながら，IEC 62304 箇条 B.4 にて，**医療機器ソフトウェア**の**安全**性を向上させる三つの大原則として **リスクマネジメント**，品質マネジメント，ソフトウェアエンジニアリングが挙げられ，**開発ライフサイクル**での品質マネジメントの重要性に言及する。また，本来の IEC 62304 の開発では，**医療機器ソフトウェア**の**製造業者**は，顧客要求事項及び該当する規制要求事

項に適合する**医療機器ソフトウェア**を提供する能力があることを証明することが求められており（IEC 62304 箇条 4.1），例として ISO 13485 などの品質マネジメント**プロセス**への適合が挙げられている。このように実質的に，IEC 62304 を実施する製造事業者には提供能力が求められることには変わりはない。したがって，品質マネジメント**システム**の関連する要求事項について必須ではないが，推奨される。具体的には，**トップマネジメント**がコミットした，**安全**を含めた開発管理**システム**が構築され，設計開発規定などで**安全**な製品を実現するための**プロセス**が規定化される。**安全**活動が行われるのに十分なリソースが整備され，計画➡実行➡**検証**➡改善が適切に行われながら開発が進められ，**記録**が文書化されることが必要である。
このように電子制御回路を用いた**安全**確保には多岐にわたる準備と活動が求められる。
注記：開発の実際の時系列とは一致しない場合がある。例えばソフトウェアの開発計画は全体開発のスケジュール都合上，ソフトウェアコンポーネントに要求を割り付ける以前に行われる場合が一般的である。

ここまでの解説で，**ロボット**介護機器の**リスク**低減を制御で行うための背景と要求概要。国際的には**医療機器**同等の要求となる事情。国際規格 ISO 21856 原案に従って開発を行うための道筋を説明した。**医療機器**の規格要求に馴染みの無い開発者にとって導入の参考になれば幸いである。
第 3 章以降では，実際に導入をする開発者を対象に医療系電子制御回路の安全規格と機械系**機能安全**規格の共通項目と差分項目に焦点を当て，各規格要求の解説を行う。また，第 6 章は，これらの規格に準拠した開発の流れをスタディケースとして紹介する。

① 第 3 章 ・・・ ロボット介護機器の**リスクマネジメント**のためのガイダンス（ISO 14971 の要求解説）
② 第 4 章 ・・・ ロボット介護機器の安全制御回路のための**システム**開発のガイダンス（IEC 60601-1， IEC 60601-1-2 の要求解説）
③ 第 5 章 ・・・ ロボット介護機器の安全制御回路のためのソフトウェア開発のガイダンス（IEC 62304 の要求解説）
④ 第 6 章 ・・・ **ロボット介**護機器の安全制御回路の開発事例

注記 この章では，国際規格 ISO 21856 に適用するロボット介護機器の安全制御回路への開発要求に沿って，適合すべき規格とその箇条を説明した。この流れを，欧州 CE マーキングへの適合手順と誤解しないようにご注意願いたい。CE マーキング（**医療機器**規制）への適合を欧州委員会官報に記載される整合規格を用いる時，以下の規格はいずれも整合規格リストに含まれ，すべての箇条に適合する必要がある。
EN ISO 14971:2012，EN 60601-1:2006，EN 62304:2006，EN ISO 13485:2016
（EN Official Journal of the European Union, No. L 90 I/6）

3　リスクマネジメント実施ガイド（ISO 14971）

3 章では，**医療機器**規格に馴染みのない，一般の生活支援**ロボット**の開発者が，海外展開用のロボット介護機器を開発する際に要求される**医療機器**の**リスクマネジメント**に対応するケースを想定する。
ISO 21856 原案では，医療系**リスクマネジメント**規格 ISO 14971 をメインに，関連する部分を機械系**リスクアセスメント**規格 ISO 12100 を引用して，**リスク**をマネジメントとすることが要求されている。
ISO 14971 の**リスクマネジメント**要求は，ISO 12100 の**リスクアセスメント**要求と共通する部分が多いので，機械の**リスクアセスメント**を十分に理解済みの開発者にとっては，差分を理解した上で，**ロボット**介護機器のための開発**プロセス**として、仕立て直し（テーラリング）を行うことが効率的である。
この 3 章では，まず医療系**リスクマネジメント**規格 ISO 14971（以後「この規格」と呼ぶ）の全体像を説明し，その後に，図 3-1 に示すように，機械**安全**の**リスクアセスメント**との比較を行い，この規格特有な要求事項をメインに解説を述べる。

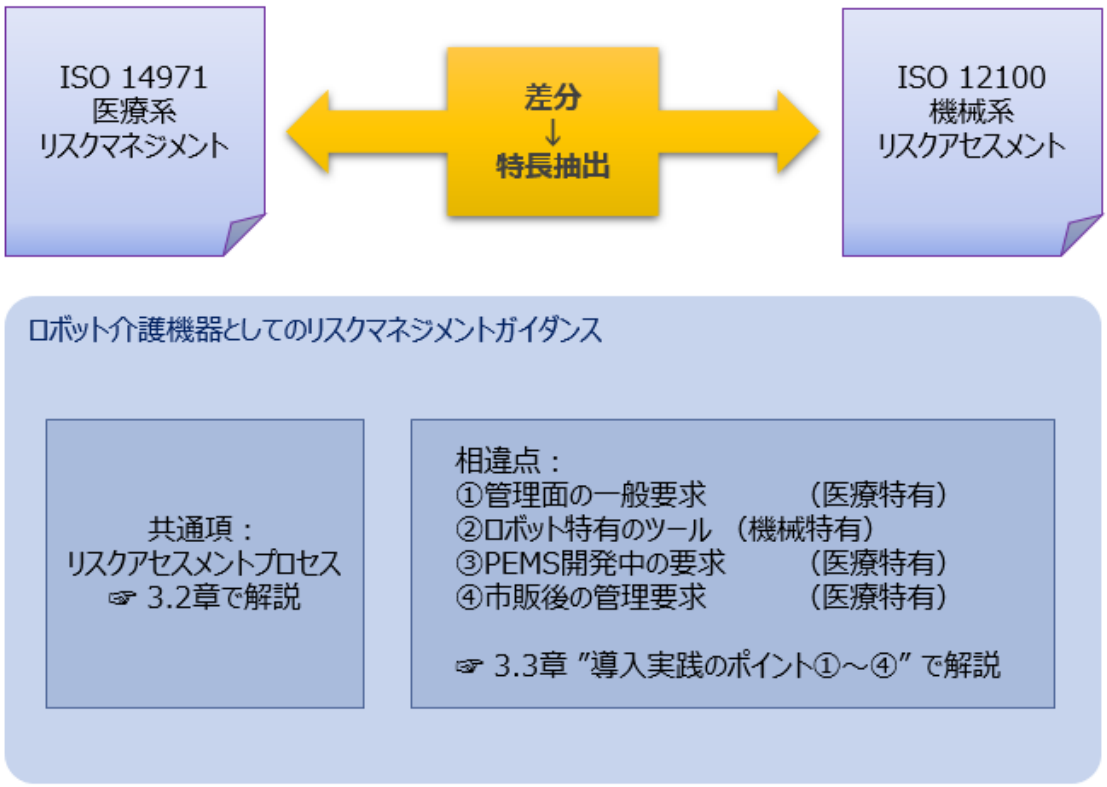


図 3-1　医療機器規格と機械系規格のギャップ

3.1 ISO 14971 規格の全体像

まず，この規格の構成を簡単に説明する。現行の ISO 14971:2019 の構成は本文 16 ページに対し，附属文書は 19 ページあり，附属文書の情報ボリュームは大きい。要求事項は本文のみに記載があり，附属文書はあくまで参考情報の位置付けである。

規格本文では，箇条 1 には本規格の適用範囲が，箇条 2 には用語や定義が記載されている。箇条 3 には，**リスクマネジメント**全体に共通した一般要求事項が記載されている。**リスクマネジメント**を実施する前提として，**プロセス**が確立され，具体的な活動が計画されていることがあり，この要求内容が示される。続いて，箇条 4 の「**リスク分析**」から箇条 9 の「製造中及び製造後の情報」には，**リスクマネジメント**の**プロセス**毎の具体的な説明と要求事項が記載されている。箇条 4 と箇条 5 の**プロセス**を合わせて**リスクアセスメント**と呼ばれる。また箇条 6 の**プロセス**は機械**安全**の**リスク**低減**プロセス**に相当するものである。

附属文書は，あくまでも参考情報なので適用は任意であるが，**リスクマネジメント**活動を行う上で活用できる具体的な情報が盛り込まれている。

医療機器の規格 ISO 14971 と，機械**安全**の規格 ISO 12100 は，ともに ISO/IEC Guide 51 を参照し，この Guide のコンセプトを踏襲して開発された規格であり，要求の根幹である**リスクアセスメントプロセス**については双方の規格とも同様となっている。図 3-2 は ISO 14971 規格本文の構成を図示したもので，図内の番号は規格の箇条を示す。図 3-2 は ISO 12100 と同様の**プロセス**を薄黄色に，差異がある**プロセス**を水色に色別しており，ここから**医療機器**の**リスクマネジメント**の大半の**プロセス**が，一般の生活支援**ロボット**の開発者にもお馴染みの機械の**リスクアセスメント** ISO 12100 の**プロセス**と同様であることが見て取れる。差異がある部分（水色）は，箇条 3 と箇条 9 である。ISO 21856 原案の箇条 4.1「**リスク分析**と**リスクマネジメント**」では，「支援機器の**安全**性は，ISO 14971 及び関連する場合は ISO 12100 で規定された**手順**を用いて，**ハザード**を特定し，それらに関連する**リスク**を推定することによってアセスメントされる。」とあり，ISO 12100 の共通**プロセス**をベースに ISO 14971 の要求コンセプトと差分取り組みを理解し，効果的に対応していくことがポイントになる。以下では**リスクマネジメント**の考え方を解説した上で，差分である箇条 3 と箇条 9 を重点ポイントとして解説し，一般の生活支援**ロボット**の開発者が，海外展開の**ロボット**介護機器を開発する際の**リスクマネジメント**を支援する。

注記： ISO 12100 （JIS B 9700 ） の**リスクアセスメント**に馴染みがなく，**ロボット**介護機器に適した**リスクアセスメント**基礎から習得する場合は，安全ハンドブック『2-1 リスクアセスメントの基礎と RA シートひな形説明』を参照することをお勧めする。

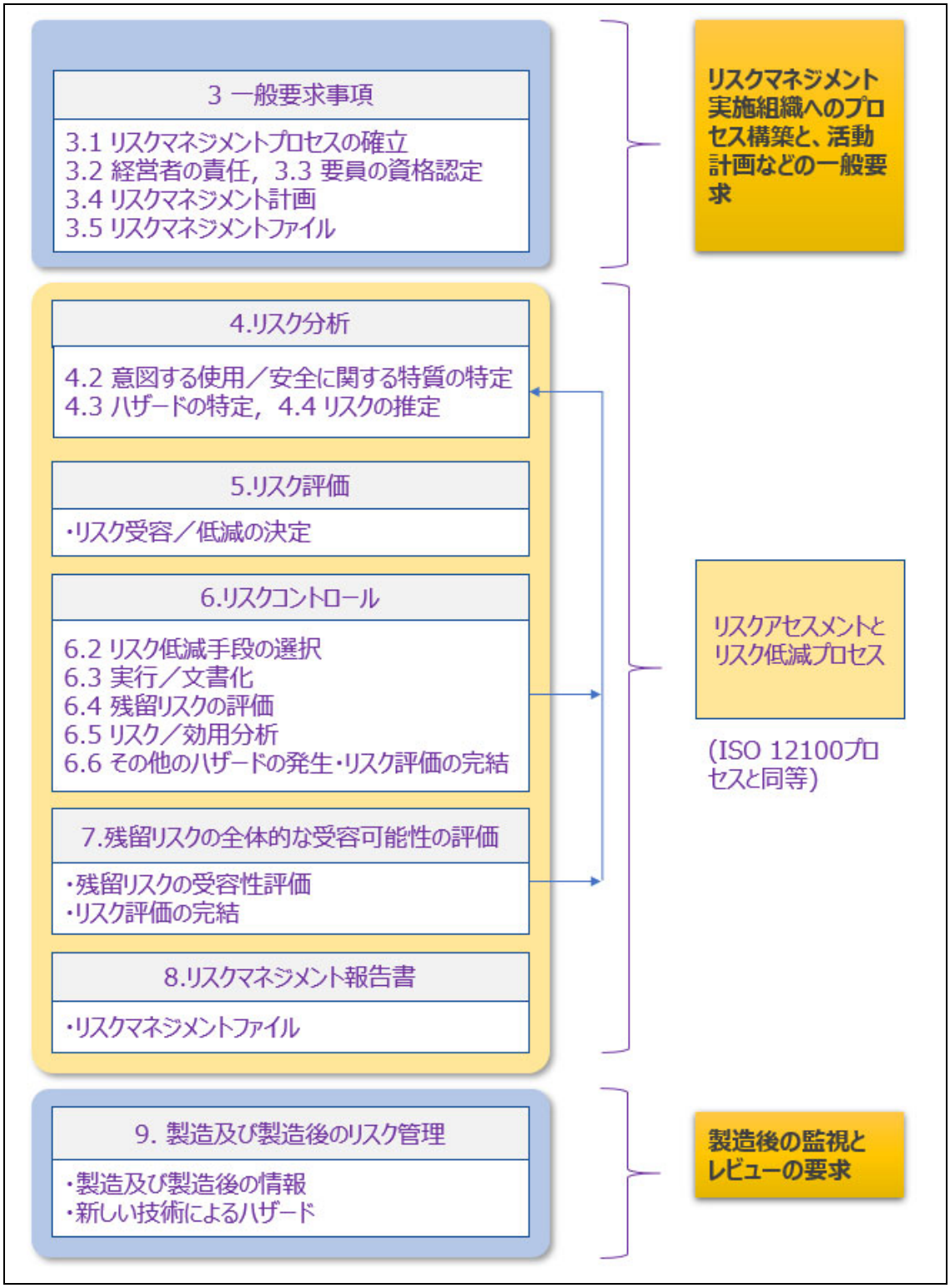


図 3-2　ISO 14971（要求事項部分）本文の構成

3.2 ISO 14971 附属書の解説

ここでは，この規格の附属書について紹介する。この規格の附属文書は，あくまでも参考情報であり，要求の強制力はないが，実務を行う上において便利な情報を扱っており，**リスクマネジメント**の適切な**プロセス**において有効に活用したい。手短に記載内容をつかむため，表 3-1 にその概要と活用方法を記す。

表 3-1　ISO 14971:2007 附属書の内容とその活用方法

ISO 14971:2007 附属書	解説と活用方法
Annex A Rationale for requirements	・規格要求事項の解説。この規格の要求コンセプトを理解するために一読をされたい。 ・旧版からの改訂された際の議論についても触れており，より深く理解できる。 ・**トップマネジメント**による方針策定の要求などが最新版で強化され，この規格にて重要であることが説明されている。
Annex B Overview of the risk management process for medical devices	・**リスクマネジメント**の詳細フロー。 ・本文の図１（簡易版フロー）をより正確に理解する場合にはこちらのフローを参照する。 ・フローにおける一つ一つの**要素**は規格の箇条番号に対応する。旧版規格ではこの**要素**を Step1-13 とステップの呼称として扱われていた。
Annex C Questions that can be used to identify medical device characteristics that could impact on safety	・本文箇条 4.2 で要求されている**医療機器**の**安全**に影響する特質の明確化をチェックリスト形式で行うツール。 ・非常に多くの**医療機器**製造事業者に活用されている実績がある。 ・ロボット介護機器についても活用をお勧めするが，その場合は介護機器用に質問事項を見直すのが良い。

ISO 14971:2007 附属書	解説と活用方法
Annex D Risk concept applied to medical devices	・**リスクマネジメント**における考え方の指針を示しており，**リスクアセスメント**および**リスクコントロールプロセス**は ISO 12100 の該当部分と考え方に本質的に差異が無いことが分かる。 ・一方で、「D.5.4 製造**プロセス**及び**リスクコントロール**」や、「D.6 **リスク**／効用 分析」など，特長的な考え方についての解説がある。 ・定性的／準定量的アプローチにおける 5x5 の**リスク**マトリクス法が参考として紹介されており，実際の開発でも**リスク**の受容可能性の判断基準はこのようなマトリクス表などにより製造事業者が規定することが一般的である。 ・あくまで参考情報なのでこの方法及び受容性判断例が強制されているわけではない。
Annex E Examples of hazards, Foreseeable sequences of events and hazardous situation	・**ハザード**，**危険状態**，**危害**の関係が分かりやすく説明されているため，**ハザード**の特定と**リスク**の推定の際に参考になる。ここでも, ISO 12100 の考え方に本質的な差異が無いことが分かる。 ・**ハザード**の特定の際には，”引き金事象”，”**危険状態**”，”**危害**”まで一連の情報が備わっていることがポイントであるが，その考え方の例として表 E.3 に記されている。 ・表 E.1 は機器の**ハザード**がバランスよくまとまっており，**ハザード**の特定**プロセス**で文書化に使用するのに便利かもしれない。しかしながら，**ロボット**特有の情報はほぼ無いので補強する必要がある。 ☞このガイダンス 3.4.2 章に活用方法を示す。
Annex F Risk management plan	・**リスクマネジメント**計画に関する解説 ・**医療機器**特有の**プロセス**である**リスクマネジメント**計画の**アクティビティ**（活動すべき内容）について解説されている。計画書類を策定し，それに従って開発することは**機能安全**の**開発ライフサイクル**でも求められているため理解する必要がある。
Annex G Information on risk management techniques	・PHA，**FMEA**，FTA， HAZOP など**リスクマネジメント**と組み合わせて使用することができる品質工学を用いた**リスク分析**ツールの紹介。

ISO 14971:2007 附属書	解説と活用方法
Annex H Guidance on risk management on lVD medical devices	・体外診断用(IVD)医療機器に関する指針。 ・体外診断用医療機器における危除状態の考え方などが記載されている。 ・IVD 機器の特質の明確化ではこの指針・情報が活用されている。
Annex I Guidance on risk analysis process for biological hazards	・生物学的**ハザード**に関する解説。 ・生物学的**ハザード**の特定をする場合に活用できる。
Annex J Information for safety and information about residual risk	・**残留リスク**がある場合にユーザに提供すべき情報について言及されている。

3.3 リスクマネジメントの説明

ここでは，**リスクマネジメント**と**リスクアセスメント**との差異を解説する。国際規格 IEC/ISO 31010「**リスクマネジメント－ リスクアセスメント**技法」では，**リスクマネジメントプロセス**全体を**図 3-3** のような構成で記述しており，**リスクアセスメント**は**リスクマネジメント**の中核**プロセス**としている。**リスクアセスメント**は独立した活動ではなく，**リスクマネジメントプロセス**の他の構成**プロセス**と密接に結びつき,経営組織の中で体系的に管理されることが重要とある。

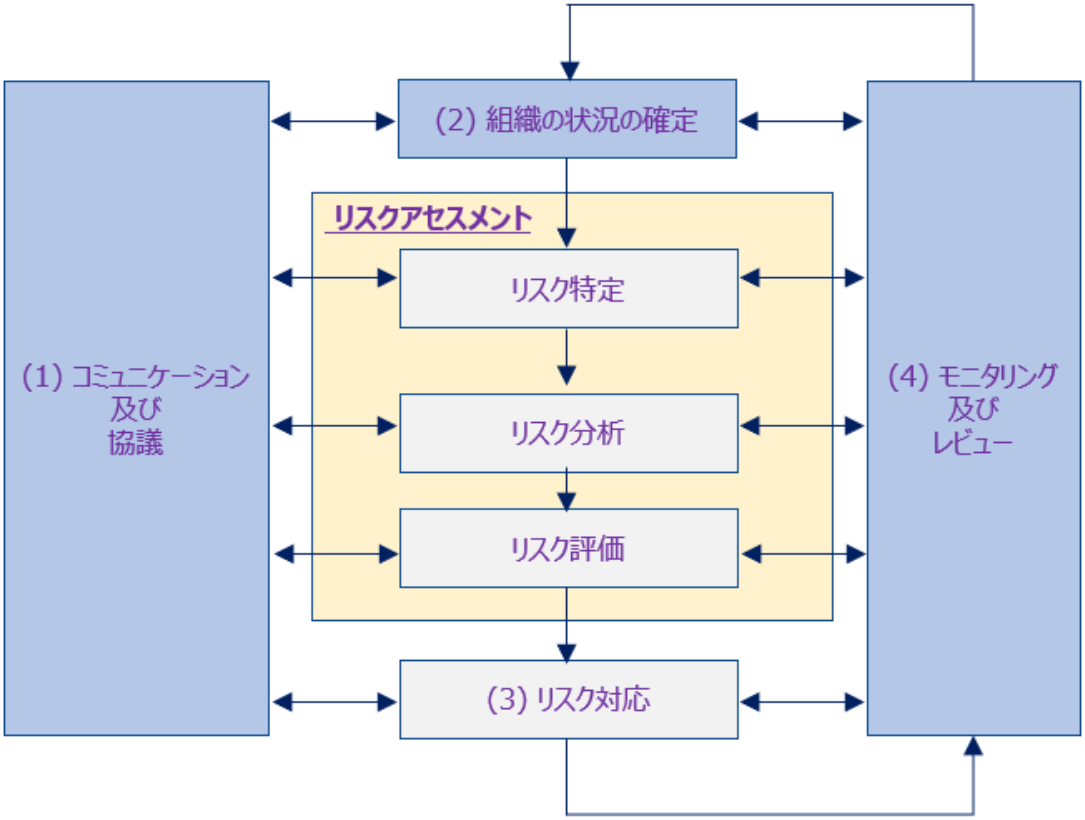


図 3-3 リスクマネジメントプロセスに対するリスクアセスメントの寄与（IEC/ISO 31010）

他の構成**プロセス**とは図 3-3 の白枠の部分であり，各**プロセス**を簡単に説明する。

(1) **コミュニケーション及び協議**

ステークホルダとの有効なコミュニケーション，及び協議があって**リスクアセスメント**は成功する。そのため，コミュニケーション計画を策定し，この計画は組織的に承認及び支援される。その結果，適切な条件の決定，ステークホルダとの利害の理解，異分野の専門知識の収集，多様な見解の考慮など，**リスクアセスメント**で有効な効果が期待できる。

(2) **組織の状況の確定**

リスクベースの開発を管理するための，組織としての基本的な条件を決定しておく。また，**リスクアセスメント**や**リスク**対応などの後工程に対する活動範囲や管理基準を計画策定にて明確にし，組織内で合意を図るようにする。基本的な条件とは，組織の内部条件（リソースや知識，情報の流れ，意思決定**プロセス**などを言う），及び外部条件（規制や市場の情報，ステークホルダの価値観などを言う）を含む。

ISO 14971 の箇条 3 には，**リスクマネジメント**を実施する前提として，**プロセス**が確立され，具体的な活動が計画されていることを要求するが，この**プロセス**に該当する。

(3) **リスク対応**

IS0/IEC Guide 51「Safety aspects - Guidelines for their inclusion in standards」にて言及されるように，製品安全では一般的に**リスク**低減 （**リスクコントロール**や**リスク**の最適化とも言う）を実施することが一般的であるが，ISO/IEC Guide 73「Risk management — Vocabulary」では，それ以外にも**リスク**の回避（撤退する。巻き込まれないようにする），移転（保険などで他者と共有する），保有（損失・**障害**を受容する）なども手段として定義されている。ロボット介護機器の安全制御回路の開発取り組みは,第 2 章で説明した通り，多岐にわたり,厳しい管理が要求されるため，製造会社として**リスク**が取れるのか経営判断が必要になるかもしれない。

(4) **モニタリング及びレビュー**

リスク管理策を定期的に**監視**し，レビューを行うことが求められる。また，**安全**な製品を提供する**リスクマネジメント**活動のアカウンタビリティ (説明責任)を確定することが望ましい。

レビューは，以下の視点で行うこととなる。

- **リスク**に関する前提条件が依然として有効であるか？
- 内部及び外部状況の仮定が依然として有効であるか？
- 予想した結果を達成しているか？
- **リスク**対応策が有効であるか？

ISO 14971 の箇条 9 の「製造中及び製造後の情報」では，製造後も**リスクマネジメント**の継続を要求するが，この**プロセス**に該当する。

以上のように**リスクアセスメント**のメイン**プロセス**に加え，関連する構成**プロセス**までを含んだ取り組みが**リスクマネジメント**では求められ，特徴的な部分だと言える。

3.4 ロボット介護機器のリスクマネジメントのポイント

ここでは，一般の生活支援ロボットの開発者が，**医療機器**としての**ロボット介護**機器のため**リスクマネジメント**活動を行う上で，追加で考慮すべき取り組みを説明する。

ISO 21856 原案では，**リスクマネジメント**の引用規格として，ISO 14971 と ISO 12100 の 2 つの規格が示され，2 つの規格の使い方について，具体的に示していない。（**図 3-4**） このガイダンスでは，基本的には非医療の**ロボット**介護機器の開発者向けなので，ISO 12100 の**プロセス**（既知領域）をベースに ISO 14971 の差分（新規領域）を理解し，効果的な**ロボット**介護機器の**リスクマネジメント**を実施するためのテーラリングを行うことを推奨する。

4 General requirements 4.1 Risk analysis and management ● The safety of an assistive product shall be assessed by identifying hazards and estimating the risks associated with them using the procedures specified in ISO 14971 and, if relevant, ISO 12100. ● (参考和訳) 4 一般要求事項 4.1 **リスク分析**と**リスクマネジメント** ● 支援機器の安全性は，ISO 14971 及び関連する場合は ISO 12100 で規定された**手順**を用いて，**ハザード**を特定し，それらに関連する**リスク**を推定することによってアセスメントされる。

図 3-4 ISO 21856 原案の箇条 4.1 Risk analysis and management を抜粋

非医療の一般生活支援ロボットの開発者が、**医療機器**と見なすロボット介護機器の**リスクマネジメント**を実施するためのテーラリングのポイントを説明する。**図 3-5** は ISO14971 **リスクマネジメントプロセス**の簡易フローにテーラリング実践ポイント①～④を示したものである。この図のポイント①～④は，**医療機器**と機械**安全**の双方の規格の相違点に着目し、導出したものである。

- ①及び④は，ISO 14971 **リスクマネジメントプロセス**おいて、比較的具体的な要求事項が定められている工程である。医療系の**リスクマネジメント**に馴染みがない場合は，考慮しておきたい。
- ③では，**リスクマネジメント**後の **PEMS 開発ライフサイクル**での活動について説明する。**リスクマネジメント**は，試作品がない構想の段階で開始され，設計**プロセス**を実施し，設計仕様や構造が明らかになっていく中で，**リスク**の推定が具体的になり，正確になっていく。特に **PEMS** や医療系ソフトウェアでは開発**プロセス**中の**リスクマネジメント**が規格で求められるので，その関係を関連する規格を挙げて説明する。
- ②は，ISO 14971 は，対象機器が異なるので，**ロボット**など機械製品特有の**ハザード**を扱う

具体的な情報源が不足している。多くの開発者は，ISO 13482 や，ISO 12100 などを参照することを試みるとは予想するが，初めて取り組む開発者向けに，**ロボット**特有の**ハザード**を補うための情報を紹介する。

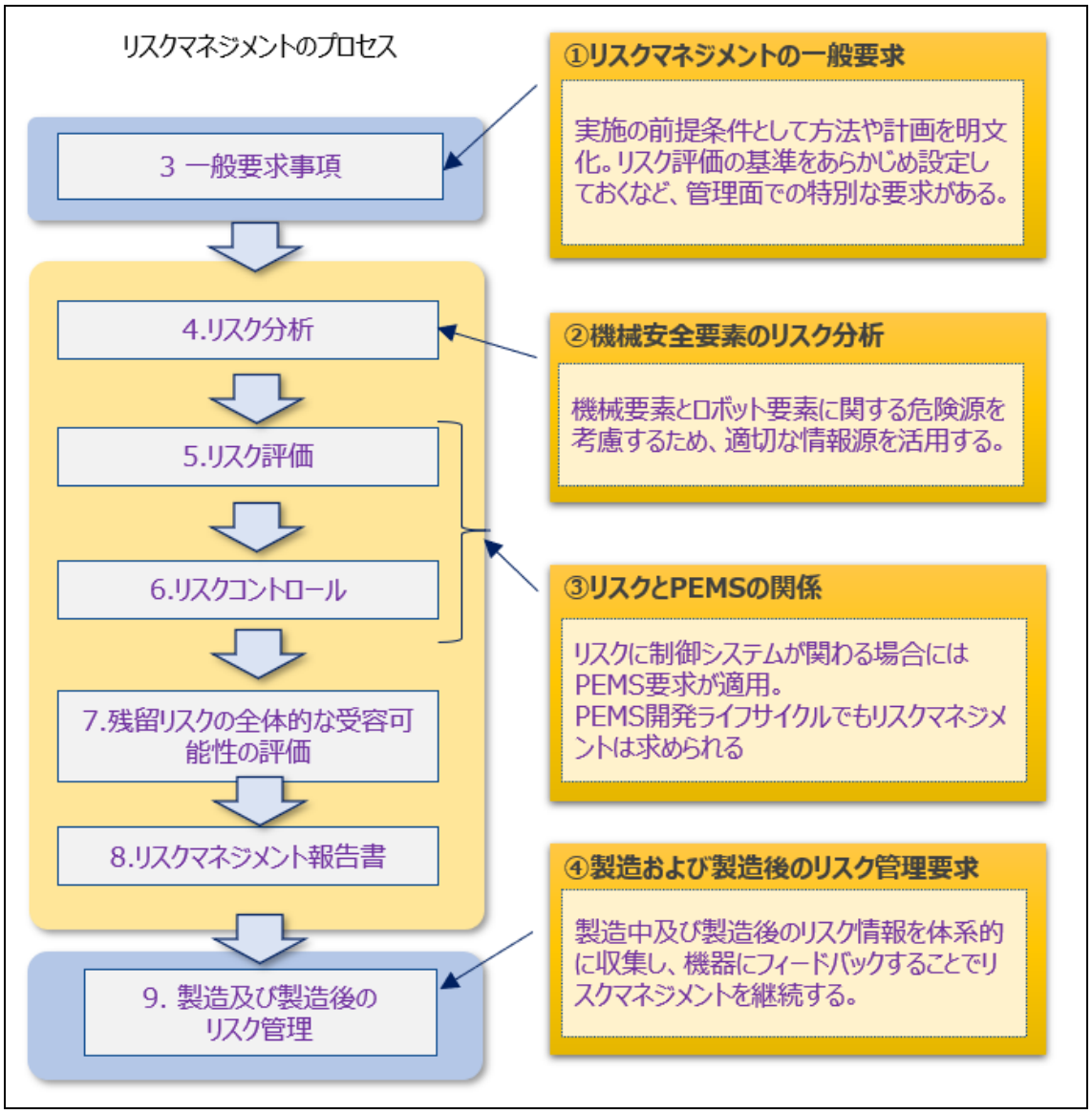


図 3-5 リスクマネジメント導入実践のポイント

3.4.1 ポイント① リスクマネジメントの一般要求

この規格の特徴として規格の箇条 3 では，製品開発の前段で**製造業者**（会社組織）として又は特定の開発プロジェクトとして，**リスクマネジメント**の実施規定や具体的な活動計画を文書化する要求がある。

本来，**医療機器製造業者**は，QMS 省令などの法規制や ISO 13485 などの品質マネジメント**システム**の要求にて，**リスクマネジメント**体制の維持・管理がなされているのが一般的で，この規格についても，**リスクマネジメント**の管理面での一般的な要求を箇条 3.1～3.5 までの各箇条で述べている。

(1) リスクマネジメントプロセス （ISO 14971 箇条 3.1）

製造業者は，製品ライフサイクルを通じて，ロボット介護機器に関連する**ハザード**を特定し，関連する**リスク**を分析，コントロールし，その**プロセス**の有効性を**監視**する**システム**を確立し，維持する。製品のライフサイクルとは，初期構想⇒企画段階➡設計段階➡試作段階➡製造段階➡出荷後⇒最終的な使用停止・廃棄に至るまでの各段階で，**リスクマネジメント**を行えるよう**プロセス**を確立し，文書化されていることが求められる。**リスクマネジメント**は一度だけでは無く，製品ライフサイクルの適切な局面で繰り返される。当然 **PEMS 開発ライフサイクル，ソフトウェアライフサイクル**も含まれる。電子制御回路の開発フェーズで**リスクマネジメント**は反復され，物理的な**故障**や機能ブロック間のインターフェースに関連する**リスク**は勿論。設計漏れや実装ミスなどの**リスク**も含まれ，受け入れ可能なレベルまで**リスク**は低減される。この説明は導入のポイント③で解説する。

リスクマネジメント活動は**安全**な**ロボット介護機器**を開発するベースとなる活動であり，製造事業者として組織的に管理され，経営トップのコミットメントのもと，設計・開発，資材・購買，生産技術，製造，品質保証，フィールドサポートまで適材適所にリソースが分配され運用されていることが肝要である。

リスクマネジメントプロセスでは，一般的に図 3-6 に示すように，社内の品質マネジメント**システム**の一部としての横断的な**リスクマネジメント**の規定と，対象製品の事情を考慮した開発プロジェクトとしての**リスクマネジメント**計画書から構成されることが多いようである。ISO 21856 では，**医療機器**の品質マネジメント**システム** ISO 13485 への適合を求めてはいないが，適用する場合は，**リスクマネジメントプロセス**は，品質マネジメント**システム**に統合されて行われることが望ましい。**リスクマネジメント**計画は，箇条 3.4 で要求されている。いずれにしても，**リスクマネジメント**は事前の組織的なルールと準備基づいた運用が行われることが肝要である。

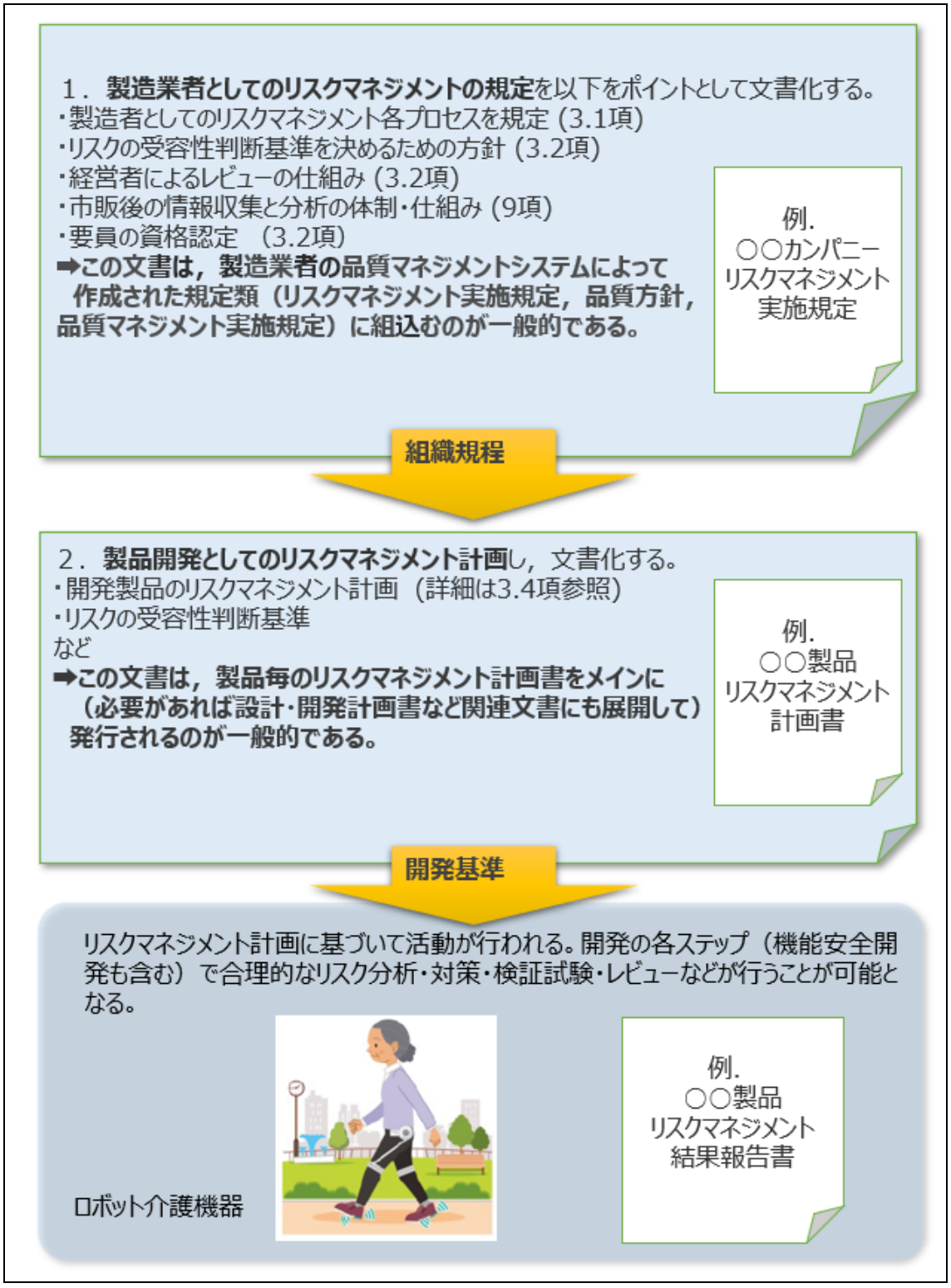


図 3-6 リスクマネジメントプロセスの組織的な規定の実際

(2) 経営者の責任　（ISO 14971 箇条 3.2）

リスクマネジメントプロセスには，**トップマネジメント**による遂行責任が重要であり，各**トップマネジメント**は，**リスクマネジメントプロセス**の全体的指針に対して責任を負うことが望ましい。かつての旧版規格 ISO14971:2007 では，“**製造業者**の責任”において，**リスクマネジメント**体制を構築及び維持することを言及していたが，2007 年版から ”**トップマネジメント**の責任”と言及されることになった。**リスクマネジメント**は開発組織のリソースを適切に投入して行う活動であることが前提と理解することができる。
具体的には以下の項目を組織的に実施できるような体制と仕組みを作り，それが維持できているかを，経営トップがマネジメントレビューなど（QMS のスコープに含めることも多い）で確認する責務を果たす。

- **リスクマネジメント**のための適切な経営資源を確保できるようにする。
  ☞QMS で実施する内容に，**リスクマネジメント**活動を含めることも一つの方法。
- **リスクマネジメントの資格者の確保**
  ☞**リスクマネジメント**には，専門的な分野もあり，手法や各技術の訓練を受けた要員の参加が必要である。
- **受容リスク基準を決定するための方針の文書化**
  ☞**リスクマネジメント**計画段階で行われる「**リスク**の受容性判断基準の決定」は経営者の責任の枠内で扱われる。
  ☞品質方針に含めるのも一つの方法。
  ☞受容**リスク**基準を決定するための方針の文書化
- **リスクマネジメントプロセスと運営結果のプロセス有効性を確認するレビュー**
  ☞**リスクマネジメント**は継続的に PDCA を推進していく**プロセス**であり，それが適切に実施されているかどうかをレビューする。QMS のマネジメントレビューに含めるのも一つの方法。
  ☞決定・実施処置の文書化

(3) 要員の資格認定　（ISO 14971 箇条 3.3）

この規格では，**プロセス**要求が大半を占めているが，**リスクマネジメント**活動，特に**機能安全**のための開発は，十分な専門知識と経験を持つ要員が参画し，多面的な意見集約が有効となる。**リスクマネジメント**活動に参画すべき要員は，**ロボット**の構成**要素**，機能・効能，使われ方，開発技術，製造方法によって変わってくる。典型的な例としては，**ロボット**介護機器の**リスクマネジメント**及び**機能安全**の開発のためには以下のような専門家の参画が望ましいだろう。
開発するロボット介護機器の機能・使用方法・使用環境を理解している要員
（可能であれば，使用者もしくは介護者，PT，ケアマネージャなど近い立場のメンバーも加える。）

- 開発するロボット介護機器に内在する**ハザード**に関して技術的知識がある要員
  （例えば，電気・メカ・**システム**・ケミカル・臨床での情報など）
- 関連する規制・規格について知識を有する要員
- 開発する介護機器が持つ臨床的効果と副作用について知識を有する要員

- **リスクマネジメント**や **PEMS 開発ライフサイクル**・ソフトウェア**開発ライフサイクル**の**プロセス**・実践方法について知識を有する要員
- **機能安全**の技術要求について知識を有する要員

要員は，その経験と能力を資格認定するなど，組織的に明らかにすることが求められる。また，教育訓練**記録**を残す必要がある。

（秘匿性の観点から，この規格では**リスクマネジメントファイル**で管理することを要求していない。社内の教育訓練**システム**にリンクして運用するのが一般的である。）

【参考： 要員の要求や管理については第 4.1 章 **PEMS 開発ライフサイクル**実施ガイドにも解説がある。】

(4) リスクマネジメント計画 （ISO 14971 箇条 3.4）

適切な**リスクマネジメント**には，組織的な取り組みが不可欠である。**製造業者**は，社内の**リスクマネジメント**の規定を定めた**プロセス**に整合するように，開発対象の**ロボット**介護機器のための**リスクマネジメント**計画を作成する。計画書を作成することで，活動の客観性が増し，活動の再現性を向上させ、必要な**要素**の漏れを防ぐのに役立つ。計画の構成及び記載レベルは開発対象機器に関連する**リスク**のレベルに見合ったものであることが望ましい。

その中で製品への**安全**要求（適用規格やガイドライン，市場の**安全**情報など），**リスクマネジメント**に基づいた開発の工程表，使用する**リスク分析**手法・**検証**ツール，**リスク**受容基準を選択した理由説明などが、計画される。

リスクマネジメント計画では設計の上流段階で開発活動について十分に考慮し，製品**安全**の説明責任を果たす点で非常に重要な意味を持つ。

以下に規格で求められている**リスクマネジメント**計画記載事項について解説をする。

リスクマネジメント計画書の記載事項の説明

- 計画された**リスクマネジメント**活動の範囲

・ここでは，対象機器を明確に特定し，内在する**リスク**をマネジメントする活動内容を洗い出し，各活動を製品ライフサイクルのどの段階に適用するかを計画する。

・**リスクマネジメント**の活動内容は，ロボット介護機器の**タスク**，使用環境，使われ方，及び開発技術の新規性や難易度などを考慮する。また，活動の厳しさは，対象製品に求められる**リスク**レベルを反映し，厳しい設計管理，**検証**やアセスメントの計画などを，活動できるよう明示する。

・製品（**医療機器**）のライフサイクルとは，ISO 13485 などの品質マネジメント**システム**で，**製造業者**が確立した製品実現の各段階ことで，初期構想，設計，製造，出荷，輸送，保管，据付，製品使用，廃棄に至るまでの全**プロセス**を考慮する。ISO 14971 規格の特長としては，製造後の段階でも情報収集することも要求することである。

・**リスクマネジメント**活動を製品のライフサイクルのどこからどこまでを対象にするのか活動範囲を明記することで，各段階での具体的な活動，必要な要員などが明確になってくる。

・開発における自組織の役割によっては，その中で自組織の担当する範囲を限定する場合もあり。責任を

明確にすることが重要になる。対象製品の電気電子回路の開発を部分的に外部委託する場合，その範囲の**リスクマネジメント**活動は，外部委託開発業者の**リスクマネジメントプロセス**で扱うか？自社で扱うか？で具体的な活動内容は変わってくる。

・場合によっては，複数の計画書が存在する。文書の対象範囲を明確にし，製品ライフサイクル全体を協調してカバーすることが肝要である。また，他の文書の参照によって示してもよい。

・上位既定の**リスクマネジメント**規定（(1)参照）に合致することを確実にする。また，**リスクマネジメント**計画は，後工程になる **PEMS 開発ライフサイクル**や**ソフトウェアライフサイクル**の活動計画にトレースされるため，相互に齟齬が無いよう維持管理することを考慮する。

➢ **リスクマネジメント**業務の責任と権限

・リスクマネジメントの活動範囲を明確にし，全段階もしくは各段階において，単独もしくは複数の適任な責任者を任命し，適切な活動ができるよう権限や決裁権を与える。例えば，ソフトウェア開発フェーズでの適任者とは，十分なソフトウェアエンジニアリングやソフトウェア品質管理の知識・経験を持ち，開発組織の中で従来から相応の立場で職務を行う人員だろう。

・責任及び権限の割当ては，責任の所在が不明確になるのを防ぐために行われる。

・また，設計担当者，レビュア（専門家），アセッサ，承認権限者など，**リスクマネジメント**活動に必要な人員も事前に特定する。

医療機器ソフトウェアを ISO 14971 の**リスクマネジメント**に適用するためのガイダンスである IEC TR 80002-1「Medical device software – Part 1: Guidance on the application of ISO 14971 to medical device software」では，特に次のソフトウェア開発**タスク**には経験豊富なスタッフを割り当てることが重要とある。

- ソフトウェア欠陥が起こり得る方法の特定
- ソフトウェア**障害**に関連する**リスク分析**
- **リスクコントロール**手段の特定
- **リリース**後発行される PROBLEM REPORTS の分析
- ソフトウェア変更の設計と実装（特に**リリース**後）

このような**安全**に影響する開発**タスク**には，能力を持つ人員の割り当てが必要であることを認識したい。

➢ **リスクマネジメント**活動のレビューに関する要求事項

ここでは，**リスクマネジメント**活動のレビューをどの段階で，どのように行うかあらかじめ計画する。

・開発の各段階で，開発（作成）された**成果物**に対して，目的に応じた様々な**リスクマネジメント**活動が行われる。特に**ロボット介護機器**の**安全**性に関連する **PEMS** 開発では，各開発対象物に応じた**リスク分析**手法（例えば，FTA や **FMEA** など）を用い，欠陥が検出**・評価**され，必要に応じて是正措置（誰が，どの工程で，どのように行うか）が決定される。このような**リスクマネジメント**活動が多く行われるわけだが，この活動が組織的に管理され，**リスクマネジメント**計画通りに適切に行われているかを，中立的な立場の人員がレビューすることを具体的に計画し，文書化する。

➢ 受け入れ可能な**リスク**の判断基準

この規格は受容可能な**リスク**の基準を規定していない。受け入れ可能な**リスク**の判断基準の決定は**製造業者**にゆだねられる。したがって，**リスクマネジメント**活動の事前に，組織的に認められた判断基準が決定される。

受容可能な**リスク**の基準は，**トップマネジメント**の方針に基づき決定される。組織としての共通の基準があれば，それが適用される場合もあるかもしれない。もし，開発者個人の経験で受容可能な**リスク**の基準を決定した場合，その基準は一般的な認識と異なることがある。何故このレベルで OK としたのか，説明を求められる場合もあり，利害関係者による**リスク**認識を広範囲に確認し，組織的に**検証**され，認められたものを準備しておく。

医療機器としてのロボット介護機器の場合，健常者だけではなく，特別な健康状態の使用者に対して，治療を行わないことによる健康を損なう**リスク**と，行ったことによる健康を取り戻す・維持する・緩和するなどの医療的な効能とのバランスを考慮した機器開発をすることもある。一般的に，大きな効能が期待される場合は，その効能に見合うだけのある程度の**リスク**は許されるので，医療関係者の意見を求めることも有効である。この**医療機器**に適用する**リスク**の概念についてはこの規格の附属書 D が参考になる。

また，判断基準は時代によって変化することがある。例えば，昨今の新型コロナ禍では，感染**リスク**への関心が高まっている。肌や体液に触れる構造物を経由しての，高齢者への感染**リスク**など，世論の受け入れ基準は厳しくなっているかもしれない。時代の動向に合うように見直す場合もあるかもしれない。

機器の受容可能な**リスク**の判断基準の一般的な規定方法としては，ISO 14971 では図 3-7 のようなマトリクス表を用いて，どの**危害**の発生確率と**危害**の**重大さ**との組み合わせなら受容できるかをチャートで示す方法を例示している。

半定量的な確率レベル	定性的な重大さレベル				
	無視できる	軽微な	きわどい	重大な	破局的
頻繁					
可能性が高い	R_1	R_2			
時々		R_4		R_5	R_6
僅かに					
起こりそうにない			R_3		

記号（網掛けの部分）
■受容できないリスク
□受容できるリスク

図 D.5－準定量的リスク評価マトリクスの例

図 3-7 準定量的リスク評価マトリクスの例（ISO 14971 附属書 D）

機器の受容可能な**リスク**の決定方法には次の考慮があるが，これに限らない。

➢ 特定の機器又は特定の**リスク**に関して，受容可能性の達成を示した要求事項が実施されていれば，それを規定した適用できる規格を使用する。

➢ 既に市場で認められている（例えば，第三者認証されているなど）類似の機器で明らかになっている**リスク**レベルと比較する。

➢ 一般に容認された最新技術及び既知の利害関係者の関心など，利用可能な情報を考慮する。

- 特に新技術又は**意図する使用**については，臨床試験データを**評価**する。

これらの考慮をする場合，その時点で存在している最新技術，実施例などの最新の状況及び利用可能な客観データを含むことが重要である。最新技術とは，**安全**の分野においては，” state of the art“と呼ばれ，「最大限の努力を用いて実現し得る最良の技術や対策によって安全性を確保すべき」という考え方で，相当な説明責任を果たすことができるということである。” state of the art“を示すには，次の方法があるが，これに限らない。

- 同一又は類似の機器に用いられる規格（国際規格，国家規格，工業規格など）
- 同一又は類似の他の機器での望ましい実施例（市場にある同種製品の一般的な最先端技術など）
- 受け入れられている科学的研究の結果（文献等で公知な技術など）

(ISO 14971 D.4 より)

リスク低減のイメージを下図に示す。

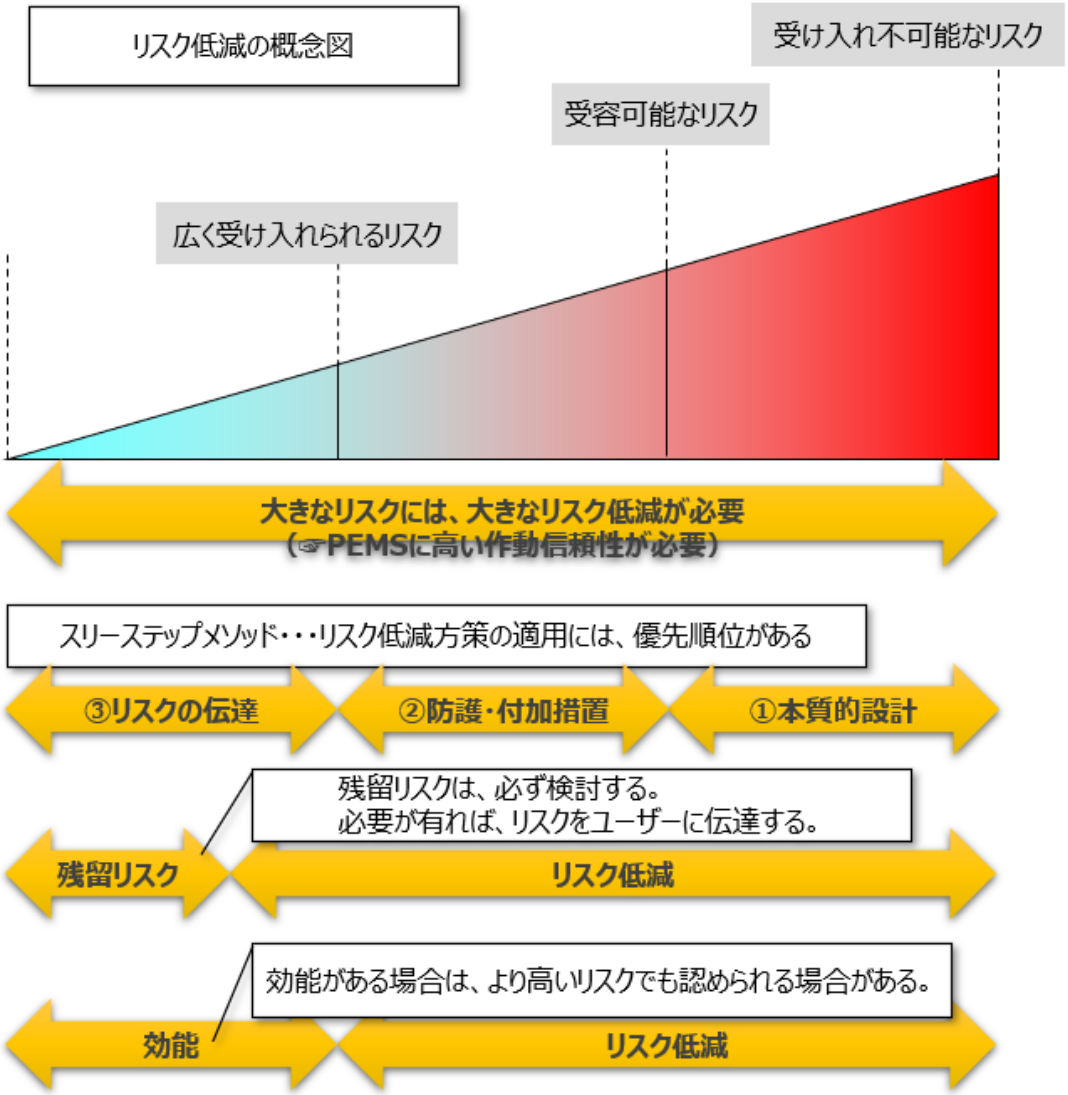


図 3-1 リスク低減のイメージ

ここまでが，機器自体の**リスク推定・評価**の考え方になる。
ここで，ソフトウェア部分に起因する**リスク**に対する受け入れ基準で，「まあ，バグはそれほど起こりそうにない」と科学的な証拠なく発生確率を緩く推定することは，乱暴なやり方である。（詳細は第 5 章の「安全クラス分類」で解説するが，）IEC 62304 では，ソフトウェアに起因する**リスク**の**危害**発生確率を 1（100%）と見なす。**リスク**の定義は，**危害**の発生確率とその**危害**の**重大さ**の組み合わせではあるが，「ソフトウェアの**故障**発生確率（欠陥が顕在化する確率）を定量的に推定する広く認められた方法は無く，一般には発生確率を考慮することができない。」という考えに基づき，**危害**の**重大さ**のみを考慮する。この場合，**リスク**の受け入れ基準は，**危害**の**重大さ**に基づいてソフトウェアの**安全**クラスを決定し，重大な害を与える可能性のある**ハザード**については，ソフトウェアの**信頼性**を高めるため実施された**リスクコントロール**対策（つまり，厳しい開発管理）と，**危害**の発生確率を低減する**リスクコントロール**対策（つまり，追加の**保護方策**。例えばハードウェアによる保護）の有効性を考慮に入れ，**リスク**を推定・**評価**する。このように ISO 14971 では，ソフトウェアについては，ハードウェアなどの物理的な部分とは異なる考え方であることに注意したい。（ISO 14971 D.3.2.3 確率が推定できない**リスク**を参照。）

- **リスクコントロール**の**検証**活動

リスクマネジメント活動の主要な**タスク**の一つである**検証 (Verification)** とは，規定した要求事項を満たしたことを**客観的証拠**の提供によって確認すること。と定義される(箇条 2.28)。具体的には要求文書で示した内容とその**成果物**である試作機との比較による適合性の確認や，設計管理規定に基づく，記述ルールや様式の一貫性など，規定した内容どおりか確認を行うことである。
どのような**検証活動**を実施するのかは，**リスクマネジメント**計画書で規定すべき項目の一つであり，**検証**活動を具体的に明記するか，他の**検証**活動の計画書を利用することができる。典型的な**検証**手段にはレビューがある。レビューの目的・対象・要員・**手順**・形式などについて，あらかじめ計画することにより，未実施や活動内容の抜け・漏れ・ブレなどを防ぐことにつながり，**検証**として有効に実施される。**機能安全**の**検証**活動の例を図 3-8 にて示す。**PESS** の詳細設計を行う**プロセス**で、**単一故障安全**(*)確保の上位設計要求ための電気回路**検証**が行われるだろう。**検証**の具体的な内容として、PESS に関わる回路ブロックの**成果物**（設計書，回路図，部品表，試作機など）を対象とし，いつまでに，電気回路解析チームによる設計文書 **FMEA** 結果と実際の試作基盤での**故障**注入試験を実施するのか。また，その準備として必要な試作基盤や対象動作を再現するためのテスト機能やログ取得など，計画を立案して，実行する。このような**検証**活動を実施し，**安全**に関わる要求事項が**検証**されるよう開発規定でルール化することも**リスクマネジメント**活動の要求の一つである。
(*)**単一故障安全**は IEC 60601-1 を適用する際の要求の一つである。（第 4.2 章参照）

PEMS○○ブロックハードウェア詳細設計の検証
対象物・・・H/W要求仕様書#、H/W設計書#、H/W回路#
内容・・・ 電気回路動作(要求仕様である環境条件、i/f仕様、余裕度を含めて)説明、
FMEA実施結果，故障注入試験結果
対応メンバー・・・電気回路設計チーム、解析チーム
期日・・・開発判定会議(●●)前までに、出力した異常が解決もしくは管理可能なこと
異常時プロセス・・・異常検出運用規定#にて報告・対策・再投入検討すること

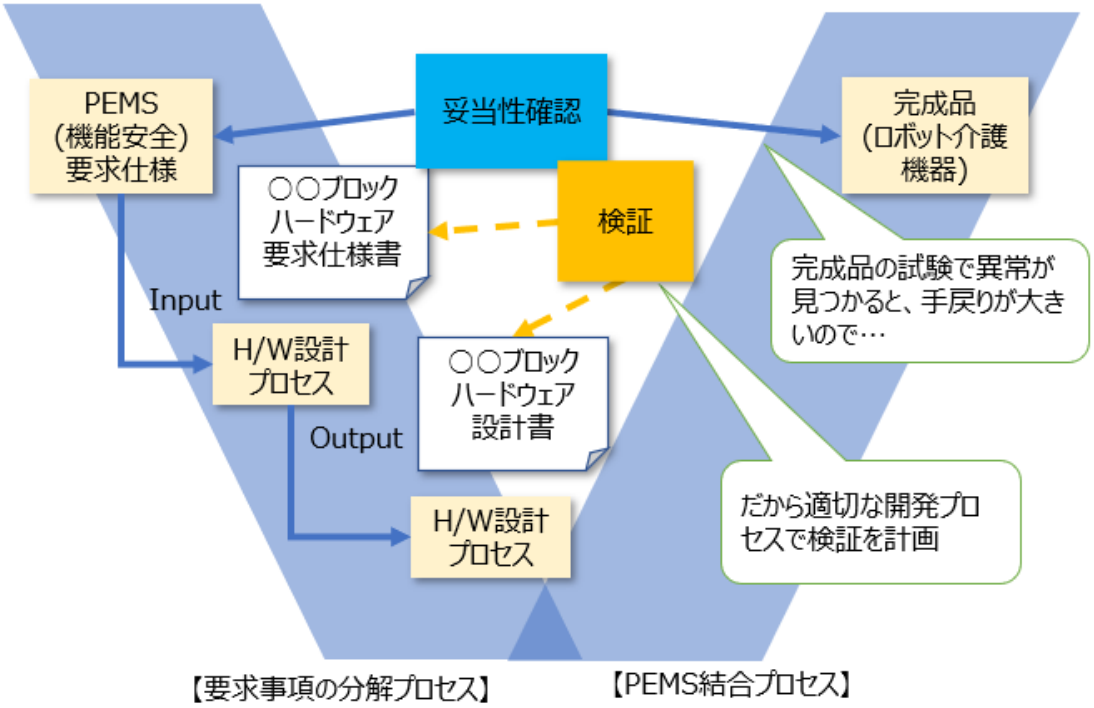


図 3-8 リスクコントロールの検証活動

- 製造及び製造後情報の収集とレビューに関する活動

ここでは，対象とする機器に特有の製造時及び出荷後の情報を得るための方法を確立する。

尚，**リスクマネジメント**計画書は**リスクマネジメントファイル**の一部として文書化し，維持される。

(5) リスクマネジメントファイル（ISO 14971 箇条 3.5）

リスクマネジメントファイルとは，**医療機器**と見なすロボット介護機器の**リスクマネジメント**活動の，各段階のすべての文書と**記録**を指す。

この文書パッケージを確認することによって、明確な安全要求、安全達成の論証、証拠(作業成果物)が分かるように構成される。

例えば以下のようなものがある。

- **リスクマネジメント**段階

リスクマネジメント計画書，受容可能性の判断基準，**リスクアセスメント**結果，**保護方策**を実現するための仕様書・設計書・**検証**計画書及び報告書，**妥当性確認**計画書及び報告書，**残留リスク**の受容性の**評価**結果など

- **機能安全段階**　（電子制御回路による**保護方策**を採用する場合）

機能安全計画書，安全要求仕様書，**PEMS 妥当性確認**計画書及び報告書など

【参考： **PEMS** 開発に関連する文書については第 4 章 **PEMS システム**開発実施ガイドに，ソフトウェア開発段階での文書については第 5 章ソフトウェア開発実施ガイドにも解説がある。】

リスクマネジメント活動では，ロボット介護機器が意図した状況で使用された場合に、受容できない**リスク**が無い事を論証可能な構成とする。個々の**ハザード**識別，及び，その取り扱いがどのように適切に進められているかを文書化する。これらの活動文書は**検証**されるため，各文書間の**トレーサビリティ**は確保され，各々の文書に変更があった場合は派生する箇所は見直され，維持される。このように適切な**リスクマネジメント**活動が行われたエビデンス文書が**リスクマネジメントファイル**になる。**医療機器**の承認審査の場合，**リスクマネジメントファイル**を書面審査し，その内容に応じて適宜インタビューなどが行われるのが一般的である。適切な**リスクマネジメント**活動のスムーズな証明のため，口頭での補足説明無しに，文書単体で活動の適切さを論証できるような明確な作りが受審の秘訣と言われている。

実際の**リスクアセスメント**では，発生頻度と**危害**の程度で表せる**図 3-7** のようなマトリックスを用い，**リスク**領域のうち，無視できる又は合理的に受け入れ可能と考えられる領域まで**リスク**低減を達成する。達成の論証は，**PEMS** で言えば，予想されるあらゆる使用環境での適用に対して，**PEMS** が**安全**であるという説得力のある論証を，事実に基づいた有効なエビデンスによって組み立てることが実際の**リスクマネジメントファイル**の作成活動になる。

医療機器の**リスクマネジメント**は，**リスクアセスメント**及び**リスク**低減**プロセス**活動を**製造業者**の規定化された**プロセス**に則って，よりシステマティックに行うことを定めている。

機器の**リスク**が直ちに患者の健康被害につながる**医療機器**において，効果的な**リスクマネジメント**活動を達成するためには，**トップマネジメント**が**安全**を考慮した方針を立て，必要な組織のリソースが適切に投入され，組織体制の整備により要員の責任と権限が明確にされ，具体的活動は組織的に計画・管理される。など，いくつかの共通要求がベースにあると言える。**医療機器**規格に馴染みのない，一般の生活支援ロボットの開発者は，そのことを理解し，効果的なロボット介護機器の開発を行いたい。

3.4.2 ポイント② 機械安全要素のリスク特定

リスクマネジメントプロセスは，大まかに「製品の特性を明確化 → **ハザード**の特定 → **リスク**の見積り → **リスク**の**評価** → **リスクコントロール** → 再**リスク評価** → **文書化**」の流れで進められる。
この規格では**医療機器**の一般的な**ハザード**が体系的にコンパクトにリストされた表 E.1 が**ハザード**の特定ツールとして提供されている。

表 E.1－ハザードの例

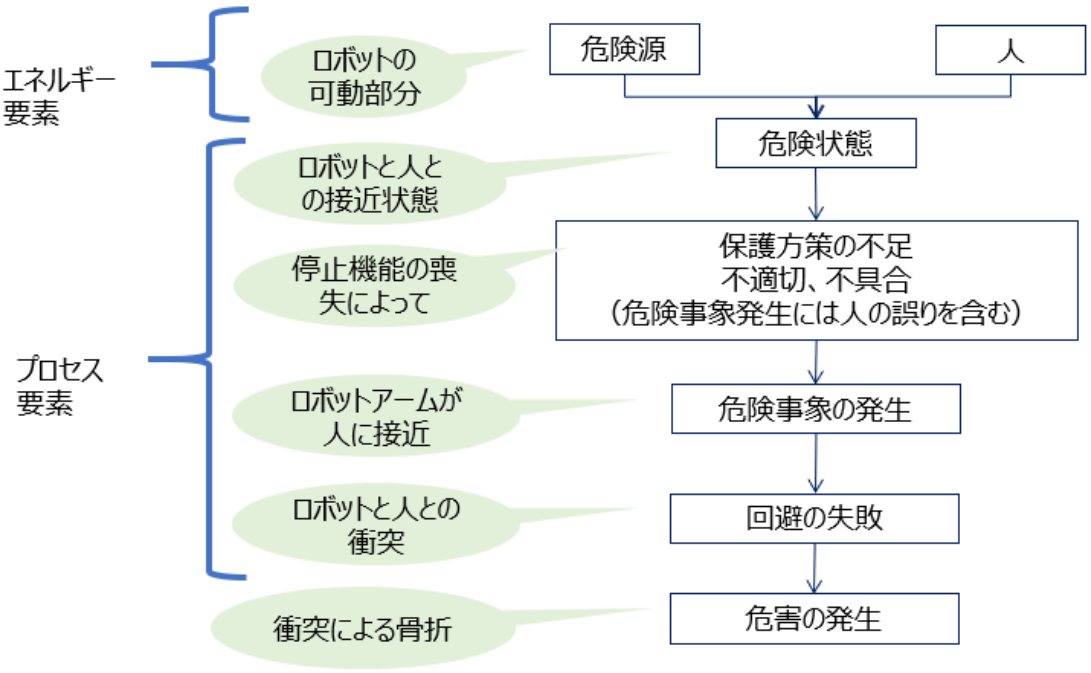
エネルギーに関連するハザードの例	生物学的及び化学的なハザードの例	操作に関連するハザードの例	情報に関連するハザードの例
電磁エネルギー 商用電圧 漏れ電流 － 外装漏れ電流 － 接地漏れ電流 － 患者漏れ電流 電界 磁界 放射線エネルギー 電離放射線 非電離放射線 熱エネルギー 高温 低温 機械的エネルギー 重力 － 落下 － 懸垂物体 振動 蓄積エネルギー 可動部分 ねじれ，ずれ，及び張力 患者の移動及び位置決め 音響エネルギー － 超音波エネルギー － 不可聴音響エネルギー － 音 高圧液体流入	生物学的なハザード 細菌 ウイルス その他の病因（プリオンなど） 再感染又は交差感染 化学的なハザード － 気道，組織，環境又は設備が異物などにさらされる － 酸又はアルカリ － 残留物 － 汚染 － 添加物又は加工助剤 － 洗浄剤，消毒剤又は試験薬剤 － 劣化物 － 医療ガス － 麻酔物質 生体適合性 化学成分の毒性 例えば － アレルギー誘発性／刺激性 発熱性	機能的なハザード 不正確又は不適切な出力若しくは機能性 不正確な測定 間違ったデータ転送 機能の喪失又は劣化 誤使用に関連するハザード 不注意 物忘れ 規則に基づく失敗 知識に基づく失敗 日常的な違反	ラベリング 使用上の注意の不備 性能特性の説明の不備 意図する使用に関する不適切な仕様 限界値に関する不適切な開示 操作指示 医療機器附属品の仕様の不備 使用前点検に関する不適切な仕様 複雑すぎる操作指示 警告 副作用に対する警告 単回使用医療機器を再使用した場合のハザードに関する警告 サービス及び保守の仕様

機械的**ハザード**（エネルギー**要素**）

図 3-9 ISO 14971 Annex E ハザードリスト

このリストは，**医療機器**全般で使用することを考慮した補助ツールで，生体適合性や生物的な**ハザード**など，医療現場特有の**ハザード**も含み，広く扱っている。一方で，可動部や大きな動力源を持つ**ロボット**介護機器では，機械的な**ハザード**はより重点的に考慮したいところであり，図 3-9 に示した機械的**ハザード**は些か情報量が少ない。**ロボット**の**タスク**作業中には操作ミス，**誤使用**などがあり，機械的な**危害**につながるケースがある。**リスク**の分析におけるポイントは，事象の発生過程を追跡して**要素**を押さえていくことである。図 3-10 では，**ハザード**（エネルギー**要素**）に人が晒される時点を**危険状態**と

し，この状態において**保護方策**の**故障**や**誤使用**などの**ハザード（プロセス要素）**によって**危険事象**が発生し，**危害**が生じるとされる。このように**危険事象**に導くまでの事象の連鎖を考慮して，**ハザード**リストを活用していく。



（ISO14121:1999 機械類の安全性-リスクアセスメントの原則を編集）

図 3-10 危険事象に導く事象の連鎖『 人とロボットの衝突 』

この規格で**リスクマネジメント**を進めていく時に，メカニカル**ハザード**に対しての具体的な情報が乏しく，**ロボット**機能を持つ製品特有の**ハザード**も情報として提供されていない難しさがある。そこで**ハザード**リストを拡充することをお勧めする。

図 3-11 ロボット特有の危険源サポート情報（機械安全規格から）

ISO 12100 の附属書 B に掲載の**ハザード**リスト 表 B.1 では機械類の**リスクアセスメント**を助けるより

多くの**ハザード**が列記され，特に機械的**ハザード**の原因系はこの規格の表 E.1 のエネルギに関する**ハザード**の例を補完できる。

表 3-2　ISO 14971 の機械的ハザードを補強する情報（ISO 12100 より）

種類	結果系	原因系
機械的**ハザード**	ひ(轢)かれる	加速度，減速度
	投げ出される	角張った部分
	押しつぶし	固定部分への可動**要素**の接近
	切傷又は切断	切断部分
	引込み又は捕捉	弾性**要素**
	巻き込み	落下物
	こすれ又はすりむき	重力
	衝撃	床面からの高さ
	噴出による人体への注入	高圧
	せん断	不安定
	滑り	運動エネルギ
	つまずき及び墜落	機械の可動性
	突き刺し又は突き通し	可動**要素**
	窒息	回転**要素**
		粗い，滑りやすい表面
		鋭利な端部
		蓄積エネルギ
		真空

ISO 13482 の附属書 A では生活支援**ロボット**特有の**ハザード**リストが提供されているため，機械**要素**の**リスクアセスメント**を助ける情報として活用できる。このガイダンスの付録 B ではこの規格では扱われていない**ロボット**特有の**ハザード**を青文字で示したので参考になれば幸いである。

以上，ロボット介護機器の**リスクマネジメント**において効果的に**ハザード**の特定を行うためのこの規格と機械安全規格の**ハザード**の特定ツールの活用方法を示した。まとめると**図 3-12** のように実施する事をお勧めする。

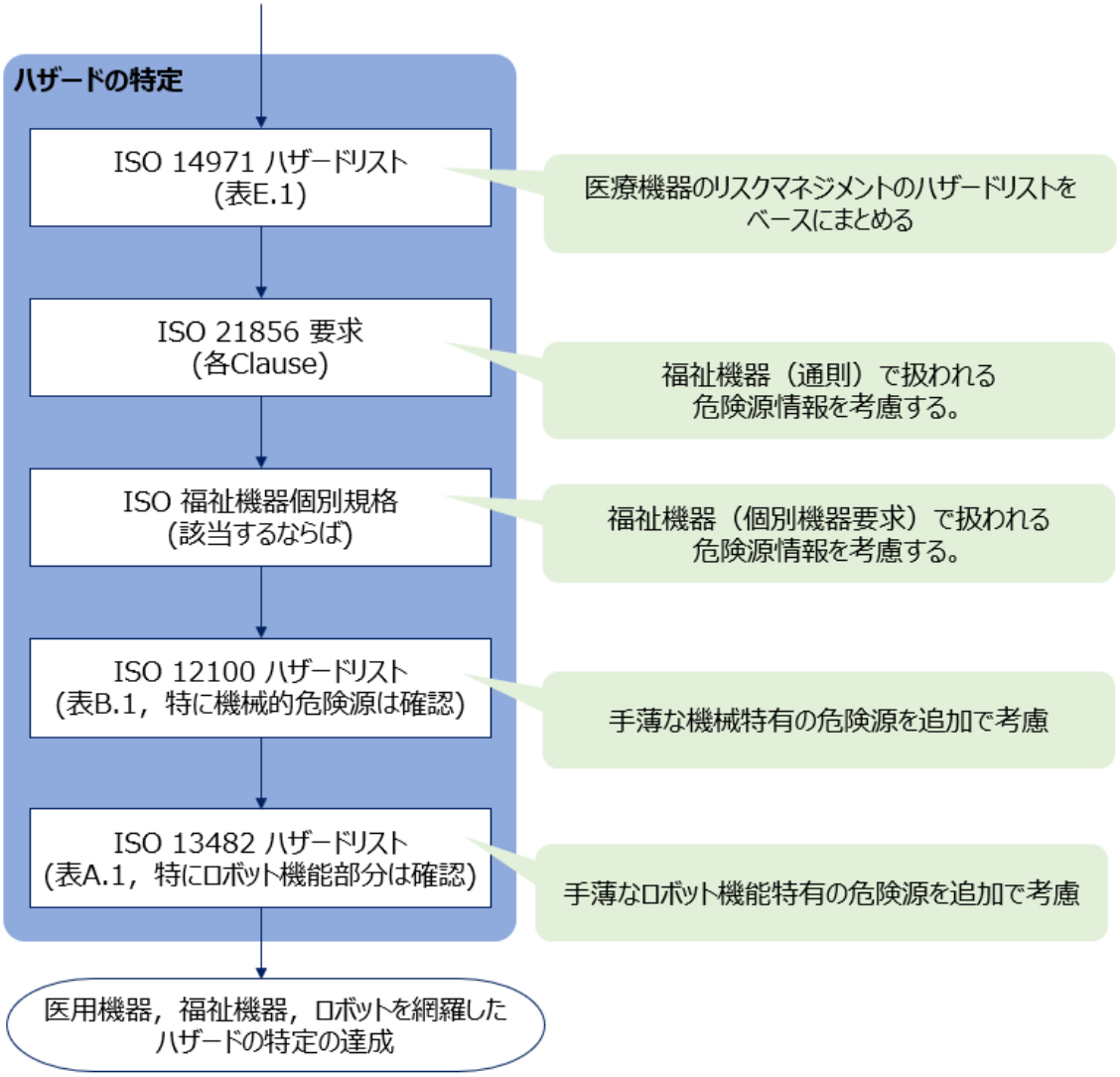


図 3-12 ロボット介護機器の効果的なハザード特定の流れ

ただし，図 3-12 のフローは**システム**及びハードウェア的な**ハザード**をカバーするが，個別の電子**制御システム**設計やソフトウェア設計では別の**ハザード**リストの追加をすることで**システム**設計もしくは詳細設計時に新たな**ハザード**の発見が可能となる。設計段階での**リスク分析**については次ページに述べる。
【ハードウェア設計時の**リスク分析**ツール：**FMEA** や FTA については第 3 章**システム**開発編にも解説がある。】

3.4.3 ポイント③ PEMS 開発中のリスクマネジメント

(1) リスクマネジメントの反復

リスクマネジメントは，”導入実践のポイント② 機械安全要素の**リスク**特定”にて解説したような ロボット介護機器自体の機能や使われ方からの**ハザード**を特定し，**リスク**低減をする**リスクマネジメント**を行うが，この 1 回で終わりではなく，**PEMS 開発ライフサイクル（ソフトウェアライフサイクルを含む）**全体を通して適切な設計の局面で反復され，安全性が維持されてゆくことが重要である。

例えば，図 3-13 において機器の**リスク**低減策を電子**制御システム**で担ったとする。この場合，**安全**でない**システム**要求仕様を作成してしまったり，ソフトウェアの設計と実装を誤ったりすると，不安全な動作を発生する可能性がある。

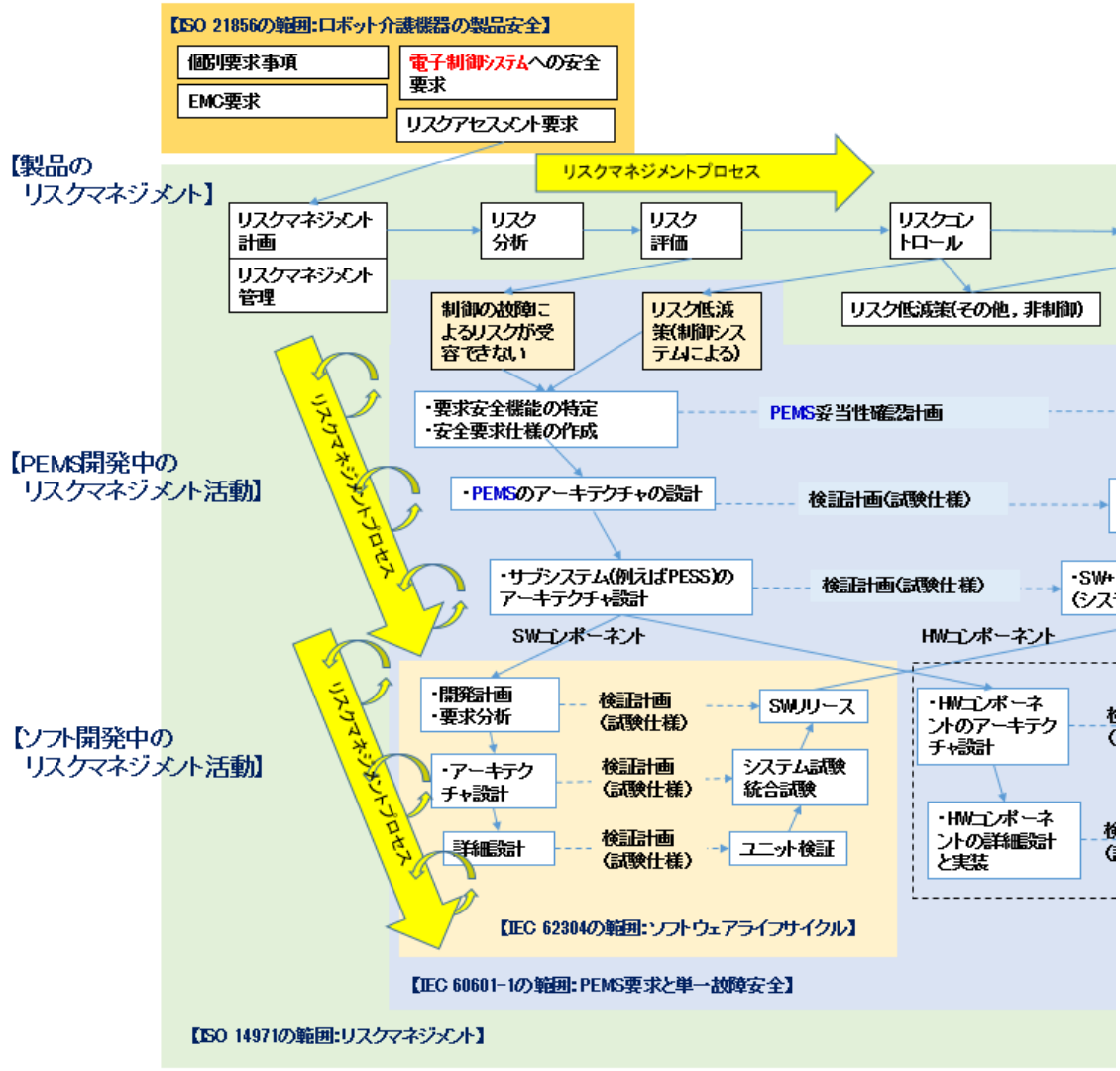


図 3-13 リスクマネジメントの反復

この規格では，**PEMS システム**やソフトウェアの開発段階での**リスクコントロール**の具体的な方法につい

てまでは述べられていないが，**PEMS** の**システム**開発には、IEC 60601-1 の箇条 14 で要求される **PEMS** の**リスクマネジメントプロセス**（IEC 60601-1 箇条 14.6）の実施が求められる。また，**PEMS** のソフトウェア開発には、IEC 62304 のソフトウェア**リスクマネジメントプロセス**（IEC 62304 箇条 7）の実施が求められる。

PEMS の開発は，**安全**要求仕様作成➡**アーキテクチャ**設計➡詳細設計➡実装などの**手順**で進んでいくが，適切な段階で**リスクマネジメントプロセス**を繰り返し実施すべきである。これは、設計の各段階で、新たな**リスク**が生じていないかを確認し、検出次第に**リスクアセスメント**する**リスクマネジメント**活動となる。例えば，要求仕様作成の段階で，機器の機能や性能などの特質が整理されるが，この時点で安全性に影響する開発**要素**は記録しておく，続く**アーキテクチャ**設計で詳細な機能や**安全**性の実現方法やそのための構造までが決定されるので，機能ブロック間のインタフェースや構造上の脆弱箇所など，**安全**性に影響する部分をより詳細に分析できる（例えば，FTA や **FMEA** などの分析手法を用いてもよい）。一例として，電子制御回路を構成する部品の**故障**や電磁ノイズなどの悪環境に関わる設計レベルの**ハザード**などが明らかになるかもしれない。そのように，**PEMS** 開発の各段階では異なる粒度での**リスク分析**が可能となる。そのように反復された**リスクマネジメント**活動を経ることで，量産品では計画した通りの**リスク**レベルに到達する算段が立ち，最後に**妥当性確認**を行い，滞りなく市場に投入していくことが用意にとなる。逆に，この開発途中の**リスクマネジメント**活動を怠ると，製品の出荷間際の**妥当性確認**で予想もしなかった欠陥が検出されたり，市場で予想外の**安全**問題が発生したりするなど，開発の手戻りやリコールが発生する恐れがある。

PEMS の**システム**開発中の具体的な活動要求は IEC 60601-1，IEC 62304 の規格に譲っているが，これら**システム**開発，ソフトウェア開発で共通して要求されるのは**リスクマネジメント**活動を適切に組み込みながら開発を行うことであることを認識すべきである。

(2) リスクマネジメントと PEMS 開発要求の関係

前述のように、**PEMS** の開発中の**リスク**を受容可能なレベルに維持するために、**PEMS** の開発を管理する。この章では、**PEMS** の開発管理が求められる条件を解説する。

端的に言うと，**PEMS** 内の **PESS** が**安全**に関わる時のみに，IEC 60601-1 の **PEMS** への厳しい開発管理（14.2-12）が適用される。

“PESS が**安全**に関わる時”とは次の 2 つのケースであると箇条 14.1 で規定される。

IEC 60601-1 箇条 14.1
①．PESS が，**基礎安全**又は**基本性能**に必要な機能を提供する場合。
②．**リスクマネジメント**の適用によって，PESS の**故障**が受容できない**リスク**を生じる可能性がある場合

① **PESS** が，**基礎安全**又は**基本性能**に必要な機能を提供する場合。とは，電子制御**サブシステム**が，例えば（**基礎安全**の例）非接触**障害**物検知や保護停止などの制御機能を提供することによって，メカニカルな衝突の**リスク**を軽減する場合。又は，（**基本性能**の例）リハビリ効果を

提供する**ロボット**機器において，適切なアシストトルク範囲を保証し，意図した臨床性能を保証することに関与する場合。など**安全機能**を提供する場合と考える。

② **リスクマネジメント**の適用によって，**PESS** の**故障**が受容できない**リスク**を生じる可能性がある場合。とは，**リスク分析プロセス**において，メイン**制御システム**（これも PESS である。ただし，**安全機能**を提供するわけではない）の**故障**を考慮した時に，受容できない**危険事象**が予見できる場合と考える。ここまでの流れは以下の図 3-14 の通りである。

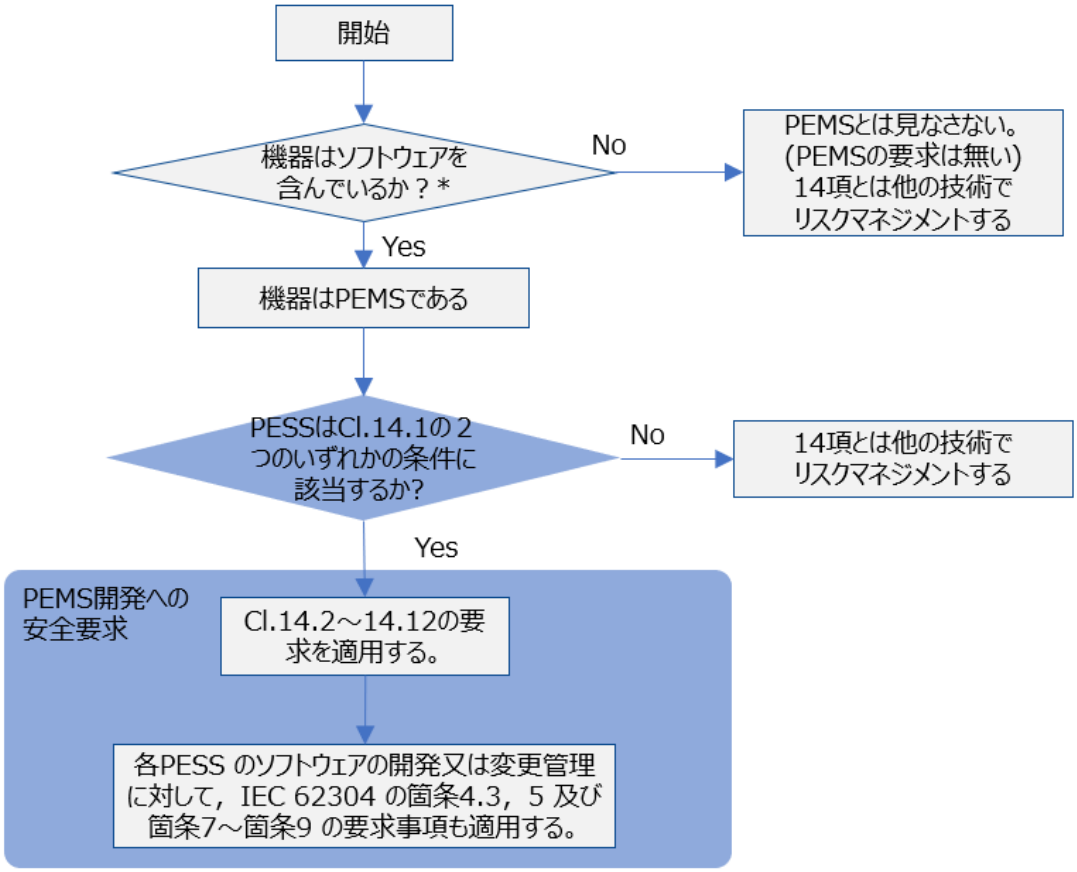


図 3-14 製品のリスクマネジメントから PEMS 開発への特別な安全要求への条件分岐

ここで，**基礎安全**と**基本性能**という非医療の機械系**ロボット**の開発者には，馴染みのない用語が出てくる。ISO 21856 では，現在のところ(2021 年 1 月)，この用語は扱われないため，深い理解までは要らないかもしれないが，**PEMS** 要求を満たすために IEC 60601-1 を読むと，頻出するので，ここで説明をしておく。

これらは，IEC 60601-1 で次のように定義される。

基礎安全（BASIC SAFETY） **ME 機器**（ロボット介護機器）を**正常状態**及び**単一故障状態**で使用する時，物理的**ハザード**に直接起因する受容できない**リスク**がないこと。<IEC 60601-1， 箇条 3.10>

基礎安全は，一般的な電気**医療機器**としての**ハザード**を扱うものと考える。非医療の**ロボット**や家電などのコンシューマ製品の開発者には比較的馴染みがある電気や機械エネルギなどの一般的に存在する**ハザード**による**リスク**からの**安全**を指す。**医療機器**では平常時は勿論，一つの**故障**発生状態でもユーザが不**安全**にならないように要求される。

基本性能（ESSENTIAL PERFORMANCE） **基礎安全**に関連する以外の”臨床機能の性能”において，**製造業者**の指定した限界を超えた低下又は欠如が生じた時に受容できない**リスク**を生じる性能。< IEC 60601-1， 3.27>

基本性能は，ロボット介護機器が医療的な効能を持つ場合，その機能の性能が一定よりも下回ることによって**危害**にまでつながる**ハザード**を扱うものと考える。例えば，内視鏡や AED などはエネルギー（X 線，侵襲性，電力印加など）を患者に与えることが本来の目的である医療行為自体であるため，本来機能を含めた**安全**への要求もあり，**医療機器**の規格では機器毎の個別則（IEC 60601-2 シリーズ）では代表的な**基本性能**への要求が示されることがある。

基本性能が侵害される例としては，

（例）–生命維持機能の精度又は輸液ポンプによる薬剤の投与の精度において，投与が低精度/不正確であると，受容できない**リスク**を患者に引き起こす。

・心電計/モニタが除細動器の放電の影響から回復する能力において，回復できないと医療スタッフが正しく対応できず，受容できない**リスク**を患者に与える。などがある。

医療機器特有の定義なので，国内の**ロボット**介護機器の場合，これに該当するものは稀かもしれないが，臨床機能（治療のための診断，健康維持・予防やハンディキャップの補完など）を有する機器については，その性能が欠如や低下したことによって受容できない**リスク**が生じるかどうか考慮する必要がある。一定の性能を維持することが**安全**状態の場合，機器を電源遮断することはできず，二重化や冗長化構造による性能維持が求められるかもしれない。

まとめとして図 3-15 に，**PEMS** 開発への特別な**安全**要求が求められる 2 つのケースを示した。

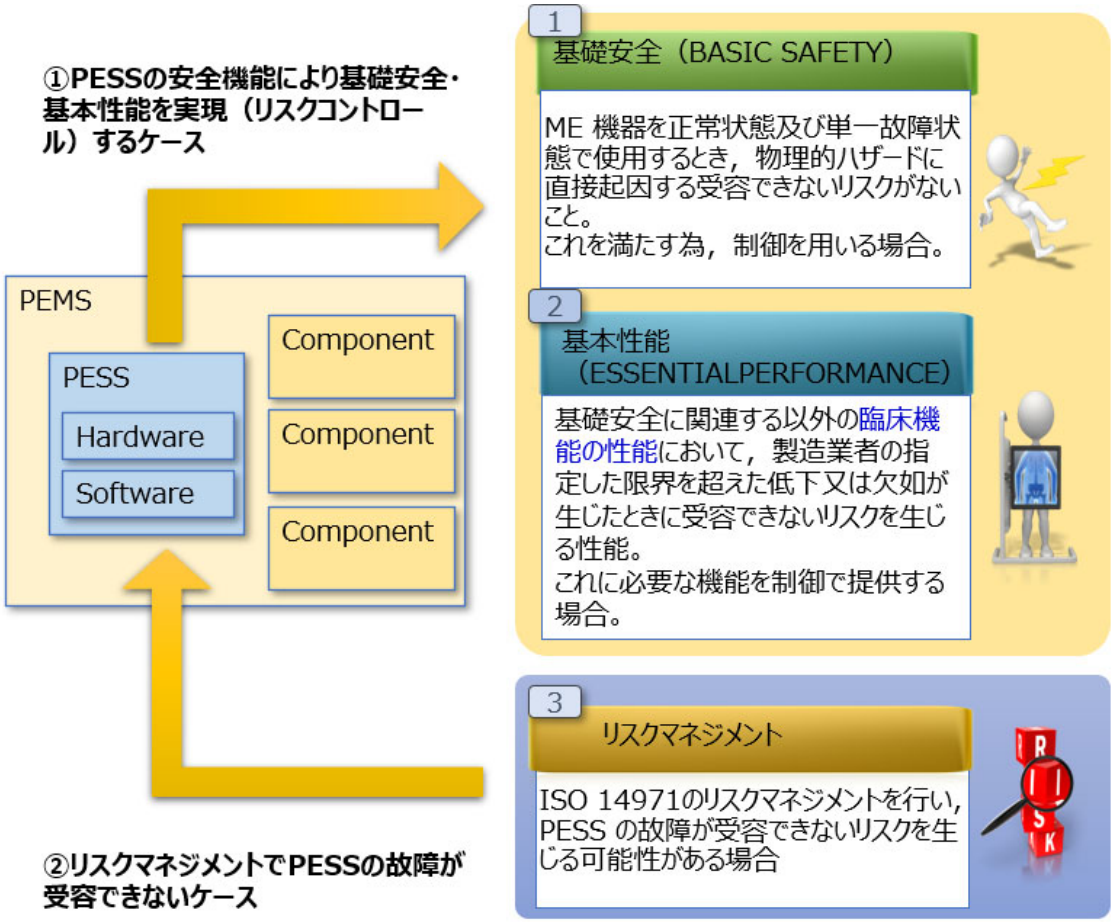


図 3-15　PEMS 開発への特別な安全要求が求められるケース

3.4.4 ポイント④ 製造及び製造後のリスク低減の有効性を監視

この規格が求める**リスクマネジメント**は，設計から製造に引き継がれた後，製造時及び製品を市場に投入した後も継続した**リスクマネジメント**活動要求するのが特徴である。
機械**安全**の ISO 12100 では，この活動は明記されていないが，**リスク**低減**プロセス**において，使用者からの入力（フェードバック）を**リスクアセスメント**の**意図する使用**に活かしたり，**保護方策**の妥当性を判断することに活かしたりする活動と同義である。

ここでは製造及び市場での，該当機器及び類似機器についての事故情報・クレーム・ご意見・ヒヤリハット情報などを収集し，レビューする系統的な**プロセス**を求めている。を製造及び製造後の情報を**リスクマネジメントプロセス**にフィードバックすることで，開発中（特に企画・試作段階）に行っていた**リスクマネジメント**の妥当性を確認し，より正確な**プロセス**に改善することができる。・開発・市場投入時点では認識していなかった**ハザード**又は**危険状態**は無いか，**監視**する。
・想定を超える**リスク**の大きさでではないか**監視**をする。
・社会が受容するレベルが変化するなど，推定した**リスク**が”もはや受容できない”か，**監視**する。
などが目的の例である。
収集のために，品質マネジメント**システム**の規定に含める場合もあるが，例えば，**PEMS** に関連する情報など，製品固有の要求事項に関しては，**リスクマネジメント**計画書に追加して，担当部門が取集・分析活動を実施することも**リスクマネジメント**活動の一環である。
製造業者は，使用者，サービス要員，訓練要員，事故報告担当者，及び顧客からのフィードバックなどの種々の情報源から情報を収集する。収集は，製品の**リスク**レベルに応じて受身的な収集で十分か，積極的な調査が必要かを判断し，**リスク分析**に基づき，どのような内容の調査が必要かを**リスクマネジメント**計画で文書化する。臨床的な**評価**を必要とする場合には，適切な手段を参照し，より詳細に規定する必要があるだろう。

(1) 製造時のリスク情報の取集

製造時まで**リスクマネジメント**を広げたことにより，PESS のソフトウェアを海外工場の工程で ROM ライティングする際に，類似製品のソフトウェアを誤って選択してしまい，**安全機能**が正常に作動せず，結果 **PEMS** の重大な事故が発生する**リスク**も例えば工程 **FMEA** などで特定できる。開発者は，メインのソフトウェアをビルドする際には，**リスクマネジメント**規定に基づく**手順**でこのソフトウェアを扱っており，系統的なミスを防止していたが，製造工程で行うマイナーチェンジ時の作業ミスへの配慮が行き届いていなかった。**リスクコントロール**策として，現地語での**手順**書の整備，安全重要作業工程の作業者を認定する資格制度やパスワードの付与，サムチェックを用いた**エラー**検査などが検討された。
製品の多様化，物流の複雑化に伴い，設計者の守備範囲だけでは，安全制御回路の安全性の確保が難しい状況になってきている。製造事業者が調達する材料，部品やユニットのブラックボックス化やサイレントチェンジの問題，製品の最終生産工程が海外の EMS 事業者委託で**監視**が難しいなど，新た

な**ハザード**も昨今では発生しており，使用に供するまでの**リスクマネジメント**が重要になってきている。

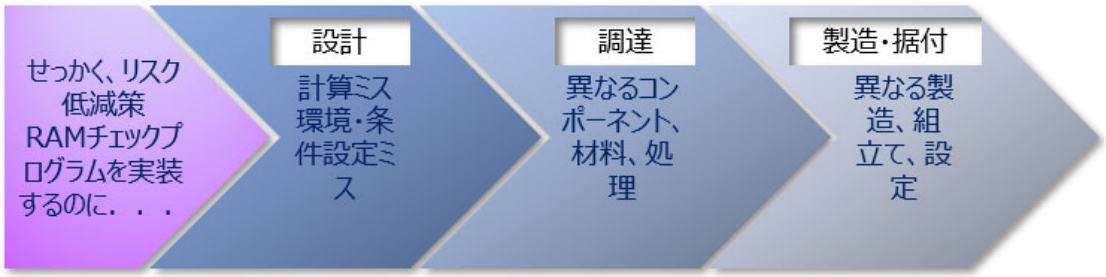


図 3-16 リスク低減策の劣化要因の例

(2) 製造後のリスク情報の収集

製品を市場投入した後も，3 か月後，6 か月後などの市場からのヒアリング・事故情報収集・戻入解析を行うなどして，対象製品を引き続き**リスクマネジメント**することも求めている。加えて，類似製品を含めた市場の事故情報，適用規格の改正情報などを収集し，これをレビューすることで，**リスクコントロール**手段が有効に働いているか，当時は分からなかった新たな**リスク**が発生していないか，などを**監視**する。製品が市場に投入される前の開発時点では**リスク評価**を定量的に行うことは実際には難しく，**危険事象**の発生確率などは定性的に推測せざるを得ない場合が多く，見積り精度に不安が残る場合もある。そこで実際に市場に製品を投入し，実際の稼働状況や不具合データから定量的な**評価**をするなど，**検証**を行うことも有益である。

市場**監視**により，新たな**リスク**や受容できない**リスク**の発生を見つけた場合には，再**リスクマネジメントプロセス**のインプット情報としてフィードバックし，**リスクマネジメント**結果の見直しにより，最悪のケースではリコールを検討するなどの，問題発生**プロセス**の仕組みを確立しておくこととが，被害の最小化につながる。

例えば，製品に **SOUP**（**開発過程が不明なソフトウェア**，第 5 章参照）を組み込む場合，継続的に**監視**を行い、入手可能な**異常**リストと，フィールドのパフォーマンスに関する情報を**評価**することが必要になる。可能な場合，SOUP の採用時にサプライヤーとの契約によってサポートされれば運用がしやすくなる。例えば，パッチやアップデートなど，製品のユーザが意図的に SOUP を変更することが可能な場合，**バージョン**提供の管理・**監視**も注意が必要となる。**製造業者**は，万一の苦情の際，ユーザが機器の**バージョン**を特定して報告することを可能にする必要がある。

市場に投入した後に，**PEMS** の改修が必要な場合，製品化した後の設計変更はとても重く扱う必要がある。もともとの設計は **PEMS 開発ライフサイクル**を通じて**リスク分析**され，丹念に**検証**や**妥当性確認**がされたものであるため，安易に設計変更をしたことによって，不具合が生じることを避けなければならない。その変更が**安全**にどう影響するのかを**評価**をしてから，関連する文書で設計への影響を隈なく見渡し，やり直し対象の活動に漏れがないように再投入の**プロセス**を決定する。これを**機能安全**では影響度分析（Impact Analysis）と呼んでいる。その問題発生管理**手順**もあらかじめ**リスクマネジメント**計

画やその上位規定などに含めておかなければならない。
このように，製造事業者は，製造及び製造後の段階において，該当製品又は類似機器についての情報を収集し，レビューする体系的**手順**，及び**リスクマネジメント**する**手順**を確立し，文書化し，維持する必要があり，この規格で要求されている。
尚，出荷国にもよるが，そもそも**医療機器**では，問題が起きた場合には，ユーザと規制当局へのタイムリーな報告義務が課せられるのが一般的であり，そのような規制への対応としても保守**プロセス**をあらかじめ確立する必要がある。

備考：類似製品を含めた市場の事故情報は以下のリンクが参考になる。
http://www.techno-aids.or.jp/hiyari/search.php?mode=search
（福祉機器ヒヤリ・ハット情報／テクノエイド協会 Web site）

4　PEMS のためのシステム開発実施ガイド（IEC 60601-1）

4 章では，**医療機器**と見なされるロボット介護機器の**システム**開発に要求される内容を，IEC 60601-1 及び IEC 60601-1-2 規格をベースに解説する。

ロボット介護機器に適用する国際規格 ISO 21856 では，電気的に操作される支援機器には IEC 60601-1 の要求を満たすよう記述がある。**安全機能**を実現する電子制御回路を構成する部品の**故障**や**障害**により，不**安全**事象が発生するかも知れない。また，特にソフトウェアとの組み合わせで電子制御される機器は，電子制御回路開発時の仕様の考慮漏れ，設計ミスなどが，不**安全**事象につながる**リスク**もある。電子制御回路の開発要求を満たすように言及されている。

この 4 章では，**図 4-1** に示すように，ISO 21856 が引用するロボット介護機器のシステム開発に関連する規格要求を具体的な例などを用いて説明する。まず，『**PEMS 開発ライフサイクル**の実施ガイド（IEC 60601-1 箇条 14）』にて，**PEMS** に求められる電子**制御システム**設計の要求を説明する。続いて，ハードウェアの**故障**が **PEMS** の受容できない**リスク**に至らぬよう，『**単一故障安全**の実施ガイド（箇条 4.7，箇条 13.1 及び 13.2）』にて，どのように対策をするか説明を行う。最後に，**安全**に関連する電子**制御システム**で考慮すべき『イミュニティ(電磁ノイズ耐性)の要求』を解説する。

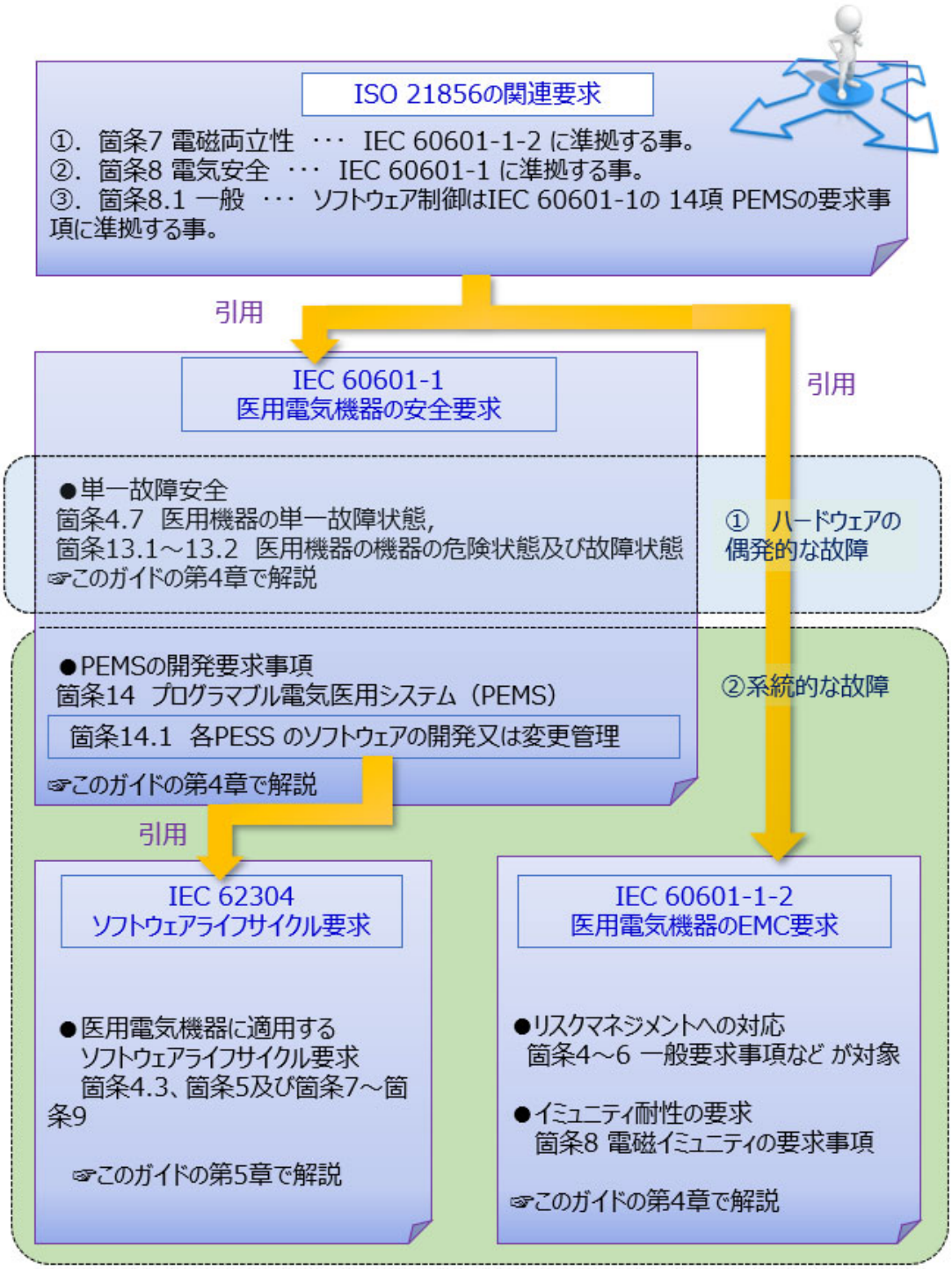


図 4-1　ISO 21856 の安全制御回路開発要求

4.1 PEMS 開発ライフサイクルの実施ガイド （IEC 60601-1 箇条 14）

ロボット介護機器が**医療機器**と見なされる場合，電気に関する**安全**は**医療機器**の規格（IEC 60601-1）（以後「この規格」と呼ぶ）が引用され，ソフトウェア制御も電気に関する技術として同様にこの規格が引用される。**ロボット**の場合，いくつかの機能が自動化され，そのための入力信号を処理する必要があり，多くの場合，プログラム可能な電子部品を用いた**システム**構成となる。これをこの規格では **PEMS(Programmable Electrical Medical Systems プログラマブル電気医用システム)** と呼んでいる。**PEMS** は，「一つ又は複数の**プログラマブル電子サブシステム（PESS，Programmable Electronic Subsystem）**を含む**医用電気機器（ME 機器）**もしくは**医用電気システム（ME システム）**」と定義される。**PEMS** を構成する**プログラマブル電子サブシステム（PESS）**は，「ソフトウェア及びインターフェースを含む一つ又は複数の中央演算処理装置（CPU）に基づいた**システム**」と定義される。

PESS が，ロボット介護機器の**安全**性（この規格では「**基礎安全**又は**基本性能**」という）に必要な機能を提供する場合や，「**PESS** の**故障**が受容できない**リスク**を生じないことを立証できない場合」（回りくどい表現だが，要するに，**PESS** の**故障**が危険をもたらす可能性がある場合），**PEMS** に対して固有の**安全**要求事項が生じる。

基礎安全とは，**正常状態**及び**単一故障状態**で機器を使った時に，受容できない**リスク**を生じないこととされ，例えば，コンデンサの短絡によりロボット介護機器が火災や感電の危険をもたらさないことを言う。ハードウェアの単一**故障**に関しては，第 4.2 章に記載する。

基本性能とは，**基礎安全**に関連する以外の臨床機能の性能において，**製造業者**の指定した限界を超えた低下又は欠如が生じた時に受容できない**リスク**を生じる性能で，要はロボット介護機器特有の医療効果に関する支援機能が劣化して，そのことで通常の健康を損なう，又は，身体への悪影響につながる**ハザード**を扱うものと考える。

サブシステムには，例えば FPGA や CPLD など，中央演算処理装置（CPU）を使用しない**システム**も存在する。これら必要な回路情報を書き込んで，所望の機能を実現できるプログラマブルなデジタルデバイスは同様の設計要求を満たすことがふさわしいと考える。

尚，**PEMS** のソフトウェア部分に関しては，第 5 章に記載する。

4.1.1 故障の考え方

ロボット介護機器の**安全**を考える場合，どんなに低い確率であろうと**故障**は必ず起こるということが前提になっている。この章では**ロボット**介護機器の**安全**性を取り扱っているので，ロボット介護機器（**PEMS**）完成体の**安全**性に関係しない，言い換えれば，**故障**しても危険にならない，あるいは，**リスク**が増加しない場合は対策の必要はない。このような**故障**を非**危険側故障**あるいは**安全側故障**と呼ぶ。

安全に関係する**故障**とは，何らかの形でロボット介護機器が危険な状態になる，あるいは，**リスク**が増加し受容可能レベルを超える場合の**故障**を指す。つまりこの規格で言うところの「**基礎安全**及び**基本性**

能」を損なう場合がある**故障（危険側故障）**の対策を必要とする。

① 故障の種類と対処法

故障の種別は　**危険側故障**と**安全側故障**の区分以外に，**故障**の性質とその対策方法から次のような区分もある。ここでは，それらの説明と設計での対処法の概略を述べる

② 偶発的な故障

偶発的な故障は，時間に関係なくハードウェアの多様な劣化から生じる**故障**で，ハードウェアの**偶発的な故障**とも呼ばれる。**リスク**を低減するために**故障率**が十分に低い部品やデバイスを選定することになるが，多くの場合この「十分に低い」という条件を単体部品で満たすことは難しいため，この規格では基本的には単一**故障**をシミュレーションして，ロボット介護機器の**システム**全体としてとして危険な状態にならないことを回路確認することになっている。これを**単一故障安全**という。

単一故障安全の考えでは，2 つ以上の独立した**故障**は同時に起こらない，もしくは，その確率は極めて低いという考えで，一つの部品についてだけ**故障**が起きた状態で**安全**かどうかを判断する。注意しなければならないのは，**故障**が検出されずに潜在化し，その状態で他の**故障**が起き，危険な状態に至る場合（累積**故障**）もある。このような**故障**の累積は，定期点検（機械安全では**プルーフテスト**と呼ぶ）などにより検出され修理されることになる。**故障**の累積が考**えら**れる場合は，製品寿命（この規格では**予測耐用期間**と呼ぶ）や定期点検内容など必要に応じ，合理的な方法を検討しておく必要がある。また，一つの**故障**が複数の機能に影響する場合（**共通原因故障**）や，一つの**故障**が他の部品の過負荷状態を起こしその寿命に影響する場合（**従属故障**）も単一**故障**に含まれることである。

典型的な**共通原因故障**の例として，電源部分の**故障**がある。例えば，電圧の変化や変動が 2 つ以上の**安全機能**に同時に影響を及ぼす場合がある。**従属故障**としては，例えば空冷ファンの停止が温度上昇を招き，電子回路の一部が**異常**発熱で**故障**して，**安全機能**喪失をもたらす場合などがある。

この規格では，「**高信頼性部品**」という概念を用いて**故障**除外を認めているが，ロボット介護機器の生涯を通じて「この規格の**安全**要求事項について機能を失わないことを確実にする特性を持った部品」であり，製造事業者はそれを証明することになる。

ちなみに，**偶発的な故障**は，先に述べたように，ハードウェアの**故障**であり，ソフトウェアでは生じない。

③ 系統的な故障

特定の条件において**安全機能**を喪失する**故障**で，正しい知識，認識，対策の欠如などを原因とする。この原因は，設計，製造過程，運転**手順**，その他の関連する原因の修正によってだけ取り除くことができる。他の規格では，**システマチック故障**や**決定論的原因故障**と呼

ばれることもある。

設計時には予期しなかった使われ方，状況，入力順序，タイミングなどの特定の条件下で必ず起こる**故障**である。典型的な**系統的な故障**は，ソフトウェアの**故障**で，いわゆる「バグ」である。また，人間工学を考慮しない設計によるヒューマン**エラー**も**系統的な故障**と考えることができる。**系統的な故障**へ対処するためには，設計段階で問題を洗い出し解決する必要があり，以降に記載するように，設計・開発の**成果物**に対して**リスクアセスメント**で制御設計に起因する不**安全**事象を分析し，設計管理（**機能安全**管理と呼ぶ規格もある）により必要な**リスクコントロール**手段を漏れなく**検証**して対応する必要がある。

系統的な故障はソフトウェアだけでは無くハードウェアでも考慮する必要がある。例えば，宇宙線や放射線などの影響によるメモリビット化けなどのソフト**エラー**，ヒューズの溶断特性の選定間違え，特別な医務室などの使用環境が考**えら**れるのであれば，鉛などでシールドするなどして対応すべきであり，このような考慮・対処の漏れは**系統的な故障**と扱われる。このような**故障**は設計**プロセス**に起因するため，本章の活動が必要になる。

4.1.2 設計管理

系統的な故障へ対処するためには，設計段階で課題をすべからく検討し，必要な対応を取るための管理が重要になる。特に，ソフトウェアや複雑なハードウェアから構成される **PEMS** では，その設計に漏れや見落としがなく正確であることを示すことが難しくなる。このため，**PEMS** の設計は，開発工程を定義することで管理可能とし，その開発工程内で**リスクマネジメント**を実施することが肝要である。つまり，ソフトウェアのバグや，ハードウェアの設計考慮漏れを試験だけで検出するのではなく，**PEMS** への要求事項を明確化し，それを実現する開発工程の管理活動を上流で計画し，実行するとともに，開発工程の中で，都度発生する**リスク**を解析，レビューや試験など適切な方法により確認し，対応策を講じる。これらの管理の結果を文書化して推進することである。

この規格の箇条 14 では図 4-2 に表わす **PEMS 開発ライフサイクル**の実施を要求する。この **PEMS** ライフサイクルのメイン**プロセス**となる開発モデルで工程を管理し，メイン**プロセス**を通じて文書化，**リスクマネジメント**を実施していくことで，**PEMS** への要求事項に対し，適切な品質で作られたこと。及び，**PEMS** の**リスク**が受容できるレベルまで減少できた安全性を示すことになる。

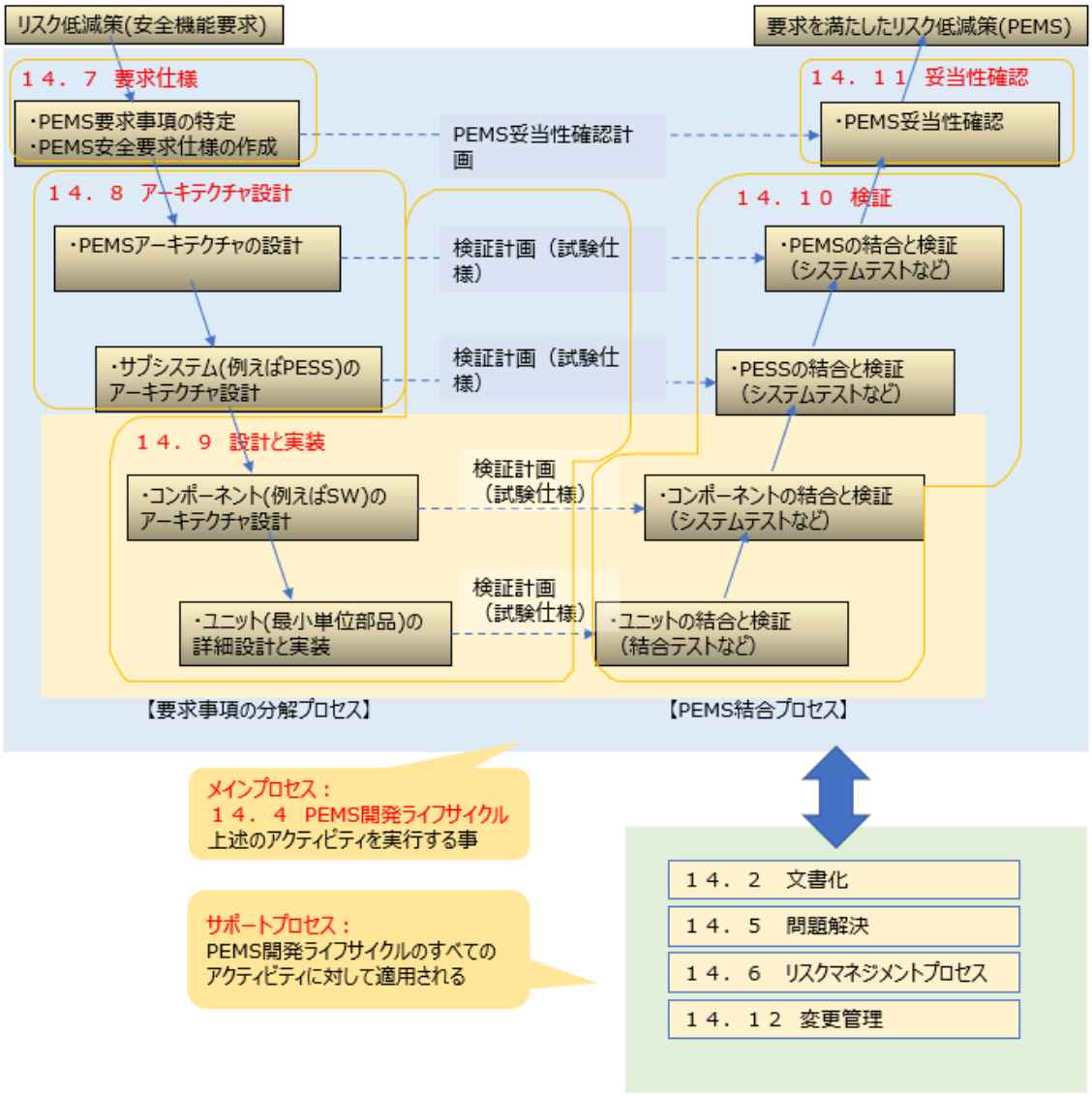


図 4-2 IEC 60601-1 箇条 14 で要求される開発プロセス

① 文書化 （IEC 60601-1 箇条 14.2）

リスクマネジメントの一環として文書化が要求される。**PEMS** 設計の各工程において必要な文書が作成され維持されることになる。これらの文書を適切に管理して運用すれば，第三者に対して必要な開発工程が正しく行われたことを示すことや，将来考**えら**れる設計変更時に必要な**影響解析**を行うことも可能になる。

基本的には，各工程の入力になる仕様書，各工程で作成される回路図など**成果物**，**成果物**の**検証**結果，次の工程へ引き継ぐ報告書などで構成される。必要に応じ，**PESS** あるいはその他の**サブシステム**単位で文書化が必要になるかもしれない。

目的とする **PEMS** あるいは **PESS** を含む**サブシステム**の**安全**性が達成されたことを示すには，文書に

依存することになるため，文書化が確実に実行されたことを示す必要がある。文書類は，製品全体の**リスクマネジメント**でも要求されるように，正式な文書管理**システム**のもとで，文書の作成，改定，維持がされ，**リスクマネジメントファイル**（ガイダンスの第 3.4.1.5 章を参照）の一部を形成することになる。文書類は，将来の設計変更時などにも参照されるため，また，後述する **PEMS 開発ライフサイクル**の確実な実行を示すため，各文書間で**トレーサビリティ**を確保する必要がある。**トレーサビリティ**を確保するには，専用の支援ツールがあるので，それを用いて行うこともできるが，簡単な**システム**であれば，文書番号に**システム**の識別，開発フェーズの識別，文書の親・子・孫等の関連を示す識別などを組み込むことによっても可能であろう。

以下に，開発フェーズでの製品に関係する作成文書（**リスクマネジメントファイル**）の例を示す。

表 4-1 製品関連作成書類の例

コンセプトフェーズ	**リスクアセスメント**レポート	コンセプトフェーズから**リスクアセスメント**を行う。開発が進み製品が具体化する毎に，繰り返し行う。旧版は廃棄せずに，保存すること。
	安全要求仕様書	製品の特定した**ハザード**に関する**リスク**を管理するための**リスクコントロール**手段について，何をどのように実行するかを明確にするために**安全**要求（機能や性能など）を記載する。詳細設計の進行に従って，改定されていく。 尚，この規格では箇条 14 **プログラマブル電気医用システム**（**PEMS**）にて”要求仕様”と呼称されている。
	妥当性確認仕様書	**妥当性確認**項目，判定基準，方法，計画などを記載する。（**妥当性確認**は**安全**要求仕様で規定した通り，**PEMS** 完成品が要求事項を満たしているかを確認する。**PEMS 開発ライフサイクル**の最後に行うが，開発上流から検討・調整することで，実行性のある計画が可能となる。）
PEMS 設計フェーズ	設計仕様書	**安全**要求仕様を満たすために必要な **PEMS** の設計仕様を記載する。**安全機能**の要求頻度などを考慮し，動作の流れやタイミングなども仕様化される。
	機能ブロック図	**安全**要求仕様を満たすように **PESS** を含む**サブシステム**を配置する。各**サブシステム**の機能や性能，入出力のつながり，信号の流れ，各々の**サブシステム**の相互関係を明確にする。

表 4-2 （続き）製品関連作成書類の例

PEMS 設計フェーズ	**検証**仕様書	**PEMS** の**検証**項目，判定基準，方法，計画などを記載する。 試作機での試験をはじめ，設計レビュー，自動解析ツールやシミュレーション結果などにより，内容に適した**検証**手法を定める。
PESSを含む**サブシステム**の設計フェーズ	設計仕様書	**サブシステム**に要求される**信頼性**，入出力（指令やデータの流れ・形式など），タイミング，レベル・信号処理など，**検証**可能な様式で仕様化し記載する。
	機能ブロック図	複雑な**サブシステム**の場合，**PEMS** 同様，機能配置図を作成し，更に詳細を詰める。
	検証仕様書	**サブシステム**の**検証**項目，判定基準，方法，計画などを記載する。
	検証報告書	**サブシステム**の設計仕様書を満たすかどうかを**サブシステム**の**検証**仕様書に従い**検証**した結果の報告書。
PEMS 統合フェーズ	**検証**報告書	**PEMS** 設計仕様書を満たすかどうかを **PEMS 検証**仕様書に従い**検証**した結果の報告書。
製品化フェーズ	**妥当性確認**報告書	**妥当性確認**仕様書に従い製品における**妥当性確認**を行い，報告書を作成する。

その他，回路図，部品表，部品配置図なども必要に応じ含まれる。

② 要員管理

この規格では，要員の管理について，明確な規定はないが，設計，**検証**，**妥当性確認**などの重要な業務において遂行能力のある要員が担当することを前提としており，重要と考える管理内容を説明する。

PEMS 開発ライフサイクルでは，要員の資質，経験などを判断し，能力に応じた業務を担当する。メンバーには，開発ゴールとともに，その役割と責任範囲を明示する。メンバー間では，原則的には，良好なコミュニケーションが保たれ，進捗や課題が共有される。例外として，**多様性**（要求される機能を実行する異なる手段。付録 C の用語解説を参照）を用いた設計の場合，異なるメンバーが設計し，技術的な情報交換を避けることにより，異なった思想による設計を実現することができる可能性が高まることもある。

教育・訓練は，定められた**手順**に従って行い，常に能力の向上に励む。

原則として，あるメンバーが作成した文書は，他のメンバーが照査するようにし，同一人物による思い違いなどに起因する間違いを防ぐ必要がある。複数の **PESS** や**サブシステム**の開発が同時進行する場合が多いので，それらを取りまとめ進捗を管理する人物も必要になる。

その他，開発部門とは異なるが，市場データの収集解析，製造部門での設計仕様に基づいた製造，製品の保守点検（**プルーフテスト**を含む）など行うサービス部門も**系統的な故障**への対応に関係してくる。

③ リスクマネジメント計画 （IEC 60601-1 箇条 14.3）

ISO 21856 が求める一連の製品**安全**のための開発では，**PEMS** に限定せず，ISO 14971 の要求で**リスクマネジメント**計画を作成することになる（第 3.4.1.4 章参照）。**PEMS** 開発の各フェーズにおいても，**PEMS** 及び PESS に内在する**ハザード**を分析・**評価**・コントロールする具体的な活動を計画し，それに従い反復して**リスクマネジメント**を実行する。加えて，この規格では **PEMS 妥当性確認**計画を作成し，**リスクマネジメント**計画から参照することも求めている。**PEMS 妥当性確認**（詳細は後述 4.1.3 章参照）は**安全**要求仕様を **PEMS** 完成品が満たすかを確認することだが，開発上流から準備を検討・調整しないと，実行ができない場合があり（例えば，テストモードをあらかじめ用意しておくことで，完成品において最悪条件が模擬できる場合など），この段階から検討したい。尚，**リスクマネジメント**計画は，**リスクマネジメントファイル**の一つとして文書化する。

④ リスクマネジメントプロセス （IEC 60601-1 箇条 14.6）

(1) ハザードの特定 （IEC 60601-1 箇条 14.6.1）

PEMS 開発ライフサイクルの各工程において，**リスクマネジメント**活動が実施される。第一段階は，その**システム**がもたらす**ハザード**の特定になる。（**ハザード**の定義は，箇条 3.39 にて**危害**の潜在的な源。とされ，つまり危険の因子のことである。）

ハザードの特定は，**PEMS** 以外にも要求される活動であり，そのまま適用することができる。ロボット介護機器で適用できる**ハザード**のリストに関する情報は第 2 章に記載されている。それに加え **PEMS** では，内部及び外部で多くの通信が行われているため，それらの通信**エラー**や間違ったデータによる**ハザード**も予見が必要になる。更に，電磁妨害によるデータの変更や，外部からの意図的な改ざん（**セキュリティ**）に対する考慮も必要になる。

ハザードを特定するには，その**システム**の機能，適用（使われ方，環境，時間など），仕様や構造を明確にし，**ハザード**を特定する活動の関係者が同じ理解を持つようにする必要がある。同じ理解を有しても，**ハザード**特定作業中に，異端の意見が出てくる可能性があるが，それを無視することなく検討すべきである。新たに開発する**システム**が，従来の**システム**と同じか似ていれば，いくつかの**ハザード**は既に分かっている。それに加えて，新たに予見可能な**ハザード**の存在を検討する。したがって新規性のある**システム**開発では，より入念な分析，厳しい管理が行われるであろう。

PEMS に関連した**ハザード**リストには，次のものが含まれるべきである。

- 好ましくない（物理的及びデータの）フィードバック（考**えら**れるものとしては，想定外入力，範囲外又は相反する入力，及び電磁**障害**から生じた入力がある。）
- 利用できないデータ
- 不完全なデータ
- 誤ったデータ
- 誤ったタイミングのデータ
- **PESS** 内及び **PESS** 間での意図しない相互作用
- 第三者が製造した未知な側面又は品質を持ったソフトウェア
- 第三者が製造した未知な側面又は品質を持った PESS
- データの機密性に関わる影響及び特に不正変更に対するデータの脆弱性も含めた**セキュリティ**（**安全**性）が不十分なデータ，他のプログラムとの意図しない相互作用，及びウイルス
- **PEMS** が，その**基礎安全**又は**基本性能**を達成するのに必要な特性を提供するための
  IT ネットワークの**故障**。（規格の IEC 60601-1 H.7.2 に例を示す。）

これらの**ハザード**の特定に有効な手法として FTA，HOZAP study や最近では STAMP/STPA などがある。

(2) リスクコントロール （IEC 60601-1 箇条 14.6.2）

リスクコントロールは，特定した**ハザード**に起因する**リスク**を，受容可能なレベルまで低減及び維持することであり，**PEMS** 以外にも要求される活動である。
リスク低減を **PEMS** への開発要求（IEC 60601-1 の箇条 14.2～14.12 参照）に依存する場合は，その**リスクコントロール**手段が，特定した**リスク**を十分に低減することを保証する必要がある。より高い**リスク**の低減には，より高い**信頼性**が **PEMS** に要求されることになる。
この規格では，例えばハードウェアによる**安全機能**の喪失確率など，**PEMS** に要求される**信頼性**に関して詳細の記載が無いので他の規格を参照する必要があるかもしれない。**ロボット**介護機器の場合，付録 B に記載する，機械**安全**に用いる確率を用いることができるかもしれないが，その前提となる使用環境の違いなどは慎重に考慮して用いる必要がある。もし，適切な基準を見つけることができない場合は，社会一般が受け入れることができるレベルを，天災による事故確率などを参考に，推測して決めることになるだろう。

⑤ 問題解決 （IEC 60601-1 箇条 14.5）

定めた **PEMS 開発ライフサイクル**に従って開発を進め，何も問題が無ければ，予定通りに終了すればよい。しかし，往々にして問題が生じるので，問題解決の**手順**などあらかじめ対応を決めておき，その**手**

順に沿って対処する。

PEMS 開発の**プロセス**中及び**プロセス**間の典型的な問題の例として，次がある。

- 相反する要求事項
- 不明瞭な要求事項
- 仕様の抜け
- コーディング**エラー**
- **PEMS** の誤った操作

この規格は，全ての**問題報告**に対して設計変更を要求するものではなく，軽微な誤解，**故障**又は事象については，処置の対象としなくてもよい。ただし，系統的な**手順**を定めて問題を**評価**し，解決に責任を持つ必要がある。問題解決のための場当たり的な方法は，折角行っている系統的な開発を妨害するので，厳に慎むべきである。

問題解決の**手順**書には，問題の報告に関する**手順**，既知の**ハザード**に対する影響，問題の**リスク評価**，問題解決のための手法，解決手法により生じる影響の分析，解決できたと確認できるための基準，**回帰テスト**（変更による悪影響が無いことを判定するために要求される試験）などの**検証**や**妥当性確認**など，その他問題解決に必要な活動などを定めることになる。

問題解決活動も，その**記録**を残す必要があるため，文書化の**手順**に従い履歴を残す。問題解決の履歴は，**PEMS 開発ライフサイクル**の技術文書の一部として文書化してもよく，自社の品質管理文書の文書管理の**手順**で文書化してもよい。

ここまでの要員管理，文書管理，**リスク**管理および問題解決管理と，後述する変更管理は **PEMS** の開発**プロセス**の全般にわたって**リスク**を管理する いわゆるサポート**プロセス**の位置付けとなる。

続いて，製品の**リスク**を管理しながら，**安全**要求，設計，実装を行っていく **PEMS 開発ライフサイクル**のメイン**プロセス**について解説する。

① **PEMS 開発ライフサイクル** （IEC 60601-1 箇条 14.4）

PEMS 開発ライフサイクルでは，一連の工程（この規格では，マイルストーンという言葉を使用している）を決定し，各工程の活動や活動結果の**検証**方法を決定し，文書化する。また，各工程における活動のためのインプット，活動結果のアウトプット，ならびに，日程も決定し，文書化する必要がある。**PEMS 開発ライフサイクル**は，必要に応じ，開発期間を通じて改定されることもある。

文書化されたライフサイクルは，**安全**性の問題が **PEMS** に限らず製品開発の全般にわたって考慮されていることを示すことになる。この規格が対象とする製品は多岐にわたるため，製造事業者はその製品に適したライフサイクルモデルを用いて推進することができるようになっているが，この規格では，Ｖ字開発モデルを参考として示しているため，それに基づいて説明する。（図 4-3 を参照）

一般的に製品開発のきっかけは，市場やユーザからの要求である。この要求をもとに，製品が企画されイメージされ，具現化されることになる。ある程度具現化されると，**リスクアセスメント**の実施が可能になり，**リスク**低減活動の結果として，その製品における必要な**安全機能**が明らかになり，**PEMS** の要求

事項を仕様化できる。これがＶ字開発モデルの左上部の出発点になる。左上部から中央下部への流れは，**PEMS** の仕様から，その実現に必要な細部の仕様へと向かっている。図 4-3 の【要求事項の分解**プロセス**】。中央下部から右上へ向かう流れは，**PEMS** の実現工程で，細部の仕様に従って実現された部分を **PEMS** へと統合する流れになっている。図 4-3 の【**PEMS** 統合**プロセス**】。

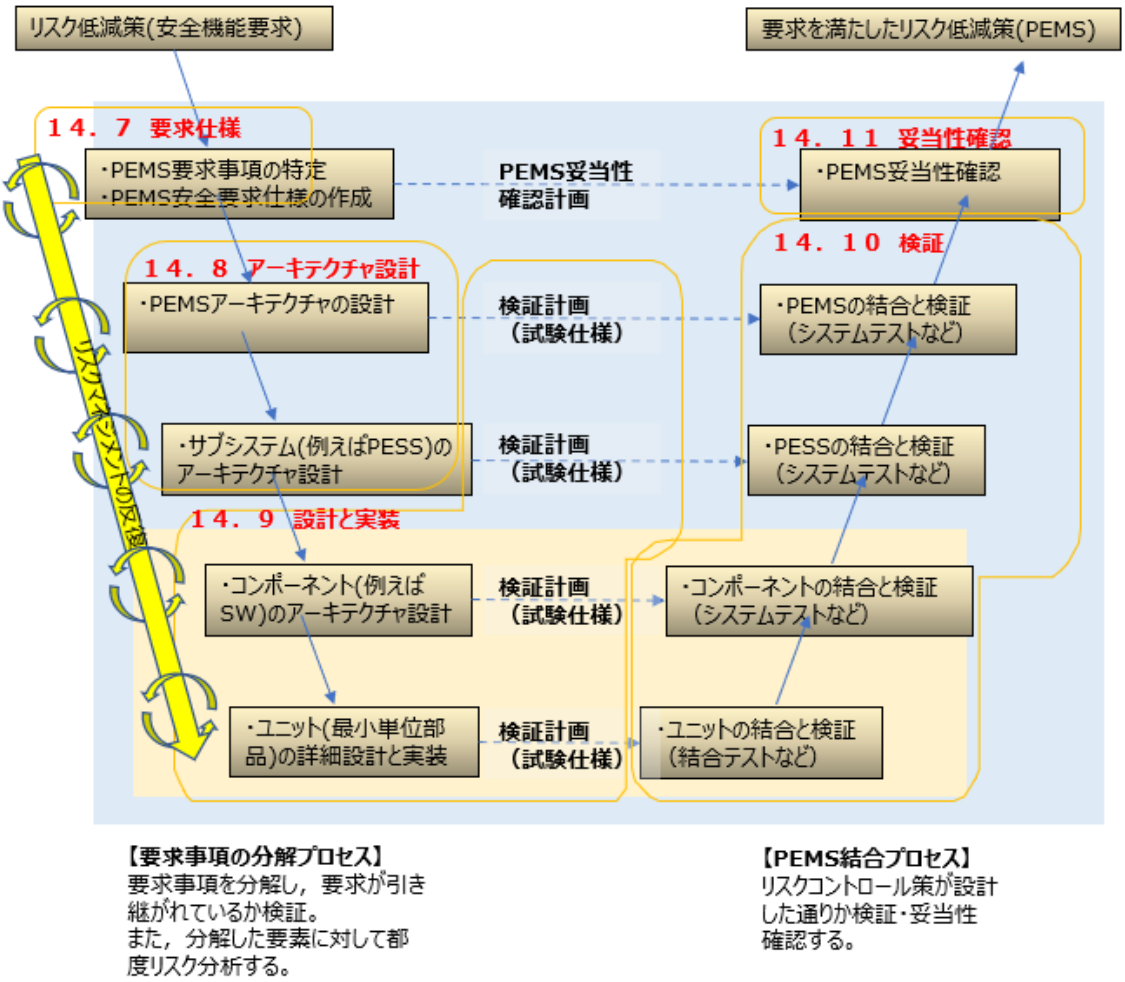


図 4-3 PEMS 開発ライフサイクル(IEC 60601-1 図 H.2 を簡素化)

PEMS の要求事項を **PESS** や他の**サブシステム**へ分解する時は，必要な機能に分け合理的な**サブシステム**の組み合わせになるよう構造（**アーキテクチャ**）を決定する。高い**安全**性が要求され，**冗長性**などの**安全**を考慮した構造が必要な場合は，この段階で考慮しておく必要がある。この段階で **PESS** を含む各**サブシステム**に対する要求事項が明確になるので仕様を文書化する。次いで各**サブシステム**の仕様を満たすように**サブシステム**の構造（**アーキテクチャ**）を決定する。**サブシステム**を構成する部分を，この規格の附属書ではコンポーネントと呼んでいる。一つもしくは複数のコンポーネントを組み合わせて，**サブシステム**を構成する。この規格では，コンポーネントは，更にユニットに分解される記述になっている。図 4-4 は，規格の図 H.1 a）複雑な**システム**の例をベースに，より簡単に階層を理解するために編集したものである。（正しくは規格を確認する必要がある。）

どこまで分解するかは，**PEMS** の複雑さによる。複雑な回路は，**検証**が困難になる。あるいは，第三者に**検証**の正当性を説明困難な状態になるため，少なくとも**検証**可能な大きさにまで分解する必要がある。あまり複雑では無い **PEMS** あるいは **PESS** の場合，**PESS** を構成する**サブシステム**まで分解すれば十分かもしれない。

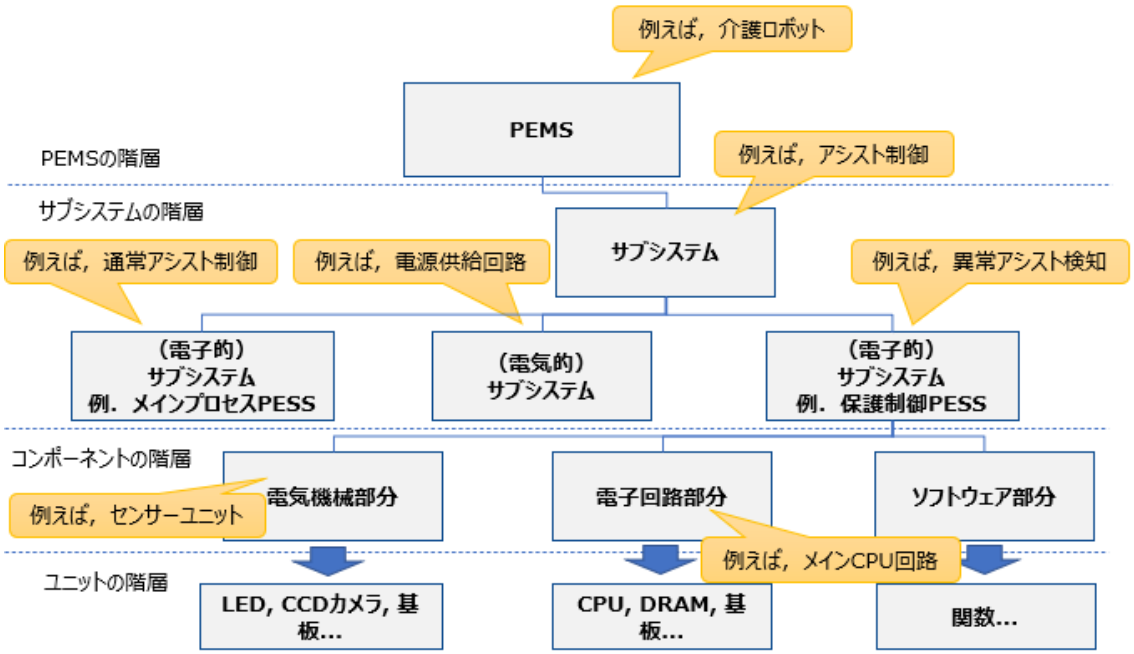


図 4-4 PEMS/PESS の階層構造（IEC 60601-1 図 H.1 を簡素化）

ここでは，ユニットを**検証**可能な最小単位として，説明を行う。**PEMS** 統合**プロセス**では，分解段階の最終出力であるユニットの仕様に従ってユニットを設計し実現することから始まる。実現したユニットはその仕様を満たすことを**検証**し**検証**結果を文書化する。次に，ユニット同士を統合して**サブシステム**（例えば **PESS**）を実現する。**サブシステム**はあらかじめ作成されている**サブシステム**の仕様（設計仕様書と**検証**仕様書）により**検証**され，**検証**結果は文書化される。最後に**サブシステム**を統合し **PEMS** を実現し**検証**し，結果を文書化する。その後，製品に組み込み，**PEMS** が**リスク**低減活動の結果として求められた当初の **PEMS** への要求事項を満たし，意図するように機能するかどうかの判断（**妥当性確認**）を行う。

PESS が複雑な場合など，PESS 開発自体で，**開発ライフサイクル**（例えば，V 字モデル）を回す必要があるかもしれない。重要なことは，行うべき開発活動（これをソフトウェアでは**アクティビティ**における**タスク**と言う。第 5 章参照）が漏れなく正しく行われることを確実にし，その実施を証明することにあるので，自社製品の複雑さに合わせて，使いやすい方法を選ぶべきである。

開発を進めると何かと問題が生じるため，**PEMS 開発ライフサイクル**は，都度見直し，必要に応じ変更することになる。当然ながら，変更履歴を残すなどの管理は必要になる。

4.1.3 設計プロセス

設計は，**PEMS 開発ライフサイクル**に定められた工程に従って行われる。

① 要求仕様 （IEC 60601-1 箇条 14.7）

ここでは，図 4-3 の **PEMS 開発ライフサイクル**において，**リスクコントロール**で特定された，**PEMS** 及び必要に応じて **PESS** からユニットに至るまでの**サブシステム**が担うべき**安全機能**やその**安全**度が要求仕様として文書化される。

PEMS やその**サブシステム**(**PESS** を含む)の**安全機能**には，ロボット介護機器の**基礎安全**又は**基本性能**に必要な機能をどのように提供するか，又は，**PESS** の**故障**が受容できない**リスク**を生じないことをどのような**安全機能**で達成するか。が示されるのは勿論。その**安全**関連対象物，作動頻度や環境などの使用条件や，応答時間などの要求事項を含む。

要求仕様は，当然 **PEMS** やその**サブシステム**の設計仕様となるが，同時に，作成された **PEMS** やその**サブシステム**の**検証**にも用いるので，仕様の記述には**検証**可能であることが求められる。

検証計画のポイントとしては，**安全機能**の振る舞い及びそれがどのくらい正しく作動するかの両方に対して明確にする。この規格では通常，ハードウェアに対しては、**単一故障安全**確保の**安全**仕様が用いられる（詳細は 4.2 章を参照されたい。）。または、不作動率の定量的な**検証**を行い，高**信頼性**を保証することを選択するかもしれない。ソフトウェアに対しては定性的アプローチとして，適切な**アクティビティ**が行われたことを**検証**することによって行うことが一般的である。

安全機能やその**信頼性**の記載は，当初の**リスク**がどの程度低減されるか示すことになるので，**残留リスク**の推定にも用いることができる。

PEMS がいくつかの **PESS** や**サブシステム**で構成される場合，各々の **PESS** や**サブシステム**に対して要求仕様として文書化し，**PEMS** の要求仕様に統合する方が，後日の **PESS** や**サブシステム**の**検証**などにおいて使い勝手が良いかもしれない。

要求仕様は，更に，上位の仕様（例えば製品仕様）を満たすことを**検証**する必要がある。

要求仕様が明確になった時点で，その**検証**仕様，及び，**妥当性確認**仕様や計画を立てることができる。

② 構造（アーキテクチャ） （IEC 60601-1 箇条 14.8）

ここでは，図 4-3 の **PEMS 開発ライフサイクル**において，**リスク**低減策としての **PEMS 安全**要求事項・仕様を設計後，その**リスク**低減策を実現するため，**図 4-4** のようにどのような構造で，どの**サブシステム**及びコンポーネントに**リスク**低減策の部分を割り当てるかを設計する。

一般的には，要求仕様を満たすための各アイテムの機能説明を始め，実現するための構造（この規格では「**アーキテクチャ**」と呼んでいる）やインタフェースの仕様が機能図，ブロック図，配置図などで示される。

また，単一**故障**時の**フォールト**トレラント性を考慮し，**冗長化**の構造が必要になるかもしれない。あるいは，処理速度を上げるために，特別な**アーキテクチャ**が必要になるかもしれない。要求仕様を合理的に満足するため以下のように **PEMS** や**サブシステム**，**PESS** の**アーキテクチャ**を決定する必要がある。

- **フェールセーフ**機能の採用
  たとえ**故障**しても，**安全**状態に遷移するような構造にする
- **冗長性・多様性**の使用
  1 チャンネルが**故障**している間は，他チャンネルの**安全機能**が作用して**安全**を確保し，他チャンネルが機能している間に**故障**を取り除く。**冗長性**（要求された機能を実行するための，二つ以上の手段）はハードウェアの偶発**故障**に対してのみ有効。**多様性**（要求される機能を実行する異なる物理的原理又は異なる設計方法で達成される手段。）は**系統的な故障**も有効。例：チャンネル A の**サブシステム**とチャンネル B を双方互いから独立した開発チームで設計し，同様のバグを回避する。
- 機能分割の手法
  サブシステムの機能を階層的に区分し、機能毎にアイテムを構成することで、視認性の高い設計が実現できる。また、**リスク**低減に関係するハードウェア部分と，そうでないハードウェア部分を明確に分離することで、**安全**関連部を最小限にする。また、IEC 62304 では、分割した**ソフトウェアアイテム**を**リスク**の大きさに応じて、**安全**クラス分類し、開発管理の厳しさを最適化することを求めている。
- **高信頼性部品**の使用
  この規格の**安全**要求事項につながるそのアイテムの要求機能を失わないことを確実にする特性を持つことの証明を要する。

更に，**アーキテクチャ**の決定にあたっては，次の事柄も考慮する。

- **PEMS** に要求される**安全機能**をいかに **PESS** や他の**サブシステム**に配分するか
- 部品やデバイスの**故障**モードとその影響
- **共通原因故障**の影響
- **系統的な故障**の影響
- **診断テスト間隔**及び**診断カバー率**
- 保守性　（保守のし易さ，**サブシステム**の補修カバー率）
- 合理的に予見できる**誤使用**に対する保護
- 通信仕様

アーキテクチャを明確にすることは，**PEMS** や**サブシステム**の**安全**度の**検証**に役立ち，また，その計算の正当性を第三者へ説明する際にも使うことができる。

また，**アーキテクチャ**を明確にすることで，**システム**の分割を論理的に実施できるようにする。分割により**システム**の複雑さ（いわゆるスパゲッティ化）を避けることは，管理しやすく，結果として，正しい設計や漏れの無い試験を期待できる。更に，将来の設計変更への対応や，第三者へ設計の正しさを示しやすくなる。

また，物理的な**サブシステム**配置をよく考えた分割は，ハードウェア**故障**時の**システム**の**障害**抑制に役立つ。電源喪失時の**安全機能**の維持。外界からの衝撃・静荷重ストレスに対する制御ブロックの保護。ハーネスへのノイズ干渉・クロストークへの耐性。診断及び修理などの保守性にも寄与する。
アーキテクチャの文書化は，要求仕様に含めてもよいし，**アーキテクチャ**仕様として独立してもよい。

③ 設計及び実装 （IEC 60601-1 箇条 14.9）

ここでは，**PEMS** 要求仕様及び**アーキテクチャ**検討の結果，決定された**サブシステム**について，それらを満たす設計仕様や**検証**仕様が文書化される。
複雑な **PEMS** の場合，**サブシステム**は更にそれを構成する**サブシステム**へと分割され，最終的には，**検証**可能な最小単位の**サブシステム**になる。ここでは，この**検証**可能な最小単位をユニット（**ソフトウェアユニット**を含む）と呼ぶことにする。設計仕様や**検証**仕様はこのユニットに対しても作成される。機能性を分割し，複雑性を抑制することをこの規格ではモジュール方式と呼んでいる。例えば，外界の画像認識による**障害**物検出などの複雑な **PESS** では，カメラ制御，ランプ制御，ダイナミックレンジの調整，ノイズに対するフィルタリングなどのアナログデータ処理，アナログ／デジタル変換処理，デジタル画像処理（抽象化のためのエッジ検出など）など，多様な**サブシステム**が連動する。これらの**アーキテクチャ**や相互作用を示し，機能ブロック図など関係性（配置）を図式化することで**リスク分析**が容易となる。複雑な**サブシステム**の場合，更に**検証**可能な単位まで機能分解し，最終的にコンパレータ回路，DMA，波形成形，関数（SW）などのユニットに分解・されることで，**システム**が**システム**の複雑化を避け設計および**検証**への理解が容易になり，既に確認済みの**サブシステム**の再利用や**システム**の機能性の拡張が容易になる。
また，**サブシステム**毎の設計仕様を明確にすることにより，異なった設計者が各々独立して設計することも有効な場合がある。これは特に**多様性**を用いた設計で効果があり，設計グループを独立させることにより，異なった設計思想の**サブシステム**が設計され，**共通原因故障**を抑制することが期待できる。設計仕様書などの文書化が行われるが，例えば，開発中に，**基本性能**又は**リスクコントロール**手段を変更する必要になる場合もあるので，影響する**要素**（**サブシステム**，コンポーネント，ユニット及びそれらに付随する設計**要素**）が追跡可能であることに注意が必要である。そのことで影響する**要素**が漏れなく**評価**されることを確実にする。
PEMS の設計及び実装では，次の**要素**について考慮する。

a) 設計環境，例えば，
- ソフトウェアの開発方法
- コンピュータ支援ソフトウェア開発（CASE）ツール
- プログラム言語
- ハードウェア及びソフトウェア開発のプラットフォーム
- シミュレーションツール
- 設計及びコーディング規約

b) 電子部品の性能・品質
c) 冗長ハードウェア
d) 人間と **PEMS** とのインターフェース
e) エネルギ源（電力喪失や変動などの考慮）
f) 環境条件
g) 第三者ソフトウェア
h) ネットワーク構築の選択肢

これらの**要素**の考慮は，設計の特性を明確にすることができ，それによって，設計及び実装の**プロセス**において，特性に着目した**リスク分析**を行い，適切な **PEMS 開発ライフサイクル**の実現に貢献する。

④ 検証 （IEC 60601-1 箇条 14.10）

ここでは，**PEMS** 及び実装された**サブシステム**が，**検証**仕様に基づき要求仕様を満たすことが**検証**される。

すべての**サブシステム**及びそれらの組み合わせに対して**検証**が行われるよう，**検証**計画が作成される。

検証計画には，**検証**方法のほか，以下の事項も含む。

- 各機能（**サブシステム**）に対して，どの工程で**検証**を実施するか。
- 担当部門，活動，技法
- 要員の資質，（設計部門からの）適切な独立性
- 手段の選択と用い方
- **検証**の範囲と基準

検証方法には，例えば次のものがある。

- 検査
- 文書照査
- 静的解析
- 動的解析
- 統計的解析
- **故障**挿入（単一**故障**を含む）

この規格では，多くは**単一故障安全**で確認されるが，ここでの**検証**は**安全機能**の確認であり，たとえ**単一故障安全**の判断基準で，この規格が箇条 13.1 で具体的に規定する**危険状態**に至らなくても，**ロボット**介護機器の**リスク**低減を目的とした**安全機能**が喪失，あるいは，低下（**リスク**が増大）する場合は，その程度により目的は達成せず，不適合となり得る。例えば，単一**故障**によるセンサの感度低下，応答タイミングの遅れなどが発生した場合，要求仕様であらかじめ規定した閾値を下回った場合に不適合となる。

大きな**リスク**に対応する場合，部品の**故障**モードとして，単純に短絡・開放だけでなく部品定格値の 50%や 200%への変化も考慮する。更に，タイミングや閾値に影響する部分に対しては更に詳細の検討が必要になるかもしれないので，対応する**リスク**に対してどの程度まで考慮が必要になるかよく検討す

る必要がある。（第 4.2 章で説明する。）

検証を行う人員や部門は，対象とする**リスク**にもよるが，設計部門（設計者）からの独立性が求められる。大きな**リスク**を対象とする**システム**の**検証**は，より独立性の高い部門（人）が行う。**医療機器**の場合，国や地域によっては，第三者による**検証**が要求される。独立性は，例えば，次のように考えることができる。

- 異なる人物： 同じ設計チームに属していても，設計者とは異なる人物（上司とは限らない）が**検証**する
- 異なる部門： 設計部門の設計を，品質管理部門が**検証**する
- 異なる組織： 外部試験所が**検証**する

この規格は，**リスク**のレベルと独立性のレベルの関係を明確に規定していないため，製造事業者自ら決定し，その根拠を文書化しておく。他の規格では，次の表のように規定している。

表 4-3 独立性の水準 (IEC 61508-1 表４から変更)

独立性の最低水準	**系統的な故障**がもたらす結果			
	A	B	C	D
異なる人物	X	X 1	Y	Y
異なる部門		X2	X1	Y
異なる組織			X2	X

A: 軽微な損傷，
B: 一人または複数の人に対する深刻な永久**障害**や一人の死亡
C: 数人の死亡
D: 多数の人の死亡
X: 最低限の独立性の水準
X1: 過去の経験が少ない場合や設計の複雑さがある場合の独立性の水準
X2: X 1 よりより経験が少ない場合や設計が複雑な場合の独立性の水準
Y: 独立性の水準が不十分

例えば、**系統的な故障**がもたらす結果は，この表のＢまでではないかと考えた場合，複雑さや経験の有無から**検証**を行うには「異なる人物」か「異なる部門」で十分と読めるかもしれない。しかし，この表が記載されている規格は，もともとプラントなどを念頭に考**えら**れており，**ロボット**介護機器とは生産数や受容可能な**リスク**レベルが大きく異なるので，製品やその市場の特性を理解し，**系統的な故障**が及ぼす結果に関して考慮が必要になる。

検証結果の報告書には，後日同じ項目の**検証**を行った場合の再現性を保証する情報を含む必要がある。温度や湿度などの周囲環境はもとより試験サイトの特定，使用測定器の特定，試験者名や，場合によっては，測定に用いた測定レンジやスイッチの位置，測定器の精度，校正の要求レベルおよび測定の不確かさ，用いたソフトウェアやツールの**バージョン**，パラメータ設定などが考**えら**れる。試験時の

記入漏れを避けるため，あらかじめ試験**記録**の様式を定め，考**え**られる項目の記入欄を設けることにより対応できるかもしれない。

⑤ PEMS 妥当性確認 （IEC 60601-1 箇条 14.11）

ここでは，**検証**を終えた **PEMS** が，**ロボット**介護機器に組み込まれ，当初の **PEMS** への要求事項を満たし意図するように機能するか（**リスク**低減するか）どうかの判断（**妥当性確認**）が行われる。
妥当性確認は，あらかじめ定められた計画に従い行う。**妥当性確認**に用いた方法・仕様や結果は報告書に記載し，文書管理の**手順**に従って管理する。報告書には，**検証**で述べたと同様の再現性を担保する情報を含める。
PEMS 妥当性確認は，**妥当性確認**によってだけで発見されるような予期しない相互作用が機能間で起こる可能性があるので，**PEMS** の**安全**性に対して重要である。また，**PEMS 妥当性確認**は，例えば大量のデータに対する試験，重い負荷又はストレスなどの機能限界，人的要因，**セキュリティ**，性能，構成**要素**の両立性，**故障**試験，文書化及び**安全**性を含めることができる。
PEMS 妥当性確認に責任を持つ者は，対象とする**リスク**のレベルに関わらず，設計チームから独立している必要がある。製造事業者は，その独立性に対する根拠を文書化する。また，設計チームのいかなるメンバーも，自ら設計した結果に対して **PEMS 妥当性確認**の最終判定責任を負うことはできない。
PEMS 妥当性確認チームの要員と設計チームの要員との全ての職務上の関係を，**リスクマネジメントファイル**に文書化する必要があり，これにより**評価**の客観性を示すことになる。
PEMS 開発ライフサイクルの有効性は，最終製品および開発の各段階の文書（証跡）を用いて第３者による客観的な**評価**がされるため，**妥当性確認**は重要である。また，**PEMS 開発ライフサイクル**の最終局面で行われるため，ここで問題が検出されると，開発の大きな手戻りとなる場合が多い。これを防ぐため，上流段階から設計と対になって**妥当性確認**活動も管理していくことが肝要である。

4.1.4 PEMS 内外の通信 （IEC 60601-1 箇条 14.13）

この規格では，**PEMS** を，**PEMS** 製造事業者にて**妥当性確認**されていない **IT ネットワーク**に組み込む場合の要求について規定する。しかし，**PEMS** 内部および外部との通信も，**安全**性に影響する場合があるので注意が必要となる。
この規格の規定は，以下の内容を取扱説明書などへ記載し，ユーザへ情報提供することを述べている。

a) **PEMS** 接続の目的
b) ネットワークに必要な特性
c) ネットワークの構成
d) ネットワーク接続の技術仕様
e) ネットワーク接続された他の装置との情報の流れ・経路
f) ネットワーク**故障**時の**危険状態**のリスト

これらの情報を合理的に特定するためには，**PEMS** の意図する接続環境を規定し，脅威の分析活動を行う必要があるかもしれない。

更に，以下の内容もユーザへ知らせることになっている。

- ネットワークへの接続が他の**リスク**を生じる可能性があること
- これらの**リスク**を特定・分析・**評価**・管理すること
- ネットワークの変更は，新たな**リスク**を生じる可能性があるので，分析すること
- ネットワーク変更には次のようなものがあること
  - ネットワーク構成の変更
  - 接続機器の追加
  - 接続機器の取り外し
  - 接続機器のアップデート
  - 接続機器のアップグレード

これらは，記載された文書類（取扱説明書や設置マニュアルなど）の確認で行うことになっている。

PEMS 内部および外部との通信が**安全**性に影響する場合は，通信**エラー**検出して対処することになる。

高い**リスク**を生じる通信には，低い通信**エラー**（信頼できる通信）が必要になるが，この規格にはその値は明記されていない。しかしながら，通信**エラー**は，ハードウェア**故障**と同様に考えることができるので，許容できるハードウェアの危険側**故障率**を自部門で決定し，これと同じ値を用いることができるかもしれない。

一般的には，次のような**エラー**が考**えら**れる。

- データの破壊
- 意図しない反復
- 正しくない順番
- 喪失
- 受容できない遅延
- 挿入
- なりすまし
- 誤配（アドレス違い）

通信**エラー**への対処としては，次のようなものがある。

- シーケンス番号
- タイムスタンプ
- 時間予測
- 接続承認
- フィードバック
- データ完全性保証
- 相互確認冗長
- 異なる完全性保証**システム**

このようなことを検討し，どのような方法を用いるかを決めることになるが，どの方法を用いるとどの程度の**エラー**レートになるかといった規定は無いので，最終的には**エラー**レートを実測することになるかもしれない。
【参考】機械**安全**で用いられる**安全**データ通信の一般的な手法は付録 C に記している。

4.1.5 変更管理 （IEC 60601-1 箇条 14.12）

PEMS を新しく設計する場合は，**PEMS 開発ライフサイクル**を新たに進めることもできるが，一般的には，すべてを新しく設計せず，過去の設計を流用する場合がある。この場合，あたかも新規設計として取り扱い，以前の文書類を引用することなく，すべての工程を適用し，**リスクマネジメント**の報告書を作成し，この規格への適合を示すことができる。
以前の設計の一部を設計変更して用いる場合で，全工程を適用しない場合は，以前の設計が引き続き有効であり，かつ，変更内容を定められた変更**手順**に沿って**評価**してその適合性を示すことになる。
変更管理の**手順**には，現行の **PEMS** に何らかの問題が生じた場合の，その問題解決のための変更活動も含めることができる。この場合，変更活動を開始するためには，変更理由などを記した変更申請を作成し，責任部署が開始の判断をすることになる。変更された設計は，変更が及ぼす影響を解析し，**PEMS 開発ライフサイクル**のどの部分から開始する必要があるか，言い換えれば，変更前の **PEMS 開発ライフサイクル**のどの部分が有効であるかの判断を行い，しかるべき工程を繰り返すことになる。最終的には変更の**妥当性確認**を行い変更申請が了承された後，設計変更が承認される。新規開発と同様，活動は文書化され管理される。当然ながら，担当部署の責任は明確になっている必要がある。
尚，ソフトウェアの場合にはその変更容易性から特に変更管理について留意する必要がある。そのため IEC 62304 では **PEMS 開発ライフサイクル**よりも更に詳細な要求があり，第 5 章で解説を行う。

4.1.6 ハードウェアの系統的な故障への対応策

ハードウェアの**系統的な故障**への対応の多くは，先に述べた設計管理により達成することになるが，具体的には，次のようなハードウェアの構成や技法の選択を考慮することになる。

- 安全制御部への動力が喪失した場合に**安全状態**を維持できるようにする
- **安全機能**喪失をもたらす電源喪失，電圧変動，過電圧，低電圧，周波数変動への対応
- 温度，湿度，振動，塵埃，腐食などの環境への対応
- 電力系と信号系の分離
- 信号系の断線や地絡の**監視**
- 厳しい電磁イミュニティ試験
- 制御回路を冗長化する（単純冗長，**多様性**を用いた冗長化，冗長回路の相互**監視**など）
- **故障**検出
- ポジティブモードによる操作（エネルギーを加えることによる起動など）
- 機械的に結合された接点（接点が連結されたリレーなど）
- 直接開離作用（ばねや電気回路などを仲介せずに直接力を加え接点を開くなど）

- 非対称**故障**モード（A 接点と B 接点の組み合わせなど）
- 少なくとも 1.5 倍以上の大きな定格部品の使用

残念ながら，どの**リスク**レベルに対応するためにはどの手法を取る必要があるか，どの程度対応する必要があるかなどといった明確な規定は無いため，**製造業者**が独自に検討して選択する必要がある。重要なことは，自社製品に採用した手法の選択理由とその**検証**結果を文書として残し，第三者へその正当性を説明できるところにある。

尚，ソフトウェアの**系統的な故障**については第 5 章にて説明する。

4.2 単一故障安全の実施ガイド （箇条 4.7，箇条 13.1 及び 13.2）

ロボット介護機器が**医療機器**と見なされる場合，この規格により，ハードウェアの**偶発的な故障**に対して，箇条 4.7，箇条 13.1 及び箇条 13.2 に示される**単一故障安全**の**評価**を行う。

箇条 4.7 では，医療電気機器は**単一故障安全**を確保できるように設計するか，又は**リスクマネジメント**を適用して**リスク**が受容できる状態にすることを求めている。これは純粋なハードウェアの組み合わせで**単一故障安全**を満足するケースと，ソフトウェアを含む電子**制御システム**で**リスクコントロール**を行い，**PEMS** の**安全**要求を満たすことで**安全**性を確保する場合の 2 つのケースを示している。

箇条 13.1 及び箇条 13.2 では医療電気機器の典型的な**危険状態**と**単一故障状態**について，主に電気**安全**の観点で示されている。このガイダンスでは，これらの要求を**機能安全**の視点で満足するための実践的な方法を解説する。

機能安全では，『部品とはいつかは壊れる。』という考え方をする。**ロボット**の寿命までに，ある程度の確率で必ず発生するハードウェアの**偶発的な故障**を想定し，**危険側故障**に至る**リスク**が許容できる程度になるよう設計する必要がある。一般的な製品**安全**でも，規格が具体的に言及する感電や火災の**リスク**を**評価**するために**単一故障状態**の**安全**の確保を要求している。**ロボット**介護機器の**機能安全**の場合は，**リスクコントロール**で特定された，**PEMS** 及び PESS が担うべき**安全機能**への要求仕様（4.1.3 章②参照）が，**単一故障状態**で**障害**状態にならないような構造が要求され，その**検証**も要求される。この**検証**は，実際の**故障**のシミュレーションを行い，**PEMS** が**障害**状態にならないことを確認することがメインであり，**図 4-5** に示す **PEMS 開発ライフサイクル** V 字モデルの右側にて行われ，できるだけ実環境を想定したシミュレーションをする必要がある。また，すべての**故障**シミュレーションは，特に端子数が多いマイコンなど，多大な時間を要したり，実際に**故障**状態を実現することが現実的では無かったりするため，回路図を読んで **FMEA** などの**故障**解析を V 字モデルの左側で行い，実際の**故障**シミュレーション試験を省略できる場合もある。これらの**検証**を適切かつ効率的に行うためには，**PEMS 開発ライフサイクル**の設計段階 V 字モデルの左側から実際には取り組むことがポイントである。

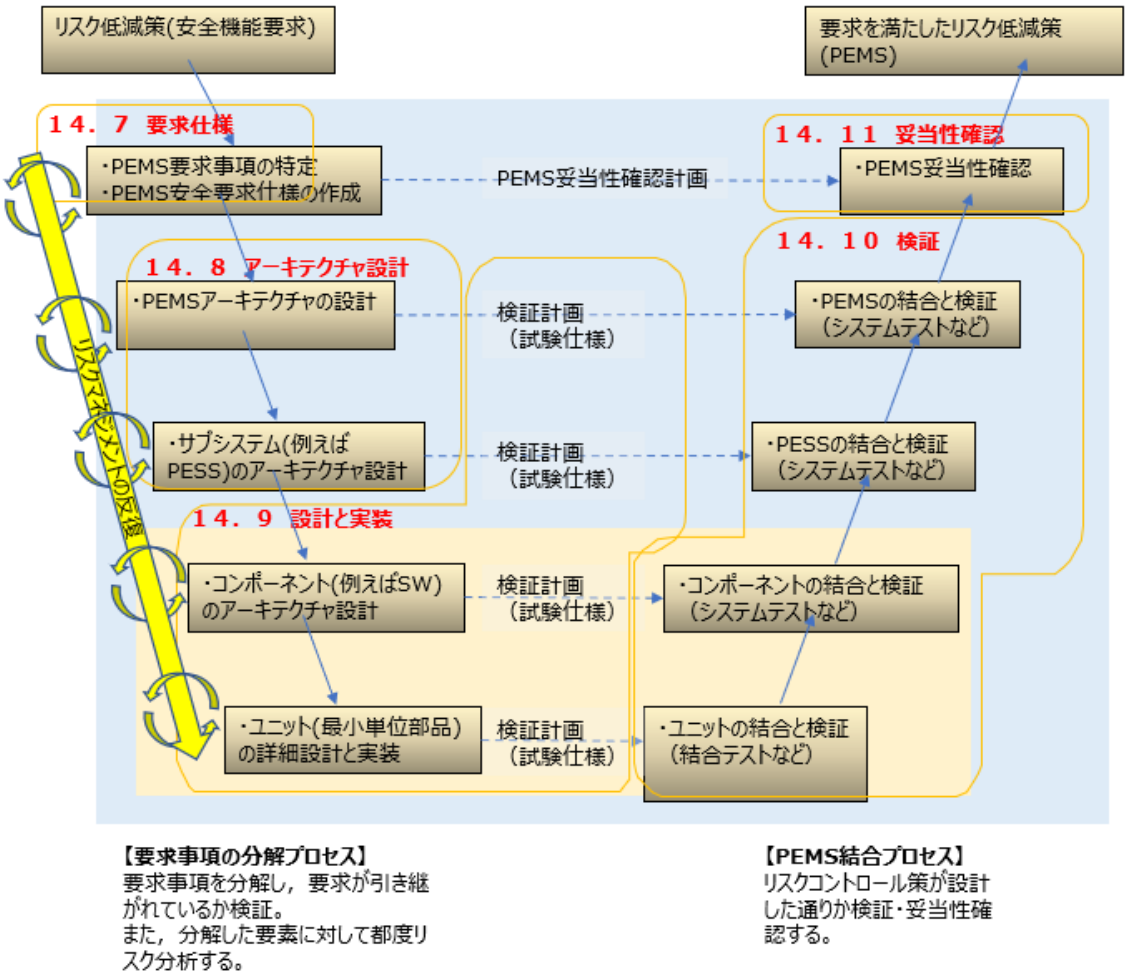


図 4-5　PEMS 開発ライフサイクルの V 字モデル

4.2.1 単一故障安全

この規格には，「単一**故障**」という言葉は定義されていない。定義されているのは，「**単一故障状態**」と「**単一故障安全**」とい言う言葉である。**単一故障状態**とは，「**リスク**を低減させる手段の一つが**故障**しているか，又は一つの**異常**状態が存在する **ME 機器**の状態」と定義されている。すなわち，**単一故障状態**というのは，単に抵抗やコンデンサなどの部品**故障**だけではなく，**リスク**低減を提供する「手段」の**故障**や，**リスク**低減するしないにかかわらず，一つの**異常**状態も含むことになる。尚，家電や事務機器の規格では，抵抗やコンデンサなどの部品だけを指し，その**故障**を単一**故障**としている。

この規格では，**安全機能**の**障害**以外にも**単一故障状態**における，火災・感電・ケガなどの**基礎安全**の不適合も**評価**している。このガイダンスは，あくまで**ロボット**介護機器の**安全機能達**成を目標とするが，理解を深めるため，**安全機能**の**障害**以外にもそれに付随して生じるこれらの**リスク**も述べている。

① 単一故障状態

この規格で**単一故障安全**は，「**予測耐用期間**中の**単一故障状態**においても受容できない**リスク**を生じない **ME 機器**又はその部分の特性」と定義され，この状態を維持できるように設計することになる。
この規格では，受容できない**リスク**として，以下のような状態を**危険状態**としている。製品ライフサイクルのあらゆる**単一故障状態**でこのような**危険状態**にならないことが**単一故障安全**ということになる。

- 炎，溶融物質，危険な量の有毒物質及び発火性物質の放出
- 危険部位への接触を生じるような外装の変形
- 温度が許容値を超える
- 絶縁の劣化による漏れ電流の増加や感電
- 意図しない動き
- 不安定姿勢
- 騒音の発生
- 圧力の上昇
- その他，機械的**ハザード**の発生

そこで，まず**単一故障状態**の理解が必要になる。

② 単一故障状態の範囲

一つの**単一故障状態**が更なる**単一故障状態**を引き起こす場合や，更にその**故障**が他の**単一故障状態**の誘因となる場合などはいわゆる**従属故障**と呼び，これらを一塊（一つ）の**単一故障状態**と見なす。
このような状態は，最初の**単一故障状態**で他の部分が過負荷状態になる場合などに起こり得る。
また，電源部分の**単一故障状態**では，電圧の上昇や下降が生じ電源部分以外の多くの箇所が機能低下する場合もあるが，これを**共通原因故障**と呼び，これも**単一故障状態**と考える。この規格では，**単一故障状態**のシミュレーション中に，その状態で過負荷などによって**故障**が起こりやすくなる部品や**故障**検出ができなくなる部品の**故障**を考慮することになっている。場合によっては，**単一故障状態**を検出できない場合もある。検出できない**単一故障状態**がたとえ**リスク**を増大させることがなくても，検出できない**単一故障状態**が潜在する状態で起きる次の**単一故障状態**も，その可能性が無視できなければ，あわせて**単一故障状態**として検討して**リスク**が受容できるレベルを超えないことを確認する必要がある。
この規格では，確率が高くかつ予測も検出もできない**故障**は常に存在すると考えている。更に，そのような**故障**が一つあるいは複数潜在することも想定することになっている。それゆえ，それらの**故障**は個別，及び，組み合わせて考慮する場合があるとしている。

③ 単一故障状態の除外例

この規格では，**単一故障安全**を**単一故障状態**で「**リスク**を生じない」と言い切っているが，実際には，**故障**確率が無視できるほど低い場合は，「**故障**しない」と見なすということである。ただし，**故障**確率がど

の程度であれば無視できるかとの記述は無い。他に，「**故障**しない」と見なす例として，**強化絶縁**のように通常の絶縁の 2 倍以上の強度を有する十分に強い絶縁は絶縁破壊を起こさないと見なしている。**強化絶縁**に関しては，他の規格においても同様の考えをしている。十分に強くして**故障**しないと見なすという考えは，機械部品にも適用され，何かを吊り下げる場合に 8 倍の**安全**率があれば，**故障**しないと見なすことができるとしている。他にこの規格では，「**高信頼性部品**」が定義されており，製品の**予測耐用期間**中の考**えら**れる環境条件・ストレスがあっても，**安全機能**に**障害**が無いことが確実であれば，同様に**故障**しないと見なすことになっている。

また，二重化により**単一故障安全**を達成することもできる。この場合，一つは，最初の**故障**が製品の**予測耐用期間**内に検知でき，かつ，第 2 の**保護手段**が**故障**する前に検知できる場合である。もう一方は，**リスク**を低減するための第 2 の**保護手段**が製品の**予測耐用期間**中に**故障**する確率を無視できるほど低くするというもので，この第 2 の手段が**高信頼性部品**として取り扱われていることになる。このように**アーキテクチャ**の工夫で**故障**を抑制することが有効である。二重化による**単一故障安全**の達成というと，**二重絶縁**が連想できる。**二重絶縁**も**故障**しないと見なすことができ，次章で解説をする。

この規格では，「小さな電力では発火しない」という発想で，**単一故障状態**での電力消費が 15W 未満やエネルギ消費が 900J 未満の**単一故障状態**を除外しているが，これはあくまで電気**安全**観点の”発火“に関しての条件であり，**安全機能**の**評価**に関しては，そのような除外は適用しない。

【参考】ISO 13849-2 の附属書 D に，基本**安全**原則，**故障**の除外例の記載がある。

④ 考慮すべき単一故障状態

一般的に**単一故障状態**というと，コンデンサや抵抗，半導体類の短絡や開放を指す。この規格では，絶縁破壊による感電や発火などの**安全機能**の**障害**以外の**リスク**も規定しているが，それらの**単一故障状態**は**安全機能**の**障害**の**評価**にも用いることができる。規格の箇条 8.1 が言及する典型的な例をここで要約して以下に記す。

- **絶縁の短絡： 基礎絶縁**を構成する，**沿面距離**，**空間距離**，および絶縁物（**二重絶縁**のいずれか片方も含む）の短絡
- 部品の短絡： 絶縁物，**空間距離**，**沿面距離**と並列に接続された部品の短絡（但し，**高信頼性部品**と短絡モードが生じえない部分は除く）
- **保護接地**線や内部保護接地接続の一つの開路（但し，永久設置形の保護接地は除く）
- 電源導線のいずれか 1 本の断線（但し，多相機器，永久設置形の機器の中性線を除く）
- 外装が独立した機器の部分間で電源を供給する導線が，その許容限度を超える可能性がある場合，導線のいずれかの断線
- 部品の意図しない移動（不十分な固定による部品の移動）
- 導線やコネクタの外れ（機械的固定手段の一つが外れることは**単一故障状態**と見做す）

絶縁の短絡 要求により，**安全機能**を制御する回路のパターンは所定の間隔を満たさない隣接するパ

ターンと短絡されることを考慮する。**基礎絶縁**，**沿面距離**や**空間距離**など短絡すべき絶縁に関する専門用語について，ここで規格の定義と **PEMS 安全**要求としての扱いを解説する。

- **基礎絶縁**：電撃に対する基礎的な保護のために備える絶縁。（箇条 3.9）
  規格では，**故障**の無い状態で人体の直接接触による感電から保護するための基本的な絶縁を意味する。**単一故障状態**では短絡されるものと考慮する。
  →【**PEMS** の要求としても短絡しうると考える。】
- **補強絶縁**：**基礎絶縁**の不良時における電撃に対する保護のために，**基礎絶縁**に追加して使用する独立した絶縁。（箇条 3.119）
  他の**安全**規格だと**付加絶縁**や追加絶縁と呼ぶ場合もある。感電に対する**故障**保護として，**基礎絶縁**がある前提で，それに加えて施す独立した絶縁のこと。
  →【**基礎絶縁**が**故障**した後，2 つ目の**故障**が短時間で発生することまでは考慮しない。】
- **二重絶縁**：**基礎絶縁**及び補強絶縁の両方で構成した絶縁。（箇条 3.23）
  基礎絶縁及び**補強絶縁**の二つの分離可能な**保護手段**から構成される絶縁のこと。
  →【2 つの絶縁が短時間で発生することまでは考慮しない。】
- **強化絶縁**：二つの**保護手段**を備えた単一の絶縁**システム**。（箇条 3.99）
  感電に対して，**二重絶縁**と同等の保護となる分離不可能な単一の絶縁**システム**のこと。
  →【規格で定められた堅牢な絶縁であり，**故障**が発生することを考慮しない。】
- **機能絶縁**：機器が正しい機能を果たすためだけに必要な絶縁で，この規格で定義されている人体への感電保護目的の絶縁ではない。
  →【**PEMS** の要求としても短絡しうると考える。】

上記解釈から、**機能絶縁**と**基礎絶縁**の**沿面距離**，**空間距離**は短絡する。対して**追加絶縁**，**二重絶縁**と**強化絶縁**まで満たした距離であれば短絡は考慮しない。

単一故障状態を考慮する時，パターンギャップや，パターンと部品間などのギャップとして**沿面距離**と**空間距離**の 2 種類の距離を考慮してパターン設計する。規格による用語の定義と **PEMS** への**安全**要求を以下に説明する。

・ **沿面距離**：二つの導電性部分間の絶縁物の表面に沿った最短距離。（箇条 3.19）

・ **空間距離**：二つの導性部分間の空気中の最短距離。（箇条 3.5）

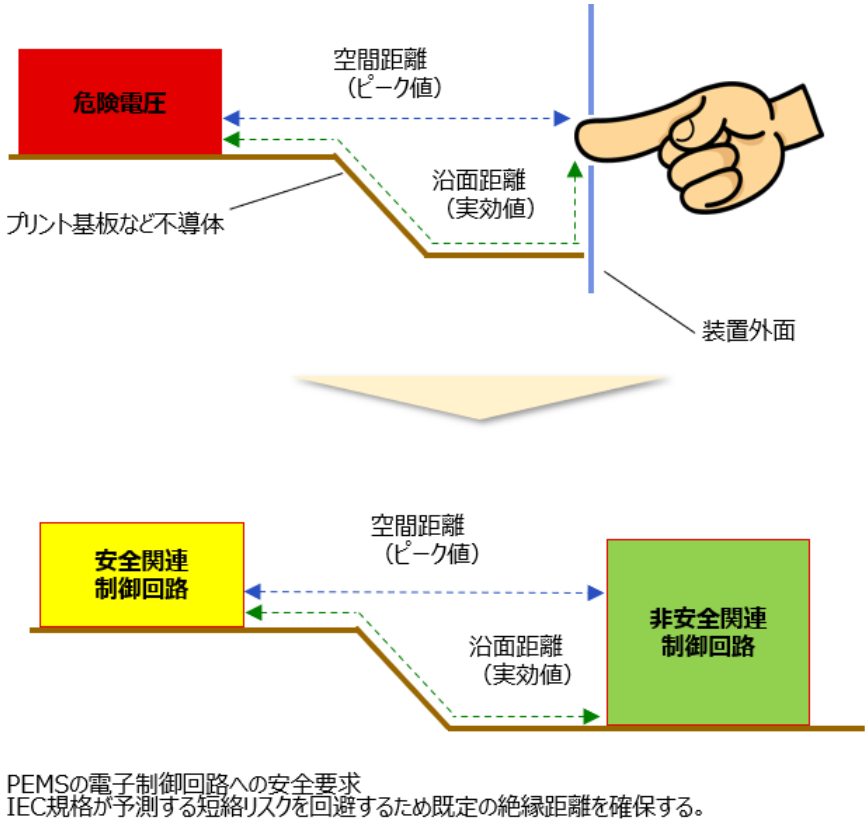


図 4-6 回路間の短絡の考慮

・

尚，保護接地とは，IEC の製品安全規格で感電を保護するための一つの保護**システム**と定義づけられている。

- **保護接地**：絶縁破壊に際し，機器の電位を大地と同じに保つための定義された電気安全のための接地。
- **機能接地**：電気安全以外の目的で，機器の機能のために接地すること。

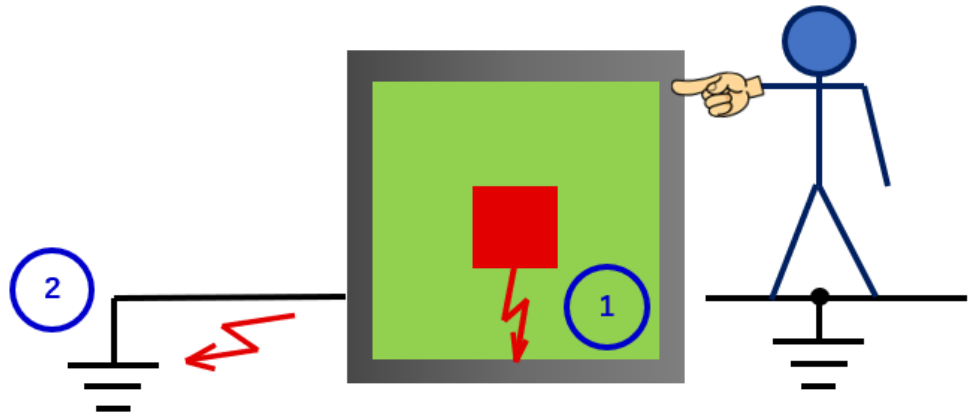


図 4-7 保護接地の説明図

保護接地は一定の規格要件を満たした「**信頼性**のあるアース」であり，**基礎絶縁**が破壊したときに,外殻の電位を低く保つことにより、人への感電を防ぐ役割がある。**基礎絶縁**が**故障**したとき，対地に電流が逃げれば，適切に選定したヒューズなどが溶断し，機器への電力供給が遮断されるので，ユーザーは**故障**に気づき、製品として感電**リスク**を抑制し、**基礎安全**を確保する。一方で、**医療機器**としての性能（心臓ペースメーカーや血液透析器など）を継続することが**安全**仕様として求められる場合、この**基本性能**は満たせなくなる。このように、**PEMS** の単一**故障**は、上位の**安全**要求に基づいて考慮される。

話をパターン設計に戻す。前述の通り，単一の**基礎絶縁**は**故障**すると考えるが，一方で**故障**しないと想定する絶縁もある。4.2.1 章③で述べた通り，**単一故障安全**を達成する手段とは，

- 最初（一つの，例えば**基礎絶縁**）の**故障**は起こり得るが，２つ目の（例えば追加絶縁）の**故障**が発生する前に，最初の**故障**が検出されて，**安全**状態に移行する。
- ２つ目の**故障**の発生が**予測耐用期間**より長い場合は２つ目の**故障**（例えば，強化絶縁の**故障**）は想定しない

という規格のコンセプトによる。

この規格では単一ユニットである**基礎絶縁**の絶縁距離，要はパターン間や可触部へのギャップに求められる**空間距離**と**沿面距離**に必要な寸法は規格の箇条 8.9 にて規定され，以下の要因により要求寸法は変化する。

- 電圧： **システム**の定格電源電圧，実際の対象個所の動作電圧の実効値，直流値またはピーク値，過電圧**カテゴリ**毎に規定された電力網から到来するインパルス電圧

- 汚染度： 絶縁が汚染される事による絶縁劣化を考慮するための周辺環境の分類
- ＣＴＩ（比較トラッキング指数）： 絶縁材料表面が電圧と湿度によりどれだけ炭化されにくいかを示す指数。

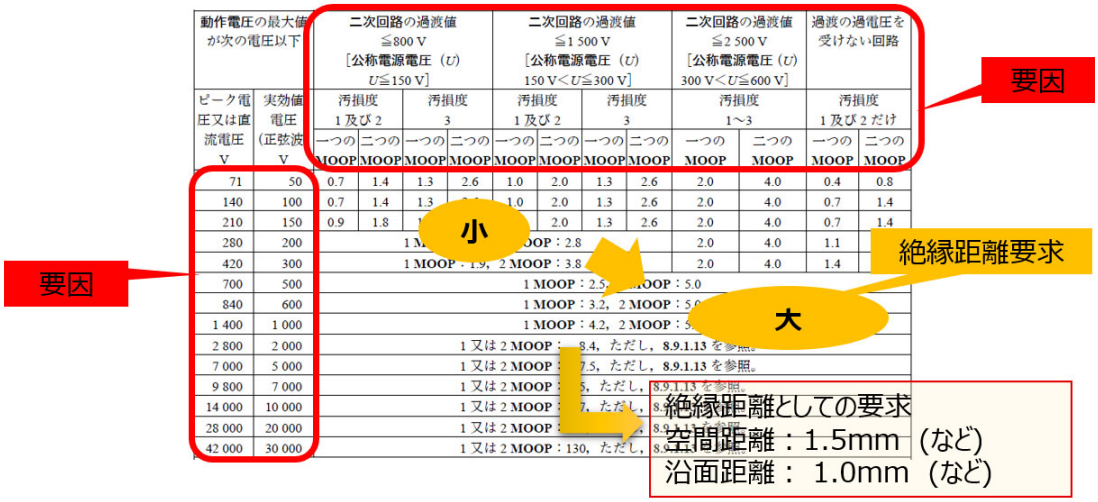


図 4-8 絶縁距離に影響する要因

基礎絶縁として隣接する基盤パターン間を 3.0mm の**沿面距離**を確保したとする。**基礎絶縁**は１つの絶縁**システム**なので『**故障**（絶縁破壊）する。』と考えるが，

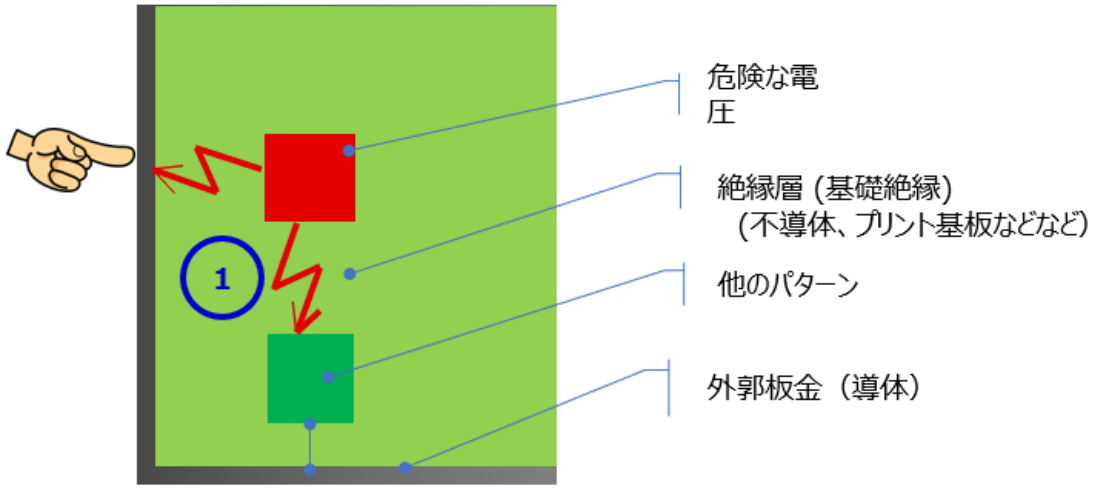


図 4-9 基礎絶縁（1 重の絶縁）の故障の想定

基礎安全を２つ重ねた場合，２つ同時に『**故障**（絶縁破壊）は想定しない。』（絶縁のみに関して言えば規定された耐用期間中の２つの絶縁破壊は無いと見なされる。）。**強化絶縁**は**基礎絶縁**と**補強絶縁**の２つの絶縁**システム**であるため**故障**しないと考える。

注記： ただし，実際の現象としては，絶縁破壊の特性に基づく**故障**回避の手段という意味もある。

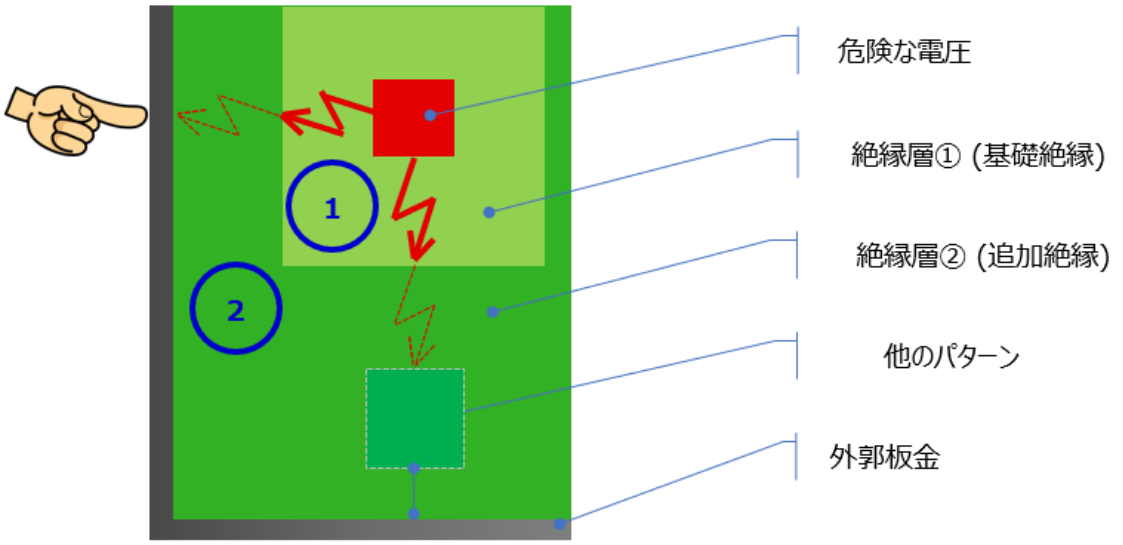


図 4-10 二重絶縁（基礎安全を２つ重ねた場合）の故障（絶縁破壊）の除外

一般的な回路では，ヒューズなどの遮断器を備える場合が多いため，**基礎絶縁**が破壊しても，保護接地されている場合にはヒューズが作動し，機器は使用できないことがユーザにとって明らかであり，**安全**上は，最初の絶縁**システム**の**障害**が，２ つ目の保護**システム**であるヒューズにより検出されて，電力遮断という**安全状態**に移行する。と見なされる。（図 4-7 参照）

強い絶縁（**二重絶縁**と同等の保護）となる１つ（単層）の絶縁**システム**は**故障**（破壊）しないと考える。規格には**強化絶縁**の**沿面距離**及び**空間距離**の寸法が規定され，この距離を満たしていれば機器の**予測耐用期間**中に**故障**（絶縁破壊）は無いとして扱われる。尚，距離のみではなく絶縁体（厚みのある不導体又は ２ 層以上の薄膜絶縁）についても**強化絶縁**の規定が規格（箇条 8.8）にはある。実際の設計時には確認することが必要である。

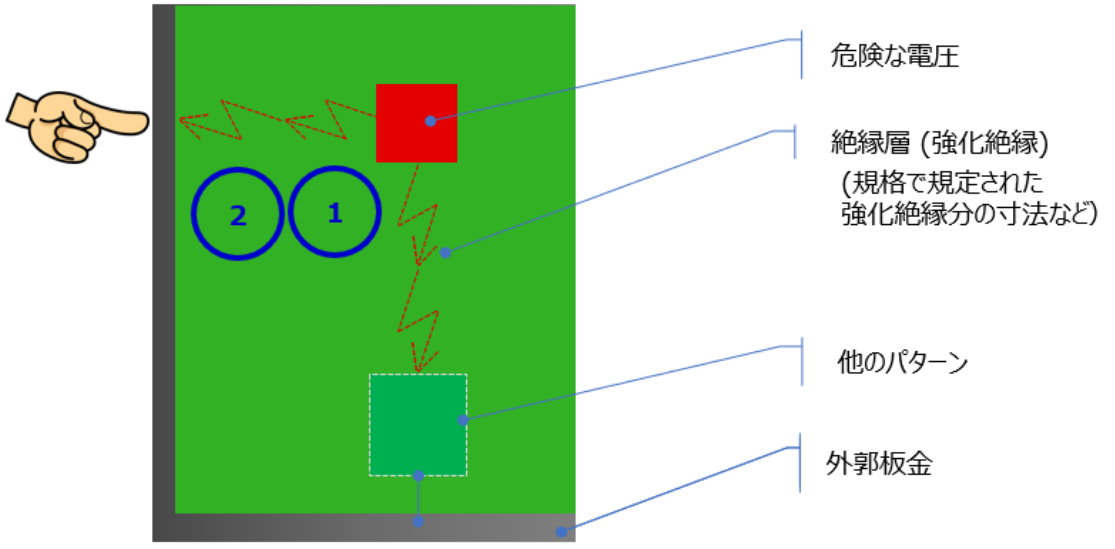


図 4-11 強化絶縁の説明図

⑤ 単一故障状態の例

PEMS が持つ**安全**性を考えた時，一般的により高い**リスク**は，より詳細な**故障**モデルの考慮が求められる。**医療機器**として，**故障**の想定に具体的な要求はないので，各**製造業者**が**リスク分析**で**故障**の想定リストを作成する。その際には，**保護方策**，**基礎安全**及び**基本性能**を考慮して，その**安全**性を侵害する**故障**状態を考慮する。ただし，機器の**予測耐用期間**の製品ライフサイクルにおいて**故障**が考えにくいケースについては，考慮することは効果的ではない。
この章では，**ロボット**介護機器の設計者が参考にするための電気電子デバイスの典型的な**故障**ケースを挙げているが，この例だけではないので注意を要する。

- 抵抗類

一般的には，短絡と開放を**単一故障状態**として検討する。プルアップ抵抗の**故障**により，信号の論理が固定されてしまうこともあるだろう。
金属皮膜抵抗やフィルムタイプ抵抗の短絡が除外できるなど，抵抗の構造により**故障**のあるモードを除外が可能な場合もある。ただし，電蝕やパルス性電流の影響により開放することがあるので，使われる場所によっては**故障**が無視できない。
故障がもたらす**リスク**が非常に高い場合は，抵抗値の倍(200%)や半分(50%)への変化までも考慮するなどの方法がある。更に，**リスク**が非常に高く，高い**信頼性**が要求される場合において，時定数が回路動作に関係する場合は，時定数に影響する値の考慮が必要になるかもしれない。

- コンデンサ類

以前は，単純な構造のセラミックコンデンサの短絡除外を認める規格もあったが，現在では，電源回路に用いる電磁妨害対策用の**強化絶縁**と同等の絶縁性能を有すると見なされる一部のコンデンサ以外では，短絡並びに開放を**単一故障状態**として検討することが望ましいと考える。また，容量の減少や力率の変動も考慮が必要になる。特に，容量変化が**安全機能**に影響する場合は，注意を要する。
【参考：IEC 60384-14 の Y1，Y2 キャパシタは強化絶縁と見做すことができる】

- 半導体類

ここで言う半導体類は，各種ダイオード，トランジスタ，IC などの固定ロジック半導体を指す。ダイオードやトランジスタなど単純な構造の半導体は，各端子の開放と各端子間の短絡を**単一故障状態**として考慮する。ツェナーダイオードのツェナー電圧のドリフト及びトランジスタの増幅率の変化，周波数特性などの細かな特性変化まで考慮するかは，**製造業者**が**リスクマネジメント**に基づいて決定すべきことである。
IC 類は，内部回路が分かり，短絡が起きないことを示すことができない限り，すべての端子の開放と，すべての端子間の短絡を**単一故障状態**として検討する。IC では寄生発振も必要に応じ考慮する。
オプトカプラのように，入力と出力が内部で分離されている場合で，**強化絶縁**や**二重絶縁**で分離されていることが仕様上確認できる場合は，入力と出力の短絡は基本的には考慮しない。（ただし，リード間

の空間距離や，基板パターンや外部シリコン表層に沿った**沿面距離**は**ロボット製造事業者により寸法確認が個別に必要かもしれない。）**

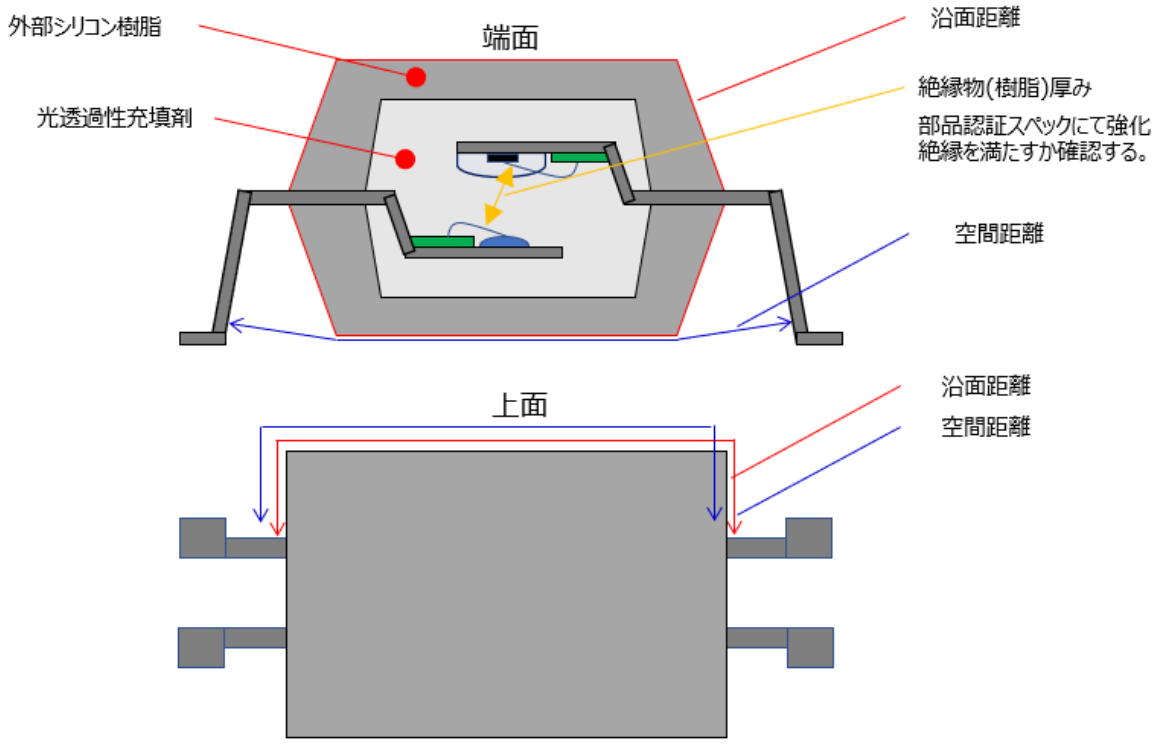


図 4-12 フォトカプラの絶縁距離測定の例

尚，CPU のように多くの端子が出ている場合，全ピン間の短絡及び開放，スタックアット"0"，"1"，発信などを想定すると多大な**評価**工数になるが，そもそもそれらの**単一故障状態**が**安全機能**の低下をもたらさないことを回路動作から理論的に示すことができれば，実際の試験を省くことができるので，検討の価値がある。

【参考：本章の 4.2.4 章 には，CPU や MPU 関連の一般的な**故障/エラー**状態と必要な対策の例を参考として記載する。】

➢ トランス類

電源トランスやスイッチングトランスは PESS の電源供給を全部もしくは部分的に行っている場合があり，電源喪失時の状態を分析する必要がある。

トランス類は既に部品としての規格に適合している場合が多く，その場合，部品としての**単一故障状態**の検討は省略できる場合もあるので，まずは適合状態を確認する。もし適合していない場合は，個別完成品などの該当規格（例えば，IEC 60601-1 など）を用いて試験することになる。基本的には，**基礎絶縁**以下の部分の短絡，層間の短絡など行う。

【参考：トランス類の部品規格として IEC 61558 シリーズがある。】

➢ モータ類

ロボット介護機器の動力源となるモータ類の**故障**は，可動部の意図しない危険な動作を引き起こすのは勿論，コイル部分からの発熱や発火に関する**基礎安全**の侵害も分析する必要がある。
コイルの短絡・開放，並びに回転軸の固着・拘束や可能性があればモータの過負荷も，**単一故障状態**として検討する。
【参考：モータ類の部品規格として IEC 60034 シリーズがある。】

➢ 導体・ケーブル類

単一故障状態としては，導体の開放がある。規格でも保護接地線の開放や電源導線の遮断を典型的な**単一故障状態**として挙げている（本ガイダンス 4.2.1 章④参照）。
また，線間の短絡も以下に述べるいくつかの除外例を除き**単一故障状態**として検討する。

- 機器内部の配線: 恒久的に接続され，ワイヤダクトなどで保護されている
- 多 芯 のケーブル: 個別に接地シールドされた芯線

ロボット介護機器内部の配線であっても，振動環境に設置される場合，又はケーブルや導体が機構部分に取り付けられて摺動するなど，機械的なストレスがかかる場合は，そのようなストレスに対応できる定格を有することが証明できなければ，線間の短絡を無視することはできない。
【参考：機器内部・外部の配線に関しては，IEC 60204-1 に記載がある】

➢ プリント基板

該当する規格に適合しない限り，銅箔の剥離による開放や隣接する銅箔との短絡は，**単一故障状態**として検討する。トランスなどの重量部品を支持する部分においては振動によるスルーホールの剥離・クラック。長いパターンにおいては温度変化による基材の膨張収縮ストレスやたわみなどに注意が必要である。
また，隣接する銅箔との絶縁が**基礎絶縁**以下の場合は，本ガイダンス 4.2.1 章④で詳述した通り，銅箔間の短絡も検討する。
環境によって，ハンダのマイグレーション現象やウィスカなどに特別な注意が必要となる。
【参考：**安全**規格に関しては，UL796 シリーズがある】

➢ スイッチ類

圧力スイッチの規格に適合する接点以外は，スイッチ接点が閉じないことは**単一故障状態**として検討する。
強制乖離スイッチの規格に適合する接点以外は，スイッチ接点が開かないことを**単一故障状態**として検討する。
その他のスイッチ類は，該当規格に適合していない場合は，隣接する接点間の短絡や，可動接点と 2 つの固定接点の短絡，及びすべての端子の短絡，開放を考慮する。
【参考規格；IEC 60947-5-1， IEC 60947-5-5】

➢ リレー・コンタクタ類

電磁力で接点を開閉するスイッチ類の場合，接点が閉じないことと，接点が開かないことを**単一故障状態**として検討する。該当規格に適合しない場合は，可動接点と 2 つの固定接点の短絡，2 組の接点間の短絡や接点とコイル端子の短絡も検討する。
【参考規格：IEC 61810-3】

- サーミスタ

温度検知機能の**故障**により受容できない**リスク**を生じる場合，短絡，開放を検討する。**故障**がもたらす**リスク**が非常に高い場合は，抵抗値の倍(200%)や半分(50%)への変化も考慮する必要がある。

- 近接スイッチ

出力が高く，あるいは，低くなったままの状態を**単一故障状態**として検討する。更に，供給電源の遮断や，動作不良，可動接点と 2 つの固定接点の短絡も検討する。

- ソレノイド/ソレノイドバルブ

コイルの断線による不作動や励磁継続状態。軸の固着・拘束。バルブであれば閉じないことや開かないことにつながる単一の**故障**状態及び**異常**状態を検討する。
モータ類同様，可動部の意図しない危険な動作を引き起こすのは勿論，コイル部分からの発熱や発火に関する受容できない**リスク**も分析する必要がある。

- コイル類

短絡やインダクタンスの半減及び定格の最大値への変動を**単一故障状態**として検討する。ただし，アキシャルコアに単層の巻き線や，絶縁や含侵されている場合は開放のみ考慮する場合もある。

- ネットワーク抵抗

開放，全端子並びに各 2 端子間の短絡を**単一故障状態**として検討する。抵抗の構造によっては，抵抗値の半減や倍増の検討も必要になる。

- ポテンショメータ

各端子の開放，全端子間のならびに各 2 端子間の短絡を**単一故障状態**として検討する。抵抗の構造によっては，抵抗値の半減や倍増の検討も必要になる。

- 外部入出力端子

ユーザがアクセスできる外部端子がある場合には，導電物質の侵入・付着により誤って短絡した場合を考慮する。また，指定外の周辺機器などの過負荷を接続される可能性について考慮する必要がある。

- 部品の保持方法

ロボット介護機器の部品／部分の機械的な固定の**故障**により受容できない**リスク**が生じる可能性がある。

以下は，**単一故障状態**にあたる。

- 固定用のビスの 1 本が緩む
- 接着剤がはがれる（寿命と**信頼性**を証明できる場合を除く）
- 摩擦による接合が外れる（爪などの機械的な外れ防止がある場合を除く）

➢ 交換可能なバッテリ・補給品など

ユーザによって交換可能なバッテリなどの補給品が，逆接続，短絡，異品交換などされることにより受容できない**リスク**が生じる場合は**単一故障状態**に当たる。

➢ 外部の好ましくない事象

ロボット介護機器の部品の**故障**分析の条件として，製品ライフサイクル中に予見されるストレスを考慮する。

静的負荷，動的負荷，振動，衝撃及び圧力の負荷などのメカニカルストレス，基本動作及び非定常時の扱われ方，温度，化学的作用，環境ストレスなどの**ロボット**が晒される外的環境も考慮する。これらは，部品の構造やその材料の性質により，過度のたわみ，塑性変形，延性又は脆性破壊，疲労破壊，不安定（座屈），応力腐食割れ，磨耗，材料のクリープ，材料の劣化などが考**えら**れるからである。

また，製造**プロセス**におけるストレス，例えば，機械加工，組立，溶接，熱処理又は表面処理に起因する残留応力などによる脆弱性が誘引する**故障**が使用中に顕在化するかも知れない。

4.2.2 ハードウェア偶発故障への対応策

① 設計仕様書

ロボット介護機器に必要な機能を実現する回路ブロックが検討され，機能ブロック図が作成され，いくつかの機能ブロックが組み合わされて 1 枚の基板に搭載される。ここでは，これらの機能ブロックがどのような**障害**状態に至った時に，**ロボット**介護機器が危険な状態になるのか。**システム**の弱点を分析し，設計の時点で可能な範囲で**保護方策**を検討しておく。

設計仕様書は，各社各様であるが，**検証**は設計仕様の複雑さに対し指数関数的に増大するため，同一の仕様書内であっても，**検証**対象は明確に区分し，できるだけ単純化する方が良い。見やすさのため，**安全**に関する要求事項に特化した，**安全**要求仕様書を作成することもある。この方が第三者への説明に都合が良い場合もあるが，それほど複雑でなければその必要性は薄い。

開発が進むにつれ，仕様書の内容は必要に応じ修正・追加され，これらの仕様が今後進める**故障**解析の基本となる。

② 検証仕様書

検証仕様書には，設計仕様を満足することを確認するために必要な**検証**項目，**検証**方法，適合・不適合の判定基準を示す。もし，**検証**のために特別な設備が必要であれば，それらの内容と要件も記載しておくとよい。**検証**仕様書は，設計仕様書の一部をなしていても個別であってもよい。

③ テストプログラム

検証は原則的に設計者から独立した組織で行う。このため，簡単な**検証**の場合は，**検証**仕様書をそのまま用いることができるが，そうでない場合は，テストプログラムを作成する。
検証の順番，**検証**方法，測定器の選定など，**検証**仕様書以外の詳細が，正しい**検証**結果を得るために必要な場合がある。テストプログラムには，試験環境や試験要員の資質，あるいは，特殊な**検証**試験の場合は，試験や結果の項目を網羅した試験報告書の様式も含むことがある。

④ 試験報告書

報告書には，試験結果以外にも，試験結果の再現を担保するに必要な情報を盛り込む必要がある。

- 試験日
- 試験者
- 試験サイト
- 温度，湿度，必要ならば，気圧
- 入力電圧条件
- 試験に用いた測定器（用いた測定器を特定できる情報を含み，測定器は校正され標準器への**トレーサビリティ**が確保されていること）
- 試験品を特定できる情報（必要があれば，試験品に組み込まれたソフトウェアの**バージョン**を含む）

尚，試験の合否判定は，設計仕様書や**検証**仕様書に基づいて行われる。原則的には，試験員は試験結果の合否判定を行わず試験結果を**記録**するだけである。これにより，試験部門と判定部門の独立性が確保される。

⑤ 故障解析手法

システムの弱点や問題点を検討する手法の一つに「**故障**の木解析」(FTA: Fault Tree Analysis)（以下「FTA」と記述）がある。FTA では，**ロボット**介護機器の好ましくない事象（落とす・衝突するなど）をあらかじめ想定し，そのような事象に至る道筋を，もし定量的な解析が必要であれば発生確率とともに分析を進める。分析は，好ましくない事象（上位）からその原因（下位）へと進める。機能不良の発生確率が必要であれば，それをつかさどる部分の**故障**解析をして求めることができる。
例えば，**ロボット**介護機器が，何かを「落とす」という事象を起こす場合，その原因となる事象が「アームの破損」や「把持力低下」にある場合，それを図にしたものを FTA 図と呼び，以下のようになる。

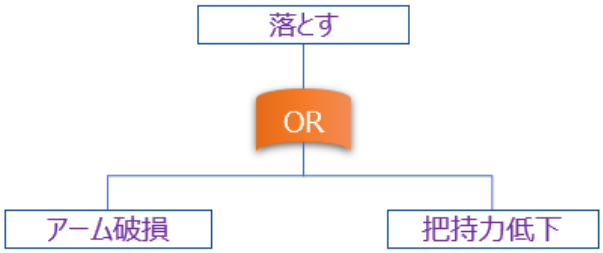


図 4-13 FTA 図 例 1

更に，「アームの破損」の原因が「強度不足」や「**誤使用**」にあり，「把持力低下」の原因が「間違ったトルク指令」や「把持バネ破損」にある場合は，それらを追加して，FTA は以下のようになる。

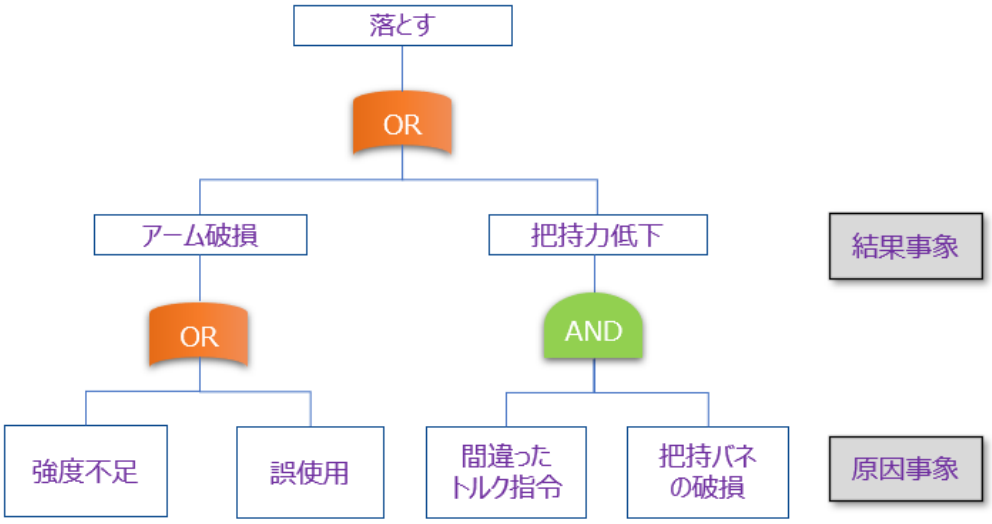


図 4-14 FTA 図 例 2

同様の作業を深堀していくと，最終事象の原因を求めるとともに，どの部分を変更することが最も合理的な対応になるかを検討できる。この例では，「間違ったトルク指令」と「把持バネ破損」が AND 論理で接続している。このように原因事象が AND 論理で結合された場合は，そこにつながる原因事象の一つでも生じなければその結果事象は生じないので，いくつかの原因事象のうち一番対応しやすい事象に対処することで，対策できることになる。原因事象が OR 論理で接続している場合は，どれか一つの原因事象がその結果事象を起こすことになるので，すべての原因事象への対応が必要になる。このようにして，**危険事象**に関してその原因を追究していき，必要な対応を取ることにより，合理的で効果的な対策が期待できるとともに，第三者に対しても説明しやすくもなる。

大きな**システム**の場合は，一つの機能を更に小ブロックに分け，一つのブロックを単純化して解析しやすくできる。例えば，入力部，論理処理部，出力部のように分けることもできるし，温度検出，速度検出，電流検出のように機能別に分けることも可能である。これらのブロックの合理的配置を検討するのが，第 2 章で述べた V-モデル開発における**アーキテクチャ**設計にあたる。

アーキテクチャがはっきりしてくると，分割された各ブロックはその機能を実現するために具体化され回路構成が決まってくる。各ブロックの回路構成が決まり，入力や内部**故障**の出力に対する影響からブロックの挙動が分かると，ブロックへのどのような入力や内部**故障**が**危険事象**を起こすかが分かってくる。センサ

やデバイスに市販品を用いる場合は，その仕様を詳細に理解し，入力や内部**故障**の出力に対する影響からブロックの挙動を求める。ここまでくると，先に述べた FTA の手法による，より実際の回路や構造に即した**故障**解析が可能になる。その結果，場合によっては，いくつかのブロックの設計変更が必要になるかもしれないし，**アーキテクチャ**設計の見直しの必要があるかもしれない。そして，更に FTA による解析を繰り返し最終形へと近づく。

この規格は，必ずしも**故障**確率を求めることは要求していないが，**高信頼性部品**を採用した場合など，**ロボット**介護機器の**予測耐用期間**に対して**危険側故障**が十分に低いことを示す必要が出てくることがある。FTA 分析で，原因事象の発生確率を求めて，最終的な**危険事象**の発生確率を推測することが可能なので，もし，各ブロックの**故障**確率が分かっていれば，PESS の**故障**確率を計算できる。

しかしながら，FTA で求めた原因事象となるブロックが内製部品などの場合で，**故障率**が分からない場合や，**高信頼性部品**を用いたブロックの**故障率**が分からない場合がある。この場合，そのブロックの**故障**確率を「**故障**モード**影響解析**」（**FMEA**: Failure Mode and Effect Analysis）（以下 **FMEA** と記述）で推定することができる。FTA では，ブロック毎にその**故障**モードと**故障**の影響を解析して**安全機能**喪失の確率を推定し，必要な防護処置を検討する方法を例示したが，**FMEA** では，部品単位でその**故障**モードと**故障**の影響を解析し，構成する部品の**故障**確率から，上位**システム**の**障害**確率を求め，最終的に**安全機能**の喪失確率を推定することもできる。表-4.1 に単純化した **FMEA** シートの例を示す。

表 4-4 FMEA シートの例

番号	部品 ID	**故障**確率（fit）	**故障**モード	症状	**故障**検出	1. **故障**確率(fit)	
						安全側	危険側
1	R1	0.03	短絡	出力が 1 にスタック	可		0.015
			開放	出力が 0 にスタック	可	0.015	
2	C1	0.06	短絡	出力が 1 にスタック	可		0.04
			開放	出力が 0 にスタック	不可	0.02	

記載の順序は，以下のようになる。

1）**故障**を起こす部品の**故障**確率をメーカーデータなどから求める。メーカーデータを入手できない場合は，実績のあるデータベースの値を参照することもできる。**故障率**が部品の使われ方により異なる場合もあるので，実際の使用状態に近い値を求める。

【参考】部品の**故障率**データベースとして，SN 29500 シリーズや IEC/TR 62380 がある。

2）解析すべき部品の**故障**モードを決める。通常は，例えば，抵抗なら開放と短絡でよいが，対象とする**リスク**が大きい場合は，抵抗値の増減も考慮する。

3）場合によっては，**故障**モード毎の確率を示したデータもあるので，その場合は，**故障**モードに対して該当する**故障率**を当てはめる。**故障**モード毎のデータがない場合は，**故障率**を各モードに按分する。

【参考】IEC 62061 の附属書 D に，部品の**故障**モードの記載がある。

4）各**故障**が起きた結果，**評価**対象物（最終的には**ロボット**介護機器）がどのような状態になるかを記載する。結果が明らかな場合は，机上推定でも記載できるが，不確実な場合は，実際の**故障**を模擬実験してその結果を記載する。

5）生じた**故障**を何らかの形で検出できるかできないかを記載する。検出できない**故障**は潜在する。この場合は，更なる**故障**の影響を検討する必要がある。

6）設計仕様書に従い，**危険側故障**になるか否かを判断し，該当する**故障率**を記載する。

7）これらの作業を関係する部品すべてに関して行う。**危険側故障**により**リスク**が受容できるレベルを超えなければ，**単一故障安全**が達成されたことになる。

ハザード	危険状態	危害	危害の重大さ	発生確率
重力エネルギ	意図しないアシストトルクにより転倒	上腕の骨折	重大な	起こりそうにない

発生確率	確　率	無視できる	軽微な	きわどい	重大な	破局的（死亡）
頻繁	$> 10^{-3}$	受容不可	受容不可	受容不可	受容不可	受容不可
可能性が高い	$10^{-3} < 10^{-4}$	受容不可	受容不可	受容不可	受容不可	受容不可
時々	$10^{-4} < 10^{-5}$	受容可能	受容可能	受容不可	受容不可	受容不可
僅かに	$10^{-5} < 10^{-6}$	受容可能	受容可能	受容不可	受容不可	受容不可
起こりそうにない	$< 10^{-6}$	受容可能	受容可能	受容可能	受容可能	受容可能

R001

図 4-15　ISO 14971:2007 附属書 D で示されている確率レベルと評価基準の例

検出できる**故障**は直ちに対処されるとすれば，検出されない**危険側故障**の**故障**確率の総和が，**評価**対象ブロックが危険な状態を起こす確率になる。この**評価**対象ブロックを，**高信頼性部品**と捉えるならば，この**故障**確率が，**ロボット**介護機器の**予測耐用期間**中にこの規格の**安全**要求事項について機能を失わないことが確実であると見なせる場合は，規格に適合すると考えることができる。

例示した **FMEA** シートは簡略化されているが，一般的には，表計算ソフトを用いて，**故障率**とその比

率を入力して自動計算するなど，自社に合うシートを作る事が多い。

⑥ 対応策

単一故障安全を達成できない場合の対応策は，**ロボット**介護機器毎に最適な方法を選択すべきだ。対策には大別すると，壊れにくくする方法と，どうせ壊れてしまうのだったらさっさと壊してしまう方法がある。以前の我が国の電気製品は，とにかく丈夫に壊れにくく作ったため，何十年もしてから危険な状態になることがあり，2002 年に「長期使用製品**安全**表示制度」が制定された。これは，使用者にその製品の設計寿命を知らせることにより，点検や交換を即し事故を防ごうとするものである。このような背景から，昨今は「いかに**安全**に壊すか」といった観点から設計している製造事業者も出てきている。対応策は，例えば:

保護装置を設ける：従来から代表的な対策といえる。例えば，過電流保護のヒューズがある。
過電流などの**危険状態**を検出して（**保護接地端子**を通じてアースに流すことで）電力を遮断し，介助者，ユーザに明確に**故障**である事が識別できる状態にする。
又は，ディスプレイの**異常**表示，警報，警告装置，筐体の変形，大きな騒音や擦れによる使用困難などは認識の程度が異なるため**リスクアセスメント**で対策の妥当性を**評価**される必要がある。
またヒューズも広く捉えるなら，以下に述べる**故障**検出や**故障**診断の一つにも含まれる。

故障診断を設ける：電流や電圧，温度，振動，信号などを**監視**し，閾値を超えたら**ロボット**介護機器を**安全**状態へ移行させる処置を取る。

冗長化する：回路を 2 重化するなどして，一つの開路が**故障**しても残りの回路が機能して**安全**を確保する。同じ回路で多重化する単純冗長の場合，ハードウェアの**偶発的な故障**には対応できるが，**系統的な故障**には対処できない。それに対し，異なる方式を用いる**多様性**による多重化は，**系統的な故障**にも対応できる。

定期点検：どのような対応も取れない場合は，定期点検で**故障**を発見し修復することになる。
ロボット介護機器の場合，停止させることが可能で停止状態で点検を行うことは容易だが，もし連続稼働する場合は，点検中の**安全**確保に注意が必要になる。
定期点検の期間は，その間の**危険側故障**確率が十分に低くなるように設定する必要がある。

4.2.5 単一故障状態試験のためのガイダンス

① 一般

単一故障状態は，結果次第では危険を伴うため，試験員の**安全**確保には十分注意する必要がある。最低限，保護メガネの着用や，燃焼を伴う試験の場合，排煙設備や消火器の準備など必要になる。また，**単一故障状態**は，**正常状態**との最も不利な組み合わせで行う必要がある。例えば，使用環境での電源電圧範囲が変動（±10%など）したり，バッテリの状態が変化するのであれば，その範囲の最も厳しい条件を考慮したり，消費電力負荷の影響を検討する必要がある。この規格の箇条 5.3 ～箇条 5.6 には，試験を行う際の一般的な環境条件に関する要求がある。

基本的には，電源を入れて安定した状態で，短絡や開放を行うが，場合によっては，短絡や開放を行った状態で電源を投入することになるかもしれない。その他，ハンドルを切った状態や，単一**異常**状態を起こした状態でハンドルを切ることが必要かもしれない。いずれにせよ，回路を読みながら最も不利な状態で行うことになる。

短絡試験は，対象物の端子にリード線をつなぎ，スイッチを用いて短絡することになる。短絡によりその回路につながった容量性部品からの放電により瞬間的に大電流が流れることがよくあるので，太いリード線をできるだけ短く使い，大容量接点のスイッチを用いて行う。この事は，リード線やスイッチなど短絡回路のインピーダンスを低くすることにより試験結果への影響が減り，試験結果が安定することにもなる。

開放試験は，回路の途中を，場合によっては銅箔を切ることで開放し，そこにリード線とスイッチをつなぎ，スイッチを閉じた状態で電源を入れるなど，試験前の安定状態にし，その後スイッチを開いて状態を観察する。この場合も，開放回路の閉路時のインピーダンスが高いと，開放前から発振を起こすなどして，試験結果に影響することがある。

安全機能の確認がこの文書の目的であるが，場合によっては，温度測定が必要になるかもしれない。どのような温度計を用いるかは規格には規定されていないが，一般的には，熱電対を用いて測定している。巻き線温度に関しては，一般的には，抵抗法を用いて測定するが，被測定物の特性によっては，熱電対で測定することもある。放射温度計を使って測定もできるが，常に測定誤差を念頭に置き，規格への適合を判断すべきである。常に「何のために測定しているか」という目的を意識し，適切な測定法を選定すべきである。

【参考】この規格の箇条 11 には機器の過度の温度測定方法，箇条 13 には機器の**危険状態**及び**故障**状態の試験方法の記載がある。

② 部品毎の故障注入方法

➢ 抵抗の**故障**

短絡や開放は既に述べたように行う。抵抗値の変更の模擬は，動作中に抵抗値がいきなり変化することは考えにくいので，同種類で異なる値の抵抗に取り換えて，動作を確認することになる。**安全機能**の確認を行うので，影響が及ぶと思われる機能が正常に発揮できることを観察する。

➢ コンデンサの**故障**

短絡や開放は既に述べたように行う。大容量のコンデンサの短絡は，大きな放電電流を伴うので注意が必要になる。アルミ電解コンデンサやフィルムコンデンサなどコンデンサの種類によっては，部分的に絶縁破壊が起こり，中途半端に短絡する場合がある。更に経年劣化による容量抜けが生じる種類もあるので，用いられる場所によっては，検討が必要になるかもしれない。

➢ 半導体類の**故障**

短絡や開放は既に述べたように行う。通常は，平常使用状態で試験する。

➢ 絶縁の**故障**

絶縁に関しては，先に述べた，絶縁部分の短絡を行う。基本的な考えは，**基礎絶縁**の短絡と機械的なストレスがかかる絶縁物の短絡になるが，絶縁物には機械的なストレスをかけないように設計することが大前提である。

機能絶縁であっても，**安全機能**の低下をもたらす可能性がある場合は，短絡する。ただし，この規格に規定される最小**沿面距離**及び**空間距離**を満たす場合を除く。

➢ トランスの**故障**

変圧器（トランス）に関しては，**単一故障状態**における過熱と絶縁破壊の結果としての火災や感電が主になる。それらは，**ロボット**介護機器の一つの部品として**評価**してもよいが，規格適合品を用いることでいくつかの試験を回避できるだろう。**安全機能**に関しては，電源遮断などの**共通原因故障**として影響する場合が多い。

➢ サーモスタットの**故障**

「サーモスタット」と聞くと水冷エンジンのラジェータキャップを思い出すかもしれないが，この規格で言う「サーモスタット」とは，広く「温調器」を指している。サーモスタットには，数種類の動作原理があり，各々**故障**が異なるためこの規格では，「短絡又は開放のいずれか好ましくない方」で試験することになっている。トリップ特性によっては，**故障**が検出できない場合があるので，その場合，更なる**故障**を含めた**検証**をする必要があるので，注意を要する。また，一度過昇温度を検知してトリップ（電力遮断など）した後，温度が常温に戻ると，トリップが解除され，再び電力が供給されてしまう可逆性のある部品もあるので，そ

の振る舞いには注意が必要である。

- 温度制限器の**故障**

このような制限器の場合は，過負荷状態を模擬し，短絡や開放の試験を行う。温度ヒューズのように，該当規格に適合し，その動作が信頼できる場合は，試験対象から外すことができる。

- 冷却**システム**の**故障**

冷却**システム**の**故障**が**安全機能**に影響することはあまりないと思われるが，もし懸念される場合は以下のように行う。

・ 冷却ファンを停止させる（複数のファンを有する場合は，一つずつ停止させる）
・ 放熱用の開口部の上面は塞ぐ，側面は壁に近づける
・ フィルタの目詰まりを模擬して塞ぐ
・ 冷媒の流れを止める

③ 判定方法

単一故障状態の概念は以下の考慮を行うものによる。

(1) 最初の**故障**は常に起こりうる。と考える。したがって，最初の**故障**は危険なものであってはならない。

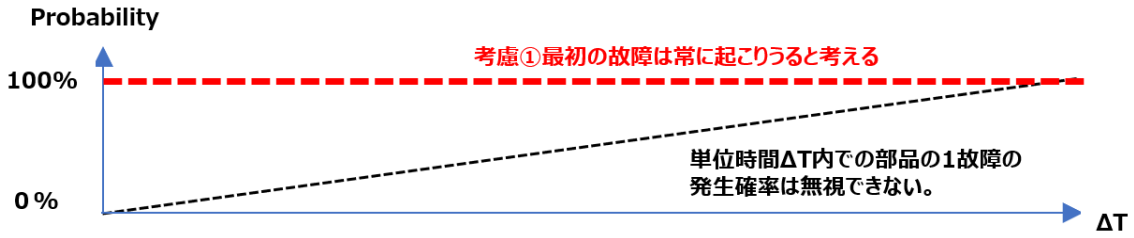


図 4-16 最初の故障の発生確率の考え方

最初の**故障**が目に見えるものであるならば（例：警報がなる。電源遮断で起動しない。）
その機器がそれ以上使われず，修理されると見込むことができる ➔ **故障**分析の終了 【結果･･･適合】

(2) 最初の**故障**が検知可能でないと，その**故障**は潜在し，機器はそのまま使用されることを考慮する。２つ目の**故障**や**危険事象**はすぐには起こらないが（ただし，**従属故障**は除く），ある程度の時間がたってから，起こることも場合によっては想定しなければならない。
したがって，このケースでの２つ目の**故障**は危険なものであってはならない（**安全**状態が維持できなければならない。）。

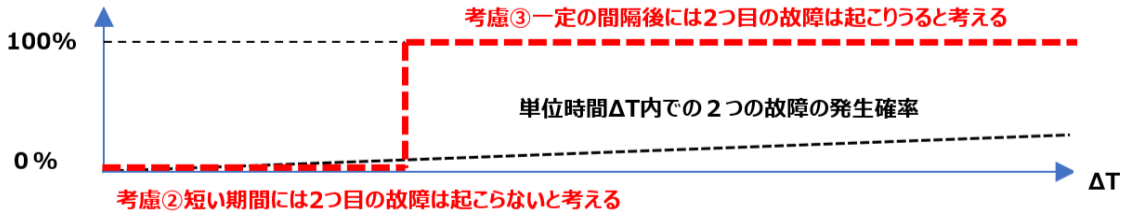


図 4-17 ２つ目の故障の発生確率の考え方

(3) 原則，この規格の**単一故障安全**では，**予測耐用期間**中の３つ目の独立した**故障**の発生は稀と考える。

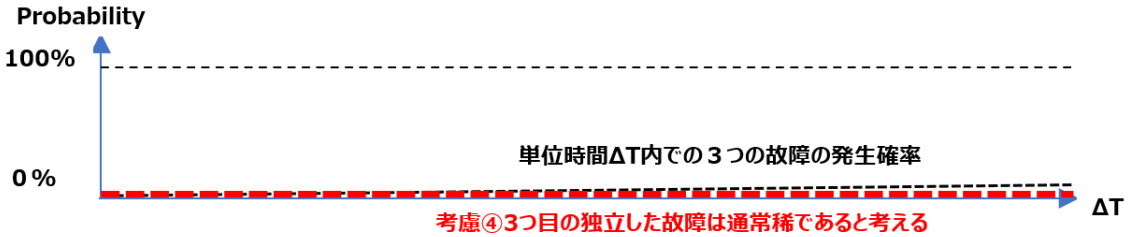


図 4-18 ３つ目の故障の発生確率の考え方

リスクが非常に高い，又は部品にとって条件が悪い場合には，特段に考慮する場合があるので注意が必要となる。以上が電気**安全**も含めた**単一故障安全**での考慮すべき**故障**の扱いである。ただし，**危険**

事象への**プロセス**が複雑な **PEMS** の場合，前述の（１）までの振る舞いで歯止めがかかるように適切な**アーキテクチャ**が **PEMS 開発ライフサイクル**の中で考慮されることが望ましいと考える。
図 4-19 は，前頁のページ示した**単一故障安全**の概念に応じた判定フローである。

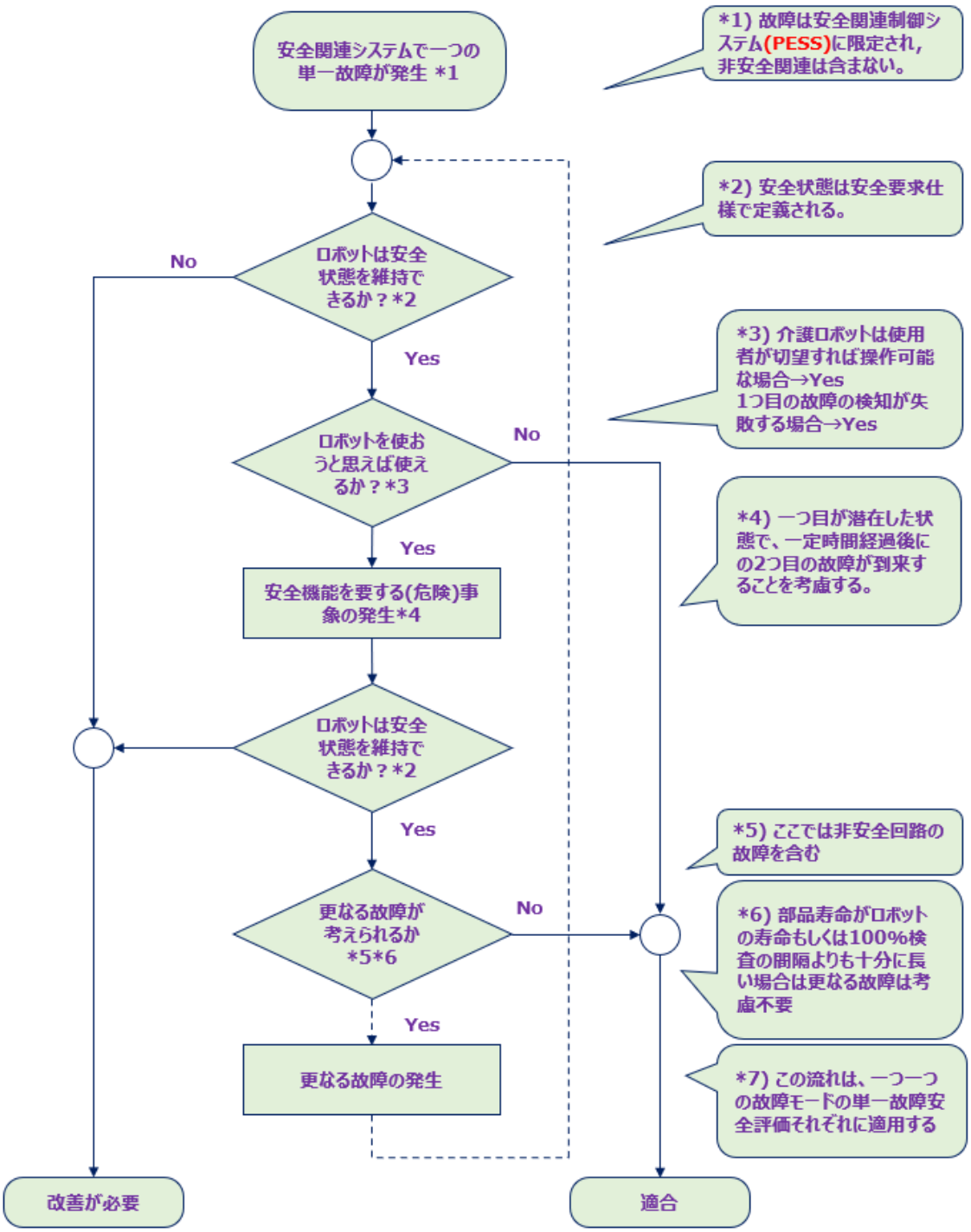


図 4-19 単一故障安全評価の流れ

4.2.6 CPU/MPU 関連の故障への対応

この規格では，CPU や MPU あるいはその周辺機器などの**故障**への対応は，**単一故障安全**の実現が要求されるだけで，その手法などの記載は無いため，製造事業者自らが対策の妥当性を示す必要がある。昨今の CPU や MPU などの集積回路は複雑度が増すにつれ**フォールト**モデル及びテストケースの特定がより難しくなってきている。そのため**フォールト**モデルに対して意味のある内部診断技法及び抑制方策を実装することで，**故障**を回避・抑制することが期待できる。そこで，参考になる情報を記述する。数多くの対応技術が考**えら**れるが，他のハードウェア同様，より高い**リスク**の制御に用いる場合は，より確実な（診断率の高い）**故障**や**エラー**への対策が必要になる。以下は，一般的に想定される，CPU や MPU の**故障**とその対策で，制御対象の**リスク**が低いか高いかに分けて考慮すべき**故障**とその対応策を述べる。ここでは，高**リスク**の場合，CPU の冗長使用が前提になっている。この表は，IEC 60335-1（：家庭用及びこれに類する電気機器の**安全**性－第 1 部：通則）の記述をもとに作成した。

【参考】 IEC 61508-2 の附属書 A にも要求**診断カバー率**を達成するためのハードウェア**故障**を管理する技法及び手段で検出しなければならない**フォールト**又は**故障**の要求事項に関する情報が示されている。

表 7.1 CPU や MPU 関連の一般的な故障/エラー状態

部品/機能		考慮すべき**故障**		必要な対策
		低**リスク**	高**リスク**	
CPU/MPU	レジスタ	縮退		機能試験，もしくは， 以下のいずれかによる定期的自己テスト ・ 静的メモリ試験 ・ 単一ビット**冗長性**によるワード保護
			DC **故障**	以下のいずれかによる冗長 CPU の比較 ・ 相互交換比較 ・ 独立したハードウェアによる比較器，もしくは内部**エラー**検出，もしくは冗長メモリの比較，もしくは 以下のいずれかによる定期的自己テスト ・ ウォークパットメモリテスト ・ アブラハムテスト ・ 透過性ガルパットテスト，もしくは 多重ビット**冗長性**によるワードの保護，もしくは 静的メモリテストと単一冗長ビットによるワード保護

表 7.1 （続き）CPU や MPU 関連の一般的な故障/エラー状態

部品/機能		考慮すべき**故障**		必要な対策
		低**リスク**	高**リスク**	
	命令の復号と実行		復号や実行の間違い	以下のいずれかによる冗長 CPU の比較 ・ 相互交換比較 ・ 独立したハードウェアによる比較器， もしくは 内部**エラー**検出，もしくは 等価性クラス試験を用いた定期的自己テスト
	プログラム・カウンタ	縮退		機能試験，もしくは 定期的自己テスト，もしくは 独立したタイムスロット**監視**，もしくは プログラムシーケンスの論理的**監視**
			DC **故障**	以下のいずれかによる定期的自己テストと**監視** ・ 独立したタイムスロットと論理的**監視** ・ 内部**エラー**検出，もしくは 以下のいずれかによる冗長化された機能チャンネルの比較 ・ 相互交換比較 ・ 独立したハードウェアによる比較器
	アドレス指定		DC **故障**	以下のいずれかによる冗長 CPU の比較 ・ 相互交換比較 ・ 独立したハードウェアによる比較器， もしくは 内部**エラー**検出，もしくは 以下のいずれかによる定期的自己テスト ・ アドレス線のテスト用パターン ・ 全バス冗長 ・ アドレスを含むマルチビットバスパリティ
	データ経路命令複合		DC **故障**および実行	以下のいずれかによる冗長 CPU の比較 ・ 相互交換比較， ・ 独立したハードウェアによる比較器 ・ 内部**エラー**検出 ・ 試験パターンを用いた定期的自己テスト ・ 冗長データ ・ マルチビットバスパリティ

表 7.1 （続き）CPU や MPU 関連の一般的な故障/エラー状態

部品/機能		考慮すべき**故障**		必要な対策
		低リスク	**高リスク**	
割込みの取り扱いと実行		割り込みしないか，頻繁な割り込み		機能テスト，もしくは タイムスロット**監視**
			割り込み無しや，異なる原因によるあまりにも頻繁な割り込み	以下のいずれかによる冗長化された機能チャンネルの比較 ・ 相互交換比較 ・ 独立したハードウェアによる比較器 ・ 独立したタイムスロットと論理的**監視**
クロック		間違った周波数（水晶同期のクロックに関しては，高調波，副高調波だけ）		周波数**監視**，もしくは タイムスロット**監視**
			間違った周波数（水晶同期のクロックに関しては，高調波，副高調波だけ）	周波数**監視**，もしくは タイムスロット**監視**，もしくは 以下のいずれかによる冗長化された機能チャンネルの比較 ・ 相互交換比較 ・ 独立したハードウェアによる比較器

表 7.1 （続き）CPU や MPU 関連の一般的な故障/エラー状態

部品/機能		考慮すべき**故障**		必要な対策
		低**リスク**	高**リスク**	
メモリ	不変メモリ	いずれか 1 ビットの**故障**		定期的な変形チェックサム，もしくは 定期的な多重チェックサム，もそくは 単一ビット**冗長性**によるワードの保護
			全ての情報に関する**エラー**の 99.6 % をカバー	以下のいずれかによる冗長 CPU の比較 ・ 相互交換比較 ・ 独立したハードウェアによる比較器， もしくは 冗長メモリの比較，もしくは 以下のいずれかによる定期的 CRC ・ 単一ワード ・ 二重ワード ，もしくは マルチビット冗長によるワード保護
	可変メモリ	DC **故障**		定期的な静的メモリテスト，もしくは 単一ビット**冗長性**によるワードの保護
			DC **故障**および動的クロスリンク	以下のいずれかによる冗長 CPU の比較 ・ 相互交換比較 ・ 独立したハードウェアによる比較器， もしくは 冗長メモリの比較，もしくは 以下のいずれかによる定期的自己テスト ・ ウォークパットメモリテスト ・ アブラハム試験 ・ 透過性ガルパット試験，もしくは マルチビット冗長によるワードの保護

表 7.1 （続き）CPU や MPU 関連の一般的な故障/エラー状態

部品/機能		考慮すべき**故障**		必要な対策
		低**リスク**	高**リスク**	
	不変メモリや可変メモリのアドレス指定	縮退		アドレスを含む単一ビット**冗長性**によるワードの保護
			DC **故障**	以下のいずれかによる冗長 CPU の比較 ・ 相互交換比較 ・ 独立したハードウェアによる比較器， もしくは 全バス**冗長性**，もしくは 試験用パターン，もしくは 以下のいずれかによる定期的 CRC ・ 単一ワード ・ 二重ワード ，もしくは アドレスを含むマルチビット冗長によるワードの保護
内部通信	内部データパス	縮退		単一ビット**冗長性**によるワードの保護
			DC **故障**	以下のいずれかによる冗長 CPU の比較 ・ 相互交換比較 ・ 独立したハードウェアによる比較器， もしくは アドレスを含むマルチビット冗長によるワードの保護，もしくは 冗長データ，もしくは 試験用パターン，もしくは プロトコル試験
	アドレス指定	間違ったアドレス		アドレスを含む単一ビット**冗長性**によるワードの保護
			間違ったアドレス指定や多重アドレス指定	以下のいずれかによる冗長 CPU の比較 ・ 相互交換比較 ・ 独立したハードウェアによる比較器， もしくは アドレスを含むマルチビット冗長によるワードの保護，もしくは 全バス**冗長性**，もしくは アドレスを含む試験用パターン

表 7.1 （続き）CPU や MPU 関連の一般的な故障/エラー状態

部品/機能		考慮すべき**故障**		必要な対策
		低リスク	**高リスク**	
外部通信		ハミング距離 3		多重ビット**冗長性**によるワードの保護，もしくは CRC – 単一ワード，もしくは 転送**冗長性**，もしくは プロトコル試験
			ハミング距離 4	CRC－二重ワード，もしくは データ**冗長性**，もしくは 以下のいずれかによる冗長化した機能チャンネルの比較 ・ 相互交換比較 ・ 独立したハードウェアの比較器
	アドレス指定	アドレス間違い		アドレスを含むマルチビット冗長によるワード保護，もしくは アドレスを含む CRC－単一ワード，もしくは 転送**冗長性**，もしくは プロトコル試験
			アドレス間違いや，複数のアドレス指定	アドレスを含む CRC－二重ワード，もしくは データおよびアドレスの全バス**冗長性**，もしくは 以下のいずれかによる冗長通信チャンネルの比較 ・ 相互交換比較 ・ 独立したハードウェアの比較器
	タイミング	タイミング間違い		タイムスロット**監視**，もしくは 計画的送信，もしくは タイムスロット及び論理的モニタ，もしくは 以下のいずれかによる冗長通信チャンネルの比較 ・ 繰り返し比較 ・ 独立したハードウェアの比較器
			タイミング間違い	タイムスロット**監視**，もしくは 計画的送信
		間違った順序		論理**監視**，もしくは タイムスロット**監視**，もしくは 計画的送信

表 7.1 （続き）CPU や MPU 関連の一般的な故障/エラー状態

部品/機能		考慮すべき**故障**		必要な対策
		低**リスク**	高**リスク**	
入出力	デジタル I/O	単一**故障**		**信頼性**試験
			単一**故障**	以下のいずれかによる冗長 CPU の比較 ・ 相互交換比較 ・ 独立したハードウェアの比較器， もしくは 入力比較，もしくは 多重並列出力，もしくは 試験用パターン，もしくは コードの**安全**性
	A/D，D/A コンバータ	単一**故障**		**信頼性**試験
			単一**故障**	以下のいずれかによる冗長 CPU の比較 ・ 相互交換比較 ・ 独立したハードウェアの比較器， もしくは 入力比較，もしくは 多重並列出力，もしくは 出力**検証**，もしくは 試験用パターン
	アナログマルチプレクサ	間違ったアドレス指定		**信頼性**試験
			間違ったアドレス指定	以下のいずれかによる冗長 CPU の比較 ・ 相互交換比較 ・ 独立したハードウェアの比較器， もしくは 入力比較，もしくは 試験用パターン，
監視用デバイスや比較器			機能仕様外の全ての静的並びに動的出力	試験済み**監視**，もしくは 冗長**監視**及び比較，もしくは **エラー**認識手段

表 7.1 （続き）CPU や MPU 関連の一般的な故障/エラー状態

部品/機能		考慮すべき**故障**		必要な対策
		低リスク	**高リスク**	
ASIC，ゲートアレイ，など		機能仕様外の全ての静的並びに動的な出力		定期的な自己チェック
			機能仕様外の全ての静的並びに動的な出力	定期的自己テスト，もしくは **多様性**による冗長チャンネル間の比較，もくしは **エラー**認識方策

4.3 電磁ノイズ耐性の要求（IEC 60601-1-2)

ロボット介護機器に適用できる福祉機器の通則 ISO 21856 では Electromagnetic compatibility
の要求として以下の内容が言及されている。

Clause 7 Electromagnetic compatibility Assistive products containing electrical or electronic devices/components shall comply with requirements of IEC 60601-1-2: 2014. （参考和訳） 箇条 7 電磁両立性 電気または電子機器/コンポーネントを含む支援製品は，IEC 60601-1-2:2014 の要件に適合しなければならない。

Electromagnetic compatibility とは電磁両立性の事で略称 EMC と呼ばれる。EMC とは，図 4-20 に示すように，機器から発生する電磁エネルギが，その他の機器に妨害を与えない電磁干渉性（EMI： Electromagnetic interference）と，他の機器からの電磁エネルギによって妨害を受けない能力である電磁感受性（EMS： Electromagnetic susceptibility)の 2 つを満たす要求である。**ロボット**介護機器では両方の要求を満たす必要があるが，このガイダンスでは**機能安全**に関連する EMS のみについて解説をする。

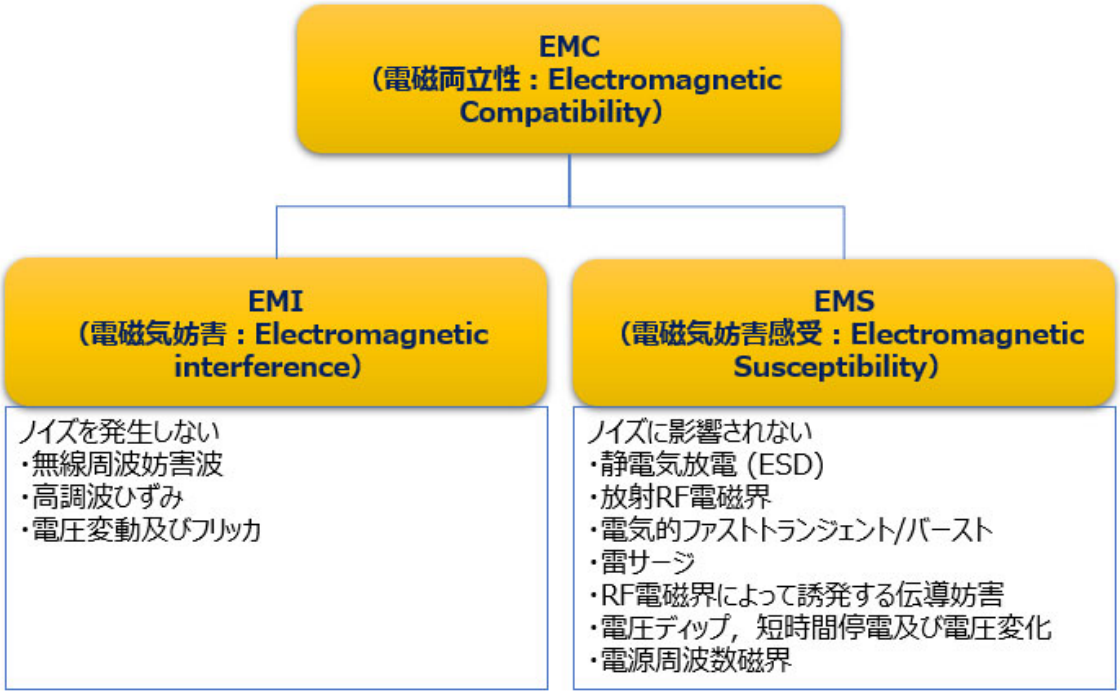


図 4-20 電磁両立性の関係

ロボット介護機器は，いざという時に正常に**安全機能**が作動しなければならない。
機器は様々な機能を実現するために多数の電子回路を内蔵している。電子回路は非電子式の回路に比べ，外来の電磁ノイズに干渉され誤動作を生じやすい。また，昨今の介護現場はスマートフォンやタブレット端末に代表される無線通信機器が導入され，公衆 Wi-Fi サービスも普及しているように，電波の利用が避けられず，これは電磁干渉の機会（**危険状態**への暴露頻度）を増大させている。このような電磁環境において，機器に到来する電磁ノイズの影響で**安全機能**の正常な作動が侵害される**リスク**を考慮しなければならない。**PEMS** 開発では，**ロボット**の使用環境の決定，適切なノイズ設計と**検証**の活動を通じて適切なイミュニティ（電磁ノイズ耐性）特性が実現される必要があり，設計配慮の漏れや**検証**の不足は，**機能安全**上では一つの**系統的な故障**と見なされる。
ISO 21856 が引用する IEC 60601-1-2 (: 医用電気機器－ 第 1-2 部：**基礎安全**及び**基本性能**に関する一般要求事項－副通則：電磁妨害－ 要求事項及び試験) は，**医療機器**に対して要求される EMC の国際規格である。欧米では介護機器は**医療機器**として扱われ，介護機器は在宅に加えて，介護施設内，病院内など様々な医療関連施設で使用されため，同様の要求が適用されることとなった。この EMC 規格の特徴は，**医療機器**に想定される電磁環境下における，必要な EMC 試験の方法を示すだけでは無く，電子制御機器の**リスク**を低減するための**リスクマネジメントプロセス**を適用している。つまり，想定電磁環境下における誤動作の**リスク**を分析し，**リスク**低減と**検証**方法を示し，多様な電磁環境下における機器の**リスクマネジメント**を行うことを求める。本章では，**医療機器**に分類される**ロボット**介護機器に適した**リスクマネジメント**ベースの EMC 設計・開発の方法についての解説を行う。

4.3.1 EMC 設計と開発

EMC 設計は，**リスクマネジメント**計画に定められた**手順**に従って行われる。

① ハザードの特定

リスクマネジメント活動の中で，最初に**ハザード**（電磁ノイズがもたらす**危害**へのシナリオ）を特定する。この規格で言う**ハザード**とは，不十分，不適切なイミュニティ（電磁ノイズ耐性）によって，「**基礎安全**（：**ME 機器**を**正常状態**及び**単一故障状態**で使用する時，物理的**ハザード**に直接起因する受容できない**リスク**がないこと。）」と，「**基本性能**（Essential Performance）（：**基礎安全**に関連する以外の臨床機能の性能において，**製造業者**の指定した限界を超えた欠如，又は低下が生じた時に受容できない**リスク**を生じさせる性能。）」を侵害する**リスク**シナリオの事である。

PEMS では，内部及び外部で多くの通信が行われているため，それらの通信**エラー**や電磁妨害によるデータ化けなどによって誤動作したり，期待していた**安全機能**が失敗したりすることの予見が必要になる。**ハザード**を特定するには，その**ロボット**介護機器が使用されるノイズ環境，基本構造や使用方法を特定し，EMC 専門家を加えた関係者が，**予測耐用期間**中の**ロボット**介護機器の電磁妨害による**ハザード**の特定を行い文書化する。図 4-21 にあるように，ISO 21856 では，**ロボット**介護機器が使用されるノイズ環境に応じた，電磁両立性の実力と，必要に応じ，処置の方法を明記することを要求している。

A.7 Electromagnetic compatibility

When specifying the EMC performance of an assistive product, manufacturers are recommended to consider the already widely established environments:

— residential, commercial and light industrial;

— industrial;

— other (typically meaning more harsh environments and some specific places such as surgical theatres or near specific machinery, e.g. transmitters).

A user should be able to use an assistive product in all the manufacturer's intended environments of use for the assistive product with the minimum of limitation. The manufacturer should make it clear in simple language when limitations exist by describing the circumstances that must be avoided and should explain the consequences of exposing the assistive product to a potentially dangerous environment, e.g. radio transmitters. If possible, any appropriate actions that will offset any hazard should be described.

（参考和訳）

支援製品の電磁両立性の実力を規定する場合，製造者は，すでに広範に確立された環境を考慮することが推奨される。

- 住宅，商業，軽工業

- 産業
- その他（一般的には，外科手術室や特定の機械(送信機など)近傍など、より過酷な環境を意味します。

ユーザは，製造者が意図した環境で，最低限の制限で支援機器を使用できるべきである。

製造業者は、回避しなければならない状況を記述することによって制限を設けるとき，簡単な言語で明確に表示しなければならない。また、無線送信機など、潜在的に危険な環境に支援製品を暴露することの結果を説明すべきである。可能であれば、あらゆる危険を相殺する適切な処置を表示すべきである。

図 4-21 ISO 21856 の附属書 A.7 電磁両立性

同様に，IEC 60601-1-2 においても，ノイズ環境の区分（**図 4-22**），基本構造の特定（図 4-23）を行い，**ロボット**介護機器の電磁妨害による**ハザード**の特定を要求する。

【機器の使用環境】

医用電気機器の**基礎安全**及び**基本性能**に対するイミュニティ試験レベルは，使用する環境に基づいて，「専門的ヘルスケア施設環境」，「ホームヘルスケア環境」，「特殊環境」に区分する。

（IEC 60601-1-2 表 5 参照）。

使用環境	典型的な例
専門の医療施設環境	診療所、病院、歯科診療所、介護施設、外来手術センター、 外来産科センターなど
在宅医療環境	レストラン、カフェ、店舗、学校、ホテル、居住区、乗り物（車、バス、飛行機、ヘリコプタ）など
特殊環境	軍事区域（潜水艦、レーダー施設近傍など）、重工業地帯（発電所、鉄鋼・製紙工場）、高出力医療電気機器（電気手術器、短波治療機器など）を用いた医療現場など

図 4-22 意図する使用の環境の例

【参考：使用環境については，IEC 60601-1-2 の Figure 3，及び Annex E が参考になる。】

【機器の構造】

・この規格では **ME 機器**の構成に対してポート別の電磁ノイズ印加を規定しているため。その構造をあらかじめ明確化しておく。

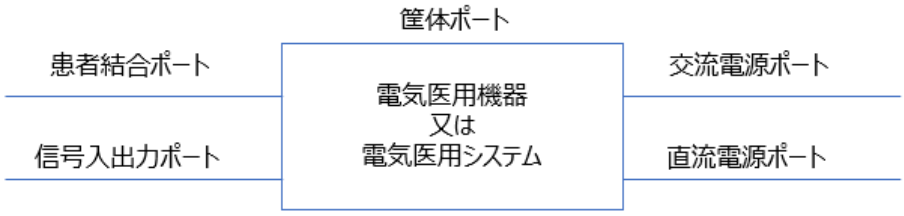


図 4-23 ME 機器および ME システムのポート

新たに開発する製品が，従来の製品と同じか似ていれば，いくつかの**ハザード**は既に分かっている。それに加えて，新たに予見可能な**ハザード**の存在を検討する。電磁ノイズの到来にて，**安全機能**を妨げる電子機器の危険な挙動（結果事象）は以下のような例が予見できる。

- 意図しない突然の起動
- 指示した動作の突然の停止，中断，リセット
- 動作モードの意図しない変化，もしくはループ化
- 診断や治療に影響する取得データの誤り
- 診断，治療又は**監視**を妨げる雑音や誤った**異常**所見
- 誤警報

電子制御機器が，要求どおりに機能しない**故障**原因や**誤使用**（原因事象）の例は，次の通りである。

- 部品の**故障**（素子のラッチアップ，フィルタ部品の容量劣化など）による DC **故障**，信号の歪み
- プログラム可能なパラメータ，工場出荷時のプリセット値の意図しない変化
- コネクタなどの接続部分での断続的な接触
- 最大定格，許容誤差範囲を超える電子部品の使用
- シールド又は RF 結合部分に関連する不適切な緩み又は留め具の欠損
- 導電性ガスケットの損傷，腐食又は欠損
- サージ保護装置の**故障**，磨耗
- 不適切なケーブルの使用や配線

ハザードの特定では，防護不十分なポートがある場合，電磁妨害が**基礎安全**又は**基本性能**に影響を与えるような信号の劣化，ひずみ又はデータの欠損などを考慮する。イミュニティ（電磁ノイズ耐性）関連の**ハザード**の場合，次のように**共通原因故障**をも含めて考慮することが肝要である。

- 機器の一つの**サブシステム**の（防護が不十分な）ポートに生じる，信号劣化，歪み，**故障**
- 単一部品が持つ複数の(防護不十分な)ポートに，同時に発生する信号劣化，歪み，**故障**
- 2 つ以上の異なる部品の複数の(防護不十分な)ポートに，同時に生じる，類似又は異なる信号劣化，歪み又は**故障**

複数のポートに同時に現れる上記のような信号に対し，**PEMS** の**信頼性**を改善させるための一つの手段は，**冗長性**の考慮である。

以下は，同時に**障害**状態を引き起こす原因となる要因の例である。

- 高い周囲温度
- 振動
- 交流電源からのひずんだ電圧波形
- RF 電磁界
- 静電気放電事象
- シールド用ガスケットの腐食
- 不適切なケーブルの使用と設置

製品のライフサイクル，**予測耐用期間**を通じて，物理的環境によっては電磁ノイズ干渉において重大な影響を受ける場合もある。

② リスク評価

第 2 章で扱った**リスクマネジメント**規格 ISO 14971 では，**リスク評価**の**プロセス**を記載している。機器の**予測耐用期間**にわたって，電磁妨害により**基礎安全**及び**基本性能**を損なわないか，この**プロセス**で**評価**・判断する。

【参考： EMC 指針（Guide on EMC for Functional Safety）の 3.4～3.8 及び 4.2 には，より多くの情報がある。】

Guide on EMC for Functional Safety, The Institution of Engineering and Technology (IET), formerly the IEE, London, UK, 2008, www.theiet.org/factfiles/emc/index.cfm

③ リスクコントロール

電磁ノイズに関する**保護方策**とは，所謂 EMC ノイズ対策になる。基本的な EMC ノイズ対策としてボンディング，フィルタリング，シールディング，ガルバニック絶縁，過電圧保護などの対策セオリーがあり，ノイズ源と侵入ルートによって合理的な対策が選択される。

④ 要求仕様

リスクコントロールで特定された**保護方策**の要求仕様は文書化される。

ISO 21856 は EMC 要求を IEC 60601-1-2 適用としているので，この規格から要求イミュニティレベルとその試験法を選定することとなる。IEC 60601-1-2 ではイミュニティ試験開始前に，**製造業者**が試験所に対して試験計画書（テストプラン）を提供することが規定される。【試験計画書の項目については，*IEC 60601-1-2:2014* の *Annex G* を参照のこと。】

要求されるイミュニティ試験は複数存在し，更にその試験毎の専用の規格を引用して実施することを規定している。4.3.2 章で具体的な試験項目を説明する。

イミュニティ試験では，最終目的は機器の**基礎安全**及び**基本性能**を満たすことである。したがって一概に，部品が壊れたから，正常動作を損なったから，NG と見なされるわけではない。**リスクマネジメント**から導出される受容可能な**故障**や劣化の状態を特定し，合理的な判定基準を明らかにしておけば，後工程での不必要な**リスク**低減策の追加が避けられ，スムーズな**評価**を行うことができる。

また，**基礎安全**及び**基本性能**に対し，受容できない**リスク**を最も生じさせそうな動作モード及び条件で試験可能なよう計画する。**安全機能**の作動と電磁ノイズ印加の方法・タイミング，及び正しく作動したかを判断する具体的な確認方法をこの時点で明確にすることは，目的とする試験の実現性を向上させる。

PEMS 評価の場合は，PESS が持つ**安全機能**の要求仕様を明確にしておくことが重要である。**安全機能**の要求仕様を侵害しないことが，イミュニティ試験での判定基準の一つとなる。

また，設計変更不可能な市販品や外注購入品のサブアッセンブリを組み込む場合には，EMC に対す

る仕様を，採用する事前に明確にしておく事が必要であろう。
【参考】安全ハンドブックの 3-2 項『安全性評価項目 安全性評価項目候補のリスト(電磁両立性の確認内容)』は代表的なロボット介護機器毎の典型的な試験要求の例が示されており，参考にできる。

⑤ 設計及び実装

保護方策として導出したノイズ対策を要求仕様通りに実装可能なように EMC 対策設計を行う。ノイズ源と侵入ルートによって EMC 対策が選択されるわけだが，典型的な対策例としては，伝導イミュニティであれば，通信線入力回路に侵入する妨害波の周波数に適合するコモンモードチョークコイルを通信線端子に挿入することで，コモンモード誘導電流を低減させる。コモンモードチョークコイルとは，信号を伝送する 2 本の導線を**フェライト**コアに巻きつけたものであり，2 本の導線間は低インダンスに 2 本の導線と大地間は高インピーダンスとすることにより，有効な信号は通しつつ，コモンモードノイズのみをフィルタリングする。また，雷サージには 3 極避雷管やバリスタ等を，通信線と大地間に挿入して，通信ポートに侵入するサージ電圧を大地に逃がすことで，機器を過電圧保護する。
安全機能の**危険側故障**を回避／抑制するためには，**エラー**回復やフェールセーフの技法もある。これらの技法は，イミュニティにおける**故障**の影響範囲の予想をすることが困難な場合に有効である。
EMC 関連部品を実装する場合には，ハーネスの固定やフィルタの空中配線など，**リスク**低減効果を阻害する要因を避けることが望ましい。このように**リスク**低減効果を管理しながら開発を進める。
【参考： 電磁妨害によって生じる可能性がある**リスク**を低減させる方法は EMC 指針（Guide on EMC for Functional Safety）の 4.3～4.8 及び第 6 章，並びに IEC/TS 61000-1-2:2008 の附属書 B では，**リスクコントロール**手段について，より多くの情報がある。】
ISO 14971 の箇条 6.3 では，各**リスクコントロール**手段の有効性を**検証**し，その結果を**リスクマネジメントファイル**に**記録**することを求めている。重要なことは，EMC 設計中も**リスクマネジメント**を反復して行うことであり，カット＆トライの対策は慎むべきである。
具体的な**検証**手法は，次を含むが，これに限定しない。

- イミュニティ試験（部品レベル。完成品としては **PEMS 妥当性確認**で実施。）
- チェックリスト
- レビュー及び**評価**
- 監査（品質管理の一部として）
- 個々の，及び／又は統合したハードウェア試験
- 妥当性が確認されているコンピュータシミュレーション

⑥ PEMS 妥当性確認

検証を終えた **PEMS** は，**ロボット**介護機器に組み込まれ，**PEMS** への要求事項を満たし，意図するように機能するかどうかの判断（**妥当性確認**）を行う。**PEMS** の電磁ノイズからの影響は要求仕様書から引き継いだ試験計画書（テストプラン）で指定した EMC 試験を最終完成品で実施する事で要求

仕様満たすことが確認される。
すべての**安全機能**，機器接続構成，動作状態の組み合わせに対して**検証**が行われるよう，試験計画は作成される。例えば，印加ノイズの周波数変動に対する誤作動の十分な観察時間，大量データ転送に配慮した試験，重い電気的負荷状態，性能限界部分での見極めなどの考慮を含めることができる。また，試験を成立させるために，必要に応じて接地線を遮断したり，リレーやスイッチを閉路させたりするなど，正常動作内の最も不利な条件を考慮・再現する必要がある。
尚，**ロボット**介護機器に適用する IEC 60601-1 規格では，4.2 章で解説したように，**PEMS** には**単一故障安全**が要求されるが，イミュニティ（電磁ノイズ耐性）については**系統的な故障**の**検証**と考え，単一**故障**条件下で更に電磁ノイズからの影響（**系統的な故障**）を確認することまでは一般的には考慮しない。
試験報告書の記載項目については IEC 60601-1-2 の Table 10 にて示される。試験報告書は文書管理の**手順**に従い，後日同じ項目の**検証**を行った場合の再現性を保証する情報を含む必要がある。温度や湿度などの周囲環境はもとより試験サイトの特定，使用測定器の特定，校正などの管理状況，試験者名などが考**え**られる。

4.3.2 EMC 試験の方法

① EMC 試験の項目

この規格で要求される EMC 試験は**表 4-5** の通り複数存在し，それぞれ専用の試験規格を引用する。**PEMS** が使用されるノイズ環境，基本構造や接続方法に応じて選定する。

表 4-5 IEC 60601-1-2 に適用される EMC 試験の概要

	試験項目	試験の概要	引用する EMC 基本規格
エミッション（EMI）	無線周波妨害波	・**医療機器**からの放射妨害波を CISPR 規格に準じて測定する。	・CISPR 11
	高調波ひずみ	・**医療機器**から商用電源系統に流入する電流の高調波成分を測定する。	・IEC 61000-3-2
	電圧変動及びフリッカ	・**医療機器**が発生する電圧変動(フリッカ) を測定する。	・IEC 61000-3-3

表 4-6 （続き）IEC 60601-1-2 に適用される EMC 試験の概要

	試験項目	試験の概要	引用する EMC 基本規格
イミュニティ（EMS）	静電気放電(ESD)	・静電気に対する感受性を試験する。	・IEC 61000-4-2 に指定した試験方法及び試験機器を，一部修正を加えて適用する。
	放射 RF 電磁界	・無線周波電磁界（80MHz～2.5GHz）に対する感受性を試験する。	・IEC 61000-4-3 に指定した試験方法及び試験機器を，一部修正を加えて適用する。
	電気的ファストトランジェント/バースト	・繰り返しの速い高周波ノイズに対する感受性を試験する。	・IEC 61000-4-4 に指定した試験方法及び試験機器を，一部修正を加えて適用する。
	雷サージ	・落雷によって電源ライン又は電線に伝搬したサージ（高エネルギの誘導雷ノイズ)に対する感受性を試験する。	・IEC 61000-4-5 に指定した試験方法及び試験機器を，一部修正を加えて適用する。
	RF 電磁界によって誘発する伝導妨害	・無線周波電磁界（～80MHz)に対する感受性（伝導性イミュニティ)を試験する。	・IEC 61000-4-6 に指定した試験方法及び試験機器を，一部修正を加えて適用する。
	電圧ディップ，短時間停電及び電圧変化	・電源の電圧ディップ（電源電圧の一時的な低下)・瞬停及び電圧変化に対する感受性を試験する。	・IEC 61000-4-11 に指定した試験方法及び試験機器を，一部修正を加えて適用する。
	電源周波数磁界	・電源周波数の磁界に対する感受性を試験する。	・IEC 61000-4-8 に指定した試験方法及び試験機器を，一部修正を加えて適用する。

② 電磁両立性への適合性を確認するための試験の例

機能安全のイミュニティ試験を理解するために，以下のような動作モードに対してイミュニティ試験を実施する。（ここでは IEC 60335-1 試験要求を参考にした。）

試験動作モード ： 電子的遮断からの意図しない再起動が無いこと。

電子的遮断によって OFF 位置を得る**ロボット**介護機器又は機器を待機モードに置くことができる**ロボット**介護機器は，以下の試験を実施する。試験は，機器に定格電圧を給電し，OFF 位置又は待機モードに設定した状態で行う。電子的遮断が保持できず閉路してしまう場合は NG となる。

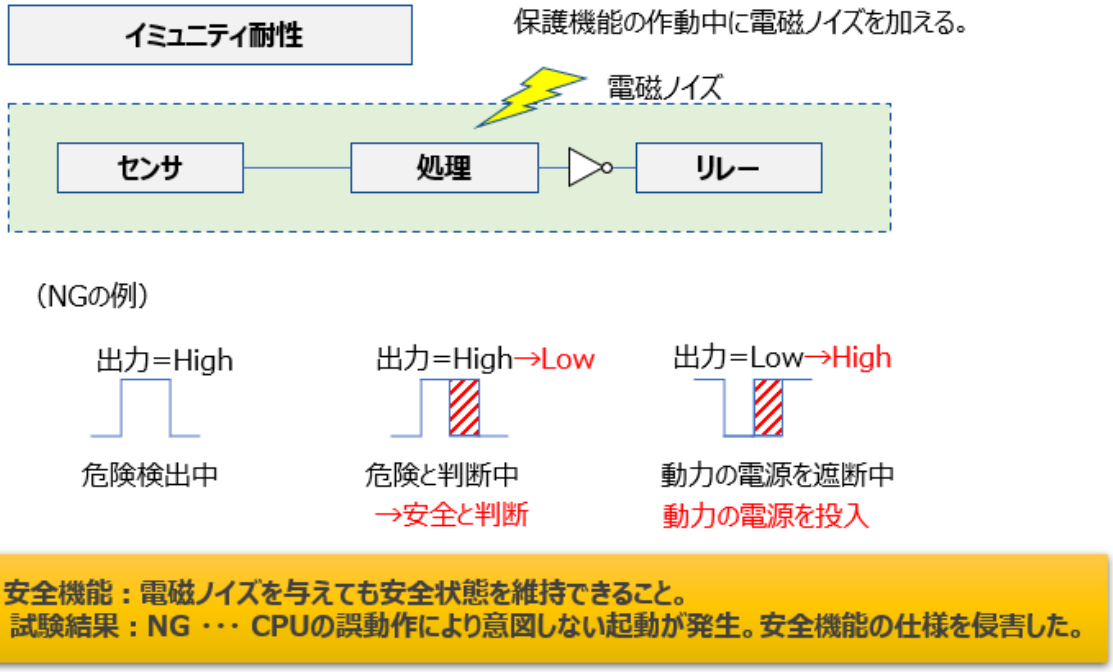
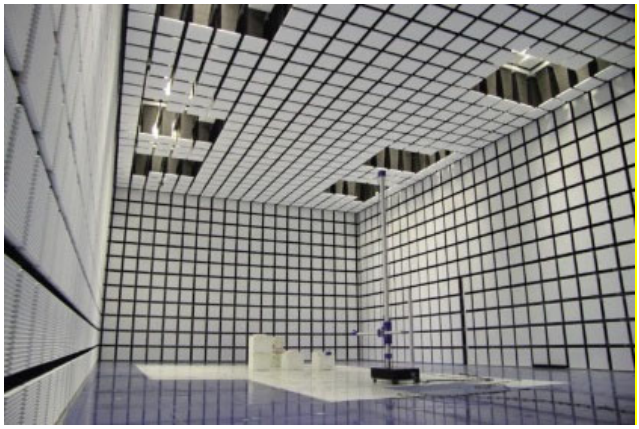


図 4-24 電子的遮断時の意図しない再起動

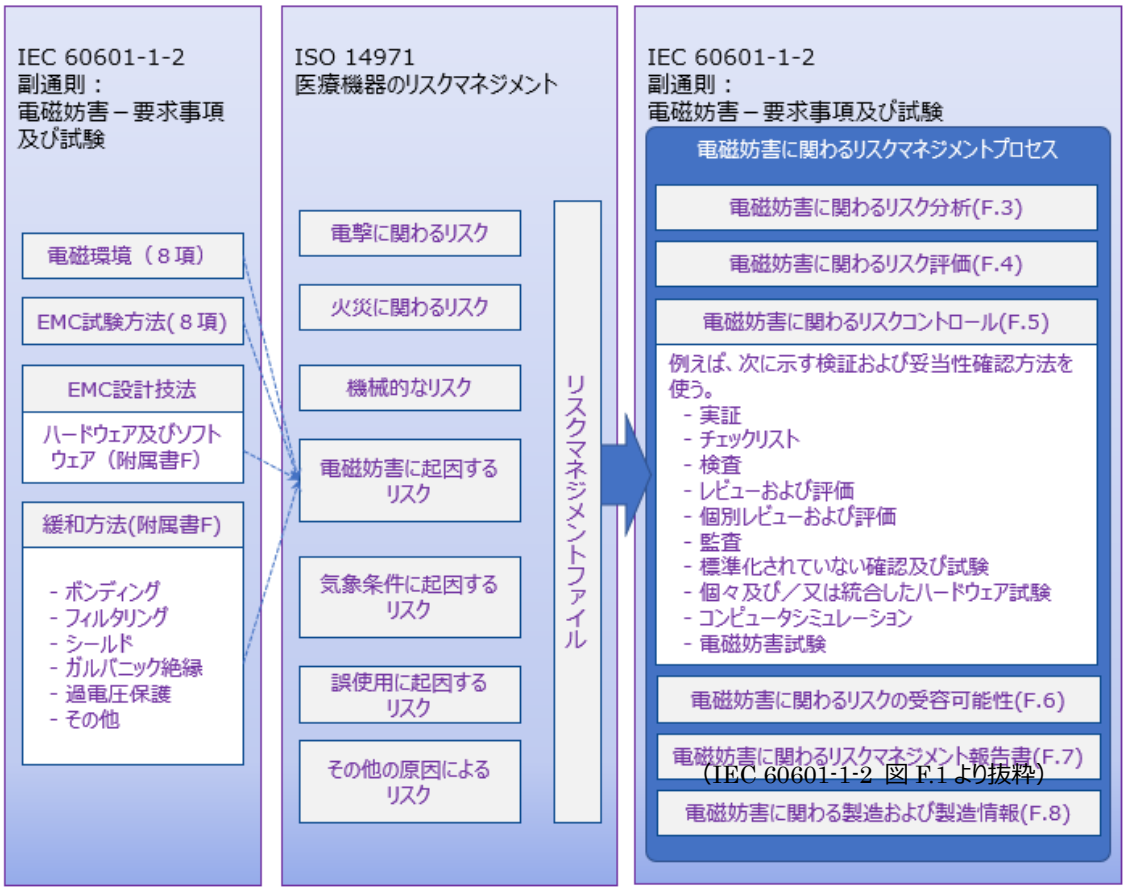


4.3.3 電磁妨害に関するリスクマネジメント

ISO 14971 では**ロボット**介護機器の**ハザード**を特定し，**リスクコントロール**することが求められる。**PEMS** 開発ではイミュニティ（電磁ノイズ耐性）に係る**ハザード**に着目し，**リスクマネジメントプロセス**が求められる。**PEMS** が**安全**を達成するために，単純にイミュニティ試験レベルで試験すればよいと考えてはならないことに注意する必要がある。

“**安全**”という用語は，ISO 14971 で定義している通り，受容できない**リスク**がないという意味で使う。**基礎安全**及び**基本性能**は，ここで言う**安全**の定義に含まれる。

図 4-25 は，**リスクマネジメントプロセス**の中で，この規格をどのように当てはめればよいかを示している。



（IEC 60601-1-2 図 F.1 より抜粋）

図 4-25 図 F.1－リスクマネジメントプロセスにおけるこの副通則の機能

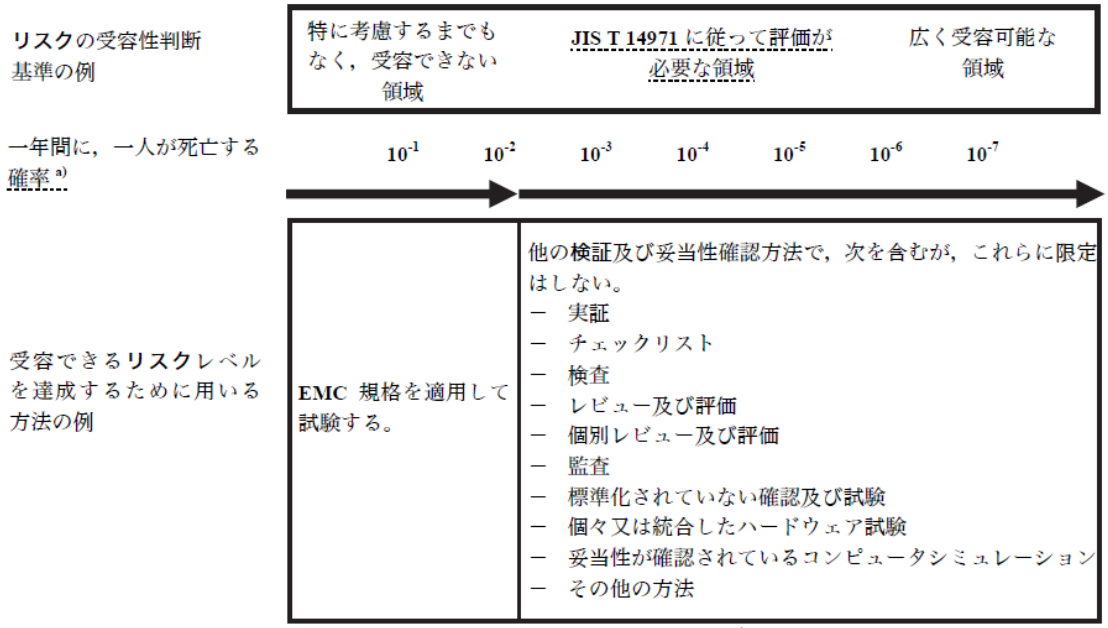
図 4-25 の左側の枠内のように，IEC 60601-1-2 の各箇条は，ガイダンスの第 4.3.1 章で概説した開発**プロセス**を要求している。この開発**プロセス**中，反復して電磁妨害に起因する**リスク**をマネジメントする。**リスクマネジメント**は，ISO 14971 に示す，一般要求事項（箇条 3），**リスク分析**（箇条 4），**リスク評価**（箇条 5），**リスクコントロール**（箇条 6），**残留リスク**の全体的な受容可能性の**評価**（箇条 7），**リスクマネジメントファイル**（箇条 8），製造及び製造後情報（箇条 9）の**プロ**

セスに従う（第 3 章を参照）。その技術的な検討**要素**をサポートするため，図 4-25 の右枠に示すように，IEC 60601-1-2 の附属書 F に，電磁妨害の影響に関わる事項について，**リスク**を改善することが可能な技術的な補足情報を示している。

尚，**リスクマネジメントファイル**には，次を含めるか，又は参照してもよい。

- 技術的な根拠，計算及びシミュレーション
- 試験計画を含む**検証**計画及び**妥当性確認**計画
- 試験結果を含む**検証**結果及び**妥当性確認**結果

また，図 4-26 は，電磁妨害の影響に関わる**リスク**レベルを改善するために，扱う**リスク**レベルに応じて，より厳格な**検証**活動が求められることを示している。



（IEC 60601-1-2 図 F.2 より抜粋）

図 4-26 リスクレベルの信頼性を改善させるための検証方法の例

5　ソフトウェア開発実施ガイド (IEC 62304)

5 章では，**医療機器**と見なされる**ロボット**介護機器のソフトウェア開発に要求される内容を，IEC 62304 規格「**医療機器ソフトウェアーソフトウェアライフサイクルプロセス**」（以後「この規格」と呼ぶ）をベースに解説する。

ロボット介護機器に適用する国際規格 ISO 21856 では，「支援機器の動作を制御するためにソフトウェアを使用する場合は，IEC 60601-1:2005 + A1:2012 の要求が適用される。」とあり，具体的な対象箇所が分かりにくいが，**図 4-1** に示すように，IEC 60601-1 の箇条 14.1 にて言及されている「ソフトウェアを含む場合は，各 PESS のソフトウェアの開発又は変更管理に対して，この規格の箇条 4.3，箇条 5 及び箇条 7～箇条 9 を適用すること」が要求されている。これらの箇条では，ソフトウェアに求める**安全**度を定義し，**安全**度に応じたソフトウェア開発**プロセス**を管理し，開発**プロセス**中に**リスクマネジメント**を導入することを要求している。

安全機能を実現するプログラマブルな電子**制御システム**のソフトウェアの欠陥により，不**安全**事象が発生するかも知れない。このような欠陥は，この規格では**系統的な故障**と呼ばれる。この**故障**による製品の**リスク**を低減するため，この規格は，**ソフトウェアライフサイクル**を通じて，開発（および保守）**プロセス**を管理することを要求している。

このガイダンス 5 章では，**医療機器**規格に馴染みのない，一般の生活支援**ロボット**の開発者が，海外展開の**ロボット**介護機器を開発する際に要求される**医療機器**のソフトウェア開発要求に対応するケースを想定する。

この規格の要求は，**ソフトウェアライフサイクル**を通じた開発**プロセス**での管理がメインである。そこで，この 5.1 章では，この規格の目的を理解し，ソフトウェアの**安全**性への考え方とそれを実現する方法に触れ，その後，この規格がソフトウェアの**安全**性を確保するため，どのようなコンセプトと流れで要求をしているか概観する。

5.2 章では，この規格の箇条 4 で扱う一般要求事項を説明する。この規格の箇条 5 からは，**ソフトウェアライフサイクル**の各工程での活動の要求が述べられているが，その前に，全工程に一貫して関係する「品質マネジメント**システム**(箇条 4.1)」，「**リスクマネジメント**(箇条 4.2)」，「ソフトウエア**安全**クラス分類(箇条 4.3)」，「**レガシーソフトウェア**(箇条 4.4)」について，規格の条文をベースにかみ砕いた説明を行う。

5.3 章では，この規格の箇条 5 から箇条 9 までの，**ソフトウェアライフサイクル**の各工程での活動の要求を説明する。ここまでの章で，この規格のコンセプトを理解し，各々の要求への理解度が上がっていることを期待する。この章では規格の条文をベースにその要求事項の解説を試みた。言い回しを変えることで理解が進む場合もあると考え，かみ砕いた言い回しを考慮した。また，どのようなことをすれば適合するのかについて，いくつか例示を試みたので，参考になれば幸いである。ただし，例示は理解を促進するためのものであり，例示を単に真似ても適合するわけではなく，全体として論理的かつ首尾一貫して**安全**を説明できるものになっていることがこの規格の要求の主眼であると考える。

5.4 章では，**ロボット**介護機器の開発に参考になり得る情報をいくつか記述した。

この規格の要求は，**ソフトウェアライフサイクル**を通じた開発**プロセス**での管理がメインなので，ソフトウェア開発**プロセス**に馴染みの無い開発関係者については，ソフトウェア開発エンジニアリングの方法論，及びソフトウェア品質保証の方法論に関する基礎知識が必要と考える。また，**ロボット**介護機器開発に一貫して必要な，**リスクアセスメント**に関する基礎知識も必要と考える。このガイダンスはそれらの基礎知識を網羅するものではなく，別途入門書などで補足学習することを前提とする。

5.1 IEC 62304 規格の目的と要求の概要

5.1.1 ソフトウェアの安全性を向上する 3 大原則

この規格の目的は，「**プロセス**」を示すことである。（以下，箇条 1.4 抜粋より）

> (参考和訳)
> この規格は，高品質で**安全**な**医療機器ソフトウェア**を，常に製造する開発**プロセス**を示すことが目的である。この目的の達成のために，この規格では，**信頼性**が高く，**安全**なソフトウェアを生産できる方法で開発されたということを確実にするため，最低限実施すべき**アクティビティ**及び**タスク**を特定する。(箇条 1.4)

現時点において，高品質で**安全**なソフトウェアを製造するための，もっとも一般的な方法論は，**プロセス**管理である。そのため，この規格は，適切な**プロセス**管理を要求することで，高品質で**安全**なソフトウェアを常に製造できることを意図している。ここで言う「高品質で**安全**なソフトウェア」実現のため，**リスクマネジメント**を適用して**安全**を確保し，ソフトウェアエンジニアリングを導入して適切な工法と技術を適用し，品質マネジメントに基づき組織的に設計・製造品質を管理することにより**安全**に対する高い品質が確保されたソフトウェアが製造できることを意図する。

規格の附属書 B にて，**医療機器ソフトウェア**の**安全**性を向上させる次の三つの大原則を述べている。この規格は，これら「三つの大原則」を組み合わせて適用することを意図していて，一般的には次の規格の適用を意図している。

① **リスクマネジメント** …… ISO 14971 (JIS T 14971)
② 品 質 マネジメント …… ISO 13485 (JIS Q 13485) など
③ ソフトウェアエンジニアリング …… この規格： IEC 62304 (JIS T 2304)

> (参考和訳)
> いずれのソフトウェアについても，100%の**安全**を保証する既知の方法は無い。
> **医療機器ソフトウェア**の**安全**性を向上させるには，次の三つの大原則が存在する。
> – **リスクマネジメント**
> – 品質マネジメント
> – ソフトウェアエンジニアリング
> （中略）上記三つの原則を組み合わせれば，**医療機器**の**製造業者**の意思決定**プロセス**が明確な体系をとり，首尾一貫した再現性のあるものとなり，**医療機器ソフトウェア**の**安全**性が促進される。
> （附属書 B「この規格の適用についての指針」より）

この規格は，受け入れ可能な**リスク**の達成及び**リスク**を低く保ち続けるための**リスクマネジメント**を基盤として，それを実現するための技術として，ソフトウェア開発及び保守に対して**ソフトウェアエンジニアリング**を適用し，その品質を確実にするためのフレームワークとして**品質マネジメント**を適用して，これらを組み合わせた方法により，ソフトウェアに関する**安全**を達成するやりかたを確立することを意図している。この規格を読む前に，まずこの目的・背景を理解したい。具体例を入れて詳細の説明を続ける。

5.1.2 他の規格との関係性

この規格の適用範囲は，**医療機器ソフトウェア**の開発及び保守である。ただし，このガイダンスでは，**ロボット**介護機器が**医療機器**として扱われる場合を想定し，その**ロボット**介護機器に組み込まれるソフトウェアを対象とする。この規格の箇条 1.3 でも，他の規格との併用を意図することを述べており，機器全体の**安全**を適用範囲とする規格が存在し，その規格がこの規格を引用することを前提としている。

医療機器と見なされる**ロボット**介護機器では，全体の**安全**性については ISO 21856 草案が役割を担い，**リスクマネジメント**は ISO14971 が担当し，そのうち **PEMS** については IEC 60601-1 が担当する。そして，**PEMS** のソフトウェア部分について，この規格を引用する形で適用がなされる。つまり，この規格は，全体の**安全**性の中でソフトウェア部分について分担しているにすぎない。ソフトウェア自体が製品である場合（ＰＣにインストールして使用するソフトウェア製品など）であったとしても，その製品全体の**安全**性を適用範囲とする規格（例えば IEC 82304-1）を適用し，その規格からこの規格を引用することが必要である。

特に，この規格は，**リスクマネジメント**の規格である ISO 14971 を切り離して考えることはできない。この規格の箇条 7 にソフトウェア**リスクマネジメント**の要求事項が規定されているが，それは，ソフトウェアを含めた製品全体に対し ISO 14971 が適用されていることが前提であり，それ無くしては，ソフトウェアと**リスク**との関連も明らかにできず，**リスク**に基づいた**アクティビティ**及び**タスク**の実施という，この規格のコンセプトが成り立たなくなる。このような関係性は，機械の**機能安全**とは異なるため，導入に際しては注意する必要がある。

また，この規格は，品質マネジメント規格（例えば ISO 13485）を引用していて，これは，組織が品質に関する適切な開発をするための基盤を提供する。

5.1.3 ソフトウェアの安全性

ソフトウェアは，動作しなければ（プログラムメモリ上に置かれているだけの場合は），単なる１と０の集まりであり，実体は無いも同然である。動作しなければ，**危険状態**を発生させることも，**リスク**をコントロールすることも無く，**安全**とは無関係と考**えら**れる。ソフトウェアは，その実行時にハードウェアと相互作用し，更に機能が人などへ作用することにより，**危害**を加えてしまう場合があり得る。一方で，ソフトウェアは，実装された**リスクコントロール**方策の実行により，**危険状態**に対処し傷害の発生を回避することも可能である。

つまり，ソフトウェアはハードウェアなどとの相互作用の結果として，**リスク**を顕在化させたり，低減したりする場合がある。

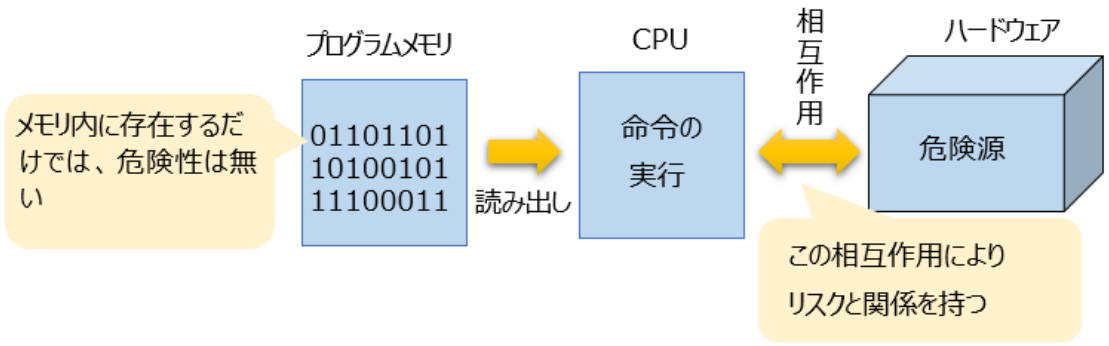


図 5-1 ソフトウェアとリスクの関係

そのため，ソフトウェアが**リスク**に関してどのように振舞うべきかを明確にすることが，**安全**なソフトウェアを開発するうえで，最も重要である。この明確化は，実現すべき振る舞いだけでなく，禁止すべき振る舞いを明確化することも重要である。

実現すべき振る舞いの例：

当該移動作業型**ロボット**は，走行中における人との衝突に関する**リスク**を回避するため，近くに人がいる場合は，走行を停止しなければならない。よって，ソフトウェアは，周囲の人を検知し，1m 以内に人がいると判断した場合は，ブレーキを作動させ，**ロボット**の走行を停止させること。

禁止すべき振る舞いの例：

当該移動作業型**ロボット**は，走行開始時における人への追突に関する**リスク**を回避するため，近くに人がいる場合は，走行を開始してはならない。よって，ソフトウェアは，周囲の人を検知し，1m 以内に人がいると判断した場合は，走行モータを駆動してはならない。

ロボット介護機器が**安全**を達成するためのソフトウェアへの要求は，**ソフトウェア安全要求事項**として明確化する。これは，**リスクマネジメント**から導いた機器全体の**安全**要求に基づいて，（**PEMS** 関連部分が抽出され），ソフトウェア関連部分を抽出したものになっている。このソフトウェア要求事項は，客観的明確に仕様を定義し，「ソフトウェア**安全**要求仕様」とすることが重要である。

◇客観的明確な（に）

このガイダンスでは，仕様の記述などについて，人によって解釈の差が出ない水準で明確な状態を「客観的明確な」と表現する。例えば，過熱防止機能の作動温度について，「高温になったら」では，高温と判断する温度について解釈の余地があるため，客観的明確とは言えず，「センサからの信号が 40℃以上を示した場合」は，温度について人による解釈の余地はなく，客観的明確であると表現する。

ソフトウェア**安全**要求仕様の定義後，そのソフトウェア**安全**要求仕様を満たすソフトウェアを作成する。このとき，何らかの間違いによりソフトウェアに欠陥（バグ）が混入すると，ソフトウェア**安全**要求仕様を満たせず，それが**危害**に至る原因になり得る。

ソフトウェア作成時の欠陥の混入を防ぐには，ソフトウェア**安全**要求仕様に対する品質を確保する必要がある。品質を確保するには，主に「適切に設計する」こと，および「適切に確認を行う」こと，およびそれらが適切に実施されるよう「管理する」ことも重要であり，この管理環境を提供することが，**①品質マネジメント**が必要な理由である。

◇欠陥（defect）
このガイダンスでは，ソフトウェアの問題点の原因をひっくるめて「欠陥」と表現する。
欠陥には，コーディングのミスやソフトウェア設計時のミスなどの，いわゆる「バグ」だけでなく，ソフトウェアへの要求の間違いや，既存ソフトウェアの間違った流用など，ソフトウェア作成時以外の間違いも含む用語として用いる。ただし，このガイダンスでは，ソフトウェア自体に含まれるものに限定し，文書上のもの（例えば誤記がある，**トレーサビリティ**が示せていないなど）は，欠陥には含めない。文書上の間違いによりソフトウェアも間違ったものになった場合は，そのソフトウェアの間違いは欠陥に含める。

ここまで述べた考え方をまとめると，次の通りになる

- （**システム**全体の**安全**要求仕様に基づき） ソフトウェア**安全**要求仕様を適切に定義する。
- ソフトウェア**安全**要求仕様を適切に満たすソフトウェアを実現するために管理する。
- 欠陥を混入させないように適切に設計する。
- 適切に設計されたことを適切に確認する。

ただし，ソフトウェア**安全**要求仕様が完全であることを前提に，それに対する品質だけを考えていては，不充分である。例えば，ソフトウェア**安全**要求仕様が完全ではなく，条件に抜けがあった場合，ソフトウェアをいくら高品質に作成しても，**安全**上の問題が発生してしまうことがあり得る。そこで，ソフトウェアを設計している途中においても，**安全**に対して適切なソフトウェアになっているか，反復して分析し，問題があれば見直し，**安全**に対して適切であるかどうか確認し続けることが重要である。

また，ソフトウェア設計中に，ソフトウェアに起因する新たな**リスク**に気づくこともあり得る。例えば，メモリアクセスに関する他のソフトウェアとの排他処理が，機能の**障害**を引き起こし事故に至る可能性に気付くかもしれない。そのような場合があることを念頭に，**安全**に対して適切かどうか確認し続けることが重要である。これらは，**②リスクマネジメントが必要**な理由である。

安全関連**制御システム**の設計・製造に関する包括的な方法論を提供するため，2000 年に国際電気標準会議（International Electrotechnical Commission）が広範囲の機械類に適用できるグループ**安全**規格として IEC 61508 シリーズ「電気・電子・プログラマブル電子**安全関連系**の**機能安全**」を発行し，その後の 2006 年に**医療機器**産業分野について，高品質で**安全**なソフトウェアを製造する

ための規格 IEC 62304「**医療機器ソフトウェアーソフトウェアライフサイクルプロセス**」が発行された。双方の規格に共通するのは，ソフトウェアの**安全**性を確保する方法論として，③**ソフトウェアエンジニアリング**に重きを置いていることにある。この規格では，ソフトウェア**安全**要求仕様に対して適切なソフトウェアを作成することを目的としたソフトウェア開発**プロセス**（ソフトウェア**開発ライフサイクル**と呼ぶ）の管理と，求められる**安全**度に応じて，ソフトウェアの**安全**を問い続け，確認し続けるソフトウェア開発技法の両方の取り組みを重視し，ソフトウェアエンジニアリングを推進することを求めている。

① プロセス管理の重要性

この規格は，高品質で**安全**な**医療機器ソフトウェア**を，常に製造する開発**プロセス**を示すことを目的としており（附属書 B）。開発**プロセス**の管理の重要性を説明してきた。ここで，次のような疑問を感じるかもしれない

「なぜ**プロセス**なのか？ ソフトウェアが**安全**を達成したかどうかは，作ったソフトウェアの**安全**性試験により**評価**すれば可能なのではないか？」

結論は NG である。ソフトウェアの品質を確保するには，試験だけで**評価**するのではなく，適切なソフトウェア要求を明確化し，それに対して品質を適切に作り込み，適切に作られたことをレビュー及び試験により確認する。これら一連の**プロセス**によりソフトウェアの品質を確保するのが現在の主流の考え方なのである。その考え方を**安全**の視点で適用することを，この規格は意図している。

> (参考和訳)
> ソフトウェアの試験を実施しただけでは，その使用が**安全**であると判断するには十分ではないという信念に基づいている。（附属書 A 抜粋）

注記： 念のため記すが，規格は，試験が不要と主張しているわけではない。規格の箇条⑥及び箇条⑦では試験を要求している。また，箇条 1.15.3.5 の問題解決**プロセス**においても試験実施に関する要求が含まれている。

② ソフトウェア試験の限界

安全規格には，「仕様規定規格」と呼べるような，試験方法及び判定基準を具体的に示した規格もある。例えば**医療機器**の**安全**規格である IEC 60601-1 は，そのような側面を含む規格のひとつである。**ハザード**とその**保護方策**のメカニズムが典型的であるなど，具体的な構造要求に加え，**安全**試験方法や判定基準を示すことが適切な場合はこのような要求体系をとる。しかし，ソフトウェアの場合，試験だけで**安全**性を確認するのは，不適切である。ソフトウェアの欠陥による**障害**の発生は，一般的に，「条件を満たせば発生する。」と考**え**られる。その発生条件は，条件の**要素**の組み合わせで表すことができる。例えば，ある特定の**手順**や，ある設定項目が特定の値である場合や，ソフトウェア外部からは見えない，ソフトウェア内部の条件も含まれる。また，放射線によるソフト**エラー**のように，時間的にはランダムに発生する現象であっても，その現象が起こった場合を一つの条件と考えれば，条件の問題と考え

ることができる。そこで，その条件の組み合わせをすべて試験すれば，すべての欠陥を洗い出せるはずである。しかし，残念ながら，その「組み合わせをすべて試験する」ことは，非現実的である。ほとんどのソフトウェアは複雑であるため，その組み合わせの数が，容易に天文学的な値になる（これは「組み合わせ爆発」と呼ばれることがある）。それをすべて試験するのは，あまりにもコストがかかりすぎる。そのため現実には，できる範囲の試験だけを実施することしかできず，その結果，試験を実施しなかった条件の組み合わせで，後日問題が発生する。試験だけでは，ソフトウェアの**安全**性が判断することができない最大の事情である。

加えて，適切な**検証**試験を定めることの難しさもある。ソフトウェアの**検証**試験は，ソフトウェアの仕様を適切に考慮して実施する必要がある。ソフトウェアの仕様（外部仕様及び内部仕様の両方）が異なれば，実施すべき試験は異なり，ソフトウェアごとに試験を定める必要がある。このとき，複雑なソフトウェアの全ての仕様が客観的明確に文書化されるとは限らないため，試験条件の洗い出しや，その依存関係の明確化などを漏れなく適切に行うことは困難を伴う。実際には，市場で問題が発生してから，テストケースの漏れに気付くことも珍しくない。また，ソフトウェア修正がなされたとき，影響範囲を分析して必要な試験を実施するが，予想外の副作用が発生したり，実施した試験に不足があったりすることがある。

これらについて改善を重ねる考え方もあるだろうが，それよりも，試験だけに頼るのではなく，適切な設計手法や開発**手順**も含めた適切な**プロセス**管理を用いることが現在の主流の考え方であり，また実績に基づいた方法である。

高品質なソフトウェアを実現する開発**プロセス**に対し，試験は，次のような位置づけとイメージしてこの規格を読むと良い。

高品質なソフトウェアを実現する ＝ 適切な**安全**要求を定義する ＋ 適切に設計する ＋ 適切に設計したことを**検証**する＋ これらの**プロセス**を管理する 適切に設計したことを**検証**する ＝ レビューする ＋ 試験する （静的**検証** ＋ 動的**検証**）

レビュー及び試験については，**検証**と**妥当性確認**の 2 種類に分けることができる。この規格には，**検証**の要求事項が含まれるが，**妥当性確認**は適用範囲外である。

検証（verification）は，仕様や要求事項などに対し，それを満たしている（一致している）ことを確認することを言う。「適合性確認」や「一致性確認」ということもある。「正しく作ったか？」という観点での確認とも言える。一般には，一致していることを示す**客観的証拠**の**記録**を含める。**検証**の方法には，試験による動的確認，レビューによる目視確認（静的確認）などがある。

一方，**妥当性確認（validation）**は，目的（ゴール）を達成したかどうかを確認するものである。「正しいものを作ったか？」という観点での確認とも言える。**安全**規格における **PEMS 妥当性確認**は，「ソフトウェアを組み込んだ **PEMS** は結果として特定した**安全**要求（振る舞いと**安全**度）を満たしているか？有効(valid)であるか？」を確認することである。この規格は IEC 60601-1 との組み合わせで適用することを前提としているため，**妥当性確認**はこの規格では扱っていないが，IEC 60601-1 の箇条

14.11 **妥当性確認**の要求事項に従い，実施する必要がある。**妥当性確認**については，このガイダンスの 5.7.6 章を参照されたい。

ここまでの説明で，仕様を充分に吟味しないままでソフトウェアを作り，問題があればバグ出し試験で洗い出して修正する，というやり方では，高品質で**安全**なソフトウェアを実現できたことをステークホルダに示せないことに気づくだろう。例えば，あるテストケースをひと通り実施した結果，その範囲では欠陥が見つからないことは示せるが，残された欠陥が見つかっていない可能性を否定することはできない。実際，市場で見つかる欠陥に対して，なぜ見つけられなかったのか?これで二度と欠陥は顕在化しないのか？と話題になるが，場当たり的に試行錯誤とモグラ叩きを繰り返す開発ではこれを説明できない。そのため，適切な品質を確保する方法を用いて，正しいソフトウェアを正しく作ることが重視される。つまり，「開発の上流から品質を作りこむ」という考え方が重要なのである。この考え方の場合，試験は，（バグ出しのための試験ではなく）適切なソフトウェアが作られたことを確認（**検証**と**妥当性確認**）するための一つの手段であり，試験結果は高品質で**安全**なソフトウェアを実現できたことのエビデンスの一部と位置付けられる。

以上のような考え方から，この規格は，ソフトウェアの**安全**性を確保するために，ソフトウェア開発**プロセス**の管理活動，加えて，その**プロセス**において欠陥の混入を抑制する適切なエンジニアリング技法の採用。（ソフトウェアエンジニアリング） ソフトウェアに起因する**リスク**を反復して分析する活動。（**リスクマネジメント**） その２つの開発活動を体系的に品質管理する活動（**リスクマネジメント**）を３つの大原則としていると考**えら**れる。

5.1.4 IEC 62304 規格の要求概要

この規格は，ソフトウェアに起因する**安全**度に応じて，関わる**ソフトウェアアイテム**の**リスク**を低減するために，以下のアプローチを行うことを求めている。

① **ソフトウェアシステムのソフトウェア安全クラス分類**
ソフトウェアが関連する**システム**の**安全**性に関わる**ハザード**を特定，その**リスク**を**評価**し，**ソフトウェアシステム**のソフトウェア**安全**クラスとして分類する。

② **ソフトウェアアイテムへの分解**
ソフトウェアシステムを機能部品に分割し，**ソフトウェアアイテム**とする。列挙した**システム**の**安全**性に関わる**リスク**低下が，どの**ソフトウェアアイテム**の**障害**により発生するか特定し，各**ソフトウェアアイテム**のクラス分けを行う。

③ **実施すべきアクティビティ及びタスクの特定**
ソフトウェア**安全**クラスに従って，この規格に明示されたすべての**プロセス**，**アクティビティ**，及び**タスク**を実施する。

① ソフトウェアシステムのソフトウェア安全クラス分類

この規格は，**ソフトウェアシステム**及び**ソフトウェアアイテム**を，３つの**ソフトウェア安全クラス**へ分類することを求めている。これは，**プロセス**を**ソフトウェアアイテム**の**リスク**の大きさ応じて実施するためである。この規格の要求**プロセス**（つまり要求事項）は，附属書 A によると，次の 2 種類に分類できる。この考え方を実現するため，ソフトウェア**安全**クラスへの分類を行い，分類されたソフトウェア**安全**クラスに基づいて，適切な**プロセス**を実施する。

(参考和訳)
この規格が要求する**プロセス**は，次の 2 種類の**カテゴリ**に分類できる。
－ソフトウェアの各**ソフトウェアアイテム**の動作に起因する**リスク**を**評価**するために必要となる**プロセス**
－ **評価**した**リスク**に基づいて選択される各**ソフトウェアアイテム**にソフトウェアの**故障**が発生する確率を低い水準に抑えるために必要となる**プロセス**
この規格は，最初の**カテゴリ**は全ての**医療機器ソフトウェア**に対して実施し，2 番目の**カテゴリ**は選択した**ソフトウェアアイテム**に対して実施することを要求している。
（附属書 A）

ここで理解のため，まずは，この規格が用いる**ソフトウェアシステム**，**ソフトウェアアイテム**，**ソフトウェアユニット**の関係を説明する。これらは，例えば次のような意味で捉えることができる。（付録 C の用語集も参照のこと。）

・**シ　ス　テ　ム　：** 例えば，**ロボット**介護機器全体。ただし，例えば，**ロボット**介護機器が，独立に稼働する２つの機器から構成されている場合は，そこには２つの**システム**があると考える。

・**ソフトウェアシステム：** ひとつのソフトウェア全体。例えば，**ロボット**介護機器のマイコンに搭載するソフトウェア全体。ただし，例えば，２つのマイコンにそれぞれ搭載されたソフトウェアが独立に稼働する場合は，ここには２つの**ソフトウェアシステム**があると考える。

・**ソフトウェアアイテム：** 例えば，**安全**関連ソフトウェア部分，又は**安全**関連メモリへのアクセスを担当するコンポーネント。ある観点でひとつと考えることができる，**ソフトウェアシステム**の部分。なお，**ソフトウェアシステム**や**ソフトウェアユニット**も，**ソフトウェアアイテム**であるということができる。

・**ソフトウェアユニット：** それ以上は分割して考えることができない部分。例えば，個別のサブルーチン。

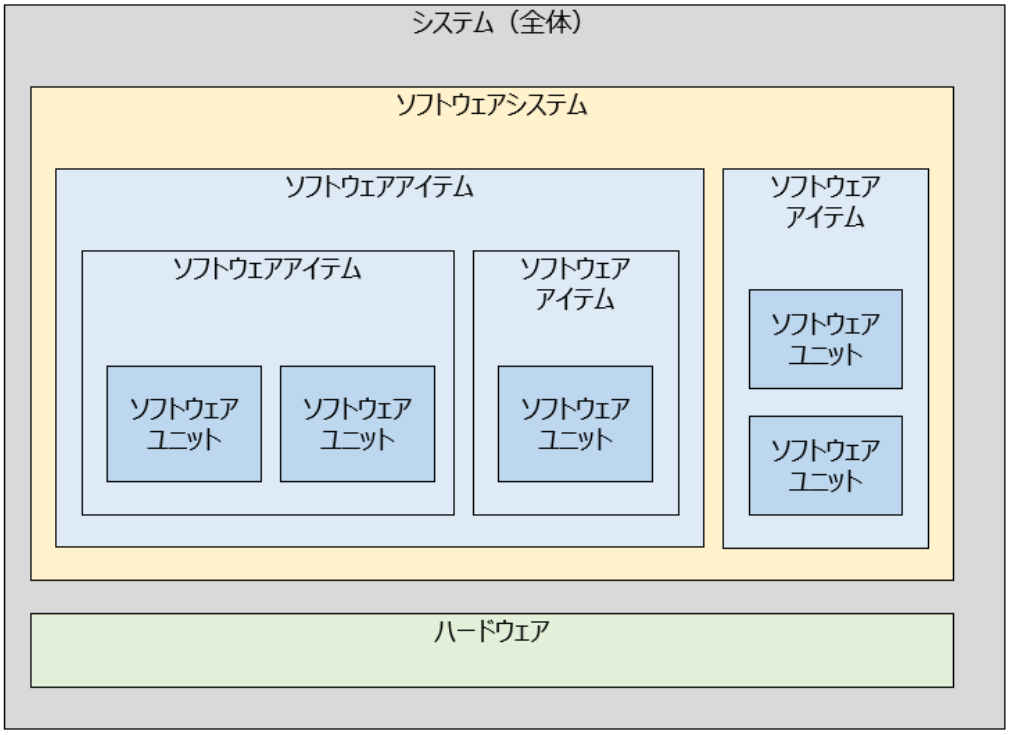


図 5-2 ソフトウェアシステム，ソフトウェアアイテム，及びソフトウェアユニットの関係

先ずは，**ソフトウェアシステム**のソフトウェア**安全**クラスへの分類は，次の条件で行う。

表 5-1 ソフトウェアシステムのソフトウェア安全クラスの分類条件

ソフトウェア**安全**クラス	分類条件
クラス A	次のいずれかの場合： – **ソフトウェアシステム**が**危険状態**の一因とならない場合。 – **ソフトウェアシステム**が**危険状態**の一因となるが，その**ソフトウェアシステム**以外（外部）で実施する**リスクコントロール**手段を考慮すれば，受容できない**リスク**は生じない場合。
クラス B	**ソフトウェアシステム**が**危険状態**の一因となり，その**ソフトウェアシステム**以外で実施する**リスクコントロール**手段を考慮しても，受容できない**リスク**が生じる場合で，かつ**重傷**の可能性はない場合。
クラス C	**ソフトウェアシステム**が**危険状態**の一因となり，その**ソフトウェアシステム**以外で実施する**リスクコントロール**手段を考慮しても，受容できない**リスク**が生じる場合で，かつ死亡又は**重傷**の可能性がある場合。

単純化すると，そのソフトウェアが受容できない**リスク**とは無関係であれば（例えば誤動作しても**安全**であれば）クラスＡであるが，重大な**リスク**と関係があれば（例えば誤動作が死亡事故の要因になりうるのであれば）クラスＣである。**リスク**と関係はあるが重大な**リスク**との関係は無ければ，クラスＢである。

② ソフトウェアアイテムへの分解

次に，**ソフトウェアシステム**を図 5-2 のように**ソフトウェアアイテム**および最少単位である**ソフトウェアユニット**まで分解する。分解された**要素**はすべて**ソフトウェアアイテム**として特定され，この規格は，**ソフトウェアアイテム**に対しても，ソフトウェア**安全**クラスを明確にすることを要求する。基本的には**ソフトウェアシステム**（又は上位の**ソフトウェアアイテム**）のソフトウェア**安全**クラスを継承するが，正当な根拠を示せば変更して良い。（ソフトウェア**安全**クラスの分類に関する規格の要求事項は，このガイダンスの 5.3.3 章を参照されたい。）

③ 実施すべきアクティビティ及びタスクの特定

この規格は，分類された各**ソフトウェアアイテム**のソフトウェア**安全**クラスに基づいて，実施すべき**プロセス**内の活動内容を特定し，規格に示している。実施すべき活動内容とは，**アクティビティ**及び**タスク**と定義され，それらの**プロセス**との関係は，図 5-3 のとおり。**プロセス**は業務フロー，**アクティビティ**は作業工程，**タスク**は作業項目とイメージしてみると良い。

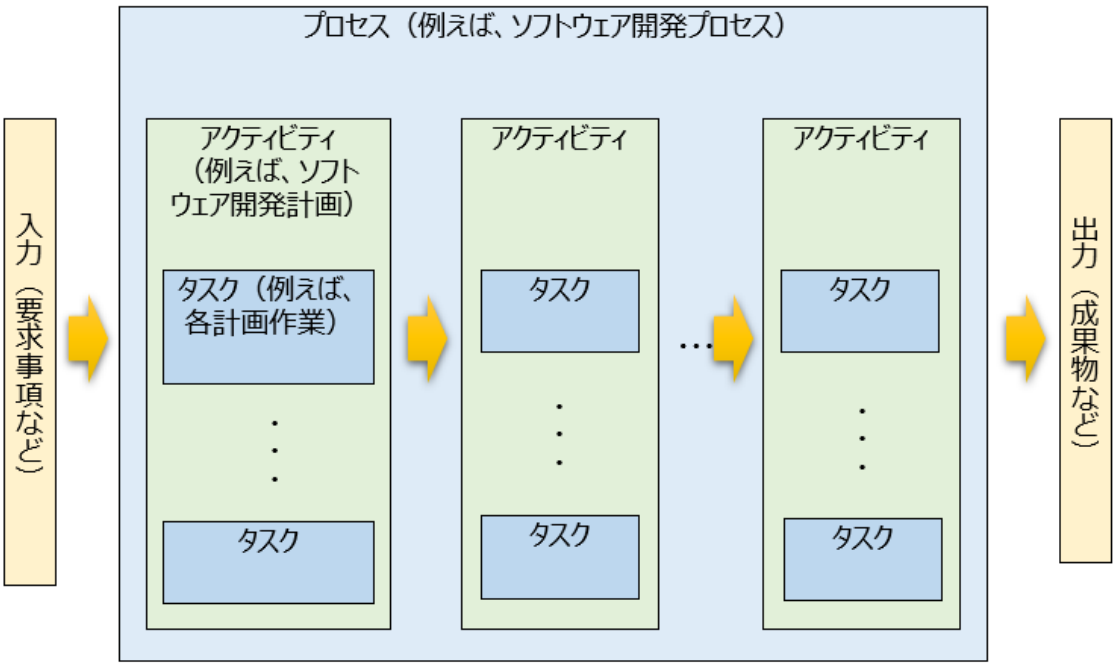


図 5-3 プロセス，アクティビティ，及びタスクの関係

この規格の表 A.1 では，実施すべき活動内容の一覧を示している。分かりやすさのために，少しまとめて表にしたものが表 5-2 である。「○」は要求することを，「―」は要求しないこと（禁止ではない）を意味する。（ただし，正しくは規格を確認されたい。）

危険状態の一因とならないソフトウェア**安全**クラス A のアイテムは，ソフトウェア**リスクマネジメント**の対象範囲から除外される。**危険状態**の一因となり，重症の可能性があるソフトウェア**安全**クラス C のアイテムは，ソフトウェア**安全**クラス B と比較し，さらに高度なソフトウェア開発技術・技法の適用が要求される。

表 5-2 ソフトウェア安全クラスと実施の必要性

プロセス／アクティビティ／タスク	ソフトウェア**安全**クラス		
	クラスA	クラスB	クラスC
品質マネジメント**システム**	○	○	○
リスクマネジメント	○	○	○
ソフトウェア開発			
ソフトウェア開発計画	○	○	○
ソフトウェア要求事項分析	○	○	○
設計～結合試験			
一般的な開発技術・技法の適用	—	○	○
高度な開発技術・技法の適用	—	—	○
ソフトウェアシステム試験	○	○	○
ソフトウェア**リリース**	○	○	○
ソフトウェア保守			
ソフトウェア保守計画	○	○	○
問題及び修正の分析	○	○	○
修正の実装	○（分析の結果により範囲が異なる）		
再**リリース**	○	○	○
ソフトウェア**リスクマネジメント**	—	○	○
ソフトウェア**構成管理**	○	○	○
ソフトウェア問題解決	○	○	○

以上，この章の目的として，規格の要求の流れを解説した。①**ソフトウェアシステム**の**安全**性に関わる**ハザード**を特定，その**リスク**を分析し，**ソフトウェアシステム**のソフトウェア**安全**クラスとして分類する。**図 5-4** に示すように，ソフトウェア開発中も引き続き ISO 14971 **リスクマネジメント**の考え方がベースになる。②**ソフトウェアシステム**を機能部品に分割し，**ソフトウェアアイテム**とする。**システム**の**安全**性に関わる**リスク**低下が，どの**ソフトウェアアイテム**の**障害**により発生するか特定し，各**ソフトウェアアイテム**のクラス分けを行う。目的は上位の**システム**もしくはアイテムの**リスク**度合い引継ぎ，開発を行うことと考**えら**れる。③ソフトウェア**安全**クラスに従って，この規格で要求されたすべての**プロセス**，**アクティビティ**，及び**タスク**を特定する。**図 5-4** のように**安全**クラスにより，その**ソフトウェアアイテム**の開発**プロセス**，活動は厳格さが要求される。

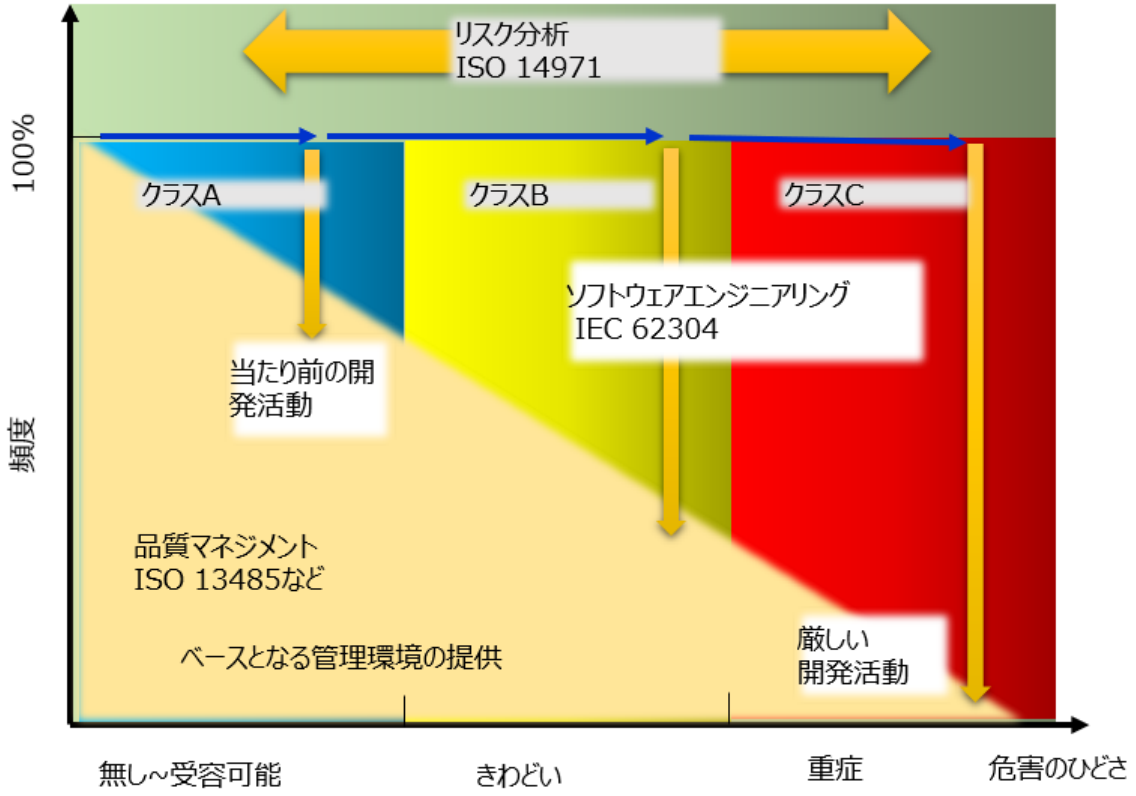


図 5-4 ソフトウェア開発への IEC 62304 の品質要求のイメージ

注記： この規格を適用するかどうかを IEC 60601-1 の箇条 14.1 の要求事項に従って決定する場合，**基礎安全**，**基本性能**および受容できない**リスク**にも関わらない**安全**クラスＡの**ソフトウェアシステム**に対しては，この規格を適用することは，箇条 14.1 の条件からは無いと考える（ただし規制当局などからの要求がある場合を除く）。その場合，上記の表 5-2 における「クラスＡ」の欄の活動は，クラスＢ又はクラスＣの**ソフトウェアシステム**に含まれるクラスＡの**ソフトウェアアイテム**に，適用されると考えてよいだろう。

5.1.5 ソフトウェア開発モデルとその管理について

ソフトウェア開発モデルについては，複数のモデルが提案されている。この規格は，そのひとつであるウォーターフォールモデルを想定しているかのように見えるかもしれない。しかしそれは，説明上そのように並べてあるだけであり，他の開発モデルを使用して良い。

> (参考和訳)
> この規格は，特定の**ソフトウェア開発ライフサイクルモデル**を要求するものではない。（中略）この規格の**プロセス**は，“ウォータフォール”又は“ワンススルー”ライフサイクルモデルを示唆するシーケンスで説明するのが最も容易である。しかし，他のライフサイクルモデルも使用可能である。
> （附属書 B）

この規格では，ウォーターフォールモデル，繰返しモデル，及び進展的モデルの３つのモデルが例示されている。他にも，例えば，Ｖモデル，Wモデル，スパイラルモデル，プロトタイピング，アジャイル開発などがあり，これらは，このガイダンスの 5.4 章に紹介するソフトウェアエンジニアリング基礎知識体系（SWEBOK）などで概要を知ることができるので，参考にするのも良い。

組み込みソフトウェアの場合，例えば次のように組織の成熟度に応じてソフトウェア開発モデルを段階的に使いこなすことも良いだろう。

(1) まず，ウォーターフォールモデルを理解する。これは，開発をトップダウンで行うモデルで，各**アクティビティ**を順次実施する，もっとも単純なモデルである。これは，ひとつ前の**アクティビティ**に間違いが無いことを前提としていて，間違いがあった時の後戻りを考慮していないモデルと言える。

(2) Ｖ字開発モデルを意識して，ソフトウェア開発**プロセス**を構築する。Ｖ字開発モデルは，設計工程とテスト工程との関係に注目したモデルであるが，同時に，後工程からのフィードバックに注目したモデルでもある。**成果物**を**検証**し，フィードバックによる修正を計画に考慮し，高品質を目指す。このとき，テスト専門チームを作り，テスト能力の会得を目指す。

(3) テストチームが熟練してきたら（特に設計書読解とテスト設計の熟練），設計の**成果物**をテストチームがレビューする**タスク**を**プロセス**に含めることにより，Wモデルへ移行し，更なる高品質を目指す。Wモデルは，レビューをＶモデルよりも重視し，設計の上流での品質向上を意図したモデルであり，後工程での欠陥修正の削減を期待できるモデルである。ただし，Wモデルの実施には相応の能力が必要である。また，テスト工程の前倒し（例えば上流でのテストケース作成）ではないことを理解することが重要である。

なお，実施すべき**アクティビティ**及び**タスク**を，**ソフトウェア安全クラス**に基づいて選択することを，この規格は要求するが，**ソフトウェアアイテム**の**ソフトウェア安全クラス**は，基本的にはソフトウェア**アーキテクチャ**設計の後でないと明確にできないだろう。そのため，**プロセス**の構築が難しいかもしれないが，**ソフトウェアアイテム**の**ソフトウェア安全クラス**を明確化する**タスク**を**プロセス**上に定めて段階的に設計を進める**プロセス**としても良いし，この部分はフィードバックによる**プロセス**の反復と捉えても良いだろう

この規格は，特定のソフトウェア開発モデルを要求しないが，箇条 5.1.1 において，どのような開発**プロ**

セスを用いるのか計画することを求める。また，その**プロセス**の各**アクティビティ**及び**タスク**の**成果物**の計画を求められる。この計画においては，次を考慮することが重要である。

Tech. Tips

W（字型）モデル

V（字型）モデルのデメリットを補えるモデルとして，W モデルがある。W モデルでは、V 字型モデルの右部分の試験**プロセス**で行われる作業のうち，試験設計を左部分で行う。このため，要求分析，基本設計，詳細設計の各設計**プロセス**と，**システム**試験設計，機能試験設計・結合試験設計，単体試験設計の各試験**プロセス**とが並行して行われることになる。メリットは，開発の初期段階で試験設計を行うことで，要求や設計の抜け，漏れ，あいまいな点，矛盾点などを見つけることが可能となり，設計**プロセス**から，より品質を高めることができる。デメリットとしては，設計**プロセス**で仕様変更が発生した場合，同時に試験設計の見直しも必要になり，見直しの必要な範囲が拡大する可能性がある。

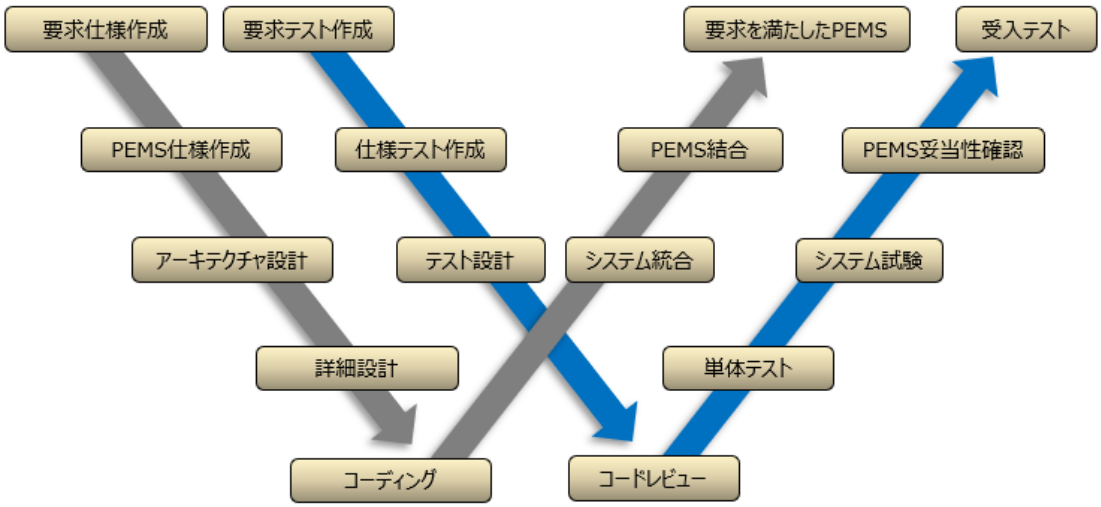


図 5-5 W（字型)モデルの概念図

Wモデルの効果的な実施には相応の能力が必要である。よくあるケースとしては，開発上流でＶ字設計の対になるテストケースを単純に作成してしまう取り組みを行うと、設計が進み，仕様変更が発生したときに，テストケースの修正が発生し，また仕様変更によりテストケースを修正し・・・，結果として無駄な工数が積みあがっていく。そして，何のメリットも得られなかったことに気付く場合がある。

目的は，あくまで上流でテストの難易度や注意点を把握した上でテスト要求を検討したり，テスト設計を行い，ベースとなる要求仕様書や設計書の弱いところをあぶり出すことを認識すべきである。

(参考和訳)
次の原則は，使用する**ソフトウェア開発ライフサイクルモデル**にかかわらず重要である。
– 全ての**プロセス**アウトプットの整合性を維持することが望ましい。**プロセス**アウトプットを作成する又は変更するときは，関連する全ての**プロセス**アウトプットを直ちに更新して，相互の整合性を維持し，この規格が明示的又は暗示的に要求している全ての依存性を維持することが望ましい。
– **プロセス**アウトプットは，ソフトウェアについて更に作業するためのインプットとして必要なとき，全てが利用可能になっていることが望ましい。
– **医療機器ソフトウェア**を**リリース**する前の段階で，全ての**プロセス**アウトプットに相互に整合性があり，この規格が明示的又は暗示的に要求している**プロセス**アウトプット間の依存性が，全てあることが望ましい。
（附属書 B）

アウトプットの整合性とは，例えば，ソフトウェア要求事項に無い機能が，ソフトウェア**アーキテクチャ**設計の**成果物**に記述されていないことや，ソフトウェア**アーキテクチャ**設計で**ソフトウェアアイテム**に割り振られた仕様と詳細設計における**ソフトウェアアイテム**の仕様が一致していること，設計された仕様に対して実施した試験の内容が適切であること，などである。ソフトウェア開発**プロセス**の各**アクティビティ**の全ての**成果物**について整合していること，つまり相互に矛盾が無く一貫性があることは，ソフトウェアの品質を高め**安全**を確実にするために重要である。この整合性を維持するためには，**トレーサビリティ**の確認が重要である。

トレーサビリティ（追跡性ともいう）とは，各**アクティビティ**の入力の各事項と出力の各事項との間の関係が追えることと理解して良い。各**アクティビティ**での**トレーサビリティ**を明確にすれば，その結果，ある**システム安全**要求（例えば**リスクコントロール**手段の要求）が，どのソフトウェア要求事項として定められ，それがソフトウェア**アーキテクチャ**設計の結果にどのように反映され，それがソフトウェア詳細設計でどのように実現され，それらをどのように**検証**し，**検証**結果がどうであったかが，追跡（トレース）できる。この追跡は，逆方向にも追跡できることが重要である。

ソフトウェア開発**プロセス**のアウトプットとして何が必要かを考えるとき，例えば次の観点を考慮することが望ましい。

- ある**アクティビティ**に注目したとき，その**アクティビティ**は，次の**アクティビティ**が適切に実施できるように，適切な情報を用意し**成果物**として出力することが重要である（図 5-6 参照）。その観点で，必要な情報が網羅されるように**成果物**を作成することが望ましい。

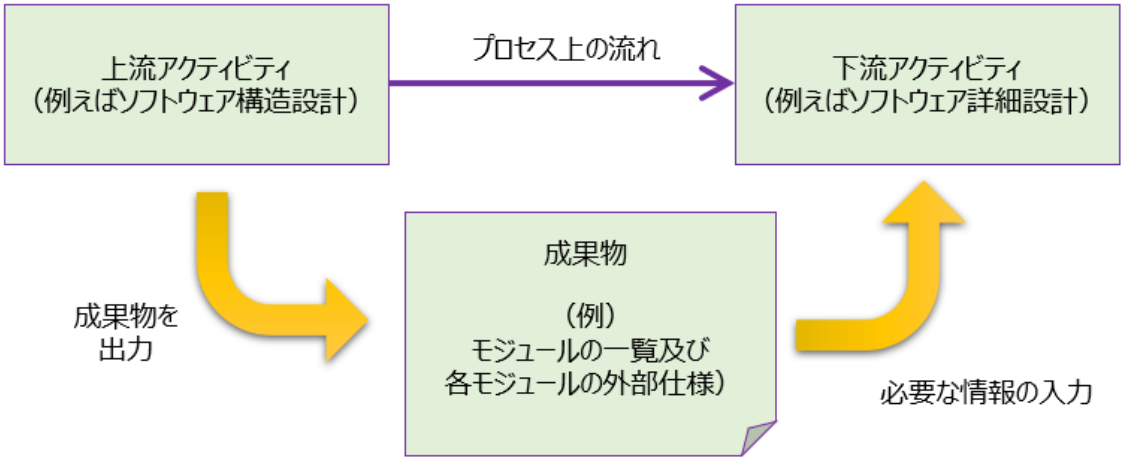


図 5-6 上流アクティビティの出力と下流アクティビティの入力の関係

- ソフトウェアは，後日に保守が行われることが予定される。保守を行う場合，ソフトウェアをどのように変更するかを検討し，それによる弊害の無いこと（特に**リスク**の増大の無いこと）を確認しなければならない。そのとき，既存のソフトウェアに関し，**トレーサビリティ**が確保され，利用できる適切な情報が充分に維持されていることが重要である。

5.1.6 この規格への適合を依頼する場合のマネジメント

ここまで，この規格の要求概要を説明し，大まかなソフトウェア開発のイメージが出来たことを期待する。この章では，ソフトウェア開発を，社内のソフトウェア開発チーム又は社外に依頼する場合に，併せてこの規格への適合を依頼する場合を考えてみる。

その場合，依頼内容に「IEC 62304 への適合」を含めただけでは不充分である。この規格への適合は，ソフトウェア開発側だけの努力では実現できないためである。

この規格への適合は，以下を考慮したマネジメントが求められる。

- この規格は，単独で用いることができず，他の規格と組み合わせて使用する必要がある。これは，業務的にも連携の必要性があると理解することができる。
- ソフトウェア開発**プロセス**への入力（主に何を開発すべきかの指示）と出力（主に**システム**側へのソフトウェア**リリース**）に関して，**システム**開発側とソフトウェア開発側との協力が重要な事項があり，そのためのマネジメントが求められる。このガイダンスで後述する 5.3.6 章を参照されたい。
- ソフトウェア**リスクマネジメント**（規格の箇条 7）を適切に実施するためには，製品全体の**リスクマネジメント**との整合及び連携が重要であり，そのためのマネジメントが求められる。このガイダンスの 5.3.3 章の説明が参考になれば幸いである。
- 例えば，IEC 60601-1 は，この規格を引用するにあたり，箇条 6 のソフトウェア保守を除外している。一方でこの規格には，箇条 6 に重要な要求が規定されている。ここをどう扱うかは，規格の問題というより，運用範囲の問題と位置付けるのが適切と考える。そのため，

依頼側が目的を把握し運用範囲を明確にすることが求められる。このガイダンスの 5.3.2 章の説明が参考になれば幸いである。

以上を考慮すると，この規格への適合のためのマネジメントは，**PEMS システム**開発側（つまりソフトウェア開発を依頼する側）が主導して行うことが望ましい。一方，この規格に適合する**プロセス**の実施は，ソフトウェア開発側が主導して行うのが良いだろう。

この 5.1 章では，この規格の目的と，この規格が**プロセス**管理に重点をおく理由。および，要求の概要と進め方の流れを概説した。次章からは，この規格の要求条文に従って，ソフトウェア**開発ライフサイクル**の**プロセス**ごとの活動要求の説明（5.3 章）と，全**プロセス**を通じての一般要求事項（5.2 章）を説明する。

5.2 IEC 62304 の一般要求事項（箇条 4）

5.2.1 品質マネジメントシステム（箇条 4.1）

この規格は，『顧客要求事項及び該当する規制要求事項に適合する**医療機器ソフトウェア**を提供する能力があることを実証する』ことを求めている。これは，次により実証できるとしている。

- ISO 13485「**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」
- **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

ISO 13485 は，表題にあるように，**医療機器**を意図した規格である（一部，**医療機器**らしい視点の要求事項がある。）。我が国では介護は医療とは区別されるものの，国際的には，ISO 21856 は**医療機器**と見做される福祉機器を対象とするため，ISO 13485 を適用することも，合理性があると言える。，

日本以外の場合は，次のいずれかにより実証できるとされるが，国や地域により規制が異なるため，仕向け国の省令等について情報を収集して対処されたい。

- ISO 13485; or
- a national quality management system standard; or
- a quality management system required by national regulation.

注記 ，ISO 21856，IEC 60601-1 の箇条 14.1 の要求事項に基づいて，この規格の箇条を適用する場合，（規制当局などからの要求が無い限り）厳密にはこの箇条は適用することは言及していない。，その場合でも，この箇条の要求事項の主旨から，ソフトウェア品質が向上するような品質管理環境を構築することを考慮すべきである。

5.2.2 リスクマネジメント（箇条 4.2）

規格は，次の規格に規定した**リスクマネジメントプロセス**の適用を求める。

- ISO 14971「**医療機器** ― **リスクマネジメント**の**医療機器**への適用」

ロボット介護機器の**リスクマネジメント**については，『第 3 章 **リスクマネジメント**実施ガイド』に詳述している。**PEMS システム**開発時だけでなく，ソフトウェア開発**プロセス**においても，ソフトウェア設計に起因する**リスク**を反復して洗い出し，コントロールしていくことが求められる。そのため，この規格の箇条 7 において，ソフトウェア**リスクマネジメントプロセス**の要求事項も規定している。ソフトウェア**リスクマネジメントプロセス**については，このガイダンスの 5.3.3 章で解説している。

5.2.3 ソフトウェア安全クラス分類（箇条 4.3）

4.3 ソフトウェア安全クラス分類

(参考和訳)

a）**製造業者**は，**ソフトウェアシステム**に起因する**危険状態**が，最悪の場合に患者，操作者，又はその他の人にもたらす**危害**の**リスク**に応じて，図 3 に示すように，各**ソフトウェアシステム**をソフトウェア**安全**クラス（A，B 又は C）に分類する

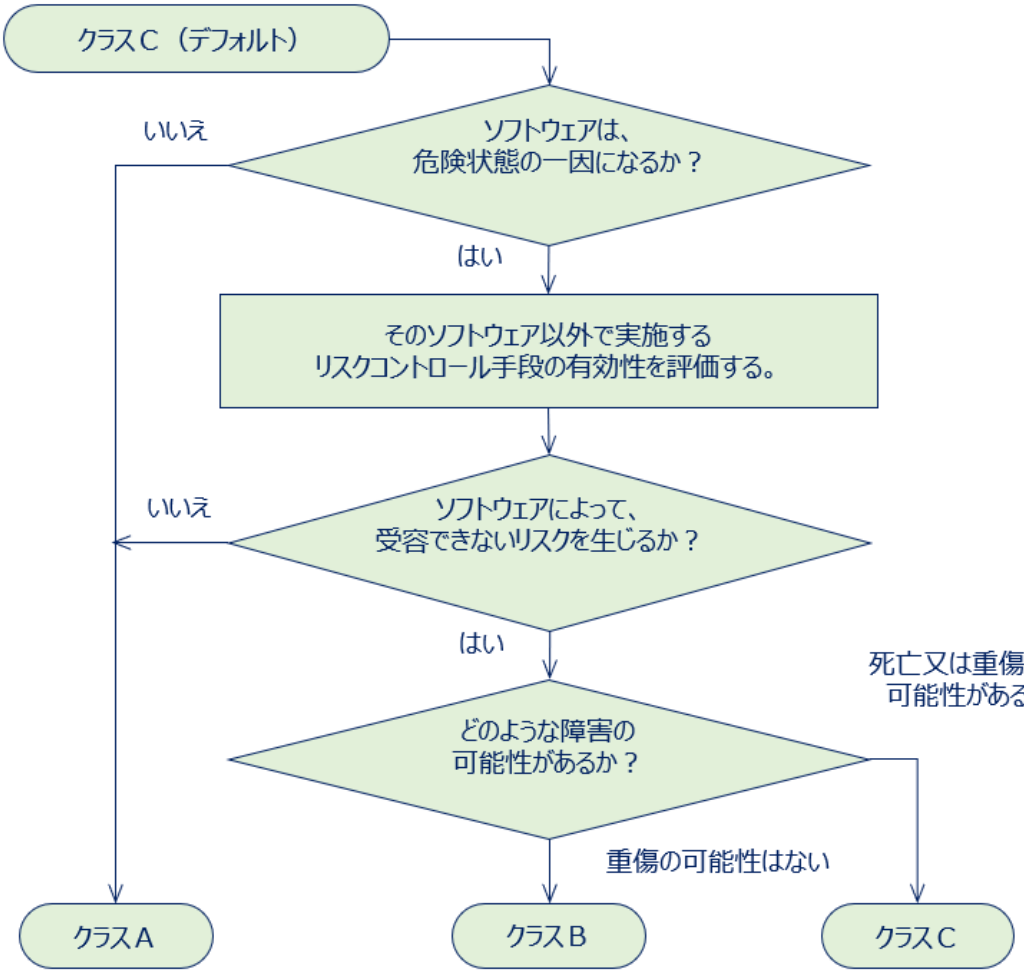


図３　ソフトウェア安全クラスの割当て

ソフトウェアシステムのソフトウェア**安全**クラスが A となるのは，次のいずれかの場合である。

－　**ソフトウェアシステム**が**危険状態**の一因とならない場合。

－　**ソフトウェアシステム**が**危険状態**の一因となるが，その**ソフトウェアシステム**以外（external to）で実施する**リスクコントロール**手段を考慮すれば，受容できない**リスク**は生じない場合。

ソフトウェアシステムのソフトウェア**安全**クラスが B となるのは，次の場合である。

－　**ソフトウェアシステム**が**危険状態**の一因となり，その**ソフトウェアシステム**以外で実施する**リスクコント**

ロール手段を考慮しても，受容できない**リスク**が生じる場合で，**重傷**の可能性はない場合。
ソフトウェアシステムのソフトウェア**安全**クラスが C となるのは，次の場合である。
－ **ソフトウェアシステム**が**危険状態**の一因となり，その**ソフトウェアシステム**以外で実施する**リスクコントロール**手段を考慮しても，受容できない**リスク**が生じる場合で，死亡又は**重傷**の可能性がある場合。
当初，ソフトウェア**安全**クラスを B 又は C に分類した**ソフトウェアシステム**について，**製造業者**は，その**ソフトウェアシステム**以外（external to）で実施する**リスクコントロール**手段（その**ソフトウェアシステム**が含まれる**システムアーキテクチャ**の改善など）を追加で実施して，その**ソフトウェアシステム**を新しいソフトウェア**安全**クラスに分類することができる。
注記 1 その**ソフトウェアシステム**以外で実施する**リスクコントロール**手段は，ソフトウェアが**危険状態**の一因となる可能性を最小限に抑えるために，ハードウェア，独立した**ソフトウェアシステム**，医療処置又は他の手段とすることができる。
注記 2 **リスク**の受容可能性の定義は，ISO 14971 の 3.2（経営者の責任）を参照する。
b) （対応国際規格で削除されている。）
c) **製造業者**は，分類した各**ソフトウェアシステム**の**安全**クラスを，**リスクマネジメントファイル**に文書化する。
d) **製造業者**は，**ソフトウェアシステム**を**ソフトウェアアイテム**に分割する場合，及び**ソフトウェアアイテム**を更に幾つかの**ソフトウェアアイテム**に分割する場合，それらの**ソフトウェアアイテム**は，元の**ソフトウェアアイテム**（又は**ソフトウェアシステム**）のソフトウェア**安全**クラスを継承する。ただし，別のソフトウェア**安全**クラスに分類することの正当な根拠を文書で示せば，その分類を変更してもよい。根拠の文書化に当たっては，新しい**ソフトウェアアイテム**をどのように分離するのかを説明して，別分類としてもよいことを示す［ソフトウェア**安全**クラスは，4.3 a) の “**ソフトウェアシステム**” を “**ソフトウェアアイテム**” に読み替えて分類する。］。
e) 分割によって作成した**ソフトウェアアイテム**のソフトウェア**安全**クラスが，元の**ソフトウェアアイテム**のクラスと異なる場合，**製造業者**は，各**ソフトウェアアイテム**のソフトウェア**安全**クラスを文書化する。
f) この規格をある**ソフトウェアアイテム**のグループに適用する場合，この規格に適合するためには，**製造業者**は，そのグループの中で最も高い**安全**クラスに分類している**ソフトウェアアイテム**が必要とする**プロセス**及び**タスク**を使用する。ただし，**リスクマネジメントファイル**の中で根拠を示すことによって，より低いクラスの**プロセス**及び**タスク**を使用できる。
g) ソフトウェア**安全**クラスを分類するまで，各**ソフトウェアシステム**には，クラス C の要求事項を適用する。

この箇条では，**ソフトウェアシステム**を，以下のいずれかのソフトウェア**安全**クラスに分類（classification）することを要求している。分類の条件は，次の表のとおりである。

表 5-3 ソフトウェアシステムのソフトウェア安全クラスの分類条件

ソフトウェア**安全**クラス	分類条件
クラス A	次のいずれかの場合： – **ソフトウェアシステム**が**危険状態**の一因とならない場合。 – **ソフトウェアシステム**が**危険状態**の一因となるが，その**ソフトウェアシステム**以外（外部）で実施する**リスクコントロール**手段を考慮すれば，受容できない**リスク**は生じない場合。
クラス B	**ソフトウェアシステム**が**危険状態**の一因となり，その**ソフトウェアシステム**以外で実施する**リスクコントロール**手段を考慮しても，受容できない**リスク**が生じる場合で，かつ**重傷**の可能性はない場合。
クラス C	**ソフトウェアシステム**が**危険状態**の一因となり，その**ソフトウェアシステム**以外で実施する**リスクコントロール**手段を考慮しても，受容できない**リスク**が生じる場合で，かつ死亡又は**重傷**の可能性がある場合。

上記の分類を行うとき，**危険状態**の発生がソフトウェアに起因する場合は，一般に**危害**の発生確率を１（100%）とする。**リスク**の定義は，**危害**の発生確率とその**危害**の**重大さ**の組み合わせであるが，ソフトウェアの**故障**発生確率（欠陥が顕在化する確率）を定量的に推定する広く認められた方法は無く，一般には発生確率を考慮することができない，という考えに基づき，**危害**の**重大さ**のみを考慮する。なお，ソフトウェア**安全**クラスの分類を行うとき，**ソフトウェアシステム**自体が持つ**リスクコントロール**手段は，前提として考慮しないこと。**ソフトウェアシステム**外部の**リスクコントロール**手段（例えばヒューズなどのハードウェア手段や，他の独立したソフトウェア手段など）を前提として考慮することはできる。また，**ソフトウェアシステム**外部の**リスクコントロール**手段を追加で実施して，**ソフトウェアシステム**を新しいソフトウェア**安全**クラスに分類することもできる。

分類が未確定の場合，クラス C と位置付ける必要がある。

ソフトウェアシステムをいくつかの**ソフトウェアアイテム**に分割する場合，各**ソフトウェアアイテム**のソフトウェア**安全**クラスは，基本的には元の**ソフトウェアシステム**のソフトウェア**安全**クラスを継承する必要がある。ただし，他のソフトウェア**安全**クラスに分類してよいという正当な根拠を示すことができれば，その**安全**性クラスに分類してよい。ここでいう正当な根拠の例としては，その部分の**リスク**が新たなソフトウェア**安全**クラスの分類について適切であることが示せ，かつその部分の独立性を確保することで，他のアイテムからの影響による**リスク**増大の可能性を充分に低減できている証拠を示せることなどである。**ソフトウェアアイテム**をさらに分割する場合も同様である。

分割による独立性とは，例えば，**プロセス**系 CPU にて制御される**ソフトウェアアイテム**の**障害**時**リスク**を，物理的に分離された保護系 CPU（メモリも異なるアドレス空間を使用）の**監視ソフトウェアアイテム**により受容可能な**リスク**レベルまで低減出来れば，**プロセス**系の**ソフトウェアアイテム**のクラスは C →

B or A に下げることが出来る可能性がある。（物理的な独立）
もしくは，一つの CPU しかない場合，**ソフトウェアシステム**を 2 つの**ソフトウェアアイテム**に分割し，保護系の**ソフトウェアアイテム**の実行を確実とするため，共有リソースのロックにより他のアイテムの処理をブロックする。または，利用可能なプロセッサ実行時間の割り当てを過度なほど高くするなど，他のアイテムからの論理的な干渉がないことを設計で示し，正常動作に加え，過負荷状態や**異常**時，**故障**時などあらゆるケースでの**リスク**を**検証**試験することで，本来は 2 つの**ソフトウェアアイテム**ともにクラス C が割り振られるところ，**プロセス**系のソフトアイテムをクラス B or A，保護系の**ソフトウェアアイテム**をクラス C とすることが出来るだろう。但し，条件として，例えば，干渉が無いなど，クラス変更の根拠を示す必要がある。

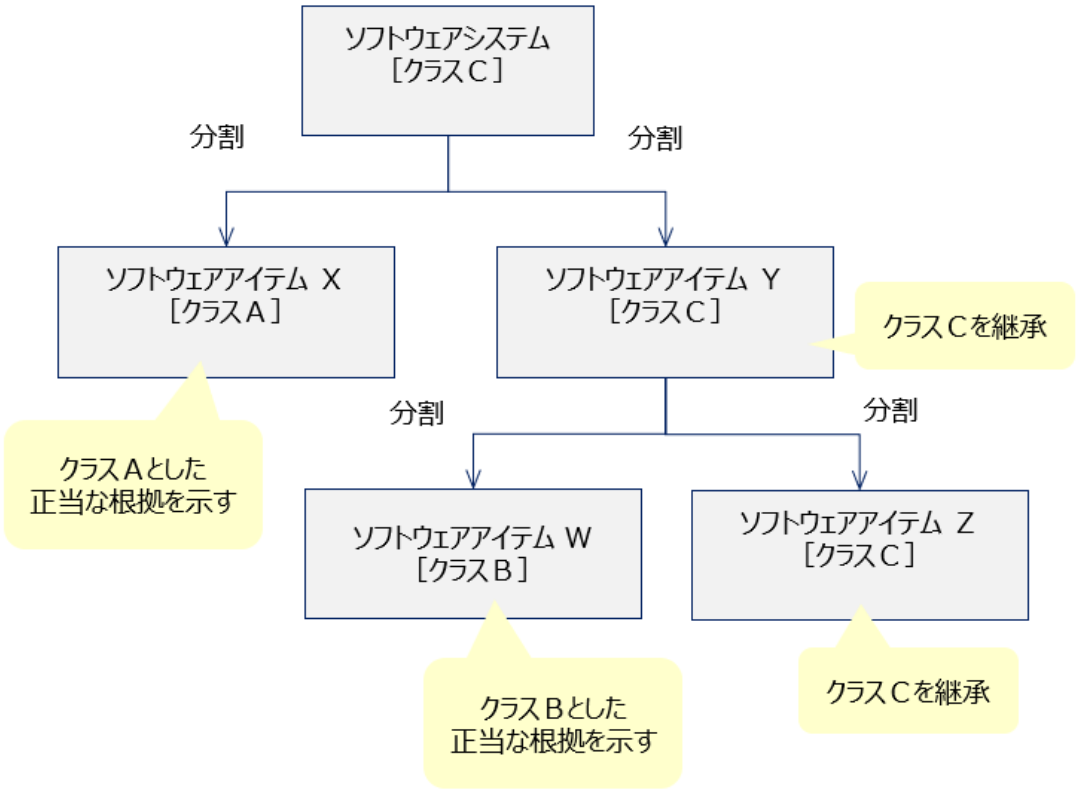


図 5-7 ソフトウェアシステム／ソフトウェアアイテムの分割とソフトウェア安全クラスの例

ソフトウェアの開発及び保守では，上記の通り分類されたソフトウェア**安全**クラスに基づいて，規格に要求された**アクティビティ／タスク**を実施する必要がある。どのソフトウェア**安全**クラスに対してどの箇条への適合が要求されるかについては，各箇条に明記されている。
ここでひとつ注意すべき点を述べる。**ソフトウェアアイテム**のソフトウェア**安全**クラスを決定できるのは，ソフトウェア**アーキテクチャ**が設計され，各**ソフトウェアアイテム**の役割や振る舞いが明らかになり，それにより**ソフトウェアアイテム**がどのように**リスク**と関係するかが明確になった後であろう。そのため，「ソフトウェア**安全**クラスを選定し，それに従ってソフトウェアを開発する。」という流れが，単純なウォーターフォールモデルに収まらない場合も考慮すべきである。例えば，**ソフトウェアシステム**のソフトウェア**安全**クラスを分類し，

それに基づいてソフトウェア開発計画及びソフトウェア**アーキテクチャ**設計を実施した後，**ソフトウェアアイテム**のソフトウェア**安全**クラスを選定し，それに基づき計画を見直し，必要に応じてソフトウェア開発計画の変更やソフトウェア**アーキテクチャ**設計の変更を実施する進め方があると考える。この場合，当初のソフトウェア**安全**クラスの分類は，予備的なものと捉え，**プロセス**の省略を正当化する目的に使用しないことが重要である。

5.2.4 レガシーソフトウェア（箇条 4.4）

4.4.1 一般

ソフトウェアの特長として非連続性があり，たとえ，小さな変更でも**システム**全体にインパクトを与え得る。そこで，巨大な**ソフトウェアシステム**に対して，小さな変更をかける時，何をすべきかの明瞭さを与えるために，この箇条 4.4 の要求が存在する。

レガシーソフトウェアとは，「当時の法規制に適合して市場に出荷され，現在も市販されているが，この規格の現行版に適合して開発された。という客観的な証拠が不十分な**医療機器ソフトウェア**のこと。」である。地域によっては，この規格の現行版ができる前に設計されたものであっても，規制当局の承認を得るために，**製造業者**が規格への適合性を示さなければならないことがある。そのような場合に，この箇条 4.4 に規定する方法によって，**レガシーソフトウェア**が規格に適合していることを示すことができる。

レガシーソフトウェアの場合は，箇条 5 を適用する代わりに，箇条 4.4.2～4.4.5 を適用して，この規格への適合性を示すことが可能である。これは，出荷当時の規制とこの規格の要求事項との差分を分析してその差分を解消した**り，リスクマネジメント**視点の再確認をしたりすることによって，適合性を実証する方法である。

この箇条 4.4 の要求事項は，次を前提としている。

- 必要な**アクティビティ**及びそれに伴う文書化は，可能な限り既存の文書を信頼して，これを活用する。
- **製造業者**は，**リスク**を低減するために，リソースをできるだけ有効活用する。

これらの前提の下，実行する必要のある**アクティビティ**を特定し，収集すべき客観的な証拠を集め，**レガシーソフトウェア**を**安全**に継続使用できる根拠としてまとめるのが，この箇条 4.4 が示す**プロセス**の内容である。

注記　なお，この箇条 4.4 が適用できる条件については，確認が必要な場合があるかもしれない。例えば次のような件については，必要に応じて規制当局又は認証機関に確認されたい。

IEC 60601-1 の箇条 14.1 の要求事項に基づいてこの規格の箇条を適用する場合，基本的にはこの箇条 4.4 を適用することに言及していない。これは IEC 60601-1 の適用範囲として保守**プロセス**を対象としていないことによるものと考える。

また，この箇条 4.4 は，**レガシーソフトウェア**を利用した**ソフトウェアシステム**の変更を許容する。これは，ソフトウェアの保守，または，後継機種の開発を目的とし，**レガシーソフトウェア**を再利用した派生開発の場合なども含まれる。

4.4.2 リスクマネジメントアクティビティ

箇条 4.2 が要求する ISO 14971 の規定に従って，次を実施する必要がある。

a) **レガシーソフトウェア**に関連する事故事例やヒヤリ・ハット事例について，情報を収集する必要がある。この情報収集は，製造後情報を含めて，社内／社外を問わずあらゆるフィードバックを活用する。そして収集した情報に基づき，**安全**性を**評価**する必要がある。

具体的には，機器の管理者や使用者などから，及び**製造業者**自身から，以下のように収集することが考**えら**れる。

- 既に上市している機器の使用者からのフィードバック
- **製造業者**が発見した**異常**
- **レガシーソフトウェア**に起因する有害事象
  （**医療機器**規制当局のデータベースの利用）PMDA や FDA WEB サイトの製品事故データベース。

収集した情報に基づく**安全**性の**評価**は，**リスク**に関する開発時の想定からの差異の分析を重視することが望ましい。

b) **レガシーソフトウェア**の継続使用に伴う**リスクマネジメントアクティビティ**を実施する必要がある。これは，次の点を考慮して実施する。

- **レガシーソフトウェア**の**医療機器アーキテクチャ**全体への統合
- **レガシーソフトウェア**の一部として実装した**リスクコントロール**手段の継続的有効性
- **レガシーソフトウェア**の継続使用に伴う**危険状態**の特定
- **レガシーソフトウェア**が**危険状態**の一因となる場合の潜在的原因の特定
- **レガシーソフトウェア**が**危険状態**の一因となる場合の潜在的原因のそれぞれに対する**リスクコントロール**手段の定義

規格の附属書 B の B.4.4 の解説によれば，**レガシーソフトウェア**が，**ロボット**介護機器**アーキテクチャ**全体の中で，どのように使用されるかを特定することにより，考慮すべき**リスク**が変わるため，それを明確にして**リスクマネジメントアクティビティ**の入力とする。考慮すべき**リスク**について，次に例示する。

- **レガシーソフトウェア**が**安全**，かつ，確実に使用されていて，その継続使用を**製造業者**が希望する場合，継続使用の根拠は，主に製造後の**記録**に基づく**リスクアセスメント**による。【継続使用】
- **レガシーソフトウェア**を再利用して新しい**ソフトウェアシステム**を作成する場合，**レガシーソフトウェア**の**意図する使用**が当初のものと異なることがある。この場合，**レガシーソフトウェア**の**故障**に起因する**危険状態**を見直して，**リスクアセスメント**で考慮しなければならない。【再利用】
- 再利用する**レガシーソフトウェア**が，新しい**ソフトウェアシステム**に結合されている場合でも，同様の**意図する使用**に用いていることがあるかもしれない。この場合は，箇条 5.3 に従って，**アーキテクチャ**上の**リスクコントロール**手段を修正して，**リスクアセスメント**で考慮するのがよい。【再利用】

なお，**レガシーソフトウェア**を変更して新しい**ソフトウェアシステム**で使用する場合，**製造業者**は，これ

まで**安全**で確実に使用されていたことの**記録**が，変更によってどの程度無効になるか検討するのが望ましい。

リスクを見積もるとき，この規格は，ソフトウェアの**故障**（**障害**）の発生確率を 1 （100%）とする方針を示している。これは，ソフトウェアの**故障**（**障害**）の発生確率を定量的に見積もる方法については，合意が形成されていないと考えているためである。しかし，**レガシーソフトウェア**については，上記 a）で収集した情報の**評価**に基づいて，発生確率の定量的な推定が可能な場合があるであろう。（例；製造後の**記録**に基づく**リスクアセスメント**）
その場合，収集した情報が客観的な証拠であり，継続使用する根拠として示せればその確率値を使用して良い。ただし，ソフトウェアの使用条件の変化や，ソフトウェア又はハードウェアの設計変更などにより，既存の情報に基づく推定が無意味になる場合があるので注意されたい。
過去の災害事例として，アリアン 5 型ロケットは，アリアン 4 型ロケットで使用された，実績のあるソフトウェアを使用した。しかし，ロケットの加速度が増加していたため，オーバーフローが発生し，それが**異常**制御を引き起こして空中爆発してしまった。また，放射線治療機の Therac25 は，親機でのソフトウェアの実績に基づき，ソフトウェアの**故障**（**障害**）の確率を低く見積もっていたが，ハードウェア設計の違いにより隠れていたバグが危険な誤動作につながってしまい，患者の死亡事故を起こしてしまった。ソフトウェア内外に変更点がある場合は，それが**リスク**の増大につながっていないかどうかよく注意されたい。

Tech. Tips

『 アリアン 5 型ロケットが制御不能で 4 0 秒後に爆発 』
このロケットは打ち上げから約 30 秒後に誘導姿勢情報を完全に失った。これは、慣性座標**システム**のソフトに仕様と設計の**エラー**によるもので、この**エラー**は、ロケットの水平速度に関連する 64 ビット浮動小数点を 16 ビット符号付整数へ変換する際、数字が 16 ビット符号付整数として保存できる最大値の 32,768 を超えてしまい、変換が失敗に終わった。

被害金額	ロケットおよび積荷 5 億ドル
全経済損失	10 年にわたる開発費用 70 億ドル

(出展：特定非営利活動法人
失敗学会ホームページより)

4.4.3 ギャップ分析

レガシーソフトウェアのソフトウェア**安全**クラスを箇条 4.3 に従って明確にし，そのソフトウェア**安全**クラスに基づき，次の箇条の要求事項に対し，使用可能な**成果物**とのギャップ分析を行う必要がある。

- 箇条 5.2 ソフトウェア要求事項分析
- 箇条 5.3 ソフトウェア**アーキテクチャ**設計
- 箇条 5.7 **ソフトウェアシステム**試験
- 箇条 7 ソフトウェア**リスクマネジメントプロセス**

規格の附属書 B の B.4.4 によれば，上記以外の箇条については，例えば詳細設計及びユニット**検証**については，目的が計画に明示されずに，ただ**アクティビティ**を実施する（及びその結果を**記録**する）だけでは，実施をする利点（**リスク**を低減する効果）がほとんどないか，または全くない可能性がある。その理由により，上記以外の箇条に対するギャップ分析は，要求事項には含まれていない。

ギャップ分析は，次のように実施する。

a) **製造業者**は，使用可能な**成果物**の継続的有効性を**評価**する。
レガシーソフトウェアについての既存の各**成果物**について，上記の各箇条が要求する文書として有効であるかを**評価**し，もしギャップ（不足している差分）があれば，そのギャップを特定する。

b) ギャップが特定された場合，**製造業者**は，不足する**成果物**を作成し関連**アクティビティ**を実施することによって，**リスク**をどの程度低減できるか**評価**する。
上記 a) で特定されたギャップがあれば，そのギャップについて，不足に関連する**アクティビティ**を実施して**成果物**の不足分を作成することにより，（**リスク**を充分に低減して）規格の要求事項に適合できるかどうかを判断する。

c) **製造業者**は，この**評価**に基づいて，作成する**成果物**と実施する関連**アクティビティ**とを決定する。**成果物**は，少なくとも**ソフトウェアシステム**試験**記録**（5.7.5 参照）を含むものとする。
上記 b) の結果に基づき，作成すべき**成果物**，及び（その**成果物**に関連して）実施すべき**アクティビティ**を決定する。

この箇条の注記にあるように，**レガシーソフトウェア**に実装された**リスクコントロール**手段について，それらを要求する旨がソフトウェア要求事項として**成果物**に明示されていることは重要である。つまり，該当する要求事項が無ければ，それはギャップのひとつである。また，この箇条の c) に記述されたとおり，各ソフトウェア要求事項に対する**検証**が適切に実施されたことを示す**ソフトウェアシステム**試験の**記録**の存在も重要である。

4.4.4 ギャップ解消アクティビティ

ギャップ解消は，次のように計画し及び実行する必要がある。

a) **製造業者**は，特定した**成果物**を作成するための計画を確立し実行する。客観的な証拠を利用できる場合は，5.2，5.3，5.7 及び箇条 7 で要求する**アクティビティ**を行わずに，その証拠を用いて必要な**成果物**を作成してもよい。
特定されたギャップを解消するために，箇条 4.4.3 の c) で特定された，作成すべき**成果物**を作

成し，及び実施すべき**アクティビティ**を実施するための計画を作成する必要がある。

b) **成果物**の作成に利用できる既存の証拠（例えば文書化されていない設計**記録**や試験**記録**など）が存在すれば，それらを用いても良く，その結果，**成果物**の作成に関連する**アクティビティ**を実施する必要が無ければ，実施しなくても良い。

c) この計画では，箇条 9 に従って発見した**レガシーソフトウェア**及び**成果物**の問題に対処するため，問題解決**プロセス**を使用する。

この計画には，箇条 9 に基づいて問題解決**プロセス**を使用することを含める必要がある。問題解決**プロセス**は，**レガシーソフトウェア**及び**成果物**の問題に対処するために使用する。

レガシーソフトウェアに対する変更は，箇条 6 に従って実施する。

レガシーソフトウェアの変更は，この規格においては，箇条 6 のソフトウェア保守**プロセス**に従って実施する必要がある。

4.4.5 レガシーソフトウェアを使用する根拠

レガシーソフトウェアを継続使用する根拠を，文書化する必要がある。この文書には，継続使用する**レガシーソフトウェア**の**バージョン**を含める必要がある。

この規格の箇条 4.4 の要求事項に従って，利用可能な既存の情報を収集してギャップを分析し，不足を埋めるための**タスク**及び文書化を実施して，継続使用するための根拠とする。

5.3 ソフトウェアライフサイクルの実施方法 （IEC 62304 箇条 5～9)

ロボット介護機器の**ソフトウェアライフサイクル**での各**プロセス**における要求と具体的な取組みを解説する。

この規格の構造は，箇条ごとに“**プロセス**”が規定され，その**プロセス**に従属する“**アクティビティ**”が，細分箇条になっており，その**アクティビティ**内で行う“**タスク**”が，さらに下層の細分箇条の中で定義されている。箇条の構造は以下の通り。

- 箇条 5 ソフトウエア開発**プロセス** （**プロセス**）
- 細分箇条 5.1 ソフトウェア開発計画 （**アクティビティ**）
- 細分箇条 5.1.1 ソフトウエア開発計画 （**タスク**）

この**プロセス**構成の概念は ISO/IEC 12207（JIS X 0160（IDT））「**ソフトウェアライフサイクルプロセス**]にて定義され，この規格の箇条 5～9 で参照されている。

プロセス，**アクティビティ**，**タスク**の意味，関係は**図 5-8** のとおり。

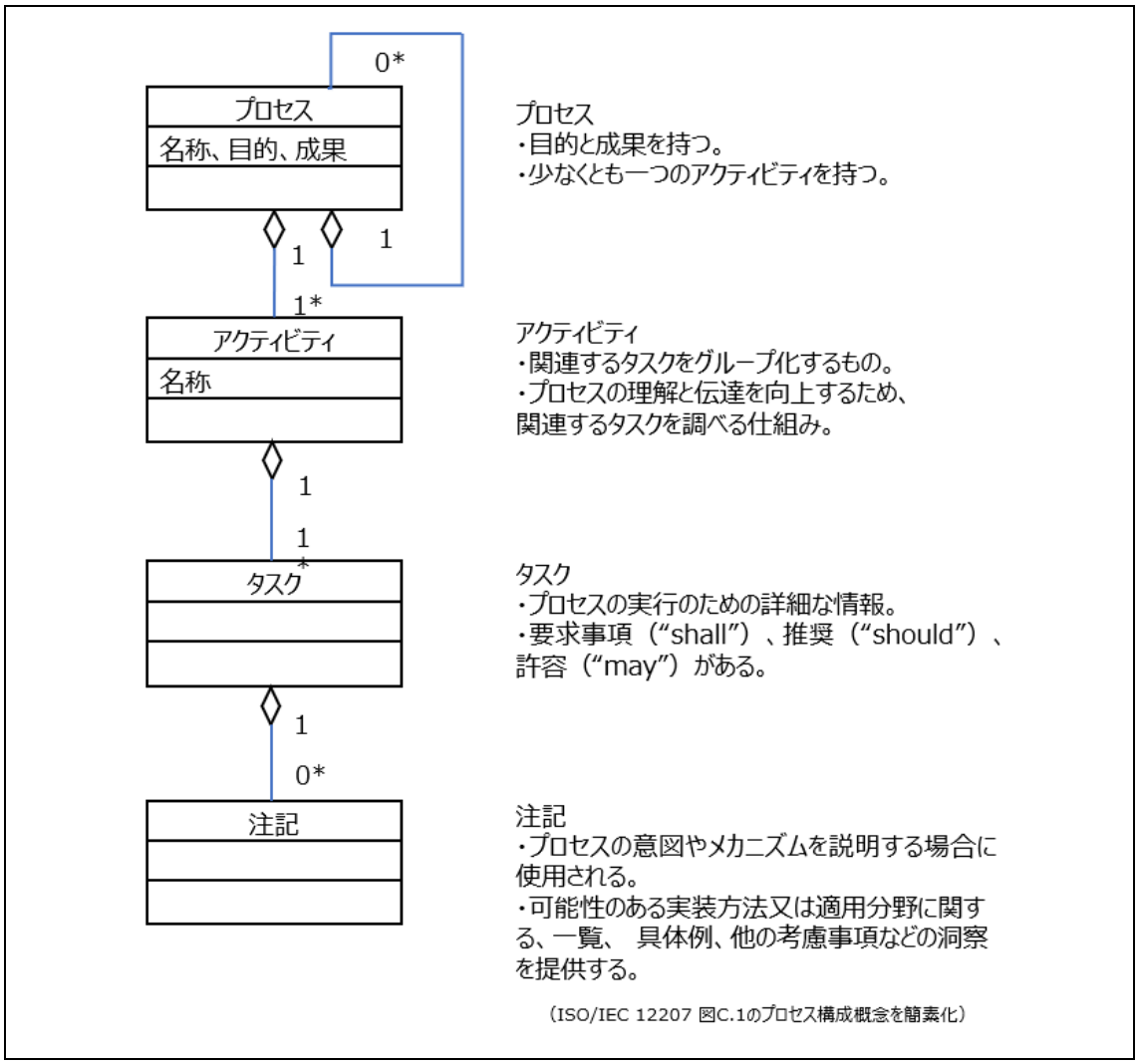


図 5-8 プロセス構成概念

5.3.1 ソフトウェア開発プロセス （箇条 5）

ソフトウェアの開発は，この箇条に規定されたソフトウェア開発**プロセス**を用いて実施する。ソフトウェアを開発した後のソフトウェア保守については，箇条 6 ソフトウェア保守**プロセス**を用いる。
ソフトウェア開発**プロセス**は，示すように

，一連の**アクティビティ**で構成され，規格の細分箇条ごとに示されている。全体の概要を，下図 5 9 に示す。

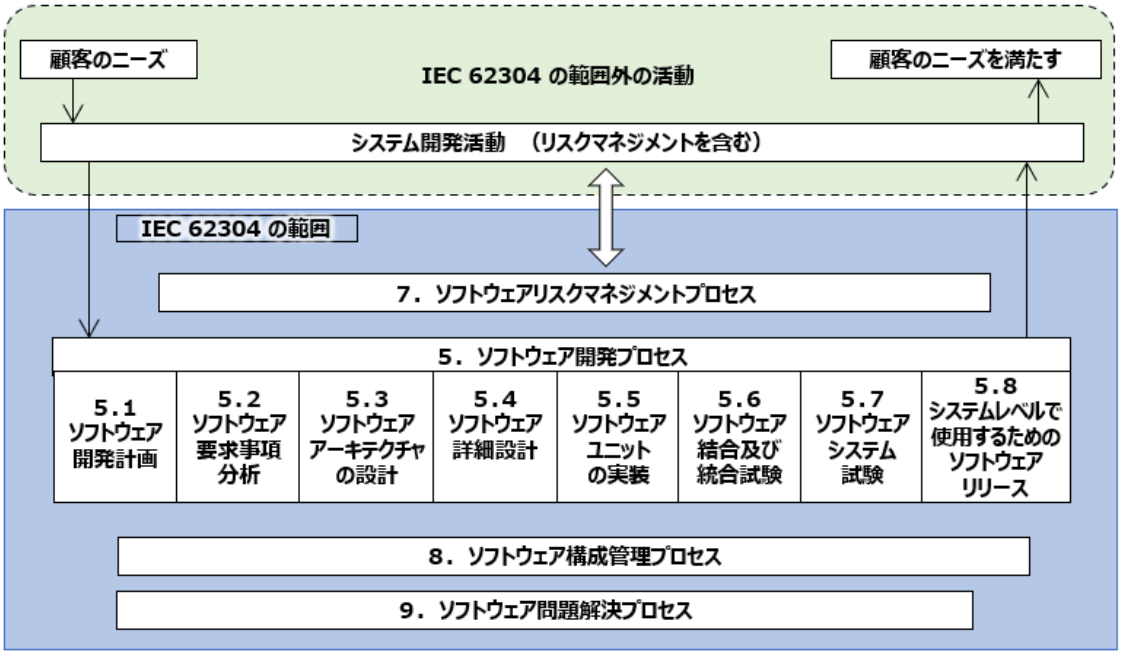


図 5-9 ソフトウェア開発プロセスの概要

ソフトウェア開発**プロセス**の実施については，箇条 4.3 に従って分類したソフトウェア**安全**クラスに基づいて，規格にて要求された**アクティビティ**／**タスク**を実施する必要がある。
どのソフトウェア**安全**クラスの場合に，どの**アクティビティ**及び**タスク**を実施するかは，各箇条の説明を参照されたい。

① ソフトウェア開発計画

5.1.1 ソフトウェア開発計画

ソフトウェア開発計画を確立する必要がある。その計画が示す**プロセス**の**アクティビティ**は，開発する**ソフトウェアシステム**の適用範囲，規模及びソフトウェア**安全**クラス分類に適したものである必要がある。
ソフトウェア開発計画の目的は，附属書 B によれば，『ソフトウェアに起因する**リスク**を低減するためのソフトウェア開発**タスク**を計画し，開発チームのメンバーに**手順**及び目標を周知し，ソフトウェアの**システム**

品質要求事項に確実に適合することである』。ソフトウェア開発を成功させるためには，事前の適切な計画の作成と，計画に基づく管理が重要である（PDCA が重要という言い方をしても良いだろう）。作成が初めてのため何を書くべきか悩んだ場合は，今までの業務における計画書と，この規格の要求事項の，両方を考慮してバランスをとるところから始めることを提案する。計画は，複数の計画に分かれていても良い（例えば複数のチームに対し分割された計画を立てる場合など）。また，製造事業者によっては，すでに適切な計画（または計画の部分）が規程として定められているかもしれない。そのような場合は，その規程を引用しても良い。計画の詳細度について，**リスク**が高い**ソフトウェアシステム**及びアイテムに対しては，より詳細に計画することが望ましい。

計画は，次を含む必要がある。

a) **ソフトウェアシステム**の開発に使用する**プロセス**

どのような**プロセス**で**ソフトウェアシステム**を開発するのかを計画する必要がある。この規格は，ソフトウェア開発の**プロセス**を具体的に指定してはいない。図 5-9 に示された**プロセス**は，規格の要求事項が，おおよそそのようなイメージで並べられているという説明でしかないと理解するのが良い。一方，実際の業務については，業務**プロセス**を明確に計画しなければならない。これは，どのような**アクティビティ**及び**タスク**があるのか明確であり，その依存関係が明確であり，及びそれらの**成果物**が何であるか明確である水準で記述する必要がある。この計画は，適切なソフトウェア品質を確保するために重要である。

b) **アクティビティ**及び**タスク**の**成果物**（文書化を含む。）

各**アクティビティ**及び**タスク**の実施結果として，作成されるべき**成果物**を記述する必要がある。これは，文書名などの識別名，及びそれぞれに記述される内容又は**記録**される内容を明示するか，あるいはそれらを明確化する計画を立てることが望ましい。**成果物**については，少なくともこの規格が文書化を要求する内容を記述する文書を含める必要がある。それ以外にも，計画したソフトウェア開発**プロセス**において，作成することが計画された設計書や，**タスク**を実施した結果の**記録**（例えば各**検証記録**）なども含めることが重要である。

c) **システム**要求事項，ソフトウェア要求事項，**ソフトウェアシステム**試験及びソフトウェアに実装する**リスクコントロール**手段の間の**トレーサビリティ**

ソフトウェア開発**プロセス**全体について，その入力と出力に関連する上記 4 種の文書間は**トレーサビリティ**を確保する必要があり，そのための計画を立てる必要がある。

この目的は，ソフトウェアに実装すべき**リスクコントロール**手段の実現に必要なソフトウェア要求事項の内容が，確実にソフトウェア開発**プロセス**に入力され，適切に実現され，及び確実に試験されるようにすることであり，さらには，それらにより確実に**リスクコントロール**がなされることを保証することにある。**トレーサビリティ**の明示の方法には，例えば，以下“技法の例”で説明する**トレーサビリティ**マトリクスを用いる方法がある。

d) **SOUP 構成アイテム**及び開発支援用ソフトウェアを含む，ソフトウェア**構成管理**及び変更管理

ソフトウェア**構成管理**及び変更管理について，その手段や**手順**などについて計画する必要がある。これは，規格の箇条 8 に適合できる内容である必要がある。計画する手段及び**手順**には，

SOUP **構成アイテム**や，開発支援ソフトウェアも含める。

SOUP とは，"**開発過程が不明なソフトウェア**，SOUP（software of unknown provenance"のことで，既に開発されていて一般に利用できるが，**医療機器**に組み込むことを目的に開発したものではない**ソフトウェアアイテム**［“OTS ソフトウェア（off-the-shelf：既製品）”として知られているソフトウェア］又は以前開発された**ソフトウェアアイテム**でその開発**プロセス**についての十分な**記録**が利用できないもの。と定義づけられている。この規格に合致した開発**プロセス**により作成されたことを証明できないソフトウェアであり，以下のようなソフトウェアと考えると良いだろう。

- **医療機器**に組み込むことを目的に開発したものではない既製品。
  例えば，市販の OS やオープンソースのデバイスドライバ，ライブラリなどは，一般的に SOUP にあたる。
- 以前開発された**ソフトウェアアイテム**で，その開発**プロセス**についての充分な**記録**が利用できないもの。
- また，開発支援用ソフトウェアとは，ソフトウェアを開発するときに使用するツール類のことで，統合開発環境，コンパイラ／リンカ，エディタ，静的解析ツール，メトリクス測定ツール，テストツール，**バージョン**管理ツールなどが考**えら**れる。

SOUP や，開発支援用ソフトウェアも，**ソフトウェアシステム**の**安全**性を決める**要素**として管理下にあると考える。適宜，使用目的や使用**バージョン**なども記述することが望ましい。

e) ライフサイクルの各段階で発見される**医療機器ソフトウェア**，**成果物**及び**アクティビティ**の問題に対処するためのソフトウェア問題解決

ソフトウェア問題解決について，その手段や手法について計画する必要がある。これは，規格の箇条 9 に適合できる内容である必要がある。一般的には，多数の問題を並行して処理することになるため，それを前提とした手法にする。

扱う問題は，ソフトウェアのコード上の問題だけではなく，各**アクティビティ**又は**タスク**の**成果物**の問題も扱うことが求められている。例えば，ソフトウェア構造設計書の記述ミスは，ソフトウェアの構造的欠陥を作る原因になりうる。つまり**安全**性を低下させる可能性が考**えら**れるため，ソフトウェア構造設計書の問題は管理する必要がある。どの**成果物**の問題が**安全**性の低下につながり得るのかを考えたうえで，どの**成果物**の問題を管理対象とするかを計画に含めることが望ましい。

また，扱う問題は，ソフトウェア試験の段階で発見されるものだけでなく，ソフトウェア開発**プロセス**の各段階で発見されるものを含む。また，それ以降の段階（**システム**試験や市場での使用の段階など）も考慮することが望ましい。よって，問題を扱う範囲・期間も考慮することが望ましい。

Tech. Tips

トレーサビリティマトリクス

トレーサビリティを確認する手段として，及び**トレーサビリティ**の確認結果の**記録**のため，**トレーサビリティ**マトリクスを使用する方法がある。

トレーサビリティマトリクスの書き方には，いくつかの方法がある。一つ目の例として，複数の文書間の関係をまとめて示す形式のイメージを図 5-10 に示す。ソフトウェアの構造がシンプルな場合に向いている。

システム要求仕様書	ソフトウェア要求仕様書		ソフトウェア構造設計書	ソフトウェア詳細設計書	ソフトウェア試験設計書	ソフトウェア試験結果
要求事項 ID	要求仕様 ID		構造仕様 ID	詳細設計 ID	試験分類 ID	試験**記録** ID
RQ01	SRQ01	SRS01-01	SA001	MU001	TS001	TR001
		SRS01-02	SA002	MU002	TS002	TR002
			SA003	MU003	TS003	TR003
		SRS01-03	SA004	MU004	TS004	TR004
…	…		…	…	…	…

図 5-10 トレーサビリティマトリクスの形式のイメージ（その１）

二つ目の例として，２つの文書の各項目間に関連がある場合に印を記す形式のイメージを**図 5-11** に示す。ソフトウェアの構造が比較的複雑な場合は，この形式を用いる方が良い。

		ソフトウェア構造設計書							
		<Group1>	Arch01-01	Arch 01-02	Arch 01-03	<Group2>	Arch 02-01	Arch 02-02	. . .
ソフトウェア要求仕様書	要求：SRQ01								
	要求仕様：SRQ01-01		●				●		
	要求仕様：SRQ01-02			●	●				
	要求仕様：SRQ01-03				●				
	要求：SRQ02								
	・ ・ ・								

図 5-11 トレーサビリティマトリクスの形式のイメージ（その２）

5.1.2 ソフトウェア開発計画の継続更新（クラス A，B，C）

開発の進捗に応じて，計画を見直し，適宜更新する必要がある。

開発は，事前に計画したとおりに実施することが適切であり続けるとは限らず，また，事前に詳細まで完全なものを立案できるとは限らない。例えば，ハードウェアやソフトウェアの設計及びそれらの**リスクマネジメント**の結果，**ソフトウェアシステム**のソフトウェア**安全**性クラスの指定を変える決定がなされるかもしれない。あるいは，製品設計の前提となる使用目的や使用条件が，顧客の希望により変更され，設計全体の見直しが必要になるかもしれない。開発が進むにつれて生じた状況変化や明らかになった詳細に応じ，より適切な計画へ更新する。

もし，計画をそのままに現実だけ変更すると，計画を無意味化させ，管理に関する混乱を招きかねず，それがソフトウェアの品質低下及び**安全**性低下を招きかねないと考える。現実を変更する場合は計画を更新するべきである。

どのような場合に計画を更新するのかルールを設けたり，計画を見直すためのマイルストーンを設けたりする（例えば新しい**アクティビティ**を開始する時点で見直す）など，更新に関する計画を開発計画に含めることが望ましい。

5.1.3 ソフトウェア開発計画におけるシステム設計及びシステム開発の引用 （クラス A，B，C）

ソフトウェア開発は，（**ロボット**介護機器の）**システム**開発との整合が取れている必要があるため，次の a）及び b）について，計画の中で明確にする必要がある。

もし，**システム**開発側がソフトウェアに期待したことと，ソフトウェア開発側が実現したこととが異なると，その差異により予期せぬ（期待外れの）結果を招き，**安全**性が脅かされることが起こり得ると考えるためである。

a） ソフトウェア開発のためのインプットとなる**システム**要求事項は，**製造業者**がソフトウェア開発計画の中で引用する。

・・・これは，ソフトウェア開発**プロセス**の入力（インプット）についての要求事項である。

ソフトウェア開発が適切に行われるためには，その前段として，**システム**開発において**システム**要求事項が適切に定義され，それをソフトウェア開発側が，正しく継承しなければならない。正しい継承のため，**システム**要求事項をソフトウェア開発計画の中で引用する。

引用の粒度（内容の詳細さ）は，少なくとも，要求事項を個別に識別できる状態において，どの要求事項（requirements）がソフトウェア側の担当であるかを識別できる水準である必要がある。可能であれば要求仕様（required specification）まで明確な状態で，引用することが望ましいが，要求仕様は，箇条 5.2 のソフトウェア要求事項分析を実施する中で明確化する計画でも良いと考える。

b） **製造業者**は，ソフトウェア開発計画に，4.1 に適合するために必要な，ソフトウェア開発と**システム**開発との整合性をとるための**手順**（**システム**結合，**検証**，**妥当性確認**など）を示すか又は引用する。

・・・これは，ソフトウェア開発**プロセス**の出力（アウトプット）についての要求事項である。

ソフトウェア開発**プロセス**の**成果物**として作成された**ソフトウェアシステム**が，**システム**(**PEMS**)と整合した適切なものであることを確認及び**評価**する必要がある。これは，箇条 4.1「品質マネジメント**システム**」に適合するためには必要である。

手順としては一般的に，**ソフトウェアシステム**を**システム**に組み込んだ後，**システム**要求事項（及び**システム**要求仕様）に基づき，**システム**側が意図した仕様どおりであるかどうか**検証**し，及び**システム**全体が適切に完成したかどうか**妥当性確認**をする。これらは，**システム**開発**プロセス**の一部であり，この規格の適用範囲外と考えることも可能であるが，これらの**タスク**について，ソフトウェア開発側も責任を持つべきである。よって，これらについて計画に含める必要がある。なお，**システム**開発において計画されたものを引用しても良いと考える。

なお，注記にあるように，**ソフトウェアシステム**がスタンドアロン**システム**の場合（例えば PC などの汎用機にインストールして使用するソフトウェアの場合）は，**ソフトウェアシステム**要求事項と**システム**要求事項とに差異がない場合もあり得る。その場合は，それを前提とする計画で良い。

5.1.4 ソフトウェア開発規格，方法及びツールの計画（クラス C）

ソフトウェア**安全**クラス C の場合，**ソフトウェアアイテム**の開発に関し，次の a) ～ c) を，計画に含める必要がある。なお，**ソフトウェアアイテム**の開発には直接は関わらない範囲に関しては，必ずしも含める必要は無いと考えるが，ソフトウェアの品質に影響がある**要素**は，含めることが望ましい。

a) 規格

・・・**ソフトウェアアイテム**を開発する時に適用すると決めた規格（又は規格的なもの）があれば明確化する。例えば，コーディング規約として MISRA-C を適用する計画であれば，記述する。また，社内で規定した標準（例えばソフトウェア設計に関する技術標準）なども，ソフトウェアの品質や**安全**性を高めるためのものであれば，記述する。

b) 方法

・・・高品質で**安全**なソフトウェアの作成を推進すると考**えら**れる方法を記述する。これには，方針や手法などを含んで良い。

方針や方法の例としては，設計の上流での欠陥防止を目的として，次の**アクティビティ**へ進む前に必ずレビューを実装する，メトリクス（例えばソースコードの複雑度など）を計測して一定値を超えたらレビューする，などが考**えら**れる。

手法の例としては，構造化設計，形式手法又は半形式手法の使用，カプセル化及び情報隠ぺい（オブジェクト指向）などが考**えら**れる。

c) ツール

ソフトウェアアイテムを開発するときに使用するツール類（主にソフトウェアツール）を記述する。ツールの例には，統合開発環境，コンパイラ／リンカ，エディタ，静的解析ツール，メトリクス測定ツール，テストツールなどが考**えら**れる。これには，使用目的や使用**バージョン**も記述することが望ましい。

また，例えば，**ソフトウェアアイテム**の試験に，スタブ（試験対象の**ソフトウェアユニット**が呼び出

すための下位の仮の**ソフトウェアアイテム**）や，テストドライバ（試験対象を呼び出すための上位の仮の**ソフトウェアアイテム**）など，仮の**ソフトウェアアイテム**を作成して使用する場合は，それも含める。なお，これらのツールの管理については，箇条 5.1.10 で規定している。

5.1.5 ソフトウェア結合及び結合試験計画（クラス B，C）

ソフトウェア**安全**クラス B 又は C の場合，**ソフトウェアアイテム**の結合の実施計画，及び結合試験の計画をする必要がある。結合の度合いは，2 つの**ソフトウェアユニット**の結合のレベルから，全ての**ソフトウェアアイテム**を**ソフトウェアシステム**へ結合するレベルまでを含むと考える。

結合試験は，主に**ソフトウェアアイテム**間のインタフェース及び相互作用を確認する試験と考えると良いだろう。一般的に，確認したいインタフェースに関する**ソフトウェアアイテム**を結合し，そのインタフェースの仕様に基づき試験を実施する。その組み合わせの順番（あるいは一気に結合するのか）や，試験の観点，作業の進め方などを明確化するのが望ましい。また，試験対象を呼び出すための仮のソフトウェア「テストドライバ」や，試験対象が呼び出す仮のソフトウェア「スタブ」を用いる場合は，それらに関する計画を含めることが望ましい。

なお，計画に関する要求事項には，**ソフトウェアユニット**の**検証**が明示されていないが，実施する必要はある。箇条 5.5.5 を参照されたい。その計画は，次の箇条 5.1.6 に含まれると考えるが良いだろう。

5.1.6 ソフトウェア検証計画（クラス A，B，C）

計画に，ソフトウェア**検証**計画を含める必要がある。これは，次の a）～ d）を含める必要がある。

a） **検証**が必要な**成果物**

・・・各**アクティビティ**及び**タスク**の**成果物**（箇条 5.1.1 の b）参照）のうち，**検証**が必要なものを明確化する。一般に，下流の（後続の）**アクティビティ**への入力となる**成果物**及び（**ロボット**介護機器の **PEMS**）**システム**設計への入力となる**成果物**は，**検証**しなければならない。

b） 各ライフサイクル**アクティビティ**に必要な**検証タスク**

・・・上記 a）で明確化された**検証**が必要な**成果物**に対し，**検証タスク**を計画する。これは，どの**アクティビティ**において何が必要な**検証タスク**であるかを明確化する。各**検証タスク**について，**検証**の目的及び観点を明確化することが望ましい。また，**検証**の方法（例えば，動的試験，静的解析，レビュー）についても明確化することが望ましい。

c） **成果物**を**検証**するマイルストーン

・・・上記 b）で明確化された**検証タスク**を，いつ実施するのかを，又は実施する条件を明確化する。

d） **成果物検証**の合否判定基準

・・・**検証**した**成果物**を合格と判定する基準を明確化する。判定基準は，**検証**の観点に従い全ての**検証**が終了したか，問題の修正に関して再**検証**が終了したか，**検証**結果に残問題がないか，残問題がある場合はその影響をどう分析しどのような体制又は責任において判断するか，などを明確化しておくことが望ましい。

判定基準には，下流の**アクティビティ**をスタートして良いかどうかの判断基準を含めることが望ましい。その場合，合否判定基準は，合格と不合格の二択ではなく，仮合格を含めた三択とし，仮合格の場合は，下流の**アクティビティ**はスタートするが，正式な合格まで再判定を繰り返す，という方法もある。

Tech. Tips

レビューの技法

レビューは，**アクティビティ**や**タスク**の**成果物**を，主に目視により調査し，問題を摘出する活動である。特に開発**プロセス**の上流工程での問題を早期に摘出することに効果がある。高品質で**安全**なソフトウェアを製造するためには，レビューと試験の両面から確認することが重要である。

◆レビューの形態の例として，次のようなものがある：

- ピアレビュー： 同僚など，作成者以外の誰かに依頼する，比較的即席のレビューである。
- パスアラウンド： 複数名で実施するが，会議形式ではなく，回覧又は配布の形で実施するレビューである。
- ウォークスルー： 会議を開き，作成者が説明をし，参加者が質問や指摘をする形のレビューである。
- インスペクション： モデレータ（リーダ）が計画して開催する会議型のレビューである。インスペクタ（レビューする人）は事前に対象をチェックしておき，会議時には進行に従って指摘する。他に読み手，**記録**係，**検証**係などの役割分担がある。作成者の参加はオブザーバと位置付けられる。

◆レビューの技法の例として，次のようなものがある：

- チェックリスト： チェックすべきことをリストにしておき，それに従って確認する。
  実施しやすく応用範囲が広いが，リストに書かれていないことについての確認は期待できない。
- キーワードによるチェック： 経験上，特定の単語があると問題が存在する可能性が高まることが知られている。そのような単語にフォーカスし，一覧を用いてチェックする。
  例１ 「～の場合」 → それ以外について明確であるか？
  例２ 「～など」 → あいまいであり明確にすべきでは？
  例３ 「要検討」 → 未決事項と推測できる。要管理項目では？
- シナリオベースのリーディング： 想定するシナリオ（例えば，遊びに来た子供がおもちゃ代わりに使おうとした）を割り当て，そのシナリオに沿って問題点を探す。多様な視点でのレビューが重要な場合に効果的である。
- **トレーサビリティ**のチェック： 各**成果物**（例えば，ソフトウェア**安全**要求，各設計仕様，ソースコード，試験内容及び試験結果）の内容が，相互に追跡（トレース）可能で，かつ整合していることを確認することで，抜けなどの問題点を探す。

レビューは，「観点」が重要である。つまり，摘出すべき問題を明確にし，その問題に集中することが重要

である。また，人間関係のトラブルにならないよう，レビューにおける「心得」や「べからず」についてまとめられた資料もあるため，検索し参照されることを推奨する。

参考： コードレビューに関して「ソースコードの**妥当性確認**」という表現に出会ったことがあり，面白い発想だと感じたため，ここに記す。一般に，コードレビューで行うのは**検証**（設計仕様通りであることの確認）であり，**妥当性確認**（要求が満たされていることの確認，つまり**安全**規格の文脈においては**安全**であることの確認）は**システム**レベルで行うべきものである。一般的ではない表現であったため質問したところ，『ソースコードをレビューしながら，もしこのコードが動作したら何が起こり得るのか，それは**安全**なのか，を考えながら読むこともしている。これをソースコードの**妥当性確認**と呼んでいる。』との回答を得た。有意義な方法なのかもしれない。

テストプロセス

ソフトウェアテスト（ソフトウェアの試験）は，計画的及び体系的に実施するべきである。
ソフトウェアテストは，思いつくままに試してみる場当たり的な方法では，テストできていなかったケースの発生を防げない。また，仕様をよく理解せずにテストを実施していては，予期せぬ振る舞いについて「そのような仕様なのかと思っていました」という勘違いを防げない。
検証をソフトウェアテストにより実施する場合，仕様を充分に分析したうえで，仕様に基づいて網羅的なテスト設計を行い，テスト設計に基づいてテストを実装及び実施することが重要である。それら一連の活動を適切に実施するために，テスト**プロセス**の確立を含めた計画が重要である。
ソフトウェアテストは，体系的及び網羅的に実施することにより，適切なソフトウェアが作成されたことの証拠を示す活動とすることができる。
図 5-12 に，テスト**プロセス**のおおよその流れを例示する。

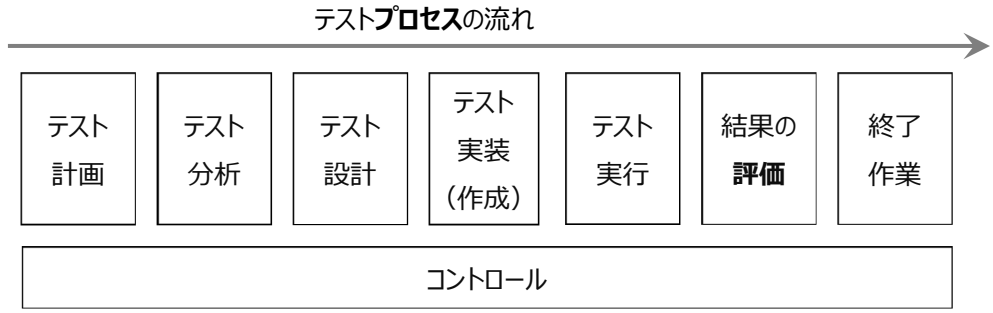


図 5-12 テストプロセスの例

5.1.7 ソフトウェアリスクマネジメント計画 （クラス A，B，C）

ソフトウェア**リスクマネジメントプロセス**の**アクティビティ**及び**タスク**を，箇条 7 に適合する形で実行できるよう，計画する必要がある。この計画は，ソフトウェア開発計画に記載するか，又は引用する必要がある。

この計画は，ソフトウェアについて**危険状態**を引き起こす可能性を分析し，必要な場合は**リスクコントロール**手段を選択，開発，及び**検証**する**アクティビティ**を含めることが重要である。また，ソフトウェア変更に関する**リスクマネジメント**も計画に含めることが重要である。なお，**ソフトウェアシステム**が SOUP を含む場合は，**製造業者**が SOUP に関連する**リスクマネジメント**の責任を持つ必要がある。SOUP は，もし，エビデンス文書の欠落（ソースコードしか残されていない，など）の場合，リバースエンジニアリングにより設計構想や設計過程の分析は限界があるだろう。採用にあたっては，契約の内容を含めた**リスク**をマネジメントする必要があるだろう。このガイダンスの 5.3.3 章も参照されたい。

5.1.8 文書化計画（クラス A，B，C）

ソフトウェア開発**プロセス**を実施した結果として作成する文書について，その情報を，ソフトウェア開発計画に含める必要がある。その情報は，次の a) ～ d) を含める必要がある。

a) 題名，名称又は命名規則（naming convention）

・・・各文書について，固有の文書名を特定できるのであれば，その文書名を記述する。計画段階では特定できない場合は，どのような文書を作成するのかを示す名前，又は命名規則により記述する。これは，開発終了時に，計画された全ての文書が作成されたことを確認できる水準で記述することが重要である。

b) 目的

・・・各文書について，何を記述することを目的とした文書であるかを記述する。

c) 開発，レビュー，承認及び修正のための**手順**並びに責任

・・・文書の作成，レビュー，修正および承認について，どのような**手順**で実施するか，及びその責任の所在を明確にする。これは，管理されない文書化を防ぐために重要である。

5.1.9 ソフトウェア構成管理計画（クラス A，B，C）

ソフトウェア開発計画書に，ソフトウェア**構成管理**情報を含める必要がある。ソフトウェア**構成管理**情報とは，次の a) ～ f) である。

a) 管理対象アイテムのクラス，タイプ，**カテゴリ**又はリスト

・・・**構成管理**対象のアイテムについて，クラス，タイプ又は**カテゴリ**の分類方法を用いて，あるいはリストを用いて，記述する。ここで用いるクラス，タイプ及び**カテゴリ**の意味は，**製造業者**が定義して良いと考える。計画段階では，すべての管理対象のアイテムを特定でき及び名称を明確にできるとは限らないので，何らかの分類方法を用いて良いが，管理対象の範囲を明確に示すことが重要である。

b) ソフトウェア**構成管理アクティビティ**及び**タスク**

・・・ソフトウェア**構成管理**を，どのような**手順**及び活動により実施するかを記述する。ここで言うソフトウェア**構成管理**は，変更管理及び**バージョン**管理を含むものである。**バージョン**管理ツールなどのツールを用いる場合は，その運用方法を含めて記述する。

c) ソフトウェア**構成管理アクティビティ**の実行に責任を負う組織

・・・ソフトウェア**構成管理**の各**アクティビティ**について，その実行に責任を負う組織を記述する。特に承認に関する**アクティビティ**について，責任の明確化は重要である。ソフトウェア**構成管理**全体の統括についての責任組織又は責任者も記述することが望ましい。

d) それらの組織と他の組織（例えば，ソフトウェア開発又は保守など）との関係

・・・上記 c) に記述した組織以外に関係する組織があれば，それらの組織及び関係を記述する。例えば SOUP を開発した組織や，保守を別組織に委託する場合の委託先などが該当する。

e) アイテムを**構成管理**下に置く時期

・・・アイテムを，計画的に**構成管理**下に置くために，その時期を記述する。アイテムは，その作成開始から**構成管理**下に置く必要は無いが，指定された時期以降は，**構成管理**下に置き，あらゆる変更を含め厳格に管理するべきである。この時期は，**検証**の開始より前でなければならない（箇条 5.1.11 も参照されたい）。なお，あまり早くに管理下に置くと，変更管理の手間が無意味に増える可能性があるので注意されたい。

f) 問題解決**プロセス**を使用する時期

・・・問題解決の管理を計画的に実施するために，問題解決**プロセス**を使用する時期を記述する。開始時期については，アイテムの**検証**の開始がひとつの目安となると考える。**検証**により発見された問題は，問題解決**プロセス**を使用して解決するべきである。一方，終了時期については，**リリース**後の**システム**試験への対応を考慮することが望ましい。

ソフトウェア**構成管理**については，このガイダンスの 5.3.4 章を参照されたい。

5.1.10 管理が必要な支援アイテム（クラス B，C）

ソフトウェア開発に使用するツール，アイテムまたは設定について，それに欠陥があると開発するソフトウェアに影響を及ぼす可能性がある場合は，管理対象とする必要がある。

ソフトウェア開発においては，多くの支援アイテムが用いられる。支援アイテムには，箇条 5.1.4 の c) に基づいて記述されるツール以外にも，**バージョン**管理ツール，問題点管理ツール，**トレーサビリティ**管理ツール，各種の分析ツールや可視化ツール，作業自動化ツールなど，多様なツールがある。それらについて，使用したツールの名前及びその**バージョン**，使用時の設定などを管理し，何か問題が発生した時に，使用状況を再現できる水準で管理することが望ましい。

設定とは，例えばコンパイラのコンパイルスイッチのように，その値が変わればソフトウェアが変わり得るパラメータをイメージすると良い。バッチファイルの内容などの，作業自動化に関する設定も，ソフトウェアに影響を及ぼす可能性があるならば，対象と考える。

それら以外にも，例えば，ICE（In-Circuit Emulator）の装置部分のようなハードウェアなども，ソフ

トウェアに影響を及ぼす可能性がある場合は管理対象とするべきである。
これらソフトウェア開発支援に用いられるものに欠陥があった場合，それが作成するソフトウェアの品質を阻害し，ソフトウェアの問題を引き起こしてしまう可能性のある場合がある。その可能性が考**えら**れる場合は，管理対象とし，その既知問題の有無及び内容を把握し，作成するソフトウェアへの影響を回避し，作成するソフトウェアの品質の確からしさを高めることは重要なことである。

コンパイル／ビルドについて
ソフトウェア設計者は多くの場合，ソースコードをオブジェクトコード（中間形式）に変換することを「コンパイル」と呼ぶ。オブジェクトコードは，そのままでは実行できず，他の必要なオブジェクトコード及び必要なライブラリなどを「リンク」し（つまり合体させて），実行形式にする必要がある。コンパイル及びリンクを行い，ソースコードから実行形式ファイルを作成することを，「ビルド」と呼ぶことが多い。しかし，規格は用語「ビルド」を用いず，その意味も含めて用語「コンパイル」を用いているようである。また，用語「ビルド」をあまり用いない現場もあるため，これらを考慮し，このガイダンスの説明においては「コンパイル／ビルド」と記述する。

5.1.11 検証前のソフトウェア構成アイテムのコントロール（クラス B，C）

ソフトウェア**構成アイテム**を**構成管理**下に置く時期について，その**検証**を実施する前に**構成管理**下に置くように計画する必要がある。この件は，箇条 5.1.9 の e)も参照されたい。

5.1.12 既知のソフトウェア欠陥の特定及び回避（クラス B，C）

ソフトウェア開発計画書に，次の**手順**を含める必要がある。

a) **ソフトウェアシステム**に対して選択したプログラミング技術によって生じる可能性のある欠陥を分類するための**手順**。
・・・ソフトウェアに生じる可能性のある欠陥を分類するための手段を示す必要がある。この分類の明確化は，ソフトウェアの欠陥に起因する**リスク**の可能性を論理的に分析するための足掛かりのひとつである。
欠陥の分類又は**危険状態**の一因となる原因の例については，IEC TR 80002-1:2009 の附属書 B ソフトウェアの原因の例 が参照先として示されている。ここでは，**医療機器ソフトウェア**の機能領域別の頻出原因と改善につながる提案の例が，検討の足がかりとして示されており，**ロボット**介護機器の開発者も参考になる。
分類の例示： ゼロ除算，数値のオーバーフロー／アンダーフロー，ポインタの誤り，初期化の誤り，スタックのオーバーフロー，メモリリーク，無限ループなど。

b) これらの欠陥が受容できない**リスク**の一因にならないことを示す証拠を文書化する**手順**。
・・・ソフトウェアが**安全**であることを示すためには，ソフトウェアの欠陥が受容できない**リスク**の一因にならないことを示す必要がある。それを示すための証拠を入手し，及び文書化する**手順**を示す必要がある。ここで求められる計画は，例えば次のような**手順**を含めた，証拠の提示方法の明

確化である：
プログラミング技術を明確にすることで，そのプログラミング領域で発生し得る典型的な欠陥（バグ）がある程度，予想可能となる。上記 a）で示した分類を利用し，それらが**リスク**の一因になり得る可能性があるかを分析し，理屈上は可能性が無い場合はその根拠を文書化する。可能性がある場合は，それらを回避する手段（発生しないようにする手段又は発生を検出し対処する手段）を検討及び選定し，それらの手段を用いた結果**リスク**の一因とならないことを示す証拠（**検証**結果など）を入手し，そしてこれらを文書化する。
例えば，「ゼロ除算」に対し「割り算の実施直前に，値がゼロでないことをチェックするコードを必ず書き，コードレビューで確認する」ことで，ゼロ除算の際の欠陥は回避できるという主張を文書化する。

使用したプログラミング技術（プログラミング言語の特性やコード解析ツールの機能でカバーするなどを含む）によっては，特定の種類の欠陥が発生しない場合や，あるいは発生しても自動検出できる場合があるため，その活用を含めることは許容できる。

② ソフトウェア要求事項分析

5.2.1 システム要求事項からのソフトウェア要求事項の定義及び文書化（クラス A，B，C）

システム要求事項（例えばIEC 60601-1の箇条14.7に従って文書化された要求事項）に基づき，**ソフトウェアシステム**のソフトウェア要求事項を定義して文書化する必要がある。複数の**ソフトウェアシステム**を開発する場合は，これを**ソフトウェアシステム**ごとに行う必要がある。記述する内容については，**安全**に関連する内容だけでなく，**ソフトウェアシステム**が実現すべきことを網羅して記述する必要がある。
ソフトウェア要求事項の定義は，**ソフトウェアシステム**が解決すべき課題（要求）を明確にするとともに，それに基づく要求仕様を，箇条 5.2.2 に適合する形で客観的明確に記述したものであることが望ましい。ここで記述する要求仕様は，**ソフトウェアシステム**の外部仕様であることに注意されたい。つまり，内部仕様は後続の**アクティビティ**にて要求仕様に基づいて設計するものであり，ここで記述するものではないとお考え頂きたい。
ソフトウェア要求事項の定義は，**システム**開発担当とソフトウェア開発担当が協力して作成し及び合意することが望ましい。この件は，このガイダンスの 5.3.6 章も参照されたい。

5.2.2 ソフトウェア要求事項の内容（クラス A，B，C）

ソフトウェアシステムに対するソフトウェア要求事項を定義して文書化するとき，次の事項を含めるかどうかを検討し，必要に応じて記述する必要がある。これらは，**ソフトウェアシステム**の外部仕様を客観的明確に記述することが望ましい。記述内容は，**検証**実施時に，試験条件及び期待結果を明確に思い描ける水準で記述することが望ましい。また，正常系（通常の使用方法など）だけでなく，**異常**系（**故障**時や**誤使用**時など）についても網羅して明確化することが重要である。各要求事項について，それが**安全**を意図した要求事項であるかどうかを明確にすることが望ましい。また，各要求事項には，**トレーサビリティ**の明確化を意図して，要求事項番号を付けるなど識別することが重要である。

a) 機能及び能力についての要求事項

・・・ソフトウェアシステムへの要求事項について，例えば次のような内容を必要に応じて記述する。

- 目的（その要求事項は何を目的としたものであるか）
- 機能（要求する機能の具体的内容）
- 性能（例えば，反応速度や処理可能量，精度，タイミングなどについての要求事項）
- ハードウェア環境（例えば，使用するマイコンやデバイスなどに関連する要求事項）
- ソフトウェア環境（例えば，使用する言語，プラットフォーム，OS などについての要求事項）
- その他の制約条件（例えば，アップグレード，複数の SOUP 又は他機器との互換性に関する要求事項）

b) **ソフトウェアシステム**のインプット及びアウトプット

・・・ソフトウェアシステムへの入力，及び**ソフトウェアシステム**からの出力に関する要求事項について，例えば次のような内容を必要に応じて記述する。

- データ（又はコントロール）の，型（論理型，整数型，実数型など），範囲（上限値や下限値など），制限事項など
- デ**フォルト**を用いる場合は，その値や条件など

なお，これらはインタフェースについての要求事項の一部と考えることもできる。

c) **ソフトウェアシステム**と他の**システム**との間のインタフェース

ソフトウェアシステムが，その外部と何らかの関係を持つならば，そこにインタフェースがあるはずであるため，そのインタフェースに関する要求事項を記述する。これは，単につながりを記述するだけではなく，ソフトウェア的インタフェースであれば，そのプロトコル及びフォーマットを，ハードウェア的インタフェースであればその特性などを含めて記述することが重要である。

d) ソフトウェアによる警報，警告及び操作者へのメッセージ

ソフトウェアを用いて，使用者や周囲の人などに警告や警報を出す場合，及び**システム**を操作する人などにメッセージを出す場合，その要求事項を記述する。記述内容は，警告や警報を出す条件，方法，メッセージを出す場合の内容などに加え，期待する対処方法や禁止すべき事態などについても記述することが望ましい。

e) **セキュリティ**要求事項

セキュリティに関する要求事項を，例えば次のような内容について，必要に応じて記述する。

- 機密情報の漏洩に関連する事項（情報管理方法など）
- 認証（正当な使用者であることの確認など）
- 認可（アクセスの許可など）
- 監査証跡（audit trail）（アクセスログなど）
- 通信の完全性（暗号化などを用いた改ざん防止など）
- **システムセキュリティ**／マルウェアからの保護（**システム**及び**ソフトウェアシステム**の破壊の防止や，情報漏洩の防止など）

この規格への適合を考慮する場合，情報**セキュリティ**のような機密情報の漏洩防止を重視した**セキュリ**

ティだけでなく，**安全**性の破壊の防止に視点を置いた**セキュリティ**も考慮することが望ましい。より具体的には，例えば次のような観点を考慮した要求事項を記述することが望ましい。

- **安全**に関連したプログラムの，外部からの破壊（書き換え）の防止
- **安全**に関連したデータ（通信メッセージを含む）の，外部からの破壊（置換，消去又は挿入）の防止
- **安全**に関連したソフトウェアのダウンロード及びインストールにおける，外部からの改ざんの防止。

f) ソフトウェアで実装するユーザインタフェースの要求事項

ソフトウェアシステムを用いて実現するユーザインタフェースに関する要求事項を，必要に応じて記述する。より具体的には，例えば次のような観点を考慮した要求事項を記述することが望ましい。

- 手動操作の支援（操作手段の提供や操作を誘導するメッセージ表示など）
- 人間と機器との相互作用（シーケンス及びそれがもたらす結果など）
- 人員についての制約（操作者の認証など）
- 人間の注意を集中させる必要がある領域（GUI のユーザーガイドなど）

なお，この規格は，ユーザビリティエンジニアリング要求事項について，IEC 62366-1 ほか（例えば IEC 60601-1-6）の規定を例示しているため，参照する。

g) データ定義及びデータベース要求事項

ソフトウェアシステムが使用するデータ及びデータベースに関する要求事項について，例えば次のような内容を必要に応じて記述する。

- 形式（データ形式やメッセージ形式など）
- 整合性（データベースのテーブル間における，変数の欠落や不整合の防止など）
- 機能（データベースのトランザクション処理機能や**障害**対処機能など）

h) 納入した**医療機器ソフトウェア**の，操作現場及び保守現場におけるインストール及び受入れの要求事項

ソフトウェアを，操作現場又は保守現場においてインストールすることが想定される場合や，受け入れ先による受け入れ作業が想定される場合は，それらに関してソフトウェアが実現すべき要求事項を記述する。

i) 操作及び保守の方法に関わる要求事項

使用者などによる機器（**ロボット**介護機器）の操作，又は保守担当者などによる**システム**の保守を想定する場合，それらに関してソフトウェアが実現すべき要求事項を記述する。

j) **IT ネットワーク**に関連する要求事項

IT ネットワークに接続することを想定する場合，それに関する要求事項について，例えば次のような内容を記述する。

- 通信内容（警報，警告及び操作に関するメッセージなど）
- 通信方式（ネットワーク通信のプロトコル及びフォーマットなど）
- 状況に応じた対応（ネットワークサービスが利用できない場合の処理など）

k) ユーザ保守要求事項
使用者が保守を行うことを想定する場合，そのことに関して**ソフトウェアシステム**が実現すべき要求事項を記述する。

l) 規制要求事項
ソフトウェアに関する規制（国による規制など）があれば，要求事項として記述する。

要求事項は，必ずしも上記の a) ～ l) に従って分けて記述する必要は無いと考える。この規格のこの箇条の注記 8 が指摘する通り，a) ～ l) に関する要求事項は，重複することもある。
この規格のこの箇条の注記 9 が指摘する通り，ソフトウェア開発の初期には，必ずしもすべての要求事項が確定し，ソフトウェア開発のインプットとして利用可能であるとは限らない。一部の要求事項が確定しないままソフトウェア開発を開始することは，製造事業者の判断で可能である。しかし，いずれかの時点において，全ての要求事項を確定するべきであり，確定するまで計画的に管理されるべきである。
なお，この箇条の注記 10 に ISO/IEC 25010「**システム**及びソフトウェア製品の品質要求及び**評価**（SQuaRE）―**システム**及びソフトウェア品質モデル」が例示されているとおり，ソフトウェア要求事項の定義を検討するときに，ソフトウェアの品質特性を観点として利用すると，例えば要求事項の網羅性を検討できるなど，有用である場合がある。ソフトウェア製品の品質特性には，機能適合性，性能効率性，互換性，使用性，**信頼性**，**セキュリティ**，保守性，移植性がある。また，ソフトウェアの利用時の特性には，有効性，効率性，満足性，**リスク**回避性，利用状況網羅性がある。これらの特性について，及びそれらを細分化した副特性について，詳しくは ISO/IEC 25010 を参照されたい。
また，ソフトウェア要求事項の文書化の参考として，IEEE 830 "IEEE Recommended Practice for Software Requirements Specifications" が役立つかもしれない。
ソフトウェア要求及び要求仕様の客観的明確な記述の例として，USDM について後述**図 5-13** にて簡単に紹介する。

Tech. Tips

ＵＳＤＭ（Universal Specification Describing Manner）

ソフトウェアの欠陥は，ソフトウェアに対する要求及び要求仕様の不適切さ（特に曖昧さ）に起因することも多い。ソフトウェア品質を高めるためには，ソフトウェアに対する要求及び要求仕様を適切に記述することが，重要な課題のひとつであると言って良い。

ソフトウェアに対する要求及び要求仕様の曖昧さを低減し明確化する記述方法のひとつに，ＵＳＤＭがある。ＵＳＤＭは，階層構造を持つ表を用いて，「要求」，「要求仕様」，「理由」及び「説明」を区別して記述する。また，各要求及び要求仕様に ID を付ける。

ＵＳＤＭを用いた記述により，要求仕様を明確に個別識別できるようになり，及びその元となる要求や理由との関係も明確になる。更には要求仕様 ID を用いた追跡や，仕様ラベルを用いた合意の管理も可能である。ただし，書き方にはコツがある。説明資料がインターネット上などにあるので，情報を検索されたい。また，USDM を使用した記述の例としては，「大阪電気やかん 要求仕様書」（参考文献に記載）がある。

No.	**カテゴリ**	要求／仕様	ID	内容
01	火傷防止	要求	SSR_01	可触部の温度をモニタし，火傷する可能性のある温度を検出した場合は，回路の通電を停止する。
			理由	回路の発熱による火傷の危険を回避する。
			説明	装着中は低温火傷の可能性がある。その条件は，文書番号 D012「温度と低温火傷するまでの時間」参照。
		＜回路温度**異常**処理＞		
		□	SSR_01-01	センサー回路からの信号を用いて温度をモニタする。
			説明	センサ回路の仕様については，文章番号 XXX「〇〇」を参照。
		□	SSR_01-02	温度が〇℃以上の状態が，累積で〇秒以上続いた場合，「回路温度**異常**」と判断する。
			説明	〇℃の場合，〇時間で低温火傷になる可能性があるため，**異常**と判定し，・・・
		□	SSR_01-03	「回路温度**異常**」と判断した場合，・・・

要求　説明　仕様ラベル　要求仕様

図 5-13 ＵＳＤＭを用いたソフトウェア安全要求仕様定義のイメージ

5.2.3 リスクコントロール手段のソフトウェア要求事項への包含（クラス B，C）

クラスＢ又はクラスＣの場合，**ソフトウェアシステム**が実装すべき**リスクコントロール**手段についての要求事項を，ソフトウェア要求事項に含めて記述する必要がある。この要求事項は，**リスクコントロール**手段を確実に実装し，適切に**リスクマネジメント**を達成するために重要な事項である。

なお，注記が言及しているとおり，ソフトウェア開発の初期には要求事項を立てられない又は適切に定義できないことがあり得る。例として，ソフトウェア**アーキテクチャ**の設計中に，ソフトウェア要因により新たな**危険状態**が発生し得ることが明らかになり，新たな**リスクコントロール**手段を追加することを判断する場合が考**えら**れる。より具体的な例としては，ソフトウェアによる主電源制御は，**リスク**の要因にならないとの判断であったため，主電源制御に関連する**リスクコントロール**手段は不要と判断されていたが，ハードウェアによる**リスクコントロール**手段が，主電源が切れるとコントロール能力を失い**ハザード**の要因になり得ることが判明したため，主電源制御に関連する**リスクコントロール**手段が必要だとの判断に変わった，という場合が考**えら**れる。このような場合は，新たな**リスクコントロール**手段の必要性が明らかになった段階でソフトウェア要求事項として追加定義し，及び関連する計画変更や設計変更を行うべきである。

5.2.4 医療機器のリスク分析の再評価（クラス A，B，C）

ソフトウェア要求事項が確定し，**ソフトウェアシステム**の振る舞い（特に**リスクコントロール**手段の外部仕様）が明確になった時点で，機器（**ロボット**介護機器）全体の**リスク**の再分析及び再**評価**を実施し，必要に応じてそれらを更新する必要がある。例として，見えていなかった**リスク**に気づいた場合や，要求事項に含まれる**リスクコントロール**手段が新たな**リスク**の要因になり得ることが判明した場合などに，内容の更新が考**えら**れる。

5.2.5 要求事項の更新（クラス A，B，C）

ソフトウェア要求事項分析**アクティビティ**（箇条 5.2 に基づくここまでの活動）の結果を受けて，この時点で明らかになっているソフトウェア要求事項及びその上位要求である**システム**要求事項について，再**評価**を行い，必要に応じてそれらを更新する必要がある。

この再**評価**は，箇条 5.2.6 に示された観点を含めて実施することが望ましい。また，この再**評価**は，**システム**設計側と協力して実施し，両者の視点で実施すると共に，両者の理解の間に齟齬の無いことを確認することが望ましい。

5.2.6 ソフトウェア要求事項の検証（クラス A，B，C）

ソフトウェア要求事項について，以下の観点で**検証**を行い及び文書化する必要がある。なお，**検証**内容及び結果も**記録**することが望ましい。

a） **システム**要求事項（**リスクコントロール**に関わるものを含む。）を実装している。

各**システム**要求事項について，それをソフトウェアにより実現する場合，又はソフトウェアを用いて

実現する部分がある場合，それが適切にソフトウェア要求事項に反映されていることを**検証**する。特に**リスクコントロール**に関連する**システム**要求事項が，適切にソフトウェア要求事項へ反映されていることを**検証**することは重要である。

なお，これらのソフトウェア要求事項及び**システム**要求事項をすべて実現すれば，想定したすべての**リスク**を許容可能な水準にすることができるかどうかを併せて確認することは，更に望ましい。

b) 相互に矛盾しない。

ある要求事項を実現すると別の要求事項が実現不可能にならないか，あるいは，ある要求事項に基づく機能が別の要求事項に基づく機能を阻害したりしないか，などを確認する。また，上位要求事項である**システム**要求事項と，下位要求事項であるソフトウェア要求事項とが，整合していることも重要である。

c) 曖昧さを回避した用語で表現している。

ソフトウェアに対する要求仕様が，曖昧さを避けた客観的明確な表現であることを確認する。つまり抽象的な表現を避けた，人により解釈の差が出ることのない表現であることを確認する。このとき，極力数学的に明確な表現であることが望ましい。

例： ×「熱くなったら」 （人により「熱い」の解釈に差が出る可能性がある）

〇「計測した温度が 40℃以上になった場合」 （温度の値が客観的明確である）

要求事項の内容が，例えば仕様と要望と理由と参考情報とが混在した混沌とした記述は，適切とは言えない。少なくとも，ソフトウェアで実現すべき要求仕様はどの記述であるが明確である必要がある。

状況よっては，ソフトウェア（ソースコードで表せるもの）で実現するものではないが要求事項として記述はする，という場合はあっても良い。これは，例えば，アセンブルのオプションで指定するマイコンの設定などである。そのような場合は，ソフトウェアで実現するものではないことを明記し，区別することが望ましい。

d) 試験基準を確立して，試験が実施できる表現で記載している。

ソフトウェア要求事項の**検証**試験の条件や**手順**，期待結果を明確に読み取れる記述になっているかどうかを確認する。

例として，ある条件を満たした場合の要求仕様は明確であるが，満たさなかった場合の記述が無い場合，期待結果が不明確なためにテストケース（試験の条件や**手順**と期待結果の組み合わせを明確にしたもの）を明確にできない場合がある。また，上記 c）の悪い例にあるような曖昧な記述の場合は，境界値（ある動作結果をもたらす上限値又は下限値）が不明確であり，やはりテストケースを明確にできない場合がある。そのような不充分な個所が無いかを確認する。この確認には，意図しない場合（**異常**系）についての試験も考慮することが望ましい。**異常**系には，例えば，使用者による**異常**使用の試験や，**システム**の**異常**が発生した場合の試験などが考**えら**れる，

e) 一意に識別できる。

各要求事項が個別に一意に識別できることを確認する。

識別のために，各要求事項に識別番号を付ける。識別番号は，**トレーサビリティ**を確認するときにも利用できる。

f) **システム**要求事項又は他の要求事項を追跡できる。

各ソフトウェア要求事項について，**システム**要求事項との間の**トレーサビリティ**（追跡性）を確保する。また，関連する他の要求事項（例えば**リスク**低減の要求事項や，ハードウェア要求事項）との間の**トレーサビリティ**も可能な限り明確にする。これは，**トレーサビリティ**マトリクスなどを用いて可視化する方法がある。

なお，ソフトウェア要求事項は，一般的には上位の要求事項が必要である。上位要求事項が無い場合は，それが理由なく立てられたものでないことを示すために，理由を明記することが望ましい。

これら以外に，次のようなことも確認すると良いと考える。

- 各ソフトウェア要求事項は，実現可能か。
- ソフトウェア開発を実施するために必要な情報がそろったか。
- 意図した状況（例えば製品の意図どおりの使用）だけでなく，予見可能な**異常**（例えば製品の**誤使用**やハードウェアの**故障**など）についても考慮されたか。
- ソフトウェアの内部仕様にまで必要以上の粒度まで踏み込んでしまっていないか。
- 以前の製品のソフトウェア要求事項を流用する場合，そのソフトウェア要求事項は，開発中の製品に関しても正しい要求事項であるか。
- 全ての要求事項について，**システム**開発側と合意できたか。

注記： 既存のソフトウェア（**レガシーソフトウェア**に限らない）を流用して使用する場合，その仕様が現在の**システム**要求事項に対して適切であるか，をよく確認することが重要である。例えば，**システム**（製品）の使用環境が変化しているにもかかわらず既存のソフトウェアをそのまま利用したために，**ソフトウェアシステム**が対応しきれなくなるという問題（特に限界値越え）が，時々発生している（例：オーバーフローによるアリアン 5 型ロケットの打ち上げ失敗や，大量の義援金による銀行の大規模**システム障害**，処理量の上限値越えによる新幹線運行**システム** COSMOS の**障害**など）。環境変化などによる，ソフトウェアの相対的劣化に注意されたい。

③ ソフトウェアアーキテクチャの設計

5.3.1 ソフトウェア要求事項のアーキテクチャへの変換（クラス B，C）

クラス B 又はクラス C の場合，ソフトウェア要求事項に基づき，それらを実現できるソフトウェア**アーキテクチャ**を設計し文書化する必要がある。

ソフトウェア**アーキテクチャ**は，例えば次のような観点で表現することが可能である。それぞれ公知な表現技法又は独自の表現記法から，望ましいと考える表現技法を用いる。第三者にも理解できるように（特に認証を求める場合は認証機関にも理解できるように）わかりやすく記述する。

- 機能的構造（例えば機能ブロック図など）
- **ソフトウェアアイテム**等から構成する構造（例えばコンポーネント図など）
- データの流れの構造（例えばデータフロー図など）
- 動作モードなどの状態の変化（例えば状態遷移図など）
- **ソフトウェアアイテム**間や外部との相互作用（例えばシーケンス図など）
- 各**ソフトウェアアイテム**の識別（例えば**ソフトウェアアイテム**名の定義及びその役割の一覧）
- **リスクコントロール**手段に関する役割の，**ソフトウェアアイテム**への割り当て
- 各**ソフトウェアアイテム**のソフトウェア**安全**クラス

構造設計においては，どのように**リスクコントロール**手段を実現するかということに，特に注意を払うことが望ましい。また，**リスクコントロール**手段に関係ない部分（非**安全**関連部分）が，**リスクコントロール**手段に関する部分（**安全関連系**部分）へ悪影響を及ぼすことが無いことを確認し文書化すことが望ましい。

ソフトウェア**アーキテクチャ**の分かりやすい表記方法の例として，UML について後述図 5 13 から図 5-22 にて簡単に紹介する。

Tech. Tips

UML

ここでは，ソフトウェアを記述する手段を紹介する。ソフトウェアを記述するときは，なるべく異なる解釈の余地が無いように，客観的明確な記法を用いることが望ましい。そのため，文章を用いて記述するより，例えば，以下の記法を用いて可視化を行うことも有効である。

UML（統一モデリング言語）は，ソフトウェアを記述するための記法を定めたものである。基本的にはオブジェクト指向のソフトウェアの記述に適した記法であるが，その他のソフトウェアの記述や，ソフトウェア以外の，例えば業務の記述に用いることも可能である。用途ごとに，いろいろな記法が定められている。以下に主なものを簡単に紹介する。

a） ユースケース図

システム（例えば**ソフトウェアシステム**）に要求される機能と，その外部の**要素**との関係を示す図。これに，相互作用の流れを文章で追記する場合もある。この図の活用により，複雑な**システム**の全体像を関係者が一緒に**評価**しやすくなる。例えば，完成後の**システム**がユーザの要望に合わないという問題を軽減する効果が期待できる。

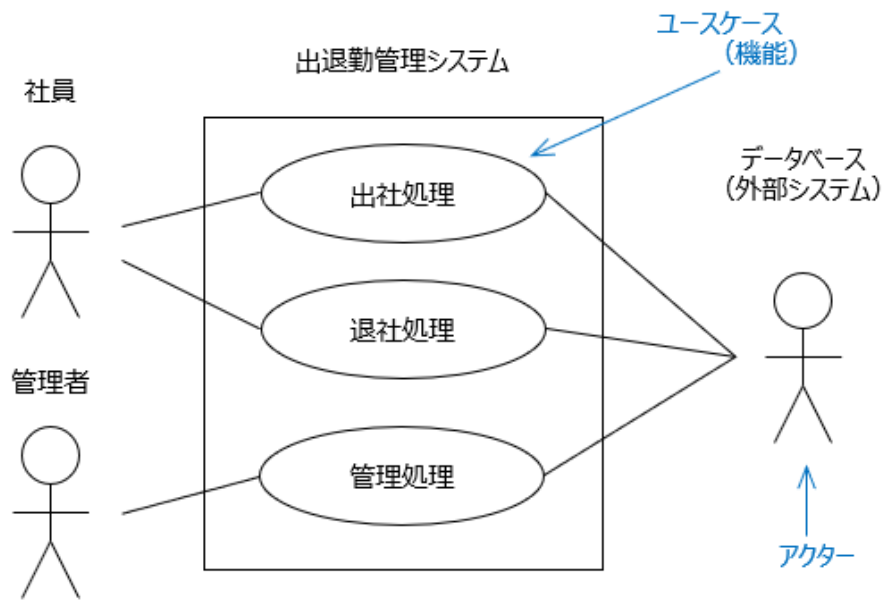


図 5-14 ユースケース図の例

b） コンポーネント図

コンポーネント（**ソフトウェアアイテム**）及びそれらの間の依存関係を描くことにより，**システム**の構成を示す図。コンポーネントの内部構造を書き加えることもある。

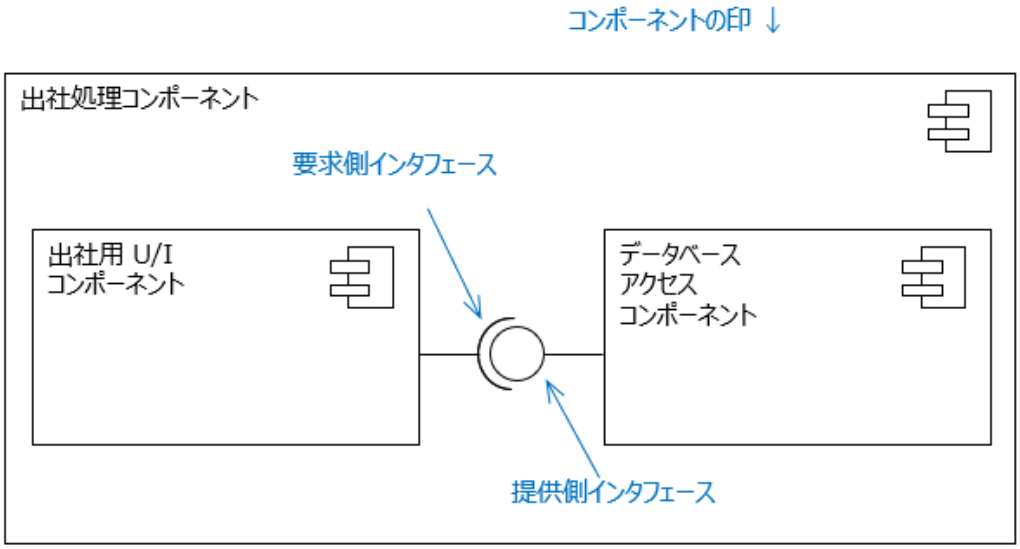


図 5-15 コンポーネント図の例

c） クラス図

ソフトウェアシステムを構成するクラスと，それらの間に存在する関連の構造を表現する図である。類似した図に「オブジェクト図」がある。これらは，オブジェクト指向以外での使用には適していないと考える。

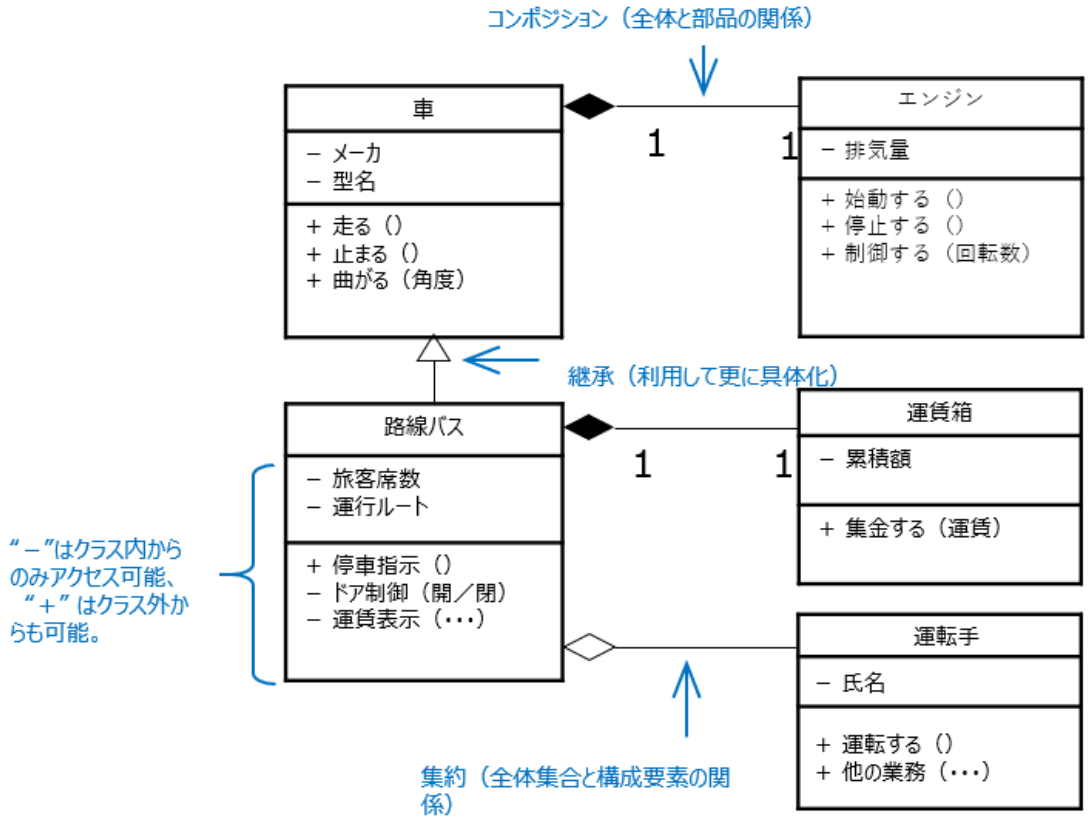


図 5-16 クラス図の説明

d） シーケンス図

イベントの発生順序や，オブジェクト間（又はモジュール間）のやりとりの流れなどを，時系列で表す図。連携の様子を表現できる。

基本的には，ひとつの図でひとつのストーリを表すものと考えると良い。複数の場合を併記することも可能ではあるが，図が複雑化して見通しにくくなりやすい。

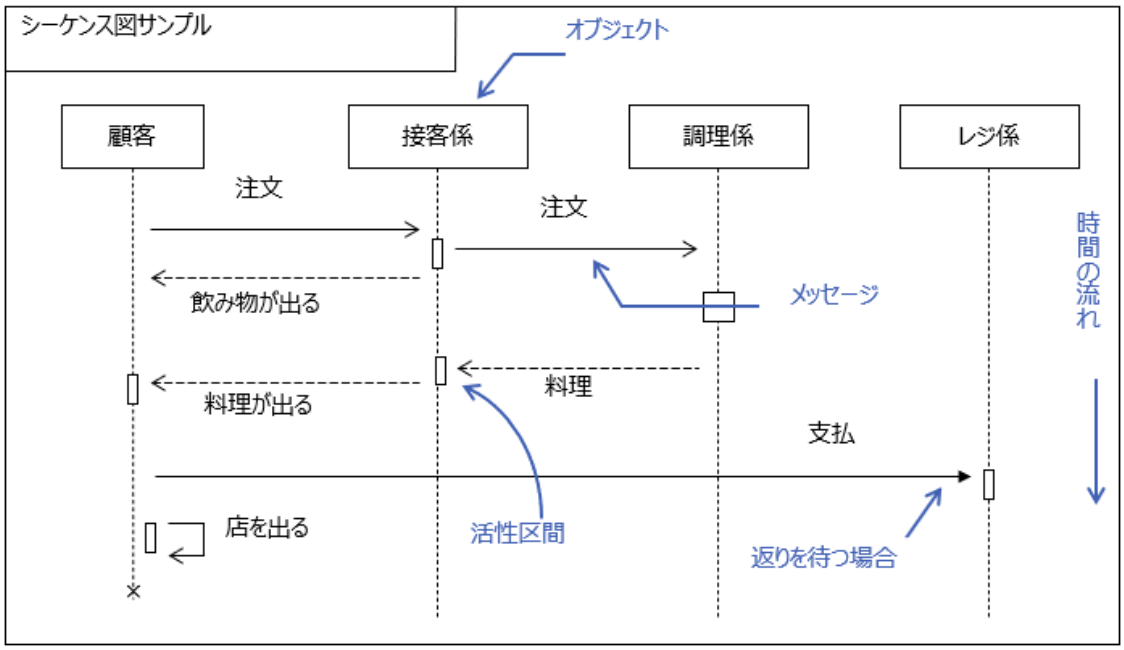


図 5-17 シーケンス図の説明

e） アクティビティ図

処理（手続き）の流れを表現する図。フローチャートのようなものと考えて良い。ただし，業務フローなどの流れを記述するのに向いていて，アルゴリズムの表現にはあまり向いていないかもしれない。

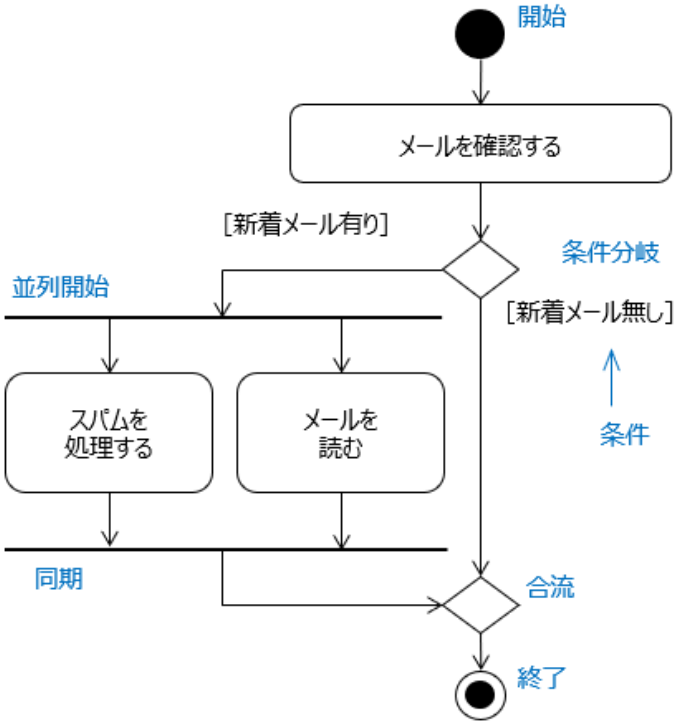


図 5-18 アクティビティ図の例

f） ステートマシン図

状態（ステート）に着目し，状態の遷移，及び遷移の条件を表現する図。状態遷移図ともいう。

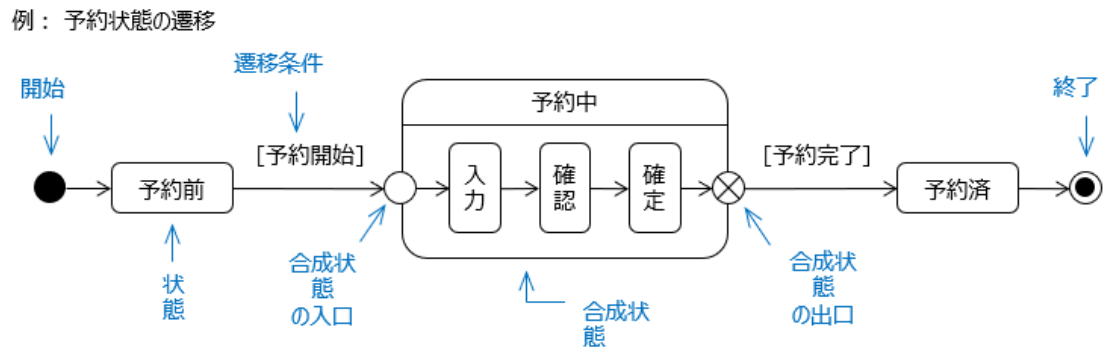


図 5-19 ステートマシン図の例

g） タイミング図

状態の変化を，時系列に表した図。タイミングの順番や継続時間，相互作用などを表現できる。

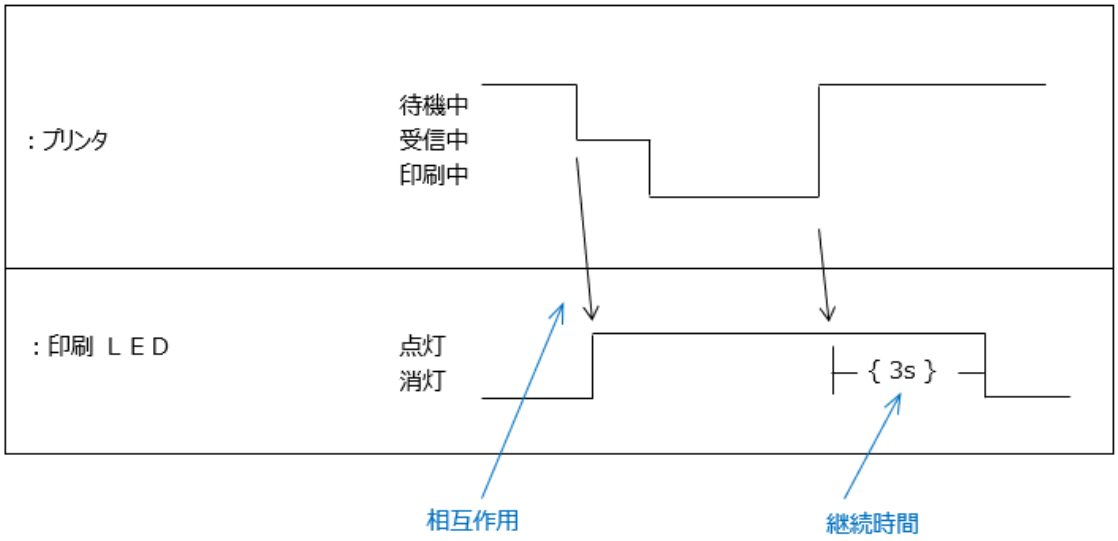


図 5-20 タイミング図の例

h） デシジョンテーブル（決定表）

入力の条件の組み合わせを列記し，対応する動作を記述する，表形式の記法である。デシジョンテーブルを

用いて，条件と動作の関係を論理的に整理することにより，設計における論理の抜けや試験におけるテスト条件漏れを防止する効果が期待できる。

			ケース1	ケース2	ケース3	ケース4	ケース5
条件	電源ON		N	Y	Y	Y	Y
	過熱エラー		—	N	Y	N	Y
	過負荷エラー		—	N	N	Y	Y
動作	異常時用リレー	ＯＦＦ	—	—	X	X	X
		ＯＮ	X	X	—	—	—

図 5-21 デシジョンテーブル（決定表）の説明図

i) フローチャート

フローチャートは，多くの人が知っている使いやすい記法であるが，使用するときは注意が必要である。特に，複雑なフローの場合は使用を避けるべきである。

・ 任意のフローを記述できるため，混乱したフローを書けてしまう。構造化を阻害する。

・ 複雑なフローチャートは，読み取りにくく，問題に気付きにくい。また保守性も良くない。

似た記述技法の例として，ＰＡＤ（Problem Analysis Diagram）というものがある。ＰＡＤはソフトウェアの構造を視覚化し，構造化を促進する点が優れている。

あるいは，ＵＭＬの**アクティビティ**図を用いる方法もある。ただし，**アクティビティ**図は，作業の流れなどを表現することに向いていて，アルゴリズムの表現にはあまり向いていないようだ。

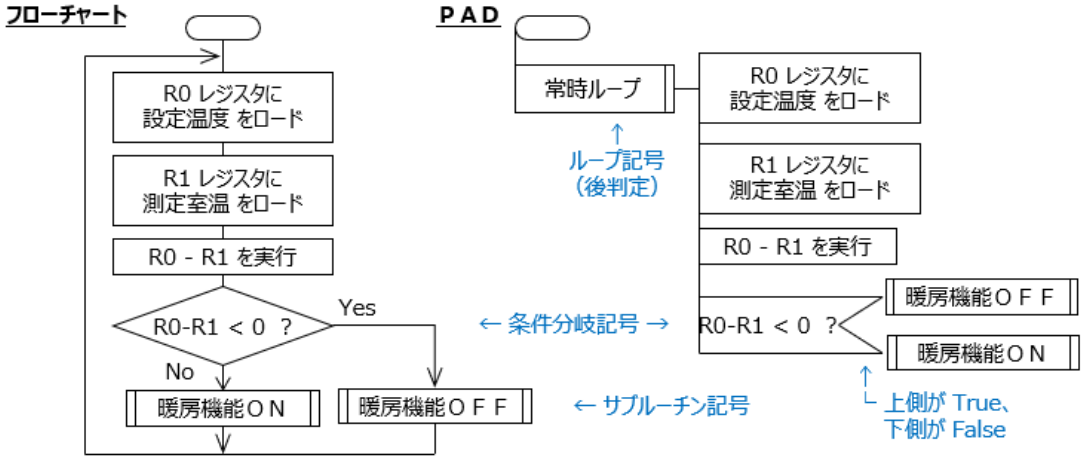


図 5-22 フローチャートおよび PAD の説明図

5.3.2 ソフトウェアアイテムのインタフェース用アーキテクチャの開発（クラス B，C）

クラスＢ又はクラスＣの場合，ソフトウェア**アーキテクチャ**開発の一環として，以下のインタフェースを設計し文書化する必要がある。

- **ソフトウェアシステム**内の**ソフトウェアアイテム**と，**ソフトウェアシステム**外部のソフトウェアとの間
- **ソフトウェアシステム**内の**ソフトウェアアイテム**と，ハードウェアとの間
- **ソフトウェアシステム**内の，ある**ソフトウェアアイテム**と別の**ソフトウェアアイテム**との間

インタフェースは，つながりを明確化するだけでなく，データ又はメッセージの形式，及びそれらのやり取りの**手順**を明確化することが望ましい。また，**ソフトウェアシステム**外部とのインタフェースについては，**異常**系（**異常**なデータや**異常**なタイミングなど）も検討して，その可能性があれば，そのコントロールを盛り込むことが望ましい。

5.3.3 SOUP アイテムの機能及び性能要求事項の指定（クラス B，C）

クラスＢ又はクラスＣの場合，SOUP であるとした**ソフトウェアアイテム**があるならば，その SOUP アイテムに対する要求事項を明確にする必要がある。これは，SOUP アイテムの**意図する使用**（想定する使用）に必要な事項を，機能及び性能の両面について，明確にする必要がある。

なお，それら SOUP に対する要求事項が，SOUP により充分に実現可能であること（例えば，SOUP の機能の限界や動作上の制約などにより，SOUP に対する要求事項を満たせない場合の無いこと）も併せて明確化することが望ましい。

5.3.4 SOUP アイテムが要求するシステムハードウェア及びシステムソフトウェアの指定（クラス B，C）

クラスＢ又はクラスＣの場合，SOUP であるとした**ソフトウェアアイテム**があるならば，その SOUP アイテムの正常な動作に必要な**システム**ハードウェア及び**システム**ソフトウェアを明確にする必要がある。

ハードウェアの例 ： マイコン又は CPU の種類又は仕様，メモリ又は外部記憶装置の必要サイズ，外部デバイスの種類（例えば通信デバイスの指定，表示デバイスの指定）など

ソフトウェアの例 ： OS の種類及びその**バージョン**の指定，ライブラリの指定，ミドルウェア又はアプリケーションの指定など

なお，**ソフトウェアシステム**の開発時に，SOUP の使用に関して注意すべき事項（例えば制限事項や既知の欠陥など）があれば，それも明確にしておくことが望ましい。

5.3.5 リスクコントロールに必要な分離の特定（クラス C）

クラスＣの場合，**リスクコントロール**に必要な**ソフトウェアアイテム**について，必要な分離を明確にする必要がある。そして，その分離を有効に実現することを確実にする（保証する）方法を明示する必要がある。

リスクコントロール手段を実現するための**ソフトウェアアイテム**は，何らかの原因により**障害**を起こすと，意図した**リスク**低減が達成できない可能性が考**えら**れる。その原因は，（それ自身の欠陥の場合も考**えら**れるが）他からの悪影響（特に**リスクコントロール**に関係しない**ソフトウェアアイテム**に**異常**が発生した時の悪影響）が考**えら**れる。その悪影響を防ぐためには，分離を行う（影響を受ける可能性を断つ）ことが重要である。この分離は，**リスクコントロール**手段を実現するための**ソフトウェアアイテム**同士の間であっても，悪影響を防ぐ必要がある場合は，分離することが重要である。

この分離が確実であることを示すには，例えば，物理的に分離できていて影響を及ぼせないことを説明する，又はソフトウェア構造的に分離しそれが有効であることを説明する，などの方法がある。

分離の例としては，この箇条の注記が言及しているとおり，次のような例がある。

- 異なるプロセッサ上で**ソフトウェアアイテム**を実行させる。
  例えば，一般機能を実行するプロセッサと，**リスクコントロール**手段を実行するプロセッサを，別のプロセッサにすることにより分離する，という方法がある。２つのプロセッサ間に共有リソースを持たないことにより，悪影響が無いことを保証できる。
- ソフトウェア**アーキテクチャ**の設計により実現する（B.4.3 参照）
  ソフトウェアシステムを**ソフトウェアアイテム**へ分割するとき，死亡または**重傷**を引き起こす可能性のある**危険状態**の要因となり得る部分を，特定の**ソフトウェアアイテム**へ集め，それを他の**ソフトウェアアイテム**と分離することにより，他の**ソフトウェアアイテム**のソフトウェア**安全**クラスを下げることが可能である。分離は，**ソフトウェアアイテム**間の独立性を高めて（例えば結合度を下げるなどして），及びデータの共有を排除し，ソフトウェアの正常な及び**異常**な振る舞いにおける意図しない相互作用の可能性を極力排除することにより，実現する方法がある。

5.3.6 ソフトウェアアーキテクチャの検証（クラス B，C）

クラスＢ又はクラスＣの場合，ソフトウェア**アーキテクチャ**について，次の事項を**検証**し，及び文書化する必要がある。

a) ソフトウェアの**アーキテクチャ**が，**リスクコントロール**に関わる要求事項を含む，**システム**及びソフトウェアの要求事項を実装している。
   各ソフトウェア要求事項が，設計されたソフトウェア**アーキテクチャ**により実現できていることを**検証**する（**システム**要求事項はソフトウェア要求事項に反映されているものと考えるため，ここでは明示しなかった）。これは，特に**リスクコントロール**に関わる要求事項に関して，注意深く**検証**することが望ましい。
   確認の観点としては，ソフトウェア要求事項の内容が，適切に**ソフトウェアアイテム**へ割り振られ，その結果として，関連する**ソフトウェアアイテム**が役割を果たすとソフトウェア要求事項が満たされることを確認することが重要である。これは，例えばコンポーネント図で表せるような静的構造の確認だけでなく，シーケンス図で表せるような時間軸上の振る舞いや，データフロー図で表せるようなデータの流れ，状態遷移図などで表せるような状態変化などについても確認することが望ましい。

この箇条の注記が言及したとおり，この要求事項に関しては，ソフトウェア要求事項に対するソフトウェア**アーキテクチャ**の**トレーサビリティ**分析を行い，その結果により適合性を示しても良い。

b) ソフトウェア**アーキテクチャ**が，**ソフトウェアアイテム**間及び**ソフトウェアアイテム**とハードウェアとの間のインタフェースを支援できる。
ソフトウェア**アーキテクチャ**と各インタフェースとの整合性を調べるなど，ソフトウェア**アーキテクチャ**が，各インタフェースの実現に対して適切であることを確認する。対象は，**ソフトウェアアイテム**間のインタフェース，及び**ソフトウェアアイテム**とハードウェアとの間のインタフェースであるが，**ソフトウェアシステム**とその外部の**システム**との間のインタフェースに関する確認も含めることが望ましい。
確認の観点としては，データ又はメッセージの形式，やり取りの**手順**，及びデータフローなどが考**えら**れる。

c) **医療機器アーキテクチャ**が，全ての SOUP アイテムの正常な動作を支援している。
機器（**ロボット**介護機器）の**アーキテクチャ**（構造的仕様）が，当該**ソフトウェアシステム**が用いる全ての SOUP アイテムが適切に動作するために必要な条件を満たしていることを確認する。
この要求事項は，開発する**ソフトウェアシステム**を対象とした確認に留まらず，ハードウェアを含めた**システム**全体を対象として確認すべきものである。注意が必要な要求事項である。

なお，ソフトウェア品質を高めるためのソフトウェア**アーキテクチャ**設計手法（TR 分割や STS 分割など）がいくつか提案されているため，そのような観点での確認も実施することが望ましい。

④ ソフトウェア詳細設計

5.4.1 ソフトウェアのソフトウェアユニットへの分解（クラス B，C）

クラス B 又はクラス C の場合，ソフトウェアを，それ以上分割しない**ソフトウェアユニット**にまで分割する必要がある。そして，全ての**ソフトウェアユニット**を特定（個別に管理識別できる水準に明確化）し文書化することが重要である。

ソフトウェアユニットへの分割については，**ソフトウェアユニット**（モジュール）からなる構造の形，個々の**ソフトウェアユニット**の大きさ，**ソフトウェアユニット**間の独立性，**ソフトウェアユニット**の領域などを考慮して分割すると良い。

5.4.2 ソフトウェアユニットごとの詳細設計の開発（クラス C）

クラス C の場合，各**ソフトウェアユニット**を正しく実装するために，充分な詳細設計を実施し，及び文書化する必要がある。

ここで言う「充分な詳細設計」とは，箇条 5.5.1 において正しく**ソフトウェアユニット**を実装できる水準にまで，**ソフトウェアユニット**内部の設計を詳細化することを意味している。これは，ソースコードと同じ水準での詳細化は必ずしも必要ではないが，例えばアルゴリズムやデータ形式などについて客観的明確な仕様を記述することが望ましい。

一方，この詳細設計は，**ソフトウェアユニット**が，ソフトウェア**アーキテクチャ**設計により与**えら**れた役割

を正しく実現できるように，適切に詳細化することも重要である。

5.4.3 インタフェース用詳細設計の開発（クラス C）

クラスＣの場合，**ソフトウェアユニット**のインタフェースについての設計を文書化する必要がある。インタフェースは，**ソフトウェアユニット**と外部コンポーネント（ハードウェア又はソフトウェア）との間，及び**ソフトウェアユニット**間の全てのインタフェースが対象である。

インタフェースの設計は，**ソフトウェアユニット**のインタフェースを正しく実装するために充分に詳細化されたものである必要がある。これは，客観的明確な水準で記述されることが重要である。

5.4.4 詳細設計の検証（クラス C）

クラスＣの場合，ソフトウェアの詳細設計が，ソフトウェア**アーキテクチャ**設計に基づき正しく作成されたことを**検証**し，及び文書化する必要がある。この**検証**は，次による。

a) ソフトウェア**アーキテクチャ**を実装している。

ソフトウェアアークテクチャ設計により明確化された**ソフトウェアアイテム**（その役割や振る舞いを含む）や，**ソフトウェアシステム**外部及び内部のインタフェースなどが，詳細設計により正しく実現できていることを**検証**する。

この**検証**は，この箇条の注記が言及しているとおり，ソフトウェアアークテクチャ設計からソフトウェア詳細設計への**トレーサビリティ**の確認によっても良い。

b) ソフトウェア**アーキテクチャ**との矛盾がない。

ソフトウェア詳細設計の内容が，ソフトウェアアークテクチャ設計の内容と矛盾しないことを**検証**する。例えば，ソフトウェア詳細設計の内容から考**えら**れるソフトウェエアユニット同士の相互作用から考**えら**れるシーケンスが，ソフトウェアアークテクチャ設計に示されたシーケンスと矛盾しないことを**検証**する。

⑤ ソフトウェアユニットの実装

5.5.1 各ソフトウェアユニットの実装（クラス A，B，C）

ソフトウェアユニットを実装（コード化）する必要がある。この実装は，詳細設計に基づいて実装するべきである。

アセンブリ言語や FORTRAN など構造化を意識していない言語を用いる場合，及びＣ言語など構造化を容易に逸脱できる言語を用いる場合，実装は，**ソフトウェアユニット**内部の構造化を意識することを推奨する。ここでいう構造化は，プログラムを，連接／選択／反復の３つの基本構造の組み合わせで構成することを意味する。これにより，こんがらがったコード（俗にいうスパゲティコード）を排除して見通しを良くし，それにより欠陥を見つけやすくしたり問題を修正しやすくしたりすることができ，品質を確保しやすくなる。

なお，実装における品質向上には，コーディング規約が有効であると一般に言われているため，コーディング規約を定め，それに従って実装する。

5.5.2 ソフトウェアユニット検証プロセスの確立（クラス B，C）

クラスＢ又はクラスＣの場合，**ソフトウェアユニット**を**検証**するための方針，方法及び**手順**を確立する必要がある。また，**検証**を試験によって実施する場合は，その試験**手順**の適切性について**評価**する必要がある。

この**検証**は，一般的には，ソースコードで表現された各**ソフトウェアユニット**が，詳細設計どおりに作成されたことを**検証**するものである。

検証の方法には，例えば，目視によりコードレビューを行う，ソースコードの解析ツールを用いて静的試験を行う，テストプログラムを用いて動的試験を行うなどの方法があり，それぞれ長所及び短所があるため，組み合わせて用いることが望ましい。

この箇条へのために明確化することが望ましい内容には，例えば次のような事項がある。

- **検証**の目的
- **検証**の観点（例えば，機能／性能ごとの確認，ありがちな欠陥の一覧に基づく確認，など）
- **検証**の方法（複数の方法を用いる場合は，その組み合わせ方を含む）
- **検証**の内容（具体的にどのような**検証**を実施するか）

試験により**検証**を行う場合，適切な試験を実施するために，試験**プロセス**を用いることを推奨する。（図 5-12 参照）

試験**手順**の適切性の**評価**は，その試験**手順**により，**ソフトウェアユニット**が詳細設計に基づき正しく実装されたことを説明（証明）できるか，が重要な観点である。

- **検証**項目の網羅性（詳細設計書に記述されたすべての仕様に対する**検証**項目の適切な用意）
- テストケースの網羅性（例えば，命令網羅／分岐網羅／条件網羅のいずれかの選択，など）
- 各試験の内容の適切さ
- 合否判定基準（箇条 5.5.3 の要求事項）

試験**手順**の内容は，各テストケースの実施**手順**の明確化よりも，一連の試験が全体として適切であること（例えば，各仕様に対するテストケースが適切に用意され，かつ各テストケースの内容が適切であるため，全体として網羅的に仕様を確認できること）の観点で**評価**することが重要である。

5.5.3 ソフトウェアユニットの合否判定基準（クラス B，C）

クラスＢ又はクラスＣの場合，必要に応じて**ソフトウェアユニット**の**検証**の合否判定基準を確立し，及び**ソフトウェアユニット**が合否判定基準に対して確実に適合するようにする必要がある。これらは，**ソフトウェアユニット**の結合の前に実施する必要がある。

場合により，特定の事項について**ソフトウェアユニット**の合否判定を行わずに**プロセス**を先へ進めることは許容できる。例えば，その**検証**は，別の**ソフトウェアユニット**との結合後の結合試験において適切に**検証**することが可能であると説明できるのであれば，その方針で進めることは許容できる。

合否判定のための観点の例は，この箇条の注記に例示されている。それ以外にも，**製造業者**の知見に基づいた基準を設けて良い。例えば，クラス B の場合において，箇条 5.5.4 の a) ～ h) を含めることが考**えら**れる。

この箇条でいう「**ソフトウェアユニット**が合否判定基準を確実に適合するようにする」とは，箇条 5.5.5「**ソフトウェアユニット**の**検証**」の実施の結果において適合していないと判断された項目があった場合は，問題解決**プロセス**を適用するか，又は同等の修正および再**検証**を実施するなどして，最終的には必ず適合させることを意味している。

5.5.4 追加のソフトウェアユニット合否判定基準（クラス C）

クラスＣの場合，**ソフトウェアユニット**の**検証**の合否判定のための観点として，必要に応じて次の事項を含める必要がある。これらの事項を合否判定基準に含める必要が無い場合は，その理由を明確化することが望ましい。なお，これらの事項以外にも，**製造業者**の知見に基づいた基準を追加して良い。

a) 適正なイベントシーケンス
ソフトウェアユニットが，仕様どおりに適正なイベントシーケンスを実現できるように，例えばロジック及び状態遷移が正しく実装されたか。

b) データ及び制御フロー
ソフトウェアユニットが，仕様どおりにデータフロー及び制御フローを実現できるように，例えばロジック及び変数が正しく実装されたか。

c) 計画したリソース配分
ソフトウェアユニットが，例えば，仕様どおりに CPU リソースの配分や，メモリリソースの配分をするように，正しく実装されたか。

d) **異常**処理（**エラー**の定義，特定及び復帰）
ソフトウェアユニットが，例えば，仕様どおりに入力値の**エラー**の検出やイベントシーケンスの**異常**を検出し，及び**異常**検出時には求められた処理を実行するように実装したか。または，**異常**検出状態からの復帰について，仕様どおりに適切な処理を実行するように実装したか。
これについては，詳細設計において，**エラー**が定義（明確化）され，その判別方法が明確化され，及び検出時の処理が明確化されている必要がある。

e) 変数の初期化
ソフトウェアユニットが，使用する変数を仕様どおりに適切に初期化できているか。
変数の初期化忘れは，典型的なケアレスミスのひとつと考える。

f) 自己診断
ソフトウェアユニットが，必要な自己診断の機能を仕様どおりに実装したか。
自己診断とは，ハードウェアの**故障**又はソフトウェアの**エラー**を，ソフトウェア（又はハードウェア）を用いて**システム**自ら検出する技術である。それらを検出した場合は，それが**危険状態**又は**危険事象**に至らないように，対処することは重要である。
ソフトウェアに関する自己診断の例： データ**エラー**検出，シーケンス**異常**の検出など。

ハードウェアに関する自己診断の例： CPU **故障**，メモリ**故障**，デバイス**故障**などの検出。
なお，防御的プログラミングも，自己診断のひとつと位置付けて良いと考える。防御的プログラミングの例には，入力値の**異常**の検出や assertion の利用などがある。

g) メモリ管理及びメモリオーバーフロー
ソフトウェアユニットが，例えば，メモリリークが発生しないように仕様どおり適切なメモリ管理を実装したか，あるいは，例えば，スタックのオーバーフロー時の**異常**処理を仕様どおり適切に実装したか。
メモリを動的に管理する場合は，過剰なアクセスなどの特殊な事態を含めて，注意が必要である。

h) 境界条件
ソフトウェアユニットが，例えば，動作を変える判断の条件を，仕様どおり実装したか。例えば，“≦”と“＜”を間違えていないか。
境界条件の間違いは，典型的なケアレスミスのひとつである。境界条件については，正常動作の範囲内における境界だけではなく，正常と**異常**の境界も含めて境界値分析を行い，これを考慮することが望ましい。

5.5.5 ソフトウェアユニットの検証（クラス B，C）

クラスＢ又はクラスＣの場合，**ソフトウェアユニット**の**検証**を実行し，その結果を文書化する必要がある。これは，箇条 5.5.2 ～ 5.5.4 の結果に基づいて実施することが重要である。特に，合否判定基準に対する適否を文書化することが重要である。

⑥ ソフトウェア結合及び結合試験

5.6.1 ソフトウェアユニットの結合（クラス B，C）

クラスＢ又はクラスＣの場合，箇条 5.1.5 にて定めたソフトウェア結合計画に従って**ソフトウェアユニット**を結合する必要がある。

5.6.2 ソフトウェア結合の検証（クラス B，C）

クラスＢ又はクラスＣの場合，**ソフトウェアユニット**の結合が，箇条 5.1.5 にて定めたソフトウェア結合計画に従って実施されたことを**検証**し，及び**検証**の**記録**を保存する必要がある。
ここで行う**検証**は，この箇条の注記が言及しているとおり，結合が計画に従って実施されたことだけを確認するものであり，結合試験を含めない。
この**検証**は，結合を実施した者以外が結合の結果を目視確認する方法がある。結合を実施した者は，結合を実施したと認識しているため，思い込みによる間違いが発生する可能性が比較的高いと考えるため，別の者が確認することが望ましい。

ソフトウェア結合の**検証**結果の**記録**は，結合結果の正しさの証拠となるよう，各確認の内容及び各確認の結果を含めることが重要である。

5.6.3 ソフトウェア結合試験（クラス B，C）

クラスＢ又はクラスＣの場合，箇条 5.1.5 にて定めた結合試験計画に基づいて，結合した**ソフトウェアアイテム**の試験を実施し，及び試験結果を文書化する必要がある。

試験結果の**記録**は，結合結果の正しさの証拠となるよう，各試験の内容及び各試験結果を含めることが重要である。各試験の内容については，箇条 5.6.4 を考慮する必要がある。

5.6.4 ソフトウェア結合試験の内容（クラス B，C）

クラスＢ又はクラスＣの場合，ソフトウェア結合試験において，結合した**ソフトウェアアイテム**が意図したとおりであることを確認する必要がある。ここでいう「意図したとおり」とは，主にソフトウェアアークテクチャ設計のとおりに，という意味であるが，それに留まらず，詳細設計やソフトウェア要求事項などのとおりであることの確認も，適宜含めて良い。

ここで確認する内容について，この箇条の注記 1 が言及したとおり，次を考慮することが望ましい。

- ソフトウェアに要求している機能
  ソフトウェアアイテムが，設計の中で明確化された機能に対して，整合した振る舞いをするか。
- **リスクコントロール**手段の実装
  ソフトウェアアイテムが，設計の中で明確化された**リスクコントロール**手段を実現するための仕様に対して，整合した振る舞いをするか。
- 指定したタイミング及びその他の動作
  ソフトウェアアイテムが，設計の中で明確化されたタイミングで動作するか。その他，設計の中で明確化された動作に対して，整合した振る舞いをするか。
- 内部及び外部インタフェースの指定した機能
  ソフトウェアアイテム間のインタフェースが，及び**ソフトウェアアイテム**とソフト**システム**外部とのインタフェースが，設計の中で明確化されたとおりに機能するか。
- 予見可能な**誤使用**を含む**異常**な条件下での試験
  ソフトウェアアイテムが，予見可能な**故障**，予見可能な**エラー**，予見可能な**誤使用**などの**異常**な状態において，設計の中で明確化されたとおりの振る舞いをするか。

これらの試験内容及び試験結果については，箇条 5.6.3 における試験結果の文書化に含めることが重要である。なお，この箇条の注記 2 にあるとおり，ソフトウェア結合試験と**ソフトウェアシステム**試験は（更には**ソフトウェアユニット**試験も），必ずしも明確に分ける必要は無く，ひとまとめの**アクティビティ**に統合して実施することは許容できると考える。

なお，この箇条は，試験にのみ言及しているが，レビューを含めることも有効である。

5.6.5 ソフトウェア結合試験手順の評価（クラス B，C）

クラスＢ又はクラスＣの場合，結合試験**手順**が適切なものであったかどうかを**評価**する必要がある。
箇条 5.5.2 において，**ソフトウェアユニット**の試験**手順**の適切性を**評価**しているが，結合試験についても，同様に適切性を**評価**するものである。つまり，箇条 5.1.5 にて定めた結合試験計画に基づき，箇条 5.6.4 で明確化した試験内容を，箇条 5.6.3 において試験実施したことについて，それが適切な**検証**であったことを**評価**するものである。この**評価**においては，設計したとおりに実装されていることが証拠を用いて説明できることが重要である。
なお，この箇条では，試験**手順**にのみ言及しているが，レビュー**手順**を含めて**評価**することが望ましい。

5.6.6 回帰テストの実施（クラス B，C）

クラスＢ又はクラスＣの場合，結合試験を実施済みの**ソフトウェアアイテム**に，別の**ソフトウェアアイテム**を結合したときに，**回帰テスト**を適宜実施する必要がある。これは，結合前には無かった欠陥が新たに生じていないことを確認するためである。また，結合前には見つけられなかった欠陥を見つけることも意図していると考える。
回帰テストは，一般には，ソフトウェアの変更の後に，その変更による新たな欠陥の発生の無いことの確認のために，以前に実施済みの試験（の一部）を再度実施することを意味するが，ここでいう**回帰テスト**は，新たな**ソフトウェアアイテム**を結合した後に，すでに実施済みの結合試験（場合により**ソフトウェアユニット**の試験を含む）を再度実施することを意味していると考える。
回帰テストの内容について，一般的には，実施済みの結合試験（又は**ソフトウェアユニット**試験）をすべて実施することを求めてはいない。どのような内容とするかは，**製造業者**が各試験の重要度などを考慮して決定して良いと考えるが，その適切さを，箇条 5.6.5 のように**評価**することが重要である。

5.6.7 結合試験記録の内容（クラス B，C）

クラスＢ又はクラスＣの場合，結合試験の結果を文書化し，及び結合試験に関する**記録**を保存する必要がある。これは，以下を含む必要がある。

a) 試験結果（合否及び**異常**箇所のリスト）を文書化する。
試験結果については，結合の結果としての合否の記載だけではなく，各テストケースに対して個別の合否を明記することが重要である。**異常**個所（問題個所）のリストについては，単に一覧表示するだけではなく，**異常**（問題等）の詳細がわかるようにすることが重要である。これらについて，別資料の引用は許容できると考える。

b) 試験を再現できるように，十分な**記録**を保存する。
後日，試験を再現するために必要となりそうな情報を保存する。例えば，テストケース，試験対象，試験環境，試験データ，試験ツールなどが考**えら**れる。保存方法は，紙でも電子データでも，保存しやすく利用しやすい形を選択して良いと考える。

c) 試験者を明示する。

試験実施者（試験責任者ではない）を明記する。試験は，基本的には属人的であってはならないと考えるが，試験実施者が異なると結果が再現できないことが起こることがあり，隠れた条件を探し出すために試験実施者の特定が重要になることがある。そのため，試験実施者の**記録**も重要である。

以上に加えて，実施した試験の内容が適切であったことを確認できるように，箇条 5.6.5 で実施した結合試験**手順**の適切性の**評価**内容及び**評価**結果への**トレーサビリティ**を確保することが望ましい。

この箇条では，試験にのみ言及しているが，レビュー**記録**を含めることが望ましい。

5.6.8 ソフトウェア問題解決プロセスの使用（クラス B，C）

クラス B 又はクラス C の場合，ソフトウェア結合の実施時，及び結合試験の試験時に発見した**異常**（問題等）を，ソフトウェア問題解決**プロセス**を用いて処理する必要がある。**異常**を発見したときに，よく検討せずに安直にソフトウェアを変更すると，不充分な又は不必要な修正であったり，新たな問題を発生させてしまったりするなど，混乱を引き起こしてしまうことがあるため，ソフトウェア問題解決**プロセス**を用いて，**異常**の解決を管理することが重要である。ソフトウェア問題解決**プロセス**については，箇条 9 を参照されたい。

⑦ ソフトウェアシステム試験

5.7.1 ソフトウェア要求事項についての試験の確立（クラス A，B，C）

ソフトウェア要求事項についての試験を確立し，及びその適切性を**評価**する必要がある。

a) **製造業者**は，**ソフトウェアシステム**試験の実施のために，個々のソフトウェア要求事項を対象として，インプット内容，予想する結果，合否判定基準及び**手順**を定めた一連の試験を確立し，実施する。

ソフトウェアシステム試験においては，各ソフトウェア要求事項に対し，適切な試験を確立し，及び実施する必要がある。各テストケースは，試験の前提（試験環境を含む），**ソフトウェアシステム**への入力，（**ソフトウェアシステム**からの出力などの）期待結果，確認**手順**，合否判断基準などを，必要に応じて適切に記述することが望ましい。それらのテストケースは，ソフトウェア要求事項を満たしたことを説明（証明）するための方針に基づき網羅的に導出されたものであることが望ましい。

試験を実施した結果は，**評価**され**記録**される必要がある。箇条 5.7.4 及び箇条 5.7.5 を参照されたい。

b) **製造業者**は，**検証**方針及び試験**手順**の適切性を**評価**する。

上記 a) で作成された試験について，その**検証**方針及び試験**手順**が，ソフトウェア要求事項に対する**検証**として適切であるかを**評価**する必要がある。この**評価**においては，要求されたとおりの実装が実現されたことを示す証拠の説明が重要である。

箇条 5.1.6 で作成したソフトウェア**検証**計画において，この**検証**の目的，観点，**検証**方法などを明確化した場合は，それを考慮することが望ましい。

なお，**ソフトウェアシステム**試験は，主にソフトウェア要求事項に対する試験であり，及びソフトウェアの外部仕様に対する試験であるが，**製造業者**の判断により，例えばソフトウェア**アーキテクチャ**に関する試験を含んで良いと考える。

この箇条の注記 1 が言及しているとおり，結合試験及び**ソフトウェアシステム**試験は，ひとつの計画にまとめたうえで一連の**アクティビティ**として実施しても良い。また，ソフトウェア要求事項は，より早い段階で試験しても良い。例えば，結合試験の中に，ソフトウェア要求事項に基づく試験が含まれていても良い。ただし，最終的には**ソフトウェアシステム**がソフトウェア要求事項を満たしていることを示すことが重要である。

この箇条の注記 2 が言及しているとおり，要求事項の間に依存性が存在する場合などは，それらの要求事項を同時に考慮した組み合わせ試験を実施することも可能である。

5.7.2 ソフトウェア問題解決プロセスの使用（クラス A，B，C）

ソフトウェアシステム試験中に発見した**異常**は，ソフトウェア問題解決**プロセス**を用いて処理する必要がある。

この箇条の要求事項の内容は，結合試験に対する箇条 5.6.8 の要求事項に似ているが，この箇条は，クラスＡの場合であっても適用される点に注意されたい。

5.7.3 変更後の再試験（クラス A，B，C）

ソフトウェアシステム試験の実施中に，ソフトウェア変更があった場合，次の処理をする必要がある。

a) 必要に応じた試験のやり直し，試験の修正及び実施，又は追加試験の実施によって，変更が問題の訂正にどの程度有効かを**検証**する。
   ソフトウェア変更の内容に応じて，既に実施済みの試験の場合であっても，その変更が正しく実施され問題解決に有効であることを確認するために，必要な試験を実施する。ソフトウェアの仕様が変更されたり新たな仕様が追加されたりした場合は，対応する試験の修正や適切な試験の追加を行い実施する。これらの試験の実施により，ソフトウェア変更の意図（例えば欠陥の修正や仕様の追加など）を適切に実現したことを**検証**する。

b) 副作用が発生しなかったことを示すための適切な試験を実施する。
   ソフトウェエア変更は，時には意図しない副作用（デグレード）を引き起こすことがあり，それを防止することは重要な課題のひとつである。副作用が発生しなかったことを示す試験には，変更の影響があり得る範囲を分析し，変更の影響は無いと言い切れない範囲に対して実施する**回帰テスト**や，副作用の発生を仮定しそれを検出するための追加試験などがある。

c) 7.4 で規定する，関連する**リスクマネジメントアクティビティ**を実行する。
   ソフトウェア変更に対し，箇条 7.4 に規定されたソフトウェア変更の**リスクマネジメント**のうち必要な**アクティビティ**を実施し，ソフトウェア変更によ**り，リスクコントロール**手段による**リスク**低減が阻害されたり，新たな**リスク**の要因が発生したりしていないかを確認する。

発見した問題を解決するためにソフトウェアを変更する場合，この規格に適合するためには，基本的に

はソフトウェア問題解決**プロセス**及び変更管理**プロセス**を用いる必要がある。その中に当然，変更後の試験に関する要求事項があって然るべきであるが，その要求を担当する箇条 8.2.3「変更の**検証**」は，**検証**の内容についてはこの箇条を考慮することを要求している。（規格の文面としては，そのような構造になっている）

この箇条では，**ソフトウェアシステム**試験後（ソフトウェア**検証**完了後）に変更があった場合に言及していないが，箇条 5.1.9 で定めた問題解決**プロセス**を使用する時期によっては，**ソフトウェアシステム**試験がいったん完了した後に，この箇条を準用する形で追加の試験を実施することが望ましい。その場合は，関連する**評価**及び**リリース**を再実施し，及び関連する**記録**を更新することが望ましい。

5.7.4 ソフトウェアシステム試験の評価（クラス A，B，C）

ソフトウェアシステム検証の方針及び試験**手順**の適切性を**評価**する必要がある。これは，次の事項の**検証**（レビュー）を実施することにより明確にする必要がある。

a) 全てのソフトウェア要求事項を対象に，試験又は**検証**を実施している。
全てのソフトウェア要求事項について，試験などの方法で**検証**が実施されたことを確認する。また，その内容について，その要求事項が実現できたことを適切に**検証**できたことを**評価**することも重要である。

b) ソフトウェア要求事項と試験又は**検証**との間の**トレーサビリティ**が**記録**されている。
試験などの方法による**検証**（**検証**内容及び**検証**結果）について，各ソフトウェア要求事項との**トレーサビリティ**が**記録**されたことを確認する。これは，例えば識別ラベル及び**トレーサビリティ**マトリクスの形で**記録**する方法がある。また，**トレーサビリティ**の**記録**の内容が適切であることの**評価**も重要である。

c) 試験結果が，要求する合否判定基準に適合する。
ここで求められる適合は，基本的には箇条 5.1.6 で定めた**ソフトウェアシステム**試験（その全体）としての合否判定基準への適合を意味する。その適合のためには，一般には個別の試験の合否判定基準への適合も必要となる。ただし，発見された問題について，問題解決**プロセス**において，正当な理由のもと処置を行わない決定をすることはあり得るため，個別の試験の判定基準への不適合は残留することがあり得る。その場合，箇条 5.8.2 で文書化する対象になると考える。

5.7.5 ソフトウェアシステム試験記録の内容（クラス A，B，C）

ソフトウェアシステム試験について，次の事項を文書化する必要がある。これは，同じ試験を再現できる水準である必要がある。再現性が重要な理由は，試験**記録**をエビデンスとして利用可能な水準にする意図もあると考えるが，それと同時に，例えば，後日同様な問題が見つかった時などに，過去の試験を再現して詳細を再確認する必要性が発生することがあるため，再**検証**可能性を確保するためでもある。

a) 要求される処置（action）及び期待される結果を示すテストケース**手順**書への参照表記
この参照表記は，次を記述した別紙を参照先とすることが一般的と考える。

参照される資料は，要求される処置（例えば，**危険状態**検出時の具体的な保護動作の内容）及び期待される結果（例えば，ある具体的な**安全**状態へ移行する結果になることが期待される）を明示したテストケース，及び試験の実施**手順**が記載されたものであると考える。
また，試験の再現に必要と考える試験環境や試験条件なども記述した資料であることが望ましい。

b) 試験結果（合否及び**異常**箇所のリスト）
試験結果は，**ソフトウェアシステム**試験の総括としての合否判断だけでなく，個別のテストケースごとの合否を追えるようにするための記述を含めることが重要である。これは，上記 a）で参照する資料に記述されていても良い。
また，発見された**異常**についての一覧を**記録**に含める必要がある。これは，各**異常**の詳細（**異常**個所，**異常**内容，対応するテストケースなど）への追跡が可能であることが重要である。

c) 試験したソフトウェアの**バージョン**
全ての試験を最終**バージョン**の**ソフトウェアシステム**で実施した場合は，そのソフトウェア**バージョン**を**記録**する。複数の**バージョン**を用いた場合は，どのテストケースをどの**バージョン**の**ソフトウェアシステム**で実施したかがわかるように**記録**する。

d) 関連するハードウェア及びソフトウェアテスト構成
ソフトウェアシステム試験の実施時に使用した，ソフトウェアを動作させるためのハードウェアを識別できる情報（例えば，試作機番号又はハードウェア**バージョン**）や，試験実施時に用いた外部ハードウェア（例えば，機種名及び識別番号）など，テスト環境に関するハードウェアの情報を**記録**する。
また，**ソフトウェアシステム**試験の実施時に使用した，例えば外部**ソフトウェアシステム**を識別できる情報（例えば，名前および**バージョン**）など，テスト環境に関するソフトウェアの情報も**記録**する。

e) 関連試験ツール
ソフトウェアシステム試験の実施時に使用した，試験ツール，**記録**ツール，統合環境など，試験に使用したツールを識別できる情報（例えば，その名前及びその**バージョン**）を**記録**する。

f) 試験実施日
ソフトウェアシステム試験を実施した日又は期間を**記録**する。一般的には，全ての試験を一度に実施することは少ないと考えるため，どのテストケースをいつ実施したのか追えるように**記録**することが望ましい。

g) 試験の実施及び試験結果の**記録**に関わる責任者の識別
ソフトウェアシステム試験の実施及びその試験結果の**記録**について，責任を持つ者（試験責任者）を識別できる情報を**記録**する。

⑧ システムレベルで使用するためのソフトウェアリリース

5.8.1 ソフトウェア検証の完了確認（クラス A，B，C）

ソフトウェアの**リリース**前に，全てのソフトウェア**検証アクティビティ**が完了し，及びその結果を**評価**したことを確認する必要がある。これは，例えば**リリース**判定会議の形で実施する方法がある。
この**リリース**は，基本的には，量産を前提とした**リリース**でなく，ハードウェアへ組み込んで**システム検証**を実施するための**リリース**を意図している。**リリース**は，一般的には一度きりではなく繰り返されるため，この確認は，**リリース**のたびに実施されるべきである。

5.8.2 既知の残留異常の文書化（クラス A，B，C）

リリースするソフトウェアに残留している既知の**異常**を，全て文書化する必要がある。
対象としては，基本的には問題解決**プロセス**に載せられたソフトウェアの**異常**のうち，残留しているものが対象である。ここでいう残留は，ソフトウェア変更により解決したものや，調査の結果正常であったと判断できたものなどを除いた，未解決又は未対処なものを意味する。例えば，仕様を逸脱した振る舞いであったが再現しないものや，再現し原因も特定できたが軽微な欠陥であるため修正しないと判断されたものなどである。
残留**異常**には，試験で見つかったものだけでなく，設計中に見つかったものやレビューにより見つかったものなどを含める。

5.8.3 既知の残留異常の評価（クラス B，C）

クラスＢ又はクラスＣの場合，箇条 5.8.2 で文書化したすべての残留**異常**について，その**評価**（特に**安全**性についての**評価**）を実施したことを確認する必要がある。また，それら残留**異常**が，受容できない**リスク**の原因にならないことを確認するか，又は受容できない**リスク**の原因にならないように対処する必要がある。
対処については，ソフトウェア変更による欠陥の除去，新たな**リスクコントロール**手段の追加，警告文や警報などによる使用者への情報提供などがある。

5.8.4 リリースするバージョンの文書化 （クラス A，B，C）

リリースする**ソフトウェアシステム**の**バージョン**を文書化する必要がある。ここで文書化する**バージョン**は，一般には**ソフトウェアシステム**全体についての**バージョン**だけで充分と考える。一方で（この箇条の要求事項ではないが），**ソフトウェアシステム**の**バージョン**が特定できれば，その**ソフトウェアシステム**を構成する**ソフトウェアアイテム**及び**ソフトウェアユニット**を特定できるように管理されていることも重要である。

5.8.5 リリースするソフトウェアの作成方法の文書化（クラス B，C）

クラスＢ又はクラスＣの場合，**リリース**する**ソフトウェアシステム**の作成**手順**及び作成環境を文書化する必要がある。例えば，コンパイル／ビルドを実施するために用いるコンパイラなどのツール類や，それを使用するための環境などを文書化し，及びコンパイル／ビルドを実施する**手順**や，コンパイラのオプションなどの設定類などを文書化する。この文書化は，これらの情報だけでコンパイル／ビルドを再現できる水準

で記述することが望ましい。

5.8.6 アクティビティ及びタスクの完了確認（クラス B，C）

クラスＢ又はクラスＣの場合，箇条 5.1 に基づき作成したソフトウェア開発計画の中で計画した全ての**アクティビティ**及び**タスク**が完了し，及び関連する文書化が完了していることを確認する必要がある。
なお，この箇条の注記に「5.1.3 b）参照」とある。これは，ソフトウェア開発と**システム**開発との整合性をとるための**手順**（**システム**結合，**システム検証**，**妥当性確認**など）を忘れないように，という意味と考える。これらは，**システム**レベルで実施するものであるが，これらの**タスク**について，ソフトウェア開発側も責任を持つべきである。そのため，最終的には，これらの**タスク**の完了の確認，及び関連する文書化を含めることが望ましい。その方法として，**システム**設計側の文書を引用することは許容できる。

5.8.7 ソフトウェアのアーカイブ（クラス A，B，C）

次の２つについて，保管期間を定めて保管する必要がある。保管期間は，**製造業者**自身が決定した**ソフトウェアシステム**の耐用期間，又は関連する規制要求事項が規定する期間の，いずれか長い方を最低保管期間として，それ以上の期間とする必要がある。対象範囲は，**リリース**した**ソフトウェアシステム**を網羅することが望ましい。

a） **医療機器ソフトウェア**及び**構成アイテム**

b） 文書

保管は，保管方法などを規程に定め，及び保管管理者を定めるなどして，適切に保管できることを示すことが望ましい。

5.8.8 ソフトウェアリリースの信頼性の確保（クラス A，B，C）

リリースした**ソフトウェアシステム**が，使用する箇所に，信頼できる形で納められることを確実にする**手順**を確立する必要がある。考慮する必要がある事項は，納められるまでに**ソフトウェアシステム**の破損（corruption）の無いこと，及び無断で変更されることの無いことである。
この箇条の要求事項は，ハードウェアへ組み込むために**ソフトウェアシステム**を供給する媒体の製造及び取り扱いに関する事項についてであり，例えば次のようなことを防止し確実に収められるように**手順**を構築すること，及び正しく収められたことを確認する**手順**を構築することである。

- **ソフトウェアシステム**の取り違え（例えば**バージョン**間違い）の無いこと
- 媒体（例えば USB メモリ）へ複製するときの手違いの無いこと
- 媒体の取り違えやすり替えの無いこと
- 媒体上（例えば Ethernet 上）でのファイルの破損の無いこと
  (破損は，例えばデータ化けやアタックなどにより発生しうる)
- **ソフトウェアシステム**をハードウェア内に収めるときの手違いの無いこと

そのため，必要に応じて，次に関することを含めて明確化する必要がある。

- 複製
- 媒体のラベリング
- 梱包
- 保護
- 保管
- 納品

この箇条の要求事項は，**手順**の確立までであるが，その**手順**に従い実施し，及びその結果を**記録**することが望ましい。

5.3.2 ソフトウェア保守プロセス （箇条 6）

ソフトウェア保守**プロセス**は，この規格に適合したソフトウェアを**リリース**した後，そのソフトウェアを修正する**プロセス**である。いわゆる**バージョン**アップのイメージで捉えても良い。
機器全体（**ロボット**介護機器）の**安全**性を IEC 60601-1 に適合させる場合，一般的には，ソフトウェアに対し，この規格の箇条 6 の適用はしない。その理由は次のとおりと考える。

- IEC 60601-1 は，**安全**な機器の設計を意図した規格であり，例えば市販後の**監視**（例えば市場での事故情報の収集など）及び市販後の作業（機器の保守や管理など）は，適用範囲外である。そのため，ソフトウェアに対しても，（IEC 60601-1 の箇条 14.1 の注記 5 にあるように）市販後**監視**及び保守を含まないのである。
- IEC 60601-1 は，機器の変更（問題点の修正など）を直接的には扱っていない。認証後に機器の変更があった場合，一般的には，認証者（第三者認証の場合は認証機関，自己宣言の場合は**製造業者**自身）が，変更の内容を分析し，例えば再試験が必要な箇条があれば再試験を実施し，変更後の規格適合性を判断する。この考えをソフトウェアにも適用するなら，この規格の箇条 6 を適用するのではなく，既に実施した箇条 5 に関して必要な再**評価**を実施する方針になる。それが，結果的に，箇条 6 の適用と同等になる場合はあるかもしれないが，あくまで箇条 5 に関する再**評価**と考える。

派生機種のためのソフトウェアの派生開発は，（世間的には）ソフトウェア保守であると考えることも可能であろうが，上記の理由から，この規格の箇条 6 （ソフトウェア保守**プロセス**）を適用するのは難しい。また，派生開発においても，一般的には，製品の**リスクアセスメント**から再度実施することが望ましいと考えるため，派生開発であっても，箇条 5 （ソフトウェア開発**プロセス**）を適用するのが適切と考える。

ソフトウェア保守**プロセス**全体の概要を下図に示す（規格に示された図とは少し変えてある）。箇条 6.1「ソフトウェア保守計画」及び箇条 6.2「問題及び修正の分析」は，箇条 5「ソフトウェア開発**プロセス**」とは異なる要求事項であるが，それ以降は箇条 5 の必要な**アクティビティ**を実施する形である。

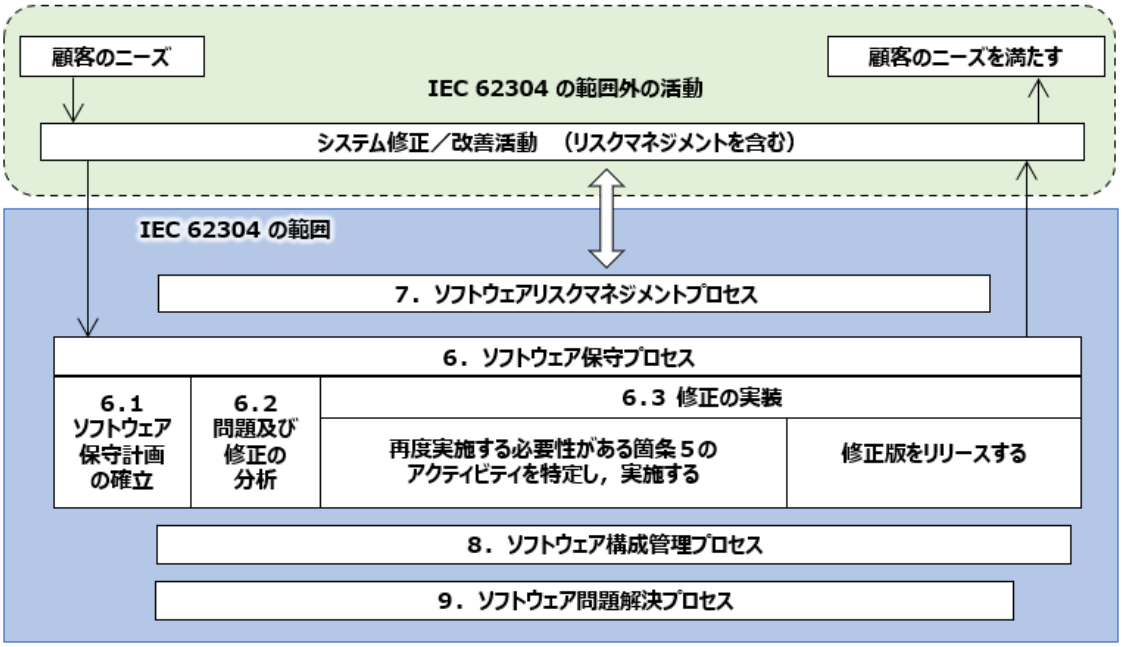


図 5-23 ソフトウェア保守プロセスの概要

① ソフトウェア保守計画の確立

6.1 ソフトウェア保守計画の確立（クラス A，B，C）

ソフトウェア保守計画を確立する必要がある。これは，ソフトウェア保守**プロセス**の**アクティビティ**及び**タスク**を適切に実行するための計画である。計画の内容は，次を考慮したものである必要がある。

a) **医療機器ソフトウェア**の**リリース**後に発生する情報をフィードバックするための**手順**

ソフトウェア**リリース**後の情報を，どのように取得し，文書化し，**評価**し，解決するかを明確にし，計画とする必要がある。そして，これらの**トレーサビリティ**を確保する**手順**を明確にし，計画に含める必要がある。

なお，ソフトウェアの問題に関する情報，特に**安全**性に関わる情報をいかに取得するかは，重要な点である。

b) フィードバックした情報に問題があるかを判断するための基準

上記 a) の，情報の**評価**について，問題点として判断する基準を明確化し，計画に含める必要がある。これは，判断のための体制，運用**手順**，責任などを明確にする方法がある。

c) ソフトウェア**リスクマネジメントプロセス**の使用

上記 b) の基準に従って問題とされた情報に対し，ソフトウェア**リスクマネジメントプロセス**を適用する計画をする必要がある。この**プロセス**は，規格の箇条 7 に適合する**プロセス**であるべきである。このガイダンスの 5.3.3 章も参照されたい。

なお，上記 b) の基準に従って問題ではないとされた情報についても，**リスク分析**を行い，必要に応じてソフトウェア**リスクマネジメントプロセス**を適用することが望ましい。

d) **医療機器ソフトウェア**の**リリース**後に発生した問題を分析及び解決するためのソフトウェア問題解決**プロセス**の使用

上記 b) の基準に従って問題とされた情報に対し，ソフトウェア問題解決**プロセス**の使用を計画する必要がある。この**プロセス**は，規格の箇条 9 に適合する**プロセス**であるべきである。このガイダンスの 5.3.5 章も参照されたい。

e) 既存**ソフトウェアシステム**の修正を管理するための，ソフトウェア**構成管理プロセス**（箇条 8 参照）の使用

上記 d) においてソフトウェア変更を行うことが決定された場合に，そのソフトウェア変更にソフトウェア**構成管理プロセス**を適用することを計画する必要がある。この**プロセス**は箇条 8 に適合する**プロセス**である必要がある。このガイダンスの 5.3.4 章も参照されたい。

f) SOUP について，次の事項を**評価**し実行する**手順**

使用している SOUP について，そのアップグレード，バグ修正，パッチ，陳腐化（保守契約の期限切れなど）などの情報を収集し，内容を**評価**し，対処する**手順**を計画する必要がある。

② 問題及び修正の分析

6.2.1.1 フィードバックの監視（クラス A，B，C）

リリースしたソフトウェアについて，そのフィードバックを**監視**（情報収集）する必要がある。これは，箇条 6.1 の計画に基づいて実施するものである。以下の箇条についても，計画に従って実施するものである。

6.2.1.2 フィードバックの文書化及び評価（クラス A，B，C）

以下の**手順**を実施する必要がある。

- フィードバック（情報）を文書化する。
- フィードバックを**評価**する（例えば，原因や影響を分析し，許容可能かなどを考察する）。
- ソフトウェアに問題が無いかを判断する。
- 問題があると判断した場合は，その問題を**問題報告**として**記録**する。これは，箇条 9 の問題解決**プロセス**を適用することを意味する。作成する**問題報告**には，該当する場合，実際に悪影響を及ぼす事象，悪影響の可能性のある事象，及び仕様から逸脱した事象を含める必要がある。

なお，どのような**問題報告**が望ましいかを事前に検討し，**問題報告**様式を定めておくことが望ましい。

6.2.1.3 安全性に影響する問題報告の評価（クラス A，B，C）

問題報告は，個々に以下を実施する必要がある。

- 問題の内容を**評価**する。
- **リリース**したソフトウェアの**安全**性にどのような影響があるかを判断する。

- 問題に対処するためにそのソフトウェアに変更を加える必要があるかを判断する。

これらは，箇条 9.2 に適合する形で実施するべきである。

6.2.2 ソフトウェア問題解決プロセスの使用（クラス A，B，C）

問題報告の対処は，ソフトウェア問題解決**プロセス**を使用する必要がある。この**プロセス**は，箇条 9 に適合する**プロセス**であるべきである。

この箇条の注記にあるとおり，問題の調査により，**ソフトウェアシステム**又は**ソフトウェアアイテム**のソフトウェア**安全**クラスの修正が示唆されることがあり得る。その場合は，正しいソフトウェア**安全**クラスへの変更及び必要な対処がともに実施されることが望ましい。

市場で発生した問題に対しては，ビジネス上の理由から，素早く対処することが求められることが多い。しかし，素早さを優先するあまり，問題の分析や変更の影響分析が不充分なままソフトウェア変更を実施すると，それが別のより大きな問題を引き起こす場合もある。急ぎの場合であっても，適切な問題解決**プロセス**に従って処理することは重要である。

6.2.3 変更要求の分析（クラス A，B，C）

変更要求の分析は，箇条 9 で要求されている分析を実施する必要がある。それに加え，変更要求が，組織，**リリース**したソフトウェア，及び連携する**システム**に及ぼす影響について分析を行う必要がある。

ここで注意したいのは，影響の分析は，ソフトウェアやそれを搭載した**システム**の範囲に留まらず，例えばその機器（**ロボット**介護機器）を使用している組織への影響や，例えば連携する他の**システム**への影響についても分析することが求められている点である。

6.2.4 変更要求の承認（クラス A，B，C）

変更要求について，**リリース**したソフトウェアの修正を要求する変更要求については，その変更要求を**評価**し，承認する必要がある。箇条 8.2.1 と同様に，ソフトウェアを変更する場合は，必ず承認されることが重要である。

6.2.5 ユーザ及び規制当局への通知（クラス A，B，C）

リリースしたソフトウェアに影響がある，承認済みの変更要求を明らかにする必要がある。そして，それらを，地域の法令の要求に応じて，ユーザ及び規制当局に対して次の事項を通知する必要がある。

a) **リリース**した**医療機器ソフトウェア**についての全ての問題及び変更せずに継続使用した場合の結果。

   リリースしたソフトウェアに関する全ての問題を通知する必要がある。また，その問題を変更せずに継続した場合に考**えら**れる結果を併せて通知する必要がある。

b) **リリース**した**医療機器ソフトウェア**に対して利用可能な変更の本質（nature），並びにそれらの変更の入手及びインストールの方法。

リリースしたソフトウェアの変更の本質（コードをどう変更したかではなく，何を意図してどのような振る舞いに関して変更したかなど）を通知する必要がある。また，変更したソフトウェアの入手方法及びインストール方法を通知する必要がある。

③ 修正の実装

6.3.1 確立したプロセスを使用した修正の実装（クラス A，B，C）

ソフトウェアの変更を行った結果，再度実施する必要性がある箇条 5 の**アクティビティ**を特定し，実施する必要がある。

これは，ソフトウェア変更が，各**アクティビティ**に関係があるかを調べることが重要である。ここでいう関係があるとは，その**アクティビティ**で実施した内容に変更が生じること，特に**成果物**の内容に変更が生じることを意味すると考えて良いだろう。例えば，ソフトウェア**アーキテクチャ**に修正を加える必要があるなら，ソフトウェア**アーキテクチャ**設計の**アクティビティ**と関係がある。その修正をすると，それに対応した**検証アクティビティ**の内容の変更も必要になる。これら，関係がある**アクティビティ**については，必要な再実施を行う。

複数の**アクティビティ**の再実施が必要な場合は，上流（箇条番号の小さい方）から下流へ向けて実施することが重要である。

なお，注記にあるように，ソフトウェア変更の**リスクマネジメント**を忘れてはならない。その要求事項については，このガイダンス 5.3.3 章を参照されたい。

また，これらを実施した結果において，**トレーサビリティ**が確保されていることは重要である。

6.3.2 修正ソフトウェアシステムの再リリース（クラス A，B，C）

変更したソフトウェア（修正版）は，箇条 5.8 に従って**リリース**する必要がある。

なお，機器のソフトウェアが正しく修正版へ変更されるのであれば，この規格は，再**リリース**の方法（及び提供方法）は問わないようだ。

5.3.3 ソフトウェアリスクマネジメントプロセス （箇条 7）

ISO 21856 は**ロボット**介護機器の ISO 14971 に基づく**リスクマネジメントプロセス**の適用を要求している。また，この規格の箇条 4.2 において，ISO 14971 に基づく**リスクマネジメントプロセス**の適用を要求している。

加えて，この規格は，この箇条 7 においても，ソフトウェアに関する**リスクマネジメント**の要求事項を追加している。この箇条 7 の要求事項に基づく活動は，ISO 14971 に基づく**リスクマネジメントプロセス**の活動と一体を成すべきであり，分離して実施するのは不適切である。にもかかわらず，この箇条 7 の要求事項が，この規格に記載されているのは，次の理由からである。

(参考和訳)
a) この規格の利用者は，ソフトウェアという責任領域における**リスクコントロール**手段の最低限の要求事項を理解する必要がある。
b) この規格に引用規格として示している，一般的な**リスクマネジメント**を扱う規格 ISO 14971 は，ソフトウェアの**リスクコントロール**及びソフトウェア**開発ライフサイクル**への**リスクコントロール**導入について特に扱うものではない。
（附属書 B の箇条 B.7 より抜粋）

ソフトウェアの**リスクコントロール**及びソフトウェア**開発ライフサイクル**への**リスクコントロール**導入について，ISO 14971 は特段に扱ってはいないが，一方で，それらの重要性を理解し実践すべきである。
リスクコントロールとは，『規定したレベルまで**リスク**を低減するか又はそのレベルで**リスク**を維持するという決定に到達し，かつ，そのための手段を実施する**プロセス**。』である。
リスクコントロールは，おおよそ次を実践する**プロセス**である。

(1) **リスク**低減策を選択する。
(2) **リスク**低減策を実装する。
(3) **残留リスク**を**評価**する。
(4) **リスク**低減策によって発生した**リスク**をレビューする。
(5) **リスク**低減の達成を確認する。

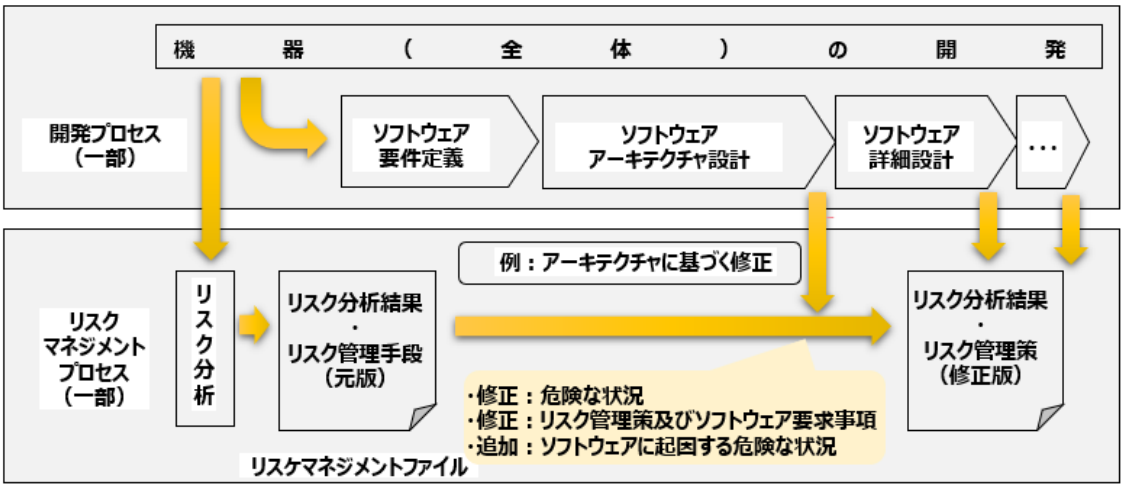


図 5-24 ソフトウェアリスクマネジメントの必要性

例えば，ソフトウェア**アーキテクチャ**の設計中に，ソフトウェアに起因する新たな**リスク**がないか**リスク分析**した**り**，**リスクコントロール**手段に関するソフトウェア要求事項が確実に**リスク**を低減できるものであるかどうかを再検討したりし，問題が見つかれば対処し，有効な**リスクコントロール**手段を改定しなければならない。ソフトウェアの**安全**性を確保するうえでも不可欠な活動であるため，この規格のこの箇条に記載されたものである。そして，このソフトウェア**リスクマネジメントプロセス**により，機器の**リスクマネジメント**の実践に関与し，ソフトウェアの合理的に予見可能な**リスク**を確実に低減することが重要である。
注記 この規格では，「**リスクコントロール**手段」という用語が使われることが多い。この用語については，

主にソフトウェアなどによる**リスク**低減策をイメージし，それに**リスク**低減策を確実にする方策（例えばソフトウェアの**異常**な振る舞いが**リスク**低減策を無効にしないようにする方策）を加えた言葉とイメージすると良い。
ソフトウェア**リスクマネジメント**に関する計画書，**手順**書及び資料は，**ロボット**介護機器に関するそれらの一部分であっても，別紙であっても良い。

① 危険状態を引き起こすソフトウェアの分析

7.1.1 危険状態の一因となるソフトウェアアイテムの特定（クラス B，C）

クラスＢ又はクラスＣの場合，ISO 14971 に規定された**リスク分析**を行い，発生する可能性のある**危険状態**，及びその**危険状態**を引き起こす可能性のある**ソフトウェアアイテム**を特定する必要がある。
ここで求められるのは，機器（**ロボット**介護機器）の**リスク分析**を，**ソフトウェアアイテム**領域にまで広げることである。それを，ISO 14971 の要求事項に従って実施することである。
ソフトウェアアイテム領域の**リスク分析**は，**システム**開発の初期には困難がある。ソフトウェアの**アーキテクチャ**が明らかになり，各**ソフトウェアアイテム**の役割や振る舞いなどが明確になるまで，**危険状態**の一因となり得る**ソフトウェアアイテム**及びその潜在的原因を特定することはできないと考えるためである。そのような理由により，この箇条に基づく特定は，ソフトウェアアークテクチャ設計の結果を入力のひとつとして実施することが適切である。
この箇条の注記が言及しているとおり，**危険状態**は，次が原因となる場合が考**えら**れる。よって，この２つを観点に含めて**リスク分析**をすることが重要である。

- ソフトウェアの**故障**（**障害**）が直接の原因となる場合
  （例えば，装着して使用する人に過大な力がかからないようにモータを制御する**ソフトウェアアイテム**が**異常**動作しモータを過大に駆動すると，使用者に**危害**を加えてしまう可能性がある場合。この場合，ソフトウェアは通常の機能を実現するためのものでもある。）
- ソフトウェアに実装した**リスクコントロール**手段の**故障**（**障害**）が原因となる場合
  （例えば，火傷を防ぐための過熱防止手段として実装された**ソフトウェアアイテム**が正常動作しなくなり，過熱を防止できなくなると，使用者が火傷をしてしまう可能性がある場合。この場合，ソフトウェアは保護を目的としたものである。）

ここでは，ソフトウェアの一般機能に関する単一**異常**（単一欠陥など），又はソフトウェアに実装した**リスクコントロール**手段の単一**異常**までを考慮することが一般的であるが，**リスク**を許容可能な水準まで低減するためには，多重**異常**を考慮する必要がある場合があるかもしれない。その判断は**リスクマネジメント**に従うべきものである。
なお，クラスＡの場合でも，**危険状態**の発生は想定でき無いことを，この段階で再確認することが望ましい。

7.1.2 危険状態の一因となるソフトウェアアイテムの潜在的原因の特定（クラス B，C）

クラスＢ又はクラスＣの場合，箇条 7.1.1 で特定した**危険状態**の一因となり得る**ソフトウェアアイテム**について，その潜在的原因を特定する必要がある。具体的には，次に挙げるような潜在的原因を必要に応じて検討する。特定された潜在的原因は，**リスクマネジメントファイル**に記載する必要がある。箇条 7.1.4 も参照されたい。

a) 誤った又は不完全な機能仕様

機能の仕様に誤りがあったり，又は不完全であったりした場合に，それが**危険状態**の一因になり得るならば，それを潜在的原因として特定する。

例えば，装着型**ロボット**のモータ制御の仕様に間違いがあり過大な駆動を行うと，使用者に**危害**を加えてしまう可能性がある場合，その仕様間違いによるモータの過大な駆動を，潜在的原因として特定する。

b) 特定した**ソフトウェアアイテム**の，機能におけるソフトウェア不具合

箇条 7.1.1 で特定した**ソフトウェアアイテム**の機能に欠陥があった場合に，それが**危険状態**の一因になり得るならば，それを潜在的原因として特定する。

例えば，過熱防止のための**リスクコントロール**手段を構成する温度検知モジュールが，**異常**温度の検出に失敗すると危険である場合，その**ソフトウェアアイテム**による**異常**温度の検出の失敗を潜在的原因として特定する。

c) SOUP に起因する，**故障**（**障害**）又は予期せぬ結果

SOUP に起因する**故障**（**障害**）又は予期せぬ結果が，**危険状態**の一因になり得るならば，それを潜在的原因として特定する。これについては，SOUP の既知の**異常**を考慮に含めることが重要である。箇条 7.1.3 も参照されたい。

一方，SOUP が正常に動作した場合であっても，他の**ソフトウェアアイテム**との整合性が**危険状態**の一因となり得る場合について，それも潜在的原因として特定することが重要である。例えば，ある設計した**ソフトウェアアイテム**が求める応答速度に対し，SOUP アイテムの応答速度が遅い場合があり得て，それが**危険状態**の一因となり得る場合，などである。

d) 予測できないソフトウェア動作を引き起こす可能性のある，ハードウェアの**故障**又は他のソフトウェアの欠陥

ハードウェアの**故障**又は他のソフトウェアの欠陥が，予測できないソフトウェア動作を引き起こす可能性があり，それが**危険状態**の一因になり得るならば，それを潜在的原因として特定する。

例えば，**安全**に関連するデータを保存するメモリが**故障**してデータ化けが発生した場合，それが**危険状態**を引き起こし得るならば，それを潜在的原因として特定する。

e) **合理的に予見可能な誤使用**

合理的に予見可能な誤使用が**危険状態**の一因になり得るならば，それを潜在的原因として特定する。

例えば，装着型**ロボット**の装着場所や装着**手順**を間違えた状態で使用した場合に，使用者に**危害**を与えてしまう可能性があるならば，それを潜在的原因として特定する。なお，これら以

外にも潜在的原因が考**えら**れるのであれば，それを含めて特定することが重要である。

7.1.3 公開された SOUP 異常リストの評価（クラス B，C）

クラスＢ又はクラスＣの場合，箇条 7.1.2 で特定した，SOUP に起因する**故障**又は予期せぬ結果が，**危険状態**の一因となる**ソフトウェアアイテム**の潜在的原因になっている場合について，次を行う必要がある。

a) 機器（**ロボット**介護機器）に使用している SOUP アイテムの**バージョン**を特定する。

b) 上記 a) に関係する，SOUP アイテムの供給者が公開している**異常**リストの内容について，その影響を**評価**する。また，必要に応じて類似の情報を**評価**することも重要である。

c) 上記 b) に基づき，既知の**異常**のいずれかによって，**危険状態**の原因となる可能性がある一連の事象が生じるかを判断する。判断の結果は，文書化することが望ましい。箇条 7.1.4 も参照されたい。

7.1.4 潜在的原因の文書化（クラス B，C）

クラスＢ又はクラスＣの場合，箇条 7.1.2 で特定した，**危険状態**の一因となる**ソフトウェアアイテム**の潜在的原因を，**リスクマネジメントファイル**に文書化する必要がある。これには，箇条 7.1.3 で判断した，SOUP の既知の**異常**によって生じ得る，**危険状態**の原因となる可能性がある一連の事象を含めることが望ましい。

なお，この文書化は，**リスクマネジメントファイル**の一部として位置づけられれば，ひとつのファイルにまとめられた形でも，別ファイルに分けられた形でも，良い。

② リスクコントロール手段

7.2.1 リスクコントロール手段の選択（クラス B，C）

クラスＢ又はクラスＣの場合，**リスクマネジメントファイル**に文書化した，**ソフトウェアアイテム**が**危険状態**の一因となるケースのそれぞれについて，**リスクコントロール**手段を適切に選択し，それを文書化する必要がある。**リスクコントロール**手段の選択は，ISO 14971 に適合する方法で実施する必要がある。この箇条の注記に言及があるように，選択する**リスクコントロール**手段（**リスク**低減策）は，ソフトウェアに限る必要は無く，ハードウェアにより実現する方法（例えば装着型**ロボット**の過熱防止の制御に失敗したときのために温度ヒューズを付けるなど）や，動作環境において実施する方法（例えば移動型**ロボット**の制御の失敗により**ロボット**が階段から転落して事故を起こさないように，階段前には**ロボット**が乗り越**えら**れない高さの段差を設けるなど），取扱説明書に記載する（例えば注意書きを記載する），などの方法によっても良い。ただし，ISO 14971 の箇条 6.2 に記載された優先順位（3 step method）に従って選択することが重要である。

7.2.2 ソフトウェアに実装するリスクコントロール手段（クラス B，C）

クラスＢ又はクラスＣの場合，**リスクコントロール**手段を**ソフトウェアアイテム**の機能の一部として実装する場合について，次の事項を実施する必要がある。

a) **リスクコントロール**手段をソフトウェア要求事項に含める。

リスクコントロール手段を実装する場合は，その**リスクコントロール**手段を要求することを，ソフトウェア要求事項のひとつとして文書に含める必要がある。

ソフトウェア要求事項に無い事項を実装することは，何をもって正しいソフトウェアであると判断するかの基準であるソフトウェア要求事項と，実際に実現するソフトウェアとの間の不整合を引き起こし，そのことによる**トレーサビリティ**の混乱や，適切な**検証**の基準の混乱などを引き起こし，結果としてソフトウェアの品質を低下させてしまう可能性がある。よって，実装する内容は，必ずソフトウェア要求事項を示して，整合性を確保し，そして**トレーサビリティ**を確認することが重要である。

ここで，新たなソフトウェア要求事項を追加する場合，又は既存のソフトウェア要求事項を修正する場合は，**システム**要求事項との整合性も併せて確保することが望ましい。

b) **リスクコントロール**手段の実施に寄与する各**ソフトウェアアイテム**に対して，その**リスクコントロール**手段によってコントロールしている**リスク**に基づいて，ソフトウェア**安全**クラスの分類を行う［4.3 a）参照］。

リスクコントロール手段の実現に関わる各**ソフトウェアアイテム**について，ソフトウェア**安全**クラスの分類を行う必要がある。この分類は，**リスクコントロール**手段によってコントロールする**リスク**に基づき，箇条 4.3 の a）に記載された基準を適用して決定する必要がある。

このとき，既にソフトウェア**安全**クラスの分類が行われた**ソフトウェアアイテム**に対しても再検討を行い，必要に応じて別のソフトウェア**安全**クラスへ変更することは重要である。

c) 箇条 5 に従って**ソフトウェアアイテム**を開発する。

上記 b）で明確化したソフトウェア**安全**クラスに基づき，箇条 5 のソフトウェア開発**プロセス**の要求事項に従って，**ソフトウェアアイテム**を開発する必要がある。

なお，箇条 7.1.1 の実施は，ソフトウェア開発**プロセス**の成果の一部（特にソフトウェア**アーキテクチャ**設計の成果）を入力に含めることが重要であることを踏まえると，この規格は，**プロセス**の繰り返しを要求しているかのように見える。これを，どう解釈してどのような**プロセス**に落とし込むかは，**製造業者**が選択して良いと考える。例えば，反復が必要と考えて反復**プロセス**としても良いし，当初のソフトウェアアーキクテクチャ設計までをプロトタイピングとしても良いと考える。

③ リスクコントロール手段の検証

7.3.1 リスクコントロール手段の実施の検証（クラス B，C）

クラスＢ又はクラスＣの場合，箇条 7.2 で文書化した**リスクコントロール**手段について，それらを全て実現していることを**検証**し，その**検証**結果を文書化する必要がある。また，それらの**リスクコントロール**手段をレビューし，その手段によって新たな**危険状態**に至ることがないか判断する必要もある。

これは，箇条５のソフトウェア開発**プロセス**の最終段階だけに実施するのではなく，例えばソフトウェア**アーキテクチャ**設計の**成果物**に対しても**検証**を行うなど，ソフトウェア開発**プロセス**の途中段階においても実施することが望ましい。

リスクコントロール手段により新たな**危険状態**に至る例としては，移動型**ロボット**の移動停止方法の例が考**えら**れる。人との衝突を避けるために，人との距離を**監視**して，危険な距離の場合は移動を停止する**リスクコントロール**手段を実装したとする。距離がとても近いときには，瞬時に移動を停止させる仕様としたところ，ブレーキが急すぎて，移動型**ロボット**が人の方向に倒れてしまうという，新たな**危険状態**が発生する可能性が考**えら**れる。別の例としては，複数の**リスクコントロール**手段が衝突（conflict）して危険を招く例として，（ソフトウェアの例ではないが）自動車にチャイルドシートを取り付ける場合の例がある。チャイルドシートを助手席に取り付けた場合，取り付け方によっては，その席のエアバッグを停止させておかないと，エアバッグ作動時に，エアバッグがチャイルドシートを突き飛ばして，子供を車の座席にたたきつけてしまう事故が発生する可能性が考**えら**れる。**安全**のための方策が思わぬ危険を招かないように注意されたい。

7.3.3 トレーサビリティの文書化（クラス B，C）

クラスＢ又はクラスＣの場合，ソフトウェアに関連する事項の**トレーサビリティ**について文書化する必要がある。内容については，次の**トレーサビリティ**を適宜文書化する。文書化の方法として，例えば**トレーサビリティ**マトリクスを使用する方法がある。

a) **危険状態**から**ソフトウェアアイテム**まで
リスク分析により特定された**危険状態**と，関連する**ソフトウェアアイテム**との間の**トレーサビリティ**を，文書化する。

b) **ソフトウェアアイテム**から特定のソフトウェアの原因まで
各**ソフトウェアアイテム**と，**危険状態**の一因となり得る**ソフトウェアアイテム**の潜在的原因との間の**トレーサビリティ**を，文書化する。

c) ソフトウェアの原因から**リスクコントロール**手段まで
ソフトウェアアイテムの各潜在的原因と，対応する**リスクコントロール**手段との間の**トレーサビリティ**を，文書化する。

d) **リスクコントロール**手段から**リスクコントロール**手段の**検証**まで
各**リスクコントロール**手段と，対応する**リスクコントロール**手段の**検証**（内容及び結果）との間の**トレーサビリティ**を，文書化する。

④ ソフトウェア変更のリスクマネジメント

7.4.1 医療機器ソフトウェアの安全性に関わる変更の分析（クラス A，B，C）

機器（**ロボット**介護機器）のソフトウェアの変更について，その変更の内容を，次の観点で分析し，及び判断を決定する必要がある。この分析は，SOUP を含める必要がある。

a) **危険状態**の一因となる潜在的原因が新たに生じていないか。
ソフトウェアの変更により，例えば変更した**ソフトウェアアイテム**が他の**ソフトウェアアイテム**へどのような影響を与えるかを調査するなどして，ソフトウェアの振る舞いがどのように変化するか及びその変化が**システム**へどのような影響を及ぼすかを分析し，**危険状態**の一因となる潜在的原因が新たに生じていないかどうかを判断する。

b) 新たなソフトウェア**リスクコントロール**手段が必要でないか。
ソフトウェアの変更により，例えば，**危険状態**の一因となる潜在的原因が新たに生じていた場合や，あるいは，既知の潜在的原因ではるが**危険状態**に至る可能性がそれまでよりも高まった場合などに，新たな**リスクコントロール**手段が必要となるかもしれない。そのようなことの有無を分析に基づいて判断する。

ソフトウェア変更は，その影響をよく分析しないと，思わぬ副作用を招く場合があるため，**リスク**に関する悪影響をよく分析することが重要である。次の箇条 7.4.2 の重要性についても，同じ理由である。
分析及び判断の結果は，箇条 7.4.3 で用いる。

7.4.2 ソフトウェア変更が既存のリスクコントロール手段に与える影響の分析（クラス B，C）

クラス B 又はクラス C のソフトウェアの変更について，その変更の内容を，次の観点で分析し，及び判断を決定する必要がある。これは，SOUP を含める必要がある。

a) ソフトウェアの修正が既存の**リスクコントロール**手段の妨げとなる危険性がないか
ソフトウェア変更により，例えば変更した**ソフトウェアアイテム**が，**リスクコントロール**手段を実現するための**ソフトウェアアイテム**の機能や性能を阻害したり，あるいは，ソフトウェア変更が**リスクコントロール**手段そのものを無効化したりしていないかなどを分析し，危険性の有無を判断する。
分析及び判断の結果は，箇条 7.4.3 で用いる。

7.4.3 分析に基づくリスクマネジメントアクティビティの実行（クラス B，C）

クラス B 又はクラス C の場合，ソフトウェア変更に関する箇条 7.4.1 及び箇条 7.4.2 の分析（及び判断）の結果に基づき，箇条 7.1～7.3 で規定した**リスクマネジメント**の**アクティビティ**を実行する必要がある。実行する内容につては，箇条 7.1～7.3 を参照されたい。

5.3.4 ソフトウェア構成管理プロセス （箇条 8）

ソフトウェア**構成管理**とは，ソフトウェア開発／保守**プロセス**をとおして，**成果物**及び関連する**要素**を識別し，その関係と変化を管理することと言えるだろう。ソフトウェア**構成管理**により，特定の時点における構成の再現及び追跡を可能にする。ソフトウェア**構成管理**は，一般に変更管理（構成**要素**などの変更実施の管理）及び**バージョン**管理（構成**要素**などの変更履歴の管理）を含む。これらにより，特定の時点における構成**要素**の再現及び追跡も可能にする。

ソフトウェア**構成管理**は，箇条 5.1.9「ソフトウェア**構成管理**計画」に基づいて計画され実施される必要がある。ソフトウェア**構成管理**の対象として，この規格は，コンパイル／ビルドに関係する，ソースコード，ライブラリ及び実行形式だけでなく，管理すべき文書も含めることを意図している。箇条 5.1.8「文書化計画」の注記を参照されたい。

① 構成識別

8.1.1 構成アイテム識別手段の確立（クラス A，B，C）

ソフトウェア**構成管理**の基本として，管理すべき**構成アイテム**を一意に識別する仕組み及びそれらの**バージョン**を一意に識別する仕組みを確立する必要がある。例えば全ての**構成アイテム**の名を一意に付与し，及びそれらの変更時に**バージョン**を一意に付与するルールなどを設け，これを文書化することが望ましい。ここでは，「仕組みを確立する」ことが要求されているため，「一意に識別できた」という結果だけでは，この箇条に適合しない。

8.1.2 SOUP の特定（クラス A，B，C）

構成アイテムが SOUP である場合は，SOUP の識別に関して上記 a) ～ c) を文書化する。この情報は，例えば SOUP の製造事業者から SOUP の特定の**バージョン**における不具合の情報が提供されたとき，使用した SOUP が該当するかどうか判別できる内容である必要がある。

標準ライブラリとは，プログラミング言語がもともと用意している，サブルーチン，マクロ定義，グローバル変数，クラス定義などのことだと言って良いだろう。例えば，C 言語であれば，include 文を用いて ”stdio.h” を含める宣言をすれば，文字列を出力する関数 “printf()” などが使えるようになる。これは，標準ライブラリの使用の一例である。標準ライブラリを使用した場合も，上記要求事項に従い，文書化しなければならない。

8.1.3 システム構成文書の特定（クラス A，B，C）

コンパイル／ビルドを実行して作成した**ソフトウェアシステム**について，それを構成する**構成アイテム**と，各**構成アイテム**の**バージョン**を，一組のものとして文書化する必要がある。

ソフトウェアの開発／保守を行う過程で，ソフトウェアは繰り返しコンパイル／ビルドされ提供される。これ

は，完成版としての正式**リリース**だけではなく，各種の**検証**及び**妥当性確認**のためにも提供される。それらの場合でも，この文書化の対象になり得る。ただし，どの範囲を文書化の対象にするのか（例えば，**システム**設計側へ提供するものを対象とするのか，あるいはソフトウェア設計者が自ら試験したりデバッグしたりするためのコンパイル／ビルドも含めるのか）は，**製造業者**の計画による。

Tech. Tips

バージョン管理ツール

バージョン管理は，一般に，**バージョン**管理ツールを用いて実施する。

バージョン管理ツールの使用は，次のようなメリットがあると考える：

・ 変更履歴の**記録**： どのファイルに，いつ，どのような変更がなされたのか，全て**記録**される。これにより，後日，全ての変更の確認が可能である。

・ 競合の解消： 複数名が同じファイルを同時に変更しようとした場合，例えば後から上書きした人が，別の人による前の変更を消してしまわないように，処理できる。

・ 以前の状態への復帰： 例えば，変更した結果に大きな問題が見つかり，その変更を元に戻したい場合，元に戻せる。あるいは，うっかりファイルを削除してしまったとしても，元に戻せる。

・ デグレードの防止： デグレードの原因になり得ることのひとつが，バグのある古いファイルをうっかり使ってしまうことである。そのような手動では起こり得るミスを防ぐ。

・ 派生版の管理： 例えば，試験のために特別な改造をした派生版を，本来の版と混じらないように並行して管理できる。

・ 工数削減： **バージョン**管理を自動化することにより，工数を削減できる。

バージョン管理ツールは，ソースコードなどのソフトウェア自体のファイルだけでなく，それに関連するファイル（例えば，設計仕様書や**トレーサビリティ**文書など）も，合わせてファイル管理することも可能である。ただし，**バージョン**管理**システム**はテキスト前提のものが多いようなので，限界がある。

［備考］ **バージョン**管理**システム**としては，以前は Subversion（SVN）が多く用いられていたようだ。これはサーバにて集中管理することを中心に考**えら**れた**システム**である。最近は，Git が人気のようだ。これは各作業者のＰＣ上での分散管理を中心に，その結果をサーバへ反映させる考え方の**システム**である。

② 変更管理

8.2.1 変更要求の承認（クラス A，B，C）

ソフトウェア**構成管理**の対象とした**構成アイテム**の変更は，変更実施の前に変更の承認が必要である。管理されていない変更は，容易に欠陥を呼び込み，予測困難な弊害を発生させ得る。また，文書間（例えば詳細設計書とソースコードとの間）の乖離が起こり，ソフトウェアの振る舞いが予想できなくなっていき，予期せぬ事態を招き得る。

変更を管理するため，変更は，変更要求の形で変更したい内容を明示し，それを承認の権限を持つ者（又は組織）により承認し，それが**記録**されることが望ましい。ただし，その承認の**記録**は，規格の附属書Ｂによれば，『変更管理会議議事録，承認署名又はデータベース上の**記録**であっても良い』。

変更管理の開始は，5.1.9「ソフトウェア**構成管理**計画」に従って開始する。

8.2.2 変更の実装（クラス A，B，C）

変更要求が承認されたら，変更を変更要求に記述されたとおりに実施しなければならない。例えば，承認された変更のついでに，更なる改善をしようとしたり，別のちょっとした変更もやってしまったりすると，それが予期せぬ結果を招きかねない。それらも必要と考えるのであれば，変更要求を提出し承認を受けるべきである。一方，承認された変更要求を放置し実装しないことも不適合にあたる。

変更は，その手続きを事前に定め，その手続きに従って実施することが望ましい。

変更は，例えばソフトウェア**アーキテクチャ**の変更を含むかもしれない。その場合は，箇条 5.3「ソフトウェア**アーキテクチャ**の設計」以降の**アクティビティ**をやり直さなければならないかもしれない。また，その変更により，各**ソフトウェアアイテム**のソフトウェア**安全**性クラスの分類を見直すべきかもしれないし，新たな**リスク**の可能性を調査しなければならないかもしれない。よって，やり直しが必要な**アクティビティ**を特定し，それらを実施する必要がある。

8.2.3 変更の検証（クラス A，B，C）

変更は，**検証**する必要がある。

箇条 5.7.3「変更後の再試験」及び箇条 9.7「ソフトウェア問題解決の**検証**」を考慮して，変更の適切さを，試験やレビューにより**検証**しなければならない。**検証**内容には，例えばメモリアクセスの方法を変えた場合は，メモリアクセスが関連する試験をやり直すなど，必要なやり直しを含める。また，特に問題解決のための変更の場合は，新たな問題が発生していないことの確認を含める。

検証に関する手違いの無いように，事前に計画して**手順**に従い実施することが望ましい。

8.2.4 変更のトレーサビリティを実現する手段の提示（クラス A，B，C）

ここでは、以下の a）～ c）について，それらの間の関連性及び依存関係をいつでも追えるように，**記録**を残す必要がある。この**記録**は，最新の状態に維持（maintain）する。

a) 変更要求
b) 当該**問題報告**
c) 変更要求の承認
この**記録**は，変更が管理されたものであることのエビデンスとして有効なものであるべきである。また，後日問題が発生したときに，その原因の調査に役立つものであるべきである。
この**記録**は，何らかの管理ツールを用いた**記録**でも良い。

③ 構成状態の記録

8.3 構成状態の記録（クラス A，B，C）

ソフトウェアの**システム**構成及び各**構成アイテム**について，それぞれの履歴を保存する必要がある。これは，すべての変更について，いつどのような変更がなされたのかを検索できるものである必要がある。この**記録**は，8.2.4 の**トレーサビリティ**の**記録**と同様に，役立つものであるべきである。
この**記録**は，例えば**バージョン**管理ツールを用いた**記録**でも良い。

5.3.5 ソフトウェア問題解決プロセス （箇条 9）

ソフトウェアに問題が見つかった時には，ソフトウェア問題解決**プロセス**を適用する必要がある（ただし，ソフトウェア問題解決**プロセス**の適用期間外を除く）。ここで言う問題とは，**安全**性に関係するソフトウェアの欠陥だけでなく，ソフトウェアの振る舞いが**意図する使用**に対して不適切である場合や，単にソフトウェアの設計仕様と一致していない場合などを含む。
注記：複雑化してしまったフローチャートを整理したい場合のような，一般に言う問題ではないが，ソースコードを変更したい場合も含めることも可能であるが，この場合については，**安全**性に関する分析及び**検証**を，箇条 8.2 の変更管理にて実施できるので，含めなくても良い。
ソフトウェア問題解決**プロセス**は，すべてのソフトウェア**安全**クラスに対して適用する。これは，次のような理由によるためと理解すると良い：

- **安全**性に無関係な問題のように見えていたが，よく調べてみたら関係していた，ということがあり得るため，すべての問題に対し**安全**性の分析が必要である。
- 問題解決のための変更を，弊害をよく考えずに実施したところ，**安全**性に悪影響が出た，ということがあり得るため，変更の**安全**性に対する影響を分析する必要があり，**安全**性に悪影響のない解決方法が明確化できた場合は，その実装を間違えずに行う必要がある。

ソフトウェア問題解決**プロセス**は，基本的には問題ごとに実施する。異なる問題に対して同一の変更で対処する場合は，一方がもう一方の記述を引用しても良い。
ソフトウェア問題解決**プロセス**の開始は，箇条 5.1.9「ソフトウェア**構成管理**計画」にて作成した計画による。

① 問題報告の作成

9.1 問題報告の作成（クラス A，B，C）

問題解決の**プロセス**は，まず，発見された問題の報告から始まる。**問題報告**は，問題ごとに作成する。

問題報告の内容として要求されているのは，次の２点である：

・重大性に関する記載：例えば，機能，性能，**安全**又は周囲に関して，どのような影響を及ぼす問題なのかを記述する。特に受容できない**リスク**が予想される場合は，それを記述する必要があると考える。

・問題解決に役立ちそうな他の情報：もし影響を受ける機器などがあれば記述する。他には，問題発見時の状況（使用環境など），発生条件（試験**手順**や設定，発生確率など），期待結果からの差異，ソフトウェア**バージョン**などを記述すると良い。
その他，表題，プロジェクト名，発見者及び発見日を記述するのも一般的である。また，重大度ランクや期限などを記述しても良い。

注記にあるように，**リリース**後に見つかる問題，及び組織外部（例えば使用現場）で見つかる問題点についても，放置せずに対処する仕組みが確立されているべきである。

問題報告の様式には指定が無く，**製造業者**が任意に定めて良い。また，必ずしも責任者が押印した紙の文書として作成する必要はないと考える。例えば「バグ管理**システム**」（図 5-25 一般的な問題処理の流れ を参照）に登録された「バグ票／チケット」であっても，規格に適合するよう適切に運用及び管理されていれば，適合すると考える。

② 問題の調査

9.2 問題の調査（クラス A，B，C）

問題報告を受け，次の**タスク**を実施する：

a) 問題を調査し，可能であれば原因を特定する。
問題の調査方法には，動的な調査（再現試験など）及び静的な調査（設計書の調査など）がある。問題の原因は，あるコーディングのミスかもしれないし，ある要求仕様に書かれた条件の抜けかもしれない。原因の特定は，その原因により引き起こされうる振る舞いの説明を含むことが望ましい。

b) ソフトウェア**リスクマネジメントプロセス**（箇条 7 参照）を用いて，その問題の**安全**性への関わりを**評価**する。
問題に関して**リスク分析**を行い，問題が**危険状態**の一因となり得るのかどうかを判断し，なり得る場合は一因となり得る**ソフトウェアアイテム**を特定し，**リスクコントロール**手を用いて対処できるかなどを検討し**評価**する。

c) 調査及び**評価**の結果を文書化する。

上記 a) 及び b) について文書化する。可読性のため，事前に様式を定めておくことを推奨する。

d) 問題の是正に必要な処置のための変更要求を作成する，又は処置を行わない場合の正当な根拠を文書化する。

問題点を修正するための変更を行いたい場合は，変更要求を作成する。これは，上記 c) に基づく形で，何をどのように変更することを要求するのかを明確化し文書化する。これは，ツール上の文書化でも良いと考える。

一方，処置を行わない場合は，その旨及び根拠を文書化する。これには，受容できない**リスク**の無いこと及びその根拠を示すことが重要である。

注記に，ソフトウェア問題解決**プロセス**を用いなくて良い条件について記述があるが，少なくとも**安全**性との関連の有無は，調査して明確化する必要がある。そのため，すべての問題に対しソフトウェア問題解決**プロセス**を用いても良い。その理由には，ソフトウェア問題解決**プロセス**の各箇条はすべて『（クラス A，B，C）』と指定されていること，また，実際のソフトウェア開発／保守においては，**安全**性に関連する問題への対処と，**安全**性に関連が無い問題への対処を，分けて管理することは，業務**手順**の複雑化を招くと考**えら**れること，がある。

③ 関係者への通知

9.3 関係者への通知（クラス A，B，C）

問題は，通知すべき関係者へ通知する必要がある。これは，問題（特に**安全**に関連する問題）の存在を共有しトラブルを回避することを目的にしていると考**えら**れる。

通知すべき関係者は，例えば作成したソフトウェアが共有された範囲に応じて変わってくる。問題が発生してから状況を考え通知先を選ぶのではなく，事前にルールを設けることが望ましい。

④ 変更管理プロセスの使用

9.4 変更管理プロセスの使用（クラス A，B，C）

変更する場合は，箇条 8.2「変更管理」の要求事項に適合する**プロセス**を用いて，変更要求を承認し，承認された通りに実装し，実装の結果を**検証**するとともに，**トレーサビリティ**に関する**記録**を維持する必要がある。

なお，『全ての変更要求を承認し，実行する』という記述は，「変更要求が提出された場合は全て，却下せず承認して変更を実行すること」を要求しているのではなく，「変更要求を放置してはならない」という意味である。提出されたある変更要求が，正当な理由（例えば副作用として重大な**リスク**が予想される）により，却下され戻されることは，不適合に当たらない。その場合は，新たな変更要求を作成するか，又は変更を行わない正当な根拠を文書化する。

⑤ 記録の保持

9.5 記録の保持（クラス A，B，C）

問題報告，実施した解決策，及び**検証**結果について，**記録**を保持する必要がある。保持の期間は，**製造業者**が定めて良いと考える。この**記録**は，箇条 9.4 における承認及び実施の**記録**など，関連する**記録**も保持することが望ましい。

また，実施したソフトウェア**リスクマネジメント**（箇条 9.2 など）に従い，**リスクマネジメントファイル**を適宜更新し保持する必要がある。

⑥ 問題の傾向分析

9.6 問題の傾向分析（クラス A，B，C）

ソフトウェアの欠陥は偏在すると言われることがある。例えば特定の機能で症状が多発したり，特定の**ソフトウェアアイテム**に欠陥が集中したりする。**問題報告**を集めて傾向分析を実施し，把握する必要がある。

分析は，機能，性能，品質特性，ソフトウェア構造，**アクティビティ**，デグレードなど，いろいろな切り口で行うことができる。この分析により，まだ発見できていない問題がありそうな不安な部分を示すことができる。

併せて，問題の発生が収束して充分な品質が達成できたと見なせる傾向であるかどうかも分析することが望ましい。これは，一般に「バグカーブ」とか「信頼度成長曲線」などと呼ばれるグラフを用いて分析することが多い。

⑦ ソフトウェア問題解決の検証

9.7 ソフトウェア問題解決の検証（クラス A，B，C）

問題の解決の判断に必要な**検証**（分析を含む）を実施して，次の項目について判断する必要がある。これらの項目について合致しない項目があれば，それを問題として，ソフトウェア問題解決**プロセス**を行う必要がある。

a) 問題を解決し，**問題報告**を完了した。
問題報告に記された問題が修正され，試験又は／及びレビューによる確認が行われ，問題が解決した報告が完了したことを，確認する。

b) 好ましくない傾向を改善した。
箇条 9.6「問題の傾向分析」での分析の結果が，特に悪い傾向を示さないことを確認する。

c) 変更要求を，適切な**医療機器ソフトウェア**及び**アクティビティ**に実装した。
この意味は，「変更要求を，ソフトウェアに適切に実装し，及びその実装は適切な**アクティビティ**で実行した。」という意味であると解釈すると良い。このことを確認する。

d) 新たな問題が発生していない。

この判断基準については，基本的には修正による弊害がないことを意図している。つまり，弊害の無いことを確認するための**回帰テスト**も必要に応じて実施する必要がある。そのような意味で，新たな問題が発生していないことを確認する。

⑧ 試験文書の内容

9.8 試験文書の内容（クラス A，B，C）

変更の**検証**のために実施した試験について，以下 a) ～ g) の**記録**を文書化する必要がある。

a) 試験結果

b) 発見した**異常**

c) 試験したソフトウェアの**バージョン**

d) 関連するハードウェア及びソフトウェアテスト構成

e) 関連試験ツール

f) 試験実施日

g) 試験者の識別

記述する内容について，後日，同じ試験を再現し同じ判断ができる程度に詳細であることが望ましい。特に「試験結果」については，試験観点，試験環境及びテストケースを含めるか，又はそれらが追跡可能であることが望ましい。

なお，「変更の後に実施する」の意味は，スケジュール上の前後の話ではなく，変更を理由として実施するもの，という意味である。

Tech. Tips

問題管理のためのツール

ソフトウェアに関する問題の管理は，「BTS（Bug Tracking System）」，「DMS（Defect Management System)」，あるいは「バグ管理**システム**」などと呼ばれるツールを使用することが一般的である。規格は，このような**システム**の使用を要求してはいないが，使用することを推奨する。

◇どのような場合にバグ管理**システム**が必要か

特に次のような場合は，バグ管理**システム**を使用することを強く推奨する：

・ ソフトウェアの規模がある程度大きく，ソフトウェア設計者やソフトウェア試験担当者が，複数名いる場合。

・ 問題の数が少なくない場合（例えば数十件を超える場合）。

・ 修正漏れや連絡ミスなど，作業に関する「うっかり」を防止するために，作業フローを自動化したい場合。

問題の数が少数で，かつ関係者が少人数なら，問題の管理者が，表計算ソフトウェアなどを利用して手

動で管理することも現実的と思われるが，それ以外の場合，バグ管理**システム**を用いることを推奨する。理由としては，例えば箇条 9.3「関係者への通知」への適合の確認のため，通知漏れがないかどうか確認するとき，通知を手動で行っていた場合は，個別の連絡をそれぞれ確認しないと通知漏れがあったかどうか明らかにならないが，バグ管理**システム**を用いた自動化を行っていた場合は，その自動化の内容及び 1 件の事例を確認すれば充分と考**え**られる。これは，問題点数が多くなれば，及び関係者が多くなれば，大きなメリットになる。

◇バグ管理**システム**を用いた作業フローの例

バグ管理**システム**を用いた問題の処理の流れは，職場ごとに少しずつ異なるであろうが，一般的には次のような流れをイメージすると良い。

	ステータス
問題の発見者が，バグ票を起票する（「チケットを発行する」とも言う）。	Open
↓	
問題管理者が，修正担当者を指名する。	Assigned
↓	
修正担当者が，問題を修正し報告する。	Resolved
↓	
発見者が，修正を確認し報告する。	Confirmed
↓	
問題管理者が，完了を確認する。	Closed

図 5-25 一般的な問題処理の流れ

これらの作業を，各担当者がブラウザ画面上で行う**システム**が多い。作業を行ったとき，関係者へ電子メールが自動で送信されるようにすることができる。他にも，いろいろな機能がある場合が多い。

◇バグ管理**システム**に関する追加情報

問題点管理者は，問題点の処理を管理するだけでなく，全体を俯瞰したマネジメント（分析，課題抽出，対処など）も実施することが一般的と考える。典型的な例が，「バグカーブ」とか「信頼度成長曲線」などと呼ばれるグラフを用いた，進捗や問題点収束の把握であろう。別の例は，発生した問題点の傾向を分析して，対策を検討し実施することである。

なお，問題点の書き方や，修正内容の書き方などについて，ルールを設けることを推奨する。これは，必要な情報が抜けていたり，内容が読み取れなかったりなどによる，作業フローの阻害（確認コストの増大やストレスの増大など）を防止することが主な目的である。

バグ管理**システム**は，いろいろなものがあり，それぞれ違いがあり，比較サイトもある。導入する場合は（または見直す場合は），**システム**導入による混乱も起こり得ることを念頭に，適切な作業フロー及び管理方法を事前によく考えてから導入することを推奨する。

5.3.6 システム開発側との調整事項

① ソフトウェア安全要求事項の作成

規格の箇条 5.2.1 において，**システム**レベルの要求事項から**ソフトウェアシステム**要求事項を定義して文書化することが要求されている。この要求事項は，この規格の要求事項であり，つまりソフトウェア開発側に対する要求事項の位置づけである。しかし，ソフトウェア開発側だけで実施せず，**システム**開発側（可能ならハードウェア開発側も含めて）と共に協力して実施し，及び作成したものについて合意することが望ましい。

ソフトウェアの欠陥の発生要因のひとつが，ソフトウェアに対する要求および要求仕様の曖昧さや不適切さであるといわれている。**システム**開発側の期待とソフトウェア開発側の理解との間に不整合があれば，それは欠陥の要因になり得る。また，ハードウェアとの適切な役割分担及び適切な連携を実現できなければ，適切な**システム**を作れず**安全**を達成できない可能性がある。また，**システム**要求事項とソフトウェア要求事項との相互の**トレーサビリティ**に欠落があれば，それも欠陥の要因になり得る。

ソフトウェアシステム要求事項の定義及び文書化は，協力して客観的明確なものを作成し，及び合意することが望ましい。

ソフトウェアシステム要求事項の定義については，要求（requirements：何を達成すべきか）の定義だけではなく，要求仕様（required specifications：実現すべき仕様）のレベルまで定義することが望ましい。**システム**及びハードウェアとの整合を要求仕様のレベルで確認しないと，仕様解釈の幅のぶんだけ不確定**要素**が存在し，それが**システム**全体の振る舞いを不明確にすると考えるためである。

なお，**ソフトウェアシステム**要求事項は，IEC 60601-1 の箇条 14.7 で要求されている PESS についての要求仕様と強い関連があり，同等の内容になる場合もある。少なくとも整合性が取れていなければならないと考える。

② ソフトウェアの妥当性確認

この規格には，ソフトウェア**妥当性確認**に関する要求事項が無い。**妥当性確認**は，**システム**に統合し全体として確認すべきものであるからである。その意味では，ソフトウェアを含めた**妥当性確認**は，**システム**設計側が担当する形とするのは適切と考える。（参考までに，IEC 60601-1 は，その箇条 14.11 において，**PEMS** の**妥当性確認**の要求事項を規定しているが，この要求事項は，ソフトウェアを除外せず，つまりソフトウェアを含めた要求事項になっていると読める。）

しかし，**妥当性確認**を**システム**設計側だけで実施するのは不適切と考える。

- **妥当性確認**試の網羅性について，ソフトウェアの振る舞いを考慮するべきである。そのためには，ソフトウェア開発担当が**妥当性確認**に参加することが重要である。
- **妥当性確認**の中で**異常**が見つかった時，その原因を探るためには，ハードウェアとソフトウェアの両方の詳細な知識が必要である。そのため，ソフトウェア開発担当が**妥当性確認**に参加することが重要である。

- **異常**の原因がソフトウェアの欠陥であった場合，あるいは**異常**の解決のためにはソフトウェアの変更が必要と判断された場合，ソフトウェア変更はソフトウェア開発担当が実施することになるであろうが，そのとき，ソフトウェア開発担当が**異常**に関する充分な情報を得ることが重要である。ソフトウェア開発担当が**妥当性確認**に参加していれば，情報共有に関してとても有利である。

ただし，**妥当性確認**に関わる関係者の役割分担や連携について，特に問題解決**プロセス**における判断（割り切りの判断など）及び責任（市場問題の可能性への責任など）について，事前に計画しておくことが望ましい。開発終盤の問題解決は，管理が疎かになると混乱に陥りやすいためである。

5.4 ソフトウェアに関する情報

書籍

次のような書籍が参考になるかもしれないので，紹介する。

- ソフトウェアエンジニアリング基礎知識体系（SWEBOK）
  この本は，ソフトウェアエンジニアリングに関する知識の案内図のようなものである。内容は，知識分野ごとに各知識の概要を説明し及び文献を紹介している。この本だけで深く理解することは難しいが，不足している知識を洗い出すのに役立つ。これは，規格としても出版されている。
  ISO/IEC TR 19759 “Software Engineering - Guide to the software engineering body of knowledge (SWEBOK)”
  ソフトウェアの設計／開発に関わる方は，お手に取ってみることをお勧めする。
- ソフトウェア品質知識体系ガイド（SQuBOK）この本は，ソフトウェアの品質保証に関連する知識の案内図のようなものである。
  ソフトウェアのテストやレビュー，及びソフトウェア品質保証に関わる方は，お手に取ってみることをお勧めする。
- IEC 62304 実践ガイドブック **医療機器ソフトウェア**に関する各国規制対応のための実例解説この本は，表題どおり IEC 62304 のガイドブックである。規格の各箇条の解説に加え，この規格が策定された背景や，各国の規制に関する情報なども掲載されている。
- 組込みソフトウェア開発向け コーディング作法ガイド［C 言語版］
- IPA から公開されており，コーディング規約の作成に役立つ。
  https://www.ipa.go.jp/sec/reports/20180215.html

6　開発の具体例：装着型歩行支援機器での開発事例

この章では，架空の**製造業者**“Ａヘルスケアロボティクス社”が，架空の装着型移動支援機器“B”を開発する想定で，**安全**制御回路が**リスクマネジメントプロセス**内でどのように位置づけられ，どのように開発されていくかの例を，開発の時系列にそって紹介する。

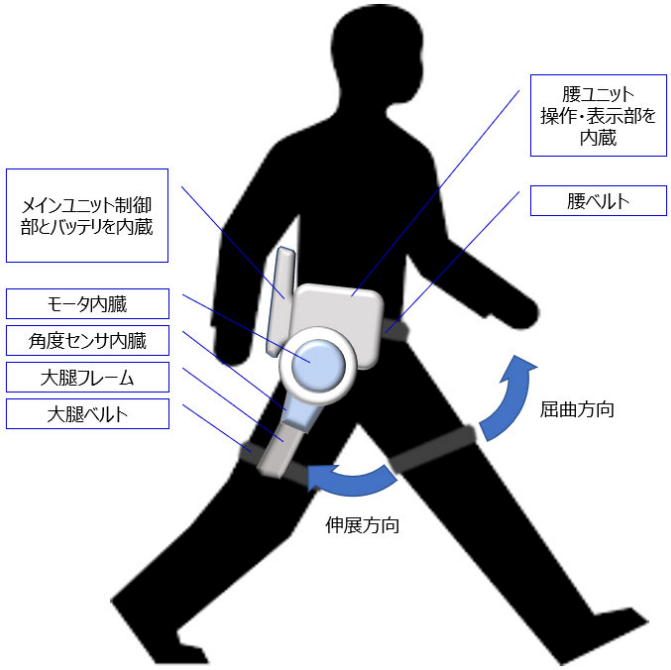
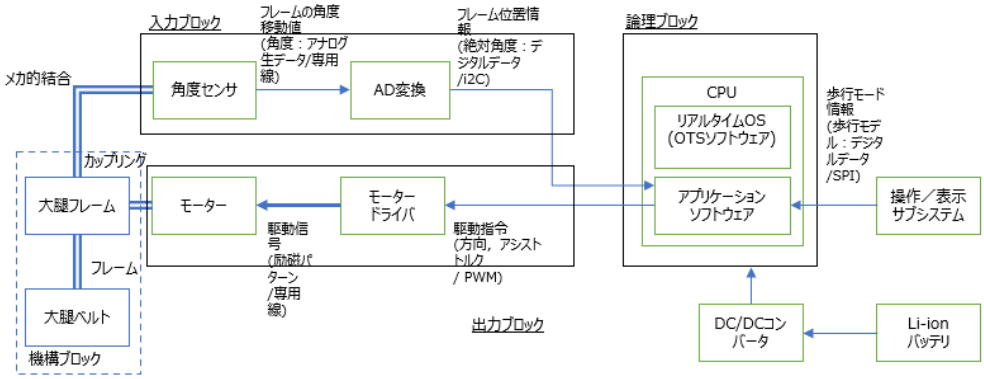
①　製品仕様

B の製品仕様は以下のように想定した。

表 6-1　架空の装着型移動支援機器 B の製品仕様表

項目	内容
使用者	筋力が低下気味のお年寄り 身長 140～180 cm 体重 40～80 kg
使用環境	屋外 気温：0～40 ℃
基本機能	使用者が一定リズムで歩行するとき，B は股関節の繰り返し運動の振幅と周期に合わせたモータートルクを，位相を 0.2 秒早めて出力する。
最大歩行速度	4 km/h @ 2 step/s
モーター	ブラシレス DC モーター x2 [pcs]
最大トルク	20 [Nm]
電源	Li-ion バッテリー（DC 24 V）
連続使用時間	1 時間
質量	3.0 [kg]
ユーザーインターフェース	• 電源 ON/OFF ボタン • ゲイン調整ボタン（弱，中，強の 3 段階） • バッテリ残量表示

表 6-2 （続き）架空の装着型移動支援機器 B の製品仕様表

項目	内容
構造	
制御系アーキテクチャ	
製品寿命	5 年

② リスクマネジメント計画

ISO 14971 の 3.4 に従って，**リスクマネジメント**計画を立案した。
V 字開発**プロセス**を意識し，以下の概念

- **意図する使用**を明確にして**リスクアセスメント**を実施し，
- **リスクコントロール**手段を設計し，
- **リスクコントロール**手段が適切に実装されたことを試験または検査で**検証**し，
- **意図する使用**をした場合に，受容できない**残留リスク**が無いこと（**安全**目標）を**妥当性確認**する。

をポイントとする活動を行うことを**リスクマネジメント**計画に加えた。（ISO 14971 の 3.5 に言及される通り，これらの各活動の**記録**は**リスクマネジメントファイル**に含まれることが意図されている。）
リスクアセスメントに必要な**リスク**マトリクスと受容性の基準は，ISO 14971 の附属書のものを使用した。装着型移動支援機器 B は A ヘルスケアロボティクス社で初めて開発するものであり，生産台数も当初は少ない予定なので，**危害**の発生確率を定量的に見積もれないことから，準定量的な基準で**リスクアセスメント**を行うとした。

表 D.4－準定量的な確率レベルの例

一般的な用語	確率の範囲の例
頻繁	10^{-3} 以上
可能性が高い	10^{-4} 以上 10^{-3} 未満
時々	10^{-5} 以上 10^{-4} 未満
僅かに	10^{-6} 以上 10^{-5} 未満
起こりそうにない	10^{-6} 未満

表 D.3－5 段階の定性的な重大さレベルの例

一般的な用語	想定する危害の程度
破局的	患者の死亡
重大な	永続的な障害又は生命を脅かす傷害
きわどい	専門家による医学的介入を必要とする傷害又は障害
軽微な	専門家による医学的介入を必要としない一時的な傷害又は障害
無視できる	不都合又は一時的な不快

半定量的な確率レベル	定性的な重大さレベル				
	無視できる	軽微な	きわどい	重大な	破局的
頻繁					
可能性が高い	R_1	R_2			
時々		R_4		R_5	R_6
僅かに					
起こりそうにない			R_3		
記号（網掛けの部分） ■受容できないリスク □受容できるリスク					

図 D.5－準定量的リスク評価マトリクスの例

③ 意図する使用の決定

試作品がまだ無いため，**リスクアセスメント**の出発点となる**意図する使用**には，①の製品仕様を用いるとした。路面条件や，使用者に関する禁忌などの条件が足りないように思われたが，**リスクアセスメント**活動によっていずれは特定されるだろうと期待し，更新・維持活動をすることにした。

④ リスクアセスメントの実施

複数人（4 人程度）のコアチームを結成して，**ハザード**の特定から活動を始めた。試作品がまだ無いため，B のユースケースを想像しながら列挙していった。

リスクアセスメントの途中で，［階段で］＋［**ハザード**：誤動作して］＋［**ハザード**：足を踏み外して］→［**ハザード**：転落］→［**危険状態**：頭部が路面に衝突］＝［**危害**：死亡］のように，悪い状況の組み合わせで死亡する**リスク** Ra があると特定されてしまい極端に厳しい初期**リスク**が多種多様に発散し，頭を悩ませた。しかし，この**リスク** Ra は組み合わせの問題であり，一つ一つの**ハザード**の独立性や因果関係を考慮しなければ適切な確率を見積もれないと分かったため，すべての**ハザード**について**リスク**レベルを割り当てることはせず，どのような**リスクコントロール**手段が採りえるのかを想像しながら**リスクアセスメント**していく方が結果的に**適切なリスク低減**，**リスク評価**が行えるよう考えた。この例であれば，［階段が無い場所で使用する］や，［階段前にフェンスを置く］という**リスクコントロール**手段や，［手すりを持ちながら使用する］使い方で制限をするのであれば，［**ハザード**：転落］の確率を「起こりそうにない」レベルまで落とすことができると考**えら**れた。つまり，［**ハザード**：誤動作して］の確率（＝制御部の**信頼性**）の多寡は，**リスク** Ra のレベルに影響が無いことになった。

リスクアセスメントを進めると，［平地で］＋［**ハザード**：誤動作して］＋［**ハザード**：つまずいて］→［**ハザード**：転倒］→［**危険状態**：頭部が路面に衝突］＝［**危害**：死亡］という**リスク** Rb もあると特定された。この**リスク**は，［つまずいても使用者がバランスを維持できる］のであれば，［**ハザード**：転倒］の確率を起こりそうにないレベルまで落とすことができると考**えら**れた。一方で，［つまずいても使用者がバランスを維持できる］ためには，B がどのようなモータートルクを出している場合でも，使用者が

抗ってバックドライブできる必要があった。文献（規格 JIS B 8446-2）によると，高齢女性が出せる股関節トルクはモーターの最大トルク 20 Nm よりも十分に大きいとあるため，バックドライブ可能であると結論づけた。

さらに**リスクアセスメント**を進めると，［**ハザード**：電源が喪失］または［**ハザード**：制御ソフトウェアがハングアップ］→［**ハザード**：関節がロック］→［**ハザード**：つまずいて］→［**ハザード**：転倒］→［**危険状態**：頭部が路面に衝突］＝［**危害**：死亡］という**リスク** Rc があると特定された。この**リスク**については，［**ハザード**：関節がロック］の確率を十分に減らさなければ受容可能なレベルにならないと考**えら**れたため，［**ハザード**：関節がロック］を頂点として FTA を実施したところ，下図となった。

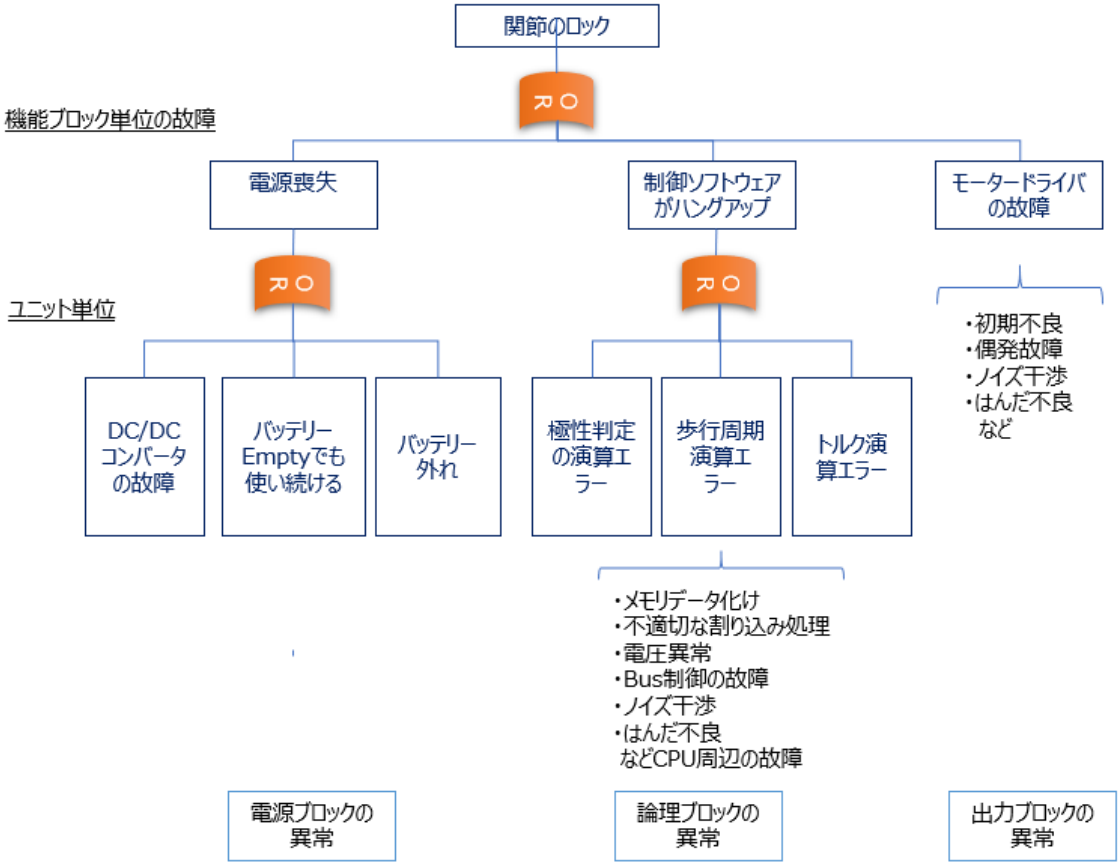


図 6-1 リスク分析：FTA［ハザード：関節がロック］

⑤ リスクコントロール手段の特定

リスク Rc を受容可能なレベルにするべく，**リスクコントロール**手段を検討した。FTA 図に基づき，［**ハザード**：電源が喪失］，［**ハザード**：制御ソフトウェアがハングアップ］，［モータードライバの**故障**］のそれぞれについて，以下の**リスクコントロール**手段を講じることで，**リスク** Rc を受容可能なレベルにできると考**えら**れた。

【 **リスク** Rc「［**ハザード**：電源が喪失］または［**ハザード**：制御ソフトウェアがハングアップ］→［**ハザード**：関節がロック］→［**ハザード**：つまずいて］→［**ハザード**：転倒］→［**危険状態**：頭部が路面に衝突］＝［**危害**：死亡］」の**リスクコントロール**手段 】

① ［DC/DC コンバータの**故障**］： 製品寿命に比して十分な寿命を持つ**高信頼性部品**を採用することとした。

② ［バッテリーEmpty でも使い続ける］： バッテリーが Empty に近づいた場合，モータードライバにフリー状態を命令することとした。

③ ［バッテリー外れ］： バッテリーと本体の間に機械的なロックを追加することにした。

④ ［制御ソフトウェアがハングアップ］： Watchdog タイマーがソフトウェアのハングアップを検知[7]したら，モータードライバにフリー状態を維持する信号を入力するハードウェア回路を追加することにした。

⑤ ［モータードライバの**故障**］： 製品寿命に比して十分な寿命を持つ**高信頼性部品**を採用することとした。

.

これらの**リスクコントロール**手段は②を除き，機械的，電気的（非電子的）な方法のみで実現可能であった。②についても電気的にしきい値を設ける方法でソフトウェアなしに実現できる可能性もあったが，製品の構成上異なる特性のバッテリーなど多様な条件に対応しなければならず，ソフトウェアで処理を行うこととなった。

⑥ リスクコントロール手段の実施と検証

リスクコントロール手段①から⑤について一つ一つ実施し，**検証**した。0 で特定した**リスクコントロール**手段についての**検証**は，

【 **リスク** Rc の **リスクコントロール**手段 の **検証**方法】

---

[7] Watchdog カウンタはクロック信号に合わせてデクリメントされていって、0 になったらリセットする機能。アプリケーションソフトウェアのメイン制御ループごとに、所定のレジスタに書き込んで Watchdog カウンタをリフレッシュする。

① [高信頼 DC/DC コンバータの採用]： DC/DC コンバータの製造元が提供したデータシートの以下の点を確認し，**検証**とした。
- B の電気的な仕様が，素子の定格内に収まっている。
- B の使用環境の範囲が，素子の使用環境と保管環境に収まっている。
- MTTF が，製品寿命に比して十分に大きい。

② [バッテリー残量低下時のモータードライバへの入力]： 関連する**システム**について，**PEMS 開発ライフサイクル**を適用することにした。

③ [バッテリー外れ防止ロック機構]： ロック機構を新たに設計し，部品変更を行った。バッテリーの引き抜き試験と振動試験を行うことで**検証**とした。

④ [ハングアップ時のモータードライバへの入力]： 必要なハードウェア回路を追加し，モータ駆動基板へ実装した。追加したハードウェア回路について機能確認と低温／高温環境などでの動作の**信頼性**試験を行い，かつ，**FMEA** や**故障**注入試験を実施してその**信頼性**が製品寿命に比して十分にあることを確認して**検証**とした。

⑤ [高信頼モータードライバの採用]： モータードライバの製造元が提供したデータシートの以下の点を確認して，**検証**とした。
- モーターをロックする**故障**モードの有無
- B の電気的な仕様が，素子の定格内に収まっている。
- B の使用環境の範囲が，素子の使用環境と保管環境に収まっている。
- MTTF が，製品寿命に比して十分に大きい。

注）IEC 60601-1 への適合では，**単一故障安全**を確保することが重要な要求となっている。IEC 60601-1 の箇条 4.7 には，

> （参考和訳）
> **ME 機器**は，次のいずれかの場合，**単一故障安全**とみなす。
> a） **故障**する確率を無視できるレベルに減らして**リスク**を低減させる単一の手段を用いる場合（例えば，強化絶縁，機械的保護装置のない懸垂質量には 8 倍の**安全**率，**高信頼性部品**などの採用）。
> b） **単一故障状態**は起きても，次のいずれかの場合，
> - 最初の**故障**が **ME 機器**の**予測耐用期間**中に検知でき，かつ，**リスク**を低減させる第二の手段も**故障**する前に検知できる（例えば，懸垂質量に機械的保護装置を備える）。
> - **リスク**を低減させる第二の手段が，**ME 機器**の**予測耐用期間**中に**故障**する確率を無視できるほど低くする。

と明記されており，**高信頼性部品**は，3.17 に，

（参考和訳）
予測耐用期間の間に **ME 機器**が**正常な使用**又は**合理的に予見可能な誤使用**において，この規格の**安全**要求事項について機能を失わないことを確実にする特性をもった部品。

と定義されている。これらの考え方は，IEC 61508-1 や ISO 13849-1 などの機械製品の**機能安全**規格の考え方（構造）と一致している。つまり，**リスクマネジメントプロセス**において適切と判断できるならば，例えば **SIL**2 や **PL**b のコンポーネントを**高信頼性部品**として採用することで，その部分は製品寿命中に**故障**しないと判断して良いことになる。

4.6 項で例示した**リスクコントロール**手段のうち，**リスクコントロール**手段①は上記 a)の方法（**高信頼性部品**であることを確認），④は上記 b)の 2 項目の方法（**故障**＝ハングアップを検出して**安全**化する回路の**信頼性**が高いことを確認）を採用している。

また本章では，簡単のため**故障率**だけで判断する例とした。単純な**故障率**の積算だけでは必要な**信頼性**の基準に満たないようであれば，**機能安全**規格が規定するように，危険側**故障率**を基準とし，**FMEDA** を利用してもよい。本ガイダンス 第 4 章 **PEMS** のための**システム**開発ガイド にも方法が記載されており，参考になる。

⑦ PEMS 開発ライフサイクルの適用

B はソフトウェアによるアクチュエータ制御を行うため，IEC 60601-1 の **PEMS**（**プログラマブル電気**

（参考和訳）
14.2~14.12 の要求事項は，次のいずれかに該当する場合は，**PEMS** に適用する。
- **プログラマブル電子サブシステム**(PESS)が，**基礎安全**又は**基本性能**に必要な機能を提供する場合。
- 4.2 に従った**リスクマネジメント**の適用によって，PESS の**故障**が受容できない**リスク**を生じないこと

を立証できない場合。

（中略）

（試験）
適合性は，必要な全ての文書の調査によって決定され，必要な場合は，14.2～14.13 の要求事項の**評価**によって決定する。

14.2～14.13 の要求事項を適用する場合は，各 PESS のソフトウェアの開発又は変更管理に対して，IEC 62304 の 4.3，箇条 5 及び箇条 7～箇条 9 の要求事項も適用する。
（試験）
適合性は，IEC 62304 の 1.4 に従って，必要な検査及び**評価**によって確認する。

医用システム）に該当する。IEC 60601-1 の 14.1 には，以下のように言及している。

[バッテリー残量低下時のモータードライバへの入力] を担当するソフトウェアを含む**サブシステム**（PESS）は，**故障**が即座に受容できない**リスク**となるわけではないが，**リスク** Rc に基づく **基礎安全** に必要な機能を提供するソフトウェアと言えるため，14.2～14.12 の要求事項を適用すべきと判断した。ただし，適合性**評価**は IEC 62304 に従って行われるため，IEC 60601-1 の 14.2～14.12 を直接利用せず，より具体的な要求事項が規定されている IEC 62304 を主として参照することにした。なお，ハードウェアはコンデンサでノイズを除去した分圧 MOSFET を介して CPU の ADC で測定するだけものであったので，14.11 の**妥当性確認**でカバーすることにした。
念のため，IEC 62304 の表 C.3 にある，IEC 60601-1 の 14 の要求事項との対応表を確認した。IEC 62304 では，

- **IT ネットワーク**については触れられていない
- **PEMS 妥当性確認**を含まない

とあった。B は **IT ネットワーク**への接続を意図しないため，**PEMS 妥当性確認**への要求事項のみ，IEC 60601-1 を参照することにした。

⑧ ソフトウェア開発計画

B の製品開発計画書とは別に，IEC 62304 の 5.1 に従ってソフトウェア開発計画書を作成することにした。 [バッテリー残量低下時のモータードライバへの入力] を行う機能は，B の**ソフトウェアシステム**の一部であるため，全体のソフトウェア開発計画書に記載することにした。

B のソフトウェア開発計画書では，以下のようにした

表 6-3 架空の装着型移動支援機器 B の開発計画書

項目	内容
開発モデル	チケット駆動 [1] アジャイル型
開発プラットホーム	GitHub Enterprise (GHE) [2]
ソフトウェア**構成管理**	GHE
トレーサビリティ	GHE の Issue（チケット）と Pull Request を紐付け [3]
ソフトウェア結合	常時（CI[4]を利用し，Pull Request ごとに結合） （IEC 62304， 5.6.2）
ソフトウェア結合試験	Pull Request 時に CI を実施。フォーマッター， 静的解析ツールを通った場合に，その時点での全テストケースを実施。 （IEC 62304， 5.6）
ソフトウェア問題解決	GHE の Issue（bug）として追加。**安全**上の重要度に基づいて優先度を上げる。 （IEC 62304， 5.6.8， 5.7.2， 6， 9）
SOUP の**構成管理**	SOUP の**バージョン**を固定（IEC 62304， 8.1.2）。変更時は結合試験を実施。**セキュリティ**情報，バグ情報を収集するために関連するサイトを定期巡回。 （IEC 62304， 6.1， 7.1.3）
リリース基準	必須の機能実装 Issue と，**安全**上重大な Bug が無い場合，ソースコードにタグを付け，**リリース**とする。 （IEC 62304， 5.8）
PEMS 妥当性確認	**リリース**されたソフトウェアをインストールした B を用いて，**ソフトウェアシステム**試験を実施する（IEC 62304， 5.7）。試験は機能毎の動作試験と，ユースケースに従ったシナリオベースの動作試験を含み，B の**システム**全体としての**妥当性確認**（**PEMS 妥当性確認**）を兼ねるとした（IEC 60601-1， 14.11）。

[1] チケット駆動開発：開発**タスク**（機能開発やバグ修正）をチケットとし，チケットに対して，議論，進捗管理，テストケース，ソースコードを紐付ける開発手法

[2] GitHub Enterprise：**バージョン**管理**システム** Git をベースにした GitHub 社が提供するプラットフォームサービス。コードレビューや Issue（チケット）管理，ワークフローの適用をしやすくする。類似サービス

に GitLab などがある。

[3] Issue（チケット）と Pull Request を紐付け：Issue に対して開発するワークフローを採用している場合，ソースコードへの変更はその Issue に紐付けられる。Pull Request は Git における，ソースコード変更を他の開発者（レビュワー）に通知し，メインのソースコードにマージしてもらう操作のこと。

[4] CI（Continuous Integration）：ソースコードの変更ごとに，ビルドとテストを行うこと。Jenkins や Circle CI などのツールを使うことで自動化でき，早期の問題発見を実現できる。

⑨ ソフトウェアアーキテクチャ

ソフトウェアシステムの**アーキテクチャ**は下表とした。（IEC 62304， 5.3.1）

ソフトウェアアイテム間のインターフェースは，リアルタイム OS 提供の API を利用した。（IEC 62304，5.3.2）

リアルタイム OS には，利用している CPU ボードをサポートしているものを採用した（IEC 62304，5.3.4）

ソフトウェア**アーキテクチャ**については，IEC 62304， 5.3.5 及び 5.3.6 の視点でレビューによる**検証**を行った。

表 6-4 ソフトウェアシステムのアーキテクチャ

ソフトウェアアイテム	機能	SOUP
リアルタイム OS	- **タスク**スイッチ - 割り込み管理 （IEC 62304， 5.3.3）	○
アプリケーションソフトウェア	- 以下の受信・格納 ➢ 操作**サブシステム**からの入力情報 ➢ 角度センサー情報 - 電源電圧（バッテリー残量）の測定 - 歩行パターン（振幅，周期）の推定 - モータートルクの計算 - モータードライバへの命令送信 - 表示**サブシステム**への描画命令送信 - Watchdog タイマーのリセット	-

⑩ ソフトウェア安全クラス

関節がロックした場合に，つまずくかどうか，転倒するかどうか，頭部を路面にぶつけるかどうかはユーザーによって確率が異なるが，IEC 62304 の 4.3 と図 3 に従って検討したところ，**ソフトウェアシステム**としてはクラス C となった。

上表の**ソフトウェアアイテム**を機能ごとに**ソフトウェアユニット**に分割（IEC 62304， 5.4.1）し，それ

ぞれのソフトウェア**安全**クラスを以下のように割り当てた（IEC 62304， 7）

表 6-5 ソフトウェアユニットと安全クラスの割り当て

ソフトウェアアイテム	**ソフトウェアユニット**	SOUP	ソフトウェア**安全**クラス	根拠
リアルタイム OS	-	○	A	⑥の④ [ハングアップ時のモータードライバへの入力] があるため，ソフトウェアによって受容できない**リスク**はない
アプリケーションソフトウェア	操作**サブシステム**からの入力情報の受信・格納	-	A	設定操作を受け付けなくなるが，④の**リスク** Rb 検討した通り，B のモータートルクはユーザーが抗えるレベルであるため，受容できない**リスク**はない。
	角度センサー情報の受信・格納	-	A	モーターの誤動作の原因となりえるが，④の**リスク** Rb 検討した通り，B のモータートルクはユーザーが抗えるレベルであるため，受容できない**リスク**はない。
	DC/DC コンバータからの電源情報の受信・格納	-	C	[バッテリー残量低下時のモータードライバへの入力]を行う機能に必須のため。
	歩行パターン（振幅，周期）の推定	-	A	モーターの誤動作の原因となりえるが，④の**リスク** Rb 検討した通り，B のモータートルクはユーザーが抗えるレベルであるため，受容できない**リスク**はない。
	モータートルクの計算	-	A	モーターの誤動作の原因となりえるが，④の**リスク** Rb 検討した通り，B のモータートルクはユーザーが抗えるレベルであるため，受容できない**リスク**はない。
	モータードライバへの命令送信	-	C	[バッテリー残量低下時のモータードライバへの入力]を行う機能に必須のため。
	表示**サブシステム**への描画命令送信	-	A	表示を更新できなくなるが，受容できない**リスク**ではない。
	Watchdog タイマーのリセット	-	A	⑥の④ [ハングアップ時のモータードライバへの入力] があるため，ソフトウェアによって受容できない**リスク**はない

⑪ ソフトウェア安全クラス C への対応

ソフトウェア**安全**クラスがクラス C の**ソフトウェアユニット**については，その仕様及び API を予め設計し，文書化した（IEC 62304， 5.4.2， 5.4.3， 5.5.3）。また，ユニットテストのテストケースと，結合時の［バッテリー残量低下時のモータードライバへの入力］機能のテストケースを先に作った（IEC 62304， 5.4.4， 5.5.2， 5.5.3， 5.5.4， 5.6）。これらのテストケースは，CI 時にかならず合格するかがチェックされ，**記録**されるようにした（IEC 62304， 5.5.5）。
開発プラットフォーム，ビルドに用いるツールチェーン，CI ツールについても，⑨の表に追記する形で SOUP の**ソフトウェアアイテム**として**構成管理**を行うこととした（IEC 62304， 5.1.4， 5.1.10）。

表 6-6 SOUP として扱うソフトウェアアイテム

ソフトウェアアイテム	機能	SOUP
開発プラットフォーム GHE	- ソフトウェア**構成管理** - Issue トラッカー（**トレーサビリティ**） （IEC 62304， 5.3.3）	○
ツールチェーン	ソースコードをリアルタイム OS が実行可能な形式に変換	○
CI ツール	自動的にソフトウェア結合し，結合テストを実施	○

⑫ PEMS 妥当性確認

0 で計画した通り，必須機能の実装 Issue と，**安全**上重大な Bug が無い状態となったため，ソースコードに**リリース**番号のタグを付け**リリース**した。
リリースしたソフトウェアをインストールした B を用いて，**PEMS 妥当性確認**試験として以下を実施した。

- 実際にバッテリー残量低下状態を起こし，適切にモーターがフリーになる機能を確認した。
- 歩行時の股関節運動を模擬するダミーに取り付け動作させた。想定するユースケースに従ったシナリオすべてにおいて，不具合なく意図したとおりにモータートルクが出力されることを確認した。

以下のものをまとめ，**PEMS 妥当性確認記録**とした。

- **PEMS 妥当性確認**試験と結果の概要
- IEC 62304 への適合性**評価**結果のまとめ
- ソフトウェア開発計画が計画通り実施されたこと

⑬ リスクコントロール手段実施後のリスク評価

リスク管理表（末尾の表）を walk through で点検し，

- 受容できない**残留リスク**がないこと
- **リスクコントロール**手段の**検証**が網羅的にされていること
- 思わぬ副作用がないこと

を確認した。

⑭ リスクマネジメント報告書の作成

全ての**記録**をファイルし，まとめとして**リスクマネジメント**報告書を作成した。
規制当局や認証機関とのコミュニケーションを円滑にすすめるために，以下の内容を数ページにまとめた。

- **リスクマネジメント**計画書，**リスク**管理表への参照
- **リスクアセスメント**時に受容できないと特定された**リスク**のリスト
  - その**リスク**を受容できるレベルまで低減する**リスクコントロール**手段
  - その**リスクコントロール**手段の**検証**方法と結果の概要
- ISO 14971 の 8 の各項目への適合性**評価**結果
  - **リスクマネジメント**計画書の各項目の実施状況（**記録**への参照）
  - 全体的な**残留リスク**が受容可能であること
  - 品質マネジメント**システム**の適用計画

規制当局や認証機関は，この**リスクマネジメント**報告書を見て，
リスク管理上重要な**リスク**と**リスクコントロール**手段を素早く把握し，また，**プロセス**が適切に実施されていることを把握できたようだった。この**リスクマネジメント**報告書を出発点に，彼らが気になる仕様書や**検証記録**を芋づる式に開陳し，都度説明や議論を行うことで審査はスムーズに行われた。特に重要だったのは，**リスク** ID や文書番号を利用した，関連する情報への確実な参照であった。

表 6-7 架空の装着型移動支援機器 B のリスク管理表

ID	**ハザード/危険状態**	原因**ハザード** ID	次**ハザード/危険状態/危害** ID	**リスクコントロール**手段	**リスクコントロール**手段実施の**検証**	次**ハザード/危険状態/危害**の発生確率	**危害の重大さ**	受容
1	頭部が路面に衝突	2	死亡			可能性が高い	破局的	否
1-1				原因**ハザード**の発生確率を下げる	**リスク**管理表の点検	起こりそうにない	破局的	可
2	転倒	3， 4， 5	1			時々		
2-1				原因**ハザード**の発生確率を下げる	**リスク**管理表の点検	起こりそうにない		
3	階段でつまずく	-	2			時々		
3-1				使用場所を階段が無い場所に制限する。 階段前にフェンスを置く。	取扱説明書の警告文の点検	起こりそうにない		
4	誤動作してつまずく	-	2			時々		
4-1				使用者のバランス維持を邪魔しないできるモータートルク	製品仕様と文献の点検	起こりそうにない		
5	関節がロックしてつまずく	6， 7， 8	2			時々		
5-1				原因**ハザード**の発生確率を下げる	**リスク**管理表の点検	起こりそうにない		
6	電源喪失	9， 10， 11	5			時々		
6-1				原因**ハザード**の発生確率を下げる	**リスク**管理表の点検	起こりそうにない		

表 6-8 （続き）架空の装着型移動支援機器 B のリスク管理表

ID	**ハザード/危険状態**	原因**ハザード** ID	次**ハザード/危険状態/危害** ID	**リスクコントロール**手段	**リスクコントロール**手段実施の**検証**	次**ハザード/危険状態/危害**の発生確率	**危害の重大さ**	受容
7	制御ソフトウェアがハングアップ	-	5			時々		
7-1				Watchdog タイマーでハングアップを検出してモーターをフリーにする追加回路	追加回路の動作試験，**信頼性評価**	起こりそうにない		
8	モータードライバの**故障**	-	5			時々		
8-1				製品寿命に比して十分な寿命を持つ**高信頼性部品**を採用	製造元が提供したデータシートの点検	起こりそうにない		
9	DC/DC コンバータの**故障**	-	6			時々		
9-1				製品寿命に比して十分な寿命を持つ**高信頼性部品**を採用	製造元が提供したデータシートの点検	起こりそうにない		
10	バッテリーEmpty でも使い続ける	-	6			時々		
10-1				バッテリー低下時に，モータードライバにフリー命令	バッテリー低下時の動作試験，**PEMS 妥当性確認記録**の点検	起こりそうにない		

表 6-9 （続き）架空の装着型移動支援機器 B のリスク管理表

11	バッテリー外れ	-	6			時々		
11-1				バッテリーロック機構の追加	引き抜き試験，振動試験	起こりそうにない		

AMED ロボット介護機器開発・標準化事業　安全化設計手法の開発
研究成果報告

これから機能安全に取り組む開発者のための

ロボット介護機器の安全制御回路
開発ガイダンス

【付録】

初版

付録A 主要国における医療機器への該当を調査する方法

医療機器と一般機械製品のボーダーに位置づく介護機器

ロボット介護機器開発・標準化事業において対象とするロボット介護機器は以下のタイプである。

図 6-1 AMED プロジェクト：ロボット介護機器開発・標準化事業の対象ロボット

これらの製品は高齢者や障害者に直接作用し，心身のハンディキャップを軽減・補完する医療機器的な使われ方が想定される製品や，障害を治療・回復するリハビリに用いられる医療機器的な側面を持つ製品がある一方，健常者の日常生活をより活発にするようアシストする製品や，介護士の肉体労働の負荷軽減のための一般製品が含まれる。つまりこれらの製品は，想定される環境や使用者や意図する機能が作用する対象者，医学的な効果・効能の有無などにより，一般的な機械(非医療機器)にも医療機器どちらにも当てはまり得る機器であり。双方の境界線付近に位置づけられる装置も多くみられる。
本ガイダンス文書で前述した通り，**制御システム**を用いた安全への要求については，医療機器への該非によって進むべき要求規格体系が大きく異なり，開発者に対してインパクトがあるため注意したい。
医療機器では無い一般的なロボットを医療機器関連の**制御システム**への安全要求関連規格を当てはめようとすると，医療機器特有の用語やプロセス要求など理解しにくい要素も多く，適合させることに苦労する恐れがある。
従って，初期段階で明確に該当／非該当を明らかにしておくことを推奨する。
医療機器への該非判定は仕向け国による規制により異なる場合があり，その概要を次ページより記す。

(ア)　日本での扱われ方

日本国内の場合，一般的には介護機器は医療機器とは見なされないことが多いが，規制は以下のとおり，当然確認は必要となる。
国内では医療機器は"医薬品医療機器等法"（医薬品，医療機器等の品質，有効性及び安全性の確保等に関する法律）にて，規制される。この中で，『医療機器とは，人若しくは動物の疾病の診断，治療若しくは予防に使用されること，又は人若しくは動物の身体の構造若しくは機能に影響を及ぼすことが目的とされている機械器具等であって，政令で定めるもの』と定義されている。つまりロボット介護機器が上記の目的に合っていたとしても，政令で定めるものでなければ，医療機器には該当しない場合がある。

この政令とは医薬品医療機器等法施行令を指しており，医薬品医療機器等法施行令 別表第一で医療機器の一般的名称が定義されている。医療機器は医療機器”一般的名称”およびその”定義”から該当性を評価でき，PMDA の Web サイトなどで医療機器一般名称を検索できるので大よそ推測ができる。このリストには，ロボット介護機器のような新規性の高いものは含まれておらず，一般的には医療機器として扱われていない実情と考えられる。しかし，疑義や不安がある場合については PMDA もしくは認証機関に問い合わせるのが正しい方法である。

(独立行政法人 医薬品医療機器総合機構の Web サイトより)

図 1-2　PMDA の医療機器一般名称検索の URL と Web サイト

https://www.std.pmda.go.jp/stdDB/index_jmdn.html

付録 A　　主要国における医療機器への該当を調査する方法

医療機器開発に関する相談窓口

- 独立行政法人 医薬品医療機器総合機構（PMDA）
  http://www.pmda.go.jp/
- 各都道府県薬務担当部署
- 医薬品医療機器法における厚生労働大臣の登録を受けた「登録認証機関」
  厚生労働省ホームページ「登録認証機関制度について」
  https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryou/iyakuhin/touroku/index.html

(イ)　欧州での扱われ方

欧州の場合，日本とは異なり，医療機器指令 93/42/EEC（規則）の医療機器の定義に該当するかどうかで該非を確認する。

✧ 医療機器指令 93/42/EEC の医療機器の定義

第 2 条　定義 本規則のために，以下の定義を適用する。 (1)「医療機器」とは，あらゆる計器，器械，用具，ソフトウェア，インプラント，試薬，材料又はその他の品目であり，製造業者が次の一つ以上の医療目的のために，単独又は併用で，ヒトへの使用を意図するものを意味する。 - 疾患の診断，予防，監視，予測，予知，治療又は緩和 - 負傷又は身体障害の診断，監視，治療，緩和又は補償 - 解剖学的又は生理学的又は病理学的プロセス又は状態の検査，代替又は修復 - 提供された臓器，血液及び組織を含む，人体由来の検体の invitro 検査による情報提供 （以降省略） 出展：European Medical Device Regulation より

図 1-3 医療機器指令 Article 1.2.a 医療機器の定義（参考和訳）

ここでは定義の 1 番目と 2 番目の条項が関わってくる可能性がある。
対象の機器がこの定義の 1 番目と 2 番目に関わってくるかを，使用者・対象者および医学的な効果効能の有無などから判断する。例えば使用者や装置が直接作用する対象者は自力で生活が不可能なハンディキャップを持っているかどうか，目的をする機能はそのハンディキャップを補ったりするのが目的か，確認する必要がある。

✧ 欧州委員会発行のガイダンス文書

欧州委員会より，医療機器の判定区分をするための具体的な事例や指針が示されたガイド文書が発行されているので参考にしたい。

a) MEDICAL DEVICES: Guidance document (MEDDEV 2.4/1 Rev.9)- Classification of medical devices

医療機器に関する理事会指令 93/42/EEC の適用に関連する指針『医療機器クラス分類』クラス分類規則の詳細説明やクラス分類の実施ガイドが示される。MDD を補足するガイダンス。

Index
1. PURPOSE AND PHILOSOPHY OF MEDICAL DEVICE CLASSIFICATION
2. PRACTICAL RELEVANCE OF CLASSIFICATION
2.1. General requirements
2.2. Conformity assessment
2.3. Clinical evaluation and investigation
2.4. Instructions for use
2.5. Miscellaneous
3. HOW TO CARRY OUT CLASSIFICATION
3.1. Basic definitions
3.2. Application of the classification rules
3.3. How to use the rules
3.4. Practical example
3.5. Handling of interpretational problems
4. EXPLANATIONS OF INDIVIDUAL RULES
4.1. Graphical summary - Guidance chart
4.2 General explanation of rules/practical issues/examples

b) MANUAL ON BORDERLINE AND CLASSIFICATION IN THE COMMUNITY REGULATORY FRAMEWORK FOR MEDICAL DEVICES (Version 1.18 (12-2017))

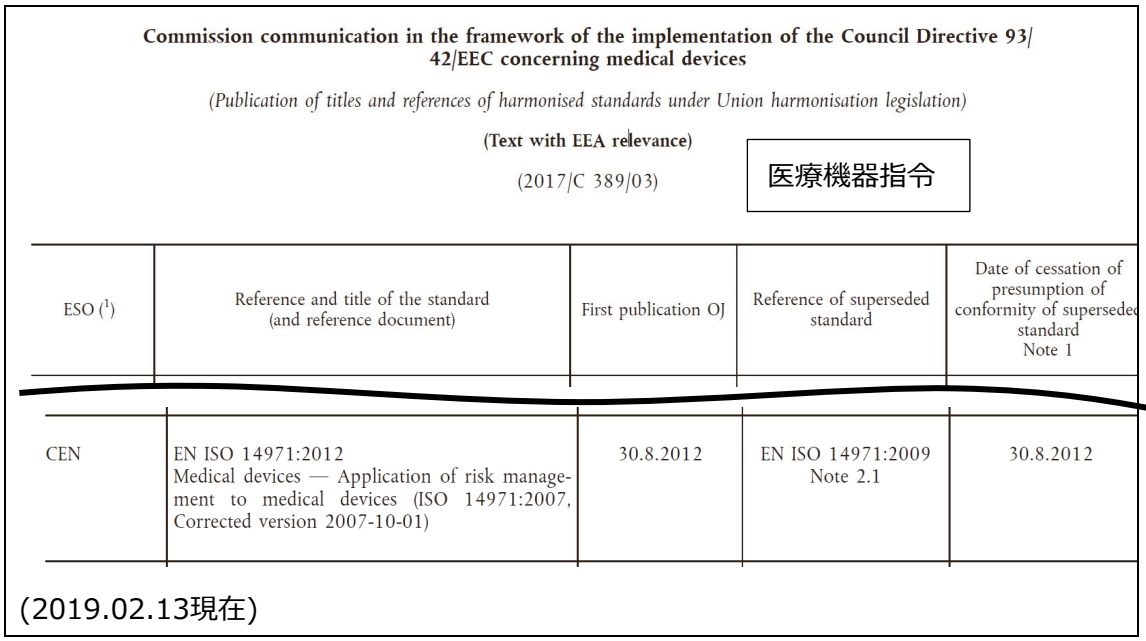
付録 A　　主要国における医療機器への該当を調査する方法

医療機器の共同体規制フレームワークにおける医療機器の境界と分類に関するマニュアル
・・・MDD では，医療機器と見なされるのは，特定の製品に対して，医療的性質の「主張」がなされる場合であり，その主張の科学的証拠が，不十分な場合は，MDD の要件を満たさず、医療機器としての CE マークが付けることが出来ない可能性がある。
医療機器／非医療機器およびクラスの分類は、まず MDD の分類規則を適用するが，要件の判断が難しいケースがある。そこで，欧州委員会の専門家グループが，利害関係者との協議，規制当局の合意をはかり，代表的な製品毎に，分類の考え方を具体的に示したマニュアルを発行した。
但し，このマニュアルは単なるツールであり，法的拘束力を持たないことを理解するよう注記がある。
MANUAL ON BORDERLINE AND CLASSIFICATION IN THE COMMUNITY REGULATORY FRAMEWORK FOR MEDICAL DEVICES (europa.eu)

✧ 欧州 医療機器指令整合規格リスト

欧州官報により医療機器指令（規則）に適合するために整合規格リストが提供される。
一般的な介護機器として，車椅子や介護用リフトの EN 規格がリストアップされている。これらの製品は Notified body により実際に製品認証も行われている。

◇ Harmonized standards for medical devices



Commission communication in the framework of the implementation of the Council Directive 93/42/EEC concerning medical devices

(Publication of titles and references of harmonised standards under Union harmonisation legislation)

(Text with EEA relevance)

(2017/C 389/03)

医療機器指令

ESO (1)	Reference and title of the standard (and reference document)	First publication OJ	Reference of superseded standard	Date of cessation of presumption of conformity of superseded standard Note 1
CEN	EN ISO 14971:2012 Medical devices — Application of risk management to medical devices (ISO 14971:2007, Corrected version 2007-10-01)	30.8.2012	EN ISO 14971:2009 Note 2.1	30.8.2012

(2019.02.13現在)

(欧州委員会の Web サイトより)

図 1-4 Official Journal of the European Union (2017/C 389/03)

必要があれば欧州医療機器指令のノーティファイドボディである認証機関に確認する事をお勧めする。

◇ Nando (New Approach Notified and Designated Organizations) Information System
Nando(ニューアプローチにおける通知および指定機関)情報システム
加盟国が，欧州委員会および他の加盟国に対し通知した。規制に関連する要件を満たす機関を検索できます。
https://ec.europa.eu/growth/tools-databases/nando/index.cfm

注記：尚，製品個別規格は ISO 21856 草案は将来に医療機器規則の整合規格リストに載ることも考慮に入れて開発されており，そのような背景より，電子**制御システム**の安全要求に医療機器系の規格が採用されている。

付録 A　　主要国における医療機器への該当を調査する方法

【 医療機器指令に該当するロボット介護機器の場合 】

欧州でロボット介護機器を医療機器指令に適合させる場合，介護機器である前に医療機器であるこの場合は EN 整合規格リストに従って，製品安全規格のみではなく，次のような医療系規格へのすべての要求事項への適用が規制として（強制で）要求されるだろう。（厳密には EN 整合規格を用いない方法もレアケースとしては認められる。）

ISO 14971(リスクマネジメント)， ISO 13485(品質マネジメントシステム)， IEC 60601-1(電気医用機器の製品安全)， IEC 60601-1-2(電気医用機器の電磁両立性)， IEC 62304(ソフトウェアライフサイクル)， IEC 62366（ユーザビリティ）などが，電子**制御システム**に関わらず機器のすべてに関わるので注意が必要である。

【 医療機器指令に該当しない介護機器の場合 】

一方，医療機器指令には適用しない介護機器も存在する。これらの非医療機器扱いの介護機器は機械指令などへの適用となるため，医療系規格に適用することを直接要求されることはない。

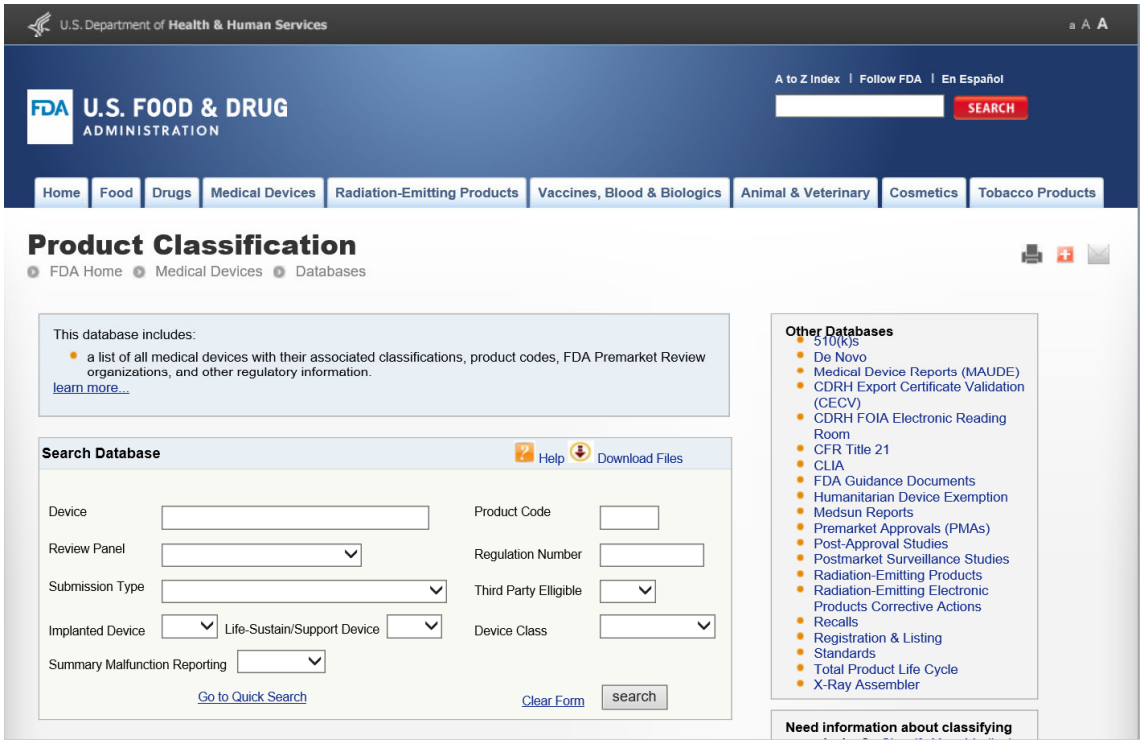
機械指令の整合規格群から引用すると，ISO 13482， ISO 12100， ISO 13849， IEC 62061 などの規格が採用され，適切な QMS のベースの上に成り立つ，機能安全管理がなされる。一般のロボットであればこれら機械指令の整合規格がマッチングしやすい。

(ウ)　米国の場合

米国では一般的に，介護機器は医療機器として見做される。FDA（U.S. Food and Drug Administration)の WEB サイトで Medical device name と Associated product codes.から FDA として一般的な医療機器の製品カテゴリが検索できる。

◇　FDA, Product Classification

https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfPCD/classification.cfm



(FDA の Web サイトより)

図 1-5 FDA の Product classification 検索ページ

(エ)　開発する医療機器を海外で販売したい時の相談窓口

- NPO 法人　海外医療機器技術協力会（OMETA）
  http://www.ometa.or.jp/
- 独立行政法人　日本貿易復興機構（JETRO）
  http://www.jetro.go.jp/indexj.html

付録B 機能安全で用いられる技法

本章では，機械安全で良く用いられる方法を中心に，機能安全開発で参考になる手法及び技法を紹介する。
機能安全では，まず機器のリスクアセスメントを行い，リスク低減策を導出する。リスク低減策に制御を用いる場合，要求される安全度に応じた開発エンジニアリングが行われる。というのが大きな流れとなる。

(ア)　ハザードの特定で用いる技法

(1) チェックリスト

チェックリストは，前回のリスクアセスメントの結果，過去の失敗の結果，または専門家による知見・経験によって作成した，ハザード，リスクのリストである。通常，ハザードの特定にて使いやすいが、製品やシステムのライフサイクルのどのステップでも使用可能な技法である。他のリスクアセスメント技法の一環として使用してもよいが，新たな問題を特定する更に想像力を必要とする技法を適用した後に，全てが万全であるかを検査するために適用する場合にも有用である。
[利用手順]
手順は，次のとおりである。
① 作業の適用範囲を定義する。
② 十分に適用範囲をカバーするチェックリストを選択する。
③ チェックリストを使用する人又はチームは，製品又はシステムの各要素にわたり，チェックリストにあるアイテムの有無についてレビューを行う。
[長所及び短所]
長所の例を，次に示す。
・ 専門家でない人が用いてもよい。
・ うまく作成されているときは，多様な専門知識を組み込んで使いやすいシステムになる。
・ 共通の問題を見逃さないことを確実にする手助けになる。
短所の例を，次に示す。
・ リスクの特定において，想像力を妨げる傾向がある。
・ “知っていると分かっていること”は取り上げるが，“知らないと分かっていること”又は“知らないということが分かっていないこと”は取り上げない。
・ “チェックマークを入れる”行動を勧めてしまう。
・ 観察中心になる傾向があるので，簡単には見えてこない問題を見逃す。
ロボット介護機器の特質を考慮し，次の項目のチェックリストが活用できるかもしれない。

(2) 医療機器の重要ハザードのリスト（チェックリスト）

以下のハザードリストは，ISO 14971 表 E.1 で提供される医療機器に関連した，患者又はその他に最終的に危害を生じさせるハザードを特定する手助けとして使用できるチェックリストである。

表 1-1 医療機器の重要ハザードのリスト表（ISO 14971 表 E.1 より）

エネルギーに関連するハザードの例
電磁エネルギー
商用電圧
漏れ電流
- 外装漏れ電流
- 接地漏れ電流
- 患者漏れ電流
電界
磁界
放射線エネルギー
電離放射線
非電離放射線
熱エネルギー
高温
低温
機械的エネルギー
重力
- 落下
- 懸垂物体
振動
蓄積エネルギー
可動部分
ねじれ，ずれ，及び張力
患者の移動及び位置決め
音響エネルギー
- 超音波エネルギー
- 不可聴音響エネルギー
- 音
高圧液体流入

表 1-2 （続き）医療機器の重要ハザードのリスト（ISO 14971 表 E.1 より）

操作に関連するハザードの例
機能的なハザード
不正確又は不適切な出力
若しくは機能性
不正確な測定
間違ったデータ転送
機能の喪失又は劣化
誤使用に関連するハザード
不注意
物忘れ
規則に基づく失敗
知識に基づく失敗
日常的な違反
エネルギーに関連するハザードの例
電磁エネルギー
商用電圧
漏れ電流
- 外装漏れ電流
- 接地漏れ電流
- 患者漏れ電流
電界
磁界
放射線エネルギー
電離放射線
非電離放射線
熱エネルギー
高温
低温
機械的エネルギー
重力
- 落下
- 懸垂物体
振動

表 1-3 （続き）医療機器の重要ハザードのリスト（ISO 14971 表 E.1 より）

蓄積エネルギー
可動部分
ねじれ，ずれ，及び張力
患者の移動及び位置決め
音響エネルギー
- 超音波エネルギー
- 不可聴音響エネルギー
- 音
高圧液体流入
操作に関連するハザードの例
機能的なハザード
不正確又は不適切な出力
若しくは機能性
不正確な測定
間違ったデータ転送
機能の喪失又は劣化
誤使用に関連するハザード
不注意
物忘れ
規則に基づく失敗
知識に基づく失敗
日常的な違反

以下は，ISO 14971 表 E.2 で提供されるハザードを特定する手助けとして使用できる情報源のリストである。リスクの同定で予見できる一連の事象を特定するためには，事象の発生過程を追跡して要素を押さえていくことである。ここで，事象発生の引き金となる事象及び周囲の状況についての検討が有効である場合が多く。表 E.2 は引き金になる事象及び周囲の状況の例を一般的な分類にまとめたものである。

表 1-4 引き金になる事象及び周囲の状況の例（ISO 14971 表 E.2 より）

一般的な分類	引き金となる事象及び周囲の状況の例
不完全な要求事項	次に関する不完全な仕様
	・ 設計のパラメータ
	・ 操作のパラメータ
	・ 性能の要求事項
	・ **サービス**に関する要求事項(保守,再処理など)
	・ 製品寿命
製造プロセス	製造プロセス変更管理が不十分
	材料又は材料の適合性に関する情報の管理が不十分
	製造プロセス管理が不十分
	下請負業者の管理が不十分
輸送及び保管	不適切な包装
	汚染又は劣化
	不適当な環境条件
環境要因	物理的要因（熱，圧力，時間など）
	化学的要因（腐食，分解，汚染など）
	電磁場（電磁干渉による影響など）
	電力の不適切な供給
	冷却材の不適切な供給
洗浄，消毒及び滅菌	洗浄，消毒及び滅菌に関する有効な手順が存在しない，又は不適切な仕様
	洗浄，消毒及び滅菌の不適切な実施
廃棄及び解体	情報が提供されない，又は不適切な情報提供
	誤使用
組成	生分解性
	生体適合性
	情報が提供されない，又は提供された仕様が不適切
	不正確な組成に起因するハザードに関する不適切な警告
	誤使用

表 1-5（続き）引き金になる事象及び周囲の状況の例（ISO 14971 表 E.2 より）

一般的な分類	引き金となる事象及び周囲の状況の例
人的要因	設計上の欠陥に起因する誤使用の可能性，例えば次がある。
	・ 取扱い説明がない,又は分かりにくい。
	・ **制御システム**が複雑又は分かりにくい。
	・ 医療機器の状態が紛らわしい,又は明確でない。
	・ 設定,計測値又はその他の情報の表示が紛らわしい,又は明確でない。
	・ 結果の誤表示
	・ 視認性,可聴性又は感触性が不十分
	・ 動作に対する制御の割当て,又は実際の状態に対する表示情報の割当てが不適切
	・ 既存の装置と比べ問題を引き起こしやすいモード又は配置
	・ 熟練していない,又は訓練を受けていない者が使用
	・ 副作用に関する警告が不十分
	・ 単回使用医療機器を再使用した場合のハザードに関する警告が不適切
	・ 計測及びその他の計量が不正確
	・ 消耗品,附属品及びその他の医療機器との不適合
	・ うっかりミス,過失及び誤り
故障モード	電気的又は機械的な完全性の予想外の喪失
	老化，摩耗及び反復使用による機能の劣化（例えば，液体又はガス流路が徐々に閉塞する，流動抵抗及び電気伝導度の変化）
	疲労故障

(3) 生活支援ロボットの重要ハザードのリスト

・以下の表は生活支援ロボットの安全要求事項(JIS B 8445：2016 (ISO 13482：2014))から抜粋したハザードリストである。この中では特に ISO 14971 のハザードリストで扱われていないロボット特有のハザードに注意を払うためのチェックリストとして用いたい。
ロボット特有のハザード･･･下表＃１，２，３，４などの太文字で表した項目

表 1-6　ISO 14971 のロボット機能の危険源を補強する情報（ISO 13482 より）

番号	危険源の種別	危険源分析		関連する安全要求事項の項番号	注記
		危険源	潜在的結果		
1	電池充電の危険源，エネルギーの蓄積及び供給の危険源	電池の過負荷	火災，危険な煙又は物質の放出	5.2	
2		過放電した電池の充電	火災，危険な煙又は物質の放出	5.2	
3		電池活端子との接触	感電	5.2	
4		電池の短絡	火災，危険な煙又は物質の放出	5.2	
5	エネルギーの蓄積及び供給の危険源	高い電気エネルギー源との危険な接触	感電，やけど	5.3.1	
6		障害（不具合）条件下で電気構成部品･部品が帯電部となること	感電	5.3.1	
7		高い機械的エネルギー源との危険な接触	押し潰し，切断，閉込み，やけど	5.3.1	高エネルギーの機械部品には，回転･高速な可動部，高圧の水圧又は空圧，燃料燃焼サブアセンブリを含む。

表 1-7　(続き)ISO 14971 のロボット機能の危険源を補強する情報（ISO 13482 より）

番号	危険源の種別	危険源分析		関連する安全要求事項の項番号	注記
		危険源	潜在的結果		
8		高い空圧エネルギー源との危険な接触	押し潰し，切断，閉込み，噴射	5.3.1	
9		高い油圧エネルギー源との危険な接触	押し潰し，切断，閉込み，噴射	5.3.1	
10		高い化学エネルギー源との危険な接触	やけど，炎症	5.3.1	
11		高温･高熱エネルギー源との危険な接触	やけど	5.3.1	
12		貯蔵エネルギーの制御されない解放（急激な放出，爆発）	火災，やけど，押し潰し，突き刺し，切断	5.3.2	貯蔵エネルギーは，空圧及び油圧の蓄圧器，コンデンサ，電池，ばね，釣合いおもり，フライホイールなどの中で発生することがある。
13		動力故障	押し潰し，閉込み，負荷の落下，暴走	5.3.3	
14		意図しない運転停止	押し潰し，閉込み，負荷の落下	5.3.3	
15		電力過負荷	火災	5.3.3	
16		部分的動力故障（部分停電）	その他の危険源	5.3.3	
17		危険な静電放電	感電	5.5.1	

表 1-8　(続き)ISO 14971 のロボット機能の危険源を補強する情報（ISO 13482 より）

番号	危険源の種別	危険源分析		関連する安全要求事項の項番号	注記
		危険源	潜在的結果		
18	ロボットの起動による危険源	意図しない･予期しない起動	その他の危険源	5.4	
19		起動時又は再起動時にとる危険な動作	その他の危険源	5.4	
20	ロボット形状による危険源	鋭利な端部	切断，断裂，突き刺し，擦過	5.6	
21		可動部間の穴又は隙間	押し潰し，閉込み，挟まれ，切断，断裂，擦過	5.6	
22		部品の危険な脱離･落下	押し潰し，閉込み	5.6	
23		衝突時に危険なロボット外形形状	衝撃傷害，押し潰し，閉込み，切断	5.6	
24	騒音による危険源	有害な音響ノイズレベル	難聴，ストレス，不快感，失調，意識低下	5.7.1	
25	ロボットの有害な超音波	放射	難聴，ストレス，不快感，失調，意識低下	5.7.1	
26	認知不足による危険源	騒音が小さい又は無音の運転	人との衝突（衝撃傷害を引き起こす），又はその他の安全関連障害物との衝突	5.14	この危険源は，もし生活支援ロボットのユーザに聴覚障害がある場合，ロボットがたとえ騒音を立てていても気付かないという可能性について検討することが望ましい。人間装着型身体アシストロボットには適用しない。

表 1-9　(続き)ISO 14971 のロボット機能の危険源を補強する情報（ISO 13482 より）

番号	危険源の種別	危険源分析		関連する安全要求事項の項番号	注記
		危険源	潜在的結果		
27	有害な振動	有害な振動レベル	けん（腱）の炎症，腰痛，不快感，神経症，関節炎，乗物酔い，及びその他の振動関連の傷害	5.7.2	
28		振動による，ディスプレイの読み取りやすさの低下	ユーザの正しくない行動，又はユーザが制御失うことで生じる有害な事象	5.7.2	
29	有害物質及び流動体	生活支援ロボットから放出された有害物質，流動体（作動油など）との接触	やけど，炎症，感作	5.7.3	
30		生活支援ロボットの放出する揮発性溶媒，煙	感作，炎症，窒息，失明	5.7.3	
31	ロボット表面との接触によるアレルギー反応	炎症，感作	5.7.3		

表 1-10　(続き)ISO 14971 のロボット機能の危険源を補強する情報（ISO 13482 より）

番号	危険源の種別	危険源分析		関連する安全要求事項の項番号	注記
		危険源	潜在的結果		
32	危険な環境条件	高いレベルのじんあい	火災，その他の危険源	5.15	次のようなところで生活支援ロボットを運転する意図がある場合に検討する。 – 家庭内環境 – 大量の粉体又は細かい粒状物質があるところ（キッチンなど） – ロボットの保守点検の間隔を長期間とって運転するように意図されている場合
33		砂	鋭利な端部を形成するすりそがれた表面，不安全な姿勢・配置の原因となる可動部のジャミング，衝突の原因となる制動性能の低下	5.15	生活支援ロボットを屋外環境で運転するように意図されている場合に検討する。
34		生活支援ロボットの雪，氷などへの暴露	可動部のジャミング，短絡危険源，センサの干渉による正しくない動作，その他の危険源	5.15	生活支援ロボットを冬の環境又は寒帯で運転するように意図されている場合に検討する。

表 1-11　(続き)ISO 14971 のロボット機能の危険源を補強する情報（ISO 13482 より）

番号	危険源の種別	危険源分析		関連する安全要求事項の項番号	注記
		危険源	潜在的結果		
35		生活支援ロボットの水，水蒸気への暴露	機能不良，火災，出力低下の原因となる短絡	5.15	生活支援ロボットを大洋，海又は他の塩水域近くの屋外環境（又はボート上若しくは船上）で運転するように意図されている場合に検討する。
36		ロボットの塩水環境又は塩水噴霧（例えば，海洋又は海岸環境）への暴露	構造故障，その他，腐食誘起機能故障を原因とする危険源，電池・動力装置の故障，短絡の危険源	5.15	生活支援ロボットを大洋，海又は他の塩水域近くの屋外環境（又はボート上若しくは船上）で運転するように意図されている場合に検討する。
37	極端な温度	高温表面	やけど，ストレス，不快感	5.7.4	
38		低温表面	やけど，凍そう（瘡），ストレス，不快感	5.7.4	
39		ディスプレイの読み取りやすさの低下	正しくないユーザの行動又はユーザが制御を失うことによって生じる有害事象	5.7.4	
40	有害な非電離放射	ロボットが有害な非コヒーレント光線（レーザ）を発する。	やけど，眼の外傷	5.7.5	
41		ロボットが有害なコヒーレント光線（レーザ）を発する。	眼の外傷（盲点，全盲）	5.7.5	人間装着型身体アシストロボットには適用しない。

表 1-12　(続き)ISO 14971 のロボット機能の危険源を補強する情報（ISO 13482 より）

番号	危険源の種別	危険源分析		関連する安全要求事項の項番号	注記
		危険源	潜在的結果		
42		ロボットが有害なレベルの EMI を発する。	医療インプラント・装置への有害な作用，外部の機械，電子装置への有害な作用，インフラ**制御システム**（例えば，輸送，配電，照明システム，電気通信）への有害な作用	この規格の対象外。関連要求事項については EMC 規格（例えば，IEC 61000 規格群）を参照	
43	有害な電離放射線	ロボットが有害なレベルの電離放射線を発する。	放射線病，生殖機能への影響，突然変異	5.7.6	電離放射線源は，ロボットの意図した用途に対し，代用可能なものがない限り，生活支援ロボットには使用しないことが望ましい。電離放射線の使用については全て，個別なリスクアセスメントを受けることが望ましい。
44	EMI・EMC の危険源	外部からの EMI による安全機能の喪失	機能ごとに定義	5.8	生活支援ロボットの全ての安全機能について検討する。

表 1-13　(続き)ISO 14971 のロボット機能の危険源を補強する情報（ISO 13482 より）

番号	危険源の種別	危険源分析		関連する安全要求事項の項番号	注記
		危険源	潜在的結果		
45		外部からの EMI に誘発された，機能の偶発的な作動	機能ごとに定義	5.8	生活支援ロボットの全ての機能（アプリケーション・**サービス**機能及び安全機能の両方）について検討する。結果及び影響を受ける領域は，機能的危険源分析（番号 78.参照）によって決めたとおりにする。
46		外部からの EMI に誘発された，生活支援ロボットの危険な動作（例えば，暴走，意図しないアームの動き）	押し潰し，閉込み，衝撃，衝突，切断，断裂	5.8	
47		外部からの EMI に誘発された，安全ではないロボットの状態	押し潰し，閉込み，衝撃，切断，断裂，火災，やけど	5.8	
48	ストレス，姿勢及び使用法による危険源	ロボットの運転に要求される無理な姿勢	筋骨格の不調	5.9.2	
49		身体的不快感の原因となる運転環境	過労，筋肉硬直	5.9.2	過労は，不快なレベルの音・騒音，光，熱，又はその他の要素への恒常的暴露が原因のことがある。

表 1-14　(続き)ISO 14971 のロボット機能の危険源を補強する情報（ISO 13482 より）

番号	危険源の種別	危険源分析		関連する安全要求事項の項番号	注記
		危険源	潜在的結果		
50		ユーザの身体サイズに対する正しくない思い込み	無理な姿勢，ユーザの疲労，筋肉傷害・不調	5.9	
51		貧弱なユーザインタフェース設計，表示器及び画像指示器の位置	ユーザの生活支援ロボットへの誤解による不快感	5.9.3	
52			危険な状況でのユーザの反応遅れ	5.9.3	ユーザインタフェースを介してユーザにタイムリーな操作を要求する，全ての安全機能について検討する。
53			誤検知によってアラームが多すぎて，ユーザにアラームの無視，スイッチオフの行動を引き起こし，そのためにアラーム信号への対応不履行へ繋がる。	5.9.3	
54			制御と表示との関係が分かりにくく，そのためにユーザの反応が誤った不適切なものとなる。	5.9.3	ユーザの体調が悪化している場合は，ユーザの能力が変化することにも配慮しなければならない
55		生活支援ロボットの貧弱な視認性	ヒューマンエラーの結果として，その他の危険源が発生	5.9	
56	ロボットの動作による危険源	機械的な不安定性（転倒，転落，過度の傾き）	押し潰し，閉込み，負荷の落下	5.10.2	

表 1-15　(続き)ISO 14971 のロボット機能の危険源を補強する情報（ISO 13482 より）

番号	危険源の種別	危険源分析		関連する安全要求事項の項番号	注記
		危険源	潜在的結果		
57		機械的な不安定性 – 荷重取扱中の転倒	押し潰し，閉込み，負荷の落下	5.10.2	
58		移動の不安定性 – 基本の行動パターンでの横転	押し潰し，閉込み，切断・断裂，負荷の落下	5.10.3	基本の行動パターンは，次のものを含む。 – 前進・後退移動 – 回転- ターン・Uターン – 加速- 減速 人間装着型身体アシストロボットには適用しない。
59		移動の不安定性 – 基本の行動パターンでの暴走	衝突，負荷の落下，環境の損傷	5.10.3	
60		移動の不安定性 – 搭乗者の位置が悪いことによる横転	押し潰し，閉込み，切断・断裂，負荷の落下	5.10.3	搭乗型ロボットにだけ適用
61		負荷運搬中の不安定性 – タスク実行中に安全関連物体が転落又は落下	環境の損傷，有害物質の放出，やけど（高温流体の場合），切断・断裂（鋭利な物体の場合）	5.10.4	
62		衝突時の不安定性 – 衝突後の横転又は転倒	押し潰し，閉込み，切断・断裂，負荷の落下	5.10.5	人間装着型身体アシストロボットには適用しない。
63		衝突時の不安定性 – 衝突後の暴走	衝突，負荷の落下，環境の損傷	5.10.5	人間装着型身体アシストロボットには適用しない。

表 1-16　(続き)ISO 14971 のロボット機能の危険源を補強する情報（ISO 13482 より）

番号	危険源の種別	危険源分析		関連する安全要求事項の項番号	注記
		危険源	潜在的結果		
64		衝突後の本体部品の脱落	押し潰し，閉込み	5.10.5	
65		人間装着型身体アシストロボット装着中の不安定性	押し潰し，閉込み，衝撃傷害	5.10.6	人間装着型身体アシストロボットにだけ適用
66		人間装着型身体アシストロボット取外し中の不安定性	押し潰し，閉込み，	5.10.6	人間装着型身体アシストロボットにだけ適用
67		搭乗者乗降時の横転	搭乗者が転落し，傷害，押し潰し，閉込みを被る。	5.10.7	搭乗型ロボットにだけ適用
68		搭乗者乗降時の暴走	搭乗者が転落し，傷害，押し潰し，閉込みを被る。	5.10.7	搭乗型ロボットにだけ適用。
69	安全関連障害物との衝突	安全関連物体との衝突	鈍的外傷，切断・断裂	5.10.8	人間装着型身体アシストロボットには適用しない。

表 1-17　(続き)ISO 14971 のロボット機能の危険源を補強する情報（ISO 13482 より）

番号	危険源の種別	危険源分析		関連する安全要求事項の項番号	注記
		危険源	潜在的結果		
70		飼育動物との衝突	動物の死傷　パニック状態に陥った動物が人を傷付け，又は環境に損害を与える。	5.10.8	動物の反応には，次のものが含まれる。 – 動物がロボットにかみ付く。 – 動物がロボットを踏みつける。 – 動物がロボットを恐れて逃げる。– 動物がロボットの存在に衝撃又は苦痛を受ける。 – ロボットのタスク行動で動物が怪我をする。人間装着型身体アシストロボットには適用しない。
71		他のロボットとの衝突	押し潰し，閉込み，負荷の落下	5.10.8	人間装着型身体アシストロボットには適用しない。
72		壊れやすい安全関連物体との衝突	環境の損傷，負荷の落下，有害物質の放出，やけど（高温流体の場合），切断・断裂（鋭利な安全関連物体の場合）	5.10.8	人間装着型身体アシストロボットには適用しない。
73		壁，恒久的・動かせない障壁との衝突	環境の損傷，負荷の落下，有害物質の放出，やけど（高温流体の場合），切断・断裂（鋭利な安全関連物体の場合）	5.10.8	人間装着型身体アシストロボットには適用しない。

表 1-18　(続き)ISO 14971 のロボット機能の危険源を補強する情報（ISO 13482 より）

番号	危険源の種別	危険源分析		関連する安全要求事項の項番号	注記
		危険源	潜在的結果		
74		活動空間内での安全関連物体の検知失敗	安全関連物体との衝突（番号 69.参照）	5.10.9	全ての機能及びタスクについて検討する（**サービス・**アプリケーション関連及び安全関連）。人間装着型身体アシストロボットには適用しない。
75		触覚インタラクション中の有害な身体反応レベル	切断・断裂，押し潰し，閉込み	5.10.9	計画された全ての人とロボットとの触覚インタラクションタスクについて検討する。インタラクションの物理的パラメータには，次のものを含めることが望ましい（該当する場合）。– 皮膚とロボットとの摩擦 – せん断応力 – 動的衝撃 – トルク – 重心の描く弧 – 荷重がかかったままの移動 – 人体の支持
76		触覚インタラクションが意図されていないロボット部分との触覚インタラクション	鈍的外傷，閉込み，押し潰し	5.10.9	

表 1-19　(続き)ISO 14971 のロボット機能の危険源を補強する情報（ISO 13482 より）

番号	危険源の種別	危険源分析		関連する安全要求事項の項番号	注記
		危険源	潜在的結果		
77	耐久性不足	耐久性不足によるロボット部品の故障	その他の危険源	5.11	全ての機能及びタスクについて検討する。耐久性不足には，次のものが含まれる（該当する場合）。 – 機械的応力による疲労 – 温度サイクルによる疲労 – 材料及びその特性 – 振動及び他の放射 – 環境条件（平常及び劣悪） – 正常運転 – 予見可能な異常運転（予期せぬ移動パターン，負荷） – 予見可能な誤使用（例えば，過負荷，破壊行為）
78	危険な自律行動	タスク実行時の危険な行動	その他の危険源	5.12	生活支援ロボットの全ての機能及びタスクに対する，機能危険源特定分析が必要（安全関連と**サービス・**アプリケーション関連との両方）

表 1-20　(続き)ISO 14971 のロボット機能の危険源を補強する情報（ISO 13482 より）

番号	危険源の種別	危険源分析		関連する安全要求事項の項番号	注記
		危険源	潜在的結果		
79	運動部との危険な接触	運動中の機械部品との危険な接触	巻込み，閉込み，押し潰し，切断	5.13	
80	位置確認及びナビゲーションの誤差による危険源	生活支援ロボットの予期せぬ動きの原因となる位置確認誤差	押し潰し，閉込み，衝撃傷害，負荷の落下	5.16	
81		禁止区域への侵入の原因となる位置確認誤差	衝突，押し潰し，閉込み，衝撃傷害，負荷の落下	5.16	
82		機械的な不安定の原因となる位置確認誤差	横転，押し潰し，閉込み，負荷の落下	5.16	
83		目的地への到達又は安全関連障害物の回避を妨げるナビゲーション誤差	衝突，押し潰し，閉込み，衝撃傷害，環境の損傷	5.16	
84	その他の危険源の種別	貧弱・不適切な取扱説明及びトレーニング資料	ユーザの過失又は誤った行動を原因とする危険事象	全て	
85		手袋，帽子，サングラス，ブーツを含む屋外用衣類の着用による，ユーザの制御能力の低下	ユーザの過失又は誤った行動を原因とする危険事象に至る，感覚の鈍化，精度の落ちる制御	全て	

(4) ロボット介護機器の特質の調査の例

下表は ISO 14971 箇条 4.2 特質の明確化 プロセスにて使用可能なツールである。
開発を開始する前に，ロボット介護機器の安全に関する特質を導出し，機械の制限範囲の決定に役に立つ，または，リスクマネジメント計画に反映するためのチェックリストの例である。
（ISO 14971 附属書 C の医療機器への質問事項をロボット介護機器用に置き換えた文書。）

表 1-21 ロボット介護機器の安全に関する特質チェックリスト（例）

ロボットタイプ名： 装着型歩行アシストロボット
商品企画書＃：

No.	安全に関する特質の明確化 ※安全に関する特質を記録。可能な場合，関連するハザードも記録する。		
	チェック観点	特質	ハザード／危険状態／危害の特定
1	ロボット介護機器の意図する用途はなにか？	（例）屋外での使用あり	（例）雨濡れによる製品発火
2	ロボット介護機器は誰にどのように使用されるか？（高齢者？障害者も使用し，特段の配慮が必要か？）	（例）高齢者，障害者が使用	
3	ロボット介護機器は疾病の診断，予防， 監視， 治療， 苦痛緩和等の医療行為を果たすか？		
4	ロボット介護機器は埋込みを意図しているか？		
5	ロボット介護機器は患者またはその他の人に接触することを意図しているか？ ・接触の期間？ ・接触の頻度？・表面的接触か？空間共有か？		

特質を考慮した場合の考えうるハザード

対象製品特有の用途・特性・使われ方の（制限）範囲

表 1-22 （続き）ロボット介護機器の安全に関する特質チェックリスト（例）

No.	安全に関する特質の明確化 ※安全に関する特質を記録。可能な場合，関連するハザードも記録する。		
	チェック観点	特質	ハザード／危険状態／危害の特定
6	どのような材料または部品がロボット介護機器に使用されているか？ またはロボット介護機器と一緒に，あるいは接触して使用されるか？ 材料の安全性に関する特性が既知であるか否か？		
7	使用者にエネルギを与えるかまたは使用者からエネルギを取り出すか？ ・エネルギの種類は？　・制御方法／持続時間は？		
8	使用者（患者）に投与及び／または採取する物質はあるか？		
9	ロボット介護機器によって生体材料が処理されるか？		－
10	ロボット介護機器は滅菌・清掃されて供給されるか？		
11	ロボット介護機器は，ユーザが定期的に洗浄及び消毒をすることを意図しているか？ ・洗浄剤や消毒剤の種類は？ ・洗浄サイクルと回数は？ ・使用人数，回数は？ ・有効期限は？		
12	ロボット介護機器は使用者の環境を変えることを意図しているか？ ・温度　・湿度　・防塵防滴　・屋内／屋外　・照明　・居室／トイレ　・監視者の不在		
13	ロボット介護機器は測定をするか？ ・測定される変数は？　・必要な精度は？		

表 1-23 （続き）ロボット介護機器の安全に関する特質チェックリスト（例）

No.	安全に関する特質の明確化 ※安全に関する特質を記録。可能な場合，関連するハザードも記録する。		
	チェック観点	特質	ハザード／危険状態／危害の特定
14	ロボット介護機器は分析・判断機能を持っているか？ ・安全に影響するか？　・使用するアルゴリズム		
15	ロボット介護機器は医薬品またはその他の医療技術との併用が予見されるか？ ・どのような医薬品か？　・どのような医療技術か？		
16	ロボット介護機器は好ましくないエネルギまたは物質を排出するか？ ・騒音，振動 ・化学物質 ・熱 ・放射線，磁界 ・電波		
17	ロボット介護機器は環境的影響を受けやすいか？ ・使用時の環境・輸送時の環境，保管時の環境 ・温度，湿度，振動		
18	ロボット介護機器は環境に影響を及ぼすか？ ・発熱・毒性のある物質の排出 ・EMC		
19	ロボット介護機器に関連する消耗品及び付属品は存在するか？ ・どのような消耗品，付属品か？ ・正しくない消耗品，付属品が使用される可能性		

表 1-24 （続き）ロボット介護機器の安全に関する特質チェックリスト（例）

No.	安全に関する特質の明確化 ※安全に関する特質を記録。可能な場合，関連するハザードも記録する。		
	チェック観点	特質	ハザード／危険状態／危害の特定
20	保守または校正が必要か？ ・どのような保守，校正か？ ・校正を誰が行うか？		
21	ロボット介護機器はソフトウェアを含んでいるか？ ・受容できないリスクを発生させるか？または受容できるレベルに低減させるソフトウェアか？		
22	ロボット介護機器には使用期限に関する制約があるか？ ・使用期限に達した際の処置		
23	使用が遅れた場合または長期使用の影響はどうか？ ・材料の劣化 ・電池の消耗 ・滅菌保証		
24	ロボット介護機器は，どのような機械的なカを受けるか？ ・ユーザの意図された使用の上でかかるカ ・他の装置・設備等とのインタフェースによるカ ・意図されていない負荷（落下等）		
25	何がロボット介護機器の寿命を決めるか？ ・材料の劣化 ・電池の消耗 ・滅菌保証		
26	ロボット介護機器は，使い捨てを意図するか？ ・使用前，使用後が明瞭か？		－

表 1-25 （続き）ロボット介護機器の安全に関する特質チェックリスト（例）

No.	安全に関する特質の明確化 ※安全に関する特質を記録。可能な場合，関連するハザードも記録する。		
	チェック観点	特質	ハザード／危険状態／危害の特定
27	ロボット介護機器は，安全に使用停止または廃棄することが必要か？ ・廃棄物として毒性や危険性のある物質をもつか？		
28	ロボット介護機器の据え付けまたは使用は特別な訓練を必要とするか？ ・据え付け方法　・使用方法　・訓練の必要性		
29	安全な使用に関する情報をどのように提供するか？ ・取級説明書・ラベル ・ユーザの教育・再教育の必要性		
30	新たな製造工程を確立または導入する必要があるか？ 新たな製造設術は？　・製造規模の増大は？		
31	ロボット介護機器の適切な適用は，ユーザインタフェースのようなヒューマンファクタに依存するか？		
32	ユーザインタフェース上の設計特性が使用ミスの誘因となるか？		
33	ロボット介護機器は，不注意が使用ミスを招くような環境で使用されるか？		
34	ロボット介護機器は，接続部または付属品を持っているか？		
35	ロボット介護機器は，制御インタフェースをもっているか？		
36	ロボット介護機器は，情報を表示するか？		
37	ロボット介護機器は，メニューで制御するか？		

表 1-26 （続き）ロボット介護機器の安全に関する特質チェックリスト（例）

No.	安全に関する特質の明確化 ※安全に関する特質を記録。可能な場合，関連するハザードも記録する。		
	チェック観点	特質	ハザード／危険状態／危害の特定
38	ロボット介護機器は，特別なニーズのある人により使用され得るか？		
39	インタフェースはユーザのアクションを開始させられるか？		

(イ)　リスク分析で用いる技法

以下の記述は，**ISO/TR 14121-2** からの抜粋である。この文書は JIS 化されていない。

(1) リスクマトリックス法

リスクマトリックス法は，傷害のひどさの程度と傷害が起こる可能性の組み合わせからリスクを推定する方法であり，一般的にこれら 2 つの組み合わせで表す。
各々の特定された危険な状態に関して，それぞれに該当するパラメータを選び，その組み合わせからリスクの程度を推定することになる。一つの例を下に示す。

表 1-27 リスク評価マトリックス（例）

傷害の起こる可能性	傷害のひどさ			
	破滅的	重篤	中程度	軽度
起こって当たり前	高い	高い	高い	中間
起こるだろう	高い	高い	中間	低い
起こるかもしれない	中間	中間	低い	無視できる
起こらないかもしれない	低い	低い	無視できる	無視できる

各々の特定された危険な状態に対して傷害のひどさを推定するが，自社の過去の事例などを参考に求めることになる。傷害のひどさに関しては，例えば以下のように考える。

- 破滅的　－　回復不能で仕事への復帰もできないような障害や死亡
- 重篤　－　いずれ仕事に復帰できるが，重篤な傷害
- 中程度　－　応急手当ではすまないかなりの傷害だが，同じ仕事に復帰できる
- 軽度　－　応急手当で済むかそれ以下の傷害で，作業時間に影響しないか影響がわずか

傷害のひどさに関しては，低位の推定になることを避けるため，一般的に起こった場合の最悪の状態を想定する。
傷害の起こる可能性の推定には，自社の過去の履歴を参考にする。しかし，傷害の発生はまれなのが一般的なので，主観的にならざるを得ない。結果的には，何人かで集まって協議することになる。傷害のひどさ同様，例えば以下のように考える。

- 起こって当たり前：　ほぼ間違いなく起こる
- 起こるだろう：　十分に起こりえる
- 起こるかもしれない：　起こるとは考えにくい
- 起こらないかもしれない：　ほぼ無視できるかまず起こらない

これらの結果を導くためには，以下のことなどを考慮することになる。

a） 危険源にさらされる頻度と長さ
b） 危険源にさらされる人数
c） 仕事を担当する人物（熟練，非熟練など）
d） ロボット介護機器やその業務の履歴
e） 作業環境
f） 人的要因（人間工学，業務状態など）
g） 安全機能の信頼性
h） 安全機能の無効化や保護などのリスク低減策の回避の可能性
i） 保護やリスク低減策の維持のしやすさ
j） 傷害の防ぎやすさ

上の表（表 3-3）では，傷害の起こる可能性が「起こるだろう」で，傷害にひどさが「重篤」の場合，リスクは「高い」という結果になり，リスク低減策が必要になる。ここにあげた例はいくつかあるリスクマトリックス法の一つにすぎず，他の分類方法もあるので，自社のロボット介護機器に合う方法を検討してもよい。当然ながら，傷害の起こる可能性や傷害のひどさを細分化すると，評価者による結果のばらつきは少なくなる。しかしながら，所詮，リスクの推定が主観的なので，その結果であるリスクレベルも主観的なものになる。

(2)

(3) リスクグラフ法

リスクグラフ法は，リスクの推定要素である，傷害のひどさ，危険源にさらされる頻度，危険事象の発生確率，回避の可能性などを分岐点にし，大小あるいは大中小のように二分岐や三分岐してその結果を求める方法である。その例を下に示す。

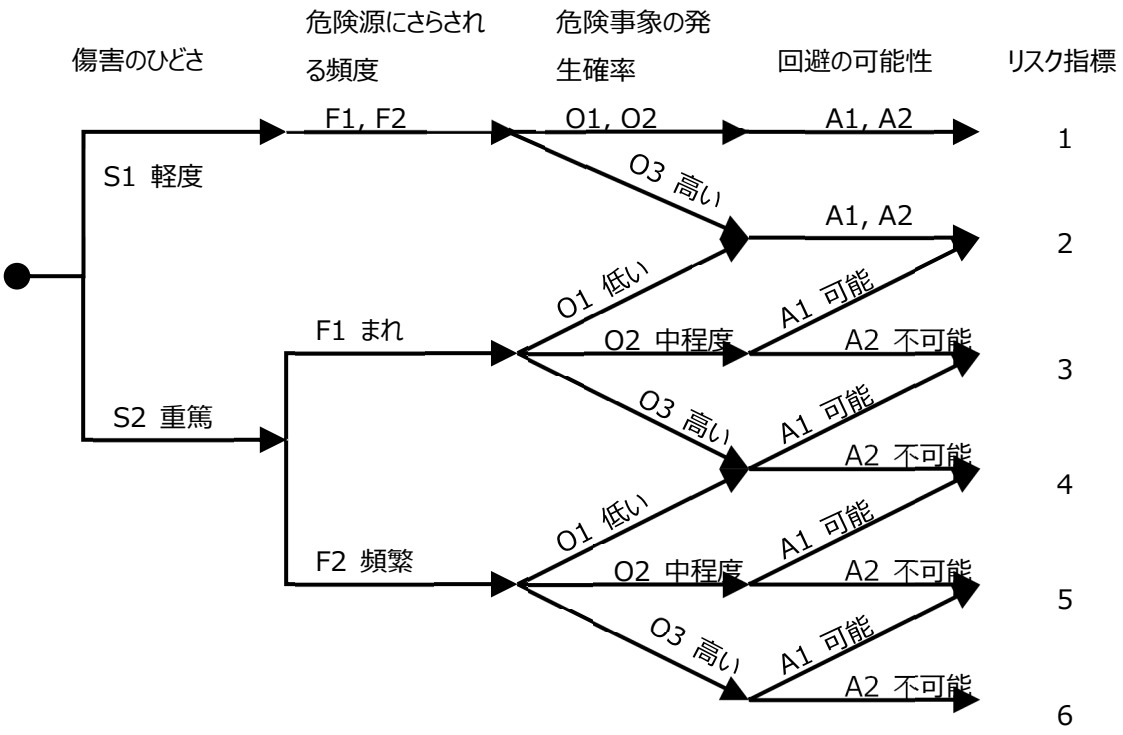


図 3-2 リスクグラフによるリスク推定の例（ISO TR 14121-2，図３から変更）

各々の危険事象に対して，要素を当てはめ，リスク指標を求める。リスクグラフは，評価対象のリスクに対して，どの要素が大きく影響しているかがよくわかり，どのようなリスク低減策が有効かを知ることができる。リスク指標は，一般的に以下のように理解される。

a） 1 から 2： 低いリスク

b） 3 から 4： 中程度のリスク

c） 5 から 6： 高いリスク

各リスク推定要素に関しては，次のように決めることができる。

傷害のひどさ： S

- S1: 擦り傷，切り傷，青あざ，応急処置を要する外傷で同じ仕事への復帰に 2 日もかからないような傷害
- S2: 手足の骨折，裂傷，骨折，縫合を必要とする傷害，主要な筋骨格外傷など一般的に完治できない傷害

危険源にさらされる頻度：　F

- F1：まれもしくは短時間だけ危険源にさらされる。危険源にさらされることが 1 シフトで 2 回以下，または，1 シフトあたりの 15 分未満
- F2：頻繁や連続もしくは長い時間危険源にさらされる。危険源にさらされることが 1 シフトで 3 回以上，または，1 シフトあたり 15 分以上

危険事象の発生確率　O

- O1：　起こりそうもなく，過去に発生していないと思われる。成熟した技術で，安全が立証されている，あるいは，信頼できる
- O2：　いつか起こりそう。技術的な不具合が過去 2 年内に起こった。訓練されリスクを認識し 6 か月以上の経験を持つ人による不適切な行動
- O3：　頻繁に起こりそう。6 か月もたたずによく起こる技術的な不具合。訓練されず 6 か月に満たない経験を持つ人による不適切な行動

回避の可能性　A

- A1：　条件付きで可能
  危害を生じる部分が秒速 25cm 未満で動き，かつ，作業者はリスクを理解し，迫ってくる危険を示す表示がある。作業者は，危険を認識できそれに対応する能力を有する。温度，騒音，扱いやすさなど，いくつかの状況による
- A2：　不可能

リスクグラフは，後述するように，他の規格で，安全制御系の安全度を推定するための参考情報として使われている

(4)　点数法

２つ以上の要素を数値化し，それらの計算結果からいくつかの等級を求める方法である。定性的ではなく，異なる値を要素に関連付けして定数的に求める。数値は，要素のリスクへの影響度により重み付けする。いくつかの方法があるが，以下に一つの例を示す。

ここでは，傷害のひどさと傷害の起こる可能性の二つの要素の各々を４つの等級に分けて点数付けしている。

傷害のひどさの要素を以下の重篤度点数(SS で示す)とする。

- 破滅的　　SS=100
- 重篤　　99≧SS≧90
- 中程度　　89≧SS≧30
- 軽度　　29≧SS≧0

傷害の起こる可能性を以下の可能性点数(PS)とする

- 起こって当たり前　　PS=100
- 起こるだろう　　99≧PS≧70
- 起こるかもしれない　　69≧PS≧30

- 起こらないかもしれない　29≧PS≧0

この例では，これら二つの点数を加算してリスク点数(RS)とし，以下の表のように分ける。

表 1-28 リスク点数と等級（例）

—	高い	≧160
159≧	中間	≧120
119≧	低い	≧90
89≧	無視できる	≧0

例えば，傷害のひどさが 75 点で，傷害の起こる可能性が 50 点の場合，その合計は 125 点なので，リスクは中間のレベルになる。

この方法は，何人かで採点してその平均を集計して求めることができるので，評価者による結果のばらつきを抑えることができる.

(5) ハイブリッド法

ここでは，リスクマトリックス法と点数法を組み合わせた方法を紹介する。また，報告書に使えるような様式も提示してあるので，独自の報告書を作成する場合の参考にできる。

この様式の使い方を，以下に述べる。

リスクの推定は，通常一度では済まず，開発の各段階やリスク低減を行った後に繰り返すことになる。このため提示した様式には，何度目のリスク推定かを書くようにしている。回数ではなく，開発段階を示す言葉を書くようにしてもよい。初回は，おそらく企画段階でまだ製品のコンセプトが出来上がった程度で行うことになるだろう。その後，製品の詳細が決まるに従い繰り返される。参照番号など，使い方は自由であるが，例えば同じリスクに同じ番号を与えることにより，履歴を追跡できる。同様に，危険源番号は，危険源の種類ごとに番号を付与することなどにより，その製品の有する主たる危険源が明確になる。

危険源の欄には，どのような危険源があるかを記載する。挟み込みがある場合でも，使用状況により，リスク推定が異なるかもしれないので，それらの詳細は，詳細欄に記入する。

重篤度(Se)の欄には，推定される傷害の大きさにより 1 から 4 の点数を入れる。

1　応急処置で対処できる軽い傷害（すり傷，打撲傷など）を意味する。
2　医師の手当てを必要とする回復可能な傷害（ひどい裂傷，突き刺し，ひどい打撲傷など）を意味する。
3　重傷又は回復不可能な傷害を意味する。治った後に以前の仕事を続けることが可能である。手足骨折のような回復可能ではあるが重い傷害を含めてもよい。
4　死亡，眼や腕をなくす致命的又は回復不可能な重大傷害を意味する。もし治ったとしても，以前の仕事を続けることは非常に難しい。

頻度(Fr)は，危険な状況にさらされる頻度の平均であり，以下のように点数付けする。点数には重みづけがしてある。

1　危険源にさらされる間隔が 1 年以上

2　危険源にされられる間隔が 2 週間より長いが，1 年未満
3　危険源にさらされる間隔が 1 日より長いが，2 週間以下
4　危険源にさらされる間隔が 1 時間より長いが，1 日以下
　この場合，一回当たりのさらされる時間が１０分より短い場合は，点数を 1 点減らすことができる
5　危険源にさらされる間隔が 1 時間以下　－　この場合，条件によりこの値は減らすことはできない

頻度Ｆｒは，この後に述べる可能性 Pr や回避性 Av とも関係が深いが，出来るだけ互いに独立に推測するようにする。

可能性(Pr)は，危険な事象が発生する可能性である。例えば，人の特性や，制御の信頼性などが影響する。自社や工業会などで所有する事故履歴なども参考にできる。その他，異なる運転モードでロボット介護機器が通常と異なる動きをする場合や，その動きが予測できない場合，また，関与している人のストレスなども考慮して推測する。その点数を以下に示す。

1　部品が，危険な状態を起こすような不具合を起こすとは決してない。人間工学に基づく設計がなされて，人の間違いが考えられない。
2　部品が，危険な状態を起こすような不具合を起こすことはまれである。人の間違いが起こるとは，考えにくい。
3　部品が，危険な状態を起こすような不具合を起こすかもしれない。人の間違いが起こるかもしれない。
4　部品が，危険な状態を起こすような不具合をおそらく起こすだろう。人の間違いが考えられる。
5　部品が，このような用途には作られていない。部品の不具合が危険事象を起こす。人の間違いを起こす可能性が非常に高い。

回避性(Av)のパラメータは，危険源による危害を回避又は限定できるかといった，ロボット介護機器の設計や意図する使用法を考えて，見積もることになる。例えば，以下のことを考える。

- 操作する人が，熟練しているか否か
- 危険な状態がいきなり危害につながるかどうか
- 危険な状態が直接目視あるいは感知できるかどうか
- 警告などによる，リスクへの気づきの有無

その点数は以下のように考える。

1　例えば，機械などでは，動く部分（危険源）がインターロックされた防護柵の中にある場合など，危険な状態になるためには 2 つ以上の条件が必要な場合。
3　例えば，機械などでは，機械への巻き込みという危険源は，それがゆっくり回転し，なおかつ，作業者との間に十分なスペースがあれば，防ぐことは可能である。
5　装着型のロボット介護機器のように，直ちに脱出できない状況で，急に大きな力で意図しない動きがあった場合，それから逃れることはできないだろう。

等級(ＣＩ)は，これまでに求めた，頻度(Fr)，可能性(Pr)，回避性(Av)の各点数の合計になる。
この例の場合，重篤度(Se)と等級(Cl)の組み合わせで，リスクレベルを求めることになる。例えば，
重篤度が２の場合で，等級が７以下であれば，低いリスク，
重篤度が２の場合で，等級が８から１０の場合は，中程度のリスク，
重篤度が２の場合で，等級が 11 以上の場合は，高いリスクとなる。

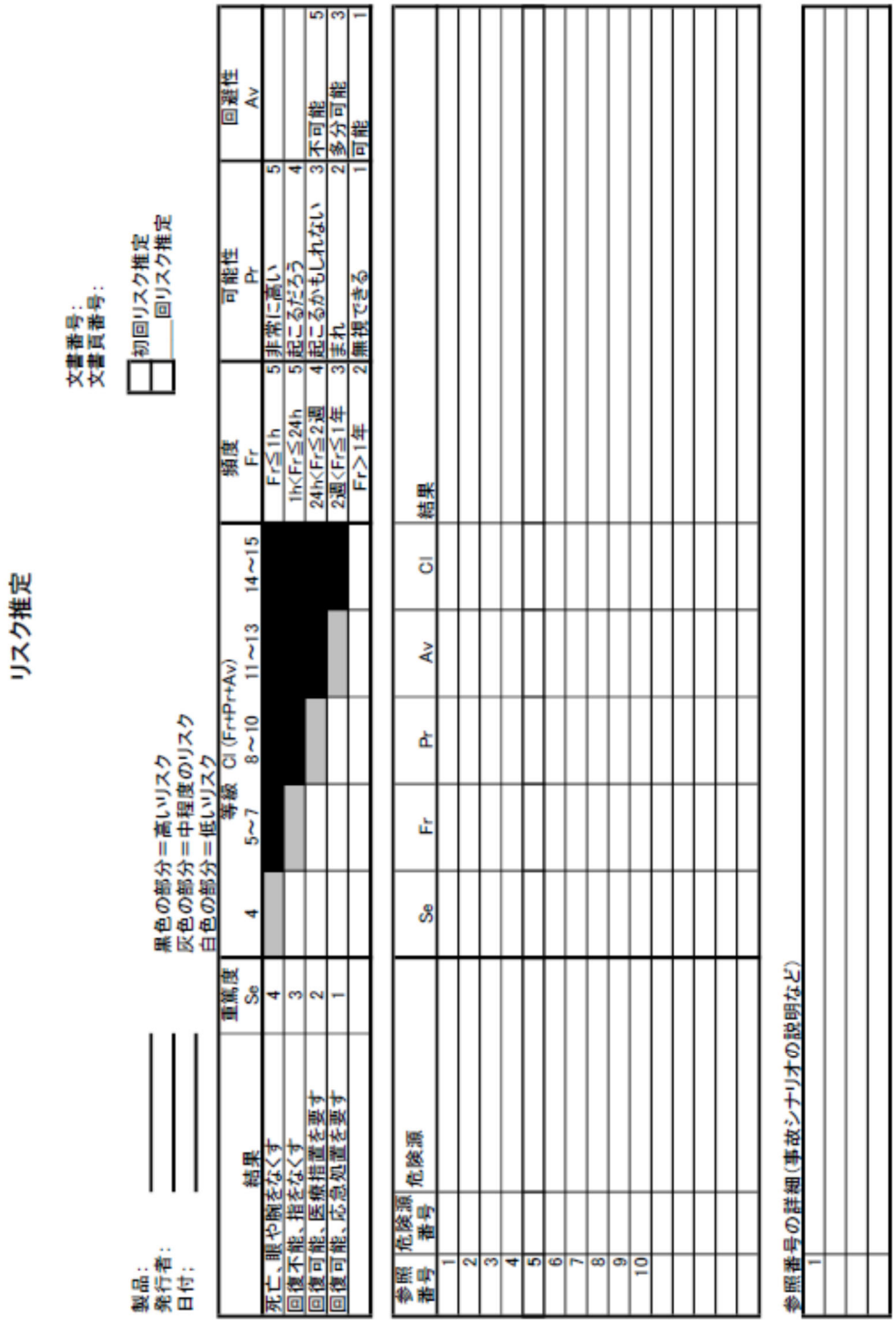


図 1-6 ハイブリッド方式のリスクアセスメント例

(6) 確率が推定できないリスク(ISO 14971 D.3.2.3)

リスクの大きさを評価の際，系統的な故障の確率を推定することは困難である。確率推定が困難な例として、以下がある。

- ソフトウェアの故障
- 医療機器での手順の省略又は不正行為
- 十分解明されていない新たな医学的，毒性学的などのハザード。

確率推定値の確度が疑わしい場合には，より広範囲の確率の推定を行うか，又はある特定の値と比較をして判断することなどが行われる。しかし，危害の発生確率についてのデータが存在しなければ，リスクの推定も不可能であり，その場合，危害の特質だけに基づいてリスクを評価することが通常必要となる。ハザードが現実的にはほとんど危害を引き起こさない場合，リスクは受容可能であると判断することができるので，リスクコントロール手段は不要である。しかし，重大な危害に至るハザードについては，許容可能なリスクレベルに低減するようなハザードの曝露のレベルは特定できない。そのような場合には，危険事象の発生確率の推定として合理的に最悪である値を基にして，リスクを推定するのが望ましい。図 1-7 に示すように，IEC 62304 では，そのような考え方で開発エンジニアリングの厳しさを決定する。

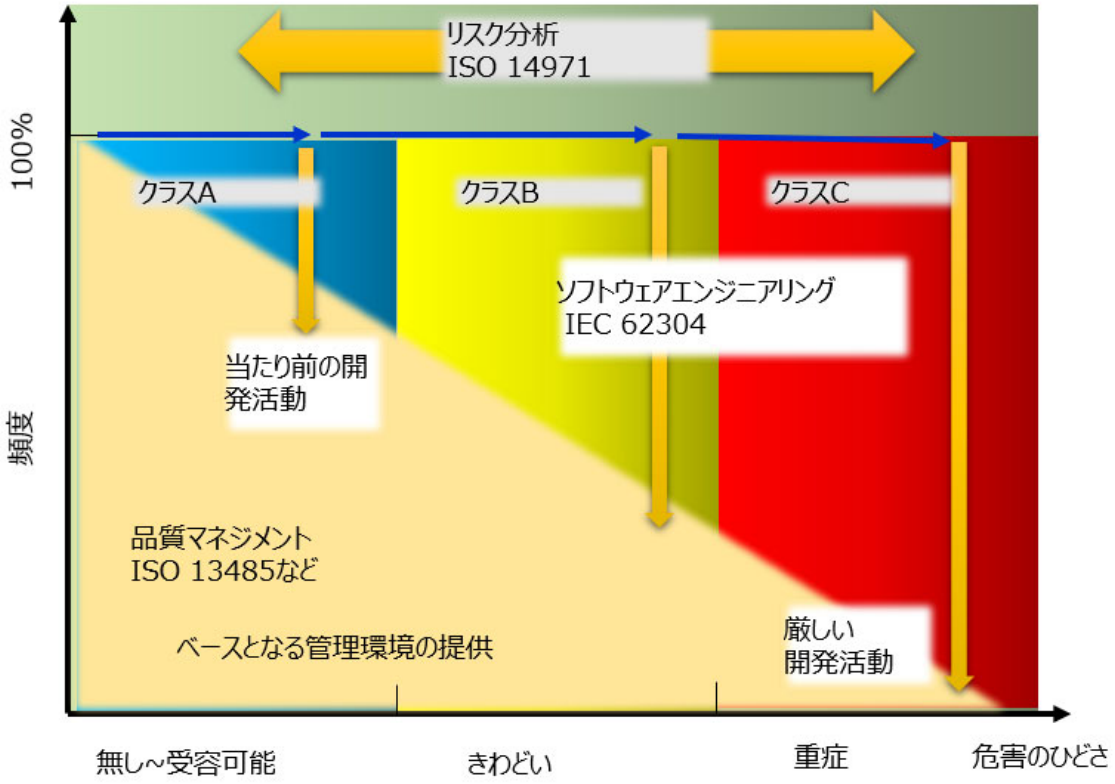


図 1-7 ソフトウェア開発への IEC 62304 の品質要求のイメージ

IEC 62304 では，危険状態の発生がソフトウェアに起因する場合は，一般に危害の発生確率を 1

（100%）としている。つまり，危険事象の発生確率を 1（100 %）とみなした上で，外部のリスクコントロール手段によりハザードが危険状態になることがないようにするか，危害が発生する確率を受容可能なレベルまで低減するか，又は危害の重大さを低減できるリスクコントロール手段を用いることになる。設計・開発プロセスの厳格さと，作り込まれ，検出されずに潜在する系統的な故障の確率との間には関連性があり，
IEC 62304 では，危害の重大さとそのリスクコントロール手段の効果に応じて，開発プロセスに必要とされる厳格さを特定する。結果が悪いほど，かつ，外部のリスクコントロール手段の効果が少ないほど，開発プロセスの要求品質は更に高くなる。

(ウ)　　リスク評価で用いる技法

リスクを推定できたら，次にそのリスクを評価する作業にうつる。リスクアセスメントという言葉は他の章でも何度か出てきているが，リスクアセスメントの結果は，「リスクは受容できるか？」といった問いに対する答えで，「はい」か「いいえ」の 2 択であり，開発において，慎重かつ合理的な判断が必要となる。「はい」の場合は，そのまま設計を続け，「いいえ」の場合は，リスク低減が必要になる。その判断を下す作業がリスク評価と呼ばれる作業になる。初回以降のリスク評価の場合で，保護方策やリスク低減策がとられた場合，その効果として，リスクが充分に低減され，受容できるレベルになったかどうかの判断になる。
例えば，リスクの推定結果が「低いリスク」とか「無視できる」の場合を「リスクは受容できる」と判断するなど，その時点における自社製品の履歴，業界動向，社会情勢など広く判断して，受容可能なリスクのレベルを決める必要がある。あるいは，先にも述べたが，自然災害の確率などを参考に，「これは事故なのでやむを得ない」と判断されるレベルを求めて決めることになるかもしれない。おそらく，どの規格を探しても，「このリスクレベルは受容できる」といった記載はないだろう。
一般的に，ロボット介護機器などはその使用される国や地域の法律や決まりが適用される可能性があり，医療機器と見なされる場合もある。従って，これらも考慮の上で，結論を出すことになる。

(1) リスク／効用 分析 (ISO 14971 D.6)

ISO 14971 では，製造業者は効用に照らしてリスクを受容できるかどうかを判断するリスク／効用 分析を実施する機会をもつことができる。但し，あらゆるリスクに対してリスク／効用 分析を要求するわけではない。
リスク／効用について考慮する前に，更なるリスク低減が実現できないかを検討することが望ましい。そのリスクに暴露されることを防止する，あるいは低減できる治療法や代替設計の採用によって，期待する臨床的効用を得ることができるか，をまず考察する。実現可能な全てのリスクコントロール手段を適用した後，リスクが受容可能性についての判断基準を満たさない場合は，一般的には設計を断念することになる。しかし，医療機器の使用に期待される効用がそのリスクを上回る場合に，比較的大きな残留リスクを正当化できることもあり，この場合，リスク／効用 分析を実施する機会をもつことができる。
ISO 14971 では，リスクを推定するためのプロセスは規定しているが，効用を推定するための手法は規定していない。専門的，臨床的，規制的，経済的及び社会的状況を理解した者が，これらを考慮し，

リスク／効用の判定に責任を持つとある。この責任には，想定する使用状況において当該製品に適用できる規制や規格の要求事項も含まれる。

効用の推定では，次のような事項を考慮する。

・　臨床使用時に期待される医療機器の性能
・　その性能から期待される臨床的結果
・　他の治療の選択肢におけるリスク及び効用に関連する要因

上記に関する証拠がどの程度信頼できるかによって，効用の推定の確からしさが決まる。

リスク／効用は，次のような特質を考慮して比較をする。

・　異なる結果を比較するのは難しい。例えば，疼痛が緩和されるが，運動性の喪失が伴う場合では，どちらの方が好ましくないかを比較するのは困難である。
・　初期には問題とならなかった副作用によって，異なった結果になる場合もある。
・　不確定な効用の結果を推定することは難しい。不確定な結果には，回復期間に現れるものもあれば，長期的な影響として生じるものもある。

リスクと効用を直接比較することが妥当であるのは，共通の尺度が使える場合に限られる。共通の尺度を用いる場合は，リスク／効用の比較を定量的に評価してもよい。リスクと効用を間接的に比較する場合は，共通の尺度を使用するのでなく，定性的に評価を行う。

リスク／効用 分析を行う場合，次を注意点を考慮する。

・　該当するハザード及び製品について十分な文献を検索する。
・　高効用／高リスクの機器は，通常，最良の技術が使われており，効用がある一方で，損傷又は疾病のリスクを完全には取り除くことはできない場合がある。したがって，正確なリスク／効用分析には，実際の医療に関連した最新の技術を理解することが必要となる。
・　受容可能なリスク／効用の判断基準を満たしていることを示すために，臨床試験がしばしば必要となる。臨床試験では，患者だけでなく，使用者及び医療従事者を含めて社会的に受け入れられるかを評価することもできる。
・　高リスク／高効用の機器を使用する前に，リスク／効用に関する適切な判断を下せるように，使用者，患者及び医療従事者に十分な情報を提供することが望ましい。
・　高リスク／高効用の機器については，通常，規制における追加要求事項があり，市販前にこれを満たす必要がある。
・　リスク／効用 分析を必要とする新規製品又は改良製品を市場に出すに当たり，製造業者は，リスク／効用の推定に関連する利用可能な情報を要約し，適用できる根拠とともにリスク／効用 分析を実施した結論を文書化することが望ましい。

(エ)　機能安全で用いる技法

(1) 安全機能を担う制御回路の安全度

より高いリスクを制御する回路に対しては，より高い信頼性が必要であることは，容易に想像できるであろう。その等級を表現するために，機械安全では，PL や SIL という指標が使われる。PL は Performance Level の略で安全機能の制御回路の性能を示す。SIL は Safety Integrity Level の略で JIS では「安全度」と訳されている。PL という指標は，ISO 13849-1 で導入され，SIL という指標は，IEC 61508 で導入され，機械安全には IEC 62061 で導入された。これらの指標は，いずれも安全機能の喪失確率をもとに規定されている。その確率を単純比較した関係を以下に示す。なお，これらの指標の決定には他の要素も関係するため，双方での単純比較は危険であり，単なる参考にとどめることとする。

表 1-29　1 時間当たりの安全機能喪失頻度

安全度	1 時間当たりの安全機能喪失頻度	パフォーマンスレベル
対象範囲外	$10^{-5} \leqq PFHd < 10^{-4}$	PL a
SIL 1	$3X10^{-6} \leqq PFHd < 10^{-5}$	PL b
	$10^{-6} \leqq PFHd < 3X10^{-6}$	PL c
SIL 2	$10^{-7} \leqq PFHd < 10^{-6}$	PL d
SL 3	$10^{-8} \leqq PFHd < 10^{-7}$	PL e
SIL 4	$10^{-9} \leqq PFHd < 10^{-8}$	対象範囲外

表からわかるように，パフォーマンスレベルの方が安全度よりも一桁大きい数字までカバーし，かつ，細かく区分していることがわかる。これは，機械においては，この程度の頻度を詳しく検討する必要があることによる。また，SIL 4 は，プラントなど大規模な設備に適用されるレベルで，一般的に，機械に適用する機会が無いので，PL の方ではカバーしていない。

このように，これらの数字の背景には，その規格の対象物の特性が関係しているので，自社製品をよく理解して，これらの考え方を用いることが肝要になる。

(2) 制御回路に要求される安全性能の求めかた

機械の安全関連の制御回路を評価する場合，パフォーマンスレベルがよく使われる．
ここでは，リスク評価の結果，リスク低減が必要と判断され，リスク低減手法に制御を用いる場合，その制御回路に要求されるパフォーマンスレベルの求め方を述べる。
リスクの推定が主観的であることから，リスクレベルも主観的にならざるを得ず，このような理由で，どのリスクレベルにどのようなパフォーマンスレベルを適用するかといった規定はない。ISO 13849-1 では，安全制御回路に要求されるパフォーマンスレベル（PLr と表す）の求め方を付属書 A に参考として**図 1-8** のようにリスクグラフ法を用いて記述している。ここでは，危害のひどさ(S)，危険源にさらされる頻度や時間(F)，および，危険源の回避や制限の可能性(P)の 3 つのパラメータの大小をリスクグラフにしている。

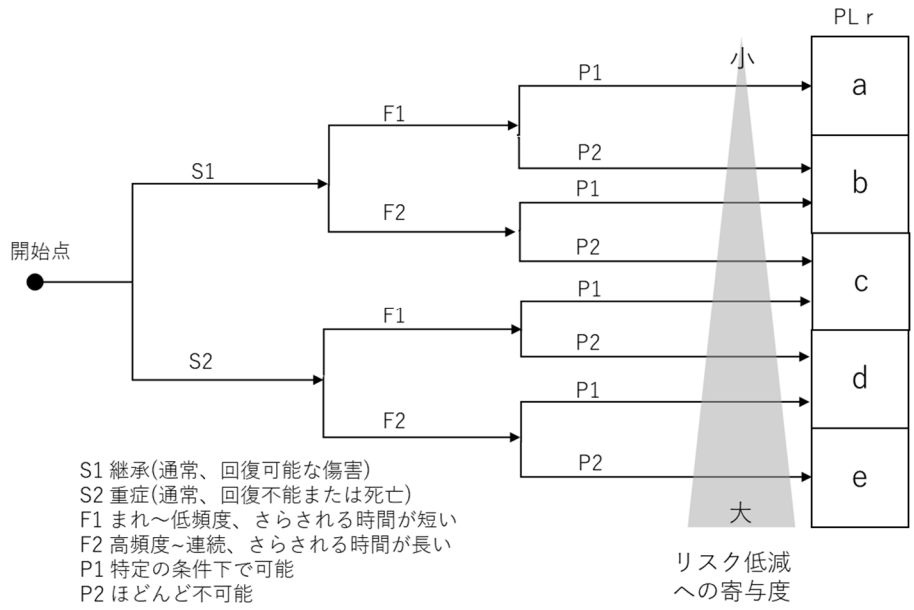


図 1-8　PLr を求める例(ISO 13849-1 から変更)

今のところこれ以外に，参考になる記述は無いので，自社で選択したリスク推定の方法をこのリスクグラフと見比べて，制御回路に要求される性能(PLr)を求めることになる。
先にも述べたように，ロボット介護機器の規格として開発中の ISO 21856 は，IEC 0601-1 の考え方をもとにしており，ハードウェアの偶発的な故障は，単一故障のシミュレーションで対応している。ここで求めた，安全制御回路に要求される性能は，系統的な故障へ対応するための目標になる。

(3) データ通信のための安全技術の例

データ通信が，安全機能の実装において使用される時，通信プロセスの残留欠陥率のような故障限界値は，以下の項目に注意を払う必要がある。
この故障限界値は，ランダム故障からの安全機能の故障限界値を見積もる時，注意を払うべきである。

No.	通信欠陥	概要説明
1	通信エラー	メッセージの破損
2	反復	古いメッセージが繰り返し受信される
3	喪失	メッセージが消去される
4	挿入	別のメッセージが挿入される
5	誤配列	メッセージの受信順序を誤る
6	書換え	メッセージの内容が書き換えられる
7	遅延	規定の時間内に通信が完了しない
8	偽装（なりすまし）	認証されていない機器から信頼できない情報を受信する、又は、不正なアドレス指定を含む

図 1-9 データ通信で考慮すべき欠陥

上記の通信欠陥の 1 つの偽装“masquerade”は，メッセージの発信源が正しく確認されることである。例えば，非安全の要素からのメッセージが安全要素のメッセージとして不正に確認されることであり，通信の分野ではこのような不正アドレス指定の事例が多くなっている。

これらの要件を組み込む通信データとして，IEC61784-3 の従った，以下の例に示すような方法も広く行われている。

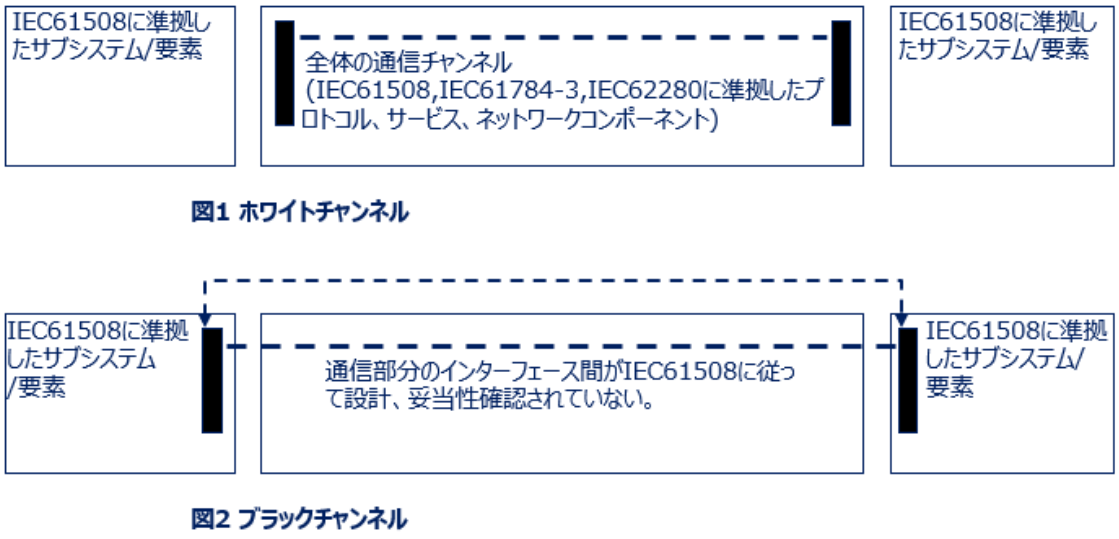


図 1-10　IEC 61784-3 に準拠したデータ通信の構造

IEC 61784-3 に準拠した安全通信

安全データの通信には，一般的に使用されるデバイスネットやイーサネットが使用されることがある。このような通信は，通信データを保護するため様々な方法が使用される。

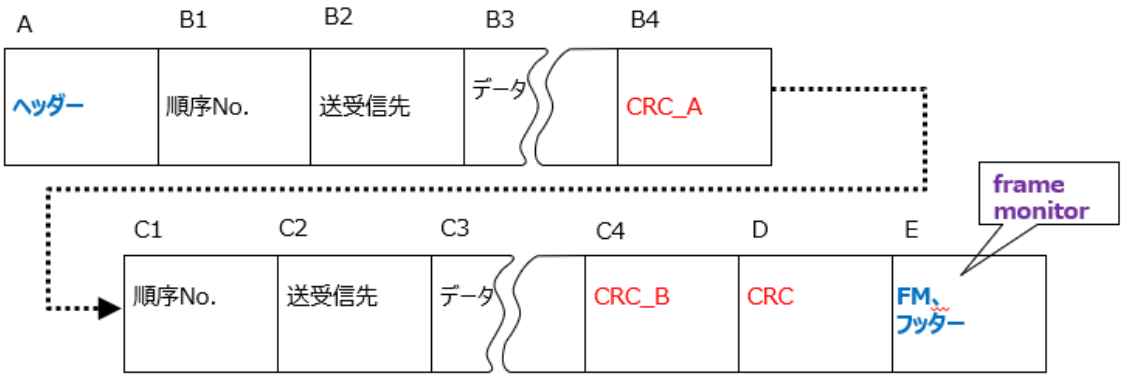


図 1-11 安全通信データの構成

通信データの形式を以下の条件とする。

(1) A と E は，通信のファームウェアによって作られる。

(2) B4 は，B1 から B3 の CRC。これは，個別の安全関連系アプリケーションの通信制御ソフトウェアによって作られる。

(3) C1 から C3 は，B1 から B3 の反転データ(1 の補数又は 2 の補数)

(4) C4 は，C1 から C3 の CRC。(2)と同様，個別の安全関連系アプリケーションの通信制御ソフトウェアによって作られる。

(5) D は，通信のファームウェアによって作られる。例えば，B1 から C4 までの CRC。

(6) E のフッターには，通信フレームの良否診断情報が含まれる。

No.	通信欠陥	通信データの判定要素
1	通信エラー	D,Eで判定可能
2	反復	B1,C1　順序No.が更新されることで判定可能
3	喪失	B1からB4、C1からC4のデータを比較することで判定可能
4	挿入	B1からB4、C1からC4のデータを比較することで判定可能
5	誤配列	B1からB4、C1からC4のデータを比較することで判定可能
6	書換え	B1からB4、C1からC4のデータを比較することで判定可能
7	遅延	B1,C1が規定の時間で更新されないことで判定可能
8	偽装（なりすまし）	B2,C2の一致とB1からB4、C1からC4のデータを比較することで判定可能。更に暗号化を加えることもある。

図 1-12 通信データの形式

付録C 関連用語集

本ガイダンス文書で使用する関連規格の定義，および関連する専門用語を表形式にてまとめ，解説を加える。

注記：

・出典は医療系の国際規格に加え，機械安全や機能安全規格の定義からも参照している。規格が異なれば定義の言い回しも異なる場合があるので注意が必要である。

・国際規格・JIS 規格などの規格に定義されていない専門用語は独自の説明を記述している。

(ア)　ロボットおよびロボティクスデバイスに関する用語（ISO 8373 Robots and robotic devices — Vocabulary）

表 1-30 ロボットおよびロボティクスデバイスに関する用語

用語	説明
ロボット [ISO 8373 Cl.2.6]	二つ以上の軸についてプログラムによって動作し，ある程度の自律性をもち，環境内で動作して所期の作業を実行する運動機構。 注記 1 ロボットは，制御システム及び制御システムとのインタフェースを含む。 注記 2 ロボットを産業用ロボット又はサービスロボットに分類するには，所期の用途によるものとする。 (対応英語 robot)
自律性 [ISO 8373 Cl.2.2]	人の介入なしに，現在の状態及びセンシングに基づいて所期の作業を実行する能力。 (対応英語 autonomy)

表 1-31 （続き）ロボットおよびロボティクスデバイスに関する用語

用語	説明
制御システム [ISO 8373 Cl.2.7]	ロボットの機械構造の監視・制御及び環境（装置及び使用者）との通信を可能にする論理制御及び動力機能の全体。 (対応英語 control system)
ロボティックデバイス [ISO 8373 Cl.2.8]	産業用ロボット又はサービスロボットの特徴を満たすが，プログラムできる軸数又は自律性の程度に不足のある運動機構。例 パワーアシスト装置，遠隔操縦装置，2 軸の産業用マニピュレータ。 (対応英語 robotic device)
産業用ロボット [ISO 8373 Cl.2.9]	自動制御され，再プログラム可能で，多目的なマニピュレータであり，3 軸以上でプログラム可能で，1 か所に固定して又は移動機能をもって，産業自動化の用途に用いられるロボット。 注記 1 産業用ロボットは，次のものを含む。 – マニピュレータ（アクチュエータを含む。）。 – 制御装置［ペンダント及び通信インタフェース（ハードウェア及びソフトウェア）を含む。］。 注記 2 産業用ロボットは，統合による追加軸を含む。 (対応英語 industrial robot)
サービスロボット [ISO 8373 Cl.2.10]	人又は設備にとって有益な作業を実行するロボット。産業自動化の用途に用いるものを除く。 注記 1 産業自動化の用途には，製造，検査，包装，組立などがある。 注記 2 多関節ロボットは，生産ラインで使われる場合は産業用ロボットであるが，食事支援に使う場合はサービスロボットである。 (対応英語 service robot)

(イ)　リスクマネジメント･リスクアセスメントに関連する用語（ISO 14971, ISO 12100）

表 1-32 リスクマネジメント･リスクアセスメントに関連する用語

用語	説明
安全 （safety） [ISO 14971:2007, Cl.2.24]	受容できないリスクがないこと。 ［ISO/IEC Guide 51:1999 定義 3.1］
リスク（risk）[ISO 14971:2007, Cl.2.16]	危害の発生確率とその危害の重大さとの組合せ。［ISO/IEC Guide 51:1999 定義 3.2］ [ISO 12100 の定義] 3.12 リスク（risk）危害の発生確率と危害のひどさとの組合せ。
重大さ （severity） [ISO 14971:2007, Cl.2.25]	ハザードから生じる可能性がある結果（危害）に対する尺度。
危害（harm） [ISO 14971:2007, Cl.2.2]	人の受ける身体的傷害若しくは健康障害，又は財産若しくは環境の受ける害。 ［ISO/IEC Guide 51:1999 定義 3.3］ ［ISO 12100 の定義］ 3.5 危害（harm） 身体的傷害又は健康障害。

表 1-33　（続き）リスクマネジメント・リスクアセスメントに関連する用語

用語	説明
ハザード　（hazard） [ISO 14971:2007, 2.3]	危害の潜在的な源。 ※規格によっては”危険源”という。 ［ISO/IEC Guide 51:1999 定義 3.5］ [ISO 12100 の定義] 3.6 危険源 危害を引き起こす潜在的根源。 注記 1 用語“危険源”は，その発生原因（例えば，機械的危険源，電気的危険源）を明確にし，又は潜在的な危害（例えば，感電の危険源，切断の危険源，毒性による危険源，火災による危険源）の性質を明確にするために修飾されることがある。 注記 2 この定義において，危険源は，次を想定している。 － 機械の“意図する使用”の期間中，恒久的に存在するもの（例えば，危険な動きをする要素の運動，溶接工程中の電弧，不健康な姿勢，騒音放射，高温）又は － 予期せずに現れ得るもの（例えば，爆発，意図しない及び予期しない起動の結果としての押しつぶしの危険源，破損の結果としての放出，加速度又は減速度の結果としての落下）

表 1-34　（続き）リスクマネジメント・リスクアセスメントに関連する用語

用語	説明
危険状態（hazardous situation） [ISO 14971:2007, Cl.2.4]	人，財産又は環境が，一つ又は複数のハザードにさらされる状況。 ［ISO/IEC Guide 51:1999 定義 3.6］ ［ISO 12100 の定義］ 3.7 危険状態（hazardous situation） 人が少なくとも一つの危険源に暴露される状況。 注記 暴露されることが，直ちに又は長期間にわたり危害を引き起こす可能性がある。
危険事象（hazardous event） [ISO 12100, Cl.3.9]	危害を起こし得る事象。 注記：危険事象は短い期間又は比較的長期にわたって発生する可能性がある。
残留リスク（residual risk） [ISO 14971, Cl.2.15]	リスクコントロール手段を講じた後にも残るリスク。 注記 *1 ISO/IEC Guide 51:1999*，定義 *3.9* に基づく。 注記 *2 ISO/IEC Guide 51:1999*，定義 *3.9* は，“リスクコントロール手段”ではなく“防護手段”という用語を用いている。しかしこの規格では，*6.2* に規定するとおり，“防護手段”はリスクをコントロールするための選択肢の一つである。 [ISO 12100 の定義] *3.13* 残留リスク（*residual risk*） 保護方策を講じた後に残るリスク（図 *1* 参照）。 注記 *1* この規格は次の二つに区別する。– 設計者が保護方策を講じた後の残留リスク– 全ての保護方策を実施した後の残留リスク 注記 *2* 図 *2* 参照。

表 1-35　（続き）リスクマネジメント・リスクアセスメントに関連する用語

用語	説明
タスク（task） [ISO 12100:2010, 3.25]	機械のライフサイクルの間，機械に対して，又は機械の近傍で一人以上によって遂行される特定の活動。
意図する使用（意図する目的）（intended use/intended purpose） [ISO 14971:2010, Cl.2.5]	製造業者が供給する仕様，説明及び情報に従った製品，プロセス又はサービスの使用。 [ISO 12100 の定義] 3.23 “意図する使用”（intended use） 指示事項の中で提供されている使用上の情報に基づく機械の使用。
合理的に予見可能な誤使用（reasonably foreseeable misuse） [ISO 12100:2010, 3.24]	設計者が意図していない使用方法であるが，容易に予測できる人間の挙動から生じる機械の使用。
誤使用　（use error） [ISO 14971:2007, Cl.2.27]	製造業者が意図する又は使用者が予期する医療機器の動き（反応など）と異なる結果を招く行為又は行為の省略。 注記 1 誤使用には，うっかりミス（slips，不注意による間違い），過失（lapses，記憶に起因する間違い），誤り（mistakes，手順の無視，間違った知識，無知などに基づく間違い）を含む。 注記 2： IEC 62366:2007 Annex B 及び D.1.3 を参照する。 注記 3： 予期しない患者の物理的な反応は，誤使用とは見做さない。 ［IEC 62366:2007 定義 3.21］

表 1-36　（続き）リスクマネジメント・リスクアセスメントに関連する用語

用語	説明
リスク推定（risk estimation） [ISO 14971:2007, Cl. 2.20]	危害の発生確率とその危害の重大さに対して重み付けをするために用いるプロセス。
リスク分析　（risk analysis） [ISO 14971:2007, Cl.2.17]	利用可能な情報を体系的に用いてハザードを特定し，リスクを推定すること。 ［ISO/IEC Guide 51:1999 定義 3.10］ 注記 リスク分析は，危険状態及び危害を生じる可能性のある様々な一連の事象の検討を含む。 ［ISO 12100 の定義］ 3.15 リスク分析（risk analysis） 機械の制限に関する仕様，危険源の同定及びリスク見積りの組合せ。
リスク評価（risk evaluation） [ISO 14971:2007, Cl.2.21]	判断基準に照らして推定したリスクが受容できるかを判断するプロセス。 ［ISO 12100 の定義］ 3.16 リスク評価（risk evaluation） リスク分析に基づき，リスク低減目標を達成したかどうかを判断すること。

表 1-37　（続き）リスクマネジメント・リスクアセスメントに関連する用語

用語	説明
リスクアセスメント（risk assessment） [ISO 14971:2007, Cl.2.18]	リスク分析及びリスク評価からなる全てのプロセス。 ［ISO/IEC Guide 51:1999 定義 3.12］ [ISO 12100 の定義] 3.17 リスクアセスメント（risk assessment） リスク分析及びリスク評価を含む全てのプロセス。
適切なリスク低減（adequate risk reduction） [ISO 12100:2010, 3.18]	現在の技術レベルを考慮したうえで，少なくとも法的要求事項に従ったリスクの低減。 注記 いつ適切なリスク低減が達成されたかを決めるための基準を *5.6.2* に示す。
リスクコントロール（risk control） [ISO 14971:2007, Cl.2.19]	規定したレベルまでリスクを低減するか又はそのレベルでリスクを維持するという決定に到達し，かつ，そのための手段を実施するプロセス。
リスクマネジメント（risk management） [ISO 14971:2007, Cl.2.22]	リスクの分析，評価，コントロール及び監視に対して，管理方針，手順及び実施を体系的に適用すること。 (ISO Guide 73 : 2009) *2.1* リスクマネジメント（*risk management*） リスクについて，組織を指揮統制するための調整された活動。 ※IEC 60601-1 では，リスクマネジメントには，製造情報及び製造後情報の計画又は監視を含まないが，これらは ISO 14971 に適合するためには必要である。

表 1-38　（続き）リスクマネジメント・リスクアセスメントに関連する用語

用語	説明
リスクマネジメントファイル（risk management file） [ISO 14971:2007, Cl.2.23]	リスクマネジメントによって作成した記録及び他の文書のまとまり。 ※IEC 60601-1 注記 製造業者の計算書，試験結果などを含む全ての安全関連情報は，リスクマネジメントファイルの一部であるとみなす。
客観的証拠（objective evidence） [ISO 14971:2007, Cl.2.10]	あるものの存在又は真実を裏付けるデータ。 ［ISO 9000 定義 3.8.1］
手順 （procedure） [ISO 14971:2007, Cl.2.12]	活動又はプロセスを実行するために規定された方法。 ［ISO 9000 定義 3.4.5］
プロセス （process） [ISO 14971:2007, Cl.2.13]	インプットをアウトプットに変換する，相互に関連する又は相互に作用する一連の活動。 ［ISO 9000 定義 3.4.1］
記録 （record） [ISO 14971:2007, Cl.2.14]	達成した結果を記述した，又は実施した活動の証拠を提供する文書。 ［ISO 9000 定義 3.7.6］

表 1-39　（続き）リスクマネジメント・リスクアセスメントに関連する用語

用語	説明
検証　（verification） [ISO 14971:2007, Cl.2.28]	規定した要求事項を満たしたことを客観的証拠の提供によって確認すること。 注記 1 “検証された”という用語は，対応する状態を示す場合に用いる。 注記 2 確認作業の例には次がある。 － 別の方法での計算の実施 － 新たな設計仕様と実証済みの類似設計仕様との比較 － 試験及び実証 － 発行前の文書のレビュー ［ISO 9000 定義 3.8.4］ ※尚，JIS C 0508-4 では，verification を「適合確認」と訳している。従って，付録「機能安全開発における考慮すべきポイント」では”適合確認”と記述している。
保護方策 **（protective measure）** [ISO 14971:2007, Cl.3.19]	リスク低減を達成することを意図した方策。次によって実行される。 － 設計者による方策（本質的安全設計方策，安全防護及び付加保護方策，使用上の情報）及び － 使用者による方策［組織（安全作業手順，監督，作業許可システム），追加安全防護物の準備及び使用，保護具の使用，訓練］

表 1-40　（続き）リスクマネジメント・リスクアセスメントに関連する用語

用語	説明
本質的安全設計方策（inherently safe design measure） [ISO 14971, Cl.3.20]	ガード又は保護装置を使用しないで，機械の設計又は運転特性を変更することによって，危険源を除去する又は危険源に関連するリスクを低減する保護方策。
安全防護（safeguarding） [ISO 12100, Cl.3.21]	本質的安全設計方策によって合理的に除去できない危険源，又は十分に低減できないリスクから人を保護するための安全防護物の使用による保護方策。

表 1-41　（続き）リスクマネジメント・リスクアセスメントに関連する用語

用語	説明
医療機器 **（medical device）** [ISO 14971, Cl.2.9]	あらゆる計器，器械，用具，機械，器具，植込み用具，体外診断薬，キャリブレータ，ソフトウェア，材料又はその他の同類のもの若しくは関連する物質であって，単独使用か組合せ使用かを問わず，製造業者が人体への使用を意図し，その使用目的が次の一つ以上であり， － 疾病の診断，予防，監視，治療又は緩和 － 負傷の診断，監視，治療，緩和又は補助 － 解剖学的又は生理学的なプロセスの検査，代替又は修復 － 生命支援又は維持 － 受胎調整　　－ 医療機器の殺菌 － 人体から採取した検体の体外試験法による医療目的のための情報提供 薬学，免疫学，又は新陳代謝の手段によって体内又は体表において意図したその主機能を達成することはないが，それらの手段によって機能の実現を補助するものである。［ISO 13485 定義 3.7］ 注記 1：医療機器規制国際整合化会議［Global Harmonization Task Force (GHTF)］によって定義された。参考文献[38]を参照する。 注記 2：国又は地域によって医療機器と見做される場合もあるが，整合した取組みがまだ存在しない製品として次がある。 － 身体障害又は障害者のための補助器具 － 動物の疾病及び傷害の治療又は診断のための機器 － 医療機器の附属品（注記 3 参照） － 消毒剤 － 動物及び人の組織に由来する機器で，上記の定義を満たす場合もあるが，異なる法規制の対象となる機器 注記 3 医療機器の意図する目的を達成するために，その医療機器と組み合わせて使用することを， 製造業者が指定した附属品は，この規格の対象とする。

表 1-42　（続き）リスクマネジメント・リスクアセスメントに関連する用語

用語	説明
製造業者 **（manufacturer）** [ISO 14971, Cl.2.8]	医療機器の市場出荷又は使用開始の前に，医療機器の設計，製造，こん（梱）包若しくはラベリング又はシステムの組合せ若しくは変更に責任を負う個人又は法人。その業務をその個人若しくは法人又は代理を受けた第三者が行うか否かを問わない。 注記 1：国又は地域の法規制で製造業者を定義している場合があることに注意する。 注記 2：ラベリングの定義は，ISO 13485 定義 3.6 を参照する。
トップマネジメント **（top management）** [ISO 14971, Cl.2.26]	最高位で製造業者（組織）を指揮し，管理する個人又はグループ。 注記 ISO 9000 定義 3.2.7 に基づく。

(ウ)　医用電気機器（プログラマブル電気医用システム：PEMS を含む）に関連する用語（IEC 60601-1）

表 1-43 医用電気機器（プログラマブル電気医用システム：PEMS を含む）に関連する用語

用語	説明
ME 機器 **（ME EQUIPMENT）** [IEC 60601-1, 3.63]	医用電気機器（MEDICAL ELECTRICAL EQUIPMENT）の略。 装着部をもつか，患者との間でエネルギーを授受するか，又は患者に与えるか若しくは患者からのエネルギーを検出する次の電気機器。 a) 特定の電源（商用）への接続をする場合は，一か所で行う。 b) 製造業者が意図する次のいずれかの用途をもつ。 1) 患者の診断，治療又は監視 2) 疾病，負傷又は障害の補助若しくは緩和 注記 1 ME 機器には，製造業者が指定した ME 機器の正常な使用を可能にするのに必要な附属品も含まれる。 注記 2 医用に供する電気機器が全てこの定義に入るとは限らない。例えば，ある種の体外診断機器。 注記 3 能動植込形医療機器の植込み部分は，この定義に該当するようにみえるが，箇条 1 で規定したようにこの規格の適用範囲外である。 注記 4 この規格では，“電気機器”という用語を用いているが，これは，ME 機器又は他の電気機器を意味している。 注記 5 4.10.1，8.2.1 及び 16.3 参照
ME システム **（ME SYSTEM）** [IEC 60601-1:2014, 3.64]	*医用電気システム（MEDICAL ELECTRICAL SYSTEM）の略。 製造業者が指定した，機能接続によって又はマルチタップを用いて相互接続をした少なくとも一つの ME 機器を含む機器の組合せ。 注記 この規格で“機器”と表現した場合は，ME 機器を含むと解釈をしている。

表 1-44 （続き）医用電気機器（プログラマブル電気医用システム：PEMS を含む）に関連する用語

用語	説明
基礎安全（BASIC SAFETY） [IEC 60601-1:2014, 3.10]	ME 機器を正常状態及び単一故障状態で使用するとき，物理的ハザードに直接起因する受容できないリスクがないこと。
単一故障安全（SINGLE FAULT SAFE） [IEC 60601-1:2014, 3.117]	予測耐用期間中の単一故障状態においても受容できないリスクを生じない ME 機器又はその部分の特性。
単一故障状態（SINGLE FAULT CONDITION） [IEC 60601-1:2014, 3.116]	リスクを低減させる手段の一つが故障しているか，又は一つの異常状態が存在する ME 機器の状態。
正常状態（NORMAL CONDITION） [IEC 60601-1:2014, 3.70]	危険状態又は危害に対する保護のために備えた全ての手段が機能している状態。

表 1-45 （続き）医用電気機器（プログラマブル電気医用システム：PEMS を含む）に関連する用語

用語	説明
正常な使用（NORMAL USE） [IEC 60601-1:2014, 3.71]	取扱説明書に従った操作者が行う日常の点検及び調整を含む操作並びに事前準備。 注記 正常な使用と意図する使用とを混同しないことが望ましい。両方とも製造業者の意図する使用という概念を含んでいるが，意図する使用は，医療目的に着目した用語である一方，正常な使用は，医療目的だけでなく保守，輸送なども同様に含んでいる。
高信頼性部品（COMPONENT WITH HIGH-INTEGRITY CHARACTERISTICS） [IEC 60601-1:2014, 3.17]	予測耐用期間の間に ME 機器が正常な使用又は合理的に予見可能な誤使用において，この規格の安全要求事項について機能を失わないことを確実にする特性をもった部品。
沿面距離（CREEPAGE DISTANCE） [IEC 60601-1:2014, 3.19]	二つの導電性部分間の絶縁物の表面に沿った最短距離。 （IEV 151-15-50，修正）
基礎絶縁（BASIC INSULATION） [IEC 60601-1:2014, 3.9]	電撃に対する基礎的な保護のために備える絶縁。 （IEV 826-12-14，修正） 注記 1 基礎絶縁は，一つの保護手段である。 注記 2 IEV とは，国際電気標準用語集（International Electrotechnical Vocabulary）である。

表 1-46 （続き）医用電気機器（プログラマブル電気医用システム：PEMS を含む）に関連する用語

用語	説明
二重絶縁（DOUBLE INSULATION） [IEC 60601-1:2014, 3.23]	基礎絶縁及び補強絶縁の両方で構成した絶縁。 （IEV 195-06-08） 注記 二重絶縁は，二つの保護手段を備えている。
基本性能（ESSENTIAL PERFORMANCE） [IEC 60601-1:2014, 3.27]	基礎安全に関連する以外の臨床機能の性能において，製造業者の指定した限界を超えた低下又は欠如が生じたときに受容できないリスクを生じる性能。 注記 その性能が欠如又は低下したことによって，受容できないリスクが生じるかどうかを考えてみると，基本性能が最も容易に理解できる。
予測耐用期間（EXPECTED SERVICE LIFE [IEC 60601-1:2014, 3.28]	製造業者の指定した期間で，その期間内は ME 機器又は ME システムが安全に使用できると予測する期間（すなわち，基礎安全及び基本性能を維持する期間）。 注記 予測耐用期間の間に，保守が必要な場合がある。
意図する使用，意図する目的（INTENDED USE, INTENDED PURPOSE） [IEC 60601-1:2014, 3.44]	製造業者が供給する仕様，説明及び情報に従った製品，プロセス又はサービスの使用。 （ISO 14971 の 2.5） 注記 意図する使用は正常な使用と混同しないことが望ましい。両方とも製造業者が意図する使用の概念を含むが，意図する使用は，医療目的に焦点を合わせている。一方，正常な使用は，医療目的だけではなく，保守，輸送なども含む。

表 1-47 （続き）医用電気機器（プログラマブル電気医用システム：PEMS を含む）に関連する用語

用語	説明
製造業者（MANUFACTURER） [IEC 60601-1:2014, 3.55]	次のいずれかに責任を負う個人又は法人。 – ME 機器の設計，製造，こん（梱）包又はラベリング – ME システムの組合せ – ME 機器又は ME システムの変更 なお，その業務がその個人若しくは法人又は代理を受けた第三者によって行われるか否かを問わない。 注記 1 ISO 13485 では，ラベリングを次のように定義している。 文章，印刷物又は図表示であって， – 医療機器又は全ての容器若しくは包装に貼付され， – 又は医療機器に添付され， 医療機器の識別，技術解説及び使用に関係するものをいう。ただし，出荷用の文書は除く。 この規格では，そのような資料は表示又は附属文書として記載する。 注記 2 “変更”とは，既に使用中の ME 機器又は ME システムを部分変更することを含んでいる。 注記 3 一部の法規制では，上記の活動に関与する責任部門は，製造業者とみなしている。 注記 4 ISO 14971 の 2.8 を引用。
保護手段（MEANS OF PROTECTION）MOP [IEC 60601-1:2014, 3.60]	この規格の要求事項に従って，電撃のリスクを減らすための手段。 注記 保護手段は，絶縁，空間距離，沿面距離，インピーダンス及び保護接地接続を含む。

表 1-48 （続き）医用電気機器（プログラマブル電気医用システム：PEMS を含む）に関連する用語

用語	説明
PEMS 開発ライフサイクル（PEMS DEVELOPMENT LIFE-CYCLE） [IEC 60601-1:2014, 3.82]	プロジェクトの構想段階から始まり，PEMS 妥当性確認が完了した時点で終了する期間内に発生する必要なアクティビティ。
PEMS 妥当性確認（PEMS VALIDATION） [IEC 60601-1:2014, 3.83]	開発プロセスの間及び終了時に，PEMS 又は PEMS のコンポーネントが意図する使用のための要求事項を満たすかどうか決めるための評価プロセス。 注記 3.90 参照
プロセス（PROCESS） [IEC 60601-1:2014, 3.89]	インプットをアウトプットに変換する，相互に関連する又は相互に作用する一連の活動。 （ISO 14971 の 2.13）
プログラマブル電気医用システム（PROGRAMMABLE ELECTRICAL MEDICAL SYSTEM） **PEMS** [IEC 60601-1:2014, 3.90]	一つ又は複数のプログラマブル電子サブシステム（PESS）を含む ME 機器又は ME システム。

表 1-49　（続き）医用電気機器（プログラマブル電気医用システム：PEMS を含む）に関連する用語

用語	説明
プログラマブル電子サブシステム（PROGRAMMABLE ELECTRONIC SUBSYSTEM） **PESS** [IEC 60601-1:2014, 3.91]	ソフトウェア及びインタフェースを含む一つ又は複数の中央演算処理装置に基づいたシステム。
残留リスク（RESIDUAL RISK） [IEC 60601-1:2014, 3.100]	リスクコントロール手段を講じた後にも残るリスク。 （ISO 14971 の 2.15）
IT ネットワーク（IT-NETWORK） [IEC 60601-1:2014, 3.145]	物理的なリンク伝送又は無線伝送を二つ以上の指定されたノード間で提供する通信ノード及び伝送リンクからなるシステム（複数可）。 （IEC 80001-1:2010 の 2.12）

(エ)　医療機器のソフトウェアライフサイクルプロセスに関連する用語（IEC 62304）

表 1-50　医療機器のソフトウェアライフサイクルプロセスに関連する用語

用語	説明
アクティビティ（ACTIVITY） [IEC 62304/A1:2015, 3.1]	一組以上の相互関係又は相互作用のあるタスク。セーフは，本来，形容詞として用いられる。
異常　（ANOMALY） [IEC 62304/A1:2015, 3.2]	要求仕様書，設計文書，規格など，又は既存の認識若しくは経験に基づいて予想した結果を逸脱する状態。異常は，医療機器ソフトウェア又は該当する文書のレビュー，試験，分析，コンパイル又は使用中に発見されることがあるが，これには限定しない。
アーキテクチャ（ARCHITECTURE） [IEC 62304/A1:2015, 3.3]	システム又はコンポーネントの構造。 （IEEE 610.12:1990 参照）
構成アイテム（CONFIGURATION ITEM） [IEC 62304/A1:2015, 3.5]	決められた時点で一意に特定できる“もの（entity）”。 （ISO/IEC 12207 の 4.7 参照）

表 1-51　（続き）医療機器のソフトウェアライフサイクルプロセスに関連する用語

用語	説明
成果物（DELIVERABLE） [IEC 62304/A1:2015, 3.6]	アクティビティ又はタスクで要求される結果又はアウトプット（文書を含む。）。
評価　（EVALUATION） [IEC 62304/A1:2015, 3.7]	対象とする“もの（entity）”が，特定の基準に達していることを系統的に決定すること。 （ISO/IEC 12207 の 4.12 参照）
医療機器ソフトウェア（MEDICAL DEVICE SOFTWARE） [IEC 62304/A1:2015, 3.12]	医療機器に組み込むことを目的として開発した，又は医療機器として使用することを意図したソフトウェアシステム。 注記 それ自体が医療機器である医療機器ソフトウェア製品を含む。
問題報告（PROBLEM REPORT） [IEC 62304/A1:2015, **3.13**]	ユーザ又はその他の関係者が，安全でない，意図する使用に対して不適切である又は仕様に反すると判断した，医療機器ソフトウェアの実際の又は潜在的な動作の記録。 注記 1 この規格は，全ての問題報告に対して医療機器ソフトウェアの変更を要求するものではない。製造業者は，誤解，故障又は軽微な事象について，問題報告を処置の対象としなくてもよい。 注記 2 問題報告は，リリースした医療機器ソフトウェア又は開発中の医療機器ソフトウェアに適用する。 注記 3 この規格は，リリースした製品についての問題報告の法的な対応処置を，確実に特定及び実行できるようにするため，製造業者に別途方針決定を行うことを要求している。

表 1-52 （続き）医療機器のソフトウェアライフサイクルプロセスに関連する用語

用語	説明
プロセス （PROCESS） [IEC 62304/A1:2015, 3.14]	インプットをアウトプットに変換する，相互に関連する又は相互に作用する一連のアクティビティ。 （ISO 9000 の 3.4.1 参照） 注記 用語“アクティビティ”は，資源を利用することも含む。
回帰テスト（REGRESSION TESTING） [IEC 62304/A1:2015, 3.15]	システムコンポーネントの変更が，機能性，信頼性又は性能に悪影響を与えないこと，及び更なる欠陥を招かないことを判定するために要求される試験。 （ISO/IEC 90003:2004 の 3.11 参照）
セキュリティ（SECURITY） [IEC 62304/A1:2015, 3.22]	権限を与えられていない者又はシステムが，読み込んだり，変更できないように，かつ，権限を与えられている者又はシステムがアクセスを拒否されないように，情報及びデータを保護すること。 （ISO/IEC 12207 の 4.39 参照）
重傷（SERIOUS INJURY） [IEC 62304/A1:2015, 3.23]	次のいずれかの結果を引き起こすけが又は病気。 a) 生命の危険 b) 身体機能又は身体構造の永久的障害 c) 身体機能又は身体構造の永久的障害を防止するために，内科的又は外科的処置を必要とする障害 注記 永久的障害とは，軽微な障害又は損害を除く，身体構造又は機能の不可逆性の障害若しくは損害を意味する。

表 1-53 （続き）医療機器のソフトウェアライフサイクルプロセスに関連する用語

用語	説明
ソフトウェア開発ライフサイクルモデル（SOFTWARE DEVELOPMENT LIFE CYCLE MODEL） [IEC 62304/A1:2015, 3.24]	概念上の構造。 – 医療機器ソフトウェアの開発に関与しているプロセス，アクティビティ及びタスクを明確にする。 – アクティビティとタスクとの間のシーケンス及び依存性を表す。 – 規定した成果物の完全性を検証するマイルストーンを明確にする。
ソフトウェアアイテム（SOFTWARE ITEM） [IEC 62304/A1:2015, 3.25]	コンピュータプログラムの識別可能な部分（例えば，ソースコード，オブジェクトコード，制御コード，制御データ又はこれらのアイテムの集まり）。 注記 1 ソフトウェアの構造は，三つの用語によって識別できる。最上位のレベルは，ソフトウェアシステムである。最下位のレベルは，それ以上分解できないソフトウェアユニットである。 最上位及び最下位レベルを含む構成の全てのレベルを，ソフトウェアアイテムということができる。ソフトウェアシステムは，一つ以上のソフトウェアアイテムで構成され，各ソフトウェアアイテムは，一つ以上のソフトウェアユニット又は分割可能なソフトウェアアイテムで構成される。製造業者は，ソフトウェアアイテム及びソフトウェアユニットの粒度（granularity）を提示する責任がある。 注記 2 ISO/IEC 90003:2014 の 3.14，ISO/IEC 12207 の 4.41 に基づく。
ソフトウェアシステム（SOFTWARE SYSTEM） [IEC 62304/A1:2015, 3.27]	特定の機能又は特定の機能群を達成するために組む，複数のソフトウェアアイテムを結合した集合体。

表 1-54 （続き）医療機器のソフトウェアライフサイクルプロセスに関連する用語

用語	説明
ソフトウェアユニット（SOFTWARE UNIT） [IEC 62304/A1:2015, 3.28]	他のアイテムに分割できないソフトウェアアイテム。 注記 ソフトウェアユニットの粒度は，製造業者が定義する（B.3 参照）。
開発過程が不明なソフトウェア，SOUP（software of unknown provenance，SOUP） [IEC 62304/A1:2015, 3.29]	既に開発されていて一般に利用できるが，医療機器に組み込むことを目的に開発したものではないソフトウェアアイテム［“OTS ソフトウェア（off-the-shelf：既製品）”として知られているソフトウェア］又は以前開発されたソフトウェアアイテムでその開発プロセスについての十分な記録が利用できないもの。 注記 医療機器ソフトウェアシステム全体を SOUP であると主張することはできない。
システム （SYSTEM） [IEC 62304/A1:2015, 3.30]	一つ以上のプロセス，ハードウェア，ソフトウェア，設備及び人を統合化して，規定のニーズ又は目的を満たす能力を提供するまとまり。
タスク （TASK） [IEC 62304/A1:2015, 3.31]	行う必要がある一つの作業。
トレーサビリティ（TRACEABILITY） [IEC 62304/A1:2015, 3.32]	開発プロセスの二つ以上の成果物間の関係を明らかにできる程度。 （IEEE 610.12:1990 参照） 注記 要求事項，アーキテクチャ，リスクコントロール手段などは，開発プロセスの成果物の例である。

表 1-55　（続き）医療機器のソフトウェアライフサイクルプロセスに関連する用語

用語	説明
バージョン（VERSION） [IEC 62304/A1:2015, 3.34]	ある構成アイテムの識別された実例。 注記　医療機器ソフトウェアのバージョンの変更を行って新しいバージョンとする場合は，ソフトウェア構成管理を実施する必要がある。 （ISO/IEC 12207 の 4.56 参照）
レガシーソフトウェア（LEGACY SOFTWARE） [IEC 62304/A1:2015, 3.36]	法規制に適合して市場に出荷され，現在も市販されているが，この規格の現行版に適合して開発されたという客観的な証拠が不十分な医療機器ソフトウェア。
リリース（RELEASE） [IEC 62304/A1:2015, 3.37]	特定の目的のために用意された構成アイテムの特定のバージョン。 （ISO/IEC 12207 の 4.35 参照）

(オ)　機能安全に関する用語（IEC 61508 シリーズなど）

表 1-56 機能安全に関する用語(主に機械安全分野でよく使用するもの)

用語	説明
機能安全 （functional safety） [IEC 61508-4 Cl.3.1.12]	EUC 及び EUC 制御系の全体に関する安全のうち，E/E/PE 安全関連系及び他リスク軽減措置の正常な機能に依存する部分。
安全制御回路開発 [このガイダンス文書のオリジナル]	このガイド文書による造語である。 電子制御システムによりリスクの低減を行うことを指す。PEMS により実現される安全を”機能安全”とは呼べないため，このように表現している。
安全機能（safety function） **[ISO 13849-1, Cl.3.1.20]**	故障がリスクの増加に直ちにつながるような機械の機能。 （ISO 12100-1 の 3.28 参照）

表 1-57 （続き）機能安全に関する用語(主に機械安全分野でよく使用するもの)

用語	説明
信頼性（reliability, <of an item) [JIS Z 8115：2019　192-01-24]	アイテムが，与えられた条件の下で，与えられた期間，故障せずに，要求どおりに遂行できる能力。 注記 1 持続時間間隔は，例えば暦時間，動作サイクル，走行距離などのような，当該アイテムに適切な単位で表現されてもよく，かつ，当該単位は常に明確に記載することが望ましい。 注記 2 与えられた条件には，動作モード，ストレス水準，環境条件及び保全のような，信頼性に影響する側面が含まれる。 注記 3 一般的には，使用期間の始点で，要求機能が遂行できる状態にあることを仮定する。 注記 4 信頼性は分類 e) 192-05（信頼性性能）の尺度で定量化し得る。 注記 5 ソフトウェアアイテムの場合，信頼性は系の運用経過時間中に発生する故障要因の修正及び変更で改善が進み，一般的には，信頼度は経過時間とともに向上していく［信頼性成長（192-12-03）参照］。 注記 6 ソフトウェア信頼性は，特定条件下で使用するときのある性能を維持する能力を指す場合がある。 注記 7 附属書 JC 及び附属書 JF 参照。
安全な状態　（safe state） [IEC 61508-4 Cl.3.1.13]	安全が達成されている EUC の状態。 注記 1 EUC は，潜在的に危険な状態から最終的に安全な状態に移行する間，幾つかの中間的な状態を遷移する場合がある。幾つかの状態では，安全な状態は，EUC が制御し続ける場合だけ存在する。そのような連続制御は，短時間又は無期限にわたることもある。 注記 2 中間的な状態とは，例えば，自動車の ABS がブレーキの制動力を ON-OFF 制御して最終的安全状態，すなわち，自動車の停止（又は減速）を行うような場合である。制動力は，停止又は減速状態に至るまで，幾つかの ON 状態と OFF 状態を遷移する（繰り返す）ことになる。 このような遷移では，安全状態があらかじめ ON 側又は OFF 側の一方に定められないので，いわゆるフェールセーフの概念が適用できない。すなわち，ABS が制動力の ON 又は OFF のいずれの側に故障しても事故の可能性が生じる。

表 1-58　（続き）機能安全に関する用語(主に機械安全分野でよく使用するもの)

用語	説明
安全度水準（SIL） **（safety integrity level, SIL）** [IEC 61508-4, Cl.3.5.8]	安全度の値の範囲に対応する離散的水準（4 水準のうちの一つ）。 安全度水準 4 は最高の安全度水準であり，1 は最低である。 注記 1 四つの安全度水準に関わる目標機能失敗尺度（3.5.17 参照）は，IEC 61508-1 の表 2 及び表 3 に規定している。 注記 2 安全度水準は，E/E/PE 安全関連系に割り当てられた安全機能の安全要求事項を規定するために用いる。 注記 3 安全度水準（SIL）は，システム，サブシステム，要素又はコンポーネントの特性ではない。 “SIL n 安全関連系”（ここで，n は 1，2，3 又は 4）という表現の正しい解釈は，その系が n までの安全度水準をもつ安全機能に潜在的に対応できるということである。
冗長性 （redundancy） [IEC 61508-4, Cl.3.4.6]	要求された機能を実行するため，又は情報を表すための，二つ以上の手段の存在（IEC/TR 62059-11 に基づく。）。 例 二重の機能要素及びパリティビットの追加は，共に冗長性の例である。 注記 1 冗長性は，一義的には，信頼性（指定した期間にわたり確実に機能する確率），又はアベイラビリティ（指定した瞬間に確実に機能する確率）を向上させるために用いる。2oo3 のように，アーキテクチャとして誤作動を最小化するために用いてもよい。 注記 2 IEV 191(IEC 60050-191)-15-01 の定義は，不完全である。 注記 3 冗長性は，“ホット”すなわち“アクティブ”（全ての冗長なアイテムが同時に動作する。），“コールド”すなわち“スタンバイ”（冗長なアイテムは同時に動作しない。），“混在”（同じ時刻に一つ又は幾つかのアイテムが待機状態，かつ，一つ又は幾つかのアイテムが動作状態となる。）であってもよい。
多様性 （diversity） [IEC 61508-4 Cl.3.3.7]	要求される機能を実行する異なる手段。 注記 多様性は，異なる物理的原理又は異なる設計方法で達成される。

表 1-59 （続き）機能安全に関する用語(主に機械安全分野でよく使用するもの)

用語	説明
チャネル （channel） [IEC 61508-4 Cl.3.3.6]	ある要素安全機能を独立して実行する要素又は要素群。 例 2 チャネル構成。同一の機能を独立して実行する 2 チャネルをもつ構成。 注記 この用語は，完全なシステムを表すことも，システムの部分（例 センサ，最終要素）を表現することもできる。
フォールト（fault） [IEC 61508-4, Cl.3.6.1]	機能ユニットに要求される機能遂行能力の低下又は喪失を引き起こす可能性がある異常状態（ISO/IEC 2382-14 の 14.01.10）。 注記 IEV 191(IEC 60050-191)-05-01 では，“フォールト”は，予防保全，他の計画的な活動による機能停止状態，又は外部資源の不足による機能喪失状態以外の，要求される機能を遂行すること+C31 のできない状態として定義している。この規格での定義，及び IEC 60050-191 の 191-05-01 の定 義の説明を図 4 に示す。 ※別欄の[ISO 13849-1, Cl.3.1.3]の定義 ”障害（fault）” にも注意。
障害 （fault） [ISO 13849-1, Cl.3.1.3]	予防保全又はその他の計画的行動若しくは外部資源の不足によって機能を実行できない状態を除き，要求される機能を実行できないアイテムの状態。 注記 1 障害は，しばしばアイテム自体の故障の結果であるが，事前の故障がなくても存在することがある。 （IEC 60050-191 の 05-01 参照） 注記 2 この規格では，障害はランダム障害を意味する。 注記 3 障害（fault）は，ISO12100-1 では“不具合（障害）”としているが，この規格で定義する障害と同じ意味である。“不具合”は主に機械に対して用いられる。
フォールトアボイダンス （fault avoidance） [IEC 61508-4, Cl.3.6.2]	安全関連系の安全ライフサイクルの任意のフェーズで，フォールトを導き入れないようにするための技法及び手続きの使用。

表 1-60　（続き）機能安全に関する用語(主に機械安全分野でよく使用するもの)

用語	説明
フォールトトレランス（fault tolerance） [IEC 61508-4, Cl.3.6.3]	フォールト又はエラーの存在下で，要求される機能を遂行し続ける機能ユニットの能力（ISO/IEC 2382-14 の 14.04.06）。 注記 IEV 191(IEC 60050-191)-15-05 での定義は，サブアイテムのフォールトだけを考慮している。 3.6.1 の用語“フォールト”の注記を参照。
故障（機能失敗）（failure） [IEC 61508-4, Cl.3.6.4]	ある機能ユニットの要求機能の遂行能力の終結，又は要求された以外の機能の誤運用。 注記 1 これは IEV 191(IEC 60050-191)-04-01 に基づいているが，例えば，仕様又はソフトウェアの欠陥による決定論的原因故障を含むように変更されている。 注記 2 IEC 61508 規格群及び JIS Z 8115 でのフォールトと故障との関係については，図 4 参照。 注記 3 要求される機能の実行は，必然的にある種の挙動を除外し，そして幾つかの機能は避けなければならない挙動として指定することもある。そのような挙動の発生は故障（機能失敗）となる。 注記 4 故障は，（ハードウェアでの）ランダム故障と（ハードウェア又はソフトウェアでの）決定論的原因故障とのどちらかである。3.6.5 及び 3.6.6 参照。 ※別欄の[ISO 13849-1, Cl.3.1.4]の定義 ”故障（failure）” にも注意。
故障（failure） [ISO 13849-1, Cl.3.1.4]	要求される機能を遂行する能力がアイテムになくなること。 注記 1 故障後に，そのアイテムは障害をもつ。 注記 2 “故障”は事象であって，状態を示す“障害”とは異なる。 注記 3 ここに定義する概念は，ソフトウェアだけで構成されるアイテムには適用しない。 （IEC 60050-191 の 04-01 参照） 注記 4 制御下のプロセスのアベイラビリティにだけ影響する故障に関しては，この規格の適用範囲外である。

表 1-61　（続き）機能安全に関する用語(主に機械安全分野でよく使用するもの)

用語	説明
偶発的な故障 **（＝）ランダムハードウェア故障** **（random hardware failure）** [IEC 61508-4, Cl.3.6.5]	時間に関して無秩序に発生し，ハードウェアの多様な劣化メカニズムから生じる故障。 注記 1 異なる部品ごとに異なる率で生じる多くの劣化メカニズムが存在し，製造上の許容誤差がそれらのメカニズムによって部品の故障を運転中の異なる時刻に引き起こす。したがって，多くの部品から成る装置全体の故障は，予測可能な率で生じるが予測不可能な（ランダムな）時刻で発生する。 注記 2 ランダムハードウェア故障と決定論的原因故障（3.6.6 参照）とを区別する主な性質は，ランダムハードウェア故障から生じるシステムの機能失敗率（又は適当な他の尺度）が合理的な精度で予測可能であるのに対して，決定論的原因故障（による機能失敗）が，その性質上，正確には予測できない点にある。すなわち，ランダムハードウェア故障によるシステムの故障（機能失敗）率が合理的な精度をもって定量化できるのに対して，決定論的原因故障によるものは，故障へと導く事象が容易には予測できないので，正確な統計量として把握できない。
系統的な故障 **（＝）決定論的原因故障** **（systematic failure）** [IEC 61508-4, Cl.3.6.6]	正しい知識，認識，対策の欠如などの原因の決定的に関連する想定外の故障又は失敗。この原因は，設計の部分改修，製造過程，運転手順，文書化又はその他の関係する要因の修正によってだけ除くことができる［IEV 191(IEC 60050-191)-04-19］。 注記 1 部分改修がない事後保全では，通常，決定論的原因故障の原因は除去されない。 注記 2 決定論的原因故障は，同様な原因が生じると再び誘発される。 注記 3 決定論的原因故障の原因事例には，次のような項目中のヒューマンエラーがある。 － 安全要求仕様（中のヒューマンエラー） － ハードウェアの設計，製造，設置及び運転（中のヒューマンエラー） － ソフトウェアの設計，実施，その他（中のヒューマンエラー）。 注記 4 この規格群では，安全関連系の故障はランダムハードウェア故障（3.6.5 参照）と決定論的原因故障とに分類される。

表 1-62　（続き）機能安全に関する用語(主に機械安全分野でよく使用するもの)

用語	説明
エラー（error） [IEC 61508-4, Cl.3.6.11]	“計算，観察，又は測定された”値又は状態と，“真の，規定された，又は理論的に正しい”値又は状態との不一致［IEV 191(IEC 60050-191)-05-24 修正］。
危険側故障 **（dangerous failure）** [IEC 61508-4, Cl.3.6.7]	安全機能を実行するときにある役割を果たす，要素及び／又はサブシステム及び／又はシステムに関する次のような故障。 a）EUC が危険状態又は危険になり得る状態に陥るように，作動要求モードで要求された場合に安全機能の作動を阻止する，又は連続モードで安全機能を失敗させる。 b）要求された場合に安全機能が正しく作動する確率を下げる。 [ISO 13849-1, Cl.3.1.5]の定義 危険側故障（dangerous failure） SRP/CS を危険状態又は機能不能状態に導く潜在性をもつ故障。 注記 故障が現実に危険側故障を導くかどうかは，システムのチャネルアーキテクチャに依存することがある。冗長システムにおいては，危険側ハードウェア故障が SRP/CS 全体を危険状態又は機能不能状態に導く可能性は少ない
安全側故障 **（safe failure）** [IEC 61508-4, Cl.3.6.8]	安全機能を実行するときに役割を果たす，要素，サブシステム及び／又はシステムに関する次のような故障。 a）安全機能の誤作動が，EUC（又はその部品）を安全状態にする，又は安全状態を維持する結果となる。 b）EUC（又はその部品）を安全状態に置く，又は安全状態を維持するように安全機能が誤作動する確率を上げる。

表 1-63　（続き）機能安全に関する用語(主に機械安全分野でよく使用するもの)

用語	説明
従属故障 **（dependent failure）** [IEC 61508-4, Cl.3.6.9]	その存在確率が，故障を引き起こす各々の原因の無条件存在確率の単純な掛け算として表現できない故障。 注記　二つの状態 A, B は，次のときにだけ従属である。 P（A かつ B）＞P(A)×P (B) 要は一つの故障状態がさらなる故障状態を引き起こす場合や，さらにその故障が他の故障状態の誘因となる場合のことをいう。
共通原因故障 **（common cause failure, CCF）** [IEC 61508-4, Cl.3.6.10]	一つ以上の事象を原因とする故障で，それが複数チャネル系の二つ以上の分離したチャネルそれぞれに故障を同時に引き起こし，システムの故障を生じさせるもの。 [ISO 13849-1, Cl.3.1.6]の定義 共通原因故障（common cause failure (CCF)） 単一の事象から生じる異なったアイテムの故障であって，これらの故障が互いの結果ではないもの。 （IEC 60050-191 Amd. 1 の 04-23 参照） 注記　共通原因故障は共通モード故障と混同してはならない。
故障率 **（failure rate）** [IEC 61508-4, Cl.3.6.16]	あるエンティティ（単一の部品又は系）の信頼性のパラメータ［λ(t)］。例えば，λ(t).dt は，［0, t］には故障が起きないとしたときに，［t, t＋dt］にこのエンティティの故障が起きる確率を示す。

表 1-64　（続き）機能安全に関する用語(主に機械安全分野でよく使用するもの)

用語	説明
単位時間当たりの時間平均危険側故障頻度（average frequency of a dangerous failure per hour, PFH） [IEC 61508-4 Cl.3.6.19]	指定する期間にわたって規定の安全機能を実行する E/E/PE 安全関連系の危険側故障の平均頻度。 注記 1 この規格群では，“単位時間当たりの危険側故障率”という用語を使わないが，略語 PFH は，“危険側故障の平均頻度［時間］”という意味で使われる場合のために残している。 注記 2 理論的な見地では，PFH は，無条件故障度の平均値であり，故障頻度とも呼ばれ，一般的に w(t)で表記する。故障率と混同しないほうがよい（IEC 61508-6:2010 の附属書 B 参照）。 注記 3 E/E/PE 安全関連系が最終の安全層である場合，PFH は不信頼度 F(T)＝1－R(t)（上記の“故障率”参照）から計算するのがよい。最終の安全関連系ではない場合，PFH はアンアベイラビリティ U(t)（上記の PFD 参照）から計算するのがよい。PFH の近似値は，最初の場合は F(T)/T 及び 1/MTTF，2 番目の場合は 1/MTBF で求める。 注記 4 E/E/PE 安全関連系が急速修理を受けた，明らかになった故障だけを明示する場合，漸近的故障率λasに急速に達する。これは，PFH の推定値を示す。

表 1-65　（続き）機能安全に関する用語(主に機械安全分野でよく使用するもの)

用語	説明
FMEA **(Failure Mode and Effects Analysis)** [JIS Z 8115, 192-11-05]	故障モード・影響解析 下位アイテムに生じ得る故障モード及びフォールト（故障状態）の調査，並びに様々な分割単位に及ぼすそれらの影響を含む定性的な解析方法。 注記 1 FMEA は，設計の不具合，潜在的な欠点などを抽出するために一覧表を用いて解析する。この一覧表を“FMEA 表”という。 注記 2 ハードウェア及びソフトウェアの機能の構造又は構成に着目して行う FMEA を“機能 FMEA”という。特に製品機能について設計段階で行う機能 FMEA を“設計 FMEA”という。また，作業プロセス又は製造工程で使用する設備の機能に着目して行う機能 FMEA を“設備 FMEA”という。 注記 3 作業システム又は管理システムを構成するプロセス機能に着目して行う FMEA を“プロセス FMEA”という。特に，製造工程に対して行うプロセス FMEA を“工程 FMEA”という。 注記 4 FMEA で取り上げる“故障”は，192-03-01 で定義する“故障”よりも広い意味で使われる。 すなわち，“要求された任務の遂行能力を失うこと”の意味で用いられ，故障，不具合，失敗など不都合な事象を全て対象とする。これによって，医療，教育，接客などのサービス業でも FMEA が使われる。 注記 5 附属書 JC～附属書 JE 参照。 注記 6 “fault mode and effects analysis”は，故障モード・影響解析の対応英語としては使用できない。 ⇒ 設計の潜在的問題点を見出すために構成要素の故障モードとその上位アイテムへの影響を解析する手法 参考規格 *IEC 60812 Failure modes and effects analysis (FMEA and FMECA)*

表 1-66　（続き）機能安全に関する用語(主に機械安全分野でよく使用するもの)

用語	説明
FMEDA **(Failure Modes, Effects and Diagnostic Analysis)**	FMEA に故障診断(Diagnostic)を加えたシステムの安全に係わる問題点を分析する手法の一つ。システムを要素に分解し，それぞれの故障モードごとに，安全側故障か危険側故障か，故障率，診断による故障検出率等を考慮し，システム全体での 診断率を算出する。
診断カバー率（DC） **（diagnostic coverage)** [IEC 61508-4, Cl.3.8.6]	自動的なオンライン診断テストによって検出される危険側故障の比率。危険側故障の比率は，検出された危険側故障に付随する危険側故障率を，総危険側故障率で除して計算する。 ※別欄の[ISO 13849-1, Cl.3.1.26]の定義 ”診断範囲，DC（diagnostic coverage）” にも注意。
診断テスト間隔 **（diagnostic test interval）** [IEC 61508-4, Cl.3.8.7]	安全関連系のフォールトを検出するために指定した診断範囲をもつオンラインテストを実施する時間間隔
安全関連系 **（safety-related system）** [IEC 61508-4, Cl.3.4.1]	次の両方を満足するシステム。 – EUC を安全な状態に移行させるため，又は EUC の安全な状態を維持するために必要な，要求された安全機能を行う。 – それ自体で，又はその他の E/E/PE 安全関連系及び他リスク軽減措置によって，要求される安全機能に対して必要な安全度を達成する。

表 1-67 （続き）機能安全に関する用語(主に機械安全分野でよく使用するもの)

用語	説明
サブシステム（subsystem） [IEC 61508-4, Cl.3.4.4]	安全関連系の最上位アーキテクチャ設計上の部分。当該部分は，3.6.7 a)による安全機能の危険側故障に帰着する。
要素（element） [IEC 61508-4, Cl.3.4.5]	一つ又は複数の要素安全機能を実行する，一つの部品又は部品の集まりを含んだサブシステムの部分（IEC 62061 の 3.2.6 修正）。 注記 1 要素はハードウェア及び／又はソフトウェアで構成してもよい。 注記 2 代表的な要素は，検出端（センサ），プログラマブルコントローラ，操作端である。
他リスク軽減措置（other risk reduction measure） [IEC 61508-4, Cl.3.4.2]	E/E/PE 安全関連系から分離，区分され，かつ，それらを用いないリスクを軽減又は緩和する措置。 例 逃がし弁（リリーフバルブ）は，他リスク軽減措置である。
安全ライフサイクル（safety lifecycle） [IEC 61508-4, Cl.3.7.1]	安全関連系の遂行上に必要な業務。プロジェクトの概念フェーズから出発して全ての E/E/PE 安全関連系及び他リスク軽減措置の必要性が終了するまでの期間に生じる。 注記 1 “機能安全ライフサイクル”が正確な用語であるが，この規格群では“機能”が付加されない。 注記 2 この規格群に使用される安全ライフサイクルモデルは，IEC 61508-1 の図 2，図 3 及び図 4 に指定している。
ソフトウェアライフサイクル（software lifecycle） [IEC 61508-4, Cl.3.7.2]	ソフトウェアが，着想されてから完全に廃棄されるまでの間に生じる業務。 注記 1 ソフトウェアライフサイクルは，典型的に，要求事項フェーズ，開発フェーズ，テストフェーズ，統合フェーズ，設置フェーズ及び部分改修フェーズを包含する。 注記 2 ソフトウェアは，保全できないので部分改修される。

表 1-68　（続き）機能安全に関する用語(主に機械安全分野でよく使用するもの)

用語	説明
構成管理（configuration management） [IEC 61508-4, Cl.3.7.3]	ライフサイクルを通じて，進展するシステム要素の変化を管理し，連続性及び追跡性を保持するために，そのような要素を同定するための規律。 注記 ソフトウェア構成管理の詳細については，IEC 61508-7:2010 の附属書 C の 5.24 参照。
影響解析（impact analysis） [IEC 61508-4, Cl.3.7.5]	あるシステムの機能又は要素の変化によって生じる，当該システムのその他の機能，要素又はその他のシステムへの影響を特定する業務。 注記 ソフトウェアに関しては，IEC 61508-7:2010 の附属書 C の 5.23 参照。
適合確認（verification） [IEC 61508-4, Cl.3.8.1]	要求事項が満足されていることを調査して客観的証拠を提示することによって確認する業務（ISO 8402 の 2.17 修正）。 注記 この規格群では，適合確認とは，関連する安全ライフサイクル（全 E/E/PE 系及びソフトウェア）の各フェーズで，解析，数学的推論及び／又はテストによって，特定の引継ぎ事項に対して，引渡し事項【Input：入力情報】が全ての観点から当該フェーズに関わる目的と要求事項との組合せ【Output：成果物】に対して適合していることを明示する業務【Process】である。例 適合確認業務は，次の事項を含む。 － あるフェーズへ引き継がれる特定の事項を考慮に入れ，引渡し事項（安全ライフサイクル全てのフェーズの文書）が，当該フェーズの目的及び要求事項に整合していることを保証するための審査。 － 設計審査。 － 設計された製品がその仕様に合致する性能をもつことを確認するためのテスト。 － システムの各々の部分が組み立てられる場所で段階的に実施され，それらの部分が指定したように協調して作動することを確認するための環境テストによる統合テスト。

表 1-69　（続き）機能安全に関する用語(主に機械安全分野でよく使用するもの)

用語	説明
妥当性確認 **（validation）** [IEC 61508-4, Cl.3.8.2]	仕様上に定めた使用法に関する特定の要求事項が満足されていることの審査，及び客観的な証拠の提供による確認［ISO 8402 の 2.18 修正］。 注記 1 この規格群では，次の三つの妥当性確認フェーズを取り扱う。 － 全安全妥当性確認（IEC 61508-1 の図 2 参照） － E/E/PE 系妥当性確認（IEC 61508-1 の図 3 参照） － ソフトウェア妥当性確認（IEC 61508-1 の図 4 参照） 注記 2 妥当性確認は，検討段階又は設置前後の安全関連系が全ての観点から安全要求仕様に適合していることを実証する業務である。そのため，例えば，ソフトウェア妥当性確認は，客観的な根拠を審査し提示することによって，当該ソフトウェアがソフトウェア安全要求仕様を満足することの確認を意味する。

表 1-70　（続き）機能安全に関する用語(主に機械安全分野でよく使用するもの)

用語	説明
プルーフテスト **（proof test）** [IEC 61508-4, Cl.3.8.5]	必要に応じて，修理によって新品又は実際上これに近い状態にシステムを修復することができるように，安全関連系の危険側隠れ故障状態を見付けるために実施する定期テスト。 注記 1 この規格群では，“プルーフテスト”という用語が使用されるが，“定期テスト”も同義語として認められる。 注記 2 プルーフテストの効果は，故障範囲及び修復実効性に依存している。実際上は，低複雑度 E/E/PE 安全関連系を除いて潜在した危険側故障を 100 %検出することは容易ではない。努力目標と考えるのがよい。 最小限，実施される全ての安全機能が，E/E/PE 系安全要求事項仕様に従って検査される。分離したチャネルが用いられている場合，それらのテストは，各々のチャネルごとに独立して実行される。 複雑な要素の場合は解析を行って，プルーフテストで検出されない隠れ危険側故障の確率が，E/E/PE 安全関連系の寿命期間全体にわたって無視できるものであることを実証する必要がある。 注記 3 プルーフテストの実施には，ある程度の時間が必要である。この期間，E/E/PE 安全関連系は，部分的又は全面的に禁止されてもよい。運転要求がある場合にテスト対象の E/E/PE 安全関連系の部分が利用可能なままであるときだけ，又はテスト中 EUC がシャットダウンされているときだけは，プルーフテストの期間を無視できる。 注記 4 プルーフテストの間，E/E/PE 安全関連系が，運転要求に対して部分的又は完全に応答しないことがある。EUC が修復中にシャットダウンされているときだけ，又は他リスク軽減措置が同等の実効性をもって実施されているときだけは，SIL の計算において MTTR を無視することができる。

表 1-71　（続き）機能安全に関する用語(主に機械安全分野でよく使用するもの)

用語	説明
アーキテクチャ，構造 architecture） [IEC 61508-4, Cl.3.3.4]	システムでのハードウェア及びソフトウェア要素の構成法。
制御システムの安全関連部，SRP/CS（safety-related parts of a control system） [ISO 13849-1, Cl.3.3.1]	安全関連入力信号に応答し，安全関連出力信号を生成する制御システムの部分。 注記 1 制御システムに組み合わされた安全関連部は，安全関連入力信号の発生するところ（例えば，位置スイッチの作用カム及びローラを含む。）で始まって，動力制御要素（例えば，接触器の主接点を含む。）の出力で終わる。 注記 2 監視システムが診断に使用される場合，これは SRP/CS と見なされる。
カテゴリ（category） [ISO 13849-1, Cl.3.1.2]	障害に対する抵抗性（フォールト・レジスタンス），及び障害条件下におけるその後の挙動に対する制御システムの安全関連部の特性に関する分類であって，当該部の構造的配置，障害検出及び／又はこれらの信頼性によって達成される。
システマティック故障（systematic failure） [ISO 13849-1, Cl.3.1.7]	何らかの原因に確定的に関係する故障であって，設計，製造プロセス，運転手順，文書又は他の関連要因を変更しなければ除去できない故障。 注記 1 変更を伴わない修理では，通常，システマティック故障の原因を除去できない。 注記 2 故障原因をシミュレートすることによって，システマティック故障を再現することができる。 （IEC 60050-191 の 04-19 参照） 注記 3 システマティック故障の原因の事例には，次の段階で起こす人間の過誤を含む。 – 安全要求仕様 – ハードウェアの設計，製造，据付及び運転 – ソフトウェアの設計，実装など

表 1-72　（続き）機能安全に関する用語(主に機械安全分野でよく使用するもの)

用語	説明
監視（monitoring） [ISO 13849-1, Cl.3.1.21]	コンポーネント又は要素の機能を実行する能力が低下する場合，又はリスク低減機能の低下を招くような方向でプロセス条件が変化する場合，保護方策の始動を確実にする安全機能。 監視も安全機能の一つということである。
制御システムの安全関連部，SRP/CS（safety-related parts of a control system） [ISO 13849-1, Cl.3.1.1]	安全関連入力信号に応答し，安全関連出力信号を生成する制御システムの部分。 注記 1 制御システムに組み合わされた安全関連部は，安全関連入力信号の発生するところ（例えば，位置スイッチの作用カム及びローラを含む。）で始まって，動力制御要素（例えば，接触器の主接点を含む。）の出力で終わる。 注記 2 監視システムが診断に使用される場合，これは SRP/CS と見做される。装置のようなシステムの全ての要素を含む。
パフォーマンスレベル，PL（performance level） [ISO 13849-1, Cl.3.1.23]	予見可能な条件下で，安全機能を実行するための制御システムの安全関連部の能力を規定するために用いられる区分レベル。
平均危険側故障時間，MTTFd（mean time to dangerous failure） [ISO 13849-1, Cl.3.1.25]	危険側故障を生じるまでの平均時間の期待値。 （IEC 62061 の 3.2.34 から採用）

表 1-73　（続き）機能安全に関する用語(主に機械安全分野でよく使用するもの)

用語	説明
診断範囲，DC **（diagnostic coverage）** [ISO 13849-1, Cl.3.1.26]	診断効果の尺度であり，検出される危険側故障率（分子）と全危険側故障率（分母）の間の比として決定することができる。 注記　診断範囲は，安全関連システムの全体又は一部に対してあり得る。例えば，診断範囲は，安全関連部の全体又は一部として，例えば，センサ及び／又は論理システム及び／又は最終要素の組合せとして存在することがあり得る。 （IEC 61508-4 の 3.8.6 から採用）

付録D 関連・参考規格リスト

本ガイダンス文書で使用する関連規格を表形式にてまとめる。

注記：　国際規格をメインとし，対応する JIS 規格があれば記載する。

(ア)　安全原則に関するガイド

表 1-74　安全原則に関するガイド

規格番号	タイトル	対応する JIS 規格	タイトル
ISO/IEC Guide 51:2014	Safety aspects - Guidelines for their inclusion in standards	JIS Z 8051:2015	安全側面―規格への導入指針
ISO/IEC Guide 63:2019	Guide to the development and inclusion of safety aspects in International Standards for medical devices	JIS T 0063:2020	医療機器規格における安全側面の開発及び導入の指針
ISO/IEC Guide 71:2014	Guidelines for standards developers to address the needs of older persons and persons with disabilities	JIS Z 8071:2017	規格におけるアクセシビリティ配慮のための指針
ISO/IEC Guide 73:2009	Risk management — Vocabulary	JIS Q 0073:2010	リスクマネジメント－用語

(イ)　福祉機器関連規格(ISO TC173)

表 1-75 福祉機器関連規格

規格番号	タイトル	対応する JIS 規格	タイトル
ISO 21856 **（草案）**	Assistive products— General requirements and test methods (福祉機器－通則 一般要求と試験方法) ※尚，このガイダンスは作成時点(2021 年 1 月)の最新バージョン：ISO DIS 21856 に対応している。	–	
ISO 10535:2006	Hoists for the transfer of disabled persons — Requirements and test methods	–	
ISO 17966:2016	Assistive products for personal hygiene that support users — Requirements and test methods (個人衛生用支援機器)	–	
ISO 11199-1:1999	Walking aids manipulated by both arms — Requirements and test methods — Part 1: Walking frames (歩行車／ワーキングフレーム型)	–	
ISO 11199-2:2005	Walking aids manipulated by both arms — Requirements and test methods — Part 2: Rollators (歩行車／ロレータ型)	–	
ISO 11199-3:2005	Walking aids manipulated by both arms — Requirements and test methods — Part 3: Walking tables (歩行車／ワーキングテーブル型)	–	

表 1-76 （続き）福祉機器関連規格

規格番号	タイトル	対応する JIS 規格	タイトル
ISO 19894:2019	Walking trolleys — Requirements and test methods (シルバーカー)	–	
ISO 11334-1:2007	Assistive products for walking manipulated by one arm — Requirements and test methods — Part 1: Elbow crutches	–	
ISO 11334-4:1999	Walking aids manipulated by one arm — Requirements and test methods — Part 4: Walking sticks with three or more legs	–	
ISO/TR 11548-1:2001	Communication aids for blind persons — Identifiers, names and assignation to coded character sets for 8-dot Braille characters — Part 1: General guidelines for Braille identifiers and shift marks	–	
ISO/TR 11548-2:2001	Communication aids for blind persons — Identifiers, names and assignation to coded character sets for 8-dot Braille characters — Part 2: Latin alphabet based character sets	–	
ISO 16201:2006	Technical aids for persons with disability — Environmental control systems for daily living	–	

表 1-77 （続き）福祉機器関連規格

規格番号	タイトル	対応する JIS 規格	タイトル
ISO 20342-1:2019	Assistive products for tissue integrity when lying down — Part 1: General requirements (全身床ずれ防止用具等)	–	
ISO 21802:2019	Assistive products — Guidelines on cognitive accessibility — Daily time management (認知症に関するアクセシビリティ)	–	
ISO 23599:2019	Assistive products for blind and vision-impaired persons — Tactile walking surface indicators	–	
ISO 23600:2007	Assistive products for persons with vision impairments and persons with vision and hearing impairments — Acoustic and tactile signals for pedestrian traffic lights	–	
ISO 24415-1:2009	Tips for assistive products for walking — Requirements and test methods — Part 1: Friction of tips	–	
ISO 24415-2:2011	Tips for assistive products for walking — Requirements and test methods — Part 2: Durability of tips for crutches	–	
ISO 7176-1:2014	Wheelchairs — Part 1: Determination of static stability	–	

表 1-78 （続き）福祉機器関連規格

規格番号	タイトル	対応する JIS 規格	タイトル
ISO 7176-2:2017	Wheelchairs — Part 2: Determination of dynamic stability of electrically powered wheelchairs	–	
ISO 7176-3:2012	Wheelchairs — Part 3: Determination of effectiveness of brakes	–	
ISO 7176-4:2008	Wheelchairs — Part 4: Energy consumption of electric wheelchairs and scooters for determination of theoretical distance range	–	
ISO 7176-5:2008	Wheelchairs — Part 5: Determination of dimensions, mass and manoeuvring space	–	
ISO 7176-6:2018	Wheelchairs — Part 6: Determination of maximum speed of electrically powered wheelchairs	–	
ISO 7176-7:1998	Wheelchairs — Part 7: Measurement of seating and wheel dimensions	–	
ISO 7176-8:2014	Wheelchairs — Part 8: Requirements and test methods for static, impact and fatigue strengths	–	
ISO 7176-9:2009	Wheelchairs — Part 9: Climatic tests for electric wheelchairs	–	

表 1-79 （続き）福祉機器関連規格

規格番号	タイトル	対応する JIS 規格	タイトル
ISO 7176-10:2008	Wheelchairs — Part 10: Determination of obstacle-climbing ability of electrically powered wheelchairs	–	
ISO 7176-11:2012	Wheelchairs — Part 11: Test dummies	–	
ISO 7176-13:1989	Wheelchairs — Part 13: Determination of coefficient of friction of test surfaces	–	
ISO 7176-14:2008	Wheelchairs — Part 14: Power and control systems for electrically powered wheelchairs and scooters — Requirements and test methods	–	
ISO 7176-14:2008	Wheelchairs — Part 14: Power and control systems for electrically powered wheelchairs and scooters — Requirements and test methods	–	
ISO 7176-15:1996	Wheelchairs — Part 15: Requirements for information disclosure, documentation and labelling	–	
ISO 7176-16:2012	Wheelchairs — Part 16: Resistance to ignition of postural support devices	–	

1-80　（続き）福祉機器関連規格

規格番号	タイトル	対応する JIS 規格	タイトル
ISO 7176-19:2008	Wheelchairs — Part 19: Wheeled mobility devices for use as seats in motor vehicles — Amendment 1: Annex G	–	
ISO 7176-21:2009	Wheelchairs — Part 21: Requirements and test methods for electromagnetic compatibility of electrically powered wheelchairs and scooters, and battery chargers	–	
ISO 7176-22:2014	Wheelchairs — Part 22: Set-up procedures	–	
ISO 7176-25:2013	Wheelchairs — Part 25: Batteries and chargers for powered wheelchairs	–	
ISO 7176-26:2007	Wheelchairs — Part 26: Vocabulary	–	
ISO 7176-28:2012	Wheelchairs — Part 28: Requirements and test methods for stair-climbing devices	–	
ISO 7176-30:2018	Wheelchairs — Part 30: Wheelchairs for changing occupant posture — Test methods and requirements	–	

1-81　（続き）福祉機器関連規格

規格番号	タイトル	対応する JIS 規格	タイトル
ISO/TR 13570-1:2005	Wheelchairs — Part 1: Guidelines for the application of the ISO 7176 series on wheelchairs	–	
ISO/TR 13570-2:2014	Wheelchairs — Part 2: Typical values and recommended limits of dimensions, mass and manoeuvring space as determined in ISO 7176-5	–	
ISO/TR 13570-1:2005	Wheelchairs — Part 1: Guidelines for the application of the ISO 7176 series on wheelchairs	–	
ISO 16840-1:2006	Wheelchair seating — Part 1: Vocabulary, reference axis convention and measures for body segments, posture and postural support surfaces	–	
ISO 16840-2:2018	Wheelchair seating — Part 2: Determination of physical and mechanical characteristics of seat cushions intended to manage tissue integrity	–	

1-82　（続き）福祉機器関連規格

規格番号	タイトル	対応する JIS 規格	タイトル
ISO 16840-3:2014	Wheelchair seating — Part 3: Determination of static, impact and repetitive load strengths for postural support devices	–	
ISO 16840-4:2009	Wheelchair seating — Part 4: Seating systems for use in motor vehicles	–	
ISO 16840-6:2015	Wheelchair seating — Part 6: Simulated use and determination of the changes in properties of seat cushions	–	
ISO/TR 16840-9:2015	Wheelchair seating — Part 9: Clinical interface pressure mapping guidelines for seating	–	
ISO 16840-10:2014	Wheelchairs — Resistance to ignition of non-integrated seat and back support cushions — Part 10: Requirements and test methods	–	
ISO/TS 16840-11:2014	Wheelchair seating — Part 11: Determination of perspiration dissipation characteristics of seat cushions intended to manage tissue integrity	–	

1-83　（続き）福祉機器関連規格

規格番号	タイトル	対応する JIS 規格	タイトル
ISO/TS 16840-12:2015	Wheelchair seating — Part 12: Apparatus and method for cushion envelopment testing	–	

(ウ)　リスクマネジメント・リスクアセスメント関連の規格

表 1-84 リスクマネジメント・リスクアセスメント関連の規格

規格番号	タイトル	対応する JIS 規格	タイトル
ISO 14971:2019	Medical devices -- Application of risk management to medical devices ※尚，このガイダンスは，第 3 章作成時点(2019 年 1 月)の最新バージョン：ISO 14971:2007 に対応している。	JIS T 14971:2020	医療機器－医療機器へのリスクマネジメントの適用
ISO 31000:2018	Risk management — Guidelines	JIS Q 31000:2019	リスクマネジメント－指針
IEC 31010:2019	Risk management — Risk assessment techniques	JIS Q 31010:2012	リスクマネジメント－ リスクアセスメント技法 ※国際規格 IEC/ISO 31010:2009 と IDT（技術的内容一致）であり、左欄のとはバージョンの差異あり。

備考： ISO 12100:2010 ／ JIS B 9700: 2013 「機械類の安全性 －設計のための一般原則－リスクアセスメント及びリスク低減」は

(エ)　機械安全に関する規格（ISO TC199)

表 1-92 に記載。

(オ)　医療機器(医用電気機器) 関連の規格

表 1-85 医療機器(医用電気機器)関連の規格

規格番号	タイトル	対応する JIS 規格	タイトル
IEC 60601-1/ A2:2020	Medical electrical equipment -- Part 1: General requirements for basic safety and essential performance ※尚，このガイダンスは，ISO DIS 21856 が箇条 2 で指定するバージョン：IEC 60601-1/A1:2012 に対応している。	JIS T0601-1:2017	医用電気機器 - 第一部：安全に関する一般的要求事項 ※国際規格 IEC 60601-1:A1:2012 と IDT（技術的内容一致）であり、左欄とはバージョンの差異あり。
IEC 60601-1-2:2014	Medical electrical equipment - Part 1-2: General requirements for basic safety and essential performance - Collateral Standard: Electromagnetic disturbances - Requirements and tests	JIS T0601-1-2:2018	医用電気機器 - 第一部：安全に関する一般的要求事項 - 第二節：副通則 - 電磁両立性 - 要求事項及び試験
IEC TR 60601-4-1:2017	Medical electrical equipment –Part 4-1: Guidance and interpretation – Medical electrical equipment and medical electrical systems employing a degree of autonomy	–	
IEC 60601-2-52:2009/A1:2015	Medical electrical equipment — Part 2-52: Particular requirements for the basic safety and essential performance of medical beds — Amendment 1	–	

表 1-86　（続き）医療機器(医用電気機器)関連の規格

規格番号	タイトル	対応する JIS 規格	タイトル
IEC 80601-2-78:2019	Medical electrical equipment –Part 2-78: Particular requirements for basic safety and essential performance of medical robots for rehabilitation, assessment, compensation or alleviation	–	
IEC 62304/2006 A1:2015	Medical device software－Software life cycle processes ※尚，このガイダンスは，第 5 章作成時点(2019 年 1 月)の最新バージョン：IEC 62304/A1:2015 に対応している。	JIS T 2304:2017(IDT)	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
IEC 82304-1:2016	Health software－Part 1: General requirements for product safety	JIS T 82304-1:2018	ヘルスソフトウェア－第 1 部：製品安全に関する一般要求事項
IEC 80001-1:2010	Application of risk management for IT-networks incorporating medical devices-Part1: Roles, responsibilities and activities 医療機器に結合する IT ネットワークへのリスクマネジメントの適用	–	

表 1-87　（続き）医療機器(医用電気機器)関連の規格

規格番号	タイトル	対応する JIS 規格	タイトル
IEC/TR 80002-1:2009	Medical devices software - Part:1 Guidance on the application of ISO 14971 to medical device software 医療機器ソフトウェア-第一部：医療機器ソフトウェアへの ISO14971 の適用の手引き	–	
ISO/TR 80002-2:2017	Medical devices software - Part 2: Validation of software for medical device quality systems 医療機器ソフトウェア-第二部：医療機器の品質システムで使用するソフトウェアのバリデーション	–	
IEC 62366-1:2015	Medical devices -- Part 1: Application of usability engineering to medical devices	JIS T 62366-1:2019	医療機器―第 1 部：ユーザビリティエンジニアリングの医療機器への適用
ISO 10993-1:2018	Biological evaluation of medical devices — Part 1: Evaluation and testing within a risk management process	JIS T 0993-1:2020	医療機器の生物学的評価 - 第 1 部：リスクマネジメントプロセスにおける評価及び試験

(カ)　システム・ソフトウェア関連の規格

表 1-88 システム・ソフトウェア関連の規格

規格番号	タイトル	対応する JIS 規格	タイトル
ISO/IEC/IEEE 12207:2017	Systems and software engineering – Software life cycle processes	JIS X 0160:2021	ソフトウェアライフサイクルプロセス
ISO/IEC/IEEE 90003:2018	Software engineering -- Guidelines for the application of ISO 9001:2015 to computer software ソフトウェア工学－コンピュータソフトウェアへの ISO9001:2015 の適用の指針	–	
ISO/IEC 15288:2015	Systems and software engineering-System life cycle processes	JIS X 0170:2020	システムライフサイクルプロセス
ISO/IEC/IEEE 24765:2017	Systems and software engineering - Vocabulary	–	
ISO/IEC 25010:2011	Systems and software engineering-Systems and software Quality Requirements and Evaluation (SQuaRE)-System and software quality models	JIS X 25010:2013	システム及びソフトウェア製品の品質要求及び評価（SQuaRE）－システム及びソフトウェア品質モデル

(キ)　品質マネジメントシステム関連の規格

表 1-89 品質マネジメントシステム関連の規格

規格番号	タイトル	対応する JIS 規格	タイトル
ISO 13485:2016	Medical devices -- Quality management systems -- Requirements for regulatory purposes	JIS Q 13485:2018	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
ISO 9000:2015	Quality management systems- Fundamentals and vocabulary	JIS Q 9000 : 2015	品質マネジメントシステム－基本及び用語
ISO 9001:2015	Quality management systems -- Requirements	JIS Q 9001:2015	品質マネジメントシステム－要求事項

(ク)　ロボット関連の規格

表 1-90 ロボット関連規格

規格番号	タイトル	対応する JIS 規格	タイトル
ISO 8373:2012	Robots and robotic devices — Vocabulary	JIS B 0134:2015	ロボット及び**ロボティックデバイス**−用語
ISO 13482:2014	Robots and robotic devices - Safety requirements for personal care robots	JIS B 8445:2016	ロボット及び**ロボティックデバイス**− 生活支援ロボットの安全要求事項
-		JIS B 8446-1 : 2016	生活支援ロボットの安全要求事項− 第 1 部：マニピュレータを備えない 静的安定移動作業型ロボット
-		JIS B 8446-2 : 2016	生活支援ロボットの安全要求事項−第 2 部：低出力装着型身体アシストロボット
-		JIS B 8446-3 : 2016	生活支援ロボットの安全要求事項−第 3 部：倒立振子制御式搭乗型ロボット
-		JIS B 8456-1:2017	生活支援ロボット−第 1 部：腰補助用装着型身体アシストロボット
ISO/TR 23482-1:2020	Robotics — Application of ISO 13482 — Part 1: Safety-related test methods	−	
ISO/TR 23482-2:2019	Robotics — Application of ISO 13482 — Part 2: Application guidelines	−	
ISO 10218-1:2011	Robots and robotic devices−Safety requirements for industrial robots −Part 1: Robots	JIS B 8433-1:2015	ロボット及び**ロボティックデバイス−産業用ロボット**のための安全要求事項−第 1 部：ロボット

表 1-91　（続き）ロボット関連規格

規格番号	タイトル	対応する JIS 規格	タイトル
ISO 10218-2:2011	Robots and robotic devices－Safety requirements for industrial robots　－Part 2: Robot systems and integration	JIS B 8433-2:2015	ロボット及び**ロボティックデバイス－産業用ロボット**のための安全要求事項－第 2 部：ロボットシステム及びインテグレーション
ISO/TS 15066:2016	Robots and robotic devices - Collaborative robots	TS B 0033:2017	ロボット及び**ロボティックデバイス－**協働ロボット

(ケ)　機械安全に関する規格（ISO TC199)

表 1-92 機械安全に関する規格

規格番号	タイトル	対応する JIS 規格	タイトル
ISO 12100:2010	Safety of machinery - General principles for design - Risk assessment and risk reduction	JIS B 9700: 2013	機械類の安全性 －設計のための一般原則－リスクアセスメント及びリスク低減
ISO/TR 14121-2:2012	Safety of machinery — Risk assessment — Part 2: Practical guidance and examples of methods		
ISO 13849-1 : 2015	Safety of machinery -- Safety-related parts of control systems -- Part 1: General principles for design	JIS B 9705-1:2019	機械類の安全性 - **制御システム**の安全関連部 - 第 1 部：設計のための一般原則
ISO 13849-2:2012	Safety of machinery -- Safety-related parts of control systems -- Part 2: Validation	JIS B 9705-2:2019	機械類の安全性 - **制御システム**の安全関連部 - 第 2 部：
ISO 13854:2017	Safety of machinery -- Minimum gaps to avoid crushing of parts of the human body		
ISO 14119 : 2013	Safety of machinery-Interlocking devices associated with guards- Principles for design and selection	JIS B 9710:2019	機械類の安全性－ガードと共同するインタロック装置－設計及び選択のための原則
ISO 14118:2017	Safety of machinery -- Prevention of unexpected start-up		

表 1-93　（続き）機械安全に関する規格

規格番号	タイトル	対応する JIS 規格	タイトル
ISO 13855:2010	Safety of machinery-Positioning of safeguards with respect to the approach speeds of parts of the human body	JIS B 9715:2013	機械類の安全性－人体部位の接近速度に基づく保護設備の位置決め
IEC 60204-1:2016	Safety of machinery -- Electrical equipment of machines -- Part 1: General requirements	JIS B 9960-1:2019	機械類の安全性－機械の電気装置－第 1 部：一般要求事項

(コ)機能安全に関する規格

表 1-94 機能安全に関する規格

規格番号	タイトル	対応する JIS 規格	タイトル
IEC 61508-1:2010	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1: General requirements	JIS C 0508-1:2012	電気・電子・プログラマブル電子安全関連系の機能安全－第 1 部：一般要求事項
IEC 61508-2:2010	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems	JIS C 0508-2:2014	電気・電子・プログラマブル電子 安全関連系の機能安全－第 2 部：電気・電子・プログラマブル電子安全関連系に対する要求事項
IEC 61508-3:2010	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 3: Software requirements	JIS C 0508-3:2014	電気・電子・プログラマブル電子安全関連系の機能安全－第 3 部：ソフトウェア要求事項
IEC 61508-4:2010	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 4: Definitions and abbreviations	JIS C 0508-4:2012	電気・電子・プログラマブル電子安全関連系の機能安全－第 4 部：用語の定義及び略語

表 1-95　（続き）機能安全に関する規格

規格番号	タイトル	対応する JIS 規格	タイトル
IEC 61508-5：2010	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 5: Examples of methods for the determination of safety integrity levels	JIS C 0508-5：2019	電気・電子・プログラマブル電子安全関連系の機能安全－第 5 部：安全水準決定方法の事例
IEC 61508-6:2010	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3	JIS C 0508-6:2019	電気・電子・プログラマブル電子安全関連系の機能安全－第 6 部：第 2 部及び第 3 部の適用指針
IEC 61508-7:2010	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 7: Overview of techniques and measures	JIS C 0508-7:2017	電気・電子・プログラマブル電子安全関連系の機能安全－第 7 部：技術及び手法の概観
ISO/IEC 2382:2015	Information technology - Vocabulary		
IEC 60812:2018	Failure modes and effects analysis (FMEA and FMECA)		

表 1-96　（続き）機能安全に関する規格

規格番号	タイトル	対応する JIS 規格	タイトル
JIS Z 8115：2019	ディペンダビリティ（総合信頼性）用語		
SN 29500	Components, failure rate, expected value, reliability	–	
IEC 61709:2017	Electric components - Reliability - Reference conditions for failure rates and stress models for conversion	–	

参考文献

[1] ロボット介護機器開発のための安全ハンドブック リスクアセスメントの基礎と RA シートひな形説明（安衛研）AMED ロボット介護機器開発・導入促進事業 基準策定評価コンソーシアム

[2] ISO 21856 （草案） Assistive products — General requirements and test methods

[3] ISO 14971 Medical devices -- Application of risk management to medical devices

[4] IEC 60601-1 Medical electrical equipment -- Part 1: General requirements for basic safety and essential performance

[5] IEC 60601-1-2 Medical electrical equipment - Part 1-2: General requirements for basic safety and essential performance - Collateral Standard: Electromagnetic disturbances - Requirements and tests

[6] IEC 62304 Medical device software－Software life cycle processes

[7] IEC 80601-2-78:2019 Medical electrical equipment –Part 2-78: Particular requirements for basic safety and essential performance of medical robots for rehabilitation, assessment, compensation or alleviation

[8] IEC TR 60601-4-1:2017 Medical electrical equipment –Part 4-1: Guidance and interpretation – Medical electrical equipment and medical electrical systems employing a degree of autonomy

[9] ISO 10535:2006 Hoists for the transfer of disabled persons — Requirements and test methods

[10] ISO 17966:2016 Assistive products for personal hygiene that support users — Requirements and test methods

[11] ISO 7176-6:2018 Wheelchairs — Part 6: Determination of maximum speed of electrically powered wheelchairs

[12] ISO/IEC Guide 51:2014 Safety aspects - Guidelines for their inclusion in standards

[13] ISO/IEC Guide 73:2009 Risk management — Vocabulary

[14] ISO 14971:2019 Medical devices -- Application of risk management to medical devices

[15] ISO 31000:2018 Risk management — Guidelines

[16] IEC 31010:2019 Risk management — Risk assessment techniques

[17] ISO 13485:2016 Medical devices -- Quality management systems -- Requirements for regulatory purposes

[18] ISO 9001:2015 Quality management systems -- Requirements

[19] ISO 8373:2012 Robots and robotic devices — Vocabulary

[20] ISO 13482:2014 Robots and robotic devices - Safety requirements for personal care robots

[21] JIS B 8446-1：2016 生活支援**ロボット**の**安全**要求事項－第 1 部：マニピュレータを備えない静的安定移動作業型**ロボット**

[22] JIS B 8446-2：2016 生活支援**ロボット**の**安全**要求事項－第 2 部：低出力装着型身体アシスト**ロボット**

[23] JIS B 8446-3：2016 生活支援**ロボット**の**安全**要求事項－第 3 部：倒立振子制御式搭乗型**ロボット**

[24] JIS B 8456-1:2017 生活支援**ロボット－**第 1 部：腰補助用装着型身体アシスト**ロボット**

[25] ISO 12100:2010 Safety of machinery - General principles for design - Risk assessment and risk reduction

[26] ISO/TR 14121-2:2012 Safety of machinery — Risk assessment — Part 2: Practical guidance and examples of methods

[27] ISO 13849-1 : 2015 Safety of machinery -- Safety-related parts of control systems -- Part 1: General principles for design

[28] IEC 61508-1:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1: General requirements

[29] ISO/IEC/IEEE 12207:2017 Systems and software engineering −Software life cycle processes

[30] ISO/IEC/IEEE 90003:2018 Software engineering -- Guidelines for the application of ISO 9001:2015 to computer software

[31] ISO/IEC 15288:2015 Systems and software engineering-System life cycle processes

[32] IEEE 610.12:1990 IEEE Standard Glossary of Software Engineering Terminology

[33] ISO/IEC/IEEE 24765:2017 Systems and software engineering - Vocabulary

[34] ISO/IEC 25010:2011 Systems and software engineering-Systems and software Quality Requirements and Evaluation (SQuaRE)-System and software quality models

[35] IEC 82304-1:2016 Health software－Part 1: General requirements for product safety

[36] IEC 80001-1:2010 Application of risk management for IT-networks

incorporating medical devices- Part1: Roles, responsibilities and activities

[37] IEC/TR 80002-1:2009 Medical devices software - Part:1 Guidance on the application of ISO 14971 to medical device software

[38] IEC 62366-1:2015 Medical devices -- Part 1: Application of usability engineering to medical devices

[39] REGULATION (EU) 2017/745 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC（欧州**医療機器**規則（Medical Device Regulation））

[40] MANUAL ON BORDERLINE AND CLASSIFICATION IN THE COMMUNITY REGULATORY FRAMEWORK FOR MEDICAL DEVICES

[41] MEDICAL DEVICES: Guidance document (MEDDEV 2.4/1 Rev.9) Classification of medical devices

[42] 産業タイムズ社 **ロボット**産業最前線 2019

[43] 一般社団法人電子情報技術産業協会(JEITA) **医療機器**用電子部品の**信頼性**ガイド

[44] 一般社団法人電子情報技術産業協会(JEITA) 電子部品部会電子部品の **FMEA** 実施ガイド

[45] 一般財団法人 日本電子部品**信頼性**センター 平成２７年度 **機能安全**規格の動向及び電子部品**故障率**モデルの IEC/TR 62380、FIDES 及び 217Plus を用いた**故障率**算出例と比較

[46] 松本吉弘（訳）「ソフトウェアエンジニアリング基礎知識体系 - SWEBOK V3.0 - 」オーム社，2014 年

[47] SQuBOK 策定部会（編）「ソフトウェア品質知識体系ガイド - SQuBOK Guide V2 - 」オーム社，2014 年

[48] 一般社団法人 電子情報技術産業協会 ヘルスケアインダストリ事業委員会／医療用ソフトウェア専門委員会（著）「IEC 62304 実践ガイドブック」じほう，2016 年

[49] 経営情報研究会（著）「図解でわかる ソフトウェア開発のすべて」日本実業出版社，2000 年

[50] 宇宙航空研究開発機構（著）「IV&V ガイドブック【虎の巻】」宇宙航空研究開発機構，2013 年，URL: https://jaxa.repo.nii.ac.jp/?action=pages_view_main&active_action=repository_view_main_item_detail&item_id=4174&item_no=1&page_id=13&block_id=21

[51] JaSST Kansai 実行委員会（著）「大阪電気やかん 要求仕様書」JaSST Kansai 実行委員会，2012 年，URL: http://jasst.jp/symposium/jasst12kansai/pdf/A2-7.pdf

[52] Sakai WEB サイト「Embedded Software Manufactory」URL:

https://embeddedsoftwaremanufactory.blogspot.com/

[53] 「はじめての STAMP/STPA Ver.1.0 」発行 独立行政法人 情報処理推進機構（IPA), 2016 年

[54] 組込みソフトウェア開発のための構造化モデリング 翔泳社，2006 年

[55] 一般社団法人電子情報技術産業協会(JEITA) 参考和訳 EN 62304 2006 の実施におけるよくある質問（MDD 93/42/EEC 関連

[56] 【改訂版】組込みソフトウェア開発向け コーディング作法ガイド［C 言語版］ESCR Ver. 3.0 独立行政法人情報処理推進機構 2018 年

[57] 組込みソフトウェア向け プロジェクトマネジメントガイド［計画書編］（ESMR Ver 1.0 : Embedded System development Management Reference）