附属書 E
（参考情報）

セーフティケース

セーフティケースとは、「医療機器が所与の動作環境における所与の意図する使用について安全であることの説得力のある、分かりやすい、正当な事例を提供する一連の証拠によって裏付けられた、構造化された論拠」をいう (UK MoD Def Stan 00-56 から一部修正)。

セーフティケースという概念は軍用システム、海底石油採掘産業、鉄道輸送、及び原子力産業では広く知られているが、医療機器産業ではこの手法は必須ではなく、またこの附属書で ISO 14971 を超える要求事項を追加することを意図するものでもない。

この技術報告書では、セーフティケースが医療機器の十分なレベルの安全性の証明を構造化し、文書化し、伝達する手段となりえる、ということを提案するものである。セーフティケースはまた、医療機器の全寿命を通して安全性が維持されることを保証する手助けにもなりえる。

セーフティケースは、リスクマネジメントプロセスの結果を使用して、ソフトウェアが意図する使用のために十分に安全である理由、及びすべての当該規制当局の要求事項を満たす（そして当該規制当局の用語において満たすことができる）理由を明確に示す。

セーフティケースは、リスクマネジメントファイル内の情報や証拠を裏付けるより詳細な文書記録への参照表記が付いた、リスクマネジメント又は残留リスクの要約としてとらえることもできる。また、セーフティケースには、すべてのリスクコントロール手段に関する仕様及び試験範囲を示すクロスリファレンスを含めることもできる。

セーフティケースを構築するには、次の段階が必要である。

- システムについての明示的な主張
- 根拠となる証拠の提供
- 主張を証拠に結びつける安全性の論拠
- その論拠の基礎となる仮定及び判断
- 異なる観点及び詳細レベルの容認

セーフティケースには以下の主要な要素がある。

- 主張：システム又は一部のサブシステムの特性についての主張
- 証拠：安全性論拠の根拠として使用される証拠。これは事実（例：既に立証されている科学原理及び事前研究に基づいた事実）、又は下位レベルの下位論拠から導き出された仮定又は下位主張。
- 論拠：証拠を主張に結びつけること。確定的、確率的、又は定量的なもの。
- 推論：論拠に変形規則を与えるメカニズム。

セーフティケースの要素及び構成の詳細については、*A Methodology for Safety Case Development* (セーフティケース開発のための方法論) [9] を参照のこと。

セーフティケース及び目標構造化の表記法に関する概要は、*Systematic Approach to Safety Case Management* (セーフティケースマネージメントに対する系統的アプローチ) [10] 及び *The Goal Structuring Notation – A Safety Argument Notation* (目標構造化の表記法 - 安全性論拠の表記法) [11]. のふたつの論文を参考にするとよい。

参考文献

注記 : 合同作業グループは、掲載する技術的参考文献の内容を保証するものではない。これらの文献は、ISO 14971の要求事項を医療機器ソフトウェアへ適用するための指針に関連する追加的情報を提供するものとして提示している。

[1] ISO 13485 医療機器の品質マネジメントシステム－規制目的に関する要求事項 (ISO 13485, Medical devices – Quality management systems – Requirements for regulatory purposes)

[2] IEC 60812 システム信頼性のための解析手法－故障モード影響解析 (FMEA) の手順 (IEC 60812, Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA))

[3] IEC 61025 フォルトツリー解析 (FTA) (IEC 61025, Fault tree analysis (FTA))

[4] IEC 61882 ハザード及び操作性の研究 (HAZOP の研究) －応用ガイド (IEC 61882, Hazard and operability studies (HAZOP studies) – Application guide)

[5] IEC 62366 医療機器－ユーザビリティエンジニアリングの医療機器への適用 (IEC 62366, Medical devices – Application of usability engineering to medical devices)

[6] IEC 80001-1[2], リスクマネジメントの医療機器を組込んだ情報技術 (IT) ネットワークへの適用－第 1 部：役割、責任及び活動 (IEC 80001-12), Application of risk management to information technology (IT) networks incorporating medical devices – Part 1: Roles, responsibilities and activities)

[7] Pullum, L. ソフトウェアフォールトトレラント手法とその実装 *(Software fault tolerant techniques and implementation)*. Boston: Artech House, 2001

[8] Banatre, M., Lee, P. フォールトトレランスのためのハードウェア及びソフトウェアのアーキテクチャ：経験と展望 (Hardware and Software Architectures for Fault Tolerance: Experiences and Perspectives) Berlin, Germany: Springer-Verlag

[9] BISHOP, P., BLOOMFIELD, R. (1998), セーフティケース開発のための方法論 (*A Methodology for Safety Case Development*). Safety-Critical Systems Symposium
http://www.adelard.co.uk/resources/papers/pdf/sss98web.pdf

[10] KELLY, T. P., セーフティケースマネージメントに対する系統的アプローチ (*Systematic Approach to Safety Case Management*). Proceedings of SAE 2004 World Congress, Detroit, March 2004 (Proceedings published by the Society for Automotive Engineers)

[11] WEAVER, R. A., KELLY, T. P., 目標構造化の表記法 - 安全性論拠の表記法 (*The Goal Structuring Notation – A Safety Argument Notation*). Proceedings of the Dependable Systems and Networks 2004 Workshop on Assurance Cases, July 2004

2) 近日発行予定

完全な system validation 及び Part 11 に関する最近の FDA Warning Letter から学ぶこと

三浦

表題の CD は FDA が作成した e-learning 用教材であり、40 枚以上の slide で構成されている。Ludwig Huber 氏が slide 毎に音声で解説している。概要を次に示す。

1.教材の源

この教材は、2003 年以降に FDA が software に対する査察（FDA は監査（audit）ではなく査察（inspection）と云う）を通じて企業に発行した 483 通の "Warning Letter" を分析して作成したものである。①目次、②前書き、③Warning Letter の内容（指摘事項）及び、それらの分析に基づく推奨事項、④以上のまとめから構成されている。

2.事例全体のまとめ

1)完全な system validation の指摘事項（不適合）の要約

- Software の変更に対する risk 評価が実施されていない。
- 市販 (OTS) software について意図した用途に対する validation が実施されていない。
- 供給者の site における validation は実施されているが、使用者の site では実施されていない。
- 第三者による validation について review が行われていない。
- Software version について validation が実施されていない。
- 必ずしも全ての test の script が入手できるとは限らない。
- Test の結果が受入れ基準を満たさない。

2)上記の指摘事項に対する check 上の推奨事項

- Data が破損されたり失われたりしていないこと。
- System の安全が確保（secure）されていること。
- Data の access が管理され、文書化されていること。
- Data の属性が明確であり、拒絶できないこと。
- Data の変更が追跡（trace）できること。
- 規制対象の企業が全面的に責任を負うこと。
    - 機器の機能について。
    - 開発及び使用中に validation が行なわれること。
- Validation
    - 高 risk system 及び機能に焦点を合わせる。
    - 応用に焦点を合わせる。

改正 EU 医療機器指令の software 関連事項

三浦

厚科研で厚生労働省より要請があった“改正 EU 医療機器指令の software 関連事項”は、次の通りである。

1.改正 EU 医療機器の正式名称

正式名称は “閣僚理事会指令 93/42/EEC、1993 年 6 月 14 日、医療機器に関する指令” (OJ L 169, 12.7.1993.p.1) である。なお、薬事日報社より日本医療機器産業連合会による翻訳版が発行されている。

2.医療機器指令の改訂の経緯

医療機器指令は過去に 5 回、改訂されている。次に EU 官報に掲載された順に示す。
本文中に M1~M5 の記号が記載されており、何時の改訂によるものかを把握できる。
因みに、software に関する事項は、全て M5 によって追加されている。

		官報 番号	頁	日付
M1	1998 年 10 月 27 日 欧州議会及び閣僚理事会指令 98/79/EC	L331	1	1998/12/7
M2	2000 年 11 月 16 日 欧州議会及び閣僚理事会指令 2000/70/EC	L313	22	2000/12/13
M3	2001 年 12 月 7 日 欧州議会及び閣僚理事会指令 2001/104/EC	L8	30	2002/1/10
M4	2003 年 9 月 29 日 欧州議会及び閣僚理事会規定(EC)No.1882/2003	1		2003/10/31
M5	1998 年 9 月 5 日 欧州議会及び閣僚理事会指令 2007/47/EC	L247	21	2007/9/21

3.Software に関する記載事項 (M5 による追加事項)

Software に関する記載事項は①～③の 3 項目であり、①は要求事項、②及び③はクラス分類に関する規定である。太字は改正 EU 医療機器指令の表題を示す。

①Ⅱ.設計及び組立に関する要求事項

12.エネルギー源に接続される機器、又はエネルギー源を有する機器に対する要求事項

M5

12.1a ソフトウェアを組込んでいる機器又はそれ自体が医療用ソフトウェアである場合、そのソフトウェアに対して、開発ライフサイクル、リスクマネジメント、妥当性確認 (validation) 及び検証 (verification) の原理を考慮し、最新技術によってバリデーションを実施しなければならない。

注) 上記の要求事項は、ソフトウェアバリデーションに、ISO 9000 で定義されている妥当性確認及び検証が含まれることを示唆している。プロセスバリデーション及び滅菌バリデーションなど、バリデーションに接頭語が付けられる場合、定義されている “バリデーション” とは異なった意味になる。

②附属書Ⅸ　クラス分類基準、Ⅰ.定義

1. クラス分類規定のための定義

1.4 能動医療機器

電気エネルギー源又は、人力若しくは重力によって直接発生する以外の、あらゆる動力源によって機能し、また、そのエネルギーを変換することによって動作するあらゆる医療機器をいう。能動医療機器と患者との間で、エネルギー、物質又はその他の要素を、いかなる大幅な変化なしに伝達することを意図する医療機器は、能動医療機器とみなさない。M5 スタンドアロンソフトウェアは能動医療機器とみなす。

注）能動医療機器のクラス分類（用途によって、能動医療機器のクラスは異なる）

附属書Ⅸ　クラス分類基準、Ⅲ.クラス分類

3.能動機器に適用する追加規定

3.1 規定 9

エネルギーを供給する又は交換することを意図する全ての能動治療機器はクラスⅡaである。ただし、機器の特性がそのエネルギーの適用の性質、密度及び位置を考慮すると潜在的に危害の源になり得るような場合、それらはクラスⅡbである。

3.2 規定 10

診断用の能動機器はクラスⅡaである。

— 可視光で患者の体を照らすために使用する機器を除き、機器が人体に吸収されるエネルギーを供給することを意図する場合、
— 機器が放射線薬品の生体内の分布を画像化することを意図する場合、
— 機器が生体の生理学的プロセスを直接診断又は監視することを意図する場合。ただし、その変動の性質が患者に対して直ちに危険をもたらし得るような、例えば心臓の機能、呼吸、中枢神経系の活動のように重要な生理学的パラメータの監視を機器が特に意図する場合を除く。

電離放射線の発生を意図し、また、診断及び治療用の放射線医学に使用することを意図し、それらの機器を制御又は監視する機器を含め、それらの機器の性能に直接影響を与える能動機器は、クラスⅡbである。

3.3 規定 11

次の方法による場合を除き、医薬品、体液又はその他の物質を人体に対して又は人体から投与及び/又は除去する全ての能動機器は、クラスⅡaである：

— 含まれている物質の性質、関与する人体の部位及び適用のモードを考慮すると潜在的に危害の源になり得るような場合、クラスⅡbである。

3.3 規定 12

その他の全ての能動機器はクラスⅠである。

③附属書IX　クラス分類基準

Ⅱ.施行規定

2.施行規定

2.3　機器を動作させる又は機器の使用に影響を与えるソフトウェアは、自動的にその機器と同一のクラスになる。

医療機器 software に関わる問題/課題について“規制分野別”に整理した。太字が未だ不十分な要素であり、今後の“action item”になろう。

1. 医療機器 software の種類

医療機器 software には、①Standalone software 及び②機器組み込み software がある。

2 .医療機器規制

医療機器の規制は、①市販前審査（GHTF SG 1/SG 5 担当）、②市販後監視（GHTF SG 2 担当）、③QMS 及びその監査（GHTF SG 3/SG 4 担当）の 3 分野に分けられる。

3. 市販前審査

Standalone software：安全性及び品質について、効果的に審査することは至難である。それらについては、当該組織における software 開発管理体制の有無及び水準を審査することになる。有効性は医療機器であるか否かの判断基準になる。GHTF Software AHWG の推奨事項に基づいて SG 1 が作成する“基本要件の修正の内容”が参考になる。また、“他国（特に米国）で規制対象とされている standalonesoftware の事例”及び“Standalone software の市販前審査基準”について調査する必要がある。また、“EU における software validation の監査基準“に関しても継続して調査すべきである。

機器組み込み software：Software を含まない機器の審査と本質的に異なる点はない。

4. QMS

	監査（査察）基準	監査（査察）における不適合の指摘
日本	なし	なし
米国	なし	あり

規制における不適合とは、規制要求事項との乖離（gap）である。規制要求事項が明示されていない状況下において不適合を指摘することには無理がある。FDA の場合、QMS の査察基準は“QSR”であり、QSR では、software に関する要求事項には全く言及していない。ただし、FDA は software に関しても査察を実施し、不適合の指摘及び warning letter 発行を行なっている。本来、QSR を改正すべきであるが、software に関する査察が如何なる法的根拠に基づくものか、“Software の規制に関わる指針文書の調査”などによって、規制に援用される文書について確認する必要がある。なお、FDA の場合、指針文書には、強制される“guideline”と参考資料の“guidance”があることに留意する必要がある。

5. 市販後監視

規制は事実/証拠に基づくべきであり、“Software に起因する不具合事象を精査”する必要がある。規制要求事項は、事例が多い共通的原因に対処するものであるべきである。また、規格及び規則は、監査/査察の基準であるのみならず、製造業者に対して安全/品質の確保のための有効かつ有用な情報を提供することが最も重要である。

医療機器ソフトウェアの開発指針について

古川 孝，中里 俊章

2009年はIEC 62304発行から3年が経過し，欧州を中心とした提案を元に同規格の見直しがNWIPとして検討されている。また，欧州では，先行して同規格のIEC 62304:2006の規制・認証目的での利用が始まっている。また，米国ではFDAが認証規格として同規格を採用しており，市販前審査において，既に利用している。

この医療機器ソフトウェアの開発指針は，製造業者が導入することを想定したガイダンス文書であり，前述の状況から見て，IEC 62304の視点から検討することが重要であり，また見直し時期でもあることから，さらに考察を加えて案をまとめることにした。

主要な修正点（IEC 52304:2006との乖離点）は，以下の通りである。　（現：IEC 62304:2006を参照）

1．「手法・ツール」又は手順等詳細記載部分の本文からの削除
　Ed.1開発時に日本コメントとして強く主張したが，一部残った。
　（現5.1.4，5.1.10，5.1.11，5.2.2，5.6.8，7.1.3，8.1.2）

2．ソフトウェア安全クラス分類の撤廃
　IEC 62304の根幹をなす部分ではあるが，分類にかける作業が困難で効果が見え難く，規格を複雑にしている。全体をよりシンプルにすることで撤廃は可能と考える。（現5.3.5，他全般）

3．ソフトウェア開発に一般的な部分の記載省略
　医療機器ソフトウェア開発の要求事項にできる限り絞る。一般的な要求事項の詳細は記述しない。
　（現5.3.4，5.4.3，5.5.3，5.5.4，5.6.4，5.6.5，5.6.6，5.7.3）

4．ソフトウェア以外に共通な内容の記載省略
　他規格や指針があるため詳細は記述しない。（現7.1.2，7.1.5）

5．重複内容の記載統合
　重複説明の省略（現5.1.3）
　試験文書の内容に関しては，同一内容，且つ1箇所にまとめた。（現5.6.7，9.8）

6．ソフトウェア・バリデーション（妥当性検証）の包含
　IEC 62304は，バリデーションを範囲外としたが，ソフトウェア単体が医療機器の場合，ソフトウェア・リリースは，ソフトウェア・バリデーション済みソフトウェアのリリースと考えるのが，理解しやすい。（下記1.2, 3.22, 5.1.1, 5.7.1）
　ただし，後述のようにソフトウェア場合，多くは繰り返し作業を伴い，検証も同時に繰り返されることになる。「最終段階での試験」に近い用語として使われがちな妥当性確認だが，ソフトウェア・バリデーションはその前後のアクティビティをも含む広義の定義を必要とするように思われる。

また，欧米の規制当局の審査・指導，公的教育等を参考にし，重要と考えられる点は維持している。
例えば，開発（保守）計画，アーキテクチャ設計，検証，構成管理，変更管理，リスクマネジメント，異常の傾向分析と対策等である。
一方，ソフトウェアは容易に変更できる反面，その影響分析が複雑さ故に困難になってきている。このため，すべての工程を通して，分析，設計（変更）又は実装，検証，文書化を繰り返し実行していくこ

とが，エラー（異常）を減らす上で必要であり，IEC 62304 の大切な概念でもあり，踏襲している。
変更により，検証の繰り返しが必要となるが，これは，構成管理プロセスにある“変更管理”アクティビティ及びタスクによることとし，全体をシンプルにした。
デザインコントロールの起点は，開発計画に規定しておけばよく，この指針の運用上のポイントである。

参考）IEC 62304 の章立て（一部抜粋）

5　ソフトウェア開発プロセス
5．1　ソフトウェア開発計画
5．1．1　ソフトウェア開発計画
5．1．2　ソフトウェア開発計画の継続更新
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
5．1．4　ソフトウェア開発規格，方法及びツールの計画
5．1．5　ソフトウェア結合及び結合計画
5．1．6　ソフトウェア検証計画
5．1．7　ソフトウェアリスクマネジメント計画
5．1．8　文書化計画
5．1．9　ソフトウェア構成管理計画
5．1．10　管理が必要な支援アイテム
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
5．2　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
5．2．2　ソフトウェア要求事項の内容
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
5．2．4　医療機器リスク分析の再評価
5．2．5　システム要求事項の更新
5．2．6　ソフトウェア要求事項の検証
5．3　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
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
5．3．3　SOUP アイテムの機能及び性能要求の指定
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
5．3．5　リスクコントロールの必要な分離の特定
5．3．6　ソフトウェアアーキテクチャの検証
5．4　ソフトウェア詳細設計
5．4．1　ソフトウェアアーキテクチャのソフトウェアユニットへの分解
5．4．2　ソフトウェアユニットごとの詳細設計の開発
5．4．3　インタフェース用詳細設計の開発
5．4．4　詳細設計の検証
5．5　ソフトウェアユニットの実装及び検証
5．5．1　各ソフトウェアユニットの実装

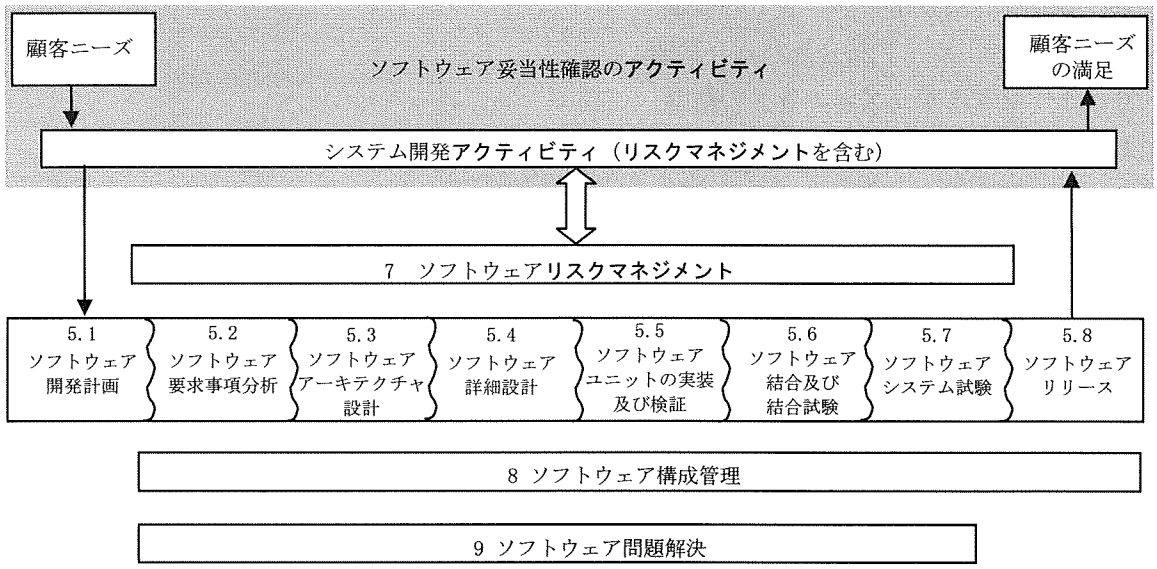

図 1－ソフトウェア開発プロセス及びアクティビティの関連図

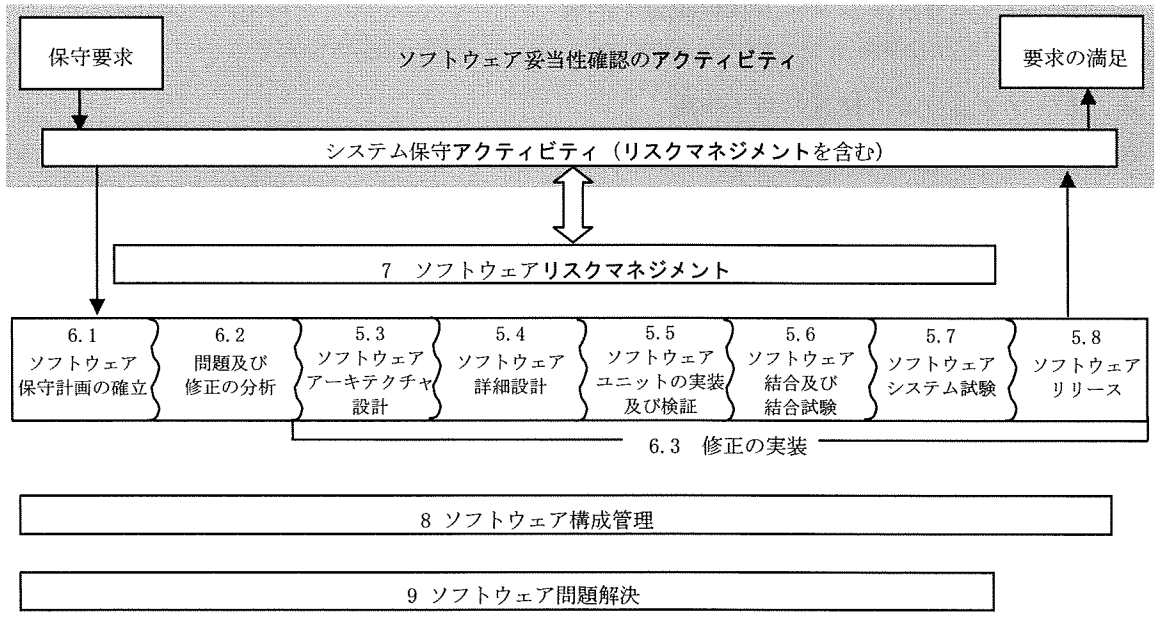

図 2－ソフトウェア保守プロセス及びアクティビティの関連図

この指針は，**医療機器ソフトウェア**の**安全**設計及び保守に必要な**アクティビティ**及び**タスク**からなるライフサイクル**プロセス**のフレームワーク並びに各ライフサイクル**プロセス**に対する要求事項を規定する。各ライフサイクル**プロセス**は，一連の**アクティビティ**に分割する。さらに大部分の**アクティビティ**は，一連の**タスク**にそれぞれ分割する。

通常，**医療機器ソフトウェア**は，品質マネジメントシステム（**4.1** 参照）及び**リスクマネジメント**システム（**4.2** 参照）の範囲内で開発し，維持することを前提とする。**リスクマネジメントプロセス**は，**JIS T 14971** に規定している。

ソフトウェア開発**プロセス**は，多くの**アクティビティ**によって構成する。これらの**アクティビティ**については，**図 1** に示し，箇条 **5** に記載する。現場で発生する多くの事故が，ソフトウェアの不適切なアップデート及びアップグレードを含む，**医療機器システム**のサービス又は保守に関連するため，ソフトウェア保守**プロセス**は，ソフトウェア開発**プロセス**と同様に重要とみなすことができる。ソフトウェア保守**プロセス**は，ソフトウェア開発**プロセス**と非常に類似している。これについては，**図 2** に示し，箇条 **6** に記載する。

また，この指針は，安全な**医療機器ソフトウェア**を開発するために不可欠な二つの**プロセス**，すなわちソフトウェア構成管理**プロセス**（箇条 **8** 参照）及びソフトウェア問題解決**プロセス**（箇条 **9** 参照）について規定する。

この指針は，**製造業者**の組織の構成，及び**プロセス**，**アクティビティ**又は**タスク**を実行する組織の部門は規定しない。この指針が要求するのは，この指針への適合性を確立するために**プロセス**，**アクティビティ**又は**タスク**を完備することが望ましいということだけである。

この指針は，作成する文書の名称，書式及び記載すべき内容のいずれも規定しない。この指針は，**タスク**の文書化を要求するが，文書をどのようにまとめるかは指針の利用者にまかせている。

目的及び適用範囲

1.1 *目的

この指針は，**医療機器ソフトウェア**のライフサイクルについての要求事項を規定する。この指針に規定する一連の**プロセス**，**アクティビティ**及び**タスク**は，**医療機器ソフトウェア**ライフサイクル**プロセス**に共通のフレームワークを確立する。

1.2 *適用範囲

この指針は，ソフトウェアそれ自体が**医療機器**である場合，又はソフトウェアが完成品である**医療機器**に組み込まれている若しくは不可欠な部分となっている場合の，**医療機器ソフトウェア**の開発及び保守について規定する。

この指針は，その**医療機器**がすべてソフトウェアで構成されている場合，**医療機器**の妥当性確認及び最終的な出荷の合否判定を対象としている。

2 *引用規格

次に掲げる規格は，この規格に引用されることによって，この規格の規定の一部を構成する。この引用規格は，その最新版（追補を含む。）を適用する。

JIS T 14971 医療機器－リスクマネジメントの医療機器への適用

注記 対応国際規格 **ISO 14971** , Medical devices – Application of risk management to medical devices (IDT)

3 用語及び定義

この規格で用いる主な用語及び定義は，次による。

3.1

アクティビティ（ACTIVITY）

一組以上の相互関係又は相互作用のある**タスク**

3.2

異常（ANOMALY）

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，**ソフトウェア製品**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。

（**IEEE 1044**:1993 定義 **3.1** 参照）

3.3

アーキテクチャ（ARCHITECTURE）

システム又はコンポーネントの構造

（**IEEE 610.12**:1990 参照）

3.4

変更要求（CHANGE REQUEST）

ソフトウェア製品に対する変更内容を文書化した仕様

3.5

構成アイテム（CONFIGURATION ITEM）

決められた時点で一意に特定できる“もの”(entity)

注記 **JIS X 0160**:1996 定義 **3.6** による。

3.6

成果物（DELIVERABLE）

アクティビティ又は**タスク**の要求される結果又はアウトプット（文書を含む）

3.7

医療機器ソフトウェア（MEDICAL DEVICE SOFTWARE）

開発中の**医療機器**に組み込むことを目的として開発した，又はそれ自体を**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**。

3.8

問題報告（PROBLEM REPORT）

ユーザ又はその他の関係者が，安全でない，意図した用途に対して不適切である又は仕様に反すると判断した，**ソフトウェア製品**の実際の又は潜在的な動作の記録。

注記 1 この規格は，すべての**問題報告**に対して**ソフトウェア製品**の変更を要求するものではない。**製造業者**は，誤解，エラー又は軽微な事象として**問題報告**を拒絶できる。

注記 2 **問題報告**は，リリースした**ソフトウェア製品**又は開発中の**ソフトウェア製品**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（箇条 **6** 参照）。

3.9

プロセス（PROCESS）

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**

（**JIS Q 9000**:2006 定義 **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。

3.10

安全（SAFETY）

受容できない**リスク**がないこと

（**JIS T 14971**:2003 定義 **2.20** 参照）

3.11

セキュリティ（SECURITY）

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情報及びデータを保護すること。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。

（**JIS X 0160**:1996 定義 **3.25 参照**）

3.12

ソフトウェア開発ライフサイクルモデル（SOFTWARE DEVELOPMENT LIFE CYCLE MODEL）

ソフトウェア要求事項の定義から製造のためにリリースするまでの，ソフトウェアのライフサイクルにかかわる次のような概念上の構造。

- **ソフトウェア製品**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。

3.13

ソフトウェアアイテム（SOFTWARE ITEM）

コンピュータプログラムの識別可能な部分

（**ISO/IEC 90003**:2004 定義 **3.14** 修正）

注記 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，それ以上分割できない**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すべてのレベルを，**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**の定義及び粒度（granularity）を提示する責任がある。

3.14

ソフトウェア製品（SOFTWARE PRODUCT）

コンピュータプログラム，手続き並びに関連する文書及びデータのまとまり。

（**JIS X 0160**:1996 定義 **3.26 参照**）

3.15

ソフトウェアシステム（SOFTWARE SYSTEM）

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。

3.16

ソフトウェアユニット（SOFTWARE UNIT）

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**は，ソフトウェア構成管理又は試験の目的で使用できる。

3.17

SOUP

開発過程が不明なソフトウェア（“Software Of Unknown Provenance”の頭字語）

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**［“市販品（off-the-shelf）”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。

3.18

システム（SYSTEM）

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。

（**JIS X 0160**:1996 定義 **3.31 参照**）

3.19

タスク（TASK）

行う必要がある一つの作業

3.20

トレーサビリティ（TRACEABILITY）

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）

3.21

検証（VERIFICATION）

客観的証拠を提示することによって，規定要求事項が満たされていることを確認すること。

注記 1 “検証済み”という用語は，**検証**が済んでいる状態を示すために用いられる。

（**JIS Q 9000**:2006 定義 **3.8.4 参照**）

注記 2 設計及び開発における**検証**は，ある**アクティビティ**に対して定義した規定要求事項に適合しているかを確定するために，その**アクティビティ**の結果に対して吟味を行う**プロセス**である。

3.22

妥当性確認（VALIDATION）

客観的証拠を提示することによって，特定の意図された用途又は適用に関する要求事項が満たされていることを確認すること。

注記 1 “妥当性確認済み”という用語は，妥当性確認が済んでいる状態を示すために用いられる。

（**JIS Q 9000**:2006 定義 **3.8.5 参照**）

注記 2 開発及び保守における妥当性確認は，システムのニーズ，目的又は規制を満たす能力を規定するアクティビティに対して定義した要求事項に適合しているかを確定するために，その**アクティビティ**の結果に対して吟味を行う**プロセス**である。

3.23

バージョン（VERSION）

構成アイテムの（時間によって）識別された段階

注記 1 **ソフトウェア製品**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。

注記 2 **JIS X 0160**:1996 定義 **3.37** による。

4 *一般要求事項

4.1 *品質マネジメントシステム

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実証する。

注記 1 この能力は，次のいずれかに適合する品質マネジメントシステムを使用して実証できる。

- **JIS Q 13485** [7]
- 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

注記 2　品質マネジメントシステム要求事項をソフトウェアに適用するための指針は，**ISO/IEC 90003** [11]に規定している。

4.2　*リスクマネジメント

製造業者は，**JIS T 14971**，**又は製造業者が規定したリスクマネジメントプロセス**を適用する。

5　ソフトウェア開発プロセス

5.1　*ソフトウェア開発計画

5.1.1　ソフトウェア開発計画

製造業者は，開発する**ソフトウェアシステム**の適用範囲，規模，環境及びソフトウェア安全性に適した，ソフトウェア開発**プロセス**の**アクティビティ**を実施するために，（一つ又は複数の）ソフトウェア開発計画を確立する。

a)　**ソフトウェアシステム**の開発に使用する**プロセス**

b)　**成果物**（文書を含む）

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**

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

e)　ライフサイクルの各段階で発見される，**ソフトウェア製品**，**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

注記 3 ソフトウェア開発計画は，全体の**システム**開発計画に統合してもよい。

注記 4 **ソフトウェアシステム**がスタンドアロン**システム**（ソフトウェア単独）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る。この場合，ソフトウェアシステム試験は，妥当性確認を含む計画とする。

5.1.2　ソフトウェア開発計画の継続更新

製造業者は，開発の進ちょく（捗）に応じて，計画を適宜更新する。

5.1.3　ソフトウェア結合及び結合試験計画

製造業者は，**ソフトウェアアイテム**（**SOUP** を含む）を結合して，結合時に試験を実施するための計画を，ソフトウェア開発計画書に示すか又は引用する。

注記　結合試験及び**ソフトウェアシステム**試験は，一つの計画及び一連の**アクティビティ**に統合してもよい。

5.1.4　ソフトウェア検証計画

製造業者は，ソフトウェア開発計画書に，次の**検証**情報を示すか又は引用する。

a)　**検証**が必要な**成果物**

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**

c)　**成果物**を**検証**するマイルストーン

d)　**成果物検証**の合否判定基準

5.1.5　ソフトウェアリスクマネジメント計画

製造業者は，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**の実行計画（**SOUP** に関連した**リスク**の管理を含む）を，ソフトウェア開発計画に示すか又は引用する。

5.1.6　文書化計画

製造業者は，ソフトウェア開発ライフサイクルにおいて作成する文書についての情報を，ソフトウェア開発計画書に示すか又は引用する。

5.1.7　ソフトウェア構成管理計画

製造業者は，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示すか又は引用する。

5.2　*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

製造業者は，**医療機器**の**ソフトウェアシステム**ごとに，**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。

注記　**ソフトウェアシステム**がスタンドアロン**システム**（ソフトウェア単独の機器）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る。

5.2.2　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

製造業者は，ハードウェアの故障及び潜在的なソフトウェア不具合に対してソフトウェアに実装する**リスクコントロール**手段を，**医療機器ソフトウェア**の要求事項に含める。

注記　これらの要求事項は，ソフトウェア開発の初期には利用できないこともあり，ソフトウェアの設計及び**リスクコントロール**手段の追加定義を行うことで変更できる。

5.2.3　医療機器リスク分析の再評価

製造業者は，ソフトウェア要求事項が確定した時点で**医療機器リスク分析**を再**評価**し，適宜，更新する。

5.2.4　システム要求事項の更新

製造業者は，ソフトウェア要求事項分析**アクティビティ**の結果を受けて，適宜，**システム**要求事項を含む既存の要求事項の再**評価**及び更新を実施する。

5.2.5　ソフトウェア要求事項の検証

製造業者は，ソフトウェア要求事項について**検証**し，文書化する。

5.3　*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

製造業者は，**医療機器ソフトウェア**の要求事項を，文書化した**アーキテクチャ**（ソフトウェアの構造の説明及び**ソフトウェアアイテム**の特定をしているもの）に変換する。

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

製造業者は，**ソフトウェアアイテム**と**ソフトウェアアイテム**外部のコンポーネント（ソフトウェア及びハードウェア）との間，及び**ソフトウェアアイテム**間のインタフェースについて，**アーキテクチャ**を開発し，文書化する。

5.3.3　SOUP アイテムの機能及び性能要求事項の指定

ソフトウェアアイテムを **SOUP** と特定している場合，**製造業者**は，その **SOUP** アイテムについて，その意図した用途に必要な機能性能要求事項を明確にする。

5.3.4　ソフトウェアアーキテクチャの検証

製造業者は，ソフトウェアアーキテクチャーについて検証し，文書化する。

5.3.5　医療機器リスク分析の再評価

製造業者は，ソフトウェアアーキテクチャーが確定した時点で**医療機器リスク分析**を再**評価**し，適宜，更新する。

5.4　*ソフトウェア詳細設計

5.4.1　ソフトウェアアーキテクチャのソフトウェアユニットへの分解

製造業者は，最小単位である**ソフトウェアユニット**によって表現できるまで，ソフトウェア**アーキテクチャー**を分解する。

5.4.2　ソフトウェアユニットごとの詳細設計の開発

製造業者は，**ソフトウェアアイテム**の**ソフトウェアユニット**ごとに詳細設計を開発する。リスクコントロール手段に使用するソフトウェアユニットの詳細設計は，文書化する。

5.4.3　詳細設計の検証

製造業者は，ソフトウェアの詳細設計を検証し，文書化する。

5.5　*ソフトウェアユニットの実装及び検証

5.5.1　各ソフトウェアユニットの実装

製造業者は，各**ソフトウェアユニット**を実装する。

5.5.2　ソフトウェアユニット検証プロセスの確立

製造業者は，各**ソフトウェアユニット**を検証するための方針，方法，合否判定基準及び手順を確立する。**検証**を試験によって実施する場合は，その試験手順の正確さについて**評価**する。

注記　結合試験及び**ソフトウェアシステム**試験は，一つの計画及び一連の**アクティビティ**に統合してもよい。

5.5.3　ソフトウェアユニットの検証

製造業者は，**ソフトウェアユニット**の**検証**を実行し，結果を文書化する。

5.6　*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

製造業者は，結合計画に従って**ソフトウェアユニット**を結合する（**5.1.3** 参照）。

5.6.2　ソフトウェア結合の検証

製造業者は，結合計画に従って，ソフトウェアユニットが，ソフトウェアアイテム及びソフトウェアシステムに結合されていることを**検証**し，記録する。

5.6.3　結合したソフトウェアの試験

製造業者は，結合計画（**5.1.3** 参照）に従って，結合した**ソフトウェアアイテム**を試験し，結果を文書化する。

注記 1　結合試験及び**ソフトウェアシステム**試験は，一つの計画及び一連の**アクティビティ**に統合してもよい。

5.6.4　結合試験記録の内容

製造業者は，試験を再現できるように，記録を保存し，実施する。

5.7　*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

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規定した一連の試験を確立し，実施する。

注記 1　結合試験及び**ソフトウェアシステム**試験は，一つの計画及び一連の**アクティビティ**に統合してもよい。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よい。

妥当性確認を実行するソフトウェアシステム試験は，システムの意図された用途，適用，顧客ニーズ又は規制を満たす要求事項に従った環境を確立し，実施する。

5.7.2　ソフトウェア問題解決プロセスの使用

製造業者は，**ソフトウェアシステム**試験中に発見した**異常**を，ソフトウェア問題解決**プロセス**で処理する。

5.7.3　ソフトウェアシステム試験の検証

製造業者は，次の事項を検証する。

a)　使用した**検証**方針及び試験手順が適切である。

b)　**ソフトウェアシステム**試験手順が，ソフトウェア要求事項に従っている。

c)　すべ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。

d)　試験結果が，合否基準を適合する。

5.7.4　ソフトウェアシステム試験記録の内容

製造業者は，試験を再現できるように，記録を保存し，実施する。

5.7.5　試験文書の内容

製造業者は，**ソフトウェアアイテム**及び**システム**の試験，結合試験，再試験に当たって，試験文書の中に次を含める。

a)　テストケース仕様

b)　試験結果

c)　発見された**異常**

d)　試験したソフトウェアの**バージョン**

e)　関連するハードウェア及びソフトウェアテスト構成

f)　関連試験ツール

g)　試験実施日

h)　試験者の識別

5.8　*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

製造業者は，ソフトウェア**検証**が完了し，結果を**評価**したことを，ソフトウェアのリリース前に確認する。

5.8.2　既知の残留異常の文書化

製造業者は，残留している既知の**異常**をすべて文書化する。

5.8.3　リリースしているバージョンの文書化

製造業者は，リリースしている**ソフトウェア製品**の**バージョン**を文書化する。

5.8.4　リリースしたソフトウェアの作成方法の文書化

製造業者は，リリースしたソフトウェアの作成手順及び作成環境を文書化する。

5.8.5　アクティビティ及びタスクの完了確認

製造業者は，すべての**アクティビティ**及び**タスク**が，すべての関連する文書化とともに完了していることを確認する。

5.8.6　ソフトウェアのアーカイブ

製造業者は，次について，**製造業者**自身が決定した機器の耐用期間，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保管する。

a)　**ソフトウェア製品**及び**構成アイテム**

b)　文書

5.8.7　ソフトウェアリリースの反復性の確保

製造業者は，リリースした**ソフトウェア製品**が，変造又は無断で変更されることなく，使用する場所に確実

に納品されるようにするための手順を確立する。

6　ソフトウェア保守プロセス

6.1　*ソフトウェア保守計画の確立

製造業者は，保守**プロセス**の**アクティビティ**及び**タスク**を実行するためのソフトウェア保守計画を確立する。計画の内容は，次による。

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，次の手順
- 取得
- 文書化
- 評価
- 解決
- 追跡

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

c)　ソフトウェア**リスクマネジメントプロセス**の使用

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

e)　既存**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

f)　**SOUP** について，次の事項を**評価**し実行する手順
- アップグレード
- バグ修正
- パッチ
- 陳腐化，及び支援体制の確認

6.2　*問題及び修正の分析

6.2.1　フィードバックの文書化及び評価

6.2.1.1　フィードバックの監視

製造業者は，リリースした**ソフトウェア製品**について，自身の組織内部及びユーザからのフィードバックを監視する。

6.2.1.2　フィードバックの文書化及び評価

フィードバックを文書化するとともにそれを**評価**し，リリースした**ソフトウェア製品**に問題がないかを判断する。問題があった場合は，**問題報告**として記録する（箇条 **9** 参照）。**問題報告**には，実際に悪影響を及ぼす又はそ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。

6.2.1.3　安全性に影響する問題報告の評価

問題報告は，個々に**評価**を実施し，リリースした**ソフトウェア製品**の**安全**性にどのような影響があるかを判断するとともに，問題に対処するためにリリースした**ソフトウェア製品**に変更を加える必要があるかを判断する。

6.2.2　ソフトウェア問題解決プロセスの使用

製造業者は，**問題報告**の対処に当たり，ソフトウェア問題解決**プロセス**（箇条 **9** 参照）を使用する。

6.2.3　変更要求の分析

製造業者は，箇条 **9** で要求している分析を実施するほか，各**変更要求**が，組織，リリースした**ソフトウェア製品**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。

6.2.4　変更要求の承認

製造業者は，リリースした**ソフトウェア製品**に修正が生じる**変更要求**を**評価**し，承認する。

6.2.5　ユーザ及び規制当局への通知

製造業者は，リリースした**ソフトウェア製品**に影響がある，承認済みの**変更要求**を明らかにする。

法令の要求に応じて，**製造業者**は，ユーザ及び規制当局に対して次の項目を通知する。

a)　リリースした**ソフトウェア製品**についての問題，及び変更せずに継続使用した場合の結果。

b)　リリースした**ソフトウェア製品**に対して利用可能な変更の本質，及びそれらの変更の入手及びインストールの方法。

6.3　*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

製造業者は，ソフトウェア開発**プロセス**（箇条 **5** 参照）又は確立した保守**プロセス**を使用して，修正を実装する。

注記　ソフトウェア変更の**リスクマネジメント**にかかわる要求事項については，**7.4** 参照。

6.3.2　修正ソフトウェアシステムの再リリース

製造業者は，**5.8** に従って，修正した**ソフトウェアシステム**をリリースする。

7　*ソフトウェアリスクマネジメントプロセス

7.1　*危険状態を引き起こすソフトウェアの分析

製造業者は，医療機器ソフトウェア（**SOUP** を含む）を分析して，危険状態を引き起こす可能性のある，又は一因となる**ソフトウェアアイテム**を**特定し**，その潜在的原因とイベントシーケンスを，**リスクマネジメントファイル**に文書化する（**JIS T 14971** 参照）。

7.2　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定義

製造業者は，**リスクマネジメントファイル**に文書で示した，危険状態の一因となる**ソフトウェアアイテム**の，潜在的原因のそれぞれについて，**リスクコントロール**手段を定義し，文書化する。

注記　**リスクコントロール**手段は，ハードウェア，ソフトウェア，動作環境又は取扱い説明書に実装できる。

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

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，**製造業者**は，**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。

7.3　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検証

7.2 で文書化した**リスクコントロール**手段をすべて実装していることを**検証**し，その**検証**結果を文書化する。

7.3.2　新しいイベントシーケンスの文書化

リスクコントロール手段を**ソフトウェアアイテム**として実装した場合，**製造業者**は，**リスクコントロール**手段を**評価**して，危険状態を引き起こす可能性のある新たなイベントシーケンスを特定し，**リスクマネジメントファイル**に文書化する。

7.3.3　トレーサビリティの文書化

製造業者は，ソフトウェア**ハザード**の**トレーサビリティ**について，適宜文書化する。