

表 C.1-1 回避すべき潜在的なソフトウェア関連の落とし穴 (続き)

<p><b>IEC 62304:2006 細分簡条 5.6-5.7 ソフトウェア統合、統合試験、及びシステム試験 (Subclauses 5.6-5.7 Software integration, integration testing, and SYSTEM testing)</b></p> <ul style="list-style-type: none"> <li>- 試験の計画及び試験者の教育にリスクアセスメント情報を使用しない。</li> <li>- 100%の試験は不可能にもかかわらず、リスクコントロール手段として試験に依存する。</li> <li>- リスクコントロール手段検証のための試験の一環として、システム又はソフトウェアの故障モードシミュレーションを行わない。</li> <li>- 承認も管理もされていない試験用自動化ツールを使用し、その結果に依存する。</li> <li>- 試験で発見できない異常を検出するためのコード分析が適切に行われない。</li> </ul>
<p><b>IEC 62304:2006 細分簡条 5.8 ソフトウェアリリース (Subclause 5.8 Software release)</b></p> <ul style="list-style-type: none"> <li>- リリースした文書のバージョンとリリースしたソフトウェアが一致せず、開発/試験チームが将来の製品のリリースについて誤解する可能性がある。不正確な文書記録及びドキュメンテーションは、リリースの喪失、ひいてはリスクコントロール手段の見落とし、又は安全関連ソフトウェアの不十分な検証に至るおそれがある。</li> <li>- 残留異常の評価において、臨床知識を十分に持っている者を見落とさない。</li> <li>- 残留異常の重要性を、様々な状態下ですべての潜在的な悪影響を判断するための完全な根本原因分析ではなく、機能的な兆候だけに基づいて評価する。</li> <li>- サードパーティが特定のSOP/バージョンの配布を行わなくなると、そのバージョンは故障の調査及び現場での修正作業に使用できなくなるという事実を見落としている。</li> <li>- 特定のツール又はバージョンのバージョンアップがアライメントを妨げないため、特定のソフトウェアバージョンを作成することができない。</li> <li>- 医療機器の寿命は、現在使用しているアーカイブメディアの寿命よりも長いと思われる。製造業者が古いアーカイブメディアを新しいものに交換するときは、古いアーカイブを新しいメディアに移すためのデータ移動バスを計画するのが望ましい。</li> </ul>
<p><b>IEC 62304:2006 細分簡条 6.1 ソフトウェアメンテナンス計画の確立 (Subclause 6.1 Establish software maintenance plan)</b></p> <ul style="list-style-type: none"> <li>- 変更のリスクをマネジメントに對して明確なアプローチを持たないメンテナンスプロセスを確立する。</li> <li>- 変更の意図する機能性のみを対象とし、影響を受けるコンポーネント及びそれに関連するリスクは対象としない変更のリスクをマネジメントを確立する。</li> </ul>
<p><b>IEC 62304:2006 細分簡条 6.2-6.3 問題と修正の分析及び実施 (Subclauses 6.2-6.3 Problem and modification analysis and implementation)</b></p> <ul style="list-style-type: none"> <li>- 機能上の小さな変更が安全性に影響を及ぼすことはありえないと決め込む。</li> <li>- 既存のリスクコントロール手段及びユーザーインターフェースの適切性を再調査することなく、医療機器の使用を新しい対象母集団、新しい疾患の兆候、新しいタイプの使用者 (例：外科医ではなく看護師)、又は新しいソフトウェアチームに拡大する。</li> <li>- 問題解決リソースの優先度を、根本原因及び潜在的な悪影響を見極めることなく、報告された現地問題の現象に基づいて設定する。</li> <li>- 非臨床目的で設計されたソフトウェア (例：請求書作成) に、後に適切なリスクマネジメントを施ることなく臨床目的で配給される臨床データが含まれている。</li> </ul>

附属書 D (参考情報)

ライフサイクル/リスクマネジメント表

表 D.1 に、IEC 62304:2006 の開発活動及び関連するソフトウェアリスクマネジメント活動を掲げる。なお、この表は、厳密な順序で流れるライフサイクルを表すことを意図したものではない。

表 D.1 - ライフサイクル/リスクマネジメント表

ソフトウェア要求事項	ISO 14971:2007	
	4 リスク分析	5 リスク評価
<p><b>5.1 ソフトウェア開発プロセス</b></p> <p>リスクマネジメント計画 (ISO 14971:2007 の細分簡条 3.4) 計画及び文書:</p> <ul style="list-style-type: none"> <li>a) 計画したリスクマネジメント活動の適用範囲。計画の要約を適用する医療機器及びソフトウェアの政府を明らかに記載する。</li> <li>b) 責任及び権限の割り当て</li> <li>c) リスクマネジメント活動のレビューに関する要求事項</li> <li>d) 製造業者の許容リスク決定方針に基づいたリスク評価の基盤。危害の発生確率が推定不能の場合のリスク評価基準を含む。</li> <li>e) 検証活動</li> </ul> <p>り関係する生産/生産後情報の収集及びレビューに関係する活動</p>	<p>5.1.1 特定されたリスク (例：ハードウェア故障やユーザーエラー) についてソフトウェアリスクコントロール手段を特定する。</p> <ul style="list-style-type: none"> <li>- 設計に影響を及ぼしうるソフトウェア故障に対するソフトウェアリスクコントロール手段の初期の特定。(例：本質安全設計又は保護手段)</li> <li>- 快速性の向上、重症性の低減、発生率の低減のためにソフトウェアを特定する。</li> <li>- 新しいハードウェアについてソフトウェアを特定する。</li> </ul>	
<p><b>5.2 ソフトウェア要求事項分析</b></p> <p>5.2.1 特定された要求事項の適用範囲、適用する使用並びに命に関与する可能性がある使用及び他の患者を分析する。</p> <ul style="list-style-type: none"> <li>- 臨床試験、患者、及びサービス提供者、製造業者、医療従事者、他の関係者との関係から、既知のハードウェア及びソフトウェアの潜在的な見落としを特定する。</li> <li>- 誤用及び誤用、教育、使用、アップグレード、並びにメンテナンスなどの悪影響を考慮する。</li> <li>- ハザード状態を招くおそれのあるイベントシーケンス又は組み合わせを特定する。</li> <li>- 特定した各ハザード状態について考えられる結果の重大性を考慮に入れてリスクを特定する。</li> <li>- 4.3 ソフトウェア安全クラス分類 (IEC 62304 要求事項)</li> </ul>	<p>5.2.1 特定されたリスクについてリスクの厳格さが必要か否かを判断する。</p> <ul style="list-style-type: none"> <li>- ソフトウェアのリスクコントロール手段が十分か、又はハードウェアのリスクコントロール手段が必要か若しくは望ましく、其現可能性を判断する。</li> </ul>	

表 D.1 - ライフサイクル/リスクマネジメント表 (続き)

活動	リスク分析	リスク評価	リスクコントロール
5.3 ソフトウェアキーチャタ設計	<ul style="list-style-type: none"> <li>重要なデータ及びコンポーネント並びにハザードを招くおそれのある欠陥のクラスを特定する。ソフトウェア原因に特に注意する。</li> <li>関連ハザードを特定する。</li> <li>インタフェース内容及びタイミング通信の内容及びタイミング性能の基準及び制限を評価する。</li> <li>4.3 ソフトウェア安全クラス分類 (IEC62304要求事項)</li> </ul>	<ul style="list-style-type: none"> <li>リスクの観点からソフトウェアに割り当てられた役割の性質を再評価する。</li> <li>安全性に関係しない機能性によって影響を受けるコンテロール手段の感受性を評価する。</li> <li>適切な冗長性を与えることに特に注意を払う。</li> <li>冗長性に關わるハザードを特定する。</li> <li>検出及びソフトロールのための追加的方法を特定する。</li> </ul>	<ul style="list-style-type: none"> <li>重要コンポーネントを網羅し、ハザードの長期的なソフトウェア原因の発生又は検出するためのアーキテクチャ上のリスクコンテロール手段を特定する。</li> <li>適切な冗長性を与えることに特に注意を払う。</li> <li>冗長性に關わるハザードを特定する。</li> <li>検出及びソフトロールのための追加的方法を特定する。</li> </ul>
5.4 ソフトウェア設計	<ul style="list-style-type: none"> <li>ハザードの追加的な潜在的な原因を特定する。</li> <li>データコーディング、及び転送のエラーを想定する。</li> <li>ハードウェア破壊を想定する。</li> </ul>	<ul style="list-style-type: none"> <li>リスクコントロール手段の妥当性を再評価する。</li> <li>安全性に關係するエラー及び安全性に關係しないエラーの區別を定める。</li> </ul>	<ul style="list-style-type: none"> <li>具体的なリスクコントロール手段及び防衛的設計/プログラミングの定石を及ぼす。</li> <li>リスクコントロール手段が、細部に実装されるように、トレーサビリティ分析及び詳細不明の機能が実装されていないかかを判断する。</li> </ul>
5.5 ソフトウェアユニットの実装及び検証	<ul style="list-style-type: none"> <li>ハザードの追加的な潜在的な原因を特定する。</li> <li>同様のエラーの発生について各試験の実装を評価する。</li> </ul>	<ul style="list-style-type: none"> <li>リスクコントロール手段の妥当性を、一連の条件下で代表的な現象における代表的な使用者で試験することによって再評価する。</li> </ul>	<ul style="list-style-type: none"> <li>リスクコントロール手段を、様々なプラットフォーム上で様々な状態で検証する。</li> <li>最終リリースの前にリスクコントロール手段の回帰試験を行う。</li> <li>リスクコントロール手段が確実に実装され、試験されるように、トレーサビリティ分析及びカバレッジ分析を行う。</li> </ul>
5.6 ソフトウェアの統合及び統合試験			<ul style="list-style-type: none"> <li>最終リリースの前にリスクコントロール手段の回帰試験を行う。</li> <li>リスクコントロール手段が確実に実装され、試験されるように、トレーサビリティ分析及びカバレッジ分析を行う。</li> </ul>

表 D.1 - ライフサイクル/リスクマネジメント表 (続き)

活動	リスク分析	リスク評価	リスクコントロール
5.7 ソフトウェアテスト			<ul style="list-style-type: none"> <li>最終リリースの前にリスクコントロール手段の回帰試験を行う。</li> <li>リスクコントロール手段が確実に実装され、試験されるように、トレーサビリティ分析及びカバレッジ分析を行う。</li> </ul>
5.8 ソフトウェアリリース	<ul style="list-style-type: none"> <li>コンフィギュレーション項目及び相互依存性を含むコンフィギュレーション管理計画を特定する。</li> </ul>		<ul style="list-style-type: none"> <li>適切なバージョンのカスタムビルド、テスト及びSQUAPテストがリリースされることを検証する。</li> <li>ビルド環境がコンプライアンスレギュレーション下にあることを検証する。</li> </ul>
6 メンテナンスプロセス			
6.1 ソフトウェアメンテナンス計画の確立	<ul style="list-style-type: none"> <li>変更、機能向上、及び修理の場合のリスクマネジメントの取行方法、並びにリスクコントロールの妥当性及び追加的リスク軽減の機会を評価するための現場情報の監視及び分析を行う方法を計画する。</li> </ul>		
6.2 問題と修正の分析	<ul style="list-style-type: none"> <li>以前には認識されなかったハザード又は追加的なハザード及びハザードの原因を特定するために機器性能を分析する。</li> </ul>	<ul style="list-style-type: none"> <li>リスクコントロール手段及びリリースの再評価を再評価する。</li> </ul>	<ul style="list-style-type: none"> <li>追加的なリスクコントロール手段の必要性又は既存手段の修正の必要性を特定する。</li> </ul>
6.3 修正の実装		<ul style="list-style-type: none"> <li>開発プロセスと同等な方法のような変更の影響に焦点を置いている。</li> <li>既存のリリースと同等な方法のような変更の影響に焦点を置いている。</li> <li>ハザードの新しい問題を招く。</li> <li>新しいハザードを招く原因を特定する。</li> <li>安全関連エラーの回帰試験</li> </ul>	<ul style="list-style-type: none"> <li>IEC 62304:2006の編分節条 5.8 に従ったソフトウェアのリリース</li> </ul>

## 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がある、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、ということを探査するものである。セーフティケースはまた、医療機器の全寿命を通じ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プロセス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、次の要階が必要である。

- システムについての明示的決定事項
- 証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 フォールトツリー解析 (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<sup>2</sup>, リスクマネジメントの医療機器を組み込んだ情報技術 (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ス手法とその実装 (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/ss98web.pdf>
- [10] KELLY, T. P., セーフティケースマネ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] WEAYER, 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。

#### ① II.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 II a 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 II b である。

#### 3.2 規定 10

診断用の能動機器はクラス II a 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 II b 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 II a 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 II b 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の規制

サクラテック株式会社  
三浦

- 1.はじめに
- 2.GHTFの動向
  - 1) GHTFの組織
  - 2) Software臨時作業班及びその経緯
  - 3) Software臨時作業班の推奨事項
  - 4) GHTF各研究会の対応
  - 5) GHTF総会における三浦講演
- 3.EUの医療機器指令改訂版
- 4.IEC 62304概要及びN.B.対応例
- 5.厚科研の動向
- 6.まとめ

## 1.はじめに

- ・医療機器規制の主目的は安全性/有効性/品質の確保、安全性最優先。
- ・1996年に発行された米国の品質system規則(QSR)は前文で医療機器の回収/改修の多くがsoftwareを含む設計に起因していることを指摘している。ただし、QSRの本文にsoftwareに関する要求事項の具体的な規定はない。
- ・2004年～2006年、GHTF議長を担当したEUは、主な課題として①患者安全のための設計、②医療機器software、③新技術をあげた。
- ・2005年3月に開催されたGHTF運営委員会(SC)で、FDAは医療機器softwareの重要性を強調。その規制の検討に着手することを提案した。
- ・EUは、医療機器指令(MDD)を改訂。2010年内に加盟各国の法令として発効する。医療機器指令改訂版は、“Software validation”を要求している。

## 2.GHTFの動向(1)

- 1) GHTFの組織
    - 1-1) GHTF 研究班 (Study Group, SG)
      - ・SG 1: 市販前審査/医療機器規制全般
      - ・SG 2: 市販後監視/不具合事象報告
      - ・SG 3: 品質management system (QMS)
      - ・SG 4: QMSの法的監査
      - ・SG 5: 臨床評価
    - 1-2) GHTF 臨時作業班 (Ad Hoc Working Group, AHWG)
      - ・11種の臨時作業班が編成されており、次の2分野に分けられる。
        - a) GHTFの組織改革及び業務改善に関わる作業班。
        - b) 医療機器規制の新しい課題に対応するための作業班。
- それらには、Software、Combination productなどが含まれる。

## 2.GHTFの動向(2)

- 2) Software臨時作業班及びその経緯
  - 2-1) 活動(課題)の提案
    - ・2005年11月に開催されたGHTF SC会議で、Software臨時作業班の編成を決定。同作業班は、2006年5月、下記活動(課題)を提示した。
      - 1) 市販前審査におけるsoftwareを含む申請の検討
      - 2) SOUP (OTS) の評価
      - 3) Network接続された医療機器のCyber securityの確保
      - 4) Software安全性の設計基準
      - 5) Software開発life cycleの適合性評価
      - 6) Software開発processに使用されているsoftwareの評価
      - 7) System software設計のtraceability
      - 8) 電子署名



## 2. GHTFの動向(3)

- 2) Software臨時作業班及びその経緯
- 2-1) 活動(課題)の提案(続き)
  - 9) Network接続された医療機器における患者のprivacy保護
  - 10) Software processの監査及び監査員の資格
  - 11) Softwareのclass分類
- 2-1) 活動(課題)の絞り込み
  - 2006年6月に開催されたSC会議で、Software臨時作業班が提案した11件の活動案から、下記の3件を選択した。増加しつつあるsoftwareに起因する有害事象など緊急に対処すべき重要事項に焦点を合わせた。
  - 1) Softwareを含む市販前承認申請の審査の指針
  - 2) Software開発processに使用されるsoftware審査の指針
  - 3) Software process (QMS)の監査及び監査員の資格に関する指針

## 2. GHTFの動向(4)

- 3) Software臨時作業班の推奨事項
  - 2007年1月に臨時作業班がまとめ、2007年5月に開催されたGHTF SC会議に提案された推奨事項
  - 3-1) 市販前審査の関係(SG 1.1に対する推奨事項)
    - ・ Standalone softwareに関する基本要件の変更
    - ・ 基本要件のsoftwareの規定を、医療機器指令改訂版に合わせる。
    - ・ 用語“Software”を定義する(関連用語を含む)。
    - ・ STEDに、softwareとの相互関係に関する記述を追加する。
  - 3-2) 市販後監視の関係(SG 2.1に対する推奨事項)
    - ・ 不具合事象報告の事例を追加する(特にnetwork関係)

## 2. GHTFの動向(5)

- 3-3) 品質management system(QMS)の関係(SG 3.1に対する推奨事項)
  - ・ Task groupを編成する。
  - ・ 指針にsoftwareの調達 outsourcingに関する記述を追加する。
  - ・ Processの妥当性確認を、softwareの開発にも適用する。
- 3-4) QMS監査の関係(SG 4.1に対する推奨事項)
  - ・ SoftwareのQMSの法的監査指針を開発する。
- 3-5) 臨床評価の関係(SG 5.1に対する推奨事項)
  - ・ Softwareの一部に対して、臨床証拠を要求する。
- 3-6) 全般(共通)
  - ・ Accessory, dataに対する要求を追加する。
  - ・ SoftwareのQMSの法的監査基準を開発することの要否を検討する。

## 2. GHTFの動向(6)

- 4) GHTF各研究班の対応
  - ・ SG 1: Software臨時作業班の推奨事項を受け入れ、GHTF指針文書の“基本要件”の変更を検討している。
  - ・ SG 3: Software臨時作業班の推奨事項の検討を拒否。また、医療機器のsoftware及びその開発より製造用softwareが重要と主張。
  - ・ SG 4: 2009年5月に開催されたSG 4 Toronto会議で、Software臨時作業班の推奨事項の検討に着手した。
  - ・ 医療機器規制におけるsoftwareに対する主な対応は、①市販前審査、特に基本要件の変更及び②QMS規制及びその法的監査の指針に帰結する。後者は、ISO 13485:2003を改正することに他ならない。

## 2.GHTFの動向(7)

- 5) GHTF総会における三浦講演(問題提起)(1)
- 5-1) 規格 (standard)
- ・原則として、組織における適用は任意(自主的)。
  - ・規格開発時点における技術を網羅する。
  - ・規格によって認証制度がある。例えば、JIS Q 13485:2003認証のため、(財)日本適合性認定協会(JAB)が審査登録機関を認定する。
  - ・規格に対する重大な不適合に対して、認証が取り消されることがある。
- 5-2) 規則 (regulation)
- ・適用は強制。
  - ・重大な不適合に対して、各国規制当局は、回収/改修、出荷停止、工場閉鎖、罰金などを命じることがある。
  - ・効率(出力/入力)が問われる。有限資源による最大効果を期待。

## 2.GHTFの動向(8)

- 5) GHTF総会における三浦講演(問題提起)(2)
- 5-3) 規格と規則
- ・自主的/任意の適用を意図して開発された規格を、規則として強制すべきではない。
  - ・ISO 13485:2003は例外。規制目的のために、GHTF SG3とISO/TC 210/WG 1との合同作業班によって開発された。
  - ・ISO 13485:2003の“設計・開発”の要求事項は、4頁に過ぎない。本来、それにはsoftware開発も含まれる。
  - ・ISO 13485:2003の設計・開発の対する要求事項に、softwareに対する要求事項は含まれていない。
  - ・規則は凝縮された必須要求事項であり、規格より難しい。効率が求められる。

## 2.GHTFの動向(9)

- 5) GHTF総会における三浦講演(問題提起)(3)
- 5-4) GHTF指針文書“規格の役割”(GHTF SG 1/N12)の推奨事項
- ・国際規格は、整合化された規制processの“building block”である。
  - ・医療機器の基本要件に対する適合を立証するために、官民は国際規格の開発を推奨し、支援すべきである。
  - ・規則では、国際規格の利用を推奨すべきである。
  - ・規制当局は、国際規格を認知する仕組みを設けるべきである(例に、米国の認知規格、EUの整合規格がある)。
  - ・規格開発機関は、規格が基本要件への適合を立証するのに適するよう考慮すべきである。
  - ・規格の使用は、規制当局が強制すべきであると判断する特例を除き、任意である。製造業者が、それに対する代替案を自由に選択できるようにすべきである。

## 2.GHTFの動向(10)

- 5) GHTF総会における三浦講演(問題提起)(4)
- 5-3) 医療機器softwareの規格
- ・IEC 62304は医療機器softwareのための唯一の国際規格である。
  - 2002年～2006年、IEC 62AとISO/TC 210との合同作業班(JWG)によって開発された。
  - ・医療機器sectorは規制されており、何れの規格も、規制を支援するために採用される可能性がある。
  - ・そのため、IEC 62304の開発時に、日本は要求事項を簡略化することを提案した。ただし、それが十分に反映されたとは云えない。
  - ・IEC 62304は、規制目的に使用するには複雑過ぎ長過ぎる。Softwareの専門家向けであり、法的監査基準としては不適切である。

## 2. GHTFの動向(11)

### 5) GHTF総会における三浦講演(問題提起)(5)

#### 5-4) Software開発のkey point

- Softwareの製品表現 (product realization) に製造processはしない。
- Softwareの安全性/有効性/品質は、設計・開発processで作ら込まれる。
- Hazard識別が、安全確保のための“Risk management”の出発点。Softwareの場合、共通的なhazardはsoftware error (bug) である。その識別は容易ではないので、ISO 14971を、そのまま適用することは出来ない。
- Softwareの場合、errorの重大さと、その結果の深刻さとの間に相関関係はない (non-linear)。些細なprogram errorも、重大問題を惹起する可能性がある。
- 誤りを犯さない人はいない。Software error検出/是正がkey point。

## 2. GHTFの動向(12)

### 5) GHTF総会における三浦講演(問題提起)(5)

#### 5-5) 産業界からの提言

- 規格及び規則は製造業者に対して、安全性/有効性/品質確保のために、有効かつ有用な情報を提供すべきである。ISO 13485:2003はsoftwareの開発に対して不十分。
- “Vital few, trivial many”。規則は重要事項に焦点を合わせ、最小限の要求事項 (minimum requirements) とすべきである。
- 規則は凝縮された必須要求事項であるべきで、安全性/有効性/品質確保の最良手段を提示すべきである。
- 市販前審査の場合、組込み型softwareに対しては現行の規則が適用出来る。Softwareに対して新しい規則が必要な分野は、①Standalone softwareの市販前審査及び②QMSの要求事項(ISO 13485改正) である。

## 3. EUの医療機器指令(1)

- 2008年9月5日、医療機器指令改訂版 (MDD、2007/47/EC) が発行された。
- EU各加盟国によって、同指令改訂版を夫々の国の法令として発行される。それらは、2010年3月前後に発効する予定である。
- 同指令改訂版の“必須要求事項 (Essential Requirements)”は、GHTFの“基本要件 (Essential Principles)”の基礎になった。
- 医療機器指令は、1985年、Old approachの難点を解消するために提案されたNew approachに基づき付随する規格類と共に開発された。
- New approachの基本概念は、①指令には必須要求事項のみを記載する、②別に適切な技術的仕様を規格で規定する、③整合規格 (harmonized standard) に適合する製品は、指令に適合するものとみなすの3項目である。

## 3. EUの医療機器指令(2)

- 医療機器指令改訂版の前文に、EC委員会による推奨事項が記載されている。Softwareに関して、次の事項が推奨されている。
- ① 医療目的で使用するsoftwareを医療機器に含めることの明確化が必要である、② Standalone softwareであれ、組込みsoftwareであれ、software validationを必須要求事項に含めるべきである。
- 以上に基づき、医療機器指令の医療機器の定義が変更され、softwareを含めることが明記された。
- 必須要求事項の設計及び組立ての規定に、software validationが追加された。このvalidationは、ISO 9000に定義されている妥当性確認ではなく、software error検出/是正のための全ての活動を含む。
- 医療機器指令改訂版に、software validationの具体的規定はない。
- 医療機器指令改訂版の和訳は、薬事日報社から発行されている。

#### 4. IEC 62304概要及びN.B.対応例(1)

- 1) 名称: 医療機器software – Software life cycle processes
- 2) 適用範囲: 医療機器softwareに対する要求事項を規定する。  
Process, Activity, Taskが共通的枠組みを与える。
- 3) 適用対象: a) Software自体が医療機器(Standalone software)  
b) 医療機器に組み込まれるsoftware
- 4) 基盤となる要素: 品質management system及びRisk management system
- 5) 引用規格: ISO 14971 (ISO 13485:2003は引用規格ではない)
- 6) 規格を構成するprocess: Software開発process、Software保守process、Software risk management process、Software構成管理process、Software問題解決process
- 7) 基本方針: Software開発の各段階において、test及び検証を反復する。

#### 4. IEC 62304概要及びN.B.対応例(2)

- ・IEC 62304は、EUの整合規格として採用されている。
- ・EUでは整合規格を規則として使用する例が少なく、その強制に対する抵抗感は小さい。
- ・一部のN.B.は、既に、softwareに対するQMS監査の基準として、IEC 62304を使用している。
- ・GHTF SG 4は、softwareの法的監査基準について検討を開始。
- ・GHTFにおいて、QMSの法的監査基準は単一であり、それはISO 13485:2003であることは基本的合意事項である。関連する指針類(GHTF SG 3文書など)は、QMS法的監査に使用してはならない(GHTF指針文書類に明記されている)。
- ・IEC 62304は任意規格であり、規則として強制するには複雑かつ長過ぎる(60頁以上)。

#### 5. 厚生科学研究班の動向

- ・医療機器の国際動向を踏まえた、品質、有効性及び安全性の評価に関する研究を担う厚生科学研究班が編成された。
- ・その活動の一環として、医療機器softwareが取り上げられている。
- ・2009年は、その活動の最終年度に当たる。
- ・現時点まで、①GHTF Software AHWG、②IEC 62A～ISO/TC210 JWG、③FDA、④EUなどの医療機器softwareに関する活動を調査。
- ・2009年度は、米国及びEUのsoftwareに関する規制の実状の詳細調査及び医療機器softwareの規制に対する具体的提言をまとめる。

#### 6. まとめ

- ・この10年間、各方面から医療機器software、特にその安全性が重要であることが指摘されて来た。関連する有象無象の多発に因る。
- ・日本の場合、softwareを医療機器と定義することが先決。
- ・医療機器softwareの規制上の対応は、①市販前審査、特にstandalone softwareに対する基本要件の変更、②QMS規則の変更(ISO 13485改正)に絞られる。前者は進行中。後者は未着手。
- ・ISO/TC 176は、ISO 9001の次期改正版発行を2015年と予告した。過去の実績に基づけばISO 13485改正版発行は2018年以降になる。
- ・一方、IEC 62304は、規制目的にはなじまない。その骨子を、ISO 13485改正版に反映させるべきである。
- ・日本から積極的|上記の“原案”を提出することも検討すべきである。
- ・Risk managementの基礎は同一/同種不具合事象を再発させないこと。
- ・規則の開発/改正は事実(不具合事象)の分析に基づくべきである。EBMのように、EBR (Evidence Based Regulation)が求められる。

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”になるう。

### 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

	<u>監査（査察）基準</u>	<u>監査（査察）における不適合の指摘</u>
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箇所にとまとめた。(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

- 5. 5. 2 ソフトウェアユニット検証プロセスの確立
- 5. 5. 3 ソフトウェアユニットの合否判定基準
- 5. 5. 4 追加のソフトウェアユニット合否判定基準
- 5. 5. 5 ソフトウェアユニットの検証
- 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
  - 5. 6. 2 ソフトウェア結合の検証
  - 5. 6. 3 結合したソフトウェアの試験
  - 5. 6. 4 結合試験の内容
  - 5. 6. 5 結合試験手順の検証
  - 5. 6. 6 レグレッションテストの実施
  - 5. 6. 7 結合試験記録の内容
  - 5. 6. 8 ソフトウェア問題解決プロセスの使用
- 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
  - 5. 7. 2 ソフトウェア問題解決プロセスの使用
  - 5. 7. 3 変更後の再試験
  - 5. 7. 4 ソフトウェアシステム試験の検証
  - 5. 7. 5 ソフトウェアシステム試験記録の内容
- 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
  - 5. 8. 2 既知の残留異常の文書化
  - 5. 8. 3 既知の残留異常の評価
  - 5. 8. 4 リリースしているバージョンの文書化
  - 5. 8. 5 リリースしたソフトウェアの作成方法の文書化
  - 5. 8. 6 アクティビティ及びタスクの完了確認
  - 5. 8. 7 ソフトウェアのアーカイブ
  - 5. 8. 8 ソフトウェアリリースの反復性の確保
  
- 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
    - 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
    - 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
    - 7. 1. 3 公開された SOUP 異常リストの評価
    - 7. 1. 4 潜在的原因の文書化
    - 7. 1. 5 イベントシーケンスの文書化



<簡易指針構成案>

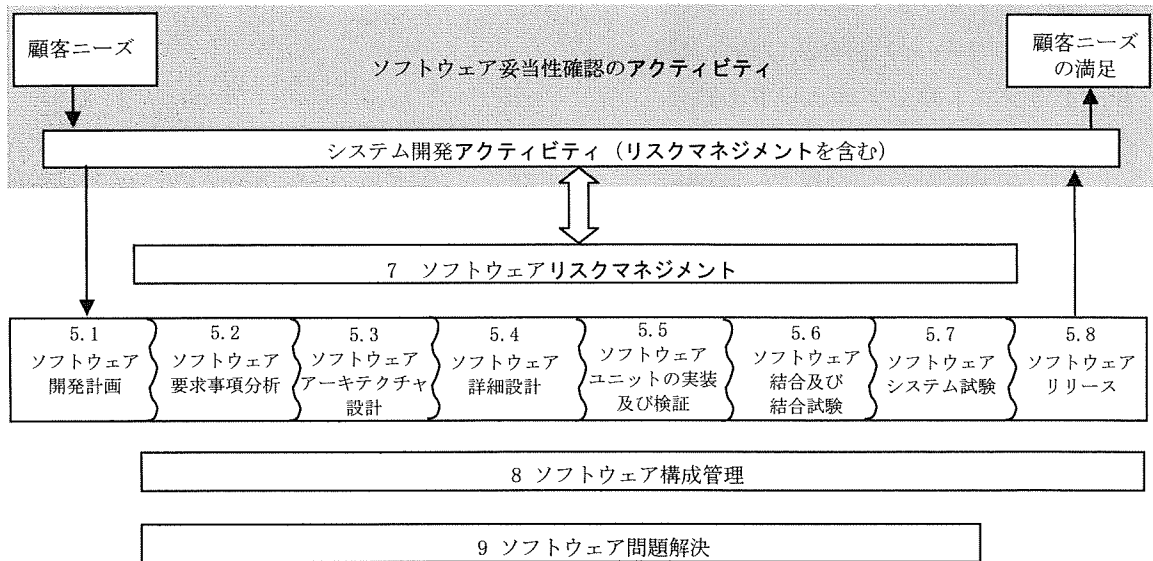


図1—ソフトウェア開発プロセス及びアクティビティの関連図

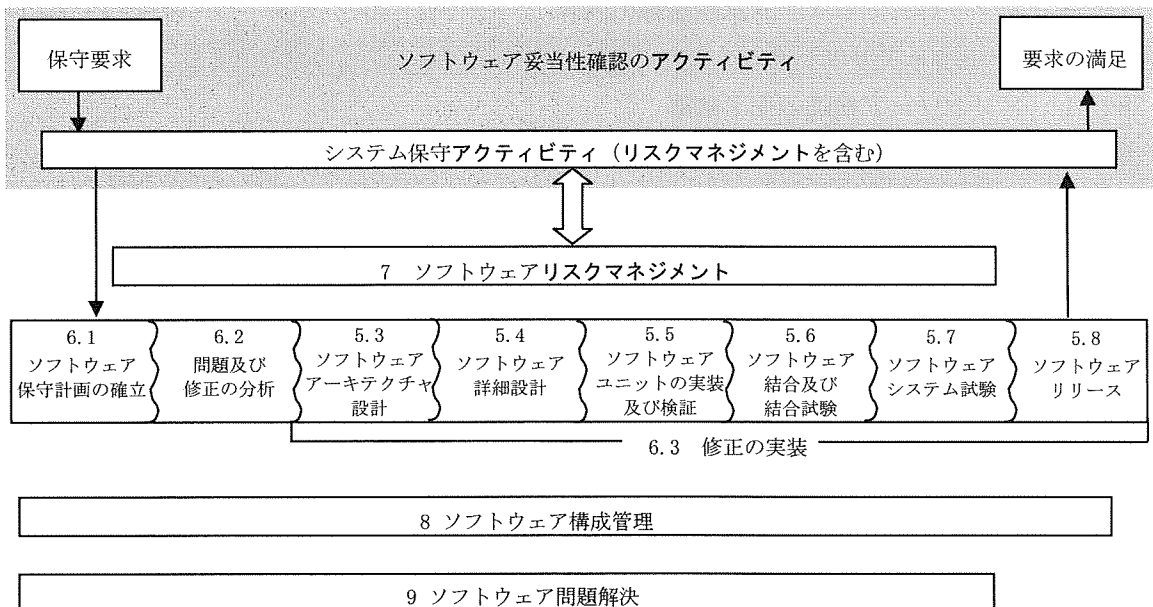


図2—ソフトウェア保守プロセス及びアクティビティの関連図

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することができる。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