

低—欠陥または潜在的な設計上の欠陥によって、患者および操作者またはそのいずれかが損傷を来たすとは考えられない場合、重要度は「低」とする。

重篤な損傷—以下の損傷または疾患をいう。米国連邦規則集21 CFR 803.3 (aa)の医療機器報告 (MDR) 規則を採用した。

- i. 生命を脅かすもの。
- ii. 永続的な身体機能の障害または永続的な身体構造の損傷に至るもの。
- iii. 永続的な身体機能の障害または永続的な身体構造の損傷を除くために内科的または外科的介入を必要とするもの。

永続的—ここでは、身体構造または身体機能の不可逆的な障害または損傷をいい、軽微な障害または損傷は除く。

### 2.2.2 決定プロセス

緩和策を講じる前に、以下の5項目の重要な質問に順次回答していくことにより医療機器用ソフトウェアの重要度を決定する。いずれかひとつ（または複数）の質問に対する回答が「はい」の場合、当該ソフトウェアの重要度は「高」または「中」と考えられる。いずれかの質問に対する回答が「いいえ」の場合には、次の質問に進む（図2参照）。

1. 当該医療機器用ソフトウェアは、生命支援装置または生命維持装置を制御するものであるか。
2. 当該医療機器用ソフトウェアは、放射線治療システム、除細動器のような死亡または重篤な損傷を引き起こすおそれのある危険なエネルギーの放出を制御するものであるか。
3. 当該医療機器用ソフトウェアは、治療法の送達を制御し、送達の誤りまたは異常によって死亡または重篤な損傷を引き起こすものであるか。
4. 当該医療機器用ソフトウェアにより処置または治療を決定する診断情報が得られ、適用

を誤った場合には重篤な損傷または死亡を引き起こすおそれがあるか。

「はい」の場合、特に診断情報が紛らわしいものであるか不正確である場合、あるいは不適切な治療が行われると考えられる場合には、当該医療機器の重要度は「高」とする。このような状況では、重篤な医学的状態の不適切な診断または不適切な処置によって患者に重篤な損傷を負わせることがある。

医療機器より臨床医が独自の判断を下すことはないと考えられるデータが得られることがある。以下に考えうるシナリオの例を示す。

高：ユーザに知識がない場合に危険なものとなりうる放射線を放出する放射線治療システム。

中：患者の背景、症状および他の検査に基づいて、迅速かつ容易に看破され無効にされる不正確な診断情報を提供するシステム。

後者の場合、医療機器により得られる情報を無効にする臨床的判断が下される場合には（データが不正確である場合にも）、当該医療機器の重要度は低いと考えられる。

5. 当該医療機器用ソフトウェアによってバイタルサインのモニタリングが行われ、介入が必要な致命的な状況に対する警告が得られるか。

以上の質問のうちいずれかの回答が「はい」であれば、次の質問に進む。

当該ソフトウェアは患者に直接影響を及ぼし、欠陥または潜在的な設計上の欠陥によって患者が死亡または重篤な損傷を来すおそれがあるか、あるいは間接的に患者に影響を及ぼし、不正確な情報または遅れた情報によって患者が死亡または重篤な損傷を来すおそれがあるか。

「はい」の場合、重要度は「高」とする。「いいえ」の場合には次の質問に進む。

当該ソフトウェアは直接患者に影響を及ぼし、欠陥または潜在的な設計上の欠陥によって、患者が軽微ないし中等度の損傷を来たすおそれがあるか、あるいは間接的に患者に影響を及ぼし、不正確な情報または遅れた情報によって、患者が重篤でない損傷を来たすおそれがあるか。

「はい」の場合、重要度は「中」とする。「いいえ」の場合、重要度は「低」とする。

以上をまとめると、審査官は、医療機器用ソフトウェアの重要度決定の根拠となる完全性の高い証拠を要求する必要がある。

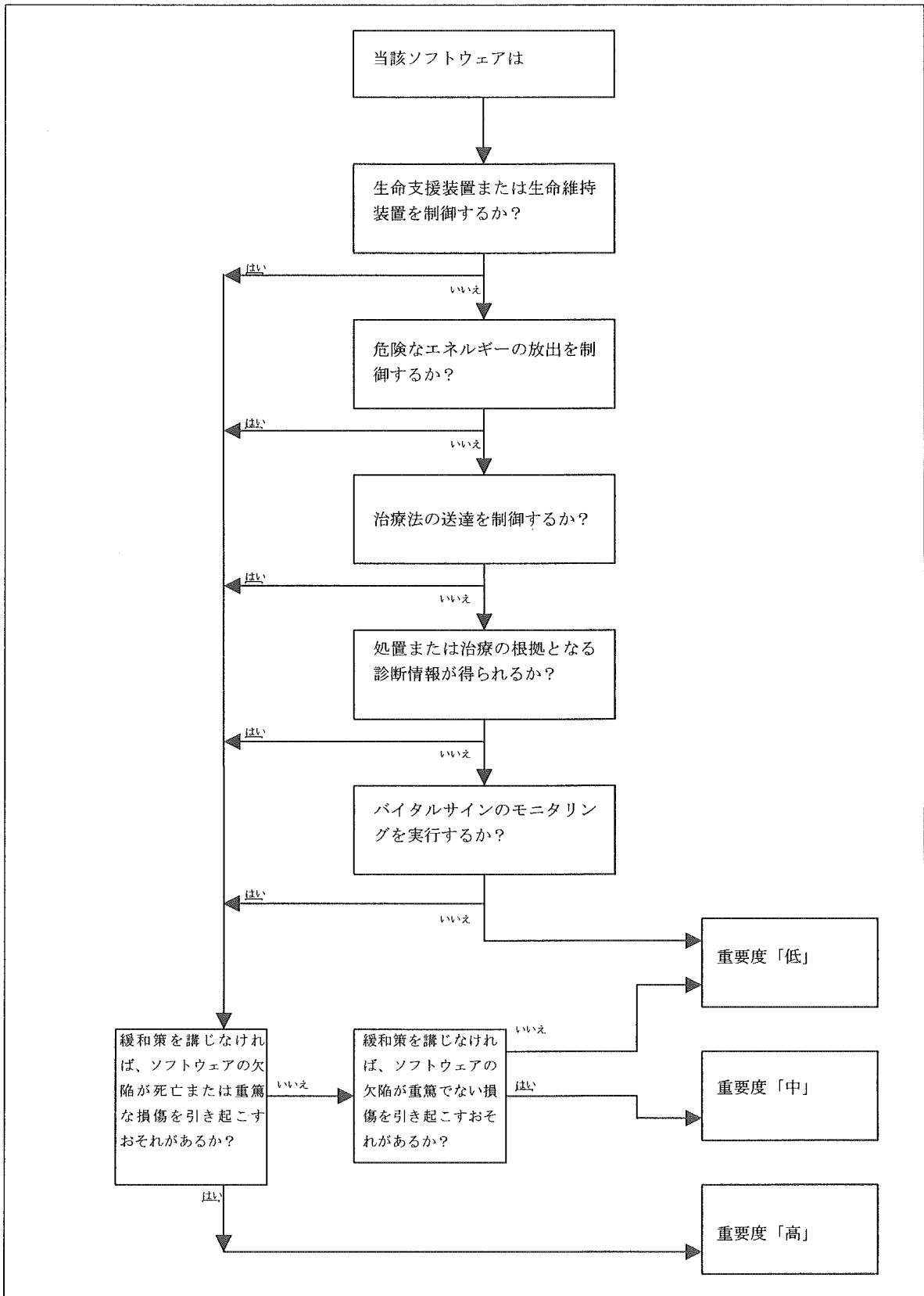


図2：重要度の決定

### 第3項 市販前申請に含める文書

市販前申請に含めるソフトウェア文書は、医療機器の用途、ソフトウェアの重要度および市販前申請の種類に応じたものでなければならない。それぞれの重要度において医療機器に関して一般に提出されるべき文書の種類を表1にまとめる。なお、特定の医療機器に関するガイダンスがあれば、それを表1に優先すること。製造業者はさらに関連情報を得るため、申請を提出する前にODE審査部門と連絡をとることができる。

以下の考察を通じて、表1に記載したソフトウェア文書の各カテゴリーについてさらに情報が得られる。ソフトウェアの重要度によっては、各カテゴリーに記載した文書の一部または全部について製造業者が提出する必要がない場合がある。

#### 3.1 重要度

当該ソフトウェアの重要度とそれを裏付ける根拠を示す（詳細については第2項参照）。重要度が「高」であり、以前にこのタイプの医療機器の市販前申請をODEに提出していない場合には、申請提出前に該当する部門と連絡をとることが強く推奨される。

#### 3.2 ソフトウェア記述

ソフトウェアによって制御される医療機器の特徴の包括的な概要を示し、意図する操作環境を記載する。

##### 3.2.1 ソフトウェアにより制御される医療機器の特徴

当該医療機器において当該ソフトウェアはどのような役割を演じているか。当該ソフトウェアは何を実行し、重要なことには、何を実行しないか。ユーザと当該ソフトウェアはどのように相互作用するか。ユーザは当該ソフトウェアのどのような機能を制御または変更することができるか、変更することができないのはどのような機能か。もしあれば、ハードウェアは当該ソフトウェアのどのような特徴を無効にするかまたは支援するか。

このような情報は一般にパラグラフ形式で記載し、主要または重要なソフトウェアの特徴が目立つようにする。ソフトウェア要件の詳細については、3.5項ソフトウェア要件仕様書に記載している。

### 3.2.2 操作環境

意図する操作環境には以下の項目を記載すること。

- プログラミング言語
- ハードウェアプラットフォーム
- オペレーティングシステム（該当する場合）\*
- 市販コンポーネントの使用（該当する場合）\*

\* 当該医療機器が市販コンポーネントを使用している場合には、医療機器における市販ソフトウェアの使用に関するFDAガイダンス（案）（FDA's (draft) Guidance for Off-the-Shelf Software Use in Medical Devices）を参照すること（付属書C.6参照）。

### 3.3 医療機器のハザード解析

重要度に関する申請資料には用途、ハードウェアおよびソフトウェアに起因する医療機器のあらゆるハザードを考慮に入れた医療機器のハザード解析を含める必要がある。ハザード解析は以下のものを対象とすること。

- a) 危険な事象
- b) ハザードの重要度
- c) ハザードの原因
- d) 制御の方法
- e) 医療機器の設計および要件の側面を含み、危険な事象を排除、緩和、または警告するような是正措置。その適切性に関する考察を含む。
- f) 制御の方法が正確に実施されたことを明らかにするための試験

このような情報は通常表形式で記載する。製造業者は、ハザード解析を実施する場合には、当該医療機器の意図的な誤用または不注意による誤用によって生じたハザードをはじめ、予測可能なハザードを全て対象とすること。

ソフトウェアの故障に関する木解析（fault tree analysis; FTA）が有用な場合がある。特定された個々のハザードについて、そのハザードを引き起こすおそれのある状態を見出す

ために詳細な分析を実施する必要がある（上記(c)参照）。手法には様々なものがあり、そのひとつには、好ましくない事象を特定し、ハザードの原因を明らかにするため同事象を後ろ向きに検討する故障の木解析がある。

### 3.4 ソフトウェア要件仕様書（SRS）

ソフトウェア要件仕様書にはソフトウェアの要件を記載する。通常、これには機能、性能、インタフェース、設計および開発に関する要件が含まれる。SRSに記載する典型的な要件の例を挙げる。

- a) マイクロプロセッサ、記憶装置、センサー、エネルギー源、安全機能、通信をはじめとするハードウェアの要件
- b) プログラミング言語およびプログラムサイズ
- c) システムコンポーネント間の対話およびユーザとの対話をはじめとするインタフェースの要件（プリンタ、モニタ、キーボード、マウスなど）
- d) ソフトウェアの性能および機能の要件。例を以下に挙げる。
  - 治療、診断、モニタリング、警告、分析および解釈のアルゴリズムまたは制御特性（必要に応じて、全文の参考文献または裏付けとなる臨床データを提示する）
  - ソフトウェアによる医療機器の制限
  - ソフトウェアの内部試験および内部検査
  - 誤りおよび割込みの取扱い
  - 故障検出、耐久性および回復の特性
  - 安全要件
  - タイミングおよびメモリの要件
  - 市販ソフトウェアの識別（該当する場合）

重要度が「低」の医療機器については、通常SRSの機能の要件の項のみを提示すれば十分である。重要度が「中」および「高」の医療機器については、完全なSRSを提示する必要がある。

### 3.5 アーキテクチャ設計図

重要度が「低」の医療機器については、申請資料には機能的サブシステムへのソフトウ

エアの分配を示す図を記載する。全てのソフトウェアモジュールを含める必要はない。この図では当該機能レベルでのソフトウェアアーキテクチャを示すこと。

重要度が「中」および「高」の医療機器については、さらに詳細な設計図が必要であるが、機能レベルに焦点をあてたものとする。申請資料には機能モジュールの一覧のほか、ソフトウェアの要件を満たす上でそれぞれのモジュールが演じている役割を記載する。

### 3.6 設計仕様書

ソフトウェアの設計仕様書とは、プログラムが何をすべきか、それをどのようにすべきかを記載したものである。これには高水準の設計の要約に加え、プログラマーが任意で設計に関する決定を下す必要がないような詳細な仕様を記載する必要がある。ソフトウェアの設計仕様書には、以下に挙げる要素に関する文書を含めるものとする。いくつかの要素については参照しやすいよう別々の文書をつけることがある。

- 予め設定したプログラムの受け入れに関する基準をはじめとするソフトウェア要件仕様
- 開発基準およびプログラミング基準
- ハザード解析
- システム文書（プログラムが機能するためのコンテキスト。たとえば、システム文書またはコンテキスト図）
- 使用するハードウェア
- 測定または記録するパラメータ
- 論理（論理構造、制御論理、論理的処理）
- データ構造およびデータ流れ図
- 変数（制御およびデータ）の定義およびその変数が使用されている場所に関する説明
- 誤りおよび警告のメッセージ
- サポートソフトウェア（オペレーティングシステム、ドライバおよび他のアプリケーションソフトウェアなど）
- 通信リンク（当該ソフトウェアの内部モジュール間のリンク、サポートソフト



トウェアとのリンクおよびハードウェアとのリンク)

- セキュリティ対策（物理的セキュリティおよび論理的セキュリティ）

### 3.7 トレーサビリティ分析

要件、設計仕様、ハザードおよびバリデーションを関連づけるトレーサビリティ分析またはトレーサビリティマトリックスを提示する。このような業務と文書間のトレーサビリティが重要である。この文書は、情報がどこにあるかを明らかにするのに必要な関連性を示す地図としての機能を果たしている。共通の組織構成および共通の付番体系によってトレーサビリティを文書化することは可能であるが、申請資料に記載される情報を審査の指針とするには、適切な情報を提示する必要がある。

### 3.8 開発

重要度が「中」および「高」の医療機器については、依頼者がソフトウェアの開発ライフサイクル計画の要約（通常2～4ページ以内）を提示する。この要約には様々なソフトウェア開発ライフサイクル業務を管理するために適切なプロセスを記載する必要がある。重要度が「中」の医療機器については、依頼者はコンフィギュレーション管理および保守管理計画の要約を提示する。

また、重要度が「高」の医療機器については、申請資料にはソフトウェアの開発プロセスのほか、コンフィギュレーション管理および保守管理計画時に作成した制御／ベースラインに関する文書の注釈付き一覧を含めること。

### 3.9 バリデーション、確認および試験

ソフトウェアの確認には、ソフトウェア開発プロセスの各段階において、その段階に規定された要件を全て満たしていることを確認するため、ソフトウェアとその関係文書の様々な分析、評価、保証および試験を系統的に適用することが含まれる。ソフトウェアバリデーションにもほぼ同じ解析手法を用いるが、この場合には医療機器の最終製品（これに内蔵されるソフトウェアを含む）が用途に適したもので、信頼性がありかつ安全であることを可能な範囲内でさらに確認することができる。

次のような試験情報を提示する。

- a) ソフトウェアの重要度が「低」と考えられる医療機器
  - ソフトウェアの機能試験計画。適合・不適合基準、データおよび結果の分析も提示する。
- b) ソフトウェアの重要度が「中」と考えられる医療機器
  - 単体レベル、統合レベルおよびシステムレベルでの確認業務の詳細
  - システムレベルの試験プロトコール。適合・不適合基準および試験結果を含む。
- c) ソフトウェアの重要度が「高」と考えられる医療機器
  - 単体レベル、統合レベルおよびシステムレベルでの確認業務の詳細
  - 単体レベル、統合レベルおよびシステムレベルの試験プロトコール。適合・不適合基準、試験報告、要約および試験結果を含む。

試験情報には全て当該ソフトウェアのバージョン識別子および修正識別子を記載し、(該当する場合には) 試験結果の考察に以下の項目がどのように検査されたかを含めること。

- 故障、警告およびハザードの試験
- 誤り、範囲検査および境界値の試験
- タイミングの解析および試験
- 特殊なアルゴリズムおよび解釈の試験および解析
- 負荷試験
- 医療機器のオプション、付属品およびコンフィギュレーションの試験
- 通信試験
- メモリ使用量の試験
- 市販ソフトウェアの適格性 (付属書C.6参照)
- 受入試験およびベータ試験
- 回帰試験

### 3.10 リビジョンレベル履歴

重要度が「中」および「高」のソフトウェアについては、申請資料には開発サイクル時のソフトウェアの重要な変更を全て記録した修正履歴のログを含めること。

### 3.11 未解決の異常（バグ）

重要度が「中」および「高」のソフトウェアについては、申請資料にソフトウェアに関する未解決の全異常の一覧を含めること。それぞれの異常について、問題および医療機器の性能に対する影響のほか、適切な場合には問題修正の計画または期限を示す。ユーザに対しては、バグの一覧を当該医療機器のラベル表示に記載し通知すること。

### 3.12 リリースバージョン番号

いずれの重要度についても、申請資料には市販医療機器に内蔵されるソフトウェアのリリースバージョン番号および日付を記載するものとする。

項番号	ソフトウェア文書	重要度「低」	重要度「中」	重要度「高」
2, 3.1	重要度	全重要度		
3.2	ソフトウェア記述	全重要度		
3.3, 4.3	医療機器のハザード解析	全重要度		
3.4, 4.2	ソフトウェア要件仕様書 (SRS)	SRSのうちソフトウェア機能の要件	SRS	
3.5	アーキテクチャ設計図	機能的サブシステムへの当該ソフトウェアシステムの分配を示す図	機能的サブシステムへの当該ソフトウェアシステムの分配を示す図、機能モジュールの一覧、個々の機能モジュールがどのように要件を満たしているかに関する説明	
3.6	設計仕様書	申請に必要な文書なし	ソフトウェア設計仕様文書	
3.7	トレーサビリティ分析	申請に必要な文書なし	各要件、特定したハザードおよび確認・バリデーション試験間のトレーサビリティ	
3.8, 4.1	開発	申請に必要な文書なし	ソフトウェアライフサイクル開発計画の要約。コンフィギュレーション管理および保守管理業務の要約を含む。	ソフトウェアライフサイクル開発計画の要約。開発プロセス時に作成した制御に関する文書の注釈付き一覧。コンフィギュレーション管理および保守管理計画に関する文書を含む。
3.9	バリデーション、確認および試験 (VV&T)	ソフトウェア機能試験計画、適合・不適合基準および結果	単体レベル、統合レベルおよびシステムレベルでのVV&T業務の詳細。適合・不適合基準および試験結果を含むシステムレベルの試験プロトコル。	単体レベル、統合レベルおよびシステムレベルでのVV&T業務の詳細。適合・不適合基準、試験報告、要約および試験結果を含む単体レベル、統合レベルおよびシステムレベルの試験プロトコル。
3.10	リビジョンレベル履歴	申請に必要な文書なし	修正履歴のログ	
3.11	未解決の異常 (バグ)	申請に必要な文書なし	当該医療機器に残存するエラーおよびバグの一覧、操作者の使用およびヒューマンファクターをはじめ、安全性または有効性に影響を及ぼすものでないと判断した理由。	
3.12	リリースバージョン番号	いずれの重要度についてもバージョン番号および日付		

表1 市販前申請に含める文書

## 第4項 ソフトウェアライフサイクルにおけるリスク管理業務

本稿では、リスク管理業務の概要と、このような業務が医療機器のソフトウェアライフサイクルのどの段階に一致するかを記載する。ソフトウェアライフサイクルについて簡潔に説明する。ライフサイクル業務の詳細については、「ソフトウェアバリデーションの一般原則」に関するFDAガイダンスを参照のこと。

### 4.1 ライフサイクルモデルおよび開発方法

ソフトウェアライフサイクルは医療機器のライフサイクル全体の縮図である。製造業者は、製造する医療機器および製造業者の組織に適したソフトウェアライフサイクルモデルおよび開発方法を選択することができる。一般に、選択したライフサイクルモデルにはリスク管理、要件分析および要件仕様、(上位レベルおよび詳細な)設計、実施(コーディング)、統合、バリデーションおよび保守管理に関する業務を含めるものとする。ソフトウェアライフサイクルモデルはわかりやすく、不足なく文書化され、結果重視で監査可能かつ追跡可能なものであり、開発プロセスにおいて適切なフィードバックを促進するものでなければならない。“Code-and-fix”というアプローチがよく用いられているが、開発プロセスの初期にリスクの特定、品質の評価、異常の特定ならびに排除の方法が得られないため、ソフトウェアライフサイクルに対してはそれほど効果的であるとはいえない。

ライフサイクルモデルにはウォーターフォール型、スパイラル型、進化型、インクリメンタル型、トップダウン機能分割型(または段階的詳細化)、形式的変換型など様々なものがある。医療機器のソフトウェアは、選択したモデルが十分なリスク管理業務とフィードバックプロセスが組み込まれているものである限り、以上のモデルまたは他のモデルを用いて製造することができる。サブシステムおよびサブコンポーネント(ハードウェア、ソフトウェア、材料など)に様々なライフサイクルモデルおよび方法を混ぜることもできる。用語はモデル毎および方法毎に異なる場合がある。図3にリスク管理業務とライフサイクル業務との関係を示した一般的なライフサイクルモデルを示す。

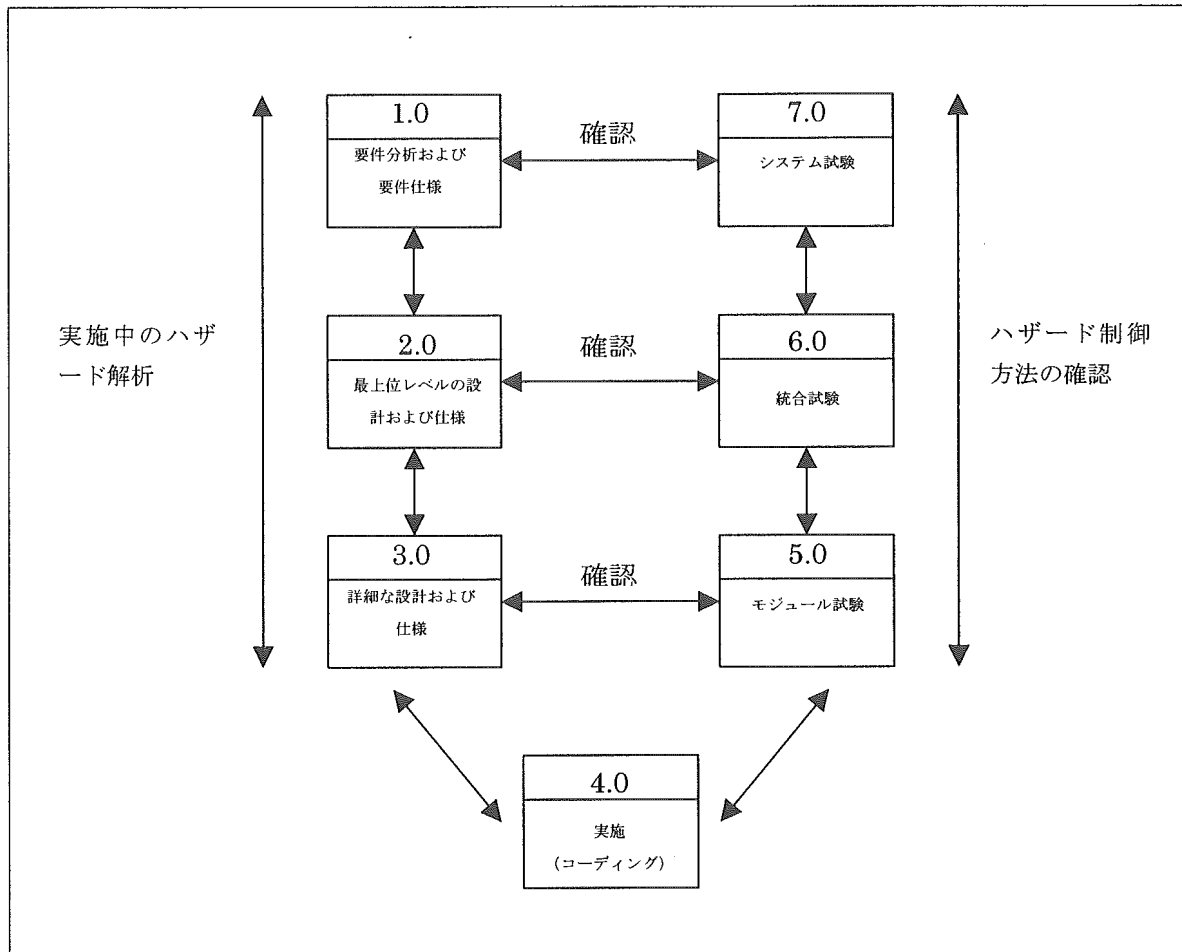


図3：一般的なソフトウェアライフサイクルモデル

#### 4.2 要件分析および要件仕様

医療機器の設計プロセスの初期には、顧客またはエンドユーザが求める医療機器の機能および性能に関する要件を特定および分析し、その医療機器（システム）の要件のうちいずれの要件をソフトウェアに配分するかを決定する業務がある。この時点で、特にリスクにかかわる機能について、ソフトウェアが医療機器において果たす役割を規定することが重要である。このような要件に関する業務では、ソフトウェアによって実行、制御または監視される機能を文書化する。ヒューマンファクター、機能特性、応答時間、アウトプット、安全要件といったソフトウェアの品質特性とともに、受入基準を規定する。

要件はライフサイクルプロセスを通じて更新されるものであるため、ソフトウェアの安全要件は予備的ハザード解析および実施中のリスク管理業務から導き出す。危険なソフト

ウェアの機能を全て特定し評価するほか、そのような機能によるリスクが許容レベルまで緩和されることを明らかにすることができるよう追跡する。

#### 4.3 リスク管理

リスク管理とは、リスク分析とリスク制御業務を組み合わせたものである。リスク分析は医療機器の使用によるリスクを推定するのに用い、リスク制御はそのリスクを許容レベルまで緩和するのに用いる。通常、製造業者はリスク分析およびリスク制御業務の規定および管理に用いるリスク管理計画を整備している。このような業務は医療機器のライフサイクルを通じて実施される。リスク分析は、エンティティとしてのほかに主要コンポーネント/サブシステムとしての医療機器について実施する必要がある。ソフトウェア、電子機器、生体材料などのリスク分析が医療機器レベルおよびサブシステムレベルで効果的に統合され分析されるよう、適切な方法を選択すること。

このプロセスでは、製造業者には付属書Bに引用した様々な国家のおよび国際的合意基準が有用であると思われる。

リスクにはコスト、完全性、セキュリティ、安全性など多くの側面がある。FDAによる医療機器の審査では、リスクの安全性に関する側面に主な焦点をあてている。ソフトウェアのリスク管理は医療機器の総合的なリスク管理のサブセットである。ハザードの影響の程度が低下するか、ハザードが発生する可能性が低下するとリスクが軽減される。ハザードが具体的にソフトウェアと関係する場合、ハザードが発生する可能性はソフトウェアの欠陥率と直接相関する。ソフトウェアの欠陥率を正確に算出するのは、不可能ではないとしても困難である。このため、ハザードが発生する可能性が許容レベルを超えるほど高いと仮定すると、ハザードの重大性を制御するためにソフトウェアのリスクを軽減し緩和させる方法を用いる必要がある。

##### 4.3.1 リスク分析業務

リスク分析にはハザード解析およびリスク推定が含まれる。ハザード解析では考えうる医療機器のハザードに関する確認書が作成される。あらゆる合理的に予測可能な状況について、考えうる医療機器のハザードが特定される。ハザード解析は確立された手順に従っ

て実施する。ハザード緩和の有効性を評価し新たなハザードがもたらされたかどうかを評価するには、ハザード解析を要件が規定されるライフサイクルの初期に開始し、開発が進むに従って更新する必要がある。医療機器のハザードに関しては、患者、操作者、傍観者、サービス担当者および周囲の環境に対する影響について検討すること。

特定されたそれぞれのハザードについて、誘発原因の一覧を作成する。誘発原因はヒューマンファクター、ハードウェアの故障、ソフトウェアの故障、統合の誤りおよび環境条件のいずれかに由来すると考えられる。ハザード解析の実施には様々な方法（故障の木解析、欠陥モード影響解析など）を用いることができる。一般に、最終製品に関する情報が多く得られるよう、開発ライフサイクルの段階毎に別々の方法を用いる。製造業者は製造する医療機器およびその用途に適した方法を選択すること。本書では、ソフトウェアに関連するハザードを、誘発原因または主な寄与原因がソフトウェアにある医療機器のあらゆるハザードであると定義する。ソフトウェアに関連するハザードについては、ハザード解析に関する文書では、医療機器レベルからソフトウェアの特定の原因までのトレーサビリティを明らかにすること。

特定されたそれぞれのハザードについてリスク推定を実施する。リスク推定は、結果として生じる影響の程度および発生の可能性に基づいて実施する。それぞれのハザードに重大性レベルを割り当てる。重大性レベルは本書で用いる重要度の用語（高、中および低）を用いて定義することができる。

それぞれのハザードについて、発生の可能性を割り当てる。ソフトウェアに関連するハザードの場合、この可能性のひとつの要素がソフトウェアの欠陥率に直接関連する。ソフトウェアの欠陥率は、系統的（vs 偶発的）なソフトウェアの故障を反映するものである。系統的な故障の性質上、ソフトウェアの欠陥率を正確に推定するのは困難である。ソフトウェアの欠陥率の正確性を確認することができない場合には、推定したソフトウェアの欠陥率に基づいてリスクを制御するのは適切でないと思われる。ソフトウェアに関連するハザードについては、製造業者がソフトウェアの欠陥率が許容レベルを超えると考える場合、ソフトウェアの欠陥率を求める必要はない。製造業者はこのアプローチを用いることにより、ハザードの程度を低下させるか、排除する設計ソリューションの開発に資源を集中さ



せることができる。

医療機器には複数のハザードがみられる場合がある。それぞれのハザードにも同じく、複数の原因があると思われる。最終目標は、それぞれのハザードに対して考えうる原因を全て明らかにすることである。ハザードの原因を明らかにする上での取り組みおよび詳細の程度は、結果として生じる影響の程度に応じたものとする。ハザードとその原因を明らかにし、重大性を分類するのに用いた方法を文書化すること。

#### 4.3.2 リスク制御業務

リスク制御の目的は、ハザードを排除するか推定されるリスクを許容レベルまで緩和することにある。リスク制御の方法はハザードの原因によって決まる。いくつかのリスク制御の方法およびその優先度を以下に示す。

- 1) 本来安全な設計または再設計によりリスクを排除するか軽減させる。
- 2) 保護対策によりリスクを軽減させる。
- 3) 十分な警告など適切なユーザ情報によりリスクを軽減させる。

製造業者は特定されたそれぞれのハザードについて、リスクを排除するか許容レベルまで軽減するのに用いたリスク制御の方法を明らかにする。製造業者は、ソフトウェアに関連するそれぞれのハザードについて、リスク制御の方法を実施した後の重大性レベルを示すこと。最終目標は、あらゆるソフトウェアに関連するハザードを重要度「低」まで軽減することである。

それぞれのハザードと原因の組み合わせに関して、残存するリスクが適切であるかどうかを判断する。次に、リスク制御の措置によって新たなハザードが生じたかどうかを判断する。新たなハザードが生じた場合には、このプロセスを繰り返す。図4を参照すると、考えうるそれぞれのハザードについてはステップ2～7を繰り返し、考えうるそれぞれの原因についてはステップ4～6を繰り返している。考えうるハザードを全て評価すると、医療機器の安全性に関する最終判断が下される。

#### 4.3.3 文書化

進行中のリスク管理プロセスにより、いくつかの作業生産物が生じる。ハザード解析単独では十分でない。製造業者は以下の項目も文書化する必要がある。

- 1) 特定されたハザードの詳細
- 2) そのハザードの重大性レベル（高、中または低）
- 3) 特定のソフトウェアにみられるハザードの原因。これによりソフトウェアの特定の位置まで追跡することができる。
- 4) 使用したリスク制御の方法
- 5) 使用したリスク制御の方法を確認するのに用いた試験または確認の方法
- 6) リスク制御の方法を実施した後のハザードの重大性レベル
  - 推定した重大性レベルおよびそのカテゴリー
  - 実施したリスクの軽減および緩和の方法、およびその有効性の評価方法
  - 安全機能の遂行を明らかにする試験および評価

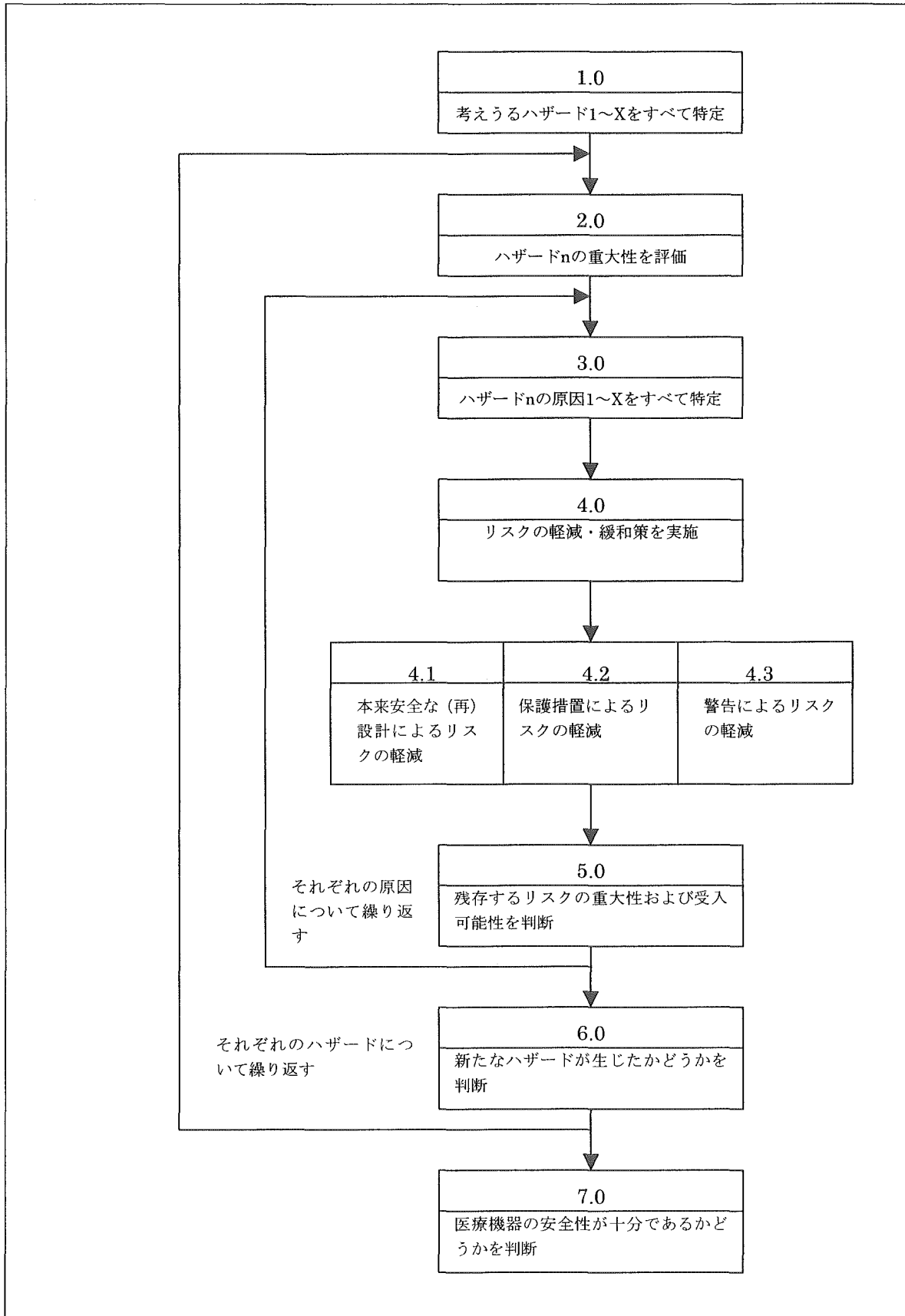


図4：リスク管理プロセス（IEC 60601-1-4から変更を加えて転載した）

## 付属書 A 技術的問題および特殊なテーマ

この付属書では、ソフトウェアおよび市販前申請に関する種々の特殊なテーマを簡潔に考察している。このようなテーマを記載したのは、審査官に対してソフトウェアにはこのような特徴が含まれており、特別な注意またはさらなる調査が必要であるという「注意」を喚起するためである。個々のテーマに関するさらに包括的な考察については、付属書DおよびEの参考文献を参照すること。

### A.1 人工知能、エキスパートシステムおよびニューラルネットワーク

人工知能（AI）は、コンピュータ機器が人間をはじめとする生物とほぼ同じ行動および反応を示す方法および技術を検討するコンピュータ科学における研究分野のひとつである。人工知能の研究から導き出された概念が問題解決タスクに適用された領域が、エキスパートシステムと人工ニューラルネットワークである。

エキスパートシステムでは、専門家の経験をソフトウェアによって実行可能な一組のアルゴリズムに集約させることにより、きわめて特殊な人間の知識または専門知識のモデル化を試みている。エキスパートシステムの多くは（規則、経験則またはオブジェクトあるいはデータ間の関係からなる）知識ベースと、選択した基準に従ってその知識を操作する推論エンジンからなる。エキスパートシステムでは、狭く明確な範囲または領域における問題を解決するために、システムに入力する事実に関してこのような規則または経験則を用いる。エキスパートシステムの典型的な応用例には、回路の分析および設計、故障の検出および診断、自動財務評価およびローン処理、医学的診断および治療の提案が挙げられる。

人工ニューラルネットワーク（ANN）は自然または生物学的なニューラルネットワークにおいて示される原則を手本にしたデータ処理アーキテクチャである。人工ニューラルネットワークの多くは、大規模なデータセットに適用される非線形機能を示すか処理するために用いられる。人工ニューラルネットワークエンジンは、ソフトウェア、ハードウェア（並列処理アーキテクチャを用いて）または両方の組み合わせにおいて実行することができる。人工ニューラルネットワークは、データにみられる傾向またはパターンの検出に適しており、通常発話および自然言語の処理、機械視覚および画像認識、財政動向の予測、