医療用ソフトウェア分野
ヘルスソフトウェア開発に関する基本的考え方
開発ガイドライン 2014
（手引き）

平成 26 年 7 月

経済産業省

目　　次

1. 序文 1
2. 目的 1
3. 定義及び適用範囲 2
3.1 定義 2
3.2 適用範囲 2
4. **ヘルスソフトウェア**開発で推奨される要求項目 4
4.1 要求概要 4
4.2 品質マネジメント 7
4.3 リスクマネジメント 7
4.3.1 リスク分析 8
4.3.2 リスク評価 8
4.3.3 リスクコントロール 8
4.3.4 残留リスク評価 8
4.3.5 開発段階及び市販後情報の管理 9
4.4 ソフトウェアの製品安全 9
4.4.1 ユーザー要求分析及び定義 9
4.4.2 ソフトウェアバリデーション 9
4.4.3 ソフトウェアの識別及び関連文書作成 10
4.4.4 市販後の考慮 10
4.5 ソフトウェアライフサイクルプロセス 10
4.5.1 ソフトウェア開発計画 11
4.5.2 ソフトウェア要求分析 11
4.5.3 ソフトウェア構成管理プロセス 11
5. 本ガイドラインに基づく詳細ガイドラインの策定 11
付録 A：品質マネジメントの実現の参考となる規格類 13
付録 B：リスクマネジメントの実現の参考となる規格類 14
付録 C：ソフトウェアの製品安全の実現の参考となる規格類 16
付録 D：ソフトウェアライフサイクルプロセスの実現の参考となる規格類 17
付録 E：**ヘルスソフトウェア**開発の参考となるその他の国際規格及び文献 20

文中の**ゴシック体**の用語は、3.1（定義）で規定している用語を示す。

1. 序文

平成 24 年度より、医療関連目的のソフトウェアについて、現状や課題を「医療用ソフトウェアに関する研究会」（以下、研究会）にて検討してきた。平成 25 年度には、前年度までの研究会の成果を引きついで、医療関連目的のソフトウェアの開発に関する基本的な考え方を開発ガイドラインとしてまとめるワーキンググループ（以下、本 WG）を組織するとともに、研究会においてはそのようなソフトウェアに対する業界自主基準及びその普及啓発活動について検討した。本ガイドライン（手引き）は、本 WG の成果物である。

平成 24 年度及び、25 年度の研究会を通じて、**ヘルスソフトウェア**開発の際に推奨される 4 つの項目（品質マネジメント、リスクマネジメント、ソフトウェアの製品安全、ソフトウェアライフサイクルプロセス）及び参考となる国際規格が例示された。また、ソフトウェアの安全のほか、ソフトウェアのユーザビリティの要因、IT ネットワーク接続環境が要因となるリスクの存在についても議論された。これらのリスクファクターは重要であるものの国際標準が検討中であることもあり、まずは**ヘルスソフトウェア**の安全についての施策を先行して進めることとし、情報セキュリティ、サイバーセキュリティ等を加えた残りの要因については今後の課題とすることとした。また、ガイドラインの策定と並行して、ガイドラインの周知及びガイドラインが推奨する施策を実践できるようになるための教育を行うことが必要であることが指摘された。

さらに、本 WG では、**ヘルスソフトウェア**の開発者、事業者及び新規参入者が、法規制対象となる**医療機器ソフトウェア**の開発、事業に移行すること、あるいは**ヘルスソフトウェア**を輸出するために国際標準への適合を目指すことを容易にすることも視野に検討した。

本ガイドラインは基本的な考え方を示したものであり、実際には本ガイドラインの考え方をもとに、工業会等による具体的に実施可能かつ詳細なガイドライン（以下、詳細ガイドライン）が策定され、必要に応じて更新され、ソフトウェアの利用者の信頼を高め、**ヘルスソフトウェア**の健全な発展と医療機器産業の振興が図られることを期待する。

2. 目的

本ガイドライン（手引き）の目的は、**ヘルスソフトウェア**の開発者、事業者及び新規参入者が本ガイドラインを適用することによって、ソフトウェア利用者に安全なソフトウェアやサービスを提供できるようになることである。利用者が安心して**ヘルスソフトウェア**を利用できることで、利用範囲及び利用者が拡大して、本ガイドラインはソフトウェア産業の振興に寄与することができる。

また、本ガイドラインは、関係する国際標準との関係性についても考慮している。

なお、本ガイドラインは万能の正解を示すものではなく、執筆時点における原則的な考え方とより詳しい情報の入手の仕方を示すものである。

よって、本ガイドラインは強制性を伴うものではなく、開発したソフトウェアが本ガイドラインに適合することでその品質、有効性、安全性を保証するものでもない。また，本ガイドラインは既存の国際標準、工業標準、法令、通知、指針類を置き換えるものでもない。

3. 定義及び適用範囲

3.1 定義

以下は、本ガイドラインにおける定義である。関連する国内法令及び国際標準の定義が変更される可能性があることに留意されたい。

① ヘルスソフトウェア Health Software

個人の健康管理・維持・向上目的または、医療の提供に使用されることを意図したソフトウェア　（出典：IEC 82304-1/CD 参考訳）

注記　IEC 82304-1/CD 版では、HEALTH SOFTWARE を “software intended to be used specifically for maintaining or improving health of individual persons, or the delivery of care”と定義している。

② ヘルスソフトウェア開発組織

ヘルスソフトウェアの開発者、事業者、新規参入者

③ 医療機器ソフトウェア Medical Device Software

ヘルスソフトウェアのうち、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（医薬品医療機器等法）の規制の対象となるソフトウェア

注記　JIS T2304:2012（及び IEC62304）では、**医療機器ソフトウェア**を「開発中の医療機器に組み込むことを目的として開発された、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」と定義している。

④ 法規制対象外のヘルスソフトウェア

ヘルスソフトウェアのうち、汎用（非医療用）コンピューティングプラットフォーム上で実行可能なソフトウェアでかつ、医薬品医療機器等法の定める医療機器（あるいはその一部）に該当しないソフトウェア

3.2 適用範囲

本ガイドラインは、利用者の安全の観点から推奨される**ヘルスソフトウェア開発組織**の設計・開発マネジメント、リスクマネジメント及び**ヘルスソフトウェア**の製品安全とそのソフトウェアライフサイクルプロセスに対して適用する。ただし、医薬品医療機器等法により医療機器として規制対象となる 3.1 の③のソフトウェアについては、同法の規定に従

う。

利用者の安全のためには市場の障害の是正を含む市販後の保守管理も重要であるため、本ガイドラインは**ヘルスソフトウェア**の市販後の推奨保守要求が実現可能な組織[注記１]を対象とする。また、本ガイドラインは日本国内で使用される**ヘルスソフトウェア**を対象とする。[注記２]

注記１　市販後の推奨保守要求が実現可能でない組織や**ヘルスソフトウェア**の個人開発者、事業者や組織構成されていないグループが本ガイドラインの適用を目指すことを妨げない。

注記２　海外で販売・提供されているソフトウェアを日本国内で販売・提供する場合には、本ガイドラインの適用対象となるかどうかを確認し、その製品の海外規制等への対応状況と本ガイドライン（詳細ガイドラインが存在する場合は、詳細ガイドライン）との差分について確認・対応することが望まれる。

表１ヘルスソフトウェアの特徴

（出典：平成 25 年度経産省医療用ソフトウェアに関する研究会報告書 図表－３を一部改変）

<table>
<tr><th>ソフトウェアの種類</th><th>プラットフォーム</th><th>説　明</th><th>法規制対象の有無</th></tr>
<tr><td rowspan="4">ヘルスソフトウェア</td><td>医療機器または医療機器の一部のハードウェアで動作する</td><td>「医療機器ソフトウェア」のうち、医療機器に組み込むことを目的として開発されたもの</td><td rowspan="2">法規制対象</td></tr>
<tr><td rowspan="3">汎用（非医療用）コンピューティングプラットフォームで動作する</td><td>A:「医療機器ソフトウェア」のうち、それ自体を医療機器として使用することを意図したもの</td></tr>
<tr><td>B:「法規制対象外のヘルスソフトウェア」のうちリスクの考慮が必要なもの</td><td rowspan="2">法規制対象外</td></tr>
<tr><td>C:「法規制対象外のヘルスソフトウェア」のリスク考慮の必要がないもの</td></tr>
</table>

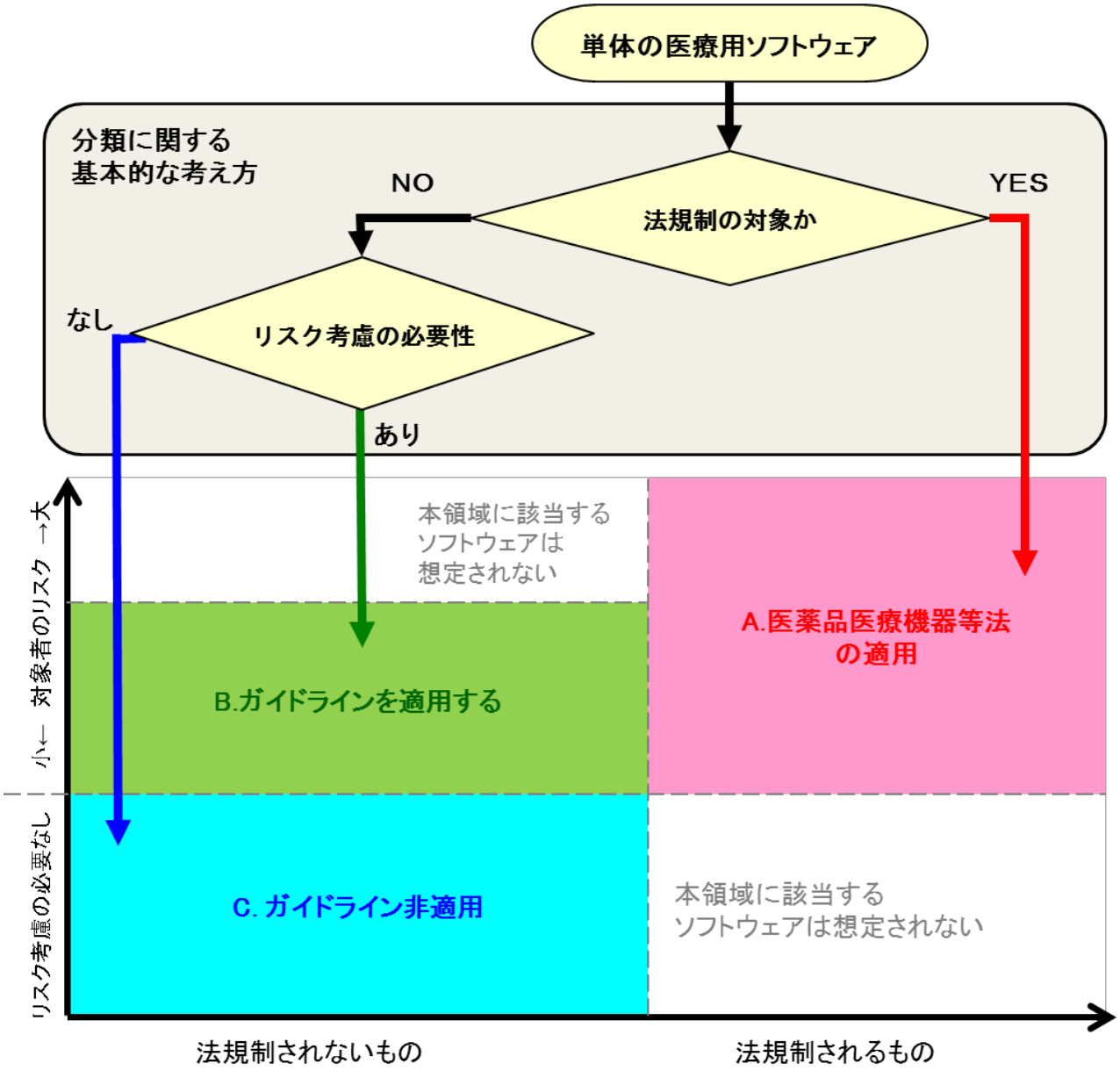

図 1　単体の**ヘルスソフトウェア**とガイドライン等の分類

（出典：平成 25 年度経産省医療用ソフトウェアに関する研究会報告書 図表－1 を一部改変）

4. ヘルスソフトウェア開発で推奨される要求項目

4.1　要求概要

図 1 の B 領域のソフトウェアは医療のみならず、健康、介護など幅広い領域での使用が想定される。これらのソフトウェアやソフトウェアサービスの使用環境においては、何らかのリスクが内在していると想定されるが、そのリスクは、ほとんどリスク考慮の必要がないレベルのものから、十分な考慮が必要となるレベルまで幅があると考えられる。

そのリスクがどの程度のものなのか、想定される危害は何か、リスク対策を行った後に残留リスクが残るのかどうかといったリスク評価の項目はリスク分析の手法を使って分析

することができる。そして、ソフトウェアの使用目的に照らし合わせてリスクを分析したり、市場で発生した障害をインプットにして、障害の再発防止を行ったりするには、**医療機器ソフトウェア**で実施されているリスクマネジメントの要求を参考にするとよい。

また、汎用（非医療用）コンピューティングプラットフォーム上で動作するソフトウェアは、ソフトウェアのアップデートが比較的容易であり、すばやい障害対策を行うことができる。ただし、ソフトウェアにおいて障害対策を行う場合は、その変更がソフトウェアの基本性能やリスク低減を目的に実装したリスクコントロール手段を壊さないようにすることが重要である。

さらに、大規模・複雑化したソフトウェアに対して効果的にリスクを低減するには、**医療機器ソフトウェア**の開発で使われる、想定したリスクに対するフェールセーフ、フォールトトレランス、ユーザビリティエンジニアリングといった設計手法を用いるとよい。

本ガイドラインの目的である安全な**ヘルスソフトウェア**の提供と、ソフトウェア産業振興を両立させるためには、**医療機器ソフトウェア**に求められている要求事項のうち、安全の確保に対して有効かつ必要不可欠なものを抽出して適用することが望ましい。また、将来このようなソフトウェアを海外で販売することを想定するならば、組織内での品質マネジメントシステムの確立やソフトウェアの開発プロセスの定義と実行についても考慮すると良い。

リスクの考慮が必要になる図 1, 表 1 の B 領域の**ヘルスソフトウェア**に関しては、医療機器としての法規制対象外ではあるが、市場の変化にすばやく対応する即応性や IT ネットワークに接続した際のさまざまな問題への対応なども求められるため、市販後に発生する障害のモニタリングと、発生した障害のリスク分析と再発防止策に注力することが重要である。（図 2 参照）

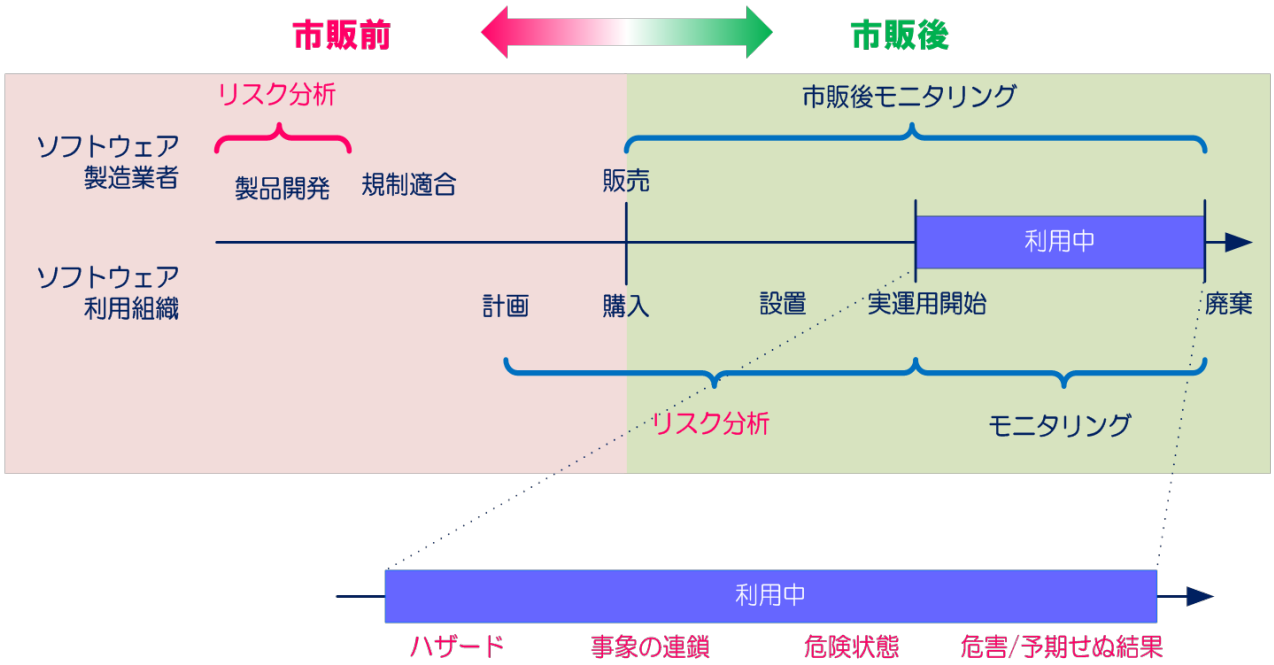

図 2 リスク分析と評価のタイミング

（出典：平成 25 年度経産省医療用ソフトウェアに関する研究会報告書 図表－4 を一部改変）

これらのことを総合的に考えると、**ヘルスソフトウェア開発組織**及び**ヘルスソフトウェア**製品は、次のカテゴリの推奨要求事項を満たすことが望ましい。

表 2 **ヘルスソフトウェア**開発で推奨される要求事項と参考になる国際規格
（出典：平成 25 年度経産省医療用ソフトウェアに関する研究会報告書 図表－5 を一部改変）

対象	カテゴリ	推奨される要求事項	参考になる国際規格
ソフトウェア開発者等	品質マネジメント	- 設計・開発プロセス	ISO 9001:2008 (JIS Q 9001:2008) 品質マネジメントシステム－要求事項
	リスクマネジメント	- リスク分析 - リスク評価 - リスクコントロール - 残留リスク評価 - 開発段階及び市販後情報[注記]の管理	ISO 14971:2007 (JIS T 14971:2012) 医療機器－リスクマネジメントの医療機器への適用
ヘルスソフトウェア製品	ソフトウェアの製品安全	- ユーザー要求分析及び定義 - ソフトウェアバリデーション - ソフトウェアの識別及び関連文書作成 - 市販後の考慮	IEC 82304-1 CD Health software -- Part 1: General requirements for product safety (策定中)
	ソフトウェアライフサイクルプロセス	- ソフトウェア開発計画 - ソフトウェア要求分析 - ソフトウェア構成管理プロセス	IEC 62304:2006 (JIS T 2304:2012) 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

注記　JIS T14971 では「製造後」と表記されている。

4.2 品質マネジメント

ヘルスソフトウェア開発組織は、安全なソフトウェアを設計・開発するために、製品要求事項に関連するインプットを明確にし、設計・開発のインプットに対応したアウトプットを作成する。また、設計・開発の適切な段階において体系的なレビューを行い、設計・開発のアウトプットが、設計・開発のインプットで与えられている要求事項を満たしていることを確実にするための検証を積み重ねる。その後、検証の結果として得られた製品が、指定された用途または意図された用途に応じた要求事項を満たしていることを確実にするために妥当性確認を行う。

4.3 リスクマネジメント

ISO/IEC GUIDE 51:1999 [注記] (JIS Z 8051:2004) 及び ISO/IEC GUIDE 63:2012 によれば、安全（セーフティ）とは「受容できないリスクがないこと」と定義され、リスクが受容可能かどうかは「使用者の利便性」「目的適合性」「費用対効果」など諸要因のバランスで決定される。また、今後の技術の進展、安全に対する認識、社会的ニーズ等が変化していけ

ば、それらに応じて判断基準を見直していくことも必要である。リスクマネジメントは、**医療機器ソフトウェア**の開発においては必須要求となっており、**法規制対象外のヘルスソフトウェア**の開発においても有用であると考えられる。**ヘルスソフトウェア開発組織**がソフトウェアの市販後の市場で発生した障害を監視し、再発防止のためのリスクアセスメント及びリスク低減を実施しこれらのプロセスを反復することは、ソフトウェア利用者の信頼を得るために役立つ。

これらのことから、**ヘルスソフトウェア開発組織**は**法規制対象外のヘルスソフトウェア**を開発する場合であっても、リスクマネジメントの活動として「リスク分析」「リスク評価」「リスクコントロール」「残留リスク評価」「開発段階及び市販後情報の管理」を行えるようになることを推奨する。

注記　ISO/IEC GUIDE 51 は 2014 年 3 月に最新版が発行されたが、医療機器系のリスクマネジメント規格との整合がまだ十分に取れていないため、本ガイドラインでは 1999 年版を参照している。

4.3.1 リスク分析

ヘルスソフトウェアの意図する使用、合理的に予見できる誤使用及びソフトウェア利用者の安全に影響する定性的、定量的な特質を明確化し、既知及び予見可能なハザードを特定する。また、危険状態を起こすような事象または事象の組合せを分析し、個々の危険状態に対するリスクを推定する。

例えば、ある**ヘルスソフトウェア**が扱う健康上のデータ一件ごとの重要性が低かったとしても、そのソフトウェアが健康上のデータを経時的に蓄積し、他の健康上の入力データと組み合わせて分析、閲覧する機能を提供するのであれば、これらのデータ群及び経時的付加情報が意図せず改変されてしまったり消去されてしまったりする不具合は利用者に対してリスクとなるかもしれない。**ヘルスソフトウェア**に関連してどのような利用上のリスクが存在するのかを分析し、設計対策を実装したり、表記上の対策を実施したりすることはソフトウェアの潜在的価値を向上させることに役立つ。

4.3.2 リスク評価

特定した各危険状態について、リスク低減が必要かどうかを評価する。リスク低減が必要でないと評価した場合においても、その根拠を残しておくことが設計変更時のリスク再評価の必要判定の際に役立つ。

4.3.3 リスクコントロール

リスク低減が必要な場合は、リスクを受容可能なレベルまで低減するためのリスクコントロール手段を選択し、リスクコントロール手段を実施し、実施を検証し、有効性を確認する。

4.3.4 残留リスク評価

リスクコントロール手段の実施後に残る残留リスクを評価する。リスク低減を目的に設

計したリスクコントロール手段が新たなリスクを生んだり、4.3.1 で分析したリスクの大きさを変えることはある。したがって、リスクコントロール手段の実施後に残る残留リスクを評価することは重要である。

4.3.5 開発段階及び市販後情報の管理

ヘルスソフトウェアの開発段階のみならず市販後[注記]においても、以前に認識されていなかったハザードまたは危険状態はないか、危険状態によって推定されるリスクが受容し続けられているかどうかの情報を収集し、リスクマネジメントにフィードバックできるようにする。

注記　JIS T214971（及び ISO14971）では、製造後と表記している。

4.4　ソフトウェアの製品安全

開発したソフトウェアが意図した仕様に合致しているか、ユーザーに受け入れられるか、設計したリスクコントロール手段が漏れなく実装されているかといったソフトウェアバリデーションの取り組みは、セーフティ・クリティカルなソフトウェアが求められる分野（航空・宇宙、自動車、鉄道、原子力、医療機器等）で特に重要視されている。

このため、**ヘルスソフトウェア**の開発においては、ソフトウェアの製品安全の実現手段として、ソフトウェアの「ユーザー要求分析及び定義」「ソフトウェアバリデーション」「ソフトウェアの識別及び関連文書作成」「市販後の考慮」の実施を推奨する。

4.4.1 ユーザー要求分析及び定義

ヘルスソフトウェアに求められるユーザー要求を分析し、ソフトウェア製品の意図する使用、ユーザビリティ、ソフトウェア・ハードウェア環境等を定義する。ソフトウェア製品の意図する使用が定まらなければ、有効なリスク分析はできない。意図する使用を特定しなければ、合理的に予見できる誤使用や既知及び予見可能なハザードの抽出を収束させることができず、リスク分析が終わらないからである。また、ソフトウェアの変更容易性により、ソフトウェアの設計変更がソフトウェア製品の使用目的を意図せずして変えてしまう可能性がある。使用目的の変化は、想定していない新たなリスクを発生させる危険があるため、ソフトウェアの変更によって意図する使用が変わっていないかどうかを確認することが重要である。設計変更によって意図する使用が変化した場合は、リスク分析をやり直す必要がある。そのためには、事前にユーザー要求分析及び意図する使用の定義が必要になる。

4.4.2 ソフトウェアバリデーション

ソフトウェアバリデーション計画を立案し、バリデーションのインプット、アウトプット、バリデーションの活動と方法を定義する。また、バリデーションを実施したレポートを作成する。

大規模・複雑化したソフトウェアは分割・分業して開発され、国内・海外の協力会社に

アウトソースされることも多い。各ソフトウェアモジュールのパートを任された組織やプロジェクトが仕様通りにソフトウェアを作成しても、ソフトウェアシステムとして各パートを結合したときに、**ヘルスソフトウェア開発組織**が策定した意図する使用やソフトウェアのエンドユーザーの要求に合致していない部分が現れることがある。そのため、ソフトウェアバリデーションによってソフトウェアの妥当性を確認するのだが、ソフトウェアのリリースが間近に迫った状態で場当たり的なバリデーションを行っていると、十分なバリデーションが行われないままソフトウェアが市販されてしまう危険性がある。これを防止するためにも、バリデーションのインプット、アウトプットの定義、バリデーション活動として何を実施するのか、合格の判定基準は何かといった項目をソフトウェアバリデーション計画として、また、設計の上流工程で立案しておくことが重要である。

注記　本ガイドラインでは、ISO 9001:2008 (JIS Q 9001:2008) で使われるソフトウェアに特化しないバリデーションを「妥当性確認」と記し、IEC 82304-1 で使用されるソフトウェアに特化したバリデーションを「（ソフトウェア）バリデーション」と記して、区別している。

4.4.3 ソフトウェアの識別及び関連文書作成

ヘルスソフトウェア製品を識別するために、製造業者、製品名及びバージョン、リリース日などを明確化する。また関連文書として、使用説明や技術情報、ネットワーク環境情報などを示す。

何らかのリスクを内包する可能性がある**ヘルスソフトウェア**においては、ソフトウェア製品を確実に識別することが重要である。なぜなら、市場において障害が発生したときに、障害の重大度によっては、速やかにソフトウェアのアップデートを行う必要があり、対象となるソフトウェアを特定するためにソフトウェア製品の識別情報が重要だからである。また、**ヘルスソフトウェア**を正しく使うための使用説明や技術情報、ネットワーク環境やハードウェア環境の制限事項などの表示が必要である。ソフトウェアの関連文書は、取扱説明書という形で提供する他、電子的な表示や事業者のウェブサイトで示すこともある。

4.4.4 市販後の考慮

ヘルスソフトウェアの保守、再バリデーション、市販後情報の管理、ソフトウェアの廃棄等に関しての手順を示す。

市販後に発生した設計変更において、再バリデーションを行う際の条件、また、ソフトウェアを廃棄する際に必要な機能や手順を明確にする。市販後のソフトウェアの管理の手順はソフトウェアの設計変更によるデグレードや市場で発生した障害の再発防止に役立ち、ソフトウェアの廃棄機能や手順の明確化は個人情報の漏洩防止などに役立つ。

4.5 ソフトウェアライフサイクルプロセス

ヘルスソフトウェアに対して試験を実施しただけで、その使用が安全であると判断することは難しい。**ヘルスソフトウェア**の開発及び保守において、利用者のリスクに対して適切なプロセスを実施することが安全の実現に貢献すると考えられる。

本ガイドラインの対象となっている**ヘルスソフトウェア**では、意図する使用に基づき、分析したリスクに対するリスクコントロールを実施し、かつ、設計変更後にもそれらが保たれていることを確実にするため、ソフトウェアライフサイクルプロセスのうち「ソフトウェア開発計画」「ソフトウェア要求分析」「ソフトウェア構成管理プロセス」を実施することを推奨する。

4.5.1 ソフトウェア開発計画

V モデルのみならず、インクリメンタル、アジャイルといったソフトウェアの開発プロセスを採用する場合においても、ソフトウェアの設計・実装前に開発計画を立てることは重要である。具体的には、ユーザー要求の分析及び意図する使用の定義、リスク分析、リスク評価、リスクコントロール、残留リスクの評価をソフトウェアの設計前に実施する計画が望まれる。

4.5.2 ソフトウェア要求分析

ソフトウェア要求事項としてシステムに求められる本質的な機能及び性能の他、ソフトウェアシステムと他のシステム間のインタフェースや、データ定義やデータベース要求事項、ソフトウェアで実施するリスクコントロール手段の要求事項等を分析する。

ソフトウェア要求分析では、単なるソフトウェアの機能の抽出ではなく、ユーザー要求から展開される要求を実現可能、検証可能な要求に落とし込み、リスク分析の結果、必要と判断された設計対策を要求事項に盛り込む。ここで定義されたソフトウェア要求事項の検証がソフトウェアバリデーション活動のひとつとなる。

4.5.3 ソフトウェア構成管理プロセス

ヘルスソフトウェアの構成要素（例えばソースファイル）及びそのバージョンを一意に識別するための仕組みを準備する。また、ソフトウェアの変更要求に応じる場合の変更管理の手順及び、変更のトレーサビリティを実現する手段を用意する。

ソフトウェアは頻繁に修正要求が発生する場合もあり、安易な修正はデグレードを引き起こす危険があるため、ソフトウェア構成管理の仕組みを作ることが重要である。また、ソフトウェアの試作段階、市販前、市販後といった開発ライフサイクルのフェーズによって構成管理の管理状態を変えることも重要である。特に市販後の構成管理、変更管理はあらかじめ定められた手順を使って組織的に実施することが迅速な障害対応の実現につながる。

5. 本ガイドラインに基づく詳細ガイドラインの策定

本ガイドラインは**ヘルスソフトウェア**の開発に関する基本的な考え方を示したものであり、実際には工業会等が、本ガイドラインの考え方をもとに具体的に実施可能かつ詳細なガイドラインを策定することが望まれる。

本ガイドラインの策定の段階では、医薬品医療機器等法が未施行であること、関連する国際標準に策定中のものもあることに留意して、本ガイドラインを適宜見直しを図っていく必要がある。

付録 A：品質マネジメントの実現の参考となる規格類

- ISO 9001:2008 (JIS Q 9001:2008) 品質マネジメントシステムー要求事項

品質マネジメントシステムに対する要求事項を定義した ISO 9001:2008 (JIS Q 9001:2008) では、品質マネジメントシステムの有効性の改善のために、プロセスアプローチを採用することを推奨している。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、特にそのプロセス間の相互作用を体系的に明確にし、運営管理することを言う。品質マネジメントシステムへプロセスという考え方を持ち込むことによって、インプットの変換活動を経て、アウトプットするという流れの中でシステム構成要素を整理できるとともに、構成要素間の影響を明らかにすることができる。このため、品質に関する問題が発生したときに、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するというサイクルを容易に実行できるようになる。

品質マネジメントシステムのプロセス全体において、安全なソフトウェアを市場に供給し続けることを目的にする組織がソフトウェア開発の中核のプロセスである「設計・開発」プロセスの要求を実現できるようになることは有益であると考えられる。なお「設計・開発」プロセスだけでなく、ソフトウェア開発組織が ISO 9001 全体に適合してもよい。

なお、ISO 9001:2008（または JIS Q 9001:2008）または ISO 13485:2003（または JIS Q 13485:2005）に適合している開発者または組織は品質マネジメントに関する推奨要求事項は実現できているとみなすことができる。

下記に設計・開発の活動例を示す。ISO 9001:2008 (JIS Q 9001:2008)参照

設計・開発の計画
設計・開発へのインプット
設計・開発からのアウトプット
設計・開発のレビュー
設計・開発の検証
設計・開発の妥当性確認
設計・開発の変更管理

付録 B：リスクマネジメントの実現の参考となる規格類

- ISO 14971:2007(JIS T 14971:2012) 医療機器－リスクマネジメントの医療機器への適用
- ISO/IEC GUIDE 51:1999 Safety aspects － Guidelines for their inclusion in standards (JIS Z 8051:2004 安全側面-規格への導入指針)
- ISO/IEC Guide 63:2012 Guide to the development and inclusion of safety aspects in International Standards for medical devices
- 安全設計の基本概念，宮崎浩一，向殿政男，安全設計の基本概念，日本規格協会, 2007

図 B-1 は ISO 14971:2007(JIS T 14971:012) の基本となるリスクマネジメントプロセスの流れを示している。

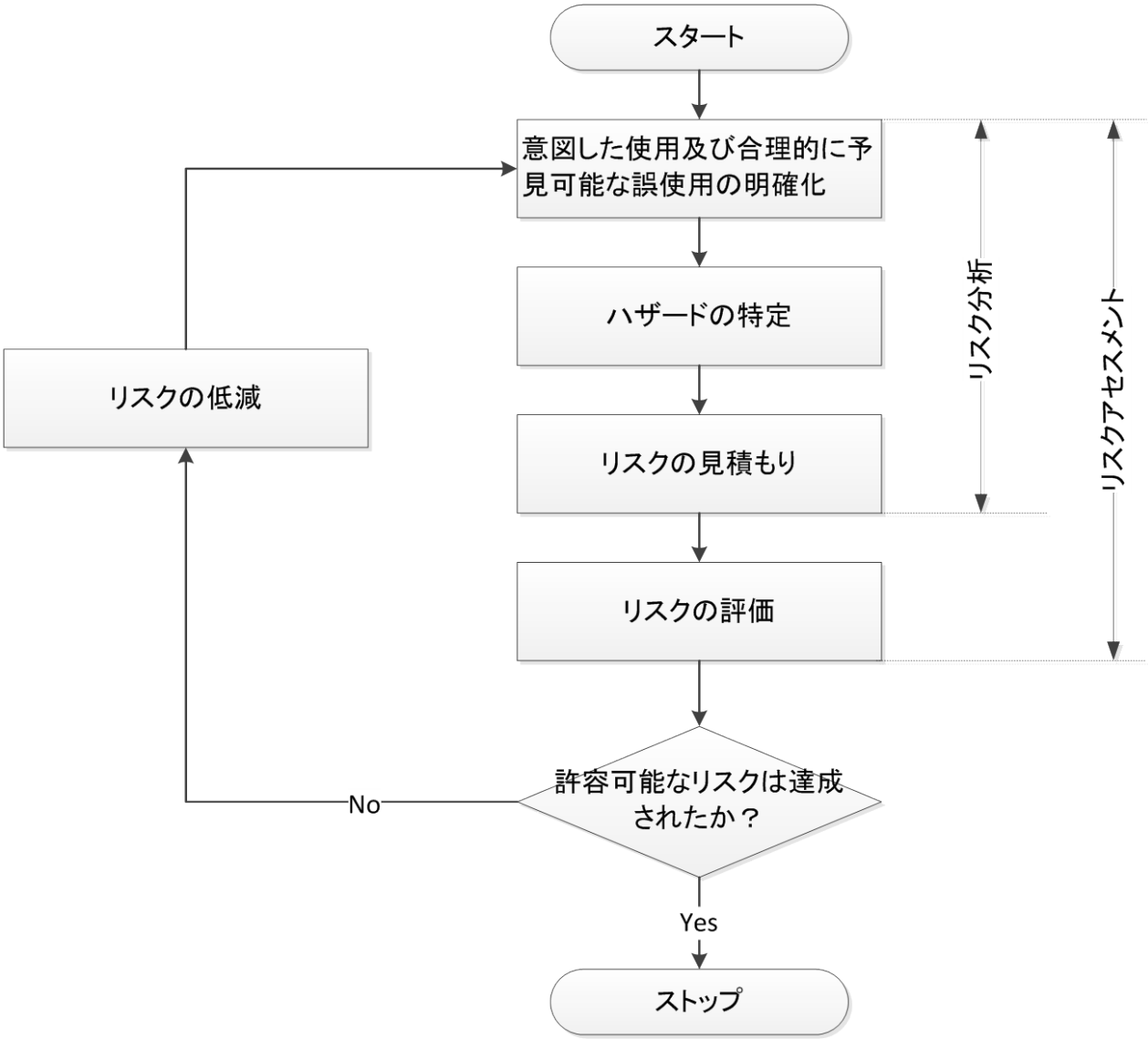

図 B-1 リスクマネジメントプロセスの流れ

なお、ISO/IEC GUIDE 51:1999 ではリスクアセスメント及びリスク低減に関する用語を次のように定義している。

- 安全：受容できないリスクがないこと。
- リスク：危害の発生確率及びその危害の程度の組合せ。
- 危害：人の受ける身体的障害もしくは健康障害、または財産もしくは環境が受ける害。
- 危険事象：危険状態から結果として危害に至る出来事。
- ハザード：危害の潜在的な源。
- 危険状態：人、財産または環境が、一つまたは複数のハザードにさらされる状況。
- 受容可能なリスク：社会における現時点での評価に基づいた状況下で受け入れられるリスク。
- 保護手段：リスクを低減するための手段。
- 残留リスク：保護手段を講じた後にも残るリスク。
- リスク分析：利用可能な情報を体系的に用いてハザードを特定し、リスクを見積もること。
- リスクの評価：リスク分析に基づき、許容可能なリスクに到達したかどうかを判定する過程。
- リスクアセスメント：リスク分析及びリスクの評価からなるすべてのプロセス。
- 意図する使用：供給者が提供する情報に基づいた製品、プロセスまたはサービスの使用。（使用上の指示事項の中に提供された情報に基づいた機器の使用）
- 合理的に予見可能な誤使用：供給者が意図しない方法であるが、人間の挙動から生じる容易に予測しうる製品、プロセスまたはサービスの使用。（設計者が意図していない使用法で、容易に予測できる人間の挙動から生じる機器の使用）

付録Ｃ：ソフトウェアの製品安全の実現の参考となる規格類

- IEC 82304-1 CD Health software -- Part 1: General requirements for product safety

IEC 62304:2006(JIS T 2304:2012) が**医療機器ソフトウェア**のライフサイクルプロセスを示しているのに対して、2014 年 3 月現在、検討中の国際規格 IEC 82304-1 は**ヘルスソフトウェア**の製品安全に対する一般要求事項を示している。

IEC 82304-1 は従来の**医療機器ソフトウェア**に加え、その他のヘルスユースで使用されるソフトウェアも含めて**ヘルスソフトウェア**を定義し、広義の**ヘルスソフトウェア**の製品安全に対する要求事項を策定しようとしている。

本ガイドラインの初版が策定された 2014 年 3 月時点では、**ヘルスソフトウェア**の製品安全に対する参照すべき他の国際規格が存在しなかったため CD 版の IEC 82304-1 を参照している。IEC 62304:2006(JIS T 2304:2012) は、妥当性確認及び最終的な出荷の合否判定は対象としていない。したがって、汎用（非医療用）コンピューティングプラットフォームでの使用が可能であるソフトウェアの製品安全については、IEC 82304-1 CD の「ユーザー要求分析及び定義」「ソフトウェアバリデーション」「ソフトウェアの識別及び関連文書作成」「市販後の考慮」が参考になると考えられる。

IEC 82304-1 CD は、**ヘルスソフトウェア**の開発プロセスに対して、IEC 62304:2006 を参照している。今後、IEC 62304 の Ed.2 は Ed.1 のスコープを拡大して**ヘルスソフトウェア**全体を適用範囲とし、IEC 82304-1 からの参照にも矛盾なく対応できるように改訂しようとしている。

IEC 82304-1 や IEC 62304 Ed.2 が正式発行された後には、本ガイドラインの推奨要求事項も再考が必要になるかもしれない。

付録 D：ソフトウェアライフサイクルプロセスの実現の参考となる規格類

- IEC 62304:2006(JIS T 2304:2012) **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 62304:2006(JIS T 2304:2012) 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した規格である。この規格は、**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成るライフサイクルプロセスのフレームワークと各ライフサイクルプロセスに対する要求事項を規定している。IEC 62304:2006 (JIS T 2304:2012) は汎用（非医療用）コンピューティングプラットフォームでの使用が可能な**医療機器ソフトウェア**に対しても適用される。

各ライフサイクルプロセスは、一連のアクティビティで構成され、アクティビティは一連のタスクで構成される。図 D-1 に IEC 62304:2006 (JIS T 2304:2012)の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を示す。

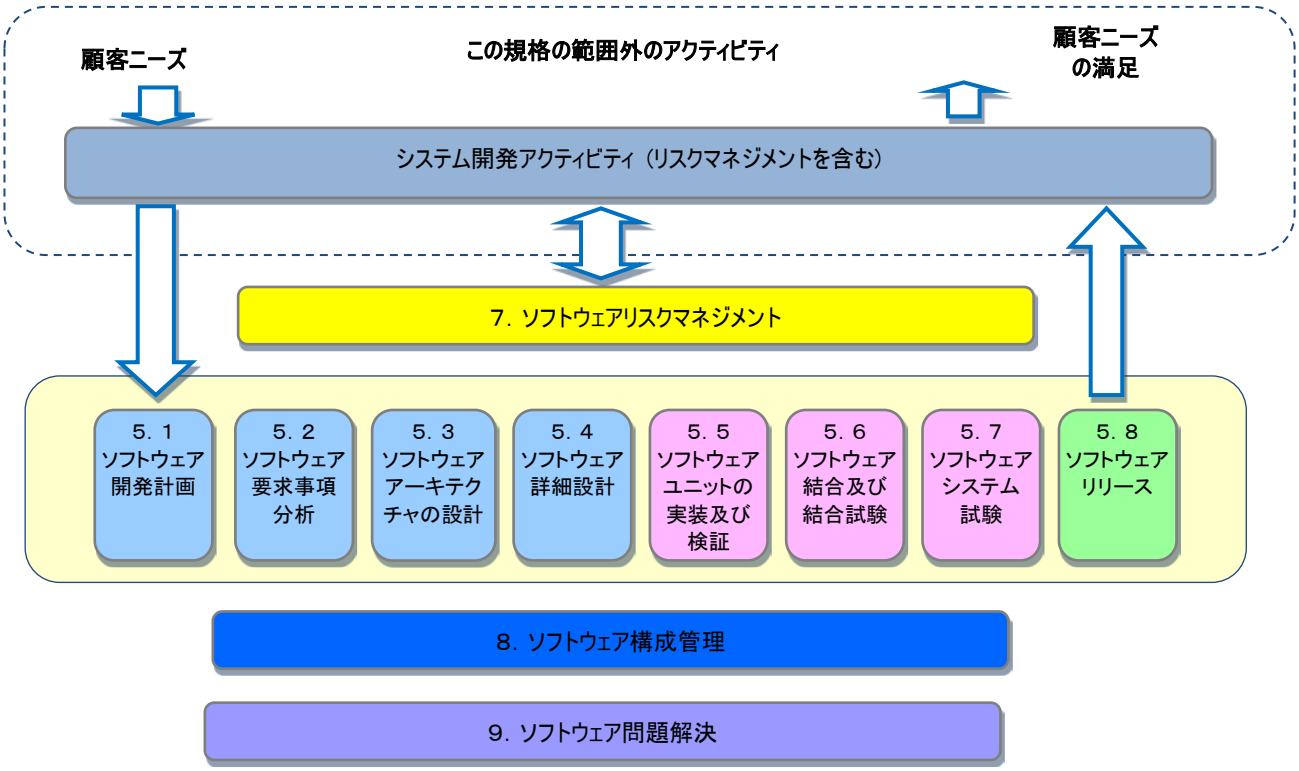

図 D-1 ソフトウェア開発プロセス及びアクティビティの関連図

医療機器ソフトウェアの安全性を向上させるためには次の三つの原則が存在し、これらを組み合わせることで**医療機器ソフトウェア**の安全性が促進されると解説されている。

- 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

IEC 62304:2006(JIS T 2304:2012) 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いる。この目的を達成するために、ソフトウェア安全クラスに応じた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いる。

各ライフサイクルプロセスは、一連のアクティビティで構成され、アクティビティは一連のタスクで構成される。製造業者は、ソフトウェアシステムに起因する危害が患者、操作者、またはその他の人に及ぼす影響に応じて、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 または C）に分類する。そして、分類されたソフトウェア安全クラスに応じてプロセス、アクティビティ、タスクが割り当てられる。

ソフトウェア安全クラス分類は次のように 3 つのクラスがある。

クラス A：負傷又は健康障害の可能性はない。

クラス B：重傷の可能性はない。

クラス C：死亡又は重傷の可能性がある。

IEC 62304:2006(JIS T 2304:2012) への適合は、ソフトウェア安全クラスに従って、この規格で特定した全てのプロセス、アクティビティ及びタスクを実行することで示す。例えば、ソフトウェア開発計画プロセスにおいては、下記のアクティビティが要求される。（ソフトウェア安全クラスが B の場合は「ソフトウェア開発規格、方法及びツールの計画」の要求は必須ではない。）

ソフトウェア開発計画

- ソフトウェア開発計画の継続更新
- 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
- ソフトウェア開発規格、方法及びツールの計画
- ソフトウェア結合及び結合試験計画
- ソフトウェア検証計画
- ソフトウェアリスクマネジメント計画
- 文書化計画
- ソフトウェア構成管理計画
- 管理が必要な支援アイテム
- 検証前のソフトウェア構成アイテムのコントロール

IEC 62304:2006(JIS T 2304:2012) ではソフトウェア安全クラスに応じて下記のようなプロセス、アクティビティ、タスクの実施が求められる。なお、本ガイドラインでは、ソフトウェアライフサイクルプロセスのカテゴリにおいて「ソフトウェア開発計画」「ソフトウェア要求分析」「ソフトウェア構成管理プロセス」のみを参照し、他のプロセス、アクティビティ、タスクを参照しなかった。IEC 62304:2006(JIS T 2304:2012) のソフトウェア安全クラス A（負傷又は健康障害の可能性はない）で要求されるプロセス、アクティビティ、タスクを上回らないことを考慮するとともに、品質マネジメント、リスクマネジメント、

ソフトウェアの製品安全のカテゴリですでに推奨されている同等の要求事項がある場合、関連するプロセス、アクティビティ、タスクが二重にならないようにしたからである。

また、4.5 節においてユニットテスト、結合テスト、システムテストをソフトウェアライフサイクルプロセスの推奨要求事項に含めなかったのは、**ヘルスソフトウェア**の製品安全のカテゴリにおけるソフトウェアバリデーションの計画、方法論の定義、レポートの作成といった活動の中で、それらの検証が計画・実施されることを期待しているからである。

4.5 節で推奨した要求事項「ソフトウェア開発計画」「ソフトウェア要求分析」「ソフトウェア構成管理プロセス」は一般的なソフトウェアのソフトウェアライフサイクルプロセス規格（例：ISO/IEC 12207:2013）においても参照できるが、本ガイドラインではリスクマネジメントを基本理念とし、**医療機器ソフトウェア**への適用が求められる IEC 62304 のプロセス、アクティビティ、タスクを参照している。

IEC 62304:2006(JIS T 2304:2012) が要求する主なプロセス、アクティビティ、タスク

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
5.2 ソフトウェア要求事項分析
5.3 ソフトウェアアーキテクチャの設計
5.4 ソフトウェア詳細設計
5.5 ソフトウェアユニットの実装及び検証
5.6 ソフトウェア結合及び結合試験
5.7 ソフトウェアシステム試験
5.8 ソフトウェアリリース
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

付録Ｅ：ヘルスソフトウェア開発の参考となるその他の国際規格及び文献

- IMDRF (International Medical Device Regulators Forum) Final Document, Title: Software as a Medical Device (SaMD): Key Definitions, 医療機器としてのソフトウェア：重要な定義

世界各国の医療機器規制当局からなる任意団体、国際医療機器規制当局フォーラム（IMDRF）により作成された文書で、汎用（非医療用）コンピューティングプラットフォーム での使用が可能である 1 つまたはそれ以上の医療目的で使用するソフトウェアを SaMD (Software as a Medical Device) と定義している。

本ガイドラインでは、日本国内で使用される医薬品医療機器等法の規制対象外のソフトウェアを扱い、IMDRF の定義する SaMD の一部がガイドラインの対象に含まれる。

- 平成 24 年度　医療機器等の開発・実用化促進のためのガイドライン策定事業（医療用ソフトウェアの実態調査事業）報告書，平成 25 年 3 月，経済産業省商務情報政策局 ヘルスケア産業課 医療・福祉機器産業室

本ガイドラインが検討された背景や医療用ソフトウェアに関連した調査情報を知ることができる。

医療用ソフトウェアの実態調査報告書（表紙、目次）
1. 医療用ソフトウェアに関する研究会中間報告書
2. 医療用ソフトウェアの関連調査結果
3. 参考資料

- Mobile Medical Applications Guidance for Industry and Food and Drug Administration Staff, モバイル・メディカル・アプリケーション・ガイダンス

米国 FDA が 2013 年 9 月 25 日に発行した携帯医療用ソフトウェアを対象にしたガイダンス。本ガイダンスには付属文書に規制対象とするアプリケーションや規制対象でないアプリケーションの事例が多数掲載されているため、開発するソフトウェアに本ガイドラインを適用させるべきかどうか検討する際に参考になる。

注記　IT ネットワークに関するリスクマネジメントの国際規格 IEC 80001-1 シリーズ Application of risk management for IT-networks incorporating medical devices は、策定中の関連規格が多数あるため本ガイドラインの参照規格としなかった。今後、IT ネットワークに関連したヘルスソフトウェアの障害事例が増加してきた場合は、本ガイドラインで参照することも想定される。

- IEC 80001-1 シリーズの国際規格（検討中の規格含む）

IEC 80001-1:2010 Application of risk management for IT-networks incorporating medical devices -- Part 1: Roles, responsibilities and activities
IEC80001-2-1 Step by step risk guidance
IEC80001-2-2 Security Guidance
IEC80001-2-3 Wireless guidance

IEC80001-2-4 HDO（Health Delivery Organization） Guidance
IEC80001-2-5 Alarm Guidance
IEC80001-2-6 Guidance on Responsibility Agreements

- IEC 62366:2007 Medical devices -- Application of usability engineering to medical devices

医療現場では患者の観察及び治療に医療機器を利用する頻度が増えている。不適切な医療機器のユーザビリティに起因する使用ミスがますます危惧すべき原因となってきていることから、医療機器を対象とした国際規格 Medical devices – Application of usability engineering to medical devices (IEC62366: 2007) “医療機器へのユーザビリティエンジニアリングの適用”が制定された。この国際規格は、医療機器の安全に関係する範囲で、製造業者が、そのユーザビリティを分析し、指定し、設計し、検証し、妥当性確認をおこなうためのプロセスを規定したものである。

このユーザビリティエンジニアリングプロセスは、正しい使用法と使用ミス、すなわち正常使用に付随するリスクを評価し、軽減するものである。この規格は異常使用（意図的に間違った使用）に付随するリスクの評価又は軽減をおこなうものではないが、その特定に利用することができる。

本ガイドラインではユーザビリティエンジニアリングに関して、リスク分析の中でユーザビリティに関するリスクを分析し、必要な設計対策をソフトウェア要求仕様に盛り込み、ソフトウェアバリデーションにて妥当性を確認することを想定している。2014 年 3 月現在、IEC 62366 はユーザビリティエンジニアリングの設計及び開発プロセスの強化を含む改訂が検討されており、IEC 62366 改訂後にその考え方を本ガイドラインとして参照することも考えられる。

平成 25 年度　医療用ソフトウェア分野
医療用ソフトウェア開発 WG 委員名簿

座長	楠岡　英雄	国立病院機構 大阪医療センター　院長
	大竹　正規	コンティニュア・ヘルス・アライアンス 日本地域政策委員会 委員長
	岡田　美保子	川崎医療福祉大学 医療福祉マネジメント学部　医療情報学科　教授
	土居　篤博	富士フイルム株式会社 ヘルスケア事業推進室 兼 メディカルシステム事業部　シニアエキスパート
	中野　壮陛	公益財団法人医療機器センター　医療機器産業研究所　主任研究員
	橋詰　明英	一般社団法人　保健医療福祉情報システム工業会 標準化推進部会 安全性・品質企画委員会　委員長
	服部　徹	日本電気(株)　ソリューションプラットフォーム統括本部 ビジネスインテリジェンス競争力創出センタ長　マネージャ
	平井　正明	日本光電工業株式会社　技術推進センタ　工業会担当
	古川　浩	東芝メディカルシステムズ株式会社　社長附
	横井　英人	香川大学 医学部附属病院 医療情報部　教授