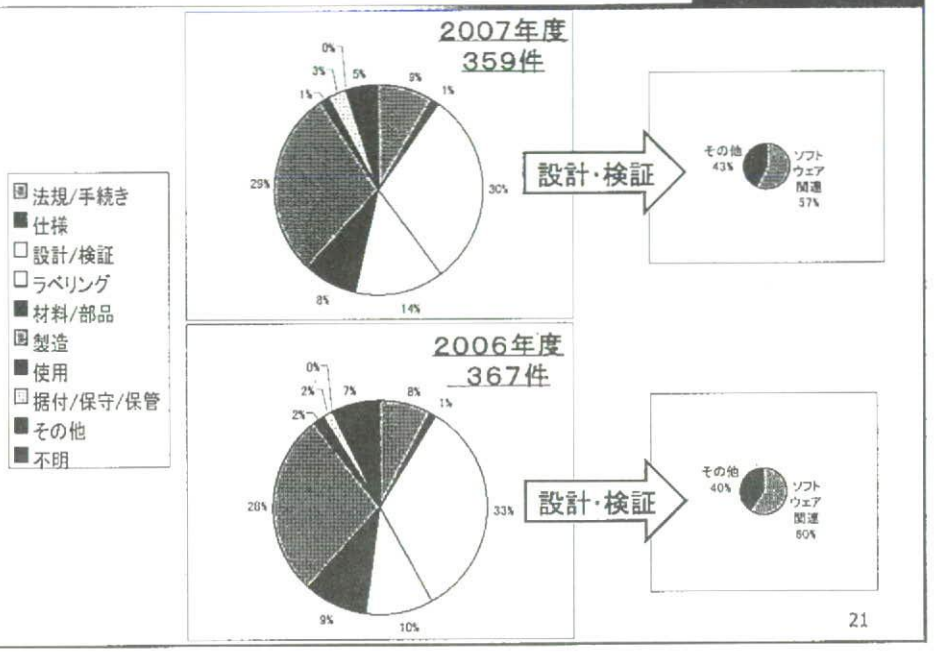
回収・改修の原因分類(日本のクラスⅠ～Ⅲ)

TY ASSURANCE ORGANIZATION



21

附属書(参考)

JAPAN QUALITY ASSURANCE ORGANIZATION

	2000年版		2007年版
A	安全に影響する医療機器の特質を明確化するために使用できる質問事項		要求事項のための論理的根拠
B	IVD診断機器に関するリスク分析の指針		医療機器のRMプロセスの概要 (2000年版「図2 医療機器に適用するRM活動の概要」類似)
C	毒性学的なハザードに関するリスク分析手順の指針		安全に影響する医療機器の特質を明確化するために使用できる質問事項
D	医療機器に関連して起こる可能性があるハザード及び関連する要因の例		医療機器に適用するリスク概念
E	医療機器に適用するリスク概念		ハザード、予見できる一連の事象及び危険状態の例
F	リスク分析手法に関する情報		RM計画
G	この規格で記載したRMの諸要素に関連する情報を含むその他の規格		RM手法に関する情報
H			IVD診断用医療機器に関するRMの指針
I			生物学的ハザードに関するリスク分析プロセスの指針
J			安全に関する情報及び残留リスクに関する情報

22

厚生労働科学研究費補助金（医薬品・医療機器等レギュラトリーサイエンス総合研究事業）
分担研究報告書
医療機器の国際的な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
国際的トピックスに係る海外規制状況調査
分担研究者　戸高　浩司　九州大学病院　循環器内科講師

研究要旨
本邦での医療機器開発に纏わる障壁への対策を講じるために、機器開発が盛んな欧州の規制当局、第三者認証機関、業界団体、治験施設を訪問し比較調査した。27の国、22の言語を持つ地域が一つの承認システムの下に動いているが特に不具合はないとの現地の認識であった。50年の歴史的背景を元に構築されているが、医師に対する患者の厚い信頼により試験への同意率も又高いようである。新しい技術を導入するにはリスクが伴うということも社会的に理解されており、本邦の安全性を最優先する考え方とは文化的違いがある。彼我の医療機器規制制度上の隔たりは非常に大きいが、GHTFでの歩み寄り内容などを参考にしつつ、社会としてどのような方向性が今後望ましいのか、国民的議論をする時期に来ていると考えられる。

A. 研究目的
医療機器規制に関する欧州と我が国の比較をした上で、それらの科学的根拠を明確にしつつ、適切な規制のあり方について提言する。

B. 研究方法
今年度は医療機器開発が盛んな欧州の規制当局、第三者認証機関、業界団体、治験施設を訪問し調査した。

（倫理面への配慮）
本研究は調査研究であり倫理的問題は特に生じない。

C. 研究結果
訪問先
1）英国　①MHRA (Medicines and Healthcare products Regulatory Agency)、BSI (British Standards Institution) ②Imperial College London, Hammersmith Campus
2）ドイツ　③Munich Univ. Klinikum Grosshadern、④TUV-SUD (テュフズート)
3）ベルギー　⑤EU 委員会、⑥Eucomed（European Medical Technology Industry Association 欧州医療機器産業連合会）、⑦Katholieke Universiteit Leuven

面談者
1）①-1 Susanne Ludgate, Clinical Director, 2 Christopher Brittain, Senior Medical Officer, 3 Rebecca Sugden, Regulatory Affairs Specialist, 4 Suzanne Halliday, Team Leader, Dental/Orthopaedics, Healthcare, BSI
② Joanna Nicholls, Research Manager, Department of Surgery
2）③ Klaus G. Parhofer, Oberarzt Medizinischen Klinik II
④ Christian Schuebel, Medical Evaluation, Clinical Affairs
3）⑤-1 Laurent Selles, Deputy Head of Unit

F3 -Cosmetic & Medical Devices, 2 Celine Bourguignon: Cosmetics and Medical Devices

⑥-1 John Brennan: Director, Regulatory Affairs, 2 Philippe Auclair, Director, Regulatory Affairs, Quality Assurance & Compliance, Abbott Vascular International.

⑦-1 Anne van Hecken, Site Coordinator, Center for Clinical Pharmacology, 2 Gina van Oosterwijck, Study Coordinator, Interventional Cardiology

英国、ドイツ、ベルギーの3カ国を訪問したが、ベルギー以外は治験に限らず臨床試験について全てが政府機関に事前承認されなければならないというのがここ 2-3 年の大きな変化であった。共通の書式も定められており、米国のシステムに似通ったものとなる。試験実施者には大変な負担となっているようである。

EU では植え込み型機器でも臨床試験なしで文献による説明が可能であれば承認可能であったが、批判も多く Medical Device Directive, MDD が補填された。

GCP は薬剤溶出性冠動脈ステントなどを除いて ISO 14155 が使われている。これは GCP ではなく guidance であるとの規制当局側認識もある。

承認申請を担う Notified Body が現在 EU 全体で 80 もあり、その均質性が問題とされている。近い将来に何らかの規制が入る模様である。

実際に承認申請される Reference State は sponsor の国となることが多く、その後の相互認証も特に問題なくされている。

治験費用についてはどの国でもプロトコルに直接関わるもの以外は通常の医療保険で賄われ、本邦でいわれるような混合診療の問題は生じていない。

無過失補償を含めて Liability insurance は現実問題として殆どの場合、site 側で加入しているようである。

正確な統計は無いが一般に患者が試験に同意する率は高く、その背景として EU での患者側の医師・病院に対する信頼の厚さがある。CE マーク制度など機器については患者には余り理解されておらず、自分の信頼する医師が試験参入を勧めるので、勿論説明は尽くされているが、特に問題なく受け入れるようである。この場合の CRC の役目は本邦と異なり意外に小さい。医学に貢献したいという概念もあり、臨床試験というものの意義、重要性が文化としてよく根付いている。

D. 考察

27 の国、23 の言語を持つ地域が一つの承認システムの下に動いているのはある意味驚愕に値する。構築するのに 50 年かかったとのことであるが、元々車検を非政府組織が行っていたような歴史的背景があり、規制が必要なものとして現場から上に上がっていった経緯がある。

もう一つの大きな要素として医師に対する患者の厚い信頼がある。世界で始めての臨床試験が欧州で行われることが多いが、信頼している医師が説明すれば特に問題なく受け入れられている。結果が例え悪くても大きな問題になることは少なく、マスコミもセンセーショナルに扱うことは殆ど無い。新しい技術を導入するにはリスクが伴うということもよく認識されており、本邦社会の安全性を最優先する考え方とは対極をなす。

このように臨床試験の意味、重要性が社会に広く認知されており、本邦とは文化的違いがある。

E. 結論

本邦と欧州の医療機器規制制度上の隔たりは非常に大きいが、歴史的背景、文化的背景の違いによる部分が多いと考えられる。GHTF

での歩み寄り内容などを参考にしつつ、医療機器の規制に関して、社会としてどのような方向性が今後望ましいのか、国民的議論をする時期に来ていると考えられる。

F. 健康危険情報

該当なし。

G. 研究発表

1. 論文発表

戸高浩司、砂川賢二　九州大学医学部循環器内科
肥大型心筋症、Ca 拮抗薬。「循環器治療薬ハンドブック－エビデンズに基づいたよく使う薬剤 196」、北風政史編、中外医学社、in press, 2009

戸高浩司、砂川賢二　九州大学医学部循環器内科
圧負荷を治す。「重症心不全の予防と治療」、北風政史編、中外医学社、in press, 2009

2. 学会発表

戸高浩司
難治性疾患治療の update－難治性心不全の内科的治療
第 12 回日本心不全学会　イブニングセミナー、2008 年 10 月 17 日、ホテルパシフィック東京

戸高浩司
診療プラクティスと保険償還の Gap をいかに埋めるか
第 8 回日本心血管カテーテル治療学会　タウンホールミーティング、2008 年 11 月 25 日、京都国際会議場

戸高浩司
市販後調査・試験の今後のあるべき方向と課題
第 4 回医薬品評価フォーラム、2009 年（平成 21 年）2 月 16 日、日本薬学会長井記念ホール

H. 知的財産権の出願・登録状況

（予定を含む。）

1. 特許取得
特になし。

2. 実用新案登録
特になし。

3.その他
特になし。

Ⅲ. 資料編

【P.1】

委員会原案 ISO/DTR 80002	
作成日 2008年5月6日	参照番号
この原案によって差替えられる文書	ISO/TC 210　N 333

警告：この文書は、ISO国際規格ではない。この文書は、レビュー及びコメントのために回覧されるものである。この文書は予告なく変更されることがあり、国際規格として引用してはならない。
この原案の受領者が認識している関連特許権があれば、コメントを付けて通告書を提出するとともに、関係書類を提供するよう求める。

ISO/TC 210 名称 医療機器の品質管理と関連する一般事項 事務局　米国医療計測機器振興協会（AAMI）　（ANSI向け）	次の目的のために、P メンバー及び O メンバー、並びに専門委員会及びリエゾン関係にある機関に配布される： □（場所）で（議題）について検討 ［会合の日時／場所］ ☒2008年8月15日までにコメント提出 ［日付］ □ISO/IEC 指令第1部 2.5.6 に基づく DIS 登録の承認 ［日付］ （P メンバーのみによる投票：投票用紙を添付） 関連専門委員会又は分科委員会の P メンバーは投票の義務を負う。

英文題名
医療機器ソフトウェア－ISO 14971 の医療機器ソフトウェアへの適用に関する指針

仏文タイトル

基準記述言語：　☒英語　□フランス語　□ロシア語

全般的注記
この委員会原案（CD）は IEC/SC 62A 及び ISO/TC 210 の合同作業グループ（JWG）が作成したものであり、コメントを求めるためにのみ両委員会に回付している。
会員団体は、コメント提出に際しこの文書の行番号を使用されたい。

【P.2】

目次

研究用翻訳につき再配布禁止

【P.3】

国際電気標準会議

医療機器ソフトウェア —
ISO 14971 の医療機器ソフトウェアへの適用に関する指針

まえがき

1) 国際電気標準会議（IEC）は、各国の電気専門委員会（IEC 国内委員会）が参加する標準化のための世界的な機関である。IEC は電気及び電子分野における標準化に関するすべての問題点について、国際的協力を推進することを目的としている。この目的のため、他の諸活動に加えて、IEC は国際規格、技術仕様書、技術報告書、公開仕様書(PAS)、及びガイド（これ以降、"IEC 出版物"と呼ぶ）を発行している。これらの作成は、専門委員会に委嘱しており、取り扱われるテーマに関わりのあるすべての IEC 国内委員会も、この作成作業に参加できる。また、IEC と提携している国際機関、政府機関及び非政府機関もこの作成作業に参加している。IEC は国際標準化機構（ISO）との協定条件に従って同機構と緊密な協力をしている。
2) それぞれの専門委員会は関わりを持つすべての IEC 国内委員会を代表しているため、技術的問題に対する IEC の正式な決定又は合意は、関連内容に関し国際的コンセンサスをできるだけ正確に示している。
3) IEC 出版物は、国際的に使用されるものとしての勧告の形式を取っていて、この意味で IEC 国内委員会によって承認されている。IEC 出版物の技術内容が正確であることを確実にするためあらゆる適切な努力を払っているが、IEC はすべての最終使用者によるそれらの使われ方又は誤った解釈に関して責任を負うものではない。
4) 国際的な統一を推進するために、IEC 国内委員会は、IEC の出版物をそれぞれの国内規格及び地域規格として可能な限り広い範囲まで適用することを保証する。IEC 出版物及び対応する国内規格又は地域規格の間に相違がある場合は、後者の規格に明示されなければならない。
5) IEC は、その承認を示すマーキングの手順を規定しておらず、かつ、IEC 出版物に適合している旨を表示してあるすべての機器についていかなる責任も負うものではない。
6) すべての使用者は、この出版物の最新版を保持していることを確認することが望ましい。
7) 個別の専門家及び IC の専門委員会のメンバー並びに、IEC 国内委員会を含む IEC 又はその役員、従業員、使用人若しくは代理人に対して、人権被害、物的損害若しくは直接又は間接的にいかなる種類の損害、又は出版物に起因する費用（法的費用を含む）及び経費、この IEC 出版物又はその他いかなる IEC 出版物の使用、若しくは信頼性に関して責任を問うことはできない。
8) この出版物で言及する引用規格に注意が必要である。この出版物を正しく適用するためには、引用された出版物の使用は不可欠である。
9) この IEC 出版物の一部の要件は、特許権の対象となっている可能性があることに注意が必要である。IEC では、これらの特許権の一部又はすべてを特定する責任を負うものではない。

IEC 専門委員会の主要任務は、国際規格の作成である。しかしながら、例えば「最先端技術」など、国際規格として通常発行されるものとは異なる種類のデータを収集した際は、技術報告書の発行を提言できる。

IEC 80002 は技術報告書であり、IEC 専門委員会 62 *医療用電気機器* (62: Electrical equipment in medical practice)の分科委員会62A *医療に使用する電気機器の共通事項* (62A: Common aspects of electrical equipment used in medical practice)及び ISO 専門委員会 210 *医療機器の品質管理と関連する一般事項*(210、 Quality management and corresponding general aspects for medical devices)の合同作業グループによって作成された。

この技術報告書の本文は、次の文書に基づいている：

参照原案	投票に関するレポート
62A/XX/DTR	62A/XX/RVC

【P.4】

この規格の承認投票に関するすべての情報は、上の表に示した投票結果報告書に記載されている。

この出版物は、ISO/IEC 指令、第 2 部に従って起草されている。

委員会は、IEC ウェブサイト"http://webstore.iec.ch"において保守結果期日 [1]が特定の出版物と関係するデータ中に明示されるまで、この出版物の内容を変更しないことを決定した。その期日に、この出版物には、次のいずれかの処置を行う。

- 再確認
- 廃止
- 改訂版と置き換え
- 修正

[1] 国内委員会は、この出版物の保守結果期日が(月付)であることに注意しなければならない。

【P.5】

医療機器ソフトウェアー
ISO14971 の医療機器ソフトウェアへの適用に関する指針

1 適用範囲

この技術報告書は、ISO 14971:2007 *医療機器－医療機器へのリスクマネジメントの適用* (ISO 14971:2007、Medical devices- Application of risk management to medical devices)に規定されている要求事項を、IEC 62304：2006 *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* (IEC 62304：2006、 Medical device software- Software life cycle processes)に従って医療機器ソフトウェアに適用するための指針を記載したものである。この報告書は、ISO 14971:2007 や IEC 62304:2006 の要求事項に追加や変更を加えるものではない。

この技術報告書の対象者は、医療機器／システムにソフトウェアが含まれている場合のリスクコントロールの実施方法を知っておく必要があるリスクマネジメント実施担当者、及び ISO 14971:2007 *医療機器－医療機器へのリスクマネジメントの適用* で規定されているリスクマネジメントに関する要求事項の実現方法を理解しておく必要がある工学技術実施担当者である。

世界各国の規制当局に認識されている ISO 14971:2007 *医療機器－医療機器へのリスクマネジメントの適用* は、医療機器のリスクマネジメントを実施するときに使用する主要規格として広く認められている。そして、IEC 62304：2006 *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* は、ISO 14971 を引用規格としている。これら二つの規格の内容が、この技術報告書の基礎になっている。この技術報告書の構成は、ISO 14971:2007 のそれに倣っている。

ISO 14971:2007 は、医療機器のリスクマネジメントに関するフレームワークや分類法は規定しているが、ソフトウェア開発に関連する要求事項については詳細情報も説明も規定していない。IEC 62304:2006 は、ソフトウェア開発プロセスに焦点を当てており、各開発プロセス内のリスクマネジメント活動に対して具体的に言及している。ただしこの規格は、ソフトウェアリスクマネジメントの詳細な方法は規定しておらず、ソフトウェアリスクマネジメントを医療機器リスクマネジメント（全体）に統合する方法についても十分には説明していない。
そこでこの報告書では、できるだけそれらの詳細情報を説明するようにした。

この技術報告書は、以下に記載する多様な医療機器ソフトウェアのリスクマネジメントに該当する情報を含んでいる：
- 組込みソフトウェアシステム
- スタンドアローンソフトウェアシステム（例：線量計算プログラム）
- 情報システム（例：臨床情報システム RIS）
- 附属システム（例：放射線治療計画システム）
- 遠隔医療システム

この技術報告書は、以下の事項は扱っていない：
– 既存の規格又は計画中の規格によって既にカバーされている分野。例えば、警報、人間工学、ネットワークなど。
– 生産／品質システムソフトウェア
– ソフトウェア開発ツール

この技術報告書では、" should"、" can"、及び" might" は以下の意味で用いる。
" Should、（することが）望ましい" は、ISO 14971:2007 の要求事項を満たす可能性が複数ある場合に、その中の一つを特に適合するものとして、他の選択肢に言及したり他の選択肢を排除したりすることなく、勧告するときに使用する。また、行動方針は好ましいが必ずしも必要というわけではないことを示すためにも使用する。
" Can、（することが）できる、可能である" 及び" might、かもしれない、してもよい" は、可能性又は選択肢を示すときに使用する。これらの用語は、要求事項を示すものとして解釈してはならない。

【P.6】
2 用語と定義

この技術報告書のために、ISO 14971:2007 及び IEC 62304:2006 で定める用語と定義を適用する。

3 リスクマネジメントに関する一般要求事項
3.1 リスクマネジメントプロセス

ISO 14971:2007 から抜粋
3 リスクマネジメントに関する一般要求事項

3.1 リスクマネジメントプロセス

製造業者は製品のライフサイクルを通し、医療機器に関係する「ハザード」を特定し、関係リスクの推定及び評価を行い、これらのリスクを管理し、管理の有効性を監視するという継続的なプロセスの確立、文書記録、及び保守を行う。このプロセスには、以下の要素を含める。

- リスク分析
- リスク評価
- リスクコントロール
- 生産／生産後情報

ISO 13485:2003 箇条 7 [8]で示すような文書化された製品実現プロセスが存在する場合、そこにリスクマネジメントプロセスの該当部分を組み込むこと。

注記 1：文書化された品質マネジメントシステムプロセスは、安全性への体系的な対応、特に、複雑な医療機器及び医療システムでのハザード及びハザード状態の早期特定の実現に使用できる。

注記 2：リスクマネジメントプロセスの概略図を図 1 に示す。具体的なライフサイクルの段階によって、リスクマネジメントの個別要素の持つ重要性は変わりうる。また、リスクマネジメント活動は、医療機器に対して反復的に又は複数段階に分けて適宜実施することもできる。附属書 B には、リスクマネジメントプロセスの各段階のより詳しい全体像が含まれている。

適合性は、該当文書の検査によって確認する。

【P.7】

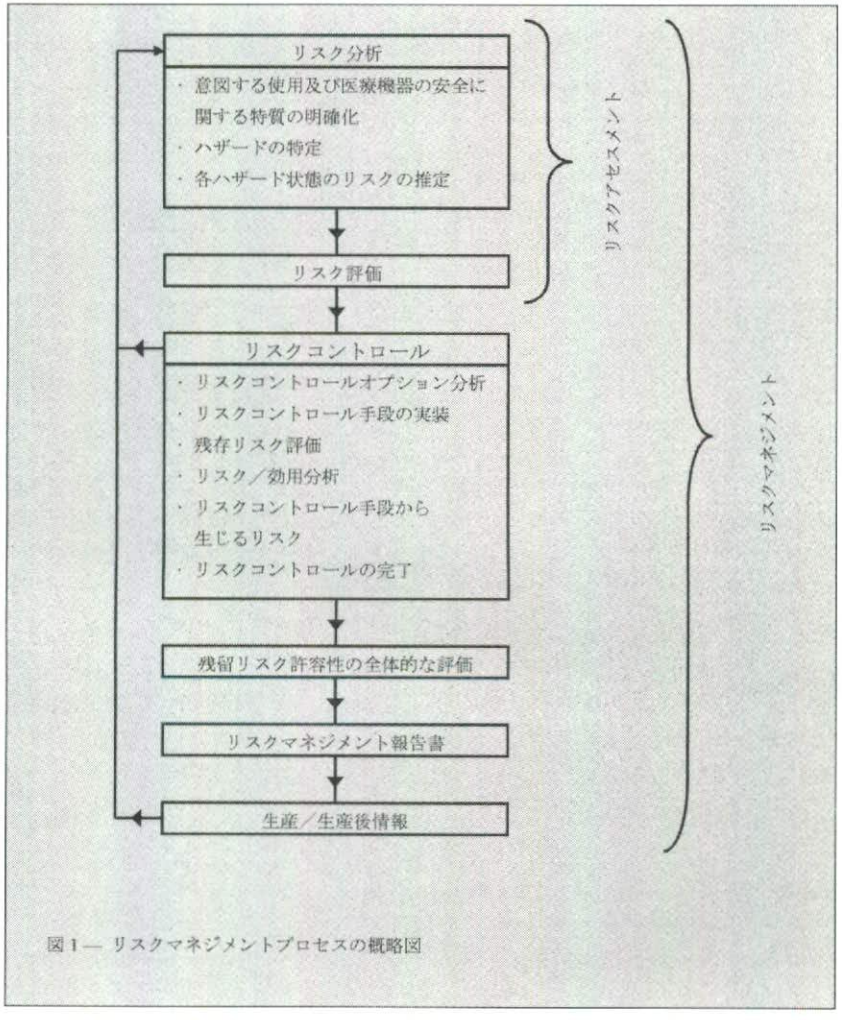


図1— リスクマネジメントプロセスの概略図

3.1.1 一般

この報告書はソフトウェア[2]に主眼を置いているため、ソフトウェアのリスクマネジメントプロセスは独立したプロセスであるようかのように思えるかもしれない。しかし、安全性はシステムの属性である。ソフトウェアのリスクマネジメントを医療機器（システム）のリスクマネジメントから切り離せば、システムに対する近視眼的な見方と安全性要求事項への不適合の大きな可能性を伴う、不完全な機器分析に終わるだろう。ソフトウェアのリスクマネジメント活動は、医療機器ハザードのソフトウェアの原因及び医療機器ハザードに対するソフトウェアリスクコントロール手段に関連する、システムレベルのリスクマネジメントの一部に過ぎない。

リスクマネジメントのソフトウェアの部分は、医療装置全体のリスクマネジメントから切り離すと有効に実施できないが[3]、ソフトウェアエンジニアがソフトウェアライフサイクルの不可欠な一部として実施することで最善となりうる活動や、医療機器のリスクマネジメント全体について規定している ISO 14971:2007 よりも詳細で異なる説明を要するソフトウェア要素[4]もある。医療機器のリスクマネジメントのこの側面を、単純に「医療機器ソフトウェアのリスクマネジメント」と呼ぶ。強調しておきたい重要なことは、リスクマネジメントが有効になるためにはリスクマネジメントのソフトウェアの部分でさえも、リスク（単なるソフトウェア故障のリスクではなく）に重点を置く必要があるということである。

2 IEC 62304:2006 の適用範囲は、ソフトウェア開発に限定されている。この限定のため、システム開発はほとんど取り上げられていない。ソフトウェア開発は、ソフトウェアがシステム全体の中で果たすことを期待される機能を述べたシステム仕様に付随するソフトウェア仕様で開始されると想定している。

3 ハードウェア故障、ソフトウェア故障、及びハードウェアとソフトウェアのリスクコントロール手段の相互依存性による。

【P.8】

ソフトウェア設計者が機器設計の初期段階において医療機器全体の安全性に貢献する機会は、数多くある。医療機器設計に関する主要な決定がなされるまで、ソフトウェア設計の検討を待つべきではない。そうしないと、重大な初期の要求事項及び設計に関する決定段階で、機器レベルのリスクコントロール手段を実施する機会を逃す、あるいはリスクについての理解が不十分に終わる、ということになりかねない。

医療機器設計プロセスに参加することによって、ソフトウェアエンジニアは、設計が進む中でソフトウェアのリスク及びリスクコントロール手段に関する安全関連の決定に貢献できる。また、ソフトウェアエンジニアは、ハードウェア／ソフトウェアの分離及び機器設計の他の側面、機能性、並びに意図する使用環境及びコンピュータプラットフォームに関わる安全関連の決定を促すこともできる。

3.1.1.1 反復のための計画立案

システム設計との相互作用及びインターフェースは、ソフトウェア開発計画（IEC 62304:2006 箇条 5.1.3）で対処するのが望ましい。ソフトウェア開発計画の目的は、リスク原因をソフトウェアによって軽減し、医療機器ソフトウェアに関するシステム品質要求事項が必ず満たされるようにするソフトウェア開発作業を計画することにある。

この目標を達成するためには、ソフトウェアのライフサイクルを通してリスクマネジメント活動を反復する必要がある。しかしながら、ISO 14971:2007 は設計・開発プロセスについて規定していない。例えば、リスクコントロール手段が実装された場合、ISO 14971:2007 では単に、それがさらなるハザードを招いていないことを確認するためにレビューすることを要求しているに過ぎない。この規定は、手段実装の完了後においてだけ、この疑問を調査するよう指示していると解釈しない方がよい。

IEC 62304:2006 は、ソフトウェアのライフサイクルを通したリスクマネジメント活動の反復と、システム設計活動との連携を要求している。例えば、ソフトウェア開発において、IEC 62304:2006 の箇条 5.2.4 は、ソフトウェア要求事項が確立された際に医療機器リスク分析を再評価することを要求している。この再評価の結果、システム要求事項及び／又は医療機器リスク分析の更新が必要になる場合がある。リスク再評価は、要求事項からアーキテクチャ及び設計、そしてソフトウェアの実装までのすべての段階で反復するのが望ましい。

要求事項レベルでは、ソフトウェアのリスクコントロール手段だけで十分か、又はハードウェアのリスクコントロール手段が必要若しくは望ましく、かつ実施可能であるかどうかを決める必要がある。

アーキテクチャ及び設計のレベルでは、安全性に関係するソフトウェア（クラス B、C）の安全性に関係しないソフトウェア（クラス A）からの分離を決定する必要がある。安全性に関係しないソフトウェア（クラス A）からの潜在的影響を効果的に除去するためには、適切な分離手段を使用しなければならない。この点に関する詳細な検討は、この文書の第 6.2.2.5 項を参照のこと。

ソフトウェアユニット実装中に、一連の条件下で、代表的な環境における代表的な使用者で試験を行うことによって、適用するリスクコントロール手段を試さなければならない。

医療機器の設計が進むにつれ、ソフトウェアに関して定めた機能性が新しいハザード状態又は既に明らかになっているハザードの新たな原因を生んでいないかを検討する必要がある。

---

4 例えば、すべてのソフトウェア故障は（多くのハードウェア故障／機能停止と同様に）ランダムではなく系統的に発生するもので、その確率は正確に推定できない。したがって、リスクの確率要素をソフトウェアに適用する方法は大きく異なる。

【P9】

ソフトウェアが潜在的な原因となる各ハザードは、さらなるリスクマネジメント活動に含めるべく特定するのが望ましい。ハザードの確率若しくは重大性又はリスクコントロール手段に関する初期の想定によって、ハザードの特定が妨げられないのがよい。これは、後の分析で見つかるハザード状態との関連が明らかになる可能性があるからである。

多くの場合最良のリスクコントロール手段は、初期設計の一部として実装可能なものである。したがって、リスク分析計画及び手順が、機器及びソフトウェアのライフサイクルの各段階での関連活動に対処すること、並びにその活動及び方法がさまざまな段階によって異なることを認識することが重要である。ただし、早期のソフトウェアリスク分析は、より多くの情報が入手可能となるライフサイクルの後半の段階で使用する同一の方法で実施したとしても、効果的に行えないことに注意されたい。

なお、IEC 62304:2006 は、ソフトウェア故障の確率を考慮することなく、故障によって起こりうる危害の重大性に基づいてソフトウェア（全体として及び該当する場合は部分としての両方）を分類することを要求している。

ソフトウェア不具合の確率は、その体系的な性質から推定不能とされることが多いが、リスクの確率は最終的に危害が発生するその影響と関連している。したがって、ソフトウェアにおける不具合は、最終的に危害につながる可能性のある事象の連鎖の一部に過ぎない。（一方、ハードウェアも体系的な設計の不具合を含んでいる可能性がある。しかし、通常は製造工程や統計的な数量効果による新たな不具合が存在する）。したがって、事象の連鎖全体を考慮すると、ソフトウェアがもたらす危害のリスク評価とハードウェアがもたらす危害のリスク評価に原則として違いはない。

ソフトウェアの関与に関係なく、確率の評価の品質を最終的に決定するのは、関係情報が十分に揃わないような重大な寄与因子があるかどうかという点である。

リスクマネジメント活動の反復の必要性を生じさせるソフトウェアの別の側面としては、ソフトウェアはハードウェアに比べて変更が容易であるという点が挙げられる。ソフトウェア設計者は、要求される変更に、その他いくつかの（いわゆる「小さな」）変更を素早くひとまとめにしたいと考えることがある。また、「小さな修正」、つまり予定外の文書化されていない変更を、それを行っても一切悪影響は出ないとの見込みの下に、実施したいと考えることもある。この種の「小さなソフトウェア変更」はシステムの挙動に大きな差異をもたらし、ハザード状態を招くおそれのあるエラーを引き起こす可能性がある（例：コード1行の変更が100万行の変更につながる）。ソフトウェアの修正においては、アーキテクチャ、設計、及び実装に注意する必要があるが、以下のような変更による影響には特に注意すべきである。

- 既存のリスクコントロール手段に影響を及ぼす変更
- ハザードの新しい原因を招く変更

このような反復又はリスクマネジメント活動の必要性から、リスクマネジメント計画（この文書の第3.4項参照）を、メンテナンス（生産後）プロセスを含めたシステムとソフトウェア両方のライフサイクルと連携させなければならない。

ソフトウェアメンテナンス計画は、変更、機能向上、及び修正に対するリスクマネジメントの実施方法、並びにリスクコントロールの適切性と新たなリスクの軽減の機会を評価するための現場使用情報の監視方法及び分析方法を示す必要がある。

リスクマネジメント活動の反復は、想定外の安全性問題の特定と対処のために必要だが、ソフトウェア開発の前に実証可能な程度に安全なシステムアーキテクチャを設計することによって、ソフトウェア問題を回避するのが最良である。その後、安全性要求事項が既に整備された強い立場から反復を開始する（IEC 62304:2006 箇条5.1.3参照）。

3.1.1.2 予防的／事後的安全性

安全なシステムは以下のいずれかによって設計できる：

【P.10】

a) 医療機器の販売が見込まれる機能を特定し、それらの機能を実装したシステムを設計し、その後その設計が安全であることを確認する。
b) 安全性に必要な挙動を含めた、医療機器の望ましい挙動と望ましくない挙動をすべて特定し、それらの挙動を実装したシステムを設計する。

言い換えれば、安全性に関する挙動は (1) 事後的に、又は (2) 予防的に、設計できる。

事後的アプローチを取ることも可能で、時にはそうすることも必要であるが（例：旧型製品の改造）、通常は安全な医療機器を実現するための方法として最も有効でも、安価でも、最速でもない。

予防的安全性設計の利点は、次の通り：
- 最初から、医療機器が行わなければならないことと及び行ってはならないことがシステム仕様に含まれている。
- 最初から、非安全状態を回避又は防止しながら、望ましい機能の提供を実証可能なシステムアーキテクチャを計画できる。
- アーキテクチャを完全設計に織り込みつつ、混乱を招くような後戻りを回避しながらリスクコントロール手段を開発できる。
- 安全性アプローチの選択が早期に行える（例えば本質的な安全性確保を最大化し、文書による安全性確保を最小化できる）。

3.1.1.3 ソフトウェアの役割

システム内では通常、複雑な挙動はソフトウェアで実装される。これは、ハードウェアは比較的柔軟性が低く、機能ごとに別々の物理的メカニズムが必要となるのに対し、ソフトウェアは同じ物理的メカニズムを容易に共有して多数の機能や作動モードを実装できるためである。

安全なシステムの設計に対する一般的なアプローチは、次の通り：
1. 望ましい医療機器の機能を特定する。
2. その機能に対応するために必要な物理的メカニズムの仕様を定める。
3. その機能を実装するために必要なソフトウェアの仕様を定める。
4. リスクの特定と評価を行う。
5. リスクが最小になるようにソフトウェアを修正する。
6. ソフトウェアが仕様を確実に満たすようにするための徹底したソフトウェア試験を計画する。

このアプローチに関する問題は、安全性に対して事後的アプローチを使用するという点にある。

ステップ 1 では、医療装置がしてはならないことを特定する機会が失われる。

ステップ 2 では、非安全システム状態を防止する又は安全性に重大な影響を与えるソフトウェアを隔離する物理的メカニズムを明らかにする機会が失われる。

ステップ 4 では、予想外の事態が避けられず、システム設計への後戻りにつながる。

ステップ 5 では、混乱を招くようなシステム設計全体に対する変更を回避するため、機能性と安全性の間で妥協を図ってしまうのが一般的である。

ステップ 6 では、不可能な試みがなされている。徹底的な試験の実施は必要ではあるが、ソフトウェアが相互作用不能な非常に単純なユニットに分割されていない限り、それだけで正しいソフトウェア動作を保証することはできない。

安全なシステムの設計に対する、より優れた予防的アプローチは、次の通りである。

【P.11】

1. 医療機器の、望ましい及び望ましくない（安全でない）機能を特定する。
2. 望ましい機能に対応し、望ましくない機能を防止するアーキテクチャ（ハードウェアとソフトウェアを含む）を規定する。
3. システムの安全性を、アーキテクチャに基づく安全性事例によって実証する。
4. ソフトウェアの仕様を定める。
5. ソフトウェアが、仕様、特に安全関連仕様を確実に満たすようにするための徹底したソフトウェア試験を計画する。

ステップ 1 では、望ましくない機能に望ましい機能と同等のステータスが与えられている。リスクマネジメントは、医療機器仕様書への相当量のインプットを持って早い段階で始まる。

ステップ 3 では、安全性事例を作成することによって、早期段階で安全性を実証する機会が与えられる。特に、ソフトウェアに対する安全性要求事項が現実的なもので、大規模で複雑なソフトウェアアイテムの設計も試験も必要がないことを実証するのが望ましい。

ステップ 4 では、ソフトウェア関連要求事項を既に組み込んだソフトウェアの仕様が定められる。

ステップ 5 では、ソフトウェア試験計画がより現実的なものとなる可能性が高い。ステップ 3 で、安全性が大規模又は複雑なソフトウェアアイテムの試験に基づくものではないことが実証済みのはずだからである。

3.1.1.4 ソフトウェアの問題及び解決策

ソフトウェアを使用したシステムで特に問題になるのは、ソフトウェアが共有できる物理的インフラには限度がないという認識である。これは誤りである。

必要なタスクをすべて実行するための十分なリソースが、必要時に確保されるべきであるというのが、システム設計の原則である。この原則を、ハードウェアのみならずソフトウェアにも適用しなければならない。

ソフトウェアアイテムが安全性に関する役割を担っている場合、以下でなければならない：
- 適宜起動できること。
- 安全関連タスクの実行に十分なプロセッサ時間を確保していること。
- 他のソフトウェアアイテムの干渉から保護されていること。

理想的には、安全性に重大な影響を与えるソフトウェアは、別のプロセッサで動かすのが望ましい。他のソフトウェアとプロセッサを共有する必要がある場合は、安全性事例で以下の疑問に対処するのがよい。

- そのソフトウェアアイテムは必要時にプロセッサへのアクセスを確保できるか？
- そのソフトウェアアイテムは、非安全状態がアクシデントに発展する前に十分なプロセッサ時間を確保できるか？
- そのソフトウェアアイテムに対し、他のいかなるソフトウェアアイテムも、データの破損、割り込み、サービスの拒否、その他の干渉を行えないことを実証できるか？

上記の問題点のすべてを、設計者が目視できるようにする開発手法を選択しなければならない。例えば、オペレーティングシステムのサポートを受けている場合に、すべて問題のない状態で作動するプロセスとして、安全性に重大な影響を与えるソフトウェアアイテムを設計するだけでは不十分である。開発手法は、スケジューリング、優先順位、及びタイミングに関する計画的な設計を可能とするものでなければならない。

十分なインフラの準備と密接に関連するのが、冗長性の問題である。ハードウェア又はソフトウェアの一部が故障した後でも極めて重要な安全メカニズムが作動するように、十分なハードウェア冗長性を確保しなければならない。医療機器が安全シャットダウンモードを持っているという単純なケースでは、医療機器の電源を落とすことができる単純なウォッチドッグタイマ（独自電源）でこの冗長性を構成できるだろう。これより複雑なケースでは、マルチプロセッサが必要となる場合もある。このトピックに関する詳細は、この文書の第 6.2.2 項を参照のこと。

【P.12】

3.1.1.5 ソフトウェアを組み込んだ安全なシステムの特性

ソフトウェアを組み込んだ安全なシステムにおいて、アーキテクチャは以下である場合が多い。

- 安全性に重大な影響を与えるソフトウェアへの過度の要求を避けるため、単純なハードウェア安全性メカニズムを使用する。
- 安全性に重大な影響を与えるソフトウェアは非常に単純なものだけを使用する。
- 安全性に重大な影響を与えるソフトウェアを、多くの独立プロセッサ間に割り当てる。
- すべての必須ソフトウェアを必要時に競合を起こすことなく動かすのに十分なハードウェアを備えている。
- ソフトウェアタイミングについて確率論的設計手法を使用している。
- 使用者に対し故障を警告し、情報に基づく介入の機会を与える。
- 故障状況において巧みに機能を低下させる。
- 故障状況において、可能であればシャットダウンを安全に行う。
- 故障から素早く復帰する。
- 安全関連データの破壊を検知及び／又は防止する手段を備えている。

これらに加え、安全な医療機器のソフトウェアはシンプルである可能性が高い。つまり、設計しやすく、安全性事例で推論しやすく、試験しやすく、操作しやすい。

3.2 経営者の責任

ISO 14971:2007 から抜粋

3.2 経営陣の責任

経営陣は、以下によってリスクマネジメントプロセスへの取り組みの証拠を示すこと：
- 十分なリソースが必ず提供されるようにする。
- リスクマネジメントに必ず有資格者（3.3 参照）を割り当てるようにする。

経営陣は、以下を行うこと：
- リスク許容の基準を決めるための方針を規定し文書化する。この方針は、基準が国や地域の該当する法規制及び関係する国際規格に基づくことを確実にし、一般的に認められた最新技術や利害関係者の既知の懸念などの入手可能な情報を考慮したものであること。
- 計画した間隔でリスクマネジメントプロセスの適合性をレビューしてその効果を継続させ、すべての決定事項及び対応措置を文書に記録する。当該製造業者が品質マネジメントシステムを適切に設置している場合は、このレビューを品質マネジメントシステムレビューの一部とすることができる。

注記： 上記文書は、当該製造業者の品質管理システムによって作成される文書に組込むことができ、リスクマネジメントファイルで参照できる。

適合性は、該当文書の検査によって確認する。

3.2.1 一般

ISO 14971:2007 と IEC 62304:2006 のいずれも、品質システムが適切に設置されていることを前提にしており[5]、ISO 14971:2007 の箇条 3.2 は ISO 13485[1] の経営陣に関する要求事項に追加されたものである。

5 ISO 14971:2007 及び IEC 62304:2006 のいずれも、正式な品質マネジメントシステムを適切に設置することは求めていないという主張もある。しかしながら、ISO 14971:2007 の箇条 3.1 では、リスクマネジメントは品質マネジメントシステムの不可欠な一部となりうると述べており、IEC 62304:2006 の箇条 4.1 では、顧客の要求事項及び該当する法的要求事項を製造業者が一貫して満たす能力を有していることについての実証は、ISO 13485 に適合する品質マネジメントシステム又は当該国の法規制が要求する品質マネジメントシステムの使用によって行えると述べている。また、IEC 62304:2006 は、箇条 4.1 の条項に関する指針を附属書 B.4 で示しており、その中で、適切なソフトウェアエンジニアリング手法／技術を適用するための全体的なフレームワークとしてリスクマネジメントを品質マネジメントシステムの不可欠な一部として確立する必要があると述べている。

【P.13】

経営陣は、医療機器ソフトウェアの安全設計のためのみならず、有効なリスクマネジメントプロセスのために必要となる組織構造、十分なリソース、説明責任、及び教育（第 3.3 項「従業員の資格」参照）を整備することについて責任を負う。

ただし、さまざまなリソース制約により、製造業者はソフトウェアの開発／メンテナンスプロセス活動（例：設計、実装、試験、メンテナンス）の外部委託を検討することができる。この状況でも、計画を作成し、リスクコントロール手段が適切に適用されるようにすることにより、これらのソフトウェアプロセス及び製品に関して適切なリスクマネジメント活動を組込むことについて、経営陣は全面的に責任を負う。

製造業者は、外部委託したソフトウェアプロセス及び製品に対するコントロールの保守について責任を負い、供給業者の候補を選定する上での受入れ基準の設定を検討するのが望ましい（供給業者のコントロールについては ISO 13485[1] 箇条 7.4 参照）。そのような基準には、供給業者が以下を実証することを含めるのがよい：

- ISO 14971:2007 への適合による有効なリスクマネジメント
- IEC 62304:2006 への適合による有効なソフトウェアエンジニアリングの実践
- 顧客の要求事項及び該当する法規制の要求事項を一貫して満たす医療機器ソフトウェアを供給できること

その他の供給業者受入れ基準として、納入するソフトウェアのすべてのコンポーネントにアクセス可能であること、及びその排他的権利を保有可能であること、を含めることができる。(IEC 62304:2006 箇条 5.8 ソフトウェアリリース (IEC 62304:2006 clause 5.8 Software Release))。

外部委託するプロセスや製品に適用するリスクコントロール手段がある場合、そのリスクコントロール手段とその重要性を契約の一部として文書に記録し、供給業者に対して明確に伝えるのが望ましい。

3.3 従業員の資格

ISO 14971:2007 から抜粋

3.3 従業員の資格

リスクマネジメント作業を実行する者は、割当てられた作業について適切な知識及び経験を有していること。これには、必要に応じて、特定の医療機器（又は類似の医療機器）及びその使用についての知識及び経験、関連技術、又はリスクマネジメント手法を含めるものとする。また、適切な資格記録を保守すること。

注記： リスクマネジメント作業は、それぞれの専門知識を提供する複数の機能の代表者によって実行することもできる。

適合性は、該当記録の検査によって確認する。

3.3.1 一般

ソフトウェアシステムの開発及びメンテナンスにかかわるチームメンバーは、割当てられた作業について適切な知識及び経験を備えているのが望ましい。作業を割当てられた者がリスクマネジメントについて要求される知識を備えていることは、必須条件である。特定分野の専門家の関与並びにソフトウェアエンジニアリング／試験スタッフとのかかわり合いの程度及び種類についても、リスクマネジメントに関して考慮しなければならない事項である。

【P.14】

要求される活動を個々の作業者が完全に理解できるようにするには、研修プログラムの開発が必要となる場合がある。

また、ソフトウェアに関するリスクマネジメントチームのメンバーの資格取得も考慮しなければならず、それには特別な研修が必要となる場合がある。

以下の細分箇条で、考慮が必要な要求される知識の分野に関する概要を規定する。

3.3.2 意図する使用／特定分野の知識

正しいリソース（特定分野の専門家）を設計段階の早期から有効活用して、使用者／患者に危害をもたらすおそれのある装置の使用についてのさまざまな手段、モード、及び状況の確立に役立てることが重要である。このようなリソースには、装置の意図する使用又は予見可能な使用について経験を持つ者、医療機器環境に精通した設計者、安全性エンジニア、検証／妥当性確認の専門家、並びに製造の専門家が含まれる。グループとして、意図する使用による潜在的な（臨床上の）危害、関連するハザード状態、及びハザード状態の発生にソフトウェアがどう関わっているかについて完全に理解することが不可欠である。特定分野の専門家の関与及び彼らの公式・非公式の両面でのソフトウェアエンジニアリング／試験スタッフとのかかわり合いの程度と種類は、ソフトウェアリスクマネジメントプロセス、そして機器の最終的な安全性に大きな影響を及ぼす可能性がある。それぞれのリソースが持っている特定分野に特有な知識を共有することにより、各リソースは安全性の観点から、機器開発への貢献を事前に評価する機会を持つことができる。これは、市販後分析の状況でも同様に当てはまる。

ハザードに寄与する確率が最も大きい作業の側面に各チームメンバーが焦点を当てられるようにするのは、この知識である。この知識と認識がなければ、各個人は、ソフトウェアの安全性特性に対処することなく、ソフトウェアの特定の機能特性に焦点を当てることしかできないだろう。公式のリスクマネジメントプロセスはすべてのハザードとその原因を明らかにすることを意図したものだが、実際には、複雑なソフトウェアシステムの場合、このプロセスを完全に実行することはできない。チームメンバーに情報を与えることにより、彼らが日常の開発活動を遂行するに当たり、リスク関連の異常を発見する可能性は高まる。さらに、試験計画の作成そして特に回帰試験の実施が、ハザード要因となる可能性が最も高い、又は他のハザード要因となるおそれのある悪影響を招く可能性が最も高いこれらの範囲に焦点を当てられるようサポートするのは、この知識である。

意図する使用に関する知識並びに直接的及び間接的な臨床上のハザードに関する知識は、教育や既知のプロジェクトにおける専門家の助言で増やすことはできる。しかしながら、類似装置の開発における臨床経験は、公式のハザード分析及びリスクコントロール活動中に重大なハザードとその原因及びリスクコントロール手段の特定を確実なものにするのに役立つ知識をもたらす。

3.3.3 プログラミングの経験及び態度

経験の浅い開発者及び試験者は、ソフトウェアが失敗する可能性のある数多くのパターン、（ソフトウェアが基本としている）要求事項自体が間違いである可能性、又はソフトウェアロジック試験の実行で実際にカバーされる割合がいかに小さいかについて分かっていない場合があり、そのため起こりうる結果について楽観的な見方をしがちである。経験豊富なスタッフは、過去の設計や欠陥の経験から、より現実的といえるかもしれない。したがって、経験豊富なスタッフによる教育と監督、及び経験の浅いスタッフによる過去の前提に対する挑戦的な探求のため、ある程度両者を混ぜることが必要となる。

過去の失敗の経験を通して、又は本質的に客観的若しくは懐疑的な姿勢により、物事は予期せぬ形で失敗しうるしまたそうなるものだとの考えを持って開発や試験に臨むスタッフは、有効なリスクマネジメントを実行するために必要な存在である。

【P.15】

経営陣が、若手の開発者を生産後（メンテナンス）活動に配置することがよくある。ソフトウェアに変更を行うと、未知の悪影響が出る可能性がある。経験と知識のある開発者を、この活動の管理監督に任命するのが望ましい。

ソフトウェアの開発と試験に関する経験、及び特定のソフトウェアプラットフォーム、言語、開発ツール、SOUP（開発経路が未知のソフトウェア）、機器環境に関する技術知識は、リスクマネジメントプロセス内で故障モードとその悪影響を特定する上で不可欠である。これらの知識や経験がなければ、ハザードの潜在的原因を見逃して関連リスクのコントロール手法を省略してしまうおそれがある。

ISO 14971:2007 から抜粋

3.4 リスクマネジメント計画

リスクマネジメント活動を計画すること。したがって、検討中の特定の医療機器について、製造業者はリスクマネジメントプロセスに従い、リスクマネジメント計画を確立し文書に記録すること。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部とすること。

この計画には、少なくとも以下を含めること：

a) 計画したリスクマネジメント活動の適用範囲。計画の各要素を適用する医療機器及びライフサイクル段階を明らかにし記載する。
b) 責任及び権限の割当て。
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。
d) 製造業者の許容リスク決定方針に基づいたリスク許容の基準。危害の発生確率が推定不能の場合のリスク許容基準を含む。
e) 活動の検証。
f) 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。

注記 1：リスクマネジメント計画の開発に関する指針については、付属書 F を参照のこと。

注記 2：計画のすべての部分を同時に作成する必要はない。計画又はその一部を、段階的に作成することができる。

注 3：リスク許容の基準は、リスクマネジメントプロセスの最終的な有効性を確保するために不可欠である。各リスクマネジメント計画について、製造業者は適切なリスク許容基準を選択するのが望ましい。

特に、次のオプションを含むことができる。
- 図 D.4 及び図 D.5 のようなマトリックスで、危害の確率と危害の重大性の組合せが許容可能か否かを示す。
- マトリックスをさらに細分化し（例：無視できる、リスクの最小化で許容できる）、リスクが許容可能かどうかを判断する前に、まずは合理的に実践可能な限りリスクを小さくすることを要求する（D.8 参照）。

どちらの選択肢を選んだ場合でも、リスク許容基準の決定に関する製造業者の方針に従って決定するのが望ましく、したがって国又は地域の該当する法規制及び関係する国際規格に基づき、一般的に認められた最新技術や既知の利害関係者の懸念などの入手可能な情報を考慮するのがよい（3.2 参照）。このような基準の確立に関する指針については、D.4 を参照のこと。

【P.16】

医療機器のライフサイクル中に計画が変更された場合、変更記録をリスクマネジメントファイルで保守すること。

適合性は、リスクマネジメントファイルの検査によって確認する。

3.4.1 一般

リスクマネジメント計画は、少なくとも以下[6]を含めることにより、ソフトウェアが医療機器の一部であるという側面に対処するのが望ましい：

- ソフトウェアが、特にその機器のために開発され、SOUP として若しくはこれらのアプローチの組合せとして再利用又は使用されるというステートメント。
- ソフトウェアは IEC 62304:2006 に従って開発されるというステートメント。
- ソフトウェア開発計画への参照表記。このソフトウェア開発計画の内容は、別の一連の文書で物理的にカバーできる。そこで、リスクマネジメントに関係する部分を含むそれらの文書に、参照表記（引用先）を付けるのが望ましい（以下を参照）。
- ソフトウェアが招く又は管理するリスクについて、機器の他のコンポーネントのリスクと異なる場合のリスク許容基準。

危害発生の確率若しくは危害の重大性の定性的又は定量的分類に使用するシステムはすべて、リスクマネジメントファイルに記録するのが望ましい。分類のために、ソフトウェアが異なるシステムを必要とするか否かを考慮する必要がある。しかしながら、可能な限りそのような相違は回避するのがよい。危害発生の確率が推定不能なハザード状態については、リスク評価及びリスクコントロールで使用するために、予想される結果を列挙するのが望ましい（この文書の第 4.3.2.3 項を参照のこと）。

ただし、ほとんどの場合、ソフトウェアが招くリスクについて異なるリスク許容基準を持つ理由はないはずである（リスク推定の箇条も参照のこと）。

関係する生産／生産後情報の収集及びレビューに関連する活動を計画する際は、次の 2 つのソフトウェアの具体的側面を考慮するのが望ましい：

- 通常、SOUP 製造業者は少なくとも SOUP の新バージョンを提供するときには、潜在的な問題に関するデータを提供する。これらのデータの監視を計画し、可能であれば、SOUP 取得時に SOUP 供給業者と契約を結ぶことによってサポートするのが望ましい。機器の使用者が（故意か否かを問わず）自ら機器の SOUP 部分を修正することが可能な場合は、新しい SOUP バージョンの市場への供給に監視の目を向けるよう特に注意しなければならない。ソフトウェアの SOUP リリース後については、この文書の第 9 項を参照のこと。

- 苦情元は、ソフトウェアバージョンの識別記号を特定できること及びその情報の提供を要求できることが望ましい。これは一方では、現場には通常さまざまなバージョンが存在するためであり、他方ではほとんどの場合目視可能な識別記号の提供は（ディスプレイを駆動させるものである限り）ソフトウェアで簡単に行えるためである。ソフトウェアを組合せる場合は、現場からの情報として複数の識別記号が必要になることもある。

リスクマネジメント計画とソフトウェア開発計画の関係

- リスクマネジメント計画とソフトウェア開発計画については、ISO 14971:2007 及び IEC 62304:2006 が同一の内容（例えば責任など）を求める場合であっても、両者間での矛盾や不要な重複を避けるのが望ましい。両者間のインターフェースは、対象とする使用者に基づいたものにするのがよい（IEC 62304:2006 箇条 5.1.7 を参照のこと）。

- ISO 14971:2007 及び IEC 62304:2006 がともに、リスクマネジメント計画やソフトウェア開発計画など計画名称を明示的に示す一方、ニーズ（例：検証計画におけるハードウェアとソフトウェアの組合せ検証 vs. 前ソフトウェア活動の組合せ及び全ハードウェア関連活動の組合せ）に応じた計画の構成は各団体に委ねられている。多くの場合、これは団体内の責任構造に関連している。加えて、プロジェクト固有及び団体固有の計画を組み合わせることもできる（プロジェクト計画 vs. SOP（標準作業手順））。

---

6 ソフトウェアの開発元がサードパーティであるか否かはソフトウェア固有の問題ではなく、したがってここでは扱わない。

【P.17】

- どちらの計画を先に作成すべきかという疑問が生じる場合がある。すべてのケースに当てはまる回答はないが、計画はプロジェクトが進展する中でも一貫しているのが望ましい。リスク許容基準は早期に作成される場合もあるが、検証活動は（少なくとも詳細については）設計の詳細がある程度分かった後にのみ計画可能である。この場合、リスクマネジメント計画から始めることになるかもしれないが、リスクマネジメント計画の作成を完了する前にソフトウェア活動をある程度計画しておく必要がある。この問題を解決するためには、リスクマネジメント計画とソフトウェア開発計画を並行して作成することも、さまざまな部分に分けてそれぞれを最終的に必要になるときに備えておくこともできる。あるいは、リスクマネジメント計画の一部を概念レベルで定め、のちにソフトウェア開発計画でそれらを詳細化するというアプローチもある。また、各計画の中に同期要求事項を記載することもできる。最終的に、両計画が期限までに利用可能となりその内容が十分な権限を持つ者の承認を受けることを確実にする必要がある。

IEC62304:2006 に従ったソフトウェア開発計画に関する具体的なリスク関連トピック

多言語ラベル表示の場合の使用者情報の実装には、注意すべきである（IEC 62366[5]も参照のこと）。特に、それ自体がリスクコントロール手段であるラベル表示の部分についてはなおさらである。これに対応するためのツールは多数存在する。コードと使用者情報テキストを分けるのが良策である。以下には、特に注意すべきである。

a) 言語によって異なるスペースの必要性
b) 異なる文字セットの使用
c) 記号の代わりとしての文字使用
d) 数値結果に対して追加のスケーリングが必要となる可能性のある別の単位の使用
e) 妥当性確認への対応

- ソフトウェアの開発に関連する規格、手法、及びツールが、有効なリスクコントロール手段となるようにすること（IEC 62304:2006 箇条 5.1.4 項に従い、ソフトウェア開発計画で求められる）。これは、他の団体、供給業者、団体内の他のプロジェクトによる証拠の提供によって行ってもよい。不明な場合、プロジェクト内で有効性を計画し検証すること。

機器のリスクマネジメントプロセスを確立する際は、安全コーディング規格、検証手法（例：正式証明、ピアレビュー、ウォークスルー、シミュレーションなど）、及び構文／ロジックチェッカーの使用などソフトウェアのリスクマネジメントに特有の側面を考慮するのが望ましい。

ソフトウェアのリスクマネジメント活動は、機器開発の段階ごとに計画、手順又は訓練で適宜対処するのがよい。

ISO 14971:2007 から抜粋

3.5 リスクマネジメントファイル

検討対象となっている個々の医療機器について、製造業者はリスクマネジメントファイルを作成し保守すること。この国際規格の他の箇条の要求事項に加えて、リスクマネジメントファイルは、以下に対して明らかにした各ハザードのトレーサビリティを提示すること。

- リスク分析

- リスク評価

- リスクコントロール手段の実装及び検証

- すべての残留リスクの許容性の評価