医療機器規制に対する期待/要望

平成 20 年 5 月

1.医療機器法

医療機器は、薬事法によって規制されている。薬事法では、医療機器は医薬品等の“等”に含まれている。しかし、医薬品と医療機器との間には大きな差異がある。医療機器法制定が望まれる。因みに EU では、医療機器について独自の指令が制定されている。
また、韓国には医療機器法がある。

2.医療機器規制の国際整合化

医療機器規制は、①市販前審査、②市販後監視、③品質マネジメントシステム監査の三分野に大別される。規制内容が国ごとに異なる場合、それは非関税障壁になり、医療機器産業界の負担は多大になる。医療機器規制国際整合化会議（GHTF）によって整合化が進められている。その合意の内容が、わが国における規制に迅速に反映されることを期待する。

3.市販前審査/承認

わが国における医療機器の新製品に対する市販前審査/承認の期間は長過ぎると、内外の批判が強い（ディバイス・ラグ）。わが国における患者は、一、二世代以前の技術/製品の恩恵を受けることしかできない。市販前審査/承認期間の短縮は、焦眉の課題である。

各国とも、機器のリスクに基づいて機器の市販前審査/承認に厳しさの差異を設けている。中低リスク製品に対して EU は市販前審査/承認を適用していない。また、米国には簡略審査（510(k)）の制度がある（実績がある製品と同等の製品に対する審査簡略化）。

患者に対して迅速に新技術/新製品を提供する点からすると、EU 方式が最も望ましい。しかし、低リスク製品に対してであれ、直ちに市販前審査/承認を省略することには抵抗があろうと思われる。第一段階として、低中リスク製品に対して米国のような簡略審査制度を導入しメリハリをつけ、審査期間を大幅に短縮することを要望する。低中リスク製品は機種が多い。審査簡略化は、効果大である。一方、海外の規制当局/第三者機関による審査の結果受け入れ及び審査担当官の増強を要望する。

新しい要素はリスクを伴う可能性がある。新技術、新材料、新原理などに基づく新製品の場合、治験による安全確保は重要な意義を持つ。一方、現状の治験には、所用期間が長い、高額の費用を要するなど問題点が多い。治験の改善とともに、他国における治験の結果の受入れなどによって、同一作業の重複が除去されることを期待する。

4.市販後監視

市販後監視の一環として、不具合事象報告が義務付けられている。しかし、不具合事象報告の分析及びその結果の反映が適切に行われているとは云い難い。製品の安全確保の原点は、同一又は類似の事故（不具合事象）を再発させないことである。不具合事象報告の統計的分析の結果を、適切な形で医療機器業界/企業に伝達し、製品の安全確保に活用させることを期待する。米国の FDA では、それに類する活動を行っている。

5.品質マネジメントシステム

品質マネジメントシステムは、国際規格（ISO 13485）に基づき最も国際整合化が進んでいる分野である。しかし、各国が、その監査の結果を相互に受け入れる状態には至っていない。国際化されている企業では、毎年、各国の規制当局及び第三者機関による多数の監査を受けているのが実状である。特にわが国の場合、①品質マネジメントシステムを担当する機関が三箇所に分かれている（総合機構、都道府県、第三者機関）、②他国に例がない品目別の監査を行っている、③わが国独自の要求を行っているなど、問題点が多い。品質マネジメントシステム監査を簡略化することを要望する。また、相互承認協定（MRA）の締結などによって、わが国の監査結果を他国に受け入れさせるとともに、他国の監査結果を受入れ、同一目的の重複する監査の負担を除去することを期待する。

また、品質マネジメントシステム監査の基準（国際規格 ISO 13485）が改訂されず、実態との乖離を生じている。関連する国際組織に働きかけ、製品の安全確保のため迅速に改訂を行う体制を確立することを期待する。

6.中小企業への対応

医療機器規制に対応するための費用は、益々、増加している。一方、医療機器業界には中小企業が多い。規制上、中小企業に配慮することを要望する。米国では、市販前審査の料金低減など、中小企業優遇策が導入されている。

7.新技術開発支援

医療機器の多くは最先端技術製品であり、その進歩も速い。内視鏡を中心に、画像診断装置は国際競争力があるが、医療材料系（カテーテル、ステントなど）の製品は圧倒的入超である。最先端技術分野への戦略的集中投資、ベンチャー企業の育成、予算の統合など、わが国の医療技術及び医療機器の国際競争力強化に対する強力な支援を期待する。米国の NIH のような、医療技術分野における集中的統合組織も必要であろう。また、関連組織の連携強化も期待したい。

医療機器 software の規格/規則の概要及び現況

三浦

1.規格と規則

1)規格

規格の適用は、原則として任意（自主的）である。規格の開発は国際組織である ISO、IEC、ITU が担当する。規格には、その開発時点における最新技術も取り入れられる。規格によっては、認証制度がある（例えば、ISO 9001、ISO 13485）。規格の認証は全世界共通であり、審査/監査のための審査登録機関がある。全世界において審査登録機関を認定する機関が IAF であり、国内では（財）日本適合性認定協会が認定を担当している。また、審査/監査及び審査登録機関に適用する規格の開発は、CASCO が担当している。規格に対する不適合に対しては認証が取り消されることもある。

2)規則

規則（regulation）は法的に強制される。日本の場合、政令、省令などが規則に該当するが、夫々、政府及び各省が制定する。医療機器の場合、規則を国際整合化するために GHTF がある。GHTF による指針文書は、各国の規則の基になる。規則は確定した技術に基づく。規則の不適合は違法である。重大な不適合に対して、各国の規制当局は、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。懲役が課されることもある。規則には有限の資源で最高の効率を挙げるために効率が求められる。規則の場合、最低限の要求事項（minimum requirement）と云われることがあり、凝縮し、基本的要素で構成することが求められる。ただし、一部の規格が規制目的に使われる場合があり、その典型例が ISO 13485 である。表題にも明示されているように規制目的に開発された。また、EU では基本要求事項のみを法令として制定し（医療機器指令など）、特定の規格（調和規格）を規制目的に使用する場合がある。

2.Software の規格

医療機器 software の規格には、ISO/TC 210 と IEC 62A の間に設けられた合同作業班（ISO では JWG 2、IEC では JWG 3）が開発を担当した IEC 62304 がある。これは医療機器 software を開発するための品質 management system（QMS）に対する要求事項を規定した規格であり、Risk management も要求事項に含まれ、ISO 14971 が引用規格になっている。ISO 62304 は、FDA と AAMI が共同で開発した AAMI SW 68:2001 を基にして 2002 年に開発が開始され 2006 年に発行された。2009 年が見直し時期に当り、P-member の投票によって、①改正、②確認（現状維持）、③廃止の何れかから選択するように規定されている。因みに、JWG 3 の member の多くは、現状を維持し、見直しを延期することを望んでいる。

現在、JWG 2 は IEC 62304 の指針文書として“医療機器 software—ISO 14971 の医療機器に対する適用“の開発を進めており、委員会原案（CD）の段階にある。技術報告（Technical Report、TR）として 2010 年 3 月に発行の予定である。また、IEC 62304 の指針開発も提案されているが、正式の新提案項目（NWIP）は未発行である。

3.医療機器規制の枠組み

医療機器規制の主要素は、①市販前審査、②市販後監視、③品質 management system（QMS）である。GHTF では、市販前審査及び医療機器規制に関わる全般的事項を SG 1（第 1 研究班）、市販後監視を SG 2、QMS を SG 3、QMS の監査を SG 4 が担当している。最も新しい SG 5 は臨床評価を担当しており、これは市販前審査の一環をなす。

4.医療機器 software の規則

1)医療機器 Software と規制の動向

医療機器 software には、①医療機器に組み込まれるもの（embeded software）と、単独で使用されるもの（standalone software）がある。何れも、国際的には医療機器として扱われている。即ち、GHTF 文書及び ISO 13485 の医療機器の定義には software も含まれており、規制対象になっている。ただし、日本において software は医療機器ではなく、規制対象ではない。

一方、近年、software に起因する有害事象が増加を続けており、2006 年まで 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新技術開発を挙げた。その考え方が 2010 年に発効する改正医療機器指令に反映され、software validation が要求事項になった。

FDA も医療機器 software の重要性を強調、2005 年 3 月に Spain で開催された GHTF 運営委員会（SC）で software の規制の検討に着手することを提案、同年 11 月に Software 臨時作業班（AHWG）を編成した。

2)Software 臨時作業班の提案

Software 臨時作業班が最初に提示した活動対象項目は、次の通りであった。

1) 市販前審査における software を含む承認申請の検討
2) SOUP（OTS）の評価
3) Network 接続された医療機器の cyber security 確保
4) Software 安全性の評価基準
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
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

2006年6月にLuebeck（独）で開催されたSC会議において、臨時作業班が提案した上記の活動案の中から、当面、緊急を要する次の3件に的を絞ることが決定された。

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の審査の指針
3) Software processの監査及び監査員の資格に関する指針

上記のSCの指示により、2007年1月に臨時作業班は、次の推奨事項をまとめた。

1) SG 1に対する推奨事項（市販前審査の関係）
   - Standalone softwareに関する基本要件の変更
   - 基本要件のsoftwareに関する規定を、EUの改正医療機器指令に合わせる
   - 用語“Software（関連用語を含める）”を定義する
   - STEDに、softwareとの相互関係に関する記述を追加する
2) SG 2に対する推奨事項（市販後監視の関係）
   - 不具合事象報告の事例を追加する
3) SG 3に対する推奨事項（QMSの関係）
   - 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開発にも適用する
4) SG 4に対する推奨事項（QMS監査の関係）
   - SoftwareのQMSの監査指針を開発する
5) SG 5に対する推奨事項（臨床評価の関係）
   - Softwareの一部に臨床証拠を要求する
6) 全般（共通事項）
   - Accessory及びdataに関する要求事項を追加する
   - SoftwareのQMSの監査基準を開発することの要否を検討する

以上に基づき、SG 1は基本要件変更の検討に着手。SG 3は拒否。SG 4は準備中。

5.Software規制に対する提案

前述のように、医療機器規制には市販前審査、市販後監視、QMSとその監査がある。市販前審査について、医療機器に組み込まれたsoftwareの場合、現在も医療機器と一体として審査されているため、特に新しい問題が発生することはない。一方、standalone softwareの場合、それ自体を医療機器として規制対象とすることが先決。また、その審査については独自の審査基準が必要であるが、Software臨時作業班による推奨事項に基づいてGHTF SG 1が市販前審査の基準になる基本要件を改定するための検討を進めている。市販後監視について、特に変更すべき点はない。

最も問題が大きいのはQMSである。QMSの法的監査基準はISO 13485:2003（米国は例外でありQSRが監査基準）である。QMSの監査基準は単一であるべきであり、ISO 13485以外の文書（ISO 14971、IEC 62304、その他の指針類）を法的監査に使用

してはならない。これは国際的に合意されており、例えばGHTFのQMSの指針には“監査に使用してはならない”と明記されている。また、規格の場合も、指針文書には、“監査における使用は、この文書の意図するところではない”と記載されている。ISO 13485:2003に、製造用software及び測定用softwareに対する要求事項は既に含まれている。ただし、softwareの開発については言及していない。Softwareも製品であり、又はその一部を構成するため、本来、ISO 13485の設計･開発の要求事項の対象にはsoftwareも含まれているはずである。ただし、hardwareと異なる要素が多々あるため、現状のISO 13485の規定をsoftwareに対してそのまま適用することには無理がある。従って、現存するISO 13485:2003を変更しsoftwareに対する要求事項を明確にすることが不可欠である。ただし、ISO 13485の改正に反対する抵抗族がおり、大きな障害になっている。この状態を打破しないと、多くの患者及び医療従事者が
不具合事象に巻き込まれ犠牲になり続けることになる。

また、softwareに起因する有害事象の真の原因はsoftware error（bug）である。Softwareは非線形（nonlinear）と云われる。基本設計などのerrorと些細なprogramのerrorとの間に、引き起こす問題の大きさについては相関がないためである。Programにおける句読点の誤り又はspellingの誤りなどが大事故を惹起する可能性もある。EUが改正医療機器指令でsoftware validationを要求していることには妥当性がある。

従って、softwareに起因する有害事象報告を詳細に分析することが、software規制の検討の出発点になるべきである。その分析を通じて、softwareの開発の何れの段階で、どのような対策を実施すれば良いかが明確になる。

また、規制要求事項は簡潔で解りやすくなければならない。ISO 13485:2003の設計・開発に対する要求事項は3頁に過ぎない。一方、IEC 62304は60頁を超え、多くの専門用語が含まれているため、softwareの専門家以外の者にとって理解するのは容易ではない。Softwareを審査/監査するのは専門家とは限らない。ISO 13485に凝縮した簡潔なsoftwareに対する要求事項を取り込むべきである。

IEC/TR 80002:1
Edition1.0 2009-09

技術報告書

医療機器ソフトウェア -
第1部：ISO 14971の医療機器ソフトウェアへの適用に関する指針
(Medical device software - Guidance on the application of ISO 14971 to medical device software)

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland
Email: inmail@iec.ch
Web: www.iec.ch

IEC出版物について

IEC出版物の技術的内容は、IECによって絶えず見直されている。必ず最新版を使用すること。正誤表又は修正版が発行されている可能性がある。

IEC出版物のカタログ: www.iec.ch/searchpub
IECオンラインカタログでは、様々な検索条件（照会番号、テキスト、専門委員会名など）で検索が可能である。
また、プロジェクトに関する情報、廃止又は差し替えられた出版物に関する情報も提供している。

最新刊情報: www.iec.ch/online_news/justpub

IEC出版物の最新情報をチェック。毎月2回、新しく出版されたIEC出版物のリストを提供している。オンライン又はEメールで入手可能。

エレクトロペディア: www.electropedia.org

世界有数の電子用語及び電気用語のオンライン辞書。20000を超える用語及び定義を収録。言語は英語及びフランス語で、等価語をそれ以外の言語でも示している。エレクトロペディアは「International Electrotechnical Vocabulary online」（国際電気標準用語集オンライン）としても知られている。

顧客サービスセンター: www.iec.ch/webstore/custserv

本出版物についてご意見・ご希望がある場合は、顧客サービスセンターFAQ係又は下記連絡先に連絡のこと。

Email: csc@iec.ch
Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00

IEC/TR 80002:1
Edition1.0 2009-09

技術報告書

医療機器ソフトウェア -
第1部：ISO 14971の医療機器ソフトウェアへの適用に関する指針
（Medical device software - Guidance on the application of ISO 14971 to medical device software）

INTERNATIONAL
ELECTROTECHNICAL
COMMISION

目次

国際電気標準会議

医療機器ソフトウェア -
第1部：ISO 14971の医療機器ソフトウェアへの適用に関する指針
(Medical device software - Guidance on the application of ISO 14971 to medical device software)

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）がすべて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 80002-1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。

参照原案	投票に関するレポート
62A/639A/DTR	62A/664/RVC

この技術報告書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。ISOにおいて、P-member投票総数16のうち賛成票17によって承認された。

この出版物は、ISO/IEC指令、第2部に従って起草されている。

この技術報告書の中で、次の活字を使用した：

・要求事項及び定義：ローマン体の活字。

・注記、例及び参照のような表の外にある参考情報：より小さな活字。表の規定本文も、より小さな活字である。

・この技術報告書の全体を通して使用し、箇条3に定義し、巻末に索引を付した用語：ボールド表記で。

一般表題 医療機器ソフトウェアで出版されている、IEC 80002シリーズのすべての部品リストは、IECウェブサイトで確認できる。

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

重要 – 本出版物の表紙にある“colour inside”のロゴは、本出版物の内容を正しく理解するために有用と思われるカラー表示が含まれていることを意味する。そのため、本出版物はカラープリンターで印刷することが望ましい。

序文

医療機器にはソフトウェアが組み込まれている場合が多い。ソフトウェアを含む医療機器の安全性及び有効性を確立するには、ソフトウェアによって行おうとする処理に関する知識と、許容できないリスクを引き起こすことなくソフトウェアを実装して目的を達成できることを実証することが要求される。

ソフトウェア自体がハザードであるのではなく、ソフトウェアがハザード状態の原因となりえることを理解することが重要である。ソフトウェアは常にシステムの観点から考慮するべきであり、ソフトウェアのリスクマネジメントをシステムから切り離して実施することはできない。

ソフトウェアの設計が複雑であるほど、ハザード状態の原因となりうるイベントシーケンスも複雑になる可能性がある。ソフトウェアのリスクマネジメントでは、ハザード状態を招くおそれのあるイベントシーケンスを識別する作業、及びイベントシーケンスのどの時点でそのシーケンスを途切れさせ、危害を防止又はその確率を低めることができるかを特定する作業が大半となる。

ハザード状態を引き起こすソフトウェアのイベントシーケンスは、以下の2つのカテゴリに分類される。

a) 入力に対して予期しないソフトウェア応答を提示するイベントシーケンス（ソフトウェアの仕様の誤り）

b) 誤ったコーディングに起因するイベントシーケンス（ソフトウェアの実装における誤り）

複雑なシステムを正しく指定して実装することが困難であること、及び複雑なシステムを完全に検証することが困難であることから、上記カテゴリはソフトウェアに限定される。

ハザード状態を招くおそれのあるソフトウェア異常の確率を評価することが困難なこと、及びソフトウェアが劣化によって使用中にランダムに機能しなくなることはないことから、リスク分析のソフトウェア面については発生確率の評価でなくハザード状態を招くおそれのある潜在的なソフトウェアの機能性及び異常の特定に主眼を置くべきである。ソフトウェア異常に起因するリスクは、ほとんどの場合、危害の重大性のみについて評価する必要がある。

リスクマネジメントはどのような場合も困難であるが、ソフトウェアが関わるとよりいっそう困難になる。次箇条以降では、ソフトウェアの細部に関する詳細、及びソフトウェアの観点からISO 14971:2007を理解するための手引きを記載する。

- **技術報告書の構成**

本技術報告書はISO 14971:2007の構成に沿って組み立てられており、ソフトウェアに関するリスクマネジメントの各活動についての手引きを提供している。

提供されている情報には意図的に重複があるが、これはソフトウェアのライフサイクルにおいてリスクアセスメント活動が繰り返されるという性質によるものである。

医療機器ソフトウェア—
第1部：ISO 14971の医療機器ソフトウェアへの適用に関する指針
（Medical device software - Guidance on the application of ISO 14971 to medical device software）

1 概要

1.1 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手引き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ソフトウェアエンジニアである。

世界各国の規制当局に認識されているISO 14971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 は、ISO 14971を引用規格としている。これらふたつの規格の内容が、この技術報告書の基礎になっている。

ISO 14971及び本技術報告書は医療機器に焦点を当てているが、本技術報告書は医療環境におけるあらゆるソフトウェア（それが医療機器に分類されるかどうかに関わらず）のリスクマネジメントプロセスの実施にも適用できることに留意すべきである。

この技術報告書では、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、ユーザビリティエンジニアリング、ネットワークなど
- 生産／品質管理システムソフトウェア
- ソフトウェア開発ツール

この技術報告書は、規制調査又は認証評価の基準として使用されることを意図していない。

この技術報告書では、“Should（～することが望ましい、～すべきである）”は、要求事項を満たす可能性が複数ある場合に、その中のひと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している。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。この用語は、要求事項を示すものとして解釈してはならない。

1.2 引用規格

次の引用規格は、本規格の適用に当たって不可欠である。発行年が記載してある引用文献は、引用した版のみを適用する。発行年が記載されていない引用文献は、その引用規格の最新版（追補すべてを含む）を適用する。

IEC 62304:2006、*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*

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*

2 用語と定義

本文書では、ISO 14971:2007、IEC 62304:2006の中で示された用語及び定義、並びに次の用語と定義を適用する。

注記：定義された用語は63ページの最初に記載されている。

2.1 多様性
冗長性のひとつの形で、冗長成分が異なる（多様な）コンポーネント、技術、又は手段を使用して、共通の原因によってすべてのエレメントが同時に機能しなくなる確率を低減すること。

2.2 冗長性
ひとつの機能に複数のコンポーネント又はメカニズムを備えることによって、ひとつ以上のコンポーネント又はメカニズムが故障してもその機能の働きが妨げられないようにすること。

2.3 安全性に関係するソフトウェア
ハザード状態の原因となりえるソフトウェア、又はリスクコントロール手段の実施で使用されるソフトウェア。

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

3.1.1 一般

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[6]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。

1) 角括弧（[ ]）内の図は、参考文献を参照する。

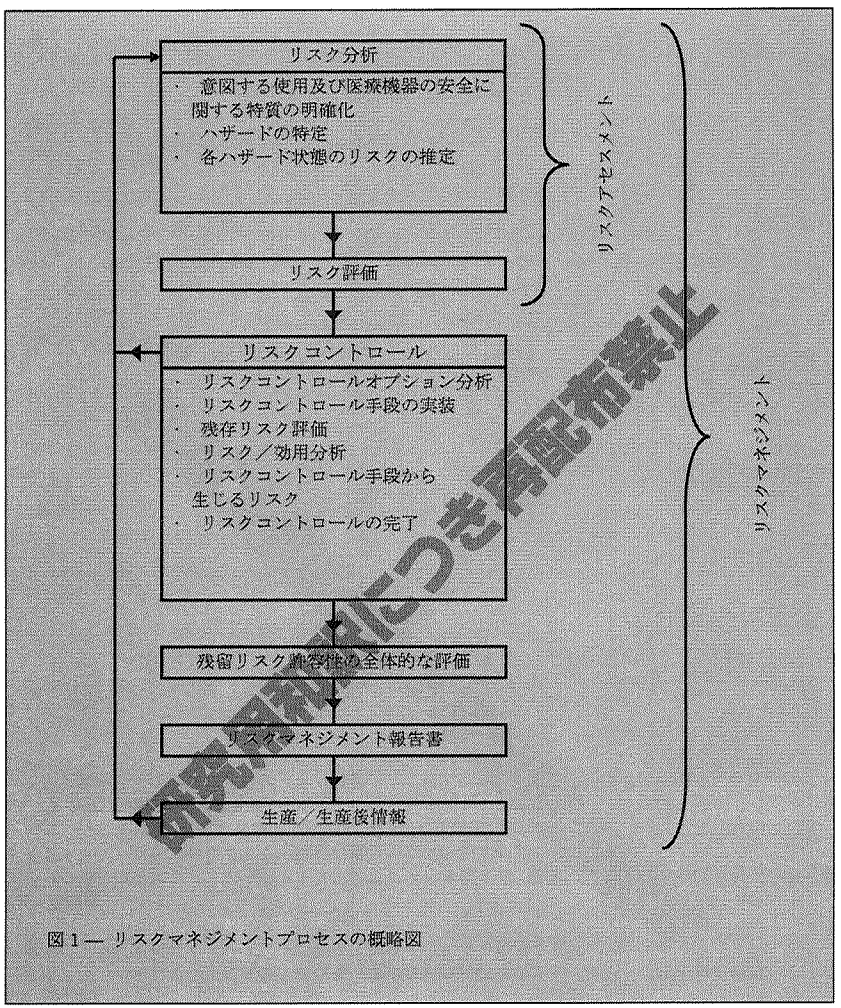


図 1 — リスクマネジメントプロセスの概略図

安全性はシステム（ここでは個々の医療機器全体）の属性のひとつであり、それにはソフトウェアが含まれることがある。リスクマネジメントは、ソフトウェアとそのハードウェア環境全体からなるシステムについて実施するべきである。ソフトウェアのリスクマネジメント活動は、システムから切り離して実施するべきではない。

リスクマネジメントのソフトウェアの部分は、医療機器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、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がある。また、ISO 14971:2007で医療機器のリスクマネジメントに対して記載されているより高いレベルの注意を必要としたり、ISO 14971:2007に記載されている説明と異なる説

明を必要とするソフトウェア要素もある。リスクマネジメントのソフトウェア部分が有効に実施されるためには、ソフトウェアの部分についても医療機器全体としてのリスクを考慮する必要がある、という点を強調することが重要である。

注記1：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が互いに依存しあっているため、リスクマネジメントのソフトウェアの部分は、医療機器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。

注記2：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あり、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。4.4.3を参照のこと。

ソフトウェアエンジニア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。システム設計が確定する前に、医療機器の安全性におけるソフトウェアの役割を考慮するべきである。

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関連のリスクに関する安全関連の決定に貢献できる。安全関連の決定には、例えば以下のものが含まれる。

・ソフトウェアを支援するための十分なハードウェア資源の提供
・ソフトウェアとハードウェアとの間での機能の分割
・医療機器全体の意図する使用、及びソフトウェア ユーザーインターフェースの意図する使用
・不必要に複雑なソフトウェアの回避

3.1.2 反復

標準的なソフトウェア開発のライフサイクルでは、反復を使用することが多い。反復を使用することにより、次のことが可能になる。

・複数の異なるソフトウェア設計の実現可能性の調査
・複数の異なる時期での複数の異なるソフトウェアアイテムの開発
・ソフトウェアの複数の異なるバージョンの段階的な納品
・ソフトウェア開発プロセス中に生じた誤りの修正

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アセスメントを再評価するよう要求している。この再評価の結果、システム要求仕様及び医療機器リスクセスメントの更新が必要になる場合がある。リスク評価は、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。

ISO 14971では設計・開発プロセスを規定しておらず、リスクマネジメント手順を設計（リスクコントロール手段を含む）の実装の前後（実装時ではなく）に実施することを要求しているのみである。例えば、リスクコントロール手段が実装された場合、ISO 14971では単に、それが更なるハザードもハザード状態も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。しかしこれを、レビューは実装が完了した後のみに実施するように、という指示と解釈するのは適切ではない。更なるハザードが明らかになった時点で、即座にそれに対処することが望ましい。これはリスクコントロール手段の実装プロセス内での反復を示唆している。

すべての成果物について常に整合性を保つことが重要である。しかし、反復は成果物の整合性にとって脅威である。そこで、ひとつの変更のすべての影響を確実に識別し、その変更後に該当するすべての成果物が確実に更新されるように、厳格なコンフィギュレーション管理を行うことが必要となる。これはソフトウェアが関わっている場合に特に重要である。なぜならば、ソフトウェアは急速に変更が可能であり、ま

た見かけは小さな変更でも予期しない副作用が生じる可能性があるからである。エンジニア同士の誤解を防ぐためにも、ソフトウェアに関連するすべての情報を最新の状態にしておく必要がある。ソフトウェア変更の提案は、その副作用、特に安全性影響する副作用について検討する。これにより、リスクマネジメント プロセスの一部を反復する結果となることもある。

3.1.3 安全性に対する予防的対応又は事後対応

リスクマネジメントは、医療機器の仕様に十分な入力を投入し、設計の早い段階で安全性を顧慮に入れ、早期に開始することが望ましい。すなわち、予防的設計対応のほうが事後設計対応よりも好ましい。予防的対応では、安全性が他の顧客ニーズと共に考慮され、初期の安全性要求事項として捕らえられる。事後対応は時に避けられないものの（レガシー製品が更新される場合など）、通常は予防的対応が安全な医療機器を実現するための最も効果的、迅速、かつ安価な方法である。

予防的安全性設計の利点として、次のことが挙げられる。

– 最初から、システム仕様に医療機器がすべきことを含めるだけでなく、リスクを低減するために回避すべきシステム挙動をシステム仕様で明確にできる。

– 最初から、不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、手直しを回避しながらリスクコントロール手段を開発できる。

– 安全性へのアプローチ及びリスクコントロール手段を早期に選択できる（例：設計による固有の安全性を最大にし、安全情報の提供を最小にできる）。

3.1.4 ソフトウェアを組み込んだ安全なシステムの特性

安全なシステムの望ましい特性：

– 安全性に関係す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。

– 安全性に関係するソフトウェアは非常に単純なものだけを使用する。

– 安全性に関係するソフトウェアを、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。

– 故障状況に適切に対処する。以下に例を挙げる。

・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。
・故障状態で縮退した機能性を提供する。
・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。

– ソフトウェアコードがその実行環境において自己書き換えにより、又はデータ入力の結果として、書き換えられるのを防ぐ手段を有している。

– 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。

3.2 経営陣の責任

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、製造所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み込むことができ、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。

ISO 14971:2007及びIEC 62304:2006は共に、品質マネジメントシステムが整備されていることを前提としている。経営陣に関するリスクマネジメント要求事項はISO 14971:2007の細分箇条3.2に列記されている。

注記：ISO 14971:2007の細分箇条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の細分箇条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、細分箇条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。

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）を整備することについて責任を負う。

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。その場合でも、経営陣は外部委託したソフトウェア開発又は保守プロセス活動について適切なリスクマネジメント活動が確実に実施されるようにすること、及び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全面的に責任を負う。

ソフトウェア開発を外部委託した場合、製造業者は適切な契約上の合意により、ISO 14971で要求されている、ソフトウェアリリース後のソフトウェア異常の修正を含むすべてのリスクマネジメントが医療機器

のライフサイクル全体を通して確実に実施されるように、製造業者がソフトウェア及びその設計を十分コントロールできるようにすべきである。

製造業者は、供給業者に対して達成要求事項を設定することを検討するべきである（供給業者のコントロールについてはISO 13485 [1] の細分箇条7.4を参照のこと）。例えば、供給業者に対して以下を実証することを求める。

– ISO 14971への適合による有効なリスクマネジメント
– IEC 62304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

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

3.3.1 一般

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、割り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、及び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してもよい。

適合性は、該当記録の検査によって確認する。

ソフトウェアシステムの開発及びメンテナンスに関わチームメンバーは、割り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べきである。リスクマネジメントに関連する作業を割り当てられた者がリスクマネジメントに必要な知識を備えていることが極めて重要となる。臨床専門家（臨床支援及び技術サービスの専門家、その他関連分野の専門家）、ソフトウェアエンジニア、システム設計者、ユーザビリティ／人間工学の専門家、特定分野の専門家などからなる分野横断的なチームをリスクマネジメントに参加させることを検討し、さらにそのチームのソフトウェア技術／試験スタッフへの介入の程度と種類を検討することが望ましい。

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

医療機器の設計のすべての段階において、意図する使用に関する知識を活用することが重要である。これは、ソフトウェアの設計者及びソフトウェアのリスクマネジメントを実施するスタッフにとって、特に特に重要である。ソフトウェアの複雑な挙動は誤使用や使用者の混乱の原因となり、事前に予見できないハザードやハザード状態につながりやすい。臨床行為をよく理解することで、リスクマネージャはハザード及びハザード状態を識別でき、ソフトウェアエンジニアはハザード及びハザード状態を回避したりリスクコントロール手段を策定することが可能になる。

製造業者は、設計活動及びリスクマネジメント活動の両方に臨床専門家（臨床支援及び技術サービスの専門家、その他関連分野の専門家）が参加できる、あるいは少なくとも助言を与えられるようにすることが望ましい。

製造業者はさらに、ソフトウェアエンジニア及びリスクマネージャに対し、医療機器の臨床使用について教育することを検討するべきである。

3.3.3 プログラミング経験及び姿勢

熟練したソフトウェア設計者及び試験者は、経験から試験時にすべてのソフトウェア欠陥を見つけ出すことの困難さ、及び試験後に残るソフトウェア欠陥の量について現実的になっている。ソフトウェア開発チームに経験豊富なスタッフを含めて、経験の少ないスタッフを指導、監督し、士気を鼓舞するための適切な権限を与えることが重要である。

以下の作業については、経験豊富なスタッフを割り当てることが特に重要である。

- ソフトウェアが故障する状況の特定
- ソフトウェア故障に関連するリスクの分析
- リスクコントロール手段の特定
- リリース後の問題報告書の分析
- 変更、特にリリース後の変更の策定と実施

上記の各作業では、経験豊富なスタッフであればソフトウェア及びソフトウェア開発プロセスにどのような問題が生じるかを識別でき、ソフトウェア設計の整合性を保ちつつ設計を変更することの困難さも承知している。

3.4 リスクマネジメント計画

3.4.1 一般

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) 責任及び権限の割り当て。
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。

注記 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み合わ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。

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。

リスクマネジメント計画は、以下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事実に対処するのが望ましい。

- 医療機器の説明（その医療機器のどの機能がソフトウェアに組み込まれるか、を含む）

– ソフトウェアはIEC 62304に従って開発されるというステートメント
– ソフトウェアのリスクマネジメントに特有のソフトウェア開発部分の記載（注記参照）
– ソフトウェアに起因するリスク又はソフトウェアでコントロールされるリスクについて、リスク許容基準がその医療機器の他のコンポーネントのリスク許容基準とは異なる場合、そのリスク許容基準

注記：ソフトウェアのリスクマネジメントに特有のソフトウェア開発の部分を含めるには、ソフトウェア開発計画に言及することが最も簡単な方法である。3.4.2及び3.4.3でリスクマネジメント計画とソフトウェア開発計画との関係、及びIEC 62304に準じたソフトウェア開発計画の特定のリスク関連トピックについて述べているので、そちらを参照のこと。

ソフトウェアに起因するリスク又はソフトウェアでコントロールされるリスクのリスク許容基準が医療機器の他のコンポーネントのリスク許容基準と異なる理由のひとつは、危害の確率を予測できないことである。この場合、リスク許容基準を危害の重大性に置くべきである（ソフトウェアに起因する危害の確率については4.4.3を参照のこと）。危害の実際の影響が些細なものであると結論付けられれば、そのリスクは許容可能と判断してよいため、リスクコントロール手段は不要になる。しかし、著しいハザード、すなわち重大性の高い危害を招きかねないハザードについては、曝露の程度が非常に小さなリスクにしか対応しないとしても、そのリスクは許容できない。この場合、リスクコントロール手段を実装する必要がある。

確率が推定できない残留リスクのリスク許容基準については、既に実装されているリスクコントロール手段、及びそのリスクコントロール手段の危害発生確率低減に対する有効性を考慮に入れるべきである。リスクコントロール手段は、妥当かつ実行可能なすべての手段の組み合わせであり、該当する規格及び法規制を満たし、かつ最新のものであることが望ましい（ISO 14971:2007の附属書D.4を参照のこと）。

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、以下のソフトウェアの具体的側面を考慮するのが望ましい。

– 出所が不明なソフトウェア（SOUP）を使用する場合、公に入手可能な異常リスト、及びそのSOUPの現地性能に関する情報の監視及び評価を計画するべきである。可能であれば、SOUP取得時にそのSOUPの供給業者との契約合意により、これを裏付けることが望ましい。医療機器の使用者が（意図的であれどうあれ）自分で医療機器のSOUPを変更（パッチ又は更新など）することが考えられる場合は、SOUPの新しいバージョンが市場に提供されているかどうかも監視する必要がある。SOUP及び生産後監視については、箇条9を参照のこと。
– 製造業者は、苦情を申し立てる者がソフトウェアのバージョンを識別し、報告できるようにするべきである。

3.4.2 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

ISO 14971のリスクマネジメント計画に関する要求事項及びIEC 62304のソフトウェア開発計画に関する要求事項では、特定の題名の特定の文書を必要としているわけではない。計画の要素は、製造業者の品質マネジメントシステムにふさわしいものであれば、どのような文書にまとめてもかまわない。ただし、以下の条件を満たす必要がある。

– 計画書を組み合わせることにより、両方の規格の要求事項を検証可能な方法で満足すること。
– すべての計画が互いに矛盾しないこと。
– すべての計画が時宜にかなった方法で使用可能であること。
– すべての計画が状況の変化を反映して最新の状態に保たれること。

3.4.3 IEC 62304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

ソフトウェア開発計画では、ソフトウェア開発プロセス、及びソフトウェアの開発に関連する基準、手法、ツール（「IEC 62304:2006の箇条5に従ったソフトウェア開発計画」に記載）が有効なリスクコントロール手段（プロセス及びリスクコントロール手段については6.2.2.6を参照のこと）になるようにすることが望ましい。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基づくものでもよい。有効性が不明な場合、プロジェクト内で有効性の検証を計画し、実施すること。

医療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。そうした側面がリスクコントロール手段と見なされた場合は、検証の対象にもなる（リスクコントロール手段の検証の例を表B.2に示す）。

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

3.5 リスクマネジメントファイル

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

注記 1： リスクマネジメントファイルを構成する記録及びその他の文書は、例えば製造業者の品質マネジメントシステムによって要求される他の文書やファイルの一部とすることができる。リスクマネジメントファイルは、すべての記録及びその他の文書を物理的に含んでいる必要はないが、少なくともすべての要求書類に対する参照表記あるいは指示要記を含んでいることが望ましい。製造業者は、リスクマネジメントファイルで参照表記する情報をタイムリーにまとめることができるのが望ましい。

注記 2： リスクマネジメントファイルの書式や媒体の種類は問わない。

ソフトウェアプロセスでは、このトレーサビリティを可能にし、ソフトウェア関連ハザード及びソフトウェアリスクコントロール手段が対応する安全関連ソフトウェア要求事項及びその要求事項を満たすソフトウェアアイテムに実現されるまでを追跡できるシステムを設けるべきである。

上記すべてはその検証の段階まで追跡可能であることが望ましい（IEC 62304:2006の細分箇条7.3.3参照）。

ソフトウェアは開発中にしばしば変更されることがあり、また異なる複数のバージョンでリリースされることもあるため、ソフトウェアに関するリスクマネジメントファイルのその部分も変更又は複数バージョンでのリリースの対象となることがある。

表1に、ISO 14971:2007の要求事項に追加して、リスクマネジメントファイルに含めるべき文書のIEC 62304:2006 要求事項を掲げる。

表1 - ISO 14971:2007の要求事項に追加してリスクマネジメントファイルに含めるべき文書の要求事項

IEC 62304:2006 細分箇条	リスクマネジメントファイルに含める文書内容
4.3c)	各ソフトウェアシステムに割り当てたソフトウェア安全クラス
4.3f)	安全関連機能を実装しないソフトウェアシステムのソフトウェアアイテムに（ソフトウェアシステムよりも）下位のソフトウェア安全クラスを使用する根拠
7.1.4	ハザード状態の一因となるソフトウェアアイテムの潜在的原因
7.1.5	IEC 62304:2006の細分箇条7.1.2に明示されているハザード状態を招くおそれのあるイベントシーケンス
7.2.1	ハザード状態の一要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定めたリスクコントロール手段
7.3.2	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する場合、製造業者はそのリスクコントロール手段を評価して、ハザード状態を招くおそれのある新しいイベントシーケンスを明らかにし文書化すること。
9.5	製造業者は問題報告及びその解決策（検証を含む）の記録を保守すること。製造業者はリスクマネジメントファイルを適宜更新すること。

4 リスク分析

4.1 リスク分析プロセス

ISO 14971:2007から抜粋

4 リスク分析

4.1 リスク分析プロセス
リスク分析は、4.2から4.4までに記載する特定の医療機器について実行すること。計画したリスク分析活動の実施及びリスク分析の結果は、リスクマネジメントファイルに記録すること。

注記 1：リスク分析又はその他関連情報が類似の医療機器について利用可能な場合、その分析又は情報を新しい分析の出発点として使用できる。関連性の度合いは機器間の差によって、及びその差が新しいハザードを招くのかあるいはアウトプット、特性、性能、若しくは結果に対して重大な差をもたらすのかによって、異なる。また既存の分析結果をどの程度使用するかは、ハザード状態の進展に当該変更が及ぼす影響の体系的評価に基づく。
注記 2：リスク分析手法のいくつかを、付属書Gに記載する。
注記 3：生体外診断医療機器のリスク分析手法に関する新たな指針を、付属書Hに示す。
注記 4：毒物学的ハザードのリスク分析手法に関する新たな指針を、付属書Iに示す。4.2から4.4の中で要求している記録に加え、リスク分析の実施及び結果の文書記録には、少なくとも以下を含めること：

a) 分析した医療機器についての説明及び識別情報
b) リスク分析を実行した者及び団体についての識別情報
c) リスク分析の範囲及び実施日

注記 5：リスク分析の範囲は、（製造業者がほとんど又は全く経験がない新しい機器の開発については）非常に広範にわたる可能性もあれば、（製造業者のファイルに多くの情報が既に存在する既存の機器への変更の分析については）非常に限定される可能性もある。

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。

ISO 14971:2007に記載されているように、リスク分析は3つの別個の活動を包括して使用される用語である。

- 意図する使用の特定、
- 既知の又は予見可能なハザード（及びその原因）の特定、及び
- 各ハザード及びハザード状態のリスクの推定

リスク分析が有効であるためには、1つ又は2つの離散事象としてではなく、ソフトウェア開発プロセス全体の不可欠な一部として実行しなければならないということを認識しておくことが非常に大切である。というのも、ハザード及び故障モードに関する情報は、ソフトウェア開発ライフサイクルプロセス全体にわたって発生し、設計の各段階で考慮する必要があるためである。

ハザード状態を招くおそれのあるソフトウェア異常の確率を推定することが非常に困難なことから、リスク分析のソフトウェア面については確率の推定でなくハザード状態を招くおそれのある潜在的なソフトウェアの機能性及び異常の特定に主眼が置かれる。確率の推定の詳細については、4.4.3を参照のこと。

ソフトウェアに起因する最悪の場合の危害の重大性は、ソフトウェア開発プロセスの厳格さのレベルを決める上で主要な情報である（IEC 62304:2006の細分箇条4.3参照）。
細分箇条4.2、4.3、及び4.4では、有効なリスクマネジメントプロセスのソフトウェアに特有な側面の特定に役立つように意図した情報を提供している。さらに、結果として作成される文書内でリスク分析のソフトウェア面が識別できること、ハードウェア故障に対するリスクコントロール手段の実装に使用したソフトウェア及びハザードのソフトウェア原因とそれに関わるリスクコントロール手段の両方を含んでいることが望ましい。

4.2 意図する使用及び医療機器の安全に関する特質の明確化

4.2.1 一般

ISO 14971:2007から抜粋
4.2 意図する使用及び医療機器の安全に関する特質の明確化

検討中の特定の医療機器について、製造業者は意図する使用及び合理的に予見可能な誤使用を文書化すること。製造業者は医療機器の安全性に影響を及ぼすおそれのある定性的及び定量的特質並びに、該当する場合は、その規定限界を明確にして文書化すること。この文書は、リスクマネジメントファイルで保守すること。

注記 1：この文脈で誤使用とは、医療機器の誤った又は不適切な使用を意味する。

注記 2：付属書Cには、安全性に影響を与えるおそれのある医療機器の特質を明確にする際に指針として利用できる、使用上の疑問などをまとめたものが含まれている。

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。

各医療機器は意図する使用を持つが、誤使用（意図的か否かを問わず）の可能性も考慮しておくことが望ましい。これはソフトウェア特有の懸念事項ではないが、以下の理由によりソフトウェアの使用が誤使用のリスク増大につながる可能性がある。

- 医療機器の挙動が（他に比べて）複雑なため、習得や理解がそれだけ難しい。
- 使用者が、その限度を理解することなく、ソフトウェアに過度に依存するようになる可能性がある。

– 医療機器は設定変更可能な場合があり、使用者が現在の設定を理解していない場合がある。
– 医療機器製造業者が詳細について予想できないような方法で、医療機器が他の医療機器及び非医療機器と通信する場合がある。

システム要求事項作成の責任者及びソフトウェアエンジニアは、ソフトウェアを含むシステムの意図する使用を、安全性及び安全使用に関連するすべてのシステム／ソフトウェア要求事項と共にリスクマネジメントファイルに記録することについて、共同責任を負う。ソフトウェアエンジニアは、システムレベルでは識別できないほど微妙な意図する使用の特徴を明らかにすることについて、特に責任を負う。

4.2.2 ユーザーインターフェース

ソフトウェアは、より柔軟なユーザーインターフェースの設計を可能にするが、それが使用者の挙動に影響を及ぼし、ひいては新しい形態の合理的に予見可能な誤使用につながる場合がある。
共通の誤使用は、過度に複雑なユーザーインターフェースに対する誤解や、エラーや不安全状態の回避についてのソフトウェアへの過度の依存から発生する。このような誤使用を予期しそれをできる限り回避するために、設計変更を行うことが重要である。

これには多国語ラベルの使用も含まれ、ラベリングがリスクコントロール手段のひとつである場合は特に必要となる。以下については特に注意すべきである。

a) 異なる複数の言語のそれぞれで異なる必要なメモリサイズ
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) 日付フォーマット及び数字の桁区切り
f) 異なる複数の言語及び／又は文字セットに必要な異なる複数のレイアウト要求事項
g) 妥当性確認への対応

ISO 14971を補完するユーザビリティプロセスについては、IEC 62366 [5]を参照のこと。

4.2.3 医療機器の相互接続

医療機器にソフトウェアを使用することにより、医療機器と非医療機器の間での広範な相互接続及び相互通信が可能になる。このような接続及び通信は、医療機器や相互接続された機器で構成されるシステムの新しい使用（及び誤使用）を生み出す可能性が高い。これらの新しい使用や誤使用が起こりうることは容易に予見できるが、相互接続及び相互通信に制限がない場合、医療機器製造業者がこれらの使用や誤使用をすべて特定することは容易ではない。

したがって製造業者は、医療機器の通信インターフェースについて意図する使用の範囲を限定して、相互接続及び相互通信を安全なものに制限できるようにインターフェースを設計することが重要である。

例えば、医用機器内蔵のインターフェースを使用して入力された治療データについて、使用者や患者の身元及びデータ作成の背景に基づき、その整合性及び合理性をソフトウェアがチェックする場合がある。しかし、データが別の場所で作成されネットワーク接続を使用して医療機器にインポートされた場合は、これと同じチェックが適用できない可能性がある。その場合、製造業者はネットワーク使用者がソフトウェアチェックをネットワークアプリケーションとして使用できるようにすること、及び／又はデータインポートを信頼できるソースに限定すること、及び臨床環境におけるネットワーク接続の責任者のために包括的なマニュアルを作成することを検討してもよい。

臨床環境における医療機器のITネットワークへの統合については、IEC 80001-1 [6] で規定している。特に、製造業者及び医療機器のITネットワークへの統合の実施者の責任を定めている。

4.3 ハザードの特定

ISO 14971:2007 から抜粋

4.3 ハザードの特定

製造業者は、正常状況及び不具合状況の両方における医療機器に関連する既知及び予見可能なハザードについて文書をまとめること。この文書は、リスクマネジメントファイルで保守すること。

注記： E.2 及び H.2.4 に示す起こりうるハザードの例は、製造業者がハザードの特定を開始する上での指針として使用できる。

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。

ハザード特定の目的は、すべての予見可能なハザードの分析、並びに有効なリスクコントロール手段の設計及び実施を可能にすることにある。

熱や電気エネルギー、懸垂部分とは違い、ソフトウェア自体はハザード源（危害の潜在的発生源）ではない。例えばソフトウェアとの接触によって負傷するおそれはない。しかし、ソフトウェアによって人がハザードにさらされる可能性はある。言い換えれば、ソフトウェアがハザード状態の原因になる可能性がある。ソフトウェア故障（その種類を問わず）は、多くの場合、ハザードからハザード状態への変化を助長する。

このように、ソフトウェアは新しいハザードを招くことはめったにないものの、ハザード状態を変化させることはよくある。製造業者にとってさらに重要なのは、ハザード状態回避の責任が使用者から製造業者に移行する可能性があることである。

例えば、外科用メスは明らかに切傷ハザードを有している。しかし、製造業者は従来から人間工学設計を超えた範囲でこのハザードの責任を負うことはしなかった。なぜならば、このハザードは完全に外科医の管理下にあると想定されるためである。一方、外科用メスが遠隔手術システムの一部である場合にも同じハザードは存在するが、この場合、切傷ハザードを回避する責任は今やメスを制御するソフトウェアをシステムに組み込んだ製造業者も共有するものとされている。
これは、一部のハザードについて、ソフトウェアがないときはそのリスクコントロールは医療機器の専門的使用のみに依存していたが、現在では製造業者によるソフトウェア リスクマネジメントに移行している、ということを意味している。

重要な例としては、誤ったデータの取扱いによる治療ミスというハザードがある。これは以前からハザードであったが、データが臨床医のデスクで処理された場合は、製造業者の責任外とされてきた。しかし現在では、多くの医療機器がデータの生成、格納、操作、又は使用にソフトウェアを使用している。その結果、ハザードの責任の一部が製造業者に発生するようになっている。

ソフトウェアは以下を含む様々な形で、ハザード状態の原因になりうる（附属書Bも参照）。

– ソフトウェアがある不安全なシステム要求事項を正しく実装しており、その挙動の危険な性質が実際の危害が発生するまで認識されない可能性がある。
– ソフトウェア仕様があるシステム要求事項を正確に実装していないため、ソフトウェア仕様上は正しいが、望ましくない挙動につながる可能性がある。
– ソフトウェアの設計及び実装に不具合があり、ソフトウェア仕様に反する挙動につながる可能性がある。ソフトウェア仕様の誤解や仕様をコード化する際のエラーに起因する不具合はすぐに分かるが、ソフトウェアアイテム同士の間、及び（ハードウェアやオペレーティングシステムを含む）インフラとソフトウェアとの間の予見不能な相互作用から生じる不具合は、分かりにくい可能性がある。

ソフトウェアを組み込んだ医療機器では、注意深く包括的にハザードを特定することにより、（リスクマネジ

メントプロセスの後の段階において）特に以下の重要な成果を得られる可能性がある。

- ソフトウェアによる危害の発生を防止するハードウェアリスクコントロール手段
- 危害を及ぼす可能性のあるソフトウェア機能の仕様からの除去
- 危害の防止にソフトウェアを使用するリスクコントロール手段（IEC 62304:2006の細分箇条5.2.3参照）
- 低い欠陥密度で実装しなければならないソフトウェアの部分、及び特別試験の対象としなければならないソフトウェア仕様の部分の特定（IEC 62304:2006の細分箇条4.3）
- 予期せぬ悪影響から生じる危害を防止するために（より低いソフトウェア安全クラスの）ソフトウェアアイテムから分離しなければならないより高い安全クラスのソフトウェアアイテムの特定（IEC 62304:2006 の細分箇条4.3及び5.3.5参照）。この点に関する詳細な検討については、第6.2.2.5項を参照すること。

ハザードを十分に明らかにするには、医療機器の臨床用途をよく理解しなければならない。また、ソフトウェアには複雑なユーザーインターフェースの可能性などの複雑性という特別な難しさがある。したがって、ソフトウェアハザードの特定だけを単独で行うことはできない。ソフトウェアハザードの特定は、臨床専門家（臨床支援及び技術サービスの専門家）、ソフトウェアエンジニア、システム設計者、及びユーザビリティ／人間工学の専門家などからなる分野横断的なチームによって、システムレベルで実施することが望ましい。

ハザードの特定では、医療機器の性質から起こりうる危害（例えば患者の切り傷、被ばく、あるいは感電）、さらにはソフトウェアの使用に関連して発生する新たなハザードを考慮するのが望ましい。後者の例として、以下が挙げられる。

- 臨床家又は患者に対する誤った情報の提供
- 患者の取り違い（医療機器に患者の詳細又は処方の情報が保存されている場合）
- ソフトウェアの異常による治療の遅れ又は拒否

注記：多くの医療機器の場合、治療の遅れや拒否は患者に危害を及ぼすとはみなされない。

特定されるハザードには、仕様に従って動作しているソフトウェアに関連するハザードと、ソフトウェア異常に関するハザードの両方が含まれることが望ましい（第6.1項も参照）。

多くの場合、医療機器のユーザーインターフェースはソフトウェアによってさらに複雑になっている。特に、ソフトウェアを組み込んだ医療機器は情報を扱うことが多い。これは患者利益の点から正当化されるだろうが、例えば次のような、誤った情報又は誤って使用された情報に関する新たなハザードを考慮することが望ましい。

- 誤ったデータ入力
- 使用者による表示の誤読
- 使用者による警報の誤解又は無視
- 過剰なデータ又は過剰な警報数による使用者への過負荷（IEC 62366[5]参照）

4.4 各ハザード状態に関するリスクの推定

4.4.1 一般

ISO 14971:2007から抜粋

4.4 各ハザード状態に関するリスクの推定

ハザード状態を招くおそれのある合理的に予見可能なイベントシーケンス又はイベントの組み合わせについて検討し、結果として生じたハザード状態を記録すること。

注記 1：過去に認識されていないハザード状態を明らかにするには、特定の状況を網羅する体系的手法を使用できる（附属書 G 参照）。

注記 2：ハザード状態の例は、H.2.4.5 及び E.4 で示している。

注記 3：ハザード状態はスリップ（動作のミス）、ラプス（記憶のミス）、及びミステイク（確認のミス）から生じうる。

特定した各ハザード状態について、利用可能な情報又はデータを使用してその関連リスクを推定する。危害の発生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、考えられる結果を列挙する。これらの活動の結果は、リスクマネジメントファイルに記録する。

危害の発生確率又は危害の重大性を定性的又は定量的に分類するために使用するシステムすべてを、リスクマネジメントファイルに記録する。

注記 4：リスクの推定には、発生確率及び結果の分析が盛り込まれている。用途によっては、リスク推定プロセスの一定要素だけが検討対象となるかもしれない。例えば、初期ハザードと結果の分析だけで十分な場合もある。D.3 も参照。

注記 5：リスクの推定は、定量的又は定性的に行うことができる。システム上の欠陥から生じるリスクの推定も含めたリスク推定手法は、附属書 D で示している。附属書 H では、生体外診断医療機器に関するリスクの推定に役立つ情報を提供している。

注記 6：リスクの推定に用いる情報又はデータは、例えば次から取得できる：

a) 公表規格
b) 科学技術データ
c) 公に報告されている事故を含む、既に使用中の類似医療機器の実地データ
d) 典型的な使用者を使ったユーザビリティ試験
e) 臨床上の証拠（エビデンス）
f) 適切な調査の結果
g) 専門家の意見
h) 外部品質評価スキーム

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。

ソフトウェア関連のリスクを推定するためには、まずソフトウェアを含むハザード状態を特定することが必要である。ソフトウェアは、ハザード状態の原因となるイベントシーケンスの根本的原因になる場合もあれば、ハードウェア故障の検出を意図したソフトウェアのように、シーケンスの他の原因になる場合もある。ソフトウェアには、SOUPコンポーネントや過去に開発したコンポーネントの再利用品が含まれる可能性もある。

リスク推定は、特定した各ハザード状態から生じる危害の確率及び危害の重大性に基づいて行われる。ソフトウェア異常から生ずる危害の確率を推定するのは非常に困難なため（箇条4.3.3参照）、危害に至るイベントシーケンスにおけるソフトウェア異常などのハザード状態のリスクを推定する際にソフトウェア異常の発生確率を使用するときには、注意が必要である。

4.4.2 特定方法

ハザード状態におけるソフトウェアの潜在的役割の特定には、様々な手法が使用できる。これらの手法はアプローチが異なり、ソフトウェア開発の様々な段階で役立つ可能性がある。唯一の正しい手法というものは存在しない。ISO 14971:2007の附属書Gにリスク分析のいくつかの手法についての情報が記載されている。

フォルトツリー解析（FTA）は、全体としての医療機器から始める、伝統的なトップダウン手法である（IEC 61025 [3] 参照）。この手法は、主として危害の原因分析に使用される。FTAは危害が発生することを前提とし、その危害について存在するはずのイベント又は条件を、ブール論理を使用して特定する。そのイベント又は条件を段階的にさらに詳細に解析していき、危害を予防すると期待されるリスクコントロール手段がひとつ以上特定できるまで解析を続ける。FTAは、ハザード状態を引き起こすイベントシーケンスに関与するソフトウェアアイテムの特定に使用できる。

故障モード影響解析（FMEA）は、コンポーネントやサブシステム（ソフトウェアの場合は、IEC 62304 におけるソフトウェアアイテム）から始め、「この要素が故障したとするとどのような結果になるか？」という問い掛けを行う、ボトムアップアプローチである（IEC 60812 [2] 参照）。

各ソフトウェアアイテムにどのソフトウェア欠陥があるかを予想するのは困難なことから、FMEAではまず各ソフトウェアの安全に関わる要求事項をリストアップし、この要求事項が満たされない場合にどのような結果になるかを考えることから始める。

そうすることにより、どのソフトウェアアイテムの故障が危害に結びつくかを特定でき、どのような種類の故障を防ぐ必要があるかも特定できる。

ハザード状態を引き起こす可能性のあるイベントのシーケンス又は組み合わせを特定するとき、医療機器の主要性能に直接関わるソフトウェア（血糖値を計算するアルゴリズムなど）及び関連するハザードに固有の原因に焦点を絞るのが最も容易である。また、軽微な故障モードを招くおそれがありしたがってひとつ以上の医療機器ハザードを発生させる可能性のあるソフトウェアの原因を考慮することも重要である。ソフトウェア原因の例については、附属書Bを参照すること。

注記：固有の原因とは、その機能性が機器の臨床機能に明らかに関わっており、機器ハザードの原因のひとつになっているソフトウェアの欠陥である。例として、試験結果を算出するアルゴリズムの欠陥が挙げられる。

ソフトウェアアイテム内で何が故障するかを厳密に予測することは困難であるが、欠陥のカテゴリを特定することは可能であり、そのカテゴリのそれぞれには周知のリスクコントロール手段がある。例えば、データ破損は、チェックサム手順を使用することで検出及び予防可能な故障に分類される。ソフトウェア原因の例とその取扱い方法については、附属書Bを参照のこと。製造業者は、自社製品に関するソフトウェア欠陥のカテゴリの独自のリストを維持管理することが望ましい。

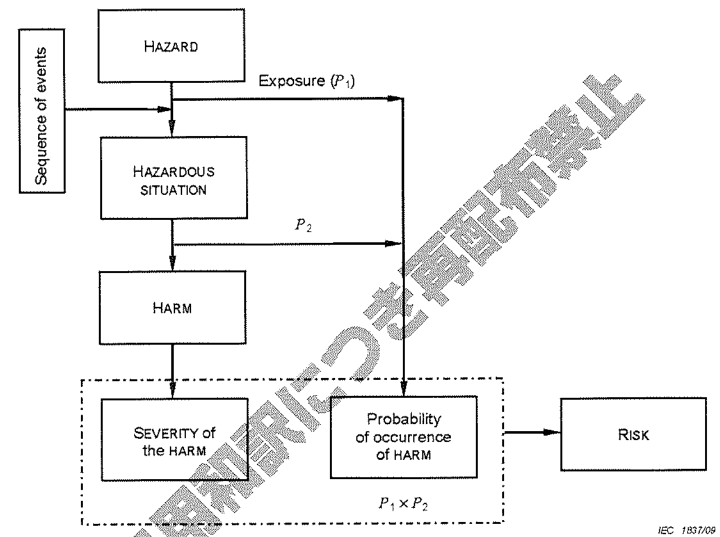
4.4.3 確率

ソフトウェアのある特定のバージョンにおけるソフトウェア異常は、そのソフトウェアのすべてのコピーにも存在する。しかし、個々のコピーへの入力がランダムであるため、そのソフトウェア異常がソフトウェア故障につながる確率を推定するのは非常に困難である。

ソフトウェア故障発生確率の推定手法について、見解の一致は存在しない。ハザード状態の原因となるイベントシーケンス内にソフトウェアが存在する場合、ハザード状態のリスクを推定するときにソフトウェア故障発

生確率を考慮に入れることはできない。このような場合、最悪のケースの確率を考えるのが適切であり、ソフトウェア故障発生確率は 1 とすることが望ましい。シーケンス内の残りのイベントの確率が推定可能な場合（そのイベントがソフトウェアでない場合）は、その確率をハザード状態の発生確率（図1のP_1）として使用してもよい。それができない場合は、ハザード状態の発生確率を 1 に設定すべきである。

ハザード状態が危害に至る確率（図1のP_2）を推定するには、通常、臨床で危害の発生を防げる見込みのあるハザード状態と、危害が発生する可能性が高いハザード状態とを識別するための臨床知識が必要とされる。



NOTE P_1 is the probability of a HAZARDOUS SITUATION occurring.
P_2 is the probability of a HAZARDOUS SITUATION leading to a HARM.

図1 – ハザード、イベントシーケンス、ハザード状態、及び危害の関係図 – ISO 14971:2007 附属書Eより

多くの場合、危害の発生確率を推定することは不可能かもしれず、リスクを危害の重大性だけに基づいて評価することが望ましい。そのような場合のリスクの推定は、ハザード状態から生じる危害の重大性に焦点を合わせるのがよい。
ソフトウェア故障の発生確率を推定することは不可能であるが、多くのリスクコントロール手段が、ソフトウェア故障がハザード状態に至る可能性を低減しているのは明らかである。ソフトウェア異常によるメモリの破損を例にとってみると、メモリのチェックサムを実施することにより、故障を検出してハザード状態の確率を低減できる可能性がある。ただし、チェックサムですべての損傷を検出できる保証はない。正確に言うと、そのような破損の大多数を検出することで、そのリスクを許容できる水準まで軽減するものである。チェックサムを実施する前又は後にハザード状態の確率を推定することはできないが、チェックサム実施後のハザード状態の確率が実施前よりも低くなることは断言できる。リスクコントロール手段がリスクマネジメント計画で特定された残留リスクの許容基準を満たすのに有効であると実証する責任は製造業者にある。

つまり、ソフトウェアのリスク推定では、起こりうるソフトウェア故障の確率を推定しようと試みるので