JAHIS技術文書　10-101

Japanese

Association of

Healthcare

Information

Systems Industry

ＪＡＨＩＳ
医療情報システムの
患者安全に関する
リスクマネジメント
ガイドライン
＜解説編＞

2010年 9月

保健医療福祉情報システム工業会
安全性・品質企画委員会

ＪＡＨＩＳ医療情報システムの患者安全に関する リスクマネジメントガイドライン＜解説編＞

ま　え　が　き

1999年末の米国IOMのレポート「To Err is Human」発表以来、医療過誤への関心が高まり、医療過誤とITシステムの関連等の議論も活発になった。また、国内においても2000年にオーダシステムにおける処方オーダミスによるアクシデントが起こり、これに対応してJAHISにおいても処方オーダミス対策プロジェクトを立ち上げ、業界共通のガイドを纏めてきた。しかし、運用上の要因が主因と考えられるが、同一薬品でのアクシデントが2008年11月に再度起こり、厚生労働省医政局医療安全推進室の指導のもと、病院薬剤師会・日本医師会他と連携してJAHIS会員への周知およびユーザからの問合せに対する対応のお願いを行った。

一方、医療機器および医療機器ソフトウェアの範疇に含まれないものを対象とした患者安全マネジメントの最初の国際標準規格案が、英国NHSから2006年3月のISO/TC215の会議において提案され、その後3年間に渡って、ISO/TC215の場で規格化の是非について議論が繰り返されてきた。最終的には医療機器および医療機器ソフトウェアに関する国際標準規格を策定しているIEC/SC62Aとの合同での策定へと移行し、現在IEC/TR80001-2として策定中である。

この議論の過程において、医療現場での使用に際してリスクのあるものは、医療機器および医療機器ソフトウェアとして扱うべきであるという考え方が主流になり、CENおよびCENELECの合同WGで、医療情報システムも含めて規制対象の検討が行われている。

また、欧州では、2010年3月からの改正MDDによる医療機器ソフトウェア単独での規制実施を行うことになっており、一方、米国FDAでは医療機器の定義に基づいて電子カルテ等の医療情報システムは医療機器ソフトウェアの定義に合致すると見なしているが、現状は裁量によって規制の対象から除外している状況である。

このような海外状況およびGHTFの勧告に基づいて、日本においても医療機器ソフトウェア規制の議論が活発化しており、従来から医療機器および医療機器ソフトウェアを製造しているメーカの工業会においても厚生労働省への働きかけを行っている。

このような状況を鑑み、日本では現在のところ医療情報システムは薬事法等の規制の対象外であるが、欧州・米国での規制動向が近い将来日本へ波及することに備えるという観点、および安全・安心なシステムの提供・運用を目指すという観点で、医療情報システムの患者安全に関するガイドラインを纏め、本ガイドラインをもとに、JAHISとして患者安全リスクマネジメントの自主規制を行い、安全性を確保する仕組みを実行した上で、将来に対処すべきであると考える。

以上の観点から、今回は、医療機器および医療機器ソフトウェアの規制に関する国際標準規格（一部はすでにJIS規格化済）の概要を解説し、患者安全確保のための一般的な管理手法の概要を理解して頂く目的で本解説編を策定し、また、医療情報システムのハイリスク業務と考えられる注射オーダ業務等を取上げ、具体的な業務に対応した患者安全ガイドラインを技術文書として並行して策定する。

本解説編の読者としては、医療機器等に関する国際標準規格や薬事法等の規制に必ずしも精通していない医療情報システムの開発等に従事している人を想定しており、国際標準規格の代表的なものについて、その概要を理解して頂く目的で作成したものである。

2010年　9月

保健医療福祉情報システム工業会
安全性・品質企画委員会

＜＜　告知事項　＞＞

本ガイドラインは関連団体の所属の有無に関わらず、ガイドラインの引用を明示することで自由に使用することができるものとします。ただし一部の改変を伴う場合は個々の責任において行い本ガイドラインに準拠する旨を表現することは厳禁するものとします。

本ガイドラインならびに本ガイドラインに基づいたシステムの導入・運用についてあらゆる障害や損害について、本ガイドライン作成者は何らの責任を負わないものとします。ただし、関連団体所属の正規の資格者は本ガイドラインについての疑義を作成者に申し入れることができ、作成者はこれに誠意をもって協議するものとします。

目　　次

1. 適用範囲

従来、リスクマネジメント(特に患者安全)の観点では、製造者側での規制が主体であったが、現在はユーザ側での運用面も含めて議論されてきており、ここ数年においては、この両面に対して国際標準規格の策定が進められてきている。また欧米では、医療機器のみでなく医療機器ソフトウェア単独での規制対象品目の拡大、さらには医療現場で使用される他のソフトウェア、すなわち医療情報システムを規制対象として、どう扱うかの議論も始められている。

一方、日本においては、医療機器（ソフトウエアを内蔵したものも含む）を薬事法の対象としており、医療情報システムはその規制の対象外である。

このような状況において、本ガイドラインにおいては、医療機器および医療機器ソフトウェア単独での患者安全に関する国際標準規格および規格案の概要に触れ、医療情報システムにおける患者安全を実現するための一般的な管理手法の概要を周知する解説編として活用することを目的として策定している。

IEC62304の付属書B.4に、医療機器ソフトウェアの安全性を向上させる三つの大原則として、

- 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

が挙げられているが、本技術文書では、この三つの大原則のうち、リスクマネジメントにフォーカスして解説する。品質マネジメントおよびソフトウェアエンジニアリングについては、該当する標準規格(JIS Q 13485等)を参照して頂きたい。

このような観点で、リスクマネジメント(特に患者安全)に関する国際標準規格および規格案の概要をいくつかの側面から説明する。ここでは、

① リスクマネジメントの共通規格としてJIS T 14971
② ソフトウェアのライフサイクルに関する規格としてJIS T 62304(原案)
③ これらを実際に適用するときのガイドとしてIEC/TR80002-1
④ ユーザに提供する患者安全情報の規格およびガイドとしてJIS T 62304、IEC/TR80002-1
⑤ ユーザビリティに関する規格としてIEC62366、IEC60601-1-6
⑥ 医療機器をネットワーク環境で使用するときのユーザと製造者の成すべきことの規格案としてIEC80001-1およびIEC80001-2-XX

他を取上げ、医療情報システムの開発時と運用時において考慮すべき管理手法の入門編として概説する。

これらの国際標準規格および規格案と、本技術文書および本技術文書と並行して策定する注射業務編等の関係を示したものが、図1－1である。

本技術文書の本論では、医療機器（ソフトウエアを内蔵したものも含む）の製造者が直接関与する国際標準規格の概要を解説し、付則には、主にこれらの国際標準規格を医療情報システムに適用した場合の例を示している。

付則AおよびBでは、JIS T 62304(原案)のクラス分類の考え方を各々電子カルテシステムと薬剤部門管理システムに適用した例を示している。さらに付則Aでは、電子カルテシステムのうち業務単位でリスクの高い業務を分類選択するプロセスを解説し、その結果として患者安全ガイドライン個別編として、まず注射業務を取り上げる必要性のあることを述べている。

本技術文書では、国際標準規格の番号については、JIS規格がある場合はJIS規格を優先して記述し、JIS規格がないものは国際規格を記載することとする。

また、図中のJIS Q 13485、 JIS T 14971、 JIS T 62304(原案)、IEC62366、IEC60601_1_6は、規制を目的とした国際標準規格であるが、IEC/TR80002-1、IEC80001-1、IEC80001-2-XX等は、規制を目的としたものではない。

将来、医療情報システムが医療機器ソフトウェアとして規制対象に指定されたときには、原典に従って対応する必要がある。

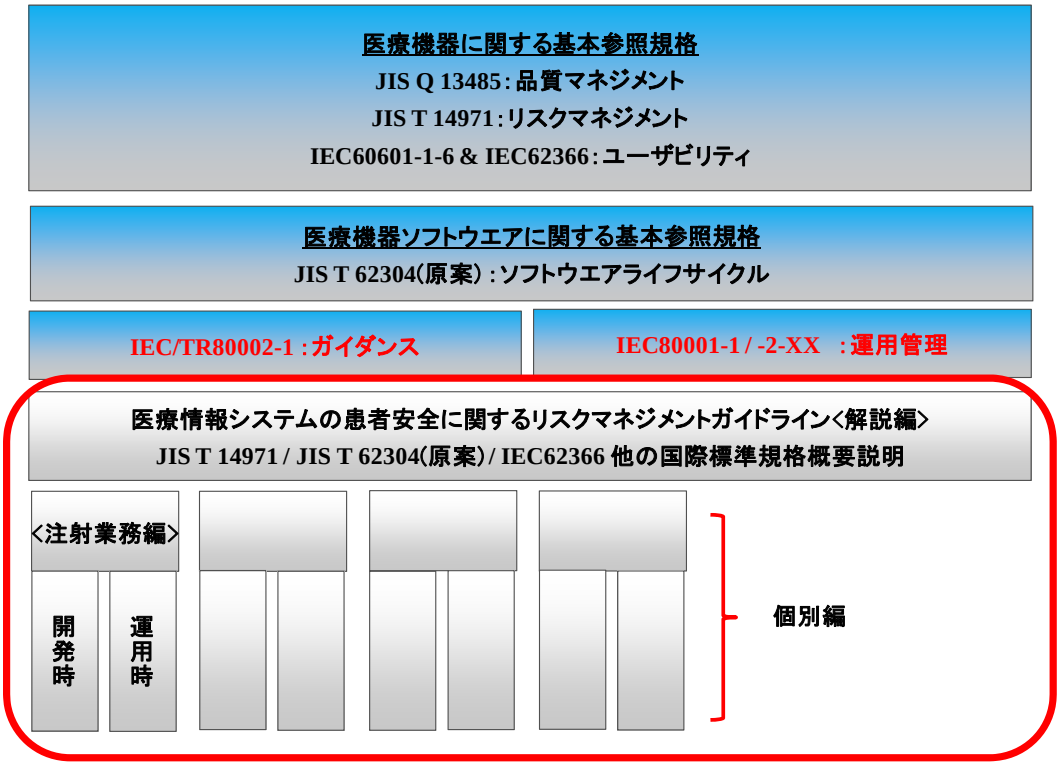


図１－１JAHIS患者安全ガイドラインとリスクマネジメント関連の国際標準規格の関係

2. 引用規格・引用文献

ISO 13485 Medical devices－Quality management systems－Requirements for regulatory purposes
JIS Q 13485:2005, 医療機器－品質マネジメントシステム－規制目的のための要求事項
対訳ISO13485　医療機器における品質マネジメントシステムの国際規格　日本規格協会
ISO 14971 Medical devices – Application of risk management to Medical devices
JIS T 14971　医療機器－リスクマネジメントの医療機器への適用
IEC 60601-1 Medical electrical equipment－Part 1: General requirements for basic safety and essential performance
IEC 62366 Medical devices – Application of usability engineering to medical devices
IEC 62304: 2006 Medical Device software – Software life cycle processes
IEC 80001-1 Application of risk management for IT-Networks incorporating medical devices
IEC TR 80002-1 Medical device software – Part 1: Guidance on the application of ISO 14971 to medical device software

3. 用語の定義

主な出典は、JIS T 14971、JIS T 62304(原案) であり、これら以外の定義は(＊)で示している。
凡例:[･･･]は出典、{･･･}は上記出典での引用または原典

3.1 **附属文書** (accompanying document): 医療機器又は附属品に附属し, かつ, 医療機器の使用者, 操作者, 設置業者又は組立業者にとって重要な, 特に安全に関する, 情報を記載した文書。
[JIS T 14971:2003 定義2.1]

3.2 **危害** (harm) : 人の受ける身体的傷害若しくは健康障害, 又は財産若しくは環境の受ける害。
[JIS T 14971:2003 定義2.2、JIS T 62304(原案) 用語及び定義3.8]{ISO/IEC Guide 51:1999 定義3.1}

3.3 **ハザード** (hazard): 危害の潜在的な源。
[JIS T 14971:2003 定義2.3、JIS T 62304(原案) 用語及び定義3.9]{ISO/IEC Guide 51:1999 定義3.5}

3.4 **危険状態** (hazardous situation) : 人, 財産又は環境が, 一つ又は複数のハザードにさらされる状況。
[JIS T 14971:2003 定義2.4]{ISO/IEC Guide 51:1999 定義3.6}

3.5 **意図する使用／意図する目的** (intended use / intended purpose): 製造業者が供給する仕様, 説明及び情報に従った製品, プロセス又はサービスの使用。
[JIS T 14971:2003 定義2.5]

3.6 **製造業者** (manufacturer): 医療機器の市場出荷及び／又は使用開始の前に, 医療機器の設計, 製造, こん(梱)包若しくはラベリング又はシステムの組合せ若しくは変更に責任を負う個人又は法人。その業務がその個人若しくは法人又は代理を受けた第三者によって行われるか否かを問わない。
[JIS T 14971:2003 定義2.6、JIS T 62304(原案) 用語及び定義3.10]

3. 7 **医療機器**(medical device):あらゆる計器, 器械, 用具, 機械, 器具, 埋め込み用具, 体外診断薬, 検定物質, ソフトウェア, 材料又はその他の同類のもの若しくは関連する物質であって, 単独使用か組合せ使用かを問わず, 製造業者が人体への使用を意図し, その使用目的が以下の一つ以上であり,

- 疾病の診断, 予防, 監視, 治療, 又は緩和
- 負傷の診断, 監視, 治療, 緩和, 又は補助
- 解剖学的又は生理学的なプロセスの検査, 代替, 又は修復
- 生命支援又は維持
- 受胎調整
- 医療機器の殺菌
- 人体から採取される標本の体外試験法による医療目的のための情報提供

薬学, 免疫学, 又は新陳代謝の手段によって体内又は体表において意図したその主機能を達成することはないが, それらの手段によって機能の実現を補助するものである。
注記1 この定義は, 医療機器規制国際整合化会議(GHTF)によって作成された。
[JIS T 62304(原案) 用語及び定義3.11]{JIS Q 13485:2005 定義3.7 参照、JIS T 14971 定義2.7 参照}

3.8 **客観的証拠** (objective evidence): 観察, 計測, 試験又は他の手段によって得られた事実に基づいて, 真実であると証明できる情報。
[JIS T 14971:2003 定義2.8]{ISO 8402:1994 定義2.19}

3.9 **手順** (procedure): ある活動を実施するため規定した方法。
[JIS T 14971:2003 定義2.9]{ISO 8402: 1994 定義1.3}

3.10 **プロセス** (process): 入力を出力に変換する, 相互に関連する資源及び活動のまとまり。
[JIS T 14971:2003 定義2.10]{ISO 8402: 1994 定義1.2}

3.11 **記録** (record): 実施した活動又は達成した結果についての客観的証拠を示す文書。[JIS T 14971:2003 定義2.11]{ISO 8402: 1994 定義3.15}

3.12 **残留リスク** (residual risk): 防護手段を講じた後にも残るリスク。
[JIS T 14971:2003 定義2.12]{ISO/IEC Guide 51:1999 定義3.9}

3.13 **リスク** (risk): 危害の発生確率とその危害の重大さとの組合せ。
[JIS T 14971:2003 定義2.13、JIS T 62304(原案) 用語及び定義3.16]{ISO/IEC Guide 51:1999

定義3.2}

3.14 リスク分析（**risk analysis**）：利用可能な情報を体系的に用いてハザードを特定し，リスクを推定すること。
［JIS T 14971:2003 定義2.14、JIS T 62304(原案) 用語及び定義3.17］{ISO/IEC Guide 51:1999 定義3.10}

3.15 リスクアセスメント（**risk assessment**）：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。
［JIS T 14971:2003 定義2.15］{ISO/IEC Guide 51:1999 定義3.12}

3.16 リスクコントロール（**risk control**）：規定したレベルまでリスクを低減するか又はそのレベルでリスクを維持するという決定に到達し，かつ，防護手段を実施する一貫したプロセス。
［JIS T 14971:2003 定義2.16、JIS T 62304(原案) 用語及び定義3.18］

3.17 リスク評価（**risk evaluation**）：社会の現在の価値観に基づく状況で，リスクが受容可能なレベルにあるかどうかをリスク分析に基づいて判断すること。
［JIS T 14971:2003 定義2.17］{備考 ISO/IEC Guide 51:1999 定義3.11 及び3.7 に基づく}

3.18 リスクマネジメント（**risk management**）：リスクの分析，評価及びコントロールに対して，管理方針，手順及び実施を体系的に適用すること。
［JIS T 14971:2003 定義2.18、JIS T 62304(原案) 用語及び定義3.19］

3.19 リスクマネジメントファイル（**risk management file**）：リスクマネジメントプロセスによって作成した記録及び他の文書のまとまりであり，必ずしも物理的に連続してなくてもよい。
［JIS T 14971:2003 定義2.19、JIS T 62304(原案) 用語及び定義3.20］

3.20 安全（**safety**）：受容できないリスクがないこと。
［JIS T 14971:2003 定義2.20、JIS T 62304(原案) 用語及び定義3.21］{ISO/IEC Guide 51:1999 定義3.1}

3.21 重大さ（**severity**）：ハザードから生じる可能性がある結果に対する尺度。
参考 危害に対する尺度をいう。
［JIS T 14971:2003 定義2.21］

3.22 検証（**verification**）：規定した要求事項を満たしたことを試験及び客観的証拠の提供によって確認すること。
備考 設計と開発において，検証は，その活動について述べた要求事項に適合しているかを判定するために与えられた活動結果を調査するプロセスに関係する。
［JIS T 14971:2003 定義2.22］

3.23 アクティビティ（**activity**）：一組以上の相互関係又は相互作用のあるタスク
［JIS T 62304(原案) 用語及び定義3.1］

3.24 異常（**anomaly**）：要求仕様書，設計文書，規格など，又は既存の認識若しくは経験に基づいて予想した結果を逸脱する状態。異常は，ソフトウェア製品又は該当する文書のレビュー，試験，分析，コンパイル又は使用中に発見されることがあるが，これには限定しない。
［JIS T 62304(原案) 用語及び定義3.2］{IEEE 1044:1993 定義3.1 参照}

3.25 アーキテクチャ（**architecture**）：システム又はコンポーネントの構造
［JIS T 62304(原案) 用語及び定義3.3］{IEEE 610.12:1990 参照}

3.26 変更要求（**change request**）：ソフトウェア製品に対する変更内容を文書化した仕様
［JIS T 62304(原案) 用語及び定義3.4］

3.27 構成アイテム（**configuration item**）：決められた時点で一意に特定できる“もの”(entity)
注記 JIS X 0160:1996 定義3.6 による。
［JIS T 62304(原案) 用語及び定義3.5］

3.28 成果物（**deliverable**）：アクティビティ又はタスクの要求される結果又はアウトプット（文書を含む）
［JIS T 62304(原案) 用語及び定義3.6］

3.29 評価（**evaluation**）：対象とする“もの”(entity) が，規定した基準に達していることを系統的に決定すること。
［JIS T 62304(原案) 用語及び定義3.7］{JIS X 0160:1996 定義3.9 参照}

3.30 医療機器ソフトウェア（**medical device software**）：開発中の医療機器に組み込むことを目的として開発した，又はそれ自体を医療機器として使用することを意図したソフトウェアシステム。
［JIS T 62304(原案) 用語及び定義3.12］

3.31 問題報告（**problem report**）：ユーザ又はその他の関係者が，安全でない，意図した用途に対して不適切である又は仕様に反すると判断した，ソフトウェア製品の実際の又は潜在的な動作の記録。

注記1 この規格は，すべての問題報告に対してソフトウェア製品の変更を要求するものではない。製造業者は，誤解，エラー又は軽微な事象として問題報告を拒絶できる。
注記2 問題報告は，リリースしたソフトウェア製品又は開発中のソフトウェア製品に適用する。
注記3 この規格は，リリースした製品についての問題報告の法的な対応処置を，確実に特定及び実行できるようにするため，製造業者に別途方針決定を行うことを要求している（箇条6参照）。
［JIS T 62304(原案) 用語及び定義3.13］

3.32 プロセス（process）：インプットをアウトプットに変換する，相互に関連する又は相互に作用する一連のアクティビティ
［JIS T 62304(原案) 用語及び定義3.14］{JIS Q 9000:2006 定義3.4.1 参照}
注記 用語“アクティビティ”は，資源を利用することも含む。

3.33 レグレッションテスト（regression testing）：システムコンポーネントの変更が，機能性，信頼性，性能に悪影響を与えないこと，及び更なる欠陥を招かないことを判定するために要求される試験。
［JIS T 62304(原案) 用語及び定義3.15］{ISO/IEC 90003:2004 定義3.11 参照}

3.34 セキュリティ（security）：権限を与えられていない者又はシステムが読み込んだり変更できないように情報及びデータを保護すること。権限を与えられている者又はシステムがアクセスを拒否されないように情報及びデータを保護すること。
［JIS T 62304(原案) 用語及び定義3.22］{JIS X 0160:1996 定義3.25 参照}

3.35 重傷（serious injury）：直接的又は間接的に次の結果を引き起こすけが又は病気。
a) 生命の危険
b) 身体機能又は身体構造の永久的障害
c) 身体機能又は身体構造の永久的障害を防止するために，内科的又は外科的処置を必要とする障害
注記 永久的障害とは，軽微な障害又は損害を除く，身体構造又は機能の不可逆性の障害若しくは損害を意味する。
［JIS T 62304(原案) 用語及び定義3.23］

3.36 ソフトウェア開発ライフサイクルモデル（software development life cycle model）：ソフトウェア要求事項の定義から製造のためにリリースするまでの，ソフトウェアのライフサイクルにかかわる次のような概念上の構造。
- ソフトウェア製品の開発に関与している，プロセス，アクティビティ及びタスクを明確にする。
- アクティビティとタスクとの間のシーケンス及び依存性を表す。
- 規定した成果物の完全性を検証するマイルストーンを明確にする。

［JIS T 62304(原案) 用語及び定義3.24］

3.37 ソフトウェアアイテム（software item）：コンピュータプログラムの識別可能な部分
{ISO/IEC 90003:2004 定義3.14 修正}
注記 ソフトウェアの構造は，三つの用語によって識別できる。最上位のレベルは，ソフトウェアシステムである。最下位のレベルは，それ以上分割できないソフトウェアユニットである。最上位及び最下位レベルを含む構成のすべてのレベルを，ソフトウェアアイテムということができる。ソフトウェアシステムは，一つ以上のソフトウェアアイテムで構成され，各ソフトウェアアイテムは，一つ以上のソフトウェアユニット又は分割可能なソフトウェアアイテムで構成される。製造業者は，ソフトウェアアイテム及びソフトウェアユニットの定義及び粒度（granularity）を提示する責任がある。
［JIS T 62304(原案) 用語及び定義3.25］

3.38 ソフトウェア製品（software product）：コンピュータプログラム，手続き並びに関連する文書及びデータのまとまり。
［JIS T 62304(原案) 用語及び定義3.26］{JIS X 0160:1996 定義3.26 参照}

3.39 ソフトウェアシステム（software system）：特定の機能又は特定の機能群を達成するために組む，複数のソフトウェアアイテムを結合した集合体。
［JIS T 62304(原案) 用語及び定義3.27］

3.40 ソフトウェアユニット（software unit）：他のアイテムに分割できないソフトウェアアイテム
注記 ソフトウェアユニットは，ソフトウェア構成管理又は試験の目的で使用できる。
［JIS T 62304(原案) 用語及び定義3.28］

3.41 SOUP ：開発過程が不明なソフトウェア（“Software Of Unknown Provenance”の頭字語）既に開発

されていて一般に利用できるが，医療機器に組み込むことを目的に開発したものではないソフトウェアアイテム[“市販品（off-the-shelf）”として知られているソフトウェア]又は以前開発されたソフトウェアでその開発プロセスについての十分な記録が利用できないもの。
[JIS T 62304(原案) 用語及び定義3.29]

3.42 システム（system）：一つ以上のプロセス，ハードウェア，ソフトウェア，設備及び人を統合化して，規定のニーズ又は目的を満たす能力を提供するまとまり。
[JIS T 62304(原案) 用語及び定義3.30]{JIS X 0160:1996 定義3.31 参照}

3.43 タスク（task）：行う必要がある一つの作業
[JIS T 62304(原案) 用語及び定義3.31]

3.44 トレーサビリティ（traceability）：考慮の対象となっているものの履歴、適用又は所在を追跡できること。
（＊）[ISO 9000:2000, ISO 13485:2003]
参考 JIS T 62304(原案) 用語及び定義3.32 では「開発プロセスの二つ以上の成果物間の関係を明らかにできる程度」と定義されている。

3.45 検証（verification）：客観的証拠を提示することによって，規定要求事項が満たされていることを確認すること。
注記1 “検証済み”という用語は，検証が済んでいる状態を示すために用いられる。
{JIS Q 9000:2006 定義3.8.4 参照}
注記2 設計及び開発における検証は，あるアクティビティに対して定義した規定要求事項に適合しているかを確定するために，そのアクティビティの結果に対して吟味を行うプロセスである。
[JIS T 62304(原案) 用語及び定義3.33]

3.46 バージョン（version）：構成アイテムの（時間によって）識別された段階
注記1 ソフトウェア製品のバージョンの変更を行って新しいバージョンとする場合は，ソフトウェア構成管理を実施する必要がある。
注記2 JIS X 0160:1996 定義3.37 による。
[JIS T 62304(原案) 用語及び定義3.34]

3.47 ユーザビリティ（usability）：有効性、効率、ユーザ学習のしやすさ、およびユーザ満足度を作り上げるユーザインターフェースの特性。
[IEC 62366:2007(英和対訳版) 用語と定義 3.17]

4. 記号および略語

CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
FDA	Food and Drug Adminstration
FMEA	Failure Mode and Effect Analysis
FTA	Fault Tree Analysis
GHTF	Global Harmonization Task Force
IEC	The International Electrotechnical Commission
IOM	Institute of Medicine
ISO	The International Organization for Standardization
MDD	Medical Device Directive
NHS	National Health Service
TC	Technical Committee
SC	Sub Committee

5. ソフトウェアライフサイクルプロセス

本章理解のポイント
- JIS T 62304 は、医療用ソフトウェアのライフサイクル(開発計画から製品保守終了まで)における各プロセスにおいて、最低限実施すべきアクティビティとタスクを規定している。
- プロセスとして、ソフトウェア開発プロセスと保守のためのソフトウェア保守プロセスの二つを規定している。
- また、各プロセスは、8 つのアクティビティから構成され、5.2 で述べるソフトウェア安全クラス分類に応じて実施すべきタスクが規定される。
- ソフトウェア安全クラス分類は製品開発の最初の段階で行い、ソフトウェアの機能・目的から生じるリスクに応じて3段階の安全クラスに分類を行う。
- ソフトウェアを分割したソフトウェアアイテム毎にソフトウェア安全クラス分類が可能であり、アイテム毎に安全クラス分類に応じた管理が可能となる。
- クラス分類の論拠やクラス分類に応じた管理履歴を保存する必要がある。

5.1 ソフトウェア開発プロセスと保守プロセス

安全な医療用ソフトウェアを開発するための確実な方法論は、現在のソフトウェアエンジニアリングでは、まだ提案されていない。しかしながら、ソフトウェアライフサイクルの各ステップを確実に行うことにより、ソフトウェアの信頼性を向上させることは可能である。

JIS T 62304「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」では、常に高品質で安全な医療機器ソフトウェアを製造する開発プロセスを示すことを目的としており、信頼性の高い安全なソフトウェア製品を生産できる方法でソフトウェア開発が行われたということを確実にするために、ソフトウェアライフサイクルの各段階において最低限実施すべきアクティビティとタスクを規定している。本規格では、医療機器ソフトウェアの開発のためのソフトウェア開発プロセスと保守のためのソフトウェア保守プロセスを定め、それぞれのプロセスを構成するアクティビティと、アクティビティごとに実施すべき要件であるタスクを規定している。また、付随的なプロセスであるソフトウェアリスクマネジメントプロセス、ソフトウェア構成管理プロセス、ソフトウェア問題解決プロセスについても、同様に規定を行っている。図5－1にソフトウェア開発プロセスにおけるアクティビティの構成と、それぞれのプロセスの関係を示している。

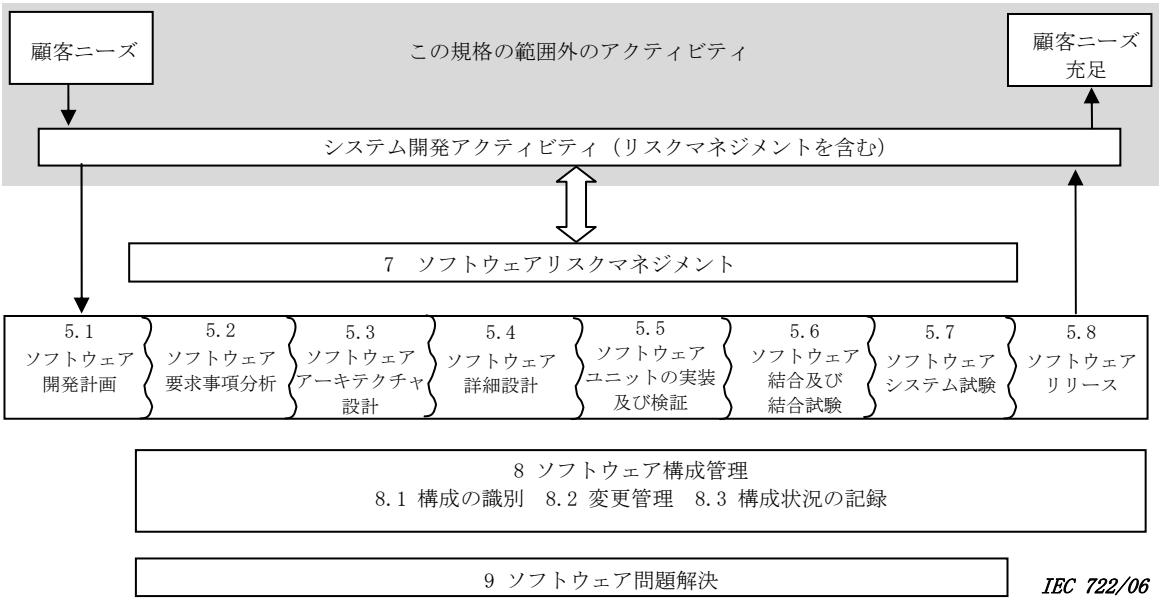


図5－1 ソフトウェア開発プロセスとアクティビティの概要（引用改変）

ここに示すように、ソフトウェア開発プロセスは、図5－1の「5.1 ソフトウェア開発計画」から「5.8 ソフト

ウェアリリース」までの、8つのアクティビティから構成されている。ソフトウェアライフサイクルについては、いくつかのモデルが提案されているが、これらのアクティビティはそれらのモデルに依存せず、共通の概念となっている。それぞれのアクティビティ毎に、後述するソフトウェア安全クラス分類に応じて実施すべきタスクが規定されている。

ソフトウェアを開発しリリースした後も、不具合の改修や機能向上などのためのソフトウェア保守プロセスも重要であり、この概要を図5－2に示している。ソフトウェア保守プロセスは、図5－2の「6.1 ソフトウェア保守計画の確立」、「6.2 問題及び修正の分析」、「6.3 修正の実装」の3つのアクティビティが定義されている。「6.3 修正の実装」においては、ソフトウェア開発プロセスの「5.3 ソフトウェアアーキテクチャの設計」から「5.8 ソフトウェアリリース」までのアクティビティが、実際には実施されることになる。

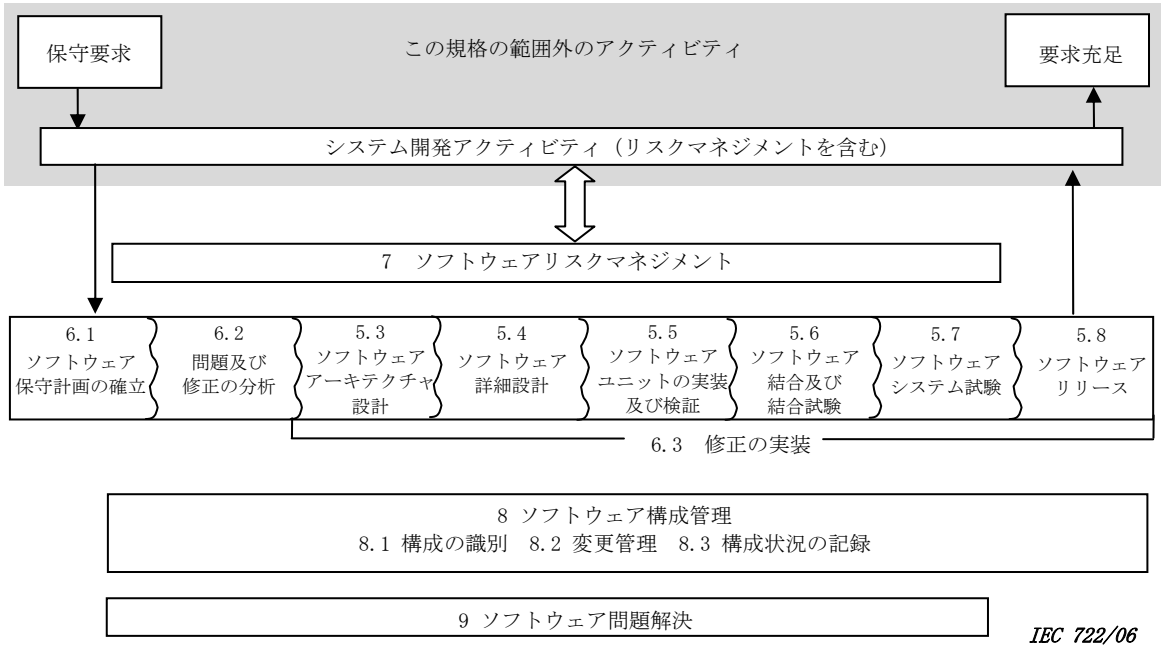


図5－2 ソフトウェア保守プロセスとアクティビティの概要（引用改変）

5.2 ソフトウェアリスク分類

JIS T 62304では、対象となるソフトウェアシステムに起因するハザードが患者やユーザ等の人に及ぼす影響のリスクに応じて、ソフトウェアシステムを次の3段階のソフトウェア安全クラスに、最初の段階で、分類することを求めている。

(1)クラスA：負傷又は健康被害の可能性がない
(2)クラスB：重傷の可能性はない
(3)クラスC：死亡又は重傷の可能性がある

ここで、重要なことは医療機器のリスク分類とは異なり、このようなハザードが発生する確率を100%とみなす、としていることである。従来の医療機器のリスク分類では、障害の重要性と発生確率との組み合わせの考え方を用いている。しかし、ソフトウェアの場合、障害の発生確率を求める方法についてはまだ定説がないため、このような考え方になっている。従って、ここでのクラス分類は、ソフトウェアシステムそのものの機能から、不具合が発生すればどのような影響を人に及ぼすかの観点で行うことになる。ただし、リスクコントロール手段を適切に行うことにより、故障の重大性を低減させたりすることが可能であれば、クラス分類をより安全な方向に変更することは可能である。

このように定めたソフトウェアクラス分類により、ソフトウェア開発プロセスで実施すべきタスクが定められる。クラスCのソフトウェアの開発プロセスでは、すべてのタスクの実施が必要であるが、クラスAの場合はかなりのタスクの実施を省略することが可能となっている。

ソフトウェア開発プロセスにおいて、ソフトウェアシステムは複数のソフトウェアアイテムに分割することが一般的に行われる。その際に、ソフトウェアクラス分類を分割したソフトウェアアイテム毎に評価し直すことが可能となっている。ソフトウェアアイテムの分割の例を図5－3に示す。

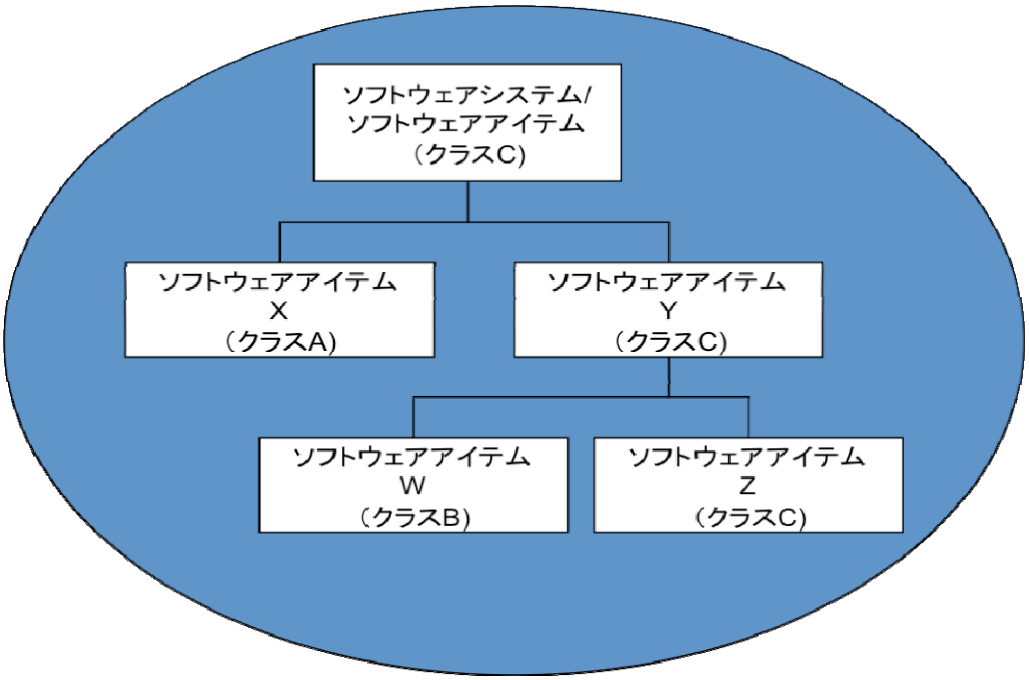


図5−3　ソフトウェアアイテムの分割例

この例では、ソフトウェアシステムとしては、その機能や目的からソフトウェア安全クラスCと予備的に分類されている。そのソフトウェアシステムを、「ソフトウェアアーキテクチャの設計」アクティビティにおいて、最終的にXとWおよびZの3つのソフトウェアアイテムとに分割する。この際に死亡又は重傷を引き起こす可能性のあるハザードの要因となる部分をすべてソフトウェアアイテムZに集約することができる。そのように分割することにより、ソフトウェアアイテムXとWのソフトウェア安全クラス分類をAやBに軽減することが可能となる。ソフトウェアアイテムWとZとから構成される中間的なソフトウェアアイテムYは、より重大なソフトウェア安全クラス分類であるクラスCに分類される。当然、最終的なソフトウェアシステムはクラスCとなる。ソフトウェアアイテムに分割することにより、それぞれのソフトウェアアイテムの開発プロセスにおいては、クラス分類に応じたタスクのみを実施すればよい。

5.3 ソフトウェア構成管理プロセス

このように分割されたソフトウェアアイテムの、ソフトウェアライフサイクル全般にわたる管理を行うプロセスが、図5－1および図5－2の「8 ソフトウェア構成管理プロセス」である。文書を含むシステムにおけるソフトウェアアイテムの識別及び定義、アイテムの修正及びリリースの管理、そしてアイテムと変更要求に関する文書の作成と報告を行う。

このプロセスは、図5－1および図5－2に示したように、「8.1 構成の識別」、「8.2 変更管理」および「8.3 構成状況の記録」の3つのアクティビティから構成されている。

「8.1 構成の識別」で実施が求められているタスクは、構成アイテムの識別手段を確立すること、使用しているSOUPアイテムを特定すること、ソフトウェアシステムの構成要素である構成アイテムの文書化の3つである。

「8.2 変更管理」では次の4つのタスク、変更要求に対する承認、変更要求で指定されているとおりに実装すること、変更された部分の検証の実施、変更要求とその承認や当該問題報告の文書化の実施、が求められている。

「8.3 構成状況の記録」では、構成アイテムに関する検索可能な履歴記録の保存が必要とされている。

これらの構成管理プロセスでのタスクは、ソフトウェア安全クラス分類によらず、すべてのソフトウェアシステムの開発で実施する必要がある。

6. ソフトウェアのリスクマネジメントプロセス

本章理解のポイント
- リスクマネジメントプロセスは、JIS T 14971で定義されている。ここでは、リスクマネジメントプロセスにおけるリスクアセスメント、リスクコントロールなど各プロセスの概要理解を目指す。
- ソフトウェアにおけるリスクマネジメントを、ソフトウェアライフサイクルマネジメントの中でどのようにすすめるべきかについてはJIS T 62304に規定されているため、その内容も合わせて紹介する。
- この二つの規格のリスクマネジメントを分かり易く要約した具体的なガイダンスとして、IEC/TR80002-1（2009/9/21発行）が挙げられる。そのポイントについては、IEC/TR80002-1のAnnex_Cを付則D（翻訳版）に記載する。

6.1ソフトウェアリスクマネジメント

製造業者は、ライフサイクルを通じて製品に関連する潜在的原因（ハザード）を特定し、関連するリスクの推定及び評価を行い、これらをリスクコントロールし、そのコントロールの有用性を監視する一連のプロセスを確立し、文書化し、かつ維持する。このプロセスは、リスク分析、リスク評価、リスクコントロール、製造中及び製造後の情報の各プロセスを含む。

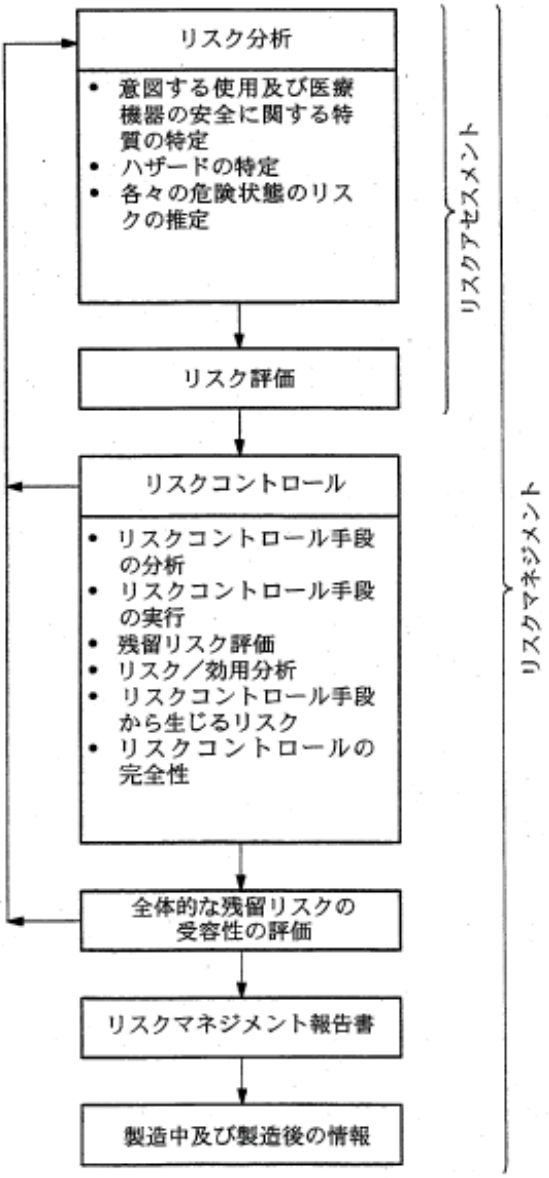


図6－1 リスクマネジメントプロセス（JIS T 14971による）

6.1.1 危険状態を引き起こすソフトウェアの分析と評価

製造業者は、危険状態（JIS T 14971に特定されている）を引き起こすおそれのあるソフトウェアアイテムと、その潜在的原因を特定し、そのイベントシーケンスとともにリスクマネジメントファイルに文書化する。必要に応じて次のような潜在的原因を検討する。

a) 誤った／不完全な機能仕様

b) 特定のソフトウェアアイテムの機能における不具合

c) SOUP に起因する、故障又は予期せぬ結果（最低限、公開されている不具合リストを評価し、危険状態の原因となり得るイベントシーケンスが生じるかどうかを評価する。）

d) 予測できないソフトウェア動作の原因となる、ハードウェア故障／ソフトウェア欠陥

e) 合理的に予見可能な誤使用

［クラスB,C］

6.1.2 リスクコントロール手段

製造業者は、潜在的原因のそれぞれについて、リスクコントロール手段を定義し、文書化する。リスクコントロール手段をソフトウェアで実装する場合、次の事項を実施する。

a) リスクコントロール手段をソフトウェア要求事項に含める

b) リスクコントロール手段によってコントロールしているハザードの影響に基づいて、当該ソフトウェアアイテムのソフトウェア安全クラス分類を行う

［クラスB,C］

6.1.3 リスクコントロール手段の検証

製造業者は、リスクコントロール手段がすべて実装されていることを検証し、その検証結果を文書化する。リスクコントロール手段を評価して、危険状態を招くおそれのある新たなイベントシーケンスを特定し、リスクマネジメントファイルに文書化する。ソフトウェアハザードの危険状態、ソフトウェアアイテム、特定のソフトウェアの原因、リスクコントロール手段、リスクコントロール手段の検証の間のトレーサビリティについて、適宜文書化する。［クラスB,C］

6.1.4 ソフトウェア変更のリスクマネジメント

製造業者は、ソフトウェア（SOUPを含む）の変更内容を分析して、次の事項を確認し、リスクマネジメントを実行する。

a) 潜在的原因が新たに生じていないかどうか ［クラスA,B,C］

b) 新たなソフトウェアリスクコントロール手段が必要ないかどうか ［クラスA,B,C］

c) ソフトウェアの修正が既存のリスクコントロール手段の妨げとならないかどうか ［クラスB,C］

6.2 ソフトウェア開発プロセスにおけるリスクマネジメント

6.2.1 ソフトウェア開発計画

製造業者は、ソフトウェアシステムの適用範囲、規模、ソフトウェア安全クラス分類に適したソフトウェア開発プロセスを実施するために、ソフトウェア開発計画を立てる。ソフトウェア開発計画には、ソフトウェアリスクマネジメントプロセスのアクティビティとタスクの実行計画（SOUPに関連したリスクの管理を含む）を含める。［クラスA,B,C］

6.2.2 ソフトウェア要求事項分析

製造業者は、システムレベルの要求事項に基づきソフトウェアシステム要求事項を定義して文書化する。［クラスA,B,C］要求事項として、ソフトウェアを実装するハードウェアの故障及びソフトウェアハザードに対するリスクコントロール手段を含める。［クラスB,C］また、ソフトウェア要求事項が確定した時点で、システムレベルのリスク分析と、既存の要求事項（システム要求事項等）を再評価し、適宜更新、検証し、文書化する。［クラスA,B,C］

6.2.3 ソフトウェアアーキテクチャの設計

製造業者は、ソフトウェアの要求事項を、アーキテクチャに変換し文書化する。[クラスB,C]リスクコントロールに不可欠なソフトウェアアイテム間の分離を特定し、確実に分離するための方法について明示する。[クラスC] ソフトウェアアーキテクチャが、リスクコントロールに関する要求事項を実現していることを検証し、文書化する。[クラスB,C]

6.2.4 ソフトウェアユニットの詳細設計・実装及び検証

製造業者は、リスクコントロール手段を含む各ソフトウェアユニットを設計し実装する。必要に応じて、より大きなソフトウェアアイテムに結合する前に、ソフトウェアコードがリスクコントロール手段を実装しているか等の検証を行う。[クラスB,C]

6.2.5 ソフトウェア結合及び結合試験

製造業者は、ソフトウェア開発計画に従ってソフトウェアユニットを結合し、検証し、記録する。結合試験内容の例として、リスクコントロール手段の実装の有無が挙げられる。[クラスB,C]

6.2.6 ソフトウェアシステム試験・リリース

製造業者は、個々のソフトウェア要件について、インプット内容、予想される結果、合否判定基準及び手順を規定した一連の試験を確立し、実施する。試験中不具合対策等で変更があった場合、6．1．4に示した関連リスクマネジメントアクティビティを実行する。既知の残留不具合を文書化し、受容できないリスクの原因にならないことを確認した後リリースする。[クラスB,C]

6.3ソフトウェア保守プロセスにおけるリスクマネジメント

6.3.1 ソフトウェア保守計画の確立

製造業者は、保守プロセスのアクティビティ及びタスクを実行するための、ソフトウェア保守計画を立てる。計画はソフトウェアリスクマネジメントプロセスの使用を含むものとする。[クラスA,B,C]

6.3.2 問題及び修正の分析・実装・リリース

製造業者は、リリースしたソフトウェア製品について、自身の組織内部及びユーザからのフィードバックを監視し、文書化するとともに評価し、そのソフトウェア製品に問題がないかを判断する。問題があった場合は、問題報告として記録し、その対処のためにリリースしたソフトウェア製品の安全性にどのような影響があるかを判断するとともに変更を加える必要があるかどうかを判断する。修正の実装・リリースについては6．2に述べたとおり。[クラスA,B,C]

7. ベリフィケーションとバリデーション（検証と妥当性確認）

本章理解のポイント
- JIS T 62304 などの標準規格では、ソフトウェアの検証や確認はひとつの概念であり、レベルや段階の区別はない。一方、各国の法規制ではベリフィケーションとバリデーションのふたつの確認を求めている。以下、ベリフィケーションとバリデーションの違いを紹介する

ベリフィケーションについては
- 製品（成果物）：設計（書）通りに作成されているかを確認すること
- 作業工程（開発、保守）プロセス：設計、コーディングをレビュー、テストなどプロセスを実行することにより正当性を確認すること。 レビュー、ウォークスルー、コードレビュー、（広義の）デバッグ、テストなどを含む

バリデーションについては
- 製品（成果物）：顧客の意図する用途・目的に対応する妥当性を確認すること
- 作業工程（開発、保守）プロセス：各活動、ベリフィケーション等の、計画、方法、結果を評価しプロセス自身の妥当性を確認（承認）すること

7.1 概要

一般にベリフィケーションは、検証、実証とか照合、バリデーションは、妥当性、有効性確認とか認証などという意味で使われているが、ソフトウェアの開発プロセスのでは、それぞれ検証、妥当性確認と訳されている。しかし、相互に関連しているうえ、多種多様な開発形態においてどこまでがベリフィケーションで、どこからがバリデーションなのかがとらえにくい面がある。そこで概念を図7－1に示す。

顧客の意図する用途・目的に対応する有効性（製品に正しく実装され、機能することを保証すること）を確認するのがバリデーション。

設計（書）通りに成果物が作成されているかを確認するのがベリフィケーションととらえておくと理解しやすいであろう。

7.2 （医療機器で求められている）ソフトウェアのベリフィケーション（検証）

1）概要

ソフトウェアのベリフィケーションはソフトウェアの品質を高め、その完成度を確認する活動である。開発プロセス、保守プロセスなどにおける各活動にはそれぞれの活動に対する検証作業が組み込まれていること。

2）ベリフィケーションの定義

ベリフィケーションとは、IEC 62304:2006 の細分箇条 3.33 項において「客観的証拠を提示することによって、規定要求事項が満たされていることを確認すること。」との内容が定義され、また、JIS Q9000:2006 (ISO 9000: 2005) 品質マネジメントシステム基本及び用語－の細分箇条 3.8.4 検証 (verification) では「客観的証拠を提示することによって、特定要求事項が満たされていることを確認すること。」と定義されている。

また、FDAガイダンスである General Principles of Software Validation（以下 GPSV）の3.1.2項には「ソフトウェアベリフィケーションは、ソフトウェア開発ライフサイクルのある特定フェーズの設計アウトプットがそのフェーズで定められている全ての要求事項を満足することを示す客観的証拠をそろえることであり、ここではソフトウェアの開発における一貫性、完全性、正確性を補完する文書が望まれている」

いずれも、客観的証拠を用いて要求事項が満たされていることを確認することが必要となる。

3）ベリフィケーションの作業手順例

a） ベリフィケーションの計画
b） ベリフィケーション手順書の作成とテスト
c） ベリフィケーション報告書の作成
d） ベリフィケーションの終了判断

7.3 医療機器ソフトウェアのバリデーション（妥当性確認）

1）概要

ソフトウェアのバリデーションはソフトウェアの品質、有効性、安全性の完成度そしてユーザが安心して使えるソフトウェアであると判断するために行う。

各製造業者は、これらの内容を選択する柔軟性を持っているが、ソフトウェアがバリデーションされていることを証明する最終的な責任を持たなければならない。[GPSV 4.10参照]

2）バリデーションの定義

バリデーションは、FDAの品質システム規則（21 CFR 820） Sec. 820.3 において

「バリデーションとは特定の Intended use のための特定の要件が一貫して実現できるという客観的証拠の提供と試験で確認することを意味する。」との内容が定義され、また、JIS Q9000 :2006 (ISO 9000: 2005) 品質マネジメントシステム－基本及び用語－の細分箇条 3.8.5 妥当性確認 (validation) では「客観的証拠を提示することによって、特定の意図された用途又は適用に関する要求事項が満たされていることを確認すること。」と定義されている。

また、FDAガイダンスであるGPSVの3.1.2項では、ソフトウェアのバリデーションについて

「ソフトウェアの仕様がユーザのニーズと Intended use に合致することを、試験と客観的証拠をそろえる事で確認し、ソフトウェアを通じて達成しようとした所定の要求事項が定常的・安定的に達成されることを確認することである。」という内容が記されている。

3）バリデーションの実行担当者

バリデーションはソフトウェア開発部門と独立した責任あるテスト専任者によって実施されることが望ましい。[GPSV 4.9参照]

4）バリデーションの作業手順例

a) バリデーションの計画
b) バリデーション手順書の作成とテスト
c) バリデーション報告書の作成
d) バリデーションの終了判断

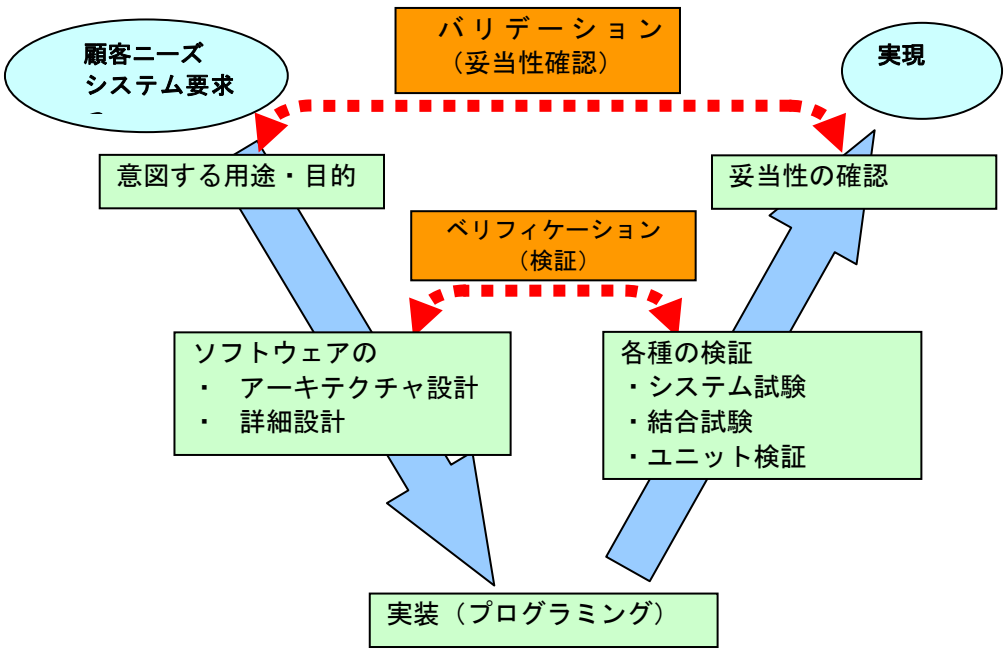


図7－1 V-model

8. リスクマネジメント報告他

本章理解のポイント
- リスクマネジメントのユーザへの報告に関しては、各規格において記述がある。本技術文書では、主なものをピックアップして記載し、ユーザから要求される可能性のある文書についての理解を深めることを目的としている。
- JIS T 62304、IEC80002-1では、ソフトウェアのリスクマネジメントプロセスを実施すると共に、エビデンスの文書化とその保存を求めている。
- JIS T 62304において、文書化について規定したものとして、「ソフトウェア構成管理プロセス」および「問題解決プロセス」がある。
- IEC80002-1において、文書化について規定したものとして、「リスクマネジメント」および「製造および市販後製造情報」の文書化がある。また、新たなものとして、Safety Caseの解説があり、これについても検討結果を文書化し保存、公開することが望ましいとされている。

本章では、JIS T 62304、IEC80002-1における“文書化と報告”についての記載を、以下にまとめて紹介する。

8.1 JIS T 62304 8章　ソフトウェア構成管理プロセス

ソフトウェア構成管理プロセスの内容は、5．3において記述されている通り、ソフトウェアライフサイクル全般に渡って管理手順と技術的手順を適用するプロセスであり、そのプロセスの文書化である。

8.2 JIS T 62304 9章　ソフトウェア問題解決プロセス

ソフトウェア問題解決プロセスは、問題の性質や源に関わらずに、問題(不適合を含む)を分析し解決するプロセスであり、問題には、開発、保守又は、その他のプロセスの実行時に発見されたものも含まれる。その目的は、適時の、責任を伴う文書化された手段によって、発見された問題が分析、解決され、その傾向が認識されるようにすることである。このプロセスは”欠陥追跡”といわれることもある。

このアクティビティは、問題又は不適合が特定されたときに、製造業者がソフトウェア問題解決プロセスを使用することを要求している。発見された問題が、安全との関連性について分析及び評価されることを確実にするために必要である。

「問題報告の作成(タイプ、適用範囲、深刻度)」「問題の調査(問題調査、原因特定、安全性へのかかわり評価、調査結果の文書化、是正措置に必要な処理の変更要求)」「関係者への通知」「変更管理プロセスの使用」「記録の保持」「問題の傾向分析」「ソフトウェア問題解決の検証(問題の完了、改善、変更要求の実装、新たな問題の発生の有無)」「試験文書の内容」が規定されている。

「試験文書」には、試験結果、発見された不具合、試験したソフトウエァのバージョン、関連するハードウェア及びソフトウェアテスト構成、関連試験ツール、試験実施日、試験者の識別を含める。

8.3 IEC80002-1 8章　リスクマネジメント報告

IEC80002-1では、以下ISO14971から以下枠内の内容を転載してある。

ISO14971:2007の本文
8 リスクマネジメントの報告書

医療機器の商品流通のための出荷に先立って、**製造業者**は、**リスクマネジメントプロセス**の見直しを実行しなければならない。この見直しでは、少なくとも次のことを確実にしなければならない:
— リスクマネジメント計画を適切に実行した;
— 全体的な残留リスクは受容可能である;
— 関連する製造中及び**製造後**の情報を得るのに適切な方法を整備した。

この見直しの結果は**リスクマネジメント**報告書として記録し、**リスクマネジメントファイル**に含めなければならない。

見直しに対する責任は、**リスクマネジメント**計画の中で、適切な権限を持つ人に割り当てることが望まし

い[3.4bを参照]。

適合性は**リスクマネジメントファイル**の調査によって確認する。

リスクマネジメントプロセスのレビューの一部として含めるためには、IEC62304:2004の第6節及び7.3.3を検討することが望ましい。

8.4 IEC80002-1 9章　製造および市販後製造情報

IEC80002-1では、ISO14971から以下の内容を転載してある。

ISO14971:2007の本文

9　製造中及び製造後の情報

製造業者は、**医療機器**又は類似の機器に関して製造又は**製造後**の段階で得た情報を、収集し見直すためのシステムを確立し、文書化し、かつ、維持しなければならない。

医療機器に関する情報を収集し見直すために**システム**を確立する場合、**製造業者**はとりわけ次のことを考慮することが望ましい:
a) 操作者、使用者又は、**医療機器**の設置、使用及び保守の責任者によって生成された情報を収集し処理するメカニズム;
b) 新規又は改正された規格。
又は
システムは、また、市場に出ている類似の**医療機器**に関する公に利用可能な情報を収集し、かつ、見直しすることが望ましい。

この情報は**安全**、特に下記事項に関連する可能性があるかを評価する:

—以前に認識さなかった**ハザード**又は**危険状態**があるかどうか、又は

—**危険状態**から発生すると推定した**リスク**が、もはや受容できないものであるかどうか。

上記の条件のうちのどれかが生じる場合:
1) 以前に実施したリスクマネジメント活動に対する影響を評価し、結果をリスクマネジメントプロセスにインプットしてフィードバックしなければならない。
2) 医療機器のリスクマネジメントファイルの見直しを実施しなければならない;もし残留リスク又はその受容性が変化した可能性がある場合、以前に実施したリスクコントロール手段に対する影響を評価しなければならない。

この評価の結果を**リスクマネジメントファイル**に記録しなければならない。

備考1　**製造後**監視の幾つかの側面は、国の規制の対象となる。そのような場合には、追加手段が要求されるかもしれない(例えば、先を見越した製造後評価)。

備考2　ISO 13485:2003の8.2も参照。

適合性は**リスクマネジメントファイル**及び他の適切な文書の検査により確認する。

ソフトウェアリスクマネジメントは、ソフトウェア保守プロセス(IEC 62304:2006　第6節参照)及びソフトウェア問題解決プロセス(IEC 62304:2006　第9節参照)を含むソフトウェアライフサイクルの間中、続く。

IEC62304:2006の第6節は、製造業者に、医療機器ソフトウェア出荷後のフィードバックを受け入れ、文書化し、評価し、追跡調査するための手順の使用について取り上げたソフトウェア保守計画の策定を要求している。保守計画では、医療機器ソフトウェア出荷後に発生する問題の分析及び解決のための、

ソフトウェアリスクマネジメントプロセス及びソフトウェア問題解決プロセスも取り上げる。

ソフトウェア問題解決プロセス（IEC62304:2006 第9節参照）を採用すればソフトウェア問題解決の調査及びその問題と安全との関連性の評価に関するリスクマネジメント活動が統合される。問題の調査及び評価には、臨床の専門家、ソフトウェア技術者、システム設計者及びユーザビリティ／ヒューマンファクタエンジニアリングの専門家を含む、学際的チームを参加させることが重要である。

SOUPも、ソフトウェア保守計画及び製造後のリスクマネジメント活動の重要な一面である。SOUPの中には、その性質上（ウイルス監視ソフトウェアなど）、頻繁に更新されるものがあるので、製造業者はソフトウェア保守計画でこの点について考慮することが望ましい。

SOUPの故障又は予外の結果、並びにSOUPの陳腐化(サポートの停止)は、医療機器の全体的残留リスク受容性に影響することがある。そのため、ソフトウェアシステムの開発及び保守に当たっては、SOUPの監視及び評価活動を実施する必要がある。このような活動では、SOUPのアップデート、アップグレード、バグフィックス、パッチ及び陳腐化を取り上げることが望ましい。SOUPの実地性能に関する一般公開異常リスト及び情報を積極的に監視し、評価を行えば、製造業者は、判明している異常が原因の危険状態を招くようなシーケンスが発生するかどうかを事前に判定することができる(IEC62304:2006の6.1(f)、7.1.2(c)、7.1.3、7.4.2参照)。

製造業者からリリースされるSOUPのパッチまたはアップデートには、医療機器の安全及び有効性にとって必須でない追加機能が含まれていることがある。このようなSOUPのアップデートに、危険状態を招く恐れのある予想外の変更を回避するために、医療ソフトウェアリリースから削除できる必要以上のコンポーネントがないか分析することが望ましい。

ソフトウェアアイテムの変更に関して、製造業者は、どのようなソフトウェアアイテムがSOUPのアップデートに影響されるかを認識し、回帰試験を実施することが望ましい（IEC62304: 2006 7.4、8.2、9.7参照)。

8.5 IEC80002-1 Annex_E　Safety Case

IEC80002-1 Annex_Eでは、セーフティケースについて以下の記載をしている。

セーフティケースとは、“医療機器が、所定の運転環境で所定の意図する使用について安全であるという、説得力のある総合的で、正当なケースを示す多数の証拠によって裏づけられる構造化された論拠”である（UK Mod DefStan 00-56を一部修正）。

軍事システム、海洋油田産業、鉄道輸送及び原子力産業界のような業界では、セーフティケースの概念は広く知られているが、医療機器産業ではこの手法は必須とされておらず、この附属書もISO14971にない要求事項を追加することを意図したものではない。

この技術報告書は、セーフティケースが、医療機器の適切なレベルの安全を構造化し、文書化し、伝達する手段となりうるものであると提案する。セーフティケースは、医療機器の寿命が尽きるまで安全の維持を確保する手助けとすることも出来る。

セーフティケースは、リスクマネジメントプロセスの結果を用いて、なぜソフトウェアは意図する使用に十分に安全か、なぜすべての要求事項をみたすのか(そして該当する規制用語でそれができるのはなぜか)を明確に述べる。

セーフティケースは、リスクマネジメントファイルの支援情報及び証拠のより詳細な文書に基づいた、リスクマネジメント又は残留リスクの要約とも見ることができる。すべてのリスクコントロール手段の使用及び試験範囲を実証するためのクロスレファレンスを、ここに含めることもできる。

セーフティケースを実現するためには、次のステップが必要である:

— システムに対する明確な主張の集合
— 裏づけとなる証拠の提示
— 主張と証拠を結びつける安全論議の集合
— 論議を基礎とする仮定及び判定
— 異なる視点及び詳細のレベルの容認

セーフティケースの主要な要素は、次のとおりである。

－ 主張　システム又はサブシステムの特性に関する;
－ 証拠　安全論議の論拠として使用するもの。事実(確立されている科学原理及びこれまでの調査に論拠を置いたものなど)でもよいし、仮定でも、下位の立論か導き出された主張でもよい;
－ 論拠　証拠を主張に結びつけるもので、決定論的なことも、蓋然論的なことも、又は定性的なこともある;
－ 推論　立論の変則規則を示す手段。

9. ユーザビリティ

本章理解のポイント
- 医療機器および医療機器ソフトウェアにおけるユーザビリティの管理の考え方を、医療情報システムの設計の参考にする。
- IEC62366: 2007は、製造業者がユーザビリティを分析、指定、設計、検証、妥当性確認を行うためのプロセスを規定したものである

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 －Applocation of usability engineering to medial 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、

医療情報システムにおいても、使用者の使用方法を想定して、設計、検証をおこなう事は非常に重要であるため、ユーザビリティエンジニアリングの管理手法の概要を以下に記載する。

ユーザビリティに関する規格としては、医用電気機器を適用範囲としたIEC60601-1-6も存在するが、内容はほとんど同じであり、医療機器全体を適用範囲としたIEC62366（2007年初版）の概要を以下に記載する。

9.1 ユーザビリティの説明

主な実施項目

(1) ユーザビリティ仕様へのインプット
(2) ユーザビリティ仕様の作成
(3) ユーザビリティ仕様の検証と妥当性確認

これらの結果はユーザビリティエンジニアファイルに記録する。ユーザビリティエンジニアリングプロセスへの適合は、ユーザビリティエンジニアリングファイルの検査によって確認する。

1.ユーザビリティ仕様へのインプット

以下の項目を明確にする。

1-1医療機器の用途

(1) 意図する医学的適用
　検査、モニタ、治療、診断もしくは予防すべき状態若しくは病気　等
(2) 意図する患者集団
　年齢、体重、健康状態、条件　等
(3) 適用する又は対応する、意図された体の部位または組織の種類
(4) 意図するユーザプロファイル
　教育、知識　言語の理解、経験、等
(5) 意図する使用条件
　衛生要求事項を含めた環境、使用頻度、場所、移動の可否
(6) 操作の原則

1-2使用頻度の高い機能

1-3ユーザビリティに関連するハザード及び危険状態の特定

(1) 安全に関係する特性の特定
　医療機器の場合は、ユーザビリティを重視した安全に関する特性の特定（リスク分析の一部）をISO14971:2007の4.2にしたがっておこなう。
(2) 既知の又は予測可能なハザード及び危険状態の特定）

医療機器の場合は、14971:2007の4.3にしたがって、ユーザビリティに関係する既知の又は予測可能なハザードを特定する。

1-4 主操作機能

主操作機能には使用頻度の高い機能、安全に関係する機能を含めなければならない、

2.ユーザビリティ仕様の作成

ユーザビリティ仕様には少なくとも次の事項を記載しなくてはならない。

2-1次の点を含めた、主操作機能に関する使用シナリオ

(1) 頻度の高い使用シナリオ

(2) 妥当に予測可能な最悪の使用シナリオ

2-2リスクを軽減する為の要求事項を含めた、主操作機能のユーザインターフェース要求事項

2-3主操作機能を使用者が容易に認識できるかどうかを判定する為の要求事項。

3. ユーザビリティ仕様の検証と妥当性確認

3-1ユーザビリティ仕様の妥当性確認計画

ユーザビリティの妥当性確認計画を作成する。以下の事項を規定しなくてはならない。

(1) 主操作機能のユーザビリティの妥当性確認に用いる方法

(2) ユーザビリティ仕様に基づいて、主操作機能のユーザビリティの妥当性確認を判定する為の基準。

(3) 意図する代表的使用者の関与の度合い。(評価者は意図する代表的な使用者を模擬できる人であること。)

また、以下の事項に対応しなければならない。(ユーザビリティ仕様で規定)

(1) 頻度の高い使用シナリオ

(2) 妥当に予測可能な最悪の使用シナリオ

3-2 ユーザインターフェースの設計及び実現

ユーザビリティ仕様に記載されたようなユーザインターフェースを設計し、実現する。

3-3 ユーザビリティの検証

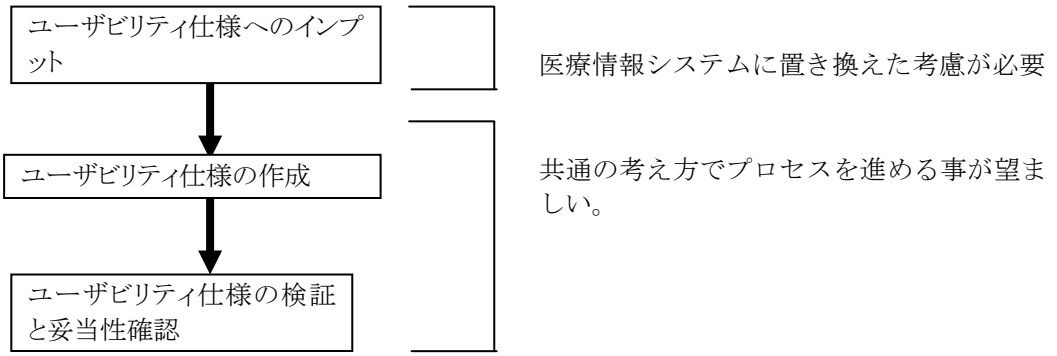
ユーザビリティ仕様の要求事項に照らして。ユーザインターフェース設計の実現度を検証する。

3-4ユーザビリティの妥当性確認

ユーザビリティの妥当性確認計画に従ってユーザビリティの妥当性確認をおこなう。

9.2 医療情報システムとして適用する場合

ユーザビリティ仕様へのインプット項目には、医療情報システムとしては適用範囲外の項目も含まれる。取り扱う医療情報システムとして共通に考慮必要な項目への置き換えを検討したうえで、以降のユーザビリティプロセスを進める事が、医療情報システムとして望ましい。



ユーザビリティ仕様へのインプットにおける置き換え例として、医療機器の電子体温計と医療情報システムの注射オーダ発行業務を対比した形で、付則Cに示す。

10. リスク回避手段のトレーサビリティ

本章理解のポイント
- リスクマネジメントの結果、採用・実施されたリスク回避手段と予防処置について、その履行状況と有効性を確認するために、医療機関は安全監視を計画・実行し、事象や証跡データを記録する。
- 上記を実現するために、製造業者は残留リスクとリスク回避手段、利用において予期されるリスクと予防処置の提案、医療用ソフトウェアに備わるトレーサビリティの情報を医療機関に提供する。
- 医療機関の安全管理責任者は記録した事象や監査証跡データを適時参照し、問題点が発見された時は是正処置を講じるとともに、必要あれば製造業者に改善を要請する。

用語説明　安全監視(vigilance)　:医療機関に供用した医療用ソフトウェアが安全に利用されているか調査・監視する一連の行為。市販後調査とも呼ばれる。
事象(event)　:「検査をオーダした」、「処方薬を出庫した」などの行為。
証跡データ(evidence)　:事象の内容を示すデータ。上記の例では「検査項目」、「薬剤名」。

前章までのリスクマネジメントプロセスの結果としての残留リスクと、診療プロセスで推定される利用上のリスクが存在し得るが、それらの対策が適切に・有効に実行されるように担保され確認するには、利用者である医療機関の協力が欠かせない。 それは、医療機関が自ら安全監視体制を確立し・実行することを意味する。

よって、本ガイドラインの適用範囲にない医療機関側の安全管理(リスクマネジメント)について、この章は必要な限りの説明を加える。

10.1 概要

(1) 製造業者は、前章までのリスクマネジメントプロセスの結果として、下記を決定する。
　－残留リスクとそのリスク回避手段
(2) 医療機関は、これらを受け入れ、さらに診療プロセスでの利用でリスクを推定・加味して、下記を策定する。
　－予防処置(安全性を担保するための作業とその手順)
　(前章までの各章では、医療用ソフトウェアそのものが具有するリスクについて解説したが、利用者の運用にもリスクがあることに留意されたい。例えば、ある機能について教育訓練を受けていない不適格者が端末を操作し診療情報が消失した。)
(3) 医療機関は、この予防処置について下記を確認(トレース)しなければならない。
　－適切に利用されているか(履行状況)
　－効果を発現しているか(有効性)
　医療機関の安全管理責任者は、上記を確認するため、記録の対象と記録手段を定め、記録した証跡データを参照・分析する。 その結果、問題点があれば、自らの是正処置(自らのリスクマネジメントプロセスにフィードバックすることも含む)を講じるか、もしくは製造業者に改善を要請する。

10.2 製造業者が提供する情報とトレーサビリティ

(1) 残留リスクと利用者に求めるリスク回避手段
　a) リスクの説明には、予想される危険状態の重篤度も併せると注意喚起になるだろう。
　b) これらは文書(添付文書)として、事前に提供されなければならない。
　　(薬事法対象の医療機器では、要求されている添付文書の記載範囲に拘らず、患者と医療従事者の安全確保の視点で必要な事項を提示することが望まれる。)
(2) 利用方法に関わるリスクと医療用ソフトウェアが備えるリスク回避手段
　a) (1)に同じ
　b) (1)に同じ
　c) 推奨できる予防処置があれば、提案する。
(3) 利用可能なトレーサビリティ(医療用ソフトウェアが備える機能)
　当該機器で記録できる事象や証跡データの種類、記録と確認の方法、データ保護手段を提供す

る。

10.3 医療機関が確立し運用するトレーサビリティ

安全管理またはリスクマネジメントの責任者は、

(1) 製造業者から提供された、残留リスクと利用者に求められたリスク回避手段、利用に関わる推定リスクと予防処置の提案、そして装置に具備されたトレーサビリティ機能を理解し評価する(10.2項、参照)。

(2) (1)で示された利用に関わる残留リスクと推定リスクも含め、診療プロセスで生じ得るリスクを分析・推定し、予防処置を検討する。

(3) トレース対象の事象や証跡データを特定する(リスク分析の結果などから導く)。

(4) 事象・証跡データの記録と参照・分析(トレース)の方法を検討し決定する(マニュアル的な方法と医療用ソフトウェアの機能の利用)。 参照と維持管理する権限(担当者など)も決定する。
医療用ソフトウェアに具備された機能を使用するときは、供給者から十分な説明または訓練を受ける。

(5) 定期的にトレースするようにスケジュールし、事象・証跡データの保存期間と廃棄方法を規定する。

(6) 以上は文書化し、関係者に周知する。

10.4 補足（関連規格）

(1) JIS Q 13485 医療機器－品質マネジメントシステム－規制目的のための要求事項

この規格は、医療機器の製造業者に対して品質システム(ISO 9001)を適用する為の要求事項を述べているが、その中で下記が述べられている。 これらの考えは、本章にも当てはまる。

4.2.4項 記録の管理

「記録は、要求事項への適合及び品質マネジメントシステムの効果的運用の証拠を示すために、作成し、維持する。 記録は、読みやすく、容易に識別可能で、検索可能とする。 記録の識別、保管、保護、検索、保管期間及び廃棄に関して必要な管理を規定するために、“文書化された手順”を確立する。」

7.5.3.2項 トレーサビリティ

「組織は、トレーサビリティに対して“文書化された手順”を確立する。 そのような手順は、製品のトレーサビリティの範囲及び要求される記録を規定する。 トレーサビリティが要求事項になっている場合は、組織は、その製品固有の識別を管理し、記録する。」

(2) JIS T 14971 医療機器－リスクマネジメントの医療機器への適用

この規格の中で下記が関連している。 これらも参考にされたい。

9章 製造中および製造後の情報

「製造業者は、その医療機器又は類似の機器に関して製造又は製造後の段階で獲た情報を収集し見直すための体系的手順を確立し、文書化し、維持しなければならない。」
本ガイドラインの8．4では、IEC 80002-1 9章での引用として紹介し、考慮すべき事柄を述べている。

附属書 E (参考) ハザード、予見できる一連の事象及び危険状態の例

表 E.1 に操作上のハザートの例、表 E.2 に人的要因による事象及び状況の例が示されている。

附属書 J (参考) 安全に関する情報及び残留リスクに関する情報

— 安全性に関する情報をどのようにリスク分析手段として提供するか
— 残留リスクはどのように開示するか
の指針が示されている。

(3) IEC 80001-1 Application of risk management for IT-network incorporating medical devices

これは医療ITネットワークでのリスクマネジメントに関する規格であり、本ガイドラインの付則Eはその概要を紹介している。

このE.8節で言及されている医療機関(責任組織)が確立すべき事柄とリスクの上昇に対する対応は、本章にも当てはまる。

(4) JIS Q 27001　情報セキュリティマネジメントシステムー要求事項
JIS Q 27002　情報セキュリティマネジメントの実践のための規範

通称 ISMS(Information Security Management Systems) と呼ばれるこれらの規格は、情報システムのセキュリティリスクを体系的に特定し、情報システムと情報資産を、機密性、完全性、可用性の観点で、脅威から保護する方法を提示している。

トレース対象のデータには、利用者のアクセス記録が含まれるかもしれない。 このトレース機能は、施設およびシステムの安全確保のための情報セキュリティ機能と連携または兼用するだろう。

付則Ａ：電子カルテシステムおよびオーダエントリシステムのソフトウェア構成例とリスク評価例

医療機関で使用される電子カルテシステムは、多数の業務対応モジュールを含む。この電子カルテシステムをIEC 62304で定義するソフトウェア安全クラスにあてはめたソフトウェア構成例とリスク評価例を以下に記載する。

Ａ－１　電子カルテシステムのソフトウェア構成例とリスク評価例

IEC 62304では、ソフトウェアシステムに起因するハザードが患者やユーザ等の人に及ぼす影響のリスクに応じて、ソフトウェアシステムを次の3段階のソフトウェア安全クラスに分類することを求めている。（「第7章　ソフトウェアリスク分類&構成管理」を参照）

（1）　クラスA：負傷又は健康被害の可能性がない
（2）　クラスB：重傷の可能性はない
（3）　クラスC：死亡又は重傷の可能性がある

Ａ－２　電子カルテシステムの定義

電子カルテシステムは病院情報システムのソフトウェアの一部として構成される。図Ａ－１－１に一般的な病院情報システムの構成を示す。

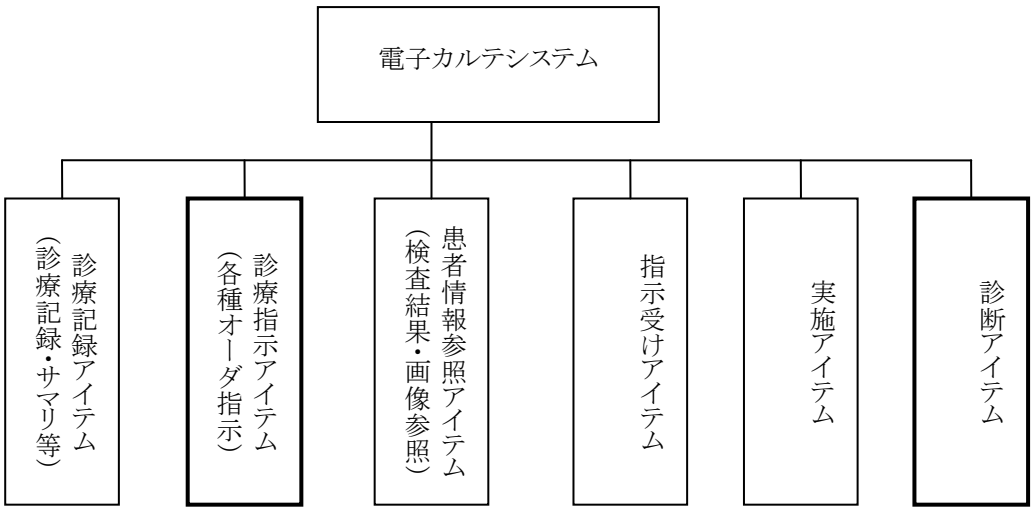
図Ａ－１－１　病院情報システムのソフトウェア構成例

電子カルテシステムの範囲については各ベンダー毎に異なり画一的に定義することは出来ない。
医療機関で使用される電子カルテシステムは狭義な意味での電子カルテシステムはカルテ記載、診療行為の指示と捉えることができるが、指示受けを行なう看護システムや、部門システムでの治療記録などを含めて電子カルテシステムとして認識されることも多い。

当ガイドラインにおいては病院情報システムの内、カルテ記載及び診療行為の指示の部分と、比較的インシデントが多い指示受けを司る看護機能について電子カルテシステムと定義し、リスク評価を行う。
なお、病院機能評価機構のアクシデント／インシデント事例においては、病院情報システムがマルチベンダー構成になっていることにより、システム間の情報伝達上のエラーや、マスタの不一致によるアクシデント／インシデントの事例が多数示されている。広義な意味での電子カルテシステムは部門システムを含めた病院情報システム全体を電子カルテシステムとして定義することができるが、各ベンダー毎に提供範囲も異なる為、ここでは部門システムを含めた範囲については割愛する。
部門システム連携を含めた患者安全のガイドラインについては「患者安全ガイドライン 〈注射業務編〉」等の個別編にて一部考察を行う。

Ａ－３ 電子カルテシステムのリスク評価

本ガイドラインで定義した電子カルテシステムにおいては患者情報を電子カルテシステム上に記載する日々の経過記録や退院サマリ等の「診療記録アイテム」と診療行為に関する全ての指示を行なうことにより部門システムに診療の指示を伝達する「診療指示アイテム」及び、検査結果や診療画像等の情報を参照する「患者情報参照アイテム」に大きく分類される。
なお、日本国内におけるオーダリングシステム、電子カルテシステムについては当然のごとく実装されているチェック機能、例えば処方オーダにおける投与量チェック、禁忌チェックや、検査結果での異常値での色分けなどについては欧米において診断支援システムとして分類されているため、電子カルテシステムの構成アイテムとして「診断アイテム」として定義する。
また指示受けを行なう看護システムにおいては電子カルテシステム（オーダリングシステム）からの指示を受け取る「指示受けアイテム」と受け取った指示を基に実施を行なう「実施アイテム」として分類する。なお、看護記録、看護計画等についても電子カルテシステムの記録の範疇であるが、リスクを発生しえない観点から省略する。
図Ａ－３－1に電子カルテシステムのソフトウェアアイテムを示す。



図Ａ－３－１ 電子カルテシステムのソフトウェアアイテム分類

電子カルテシステムの機能において「診療記録アイテム」に関しては患者経過を綴ったものであり、ソフトウェア安全クラスに照らし合わせた場合には負傷又は健康被害の可能性はなく、クラスAに分類することができる。

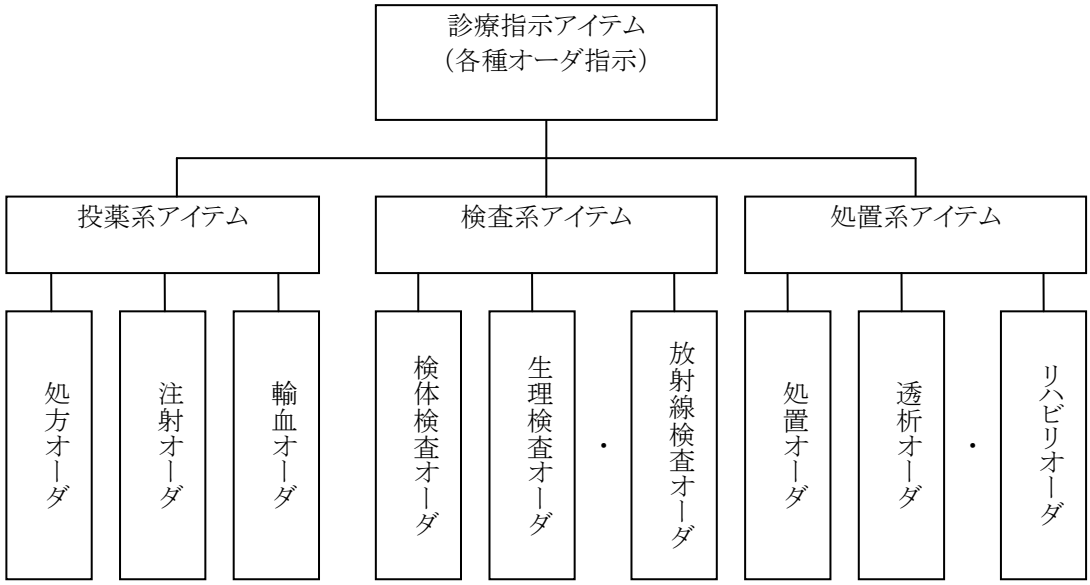
「診療指示アイテム」については診療指示内容により処方、注射、輸血等の「投薬系アイテム」、検体検査や細菌検査、病理検査等の「検体検査アイテム」、放射線検査、生理検査、内視鏡検査のような「生体検査アイテム」等、診療指示アイテムは診療行為の内容に応じて多岐にわたり存在する。

「診療指示アイテム」のうち、「検査系アイテム」に関しては死亡または重傷の可能性のある要因とはなりえずクラスAに分類できる。

「投薬系アイテム」については医師の指示により行為が行なわれることから、過去の医療事故の傾向からもクラスCに分類できる。

また「処置系アイテム」に関しては指示間違いにより患者に影響を及ぼす（不要な処置の実施等）可能性はあり、クラスBに分類することができる。

診療指示アイテムを細かく分類した図を図A－3－2に示す。



図A－3－2　診療指示アイテムの詳細分類

「患者情報参照アイテム」については検査結果の参照、画像レポートの参照等が存在し、電子カルテシステム内に情報を取り込むことも多いが、部門システムの情報を直接参照する場合もある。「患者情報参照アイテム」をソフトウェア安全クラスに照らし合わせた場合には情報の参照のみを行なっている観点ではクラスAとして考えることが可能であるが、表示ソフトウェアが情報を加工している場合においては診断上の誤謬を引き起しかねない場合があり、クラスBまたはクラスCに分類することができる。

以上のような投薬系アイテムがクラスC、及び処置系アイテムがクラスBの分類となることにより最終的な電子カルテシステムのソフトウェアリスク分類はクラスCとなる。

また電子カルテシステムの構成アイテムである「実施アイテム」については指示伝達上の不具合、例えば情報を参照した際にデータ更新が追いついていないことにより古い情報を参照することにより誤った治療行為を行う可能性もあり、ソフトウェア安全クラスにおいてはクラスCとして分類することができるが、マルチベンダー構成であることも多く、正確なデータ連携と最新の情報を留意すべき事項として詳細については「患者安全ガイドライン〈注射業務編〉」にて3点認証を含めたガイドラインを示す。

電子カルテシステムのソフトウェア構成例において、特に「投薬系アイテム」においては処方オーダ機能で2000年及び2008年に「サクシン」と「サクシゾン」の選択誤りによる患者の死亡事故も発生しており、医師の指示誤りとはいえ医師のチェック、看護師、薬剤師のチェックをすり抜けて投薬がなされることにより患者に対して死亡または重傷を引き起こす原因になりうるクラスCの機能である。

処方オーダ機能については2000年、2008年の事故報告を受け、電子カルテシステム開発ベンダーより薬品選択時の3文字検索機能や、薬品選択時のメッセージ表示機能の実装等のガイドラインを提供しているが、注射オーダ機能については幸いにして医療事故の公な報告は無いこともあり、明確なガ

イドラインが提言されていない。

注射オーダ機能は処方オーダ機能に比較し、より直接的に作用し、指示の変更も頻回に発生する。またオーダリングシステム全般の機能として注射オーダ機能は医師の指示が看護システムに伝達され、看護システム上で実施されるものもあり、システム間の連携が発生し、インシデント、アクシデントを発生させうる可能性が比較的高い。

「患者安全ガイドライン＜解説編＞」においてはソフトウェア開発モデルにおいて医療ソフトウェアとして製品を提供、販売、保守するにあたりベンダーが意識しなければいけない項目について記述しているが、医療ソフトウェアにおいては各業務機能毎に重点的に意識して開発しなければいけない項目や、利用者である医療関係者に対して意識して頂かなければならない項目についても一定のガイドラインを策定し、ベンダー側及び医療機関の方々に理解して頂くことにより、安全にシステムを使用して頂けると考える。

業界としては患者様に対して「死亡または重傷の可能性のあるハイリスク機能」についてガイドラインを策定していくことが必須のこととなっている。

付則Ｂ：薬剤部門管理システムのソフトウェア構成例とリスク評価例

医療機関では院内で流通する数多くの薬剤の管理運用を如何に間違いなく実行するかが重要な課題となっている。また、「生物由来製剤」や「麻薬」等については、厚生労働省の通達などで管理運用と記録が要求され、これらの課題・要求をクリアするため、多くの医療機関で薬剤管理システムの導入を行っている。この薬剤管理システムをIEC 62304で定義するソフトウェア安全クラスにあてはめたソフトウェア構成例とリスク評価例を以下に記載する。

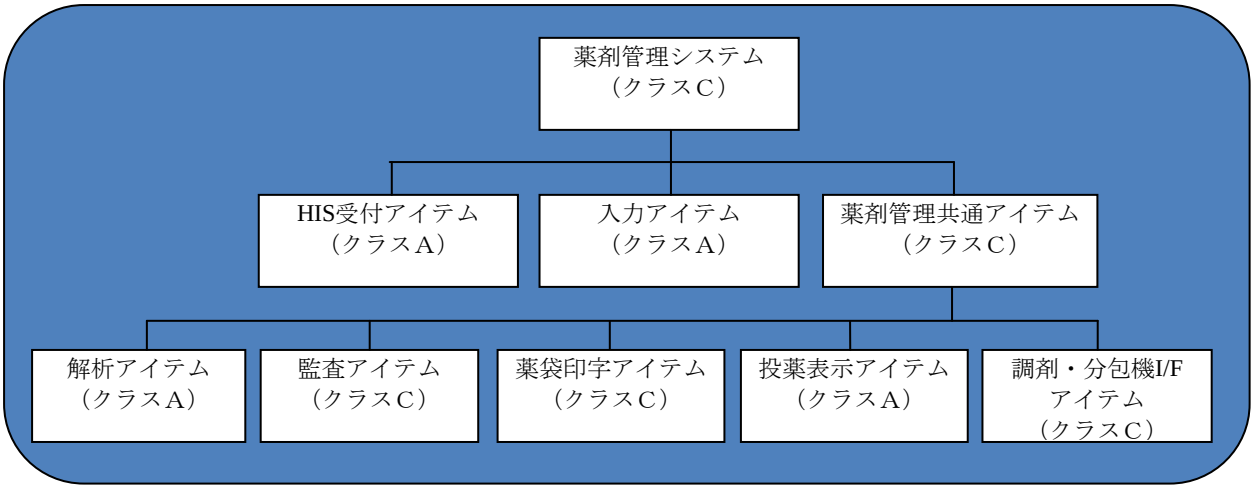
Ｂ－１　薬剤部門管理システムのソフトウェア構成例とリスク評価例

IEC 62304では、ソフトウェアシステムに起因するハザードが患者やユーザ等の人に及ぼす影響のリスクに応じて、ソフトウェアシステムを次の3段階のソフトウェア安全クラスに分類することを求めている。（「第7章　ソフトウェアリスク分類&構成管理」を参照）

（1）　クラスA：負傷又は健康被害の可能性がない
（2）　クラスB：重傷の可能性はない
（3）　クラスC：死亡又は重傷の可能性がある

薬剤管理システムは、HIS（Hospital Information System：病院情報システム。以下、HISと記す）、及び薬剤管理システムを使用して患者へ投与する薬剤情報を受付しその情報の管理を実現しているが、ここでは薬剤管理システムの一部に関しソフトウェアアイテム構成例と分割例を記載する。

患者へ投与する薬剤情報の受付窓口である2つの機能を「HIS受付アイテム」、「入力アイテム」と定義する。この2つのアイテムは何れも患者への薬剤投与情報を内部的に管理・保存する「解析アイテム」、患者への投与に際し禁忌等の各種監査機能を行う「監査アイテム」、服用方法等の薬袋情報を印字する「薬袋印字アイテム」、患者への薬剤情報の受け取りを促す「投薬表示アイテム」、患者の服用に合わせて調剤・分包を行うシステムとのインターフェースを行う「調剤・分包機I/Fアイテム」と言う5つのソフトウェアアイテムを共有する。これらのソフトウェアアイテムが有する機能をソフトウェア安全クラスに照らし合わせた場合、死亡又は重傷を引き起こす可能性のあるハザードの要因となるクラスCのソフトウェアアイテムは、システム間の情報伝達エラーやマスタ不一致によるアクシデント／インシデントを招く可能性の高い「監査アイテム」、「薬袋印字アイテム」、「調剤・分包機I/Fアイテム」となり、「解析アイテム」、「投薬表示アイテム」は負傷又は健康被害の可能性がないクラスAに位置付けることが出来る。これら5つのソフトウェアアイテムから構成される中間的なソフトウェアアイテムである「薬剤管理共通アイテム」は、より重大なソフトウェア安全クラス分類であるクラスCに分類される。また、薬剤情報の受付窓口である「HIS受付アイテム」、「入力アイテム」は、受付のみの機能であるため負傷又は健康被害の可能性がないクラスAに分類される。当然、最終的な薬剤管理システムはクラスCとなる。以下に上記で分割した薬剤部門管理システムのソフトウェアアイテム構成例を図Ｂ－１－１に示す。



図Ｂ－１－１　薬剤部門管理システムのソフトウェアアイテム構成例

解熱剤と間違って筋弛緩剤を投与した例にもある通り、人やシステムは誤りうるし、誤る物と考えるべきである。個々のシステムは相互に関連しており発生した事故は切り離して修復することが出来なく、プロセスの安全性を保つことは難しい。各システムに於いて、事故が顕在化する前にハザードに対する予見的な対策をとる必要性の観点からガイドラインを策定していく必要がある。

付則Ｃ：ＩＥＣ62366ユーザビリティ仕様へのインプット例

9章で述べたように、ユーザビリティエンジニアリングには3つのステップがあるが、ここではその第一ステップであるユーザビリティ仕様へのインプットを取り上げ、検討項目の置き換え例として、医療機器の電子体温計と医療情報システムの注射オーダ発行業務を対比した形で示す。

	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“での定義（電子体温計）	医療情報システムでの置き換え検討（注射オーダ発行業務）
1-1	医療機器の用途	医療情報システムの用途
(1)	意図する医学的適用: 人の身体温度を口または直腸の中で測定する。診断する病気:熱、低体温	意図する情報システムの目的: 医師が、注射の指示を行うための入力を行う。
(2)	意図する患者集団: 年齢:新生児から老人まで 体重:＞2．5Kg 健康状態:関係無し 国籍:問わない 患者の状態:患者が使用者の場合、注意を怠らない。患者が使用者で無い場合、関係なし	意図する患者および情報の範囲: 患者の年齢:新生児から老人まで。 患者の状態:疾患を患っており、意識がない場合もある。また、患者が薬剤に関してアレルギーを持っている場合がある。
(3)	適用する又は対応する、意図された体の部位または組織の種類: 測定場所:口、直腸 状態:傷の無い皮膚	適用する又は対応する、意図された体の部位または組織の種類: 投与経路:皮内注射、皮下注射、筋肉内注射 静脈内注射　等
(4)	意図するユーザプロファイル: 教育:少なくとも１１歳から5年間の学校教育、 知識:最低限数字の読み書きができる。口、鼻、直腸の区別ができる 言語の理解;指定の言語 経験:15歳未満の場合監督訓練、15歳以上なら特別な経験不要 容認できる障害:視力0.2以上etc…	意図するユーザプロファイル: 教育:医学部での教育を受けた医師あるいは研修医。 知識:注射薬の効能、危険性を熟知している。
(5)	意図する使用条件: 環境: 一般:家庭用途、屋内用、シャワー浴槽では使用しない。 視認性:輝度100ルクス～1500ルクス 使用頻度:年1回～1日10回 物理的:温度10℃～30℃、湿度、気圧の範囲	意図する使用条件: 環境:病院の外来診療室、外来処置室、入院のナースステーションあるいは医局。
(6)	操作の原則: 特になし	操作の原則: 操作者のID等でログインを行い、患者を選択した後、当該患者に必要な注射薬の指示を行う。指示としては、薬品名、ルートを含む用法、用量、注入速度等を入力する。重複指示や配合禁忌・相互作用等を自動的にチェックし、システムからの警告も含めて、画面で入力情報を確認後、オーダ内容を発行する。
	・・・・・	その他必要な記載があれば追記
1-2	使用頻度の高い機能:	使用頻度の高い機能:

	保護カバーをはずす 機器を口または直腸の正しい位置に入れる 測定完了した情報をみつける 表示を読む 洗浄する 機器をつかむ 機器を取り出す スイッチをオフにする。 保護カバーを元に戻す 保管する	患者選択。 注射オーダメニューの選択 新規注射オーダ指示 過去注射オーダを利用した再発行
1-3	ユーザビリティに関連するハザード及び危険状態の特定	ユーザビリティに関連するハザード及び危険状態の特定
(1)	安全に関係する特性の特定: 保護カバーのとりはずし 機器を口または直腸の正しい位置に入れる 測定完了した情報をみつける 表示を読む 洗浄 バッテリを交換する	安全に関係する特性の特定: 患者のアレルギーと注射薬のチェック 現在投与している他の注射薬との相互作用チェック 現在服用している処方薬との相互作用チェック 患者病名と注射薬との病名禁忌チェック 注射薬の極量チェック 注射薬の注入速度チェック 麻薬・毒薬類の表示明確化
(2)	既知の又は予測可能なハザード及び危険状態の特定: 正常使用時:バッテリ切れで表示が無い。 使用ミス:種類の異なるバッテリの装着 過剰な力を加える さかさまにして機器を持つ 測定範囲の読み間違い 高温の環境等	既知の又は予測可能なハザード及び危険状態の特定: 注射薬の選択ミス 他の注射薬との相互作用のチェック見過ごし 注射薬の極量のチェック見過ごし 注射薬の注入速度の指示誤り 麻薬・毒薬類の扱い時の注意喚起 注射器、注射針の未交換
(3)	もたらされる危険状態および危害:	もたらされる危険状態および危害: 投与薬品、投与量、投与方法等のミスにより患者に重篤な障害を引き起こす。最悪死亡事故となる。
1-4	主操作機能: 主操作機能には使用頻度の高い機能、安全に関係する機能を含めなければならない、	主操作機能: 患者選択。 注射オーダメニューの選択 新規注射オーダ指示 過去注射オーダを利用した再発行 注射薬の選択時のミス防止機能:薬品名に薬効を記載 注射薬と患者アレルギーとのチェック機能 注射薬の極量、注入速度等のチェック機能 特に小児に対しては投与量のチェックが重要。 他の注射薬との相互作用チェック機能

付則Ｄ：ＩＥＣ/ＴＲ80002-1のAnnex_C

表Ｄ－１に、リスクマネジメント活動（ISO14971:2007による）及びソフトウェアライフサイクル(IEC62304:2006による)活動において避けるべきソフトウェア関連の潜在的落とし穴を示す。

表D－1 IEC62304:2006 IEC62304条項におけるソフトウェア関係の潜在的落とし穴

ISO 14971:2007 ４章：リスク分析

–非現実的でほとんど起こらないようなことまでソフトウェアの不具合の見積りに入れることにより、非現実的なリスクレーティングの結果を得、そのために不適当なリスク管理策をとること。
–新たなハザードや危険な状態若しくは危険の原因が医療機器に加わったかどうか、又は、現在とられているリスク管理策で折り合うものであるかどうか（開発当初からあるもの、保守の一環としてリリース後に追加されたものの双方を含む）を決定するためのリスク分析を行わずに、ソフトウェアに機能を追加する。
–医療機器のリスク分析方法において、システムとハードウェアのレベル面からしか定義しておらず、ソフトウェアとの関係を適切に取り扱い妥当なリスク分析を行ったり、特にソフトウェアの不具合をハザード若しくは危険な状態の潜在的原因として考慮することを求めたりしていない。
–過度に厳しいリスク分析とソフトウェア開発ライフサイクル手順のために、医療機器に対する潜在的脅威に対応できていない

ISO 14971:2007 4.1項：リスク分析手順

–リスク分析方法が、システムとハードウェアのレベル面からしか定義されていない。ソフトウェアは、ハードウェア不具合に対するリスク管理策の実装という点でのみ取り扱われている。
–過度に厳しいリスク分析とソフトウェア開発ライフサイクル手順のために、医療機器に対する潜在的脅威に対応できていない。
–ソフトウェアがリスク分析の一環として考慮されるのが、製品開発ライフサイクルの終盤でしかない。

ISO 14971:2007 4.2項：使用目的の特定

–ユーザ環境および潜在的に存在するコンピュータシステムのプラットフォームだけを考慮すること。
–プラットフォームの改訂や、セキュリティの必要性、その他のSOUPのパッチは考慮しないこと。
–ユーザの誤用およびユーザの間違いの結果として発生する潜在的ハザードおよびこれに対応するリスクコントロール手段を不適切に考慮すること。

ISO 14971:2007 4.3項：ハザードの特定

FMEAかFTA手法を、それだけで十分であるかの様にリスクマネジメントに使用すること。
– FMEAかFTAの手法を、ハードウェアとソフトウェアで分離して実行すること。
–以下の様な全体のクラスのハザードと原因を無視すること：
  –予測できない影響があるソフトウェアエラー
  –ハードウェア障害を測定しリスクコントロールする為に使用されるソフト・ロジックのエラー
  – 医療機器の意図している臨床目的のためのソフト・ロジックにおけるエラー(結果計算のためのアルゴリズム等)
  –ソフトウェアプラットフォームのエラー　－　オペレーションシステム、ライブラリ、SOUP
  –コンピュータの部品と周辺機器のエラー
  –通信用インターフェースのエラー
  –ヒューマンファクタ
–以下の思い込みで、原因の特定にアプローチすること：
  –ソフトウェアの欠陥は特定のコンポーネントの機能性に影響するだけであり、他のソフトウェアアイテムやデータに副作用を持たない。
  –ソフトウェアは適切に動作する。
  –潜在的な（識別、検出、やりスク制御に使用される）ソフトウェアのエラーは、多数過ぎて予測不能である。
  －リスク制御の最初と最後にリスクを測定することで、リスク管理は十分である。

表D－1 IEC62304:2006 IEC62304条項におけるソフトウェア関係の潜在的落とし穴（続き）

ISO 14971:2007 4.4項:リスクの推定
–単一欠陥条件の概念がソフトウェア設計と事象の連鎖に適用されると仮定。 –テスト（それは徹底的にできるわけではないが）が個々の失敗の確率をゼロまで減少させると仮定すること。 –機能として、あるソフトウェア項目が、予期していない副次的影響の可能性を考慮せずに関連した項目が安全ではないものと仮定すること。 –適切な臨床知識あるいは全ての考えられる利用者や対象となる人々へのハザードの影響に対する臨床知識（ヒューマンファクタ）をもった関与なしに重篤度を割り当てること。 –臨床医が欠陥や間違った情報を検出するだろという仮定に基づく低い重篤度を割り当てること。 –すべての利用者が医療機器の注意ラベルや取扱説明書に正確にあるいは不注意による間違いなしに従うと仮定することにより低い重篤度を仮定すること。 –初期に未知のものとした部分に対してなんらかの前もって定めたリスクコントロール手段を仮定すること。もし、その仮定が間違っていると、初期の低い重篤度により不適切なリスクコントロールとして後で特定されことになるかもしれない。 –ソフトウェアによって利用者に提供された情報の間接的な利用、治療の遅れおよび医療機器の有効性や不可欠な性能に関連した他のファクターを考慮しないで、直接的な患者への危害の可能性のみを重篤度を特定するために使用すること。 –臨床医が常にソフトウェアが提供した情報をクロスチェックするであろう、あるいは誤情報を検出できるであろうと仮定し、低い重篤度を割り当て且つ他のリスクコントロール手段を実装しないことにすること。
ISO 14971:2007　５項：リスク評価
–ソフトウェア異常へ主観的確率を用いて、リスクコントロール手段が不要だと判断する。 –ハードウェア特性から推してソフトウェアによるハザードを除外し、後でそのハードウェアの変更又は取り外しを行ったために、ソフトウェアが潜在的なハザードの要因となり、ソフトウェア用のリスクコントロール手段の追加を検討しないこと。 –ソフトウェアが所定どおりに動くか、又は試験ですべての異常(ANOMALIES)が把握されると仮定しているためにハザードの要因としての潜在的ソフトウェア異常(ANOMALY)について検討しない。
ISO 14971:2007 6.3項：リスクコントロール手段の実装
– 通常の又は限定された条件下でリスクコントロール手段の検証を行っているが、幅広い異常な条件下での検証は行っていない。 – リスクコントロール手段の実施に用いるソフトウェア又はデータは、他のソフトウェアが簡単にアクセスできるコンポーネント又は場所にあり、危険な副次的影響の可能性を高くしている。 – リスクコントロール手段は、一つのオペレーティングプラットフォーム又はプログラムバリアント上でだけで検証を行っている。 –強制的発生させることがむずかしために、実際の検証を行っていないリスクコントロール手段がある (メモリ故障、競合条件、データ破損、スタックオーバフローなど)。 –すべての安全関連異常 (ANOMALIES)は開発中に発見され、試験によって、現場では適切に動作すると保証されると仮定する。 – ソフトウェア設計を著しく複雑なものにするリスクコントロール手段の実施。この複雑さは、ソフトウェア異常が付加される可能性を高めたり、新たなハザードを引き起こしたりする。
ISO 14971:2007　５章：製造後の作業に関する情報について
–追加のリスクコントロール手法を導入時に、潜在的に危険なフィールドイベントを無視すると、失策を犯す –初期の確率と重篤度推定を仮定することは、フィールドの情報を評価しないことに等しい。 –医療機器の通常の使い方以外にも、想定外の使い方についても考慮しなければ、リスクコントロール方法が不十分だった事を指すかもしれません。例えばHIVテストでのIVD（体外診断）は個人使用を想定されていましたが、（IVDは、）献血のスクリーニングにも使用されるようになりました。

表D－1 IEC62304:2006 IEC62304条項におけるソフトウェア関係の潜在的落とし穴(続き)

IEC 62304:2006 5.1項：ソフトウェア開発計画
–リスクマネジメントアクティビティが、ソフトウェア計画とライフサイクルプロセスの中で確立されていない。 –ソフトウェアリスクマネジメントアクティビティが、医療機器リスクマネジメント全体のアクティビティと関連していない。 – ソフトウェアのリスク評価が、ライフサイクルの中で唯ひとつの段階でのみ為されている。 –ソフトウェアの開発者と試験者が、リスクマネジメントについて訓練されていないし、経験もない。 –ソフトウェアリスクマネジメントは、一般的なリスクマネジメントアクティビティでカバーされていると、思い込んでいる。 –ソフトウェアリスクが、統制がとれた方法で管理されていない。 –安全性決定のトレーサビリティが、確立されていない。
IEC 62304:2006　開発過程が不明なソフトウェア(SOUP)問題
–本来安全に設計されたリスクコントロール手段が、ソフトウェアアーキテクチャを定義する時にリスク評価と統制を考慮しないことによって、失われた。 –試験は、無益なアーキテクチャを十分に安全にすると、思い込んでいる。 –アーキテクチャ要素が連続的に変更されるか削除される時の安全性リスクを知らない結果、アーキテクチャの側面に関連する係る安全を確認することに失敗する。
IEC 62304:2006 5.4項：ソフトウェア詳細設計
–エラーチェックの多重レベルの組み込みよりむしろ、コンポーネント間のインターフェースや受け渡しパラメータが正しいと仮定し正常ケースのみを扱うことに注目すること –詳細設計の後工程でのレビューと同様ブレーンストーミングを通じてハザードやハザード状態およびリスクコントロール手段に関連する潜在的なソフトウェア障害の識別をしないこと –リスク管理活動でのソフトウェア障害の原因(AnnexBを参照)を無視すること
IEC 62304:2006 5.5項：ソフトウェアユニット実装と検証
–最上のコーディングやテスト工程、手法、ツールや作業者が、貧弱で本質的に安全でなく、あるいは過度に複雑な設計を補うと信じること –重要コード開発に未経験な開発者を使うこと –特殊な防御プログラミング手法を定義し要求することの失敗 –特に重要なコンポーネントに対してコードレビューあるいは静的なコード解析をしないで、もっぱら動的テストを信頼すること –リスク管理に対する設計要件の妥当性を理解しない設計からの逸脱 –開発プロセスの早期で一度のみ重要コンポーネントの単体テストを行い、レグレッションテストの一部分として繰り返さない –もっぱら動的でブラックボックス、システムレベルの技法のテストに注目して、静的ホワイトボックス検証と動的ホワイトボックス検証を行わない
IEC 62304:2006 5.6 - 5.7項：ソフトウェア統合、統合テスト、システムのテスト
–リスクアセスメントの情報をテスト計画の策定やテスト担当者の教育に使用しないこと –リスク管理策としてテストに依存すること　－　100%のテストは不可能であるにもかかわらず。 –リスク管理策を検証するためのテストの一部としてシステムやソフトの故障モードをシミュレートしないこと。 –規定、制御されておらず結果も信頼できないテストに対して自動化されたツールを使うこと。 –テストでは発見できない「異常」を検出するためのコードの適切な分析をしないこと。

表D－1 IEC62304:2006 IEC62304条項におけるソフトウェア関係の潜在的落とし穴（続き）

IEC 62304:2006 5.8項：ソフトウェア　リリース
–リリースされたソフトウェアの取り決めの中に、リリースされたドキュメントのバージョンを盛り込んでおくことをしないと、　開発やテストチームが将来リリースする製品を誤った方向に導いてしまうかもしれない。リスクコントロール基準を使わなかったり、安全性に関連したソフトウェアを十分に検証しなかったりすると、不正確なドキュメントやトレーサビリティが原因で関連付けの欠落や危険を見落とすことにもなりかねない。 –それらのもの（リスクコントロール基準や安全性に関連したソフトウェアの検証を指す？）を未だ残っている例外の評価に関する適切な診断知識として取り込まないこと。 –残存している例外の重要性の評価が、その対象とする例外が、あらゆる起こりうることを判断するための完璧な根本分析に基づいた例外ではなくただ機能的な症状に関して基づいたものである場合には、ある条件下で影響を与える。 –サードパーティーが、ある特別なSOUPバージョンを配布していないという事実を一度でも見落としてしまうと、そのバージョンはエラー調査や現場での修正には適用されないだろう。 –　（コンパイラのような）ある特定のツールやツールのバージョンは保存されてこなかったので、ある特定のソフトウェアのバージョンを作り上げる能力は失われてしまった。 –医療機器の寿命は現在の保存媒体よりも長いかもしれない。製造者は古い媒体を新しいものにリプレイスしていくのだから、製造者は古い保存データを新しい媒体に移行する道筋を計画するべきである。
IEC 62304:2006 6.1項：ソフトウェアメンテナンス計画の確立
–変化に対するリスクマネジメントに明確なアプローチをもたないメンテナンスプロセスを確立してしまうこと。 –変化の機能的な面のみを重視してしまい、リスクに関連したリスクに影響を受けるような構成要素になっていないリスクマネジメントを確立してしまうこと。
IEC 62304:2006 6.2 - 6.3項：問題および修正の分析ならびに実装
–小さな機能的な修正は安全性に影響しないと仮定すること –医療機器の用途を、あらたな対象層、新たな疾患の検出、新たなユーザ（例えば外科医に代わる看護師）、あるいは既存のリスク管理策やユーザインターフェースの適切さをの再検討を行っていない新プラットフォームに拡張すること。 –根本的な原因や潜在的な副作用を特定せずに、問題の報告された兆候に基づいて問題解決のリソースの優先度を設定する事。 –診療用途以外（例えば会計）向けに設計され、診療目的で配付される診療データを含み、適切なリスク管理がおこなわれていないソフトウェア。

付則Ｅ：ＩＥＣ80001-1

Application of risk management for IT-networks incorporating medical devices
医療機器を組み込んだITネットワークへのリスクマネジメント適用

近年、ユーザ環境に設置された他の医療機器や医療機器以外の機器と情報を交換する医療機器が増えている。また、この情報交換は、通常のITネットワークを介して行われることが多い。医療機器に関しては、患者を危害から保護するためいろいろな規制で監視されているが、医療機器をITネットワークに接続することによる安全性、有効性、データ及びシステムセキュリティ（以下、この3つを基本特性という）の面の影響については考えられていない。このため、この規格に従って総合的なリスクマネジメントを行うことが、ユーザの責任組織や医療機器製造業者やITプロバイダに求められている。

E.1 概要

1) 目的
- 医療機器がITネットワークに組み込まれて使用される環境でのリスクマネジメントに必要な役割、責任やプロセスを定義している。許容できるリスクについて定めるものではない。

2) 適用範囲
- 医療機器を組み込んだITネットワークのライフサイクル全般に適用される。
- 総合的なリスクマネジメントを行うために、ユーザの責任組織や医療機器製造業者やITプロバイダに適用される。ただし、患者、操作者、責任組織が、同じ人であるような、個人向けのアプリケーションには適用されない。
- 規制や法的な要求を示すものではない。

E.2 役割と責任

医療ネットワークへの機器やソフトの追加や変更については、明確に責任が定義された組織のもとで実施されなければならない。この責任組織は、全てのリスクマネジメントに対して責任を負う。また、この規格で要求されているドキュメントは全て、医療ITネットワークマネジメントファイルで管理・維持されなければならない。

図E-1は、関連ステークホルダとその間の情報の流れの関係を示すものである。

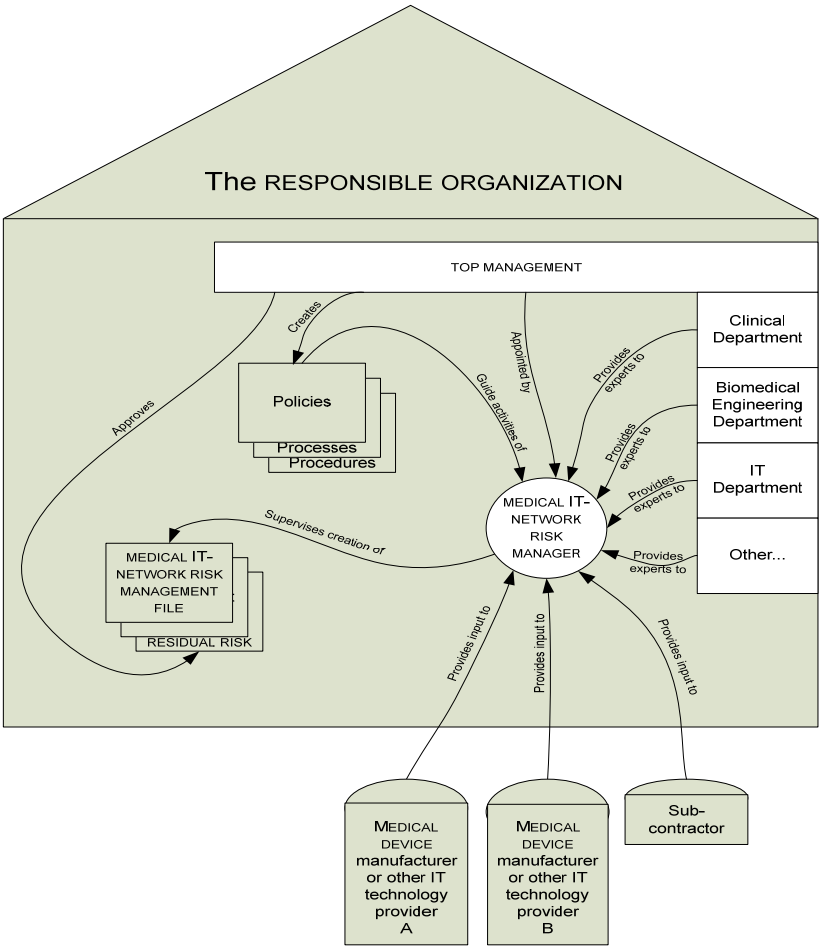
主なステークホルダとしては、トップマネジメント、医療ITネットワークリスク管理者、医療機器製造業者、ITプロバイダを想定している。

E.3 主なステークホルダの役割

1) トップマネジメント
- リスクマネジメントポリシーの確立
- 3つの基本特性(安全性、有効性、データ及びシステムセキュリティ)の配分ポリシーの定義および管理、実行、査定に対する適切な人の配置。
- 医療用ITネットワークリスク管理者の任命。
- リスクマネジメント活動の定期的な見直し　等。

2) 医療ITネットワークリスク管理者
- リスクマネジメントプロセスの全体管理、設計、維持、実行の責任、トップマネジメントへの報告。
- リスクマネジメントの関係者間の意思疎通の管理。

3) 医療機器製造業者
- 使用目的や安全的・効果的な使用方法が記載された附属文書を責任組織に提供。
- ITネットワークに接続する医療機器の使用目的。
- 医療機器を組み込むITネットワークの要求性能、要求構成の情報提供。
- セキュリティ仕様を含んだ医療機器へのネットワーク接続の技術仕様提示。
- 医療ITネットワーク上の医療機器と他の機器間の情報伝達の流れ。
- 責任組織から要求のある付加的資料の提供。（ITベンダーも同様に情報提供の責任）



図E-1　役割と関係の全体図

E.4　医療ITネットワークのライフサイクルリスクマネジメント

- 責任組織は、医療ITネットワークの基本的な管理を、ライフサイクルを通して維持しなければならない。

E.5　責任組織のリスクマネジメント

- トップマネジメントが、リスクマネジメントポリシーを確立すること。
- 医療ITネットワークマネージャは、ハザードの認識、関連リスクの推定と評価、リスク制御、とその効果の監視につき、プロセスの構築と維持を行うこと。

E.6　医療ITネットワークの計画と文書

- 責任組織は以下を考慮してリスクマネジメントを計画する。
  - リスク関連資産(ネットワーク構成要素、ITインフラの特性、患者個人データ等)の記述。
  - ITネットワーク構造(物理的・論理的構成、セキュリティ、信頼性等)を示した文書。
  - 利害関係者間において責任協定で責任の明確化(新規追加、変更を含む)。
  - 医療ITネットワークの目的や、関係部門の役割責任、ITネットワークの監視、許容リスク基準等を含んだリスクマネジメントを計画。

E.7　変更適用管理と構成管理

- 変更適用管理は、全ての変更が管理された方法を用いて、査定・承認・実行・評価のプロセスで行うことが必要。また、そのバージョンを管理するため、構成管理を文書化する必要がある。
- リスク解析により、ハザードを認識し、関係あるリスクを推定し、リスク評価を行わなければなら

ない。
- 許容できないリスクに対しては、許容できるレベルになるまでリスク制御できる手段を特定し文書化し、リスク制御手段を実行する。
- 医療ITネットワークを新設したり、変更したり、そのネットワークに医療機器を入れたり、外したり、新しいリスクとなりそうな活動が発生する場合、責任組織はプロジェクト計画を作成し、運用する前に、責任組織が医療ITネットワークの残存リスクを再評価しなければならない。

E.8 運用中ネットワークのリスクマネジメント
- 責任組織は、初期段階のリスク、リスク制御手段の効果、当初のリスクレベル推定の確かさを監視するためのプロセスを確立しなければならない。
- リスクの上昇が観測されたなら、良くない事象を捉え、文書化し、変更適用管理手順に従い問題解決のための修正や予防処置を行い、報告をしなければならない。

E.9 ドキュメント管理
- 医療ITネットワークのライフサイクルにおける全てのドキュメントは、正式な手順により、改訂、修正、査閲、承認されなければならない。
- この規定における対応は、全て医療ITネットワークリスクマネージメントファイルに保存され、各々のハザードに対して、リスク解析、リスク評価、リスク制御手段の実行と確認、及び許容な残存リスクの受容性の査定についてトレーサビリティを備えていなければならない。

この国際標準規格案に付属するガイダンスIEC80001-2-XXとして、
- Guidance for HDOs (Healthcare Delivery Organizations)
- Step-by-step risk management with examples
- Guidance for wireless networking
- Guidance for specifying security requirements

の四つのガイダンス策定が進められている。

付録：作成者名簿

作成者（五十音順）

天野　敦之	オリンパスメディカルシステムズ㈱
岡田　真一	日本電気㈱
片倉　由紀子	富士フイルム㈱
喜多　紘一	一般社団法人保健医療福祉情報安全管理適合性評価協会
中島　隆	富士フイルム㈱
野津　勤	㈱システム計画研究所
野々村　辰彦	富士通㈱
箱田　章	㈱シーエスアイ
橋詰　明英	㈱日立製作所
長谷川　茂男	ベックマン・コールター・バイオメディカル㈱
平井　正明	日本光電工業㈱
茗原　秀幸	三菱電機㈱
山口　一人	富士通㈱
吉村　仁	コニカミノルタエムジー㈱

改定履歴		
日付	バージョン	内容
2010/9/●	Ver. 1.0	初版

（JAHIS技術文書　10-101）
2010年9月発行

～ＪＡＨＩＳ医療情報システムの患者安全に関する
リスクマネジメントガイドライン＜解説編＞～

発行元 保健医療福祉システム工業会
〒105-0001 東京都港区虎ノ門1丁目19－9
（虎ノ門TBビル6F）
電話　03-3506-8010　　FAX　03-3506-8070