# 基本要件改正への対応

## ～サイバーセキュリティ等～

一般社団法人　日本画像医療システム工業会
シニアリサーチャー（医療機器規制）
古川　浩

修

# 説明の概要

Ⅰ．基本要件基準 第12条第３項の追加
Ⅱ．医療機器の基準等
Ⅲ．医療機器のサイバーセキュリティ対応
Ⅳ．基本要件基準第12条第３項の適合について
Ⅴ．ユーザビリティ
Ⅵ．医療機関のサイバーセキュリティ対応
Ⅶ．参考

※
・当日説明資料(12/01）を修正等した頁の右肩に表示
・追加した頁　：　追
・一部修正した頁：　修

# Ⅰ．基本要件基準
# 第12条第３項の追加

１）基本要件基準　第12条第3項追加改正

２）基本要件基準　第１２条　（プログラムを用いた医療機器に対する配慮）

# １）基本要件基準　第12条第3項追加改正

令和5年 3月9日　厚生労働省告示第67号

＜薬機法＞第41条第3項の規定に基づき・・・厚生労働大臣が定める医療機器の基準・・・を改正し、令和5年4月1日から適用する。
ただし・・・令和6年4月1日までの間・・・従前の例によることができることとする。

（プログラムを用いた医療機器に対する配慮）

第12条　（略）

2　（略）

3　プログラムを用いた医療機器のうち、他の機器及びネットワーク等と接続して使用する医療機器又は外部からの不正アクセス及び攻撃アクセス等が想定される医療機器については、当該医療機器における動作環境及びネットワークの使用環境等を踏まえて適切な要件を特定し、当該医療機器の機能に支障が生じる又は安全性の懸念が生じるサイバーセキュリティに係る危険性を特定及び評価するとともに、当該危険性が低減する管理が行われていなければならない。また、当該医療機器は、当該医療機器のライフサイクルの全てにおいて、サイバーセキュリティを確保するための計画に基づいて設計及び製造されていなければならない。

基本要件基準へサイバーセキュリティ対応が第１２条第３項として追加された。
適用：令和５年４月１日　（経過措置期間　１年間）

# ２）基本要件基準　第１２条　（プログラムを用いた医療機器に対する配慮）

第12条　プログラムを用いた医療機器（医療機器プログラム又はこれを記録した記録媒体たる医療機器を含む。以下同じ。）は、その使用目的に照らし、システムの再現性、信頼性及び性能が確保されるよう設計されていなければならない。また、システムに一つでも故障が発生した場合、当該故障から生じる可能性がある危険性を、合理的に実行可能な限り除去又は低減できるよう、適切な手段が講じられていなければならない。

２　プログラムを用いた医療機器については、最新の技術に基づく開発のライフサイクル、リスクマネジメント並びに当該医療機器を適切に動作させるための確認及び検証の方法を考慮し、その品質及び性能についての検証が実施されていなければならない。

３　プログラムを用いた医療機器のうち、他の機器及びネットワーク等と接続して使用する医療機器又は外部からの不正アクセス及び攻撃アクセス等が想定される医療機器については、当該医療機器における動作環境及びネットワークの使用環境等を踏まえて適切な要件を特定し、当該医療機器の機能に支障が生じる又は安全性の懸念が生じるサイバーセキュリティに係る危険性を特定及び評価するとともに、当該危険性が低減する管理が行われていなければならない。また、当該医療機器は、当該医療機器のライフサイクルの全てにおいて、サイバーセキュリティを確保するための計画に基づいて設計及び製造されていなければならない。

注

１：第12条第2項は、医療機器プログラムは平成26年12月25日から、他の機器は平成29年11月25日から適合が必須

２：第12条第３項は、令和６年４月１日から適合が必須

# Ⅱ．医療機器の基準等

１）医療機器に設けられた基準

ア：医療機器の基準（基本要件基準）

イ：42条基準

ウ：承認基準

エ：認証基準：

参考

・承認ガイドライン

・審査ポイント

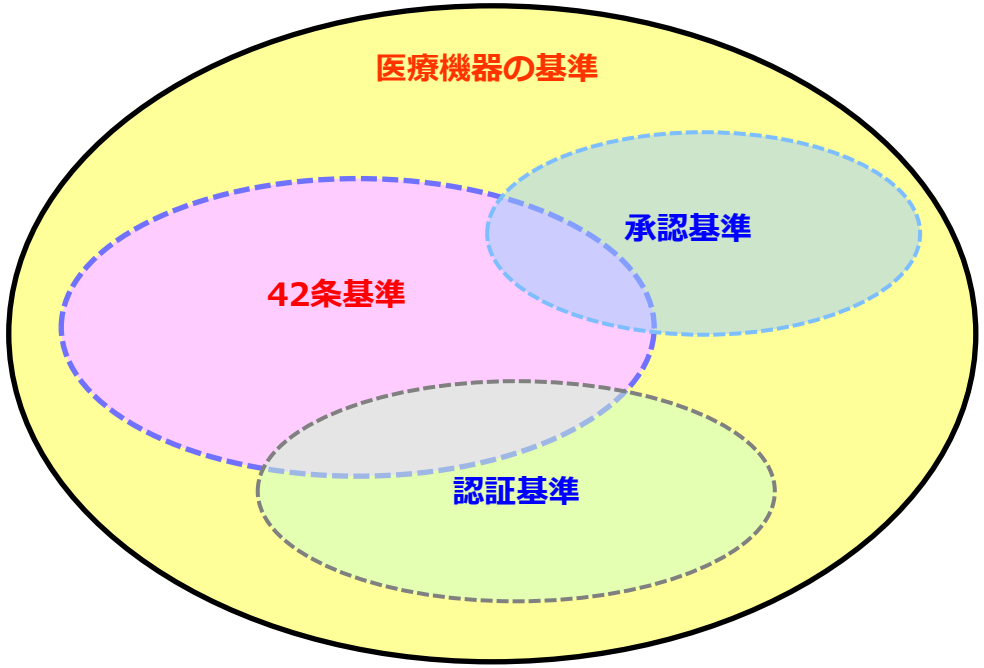
# １）医療機器に設けられた基準

ア：医療機器の基準（基本要件基準）：すべての医療機器
　薬機法第41条第3項の規定に基づく。(告示)

イ：42条基準：該当する医療機器
　薬機法第42条第2項の規定に基づく。（告示： 8基準 ）

ウ：承認基準：適合するものとして承認申請する医療機器
　薬機法関係手数料令第7条の規定に基づく。（通知：44基準）

エ：認証基準：適合するものとして認証申請する医療機器
　薬機法第23条の2の23第１項の規定に基づく。(告示： 951基準）




参考
・承認ガイドライン（10件）、
・審査ポイント（5件）

# ア：医療機器の基準（基本要件基準）

**薬機法第４１条**

３厚生労働大臣は、医療機器、再生医療等製品又は体外診断用医薬品の性状、品質及び性能の適正を図るため、薬事・食品衛生審議会の意見を聴いて、必要な基準を設けることができる。

**厚生労働省告示第122号**

薬機法（昭和35年法律第145号）第41条第３項の規定に基づき、薬機法第41条第３項の規定により厚生労働大臣が定める医療機器の基準を次のように定め、平成17年４月１日より適用する。

平成17年３月29日
厚生労働大臣 尾辻 秀久

医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律第41条第3項の規定により厚生労働大臣が定める医療機器の基準（基本要件基準）

**第１章　一般的要求事項**
- 第１条　設計
- 第２条　リスクマネジメント
- 第３条　医療機器の性能及び機能
- 第４条　製品の有効期間又は耐用期間
- 第５条　輸送及び保管等
- 第６条　医療機器の有効性

**第２章　設計及び製造要求事項**
- 第７条　医療機器の化学的特性等
- 第８条　微生物汚染等の防止
- 第９条　使用環境に対する配慮
- 第10条　測定又は診断機能に対する配慮
- 第11条　放射線に対する防御
- 第12条　プログラムを用いた医療機器に対する配慮
- 第13条　能動型医療機器及び当該能動型医療機器に接続された医療機器に対する配慮
- 第14条　機械的危険性に対する配慮
- 第15条　エネルギー又は物質を供給する医療機器に対する配慮
- 第16条　一般使用者が使用することを意図した医療機器に対する配慮
- 第17条　添付文書等による使用者への情報提供
- 第18条　性能評価及び臨床試験

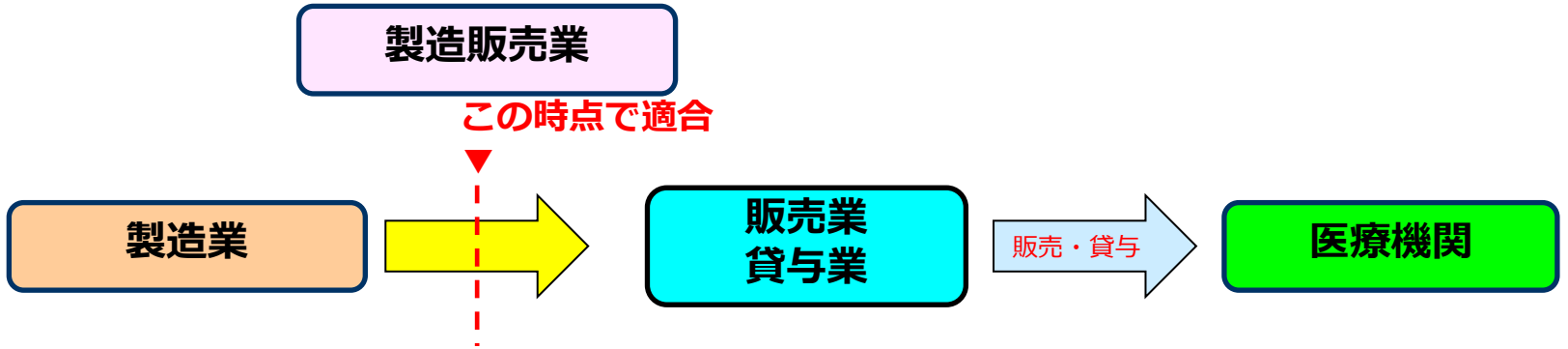
医療機器共通の概念

一般的名称ごと

一般的名称ごと

# ※　基準等への適合が求められるポイント

● 認証品における規格適合は、製造販売時　　なお、販売業での在庫品や、中古品への適用しない
（製造販売業者における出荷判定時）




薬機法

（販売、製造等の禁止）

第65条　次の各号のいずれかに該当する医療機器は、販売し、貸与し、授与し、若しくは販売、貸与若しくは授与の目的で製造し、輸入し、貯蔵し、若しくは陳列し、又は医療機器プログラムにあつては電気通信回線を通じて提供してはならない。

一　第41条第3項の規定によりその基準が定められた医療機器であつて、その性状、品質又は性能がその基準に適合しないもの

基本要件基準

(リスクマネジメント)

第二条 医療機器の設計及び製造に係る製造販売業者又は製造業者(以下「製造販売業者等」という。)は、最新の技術に立脚して医療機器の安全性を確保しなければならない。危険性の低減が要求される場合、製造販売業者等は各危害についての残存する危険性が許容される範囲内にあると判断されるように危険性を管理しなければならない。この場合において、製造販売業者等は次の各号に掲げる事項を当該各号の順序に従い、危険性の管理に適用しなければならない。

# イ：42条基準 装置基準

2023.11.15 現在

**薬機法第４２条**

２ 厚生労働大臣は、保健衛生上の危害を防止するために必要があるときは、医薬部外品、化粧品又は医療機器について、薬事・食品衛生審議会の意見を聴いて、その性状、品質、性能等に関し、必要な基準を設けることができる。

| | 告示 | 基準名 | 備考 |
|---|---|---|---|
| 1 | 昭和45年 厚生省 告示第298号 | 人工血管基準 | |
| 2 | 昭和45年 厚生省告示第299号 | 医療用接着剤基準 | |
| 3 | 平成13年 厚生労働省 告示第75号 | 医療用エックス線装置基準 | 医療機関の医療用放射線の防護は医療法施行規則（第四章）で定めらており、この装置基準と同じ。 |
| 4 | 平成13年 厚生労働省 告示第264号 | 人工呼吸器警報基準 | |
| 5 | 平成13年 厚生労働省 告示第349号 | 視力補正用コンタクトレンズ基準 | 眼球に直接接触させたとき、視力を補正することができるもの |
| 6 | 平成15年 厚生労働省 告示第210号 | 生物由来原料基準 | |
| 7 | 平成21年 厚生労働省 告示第283号 | 非視力補正用コンタクトレンズ基準 | 虹彩又は瞳孔の外観(色、模様及び形をいう。)を変えることを目的とし、視力補正機能を有しないもの |
| 8 | 平成29年 厚生労働省 告示第261号 | 再製造単回使用医療機器基準 | |

# ウ：承認基準

2023.11.15 現在　４４基準

・その基準への適合性を確認する承認審査を行う。

| | |
|---|---|
| 承01 | コンタクトレンズ基準 |
| 承02 | 眼内レンズ基準 |
| 承03 | 経皮的冠動脈形成術用カテーテル基準 |
| 承04 | 血液透析器、血液透析濾過器及び血液濾過器基準 |
| 承05 | 中心静脈用カテーテル基準 |
| 承06 | 創傷被覆・保護材基準 |
| 承07 | 加速器システム基準 |
| 承09 | X線骨密度測定装置基準 |
| 承11 | インスリンペン型注入器基準 |
| 承13 | 輸液ポンプ基準 |
| 承14 | 眼科用パルスレーザ手術装置基準 |
| 承15 | 眼科用レーザ光凝固装置基準 |
| 承16 | 眼科用レーザ光凝固装置プローブ等基準 |
| 承17 | 血液濃縮器基準 |
| 承18 | 植込み型心臓ペースメーカ等基準 |
| 承20 | 長期的使用胆管用カテーテル等基準 |
| 承21 | 長期使用尿管用チューブステント基準 |
| 承22 | 汎用冷凍手術ユニット基準 |
| 承23 | 経皮的血管形成術用カテーテル基準 |
| 承24 | 非中心循環系永久刺入向け手動式ブラキセラピー装置用放射線源基準 |
| 承25 | 非中心循環系一時留置向け手動式ブラキセラピー装置用放射線源基準 |
| 承26 | 眼科用冷凍手術ユニット基準 |
| 承27 | 脳動脈瘤手術用クリップ基準 |
| 承28 | 脳動静脈奇形手術用クリップ基準 |

| | |
|---|---|
| 承29 | インスリン皮下投与用注射筒等基準 |
| 承30 | 硬膜外投与用針及び脊髄くも膜下・硬膜外針基準 |
| 承31 | 麻酔脊髄用針基準 |
| 承32 | 麻酔用滅菌済み穿刺針基準 |
| 承33 | 硬膜外麻酔用カテーテル基準 |
| 承34 | 加圧式医薬品注入器基準 |
| 承35 | 自動腹膜灌流用装置基準 |
| 承36 | 歯科用インプラント基準 |
| 承37 | 人工腎臓装置基準 |
| 承38 | 人工肺基準 |
| 承39 | 神経内視鏡基準 |
| 承40 | 血管内視鏡基準 |
| 承41 | カテーテルイントロデューサ基準 |
| 承42 | 水頭症治療用シャント基準 |
| 承43 | 緊急時ブラッドアクセス留置用カテーテル基準 |
| 承44 | 中心循環系血管造影用カテーテル基準 |
| 承45 | 中心循環系ガイディング用血管内カテーテル基準 |
| 承46 | 中心循環系マイクロカテーテル基準 |
| 承47 | 心臓・中心循環系用カテーテルガイドワイヤ等基準 |
| 承48 | 長期的使用経腸栄養キット等基準 |

廃止基準
承8 ：放射線治療シミュレータ基準　　＝＞新規製品申請予定がなく廃止
承10: 磁気共鳴画像診断装置基準　　＝＞認証基準へ
承12: X線CT組合せ型ポジトロンCT装置基準　＝＞認証基準へ
承19: 自己検査用グルコース測定器基準　　＝＞認証基準へ

# 工：認証基準

2023.10.01 現在

| 別表 | 区分（クラス） | 基準数 | 適合方式 | 事例 | | 告示の但し書き | 備考 |
|---|---|---|---|---|---|---|---|
| | | | | 適合事項 | 使用目的又は効果 | | |
| 第一 | 高度管理（Ⅲ） | 12 | 主要評価項目への適合確認（適合に関し必要な事項は局長通知による） | 例：インスリンペン型注入器<br><br>次の評価項目について厚生労働省医薬・生活衛生局長が定める基準により評価すること。<br>1 機械的性能<br>2 投与量の精度<br>3 無ディフェクト性 | 専用医薬品カートリッジ及びペン形注入器注射針を取り付けて使用し、皮下へインスリンを注入すること。 | 高度管理医療機器の形状、構造及び原理、使用方法又は性能等が・・・既存品目・・・と実質的に同等でないときは・・・適用しない。 | 基本要件基準を満たすために引用可能な規格等一覧として通知で示す |
| 第二 | 管理（Ⅱ） | 7 | 主要評価項目への適合確認（適合に関し必要な事項は局長通知による） | 例：ナログ式口外汎用<br>歯科Ｘ線診断装置<br><br>次の評価項目について厚生労働省医薬・生活衛生局長が定める基準により評価すること。<br>1 医用電気機器の安全性<br>2 放射線防護<br>3 空気カーマの直線性<br>4 放射線出力の再現性<br>5 Ｘ線管負荷条件の正確さ<br>6 Ｘ線源装置の仕様<br>7 画像性能<br>8 線量測定値の表示 | 人体の頭部を透過したＸ線の蛍光作用、写真作用又は電離作用を利用して、歯科診療のための歯又は顎部の画像情報を提供すること。 | 管理医療機器の形状、構造及び原理、使用方法又は性能等が既存の管理医療機器と明らかに異なるときは・・・適用しない。 | |
| 第三 | 管理（Ⅱ） | 932 | 告示で指定された規格への適合確認 | 例：移動型アナログ式<br>汎用Ｘ線診断装置<br><br>JIS T0601-1-3<br>JIS Z4751-2-54 | 人体を透過したＸ線の蛍光作用、写真作用又は電離作用を利用して人体画像情報を診療のために提供すること。 | | 適合が必須な規格を告示で指定 |

# 参考：承認ガイドライン、審査ポイント

2023.11.15　現在

## 承認ガイドライン

・基準への適合性が客観的に判断できるような統一的な技術要件を定めることが困難であって、承認基準を定めることができない品目について可能な範囲で技術要件又は技術要件項目等を示したもの。

・承認審査においては『審査ガイドライン』を参考としつつ、個別品目に応じた必要事項について併せて審査が行われる。

| No | 承認ガイドライン名 |
|---|---|
| GL1 | 人工股関節審査ガイドライン |
| GL2 | 人工膝関節審査ガイドライン |
| GL3 | 脊椎内固定器具審査ガイドライン |
| GL4 | 体内固定用髄内釘審査 |
| GL5 | 体内固定用コンプレッションヒッププレート審査 |
| GL6 | 体内固定用ケーブル審査ガイドライン |
| GL7 | 体内固定用ピン審査ガイドライン |
| GL8 | 体内固定用ネジ及び体内固定用プレート審査ガイドライン |
| GL9 | 浅大腿動脈血管内ステント審査ガイドライン |
| GL10 | 歯科用漂白材等審査ガイドライン |

## 審査ポイント

- 審査ポイントは、承認申請に際し、資料の作成の効率化及び審査の迅速化に資するため、規定する適用範囲に示す医療機器について、必要な評価項目等を示すものであること。
- 審査ポイントは、現時点における科学的知見に基づき審査の考え方について示したものであり、今後の科学技術の進歩等に応じて随時見直され、改訂されるべきものであること。

| No | 一般的名称 |
|---|---|
| 1 | 腹膜透析用治療計画プログラム |
| 2 | 歯科インプラント用治療計画支援プログラム |
| 3 | 眼科手術用治療計画プログラム |
| 4 | 病変検出用内視鏡画像診断支援プログラム |
| 5 | 医用画像の読影支援を目的としたコンピュータ診断支援プログラム |

# Ⅲ．医療機器のサイバーセキュリティ対応

1）サイバーセキュリティ対応通知等

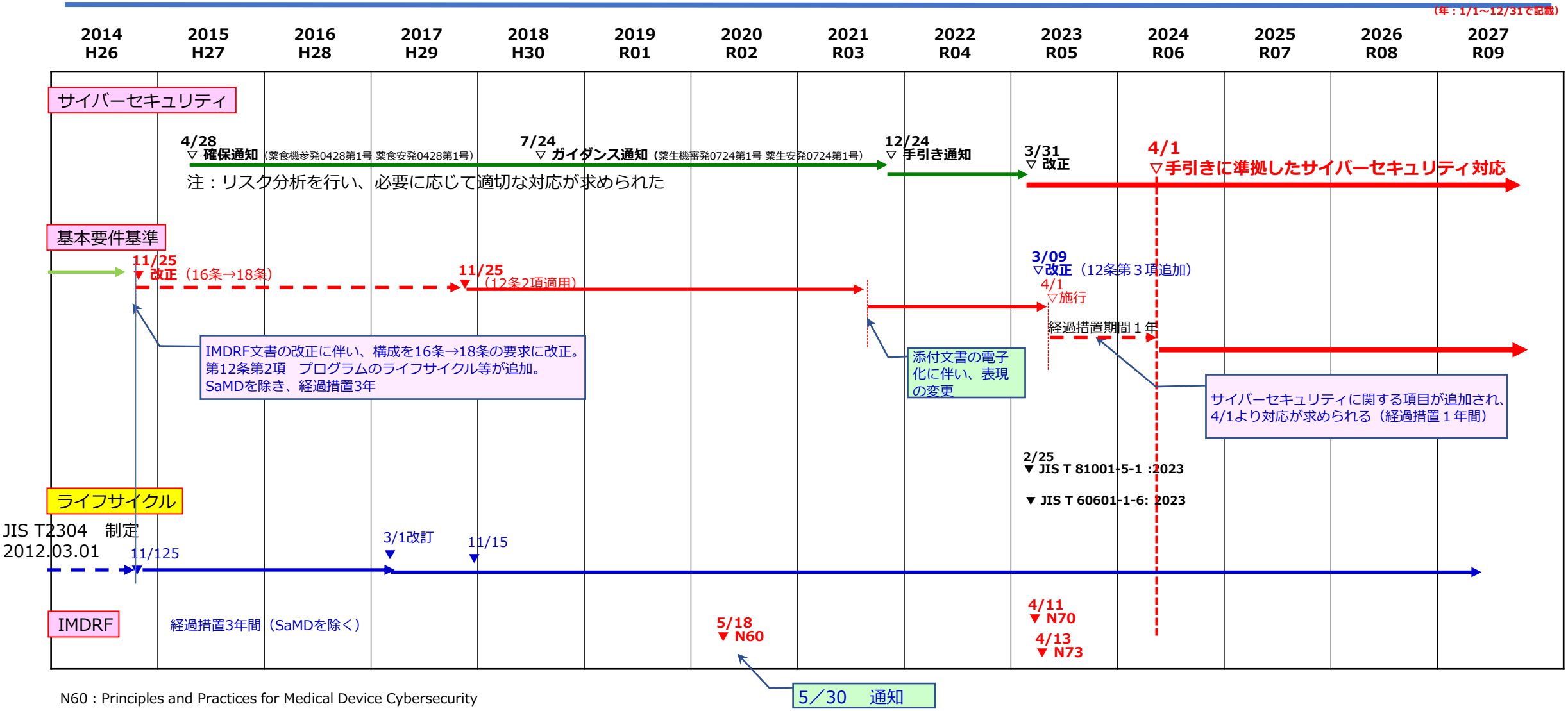
2）薬機法におけるサイバーセキュリティ対応の推移

3）医療機器におけるサイバーセキュリティの確保について

# 1）サイバーセキュリティ対応通知等

| No. | 発簡日 | 発簡番号 | タイトル |
|---|---|---|---|
| 1 | 平成27年4月28日 | 薬食機参発0428第1号<br>薬食安発0428第1号 | 医療機器におけるサイバーセキュリティの確保について |
| 2 | 平成30年7月24日 | 薬生機審発0724第1号<br>薬生安発0724第1号 | 医療機器のサイバーセキュリティの確保に関するガイダンスについて |
| 3 | 令和2年5月13日 | 薬生機審発0513第1号<br>薬生安発0513第1号 | 国際医療機器規制当局フォーラム(IMDRF)による医療機器サイバーセキュリティの原則及び実践に関するガイダンスの公表について（周知依頼） |
| 4 | 令和3年10月20日 | 事務連絡 | 「医療情報システムの安全管理に関するガイドライン」に関する「医療機関のサイバーセキュリティ対策チェックリスト」及び「医療情報システム等の障害発生時の対応フローチャート」について |
| 5 | 令和3年12月24日 | 薬生機審発1224第1号<br>薬生安発1224第1号 | 医療機器のサイバーセキュリティの確保及び徹底に係る手引書について |
| 6 | 令和5年3月9日 | 厚生労働省告示第67号 | 医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律第41条第3項の規定により厚生労働大臣が定める医療機器の基準の一部を改正する件 |
| 7 | 令和5年3月31日 | 医政参発0331第1号<br>薬生機審発0331第16号<br>薬生安発0331第8号 | 医療機関における医療機器のサイバーセキュリティ確保のための手引書について |
| 8 | 令和5年3月31日 | 薬生機審発0331第11号<br>薬生安発0331第4号 | 医療機器のサイバーセキュリティ導入に関する手引書の改訂について |
| 9 | 令和5年3月31日 | 薬生機審発0331第8号 | 医療機器の基本要件基準第12条第3項の適用について |
| 10 | 令和5年5月23日 | 薬生機審発0523第1号 | 医療機器の基本要件基準第12条第3項の適合性の確認について |
| 11 | 令和5年7月20日 | 事務連絡 | 医療機器の基本要件基準第12条第3項の適用に関する質疑応答集（Q&A）について |

# 2）薬機法におけるサイバーセキュリティ対応の推移




N60 : Principles and Practices for Medical Device Cybersecurity

N70 : Principles and Practices for Software Bill of Materials for Medical Device Cybersecurity

N73 : Principles and Practices for the Cybersecurity of Legacy Medical Devices

# 3）医療機器におけるサイバーセキュリティの確保について

平成27年4月28日 薬食機参発0428第1号 薬食安発0428第1号

1. 基本的考え方

製造販売業者は**サイバーリスクが懸念される**医療機器について、サイバーセキュリティを確保する必要があり・・・法・・・第41条第3項に基づく基本要件基準・・・に基づき、サイバーリスクについても既知又は予見し得る危害としてこれを識別し、**意図された使用方法及び予測し得る誤使用に起因する危険性を評価**し、合理的に実行可能な限り除去することが求められる。サイバーリスクが懸念される医療機器の開発に当たっては、リスクマネジメントとして必要な対策を実施し、**サイバーセキュリティを確保**すること、また、**既に製造販売を行っている医療機器に関しても、同様にサイバーセキュリティを確保すること**が**必要**である。

2. 具体的な対策について

サイバーリスクが懸念される医療機器のうち・・・他の機器・ネットワーク等・・・との接続が可能な医療機器について、製造販売業者は下記を踏まえて必要な措置を行うこと。

① 他の機器・ネットワーク等と接続して使用する又は他からの不正なアクセス等が想定される医療機器については、当該医療機器で想定されるネットワーク使用環境等を踏まえてサイバーリスクを含む危険性を評価・除去し、防護するリスクマネジメントを行い、使用者に対する必要な情報提供や注意喚起を含めて適切な対策を行うこと。

具体的には、当該医療機器と接続できる範囲を限定する、使用するソフトウェア等は製造販売業者が信頼性を認めたものに限定するなどのような対策が考えられる。

② ①の必要なサイバーセキュリティの確保がなされていない医療機器については、使用者に対してその旨を明示し、他との接続を行わない又は接続できない設定とするよう必要な注意喚起を行うこと。

③ 「医療情報システムの安全管理に関するガイドライン」を踏まえ、医療機関における不正ソフトウェア対策やネットワーク上からの不正アクセス対策等のサイバーセキュリティの確保が適切に実施されるよう、医療機関に対し、必要な情報提供を行うとともに、必要な連携を図ること。

# ４）医療機器のサイバーセキュリティの確保に関するガイダンスについて

Ｈ３０年発行

薬生機審発０７２４第１号
薬生安発０７２４第１号
平成３０年７月２４日

各都道府県衛生主管部（局）長 殿

厚生労働省医薬・生活衛生局医療機器審査管理課長
（公印省略）

厚生労働省医薬・生活衛生局医薬安全対策課長
（公印省略）

医療機器のサイバーセキュリティの確保に関するガイダンスについて

医療機器のサイバーセキュリティの確保に関しては、「医療機器におけるサイバーセキュリティの確保について」（平成 27 年４月 28 日付け薬食機参発 0428第１号、薬食安発 0428 第１号厚生労働省大臣官房参事官（医療機器・再生医療等製品審査管理担当）、厚生労働省医薬食品局安全対策課長連名通知）において、医療機器の安全な使用を確保するために、医療機器に関するサイバーリスクに対する適切なリスクマネジメントを実施し、必要な対応を行うよう、関係事業者等に対する周知を依頼しているところです。

今般、さらに具体的なリスクマネジメント及びサイバーセキュリティ対策について、平成 29 年度日本医療研究開発機構医薬品等規制調和・評価研究事業「医療機器に関する単体プログラムの薬事規制のあり方に関する研究」の研究報告を基に、「医療機器のサイバーセキュリティの確保に関するガイダンス」として別添のとおり取りまとめました。つきましては、医療機器のサイバーセキュリティの確保に当たって、同ガイダンスを参考として、必要な対応を行うよう、貴管下関係事業者等に周知方お願いいたします。

薬生機審発０７２４第１号
薬生安発０７２４第１号
平成３０年７月２４日

各都道府県衛生主管部（局）長 殿

厚生労働省医薬・生活衛生局医療機器審査管理課長
（公印省略）

厚生労働省医薬・生活衛生局医薬安全対策課長
（公印省略）

医療機器のサイバーセキュリティの確保に関するガイダンスについて

医療機器のサイバーセキュリティの確保に関しては、「医療機器におけるサイバーセキュリティの確保について」（平成 27 年４月 28 日付け薬食機参発 0428第１号、薬食安発 0428 第１号 厚生労働省大臣官房参事官（医療機器・再生医療等製品審査管理担当）、厚生労働省医薬食品局安全対策課長連名通知）において、医療機器の安全な使用を確保するために、医療機器に関するサイバーリスクに対する適切なリスクマネジメントを実施し、必要な対応を行うよう、関係事業者等に対する周知を依頼しているところです。

今般、さらに具体的なリスクマネジメント及びサイバーセキュリティ対策について、平成 29 年度日本医療研究開発機構医薬品等規制調和・評価研究事業「医療機器に関する単体プログラムの薬事規制のあり方に関する研究」の研究報告を基に、「医療機器のサイバーセキュリティの確保に関するガイダンス」として別添のとおり取りまとめました。つきましては、医療機器のサイバーセキュリティの確保に当たって、同ガイダンスを参考として、必要な対応を行うよう、貴管下関係事業者等に周知方お願いいたします。

# 別添：医療機器のサイバーセキュリティの確保に関するガイダンス

目　　次

# 5）IMDRFの医療機器サイバーセキュリティの原則及び実践に関するガイダンス

令和２年５月13日 薬生機審発0513第1号 薬生安発0513第1号

令和2年 5月13日
薬生機審発0513第1号
薬生安発0513第1号

各都道府県衛生主管部（局）長　殿

厚生労働省医薬・生活衛生局医療機器審査管理課長
厚生労働省医薬・生活衛生局医薬安全対策課長

国際医療機器規制当局フォーラム(IMDRF)による医療機器サイバーセキュリティの原則及び実践に関するガイダンスの公表について（周知依頼）

医療機器のサイバーセキュリティについては、「医療機器におけるサイバーセキュリティの確保について」（平成27年4月28日付け薬食機参発0428第1号、薬食安発0428第1号厚生労働省大臣官房参事官（医療機器・再生医療等製品審査管理担当）、厚生労働省医薬食品局安全対策課長連名通知）において、医療機器の安全な使用の確保のため、医療機器に関するサイバーリスクに対する適切なリスクマネジメントの実施を求め、「医療機器のサイバーセキュリティの確保に関するガイダンスについて」（平成30年7月24日付け薬生機審発0724第1号、薬生安発0724第1号厚生労働省医薬・生活衛生局医療機器審査管理課長、医薬安全対策課長連名通知）により、具体的なリスクマネジメント及びサイバーセキュリティ対策を取りまとめたガイダンスを示し、当該ガイダンスを参考に必要な対応を行うよう、関係事業者等に対する周知を依頼してきたところです。

今般、医療機器のサイバーセキュリティ確保の重要性や各国のサイバーセキュリティ対策の実情等を踏まえ、国際医療機器規制当局フォーラム(IMDRF)において、サイバーセキュリティ対策の国際的な調和を図ることを目的として、「Principles and Practices for Medical Device Cybersecurity」（医療機器サイバーセキュリティの原則及び実践）（以下「IMDRFガイダンス」という。）が取りまとめられました。

国際的な規制調和の推進の観点や国境の枠組みを超えて医療機器のサイバーセキュリティに係る安全性を向上させる観点から、我が国においても、今後3年程度を目途に、医療機器製造販売業者に対してIMDRFガイダンスの導入に向けて検討を行っているところです。そのため、医療機器のサイバーセキュリティの更なる確保に向けた医療機器製造販売業者等の体制確保を円滑に行えるよう、別添のとおり、国立医薬品食品衛生研究所医療機器部が作成したIMDRFガイダンスの邦訳版を参考として情報提供いたしますので、貴管下の医療機器製造販売業者等に対し、周知及び体制確保に向けた指導等よろしくお願いします。

なお、IMDRFガイダンスの原文は以下のホームページから入手可能であることを申し添えます。

URL：http://www.imdrf.org/documents/documents.asp

別　添

IMDRF/CYBER WG/N60 FINAL:2020

IMDRF International Medical Device Regulators Forum

最終文書

**タイトル:** 医療機器サイバーセキュリティの原則及び実践

**作成グループ:** 医療機器サイバーセキュリティワーキンググループ

**日付:** 2020 年 3 月 18 日

Dr Choong May Ling, Mimi, IMDRF 議長

# 目次

# 6）医療機器のサイバーセキュリティの確保及び徹底に係る手引書

薬生機審発1224第1号
薬生安発1224第1号
令和3年 12月24日

各都道府県衛生主管部（局）長　殿

厚生労働省医薬・生活衛生局医療機器審査管理課長
（公印省略）

厚生労働省医薬・生活衛生局医薬安全対策課長
（公印省略）

**医療機器のサイバーセキュリティの確保及び徹底に係る手引書について）**

医療機器のサイバーセキュリティの確保については、「医療機器におけるサイバーセキュリティの確保について」（平成27年4月28日付け薬食機参発0428第1号・薬食安発0428第1号厚生労働省大臣官房参事官（医療機器・再生医療等製品審査管理担当）・医薬食品局安全対策課長連名通知）において、医療機器の安全な使用の確保のため、医療機器に関するサイバーリスクに対する適切なリスクマネジメントの実施を求めるとともに、サイバーセキュリティ対応に係る内容をガイダンス（以下「旧ガイダンス」という。）をとりまとめ、「医療機器のサイバーセキュリティの確保に関するガイダンスについて」（平成30年7月24日付け薬生機審発0724第1号・薬生安発0724第1号厚生労働省医薬・生活衛生局医療機器審査管理課長・医薬安全対策課長連名通知）において周知したところです。その後、国際医療機器規制当局フォーラム(IMDRF)において、サイバーセキュリティ対策の国際的な調和を図ることを目的として、「Principles and Practices for Medical Device Cybersecurity」（医療機器サイバーセキュリティの原則及び実践）（以下「IMDRFガイダンス」という。）が発行され、「国際医療機器規制当局フォーラム(IMDRF)による医療機器サイバーセキュリティの原則及び実践に関するガイダンスの公表について（周知依頼）」（令和2年5月13日付け薬生機審発0513第1号・薬生安発0513第1号厚生労働省医薬・生活衛生局医療機器審査管理課長・医薬安全対策課長連名通知）により、情報提供したところです。

今般、IMDRFガイダンスの発行等の国際的な枠組みでの活動を踏まえて、旧ガイダンスを置き換え、医療機器へのサイバー攻撃に対する国際的な耐性基準等の技術要件を我が国へ導入して整備することを目的に、国立研究開発法人日本医療研究開発機構医薬品等規制調和・評価研究事業「医療機関における医療機器のサイバーセキュリティに係る課題抽出等に関する研究」及び一般社団法人日本医療機器産業連合会において、医療機器のサイバーセキュリティに係る必要な開発目標及び技術要件等を検討し、別添のとおり、「医療機器のサイバーセキュリティ導入に関する手引書」として取りまとめましたので情報提供します。

薬生機審発0331第11号
薬生安発0331第4号
令和5年 3月31日

各都道府県衛生主管部（局）長　殿

厚生労働省医薬・生活衛生局医療機器審査管理課長
（公印省略）

厚生労働省医薬・生活衛生局医薬安全対策課長
（公印省略）

**医療機器のサイバーセキュリティ導入に関する手引書の改訂について**

医療機器のサイバーセキュリティの確保については、「医療機器におけるサイバーセキュリティの確保について」（平成27年4月28日付け薬食機参発0428第1号・薬食安発0428第1号厚生労働省大臣官房参事官（医療機器・再生医療等製品審査管理担当）・医薬食品局安全対策課長連名通知）において、医療機器の安全な使用の確保のため、医療機器に関するサイバーリスクに対する適切なリスクマネジメントの実施を求めています。また、国際医療機器規制当局フォーラム(IMDRF)において、サイバーセキュリティ対策の国際的な調和を図ることを目的として、「Principles and Practices for Medical Device Cybersecurity」（医療機器サイバーセキュリティの原則及び実践。以下「IMDRFガイダンス」という。）が発行されたことを受け、「国際医療機器規制当局フォーラム(IMDRF)による医療機器サイバーセキュリティの原則及び実践に関するガイダンスの公表について（周知依頼）」（令和2年5月13日付け薬生機審発0513第1号・薬生安発0513第1号厚生労働省医薬・生活衛生局医療機器審査管理課長・医薬安全対策課長連名通知）により、情報提供しています。さらに、IMDRFガイダンスの発行等の国際的な枠組みでの活動を踏まえて、医療機器へのサイバー攻撃に対する国際的な耐性基準等の技術要件を我が国へ導入して整備することを目的に、医療機器のサイバーセキュリティに係る必要な開発目標及び技術的要件等を検討し、主に医療機器製造販売業者向けの「医療機器のサイバーセキュリティ導入に関する手引書」として取りまとめられたことを「医療機器のサイバーセキュリティの確保及び徹底に係る手引書について」（令和3年12月24日付け薬生機審発1224第1号・薬生安発1224第1号厚生労働省医薬・生活衛生局医療機器審査管理課長・医薬安全対策課長連名通知）により、お示ししたところです。

今般、IMDRFにおいて追補ガイダンスが発出されたことから、その内容に基づき、「医療機器のサイバーセキュリティ導入に関する手引書」について、一般社団法人日本医療機器産業連合会の医療機器サイバーセキュリティ対応ワーキンググループにおいて、Software Bill of Materials(SBOM)の取扱いやレガシー医療機器の取扱い、脆弱性の修正、インシデントの対応等を検討し、改訂版の「医療機器のサイバーセキュリティ導入に関する手引書」として、別添のとおり取りまとめましたので情報提供します。

医療機器のサイバーセキュリティ導入に関する手引書

目次



医療機器のサイバーセキュリティ導入に関する手引書（第2版）

目次

手引書（初版）より

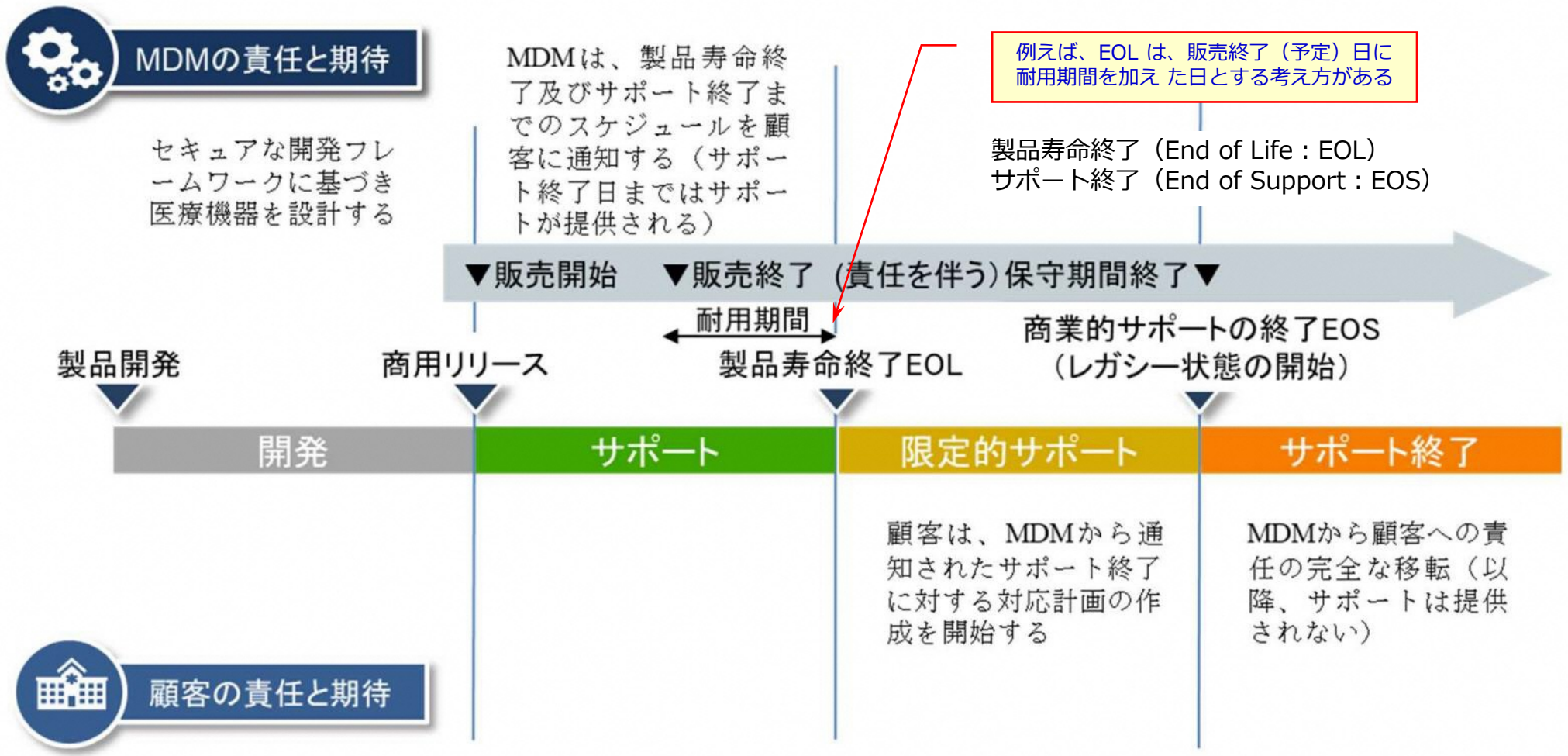



**図 2　製品ライフサイクルにおけるレガシー医療機器の概念フレームワーク**
（MDM：医療機器の製造販売業者）

# Ⅳ．基本要件基準第12条第３項の適合について

１）医療機器の基本要件基準第12条第3項の適用について

２）医療機器の基本要件基準第12条第3項の適合性の確認について

３）医療機器の基本要件基準第12条第3項の適用に関する質疑応答集（Q&A）について

# １）医療機器の基本要件基準第12条第3項の適用について

・・・改正後の・・・基本要件基準・・・第12条第3項は、令和5年4月1日から適用されます。1年間の経過措置期間が設定され・・・令和6年4月1日まで・・・なお従前の例によることができる・・・。・・・

## 1. 基本要件基準第12条第3項の趣旨

基本要件基準は、医療機器が具備すべき品質、有効性及び安全性に係る基本的な要件を規定したものであり、医療機器に対しリスクマネジメントの適用によってリスクを許容可能な範囲まで低減することが要求されている。

サイバーセキュリティ対策については、
「医療機器におけるサイバーセキュリティの確保について」（平成27年4月28日付け薬食機参発0428第1号及び薬食安発0428第1号）、
「医療機器のサイバーセキュリティの確保に関するガイダンスについて」（平成30年7月24日付け薬生機審発0724第1号及び薬生安発0724第1号）等
において必要な対応を行うよう求めてきたところであるが、今般、令和2年3月に国際医療機器規制当局フォーラム（IMDRF）において、「医療機器サイバーセキュリティの原則及び実践に関するガイダンス」が取りまとめられたことに伴い、
IMDRF N47文書（Essential Principles of Safety and Performance of Medical Devices and IVD Medical Devices）
及び
N60文書（Principles and Practices for Medical Device Cybersecurity）を
踏まえ、プログラムを用いた医療機器に対しサイバーセキュリティを確保するための設計及び製造、ライフサイクル活動として、

① 製品の全ライフサイクルにわたって医療機器サイバーセキュリティを確保する計画を備えること、

② サイバーリスクを低減する設計及び製造を行うこと、

③ 適切な動作環境に必要となるハードウェア、ネットワーク及びITセキュリティ対策の最低限の要件を設定すること、

の3つの観点を基本要件基準に盛り込むこととし、基本要件基準第12条に第3項を追加する改正を行ったものである。

## 2. 基本要件基準第12条第3項の要点・解釈

（1）「プログラムを用いた医療機器のうち、他の機器及びネットワーク等と接続して使用する医療機器」とは、他の機器（医療機器、IoT機器、周辺機器、外部記録媒体（USB、SD、HDD、CD、DVD等）、電子カルテ、PC（外部からの持ち込みPC含む））、ネットワーク（院内システム、院外システム、グローバル）等に接続して電磁的情報のやり取りをする医療機器である。

（2）「外部からの不正アクセス及び攻撃アクセス等」は、脆弱性を攻撃対象とする等の設計者が通常使用において想定していない手法等を用いた悪意を持った不正アクセスや、意図的に過剰な負荷を与える攻撃（DoS攻撃(Denial of Service Attack)、DDoS攻撃(Distributed Denial of Service Attack)等）、マルウェア（悪意のあるソフトウェア）の感染を意図する攻撃によるアクセス等を想定している。昨今のサイバー攻撃についてはその攻撃形式が多様化・高度化しており、今後はこれらの攻撃手法の他にも対応することも必要となり得る。

（3）「動作環境及びネットワークの使用環境等を踏まえて適切な要件を特定し」とは、医療機関、在宅、救急、植込み型機器等の動作環境並びに接続するネットワーク種別やオペレーティングシステム及び各種ライブラリ等のプラットフォームといった使用環境を特定し、その使用環境に適した運用体制等を含めた医療機器の意図する使用に適切な要件を設定することである。

（4）「当該医療機器の機能に支障が生じる又は安全性の懸念が生じるサイバーセキュリティに係る危険性を特定及び評価するとともに、当該危険性が低減する管理」とは、他のリスクと同様に、サイバーセキュリティに係るリスクに対しても、適切にリスクマネジメントを行い、例えば、JIS T 81001-5-1に示されている通り、サイバーセキュリティの脆弱性を特定し、その悪用によって生じる脅威や悪影響に伴うリスクを評価し、適切にリスクをコントロールすることである。

（5）「ライフサイクルの全てにおいて、サイバーセキュリティを確保するための計画に基づいて設計及び製造」とは、全ライフサイクルにわたってサイバーセキュリティを確保するため、設計・製造工程における取組だけでなく、医療機関との連携、脆弱性対策（市販後のアップデート等を含む）に係る計画等も踏まえ、それが達成できるように、また、問題点や脆弱性が見つかった場合に対応できるように設計・製造を行うことである。

## 3. 基本要件基準第12条第3項の適用・適合性の確認について

（1）プログラムを用いた医療機器の・・・製造販売業者等・・・はこれまでもJIS T 2304によって、医療機器ソフトウェアライフサイクル全体を通じて、適切なリスクマネジメントを実施することにより、医療機器の安全性と基本性能を確保することが求められてきたところであるが、プログラムを用いた医療機器については、これに加えて、JIS T 81001-5-1によって、製品ライフサイクルにおける取組を通じたサイバーセキュリティ対策をより強化し、サイバーセキュリティに関するリスクを許容可能な範囲となるまで低減し、患者への危害の発生及び拡大の防止に繋げる必要があること。

※ JIS T 81001-5-1（ヘルスソフトウェア及びヘルスITシステムの安全、有効性及びセキュリティ－第5－1部：セキュリティ－製品ライフサイクルにおけるアクティビティ）は、医療機器の製造販売業者がJIS T 2304（医療機器ソフトウェアライフサイクルプロセス）に規定する製品ライフサイクルの要求事項に加えて実施するサイバーセキュリティに関する取組を規定している。

（2）JIS T 81001-5-1の他、プログラムを用いた医療機器のサイバーセキュリティの確保について、IEC 81001-5-1等の国際的に用いられている適切な規格等への適合性を確認することをもって基本要件基準第12条第3項への適合を確認したものとして差し支えないこと。なお、承認申請（承認事項一部変更承認申請を含む。以下同じ。）又は認証申請（認証事項一部変更認証申請を含む。以下同じ。）に際しては、それらの規格等を用いることの妥当性を説明すること。

（3）製造販売業者等は、プログラムを用いた医療機器のサイバーセキュリティの確保の確認及び検証を適切に考慮及び実施する体制を整備し、その適合に関する確認等の実施を適切に記録し保管すること。・・・法・・・第23条の2の5第7項又は第23条の2の23第4項の規定による調査の調査権者の求めなどに応じて資料を提示し、適切な説明を行わなければならないこと。

（4）高度管理医療機器又は管理医療機器の承認申請又は認証申請を行う製造販売業者等は、申請に当たり、当該医療機器についてJIS T 81001-5-1等への適合性を示す資料を添付する必要があること。

また、一般医療機器についても同様に適合性を確認する必要があるが、届出の際に資料の添付は要さないこと。

## 4. 経過措置について

本改正で追加される基本要件基準第12条第3項は令和5年4月1日より適用されるが、令和6年3月31日までの間、なお従前の例によることができること。

（1）改正後の基本要件基準が適用される令和6年3月31日以前に承認若しくは認証を受けた医療機器又は届出された医療機器については、改めて申請・届出を行う必要はないものとする。

ただし、承認認証事項又は届出事項に何らかの変更が生じる等により、令和6年4月1日以降に当該医療機器の承認又は認証事項一部変更申請が必要な場合にあっては、改正後の基本要件基準への適合を確認した上で、改正後の基本要件基準への適合を示す資料を添付すること。

なお、令和6年4月1日以降に製造販売する医療機器は、改正後の基本要件基準への適合を確認した上で、改正後の基本要件基準への適合に関する資料を求めに応じて提示できるようにしておくこと。

令和6年3月31日以前に製造販売された医療機器に関する取扱いについては追って通知するものとする。

（2）令和6年3月31日以前に承認申請若しくは認証申請又は届出される医療機器については、承認申請又は認証申請若しくは届出時に、改正後の基本要件基準への適合を示す資料を添付する必要はないものとする。

令和6年4月1日以降の取扱いについては、4.（1）のただし書き及びなお書きを準用する。

（3）令和6年4月1日以降に承認申請若しくは認証申請を行う医療機器については、改正後の基本要件基準への適合を確認した上で、改正後の基本要件基準への適合に関する資料を添付する必要がある。届出を行う医療機器についても、改正後の基本要件基準への適合を確認すること。

# ２）医療機器の基本要件基準第12条第3項の適合性の確認について

令和5年 5月23日　薬生機審発0523第1号

・・・改正後の・・・基本要件基準・・・に規定されている第12条第3項は、1年間の経過措置期間が設定され、改正後の基本要件基準第12条第3項の適合が必要な医療機器においては、令和6年4月1日までの間、なお従前の例によることができるとされているところです。

その適合性の確認について、下記のとおりとする・・・

記

高度管理医療機器若しくは管理医療機器の承認申請又は認証申請を行う製造販売業者等は、当該医療機器について基本要件基準第12条第3項への適合を示すため、JIS T 81001-5-1等への適合性を確認する際には、次の事項について留意して、当該結果を示すか又は当該結果をまとめた社内文書等を特定すること。なお、一般医療機器についても同様に確認が必要であること。

## 1. JISに関連する要求事項

### （1）JIS T 81001-5-1の箇条4の一般要求事項について

・サイバーセキュリティの確保に係る活動は、品質マネジメントシステムに基づいて行われていること。
・規制当局及び顧客に対して脆弱性を適時に通知する活動を確立すること。
・医療機器のリスクマネジメントは、セキュリティの脆弱性、脅威等を考慮したものであること。

### （2）JIS T 81001-5-1の箇条5のソフトウェア開発プロセスについて

JIS T 81001-5-1の規定に基づき、ソフトウェア開発プロセスに対して、次の配慮が行われていること。
・開発計画において、セキュリティ更新や開発環境等のセキュリティについて考慮すること。
・製品のセキュリティ機能を含むセキュリティ要求事項を特定すること。
・意図する使用環境、信頼境界、多層防御等を考慮してアーキテクチャー設計を行うこと。
・セキュリティ設計のベストプラクティスを考慮した設計及び実装を行うこと。
・ソフトウェアシステム試験を行って、セキュリティ要求事項が満たされ、リスクマネジメントプロセスで特定した脅威に対応する方法が設計に実装され、有効であることを確認すること。

### （3）JIS T 81001-5-1の箇条6のソフトウェア保守プロセスについて

顧客に対するセキュリティ更新の通知方針について定めておくこと。

### （4）JIS T 81001-5-1の箇条7のセキュリティに関連するリスクマネジメントプロセスについて

医療機器のリスクマネジメントにおいて、医療機器の意図する使用及び使用環境を考慮して、関連する脆弱性を特定し、関連する**脅威を推定して評価し、リスクコントロール手段によって脅威をコントロールし、その有効性を監視すること。**

### （5）JIS T 81001-5-1の箇条8のソフトウェア構成管理プロセスについて

医療機器の開発、保守及びサポートのための、変更管理及び変更履歴を伴う構成管理プロセスを確立すること。

### （6）JIS T 81001-5-1の箇条9のソフトウェア問題解決プロセスについて

セキュリティの脆弱性に関する情報伝達及び処理の手順を定め、セキュリティ問題に対して、情報開示を含めて手順に従って実施すること。

## 2. JISに関連する既存通知等の要求事項

下記の項目については、規格への適合性を確認する際、追加で確認すること。

### （1）JIS T 81001-5-1の箇条4の一般要求事項について

規制当局及び顧客に対して脆弱性を適時に通知する活動は、「医療機器のサイバーセキュリティの確保に関するガイダンスについて」（平成30年7月24日付け薬生機審発0724第1号及び薬生安発0724第1号）に求める通り、品質マネジメントシステムにおいて、セキュリティに対する対応方針、セキュリティに対する問い合わせ窓口を明確化し、顧客に対する脆弱性等の開示手順が定められていることによって確認することあ。

### （2）JIS T 81001-5-1の箇条5のソフトウェア開発プロセスについて

セキュリティ要求事項の特定においては、基本要件基準第12条第3項に規定する通り、当該医療機器における動作環境及びネットワークの使用環境等を踏まえて行うことが必要であり、意図する使用環境をシステム構成図やネットワーク構成図等を用いて明示することで確認すること。

### （3）JIS T 81001-5-1の箇条6のソフトウェア保守プロセスについて

基本要件基準第12条第3項に規定する「医療機器のライフサイクルの全てにおいて、サイバーセキュリティを確保するための計画」として、ソフトウェア保守計画において、サポート終了等の製品寿命に対して計画し、脆弱性の監視、セキュリティ更新等の将来的な脆弱性対策の実施計画等をあらかじめ定めておき、その計画の一環として顧客に対するセキュリティ更新の通知方針を明確化すること。

### （4）JIS T 81001-5-1の箇条8のソフトウェア構成管理プロセスについて

構成管理プロセスは、当該医療機器のソフトウェア部品表（SBOM）を適切に作成することによって確認すること。

# ３）医療機器の基本要件基準第12条第3項の適用に関する質疑応答集（Q&A）について

令和5年 7月20日　事務連絡

薬機法第41条第3項の規定により厚生労働大臣が定める医療機器の基準の一部を改正する件」（令和5年厚生労働省告示第67号）による改正後の「医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律第41条第3項の規定により厚生労働大臣が定める医療機器の基準」（平成17年厚生労働省告示第122号。以下「基本要件基準」という。）第12条第3項については、「医療機器の基本要件基準第12条第3項の適用について」（令和5年3月31日付け薬生機審発0331第8号）にて取扱いを、「医療機器の基本要件基準第12条第3項の適合性の確認について」（令和5年5月23日付け薬生機審発0523第1号）にて適合性の確認を示しているところです。

　今般、医療機器の基本要件基準第12条第3項の適用に関する質疑応答集を別紙のとおり取りまとめましたので、貴管内の製造販売業者において浸透が図られるよう、周知方御配慮願います。

別紙

医療機器の基本要件基準第12条第3項の適用に関する質疑応答集（Q&A）

**【用いた略語】**

**基本要件基準**：「医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律第41条第3項の規定により厚生労働大臣が定める医療機器の基準」（平成17年厚生労働省告示第122号）

**確保通知**　：平成27年4月28日付け薬食機参発0428第1号・薬食安発0428第1号厚生労働省大臣官房参事官（医療機器・再生医療等製品審査管理担当）・医薬食品局安全対策課長連名通知「医療機器におけるサイバーセキュリティの確保について」

**ガイダンス通知**：平成30年7月24日付け薬生機審発0724第1号・薬生安発0724第1号厚生労働省医薬・生活衛生局医療機器審査管理課長・医薬安全対策課長連名通知「医療機器のサイバーセキュリティの確保に関するガイダンスについて」

**取扱い通知**　：令和5年3月31日付け薬生機審発0331第8号厚生労働省医薬・生活衛生局医療機器審査管理課長通知「医療機器の基本要件基準第12条第3項の適用について」

**製販向け手引書通知**：令和5年3月31日付け薬生機審発0331第11号・薬生安発0331第4号厚生労働省医薬・生活衛生局医療機器審査管理課長・医薬安全対策課長連名通知「医療機器のサイバーセキュリティ導入に関する手引書の改訂について」

**適合性確認通知**：令和5年5月23日付け薬生機審発0523第1号厚生労働省医薬・生活衛生局医療機器審査管理課長通知「医療機器の基本要件基準第12条第3項の適合性の確認について」

**JIS T 81001-5-1**：JIS T 81001-5-1「ヘルスソフトウェア及びヘルスITシステムの安全有効性及びセキュリティ―第5-1部：セキュリティー製品ライフサイクルにおけるアクティビティ」

**Q1：取扱い通知にて、基本要件基準に新たに設定された条項の解釈が示されているが、その後に発出された適合性確認通知はどのような位置づけか。**

A1：適合性確認通知は、取扱い通知で示されている「JIS T 81001-5-1等への適合性を示す資料」をより具体的にした通知であり、基本要件基準への適合を示すために、JIS T 81001-5-1以外にも既存のサイバーセキュリティに関する通知にて求めてきた要件もあわせて記載し、医療機器におけるサイバーセキュリティへの対応の具体的な要件として示している。例えば、「セキュリティに対する窓口の明確化」、「顧客に対する脆弱性等の開示手順」はJIS T 81001-5-1の要求に明示的には含まれていないが、適合性確認通知による要求事項として対応する必要があり、具体的にはガイダンス通知にて示されている。

**Q2：「高度管理医療機器又は管理医療機器の承認申請又は認証申請を行う製造販売業者等は、当該医療機器について基本要件基準第12条第3項への適合を示すため、JIS T 81001-5-1等への適合性を確認する際に、次の事項について留意して、その結果を示すか又は結果をまとめた社内文書等を特定すること」とは、適合性確認通知の1の（1）～（6）及び2の（1）～（4）のそれぞれの要件に対して、文書番号等の社内文書を特定する情報を示すことでよいか。**

A2：貴見のとおり。別添の記載事例を参照とし、承認（認証）申請書添付資料4項の電気安全・電磁両立（ソフトウェアライフサイクルの後ろ）に記載する。なお、現在既に製造販売されている医療機器であって、令和6年4月1日以降も引き続き製造販売する医療機器についても、改正後の基本要件基準への適合を確認する上では、適合性確認通知の1の（1）～（6）及び2の（1）～（4）のそれぞれの要件に対する社内文書を特定する情報を提示できるようにしておくこと。

**Q3：製造販売承認・認証・届出済みで今後も製造販売する予定の品目であるが、JIS T 81001-5-1を適用して開発していない既存品目に関しては、JIS T 81001-5-1の附属書Fトランジションヘルスソフトウェアを適用することでよいか。**

A3：貴見のとおり。適合性確認通知の1の（1）～（6）の要件に対して、JIS T 81001-5-1の附属書Fトランジションヘルスソフトウェアにあるように、「セキュリティ運用ガイドラインを更新する」、「補完的コントロールを義務付ける」、「ヘルスソフトウェアの一部を書き直す」などの対策も可能である。なお、セキュリティに関するリスクアセスメントを行い、リスク評価の結果、受容できないリスクがないことを確認すること。医療機器外部の補完的対策が必須になる場合もあり、リスクが受容できないと判断された場合は、医療機器製造販売業者が医療機関に対して当該医療機器使用の中止勧告を検討すること。

また、JIS T 81001-5-1の附属書Fトランジションヘルスソフトウェアを適用する場合は、その旨を承認（認証）申請書添付資料4項に記載すること。

**Q4：「セキュリティに対する問い合わせ窓口を明確化」とは、具体的にどのようなことが求められるのか。承認・認証申請時には、どのように示すことが想定されるか。**

A4：「問い合わせ窓口」は、セキュリティに関して緊急に対応できる窓口（連絡先）の設定が想定され、例えば、医療機器製造販売業者のホームページにあるセキュリティポリシー、取扱説明書、又は注意事項等情報等に、セキュリティに関して緊急で対応できる窓口（連絡先）であることがわかるように記載することが望ましい。注意事項等情報として記載する場合は、「製造販売業者及び製造業者の氏名又は名称等」欄に記載すること。
また、承認・認証申請時に適合していることを示す方法としては、窓口を明確にしている文書名を示すことが想定される。

**Q5：JIS T 81001-5-1の箇条8の構成管理プロセスでは、当該医療機器のソフトウェア部品表（SBOM）を適切に作成するとあるが、このSBOMを承認・認証申請時に提出する必要があるか。**

A5：申請時に提出する必要はないが、承認・認証申請時にはSBOMを作成していることを明示する必要があり、例えばSBOMの文書名を記載する。なお、申請の際はSBOMを提示できるように準備しておくこと。

**Q6：SBOMの構成として定められているものはあるか。**

A6：SBOMは、JIS T 81001-5-1の箇条8の構成管理プロセスが対象としている全てのコンポーネント（ソフトウェアアイテム）で、自社製（開発委託したものも含む）及び外部調達ソフトウェア（OSS（オープンソースソフトウェア）を含む）が含まれるように作成すること。少なくとも製品の最上位のコンポーネント及びそれに直接含まれるコンポーネントの情報を含めること。
また、コンポーネントの各々について、①サプライヤの名前、②コンポーネントの名前、③バージョン、④固有識別子、⑤上流のコンポーネントとの関係、⑥作成者名（これらの情報を作成した組織名または担当者名）、⑦タイムスタンプ（情報を登録した日時）を明示すること。
（製販向け手引書通知の附属書Aソフトウェア部品表（SBOM）の扱い参照）

**Q7：ソフトウェアシステム試験にてセキュリティ要求事項を満たし有効であることを確認するとあるが、セキュリティを確認する試験は、第三者試験であることが必要か。**

A7：リスクマネジメントプロセスで特定した脅威に対する方法が実装され、有効であることが確認できれば第三者試験であることは必須ではない。

別　添

記載事例

**2.基本要件と基本要件への適合性**

**2.1 参照規格一覧**

基本要件への適合性を示すために用いた規格

| |
|---|
| JIS T 14971:2020 医療機器-リスクマネジメントの医療機器への適用 |
| … |
| JIS T 2304:2017 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 |
| JIS T 81001-5-1:2023 ヘルスソフトウェア及びヘルス IT システムの安全, 有効性及びセキュリティー第 5-1 部:セキュリティー製品ライフサイクルにおけるアクティビティ |
| … |

＜省略＞

**第二章　設計及び製造要求事項**

| 基本要件 | 当該機器への適用・不適用 | 適合の方法 | 特定文書の確認 | 該当する社内文書番号等 |
|---|---|---|---|---|
| (プログラムを用いた医療機器に対する配慮) | | | | |
| 第十二条　プログラムを用いた医療機器(医療機器プログラム又はこれを記録した記録媒体たる医療機器を含む。以下同じ。)は、その使用目的に照らし、システムの再現性、信頼性及び性能が確保されるよう設計されていなければならない。また、システムに一つでも故障が発生した場合、当該故障から生じる可能性がある危険性を、合理的に実行可能な限り除去又は低減できるよう、適切な手段が講じられていなければならない。 | 適用 | 認知された基準に適合することを示す。<br><br>認知された規格に従ってリスク管理が計画・実施されていることを示す。 | 医療機器及び体外診断用医薬品の製造管理及び品質管理の基準に関する省令(平成16年度厚生労働省令第169号)<br><br>JIST14971:「医療機器-リスクマネジメントの医療機器への適用」 | 本添付資料「2.4 適合宣言書」<br><br>本添付資料6. リスクマネジメント |
| 2　プログラムを用いた医療機器については、最新の技術に基づく開発のライフサイクル、リスクマネジメント並びに当該医療機器を適切に動作させるための確認及び検証の方法を考慮し、その品質及び性能についての検証が実施されていなければならない。 | 適用 | 認知された規格の該当する項目に適合することを示す。<br><br>認知された規格に従ってリスク管理が計画・実施されていることを示す。 | JIS T 2304:「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トセス」<br><br>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」 | 本添付資料4. (3) JIS T 2304 の実施状況<br><br>本添付資料6. リスクマネジメント |
| 3　プログラムを用いた医療機器のうち、他の機器及びネットワーク等と接続して使用する医療機器又は外部からの不正アクセス及び攻撃アクセス等が想定される医療機器については、当該医療機器における動作環境及びネットワークの使用環境等 | 適用 | 認知された基準の該当する項目に適合することを示す。 | 医療機器の基本要件基準第12条第3項の適合性の確認について(薬生機審発0523第1号:令和5年5月23日) | 本添付資料4. (4) JIS T 81001-5-1 の実施状況 |



| | | | | |
|---|---|---|---|---|
| を踏まえて適切な要件を特定し、当該医療機器の機能に支障が生じる又は安全性の懸念が生じるサイバーセキュリティに係る危険性を特定及び評価するとともに、当該危険性が低減する管理が行われていなければならない。また、当該医療機器は、当該医療機器のライフサイクルの全てにおいて、サイバーセキュリティを確保するための計画に基づいて設計及び製造されていなければならない。 | | | | |

＜省略＞

**2.3 適合性を確認するために用いた規格等の適用に関する妥当性説明**

＜省略＞

**2.4 適合宣誓書**

本資料に適合宣言書を添付する。

**4. 設計検証及び妥当性確認文書の要約**

＜省略＞

**4.3 適合性認証基準等に適合することを証明する資料**

**(1) 基本要件第 6 条への適合性を示す資料**

＜省略＞

**(3) JIS T 2304 の実施状況**

＜省略＞

**(4) JIS T 81001-5-1 の実施状況**

| JIS T 81001-5-1 の確認項目 | | 記載文書 |
|---|---|---|
| 4 | 一般要求事項 | 規程の各要求事項に対して、「医療機器の基本要件基準第 12 条第3項の適合性の確認について」(薬生機審発 0523 第 1 号:令和5年 5 月 23 日)に示す内容も含めて、別添資料1に示す通り、関連する文書を調査し、適合性を確認した。(別添資料1参照) |
| 5 | ソフトウェア開発プロセス | |
| 6 | ソフトウェア保守プロセス | |
| 7 | セキュリティに関連するリスクマネジメントプロセス | |
| 8 | ソフトウェア構成管理プロセス | |
| 9 | ソフトウェア問題解決プロセス | |

**別添資料1**

サイバーセキュリティに関する概要報告書

販売名「○○○」

適合規格及び関連通知
JIS T 81001-5-1:2023
医療機器の基本要件基準第12条第3項の適合性の確認について
（薬生機審発0523第1号：令和5年5月23日）

| 文書番号 | | ××××－××× |
|---|---|---|
| 作成 | 令和○○年○月○日 | □□ □□ |
| 承認 | 令和○○年○月△日 | △△ △△ |

株式会社　××××

7

サイバーセキュリティへの適合に関する調査は社内規定通り実施され、結果は下記の通り資料が作成されている。

| | JIS T 81001-5-1 の確認項目 | 実施内容概要 | 社内ドキュメント名 | 文書番号 |
|---|---|---|---|---|
| 1 | **一般要求事項** | サイバーセキュリティの確保に係る活動は、品質マネジメントシステムに基づいて行われていること。 | ・サイバーセキュリティ対応手順書 | 社内文書〇〇 |
| | | 規制当局及び顧客に対して脆弱性を適時に通知する活動を確立すること。 | ・サイバーセキュリティ対応手順書 | 社内文書〇〇 |
| | | 品質マネジメントシステムにおいて、セキュリティに対する対応方針、セキュリティに対する問い合わせ窓口を明確化し、顧客に対する脆弱性等の開示手順が定められていること。 | ・サイバーセキュリティ対応手順書 | 社内文書〇〇 |
| | | 医療機器のリスクマネジメントは、セキュリティの脆弱性、脅威等を考慮したものであること。 | ・サイバーセキュリティリスクマネジメント報告書 | 社内文書〇〇 |
| 2 | **ソフトウェア開発プロセス** | 開発計画において、セキュリティ更新や開発環境等のセキュリティについて考慮すること。 | ・ソフトウェア開発計画書 | 社内文書〇〇 |
| | | 製品のセキュリティ機能を含むセキュリティ要求事項を特定すること。 | ・ソフトウェア開発計画書 | 社内文書〇〇 |
| | | 意図する使用環境、信頼境界、多層防御等を考慮してアーキテクチャー設計を行うこと。 | ・ソフトウェア設計文書 | 社内文書〇〇 |
| | | 意図する使用環境をシステム構成図やネットワーク構成図等を用いて明示すること。 | ・システム構成図（信頼境界含む） | 社内文書〇〇 |
| | | セキュリティ設計のベストプラクティスを考慮した設計及び実装を行うこと。 | ・ソフトウェア設計文書 | 社内文書〇〇 |
| | | ソフトウェアシステム試験を行って、セキュリティ要求事項が満たされ、リスクマネジメントプロセスで特定した脅威に対応する方法が設計に実装され、有効であること。 | ・システム試験成績書 | 社内文書〇〇 |
| 3 | **ソフトウェア保守プロセス** | 顧客に対するセキュリティ更新の通知方針について定めておくこと。 | ・ソフトウェア保守計画書 | 社内文書〇〇 |
| | | ソフトウェア保守計画において、サポート終了等の製品寿命に対して計画し、脆弱性の監視、セキュリティ更新 | ・ソフトウェア保守計画書 | 社内文書〇〇 |

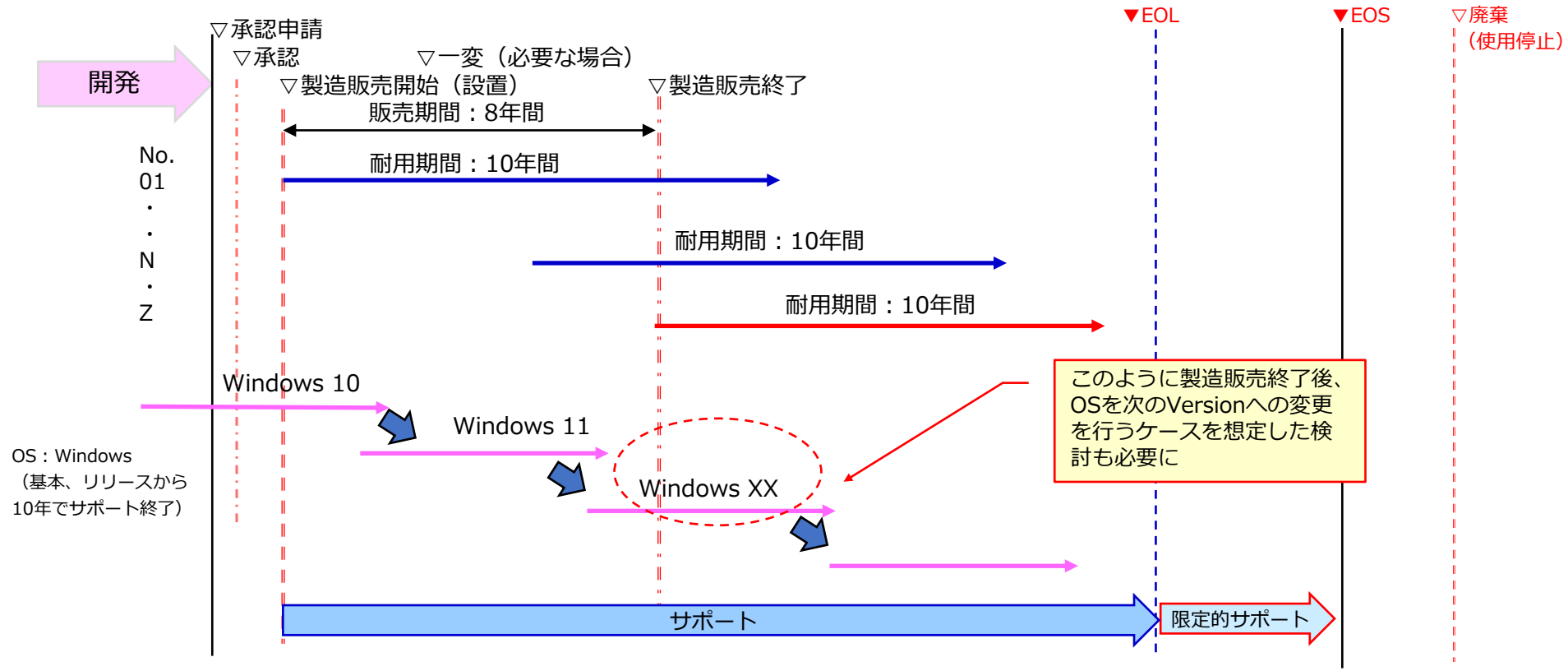


| | | | | |
|---|---|---|---|---|
| | | 等のための計画を行い、その計画の一環として顧客に対するセキュリティ更新の通知方針を明確化すること。 | | |
| 4 | **セキュリティに関連するリスクマネジメントプロセス** | 医療機器のリスクマネジメントにおいて、医療機器の意図する使用及び使用環境を考慮して、関連する脆弱性を特定し、関連する脅威を推定して評価し、リスクコントロール手段によって脅威をコントロールし、その有効性を監視すること。 | ・サイバーセキュリティリスクマネジメント報告書 | 社内文書〇〇 |
| 5 | **ソフトウェア構成管理プロセス** | 医療機器の開発、保守及びサポートのための、変更管理及び変更履歴を伴う構成管理プロセスを確立すること。 | ・ソフトウェア構成管理プロセス手順書 | 社内文書〇〇 |
| | | 構成管理プロセスは、当該医療機器のソフトウェア部品表（SBOM）を適切に作成すること。 | ・SBOM | 社内文書〇〇 |
| 6 | **ソフトウェア問題解決プロセス** | セキュリティの脆弱性に関する情報伝達、処理の手順を定め、セキュリティ問題に対して、情報開示 を含めて手順に従って実施していること。 | ・サイバーセキュリティ脆弱性対応手順書 | 社内文書〇〇 |

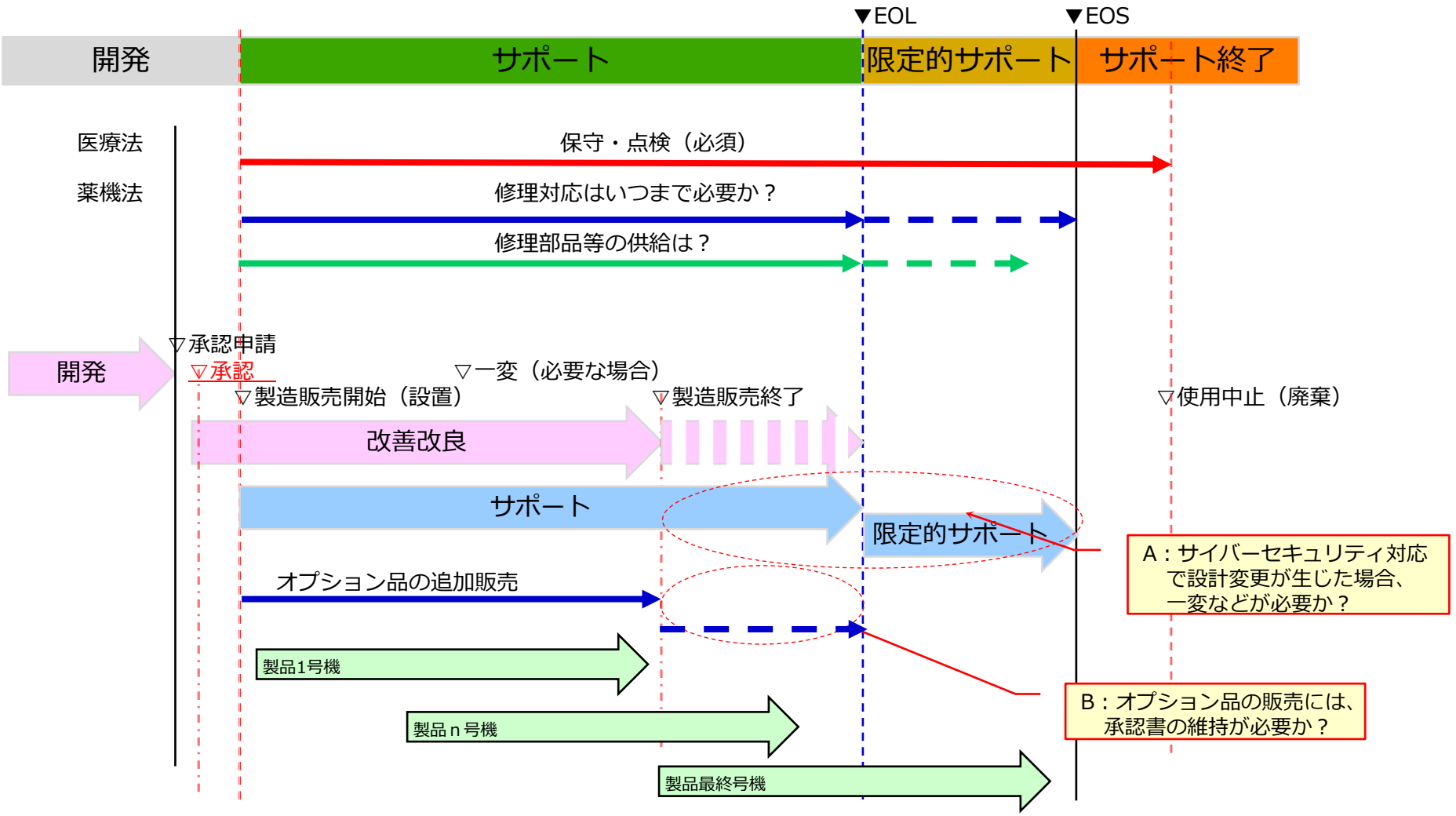
# 開発時：製品の耐用期間、販売期間の明確化

製品の耐用期間、販売期間を利用するOSのサポート期間を踏まえ、計画が重要に

・耐用期間：10年、販売期間を8年とした場合、最終製品を製造販売してから10年間はサポートが必要に



# EOL、EOS、耐用期間について



# Ⅴ．ユーザビリティ

1）JIS T62366-1制定に伴う薬機法上の取扱い　（令和元年）
2）JIS T62366-1改正に伴う薬機法上の取扱い　（令和４年）
3）ユーザビリティの定義
4）ユーザビリティ、ユーザビリティエンジニアリング
5）ユーザビリティエンジニアリング適用による期待される効果
6）『使用』の種類の関係

# 1）JIS T62366-1制定に伴う薬機法上の取扱い

令和元年

令和元年10月1日 薬生機審発1001第1号 薬生監発1001第1号

薬生機審発1001第1号
薬生監麻発1001第5号
令和元年10月1日

各都道府県衛生主管部（局）長　殿

厚生労働省医薬・生活衛生局医療機器審査管理課長
（　　公　　印　　省　　略　　）

厚生労働省医薬・生活衛生局監視指導・麻薬対策課長
（　　公　　印　　省　　略　　）

ユーザビリティエンジニアリングの医療機器への適用に関する日本産業規格の制定に伴う医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律上の取扱いについて

人間工学的特性に関連した傷害の危険性や人間工学的特性に起因した誤使用の危険性等に対して、合理的かつ適切に除去又は低減されるように医療機器を設計及び製造しなければならないことは、薬事法第四十一条第三項の規程により厚生労働大臣が定める基準（平成17年厚生労働省告示第122号。以下「基本要件」という。）第9条、第16条等において定められているところです。

今般、産業標準化法（昭和24年法律第185号）に基づく日本産業規格「医療機器－第1部：ユーザビリティエンジニアリングの医療機器への適用（ＪＩＳ　Ｔ６２３６６－１：２０１９）」が発行されたことに伴い、医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律（昭和35年法律第145号）における取扱いを下記のとおり定めましたので、貴管下関係事業者に周知願います。

なお、本通知の写しを各地方厚生局長、独立行政法人医薬品医療機器総合機構理事長、一般社団法人日本医療機器産業連合会会長、一般社団法人日本臨床検査薬協会会長、一般社団法人米国医療機器・IVD 工業会会長、欧州ビジネス協会医療機器・IVD委員会委員長、医薬品医療機器等法登録認証機関協議会代表幹事あて送付することとしています。

1．基本要件におけるJIS T62366-1の取扱いについて

基本要件第9条、第16条等で規定する事項を考慮した設計及び製造において、JIS T62366-1で規定するユーザビリティエンジニアリングプロセスを適用しても差し支えないこと。当該規格を適用した場合には、承認申請書又は認証申請書に添付する資料などにより、当該規格を適用している旨説明すること。

なお、令和4年9月30日までに、当該規格を適用したプロセスを構築することが望ましい。

2．医療機器及び体外診断用医薬品の製造管理及び品質管理の基準に関する省令（平成16年厚生労働省令第169号。以下「QMS省令」という。）におけるJIS T62366-1の取扱いについて

上記1によりJIS T62366-1を適用した場合には、QMS省令第26条で規定する製品実現、第30条から第36条で規定する設計開発等において、当該規格を遵守した活動を実施しているかを確認する場合があること。

本通知は、通知2の発出にて廃止

# 2）JIS T62366-1改正に伴う薬機法上の取扱い

令和４年

令和4年9月30日 薬生機審発0930第1号 薬生監発0930第1号

薬生機審発 0930 第１号
薬生監麻発 0930 第１号
令 和 ４ 年 ９ 月 30 日

各都道府県衛生主管部（局）長　殿

厚生労働省医薬・生活衛生局医療機器審査管理課長
（　　公　　印　　省　　略　　）

厚生労働省医薬・生活衛生局監視指導・麻薬対策課長
（　　公　　印　　省　　略　　）

医療機器のユーザビリティエンジニアリングに係る要求事項に関する
日本産業規格の改正の取扱いについて

医療機器のユーザビリティエンジニアリングに係る「医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律第四十一条第三項の規定により厚生労働大臣が定める医療機器の基準」（平成 17 年厚生労働省告示第 122 号。以下「基本要件基準」という。）の適用については、「ユーザビリティエンジニアリングの医療機器への適用に関する日本産業規格の制定に伴う医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律上の取扱いについて」（令和元年 10 月１日付け薬生機審発 1001 第１号・薬生監麻発 1001 第５号、厚生労働省医薬・生活衛生局医療機器審査管理課長及び監視指導・麻薬対策課長連名通知。以下「令和元年課長通知」という。）において、日本産業規格「医療機器－第１部：ユーザビリティエンジニアリングの医療機器への適用」（JIS T 62366-1：2019）の取扱いを示しているところです。

今般、JIS T 62366-1 の引用規格である「医療機器－リスクマネジメントの医療機器への適用」（JIS T 14971）において、ユーザビリティ等の分野への適用を明確化した改正が行われたこと等を受け、JIS T 62366-1:2022（以下「改正後の JIS」という。）へ改正されました。これに伴い、「医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律」（昭和 35 年法律第 145 号。以下「法」という。）における取扱いを下記のとおり定めましたので、御了知の上、貴管内関係団体、関係機関等に周知いただきますよう御配慮願います。なお、本通知は令和４年 10 月１日より適用することとし、本通知の適用に伴い、令和元年課長通知は廃止します。

記

**1．基本要件基準への適合性確認について**

（1）製造販売業者、外国製造医療機器等特例承認取得者又は外国指定高度管理医療機器製造等事業者（以下「製造販売業者等」という。）は、令和6年3月31日（以下「経過措置期間終了日」という。）の翌日以降に、製造販売される医療機器に対して、改正後のJISへの適合をもって基本要件基準第9条、第16条等で規定するユーザビリティに係る事項への適合の確認を行う体制を整備すること。

なお、経過措置期間終了日までに改正後のJISに適合するよう手順書改訂など、必要な措置を講ずること。

（2）改正後のJISの他、国際的に用いられている適切な規格等がある場合については、それらの規格等への適合性を確認することをもって基本要件基準第9条、第16条等への適合を確認したものとして差し支えないこと。新規の承認申請又は認証申請（承認事項一部変更承認申請及び認証事項一部変更認証申請を含む。以下「承認申請等」という。）に際しては、それらの規格等を用いることの妥当性を説明すること。

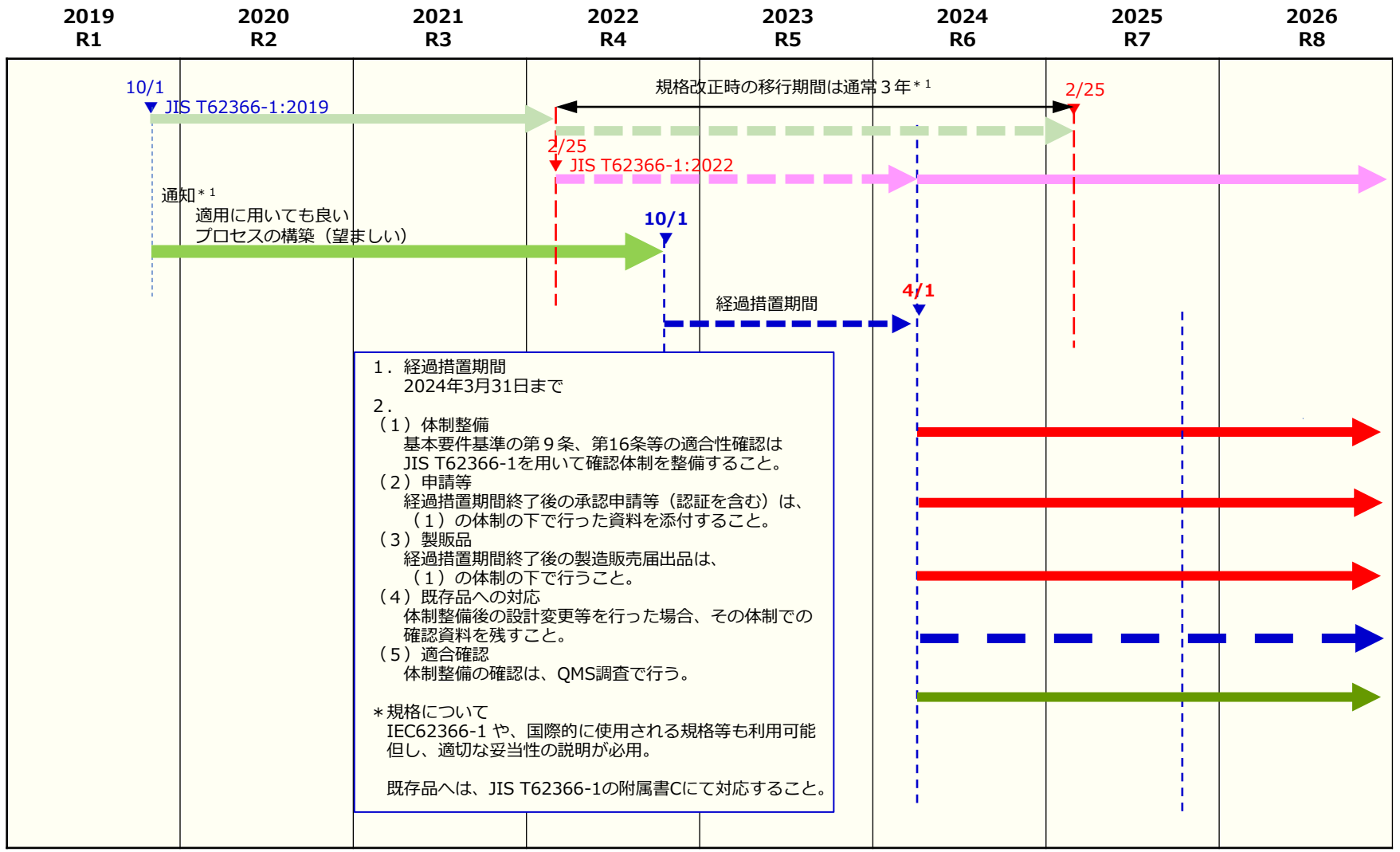
（3）経過措置期間終了日の翌日以降に、高度管理医療機器又は管理医療機器の承認申請又は認証申請を行う製造販売業者等は、当該医療機器について上記（1）で整備した体制で適合性を確認すること。承認申請等の添付資料において改正後のJISへの適合性を説明すること。

（4）経過措置期間終了日の翌日以降に製造販売届出を提出する場合についても、上記（1）で整備した体制で適合性を確認すること。

**2．製造販売業者等は、医療機器及び体外診断用医薬品の製造管理及び品質管理の基準に関する省令**（平成16年厚生労働省令第169号）第26条で規定する製品実現及び第30条から第36条で規定する設計開発等において、改正後のJISに基づく活動を行い、その適合に関する確認等を適切に記録し保管すること。

なお、法第23条の2の5第7項又は第23条の2の23第4項の規定による調査の調査権者の求めなどに応じて資料を提示し、適切な説明を行わなければならないこと。

# ※　JIS T62366-1:2022 への適合要求




＊１：規格改正時の移行期間は通常３年（共通規格のJIS T0601-１やJIS T0601-1-2などは５年）

# 3）ユーザビリティの定義

JIS規格（JIS T62366-1）

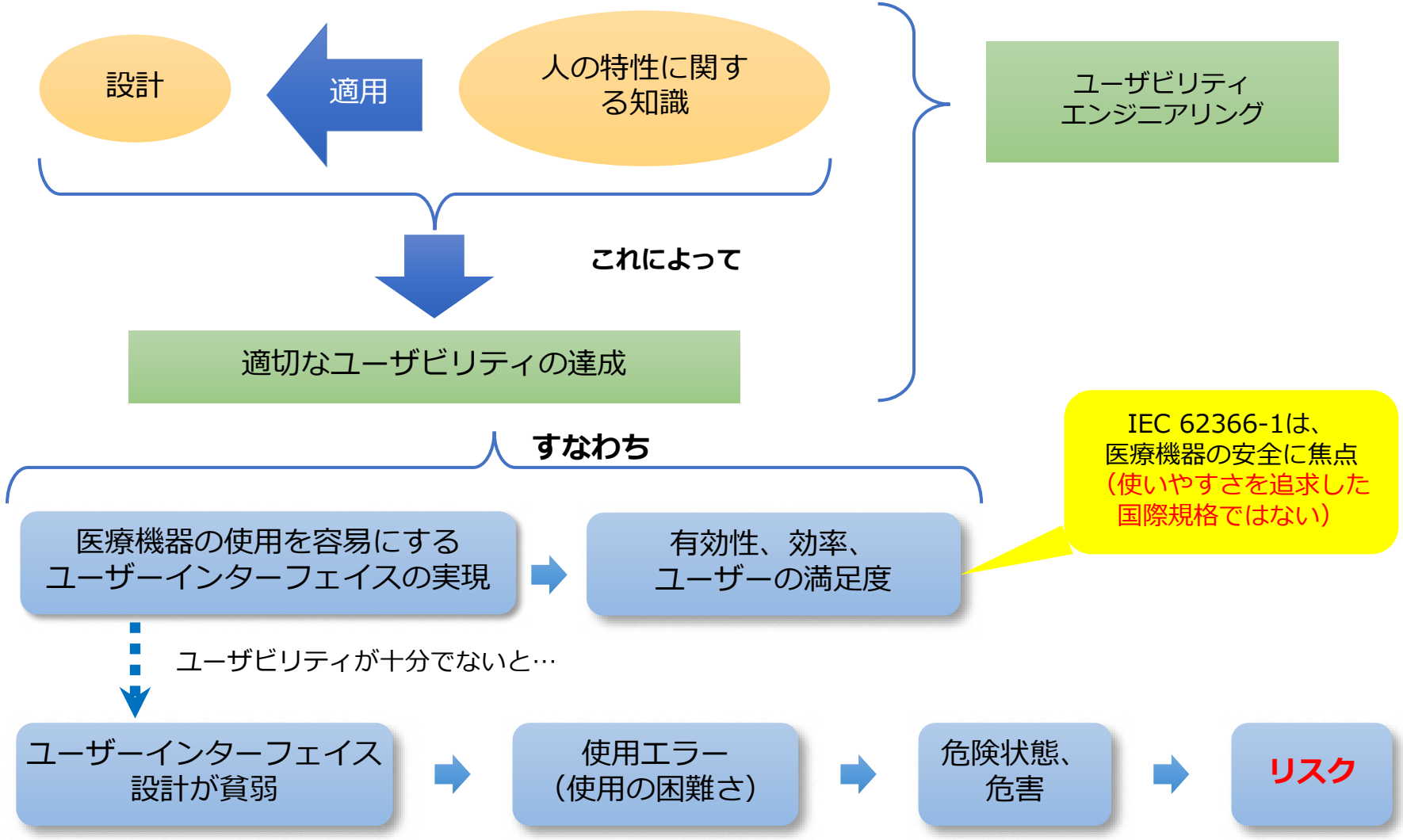
**ユーザビリティ（Usability）：**意図する使用環境における使用を容易にし、有効性、効率、及びユーザーの満足度を確立するユーザーインターフェースの特性

注釈１：有効性、効率及びユーザーの満足度を含むユーザビリティの全ての側面は、安全を向上又は低下させることがある。

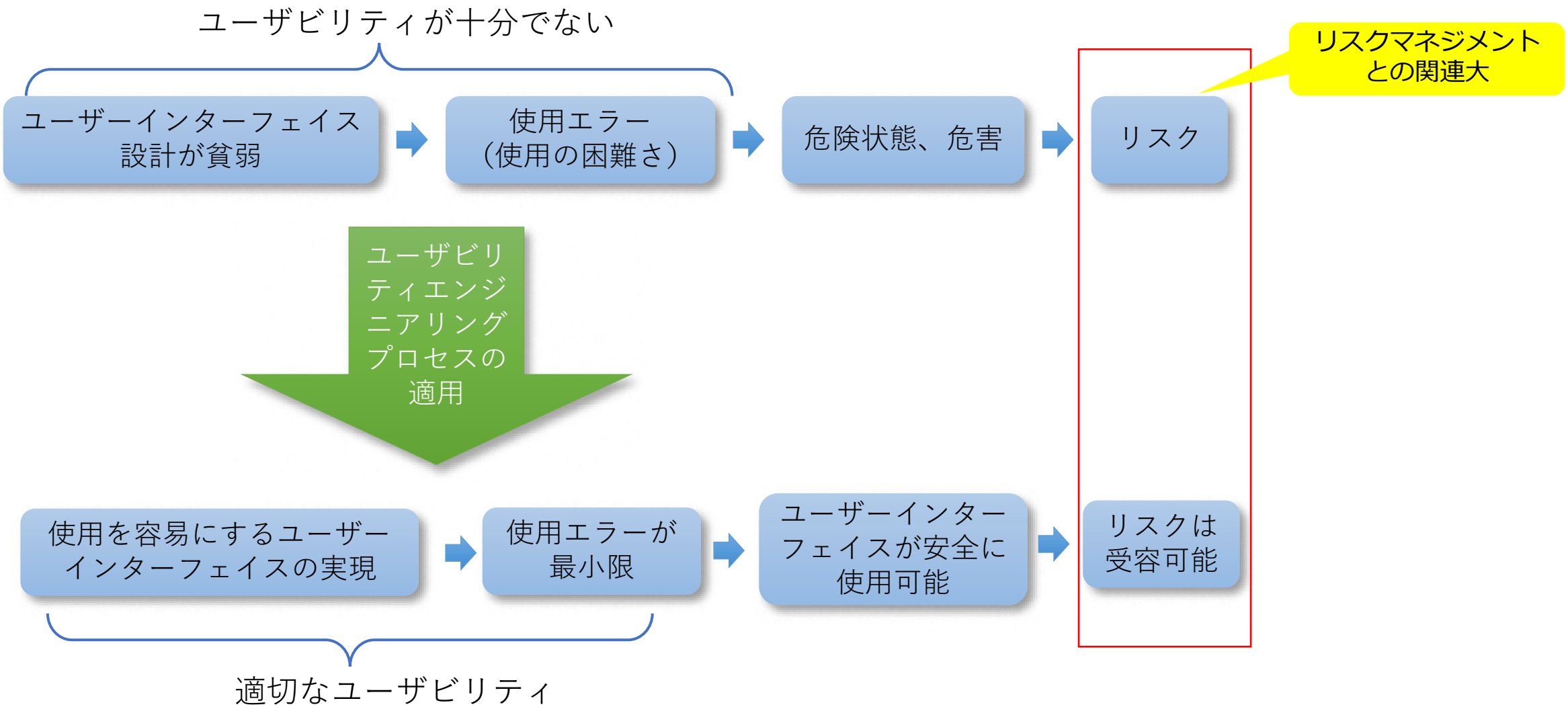
ＱＭＳ省令
（定義）
第2条
26　この省令で「使用性」とは、製品に係る医療機器等の特性のうち、使用者による安全かつ適正な使用又は操作のために必要であって、意図した用途に応じた機能、性能及び安全性が十分に発揮され、かつ、使用者の要求を充足させるために必要な性質をいう。

局長通知（令和3年 3月26日　薬生監麻発0326第4号）
（26）「使用性」とは、ISO13485:2016の「Usability」に相当するものであり、製品に係る医療機器等の特性のうち、使用者による安全かつ適正な使用又は操作のために必要なものであって、意図した用途に応じた機能、性能及び安全性が十分に発揮され、かつ、使用者の要求を充足させるために必要な性質をいうものであること。

# 4）ユーザビリティ、ユーザビリティエンジニアリング



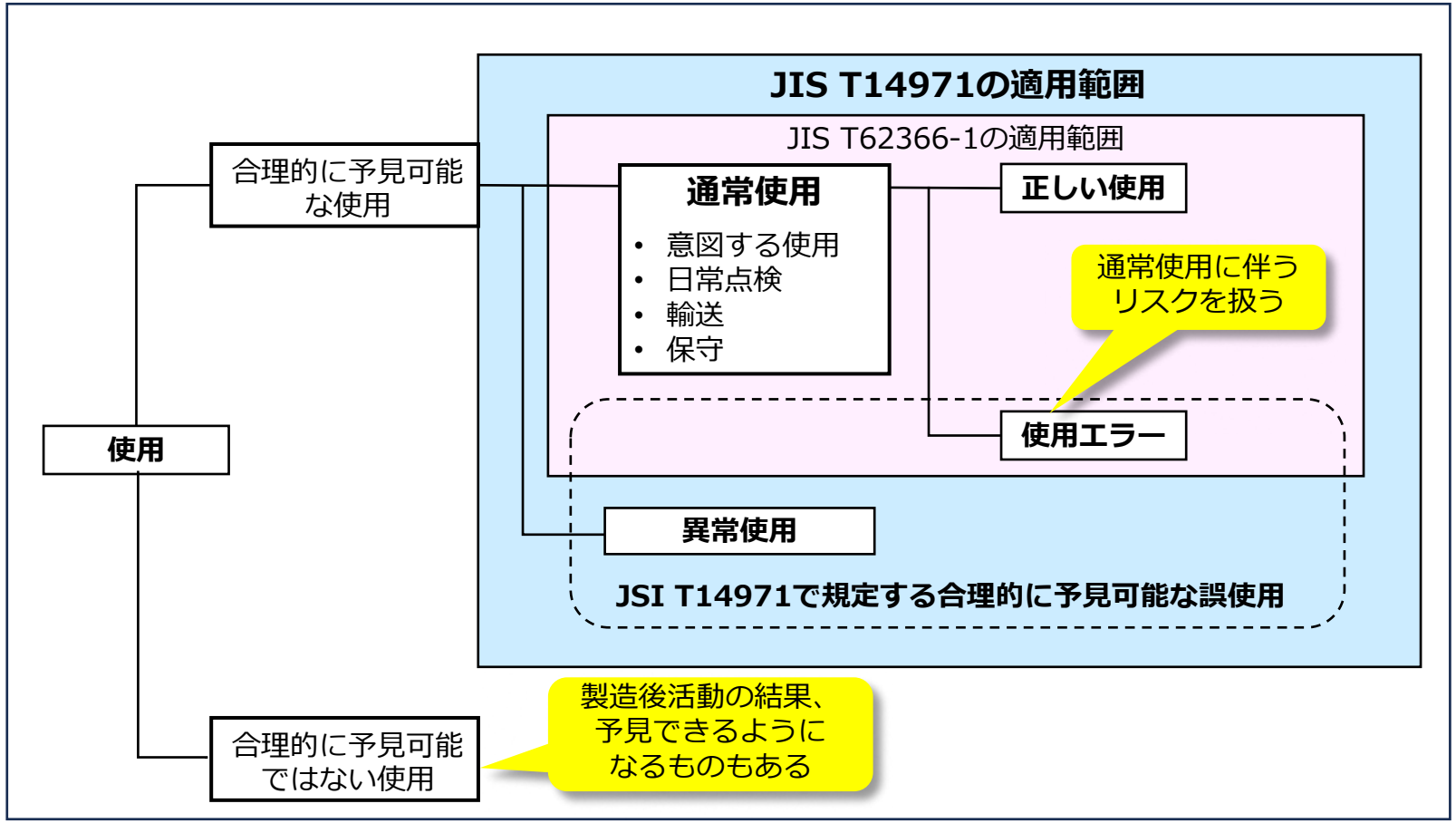
# 5）ユーザビリティエンジニアリング適用による期待される効果



# 6）『使用』の種類の関係

**医療機器**の使用（MEDICAL DEVICE use）

- **通常使用**（NORMAL USE）
  - **正しい使用**（CORRECT USE）
  - **使用エラー**（USE ERROR）
- **異常使用**（ABNORMAL USE）



# ユーザビリティエンジニアリングに係る基本要件基準の適用（Q&A）

医療機器のユーザビリティエンジニアリングに係る・・・基本要件基準・・・の適用については、「医療機器のユーザビリティエンジニアリングに係る要求事項に関する日本産業規格の改正の取扱いについて」（令和4年9月30日付け薬生機審発0930第1号・薬生監麻発0930第1号、厚生労働省医薬・生活衛生局医療機器審査管理課長及び監視指導・麻薬対策課長連名通知）において、日本産業規格「医療機器－第1部：ユーザビリティエンジニアリングの医療機器への適用」・・・改正後のJIS・・・の取扱いを示しているところです。

今般、医療機器のユーザビリティエンジニアリングに係る基本要件基準の適用に関する質疑応答集を別紙のとおり取りまとめましたので、貴管内の製造販売業者において浸透が図られるよう、周知方御配慮願います。

【別紙】

医療機器のユーザビリティエンジニアリングに係る基本要件基準の適用に関する質疑応答集（Q&A）

Q1:「基本要件基準第9条、第16条等」の「等」は何か。
A1:第9条第4項第1号、第2号及び第16条の他に、ユーザビリティに関連する内容が条文に含まれる条項としては、医療機器の特性によるが、例えば第10条第4項、第5項、第15条第3項及び第17条が挙げられる。

Q2:「ユーザビリティに係る事項への適合の確認を行う体制」とはどのようなものか。

A2:QMS省令で規定する使用性に関し、改正後のJIS等に適合するため、製造販売業者等がリスクマネジメントを含む製品実現や設計開発に係る手順書の改訂等を行い、適合性の確認を行う体制のことである。なお、製造販売業者と設計製造業者が異なる場合、設計製造業者がQMS省令に基づき、使用性について改正後のJIS等を適用した体制を整備し、製造販売業者が設計製造業者による適合性確認の記録を確認し、その適切性を根拠に基づいて説明できるようにするなど、改正後のJIS等への適合性確認を行える体制を整備しておくことでもよい。

Q3:「令和6年3月31日（以下「経過措置期間終了日」という。）の翌日以降に、製造販売される医療機器に対して、改正後のJISへの適合をもって基本要件基準第9条、第16条等で規定するユーザビリティに係る事項への適合の確認を行う体制を整備すること。」とあるが、要求事項は手順書改訂や実施組織の体制整備までであり、個々の品目についての記録書等、適合性の証左の作成までは不要との理解でよいか。

A3:貴見のとおり。

なお、体制整備等を行った手順書（改訂版）の適用日（遅くとも令和6年4月1日）以降に、設計変更を行う際に改正後のJISを用いた適合記録を作成すること。

Q4:令和6年3月31日までに承認、認証及び届出がされている品目における改正後のJISの適用については、何を行えばよいか。

A4:令和6年3月31日までに承認、認証及び届出がされている品目に関しては、設計変更が生じた際などに、それぞれ整備された手順書に従いユーザビリティに関する適合性確認を行うこと。

なお、経過措置期間終了日までに設計・開発され、商品化したユーザーインターフェイス又はユーザーインターフェイスの一部については、開発過程が不明なユーザーインターフェイス(UOUP)とみなして、改正後のJISの附属書C「開発過程が不明なユーザーインターフェイス(UOUP)の評価」に基づいて適合性を判断し、設計変更された部分等に対しては、改正後のJISの5.1～5.9に従ってユーザビリティに関する適合性確認を行うことでもよい。

Q5:「改正後のJISの他、国際的に用いられている適切な規格等がある場合」とあるが、重要なのはこの規格への適用に限定することではなく、ユーザビリティに関する基本要件基準の要求を満たすことであって、JIS T 62366-1以外でもその適切性を説明できるのであれば差し支えないとの理解でよいか。

A5:貴見のとおり。ユーザビリティに関する基本要件基準の要求を満たすにあたり、JIS T 62366-1以外にその適切性を説明できる、国際的に認められている規格又は日本産業規格があれば、それを用いて差し支えない。（例えば、IEC 62366-1:2015及びAmendment1:2020, JIS T 60601-1-6:2023など。JIS T 60601-1-6の場合、要求事項はJIS T62366-1が引用されている。）

Q6:「経過措置期間終了日の翌日以降の承認申請等の添付資料において、改正後のJISへの適合性を証明すること」とあるが、添付資料にはどの項目に記載すればよいか。

A6:ユーザビリティに関する記述は、添付資料の設計検証及び妥当性確認文書の概要の項目に参照した規格（例えば、JIS T 62366-1）及び評価の概要を簡潔に記載すること。別添に改正後のJISを用いた場合の記載例を示すが、この記載に限るものではない。

Q7:「経過措置期間終了日の翌日以降に、高度管理医療機器又は管理医療機器の承認申請又は認証申請を行う」とあるが、申請日が経過措置中であれば、承認又は認証日が経過措置期間終了日の翌日以降となる見込みであっても、改正後のJISの適用及び適合性の説明は不要と考えてよいか。

A7:貴見のとおり。

Q8:例えば、製造所の変更・追加、滅菌方法の変更、有効期間の延長、ユーザビリティに影響しない原材料の供給業者変更やグレード変更、サイズの変更・追加については、ユーザビリティに影響がない一部変更申請と考えられる。このような場合には、基本要件のユーザビリティへの適合性に関する記載は不要との理解でよいか。

A8:貴見のとおり。ユーザビリティに影響しない変更の場合には、当該基本要件への適合性に影響を及ぼさないことから記載は不要である。なお、製造所迅速一変や有効期間延長等の明らかにユーザビリティに影響しない変更を除き、当該変更によりユーザビリティに影響がないことを承認（認証）申請書添付資料4項にて説明すること。

Q9:コンタクトレンズにおけるユーザーインターフェイスとは、どのようなものか。

A9:改正後のJISにおいて、ユーザーインターフェイスは「ユーザーと医療機器とがやり取りをする手段」と定義されている。例えば、コンタクトレンズの場合は、使用者が一般人であり、通常の使用方法を習得し使用エラーを防止する手段としては、添付文書や取扱説明書を含む附属文書もユーザーインターフェイスの一部とみなし、使用には教育やトレーニングの内容が含まれると考えられる。

なお、教育やトレーニングの必要性については、附属文書の適切性（例えば、コンタクトレンズの添付文書が平成28年6月20日厚生労働省医薬・生活衛生局安全対策課事務連絡「視力補正用及び非視力補正用コンタクトレンズの添付文書及び表示に関する自主基準の改定について」に従った内容で作成されたものである場合など）等により判断することで差し支えない。

**別添資料1**

ユーザビリティエンジニアリングプロセスへの適合に関する概要報告書

販売名「○○○」

適合規格:JIS T 62366-1:2022

| 文書番号 | | ××××－××× |
|---|---|---|
| 作成 | 令和○○年○月○日 | □□ □□ |
| 承認 | 令和○○年○月△日 | △△ △△ |

株式会社　××××



ユーザビリティエンジニアリングプロセスの各要求事項については、下記の文書を調査して適合性を確認した。

| JIS T 62366-1:2022 に規定するユーザビリティエンジニアリングプロセス | | 適合方法及び適合性検証結果 |
|---|---|---|
| 5.1 | 使用関連仕様の作成 | 使用関連仕様書(社内文書○○) |
| 5.2 | 安全に関連するユーザーインターフェイス特性及び潜在的な使用エラーの特定 | リスクマネジメントファイル(社内文書○○) |
| 5.3 | 既知の又は予見可能なハザード及び危険状態の特定 | リスクマネジメントファイル(社内文書○○) |
| 5.4 | ハザード関連使用シナリオの特定及び記述 | ハザード関連使用シナリオ(社内文書○○) |
| 5.5 | 総括的評価のためのハザード関連使用シナリオの選択 | 総括的評価計画書(社内文書○○) |
| 5.6 | ユーザーインターフェイス仕様の確立 | ユーザーインターフェイス仕様書(社内文書○○) |
| 5.7 | ユーザーインターフェイス評価計画の確立 | ユーザーインターフェイス評価計画書(社内文書○○) |
| 5.8 | ユーザーインターフェイス設計、実装及び形成的評価の実施 | 形成的評価報告書(社内文書○○) |
| 5.9 | ユーザーインターフェイスのユーザビリティに関する総括的評価の実施 | 総括的評価報告書(社内文書○○)、リスクマネジメント報告書(社内文書○○) |

記載事例は一例であり、適合の示し方は各社及び個々の製品特性により異なる。例えば、JIS T 62366-1 の 4.3「ユーザビリティエンジニアリング作業の調整」に基づき、個々の製品特性に応じて該当するユーザビリティエンジニアリングプロセスを適用し、検証の深さも個々の製品特性により異なることがある。

記載事例2

**2.基本要件と基本要件への適合性**

**2.1 参照規格一覧**

基本要件への適合性を示すために用いた規格

| |
|---|
| JIS T 14971:2020 医療機器-リスクマネジメントの医療機器への適用 |
| … |
| JIS T 62366-1:2022 医療機器－第 1 部:ユーザビリティエンジニアリングの医療機器への適用 |
| … |

＜省略＞

**第二章　設計及び製造要求事項**

| 基本要件 | 当該機器への適用・不適用 | 適合の方法 | 特定文書の確認 | 該当する社内文書番号等 |
|---|---|---|---|---|
| (使用環境に対する配慮) | | | | |
| 第九条 | | | | |
| 4 医療機器は、その使用に当たって患者、使用者及び第三者(医療機器の使用に当たって次の各号に掲げる危険性がある者に限る。)に生じる次の各号に掲げる危険性が、合理的かつ適切に除去又は低減されるように設計及び製造されなければならない。<br>一　物理的及び人間工学的特性に関連した傷害の危険性 | 適用 | 認知された規格に従ってリスク管理が計画・実施されていることを示す。<br><br>認知された規格の該当する項目に適合することを示す。 | 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」<br><br>JIS T 62366-1:「医療機器－第 1 部:ユーザビリティエンジニアリングの医療機器への適用」 | 本添付資料6．リスクマネジメント<br><br>本添付資料4．4 ユーザビリティ |
| 二　医療機器の意図された使用目的における人間工学的特性、人的要因及びその使用環境に起因した誤使用の危険性 | 適用 | 認知された規格に従ってリスク管理が計画・実施されていることを示す。<br><br>認知された規格の該当する項目に適合することを示す。 | 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」<br><br>JIS T 62366-1:「医療機器－第 1 部:ユーザビリティエンジニアリングの医療機器への適用」 | 本添付資料6．リスクマネジメント<br><br>本添付資料4．4 ユーザビリティ |
| (一般使用者が使用することを意図した医療機器に対する配慮) | | | | |
| 第十六条　一般使用者が使用することを意図した医療機器(医療機器のうち、自己検査医療機器又は自己投薬医療機器その他のその使用に当たり専門的な知識を必ずしも有しない者が使用することを意図したものをいう。以下同じ。)は、当 | 適用 | 認知された規格に従ってリスク管理が計画・実施されていることを示す。<br><br>認知された規格の該当する項目 | 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」<br><br>JIS T 62366-1:「医療機器－第 1 部: | 本添付資料6．リスクマネジメント<br><br>本添付資料4．4 ユーザビリティ |



| | | | | |
|---|---|---|---|---|
| 該医療機器の使用者が利用可能な技能及び手段並びに通常生じ得る使用者の技術及び環境の変化の影響に配慮し、用途に沿って適正に操作できるように設計及び製造されていなければならない。 | | に適合することを示す。 | ユーザビリティエンジニアリングの医療機器への適用」 | |
| 2　一般使用者が使用することを意図した医療機器は、当該医療機器の使用、検体の使用(検体を使用する当該医療機器に限る。)及び検査結果の解釈に当たって、使用者が誤使用する危険性を合理的に実行可能な限り低減するように設計及び製造されていなければならない。 | 適用 | 認知された規格に従ってリスク管理が計画・実施されていることを示す。<br><br>認知された規格の該当する項目に適合することを示す。 | 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」<br><br>JIS T 62366-1:「医療機器－第 1 部:ユーザビリティエンジニアリングの医療機器への適用」 | 本添付資料6．リスクマネジメント<br><br>本添付資料4．4 ユーザビリティ |

＜省略＞

**2.3 適合性を確認するために用いた規格等の適用に関する妥当性説明**

＜省略＞

**2.4 適合宣誓書**

＜省略＞

**4. 設計検証及び妥当性確認文書の要約**

＜省略＞

**4.4 ユーザビリティ**

実施状況

| JIS T 62366-1:2022 に規定するユーザビリティエンジニアリングプロセス | | 適合方法及び適合性検証結果 |
|---|---|---|
| 5.1 | 使用関連仕様の作成 | 各規定要求事項に対して、別添資料1に示す通り、関連する文書を調査し、適合性を確認した。(別添資料1参照) |
| 5.2 | 安全に関連するユーザーインターフェイス特性及び潜在的な使用エラーの特定 | |
| 5.3 | 既知の又は予見可能なハザード及び危険状態の特定 | |
| 5.4 | ハザード関連使用シナリオの特定及び記述 | |

| | | |
|---|---|---|
| 5.5 | 総括的評価のためのハザード関連使用シナリオの選択 | |
| 5.6 | ユーザーインターフェイス仕様の確立 | |
| 5.7 | ユーザーインターフェイス評価計画の確立 | |
| 5.8 | ユーザーインターフェイス設計、実装及び形成的評価の実施 | |
| 5.9 | ユーザーインターフェイスのユーザビリティに関する総括的評価の実施 | |

修

# Ⅵ. 医療機関のサイバーセキュリティ対応

1）サイバーセキュリティ対応通知等

2）薬機法におけるサイバーセキュリティ対応の推移

3）医療機器におけるサイバーセキュリティの確保について

# 医療法施行規則の改正（令和５年３月10日）

**第二章　病院、診療所及び助産所の管理**

（認定を受けた臨床研修等修了医師を管理者とする病院等）
第14条　病院又は診療所の管理者は、その病院又は診療所に存する医薬品、医療機器及び再生医療等製品につき医薬品医療機器等法の規定に違反しないよう必要な注意をしなければならない。
２　病院、診療所又は助産所の管理者は、医療の提供に著しい支障を及ぼすおそれがないように、サイバーセキュリティ（サイバーセキュリティ基本法（平成26年法律第104号）第2条に規定するサイバーセキュリティをいう。）を確保するために必要な措置を講じなければならない。

施行期日：令和５年４月１日から施行する。

留意事項：病院、診療所及び助産所におかれては、規則第 14 条第２項に規定する「必要な措置」として、最新の「医療情報システムの安全管理に関するガイドライン」（以下「安全管理ガイドライン」という。）を参照の上、サイバー攻撃に対する対策を含めセキュリティ対策全般について適切な対応を行うこと。
　なお、安全管理ガイドラインに記載されている内容のうち、優先的に取り組むべき事項については、厚生労働省において別途チェックリストを作成し、後日通知する。

産情発 0310 第 2 号
令 和 5 年 3 月 1 0 日

# 第15回　資料　[特集] 医療機関等におけるサイバーセキュリティ（案）

[特集] 医療機関等におけるサイバーセキュリティ　（案）

目次



## 1．はじめに

診療情報等の機微な情報を扱う電子カルテをはじめとする医療情報システムは、情報の利用性を高めて連携を容易にし、質の高い医療の提供に極めて有用ですが、短時間で大量の情報を処理できることが可能であるために、何かセキュリティ上の問題が起こると被害や業務影響が大きくなる可能性があります。セキュリティ上の問題としては、例えば、システム利用終了時にログアウトし忘れるといった運用上の問題から、停電や機器の故障、さらにはマルウェア（コンピュータウイルス）と呼ばれる悪意のある不正ソフトウェアの混入など様々な事象があります。「医療情報システムの安全管理に関するガイドライン」は、これらすべてに対応するためのガイドラインで、どうしても扱う項目が多くなります。一方でサイバー攻撃と呼ばれる外部からの不正ソフトウェアの混入による被害が昨今増えてきており、最悪の場合は診療機能停止に至るなど、社会的にも問題になっています。そこで、「医療情報システムの安全管理に関するガイドライン」の中で、サイバーセキュリティに関係する部分を要約し、できるだけ具体的な例などにも触れてまとめたものがこの特集です。一読いただいて、ご自身の所属する医療機関の対策に役立てていただければ幸いです。

最初に述べなければならないことは、サイバーセキュリティは導入している医療情報システムによって異なるということです。例えば、フルクラウドの電子カルテサービスを導入している診療所など小規模医療機関等の場合は、サイバーセキュリティを踏まえたシステムやデータ、サービスが用意された適切なシステム関連事業者のサービスを採用していれば、医療機関等が主に取り組むことは医療情報システムの利用者認証を適切に行うことと想定されますので、当該事業者にサイバーセキュリティに関して医療機関等側が取り組むべきことを確認し、認識の齟齬や漏れがないようにして、適切に医療情報システムを利用してください。

これ以降の記載はオンプレミス型の医療情報システムや、オンプレミス型とクラウド型の混在した医療情報システムを導入・利用している医療機関等を想定しており、地域において地域医療の基幹を担う医療機関は必要最小限の対策に留まることなく、地域で担っている役割を維持できるよう各種対策に注力してください。

## 2．サイバーセキュリティとは

不正ソフトウェアによる感染被害や、外部から不法に医療情報システムに侵入し、データを盗み取ったり、または破壊したりするような被害を受けるか、または被害には至らなくとも対応が必要になる事象をサイバーインシデントと呼び、これに対応する対策がサイバーセキュリティです。

外部からネットワーク等を介して、侵入または不正ソフトウェアの送り込みをサイバー攻撃と呼びますが、例えばユーザや保守事業者の自宅のパソコンが不正ソフトウェアに感染し、USB メモリやCD/DVD、外付けHDD 等の可搬媒体を介して医療情報システムに不正ソフトウェアが入り込むこともあります。

# 医療機関におけるサイバーセキュリティ対策チェックリスト

医療機関等におけるサイバーセキュリティ対策については、ガイドラインを参照の上、適切な対応を行うこととしているところ、このうちまずは医療機関が優先的に取り組むべき事項をチェックリストにまとめました。また、医療機関におけるチェックリストを用いた確認の実効性を高めるために、チェックリストマニュアルを作成しました。　医療機関及び医療情報システム・サービス事業者は、本マニュアルを参照しつつチェックリストを活用して、サイバーセキュリティ対策を行ってください。

- 医療機関におけるサイバーセキュリティ対策チェックリスト　[534KB]　（令和５年６月）
- 医療機関におけるサイバーセキュリティ対策チェックリストマニュアル［977KB］別ウィンドウで開く ～医療機関・事業者向け～（令和５年６月）
- （医療機関確認用）医療機関におけるサイバーセキュリティ対策チェックリスト（Excel）（令和５年６月）
- （事業者確認用）医療機関におけるサイバーセキュリティ対策チェックリスト（Excel）（令和５年６月）

医療機関確認用

# 医療機関におけるサイバーセキュリティ対策チェックリスト

医療機関確認用

| | チェック項目 | 確認結果（日付） | 備考 |
|---|---|---|---|
| 医療情報システムの有無 | 医療情報システムを導入、運用している。<br>（「いいえ」の場合、以下すべての項目は確認不要） | はい・いいえ<br>（　/　） | |

## ○　令和５年度中

*以下項目は令和５年度中にすべての項目で「はい」にマルが付くよう取り組んでください。
*２（２）及び２（３）については、事業者と契約していない場合には、記入不要です。
*1 回目の確認で「いいえ」の場合、令和５年度中の対応目標日を記入してください。

令和５年度：
体制構築・責任者お
設置の記載あり

| | チェック項目 | 確認結果（日付） | | | 備考 |
|---|---|---|---|---|---|
| | | １回目 | 目標日 | ２回目 | |
| 1<br>体制構築 | （1）　医療情報システム安全管理責任者を設置している。 | はい・いいえ<br>（　/　） | （　/　） | はい・いいえ<br>（　/　） | |
| 2<br>医療情報システムの管理・運用 | **医療情報システム全般について、以下を実施している。** | | | | |
| | （1）　サーバ、端末 PC、ネットワーク機器の台帳管理を行っている。 | はい・いいえ<br>（　/　） | （　/　） | はい・いいえ<br>（　/　） | |
| | （2）　リモートメンテナンス（保守）を利用している機器の有無を事業者等に確認した。 | はい・いいえ<br>（　/　） | （　/　） | はい・いいえ<br>（　/　） | |
| | （3）　事業者から製造業者/サービス事業者による医療情報セキュリティ開示書（MDS/SDS）を提出してもらう。 | はい・いいえ<br>（　/　） | （　/　） | はい・いいえ<br>（　/　） | |
| | **サーバについて、以下を実施している。** | | | | |
| | （4）　利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。 | はい・いいえ<br>（　/　） | （　/　） | はい・いいえ<br>（　/　） | |
| | （5）　退職者や使用していないアカウント等、不要なアカウントを削除している。 | はい・いいえ<br>（　/　） | （　/　） | はい・いいえ<br>（　/　） | |
| | （6）　アクセスログを管理している。 | はい・いいえ<br>（　/　） | （　/　） | はい・いいえ<br>（　/　） | |
| | **ネットワーク機器について、以下を実施している。** | | | | |
| | （7）　セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。 | はい・いいえ<br>（　/　） | （　/　） | はい・いいえ<br>（　/　） | |
| | （8）　接続元制限を実施している。 | はい・いいえ<br>（　/　） | （　/　） | はい・いいえ<br>（　/　） | |
| 3<br>インシデント発生に備えた対応 | （1）　インシデント発生時における組織内と外部関係機関（事業者、厚生労働省、警察等）への連絡体制図がある。 | はい・いいえ<br>（　/　） | | | |

- 各項目の考え方や確認方法等については、「医療機関におけるサイバーセキュリティ対策チェックリストマニュアル～医療機関・事業者向け～」をご覧ください。
- 立入検査の際は、チェックリストに必要な事項が記入されているかを確認します。



# 医療機関におけるサイバーセキュリティ対策チェックリスト

医療機関確認用

## ○　参考項目（令和６年度中）

*以下項目について、令和６年度中にすべての項目で「はい」にマルが付くよう取り組んでください。

| | チェック項目 | 確認結果（日付） | | | 備考 |
|---|---|---|---|---|---|
| | | １回目 | 目標日 | ２回目 | |
| 2<br>医療情報システムの管理・運用 | **サーバについて、以下を実施している。** | | | | |
| | （7）　セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。 | はい・いいえ<br>（　/　） | （　/　） | はい・いいえ<br>（　/　） | |
| | （9）　バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。 | はい・いいえ<br>（　/　） | （　/　） | はい・いいえ<br>（　/　） | |
| | **端末 PC について、以下を実施している。** | | | | |
| | （4）　利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。 | はい・いいえ<br>（　/　） | （　/　） | はい・いいえ<br>（　/　） | |
| | （5）　退職者や使用していないアカウント等、不要なアカウントを削除している。 | はい・いいえ<br>（　/　） | （　/　） | はい・いいえ<br>（　/　） | |
| | （7）　セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。 | はい・いいえ<br>（　/　） | （　/　） | はい・いいえ<br>（　/　） | |
| | （9）　バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。 | はい・いいえ<br>（　/　） | （　/　） | はい・いいえ<br>（　/　） | |
| 3<br>インシデント発生に備えた対応 | （2）　インシデント発生時に診療を継続するために必要な情報を検討し、データやシステムのバックアップの実施と復旧手順を確認している。 | はい・いいえ<br>（　/　） | （　/　） | はい・いいえ<br>（　/　） | |
| | （3）　サイバー攻撃を想定した事業継続計画（BCP）を策定、又は令和６年度中に策定予定である。 | はい・いいえ<br>（　/　） | （　/　） | はい・いいえ<br>（　/　） | |

- 各項目の考え方や確認方法等については、「医療機関におけるサイバーセキュリティ対策チェックリストマニュアル～医療機関・事業者向け～」をご覧ください。

事業者確認用

# 医療機関におけるサイバーセキュリティ対策チェックリスト

**事業者確認用**

令和５年度：
体制構築・責任者お
設置の記載あり

## ○　令和５年度中

*以下項目は令和５年度中にすべての項目で「はい」にマルが付くよう取り組んでください。
*1 回目の確認で「いいえ」の場合、令和５年度中の対応目標日を記入してください。

| | チェック項目 | 確認結果（日付） | | | 備考 |
|---|---|---|---|---|---|
| | | 1 回目 | 目標日 | 2 回目 | |
| 1 体制構築 | （1） 事業者内に、医療情報システム等の提供に係る管理責任者を設置している。 | はい・いいえ（ / ） | （ / ） | はい・いいえ（ / ） | |
| 2 医療情報システムの管理・運用 | **医療情報システム全般について、以下を実施している。** | | | | |
| | （2） リモートメンテナンス（保守）している機器の有無を確認した。 | はい・いいえ（ / ） | （ / ） | はい・いいえ（ / ） | |
| | （3） 医療機関に製造業者/サービス事業者による医療情報セキュリティ開示書（MDS/SDS）を提出した。 | はい・いいえ（ / ） | （ / ） | はい・いいえ（ / ） | |
| | **サーバについて、以下を実施している。** | | | | |
| | （4） 利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。 | はい・いいえ（ / ） | （ / ） | はい・いいえ（ / ） | |
| | （5） 退職者や使用していないアカウント等、不要なアカウントを削除している。 | はい・いいえ（ / ） | （ / ） | はい・いいえ（ / ） | |
| | （6） アクセスログを管理している。 | はい・いいえ（ / ） | （ / ） | はい・いいえ（ / ） | |
| | **ネットワーク機器について、以下を実施している。** | | | | |
| | （7） セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。 | はい・いいえ（ / ） | （ / ） | はい・いいえ（ / ） | |
| | （8） 接続元制限を実施している。 | はい・いいえ（ / ） | （ / ） | はい・いいえ（ / ） | |

事業者名：

● 各項目の考え方や確認方法等については、「医療機関におけるサイバーセキュリティ対策チェックリストマニュアル～医療機関・事業者向け～」をご覧ください。


# 医療機関におけるサイバーセキュリティ対策チェックリスト

**事業者確認用**


## ○　参考項目（令和６年度中）

*以下項目について、令和６年度中にすべての項目で「はい」にマルが付くよう取り組んでください。

| | チェック項目 | 確認結果（日付） | | | 備考 |
|---|---|---|---|---|---|
| | | 1 回目 | 目標日 | 2 回目 | |
| 2 医療情報システムの管理・運用 | **サーバについて、以下を実施している。** | | | | |
| | （7） セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。 | はい・いいえ（ / ） | （ / ） | はい・いいえ（ / ） | |
| | （9） バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。 | はい・いいえ（ / ） | （ / ） | はい・いいえ（ / ） | |
| | **端末 PC について、以下を実施している。** | | | | |
| | （4） 利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。 | はい・いいえ（ / ） | （ / ） | はい・いいえ（ / ） | |
| | （5） 退職者や使用していないアカウント等、不要なアカウントを削除している。 | はい・いいえ（ / ） | （ / ） | はい・いいえ（ / ） | |
| | （7） セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。 | はい・いいえ（ / ） | （ / ） | はい・いいえ（ / ） | |
| | （9） バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。 | はい・いいえ（ / ） | （ / ） | はい・いいえ（ / ） | |


● 各項目の考え方や確認方法等については、「医療機関におけるサイバーセキュリティ対策チェックリストマニュアル～医療機関・事業者向け～」をご覧ください。

# 医療機関等がサイバー攻撃を受けた際の厚生労働省連絡先

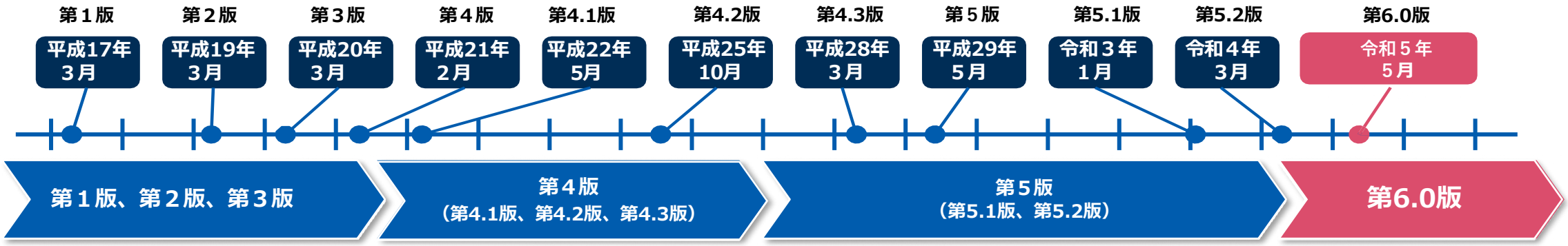
「医療情報システムの安全管理に関するガイドライン」では、医療機関等がサイバー攻撃を受けた（疑い含む）場合等の際には、厚生労働省等の所管省庁への連絡等、必要な対応を行うほか、そのための体制を整備する必要があることを示しています。

**医療機関等がサイバー攻撃を受けた場合の厚生労働省連絡先**

医政局特定医薬品開発支援・医療情報担当参事官室
TEL:　03-6812-7837
MAIL:　igishitsu@mhlw.go.jp

# 医療情報システムの安全管理に関するガイドライン策定の背景及び改定の経緯

- 医療情報システムの安全管理に関するガイドラインは、e-文書法、個人情報保護等への対応を行うための情報セキュリティ管理のガイドラインとして、平成17年3月に第１版を策定。
- 以降、各種制度の動向や情報システム技術の進展等に対応して改定。今般、**令和５年５月に第6.0版を策定。**




**策定・改訂概要**

**第１版**
- 医療情報システムのセキュリテ管理を目的とて策定

**第２版**
- 重要インフラとしての医療情報システムという観点からの対応

**第３版**
- 個人情報施策の議論およびモバイル端末普及への対応

**第4版**
- 個人情報保護施策の議論およびモバイル端末普及への対応

**第4.1版**
- 民間事業者のデータセンターにおける外部保存に関する対応

**第4.2版**
- 調剤済み処方せん及び調剤録等の外部保存への対応

**第4.3版**
- 「電子処方せんの運用ガイドライン」への対応

**第5版**
- 医療機関等の範囲の明確化
- 改正個人情報保護法対応
- サイバー攻撃の動向への対応

**第5.1版**
- クラウドサービスへの対応
- 認証・パスワードに関する対応
- サイバー攻撃等による対応
- 外部保存受託事業者の選定基準対応

**第5.2版**
- ２省（総務省、経産省）GL等との整合性
- 改正個人情報保護法への対応 等
- 医療機関へのサイバー攻撃の多様化・巧妙化
- 「規制改革実施計画」等への対応
- 電子署名
- 外部ネットワーク 等

**第6.0版**

<u>全体構成の見直し</u>
- 概説編、経営管理編、企画管理編、システム運用編の４編に再構成
- Q&Aの充実 等

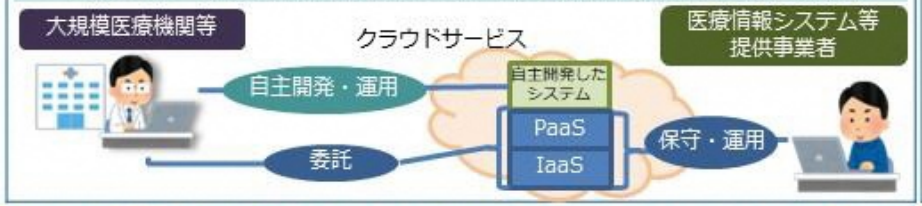
<u>技術的な動向</u>
- 外部委託、外部サービスの利用に関する整理
- 情報セキュリティに関する考え方の整理
- 新技術、制度・規格の変更への対応 等

# 医療情報システムの安全管理に関するガイドライン 第6.0版主な改定ポイント（概要）

## 外部委託、外部サービスの利用に関する整理

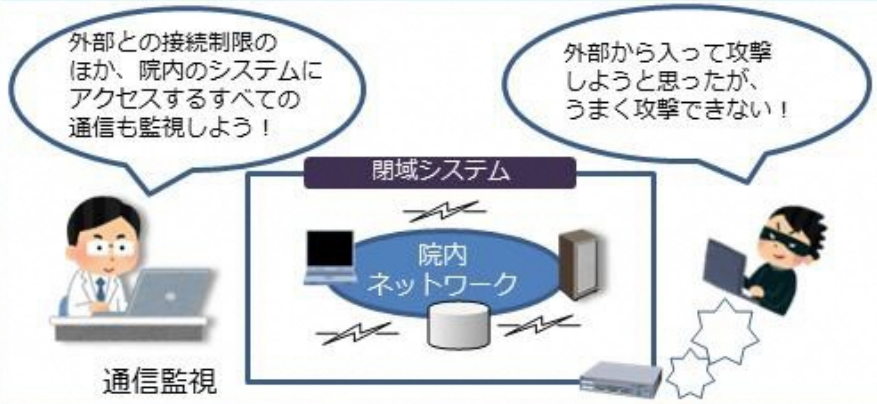
クラウドサービスに医療情報システムの運用管理を、すべてを外部に任せる場合


クラウドサービスに医療情報システムの一部を運用管理を外部に任せる場合




## ネットワーク境界防御型思考／ゼロトラストネットワーク型思考

ゼロトラストの思考を取り入れることで、個々の外部からの侵入にも適切な対応が可能となります。




## 災害、サイバー攻撃、システム障害等の非常時に対する対応や対策

非常時場面ごとのバックアップの考え方の違い（例）


## 本人確認を要する場面での運用（eKYCの活用）の検討

# 医療情報システムの安全管理に関するガイドライン　第6.0版（令和5年5月）

「医療情報システムの安全管理に関するガイドライン」（以下「ガイドライン」という。）については、直近では令和４年３月に第5.2版を策定し、医療情報システムの適切な取扱い等についてお示ししてきたところです。今般、ガイドラインの見直しを行い、以下のとおり「医療情報システムの安全管理に関するガイドライン第6.0 版」を策定するとともに、別添、特集、Q&A等の参考資料を作成しました。なお、改定の趣旨、概要については以下のとおりです。

**第１ 改定の趣旨**

保険医療機関・薬局においては令和５年４月からオンライン資格確認の導入が原則義務化されており、今後はガイドラインに記載されているネットワーク関連のセキュリティ対策がより多くの医療機関等に共通して求められることとなる。よって、医療機関等にガイドラインの内容の理解を促し、医療情報システムの安全管理の実効性を高めるため、構成の見直しを行う。また、医療等分野及び医療情報システムに対するサイバー攻撃の一層の多様化・巧妙化が進み、医療機関等における診療業務等に大きな影響が生じていること等を踏まえ、医療機関等に求められる安全管理措置を中心に内容の見直しを行う。

**第２ 改定の概要**

１．全体構成の見直し
本文を、概説編、経営管理編、企画管理編及びシステム運用編に分け、各編で想定する読者に求められる遵守事項及びその考え方を示すとともに、Ｑ＆Ａ等において現状で選択可能な具体的な技術にも言及するなど、構成の見直しを行う。

２．外部委託、外部サービスの利用に関する整理
クラウドサービスの特徴を踏まえたリスクや対策の考え方を整理するとともに、医療機関等のシステム類型別に責任分界の考え方等を整理する。

３．情報セキュリティに関する考え方の整理
ネットワークの安全性の考え方や認証のあり方を踏まえて、ゼロトラスト思考に則した対策の考え方を示すほか、サイバー攻撃を含む非常時に対する具体的な対応について整理する。

４．新技術、制度・規格の変更への対応
オンライン資格確認の導入に必要なネットワーク機器等の安全管理措置等について整理する。

# サイバーセキュリティ対応における課題

1. 医療機関等への情報提供の明確化
2. 医療機関との連携した対応の確立
3. 効率的な対策実施の検討
4. 市販前手続きの簡素化・迅速化
5. その他

追

# Ⅶ. 参考

# 令和4年度　登録認証機関向けトレーニング　資料一覧 | 独立行政法人 医薬品医療機器総合機構 (pmda.go.jp)

https://www.pmda.go.jp/review-services/reexamine-reevaluate/registered-cb/0009.html

追


| トレーニングテーマ | セクションテーマ | 資料 | |
|---|---|---|---|
| 3 | 医療機器プログラム（SaMD）に使われる規格解説 | i. 医療機器のユーザビリティ規格 JIS T 62366-1について | スライド |
| | | ii. 医療機器のセキュリティ規格 IEC 81001-5-1について | スライド |
| | | iii. ヘルスソフトウェアの製品安全規格 JIS T 82304-1について | スライド |
| | | ii. 放射線治療計画プログラム | スライド |

# 医療機器のセキュリティ規格　IEC 81001-5-1について

追

独立行政法人 医薬品医療機器総合機構
Pharmaceuticals and Medical Devices Agency

医療機器のセキュリティ規格 IEC 81001-5-1について

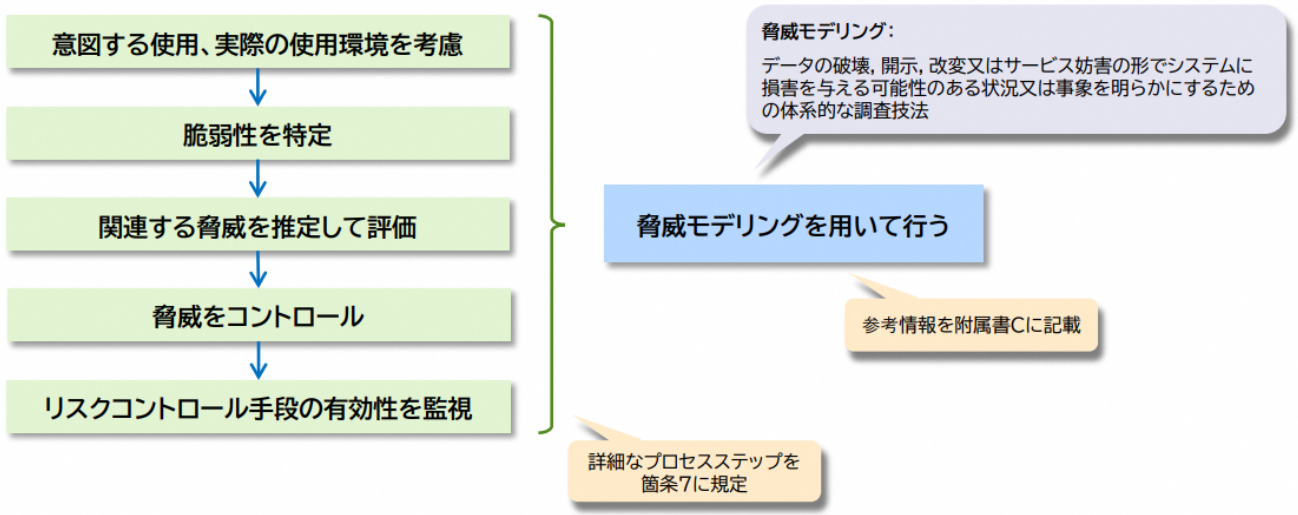
医薬品医療機器総合機
医療機器調査・基準
医療機器基準



独立行政法人 医薬品医療機器総合機構
Pharmaceuticals and Medical Devices Agency

## 4.2 セキュリティに関連するリスクマネジメント

- セキュリティに関連するリスクマネジメントのプロセスを確立する




- 各脆弱性に対応するための適切な方法を決定する際に適用するリスクの受容可能性の判断基準を確立する

メルマガへの登録で入手可能　https://www.trendmicro.com/ja_jp/business/campaigns/aws.html

追


深刻化する脆弱性を悪用した攻撃
近年、ソフトウェアにおける脆弱性の公開数は年々増加しており、アメリカのMITRE社が2021年にCVE（共通脆弱性識別）番号を付与し公表した脆弱性の数は2万件を超えました。これは1999年の公表以来過去最高を記録しています。サイバー犯罪者にとって、そうした脆弱性は、組織を攻撃する際に悪用することでネットワークへの侵入や感染拡大などの活動を実現できる絶好の手段となっています。攻撃者によって既に悪用が確認されており、早急に対策を講じる必要がある脆弱性の一覧として「KNOWN EXPLOITED VULNERABILITIES CATALOG（既知の悪用された脆弱性カタログ）」をCISA（アメリカ合衆国サイバーセキュリティ・社会基盤安全保障庁）では公開しています。

一方で多くの製品にはOSS（オープンソースソフトウェア）が組み込まれており、そのOSSにおいてもさまざまな脆弱性が存在します。2021年12月に公表され、多くの組織のシステム担当者が対応に追われたであろうApache Log4jの脆弱性「Log4Shell（CVE-2021-44228）」もその一つです。Log4jはオープンソースのJavaベースのロギングライブラリであり、さまざまなソフトウェアやアプリケーションに組み込まれていたことから、深刻な脆弱性が公開されたものの、自組織のどのシステムがLog4jを使用しているか把握することが多くの組織における課題となりました。そして、「Trend Micro Deep Security™」のデータによると、2022年1月～6月の間にこの脆弱性を悪用する攻撃通信を約48億検知していたことから、攻撃者が好んで悪用していたことが伺えます。

そのようなLog4jの脆弱性の影響と脆弱性管理における課題を受けて、世界中でOSSおよびソフトウェア・サプライチェーンに対するセキュリティの重要性が改めて語られるようになりました。本稿ではそうしたソフトウェア・サプライチェーンの構造的な課題とその脆弱性管理の解決策の一つとして注目されている「SBOM（Software Bill Of Materials）」について、各組織が把握しておくべき点を解説していきます。

ご清聴ありがとうございました