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

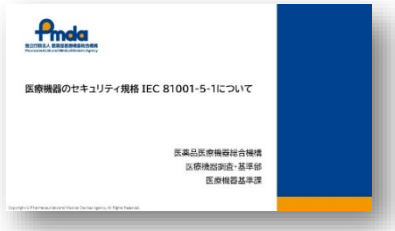
医療機器のサイバーセキュリティ要件に対する JIS T 81001-5-1の適用について

医薬品医療機器総合機構
医療機器調査・基準部
医療機器基準課

医療機器のサイバーセキュリティに関する要求事項

- 基本要件基準は、令和5年3月9日に改正され、サイバーセキュリティに関する要求事項が第12条第3項として新設された。（基本要件基準とは、全ての医療機器又は体外診断用医薬品が具備すべき品質、有効性及び安全性に係る基本的要件を規定したもの。）
- 基本要件基準第12条第3項の適用については、令和5年3月31日付け薬生機審発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」にて、基本的な考え方が示されており、その中で、基本要件基準第12条第3項への適合を示すために、JIS T 81001-5-1等への適合性を確認することが求められている。
- JIS T 81001-5-1等への適合性を確認する際に特に留意する点については、令和5年5月23日付け薬生機審発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」に示されており、医療機器のサイバーセキュリティ対応の具体的な要件と考えることができる。
- 関連して、令和5年7月20日付け事務連絡「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」、令和6年1月31日付け事務連絡「医療機器のサイバーセキュリティに関する質疑応答集（Q&A）について」が発出されている。
- JIS T 81001-5-1の原典であるIEC 81001-5-1については、令和4年度　製造販売業者向け医療機器プログラム（SaMD）の審査ポイント等に関する説明会において、規格の全体的な解説を行っており、次の資料が参考にできる。

説明用スライド（https://www.pmda.go.jp/files/000250907.pdf）
読み原稿付きノート（https://www.pmda.go.jp/files/000252686.pdf）
スライドショー（https://www.youtube.com/watch?v=6wrXnMZLP5E）



略語の一覧

関連する通知等について次のように略する。

略語	日付	対象
基本要件基準	令和5年(2023年) 3月9日改正	**「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(2015年) 4月28日	**「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」**(薬食機審発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・再生医療等審査管理担当)・医薬食品局安全対策課長連名通知)
ガイダンス通知	平成30年(2018年) 7月24日	**「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」**(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)
取扱い通知	令和5年(2023年) 3月31日	**「医療機器の基本要件基準第12条第3項の適用について」**(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)
製販向け手引書通知	令和5年(2023年) 3月31日	**「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」**(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)
適合性確認通知	令和5年(2023年) 5月23日	**「医療機器の基本要件第12条第3項の適合性の確認について」**(薬生機審発0523第1号厚生労働省医薬・生活衛生局医療機器審査管理課長通知)
QA事務連絡(QA)	令和5年(2023年) 7月20日	**「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」**厚生労働省医薬・生活衛生局医療機器審査管理課事務連絡
QA事務連絡2(QA2)	令和6年(2024年) 1月31日付け	**「医療機器のサイバーセキュリティに関する質疑応答集(Q&A)について」**厚生労働省医政局特定医薬品開発支援・医療情報担当参事官室、厚生労働省医薬局医療機器審査管理課・医薬安全対策課・監視指導・麻薬対策課連名事務連絡

基本要件基準第12条第3項について

基本要件基準第12条第3項

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。

対象となる医療機器の明確化

他の医療機器、IoT機器、外部記憶媒体、電子カルテや病院内外のネットワーク等に接続する医療機器

悪意をもった不正アクセス、過剰な負荷を与える攻撃、マルウェア感染などが想定される医療機器

取扱い通知

該当する場合、以降を適用し、適合性を確認する

ソフトウェアを意図したとおりに動作させるために必要最低限な要件（動作環境及び使用環境）の特定

← IMDRF N47文書の5.8.4及び確保通知

サイバーリスクを適切に低減する設計及び製造（サイバーリスクの特定及び評価）

← IMDRF N47文書の5.5.6及び確保通知

リスクマネジメント

製品の全ライフサイクルにわたって、適切なレベルのサイバーセキュリティを提供する設計、製造及び保守

← IMDRF N47文書の5.8.5及びIMDRF N60文書の4. 2

ライフサイクルプロセス

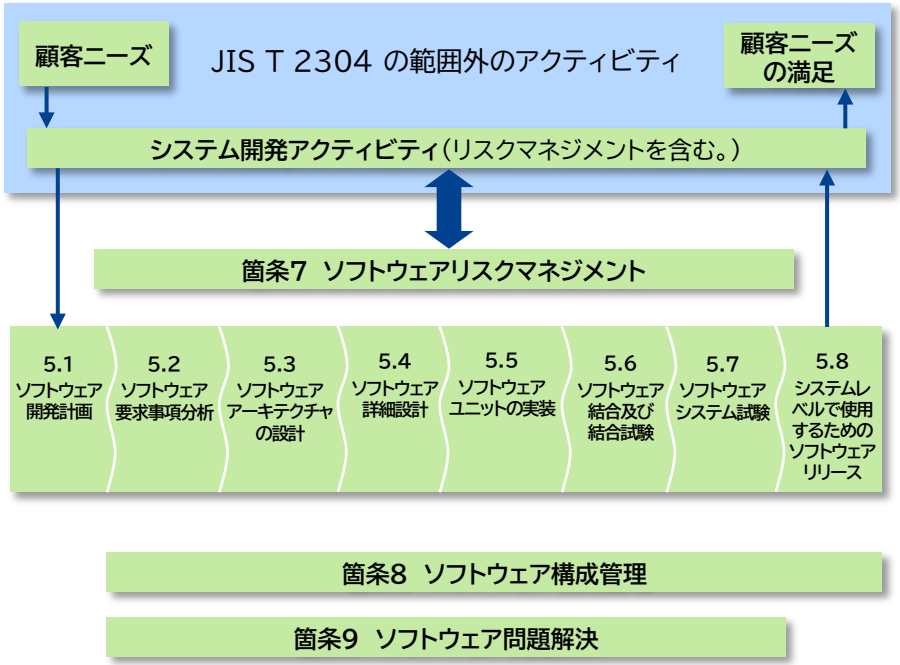
- IMDRF N47文書：IMDRF/GRRP WG/N47 FINAL:2018 “Essential Principles of Safety and Performance of Medical Devices and IVD Medical Devices”
- IMDRF N60文書:IMDRF/CYBER WG/N60 FINAL:2020 “Principles and Practices for Medical Device Cybersecurity”

JIS T 2304のソフトウェアライフサイクルプロセス

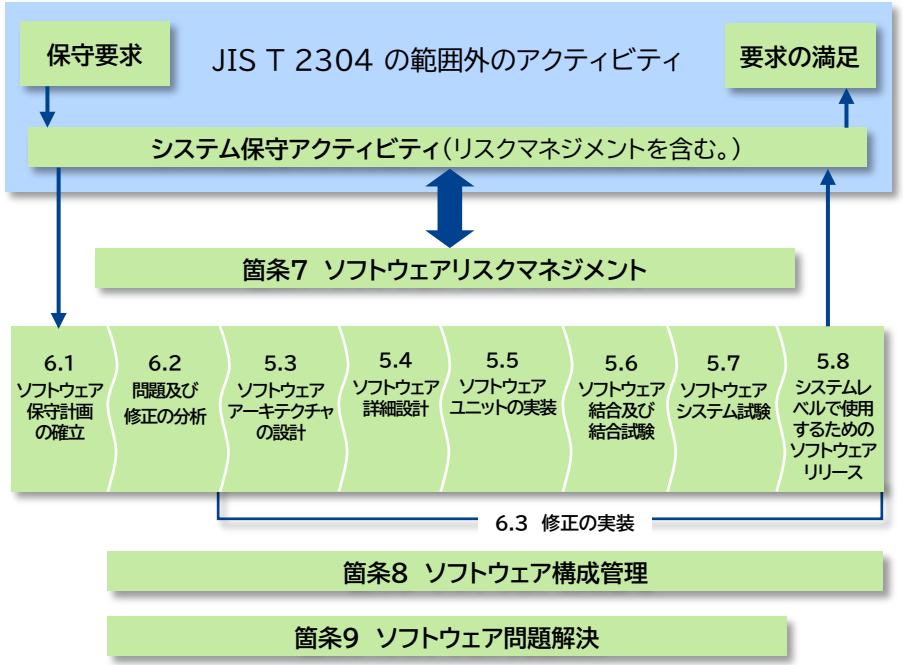
安全なソフトウェアを実現するためには、試験を実施するだけではなく、次が必要

- ハザードを特定し、関連するリスクが受容可能なレベルにまで低減されている。(リスクマネジメント)
- 適切なプロセスを規定し、それが効果的に実施されている。(ライフサイクルプロセス)

基本要件基準第12条第2項への適合は、JIS T 2304への適合によって確認する。



JIS T 2304:2017 図1－ソフトウェア開発プロセス及びアクティビティの関連図より



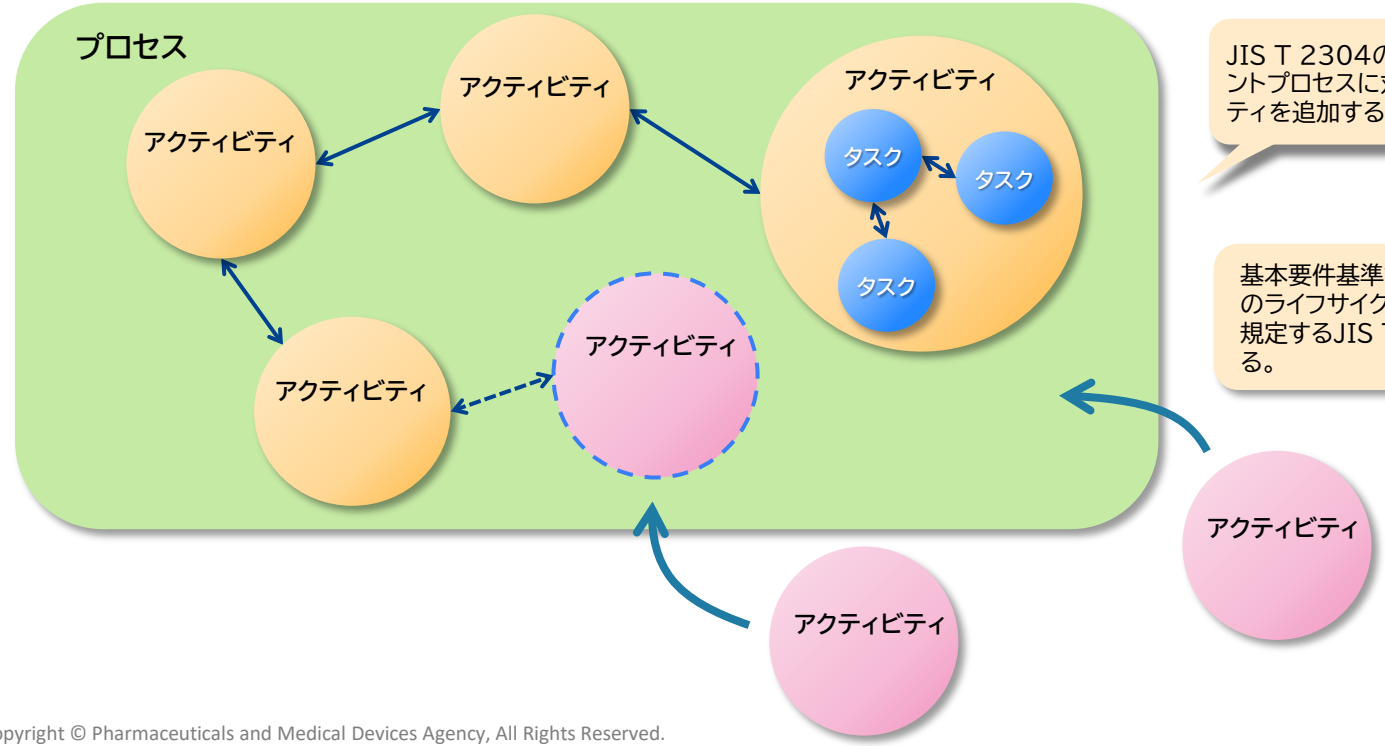
JIS T 2304:2017 図2－ソフトウェア保守プロセス及びアクティビティの関連図より

JIS T 81001-5-1の構成のイメージ

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－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）

JIS T 81001-5-1は、サイバーセキュリティを強化するために、ライフサイクルにおいて実行するアクティビティを規定し、品質マネジメントシステム及びリスクマネジメントシステムの下でソフトウェアを開発・保守することを規定している。



JIS T 2304のライフサイクルプロセスやリスクマネジメントプロセスに対して、セキュリティに必要なアクティビティを追加するイメージ

基本要件基準第12条第3項への適合は、JIS T 2304のライフサイクル要求事項の構成でセキュリティ対応を規定するJIS T 81001-5-1への適合によって確認する。

基本要件基準第12条第3項の適合性の確認について

基本要件基準第12条第3項

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、

対象となる医療機器の明確化

「…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…」

「…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…」

取扱い通知の3の(1)より

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。

JIS T 81001-5-1等への適合性を確認することによって、これらへの適合を示す。

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(QA#2)

この際の留意事項として、
JISに関連する要求事項及び
JISに関連する既存通知等の要求事項
を具体的に示している。

適合性確認通知

適合性確認通知の内容

1.は、規格要求事項の要約や抜粋の形になっており、特にこれらに留意して基本要件基準への適合を確認する。2. は、規格に関連して追加で確認する内容を示している。

箇条	1. JISに関連する要求事項	2. JISに関連する既存通知等の要求事項
4 （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。	
	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。	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。
	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。	
5 （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。	
	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。	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。
	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。	
6 （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をあらかじめ定めておき、その一環として顧客に対するセキュリティ更新の通知方法を明確化すること。
7 （リスクマネジメント）	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。	
8 （構成管理）	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。	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。
9 （問題解決）	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。	

以下、この内容を考慮して規格の要点を説明する。

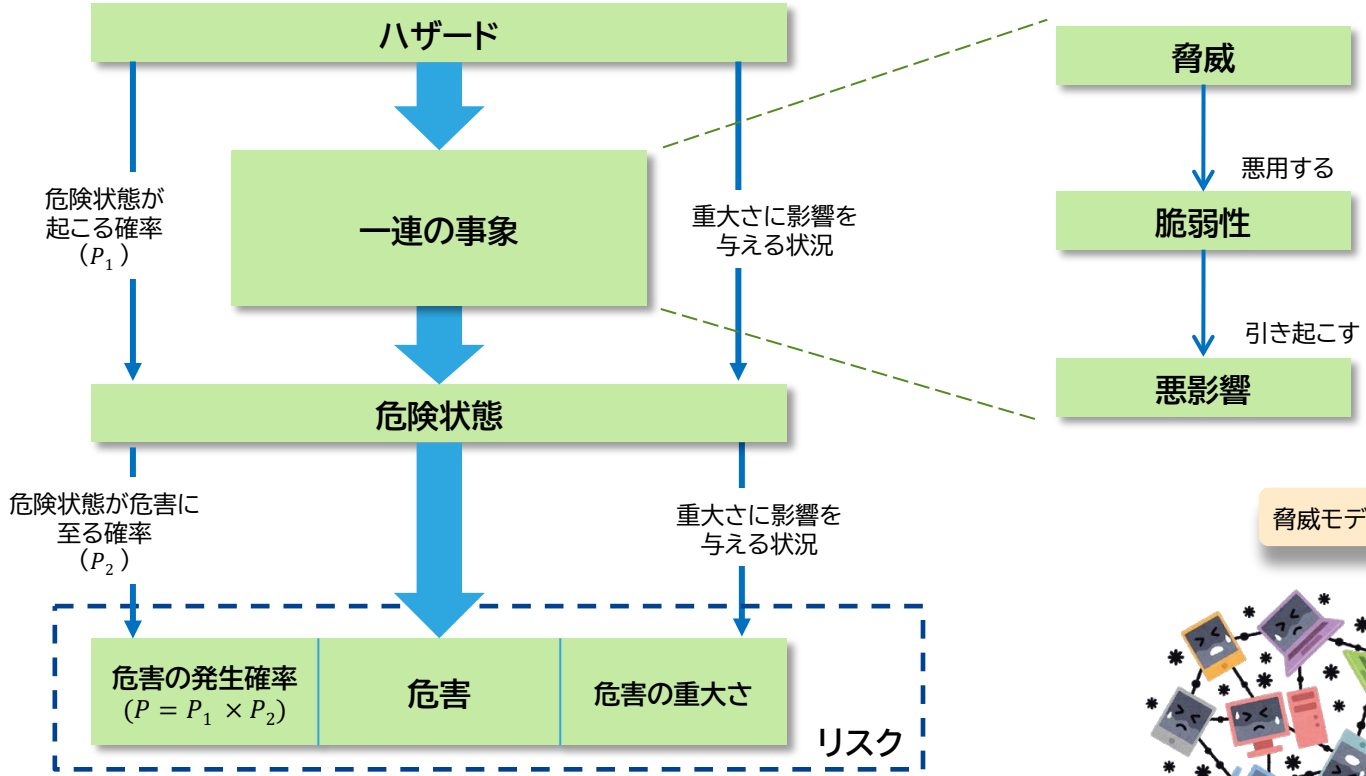
箇条4の一般要求事項、箇条7のリスクマネジメントプロセスについて

箇条	1. JISに関連する要求事項	2. JISに関連する既存通知等の要求事項
4 （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。	
	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。	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。
	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。	

- 規格の箇条4では、製造業者が品質マネジメントシステム、リスクマネジメントの下でソフトウェアを開発し保守することを規定している。
- 適合性確認通知は、規格の4.1.1、4.1.7及び4.2をフォーカスした内容になっている。
- 追加確認事項として、確保通知の関連する内容が示されている。セキュリティに対する問い合わせ窓口を明確化するとは、具体的には、セキュリティに関して緊急に対応できる窓口（連絡先）の設定が想定されており、ホームページ、取扱説明書、注意事項等情報等に、セキュリティに関して緊急に対応できる窓口（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（QA#4）。
- リスクマネジメントは、セキュリティ特有の脆弱性、脅威等を考慮して行う必要があるが、規格においては、JIS T 14971の枠組みの下で、脆弱性、脅威等を適切にマッピングして、セキュリティ関連のアクティビティを追加して実施可能と説明されている。

箇条	1. JISに関連する要求事項	2. JISに関連する既存通知等の要求事項
7 （リスクマネジメント）	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。	

脆弱性、脅威及び他のセキュリティ関連の用語のマッピングの例



JIS T 14971:2020, 図C.1－ハザード, 一連の事象, 危険状態及び危害の関係の図解例より

JIS T 14971のリスクマネジメントプロセスとの対応

JIS T 14971のリスクマネジメントプロセスの概略

リスクマネジメント計画

リスク分析
- 意図する使用及び合理的に予見可能な誤使用
- 安全に関する特質の明確化
- ハザード及び危険状態の特定
- リスク推定

↓

リスク評価

↓

リスクコントロール
- リスクコントロール手段の選択
- リスクコントロール手段の実施
- 残留リスクの評価
- ベネフィット・リスク分析
- リスクコントロール手段によって発生したリスク
- リスクコントロールの完了

↓

全体的な残留リスクの評価

↓

リスクマネジメントのレビュー

↓

製造及び製造後の活動
- 一般
- 情報の収集
- 情報のレビュー
- 処置

JIS T 81001-5-1のセキュリティ関連のリスクマネジメントプロセス

製造業者は，ヘルスソフトウェアに関連するセキュリティに関連するリスクをマネジメントするプロセスを，その製品リスクマネジメントのアプローチの一部として確立し，維持する。(7.1.1より)

意図する使用、実際の使用環境を考慮 (7.1)

↓

脆弱性等を特定 (7.2)

↓

関連する脅威を推定して評価 (7.3)

↓

脅威をコントロール (7.4)

↓

リスクコントロール手段の有効性を監視 (7.5)

脅威モデリングを用いて行う

このプロセスは，既存の一般的なリスクマネジメントプロセスの一部とすることが可能である。(4.2 注記2より)

既存のリスクマネジメントの手順に従って、サイバーセキュリティの特質を考慮してアクティビティを実施する

リスクマネジメントプロセスと他のプロセスとの関連

箇条4　一般要求事項

4.2　セキュリティに関連するリスクマネジメント

詳細を箇条7に規定

セキュリティコンテキストは、製品レベルの意図する使用環境から導き出し、設計に反映する

多層防御を考慮し、信頼境界を文書化

箇条5　ソフトウェア開発プロセス

5.3　ソフトウェアアーキテクチャー設計

5.4　ソフトウェア設計

5.7　ソフトウェアシステム試験

リスクマネジメントプロセスは、脅威モデリングの手法を用いて行い、その結果を文書化した脅威モデルは、開発プロセスや問題解決プロセスで参照して、対処する

特定した脅威に対応する方法を設計に含めて、システム試験で有効性を確認する

脅威モデル:
脅威モデリングのアクティビティを文書化した結果

脅威モデル

特定したすべての問題を対処する

箇条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

7.1　リスクマネジメントのコンテキスト

7.2　ぜい(脆)弱性, 脅威及び関連する悪影響の特定

7.3　セキュリティに関連するリスクの推定及び評価

7.4　セキュリティに関連するリスクのコントロール

7.5　リスクコントロールの有効性の監視

脅威モデリング

箇条9　ソフトウェア問題解決プロセス

9.4　ぜい(脆)弱性の分析

9.5　セキュリティ関連の問題への対応

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。(適合性確認通知の1.の(4))

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。(適合性確認通知の1.の(6))

箇条5のソフトウェア開発プロセスについて

箇条	1. JISに関連する要求事項	2. JISに関連する既存通知等の要求事項
5 （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。	
	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。	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。
	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。	

- 開発計画においては、セキュリティ更新に関連するアクティビティを計画しておく（5.1.1）。また、開発、生産、配送及び保守に用いるITインフラストラクチャーに関連するサイバーセキュリティ対策を確立する（5.1.2）。
- セキュリティ要求事項は、製品（ソフトウェア）がセキュリティについて求められていることであり、設計上の配慮、製品のセキュリティ機能、附属資料における配慮などを要求事項として特定する。（セキュリティ機能については、IEC 80001-2-2やIEC TR 60601-4-5、MDS2などを参照。）
- システム構成図やネットワーク構成図等を用いて、医療機器の想定する使用状況等を明確化し、信頼境界を行き来する情報を特定し、様々な脅威に対応するための足掛かりにする、多層防御を考慮することによって、しっかりとした防御につなげる他、機器以外での対策の可能性についても検討する。
- セキュリティ設計のベストプラクティスについては、5.3.2及び5.4.1の例示、製販向け手引書通知別添の5.1が参考になる。（QA2＃7）
- ソフトウェアシステム試験は、システム全体に対して何らかの試験を行って、例えば、特定したセキュリティ要求事項が満たされていることや、製品に実装したリスクコントロール手段が有効であることを確認して、確かにシステム全体としてセキュリティが確保できていることを実証する。試験は、必ずしも第三者試験である必要はない（QA＃7）。試験方法は、これらの他にも脆弱性試験や侵入試験が規格に記載されている。

箇条6のソフトウェア保守プロセスについて

箇条	1. JISに関連する要求事項	2. JISに関連する既存通知等の要求事項
6 （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をあらかじめ定めておき、その一環として顧客に対するセキュリティ更新の通知方法を明確化すること。

- ソフトウェア保守プロセスにおいては、製造業者が保守アクティビティを行うためのソフトウェア保守計画を確立することが、JIS T 2304のライフサイクルプロセスに定められており、保守段階も含めた製品の全ライフサイクルに対応するために重要である。
- セキュリティに関連する保守アクティビティとしては、規格には、セキュリティ更新の通知方針等が示されているが、セキュリティ更新の通知方針を明確化するには、追加確認内容として通知に示されているように、サポート終了等の製品寿命に対して計画を行い、脆弱性の監視やセキュリティ更新等の脆弱性対策の実施計画をあらかじめ定めておくことが必要になる。
- なお、サイバーセキュリティに係る不具合報告等については、厚労科研でまとめた基本的な考え方が令和6年1月15日医薬安発0115第2号「医療機器サイバーセキュリティに関する不具合等報告の基本的考え方について」で紹介されている。

箇条8のソフトウェア構成管理プロセスについて

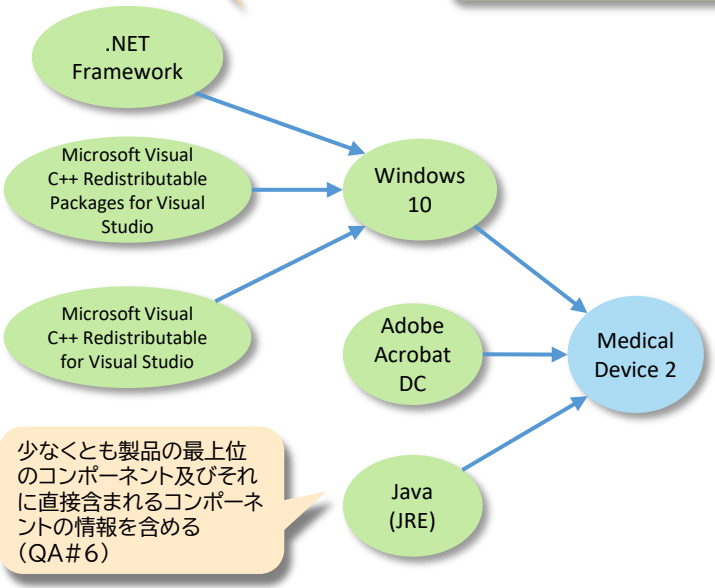
箇条	1. JISに関連する要求事項	2. JISに関連する既存通知等の要求事項
8 （構成管理）	医療機器の開発、保守及びサポートのための、変更管理及び変更履歴を伴う構成管理プロセスを確立すること。	構成管理プロセスは、当該医療機器のソフトウェア部品表（SBOM）を適切に作成することによって確認すること。

- SBOMの作成については、適合性確認通知の第2項で追加要求事項として示されているが、これは、箇条8の構成管理プロセスの実施を端的に示す資料として求められている。
- SBOMは、申請時に提出する必要はないが、作成していることを文書名等の記載によって明示する。また、提示できるよう準備しておく（QA#5）。
- 平成26年（2014年）の基本要件基準改正によって、平成29年（2017年）11月25日以降はJIS T 2304への適合が求められているので、それ以降に設計開発された品目については、構成管理情報があり、そこからSBOMは作成可能である。それまでに設計が完了されている品目については、平成29年5月17日付け薬生機審発0517第1号「医療機器の基本要件基準第12条第2項の適用について」において、「JIS T 2304等の要求事項と当該医療機器に関して利用可能な情報等との差分を分析し、リスクが受容可能になるようリスクマネジメントの中で対応し、必要な記録を残すこと等」を求めてきた経緯があり、サイバー攻撃の観点からリスクを考慮し、使用時の注意の周知等、そのリスクが受容可能になるように対応し、継続使用に適することを確実にする必要がある。（QA2＃9）

医療機器のSBOMの概念的なイメージ

MDM1社のMedical Device 2の構造（仮想的な例）

そのSBOMの概念的イメージ（SBOMの構成は、QA#6を参照）



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（QA#6）

この例の固有識別子は、PURL（package URL）を用いているが、CPE活用等様々な表現方法がある。また、SBOMの各要素の粒度や深さ等は、使用するツールによっても変わってくる。

JIS T 2304:2017

8.1.1「製造業者は、（中略）構成アイテム及びそのバージョンを，一意に識別するための仕組みを確立する。」

8.1.2「現在使用中のSOUP構成アイテム（標準ライブラリを含む。）のそれぞれについて，製造業者は，次を文書化する。a）名称、b）製造業者、c）SOUPを特定する識別子」

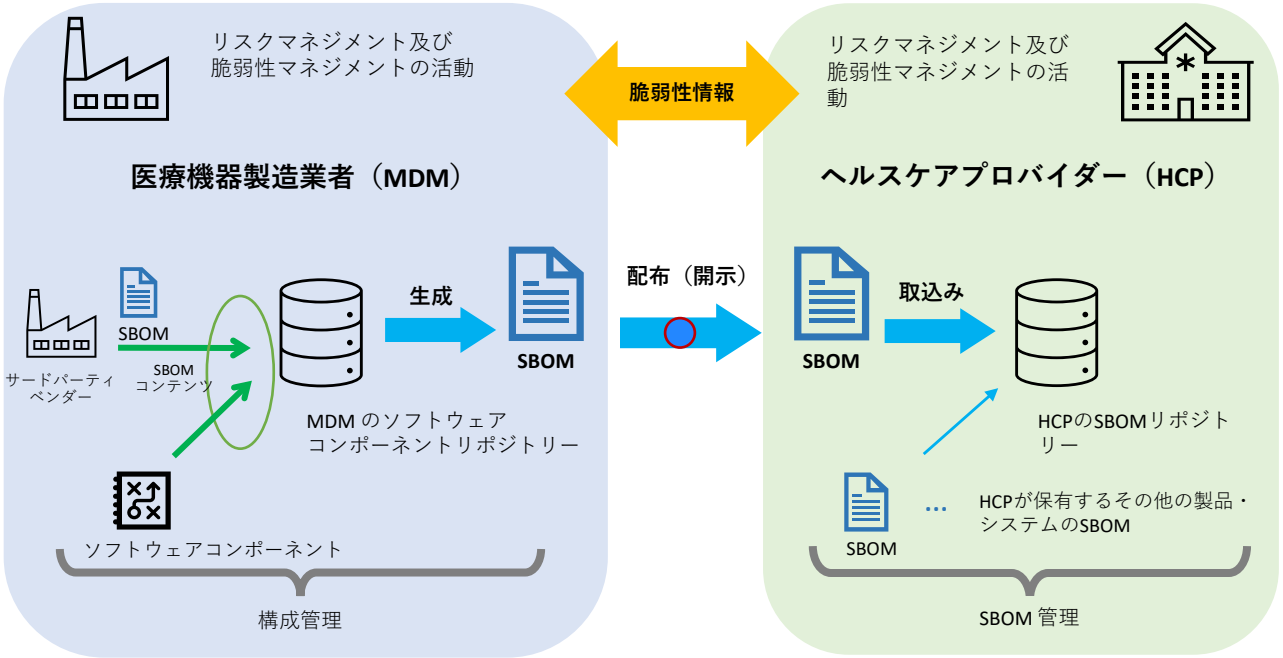
（cの例としては、バージョン、リリース年月日、パッチ番号、アップグレードの識別子）

id	サプライヤーの名前	コンポーネントの名前	バージョン	固有識別子	上流のコンポーネントとの関係	作成者名	タイムスタンプ
1	MDM1	Medical Device 2	2.5.9	pkg supplier/MDM1/Medical Device 2@2.5.9	self	MDM1	2021-08-19 T08:14:01Z
2	Microsoft	Windows 10	1903	pkg supplier/Microsoft/Windows 10@1903	Included in id#1	Microsoft	2021-01-21 T03:14:07Z
3	Microsoft	.NET Framework	4.5.2	pkg supplier/Microsoft/.NET Framework@4.5.2	Included in id#2	Microsoft	2021-01-13 T05:54:00Z
4	Microsoft	Microsoft Visual C++ Redistributable Packages for Visual Studio	2013 update_5	pkg supplier/Microsoft/Microsoft Visual C++ Redistributable Packages for Visual Studio@2013 update_5	Included in id#2	Microsoft	2015-08-11 T05:54:00Z
5	Microsoft	Microsoft Visual C++ Redistributable for Visual Studio	2012 update_5	pkg supplier/Microsoft/Microsoft Visual C++ Redistributable for Visual Studio@2012 update_5	Included in id#2	Microsoft	2014-01-14 T05:54:00Z
6	Adobe	Adobe Acrobat DC	19.008	pkg supplier/Adobe/Adobe Acrobat DC@19.008	Included in id#1	MDM1	2021-01-19 T03:14:07Z
7	Oracle	Java (JRE)	1.8.0 update_191	pkg supplier/Oracle/Java (JRE)@1.8.0 update_191	Included in id#1	MDM1	2017-12-21 T03:14:07Z

「医療機器のサイバーセキュリティ導入に関する手引書」も参照。

SBOM の全体的なフレームワーク

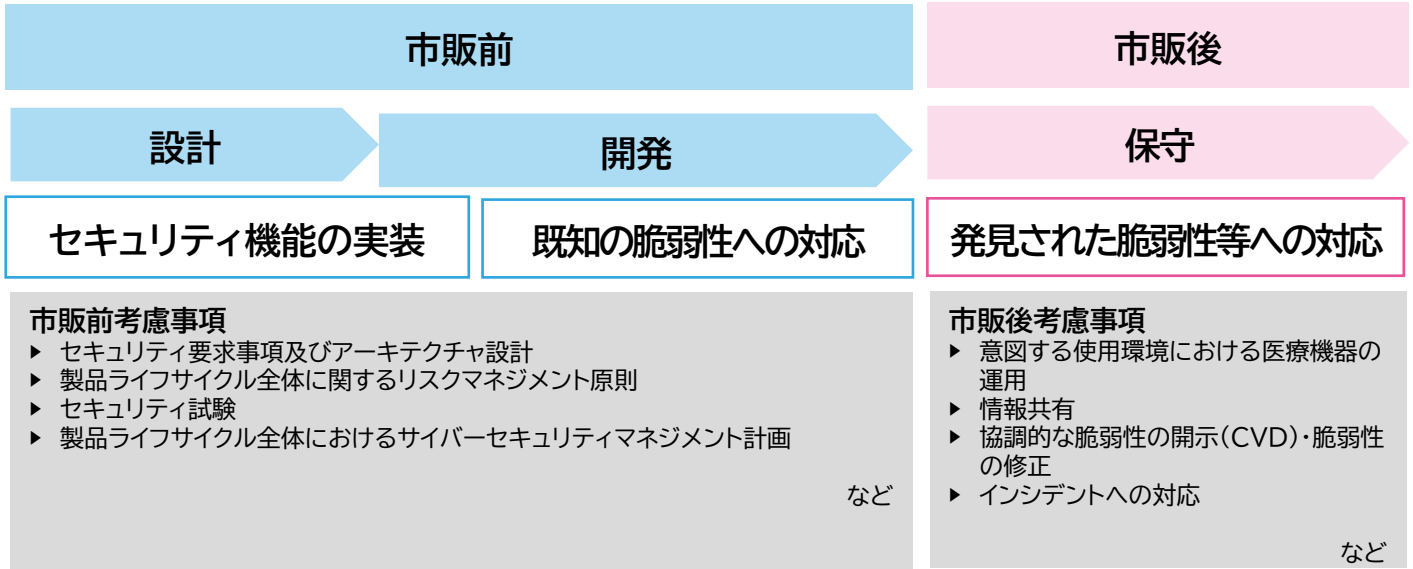
ソフトウェア部品表(Software Bill of Materials、SBOM)は、一つ又は複数の識別したコンポーネント、それらの関係及びその他の関連する情報のリスト



※ IMDRF/CYBER WG/N73FINAL:2023(2023年4月発行)
「医療機器サイバーセキュリティのためのソフトウェア部品表の原則及び実践」より引用

構成管理プロセスの確立について

SBOMは、市販前および市販後活動（すなわち、製品ライフサイクル全体）でサイバーセキュリティのリスクマネジメントプロセスを改善するために活用可能なリソース



※ IMDRF/CYBER WG/N60FINAL:2020（2020年4月発行）
「医療機器サイバーセキュリティの原則及び実践」より作成

箇条9の問題解決プロセスについて

箇条	1. JISに関連する要求事項	2. JISに関連する既存通知等の要求事項
9 （問題解決）	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。	

- JIS T 81001-5-1の箇条9は、セキュリティ関連の問題を取り扱うために使用されるアクティビティとして、次を規定している。
  - 9.2 ぜい(脆)弱性についての通知の受領
  - 9.3 ぜい(脆)弱性のレビュー
  - 9.4 ぜい(脆)弱性の分析
  - 9.5 セキュリティ関連の問題への対応
- 適合性確認通知に示されている内容は、この規定のサマリーと考えることができ、手順を定めて、手順に従って実施することが求められる。

承認申請書等の添付資料の示し方（一例）（参考：QA事務連絡）

STED

4. 設計検証及び妥当性確認文書の概要

＜省略＞

・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	規定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に示すとおり、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
（以下、略）				

適合性確認通知の各留意点について、該当する手順書、計画書、設計文書、報告書等の社内文書等を特定する

第3者機関による試験を活用してJIS T 81001-5-1への適合を示す場合でも、適合性確認通知の第2項の確認事項についての実施を示すこと（QA2＃4）

トランジションヘルスソフトウェア(附属書F)について

トランジションヘルスソフトウェア:
この規格の発行前にリリースされ、この規格の箇条4～箇条9に規定する全ての要求事項には適合していないヘルスソフトウェアのこと

ソフトウェアを再開発することなく、F.2～F.4のアクティビティを実施して、セキュリティを改善し、規格への適合を行う

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、適合性確認通知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(QA#2)

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を適用することでよい(QA#3)

F.2 開発の評価及びギャップ解消アクティビティ

箇条4(一般要求事項)を実施する

次のギャップ分析、ギャップ解消を行う

- a) システムレベルのセキュリティ要求事項を文書化
- b) システムレベルの試験を行い、結果を文書化
- c) セキュリティのリスクアセスメント及び評価
- d) セキュリティのリスクコントロール
- e) セキュアな運用指針、アカウント管理の指針を作成又は更新
- f) 全体の残留リスクを評価し、継続使用の適切性を判断

F.3 トランジションヘルスソフトウェアを使用する根拠

ギャップ解消アクティビティに基づく継続使用の根拠をソフトウェアのバージョンとともに文書化

箇条6～箇条9に適合させる移行計画

- 開発が完了しているので、箇条5は実施できないが、引き続きこの製品を使用してもサイバーセキュリティ的に大丈夫であることをはっきりさせる
- 箇条5以外は、計画的に実施する

F.4 リリース後のアクティビティ

箇条6～箇条9のアクティビティを実施

箇条4: 一般要求事項
箇条5: ソフトウェア開発プロセス
箇条6: ソフトウェア保守プロセス
箇条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
箇条8: ソフトウェア構成管理プロセス
箇条9: ソフトウェア問題解決プロセス

承認申請書等の添付資料の示し方（附属書Fの一例）（参考：QA事務連絡2）

STED

4. 設計検証及び妥当性確認文書の概要

＜省略＞

・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	規定の各要求事項に対して、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を適用し、「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に示すとおり、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

開発が既に完了しているため、ソフトウェア開発プロセスに関する確認項目のいくつかは、記載不要。

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。

1. 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基づく適合性の判断

実施内容概要	社内ドキュメント名	文書番号
JIS T 81001-5-1の要求事項とのギャップ分析を行い、ギャップ解消アクティビティを実行し、ギャップ解消アクティビティのアウトプットに基づくトランジションヘルスソフトウェアの継続使用の根拠をトランジションヘルスソフトウェアのバージョンとともに文書化すること。	トランジションヘルスソフトウェアへの適合宣言報告書	社内文書〇〇

2. 医療機器の基本要件基準第12条第3項の確認について（薬生機審発0523第1号：令和5年5月23日）の各項目に対する実施状況

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
		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
（以下、略）				

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

ご清聴ありがとうございました。