事　務　連　絡
令和５年７月２０日

各都道府県衛生主管部（局）薬務主管課　御中

厚生労働省医薬・生活衛生局医療機器審査管理課

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

「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」（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。 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) 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」 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。 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-ソフトウェアライフサイクルプトセス」 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 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　××××

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