事　務　連　絡
令和６年２月１日

岡山県薬業協会　御中

岡山県保健医療部医薬安全課

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

このことについて、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、同省医薬局医療機器審査管理課、同局医薬安全対策課及び同局監視指導・麻薬対策課から別添のとおり事務連絡がありましたので御了知の上、貴会員への周知方よろしくお願いします。

事　務　連　絡
令和６年１月３１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
厚生労働省医薬局医薬安全対策課
厚生労働省医薬局監視指導・麻薬対策課

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

「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、「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 日付け事務連絡）にて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、それぞれ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項の適用等を含めた医療機器のサイバーセキュリティ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内容につき浸透が図られるよう、周知方御配慮願います。

別　紙

医療機器のサイバーセキュリティに関する質疑応答集（Q＆A）

Q1：WiFi や Bluetooth、有線（LAN や USB デバイス）で接続できる仕様は有するものの、患者への使用時等においては接続されず、製造販売業者等による保守や修理作業においてのみ接続され、注意事項等情報や使用者との契約で接続制限が合意された医療機器については、医療機関のネットワークに常時繋がって使用・管理されているものとは異なり、想定される使用環境下に限定したサイバーセキュリティにおける評価のみを行うことで良いか。

また、汎用 PC などにインストールすることなく、端末からクラウドにアクセスして用いる医療機器プログラムについても、医療機器におけるサイバーセキュリティ対応は適用になるのか。

A1：基本要件基準第 12 条第3項に示されているとおり、製造販売業者等による保守や修理作業においてのみ接続される医療機器であっても、『①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『②外部からの不正アクセス及び攻撃アクセスが想定される医療機器』が適用されるため、「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、リスク分析を行うことにより必要なセキュリティ対応・管理を行うこと。また、クラウドにアクセスして用いる医療機器プログラムについても同様に、医療機器であるプログラム部分のセキュリティ対応が必要になる。

なお、リスク分析の際には、システム構成図やネットワーク構成図を作成し、どのようなリスクが存在するのかを明確にし、合理的に予見可能な誤使用を踏まえた脅威分析を行った上で、運用上の注意点を明確にしていくことが重要になる。

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においては、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確認することが求められているが、図等の様式の指定はない。

Q2：基本要件基準第 12 条第3項の経過措置期間中に承認申請・認証申請を行い、承認申請・認証取得が経過措置期間終了後となった場合であっても、承認申請・認証審査の中で基本要件第 12 条3項の適合確認は行われないとの理解で良いか。

A2：貴見のとおり。なお、製造販売業者において製造販売出荷までに適合性確認を行うこと。

Q3：承認申請・認証申請書の「性能及び安全性に関する規格欄」において、JIS T 81001-5-1 は JIS T 2304 と同様に記載する必要はないとの理解で良いか。

A3：貴見のとおり。

Q4：承認申請・認証申請において基本要件基準第 12 条第 3 項への適合を示す際、試験機関による JIS T 81001-5-1 への適合証明書を特定することで良いか。

A4：基本要件基準第 12 条第 3 項の適合性の確認のための第三者機関による試験は必須ではないが、試験機関を活用した場合、申請時においては、適合証明書に加えて、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の「2. JIS に関連する既存通知等の要求事項」に記載されている項目に対する適合性の確認結果を示すか又は確認結果をまとめた社内文書等を特定すること。

Q5：承認審査の際に要求されるサイバーセキュリティに係る別添資料は、信頼性書面調査（非臨床）の対象になるのか。もし対象になる場合、提出すべき根拠資料は何か。

A5：令和4年8月8日付薬生機審発 0808 第1号の適合性書面調査実施要領にあるとおり、規則第 114 条の 19 第1項第1号のロ及びホに規定する資料は、調査対象となる承認申請資料となっており、サイバーセキュリティに係る別添資料も信頼性調査の対象になり得る。なお、対象になった場合は、別添資料に添付する社内文書が根拠資料となる。

Q6：医療情報システムを対象とした「医療情報システムの安全管理に関するガイドライン」は、いわゆる「3省2ガイドライン」と呼ばれているもののひとつであるが、この「医療情報システムの安全管理に関するガイドライン」は医療機器も対象として扱われるガイドラインなのか。

A6：「医療情報システムの安全管理に関するガイドライン」は、医療情報（医療に関する患者情報（個人識別情報）を含む情報）を取り扱う医療機器（電子カルテ等医療情報を扱うシステムとネットワークがつながっている医療機器も含む）においても対応が必要となる。なお、医療情報の定義については、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）用語集を参照すること。

Q7：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に「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」とあるが、具体的に参考となる資料などはあるか。

A7：セキュリティ設計のベストプラクティスについては、JIS T 81001-5-1 の 5.3.2 及び 5.4.1 に例示されている。その他、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の別添「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）」の「5.1 セキュリティ要求事項及びアーキテクチャー設計」も参照すること。

Q8: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た場合、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の1.(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のうち、「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。」、「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。」及び「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。」の記載をどのようにすれば良いか。

A8: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、箇条4を実施し、5.2、5.7 及び 7.1 から 7.3 までの要求事項とのギャップ分析を含む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。また、トランジションヘルスソフトウェアを箇条6から箇条9までの要求事項に適合させるために移行計画を確立し、利用可能にすること。箇条6から箇条9までに規定するリリース後のアクティビティを履行すること。

なお、結果として、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で求める確認の際の留意点のうち、箇条5のソフトウェア開発プロセスに係る次の事項については、記載が不要とできるが、その他の項目については、確認が必要であり、継続仕様の根拠等についても示す必要がある。

- 開発計画を策定する際に、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。
- 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。

別添にトランジションヘルスソフトウェアを適用した場合の記載事例を示す。

Q9:外部委託先で製造されているが、開発時期が古く、製品標準書や設計開発の文書では使用ソフトが明らかになっていない医療機器について、SBOM を作成するために必要な情報が外部委託先から十分に提供されない場合や、独自開発されたソフトで脆弱性や脅威に関する情報やセキュリティに関する情報が保管されていない場合、この医療機器の製造販売を継続するためには製造販売業者としてどのように対処すれば良いか。

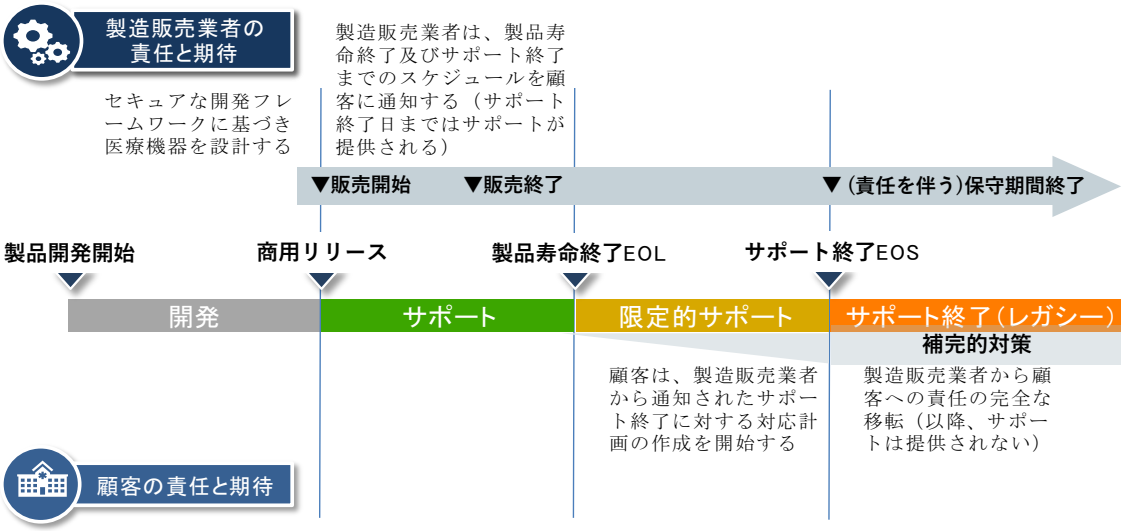
A9:基本要件基準の平成 26 年改正で、ソフトウェアのライフサイクル要件(JIS T 2304 等)が導入され、平成 29 年 11 月 25 日以降は基準への適合が必須となったことから、それ以降に設計開発された品目では構成管理情報が存在するため、そこから SBOM は作成可能である。

また、ライフサイクル要件が求められる前に開発された品目に対しては、平成 29 年5月 17 日付け薬生機審発 0517 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が含まれる。」と求めてきた経緯があるため、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て、継続使用に適することを確実にすること。

Q10：製品の寿命となる EOL 及び限定的サポート期間を経て商業的サービスも終了する EOS については、この限定的サポート期間を設けずに両者の日付を同日に設定することは可能か。

A10：医療機関にて新たな医療機器への買替え、ソフトウェアの更新等の対応を行う必要があることから、EOL と EOS との間の限定的サポート期間を考慮する必要がある。そのため、限定的サポート期間における計画を立案し、医療機関に対してあらかじめ提示する必要になる。



Q11：医療機器の市販後のサイバーセキュリティの確保は、製造販売後安全管理において実施することでよいか。

A11：貴見のとおり。製造販売業者は医薬品、医薬部外品、化粧品、医療機器及び再生医療等製品の製造販売後安全管理の基準に関する省令（平成 16 年厚生労働省令第 135 号）に則り製造販売後安全管理を行う必要がある。当該省令第七条から九条に規定されるとおり、サイバーセキュリティを確保するために必要な情報を収集し、遅滞なく検討した結果、必要があると認める時は、安全確保措置（医療関係者への情報提供、脆弱性対策（市販後のアップデート等を含む）等）を実施する必要がある。

なお、安全管理情報の収集にあたっては、安全管理責任者は国内品質業務運営責任者

等、その他の製造販売後安全管理に関係する部門の責任者と密接な連携を図り、国内品質業務運営責任者等が入手した情報のうち、品質に関するものについては、引き続きQMS 省令に基づき国内品質業務運営責任者等が必要な検討・措置を行うこと。

別　添

記載事例

4. 設計検証及び妥当性確認文書の要約

＜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、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「〇〇〇」
適合規格及び関連通知
JIS T 81001-5-1:2023 附属書F トランジションヘルスソフトウェア
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	令和〇〇年〇月〇日	□□ □□
承認	令和〇〇年〇月△日	△△ △△

本事例の注釈：Q10 に基づき、次頁の２項から、
説明が不要となる記載を省略した報告書の作成事例

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、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の規定を踏まえ、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)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分析書	社内文書〇〇
2	ソフトウェア開発プロセス	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。	・セキュリティ要求事項	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。	・システム構成図等(信頼境界含む)	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、セキュリティ更新等のための計画を行い、そ	・ソフトウェア保守計画書	社内文書〇〇

		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