ひと、くらし、みらいのために

厚生労働省
Ministry of Health, Labour and Welfare

pmda
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について

厚生労働省　医薬局医療機器審査管理課
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

この説明で用いる略語の一覧

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)
JIS T 81001-5-1	令和5年(2023年) 2月25日	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
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

ひと、くらし、みらいのために

厚生労働省
Ministry of Health, Labour and Welfare

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

- 医療機器を取り巻くサイバーセキュリティについて
- サイバーセキュリティに係る規制の概要について
- 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（Q&A）について
- 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

ひと、くらし、みらいのために

厚生労働省
Ministry of Health, Labour and Welfare

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

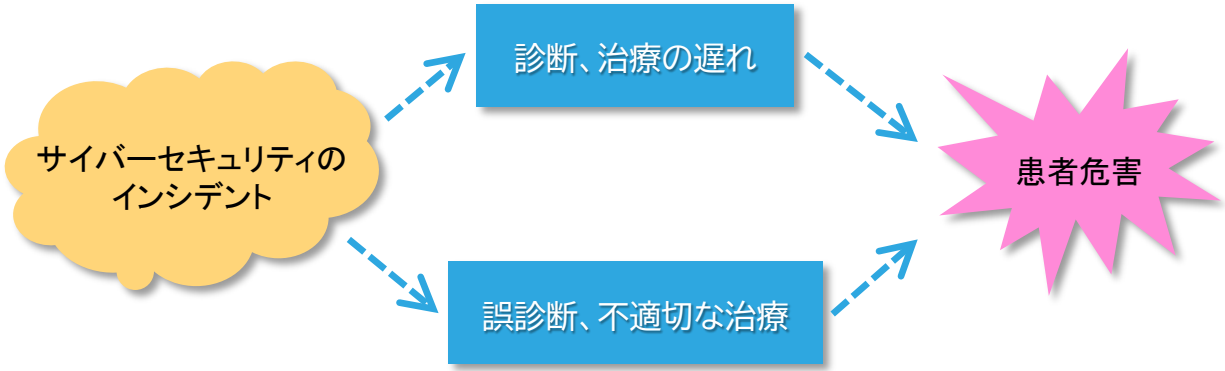
- **医療機器を取り巻くサイバーセキュリティについて**
- サイバーセキュリティに係る規制の概要について
- 医療機器の基本要件基準第12条第3項の適用に関する質疑応答集（Q&A）について
- 医療機器のサイバーセキュリティに関する質疑応答集（Q&A）について

医療機器のサイバーセキュリティについて

サイバーセキュリティのインシデントは、医療機器及び病院ネットワークを使用不能にすると共に、ヘルスケア施設における患者ケアの提供を中断させてきた経緯がある。

これらのインシデントは、診断及び治療介入の遅延、誤診断又は不適切な治療介入等の発生により、患者危害に至る可能性がある。

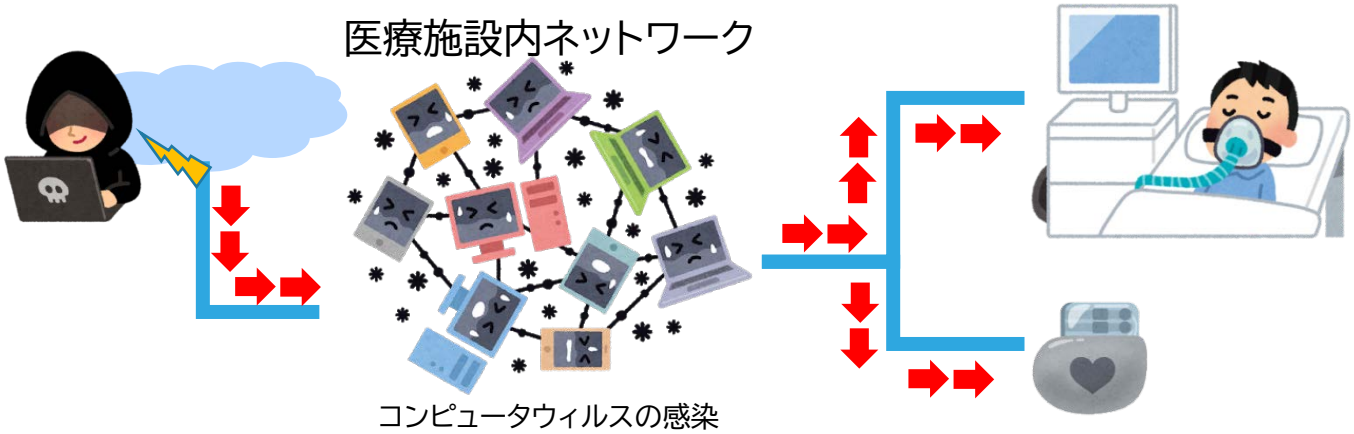
IMDRF　医療機器サイバーセキュリティの原則及び実践「1.0 はじめに」より



医療機器においては、製品ライフサイクル全体において、患者危害のリスクを最小限にすることが求められるが、サイバーリスクに対しては、情報やシステムを適切に保護し、機密性・可用性・完全性に係るリスクを最低限にする、すなわちサイバーセキュリティの確保によって、患者安全を担保する。

医療機器へのサイバーリスクとその対応の基本的考え方①

事例）医療機関のネットワーク等に接続された他のコンピュータ等がサイバー攻撃を受けた際に、ネットワークを介して医療機器がサイバー攻撃を受けるリスク

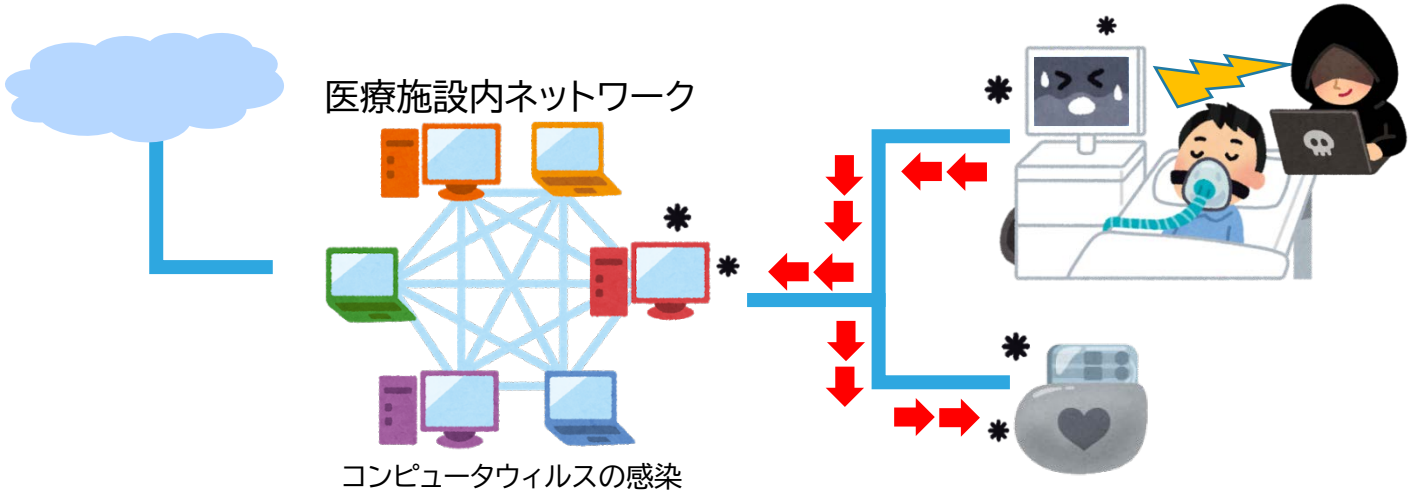


このリスクを低減するために

基本的考え方①
医療機器が**サイバー攻撃による影響を受けない**ように、**製品としての耐性**を持ち、かつ、**医療施設内での管理**のために医療機関と製販との連携が必要

医療機器へのサイバーリスクとその対応の基本的考え方②

事例）医療機器がサイバー攻撃を受けた際に、接続された医療機関等のネットワークを介して他の医療機器やコンピュータ等もサイバー攻撃を受け、障害が引き起こされる可能性



このリスクを低減するために

基本的考え方②
医療機器が感染源にならないように設計・製造され、かつ、市販後に適正な管理がなされることが必要

医療機器を取り巻くサイバーセキュリティについて

製造販売業者 ⟷ 連携 ⟷ **医療機関**

○製造・販売・流通する医療機器については、サイバーリスクを低減する措置を講じること。

※医薬品医療機器等法に基づく基本要件基準に規定

○病院等（病院、診療所又は助産所）の管理者は、安全管理のための体制（医療機器の保守点検の実施体制も含む）を確保すること。

○病院等の管理者は、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を確保するために必要な措置を講じること。

※医療法施行規則に規定

医療機器を取り巻くサイバーセキュリティに係る関連法令及びガイダンス

医療法施行規則第14条第2項と基本要件基準第12条第3項では目的や位置づけが異なる事から、主体となる組織や適用範囲が異なる。

【医療法施行規則第1条の11第1項】
病院等の管理者は、法第6条の12の規定に基づき、次に掲げる**安全管理のための体制を確保**しなければならない。
一　医療に係る安全管理のための指針を整備すること。

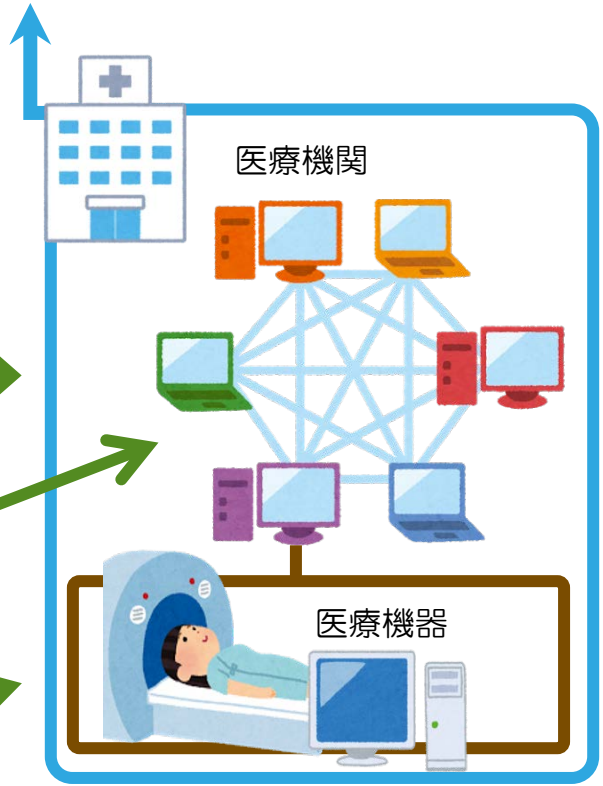
【医療法施行規則第14条第1項】
病院又は診療所の管理者は、その病院又は診療所に存する医薬品、医療機器及び再生医療等製品につき**医薬品医療機器等法の規定に違反しないよう必要な注意**をしなければならない。

【医療法施行規則第14条第2項】
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。

【医療情報システムの安全管理に関するガイドライン】
医療機関が主体となって医療情報システムの機密性・完全性・可用性を確保するために**医療情報システムの安全管理**を行う。

※1 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）

【基本要件基準第12条第3項】
医療機器製造業者が主体となって、サイバーリスクに対する**医療機器の機能性**と**患者の安全を保持**する。
医療機関に対して必要な情報提供及び連携を図る。
※根拠法：医薬品医療機器等法



ひと、くらし、みらいのために

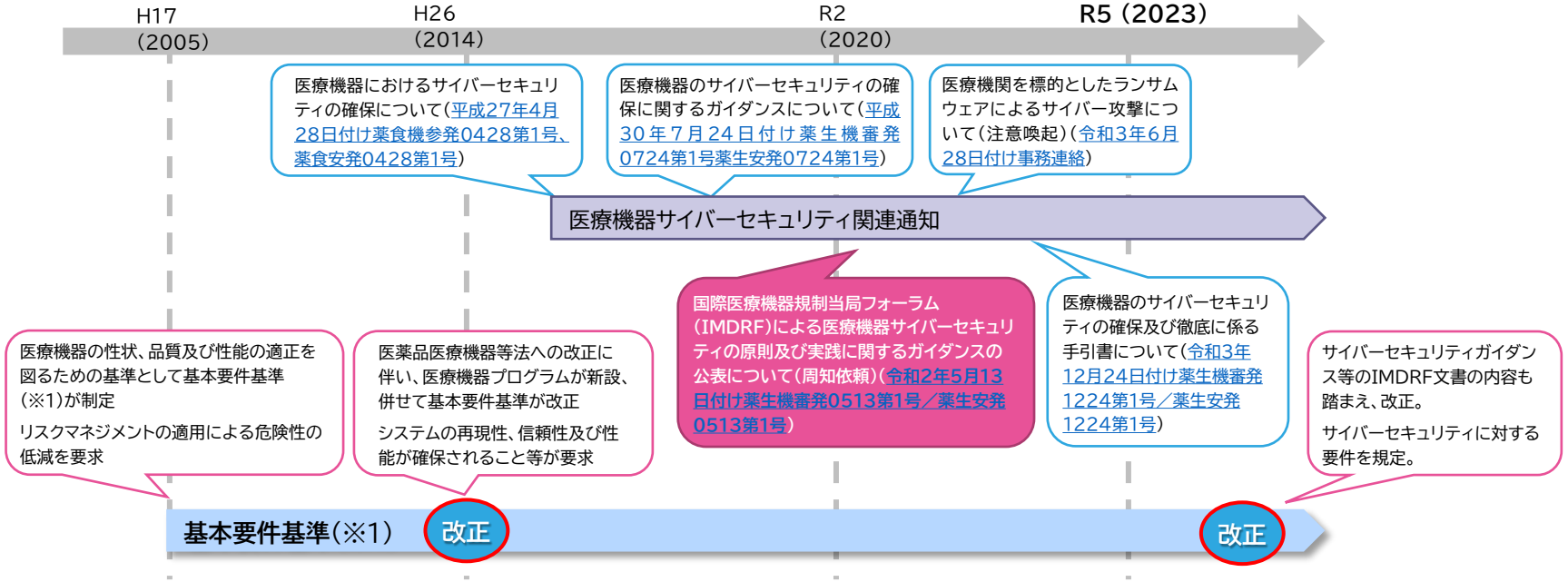
厚生労働省
Ministry of Health, Labour and Welfare

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

- 医療機器を取り巻くサイバーセキュリティについて
- **サイバーセキュリティに係る規制の概要について**
- 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（Q&A）について
- 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

サイバーセキュリティ対応のための基本要件基準改正の経緯

平成27年に医療機器に対するサイバーセキュリティ対応を明確化し、製造販売業者に対する対応を指示したところ。
その後も必要に応じて関連通知を発出。
令和5年3月に、サイバーセキュリティガイダンス等のIMDRF文書の内容を踏まえ、基本要件基準を改正。



※1 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、平成26年厚生労働省告示403号一部改正、令和5年厚生労働省告示67号一部改正）

医療機器サイバーセキュリティに関連する主な通知

平成27年4月28日付 薬食機参発 0428 第1号、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 【確保通知】
平成30年7月 24 日付 薬食機参発 0724 第1号、薬食安発 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 【ガイダンス通知】
令和2年5月13日付 薬生機審発0513第1号、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)
令和2年10月7日付 事務連絡	臨床試験におけるサイバーセキュリティインシデントについて
令和3年6月28日付 事務連絡	医療機関を標的としたランサムウェアによるサイバー攻撃について(注意喚起)
令和3年10月20日付 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
令和3年11月26日付 事務連絡	医療機関を標的としたランサムウェアによるサイバー攻撃について(再注意喚起)
令和3年12月24日付 薬生機審発1224第1号、薬生安発1224第1号【廃止】	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4年3月1日付 事務連絡	医療機器等に関するサイバーセキュリティ対策の強化について(要請)
令和4年11月10日付 事務連絡	医療機関等におけるサイバーセキュリティ対策の強化について(注意喚起)
令和5年3月31日付 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 【取扱い通知】
令和5年3月31日付 薬生機審発0331第11号、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 【製販向け手引書通知】
令和5年3月31日付 医政参発0331第1号、薬生機審発0331第16号、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
令和5年5月23日付 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 【適合性確認通知】
令和5年7月20日付 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 【QA】
令和6年1月31日付 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 【QA2】

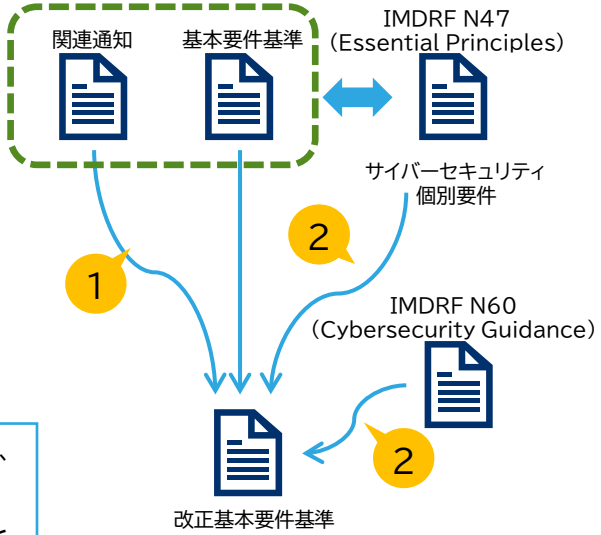
R05.03.09 基本要件基準改正
(厚生労働省告示第69号)

医療機器のサイバーセキュリティ対応のための基本要件基準改正

基本要件基準：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、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を要求

1. サイバーセキュリティ対策については、平成27年4月28日付の確保通知や平成30年7月24日付のガイダンス通知において必要な対応を行うよう求めてきたところ

2. 令和2年のIMDRF「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」において、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、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きたところ（IMDRF N47文書及びN60文書）



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。

⇒ 令和5年3月9日基本要件基準を一部改正し第12条3項を規定。
（令和5年4月1日より運用開始（経過措置1年間））

「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）**【取扱い通知】**

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。

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

対象となる医療機器の明確化

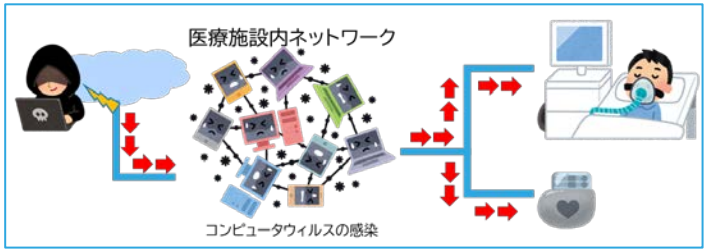
ソフトウェアを意図したとおりに動作させるために必要最低限な要件（動作環境及び使用環境）の特定

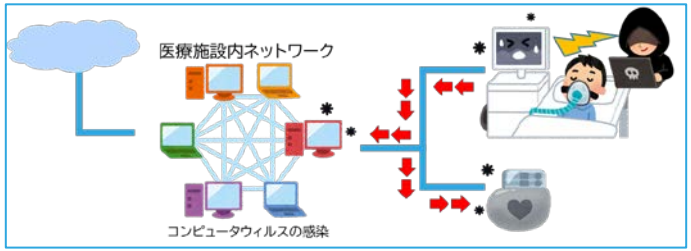
サイバーリスクを適切に低減する設計及び製造（サイバーリスクの特定及び評価）

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

該当する場合、サイバーセキュリティのリスクを考慮して、以降の事項に対する適合性を確認する。

想定すべきサイバーリスクの例





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。

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

対象となる医療機器の明確化

ハードウェア、ネットワーク、ITセキュリティ対策の最低限の要件設定

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

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）

サイバーリスクを低減する設計、製造

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

製品ライフサイクル全体に対する配慮

サイバーセキュリティを確保する設計、製造及び保守

IMDRF N47文書の5.8.4

Manufacturers should set out minimum requirements concerning hardware, IT networks characteristics and IT security measures, including protection against unauthorized access, necessary to run the software as intended.

（製造販売業者は、ソフトウェアを意図したとおり動作させるのに必要なハードウェア、ITネットワーク特性、及び不正なアクセスに対する防護を含むITセキュリティ対策について最低限の要件を設定しなければならない）

IMDRF N47文書の5.5.6

Medical devices and IVD medical devices should be designed and manufactured in such a way as to appropriately reduce the risk of unauthorized access that could hamper the device from functioning as intended or impose a safety concern.

（医療機器及びIVD医療機器は、意図する機能を妨げる又は安全性の懸念を課す不正アクセスの危険性を適切に低減するよう設計及び製造されていなければならない）

IMDRF N47文書の5.8.5

The medical device and IVD medical device should be designed, manufactured and maintained in such a way as to provide an adequate level of cybersecurity against attempts to gain unauthorized access.

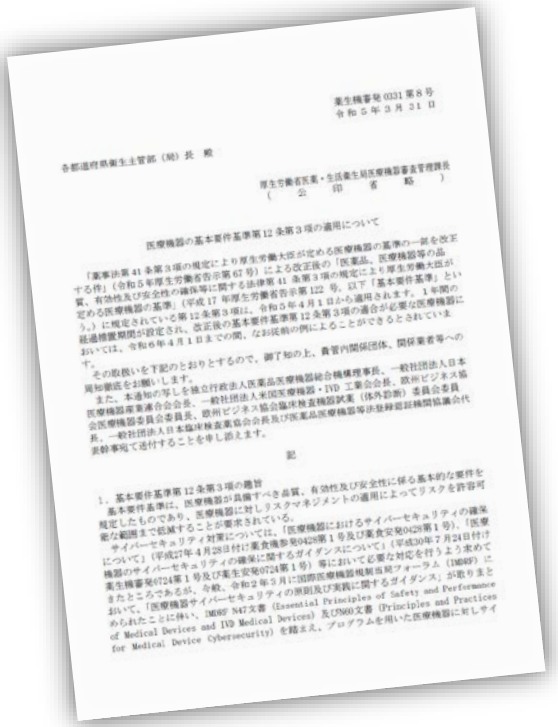
（医療機器及びIVD医療機器は、不正アクセスの侵入に対するサイバーセキュリティの適切なレベルを提供するよう、設計、製造及び保守されていなければならない）

IMDRF N60文書

4.2 Total Product Life Cycle（製品ライフサイクルの全体）
To effectively manage the dynamic nature of cybersecurity risk, risk management should be applied throughout the total product life cycle (TPLC) where cybersecurity risk is evaluated and mitigated in the various phases of the TPLC including but not limited to design, manufacturing, testing, and post-market monitoring activities.
（サイバーセキュリティの動的特性を効果的に管理するためには、リスクマネジメントを製品の全ライフサイクルに渡って適用し、設計、製造、試験及び市販後監視等の各過程においてサイバーセキュリティリスクを評価及び緩和することが望ましい。

- 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”

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）【取扱い通知】



薬生機審発 0331 第 8 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 ）

医療機器の基本要件基準第 12 条第 3 項の適用について

「薬事法第 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。）に規定されている第 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、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ついては、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ます。

その取扱いを下記のとおりとするので、御了知の上、貴管内関係団体、関係業者等への周知徹底をお願いします。

また、本通知の写しを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、一般社団法人米国医療機器・IVD 工業会会長、欧州ビジネス協会医療機器委員会委員長、欧州ビジネス協会臨床検査機器試薬（体外診断）委員会委員長、一般社団法人日本臨床検査薬協会会長及び医薬品医療機器等法登録認証機関協議会代表幹事宛て送付することを申し添えます。

記

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CN60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

- 基本要件基準の第12条第3項の取扱いについて、次の内容を示したもの
  - ✓ 基本要件基準第12条第3項の趣旨
  - ✓ 基本要件基準第12条第3項の要点・解釈
  - ✓ 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
  - ✓ 経過措置について

販売、製造等の禁止

基本要件基準に適合しない医療機器は、販売、製造等を禁止。

（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

二　第23条の2の5若しくは第23条の2の17の厚生労働大臣の承認を受けた医療機器又は第23条の2の23の認証を受けた医療機器であつて、その性状、品質又は性能がその承認又は認証の内容と異なるもの（第23条の2の5第16項（第23条の2の17第5項において準用する場合を含む。）又は第23条の2の23第8項の規定に違反していないものを除く。）

三　第42条第2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、その基準に適合しないもの

四　その全部又は一部が不潔な物質又は変質若しくは変敗した物質から成つている医療機器

五　異物が混入し、又は付着している医療機器

六　病原微生物その他疾病の原因となるものにより汚染され、又は汚染されているおそれがある医療機器

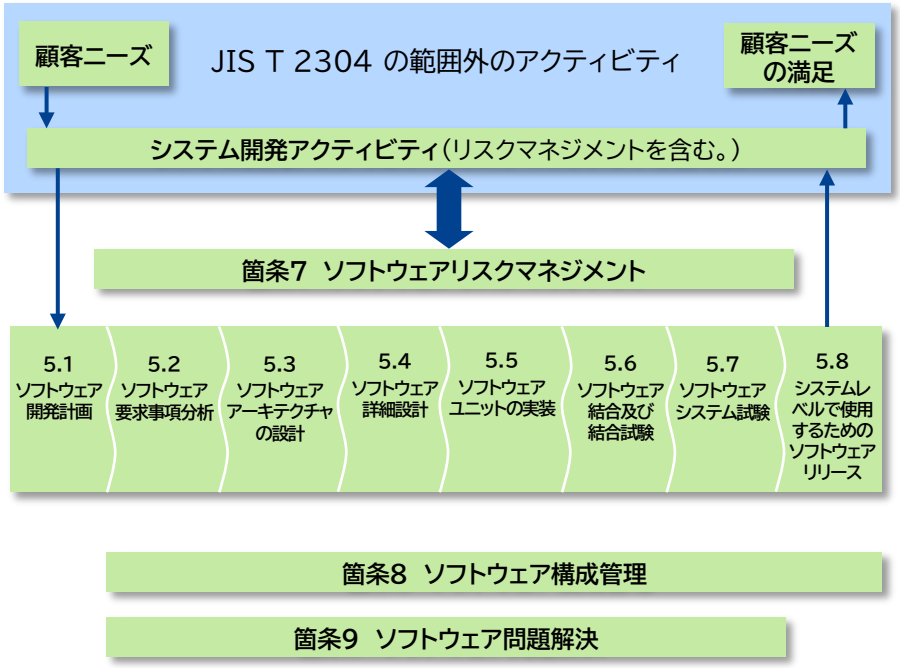
七　その使用によつて保健衛生上の危険を生ずるおそれがある医療機器

JIS T 2304のソフトウェアライフサイクルプロセス

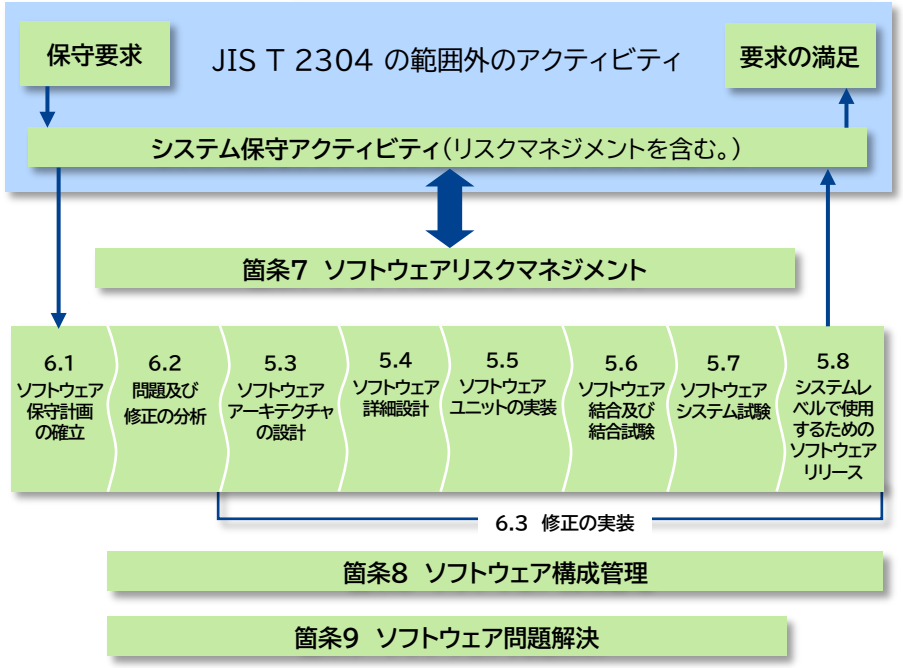
安全なソフトウェアを実現するためには、試験を実施するだけではなく、次が必要

- 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。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。



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

ヘルスソフトウェアの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JIS T 2304の順序で記載

JIS T 2304	JIS T 81001-5-1
4. 一般要求事項	4. 一般要求事項
5. ソフトウェア開発プロセス	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	6. ソフトウェア保守プロセス
7. ソフトウェアリスクマネジメントプロセス	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	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	9. ソフトウェア問題解決プロセス

製造業者が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、ヘルスソフトウェアを開発し保守することを規定

製造業者が実施するソフトウェアライフサイクルプロセスの一部として、アクティビティ及びその結果のアウトプットを規定

製造業者が実施する問題解決プロセスの一部として、アクティビティ及びその結果のアウトプットを規定

医療機器の場合、ソフトウェア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が求められていることから、JIS T 81001-5-1では、セキュリティライフサイクルプロセスを別途規定するのではなく、既存のプロセスの枠組みに追加するアクティビティを規定。

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、

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

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。

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、ソフトウェアの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。

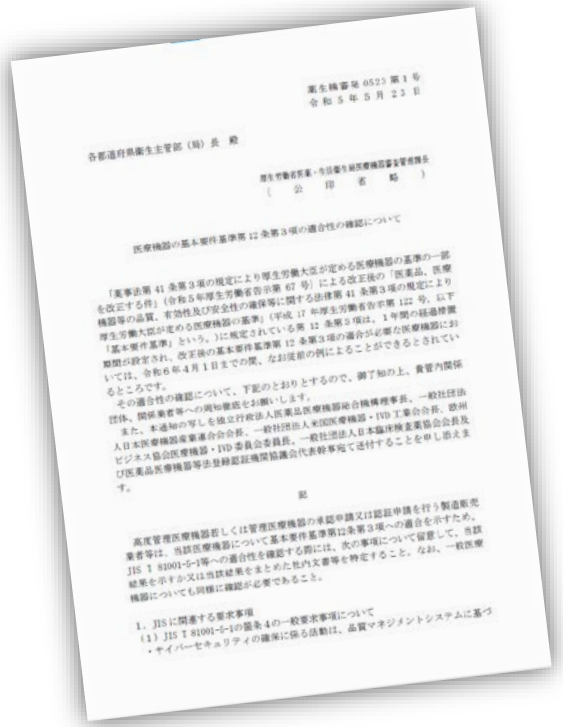
それぞれの要件に対して、文書番号等の社内文書を特定する情報を示し、提示できるようにしておく(Q&A＃2)

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。

「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)**【取扱い通知】**
「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」
(令和5年5月23日付け薬生機審発0523第1号)**【適合性確認通知】**

「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)も発出

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）【適合性確認通知】



薬生機審発 0523 第 1 号
令 和 5 年 5 月 23 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 ）

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

「薬事法第 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。）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ついては、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ので、御了知の上、貴管内関係団体、関係業者等への周知徹底をお願いします。

また、本通知の写しを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、一般社団法人日本臨床検査薬協会会長及び医薬品医療機器等法登録認証機関協議会代表幹事宛て送付することを申し添えます。

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、当該結果を示すかぶ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

Q&A#1

- 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
- 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を示したもの

  Ex）「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」

※ JIS T 81001-5-1の原典であるIEC 81001-5-1の全体的な解説は、PMDAの以下サイトをご参照ください。

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）

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）【適合性確認通知】

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。	

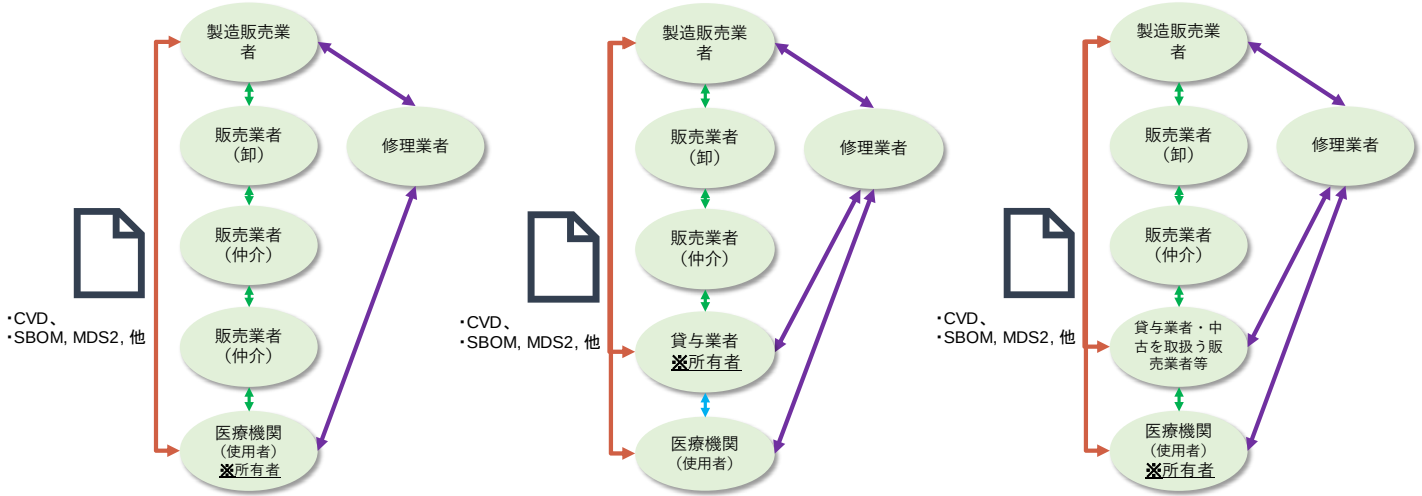
医療機器の基本要件基準第12条第3項の適合性の確認 について（令和5年5月23日付け薬生機審発0523第1号）【適合性確認通知】

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	
5 （開発プロセス）		
6 （保守プロセス）		寿命に対して計画し、脆 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。	

- 詳細については、別資料にて説明する。
- 申請においては、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**社内文書を特定**する。
- 第3者機関による試験を活用して適合を示す場合も、適合性確認通知の**第2項の確認事項の実施**について示すこと。

サイバーセキュリティ対応における連携

サイバーセキュリティ対応においても、他の安全確保処置と同様に販売業者等を含めた連携が必要
SBOM、脆弱性情報、アドバイザリー等情報の性格上、確実性に加え即時性が必要



通常　　リース医療機器の場合　　中古医療機器の場合

※ 令和5年3月31日薬生機審発0331第11号・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」より引用

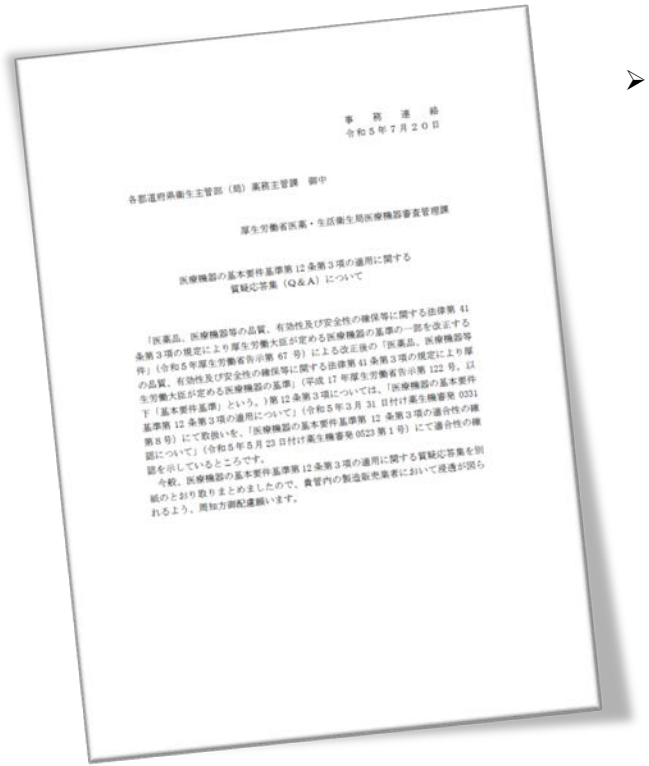
ひと、くらし、みらいのために

厚生労働省
Ministry of Health, Labour and Welfare

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

- 医療機器を取り巻くサイバーセキュリティについて
- サイバーセキュリティに係る規制の概要について
- **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（Q&A）について**
- 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）【QA事務連絡】



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遺漏が無られるよう、周知方御配慮願います。

- 医療機器の基本要件基準第12条第3項の適用に関して、質疑応答集として取りまとめたもの

QA#1： 適合性確認通知の位置づけ

Q	A
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。

QA＃2： 承認、認証申請におけるJIS T 81001-5-1への適合は、社内文書を特定する情報を示すことでよいか

Q	A
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。

QA#3： 既存品目に対しては、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

Q	A
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 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。

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

QA#4：セキュリティに対する問い合わせ窓口の明確化とは具体的に何か

Q	A
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。

QA＃5： 承認、認証申請においてSBOMを提出する必要はあるか

Q	A
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。

QA＃6： SBOMの構成として定められているものは

Q	A
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）

QA#7: 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

Q	A
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。

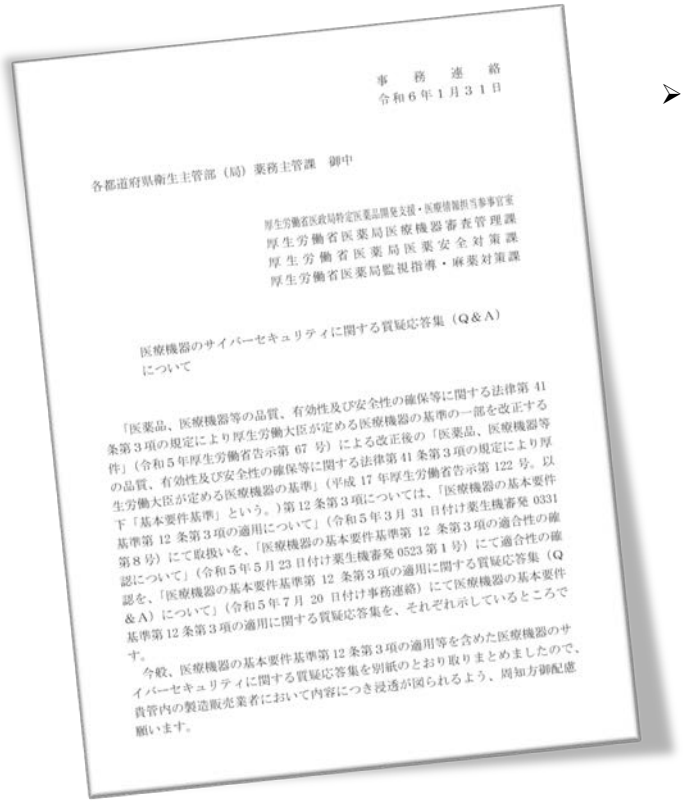
ひと、くらし、みらいのために

厚生労働省
Ministry of Health, Labour and Welfare

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

- 医療機器を取り巻くサイバーセキュリティについて
- サイバーセキュリティに係る規制の概要について
- 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（Q&A）について
- **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（令和6年1月31日付け事務連絡）【QA事務連絡2】



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。

- 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して、質疑応答集として取りまとめたもの

QA2＃1： 保守や修理作業のみでネットワーク接続する場合のサイバーセキュリティ評価

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。 適合性確認通知においては、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。

QA2＃2： 経過措置期間中の承認・認証申請に対する審査

Q	A
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。

QA2＃3： 承認・認証申請書の「性能及び安全性に関する規格欄」にJIS T 81001-5-1の記載は必要か

Q	A
Q3 承認・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よいか。	A3 貴見のとおり。

QA2＃4： 基本要件基準第12条第3項への適合は、試験機関によるJIS T 81001-5-1の適合証明書の特定でよいか

Q	A
Q4 承認申請又は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よいか。	A4 基本要件基準第12条第3項の適合性の確認する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、申請時において適合証明書に加えて、適合性確認通知の「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。

QA2＃5： 承認審査の場合、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

Q	A
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号の口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、別添資料に記載する社内文書が根拠資料となる。

QA2＃6： 医療情報システムの安全管理ガイドラインは、医療機器も対象か

Q	A
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。

QA2＃7：セキュリティ設計のベストプラクティスについての参考資料は

Q	A
Q7 適合性確認通知に「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、製販向け手引書通知の別添「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。

QA2＃8： 附属書Fを適用した場合、適合性確認通知の開発プロセスに係る項目の記載はどうしたらよいか

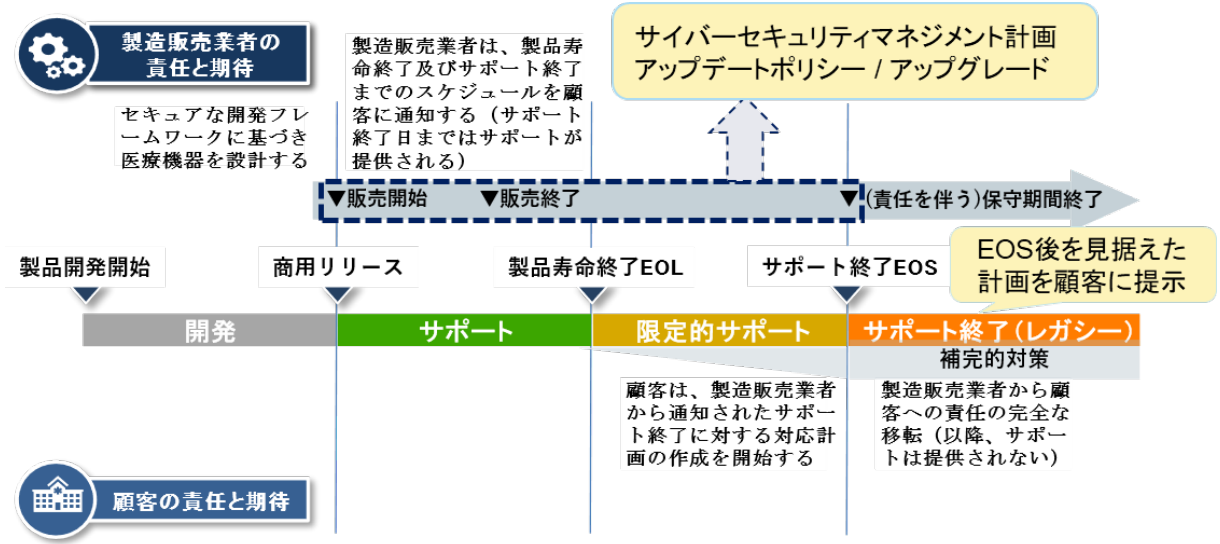
Q	A
Q8 JIS T 81001-5-1の附属書F トランジションヘルスソフトウェアを適用した場合、適合性確認通知の1.(2) JIS T 81001-5-1の箇条5のソフトウェア開発プロセスについてのうち、「開発計画において、セキュリティ更新や開発環境等のセキュリティについて考慮すること。」、「意図する使用環境、信頼境界、多層防御等を考慮してアーキテクチャー設計を行うこと。」及び「セキュリティ設計のベストプラクティスを考慮した設計及び実装を行うこと。」の記載をどのようにすればよいか。	A8 JIS T 81001-5-1の附属書F トランジションヘルスソフトウェアを適用する場合は、箇条4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。

QA2＃9： 開発時期が古い製品のSBOMの作成について

Q	A
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（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、ライフサイクルの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、継続使用に適することを確実にすること。

QA2#10：EOLとEOSの日付を同日に設定できるか

Q	A
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ことが必要になる。



サポート終了（End of Support：EOS）

製品のライフサイクルにおいて、顧客への責任移転が完了し、製造販売業者が、全てのサポート活動を終了する時点。

レガシー医療機器

現在のサイバーセキュリティの脅威に対して合理的な手段で保護できない場合は、販売開始以降の年数にかかわらずレガシーであるとみなされる。

QA2＃11： 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ればよいか

Q	A
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、品質に関する情報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。

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

医薬安発0115 第２号
令和６年１月15 日

各都道府県衛生主管部（局）長 殿

厚生労働省医薬局医薬安全対策課長
（ 公印省略）

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

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、医療機器のサイバーセキュリティに関する具体的なリスクマネジメント並びにサイバーセキュリティ対策及び処置の考え方については、「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・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）として取りまとめられており、製造販売業者は、サイバーリスクに伴う医療機器の不具合等を「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）における安全管理情報として取り扱い、適切な製造販売後安全管理を行う必要があることを示しています。

製造販売業者等が行う不具合等の報告については、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）第68 条の10 第1 項により規定され、その取扱いは「「医薬品等の副作用等の報告について」の一部改正について」（令和３年７月30 日付け薬生発0730 第８号厚生労働省医薬・生活衛生局長通知）により示しているところです。

今般、医療機器に対するサイバーセキュリティの確保を一層強化するため、製造販売業者等が行う不具合等の報告について、「新たな形態の医療機器等をより安全かつ有効に使用するための市販後安全対策のあり方に関する研究」（厚生労働行政推進調査事業費補助金（医薬品・医療機器等レギュラトリーサイエンス政策研究事業）、研究代表者 国立医薬品食品衛生研究所 医療機器部 サイバーセキュリティワーキンググループにおいて、別添のとおり「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」が取りまとめられましたので、御了知の上、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の製造販売後安全管理が円滑に行えるよう、貴管下関係製造販売業者等への周知及び指導等よろしくお願いいたします。

医療機器のサイバーセキュリティに関する情報について

https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/0000179749_00009.html

関連通知やIMDRF文書も含め厚労省HPにて掲載

ひと、くらし、みらいのために

厚生労働省
Ministry of Health, Labour and Welfare

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。