

医療機器のサイバーセキュリティについて (2023年度 登録認証機関向けトレーニング資料)

Slide 0



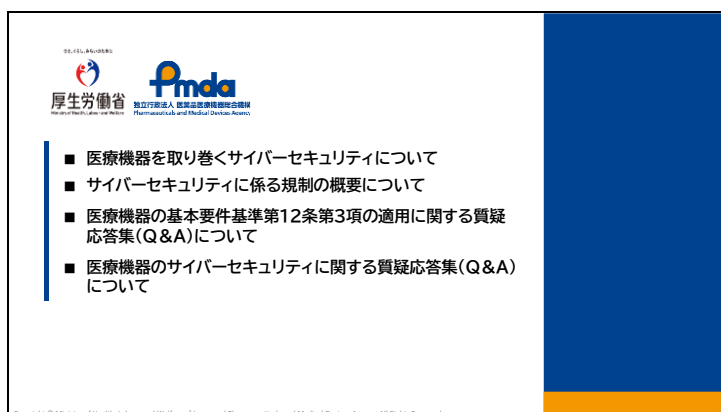
医療機器のサイバーセキュリティについて説明します。

Slide 1

| 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」(食食機審発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指導係 |
| 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」厚生労働省医薬局特定医薬品開発支援・医療情報担当参事官至、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 |

この資料においては、関連する通知等について、次のように略しています。

Slide 2



ここでは、医療機器に求められるサイバーセキュリティについて、次の流れで説明します。

はじめに、医療機器を取り巻くサイバーセキュリティについて、次に、サイバーセキュリティに係る規制の概要について、説明します。

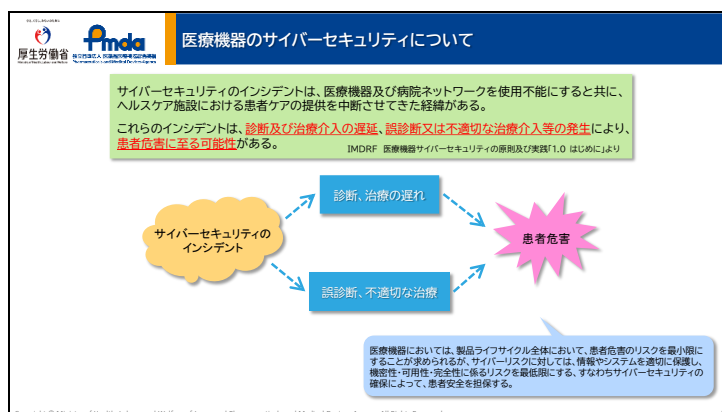
その後、Q&A形式の事務連絡が2件発出されていますので、Q&Aの内容について説明します。

Slide 3



まず、医療機器を取り巻くサイバーセキュリティについて説明します。

Slide 4



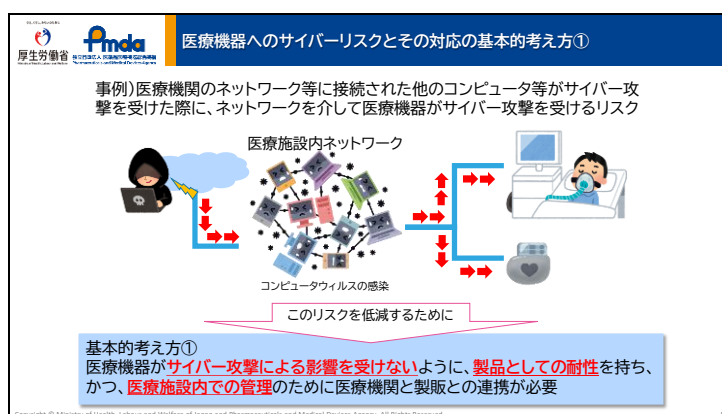
医療機器を取り巻くサイバーセキュリティの状況について、説明します。

このスライドはIMDRF 医療機器サイバーセキュリティの原則及び実践の「はじめに」に記載されている内容になりますが、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要にするとともに、ヘルスケア施設における患者のケアの提供を中断させてきた経緯があります。

そして、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、患者危害の発生につながる可能性があります。

そのため、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求められますが、サイバーリスクに対して、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ことが求められます。

Slide 5



次に、医療機器へのサイバーリスクとその対応について、基本的な考え方を説明します。

医療機器に対するサイバーリスクは、大きく2つのリスクがあります。

一つ目は、医療機関のネットワーク等に接続された、他のコンピューター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

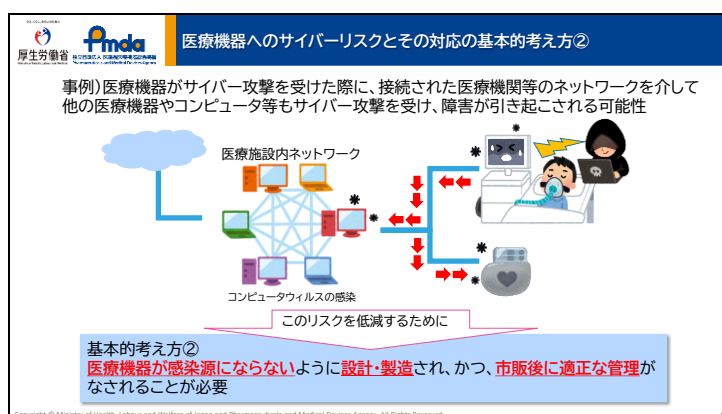
クの事例です。

院内のネットワークにつながる機器がコンピュータウイルスに感染し、それが医療機器の誤動作や動作停止を招いてしまうといった例になります。

この例では、人工呼吸器のようなものとペースメーカーのようなものをポンチ絵で描いていますが、人工呼吸器自体がネットワークで直接つながっていないとしても、USBメモリ等を経由してマルウェアが持ち込まれるとか、ペースメーカーの場合は、ペースメーカーのプログラマーが攻撃を受けて、最終的にペースメーカーの誤動作等につながるなどのシナリオになるかと思います。

このリスクを低減するための基本的な考え方としては、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なされることが必要、ということになります。

Slide 6



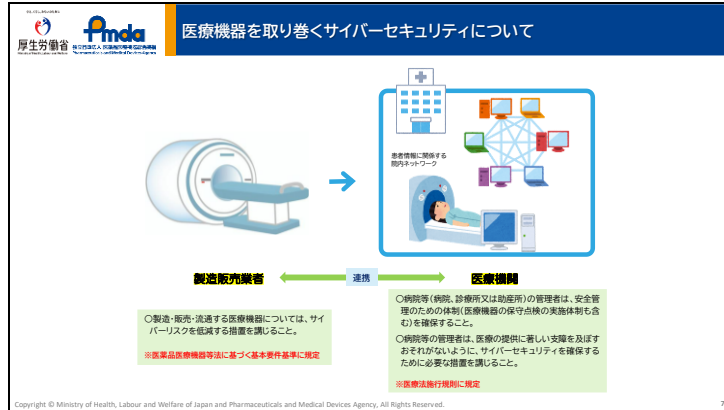
もう一つは、医療機器がサイバー攻撃を受けた際に、接続された医療機関等のネットワークを介して、他の医療機器やコンピュータ等もサイバー攻撃を受け障害が引き起こされる可能性、ということになります。

このリスクを低減するための基本的な考え方は、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、となります。

いずれの場合にも、製造販売業者における、設計、製造が適正に行われていることはもちろんですが、医療機関における医療機器の適正な管理も重要になります。

たとえば、セキュリティのアップデートをきちんと適用するとか、パスワードの管理を適正に行う、プログラム医療機器が動作するプラットフォームのネットワーク設定等を適切に行う等が必要になります。

Slide 7



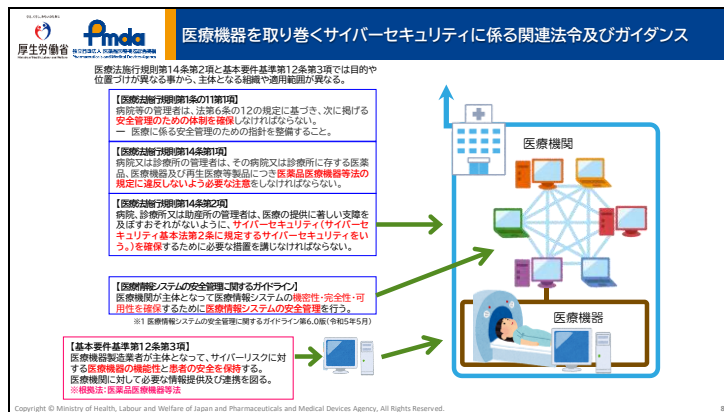
これら二つの側面のサイバーリスクを考えると、医療機関のネットワークに接続される医療機器については、製造販売業者と医療機関とで連携して対応していく必要があることがわかつています。

製造販売業者及び医療機関に求められるサイバーセキュリティに対する要件は、それぞれ薬機法、医療法の下で定められています。

薬機法については、基本要件基準の改正によってサイバーセキュリティの要件が規定されております。

医療法については、医療法施行規則に規定があります。

Slide 8



具体的には、医療法施行規則のこれらの規定、及び、基本要件基準の第12条第3項が対応します。

基本的にはサイバーセキュリティの確保という共通の目標に対応するが、医療法施行規則と基本要件基準とでは、目的や位置づけが異なることから、主体となる組織や適用範囲が異なります。

なお、医療機関が主体となって医療情報システムの機密性、可用性、完全性を確保するために医療情報システムの安全管理ガイドラインが定められていますが、医療機関の

医療機器のサイバーセキュリティについて

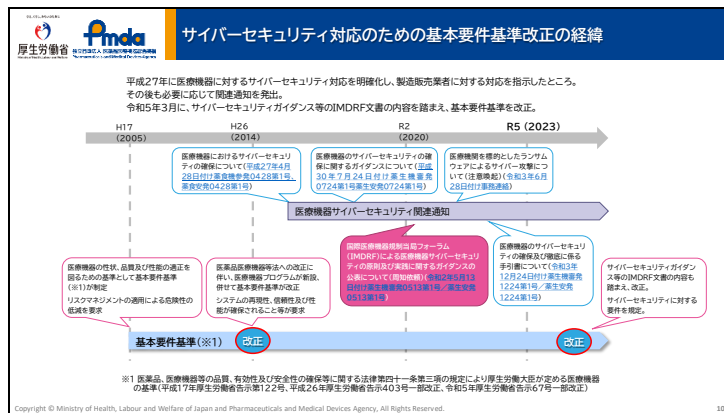
ネットワークに接続され、患者処方等の医療情報のやり取りを行う医療機器についてもこのガイドラインの対象となるため、医療機関の求めに応じて、情報提供や連携が求められることに注意が必要です。

Slide 9



続いて、サイバーセキュリティに係る規制の概要について説明します。

Slide 10



医療機器のサイバーセキュリティ対応に関する変遷について、まとめたものになります。

平成27年4月28日付で「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」を发出し、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ものとして明示化したところです。

また、令和2年5月には、サイバーセキュリティガイダンスの公表について周知のための通知が发出され、その中で3年をめぐりにIMDRFサイバーセキュリティガイダンスを国内に導入することが示されました。

医療機器のサイバーセキュリティについて

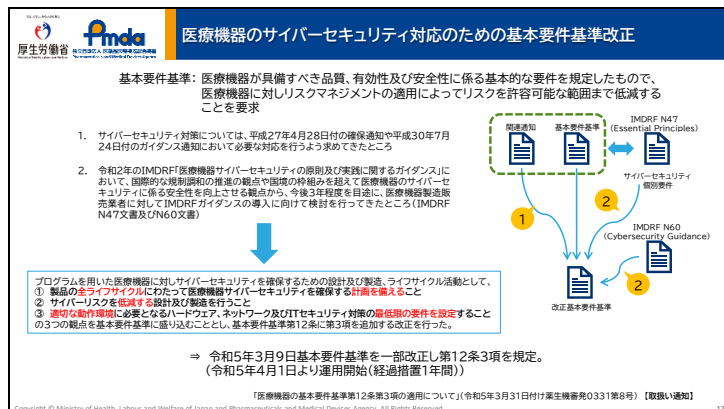
その後、サイバーセキュリティガイダンスを基に国内の状況を考慮してまとめた、手引書が令和3年12月に発行され、サイバーセキュリティガイダンス等のIMDRF文書の内容を踏まえ、令和5年3月に基本要件基準を改正いたしました。

Slide 11

| 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シナリオについて |
| 令和3年6月28日付 事務連絡 | 医療機器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「医療機器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 | 医療機器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【修正】 | 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(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【製薬向け手引書通知】 |
| 令和5年3月31日付 医政学発0331第1号、薬生機審発0331第16号、薬生安発0331第1号 | 医療機器における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】 |

医療機器サイバーセキュリティに関連する主な通知は表のとおりで、先ほどご説明した通知以外にもサイバー攻撃に関する通知を発出しています。

Slide 12



基本要件基準第12条第3項の制定の趣旨です。

医療機器のサイバーセキュリティ対応に関する変遷について、先ほどご説明させていただいたところですが、令和5年3月31日付けの取扱い通知でも示しておりますが、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なハードウェア、ネットワーク及びITセキュリティ対

医療機器のサイバーセキュリティについて

策の最低限の要件を設定すること

の3つの観点の基本要件基準に盛り込むこととし、基本要件基準を改正いたしました。

Slide 13

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、外部記録媒体、電子システム接続のためのソフトウェア等に接続する医療機器
対象となる医療機器の明確化

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

ハードウェア、ソフトウェア、ITセキュリティ対策の適切な要件特定

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

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。

医療機器ネットワーク
コンピュータシステム環境

医療機器ネットワーク
コンピュータシステム環境

想定すべきサイバーリスクの例

Copyright © Ministry of Health, Labour and Welfare of Japan and Pharmaceuticals and Medical Devices Agency. All Rights Reserved.

基本要件基準第12条第3項の内容についてですが、ここに示しているような内容になっています。

最初のパートでは、対象となる医療機器の明確化を行い、

次にソフトウェアを意図したとおりに動作させるための必要最低限な要件（動作環境や使用環境）を特定すること、

そしてサイバーセキュリティのリスクを適切に低減する設計及び製造を行うこと、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数々な設計、製造及び保守を行うこと、を求めています。

Slide 14

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。

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に動作させるために必要となるハードウェア、ソフトウェア、及び不正アクセスに対する保護を含む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発生させる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、製造及び保守が行わ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管理)

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, etc.).

(サイバーセキュリティの動的な性質を効果的に管理するためには、製品ライフサイクルのさまざまな段階を通じて、設計、製造、試験及び市場監視の各段階においてサイバーセキュリティリスクを評価及び軽減することが望ましい。)

IMDRF N47 文書: IMDRF/GRSP 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"

Copyright © Ministry of Health, Labour and Welfare of Japan and Pharmaceuticals and Medical Devices Agency. All Rights Reserved.

この内容については、平成27年に出されているサイバーセキュリティ確保通知の内容に加えて、IMDRFで定めた、医療機器の基本要件についてのN47文書及びサイバーセキュリティについてのN60文書を踏まえたものになっています。

つまり、N47文書における

5.8.4のハードウェア、ネットワーク、ITセキュリティ対策の最低限の要件設定

5.5.6のサイバーリスクを低減する 設計、製造

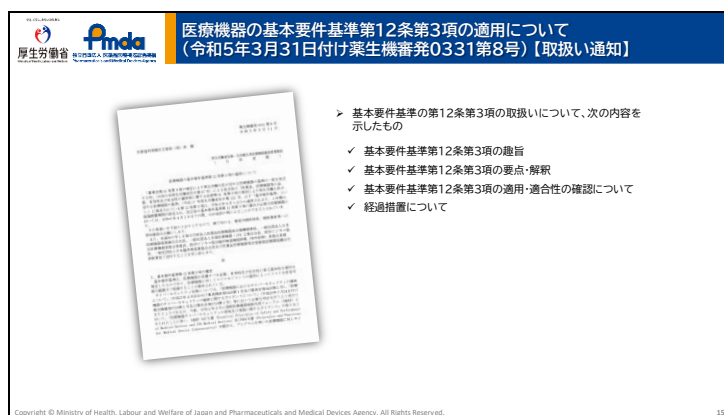
5.8.5のサイバーセキュリティを確保する設計、製造及び保守

N60文書における

4.2の製品ライフサイクル全体に対する配慮

を反映しています。

Slide 15



次に3月31日付けの取扱い通知に関する説明をいたします。

まず、基本要件基準第12条第3項の対象範囲を、
2の(1)では電磁的情報のやり取りをする医療機器として、
(2)で外部からの不正アクセスや攻撃を受ける可能性があるものを対象とすることを示しています。

次に、動作環境及び使用環境の特定に関して、
2の(3)で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を示しています。

3の基本要件基準第12条第3項の適用・適合性の確認については、
JIS T 2304による構成管理に加えて、JIS T 81001-5-1によるサイバーセキュリティ対策の強化や、サイバーセキュリティに関するリスクの低減することで、
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、
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旨を記載しています。

Slide 16

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
 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9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 その使用によって保健衛生上の危険を生ずるおそれがある医療機器

なお、基本要件基準に適合しない医療機器は、法第65条に定められているとおり、販売、賃貸、製造等が禁止されています。

また、医療機器プログラムの場合は電気通信回線を通じての提供も禁止されています。

Slide 17

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。

開発プロセス (左側): 顧客ニーズの特定 → システム開発アクティビティ(リスクマネジメントを含む) → 開発7 ソフトウェアリスクマネジメント → 5.1-5.8 (開発プロセス) → 8.1-8.9 (保守プロセス)

保守プロセス (右側): 保守要求の特定 → システム保守アクティビティ(リスクマネジメントを含む) → 保守7 ソフトウェアリスクマネジメント → 6.1-6.8 (保守プロセス) → 8.1-8.9 (保守プロセス)

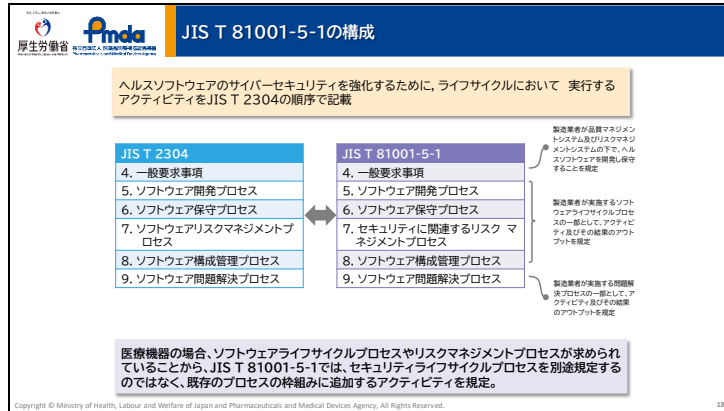
基本要件基準第12条第2項への適合で確認されるJIS T 2304のソフトウェアライフサイクルプロセスになります。

安全なソフトウェアを実現するためには、ハザードを特定し、関連するリスクが受容可能なレベルまで低減されているというリスクマネジメントの考え方と、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というライフサイクルプロセスの考え方が必要です。

JIS T 2304においては、開発及び保守について、ライフサイクルプロセス及びそれを支援するリスクマネジメント、構成管理、問題解決のプロセスが規定されていて、第12条第2項の適合のために、各製造販売業者において、これらが実装されていると思います。

第12条第3項のサイバーセキュリティについては、JIS T 2304のライフサイクルの構成でセキュリティ対応を規定するJIS T 81001-5-1を用いて、JIS T 2304に規定するプロセスに対してアドオンする形で、セキュリティのためのアクティビティを実施するということしております。

Slide 18



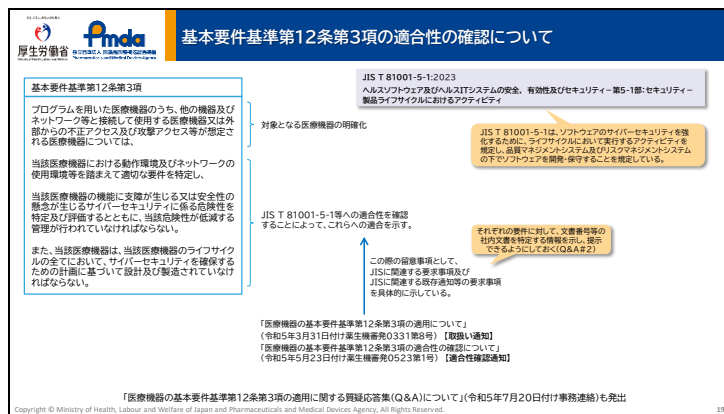
従いまして、JIS T 81001-5-1の構成については、ヘルスソフトウェアのサイバーセキュリティを強化するために、ライフサイクルにおいて実行するアクティビティをJIS T 2304の順序で記載されていることとなります。

規格の箇条4では、一般要求事項として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し、

箇条5から8では、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され、

箇条9では、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しています。

Slide 19



令和5年3月31日付けの取扱い通知において、基本要件基準第12条第3項の適合性の確認は、JIS T 81001-5-1等への適合性を確認することによって示す、としております。

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の下でソフトウェアを開発・保守することを規定しております。

また、令和5年5月23日付の適合性確認通知において、基本要件基準への適合を示すために、規格への適合を確認する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ます。

さらに、7月20日付の質疑応答集のQ2において、適合性を示す際には、適合性確認通知で示され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すということにしております。

Slide 20

The slide contains the following information:

- 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」をより具体的に示した通知
- 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) (<https://www.pmda.go.jp/files/000250907.pdf>)
[読み添付メモ](https://www.pmda.go.jp/files/000252686.pdf) (<https://www.pmda.go.jp/files/000252686.pdf>)
[スライドショー](https://www.youtube.com/watch?v=6wrXnM7LP5E) (<https://www.youtube.com/watch?v=6wrXnM7LP5E>)

こちらに示す通知は令和5年3月31日付の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」をより具体的に示した令和5年5月23日付の適合性確認通知になります。

その中で、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ています。

Slide 21

| 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】 | | |
|--|--|--|
| 区分 | 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。 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。 | 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開き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る確認すること。 |
| 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、危険増幅、多難防衛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。 | 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体系的な脆弱性対策の実施計画をあらかじめ定めておくこと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、関連する脅威を特定して評価し、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る確認すること。 |
| 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。 | |

適合性確認通知の内容ですが、JIS T 81001-5-1の箇条4~9に対して、各箇条の要求事項の要約や抜粋の形で、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になります。

1の「JISに関連する要求事項」では、JISに関連する要求事項がまとめられており、特にこれらに留意して基本要件への適合を確認していただくことになり、

2の「JISに関連する既存通知等の要求事項」では、既存の通知ですでに要求されていた内容や規格への適合状況を端的に示す内容など、規格に関連して追加で確認すべき内容が示しています。

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」があります。

Slide 22

| 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】 | | |
|--|--|--|
| 区分 | 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。 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。 | 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開き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る確認すること。 |
| 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、危険増幅、多難防衛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。 | 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体系的な脆弱性対策の実施計画をあらかじめ定めておくこと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、関連する脅威を特定して評価し、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る確認すること。 |
| 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、別資料にて説明します。

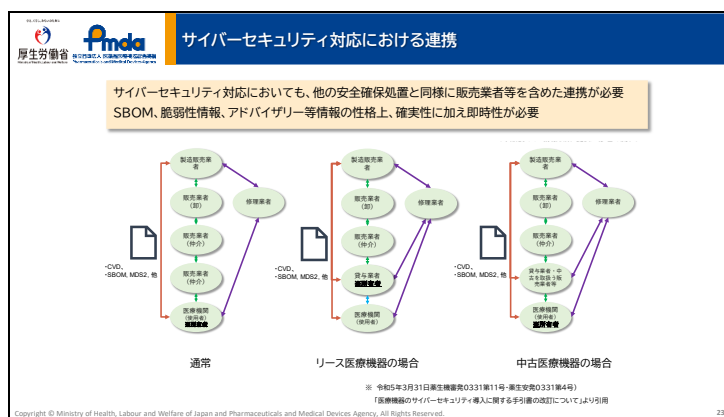
この適合性確認通知で伝えたいポイントとして、2点あります。

1つ目は、承認・認証申請においては、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ようにしておくこと。

2つ目は、第三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。
となります。

Slide 23



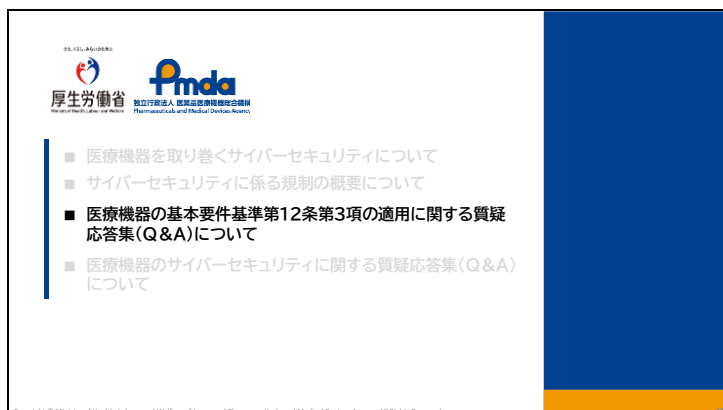
サイバーセキュリティ対応においても、製造販売業者が、販売業者又は貸与業者を介して医療機関等へ医療機器を提供する際には、安全性情報の提供、収集その他の安全確保に必要となる処置を実施し、連携する必要があります。

製造販売業者は、単一又は複数の販売業者を介し、その医療機器が医療機関において適切なセキュリティ対応がとられるよう、医療機関及び販売業者と必要な連携をとり、必要に応じてSBOMやCVDなどの必要となる情報提供やセキュリティパッチの適用等を適切かつ遅滞なく実施できるよう、必要な処置を行う必要があります。

また、医療機器の修理が必要となった場合には、製造販売業者は、医療機関等と連携し、修理業者との間において、脆弱性情報等の情報共有を行う等のCVDに必要な情報共有を行うとともに、医療機関等との間にて修理に係るセキュリティ上の脆弱性に係る情報共有を行う必要があります。

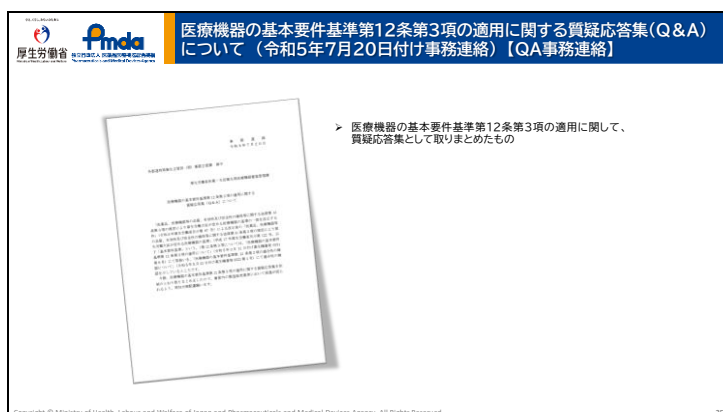
より詳細な説明が令和5年3月31日付通知の「医療機器のサイバーセキュリティ導入に関する手引書の改訂について」に記載されていますのでご確認いただければと思います。

Slide 24



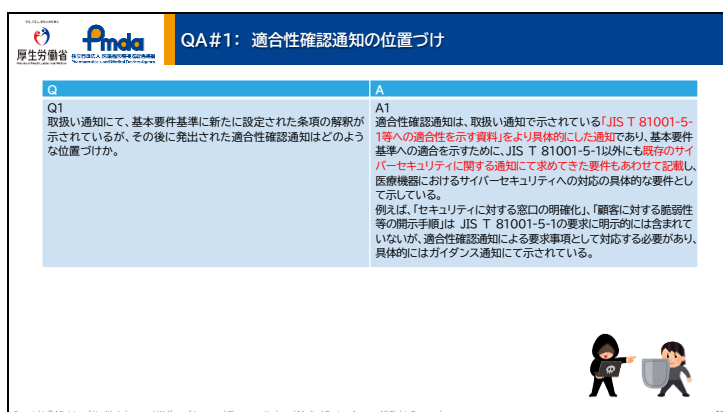
ここからは、医療機器のサイバーセキュリティに関して、Q&A形式の事務連絡が2件発出されていますので、Q&Aの内容について説明します。

Slide 25



まず、令和5年7月20日付の事務連絡の質疑応答集について説明いたします。

Slide 26



Q1は、令和5年5月23日付けの適合性確認通知の位置づけについてです。


医療機器のサイバーセキュリティについて

適合性確認通知は、JIS T81001-5-1等への適合性を示す資料をより具体的にした通知です。

医療機器のサイバーセキュリティ対応に関する変遷や趣旨でお判りになるかと思いますが、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た、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ております。

Slide 27

| 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等12条第3項への適合性を示すため、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、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 真見のとおり、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も、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。 |




Copyright © Ministry of Health, Labour and Welfare of Japan and Pharmaceuticals and Medical Devices Agency. All Rights Reserved.

Q2は、承認、認証申請における、JIS T81001-5-1等への適合結果をどのように示すかについてです。

基本要件基準第12条第3項への適合性を示す際には、適合性確認通知のJIS T 81001-5-1等のそれぞれの要件を満たしていることを示す、社内文書の文書番号等の特定する情報を提示することによりしております。

Slide 28

| 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、「 セキュリティ適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要になる場合もあり、 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。 |



Copyright © Ministry of Health, Labour and Welfare of Japan and Pharmaceuticals and Medical Devices Agency. All Rights Reserved.

Q3は、製造販売承認・認証・届出済みの品目における附属書 F「トランジションヘルスソフトウェア」の適用についてです。

国内のサイバーセキュリティ対応において、経過措置期間終了後の令和6年4月以降

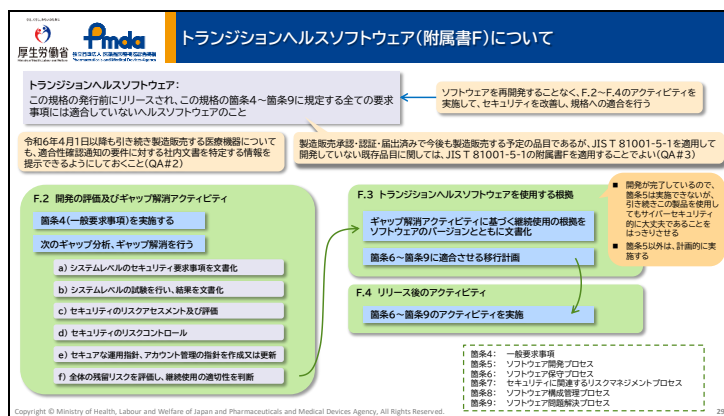
も引き続き製造販売する医療機器についても、適合性確認通知の要件に対する社内文書
を特定する情報を提示できるようにしておくことが必要ですが、JIS T 81001-5-1
を適用して開発していない既存品目については、このトランジションヘルスソフトウェ
アを適用することでもよいとされています。

トランジションヘルスソフトウェアについては、例えば、「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」等の対策を講じることで、規格への適合を示すということで、詳細は
次のスライドの通りです。

リスクマネジメントの結果、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も必要
となります。

また、QA3での「医療機器外部の補完的対策が必須になる場合」とは、セキュリ
ティのリスクアセスメントを行い、製品の既存機能・設定によって、未使用のネット
ワークポートを閉じる、脆弱性対策アップデートの適用を速やかに行う等の対策を実
施することができないため、DDOS攻撃やマルウェア感染によって機能不全に陥る等
が発生して、受容できないリスクにつながる可能性があることが判明した場合に、こ
れを軽減するための対策として、補完的対策が必須となることを想定しています。

Slide 29



JIS T81001-5-1附属書Fのトランジションヘルスソフトウェアに係る規定は、開
発が完了しているソフトウェアについて、ソフトウェア全体を再開発することなく、セ
キュリティの改善によって規格への適合を示す、という観点からの規定です。

開発が完了しているので、規格の箇条5のソフトウェア開発プロセスについては完全
には実施できませんが、規格の規定とのギャップ分析を行い、ギャップ解消アクティビ
ティに基づいて、ソフトウェアの継続使用の根拠を文書化することが必要です。つまり、
引き続きそ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
させる必要があります。また、その他の箇条の要求事項については、計画的に実施し

ていくことになります。

最終的な申請書等の記載事例については、この後別のQAで解説しますが、箇条5に関する確認項目は一部が記載不要となるが、その他の箇条の確認項目については、全て確認結果を示すことが必要です。

Slide 30

厚生労働省 fmda 品質・安全・有効性の確保

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。 |

Copyright © Ministry of Health, Labour and Welfare of Japan and Pharmaceuticals and Medical Devices Agency. All Rights Reserved.

Q4は、「セキュリティに対する問い合わせ窓口」についてです。

ここでは、セキュリティに関して緊急に対応できる窓口や連絡先の設定が想定されません。

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としております。

なお、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」欄に記載をお願いいたします。

Slide 31

厚生労働省 fmda 品質・安全・有効性の確保

QA # 5: 承認、認証申請においてSBOMを提出する必要があるか

| 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ます 、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。 |

Copyright © Ministry of Health, Labour and Welfare of Japan and Pharmaceuticals and Medical Devices Agency. All Rights Reserved.


Q5は、承認・認証におけるソフトウェア部品表「SBOM」の取扱いについてです。

申請時に提出する必要はありませんが、承認・認証申請時にはSBOMを作成している

ことを明示できるよう準備してください。

Slide 32

| 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」) |



Copyright © Ministry of Health, Labour and Welfare of Japan and Pharmaceuticals and Medical Devices Agency. All Rights Reserved.

Q6は、「SBOMの構成」に関する内容です。


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していただき、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てください。

また、コンポーネントの各々について、ここに示す7つの項目を明示してください。

詳しくは、令和5年3月31日付事務連絡の「製販向け手引書通知」の附属書A(IMDRFの追補ガイダンスを基本として追加)をご参照ください。

Slide 33

| QA # 7: セキュリティを確認する試験は、第三者試験である必要があるか | |
|--|---|
| 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が、セキュリティを確認する試験は、第三者試験である必要があるか。 | 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。 |



Copyright © Ministry of Health, Labour and Welfare of Japan and Pharmaceuticals and Medical Devices Agency. All Rights Reserved.

Q7はセキュリティを確認する試験についてです。

第三者試験を行うことは必須ではございません。

医療機器のサイバーセキュリティについて

Slide 34

厚生労働省 fmda
Pharmaceutical and Medical Device 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

Copyright © Ministry of Health, Labour and Welfare of Japan and Pharmaceutical and Medical Device Agency. All Rights Reserved.

次に、令和6年1月31日に発出された事務連絡の質疑応答集について説明いたします。

Slide 35

厚生労働省 fmda
Pharmaceutical and Medical Device Agency

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】

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

Copyright © Ministry of Health, Labour and Welfare of Japan and Pharmaceutical and Medical Device Agency. All Rights Reserved.

令和6年1月31日に質疑応答集第2弾が事務連絡として発出されております。

Slide 36

厚生労働省 fmda
Pharmaceutical and Medical Device Agency

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 |
|--|--|
| <p>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。</p> | <p>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となる。 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、こ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。</p> |

Copyright © Ministry of Health, Labour and Welfare of Japan and Pharmaceutical and Medical Device Agency. All Rights Reserved.

Q1は、対象となる医療機器についてになります。

医療機器のサイバーセキュリティについて

Q1の一番のポイントとしては、「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」の部分です。

回答としては、基本要件基準第12条第3項に示されている通り、「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適切な要件を特定」したうえで、対応・管理を行うこととなります。

『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』については適用となります。

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となります。

Slide 37

| 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た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。 |

Q2は、経過措置期間中に承認・認証申請を行った品目の取扱いについてです。たとえ経過措置期間終了後に承認・認証取得することになっても、基本要件基準第12条第3項への適合確認はおこなわれません。ただし、製造販売業者において、製造販売出荷までには適合性確認を行う必要があります。

Slide 38

| 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。 |

Q3です。

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ありません。

Slide 39

厚生労働省 **fmda** 医療機器の認証・承認

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によい。 | 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。 |

Copyright © Ministry of Health, Labour and Welfare of Japan and Pharmaceuticals and Medical Devices Agency. All Rights Reserved.

Q4は、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への適合証明書についてです。

令和5年7月20付事務連絡のQA7で言及させていただいておりますが、第三者機関による試験は必須ではないのですが、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して、適合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必要がありますことにご留意ください。

Slide 40

厚生労働省 **fmda** 医療機器の認証・承認

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。 |

Copyright © Ministry of Health, Labour and Welfare of Japan and Pharmaceuticals and Medical Devices Agency. All Rights Reserved.

Q5は、承認申請における、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)の対象となるのか、についてです。

サイバーセキュリティに係る別添資料は、信頼性調査の対象になり得ます。調査対象となったあかつきには、別添資料に記載する社内文書は根拠資料になります。なお、このQ&A5は、認証においては、信頼性調査がありませんので、関係のないお

話になります。

Slide 41

The slide is titled "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" (QA2 #6: Are medical information system security management guidelines also applicable to medical devices?). It features a Q&A format with a question (Q6) and an answer (A6). The question asks if the guidelines for medical information systems also apply to medical devices. The answer states that the guidelines do apply, covering patient information and personal identification information, and that they also apply to medical devices connected to the system. It references the 6.0 edition of the guidelines (issued in May 2023).

| 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。 |

Copyright © Ministry of Health, Labour and Welfare of Japan and Pharmaceutical and Medical Devices Agency. All Rights Reserved.

Q6は、先ほども説明いたしましたが、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ります。

「3省2ガイドライン」は、経済産業省・総務省から発出されている「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」（健康医療分野に特化した情報システム・サービス事業者向けの指針）と、厚生労働省医政局より発出されている「医療情報システムの安全管理に関するガイドライン」からなっています。

基本要件基準においては、製造・販売・流通する医療機器について、サイバーリスクを低減する措置を講じることとしている一方で、「医療情報システムの安全管理に関するガイドライン」は、医療情報を扱うシステムと同システムに関わる人または組織を対象とし、情報セキュリティマネジメントシステムの実践、組織的・物理的・技術的・人的安全対策、サイバー攻撃等の非常時の対応等の指針が示されています。

したがって、医療現場において、例えば電子カルテ等の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においても対応が必要となります。つまりは、患者情報を取り扱う医療機器も対応が必要となります。

Slide 42

厚生労働省 fmda

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。 |

Copyright © Ministry of Health Labour and Welfare of Japan and Pharmaceuticals and Medical Devices Agency. All Rights Reserved.

Q7は、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」に関する具体的に参考となる資料についてです。

JIS T 81001-5-1の5.3.2及び5.4.1に例示がありますが、その他、製販向け手引書通知の「5.1 セキュリティ要求事項及びアーキテクチャー設計」が参考になります。

Slide 43

厚生労働省 fmda

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。 |

Copyright © Ministry of Health Labour and Welfare of Japan and Pharmaceuticals and Medical Devices Agency. All Rights Reserved.

Q8は、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についてです。

令和5年7月20付事務連絡のQA3（スライド28枚目）でトランジションヘルスソフトウェアを適用する際の全般的な説明をしているので後ほど確認していただければと思いますが、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になります。

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、それによって、開発プロセス以外の箇条6から9を実施していくこととなります。

その結果として、適合性確認通知で求める確認の際の留意点のうち、箇条5のソフト

医療機器のサイバーセキュリティについて

ウェア開発プロセスに係る次の事項については、記載が不要とできますが、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ります。

Slide 44

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。 |

Q9は、開発時期が古い製品のSBOM作成についてになります。

製販向け手引書通知の附属書A.1にあるように第12条第3項ではソフトウェアコンポーネントを明らかにしなくてはならず、製販業者がツールによって洗い出し、その結果でリスクアセスメントすることが求められています。したがって、製販業者は何かしらの対応が求められていることになります。

では、どうしたらよいかという話になりますが、平成26年の基本要件基準改正で、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月以降は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は構成管理情報があるため、そこからSBOMは作成可能かと考えられます。

Slide 45

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ります 。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。 |

製品開発開始 → **商用リリース** → **製品寿命終了EOL** → **サポート終了EOS**

※ EOLとEOSの日付を同日に設定可能

サイバーセキュリティマネジメント計画
 アップデートポリシー / アップグレード

※ 責任を伴う保守期間終了

サポート終了(End of Support:EOS)
 製品のライフサイクルにおいて、顧客への責任義務が完了し、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、後述のEOL以降の年数にわかわらずレガシーであるとみなされる。

限定的サポート → **サポート終了(レガシー)**

顧客は、製造販売業者から通知されたサポート終了に対する対応計画の作成を依頼する

製造販売業者から顧客への責任の完全な移行（EOL、サポートは継続されない）

Q10は、製品の寿命となるEOLと、全てのサポートが終了となるEOSの関係についてになります。

ここ(左下)に示している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医

療機器のライフサイクルの図をもとに、EOLとEOSの間の限定的サポート期間に関連した質問となっています。

サポート終了を迎えた、サイバーセキュリティの対応が取れない、いわゆるレガシー医療機器については、そのまま医療機関のネットワークに接続して使用し続けることには問題があるため、新しい医療機器に買い替える等の対応を医療機関で行う必要がありますが、そうした対応を行うためには、ある程度の時間がかかることが想定されます。

製品寿命終了を迎えてすぐにサポート終了となると、医療機関側で対応を行う時間が確保できないので、製品寿命終了やサポート終了の時期については、十分な時間の余裕をもって事前連絡する必要があります。

それに加えて、例えば、本体のプログラムのアップデートは提供できないが、関連するソフトウェアに関するサイバーセキュリティ情報等を提供するとか、最終的なサポート終了に対する計画等をあらかじめ提示して、引き続き医療機関とのコミュニケーションを継続する期間として、限定的サポート期間を置いて対応することが、医療機関側でのスムーズな移行を助けるために重要となります。

Slide 46

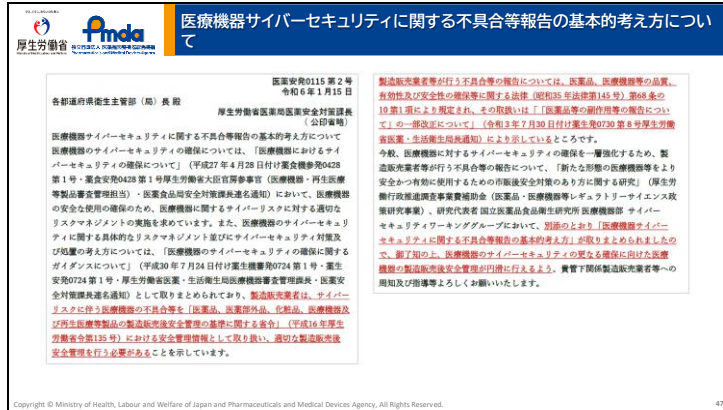
QA2 #11: 市販後のサイバーセキュリティの確保は、製造販売後安全管理において実施すればよいか

| 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によいか。 | A11 貴国のとおり、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7条から9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、速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係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。 |

Q11は、市販後のサイバーセキュリティの確保についてです。

製造販売業者は、GVP省令に則り、製造販売後安全管理を行う必要があります。GVP省令第7条から9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、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ります。

Slide 47



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まとめられた通知が、令和6年1月15日に医薬安全対策課長通知として発出されましたので、詳しくは、こちらの通知を参照してください。

Slide 48



厚生労働省のホームページにて、基本要件基準をはじめ、これまで発出した医療機器のサイバーセキュリティに関連する通知やIMDRF文書を掲載していますので、ご紹介させていただきます。

一部、通知の英文の参考情報も掲載していますので、あわせてご活用ください。

Slide 49



ご清聴ありがとうございました。

以上