政情連発 0924 第１号
医薬機審発 0924 第１号
医薬安発 0924 第１号
令和８年９月 24 日

各｛都道府県／保健所設置市／特別区｝衛生主管部（局）長　殿

厚生労働省政策統括官付参事官（医療情報連携担当）
（　　公　　印　　省　　略　　）
厚生労働省医薬局医療機器審査管理課長
（　　公　　印　　省　　略　　）
厚生労働省医薬局医薬安全対策課長
（　　公　　印　　省　　略　　）

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の改定について

医療機関における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３月 31 日付け医政参発 0331 第１号・薬生機審発 0331 第 16 号・薬生安発 0331 第８号厚生労働省医薬・生活衛生局医薬品審査管理課長、医療機器審査管理課長、医薬安全対策課長連名通知。以下「手引書」という。）により、お示ししているところです。

今般、一般社団法人日本医療機器産業連合会の医療機器サイバーセキュリティ対応ワーキンググループにおいて、別添のとおり手引書の改定が行われました。つきましては、貴管内の関係機関、関係団体等に対する周知、体制確保に向けた指導等よろしくお願いいたします。

主な改正内容としては、以下のとおりです。

○　電子カルテシステム等の医療情報を取り扱うシステムのネットワークに接続して電磁的情報のやりとりを行う医療機器は、医療情報システムに該当し、「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・薬局におけるサイバーセキュリティ対策チェックリスト」の対象となることを明確化（手引書 p. ４、５）

○　医療情報システムの一部として、優先的にサイバーセキュリティの対策を行うことが望ましい医療機器を明示（手引書 p. ６）

○　医療機器の導入時に契約等によって医療機関と医療機器事業者との間で明確にしておくべき点を記載（手引書 p. ６）
○　医療機器のライフサイクル（EOL 前、EOL～EOS、EOS 後）における対応について、「医療機器のサイバーセキュリティ対策に関連する情報提供について」（令和７年４月 17 日付け医薬機審発 0417 第１号）を踏まえて見直し（手引書 p. 10、11）
等

また、昨今、医療機関等を標的としたサイバーインシデントが発生しており、医療機関においては、電子カルテ等の患者情報を取り扱う情報システムのみならず、ネットワーク等に接続される医療機器についても、適切なサイバーセキュリティ対策を講じることが求められています。

医療機関においては、「医療情報システムの安全管理に関するガイドライン第 7.0 版」等に基づき必要な対策を実施いただいているところですが、本手引書についてもご活用いただき、医療機器事業者と連携しながら、医療機器のサイバーセキュリティ対策を含めた取組を推進いただくよう、併せて周知方お願いいたします。

別添

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（第２版）

一般社団法人日本医療機器産業連合会 サイバーセキュリティタスクフォース（初版）
医療機器サイバーセキュリティ対応 WG 編集

目　次

１．はじめに

医療分野における情報化・ネットワーク化が進展し、それに伴い医療機関におけるサイバーセキュリティ対応がますます重要になっている。特に医療機関で使用される医療機器においては、サイバー攻撃により発生する医療機器の不具合が患者の健康被害に直接つながる可能性があるため、医療機器のサイバーセキュリティ対策は重要な課題となっており、医療機関、医療機器事業者*2及び他の全てのステークホルダーが連携して取組む必要がある。
我が国でも医療法施行規則の改正や、「安全管理ガイドライン*3」の継続的改定等に加え、医療機器事業者は、サイバーセキュリティに関して、医薬品医療機器等法*4に紐づく基本要件基準改正及び関連する通知への適合によって、医療機器の安全性を確保し、患者の安全*1の視点から医療機関のサイバーセキュリティ対策を支援する取組みを行っている【参考 1】。

医療機器は、複数国に流通する場合が多いことや、国境の枠組みを超えてサイバー攻撃が行われる可能性が高いと考えられていることから、サイバーセキュリティ対応の国際調和を図ることを目的として、国際医療機器規制当局フォーラム（IMDRF）*5から「医療機器サイバーセキュリティガイダンス（以下、IMDRF ガイダンスという）」【参考 4】が発行され、我が国の規制へも導入されている。これを推進するために、医療機器事業者に対して「医療機器のサイバーセキュリティ導入に関する手引書」（以下、製造販売業者向け手引書という）が別途作成・公表されている。さらに IMDRF から、より実践的なレガシー医療機器及びソフトウェア部品表（以下、SBOM という）に関する 2 つの追補ガイダンスが発行され、製造販売業者向け手引書が改訂されている。IMDRF ガイダンスだけでなく、各地域の規制は、国際的な枠組みの中で“設計によるセキュリティ確保：Secure by Design）の考え方を基本にしており、製品自体でサイバーセキュリティを維持可能なことが求められるようになってきている。また、医療機器事業者が、セキュリティ文書等をタイムリーに医療機関に提供することによって、医療機関と連携する重要性も増している。

本手引書「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」（以下、医療機関向け手引書という）は、医療機器が、医療情報を扱う機器として求められる事項に加えて、医薬品医療機器等法に基づいて医療機器の安全性確保のために実施するサイバーセキュリティ対策及び情報共有による医療機関との連携等の取組みを中心に紹介し、医療機関における医療安全を確保するための取組みの一助となるべく作成した。

本手引書作成にあたり、国立研究開発法人日本医療研究開発機構（AMED）医薬品等規制調和・評価研究事業「医療機関における医療機器のサイバーセキュリティに係る課題抽出等に関する研究」研究班（研究開発代表者：公益財団法人医療機器センター専務理事 中野壮陛）の活動及び厚生労働省、独立行政法人医薬品医療機器総合機構にご協力いただいた。初版は、一般社団法人日本医療機器産業連合会 サイバーセキュリティタスクフォースが作成し、第２版以降は医療機器サイバーセキュリティ対応WGが継承している。

本手引書の位置付けのイメージを図１に示す。

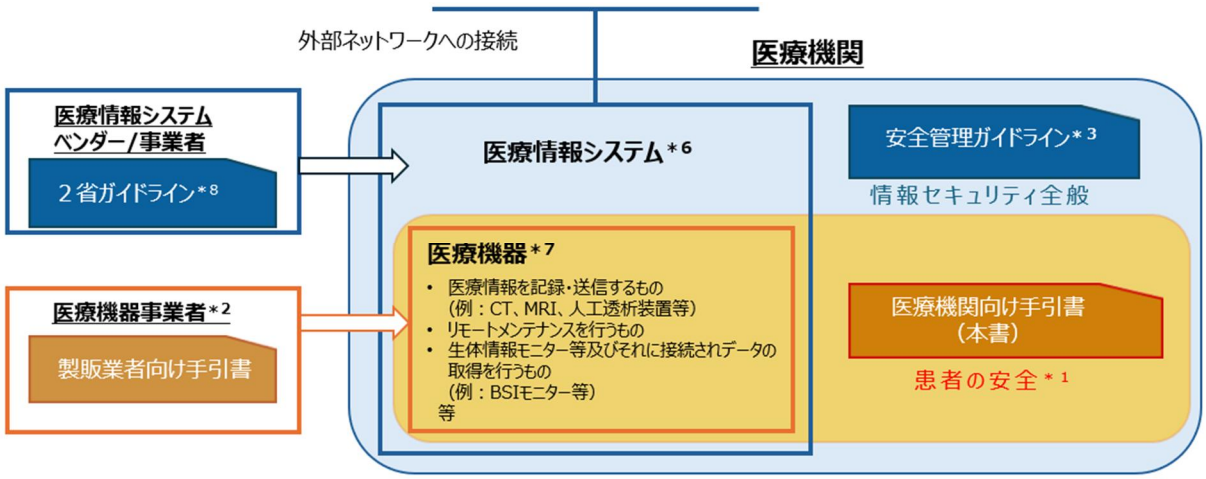

図1　医療機関向け手引書の位置付け（イメージ）

（＊1）　患者の安全：本手引書では、医療安全のうち、患者の安全を中心に扱うが、使用者、医療従事者等の安全も含む。医療機器が同じネットワークに接続される他の機器やシステムに影響を及ぼすことで患者の健康被害にリスクが生じる場合も含める。

（＊2）　医療機器事業者：製造販売業者、製造業者、販売業者、貸与業者、修理業者等を指す。

（＊3）　安全管理ガイドライン：医療情報システムの安全管理に関するガイドライン【参考 2】

（＊4）　医薬品医療機器等法：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【参考 3】

（＊5）　国際医療機器規制当局フォーラム（International Medical Device Regulators Forum：IMDRF）

（＊6）　医療情報システム：医療情報システムは、医療情報を保存するシステムだけではなく、医療 情報を扱う情報システム全般である。医療情報とは、医療に関する患者情報（個人識別情報）を含む情報を想定する。本書では、例えば電子カルテシステムのような医療情報を取り扱うシステムだけでなく、そのようなシステムがつながるネットワークに接続して電磁的情報のやりとりを行う医療機器も該当する。

（＊7）　本書で対象とする医療機器は、電子カルテシステム等の医療情報を取り扱うシステムに接続して電磁的情報のやりとりを行う医療機器が対象となる。別の機器を介して、間接的に接続される医療機器も含まれる。

（＊8）　2 省ガイドライン：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（総務省・経済産業省）

2．本書の目的と対象

2．1　目的

医療機関において医療機器のサイバーセキュリティを確保し、サイバー攻撃により医療機器の不具合や患者不利益が発生しないように未然に防ぐことを目的に、医療機器事業者が実施する対策及び医療機関に提供する情報、並びに医療機関と連携して実施する事項等について取りまとめている。

２．２　本書の対象について

（１）対象とする読者

医療機器事業者及び施設の規模によらず医療機関等で医療機器に関わる全ての人を対象としている。本書で示す事項は、大規模施設から小規模施設まで共通するが、実際の管理、運用の体制及び具体的な実施事項等については、施設の規模や形態、医療機器の特性や使用環境等に応じて、医療機関と医療機器事業者が連携して適切に実施することを想定している。

（２）対象とする医療機器

医薬品医療機器等法第 2 条第 4 項に定義された医療機器のうち、無線又は有線により、メディア媒体を含む他の機器、ネットワーク等との接続が可能なプログラム医療機器（SaMD ：Software as a Medical Device）を含む医療機器及びプログラムを用いた附属品等を対象とする。

なお、医療機器事業者が当該医療機器を保守するにあたって、契約等によって提供・設置されるサーバーや端末、ネットワーク機器等の医療機器としての登録に含まれない周辺機器についても、当該医療機器を含む使用環境の安全性確保及びサイバーセキュリティ維持に不可欠なものとしてこの手引書の対象に含むものとする。

（３）想定されるリスク

医療機器に係るサイバー攻撃により、医療機器の不具合や患者の健康被害に影響を与えるリスクを対象とする。例えば、医療機器の性能に影響を与えること（性能や機能の低下、誤動作、動作停止等）、診療活動に影響を与えること（患者情報やオーダー情報へのアクセス停止等）、誤った診療につながること（情報の欠落や改ざんによる誤診断や不適切な治療等）等によって患者の健康被害に及ぶことが考えられる。また、当該医療機器がサイバー攻撃の被害を受けたことにより、同じネットワーク等に接続された他の医療機器やシステムに影響を及ぼし、患者の健康被害に影響を与えるリスクにも考慮が必要である。

（４）医療情報システムに接続される医療機器の情報セキュリティについて

医療機関における医療情報システムの情報セキュリティの維持のための要件全般については、厚生労働省の安全管理ガイドラインに定められており、「医療機関・薬局におけるサイバーセキュリティ対策チェックリスト」も提供されている。本書の対象となる医療機器も医療情報システムの一部であり、これらのガイドラインやチェックリストの対象となる。なお、患者情報を扱わず、医療情報システムのネットワークに接続しない医療機器であっても、リモートメンテナンスにより外部のネットワークと接続する医療機器については、ガイドラインやチェックリストの対象とはならないが、本書の対象となる。

患者情報等を扱う医療機器も多く、情報セキュリティ（例えば情報漏洩やデータプライバシーに関するセキュリティ等）が確保できる環境の整備は医療機関においては重要であり、医療機器事業者は、医療機関との間で想定リスク、リスクシナリオについての合意形成を十分に行うべき点に留意が必要である。本書では、特に医療機器の安全性の視

点から必要となる対策について説明する。(図１参照。)
なお、サイバー攻撃による情報セキュリティへの侵害が、医療機器の安全性の侵害につながることがあることにも考慮する必要がある。
一例であるが、医療情報を記録・送信する医療機器（CT、MRI、人工透析装置、輸液ポンプ、心電計等)、リモートメンテナンスを行う医療機器（CT、MRI、超音波診断装置、内視鏡等）及びリモートメンテ用周辺機器、医療機関の管理の下で在宅においても使用される医療機器（ペースメーカー及び中継器、CPAP 等)、医療用アラームシステムに組み込まれる医療機器（生体情報モニター等）等については、医療機関は、医療情報システムの一部としてサイバーセキュリティを監視し優先的に対策を行うことが望ましい。

３．医療機器のサイバーセキュリティ確保について

３．１　導入時の医療機関と医療機器事業者との連携

医療機器事業者は、医療機器の販売及び設置の検討に際し、医療機関との間で行う協議により相互の役割・責任の範囲を明確にすることが重要で、医療機器事業者は、医療機関に対し、ネットワーク構成図等（後述）を用いて医療機器と医療機関の IT インフラとの間の信頼境界について、その範囲と医療機器及び２．２（２）で追加された周辺機器（ある場合）の関係を提示し、これらが妥当且つ正しいことを相互に確認し、契約等によって合意を確実にする。
特に周辺機器は、運用開始後におけるパッチ等のアップデートの対応等の役割・責任が不明確になりやすいため注意する必要がある。
また、医療機器事業者は、医療機器の導入、管理、保守、医療機関との連携等について、適切な文書・資料、サイバーセキュリティに関するサポート終了（EOS）までの保守内容、その実運用期間に対する妥当性等を提示し、医療機関と十分に協議し、契約によって合意を確実にする。
運用開始後に、信頼境界が変化してしまうようなシステム構成の変更をする場合も、同様に医療機関と十分に協議し、必要に応じて契約を見直し、合意を確実にする。

３．２　製品ライフサイクル全体（TPLC）とリスクマネジメント

医療機関が医療機器を導入した後も、サイバー攻撃は年々高度化し、リスクが新たに発生又は報告される。医療機器事業者は、これらのセキュリティ情報の提供に加え、EOL（製品寿命終了）/EOS 等の製品ライフサイクルに関して、医療機器の製品寿命及びサポート条件に関する情報を提示する。提示された EOS 後は、医療機関にて買替え、更新又は廃止等の対応をすることが期待されるが、医療機器買換えまでの一時的な期間、EOS を過ぎた医療機器を利用しなければならない状況においては、当該医療機器の使用を継続することによって発生し得るリスクは、医療機関が引き受けてマネジメントしていくことになるため、医療機関は、ログや通信の監視等によるリスク低減、適切なネットワークのセグメンテーション及び多層防御等の対策を講じることが求められる。
このように、医療機関は、医療機器の導入時に必要な情報を収集し、想定されるリスク

を評価し、受容可能なレベルまで低減するというリスクマネジメントを行うとともに、医療機器を導入した後も、医療機器の使用を終了するまでの製品ライフサイクル全体（TPLC）にわたり、関連する情報を逐次収集し、脅威の増加に伴うリスクを評価し、対策を検討し、リスクが受容されるまで低減できるかを評価したうえで、適切な対策を追加するといったリスクマネジメントの PDCA を継続して実施することが求められる。
医療機器事業者は、医療機関がこのようなリスクマネジメントを確実に実施できるよう、医療機関に先んじて積極的にリスクマネジメントを実施し、脆弱性等に関する情報を開示して、相互に連携して対策を実施する必要がある。

４．医療機関と医療機器事業者との連携

医療機関と医療機器事業者がサイバーセキュリティ対策で行うことの概要例を表 1 に示す。
医療機関における医療機器のサイバーセキュリティ対策のためには、その使用環境である IT インフラを含めた環境の整備が基本となる。このため、安全管理ガイドラインで示されている情報セキュリティを確保するために実施する対策に加えて、医療機関は、患者の安全の視点で、医療機器事業者と連携して医療機器のサイバーセキュリティ対策を行うことになる。

表 1 医療機関と医療機器事業者がサイバーセキュリティ確保のために実施すること（概要例）

<table>
<tr><th colspan="2">ステータス</th><th>医療機器事業者</th><th>医療機関</th></tr>
<tr><td colspan="2">４．１
医療機器の導入に向けた準備</td><td>○製品セキュリティポリシーの作成と開示
○製品保守計画の作成
○医療機関向け文書の作成・提示
・注意事項等情報及び取扱説明書
・セキュリティ文書（システム（ネットワーク）構成図、信頼境界、MDS2、SBOM、MDS、SDS 等）・製品保守計画及び契約案
○必要なトレーニングの準備</td><td>①医療機器の使用環境の特定、セキュリティ仕様及びセキュリティレベルの評価特定
②医療機器の医療機関におけるセキュリティ管理体制への組込み及びネットワーク構成更新
③保守計画の確認及び契約準備</td></tr>
<tr><td colspan="3">○使用環境（設置環境）に応じたセキュリティ文書（更新）等の提示
○保守に関する範囲・役割・責任・連携等に関する契約条項の調整</td><td>①導入した医療機器を含めた医療機関内 IT インフラのセキュリティレベルの確認
②保守に関する契約締結</td></tr>
<tr><td>４．３
医療機器の運用</td><td>（1）
製品ライフサ</td><td>○製品寿命終了（EOL）、サポート終了（EOS）の通知</td><td>①製品ライフサイクル全体の理解及び EOS 後の対応計画</td></tr>
</table>

	イクルにおける対応（レガシー医療機器に関する対応を含む）	○医療機関のEOS後の対応計画作成に関する支援・協力 ○製品保守計画に従った具体的な実施計画の提示 ○情報収集、セキュリティ文書の更新 ○脆弱性に関するセキュリティアドバイザリー情報開示、セキュリティ対策又は補完的対策を含む緩和策の提示 ○協調的な脆弱性開示（CVD）の対応として、調査又は関係部門へ注意喚起	②保守実施計画の理解と実施の調整 ③医療機器の使用環境におけるセキュリティ情報収集 ④セキュリティ文書の更新確認 ⑤医療機器の脆弱性対策実施 ⑥医療機関内の情報共有 ⑦レガシー医療機器への対策 ⑧協調的な脆弱性の開示（CVD）の対応
	（2） インシデント発生時の対応	○医療機関との連携活動 ○規制当局等への報告、情報提供 ○医療機器等の回復・復帰のための措置及び支援	①医療情報や医療サービスの提供体制に関わるインシデントの対応 ②患者に重篤な健康被害が発生するおそれのあるインシデントの対応

4．1　医療機器の導入に向けた準備

① 医療機器の使用環境の特定、サイバーセキュリティ仕様及びセキュリティレベルの評価特定

医療機関は、導入予定の医療機器の設置及び使用環境を特定し、医療機器に求める医療機関側のセキュリティ仕様を定める。医療機関は、この医療機関側のセキュリティ仕様を医療機器事業者に提示し、医療機器の導入可能性を協議して決定する。その際、医療機関は、医療機器事業者から提供される注意事項等情報、取扱説明書、セキュリティ文書（一部は取扱説明書に含まれている場合もある）を確認し、相互運用性の側面及び初期のサイバーセキュリティの妥当性を検証する。また、製品の保守計画を確認し、医療機関のサイバーセキュリティ対策のポリシーとの合致及び製品ライフサイクルにおける脆弱性マネジメントが適切に実施可能か、これらに必要な事項が契約等で記載されるかを確認する。サイバーセキュリティに関する仕様上の不明点は、医療機器事業者に確認し、明確にしておく。

［医療機器事業者が提示する取扱説明書やセキュリティ文書に含まれる内容の例］

・ 医療機器を使用するために必要な、医療機器周辺の一般ITインフラについての具体的なガイダンス
・ セキュアなネットワーク接続及びサービスを可能にするための設定等を含む技術的指示（マルウェア対策、ファイアウォール設定、ホワイトリスト、物理的セキュリティ検出等）
・ サイバーセキュリティ上の脆弱性又はインシデントが検知された際の対応方法に

関する指示

- 医療機器に係るセキュリティインシデントが検出された場合に、これを通知する方法に関する説明。なお、セキュリティインシデントの例としては、意図しない設定変更、ネットワーク異常、不正なログイン試行等が挙げられる。
- 医療機器の設定を保存し、復旧するための方法の説明。ただし、医療機関が実行するためには医療機器事業者からの権限の付与が必要な場合がある。
- 医療機器事業者からアップデート情報を入手してインストールするための対応手順の説明。ただし、医療機関が実行するためには医療機器事業者からの権限の付与が必要な場合がある。
- 医療機器のサポート終了に関する情報（附属書「レガシー医療機器」参照）
- 医療機器に実装されているオープンソース及び市販のソフトウェアに関する情報を含むSBOM（ソフトウェア部品表）。なお、SBOMは、販売時及び変更があった場合に提供される。また、医療機関が医療機器の導入検討のために提示を求める場合もある。いずれの場合も、機密保持契約等によって、医療機器事業者の許可なく第三者に提供されることがないようにする。
- 医療機器の意図する使用及び使用環境に対して設計したセキュリティ機能を俯瞰可能な、製造販売業者による医療機器セキュリティ開示書（Manufacturer Disclosure Statement for Medical Device Security：MDS2）

② 医療機器の医療機関におけるセキュリティ管理体制への組込み及びネットワーク構成更新

医療機関は、医療機関全体のIT インフラを管理するためのネットワーク管理図の中において、導入する医療機器の位置及び接続（データの流れ等）を特定し、導入する医療機器及び附属して導入される周辺機器を含めたサイバーセキュリティに関連する機器との関連を明確にするため、医療機器事業者から導入するシステム全体のネットワーク構成図及び信頼境界に関する情報の提供を受ける。これによって、医療機関は、医療機関全体のネットワーク構成図を整備すると同時に、医療機器の導入予定日までに必要な医療機関内のITネットワークの調整・準備を実施する。

ネットワーク構成図等には、機器の物理的な配置を把握するための情報と、データの流れや相互接続関係を把握するための情報を含める必要があり、必要に応じて逐次更新する。

［ネットワーク構成図等に含める情報の例］

- ネットワークに接続される可能性のあるすべての医療情報システム・医療機器
- 配置されているフロアや部屋、ラック等
- スイッチ、ルーター等の物理配線や接続ポート
- インターネットへの接続経路や接続形式、設定
- ファイアウォール、VPN
- IPアドレス、サブネット

・ 物理、仮想サーバー
・ サーバーのホスト名、役割

③ 保守計画の確認及び契約等準備

医療機関は、医療機器事業者から提供された信頼境界に関する情報及び保守計画を基に、医療機器を運用する上で、医療機関のセキュリティレベルを維持するために必要な協議を行い、保守契約等の締結準備を行う。

4．2　医療機器の導入、運用開始

① 導入した医療機器を含めた医療機関内 IT インフラのセキュリティレベルの確認

医療機器事業者は、医療機関と連携して医療機関が特定した使用環境に医療機器を導入（設置）する。医療機関は、医療機器事業者から提供されたセキュリティ文書等の情報及び実際の稼働状況が、医療機関が定めた医療機関内 IT インフラのセキュリティレベル対して十分であることを確認する。

② 保守に関する契約締結

医療機関は、主体となって医療機器の保守を実施し、医療機器に関する「説明責任」「管理責任」「維持・改善の責任」及び「善後策を講じる責任」を果たすことになる。

導入時に運用上、使用環境（設置環境）等に変更が発生し、相互で合意した信頼境界等に影響がある場合、医療機器事業者は、関係するセキュリティ文書を更新し、必要に応じて医療機関と協議して保守契約を締結する。

また、医療機関は、インシデント発生時等、サイバーセキュリティに係る可能性がある事象に関する医療機器事業者の問合せ先、相互の対応手順等についても確認し、特記事項等あれば必要に応じて医療機器事業者と協議して保守契約等に記載する。

医療機関との間に保守契約を締結しない場合、医療機器事業者は、適切な対応及び速やかな対策の実施が困難になる可能性がある等の免責事項等を提示した上で一時的な対応で応答可能な範囲を提示する。

4．3　医療機器の運用

（1）製品ライフサイクルにおける対応（レガシー医療機器に関する対応）

① 製品ライフサイクル全体の理解及び EOS 後の対応計画

医療機器は、EOS 以降は医療機器事業者におけるサポートが受けられなくなり、顧客に責任が完全に移転するため、EOS となる前に顧客が十分に対応可能な期間を配慮する必要がある。このため、医療機関は医療機器の EOL～EOS までの限定的なサポートが受けられる期間も利用して、医療機器事業者と連携しながら、EOS 後の対応を検討する必要がある（図２）。医療機器は、ソフトウェア部品表（SBOM）で示される様々なソフトウェアコンポーネントを含んでおり、医療機器事業者は、それらの寿命とロードマップ等を統合して医療機器としての製品寿命を定め、こ

の期間の終了（EOL）を医療機関に通知すること、EOL 後のパッチ又は外部に設置するファイアウォール等の補完的対策によって保守を保証できる期間を定め、この期間の終了（EOS）を医療機関に通知することが求められている。
医療機関は、これらの医療機器のライフサイクル（サポート段階）の把握に努め、医療機器事業者と連携して使用中の医療機器及びその使用環境のセキュリティを適切に維持し、正常な稼働を確保する。
a. サポート期間の対応（～EOL まで）
医療機関は、導入時に医療機器事業者から EOL 又は EOL 通知時期の計画を入手できる。EOL に備え、医療機器事業者と連携して、必要に応じて補完的対策等によるセキュリティ強化の計画を検討する。また、突然緊急性の高い脆弱性が明らかになることによって、急にレガシー医療機器として扱わねばならなくなる危険性があることに留意する。
b. 限定的サポート期間の対応（EOL～EOS）
医療機関は、EOL までには医療機器事業者から EOS 又は EOS 通知時期の計画を入手できる。EOS に備え、医療機器事業者と連携して、必要に応じて補完的対策等によるセキュリティ強化策を実施する。また、突然緊急性の高い脆弱性が明らかになることによって、急に突然レガシー医療機器として扱わねばならなくなる危険性があることに留意する。この期間を利用して、当該医療機器の更新、廃止又はネットワークからの分離等、EOS 後の計画を検討する。このため、医療機器事業者は、EOL 後に適切な限定的サポート期間を置いて EOS となる計画を定める必要がある。
c. サポート終了の対応（EOS 以降）
医療機関は、EOS 後の医療機器については、新たな脆弱性が発見されても医療機器事業者からパッチ等の対策は得られない。医療機関は、予め定めた EOS 後の計画に基づいて対応する必要がある。当該医療機器を EOS 後も使い続ける場合、医療機関は、緊急性の高い脆弱性が明らかになる可能性によって、危険性が高い状況にあることを常に意識してリスクマネジメントを実施しなければならない。
医療機器事業者は、EOS 後であっても、薬機法において、医療機器の有効性及び安全性に関する事項その他製品の適正な使用のために必要な情報を収集し、医療機関への情報提供を行うよう努めなければならないことや、医療機器に不具合が発生し、健康被害が発生した又は健康被害の発生のおそれがあることを知った場合には、必要な措置を講じなければならないこととされており、サイバーセキュリティに関する事項についてもこれに基づく対応を行う必要がある（医療機器のサイバーセキュリティ対策に関連する情報提供について（令和７年４月 17 日付厚生労働省医薬局医療機器審査管理課長他連名通知）参照）。

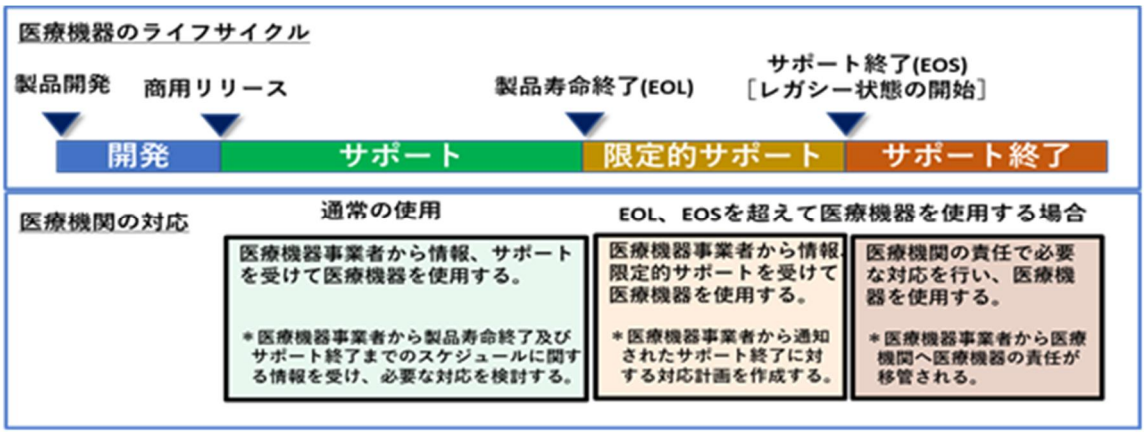

図２　サイバーセキュリティに関する医療機器のライフサイクルと医療機関の対応

② 保守実施計画の理解と実施の調整

予測できない緊急性の高い脆弱性が明らかになった場合を除き、通常のパッチ等のアップデートは定期点検等のタイミングで行われることが多い。医療機関は、医療機器事業者が実施するサイバーセキュリティに関する保守項目、実施時期について、他の医療機器及びシステムを含め IT インフラ全体の保守計画を考慮して、適切に実施されるよう具体的な実施計画について把握し調整する。特記事項等があれば必要に応じて医療機器事業者と協議して合意事項を保守契約等に記載する。

③ 医療機器の使用環境全体のセキュリティ情報収集

医療機関は、医療機器事業者から提示される SBOM を中心とするセキュリティ文書によって、使用されているソフトウェア部品を把握し、医療セプター、独立行政法人 情報処理推進機構（IPA）、一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC）等から開示される脆弱性情報及び医療機器事業者から開示される当該医療機器に対する脆弱性情報（以下、アドバイザリー情報という）を活用してリスク評価を行う。

④ 医療機器の脆弱性対策実施

医療機器事業者は、医療機器に使用しているソフトウェア部品に関する脆弱性について情報収集し、1)の緊急性が高い脆弱性（例えば、CVSS（共通脆弱性評価システムの脆弱性スコア）値 9.0 以上）については、医療機関の求めに応じて、当該医療機器への影響の有無、影響有の場合の対策実施内容及び時期等についてまとめ、アドバイザリー情報として開示する。

医療機関は、このアドバイザリー情報を利用して、最終的なリスク評価及び対策が可能となる。ただし、サイバーセキュリティの評価は時間と共に変化することがあるので、これに伴って医療機器事業者の判断及び指示等の内容も変化し、複数回に渡って通知されることがある。

例えば、当初予定した期間内にアップデートが適用できない場合、当面の間ネットワークのセグメント分離等の補完的対策又は医療機器の設定の一時的な変更等

が必要となることもあり、アドバイザリー情報を通して医療機器事業者と連携して対応する。

⑤ 医療機関内の情報共有

医療機器に関する医療機器事業者との医療機関の連絡窓口は、医療機器導入先の部門であることが多いが、医療機関の IT インフラ管理部門等、医療機関内の情報共有が円滑に実施されるように定め、保守契約等に記載する。

⑥ レガシー医療機器への対策

レガシー医療機器（EOS の到達又は新たな脆弱性の発見によって、医療機器本体及び医療機器事業者が指定した補完的対策では対応が困難な状態となった機器）に対して、医療機関は、医療機器事業者と連携して、即座にリスクが高まらないように、多層防御の強化、ネットワークの分離等の対策を実施する。多層防御を強化する際は、それによって医療機器の性能が劣化し、医療機器の安全性及び有効性が低下することがないよう医療機器事業者と連携して確認する。

⑦ 協調的な脆弱性の開示（Coordinated Vulnerability Disclosure: CVD）への対応

ブルートゥース等の共通技術に関連した重大な脆弱性に対しては、不正な即時攻撃等を防止するために、一般に開示される前に JPCERT/CC、国家サイバー統括室（NCO）又は厚労省から、情報周知、状況把握等の目的で、緊急通知が届く場合がある。医療機器事業者から同様に通知が届く場合もある。医療機関は、これら通知に対し、速やかに応答し、関係部門への情報共有、注意喚起等を行う。

（２）インシデント発生時の対応

① 医療情報や医療サービスの提供体制に関わるインシデントの対応

個人情報の漏洩や医療サービスの提供体制に支障が生じる又はそのおそれがある事案であると判断された場合には、安全管理ガイドライン及び「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」（平成 30 年 10 月 29 日付け医政総発 1029 第１号・医政地発 1029 第３号・医政研発 1029 第１号厚生労働省医政 局関係課長連名通知）に基づき、所管官庁への連絡等の必要な対応を行うほか、そのために必要な体制を整備する。また、上記に関わらず、医療情報システムに障害が発生した場合も、必要に応じて所管官庁への連絡を行う。

② 患者に重篤な健康被害が発生するおそれのあるインシデントの対応

医療機器の信頼境界に沿った責任範囲に従って、医療機器事業者と連携して、状況を分析し、患者の安全を優先した上で原因を究明し、医療機器等の回復・復帰のための措置を講じる。

医療機器については、医薬品医療機器等法第 68 条の 10 第 2 項に基づき、医薬関係者が厚生労働大臣に報告する制度があり、医療機関は、報告窓口である独立行政法人医薬品医療機器総合機構（以下、PMDA という）に適宜速やかに報告する。PMDA ホームページ上の専用サイト『報告受付サイト』からオンライン報告が可能である。

https://www.pmda.go.jp/safety/reports/hcp/0002.html
なお、同インシデントについては当該医療機器事業者も同様に PMDA に報告することが求められており、医療機関からの報告との齟齬がないことが確認されることになる。

附属書

用語及び参考定義（五十音順）

五十音順	用語	出典
あ	**アップデート** 医療機器ソフトウェアを対象とした修正、予防、適応又は完全化に関する変更 注釈 1:　JIS X 0161:2008 に規定するソフトウェア保守活動に由来する。 注釈 2:　アップデートには、パッチ及び設定変更が含まれる。 注釈 3:　適応及び完全化に関する変更は設計仕様時になかったソフトウェアの改良である。"	IMDRF ガイダンス和訳より （製造販売業者向け手引書より）
い	**医療セプター** セプターは、重要インフラ事業者等の情報共有・分析機能及び当該機能を担う組織であり、15 分野に 21 セプターが活動している。その一つに医療セプター（事務局：日本医師会情報システム課）があり、医機連及び JAHIS（一般社団法人保健医療福祉情報システム工業会）はオブザーバとして参加しており、この各加盟団体及び加盟企業は医療セプターのサイバーセキュリティ情報を活用できる。また、厚生労働省は自治体に対し「医療セプター活用と連携・協力」について要請している	
え	**MDS2（製造業者による医療機器セキュリティ開示書）** Manufacturer Disclosure Statement for Medical Device Security 医療機器製造業者が、ヘルスケア事業者（医療機関）に対してセキュリティ関連情報を開示するための記載様式を提供するセキュリティ宣言書。米国において HIPAA 法におけるセキュリティ規則対応のため、HIMSS が 2004 年 12 月に作成、公表したテンプレート文書のことで、2019 年に最新版が公開された。MDS2 は、医療機関と製造販売業者との間の情報共有ツールとして定着し、広く利活用されている。 一般社団法人日本画像医療システム工業会（JIRA）のホームページに和訳掲載 https://www.jira-net.or.jp/publishing/security.html	ANSI/NEMA HN 1-2019 （製造販売業者向け手引書より）
	MDS（製造業者による医療情報セキュリティ開示書） Manufacturer Disclosure Statement for Medical Information Security MDS は、厚生労働省「医療情報システムの安全管理に関するガイドライン」への適合性を示すため、医療機器を含む医療情報システムの製造業者が、提供する医療情報システムのセキュリティに関して、医療機関等に関連情報を開示する記載書式である。MDS2 とは、目的、適用範囲が異なるが、医療機器を含む医療情報システムの情報セキュリティの顧客向け文書として用いられている。	JAHIS/JIRA 「製造業者/サービス事業者による医療情報セキュリティ開示書」 ガイド Ver.5.0 （製造販売業者向け手引書より）
	SDS（サービス事業者による医療情報セキュリティ開示書） Service Provider Disclosure Statement for Medical Information Security SDS は、厚生労働省「医療情報システムの安全管理に関するガイドライン」への適合性を示すため、医療情報サービスのサービス事業者が、提供する医療情報サービスのセキュリティに関して、医療機関等に関連情報を開示する記載書式である。	JAHIS/JIRA 「製造業者/サービス事業者による医療情報セキュリティ開示書」 ガイド Ver.5.0 （製造販売業者向け手引書より）
き	**共通脆弱性評価システム（CVSS）** 情報システムの脆弱性に対するオープンで汎用的な評価手法であり、事業者に依存しない共通の評価方法を提供。CVSS を用いると、脆弱性の深刻度を同一の基準の下で定量的に比較可能である。 IPA　共通脆弱性評価システム CVSS v3 概説 https://www.ipa.go.jp/security/vuln/CVSSv3.html FIRST Common Vulnerability Scoring System Version 4.0 https://www.first.org/cvss/v4-0/	（製造販売業者向け手引書より）

五十音順	用語	出典
こ	**攻撃** 資産の破壊、暴露、改ざん、無効化、盗用、又は認可されていないアクセス若しくは使用の試み	JIS Q 27000:2019 （製造販売業者向け手引書より）
	国家サイバー統括室（NCO（National Cybersecurity Office） 2025 年５月のサイバー対処能力強化法等の成立等を踏まえ、2025 年７月、内閣サイバーセキュリティセンター（NISC）を改組し、内閣官房に設置。	
さ	**サイバーセキュリティ** 情報及びシステムが不正な活動（不正なアクセス、使用、開示、中断、改変、破壊等）から保護されており、機密性、完全性、可用性に関するリスクがライフサイクル全体に渡って受容可能なレベルに維持されている状態	JIS T 81001-1:2022、 IMDRF ガイダンス和訳より（製造販売業者向け手引書より）
	サポート終了（End of Support：EOS） 製品のライフサイクルにおいて、製造業者が全てのサポート活動を中止する時点。サービスサポートは、この時点を超えない。	IMDRF ガイダンス和訳より（製造販売業者向け手引書より）
	情報共有分析機関(Information Sharing and Analysis Organizations：ISAOs) サイバーセキュリティ関連情報の収集、分析、共有及び発信のために設置された組織。製造販売業者が ISAO に積極的に参加することで、患者やユーザーとの連絡や調整を含む展開を通じて、サイバーセキュリティの脆弱性に積極的に取り組み、悪用を最小限に抑えることで、企業、医療機器コミュニティ、医療・公衆衛生分野を支援することが可能である。情報共有分析センター（Information Sharing and Analysis Centers：ISAC）と呼ばれる組織もある。 国際的な組織として、H-ISAC（Health Information Sharing and Analysis Center: https://h-isac.org/）、MedISAO（https://www.medisao.com/）がある。国内では、NISC（内閣サイバーセキュリティセンター）によって立ち上がった情報共有組織セプターのひとつ医療セプター（事務局：日本医師会情報システム課）がある。医機連（一般社団法人日本医療機器産業連合会）及び JAHIS（一般社団法人保健医療福祉情報システム工業会）はオブザーバーとして参加しており、この各加盟団体及び加盟企業は医療セプターのサイバーセキュリティ情報を活用できる。	（製造販売業者向け手引書より）
し	**信頼境界** 認証が要求される又は信頼レベルの変更（高いレベルから低いレベルへの変更又はその逆）が起こる境界を表現する脅威モデルの要素 注釈 1：製品のユーザーに対する信頼境界の実施メカニズムは、通常、認証（例えば、 チャレンジ・レスポンス、パスワード、生体認証、デジタル署名）及び関連する権限付与（例えば、アクセスコントロールのルール）を含む。 注釈 2：データに対する信頼境界の実施メカニズムは、通常、ソースの認証（例えば、 メッセージ認証コード、デジタル署名）及び／又はコンテントバリデーションを含む。	JIS T 81001-5-1:2023 より
せ	**脆弱性** システムのセキュリティポリシーを破るために悪用される可能性のある、システムの設計・実装又は運用・管理における欠陥又は弱点 一つ以上の脅威によって悪用される可能性のある資産又は管理策の弱点	JIS T 81001-1:2022 より JIS Q 27000:2019 （製造販売業者向け手引書より）
	セキュリティアドバイザリー 次のような情報を提供する。 ・他社製品あるいは一般的な技術に関する脆弱性で自社製品に大きな影響を与えるもの ・自社関連の脆弱性に関する情報の捕捉、追加 ・まだ修正モジュールが作成されていない脆弱性に関する情報	（製造販売業者向け手引書より）
	製品寿命終了（End of Life：EOL） 製品のライフサイクルにおいて、製造業者が定めた有効期間を超えた製品の販売を終了し、製品について正式な EOL プロセス（ユーザーへの通知等）を実施する段階。	IMDRF ガイダンス和訳より（製造販売業者向け手引書より）

五十音順	用語	出典
そ	**ソフトウェア部品表（SBOM）** 医療機器製品に実装されているオープンソース及び市販のソフトウェア部品表患者を含む医療機器のユーザーが、その資産を効果的に管理し、医療機器及び接続されるシステムに対して識別された脆弱性の潜在的影響を理解し、医療機器の安全性及び性能を維持するための対応を可能にするものとして位置づけられる。SBOM は販売時及び変更があった場合、顧客に通知する。またこれ以外に、製品導入の検討にあたって開示を求められる場合もある。	（製造販売業者向け手引書より）
ひ	**PSIRT** 組織が提供する製品の脆弱性に起因するリスクに対応するための組織内機能。自社製品の脆弱性への対応、製品のセキュリティ品質管理・向上を目的とした組織 JPCERT　https://www.jpcert.or.jp/research/psirtSF.html （一般社団法人コンピュータソフトウェア協会、JPCERT/CC） 脆弱性対処に向けた製品開発者向けガイド（IPA） https://www.ipa.go.jp/files/000085024.pdf PSIRT Services Framework 1.0 日本語版 https://www.first.org/standards/frameworks/psirts/FIRST_PSIRT_Services_Framework_v1.0_jp.pdf	（製造販売業者向け手引書より）
れ	**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アップデート又は補完的対策等の合理的な手段で保護できない医療機器で、販売開始以降の年数にかかわらない。	IMDRF ガイダンス和訳より、一部修正（製造販売業者向け手引書より）

【参考 1】医療機器のサイバーセキュリティに関連する通知、ガイドライン等

厚生労働省ホームページ「医療機器におけるサイバーセキュリティについて」に関連する医療機器の基本要件基準第 12 条第 3 項の規定、関連する通知、IMDRF ガイダンス及び医療機器のサイバーセキュリティ対策に役立つ資料等が掲載されている。

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

以下の３つの IMDRF ガイダンスは、医療機器事業者を対象としているが、医療機関の医療機器のサイバーセキュリティ対策にも役立つ。

「N60　医療機器サイバーセキュリティの原則及び実践(IMDRF ガイダンス)」(2020/03/18)

「N70 レガシー医療機器サイバーセキュリティの原則及び実践」(2023/03/28)

「N73 SBOM の原則及び実践」(2023/03/28)

【参考 2】安全管理ガイドライン（医療情報システムの安全管理に関するガイドライン）

医療機関の医療情報システムに関しては、厚生労働省から「医療情報システムの安全管理に関するガイドライン」（第 1 版が 2005 年 3 月に示され、情勢に応じた改定が随時行われている。以下、「安全管理ガイドライン」という）が発出されている。情報セキュリティの対策は、本手引書に示したものに限らず、安全管理ガイドライン及び情報セキュリティマネジメントシステム（ISMS）の実践等によって適切な対策を取るべきことに十分留意することが必要である。

安全管理ガイドラインは、近年のサイバー攻撃の手法の多様化・巧妙化、情報セキュリティに関するガイドラインの整備、地域医療連携や医療介護連携等の推進、クラウ

ドサービス等の普及等に伴い、医療機関等を対象とするセキュリティリスクが顕在化していることへの対応として、情報セキュリティの観点から医療機関等が遵守すべき事項等の規定を設けるなど所要の改定が繰り返しなされている。

また安全管理ガイドラインに関する「医療機関・薬局におけるサイバーセキュリティ対策チェックリスト（https://www.mhlw.go.jp/content/10808000/001253950.pdf）」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」が公開されている。
ここでは、『なお、「医療情報システムの安全管理に関するガイドライン」の内容が e-文書法、個人情報保護法等への対応を行うためのセキュリティ管理等も含めて多岐に渡る一方、本チェックリストは「医療情報システムの安全管理に関するガイドライン」のみを遵守しているかのチェックリストではなく、幅広くサイバーセキュリティ対策に特化した内容となっていることに留意されたい。』となっており、IoT 機器を利用する場合の項目も含まれている。

【参考 3】医薬品医療機器等法（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）

我が国においては、医療機器の製造販売を規制する医薬品、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）に紐づく医薬品、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 3 月 29 日付け厚生労働省告示第 122 号、以下「基本要件基準」という）によってサイバーセキュリティを含むリスクマネジメントが求められ、使用者に対する情報提供や注意喚起を含めて最新の技術に立脚して医療機器の安全を確保しなくてはならないこととされている。

【参考 4】IMDRF ガイダンス（医療機器サイバーセキュリティガイダンス）

- N60 Principles and Practices for Medical Device Cybersecurity
  （医療機器サイバーセキュリティの原則及び実践）
- 発行：IMDRF（国際医療機器規制当局フォーラム）、2020 年 3 月 18 日
- 原文ＵＲＬ：http://www.imdrf.org/documents/documents.asp
- 一般原則：
  医療機器を開発、規制、使用、監視する際に責任関係者が検討すべき、医療機器のサイバーセキュリティに関する一般指針原則を示す。本ガイダンスの全体を通して述べられている当該原則は、医療機器の全体的なサイバーセキュリティを向上させるために重要であり、これに従うことで、患者の安全を確保する上で有益な効果を得られることが期待される。

（１）国際整合（Global Harmonization）
サイバーセキュリティに対する取り組みの国際的整合は、イノベーションを促進し、安全で効果的な医療機器を遅滞なく患者の治療に使用可能とすると共に、患者の安全

を確保するために必要である。

（２）製品ライフサイクルの全体（Total Product Life Cycle（TPLC））

サイバーセキュリティの脅威及び脆弱性に関するリスクは、初期構想段階からEOS に至る、医療機器の製品寿命に関する全ての段階を通して検討することが望ましい。リスクマネジメントを製品の全ライフサイクルにわたって適用し、サイバーセキュリティのコントロール及び緩和策を組み込む際、医療機器の安全性及び基本性能を維持することが重要である。

（３）共同責任（Shared Responsibility）

医療機器のサイバーセキュリティは、製造販売業者、医療機関、規制当局及び脆弱性発見者の共同責任である。全ての責任関係者は、医療機器の全ライフサイクルを通して、潜在的なサイバーセキュリティリスク及び脅威を継続的に監視、評価、緩和、情報共有、対応するため、自らの責任を理解し、他の責任関係者と密接に連携する必要がある。

（４）情報共有（Information Sharing）

サイバーセキュリティに関する情報の共有は、安全でセキュアな医療機器を実現するためのTPLC アプローチの基礎原則である。サイバーセキュリティの情報を共有するため、全ての責任関係者が、市販前及び市販後に積極的に対応することが奨励される。その一環として、全ての責任関係者は、情報共有分析機関（Information Sharing Analysis Organizations：ISAOs）に積極的に参加することが奨励される。もう一つの情報共有手法として、協調的な脆弱性の開示（CVD）が挙げられる。