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

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

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ます。特に医療機関で使用される医療機器*1は医療安全*2に直接つながるため、医療機器のサイバーセキュリティ対策は今後の重要な課題となっており、医療機関、医療機器事業者*3、及び他の全てのステークホルダーが連携して対応することが必須となっています。

我が国でも医療機関等に向けた「安全管理ガイドライン*4」等に加え、医療機器事業者等に向けたサイバーセキュリティに関する多くの通知を発出するなどの取り組みが行われています【参考 1】。また、医療機器規制の国際調和を目指す IMDRF（国際医療機器規制当局フォーラム）*5からは「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、日本でも薬機法*6による医療機器に関する規制に IMDRF ガイダンスを取り入れ、2023 年を目途に本格運用するとの方針が示されており、医療機器事業者に対して製造販売業者向け手引書*7が別途作成・公表されています。

こうした状況を踏まえ、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）の活動として、一般社団法人日本医療機器産業連合会において、医療機関における医療安全を確保するための医療機器のサイバーセキュリティ対策についての手引書を作成しました。

まず、本書の位置付け及び安全管理ガイドライン等との関係などのイメージを図１に示しますので、確認してください。

以下、「２．本書の目的と対象」「３．サイバーセキュリティ対策について」「４．医療機関の取り組みの実際」の順で、医療機関において実施すべき取り組みについて説明しています。

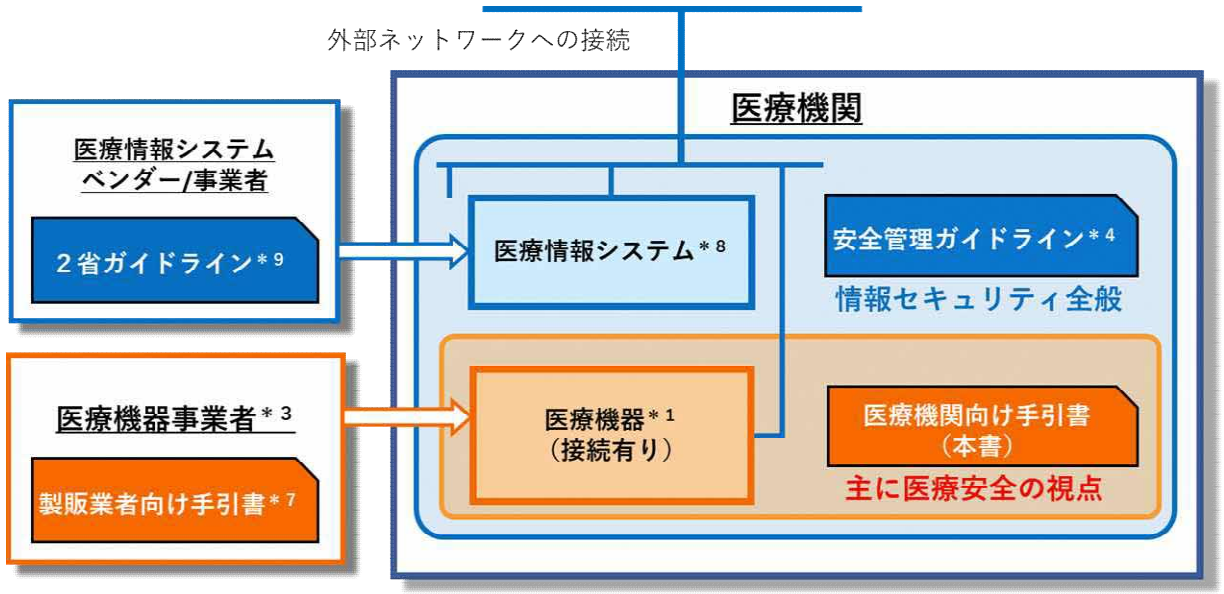

図１　医療機関向け手引書（医療機器のサイバーセキュリティ確保のための手引書：本書）と安全管理ガイドライン等の位置付け（イメージ）

(＊1) 医療機器：薬機法*6の対象となるものが医療機器です。ヘルスソフトウェアのうち薬機法の対象となるSaMD（Software as a Medical Device）も対象となります。また、契約により構成、導入される保守のためのネットワーク機器やシステムも本書の対象となります。

(＊2) 医療安全：本書では患者安全を中心に、使用者、医療従事者等の安全も含めます。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安全にリスクが生じる可能性も含めます。

(＊3) 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、修理業者等を指します。

(＊4) 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】

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

(＊6) 薬機法：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】

(＊7) 製造販売業者向け手引書：医療機器のサイバーセキュリティ導入に関する手引書

(＊8) 医療情報システム：本書では、例えば電子カルテシステム、オーダリングシステム、医事会計システム、各部門システム等を指します。

(＊9) 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

医療機関における医療機器のサイバーセキュリティ対策を確実に行い医療機器の医療安全を確保することを目的に、医療機関が主体的に実施することを示し、加えて医療機器事業者やサービス提供者等のステークホルダーと連携して実施する内容及びその役割と責任について説明します。また、医療機器事業者及びサービス提供者が、医療機関が安全確保を遂行するために実施する取り組みについても紹介します。

2．2　本書の対象について

（1）対象とする読者

医療機関等で医療機器に関わる全ての方を対象としています。大規模施設では経営者、医療機器安全管理責任者、医療情報システム安全管理責任者、医療機器運用担当者、医療情報システム運用担当者等が主な対象となり、クリニックを含む小規模施設では経営者、施設管理者等が主な対象と考えられます。

本書で説明する内容は大規模施設から小規模施設まで共通する項目ですが、実際の管理、運用の体制や、具体的な内容は、施設の規模や形態、医療機器の使用状況に応じて、適切に判断して実施していただくことが必要です。

なお、医療機器事業者、医療情報システム事業者、関連するサービス事業者等のステークホルダーにも参照していただき、連携強化に役立てていただくことも想定しています。

（2）対象とする医療機器

医療安全についてサイバーセキュリティ上のリスクが懸念される医療機器を対象とします。

具体的にはネットワークや機器との接続が可能であるプログラムを用いた医療機器であり、ソフトウェア単独で医療機器となる医療機器プログラム（SaMD：Software as a Medical Device）を含みます。接続方法は有線、無線を問わず、接続対象の機器は他の医療機器、医療機器の構成品、USB メモリ等の携帯型メディアなどが含まれます。（図 2 参照）
なお、医療機器事業者やサービス事業者が当該医療機器を保守するにあたって、契約等によって設置するサーバーや端末、ネットワーク機器などの医療機器認証に含まない周辺機器を含めて提供される場合においては当該医療機器を含む安全環境の維持に不可欠なものとして対象に含むものとします。

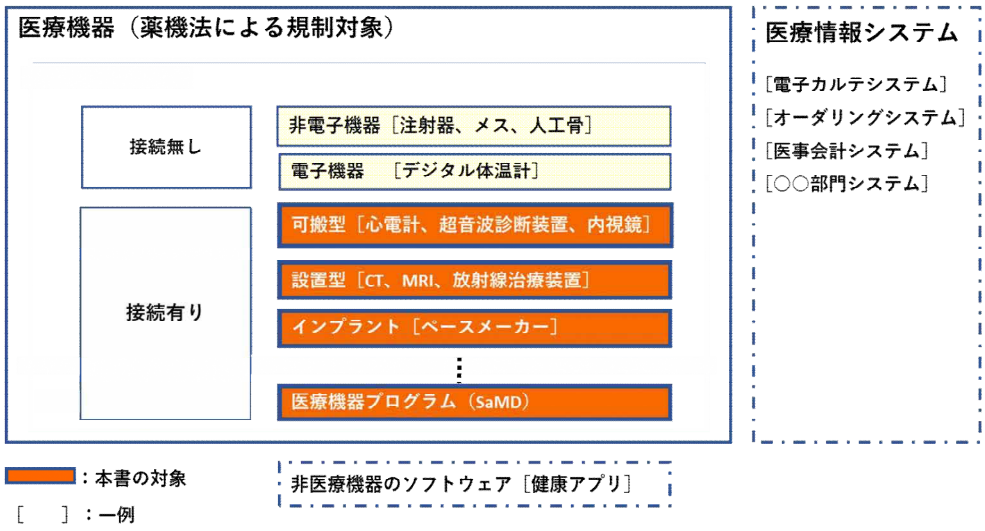

図２　本書で対象とする医療機器（イメージ）

（３）対象とするリスク

医療機器に係るサイバー攻撃の被害により、医療安全に影響を与えるリスクを対象とします。例えば、医療機器の性能に影響を与える（性能や機能の低下、誤動作、動作停止など）、診療活動に影響を与える（患者情報やオーダー情報へのアクセス停止など）、誤った診療につながる（情報の欠落や改ざんによる誤診断や不適切な治療など）、などによって医療安全が損なわれることが考えられます。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、同じネットワークに接続された他の医療機器やシステムに影響を及ぼし医療安全に影響を与えるリスクにも考慮が必要です。

（４）情報セキュリティと医療安全について

IT を用いた医療機器は、患者情報等を扱う医療情報システムを含む場合も多く、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など）が確保できる環境の整備は医療機関においては重要になりますが、本書では、これに加えて、特に医療機器の医療安全の視点から必要となる対策について説明します。（図 1 参照。）
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、別途、厚生労働省の安全管理ガイドラインに定められており、医療機関の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ます。これらは医療機器の医療安全確保のために実施すべき内容と共通又は関連する項目も多く、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す。
なお、サイバー攻撃による情報セキュリティへの侵害が、医療機器の医療安全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ります。

3．サイバーセキュリティ対策について

3．1　サイバーセキュリティ対策の基本

医療法等で求められているように、医療に関わる全ての行為は医療機関等の管理者の責任で行うことになりますので、医療機器の医療安全の確保のためのサイバーセキュリティ対策についても医療機関の責任で行います。医療機器の導入、管理、保守サービスなどについて、医療機器事業者やサービス事業者等に委託することは出来ますが、医療機関の責任の下で行うものであり、それに関する契約（役割等）を明確にしておくことが必要となります。

3．2　ステークホルダーとの連携

医療機器事業者は、薬機法に従ってサイバーセキュリティ対応を含めた医療機器の市販前、市販後の対応を行います。
医療機関においては、サイバーセキュリティ対応を行う医療機器事業者等と連携した取り組みを行うことが必要です。医療機関に医療機器を導入する際、及びこれを運用・管理する際には、医療機器事業者はもちろん、医療情報システムや医療機器の導入やメンテナンス等を担うサービス提供者との連携を図ることが重要です。一方で、医療機器事業者やサービス事業者は医療機関の要請に対して対応できるよう組織的な準備をすることになります。この連携を進めるためには、医療機関における医療機器のネットワークへの接続状況を可視化し関係者と共有出来るようにするためのネットワーク構成図等（後述）を整備することも有用です。

3．3　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明らかになります。また医療機器事業者からは EOL（製品寿命終了）/EOS（サポート終了）などに関して、医療機器の製品寿命及びサポート条件に関する情報も提供されます。提示された EOS 以降も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ります。
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必要です。
このようなリスクマネジメントは医療機関、医療機器事業者、サービス提供者、その他ステークホルダーのそれぞれで実施するとともに、互いに連携して実施することが必要です。

3．4　サイバーセキュリティ対応の国際整合

サイバー攻撃は激しさを増し、国境の枠組みを超えて行われているとともに、常に新しい脅威が出現しています。このような意図的な脅威から発生するリスクへの対応のためには、従来から行ってきた医療機器事業者による医療機器のサイバーセキュリティ対応も国際調和を図るとともに、すべてのステークホルダーとの連携による協力関係を構築することが重要になります。IMDRF ガイダンス（前述）では、一般原則として国際整合、製品ライフサイクル全体、共同責任、情報共有が示され、医療機器事業者、医療機関、サービス事業者等のステークホルダーに対して、連携してサイバーセキュリティ対応を行うことが求められており、薬機法へ取り入れられること（前述）に伴い、医療機器事業者が医療機器について対応することになります。医療機関においても、このようなサイバーセキュリティ対応の重要性を理解し、連携した取り組みをすることが必要です。

4．医療機関の取り組みの実際

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を表 1 に示します。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、そのネットワーク環境の整備が基本となりますので、取り組みの実際についての説明には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内容の一部も含まれています。

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対策・インシデント対応で行うこと（概要）

ステータス		医療機関	医療機器事業者（その他ステークホルダーを含む）
医療機器の導入まで	導入前の準備	●サイバーセキュリティポリシーの確立（医療情報セキュリティ体制の構築等） ●IT インフラの構築・ネットワーク構成図の整備 ●関係者の教育 ●アップデートオプション、保守計画の確認	○提供文書の作成 ・注意事項等情報及び取扱説明書 ・顧客向けセキュリティ文書（システム（ネットワーク）構成図、MDS2、SBOM 等）
	導入時	●医療機器に関する情報の確認 ●保守・サービスに関する役割・責任の明確化、契約締結 ●インシデント発生時の対応手順の確立	○必要情報の提供 ○保守・サービスに関する役割・責任の明確化、契約締結 ○インシデント発生時の連携体制の確認
医療機器の導入後	通常時の管理、運用	●意図する使用環境における機器の運用 ●情報共有 ●協調的な脆弱性の開示（CVD） ●脆弱性の修正	○情報収集、提供 ○脆弱性に関するセキュリティアドバイザリー情報、修正や指示等の提供

			○協調的な脆弱性の開示（CVD）
	インシデント発生時の対応	●インシデント状況の把握 ●関係方面への報告、広報 ●対応手順の実行 ●発生後のインシデントの情報整理、対応手順や通常時の管理、運用へのフィードバック	○医療機関との連携活動 ○規制当局等への報告、情報提供 ○医療機器等の対応
	レガシー状態での対応	●限定的なサポート期間、サポート終了の確認と理解 ●サポート終了後、使用を継続することに対するリスクマネジメントの実施 ●本体では対応が困難な脆弱性の暴露によって、突然レガシー状態となった場合の対応	○限定的なサポート期間、サポート終了の情報提供 ○連携した対応 ○補完的対策を含む緩和策の提供

4．1　医療機器の導入前の準備

①サイバーセキュリティポリシーの確立

医療機関では医療機器のサイバーセキュリティに対するポリシー（基本方針）を明確にする必要があります。IT インフラを整備しこれを維持管理するための方針や情報共有についてのポリシーを明確にするとともに、医療セプター等の ISAO（情報共有分析機関）からの情報を常に確認し、自施設で必要になる対策があれば実施すること及び対策が必要になる可能性について医療機器事業者等に確認することが求められます。医療セプターでは、NISC（内閣セイバーセキュリティセンター）や厚生労働省と連携し、サイバーセキュリティに関する情報共有や演習、訓練等の活動を行っています。医療機関には、医療関係団体との連携等によりこれらの活動に積極的に参画することが推奨されます。

また、サイバーセキュリティインシデントが発生した場合の対応手順についても予め定め、関係者に周知しておくことが必要です。

②IT インフラの構築とネットワーク構成図等の整備

医療機関では医療機器の使用環境としての IT インフラを整備する必要があり、そのためには安全管理ガイドラインに従って医療情報システムの情報セキュリティの確保のための体制を構築し、維持管理することが必要です。

医療機関内で医療情報システムや医療機器がどのようなネットワークを構成し、接続されているかを視覚化したネットワーク構成図やサーバー構成図、システム機能構成図を作成し、関係者への説明や状況の把握・理解のために使用します。

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、通信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します。

［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、ルーターなど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関係者の教育

医療機関は施設内のすべての関係者に対して、自施設の医療機器のサイバーセキュリティに関するポリシー、医療セプター等からの情報で必要なもの、サイバーセキュリティインシデントが発生した場合の対応手順等について教育し、周知しておくことが必要です。

厚生労働省のウェブサイトにも「医療機関向けセキュリティ教育支援ポータルサイト」が開設され、「医療機関等向けサイバーセキュリティ研修用動画」等も公開されており、参考にすることが出来ます。

４．２　医療機器の導入時

①医療機器に関する情報の確認

医療機器事業者から提供される情報が、自施設におけるサイバーセキュリティ確保のために十分であることを確認し、必要な場合にはネットワーク構成図等を更新します。

［医療機器事業者から提供される情報の例］

・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 機器等の支援インフラについての具体的なガイダンス
・安全性の強化につながる可能性のある設定に関する説明
・安全性の高いネットワーク接続及びサービスを可能にするための技術的指示（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、設定変更、ネットワーク異常、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、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。
・製造販売業者からアップデート情報をダウンロードしてインストールするための対応手順の説明。ただし、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（「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。

・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保守、サービスに関する役割・責任の明確化

医療機器の保守・サービスは医療機関の責任において行うことになり、その一部を委託する場合でも管理責任の主体はあくまでも医療機関になります。医療機関等の管理者は、患者に対して、受託する事業者の助けを借りながら、「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」を果たす義務を負います。医療機器事業者は医療機関がこれら「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」を果たせるよう情報の提供や対応の提案などを行います。万一、サイバーセキュリティに関するインシデント発生等の何らかの不都合な事態が生じた場合においても同様に、受託する事業者と連携しながら「説明責任」及び「善後策を講ずる責任」を果たす必要がありますので、受託する事業者との契約において、受託する事業者の義務を明記することが必要です。医療機器の納入前に締結し且つ定期的に見直す保守契約には、インシデント対応中に医療機器事業者及びその他の事業者が遵守すべき事項を記載する必要があります。

③インシデント発生時の対応手順の確立

医療機関は、サイバーセキュリティのインシデントを処理するためのポリシー、インシデントを緩和又は解決し、内外の責任関係者に関連情報を開示するための方法を予め確立する必要があります。その中には、脆弱性の緩和に関する計画とリソース管理についての検討を含みます。

4．3　医療機器の導入後の管理、運用

①意図する使用環境における機器の運用

1) リスクマネジメントの実施

医療機関では、自施設の IT インフラに接続される医療機器の安全性、性能及びサイバーセキュリティに対応するために、リスクマネジメントを実施することが求められ、以下のステージで適用することが推奨されます。

・IT インフラの初期開発時
・既存 IT ネットワークへの新規医療機器の統合時
・アップデート又は改良によるオペレーティングシステム、IT ネットワーク又は医療機器自体のソフトウェア及びファームウェアの変更時

2) サイバーセキュリティ対策

医療機関は、リスクマネジメントに加え、全体的なセキュリティ体制を維持するために、以下に例示したような一般的なサイバーセキュリティの対応をすることが推奨されます。なお、これらは救急時等を含めた臨床使用状況を考慮して実施する必要があります。

［サイバーセキュリティ対策の例］

・医療機器又はネットワークアクセスポイントへの不正アクセスを防ぐための物理的又は論理的セキュリティ

・ネットワークの各要素、保存情報、サービス及びアプリケーションへのアクセス制御
・現在の全ての資産を特定し、将来的な構成の変更を追跡するための、構成管理方法の採用（ネットワーク構成図等の作成、管理等）
・製造販売業者が推奨する設定及び保護対策の適用
・医療機器の通信を制限するネットワークアクセスコントロール
・確実且つ遅滞なくセキュリティアップデートを適用するためのマネジメント
・攻撃を予防するためのマルウェア対策
・無人状態で長時間放置されている医療機器に対する不正アクセスを防ぐためのセッションタイムアウト

3)全てのユーザーに対するトレーニング/教育

医療機関は、施設内におけるサイバーセキュリティのインシデントの発生を防止するため、医師、看護師、臨床工学技士、臨床検査技師等、全ての関係者のセキュリティに対する意識を高め、安全性の高い行動を習慣付けるための基本的なサイバーセキュリティトレーニングを実施することが求められます。また、在宅医療機器等、患者自身が操作する医療機器については、患者に対する同様のトレーニングも必要です。

［トレーニング内容の例］

・セキュアなネットワークのみへの接続等
・医療機器のセキュアな操作方法、ランダムなシャットダウン/再起動、セキュリティソフトウェアの一時的無効化等
・医療機器の異常動作を検知して通知する方法等

②情報共有

1) 医療機関

医療機関は、サイバーセキュリティ確保のための推奨事項を実施し、患者安全を確保するために必要なあらゆる情報にアクセスすることが求められます。これによりサイバーセキュリティのインシデントが発生した場合でも、影響を受けた医療機器に関する情報や、現場で実施する修正策や緩和策の難易度や効果に関する情報を医療機器事業者等にフィードバックすることが可能になります。

2) ユーザー（医師、患者、介護者、消費者等）

アップデート又はその他の修正の適用要否に係る最終判断を適切に行うため、医療セプター、医療機器事業者等から提供される情報を把握しておくことが必要です。

③協調的な脆弱性の開示（CVD）

製造販売業者が、自社の医療機器に影響が大きい一般的な脆弱性が発見された、又は他で発見された脆弱性が自社の医療機器に大きく影響する場合、その脆弱性情報（共通脆弱性識別子 CVE：Common Vulnerabilities and Exposures 等）とともにセキュリティアドバイザリーを開示する必要がありますが、その緩和策及び補完的対策が立案できていない状況で開示すれば、即座にサイバー攻撃の標的になってしまうこともあります。従って、脆弱性情報を開示するタイミングには注意を要します。脆弱性の影響が大きく、広く一般的である場合は、自社の対策だけでなく、場合によっては分野を超えた連携が

必要な場合があります。この場合、製造販売業者は、規制当局等と連携して、必要な調整、対策を実施する協調的な脆弱性の開示（CVD：Coordinated Vulnerability Disclosure）のために予め確立したプロセスを例外なく実施します。未知の脆弱性を考慮することは難しいので、この CVD の取組みは重要となります。

医療機関では、医療機器事業者が提供するアップデートをインストール手順に従って適用することが期待されます。

妥当な期間内にアップデートが適用できない場合には、医療 IT ネットワークのセグメント分け等の補完的対策又は医療機器のユーザー設定の変更等について医療機器事業者から指示がある可能性がありますので、必要に応じて使用環境に関連するリスクを考慮した上で、医療機器事業者の指示に従うことが推奨されます。

④脆弱性の修正

1) コミュニケーション

リスクを管理するための情報を得るため医療機器事業者等とのコミュニケーションを図ることが必要です。コミュニケーションの内容には、脆弱性解決スケジュール、脆弱性解決方法、CVSS（共通脆弱性評価システム）スコア等の脆弱性スコア、悪用可能性指標、悪用方法、暫定的なリスク緩和手法等の重要な情報が含まれますので、これらを把握し評価することが必要です。

2) 修正作業

医療機器に必要なアップデートが適用できない場合には、リスクを緩和する代替手段を補完的対策として適用する必要があります。例えば、医療機器と医療 IT ネットワークとの間にファイアウォールを設置する又は医療機器を医療 IT ネットワークから取り外す対策等が挙げられます。これらの補完的対策は、一般的には医療機器事業者から提供される情報に基づいて、医療機関が実施します。

4．4　インシデントへの対応

①対応策の実行

医療機関は、予め定めたサイバーセキュリティのインシデントを処理するためのポリシーに従って、インシデントを緩和又は解決し、内外の責任関係者に関連情報を開示するための手順に沿って対応します。その一環として、医療機関は、脆弱性の緩和のための処置と、インシデント対応中に必要に応じて代替機器を確保することも検討します。

1) ポリシー及び役割

医療機関では、サイバーセキュリティの脆弱性又はインシデントを処理するためのポリシー及び役割を予め整備し、医療機器事業者から提供される MDS2（製造業者による医療機器セキュリティ開示書）、SBOM（ソフトウェア部品表）、脆弱性及びアップデート情報等や、医療セプター等からの情報を受領し、広く共有することが求められます。

そのためには、情報提供先及び提供元の連絡先リストを定期的に管理・検証する必要があり、医療機器の納入前に締結し且つ定期的に見直す保守契約には、インシデント対応中に医療機器事業者及びその他の事業者が遵守すべき事項を記載する必要があります。医療機関は、独自のインシデント対応チームを設立することが推奨されます。

2) 役割毎のトレーニング

予め決められた役割に応じて適切なトレーニングを実施することが必要で、その内容について定期的に見直すことが推奨されます。サイバーセキュリティインシデントを評価する専門家は、実務経験に加えて、デジタル機器に残る記録を収集・解析し、法的な証拠性を明らかにするための専門的なトレーニングを受けることが推奨されます。インシデント対応プロセスに関与する人員は、実務経験に加えて、インシデント対応のプロセス及び理論に関するトレーニングを受けることが推奨されます。インシデント対応演習を行うことも有効です。

3) 分析及び対応

医療機関は、インシデント又は脆弱性の影響を報告書により評価し、医療機器事業者等の責任関係者と協力して対応することが必要です。医療機関は、対応策及び安全関連情報を患者に周知する必要があります。

②関係方面への報告

インシデント発生に関する報告は、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、都道府県、医療セプター等に対して行う必要があり、必要に応じて医療機器・医療情報システムの保守管理委託先、医療機器事業者等に協力を求めます。また、実際に保健衛生上の危害が発生し、又は拡大するおそれがある場合には医療機器に関する安全性情報として医薬品医療機器総合機構（PMDA）に報告する必要があります。

③事後対応

医療機関は、予め定めたサイバーセキュリティのインシデントを処理するためのポリシーに従って、事態の発生について公表し、その原因と対処法について説明する必要があります。また、「原因を追究し明らかにする責任」、「損害を生じさせた場合にはその損害填補責任」、「再発防止策を講ずる責任」といった善後策を講ずる責任があります。

4．5　レガシー医療機器への対応

医療機関では、各医療機器のサイバーセキュリティについて公表された EOL（製品寿命終了）を越えた使用期間を設定する場合があります。しかし、脅威の状況は時代とともに変化し、新しい脅威の出現により、時代遅れの技術を使用するリスク及び対応に要する経費が増加することになります。医療機器事業者及び医療機関は共同責任として対処する必要があります。医療機関は、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に応じて対応すべき推奨事項を考慮し、既定の EOS（サポート終了）日以前に計画を作成する必要があります。（図 3 参照。）

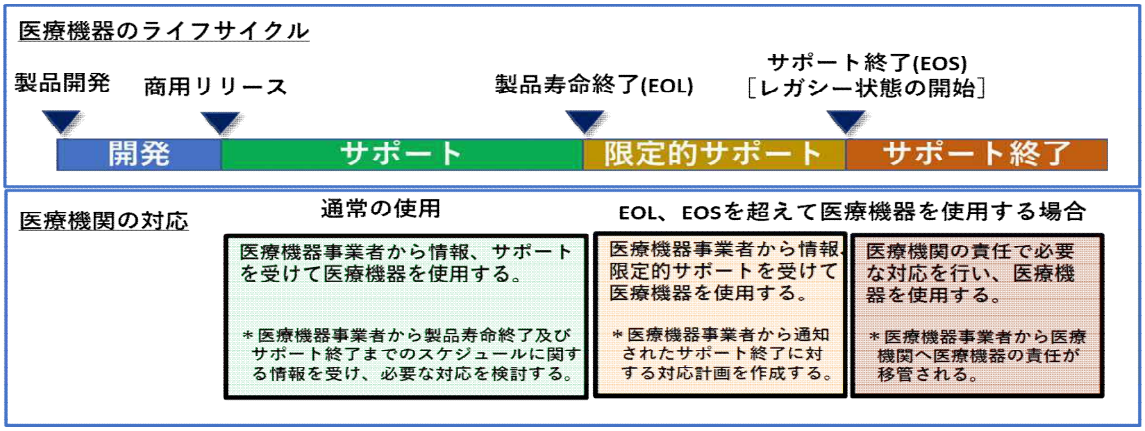

図３　サイバーセキュリティに関する医療機器のライフサイクルと医療機関の対応

1) サポート期間の対応

a. 製品ライフサイクルの計画作成、サイバーセキュリティに関する理解及び透明性を確保するために、医療機器事業者に連絡窓口と情報伝達プロセスを明確にすることを要求する必要があります。

b. サポートライフサイクルが最も短いソフトウェアコンポーネントが、最終的に医療機器のサポート及びサイバーセキュリティに影響を与えるため、医療機器事業者にSBOM（ソフトウェア部品表）の提供を要求します。医療機関は、SBOM により、医療機器のライフサイクルに影響を与えるコンポーネントをより適切に理解することが可能となるので、補完的対策等の必要性について検討することができます。

c. 医療機関は、医療機器事業者、保守・サービス事業者等と協力して使用中の医療機器を適切にサポートし、正常な稼働を維持する必要があります。例えば、ネットワークセキュリティ、アクセスマネジメント、セキュリティ業務等を行う必要があります。

d. 医療機器の使用環境における新たなリスクや進化するリスクを評価し、適切な緩和策によってリスクをコントロールするために最大限努力する必要があります。この対応策としては、ネットワークのセグメンテーション、ユーザーアクセスの制限、リスクアセスメント、セキュリティ試験、ネットワーク監視等が挙げられます。

e. サポート対象外となり、患者安全及び医療ネットワークセキュリティを脅かす可能性があるレガシー医療機器の使用を適切に段階的に終了し、セキュリティ対策で保護可能且つサポートを受けられる医療機器に置換するため、医療機器事業者が定めるサイバーセキュリティ EOS 日以前に計画を作成することが必要です。

2) 限定的なサポート期間の対応（EOL 以降）

・上記「サポート」の項目に記載した作業「c」、「d」及び「e」を引き続き行うことが必要です。

3) サポート終了への対応（EOS 以降）

a. 医療業務の継続に影響を与えることなく医療機器の使用を終了できない場合、当該医療機器のセキュリティを管理する責任及びサイバーセキュリティ EOS 日以降も使用を継続することによって発生し得るリスクを医療機関が引き受けることになります。

5．おわりに

医療機関における医療機器のサイバーセキュリティを取り巻く環境は常に変化しており、厳しさは増すばかりです。このような中で、医療安全を確保する観点から医療機器を管理する立場の方にサイバーセキュリティ対策の重要性と、そのために医療機器事業者等が実施する内容を理解していただき、すべての関係者が連携した取り組みとなるよう、医療機関において積極的に活用していただくことを目指して本書を纏めました。

多くの関係者に利用していただき、より一層の医療安全へ貢献できることを願っています。

以上

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** 内閣サイバーセキュリティセンター（NISC）により、サイバーインシデントが起こる原因等につき情報共有を行うための組織として 14 分野に 19 セプターが設置された。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、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、ヘルスケア事業者（医療機関）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.4.0 （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	（製造販売業者向け手引書より）
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）
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）

五十音順	用語	出典
	情報共有分析機関(Information Sharing and Analysis Organizations：ISAO s) 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/）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）
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）
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）
な	**内閣サイバーセキュリティセンター（NISC）** 「サイバーセキュリティ基本法」／「サイバーセキュリティ戦略」を踏まえ、「第 4 次行動計画（ 2018 年改定)」に基づき、内閣官房に設置されている	
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

［医療機関向け］

・医療情報システムの安全管理に関するガイドライン(安全管理ガイドライン)

・厚生労働省事務連絡「「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」(2021/10)

・厚生労働省通知「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」(2018/10/29)

・医療法／医療法施行規則…医療情報・医療機器の安全管理

［医療機器事業者向け］

・厚生労働省通知「医療機器におけるサイバーセキュリティの確保について」(2015/04/28)

・厚生労働省通知「医療機器のサイバーセキュリティの確保に関するガイダンスについて」(2018/07/24)

・厚生労働省通知「IMDRF ガイダンスの公表について」(2020/05/13)

・厚生労働省通知「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」(2021/12/24)

［医療機関及び医療機器事業者向け］

・IMDRF「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)

・厚生労働省事務連絡「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)」(2021/06/28)

【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」）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第 5.2 版では、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」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など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】薬機法（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」）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。

具体的には、「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 年通知）によって、サイバーセキュリティ上のリスクが懸念される医療機器のうち、無線又は有線により、他の医療機器、医療機器の構成品、インターネットその他のネットワーク、又は USB メモリ等の携帯型メディア（以下「他の機器・ネットワーク等」という。）との接続が可能な医療機器について、不正なアクセス等が想定されるため、製造販売業者は、サイバーセキュリティ上のリスクを含む危険性を評価・除去し、防護するリスクマネジメントを行い、使用者に対する必要な情報提供や注意喚起を含めて適切な対策を行うこととしている。また、必要なサイバーセキュリティの確保がなされていない医療機器については、使用者に対して必要な注意喚起を行うことや、サイバーセキュリティの確保が適切に実施されるよう、医療機関に対し、必要な情報提供を行うとともに、必要な連携を図ることが示されている。その後、医療機器のサイバーセキュリティに関する具体的な対策及び処置の考え方について「医療機器のサイバーセキュリティの確保に関するガイダンス」（平成 30 年通知）として取りまとめられた。さらに、このガイダンスを置き換えるものとして 2021 年 12 月に「医療機器のサイバーセキュリティ導入に関する手引書」が発出され、医療機器へのサイバー攻撃に対する国際的な耐性基準等の技術要件を我が国へ導入して整備することが示されている。

医療機器の使用環境の特定、意図する使用環境におけるサイバーセキュリティ上のリスクに対するリスクマネジメントの実施、必要な対策、その結果リスクが受容可能になることの説明、サイバーセキュリティ上のリスクに伴う医療機器の不具合等についても GVP 省令に基づき、GVP 省令における安全性情報として取り扱い、関係者と連携を図り、適切な市販後の安全確保が求められている。

【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）

・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
・ガイダンスの一般原則：

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、患者安全の維持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。