2023年4月5日

日本医学会分科会　事務局御中

日本医学会

医療機関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（周知依頼）

平素より，本会の事業推進にご協力を賜りまして，誠にありがとうございます.

さて，令和5年3月31日付にて，厚生労働省医薬・生活衛生局医療機器審査管理課他より，別添の通り，医療機関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きましての周知依頼がありましたので，貴会の会員各位に周知の程よろしくお願いします.

なお，詳細は，厚生労働省医薬・生活衛生局医療機器審査管理課（担当：西川氏，電話：03-5253-1111（内2916））にお問い合わせ下さいますようお願い申し上げます.

本件の担当
日本医学会事務局　高橋
Tel　03-3946-2121（内4260）
Fax　03-3942-6517

薬生機審発 0331 第 14 号
薬生安発 0331 第 7 号
令和 5 年 3 月 31 日

日本医学会　御中

厚生労働省医薬・生活衛生局医療機器審査管理課
（　　公　　印　　省　　略　　）

厚生労働省医薬・生活衛生局医薬安全対策課
（　　公　　印　　省　　略　　）

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

標記について、別添写しのとおり各都道府県衛生主管部（局）長宛て通知しましたので、御了知願います。

別添

薬生機審発 0331 第 11 号
薬生安発 0331 第４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　　）

厚生労働省医薬・生活衛生局医薬安全対策課長
（　　公　　印　　省　　略　　）

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

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、国際医療機器規制当局フォーラム(IMDRF)において、サイバーセキュリティ対策の国際的な調和を図ることを目的として、「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。以下「IMDRFガイダンス」という。）が発行されたことを受け、「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５月13日付け薬生機審発0513第１号・薬生安発0513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）により、情報提供しています。さらに、IMDRFガイダンスの発行等の国際的な枠組みでの活動を踏まえて、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を目的に、医療機器のサイバーセキュリティに係る必要な開発目標及び技術的要件等を検討し、主に医療機器製造販売業者向けの「医療機器のサイバーセキュリティ導入に関する手引書」として取りまとめられたことを「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３年12月24日付け薬生機審発1224第１号・薬生安発1224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）により、お示ししたところです。

今般、IMDRFにおいて追補ガイダンスが発出されたことから、その内容に基づき、「医療機器のサイバーセキュリティ導入に関する手引書」について、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、Software Bill of Materials(SBOM)の取扱いやレガシー医療機器の取扱い、脆弱性の修正、インシデントの対応等を検討し、改訂版の「医療機器のサイバーセキュリティ導入に関する手引書」として、別添のとおり取りまとめましたので情報提供します。

我が国においては、国境を超えて行われる医療機器に対するサイバー攻撃への対策を一層強化して医療現場における安全性を確保するため、医療機器のサイバーセキュリティに係る開発目標及び評価基準を策定し、「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）等の所要の改正を行い、許認可等において医療機器のサイバーセキュリティ対応を確認することができる体制の構築を進めています。

つきましては、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製造販売業者等の体制確保を円滑に行えるよう、貴管下関係製造販売業者等に対する周知及び体制確保に向けた指導等よろしくお願いします。

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）

(一社)日本医療機器産業連合会 医療機器サイバーセキュリティ対応 WG 編集

目　次

背景

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。以下「医薬品医療機器等法」という）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（State of the Art）に立脚して医療機器の安全性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 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）によって、サイバーリスクが懸念される医療機器のうち、少なくとも、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のうち、不正なアクセス等が想定されるものについて、製造販売業者は、サイバー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が確保されていない医療機器については、使用者（患者が使用者である場合も含む）に対して必要な注意喚起を行うこと、及び医療機関に対して、サイバーセキュリティの確保が適切に実施されるよう必要な情報提供を行うこと並びに必要な連携を図ることが示されている。

さらに、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いる。製造販売業者は、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リスクに対するリスクアセスメントの実施、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、サイバーリスクに伴う医療機器の不具合等についても GVP 省令における安全管理情報として取り扱い、販売業者、貸与業者及び修理業者の協力のもと、医療機関と連携を取り、適切な市販後の安全確保が求められている。

医療機器製品は、複数国に流通する場合が多いこと、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（International Medical Device Regulators Forum： 以下「IMDRF」という）において、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）」（以下「IMDRF ガイダンス」という）が取りまとめられ、「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 5 月 13 日付け薬生機審発 0513 第 1 号・薬生安発 0513 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)によって、我が国においても、医療機器製造販売業者に対して IMDRF ガイダンスを導入することが示された。無線、インターネット及びネットワーク接続機器の使用の増加に加え、サイバー攻撃の高度化に伴い、製造販売業者は、市販前には、医療機器のサイバー攻撃に対する耐性が確保されるよう、設計及び開発を行い、市販後には、意図する使用環境における機器の運用、情報共有、脆弱性の修正、インシデントの対応等を適切に行う必要がある。また、医療現場においても適正な管理がなされるよう、製造販売業者は、医療機関、使用者、規制当局及び脆弱性発見者等のステークホルダーと必要な情報共有等を行い積極的に連携していくことが求められている。

IMDRF では、IMDRF ガイダンス N60 を基本として、より実践的なアプローチを規定した追補 N70「Principles and Practices for the Cybersecurity of Legacy Medical Devices」（レガシー医療機器のサイバーセキュリティの原則及び実践）及び追補 N73「Principles and Practices for Software Bill of Materials for Medical Device Cybersecurity」（医療機器のサイバーセキュリティのためのソフトウェア部品表の原則及び実践）が取りまとめられている（以下、これら 2 つの追補を含めて「IMDRF 追補ガイダンス」という)。この文書は、これらの IMDRF 追補ガイダンスの内容を踏まえ、さらに国内運用における考慮事項を加えて改訂し、製造販売業者が、製品ライフサイクル全体を通じてサイバーセキュリティ対応を行う際のステークホルダーとの情報共有及び連携における販売業者、貸与業者及び修理業者との協力も含めた、IMDRF ガイダンスの国内導入における手引きを示している。

なお、この文書は IMDRF 等における検討の動向に沿って、適宜改訂又は追補等が行われることに留意されたい。

医療機関等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 版が平成 17 年 3 月に示され、情勢に応じて改定されている。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、この文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。

この文書は、IMDRF ガイダンスの内容を基本としているが、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)」及び厚生労働行政推進調査事業「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（研究開発代表者：国立医薬品食品衛生研究所医療機器部第二室室長　宮島敦子)」の分担課題「医療機器サイバーセキュリティの市販後安全対策に関する研究」における検討内容を踏まえ、我が国の状況にあわせて必要な編纂をしている。なお、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対応については、当該事業の検討結果を基に別途、取りまとめられる予定である。

1. 目的

この文書は、国際的な規制調和の観点及び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策定された IMDRF ガイダンスの要求事項を踏まえ、医薬品医療機器等法を遵守し、医療機器の品質、有効性及び安全性を確保するために、製造販売業者が、本邦の医療機器に対して導入するための対応及び組織的な取組みを行うための情報を提供する。これによって製造販売業者が適切な対応を実施し、その結果、製品ライフサイクル全体（Total Product Life Cycle、以下「TPLC」という）を通じサイバーセキュリティに関するリスクを低減し、プログラムを用いた医療機器の安全性と有効性を確保することで、患者等への危害の発生及び拡大の防止に繋げる。

2. 適用範囲

この文書は、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を用いた医療機器（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（Software as a Medical Device: SaMD）を含む）及びプログラムを用いた附属品（医療機器の薬事承認等範囲内の構成品）等に関するサイバーセキュリティを対象とする。また、医療機器の保守を目的として構成されるプログラムを用いた周辺機器についても契約等に応じて対象とする。適用の要否は、医療機器のクラス分類（Ⅰ～Ⅳ）だけで判断すべきではなく、意図する使用環境、サイバーリスクに応じた危害等を考慮したリスクベースアプローチによって判断する。また、次のような患者等への危害が発生する可能性のあるサイバーセキュリティリスクに焦点をあてる。ただし、それ以外のリスクに関しても適切な対策をとることが必要なことには十分留意する。

- 製品の性能に影響を与える
- 臨床活動に影響を与える
- 誤った診断、治療又は予防に繋がる

医療機器が疾病の診断、治療、予防等に供することを考慮し、この文書では患者等への危害の防止の観点からサイバーリスクへの対応をまとめている。一方、医療機器は患者等の個人情報等を扱う医療情報システムの一部としてもみなされるため、データプライバシー等の情報セキュリティに係るリスクへの対応も実施される必要があるが、この文書の適用範囲ではない。情報セキュリティに係る対策については、別途安全管理ガイドライン等を参照する。また、製造販売業者の一般的な企業活動に関するサイバーセキュリティ対応についてもこの文書の適用範囲から除外しているため、医療機器の製造販売業者は、一般的な個人情報の漏洩等の危害についても十分な対応をすることが社会的に求められていることに留意すべきである。

3. 用語及び参考定義

この文書で使用する用語及びその参考定義を、末尾に示している。

4. 一般原則

医療機器・システムだけでなく、高度化・複雑化した世界中のヘルス IT システムにおける患者等の安全性を確保する上で、我が国の医療機器においても、TPLC に渡ったサイバーセキュリティ対応の国際的な調和を図る。

製造販売業者は、広く知られている米国国立標準技術研究所（NIST）サイバーセキュリティフレームワークだけでなく、例えば、医療機器・ヘルス IT 共同セキュリティ計画（Joint Security Plan）のベストプラクティス等を利用して、設計・開発の段階においてセキュリティを計画・実現し、次を実施する。

- 顧客向け文書の作成
- 規制当局への申請
- 苦情処理
- 脆弱性修正
- インシデント対応
- 医療機関等のステークホルダーとの継続的な情報共有及び連携

このためには、次が必要である。

- 製品のセキュリティポリシー設定
- セキュリティの定量的評価、反復試験、侵入試験等の能力向上
- これらを支える PSIRT（Product Security Incident Response Team）等の製品セキュリティ体制の構築
- 一連のサイバーセキュリティのベースラインとなる活動を定め、QMS の中に定着させる取組み

製造販売業者は、国際整合化の背景及び「共同責任（Shared Responsibility）」における自らの責任を理解し、サイバーセキュリティベースラインを構築した上で、医療機関、使用者、規制当局及び脆弱性発見者等のステークホルダーと連携可能な体制を整備する。

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 アプローチの原則である。遅滞なく情報が共有されることによって、製造販売業者が脅威を特定し、関連するリスクを評価し、それに適宜対応するための能力が最大化する。製造販売業者は、医療機器及び接続す

るヘルスケアインフラの安全性、性能、完全性及びセキュリティに影響し得るサイバーセキュリティのインシデント、脅威及び脆弱性に対する協力及びコミュニケーションを強化するため、情報共有分析機関（Information Sharing Analysis Organizations：以下「ISAO」という）等に積極的に参加することが推奨される。

5. 市販前の考慮事項

医療機器のサイバーセキュリティは、TPLC に渡って検討する。医療機器の市販前の設計・開発段階において、製造販売業者は、次を実施する。

A. セキュリティ機能の製品への組込み

B. 最新の技術に基づくリスクマネジメント手法の適用

C. セキュリティ試験

D. 医療機器をセキュアに運用するための医療機関及び使用者に対する情報提供の準備

E. 市販後活動のための計画の立案

製造販売業者は、これらの市販前の要素を検討する際、医療機器の意図する使用環境に加え、合理的に予見可能な誤使用のシナリオを充分に評価する。

5.1. セキュリティ要求事項及びアーキテクチャー設計

製造販売業者は、積極的な市販後活動だけでなく、アーキテクチャー設計において、脅威モデリング等を用いた脅威分析を行うことによって、第三者による攻撃可能性及び脆弱性の悪用可能性を充分に評価する。これによって、製品を保護すべき信頼境界及び攻撃対象領域（アタックサーフェイスともいう）をシステム構成図において特定し、製品の特質、意図する使用及び使用環境に対して組み込む設計原則及びリスクコントロール等を含む要求事項を適切に定める。この際、これらの要求事項を自社製品の設計の範囲で考慮することが重要である。この検討に用いたシステム構成図は顧客向け文書に記載する。このセキュリティに関する設計原則及び要求事項は、医療機器セキュリティ開示書（Manufacturer Disclosure Statement for Medical Device Security：以下 MDS2 という）のセキュリティ機能に対応付けて検討するとよい。

製造販売業者が自社製品の設計で考慮することが望ましい設計原則を表 1 に示す。ただし、表 1 は完全なリストを意味するものではなく、あくまでも例示である。

表 1.　医療機器の設計における検討事項に対する設計原則

設計原則	説　　明
セキュアな通信	製造販売業者は、外部からの入力だけでなく、全ての入力を検証する設計機能を検討し、セキュリティが不十分な通信しかサポートしていない機器及び環境（ホームネットワークに接続された機器やレガシー機器等）との通信を考慮する。
	製造販売業者は、医療機器の送受信データ通信を不正アクセス、不正な改変又は反射攻撃から保護する手法について検討する。例えば、製造販売業者は、医療機器/システム間通信の相互認証方法、暗号化の要否、既に送信されたコマンド又はデータの不正再送を防ぐ方法、予め定めた設定時間後に通信を切断する妥当性等について検討する。
データ保護	製造販売業者は、医療機器に保存される又は送受信される安全性に関連するデータを暗号化等によって保護する必要性について検討する。例えば、パスワードは、暗号学的に安全なハッシュとして保存する。
機器の完全性	製造販売業者は、監査ログ機能のサポート等のデータの否認防止を確保できる設計特性の要否を判断するために、システムレベルのアーキテクチャーを評価する。
	製造販売業者は、機器のソフトウェアに対する不正な改変等、医療機器の完全性に関するリスクについて検討する。
	製造販売業者は、ウイルス、スパイウェア、ランサムウェア及びその他の悪意のあるコードが医療機器で実行されることを防ぐため、マルウェア対策等のコントロールについて検討する。
使用者の認証	製造販売業者は、医療機器の使用者の認証、様々な使用者の役割に応じたアクセス権付与又は緊急時のアクセス許可等、使用者のアクセス制御について検討する。また、複数の医療機関及び医療機器の間で同じ認証情報を共有しないようマネジメントする。認証又はアクセス許可の例としては、パスワード、ハードウェアキー、生体認証又は他の医療機器では作成できない認証信号等がある。 保守点検、修理等の役割をもつ使用者には、高いアクセス権限を与える必要がある場合があり、製造販売業者は、使用者と協力して、認証情報及びアクセス許可の方法を適切にマネジメントする。製造販売業者は、医療機器が、保守点検、修理等のため、医療機器として利用できない間、臨床目的で使用されることを禁止し、その旨を表示する等の仕組みを検討する。

ソフトウェア保守	製造販売業者は、定期的なアップデートの実施プロセスと展開プロセスを確立し、そのアップデート情報を医療機関及び使用者へ共有する。
	製造販売業者は、オペレーティングシステム（以下 OS という）、オープンソース等のサードパーティ製ソフトウェアのアップデート手法及び管理方法について検討する。また、製造販売業者は、ソフトウェアのアップデートや、古いバージョンの OS 上で動作する医療機器ソフトウェア等、サポートが終了し、管理対象外となった古い OS 環境への対処方法計画を立案し、医療機関及び使用者へ共有する。
	製造販売業者は、アップデートを実施するために必要な接続について検討するとともに、コードの署名等の方法を用いて接続又はアップデートの真正性を保証する方法について検討する。
物理的アクセス	製造販売業者は、許可されていない者による医療機器へのアクセスを防止する手法について検討する。例えば、ネットワークポートを物理的にロックする、ネットワークポートへのアクセスを物理的に制限する又は必要な認証なしに物理ケーブルを用いてアクセスすることを禁止する等の手法を検討する。
リモートアクセス	製造販売業者等は、運用支援、医療機器の保守点検、修理等の機能・効率向上のため、リモートサービスを利用して遠隔地からアクセスして作業を行う場合がある。この場合、アクセス経路のセキュリティ確保に加え、医療機器におけるアクセスログ等の収集、作業終了に関する医療機関等の責任者による確認等のための手法を検討する。また、汎用で使用するネットワークポートとは異なるネットワークポートを使用する、又は別の LAN 回線を使用する等、専用の接続手段を用いる等のリスク低減策の他、使用環境に必要なリスク回避策を講じる。 製造販売業者は、作業開始前、終了後において、その内容及び結果について、医療機関に対して説明を行い、医療機関の求めに応じてセキュリティの管理状況についても説明できるようにする。
信頼性及び可用性	製造販売業者は、医療機器の基本性能を維持するため、サイバー攻撃を検出、防御、対応及び復旧する設計特性について検討する。
	製造販売業者は、機器の完全性だけでなく、可用性を維持するために、マルウェア対策等のコントロールについて検討する。予め使用するソフトウェアを登録し、それ以外のソフトウェアの実行を禁止するホワイトリスト型コントロールがあり、負荷が比較的少なく、ソフトウェアの入れ替えが比較的少ない医療機器への利用

	に適している。パターンファイル等を伴ってリアルタイムにマルウェアを検知し駆除するためのスキャンを実行するコントロールの場合は、定期点検等の検疫作業には適しているが、通常使用においては、医療機器の基本性能に影響を及ぼす可能性があるので、論理的検証だけでなく、使用環境の負荷を考慮したバリデーションの結果をもって、利用を判定する。これらのマルウェア対策ソフトウェアは、医療機器に組み込んで使用する場合、ソフトウェア部品表（Software Bill of Materials:以下「SBOM」という）の対象となる。

5.2. TPLC に関するリスクマネジメント原則

製造販売業者は、サイバーセキュリティについても JIS T 14971:2020 及び TR T 24971:2020 によって最新の技術に基づくリスクマネジメントを TPLC に渡って実施し、必要な対策を行い、その結果、重大な脆弱性がなくリスクが受容可能になることを、許認可を受ける際には規制当局へ、市販後には医療機関、使用者又は規制当局等へ説明する。リスクマネジメントプロセスの一環として以下のステップを踏むことが望ましい。

- サイバーセキュリティに関する脆弱性の特定
- 関連するリスクの推定及び評価
- リスクを受容可能なレベルまで低減するリスクコントロールの採用
- リスクコントロールの有効性の評価・監視
- 協調的な情報開示を通じ、医療機関、患者等へのリスクに関する情報の提供
- 一連の活動の文書化

セキュリティの脆弱性の評価に関しては、共通脆弱性スコアリングシステム（Common Vulnerability Scoring System：以下「CVSS」という）等の広く採用されている脆弱性スコアリングシステムを採用して透明性を確保し分析・評価を行う。この際、一般の情報セキュリティにおける使用を想定した CVSS スコア（基本値、現状値）は、医療機器として臨床環境や患者の安全への影響へ置き換えるため、再評価をする必要がある。再評価については、例えば MITRE（米国の連邦政府が資金を提供する非営利組織）が策定した医療機器向けのガイド（MITRE Rubric for Applying CVSS to Medical Devices）があるので参考にできる。

5.3. セキュリティ試験

製造販売業者は、設計・開発の検証及びバリデーション段階において、様々な種類のセキュリティ試験

を採用することによって、セキュリティコントロールが効果的に実施されていることを証明するとともに、セキュリティの対応状況を評価することによって、既知の（すでに確認され、国際的に広く開示されている）脆弱性（少なくとも重大（「致命的（Critical)」又は「ハイリスク」）と判定された脆弱性）がコードに含まれていないことを証明する必要がある。この際、静的コード解析、動的解析、堅牢性試験、ソフトウェアコンポジション解析、ファジング等の一般的セキュリティ試験に加えて、脆弱性スキャンとも呼ばれる STIGs（Security Technical Implementation Guides)基準の達成度の確認又は CIS（Center for Internet Security）ベンチマーク等のセキュリティアセスメントツールを利用した定量的セキュリティ評価等を利用して可視化する活動が有効である。セキュリティの対応状況を客観的に評価する活動は、市販前に実施し、その結果を設計のインプットに反映し、文書化するだけでなく、市販後においても繰り返し評価を実施し、その結果を文書化する必要がある。当該試験では、医療機器が使用される状況及び医療機器が他の機器・ネットワーク等に接続される環境を考慮すること。この定量的セキュリティ評価の結果は、SBOM に記載されているソフトウェアに存在する脆弱性への対応状況を確認するためにも利用可能である。

ただし、製品に導入したソフトウェアに取り除けない既知の脆弱性が存在した場合、それが如何なる手段を持っても悪用されないという妥当な証拠があれば、これを設計文書に記載し、説明可能とする。

意図する使用及び予見可能な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した上でもなお、脆弱性が悪用された場合に予見可能な患者の安全に対する影響が大きい製品は、侵入試験を実施する場合もある。これらの試験について、経済産業省が策定した「情報セキュリティサービス基準」に適合したと認められた事業者の脆弱性診断サービス（IPA 提供）や同省に登録された登録認証機関による第三者試験も利用可能である。

5.4. TPLC サイバーセキュリティマネジメント計画

製造販売業者は、製品のセキュリティポリシーとして、次の事項を規定し、市販前の段階で具体化して計画し、必要なプロセス及び組織を確立・維持する。

- TPLC を通じた脆弱性の監視
- 脆弱性の開示：脆弱性発見者からの情報を集約した上で、緩和及び修正策を開発し、脆弱性の存在及び緩和又は修正方法をステークホルダーに開示するための正式なプロセス
- アップデート及び脆弱性の修正：医療機器の安全性及び性能を継続的に維持するための、定期的な、若しくは特定された脆弱性に対するソフトウェアのアップデート又は修正作業の実施
- 重要データや患者情報のバックアップ：製造販売業者及び使用者が、バックアップを実施するための機能及び手順
- 復旧：製造販売業者、使用者のいずれか又は両者が、サイバーセキュリティのインシデント後に、

医療機器を通常の運用状態に戻すための機能及び手順

- 情報共有：セキュリティの脅威及び脆弱性に関する更新した情報を共有する組織（ISAO 等）への参加が望ましい。
- 製品寿命の開示：製品のセキュリティポリシーにしたがって、具体的な計画及び手順書を取扱説明書等の顧客向け文書として整備する。例えば、医療機器の製品寿命終了（End of Life: 以下「EOL」という）を上市してから 10 年後と計画する場合、使用する汎用 OS 等ソフトウェア汎用部品の EOL がこれより先行することも多い。このような場合、製造販売業者は、世代の異なる部品の使用（例えば、エディションの異なる OS の使用）又は部品の切替え（例えば、サポート終了までの間に OS を変更する）を含むアップデート等を市販前に計画し、顧客又は規制当局に開示できるようにする。

5.5. 顧客向け文書

製造販売業者は、医療機器のリスクマネジメントのインプットとして、意図する使用環境だけでなく、合理的に予見可能な実使用環境を考慮した上で、使用者のフィードバックを反映させながら、医療機器製品の注意事項等情報、取扱説明書及び顧客向けセキュリティ文書を作成、更新し、拡充する。さらに、在宅医療機器等、患者自身が操作することを意図している医療機器については、通常の使用方法に加えて、基本的なサイバーセキュリティに関するトレーニングを患者に対しても行うことが求められるので、製造販売業者は、これを支援できるレベルの情報提供が必要となる。

5.5.1. 注意事項等情報及び取扱説明書

注意事項等情報及び取扱説明書には、関連するサイバーセキュリティリスクを考慮して該当するセキュリティ情報を使用者に伝達するために、次に係る医療機器の適正な使用のために必要な情報を含める。

- 意図する使用環境、使用者の遵守事項（概要）、要求された環境外で使用した場合のリスク等
- サイバーセキュリティに関連する問合せ窓口及びサイバーセキュリティに関連するサービスの照会先
- マルウェア対策ソフトウェア、システムログ管理設定、ネットワーク接続設定、ファイアウォールの使用等、意図する使用環境に適した推奨されるサイバーセキュリティコントロールに関連する医療機器の使用方法及び製品仕様
- 正常な機能を回復するためのバックアップ並びに復元の機能及び手順の説明
- データを送受信するネットワークポート及びその他のインターフェイスのリスト並びにポート機能、着信・発信ポートの説明。但し、未使用ポートは無効化することに留意する。
- 使用者向けのシステム構成図

- ファイアウォール等の補完的対策に関連する装置の設置・設定に関する情報

製造販売業者は、サイバーセキュリティに関連する問い合わせ先に加え、「医療機器の電子化された添付文書の記載要領について」（令和 3 年 6 月 11 日薬生発 0611 第 9 号）に含まれる内容は注意事項等情報として記載する。それ以外の情報については製造販売業者の責任に基づき、取扱説明書等へ記載する。

5.5.2. 顧客向けセキュリティ文書

顧客向けの文書として、注意事項等情報及び取扱説明書に加えて、製造販売業者が提供する医療機器のインストール及び設定に係る技術文書、並びに運用環境のための技術的要求事項等があり、次を含む。

- 意図したとおりの医療機器の動作を確保するための、医療機器周辺の一般 IT 機器等の支援インフラの要求事項に関する使用者への具体的なガイダンス
- セキュアな設定を用いた機器の強化あるいは強化可能性に関する説明（セキュアな設定には、マルウェア対策、ファイアウォール/ファイアウォールルール、ホワイトリスト、セキュリティイベントパラメーター、ロギングパラメーター、物理的セキュリティ検出等のエンドポイント保護が含まれる）
- 必要に応じて、セキュアなネットワーク接続の展開及びサービスを可能にするための技術的指示
- サイバーセキュリティ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使用者への指示
- 医療機器に係るセキュリティ事象が検出された場合に、医療機器又は支援システムが使用者に異常を通知する方法に関する説明。なお、セキュリティ事象の種類としては、設定変更、ネットワーク異常、ログイン試行、未知のエンティティに対する要求送信等の異常トラフィックが挙げられる。
- 必要に応じて、認証された特権使用者が、医療機器の設定を保存し、回復するための方法の説明
- 許可された使用者が、製造販売業者からアップデートをダウンロードしてインストールするための体系的な手順の説明
- 医療機器のサポート終了に関する情報（6.6「レガシー医療機器」参照）
- 医療機器製品に実装されている自製（開発委託したものも含む）、オープンソース及び市販のソフトウェア部品（製品コンポーネント）の透明性を確保するための SBOM
- 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（MDS2）

なお、SBOM は、医療機関、医療機器の使用者が、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。このため、使用するソフトウェアのサプライヤーとの使用許諾、契約等によって、製造販売業者は、当該ソフトウェア部品の最新の SBOM、EOL 及び End of Support（以下「EOS」という）を把握し、当該医療機器の SBOM には、ソフトウェア及びそのバージョン、部品間の関連性等を特定可能にする情報を含め（附属書 A「ソフトウェア部品表（SBOM）の扱い」参照)、製品のアップグレード等の計画の根拠とする。

注記　SBOM 及び MDS2 は、医療機器のセキュリティ設計及びリスクマネジメント計画を踏まえた TPLC に関する網羅的な顧客向け文書となる。SBOM 及び MDS2 は、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。

5.6.　規制当局への申請に関する文書

製造販売業者は、規制当局への申請に際し、申請予定の医療機器に関するサイバーセキュリティの対策状況に関して、関係法令等に従って、必要な文書を提出する。

6.　市販後の考慮事項

医療機器に対するサイバー攻撃及び脆弱性の影響は、時間経過に伴って変化する。医療機器の脆弱性評価に利用する CVSS スコアが継続的なアセスメントの過程で小さくなる（影響が少ないと判断される）こともあれば、逆に容易に悪用される可能性が高いことが判明することもある。つまり市販前の設計段階で実施したセキュリティ対策では、リスクが受容可能な状態を適切に維持できない場合がある。このため、製造販売業者は、医療機器のサイバーセキュリティに係る対応として、医薬品医療機器等法に基づく不具合等報告（サイバーセキュリティ上の脆弱性に起因する健康被害の発生のおそれのある事象に係る報告も含む）その他の市販後安全対策を実施する他、IPA（独立行政法人情報処理推進機構）その他のサイバーセキュリティに関係する行政機関への報告を行うことに加え、ISAO、CERT（Computer Emergency Response Team)、脆弱性発見者等を含めた製品ライフサイクルの市販後プロセスに関与する全てのステークホルダーと連携したアプローチ（6.1～6.6）を行う。

6.1.　意図する使用環境における機器の運用

医療機関は、安全管理ガイドラインにより、医療機器が接続される施設の IT インフラを開発し、サイバーセキュリティを確保するために、リスクマネジメントシステムの採用に加え、全体的なセキュリティ体制の構築を義務付けられている。このため、製造販売業者は、自らの責任範囲を明確にして、医療機関におけるサイバーセキュリティを確保するために、医療機器を医療機関へ導入する際の求めに応じて、医療機器製品のシステム構成図、SBOM 及び MDS2 等の顧客向け文書を提供する。

6.2. 情報共有

情報共有は、サイバーセキュリティの脅威及び脆弱性を管理するための基本的な活動である。製造販売業者は、医療機器について、市販前に立案されたサイバーセキュリティマネジメント計画に基づき、市販後に国内外で確認されたサイバーセキュリティの脅威及び脆弱性に関する情報並びにその他の医療機器の適正なセキュリティ対策のために必要な情報を、医薬品医療機器等法に基づき継続的に収集、分析するとともに、それを医療機関へ提供する。

一方、我が国で発生したインシデント等であっても、その医療機器が稼働している可能性がある国・地域の必要な全関係者に対して、各国・地域の規制に応じた情報共有が必要となる場合があることに留意が必要である。例を挙げるとすれば、公開された脆弱性に対する、影響を受ける製品及び影響の内容、アップデートやその他の緩和策の利用可能性又は計画等を記述したセキュリティアドバイザリー（セキュリティ報告）等がある。製造販売業者がホームページに掲載したり、場合によっては直接顧客に届けたりする場合もあるかもしれない。緊急性が高い場合等、より国際的に一貫性のある情報を可能な限り同時に情報共有していくためには、規制当局や ISAO/CERT と連携して情報の発出に積極的に協力する。また、サイバーセキュリティの特性から適切な情報更新が必要である。

情報共有のコミュニケーションは、共有された情報が商業的な優位性を得るために使用されるべきではないことを理解して、必要に応じて書面による合意をもって設定することが望ましい。情報共有を促進する方法の一つとして、共有される情報の匿名化を考慮する。

患者等への健康被害を防ぐ観点から医療機器の製造販売業者が使用者等との間で共有すべき情報としては、次の事項が挙げられる。

- 当該医療機器に影響を及ぼす又は及ぼす可能性がある脆弱性情報及びその予見可能な影響の内容
- 当該医療機器で使用していない又は直接影響を受けないが、当該医療機器以外の医療機器又は医療機関のヘルス IT ネットワークシステムにおいて、ネットワーク接続を通して、当該医療機器に影響を及ぼす可能性があるコンポーネントの脆弱性情報
- 医療機器のセキュリティに影響し得る IT 機器の情報
- 攻撃又は潜在的な攻撃に関する情報及び悪用コードの利用可能性に関する情報
- インシデント発生時の確認事項
- パッチ及びその他の緩和策（補完的対策等）の利用可能性
- 暫定処置としての医療機器の使用と結合に関する追加指示

製造販売業者が使用者等へ共有する情報には、修正策がすぐに利用できない場合等、必要に応じて脅威の緩和策及び方法も含める。例えば、医療機器に影響する脆弱性を緩和するための IT 機器の構成、既知

の悪用に対応する方法等を含める。

6.3. 協調的な脆弱性の開示（CVD）

製造販売業者が、自社の医療機器の脆弱性情報、他社の医療機器にも関係する脆弱性情報やセキュリティアドバイザリーを開示する場合、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る。従って、脆弱性情報を開示するタイミングは注意を要する。脆弱性の影響が大き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る。この場合、製造販売業者は、規制当局等と連携して、必要な調整を実施する協調的な脆弱性の開示（CVD：Coordinated Vulnerability Disclosure）のプロセスを確立し、例外なく実施する。未知の脆弱性を考慮することは難しいので、透明性を強化するこのCVDの取組みは重要である。積極的なCVDに関連して、製造販売業者は次を実施する。

- サイバーセキュリティの脆弱性及びリスクを特定及び検出するためのサイバーセキュリティの情報源の監視
- 協調的な脆弱性開示のポリシー及びプラクティスの採用（ISO/IEC 29147:2018 情報技術－ セキュリティ手法－ 脆弱性の開示）
  これには脆弱性報告の受領確認を脆弱性発見者に対して指定された期間内に通知することを含む。
- 脆弱性の検出及び処理のためのプロセス確立及び伝達（ISO/IEC 30111:2019 情報技術－ セキュリティ手法－ 脆弱性の処理プロセス）
  このプロセスは、セキュリティ研究者、医療機関等、脆弱性報告の発生源に拘わらず、明確性且つ一貫性及び再現性が求められる。
- CVSS 等の確立したセキュリティの方法論及び臨床的なリスクアセスメント手法（JIS T 14971:2020 等）に従って行う、報告された脆弱性の評価
- 修正策の実施
  修正策が可能でない場合、適切な脆弱性の緩和策又は補完的対策の実施。修正策、緩和策については、展開失敗時の報告方法及び変更のロールバック（初期化）方法を確立する。
- 脆弱性の開示予定に関する行政機関との情報共有（行政機関からの要求に基づく連携）
- ステークホルダーに対しての、脆弱性情報（適用範囲、影響、製造販売業者の現時点の理解に基づくリスクアセスメントを含む）の提供、並びに脆弱性の緩和策又は補完的対策に関する情報の提供
- 状況の変化に応じた、関係するステークホルダーに対する適切な最新情報の提供

6.4. 脆弱性の修正

脆弱性の修正に関連する対応は、患者へのリスクを低減するために必要である。脆弱性による影響は、初期の段階では明確に評価しきれない場合も多い。しかし、患者への危害が発生する可能性がありそうで、まだ確信が持てない段階においてもリスク低減のための対策が必要な場合もあることに留意が必要である。製造販売業者は、製造業者、販売業者、貸与業者及び修理業者と協力し、医療機関と連携して、遅滞のない修正によって安全確保を行う。修正には、患者への通知を含む広範な対応が含まれる。製造販売業者が、セキュリティパッチ対応等のアップデートを実施する際、医療機器としての機能の追加・変更がない場合は、都度の薬事承認を受ける必要はないことから、医療現場において、緊急性を伴うサイバーセキュリティ対策を遅滞なく進めることが可能である。また、脆弱性の修正を行うために必要なプログラム及びファイル等の提供形態は、薬事承認の内容に記載する必要はないと明確化されている。製造販売業者は、緊急性を伴う場合で、迅速な対応が困難と判断した場合には、一時的な機能の使用停止、設定変更等の応急的な処置に関する情報をセキュリティアドバイザリーとして医療機関へ提供する。

注記　アップデート等に係る一部変更申請等の取り扱いについては、「医療機器プログラムの取扱いに関する Q&A について（その 2)」（平成 27 年 9 月 30 日付け厚生労働省医薬食品局医療機器・再生医療等製品担当参事官室・監視指導・麻薬対策課事務連絡）の Q20、「医療機器プログラムの一部変更に伴う軽微変更手続き等の取扱いについて」（平成 29 年 10 月 20 日付け薬生機審発 1020 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）を参照。
なお、これらの迅速な対応については、医療機器プログラムだけでなく医療機器においても参考にすることができる。「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 6 月 28 日付け厚生労働省政策統括官付サイバーセキュリティ担当参事官室・医政局研究開発振興課医療情報技術推進室・医薬・生活衛生局医療機器審査管理課・医薬安全対策課事務連絡）も参照。

当該脆弱性の悪用を原因とするインシデントを含む安全性情報を入手した場合には、製造販売業者は、規制当局等への不具合等報告（6.5 「インシデントへの対応」参照）の要否を検討する。

製造販売業者が、セキュリティパッチ対応等のアップデートを実施する際、医療機器としての機能の追加・変更を伴う場合は、セキュリティに関する対策が他の機能、ユーザビリティ及び安全に関連するリスクコントロール手段を阻害しないこと等を確実に検証し、バリデーションを実施し、一部変更申請等を行う必要がある。

脆弱性の監視対象の多くを占めるサードパーティ製ソフトウェアコンポーネントの扱いに関しては、JIS T 2304:2017（医療機器ソフトウェアのライフサイクルプロセス）にリスクマネジメント、構成管理等に関する詳細な要求事項があり、これに基づき SBOM の構築及び市販後のアップデート等を考慮する。SBOM 等サイバーセキュリティに関連する顧客向け文書（5.5「顧客向け文書」参照）は、製品のリリースに対して必要に応じて更新する。さらに、在宅医療機器等、実際の使用環境が医療機関の施設内ではな

いことが容易に想定される医療機器については、アップデートの適用方法等に特別な配慮が必要となる。

なお、サードパーティ製ソフトウェアコンポーネントの影響を評価した上で、製品としての影響がないと評価された場合は、アップデートに代えてその旨のセキュリティアドバイザリーを提供することも重要な活動である。

6.5. インシデントへの対応

製造販売業者は、市販後のセキュリティ対策として、次を実施する。

- インシデントに対する緊急対応
  製造販売業者は、実際に発生した事象又は、発生しているかもしれない事象について、医療機器及び信頼境界内の不正アクセス、脆弱性の悪用の可能性等を調査し次の不正利用の有無及び状況を把握する。

  A. 医療機器の設定情報の不正な変更

  B. 診断・治療に対する不正な変更又は無効化

  C. 機密データの喪失、改竄又は開示

  D. 医療機器の機能停止、誤動作又は不正動作

  E. 他の機器・システムへの拡散

  マルウェア等の感染が認められた場合は、定められた手順に従って、それを除去する。また、必要に応じて、除去前に感染経路等把握のためのデータ取得を実施する。
  ネットワークへ外部から過剰なアクセスやデータ等の負荷が掛けられている場合は、医療機器側の必要ポート以外の閉鎖に加え、パケットフィルタリング等が強化されたファイアウォール、IPS（表 3 参照）等によって防御する。

- 予防的計画的な活動となるセキュリティ点検
  コンピューター・マルウェアは、感染したとしても、所定の動作を起こさず、上記 A-E を発生させないまま、機器の中に残存している場合がある。このため、製造販売業者は、定期点検等の計画された作業において、マルウェアの検疫を実施し、マルウェアが検出された場合はこれらを除去する機会を提供する。これは、予防的活動として効果的であり、残留リスクの低減につながる。

- 規制当局等への不具合等の報告
  製造販売業者は、医療機器への不正アクセス、マルウェア等への感染、ネットワークへの過剰負荷等によって、医療機器の不具合が実際に発生した場合、医薬品医療機器等法に基づき、独立行政法人医薬品医療機器総合機構（PMDA)に対する不具合等報告の要否を検討する。報告様式や報告基準、報告期限等については医薬品医療機器等法施行規則に従う他、「医療機器の不具合等報告

について」（令和 2 年 1 月 31 日薬生安発 0131 第 1 号）、「医療機器の不具合等報告の留意点について」（令和 2 年 1 月 31 日薬機品安発第 0131001 号）、「不具合報告書等の手引書」（2020 年 10 月第 8 版 日本医療機器産業連合会）等を参考にする。また、これによって医療機器に情報漏洩が発生した可能性がある場合、又は医療機関等がサイバー攻撃を受けた(疑い含む)ことに関連している場合には、「医療情報システムの安全管理に関するガイドライン」に基づき、医療機関は、医政局特定医薬品開発支援・医療情報担当参事官室への報告が必要となる場合がある。この際、製造販売業者は、医療機関の求めに応じて情報提供等を行う。

- JPCERT/CC、ISAO 等への情報共有を含むコミュニケーション
  医療機器自体の脆弱性であった場合は、JPCERT/CC を通して、共通脆弱性識別子（CVE：Common Vulnerabilities and Exposures）の取得及び脆弱性情報の登録が必要となる。製造販売業者は、これらの迅速な調整等が進められるよう、設計開発の段階で、JPCERT/CC が管理運営する「製品開発者リスト」に登録しておくこと（https://www.jpcert.or.jp/vh/register.html）が望ましい。医療機器に共通する脆弱性起因のインシデント等、広く遅滞なく情報共有する必要がある場合には、製造販売業者は、ISAO 等を積極的に活用して情報共有することが望ましい。

なお、これらを継続的かつ遅滞なく実施していくためには、製品セキュリティに特化した組織横断体制である PSIRT を構築し、対応することが望ましい。製造販売業者の企業活動に関するサイバーセキュリティのための CSIRT（Computer Security Incident Response Team）活動も重要であるが、IMDRF ガイダンスの適用範囲から除外されており、目的も異なるので留意し、適切に対応されたい。

6.6. レガシー医療機器

6.6.1. TPLC とレガシー医療機器

製品開発から始まる製品のサイバーセキュリティの TPLC を図 1 に示す。製造販売業者は、販売開始（商用リリース）に対する、製品寿命終了（EOL）及びサポート終了（EOS）について、設計開発の段階において TPLC に関するリスクマネジメント原則 (5.2) に基づき、予め計画し定める。製造販売業者は、EOL について、販売時及び変更があった場合、顧客に通知する。EOS 以降は、顧客に責任が完全に移転するため、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、製造販売業者は、遅くとも EOL までに顧客に通知し、その後変更があった場合も通知する。EOL 及び EOS の決定においては、ハードウェア部品・材料の供給、サードパーティ製ソフトウェア部品及び開発環境等のライフサイクルを考慮する。JIS T 2304 のソフトウェア構成管理及び変更管理に関する規定に従って、自製、オープンソース及び市販のソフトウェア部品（製品コンポーネント）を管理し、SBOM として提示できる仕組みを構築する。開発環境については、JIS T 2304 の「管理が必要な支援アイテム」の規定に従って管理する。

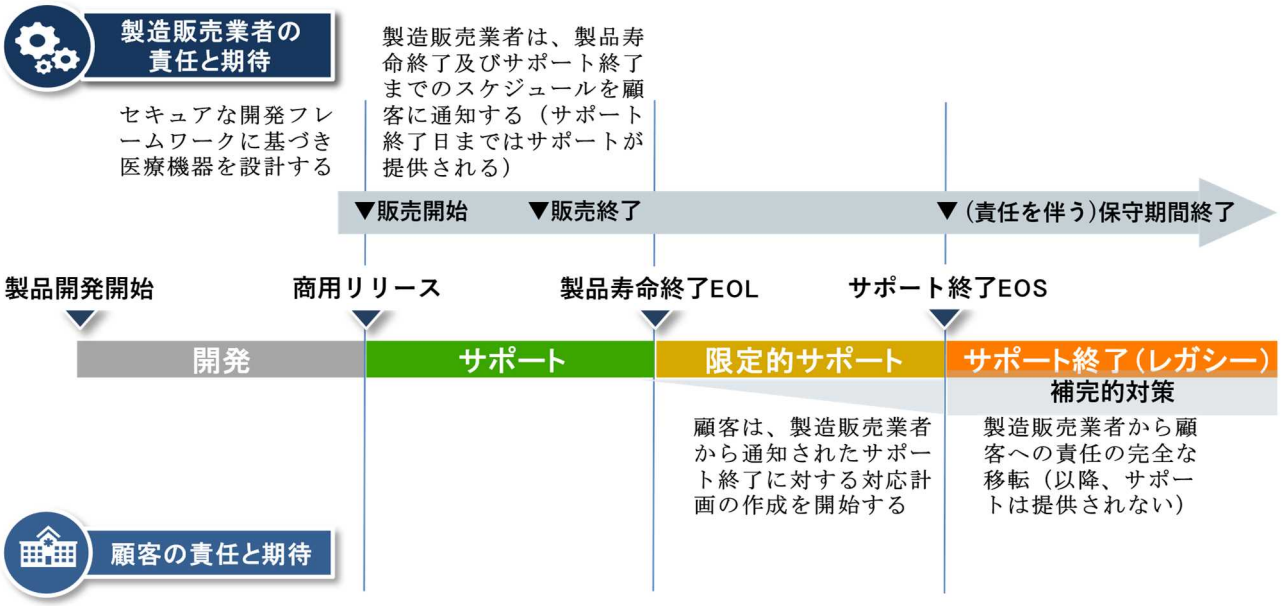

図１　製品ライフサイクルにおけるレガシー医療機器の概念フレームワーク

製造販売業者は、販売開始（商用リリース）、EOL 及び EOS に際して、表 2 に示す情報を医療機関に提供する。

表 2　各マイルストーンにおける医療機関に提供する情報

マイルストーン	提供する情報
販売開始（商用リリース）	• セキュリティポリシー • EOL 及び EOS 計画（日程） • アップグレードオプション • 取扱説明書、セキュリティ文書 • SBOM、MDS2 • 保守計画（限定的サポート段階含む）
製品寿命終了 EOL	• EOL の通知 • EOS 計画 • その他の更新情報
サポート終了 EOS	• EOS の通知 • 保守計画を除くその他の更新情報

EOL から EOS の間は限定的サポート段階と呼ばれ、計画された開発は EOL までに終了しており、セキュリティアップデート、特定の部品・材料供給のみの提供となる。限定的サポート段階は、最終的なサポート終了への移行又は製品のアップグレード・置き換えに対して、製造販売業者及び医療機関が協調し準備する移行期間となる。EOS 後は全てのサポートが終了となる。このため、EOS 後は、最新アップデートの導入等の最低限の対策が行われたとしても、「未知の脆弱性は考慮することが難しい」ため、すぐにレガシー医療機器となる可能性がある。

医療機関が医療機器を EOS 後も使用する場合、その責任は医療機関にあるため、予め医療機関との認識を共有することが重要である。ただし、EOS 後においても、医療機器において発生した脆弱性を含む不具合等に関する情報収集義務（医薬品医療機器等法 68 条の 2 の 6 第 1 項）及び行政報告義務（医薬品医療機器等法 68 条の 10 第 1 項）は製造販売業者に残る。EOS 後の継続した使用に関しては、決して推奨できる状態ではないことは、全てのステークホルダーが理解しておかねばならず、そのために製造販売業者は顧客との連携を行い、顧客への説明責任を果たす必要がある。

サイバーセキュリティが設計開発段階で十分配慮されていない製品が、そのまま市場に存在している場合は、既にレガシー医療機器となっている可能性があることに留意されたい。この場合、製造販売業者は、ファイアウォール等の補完的対策を検討すると同時に、速やかに顧客との連携を行い、顧客への説明責任を果たす必要がある。

セキュリティに関しては、老朽化の理由のみでその製品がレガシー医療機器であると判断してはなら

ないことも重要である。販売開始から 5 年以内の医療機器であっても、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医療機器とみなされる。一方、販売開始から 15 年経過した医療機器であっても、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る場合は、レガシー医療機器に該当しない。例えば、図 2 に示すように、医療機器自体はレガシー状態であっても、ファイアウォール等の補完的対策によって、セキュアな状態を保証可能な場合は、その補完的対策を含めた構成において、レガシー医療機器とはみなされない。つまり限定的サポート段階が延長可能である。製造販売業者は、この補完的対策に使用するファイアウォール等の外部機器を、当該医療機器の使用環境として指定し、その仕様及び設定情報は、顧客向け文書に含める（5.5.1「注意事項等情報及び取扱説明書」参照）。

なお、中古医療機器（貸与医療機器も含む）においても、製造販売業者が定めた製品の TPLC の範囲でサポートが提供されるため、製造販売業者が示した EOS 内で販売可能である。EOS を超えて中古医療機器が販売されることが想定される場合には、製造販売業者は、中古医療機器の顧客に対しリスクを提示するよう努める。

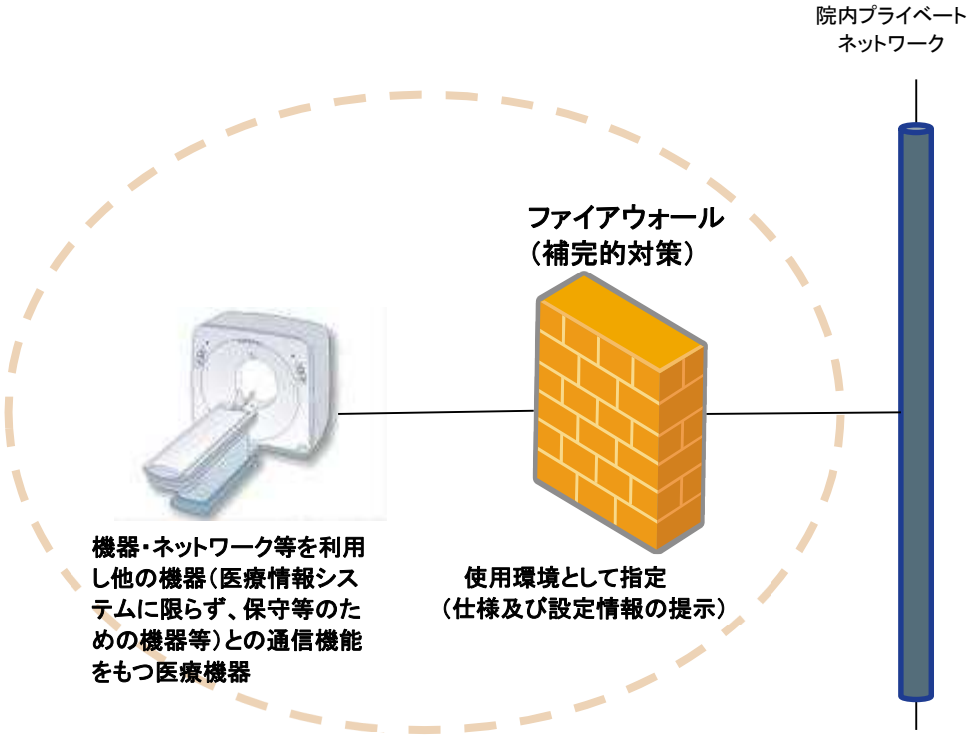

図 2　顧客向け文書の一部として扱う範囲（製造販売業者の責任範囲）

6.6.2. TPLC における考慮事項

6.6.2.1 設計・開発段階

製造販売業者は、TPLC に関するリスクマネジメント原則（5.2）に従って、サードパーティ製ソフトウェアの提供業者の倒産や買収による突然のサポート停止等を含め、脆弱性発生によるリスクがあることを理解した上で、医療機器製品の品質、有効性及び安全性が確保されるよう、製造販売業者の責任によって、EOS 後まで見据えた計画、及び必要な対策を設計段階で講じる必要がある。サードパーティ製の開発ツールを含むサードパーティ製ソフトウェア部品のライフサイクルは、医療機器製品のライフサイクルに比べ短く、合致していることは少ない。このため、製造販売業者は、サードパーティ製ソフトウェア部品について、世代を超えた管理又は代替を予め計画することも必要となる。

製造販売業者は、既知の脆弱性に対する最新のアップデートを導入し、脆弱性検査・診断ツール等を利用して定量的に対応度合いを把握・記録する。また市販後に合理的手段によってアップデートを導入できるユーザビリティが考慮された手段を機能として組み込む。

製造販売業者は、医療機器がレガシー段階に移行した場合を想定して、適用可能なファイアウォール等の補完的対策の仕様及び利用可能性等について予め検討しておく。

製造販売業者は、医療機関の責任部門に対して、いつどのように情報共有するか等、医療機器の脆弱性等サイバーセキュリティに関する情報共有の戦略を確立し、実施する。

6.6.2.2 サポート段階

製造販売業者は、市販後監視の一環として脆弱性情報を入手し、脆弱性評価の結果、製品セキュリティポリシーによって対応する必要がある脆弱性については、6.4 に従ってセキュリティアップデートを準備する。対応する必要がない脆弱性については、セキュリティアドバイザリーを顧客に提供する。製品に直接関係しない脆弱性についても、一般的に緊急性が高い（例えば、CVSS のベース基準値が 9.0 以上）等深刻度が高いことが公開されている脆弱性については、製品セキュリティポリシーに従って、当該製品が関係しないことを示すために、セキュリティアドバイザリーを顧客に提供する。情報提供を行わない場合は、その理由を含め記録を残し、顧客から提供を求められた場合に応じることができるよう準備する。

製造販売業者は、サードパーティ製ソフトウェア部品の世代交代又は代替が計画されている場合は、十分な評価を実施し、相互干渉等が発生しないことを確認した上で導入を行う。

製造販売業者は、医療機器が EOL を迎えるまでの間、一般的な不具合等の修正だけでなく、脆弱性の修正を含むセキュリティアップデートを含め、計画的に予見可能な課題に対応する。

6.6.2.3　限定的サポート段階

製造販売業者は、市販後監視の一環として脆弱性情報を入手し、脆弱性評価の結果、製品セキュリティポリシーによって対応する必要がある脆弱性については、6.4 に従ってセキュリティアップデートを準備する。対応する必要がない脆弱性については、セキュリティアドバイザリーを顧客に提供する。製品に直接関係しない脆弱性についても、一般的に緊急性が高い等深刻度が高いことが公開されている脆弱性については、当該製品が関係しないことを示すために評価記録を残す。また、顧客から提供を求められた場合に応じることができるようセキュリティアドバイザリーを準備する。

製造販売業者は、医療機器が EOL を迎えた後のこの段階においては、患者の安全に重大な影響を与える場合を除き、一般的な不具合等の修正は実施しない。

医療機関は、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を作成し、必要に応じて実施する場合がある。このため、製造販売業者は、この段階においてもファイアウォール等の補完的対策が導入されるように計画しておく。

6.6.2.4　サポート終了（EOS）段階

製造販売業者は、医療機器が EOS を迎えた後においては、一般的な不具合等の修正だけでなく、脆弱性の修正を含むセキュリティアップデートを実施しない。

製造販売業者は、EOS に際し、医療機器のセキュリティ状態に関する情報を顧客に提供すると同時に、製品に関係する深刻度が高い脆弱性（例えば、緊急性が高い脆弱性）が発見された場合等、IT ネットワーク等へ接続した状態での使用を保証できない場合は、製品をネットワークから外すことを含め、その旨を顧客に通知する（6.2「情報共有」参照）。

製造販売業者は、EOS 後においても市販後監視の一環として脆弱性情報を入手し、脆弱性評価の結果、重大と判定された脆弱性については、評価結果を記録する。また、顧客から提供を求められた場合に応じることができるよう注意喚起のためのセキュリティアドバイザリーを準備する。

6.6.3.　補完的リスクコントロールに関する考慮事項

ファイアウォール等の補完的リスクコントロールを実施することは、補完的リスクコントロール手段のコストと、新しい機器を取得するコスト及びベネフィットを比較検討すること等技術的な準備及びリソースの両面での検討が必要となる。

表 3 は、補完的リスクコントロールに対する一般的な推奨事項を示す。これらの推奨事項は、EOS 以降だけでなく、EOS 以前でも適用される可能性がある。実施にあたっては、補完的リスクコントロールが、特定の機器及びその運用環境に依存し、機器使用時の臨床的な意図を損なわないよう考慮する。表 3

のリスクコントロール手段は、網羅的なリストではなく、また、一つ以上のコントロール手段又はその組合せを利用することが適切な場合がある。

表 3　補完的リスクコントロール手段の例

コントロールのタイプ	補完的リスクコントロール手段
物理的アクセスの制限	機器を物理的に制限された領域に置いて、物理的な入室管理を適切に行うことによって、機器への物理的アクセスを許可した要員だけに制限する。
リムーバブルメディアの管理	USB ドライブ等のリムーバブルメディアの使用に関しては、システムの BIOS/UEFI*ポリシーによって、OS のポリシー又は物理的手段を通して制限する。 *BIOS: Basic input output system UEFI: Unified Extensible Firmware Interface （コンピュータープラットフォームのファームウェアと OS をインターフェイスする規約であり、UEFI は、BIOS の 16 ビット I/O・メモリ空間の制限を解決している）
ネットワークの隔離	機器をネットワークから隔離する。
ネットワークの分離	機器の VLAN（仮想 LAN）並びに機器が通信するその他のインフラストラクチャー及びサービスをセットアップする。
監視	侵入検知システム（IDS)、侵入予防システム（IPS）又はセキュリティ情報及び事象マネジメント（SIEM）を用いて、機器及びネットワークの疑わしい活動を監視する。
リモートアクセスの制限	機器からリモートアクセス機能を削除する。
ファイアウォール	機器を物理的又は仮想的なファイアウォールの背後に配置し、厳密に必要なネットワーク通信の特定ポートのみをファイアウォールで開放する。
マルウェア対策	機器にマルウェア対策ソフトウェアをインストールする。ネットワークから隔離された機器（スタンドアローン）については、定義の更新を必要としないソフトウェア、例えば、AI を用いたマルウェア対策ソフトウェアを用いる。
バックアップ及び復元	災害時、サイバー攻撃等によるデータ損失に対して保護及び早期復旧のために、バックアップ及び復元の手順を実装する。

7.　業許可に関する考慮事項

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（直接使用者の場合も含む）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することになる。そのため、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ステークホ

ルダーによる連携をとる。医薬品医療機器等法にて規定される次の事項は、サイバーセキュリティ対応においても求められる。

- 医療機器の製造販売をするときは、その医療機器に関する最新の論文その他により得られた知見に基づき、注意事項等情報（添付文書）について、PMDA ホームページにおける公表等の手段を用いて公表する。
- 製造販売業者は、医療機器を購入し、借り受け、譲り受けようとする者（電気通信回線を通じて医療機器プログラムの提供を受けようとする者も含む、以下「販売業者等」という）に対し、注意事項等情報（添付文書）の提供を行うために必要な体制を整備する。
- 製造販売業者は販売業者等とともに、医療機器の有効性及び安全性等の医療機器の適正な使用のために必要な情報を収集、検討するとともに、さらにこれらの情報について、販売業者等に対して提供するよう努める。
- 販売業者等は、医療機器の製造販売業者等が行う医療機器の適正使用に必要な情報の収集に協力するよう努める。

7.1. 業許可を持つステークホルダーの役割

医薬品医療機器等法にて規定された各業態の関係性を踏まえ、サイバーセキュリティ対応における各ステークホルダーの連携に係る考慮点を次に示す。また、図 3-1 に示す。

- 製造販売業者は、単一又は複数の販売業者を介し、その医療機器について、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、医療機器が EOL 又は EOS までの段階においては、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、MDS2 その他 CVD に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。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、医療機関と連携（販売業者も含む場合もある）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、医療機関との間（販売業者も含む場合もある）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。

- 販売業者は、製造販売業者、他の販売業者及び医療機関との情報共有を行うために必要な体制を整備する。必要に応じて、製造販売業者より共有された SBOM、MDS2 その他 CVD に必要となる情報を他の医療機関又は販売業者への共有を適切かつ遅滞なく実施できるよう、必要な処置を行う。

- 修理業者は、医療機器の脆弱性情報等の情報共有を行う等の CVD に必要な情報共有が製造販売業者から得られるよう、適切な体制を構築する。また、医療機関及び販売業者と情報共有を行うために必要な体制を整備する。なお、必要に応じて、製造販売業者より最新の SBOM、MDS2 その他 CVD に必要となる情報を取得するとともに、医療機関又は他の販売業者への共有を適切かつ遅滞

なく実施できるよう、必要な処置を行う。
なお、プログラム医療機器の場合は、基本的には修理業に相当するものはない。

7.2. リース医療機器の取扱い

医薬品医療機器等法にて規定された各業態の関係性を踏まえ、サイバーセキュリティ対応における各ステークホルダーの連携に係る考慮点を次に示す。また、図 3-2 に示す。

- 製造販売業者は、単一又は複数の販売業者を介して貸与業者へ製造販売された医療機器について、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、医療機器が EOL 又は EOS までの段階においては、販売業者と必要な連携をとり、必要に応じて貸与業者に対し、SBOM、MDS2 その他 CVD に必要となる情報を共有する。また、製造販売業者は、販売業者及び貸与業者も含めて医療機関と必要な連携をとり、必要に応じて SBOM、MDS2 その他 CVD に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。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、医療機関及び貸与業者と連携（販売業者を含む場合もある）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、修理後において医療機関及び貸与業者との間（販売業者を含む場合もある）に対してセキュリティ上の脆弱性に係る情報共有を行う。

- 販売業者は、医療機関、製造販売業者、他の販売業者及び貸与業者との情報共有を行うために必要な体制を整備する。必要に応じて、製造販売業者、他の販売業者又は貸与業者より共有された SBOM、MDS2 その他 CVD に必要となる情報を医療機関、他の販売業者又は貸与業者への共有を適切かつ遅滞なく実施できるよう、必要な処置を行う。

- 貸与業者は、医療機関、製造販売業者及び販売業者との情報共有を行うために必要な体制を整備する。必要に応じて、製造販売業者又は販売業者より共有された SBOM、MDS2 その他 CVD に必要となる情報を医療機関への共有（販売業者を含む場合もある）を適切かつ遅滞なく実施できるよう、必要な処置を行う。

- 修理業者は、医療機器の脆弱性情報等の情報共有を行う等の CVD に必要な情報共有が製造販売業者から得られるよう、適切な体制を構築する。また、医療機関及び販売業者との情報共有を行うために必要な体制を整備する。なお、必要に応じて、製造販売業者より最新の SBOM、MDS2 その他 CVD に必要となる情報を取得するとともに、医療機関及び貸与業者への共有（販売業者を含む場合もある）を適切かつ遅滞なく実施できるよう、必要な処置を行う。

7.3. 中古医療機器の取扱い

医薬品医療機器等法にて規定された各業態の関係性を踏まえ、サイバーセキュリティ対応における各

ステークホルダーの連携に係る考慮点を次に示す。また、図 3-3 に示す。

- 製造販売業者は、単一又は複数の販売業者を介して製造販売され、その後使用された医療機器について、中古販売された医療機器を使用する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、医療機器が EOL 又は EOS までの段階においては、中古医療機器を取扱う販売業者等（貸与業者が兼ねる場合もある）と必要な連携をとり必要に応じて当該販売業者等に対し、SBOM、MDS2 その他 CVD に必要となる情報を共有するとともに、当該販売業者等に対して使用された医療機器の品質等に係る注意事項等の必要な処置を指示する。また、製造販売業者は、当該販売業者等も含めて医療機関との必要な連携をとり、必要に応じて SBOM、MDS2 その他 CVD に必要となる情報提供やセキュリティパッチの適用等の必要な処置を適切かつ遅滞なく実施できるよう、必要な処置を行う。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、医療機関及び当該販売業者等と連携し、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、修理後において医療機関及び当該販売業者等との間に対してセキュリティ上の脆弱性に係る情報共有を行う。
- 販売業者は、医療機関、製造販売業者、他の販売業者、貸与業者及び中古医療機器を取扱う販売業者との情報共有を行うために必要な体制を整備する。必要に応じて、製造販売業者、他の販売業者、貸与業者及び中古医療機器を取扱う販売業者より共有された SBOM、MDS2 その他 CVD に必要となる情報を医療機関、他の販売業者、貸与業者又は中古医療機器を取扱う販売業者への共有を適切かつ遅滞なく実施できるよう、必要な処置を行う。
- 中古医療機器を取扱う販売業者等（貸与業者が兼ねる場合もある）は、医療機関及び製造販売業者との情報共有を行うために必要な体制を整備する。必要に応じて、製造販売業者又は販売業者より医療機関向けに共有される SBOM、MDS2 その他 CVD に必要となる情報を医療機関へ適切かつ遅滞なく共有（販売業者も含む場合もある）できるよう、必要な処置を行う。なお、中古医療機器を取扱う販売業者等は、使用された医療機器を他に中古販売する際、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、使用された医療機器が EOL 又は EOS までの段階においては、製造販売業者（販売業者を含む場合もある）と必要な連携をとり、使用された医療機器の品質等に係る注意事項等の必要な処置について、使用された医療機器の製造販売業者から指示を受けた場合には、医療機関に対し提供をする。
- 修理業者は、医療機器の脆弱性情報等の情報共有を行う等の CVD に必要な情報共有が製造販売業者から得られるよう、適切な体制を構築する。また、医療機関及び販売業者との情報共有を行うために必要な体制を整備する。なお、必要に応じて、製造販売業者より最新の SBOM、MDS2 その他 CVD に必要となる情報を取得するとともに、医療機関又は他の販売業者（中古医療機器を取扱う販売業者等を含む場合もある）への共有を適切かつ遅滞なく実施できるよう、必要な処置を行う。

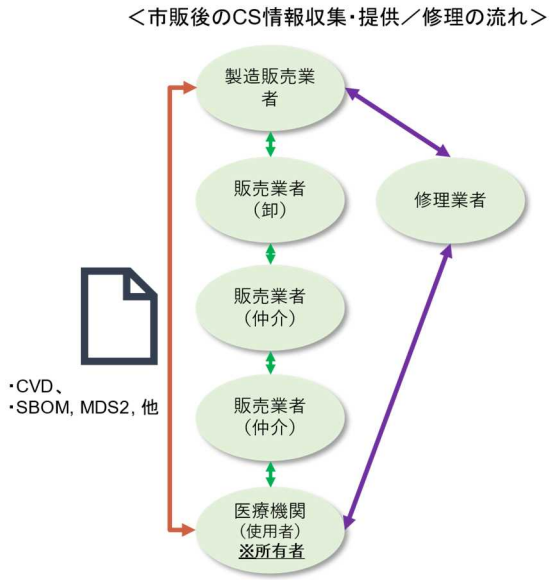

図 3-1 サイバーセキュリティ対応における各ステークホルダーの連携

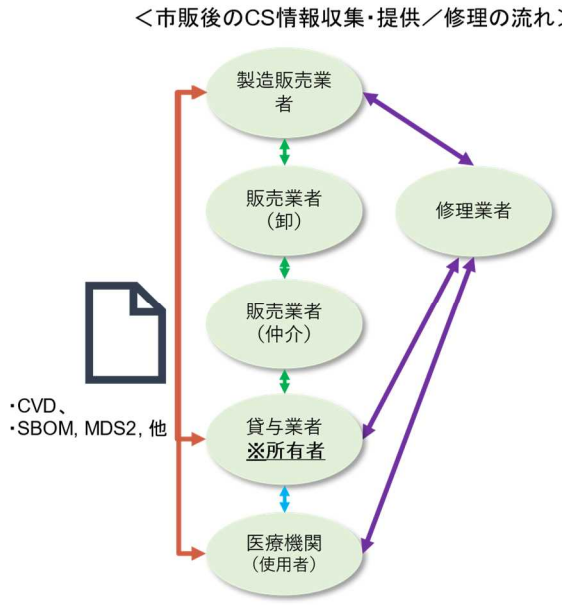

図 3-2 リース医療機器の場合

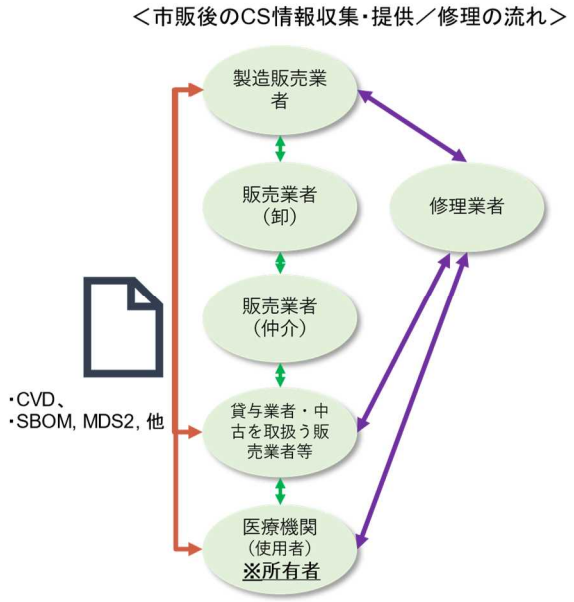

図 3-3 中古医療機器の場合

附　属　書

A.　ソフトウェア部品表（SBOM）の扱い

A.1　SBOM の全体的なフレームワーク

SBOM は、ソフトウェア部品のセキュリティ脆弱性に影響を受ける可能性のある医療機器のサイバーセキュリティを製造販売業者及び医療機関が管理するために、製造販売業者が作成する、又は開発委託先、OEM/ODM 先、海外製造元等から最終的な SBOM の提供を受ける場合等は、それが適切に作成されていることを製造販売業者が確認し管理し発行する（図 4)。製造販売業者は、医療機器のライフサイクル全体を通して実施する構成管理・変更管理プロセス及び方法論によって、SBOM を作成、管理し、ソフトウェアアーキテクチャー及びソフトウェア（を構成する）コンポーネントの情報に基づいて、SBOM を手動又はツールによって生成する。ベンダーから入手した SBOM は個別に管理するとともに、ソフトウェアコンポーネントの情報（SBOM コンテンツ）は、内部の構成管理に取り込む。

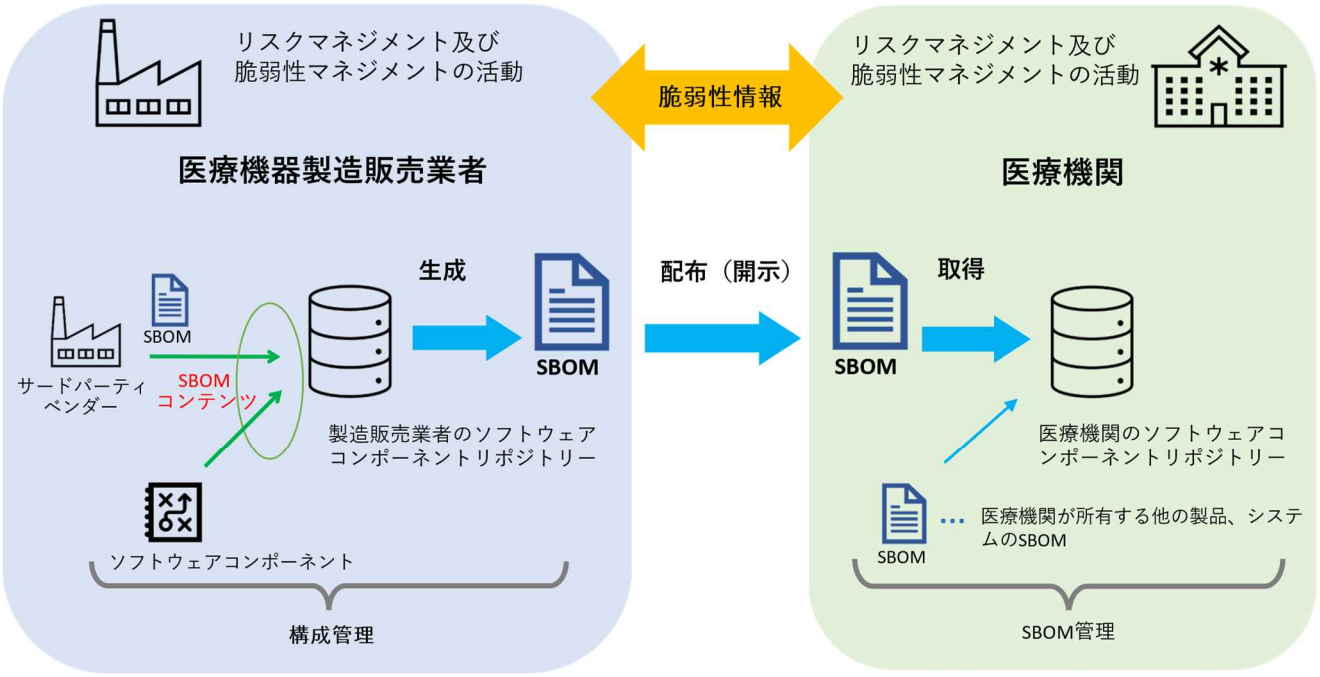

図 4　SBOM の全体的なフレームワーク

A. 2　SBOM の作成

SBOM は、内部の構成管理のために、従来から実施している方式で、ソフトウェア部品の情報が管理できる場合は、継続的に維持していけばよいが、新たに構成管理の方式を検討する場合は、SBOM フォーマットを使用したソフトウェア部品の情報からなる SBOM コンポーネントリポジトリー[注)] を利用して構築してもよい。これらの仕組みによって、医療機器のライフサイクル全体を通して、ソフトウェア

部品の情報が、更新・維持され、SBOM が作成可能であることが重要である。SBOM は、製品リリースの際に顧客に提示される。製造販売業者は、提示した SBOM について、適切な変更管理を実施する。

SBOM 作成及びツールについての追加考察は、NTIA（National Telecommunications and Information Administration、米国商務省 電気通信情報局）の“How to Guide for SBOM Generation（SBOM 作成のハウツーガイド）”にも記載されている。

医療機関においては、入手した各システム・医療機器等の SBOM から医療機関内全体のソフトウェアコンポーネントリポジトリーを構築することによって、システム構成図等とも合わせて医療機関としてのリスクマネジメントのベースを確立することになる。

注） SBOM コンポーネントリポジトリーは、マスターデータベースということもある。IPA はこの場合、後述の SWID 形式を推奨している。

A.3 SBOM の要素と推奨フォーマット

医療機関等に提供される最終的な SBOM は、定義、確立された SBOM 作成の方法論に従うことによって、出力に一貫性があるようにする。SBOM に含まれる情報の量及び種類は変わる可能性があるが、一般的には、利害関係者がリスクを遅滞なくかつ効果的に管理することができるよう SBOM は可能な限り完全なものであることが望ましい。医療機器のサイバーセキュリティについては、SBOM に用いるソフトウェア部品の構成管理情報として、最小限、NTIA に従った以下に示す表 4 の要素を含むことが望ましい。

表 4　SBOM の最小限の要素

要　素	内　　容
ソフトウェアコンポーネントのサプライヤーの名前	コンポーネントの作成、定義又は識別を行うエンティティ
ソフトウェアコンポーネントの名前	サプライヤーが定義してソフトウェアユニットに割り当てた名称
ソフトウェアコンポーネントのバージョン	以前のバージョンからの変更を特定するためにサプライヤーが用いる識別子
固有識別子	コンポーネントを識別するために使用する、又は関連するデータベースのルックアップキーとして機能する識別子
コンポーネントハッシュ	コンポーネントのバイナリーを識別するために用いる暗号化ハッシュ（オプション）

関係	上流のコンポーネント X がソフトウェア Y に含まれているというソフトウェアアーキテクチャー上の関係を特徴づける情報
作成者名	SBOM エントリーの作成者
タイムスタンプ	SBOM データの集約を行った日時の記録

含める基本要素に加えて、製造販売業者は、SBOM フォーマットについても検討することが必要である。現時点では、自動化が可能な標準的な SBOM フォーマットは、限定的である（Cyclone DX、SPDX 及び SWID)。これらのフォーマットについての追加情報並びに医療機器に対する SPDX 及び SWID の詳細例が、NTIA の“How to Guide for SBOM Generation（SBOM 作成のハウツーガイド）”に記載されている。

A. 4　SBOM の提供

製造販売業者は、製品の顧客向けセキュリティ文書のひとつとして、医療機器の使用者に対して SBOM を提供する。既に MDS2 の附属文書として提供されている場合もある。その他、製品又は製造販売業者のウェブサイトに掲載する場合や、電子ファイル又は表示のためのアプリケーションプログラミングインターフェイス（API）として提供する場合がある。また、医療機器に SBOM を内蔵して提供することも可能であろう。SBOM を配布するための最良の方法は一つだけではなく、標準化された、自動検出・交換メカニズムを使用することが望ましい。

医療機器は、頻繁に更新されるので、ネットワーク経由の標準化した方法によって製品及びソフトウェアバージョンを簡単に特定する仕組みで、自動更新をサポートすることが望ましい。

医療機器の SBOM は、覚書等の合意文書、契約、使用許諾等によって、機密情報として分類して扱われることが望ましい。製造販売業者から外部の受信者（規制当局及び医療機関）へのコミュニケーションチャネルは、文書が漏洩し、その結果、サイバーリスクの露出が増えることになる可能性を減らすために、保護手段をサポートする必要がある。

A.5　SBOM の事例

A.5.1 SBOM の構成（アーキテクチャーの展開）

製造販売業者（MDM 1 ）が、図 5 に示す医療機器（Medical Device 2： 3 つのソフトウェアコンポーネント（Windows 10, Adobe Acrobat DC, Java (JRE)）から構成されている）の SBOM を作成する場合を考える。SBOM のフォーマットは特定しないが、表 4 に示す要素を表形式で表すと例えば表 5 のようになる。

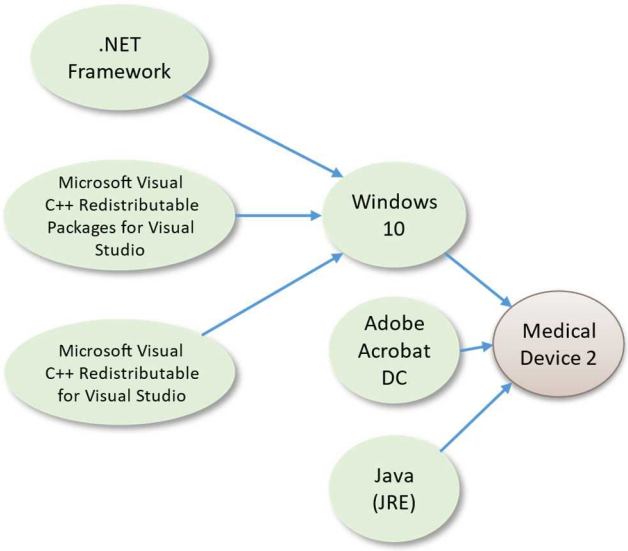

図 5　医療機器（Medical Device 2）のアーキテクチャー（抜粋）

表 5　医療機器（Medical Device 2）の SBOM を表形式で表したイメージ

id	サプライヤーの名前	コンポーネントの名前	コンポーネントのバージョン	固有識別子	ハッシュ	関係	作成者	タイムスタンプ
1	MDM1	Medical Device 2	2.5.9	pkg supplier/MDM1/Medical Device 2@2.5.9	511588e25f217cbf11a766bcb2fddd14	primary	MDM1	2021-08-19T08:14:01Z
2	Microsoft	Windows 10	1903	pkg supplier/Microsoft/Windows 10@1903	45e047fb6499d977f76c309c61a9c752	Included in id#1	Microsoft	2021-01-21T03:14:07Z
3	Microsoft	.NET Framework	4.5.2	pkg supplier/Microsoft/.NET Framework@4.5.2	7c853ca88d4ac7306ccc1867939f7795	Included in id#2	Microsoft	2021-01-13T05:54:00Z
4	Microsoft	Microsoft Visual C++ Redistributable Packages for Visual Studio	2013 update_5	pkg supplier/Microsoft/Microsoft Visual C++ Redistributable Packages for Visual Studio@2013 update_5	0b84c271caf1e918a9a2dcce8b827053	Included in id#2	Microsoft	2015-08-11T05:54:00Z
5	Microsoft	Microsoft Visual C++ Redistributable for Visual Studio	2012 update_5	pkg supplier/Microsoft/Microsoft Visual C++ Redistributable for Visual Studio@2012 update_5	8e23859aaa0bff537016c237a8df1289	Included in id#2	Microsoft	2014-01-14T05:54:00Z
6	Adobe	Adobe Acrobat DC	19.008	pkg supplier/Adobe/Adobe Acrobat DC@19.008	32b39efdfd24fc1c655c4245d51ee722	Included in id#1	MDM1	2021-01-19T03:14:07Z
7	Oracle	Java (JRE)	1.8.0 update_191	pkg supplier/Oracle/Java (JRE)@1.8.0 update_191	58d4ffc200bdf1a60fd2f3903ba18520	Included in id#1	MDM1	2017-12-21T03:14:07Z

注記　id6,7 はサプライヤーから入手した情報ではなく、製造販売業者がツール等によって得た情報に基づいて作成した例である。このため、作成者を MDM1 としている。
この例では、固有識別子として purl（Package URL）を使用している。この他に CPE（Common Platform Enumeration）等を用いる場合もある。

文　　献

1) IMDRF、N60:2020 Principles and Practices for Medical Device Cybersecurity

注記　対応邦訳は、医薬品食品衛生研究所ホームページから入手できる。
https://dmd.nihs.go.jp/cybersecurity/IMDRF_Guidance_Japanese_version.pdf

2) ANSI/NEMA、HN 1-2019 Manufacturer Disclosure Statement for Medical Device Security

3) IEC、IEC TR 80001-2-2:2012 Application of risk management for IT-networks incorporating medical devices - Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and controls

4) 日本規格協会、JIS T 2304:2017 医療機器ソフトウェア－ソフトウェアライフサイクルプロセス
IEC、IEC 62304:2006+A1:2015 Medical device software — Software life cycle processes

5) AAMI、AAMI TIR 57:2016 Principles For Medical Device Security - Risk Management

6) AAMI、AAMI TIR 97:2019, Principles for medical device security — Postmarket risk management for device manufacturers

7) 日本規格協会、JIS Z 8051:2015 安全側面－規格への導入指針
ISO/IEC、ISO/IEC GUIDE 51:2014 Safety aspects — Guidelines for their inclusion in Standards

8) 日本規格協会、JIS T 0063:2020 医療機器における安全側面の開発及び導入の指針
ISO/IEC、ISO/IEC Guide 63:2019 Guide to the development and inclusion of aspects of safety in International Standards for medical devices

9) 日本規格協会、JIS T 14971:2020 医療機器－リスクマネジメントの医療機器への適用
ISO、ISO 14971:2019 Medical devices — Application of risk management to medical devices

10) 日本規格協会、TR T 24971:2020 医療機器－JIS T 14971 適用の指針
ISO、ISO/TR 24971:2020 Medical devices — Guidance on the application of ISO 14971

11) NIST、Cybersecurity Framework 2018

12) NIST、Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF) 2020

13) HSCC/JCWG、MEDICAL DEVICE AND HEALTH IT JOINT SECURITY PLAN 2019
https://healthsectorcouncil.org/the-joint-security-plan/

14) IPA、脆弱性対処に向けた製品開発者向けガイド 2020

15) MITRE、Rubric for Applying CVSS to Medical Devices 2019

16) IPA、脆弱性診断サービス、 https://www.ipa.go.jp/files/000067318.pdf

17) NTIA、How to Guide for SBOM Generation 2021

18) NTIA、Framing Software Component Transparency: Establishing a Common Software Bill of Materials (SBOM) Second Edition 2021

19) NTIA、The Minimum Elements For a Software Bill of Materials (SBOM) 2021

20) IMDRF、N70 Principles and Practices for the Cybersecurity of Legacy Medical Devices

21) IMDRF、N73 Principles and Practices for Software Bill of Materials for Medical Device Cybersecurity

22) JAHIS、22-001 リモートサービスセキュリティガイドライン Ver. 3.1 2022

1

用語及び参考定義（五十音順）

2

五十音順	定義した用語	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
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 （参考情報） **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。	ANSI/NEMA HN 1-2019 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
か	**完全性** データが作成、送信又は保存された後、不正な方法により変更されていない特性	ISO/IEC 29167-19:2016
	可用性 要求するエンティティへのアクセス及び使用の可能性	JIS Q 27000:2019
き	**機密性** 認可されていない個人、エンティティ又はプロセスに対して、情報を開示せず、使用させない特性	JIS Q 27000:2019
	脅威 セキュリティを侵害し、情報資産の機密性、完全性、可用性に対する損害を引き起こす可能性のある状況、能力、行為又は事象がある場合に存在する、セキュリティ違反の可能性	JIS T　81001-1:2022
	脅威モデリング データの破壊、開示、改変又はサービス拒否の形でシステムに損害を与える可能性のある状況又は事象を明らかにするための体系的な調査技法	ISO 24765:2017、modified – replaced “harm” with “damage” JIS T81001-5-1 原案より

五十音順	定義した用語	出典
	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、ベンダー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	
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
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
	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
し	**資産** 個人、組織又は政府にとって価値のある、物理的又はデジタル形式のエンティティ	ISO/IEC JTC 1/SC 41 N0317、 2017-11-12
	情報共有分析機関(Information Sharing and Analysis Organizations：ISAO) 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、使用者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。	
	侵入試験（ペネトレーションテスト） 侵入試験は組織のサーバやネットワークシステムに対して攻撃者が実際に侵入できるかどうかという点に着目して検査を行う。そのため、運用上のシステムに残存している既知の脆弱性を狙ったり、設計段階での不備を突いたりして実施することになる。 IPA　https://www.ipa.go.jp/security/vuln/fuzz_faq.html	
	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、又はその逆）が起こる箇所である境界を表現する脅威モデルの要素 注釈 1：製品の使用者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、生体認証又はデジタル署名）、関連する権限付与（例えば、アクセスコントロールルール）等がある。 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、ソース認証（例えば、メッセージ認証コード及びデジタル署名）及び／又はコンテンツの検証等がある。	JIS T81001-5-1 原案より

五十音順	定義した用語	出典
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 JIS Q 27000:2019
	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（顧客への通知等）を実施する時点。	IMDRF ガイダンス和訳より
は	**補完的リスクコントロール手段（補完的手段）** 機器設計の一部として実施されるリスクコントロール手段の代替として、又はそれが実施されない場合に適用される特定のリスクコントロール手段	AAMI TIR97:2019
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/CC　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	
ふ	**ファジング** 組込み機器やソフトウェア製品のバグや未知の脆弱性を検出する、セキュリティテスト IPA　https://www.ipa.go.jp/security/vuln/fuzz_faq.html	
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

3