IMDRF International Medical Device Regulators Forum

最終文書

IMDRF/CYBER WG/N70FINAL:2023

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

AUTHORING GROUP

IMDRF サイバーセキュリティワーキンググループ

14 November 2023

序文

Andrzej Rys, IMDRF 議長

目次

1. はじめに

「医療機器サイバーセキュリティの原則及び実践（IMDRF/CYBER WG/N60 FINAL:2020、以下“IMDRF N60 ガイダンス”という。）」は、セキュリティの基本原則及び医療機器の製品ライフサイクル全体（TPLC）にわたるベストプラクティスを規定している。ガイダンスを世界的に採用するためには、ガイダンスに含まれる推奨事項をうまく着実に実施することが前提となる。その実施においては、ガイダンスの特定の課題に注目することが重要であり、医療機器サイバーセキュリティのレジリエンスを製品ライフサイクル全体でさらに高めるための自然な流れである。

現代の医療機器の設計は、サイバーセキュリティの考慮事項を改善することで恩恵を受けているが、一方で、サイバーセキュリティを考慮せずに設計された機器が、今日においても数多く使用されており、その中には、製造業者が意図する機器の使用期間を超えているものすらある。それらの機器は、現時点で推奨されるベストプラクティスに従ったかたちではサイバーセキュリティの脅威に対応できておらず、（例えば、パッチ又はアップデートによって）十分に軽減できていないリスクを患者にもたらす可能性がある。それらの機器は、セキュリティコントロールが不十分である、又は存在しない可能性があり、あるいは、開発時点では最新の技術水準のセキュリティコントロールが含まれていたが、ヘルスケア技術の寿命が長いことから、現時点では、そのセキュリティコントロールでは防御できない予期せぬ脅威に直面している可能性がある。そのような機器は、通常、“レガシー医療機器”と呼ばれ、多くの場合、製品ライフサイクル全体を通してサイバーセキュリティを維持するために様々な手段を必要とする。ただし、老朽化の理由のみでその製品がレガシーであるかどうかを判断してはならないことも重要である。比較的新しい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、発売以降の年数にかかわらず、サイバーセキュリティの状況においてはレガシーであるとみなされる。製品ライフサイクル全体の計画を適切に実行するためのスタッフやリソースが足りない組織（これは、珍しいことではないが）においては、レガシー機器及び関連するリスクがいつまでも残る可能性がある。

ヘルスケアを提供するために、今も依然としてレガシー医療機器が用いられているので、それによって患者安全に対する重大な脅威が生み出されかねない。こうした背景の中、このガイダンス文書の意図は、IMDRF N60 ガイダンスに示されたレガシー機器の概念的フレームワークを運用可能なものにすることであり、医療機器製造業者（MDM）、ヘルスケアプロバイダー（HCP）などの利害関係者に対して、詳細な推奨事項を提供している。このガイダンスで述べる HCP には、医療機関が含まれる。

このガイダンス文書は、潜在的なレガシー機器を特定するための明確な方法及びレガシー医療機器のサイバーセキュリティを維持するための実用的かつ実行可能なアプローチを提供することを意図している。地域の規制システムに影響することなく実施するための様々な選択肢を利害関係者に提供することを意図しており、この作業は、IMDRF N60 ガイダンスを補完することを意図したものである。

レガシーのサイバーセキュリティのリスクマネジメントに関連する追加推奨事項としては、米国ヘルスケア及び公衆衛生分野協調協議会（HSCC, Health and Public Health Sector Coordinating Council）の“健康産業のサイバーセキュリティーレガシー技術のセキュリティ管理（HIC-MaLTS）”を参照。

2. 適用範囲

この文書は、IMDRF N60 ガイダンスで示したフレームワークの実装を支援するために、製品ライフサイクル全体をレガシー機器に対してどのように適用するかについての具体的な推奨事項を提供することを目的に作成した。この文書は、IMDRF N60 ガイダンスを補完するものであり、医療機器［体外診断用（IVD）医療機器を含む］を適用範囲とし、患者危害の可能性に焦点をおくことに変わりはない。

この文書では、ファームウェア及びプログラマブルロジックコントローラー等のソフトウェアを含むレガシー医療機器（例：ペースメーカー、輸液ポンプ）、又はソフトウェア単独で存在するレガシー医療機器［例：プログラム医療機器（SaMD）］に関するサイバーセキュリティについて検討している。ほとんどの規制当局は、その権限が医療機器の安全性及び性能に限定されているため、この文書の適用範囲は、患者への危害が発生する可能性に関する検討に限定されていることに留意する必要がある。例えば、医療機器の性能に影響を与える、臨床活動に悪影響を及ぼす、又は誤った診断若しくは治療に繋がるような脅威は、この文書の適用範囲とみなされる。データプライバシーの侵害等、その他の危害も重要であるが、この文書では適用範囲から除外する。

レガシー機器は、すでに IMDRF N60 ガイダンスにおいて、現在のサイバーセキュリティの脅威に対して合理的に保護できない医療機器と定義されている。したがって、この文書では、サイバーセキュリティの文脈におけるレガシー機器だけを扱い、機器が“レガシー”であるとみなされる可能性のあるその他の全ての状況（例えば、古い型式の医療機器）を取り扱うものではない。

このレガシーの定義を考慮すると、現在使用されている多くの機器は、レガシー機器とみなされる可能性がある。こうした現状から、将来の、より理想的な状況へと移行するために、IMDRF N60 ガイダンスは、レガシー機器の TPLC フレームワークを提案しており、この文書において更に詳しく説明されている。このフレームワークの主要な特性は、MDM と HCP との間で効果的にコミュニケーションを行うことであり、タイムリーで計画的な機器の導入及び使用停止を行うことで、継続使用されるレガシー機器の数を最小限に抑えることである。このガイダンスの適用範囲を超えるが、MDM 及び HCP は、関連する場合には、患者に対してもライフサイクル段階の情報を伝えることが望ましい。（例えば、再ラベリングを行う）再販業者についても、多くの場合は MDM と同じ規制義務をもたないので、同様にこのガイダンスの適用範囲外である。

この文書は、特に次を意図している。

- レガシー医療機器のサイバーセキュリティを、TPLC フレームワーク（開発、サポート、限定的サポート及びサポート終了）の文脈において、各段階における MDM 及び HCP の責任を明示して説明する。
- MDM 及び HCP に対して、コミュニケーション（脆弱性マネジメントを含む）、リスクマネジメント及び HCP への責任移転の推奨事項を提供する。
- サポート終了後の補完的コントロールについての推奨事項を提供する。
- MDM 及び HCP に対して、TPLC フレームワーク以前に開発され、現在も使用されている既存のレガシー機器に対応するための考慮事項を提供する。

前回発行した IMDRF N60 ガイダンスで強調されているように、サイバーセキュリティは、全ての利害関係者（MDM、販売業者、HCP、ユーザー、規制当局及びソフトウェアベンダーを含むが、それには限定しない）の共同責任であることを、この文書では引き続き認識している。

なお、医療機器の種類や各国の規制に応じて、追加の検討事項が必要となり得ることに留意する必要がある。

3. 定義

この文書では、IMDRF/GRRP WG/N47 FINAL:2018 及び IMDRF/CYBER WG/N60 FINAL:2020 で定められている用語及び定義、並びに次を適用する。

3.1 **アプリケーションソフトウェア**（*Application software*）：1. コンピューター自体を制御するソフトウェアとは異なるものとして、ユーザーが特定のタスクを実行する又は特定の種類の問題に対処するのを助けるように設計されたソフトウェア、2. 適用する問題の解決に特化したソフトウェア又はプログラム（ISO/IEC 2382:2015）

3.2 **資産**（*Asset*）：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のエンティティ（ISO/IEC JTC1 1/SC41 N0317, 2017-11-12）

3.3 **可用性**（*Availability*）：認可されたエンティティが要求したときに、アクセスおよび使用が可能である特性（ISO/IEC 27000:2018）

3.4 **補完的リスクコントロール手段**（**補完的コントロール**）［*Compensating Risk Control Measure*（*Compensating Control*）］：医療機器の設計の一部として実装されるリスクコントロール手段の代わりに又はそれがない場合に適用される、特定のタイプのリスクコントロール手段（AAMI TIR97:2019）

注記：補完的リスクコントロール手段は、永続的でも一時的（例えば、製造業者が追加のリスクコントロール手段を組み込んだアップデートを提供できるまでの間）でもありうる。

3.5 **コンポーネント**（*Component*）：システムの物理的又は論理的な一部分を構成し、特定の機能及びインターフェイスをもち、（例えば、ポリシー又は仕様によって）システムの他の部分から独立して存在していると扱われる、システムのリソースの集まり（ISO 81001-1:2021）

注記：医療機器の文脈において、コンポーネントは、完成され、梱包され、ラベリングされた機器の部分として含めることを意図する、原材料、物質、小片、部品、ソフトウェア、ファームウェア、ラベリング又は組立部品を含む。

3.6 **機密性**（*Confidentiality*）：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、情報を使用させず、また、開示しない特性（ISO/IEC 27000:2018）

3.7 **構成**（*Configuration*）：情報処理システムのハードウェア及びソフトウェアの編成及び相互接続の仕方（ISO/IEC 2382:2015）

3.8 **構成管理**（*Configuration management*）：構成を管理及び制御するための協調的な活動（ISO/IEC TR 18018:2010）

3.9 **協調的な脆弱性の開示**（*Coordinated Vulnerability Disclosure*、*CVD*）：研究者及びその他の関係者が、脆弱性の開示に関連するリスクを低減する解決策を見つけるために製造業者と協力して行うプロセス（AAMI TIR97:2019）

注記：このプロセスには、脆弱性及びその解決策に関する情報の報告、調整、公開などの作業が含まれる。

3.10 **サイバーセキュリティ**（*Cybersecurity*）：情報及びシステムが不正な活動（アクセス、使用、開示、中断、変更、破壊など）から保護されており、機密性、完全性及び可用性の侵害に関連するリスクがライフサイクル全体を通して受容可能なレベルに維持されている状態（ISO 81001-1:2021）

3.11 **使用停止**（*Decommission*）：運用中の業務から取り除くこと（ASTM E3173-18）

3.12 **デプロイ**（*Deployment*）：システムの運用を開始し、カットオーバーの問題を解決するプロジェクトの段階（ISO/IEC/IEEE 24765:2010）

3.13 **製品寿命終了**、**EOL**（*End of Life*）：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、製品に対してユーザーへの通知を含む正式な EOL プロセスを実施する時から始まる、製品のライフサイクルの時点

注記：製品寿命終了の時点は、TPLC の限定的サポート段階の開始時点である。

3.14 **サポート終了**、**EOS**（*End of Support*）：製造業者が全てのサポート活動を中止し、これ以上はサービスサポートが延長されない時から始まる、製品のライフサイクルの時点

注記：サポート終了の時点は、TPLC のサポート終了段階の開始時点である。

3.15 **基本性能**（*Essential Performance*）：基礎安全に関連する以外の臨床機能の性能において、製造業者の指定した限界を超えた低下又は欠如が生じたときに受容できないリスクを生じる性能（IEC 60601-1:2005+AMD1:2012）

注記：基本性能を維持するために、保守、修理又はアップグレード（例えば、安全又はサイバーセキュリティに関連する変更）が必要な場合がある。

3.16 **エクスプロイト**（*Exploit*）：脆弱性を通して情報システムのセキュリティを侵害するための確立した方法（ISO/IEC 27039:2015）

3.17 **ファームウェア**（*Firmware*）：主記憶装置とは機能的に独立した方法で、通常、読み出し専用メモリー（ROM）に保存される、順序付けられた一連の命令及び関連するデータ（ISO/IEC 2382:2015）

3.18 **完全性**（*Integrity*）：データが作成、送信又は保存された後、不正な方法によって変更されていない特性（ISO/IEC 29167-19:2016）

3.19 **レガシー医療機器**（**レガシー機器**）［*Legacy Medical Device*（*Legacy Device*）］：現在のサイバーセキュリティの脅威に対して合理的に保護できない医療機器

3.20 **ライフサイクル**（*Life cycle*）：製品又はシステムの初期構想から最終的な使用停止及び廃棄に至るまでの一連の全ての段階（ISO 81001-1:2021）

3.21 **患者危害**（*Patient Harm*）：患者の受ける身体的傷害又は健康障害（ISO/IEC Guide 51:2014 を一部変更）

3.22 **患者安全**（*Patient Safety*）：患者の健康に対する受容できないリスクがないこと（ISO/IEC Guide 51:2014 を一部変更）

3.23 **プライバシー**（*Privacy*）：個人に関するデータの過度の又は違法な収集及び使用に起因する、私生活又は個人的事柄に対する侵入がないこと（ISO/TS 27799:2009）

3.24 **製品**（*Product*）：組織と顧客との間の処理・行為なしに生み出され得る、組織のアウトプット（ISO 81001-1:2021）

3.25 **レジリエンス**（*Resilience*）：機能ユニットが、故障又はエラーが存在する際に要求される機能を継続して実行する能力（ISO/IEC 2382:2015）

3.26 **リスクマネジメント**（*Risk management*）：リスクの分析、評価、コントロール及び監視に対する、マネジメント方針、手順及び実施の体系的な適用（ISO/IEC Guide 63:2019）

3.27 **リスク移転**（*Risk transfer*）：リスク要因をより軽減可能な別の組織又は機能エンティティに対する、リスク要因の管理責任の移転（ISO/IEC/IEEE 24765:2017）

3.28 **セキュリティポリシー**（*Security Policy*）：1. 各プロジェクト組織のレベルで知っておくべき情報アクセスのルール、2. 一つ以上の対象の一つ以上の活動を制限する一連のルール（ISO/IEC 10746-3:2009）

3.29 **セキュリティ試験**（*Security testing*）：試験項目並びに関連するデータ及び情報が保護されており、認可されていない人又はシステムが、使用、読出し又は変更ができず、認可された人又はシステムがアクセスを拒否されないという程度を評価するために実施する試験の種類（ISO/IEC/IEEE 29119-1:2013）

3.30 **ソフトウェア部品表**、**SBOM**（*Software Bill of Materials*）：一つ又は複数の識別したコンポーネント、それらの関係及びその他の関連する情報のリスト

注記：依存関係のない単一のコンポーネントの SBOM は、そのコンポーネント一つだけのリストである。“ソフトウェア”は、“ソフトウェアシステム”と解釈できるため、ハードウェア（ファームウェアではない真のハードウェア）及び（CPU マイクロコードのような）非常に低レベ

ルのソフトウェアを含むことが可能である。（NTIA Framing Software Component Transparency: Establishing a Common Software Bill of Material (SBOM) 2021-10-21)

3.31 **ソフトウェアコンポーネント**（*Software component*）：ソフトウェアシステム又はモジュール、ユニット、データ、文書などの要素を参照するために用いる一般的な用語（IEEE 1061）

注記：一つのソフトウェアコンポーネントは、複数のユニット又は複数のより低レベルなソフトウェアコンポーネントを含む可能性がある。

3.32 **サードパーティのソフトウェア**（*Third party software*）：関係者から独立していると認識される人又は団体から提供されるソフトウェア（ISO/IEC 25051:2014 を一部変更）

注記：関係者は、通常、供給者（“ファーストパーティ”）及び購入者（“セカンドパーティ”）の利害関係者である。

3.33 **脅威**（*Threat*）：セキュリティを侵害し、危害を引き起こし得る状況、能力、行動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（ISO/IEC Guide 120）

3.34 **脅威モデリング**（*Threat Modeling*）：データの破壊、漏洩、改ざん又はサービス拒否の形でシステムに危害を及ぼす可能性のある状況又は事象を明らかにするための調査プロセス（ISO/IEC/IEEE 24765-2017 から変更）

3.35 **製品ライフサイクル全体**、**TPLC**（*Total Product Life Cycle*）：医療機器のライフサイクルの、開発、サポート、限定的サポート及びサポート終了の段階
注記：国・地域によっては、各段階を別の言葉で参照することがある。

3.36 **アップデート**（*Update*）：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

注記 1：ISO/IEC 14764:2006 に規定するソフトウェア保守活動に由来する。
注記 2：アップデートには、パッチ及び設定変更が含まれることがある。
注記 3：適応及び完全化に関する変更は、ソフトウェアの改良である。その変更は、医療機器の設計仕様になかったものである。

3.37 **アップグレード**（*Upgrade*）：機器又は機器のコンポーネントを、より新しい若しくはより良いバージョンに、又は追加機能のものに置き換えること

3.38 **脆弱性**（*Vulnerability*）：一つ以上の脅威によって付け込まれる可能性のある、資産又は管理策の弱点（ISO/IEC 27000:2018）

3.39 **脆弱性マネジメント**（*Vulnerability management*）：ソフトウェアの脆弱性を特定し、分類し、優先順位をつけ、修正し、軽減することを繰り返し行うこと

4. 一般原則

このセクションでは、全ての利害関係者が医療機器の開発、規制、使用及び監視の際に考慮する、レガシー機器の一般原則を示す。一般原則については、この文書全体に記載しているが、レガシー機器を含む世界中のヘルスシステムに対するサイバーセキュリティ態勢を改善するための基礎となるものである。

4.1. 製品ライフサイクル全体のフレームワーク

サイバーセキュリティの脅威及び脆弱性に関連するリスクは、開発段階から EOS 段階に至る、医療機器の製品寿命の全ての段階において考慮することが望ましい。HCP が EOS を超えて機器を継続使用することを決定した場合、使用停止が EOS のしばらく後に行われることになり、臨床的な寿命は、実際には EOS を超える可能性があることが知られている。多くの場合、機器の臨床的有用性は、サポート可能な期間よりも長いことが知られている。医療機器のライフサイクルは、サイバーセキュリティについて計画されているべきであると、全ての利害関係者が認識することが望ましい。計画すべきライフサイクルには、開発段階、サポート段階、限定的サポート段階及び EOS 段階が含まれる。

限定的サポートは、サポート終了又は製品のアップグレード若しくは置換えに向けての最終的な移行に対して、MDM 及び HCP が協調して準備する移行期間である。EOS は、サイバーセキュリティの責任が主として HCP に移転するとみなされる時点である。EOS の後も、地域の規制によっては、MDM は、ある種の市販後活動に対して、引き続き責任を有する可能性がある（詳細については、7.2.1 の 3 を参照）。MDM 及び HCP がライフサイクルのそれぞれの段階に対して適切に準備できるようにするために、医療機器の EOS までの間には、コミュニケーション、リスクマネジメント及び責任移転に関連する数多くの活動がある。

4.2. コミュニケーション

脅威に対して効果的に保護するためには、利害関係者間のオープンで透明性のあるコミュニケーションが必要である。MDM は、EOL 及び EOS に対して計画することが期待される。MDM は、EOS 及び EOL の予定時期について、なるべく早く伝えるように努力することが望ましく、場合によっては機器の調達及び据付の一部として伝達することが望まれている。早期に認識することによって、ユーザーは、MDM から情報を得て、機器の保守に関する次のステップに取り込むことで、EOL 及び EOS に対して適切に計画することが可能になる。HCP は、この情報を用いて、その機器を使用停止するか、セキュリティを維持する責任を追加で引き受けるかのいずれかを行うことになる。

この文書全体を通して、MDM 又は HCP の双方からのコミュニケーションについての推奨事項は、これらの当事者間又は他の利害関係者に対して積極的に手を伸ばす及び／又は関与を伴うものであることを理解することが望ましい。“提供する”又は“コミュニケーションする”情報は、他の当事者に対して積極的に送信することが望ましい。また、そうした情報が検索可能であることを、他の当事者に積極的に認識させることが望ましい。積極的な通知を伴わず、情報が受動的にしか入手できないようなコミュニケーションのポリシー及び手順は、推奨されず、可能な限り避けることが望ましい。

4.3. 共同のリスクマネジメント

医療機器のサイバーセキュリティは、利害関係者間、特に MDM と HCP との間の共同責任である。この共同責任は、レガシー機器の場合、特に重要である。

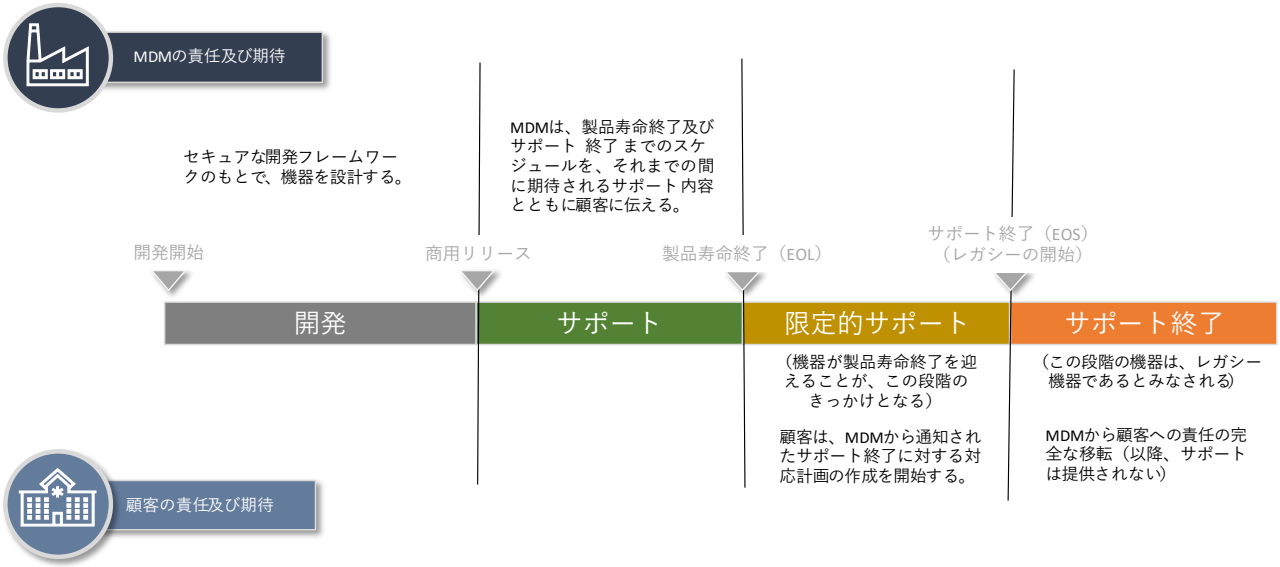
レガシー機器のリスクを適切に管理するためには、MDM は、サポート段階のサイバーセキュリティを最適化し、将来の EOS 後のセキュリティリスクを最小化するように、機器を設計することが望ましい。MDM は、この文書のセクション 7〜9 に記載するように機器をサポートすることが望ましい。HCP は、MDM と積極的に関わって SBOM を入手することが望ましく、MDM が推奨する適切なサイバーセキュリティの保護手段（IT インフラストラクチャーに関連するものも含む）を確実に行って機器を運用し、サイバーセキュリティの保護手段が確実に維持され、EOS 期日に対して確実に計画することが望ましい。MDM のサポートが受けられなくなった機器は、現在及び将来の脅威に対して脆弱になる可能性があり、HCP は、それらの機器を MDM がサポートするモデルにアップグレードすることを検討することが望ましい。SBOM に関する追加情報については、IMDRF/CYBER WG/N73 文書を参照のこと。

5. 医療機器サイバーセキュリティに対する IMDRF の TPLC フレームワークの概要

サイバーセキュリティのリスクの動的な性質を効果的に管理するためには、リスクマネジメントを製品ライフサイクル全体に渡って適用することが望ましい。サイバーセキュリティのリスクは、設計、製造、試験及び市販後監視等の製品ライフサイクル全体の様々な部分において、評価し、軽減する。安全とセキュリティとのバランスをとる必要があることも認識されている。サイバーセキュリティのコントロール及び軽減策を組み込む際には、MDM が医療機器の安全及び基本性能を確実に維持することが極めて重要である。

IMDRF N60 ガイダンスでは、レガシー医療機器のサイバーセキュリティについて、製品ライフサイクル全体の四つの段階（開発、サポート、限定的サポート及び EOS）の状況で説明している（図 1）。地域の規制によっては、各段階を別の用語で呼んでいるかもしれない。しかし、各段階で説明している概念は、一般的に適用可能であるはずである。また、製品ライフサイクル全体の段階が、それぞれ異なる長さの期間であるかもしれない（例えば、サポート段階は、限定的サポート段階よりも長いかもしれない）ことにも注意されたい。

サイバーセキュリティと製品ライフサイクル全体



*医療機器製造業者（MDM）は、医療機器の責任に関する各地域のガイダンスに従う。サポートレベルは、顧客との契約に応じて異なる可能性がある。

注記：この図の“顧客”という用語は、この文書における“HCP”の意味であると理解することが望ましい。

図 1：サイバーセキュリティの製品全ライフサイクルにおけるレガシー機器の概念フレームワークの概要

5.1. 開発段階（ステージ 1）

開発段階（ステージ 1）は、MDM が設計によってセキュリティを組み込むことが期待される市販前の段階である。MDM は、リスクアセスメントを行い、脅威を特定し、セキュリティ試験を実施し、リスクを軽減して、機器がライフサイクルの全体を通して安全で有効に動作できることを確実にすることが望ましい。この他、開発段階の成果としては、ユーザーのセキュアな機器運用をサポートするための製品関連の一連のセキュリティ文書がある。製品開発のベストプラクティスについては、この文書の適用範囲外である。制定された規格、基準には、次があるが、これには限定されない可能性がある。

- IEC 62443-4-1（製品ライフサイクル）
- IEC 62443-3-2（セキュリティリスクアセスメント）
- NIST 800-12
- NIST のセキュアなソフトウェア開発フレームワーク
- IEC 81001-5-1: 2021
- IEC TR 60601-1-4-5:2021
- IEC TR 80001-2-8:2016
- IEC 62443-4-2:2019

その他の規格については、IMDRF/CYBER WG/N60 ガイダンスも参照のこと。

5.2. サポート段階（ステージ 2）

サポート段階（ステージ 2）の機器は、次の全てを満たす医療機器であると定義される。

1. 患者ケアを提供するために用いられている。
2. 市場で入手可能である。
3. 機器の主要部分を担うソフトウェア、ファームウェア又はプログラマブルなハードウェアコンポーネント（例えば、CPU）を含み、全てがサプライヤーによってサポートされている[1]。

ステージ 2 の機器は、ソフトウェアパッチ、ソフトウェア及びハードウェアのアップデート、適切と思われるサポートなどの、サイバーセキュリティのフルサポートを受けることが望ましい。

このカテゴリーの機器は、市場においては“新しい”又は“最新の技術水準”であるとみなされているかもしれないが、その設計に組み込まれているセキュリティ機能は、様々である可能性がある。製品の設計にセキュリティのベストプラクティスが組み込まれていればいるほど、MDM は、この文書で概説しているサポート方法を容易に実行することが可能である。

---

[1] あるソフトウェアコンポーネントが、ステージ 2 の間に、予想外に EOL や EOS を宣言された場合は、MDM は、ステージの進行が思ったよりも早期に起こることを防ぐために、サポートされているバージョン又はサポートされている代替コンポーネントに機器をアップデートすることが望ましい。ライフサイクル管理のこの側面に関する更なる情報については、5.5 を参照。

この段階で確立されている主要な実践の一つは、脆弱性を特定し、協調的な脆弱性の開示（CVD）プロセスを通して通知することである。サポート契約によっては、MDM は、追加のサービス（例えば、セキュリティ監視、バックアップ・復旧など）を提供して、セキュリティをサポートする可能性もある。

ステージ 2 の実践の全てが、レガシーが進行するこの後の段階に、引き継がれるとは限らない。

5.3. 限定的サポート段階（ステージ 3）

限定的サポート段階（ステージ 3）にある機器は、次のような医療機器であると定義される。

1. 患者ケアを提供するために使用されており、
2. MDM がすでに EOL を宣言しており、現時点では、MDM から販売されていない、又は、
3. 含まれているソフトウェア、ファームウェア又はプログラマブルなハードウェアコンポーネント（例えば、CPU）が、a) 開発者によってサポートされていないが、b) それらの安全及び有効性に対するリスクは軽減されており、結果として現在のサイバーセキュリティの脅威に対して合理的に保護されている可能性がある。

ステージ 3 においては、機器の MDM は、可能な場合はサイバーセキュリティのサポート提供を継続することが望ましい。例えば、MDM が自社のソフトウェアに対するアップデートやパッチを開発できなくても、サードパーティのコンポーネント又はソフトウェアに対するパッチについては可能な限り継続して適用する。

このカテゴリーの機器は、その設計に組み込まれているセキュリティ機能が様々である可能性がある。製品の設計にセキュリティのベストプラクティスが組み込まれていればいるほど、MDM は、サポート段階で概説しているサポート方法を容易に実行することが可能である。

MDM は、制限の影響を受ける機器及びサービス、軽減されていないように見える可能性がある脅威、並びに、HCP が実施する必要があるセキュリティ保護の要素について、ユーザーに対してコミュニケーションすることが望ましい。

ステージ 3 の機器は、ステージ 2 の機器に比べて、ネットワークコントロールなどの追加で行う補完的コントロールを要求されることが多い。ステージ 3 においては、MDM 及びプロバイダーは、ステージ 2 の実践のうち合理的に実現可能なもの全てについて、引き続き従うことが望ましい。

5.4. EOS 段階（ステージ 4）

EOS 段階（ステージ 4）にある機器は、次のような医療機器であると定義される。

1. 患者ケアを提供するために使用されており、
2. MDM がすでに EOL を宣言しており、現時点では、MDM から販売されていない、又は、
3. 含まれているソフトウェア、ファームウェア又はプログラマブルなハードウェアコンポーネント（例えば、CPU）が、a) 開発者によってサポートされていない、かつ、b) それらの安全及び有効性に対するリスクは軽減されてないために、結果として現在のサイバーセキュリティの脅威に対して合理的に保護することができていない。

MDM は、ステージ 4 に入る前に、これ以上は機器のサポートを保証できないことをユーザーに伝えることが望ましい。このとき、ユーザーが承継する可能性がある潜在的リスクを伝え、軽減戦略及びアップグレードの機会についても伝えることが望ましい。

全ての医療機器は、いつかは EOS に到達する。サイバーセキュリティの EOS を超えて機器をセキュアに使うことは、運用環境のセキュリティ機能に大きく依存するので、そのような事態に備えることは、MDM と顧客との間の共同責任である。

5.5. 別のライフサイクル段階への移行のきっかけとなるリスクを評価するためのフレームワーク

医療機器及びそのソフトウェア、並びにそれらを構築する他のデジタルコンポーネントは、時間がたてば EOL や EOS に至る。この EOL や EOS の期日は、通常同期しない。サードパーティのソフトウェアコンポーネントは、機器が販売される際に、故意にサポート期間を短くされたり、MDM がアナウンスした EOS 期日よりも前に突然サポート終了が宣言されたりする可能性がある。サードパーティのソフトウェアコンポーネントのサポートが事前にわかる場合は、MDM は、機器の設計において、コンポーネントが限定的サポートや EOS に移行することに由来するリスクに対応するための適切な計画を作成することが望ましい。コンポーネントに対して、突然、異なったタイミングで起こるコンポーネントの EOL や EOS の宣言及び状態に起因するリスクを管理するためには、MDM は、別のライフサイクル段階への移行のきっかけとなる可能性のあるリスクを評価するために、次のフレームワークを活用してもよい。

1. 機器の一つのコンポーネントが EOL や EOS になる場合には、これがきっかけとなって、MDM がリスクアセスメントを行い、患者安全のリスクが生じるかどうか、生じる場合はどんなリスクかを判断することになる。
    a. 患者安全への影響がない場合は、機器は、現在のライフサイクル段階（すなわち、サポート段階又は限定的サポート段階）にとどまり、コンポーネントが EOL 又は EOS になったことをユーザーに通知する。
2. 患者安全への影響があり、機器がサポート段階にある場合には、MDM は、サポートされないコンポーネントのリスクを、アップデートやその他の設計変更によって軽減しようとすることが望ましい。サポート段階中は、サポートされないコンポーネントの機能を、サポートされる代替コンポーネント又はその他の設計変更のいずれかによって置き換えて、計画した EOS に到達するまで機器の意図する使用を安全に維持できるようにすることが、アップデートや設計変更の目標になるだろう。MDM のリスクアセスメントは、より広い分野から得られる関連する全ての脅威の情報とあわせて、この時点で段階を移行するかどうかの意思決定に反映させることが望ましい。
    a. サポートされないコンポーネントを使用せずにリスクが軽減され、機器が合理的に保護される可能性がある場合には、機器はサポート段階にとどまってよい。
    b. リスクが軽減されて機器が合理的に保護される可能性があるが、軽減策にサポートされないコンポーネントが含まれている場合は、MDM は、機器を限定的サポート段階に移行することが望ましい。サポートされないコンポーネントを活用する軽減策を使用することは、ベストプラクティスであるとはみなされず、最後の手段とすることが望ましい。MDM は、この移行を公表し、移行を容易にするためにより詳細なセキュリティ文書を提供することが期待される（このコミュニケーションに関する追加事項については、8.1.1.5 を参照）。

3. 患者安全への影響があり、機器が限定的サポート段階にある場合は、MDM は、サポートされないコンポーネントのリスクを（例えば、設計変更や補完的コントロールによって）軽減しようとすることが望ましい。MDM のリスクアセスメントは、より広いヘルスケア分野から得られる関連する全ての脅威の情報とあわせて、この時点で TPLC の段階を移行するかどうかの意思決定に反映させることが望ましい。

    a. リスクが軽減され機器が合理的に保護される可能性がある場合は、機器は、限定的サポート段階にとどまり、コンポーネントが EOL や EOS になったことをユーザーに通知する。

    b. リスクに対して合理的に保護できない場合は、機器は EOS 段階に移行することが望ましく、MDM は、この移行を公表することが期待される（このコミュニケーションに関する追加事項については、9.1.1.2 を参照）。

上記のフレームワークは、サードパーティのコンポーネントが突然 EOL や EOS を宣言されることを意図したものである。一般的に、機器の保守に対して提供されるソフトウェアのサポートレベルは、機器の保守計画に詳しく述べられている。ソフトウェアコンポーネントの EOS 期日は、TPLC 全体の医療機器リスクマネジメントを助けるために、SBOM にも含まれている可能性がある。

機器を EOL、EOS 後に継続して運用する際のリスクのバランスをとる方法についての追加情報は、HSCC HIC-MaLTS の責任移転のフレームワークを参照。

6. 開発段階の責任及び期待

このセクションでは、ライフサイクルの開発段階における利害関係者の責任を、コミュニケーション、リスクマネジメント及び責任移転について詳細に示す

6.1. コミュニケーション

レガシー機器に関する最も重要で認識すべき課題の一つは、情報の欠落である。情報の欠落は、例えば、機器のセキュリティコントロール、ソフトウェアサプライチェーン、サポート状態などの、機器の技術的特徴に関連する可能性がある。また、例えば、（MDM 及び HCP の双方の）組織内のどの部門が保守の継続に責任があるか、いつ誰にどのようにセキュリティ状態についての情報をコミュニケーションするかなどの、組織的課題にも関連することがある。結果として、MDM、HCP 及び他の関係者間のレガシー機器に関するコミュニケーションは、極めて重要である。このニーズに対応するため、組織は、機器のライフサイクルの複数の段階におけるレガシーのコミュニケーション戦略を確立し、実施することが望ましい。

6.1.1. MDM の推奨事項

ライフサイクルの様々な段階における HCP からのフィードバックは、今後の機器及び機器のアップグレードにおける MDM の設計に反映される可能性がある。この文書の開発段階以降の製品ライフサイクル段階に対するコミュニケーションのセクションには、HCP が医療機器を調達し、デプロイした後に生じる検討事項に対応するための推奨事項が記載されている。

6.1.2. ヘルスケアプロバイダーの推奨事項

HCP は、MDM の機器開発にインプットする、臨床及びサイバーセキュリティに対する HCP のニーズ及び期待事項について、この製品ライフサイクル段階においてフィードバックする可能性がある。

6.2. リスクマネジメント

6.2.1. MDM の推奨事項

1. **セキュリティコントロールのベースライン**：MDM は、セキュリティを組み込み、機器のライフサイクル全体を通じて維持できるように製品を設計することが望ましい。これは、セキュアな開発フレームワークを使用することで達成される可能性がある。管理が必要な領域及び具体的な推奨事項には、次のようなものがある。
    a. 医療機器の意図する使用に基づくセキュリティ設計及びコントロール、並びに次の事項。
        i. セキュリティリスクアセスメント
        ii. 脅威モデリング
        iii. セキュリティ試験

iv. 顧客向けの製品セキュリティ文書及びコミュニケーション

b. サイバーセキュリティの脆弱性に関する市販後監視の機能。例えば、次の事項。

i. 脆弱性の特定

ii. 機器のセキュリティ設計、コントロール及び軽減策に基づく脆弱性リスクの特定

c. セキュリティパッチ及び軽減策の入手可能性を、機器のリスクに基づいて、例えば、次を通じて確実にする。

i. 脆弱性及び対応する軽減策に関して、その影響を受ける全てのユーザーに対する協調的で明確なコミュニケーション

ii. セキュリティパッチが入手可能でない場合、その他の軽減策の選択肢の特定

2. **サードパーティのコンポーネントに対する考慮事項**：MDM は、コンポーネントに対するサードパーティベンダーのサポートが、HCP が予測する機器の使用期間内に終了する可能性があり、それによって、MDM が機器のセキュアな運用をサポートする能力が悪影響を受ける可能性があることを考慮することが望ましい。

6.2.2. ヘルスケアプロバイダーの推奨事項

HCP が調達プロセスを開始していないため、リスクマネジメントの推奨事項は、この時点ではまだ適用できない。

6.3. 責任移転

この段階では、MDM が HCP に機器を提供していないため、責任移転の推奨事項は、ない。知識及びサポート移転は、調達のための話合いの間に開始される。

7. サポート段階の責任及び期待

このセクションでは、ライフサイクルのサポート段階における利害関係者の責任を、コミュニケーション、リスクマネジメント及び責任移転について詳細に示す。

7.1. コミュニケーション

このセクションでは、機器のサポート段階の間、セキュアな運用を確実に継続するために、HCP と MDM との間でのやりとりが望ましい様々な種類のコミュニケーションに対する推奨事項を提供する。特に、サポート段階でのコミュニケーションが包括的であることが極めて重要である。サポート段階に入るとき、組織は、どのような文書や情報が必要か、また、どのようなタイミングで必要になるかを特定することが望ましい。そして、これらの要求事項を相手に伝え、合意を得ることが望ましい。具体的な文書化のニーズは、組織によって異なるかもしれないが、以下のセクションでは一般的な推奨事項を示す。医療機器のセキュリティ機能の有無に関するコミュニケーション戦略の一つの可能性については、IEC TR 60601-4-5 に記載されている。

7.1.1. MDM の推奨事項

1. **製品セキュリティ文書の提供**：MDM は、サポート段階の初期から全体を通して製品のセキュリティ文書を提供し、医療機器の調達からデプロイまでの間において、HCP がリスクマネジメントを行えるようにする。次のような文書が適切であると思われる。
    a. 医療機器セキュリティのための製造業者開示説明書（MDS2）
    b. ソフトウェア部品表（SBOM）（SBOM のベストプラクティスについての詳細は、IMDRF N73 文書を参照。）
    c. セキュリティ試験報告書サマリー、セキュリティの第三者認証又はこれらに類するもの
    d. 顧客向けセキュリティ文書（例えば、デプロイ、運用及びサービス提供のセキュリティを確実にするための技術解説。これには、インターフェイス、通信プロトコル及びネットワーク、クラウド又はシステムの通信依存性に関する情報を含む。）
2. **製品ライフサイクル文書の提供**：MDM は、主要なライフサイクルのマイルストーンについて、調達及び据付のプロセスの一環として、明確にコミュニケーションすることが望ましい。これには、（可能な場合）機器のサイバーセキュリティの EOL 及び EOS 期日を含める。MDM は、この情報を可能な限り前倒しで提供することが望ましい。現時点では、HCP をサポートするためには、少なくとも 2 年以上前に情報提供することが望ましいとされている。MDM は、次の情報を明確にコミュニケーションすることによって、HCP 及びユーザーをサポート可能である。
    a. 影響を受ける機器
    b. 機器の OS
    c. デプロイされる機器のバージョン
    d. ソフトウェアコンポーネントの特定

e. サービスが変更される予想日時

f. サービス変更の後に利用可能な保守の程度

g. 追加の補完的コントロール

3. **関連する製品セキュリティ文書及びライフサイクル文書の更新の提供**：機器のライフサイクルが進むにつれて、（開発段階でのコミュニケーションに関して、6.1.1 で述べたように）サポートする製品セキュリティ文書やライフサイクル文書が変更される可能性がある。このような場合、MDM は、HCP が新たなリスク又は変更されたリスクに対応するために、必要に応じてリスクマネジメント戦略を調整できるように、関連する文書（電子媒体でも可）を更新して HCP に提供することが望ましい。

4. **脆弱性情報及びパッチ情報の提供**：脆弱性が見つかった場合、MDM は、適切な軽減策（例えばソフトウェアパッチ）を含む関連する脆弱性情報を提供することが望ましい。患者危害又は機器の障害を防ぐために遅滞なきコミュニケーションが求められるような、リスクの大きな脆弱性に対しては、高い優先度を置くことが期待される。それに加えて、軽減の方法（例えば、ネットワーク経由のアップデート、インストールのためのサービス要員の配置）及び実装方法の指示を機器のオペレーターに対して提供することが望ましい。

5. **サードパーティのコンポーネントについての積極的なコミュニケーションの提供**：医療機器内のソフトウェア及びその他のデジタルコンポーネントが、機器自体より前に EOL や EOS に至ることがある。このような場合、コンポーネントに対するサポートがないことで、機器に対してリスクが生じてしまう可能性がある。このリスクを補償する助けとして、MDM は、次を行うことが望ましい。

   a. 機器で使用しているサードパーティのコンポーネントのサポート状態を追跡する。

   b. 機器で使用しているサードパーティのコンポーネントがサポートされなくなった場合に発生する可能性のあるリスクを評価する。

   c. HCP に対して、新しいリスク及び利用可能な軽減策を伝える。

6. **患者に対してコミュニケーションを提供する**：この文書の適用範囲から外れるが、MDM 及び HCP はいずれも、関連する場合に EOL や EOS の期日及び情報を患者に伝えることが望ましい。

7.1.2. ヘルスケアプロバイダーの推奨事項

1. **情報ニーズの特定**：HCP は、全ての機器（レガシー及びその他）に対して、機器を適切に保守し保護するために必要と考える情報の種類（詳細は下記に示す）、及び、いつどのように誰からその情報を入手し、誰にその情報を提供するかについて特定することが望ましい。

   a. 例えば、ある HCP が、特定のレガシー機器に対して、機器がアップデートを受けるかどうか、その期間、予想される時期について理解する必要があると判断する可能性がある。そして、その HCP は、その情報が HCP のセキュリティチーム及び臨床工学チームに提供され、チームが適切な運用上及び保守の決定を行うことができるようにすることが望ましいと判断する可能性がある。

   b. HCP が運用戦略を策定する際に検討が望ましい特定の領域の一つに、責任移転がある。場合によっては、HCP は、MDM が宣言した EOL 期日又は EOS 期日を超えて、機器を継続使用する。機器を安全で有効に使い続けることを確実にするために、HCP は、サポートされ

ない機器を使用するリスクの責任が、ある関係者から別の関係者にいつ移転するかを MDM に対して積極的に質問することが望ましい。

2. **調達前のコミュニケーション**：HCP が、その施設において、製品寿命の間、機器のセキュリティ管理を行う準備のため、機器の購入及び据付に先立って、MDM と HCP との間で情報共有して、導入時研修及び管理を適切に支援することが望ましい。HCP は、次を要求したいと考える可能性がある。
    a. EOL 期日（既知の場合）
    b. EOS 期日（既知の場合）
    c. 機器のソフトウェアコンポーネント（例えば、OS、サードパーティのソフトウェア、アプリケーションソフトウェア）のアップグレード戦略
    d. 機器が正しく機能するために必要なネットワークポート及びサービス
    e. 機器を分離して機能を維持するために活用できるファイアウォールルール
    f. アンチマルウェア機能及び（何をスキャン可能かの）適切な定義
    g. セキュリティスキャン機能及び（どのようにスキャンするかの）適切なスキャン定義
    h. セキュリティログ機能
    i. 機器のバックアップ及びリストアの手順
    j. 脆弱性の通知を受け取るための通知方法
    k. 特権アクセス管理ツールを通じて管理するための、管理用アカウント及びその能力
3. **継続的なコミュニケーション**：機器が据付けされ、使用されるようになったら、機器のライフサイクル全体を通して適切な運用及びリスクマネジメントを確実にするために、MDM と HCP との間のコミュニケーションが必要になる。HCP は、機器のライフサイクル全体を通して、次のコミュニケーションの準備をすることが望ましい。
    a. 評価したリスクを説明する脆弱性の開示。必要に応じてプッシュメカニズムによるアップデートを行う。
    b. 既知の脆弱性のリスクをコントロールするために推奨される軽減策
    c. 機器に現れる又はネットワーク監視の結果明らかになる可能性のある、セキュリティ侵害の指標
    d. 機械処理可能なフォーマットで、機器の製品寿命全体を通して更新される SBOM
    e. 期限切れのソフトウェアコンポーネント（すなわち、OS、サードパーティのソフトウェア）に対して、サポート終了になる前の可能な限り早い時期に対応するためのオプション

7.2. リスクマネジメント

7.2.1. MDM の推奨事項

1. **サードパーティのリスクマネジメント**：医療機器がどのライフサイクル段階にあったとしても、既に製品寿命が終了した又はサポートが終了してしまっているコンポーネントが組み込まれてい

る可能性がある。リスクアセスメントによって、安全、基本性能及びサイバーセキュリティに対する全体的な影響を判断することが望ましい。

サポートされていないコンポーネントが悪用可能な脆弱性をもっていたとしても、医療機器の内外の別の補完的コントロールによって、悪用の発生可能性を大幅に低減することが可能である。例えば、ネットワークのファイアウォールは、ネットワーク脆弱性を露呈している医療機器のネットワークポートへのアクセスを、ブロック又は限定的にコントロールすることが可能である。ただし、ファイアウォールは一つの選択肢であり、MDM が脆弱性に対応しリスクをコントロールするために、ファイアウォールの使用又はセグメンテーションだけに頼ることは、患者ケアに影響を与える可能性があるので、避けることが望ましい。

2. **コミュニケーションの期待事項**：医療機器が EOL 期日に近づいた場合、MDM は、EOL 期日及び EOS 期日について HCP 及び規制当局に対して明確なコミュニケーションを行い、HCP がライフサイクルの EOS 段階に対して計画するための適切な情報を提供することが望ましい。このライフサイクル情報には、7.1.1 に示した情報に加えて、アップグレードの選択肢が含まれる可能性がある。

   これらの追加情報は、HCP が医療機器を継続使用するために要求されるリスクマネジメント活動をサポートするために用いられることがある。

3. **市販後の期待事項**：MDM が機器の市販後に達成することが期待され、その期待が医療機器サイバーセキュリティの製品ライフサイクル全体に適用されるような活動がある。具体的には、この期待は、次のようなものである。

   a. 顧客の苦情（サービス提供に対するものを含む）の収集、文書化及び対応。

   b. 規制当局が要求する、不具合事象報告及びインシデント報告。（例えば、機器の問題によって引き起こされた事象で、死亡、重症に至るもの又は事象が再発した場合に死亡、重症に至る可能性があるもの）。

   c. 必要な場合、市場安全性是正処置（例えば、回収、改修、取説の改訂）の実施。

      i. （ライフサイクルの段階によるなど）場合によっては、MDM は、正式な処置を行わず、規制要件に従って単にサイバーセキュリティの脆弱性の存在及び既知の軽減策について伝えるだけでもよい場合がある。

      ii. 患者に直接接続される医療機器（例えば、連続グルコースモニター）については、MDM は、地域の規制要求に従って、改修及び回収の情報を直接伝えることが期待される。

   d. 積極的なリスクマネジメント（脆弱性マネジメントを含む）の実施。（例えば、機器のセキュリティ及び安全に関連するリスクに影響を及ぼすセキュリティの問題を監視、対応し、コミュニケーションするために、ツール、リソース及び要員を継続的に用いる。）

   e. 受動的なリスクマネジメント（脆弱性マネジメントを含む）の実施。（例えば、セキュリティ及び安全に関連する重大なリスクに対応し、コミュニケーションするために集めたツール、リソース及び要員を、必要に応じて用いる。）

4. **継続的監視**：MDM は、医療機器のリスクプロファイルの変化を EOS まで引き続き監視し、HCP 及び規制当局に対して、その変化を伝えることが望ましい。そうした変化が、安全、日程、予算、活動に対して、又は医療機器の継続使用に対しても影響を与える可能性があるからである。HCP

が、限定的サポート段階においても、まだサポートされている可能性があるコンポーネントのソフトウェアアップデートを受けるかどうかについては、MDM と HCP との間の特定の契約及び MDM が EOL 期日を延長する能力による可能性がある。

7.2.2. ヘルスケアプロバイダーの推奨事項

機器は、製品ライフサイクルの全体を通して継続使用されるので、リスク及び脆弱性マネジメント関連の進化するニーズを考慮し、HCP がこれらのリスクを軽減するためにどのようにベストプラクティスを実施できるかを考慮することが重要である。脅威の様相が進化するに伴い、行動及び実践もまた、変更され進化する必要性がでてくる。入念な計画がなければ、レガシー機器がもたらすリスク及びその影響の可能性は、時間と共に増加するだろう。医療機器のサイバーセキュリティは、共同責任であるが、通知された EOL 及び EOS の期日を超えて機器が継続使用される場合は、HCP は、機器のセキュリティ手段を実施するためにさらに多くの責任をもつ必要があるかもしれない。

1. **セキュリティベースラインの考慮事項**：セキュリティベースラインの推奨事項は、サポート段階で非常に重要になる。HCP のセキュリティ推奨事項のベースラインには、次が含まれることがある。
    a. リスクアセスメントプロセスによるデバイスの重要性と重要度の評価に基づくネットワークセキュリティコントロールの適用
    b. 追加のネットワークコントロール及び物理的なコントロール並びに定期的な監視を必要とする重要な機器を特定するためのリスクアセスメントの実施
    c. サポート及びパッチについて、MDM との積極的なコミュニケーションに関する推奨事項の維持
    d. 現在の全ての資産を特定し、将来の構成変更を追跡するための構成管理の採用
    e. サイバーハイジーン及び脆弱性修正をサポートする IT セキュリティ監視及びパッチプロセスの維持
    f. 論理的及び物理的セキュリティコントロールによる不正アクセスからの保護
    g. サイバーセキュリティのトレーニング及び意識向上プログラム
    h. 脆弱性マネジメント
2. **運用環境に対する考慮**：機器に対する適切なリスクマネジメント及び脆弱性マネジメントは、特定の機器及びその運用環境に依存する。アクセスコントロール及び監視に対する考慮事項は、以降の段落に記載されている。
3. **アクセスコントロール**：機器が、HCP のネットワークのうち、機器の機能を実行するために必要な部分だけをアクセスし、接続することが重要である。機器にアクセスコントロールを実装することは、機器に入出力する情報及びコマンドのフローを必要以上に制限するかもしれない。これらのコントロールは、機器の種類、その他のネットワーク機能及び機器が製品ライフサイクルのどの段階にあるかに応じて進化するかもしれないが、次世代ファイアウォールのような既存のツールによって、定義した一連のルールに基づく動的なネットワークセグメンテーション及びシステムポリシーの施行が可能になる。

4. **ネットワークセグメンテーション**：ネットワークは、セキュリティ要求事項及び業務上のニーズに基づいて、セグメンテーションされる可能性もある。しかし、ネットワークをセグメンテーションすることで、ネットワークの一部が侵害された場合でも、ネットワーク上のラテラルムーブメントの能力を制限できるかもしれない。ネットワークのセグメンテーションを行う場合は、セグメンテーション（ファイアウォールの使用を含む）が、機器の機能にどのような影響を及ぼすかについて考慮する必要がある。

   注記：多くの機器が、臨床用アプリケーションや電子カルテと統合して設計、構築されてきており、今もされている。レガシー機器の脆弱性をセグメンテーション又はファイアウォールによってコントロールすることで、管理上の負荷が発生し、患者ケアに対する悪影響の可能性があり、統合の意図するベネフィットを損なう。結果として、MDM は、脆弱性に対応してリスクをコントロールするために、セグメンテーション又はファイアウォールの使用だけに頼ることを避けることが望ましい。

5. **多要素認証**：多要素認証を導入することで、ネットワーク又は機器の機能に対してロールベースのアクセスを行ってもよい。ただし、認証の方法及び処理速度は、医療環境の状況に応じて考慮しなければならない。

6. **監視**：ネットワーク上の機器の動作を監視することによって、HCP の侵害防止を助けることができ、侵害発生時の対応にも役立つ。HCP は、機器のライフサイクル全体を通して、ネットワーク接続された機器の動作を追跡可能な、何らかの活動監視システムを実装することが望ましい。こうしたシステムは、場合によっては、機器が誤った挙動をとる可能性についても情報提供することが可能である。

   注記：これは、IDS（Intrusion Detection System、不正侵入検知システム）、IPS（Intrusion Prevention System、不正侵入防止システム）、システムロギング又はファイアウォールロギングシステムの形をとることがある。より成熟したサイバーセキュリティ態勢をもつ HCP は、これを SIEM（Security Information and Event Management、セキュリティ情報及びイベント管理）システムに組み込むことが可能である。HCP は、そうしたシステムが機器の意図する使用に影響を及ぼす可能性があるので、システムの使用については、必要に応じて MDM と協働することが望ましい。レガシー機器の性質上、特にリアルタイム OS を使用している機器では、機器自体に監視ソフトウェアをインストールして追加することができない場合がある。しかし、外部機器との間の情報の流れを監視できるツールがあり、これによって機器の動作情報を適切に収集することが可能である。

7. **インベントリ管理の考慮事項**：EOS に対する事前の計画立案は、機器が据付けされる以前の、調達に向けた話し合いの時点から始まり、EOS 期日がわかっているかどうかによらない。強力なインベントリ管理システムを用いることが助けになる可能性がある。使いやすく、正確で、リアルタイムなインベントリ管理によって、HCP は、来るべき EOS 期日に対して、事前に計画を立てるための十分な時間がもたらされる。在庫リスト中の各資産について、次のような情報を含めることが有益である。

   a. 現時点のライフサイクル段階

   b. 予想される EOS 期日

   c. SBOM（SBOM のベストプラクティスの詳細については、IMDRF N73 文書を参照）

   d. 脆弱性の状況及びソフトウェアパッチの状況

e. 運用環境（ネットワーク構成図）

f. メンテナンスのスケジュール

可能な場合は、ある種のタスクを自動化することによって、臨床スタッフがヘルスケアの提供に注力することができるようにもなる。この強固なインベントリ管理システムは、医療機関が、EOS 期日を超えた機器を引き続き臨床使用する際にも不可欠である。EOS 及び EOS 後に対する計画立案中に、HCP は、機器を継続使用するリスクを理解して受容することが望ましい。HCP は、定期的に臨床上のベネフィット・リスク分析を行って、EOS 期日を超えたレガシー機器をリスク補完手段を講じて使用することと、新しい又はアップグレードした機器を購入することとを比較検討することが望ましい。

8. **脆弱性マネジメントの考慮事項**：IMDRF N60 ガイダンスに示されている通り、HCP は、医療機器のサイバーセキュリティを管理するために、リスクに基づくアプローチを採用することを検討することが望ましい。このプロセスは、次に対して適用されることが望ましい。

a. IT インフラストラクチャーの開発、管理及びアップグレード

i. 機器が接続されるネットワークを考慮することは重要である。また、全てのネットワーク設計及びアーキテクチャーは、ネットワーク上に存在する可能性がある様々な機器（レガシー機器を含む）を考慮することが望ましい。これには、医療従事者が必要なときにタイムリーな支援を行うことを妨げることなく機器のセキュリティを高める、ゼロトラストアーキテクチャーのプロトコル実装が含まれる可能性がある。

b. SBOM の取得及び使用

i. 医療機器のアーキテクチャー及び設計の性質上、医療機器には、複数の異なるソース及びサプライヤーからのソフトウェア及びハードウェアが含まれる可能性がある（これには、組込みシステム、データロギング及びハードウェア構成部品を含むが、これに限らない）。HCP は、ネットワークインフラストラクチャーに統合する全ての機器について SBOM を要求することが重要である。入手可能な場合は、SBOM によって、機器がどのように製品ライフサイクルの全体を通して進化する可能性があるか、並びに、リスクコントロール手段及び軽減戦略のより効果的な適用方法について、顧客がよりよく理解可能である。

ii. ある種のソフトウェア又はサブシステムが、それをコンポーネントとして含む全てのシステムに影響する脆弱性をもつということは、珍しいことではない。SBOM を活用することによって、HCP は、機器自体というより、機器のコンポーネントに関係する開示された脆弱性が、機器に影響を及ぼす可能性があるかどうかをチェックすることが可能である。

iii. 機器が EOL 及び EOS 期日に近くなると、開示された脆弱性を監視して、それが使用中の機器にどのように影響するかを監視するシステムを、HCP がもつことが重要になる。

c. ネットワークに対する新たな機器の統合及び据付

i. 新しい機器は、既存のネットワークへの統合に先立ってリスクアセスメントを受ける可能性がある。これには、機器をネットワークセグメントに置くか、アクセスコントロールを適用するか、機器の動作についてネットワーク監視に統合するかの判断が含まれることがある。

d. ネットワーク接続する装置のアップデート又は変更（装置は、医療機器及びノート PC やサーバーなどの接続された装置を含むが、これに限らない。）

IMDRF N60 ガイダンスは、HCP が、リスクマネジメントプロセスを適用する際に参照できる、いくつかの推奨規格を示している。

HSCC HIC-MaLTS の“課題及び推奨事項”のセクションには、インベントリー管理及び SBOM を含む多くの課題に対する推奨事項が含まれている。

9. **使用停止についての考慮事項**：IMDRF N60 ガイダンスの 6.6.2 では、医療機器の製品ライフサイクル全体にわたる多くのセキュリティ推奨事項を示している。機器が EOS に近づくと、HCP は、機器の使用停止について調べる又は継続使用のためにサイバーセキュリティリスクを引き受けることが重要である。

7.3. 責任移転

製品の年数が経ち、製品ライフサイクルを経過するにつれ、サポート段階及び限定的サポート段階において、セキュリティが MDM 及び HCP の共同責任であることから、EOS 段階において、サイバーセキュリティのサポート責任が HCP へ移転するということを明確にすることが重要になる。機器のコンポーネントが、予期せぬサポート終了宣言を行われる場合を除いて、EOL 宣言は、MDM と HCP との協調移行期間である限定的サポート段階のきっかけとなる。別のライフサイクル段階への移行についての追加情報については、セクション 5.5 を参照。セクション 7.3 では、このライフサイクルの責任移転を実施する際の MDM 及び HCP の両者に対する推奨事項を提供している。

7.3.1. MDM の推奨事項

1. **日程についての考慮事項**：ベストプラクティスとしては、サイバーセキュリティの責任を HCP に移転するプロセスは、EOS のおおよそ 2〜3 年前に開始する。MDM が HCP に対して 2〜3 年前に通知することによって、HCP が装置の置換えを評価、計画及び予算計上できるようになる。
2. **新規又はアップグレードの「サポート」機器への移行の道筋**：サポート段階が終了する前に、MDM 及び HCP は、最終的な EOS への移行並びに／又は製品のアップグレード及び置換えに向けて、協調し準備することが望ましい。サポート機器への移行によって、MDM と HCP との間のセキュリティの共同責任は維持される。

   MDM がサポートできない機器を、HCP が置き換えていない場合は、サイバーセキュリティの責任は、HCP に移転する。HCP が利用可能な全ての選択肢を特定するために、MDM は、次の情報を明確にすることが望ましい。

   a. 限定的サポート段階への移行及び最終的な EOS 段階への移行によって影響を受ける医療機器の詳細情報

   b. EOL や EOL の時点で実装できる、構成可能なセキュリティの選択肢

   c. HCP が利用可能な、アップグレードの選択肢

      - ソフトウェアのみ
      - ソフトウェア及びハードウェアの一部
      - 完全な置き換え

- 置換えの選択肢及び戦略
- 入手可能な機器の型式及び機能

7.3.2. ヘルスケアプロバイダーの推奨事項

サポート段階の間に、HCP は、次を行いたいと考える可能性がある。

1. サイバーセキュリティ及び臨床使用の観点から、HCP が機器を管理する能力の評価
2. 機器の管理を助けるために利用可能な、サードパーティーからのサポート可能性の特定
3. 機器の置換え機会の評価
4. 機器をサポートするために利用可能な追加リソースの特定

8. 限定的サポート段階の責任及び期待

このセクションでは、ライフサイクルの限定的サポート段階における利害関係者の責任を、コミュニケーション、リスクマネジメント及び責任移転について詳細に示す。

8.1. コミュニケーション

MDM と HCP との間のコミュニケーションは、限定的サポート段階の間に増加することが望ましい。リスク情報は、HCP に提供し、HCP が受け継ぐリスクの情報を得たうえで決定できるようにすることが望ましい。軽減策についての情報及び機器置換えの選択肢に関する情報についても、入手可能にすることが望ましい。

8.1.1. MDM の推奨事項

1. **限定的サポートに移行することを示す顧客への通知の発行**：MDM は、（例えば、企業のウェブサイトにおける公表又は HCP に対する直接の通知によって）顧客への通知を発行して、サイバーセキュリティの EOS 期日まではサポートが継続するが限定的なものになること、EOS 期日を過ぎると機器はサポート不能になりレガシー状態に入ることを知らせることが望ましい。この顧客への通知のタイミングは、EOL 期日が近づいたときに行って、機器の使用停止及び HCP の事業継続計画の立案のために、事前通知できるようにする。
2. **限定的サポートに移行することを示す公開情報の発行**：MDM は、（例えば、企業のウェブサイト又はその他の永続的に利用可能なリソースにおける公表によって）公開情報を発行し、機器のサポート状態を説明することが望ましい。機器が別の段階に移行する場合には、公開情報を更新して、関係者（再販業者や中古機器の購入を計画する可能性のある組織を含む）が、そうした機器を継続使用する潜在的リスクを理解できるようにする。
3. **サービス及び文書の提供の継続**：現実的で適切である限り、サポート段階のコミュニケーション（7.1.1）のサービス及び文書を継続して提供する。これには、脆弱性についてのコミュニケーションも含まれる。
4. **ライフサイクル計画情報の提供**：MDM は、サイバーセキュリティの EOS 期日の日程を引き続きコミュニケーションして、顧客が EOS 及び関連する顧客の責任事項について、時間的に十分な余裕をもって準備できるようにする。取りうるコミュニケーションには、次が含まれる。
    a. 医療機器の部品（すなわち、機器のソフトウェア）がサポートされなくなった時に、一部の保守が終了したことを示す警告
    b. セキュリティ関連の通知及びアドバイザリー情報
    c. 補完的コントロールについての、機器特有のアドバイザリー情報
    d. 限定的サポート段階に移行したことに伴う、意図する使用の制限
5. **製品セキュリティ文書の提供**：サポート段階で推奨されるセキュリティ文書の提供（7.1.1.1 及び 7.1.1.3）に加え、MDM は、次の文書を提供することが望ましい。

a. サポートが制限されていることを考慮して推奨される、次のような補完的コントロールを示す、更新したセキュリティ文書。

   i. ファイアウォール

   ii. VPN

   iii. ネットワークの分離

b. 機器のデプロイ環境に対する期待

8.1.2. ヘルスケアプロバイダーの推奨事項

7.1.2.3 のコミュニケーションは、継続し、HCP は、受け取る追加情報及び更なる粒度の情報（すなわち、8.1.1）に対するあらゆる疑問について、MDM に質問することが望ましい。HCP は、再販機器又は中古機器を購入するかどうかを評価する可能性があるので、HCP は、契約延長又はサードパーティのサポートなどの追加サポートが利用可能かどうかについても質問したいと思う可能性がある。

8.2. リスクマネジメント

8.2.1. MDM の推奨事項

MDM は、7.2.1 のサポート段階から、市販後の期待及び監視に関する活動を継続して行うことが望ましい。しかし、リスクマネジメント活動の一部として行う積極的な脆弱性マネジメントに関連する作業の頻度及びレベルは、減少する可能性がある。

8.2.2. ヘルスケアプロバイダーの推奨事項

1. **再販機器又は中古機器を購入するかどうかを評価する場合に、EOL や EOS のリスクを検討する**：HCP は、再販機器又は中古機器の購入を選択する可能性がある。その場合、HCP は、次を行って、あらゆるサイバーセキュリティリスクの可能性を管理する助けとすることが望ましい。

   a. 望んでいる機器が、限定的サポート段階にある（つまり、EOL 期日に達している）か、又は EOS 段階にあるかどうかを調査する。

   b. その場合、HCP は、EOL や EOS 期日に達した機器を使用するリスクを注意深く検討することが望ましい。

   c. 機器を購入することを選択した場合は、HCP は、次を行うことが望ましい。

      i. 契約延長又はサードパーティのサービスなどのサポートが利用可能かどうか判断する。

      ii. サポートが利用可能な場合は、HCP は、ベンダーとの契約に、サポートを要求する及び／又は含めるという文言を含めることが望ましい。サポートがベンダーから入手可能でない場合は、HCP は、どのように HCP が機器をサポートするかを検討することが望ましい。

2. **EOS が近づいた場合の HCP の考慮事項**：EOL の後、HCP は、機器の EOS 期日が近づいていることを、MDM からの積極的なコミュニケーション及びインベントリ管理システムからの通知の両方によって、知らされる。HCP は、EOS に対してさらに準備しなければならず、次の質問事

項を検討して、サポートなしで機器を運用するリスクが適切にコントロールされているかどうかを特定することが望ましい。次の質問リストは、網羅的なものではない。

a. 予測耐用期間を超えて、どのくらいの期間、その機器が臨床で使用されると期待されるか。

d. その機器が臨床使用を期待される期間に対して、保守コストは発生するか。

c. 保守コストは、機器のアップグレードに比較してどれくらいか。

d. 新規の又はアップグレードした機器は、サイバーセキュリティのレジリエンスを改善すると同時に、どれほど臨床ケアを改善するか。

e. HCP は、この機器のセキュリティを維持するためのツールをもっているか。

f. HCP は、この機器のセキュリティを維持するための財政的リソースがあるか。

g. HCP は、この機器のセキュリティを維持するための専門知識をもっているか。

h. この機器のセキュリティが侵害された場合の、患者に対するリスクは何か。

i. この機器によって組織のセキュリティが侵害された場合の、患者に対するリスクは何か。

j. この機器が使用されず代替手段に置き換えられた場合の、患者に対するリスクは何か。

k. この機器は、ネットワークに接続しない場合に有益に動作できるか。

l. その他にどんなコントロールが実施できるか。

追加推奨事項及び追加検討事項について、HCP は、HSCC HIC-MaLTS の責任移転のフレームワークを参照してもよい。

8.3. 責任移転

この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・置換えに対して、MDM 及び HCP が協調し準備するための移行期間となる。この期間内に、双方で、機器及びサポートの選択肢を評価し、将来に向けた推奨事項を作成する。この移行において、限定的なサポートが、セキュリティの共同責任を維持するために利用可能になることがある。限定的なサポートの利用可能性及び範囲は、様々であり、双方が十分に理解して、認識することが望ましい。将来の状態が変わらず、サポートされない製品が使用されたままで、MDM がサポートできない場合、その機器の継続使用及び手入れをサポートするセキュリティの責任は、HCP にある。

サイバーセキュリティのサポート責任は、HCP に移転される。HCP が、ある責任を引き受けることができない場合は、MDM は、実現可能ならば段階的な責任移転を検討してもよい。

8.3.1. MDM の推奨事項

セキュリティの責任が HCP に対してスムースに移転することを確実にするために、次の検討事項リストをレビューし、評価することが望ましい。

1. 顧客が入手可能なもの全てを適用可能にするために（又は顧客が EOL や EOS のマイルストーンで利用可能にするために）、入手可能なソフトウェアアップデートを特定する。

2. MDM が提供するセキュリティ文書には、HCP がネットワークのセキュリティコントロールを可能とするために役立つ情報が提供されていることが望ましい。

3. HCP に対して機器の運用に必要なネットワークポート及び IP アドレスの情報を提供する、特定されたネットワーク要件。
4. HCP が「強化」可能な、（ネットワーク経由で）医療機器にアクセスする全ての不要なネットワークポート及び IP アドレスをブロックするネットワーク要求事項。
5. 入手可能な製品セキュリティ文書（SBOM を含む）。
6. 顧客のサイバーセキュリティ態勢を助ける、医療機器サイバーセキュリティのベストプラクティスに関連する利用可能なその他の情報。
7. 利用可能な限定的サポートの選択肢についてのコミュニケーション。次を含むこともあり、含まないこともある。
    a. 利用可能な場合、ハードウェアコンポーネントの置換え（例えば、ディスプレイモニター、筐体、ハードディスクドライブなど）
    b. 機器のシステム状態を回復する、リカバリーソフトウェア
    c. 利用可能な場合、（医療機器とは別の）ネットワークハードウェアセキュリティ機器の追加

8.3.2. ヘルスケアプロバイダーの推奨事項

セキュリティの責任が HCP へスムースに移行することを確実にするために、次の検討事項リストをレビューし、評価することが望ましい。

1. 機器のサイバーセキュリティ監視
2. 脆弱性マネジメント
3. 物理的又は論理的なアクセス制御を含む、補完的コントロールの実施
4. EOS 機器の適切な保護に適したデプロイ環境の確保
5. インシデント対応計画の実施
6. 事業継続計画の確立
7. HCP のリスクマネジメントプロセスに示されている要点にしたがった、リスクアセスメントの定期的実行

9. EOS 段階の責任及び期待

このセクションでは、ライフサイクルの EOS 段階における利害関係者の責任を、コミュニケーション、リスクマネジメント及び責任移転について詳細に示す。

9.1. コミュニケーション

9.1.1. MDM の推奨事項

機器が EOS 段階に入る前までに、MDM は、EOS 期日及びいつ機器が EOS 段階に達するかを HCP に通知しておくことが望ましい。この段階では、以降のサイバーセキュリティのサポート責任は、HCP に移転している可能性がある。HCP が、ある責任を引き受けることができない場合は、MDM は、実現可能ならば段階的な責任移転を検討してもよい。

1. **セキュリティ保守のために製品セキュリティ情報の提供**：MDM は、HCP が機器のサイバーセキュリティリスクを MDM の援助なしで管理できるように、関連する製品セキュリティ情報を HCP に提供することが望ましい。この情報には、次が含まれる可能性がある。
    a. 機器のセキュリティを引き続き確実にするために HCP が引き受けることになる追加責任。これには、サイト特有のコントロール（例えば、ファイアウォール、ネットワーク分離、VPN）が含まれる可能性がある。
    b. サイバーセキュリティの EOS 期日以降に受けることができるサポート
    c. 利用可能な機器のアップグレードパス
    d. 使用停止についての情報：MDM は、HCP が将来的に機器を使用停止できるように情報提供することが望ましい。
2. **EOS に移行することを示す公開情報の発行**：MDM は、（例えば、企業のウェブサイト又はその他の永続的に利用可能なリソースにおける公表によって）公開情報を発行し、機器のサポート状態を説明することが望ましい。（再販業者や中古機器の購入を計画する可能性のある組織を含む）関係者が、そうした機器を継続使用する潜在的リスクを理解できるようにすることが望ましい。
3. **市販後の期待の一部として受け取った患者リスク情報を、問題が起こった後に行う脆弱性マネジメントを通して、必要に応じてコミュニケーションする**

9.1.2. ヘルスケアプロバイダーの推奨事項

HCP は、EOS の開始時点で受け取った情報（すなわち、9.1.1）に対するあらゆる疑問について、MDM に質問することが望ましい。HCP は、再販機器又は中古機器を購入するかどうかを評価する可能性があるので、HCP が、契約延長又はサードパーティのサポートなどの追加サポートが利用可能かどうかについても質問する可能性がある。

9.2. リスクマネジメント

9.2.1. MDM の推奨事項

EOS 後も、MDM は、地域の規制によっては依然としてある種の市販後活動に対して責任がある（7.2.1.3 を参照）。ランサムウェアのシナリオ（例えば、WannaCry）のように、患者安全に対する重大なリスクがある場合は、（7.2.1.3 で示したような）対応するリスクマネジメントのアクションが、追加で必要になる可能性がある。

9.2.2. ヘルスケアプロバイダーの推奨事項

1. 8.2.2.1 に記載するように、**再販機器又は中古機器を購入するかどうかを評価する場合には、EOL や EOS のリスクを検討する。**
2. **EOS を超えた機器を使用する場合の HCP の考慮事項**：HCP が EOS 期日を超えた医療機器を使用する際のリスクを受容する場合には、次を満足することが推奨される。
    a. 強力で、適格で、（増加するリスクを管理するための）リソースが適切にあるサイバーセキュリティプログラムを、上層部の承認を受けて確実に実施する。
    b. 強固なインベントリ管理システム（可能な場合は自動化されたシステム）を確実に実装する。
    c. レガシー機器を、組織が継続的に行っているリスクマネジメント活動に含める。
    d. 信頼できる情報源を積極的に監視する。情報源としては、ISAO（情報共有分析機関：Information Sharing Analysis Organizations）、ISAC（情報共有分析センター：Information Sharing and Analysis Centers）、CERT（コンピューター緊急対応チーム：Computer Emergency Response Teams）などの普及活動を行う機関、規制当局、脆弱性データベース（例えば、サードパーティのコンポーネントのデータベース）など。
    e. 対抗手段を強化する。対抗手段は、例えば、ネットワークのセグメンテーション、ユーザーロール、セキュリティ試験、ネットワーク監視、ネットワークからの切断があるが、これらには限定しない。
    f. 入手可能な代替製品を定期的に評価し、EOS を超えた機器を運用するという決定を再検討する。

追加推奨事項及び追加検討事項について、HCP は、HSCC HIC-MaLTS の責任移転のフレームワークを参照してもよい。

9.3. 責任移転

9.3.1. MDM の推奨事項

この段階においては、エンドユーザーへの責任移転が完了している。MDM は、機器が EOS であり、責任が移転したことを伝達済みである。

9.3.2. ヘルスケアプロバイダーの推奨事項

責任及びリスクの受容、又は新規若しくはアップグレード機器への移行：様々なプレッシャーを考慮すると、HCP が予想耐用期間を超えた医療機器を使い続けるのは珍しいことではない。多くの場合、機器が故障する又は意図通りに動作しないことが、内部での点検・修理又は使用停止のきっかけになるのは、ユーザーにとって明白なことである。それ以外にも、脅威から保護するためのサポートがなくなることがきっかけになる可能性があることは、あまり明らかではない。いずれの場合においても、患者危害の可能性が存在する。HCP が強力なインベントリ管理システムをもつことが不可欠であり、各医療機器の EOS 期日が近づいた場合には、レガシー機器がもたらすリスク及び組織のサイバーセキュリティプログラムの成熟度に関して、注意深く検討することが絶対に必要である。

10. TPLC におけるサイバーセキュリティの責任及び期待のサマリー

上記のセクション 6～9 は、MDM 及び HCP の責任及び期待について、サイバーセキュリティに対する製品ライフサイクルの四つの段階（開発、サポート、限定的サポート及び EOS）の状況で、特にリスクマネジメント、コミュニケーション及び責任移転に関して、更に詳細な情報を追加で提供している。また、セクション 6～9 には、医療機器サイバーセキュリティの製品ライルサイクル全体のうち、MDM が市販後に行うことを期待する、ある種の活動についても記載している。図 2 に示す、サイバーセキュリティの製品ライフサイクル全体についてのサマリーは、製品ライフサイクル全体にわたる責任移転に伴い、責任及び期待に対する労力レベルがどのように変化するかを表している。

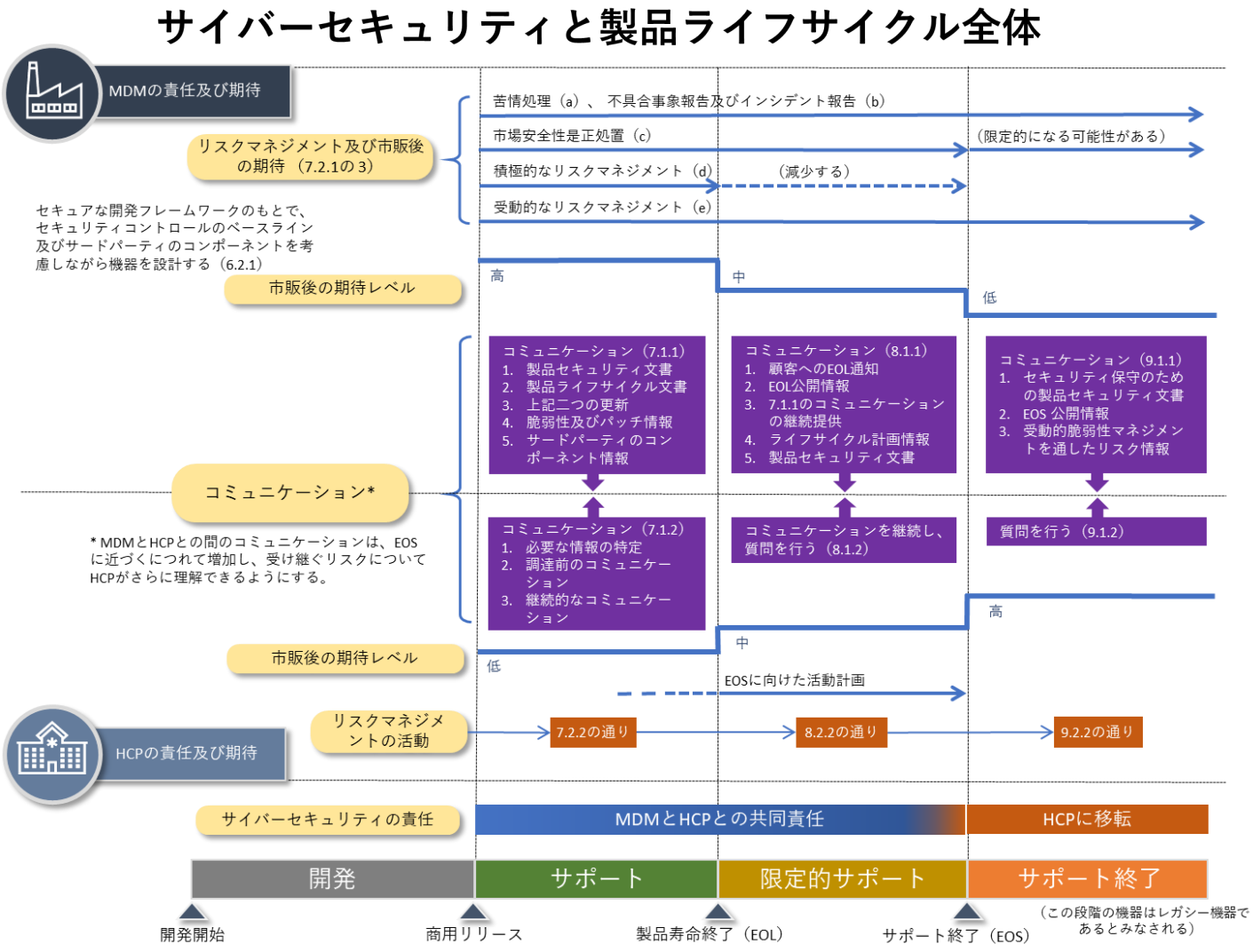


図 2：サイバーセキュリティの製品ライフサイクルにおけるレガシー機器のフレームワークの詳細

11. 医療機器の EOS 後の補完的コントロールに関する考察

補完的リスクコントロール手段（補完的コントロールともいう）は、医療機器の設計の一部として実装されたリスクコントロール手段の代わりに、あるいは、ない場合に適用される、特定のタイプのリスクコントロール手段である（AAMI TIR97:2019）。健康及び安全に関連するリスクが特定された場合又はその他の不適合がある場合に、MDM は、機器を適合状態にするために、更なる修正、是正処置を実施し、適用可能な場合は、予防処置を実施する。

機器が MDM が通知した EOS に到達したとき、レガシーな技術を使うことで引き起こされるリスクがあり、MDM の（セキュリティに関する）サポートがない状態であるにもかかわらず、HCP は、機器の運用を継続することを決定する可能性がある。継続使用の理由としては、機器を臨床使用できる期間がサポート期間より長い、市場に現実的な代替策がない、予算の限界などがあるが、これらには限らない。

EOS 後も機器を使い続けることを決定したら、HCP は、限定的サポート段階及び EOS 段階において MDM が提供する製品セキュリティ文書（このガイダンスのセクション 8 及び 9 に記載）を調べることが望ましい。この文書には、機器それ自体及び運用する IT 環境に対して適用可能な、最低限の補完的リスクコントロール手段を記載している。

11.1. 補完的リスクコントロール手段

補完的リスクコントロール手段を実施することは、技術的な準備及びリソースの両面で、HCP にとってかなりのコストになる可能性がある。そのため、HCP 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とを比較検討することが望ましい。

表 1 は、補完的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 の文脈で提供しているが、実施の実現可能性は、特定の機器及びその運用環境に依存し、機器の臨床的な意図する使用を損なうことがあってはならない。表に挙げたコントロール手段は、網羅的ではなく、複数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。補完的リスクコントロール手段を実施する場合、技術的なイノベーションについても検討することが望ましい。

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	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。適宜、不正開封防止シールを用いる。
リムーバブルメディア	USB ドライブなどのリムーバブルメディアの使用を、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。
ネットワークの分離	機器を病院ネットワークから分離する。

ネットワークの隔離	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	IDS（侵入検知システム）、IPS（侵入予防システム）又は SIEM（セキュリティ情報及び事象マネジメント）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	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ファイアウォールポートだけを開放する。
マルウェア対策	製造業者に相談したうえで、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。ネットワークから分離された（スタンドアローン）機器については、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	災害時のデータ損失に対して保護するために、バックアップ及び復元の手順を実装する。

表 1：補完的リスクコントロール手段の例

11.2. 教育

技術的及び物理的な補完的コントロール手段を実施することが、EOS 後も機器のセキュリティを保つために役立つことがあるが、その一方で、十分に訓練されたスタッフが、HCP をサイバーセキュリティの脅威から守るために非常に重要である。そのため、HCP は、セキュリティの意識を高めサイバーハイジーン管理を習慣づけるためのサイバーセキュリティトレーニングを、全てのユーザーに対して提供することが推奨される。このようなトレーニングとしては、医療機器のセキュアな操作方法（例えば、セキュアなネットワークのみへ接続する）のトレーニング、並びに医療機器の異常動作（例えば、不規則に起こるシャットダウン・再起動、セキュリティソフトウェアの無効化）を特定して通知する方法が挙げられる。それに加えて、臨床スタッフに対して、EOS 宣言後の機器のセキュリティ制限事項、及び、機器の運用時のリスクを軽減するために守ることが望ましいセキュリティのベストプラクティスについて、知らせることが望ましい。

12. 参考文献

12.1. IMDRF 文書

1. Principles and Practices for Software Bill of Materials for Medical Device Cybersecurity IMDRF/CYBER WG/N73FINAL:2023 (April 2023)
2. Principles and Practices for Medical Device Cybersecurity (IMDRF/CYBER WG/N60FINAL:2020 (April 2020)
3. Software as a Medical Device: Possible Framework for Risk Categorization and Corresponding Considerations IMDRF/SaMD WG/N12:2014 (September 2014)
4. Essential Principles of Safety and Performance of Medical Devices and IVD Medical Devices IMDRF/GRRP WG/N47 FINAL:2018 (November 2018)

12.2. 規格

5. AAMI TIR57:2016 Principles for medical device security—Risk management
6. AAMI TIR 97:2019, Principles for medical device security—Post market risk management for device manufacturers
7. IEC 60601-1:2005+AMD1:2012, Medical electrical equipment - Part 1: General requirements for basic safety and essential performance
8. IEC 62304:2006/AMD 1:2015, Medical device software – Software life cycle processes
9. IEC 62366-1:2015, Medical devices - Part 1: Application of usability engineering to medical devices
10. IEC 62443-3-2:2020, Security for industrial automation and control systems - Part 3-2: Security risk assessment for system design
11. IEC 62443-4-1:2018, Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements
12. IEC 81001-5-1:2021, Health software and health IT systems safety, effectiveness and security — Part 5-1: Security — Activities in the product life cycle
13. IEC 80001-1:2021, Application of risk management for IT-networks incorporating medical devices - Part 1: Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software
14. 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

15. IEC TR 80001-2-8:2016, Application of risk management for IT-networks incorporating medical devices – Part 2-8: Application guidance – Guidance on standards for establishing the security capabilities identified in IEC 80001-2-2
16. ISO 13485:2016, Medical devices – Quality management systems – Requirements for regulatory purposes
17. ISO 14971:2019, Medical devices – Application of risk management to medical devices
18. ISO/TR 80001-2-7:2015, Application of risk management for IT-networks incorporating medical devices – Application guidance – Part 2-7: Guidance for Healthcare Delivery Organizations (HCPs) on how to self-assess their conformance with IEC 80001-1
19. ISO/IEC 27000 family - Information security management systems
20. ISO/IEC 27035-1:2016, Information technology – Security techniques – Information security incident management – Part 1: Principles of incident management
21. ISO/IEC 27035-2:2016, Information technology – Security techniques – Information security incident management – Part 2: Guidelines to plan and prepare for incident response
22. ISO/IEC 29147:2018, Information Technology – Security Techniques – Vulnerability Disclosure
23. ISO/IEC 30111:2013, Information Technology – Security Techniques – Vulnerability Handling Processes
24. ISO/TR 24971:2020, Medical devices – Guidance on the application of ISO 14971
25. UL 2900-1:2017, Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements
26. UL 2900-2-1:2017, Software Cybersecurity for Network-Connectable Products, Part 2-1: Particular Requirements for Network Connectable Components of Healthcare and Wellness Systems

12.3. 規制ガイダンス（ドラフトガイダンスを含む）

27. ANSM (Draft): Cybersecurity of medical devices integrating software during their life cycle (July 2019)
28. China: Guidance for Premarket Review of Medical Device Cybersecurity (March 2022)
29. European Commission: REGULATION (EU) 2017/745 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (May 2017)
30. European Commission: REGULATION (EU) 2017/746 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU (May 2017)

31. FDA (Draft): Cybersecurity in Medical Devices: Quality System Considerations and Content Premarket Submissions (April 2022) [このガイダンスは、N73 文書の発行時点ではドラフトであり、実施されていない。最終ガイダンスで置き換えられる予定である。]
32. FDA: Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software (January 2005)
33. FDA: Design Considerations for Devices Intended for Home Use (November 2014)
34. FDA: Postmarket Management of Cybersecurity in Medical Devices (December 2016)
35. Germany: Cyber Security Requirements for Network-Connected Medical Devices (November 2018)
36. Germany (BSI) - Security requirements for eHealth applications Technical Guideline (BSI TR-03161) (April 2020)
37. Health Canada: Pre-market Requirements for Medical Device Cybersecurity (June 2019)
38. Japan: Ensuring Cybersecurity of Medical Device: PFSB/ELD/OMDE Notification No. 0428-1 (April 2015)
39. Japan: Guidance on Ensuring Cybersecurity of Medical Device: PSEHB/MDED-PSD Notification No. 0724-1 (July 2018)
40. Medical Device Coordination Group (MDCG) 2019-16: Guidance on Cybersecurity for medical devices (December 2019)
41. Singapore Standards Council Technical Reference 67: Medical device cybersecurity (2018)
42. TGA: Medical device cybersecurity guidance for industry (July 2019)
43. TGA: Medical device cybersecurity information for users (July 2019)

12.4. その他の文献等

44. CERT® Guide to Coordinated Vulnerability Disclosure

    https://resources.sei.cmu.edu/asset_files/SpecialReport/2017_003_001_503340.pdf

45. The NIST Cybersecurity Framework

    https://www.nist.gov/cyberframework

46. NIST's Secure Software Development Framework (SSDF)

    https://csrc.nist.gov/CSRC/media/Publications/white-paper/2019/06/07/mitigating-risk-of-software-vulnerabilities-with-ssdf/draft/documents/ssdf-for-mitigating-risk-of-software-vulns-draft.pdf

47. NIST Special Publication 800-12 Rev 1 Introduction to Information Security (June 2017)

    https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf

48. Medical Device and Health IT Joint Security Plan (January 2019)

    https://healthsectorcouncil.org/wp-content/uploads/2019/01/HSCC-MEDTECH-JSP-v1.pdf

49. MITRE medical device cybersecurity playbook (October 2018)

https://www.mitre.org/publications/technical-papers/medical-device-cybersecurity-regional-incident-preparedness-and

50. MITRE CVSS Healthcare Rubric

https://www.mitre.org/publications/technical-papers/rubric-for-applying-cvss-to-medical-devices

51. Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HIC-MaLTS)

Health-Industry-Cybersecurity-Managing-Legacy-Technology-Security-HIC-MaLTS.pdf (healthsectorcouncil.org)

52. Health Industry Cybersecurity Practices: Managing Legacy Technology Security (HIC-MaLTS)

53. Open Web Application Security Project (OWASP)

https://www.owasp.org/index.php/Main_Page

54. Manufacturer Disclosure Statement for Medical Device Security (MDS2)

https://www.nema.org/Standards/Pages/Manufacturer-Disclosure-Statement-for-Medical-Device-Security.aspx

55. ECRI approach to applying the NIST framework to MD

https://www.ecri.org/components/HDJournal/Pages/Cybersecurity-Risk-Assessment-for-Medical-Devices.aspx

56. National Telecommunications and Information Administration (NTIA) / US Department of Commerce, Vulnerability Disclosure Attitudes and Actions: A Research Report from the NTIA Awareness and Adoption Group

https://www.ntia.doc.gov/files/ntia/publications/2016_ntia_a_a_vulnerability_disclosure_insights_report.pdf