事　務　連　絡
令和２年５月１３日

公益社団法人　全日本病院協会　御中

厚生労働省医薬・生活衛生局医療機器審査管理課

厚生労働省医薬・生活衛生局医薬安全対策課

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）

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。

写

薬生機審発0513第1号
薬生安発0513第1号
令和2年5月13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　）

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）

医療機器のサイバーセキュリティについては、「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）、厚生労働省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、「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）により、具体的なリスクマネジメント及びサイバーセキュリティ対策を取りまとめたガイダンスを示し、当該ガイダンスを参考に必要な対応を行うよう、関係事業者等に対する周知を依頼してきたところです。

今般、医療機器のサイバーセキュリティ確保の重要性や各国のサイバーセキュリティ対策の実情等を踏まえ、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。）が取りまとめられました。

国際的な規制調和の推進の観点や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、我が国においても、今後３年程度を目途に、医療機器製造販売業者に対してIMDRFガイダンスの導入に向けて検討を行っているところです。そのため、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、別添のとおり、国立医薬品食品衛生研究所医療機器部が作成したIMDRFガイダンスの邦訳版を参考として情報提供いたしますので、貴管下の医療機器製造販売業者等に対し、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。

なお、IMDRFガイダンスの原文は以下のホームページから入手可能であることを申し添えます。

ＵＲＬ：http://www.imdrf.org/documents/documents.asp

別　添

IMDRF/CYBER WG/N60 FINAL:2020

IMDRF International Medical Device Regulators Forum

最終文書

タイトル: 医療機器サイバーセキュリティの原則及び実践

作成グループ: 医療機器サイバーセキュリティワーキンググループ

日付: 2020年3月18日

Dr Choong May Ling, Mimi, IMDRF 議長

1.0 はじめに

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伴い、医療機器の機能及び安全性を確保するために有効なサイバーセキュリティの重要性が増している。サイバーセキュリティのインシデントは、医療機器及び病院ネットワークを使用不能にすると共に、ヘルスケア施設における患者ケアの提供を中断させてきた経緯がある。これらのインシデントは、診断及び治療介入の遅延、誤診断又は不適切な治療介入等の発生により、患者危害に至る可能性がある。

ヘルスケア製品の製造業者、ヘルスケアプロバイダ、ユーザ、並びに規制当局及び脆弱性報告者を含む全ての関係者は、医療機器のサイバーセキュリティに関して共同責任を有する。本ガイダンスは、全関係者へ向けて、サイバーセキュリティを積極的に支援するための役割に関する理解を促し、将来起こり得るサイバー攻撃、問題又は事象を予測して、医療機器を保護してセキュアにするための情報を提供することを意図している。

ヘルスケアのサイバーセキュリティの原則及び実践に関する国際整合は、患者安全及び医療機器の性能を確実に維持するために必要である。しかし、現時点における医療機器のサイバーセキュリティに係る規制は国毎に異なっており、国際整合に至っていない。

本 IMDRF ガイダンスは、医療機器のサイバーセキュリティに関する国際整合を図るための一般原則とベストプラクティスを提供することを目的とする。本文書では、適用範囲及び用語をそれぞれ 2 項及び 3 項において定義する。4 項では、医療機器のサイバーセキュリティの一般原則について概説し、5 項及び 6 項では、医療機器のサイバーセキュリティに関する市販前管理及び市販後管理におけるベストプラクティスについて多くの推奨事項を責任関係者に提供する。市販前管理については、主に医療機器製造業者に言及する。市販後管理については、全ての責任関係者に向けた推奨事項を記載する。

本文書は、IMDRF が作成した医療機器のサイバーセキュリティに特化した最初のガイダンスであるが、セキュリティについて幅広く検討する上で参照すべき IMDRF 文書として「IMDRF/GRRP WG/N47 FINAL: 2018」が挙げられる。当該文書は、医療機器及び体外診断用（In Vitro Diagnostic：IVD）医療機器[1]の設計及び製造において充足すべき基本要件基準を提供している。これらの基本要件基準は、医療機器の全ライフサイクル（Total Product Life Cycle：TPLC）に渡って、本ガイダンスと共に参照することが望ましい。その他の関連文書である「IMDRF/SaMD WG/N12 FINAL: 2014」の 9.3 項では、安全を考慮する際の情報セキュリティの重要性について記載されており、医療機器ソフトウェア（Software as Medical Device：SaMD）の情報セキュリティに影響する幾つかの要因がまとめられている。

[1] N47 の 5.8 項には、不正アクセスからの保護等、情報セキュリティ及びサイバーセキュリティの重要な要求事項が記載されており、医療機器の全ライフサイクルに渡って、本ガイダンスと共に参照することが望ましい。

- サイバーセキュリティのインシデント、脅威及び脆弱性について、透明性を向上させ対応を強化するために幅広い情報共有のポリシーを促進する。

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。

3.0 定義

本文書で用いる用語及び定義は、以下に示した各規格、並びに IMDRF/GRRP WG/N47 FINAL: 2018 に準ずる。

3.1 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形式のエンティティ（ISO/IEC JTC 1/SC 41 N0317, 2017-11-12）

3.2 攻撃（Attack）：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（ISO/IEC 27000:2018）

3.3 認証（Authentication）：エンティティの特性の正当性に関する保証の提供（ISO/IEC 27000:2018）

3.4 真正性（Authenticity）：エンティティの信憑性（ISO/IEC 27000:2018）

3.5 権限付与（Authorization）：特権の付与。データ及び機能にアクセスするための特権を付与することを含む。（SO 27789:2013）

注記：ISO 7498-2 の定義（権利の付与。アクセス権に基づきアクセスの権利を付与することを含める）に由来する。

3.6 可用性（Availability）：要求するエンティティへのアクセス及び使用の可能性（ISO/IEC 27000:2018）

3.7 補完的リスクコントロール手段（補完的手段）（Compensating Risk Control Measure (Compensating Control)）：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）

注記:補完的リスクコントロール手段としては、製造業者が提供するアップデート等、永続的又は一時的な対応があり得る。

3.8 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、情報を開示せず、使用させない特性（ISO/IEC 27000:2018）

3.20 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、行動又は事象が存在する際のセキュリティ違反の可能性（ISO/IEC Guide 120）

3.21 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）

3.22 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。

注記 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。

3.23 バリデーション（Validation）：客観的証拠を提示することによって、意図する使用又は適用に関する要求事項が満たされていることを確認すること（ISO 9000:2015）

注記 1: "バリデート済み"とは、バリデーションが完了している状態を示す。

注記 2: バリデーションは、実環境又は模擬環境で実施される。

3.24 検証（Verification）：客観的証拠を提示することによって、規定要求事項が満たされていることを確認すること（ISO/IEC Guide 63）

注記 1: 検証のために必要な客観的証拠としては、検査結果のほか、別法による計算又は文書のレビュー等の結果であることがある。

注記 2: 検証のために行われる活動は、適格性プロセスと呼ばれることがある。

注記 3: "検証済み"とは、検証が完了している状態を示す。

3.25 脆弱性（Vulnerability）：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（ISO/IEC 27000:2018）

4.0 一般原則

本項では、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

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：ISAOs）に積極的に参加することが奨励される。このような取り組みを行うことで、透明性を向上させることができる。ベストプラクティスとして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が挙げられる。また、製造業者のみでなくヘルスケアプロバイダ及び医療機器ユーザにも当該ポリシーを適用することは、エコシステムにとっても有益となり得る。規制当局には、患者安全を国際的に保護し、維持するために、海外の規制当局と情報共有することが奨励される。

5.0 医療機器サイバーセキュリティの市販前考慮事項

医療機器のサイバーセキュリティは、製品の全ライフサイクルに渡って検討することが望ましく、製造業者が医療機器の市販前の設計段階及び開発中に対応すべき重要な要素がある。市販前の要素には、1) セキュリティ機能を製品に組み込むこと、2) 受容できるリスクマネジメント手法を適用すること、3) セキュリティ試験、医療機器をセキュアに運用するためのユーザに対する有益な情報提供及び市販後活動のための計画を立案することが含まれる。製造業者は、前述の市販前要素を検討する際、意図したとおりの利用環境に加え、合理的に予見可能な誤使用のシナリオを検討することが望ましい。以下の各項では、これらの概念を概説すると共に、製品ライフサイクルの市販前段階における製造業者への推奨事項を例示する。なお、医療機器ソフトウェアのライフサイクル活動は、IEC 62304:2006/AMD 1:2015 に規定されている。

5.1 セキュリティ要求事項及びアーキテクチャ設計

脅威モデリング等、設計段階でサイバーセキュリティに積極的に対応することによって、受動的な市販後活動のみを行うよりも患者危害の可能性をより緩和することが可能である。このような設計インプットは、要求事項の捕捉、設計検証試験又は市販前及び市販後のリスクマネジメント対応等、製品のライフサイクルを通した様々な段階において実施される。

セキュリティ要求事項も、ライフサイクルの設計プロセスの要求事項取得の段階で特定することが望ましい。セキュリティ要求事項及びセキュリティリスクコントロール手段の情報源としては、AAMI TIR 57:2016、IEC TR 80001-2-2、IEC TR 80001-2-8、ISO 27000 シリーズ、NIST 刊行物（セキュアソフトウェア開発フレームワーク（Secure Software Development Framework：SSDF）等）、OWASP 刊行物（設計原則に基づくセキュリティ等）、ENISA 刊行物、米国ヘルスケア及び公衆衛生分野協調協議会（Healthcare and Public Health Sector Coordinating Council：HSCC）合同サイバーセキュリティワーキンググループ（Joint Cyber Security Working Group：JCWG）の刊行物（合同セキュリティ計画等）等がある。

製造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 に示した。但し、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。

	できない認証信号等がある。
ソフトウェア保守	製造業者は、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、その情報を共有することが望ましい。
	製造業者は、オペレーティングシステム、サードパーティ又はオープンソースの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ことが望ましい。また、製造業者は、ソフトウェアのアップデートや、安全でないバージョンのオペレーティングシステム上で動作する医療機器ソフトウェア等、管理対象外となった古いオペレーティングシステム環境への対処方法計画を立案することが望ましい。
	製造業者は、新たに発見されたサイバーセキュリティの脆弱性に対してセキュアであるために、医療機器のアップデート手法について検討することが望ましい。例えば、アップデートにおけるユーザ介入の要否、医療機器による自動アップデートの要否、アップデートが医療機器の安全性と性能に悪影響を及ぼさないことを検証する方法等に関する検討が含まれる。
	製造業者は、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共に、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ことが望ましい。
物理的アクセス	製造業者は、未許可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ことが望ましい。例えば、ポートを物理的にロックする、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たアクセスを禁止する等の手法を検討することが望ましい。
信頼性及び可用性	製造業者は、医療機器の基本性能を維持するため、サイバーセキュリティ攻撃を検出、防御、対応及び復旧する設計特性について検討することが望ましい。

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

セキュアな開発の原則は、セキュアな機器設計にとって必要不可欠である。現在の多くのソフトウェア開発ライフサイクルモデル又は関連規格は、この原則をはじめから組み込んでいるわけではない。医療機器ソフトウェアを開発する製造業者は、自社のソフトウェア開発にセキュリティの原則を組み込むことが重要である。製造業者には、製品の全ライフサイクルを通してリスク及び緩和策を評価することで、製品のサイバーセキュリティに関する全体的な対応が求められる。

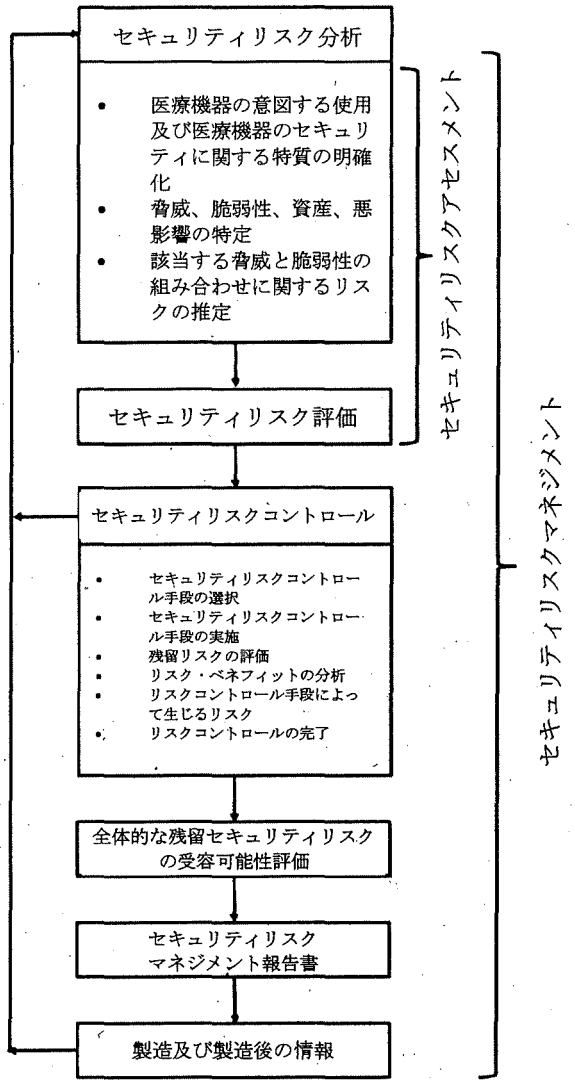


図 1. セキュリティリスクマネジメントプロセスの図解
(AAMI TIR57:2016 から許可を得て引用)

医療機器の規制に関するサイバーセキュリティのリスク分析は、サイバーセキュリティの脆弱性の悪用可能性、脆弱性が悪用された場合の患者危害の重大さを考慮して、患者危害のリスク評価に注力することが望ましい。この分析においては、補完的対策及びリスク緩和策についても検討することが望ましい。

リスク評価においては、設計を脅威モデリング、患者危害、緩和策及び検証試験と連結することにより、リスクが適切にマネジメントされるセキュアな設計アーキテクチャを確立することが重要である。この評価では、セキュリティリスク評価、脅威モデリング及び脆弱性スコアリングやその他の手法等、様々なツール及びアプローチが利用できる。

既存の ISO 14971:2019 リスクマネジメントプロセスにセキュリティリスクマネジメントプロセスを組み込む場合、脅威モデリングや脆弱性スコアリング等のセキュリティ対応を考慮することが望ましい。

5.3 セキュリティ試験

製造業者は、設計開発プロセスの検証及びバリデーションの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り、重大な既知の脆弱性がコードに含まれていないことを証明すると共に、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ことが望ましい。当該試験では、医療機器が使用される状況、並びに医療機器がその他の機器又はネットワークに接続される環境を考慮することが望ましい。ソフトウェアの仕様適合性を確保し、異常を最小化するために、ソフトウェアの検証技術を適用することが推奨される。医療機器が、悪用され得る既知の脆弱性に対して検証済みであることを明確化することも重要である。これを行うために、ソフトウェア試験や攻撃シミュレーション等、セキュリティ評価プロセス又は受入確認を対象となる医療機器に適用することが望ましい。セキュリティ試験とは、セキュアな開発フレームワークを構成するコンポーネントの一つである。試験に関する検討事項の詳細は、5.1 項に示す規格及び情報源を参照すると良い。製造業者が考慮すべき上位レベルの考慮事項を以下に例示する。

- 開発時においても、既知の脆弱性又はソフトウェアの弱点について、ソフトウェアコンポーネントとモジュールのターゲット検索を実施する。定期的なセキュリティ試験としては、静的コード解析、動的解析、堅牢性試験、脆弱性スキャン、ソフトウェアコンポジション解析等が挙げられる。

- 侵入テスト等の技術的なセキュリティ分析を実施する。技術的なセキュリティ分析としては、ファズテスト等を用いた未知の脆弱性の特定又は隠しファイル、設定、データストリーム、若しくはハードウェアのレジスタの読み出し等による代替エントリポイントのチェック等が挙げられる。

- 脆弱性評価を行う。脆弱性評価としては、バリアント解析等、自社の他製品に対する脆弱性の影響分析、対抗手段の特定、脆弱性の修正又は緩和等が挙げられる。

5.4 TPLC サイバーセキュリティマネジメント計画

サイバーセキュリティの脅威が継続的に進化している中、製造業者は、製品ライフサイクルの全体を通じたサイバーセキュリティマネジメント計画の一環として、脆弱性及び悪用を積極的に監視、特定、対応することが望ましい。製品開発の市販前段階で計画を作成することが望ましい。また、理想的には、製造業者の組織全体でその計画を維持することが望ましい。この計画では以下に示した項目を取り扱う。

- TPLC を通じた監視：新たに発見されたサイバーセキュリティの脆弱性を積極的に監視・特定すると共に、その脅威を評価して適切に対応するための計画

- 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。セキュアな設定とはマルウェア対策、ファイアウォール/ファイアウォール規則、ホワイトリスト、セキュリティイベントパラメータ、ロギングパラメータ、物理的セキュリティ検出等のエンドポイント保護を含む。

- 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、並びに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ユーザへの指示

- 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ユーザに異常を通知する方法に関する説明。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。

- 認証された特権ユーザが、医療機器の設定を保存し、回復するための方法の説明

- 許可されたユーザが、製造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。必要に応じて、セキュリティ設定又は使用環境を変更することで生じるセキュリティリスクとその影響についても説明する。

- 医療機器のサイバーセキュリティサポート終了に関する情報（6.6 項「レガシー医療機器」参照）

- 医療機器に実装される商用、オープンソース及び市販のソフトウェア部品のサイバーセキュリティに関する情報及びサポートをオペレータに提供するためのソフトウェア部品表（Software Bill of Materials : SBOM）。名前、作成元、バージョン、ビルド番号によって各ソフトウェア部品が特定されるため、SBOM を使用することで、必要とされる透明性が確保される。SBOM は、患者及びヘルスケアプロバイダを含む医療機器のオペレータが、その資産及び関連するリスクを効果的に管理し、医療機器及び接続されるシステムに対して特定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基本性能を維持するための対応を可能にする。医療機器のオペレータは、SBOM を使用することにより、脆弱性が潜んでいる可能性があるソフトウェアの特定、要件の更新及び適切なセキュリティリスクマネジメントの実施を医療機器製造業者と協力して促進することができる。SBOM を使用することにより、アプリケーションで使用されているコンポーネントを可視化して顧客に提示できると共に、潜在的セキュリティリスクを特定できるため、購入決定に必要な情報を提供することが可能となる。製造業者は、SBOM の展開で使用される形式、構文、マークアップに関する業界のベストプラクティスを活用することが望ましい。SBOM によって医療機器に関する機密情報が公開されるため、信頼できるコミュニケーションチャネルを通じて SBOM を配布することが奨励される。オペレータへの SBOM 配布方法の信頼性は製造業者が決定する。

ンポーネント又はサブシステムと既知の脆弱性データベースとの相互参照等、特定の試験に係る詳細のほか、試験報告書には、以下の事項を記載することが望ましい。

- 試験方法、結果及び結論の説明
- セキュリティリスク、セキュリティコントロール、並びにセキュリティコントロールの検証試験のトレーサビリティマトリクス
- 使用した規格及び内部 SOP/文書の参照

5.6.4 TPLC サイバーセキュリティマネジメント計画に関する文書

医療機器の全ライフサイクルを通して安全性及び性能を継続的に保証するための市販後プロセスに係る保守計画の要約である。5.4 項に記載したとおり、このプロセスとしては、TPLC 監視、計画的又は修正のためのアップデート、協調的な脆弱性の開示ポリシー及び情報共有が挙げられる。

5.6.5 ラベリング及び顧客向けセキュリティ文書

5.5 項において概説した医療機器の意図する使用環境下でユーザがリスクを効果的に管理するための関連情報を含む、サイバーセキュリティに関する全ての情報を収載したユーザ文書である。

6.0 医療機器サイバーセキュリティの市販後考慮事項

脆弱性は時間経過に伴って変化するため、市販前の設計段階で実施したセキュリティ対応は、リスクが受容可能な状態を適切に維持できない可能性がある。そのため、様々な責任関係者がそれぞれの役割を果たす市販後のアプローチが必要になる。市販後アプローチは、意図する使用環境における医療機器の運用、情報共有、協調的な脆弱性の開示、脆弱性の修正、インシデントへの対応及びレガシー医療機器等を含む様々な要素に及んでいる。製品のライフサイクルの市販後プロセスに関与する全ての責任関係者へ向けた推奨事項として、これらの要素について下項で概説する。

6.1 意図する使用環境における機器の運用

6.1.1 ヘルスケアプロバイダ及び患者

a. ヘルスケアプロバイダが採用すべきサイバーセキュリティのベストプラクティス

医療機器のサイバーセキュリティは共同責任であり、ヘルスケアプロバイダを含む全ての責任関係者の参画が必要である。ヘルスケアプロバイダは、自身の 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

b. 全てのユーザに対するトレーニング/教育

ヘルスケアプロバイダは、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、包括的に対応することが望ましい。そのため、医師、看護師、臨床工学技士、臨床検査技師等、全てのユーザのセキュリティに対する意識を高め、サイバー衛生管理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、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のトレーニング、並びに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無効化等、医療機器の異常動作を特定して通知する方法等が挙げられる。グルコース連続監視モニター、ポータブル輸液ポンプ等の在宅医療機器等、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、このようなトレーニングを患者にも行うことが望ましい。

6.1.2 医療機器製造業者

製造業者は、製品ラベリング及び顧客向けセキュリティ文書に情報を記載するほか、可能な場合には、ヘルスケアプロバイダや自社製品の販売業者及び消費者と協力して、利用者がその製品を最適な状態で使用できるように努めることが望ましい。

6.2 情報共有

情報共有は、世界経済の複数分野に渡る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重要なツールである。ヘルスケア以外の分野では、情報と脅威の共有に関する規格やベストプラクティスが作成、実施されている。医療機器関係者は、医療機器エコシステムのセキュリティを国際的に強化するため、他分野で実績のあるツールを適用することが望ましい。

リソースへのアクセス方法や使用される手法は責任関係者間で異なると共に、責任関係者の成熟度レベルも一様ではないため、有効な情報共有にも様々な方法が存在する。医療機器の種類、接続するインフラ、組織の規模及び成熟度、脅威のレベル等、幾つかの要因に係るサイバーセキュリティのベストプラクティスは、絶えず進化している。ある特定のアプローチを優先することは適切ではないため、本項では、情報共有に関する原則を提示する。なお、以下に示す事項は例示であり、要求事項を規定するものではない。

6.2.1 重要原則

- 医療機器のセキュリティに関する情報は、当該医療機器の安全な使用を確保するために、ユーザ、患者、他社の製造業者、販売業者、ヘルスケアプロバイダ、セキュリティ研究者、一般人等、その情報を必要とする全ての関係者と共有することが望ましい。
- 共有される情報は、各責任関係者にとって有意義且つ利用可能であり、対応可能なものであることが望ましい。例えば、よりセキュアなチップセットに関する情

- ヘルスケアプロバイダは、医療現場で医療機器を使用しているため、医療機器のサイバーセキュリティに関する情報の主要な生成者でもある。また、ヘルスケアプロバイダは、影響を受けた医療機器に関するフィードバックや、現実世界の環境で実施する修正策や緩和策の難易度や効果に関するフィードバックを提供できる。

d. ユーザ（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選択を行う機会が多い。ユーザが適切な判断を下すためには、明確で意味のある情報が必須である。

e. 行政及び情報共有機関を含むその他の責任関係者

- 法の執行機関、セキュリティ機関及びその他の行政機関は、医療インフラ及びその他の重要なインフラを保護するため、必要に応じて医療機器のサイバーセキュリティの脅威と脆弱性に関する情報を政府機関の各部署間で共有する必要がある。
- 情報を収集又は共有する組織や、セキュリティに関する助言若しくは専門知識を提供する組織も、セキュリティ情報の重要な情報源及びサポートリソースとなる可能性がある。これらの組織としては、 ISAO、ISAC 等の情報共有ネットワーク、コンピュータ緊急対策チーム（Computer Emergency Response Teams:CERT）等の啓発機関等の政府機関や民間機関が存在する。これらの責任関係者は、地域及び市場によって相違し得る。

6.2.3 情報の種類

サイバーセキュリティの脆弱性は、ソフトウェア及びハードウェア、自社製又はサードパーティ製の複数の製品コンポーネントに対して脅威を引き起こす可能性がある。患者危害を防ぐために共有すべき情報としては、以下に例示した事項等が挙げられる。

- 脆弱性の影響を受ける製品及びその影響の内容
- その他の製品に使用されてい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
- インシデントの確認
- パッチ及びその他の緩和策（補完的対策等）の利用可能性
- 暫定措置としての医療機器の使用と統合に関する追加指示

ことが望ましい。CVD の一環として、規制当局が情報提供する方法とタイミングは、地域によって異なる可能性がある。ただし、製造業者は、問題を評価した後、広報又は通知等を使用して、その情報を顧客に遅滞なく伝達することが望ましい。製造業者は、遅滞のない情報交換に関する各地域特有の法規制が存在することに留意することが望ましい。

ソフトウェアが搭載された医療機器を完全に脆弱性のない状態とすることは不可能であるため、CVD への取り組みを日常的な実践の一部とすることが望ましい。サイバーセキュリティに対する製造業者の評価指標は、脆弱性の開示数ではなく、その対応に係る一貫性及び適時性である。CVD は、患者の健康及び安全を改善する一助であり、医療機器のサイバーセキュリティに対する製造業者の積極的なアプローチの一部として実施されることが望ましい。積極的な CVD に関連して、製造業者は以下の事項を実施することが望ましい。

- 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を監視する。

- 協調的な脆弱性開示のポリシー及びプラクティスを採用する（ISO/IEC 29147:2014: 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が含まれる。

- 脆弱性の検出及び処理のためのプロセスを確立し伝達する（ISO/IEC 30111:2013: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、ヘルスケアプロバイダ等、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（ISO 14971:2019 等）に従って、報告された脆弱性を評価する。

- 可能であれば、緩和策を作成する。改善が不可能な場合は、展開失敗時の報告方法及び変更の初期化方法と共に、適切な脆弱性の緩和策又は補完的対策を講じる。

- 規制当局からの要求に応じて、脆弱性の開示予定に関する情報共有について規制当局と連携する。

- 責任関係者に対し、適用範囲、影響、製造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脆弱性、脆弱性の緩和策又は補完的対策に関する情報を提供する。状況が変化した場合、責任関係者にも最新情報を提供することが望ましい。

製造業者は、顧客に対する通知に加えて、自社製品の脆弱性を全世界に向けて協調的に開示することが奨励される。CERT 等の組織は、CVD プロセス全体を通して、脆弱性の発見者及び製造業者と共同で作業を行う機会が多い。特に CERT は、各地域の組織がそれぞれの言語に翻訳した勧告の発出を通じて世界的に開示する役割を果たしている。

評価によって決定されるが、リスクに対する認識に大きな乖離がある場合、適切な修正戦略について製造業者と規制当局が同意する可能性は低くなる。

製造業者及び規制当局は、リスクマネジメント、品質マネジメント及び規制に精通していない可能性があるその他の責任関係者が認識しているリスクについても考慮する必要がある。これに伴い、製造業者はセキュリティの脆弱性に対応する期限及び手法について、異なる期待が寄せられることになる。また、脆弱な医療機器を十分に保護し、患者危害のリスクを許容可能なレベルまで低減する補完的対策等のリスク低減メカニズムを理解しない責任関係者も存在する。患者へリスクを及ぼし得る不正確な情報が存在する場合、医療技術の信頼性が大きく損なわれる可能性がある。

全ての責任関係者は、医療機器に関するその他のリスクと同様に、サイバーセキュリティの脆弱性が患者及びユーザに対するリスクと同等に管理されることを認識する必要がある。

b. サードパーティ製コンポーネント

サードパーティ製コンポーネントは、ソフトウェア又はハードウェアに拘わらず、医療機器のサプライチェーンの重要な構成要素の一つである。これらのコンポーネントは、自らリスクを発生する可能性がある。当該リスクは、製造業者がリスクマネジメント、品質マネジメント及び設計の選択によって管理する。製造業者は、自社のソフトウェア及びハードウェアのコンポーネントがサイバーセキュリティに与える影響を管理することが望ましい。同様に製造業者は、サードパーティ製コンポーネントに由来する市販後の問題が医療機器のセキュリティに影響し得るリスクも管理する必要がある。ユーザは、オペレーティングシステムやプロセッサ等のコンポーネントにおけるセキュリティの脆弱性が医療機器に及ぼす影響について、製造業者が理解していることを期待する。

製造業者は、サードパーティ製コンポーネントの脆弱性に関する対応として、自社製コンポーネントの場合と同様、継続的なリスクマネジメント及び顧客やユーザとの継続的な情報共有を行うことが望ましい。製造業者がサードパーティ製品の脆弱性を解決するためのアップデートを適用するタイミングを管理することは難しいが、その場合でも製造業者は、患者及びユーザに対するリスクを低減するための対策を講じることが期待されている。

c. コミュニケーション

本文書のその他の項に記載したとおり、リスクを管理するための情報を必要とする人と明確且つ簡潔なコミュニケーションを図ることが不可欠である。このようなリスクを管理するために必要な技術的専門知識の水準を理解すべきである。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 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を含めることが望ましい。

全ての責任関係者は、アップデートの即時適用が不可能又は望ましくない場合があり、患者安全を確保する上で暫定措置が重要となり得ることを認識する必要がある。製造業者又は規制当局が直接管理することなく、責任関係者自身がこれらの対策を実施しなければならない場合は特に重要である。例えば、対策の内容によっては、病院の IT 部門以外実施できない場合がある。正しい修正戦略の実行性は、効果的な情報共有とユーザやメディア等の責任関係者の管理に依存している。なお、理想的な修正であっても、必ずしも実施できない場合があることに留意する必要がある。その場合は、適切なリスク緩和策及び補完的対策を適用することが望ましい。

6.4.2 ヘルスケアプロバイダ及び患者

a. アップデート

患者は専門の医療機関及び在宅医療環境において医療を受けるが、アップデート適用については、使用環境毎に考慮すべき特有の事項がある。[2] 例えば、在宅医療環境においては、患者、介護者、信頼できる隣人又は家族の一員がユーザとなり得る。本項では、アップデート適用に関する一般的な指針及び各使用環境に固有な考慮事項について概説する。

IEC 62304:2006+AMD1:2015 「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」の 6.2.5 項では、リリースした医療機器ソフトウェアの問題、変更の入手及びインストール方法について、製造業者がユーザ及び規制当局に通知することを要求している。製造業者が指定し、規制当局が承認した医療機器の特定のユーザは、製造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る。この特定ユーザは、製造業者の指針に従って、Web ページで提供されるサービス報告書及びその他の情報にアクセスすることが望ましい。

妥当な期間内にアップデートが適用できない場合、製造業者は、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設定の変更を推奨する可能性がある。規制当局は、特定の種類の脆弱性に対する患者危害のリスクを低減するため、製造業者に対して医療機器、付属品又はソフトウェア更新サーバ等の支援システムにおける特定の機能の無効化を指示する可能性がある。いずれの場合も、ユーザは製造業者の指針に従い、必要に応じて使用環境に関連するリスクを評価することが望ましい。[3]

[2] IEC 60601-1-11:2015 医用電気機器-第 1-11 部：基礎安全及び基本性能に関する一般要求事項 – 副通則：在宅医療環境における医用電気機器及び医用電気システムに対する要求事項では、「在宅医療環境」を専門の医療施設を除く、患者の居住地又は患者がいるその他の場所と定義している。例として、「自動車、バス、列車、船、飛行機の中、車椅子及び屋外の歩行」が挙げられている。
[3] 特定の状況ではユーザがリスクを適切に評価できないことが認識されている。

「医療機器自体に対するリスクコントロール手段は、取扱説明書又は医療機器製造業者の文書による許可に従って、医療機器製造業者又は責任組織が実施することが望ましい。医療機器製造業者の文書による同意がない場合、責任組織が医療機器に行ういかなる変更も推奨されない。」

これらの推奨事項は、医療 IT ネットワークの効果的で安全な管理を確保するために作成された。一般人には、医療 IT ネットワークに接続される医療機器にアップデートをインストールする許可を与えるべきではない。

IEC 80001-1 に記載されているとおり、責任協定書は、医療 IT ネットワーク機器を管理する上で、全ての当事者が共有責任を有することを確実に理解するための選択肢の一つである。製造業者が、医療機器の特定の機能を無効にするように指示している場合、ヘルスケアプロバイダは、患者安全の維持を確保するために、臨床ワークフローを評価することが望ましい。

c. 在宅医療環境における考慮事項

FDA ガイダンス「家庭での使用を目的とした機器に関する設計上の検討事項」に記載されているとおり、在宅医療環境では、多様な潜在的ユーザに対応する必要がある（以下参照）。

「在宅医療機器のユーザは、専門の医療施設で医療機器を操作する医療専門家と異なる。在宅医療機器のユーザは、身体的、感覚的及び認知的な能力及び障害、並びに感情的に幅広い違いを有する可能性があることを在宅医療機器の設計で考慮することが望ましい。」

在宅医療環境におけるアップデート適用については、医療機器のリスクのクラス分類、高速インターネット通信等のリソース要求事項及びユーザビリティを含む多くの要因を考慮する必要がある。ユーザの能力が大きく異なるため、多くの在宅医療機器では、表 2 に示した「サービス訪問」によるアップデート適用が必要となる。埋め込み型医療機器に対するアップデート適用については、患者のヘルスケアプロバイダとの直接的な連携が必要になる場合がある。

一部の在宅医療機器、特に SaMD に分類される製品等においては、リモートアップデート又はユーザ管理によるパッチ適用に対応しているものがある。リモートアップデートは、ユーザとの最小限の連携をもって実施できるが、ヘルスケアプロバイダが確立したプロセスに従って、患者との合意形成を必要とすることが多い。いずれのアップデート適用方法においても、患者は、ヘルスケアプロバイダ又は製造業者の指示に従うことが望ましい。

各種ソフトウェア保守作業に対する規制当局の監視を検討するための、規制当局向けの推奨フレームワークを表 3 に示した。この表に示されたレベルは規範的なものではなく、規制当局の監視に関して推奨される相対的なレベルの指針を示したものである。

アップデートの目的		提案された規制当局の要求レベル	例
セキュリティ強化（サイバー衛生管理）		低	SaMD アプリケーションの製造業者が、多層防御戦略の支援に関するセキュリティコントロールを追加するためのホストオペレーティングシステムのアップデートを通知する。SaMD アプリケーションは、ホストオペレーティングシステムのインタフェース変更に伴い、互換性に関する変更が必要である。関連する SaMD アプリケーションの変更は、既知の脆弱性と無関係である。
脆弱性の修正又は修正できない脆弱性に関するリスク低減戦略	患者危害の残留リスク：受容可能（脆弱性 A）	中	医療機器の製造業者は、血液ガス分析装置がマルウェアに感染し、データを改変し得る懸念に関するクレームをユーザから受けた。製造業者の調査及び影響評価の結果、マルウェアの存在が確認されたが、マルウェアは暗号化されていない保存データ及び通信データを改変しないことが判明した。医療機器の安全性及び基本性能はマルウェアによって影響を受けないことから、製造業者はリスクアセスメントを通じて、脆弱性による患者危害のリスクが受容可能であると判断した。[6]
	患者危害の残留リスク：受容不能（脆弱性 B）	高	製造業者は、使用していない通信ポートが開放されていることを指摘された。製造業者は、脆弱性発見者に対して脆弱性レポートの受領確認を行い、その後に行った解析において、設計上、医療機器の安全性及び基本性能を損ない得る許可されないファームウェアがダウンロードされることを防御できないことを確認した。脆弱性に関連する重大な有害事象又は死亡例は報告されていないが、リスクアセスメントによって、患者危害のリスクは受容できないと結論付けられた。[7]

[6] FDA ガイダンス「医療機器サイバーセキュリティの市販後管理」（2016 年 12 月）の記載例を一部変更した。
[7] 同上。

員は、同一又は類似の作業に対して責任を持つことが望ましい。これらのグループの役割に関する詳細情報は、附属書Aに示した。

b. コミュニケーションに対する期待

製造業者は、サイバーセキュリティのインシデントやその他の事象を報告する連絡先情報を顧客に提供することが望ましい。通常の顧客サービス受付を通してサイバーセキュリティのインシデントやその他の事象を通知しても良い。インシデント対応チームは、インシデントの影響を受ける全ての責任関係者と最新情報を共有するための日常的な活動体制を確立し、最初の発見後、可能な限り早急に顧客へ適切な情報を提供する必要がある。製造業者は遅滞なく情報共有するための特定の管轄要件を策定しておくことが望ましい。インシデント発生直後における製造業者による報告書又は通知の発行可否については、顧客に対し遅滞なく正確な情報共有を実施可能であるかに依存する。

製造業者は、患者安全及びプライバシーに影響する医療機器のサイバーセキュリティのインシデントを規制当局に報告しなければならない。調査の過程で犯罪行為が特定された場合は、所管の適切な法執行機関に通知しなければならない。CERT 及び ISAO はグローバルなサイバーセキュリティの攻撃及び事象に関して更なる連携強化を図るべきである。

6.5.2 ヘルスケアプロバイダ

ヘルスケアプロバイダは、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確立することが望ましい。その一環として、ヘルスケアプロバイダは、脆弱性の緩和に関する計画とリソース管理について検討することが望ましい。この措置には、インシデント対応中、必要に応じて代替機器を提供するための費用も含まれる可能性がある。

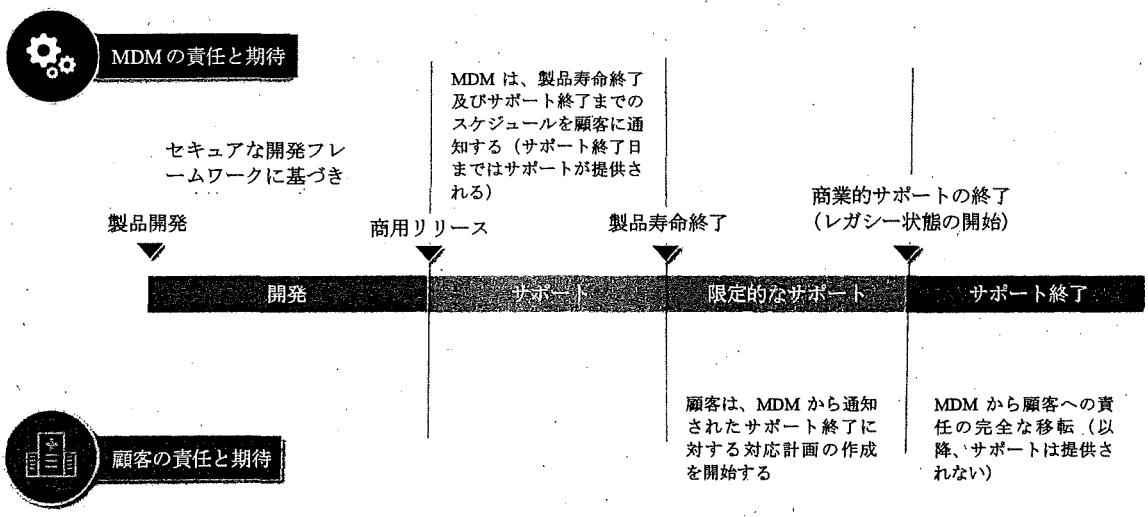
a. ポリシー及び役割

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は、ヘルスケアプロバイダの組織にも整備されていることが望ましい。ヘルスケアプロバイダは、MDS2（Manufacturer Disclosure Statement for Medical Device Security : MDS2）、SBOM、脆弱性及びアップデート情報等の製造業者の開示文書、情報共有機関又は参画している ISAO からの情報を受領し、広範に共有する方法を確立することが望ましい。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・検証する必要がある。また、医療機器の納入前に締結し且つ定期的に見直すサービスレベル契約（Service Level Agreements : SLAs）には、インシデント対応中に製造業者及びその他のベンダーが遵守すべき事項を記載しなければならない。ヘルスケアプロバイダは、独自のインシデント対応チームを設立することが奨励される。

療機器の寿命に関する新たな要求が発生した。このような組み合わせは、スキャナハードウェア等の資本設備及び一般消費財に該当するサーバ、ワークステーション、データベース及びオペレーティングシステム等のコンポーネントから構成されることが多い。ただし、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。発売開始から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、発売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、発売から 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。

医療機器の設計開発ステージから始まる、サイバーセキュリティの TPLC に関する取り組みとして、医療機器のライフサイクル全体を通じてサイバーセキュリティの脅威に対する合理的な保護手段の効果を維持することの重要性が増している。このような取り組みによって、医療現場で現在使用されている様々なレガシー医療機器に起因する不均衡（ヘルスケアプロバイダとそのネットワークに起因するセキュリティ上の脅威）が低減される。本文書の以下の項目では、医療機器サイバーセキュリティの理想的な将来像、すなわち、事業継続計画の作成にあたり、ヘルスケアプロバイダに対して必要な情報を事前に通知し、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レガシー医療機器の使用を終了又は段階的に使用を終了するための概念フレームワークについて詳述する。（図2参照）。

サイバーセキュリティ及び製品ライフサイクルの全体



*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が、サポートレベルは顧客との契約に応じて異なる。

図2. サイバーセキュリティに関する製品ライフサイクルの機能として表現したレガシー医療機器の概念フレームワーク

が終了する可能性を考慮すると共に、サポート終了によって医療機器のセキュアな運用に悪影響が及ぶ可能性を考慮することが望ましい。

b. 将来のレガシー医療機器の数を最小限に抑えることを目的としたセキュアな開発フレームワークに基づいて医療機器を設計開発する。このような医療機器については、少なくともセキュリティ基準に適合し、アップデート及びパッチの適用を可能とする環境を整備することが望ましい。

- サポート:

a. リスクマネジメントの一環として、医療機器における受容できないリスクのある脆弱性の存在可否を監視し、可能な限り最善の対応を行い、製品の全ライフサイクルの各段階に応じたリスク関連文書を継続的に更新する。

b. 医療機器の購入及び設置プロセスの一環として、各時点における顧客の責任と併せて、医療機器のサイバーセキュリティ EOL 日等、ライフサイクルの主要なマイルストーンを明確に通知する。

c. 顧客に対し、サードパーティによる機器部品のサポート終了を事前に通知する。

d. サイバーセキュリティ EOS 日まで限定的なサポートを継続することを顧客に通知する。EOS 日以降、当該医療機器はサポート対象外となってレガシー状態となる。この情報は、EOL 日が近づいた時点で顧客に通知することが望ましい。これにより、ヘルスケアプロバイダは、医療機器の使用終了又は段階的な使用終了及び事業継続計画作成のための十分な時間を確保できる。このような情報を明確に通知することにより、医療機関は、自身の責任及び導入する医療機器のリスクを理解することが可能となり、医療機器の使用終了及び交換に関する計画と予算を作成することができる。

- 限定的なサポート（EOL 開始点）:

a. 顧客が EOS 及び関連する責任に備えるための十分な時間を確保できるように、サイバーセキュリティ EOS 日に関するスケジュールを引き続き通知する。

b. 上記の「サポート」の項目に記載した作業「a」及び「c」を引き続き行う。

- サポート終了（レガシー状態開始点）：

a. 製造業者から顧客に責任が完全に移転される。当該医療機器に関する正式なサイバーセキュリティ EOS 日以降、そのユーザは、いかなるレベルのサポートも期待しないことが望ましい。

- サポート終了:

  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引き受ける。

7.0 参考文献

7.1 IMDRF 文書

1. Software as a Medical Device: Possible Framework for Risk Categorization and Corresponding Considerations IMDRF/SaMD WG/N12:2014 (September 2014)

2. Essential Principles of Safety and Performance of Medical Devices and IVD Medical Devices IMDRF/GRRP WG/N47 FINAL:2018 (November 2018)

7.2 規格

3. AAMI TIR57:2016 Principles for medical device security—Risk management

4. AAMI TIR 97:2019, Principles for medical device security—Postmarket risk management for device manufacturers

5. IEC 60601-1:2005+AMD1:2012, Medical electrical equipment - Part 1: General requirements for basic safety and essential performance

6. IEC 62304:2006/AMD 1:2015, Medical device software – Software life cycle processes

7. IEC 62366-1:2015, Medical devices - Part 1: Application of usability engineering to medical devices

8. IEC 80001-1:2010, Application of risk management for IT-networks incorporating medical devices - Part 1: Roles, responsibilities and activities

9. 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

10. 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

11. ISO 13485:2016, Medical devices – Quality management systems – Requirements for regulatory purposes

12. ISO 14971:2019, Medical devices – Application of risk management to medical devices

27. FDA: Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software (January 2005)

28. FDA: Design Considerations for Devices Intended for Home Use (November 2014)

29. FDA: Postmarket Management of Cybersecurity in Medical Devices (December 2016)

30. Germany: Cyber Security Requirements for Network-Connected Medical Devices (November 2018)

31. Health Canada: Pre-market Requirements for Medical Device Cybersecurity (June 2019)

32. 平成 27 年 4 月 28 日付薬食機参発 0428 第 1 号・薬食安発 0428 第 1 号：厚生労働省大臣官房参事官・医薬食品局安全対策課長通知「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」

33. 平成 30 年 7 月 24 日付薬生機審発 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」

34. Singapore Standards Council Technical Reference 67: Medical device cybersecurity (2018)

35. TGA: Medical device cybersecurity - Consumer information (July 2019)

36. TGA: Medical device cybersecurity guidance for industry (July 2019)

37. TGA: Medical device cybersecurity information for users (July 2019)

7.4 その他の資料及び参考文献

38. CERT® Guide to Coordinated Vulnerability Disclosure
https://resources.sei.cmu.edu/asset_files/SpecialReport/2017_003_001_503340.pdf

39. The NIST Cybersecurity Framework
https://www.nist.gov/cyberframework

40. 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

41. Medical Device and Health IT Joint Security Plan (January 2019)
https://healthsectorcouncil.org/wp-content/uploads/2019/01/HSCC-MEDTECH-JSP-v1.pdf

42. MITRE medical device cybersecurity playbook (October 2018)

8.0 附属書

	のサービスを提供する	c) インシデントを調査し、復旧作業をサポートする d) 対象インシデントの脆弱性分析を行う e) マネージャが指示したその他の活動を行う
実施グループ	インシデント対応に関する作業全般を実施する	a) インシデント対応の要求事項を分析する b) インシデント対応のポリシーとレベルを決定する c) インシデント対応のポリシーと計画を実施する d) インシデント対応計画を提案する e) インシデント対応作業の内容と報告を要約する f) インシデント対応に必要な資源を展開して利用する g) マネージャが指示したその他の活動を行う
分析グループ	インシデント分析を行う	a) チームと製造業者のための脆弱性分析を計画する b) セキュリティ分析のためのツールとチェックリストを改善する c) 監視規則を改善する d) ニュースレターを発行する e) マネージャが指示したその他の活動を行う

日本
Japan Computer Emergency Response Team/Coordination Center(JPCERT コーディネーションセンター:JPCERT/CC)
https://www.jpcert.or.jp/vh/top.html or https://www.jpcert.or.jp/english/

シンガポール
SingCERT
https://www.csa.gov.sg/singcert/news/advisories-alerts

米国
Industrial Control Systems CERT(産業制御システム CERT:ICS-CERT)
https://www.us-cert.gov/ics

US CERT(CERT 米国)
https://www.us-cert.gov/