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

本文書は、国際医療機器規制当局フォーラムによって作成された。本文書の複製又は使用に関する制限はない。ただし、本文書の一部又は全てを他の文書に組み込む場合、並びに本文書を英語以外の言語に翻訳する場合、国際医療機器規制当局フォーラムは、その責任を一切負わない。

Copyright © 2020 by the International Medical Device Regulators Forum

目次

1.0 はじめに 5
2.0 適用範囲 6
3.0 定義 7
4.0 一般原則 9
4.1 国際整合 10
4.2 製品ライフサイクルの全体 10
4.3 共同責任 10
4.4 情報共有 10
5.0 医療機器サイバーセキュリティの市販前考慮事項 11
5.1 セキュリティ要求事項及びアーキテクチャ設計 11
5.2 TPLC に関するリスクマネジメント原則 14
5.3 セキュリティ試験 17
5.4 TPLC サイバーセキュリティマネジメント計画 17
5.5 ラベリング及び顧客向けセキュリティ文書 18
5.5.1 ラベリング 18
5.5.2 顧客向けセキュリティ文書 18
5.6 規制当局への申請に関する文書 20
5.6.1 設計文書 20
5.6.2 リスクマネジメント文書 20
5.6.3 セキュリティ試験の文書 20
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 21
5.6.5 ラベリング及び顧客向けセキュリティ文書 21
6.0 医療機器サイバーセキュリティの市販後考慮事項 21
6.1 意図する使用環境における機器の運用 21
6.1.1 ヘルスケアプロバイダ及び患者 21
6.1.2 医療機器製造業者 23
6.2 情報共有 23
6.2.1 重要原則 23
6.2.2 重要な責任関係者 24

6.2.3 情報の種類 25
6.2.4 信頼できるコミュニケーション 26
6.3 協調的な脆弱性の開示 26
6.3.1 医療機器製造業者 26
6.3.2 規制当局 28
6.3.3 脆弱性の発見者(セキュリティ研究者及びその他の脆弱性発見者を含む)..... 28
6.4 脆弱性の修正 28
6.4.1 医療機器製造業者 28
6.4.2 ヘルスケアプロバイダ及び患者 31
6.4.3 規制当局 34
6.5 インシデントへの対応 36
6.5.1 医療機器製造業者 36
6.5.2 ヘルスケアプロバイダ 37
6.5.3 規制当局 38
6.6 レガシー医療機器 38
6.6.1 医療機器製造業者 40
6.6.2 ヘルスケアプロバイダ 42
7.0 参考文献 43
7.1 IMDRF 文書 43
7.2 規格 43
7.3 規制当局のガイダンス 44
7.4 その他の資料及び参考文献 45
8.0 附属書 47
8.1 附属書 A: インシデント対応の役割(ISO/IEC 27035 から引用) 48
8.2 附属書 B: 協調的な脆弱性の開示に関する各地域のリソース 50

序文

本文書は、世界各国の医療機器規制当局の団体である国際医療機器規制当局フォーラム(International Medical Device Regulators Forum: IMDRF)が協議の上、作成されたものである。本文書は、自由に複製、配布、使用して構わない。

ただし、本文書の一部又は全てを他の文書に組み込む場合、並びに本文書を英語以外の言語に翻訳する場合、IMDRFは、その責任を一切負わない。

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。

2.0 適用範囲

本文書は、全ての責任関係者に向けて、医療機器（IVD 医療機器を含む）のサイバーセキュリティに対する一般原則に係る基本的考え方と検討事項、並びに推奨されるベストプラクティスを提供することを目的として作成された。本文書では、製造業者、ヘルスケアプロバイダ、規制当局及びユーザに向けて、意図する目的に対して医療機器を使用する際に起こり得るサイバーセキュリティリスクを最小化することにより、医療機器の安全性及び性能を維持し、継続使用を確保するための具体的な推奨事項を取りまとめている。本ガイダンスで述べるヘルスケアプロバイダには、医療機関が含まれる。

本文書では、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等のソフトウェアを有する医療機器（例：ペースメーカ、輸液ポンプ）、又はソフトウェア単独で存在する医療機器（例：SaMD）に関するサイバーセキュリティについて概説されている。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、本文書の適用範囲は、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、若しくは誤った診断又は治療に繋がるサイバーセキュリティリスクは、本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、本文書では適用範囲から除外する。さらに、本文書では、製造業者の企業活動に関するサイバーセキュリティを適用範囲から除外する。製造業者の企業活動のセキュリティに関するベストプラクティスについては、米国国立標準技術研究所（National Institute of Standard and Technology：NIST）のサイバーセキュリティフレームワークが情報源としての重要な役割を果たしている。

本文書は以下の事項を意図している。

- 医療機器の設計及び開発に適切なサイバーセキュリティ対応を組み込むために、リスクベースアプローチを採用する。

- 医療機器及び接続されるヘルスケアインフラの安全性、性能及びセキュリティを確保する。

- サイバーセキュリティは、製造業者、ヘルスケアプロバイダ、ユーザ、規制当局及び脆弱性発見者等を含む全ての関係者の共同責任であることを認識する。

- それらの関係者に対して、製品ライフサイクルの全体に渡り、患者危害のリスクを最小化するために有益な推奨事項を提供する。

- 用語を定義すると共に、医療機器のサイバーセキュリティを確保するため、現時点のベストプラクティスを記載する。

- 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）

3.9 協調的な脆弱性の開示（Coordinated Vulnerability Disclosure：CVD）：研究者及びその他の責任関係者が、脆弱性の開示に関連するリスクを低減するための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、脆弱性とその解決策に関する情報の報告、調整、開示等の作業が含まれる。

3.10 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。（ISO 81001-1）

3.11 製品寿命終了（End of Life：EOL）：製品のライフサイクルにおいて、製造業者の定義に基づき有効期間を超えた製品の販売を終了する時点。EOL を迎えた製品については、正式な EOL プロセス（ユーザへの通知等）が実施される。

3.12 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。

3.13 基本性能：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時に受容できないリスクを生じる性能（IEC 60601-1:2005+AMD1:2012）

3.14 悪用（Exploit）：脆弱性を通じて情報システムのセキュリティを侵害するための明確な方法（ISO/IEC 27039:2015）

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

3.16 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

3.17 否認防止（Non-Repudiation）：発生した事象又は行動、並びにそれらを引き起こしたエンティティを証明する能力（ISO/IEC 27000:2018）

3.18 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)

3.19 プライバシー（Privacy）：個人に関するデータの過度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）

3.20 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

ために重要であり、これに従うことで、患者の安全を確保する上で有益な効果を得られることが期待される。

4.1 国際整合

医療機器のサイバーセキュリティは、国際的に注目されている。セキュリティのインシデントは、診断若しくは治療の過失を引き起こす、機器の安全な性能を脅かす、臨床活動に影響を与える、患者の救急救命の利用を妨げること等によって、世界中のヘルスケアシステムの患者安全を脅かす可能性がある。サイバーセキュリティに対する取り組みの国際的整合は、イノベーションを促進し、安全で効果的な医療機器を遅滞なく患者の治療に使用可能とすると共に、患者安全の維持を確保するために必要である。全ての責任関係者は、医療機器の全ライフサイクルに渡ったサイバーセキュリティ対応を国際整合させることが奨励される。これには、製品設計、医療機器の全ライフサイクルを通したリスクマネジメント、医療機器のラベリング、規制当局への申請に対する要求事項、情報共有、市販後活動に関する整合化が含まれる。

4.2 製品ライフサイクルの全体

サイバーセキュリティの脅威及び脆弱性に関するリスクは、初期構想段階から EOS に至る、医療機器の製品寿命に関する全ての段階を通して検討することが望ましい。サイバーセキュリティの動的特性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の全ライフサイクルに渡って適用し、設計、製造、試験及び市販後監視等の各過程においてサイバーセキュリティリスクを評価及び緩和することが望ましい。

安全性とセキュリティとのバランスを図ることも必要である。製造業者は、サイバーセキュリティのコントロール及び緩和策を組み込む際、医療機器の安全性及び基本性能を維持することが重要である。

4.3 共同責任

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

4.4 情報共有

サイバーセキュリティに関する情報の共有は、安全でセキュアな医療機器を実現するための TPLC アプローチの基礎原則である。サイバーセキュリティの情報を共有するため、全ての責任関係者が、市販前及び市販後に積極的に対応することが奨励される。遅滞なく情報が共有されることによって、全ての責任当事者が、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。その一環として、全ての責任関係者は、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：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。

設計原則	説明
セキュアな通信	製造業者は、医療機器が併用機器又はネットワークと接続される方式について検討することが望ましい。接続方式には、有線接続及び無線通信が含まれる。接続方式の例としては、Wi-Fi、イーサネット、bluetooth、USB 等が挙げられる。
	製造業者は、外部からの入力のみでなく、全ての入力の検証機能を設計することについて検討し、安全性が低い通信以外サポートされていない医療機器や、家庭内ネットワーク又はレガシー医療機器と接続して通信する等、外部環境と通信する場合を考慮することが望ましい。
	製造業者は、医療機器の送受信データ転送を不正アクセス、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ことが望ましい。例えば、製造業者は医療機器/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、予め定めた時間設定後に通信を切断する適切性等について検討することが望ましい。
データ保護	製造業者は、医療機器に保存される又は送受信される安全性関連データを暗号化等により保護する要否について検討することが望ましい。例えば、パスワードは暗号化によって保護されたハッシュとして保存することが望ましい。
	製造業者は、通信プロトコルのメッセージ制御、シーケンス領域を保護するため又は暗号鍵材料の内容が漏洩することを防ぐために、機密性に係るリスクコントロール手段の要否について検討することが望ましい。
機器の完全性	製造業者は、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、監査ログ機能のサポート等、システムレベルのアーキテクチャを評価することが望ましい。
	製造業者は、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ことが望ましい。
	製造業者は、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ことが望ましい。
ユーザの認証	製造業者は、医療機器の使用者の検証、様々なユーザ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、ユーザのアクセス制御について検討することが望ましい。また、複数の医療機器や顧客の間で同じ認証情報を共有しないことが望ましい。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生成

	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。

5.2 TPLC に関するリスクマネジメント原則

セキュリティと安全性に関する健全なリスクマネジメント原則が、医療機器のライフサイクルを通して組み込まれていることが望ましい。医療機器の安全性と基本性能又は臨床活動に影響を及ぼす、若しくは誤った診断又は治療に繋がるサイバーセキュリティリスクについても、リスクマネジメントプロセスにおいて検討されることが望ましい。製造業者は、ISO 14971:2019 に規定されているリスクマネジメント及び AAMI TIR57:2016 や AAMI TIR97:2019 等で規定されているサイバーセキュリティリスクマネジメントを使用して、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の脆弱性を特定する
- 関連するリスクを推定し、評価する
- リスクを受容可能なレベルまでコントロールする
- リスクコントロールの有効性を評価・監視する
- 重要な責任関係者に対する協調的な情報開示を通じて、リスクに関する情報を提供する

セキュリティリスクマネジメントプロセスを図 1 に示した（AAMI TIR57:2016 から引用）。これは、全体的なリスクマネジメントの一部を構成するリスクマネジメントプロセスとして実施できると共に、脆弱性、脅威及びその他のセキュリティ関連用語を対応させて、ISO 14971:2019 のリスクマネジメントプロセスに組み込むこともできる。対応付けについては ISO/TR 24971:2020 の附属書 F を参照すること。

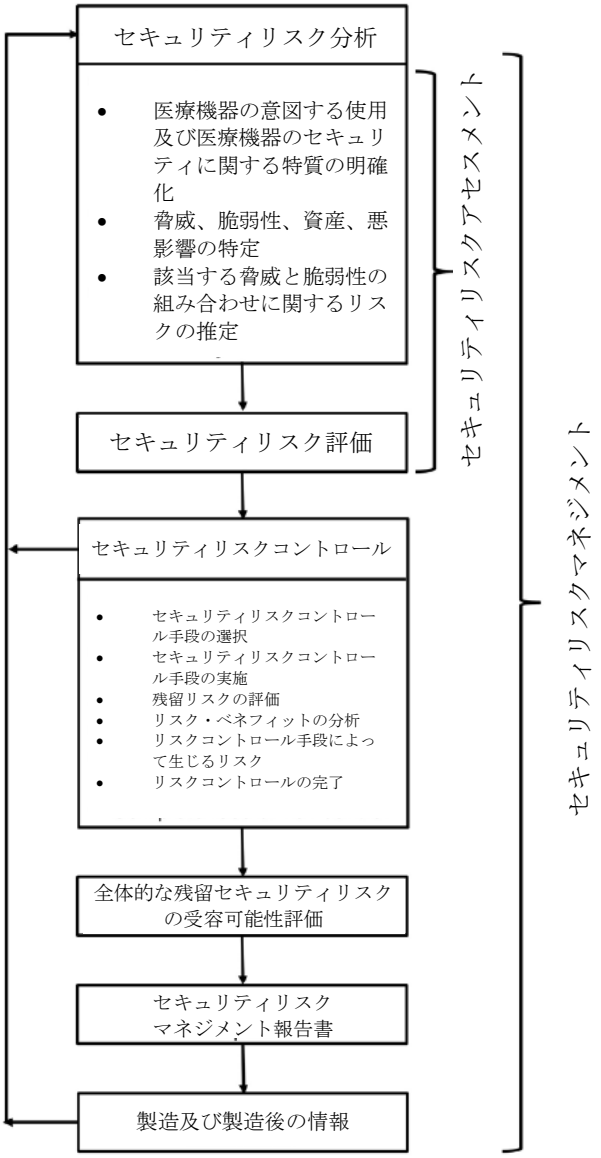

図 1.　セキュリティリスクマネジメントプロセスの図解
(AAMI TIR57:2016 から許可を得て引用)

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。

- セキュリティリスクアセスメント：製造業者は、製品の全ライフサイクルを通して、サイバーセキュリティリスク、脅威及び対応について検討することが望ましい。特定されたハザードに対する緩和策の場合、サイバーセキュリティの要求事項は、可能な限り、特定の医療機器のサイバーセキュリティの脅威及び脆弱性と相互参照することが望ましい。

- 脅威モデリング：脅威モデリングは、医療機器やシステムにおける潜在的な脅威によるリスクを特定、列挙、緩和するプロセスである。特に、脅威モデリングには、システムコンポーネント等のサプライチェーンに関連するリスクや、設計、製造、病院環境等への展開、保守に関連するリスク等の検討が含まれる。詳細なシステム設計図の作成は、サイバーセキュリティの設計要素を医療機器に組み込む手法を理解するために有益であると共に、脅威モデリングにとっても有用である。製造業者は、脅威モデルを作成する際、OWASP のガイダンスに基づいて、サイバーセキュリティに関する基本的な 4 つの質問に対する回答について検討することが望ましい。

    1) 何を構築しようとしているのか？
    2) どのような問題が発生し得るか（どのような攻撃を受ける可能性があるか）？
    3) その問題に対してどのように対処するか？
    4) 十分な対策を行ったか？

- 必要に応じて、アプリケーションアーキテクチャ、運用データフロー又はより広範囲なシステムレベルの脅威モデリングのコンテキストにおいて、これらの質問を行うこと。医療機器に発生し得る問題を脅威モデリングにおいて判断する場合、製造業者は、ソフトウェア及びハードウェアに対する故意でない誤設定又はインターネットに接続するよう設計されていない医療機器をインターネットに接続する等の悪意のある誤設定を考慮することが望ましい。

- 脆弱性スコアリング：脆弱性スコアリングは、サイバーセキュリティ脆弱性の悪用可能性及び重大さを明確化して評価する方法である。設計開発において特定される既知の一般的脆弱性曝露（Common Vulnerabilities and Exposures：CVE）については、共通脆弱性スコアリングシステム（Common Vulnerability Scoring System：CVSS）又は今後広く採用される可能性が高い脆弱性スコアリングシステム等の一貫性のある脆弱性スコアリングの方法を用いて分析・評価することが望ましい。サイバーセキュリティリスク、脆弱性スコアリング及びコントロール手段は新製品の脅威モデリング及びセキュリティリスクアセスメント、並びに故障モード影響解析（Failure Mode and Effects Analysis：FMEA）等、サイバーセキュリティに特化していない他のリスク評価ツールに対して情報を提供するために使用される可能性がある。

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

- 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責任関係者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

- 復旧：製造業者、ユーザ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復旧計画

- 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 ISAO 又は情報共有分析センター（Information Sharing and Analysis Centers：ISAC）への参加

5.5 ラベリング及び顧客向けセキュリティ文書

5.5.1 ラベリング

ラベリングは、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エンドユーザに伝達するものである。ラベリングには、以下に示した項目を含めることが望ましい。

- アンチマルウェアソフトウェア、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フェースのリスト、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が望ましいことに留意する。

- エンドユーザ向けの詳細なシステム構成図

5.5.2 顧客向けセキュリティ文書

取扱説明書に加えて、製造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は、ユーザが医療機器を安全でセキュアに使用する上で特に重要である。顧客向けセキュリティ文書については、以下に示した項目を含めることが望ましい。

- 意図したとおりの医療機器の動作を確保するための、支援インフラの要求事項に関するユーザ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。

5.6 規制当局への申請に関する文書

製造業者は、上項に概説した対応に加えて、サイバーセキュリティに関する自社の活動を明確に文書化し、要約することが望ましい。規制当局は、医療機器のクラス分類に応じて、サイバーセキュリティ対応に関する文書を市販前又は市販後の段階で要求する可能性がある。規制当局が市販前承認のためにサイバーセキュリティ文書を要求する場合、製造業者は、サイバーセキュリティに関連して、医療機器の設計機能、リスクマネジメント活動、検証試験、ラベリング及び製品の全ライフサイクルに渡って新たに発生する脅威を監視し、対応するための計画の根拠を明確に記載した文書を提出することが望ましい。これらの詳細については、下項で説明する。

5.6.1 設計文書

全てのインタフェース又は通信経路又はコンポーネント（ハードウェア及びソフトウェア）、患者危害に関するサイバーセキュリティのリスクを緩和するために、アクセスコントロール、暗号化、セキュアなアップデート、ログ機能、物理的セキュリティ等に関する対策を選択した根拠及び推定を中心として、5.1 項で概説した全ての設計機能を記載した文書である。

5.6.2 リスクマネジメント文書

サイバーセキュリティの脅威及び脆弱性、関連するリスクの推定、リスクを緩和するために行うリスクコントロール、並びにリスクコントロールが適切に検証されたことを示す根拠を明確に説明する文書である。製造業者は、その他の安全性に過度な影響を与えることなく、医療機器のサイバーセキュリティを最大化するリスクコントロールについて検討することが望ましい。特に、規制当局に提出するサイバーセキュリティに関連するリスクマネジメント文書では、明確な説明を心掛けると共に、リスクマネジメント規格（AAMI TIR57:2016、AAMI TIR97:2019 等）をガイダンスとして利用することが望ましい。この成果文書を全体的なリスクマネジメントの入力として利用できるように、ISO 14971:2019 で規定されている全体的な要件に従って成果文書を作成することが望ましい。サイバーセキュリティに関するリスクマネジメント文書には、以下のような文書がある。

- リスクマネジメント報告書やセキュリティリスクマネジメント報告書等の包括的なリスクマネジメント文書。これらの文書には、脅威モデリング及び特定されたサイバーセキュリティの脅威について記載することが望ましい。
- その他のリスクマネジメントに与えるセキュリティリスク緩和策の影響に関する考察

5.6.3 セキュリティ試験の文書

医療機器のセキュリティ及び全てのセキュリティコントロールの有効性を検証するために実施した全ての試験を要約した試験報告書である。 5.3 項に記載したソフトウェアコ

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

マネジメントプロセスの採用について検討することが望ましい。このプロセスは、以下のステージで適用することが望ましい。

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

ヘルスケアプロバイダがこれらのリスクマネジメントプロセスを実行する上で、IEC 80001-1 及び ISO 31000、並びに ISO 27799 を中心とした ISO 27000 シリーズ等の関連規格が参考となる。「医療産業のサイバーセキュリティ手法：脅威の管理と患者の保護」も、参考文書として利用できる。

ヘルスケアプロバイダは、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を維持するために、以下に示した一般的なサイバーセキュリティのベストプラクティスを導入することが望ましい。但し、以下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。

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

これらのベストプラクティスは、医療機器の臨床使用状況を考慮して実施することが望ましい。例えば、救急時等では、これらのベストプラクティスの幾つかの実施が難しい可能性がある。上記の手法の多くは、NIST のサイバーセキュリティフレームワークに記載されている。

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

報は、製造業者にとって重要と考えられるが、医療機器のエンドユーザには必ずしも特段の利益となり得ない。
- 共有される情報は、患者の安全性向上に繋がるため、商業的利益とは関係なく必要に応じて自由且つ確実に共有されることが望ましい。
- 様々な地域の責任関係者が適切に対応できるように、国際的に一貫性のある情報を必要に応じて各地域間で可能な限り同時に共有することが望ましい。

6.2.2 重要な責任関係者

現在、医療機器分野のグローバル化が進んでいるが、医療機器の製造販売については、各国毎に規制されている。複数の市場に医療機器を供給する製造業者は、情報共有について国内又は地域内の推奨事項のみでは不十分な可能性があるため、医療機器のセキュリティに関するグローバルな情報共有戦略を設ける必要がある。責任関係者は複数のネットワークを使用する際、利用するネットワークが国際的なネットワークである可能性があることを認識する必要がある。

a. 規制当局

- 医療機器のセキュリティに関する情報の重要な受信者であり、その情報の周知についても関与することが多い。
- 医療機器のサイバーセキュリティに関する情報を遅滞なく開示するプロセスの構築を目指すことが望ましい。このようなプロセスには、サイバーセキュリティ対応に関する国際調和を図るために規制当局間で相互に情報を共有すること等が含まれる。

b. 医療機器製造業者

- 情報源を問わず、脆弱性に関する情報を特定、評価、共有することが望ましい。製造業者は、規制当局が状況を把握し、適切に規制する上で役立つ情報を共有することが望ましい。
- 製造業者は、場所を問わず世界中に同じ情報を提供すると共に、可能であれば同一の対応を確保するため、影響を受ける製品が販売される地域の各規制当局による通知が一斉発出されるよう努めることが望ましい。
- 医療機器のサイバーセキュリティの脆弱性及び脅威に関する対応可能な情報を提供するため、対象ユーザの読解レベルに合わせて平易な言葉を使用することが望ましい。これにはアップデートの適用又はアップデート適用までの補完的対策に関連する臨床的なベネフィット・リスクに係る情報が含まれ得る。

c. ヘルスケアプロバイダ

- 適切に行動する又は行動を促進する責任を有することが多い。そのため、ヘルスケアプロバイダは、推奨事項を実施し、患者安全を確保するために必要なあらゆる情報にアクセスすることが望ましい。

- 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

共有する情報には、脅威の緩和策及び方法も含めることが望ましい。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ことが望ましい。

6.2.4 信頼できるコミュニケーション

情報共有の目的はセキュリティ及び患者安全の向上である。情報共有のネットワークは、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が挙げられる。

6.3 協調的な脆弱性の開示 （CVD）

未知の脆弱性等を考慮してセキュアな状態とすることは難しいため、透明性は、サイバーセキュリティのインシデントへの準備及び対応において不可欠な構成要素となる。透明性を強化する一つの手法として、CVD が挙げられる。CVD は、サイバーセキュリティの脆弱性情報を入手、評価し、緩和策及び補完的対策を開発した上で、顧客、同業他社、規制当局、サイバーセキュリティ情報共有組織及び一般人を含む様々な責任関係者に対して、当該情報を開示するための、正式なプロセスを確立する。

CVD のポリシー及び手順の採用は、影響を受ける技術のエンドユーザが、医療機器及びヘルス IT インフラをより適切に保護するための対応を情報に基づいて決定することを可能にする、積極的なアプローチである。

CVD への取り組みは、セキュリティ問題への意識向上に係る責任ある行動方針であり、その他の業界と同様、継続的な品質改善及びリスクマネジメントに関する製造業者の成熟度の判断基準になると考えることが望ましい。

前向きな CVD は、企業の積極的且つ責任ある対応を測る指標となるが、製造業者が当該ベストプラクティスを採用した結果、ネガティブキャンペーンが展開される不幸な事例が幾つか報告されている。ベストプラクティスとしては、CVD を例外なく規範として実施することが望ましい。また、医療機器の責任関係者は、CVD の導入をさらに促進させるため、CVD のポリシーについて製造業者に照会することを推奨する。

6.3.1 医療機器製造業者

医療機器のエコシステムが成熟することにより、透明性のある活動の利点が十分に認識されると考えられる。この種の情報開示は、同様の脆弱性によって影響を受ける可能性がある複数の市販製品による潜在的な危害から、一般の人々を事前に保護する点で極めて重要である。製造業者における透明性のある対応は、新規製品のセキュリティ設計の改善に関する直接的なベネフィットを得ることもできる。ヘルスケアプロバイダ及び患者は、製造業者、CERT やコンピュータセキュリティに係るインシデントに対処するための組織（Computer Security Incident Response Team：CSIRT）等のコンピュータ対応チーム又は規制当局からの CVD が脆弱性に関する権威ある情報源であることを理解する

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。

CVD に関する詳細については、協調的な脆弱性の開示に関する CERT®ガイド（CERT® Guide to Coordinated Vulnerability Disclosure）を参照すると良い。

6.3.2 規制当局

規制当局は、製造業者及び脆弱性の発見者と連携して、脆弱性の評価、影響分析、緩和策の作成と実施を支援すると共に、最終的に悪用のリスクを緩和するために公衆への遅滞のない情報共有を促進する。CVD はベストプラクティスの一部であるため、この情報共有には、必要に応じてグローバルコミュニケーションも含まれる。

6.3.3 脆弱性の発見者（セキュリティ研究者及びその他を含む）

脆弱性が発見された場合、関連する製造業者又は適切な行政機関等、調整を担う第三者機関に直接報告することが望ましい。その後、製造業者は脆弱性発見者と連携して、脆弱性の調査及び必要な対応を行った後、脆弱性の一般開示について相互に調整する。米国商務省電気通信情報局（National Telecommunications and Information Administration：NTIA）の「脆弱性開示に関する特性と対応：NTIA Awareness and Adoption Group（NTIA 認識・導入グループ）による調査報告書（2016 年 12 月）」において、開示の調整については、製造業者が脆弱性発見者の報告に対して速やかに対応し、且つ未対応の当該脆弱性を利用した攻撃の証拠がない場合、発見者は修正又はその他の緩和策が作成されるまで非開示とすることとなっている。発見者が修正以前に脆弱性を開示した場合、発見者と製造業者は、ヘルスケアプロバイダや患者等、自社製品を安全且つセキュアに運用する立場にあるユーザに向けて、可能性のある全ての緩和策について説明する。

6.4 脆弱性の修正

脆弱性の修正に関連する対応は、患者危害のリスクを低減するために重要である。修正には、患者への通知を含む広範な対応を含んでも良い。そのため、幾つかの責任関係者グループが、このプロセスにおいて極めて重要な役割を果たしている。これらの役割については以下に詳述する。

6.4.1 医療機器製造業者

a. リスクマネジメント

医療機器のサイバーセキュリティの脆弱性に関する第一の対応は、リスクアセスメントである。ISO 14971:2019 が規定するリスクマネジメントは、医療機器分野において確立・成熟した手法である。製造業者及び規制当局等は、リスクマネジメントの手法を適用して脆弱性によるサイバーセキュリティのリスクを評価し、リスクマネジメントに関連付けてサイバーセキュリティリスクマネジメントプロセスを確立することによって、脆弱性が患者の安全性に及ぼす影響を判断することが望ましい。患者安全の観点からは、十分な根拠を有する脆弱性修正戦略を開発することが合理的である。規制当局と製造業者は、このアプローチの有効性を高めるため、認識したリスク及び対応の正当性に関する情報を必要に応じて共有することが望ましい。修正の優先順位とタイミングはリスク

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。

d. 修正作業

責任関係者が行うべき対応は、医療機器の種類、地域の規制、ユーザ及び患者の安全性に対するリスク、意図する目的等、複数の要因によって異なる。本文書では、全ての医療機器に期待される特定の対応に関する詳細については言及しないが、全ての脆弱性修正作業の基礎とすることが望ましい原則を以下に示す。

- 地域の規制要求に対する適合
- 安全性及び基本性能に対する要件の遵守
- 患者及びユーザに対するリスクを低減するための責任関係者との情報共有
- 合意した修正策を達成するための責任関係者間の協力
- リスクに対する遅滞のない修正

医療機器に搭載されている基本的又は固有の保護手段が十分でなく、且つアップデートを適用できない場合、リスクを緩和する代替手段を補完的対策として適用することが望ましい。例えば、医療機器と医療 IT ネットワークとの間にファイアウォールをインストールする又は医療機器を医療 IT ネットワークから取り外す対策等が挙げられる。これらの補完的対策は、一般的には製造業者から提供される情報に基づいて、ヘルスケアプロバイダが実施する。

規制当局は、地域の法令の下で運営されており、市場に存在する医療機器に修正策を適用する際、特定の要求事項を課す可能性がある。製造業者は、脆弱性修正策を計画する際、規制当局の判断を考慮する必要がある。製造業者は修正作業を計画的に推進するため、早い段階で規制当局に情報を提供することが望ましい。これにより、暫定的な修正の支援や、責任関係者と連携してユーザ、メディア、公衆等における管理を支援しつつ、時間的に十分な余裕を持って規制に関するプロセスや必要とされる対応を開始できる。

セキュリティの脆弱性に関する情報は、世界経済の中で急速に拡散するため、脆弱性の悪用も世界中に瞬時に到達する可能性がある。これは、脆弱性を修正するグローバル且つ協調的な戦略が必要であることを意味している。ある脆弱性が特定の規制地域のみで開示・修正され、その他の規制地域では無対応となっている場合、その脆弱性は、悪意のある者に有利な条件を与えることとなり、患者や広範囲に渡る医療分野が攻撃に晒されることになる。

複数市場に製品を供給する製造業者は、タイミングのずれを最小限とするために、情報及び修正の公表を調整することが期待される。製造業者は、調整範囲を拡大し、影響を受ける製品が販売される地域の各規制当局と積極的に連携することが望ましい。

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。

HSCC が作成した「医療機器及びヘルス IT の合同セキュリティプラン」で文書化されているパッチ方法の修正版を表 2 に示した。[4] 表 2 では、医療機器製造業者が承認したアップデートを実装するために特定したユーザの主な責任を右列に示している。

アップデート方法	要約	ユーザの責任
リモートアップデート	製造業者から提供されるセキュアで認定されたリモートサービス及びサポートプラットフォームを介して適用するアップデート。	製造業者の指示に従って、リモート接続を確保する。
ユーザ管理	製造業者が指定したソースから顧客自身が取得し、インストールする承認済みのアップデート。製品あるいはコンポーネントを提供するサードパーティからの直接ダウンロードを含む。	製造業者の指示に従って、アップデートを取得してインストールする。
サービス訪問	地域のサービス施設が管理するサイバーセキュリティアップデート(オンサイトサービスを含む)。注記：誤ったアップデートの適用によって重大な危害が発生する可能性があり、現地でのサービスが必要となる場合にこの方法を適用する。	アップデート適用のために医療機器をサービス施設に渡す、オンサイトサービス訪問を受ける、アップデート適用のために専門の医療施設に出向く。

表 2. アップデート方法及び実施におけるユーザの責任

注記:サービス訪問の場合、ユーザは、アップデートのインストールに関する資格を有する専門家と連携する責任がある。

b. 医療施設環境に対する考慮事項

医療施設において、患者は、規制上有効である免許の有無に拘わらず、医師や看護師等の資格を有する医療専門家による医療を受けている。患者は、医療機器の安全且つ効果的な使用を確保するために、セキュリティ関係者も含めたヘルスケアプロバイダの指示に従うことが期待される。

IEC 80001-1:2010「医療機器を組込んだ IT ネットワークへのリスクマネジメントの適用」第 1 部「役割・責任・活動」の 3.2 項は、医療 IT ネットワークで運用されている医療機器の保守を含めて、「責任組織」が実施すべきリスクマネジメントについて規定している。責任組織は、患者を直接担当するヘルスケアプロバイダと異なる場合がある。アップデート適用は、リスクコントロール手段の一種であり、以下に示したとおり、具体的な指針が 4.4.4.3 項に記載されている。

[4] 医療機器及びヘルス IT の合同セキュリティプラン（HSCC、2019 年 1 月）。 注:リモートアップデート及びユーザ管理については、明瞭さを向上するため、「アドホックな」パッチ適用方法を削除している。

「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。

患者が海外旅行を計画している場合、患者は、医療機器のソフトウェア保守オプションを理解するために、ヘルスケアプロバイダ又は医療機器製造業者と相談することが望ましい。

6.4.3 規制当局

市販後のアップデート

脅威アクターは、悪用のテクニックを状況に合わせて絶えず適応させて進化させている。その結果として、医療機器のサイバーセキュリティの回復力を意味する「サイバー衛生管理」の向上、脆弱性の修正又は修正できない脆弱性のリスク緩和のために、頻繁なソフトウェア保守作業が必要になることが多い。「サイバーセキュリティの強化に特化」した変更が、最高レベルの規制対象とされた場合、その審査にあたり、殆どの規制当局は直ちに過負荷を強いられることになると推測される。

規制当局は、ソフトウェアの変更にあたり、サイバーセキュリティの観点から、リリース前の承認の要否を判断するため、以下に示した基本的な二つの論点を整理することが望ましい。

1) 変更は、あくまでサイバーセキュリティを強化するために意図されたものであり、ソフトウェア又は医療機器にその他の影響を与えないことが確認されているか？

製造業者は、必要な分析、試験及びバリデーションを行うことによって、その変更が医療機器の安全性及び性能に影響を与えないことを担保するためのシステム評価を行うことが望ましい。製造業者が、ソフトウェア又は医療機器にその他の偶発的又は意図しない影響が及ぶことを認識した場合、規制当局は、ソフトウェアの変更を実施する前に、提案された修正に関して審査することが適切であると判断する可能性がある。

2) 変更は、患者危害に関する受容できない残留リスクに関連する脆弱性のリスクを修正又は低減するために意図されたものか？

市販後の脆弱性リスク評価は、悪用が成功する可能性及び患者危害の重大さに基づいて評価することが望ましい。また、市販後の脆弱性リスク評価を使用して、残留リスクの受容可否を判断することが望ましい。「患者危害」の定義は、 ISO 14971:2019「医療機器－リスクマネジメントの医療機器への適用」において定義される「危害」のサブセットである。[5] 患者危害を狭く定義することにより、公衆衛生の保護に必要な変更に対する規制当局の審査を優先する効果が得られる。

[5] ISO 14971:2019 は、「危害」を「人の受ける身体的傷害若しくは健康障害又は財産若しくは環境の受ける害」と定義しており、「患者危害」は、この定義の前半部分が該当する。

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。

表 3.　ソフトウェアアップデート及び規制当局の監視に関する推奨レベル

提案されたソフトウェア変更が、複数の脆弱性に影響する又は「サイバー衛生管理」を改善し少なくとも一つの脆弱性に影響する場合、製造業者は、その後の対応を通知する際、表 3 に示した最高レベルの項目の適用について検討することが望ましい。例えば、一つのソフトウェア変更によりシステムセキュリティを強化し、脆弱性 A のリスクを低減し、脆弱性 B を修正することがある。この場合、脆弱性 B に関連する「高」レベルの規制要求事項が適用される。

いかなるレベルにおいても、規制当局は、自らの判断で、製造業者が IEC 62304:2006/AMD 1:2015 に規定されているソフトウェア保守のライフサイクルプロセス及びその他の規制要求事項に適合している科学的根拠を要求することがある。

6.5　インシデントへの対応

6.5.1　医療機器製造業者

製造業者は、製品及び患者を含む顧客に影響を及ぼす可能性があるサイバーセキュリティのインシデントやその他の事象に対応する準備を行う必要がある。製造業者は、自社製品に関するリスク管理対策を階層的に整理したポートフォリオに基づいて、拡張性のあるインシデント対応管理ポリシーを確立し、インシデント対応チームを組織しなければならない。インシデント対応チームは、サイバーセキュリティのインシデントについて評価、対応すると共に、その経験に基づいた適切な情報リスクマネジメント能力を共有し、次のインシデントが発生した際に遅滞なく適切に行動するために必要な調整、管理、フィードバック及び連携体制に関する情報を提供する。

サイバーセキュリティへの対応準備には、インシデント管理ポリシーの確立、詳細なインシデント対応計画の策定、インシデント対応チームの設立、インシデント対応の定期的な試験及び練習、並びに得られた教訓を通じて、インシデントへの対応能力を継続的に向上することが含まれる。

ISO/IEC 27035 が規定するインシデントマネジメントには、「計画及び準備」、「検知及び報告」、「評価及び決定」、「対応」及び「得られた教訓」が上位レベルとして含まれている（附属書 A 参照）。詳細は次項を参照すること。

a. 役割及び責任

インシデント対応チームは、マネージャ、計画作成グループ、監視グループ、対応グループ、実施グループ、分析グループ等の様々なグループに分割されることがあると共に、外部専門家が参画する場合もある。各グループは、それぞれの役割及び責任を有しており、スキル及び知識に基づいて人員を適切に配置することが望ましい。役職によっては、複数のグループの人員が担当する場合もある。相互に関連するグループに配属された人

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。

b. 役割毎のトレーニング

それぞれの関連する役割をトレーニングするための要求事項を確立し、更新の要否を定期的に見直すことが望ましい。サイバーセキュリティインシデントを評価する専門家は、実務経験に加えて、デジタル機器に残る記録を収集・解析し、法的な証拠性を明らかにするフォレンジック分析のトレーニングを受けることが望ましい。インシデント対応プロセスに関与する人員は、実務経験に加えて、インシデント対応のプロセス及び理論に関するトレーニングを受けることが望ましい。トレーニングプロセスは定期的に評価することが望ましく、その一環として、インシデント対応演習が行われる可能性がある。

c. 分析及び対応

ヘルスケアプロバイダは、調査結果を記載した報告書の提供を通じて、インシデント又は報告された脆弱性の影響を評価し、医療機器製造業者等の責任関係者と協力して対応することが望ましい。問題解決にあたり作業が必要な場合は、調査の状況及び日程を結果に含めることが望ましい。ヘルスケアプロバイダは、ベストプラクティス及び緩和策を含む安全関連情報を患者に周知することが望ましい。解決策に修正が含まれている場合は、その修正を施設全体に適用する前に、対象となる既存システムの機能が影響を受けないことを保証するためにレグレッション試験等のバリデーションを実施しなければならない。ヘルスケアプロバイダは、修正及び緩和策の情報を必要に応じて更新することが望ましい。

6.5.3 規制当局

医療機器のサイバーセキュリティインシデントとその対応には、規制当局も関与することが望ましい。6.5.1 項に記載したとおり、製造業者は、サイバーセキュリティのインシデントを規制当局が認識し、規制方針の決定に必要な詳細情報を規制当局が要求し、必要に応じて追加措置を実施できる環境を整備するため、インシデントについて規制当局に通知することが望ましい。必要に応じて規制当局が実施する追加措置としては、患者安全に対する影響評価、製造業者が提示した緩和策のリスク・ベネフィット評価、サイバーセキュリティ研究者等を含む責任関係者及びその他の政府機関や規制当局との連携等が挙げられる。

6.6 レガシー医療機器

本文書では、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を「レガシー医療機器」と定義する。現在使用されている多くのレガシー医療機器は、初期設計及び保守においてサイバーセキュリティについて検討されていなかった可能性があり、国際的なヘルスケアエコシステムにとって特に複雑な課題となっている。医療機器のデジタル化に伴って、古いアナログ装置では決して実現できなかった様々な機能が開発されてきた。そのため、これらの医療機器については、その臨床的有用性がセキュリティ対応のサポート期間を超えることが多いことが問題を更に悪化させている。このような技術は患者ケアにとって有益であるが、ソフトウェア、ハードウェア及びネットワーク接続を組み合わせた使用に伴い、医

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）。

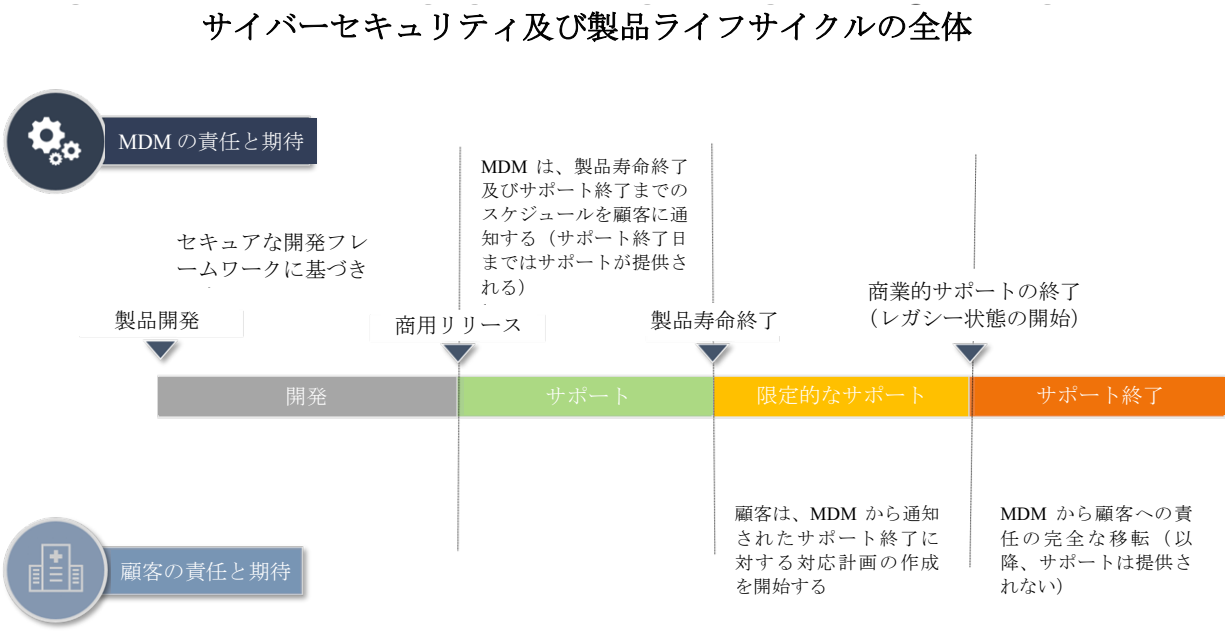

図 2. サイバーセキュリティに関する製品ライフサイクルの機能として表現したレガシー医療機器の概念フレームワーク

6.6.1 医療機器製造業者

医療機器のサイバーセキュリティ対策は、図 2 に示したとおり、商用リリース前の医療機器の設計開発段階から開始される。医療機器の完全なサポート、すなわち現在の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提供は、TPLC のフレームワークに基づいて、製造業者が公開した製品寿命終了（EOL）まで継続することが望ましい。製造業者が公表するサイバーセキュリティ EOL は、その期日以降、医療機器の総合的なサイバーセキュリティのサポートが大幅に縮小され、保証されなくなることを意味する。製造業者は、サイバーセキュリティ EOL が近づいた時点で顧客に対して、EOL 以降も限定的なサポートを提供することを通知すると共に、医療機器のサイバーセキュリティのサポート終了日（EOS 日）を明示することが望ましい。医療機器のユーザは、製造業者が指定したサイバーセキュリティ EOS の期日以降、該当する医療機器に対する全てのサポートを受けることができないと考えることが望ましい。

サイバーセキュリティ EOS の期日に達した医療機器は、この概念フレームワークに基づいて、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レガシー医療機器とみなし、使用を終了することが望ましい。医療機器のセキュリティを維持する責任及び EOS 日以降も機器を使用し続けたことによるリスクは、この時点でヘルスケアプロバイダ等の顧客に移転される。

なお、医療機器によっては、サポートが終了しておりセキュリティ上のパッチを適用できない古いオペレーティングシステムを使用している場合等、設計変更を行うことはできないが、補完的対策を実施することにより、相応に保護できる可能性がある。本フレームワークにおいて、利用可能且つ実績のある補完的対策が存在する医療機器については、レガシー医療機器とみなさない。規制当局は、ヘルスケアプロバイダが EOS 日以降の事業継続計画を作成するための十分な時間を確保できるように、必要に応じて、現在の医療機器において EOL 日以降に発生するセキュリティ上の課題に対応するための補完的対策を実施するよう製造業者に推奨する。医療機器の設計、脆弱性の管理及び顧客との情報共有は、医療機器のサイバーセキュリティに関する課題に取り組む上で全て重要な役割を果たす。製造業者へ向けた医療機器のライフサイクルステージの機能に関する推奨事項は、以下に示したとおりである。

- 開発:

    a. 医療機器を構成するハードウェア及びソフトウェアコンポーネントのサポートライフサイクルを考慮する。製造業者は、医療機器のユーザを総合的にサポートするため、品質やパフォーマンス、セキュリティに関する問題を解決するためのソフトウェア及びファームウェアのアップデート適用に関して、該当するハードウェア及びソフトウェアベンダーからのサポートを受けることが望ましい。製造業者は、利用期間中の製品の安全性と有効性を維持するために必要なサポートを予測することが望ましい。製造業者は、ヘルスケアプロバイダが想定する医療機器ライフサイクル期間中にサードパーティーベンダーのサポート

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。

6.6.2 ヘルスケアプロバイダ

ヘルスケアプロバイダは、公表されたサイバーセキュリティ EOL において製造業者が設定した医療機器の製品寿命より大幅に長い使用期間を設定することが多い。しかし、脅威の状況は時代の経過と伴に変化する。新しい脅威の出現により、時代遅れの技術を使用するリスク及び対応に要する経費が増加するが、製造業者及びヘルスケアプロバイダは共同責任として対処しなければならない。医療機器のライフサイクル段階の機能として以下に示した推奨事項は、ヘルスケアプロバイダが医療機器の課題に取り組むための一助になり、既定のサイバーセキュリティ EOS 日以前に計画を作成する上で役立つと考えられる。

- サポート:

    a. 製品ライフサイクルの計画作成、サイバーセキュリティに関する理解及び透明性を確保するために、製造業者に明確な連絡窓口と情報伝達プロセスを要求する。

    b. サポートライフサイクルが最も短いソフトウェアコンポーネントが、最終的に医療機器のサポート及びサイバーセキュリティに影響を与えるため、SBOM を要求する。顧客は、SBOM を入手することにより、医療機器のライフサイクルに影響を与えるコンポーネントをより適切に理解することが可能となり、補完的対策等のリスクコントロール手段に用いられる追加のハードウェアに関する情報を把握することができる。

    c. 製造業者、サードパーティのサービス業者又はプロバイダ自身のリソース及び管理を通じて、使用中の医療機器を適切にサポートし、正常な稼働を維持する。例えば、ネットワークセキュリティ、資産セキュリティ、アイデンティティ/アクセスマネジメント、セキュリティ業務等が挙げられる。

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

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

- 限定的なサポート:

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

- 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

13. 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 (HDOs) on how to self-assess their conformance with IEC 80001-1

14. ISO/IEC 27000 family - Information security management systems

15. ISO/IEC 27035-1:2016, Information technology – Security techniques – Information security incident management – Part 1: Principles of incident management

16. ISO/IEC 27035-2:2016, Information technology – Security techniques – Information security incident management – Part 2: Guidelines to plan and prepare for incident response

17. ISO/IEC 29147:2018, Information Technology – Security Techniques – Vulnerability Disclosure

18. ISO/IEC 30111:2013, Information Technology – Security Techniques – Vulnerability Handling Processes

19. ISO/TR 24971:2020, Medical devices – Guidance on the application of ISO 14971

20. UL 2900-1:2017, Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements

21. 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

7.3 規制当局のガイダンス

22. ANSM (Draft): Cybersecurity of medical devices integrating software during their life cycle (July 2019)

23. China: Medical Device Network Security Registration on Technical Review Guidance Principle (January 2017)

24. 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)

25. 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)

26. FDA (Draft): Content of Premarket Submissions for Management of Cybersecurity in Medical Devices (October 2018)

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)

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

43. MITRE CVSS Healthcare Rubric
https://www.mitre.org/publications/technical-papers/rubric-for-applying-cvss-to-medical-devices

44. Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP)
https://www.phe.gov/Preparedness/planning/405d/Pages/hic-practices.aspx

45. Open Web Application Security Project (OWASP)
https://www.owasp.org/index.php/Main_Page

46. Manufacturer Disclosure Statement for Medical Device Security (MDS^2)
https://www.nema.org/Standards/Pages/Manufacturer-Disclosure-Statement-for-Medical-Device-Security.aspx

47. ECRI approach to applying the NIST framework to MD
https://www.ecri.org/components/HDJournal/Pages/Cybersecurity-Risk-Assessment-for-Medical-Devices.aspx

48. 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

49. https://republicans-energycommerce.house.gov/wp-content/uploads/2018/10/10-23-18-CoDis-White-Paper.pdf

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

8.0 附属書

8.1 附属書 A: インシデント対応の役割（ISO/IEC 27035 から引用）

インシデントマネジメント – ISO/IEC 27035	
計画及び準備	情報セキュリティのインシデントマネジメントポリシーを作成し、インシデント対応チーム等を設立する。
検知及び報告	インシデントと考えられる又はインシデントになる可能性がある「事象」を検知して報告する。
評価及び決断	状況を評価し、実際のインシデントの有無を判断する。
対応	必要に応じて、インシデントの防御と解消、インシデントからの復旧、インシデントのフォレンジック分析を行う。
得られた教訓	過去に経験したインシデントに基づいて、組織の情報リスクマネジメント能力を体系的に改善する。

インシデント対応チーム		
役割	**責任**	**主なアクション**
マネージャ	サイバーセキュリティインシデント対応に関する重大な問題について、対応の指揮と決定を行う	a) インシデント対応に積極的に関与してサポートする。例えば、必要に応じて人的資源、金銭的資源、物的資源を提供する b) インシデント対応のポリシーと計画を検証して承認し、その実施を指揮する c) インシデント対応計画の見直しと改訂を行う d) インシデント対応チームの内外において必要な調整を行う
計画作成グループ	インシデント対応を運用する	a) セキュリティポリシーを確立し、その実施計画を作成する b) セキュリティプロセスを実施する c) リスクの優先順位を調整する d) 上位組織及びその他のサードパーティとの連携体制を構築する e) 経営陣をサポートする f) 対象組織に関する脆弱性レポートを検討、登録、承認する g) マネージャが指示したその他の活動を行う
監視グループ	リアルタイムのセキュリティ監視活動を行う	a) 監視と運用に関する日常業務を行う b) 侵入を検知し、インシデントを登録し、初期対応を行う c) セキュリティ関連の更新を行う d) セキュリティポリシーを実施し、経営陣をバックアップする e) ヘルプデスク f) 施設マネジメント g) マネージャが指示したその他の活動を行う
対応グループ	リアルタイム対応や技術サポート等	a) インシデントの周知と報告を行う b) 監視システム間の相関分析を行う

	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

8.2　附属書 B：協調的な脆弱性の開示に関する各地域のリソース

オーストラリア
CERT Australiac (CERT オーストラリア)
https://www.cert.gov.au/

AusCERT
https://www.auscert.org.au/

ブラジル
All Certs in Brazil(ブラジル国内の CERT 一覧)
https://www.cert.br/csirts/brazil/

カナダ
Canadian Centre for Cyber Security(カナダサイバーセキュリティセンター)
https://www.cyber.gc.ca/

欧州
CERT European Union(CERT 欧州連合)
https://cert.europa.eu

フランス
ANSM
https://ansm.sante.fr/

https://www.ansm.sante.fr/Declarer-un-effet-indesirable/Votre-declaration-concerne-un-dispositif-medical/Votre-declaration-concerne-un-dispositif-medical/(offset)/0

French Ministry of Health and Solidarity(フランス厚生省)
https://solidarites-sante.gouv.fr/soins-et-maladies/signalement-sante-gouv-fr/

Shared Health Information Systems Agency(共有医療情報システム庁)
https://www.cyberveille-sante.gouv.fr/

ANSSI - National Agency for Information Systems Security(国家情報システムセキュリティ庁)
https://www.ssi.gouv.fr/en/

ドイツ
CERT Germany(CERT ドイツ)
https://www.cert-bund.de/

イタリア
https://www.csirt-ita.it/

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/