イルス対策基準」（平成7年通商産業省告示第 429 号）、「コンピュータ不正アクセス対策基準」（平成8年通商産業省告示第 362 号）及び「ソフトウェア製品等の脆弱性関連情報に関する取扱規定」（平成 29 年経済産業省告示第 19 号）、に基づき、コンピュータウイルス・不正アクセス・脆弱性情報に関する発見・被害の届出や情報提供を受け付け、提供を受けた情報は、被害の拡大・再発の防止、情報セキュリティ対策の向上に役立てられている。製造販売業者はこれらの情報を参考にするとともに、独立行政法人情報処理推進機構（IPA）セキュリティセンターに対して医療機器のサイバーリスクに関係する情報を適切に提供していくことが望ましい。

4.市販後の安全性確保について

製造販売業者は、GVP 省令に基づき、医療機器の市販後安全対策として医療機器の不具合情報や文献等を収集・調査し、その情報を分析して、必要に応じて対策を行うことが必要となる。サイバーリスクに基づく不具合等についても、GVP 省令における安全性情報として取り扱い、販売業者・貸与業者や修理業者の協力のもと、医療機関と連携を取り、適切な市販後の安全確保を行う必要がある。

4.1 中古医療機器への対応について

プログラムを使用した医療機器の多くは耐用期間が長く、特定保守管理医療機器に指定されている。これらの医療機器を中古で販売する場合、医療機関から引き取った販売業者及び中古医療機器を医療機関へ販売する販売業者は、医療機器の整備等に関し製造販売業者へ照会し、その指示に基づいて整備を行うことが求められている（医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律施行規則（昭和 36 年厚生省令第1号）第 170 条）。このため、中古医療機器についても、製造販売業者は当該医療機器の販売業者に対し適切な指示を行い、サイバーリスクへの対応を実施させる必要がある。

また、販売業者は、医療機関に対し、販売する中古医療機器のサイバーリスクへの対応状況等について適切に説明する必要がある。

5.使用者等への情報提供

サイバーリスクが想定される医療機器については、サイバーセキュリティに関する情報を製造販売業者から使用者に提供する事が求められる。体内植込み医療機器等については装着者への提供も必要である。

また、外部との接続がないことが明確である等の理由からサイバーリスクが想定されない

場合であっても、プログラムが使用されていることが明らかな医療機器の場合には、サイバーリスクが想定されない旨の情報を使用者に対し提供を行うことが望ましい。

提供すべき情報としては、次の事項が基本となるが、サイバーリスクの程度に応じて適切に対応すること。なお、公開することにより、サイバーリスクが増大することが想定される情報については、その提供方法についての配慮が必要である。

1） 添付文書への記載事項

- 意図する使用環境
- 使用者側が遵守すべき事項（概要）
- 要求された環境外で使用した場合のリスク（リスクの重要性により必要に応じ記載）

2） 技術資料等

- 技術情報（ネットワーク環境への接続に必要な情報等）

これらの情報は、医療機関等からの求めに応じ提供できること。また、医療機関での使用を意図する医療機器の場合、「安全管理ガイドライン」に沿った情報提供が望ましい。

3） その他

- 医療機器の市販後のライフサイクルに応じた対応の方法
- 製造販売業者としてのサイバーセキュリティ対応への取組み等に関する情報
- サイバーセキュリティに関連する問合せ窓口及びサイバーセキュリティに関連するサービスの照会先

サイバーリスク対応に関する情報提供について、例えば、製造販売業者のホームページ等を利用して提供する旨を添付文書に記載し、必要な時に速やかに情報を入手できるようにすることも一つの方法である。

参考資料等

- 「医療機器プログラムの承認申請に関するガイダンスの公表について」（平成 28 年 3 月 31 日付け厚生労働省医薬・生活衛生局医療機器・再生医療等製品担当参事官室事務連絡）
- 医療情報システムの安全管理に関するガイドライン第 5 版（厚生労働省　平成 29 年 5 月）
- 「医療情報システムの安全管理に関するガイドライン第 5 版」に関するＱ＆Ａ （厚生労働省　平成 29 年 5 月）

- JAHIS標準 17-006 「製造業者による医療情報セキュリティ開示書」ガイド Ver.3.0a（一般社団法人保健医療福祉情報システム工業会 2017 年 7 月）
- JESRA TR－0039*B－2018 「製造業者による医療情報セキュリティ開示書」ガイド Ver.3.0a（一般社団法人日本画像医療システム工業会 2018 年 3 月）

規格、技術文書等

- IEC 80001-1:2010 Application of risk management for IT-networks incorporating medical devices - Part 1: Roles, responsibilities and activities
- IEC TR 80001-2-2:2012 Application of risk management for IT-networks incorporating medical devices -Part 2-2: Guidance for the communication of medical device security needs, risks and controls
- 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
- NIST SP800-53: Security and Privacy Controls for Federal Information Systems and Organizations

  （NIST: 米国国立標準技術研究所の規格で、多くのセキュリティに関する国際規格から参照されているベストプラクティスによる標準）

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

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

目次

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。

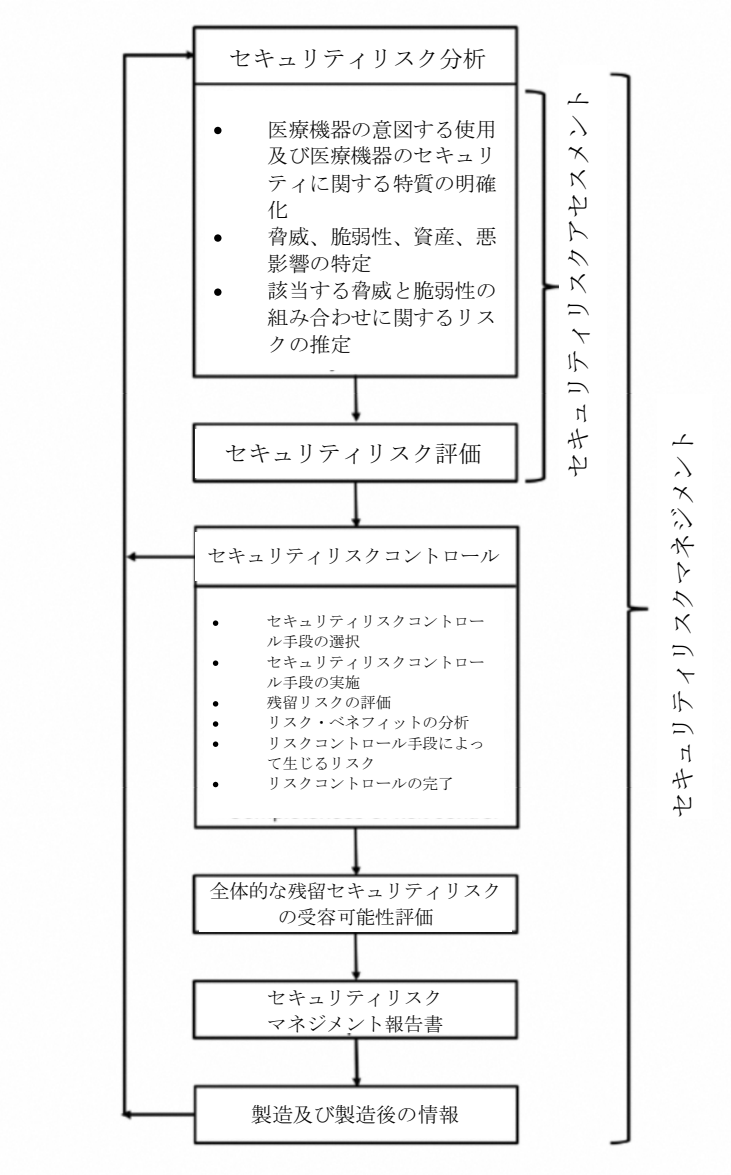

図 1.　セキュリティリスクマネジメントプロセスの図解
(AAMI TIR57:2016 から許可を得て引用)

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。