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）。

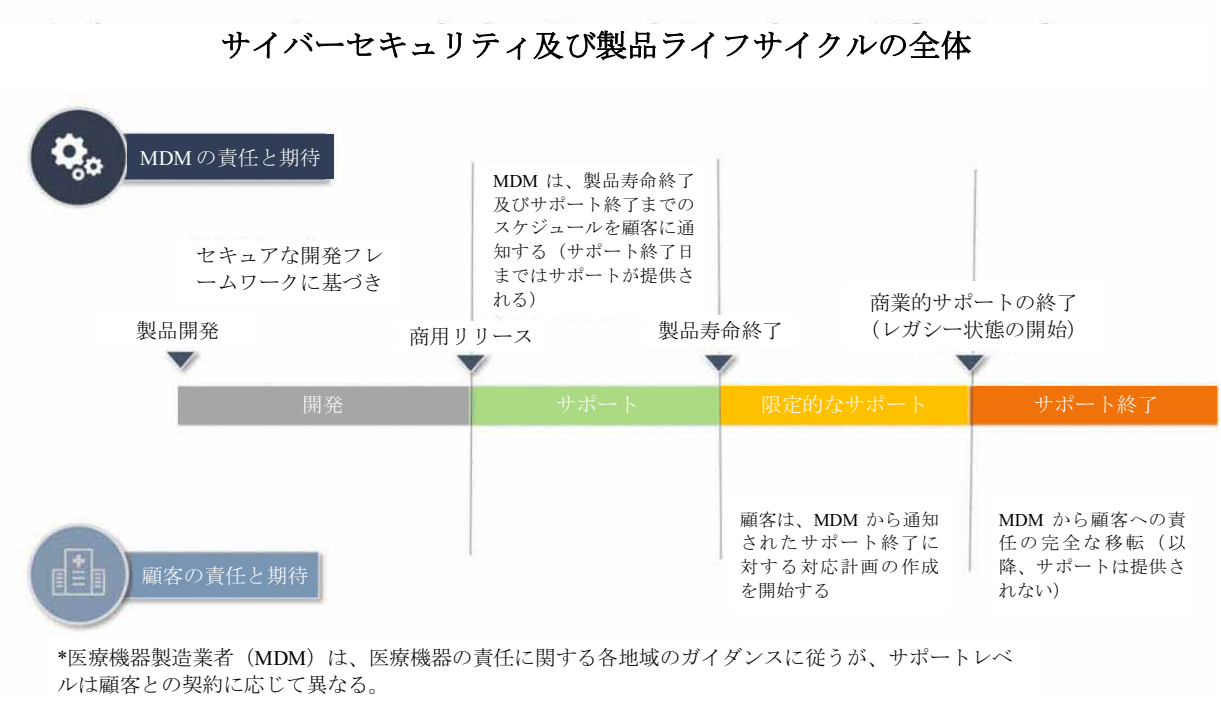

図 2.　サイバーセキュリティに関する製品ライフサイクルの機能として表現したレガシー医療機器の概念フレームワーク

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/

別添5

薬生機審発１０２０第１号
平成 29 年１０月２０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　）

医療機器プログラムの一部変更に伴う軽微変更手続き等の取扱いについて

医療機器プログラムの承認申請等の取扱いについては、「医療機器プログラムの取扱いについて」（平成 26 年 11 月 21 日付け薬食機参発 1121 第 33 号、薬食安発 1121 第 1 号、薬食監麻発 1121 第 29 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、厚生労働省医薬食品局監視指導・麻薬対策課長通知）等により示しているところです。

また、医療機器全般の製造販売承認事項一部変更申請及び軽微変更届の取扱いについては、「医療機器の製造販売承認申請の作成に際し留意すべき事項について」（平成 26 年 11 月 20 日付け薬食機参発 1120 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）通知)、「医療機器の一部変更に伴う手続きについて」（平成 20 年 10 月 23 日付け薬食機発第 1023001 号厚生労働省医薬食品局審査管理課医療機器審査管理室長通知）及び「医療機器の一部変更に伴う軽微変更手続き等の取扱いについて」（平成 29 年 7 月 31 日付け薬生機審発 0731 第 5 号厚生労働省医薬・生活衛生局医療機器審査管理課長通知）等により示してきたところです。

今般、医療機器プログラムの一部変更に伴う軽微変更手続き等の取扱いについて別添のとおりとりまとめましたので、御了知の上、貴管内関係事業者、関係団体等に周知方御配慮願います。

なお、本通知の写しを独立行政法人医薬品医療機器総合機構理事長、一般社団法人日本医療機器産業連合会会長、日本製薬団体連合会会長、一般社団法人日本臨床検査薬協会会長、一般社団法人米国医療機器・IVD 工業会会長、欧州ビジネス協会医療機器・IVD 委員会委員長及び各登録認証機関の長宛て送付することとしています。

（別添）

医療機器プログラムの一部変更に伴う軽微変更手続き等の取扱いについて

ここで示すのは、有体の医療機器とは異なり、医療機器プログラム固有に生じうる状況について特に取り上げ整理したものであることに留意すること。医療機器全体に関する一部変更に伴う軽微変更手続き等については、「医療機器の製造販売承認申請の作成に際し留意すべき事項について」（平成 26 年 11 月 20 日付け薬食機参発 1120 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）通知)、「医療機器の一部変更に伴う手続について」（平成 20 年 10 月 23 日付け薬食機発第 1023001 号厚生労働省医薬食品局審査管理課医療機器審査管理室長通知。以下「旧一変軽変通知」という。）及び「医療機器の一部変更に伴う軽微変更手続き等の取扱いについて」（平成 29 年 7 月 31 日付け薬生機審発 0731 第 5 号厚生労働省医薬・生活衛生局医療機器審査管理課長通知）に示してきた取扱い等を参考とすること。

なお、以下は例を示すものであり、軽微変更届の対象となる事例並びに一部変更承認申請及び軽微変更届のいずれも必要でない事例はこれらに限るものではない。個別の事例における取扱いについては、必要に応じ、独立行政法人医薬品医療機器総合機構又は登録認証機関に相談されたい。

１．軽微変更届の対象となる事例

次に示す事例については、これらの変更等に伴う医療機器としての機能の追加・変更等がない場合に限り、軽微変更届の対象となる。

１）医療機器プログラムのダウンロード販売への変更又は追加

（事例）

・　医療機器プログラムを DVD 等の記録媒体で販売している製品について、ダウンロード販売に変更又は追加する場合。

２）最終製品の保管を行う製造所の追加・変更・削除

（事例）

・　医療機器プログラムを記録媒体で販売していた製品をダウンロード販売へ変更したことに伴い、最終製品の保管を行う製造所を削除する場合。

・　医療機器プログラムをダウンロード販売している製品を記録媒体での販売へ変更又は記録媒体での販売を追加することに伴い、最終製品の保管を行う製造所を追加又は変更する場合。

３）動作環境である OS の種類やクラウド動作の追加・変更・削除

以下の事例のうち、動作環境である OS 等の種類の変更において、医療機器としての使用目的又は効果及びその性能に影響を与えない場合。

①汎用 PC で動作する製品について、クラウド環境での動作を追加する場合

（事例）

・　汎用ＰＣ（Windows 7）で動作する製品について、クラウド環境でも動作可能であることを追加する場合。（なお、この場合は、クラウド環境で使用するための操作方法の変更も含む。）

②異なる種類の動作環境である OS への変更・追加

（事例）

・　iOS 10 で動作する製品に対して、異なる種類の OS である Android 6.0 を動作環境として追加する場合。

４）データの入出力に使用する記録媒体の追加・削除

（事例）

・　医療機器プログラムが処理するデータの入出力を行う（読み書きする）記録媒体を DVD としていたが、USB メモリを追加又は変更する場合。

２．一部変更承認申請及び軽微変更届のいずれの手続きも要さない事例

次に示す事例については、これらの変更等に伴い医療機器としての機能の追加・変更等がない場合に限り、一部変更承認申請及び軽微変更届のいずれの手続きも必要でない。なお、次の一変申請時には記載整備を要することに留意されたい。

１）医療機器プログラムの動作環境である OS 等の変更・追加・削除（医療機器としての使用目的又は効果及びその性能に影響を与えない場合に限る。）

①動作環境である OS バージョン等の追加・変更・削除。

（事例）

・　Windows 7 での動作を指定している製品に対して、Windows X を追加する場合。

・　OS 供給元のサービス終了に伴い動作環境の OS 指定から Windows XP を削除する場合。

②動作環境として用いるデータベース等のバージョンの追加・変更

（事例）

・　MS SQL Server2012 までのバージョンを動作環境として指定している製品について、その後継バージョンを追加する場合。

・　データベースの動作環境として Java 7.0 を指定していた製品に Java 8.0 を追加又は変更する場合。

２）動作環境として推奨する汎用 PC や情報端末の追加・変更・削除

（事例）

・　添付文書に記載した推奨する汎用 PC の名称を変更する場合。（OS の種類変更は含まない。）

３）供給する記録媒体の変更・追加・削除

（事例）

・　供給する記録媒体として DVD を指定していたが、その指定を削除する場合、USB メモリへ変更する場合又は USB メモリを追加で指定する場合。

４）インストール可能数の扱いについて

医療機器プログラムを記録媒体で提供する場合、一つの製品（記録媒体）からインストールできる回数（以下「インストール可能数」という。）については、承認書等に記載を要しないものであり、インストール可能数の変更については、一部変更承認申請及び軽微変更届のいずれの手続きも必要でない。なお、インストール可能数についてあえて承認書等に記載した場合でも、インストール可能数の変更については、一部変更承認申請及び軽微変更届のいずれの手続きも必要でない。

（事例）

・　製品（DVD で供給）は、インストール可能数を１台としていたが、３台まで可能と変更する場合。

なお、インストール可能数は添付文書に記載すべき項目とはなっていないが、製造販売業が意図したインストール数を越えて使用されることを防ぐため、添付文書に注意事項としてインストール可能数を記載しても良い。この記載の変更についても、一部変更承認申請及び軽微変更届のいずれの手続きも必要でない。

以上