【徹底解説】
IEC 81001-5-1
医療機器サイバーセキュリティ

村山 浩一 著

はじめに

医療技術の進歩は、私たちの生活に計り知れない恩恵をもたらしてきた。現代の医療機器は、高度なデジタル技術を駆使し、より正確な診断、より効果的な治療、そしてより安全な医療の提供を可能にしている。しかし、この進歩は同時に新たな課題も生み出している。その最たるものが、医療機器のサイバーセキュリティである。

2022 年、大阪急性期・総合医療センターがランサムウェア攻撃を受け、医療システムが機能不全に陥るという事態が発生した。また 2021 年には、市立東大阪医療センターの医用画像参照システムへの不正アクセスが確認され、患者データの流出リスクが明らかとなった。これらの事例は、医療機器のサイバーセキュリティが、もはや単なる技術的な課題ではなく、患者の生命と安全に直結する重大な問題となっていることを示している。

本書は、このような背景のもと、医療機器のサイバーセキュリティについて、その本質から実践的な対策まで、体系的かつ詳細な解説を提供するものである。特に注目すべきは、IEC 81001-5-1:2021（JIS T 81001-5-1：2023）を中心とした最新の国際規格と、IMDRF ガイダンスに基づく実務的なアプローチの解説である。

医療機器のサイバーセキュリティは、製造販売業者、医療機関、規制当局など、多岐にわたるステークホルダーが関与する複雑な課題である。本書では、これらの関係者それぞれの視点から、必要な対策と責務を明確に示している。特に、製品ライフサイクル全般にわたるセキュリティ対策の重要性を強調し、設計段階から市販後の管理に至るまでの包括的なアプローチを提示している。

また、本書は「レガシー医療機器」という重要な課題にも焦点を当てている。既存の医療機器のセキュリティ対策は、新規開発品とは異なるアプローチが必要となる。本書では、レガシー医療機器の定義から具体的な対策まで、実践的な指針を提供している。

さらに、本書の特徴として、ソフトウェア部品表（SBOM）や脆弱性試験など、最新のセキュリティ技術と手法についても詳しく解説している。これらは、増大するサイバー攻撃のリスクに対応するための重要なツールとなっている。

医療機器のサイバーセキュリティは、常に進化する脅威に対応し続けなければならない。本書は、基本要件基準から最新の国際規格まで、幅広い知識を体系的に整理し、実務者が直面する様々な課題に対する解決の指針を示している。

特に注目すべきは、本書が単なる技術解説に留まらず、品質マネジメントシステムの観点からもサイバーセキュリティを捉えている点である。セキュリティ対策は、組織的な取り組みとして実施されなければならない。本書は、この観点から、責任の所在の明確化から継続的改善の仕組みまで、包括的な解説を行っている。

医療機器のサイバーセキュリティは、今後ますます重要性を増していくだろう。IoT技術の発展により、医療機器のネットワーク接続性は高まり、それに伴いセキュリティリスクも増大している。また、医療のデジタル化が進む中、患者データの保護も極めて重要な課題となっている。

本書は、これらの課題に対応するための実践的なガイドとして、医療機器の開発・製造に携わる技術者、品質管理責任者、そして医療機関の機器管理者など、幅広い読者に向けて書かれている。サイバーセキュリティの専門家でない読者にも理解しやすいよう、基本的な概念から段階的に解説を進めている。

医療機器のサイバーセキュリティは、患者の安全と医療の質を確保するための重要な要素である。本書が、読者の皆様の実務における道標となり、より安全で信頼性の高い医療機器の実現に貢献できれば幸いである。

2025 年 2 月
株式会社イーコンプライアンス
村山 浩一

目次

第1章

サイバーセキュリティとは

1. サイバーセキュリティとは

1.1. サイバーセキュリティの概念と医療機器におけるその特殊性

医療機器のサイバーセキュリティと一般的なサイバーセキュリティの間には、本質的かつ極めて重要な差異が存在する。この違いを正確に理解し、適切な対策を講じることは、医療機器の安全な運用と患者の生命保護において不可欠である。

一般的なサイバーセキュリティは、主として情報資産の保護に重点が置かれている。サイバーセキュリティ基本法における定義では、電子的方式、磁気的方式等により記録、伝送される情報の保護と、情報システム及び情報通信ネットワークの安全性及び信頼性の確保が主たる目的とされている。

これに対し、医療機器のサイバーセキュリティは、情報保護の枠組みを超えて、患者の生命と健康の保護を最重要目的としている。つまり、医療機器においては情報セキュリティではなく、医療機器がハッキングされることによって患者に及ぼす健康被害について安全性を担保するものでなければならないのである。医療機器がサイバー攻撃を受けた場合、検査装置または診断装置であれば検査の中断や誤った診断につながってしまう可能性が考えられる。治療に用いられる装置であれば、治療の中断等の事象の発生、放射線治療の線量計算プログラムであれば、過量照射や不十分な量の照射が発生する可能性が考えられる

このように、生命維持装置や植込み型医療機器への不正アクセスは、即座に致命的な結果をもたらす可能性があるため、医療機器のサイバーセキュリティには、通常の IT 機器をはるかに超える高度な安全性と信頼性が要求される。

医療機器のサイバーセキュリティにおいて特に重要なのは、医療機器そのものの安全性と信頼性の確保である。これには、医療機器の動作の正確性、継続性、およびリアルタイム性の保証が含まれる。生命維持管理装置では、投与量や圧力などのパラメータの精密な制御が必要であり、わずかな改ざんでも重大な結果を招く可能性がある。画像診断装置におけるデー

サイバーセキュリティ基本法

第2条（定義）

この法律において「サイバーセキュリティ」とは、電子的方式、磁気的方式その他人の知覚によっては認識することができない方式（以下この条において「電磁的方式」という。）により記録され、または発信され、伝送され、もしくは受信される情報の漏えい、滅失または毀損の防止その他の当該情報の安全管理のために必要な措置ならびに情報システムおよび情報通信ネットワークの安全性および信頼性の確保のために必要な措置（情報通信ネットワークまたは電磁的方式で作られた記録に係る記録媒体（以下「電磁的記録媒体」という。）を通じた電子計算機に対する不正な活動による被害の防止のために必要な措置を含む。）が講じられ、その状態が適切に維持管理されていることをいう。

サイバーリスクとは、そうした安全性や信頼性が損なわれ、危害（harm）が生じるリスクと考えられる。（出典：「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」）

図 1-1 サイバーセキュリティ 基本法の定義

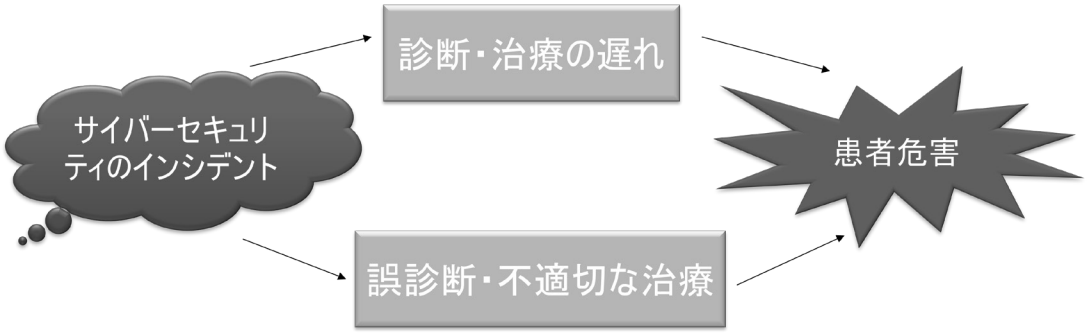

図 1-2 医療機器におけるサイバーセキュリティ

タの完全性の確保も重要である。診断画像の改ざんや劣化は、誤診や不適切な治療につながる可能性があるためである。また、手術支援ロボットにおいては、遅延のない操作応答性の確保が特に重要となる。

医療現場における緊急時の対応体制の整備と、医療従事者による適切な機器操作の確保も不可欠である。これには、サイバー攻撃発生時の代替手段の確保や、医療従事者への体系的な教育訓練が含まれる。特に、ランサムウェア攻撃発生時の手動操作への切り替えや、ネットワーク遮断時の診療継続手順を確立し、定期的な訓練を実施する必要がある。

医療機器のサイバーセキュリティでは、設計段階からのセキュリティ・バイ・デザインの実装、定期的なセキュリティアップデートの実施、多層的なセキュリティ管理体制の構築が不可欠である。製造業者には、製品のライフサイクル全体を通じたセキュリティ対策の維持と更新が求められる。これには、脆弱性の継続的なモニタリング、セキュリティパッチの迅速な提供、医療機関との緊密な連携による脅威情報の共有が含まれる。

さらに、IEC 80001 シリーズや ISO 14971 などの国際規格への準拠、各国規制当局が定めるガイドラインへの適合も重要である。急速に進化するサイバー脅威に対して適切に対応していくためには、製造業者と医療機関の双方における継続的な取り組みが不可欠である。

2. 情報セキュリティの三要素とサイバーリスクマネジメント

情報セキュリティは、デジタル社会における重要な基盤概念である。その中核を成すのは、CIA 三要素として知られる機密性（Confidentiality）、完全性（Integrity）、可用性（Availability）である。これらの要素は、ISO/IEC 27001 において国際標準として定義され、組織の情報セキュリティマネジメントシステム（ISMS）の基本的な評価基準となっている。

機密性は、正当な権限を持つ者のみが情報にアクセスできる状態を維持することを意味する。医療分野においては、診療記録、検査結果、遺伝情報など、極めて機微性の高い個人情報の保護が特に重要である。これらの情報漏洩は、患者のプライバシー侵害、社会的差別、医療機関への信用失墜、さらには個人情報保護法違反による法的制裁や多額の損害賠償請求につながる可能性がある。特に遺伝情報の漏洩は、将来の疾病リスクや治療反応性に関する情報を含むため、患者と血縁者の双方に長期的な影響を及ぼす可能性がある。

完全性は、情報の正確性と一貫性を維持し、不正な改ざんを防止することを意味する。医療システムにおいては、診断情報、治療記録、患者データの完全性が患者の生命に直接関わる。電子カルテシステムのデータ改ざんは、投薬ミスや不適切な治療方針の選択を引き起こす可能性がある。また、AI 診断支援システムにおいては、学習データの完全性が診断精度を左右するため、より厳密なデータ管理が求められる。医療画像データの完全性は、適切な診断と治療方針の決定に不可欠である。

可用性は、必要な時に必要な情報やサービスにアクセスできる状態を維持することを意味する。医療システムでは、救急医療や集中治療室における患者情報への即時アクセスが生命維持に直結する。このため、システムの冗長化、災害時のバックアップ体制、無停電電源装置の整備など、多層的な可用性確保対策が必要となる。

現代のサイバーリスクマネジメントでは、国家支援型の攻撃集団や組織的犯罪グループによる高度な脅威への対応が求められる。これらの攻撃者は、ゼロデイ攻撃や高度な社会工学的手法を用いて、従来の防御対策を迂回する能力を持つ。医療分野では、患者の安全を最優先とする包括的なリスク管理が必要であり、医療機器の安全性確保、医療サービスの継続性維持、患者データの保護など、多面的な対策が求められる。

医療のデジタル化に伴い、クラウド型電子カルテ、医療 IoT デバイス、AI 診断支援システムなど、新たな技術要素に対するセキュリティ対策も重要となっている。特に、5G 通信を活用した遠隔医療の普及により、エンドツーエンドの暗号化やゼロトラストセキュリティの導入など、より高度なセキュリティ要件への対応が必要となっている。

効果的なリスクマネジメントの実現には、最新のセキュリティ技術導入、包括的なセキュリティポリシーの整備、医療従事者への継続的な教育訓練、定期的なリスク評価と改善が不可欠である。これらの要素を適切に組み合わせることで、安全で信頼性の高い医療情報システムの構築が可能となる。

3. 本邦における医療情報システムのセキュリティガイドライン

本邦の医療情報システムに関するセキュリティ管理については、厚生労働省および経済産業省・総務省が二つの重要なガイドラインを定めている。一つは厚生労働省による「医療情報システムの安全管理に関するガイドライン」（以下、厚労省ガイドライン）であり、もう一つは経済産業省・総務省による「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」（以下、経産省・総務省ガイドライン）である。

厚労省ガイドラインは 2005 年に初版が発行され、技術の進歩や法制度の改正に応じて定期的に改定されている。2023 年 5 月に公開された最新の第 6.0 版では、全体構成が見直され、経営層向けの「経営管理編」、企画管理者向けの「企画管理編」、システム運用担当者向けの「システム運用編」という三部構成となり、より実効性の高い安全管理を目指している。主な改定ポイントとしては、外部委託・外部サービスの利用に関する整理、情報セキュリティに関する考え方の整理、新技術等への対応などが挙げられる。

経産省・総務省ガイドラインの最新版は 2023 年 7 月に発行された第 1.1 版であり、医療

情報システムやサービスを提供する事業者向けに、より詳細な技術要件と運用基準を規定している。さらに、2024 年 10 月には第 2.0 版（案）が公表され、さらなる改定が予定されている。

これらのガイドラインは、個人情報保護法に基づく患者情報の保護を主たる目的としつつ、包括的なサイバーセキュリティ対策も規定している。特に、2023 年 6 月には厚生労働省から「医療機関におけるサイバーセキュリティ対策チェックリスト」が公表され、2024 年度中にサイバー攻撃を想定した BCP（事業継続計画）策定が求められるなど、サイバーセキュリティ対策の強化が進められている。

この背景には、医療機関に対するサイバー攻撃の増加がある。2023 年の調査によると、医療業界の約 67% が過去 1 年間にランサムウェア攻撃の被害を受けたと報告されており、セキュリティ対策の重要性が一層高まっている。

医療機関および関連事業者は、これらのガイドラインに基づき、適切な安全管理措置を講じることが求められる。特に、クラウドサービスの採用、AI 技術の導入、遠隔医療の実施など、新たな技術やサービスの導入時には、ガイドラインの要件を慎重に確認し、必要な対策を実施する必要がある。

また、ISMS やプライバシーマークなどの第三者認証制度との整合性も考慮されており、医療機関はこれらの認証制度も活用しながら、より高度な情報セキュリティ管理体制を構築することが推奨される。

医療分野のデジタルトランスフォーメーション進展に伴い、今後のガイドラインには、医療 IoT デバイスのセキュリティ、AI 活用時のデータ保護、遠隔医療システムのセキュリティなど、新たな技術領域への対応がさらに求められる。また、国際的なセキュリティ基準との整合性や、グローバルな医療情報連携への対応も重要な課題となっている。

4. 医療機器のサイバーセキュリティの本質

医療機器におけるサイバーセキュリティは、患者の生命と安全を守るための根幹的要素である。これは単なる技術的課題ではなく、高度な技術的専門知識と医療現場への深い洞察を必要とする複合的な課題として認識されている。医療技術の発展に伴い、サイバーセキュリティの重要性はますます高まっている。

医療機器の製造販売業者は、製品のライフサイクル全体を通じた包括的なサイバーセキュリティアプローチを実践する必要がある。設計段階では、セキュリティ・バイ・デザインの原則に基づき、潜在的な脅威分析とリスク評価を実施する。開発過程では、脆弱性検査やペネトレーションテストなどの安全性検証を徹底する。市販後は、新たな脆弱性の継続的な監視、セキュリティパッチの提供、インシデント対応体制の整備が求められる。

医療機器のサイバーセキュリティの確保には、多様なステークホルダーの協調が不可欠である。製造販売業者は製品の設計から保守までの責任を担い、医療機関は適切な運用と管理を行う。規制当局は必要な規制枠組みを提供し、医療従事者と患者はセキュリティ意識の向上と適切な機器使用を通じて貢献する。これらのステークホルダー間の緊密な連携と情報共

有が、効果的なサイバーセキュリティ対策の基盤となる。

ライフサイクル管理においては、各段階で適切なセキュリティ対策を実施する必要がある。開発段階では、セキュアコーディング、暗号化機能の実装、アクセス制御メカニズムの構築などの技術的対策を講じる。製造過程では、製造環境のセキュリティ確保と品質管理を徹底する。運用段階では、セキュリティ監視、脆弱性管理、インシデント対応など、継続的なセキュリティ維持活動を実施する。

技術的対策と運用的対策のバランスも重要である。最新のセキュリティ技術の導入に加えて、医療現場の実態に即した運用手順の確立が必要となる。具体的には、医療従事者への定期的な教育訓練、緊急時対応手順の整備、セキュリティインシデントを想定した実践的な訓練の実施が含まれる。

グローバルな視点では、国際的な規制調和の推進と情報共有の強化が不可欠である。医療機器の国際流通が一般的となる中、各国の規制要件の整合性確保やクロスボーダーでのセキュリティ情報の共有体制の構築が重要となっている。新たなサイバー脅威に対する早期警戒システムの確立や、国際的なインシデント対応体制の整備も求められている。

医療機器のサイバーセキュリティは、医療機器の基本的な安全性と有効性を確保するための不可欠な要素である。その実現には、最新の技術動向への対応、組織間の緊密な連携、そして患者安全への強い責任感が必要となる。さらに、急速に進化するサイバー脅威に対して、継続的な技術革新と対策の更新を行い、常に最適な防御態勢を維持することが求められる。

5. 医療機器のサイバーセキュリティにおけるマルチステークホルダーアプローチ

医療機器のサイバーセキュリティは、その複雑性と重要性から、単一の組織や個人による管理では対応が困難である。IMDRF ガイダンスが示すように、これは共同責任の領域であり、多様なステークホルダー間の緊密な連携と協力が不可欠である。

製造販売業者は、IMDRF ガイダンスに基づき、製品ライフサイクル全体を通じたサイバーセキュリティ対応の中核的責任を担う。具体的には、市販前の設計・開発段階におけるセキュリティ機能の組込み、リスクマネジメントの実施、セキュリティ試験の実施、適切な情報提

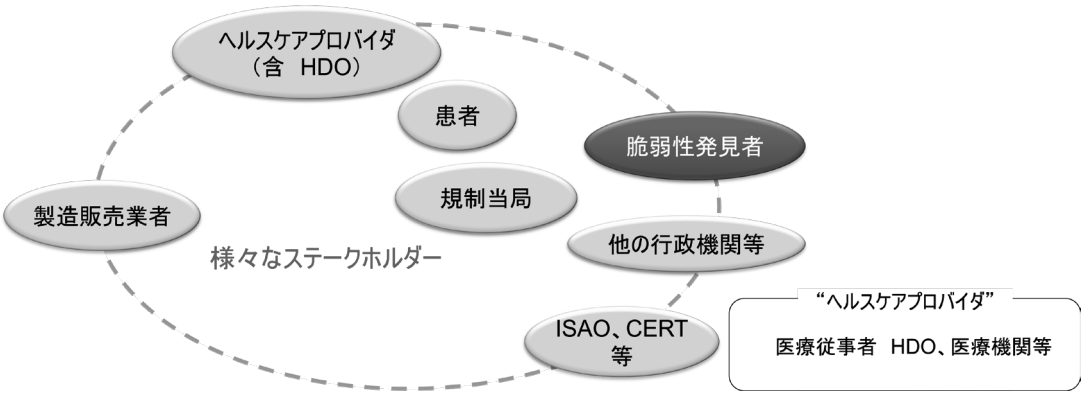

図 1-3 様々なステークホルダー

供の準備、そして市販後活動計画の立案が求められる。また、脆弱性が発見された場合の迅速な対応や、セキュリティアップデートの提供も重要な責務となる。

医療機関は、医療法に基づき、サイバーセキュリティ対策を含む医療安全確保の責任を負う。具体的には、適切なネットワーク分離の実施、アクセス制御の確立、セキュリティパッチの適時適用など、包括的な対策が必要となる。医療従事者には、セキュリティ脅威に対する適切な理解と、インシデント発生時の迅速な対応が求められる。

脆弱性発見者と研究者は、医療機器のセキュリティ向上に重要な貢献を果たす。IMDRF ガイダンスでは、製造販売業者が脆弱性発見者を含むステークホルダーと積極的に連携することの重要性が強調されている。特に、Coordinated Vulnerability Disclosure の枠組みを通じた責任ある脆弱性の開示と、製造業者との協力による適切な対策の実施が重要となる。

規制当局は、医療機器のサイバーセキュリティに関する規制の枠組みを整備し、必要なガイダンスを提供する。特に米国 FDA は、医療機器のサイバーセキュリティに関する包括的なガイダンスを発行し、製造業者に対する具体的なセキュリティ要件を定めている。

情報共有・分析組織（ISAO）の役割も重要である。IMDRF ガイダンスでは、製造販売業者が ISAO に積極的に参加することが推奨されている。特に H-ISAC は、医療分野における脅威情報の共有と分析において中心的な役割を果たしている。

これらのステークホルダー間の効果的な連携には、IMDRF ガイダンスが示すように、迅速な情報共有体制の確立が不可欠である。サイバーセキュリティに関する情報共有は、安全でセキュアな医療機器を実現するための基本原則となっている。

また、医療機器のサイバーセキュリティは国際的な課題であり、IMDRF ガイダンス自体が国際的な協力の成果である。今後も、技術の進化や脅威の変化に対応するため、国際的な協力体制の強化と継続的な知見の共有が重要となる。

このように、医療機器のサイバーセキュリティは、多様なステークホルダーの協調的な取り組みによって支えられている。各ステークホルダーがそれぞれの役割を適切に果たし、効果的な連携を維持することが、安全な医療機器の実現につながる。

6. 製造販売業者の責務

製造販売業者は、医療機器の有効性および安全性を確保する基本的責務を負う。医薬品医療機器等法に基づき、製品のライフサイクル全体を通じた安全性情報の収集・分析、必要な対策の実施が求められる。また、品質管理システム（QMS）および安全管理（GVP）の責任も負い、これには総括製造販売責任者、国内品質業務運営責任者、安全管理責任者の設置が含まれる。

サイバーセキュリティについては、使用環境を含めた医療機器の特性に応じた対応が必要となる。医療機関と適切に連携しながら、包括的なセキュリティ対策を実施する必要がある。

設計開発段階では、セキュリティ・バイ・デザインの原則に基づく取り組みが求められる。具体的には、医療機器の特性とリスクに応じた脅威分析とリスク評価を実施し、必要なセキュリティ機能を実装する。この際、各医療機器の使用目的や想定されるリスクに基づいて、適

切な技術的対策を選択する必要がある。

市販後は、新たな脆弱性や脅威の継続的な監視・評価を行い、必要に応じてセキュリティパッチやアップデートを提供する。脆弱性が発見された場合は、その影響を評価し、医療機関に適切な情報提供と対策方法の案内を行う。

製造販売業者は、インシデント発生時の対応手順と連絡体制を確立し、製品のサポート終了時期の適切な通知、必要なセキュリティ対策の提供を確実に実施する必要がある。また、医療機関職員に対して、製品の適切な使用方法やセキュリティ対策に関する教育訓練を提供することも求められる。

医療機器のサイバーセキュリティは、患者の安全を確保するための重要な要素である。製造販売業者は、規制当局の要求事項に従いながら、継続的な改善に取り組む必要がある。

国際的な医療機器の流通が一般的となる中、各国の規制要件への適合も重要となっている。特に、IMDRF ガイダンスなどの国際的な基準に基づく対応が求められる。また、AI 技術や IoT デバイスなどの新興技術を採用する場合は、それらに特有のリスクを評価し、適切な対策を講じる必要がある。

これらの責務を全うするためには、製造販売業者における組織的な取り組みが不可欠である。品質管理体制と安全管理体制を適切に整備し、患者の安全確保を最優先としたセキュリティ対策を実施することが求められる。

7. 医療機器の製品ライフサイクルにおけるサイバーセキュリティ対策

医療機器の製品ライフサイクル管理は、IMDRF ガイダンスに基づく体系的なサイバーセキュリティ対策を必要とする複合的なプロセスである。特に、JIS T 81001-5-1:2023（IEC 81001-5-1:2021）への適合性確認を通じて、セキュリティライフサイクルの要求事項を確保することが重要となる。

設計構想段階では、製品の使用目的と使用環境を考慮した詳細なセキュリティ要件分析を

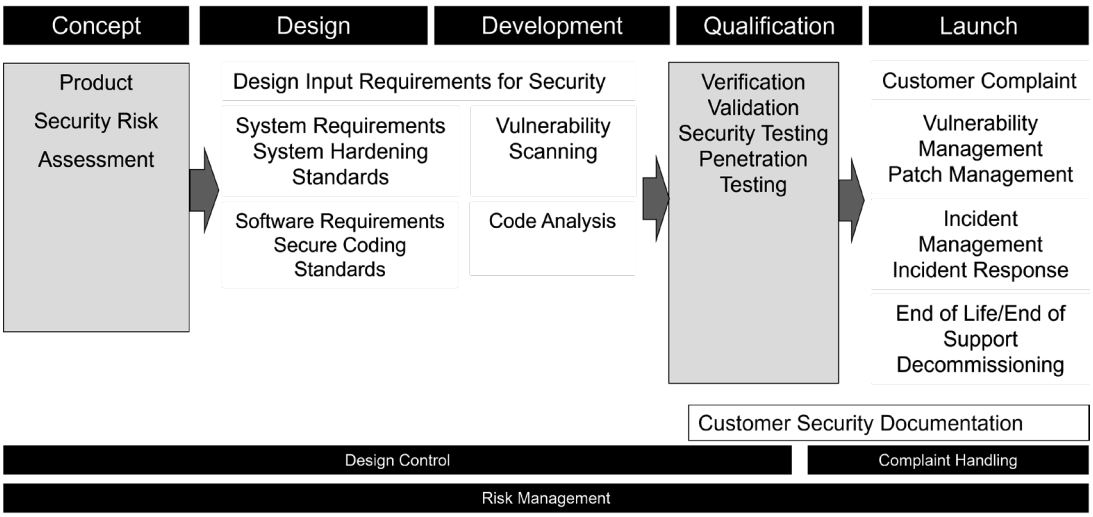

図 1-4 Total Product Life Cycle（製品ライフサイクルの全体）

実施する。この段階で、想定される脅威とリスクを特定し、必要なセキュリティ機能を定義する。医療機器の特性に応じた潜在的なセキュリティリスクの評価が不可欠である。

設計開発段階では、ISO 14971 に基づくリスクマネジメントプロセスと統合したセキュリティ対策を実装する。具体的には、セキュアな通信プロトコルの採用、アクセス制御機能の実装、データの暗号化など、必要なセキュリティ機能を組み込む。また、脆弱性スキャンやペネトレーションテストなどの包括的なセキュリティ検証を実施する。

市販後の段階では、継続的な脆弱性監視と管理が重要となる。これは新規製品だけでなく、レガシー製品を含む既存の医療機器も対象となる。製造販売業者は、新たに発見される脆弱性を評価し、必要に応じてセキュリティパッチやアップデートを提供する。

効果的なサイバーセキュリティ対策には、製造業者、医療提供者、ユーザー、規制当局、脆弱性発見者など、すべての関係者による情報共有と協力が不可欠である。インシデント対応プロセスは、製品ライフサイクル全体を通じて維持され、インシデントの検知、分析、対応、報告の体制整備が含まれる。

製品のサポート終了段階においても、適切なセキュリティ対策が必要である。製造販売業者は、サポート終了時期を適切に通知し、代替製品への移行計画や残存するセキュリティリスクへの対応策を提供する。

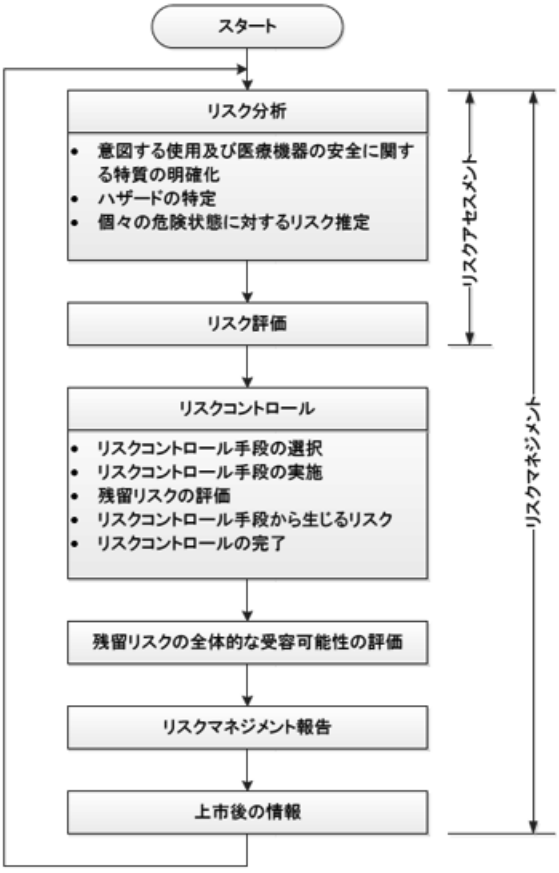

図 1-5 サイバーセキュリティとリスクマネジメント

医療機関向けの技術文書には、セキュリティ関連情報を適切に含める必要がある。これには、セキュリティ機能の説明、推奨される運用方法、既知のリスクとその対策などが含まれる。

グローバルな規制要件への対応も重要である。FDA や EU の MDR（Medical Device Regulation）など、各国・地域の規制要件に適合したセキュリティ対策を実施する必要がある。

このように、医療機器の製品ライフサイクル管理には、包括的なサイバーセキュリティ対策の実施が不可欠である。製造販売業者は、患者の安全を最優先としながら、継続的な監視と改善を通じて、適切なセキュリティレベルの維持に努める必要がある。さらに、すべての関係者との緊密な連携と情報共有を通じて、医療機器のセキュリティ確保に取り組むことが求められる。

8. 医療機器のサイバーセキュリティとリスク管理

医療機器のサイバーセキュリティは、ISO 14971 に基づく包括的なリスクマネジメントプロセスの重要な構成要素である。これは、製品のライフサイクル全体を通じた体系的なリスク管理アプローチとして実施される必要がある。

リスクマネジメントプロセスは、設計開発段階から開始される。この段階で、潜在的なサイバーセキュリティリスクを特定し、その影響度と発生確率を評価する。リスク分析を通じて想定される脅威を体系的に分析し、必要な対策を設計に組み込む。この初期段階でのリスク評価と対策の実装は、深刻な脆弱性を防ぐための基盤となる。

市販後のリスクマネジメントでは、新たな脆弱性や脅威の継続的な監視が不可欠である。これには、セキュリティ情報の収集・分析、脆弱性の影響評価、必要な対策の実施が含まれる。特に、医療機器の使用環境や接続状況の変化に伴う新たなリスクの評価と対応が重要となる。

サイバーセキュリティリスクの特徴として、技術の急速な進歩と攻撃手法の進化による状況の変化がある。このため、リスク評価は最新の脅威情報に基づいて定期的に見直す必要がある。

リスク管理プロセスは、リスク分析による潜在的な脅威と脆弱性の体系的な分析から始まり、特定されたリスクの重要度評価、適切な対策の実装へと進む。さらに、残留リスクの全体的な評価、リスクマネジメント報告書の作成、製造後の情報収集と分析までを含む包括的なプロセスとして実施される。

効果的なリスク管理を実現するためには、セキュリティ情報の収集・分析体制を整備し、インシデント対応手順を確立する必要がある。また、関係者間での情報共有体制を構築し、リスク評価結果の文書化と管理を適切に行うことが求められる。

医療機器のサイバーセキュリティリスク管理は、IMDRF ガイダンスが示す一般原則とベストプラクティスに従って実施される。また、医療機器の基本要件基準の改正により、サイバーセキュリティに関する具体的な要求事項が追加されている。

製造販売業者は、技術の進化や新たな脅威の出現に応じて、リスク管理プロセスを定期的に見直し、改善する必要がある。このプロセスは、医療機器の開発、製造、保守に関わるす

べての関係者の協力のもとで実施される必要がある。

9. 医療機器のリスク分析と評価のタイミング

医療機器のリスク分析と評価は、ISO 14971 および IMDRF ガイダンスに基づく体系的なプロセスとして実施される。このプロセスは、製品のライフサイクル全体を通じて継続的に実施され、特にサイバーセキュリティリスクについては、新たな脅威への対応を常に考慮する必要がある。

初期開発段階でのリスク分析は、製品の基本的な安全性を確保する上で最も重要である。この段階では、想定される使用環境と使用条件の特定、潜在的な脆弱性の体系的な評価、セキュリティ要件の定義と設計への組み込み、そして予測可能な誤使用の分析について詳細な分析を行う。

開発プロセスの各段階においては、設計段階でのアーキテクチャレベルでのセキュリティリスク評価、実装段階でのコードレベルでのセキュリティ脆弱性分析、検証段階でのセキュリティテストと脆弱性評価、そして妥当性確認段階での総合的なリスク評価を実施する。

市販前のリスク分析では、意図された使用環境における安全性、既知の脆弱性とその対策、セキュリティ機能の有効性、そして残留リスクの受容可能性を包括的に評価する。

市販後のリスクモニタリングでは、新たな脆弱性情報の収集と分析、実使用環境からのフィードバック評価、セキュリティインシデントの分析、必要に応じたリスク再評価を継続的に実施する。

特に生命維持装置や植込み型医療機器など、患者の生命に直接影響を与える可能性のある機器については、より厳密なリスク分析とモニタリングが求められる。これには、機器固有の重要機能の特定、詳細な脅威モデリング、厳格な安全性評価基準の適用、継続的な安全性モニタリングが含まれる。

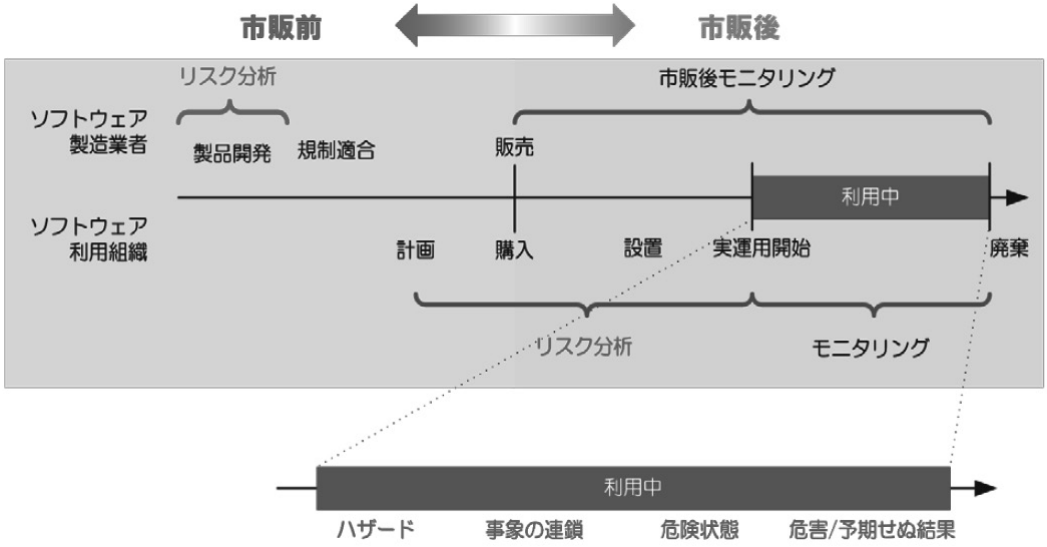

図 1-6 リスク分析と評価のタイミング

リスク分析と評価は、関連する規制要件の変更や新たな技術の導入に応じて、適切に更新される必要がある。また、グローバルな医療機器の流通を考慮し、各国の規制要件や使用環境の違いも考慮に入れる必要がある。

製造販売業者は、これらのリスク分析と評価のプロセスを文書化し、その結果に基づいて適切な対策を実施する。また、新たな脅威や使用環境の変化に応じて、リスク評価手法自体も継続的に改善していく必要がある。

10. 設計段階におけるサイバーセキュリティ対策

医療機器の設計段階におけるサイバーセキュリティ対策は、IMDRF ガイドラインが定めるセキュリティ・バイ・デザインの原則に基づき実施される。これは製品の初期設計から体系的なセキュリティ対策を組み込む取り組みであり、製品のライフサイクル全体を通じた安全性確保の基盤となる。

使用環境の分析では、医療機関内での使用形態と接続環境、外部ネットワークとの接続シナリオと潜在的リスク、モバイルデバイスとの連携における脆弱性、在宅医療における使用環境の特殊性、そして緊急時の運用における安全性確保について詳細に評価する必要がある。

セキュリティ要件の設計では、IMDRF ガイドラインおよび関連規制に基づき、多要素認証を含む堅牢な認証メカニズム、保管時および伝送時のデータ暗号化、最新の規格に準拠した通信プロトコル、役割ベースのアクセス制御、そしてセキュリティイベントの包括的なログ管理といった基本的対策を実装する。

設計段階での重要な考慮事項として、ISO 14971 に基づく体系的な脆弱性分析とリスク評価、セキュアな開発プロセスの採用と文書化、サードパーティコンポーネントのセキュリティ評価、包括的なセキュリティテスト計画の策定と実施が含まれる。

運用面での考慮事項として、効率的なセキュリティアップデートの提供メカニズム、インシデント対応手順の明確化、技術文書の整備と維持管理体制、そしてメンテナンス性を考慮したモジュール設計を設計に組み込む。

このように、設計段階でのサイバーセキュリティ対策は、技術的対策と運用的対策を統合した体系的なアプローチが必要である。製造販売業者は、最新の規制要件とベストプラクティスに基づき、患者の安全を最優先とした実効性のある対策を実装することが求められる。

11. 市販後のサイバーセキュリティ対策

医療機器の市販後におけるサイバーセキュリティ対策は、製品の安全性と有効性を継続的に確保するための重要な活動である。これは、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による共同責任として位置付けられている。

IMDRF ガイダンスによれば、レガシー医療機器は「現在のサイバーセキュリティの脅威に対して合理的に保護できない医療機器」と定義される。このような医療機器に対しては、医療機関や医療従事者に対して代替策を検討する十分な期間を設けた上で、段階的な使用停止を進めることが求められる。

製造販売業者には、新たな脆弱性の監視と評価、リスクアセスメントの定期的な実施、必要に応じたセキュリティパッチの提供、適切な技術的サポートの維持といった継続的な対応が求められる。

2023年3月31日の医療機器基本要件基準改正により、第12条第3項としてサイバーセキュリティに関する要求事項が規定された。これに基づき、市販後の段階的な対応として継続的なセキュリティモニタリング、新たな脅威への対応策の策定、セキュリティ情報の関係者との共有、インシデント発生時の迅速な対応体制の整備が必要とされる。

補完的なセキュリティ対策として、適切なネットワークセグメンテーション、多層的なアクセス制御の実装、包括的な監視体制の確立、定期的なセキュリティ評価の実施が推奨される。

製品のライフサイクル管理においては、製品や状況に応じた柔軟な対応が必要である。特に、製品寿命終了（EOL）やサポート終了（EOS）時期の対応については、製造販売業者と医療機関との間で適切な計画と合意形成が求められる。

これらの対策を効果的に実施するためには、関係者間の継続的な協力と情報共有が不可欠である。特に、新たな脅威や脆弱性が発見された場合の迅速な情報共有と対応が、医療機器の安全な運用を確保する上で重要となる。

12. レガシー医療機器の定義と課題

IMDRFガイダンスによれば、レガシー医療機器とは、現在のサイバーセキュリティの脅威に対して合理的な保護が困難な医療機器と定義される。この定義は製品の経過年数ではなく、現在のセキュリティ要件への対応能力を基準としている。

製造販売業者には、製品ライフサイクル全体を通じたサイバーセキュリティ維持計画の策定、脆弱性情報の継続的な収集と評価、セキュリティ関連情報の医療機関への提供、ソフトウェア部品表（SBOM）の提供、そしてサポート終了時期の明確な通知とリスクの説明といった責務がある。

医療機関向けの技術的対策として、エアギャップによる完全なネットワーク分離の検討、ネットワークセグメンテーションの実装、セキュアな構成設定の適用、強固なアクセス制御の実装、バックアップと復元手順の確立、そして定期的なセキュリティ評価の実施が含まれる。

重要な考慮事項として、医療機器の臨床的重要性とサイバーセキュリティリスクのバランス評価、既存のセキュリティ機能の限界の把握、レガシー機器の段階的な使用停止計画の策定、代替機器への移行計画の立案、継続的なリスク評価と対策の見直しが挙げられる。

特に重要な課題として、レガシー機器のライフサイクル段階の明確な定義、各段階における責任の共有モデルの確立、医療機器製造業者と医療提供組織間の透明性向上、効果的なデータ共有体制の構築、技術的な制約に対する現実的な対策の実装、そして運用上のリスクの継続的な評価と管理が挙げられる。

このように、レガシー医療機器の管理には、技術的対策と運用的対策を組み合わせた包括

的なアプローチが必要である。製造販売業者、医療機関、規制当局の緊密な連携のもと、患者の安全確保を最優先とした対応が求められる。この取り組みは、医療機器のライフサイクル全体を通じた継続的なプロセスとして実施される必要がある。

13. 製品ライフサイクルにおけるレガシー医療機器の概念フレームワーク

医療機器のサイバーセキュリティ管理においては、製品ライフサイクル全体を通じたフレームワークが不可欠である。このフレームワークは、製造販売業者（MDMs）と医療機関（HDOs）の役割と責任を明確に定義し、効果的なセキュリティ管理を実現する基盤となる。

開発段階における製造販売業者の責任として、セキュリティ・バイ・デザインの原則に基づく開発の実施、包括的なリスク分析と対策の設計への組み込み、セキュリティ機能の実装と検証、ソフトウェア部品表（SBOM）の作成と維持管理、そしてセキュリティテストと脆弱性評価の実施が含まれる。

商業リリース段階における製造販売業者の責任として、製品ライフサイクルの重要なマイルストーンの明確な提示、サイバーセキュリティサポート期間の明示、セキュリティアップデート提供計画の策定と通知、そして脆弱性情報の継続的な収集と評価が求められる。

製品寿命終了（EOL）における対応について、製造販売業者側では、サポート終了スケジュールの明確な通知、移行期間中の継続的なセキュリティサポート、代替製品に関する詳細情報の提供、残存リスクの評価と対策指針の提示が必要となる。医療機関側では、代替システムへの移行計画の策定、リスク評価に基づく追加セキュリティ対策の実装、運用手順の見直しと更新、職員への教育訓練の実施が求められる。

商業的サポート終了（EOS）後の医療機関の責任として、包括的なセキュリティ対策の実装、ネットワークセグメンテーションの強化、アクセス制御の厳格化、定期的なセキュリティ評価の実施、そしてインシデント対応手順の整備が含まれる。

フレームワークの実効性確保のための要件として、製造販売業者と医療機関間の緊密な情報共有体制、脅威情報の継続的な更新と評価プロセス、リスク管理戦略の定期的な見直しと

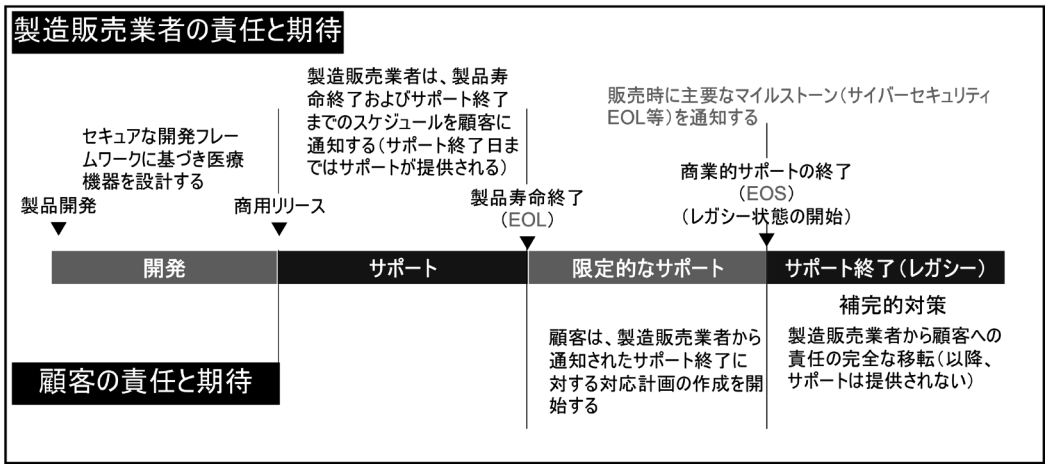

図 1-7 レガシー医療機器の概念フレームワーク

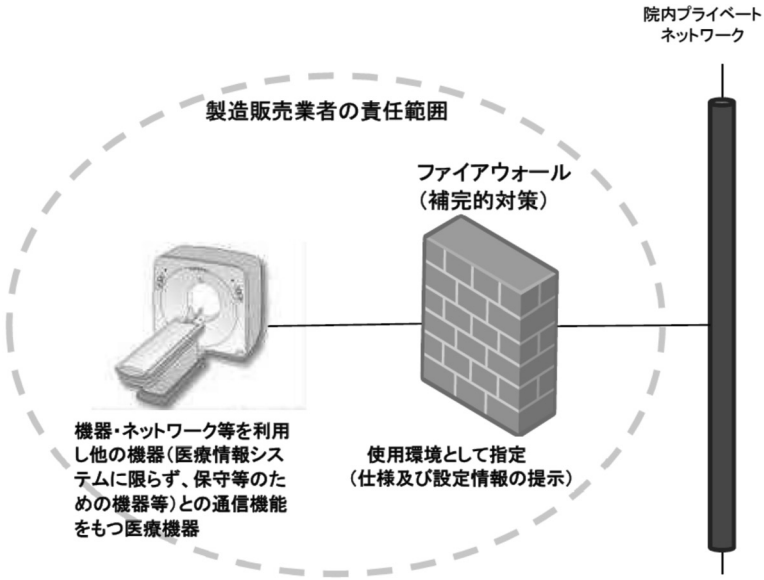

図 1-8 補完的対策としてファイアウォール等を設置する

更新、そして患者安全を最優先とした意思決定メカニズムが挙げられる。

このフレームワークは、医療機器のサイバーセキュリティを製造販売業者と医療機関の共同責任として位置付け、継続的な改善と更新を前提としている。新たな脅威の出現や技術の進化に応じて、フレームワーク自体も適切に更新される必要がある。

14. 補完的対策

医療機器のサイバーセキュリティ対策における補完的な対策は、包括的な防御体制を構築するための重要な戦略的アプローチである。特に IMDRF ガイダンスで定義される「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」であるレガシー医療機器や高度な脆弱性を内包する医療機器に対しては、ファイアウォールを基軸とした多層的な防御戦略が不可欠である。

製造販売業者は、医療機器がレガシー状態になることを想定し、適用可能なファイアウォール等の補完的対策の具体的な仕様および利用可能性について、事前に詳細な検討を行う必要がある。これには、想定されるセキュリティリスクの分析、具体的な対策手法の選定、実装方法の検討などが含まれる。

医療機関における具体的な実装としては、ネットワークポートの厳格な制限や、院外ネットワークとの接続に対する強力な制御を実施することにより、潜在的なサイバーセキュリティリスクを大幅に低減することが可能となる。さらに、医療機器に保存される、または送受信される安全性関連データについては、適切な暗号化技術の適用による保護が不可欠である。

ネットワーク分離は、特に高度なサイバーセキュリティリスクを有する医療機器に対して極めて有効な対策手法である。具体的には、VLAN の適用、物理的なネットワークの分離、

マイクロセグメンテーションなどの技術を活用することで、効果的なネットワーク分離を実現できる。これにより、一部の医療機器や端末が侵害された場合でも、他のシステムへの影響を最小限に抑制することが可能となる。

補完的対策の実効性を確保するためには、IMDRF ガイダンスに基づく国際的な調和の取り組みを考慮しつつ、医療機器の製造販売業者と医療機関との緊密な連携体制の構築が不可欠である。製造販売業者は、自社が提供する医療機器に対する具体的なセキュリティ対策の推奨事項や、効果的な防御戦略に関する詳細な技術情報を、医療機関に対して適時に提供する必要がある。

高度なセキュリティ対策として、次世代型の侵入検知システム（IDS）および侵入防止システム（IPS）の導入、セキュリティ情報とイベント管理（SIEM）システムの活用が推奨される。これらのシステムを統合的に運用することで、リアルタイムな脅威検知と対応が可能となる。また、定期的なペネトレーションテストの実施により、セキュリティ対策の実効性を継続的に評価することが重要である。

医療従事者に対する体系的かつ継続的なセキュリティ教育・訓練の実施も不可欠である。これには、最新のサイバーセキュリティ脅威に関する知識の習得、適切な対応手順の理解、実践的な訓練などが含まれる。

新たなサイバーセキュリティ脅威を継続的に監視し、評価・分析する体制の整備も重要である。特に、在宅医療や遠隔医療などの新しい医療提供形態においては、従来の医療機関内での使用環境とは異なる特有のリスクが存在するため、それぞれの利用環境に特化した追加的なセキュリティ対策の検討と実装が求められる。

15. 医療機関との連携

医療機器のサイバーセキュリティにおいて、医療機関との連携は極めて重要かつ複雑な課題である。医療機関のネットワークセキュリティに脆弱性が存在する場合、医療提供体制に影響を及ぼすリスクが生じる可能性がある。このため、医療機関は医療機器のネットワークへの接続状況を可視化し、関係者と共有するためのネットワーク構成図等を整備することが有用である。

製造販売業者は、自社の医療機器においてサイバーセキュリティの脆弱性を発見した場合、ガイドラインや業界のベストプラクティスに基づき、速やかに各医療機関への通知を行う必要がある。この通知を受けた医療機関は、リスク評価に基づき、必要に応じて当該機器の使用を一時的に停止し、ネットワークからの分離等の適切な対応を実施する必要がある。

脆弱性情報の伝達においては、情報セキュリティの三要素である機密性、完全性、可用性のバランスを考慮した慎重な対応が求められる。特に重要な懸念事項として、信頼性の確保されていない経路での脆弱性情報の伝達が、意図しない第三者への情報漏洩リスクを生じさせる可能性がある。

製造販売業者は、脆弱性の通知方法について、事前に各医療機関との間で具体的な取り決めを行う必要がある。この取り決めには、通知の具体的な手段、緊急度に応じた通知のタイ

ミング、開示する情報の範囲と詳細度、対応手順などが含まれる。また、医療機器事業者は医療機関からの要請に適切に対応できるよう、組織的な準備体制を整えておくことが重要である。

製造販売業者と医療機関の連携は、インシデント対応に限定されない、継続的かつ戦略的なパートナーシップとして構築される必要がある。これには、定期的な情報交換会の開催、共同でのリスクアセスメントの実施、最新のサイバーセキュリティ動向に関する情報共有体制の確立などが含まれる。特に、医療機関がサイバーセキュリティ対応の重要性を十分に理解し、積極的な連携体制を構築することが不可欠である。

この連携においては、技術的な対応にとどまらず、組織文化とセキュリティ意識の共有・醸成が重要である。製造販売業者は、医療機関の職員に対するサイバーセキュリティ教育プログラムの提供、リスク管理ガイドラインの策定支援、緊急時対応計画の共同開発など、包括的な支援体制を構築する必要がある。

サイバーセキュリティリスクの多様化と進化の速さを考慮すると、医療機関との連携は特定の部門や担当者のみで対応できる範囲を超えている。製造販売業者と医療機関の双方において、組織全体でセキュリティに対する高い意識と責任感を共有し、部門横断的な協力体制を確立することが、効果的なリスク管理の基盤となる。

最終的な目標は、患者の安全確保と医療サービスの継続性維持にある。製造販売業者と医療機関は、相互の信頼関係を基盤として、医療機器のサイバーセキュリティに対する積極的かつ持続的な取り組みを推進していく必要がある。この目標達成のためには、両者が共通の価値観とビジョンを持ち、継続的な改善と発展を目指す姿勢を保持することが重要である。

16. ソフトウェア部品表（SBOM）

ソフトウェア部品表（SBOM: Software Bill of Materials）は、医療機器のサイバーセキュリティ管理において不可欠な文書である。SBOM は、医療機器に使用されているすべてのソフトウェアコンポーネントを体系的に文書化し、それらの依存関係を明確化する包括的な一覧として定義される。このツールは、医療機器の開発段階から市販後の管理まで、製品ライ

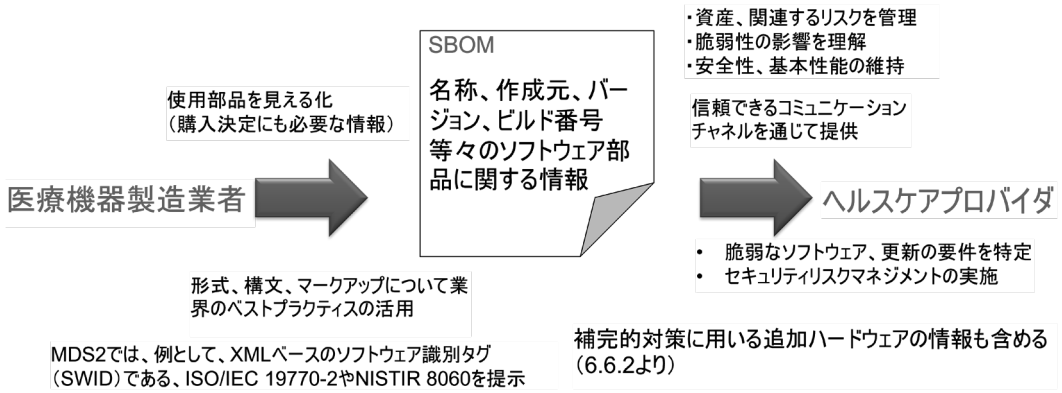

図 1-9 ソフトウェア部品表（SBOM）

フサイクル全体を通じて活用される。

SBOM の主要な目的は、医療機器製造販売業者が医療機関に対して、ソフトウェアの構成情報を透明性をもって提供することにある。SBOM には、各ソフトウェアコンポーネントの名称、サプライヤー、バージョン、ライセンス情報、依存関係、既知の脆弱性などの詳細情報が含まれる。この情報は、製品導入前のリスク評価から、導入後の継続的なセキュリティ管理まで、幅広い用途で活用される。

SBOM の戦略的機能として、すべてのソフトウェア資産とそれに関連するリスクの包括的な管理を可能にする点が挙げられる。使用されているソフトウェアコンポーネントの詳細な情報により、潜在的な脆弱性の早期特定と評価が可能となり、セキュリティインシデントへの対応時間を大幅に短縮することができる。また、特定の脆弱性がシステム全体に及ぼす影響を正確に把握することで、効果的なリスク管理が実現される。

SBOM の形式と構文については、国際的な標準規格の採用が推奨される。具体的には、SPDX（Software Package Data Exchange）、CycloneDX、SWID（Software Identification Tag）などの標準フォーマットが広く採用されている。これらの標準化された形式は、SBOM の相互運用性を確保し、効率的な情報共有を実現する。特に近年、米国 FDA は新しい医療機器申請者に SBOM の提供を要求するなど、規制要件としての重要性も高まっている。

SBOM は医療機器のライフサイクル全体を通じて継続的に更新される動的な文書として管理される必要がある。ソフトウェアの更新、セキュリティパッチの適用、新規脆弱性の発見などの変化に応じて、適時適切な更新が不可欠である。これらの更新情報は、関係するステークホルダーに対して速やかに共有される必要がある。

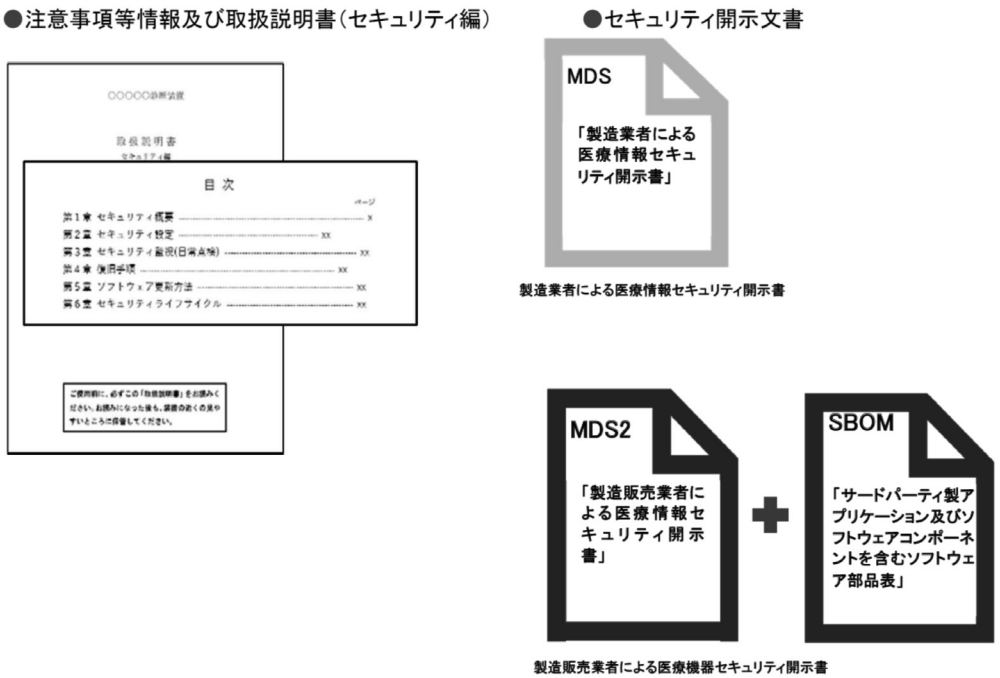

図 1-10 サイバーセキュリティに関する顧客向け文書

医療機器のサプライチェーンセキュリティにおいて、SBOMは重要な役割を果たす。製造販売業者と医療機関が協力して、SBOMを活用した継続的かつ包括的なリスク管理を実施することは、患者安全の確保において不可欠である。特に、医療機器の複雑化とソフトウェア依存度の増加に伴い、SBOMの重要性は一層高まっている。

SBOMの効果的な運用により、医療機器のサイバーセキュリティ全体の透明性と信頼性が向上し、より強固なセキュリティ管理体制の構築が可能となる。これは、医療機器の安全性確保と、効果的な医療サービスの提供に直接的に貢献する重要な要素である。

17. サイバーセキュリティに関する顧客向け文書

医療機器のサイバーセキュリティに関する顧客への情報提供は、医療機器の安全な運用と効果的なリスク管理において極めて重要な役割を果たす。医療機器製造販売業者は、製品のサイバーセキュリティに関する包括的な情報を、標準化された形式で医療機関に提供することが求められる。

製造販売業者が提供する主要な文書の一つは、製造販売業者による医療情報セキュリティ開示書（MDS2: Manufacturer Disclosure Statement for Medical Device Security）である。DS2は標準化されたフォーマットを持ち、医療機器のセキュリティ機能、脆弱性、およびリスク管理に関する情報を、特定の質問項目に対する回答形式で体系的に文書化したものである。この文書は通常、医療機関からの要請に応じて提供され、医療機関における適切なリスク評価と管理の基盤となる。

MDS2は、セキュリティ機能のケイパビリティ、認証メカニズム、監査機能、ネットワーク接続性、データの完全性とプライバシー保護機能、システムとアプリケーションの強化機能といった標準化された項目について情報を提供する。

もう一つの重要な文書であるソフトウェア部品表（SBOM）は、医療機器に使用されているすべてのソフトウェアコンポーネントの詳細な構成情報を提供する。SBOMには、各コンポーネントの名称、バージョン、サプライヤー、ライセンス情報、依存関係などが記載され、医療機関がソフトウェア構成を正確に把握し、潜在的なセキュリティリスクを評価することを可能にする。特に、2023年12月に成立した米国の法律により、「サイバーデバイス」に分類される医療機器については、SBOMの提供が義務化されている。

これらの文書は、製造販売業者の定める方針に従って提供され、必要に応じて更新される。特に、新たな脆弱性が発見された場合や、ソフトウェアが更新された場合には、適切なタイミングでの情報更新と共有が求められる。

製造販売業者は、これらの文書を通じて、医療機関に対して医療機器のセキュリティ機能と設定オプション、既知の脆弱性とその対策、推奨されるセキュリティ設定と構成、そしてインシデント発生時の対応手順といった情報を明確に提供する。

これらの文書は、単なるコンプライアンス要件の充足ではなく、医療機器の安全な運用を実現するための実践的なツールとして機能する。医療機関は、提供された情報を基に、自施設の環境に適したセキュリティ対策を検討し、実装することができる。

さらに、これらの文書を通じた情報共有は、製造販売業者と医療機関の間でサイバーセキュリティに関する共通認識を形成し、効果的な協力体制の構築を促進する。この協力体制は、変化し続けるサイバーセキュリティの脅威に対して、迅速かつ適切に対応するための基盤となる。

18. 医療機器のサイバーセキュリティに関するよくある誤解

医療機器のサイバーセキュリティ対策において、製造販売業者の間にいくつかの重要な誤解が存在し、これらが適切な対応の障壁となっている場合がある。これらの誤解を正しく理解し解消することは、効果的なセキュリティ対策の実施において極めて重要である。

最も一般的な誤解の一つは、医療機器の承認・認証後にオペレーティングシステム（OS）環境への新規パッチを適用する際に、必ず一部変更承認申請（一変申請）が必要であるという認識である。厚生労働省の通知によれば、当該更新が医療機器の有効性、品質、安全性能に影響を及ぼさないことが確認できる場合、このようなセキュリティ面の改修は軽微変更で対応可能である。ただし、個別の状況によっては一部変更承認申請が必要となる場合もあるため、製造販売業者は影響度を慎重に評価したうえで判断を行う必要がある。

第二の重要な誤解は、医療機器の OS 環境にインストールされたウイルス対策ソフトウェアのパターンファイル更新について、常に改修申請が必要であるという考えである。実際には、このようなアップデートが医療機器の機能や性能に影響を与えない場合、改修手続きの対象とはならない。ただし、製造販売業者は更新による影響を事前に評価し、その評価結果を適切に文書化することが求められる。

これらの誤解は、重要なセキュリティパッチの適用遅延による脆弱性の継続、不必要な承認申請手続きによる業務効率の著しい低下、緊急性の高いサイバーセキュリティリスクへの対応遅延、そして医療機器の安全性確保に関する判断の誤りといった具体的な問題を引き起こす可能性がある。

製造販売業者は、これらの誤解を解消し、より適切なサイバーセキュリティ対応を実施するため、セキュリティパッチの影響評価プロセスの確立、迅速な更新プロセスの構築、社内教育の充実、そして規制当局との適切な対話といった具体的な対応を行う必要がある。

製造販売業者は、セキュリティ対策の実施に関する明確な判断基準を確立し、組織内で共有する必要がある。具体的には、パッチ適用の具体的な判断基準と実施手順、影響評価の具体的な方法と必要な文書化の範囲、緊急時の対応フローと意思決定プロセス、そして規制当局への相談が必要となるケースの明確な基準といった要素を含める。

これらの誤解の解消と適切な対応の実施は、医療機器のサイバーセキュリティ全体の向上に直接的に寄与する。製造販売業者は、患者の安全確保を最優先としつつ、効果的かつ迅速なセキュリティ対策を実施できる体制を構築することが求められる。また、これらの取り組みについては、定期的な見直しと改善を行い、変化するサイバーセキュリティの脅威に適切に対応できる体制を維持することが重要である。

19. ヘルスソフトウェアと法規制対象

医療分野におけるソフトウェアの法規制は、複雑で多層的な構造を持っている。医療分野のソフトウェアは、医薬品医療機器等法（薬機法）に基づく医療機器プログラムと、規制対象外のヘルスケアソフトウェアに大別される。

医療機器プログラムには、以下の形態が含まれる。

・ハードウェアに組み込まれたソフトウェア

・独立した単体プログラム

・SaMD（Software as a Medical Device）

これらは、その使用目的や機能に基づいて医療機器としての該当性が判断される。一方、医療機器に該当しないヘルスソフトウェアであっても、サイバーセキュリティの観点からは等しく重要な保護対象となる。サイバー攻撃者は、医療機器であるか否かという法的区分を

ソフトウェアの種類	プラットフォーム	説　明	法規制対象の有無
ヘルスソフトウェア	医療機器または医療機器の一部のハードウェアで動作する	「医療機器ソフトウェア」のうち、開発中の医療機器に組み込むことを目的として開発されたもの	法規制対象
	汎用（非医療用）コンピューティングプラットフォームで動作する	A:「医療機器ソフトウェア」のうち、それ自体を医療機器として使用することを意図したもの	法規制対象
		B:「法規制対象外のヘルスソフトウェア」のうちリスクの考慮が必要なもの	法規制対象外
		C:「法規制対象外のヘルスソフトウェア」のリスク考慮の必要がないもの	法規制対象外

図 1-11 ヘルスソフトウェアと法規制対象

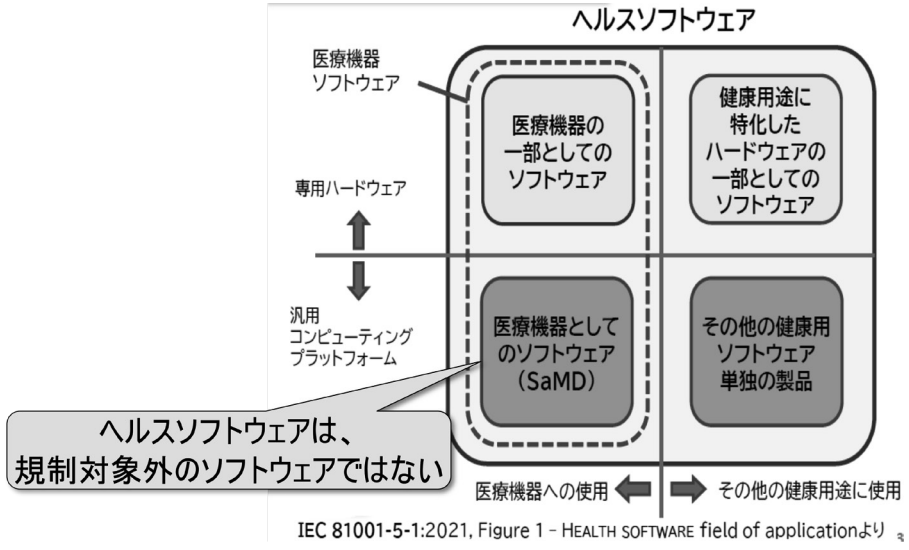

図 1-12 ヘルスソフトウェアと法規制対象

考慮せず、システムの脆弱性を標的とするため、法規制の有無にかかわらず、包括的なセキュリティ対策が必要となる。

IEC 81001-5-1 規格は、医療機器に限定されない包括的なアプローチを採用しており、ヘルスソフトウェア全般のセキュリティ要件を規定している。この規格は、ヘルスソフトウェアの安全性、有効性、セキュリティを総合的に評価するためのフレームワークを提供し、医療情報システム全体のセキュリティ確保に寄与する。

医療機関および製造販売業者は、法規制の対象であるか否かにかかわらず、すべてのヘルスソフトウェアについてサイバーセキュリティリスクを評価し、適切な対策を実施する必要がある。この対策には、技術的対策だけでなく、運用面での対策も含めた総合的なアプローチが求められる。

デジタルヘルスケアの急速な発展により、人工知能（AI）を活用した健康管理アプリケーションやウェアラブルデバイスと連携するヘルスケアソフトウェアなど、従来の法規制の枠組みでは十分に対応できない新たな形態のソフトウェアが登場している。これらのソフトウェアに対しても、適切なセキュリティ対策の実施が不可欠である。

医療分野のデジタル化が進展する中、ヘルスソフトウェアのセキュリティ確保は、医療システム全体の信頼性と安全性を維持するための重要な要素となっている。法規制の枠組みを超えた包括的なセキュリティ対策の実施が、今後ますます重要となることが予想される。

第2章

サイバーセキュリティの年表

1. サイバーセキュリティの年表

医療技術の進歩は、現代の医療機器の能力を根本的に変革し続けている。高度な診断技術から治療機器まで、医療機器の電子化とネットワーク化は、患者のケアと医療サービスの質を大きく向上させてきた。急性症状の迅速な治療や慢性疾患の長期的な管理を可能にする先進的な医療機器は、医療現場に革新的な変化をもたらしている。これらの技術革新は同時に、より複雑で高度なサイバーセキュリティの課題を浮き彫りにしている。

医療機器のサイバーセキュリティの歴史的発展は、技術の進歩と共に段階的に変化してきた。1960 年代から 1980 年代にかけては、医療機器の電子化が始まり、主にシステムの信頼性と安全性が課題となっていた。この時期のサイバーセキュリティに関する記録は限られているものの、ソフトウェアの不具合やシステムの誤作動への対応が始まっていた。

埋め込み型医療機器は 1950 年代から存在していたが、1990 年代に入ると、これらの機器のデジタル化と高度化が急速に進展した。特にペースメーカーやインスリンポンプなどの生命維持に直結する機器において、デジタル制御とプログラマブル機能の実装が進み、新たなセキュリティ課題が生まれることとなった。

2000 年代後半から 2010 年代初頭にかけて、医療機器のネットワーク接続が一般化し始め、外部からの不正アクセスやマルウェア感染のリスクが認識され始めた。特に 2014 年頃からは、医療機器のサイバーセキュリティが本格的に注目されるようになり、具体的な規制の整備が進められている。例えば、PMDA による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の発行や、製造業者による脆弱性対策の実装が積極的に進められている。

現在では、医療機器がインターネットに接続され、病院情報システム（HIS）や電子カルテシステムと連携する機会が増加している。これに伴い、医療機器のセキュリティリスク管理は、患者の安全と医療サービスの継続性を確保する上で極めて重要な課題となっている。製造業者、医療機関、規制当局が協力して、サイバーセキュリティ対策の強化に取り組んでおり、開発段階からセキュリティを考慮したセキュリティ・バイ・デザインの考え方も普及しつつある。

1.1. 第 1 期：複雑なシステムと偶発的な障害（1980 年代～現在）

1980 年代以降、医療機器システムの複雑化に伴い、偶発的な障害が重要な課題として認識されるようになった。この時期を象徴する事故として、1985 年から 1987 年にかけて発生した Therac-25 放射線治療装置の事故が挙げられる。この事故では、ソフトウェアの不具合とヒューマンエラーが重なり、6 名の患者が危険な放射線被ばくを受けるという深刻な事態が発生した。

Therac-25 は、低エネルギーの電子ビーム（ベータ粒子）と X 線の 2 種類の放射線を照射できる治療装置として開発された。開発者たちは「機器の安全性はソフトウェアでも十分に実現できる」との考えから、コスト削減を目的として従来の電気機械式の安全保護装置をソフトウェア制御に置き換えた。この判断が重大な結果をもたらすことになる。正式な訓練を受けていないプログラマーが独自に作成したオペレーティングシステムには、発見が困難

執 筆 者

村山 浩一（むらやま こういち）
株式会社イーコンプライアンス 代表取締役

【経歴】

1986 年 4 月　日本ディジタルイクイップメント株式会社（日本 DEC） ソフトウェアサービス部　入社
- GCP 管理システム、症例データ管理システム企画・開発担当
（現 ClinicalWorks/GCP/CDM）
- 改正 GCP（J-GCP）に対応した標準業務手順書作成コンサルティング
- 製薬業界におけるドキュメント管理システム導入コンサルティング

1999 年 1 月　日本ディジタルイクイップメント株式会社　退社
1999 年 2 月　日本アイ・ビー・エム株式会社　コンサルティング事業部　入社
- NY の TWG（The Wilkerson Group）で製薬業界に特化したコンサルタントとして研修
- 製薬企業におけるプロセス　リエンジニアリング担当
- Computerized System Validation(CSV)、21 CFR Part11 コンサルティング

2001 年 7 月　IBM 認定主幹コンサルタント
- アイビーエム・ビジネスコンサルティングサービス株式会社へ出向
マネージング・コンサルタント

2004 年 7 月　日本アイ・ビー・エム株式会社　退社
2004 年 8 月　株式会社イーコンプライアンス　設立
現在に至る。

【活動】

医薬品業界・医療機器業界を担当し 30 年以上のキャリアをもつ。

医薬品企業･医療機器企業における､コンピュータ化システムの品質保証（CSV､Part11 対応）をはじめ、リスクマネジメント、CAPA（是正処置および予防処置）、QMS 構築支援、FDA 査察対応等のコンサルテーションなどを幅広く展開している。

サイエンス＆テクノロジー株式会社におけるセミナー開催多数。

【主な著書】

- 実践ベンダーオーディット実施の手引き（2008 年）イーコンプライアンス刊
- コンピューターシステムバリデーション・厚労省 ER/ES 指針・21 CFR Part 11「社内監査の手引き」（2009 年）イーコンプライアンス刊
- GAMP5,Annex11, 厚労省 CSV 指針を基礎から解説【超入門シリーズ 1】コンピュータバリデーション（2009 年）イーコンプライアンス刊
- 【厚労省新ガイドライン対応シリーズ】医薬品・医薬部外品製造販売業者における「コンピュータ化システム適正管理ガイドライン」対応準備の手引き（2010 年）イーコンプライアンス刊

著 者 紹 介

- GAMP 5, FDA, ANNEX 11 に対応した【改定版】コンピュータバリデーション実施の手引き（2011 年）イーコンプライアンス刊
- 対応のためのガイドラインサンプル付【改定版】厚労省 ER/ES 指針対応実施の手引き（2011 年）イーコンプライアンス刊
- 【要点をわかりやすく学ぶ】製薬･医療機器企業におけるリスクマネジメント（2015 年）サイエンス＆テクノロジー刊
- 【要点をわかりやすく学ぶ】PIC/S GMP Annex15 適格性評価とバリデーション（2015 年）サイエンス＆テクノロジー刊
- 医療機器設計管理入門（2020 年）イーコンプライアンス刊
- 当局要求をふまえた データインテグリティ手順書作成の要点（2020 年）サイエンス＆テクノロジー刊
- 【改正 GMP 省令対応シリーズ 2】改正 GMP 省令で要求される『医薬品品質システム』と継続的改善（2021 年）サイエンス＆テクノロジー刊
- 【改正 GMP 省令対応シリーズ 3】改正 GMP 省令で要求される『CAPA(是正措置・予防措置)』導入・運用手順（2023 年）サイエンス＆テクノロジー刊
- FDA 査察対応の手引き（2025 年）イーコンプライアンス刊
- 【徹底解説】FDA 21 CFR 820 QSR から QMSR へ（2025 年）イーコンプライアンス刊
- 数式を使わない医療機器統計的手法とサンプルサイズ決定解説（2025 年）イーコンプライアンス刊
- 【徹底解説】CSV から CSA へ（2025 年）イーコンプライアンス刊
- 【徹底解説】医療機器プロセスバリデーション（2025 年）イーコンプライアンス刊
- 【徹底解説】IEC 81001-5-1 医療機器サイバーセキュリティ（2025 年）イーコンプライアンス刊

【徹底解説】
IEC 81001-5-1
医療機器サイバーセキュリティ

2025年2月15日　　第1版　第1刷発行

定価：55,000円（税込）

著　者　村山 浩一
発行人　村山 浩一
発行所　株式会社イーコンプレス
〒630-0244 奈良県生駒市東松ヶ丘1-2　奥田第一ビル102
TEL　050-3733-8134　FAX　03-6745-8626
http://eCompress.co.jp

印刷・製本　株式会社マツモト