厚生労働行政推進調査事業費補助金
医薬品・医療機器等レギュラトリーサイエンス政策研究事業

医療機関における医療機器のサイバーセキュリティ
の確保等のために必要な取組の研究

令和６年度
分担研究報告書

研究代表者　塩﨑　英司　国立大学病院長会議
分担研究者　池田　浩治　東北大学
分担研究者　宮本　裕一　埼玉医科大学
分担研究者　三宅　学　医薬品医療機器総合機構

医療機関及び製造販売業者等のそれぞれの役割や連携体制の構築

研究要旨：本研究は、医療機関内の医療機器のサイバーセキュリティ対策の体制を整えることを目的に、医療機器のサイバーセキュリティに関する医療機関及び製造販売業者等のそれぞれの役割や連携体制の構築、医療機関内における医療機器安全管理責任者と医療情報システム安全管理責任者との間の連携及び各医療機器の担当部門間の連携に係る体制の構築を含め、関係者が果たすべき役割と実施すべき事項を検討し、取りまとめ内容を示すことで、医療機関内の医療機器のサイバーセキュリティ対策の体制整備が期待される。また、医療機器全般のサイバーセキュリティ対策に関連する制度として、現在の制度において十分に対応が出来ていない分野（例えば、製造管理や品質管理で確認するべき医療機器のサイバーセキュリティ対策等）について、今後制度上の手当てを行うことを見据えて、以下の研究課題に取り組んだ。

（１） サイバーセキュリティ対策の対応状況に関する現状調査及び課題
医療機器関連の業界団体、都道府県衛生主管部等の管理するメーリングリスト等により、全国の医療機器製造販売業者、製造業者等宛てに「医療機関における医療機器のサイバーセキュリティの確保等のために必要な取組の研究に対する協力について（依頼）」（令和６年 10 月７日付け医薬機審発 1007 第２号・医薬安発 1007 第１号・医薬監麻発 1007 第３号）を送付し、一般社団法人日本画像医療システム工業会が所有する WEB システムにて回答を得るという形式でアンケート調査を実施し、医療機器製造販売業者等の 441 社から有効な回答を得た。医療機器のサイバーセキュリティ対策についての課題としては、専門家の確保、専門家以外の教育、対策費用等、リスクマネジメントの具体的方法などが挙げられた。

アンケート調査の結果から、①サイバーセキュリティ対策に関連する活動並びにサイバーセキュリティに関連するリスクマネジメント活動を実施する要員の拡充、②医療機器製造販売業者等におけるサイバーセキュリティ対策の運用の適切性に関する確認方法の検討、③医療機器製造販売業者等と医療機器の使用者である医療機関との連携、および④第三種医療機器製造販売業許可取得者に対する支援、の４点については、今後更なる検討が必要であると考えられた。

本研究にご協力を得た方々（敬称略）

一般社団法人日本医療機器産業連合会：　中里　俊章、古川　浩、吉田　容子、諸岡　直樹
一般社団法人米国医療機器・IVD 工業会：　大竹　正規
欧州ビジネス協会医療機器・IVD 委員会：　松川　智彦
医薬品医療機器等法登録認証機関協議会：　山本　義朗、鈴木　崇人
独立行政法人医薬品医療機器総合機構：　小志戸前　葉月、牧野　勤、大野　勝人、桂　崇之、池田　遼

Ａ．研究目的

サイバー攻撃により社会インフラに多大な影響をもたらす事例が多数発生しており、防護するためのサイバーセキュリティ対策（以下「CS 対策」という。）の重要性は高まっている。また、経済安全保障推進法では、基幹インフラ役務の安定的提供の確保に関する制度が、令和 6 年 5 月から運用開始しており、医療を本制度の対象とするか否かの議論が行われたところである。

医療機器の承認・認証においては、薬機法に基づく医療機器の満たすべき基準に CS 対策を取り入れる改正が行われ、令和５年度から適用されている。しかし、令和５年度に厚生労働科学研究「新たな形態の医療機器等をより安全かつ有効に使用するための市販後安全対策のあり方に関する研究」で実施した医療機関に対するアンケートによる実態調査の結果等から、医療機関納入済み医療機器等の CS 対策が万全であるとは言い難い状況であることが示唆されている。その原因は多岐に渡ると考えられるが、例えば、医療機関と医療機器製造販売業者間の連携や医療機器安全管理責任者と医療情報システム安全管理責任者間の連携が不十分であること、医療機器の種類ごとに管理部門が異なることにより部門間の連携が不十分であること、医療機器 CS 対策に関する関係者の知識不足等が挙げられる。

医療機関向けの医療機器 CS 対策に関する手引書が発出されているが、医療機関や製造販売業者、保守関係者から、その内容が不十分であることや、現場状況に適した実施事項の例示が必要であることが指摘されている。実効性のある CS 対策を実現するには、関係者が連携して取り組む必要があるが、実際には、医療機関と製造販売業者間や、同じ医療機関内にあっても医療機器安全管理責任者と医療情報システム安全管理責任者間で CS 対策について認識齟齬が生じている。関係者間での認識齟齬から生じる対策漏れが脆弱性

に繋がることから、適切なCS対策の実施についての認識共通化に向けて、対応策を至急にまとめる必要がある。

海外では胎児モニタ装置がマルウェアに感染し動作遅延等の不具合が発生した事例もあり、本邦でも医療機器へのサイバー攻撃による被害がいつ発生してもおかしくない状況であることから、喫緊な対応が求められる。

また、米国においては、2025年1月30日付けで「Cybersecurity Vulnerabilities with Certain Patient Monitors from Contec and Epsimed: FDA Safety Communication」（資料1）が公表されている。その内容は、Contec社製CMS8000患者モニタ及びEpsimed社製MN-120患者モニタについて、患者モニタのソフトウェアにバックドアが含まれており、患者モニタをインターネット回線に接続することで、個人識別情報や健康情報を含む患者データが漏出するリスクや患者モニタが接続されている他の機器や院内ネットワークが危険にさらされる可能性があることを注意喚起している。

そこで本研究では、医療機器製造販売業者、医療機器製造業者等（以下「医療機器製造販売業者等」という。）に対してCS対策の対応状況の現状調査を実施し、調査時点におけるCS対策に対する問題点及び課題の把握し、今後の対応の必要性を明確にすることを目的とする。

Ｂ．研究方法

研究班は、一般社団法人日本医療機器産業連合会、一般社団法人米国医療機器・IVD工業会、欧州ビジネス協会医療機器・IVD委員会、医薬品医療機器等法登録認証機関協議会及び医薬品医療機器総合機構の代表者からなる研究班を組織し取り組んだ。

医療機器関連の業界団体、都道府県衛生主管部等の管理するメーリングリスト等により、全国の医療機器製造販売業者等宛てに「医療機関における医療機器のサイバーセキュリティの確保等のために必要な取組の研究に対する協力について（依頼）」（令和6年10月7日付け医薬機審発1007第2号・医薬安発1007第1号・医薬監麻発1007第3号、資料2）を送付し、一般社団法人日本画像医療システム工業会が所有するWEBシステムを用いて回答を得るという方式でアンケート形式による調査を実施した。アンケート形式の設問は、資料3に示す選択式と記述式による設問とし、CS対策の対応状況の現状を把握する内容とした。

Ｃ．研究結果

全国の医療機器製造販売業者等に対し、医療機器産業連合会、各都道府県薬務主管部の管理するメーリングリスト等を用い、WEBシステムによるアンケート形式の調査を実施した。令和6年10月7日から11月15日までの期間に、WEBシステムを利用したアンケート調査を実施し、全国の医療機器製造販売業者等441社から有効な回答を得た（資料4）。

アンケートの回答者については、第一種医療機器製造販売業許可取得者が最も多く全体の52%を占めており、次いで第二種医療機器製造販売業許可取得者が24%、第三種医療機器製造販売業許可取得者が

12%、製造業登録者が 6%であった。また、製造販売業許可取得者における国内製造と外国からの輸入の割合については、国内製造が全体の 43%と最も多かった。特に第二種医療機器製造販売業許可取得者のうち、71%の会社は国内製造のみであった。また、第一種医療機器製造販売業許可取得者では、外国から輸入した医療機器のみを扱う会社が 33%であった。

CS 対策を検討しなければならない医療機器のうち、全体の 48%の製品については対応が実施できているとのことであった。社内体制に関する手順書の整備については、全体の 74%の会社で完了しており、全体の 23%の会社で準備中であることから、手順書の整備は順調に進められていると考えられた。サイバーセキュリティ情報の評価体制の整備については、全体の 56%の会社で完了しており、全体の 39%の会社で準備中であることから、評価体制の整備についても概ね順調に進められていると考えられた。

製造販売中の製品に関するソフトウェア部品表（以下「SBOM」という。）の作成状況については、全体の 90%の会社で作成完了又は準備中であり、概ね作成が進められていると考えられた。一方で、全体の 9%の会社で未着手であったことから、実務者のリソース不足に起因していることが示唆された。また、製造販売が終了した保守対象製品に関する SBOM の作成状況については、全体の 62%の会社で作成完了又は準備中であったが、全体の 39%の会社で未着手とのことで、製造販売中の製品に関する SBOM 作成に注力していることが示唆された。

セキュリティリスクに関する情報収集、分析、修正等、一連の市販後対応の仕組みについては、全体の 63%の会社で完了し、30%の会社で準備中であった。第三者から製品の脆弱性に関する報告を受けることを想定して社内体制を整備している確認したところ、全体の 67%の会社で体制整備を完了しているとのことであった。一方で使用者から広くサイバーセキュリティに関するインシデント情報を入手しているか確認したところ、全体の 43%の会社で入手していないとのことであった。

セキュリティポリシーについては、全体の 59%の会社で定めており、25%の会社で準備中、16%の会社で未着手であった。また、セキュリティポリシーの使用者への開示については、全体の 44%の会社で開示に関する仕組みを確立しており、33%の会社で準備中、24%の会社で未着手の状況であった。

脆弱性等に関する使用者への情報提供に関して、PSIRT（Product Security Incident Response Team の略で、製品やサービスに関連するセキュリティに特化した専門組織や体制のこと）等の製品セキュリティインシデント対応組織の設置については、全他の 40%の会社で設置しており、28%の会社で準備中、33%の会社で未設置の状況であった。脆弱性等に関するアドバイザリー情報の使用者への提供については、全体の 26%の会社で提供しており、30%の会社で準備中、44%の会社で未提供の状況であった。一方で、使用者から脆弱性等に対する対応状況の問合せやマルウェアによる感染確認等の依頼は、全体の 72%の会社で受けたことがなかった。

使用者のネットワーク構成図の把握については、全体の 23%の会社で使用者側から開示されない等の理由により把握したいが把握できない状況であり、53%の会社が把握していない状況であった。また、医療機器のサイバーセキュリティに関する保守契約を使用者と締結しているのは、全体の 17%の会社にとどまっており、83%の会社は保守契約を締結していなかった。

医療機器のサイバーセキュリティ対策についての課題としては、専門家の確保、専門家以外の教育、対策費用等、リスクマネジメントの具体的方法などが挙げられた。

D．考察

アンケート調査の結果から、次の 4 点の課題及び問題点が考えられた。(資料 5)

D-1. CS 対策に関連する活動及び CS 対策に関連するリスクマネジメント活動を実施する要員の拡充

医療機器の基本要件基準第 12 条第 3 項に CS 対策に関する要求事項が明確化され、令和 5 年 4 月 1 日より適用されており、サイバーセキュリティに関する必要な力量の明確化、教育訓練の実施及び力量の維持については、全体の 49%の会社で完了しており、全体の 36%の会社で準備中であるものの、未だ医療機器に関する CS 対策を実施するには不十分な面もあり、その途上にあると考えられる。

医療機器製造販売業者等においては、CS 対策を実施する要員に必要な力量の明確化、教育訓練の実施及び力量の維持を社内の品質管理監督システム（以下「QMS」という。）等に組入れ、実務者の育成と共に、CS 対策に遅れが生じないよう、CS 対策に関する業務を適正かつ円滑に遂行しうる必要十分な要員（リソース）を確保する継続的な努力が必要である。

医療機器のサイバーセキュリティ対策についての課題としては、専門家の確保（全体の 28%）、専門家以外の教育（全体の 21%）、対策費用等（全体の 19%）リスクマネジメントの具体的方法（全体の 14%）などが挙げられた。専門家の確保、教育訓練の実施等は、事業者による CS 対策の費用負担等につながることであるものの、不十分な CS 対策により生じうるビジネスリスクを考慮した場合、リスクに応じた対応を検討することが重要であると考える。

CS 対策を実施する要員に対する教育訓練については、医療機器産業界の関係団体と行政が協働で、研修会等の教育訓練の場を提供することもリソースの確保の一助となり得ると考える。

D-2. 医療機器製造販売業者等における CS 対策の運用の適切性に関する確認方法の検討

セキュリティリスクに関する情報を収集する体制は確立されつつも、自社の製品化を問わず広くサイバーセキュリティに関する脆弱性等の情報を入手できていない会社が半数以上を占めることから、能動的に情報収集できる体制にまでは至っていないこと、また、既知の脆弱性について製品への影響を評価する仕組みの整備に遅れが生じている可能性が示唆された。

医療機器製造販売業者等におけるCS対策に関連する体制及びその運用を確認する方法については、現行の「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」(以下「薬機法」という。)では明確に規定されていない。

サイバーセキュリティに関連する社内プロセスに問題がないことを確認する仕組みについては、全体の58%の会社で確立済み、29%の会社で準備中であったが、13%の会社で未着手の状況であった。

医療機器等に関するサイバーセキュリティに係る規格である JIS T 81001-5-1:2023 (IEC 81001-5-1:2021)「ヘルスソフトウェア及びヘルスITシステムの安全、有効性及びセキュリティー第5-1部:セキュリティー製品ライフサイクルにおけるアクティビティ」においても、「医療機器及び体外診断用医薬品の製造管理及び品質管理の基準に関する省令」(平成16年厚生労働省令第169号)(以下「QMS省令」という。)の元となるISO 13485 (JIS Q 13485)「医療機器ー品質マネジメントシステムー規制目的のための要求事項」の運用に組入れることを推奨している。

セキュリティポリシーの設定は進んでいるものの、セキュリティポリシーの使用者への開示に関する仕組みの確立は若干遅れ気味であり、また、製品セキュリティインシデント対応組織の設置は進められているが、使用者に対する脆弱性等に関するアドバイザリー情報の提供は遅れていることが示唆された。

医療機器製造販売業者等から使用者に対してアドバイザリー情報を含むセキュリティリスクに関連する情報が適時的確に提供され、適切な措置がとられることが重要である。

QMS省令及びISO 13485では、サイバーセキュリティに関する要求事項は規定されていない。しかしながら、JIS T 81001-5-1:2023 (IEC 81001-5-1:2021)においては、JIS Q 13485:2018 (ISO 13485:2016)の要求事項の一部として実施可能とされている。例えば、品質管理監督システム(品質マネジメントシステム)にサイバーセキュリティに関する要求事項を取込むことは可能であり、QMS省令第56条内部監査の中でCS対策の運用の適切性を確認することは有用であると考えられた。

なお、個別品目に係るCS対策の適切性、基本要件基準第12条第3項に対する適合性については、承認・認証審査の中で確認すべき事項であり、現状の対応を含め更なる検討を要すると考える。

D-3. 医療機器製造販売業者等と使用者である医療機関との連携

使用者のネットワーク構成図の把握については、全体の23%の会社で使用者側から開示されない等の理由により把握したいが把握できない状況であり、53%の会社が把握していない状況であった。

また、医療機器のサイバーセキュリティに関する保守契約を使用者と締結しているのは、全体の17%の会社にとどまっており、83%の会社は保守契約を締結していなかった。

医療機器のサイバーセキュリティ対策についての課題の一つとして、医療機関との連携・情報共有(全体の18%)が挙げられた。

医療機器の製造販売業者等と使用者（医療機関）がサイバーセキュリティに関する認識を合わせて、相互に連携、情報共有を図り取り組んでいくことが重要ではないかと考えられるため、連携のための方法を模索する必要があると考える。

D-4. 第三種医療機器製造販売業許可取得者に対する支援

第三種医療機器製造販売業許可取得者では、CS 対策に関連する社内体制に関する手順書の整備、評価体制の整備、教育訓練の実施及び力量の維持、脆弱性等に関する報告やセキュリティリスク等に関連する不具合等報告の仕組みの確立などの複数の項目において、第三種医療機器製造販売業許可取得者における対応が遅れ気味であることが示唆された。

一般医療機器（クラスⅠ）製品については、前述のとおり、サイバーセキュリティに関する要求事項を品質管理監督システム（品質マネジメントシステム）に取込み、QMS 省令第 56 条内部監査の中で CS 対策の運用の適切性を確認することは有用であると考えられた。

医療機器におけるサイバーセキュリティに関する取組みとしては、IMDRF（International Medical Device Regulators Forum:国際医療機器規制フォーラム）からもサイバーセキュリティに関するガイダンス文書が発行されている。

医療機器に関するサイバーセキュリティに関する脆弱性情報やインシデント情報を共有する戦略的な仕組みの構築も将来的には必要であると考える。一方で、総合的な情報を共有する仕組みを構築する前段階として、今回のアンケートから考えられた課題及び問題点への対応を早急に行うことが肝要であると考えられた。

Ｅ．結論

①サイバーセキュリティ対策に関連する活動並びにサイバーセキュリティに関連するリスクマネジメント活動を実施する要員の拡充、②医療機器製造販売業者等におけるサイバーセキュリティ対策の運用の適切性に関する確認方法の検討、③医療機器製造販売業者等と使用者である医療機関との連携、および④第三種医療機器製造販売業許可取得者に対する支援、の４点については、今後更なる検討が必要であると考えられた。

Ｆ．健康危害情報

なし

Ｇ．研究発表

1. 2025 年 3 月 5 日「2024 年度 医療機器の承認・認証申請等に関する説明会」（主催：一般社団法人日本医療機器産業連合会、資料 6）

Ｈ．知的財産権の出願・登録状況（予定を含む）

1. 特許出願
   なし
2. 実用新案登録
   なし
3. その他
   なし

添付資料

1. Cybersecurity Vulnerabilities with Certain Patient Monitors from Contec and Epsimed: FDA Safety Communication (2025年1月30日発行)
2. 令和6年10月7日付け医薬機審発1007第2号・医薬安発1007第1号・医薬監麻発1007第3号「医療機関における医療機器のサイバーセキュリティの確保等のために必要な取組の研究に対する協力について（依頼)」
3. 令和6年度　サイバーセキュリティ対策の対応状況アンケート(設問・選択肢)
4. 令和6年度　サイバーセキュリティ対策の対応状況に関するアンケート調査結果要約
5. 医療機器製造販売業者等に対する令和6年度アンケート結果における課題・問題点
6. サイバーセキュリティ活動報告（2025年3月5日「2024年度 医療機器の承認・認証申請等に関する説明会」(主催：一般社団法人日本医療機器産業連合会))