別紙１

研究報告書表紙

厚生労働行政推進調査事業費補助金

厚生労働科学特別研究事業

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（24CA2013）

令和６年度　総括･分担研究報告書

研究代表者　塩﨑　英司

令和7（2025）年　5月

別紙２

研究報告書目次

目　　次

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

総括研究報告書

研究代表者　塩﨑　英司　国立大学病院長会議　理事・事務局長

研究要旨：本研究は、国の重要インフラである医療分野における、医療機器のサイバーセキュリティ（以下 CS）対策の体制を整えることを目的にしている。そのうえで、医療機関及び製造販売業者の連携における課題と、医療機関内における対策と内部連携（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及び、各医療機器の担当部門間）の課題、及び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の課題について以下のとおり取り組んだ。

（1）製造販売業者等の医療機器提供側の課題
①CS 対策に関連する活動並びに CS 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 CS 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。
（2）使用者側の医療機関側の課題
①大規模病院では専門の部署や人員が確保され、医療情報システム本体については CS 対策も含めて何とか対応している現状を把握できたが、医療機器までは、対応ができていない状況であった。また、規模が小さい医療機関では、専門部署というより、属人的に対応している病院もあり、到底医療機器まで対応はできていない状況が浮き彫りとなった。②これらから病院の規模に関わらず、医療機器の CS 対策のみならず、医療情報システム本体の CS 対策に必要な人員の確保、財源の確保が課題である。③特に医療機器については、製造販売業者からの情報提供が少なく、情報提供があっても医療機関側で理解・対応ができない状況にあることの 3 点がわかった。
（3）医療機関及び製造販売業者の連携における課題
①製造販売業者等からの医療機関に対する情報提供については、提供後の活用も視野に入れた提供方法がとられていない事、②製造販売業者等にも医療機関側の担当窓

口が周知されておらず、ネットワークに関する情報が乏しい事③医療機関側も医療機器に関する内部の役割分担が不明確である。④ネットワークに関しても手作業による更新の負荷が高く、適切に関係者への情報提供ができていない事の 4 点が明らかとなった。

（4）実務的に活用可能な CS 対策の具体的実現の課題

人員確保と財源確保が厳しい中、自助だけでなく医療機関と製造販売業者双方における共助と、公的な医療機関と製造販売業者の連携体制の主導と支援体制と周知活動も含めた公助の体制整備が必要であることが確認された。自施設での努力だけでなく、規模別の医療機関と製造販売業者の連携モデルを検証し、ネットワーク管理業務の負荷を軽減する自動化ツールの導入可能性とその支援体制及び周知活動も含めた公助の体制整備が必要である。

分担研究者　池田　浩治　東北大学　特任教授
分担研究者　宮本　裕一　埼玉医科大学　教授
分担研究者　三宅　学　医薬品医療機器総合機構　医療機器調査部_課長
分担研究者　中野　壮陸　公益財団法人 医療機器センター 専務理事
分担研究者　新 秀直 東京大学医学部附属病院 企画情報運営部 講師

本研究にご協力を得た方々（敬称略）
公益社団法人日本医師会　：　長島　公之
公益社団法人全日本病院協会　：　甲賀　啓介
東京大学医学部附属病院　：　井田　有亮
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
松元　恒一郎、梶山　孝治、野々下　幸治
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

医療分野は国民の命を支える国の重要インフラであり、そこで発生するサイバーセキュリティの問題は、経営層の理解だけでなく医療機器のサプライチェーン全体も国民の命に係わる事を認識して対策に取り組まなければならない。この事を前提にして、本研究は、医療機関の医療機器のサイバーセキュリティ（以下 CS）対策の体制を整えることを目的にしている。そのうえで、今回は医療機関及び製造販売業者の連携における課題と、医療機

関内における対策と内部連携（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及び、各医療機器の担当部門間）の課題、及び製造管理や品質管理で確認するべき医療機器のCS対策等の課題について検討した。また既に発出されている医療機器のCS対策に関するガイダンスと手引書を踏まえたうえで、実務的に活用可能なCS対策の具体的実現の課題を抽出することも目的とした。

Ｂ．研究方法

研究班を医療機器提供側である①製造販売業者からアプローチするグループと使用者である②医療機関側からアプローチするグループに分け、2方向から研究を進めた。

製造販売業者からのアプローチでは、大学関係者と医薬品医療機器総合機構の研究者と、研究協力者として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、独立行政法人医薬品医療機器総合機構の関係者による協議に基づき、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から、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CS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）」のアンケートを実施した。アンケート結果についてはグループの検討会で分析した。次に医療機関側からアプローチでは、関係者へのヒアリングとして、日本医師会に医師会のCS対策に関する体制の把握と医療者への周知方法、日本臨床工学技士教育施設協議会には人材育成の観点から、臨床工学技士養成課程におけるCS対策の教育状況の確認と今後の見通しについて把握、その後に大学病院からCS対策に関する先進的な取組みを把握、以上ヒアリングを参考に、調査票を作成して、研究協力団体（四病協：日本医療法人協会、日本精神科病院協会、日本病院会、全日本病院協会）から推薦された9医療機関と、国立大学法人病院、1県立病院に対して課題を把握した。また、 厚生労働科学研究の「安全な地域医療の継続性確保に資する医療機関における情報セキュリティ人材の育成と配置に関する研究」の研究班との意見交換を行った。以上のヒアリングと実地調査から研究協力団体と国立大学病院に対してアンケート調査を行い、その結果をグループで討議して分析を進めた。

Ｃ．研究結果

（1）製造販売業者からアプローチしたグループは、全国の医療機器製造販売業者等441社からWEBシステムを利用したアンケート調査で有効な回答を得た。その結果を分析し、次の4点の課題及び問題点が考えられた。

①CS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の必要性については、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日より適用されている。しかし、アンケート結果からは、CS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た。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。

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については、CS 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 CS 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たことから、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。また、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。今後、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、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。

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については、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 CS 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。今後は医療機器の製造販売業者等と使用者（医療機関）が CS 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ことから、連携のための方法を模索する必要があると考える。

④第三種医療機器製造販売業許可取得者に対する支援については、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 CS 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。以上の４点について課題が明らかとなり、課題ごとに具体策を検討する事が必要である。

（2）医療機関側からアプローチするグループは、①医療機関の現状については、1）製造販売業者からの情報提供体制については、情報システム系については、情報提供が徐々になされている傾向にあるが、医療機器関係については、問いかけても情報提供がないことが多い。特に地方で

は医療機器メーカが対応できていない現状があることが考えられた。2）医療機関における医療機器のサイバーセキュリティ確保のための手引書の周知については、初めて知った医療機関も多く、周知が重要であると考えられた。ただし、読み込んでも医療機関では分からないことが多く、医師会などで行っているような動画での解説や見た目でわかりやすい図などを挿入するなど、受け取った医療機関側が活用できるようにする工夫が重要であると考えられた。3）サイバーセキュリティ対応のレベル差については、医療機器に限らず情報システム全体のセキュリティ担当者の中でもCS対策のレベル感が違うことが分かった。実際に対応している担当者にばらつきがある現状が浮き彫りとなった。さらには、医療機関全体のサイバーセキュリティ対策についての進捗の立ち位置が見えず、特に医療機器に関しては担当者が何をすればよいのか把握できている状況にはなかった。このことから、何をどこまでやれば良いか医療機関側で把握ができ、他院との相対化ができるような情報システム全体の内容と医療機器を整合させた形での医療機関向けのチェックリストが必要であるとともに、それを相対評価する仕組みが必要であることが示唆された。4）CS対応担当者の状況については、情報システムの担当者だけでは医療機器まで手が回らず、実務的に対応できる余裕がない状況にあった。この状況を解決するためには、CS対策を少しでもできるような既存の医療職種の裾野を広げるべく、診療情報管理士、臨床工学技士、診療放射線技師などについては、学生のころからセキュリティを学ぶ機会を作る必要があると考えられた。5）信頼境界（責任分解点に近い概念）を明示した契約書のひな型については、医療機器等のリモートメンテナンスや脆弱性、レガシー機器への対応について、信頼境界が明確にできるような契約書のひな形的なものを、専門家を交えて医療機関の機能に応じて複数のパターン作成し公開することが有益であると考えられた。6）院内のシステム担当者と医療機器担当者の連携については、情報システムについて、責任を持つ体制が構築されつつあるが、医療機器等については、各部門での対応に委ねているところが多かった。医療機関内でのCSに関する情報共有等を進めるためには、少なくとも、情報システム関連の規程の中に、CS対策が必要な医療機器等を所有する各部門から、医療機器等の担当者を任命し、責任体制を明確にする必要があることが考えられた。また、医療機関の規模によっては、各医療機関で対応するには限界があるため、地域で支援できるような体制も行政や第三者機関が中心となって対応できるような仕組みも必要であると考えられた。7）医療機器メーカと病院担当者との連携については、連携ができている医療機関はほとんどなかった。医療機器メーカと病院担当者との連携体制の構築が今後、医療機器のCS対策を進める上での課題であると考えられた。8）ネットワーク構成図の要件については、情報システムの管理部門でネットワーク構成図を把握しているものの、医療機器等のリモートメンテナンス回線が把握できていなく、細かい医療機器の接続につ

いては、一元的に管理できていない医療機関が多いことがわかった。ネットワーク回線の把握や更新するのは医療機関内での役割分担を明確にすることも必要あると考えられた。9）SBOM と MDS2/MDS の収集と具体的活用方法については、医療情報システムに関しては、MDS について令和 6 年度版医療機関における CS 対策チェックリスト（医療機関確認用）にも記載され、事業者から製造業者/サービス事業者による医療情報セキュリティ開示書（MDS/SDS）を提出してもらっている医療機関が多くあったが、医療機器特有の CS に関する情報である、SBOM と MDS2 については情報を集めている医療機関はごくわずかであった。集めようとしても、医療機器メーカが検討中として、提出されないことも多く、医療機関側では、入手しても活用方法もわからない現状にあることが分かった。SBOM や MDS2/MDS の医療機関への周知や活用方法の検討が必要であり、さらには第三者的に医療機器メーカから SBOM や MDS2/MDS を自動的に収集し、システマティックにその脆弱性や対策を医療機関に周知できるような仕組みの検討も必要であると考えられた。10）院内接続機器調査に係るアプリケーションについては、機器等を一元的に管理することが必要であると考えられる。医療情報システムの情報部門では、ネットワークに接続されている医療機器等まで管理ができるような体制とはなっていない。また、エクセルで台帳を作成するような形で、手作業で管理することは各医療機関の大きな負担となる。医療機関内のネットワーク機器等の見える化を目的として、自動化された情報を収集する取組みが今後必要となると考えられる。

②人員の確保については、病院の規模に関わらず、医療機器の CS 対策だけでなく、医療情報システム本体の CS 対策に必要な人員の確保が課題である。日本臨床工学技士教育施設協議会へのヒアリングからも臨床工学技士の養成課程では、医療情報学に関する講義や実習は行われているが、CS 単体の講義や実習などはほとんどないとのことがわかり、意見交換の結果、教科書の刷新に向けて検討中である事が分かった。臨床工学技士が医療機関内での医療機器等も含めた CS 対策の即実務者となることは難しいながらも、橋渡し的な役割を担うために、既存の医療職種である、診療情報管理士、臨床工学技士、診療放射線技師などについて卒前、卒後教育の一体的な CS 対策教育を呼びかける事も重要である。この他、医療情報システム本体の CS 対策として人材育成については、別の厚労科研において、大阪大学を中心に情報セキュリティ人材の育成と配置について研究が進められており、他の研究班とも連携して検討を進める事が重要である。

（3）医療機関及び製造販売業者の連携における課題においては、製造販売業者からアプローチと医療機関側からアプローチも共に同じ課題を抱えており、①医療機器の製造販売業者等と使用者（医療機関）が CS 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ことから、連携のための方法を模索する必要がある。また、信頼境界が明確にできる

ような契約書のひな形を、専門家を交えて医療機関の機能に応じて複数のパターン作成し公開することが有益である。

②製造販売業者と医療機関側の担当窓口を双方に周知する仕組みが必要であり、そのためには製造販売業者も担当窓口を明確にすることと、医療機関側も医療機器の担当部門とシステム全体の責任者の役割分担を行った窓口設置する事が必要である。また医療機関側にあっては、ネットワークに関する情報が乏しい機関も多くあるため、第三者へ管理委託している場合があり、その窓口も明確にして、各機関が連携できる体制整備を急ぐ必要がある。

③以上のとおり人材確保は容易でないものの連絡窓口を設置するため、医療機関側も医療機器CS対策に関する内部の役割分担を定め明確にする必要がある。

④ネットワークに関する管理については、手作業による更新の負荷が高いため、管理情報を自動的にアップデートする安価なソフトウェアの導入が必要である。

(4) 実務的に活用可能な CS 対策の具体的実現の課題については、人員確保と財源確保が厳しい中ではあるが、まずは製造販売業者のCS対策の推進状況を各社が確認し改善できる仕組み作りの検討を開始するべきである。また、同様に医療機関も自機関のCS対策を他機関に比較して進捗を認識できる評価方法の検討と、特に対策を急ぐ医療機器の特定が可能となる仕組みづくりの検討を開始しなければならない。このような自施設での努力だけでなく、医療機関と製造販売業者双方における連携推進としての共助と、医療機関相互の協力体制の共助の可能性の検討が開始されるべきである。その際には規模別の医療機関と製造販売業者の連携モデルを検証し、ネットワーク管理業務の負荷を軽減する自動化ツールの導入可能性とその支援体制及び周知活動も含めた公助の体制整備が必要である。

Ｄ．考察

D-1 製造販売業者からアプローチによる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。

D-1-1. 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

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。

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-1-2. 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

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。

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-1-3. 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

半数以上の医療機器製造販売業者は使用者のネットワーク構成図を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。

この結果から、医療機関との連携・情報共有が不十分であり、早急に連携のための方法を模索する必要があると考える。

D-1-4. 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、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。

D-2 医療機関側からアプローチによる調査の結果から、次の3点の課題及び問題点が考えられた。

D-2-1 医療機関の現状について

CS対策として先進的な取組みを行っている大学病院でも、医療機器に関しては十分に対応できているとは言えず、人材不足である実情が把握できた。また、多彩な病院でのヒアリング結果もふまえ以下のような課題があると考えられた。

・製造販売業者からの情報提供体制については、医療機器関係については、問いかけても情報提供がないことが多く、地方

では医療機器メーカが対応できていない現状があることが考えられた。

・医療機関における医療機器のサイバーセキュリティ確保のための手引書の周知については、今回の調査で初めて知った医療機関も多く、周知が重要であると考えられた。医師会などで行っているような動画での解説や見た目でわかりやすい図などを挿入するなど、医療機関側が活用できるようにする工夫が重要であると考えられた。

・サイバーセキュリティ対応のレベル差については、実際に対応している担当者にばらつきがある現状が浮き彫りとなった。医療機関全体のサイバーセキュリティ対策についての進捗の立ち位置が見えないため、他院との相対化ができるような情報システム全体の内容と医療機器を整合させた形での医療機関向けのチェックリストが必要であり、それを相対評価する仕組みが必要であることが示唆された。

・CS 対応担当者の状況については、医療機器まで手が回らず、実務的に対応できる余裕がない状況にあった。この状況を解決するために、CS 対策を少しでもできるような既存の医療職種の裾野を広げるべく、診療情報管理士、臨床工学技士、診療放射線技師などについては、学生のころからセキュリティを学ぶ機会を作る必要があると考えられた。

・信頼境界（責任分解点に近い概念）を明示した契約書のひな型を、専門家を交えて医療機関の機能に応じて複数のパターン作成し公開することが有益であると考えられた。

・院内のシステム担当者と医療機器担当者の連携については、医療機器等については、各部門での対応に委ねているところが多かった。少なくとも、情報システム関連の規程の中に、CS 対策が必要な医療機器等を所有する各部門から、医療機器等の担当者を任命し、責任体制を明確にする必要があることが考えられた。また、医療機関の規模によっては各医療機関で対応するには限界があるため、地域で支援できるような体制も行政や第三者機関が中心となって対応できるような仕組みも必要であると考えられた。

・医療機器メーカと病院担当者との連携については、連携ができている医療機関はほとんどなかった。

医療機器の CS 対策に関する情報は医療機関側にはほとんど伝わらない状況であったことから、医療機器メーカと病院担当者との連携体制の構築が今後、対策を進める上での課題であると考えられた。

・ネットワーク構成図の要件については、情報システムの管理部門でネットワーク構成図を把握しているものの、医療機器等のリモートメンテナンス回線と細かい医療機器の接続については、一元的に管理できていない医療機関が多いことがわかった。医療機器やそれに不随するネットワーク回線の把握や更新は医療機関内での役割分担を明確にすることも必要あると考えられた。

・SBOM と MDS2/MDS の収集と具体的活用方法については、医療機器特有の CS に関する情報である、SBOM と MDS2 については情報を集めている医療機関はごくわずかであった。集めようとしても、医療機器メー

カが検討中として、提出されないことも多く、医療機関側では、入手しても活用方法もわからない現状にあることが分かった。第三者的に医療機器メーカからSBOMやMDS2/MDSを自動的に収集し、システマティックにその脆弱性や対策を医療機関に周知できるような仕組みの検討も必要であると考えられた。

・院内接続機器調査に係るアプリケーションの試行については、医療機関内ネットワークに接続されている機器等を一元的に管理することが必要であると考えられる。医療機器等まで管理ができるような体制とはなっていない。また、エクセルで台帳を作成するような形で、手作業で管理することは各医療機関の大きな負担となる。情報システム担当者が把握している医療機器と実際に接続されている医療機器の数にどのくらい乖離があるか実情を調査することも今後検討が必要であると考えられた。人の手によらない自動的に医療機器等のCS対策の基礎となる情報を収集する取組みが今後重要となると考えられる。

今回のフィールドワークによる調査・ヒアリングで得た10点の前述のような知見も取り入れて、医療機器のCS対策の現状の課題を整理するためにアンケート調査を行った結果、以下のような課題が浮き彫りとなった。

D-2-2 アンケート結果からの考察

共助・公助の体制づくりについては、医療機関におけるCS対策では専門家不在の中で、自助での対応には限界があるため、共助、公助の仕組みが重要となる。医師会では、共助の仕組みとして、相談窓口を設置し、分かりやすく周知するような先進的な取組みがされていた。全国の医療機関が利用できる仕組みを検討するとともに、医療機関内でCS対策を担う人材への教育支援体制の充実なども重要となると考えられた。このような仕組みは、行政機関などの公的な支援を受けて、医療機器のCS対策に必要なチェックリストやガイドラインの作成なども含めて、公助として取り組む方向性についても検討すべき課題であると考えられた。

D-2-3 人材教育、配置について

医療機関へのヒアリングやアンケート調査の結果からも分かるとおり、医療機関内でCS対策ができる人材の不足が大きな課題であることが分かった。多くの医療機関では体制を取ることもできない。CS対策を担うような人材は他分野でも取り合いの状況であることから、給料等の見合いが合わず、医療機関で雇用できることはかなり稀なケースであると考えられる。医療機関の役割に応じたCS対策レベルの設定とそれを担う人材の育成が重要であると考えられた。裾野を広げるためには、医療従事者でもある程度の知識を持てるように卒前・卒後の教育が重要であり、診療情報管理士や医療情報技師、臨床工学技士、診療放射線技師が現在の医療資格等（学会認定等も含む）の職種を育成する教育課程へのアプローチも今後必要であることが示唆された。

D-2-4 今後の課題について

様々な団体や医療機関へのヒアリングやアンケート調査などを通じて、医療機器等の CS 対策に必要な①人材、②予算の確保③具体な方策と手順、④ネットワーク資産の可視化の仕組み、⑤医療機関内での連携体制の構築、⑥医療機関と医療機器製造販売業者との連携体制の構築、⑦各医療機関における医療機器にかかる CS 対策を評価できる仕組みが重要であると考えられた。

今後、これらの課題を解決すべく、行政、医療機器製造販売業者、医療機関が三位一体となり、協働で我が国の医療機器の CS 対策を一歩でも進めるべく検討を重ねることが重要である

Ｅ．結論

製造販売業者としては、①CS 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、②CS 対策の運用の適切性に関する確認方法の検討、③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。

また、医療機関側としては医療機器の CS 対策が実際の対応まで落とし込めている状況ではないことが浮き彫りとなった。今後、人材や予算、手段なども含めて、取り組める内容を検討し分かりやすく示すとともに、自動化できる仕組みの検討も必要であると考えられた。

Ｆ．健康危険情報

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）

2．論文発表

新秀直、黒澤壮平、中里俊章、中野壮陸、松元恒一郎、特集 医療機器のサイバーセキュリティ確保に向けた動向と製造販売業者、医療機関に求められること、医療機器学 第 94 巻 第 4 号 425-463.（2024）

3．学会発表

塩﨑英司、新秀直、中里俊章、沼館慧剛、医療機器に関するサイバーセキュリティ管理について， 第 44 回 医療情報学連合大会（2024）

Ｈ．知的財産権の出願・登録状況

１．特許取得

なし

２．実用新案登録

なし

３．その他

なし

添付資料

分担研究報告書に添付

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))

令和６年度厚生労働行政推進調査事業費補助金（厚生労働科学特別研究事業）
分担研究報告書

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

研究分担者
塩﨑　英司　一般社団法人　国立大学病院長会議　事務局　理事・事務局長
中野　壮陸　公益財団法人　医療機器センター　専務理事
新　　秀直　東京大学医学部附属病院　企画情報運営部　講師

医療機関における医療機器のサイバーセキュリティ確保に関する実態調査と課題の抽出

研究要旨
　これまで発出されている医療機器のCS対策に関するガイダンスや手引書を踏まえた総合的かつ実務上活用できるCS対策を検討すべく、各種団体の取組みや医療機関での医療機器のCS対策の具体的な対応や課題を抽出することを目的とした。
　日本医師会や日本臨床工学技士教育施設協議会、先進的な取組みを行っているA大学病院のヒアリング内容を基に調査票を作成し、研究協力団体（四病協：日本医療法人協会、日本精神科病院協会、日本病院会、全日本病院協会）から推薦された9医療機関に加え、2国立大学法人病院、1県立病院に対して多彩な病院での課題を把握することを目的としたヒアリングを行った。また、厚生労働科学研究費補助金 研究班へ医療機関での人材育成の方向性と配置に関する状況を把握することを目的とてヒアリングを行った。以上のヒアリング結果を基に、アンケート調査内容を作成し、2025年2月17日～3月17日を期間とした、医療機関における医療機器のサイバーセキュリティ確保に関する実態を把握するためのアンケート調査を行った。
　ヒアリングやアンケート結果から大規模病院では専門の部署や人員が確保され、医療情報システム本体についてはCS対策も含めて何とか対応している現状を把握できたが、医療機器までは、対応ができていない状況も確認できた。規模が小さい医療機関では、専門部署というより、属人的に対応している場合もあり、到底医療機器まで対応はできていない状況が浮き彫りとなった。病院の規模に関わらず、医療機器のCS対策のみならず、医療情報システム本体のCS対策に必要な人員の確保、財源の確保が課題であり、特に医療機器については、製造販売業者からの情報提供が少なく、情報提供があっても医療機関側で理解・対応ができない状況にあることがわかった。しかし、少ないながらの人員でも、患者を守るためにCS対策についても献身的にCS対策を進めている状況が確認できた。
　医療機器のCS対策については、行政と製造販売業者を中心に取り組んできたものの、実際の医療機関での対応まで落とし込めている状況ではないことが浮き彫りとなった。今後、人材や予算、手段なども含めて、医療機関で具体に取り組める内容を検討し分かりやすく示すとともに、自動化できるところは自動化する仕組みの検討も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）
公益社団法人日本医師会：　長島　公之
公益社団法人全日本病院協会：　甲賀　啓介
東京大学医学部附属病院：　井田 有亮
一般社団法人日本医療機器産業連合会：　中里　俊章、松元　恒一郎、梶山　孝治、野々下　幸治

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）の重要性は高まっている。2014年5月に公表された「重要インフラの情報セキュリティ対策に係る第３次行動計画」（情報セキュリティ政策会議）では、重要インフラ分野として、金融や航空、電力などとともに、医療機関も重要インフラ事業者とされている。その重要システム例として、電子カルテシステムは当然のこと、遠隔画像診断システム等とともに、医療機器（医用電気機器）等も挙げられている。
　医療機関は重要インフラの一つとして位置づけられCS対策が少しずつ進んではいるものの、ネットワークに接続される医療機器のCS対策については、盲点になりやすい。しかし、医療機器が直接サイバー攻撃を受けた場合には、患者にも影響を与える可能性もあるため、医療機器の特性を考慮したCS対策が重要となる。
　医療機器におけるサイバーセキュリティ確保については、2015年に初めて厚生労働省から医療機器製造販売業者（以下製販業者）向けに通知が発出されて以降、急速に行政と製販業者を中心に、その対策が進められてきた。この通知の中で、製販業者はサイバーセキュリティの確保がなされていない医療機器については、使用者に対してその旨を明示し、ネットワークに接続しない、できないように注意喚起することや、医療機関に対し、必要な情報提供を行うとともに、連携を図ることが明記されているものの、具体的な内容については、乏しく現実的には特に対応することなく経過してきたものと考えられる。
　一方で、国際的には、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が公表され、我が国でもCS対策の国際的な調和を図る目的で、医療機器のサイバー攻撃に対する国際的な

耐性基準等の技術要件を導入して整備するために、2024年3月9日に医薬品医療機器等法も改正された。また、医療機関側の対応については、2023年3月31日付けで初めて医療機関における医療機器のサイバーセキュリティ確保のための手引書が発出され、医療機器のCS対策の更なる確保に向けた具体的な医療機関での体制確保について示されている。

情報システム全体については、2022年の診療報酬改定で、診療録管理体制加算の施設基準として、400床以上の保険医療機関には、厚生労働省の「医療情報システムの安全管理に関するガイドライン」に基づき、専任の医療情報システム安全管理責任者の配置が求められ、職員を対象として必要な情報セキュリティに関する研修の定期的な開催も義務付けられている。さらに、2023年4月1日からは、医療法施行規則第14条第2項を新設し、病院、診療所又は助産所の管理者が遵守すべき事項として、サイバーセキュリティの確保について、必要な措置を講じることが追加されている。このことから、CS対策は医療機関の管理者が遵守するべき事項として位置づけられ、法的にも対応が迫られている状況にある。しかし、必要な措置として求められている「医療情報システムの安全管理に関するガイドライン」の対象としては医療に関する患者情報（個人識別情報）を扱う医療情報システムが対象とされていることから、患者情報を扱わないがネットワークに接続して使用する医療機器等については、ガイドラインの範疇から外れてしまうことになる。

このような背景もあり、前述の医療機器に関する手引きが作成・公表されている状況にあるが、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や新規に導入される医療機器等の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。

その原因として、医療機関と製販業者間の連携や医療機関内での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や人材不足、具体的な医療機関での対策内容が不明確であること等が挙げられる。

さらに、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、医療機関や製販業者、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、医療機関と製販業者間や、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。

そこで本研究では、これまで発出されているガイダンスや手引書を踏まえた総合的かつ実務上活用できるCS対策を検討すべく、各種団体の取組みや医療機関での医療機器のCS対策の具体的な対応や課題を抽出することを目的とした。

Ｂ．研究方法

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を参照し、現状の課題を把握した上で、日本の医療サイバーセキュリティの課題点について行うべき対応の精度を上げるために各種団体へヒアリングを行った。具体的なヒアリング先と目的は以下の通りである。

1) 日本医師会：医師会のCS対策に関する体制の把握と医療者への周知方法に関する先進的な取組みを把握することを目的とした。
2) 日本臨床工学技士教育施設協議会：人材育成の観点から、臨床工学技士養成課程におけるCS対策の教育状況の確認と今後の見通しについて把握することを目的とした。
3) A大学病院：CS対策に関する先進的な取組みを把握するとともに、医療機器のCS対策として必要な事項について把握することを目的とした。
4) 1）～3）のヒアリング内容を基に調査票を作成し、研究協力団体（四病協：日本医療法人協会、日本精神科病院協会、日本病院会、全日本病院協会）から推薦された9医療機関に加え、1国立大学法人病院、1県立病院に対して多彩な病院での課題を把握することを目的としたヒアリングを行った。
5) 厚生労働科学研究費補助金 健康安全確保総合研究分野 地域医療基盤開発推進研究 安全な地域医療の継続性確保に資する医療機関における情報セキュリティ人材の育成と配置に関する研究　研究班：医療機関での人材育成の方向性と配置に関する状況を把握することを目的とした。
6) これらのヒアリング結果を基に、アンケート調査内容を作成し、一般社団法人日本医療法人協会 1002医療機関、公益社団法人日本精神科病院協会 1205医療機関、一般社団法人日本病院会 2555医療機関、公益社団法人全日本病院協会 約2500医療機関（以上、四病協関連医療機関）、国立大学病院42医療機関、計約7300医療機関（※一部重複医療機関を含む）に協力を依頼した。四病協関係の医療機関：2025年2月17日～3月10日、国立大学病院：2025年3月8日～3月17日を期間とした、医療機関における医療機器のサイバーセキュリティ確保に関する実態を把握するためのアンケート調査を行った。
7) さらに、医療機器等のIoMT（Internet of Medical Things）可視化システム導入医療機関および大規模移転を経験した医療機関へのヒアリングを行い、医療機器等の可視化状況の把握と移転時のシステム対応について状況を確認した。

（倫理面への配慮）

本分担研究は患者を対象としたり個人が特定できる患者情報を使用したりするものではないが、関連ガイドラインや個人情報保護法の遵守と倫理

面に配慮すべき点はないかに注意した。

Ｃ．研究結果

1）日本医師会へのヒアリング(別紙1)

日本医師会では、サイバーセキュリティ支援制度を立ち上げ、有事から平時まで幅広く会員からの相談を受ける窓口や分かりやすい動画の提供など広くCS対策を相談・周知する体制を整備し、運用が行われていた。一方で、医療機器に特化する形でのサイバーセキュリティに関する相談内容はまだ届いていなかった。

2）日本臨床工学技士教育施設協議会へのヒアリング（別紙2）

臨床工学技士の養成課程では、医療情報学に関する講義や実習は行われているものの、サイバーセキュリティ単体の講義や実習などはほとんどないとのことであった。教科書には、セキュリティ関係の内容が入っているものの、個人情報保護等が中心であり、ボリュームとしては少ないことから、教科書の刷新に向けて検討中の状況にあった。臨床工学技士が医療機関内での医療機器等も含めたCS対策の即実務者となることは難しいながらも、橋渡し的な役割を担うために卒前、卒後教育の一体的な検討も重要であるとの意見があった。

3）A大学病院へのヒアリング（別紙3）

医療情報システムやCS対策について、先進的な取組みを進めているA大学病院では、ネットワークに接続する医療機器の接続方法を確認し、脆弱性を指摘しても、製造販売業者では何も改善されないという実情を把握することができた。また、医療機器のセキュリティ情報の開示や活用方法が十分されていない現状にも課題があるとの意見があった。CS対策は継続的なリスク管理の一環であり、第三者機関によるセキュリティ評価やペンテストの実施などについても示唆いただいた。さらには、医療機器の脆弱性と法規制の課題や具体的なセキュリティ対策の手順についても有用な意見をいただくことができた。医療機器のCS対策は、医療機関、行政、医療機器の製造販売業者等が協力して、単なる技術的対策だけではなく、制度設計や人材育成を含めた総合的な対応が不可欠であるとの意見があった。

4）11医療機関へのヒアリング（別紙4、別紙5）

1）～3）のヒアリング結果を基に、別紙4に示す調査票を作成し、研究協力団体が推薦する医療機関を中心に、11医療機関へヒアリングを行った。詳細の結果については11医療機関を特定できるような情報を削除したうえで、別紙5としてまとめた。大規模病院では専門の部署や人員が確保され、医療情報システム本体についてはCS対策も含めて何とか対応している現状を把握できたが、医療機器までは、対応ができていない状況も確認できた。規模が小さい医療機関では、専門部署というより、属人的に対応している場合もあり、到底医療機器まで対応はできていない状況が浮き彫りとなった。病院の規模に関わらず、医療機器のCS対策のみならず、医療情報システム本体のCS対策に必要な人員の確保、財源の確保が課題であり、特に医療機器については、製造販売業者からの情報提供が少なく、情報提供があっても医療機関側で理解・対応ができない状況にあることがわかった。しかし、少ないながらの人員でも、患者を守るためにCS対策についても献身的にCS対策を進めている状況が確認できた。

5）厚生労働科学研究費補助金　研究班へのヒアリング（別紙6）

医療機器のみならず、医療情報システム本体のCS対策として人材育成とその配置が共通した課題であり、別の厚労科研では、大阪大学を中心に情報セキュリティ人材の育成と配置について研究が進められていた。議論の中では、指導的な立場の医療機関にはグループA人材＋グループC人材、自施設の情報システムを守ることができる医療機関（400床以上をイメージ、地域医療に大きな影響を生じる医療機関）にはグループB人材＋グループC人材、他施設や企業の助けを借りて情報システムを守る医療機関にはグループC人材を配置するようなイメージで議論していた。医療安全や感染症対策のように、指導病院が地域の病院と連携して守るようなイメージであり、指導病院間での相互チェックや地域の病院へのセミナーや訓練を行うことなども想定されていた。また、各医療機関で、情報部門だけでなく、各部門システムや医療機器のCS確保のために各部門にグループC人材を配置し、面で守っていくようなイメージで検討が進んでいた。診療放射線技師や臨床工学技士などの医療職種がグループC人材を担うための具体策についても議論され、医療機関内でのCS対策を担う人材育成についても検討が進められていた。

6）医療機関へのアンケート調査（別紙7）

様々なヒアリング結果を基に別紙7に示すアンケート調査内容（基本情報、医療情報システム全般について、医療機器のCS確保について、その他）を作成し、アンケート調査を実施した。四病協関連病院では、1118アクセス、523回答（回答完了：172回答、部分的な回答：351回答）があった。国立大学病院等からは、715アクセス、109回答（回答完了：40回答、部分的な回答：69回答）があった。部分的な回答も含めて、データ内容を確認し、重複データを除外した上で、四病協関連医療機関 170回答、国立大学病院等 40回答を回答が完了していると判断し、計210回答を有効回答とした。データについては四病協関連医療機関と国立大学病院等でわけて基礎集計行うとともに、クロス集計（病院種別、病床規模、自己評価の大小等）を行い、統計解析を行った。さらに、自由記載内容についても要約し分類した。なお、一部のデータ分析支援業務は、ナレッジデータサービス株式会社に委託した。統計解析については、有意水準5%として、統計解析（$\chi 2$検定、残差分

析）を行った。なお、残差分析のp値については、多重比較を考慮しBonferroniの補正を加えたp値を算出した。四病協関連では、一般病院71%、精神科病院29%であり、病床規模としても101-200床の医療機関が42%を占めた。一方で国立大学病院等では、600床以上の病床が多かった。情報システムの管理体制については、四病協関連では、85%以上が専門の担当部門または専任者を有し、責任者も90%以上の医療機関で確保されていた。国立大学病院等では全ての医療機関で、専門の担当部門を有し、責任者が配置されていた。責任者の職種としては、四病協関連では、事務が最も多く（45%）に対して、国立大学病院等では医師・教員が担当することが90%以上を占めた。担当人数としては、四病協関連では、0人が4%、1～2人が55%であったのに対し、国立大学病院等では、10名以上が50%以上を占めていた。しかし、CS対策を担う人員は、四病協では、0名（20%）、1～2名（61%）であり、その中でも医療機器CS対策を担う人員は、0名（54%）1～2名（36%）であった。国立大学病院等でも、CS対策を担う人員は0名（15%）、1～2名（22%）であり、医療機器CS対策については、0名（60%）、1～2名（19%）であった。国立大学病院等では、CS対応者の資格について専門的な
資格（情報処理安全確保支援士、医療情報技師等）を持っている割合が52%を占めた。

ネットワーク構成図について、四病協関連では、29%は資料として持っていない状況にあったが、作成している場合には、何かのタイミングで更新している割合が高かった（90%）。国立大学病院等では、ほとんどの医療機関で作成されていた。四病協、国立大学病院等ともに、70%以上で業者が作成していた。また、リモートメンテナンス回線については、四病協関連では、80%以上、国立大学病院等でもほとんど把握がされていた。

セキュリティ対策の財源については、四病協では79.4%、国立大学病院等では85%が診療報酬での担保を望んでいた。

CS対策が必要な医療機器が存在することについては、四病協関連では、74%があまり知らない状況にあり、国立大学病院等でも45%が同様の状況にあることがわかった。

医療機器に接続される医療機器について、四病協関連病院では、情報システム部門で把握しているのは65%にとどまり、把握していても、医療機器のOSやMACアドレス、通信プロトコルなど詳細までは把握できていない状況にあった。

医療機器が更新/追加された場合に把握しているのは四病協関連では、55%に留まり、ネットワーク構成図については、医療機器の情報まで反映されているのは、23%であった。一方で、国立大学病院等でも、ネットワーク構成図に医療機器の情報まで反映できているのは9%と多くの医療機器を抱える国立大学病院等では対応できていない状況が明らかとなった。

医療機器のOSのバージョンアップやウィルス対策については四病協関連の67%で確認しておらず、国立大学病院等でも、70%で確認していなかった。医療機器に関する脆弱性情報についても、四病協関連で14%、国立大学病院等でも20%しか入手していない実情であった。

医療機器のサイバーセキュリティ確保について参照しているガイドライン等は、四病協関連では、参考資料はないとしたのが47.6%であり、国立大学病院等でも43%がないと回答している。医療機器特有の情報として、MDS2、SBOM、レガシー状態について、情報を入手しているかの質問に対して、四病協関連では、44%、国立大学病院等でも55%が情報の存在を知らないと回答し、医療機器販売業者等から提供されて入手しているのはそれぞれ、21%、13%であった。医療機器メーカからの情報提供についても、業者主導で提供されていると回答したのは、四病協関連12%、国立大学病院等5%であり、提供されたことはないと回答したのは、それぞれ、47%、55%であった。

医療機器のサイバーセキュリティ確保に向けた、院内での連携体制については、四病協関連で構築していると回答したのは、16%、国立大学病院等でも23%であった。構築ができないとの回答はそれぞれ40%程度であった。

医療機器のサイバーセキュリティ確保に関して、医療機器の製造販売業者との情報共有の連携については、四病協関連で71%がしていない状況にあり、国立大学病院等でも67%が連携していない状況にあった。また、四病協関連では、連携している場合でも、業者から医療機器のサイバーセキュリティに関する説明があったのは、70%程度であり、説明があっても理解できなかった割合が32%を占めた。

サーバーセキュリティ確保に関しての経営層との情報は四病協関連では、32%程度が共有しておらず、共有していても医療機器については、10%程度であった。国立大学病院等でも33%が共有しておらず、医療機器について共有しているのは13%程度であった。

自施設でのCS対策の評価を聞いたところ、四病協関連では、50点が20%を占めていた。国立大学病院等では、60点が最も多く30%を占めていた。また、現状から100点を目指すために必要な年数を聞いたところ、四病協関連では4年～7年が45%を占め、国立大学病院等では10年が最も多く、38%を占めていた。

ネットワークに接続されている医療機器等を可視化するツールについては、価格は別として、あれば利用したいという希望が90%前後を占め、実証事業ができた場合には、国立大学病院等では、80%の医療機関で参加希望があった。

国立大学病院等に限定して、人材派遣についての状況を聞いたところ、行っているところは15%程度であるものの、講師等の派遣や研修の実施、導入・更新時の仕様策定等、アドバイザとして教員を派遣している取組みも確認できた。

自由記載では、医療機関のセキュリティ対策は、現場のリソース不足、経営の理解不足、費用の高さなどが大きな障壁となっており、補助金や専門人材の確保を含む包括的な支援についての意見が多数を占めた。

病院機能別のクロス集計の結果、一般病院、精神科病院では、専門の部署がない、責任者が

いない傾向が見られた。一方で、医療機器のCS対策を担う人員は特定機能病院でも少ないことが分かった。ネットワーク構成図の作成や追加のシステムや保守回線の管理については、一般病院、精神科病院では、できていない傾向が見られた。

情報システムに関する脆弱性情報は一般病院、精神科病院では入手できていない傾向が見られた。また、IT-BCPの作成についても進んでいない傾向が見られた。

一般病院、精神科病院では、医療機器のCS対策が必要なことをあまり知らない傾向にあり、医療機器が更新/追加されても、情報システム部門では把握できていない傾向にあった。

一方で、どの医療機関でもネットワーク構成図に医療機器まで反映できていない傾向にあり、医療機器のOSのバージョンアップやウィルス対策の確認は精神科病院だけ高い傾向にあった。

さらに、どの医療機関でも医療機器メーカからの情報提供は少ない傾向にあり、医療機関内での連携体制も弱い傾向にあった。加えて、製造販売業者との連携をしておらず、保守契約についても結んでいない傾向であった。

7）医療機器等のIoMT（Internet of Medical Things）可視化システム導入医療機関および大規模移転を経験した医療機関へのヒアリング

可視化システム導入医療機関について、市販されているネットワークに接続されている医療機器等を可視化するツールの導入状況について確認した。今後導入する過程での、課題を抽出する会議に参加した。多職種が参加し、さまざまな部署で使用できるように議論を重ねていた。可視化はほぼ可能となっており、今後は脆弱性リスクの低減や運用方法の改善を検討していくとのことであった。ネットワークに接続されている医療機器の把握とその対応が課題となっている現状において、有益なツールであることが確認できた一方で、MDS2が不明な医療機器については、サイバーセキュリティに関するリスクは問題無しと判定されることから、今後、医療機器そのものの、サイバーセキュリティに関する情報をどのように入手して活用するかについては、課題があることも確認できた。

大規模移転を経験した医療機関については、新病院開院に伴い、情報システムの運用体制が整備されていた。ネットワーク接続機器の一元管理が進められ、情報システム部門が機器を把握できる仕組みが構築されていた。また、医療機器購入の事務的チェック・審査段階での情報システム部門の関与が確立され、確認体制が整えられていた。さらに、リモートメンテナンスの共通化も検討され、移転スケジュールの影響で一部別対応となっていたが、共通化が進められていた。共通化された仕組みでは許可制を導入し、責任者が許可を出しログを記録する運用されていた。一方で、用途不明の回線が残存する現状もあり課題とされていた。

Ｄ．考察

1）医療機関の現状について

CS対策として先進的な取組みを行っているA大学病院でも、医療機器に関しては十分に対応できているとは言えず、人材不足である実情が把握できた。また、多彩な病院でのヒアリング結果もふまえると以下のような課題があると考えられた。

・製造販売業者からの情報提供体制について

情報システム系については、情報提供が徐々になされている傾向にあるが、医療機器関係については、問いかけても情報提供がないことが多い。特に地方では医療機器メーカが対応できていない現状があることが考えられた。

・医療機関における医療機器のサイバーセキュリティ確保のための手引書の周知について

初めて知った医療機関も多く、周知が重要であると考えられた。ただし、読み込んでも医療機関では分からないことが多く、医師会などで行っているような動画での解説や見た目でわかりやすい図などを挿入するなど、受け取った医療機関側が活用できるようにする工夫が重要であると考えられた。

・サイバーセキュリティ対応のレベル差について

医療機器に限らず情報システム全体のセキュリティ担当者の中でもCS対策のレベル感が違うことが分かった。企業でSEをやっていた担当者から、事務の中での役割を宛てられた担当者まで、実際に対応している担当者にばらつきがある現状が浮き彫りとなった。さらには、医療機関全体のCS対策についての進捗の立ち位置が見えず、特に医療機器に関しては担当者が何をすればよいのか把握できている状況にはなかった。このことから、何をどこまでやれば良いか医療機関側で把握ができ、他院との相対化ができるような情報システム全体の内容と医療機器を整合させた形での医療機関向けのチェックリストが必要であるとともに、それを相対評価する仕組みが必要であることが示唆された。

・CS対応担当者の状況について

情報システムの担当者だけでは医療機器まで手が回らず、実務的に対応できる余裕がない状況にあった。この状況を解決するために

は、CS対策を少しでもできるような既存の医療職種の裾野を広げるべく、診療情報管理士、臨床工学技士、診療放射線技師などについては、学生のころからセキュリティを学ぶ機会を作る必要があると考えられた。

・信頼境界（責任分解点に近い概念）を明示した契約書のひな型について

ヒアリングの結果、医療機関で信頼境界を明示した上で、契約等を行い、CS対策を行っている医療機関はなかった。医療機器等のリモートメンテナンスや脆弱性、レガシー機器への対応について、信頼境界が明確にできるような契約書のひな形的なものを、専門家を交えて医療機関の機能に応じて複数のパターン作成し公開することが有益であると考えられた。

・院内のシステム担当者と医療機器担当者の連携について

情報システムについては、責任を持つ体制が構築されつつあるが、医療機器等については、各部門での対応に委ねているところが多かった。医療機関内でのCSに関する情報共有等を進めるためには、少なくとも、情報システム関連の規程の中に、CS対策が必要な医療機器等を所有する各部門から、医療機器等の担当者を任命し、責任体制を明確にする必要があることが考えられた。また、医療機関の規模によっては、各医療機関で対応するには限界があるため、地域で支援できるような体制も行政や第三者機関が中心となって対応できるような仕組みも必要であると考えられた。

・医療機器メーカと病院担当者との連携について

医療機器のCS対策に関しては、メーカとの連携ができている医療機関はほとんどなかった。医療機器のCS対策に関する情報は医療機関側にはほとんど伝わらない状況であったことから、医療機器メーカと病院担当者との連携体制の構築が今後、医療機器のCS対策を進める上での課題であると考えられた。

・ネットワーク構成図の要件について

情報システム関連については、情報システムの管理部門でネットワーク構成図を把握しているものの、医療機器等のリモートメンテナンス回線が把握できていなかったり、細かい医療機器の接続については、一元的に管理できていない医療機関が多いことがわかった。医療機器やそれに不随するネットワーク回線の把握や更新するのは各部門、全体掌握を情報システム担当者が行うなどの、医療機関内での役割分担を明確にすることも必要あると考えられた。

・SBOMとMDS2/MDSの収集と具体的活用方法について

医療情報システムに関しては、MDSについて令和6年度版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（医療機関確認用）にも記載され、事業者から製造業者/サービス事業者による医療情報セキュリティ開示書（MDS/SDS）を提出してもらっている医療機関が多くあったが、医療機器特有のCSに関する情報である、SBOMとMDS2については情報を集めている医療機関はごくわずかであった。集めようとしても、医療機器メーカが検討中として、提出されないことも多く、医療機関側では、入手しても活用方法もわからない現状にあることが分かった。医療機器のCSを確保するためのSBOMやMDS2/MDSの医療機関への周知や活用方法の検討が必要であり、さらには第三者的に医療機器メーカからSBOMやMDS2/MDSを自動的に収集し、システマティックにその脆弱性や対策を医療機関に周知できるような仕組みの検討も必要であると考えられた。

・院内接続機器調査に係るアプリケーションの試行について

ネットワーク機器の棚卸しという点では、CS対策を進めるにあたり、医療機関内ネットワークに接続されている機器等を一元的に管理することが必要であると考えられる。医療情報システム関係については、情報部門で管理していることが多いが、ネットワークに接続されている医療機器等まで管理ができるような体制とはなっていない。また、エクセルで台帳を作成するような形で、手作業で管理することは各医療機関の大きな負担となる。市販されている製品では、医療機器等のIoMT（Internet of Medical Things）デバイスを把握する仕組みも販売されている。ある報告では、医療情報部門では4000デバイス程がネットワーク接続されていると管理していたところ、実際には8000デバイス程がネットワークに接続されていたというような報告もある。このような機能を持つシステムを試行することで、医療機関内のネットワーク機器等を見える化をする有用性を確認し、情報システム担当者が把握している医療機器と実際に接続されている医療機器の数にどのくらい乖離があるか実情を調査することも今後検討が必要であると考えられた。人の手によらない自動的に医療機器等のCS対策の基礎となる情報を収集する取組みが今後重要となると考えられる。

・アンケート結果について

今回のフィールドワークによる調査・ヒアリングで得た新たな前述のような知見も取り入れて、医療機器のCS対策の現状の課題を整

理するためにアンケート調査を行った結果、以下のような課題が浮き彫りとなった。

アクセス数が1800件を超えていたものの、最終的な回答数が210件ということから、アンケートを見て専門的な内容で回答ができないと判断した医療機関が一定程度存在すると考えられる。このことから、回答をいただいた医療機関については、CS対策について比較的積極的に取り組んでいる医療機関であると考えられる。したがって、一定程度のバイアスが存在することを想定し、結果の解釈については、過大評価される可能性があることについて留意する必要がある。それを念頭に置いたうえでも、過去のアンケート結果（研究代表者：中野壮陛　医療機関における医療機器のサイバーセキュリティに係る課題抽出等に関する研究　2019年度～2021年度）と比較して、CS対策全般については、担当部署の設置や責任者の設置、ネットワーク構成図の把握など整ってきている状況が伺えた。これは、医療法第25条に基づく立入検査でも確認が求められる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（医療機関確認用）に記載がされたことの影響が大きいことが考えられた。

一方で、CS対策を進める上で、情報システム全体を含めた共通の課題として、人材不足、医療機関でのITリテラシーの低さ、対策に必要な予算の確保、ネットワーク構成図の作成/管理、脆弱性への対応方法、経営層の認識の低さ、現在の立ち位置が不明（評価できていない）などに課題があると考えられた。さらに、医療機器CS対策の特有の課題としては、ネットワーク構成図への医療機器の反映/可視化、医療機器導入時の確認内容やSBOM、MDS2/MDSの管理、脆弱性やレガシー機器の管理等や具体的な手順（誰が管理するのかも含めて）、医療機関内での連携体制の構築、医療機関と医療機器製造販売業者との連携体制の構築などに課題がある現状が浮き彫りとなった。

2）共助・公助の体制づくりについて

医療機関におけるCS対策では専門家不在の中で、自助での対応には限界があるため、共助、公助の仕組みが重要となる。医師会では、共助の仕組みとして、相談窓口を設置し、関連資料を分かりやすくかみ砕いて周知するような先進的な取組みがされていた。医師会会員向けとなるサービスであるが、医療機関におけるCS対策への体制作りとしては、非常に有用な取組みであると考えられた。今後は、全国の医療機関が利用できる仕組みを検討するとともに、医療機関内でCS対策を担う人材への教育支援体制の充実なども重要となると考えられた。このような仕組みは、行政機関などの公的な支援を受けて、医療機器のCS対策に必要なチェックリストやガイドラインの作成なども含めて、公助として取り組む方向性についても検討すべき課題であると考えられた。

3）人材教育、配置について

医療機関へのヒアリングやアンケート調査の結果からも分かるとおり、医療機関内でCS対策ができる人材の不足が大きな課題であることが分かった。医療機関の中では、ネットワークセキュリティの知識を持つような医療従事者は皆無である。大規模な医療機関であれば、専任の従事者が配置されていることもあるが、多くの医療機関ではそのような体制を取ることもできない。仮に人材を雇用するにしてもCS対策を担うような人材は他分野でも取り合いの状況であることから、給料等の見合いが合わず、医療機関で雇用できることはかなり稀なケースであると考えられる。このような状況下では、医療機関内で何とか対応できる人材を育成することも視野に入れる必要があるが、そのためには、医療機関の役割に応じたCS対策レベルの設定とそれを担う人材の育成が重要であると考えられた。特に広く裾野を広げるためには、医療従事者でもある程度の知識を持てるように卒前・卒後の教育が重要であり、それを担う人材としては、診療情報管理士や医療情報技師、臨床工学技士、診療放射線技師が現在の医療資格等（学会認定等も含む）では近い職種であると考えられ、このような職種を育成する教育課程へのアプローチも今後必要であることが示唆された。

4）即効性のある課題解決方法について

医療機器のCS対策については、患者の生命に影響を与える可能性もあることから、医療機関の経営層と連携し、セキュリティ文化の醸成を進めることが重要であり、この達成については、医療機関のみならず、行政、サプライチェーンも含む医療機器産業界が一体となり、業界全体で取り組むべき課題であると考える。その上で、即効性のある課題解決方法については、以下の5点が考えられ、具体に実現するためには、様々な調整が必要であることが想定されるものの、今後検討を進める必要があると考えられた。

① 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（医療機関確認用）に医療機器も対象となるように明記する。

② 厚生労働省が行っている、医療機関におけるサイバーセキュリティ確保事業として、医療機器も対象とする。

③ 医療機器のCS対策に必要な情報を日本医師会へ届けることによって、日本医師会が事務局となっているCS対策に必要な情報を提供する仕組みを用いて、医療機器のCS対策に必要な情報を発信する。

④ CS対策の好事例（大学病院、グループ病院、地域医療連携ネットワーク等）を横展開していく中に医療機器も対象として入れてもらう。

⑤ 診療録管理体制加算1だけでなく、経済産業省も含めて、医療機関を中小企業と扱っていただき、国の補助金を使えるような仕組みを検討する。

5）今後の課題について

様々な団体や医療機関へのヒアリングやアンケート調査などを通じて、医療機器等のCS対策に必要な①人材、②予算の確保が重要であるとともに、③具体な方策（ネットワーク構成図の作成、

医療機器導入時の確認やSBOM、MDS2/MDSの管理、脆弱性やレガシー機器の管理等）や手順、④ネットワーク資産の可視化の仕組み、⑤医療機関内での連携体制の構築、⑥医療機関と医療機器製造販売業者との連携体制の構築、⑦各医療機関における医療機器にかかるCS対策を評価できる仕組みが重要であると考えられた。今後、医療機器のCS対策を確保するためには、これらの課題を解決すべく、行政、医療機器製造販売業者、医療機関が三位一体となり、協働で我が国の医療機器のCS対策を一歩でも進めるべく検討を重ねることが重要である。これらの課題を解決し、医療機器のCS対策を充実させることで、患者に安心・安全な医療を提供するインフラ整備の一助に資すると考えられた。

Ｅ．結論

医療機器のCS対策については、行政と製造販売業者を中心に取り組んできたものの、実際の医療機関での対応まで落とし込めている状況ではないことが浮き彫りとなった。今後、人材や予算、手段なども含めて、医療機関で具体に取り組める内容を検討し分かりやすく示すとともに、自動化できるところは自動化する仕組みの検討も必要であると考えられた。

Ｆ．健康危険情報

（総括研究報告書にまとめて記載）

Ｇ．研究発表

１．論文発表

新秀直、黒澤壮平、中里俊章、中野壮陸、松元恒一郎、特集　医療機器のサイバーセキュリティ確保に向けた動向と製造販売業者、医療機関に求められること、医療機器学　第94巻　第4号　425-463.　(2024)

２．学会発表

塩﨑英司、新秀直、中里俊章、沼館慧剛、医療機器に関するサイバーセキュリティ管理について，第44回 医療情報学連合大会（2024）

Ｈ．知的財産権の出願・登録状況

１．特許取得

なし

２．実用新案登録

なし

３．その他

なし

別紙４

研究成果の刊行に関する一覧表

書籍

著者氏名	論文タイトル名	書籍全体の編集者名	書　籍　名	出版社名	出版地	出版年	ページ

雑誌・発表

発表者氏名	論文タイトル名	発表誌名	巻号	ページ	出版年
三宅 学	サイバーセキュリティ活動報告	2024年度 医療機器の承認・認証申請等に関する説明会			2025
新秀直、黒澤壮平、中里俊章、中野壮陸、松元恒一郎	特集 医療機器のサイバーセキュリティ確保に向けた動向と製造販売業者、医療機関に求められること	医療機器学	第94巻 第4号	425-463	2024
新秀直、中里俊章、塩﨑英司	医療機器に関するサイバーセキュリティ管理について,	第44回 医療情報学連合大会			2024

Cybersecurity Vulnerabilities with Certain Patient Monitors from Contec and Epsimed: FDA Safety Communication

Date Issued: January 30, 2025

The U.S. Food and Drug Administration (FDA) is raising awareness among health care providers, health care facilities, patients, and caregivers that cybersecurity vulnerabilities in Contec CMS8000 patient monitors and Epsimed MN-120 patient monitors (which are Contec CMS8000 patient monitors relabeled as MN-120) may put patients at risk after being connected to the internet.

Three cybersecurity vulnerabilities have been identified:

- The patient monitor may be remotely controlled by an unauthorized user or not work as intended.
- The software on the patient monitors includes a backdoor, which may mean that the device or the network to which the device has been connected may have been or could be compromised.
- Once the patient monitor is connected to the internet, it begins gathering patient data, including personally identifiable information (PII) and protected health information (PHI), and exfiltrating (withdrawing) the data outside of the health care delivery environment.

These cybersecurity vulnerabilities can allow unauthorized actors to bypass cybersecurity controls, gaining access to and potentially manipulating the device.

The FDA is not aware of any cybersecurity incidents, injuries, or deaths related to these cybersecurity vulnerabilities at this time.

Recommendations for Patients and Caregivers

- Talk to your health care provider about whether your device relies on remote monitoring features. Remote monitoring means the device uses an internet connection to allow a health care provider to evaluate patient vital signs from another location (such as a remote monitoring system or central monitoring system).
    - If your health care provider confirms that your device relies on remote monitoring features, unplug the device and stop using it. Talk to your health

care provider about finding an alternative patient monitor.

- If your device does not rely on remote monitoring features, use only the local monitoring features of the patient monitor. This means unplugging the device's ethernet cable and disabling wireless (that is, WiFi or cellular) capabilities, so that patient vital signs are only observed by a caregiver or health care provider in the physical presence of a patient.
  - If you cannot disable the wireless capabilities, unplug the device and stop using it. Talk to your health care provider about finding an alternative patient monitor.

- Be aware the FDA is not aware of any cybersecurity incidents, injuries, or deaths related to this vulnerability at this time.
- Report any problems or complications with your Contec CMS8000 patient monitor or Epsimed MN-120 patient monitor to the FDA.

Recommendations for Health Care Providers

- Work with health care facility staff to determine if a patient's Contec CMS8000 patient monitor or Epsimed MN-120 patient monitor may be affected and how to reduce any associated risk.
- Read and follow the recommendations for patients and caregivers in this safety communication.
- Check the Contec CMS8000 patient monitors and Epsimed MN-120 patient monitors for any signs of unusual functioning, such as inconsistencies between the displayed patient vitals and the patient's actual physical state.
- Report any problems with your Contec CMS8000 patient monitor or Epsimed MN-120 patient monitor to the FDA.

Recommendations for Health Care Facility Staff (including Information Technology (IT) and Cybersecurity Staff)

- **Use only the local monitoring features of the device.**
  - If your patient monitor relies on remote monitoring features, unplug the device and stop using it.
  - If your device **does not** rely on remote monitoring features, unplug the device's ethernet cable and disable wireless (that is, WiFi or cellular) capabilities. If you cannot disable the wireless capabilities, then continuing to

use the device will expose the device to the backdoor and possible continued patient data exfiltration.

- Review the Cybersecurity and Infrastructure Security Agency (CISA) "Mitigations" section (https://www.cisa.gov/news-events/ics-medical-advisories/icsma-25-030-01) in the vulnerabilities related advisory.
- Be aware, at this time there is no software patch available to help mitigate this risk.
- Check the Contec CMS8000 patient monitors and Epsimed MN-120 patient monitors for any signs of unusual functioning, such as inconsistencies between the displayed patient vitals and the patient's actual physical state.
- Report any problems with your Contec CMS8000 patient monitor or Epsimed MN-120 patient monitor to the FDA.

Device Description

Patient monitors are used in health care and home settings for displaying information, such as the vital signs of a patient, including temperature, heartbeat, and blood pressure.

Cybersecurity Vulnerabilities May Affect Contec CMS8000 and Epsimed MN-120 Patient Monitors

Three cybersecurity vulnerabilities have been identified, whose potential impacts fall into two main categories. A vulnerable device could be exploited to:

- Deny access to the device, such as cause the device to crash and be unable to work as intended.
- Take over the device to remotely control it to perform unexpected or undesired actions, such as corrupting the data.

The vulnerabilities could allow all vulnerable Contec and Epsimed patient monitors on a given network to be exploited at the same time.

Additionally, the software on the patient monitors includes a backdoor. "Backdoor" is the term used to describe hidden functionality that device users are not told about and can allow unauthorized actors to bypass cybersecurity controls. The unauthorized actors could access and potentially manipulate the device. Given the backdoor, the device and/or the network to which the device has been connected may have been or could be compromised.

Also, the FDA has authorized these patient monitors only for wired functionality (that is, ethernet connectivity). However, the FDA is aware that some patient monitors may be

available with wireless (that is, WiFi or cellular) capabilities without FDA authorization.

The Cybersecurity and Infrastructure Security Agency (CISA) has identified that once the patient monitor is connected to the internet, it begins gathering and exfiltrating (withdrawing) patient data outside of the health care delivery environment, including when the device is used in a home setting. The FDA and CISA continue to work with Contec to correct these vulnerabilities as soon as possible.

Unique Device Identifier (UDI)

The unique device identifier helps identify individual medical devices, including patient monitors, sold in the United States from manufacturing through distribution to patient use. The UDI allows for more accurate reporting, reviewing, and analyzing of adverse event reports so that devices can be identified, and problems potentially corrected more quickly.

- How do I recognize a UDI on a label? (https://www.fda.gov/medical-devices/unique-device-identification-system-udi-system/udi-basics#recognize)
- AccessGUDID database - Identify Your Medical Device (https://accessgudid.nlm.nih.gov/)
- Benefits of a UDI System (/medical-devices/unique-device-identification-system-udi-system/benefits-udi-system)

You can identify the devices affected by checking the unique device identifier (UDI), which is a unique numeric or alphanumeric code that generally includes a device identifier (DI) that identifies the labeler and the specific version or model of a device.

Brand Name	Version or Model	UDI-DI
Contec	CMS8000	06945040100034
Epsimed	MN-120	N/A

FDA Actions

The FDA takes seriously any reports of cybersecurity vulnerabilities in medical devices and will continue to work with Contec and CISA to correct these vulnerabilities as soon as possible.

The FDA will continue to assess new information concerning the vulnerabilities and will keep the public informed if significant new information becomes available.

Read more about medical device cybersecurity. (/medical-devices/digital-health-center-

excellence/cybersecurity)

Reporting Problems with Your Device

If you think you had a problem with a Contec CMS8000 or Epsimed MN-120 patient monitors, the FDA encourages you to report the problem through the MedWatch Voluntary Reporting Form (https://www.accessdata.fda.gov/scripts/medwatch/index.cfm?action=reporting.home).

Health care personnel employed by facilities that are subject to the FDA's user facility reporting requirements should follow the reporting procedures established by their facilities.

Questions?

If you have questions, contact CDRH's Division of Industry and Consumer Education (DICE) (/medical-devices/device-advice-comprehensive-regulatory-assistance/contact-us-division-industry-and-consumer-education-dice).

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
令和６年10月７日

各都道府県衛生主管部（局）長　殿

厚生労働省医薬局医療機器審査管理課長
（　　公　　印　　省　　略　　）

厚生労働省医薬局医薬安全対策課長
（　　公　　印　　省　　略　　）

厚生労働省医薬局監視指導・麻薬対策課長
（　　公　　印　　省　　略　　）

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）

標記について、令和６年度厚生労働行政推進調査事業費補助金（厚生労働科学特別研究事業）において、厚生労働省の指定に基づき下記の研究が行われております。

今般、当該研究に際して、別紙により、全国の医療機器の製造販売業許可又は製造業登録を取得されている企業を対象にアンケート調査を行います。各都道府県におかれましては、御多忙のことと存じますが、貴管内製造販売業者等への情報提供について御協力くださいますよう、よろしくお願いします。

記

研究名：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年度厚生労働行政推進調査事業費補助金（厚生労働科学特別研究事業））
研究代表者：一般社団法人　国立大学病院長会議　塩崎　英司

以上

令和６年度厚生労働科学特別研究事業「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」におけるアンケート調査へのご協力のお願い

時下、益々ご清祥のこととお喜び申し上げます。

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ます。医療機器については、令和 5 年 3 月 9 日付け厚生労働省告示第 67 号「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第 41 条第 3 項の規定により厚生労働大臣が定める医療機器の基準の一部を改正する件」により、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 6 年 4 月 1 日より適用されています。

本研究班では、医療機器全般の CS 対策に関連する制度として、現在の制度での対応が十分か検討し、制度上の手当ての必要性を含めて議論を進めています。

本アンケート調査は、全国の医療機器の製造販売業許可又は製造業登録を取得されている企業の皆さまを対象にご協力をお願い致しております。医療機器全般の CS 対策の現状を把握し、問題点、課題等の情報を研究班にて収集分析し、その結果をより適切な制度設計の提言案にまとめることを考えております。

アンケートのリンク先：https://survey.zohopublic.com/zs/49D36i

アンケートの回答期間：令和 6 年 10 月 7 日（月）から令和 6 年 11 月 15 日（金）まで

なお、アンケートの最初に、回答者の氏名、電話番号及び電子メールアドレスの記入欄がございますが、アンケートを分割して回答する場合の識別に使用しております。また、回答内容についてお問合せが必要な場合に連絡をとることを目的としており、回答集計作業において回答者の情報は利用いたしません。

是非とも本調査の趣旨をご理解いただき、ご協力を賜りますようお願い申し上げます。ご不明な点等ございましたら、下記分担研究者までご連絡くださいますようお願い申し上げます。

令和６年１０月

研究代表者：塩﨑　英司（一般社団法人　国立大学病院長会議）
分担研究者：三宅　学
独立行政法人　医薬品医療機器総合機構
医療機器調査部　登録認証機関監督課
E-mail：miyake-manabu@pmda.go.jp

アンケート質問項目一覧

		備考
1	**姓，名，電話（ハイフンは不要），メールアドレス**	
	姓 名 電話（ハイフンは不要） メールアドレス	
2	**設問1：取得している製造販売業の許可の区分は何ですか？**	
	第一種医療機器製造販売業 第二種医療機器製造販売業 第三種医療機器製造販売業 外国特例承認取得者（選任された製造販売業者を含む） なし	
3	**設問2：製造販売業の範囲に含まれる構成員の人数は何名でしょうか？**	設問1で『なし』の場合、スキップし設問3へ
	1～10名 11～20名 21～50名 51～100名 101～200名 201名以上	
4	**設問3：設問1 で「なし」を選択された方にお尋ねします。製造業（設計）の登録は行っておられますか？**	
	はい いいえ	『いいえ』の場合、ここまで終了となります。
5	**設問4：設計開発部門を有している場合、設計開発部門の構成員の人数は何名でしょうか？**	
	設計部門なし（0名） 1～5名以内 6～10名 11～20名 21～50名 51名以上	
6	**設問5：製品（医療機器）は、国内製造、外国からの輸入、又は その両方 のいずれでしょうか？**	
	国内製造 外国からの輸入 国内製造と輸入の両方	
7	**設問6：サイバーセキュリティ対策を要する品目（製造販売している又は製造販売は終了したが、使用が継続している）がありますか？**	
	はい いいえ	『いいえ』の場合、ここまで終了となります。
8	**設問7：サイバーセキュリティ対策を要するクラスⅠ一般医療機器の製造販売中の品目数を教えてください。**	
	製造販売中の品目数： 新規の製造販売は終了し、サポート中の品目数：	
9	**設問8：サイバーセキュリティ対策を要するクラスⅡ管理医療機器の製造販売中の品目数を教えてください。**	
	製造販売中の品目数： 新規の製造販売は終了し、サポート中の品目数：	
10	**設問9：サイバーセキュリティ対策を要するクラスⅢ高度管理医療機器の製造販売中の品目数を教えてください。**	
	製造販売中の品目数： 新規の製造販売は終了し、サポート中の品目数：	

11	**設問10：サイバーセキュリティ対策を要するクラスⅣ高度管理医療機器の製造販売中の品目数を教えてください。**	
	製造販売中の品目数： 新規の製造販売は終了し、サポート中の品目数：	

12	**設問11：貴社の全製品（医療機器）のうち、サイバーセキュリティ対応を検討しなければならない医療機器のうち、対応が実施できている製品はどの程度ですか。**	
	0%～20% 21%～40% 41%～60% 61%～80% 81%～99% 100%	

13	**設問12：リスクマネジメント活動に従事できる力量を有する構成員の人数は何名でしょうか？**	
	1名～3名 4名～6名 7名～10名 11名以上	

14	**設問13：社内体制に関する手順書（社内規定等）の整備は完了していますか？**	
	はい（完了） 準備中（一部未完了） いいえ（未着手）	

15	**設問14：サイバーセキュリティ情報の評価体制の整備は完了していますか？**	
	はい（入手した情報の評価、製品ごとの評価も整備済み） 準備中（一部未完了） いいえ（未着手）	

16	**設問15：製造販売中の製品に対してSBOMの作成は完了していますか？**	
	はい（すべて完了） 準備中（一部未完了） いいえ（未着手）	

17	**設問16：製造販売が終了し、保守対象製品に対してSBOMの作成は完了していますか？**	
	はい（すべて完了） 準備中（一部未完了） いいえ（未着手）	

18	**設問17：製品のサイバーセキュリティに関して必要な力量を明確にし、教育・訓練を実施し、その後の力量の維持の仕組みを確立していますか？**	
	はい（完了） 準備中（一部未完了） いいえ（未着手）	

19	**設問18：製品の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を確立していますか？**	
	はい（完了） 準備中（一部未完了） いいえ（未着手）	

20	**設問19：NVDやJVNに登録されている既知の脆弱性について、製品への影響を評価する仕組みを確立していますか？**	
	はい（完了） 準備中（一部未完了） いいえ（未着手）	

21	**設問20：社外の第三者の発見者から製品の脆弱性について報告を受けることを想定して社内体制を整えていますか？**	
	はい（完了） 準備中（一部未完了） いいえ（未着手）	

22	**設問21：使用者（医療機関等）から、自社の製品かを問わず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ますか。**	
	入手していない 入手している 入手したいが方法がわからない	

23	**設問22：脆弱性等に関する報告（IPA）、セキュリティリスク等に関連する不具合等報告に該当する仕組みを確立していますか？**	
	はい（完了） 準備中（一部未完了） いいえ（未着手） 自社は製造業であり、製造販売業経由で対応している	製造業で『はい』とされた場合のみ表示

24	**設問23：使用者（医療機関等）への通知（情報提供）の方法を決定し、情報提供する仕組みを確立していますか？**	
	はい（完了） 準備中（一部未完了） いいえ（未着手） 自社は製造業であり、製造販売業で対応（必要な情報を製造販売業へ提供）している	製造業で『はい』とされた場合のみ表示

25	**設問24：製品のEOL、EOS（責任移転）に関する情報を決定し、通知（情報提供）する仕組みを確立していますか？**	
	はい（完了） 準備中（一部未完了） いいえ（未着手） 自社は製造業であり、製造販売業で対応（必要な情報を製造販売業へ提供）している	製造業で『はい』とされた場合のみ表示

26	**設問25：製造販売中の製品（医療機器）に対してEOL、EOSを定めている状況を教えてください。**	
	はい（すべて完了） 準備中（一部未完了） いいえ（未着手） 自社は製造業であり、製造販売業で対応（必要な情報を製造販売業へ提供）している	製造業で『はい』とされた場合のみ表示

27	**設問26：製造販売が終了した、保守対象である製品（医療機器）に対してEOL、EOSを定めている状況を教えてください。**	
	はい（すべて完了） 準備中（一部未完了） いいえ（未着手） 自社は製造業であり、製造販売業で対応（必要な情報を製造販売業へ提供）している	製造業で『はい』とされた場合のみ表示

28	**設問27：製品（医療機器）の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を確立していますか？**	
	はい（完了） 準備中（一部未完了） いいえ（未着手）	

29	**設問28：製品（医療機器）のセキュリティポリシーを定めていますか？**	
	はい（完了） 準備中（一部未完了） いいえ（未着手） 自社は製造業であり、製造販売業のものを受け入れている	製造業で『はい』とされた場合のみ表示

30	**設問29：製品（医療機器）のセキュリティポリシーを使用者（医療機関等）に開示する仕組みを確立していますか？**	
	はい（完了） 準備中（一部未完了） いいえ（未着手） 自社は製造業であり、製造販売業で対応している	

31	**設問30：侵入試験等で、第三者試験を利用したことはありますか？**	
	はい（頻繁） はい（数回） いいえ	

32	**設問31：開発段階で、製品ソフトウェアの保守計画を作成する手順を確立していますか？**	
	はい（完了） 準備中（一部未完了） いいえ（未着手）	

33	**設問32：製品ソフトウェアの保守計画を使用者（医療機関等）に提示していますか？**	
	はい（完了） 準備中（一部未完了） いいえ（未着手）	

34	**設問33：製造販売中の製品（医療機器）に対して使用者（医療機関等）への情報提供体制の整備は完了していますか？**	
	はい（すべて完了） 準備中（一部未完了） いいえ（未着手） 自社は製造業であり、製造販売業で対応（必要な情報を製造販売業へ提供）している	製造業で『はい』とされた場合のみ表示

35	**設問34：製造販売が終了し、保守対象となる製品（医療機器）に対して使用者（医療機関等）への情報提供体制の整備は完了していますか？**	
	はい（すべて完了） 準備中（一部未完了） いいえ（未着手） 自社は製造業であり、製造販売業で対応（必要な情報を製造販売業へ提供）している	製造業で『はい』とされた場合のみ表示

36	**設問35：セキュリティパッチ等のアップデートを定期点検以外のタイミングで実施したことがありますか？**	
	はい（頻繁） はい（数回） いいえ 自社は製造業であり、製造販売業で対応している	製造業で『はい』とされた場合のみ表示

37	**設問36：市販後の製品の脆弱性管理として、収集又は報告された脆弱性等の分析結果（対応の判定結果）について記録がありますか？**	
	はい（完了） 準備中（一部未完了） いいえ（未着手）	

38	**設問37：脆弱性等に関するアドバイザリー情報を使用者（医療機関等）に提供していますか？**	
	はい（完了） 準備中（一部未完了） いいえ（未着手） 自社は製造業であり、製造販売業で対応（必要な情報を製造販売業へ提供）している	製造業で『はい』とされた場合のみ表示

39	**設問38：脆弱性等に関する使用者（医療機関等）への情報提供について、PSIRT等の製品セキュリティインシデント対応組織を設置していますか？**	
	はい（完了） 準備中（一部未完了） いいえ（未着手）	

40	**設問39：セキュリティリスクを扱うリスクマネジメントを実施する仕組みを確立していますか？**	
	はい（完了） 準備中（一部未完了） いいえ（未着手）	

41	**設問40：脅威分析等に基づき製品の信頼境界を決定し、使用者（医療機関等）に提示していますか？**	
	はい（完了） 準備中（一部未完了） いいえ（未着手） 自社は製造業であり、製造販売業で対応（必要な情報を製造販売業へ提供）している	製造業で『はい』とされた場合のみ表示

42	**設問41：製品のソフトウェア開発では、ソフトウェア構成管理等を含むJIS T 2304を適用した上で、サイバーリスクを扱うために必要なアクティビティを実施することが求められています。ソフトウェア開発で、アウトソース先がある場合、SBOM等ソフトウェア構成管理、脆弱性管理に必要な情報が入手可能な契約になっていますか？**	
	はい（完了） 準備中（一部未完了） いいえ（未着手）	

43	**設問42：使用者（医療機関等）から、脆弱性に対する対応状況の問合せ又はマルウェアによる感染確認等の依頼を受けたことがありますか？**	
	はい（頻繁） はい（数回） いいえ	

44	**設問43：製造販売業としてのQMS対象である製造業・委託先の管理について、製造業・委託先におけるサイバーセキュリティに関する対応状況を把握していますか。**	
	製造業者および委託先まで含めて全て把握 製造業までを把握している（委託先は把握していない） 把握していない 自社は製造業であり、求めに応じ製造販売業者へ情報を提供している	製造業で『はい』とされた場合のみ表示

45	**設問44：サイバーセキュリティに関する問い合わせ先を明確にし、使用者（医療機関等）に対して情報提供していますか。**	
	公開している 今後公開する予定 公開していない 自社は製造業であり、製造販売業で対応（必要な情報を製造販売業へ提供）している	製造業で『はい』とされた場合のみ表示

46	**設問45：明確にしている場合、医療機関から問い合わせはありましたか？**	
	あった なかった 自社は製造業であり、製造販売業経由で問い合わせがあった	製造業で『はい』とされた場合のみ表示

47	**設問46：問い合わせがあった場合、どのような内容ですか？**	設問45で『あった』とされた場合のみ表示、それ以外はスキップして、設問48へ
		記載ください

48	**設問47：問い合わせがあった場合、問い合わせに対して十分な対応ができましたか？**	設問45で『あった』とされた場合のみ表示、それ以外はスキップして、設問48へ
	できた できなかった	

49	**設問48：製造販売時におけるサイバーセキュリティに関する情報を使用者（医療機関等）に対して提供していますか。**	
	提供している 要求があれば提供する 提供していない 自社は製造業であり、製造販売業で対応（必要な情報を製造販売業へ提供）している	製造業で『はい』とされた場合のみ表示

50	**設問49：製造販売時におけるサイバーセキュリティに関する情報を使用者（医療機関等）に対して提供している場合、どのような方法で提供していますか。（複数選択可能）**	
	自社WEBサイト 添付文書 取り扱い説明書 契約書 技術資料 サイバーセキュリティに関する特別文書 自社は製造業であり、製造販売業で対応（必要な情報を製造販売業へ提供）している その他（具体的にご記入ください）	製造業で『はい』とされた場合のみ表示

51	**設問50：市販後においてサイバーセキュリティに関する情報を使用者（医療機関等）に対して提供していますか。**	
	提供している 要求があれば提供する 提供していない 自社は製造業であり、製造販売業で対応（必要な情報を製造販売業へ提供）している	製造業で『はい』とされた場合のみ表示
52	**設問51：貴社は、製品（医療機器)に関するソフトウェア部品表（SBOM）を使用者（医療機関等）に対し、開示していますか。**	設問50で『提供していない』とされた場合のみ表示、それ以外はスキップし、設問53へ
	提供している 要求があれば提供する 提供していない 自社は製造業であり、製造販売業で対応（必要な情報を製造販売業へ提供）している	
53	**設問52：提供していない場合、ソフトウェア部品表（SBOM）の提供には何か課題があると考えていますか。（複数選択可能）**	
	知的財産の流出の懸念（提供先からの情報漏洩） ソフトウェア関連の改良・改善と情報開示のタイミングのズレ どこまで公開するのかわからない（標準フォーマットが不明） 社内でどの部門まで対応しないといけないかわからない（資材、開発、生産部門など） サードパーティやオープンソフトウェアの妥当性検証の懸念 開示しても顧客（医療機関等）側が適切に理解するかが懸念（合理性のない対応を求められる懸念）	
54	**設問53：納品時、ネットワークに接続して使用することを使用者（医療機関等）に確認していますか？**	
	確認している 確認していない 自社は製造業であり、製造販売業で対応している	製造業で『はい』とされた場合のみ表示
55	**設問54：ネットワークに接続して使用する場合には、サイバーセキュリティ確保のための対応が必要であることを使用者（医療機関等）に通知していますか？**	
	通知している 通知していない 自社は製造業であり、製造販売業で対応している	製造業で『はい』とされた場合のみ表示
56	**設問55：使用者（医療機関等）のネットワーク構成図を把握していますか？**	
	把握している 把握したいが把握できない（医療機関側から開示されない） 把握していない 自社は製造業者であり、把握したいが把握できない（製販業者側から共有されない）	製造業で『はい』とされた場合のみ表示
57	**設問56：製品（医療機器）について、SBOMを作成していますか？**	
	作成している 一部作成している 作成していない	
58	**設問57：SBOMを作成していない場合、その理由は何ですか？（複数選択可能）**	
	作り方がわからない 作れる人がいない 作る意味がない その他（具体的にご記入ください）	
59	**設問58：製品（医療機器）について、MDS2を作成していますか？**	
	作成している 一部作成している 作成していない その他（具体的にご記入ください）	

60	**設問59：MDS2を作成していない場合、その理由は何ですか？（複数選択可能）**	
	作り方がわからない 作れる人がいない 作る意味がない その他（具体的にご記入ください）	

61	**設問60：製品（医療機器）のサイバーセキュリティに関して、どのような情報を医療機関に通知していますか。（製造業の場合は、製造販売業経由で通知する情報を選択してください。）（複数選択可能）**	
	SBOM MDS2 EOL EOS 脆弱性情報 レガシー医療機器に関する情報 通知していない その他（具体的にご記入ください）	

62	**設問61：製品（医療機器）のサイバーセキュリティに関する情報として、SBOM、MDS2を通知している場合、医療機関にどのような内容を通知していますか。（製造業の場合は、製造販売業経由で通知する情報を選択してください。）（複数選択可能）**	
	SBOMの意義 SBOMの管理方法 SBOMの使い方 MDS2の意義 MDS2の管理方法 MDS2の使い方 その他（具体的にご記入ください）	

63	**設問62：製品（医療機器）のサイバーセキュリティに関する情報を医療機関のどの部署に通知していますか。（複数選択可能）**	
	事務（購買）部門 事務（総務）部門 使用する診療科・部門 医療安全部門、医療機器管理部門 医療情報管理部門 自社は製造業であり、製造販売業で対応している その他（具体的にご記入ください）	製造業で『はい』とされた場合のみ表示

64	**設問63：製品（医療機器）のサイバーセキュリティに関する情報はどのようなタイミングで医療機関に通知していますか。（複数選択可能）**	
	入札時、納品時 医療機関からの求めに応じて 脆弱性などの情報がわかったとき サイバーセキュリティ対策（脆弱性等）が必要となったとき EOLの時期が決まったとき EOSの時期が決まったとき レガシー医療機器が発生したとき 自社は製造業であり、製造販売業で対応（必要な情報を製造販売業へ提供）している その他（具体的にご記入ください）	製造業で『はい』とされた場合のみ表示

65	**設問64：製品（医療機器）のサイバーセキュリティに関する情報（EOL/EOS）はどのようなタイミングで医療機関に通知していますか。**	
	EOL/EOSの2年前 EOL/EOSの1年前 EOL/EOSの半年前 EOL/EOSの3ヶ月前 EOL/EOSの1ヶ月前 自社は製造業であり、製造販売業で対応（必要な情報を製造販売業へ提供）している その他（具体的にご記入ください）	製造業で『はい』とされた場合のみ表示

66	**設問65：レガシー医療機器のサイバーセキュリティの確保に必要な情報については、どのようなタイミングでどのように把握していますか？**	
		記載ください

67	**設問66：レガシー医療機器の対応については、どのような内容を医療機関に通知していますか？（複数選択可能）**	
	使用継続のリスク 使用継続のための費用 ネットワークから遮断する方法 ファイヤーウォールなどの対応 とくに通知していない その他（具体的にご記入ください）	

68	**設問67：SBOMに含まれるソフトウェアに関連する脆弱性情報などは、どのようなタイミングでどのように把握していますか？**	
		記載ください

69	**設問68：製品（医療機器）のサイバーセキュリティに関する情報を医療機関に渡す想定で、添付文書、取扱説明書や保守点検マニュアルに記載していますか？（複数選択可能）**	
	取り扱い説明書に記載している 保守点検マニュアルに記載している 自社は製造業であり、製造販売業で対応（必要な情報を製造販売業へ提供）している 記載していない	製造業で『はい』とされた場合のみ表示

70	**設問69：記載している場合、どのような内容を記載していますか？**	
		記載ください

71	**設問70：医療機関からサイバーセキュリティに関するどのような情報を求められますか？（製造業の場合は、製造販売業からの要求で提供する情報を選択してください。）（複数選択可能）**	
	求められない ネットワーク構成図 SBOM MDS2 EOL EOS 脆弱性情報を含むアドバイザリー情報 レガシー医療機器に関する情報 その他（具体的な情報を記載してください）	

72	**設問71：医療機器のサイバーセキュリティ確保に関して、医療機関との連携の課題についてお答えください。**	
		記載ください

73	**設問72：医療機関と製造販売業者との情報共有について、具体化する等の意見をお答えください。**	
		記載ください

74	**設問73：医療機器サイバーセキュリティに関する保守契約を医療機関と締結していますか？**	
	締結している 締結していない 自社は製造業であり、直接締結していない	製造業で『はい』とされた場合のみ表示

75	**設問74：締結している場合、信頼境界及び責任分界点はどのような内容で、どのように決めていますか？**	
		記載ください

76	**設問75：販売業者、修理業者に対して、サイバーセキュリティ対策の確認や指導等を行っていますか。**	
	定期的に指導等を行っている 不定期に指導等を行っている 行っていない 自社は製造業であり、製造販売業で対応（必要な情報を製造販売業へ提供）している	製造業で『はい』とされた場合のみ表示

77	**設問76：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感じていることを選択してください。（複数選択可能）**	
	専門家の確保 専門家以外の教育 対策費用等 医療機関との連携・情報共有 リスクマネジメントの具体的方法 その他（具体的にご記入ください）	

78	**設問77：医療機器のサイバーセキュリティ対策について課題と感じていることをご記載してください。**	
		記載ください

79	**設問78：医療機器の基本要件基準第12条第3項の適用について、課題又は懸念等がありましたらご記載ください。**	
		記載ください

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

【調査の目的】

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。医療機器については、令和 5 年 3 月 9 日付け厚生労働省告示第 67 号「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第 41 条第 3 項の規定により厚生労働大臣が定める医療機器の基準の一部を改正する件」により、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 6 年 4 月 1 日より適用されている。

本研究班では、医療機器全般の CS 対策に関連する制度として、現在の制度での対応が十分か検討し、制度上の手当ての必要性を含めて議論を進めている。本調査は、医療機器全般の CS 対策の現状を把握し、問題点、課題等の情報を収集分析し、その結果をより適切な制度設計の提言案にまとめることを目的に実施する。

- 2024 年 10 月 7 日から 11 月 15 日までの期間、全国の医療機器の製造販売業者、製造業者等を対象に資料に示すアンケート調査を行った（資料１：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））
- 全 441 社の医療機器の製造販売業者、製造業者等からの回答を得た。アンケート調査の実施にあたっては、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 アンケートシステムを利用した。アンケート結果の集計、解析作業は、独立行政法人医薬品医療機器総合機構医療機器調査部登録認証機関監督課にて実施した。

【アンケート結果（要約）】（資料２：サイバーセキュリティ対策の対応状況アンケート結果（グラフ））

- アンケート回答者について
  - ✓ 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（設問 1 及び 3）。
  - ✓ 製造販売業許可取得者については、製造販売業の範囲に含まれる構成員の人数として、21～51 名の会社が最も多く、次いで 1～10 名、201 名以上と会社の規模にはバラツキが大きいと推察された（設問 2）。
  - ✓ 製造販売業許可取得者における設計開発部門の構成員の人数については、設計開発部門を有しない会社が最も多く全体の 36%であった。特に第一種医療機器製造販売業許可取得者のうち、43%の会社では設計開発部門を有していなかった。また、設計開発部門の構成員の人数としては、1～5

名の会社が多く全体の 24%であった（設問 4)。

- ✓ 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（設問 5)。

- CS 対策の対応状況について
  - ✓ 医療機器の製造販売業者、製造業者等において、CS 対策を要する製品が全体の 57%であった。外国製造医療機器特例承認取得者（選任製造販売業者を含む)、第一種医療機器製造販売業許可取得者及び第二種医療機器製造販売業許可取得者において、CS 対策を要する製品が多い傾向であった（設問 6)。
  - ✓ 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。一方で、全体の 15%の製品については、対応状況が 0～20%と低く、特に第三種医療機器製造販売業許可取得者では 19%と高い傾向であった（設問 11)。
  - ✓ リスクマネジメント活動に従事できる力量を有する構成員の人数については、11 名以上と回答した会社が最も多く全体の 33%であった。一方で、1～3 名と回答した会社も全体の 31%と多く、特に第三種医療機器製造販売業許可取得者では 50%であり、リスクマネジメントの実施やサイバーセキュリティ対策を実施するにあたり、力量を有する実務者のリソース不足が懸念された（設問 12)。
  - ✓ 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。しかしながら、第三種医療機器製造販売業許可取得者においては、手順書の整備、評価体制の整備ともに、約 14%の会社で未着手とのことで、対応に遅れが生じていることが示唆された。（設問 13 及び 14)
  - ✓ 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ことから、対応は概ね順調に進められていると考えられた。しかしながら、第三種医療機器製造販売業許可取得者においては、30%の会社で未着手とのことで、対応に遅れが生じていることが示唆された（設問 17)。
  - ✓ 製造販売中の製品に関する SBOM 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（設問 15)。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（設問 16)。

- ✓ 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（設問 18)。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（設問 20)。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（設問 21)。既知の脆弱性に対する製品の影響を評価する仕組みについては、全体の 20%の会社で確立されていないとのことであった（設問 19)。セキュリティリスクに情報収集する体制は確立されつつも、受動的な情報収集の体制であり、能動的に情報収集するまでには至っておらず、また、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。
- ✓ 脆弱性等に関する報告（IPA)、セキュリティリスク等に関連する不具合等報告に該当する仕組みについては、全体の 59%の会社で確立されており、28%の会社で準備中であった。しかしながら、第三種医療機器製造販売業許可取得者においては、26%の会社で未着手とのことで、対応に遅れが生じていることが示唆された（設問 22)。
- ✓ 製品の EOL/EOS の設定状況については、製造販売中の製品の全体の 35%の会社で設定済みであり、42%の会社は準備中で、22%の会社が未着手の状況であった（設問 25)。一方、製造販売の終了した保守対象製品は、全体の 42%の会社は設定済みであり、28%の会社は準備中で、30%の会社は未着手の状況であった（設問 26)。
- ✓ 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%の会社で確立済みであり、29%の会社で準備中、13%の会社で未着手の状況であった（設問 27)。特に、第三種医療機器製造販売業許可取得者においては、22%の会社で未着手とのことで、対応に遅れが生じていることが示唆された。
- ✓ 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（設問 28)。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（設問 29)。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ることが示唆された。

- ✓ 開発段階で製品ソフトウェアの保守計画を作成する手順を確立しているかについては、全体の 57%の会社で確立済みであり、25%の会社で準備中、18%の会社で未着手の状況であった（設問 31）。製品ソフトウェアの保守計画の使用者への提示については、全体の 23%の会社で提示しており、32%の会社で準備であったが、45%の会社で未着手の状況であった（設問 32）。製品ソフトウェアの保守計画を開発段階で作成する意識は高いが、その保守計画を使用者に提示している会社は少ないことが示唆された。
- ✓ 製造販売中の製品に対する使用者への情報提供体制の整備については、全体の 63%の会社で完了しており、27%の会社で準備中、10%の会社で未着手であった（設問 33）。製造販売が終了した保守対象製品に対する使用者への情報提供体制の整備については、全体の 46%の会社で完了しており、25%の会社で準備中、29%の会社で未着手であった（設問 33）。製造販売業者として、製造販売中の製品への対応を優先しており、製造販売が終了した保守対象製品への対応が遅れていることが示唆された。
- ✓ 脆弱性等に関する使用者への情報提供に関して、PSIRT 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（設問 38）。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（設問 37）。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（設問 42）。また、問合せを受けた場合であっても、全体の 94%の会社で十分な対応ができたとの結果であった（設問 47）。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ものの、使用者からと問合せはアンケート実施時点において多くなく、問い合わせがあった場合でも十分な対応が図られていることが示唆された。
- ✓ 製品の納品時にネットワークに接続して使用することについて、全体の 73%の会社が使用者に確認していた（設問 53）。また、ネットワークに接続する場合は、サイバーセキュリティ確保のための対応が必要であることを、全体の 63%の会社が使用者へ通知していた（設問 54）。
- ✓ 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（設問 55）。また、医療機器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（設問 73）。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（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%）、医療機関との連携・情報共有（全体の 18%）、リスクマネジメントの具体的方法（全体の 14%）の順で挙げられた（設問 76）。専門家の確保、教育訓練の実施等は、対策費用等につながることであり、製品のサイバーセキュリティに関するリスクに応じた対応が必要だと考えられた。また、上述したとおり、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た。

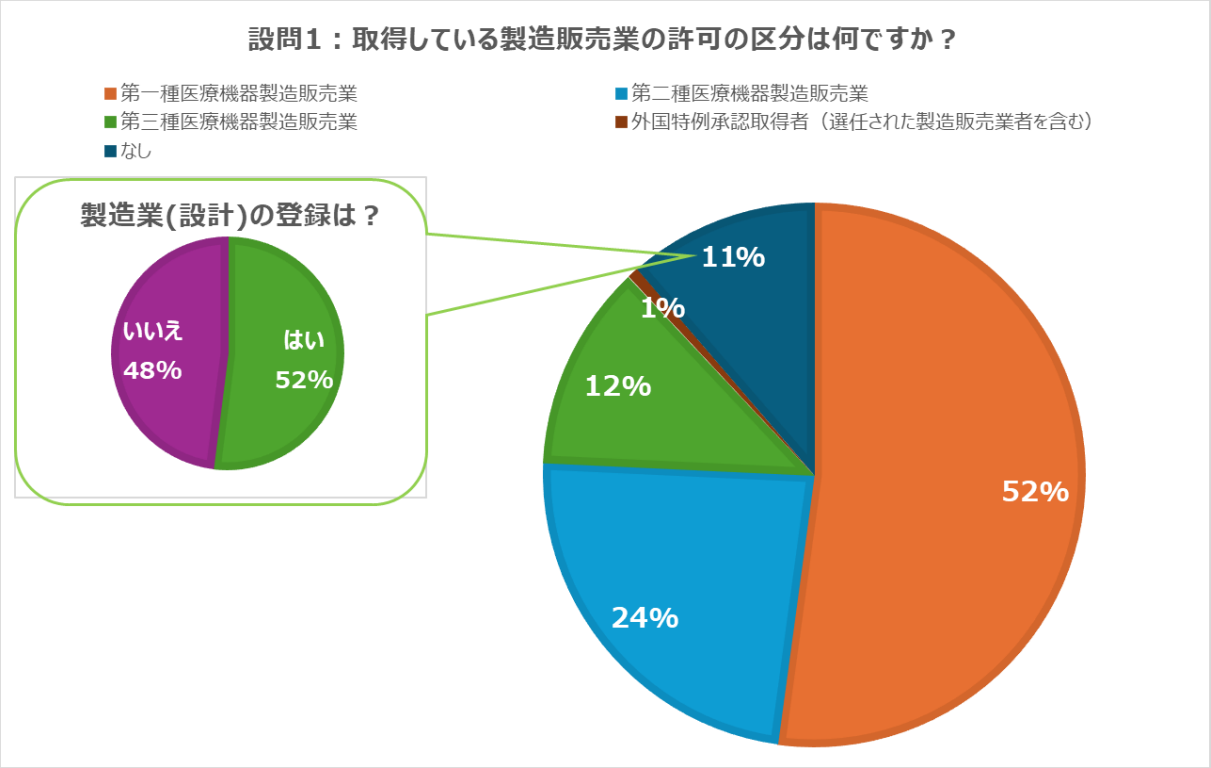
以上

設問１：取得している製造販売業の許可の区分は何ですか？

選択肢	回答数
第一種医療機器製造販売業	230
第二種医療機器製造販売業	104
第三種医療機器製造販売業	54
外国特例承認取得者（選任された製造販売業者を含む）	3
なし	50
合計	441

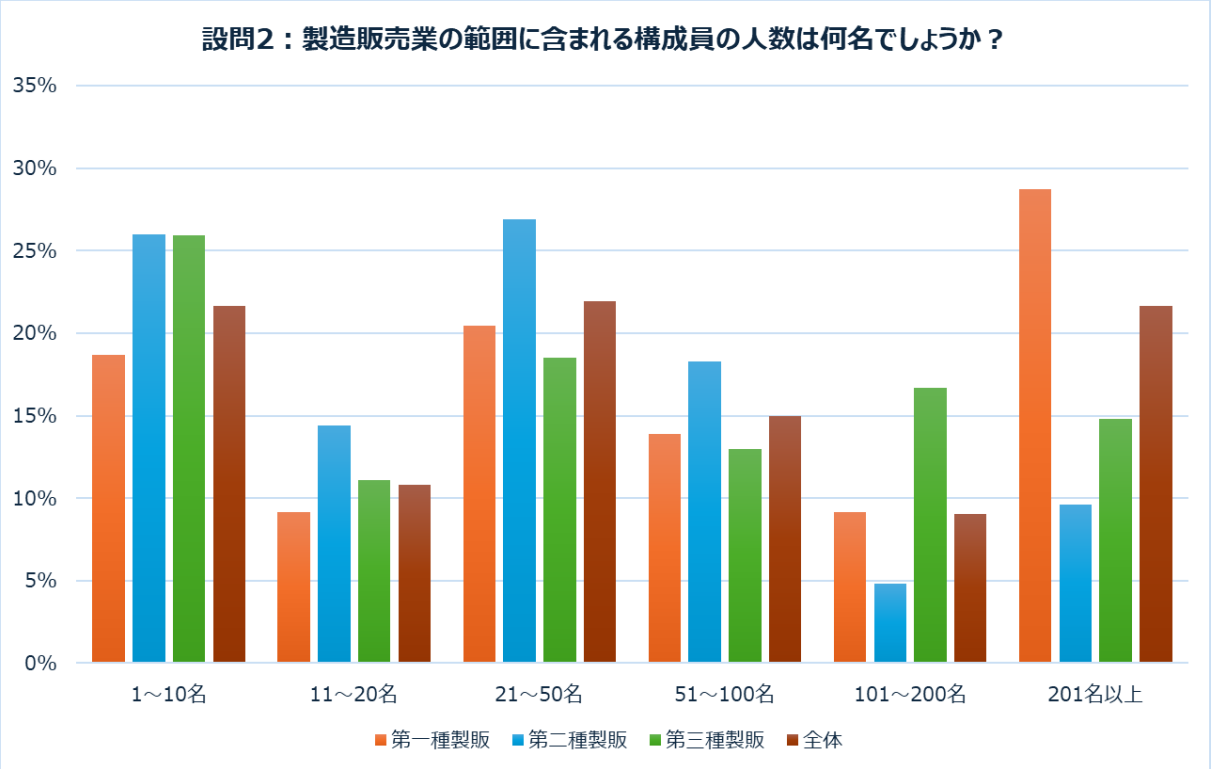
設問３：設問１ で「なし」を選択された方にお尋ねします。製造業（設計）の登録は行っておられますか？

選択肢	回答数
はい	26
いいえ	24
	50



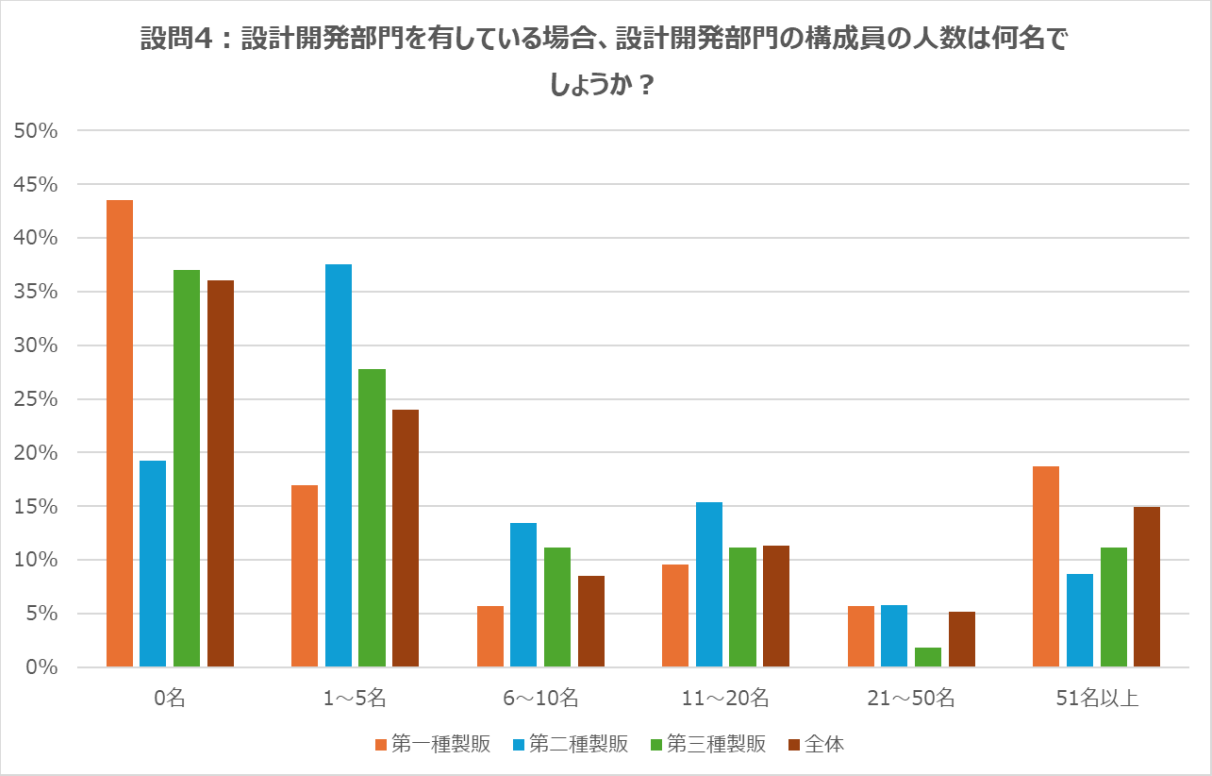
設問 2：製造販売業の範囲に含まれる構成員の人数は何名でしょうか？

選択肢	1～10 名	11～20 名	21～50 名	51 ～ 100 名	101～200 名	201 名以上
第一種製販	43	21	47	32	21	66
第二種製販	27	15	28	19	5	10
第三種製販	14	6	10	7	9	8
全体	84	42	85	58	35	84



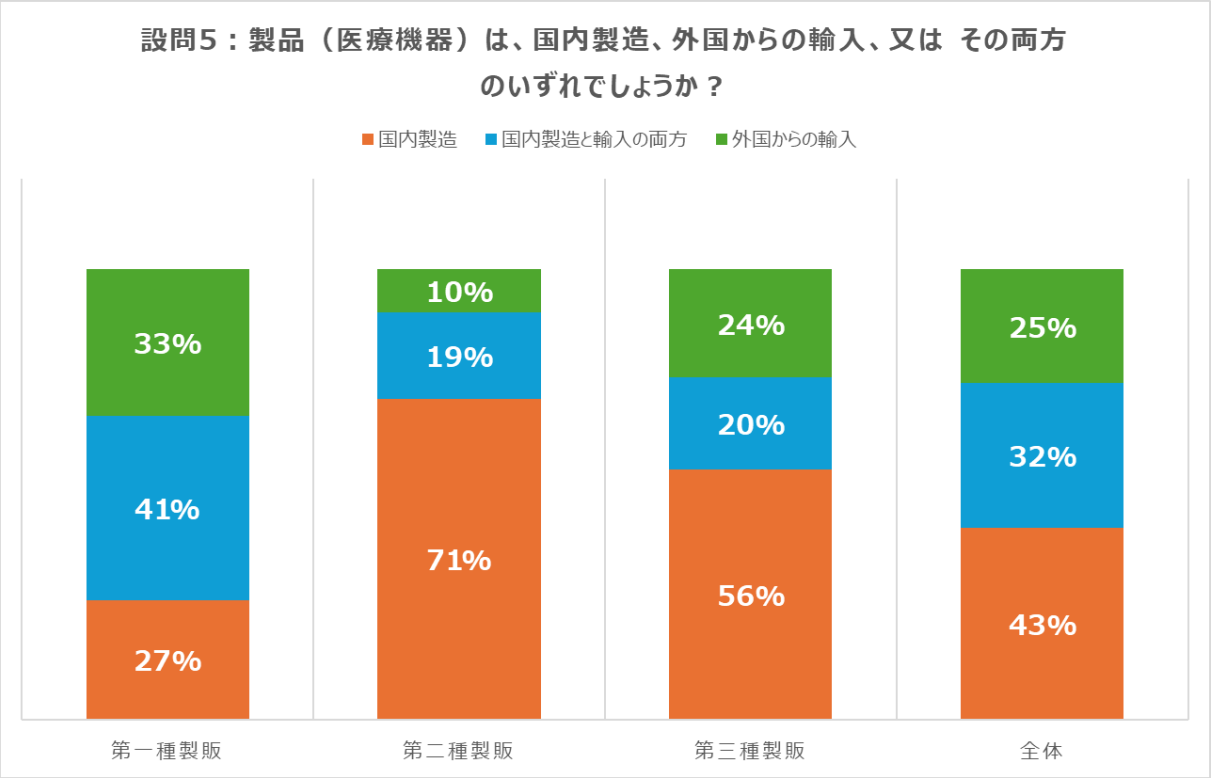
設問 4：設計開発部門を有している場合、設計開発部門の構成員の人数は何名でしょうか？

選択肢	設計開発部門なし（0 名）	1～5 名	6～10 名	11 ～ 20 名	21 ～ 50 名	51 名以上
第一種製販	100	39	13	22	13	43
第二種製販	20	39	14	16	6	9
第三種製販	20	15	6	6	1	6
全体	140	93	33	44	20	58



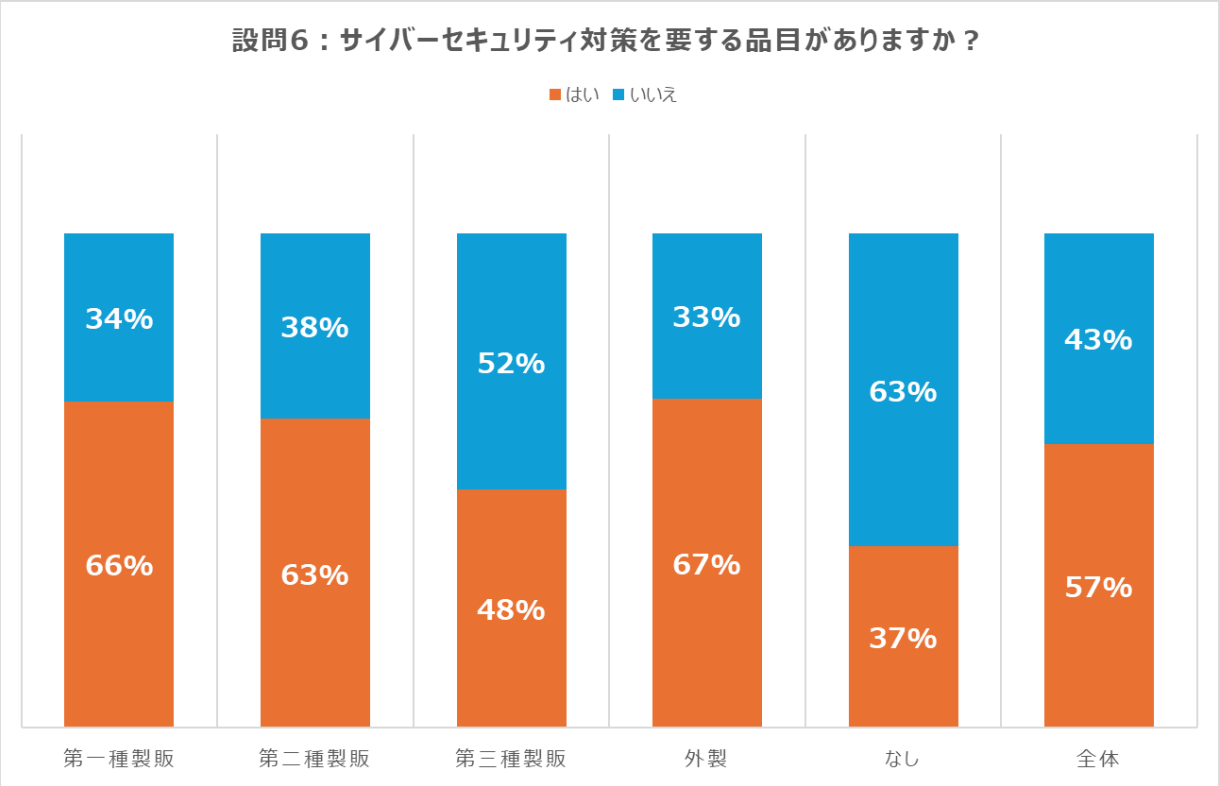
設問５：製品（医療機器）は、国内製造、外国からの輸入、又は その両方 のいずれでしょうか？

選択肢	第一種製販	第二種製販	第三種製販
国内製造	61	74	30
国内製造と輸入の両方	94	20	11
外国からの輸入	75	10	13
全体	230	104	54



設問 6：サイバーセキュリティ対策を要する品目（製造販売している又は製造販売は終了したが、使用が継続している）がありますか？

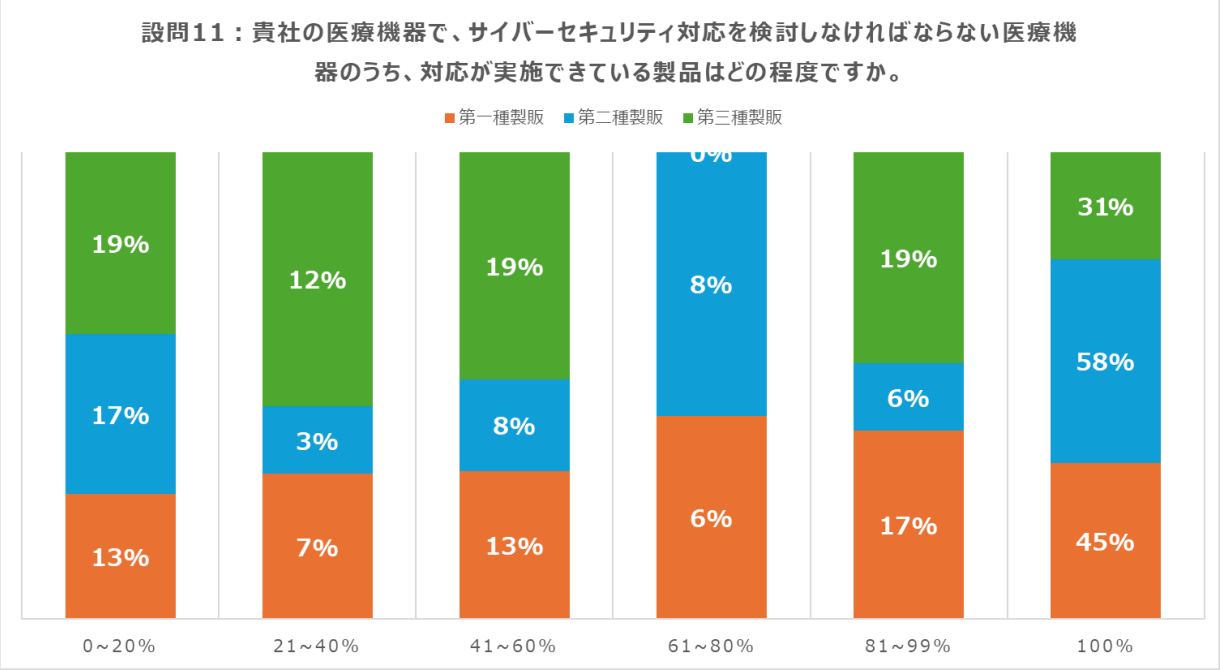
選択肢	第一種製販	第二種製販	第三種製販	外製	なし
はい	152	65	26	2	11
いいえ	78	39	28	1	19



設問 11：貴社の全製品（医療機器）のうち、サイバーセキュリティ対応を検討しなければならない医療機器のうち、対応が実施できている製品はどの程度ですか。

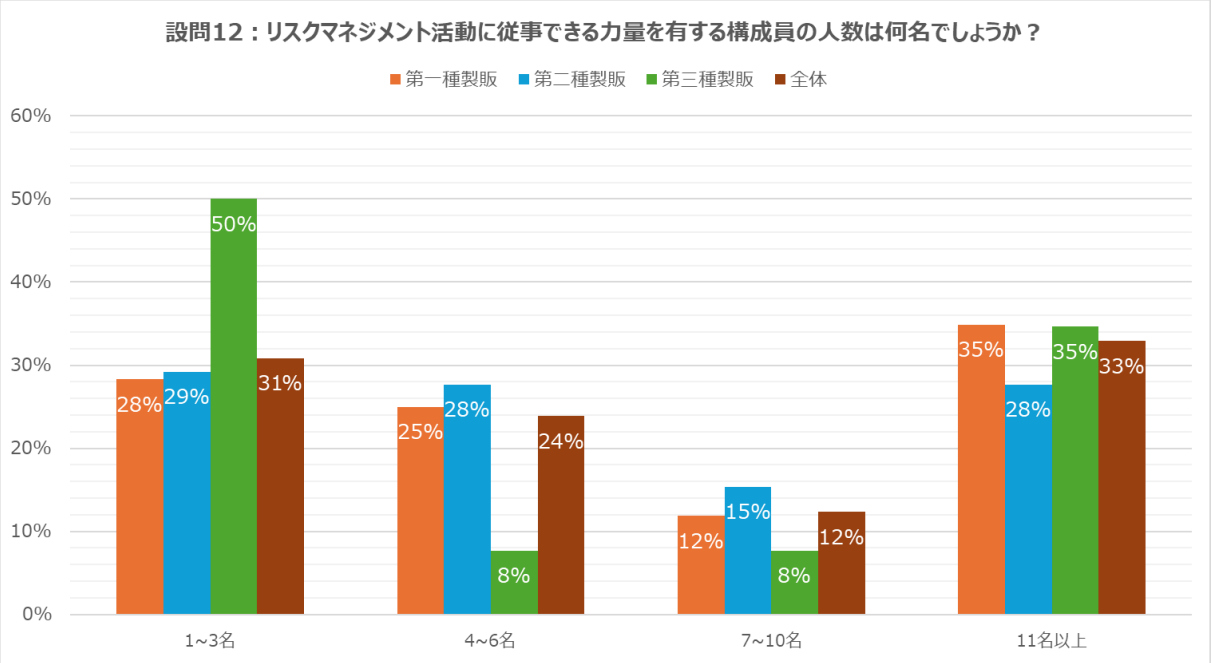
選択肢	0~20%	21~40%	41~60%	61~80%	81~99%	100%
第一種製販	20	10	19	6	21	49
第二種製販	5	2	4	5	4	29
第三種製販	4	3	1	0	4	7
外製・選任製販	0	0	1	0	0	1
なし	1	0	0	0	0	2

※　サンプルサイズが 5 件のため、外製・選任製販及びなしについては、設問 12 以降の集計から除いた。



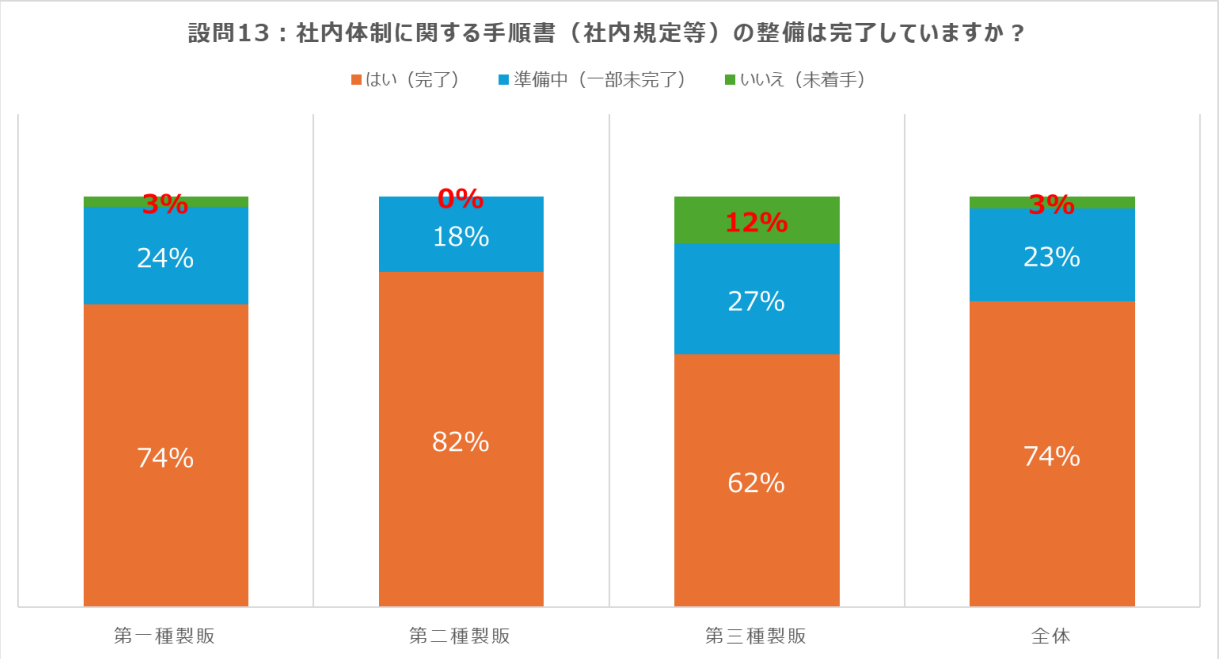
設問 12：リスクマネジメント活動に従事できる力量を有する構成員の人数は何名でしょうか？

選択肢	1~3 名	4~6 名	7~10 名	11 名以上	全体
第一種製販	43	38	18	53	152
第二種製販	19	18	10	18	65
第三種製販	13	2	2	9	26



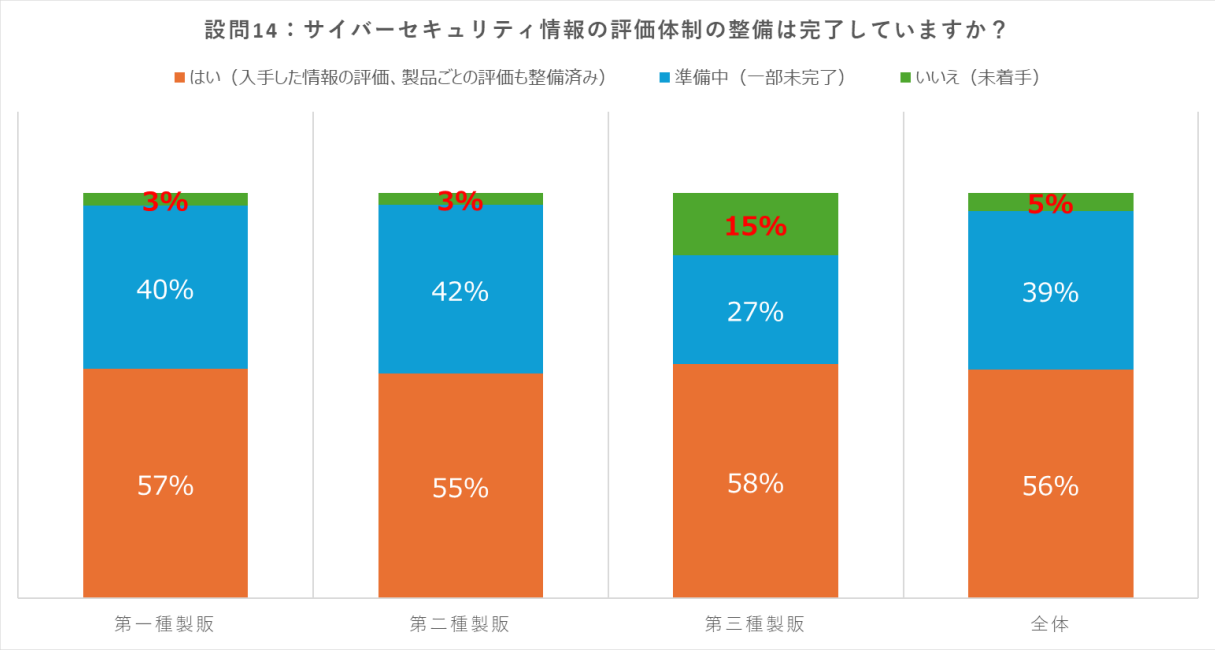
設問 13：社内体制に関する手順書（社内規定等）の整備は完了していますか？

選択肢	はい（完了）	準備中（一部未完了）	いいえ（未着手）
第一種製販	112	36	4
第二種製販	53	12	0
第三種製販	16	7	3
全体	181	55	7



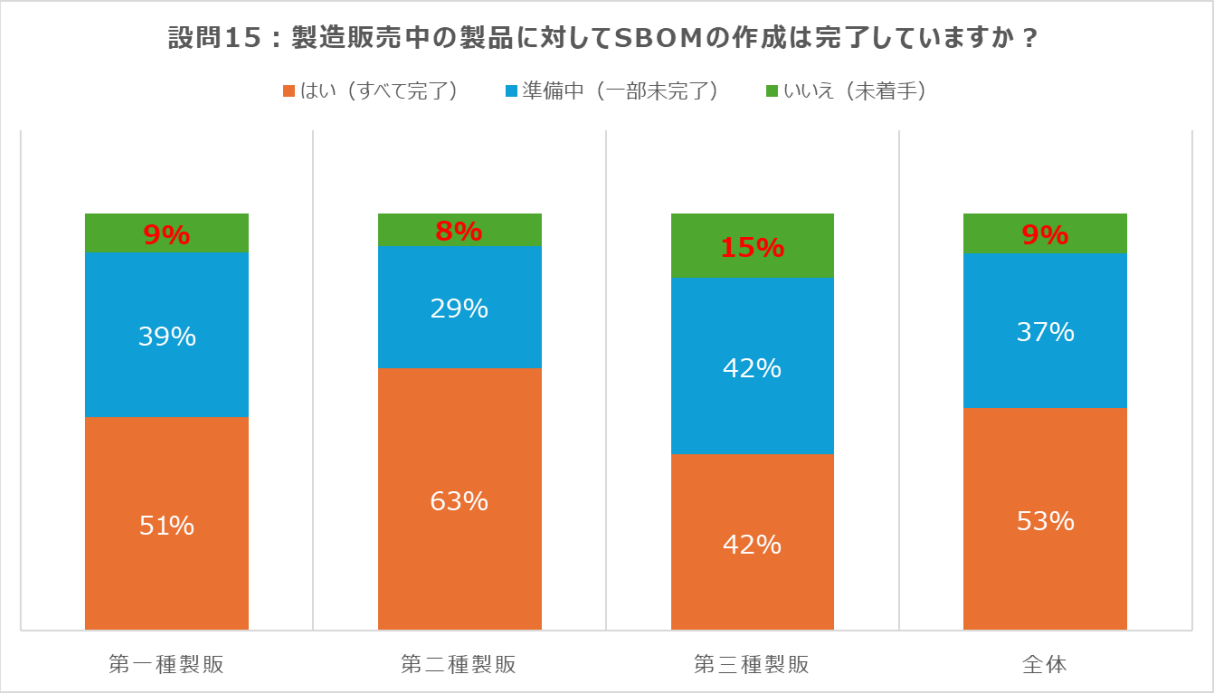
設問 14：サイバーセキュリティ情報の評価体制の整備は完了していますか？

選択肢	はい（入手した情報の評価、製品ごとの評価も整備済み）	準備中（一部未完了）	いいえ（未着手）
第一種製販	86	61	5
第二種製販	36	27	2
第三種製販	15	7	4
全体	137	95	11



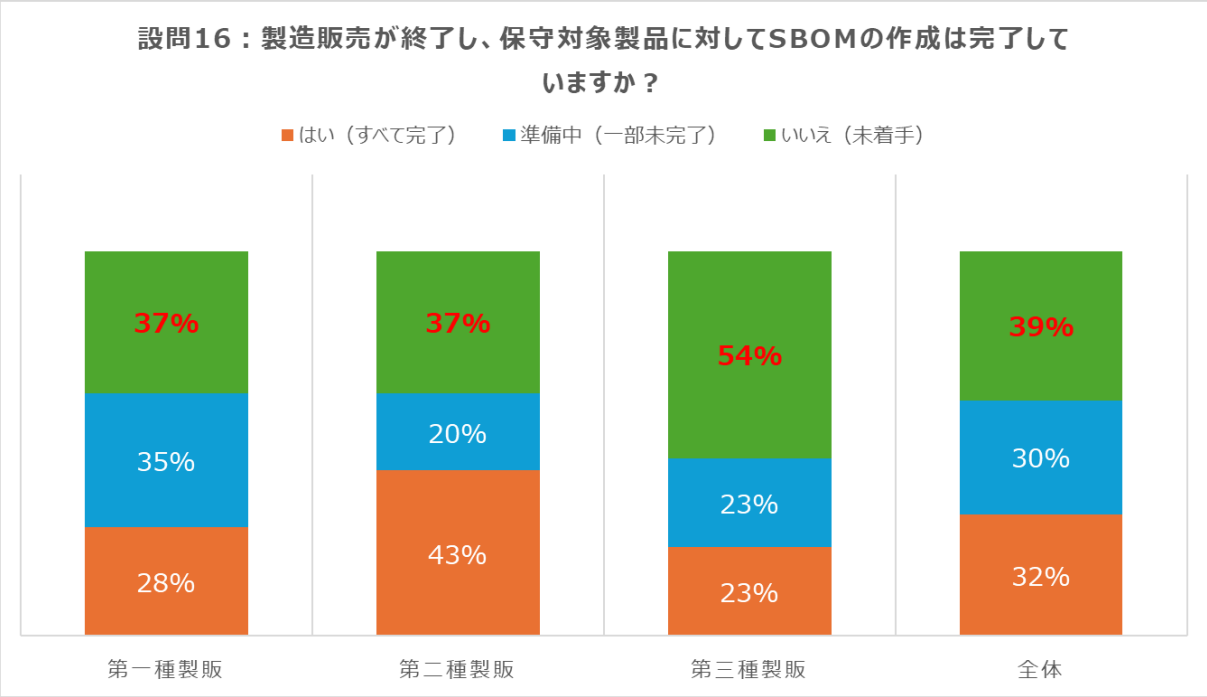
設問 15：製造販売中の製品に対して SBOM の作成は完了していますか？

選択肢	はい（すべて完了）	準備中（一部未完了）	いいえ（未着手）
第一種製販	78	60	14
第二種製販	41	19	5
第三種製販	11	11	4
全体	130	90	23



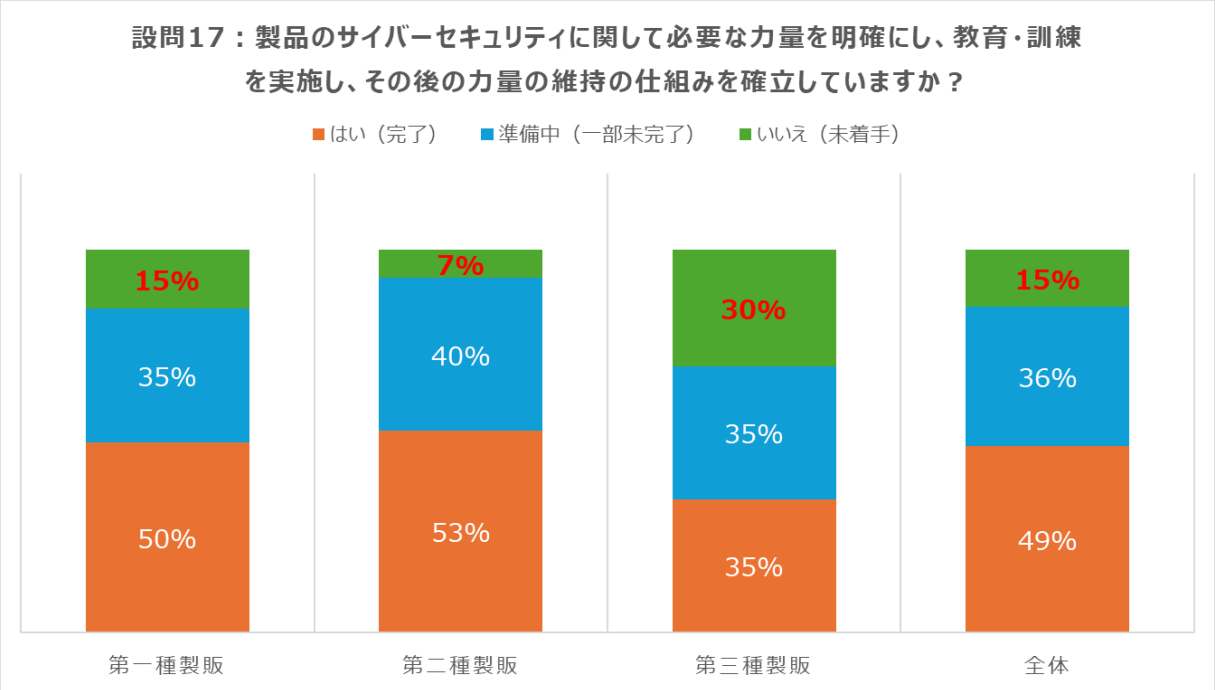
設問 16：製造販売が終了し、保守対象製品に対して SBOM の作成は完了していますか？

選択肢	はい（すべて完了）	準備中（一部未完了）	いいえ（未着手）
第一種製販	43	53	56
第二種製販	28	13	24
第三種製販	6	6	14
全体	77	72	94



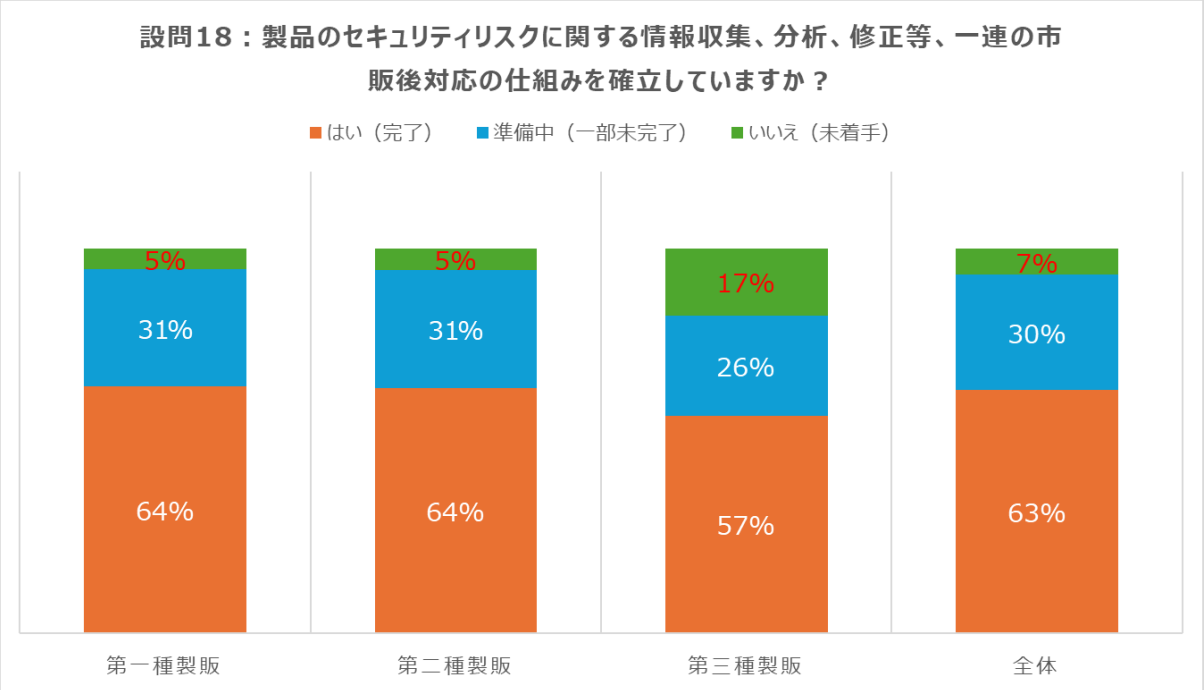
設問 17：製品のサイバーセキュリティに関して必要な力量を明確にし、教育・訓練を実施し、その後の力量の維持の仕組みを確立していますか？

選択肢	はい（完了）	準備中（一部未完了）	いいえ（未着手）
第一種製販	65	46	20
第二種製販	29	22	4
第三種製販	8	8	7
全体	102	76	31



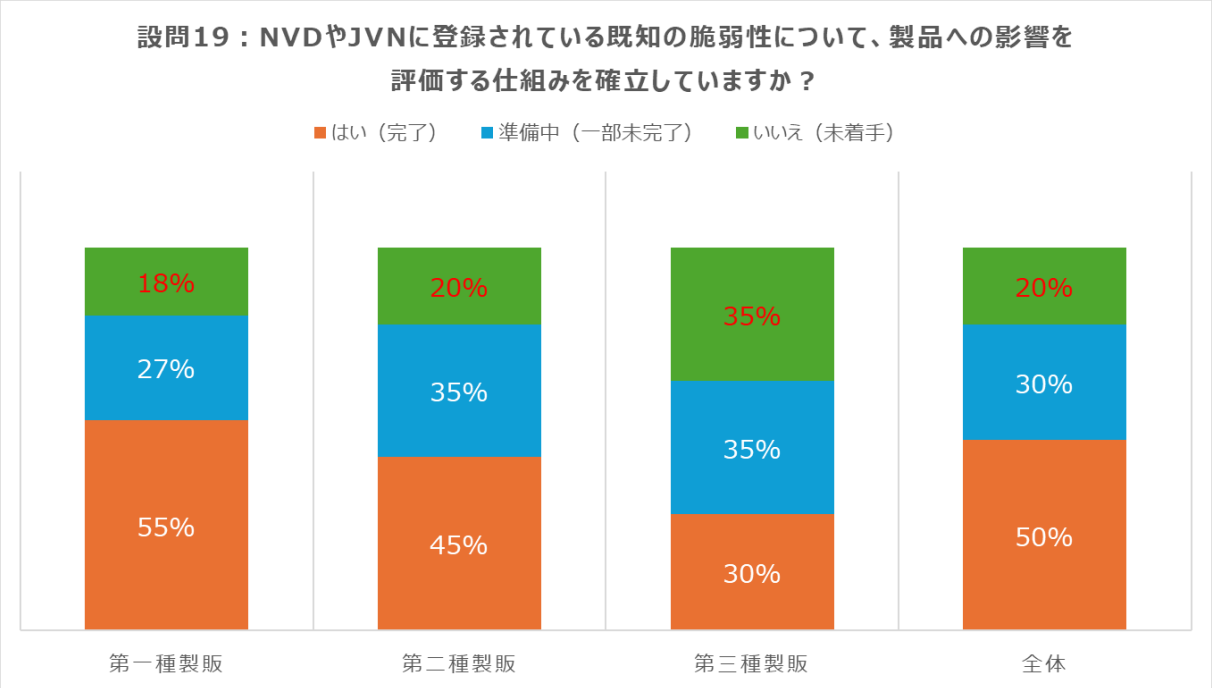
設問 18：製品のセキュリティリスクに関する情報収集、分析、修正等、一連の市販後対応の仕組みを確立していますか？

選択肢	はい（完了）	準備中（一部未完了）	いいえ（未着手）
第一種製販	84	40	7
第二種製販	35	17	3
第三種製販	13	6	4
全体	132	63	14



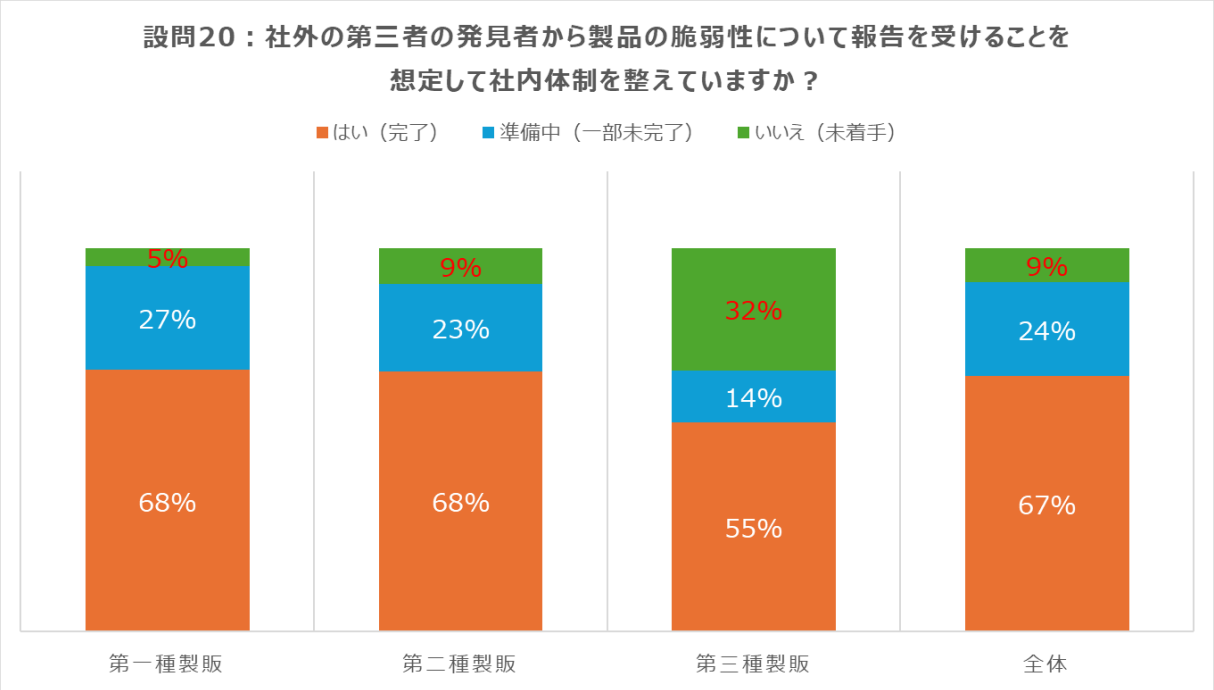
設問 19：NVD や JVN に登録されている既知の脆弱性について、製品への影響を評価する仕組みを確立していますか？

選択肢	はい（完了）	準備中（一部未完了）	いいえ（未着手）
第一種製販	72	36	23
第二種製販	25	19	11
第三種製販	7	8	8
全体	104	63	42



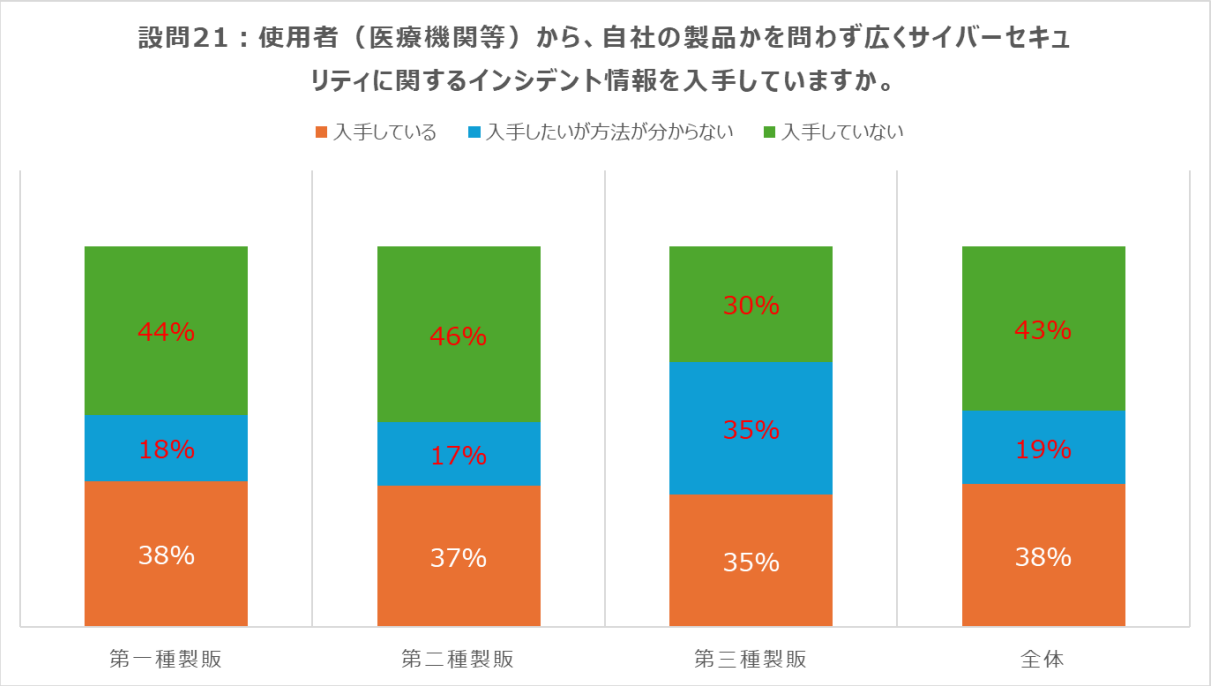
設問 20：社外の第三者の発見者から製品の脆弱性について報告を受けることを想定して社内体制を整えていますか？

選択肢	はい（完了）	準備中（一部未完了）	いいえ（未着手）
第一種製販	86	34	6
第二種製販	36	12	5
第三種製販	12	3	7
全体	134	49	18



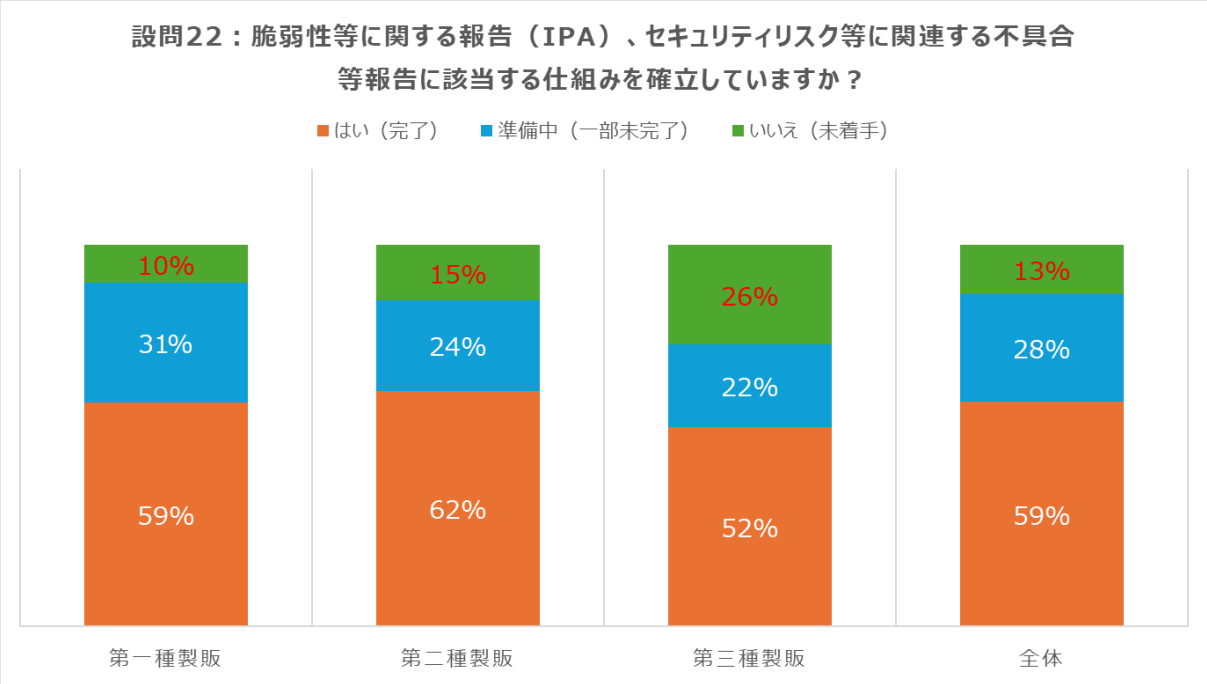
設問 21：使用者（医療機関等）から、自社の製品かを問わず広くサイバーセキュリティに関するインシデント情報を入手していますか。

選択肢	入手している	入手したいが方法が分からない	入手していない
第一種製販	50	23	58
第二種製販	20	9	25
第三種製販	8	8	7
全体	78	40	90



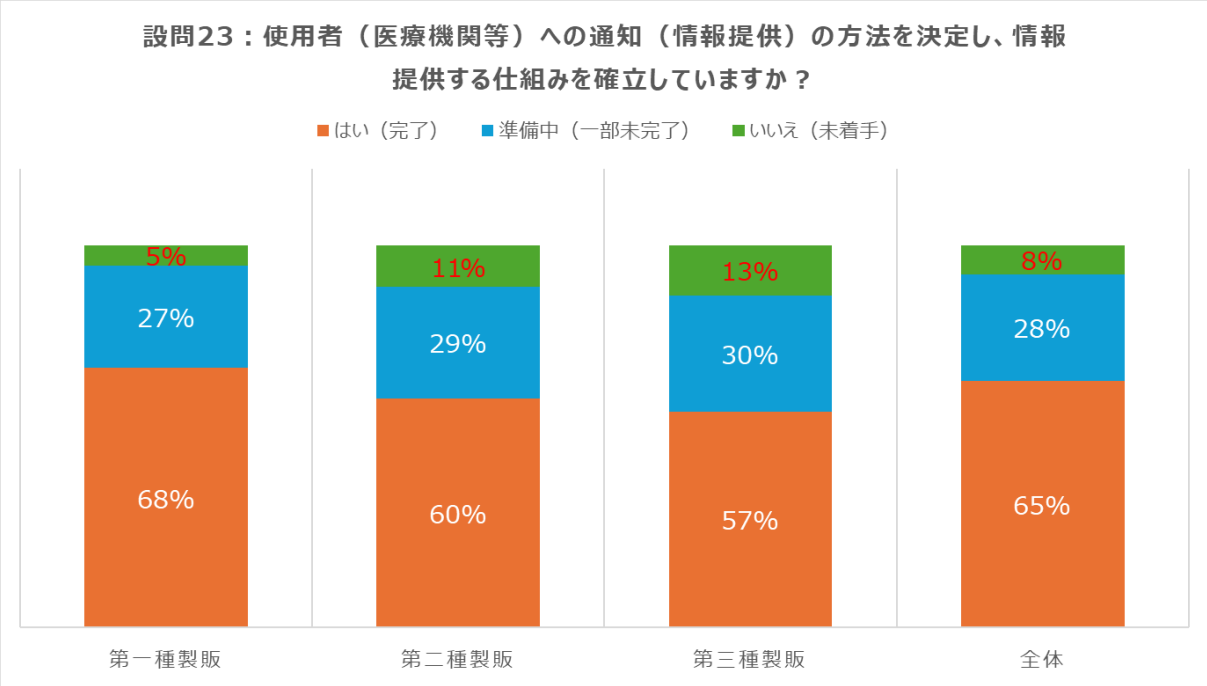
設問 22：脆弱性等に関する報告（IPA）、セキュリティリスク等に関連する不具合等報告に該当する仕組みを確立していますか？

選択肢	はい（完了）	準備中（一部未完了）	いいえ（未着手）
第一種製販	77	41	13
第二種製販	34	13	8
第三種製販	12	5	6
全体	123	59	27



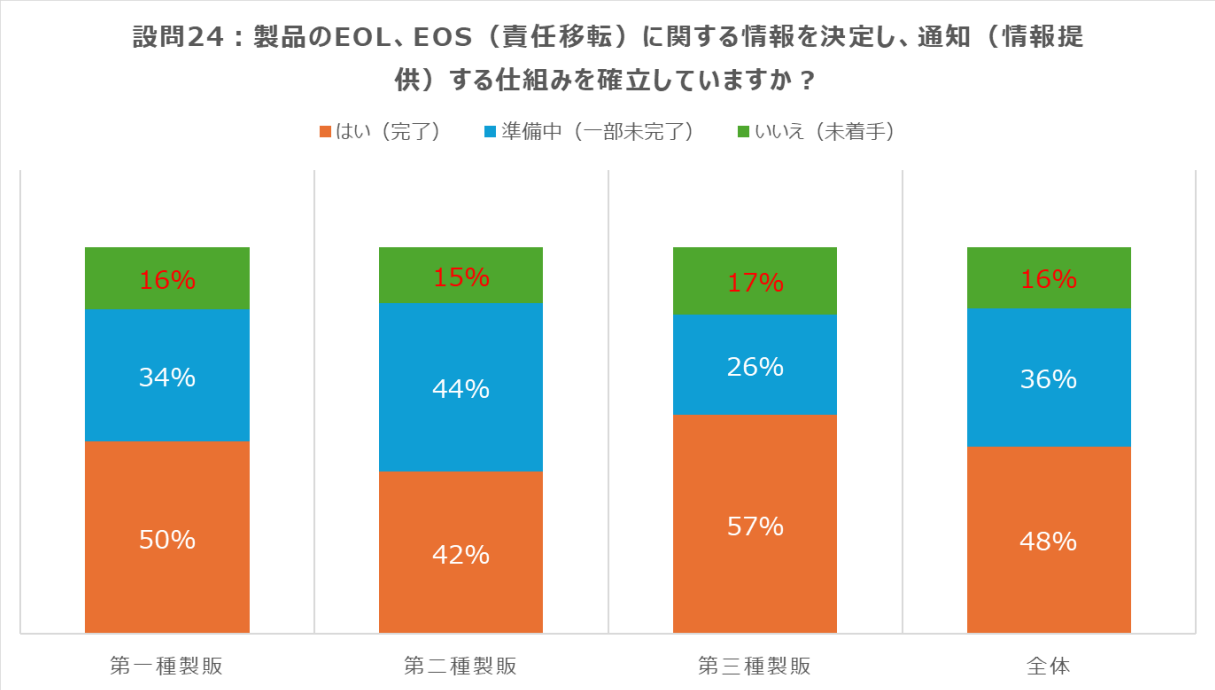
設問 23：使用者（医療機関等）への通知（情報提供）の方法を決定し、情報提供する仕組みを確立していますか？

選択肢	はい（完了）	準備中（一部未完了）	いいえ（未着手）
第一種製販	89	35	7
第二種製販	33	16	6
第三種製販	13	7	3
全体	135	58	16



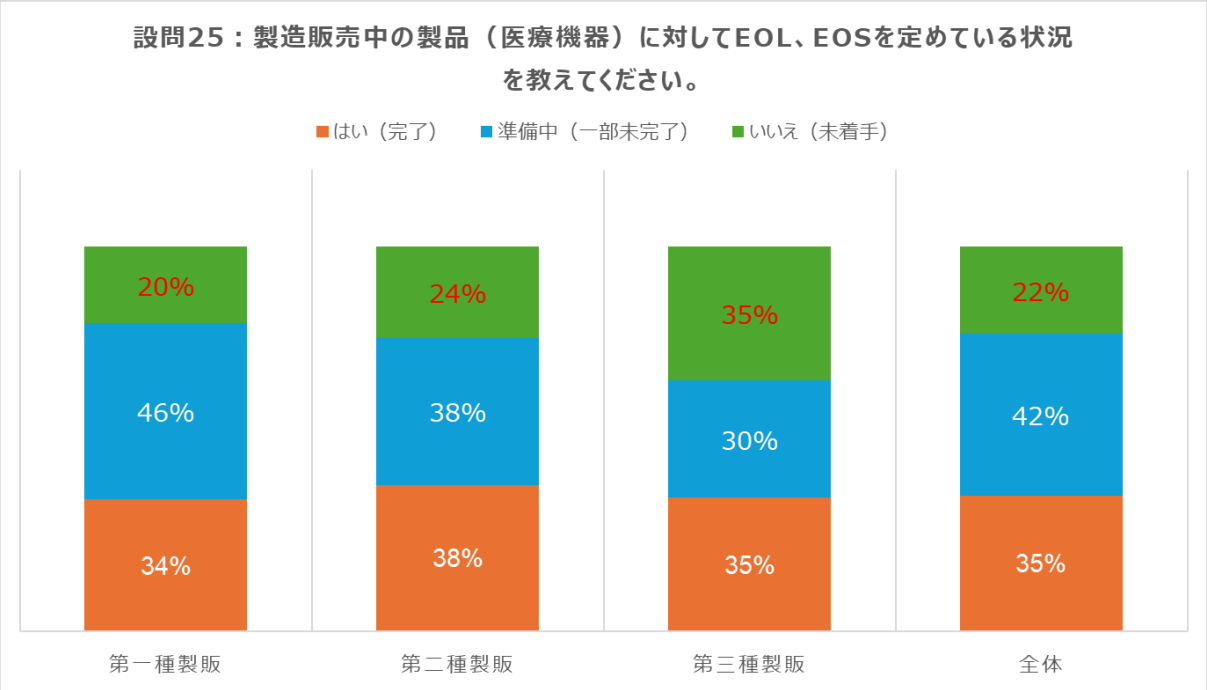
設問 24：製品の EOL、EOS（責任移転）に関する情報を決定し、通知（情報提供）する仕組みを確立していますか？

選択肢	はい（完了）	準備中（一部未完了）	いいえ（未着手）
第一種製販	65	45	21
第二種製販	23	24	8
第三種製販	13	6	4
全体	101	75	33



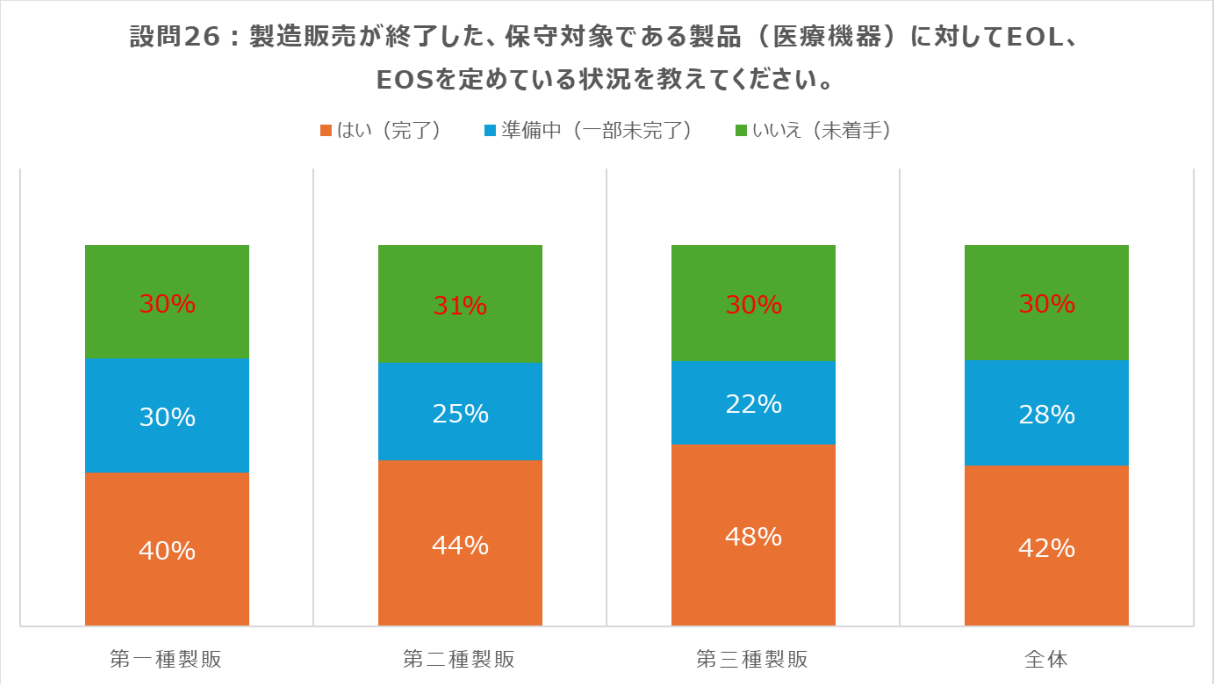
設問 25：製造販売中の製品（医療機器）に対して EOL、EOS を定めている状況を教えてください。

選択肢	はい（完了）	準備中（一部未完了）	いいえ（未着手）
第一種製販	45	60	26
第二種製販	21	21	13
第三種製販	8	7	8
全体	74	88	47



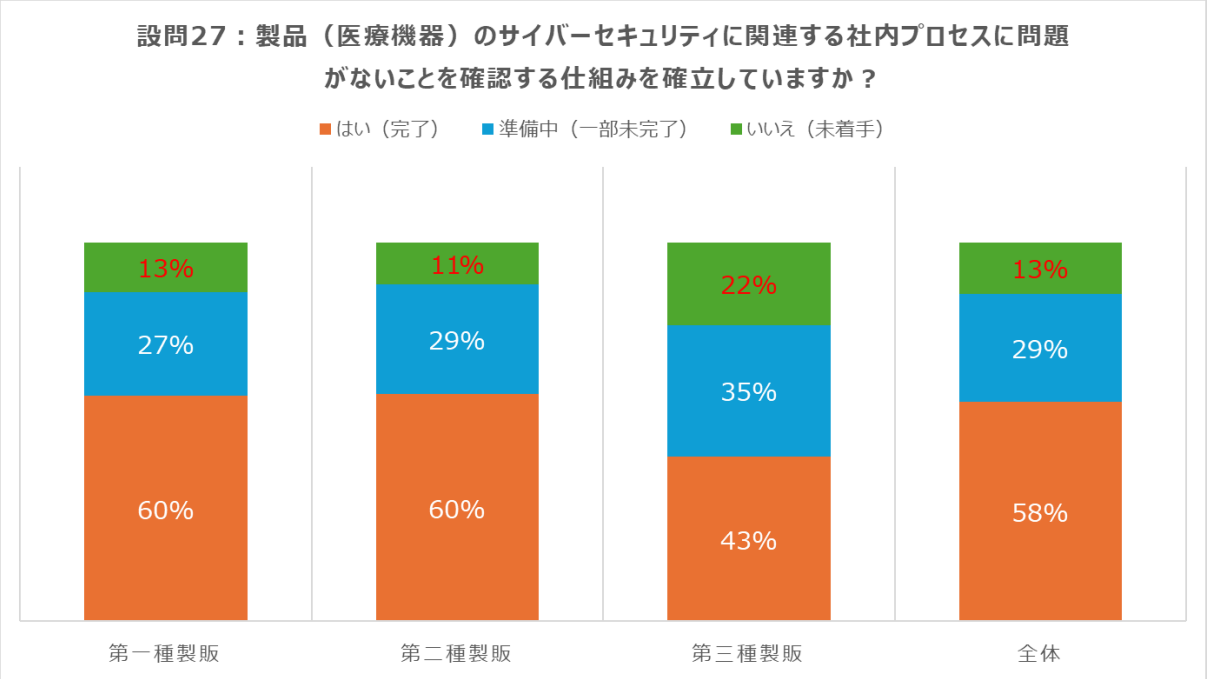
設問 26：製造販売が終了した、保守対象である製品（医療機器）に対して EOL、EOS を定めている状況を教えてください。

選択肢	はい（完了）	準備中（一部未完了）	いいえ（未着手）
第一種製販	53	39	39
第二種製販	24	14	17
第三種製販	11	5	7
全体	88	58	63



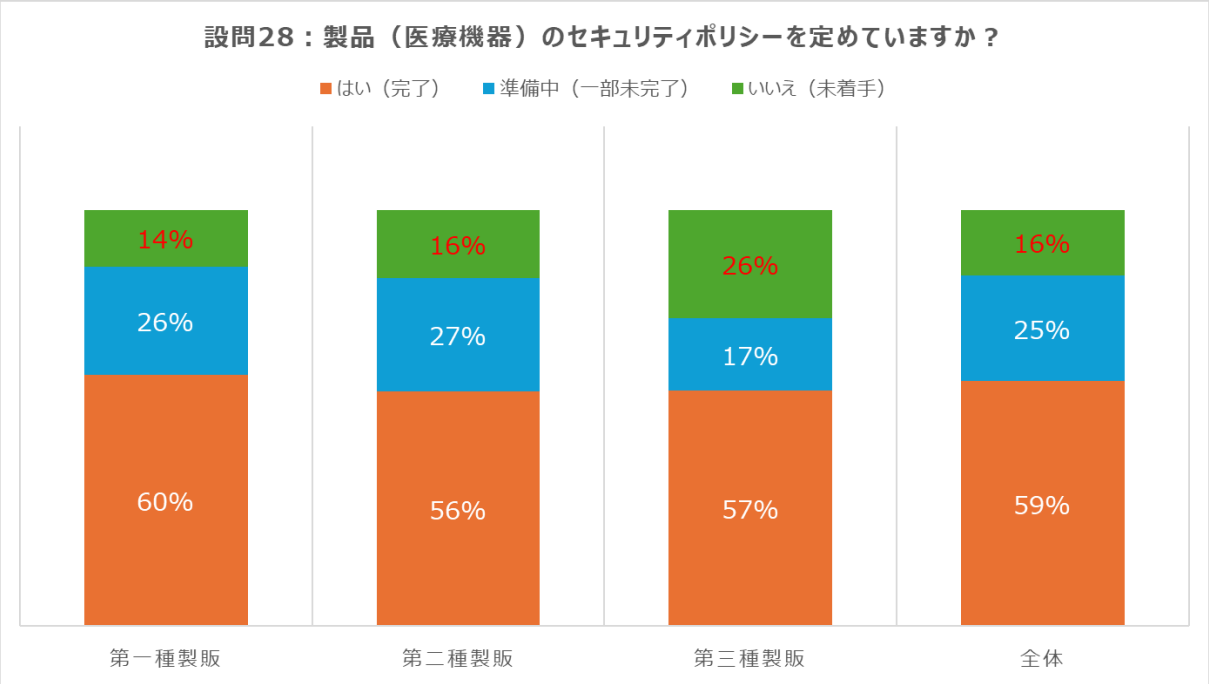
設問 27：製品（医療機器）のサイバーセキュリティに関連する社内プロセスに問題がないことを確認する仕組みを確立していますか？

選択肢	はい（完了）	準備中（一部未完了）	いいえ（未着手）
第一種製販	78	36	17
第二種製販	33	16	6
第三種製販	10	8	5
全体	121	60	28



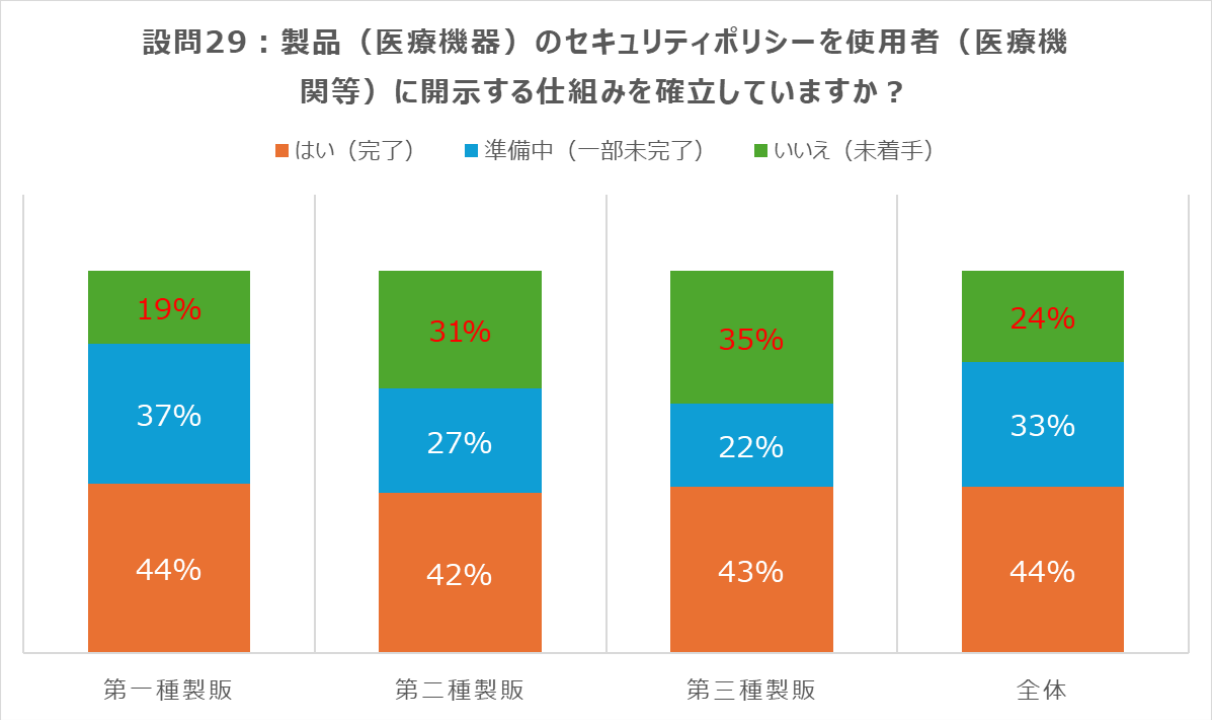
設問 28：製品（医療機器）のセキュリティポリシーを定めていますか？

選択肢	はい（完了）	準備中（一部未完了）	いいえ（未着手）
第一種製販	79	34	18
第二種製販	31	15	9
第三種製販	13	4	6
全体	123	53	33



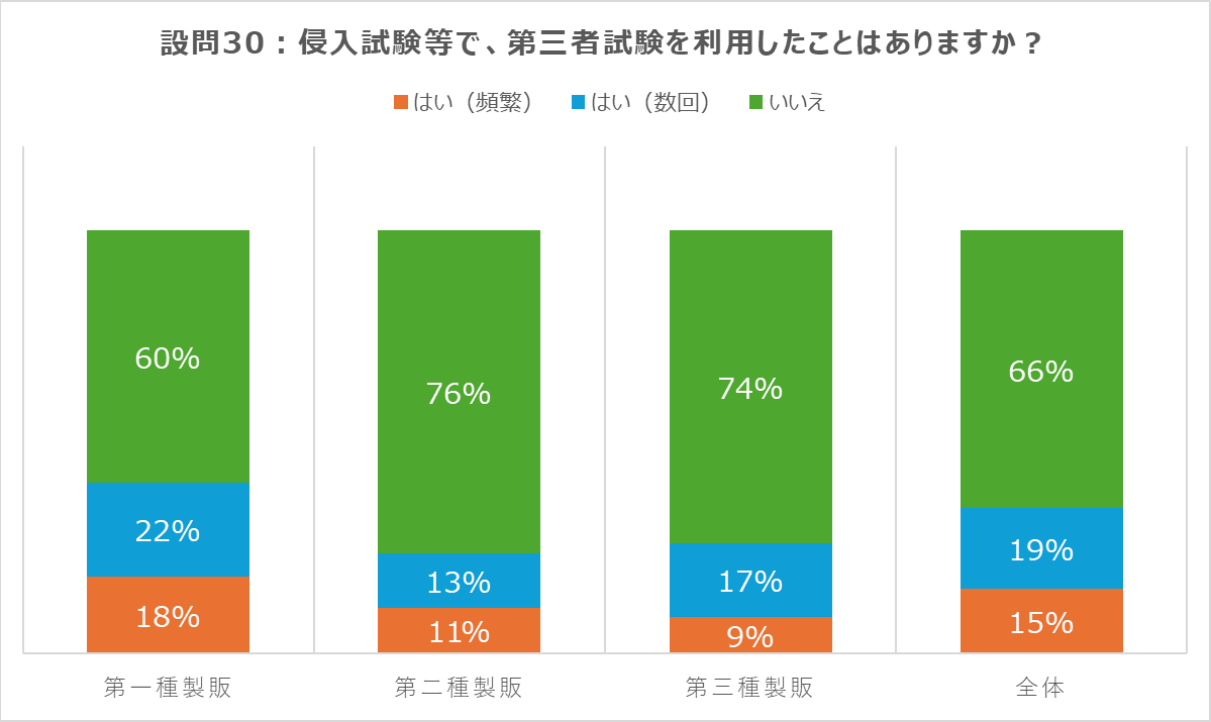
設問 29：製品（医療機器）のセキュリティポリシーを使用者（医療機関等）に開示する仕組みを確立していますか？

選択肢	はい（完了）	準備中（一部未完了）	いいえ（未着手）
第一種製販	58	48	25
第二種製販	23	15	17
第三種製販	10	5	8
全体	91	68	50



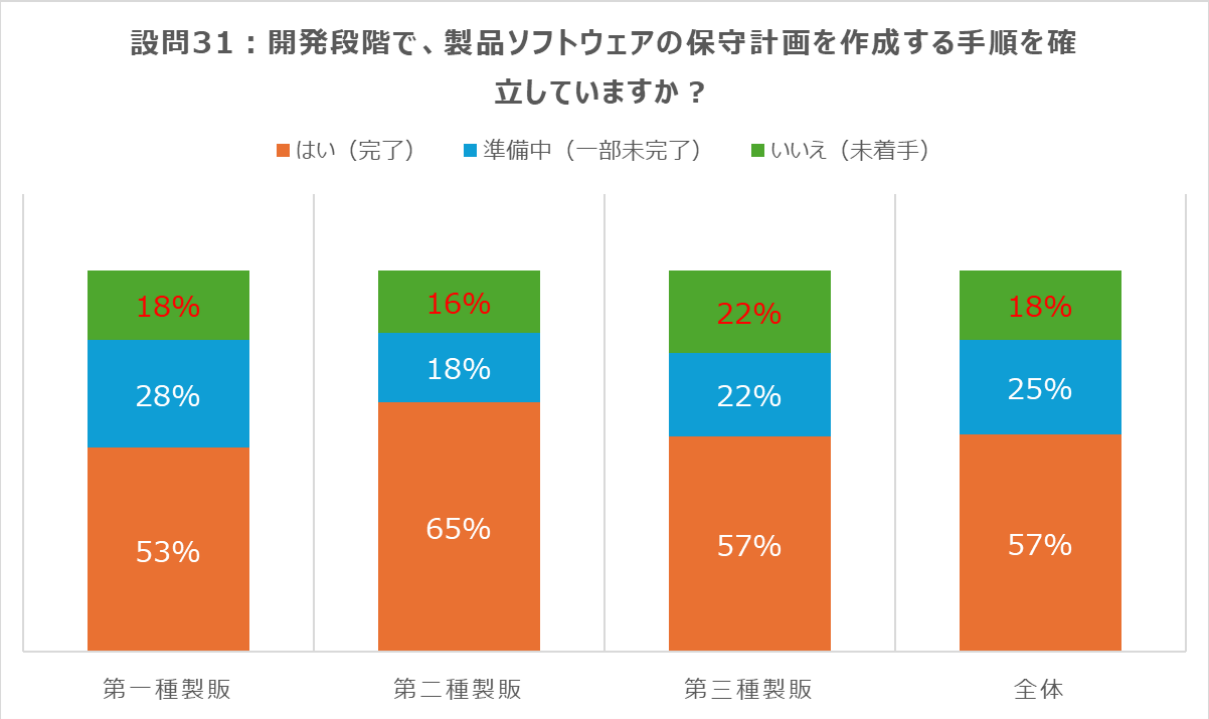
設問 30：侵入試験等で、第三者試験を利用したことはありますか？

選択肢	はい（頻繁）	はい（数回）	いいえ
第一種製販	24	29	78
第二種製販	6	7	42
第三種製販	2	4	17
全体	32	40	137



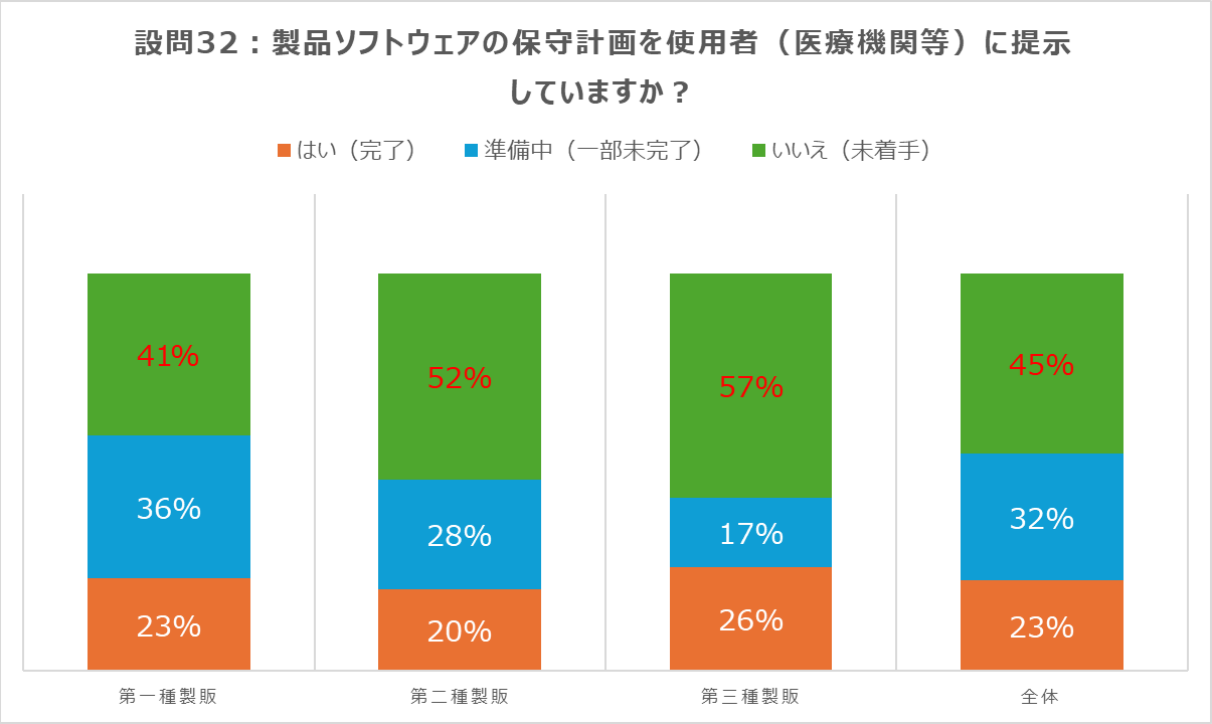
設問 31：開発段階で、製品ソフトウェアの保守計画を作成する手順を確立していますか？

選択肢	はい（完了）	準備中（一部未完了）	いいえ（未着手）
第一種製販	70	37	24
第二種製販	36	10	9
第三種製販	13	5	5
全体	119	52	38



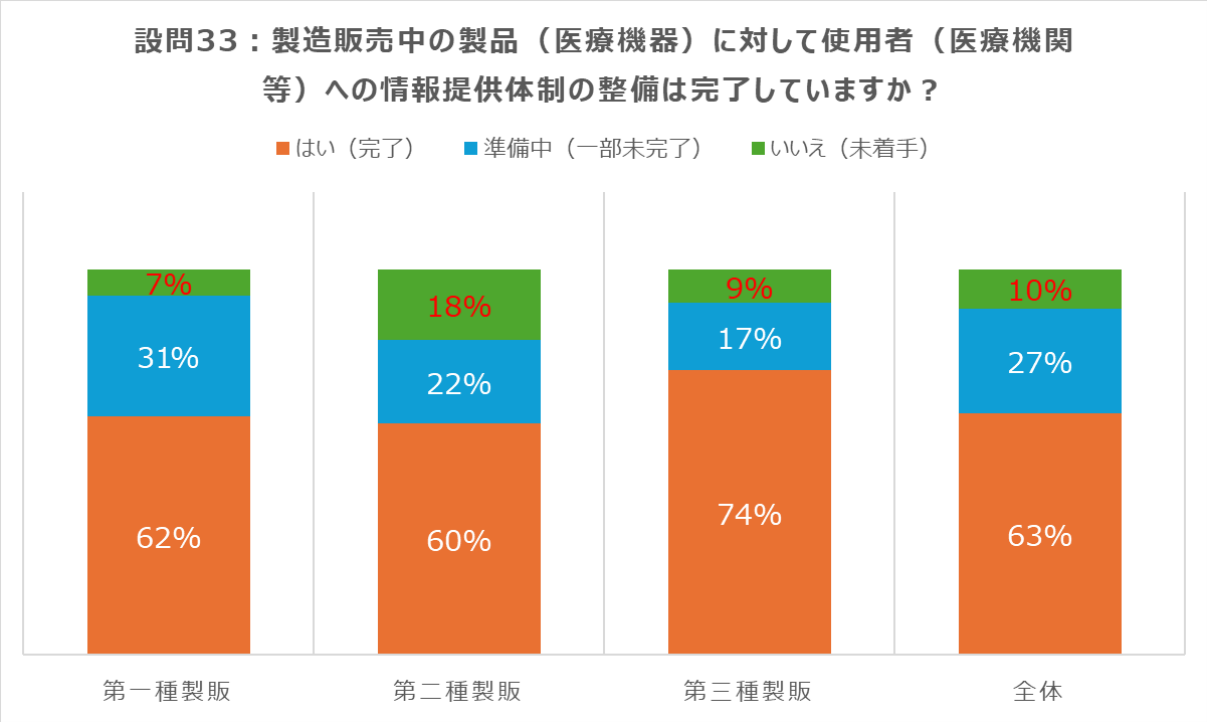
設問 32：製品ソフトウェアの保守計画を使用者（医療機関等）に提示していますか？

選択肢	はい（完了）	準備中（一部未完了）	いいえ（未着手）
第一種製販	30	47	53
第二種製販	11	15	28
第三種製販	6	4	13
全体	47	66	94



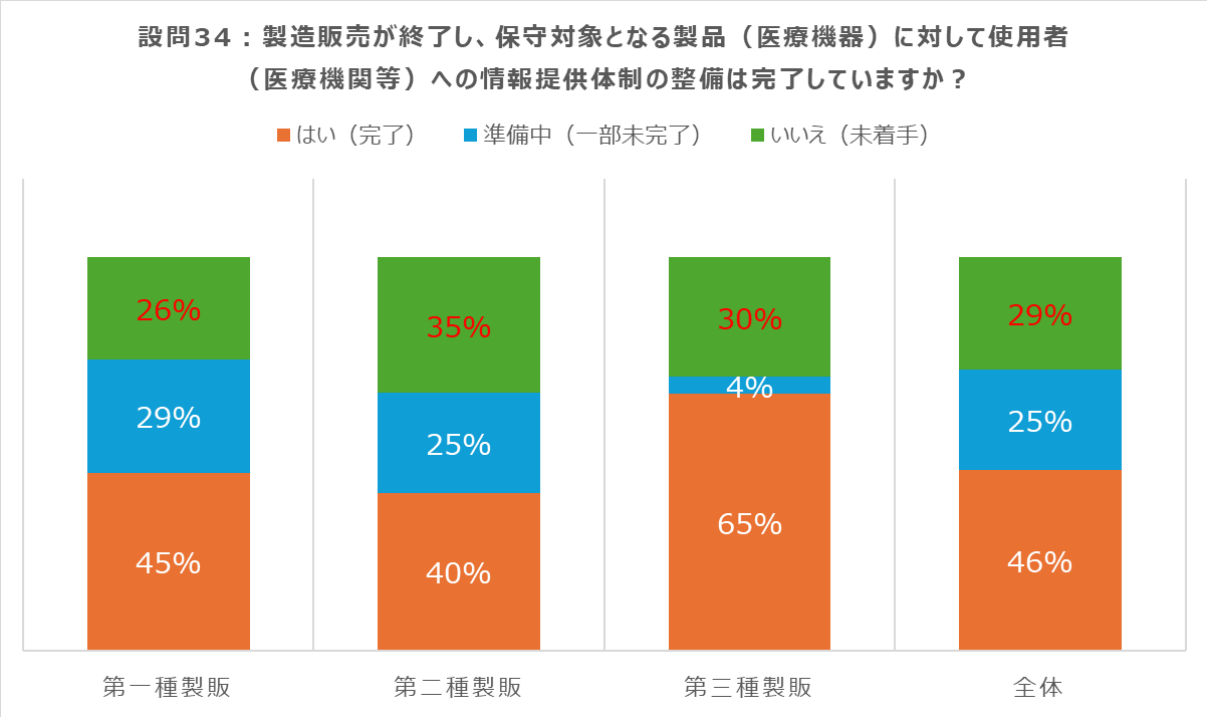
設問 33：製造販売中の製品（医療機器）に対して使用者（医療機関等）への情報提供体制の整備は完了していますか？

選択肢	はい（完了）	準備中（一部未完了）	いいえ（未着手）
第一種製販	81	41	9
第二種製販	33	12	10
第三種製販	17	4	2
全体	131	57	21



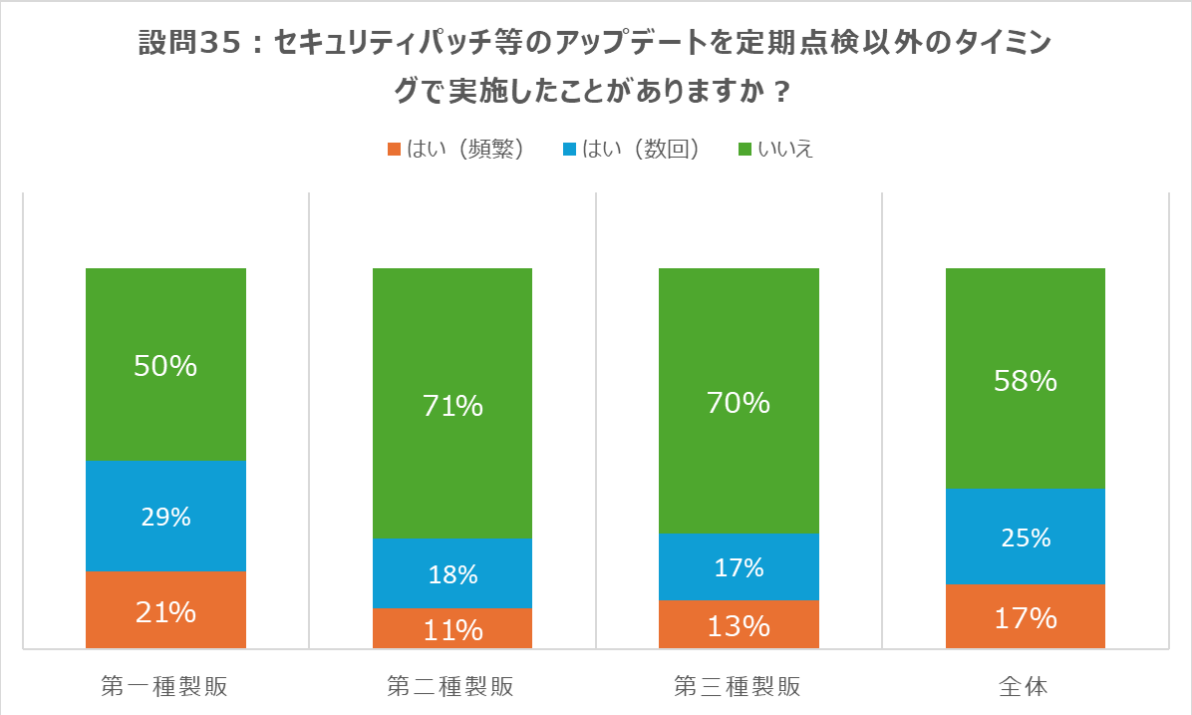
設問 34：製造販売が終了し、保守対象となる製品（医療機器）に対して使用者（医療機関等）への情報提供体制の整備は完了していますか？

選択肢	はい（完了）	準備中（一部未完了）	いいえ（未着手）
第一種製販	59	38	34
第二種製販	22	14	19
第三種製販	15	1	7
全体	96	53	60



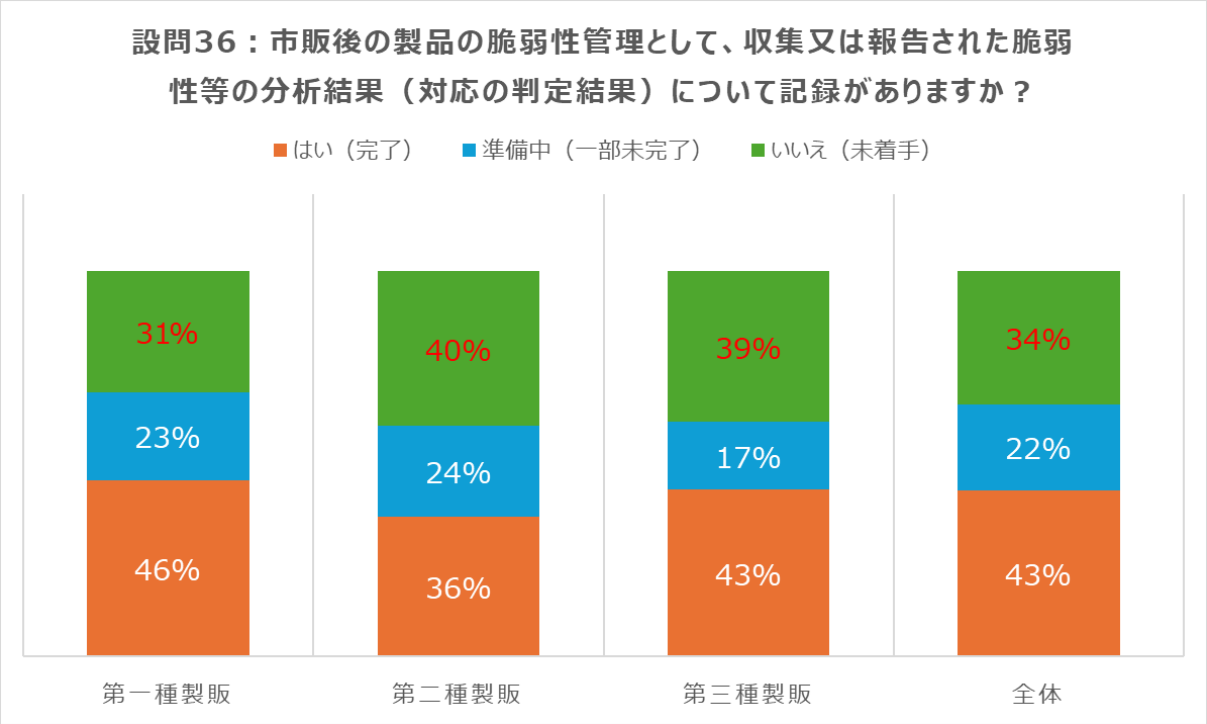
設問 35：セキュリティパッチ等のアップデートを定期点検以外のタイミングで実施したことがありますか？

選択肢	はい（頻繁）	はい（数回）	いいえ
第一種製販	27	38	66
第二種製販	6	10	39
第三種製販	3	4	16
全体	36	52	121



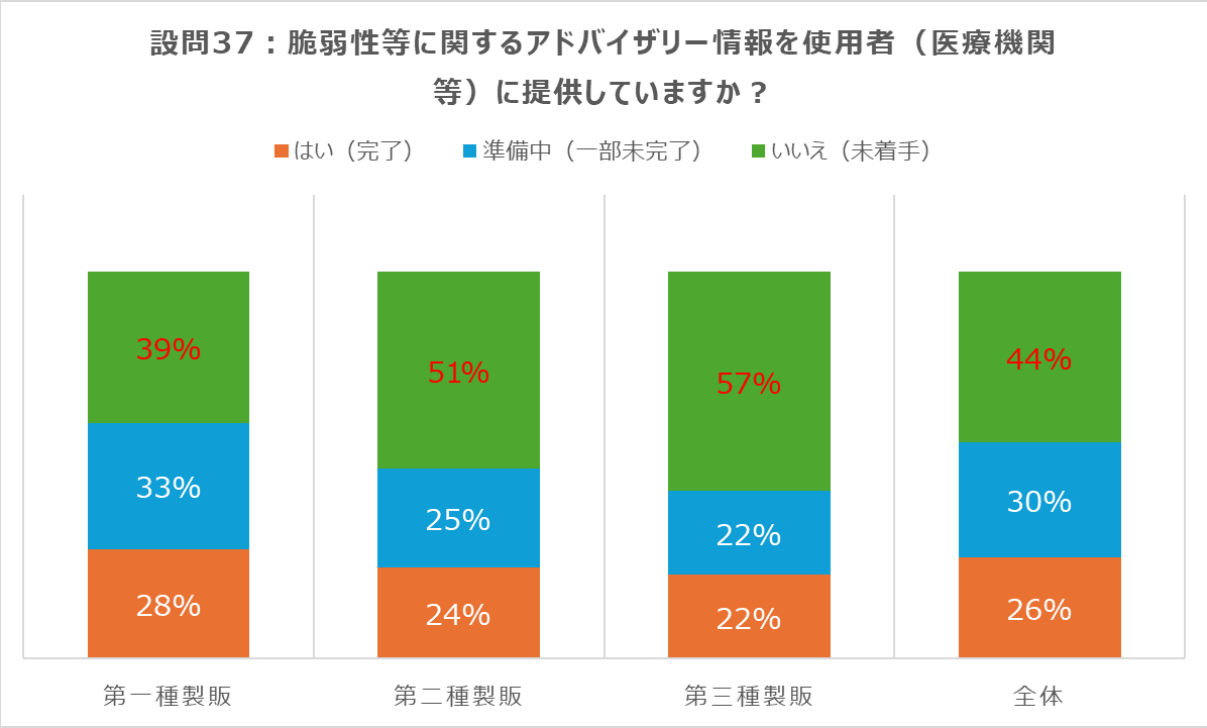
設問 36：市販後の製品の脆弱性管理として、収集又は報告された脆弱性等の分析結果（対応の判定結果）について記録がありますか？

選択肢	はい（完了）	準備中（一部未完了）	いいえ（未着手）
第一種製販	60	30	41
第二種製販	20	13	22
第三種製販	10	4	9
全体	90	47	72



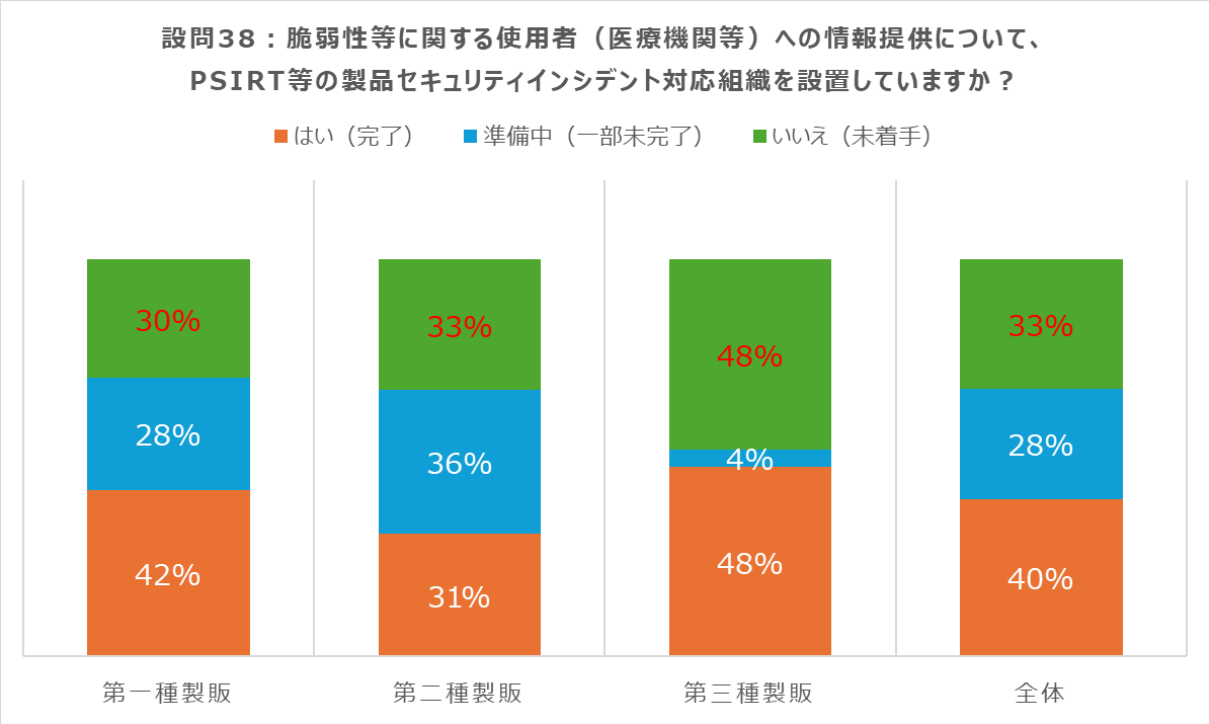
設問 37：脆弱性等に関するアドバイザリー情報を使用者（医療機関等）に提供していますか？

選択肢	はい（完了）	準備中（一部未完了）	いいえ（未着手）
第一種製販	37	43	51
第二種製販	13	14	28
第三種製販	5	5	13
全体	55	62	92



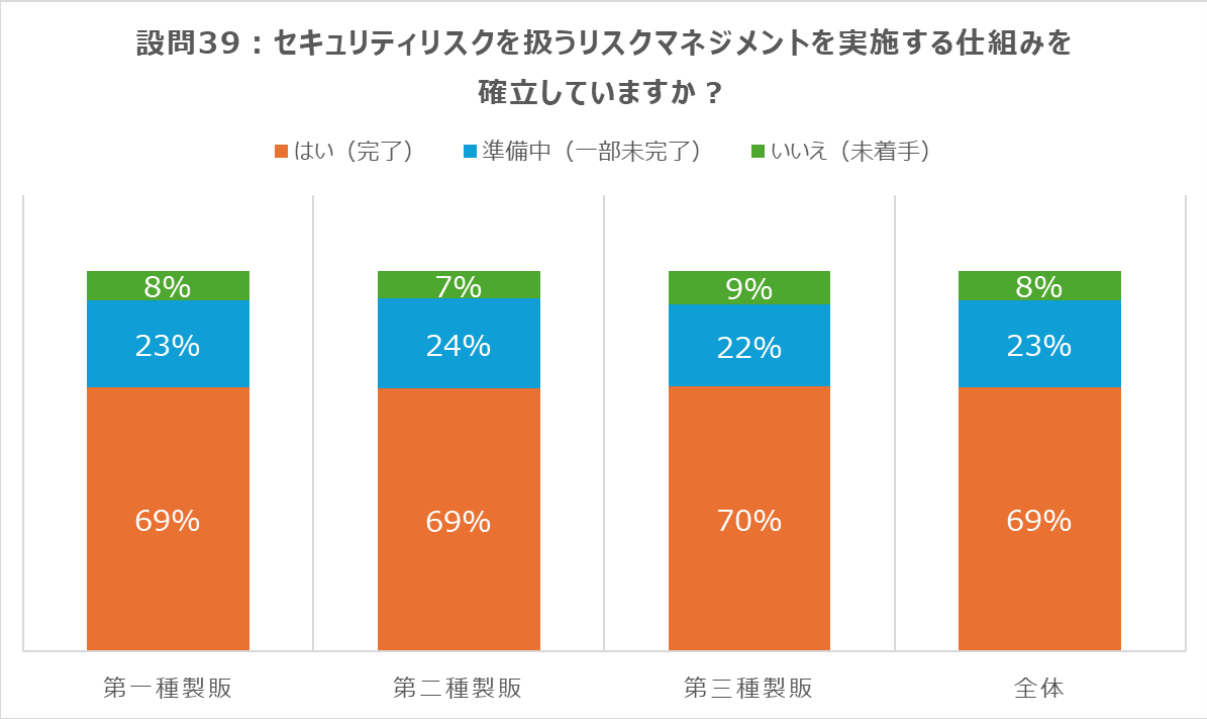
設問 38：脆弱性等に関する使用者（医療機関等）への情報提供について、PSIRT 等の製品セキュリティインシデント対応組織を設置していますか？

選択肢	はい（完了）	準備中（一部未完了）	いいえ（未着手）
第一種製販	55	37	39
第二種製販	17	20	18
第三種製販	11	1	11
全体	83	58	68



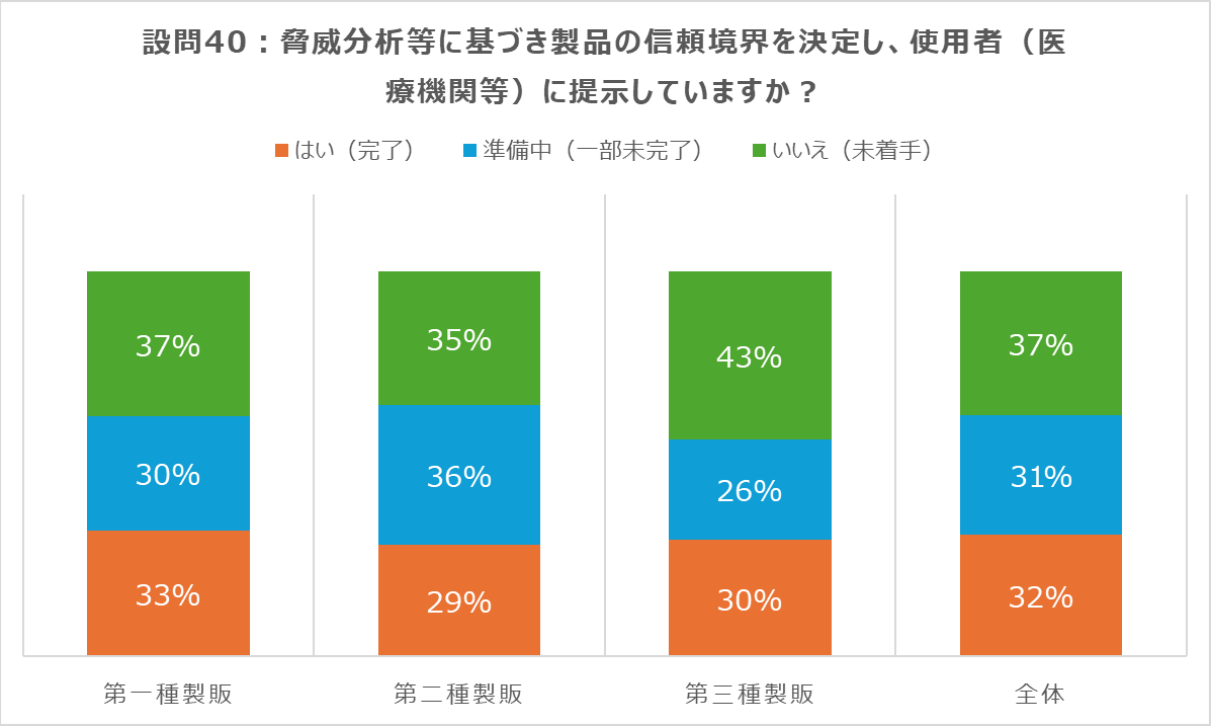
設問 39：セキュリティリスクを扱うリスクマネジメントを実施する仕組みを確立していますか？

選択肢	はい（完了）	準備中（一部未完了）	いいえ（未着手）
第一種製販	91	30	10
第二種製販	38	13	4
第三種製販	16	5	2
全体	145	48	16



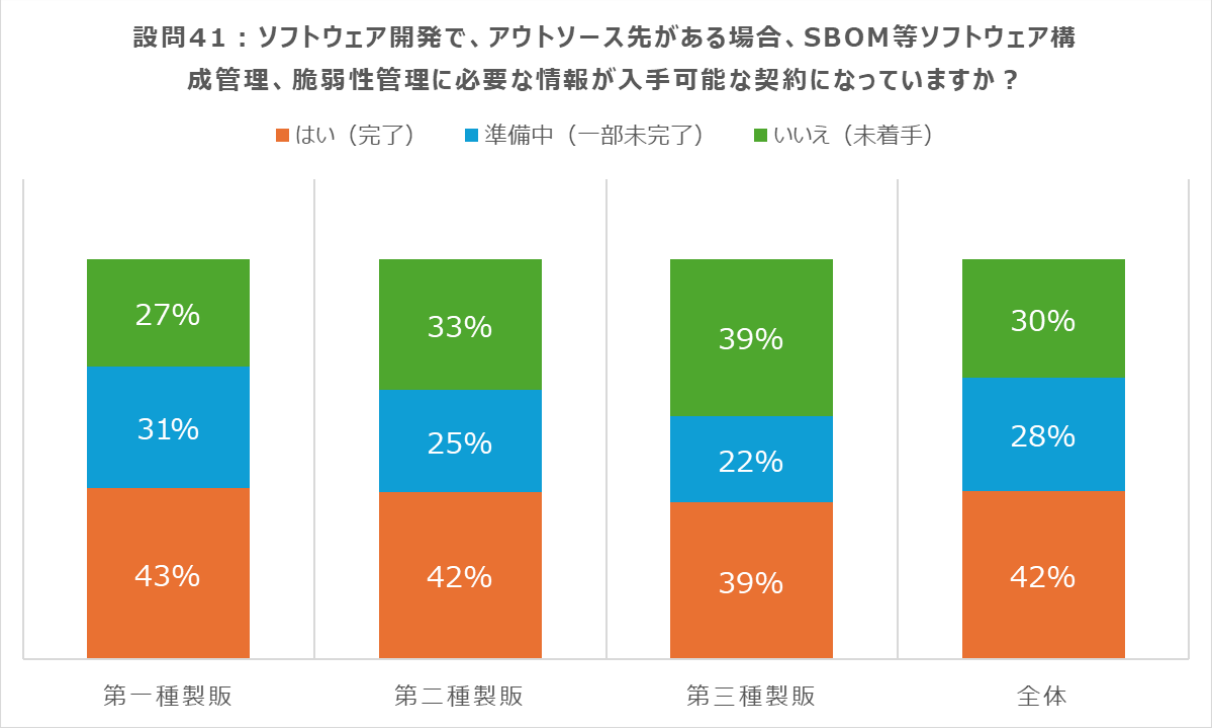
設問 40：脅威分析等に基づき製品の信頼境界を決定し、使用者（医療機関等）に提示していますか？

選択肢	はい（完了）	準備中（一部未完了）	いいえ（未着手）
第一種製販	43	39	49
第二種製販	16	20	19
第三種製販	7	6	10
全体	66	65	78



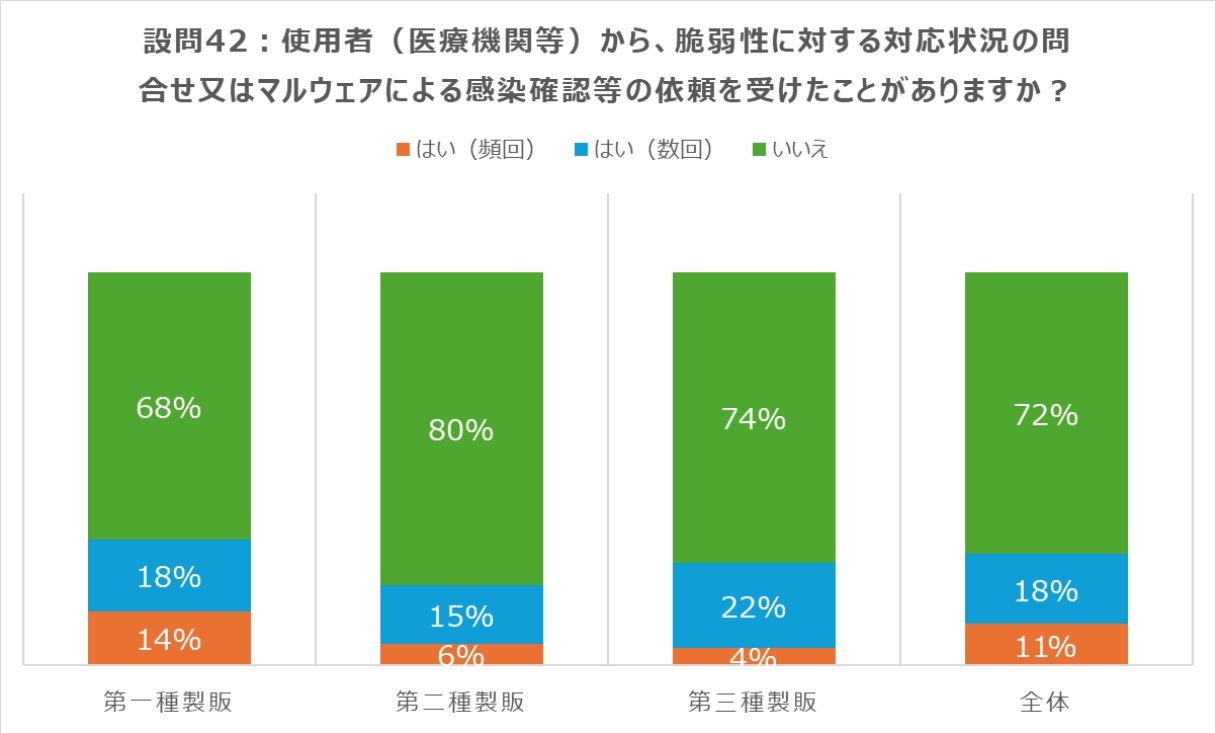
設問 41：製品のソフトウェア開発では、ソフトウェア構成管理等を含む JIS T 2304 を適用した上で、サイバーリスクを扱うために必要なアクティビティを実施することが求められています。ソフトウェア開発で、アウトソース先がある場合、SBOM 等ソフトウェア構成管理、脆弱性管理に必要な情報が入手可能な契約になっていますか？

選択肢	はい（完了）	準備中（一部未完了）	いいえ（未着手）
第一種製販	56	40	35
第二種製販	23	14	18
第三種製販	9	5	9
全体	88	59	62



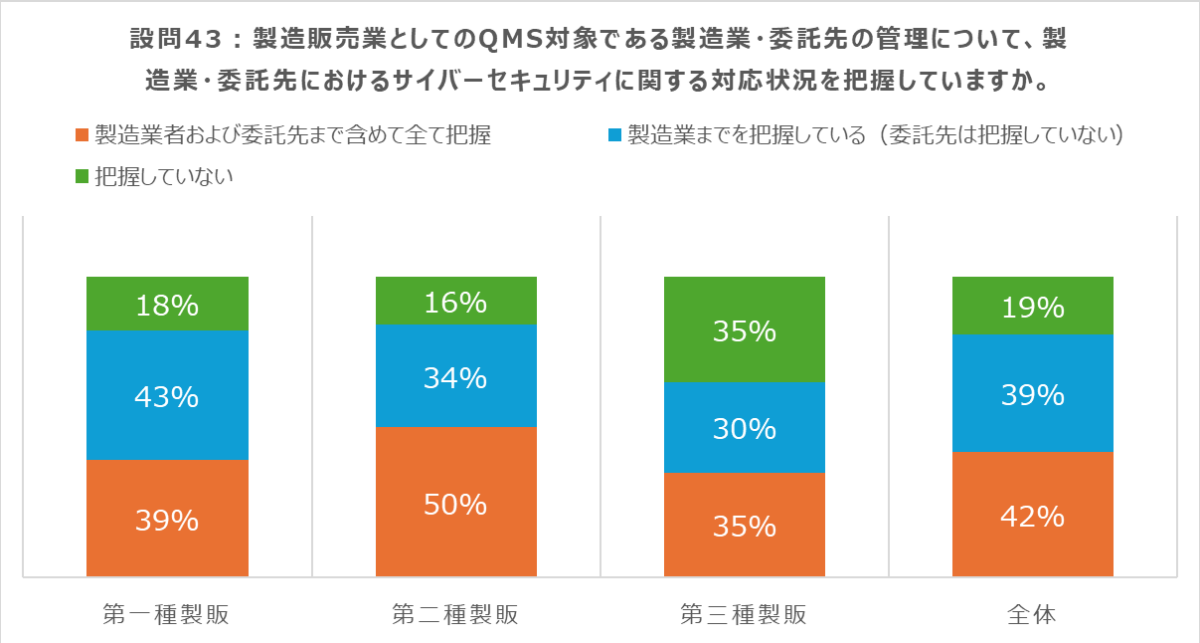
設問 42：使用者（医療機関等）から、脆弱性に対する対応状況の問合せ又はマルウェアによる感染確認等の依頼を受けたことがありますか？

選択肢	はい（頻回）	はい（数回）	いいえ
第一種製販	18	24	89
第二種製販	3	8	43
第三種製販	1	5	17
全体	22	37	149



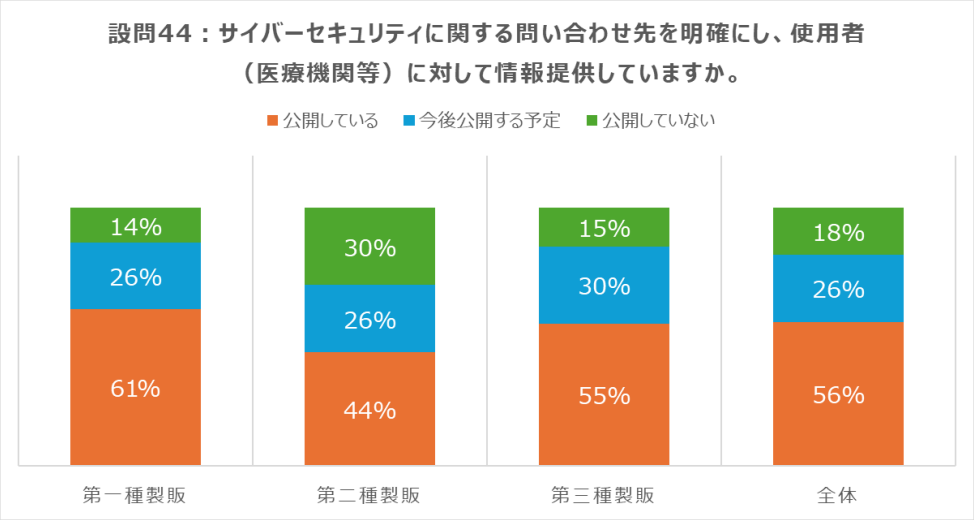
設問 43：製造販売業としての QMS 対象である製造業・委託先の管理について、製造業・委託先におけるサイバーセキュリティに関する対応状況を把握していますか。

選択肢	製造業者および委託先まで含めて全て把握	製造業までを把握している（委託先は把握していない）	把握していない
第一種製販	46	50	21
第二種製販	25	17	8
第三種製販	7	6	7
全体	78	73	36



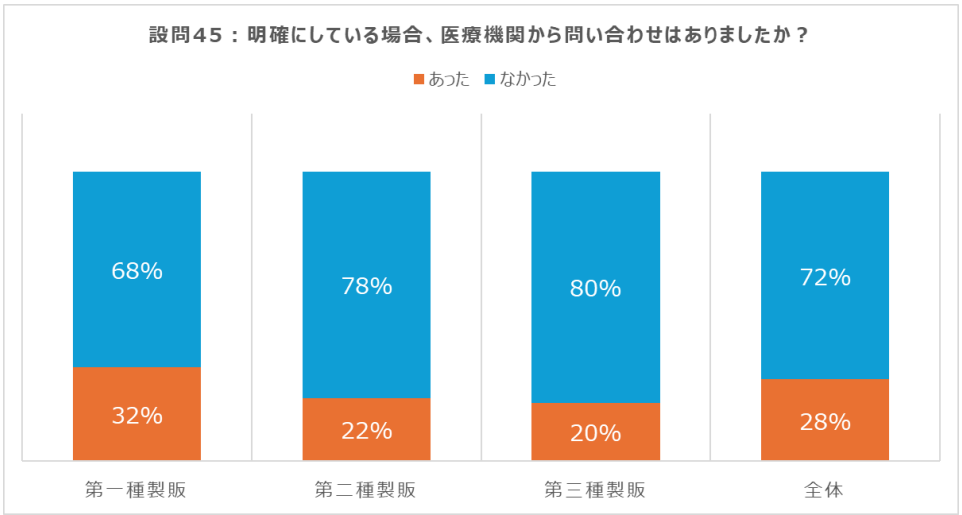
設問 44：サイバーセキュリティに関する問い合わせ先を明確にし、使用者（医療機関等）に対して情報提供していますか。

選択肢	公開している	今後公開する予定	公開していない
第一種製販	71	30	16
第二種製販	22	13	15
第三種製販	11	6	3
全体	104	49	34



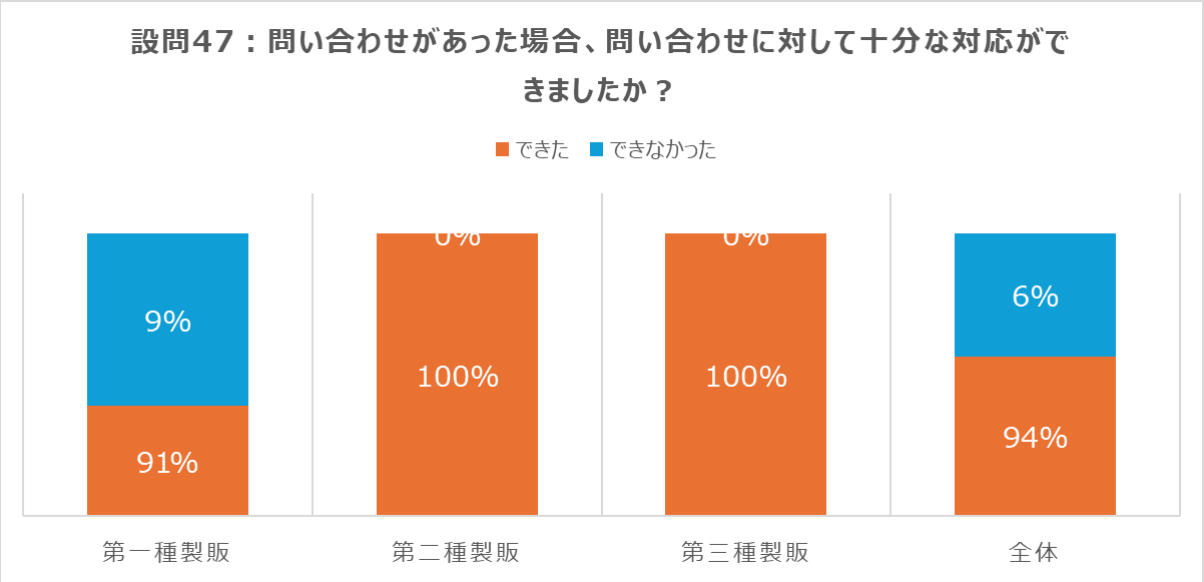
設問 45：明確にしている場合、医療機関から問い合わせはありましたか？

選択肢	あった	なかった
第一種製販	35	73
第二種製販	10	36
第三種製販	4	16
全体	49	125



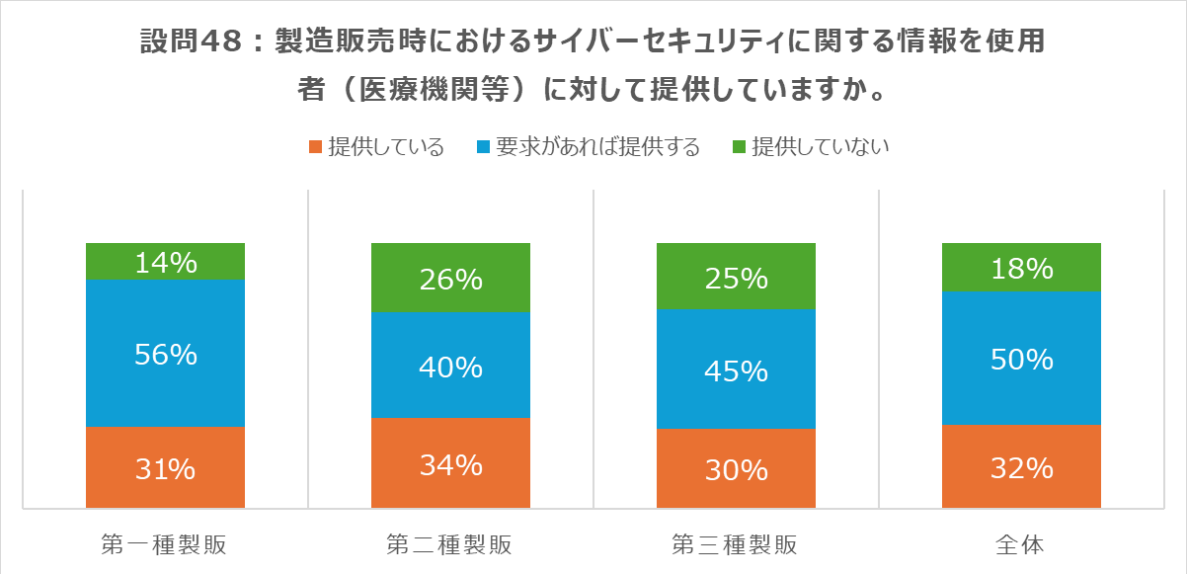
設問 47：問い合わせがあった場合、問い合わせに対して十分な対応ができましたか？

選択肢	できた	できなかった
第一種製販	32	3
第二種製販	10	0
第三種製販	4	0
全体	46	3



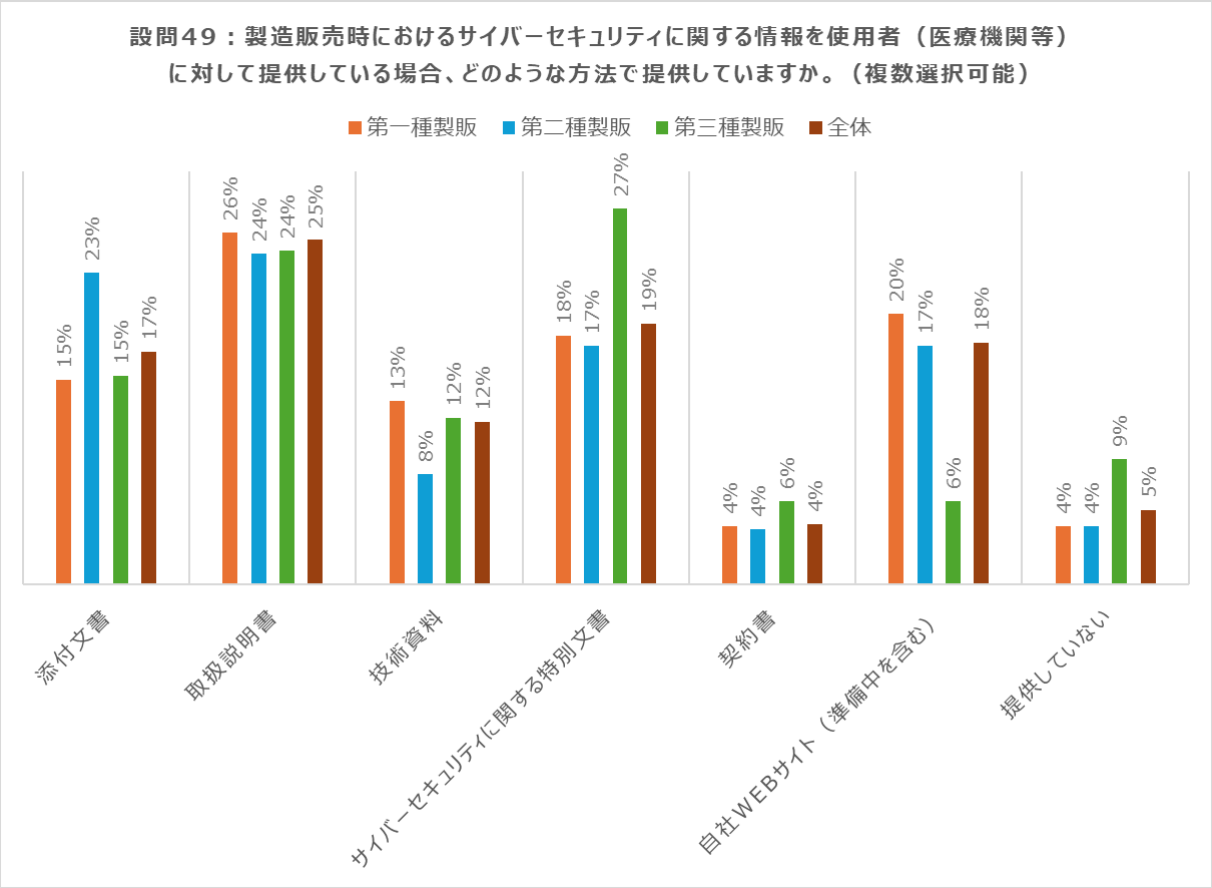
設問 48：製造販売時におけるサイバーセキュリティに関する情報を使用者（医療機関等）に対して提供していますか。

選択肢	提供している	要求があれば提供する	提供していない
第一種製販	36	65	16
第二種製販	17	20	13
第三種製販	6	9	5
全体	59	94	34



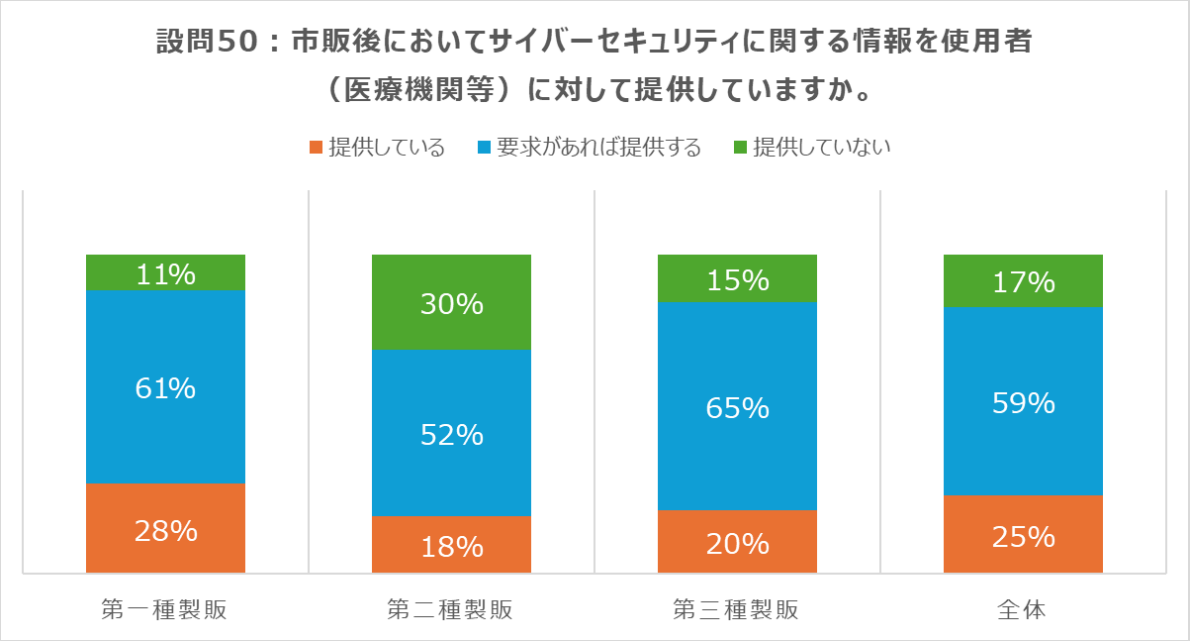
設問 49：製造販売時におけるサイバーセキュリティに関する情報を使用者（医療機関等）に対して提供している場合、どのような方法で提供していますか。（複数選択可能）

選択肢	第一種製販	第二種製販	第三種製販	全体
添付文書	28	17	5	50
取扱説明書	48	18	8	74
技術資料	25	6	4	35
サイバーセキュリティに関する特別文書	34	13	9	56
契約書	8	3	2	13
自社 WEB サイト（準備中を含む）	37	13	2	52
提供していない	8	5	3	16



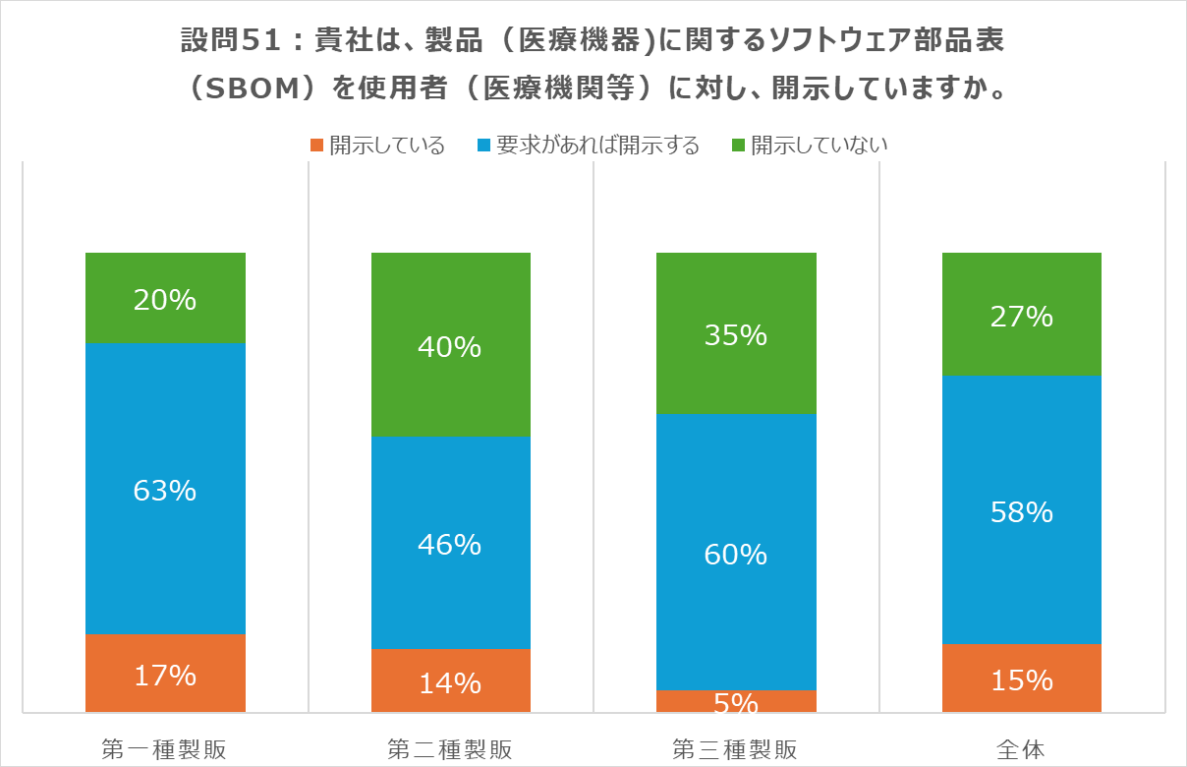
設問 50：市販後においてサイバーセキュリティに関する情報を使用者（医療機関等）に対して提供していますか。

選択肢	提供している	要求があれば提供する	提供していない
第一種製販	33	71	13
第二種製販	9	26	15
第三種製販	4	13	3
全体	46	110	31



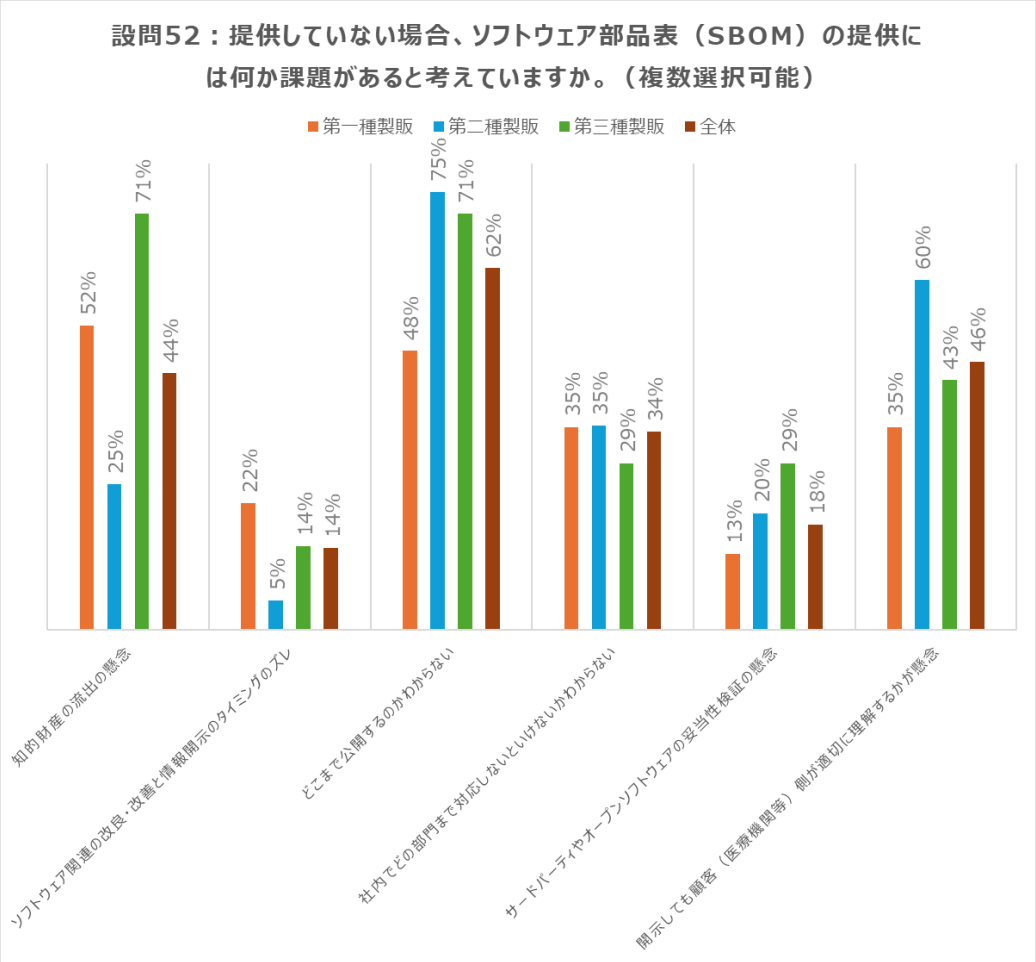
設問 51：貴社は、製品（医療機器)に関するソフトウェア部品表（SBOM）を使用者（医療機関等）に対し、開示していますか。

選択肢	開示している	要求があれば開示する	開示していない
第一種製販	20	74	23
第二種製販	7	23	20
第三種製販	1	12	7
全体	28	109	50



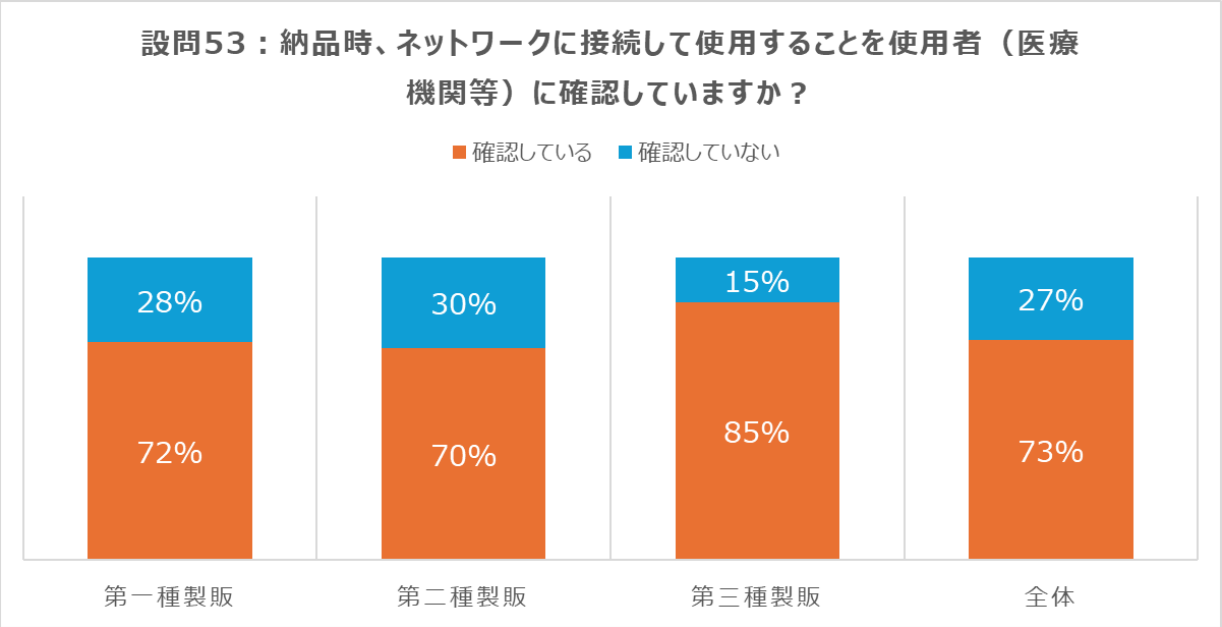
設問 52：提供していない場合、ソフトウェア部品表（SBOM）の提供には何か課題があると考えていますか。（複数選択可能）

選択肢	第一種製販	第二種製販	第三種製販	全体
知的財産の流出の懸念 （提供先からの情報漏洩）	12	5	5	22
ソフトウェア関連の改良・改善と情報開示のタイミングのズレ	5	1	1	7
どこまで公開するのかわからない （標準フォーマットが不明）	11	15	5	31
社内でどの部門まで対応しないといけないかわからない （資材、開発、生産部門など）	8	7	2	17
サードパーティやオープンソフトウェアの妥当性検証の懸念	3	4	2	9
開示しても顧客（医療機関等）側が適切に理解するかが懸念 （合理性のない対応を求められる懸念）	8	12	3	23



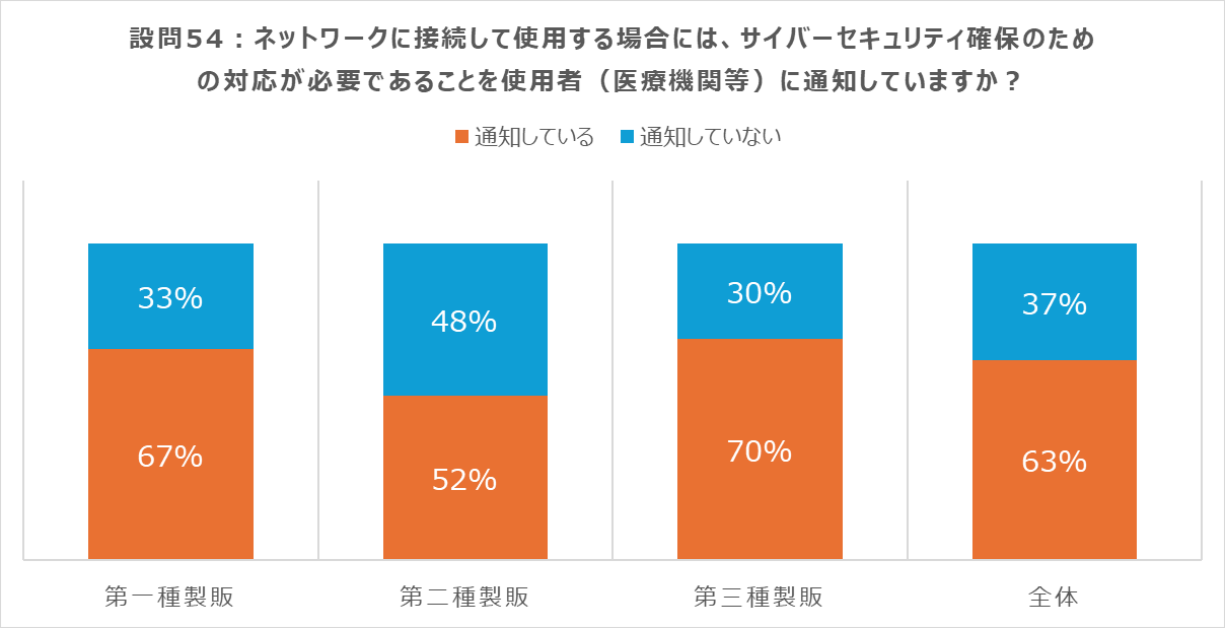
設問 53：納品時、ネットワークに接続して使用することを使用者（医療機関等）に確認していますか？

選択肢	確認している	確認していない
第一種製販	84	33
第二種製販	35	15
第三種製販	17	3
全体	136	51



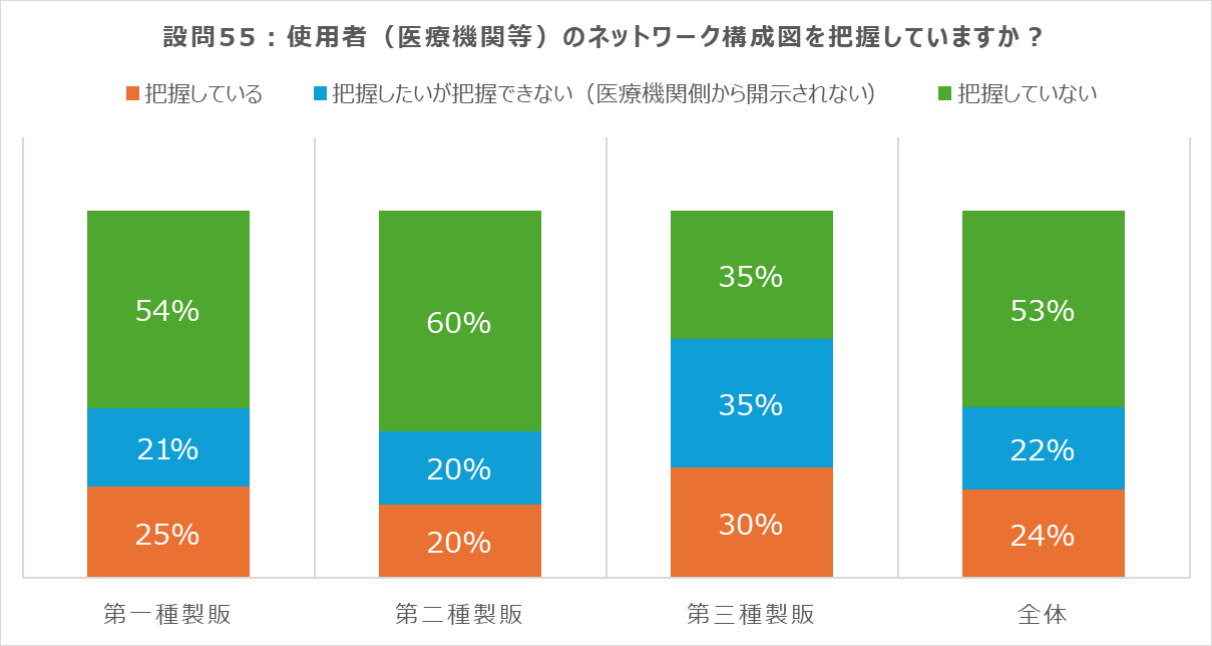
設問 54：ネットワークに接続して使用する場合には、サイバーセキュリティ確保のための対応が必要であることを使用者（医療機関等）に通知していますか？

選択肢	通知している	通知していない
第一種製販	78	39
第二種製販	26	24
第三種製販	14	6
全体	118	69



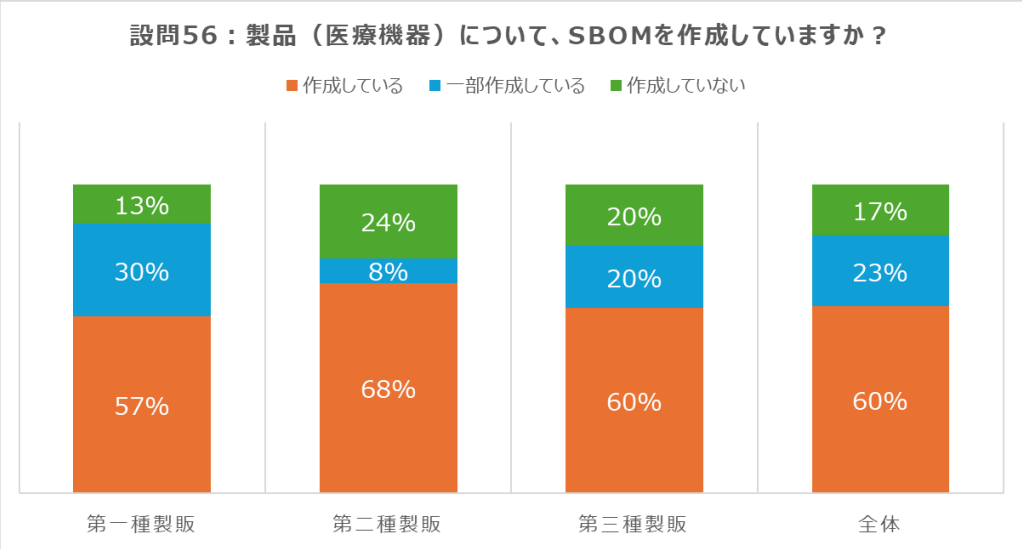
設問 55：使用者（医療機関等）のネットワーク構成図を把握していますか？

選択肢	把握している	把握したいが把握できない （医療機関側から開示されない）	把握していない
第一種製販	29	25	63
第二種製販	10	10	30
第三種製販	6	7	7
全体	45	42	100



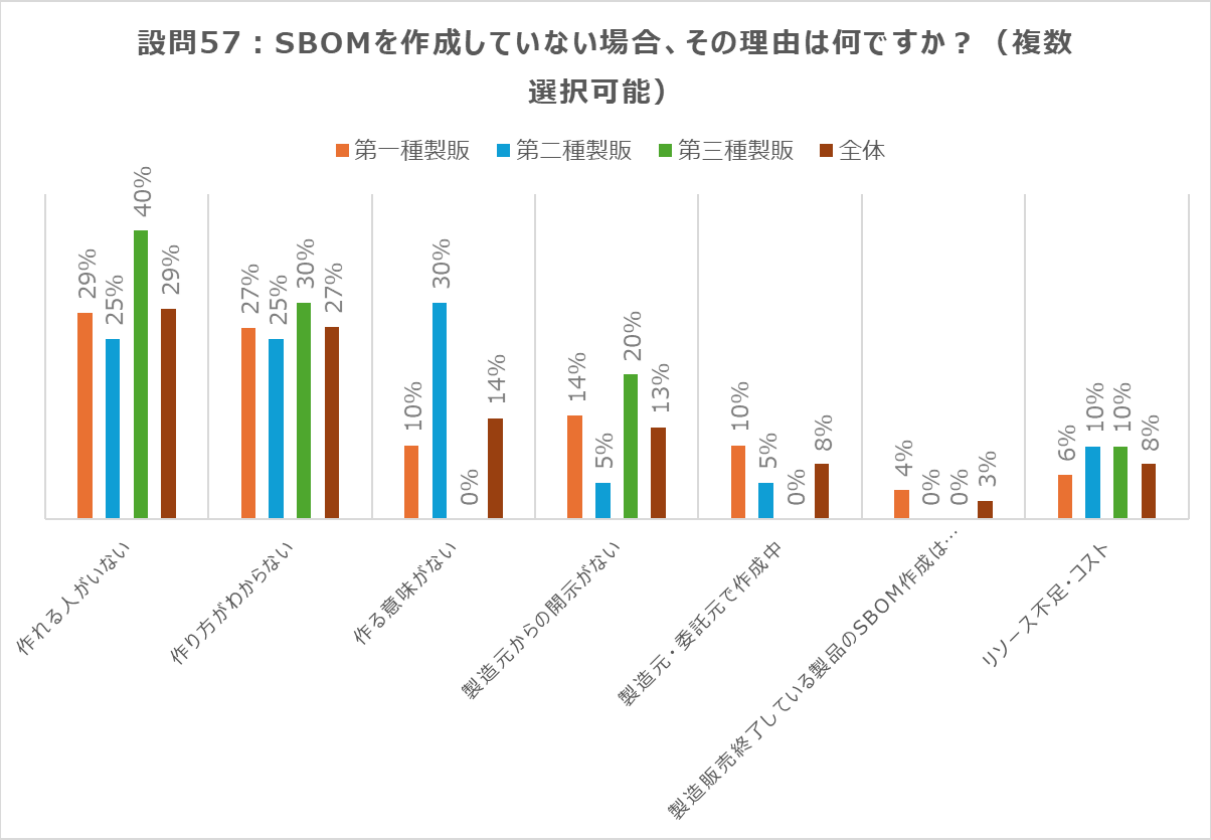
設問 56：製品（医療機器）について、SBOM を作成していますか？

選択肢	作成している	一部作成している	作成していない
第一種製販	67	35	15
第二種製販	34	4	12
第三種製販	12	4	4
全体	113	43	31



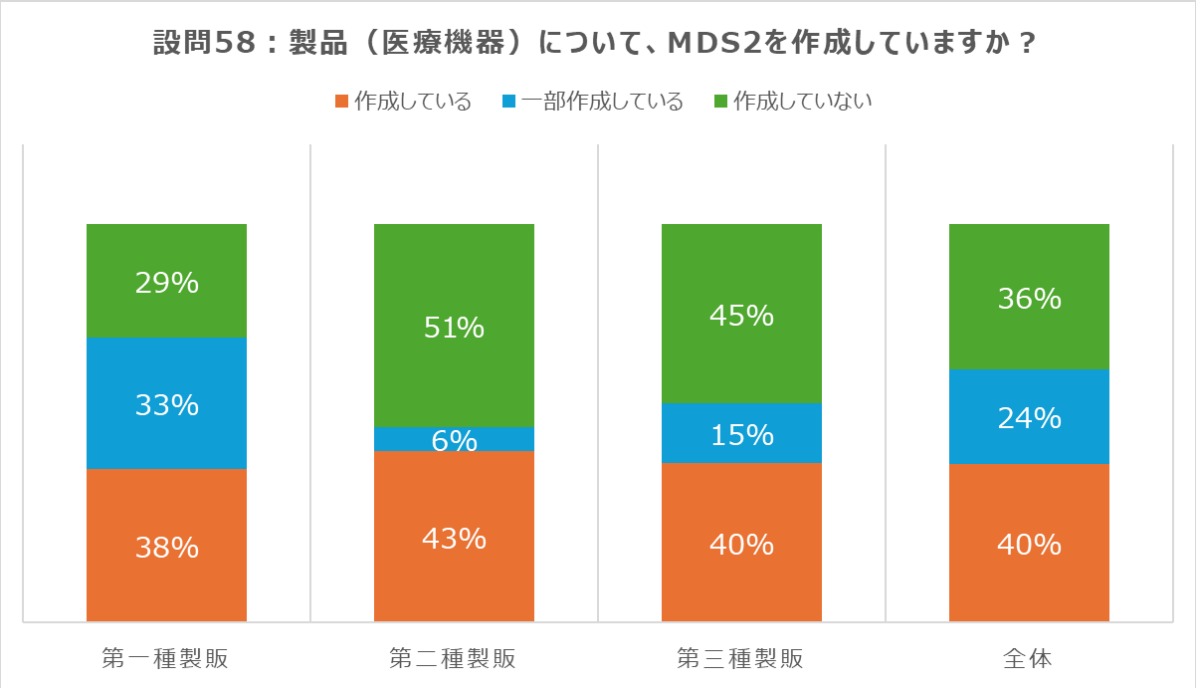
設問 57：SBOM を作成していない場合、その理由は何ですか？（複数選択可能）

選択肢	第一種製販	第二種製販	第三種製販	全体
作れる人がいない	14	5	4	23
作り方がわからない	13	5	3	21
作る意味がない	5	6	0	11
製造元からの開示がない	7	1	2	10
製造元・委託元で作成中	5	1	0	6
製造販売終了している製品の SBOM 作成は困難	2	0	0	2
リソース不足・コスト	3	2	1	6



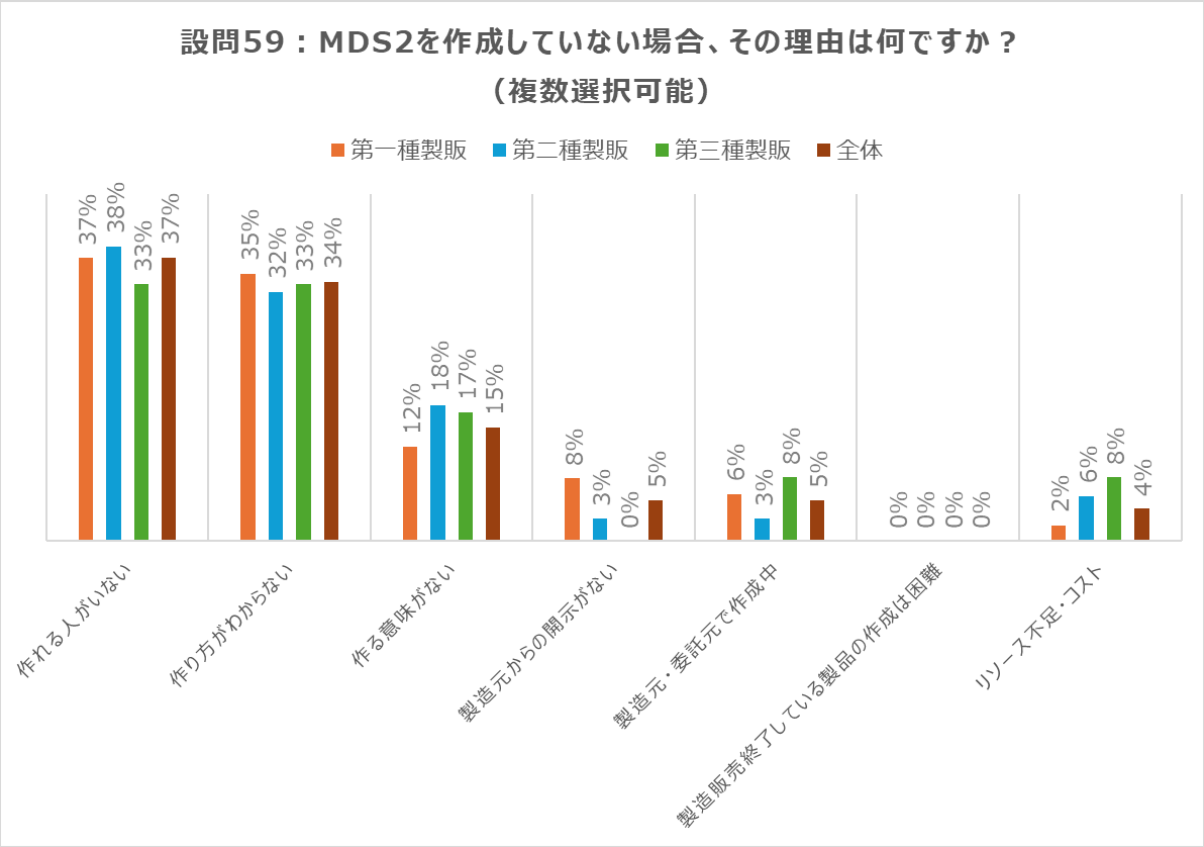
設問 58：製品（医療機器）について、MDS2 を作成していますか？

選択肢	作成している	一部作成している	作成していない
第一種製販	43	37	32
第二種製販	21	3	25
第三種製販	8	3	9
全体	72	43	66



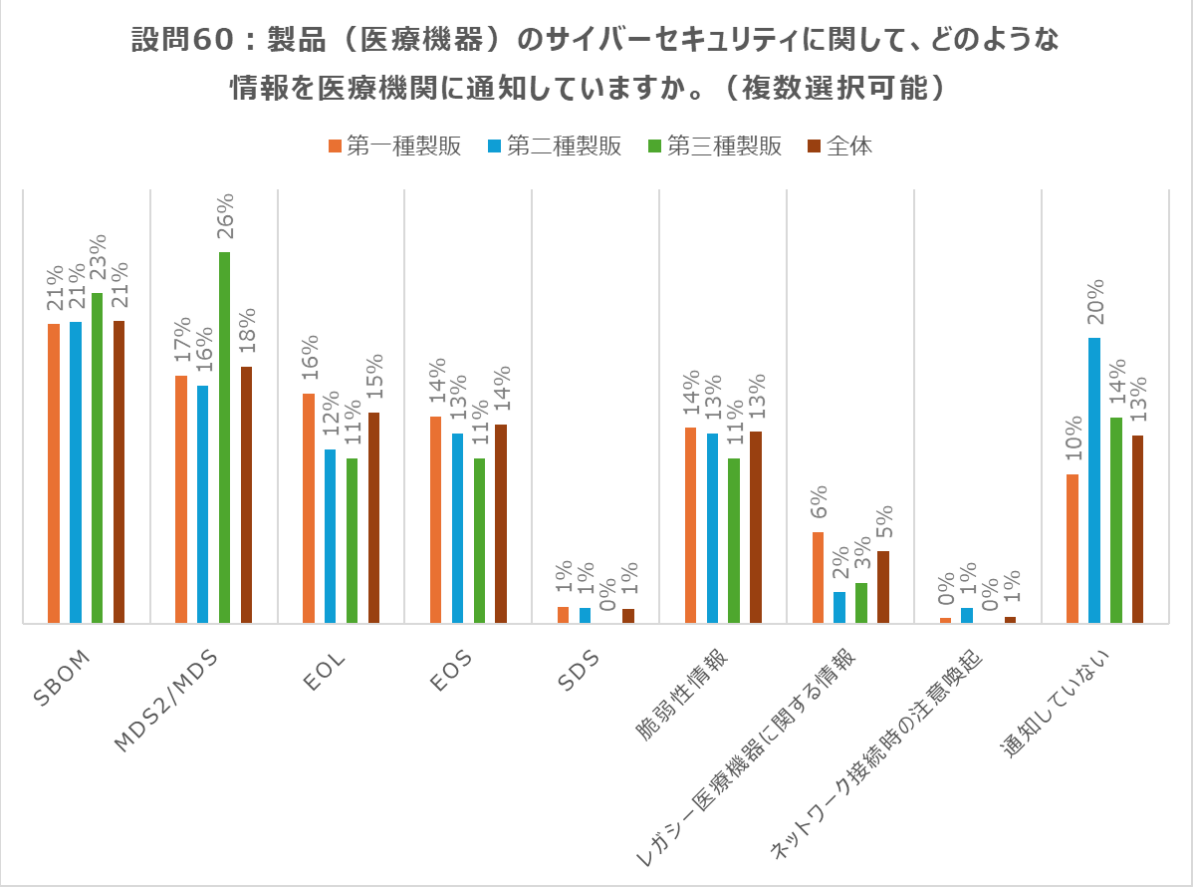
設問 59：MDS2 を作成していない場合、その理由は何ですか？（複数選択可能）

選択肢	第一種製販	第二種製販	第三種製販	全体
作れる人がいない	18	13	4	35
作り方がわからない	17	11	4	32
作る意味がない	6	6	2	14
製造元からの開示がない	4	1	0	5
製造元・委託元で作成中	3	1	1	5
製造販売終了している製品の SBOM 作成は困難	0	0	0	0
リソース不足・コスト	1	2	1	4



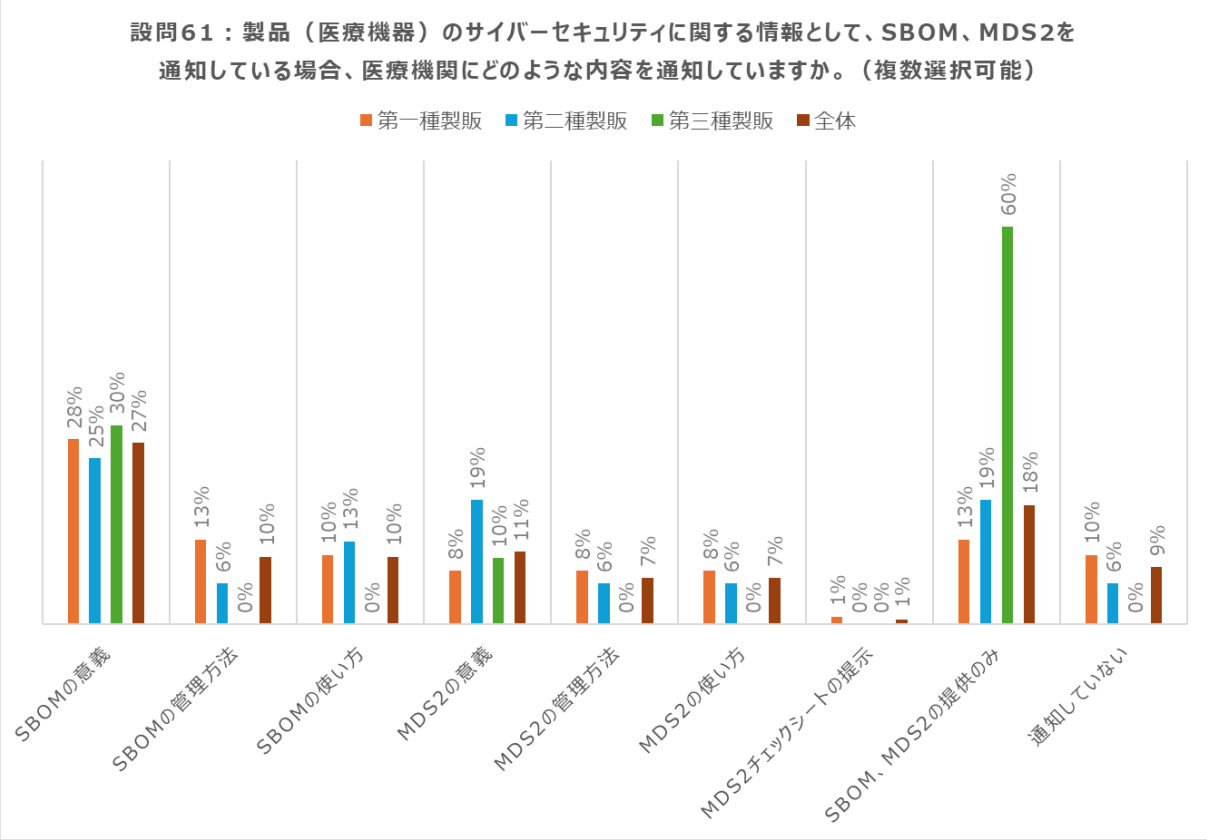
設問 60：製品（医療機器）のサイバーセキュリティに関して、どのような情報を医療機関に通知していますか。（複数選択可能）

選択肢	第一種製販	第二種製販	第三種製販	全体
SBOM	52	19	8	79
MDS2/MDS	43	15	9	67
EOL	40	11	4	55
EOS	36	12	4	52
SDS	3	1	0	4
脆弱性情報	34	12	4	50
レガシー医療機器に関する情報	16	2	1	19
ネットワーク接続時の注意喚起	1	1	0	2
通知していない	26	18	5	49



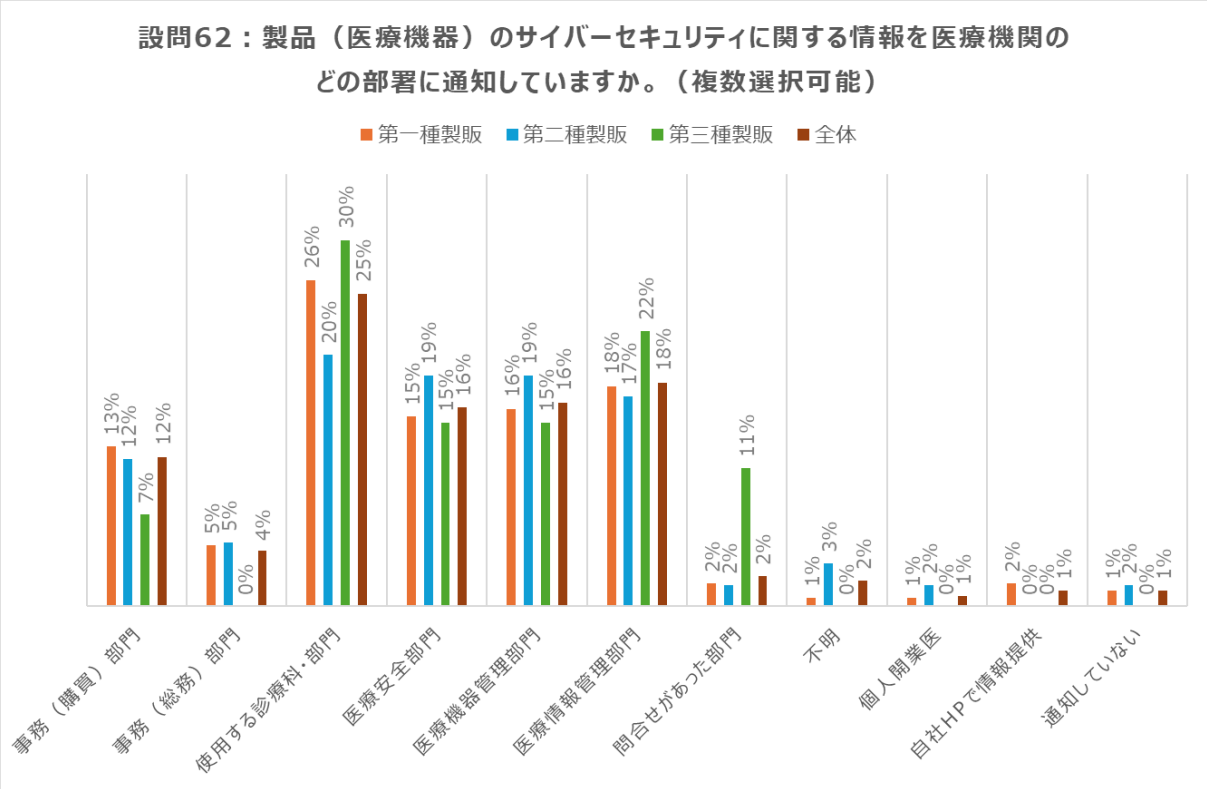
設問 61：製品（医療機器）のサイバーセキュリティに関する情報として、SBOM、MDS2 を通知している場合、医療機関にどのような内容を通知していますか。（複数選択可能）

選択肢	第一種製販	第二種製販	第三種製販	全体
SBOM の意義	24	8	3	35
SBOM の管理方法	11	2	0	13
SBOM の使い方	9	4	0	13
MDS2 の意義	7	6	1	14
MDS2 の管理方法	7	2	0	9
MDS2 の使い方	7	2	0	9
MDS2 チェックシートの提示	1	0	0	1
SBOM、MDS2 の提供のみ	11	6	6	23
通知していない	9	2	0	11



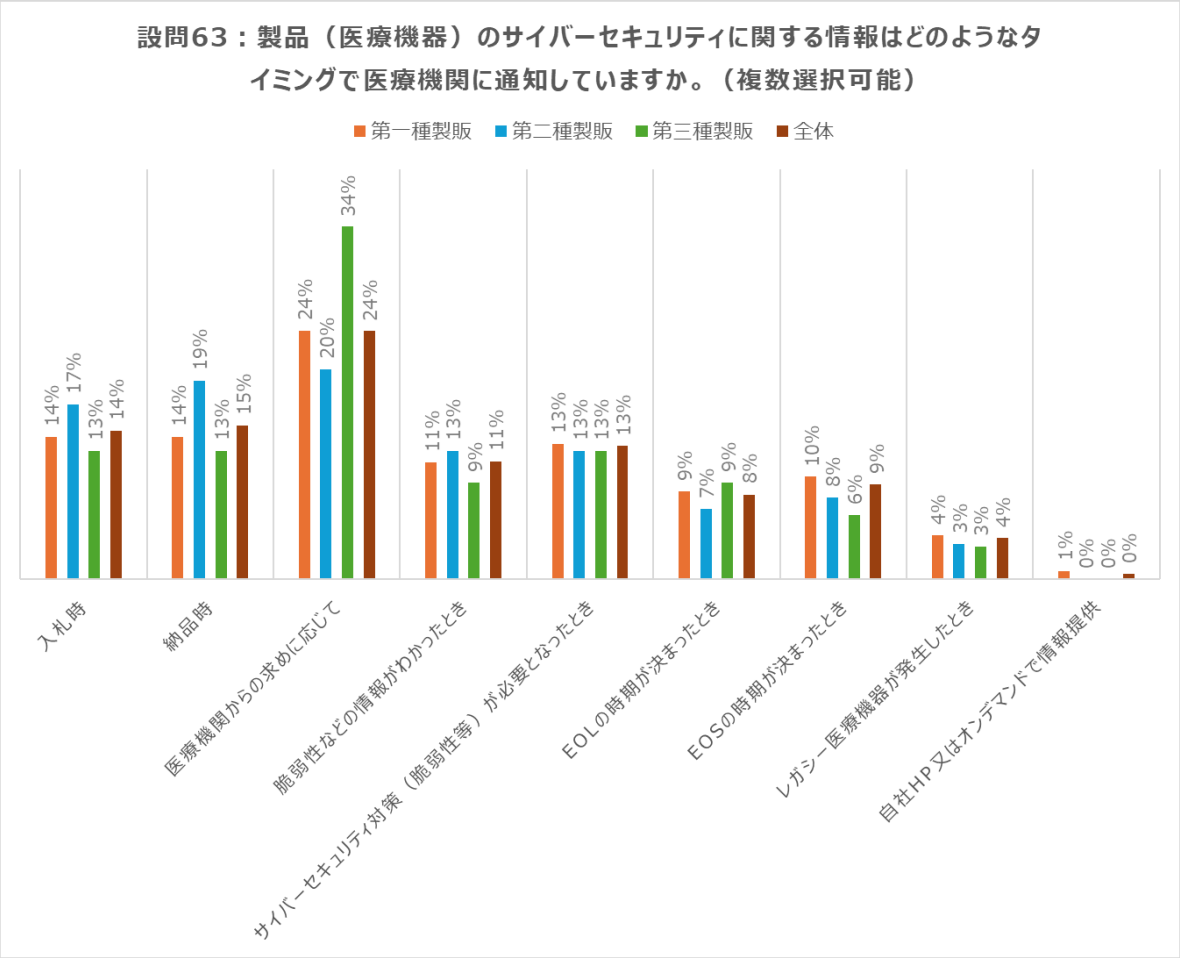
設問 62：製品（医療機器）のサイバーセキュリティに関する情報を医療機関のどの部署に通知していますか。（複数選択可能）

選択肢	第一種製販	第二種製販	第三種製販	全体
事務（購買）部門	21	7	2	30
事務（総務）部門	8	3	0	11
使用する診療科・部門	43	12	8	63
医療安全部門	25	11	4	40
医療機器管理部門	26	11	4	41
医療情報管理部門	29	10	6	45
問合せがあった部門	2	1	3	6
不明	3	2	0	5
個人開業医	1	1	0	2
自社 HP で情報提供	3	0	0	3
通知していない	2	1	0	3



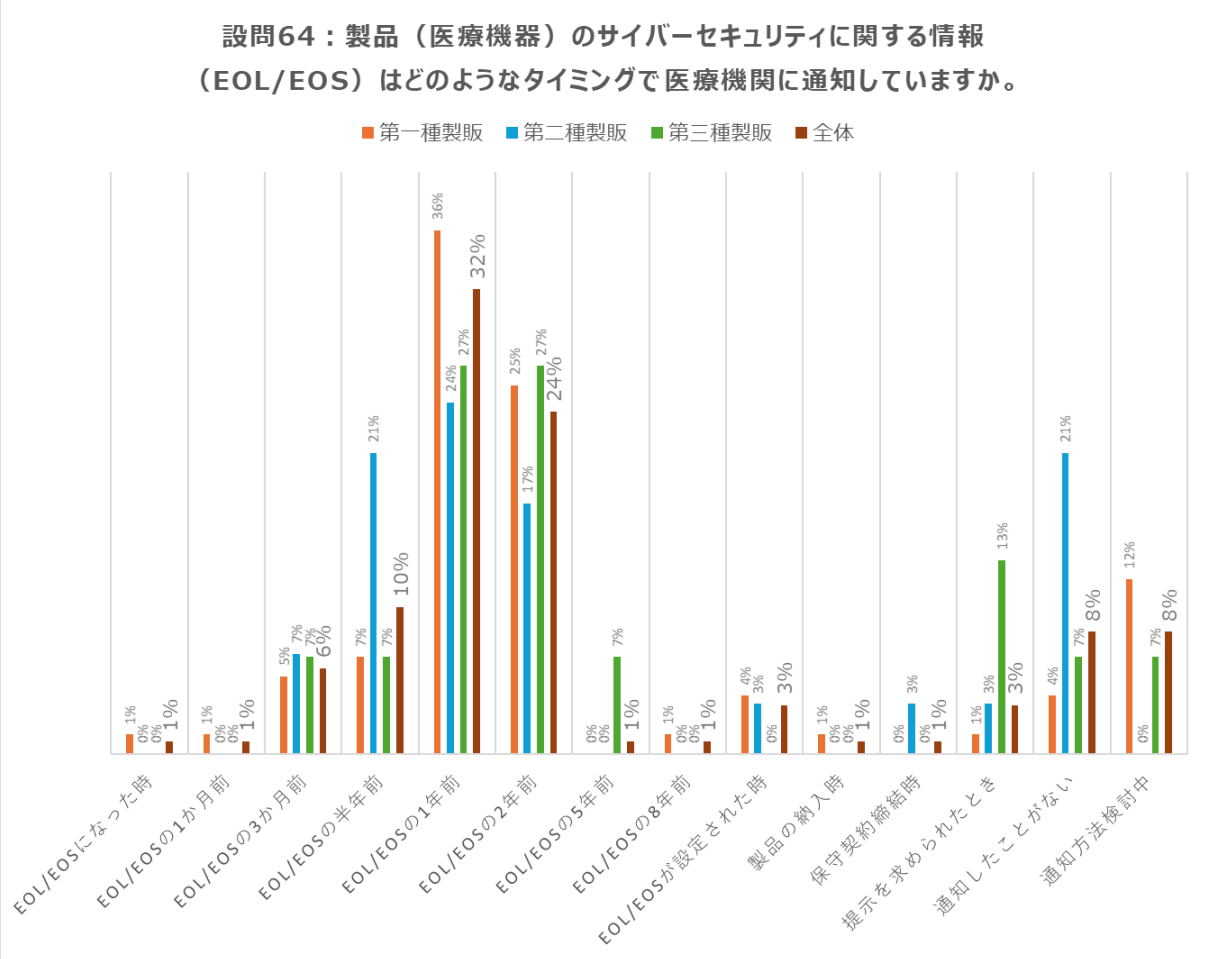
設問 63：製品（医療機器）のサイバーセキュリティに関する情報はどのようなタイミングで医療機関に通知していますか。（複数選択可能）

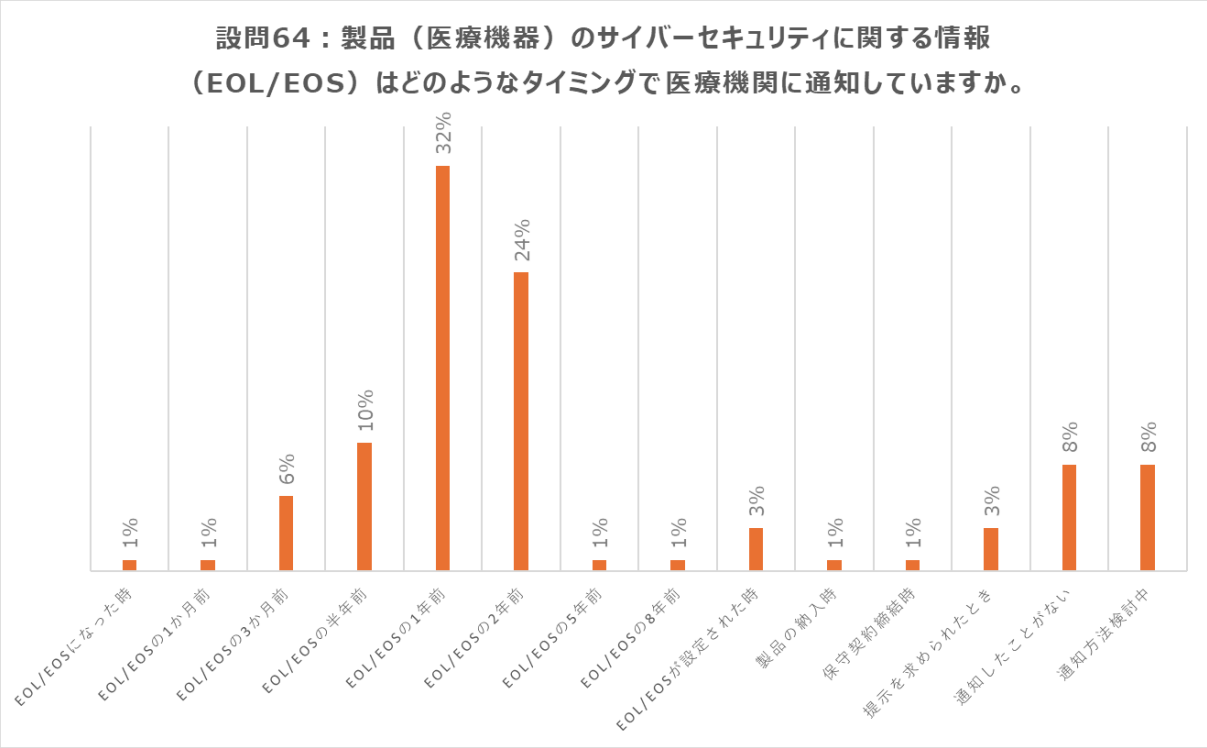
選択肢	第一種製販	第二種製販	第三種製販	全体
入札時	39	15	4	58
納品時	39	17	4	60
医療機関からの求めに応じて	68	18	11	97
脆弱性などの情報がわかったとき	32	11	3	46
サイバーセキュリティ対策（脆弱性等）が必要となったとき	37	11	4	52
EOL の時期が決まったとき	24	6	3	33
EOS の時期が決まったとき	28	7	2	37
レガシー医療機器が発生したとき	12	3	1	16
自社 HP 又はオンデマンドで情報提供	2	0	0	2



設問 64：製品（医療機器）のサイバーセキュリティに関する情報（EOL/EOS）はどのようなタイミングで医療機関に通知していますか。

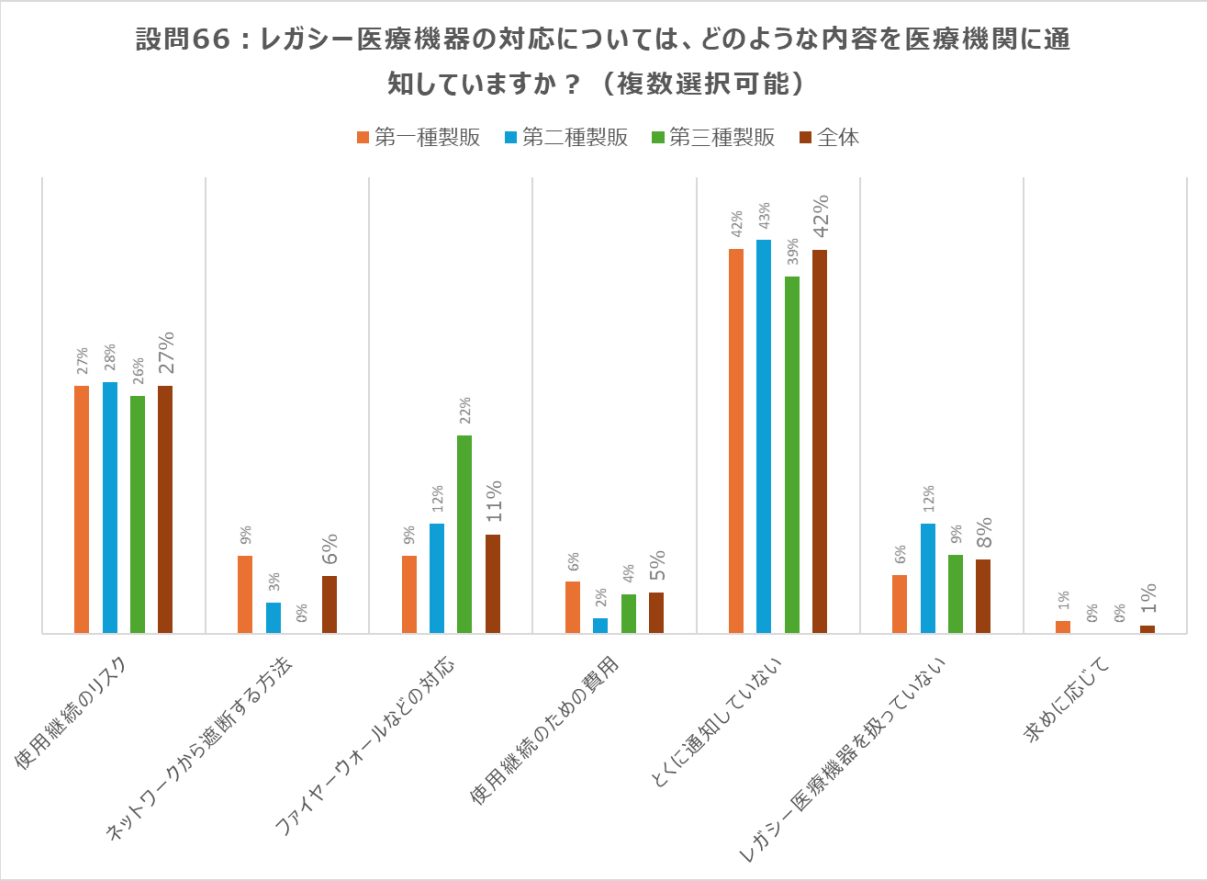
選択肢	第一種製販	第二種製販	第三種製販	全体
EOL/EOS になった時	1	0	0	1
EOL/EOS の 1 か月前	1	0	0	1
EOL/EOS の 3 か月前	4	2	1	7
EOL/EOS の半年前	5	6	1	12
EOL/EOS の 1 年前	27	7	4	38
EOL/EOS の 2 年前	19	5	4	28
EOL/EOS の 5 年前	0	0	1	1
EOL/EOS の 8 年前	1	0	0	1
EOL/EOS が設定された時	3	1	0	4
製品の納入時	1	0	0	1
保守契約締結時	0	1	0	1
提示を求められたとき	1	1	2	4
通知したことがない	3	6	1	10
通知方法検討中	9	0	1	10




設問64：製品（医療機器）のサイバーセキュリティに関する情報
（EOL/EOS）はどのようなタイミングで医療機関に通知していますか。
1%
1%
6%
10%
32%
24%
1%
1%
3%
1%
1%
3%
8%
8%
EOL/EOSになった時
EOL/EOSの1か月前
EOL/EOSの3か月前
EOL/EOSの半年前
EOL/EOSの1年前
EOL/EOSの2年前
EOL/EOSの5年前
EOL/EOSの8年前
EOL/EOSが設定された時
製品の納入時
保守契約締結時
提示を求められたとき
通知したことがない
通知方法検討中

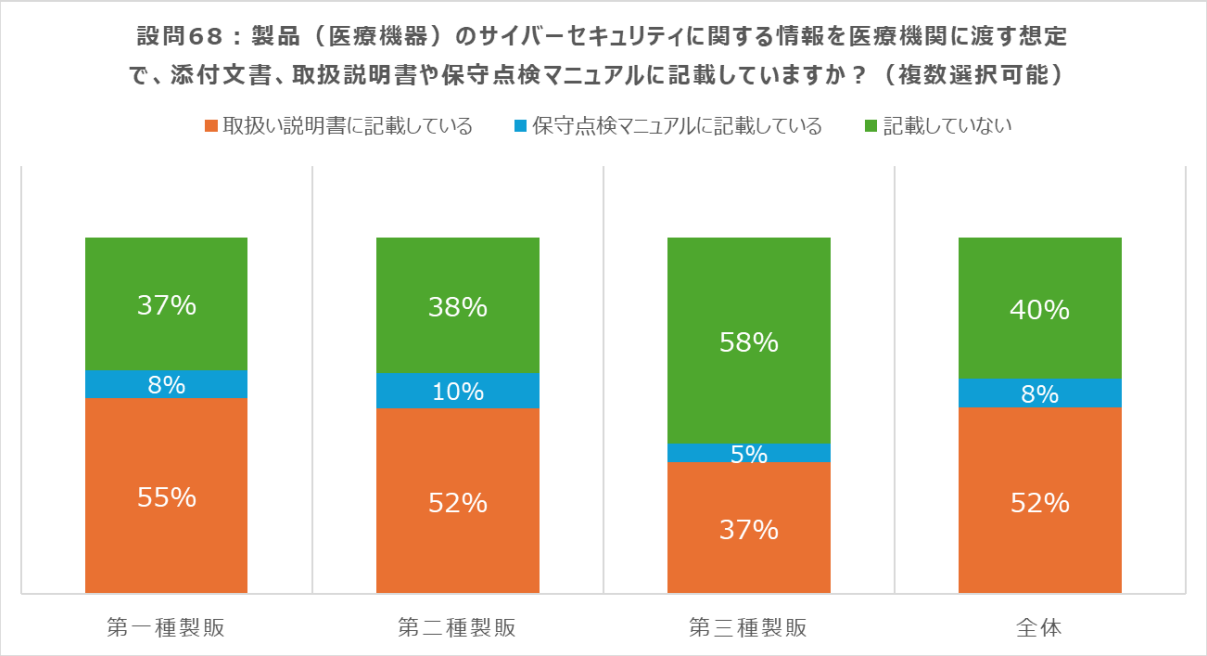
設問 66：レガシー医療機器の対応については、どのような内容を医療機関に通知していますか？（複数選択可能）

選択肢	第一種製販	第二種製販	第三種製販	全体
使用継続のリスク	38	16	6	60
ネットワークから遮断する方法	12	2	0	14
ファイヤーウォールなどの対応	12	7	5	24
使用継続のための費用	8	1	1	10
とくに通知していない	59	25	9	93
レガシー医療機器を扱っていない	9	7	2	18
求めに応じて	2	0	0	2



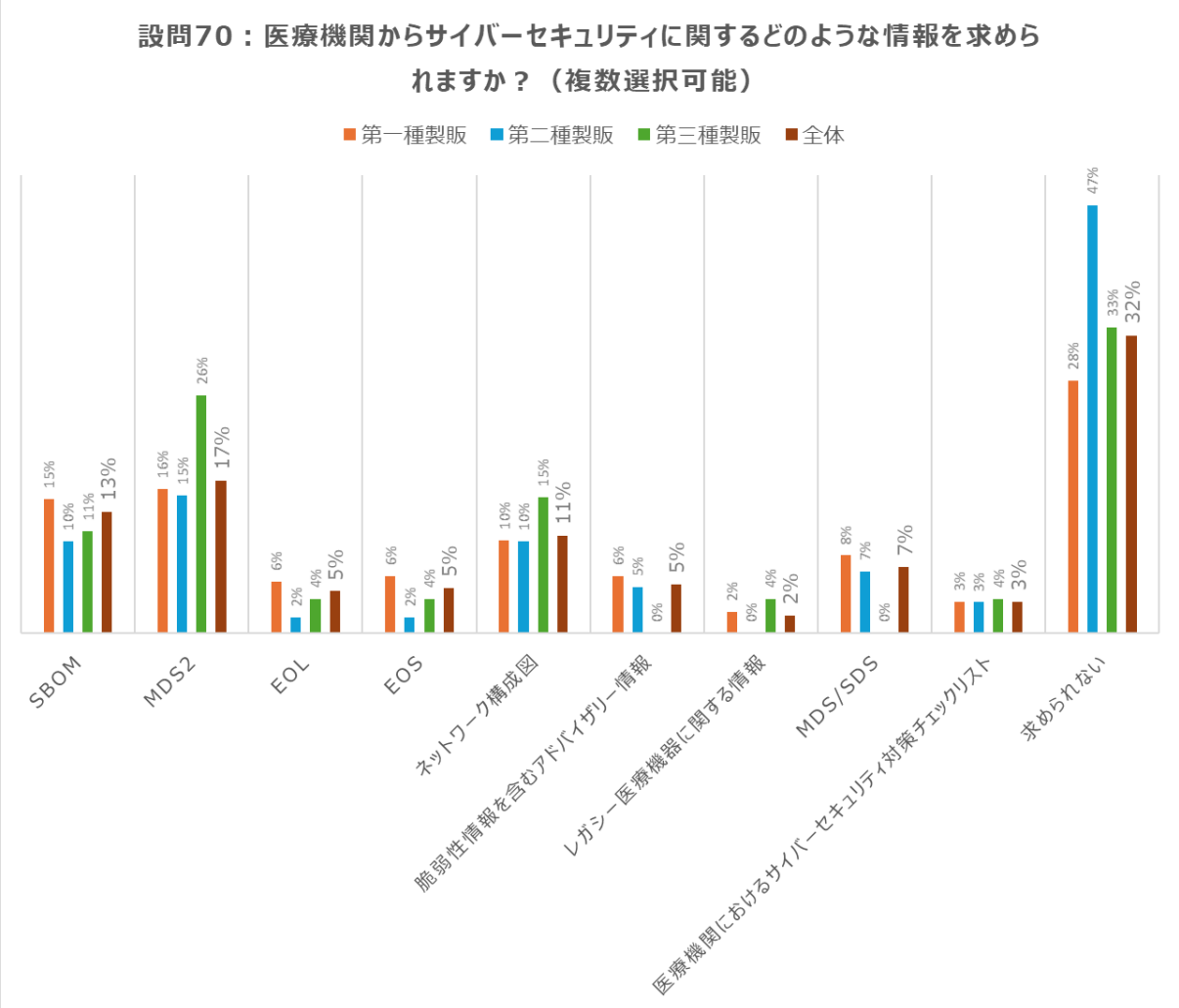
設問 68：製品（医療機器）のサイバーセキュリティに関する情報を医療機関に渡す想定で、添付文書、取扱説明書や保守点検マニュアルに記載していますか？（複数選択可能）

選択肢	第一種製販	第二種製販	第三種製販	全体
取扱い説明書に記載している	62	26	7	95
保守点検マニュアルに記載している	9	5	1	15
記載していない	42	19	11	72



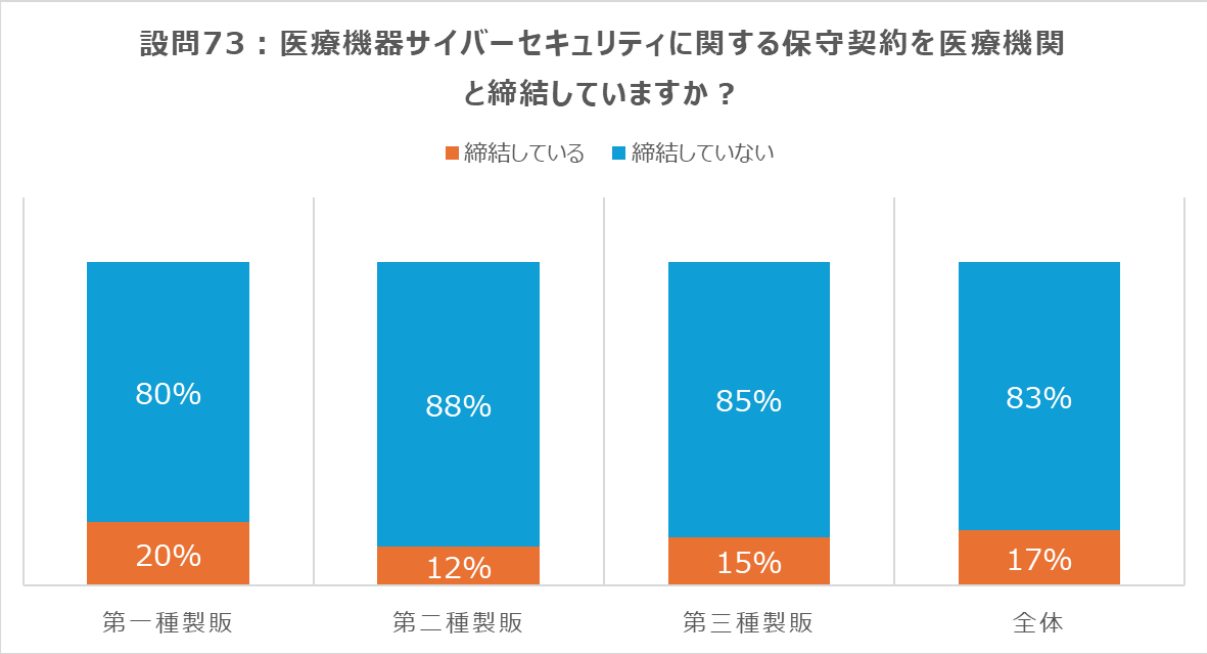
設問 70：医療機関からサイバーセキュリティに関するどのような情報を求められますか？（複数選択可能）

選択肢	第一種製販	第二種製販	第三種製販	全体
SBOM	26	6	3	35
MDS2	28	9	7	44
EOL	10	1	1	12
EOS	11	1	1	13
ネットワーク構成図	18	6	4	28
脆弱性情報を含むアドバイザリー情報	11	3	0	14
レガシー医療機器に関する情報	4	0	1	5
MDS/SDS	15	4	0	19
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のうち、事業者確認用項目の確認	6	2	1	9
求められない	49	28	9	86



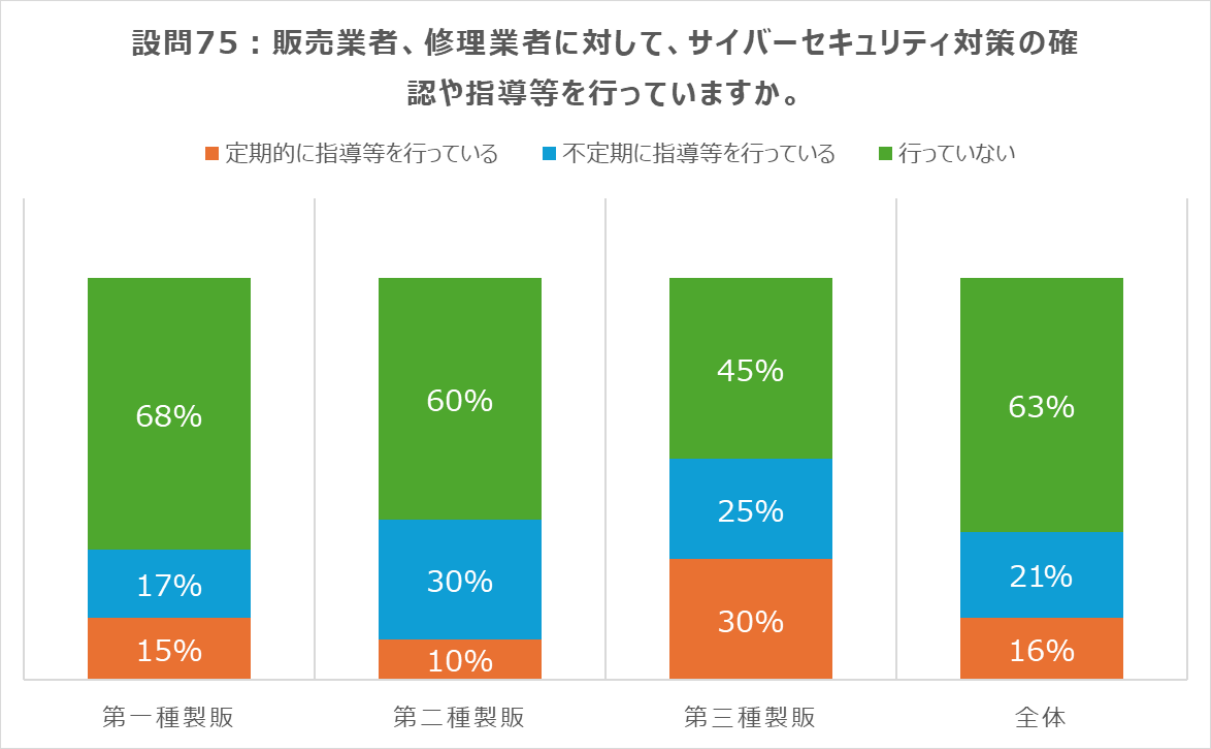
設問 73：医療機器サイバーセキュリティに関する保守契約を医療機関と締結していますか？

選択肢	締結している	締結していない
第一種製販	23	94
第二種製販	6	44
第三種製販	3	17
全体	32	155



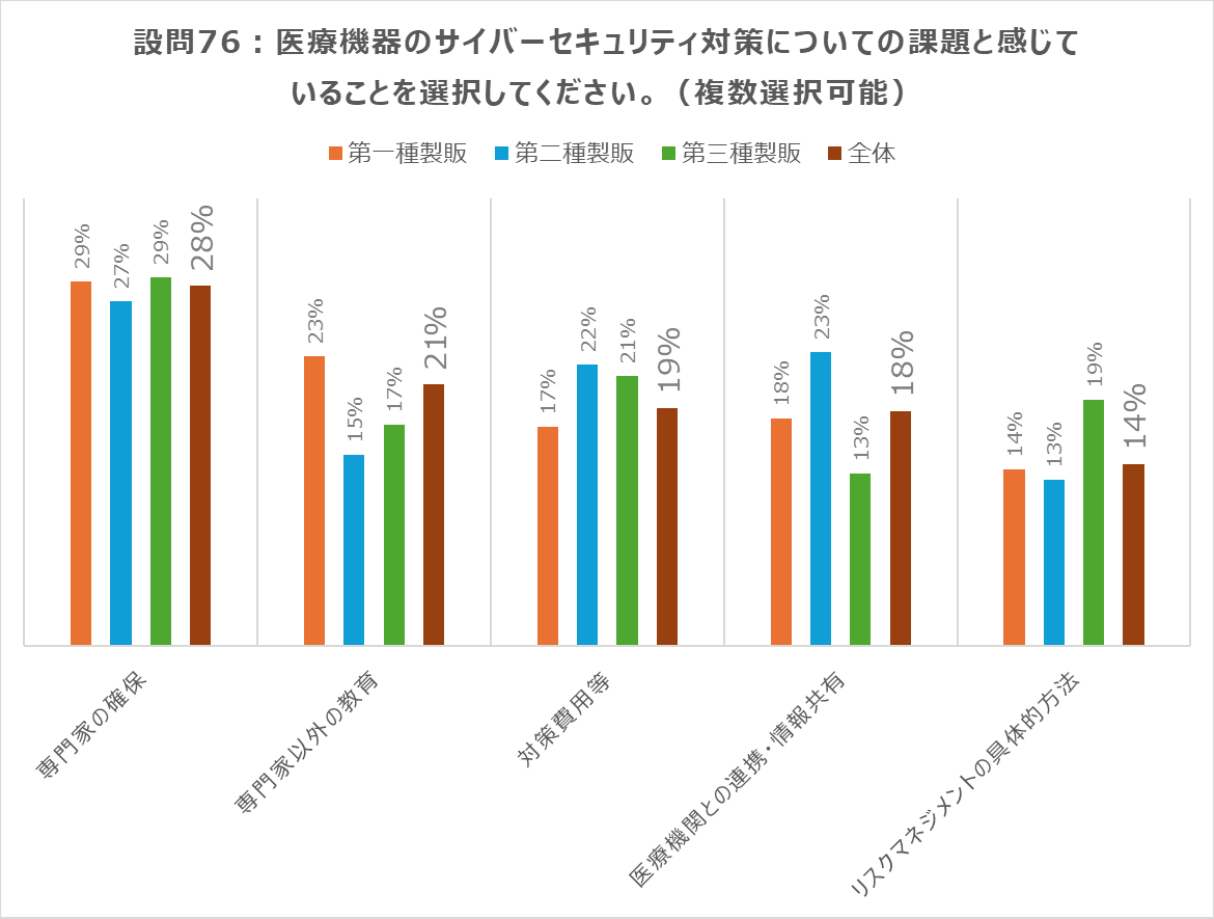
設問 75：販売業者、修理業者に対して、サイバーセキュリティ対策の確認や指導等を行っていますか。

選択肢	第一種製販	第二種製販	第三種製販	全体
定期的に指導等を行っている	18	5	6	29
不定期に指導等を行っている	20	15	5	40
行っていない	79	30	9	118



設問 76：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感じていることを選択してください。（複数選択可能）

選択肢	第一種製販	第二種製販	第三種製販	全体
専門家の確保	93	27	15	135
専門家以外の教育	74	15	9	98
対策費用等	56	22	11	89
医療機関との連携・情報共有	58	23	7	88
リスクマネジメントの具体的方法	45	13	10	68



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基づく サイバーセキュリティ対策の対応状況に関する課題及び問題点について

2024年10月7日から11月15日までの期間、全国の医療機器の製造販売業者、製造業者等を対象にアンケート調査を行った結果、次の課題及び問題点が示唆された。

1. サイバーセキュリティ対策（以下「CS対策」という。）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(設問17)、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。(設問76)。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。

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。(設問 18、19、20 及び 21)
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。(設問 27)
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 (設問 28 及び 29)、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。(設問 37 及び 38)
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、現状の対応のみで十分かについては更なる検討を要すると考える。

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（設問 55)。
また、医療機器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（設問 73)。
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（設問 76)。

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。

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（設問 13、14、17、22 及び 27）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。

以上

【会場+ライブ Web 配信+後日オンデマンド配信】

2024 年度 医療機器の承認･認証申請等に関する説明会

開催案内

開 催 日：2025 年 3 月 5 日（水）13:00～17:20

オンデマンド視聴：2025 年 4 月 1 日（火）～5 月 9 日(金)

受付期間： ＜会場、ライブWEB 配信＞

2025年1月21日（火）13時00分～2月19日（水）23時59分

＜後日オンデマンド配信のみ視聴＞

2025年1月21日（火）13時00分～3月19日（水）23時59分

会 場：日比谷国際ビルコンファレンススクエア

申込人数：会場：上限 80 名

ライブ WEB 配信：上限 1,000 名

後日オンデマンド配信のみ視聴：人数制限なし

開 催 趣 旨

本年度は、9 月に開催したプログラム医療機器に関する説明会も盛会となり、引き続き関心の高い内容であることを感じております。
また、本年度は PMDA（医薬品医療機器総合機構）の第 5 期中期計画スタートの年であり、併せて「医療機器規制と審査の最適化のための協働計画 2024」及び「体外診断用医薬品規制と審査の最適化のための協働計画 2024」も策定されたところです。ここで本年度の締めくくりとして、我が国の医療機器規制及び業界標準の動向について、必要な最新の情報をお届けしようと思います。

本説明会では、医療機器行政に係る最近の動向について（制度部会、協働計画、生物学ガイダンス、FD 申請における留意点 等）の最新の法規制動向について、厚生労働省の担当官ならびに PMDA の担当者から説明を頂きます。
また、ARCB（医薬品医療機器等登録認証機関協議会）からは、認証申請に係る留意事項等について説明を頂きます。さらに、業界からは次の法改正やサイバーセキュリティに関する検討状況報告等の最新情報を提供したいと考えております。

今回の説明会については、ハイブリッド開催（会場＋ライブ配信）＋オンデマンド配信にて開催することとさせていただきます。リアルタイム開催ならではと、短い時間ですが質疑応答の時間を設けておりますので、質問がある方は、申し込み時に質問をお寄せください。
つきましては、医療機器の製造販売業者等の薬事関連業務のご担当者、あるいは管理監督する立場の皆様におかれましては、より一層の理解を深めていただく恰好の機会でありますので、研修の場としても広くご活用いただきたくご案内いたします。

2025 年 1 月吉日

(一社)日本医療機器産業連合会
法制委員会

2024 年度 医療機器の承認・認証申請等に関する説明会

プログラム

司会 法制委員会 周知教育関連分科会 副主査 本田 一人

時間	テ ー マ	講 師（敬称略）
12:30～13:00	参 加 者 受 付	
【１】 13:00	開催挨拶	医機連 法制委員会 委員長 田中 志穂
【２】 13:05～13:35 (30 分)	最近の医療機器行政の動向 -次期薬機法改正に向けた検討状況など-	厚生労働省 医薬局 医療機器審査管理課 再生医療等製品審査管理室 室長 冨田 耕太郎
【３】 13:35～14:05 (30 分)	協働計画について ・審査報告書の対象拡大と公開、・相談制度の改善など	（独）医薬品医療機器総合機構 医療機器審査第一部 部長 矢花 直幸
【４】 14:05～14:35 (30 分)	生物学的安全性ガイダンス通知改定と原材料通知改定の概要について	（独）医薬品医療機器総合機構 医療機器審査第二部 審査役 穴原 玲子
【５】 14:35～14:50 (15 分)	生物学的安全性ガイダンス通知改定	生物学的安全性評価のガイダンス通知改定 WG 主査 田中 謙一
【５】 14:50～15:05 (15 分)	原材料通知改定	生物学的安全性評価方法変更に伴う原材料通知改定検討 WG 小原井 裕樹
休憩 15:05～15:25（20 分）		
【６】 15:25～15:45 (20 分)	サイバーセキュリティ活動報告	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に関する研究 分担研究者 三宅 学
【７】 15:45～15:55 (10 分)	FD 申請における留意点 ～フロッピーディスクを利用した申請等の受付の廃止について～	厚生労働省 医薬局 医療機器審査管理課 許可係 種田 賢一郎
【８】 15:55～16:15 (20 分)	認証関係（留意事項など）	医薬品医療機器等法登録認証機関協議会 （ARCB）
【９】 16:15～16:35 (20 分)	協働計画活動報告	法制委員会 審査関連分科会 主査 佐伯 文 基準分科会 主査 安田 典子
【１０】 16:35～16:55 (20 分)	法改正活動報告	第二次薬機法改正検討 WG 副主査 村上 邦臣 QMS 調査制度検討 WG 副主査 佐藤 央英
【１１】 16:55～17:15 (20 分)	質疑応答	モデレーター 医機連 法制委員会 委員長 田中 志穂
【１２】 17:15～17:20 (5 分)	閉会挨拶	医機連 法制委員会 副委員長 矢吹 宗男

＊：時間は目安です。プログラム、テーマ、講師については、変更になる場合があります。

サイバーセキュリティ活動報告

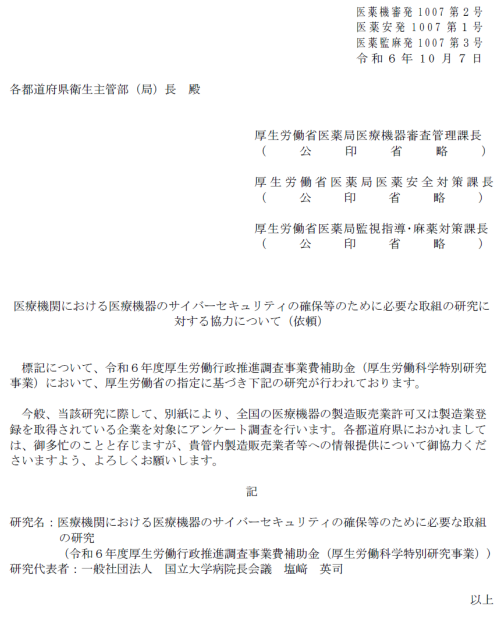
厚生労働科学研究「医療機関における医療機器のサイバーセキュリティの確保等のために必要な取組の研究」

2025年3月5日

分担研究者　三宅　学

初めに

- アンケート調査にご協力いただきました医療機器の製造販売業者、製造業者、関係企業の皆さまに御礼申し上げます。
- アンケート調査の実施にあたり、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アンケートシステムを利用しました。感謝申し上げます。
- 当該厚生労働科学研究の研究班活動にご協力いただいております研究協力者の皆さまにも御礼申し上げます。



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
令和６年１０月７日

各都道府県衛生主管部（局）長　殿

厚生労働省医薬局医療機器審査管理課長
（　公　印　省　略　）

厚生労働省医薬局医薬安全対策課長
（　公　印　省　略　）

厚生労働省医薬局監視指導・麻薬対策課長
（　公　印　省　略　）

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）

標記について、令和６年度厚生労働行政推進調査事業費補助金（厚生労働科学特別研究事業）において、厚生労働省の指定に基づき下記の研究が行われております。

今般、当該研究に際して、別紙により、全国の医療機器の製造販売業許可又は製造業登録を取得されている企業を対象にアンケート調査を行います。各都道府県におかれましては、御多忙のことと存じますが、貴管内製造販売業者等への情報提供について御協力くださいますよう、よろしくお願いします。

記

研究名：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年度厚生労働行政推進調査事業費補助金（厚生労働科学特別研究事業））
研究代表者：一般社団法人　国立大学病院長会議　塩崎　英司

以上

2

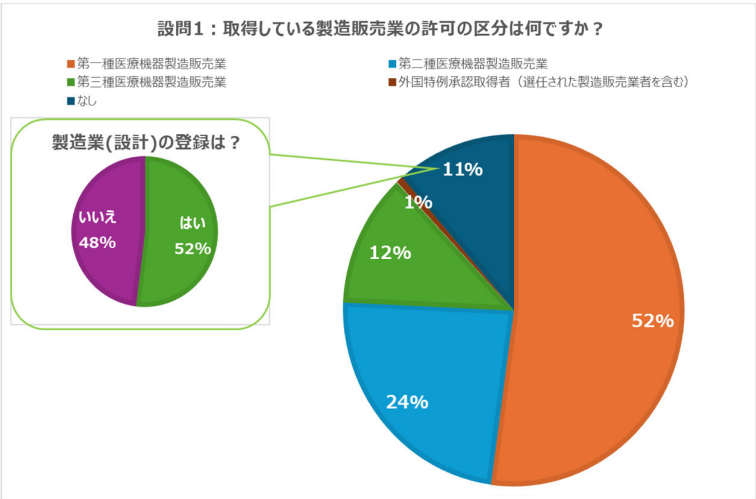
アンケート調査の目的

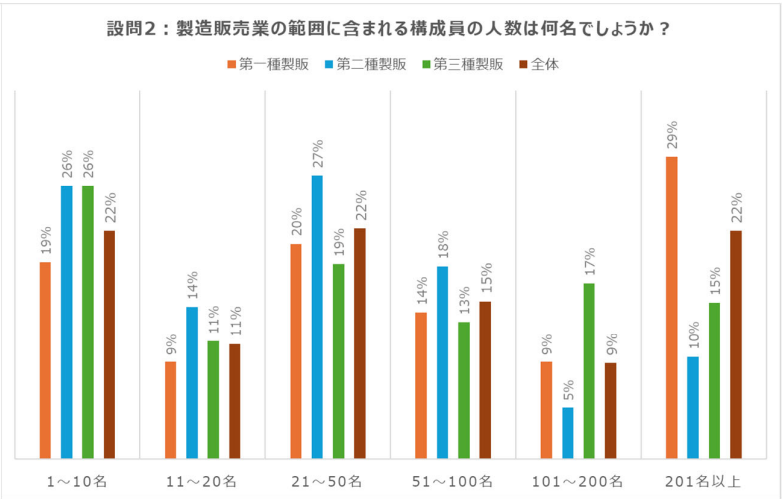
サイバー攻撃により社会インフラに多大な影響をもたらす事例が多数発生しており、防護するためのサイバーセキュリティ対策の重要性は高まっている。医療機器については、医療機器の基本要件基準第12条第3項にサイバーセキュリティ対策に関する要求事項が明確化され、令和6年4月1日より適用されている。

本研究班では、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、現在の制度での対応が十分か検討し、制度上の手当ての必要性を含めて議論を進めている。本調査は、医療機器全般のサイバーセキュリティ対策の現状を把握し、問題点、課題等の情報を収集分析し、その結果をより適切な制度設計の提言案にまとめることを目的に実施する。

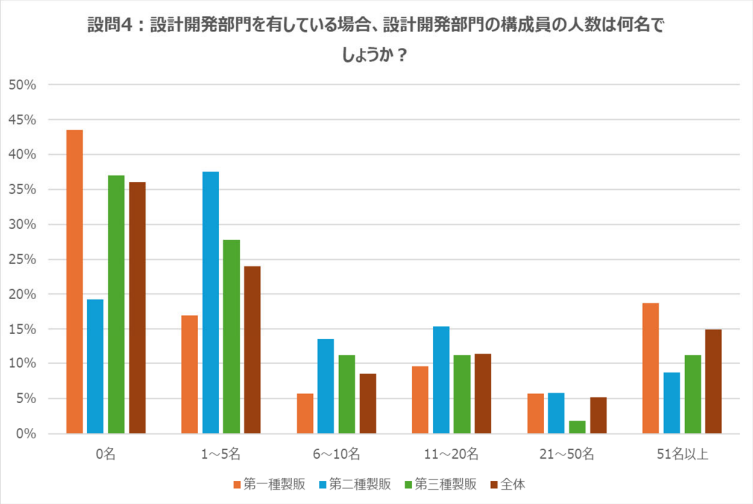
- 2024年10月7日から11月15日までの期間、全国の医療機器の製造販売業者、製造業者等を対象にアンケート調査を行った。
- 全441社の医療機器の製造販売業者、製造業者等からの回答を得た。アンケート調査の実施にあたっては、一般社団法人日本画像医療システム工業会が所有するWEBアンケートシステムを利用した。

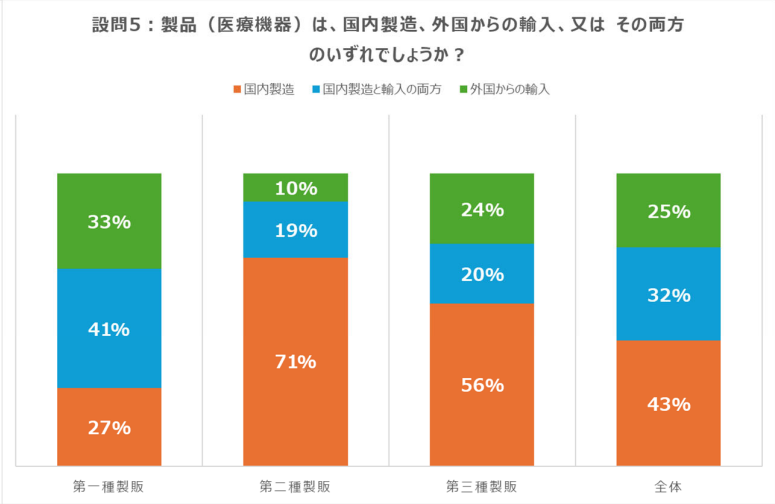
アンケート調査の回答者について(1)



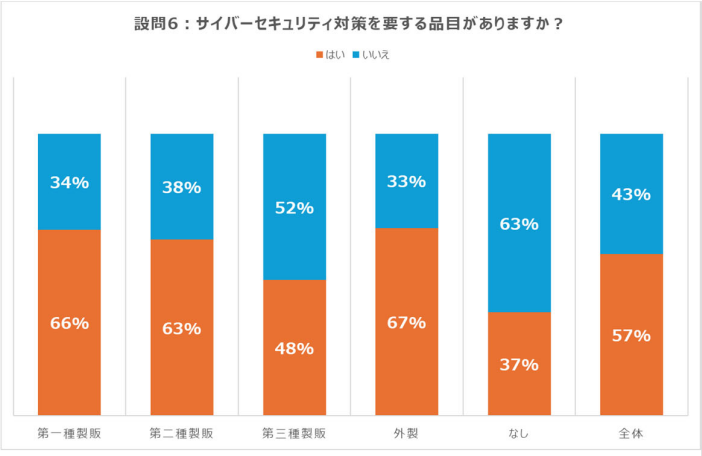


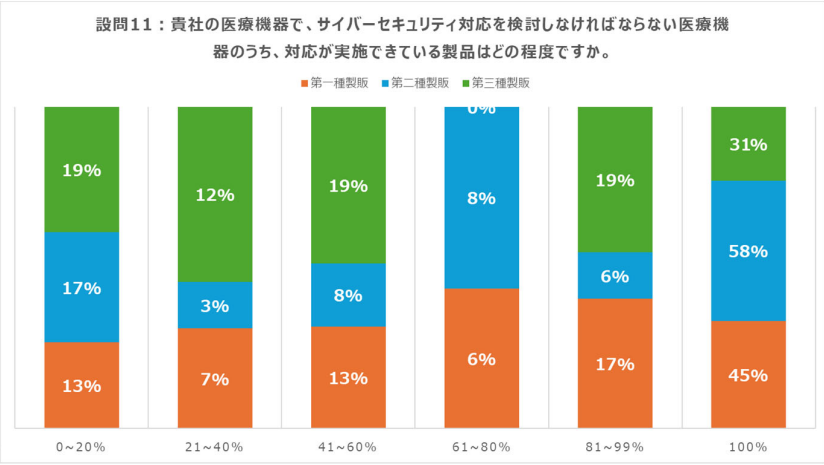
アンケート調査の回答者について(2)



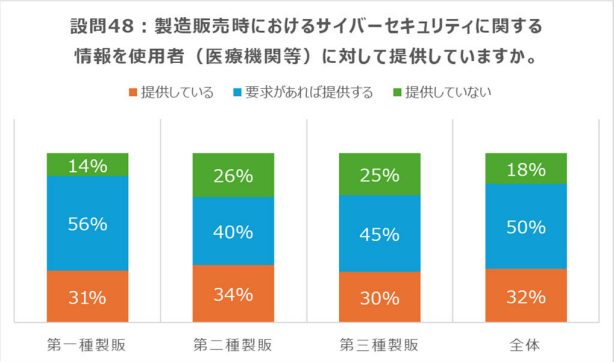


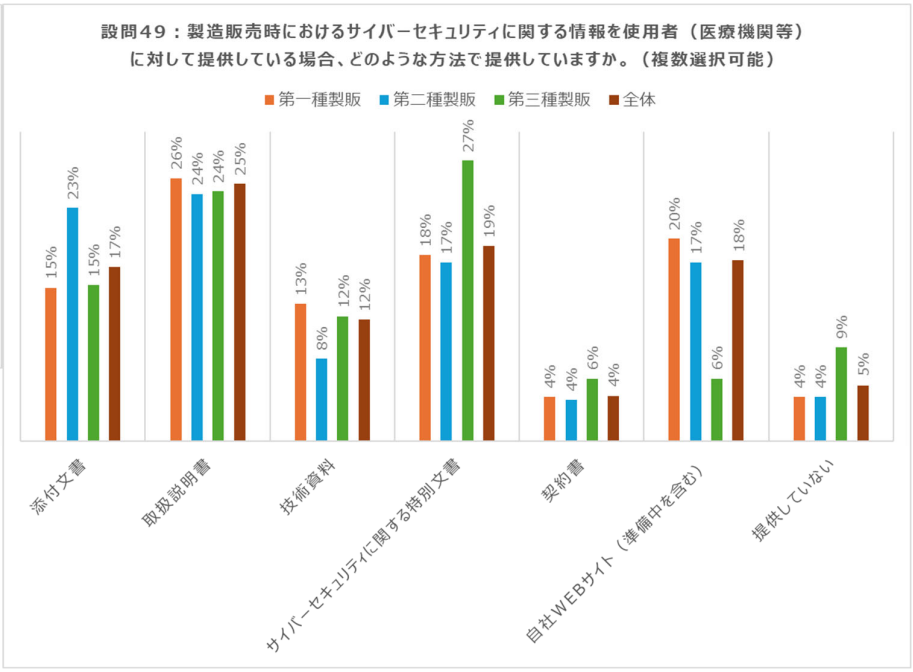
サイバーセキュリティ対策の対応状況





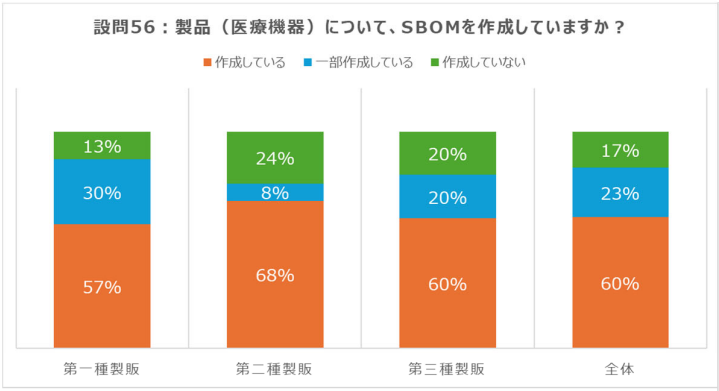
サイバーセキュリティに関する情報提供

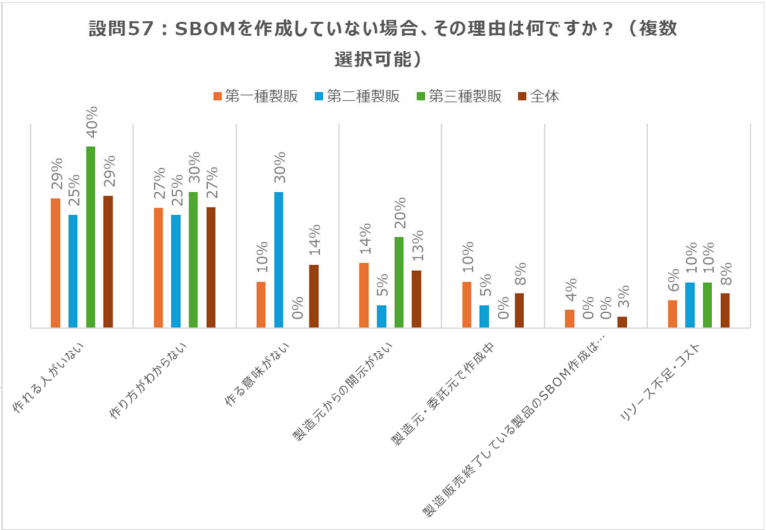




7

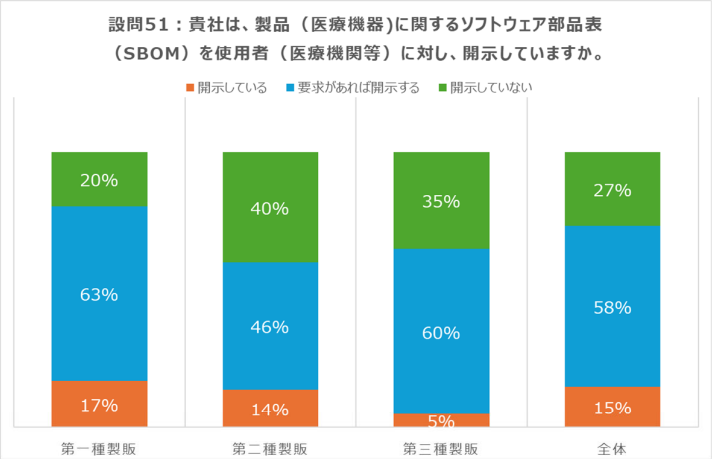
SBOMの作成状況

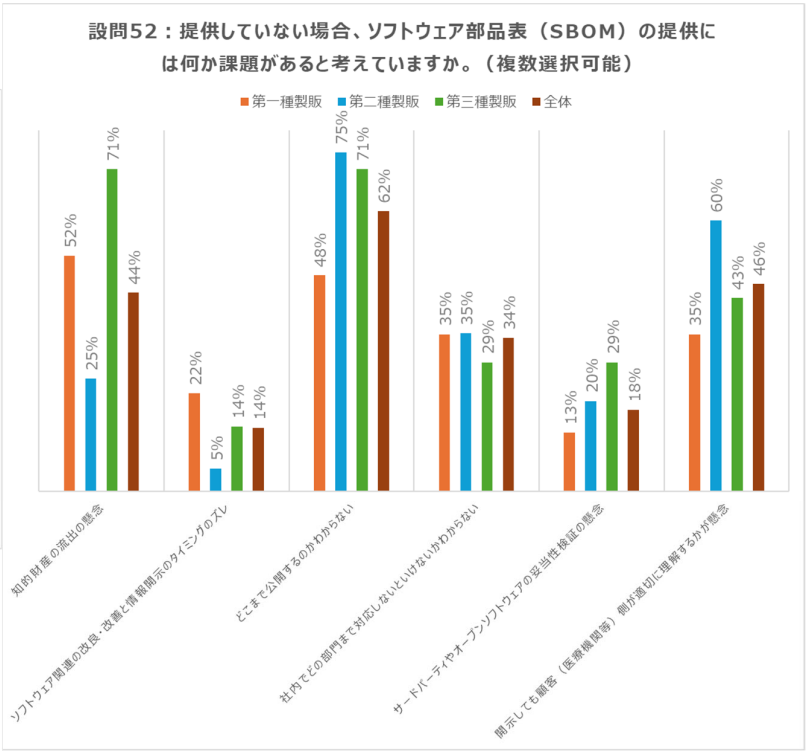




8

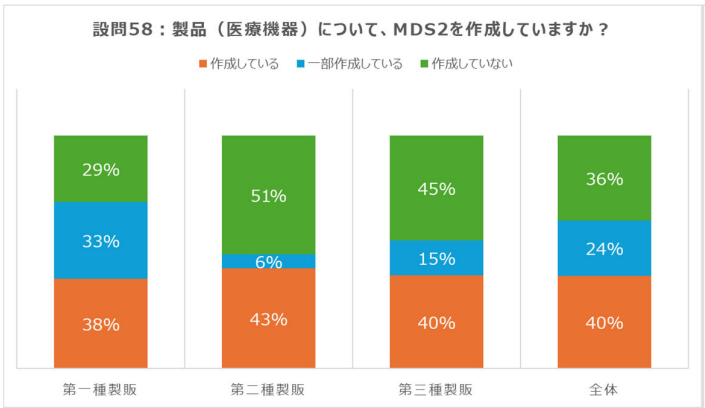
SBOMの開示状況

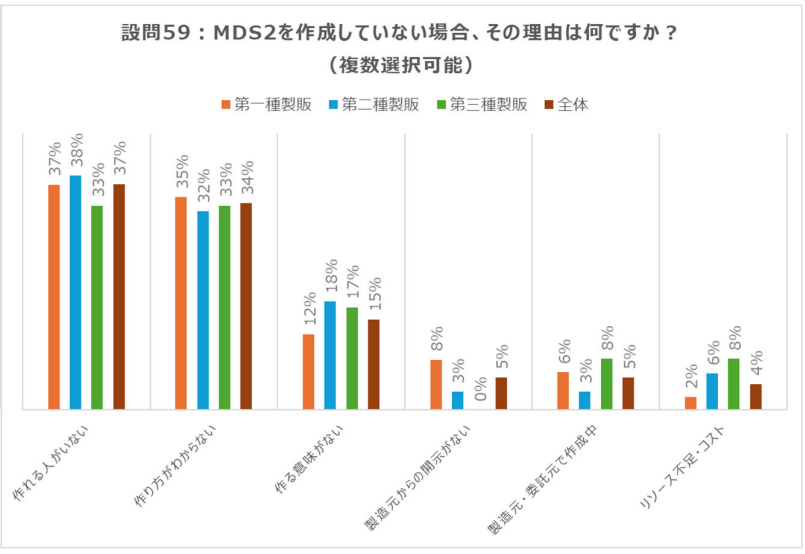




9

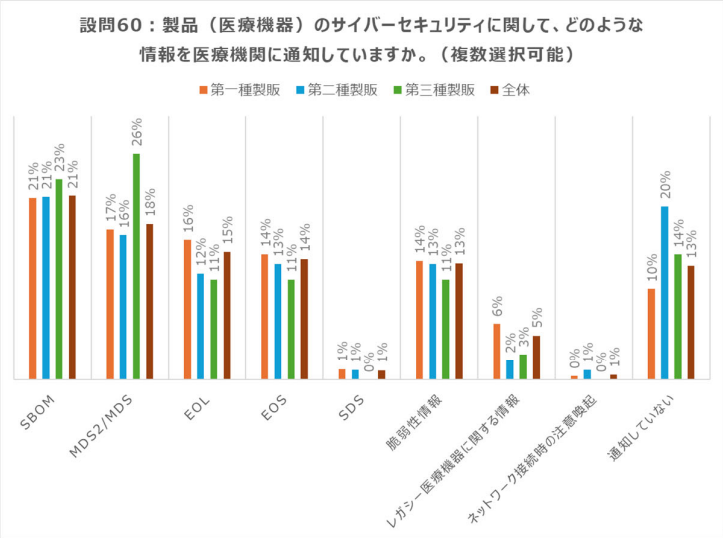
MDS2の作成状況

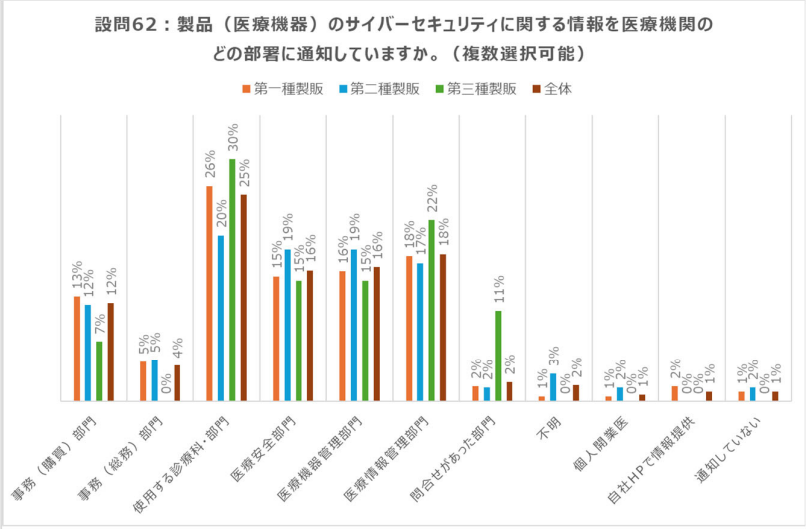




10

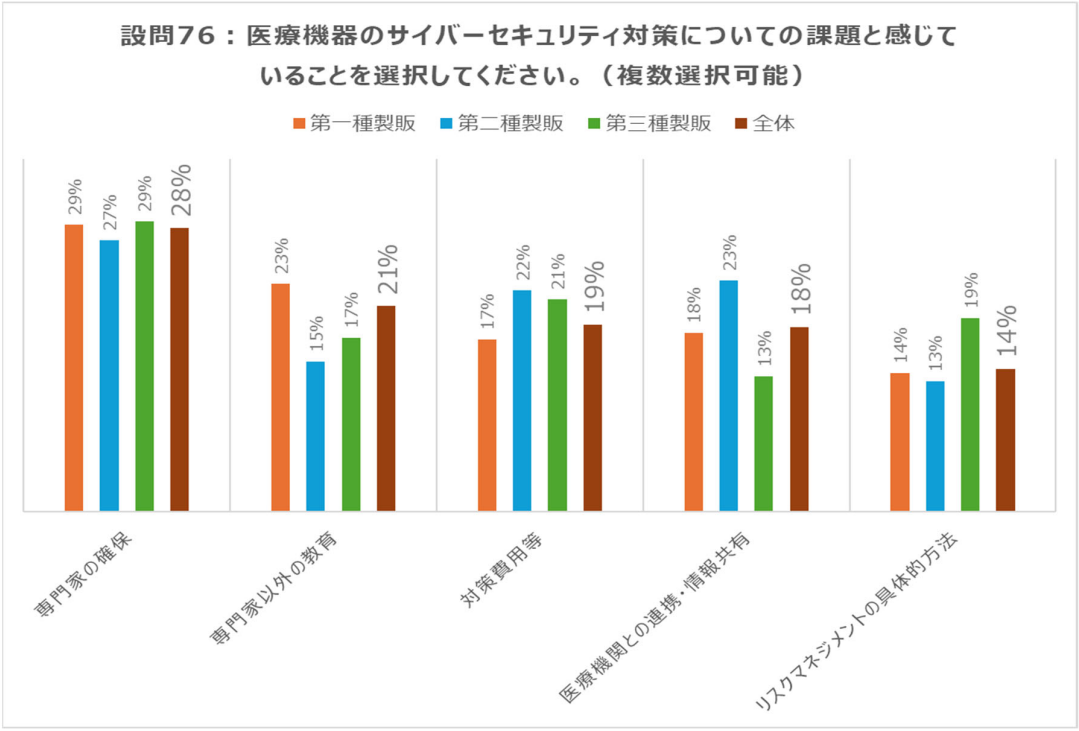
サイバーセキュリティに関する情報の医療機関への提供





11

サイバーセキュリティ対策の課題・問題点



12

参考情報

厚生労働省ホームページ：医療機器におけるサイバーセキュリティについて
https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/0000179749_00009.html

PMDAホームページ：医療機器のサイバーセキュリティについて
https://www.pmda.go.jp/review-services/drug-reviews/about-reviews/devices/0051.html

ご清聴ありがとうございました

別紙 1

日本医師会のサイバーセキュリティ相談窓口に関するヒアリング（要約）

1. 医療情報システムに関するサイバーセキュリティ確保について

サイバーセキュリティ支援制度を立ち上げ、業者に委託し運営。有事から平時まで会員からのサイバーセキュリティ相談窓口として対応。月 20-10 件程度対応している。

受付対応の人員については、サイバーセキュリティについて学んではいるものの、専門家ではない。

管理者については、情報セキュリティの資格を持った者が対応している。

より専門的な対応が必要な場合には、委託業者の専門家が対応している。国際的な資格も有し、セキュリティの専門家集団が対応している。

2. 医療機器のサイバーセキュリティ確保について

医療機器に特化した形での問い合わせは今までない。

窓口としても医療機器に特化した内容については、対応できる準備はまだできていないが、今後検討していく。

診療所などではチームを作る事も難しいが、現状把握としては、医療機器も含めた情報資産の把握を進めることが重要である。その後の脆弱性対応やアップデートなどは自力でやることが難しいので、アウトソーシングや保守契約の中で対応する必要があるのではないか。ベンダーの協力も不可欠である。ネットワークの結線を確認し、院内の全員が情報セキュリティの重要性を認識して、資産の棚卸しする必要がある。

特に医療機器に特化した形としては、現物を確認したうえで、MAC アドレスの確認やポート番号、どのような機能を使用しているかなどを確認し、担当が分からず勝手に使われてしまわないようにする必要がある。定期的に監査をすることも重要であり、医療機器のソフトウェア情報も管理する必要がある。段階的にできるところから実施していく必要がある。アウトソースをうまく利用するなども必要である。

3. その他

医療機器のサイバーセキュリティについては医機連のほうで動いているとは思うが、情報システムの端末部分であるものの、個々の医療機器は範疇外と判断されて行き届いていないのではないか。

医療機器のサイバーセキュリティ確保についても、情報システムの大枠の中で動いていくべき話し。

専門人材を医療機関に配置できるわけではないので、すぐに相談できる体制を整備することが重要ではないか。

ネットワークに接続される端末機器の資産管理が必要であり、そのことは医療機関しか知り得ない。医療機関自身で進めて行く必要がある。

トップからの号令も必要。先立つものも無い状況では何もできないので、経営層にも理解いただく必要がある。

医療現場には分かりやすく、かみ砕いたうえで伝えるような資料が必要である。医師会でもオンラインセミナーをやったり、紙面で伝えたり動画を作成して啓発している。知ってもらうことが重要である。

サイバーセキュリティ支援制度の概要(4 つの制度)

①セキュリティトラブル相談（緊急相談窓口）（電話　年中無休　6-21 時　無料）：緊急対応

②セキュリティ対策強化に向けた無料サイトの提供：最新の情報、機関紙の提供、職員向け実践テキストなど

③サイバー攻撃一時支援金・個人情報漏洩一時支援金制度：被害時に 10 万円の支援など

④医療情報システムの安全管理に関するガイドライン・サーバーセキュリティ対策チェックリストに関する支援（電話　平日 9-18 時　無料）：平時の内容についての相談窓口、チェックリストを解説した分かりやすい動画の提供など 医療機関で幅広く使えるようなガイダンス的な資料や動画を掲載している。

別紙 2

一般社団法人日本臨床工学技士教育施設協議会へのヒアリング（要約）

目　的：臨床工学技士養成課程におけるサイバーセキュリティ確保に関する教育内容の確認及び、将来的に取り込む余地があるかなど、現状と課題について意見交換を行う。

いただいた主な意見：

○どの大学や専門学校も臨床工学の養成課程において、医療情報の講義や情報系の実習はあるが、サイバーセキュリティ単体の講義はない。学会の資格系では、サイバーセキュリティに関する内容を入れようとする動きはあるが、養成校のカリキュラム自体にはそれほど入っていない。

○臨床工学技士の教科書である医用情報処理工学は作成から 17－18 年経過し、かなりの割合で養成校の教科書で使われているが、最後の章でセキュリティ関係が少し入っている程度。第 2 版　2019 年　第 1 版 2010 年であり、第 2 版から入ったと記憶している。内容としては、政策の話、DOS 攻撃、セキュリティホール、個人情報保護等が中心

○2025 年 3 月に向けて、教科書を刷新する。現在、目次案を検討中である。セキュリティに関して図等を増やして多少ボリュームを増やす方向で検討中である。

○病院実習で実習のカリキュラムにはサイバーセキュリティに関することは入っていないが、実習先の病院との話合いの中で、電子カルテシステムを実習で見学するような場合もある。

○体系的の学習ではなく、守秘義務とか個人情報保護の観点からの内容であり、いわゆるサイバーセキュリティの観点からはほとんどふれない。

○実際、臨床業務が忙しいので、医療機関内で医療機器のサイバーセキュリティ対応について責任の押し付け合いになることも予想されるが、教育は必要。病院の中で対応するためには、手当、人材、教育を充実させるべきである。

○養成校レベルの情報教育では、国家試験に出てくる問題として、サイバー攻撃の種類とかファイヤーウォールの機能とかそういったレベル。

○医療情報部門にいる臨床工学技士もごくわずか。CE がすぐに実務部隊となるかは難しい。連携をするための橋渡しの役割を担うために、卒前教育と卒後教育をどうしていくかが重要ではないか。卒前と卒後の教育が一体となることも大事ではないか。

○医療機器のサイバーセキュリティ確保に向けた人材の裾野を広げるために育成していくことは必要である。医療機器側は患者に影響を与える可能性がある。

○上層部の理解も必要であり、診療報酬で対応してくれるのかも検討が必要。

○サイバーセキュリティ対策を実施してもお金を生まない。万が一の場合に被害を少なくすることはでき、医療機器の保守管理と同じように予防的に行うことが重要であるが、誰が責任をもつのか、医療機器安全管理責任者との連携も課題。

○医療の DX 化だけでなく、サイバーセキュリティ確保等の基盤の評価が必要であり、できてないところに費用工面をするような仕組みも必要ではないか。

別紙 3

A 大学病院へのヒアリング（要約）

目　的：医療情報システムに関して先進的に実践している医療機関でのサイバーセキュリティ対策および医療機器のサイバーセキュリティ対策に関する状況把握や課題について意見交換を行う。

いただいた主な意見：

○医療機器メーカが MDS 2 等のセキュリティ情報を開示すべき（現在はできていない）。MDS 2 を集めただけでは判断材料にならない。その使い方を明示すべき。

○セキュリティ対策は 1 か 0 かではなく、環境の変化についても継続的に対応する必要がある。

○セキュリティに偏りすぎ。実は BCP としてどうするかが主目的であり、セキュリティはリスクファクターの一つでしかない。全体でどう対応するか？が重要である。

○第三者機関なようなところで、まとめてペンテスト（ペネトレーションテスト　脆弱性を検証するテスト手法の 1 つ。侵入テストとも呼ばれる）を実施するのも一つの案。

○セキュリティ開示文書について、JIRA　JAHIS の書式でも対応されていない。さらには、そのような団体に参画していない企業をどうするかも課題である。

○CIFS/1.0（Common Internet File System）を使っているのも医療ぐらいなので、そのあたりから医療機器のサイバーセキュリティ確保のためには改善が必要である。

○サイバーセキュリティ対策を自分できるのが理想であるが、人材がいない。医療情報技師がいればある程度は対応できる。そのためにも、簡単にできる方法を広める必要がある。ペンテストのサーバを配ることや、共通ソフトを配る等が必要である。

○情報システムは点数で評価できない。導入したらお金がかかる。管理するための　CSIRT、ペンテストにもお金がかかる。ネットワーク設備についても同様で、医療の収益だけだと無理がある。

○医療機器も含めてサイバーセキュリティ確保のためには、医療情報技師の拡充、診療情報管理士の拡充が必要であるが、併せてキャリアパスの検討も必要である。

○医療情報技師であれば、医療に関する知識テストもあり医療のことも知っている。IT パスポート試験には医療は入っていないし、セキュリティも入っていない。その上の資格だとレベルが高すぎ、裾野は広がらない。

○サイバーセキュリティ確保のための人材育成⇒病院運営に必要なレベル、運用マネージャーレベルが必要

○ペンテストをアウトソースすると高い。 1 台いくらという世界。脆弱性の確認については、それほど高度な技術は必要なし。最低限できてないというレベルが判別できれば良い。各医療機関でベンチマークできると良いのではないか。それによって、保険の掛け金が安くなるとかの仕組みも必要。サイバーセキュリティの対策費やサイバー攻撃による減収まで対応できるよう

な保険も今後必要となるのではないか。

○医療機関の経営者が認識すること、共通指標で評価し、自己評価ができる仕組みが必要ではないか。

○医療機器系、部門システムのサイバーセキュリティ対策は希薄。

○現在ようやく、不要なサービスをとめたりしている。ひどい場合には、ファイヤーウォールの設定もしていないし、アップデートの確認などもしていない。チェックリストで点検、端末全数把握できるような仕組みが必要。

○医療機器メーカには、ネットワーク接続前に確認しても、仕様と言われる。導入時見て、指摘しても改善されない。（できない）PMDA はセキュリティの中身の評価ができていない。承認の段階でネット―ワーク、セキュリティを併せて確認してもらわないと、いざネットワークに医療機器を接続して使用するときに、問題が生じることになる。厚生労働省や PMDA 単独ではなく、他省と連携して、専門分野が得意な省庁と連携してセキュリティは別基準で対応する必要があるのではないか。

○実際に DDos 攻撃をモニタ機器に行ったところ、ICU でバイタルサインのモニタリングが実際に停止した。しかし、製造販売業者については、その対策は承認の関係でできず、新製品では対応されている。使用する環境への配慮が足らないがそれでも、製造販売承認は下りてしまう。

○サイバーセキュリティについては、ランサムだけではない。DDos の方が怖い。医療機器のサイバー攻撃の可能性については海外では結構報告例がある。検査データの改ざんもあり得る。医療機器導入の際にその情報が情報部門にも共有され、サイバーセキュリティの観点からも確認している。基本的には、ネットワーク機器は全て情報部門で管理しているが、チェックをして指摘はするものの、その後の管理などそれ以上はできていない。

○ネットワークに接続される医療機器のポートスキャンだけでも実施した方が良い。メーカに確認する必要があるが、何番ポート使っているかも現時点では開示されていない。医療機器側の義務として、そのような情報を開示してもらう必要もある。実際のポートスキャンについては、フリーでソフトもある。サイバーセキュリティ対策の初歩としては、ポートのスキャンが基本。可能であれば、攻撃を加えて動作状況を確認することもできる。

○医療機器のサイバーセキュリティに関して、医療機関の管理者として知っているべき要件や具体にやることについての推奨を出した方が良いのではないか。

別紙 4

12 医療機関へのヒアリングシート

基本情報（病床数、施設基準、従業員数）

1. 医療情報システムに関するサイバーセキュリティ確保について
   1）管理する組織体制（職種・人数・役割）
   2）ネットワーク構成図の把握
   3）ネットワーク構成図は誰が作成して、誰が管理
   4）追加のシステムなどはどのように情報を入手して管理しているか
   5）メーカ等に対してネットワーク構成図を開示しているか（契約による場合も含む）
   6）情報システムに関する脆弱性情報はどのように入手して、どう活用しているか
   7）IT-BCPを作成しているか
      また、その中に医療機器に関してはどのような形で入っているか？

2. 医療機器のサイバーセキュリティ確保について
   1）ネットワークに接続される医療機器についてどう管理しているか
   2）管理している場合には、どのような管理体制（誰が・どこまで）をとっているか
   （医療情報システムとの違いがあるか）
   3）医療機器等も含めてネットワーク構成図を把握・管理しているか
   把握・管理している場合、 医療機器に関しては特に何を把握・管理すべきか
   4）医療機器のＯＳのバージョンアップやウイルス対策などを確認しているか
   5）医療機器に関する脆弱性情報はどのように入手して、どう活用しているか
   6）医療機器のサイバーセキュリティ確保について参照しているガイドライン等
   はあるか
   7）医療機器のサイバーセキュリティ確保に向けた医療機器特有の情報として、
   MDS2、SBOM、レガシー状態があるが、この情報はどう管理しているか
   8）医療機器メーカから、MDS2、SBOM、レガシー状態に関する情報は提供されるか
   9）医療機器のサイバーセキュリティ確保に向けた、臨床工学部門や放射線部門、
   医療機器安全管理責任者、情報システム責任者、医療安全管理者などの連携
   体制を構築しているか、構築している場合は、その内容について
   10）医療機器のサイバーセキュリティ確保について、誰がどこまで把握して、各分野
   において主体となって動くのは誰か、また、その人材として必要な知識、技術、
   人数はどうか
   11）既存システムとの整合とセキュリティ対策の望ましい体制、人材配置はどう考えるか
   （院内の連携体制なども含めて）

12）医療機器のサイバーセキュリティに関するインシデントやアクシデントが発生した場合の対応はどう行う想定しているか（周知も含め、シナリオはあるか、提供可能か）

13）医療機器のサイバーセキュリティ確保に向けて、医療従事者や在宅で使用する患者に対して、研修などをおこなっているか、行っている場合は、その内容

14）医療機器のサイバーセキュリティ確保について、重要なポイントは何か（医療機器の日常的な点検で必要な項目など）

15）医療機器を導入する際に、サイバーセキュリティ確保に関して医療機器製造販売業者との責任分界点を契約内容の中に盛り込んでいるか。 盛り込んでいる場合は、その内容

16）医療機器のサイバーセキュリティ確保に関して、医療機器の製造販売業者との連携をしているか、している場合の具体的連携

17）医療機器のサイバーセキュリティ確保に関して、経営層と情報を共有しているか。している場合は、どのような情報を共有しているか

18）医療機器のサイバーセキュリティ確保に関して、保守契約を結んでいるか、結んでいる場合、どのような内容か、契約書は提供可能か

病院名	A病院
病床数	約400床
施設基準：主たる基準	≪基本診療科施設基準届出≫ ・一般病棟入院基本料1 急性期看護補助体制加算(50対１) 看護補助体制充実加算1 ・地域包括医療病棟入院料 看護補助体制加算(50対１) 看護補助体制充実加算1 ・回復期リハビリテーション病棟入院料3
従業員数：	
医師数	常勤49名
看護師数	211名
臨床工学技士数	10名
その他職種（メディカルスタッフと事務職等）	臨床検査技師22名、診療放射線技師20名、薬剤師15名
1. 医療情報システムに関するサイバーセキュリティ確保について	
1）管理する組織体制（職種・人数・役割）	情報室3名で対応。全員事務職　内医療情報技師2名。実務的には医師はほとんど関与していない。管理組織としての委員会に医師が入っているので、院長も把握はしている。委員会規程では、**部門システムの管理者や端末機器の管理者も定めている。**委員会の規程については、1年に1回は見直したいところであるが、実際には、監査や病院機能評価のタイミングで見直しをしている。その際には、他院の情報も取り入れながら、見直してをしている。他院の情報については、ベンダーを通して情報を入手している。システム保守についても、3名がオンコール体制で対応している。プリンタが詰まったということで、呼ばれることも。特に委託はしておらず、情報システム系の全てを対応している。端末機器の引っ越しなどの対応もしている。検診システム別システムであり、連携はしているが、別部署が管理している。
2）ネットワーク構成図を把握しているか？	情報システム更新後に把握するように改善した。
3）ネットワーク構成図は誰が作成して、誰が管理しているか？	委託業者に依頼して、ネットワーク構成図を作成。 情報システム自体も大手ではなく、地方のベンダーを利用
4）追加のシステムなどはどのように情報を入手して管理しているのか？	保守契約を行い、追加工事の際にも一括で委託業者が管理。無線は医局に1本引いているが別回線で使用。ただし、部門システムまでの構成図はできていない。部門システムやそれに接続する医療機器等については、構成図には反映できず、情報部門からは見えない状況にあるのが課題。各部門での管理となる。
5）メーカ等に対してネットワーク構成図を開示しているか？（契約による場合も含む）	開示していない。申請があれば、必要に応じてIPアドレスを払い出し。
6）情報システムに関する脆弱性情報はどのように入手して、どう活用しているか？	ニュースや県警などから情報を入手。県警と合同でセキュリティの勉強会も実施。警察が直接病院に来ていただき、講師として、情報セキュリティについて講習を実施。知り合い経由で警察に依頼したところ、実現となった。パッチなどは基本あてていない。情報システムの安定稼働を重視し、更新の際に最新にするような運用。
7）IT-BCPを作成しているか？ご恵与いただくことは可能か？また、その中に医療機器に関してはどのような形で入っているか？	IT-BCPがまだ作成できていない。作成する方法もわからないので、見本が欲しい。
2. 医療機器のサイバーセキュリティ確保について	

病院名	A病院
1）ネットワークに接続される医療機器についてどう管理しているか？	ネットワークに接続する際には、声をかけてもらうような運用。部門システムの責任者が対応することになっている。いただいた情報は**IPアドレスの払い出し情報とともに、台帳で管理（機器名、使用場所など）**。
2）管理している場合には、どのような管理体制（誰が・どこまで）をとっているのか？（医療情報システムとの違いがあれば。）	ネットワークに接続する機器については、情報システム課に報告することとなっている。選定は各部門で、実際の購入は総務が担当するが、職員同士連携して対応している。ベンダーからの連絡も多い。
3）医療機器等も含めてネットワーク構成図を把握・管理しているか？ 把握・管理している場合、医療機器に関しては特に何を把握・管理すべきか？	医療機器等については、ネットワーク構成図までに落とし込めていない。リモート接続は要件を出しているが、会社で対応できないということで、結果的には許可されている事例はない。どこまでを責任分界とするか指標が難しい。
4）医療機器のＯＳのバージョンアップやウイルス対策などを確認しているか？	できていない。**診療側では知識がないので、わからない**。教育されていないので、言われても理解ができない。
5）医療機器に関する脆弱性情報はどのように入手して、どう活用しているか？	**情報が情報システム課にはあがってこない**。
6）医療機器のサイバーセキュリティ確保について参照しているガイドライン等はあるか？あれば、ご教示いただきたい。	**ガイドラインについて知ってはいるが、見ているだけで具体のアクションはない。**今回の研究班によって始めて知った。**ビジュアルで分かるようにしてほしい。**
7）医療機器のサイバーセキュリティ確保に向けた医療機器特有の情報として、MDS2、SBOM、レガシー状態があるが、このような情報はどう管理しているか？	**このような情報があることを知らない。医療機器のサイバーセキュリティ確保に関する通知を病院団体から発出されたことを確認したことがない。医政局や保険局の事務連絡は通知されている。実働部隊がいない。**
8）医療機器メーカから、MDS2、SBOM、レガシー状態に関する情報は提供されるか？	メーカから提供はされない。聞いた事もない。
9）医療機器のサイバーセキュリティ確保に向けた、臨床工学部門や放射線部門、医療機器安全管理責任者、情報システム責任者、医療安全管理者などの連携体制を構築しているか？構築しているようであれば、その内容をご教示いただきたい。	特に医療機器安全管理責任者と連携していることはない。
10）医療機器のサイバーセキュリティ確保について、誰がどこまで把握して、各分野において主体となって動くのは誰か？また、その人材として必要な知識、技術、人数をご教示いただきたい。	できていない。OSの把握等について、医療機器に関しては把握できていない。
11）既存システムとの整合とセキュリティ対策の望ましい体制、人材配置をどう考えるか？（院内の連携体制なども含めて）	病院ごとの指標があるとありがたい。**医療機器についても、セキュリティを管理する責任者がいて、情報システムと連携して対応していけると良い。**
12）医療機器のサイバーセキュリティに関するインシデントやアクシデントが発生した場合の対応はどう行う想定か？（周知も含め、シナリオがあればご恵与願いたい）	想定できていない。シナリオがあれば、こちらも欲しい。

病院名	A病院
13）医療機器のサイバーセキュリティ確保に向けて、医療従事者や在宅で使用する患者に対して、研修などをおこなっているか？行っていれば、その内容をご教示いただきたい。	できていない。
14）医療機器のサイバーセキュリティ確保について、これだけは押えておいた方が良いというポイントがあれば、ご教示いただきたい。 （医療機器の日常的な点検で必要な項目などあれば。）	わからない。
15）医療機器を導入する際に、サイバーセキュリティ確保に関して医療機器製造販売業者との責任分界点を契約内容の中に盛り込んでいるか。盛り込んでいるようであれば、その内容をご教示いただきたい。	盛り込んでいる内容はない。
16）医療機器のサイバーセキュリティ確保に関して、医療機器の製造販売業者との連携をしているか？しているようであれば、どのように連携しているか？	**医療機器メーカとの連携はない。メーカから情報を教えてほしい。物は売りにくるが、情報は持ってこない。卸からの情報もない。**見積もりや請求書は持ってくるのが早い。メーカからの情報をWEB上で情報共有ができる仕組みがあるとありがたい。
17）医療機器のサイバーセキュリティ確保に関して、経営層と情報を共有しているか。している場合には、どのような情報を共有しているか？	今回の研究班をきっかけに病院長と共有している。
18）医療機器のサイバーセキュリティ確保に関して、保守契約を結んでいるか？結んでいる場合、どのような内容か？ 可能であれば、契約書をご教示いただきたい。	費用面の問題もあり、保守契約は結べていない。
その他意見	○インフラを整備する予算が不足している。今回の診療報酬改定でも、診療録管理体制加算が1から2に下がってしまった（バックアップのオフラインでの保管ができないため。）。補助金でも1/3補助とか2/3補助が現実なので、利益率1-2%の中で、補助金にも手が出せない。ネットワーク調査には補助金が使えたが、バックアップには使えなかったので、結果的に、1⇒2に下がってしまった。 ○実際に診療情報管理体制1を取得している病院の情報などが欲しい。現在は、過去の経験などを活かして人脈で情報を入手している。 ○**病床数や機能によって、対応が違うので、何をまねしていいのかも分からない。病院規模別、機能別の具体的な対策のひな形を望む。**
追加情報	○中央の情報システムは買い取り。サーバ保守が続く限り使用する。部門システムは別予算で更新。過去はネットワーク障害が多かったが、ネットワーク設備を更新することで、障害は減った。 ○電子カルテ端末からインターネットは使用できない。院内メールは電子カルテ端末で利用できるが、外部へのメール発信は別パソコンでの運用としている。 ○セグメンテーションを切って管理していないが、セグメンテーションを切って管理した方が良いか分からない。

病院名	B病院
病床数	約100床
施設基準：主たる基準	・一般病棟入院基本料　急性期一般入院料1 急性期看護補助体制加算(25対１) 看護補助体制充実加算2
従業員数：	
医師数	32名
看護師数	111名
臨床工学技士数	0名
その他職種（メディカルスタッフと事務職等）	172名
1. 医療情報システムに関するサイバーセキュリティ確保について	
1）管理する組織体制（職種・人数・役割）	情報管理室2名。病院システム全般的な管理。ウイルスソフトの管理画面で病院内のウイルス管理。 →**VPNの設置費用や管理については、設置したベンダーの責任で対応。**ワークステーションなどで費用なVPNは個別で対応し、**システム関係のVPNはひとつに統合**している。**情報系VPNの管理は電子カルテメーカーにお願い**している。検査系については、情報システムのVPNから入るようにしている。 **部門システムのメンテナンスは各部門で対応。**遠隔で保守する場合もある。手術部門システムは定期メンテの中でVerアップなどで対応している。（契約に含まれる。） 導入の際には各部門から情報管理室へ連絡がある。 **各部署の院内窓口を決めてもらっている。**ベンダーから見ると情報管理室、各部門窓口のどちらも病院の窓口として機能するようにしている。メインとサブというようなイメージ。 以前は担当者が短期間で交代していたため連携ができていなかったが、現在の担当者は10年以上の経験があるので、時間をかけて連携して対応ができるようになった。
2）ネットワーク構成図を把握しているか？	はい。
3）ネットワーク構成図は誰が作成して、誰が管理しているか？	ネットワーク業者が作成している。簡易版を病院で作成している。
4）追加のシステムなどはどのように情報を入手して管理しているのか？	システム関連の情報であれば、ベンダーから情報を入手します。
5）メーカ等に対してネットワーク構成図を開示しているか？（契約による場合も含む）	原則、開示していません。
6）情報システムに関する脆弱性情報はどのように入手して、どう活用しているか？	厚労省、全日本病院協会、ベンダーからの通知で入手しています。ルーターなどセキュリティ機器のファームウェアは常に最新状態。 →情報システム関係の脆弱性については、対応しているが、機器側については、どう対応すれば良いか分からない。情報システムについては、外のデータセンターにデータバックアップをしている。（市販のサービスを利用）リアルタイムバックアップが可能で、世代管理も実施している。
7）IT-BCPを作成しているか？ご恵与いただくことは可能か？また、その中に医療機器に関してはどのような形で入っているか？	可能です。※医療機器を特定した形では入っていません。シナリオを作成して随時アップデートを行う予定。 ※IT-BCPについて　協議会とともに医療機関用の訓練用ロールプレイングシナリオを作成中 →トラブル時のマニュアル自体の整備はしていないが、**サイバー攻撃に備えたアクションカード**をまとめて、これに沿って各部門で対応することとしている。
2. 医療機器のサイバーセキュリティ確保について	

病院名	B病院
1）ネットワークに接続される医療機器についてどう管理しているか？	情報管理室では、IP管理しています。 →検査、大型機器などは部門で管理。
2）管理している場合には、どのような管理体制（誰が・どこまで）をとっているのか？（医療情報システムとの違いがあれば。）	医療機器の管理は、メーカーとの連絡が密となるため、部署単位で行っている。
3）医療機器等も含めてネットワーク構成図を把握・管理しているか？ 把握・管理している場合、医療機器に関しては特に何を把握・管理すべきか？	放射線科ネットワークについては、**放射線科にてIPと設置場所など管理**している。（ＣＴ、ＭＲＩ、ワークステーション、エコー等）
4）医療機器のＯＳのバージョンアップやウイルス対策などを確認しているか？	医療機器のウィルス対策は病院側では行っていない。 ・OSバージョンアップは動作保証の問題があり、行っていない。（一部機器については、有償でのバージョンアップ対応が可能である。） ・**一部でベンダー側が脆弱性チェックを行う覚書を交わしている。** →覚書きに定期的に脆弱性のチェックをすることを明記。異常がある場合に連絡。対応については、ベンダー対応であるが、費用分担の記載はない。機器の保守契約の範囲であれば、ベンダーが対応する。今後、更新の際に、このような記載を横展開していく。
5）医療機器に関する脆弱性情報はどのように入手して、どう活用しているか？	メーカーからの通知を入手している。 内容を検討してバージョンアップなどの検討は行う。 メーカーからの無償パッチは、積極的に適用する。 →実際的には、機器側については、どう対応すれば良いかわからない。機器側トラブル→パソコン側で検知されると思っている。
6）医療機器のサイバーセキュリティ確保について参照しているガイドライン等はあるか？あれば、ご教示いただきたい。	医療情報システムの安全管理に関するガイドライン　第6.0版 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 →医療機関における医療機器のサイバーセキュリティ確保のための**手引きも今回初めて見た**が、初めて見る内容が多い。**何をすれば良いのかわからないので、チェックリストなど具体のやり方を教えて欲しい。**手引きを読んでも全くわからない。玉を投げるだけでなく、拾いやすくして欲しい。
7）医療機器のサイバーセキュリティ確保に向けた医療機器特有の情報として、MDS2、SBOM、レガシー状態があるが、このような情報はどう管理しているか？	メーカーからも情報を入手していない。 →レガシー機器の対応については、10年ぐらいで更新をしているため、それほど問題とはなっていない。経営的には何とか更新できている。
8）医療機器メーカから、MDS2、SBOM、レガシー状態に関する情報は提供されるか？	メーカーからも情報を入手していない。
9）医療機器のサイバーセキュリティ確保に向けた、臨床工学部門や放射線部門、医療機器安全管理責任者、情報システム責任者、医療安全管理者などの連携体制を構築しているか？ 構築しているようであれば、その内容をご教示いただきたい。	医療機器に特化していませんが、**サイバーセキュリティ対策委員会を立ち上げて各部署連携**している。 →規約の中で、連携して対応するように明記している。
10）医療機器のサイバーセキュリティ確保について、誰がどこまで把握して、各分野において主体となって動くのは誰か？ また、その人材として必要な知識、技術、人数をご教示いただきたい。	各部署が対応を行い、問題発生時は情報管理室で対応にあたります。 **監視やインシデント対応、教育やセキュリティ対策などのセキュリティやネットワーク管理として法人で2名欲しい。**
11）既存システムとの整合とセキュリティ対策の望ましい体制、人材配置をどう考えるか？（院内の連携体制なども含めて）	SOC(監視）やCSIRT(インシデント対応やセキュリティ教育)を整備して、セキュリティ担当チームから、SOCや各部署との連携体制をとりたい。
12）医療機器のサイバーセキュリティに関するインシデントやアクシデントが発生した場合の対応はどう行う想定か？（周知も含め、シナリオがあればご恵与願いたい）	動作不良など、初期対策で各部署とメーカで対応を行う。サイバーセキュリティの可能性があれば、IT-BCP発動へのシナリオへ移行。

病院名	B病院
13）医療機器のサイバーセキュリティ確保に向けて、医療従事者や在宅で使用する患者に対して、研修などをおこなっているか？行っていれば、その内容をご教示いただきたい。	病院スタッフへは情報セキュリティ研修を行う。佐賀県警セキュリティ研修や全日病DX人材育成プログラムの内容から研修動画を作成する。11月に行う予定。
14）医療機器のサイバーセキュリティ確保について、これだけは押えておいた方が良いというポイントがあれば、ご教示いただきたい。 （医療機器の日常的な点検で必要な項目などあれば。）	医療機器の正常な動作を確認する。
15）医療機器を導入する際に、サイバーセキュリティ確保に関して医療機器製造販売業者との責任分界点を契約内容の中に盛り込んでいるか。盛り込んでいるようであれば、その内容をご教示いただきたい。	新しく契約を更新しているものから、内容を盛り込んでいる。
16）医療機器のサイバーセキュリティ確保に関して、医療機器の製造販売業者との連携をしているか？しているようであれば、どのように連携しているか？	動作不良など判明した時点でメーカーと対応する。
17）医療機器のサイバーセキュリティ確保に関して、経営層と情報を共有しているか。している場合には、どのような情報を共有しているか？	医療機器に限らず、動作不良やシステム不良時は状況を院長・事務部長と情報共有している。
18）医療機器のサイバーセキュリティ確保に関して、保守契約を結んでいるか？結んでいる場合、どのような内容か？ 可能であれば、契約書をご教示いただきたい。	医療機器のサイバーセキュリティ保守契約は結んでいないが、脆弱性のチェックに関しては横展開するように今後は追加する予定。
その他意見	○**現実的には一人で対応することはできない**。情報システムから見ると部門システムは専門外。部門システムから見ると情報システムは専門外。**お互いわからないところがある**ので、必要時に連携して対応するしか方法がない。 ○**サイバー攻撃はコロナよりかかりやすく、部門システムから入りやすい。**職員にも浸透させる必要がある。 ○**輸液ポンプやシリンジポンプがネットワークに繋がるような認識はない。**今後業者とも話し合う必要がある。 ○**医療機関向けの第三者的なセンター**が欲しい。**メーカーとつなぐ、情報を流通して整理するようなところ。公的な集団**が欲しい。医療機関では、**セキュリティに関する人材は集められない。給与も低い。** ○**医療機器まで含んだ院内規程の参考となるものが欲しい。**
追加情報	○放射線関係のシステムは部署長が管理を担当することになる。機器の選定をしているので、その流れでシステムについても管理担当となっている。 ○手術室のシステムについては、麻酔科医師と連携して対応している。手術室を担当する主任看護師がメンテナンスなどを対応することになる。その他の部門システムについては、気がついた時に対応している。経験が長く、医療機器安全管理責任者としても対応している。 ○検査部門のシステムは主任が対応を任命されている。 ○サイバー攻撃の対応訓練として、関連病院を中心に、**協議会の支援を得て、訓練をサイバーセキュリティ対策委員会を中心に机上訓練**を実施予定。 →セキュリティ対応については、専門家でないので、何をどうすれば良いかわからない。地域セキュリティ協議会は、医療だけでなく、警察、セキュリティの専門家、大学の情報管理部門の関係者が集まり協議会を設置。医療介護系のセキュリティ強化を目的に、非営利に近い団体。ネットワークを作り、BCP、サイバー対策の相談窓口としても機能することを目指している。 →1-2時間で1つの部署完結で行うような訓練。病院関係者がいないと説得力がないということで、病院関係者が理事として、協議会に入っている。**セキュリティのプロと現場をなじませる。共通言語を作る等、現場に落とし込む形での訓練を実施し、それを横展開**していくことを考えている。厚労省のガイドラインの解釈の違いについても、相談に乗っている。 ○全日病でも個人情報の研修会があり、その中でセキュリティに関する内容も入っているが、セキュリティ単体の研修はない。 ○診療放射線技師会では、情報セキュリティに関する勉強会はあるが、養成課程では情報セキュリティに関する内容はほとんどない。臨床検査技師も同じような状況。 ○看護師教育では、セキュリティ内容も入っている。医療情報に関する内容もカリキュラムに入ってきている。

病院名	C病院
病床数	約500床
施設基準：主たる基準	一般病棟入院基本料(急性期) 急性期充実体制加算 急性期看護補助体制加算 2(25対１) 看護補助体制充実加算
従業員数：	
医師数	
看護師数	
臨床工学技士数	
その他職種（メディカルスタッフと事務職等）	
1. 医療情報システムに関するサイバーセキュリティ確保について	
1）管理する組織体制（職種・人数・役割）	職種：情報部長の医師1名（兼任）、事務職員3名（専任）、外部委託業者7名 役割：医療情報に関わる導入、運用、保守、ヘルプデスク →医療情報システム系はある程度、医療情報部で抑えているが、**医療機器については、契約で購入しており、抑えていない。ベンダーと各現場とのやりとりで対応しているのが実情。HIS側は何とかなるが、医療機器までは到底対応できない。** 部門システムの管理は各部門の管理者が行っている。情報管理委員会はあるが、しばらく開催していなかったので、今後開催して、IT-BCPの承認などを得ていく予定である。また、医療機器に関する動きも情報共有していく。外部委託者はヘルプデスクと運用を行う。ネットワークの検知まで行うが、トラブル対応はベンダーにお願い。情報部は橋渡し的な役割。
2）ネットワーク構成図を把握しているか？	ネットワーク構成図のうち物理構成図はシステム更新時に作成し、必要に応じて更新を行っているが、必ずしも最新版ではない。理論構成図に関しては、設定変更の度にネットワーク業者より更新データが納品される。また、現状、構成及び機能などを全て把握できているわけではない。 →情報部範囲のネットワーク構成図はあるが、その先は各部門での管理。各部門でもそれほど認識は高く無い。その場でやっている感じ。リモートメンテの希望が多い。申請ベースで管理しているため、使わない時でも残ってしまう。**ネットワーク資産の棚卸しをどうするかが課題。**
3）ネットワーク構成図は誰が作成して、誰が管理しているか？	ネットワーク構築業者が作成し、納品したものを使っている。その後の変更等も業者に依頼した場合は、完成図書を納品してもらっている。
4）追加のシステムなどはどのように情報を入手して管理しているのか？	HIS系ネットワーク及び情報系ネットワークに接続するシステムの場合、接続するためには、情報部が管理しているIPアドレス、証明書などの情報がないと接続できない仕様になっている。そのことから、必然的に新たなシステムを導入する際は、事前に情報部に相談いただく流れとなっている。
5）メーカ等に対してネットワーク構成図を開示しているか？（契約による場合も含む）	医療機器メーカーには基本的に開示していない。求められれば、必要に応じて部分的に開示することはある。
6）情報システムに関する脆弱性情報はどのように入手して、どう活用しているか？	（入手先） ・厚労省、県庁及び協議会からの通知 ・IPAからのメール配信 ・電子カルテベンダー及びネットワークベンダー等の業者からの連絡 ・県警からの情報提供 （活用） ネットワーク機器等に脆弱性情報に合致するものがあるか確認し、合致するものがある場合は、速やかに対象ベンダーへ対策依頼を行う。
7）IT-BCPを作成しているか？ご恵与いただくことは可能か？また、その中に医療機器に関してはどのような形で入っているか？	現在、初版を作成中。完成後の提供は問題ない。現時点では、医療機器に関してはほぼ出てこない状況で、ベンダーに協力を得て感染している・していない、対策を依頼するフローとなっている。
2. 医療機器のサイバーセキュリティ確保について	

病院名	C病院
1）ネットワークに接続される医療機器についてどう管理しているか？	厚労省のサイバーセキュリティ確保事業を契機に現在洗い出しをし、脆弱性のチェックをしようとしている。 →IPを払い出しているのみで、細かいところまでは把握していない。
2）管理している場合には、どのような管理体制（誰が・どこまで）をとっているのか？ （医療情報システムとの違いがあれば。）	現時点では、電子カルテなどの医療情報システムは医療情報係が管理し、部門調達の医療機器（医療機器に付随するシステムを含む）は契約係で契約・管理、各部門で運用をしている。
3）医療機器等も含めてネットワーク構成図を把握・管理しているか？ 把握・管理している場合、医療機器に関しては特に何を把握・管理すべきか？	医療機器は含まれていないネットワーク構成図はある。※一部は理論構成図（ＩＰアドレス管理）は存在する。 →**機器までの配線管理はできていない。**
4）医療機器のＯＳのバージョンアップやウイルス対策などを確認しているか？	医療機器に関しては、契約係で調達していることもあり、契約係とディーラー間で対応を行っている。
5）医療機器に関する脆弱性情報はどのように入手して、どう活用しているか？	ディーラーからの報告等で把握しており、必要がある場合は対応を行っている。
6）医療機器のサイバーセキュリティ確保について参照しているガイドライン等はあるか？あれば、ご教示いただきたい。	・医療情報システムの安全管理に関するガイドライン6.0 ・セキュリティ教育支援ポータルサイト ・ほか医療機関のIT-BCP ・医療機関における医療機器のサイバーセキュリティ確保のための手引き書 →手引き書を見てはいるが、**最もな事を書いている反面、今全部やれとなるとパンパワーがない。今までの流れを考えるとレベルが高く、実際やるのが難しい。**
7）医療機器のサイバーセキュリティ確保に向けた医療機器特有の情報として、MDS2、SBOM、レガシー状態があるが、このような情報はどう管理しているか？	現時点では管理できていない。MDS/SDSに関して昨年度末に開示を求めた。
8）医療機器メーカから、MDS2、SBOM、レガシー状態に関する情報は提供されるか？	医療情報係で調達したシステム等は、MDS/SDSに関して昨年度末に開示を求めた。部門システム（レガシー医療機器を含む）は、把握できていない。
9）医療機器のサイバーセキュリティ確保に向けた、臨床工学部門や放射線部門、医療機器安全管理責任者、情報システム責任者、医療安全管理者などの連携体制を構築しているか？ 構築しているようであれば、その内容をご教示いただきたい。	まだできていない。
10）医療機器のサイバーセキュリティ確保について、誰がどこまで把握して、各分野において主体となって動くのは誰か？ また、その人材として必要な知識、技術、人数をご教示いただきたい。	医療情報システム障害発生時連絡体制図に沿って、動く想定だが、人材として必要な知識、技術、人数はまだ試算できていない。 また、現時点では医療情報システムが主であり、医療機器を含めたものについては、別の管轄部署と調整しながら今後行う必要あがると考えられる。
11）既存システムとの整合とセキュリティ対策の望ましい体制、人材配置をどう考えるか？ （院内の連携体制なども含めて）	現在は、医療情報システムと医療機器の調達管理担当部署が異なっており、情報が共有されることが少ない状況である。そのため情報共有できる体制を作る事が望ましいと考えている。なお、現状、医療機器調達担当及び医療情報システム担当者は事務職員が担っているため、セキュリティを含む必要な知識を持った人材を配置することが望ましいと考える。
12）医療機器のサイバーセキュリティに関するインシデントやアクシデントが発生した場合の対応はどう行う想定か？ （周知も含め、シナリオがあればご恵与願いたい）	現在、医療情報システムに関しては、IT-BCPを作成中。他院のIT-BCPを参考にしている。今年度中には病院情報システムに関するIT-BCPを作成予定であり、その後医療機器もふまえた内容に改訂していく必要があると考えられる。

病院名	C病院
13）医療機器のサイバーセキュリティ確保に向けて、医療従事者や在宅で使用する患者に対して、研修などをおこなっているか？行っていれば、その内容をご教示いただきたい。	（職員向け） ・医療従事者：1回/年の情報セキュリティに関する研修を必修としている →医療に関わるところより、一般的なセキュリティ教育。一般的なセキュリティ研修　県警職員が講師。協議会研修会でサイバーセキュリティ対策講習 机上訓練を実施（一般的なサイバーセキュリティ訓練） （在宅患者） ・在宅患者さんには、**レンタル会社などから酸素やポンプなどが貸し出されているが、サイバー攻撃の影響が考えられるものがないと思われる。** ・在宅患者さんには研修などは行っていない。
14）医療機器のサイバーセキュリティ確保について、これだけは押えておいた方が良いというポイントがあれば、ご教示いただきたい。 （医療機器の日常的な点検で必要な項目などあれば。）	・医療機器の一覧を最新にしておく運用をする ・ＯＳやバージョンを最新にしておく運用をする ・通常のログ状態の把握と異常の検知 ・IT-BCPのブラッシュアップと訓練
15）医療機器を導入する際に、サイバーセキュリティ確保に関して医療機器製造販売業者との責任分界点を契約内容の中に盛り込んでいるか。盛り込んでいるようであれば、その内容をご教示いただきたい。	現状、保守範囲や個人情報の取り扱いに関しては、契約書等で定めているが、**サイバーセキュリティ確保に関する責任分界点は定めていない。**
16）医療機器のサイバーセキュリティ確保に関して、医療機器の製造販売業者との連携をしているか？しているようであれば、どのように連携しているか？	連携のルールなどは定められていない。現状は必要に応じてディーラーから担当者に連絡されている。
17）医療機器のサイバーセキュリティ確保に関して、経営層と情報を共有しているか。している場合には、どのような情報を共有しているか？	IT-BCP、遠隔地バックアップなど個別には共有することがあるが、全体として共有はできていない。医療機器に関しては、必要に応じて、供覧・起案等で情報共有を行っている。
18）医療機器のサイバーセキュリティ確保に関して、保守契約を結んでいるか？結んでいる場合、どのような内容か？ 可能であれば、契約書をご教示いただきたい。	結んでいない。
その他意見	○**ベンダーもピンキリであり、会話にならないところもある。**何のこと？と言いながら**勝手に接続していることもある。**外資系はしっかりしているが、**今後契約で縛り、外部との接点は1本化していく必要がある。** ○**IT資産台帳が必要。**勝手に接続すると警報が出るような仕組みがあると良い。しかし、**誰が管理するかが課題。** ○**サイバーについての契約をしていないので、有事の時に協力が得られるか**も課題。 ○**資産台帳と紐付けて、サイバーリスクを管理できるような台帳が必要。** ○現状把握が大変であり、ネットワーク資産の棚卸し、ログの管理が難しい。**セキュリティと医療情報分野は別に管理**することでも良いのではないか。**良心的なコンサルが指南してくれ、仕組み作りをサポート**いただけると良い。 ○素人でもさわりが分かるようにしてもらわないとお手上げ。専門の人に丸投げする場合、検証ができないことも怖い。**セキュリティの仕様書のひな形ができると便利**であり、最低限これだけやるようなことがあると良い。ただ、固めすぎると参入業者が来なくなり、費用も高くなるので難しいところ。 ○医療機器の**認可の段階で標準的な仕様で開発**してもらい、セキュリティが問題ない機器を販売してもらわないと困る。**広まった段階で何とかせよと言っても対応できない。** ○**セキュリティができる人材は取り合い。**
追加情報	○HIS系、インターネット系、学術系で分けている。 ○2020年7月にHISはリプレース。次回は2027年予定。今年度基本方針を策定予定。部門システムについても要望が上がってくれば、同時に更新する。 ○厚労省の支援事業として、今年の春ぐらいに、**外部との接点や脆弱性のチェックを行ってくれる事業があったので、参加している。**各部門のベンダーが見えなかったので、契約の方に、ベンダー各社の情報を出してもらって、そこにメールで一斉配信して、外部接点について確認しているところ。おおよそ返答があり、リスト化できつつある。厚労省の事業で、委託側との接点の調査と脆弱性のチェックをしつつ、現場確認や診断結果をいただけるような事業。外部接点があるかどうかの確認が主目的で、それにぶら下がる端末機器や医療機器等は今後の検討となる。放射線や検査関係が多かった。情報部が把握していない**20～30の外部接続の可能性が確認できた。** ○機器更新は比較的できており、古くなったOSと言うようなコメントもあり、レガシー機器については、更新で対応できている。保守が切れるからというのが更新理由で多い。フルメンテが多い。移転した際にほぼ新規で購入した。

病院名	D病院
病床数	約600床
施設基準：主たる基準	特定機能病院
従業員数：	1574人
医師数	443人（医師　435人、歯科医師8人）
看護師数	648人
臨床工学技士数	24人
その他職種（メディカルスタッフと事務職等）	459人
1. 医療情報システムに関するサイバーセキュリティ確保について	
1）管理する組織体制（職種・人数・役割）	職種：医師、看護師、医療情報技師、事務職員、技術補佐員 人数：13人 役割：病院情報システムの運用・保守 →上記は基本、情報システム本体の対応。**部門システムについては、部門で対応**いただいている。各部門とは、調整会議で連携を図っている。情報部は情報部+学術管理部門　併せて13人。委託業者は入っていない。放射線関連のシステムは診療放射線技師が対応。副技師長を担当として任命している。副技師長の中で適任者を選任している。 小さい部署については、情報部でもサポートしている。基本的には、ネットワークに接続する際は、情報部へ連絡が来ることになっている。仕様策定の段階で情報部も加わる。 情報部ではHIS系のネットワークと学術系のネットワーク両方を管理している。 放射線機器や検査機器以外の医療機器については、基本的にはネットワークには接続していない。切り離して使用しているのが現状。接続する場合には、情報部に相談して対応。**メーカと臨床工学部門、情報部の三者協議で対応している。**
2）ネットワーク構成図を把握しているか？	ネットワーク完成図、統合管理システムのマップ上で把握 →HIS系や学術系の配線図は、情報部で管理している。最新化については、都度、新システム導入時に都度委託業者が対応。情報システム系については、委託している。部門システムの配線図は各部門での管理。部門システムで電子カルテに繋がらないものやリモートメンテに必要な接続は学術系のネットワークで対応。内容によって対応している。以前は別の配線を引いていたこともあったが、HISの更新の際に、一本化して現在は、**基本外部からの接続は統一し、集約化している。大阪の事例があった後、リモート回線を調査せよという指示もあったが、既に一本化しており、問題はなかった。**
3）ネットワーク構成図は誰が作成して、誰が管理しているか？	ネットワーク契約時に情報部にて構成図の仕様を作成。情報部にて管理している。
4）追加のシステムなどはどのように情報を入手して管理しているのか？	追加希望の部署から情報部へ依頼があり、当該部署、情報部、当該ベンダーにてヒアリングを行っている。（要件定義の整理）
5）メーカ等に対してネットワーク構成図を開示しているか？（契約による場合も含む）	開示していない。
6）情報システムに関する脆弱性情報はどのように入手して、どう活用しているか？	以下URLを適宜参照し、必要に応じてベンダーと協議している JVN:　https://jvndb.jvn.jp/ IPA: https://www.ipa.go.jp/security/vuln/index.html
7）IT-BCPを作成しているか？ご恵与いただくことは可能か？また、その中に医療機器に関してはどのような形で入っているか？	病院情報システム運用継続計画　IT-BCP作成済み（医療機器は含まれていない）。 →作成したばかり。バックアップについての規程などは定めていない。今の話題は、**バックアップ取っているが、有事の際に本当に戻せるかどうかが課題。メーカでも検証が難しい。** →大学が作成したひな形を参照して作成している。ＢＣＰとも整合性を取る形で作成。ＢＣＰの際に紙カルテ運用対応を想定して作成している。一部印刷して、準備、またはダウンロードして使えるように準備している。大学とも連携するような連絡体制を作っている。実際に事が起きれば、ＢＣＰとも連携して動くような体制を組み込んでいる。 →IT-BCPの中では部門システムについては記載はない。**部門システムのことは記載はあるが、医療機器に特化した内容は今後の課題。**
2. 医療機器のサイバーセキュリティ確保について	

病院名	D病院
1）ネットワークに接続される医療機器についてどう管理しているか？ 2）管理している場合には、どのような管理体制（誰が・どこまで）をとっているのか？（医療情報システムとの違いがあれば。）	医療情報システムに接続する機器はMACアドレス管理。 部門システムに接続する機器は、医療情報システムとはVLANを切り分け部門管理している。部門システムのリモート保守は一元管理し、医療情報システムのVPN経由でしか接続しないようにしている。 →新規接続や機器更新の際には、**部門から情報部に申請して、MACアドレスを登録しているが、実際の細かい管理は部門側で行っている。両方で管理しているのが現状。**
3）医療機器等も含めてネットワーク構成図を把握・管理しているか？ 把握・管理している場合、医療機器に関しては特に何を把握・管理すべきか？	部門システムのネットワーク構成図は設置時に提出。新規案件で接続機器が増える際は、ヒアリングを行っている。医療機器のセキュリティ状態、OS、通信形式などは把握するように努めている。 →情報部で構成図をもらえるところはもらっているが、管理まではしていない。**情報部の構成図までには落とし込めておらず、各部門で管理している。** →情報部の立場としては、**部門システムは部門システムというくくりで接続して、その中のことは現場にお願いするしかない**という立場。あとは、その**境界での対応をどうするかを整理**しているようなイメージ。振る舞い検知機能を導入したいと思っているが、高価なため最初に削減されてしまう。 →ICUのシステムについては臨床工学部門でも構成図等は把握しておらず、メーカが対応している。導入する際に、情報部門では提出を求めている。
4）医療機器のＯＳのバージョンアップやウイルス対策などを確認しているか？	**導入時にのみ**確認
5）医療機器に関する脆弱性情報はどのように入手して、どう活用しているか？	**未着手** →メーカから他院での**脆弱性があったような情報提供**はあるが、**何もしていない。どうすれば良いか分からない。** 改修が入るような不具合があれば、対応するが、**脆弱性だけだと対応方法が分からない。**
6）医療機器のサイバーセキュリティ確保について参照しているガイドライン等はあるか？あれば、ご教示いただきたい。	医療情報システムの安全管理に関するガイドライン →**医療機器の手引きは知らない。** →ガイドラインを遵守するだけでも大変 →**周知を図り分かりやすい物が必要。**
7）医療機器のサイバーセキュリティ確保に向けた医療機器特有の情報として、MDS2、SBOM、レガシー状態があるが、このような情報はどう管理しているか？	機器の上流にFWを設置するなど、必要以外の通信が発生しないように徹底。
8）医療機器メーカから、MDS2、SBOM、レガシー状態に関する情報は提供されるか？	必要な都度、依頼することにより提供 →更新が遅れている部分も有り、メーカからＯＳのサポート終了の連絡が来ても、致し方ないということで、対応しているのが現状。メーカから、ＯＳ対応についての連絡は１年から2年前にくることが多いので、それで更新の検討をするような形で対応。
9）医療機器のサイバーセキュリティ確保に向けた、臨床工学部門や放射線部門、医療機器安全管理責任者、情報システム責任者、医療安全管理者などの連携体制を構築しているか？ 構築しているようであれば、その内容をご教示いただきたい。	月一回、各部門（事務含む）との調整会議を実施している。
10）医療機器のサイバーセキュリティ確保について、誰がどこまで把握して、各分野において主体となって動くのは誰か？ また、その人材として必要な知識、技術、人数をご教示いただきたい。	基本的に情報部が主体となって把握、対応している。必要に応じて調整会議メンバーに協力依頼。全体となって動く人材は情報処理安全確保支援士　１名、医療情報技師　５名（内上級１名）
11）既存システムとの整合とセキュリティ対策の望ましい体制、人材配置をどう考えるか？（院内の連携体制なども含めて）	CSIRT同様に事務部門とも連携し、医療情報部門は問題対応のみに特化できる体制が望ましい。
12）医療機器のサイバーセキュリティに関するインシデントやアクシデントが発生した場合の対応はどう行う想定か？（周知も含め、シナリオがあればご恵与願いたい）	病院情報システム運用継続計画　IT-BCP「サイバーインシデント発生時の連絡体制図」に基づき対応

病院名	D病院
13）医療機器のサイバーセキュリティ確保に向けて、医療従事者や在宅で使用する患者に対して、研修などをおこなっているか？行っていれば、その内容をご教示いただきたい。	行っていない。
14）医療機器のサイバーセキュリティ確保について、これだけは押えておいた方が良いというポイントがあれば、ご教示いただきたい。 （医療機器の日常的な点検で必要な項目などあれば。）	医療機器は多種多様となるため、個々の機器把握は難しいと感挙げる。今後は通信状態の振る舞い検知などを徹底して行っていきたいと考える。
15）医療機器を導入する際に、サイバーセキュリティ確保に関して医療機器製造販売業者との責任分界点を契約内容の中に盛り込んでいるか。盛り込んでいるようであれば、その内容をご教示いただきたい。	→接続について指示することと、ファームウェアの更新などは契約に盛り込んでいないもののお願いしている。
16）医療機器のサイバーセキュリティ確保に関して、医療機器の製造販売業者との連携をしているか？しているようであれば、どのように連携しているか？	リモート接続をしている装置の場合、装置からシーメンスのリモート端末にVPNで接続いており、一般のインターネット回線とは違う系統を使っている。また、リモート時に使用しているルーターについても、セキュリティソフトを含めた最新のバージョンに定期的に更新を行い、万全を期している。基本的に装置と一般のインターネット回線とは違う系統に直接つながっている為、ウイルス感染した場合の補償などについては、想定していない。 →契約の中に書いているわけではない。
17）医療機器のサイバーセキュリティ確保に関して、経営層と情報を共有しているか。している場合には、どのような情報を共有しているか？	
18）医療機器のサイバーセキュリティ確保に関して、保守契約を結んでいるか？結んでいる場合、どのような内容か？ 可能であれば、契約書をご教示いただきたい。	マルウェアに起因して、対象装置が不稼働又は動作不安定になった場合は、保守の実施可否は都度協議のうえ決定することとしている。 →ある機器では、契約に含まれている。保守の除外要件として。 →ある装置ではデータ送信するだけで、メーカサイドからの送信機能はないことから、不正アクセスなどの可能性はないとの回答。
その他意見	○現在は、医療機器メーカが接続できるようになりましたとか、ぜひ接続してくださいとか売り込んでくる事が多いが、実際話しを聞いてみると、**ＩＤとかパスワードを変えているかなど聞いてみても、業者が理解していない**ことが多い。**営業担当者ベースであるが、医療機器だからパソコンと違ってウイルス感染しない**と言うような説明を平気でしてくる。カタログ情報を見るとリナックスとか記載があり、その**リスクなどを営業ベースでは把握しておらず、不確かな情報を医療機関に伝えている。それによって、医療現場が混乱することもある。** →このような機器でも接続する場合には、VLANで切って、境界で遮断するようにして、通信許可するしかない。 ○**インフラを整備するインセンティブが必要。**評価に対してつけて、チェックする必要。 ○部門システム管理する側からすると、**専門の診療業務以外の負担が大きい。**セキュリティIT人材がいるとはいえ、管理体制の強化のためには、教育面も重要であり、人材を専従させるのも難しい。現状はなかなか難しい。ベンダーさんや情報部にお願いしているところも多い。**属人化にならないようにする必要**がある。資格などについては、個人レベルでの対応。自己学習のレベルで。医療情報技師を3名程取得しているが、人員配置までには繋がっていない。 ○**医療情報技師を雇用するにも人材がいない。IT系の人材が不足。資格とっても、自己満足のレベルになってしまう。せめて学会行けるぐらいのインセンティブが必要。**
追加情報	○県警からもサイバーセキュリティに関して一度連絡あり。情報提供は随時されている。 ○有事の際は全学とも連携して、全学の方でも対応をしてくれると想定している。現在も毎週ＷＥＢでカンファで情報交換している。 ○**病院と学術が一緒で管理されており、大学本部とも連携している。** ○**医療機器については、資産台帳とは別に医療機器の安全管理システムでシリアルNoまで管理**している。そこに入力した機器は固定資産台帳の備考にも記載して相互で管理できるようにしている。10年以上前に導入しているが、別々運用とはなっているが、相互に連携を必ずしている。臨床工学部門で管理している機器はMEで、それ以外は事務的に登録している。安い機器やどこまでを管理するかが課題。納品する際に医療機器登録票をメーカに提出依頼をしている。 ○**大型の部門システムを持つ部署については、IPアドレスを渡して、部門の方で割り振り。**放射線関係だと、保守管理用の機器台帳や配線図にIPを記録して管理しているが、見直しなどはせず。 ○一般的な接続確認しているが、その程度。仮想攻撃をテストすることはない。 ○セキュリティの問題で、更新する必要などの連絡はない。エンドオブサポートの段階で連絡がくる。OSが原因で使用期間が短くなっているような感覚はない。
	○超音波装置については、業者にお願いして調査を行った。台数、検査可能内容、プローブは管理し、更新計画、台帳管理をしている。通信しているかどうかは管理できていない。2023年10月～11月調査、報告書が12月完成 ○要望者が出た段階で、台帳をみながら更新計画に落とし込んでい区作業を事務で行っている。

病院名	E病院
病床数	約500床
施設基準：主たる基準	地域医療支援病院 救急告示病院 第二次救急指定病院・第三次救急指定病院 地域災害拠点病院指定 エイズ診療拠点病院 地域周産期母子医療センター指定 医師臨床研修指定病院 歯科医師臨床研修指定病院
従業員数：	
医師数	118名、研修医　26名
看護師数	583名
臨床工学技士数	25名
その他職種（メディカルスタッフと事務職等）	391名
1. 医療情報システムに関するサイバーセキュリティ確保について	
1）管理する組織体制（職種・人数・役割）	セキュリティ対策基準に体制図を明記。システム委員会の委員長、情報セキュリティ管理者として、副院長を当てている。事務局として事務部　情報システム課を置いている。**各部門（病棟も含めて）にもセキュリティ担当者を置き、本社にもセキュリティ担当者を報告している。** **本社からひな形が送られそれに沿って、各病院で、作り込んでいる。システム委員会の委員長がセキュリティ責任者となる。**病院毎でも違うが、小さい病院では兼務となっているところもある。 **サイバーセキュリティ関係の問題が生じる前から、セキュリティ対応をしている。** 規程などはガイドラインや本社のひな形を参考にして作成している。最初は平成27年10月に作成。 電子カルテの障害対応はリモート対応、修正資源配布もリモートで対応。リモート回線の集約化は今後検討課題。1ベンダー1回線で対応しており、回線契約は病院で行い、管理は業者が行う。VPNなどは病院側で管理。**MDS（「製造業者による医療情報セキュリティ開示書」）などももらうようにしている。昨年度は、保健所の監査をきっかけに集めたが、業者が提出してくれなかった。今年度は今集めているが、問題なく提出してくれている。**MDSで【いいえ】の部分を【はい】にできるように意識している。 5人で対応。セキュリティマネジメントやITPを持つ者もいるが、無資格の者もいる。5人の内、セキュリティに関しては課長をふくめて3名で対応。残り2名は運用、メンテ専従で対応している。外部委託はしておらず、内製化して対応。課長職については、数年ごとに交代することもあったが、**現員の2名は、入社してから異動したことがない。**病院長としては、**技術職だからという認識**がある。
2）ネットワーク構成図を把握しているか？	把握している。
3）ネットワーク構成図は誰が作成して、誰が管理しているか？	委託業者が作成。管理は委託業者と情報システム課で行っている。各種サーバーや無線AP、スイッチ系を管理。**市販のネットワーク監視システムを入れて、故障やループ配線などの場所も確認できるようにしている。無線APの電波到達範囲も管理。基本は日勤帯での対応。**
4）追加のシステムなどはどのように情報を入手して管理しているのか？	**新規システムの要望はシステム委員会での検討が必要**であり、情報システム課が知らないシステムが入る事はない。システムが導入される度に配線図は最新化している。契約ではなく、ネットワークの配線については、病院が把握しなければならないという前提で、各社に最新化してもらい提出してもらっている。
5）メーカ等に対してネットワーク構成図を開示しているか？（契約による場合も含む）	開示していない。申請があれば、IPを提供している。
6）情報システムに関する脆弱性情報はどのように入手して、どう活用しているか？	脆弱性情報はベンダーから入手し、適用作業については、相談しながら実施している。
7）IT-BCPを作成しているか？ご恵与いただくことは可能か？また、その中に医療機器に関してはどのような形で入っているか？	バックアップシステムを今年度導入予定であり、併せてIT-BCPも作成予定。本社から素案が配布されて、それを基に作成予定。夏頃にひな形連絡あり。最終ひな形はまだ。**訓練シナリオも本社から届く予定。** 単体バックアップ　バックアップBCP→市販システムを導入。 院内にNAS→ランサム用。２本立てで計画
2. 医療機器のサイバーセキュリティ確保について	

病院名	E病院
1）ネットワークに接続される医療機器についてどう管理しているか？	**各部門で機器については、管理。各部門でリスト化して管理。USBを使う場合の注意点などは情報システム課から運用ルールを周知。**
2）管理している場合には、どのような管理体制（誰が・どこまで）をとっているのか？（医療情報システムとの違いがあれば。）	各部門で管理。
3）医療機器等も含めてネットワーク構成図を把握・管理しているか？ 把握・管理している場合、医療機器に関しては特に何を把握・管理すべきか？	各部門で管理。
4）医療機器のＯＳのバージョンアップやウイルス対策などを確認しているか？	各部門で管理。
5）医療機器に関する脆弱性情報はどのように入手して、どう活用しているか？	各部門で管理。
6）医療機器のサイバーセキュリティ確保について参照しているガイドライン等はあるか？あれば、ご教示いただきたい。	情報システム課では把握していない。**臨床工学課では、医療機器の手引きを把握。**
7）医療機器のサイバーセキュリティ確保に向けた医療機器特有の情報として、MDS2、SBOM、レガシー状態があるが、このような情報はどう管理しているか？	
8）医療機器メーカから、MDS2、SBOM、レガシー状態に関する情報は提供されるか？	医療機器ではないが、**診断書システムの企業からは、メールでセキュアな環境でダウンロードできる形でのMDSの送付**されてくることもある。
9）医療機器のサイバーセキュリティ確保に向けた、臨床工学部門や放射線部門、医療機器安全管理責任者、情報システム責任者、医療安全管理者などの連携体制を構築しているか？構築しているようであれば、その内容をご教示いただきたい。	情報システム委員会やセキュリティ担当者として、医療安全管理者や医療機器安全管理責任者が関与していないが、インシデントが発生し、患者安全にも影響を及ぼす場合には連携して対応することが想定される。
10）医療機器のサイバーセキュリティ確保について、誰がどこまで把握して、各分野において主体となって動くのは誰か？また、その人材として必要な知識、技術、人数をご教示いただきたい。	なし
11）既存システムとの整合とセキュリティ対策の望ましい体制、人材配置をどう考えるか？（院内の連携体制なども含めて）	なし
12）医療機器のサイバーセキュリティに関するインシデントやアクシデントが発生した場合の対応はどう行う想定か？（周知も含め、シナリオがあればご恵与願いたい）	なし

病院名	E病院
13）医療機器のサイバーセキュリティ確保に向けて、医療従事者や在宅で使用する患者に対して、研修などをおこなっているか？行っていれば、その内容をご教示いただきたい。	なし
14）医療機器のサイバーセキュリティ確保について、これだけは押えておいた方が良いというポイントがあれば、ご教示いただきたい。（医療機器の日常的な点検で必要な項目などあれば。）	なし
15）医療機器を導入する際に、サイバーセキュリティ確保に関して医療機器製造販売業者との責任分界点を契約内容の中に盛り込んでいるか。盛り込んでいるようであれば、その内容をご教示いただきたい。	**情報システム本体の契約の中でも、まだ盛り込まれていない。**
16）医療機器のサイバーセキュリティ確保に関して、医療機器の製造販売業者との連携をしているか？しているようであれば、どのように連携しているか？	医療機器メーカより院内の医療職の方の意識が高い。職員については、イーラーニングを実施しているが、一般的な内容である。**システム導入に関して、関わる内容を毎年、導入毎に各部門の担当者に周知し続けてきた結果、セキュリティに関しても文化が醸成された。**
17）医療機器のサイバーセキュリティ確保に関して、経営層と情報を共有しているか。している場合には、どのような情報を共有しているか？	部門システムについては、情報システム課が窓口となり、経営層にも情報提供している。
18）医療機器のサイバーセキュリティ確保に関して、保守契約を結んでいるか？結んでいる場合、どのような内容か？ 可能であれば、契約書をご教示いただきたい。	なし
その他意見	○規模が小さい医療機関では、**医療安全の部門にぶら下げる形でのサイバーセキュリティ対応**も考えられるのではないか。 ○**大きな医療機関でどこまでできるのか、理想像を把握した上で、小さい医療機関に落とし込む必要があるのではないか。** ○医療機器のサイバーセキュリティに関する情報については、**3年間など期間を決めて、メーカから医療機関へ提出させるなどのキャンペーンが必要ではないか。**それをどう活用するかについては、その後検討する必要があるのではないか。各医療機関のレベル間を見据えて検討する必要がある。 ○セキュリティの確保等も含めて、情報システムの運用・管理については、**人海戦術で対応しており、評価される部分も少ない。**各医療機関でのモチベーションを保つ意味でも、**評価する仕組みが必要ではないか。** ○**メーカから提出されるセキュリティに関する見積もりも複雑すぎて、メーカ自身が把握していない**場合もある。5年使用するような前提のシステムでも、ウイルス対策ソフトのライセンスは1年だけしか見積もっていないなど、不備があることも多い。
追加情報	○グループ病院でも各病院で対応している部分も多いが、同じグループ病院なので、電話でいろいろ相談できる体制となっている。係長研修や課長研修で全国のグループ病院の担当者と一緒になることも多く、そこで顔をつなぎ、情報収集も可能となっている。 ○他のグループ病院ではリモート回線の集約なども行っている。 ○**部門システムも含めてリスト化して管理しており、約7年間隔ぐらいで、更新計画を作成して、委員会へ答申**している。9年間隔では更新できるように検討している。毎年、**11月くらいに翌年度の更新リストと更新タイミングを検討して、更新計画をたて予算確保**をしている。電子カルテの更新に合せるか、合せないかも検討を行う。情報システム課から各現場に相談した上で、更新計画を挙げてもらっている。 ○地方病院だと、メーカ直接ではなく、卸がフォローアップすることも多い。**卸にサイバーセキュリティに関する知識がない**こともある。 ○情報システム課の方で、**導入するシステムについては、どこにどういう方式でデータが蓄積されるのかを確認して、病院側から接続方式を提案することもある。しかし、それを対応してくれるような場合は少ない。ペースメーカの遠隔モニタリングシステムを導入する際には、メーカと打ち合わせをしたうえで導入している。**
	○モバイルLTE回線でリモートを行いたいという提案があった際には、病院側からは、**専用回線を提案したが、結局受入れてもらえず、通信内容がログだけということもあり、許可**したこともある。中身を精査したうえで、対応している。

病院名	F病院
病床数	約200床
施設基準：主たる基準	保険医療機関 労災保険医療指定機関 生活保護法指定医療機関 指定自立支援医療機関
従業員数：	常勤職員210名、非常勤合せて250名
医師数	常勤　10名程度、非常勤23名（外来のみ10名）
看護師数	
臨床工学技士数	0
その他職種（メディカルスタッフと事務職等）	
1. 医療情報システムに関するサイバーセキュリティ確保について	
1）管理する組織体制（職種・人数・役割）	情報システム管理者として病院長を置き、安全管理責任者が事務長、企画管理者として医事課長代理を置いている。 **管理に関するガイドラインにそって作成。各部署野帳を運用責任者としておいている。**（検査、薬局、訪問、医療相談、医師など） IT-BCPは今年の6月に作成（診療録管理体制加算の取得のため。） **パソコンなどのOS管理は一元的に管理できるサーバを導入して対応している。**情報システムのサーバーについては、各メーカにお願いして対応している。HIS系の通信やアプリについては、許可されたものだけ使える仕様となっている。現在ではPCは200台前後使用している。 ネットワークに接続する機器が少ない。各部門システムもほとんどない。リモート接続については、現時点では使用しておらず、電子カルテの業者のみ外部に接続されていない、専用回線で接続して、対応する形になっている。 将来的にも必要があれば、**既に導入されているシステムを利用することで、外部からセキュアに接続できる**と考えている。担当者は主に一人で、企業でのSE経験を経て入職。
2）ネットワーク構成図を把握しているか？	**委託業者が作成。**初期の段階からネットワーク構築に関与している業者であり、イントラネット、インターネットの接続、ネットワーク保守、ハードウェア保守、設定変更の対応などしている。 配線図は変更があるたびに、最新化している。無線LANとかの設計・施工なども対応。保守契約の中に入っている。 セキュリティパッチの最新化は機器やソフトウェアの保守として対応している。設定変更などについては、現地作業やリモートで対応し、都度支払いで対応している。
3）ネットワーク構成図は誰が作成して、誰が管理しているか？	
4）追加のシステムなどはどのように情報を入手して管理しているのか？	**申請が上がってきたら対応。**技術的なところは、**ネットワーク保守委託業者と直接システム業者で対応。**
5）メーカ等に対してネットワーク構成図を開示しているか？（契約による場合も含む）	していない。開示する必要がある場合にも、委託業者と相談して決定。
6）情報システムに関する脆弱性情報はどのように入手して、どう活用しているか？	脆弱性については、**委託業者やメルマガ、ウイルスバスターからの情報提供**などがあるが、**期限を決めて、パッチを当てて対応**している。テスト端末にパッチを当て、**問題がなければ、全端末に展開**している。この作業は院内の担当者が実施している。
7）IT-BCPを作成しているか？ご恵与いただくことは可能か？また、その中に医療機器に関してはどのような形で入っているか？	作成済み。**医療機器に特化した内容は入っていない。**
2. 医療機器のサイバーセキュリティ確保について	

病院名	F病院
1）ネットワークに接続される医療機器についてどう管理しているか？	ほとんど接続されていない。接続される場合には、無線ＬANなどで接続したいなど申請があれば、MACアドレスで管理している。**安全を確認したうえで許可**している。
2）管理している場合には、どのような管理体制（誰が・どこまで）をとっているのか？（医療情報システムとの違いがあれば。）	情報システムと同じ。
3）医療機器等も含めてネットワーク構成図を把握・管理しているか？ 把握・管理している場合、医療機器に関しては特に何を把握・管理すべきか？	ほとんど接続されていない。検査については、外注しており、データだけが別回線で送られてくる。送られてきたデータを運用ルールにそって、セキュリティを担保したUSBを用いて、HISに取り込んでいる。また、仮にUSB経由でウイルスが入るような場合でもOSロックの仕組みを導入しているため発症せず、**不要なアプリを使っての攻撃ができないようなシステムも導入**している。
4）医療機器のＯＳのバージョンアップやウイルス対策などを確認しているか？	なし
5）医療機器に関する脆弱性情報はどのように入手して、どう活用しているか？	なし
6）医療機器のサイバーセキュリティ確保について参照しているガイドライン等はあるか？あれば、ご教示いただきたい。	**把握していない。**
7）医療機器のサイバーセキュリティ確保に向けた医療機器特有の情報として、MDS2、SBOM、レガシー状態があるが、このような情報はどう管理しているか？	なし
8）医療機器メーカから、MDS2、SBOM、レガシー状態に関する情報は提供されるか？	なし
9）医療機器のサイバーセキュリティ確保に向けた、臨床工学部門や放射線部門、医療機器安全管理責任者、情報システム責任者、医療安全管理者などの連携体制を構築しているか？構築しているようであれば、その内容をご教示いただきたい。	なし
10）医療機器のサイバーセキュリティ確保について、誰がどこまで把握して、各分野において主体となって動くのは誰か？また、その人材として必要な知識、技術、人数をご教示いただきたい。	なし
11）既存システムとの整合とセキュリティ対策の望ましい体制、人材配置をどう考えるか？（院内の連携体制なども含めて）	なし
12）医療機器のサイバーセキュリティに関するインシデントやアクシデントが発生した場合の対応はどう行う想定か？（周知も含め、シナリオがあればご恵与願いたい）	なし

病院名	F病院
13）医療機器のサイバーセキュリティ確保に向けて、医療従事者や在宅で使用する患者に対して、研修などをおこなっているか？行っていれば、その内容をご教示いただきたい。	なし
14）医療機器のサイバーセキュリティ確保について、これだけは押えておいた方が良いというポイントがあれば、ご教示いただきたい。 （医療機器の日常的な点検で必要な項目などあれば。）	なし
15）医療機器を導入する際に、サイバーセキュリティ確保に関して医療機器製造販売業者との責任分界点を契約内容の中に盛り込んでいるか。盛り込んでいるようであれば、その内容をご教示いただきたい。	なし
16）医療機器のサイバーセキュリティ確保に関して、医療機器の製造販売業者との連携をしているか？しているようであれば、どのように連携しているか？	なし
17）医療機器のサイバーセキュリティ確保に関して、経営層と情報を共有しているか。している場合には、どのような情報を共有しているか？	医療機器に関わらず、**事務長レベルが俯瞰的に把握**している。
18）医療機器のサイバーセキュリティ確保に関して、保守契約を結んでいるか？結んでいる場合、どのような内容か？ 可能であれば、契約書をご教示いただきたい。	なし
その他意見	○**セキュリティに関するシステムの導入は医療機関の考え方によるところが大きい。**実際的には、まだ導入されていないところが多いのではないか。この病院では、**企業側からの提案もあり、経営層レベルでもサイバーセキュリティ確保を認識したうえで導入されている。** ○**端末から感染するか、外から感染するかがほとんどであるが、それらをブロックするシステムを中心に投資**していることで、有効的な対策ができていると考えている。 ○セキュリティシステムについては、**医療機関の身の丈にあったものを導入する必要があるが、どの程度のレベルが必要かが分からない。** ○**最後の理想像だけ目標にしても、段階的に導入していかないと難しいのではないか。事業者でも提案に迷う事が多い。**規模感によってかなり変わる。 ○**医療機関の規模や特性にあったセキュリティシステムが必要ではないか。それを判断する基準がない。** ○ネットワークを開放しても、ウイルスに対して対応できるようになれば良い。全てが最新にものになっていれば安心できる。 ○**電子カルテによってはアップデートを許してくれないので、ゼロトラストの考え方が適用できない。** ○**NDR（Network Detection and Response）というツール**もあるが、なかなか、導入するのは難しいのではないか。 ○**医療機器のサイバーセキュリティ確保については、初めて知った。浸透させていくには、サイバーセキュリティ本体の対応を同様にチェックリストや監査などで対応していくしかないのではないか。** ○**医療機器側でも最新のセキュリティ対策の考え方に沿って、製品開発が必要ではないか。クラウドと接続を前提とした製品開発として、医療機器側でも認識を変える必要があるのではないか。** ○**ある一定の医療機器に特化した通信基準を作る必要もあるのではないか？または、個々の医療機器の対策と言うよりは安全な環境を作る方策を検討した方がよいのではないか？多層防御の方法も合せて検討する必要があるのではないか？**
追加情報	○当院では、20年以上前からIT化を進めてきた。精神科では多職種の情報共有が重要であることから、グループウェアの導入や電子カルテなどの導入を進めてきた結果、ネットワークの構築についても取り入れてきた経緯がある。USBの使用制限なども進めてきたが限界があり、現在は、守ることだけではなく、**内部の環境を最新化して、ウイルスから守ることを進めている。** ○段階的に導入してきたこともあり導入できている。**電子カルテがないと、若い看護師の採用ができない。** ○セキュリティ関係に費やす予算は技術レベルによって、キリがないので、**企業から提案いただくときには、松竹梅の提案をしてもらい、必要な対応について説明が付くレベルを担保できるように検討**している。ランサムウェアの対策システムも導入済み。 ○入口、出口の対策、ランサムウェア対策（設定を書き換える）もすぐに対応している。**ゼロトラストの考えや仕組を導入**している。 ○今後、**クラウド化を見据えて、新たな設備投資が不要となるように対応を進めている。** ○ネットワーク更新については、委託業者から上がってくる。**事故が起こった時に説明ができる範囲で検討**している。

病院名	G病院
病床数	約400床
施設基準：主たる基準	日本医療機能評価機構認定病院 リハビリテーション病院、一般病院2、高度・専門機能：リハビリテーション（回復期） マンモグラフィ(乳房エックス線写真）検診施設 臨床研修協力施設 下肢静脈瘤に対する血管内焼灼術の実施基準による実施施設
従業員数：	819名
医師数	91名
看護師数	293名
臨床工学技士数	10名
その他職種（メディカルスタッフと事務職等）	272名
1. 医療情報システムに関するサイバーセキュリティ確保について	
1）管理する組織体制（職種・人数・役割）	法人全体の責任者を理事長として、連絡協議会（法人内の情報管理）を設置。**病院の情報管理責任者は院長として、システム委員会を設置。各部門の長を委員に任命し、月1回情報システム連絡会議を開催。報告事項が中心であるが、機能追加や要望などの導入可否も判断している。** 電子カルテの更新は7年を想定しており、部門システムは別々に対応している。部門システムはハードの保守が受けられる上限期間で更新を検討している。 事務局として情報システム部門で対応、法人全体で6名、法人内9施設を病院で一括で対応している。 **病院機能評価、保健所の立入の結果、関連する規程を整備し、法人として承認している。**
2）ネットワーク構成図を把握しているか？	**業者に入ってもらって把握している。年間保守も契約している。** 拠点間ネットワークはVPN業者が入っている。**電子カルテ系で2系統引いている。インターネット系については、各市施設で1本づつ引いているが、最終的に1本化して、ファイヤーウォールを入れて管理している。** **リモートメンテなどに使用する回線が上記とは別に、各ベンダー毎にVPNを準備してもらっている。接続するルールを徹底し、バージョンアップなどは業者の責任で行ってもらっている。サービスの契約書の中で盛り込んでいる。病院として1本化はしていないが、接続回線は全て把握するようにしている。**
3）ネットワーク構成図は誰が作成して、誰が管理しているか？	**3年前に作成。かなりの時間がかかった。**現在は業者に入ってもらって年間保守契約の中で管理している。 **外部接続が必要な場合には、情報システム課が必ず関与し、接続方式等を含めて確認して、リスト化している。**勝手に設置されないように監視を強める方法も検討中である。
4）追加のシステムなどはどのように情報を入手して管理しているのか？	**サーバーは１つのベンダーなので、対応できるが、端末となるとコントロール不能。**
5）メーカ等に対してネットワーク構成図を開示しているか？（契約による場合も含む）	聞いてくるメーカもない。開示していない。**接続情報の申請がくれば、IPを払い出している。**
6）情報システムに関する脆弱性情報はどのように入手して、どう活用しているか？	JPCERTや医療セプターから入手。**部門システムベンダーからの情報はほとんどない。対応すべきものがあれば対策するが、目をつぶって使うしかないこともある。**
7）IT-BCPを作成しているか？ご恵与いただくことは可能か？また、その中に医療機器に関してはどのような形で入っているか？	**システムダウン時のマニュアルを策定ずみ。30分以上止まるか止まらないかで紙カルテ運用にするか否かを判断基準として示している。**ダウン後の各現場での動きは各現場で対応するように示している。今年に入り、２回地域の停電があり、その経験に基づき改めてまとめなおした。停電感知でシャットダウンしてサーバー停止の際の復旧方法の確認がそのタイミングでできた。自家発電に切り替わることが前提であったが、うまく切り替わらず、シャットダウンとなった。**実際の停電を経験して、気づいたことをマニュアルに盛り込んでいる。**
2. 医療機器のサイバーセキュリティ確保について	

病院名	G病院
1）ネットワークに接続される医療機器についてどう管理しているか？	**サーバーは１つのベンダーなので、対応できるが、端末となるとコントロール不能。** **アップデートの連絡もこない。**
2）管理している場合には、どのような管理体制（誰が・どこまで）をとっているのか？（医療情報システムとの違いがあれば。）	
3）医療機器等も含めてネットワーク構成図を把握・管理しているか？ 把握・管理している場合、医療機器に関しては特に何を把握・管理すべきか？	**IPの払い出しのみの管理。**ネットワーク配線図までには落としていない。ネットワーク接続する医療機器の調達には関わっている。物によっては、古い機器で自主点検の範囲で使用しているものもあるが、使用頻度も低くい場合にはレガシー機器でも許容せざる得ない。
4）医療機器のＯＳのバージョンアップやウイルス対策などを確認しているか？	**ウイルス対策については、インストールできる端末であれば情報システム側で対応。**パターンファイルについても手動で移し替えている。USB接続は制限している。
5）医療機器に関する脆弱性情報はどのように入手して、どう活用しているか？	特に連絡はない。
6）医療機器のサイバーセキュリティ確保について参照しているガイドライン等はあるか？あれば、ご教示いただきたい。	**知らない。読み手側が読み解けて納得の上対応できるのかも疑問。**
7）医療機器のサイバーセキュリティ確保に向けた医療機器特有の情報として、MDS2、SBOM、レガシー状態があるが、このような情報はどう管理しているか？	**データ収集はできていない。情報システムに関しては、立入検査のために対策しているが、医療機器については、できていない。**
8）医療機器メーカから、MDS2、SBOM、レガシー状態に関する情報は提供されるか？	ない
9）医療機器のサイバーセキュリティ確保に向けた、臨床工学部門や放射線部門、医療機器安全管理責任者、情報システム責任者、医療安全管理者などの連携体制を構築しているか？ 構築しているようであれば、その内容をご教示いただきたい。	**現場からもOSが古いなどの相談はない。OSの概念がない。**
10）医療機器のサイバーセキュリティ確保について、誰がどこまで把握して、各分野において主体となって動くのは誰か？ また、その人材として必要な知識、技術、人数をご教示いただきたい。	なし
11）既存システムとの整合とセキュリティ対策の望ましい体制、人材配置をどう考えるか？（院内の連携体制なども含めて）	なし
12）医療機器のサイバーセキュリティに関するインシデントやアクシデントが発生した場合の対応はどう行う想定か？（周知も含め、シナリオがあればご恵与願いたい）	なし

病院名	G病院
13）医療機器のサイバーセキュリティ確保に向けて、医療従事者や在宅で使用する患者に対して、研修などをおこなっているか？行っていれば、その内容をご教示いただきたい。	なし
14）医療機器のサイバーセキュリティ確保について、これだけは押えておいた方が良いというポイントがあれば、ご教示いただきたい。 （医療機器の日常的な点検で必要な項目などあれば。）	なし
15）医療機器を導入する際に、サイバーセキュリティ確保に関して医療機器製造販売業者との責任分界点を契約内容の中に盛り込んでいるか。盛り込んでいるようであれば、その内容をご教示いただきたい。	なし
16）医療機器のサイバーセキュリティ確保に関して、医療機器の製造販売業者との連携をしているか？しているようであれば、どのように連携しているか？	なし
17）医療機器のサイバーセキュリティ確保に関して、経営層と情報を共有しているか。している場合には、どのような情報を共有しているか？	**理事長からは気にかけてもらっており、理解いただいているのでシステム導入ができている。**
18）医療機器のサイバーセキュリティ確保に関して、保守契約を結んでいるか？結んでいる場合、どのような内容か？ 可能であれば、契約書をご教示いただきたい。	なし
その他意見	○医療機器までとなると無数にあり、どこにセキュリティホールがあるのかすらも分からない。大きな課題である。全く手つかずの状態である。 ○**メーカのサービスマンがメンテナンスのためにノートパソコンを医療機器等に接続する場合などについても対策が取られているのか？そのような責任分界点についても、契約の中に入っていない。そのような契約を結んでいる医療機関はほとんどない。** ○**医療機関の中でもとこまでが守備範囲なのかが、体制としてとられていないところが多い。**システム担当がいないところも多い。医療機器までは掌握できていない。 ○1242病院のアンケート調査でも、電子カルテの導入していない病院は10%以下であった。**中小病院でも情報システムの導入が広がっている。中小関係の病院ではシステム関係の部署もなく、今後危険な状態も危惧される。** ○オンライン資格確認システムについても、補助金で導入後1-2年でシステムに合わないから買い換えてくれとも業者から平気で言われる。国の施策だから仕方ないと。病院側は言われたら買い換えるしかない。ささいな話しであるが、業者も医療機関も素人の域をでていない。補助金で購入すると、使わなくてもしばらくは放置しておかなければならない。 ○厚労省からも五月雨式にDXに関する補助金などがでてくるので、病院側もタイミングをみている。 ○電子カルテの更新経費も高騰している。今までは1床100万程度だったが、200-300万円程度になっている。10億円以上かかっているところもある。しかし、**セキュリティには1242病院のうち2割は全く投資していない。無回答、よく分からない回答も多い。どこまでがセキュリティにかかる費用かも判断できない状況**にはあるが、**赤字がすすむにつれて、セキュリティにかかる費用は削られるのではないか。** ○**専門部署がある故に、現場からの問い合わせも多く、各部門はお客さん的に対応を迫られる。知識のアップデートも必要であるが、時間がさけない。** ○**自己評価できる指標が必要。どこまで費用をかければ良いか分からない。今までなかった仕事、新しい対策として、どう評価するかが課題。** ○**資格に対して報酬をあげることができないので、細かく言及することができない。評価する仕組みがなく、資格を取っても変わらないので、モチベーションを上げる仕組みが必要である。各法人の努力の範囲で対応している。施設維持する人員として確保するようにしないと各医療機関のレベルはあがらない。** ○**モニタリングシステムにしろ、次世代型のウイルス対策にしても費用が高額。ウイルス対策だけで言うと固定費となるが、以前は年間で1台1000円のところ、現在は10倍以上。抱え込むにも限度がある。**
追加情報	○**今年度ネットワークセキュリティ対策として、ダークトレースを導入。ネットワーク情報をモニタリングして、AIが危険性を判断してアラートを出してくれるようなシステム。**デバイス1台あたり年間5000円程度から利用可能で、ネットワークスイッチ配下に置いてモニタリング。IP管理ベースで対応。ランサムウェアの被害が他病院であり、その対策として導入。3ヶ月ほどテスト運用して導入した。NDR（Network Detection and Response）。**EDRについては、端末にインストールするタイプなので、医療機器には対応できない。NDRはデバイスに依存しない。**検知・報告の未導入。上位オプションとして、自動遮断できるような機能もある。24時間運用も可能。端末毎遮断できる。リモートデスクトップ接続などの検知も可能。導入から半年であるが、危険なものは検知されていないが、普段使っていない端末からのアクセスなどがチェック・確認できるようになった。人の手だけでやるのは無理がある。メール、スマホで確認可能。それを契機に管理画面で確認している。電子カルテ系については、リモートデスクトップの作業程度の報告であるが、インターネット側の端末については結構なイベント報告がある。岡山の病院で導入していたので検討した。怪しい動きがあれば、部門担当者に連絡して協働で対応している。 ○**大阪の私立病院の情報連携あり。**月1回IT部会あり。事務長会の下部組織として。大阪のみの取組み。京都でも同じような取組みあり。大阪と京都で交流できないか相談中。IT部会でもNDRの導入病院はまだ少ない。テストを始めた病院もある。 ○**法人内の勉強会という形でセキュリティの勉強会をした。個人情報の保護は医療安全の範囲で対応しているが、セキュリティについては、現状難しい。勉強会をしても、我々の守備範囲ではないという意見もある。** ○**セキュリティを担当する人を増やすことが難しい。財政的にも人材的にも。採用できるチャンスが巡ってきた時には、ITリテラシーを確認した上で採用している。単価が見合わないので採用できないこともある。**

病院名	H病院
病床数	グループ全体で6000床以上
施設基準：主たる基準	グループ病院で違いあり
従業員数：	グループ全体で30000名以上（常勤）
医師数	
看護師数	
臨床工学技士数	
その他職種（メディカルスタッフと事務職等）	
1. 医療情報システムに関するサイバーセキュリティ確保について	
1）管理する組織体制（職種・人数・役割）	**SE45名以上が本部に在籍**し、本部所属で各病院へ派遣している。一人やめても穴埋めができるように3年前くらいからチーム体制を取っている。システム開発、データセンター事業（中央で部門システムのサーバを管理）、PC・機器レンタルサービス（仕入れ、設定、設置までサービス提供）、病院支援常駐サービス（SE35名は病院常駐）一人3病院ぐらいを担当。情報機器貸し出し実績　5000台以上。セキュリティ対策については、ランサム対策などを導入。センターサーバ方式への切替、センター側でランサムウェア等のサイバー対応に関してサーバに導入。すべてを拒否して例外で許可する。オフラインバックアップについては、単独の病院だと2500万円ぐらいするので、中央化してサーバに導入。18病院分のバックアップを実施（オフライン） **放射線機器を導入する場合いは企画の段階から診療放線技師が関与。臨床工学については、立ち上がったばかりで現在対応中。システム関係は情報システムで対応している。** 病院個々でセキュリティ対策をするというよりは、**本部から下ろす形で対応。** 定例で毎月部会を開催。ガイドライン検討部会やＢＣＰ、**ネットワーク全体を医療機器含めたＢＣＰの策定を企画中。**部内で検討し、事務長会などで発信。反対意見に対しては本部を悪者として、本部主導で対応してもらう。 **今まではネットワークに接続される医療機器については、部門任せになっていたところもあるが、今後は情報システムの方に集約する形で検討を開始**したところである。**ネットワーク構成図なども、放射線機器メーカが作成し、部門で保管しているものの、情報システムとは共有されていない状況にあったが、それを情報システムにも集約化する方向で検討**している。 情報システム安全管理責任者：情報システム課長、医療機器安全管理責任者：臨床工学科長
2）ネットワーク構成図を把握しているか？	情報システム課が主幹で管理している。完成図書として、メーカが作成して、情報システム課へ納品してもらっている。末端の細かいところは病院で作成しているが、ネットワークの大元に関しては、保守契約を結んで対応している。
3）ネットワーク構成図は誰が作成して、誰が管理しているか？	情報システム課
4）追加のシステムなどはどのように情報を入手して管理しているのか？	**導入企画段階で情シスが関与しており、導入確定したものもすべて把握できるフローになっている。価格交渉や接続方式を確認した後に導入。** 接続する際には情報システム課に連絡が来るようになっている。30万円以上のシステムは連絡がくる。年度末などでは駆け込みの連絡も多い。関連病院も含めて、全ての調達情報が情シスに集約。システムで管理しており、５年前から運用。申請、決済　管理、もシステムで対応している。内製で作成。**価格や機能によっては、メーカ差替えなども提案している。**
5）メーカ等に対してネットワーク構成図を開示しているか？（契約による場合も含む）	これまで事例がない。**出すことがリスク。**
6）情報システムに関する脆弱性情報はどのように入手して、どう活用しているか？	厚労省HP、ベンダーからの情報提供 IPAからのメーリングリストからの情報。警察などからも情報がある。 ベンダーからはほとんどない。
7）IT-BCPを作成しているか？ご恵与いただくことは可能か？また、その中に医療機器に関してはどのような形で入っているか？	作成している。**医療機器は含まれていない。リスト化と連絡体制を取りまとめる予定。**夜間常駐していないところについての小さい病院での対応が課題。 ソフトウェアサービスのシステムについては、リモートで接続。電子カルテはベンダー毎でリモートでも対応できるようになっている。
2. 医療機器のサイバーセキュリティ確保について	

病院名	H病院
1）ネットワークに接続される医療機器についてどう管理しているか？	各部門で医療機器安全管理責任者の責任の基、台帳管理（管理システムをエクセル等で管理）を行っている。　今後情シスで集中管理をするべく議論している。
2）管理している場合には、どのような管理体制（誰が・どこまで）をとっているのか？（医療情報システムとの違いがあれば。）	各ベンダーより情シスに依頼し主幹部署が得て、情シス管理の台帳に反映するように依頼している。 ＩＰを払い出しているのみで実際何が接続されているかのフィードバックが今後の課題。
3）医療機器等も含めてネットワーク構成図を把握・管理しているか？ 把握・管理している場合、医療機器に関しては特に何を把握・管理すべきか？	部門システムまでは反映されているが、末端の機器までは盛り込めていないのが実情。現状できていないがIPやゲートウェイ情報はもちろんのこと、通信で使用するサービスポートなどは把握すべきと思う。今はそこができていない。変更の際にも連絡が来るようになっているが、知らないところで増えているような不安もある。
4）医療機器のＯＳのバージョンアップやウイルス対策などを確認しているか？	アプリケーションの動作保証の問題もあり、OSのバージョンアップはできていないのが実情、ウイルスソフトは導入しているものもあるが、パターンファイルが更新されているか把握できていない。透析管理システムはウイルス対策は未導入、単独LANの可能性あり。
5）医療機器に関する脆弱性情報はどのように入手して、どう活用しているか？	各メーカに情報収集、対応を委ねているのが実情。
6）医療機器のサイバーセキュリティ確保について参照しているガイドライン等はあるか？あれば、ご教示いただきたい。	医療除法システム安全ガイドラインを参考にしている。 医療機器については、知らない。あるのであれば、一緒の方が分かりやすい。
7）医療機器のサイバーセキュリティ確保に向けた医療機器特有の情報として、MDS2、SBOM、レガシー状態があるが、このような情報はどう管理しているか？	医療情報と同様、取り始めているところである。取得したものは内容を確認して問題ないことを確認している。 作り方についても？な部分もあり、どうすれば良いかもどうつかえが良いか不明。ＳＢＯＭの部品表から脆弱性が分かると良いが、第三者がやってくれる方が良い。業者も出してくれるところとだしてくれないところもある。出してくれても本当に正しいのかも疑問。
8）医療機器メーカから、MDS2、SBOM、レガシー状態に関する情報は提供されるか？	業者も出してくれるところとだしてくれないところもある。出してくれても本当に正しいのかも疑問。
9）医療機器のサイバーセキュリティ確保に向けた、臨床工学部門や放射線部門、医療機器安全管理責任者、情報システム責任者、医療安全管理者などの連携体制を構築しているか？構築しているようであれば、その内容をご教示いただきたい。	医療情報とのどうようの流れで、MDS/SBOMは専門知識の高い情シスにもチェックしてもらい、 問題点がないかを確認するフローを構築している最中である。課題があれば、委員会に挙げたり、関連部門と協働で対応する。
10）医療機器のサイバーセキュリティ確保について、誰がどこまで把握して、各分野において主体となって動くのは誰か？また、その人材として必要な知識、技術、人数をご教示いただきたい。	情報システム課が主体で動き、情報も情シスに全て集約化、課題となるポイントは安全管理責任者、委員会にも共有するながれ。リスク分析ができ、対策案を検討できる人材が必要と考えられるが判断に迷う際は、法人本部の医療情報部門とにも連携しながら、随時検討している状況。知識、技術という点では情報システムと同じ観点で良いと考えられるため、兼務で良いのではないかと考える。報酬で点数をつけて兼務が現実的。
11）既存システムとの整合とセキュリティ対策の望ましい体制、人材配置をどう考えるか？（院内の連携体制なども含めて）	配置したいところであるが、人が来てくれない。他分野に流れてしまう。医療資格を持っている経験者でITやっていきたい人や、子育て世代のお母さんなどを採用している。リモート環境も考えたが、現地へいかないと難しい。
12）医療機器のサイバーセキュリティに関するインシデントやアクシデントが発生した場合の対応はどう行う想定か？（周知も含め、シナリオがあればご恵与願いたい）	原則、IT-BCPで策定した流れに準じて対応する流れで考えている。最終的にはメーカなので、いかに情報伝達を早くできるか？課題。電子カルテは止まっても診療を継続できる場合もあるが、医療機器については、診療を止めなければいけないのが大きな違い。

病院名	H病院
13）医療機器のサイバーセキュリティ確保に向けて、医療従事者や在宅で使用する患者に対して、研修などをおこなっているか？行っていれば、その内容をご教示いただきたい。	実施に至っていない。情報システムについては実施しているが、**医療機器についてはできていない。**
14）医療機器のサイバーセキュリティ確保について、これだけは押えておいた方が良いというポイントがあれば、ご教示いただきたい。 （医療機器の日常的な点検で必要な項目などあれば。）	**機器の導入時にリスクを評価することが大前提**で、リスクのあるものないものに分類し、ネットワークに接続され、汎用OSソフトが導入されているものがある場合には、情報システムと同様、侵入経路の確認やウイルス検知ログの点検が必要。また、**保守回路系については、最新のファームウェアが提供されているのか確認などができることが望ましいのではないか。**
15）医療機器を導入する際に、サイバーセキュリティ確保に関して医療機器製造販売業者との責任分界点を契約内容の中に盛り込んでいるか。盛り込んでいるようであれば、その内容をご教示いただきたい。	盛り込んでいない、**メーカ側もどこまでが対応範囲かが明確にできていないところではないか。**
16）医療機器のサイバーセキュリティ確保に関して、医療機器の製造販売業者との連携をしているか？しているようであれば、どのように連携しているか？	なし
17）医療機器のサイバーセキュリティ確保に関して、経営層と情報を共有しているか。している場合には、どのような情報を共有しているか？	**本部のトップはセキュリティについては理解があるが、予算の確保は別の話しとなっている。トップが納得できる内容を提案はしているが、自院がどれくらいまできているかわからない。分かりやすい指標で評価できると良い。**
18）医療機器のサイバーセキュリティ確保に関して、保守契約を結んでいるか？結んでいる場合、どのような内容か？ 可能であれば、契約書をご教示いただきたい。	サイバーセキュリティ確保に特化した条文は特段設けていない。**責任範囲などが不明確な中、また、影響範囲をどこまでに設定するかなど、定義が難しい部分**ではないかと考えている。
その他意見	○**サイバーセキュリティに関して契約として書き込むと費用に跳ね返ってくるので、曖昧の中で紳士協定として対応**しているのがほとんどではないか。**責任分解を話しても平行線となり、押し付け合い**となってしまう。 ○**IPやゲートウェイ情報はもちろんのこと、通信で使用するサービスポートなどは把握すべきと思う。** ○**医療機器に関するサイバーセキュリティの手引きがあるのであれば、安全管理ガイドラインと一緒になっていた方が分かりやすい。分かりやすく伝える工夫が必要。** ○**ＳＢＯＭの部品表から脆弱性が分かると良いが、第三者がやってくれる方が良い。** ○**病院として、可能な範囲で業者とも協力して守り合うことが重要。** ○**医療機器メーカがガイドライン準拠しているといっても信頼性が薄い。どのようにチェックすれば良いか分からない。医療機器を接続したときにも信頼性が担保できないことも多く、閉域で対応できるところは閉域で対応している。** ○**専門部署があれば良いが、専門家がいないと対策についての判断も難しい。収入にもならない対策なので、点数をつけてもらわないと成り立たなくなる。ＤＸを進めても、セキュリティができていないのが課題。** ○**インフラを更新しても診療報酬が手厚くなるわけでもなく、物価も高騰し、保守費も高騰している。人口減少に入る中、どこに集約すべきかを検討する必要がある。**
追加情報	○**取引先500社前後に医療機器等の接続に関して、独自調査を実施。他院で被害の実例が起こったことをきっかけに実施。**侵入経路をつぶすため。医療機器の中身については、何もできないので、業者が責任を持ってもらうとして、侵入経路を確認するために調査。侵入経路となりうるネットワークの構成確認を医療情報システム・医療機器問わずグループと取引のある協力会社　約500社に対して脆弱性、調査接続方法、セキュリティ方式、暗号化方式などを調査。検査機器、放射線モダリティも含めて調査。 →**インターネット経由での接続が多く、国内業者については、別方法での接続で対応してもらった。国外事業者については、一部許容している。** ○**ウイルス対策については、医療機器については対策できていない。課題である。医療機器は薬機法で手出しができないのが実情。** ○**ランサムウェア対策についてもほとんどできていなかった。** アンケート結果については、グループないの医療の質向上委員会で企画を立てて発表。事務長会でも報告し、インターネット経由から閉域ネットワークにした際の費用捻出についても説得してきた。 ○**端末についてはウイルス感染しても、バックアップ機器で何とか対応できるが、医療機器については難しい。** ○**サイバーセキュリティのみならず、経営、運営は本部主体で各病院へ一本化**している。 ○診療情報や機能に対しては医療の質向上委員会で各部門の長、医療情報代表者が決定→**グループの答えとして、それに従うようなガバナンス体制となっている。決定したルールは守らせる。守っているかどうかは各病院の部門が後追い調査を実施し担保している。本部機能が充実し、本部が掌握している。病院の診療機能毎にレベル分けはしておらず、統一基準で対応している。**

病院名	I病院
病床数	約300床
施設基準：主たる基準	急性期一般入院料4 療養病棟入院基本料1 救急医療管理加算 診療録管理体制加算1
従業員数：	541名
医師数	32名
看護師数	看護師　219名（助産師　12名、看護師173名、准看護師34名）
臨床工学技士数	11名（ME5名、透析6名）
その他職種（メディカルスタッフと事務職等）	290名
1. 医療情報システムに関するサイバーセキュリティ確保について	
1）管理する組織体制（職種・人数・役割）	医療情報システム管理者　他２名、医療機器安全管理責任者（臨床工学技士）、放射線科技師長 **情報システムの管理は合計3人で対応**している。**部門系システムについては、書式があり、作業依頼の連絡が来た際に、確認した上で、ネットワークへの接続などを許可**している。**接続の影響度も確認した上で許可**している。 セキュリティ対策として現在は、松竹梅の梅と理事長には話しており、**松までは計画をたてて実施することで話し**をしている。**元SEが配置されたことで、改革**が進んでいる。 **リモートメンテナンスなどで、勝手に接続されることはない。**リモート端末接続用に3台準備して、ポートのID、パスワードを与えて、対応している。入ってくるところで防御している。**セキュリティ単独では難しく、更新などのタイミングで実施**している。**サイバーセキュリティの責任分界点までは入札仕様書の中にいれていない。**意識すれば良かったが、そこまではできていない。**保守にも盛り込めていない。**
2）ネットワーク構成図を把握しているか？	はい ただし、**細かいところまでは把握できていない。細かいところは記憶などで対応しているが、メインの部分については、大まかな状態を管理している。**中央棟は10年ほど前にその段階で配線図を業者の方が作成している。その他、４病棟　西、南、東などがあるが、フロアスイッチ配置されていないことから、はっきりとした配線図はなし。概要的な配線の資料はある。配下までの細かいものはない。記憶などで対応。ネットワーク保守については、**保守契約を結んで外注していたが、設置機器の脆弱性対応やバージョンアップに関しての情報提供がなく、トラブルがあった**ので、違うベンダーに変更して、現在はアップデートできるような体制となっている。（自動アップデートでなく、確認後、手動アップデートする体制。）
3）ネットワーク構成図は誰が作成して、誰が管理しているか？	ベンダーが作成、室＋ベンダーで運営
4）追加のシステムなどはどのように情報を入手して管理しているのか？	各ベンダーからシステム導入時
5）メーカ等に対してネットワーク構成図を開示しているか？（契約による場合も含む）	していない
6）情報システムに関する脆弱性情報はどのように入手して、どう活用しているか？	IPA、またはベンダーから。 **対応する場合には、限定的な端末で評価して、運用上問題ないことを確認したうえで、修正モジュールを端末に配信するようにしている。**
7）IT-BCPを作成しているか？ご恵与いただくことは可能か？また、その中に医療機器に関してはどのような形で入っているか？	はい 医療機器に関しては、外部アクセスのネットワークに接続していないので表現していない。 **バックアップデータがあれば、何とか復旧が可能なので、通信ポートを1方向として、バックアップデータを保持できるようにバックアップシステムを構築**している。 訓練シナリオなども作成して、訓練計画を策定している。メールのセキュリティ訓練も実施している。
2. 医療機器のサイバーセキュリティ確保について	

病院名	I病院
1）ネットワークに接続される医療機器についてどう管理しているか？	室＋ベンダーで運営 システム運用は室となるが、物理的な機器の管理は各部門で対応 導入の際に連絡がこなかったこともあり、購入した後に連絡がきたこともあるが、**現在では、指導的に対応していることもあり、接続する際には連絡がくることがおおよそ徹底**されている。
2）管理している場合には、どのような管理体制（誰が・どこまで）をとっているのか？（医療情報システムとの違いがあれば。）	各ベンダーからシステム導入時
3）医療機器等も含めてネットワーク構成図を把握・管理しているか？ 把握・管理している場合、医療機器に関しては特に何を把握・管理すべきか？	室からIPアドレスを払い出している。 **事務端末はHISとは別系統とはなっているが、セキュリティレベルが低く、接続端末についても把握しきれていない。**
4）医療機器のＯＳのバージョンアップやウイルス対策などを確認しているか？	ベンダーに任せているが行っていない。
5）医療機器に関する脆弱性情報はどのように入手して、どう活用しているか？	臨床工学技士会の安全情報や機器メーカ（ベンダー）からの通達
6）医療機器のサイバーセキュリティ確保について参照しているガイドライン等はあるか？あれば、ご教示いただきたい。	特になし。IPA
7）医療機器のサイバーセキュリティ確保に向けた医療機器特有の情報として、MDS2、SBOM、レガシー状態があるが、このような情報はどう管理しているか？	なし
8）医療機器メーカから、MDS2、SBOM、レガシー状態に関する情報は提供されるか？	ME、放射線部では該当なし。
9）医療機器のサイバーセキュリティ確保に向けた、臨床工学部門や放射線部門、医療機器安全管理責任者、情報システム責任者、医療安全管理者などの連携体制を構築しているか？ 構築しているようであれば、その内容をご教示いただきたい。	ME、放射線部では該当なし。
10）医療機器のサイバーセキュリティ確保について、誰がどこまで把握して、各分野において主体となって動くのは誰か？ また、その人材として必要な知識、技術、人数をご教示いただきたい。	ME、放射線部では該当なし。 情報システムも含めてセキュリティ確保のためには、**人数ではなく個々のスキルが重要**である。しかし、**病院の給料では待遇が合わず採用が難しい**。**事務職の給与体系の延長であるため、スキルが高くなったら、給与が増えるような仕組み**が必要である。
11）既存システムとの整合とセキュリティ対策の望ましい体制、人材配置をどう考えるか？（院内の連携体制なども含めて）	ME、放射線部では該当なし。
12）医療機器のサイバーセキュリティに関するインシデントやアクシデントが発生した場合の対応はどう行う想定か？（周知も含め、シナリオがあればご恵与願いたい）	障害が発生した場合は、室へ連絡。

病院名	I病院
13）医療機器のサイバーセキュリティ確保に向けて、医療従事者や在宅で使用する患者に対して、研修などをおこなっているか？行っていれば、その内容をご教示いただきたい。	ME、放射線部では該当なし。
14）医療機器のサイバーセキュリティ確保について、これだけは押えておいた方が良いというポイントがあれば、ご教示いただきたい。 （医療機器の日常的な点検で必要な項目などあれば。）	日常点検表はあるが、サイバーセキュリティに関しては行っていません。
15）医療機器を導入する際に、サイバーセキュリティ確保に関して医療機器製造販売業者との責任分界点を契約内容の中に盛り込んでいるか。盛り込んでいるようであれば、その内容をご教示いただきたい。	販売メーカ書式の売買契約書内には盛り込まれておりません。
16）医療機器のサイバーセキュリティ確保に関して、医療機器の製造販売業者との連携をしているか？しているようであれば、どのように連携しているか？	販売メーカのサービスと保守契約を締結していますが、サイバーセキュリティ連携の項目はない。
17）医療機器のサイバーセキュリティ確保に関して、経営層と情報を共有しているか。している場合には、どのような情報を共有しているか？	ME、放射線部では該当なし。情報システムについては、共有している。
18）医療機器のサイバーセキュリティ確保に関して、保守契約を結んでいるか？結んでいる場合、どのような内容か？ 可能であれば、契約書をご教示いただきたい。	サイバーセキュリティ連携の項目はない。
その他意見	○毎日のようにいろいろな情報が流れてくるが、**インターネット関係の人達は相手が同じレベルで受け取っていると思っているが、現場では受け取れていない。**拒否反応を示す職員も多い。**厚労省では通知などは出すものの、実際の現場まではとどいておらず、単なるアリバイ作りをしているのでは？** ○当院にはSEのスペシャリストがいるが、そのような**人材を配置している医療機関はない。IT業界の給与を考えると病院には来てくれない。** ○MEの教育レベルを上げて、**上級の人がサイバーを含めてできるようにするような職種の教育体制を強化することも必要ではないか。学生の時からの意識付けも重要である。セキュリティ対策の職種として担うのはMEではないか。** ○**以前は電子カルテにトラブルがあっても紙運用もできた**が、**現在は複雑になり、サイバー攻撃などで停止した場合には被害が大きい。** ○**病院側で全て対応するのは難しい。供給側で何とか対応してもらい、かかる費用について補助金などの対応も必要。** ○**ベンダーは言えば情報を出すが、言われなければ情報は出さない。情報が流れてくればベンダーに確認できるが、IPAの情報があってもそれが、自分の病院に関係するか理解できない病院が多いのではないか。ベンダーがイニシアティブを持って対応しないと解決しない。** ○**通信内容をパケットレベルで中身を解析して、モニタリングするような製品も販売されている。そのようなものを政府主導で導入して院内の設備を可視化できると分かりやすい。**どこからどう攻撃されるかも実態がわからない。**セキュリティがない状態で走っているのが危険。** ○**セキュリティ関係は投資しても売り上げにはつながらないため、費用補填の仕組みが必要。** ○**人材がいないなかでどうやって守り合うかが重要。**病院の担当者と話していてもSEレベルの話しについては、ついてこれないことも多い。 ○**サイバーセキュリティ確保に関する業者との責任分界点については、国のガイドラインなどでサンプル案を示して欲しい。この仕様を記載できるスキルがある職員がいないことが多い**ので、そのほうが対応しやすい。**病院側に不利益とならないように病院側が主体で作成**して、広めて行く必要がある。セキュリティに関しては、**底上げだけでなく、上層部を教育するような仕組み**も必要。
追加情報	○他病院との情報交換はとくにない。**今までの経験をふまえて提案**している。検討する委員会もない。 ○担当責任者は4年前に着任し、ベンダーの技術者から病院職員となった。 ○関連法人全体の管理を室で対応している。看護学校などについても、病院とは直接的にネットワークには接続されていないが、管理・設計をしている。

病院名	J 病院
病床数	約200床
施設基準：主たる基準	二次救急病院
従業員数：	521名
医師数	49名
看護師数	203名
臨床工学技士数	5名
その他職種（メディカルスタッフと事務職等）	264名
1. 医療情報システムに関するサイバーセキュリティ確保について	
1）管理する組織体制（職種・人数・役割）	病院長を責任者として、**システム安全管理責任者として、室長が対応。室長が委託業者やベンダー等のチャンネルを持っていて、やりとりしながら対応している。各部門毎に部門の責任者がシステム担当者**として管理体制図に入っている。**室長含めて、6名でシステム管理を対応。**グループ組織の方はグループの方で専従者が配置されている。ネットワークについては、兼務で対応している部分もある。情シスがもともとあって、ネットワーク周りを管理していた。その後、スマホ導入の際に、DX推進室が設置され、現在はDX推進室と情シスが一体となって動いている。 その都度ガイドラインを遵守しているかどうか確認し、ベンダーとも相談して作っている。費用対効果をみながらセキュリティレベルをどこまで導入するかを検討している。その後、サイバーセキュリティの通知が出たので、情報管理の体制だけでなく、セキュリティ関係の体制を構築。 **セキュリティに関しては各社に支援いただき、相談しながら、コスト的にはも実務的にも運用できるレベルで進めている。**部門システムとしては、PACSやエコー画像、動画サーバ、同意書スキャン、薬袋発行システム、生理検査系（心電計）、内視鏡など。院内LANの更新（3年前）の際に、ネットワーク監視を導入。変な動きがあれば、シスログが飛んでくる仕組み。振る舞い検知やEDRまでは入っていない。**何千万円のオーダとなるので、簡単には導入できない。** **情報系の担当6人については、スマホ導入の際に増員され、その後も増員してもらっている。IT知識が豊富な人ではなく、パソコン好きな人を集めて、教育しながら育成している。魅力もなく、給与も高くないので、なかなか集まらない。放射線技師や臨床工学技士も興味を示してくれない。仕事が増えても給与は上がらない。**
2）ネットワーク構成図を把握しているか？	**スマホ導入の課程の中で、セキュリティも含めて最適と考えられる構成**を構築した。 リモート回線接続については、以前は各ベンダーの責任で接続していたが、**新規は病院側がVPNアカウントを払い出して対応。**管理も病院側であるが、以前から接続がある回線は、ランサムの被害が他院であった後、調査してベンダーにしっかりとした管理をお願いしている。**調査に3ヶ月くらいかかったが、知らない間に接続されている回線もあった。**現在は新規接続は申請がある仕組みとなっている。**医療機器メーカにも確認した。**
3）ネットワーク構成図は誰が作成して、誰が管理しているか？	委託業者
4）追加のシステムなどはどのように情報を入手して管理しているのか？	購買より情シスへ連絡あり
5）メーカ等に対してネットワーク構成図を開示しているか？（契約による場合も含む）	必要な場合のみ提供
6）情報システムに関する脆弱性情報はどのように入手して、どう活用しているか？	ベンダーより連絡あり
7）IT-BCPを作成しているか？ご恵与いただくことは可能か？また、その中に医療機器に関してはどのような形で入っているか？	作成中 厚労省のテンプレートを参考にしながら進めている。
2. 医療機器のサイバーセキュリティ確保について	

病院名	J 病院
1）ネットワークに接続される医療機器についてどう管理しているか？	機器の管理は各部署。購買課→情シスに連絡があり、**IPアドレスを払い出し**。最近はベンダーの方からウイルス対策をどうするかなどの相談も多い。どちらが準備するとか。ベンダーがなんでも良いスタンスであれば、病院側指定のウイルス対策を推奨している。**ワークフローで購入申請が回ってきて、リストとして追加しているが、除却までは管理できていない。同じIPを使い回している可能性**はある。
2）管理している場合には、どのような管理体制（誰が・どこまで）をとっているのか？（医療情報システムとの違いがあれば。）	各部署管理
3）医療機器等も含めてネットワーク構成図を把握・管理しているか？ 把握・管理している場合、医療機器に関しては特に何を把握・管理すべきか？	**IPをまとめて渡して対応してもらっている。細かいところまでは把握できない。** **医療機器メーカが持ち込んだ閉鎖系のネットワークもあり、なかなか見えない。モニタ関係は閉鎖系で各ベンダーが責任を持って対応している。スマホなどで院外から生体情報を確認できることが有用であるが、実際的にはモニタからの情報はネットには出してくれない。**
4）医療機器のＯＳのバージョンアップやウイルス対策などを確認しているか？	ベンダーマター 部門にはそのような認識はない。
5）医療機器に関する脆弱性情報はどのように入手して、どう活用しているか？	ベンダーマター 部門にはそのような認識はない。
6）医療機器のサイバーセキュリティ確保について参照しているガイドライン等はあるか？あれば、ご教示いただきたい。	医療機関における医療機器のサイバーセキュリティ確保のための手引書について（令和５年３月31日） 手引き書については、**MEから情報提供があったが、ひも解いて情報展開できていない。読んでもできる人がいない。MEが手をつけてくれるとありがたい。現員では対応できない。しかし、MEも自分ところしか見えていないので、ME、検査、放射線、医療機器などという形で取り纏めないと進まない。**
7）医療機器のサイバーセキュリティ確保に向けた医療機器特有の情報として、MDS2、SBOM、レガシー状態があるが、このような情報はどう管理しているか？	**SBOMを読み取れる人が医療機関にはいない。納品時にSBOMを見た記憶はあるが、特になにもしていない。提供されていない可能性もある。** **MDSの提出を求めているが、システムベンダーからは提出されるが、医療機器については、提出してくれない。検討中が多い。メーカから連絡があれば、対応するが、最初のアクションの連絡が来ていない。**
8）医療機器メーカから、MDS2、SBOM、レガシー状態に関する情報は提供されるか？	**医療機器メーカから連絡はない。システムベンダーからは連絡があるが、医療機器は連絡はない。古い機器については、接続するなとも言えず、更新時に対応するしかない。**
9）医療機器のサイバーセキュリティ確保に向けた、臨床工学部門や放射線部門、医療機器安全管理責任者、情報システム責任者、医療安全管理者などの連携体制を構築しているか？ 構築しているようであれば、その内容をご教示いただきたい。	**医療安全とはリンクしていない。システムの安全確保だけで手一杯。**個別に各部門と案件ごとにやりとりしている。
10）医療機器のサイバーセキュリティ確保について、誰がどこまで把握して、各分野において主体となって動くのは誰か？ また、その人材として必要な知識、技術、人数をご教示いただきたい。	
11）既存システムとの整合とセキュリティ対策の望ましい体制、人材配置をどう考えるか？ （院内の連携体制なども含めて）	**資産の見える化が言われているが、IPの管理までが限界。それ以下の詳細まで管理するのが難しい。情報機器の資産管理が課題であり、継続して行うことが難しい。日常的な運用だけでも難しい。**
12）医療機器のサイバーセキュリティに関するインシデントやアクシデントが発生した場合の対応はどう行う想定か？ （周知も含め、シナリオがあればご恵与願いたい）	

病院名	J 病院
13）医療機器のサイバーセキュリティ確保に向けて、医療従事者や在宅で使用する患者に対して、研修などをおこなっているか？行っていれば、その内容をご教示いただきたい。	
14）医療機器のサイバーセキュリティ確保について、これだけは押えておいた方が良いというポイントがあれば、ご教示いただきたい。 （医療機器の日常的な点検で必要な項目などあれば。）	
15）医療機器を導入する際に、サイバーセキュリティ確保に関して医療機器製造販売業者との責任分界点を契約内容の中に盛り込んでいるか。盛り込んでいるようであれば、その内容をご教示いただきたい。	
16）医療機器のサイバーセキュリティ確保に関して、医療機器の製造販売業者との連携をしているか？しているようであれば、どのように連携しているか？	
17）医療機器のサイバーセキュリティ確保に関して、経営層と情報を共有しているか。している場合には、どのような情報を共有しているか？	
18）医療機器のサイバーセキュリティ確保に関して、保守契約を結んでいるか？結んでいる場合、どのような内容か？ 可能であれば、契約書をご教示いただきたい。	保守契約までは対応てきていない。
その他意見	○**リスクはゼロにはできないが、成果が明確でなく費用対効果が見えない**ので、なかなかスマホ導入などを進めるのが難しいところがある。 ○地元の業者だとネットワーク1つとっても、**VLANの意味も分からず話していることもあり、業者のリテラシーも千差万別。** ○事務職だけでは対応できないので、**支援してもらえるような仕組みが必要**。 ○**セキュリティの要求が上がってきている。MDRは導入しているが、EDRを導入するとなるとコストがかかる。将来的には診療データに価値を創出して、その収入でセキュリティ費用を担保するような仕組みも必要。** ○所属団体などで、**ボリュームディスカウントできると良い。機構では商材の一括購入を行っており、ウイルス対策ソフトなどもそこから購入**している。EDRも現在交渉中。 ○**セキュリティを担当する人材の評価**が必要。 ○**医療情報技師の知識はベースとしてあった方が良い。ベース知識を持った人が対話型の生成AIなどで指導してもらって解決ができるような仕組みが必要。人材育成は難しい。** ○**昔は情シスがトラブルの切り分けをしていたが、スキルがなくなってきている。**今はベンダーにお願いしているのが現状であり、情報システム自体、**自前で対応することが難しくなってきている。**電カルベンダーがネットワークの切り分けなどを行っている。 ○**セキュリティ対策をやっていることを評価してくれるような仕組みがないと、なかなか進まない。**動機付けが必要。診療報酬での誘導など。**必要だからやってくれだと対応が進まない。セキュリティ対策のゴールが見えない。他院との差が見えない。コストをクリアしないと新たなシステムが導入できない。経営者にも伝えられない。** ○**サーベイは受けなければならない。立ち位置評価のためにも。第三者評価があると病院は助かる。そうしないと、DXするにもベンダーも一歩踏み出せない。守りに入る。病院側にたって、伴走してくれるような組織が必要。監査ではなく、助言が必要。**
追加情報	○麻酔システムとして外資系業者が入っているが、システムに関する情報開示などはしてくれている。救急系は入っていない。 ○機構にシステム部会があり、半年に1回オンラインでの勉強会があり、ベンダーからのプレゼンなどで情報収集している。

病院名	K病院
病床数	約200床
施設基準：主たる基準	
従業員数：	
医師数	常勤10名、非常勤35名
看護師数	常勤65名、非常勤12名
臨床工学技士数	1名
その他職種（メディカルスタッフと事務職等）	常勤56名、非常勤12名
1. 医療情報システムに関するサイバーセキュリティ確保について	
1）管理する組織体制（職種・人数・役割）	システム委員会と電子カルテの運用を検討する委員会がある。 システム委員会→委員長は統括課長（事務）、ハード系が主。サイバーセキュリティ担当者が主に参加　ほとんど事務系で構成。セキュリティ関係も含む 電子カルテ委員会→委員長は病院長　医師、事務、外来師長で構成　運用面がメイン 双方8名づつの委員構成で、月1会程度開催。 電子カルテシステムは保守契約をしている、ハード系は業者と保守契約。セキュリティ関係の話はない。定期アップデートについては、セキュリティよりは利便性向上のため。 セキュリティパッチについては、新規導入の際に対応する程度。 **担当者は臨床工学技士として5年前に採用され、高校が情報系ということもあり、セキュリティ関係の業務を併任している。** 周知が必要な情報については、システム委員会で共有して回覧や月1回の院回会議（常勤医師全員とそれぞれの代表が集まる会議）で周知。 UTM（Unified Threat Management）を設置し、設定は担当者が自前で行っている。
2）ネットワーク構成図を把握しているか？	**電設係やそれぞれのメーカが作成。それを集めて把握**している。絶対に提出されるような仕組みではないが、ネットワーク接続の会話の中で収集している。 リモートメンテについては、回線は病院側で準備して、ルータの設定管理などは業者にお願いしている。過去には勝手に接続していたこともあるが、担当者が5年前に赴任した以降は病院側で管理している。不明な接続回線もあるが、それは目をつぶっている状態。ルータは6台程度。
3）ネットワーク構成図は誰が作成して、誰が管理しているか？	**それぞれが作成した物を担当者が収集して把握**
4）追加のシステムなどはどのように情報を入手して管理しているのか？	ネットワーク接続する際の会話の中で収集
5）メーカ等に対してネットワーク構成図を開示しているか？（契約による場合も含む）	なし
6）情報システムに関する脆弱性情報はどのように入手して、どう活用しているか？	**ネットの情報やベンダーからの情報。関係があれば対応するが、安定性をみて対応。テストした後、安定性が保てない場合には対応できない。**業者から持ち込まれる事例はないが、セキュリティパッチを当てるような事例が発生した場合には、CDから病院側で対応するか、業者に来院してもらって対応することを想定している。
7）IT-BCPを作成しているか？ご恵与いただくことは可能か？また、その中に医療機器に関してはどのような形で入っているか？	作成中。システム委員会で事務的なたたき台を作成してもらった後、担当者が手を加える予定。
2. 医療機器のサイバーセキュリティ確保について	

病院名	K病院
1）ネットワークに接続される医療機器についてどう管理しているか？	**パソコンについては、OSを10に切り替え、11に切り替えられるものは変えている。**相互互換性がなく、不便だったため切り替えを行い、システム委員会で管理している。勝手に接続できないようになっている。ベンダー側でも把握していないことが多く、病院側で管理している。外部ネットワークに直接接続されている医療機器等は2-3台、遠隔診療用の機器。閉鎖回線には200-300台接続されている。
2）管理している場合には、どのような管理体制（誰が・どこまで）をとっているのか？（医療情報システムとの違いがあれば。）	**管理というより知っている程度。**管理まではできていない。ログは取っている。
3）医療機器等も含めてネットワーク構成図を把握・管理しているか？ 把握・管理している場合、医療機器に関しては特に何を把握・管理すべきか？	
4）医療機器のＯＳのバージョンアップやウイルス対策などを確認しているか？	**メーカ任せ。こちら側は触れない。メーカ側が言ってくれれば対応する。**
5）医療機器に関する脆弱性情報はどのように入手して、どう活用しているか？	**ハードに関する脆弱性を知っていても、動かなくなることが怖いので、何もできない。メーカ検証の上であれば、対応はできる。**
6）医療機器のサイバーセキュリティ確保について参照しているガイドライン等はあるか？あれば、ご教示いただきたい。	ない。**あったとしても誰が理解できるかが不明**。**院内教育用の資材**もほしい。
7）医療機器のサイバーセキュリティ確保に向けた医療機器特有の情報として、MDS2、SBOM、レガシー状態があるが、このような情報はどう管理しているか？	**最近、輸液ポンプをWiFiにつないだが、メーカからは特にそのような情報はなかった。保守点検のデータ抽出で利用している。今回のヒアリングで初めてそのような情報があることを知った。**
8）医療機器メーカから、MDS2、SBOM、レガシー状態に関する情報は提供されるか？	**ない。**
9）医療機器のサイバーセキュリティ確保に向けた、臨床工学部門や放射線部門、医療機器安全管理責任者、情報システム責任者、医療安全管理者などの連携体制を構築しているか？構築しているようであれば、その内容をご教示いただきたい。	**医療機器安全管理責任者がサイバーセキュリティ担当者を兼ねている**ので、連携をしているといえばしている。ネットワークに接続する医療機器は現在は少ないが、クラウドに移行した場合には多くなると想定される。
10）医療機器のサイバーセキュリティ確保について、誰がどこまで把握して、各分野において主体となって動くのは誰か？また、その人材として必要な知識、技術、人数をご教示いただきたい。	**サイバーセキュリティ担当者１名。詳しく知っているというよりは、高校で情報関係を卒業したレベル。**
11）既存システムとの整合とセキュリティ対策の望ましい体制、人材配置をどう考えるか？（院内の連携体制なども含めて）	**各部門に一人は欲しい。事務が幹線のネットワークを把握してくれるのが理想。**
12）医療機器のサイバーセキュリティに関するインシデントやアクシデントが発生した場合の対応はどう行う想定か？（周知も含め、シナリオがあればご恵与願いたい）	システム委員会で連絡網の作成などを整備予定。**医療機器に特化する場合には、パターンが多すぎて、マニュアル化できない**ことに悩んでいる。

病院名	K病院
13）医療機器のサイバーセキュリティ確保に向けて、医療従事者や在宅で使用する患者に対して、研修などをおこなっているか？行っていれば、その内容をご教示いただきたい。	在宅での医療機器はない。**患者への説明が必要な場合には、オンライン診療のシステムを流用して行うことを想定**している。
14）医療機器のサイバーセキュリティ確保について、これだけは押えておいた方が良いというポイントがあれば、ご教示いただきたい。 （医療機器の日常的な点検で必要な項目などあれば。）	**UTM、ディフェンスルータの設置、セキュリティソフトの導入。MDRも導入したいができていない。** **医療機器にネットワーク接続ケーブルが何本刺さっているか把握が必要。ITパスポート程度の用語の理解が必要。**
15）医療機器を導入する際に、サイバーセキュリティ確保に関して医療機器製造販売業者との責任分界点を契約内容の中に盛り込んでいるか。盛り込んでいるようであれば、その内容をご教示いただきたい。	なし
16）医療機器のサイバーセキュリティ確保に関して、医療機器の製造販売業者との連携をしているか？しているようであれば、どのように連携しているか？	なし
17）医療機器のサイバーセキュリティ確保に関して、経営層と情報を共有しているか。している場合には、どのような情報を共有しているか？	**している。システム委員長に報告し、連絡窓口、周知を行う。レポート対応などが必要であればシステム委員長が対応。現場のトップとして統括する立場であるが、専門的な知識があるわけではない。医事課を纏めている方が担当している。その後、事務部長→院長→理事長へ情報があがっていく。**
18）医療機器のサイバーセキュリティ確保に関して、保守契約を結んでいるか？結んでいる場合、どのような内容か？ 可能であれば、契約書をご教示いただきたい。	ない
その他意見	○**医療版ISACも整理されておらず、予算もバラバラ。予算が分散化されてばらまいているので、各医療機関レベルになると数万円程度にしかならない。慢性期病院でも赤字が拡大しているので、サイバーセキュリティまでの予算が確保できない。情報システムも1床250万円の世界が、400万円以上となり、立ちゆかない。病院が1つの空間の中で公的に守ってもらえるような仕組みが良い。** ○**勉強資材として、病院事務系のセキュリティ関係のものがあると良い。**
追加情報	○**セキュリティ関係で他院とのつながりはない。**新規導入する際に声をかけるぐらい。 ○臨床工学技士としては、呼吸器18台、輸液ポンプや麻酔器の日常点検などを実施。**臨床工学技士として採用された移行、徐々に情報系の仕事が増えていき、3：7で情報系の仕事が多くなっている。**コロナきっかけやランサム被害が増えてきたこともあり、情報系の仕事が増えている。診療放射線技師は関わっていない。 ○**自前でやっているので安くすんでいる。後任として、事務の人員を育成しているが、後任の確保が課題。情報交換する先もない。**

別紙 6

厚生労働科学研究費補助金　研究班へのヒアリング（要約）

目　的：厚労科研で大阪大学を中心に取り組んでいる、情報セキュリティ人材の育成と配置についての現状と課題について意見交換を行う。

いただいた主な意見：

○厚労科研で医療機関への情報セキュリティ人材の育成と配置についてまとめている。

○指導的な立場の医療機関にはグループＡ人材+グループＣ人材、自施設の情報システムを守ることができる医療機関（400 床以上をイメージ、地域医療に大きな影響を生じる医療機関）にはグループＢ人材＋グループＣ人材、他施設や企業の助けを借りて情報システムを守る医療機関にはグループＣ人材を配置するようなイメージで議論している。

○グループＡ人材は自施設だけでなく、他施設も指導、チェックできるような人材で、グループＣ人材はグループＡ人材や企業の力を借りながら自施設の情報セキュリティ対策を講じる人材であり、情報セキュリティに関する用語を理解し、企業からの提案に対して疑問を感じることができるような人材をイメージしている。

○医療安全や感染症対策のように、指導病院が地域の病院と連携して守るようなイメージであり、指導病院間で相互チェックを行ったり、地域の病院へのセミナーや訓練を行ったりするイメージである。

○また、各医療機関で情報部門だけでなく、各部門システムや医療機器のサイバーセキュリティ確保のために各部門にグループ C 人材を配置し、面で守っていくようなイメージとしている。

○グループＡ人材は、上級医療情報技師相当野資格や実務経験、実地研修などを必要とし、グループＢ人材は、医療情報技師相当、グループＣ人材は医療情報基礎知識検定試験相当の知識を求めている。

○研究班には、診療放射線技師や臨床工学技士も入り、各職種がグループＣ人材を担うようにするにはどうすれば良いかも議論され、各団体で取組みを始めている。

○サイバーセキュリティに関しても感染症と同じように診療報酬の仕組みに取り入れられないか検討を進めている。

医療機関における医療機器のサイバーセキュリティ確保に関する実態調査内容

※選択項目については、必須回答となりますが、4-0 以降の自由記載については、任意となります。

1　基本情報

0. 姓、名、電話（ハイフンは不要)、メールアドレスの入力（必須）

回答を途中まで入力し終了し、再度継続入力するため。及び回答に事項の確認が必要な場合に、照会をするためのもので、他に使用することはありません。

回答内容：姓、名、電話番号、(内線)、メールアドレス

1-0. 病院名の匿名化を希望されますか？（単一回答）

※実名でご回答いただいた場合も一切公表しませんのでご安心ください。

A：匿名化希望　　B：実名可能　病院名、住所等（自由記載）

1-1. 病院の種類を教えてください。

病院規模別機能別に集計を行い今後のセキュリティ対策の参考となる資料を作成するためです。

A：特定機能病院　B：一般病院　C：精神科病院

1-2. 所属されている医療施設の開設者区分を教えてください。

病院規模別機能別に集計を行い今後のセキュリティ対策の参考となる資料を作成するためです。

A：国　B：公的医療機関　C：社会保険関係団体　D：医療法人　E：個人　F：その他（自由記載）

1-3. 承認病床数を教えてください。

病院規模別機能別に集計を行い今後のセキュリティ対策の参考となる資料を作成するためです。

一般病床（　　）床、感染症病床（　　）床、結核病床（　　）床、

療養病床（　　）床、精神病床（　　）床、保険外病床（　　）床

2-0. アンケート結果（医療機関名は匿名化）のフィードバックをいたします。

ご希望の場合には、連絡先のメールアドレスをご記入ください。なお、メールアドレスは、所属されている医療機関のドメインを含むものを入力してください。

必要：メールアドレス（　　）　　不要

3-0. 従業員数（常勤）を教えてください。

※その他には、上記 4 職種以外で、その他従業員数（常勤）(事務も含む）を記載してください。

医師（　）名、　看護師（　）名、臨床工学技士（　）名、診療放射線技師（　）名、

その他（　）名

Ⅱ　医療情報システム全般について

4-0. 貴院の情報システムの管理体制についてもっともよくあてはまるものをひとつ選んでお答えください。

A：管理体制がなく院長自ら管理している　B：専門の担当部門がある

C：担当部門はないが、専任者がいる　　D：外部に委託している　　E：何もしていない

4-1-1. 4-0 の質問で B～D の回答された場合には、以下をお答えください。

管理する組織体制（職種・人数・役割）を責任者とその他にわけて教えてください。

体制がない場合には、責任者の欄になしと記載してください。

外部委託の場合には、職種の欄に【委託】と記載してください。

いない場合には、人数を【0】と回答してください。

※WEB 画面では入力の関係で質問を聞く順番が変更されています。

A：責任者：職種（　　）　人数（　　）　役割（　　）

B：その他：職種（　　）　人数（　　）　役割（　　）　※1

4-1-2. そのうち、サイバーセキュリティ確保に従事する職員の人数と職種・保有資格を教えてください。
（保有資格がない場合はなしとしてください）（いない場合には【人数】を 0 と回答してください）
人数（ ）名　職種（　　） 保有資格（　　）

4-1-3. 4_1_2 のうち、医療機器のサイバーセキュリティ確保に従事する職員の人数と職種・保有資格を教えてください。いない場合には、【人数】を 0 と回答ください。
人数（ ）名　職種（　　） 保有資格（　　）

5-0. ネットワーク構成図を作成していますか？（単一回答）
A：作成していない。（6-0 項へ）
B：担当者は把握しているが、資料としてはない。（担当者の記憶のみ）。（6-0 項へ）
C：作成している。（5-1 項へ）

5-1. ネットワーク構成図がある場合、その更新のタイミングはどのようにしていますか？（単一回答）
A：更新を行っていない。　B：定期的に更新・確認を行っている。
C：追加システム導入の際に更新している。

5-2. ネットワーク構成図は誰が作成して、誰が管理していますか？（単一回答）
A：内部で作成して、内部で管理　　B：システム導入時に導入業者が作成して、内部で管理
C：ネットワーク保守管理を行う委託業者が作成して、内部で管理
D：ネットワーク保守管理を行う委託業者が作成して、委託業者が管理

5-3. 追加のシステムや追加の保守用回線などはどのように情報を入手して管理していますか？
A：入手していない　　B：入手している→詳細を教えてください。（自由記載）

5-4. ネットワーク構成図を自動作成するツールは導入されていますか？（単一回答）
A：導入している→（ツール名製品名等をご教示ください）
B：導入しておらず手作業で作成している場合について
B-1（自動的作成するツールがあれば導入したい）
B-2（自動作成ツールは不要）

5-5. リモートメンテナンス回線（企業等が遠隔メンテナンス等で利用するような回線）の把握はしていますか？
A：している→回線のセキュリティ対策の具体策について記載してください。 B：していない

6-0. 情報システムに関する脆弱性情報はどのように入手していますか？
A：入手していない　　（7-0 項へ）
B：入手している→入手先（自由記載）

6-1. 入手した情報をどのように活用していますか？
A：活用していない　　（7-0 項へ）
B：脆弱性についての対応を行う

6-2. 脆弱性についての対応を行う場合、今まで苦労した点などありますか？
（自由記載）

7-0. IT-BCP（IT-Business Continuity Plan）を作成していますか？
A：作成している
B：作成していない　（8-0 項へ）

7-1. その中に医療機器に関してはどのような形で入っていますか？
A：入っている→具体を教えてください。（自由記載）　　B：機器までは入っていない

8-0. 貴院では、サイバーセキュリティ対策に関する費用を計画的に用意していますか。（単一回答）
A：計画的費用はない　（8-3 項へ）
B：不足しているが、必要に応じて予算化している　（8-1 項へ）

C：計画的に使えるように毎年予算化して用意している　（8-1 項へ）

8-1. 用意している場合、年間どの程度を確保していますか？

年間（　　）万円程度

8-2. 具体的にどのような用途に使用していますか？

（自由記載）

8-3. セキュリティ対策の財源についてのご意見をお聞かせください。（単一回答）

A：診療報酬制度などで担保される必要がある

B：インフラ整備の一環であるため、自己財源で措置するしかいない

C：安全な医療実現のため、選定療養費などで患者からの徴収できる仕組みが必要ではないか

9-0. サイバーセキュリティ対策が必要な医療機器があることについてお答えください。（単一回答）

A：知らないまたは医療機器のセキュリティ対策の知識はない

B：必要であると思うが、医療機器のセキュリティについてあまり知らない

C：知っている

Ⅲ　医療機器のサイバーセキュリティ確保について

10-0. ネットワークに接続される医療機器について把握していますか？（複数回答）

A：情報システム部門で把握している。

B：情報システム部門では把握していない。　（11-0 項へ）

C：使用部署が把握している。　（11-0 項へ）

D：全く把握できていない。　（13-0 項へ）

10-1. どのような情報まで把握していますか？（情報システム部門として）（複数回答）

A：医療機器に接続されている IP アドレス　B：ネットワークに接続している機器の製造販売業者

C：接続している機器の機種名　D：ネットワーク接続する用途

E：医療機器の固定されている MAC アドレス　F：医療機器に関する使用 OS

G：医療機器との通信プロトコル　H：医療機器のリモート保守回線の有無

I：医療機器のリモート保守回線の接続方法

11-0. ネットワークに接続されている医療機器が更新/追加された場合にどのように情報システム部門では把握していますか？

A：把握している→詳細を記載してください。（自由記載）　B：把握していない

12-0. ネットワーク構成図には医療機器の情報まで反映されていますか？

A：反映している　B：反映していない

13-0. 医療機器のＯＳのバージョンアップやウイルス対策などを確認していますか？

A：確認している　B：確認していない

14-0. 医療機器に関する脆弱性情報を入手していますか？

A：入手している　B：入手していない(15-0 項へ)

14-1. その情報をどう活用していますか？

A：活用していない　B：パッチを当てるなどの対策を取っている

14-2. その情報はどこで入手されましたか？（複数回答）

A：医療機器製造メーカが提供してきた

B：医療機器を販売した地元等の販売会社が提供してきた

C：保守契約を締結している相手先が提供してきた

D：自分で情報を入手している

15-0. 医療機器のサイバーセキュリティ確保について参照しているガイドライン等は何ですか？

A：医療機関における医療機器のサイバーセキュリティ確保のための手引書を活用している

B：医療機器のサイバーセキュリティ対策の参考資料はない

C：これら以外（自由記載）

16-0. 医療機器のサイバーセキュリティ確保に向けた医療機器特有の情報として、MDS2、SBOM、レガシー状態があるが、このような情報を入手していますか？（単一回答）

【参考】※医療機器セキュリティのための製造業者開示説明書（MDS2：Manufacturer Disclosure Statement for Medical Device Security）は、医療機器内に組み込まれたセキュリティおよびプライバシー対策機能に関する標準化された情報を提供することにより、医療提供組織内のセキュリティリスクマネジメントを支援することを目的としている。

※SBOM（Software Bill of Materials）とは「ソフトウェア部品表」のことで、ソフトウェアに含まれる「材料」をリストアップしたもの。

※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に保護できない医療機器であり、新しい、古いにかかわらず、該当してしまう可能性がある。

A：医療機器販売会社等から提供され入手している

B：医療機器販売会社等へ問い合わせたが、一部しか入手できなかった

C：医療機器販売会社等に問い合わせたが、入手できなかったので、自分で調査している

D：情報の存在を知らない

17-0. 貴院のサイバーセキュリティ対策を検討するにあたって、個々の医療機器に施されているサイバーセキュリティ対策の情報※が必要か当てはまるものすべてお答えください。（複数回答）

【参考】※ 医療機器内に組み込まれたセキュリティおよびプライバシー対策機能に関する標準化された情報やソフトウェアコンポーネント(部品表・構成表)の情報など。このような資料を製造業者開示説明書(MDS2)と呼びます。

A：購入検討時に必要　　B：機器選定後の購入時に必要

C：現在の体制では必要ない　D：もらっても専門的過ぎてわからない。

18-0. 医療機器メーカから、MDS2、SBOM、レガシー状態に関する情報は提供されていますか？（単一回答）

A：業者主導で提供される　　B：病院側が言えば提供される

C：病院側が言っても提供されない　D：業者から提供されたことがない

19-0. 医療機器のサイバーセキュリティ確保に向けた、臨床工学部門や放射線部門、医療機器 安全管理責任者、情報システム責任者、医療安全管理者などの連携体制を構築しているか？

構築しているようであれば、その内容をご教示いただきたい。(単一回答)

A：構築している　　B：構築しているが人材育成ができていなく、名目的である

C：構築をしていないが検討中である　D：構築していなく今後も人員上構築が望めない

19-1. 構築している場合には、その内容についてお答えください（単一回答）

A：院内の規程に明記している

B：規程に明記していないが任命している

C：任命していないが毎月等の定例ミーティングを開催している

D：その他の方法（自由記載）

20-0. 医療機器のサイバーセキュリティを確保するための望ましい体制や人材配置について、どのように考えますか？（複数回答）

A：必要な人員数（増員数に関する自由記載）

B：専門部門の設置（専門部門設置に関する自由記載）　C：セキュリティ対策の予算化

D：セキュリティ関係の調査　　E：セキュリティ関係の外部委託会社等の契約の必要性

F：その他（自由記載）

21-0. 医療機器を導入する際に、サイバーセキュリティ確保に関して医療機器製造販売業者との信頼境界(責任分界点に近い概念)を契約内容の中に盛り込んでいますか？（単一回答）

A：盛り込んでいる　　B：盛り込んでいない

22-0. 医療機器のサイバーセキュリティ確保に関して、医療機器の製造販売業者と情報共有の連携をしていますか？

A：している

B：していない　（23-0 項へ）

22-1. 医療機器を購入した際に、販売業者から医療機器のサイバーセキュリティに関する説明がありましたか、また、貴院での理解度についてお答えください。(単一回答)

A：説明はなかった　　B：説明があったが、内容は理解できなかった。

C：説明があり、内容も十分に理解できた。

23-0. サイバーセキュリティ確保に関して、経営層と情報を共有していますか？（複数回答）

A：共有していない　　B：情報システムのサイバーセキュリティに関して共有している

C：医療機器のサイバーセキュリティ確保に関して共有している

24-0. 医療機器のサイバーセキュリティ確保に関して、保守契約を結んでいますか？

A：結んでいる　　B：結んでいない

25-0. 自施設でのサイバーセキュリティ対策の評価を現状で 100 満点換算で何点ぐらいと自己評価されますでしょうか。(点数は大まかな印象（10 点刻み）で入力ください。)

（　　）点

26-0. また、現状から 100 点を目指すとしたら、何年くらいかかることを想定していますか？

（　　）年

27-0. その他ご意見があれば記載をお願いします。

（自由記載）

Ⅳ　その他

28-0. ネットワークに接続されている医療機器等を可視化するツールがあれば、利用したいと思いますか？（価格は別として。）

A：利用したい　　B：既に可視化できているので、利用するつもりはない

29-0. 医療機器のサイバーセキュリティ確保に関して、ネットワークに接続されている医療機器等を可視化するような実証事業ができた場合には、参加いただくことは可能でしょうか。

A：はい　　B：いいえ

30-0. お手間をおかけしないように努力しますが、追加でヒアリングを受けていただくことは可能でしょうか？

A：はい　　B：いいえ

31-0. 研究班から連絡をとることに同意いただける場合には連絡先（所属部署・氏名・メールアドレス）を改めて教えてください。

姓、名、メールアドレス、施設名、部署名

以下、国立大学病院のみに質問

32-0. 他院の情報システム導入やネットワークセキュリティサポートに自院の人材を派遣されていますか？

A：はい（具体例について自由記載）　　B：いいえ

別紙５

「厚生労働科学研究費における倫理審査及び利益相反の管理の状況に関する報告について
（平成26年4月14日科発0414第5号）」の別紙に定める様式

令和７年４月30日

厚生労働大臣
（国立医薬品食品衛生研究所長） 殿
（国立保健医療科学院長）

機関名　国立大学病院長会議

所属研究機関長　職　名　会長

氏　名　大鳥　精司

次の職員の(元号)　　年度厚生労働科学研究費の調査研究における、倫理審査状況及び利益相反等の管理については以下のとおりです。

１．研究事業名

２．研究課題名　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（24CA2013）

３．研究者名　（所属部署・職名）　事務局　理事・事務局長

（氏名・フリガナ）　塩﨑　英司（シオザキ　エイジ）

４．倫理審査の状況

	該当性の有無 有	無	左記で該当がある場合のみ記入（※1） 審査済み	審査した機関	未審査（※2）
人を対象とする生命科学・医学系研究に関する倫理指針（※3）	□	■	□		□
遺伝子治療等臨床研究に関する指針	□	■	□		□
厚生労働省の所管する実施機関における動物実験等の実施に関する基本指針	□	■	□		□
その他、該当する倫理指針があれば記入すること（指針の名称：　　）	□	■	□		□

（※1）当該研究者が当該研究を実施するに当たり遵守すべき倫理指針に関する倫理委員会の審査が済んでいる場合は、「審査済み」にチェックし一部若しくは全部の審査が完了していない場合は、「未審査」にチェックすること。

その他（特記事項）

該当なし

（※2）未審査の場合は、その理由を記載すること。

（※3）廃止前の「疫学研究に関する倫理指針」、「臨床研究に関する倫理指針」、「ヒトゲノム・遺伝子解析研究に関する倫理指針」、「人を対象とする医学系研究に関する倫理指針」に準拠する場合は、当該項目に記入すること。

５．厚生労働分野の研究活動における不正行為への対応について

研究倫理教育の受講状況	受講 ■　未受講 □

６．利益相反の管理

当研究機関におけるＣＯＩの管理に関する規定の策定	有 □　無 ■（無の場合はその理由：東京大学医学部附属病院に委託）
当研究機関におけるＣＯＩ委員会設置の有無	有 □　無 ■（無の場合は委託先機関：東京大学医学部附属病院）
当研究に係るＣＯＩについての報告・審査の有無	有 ■　無 □（無の場合はその理由：
当研究に係るＣＯＩについての指導・管理の有無	有 ■　無 □（有の場合はその内容：

（留意事項）　・該当する□にチェックを入れること。
・分担研究者の所属する機関の長も作成すること。