日医総研ワーキングペーパー

医療機器に関わるサイバーセキュリティの動向

No.465

2022年3月22日

日本医師会総合政策研究機構

医療機器センター附属医療機器産業研究所

医療機器に関わるサイバーセキュリティの動向

日本医師会総合政策研究機構　　坂口一樹、堤　信之
医療機器産業研究所　　松橋祐輝、本田大輔、中野壮陛

キーワード
◆医療機器　◆医療ＤＸ　◆サイバーセキュリティ
◆責任分界点　◆サプライチェーン

ポイント

◆ 本稿では、医療機器のサイバーセキュリティ確保に関連するこれまでの政策と海外の状況、主要な関連団体とその取り組みを整理したうえで、製造販売業者と医療現場をそれぞれ対象とした２つの調査結果を確認した。

◆ 日本では、2014 年のサイバーセキュリティ基本法の制定を嚆矢として取り組みが進み、内閣府に本部機能を置き、戦略と行動計画が定められている。この戦略と計画において、医療は、国家機能の中枢を担う重要インフラのひとつとの位置づけであり、医療機器のサイバーセキュリティに関わる施策や規制についても、上記のような文脈で進められてきた。

◆ 研究開発やサプライチェーン、資本構成等がグローバルに跨る医療機器産業のサイバーセキュリティ確保にあたっては、規制や対処方針について、可能の限りの国際協調が求められる。現在、日本では行政と業界団体が主導して、国際医療機器規制当局フォーラム（IMDRF）のガイダンスの導入と運用の準備を進めている。欧米においても、日本とほぼ同時期に、医療機器に関するサイバーセキュリティ確保のための法整備がなされてきている。

◆ 製造販売業者を対象とした実態調査からは、対象企業の組織体制の整備が発展途上である現状とユーザーである医療現場への情報提供や説明責任に課題があることが明らかになった。一方、病院・診療所を対象とした実態調査からは、医療機器のサイバーセキュリティという課題そのものに対する現場の認知度がまだまだ低いことが浮き彫りになった。

◆ 以上を踏まえ、医療機器のサイバーセキュリティに関わる主なステークホルダーの役割分担と責任分界に留意しつつ、医療機器産業と政治・行政に対して、将来に向けた提言を行った。

目　次

１．　イントロダクション

（１）背景と問題意識

昨今、サイバーセキュリティに関わる事件・事故が世間の耳目を集めている。医療分野においても、既に複数の医療機関において、サイバー攻撃によって電子カルテが暗号化され参照不能になった事例や、院内ネットワークにつながったパソコンや医療機器のデータが暗号化され機能が停止したといった通常業務の遂行に重大な支障をきたした事例が報告されている[1]。今のところ、医療機器そのものの安全性に致命的な不具合が発生した事例は把握されていない。しかし、医療機器に対するサイバー攻撃が原因でこれらの機器が正常に機能しなくなれば、患者の身体・生命がたちまちに危険にさらされる怖れがあるという点において、医療機器のサイバーリスクは、その他のデバイスのサイバーリスクよりもはるかに深刻度が高い。また命にかかわる事態に至らずとも、サイバー攻撃により医療情報が外部に漏洩するような事態になれば、社会的なインパクトの大きい、重大インシデントとなりうる。

さらにサイバー攻撃には、一旦サイバー事故が発生すると直ちに原因を究明することが難しく、被害の全容の把握も困難という厄介な特性がある。不正アクセスの原因もさることながら、そもそも何をされたのか分からないと対策が出来ず、対応指示もできない。現実にも、インターネットアクセスができなくなることで、医療機器類のログやアップデート情報の調査もままならない、という事態に陥った事例が報告されている[2]。医療機関は、そのような状況下にあっても業務、すなわち医療行為の継続を求められることの多い、大変難しい立場にある事業体である。

---

[1]「【独自】『身代金』ウイルス、11 病院が被害　救急搬送や手術に支障も」（読売新聞オンライン、2021 年 12 月 29 日）　https://www.yomiuri.co.jp/national/20211228-OYT1T50173/
「【独自】国際ハッカー集団、都立 2 病院を標的か　チャットに職員アドレス大量掲載」（読売新聞オンライン、2021 年 12 月 30 日）　https://www.yomiuri.co.jp/pluralphoto/20211229-OYT1I50139/
その他、これまでの主な事件の関連主要記事は、以下の通り（①～③）。
① 奈良県宇陀市立病院事件については、「ランサムウェアで電子カルテが利用不能に、復旧が長引いた理由とは」（日経クロステック、2020 年 5 月 8 日）
https://xtech.nikkei.com/atcl/nxt/column/18/01157/042800010/
② 福島県立医科大学附属病院事件については、「福島の病院、サイバー被害　17 年発生　県立医大付属、公表せず　身代金ウイルス、医療機器停止　病院に攻撃海外で相次ぐ　手術延期のケースも」（日本経済新聞、2020 年 12 月 3 日）
③ 徳島県つるぎ町立半田病院サイバー事故：「身代金払わず 2 億円で新システム　徳島サイバー被害病院」（日本経済新聞、2021 年 11 月 25 日）

[2] 秋冨慎司（2021）「医療機器高度化に伴う医療情報のサイバーセキュリティマネジメントに関する研究」日医総研委託研究報告（2021 年 3 月）https://www.jmari.med.or.jp/research/research/hb_130.html

このように医療現場はサイバー攻撃に対して難しい環境に置かれているにもかかわらず、医療機関と医療機器の製造販売業者（以下「製造販売業者」と言う）のサイバーセキュリティ対策の現状と言えば、ともに外部からの攻撃を防衛するという経験自体初めてのことであり、情報やノウハウの蓄積が十分な状況にはないように見える。それだけになおのこと、医療のデジタル化や機器の IoT 化が進む将来のサイバーリスクを見越して、サイバーセキュリティ対策分野で、医療界および医療機器業界が互いに連携しつつ対応できるように、先手を打った対策の検討が肝要と考える。

一方で、医療機関と製造販売業者は、医療機器の使用者と供給者という関係でもあり、両者が連携する上ではお互いの責任分界点を明らかにする必要がある。責任分界点の意識レベルが低いと製造販売業者側には、「医療機器の取り扱いの責任は、医療機関の管理者の責任」との意識が先行しかねない。「自らが提供する製品・サービスの情報セキュリティ／サイバーセキュリティ対応が十分されていること」および「医療機関に対して管理のために必要な情報を適切に提供すること」が求められることの認識が薄まる怖れがある。他方で、医療機関側には、「医療機器に関するサイバーセキュリティは医療機器メーカ側の責任」との行き過ぎた意識を招きかねない。

また「サイバーセキュリティが必要な医療機器」については、行政ガイダンス[3]や IMDF ガイダンス[4]で一定の定義づけがされているものの、実際には医療機器は多種多様で、個々の製品について必要なサイバーセキュリティ対策が異なる上に、同じ製品でも医療機関における実際の使用環境を含めて考える必要がある。このため、製造販売業者が個別の局面で、医療機器のサイバーセキュリティについて、具体的な対策を的確に実施することは難しい状況下にあり[5]、行政ガイダンスのレベルでの責務の遵守が、必ずしも十分でない可能性がある。

---

[3] 「医療機器のうちプログラムを使用したもの（医療機器プログラムを含む。）及び付属品等にプログラムを含むものである。医療機器のクラス分類（Ⅰ～Ⅳ）を問わない。基本的に、医療機器と接続して使用する又は併用される IT 機器等（単体で医療機器に該当しないもので、プログラム単体の場合を含む。）を医療機器の構成品（付属品等）として提供する場合は、（・・・中略・・・）対象となる」
厚生労働省（2018）「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」（厚生労働省通知 薬生機審発 0724 第 1 号・薬生安発 0724 第 1 号　別添資料）より。
https://www.mhlw.go.jp/content/11121000/000346114.pdf

[4] 「ファームウェア及びプログラマブルロジックコントローラ等のソフトウェアを有する医療機器（例：ペースメーカ、輸液ポンプ）、又はソフトウェア単独で存在する医療機器（例：SaMD）」
IMDRF（2019）「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」（2020 年 3 月 18 日）より。　https://www.jrs.or.jp/uploads/uploads/files/information/mhlw_20200513.pdf

[5] 医療機器センター「医療機関の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」
http://www.jaame.or.jp/mdsi/cs21/index.html

（２）本稿の目的

本稿の目的は、医療機器のサイバーセキュリティに関連するこれまでの政策や関連団体の取り組み、そして現場の実態を概観し、将来に向けた提言を行うことである。

提言の検討にあたっては、次の２点に留意した。第一に、行政および業界団体、個別の製造販売業者、そして医療現場という主要なステークホルダーの役割分担と責任分界である[6]。第二に、サプライチェーン、すなわち医療機器が製造販売業者によって開発・供給され、医療機関の現場で使用・管理され、役割を終えて廃棄されるまで一連の流れである。かかる医療機器のサプライチェーン全体を通して、対策が切れ目なく構築され、維持される体制構築に資する提言を意識した。

（３）本稿における議論の構成

本稿における議論の構成は、次の通りである。第 2 章では、医療機器のサイバーセキュリティに関する施策の大枠を把握するために、わが国の行政のこれまでの取り組みと規制の動向、関連する主要団体の取り組み、そして海外の取り組みの動向について概観する。第 3 章では、現場の実情を複眼的に捉えることを主眼とし、医療機器の製造販売業者向け調査[7]および医療機器のユーザーである病院・診療所向け調査[8]の２つの実態調査から、医療機器のサイバーリスクの管理について、現場の実情を示すデータを明らかにする。第 4 章では、前章までの議論を総括し、今後、医業機器業界に期待されることを提示し[9]、将来に向けた政策提言を行う。なお、本稿のとりまとめにあたっては、医療機器センター附属医療機器産業研究所と日本医師会総合政策研究機構の研究者らによる共同執筆とした。前者は公益財団法人医療機器センターのシンクタンクであり、後者は公益社団法人日本医師会のシンクタンクである。

---

[6] ステークホルダーとしては、他にも「医療情報システム・サービス事業者」や「一般国民・患者」が挙げられるが、本稿では本文に挙げた３つを主要な３者とした。

[7] 医療機器センター（2019）「AMED（医薬品等規制調和・評価 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に係る課題抽出等に関する研究」（2020 年 3 月）
http://www.jaame.or.jp/mdsi/cs21/CS-industry.pdf

[8] 医療機器センター（2020）「AMED（医薬品等規制調和・評価 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に係る課題抽出等に関する研究」（2021 年 3 月）
http://www.jaame.or.jp/mdsi/cs21/CS-hdos.pdf

[9] 医療機関向けのサイバーセキュリティ確保に向けた提言については、坂口、堤（2021）にまとめたため、ここでは繰り返さないこととした。

２．施策の動向

本節では、これまでの医療機器のサイバーセキュリティに関連する政策議論の流れと現状の施策の概説を行う。

（１）行政の取り組み

①これまでの経緯

サイバーセキュリティの確保という社会課題に対する立法として、最も重要な法律は 2014 年 11 月に成立した「サイバーセキュリティ基本法」である。同法に基づき、2015 年 1 月、内閣に「サイバーセキュリティ戦略本部」が、内閣官房に「内閣サイバーセキュリティセンター」（NISC）が設置され、そこで「医療」はセキュリティ確保に注力すべき重要インフラのひとつに指定されている。内閣サイバーセキュリティセンターからは、基本法第 12 条に基づく「サイバーセキュリティ戦略」の策定に向けて、現下のサイバーセキュリティに関する情勢分析と今後の各府省庁の具体的行動計画が「サイバーセキュリティ 2021」[10]としてまとめられ、わが国の政策の大枠は形成されている。

医療機器のサイバーセキュリティが本格的に議論されるようになったのも、基本法の立法と時期を同じくする。主な契機は、情報セキュリティ政策会議[11]が公表した「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」（2014 年 5 月）[12]である。同計画でも重要インフラ分野として「医療」が設定され、事業者として医療機関（但し、小規模事業者を除く）が指定され、対象となる重要システムの例として、電子カルテシステムと共に医療機器が挙げられ、セキュリティ対策の強化が求められた。

関連して現在まで、厚生労働省と経済産業省・総務省から、それぞれ２つのガイドラインが出されている。厚生労働省は「医療情報システムの安全管理に関するガイドライン」を作成、その後も適宜改定し最新版は ver. 5.1 である[13]。医療

---

[10] （i）目下の情勢、各府省庁の関連施策の実施状況をとりまとめた 2020 年度の年次報告と（ii）次期サイバーセキュリティ戦略に基づく 2021 年度の年次計画、という２つの役割を持つ政府文書である。
https://www.nisc.go.jp/active/kihon/pdf/cs2021.pdf

[11] 情報セキュリティ政策会議とは、2005 年、情報セキュリティ問題の根幹に関する事項を決定するために、内閣官房長官を議長として IT 戦略本部（現・IT 総合戦略本部）の下に設置された会議である。
https://www.nisc.go.jp/conference/seisaku/pdf/050530seisaku-press.pdf

[12] https://www.nisc.go.jp/active/infra/pdf/infra_rt3.pdf

[13] 同ガイドラインは、2005 年 3 月に初版が作成され、その後改定が重ねられ、執筆時点での最新版は 2021 年 3 月に出された 5.1 版である。医療現場が情報セキュリティやサイバーセキュリティに取り組むうえでの最重要文書のひとつである。 https://www.mhlw.go.jp/content/10808000/000730541.pdf

情報を扱うシステムと同システムに関わる人または組織を対象とし、情報セキュリティマネジメントシステム（ISMS）[14]の実践、組織的・物理的・技術的・人的安全対策、サイバー攻撃等の非常時の対応等の指針を示してきた。また、経済産業省・総務省は、2020 年 8 月に「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」を作成、健康医療分野に特化した情報システム・サービス事業者向けの指針を示している。

さらに行政は、下表の行政文書を通じて、製造販売業者に対してサイバーリスクへの対策実施を求めてきている（図表 2-1-1）。

図表 2-1-1. 医療機器のサイバーセキュリティに関わる行政通知

年月日	文書タイトル	目的・趣旨
2015 年 4 月 28 日	「医療機器におけるサイバーセキュリティの確保について」（薬食機参発 0428 第 1 号・薬食安発 0428 第 1 号）	医療機器におけるサイバーセキュリティ確保の必要性の周知。
2018 年 7 月 24 日	「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」（薬生機審発 0724 第 1 号・薬生安発 0724 第 1 号）	製造販売業者が行うべきサイバーセキュリティへの取り組みについて、医療機器への市販前と市販後の対応をより具体的にするための情報提供。
2020 年 5 月 13 日	「国際医療機器規制当局フォーラム（IMDRF）による医療機器サイバーセキュリティの原則及び実践に関するガイダンスの公表について」（薬生機審発 0513 第 1 号、薬生安発 0513 第 1 号）	国際医療機器規制当局フォーラム（IMDRF）による医療機器のサイバーセキュリティに関わるガイダンスの周知。
2121 年 12 月 24 日	「医療機器のサイバーセキュリティの確保及び徹底に係る手引書について」（薬生機審発 1224 第 1 号・薬生安発 1224 第 1 号）	医療機器へ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についての日本への導入のための手引書の周知。

また、国際協調や現実に即した対応の立案が重要との問題意識の下、製造販売業者と医療現場の実態を調査したうえで対策立案を行うために「国立研究開発法人日本医療研究開発機構（AMED）医薬品等規制調和・評価研究事業 医療機関における医療機器のサイバーセキュリティに係る課題抽出等に関する研究」[15]が実施されている。公益法人医療機器センターが研究代表者となり、3 か年計画の研究が進められている。

②規制の現状

医療機器のサイバーセキュリティに関する規制は、開発、製造段階から患者・受診者に使用されて廃棄されるまで、医療機器のライフサイクルとサプライチェーン全体での検討が必須である。かかる問題意識の下、本節では規制の現状を

[14] 「情報セキュリティマネジメントシステム」とは、Information Security Management System の訳語であり、略して ISMS とも呼ぶ。
[15] http://www.jaame.or.jp/mdsi/cs21/index.html

捉えるにあたり、**【市販前】**と**【市販後】**に分けて記載する。

【市販前】の規制は「基本要件基準」に定められている。これは、全ての医療機器が備えるべき品質、有効性及び安全性の適正を図るための基準という位置づけであり、医機法第 41 条第 3 項に基づく[16]。この基本要件基準をチェックリストとして表形式にまとめ、その適合性を説明した文書が「医療機器に係る基本要件適合性チェックリスト」として発出されている[17]。基本要件基準は、全 2 章・全 18 の条文で構成されている。サイバーセキュリティ対策については、「第 1 章 一般的要求事項の第 2 条 リスクマネジメント」と「第 2 章 設計及び製造要求事項の第 12 条 プログラムを用いた医療機器に対する配慮」に規定されている。この基本要件基準をベースに、製造販売業者に対するサイバーセキュリティに関する要求事項が、図表 2-1-1 に示した行政通知にまとめられている。

【市販後】においては、医機法に定める「安全管理情報の収集と情報提供」と「安全確保業務」の 2 つがポイントである。医機法第 68 条の 2 の 5 の第 1 項では、製造販売業者に対して、医療機器の適正使用のために必要な情報の収集と医療現場への情報提供の努力義務を定めている。医機法第 68 条の 2 の 5 の第 2 項と第 3 項では、医療現場の情報収集への協力と提供された情報の利活用の努力義務を定めている。また、医機第 68 条の 9 は、医療機器等の使用によって保健衛生上の危害が発生、又は拡大するおそれがあると判断された場合、これを防止するために、医療機器の廃棄、回収、販売の停止、情報の提供等の必要な安全確保措置を講じなければならないとしている。

③今後の規制の方向性

近年では、新たな医療技術の開発がグローバルに行われたり、同一の医療機器が複数国に渡って流通したり、医療機器企業を構成する資本が複数国に跨ったりすることは、決して珍しい事象ではない。また、ネット接続された医療機器に対しては、国境を超えたサイバー攻撃が行われる恐れがある。かかる現況を踏まえると、各国の医療機器のサイバーセキュリティに関わる基本的な規制及び対処方針（すなわち、ガイドラインやガイダンスと呼ばれる文書）については、可能な限り国際的な整合性をとり、一般原則の合意やベストプラクティスの共有がなされる未来が望ましい。たとえば、国際医療機器規制当局フォーラム（IMDRF）のガイダンスでは、製造販売業者のみならず、あらゆる関係者間に

---

[16] 詳細は、「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四十一条第三項の規定により厚生労働大臣が定める医療機器の基準（平成 17 年 3 月 29 日付　厚生労働省告示第 122 号）」（基本要件基準）に規定されている。

[17]「医療機器に係る基本要件適合性チェックリストについて」（令和 3 年 8 月 18 日付け厚生労働省通知 薬生機審発 0818 第 1 号）

おける遅滞のない、積極的な情報共有の重要性が言及されており、そのための具体的かつ明確な行動指針が示されている。現在、2023 年を目途に IMDRF ガイダンスを本格導入して運用できるよう、行政と業界団体が主体となって検討を行っている。

（２）関連主要団体の取り組みと報告・相談窓口

①日本医療機器産業連合会の取り組み

一般社団法人日本医療機器産業連合会（医機連）は、医療機器等の開発、生産、流通に携わる医療機器関係団体（21 団体）からなる連合会である。医療機器産業界の代表として、業界の発展と国民の健康福祉の増進に寄与すべく活動している業界団体である。

医機連は、未来投資戦略が提唱する「健康寿命の延伸」や「次世代ヘルスケア・システムの構築」を支える医療機器産業を目指すために、「医機連産業ビジョン 2018　―Society5.0 を支える医療機器産業をめざして―」を提示、重点テーマとして、「データ利活用とサイバーセキュリティ強化の推進」を取りあげ、医療機器および利用環境に対する規制の検討や ISAC などの業界横断的な取り組みの検討を進めている。また、2019 年 5 月の第 16 回健康・医療戦略参与会合では、医機連会長が「データヘルスの進展によるサイバーセキュリティ対応の重要性」を示し、関連情報の開示及び対応策を含めた情報共有の仕組み構築、医療機関によるサイバーセキュリティ対応の推進と医療機器における柔軟なセキュリティ対策の推進を提言した。さらに 2019 年 8 月の医機連みらい戦略会議では、サイバーセキュリティタスクフォースを立ち上げ、サイバーセキュリティに関する業界全体の意識向上、企業、医療機関の実態把握、情報共有の体制検討、政策提言による業界の活性化などを目標に活動を行っている。

医療機器のサイバーセキュリティ対策については、IMDRF のガイダンスを 2023 年目途に本格導入する計画で進められている中で、医機連は、製造販売業者向けの手引書を 2021 年度中に発出するべく準備中である。さらに、製造販売業者と医療機関の連携を円滑にすることを目指し、医療機関向けの手引書を作成中である。

②情報処理推進機構の取り組み

独立行政法人情報処理推進機構（Information-technology Promotion Agency, Japan; IPA）は 2004 年に経済産業省所管として発足した政策実施機関である。情報セキュリティ対策の実現、IT 人材の育成、IT 社会の動向調査・分析・基盤

構築を軸として、安全で利便性の高い“頼れる IT 社会”の実現を目指して活動している機関である。本機関では、情報セキュリティに関する情報が日々発信されている。また、2014 年 4 月には医療機器における情報セキュリティに関する調査を実施しており、セキュリティ上の課題や諸外国の医療機器のセキュリティに関する取り組みの取りまとめなども行っている。

③JPCERT コーディネーションセンターの取り組み

JPCERT（ジェーピーサート）コーディネーションセンター（Japan Computer Emergency Response Team Coordination Center ; JPCERT/CC）は、国内外の他の CSIRT（Computer Security Incident Response Team）[18]との連携を図りながら日本の窓口としての役割を担うため、1996 年に特定の政府機関や企業からは独立して設立された中立組織の団体である。

インターネットを介して発生する侵入やサービス妨害等のコンピュータセキュリティ・インシデント（以下、インシデント）について、日本国内に関するインシデント等の報告の受け付け、対応の支援、発生状況の把握、手口の分析、再発防止のための対策の検討や助言などを、技術的な立場から行なっている。ウェブページ上では注意喚起、脆弱性関連情報やサイバーインシデントに関する情報の発信が行われている。

④保健医療福祉情報システム工業会の取り組み

保健医療福祉情報システム工業会（Japanese Association of Healthcare Information Systems Industry ; JAHIS(ジェイヒス)）は、1994 年に保健医療福祉情報システムに関する標準化の推進、技術の向上、品質及び安全性の確保を図ることにより、保健医療福祉情報システム産業の健全な発展と健康で豊かな国民生活の維持向上に貢献することを目的に設立された業界団体である。

標準化推進部会、医事コンピュータ部会、医療システム部会、保険福祉システム部会といった部会を設置している。例えば、医療システム部会では、電子カルテをはじめとした医療機関で運用される医療情報システムの標準化やモデル化を中心とした活動を行い、それら各システム共通のセキュリティ、相互運用性についても取り扱っている。

[18] CSIRT とは「Computer Security Incident Response Team」の略語で、「コンピュータに関するセキュリティ事故の対応チーム」のことである。

（３）海外の取り組み

①米国の取り組み

医療機器のサイバーセキュリティに関連して、米国での取り組みとしては、「医療保険の相互運用性と説明責任に関する法律」（HIPPA）と「経済的および臨床的健全性のための医療情報技術に関する法律」（HITECH）という２つの法律、そして米国食品医薬品局（FDA）が作成したガイダンスやセキュリティ評価ツール等の取り組みが重要である。

米国の医療保険の相互運用性と説明責任に関する法律（Health Insurance Portability and Accountability Act）は 1996 年に制定、HIPPA と略称される。同法により、保護対象となる医療保険の情報が明示され[19]、その使用や開示、保存、送信にあたってのセキュリティ確保がルール化された。経済的および臨床的健全性のための医療情報技術に関する法律（Health Information Technology for Economic and Clinical Health Act）は、2009 年に制定、HITECH と略称される。同法によって、HIPPA への違反に対する罰則が強化された。

また、米国食品医薬品局（FDA）は、医療機器のサイバーセキュリティに関する市販前ガイダンスを 2014 年 10 月に、市販後ガイダンスを 2016 年 12 月に公表している。これらのガイダンスは、企業に対して、米国標準技術研究所（NIST）の枠組みの利用を推奨し、サプライチェーン全体を通したリスク管理を強調している。さらに 2020 年 10 月、FDA は、医療機器の開発や評価に使用可能な公式ツール Medical Device Development Tool（MDDT）にサイバーセキュリティの評価ツールを追加した。このツールの活用によって、医療機器のサイバーセキュリティにおける脆弱性を同一の基準で定量的に評価でき、ステークホルダー間の共通認識が拡がることが期待されている。

2003 年以来、毎年 10 月が国を挙げてサイバーセキュリティを意識する月間（National Cybersecurity Awareness Month）として位置づけられている。たとえば 2020 年には、”Do Your Part. #BeCyberSmart” というテーマが設定され、自宅や職場で用いる医療機器、インターネット接続が可能な医療機器のサイバーリスクの啓発が着目されている。

---

[19] 同法において、保護対象となる保険情報のことを Protected Health Information（PHI）という。

さらに、米国 FDA では、医療提供組織（health delivery organizations；HDO）が医療機器に関するサイバーセキュリティインシデントへの備えを強化し、製造販売業者等も取り組むべき準備活動の種類を説明したプレイブック「PLAYBOOK FOR THREAT MODELING MEDICAL DEVICES(2018 年 10 月)」、行政やそのパートナー、業界の関係者がサイバーセキュリティの脆弱性について患者や一般市民に情報を提供するために重要な点をまとめた「Best Practices for Communicating Cybersecurity Vulnerabilities to Patients(2021 年 10 月)」といったホワイトペーパーを作成している。医療機器のサイバーセキュリティ対策に関しては、サイバーセキュリティの脅威のモデリング方法を学ぶ教材として「Playbook for Threat Modeling Medical Devices(2021 年 11 月)」が作成されている。

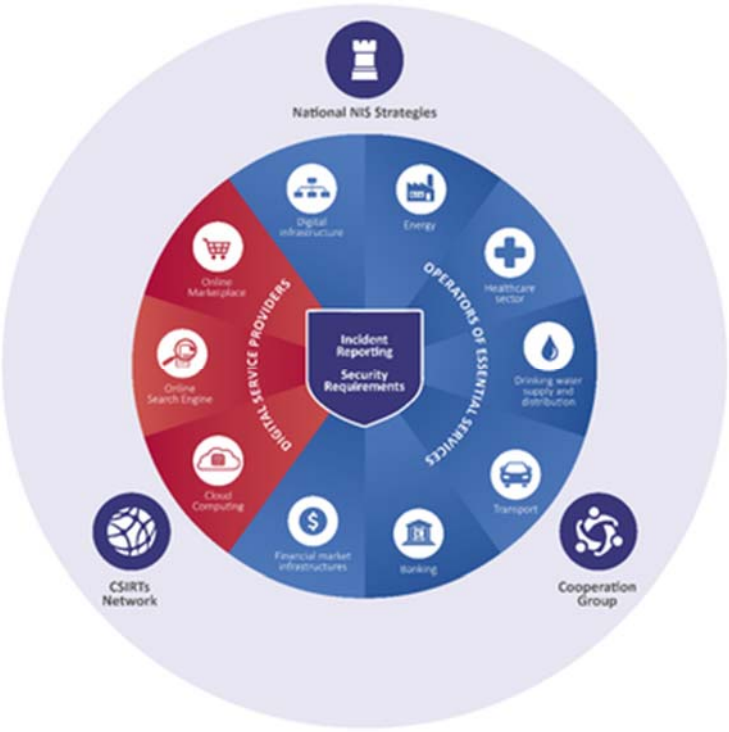
②欧州の取り組み

医療機器のサイバーセキュリティに関連して、欧州連合（EU）での取り組みとしては、「一般データ保護規則」（GDPR）と「医療機器規則」（MDR）という２つの規則、そして「ネットワークおよび情報システム指令」（NIS 指令）が重要である。

一般データ保護規則（General Data Protection Regulation）は、EU における個人情報保護のための規則であり、2016 年に制定、GDPR と略称される。医療機器規則（Medical Device Regulation）は、EU における医療機器に関する各種規制を定めた規則であり、2017 年に制定、MDR と略称される。GDPR は個人情報保護に関する罰則や違反について規定しており、MDR は医療機器の CE マーキング[20]に大きく影響する規則である。MDR は、特にソフトウェア機器について、セキュリティの確保や保護を実装するための要件を規定しており、ソフトウェアの使用環境によるリスクが強調されている。

ネットワークおよび情報システム指令（Directive on Security of Network and Information Systems）とは、2016 年に採択された EU におけるサイバーセキュリティ確保のための法令であり、NIS 指令（NIS Directive）と略称される。NIS 指令は、EU 加盟国内のネットワークおよび情報システムの安全性の強化を図るとともに、医療を含む重要なサービス事業者に対して、サイバーセキュリティやインシデントの情報提供をするように定めている（次頁図）。

[20] CE マーキングとは、EU で販売される指定の製品が EU の基準に適合していることを表示するマークのことである。



資料：EU 公式ウェブサイト

③海外文献における議論の動向

本章の最後に、海外文献の調査を基に、医学系論文における医療機器のサイバーセキュリティに関する議論の動向を述べる。

2016 年以降、年平均 8 報ほどの報告がなされている。中でも、2020 年以降の文献に注目すると、個別の医療機器に関するサイバーリスクとその対策に関する文献や現場の対応を重要視する文献が中心であった。

個別の医療機器に関するサイバーリスクとしては、糖尿病治療に使用するインスリンポンプや血糖測定器、パルスオキシメータ、温度計、体温計、心電図等の Bluetooth 技術を採用した医療機器や脊髄刺激装置等の無線技術を採用した医療機器のリスクが取り上げられていた。実際の被害報告はないとされていたが、外部との通信機能によるインスリンの誤投与や患者情報の悪用による治療効果の喪失、電池消耗の促進、知覚、筋力低下や機能障害、組織の熱傷、電気ショック等、有害事象を引き起こす危険性が指摘されていた。リスク回避のためには、各機器が取り扱うデータが有する資産価値を分析・評価して医療機器を含むシステム全体に対するサイバーセキュリティ対策を施すこと、各通信手段が有する認証や暗号化の機能を適切に使用しながら最新の仕様へとアップ

デートすること、そして、各医療機器のサイバーリスクを継続的に監視することが示されていた。

現場対応の重要性を説く文献としては、医療現場のスタッフが実行すべき要点を整理した文献や ISO 規格を導入して医療機器のリスク管理を実施した際に得られた課題や教訓に関し臨床工学の観点から整理した文献の報告があった。前者では、医療機器やシステムのサイバーセキュリティ対策では、それらを購入し、使用し、メンテし、サポートし、最終的には廃棄するまで、包括的な検討が必要としている。後者では、医療機関における医療機器のシステム管理に関するポリシーの欠如を課題として挙げている。ISO 規格の導入経験を通じて、役割と責任が明確なガバナンス構造の構築と医療機器の管理に対応したリスクマネジメント・ポリシーの整備が重要と指摘している。

これらの文献での議論を整理すると、医療機器のサイバーセキュリティ対策を実施していくためには、下記の４点に留意する必要があると言える。

1. **継続的なリスク監視とプログラムのアップデート**
   個別の医療機器のサイバーセキュリティの確保のためには、継続的なリスク監視とプログラム等のアップデートが重要

2. **相談窓口、情報の流通、レガシー機器[21]への対応**
   医療機関におけるサイバーセキュリティ対策のためには、医療機器のサイバーセキュリティに関する相談窓口、関連する情報の入手や提供体制、そしてレガシー医療機器への対応が重要

3. **医療機関内の組織体制**
   施設内に役割と責任を明確にした適切なガバナンス構造を構築することが重要

4. **リスクマネジメントに関わるポリシーと管理方法の文書化**
   施設の IT ネットワークと統合する医療機器の管理に対応したリスクマネジメント・ポリシー、医療機器に特化したサイバーセキュリティに関する管理方法を文書にて整備することが重要

[21]レガシー医療機器（レガシーメディカルデバイス）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を指す用語である。たとえば、システムの脆弱性を排除または十分に低減する方法として、プログラムの更新またはパッチを当てることができなくなった機器のこと。
https://www.mhlw.go.jp/hourei/doc/tsuchi/T200521I0040.pdf

３．実態調査からみる現場の実情

本章では、（１）医療機器の製造販売業者を対象とした調査と（２）医療機器のユーザーである病院・診療所を対象とした調査の２つの実態調査の結果を基に、現場の状況を確認する。

（１）製造販売業者向け調査結果

①調査の基本情報

まず、医療機器の製造販売業者向け調査の基本情報を示しておく。

同調査では、2019 年 12 月～2020 年 1 月にかけて、日本全国の医療機器の製造販売業者 2,722 社を対象に実施、757 件の回答を得た（回収率 27.8%）。実施主体は、公益財団法人医療機器センター附属医療機器産業研究所である。実施にあたっては、国立研究開発法人日本医療研究開発機構(AMED)の研究資金を活用し、ウェブ・アンケートを行った。

同調査における主要な調査項目は、以下の通りである。

① サイバーセキュリティに関わる対応状況
② サイバーセキュリティに関わる情報の入手状況
③ 自社製品（医療機器）の市販後対応状況
④ サイバーセキュリティに関連する意見や要望

回収できた 757 件のうち、サイバーセキュリティ対策が必要な製品を有する企業の数は 259 件であった（回収数の 34.2%）。したがって、本章で分析対象としたのは、それらの 259 社である。

図表 3-1-1～図表 3-1-3 に、今回分析対象とした 259 社の企業の基本的な属性情報（資本金、資本区分、専業・兼業、社員数、各種プログラムを用いた医療機器の製造販売状況、自社製品に占めるサイバーセキュリティ対応が必要な医療機器の割合）を示している。

図表 3-1-1. 基本情報①（n=259）

資本金	200億円超	7.7%
	50億円超～200億円以下	7.3%
	3億円超～50億円以下	18.5%
	1億円超～3億円以下	6.6%
	5000万円超～1億円以下	22.0%
	5000万円以下	37.8%
資本上の区分	内資系企業	78.8%
	外資系企業	21.2%
専業・兼業	専業	54.8%
	兼業	49.2%
社員数	1000人超	18.9%
	500人超～1000人以下	7.3%
	100人超～500人以下	23.6%
	50人超～100人以下	15.1%
	50人以下	35.1%

図表 3-1-2. 基本情報②（n=259）

組み込みプログラムを用いた医療機器を製造販売している	はい	76.4%
	いいえ	23.6%
コンピュータを用いた医療機器を製造販売している	はい	49.0%
	いいえ	51.0%
医療機器プログラムを製造販売している	はい	35.5%
	いいえ	64.5%

図表 3-1-3. 基本情報③（n=259）

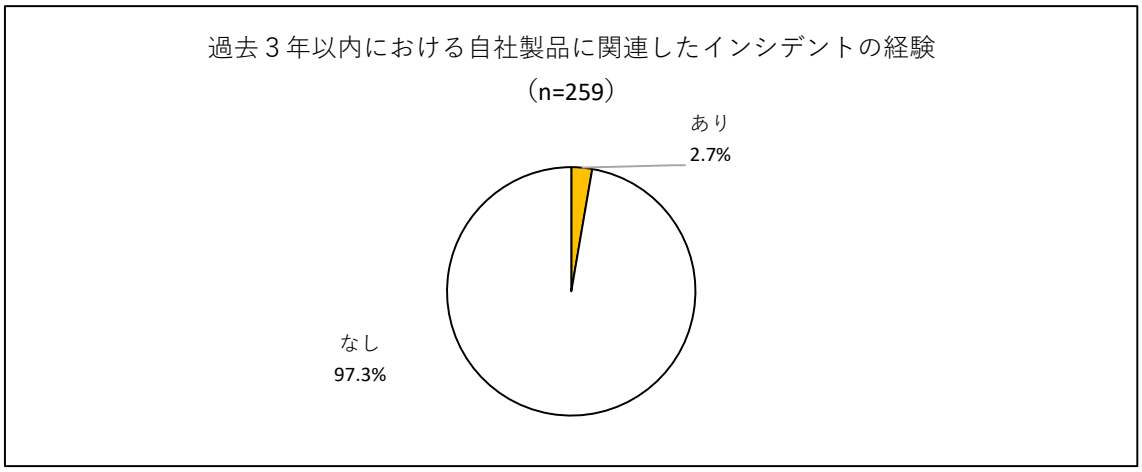
自社の全製品に占めるサイバーセキュリティ対応の検討を要する医療機器の割合	80%以上	27.0%
	60%以上～80%未満	6.6%
	40%以上～60%未満	8.5%
	20%以上～40%未満	5.4%
	20%未満	52.5%

②調査結果

実際のインシデント経験

図表 3-1-4 は、過去３年以内における自社製品に関連したサイバーセキュリティに関わるインシデントの経験について示している。インシデントを経験した割合は、2.7%であった。

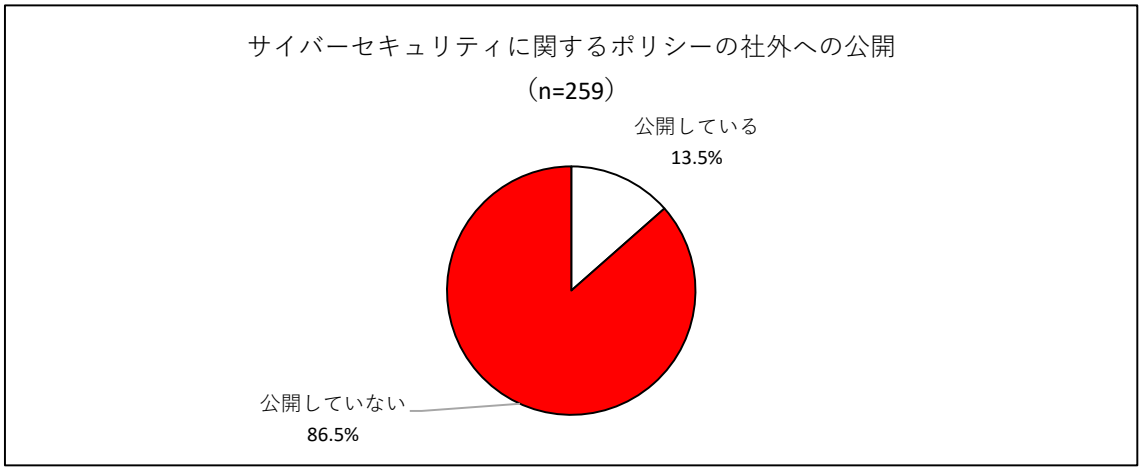
図表 3-1-4.



サイバーセキュリティ・ポリシーの社外への公開

図表 3-1-5 は、サイバーセキュリティに関するポリシーの社外への公開状況を示している。86.5%は、ポリシーを社外へ公開していなかった。

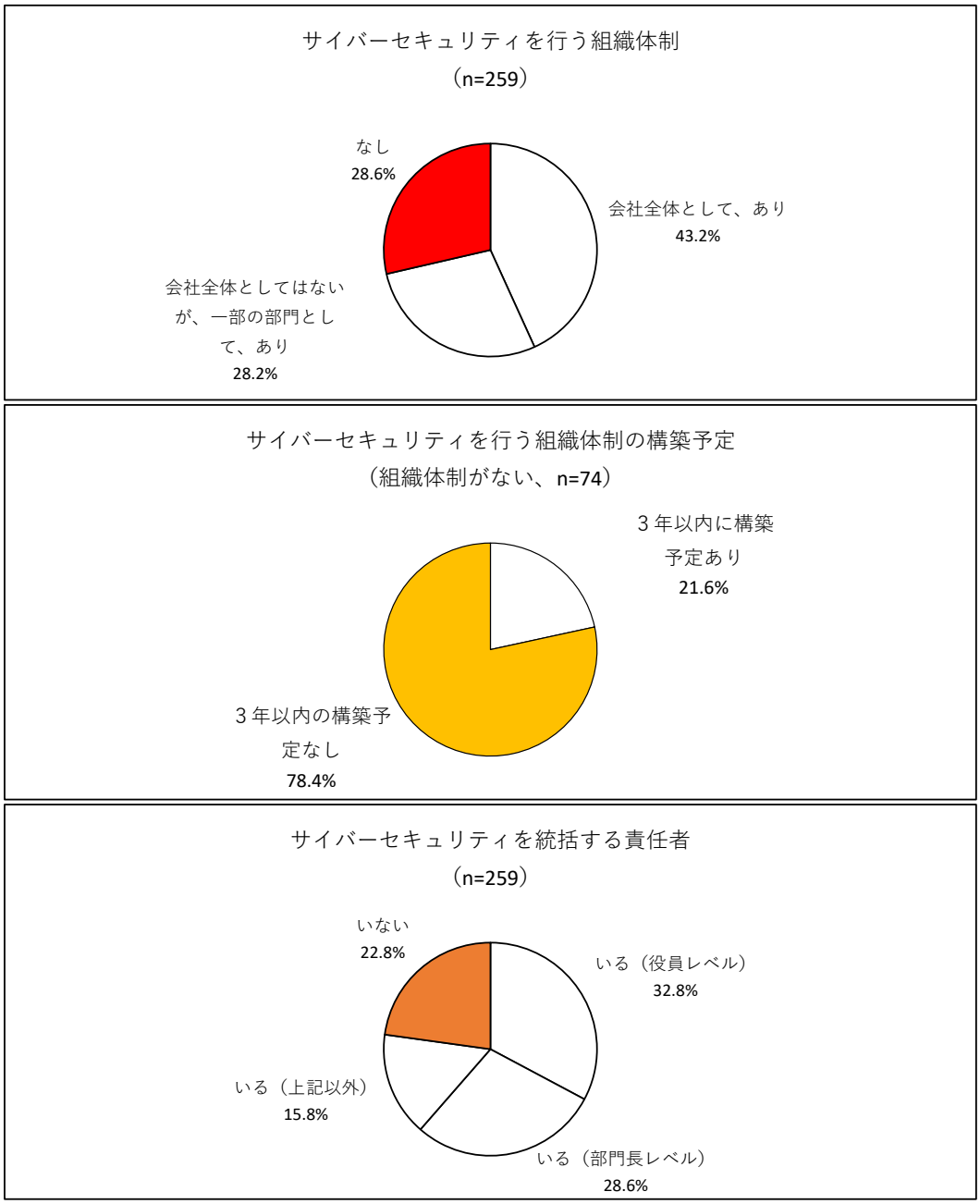
図表 3-1-5.



サイバーセキュリティ対応を行う組織体制と責任者

図表 3-1-6 は、サイバーセキュリティを行う組織体制、体制構築の予定、責任者の状況を示している。組織体制がない割合は 28.6%であり、そのうち 78.6%は 3 年以内に構築する予定もなかった。サイバーセキュリティに関わる責任者がいない割合は 22.8%であった。

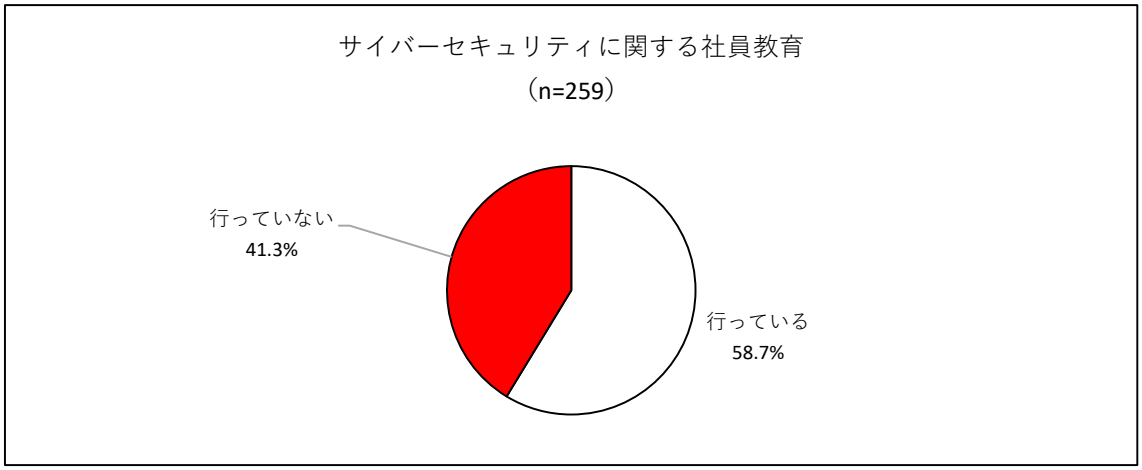
図表 3-1-6.



サイバーセキュリティに関する社員教育

図表 3-1-7 は、サイバーセキュリティに関する社員教育の実施状況を示している。41.3%は、サイバーセキュリティに関する社員教育を行っていなかった。

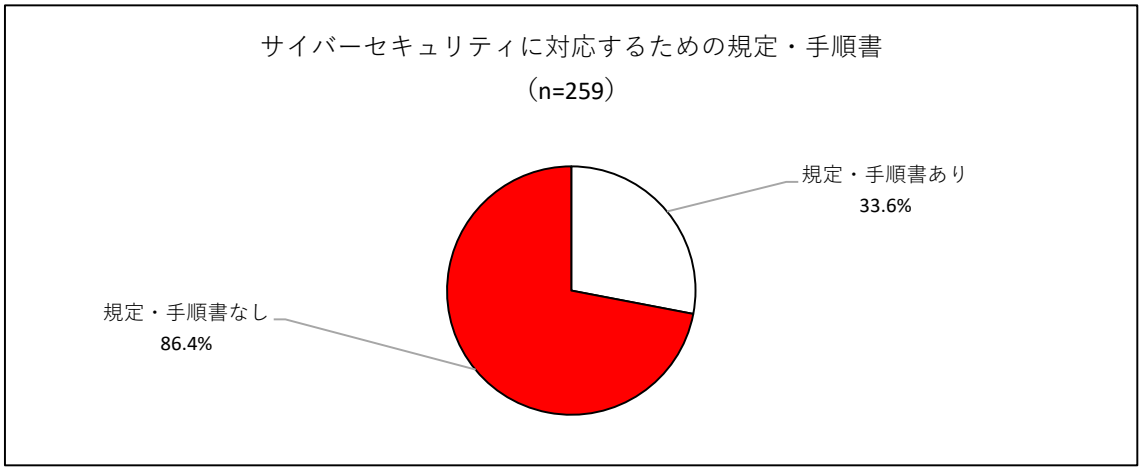
図表 3-1-7.



サイバーセキュリティに対応するための規定・手順書

図表 3-1-8 は、サイバーセキュリティに対応するための規定・手順書の整備状況について示している。86.4%は、規定・手順書が整備されていなかった。

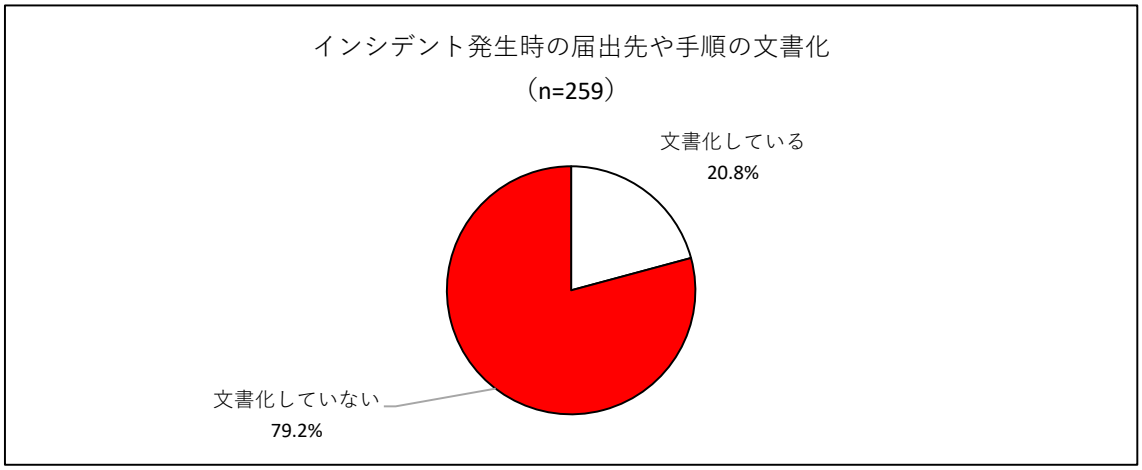
図表 3-1-8.



インシデント発生時の届け出先や手順の文書化

図表 3-1-9 は、サイバーセキュリティに関するインシデント発生時の届出先や手順の文書化の状況を示している。79.2%は、文書化していなかった。

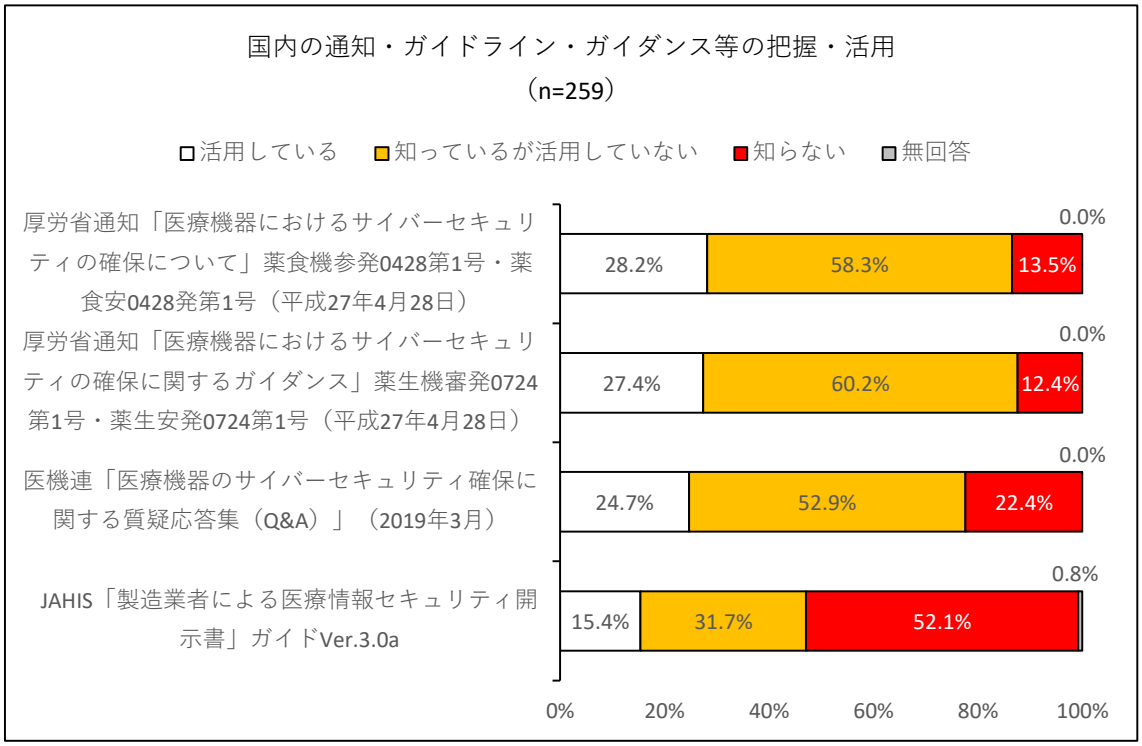
図表 3-1-9.



国内の通知、ガイドライン、ガイダンス等の把握・活用

図表 3-1-10 は、国内の行政通知やガイドライン、ガイダンスの把握・活用の状況を示している。図表中に示した３つの文書を活用している割合はいずれも３割に満たなかった。それらの文書を「知らない」との割合は１割強～2 割強であったが、「知っているが活用していない」との割合が 5 割強～6 割強だった。

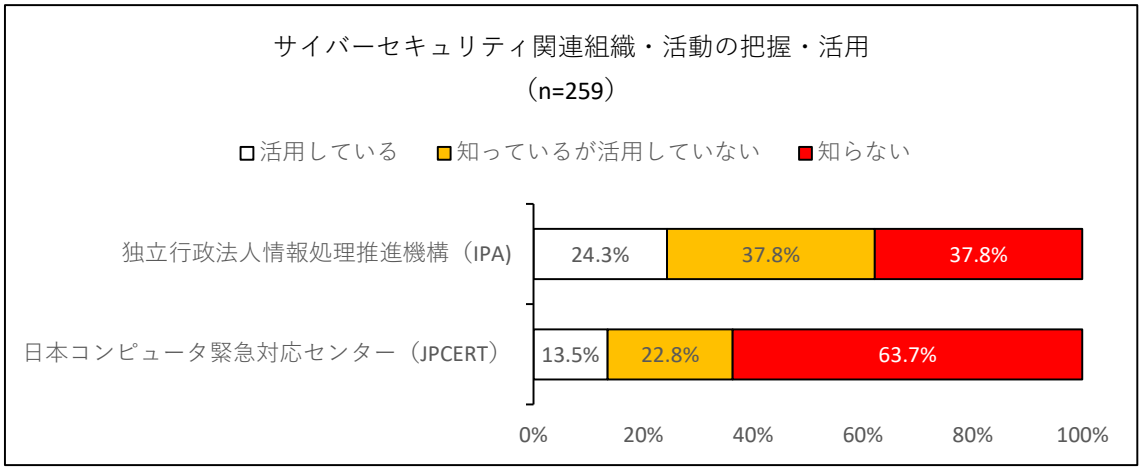
図表 3-1-10.



サイバーセキュリティ関連組織・活動の把握・活用

図表 3-1-11 は、サイバーセキュリティ関連組織・活動の把握・活用の状況を示している。情報処理推進機構（IPA）を活用しているとの割合は 24.3%、日本コンピュータ緊急対応センターを活用しているとの割合は 13.5%であった。

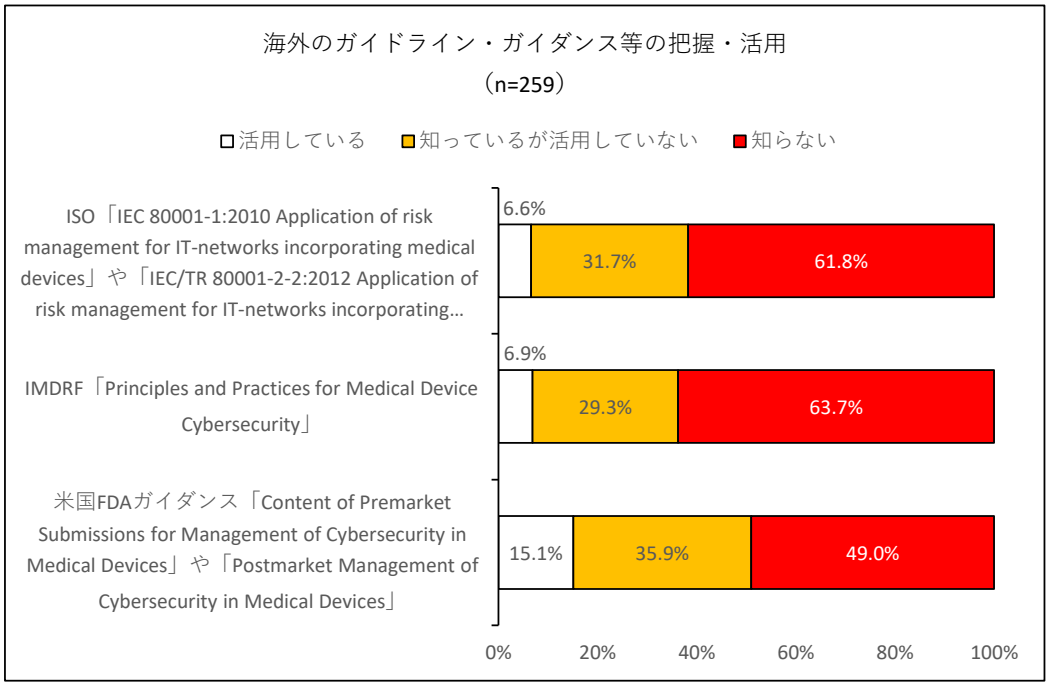
図表 3-1-11.



海外のガイダンス、ガイドライン等の把握・活用

図表 3-1-12 は、海外のガイドラインやガイダンス等の把握・活用の状況を示している。図表中に示した３つのガイドラインを活用しているとの割合は、ISO の文書で 6.6%、IMDRF の文書で 6.9%、米国 FDA の文書で 15.1%と、いずれも少数派であった。

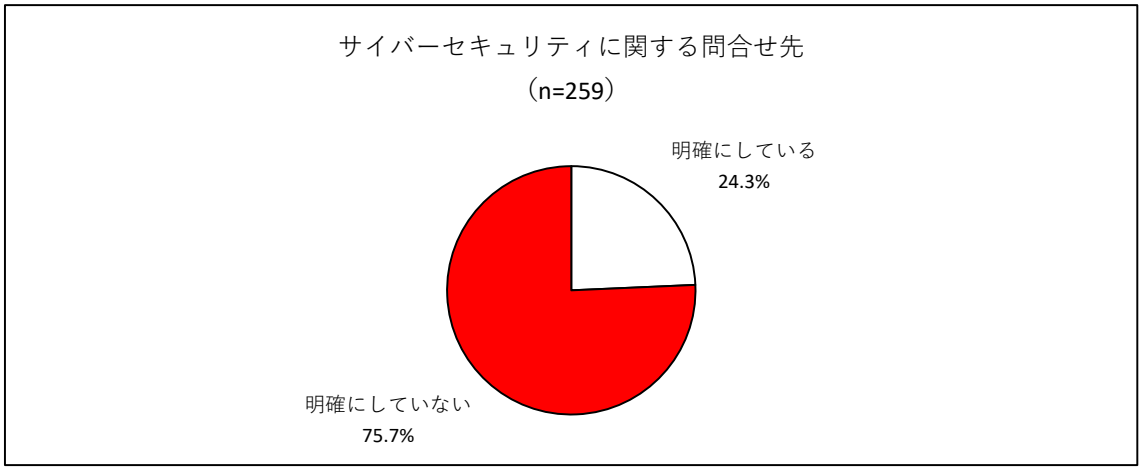
図表 3-1-12.

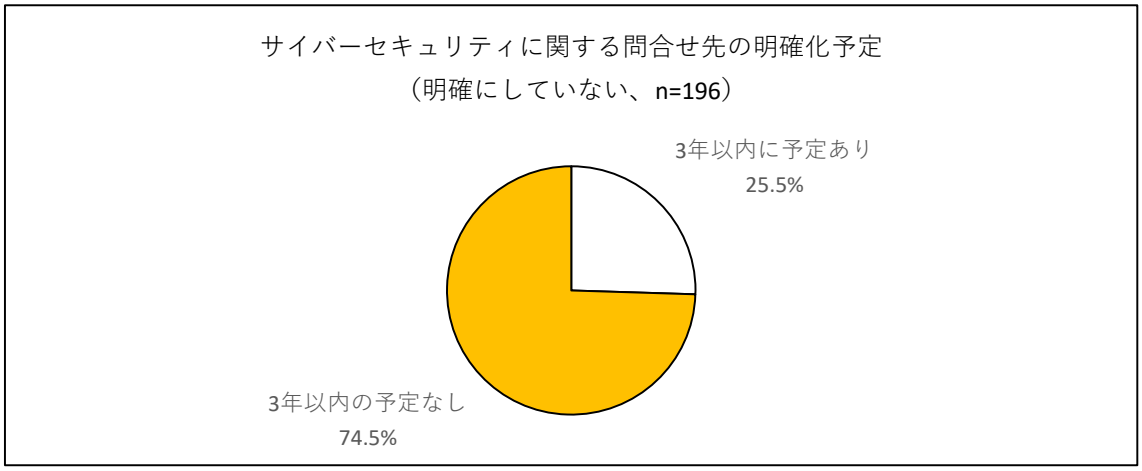


サイバーセキュリティに関する問合せ先

図表 3-1-13 は、サイバーセキュリティに関する問合せ先についての状況を示している。問合せ先を明確にしていないとの割合は 75.7%であり、明確にしていない企業のうち 3 年以内に明確にする予定がない割合は 74.5%であった。

図表 3-1-13.

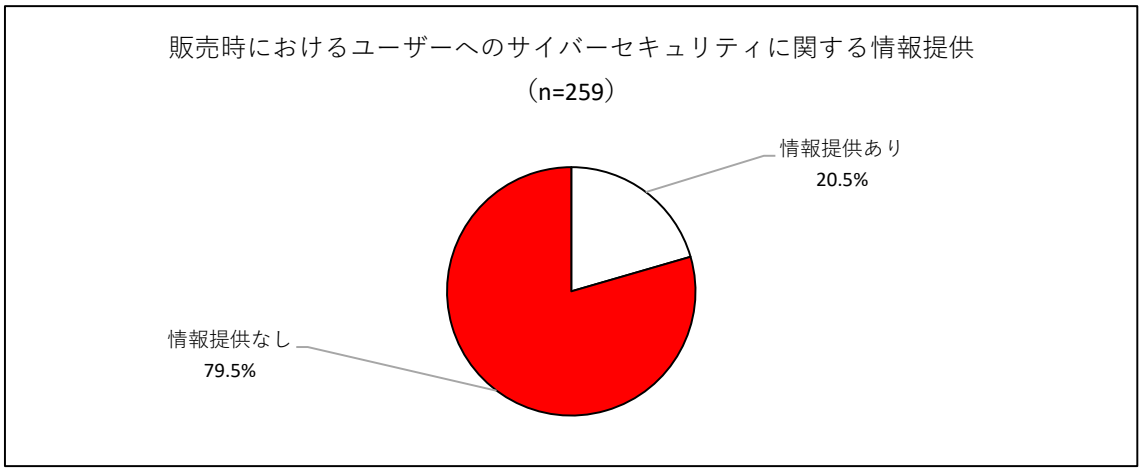


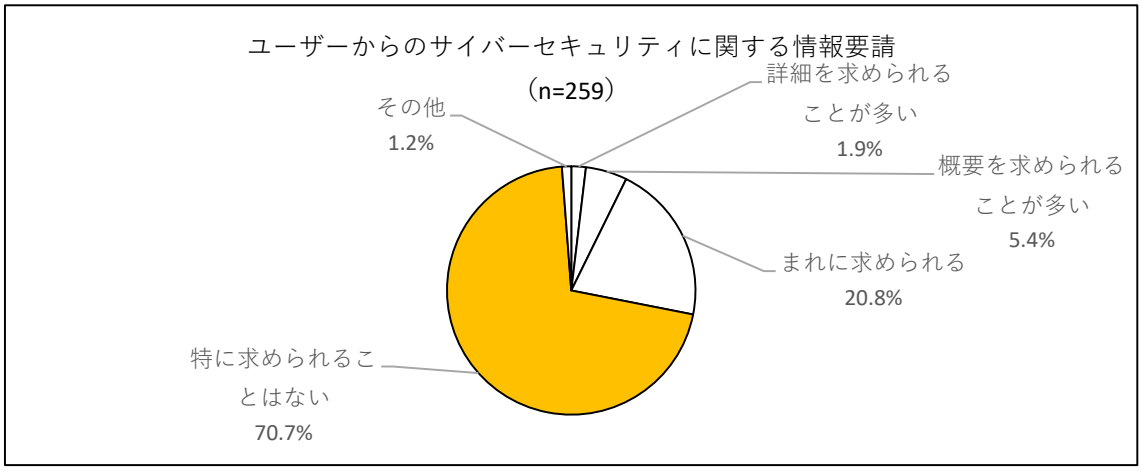


販売時におけるユーザーへの情報提供

図表 3-1-14 は、販売時におけるユーザーへのサイバーセキュリティに関する情報提供の状況とユーザーからの情報要請の状況について示している。8 割近く（79.5%）が情報提供をしていなかった。一方で、7 割強（70.7%）がユーザーから特に情報提供を求められることはないとの回答であった。

図表 3-1-14.

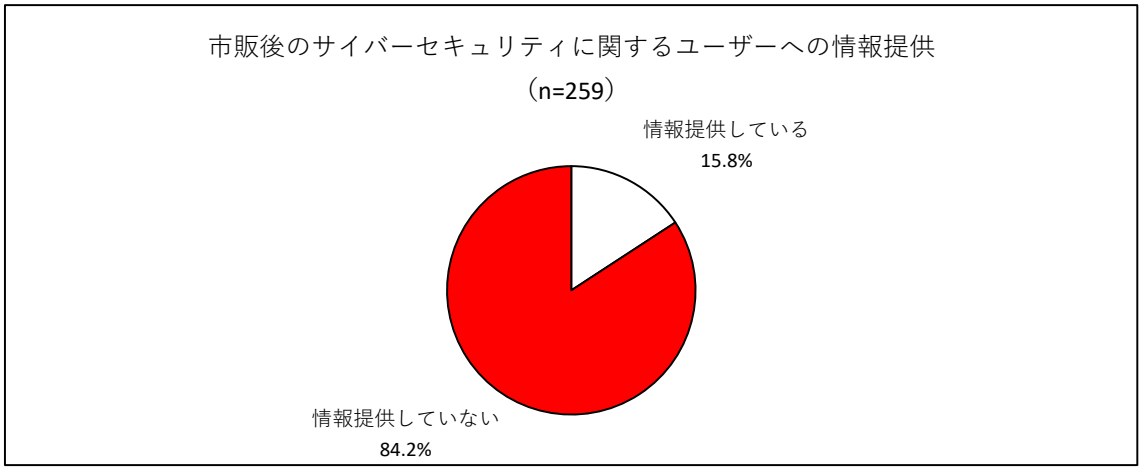




市販後のユーザーへの情報提供

図表 3-1-15 は、自社製品市販後のサイバーセキュリティに関するユーザーへの情報提供の状況について示している。情報提供していないとの割合は 84.2%であった。

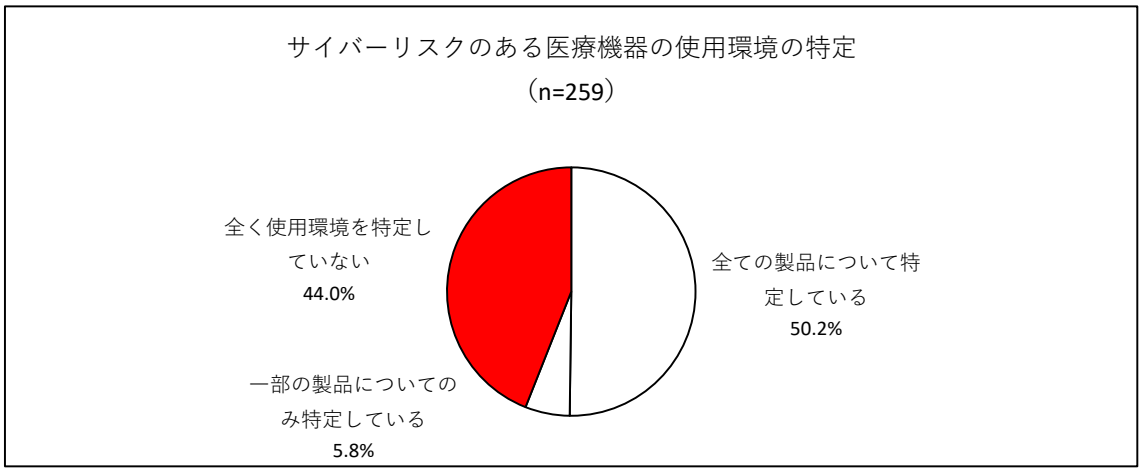
図表 3-1-15.



サイバーリスクのある医療機器の使用環境の特定

図表 3-1-16 は、サイバーリスクのある医療機器の使用環境の特定状況について示している。全く使用環境を特定していないとの割合は 44.0%であった。

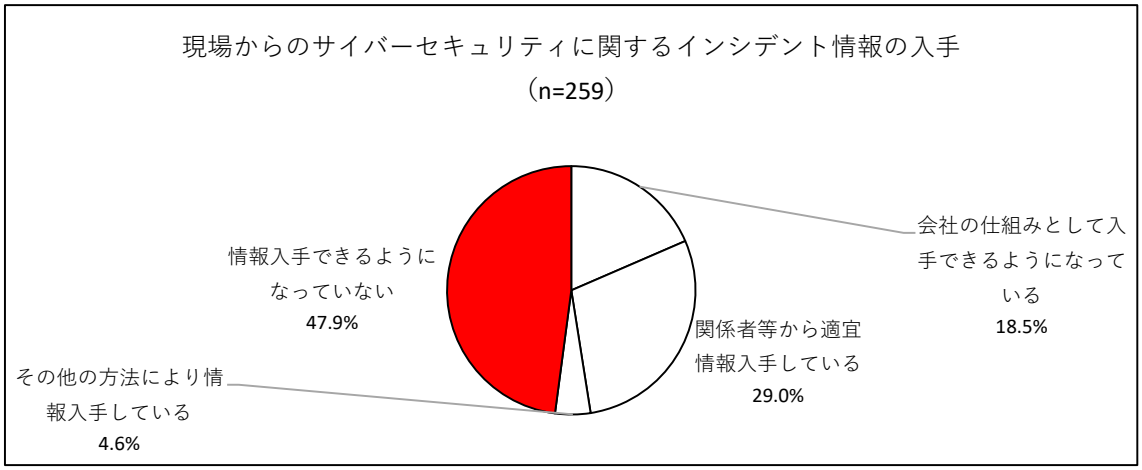
図表 3-1-16.



現場からのインシデント情報の入手

図表 3-1-17 は、現場からのサイバーセキュリティに関するインシデント情報の入手状況を示している。インシデント情報を入手できるようになっていないとの割合は 47.9%であった。

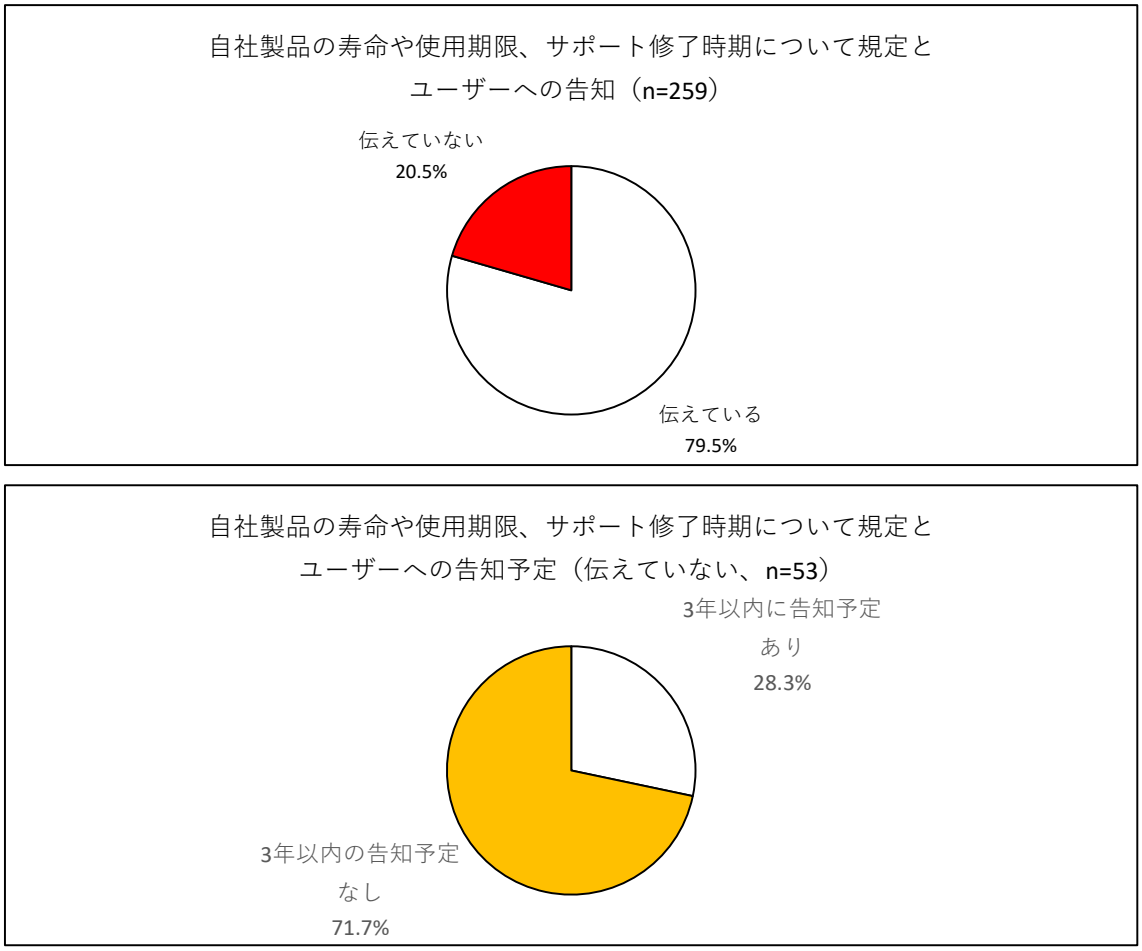
図表 3-1-17.



製品の寿命や使用期限、サポート終了時期の規定とユーザーへの告知

図表 3-1-18 は、自社製品の寿命や使用期限、サポート終了時期の規定とユーザーへの告知の状況を示している。ユーザーに伝えていない割合は 20.5%であり、伝えていない企業のうち3年以内に告知予定がない割合は71.7%であった。

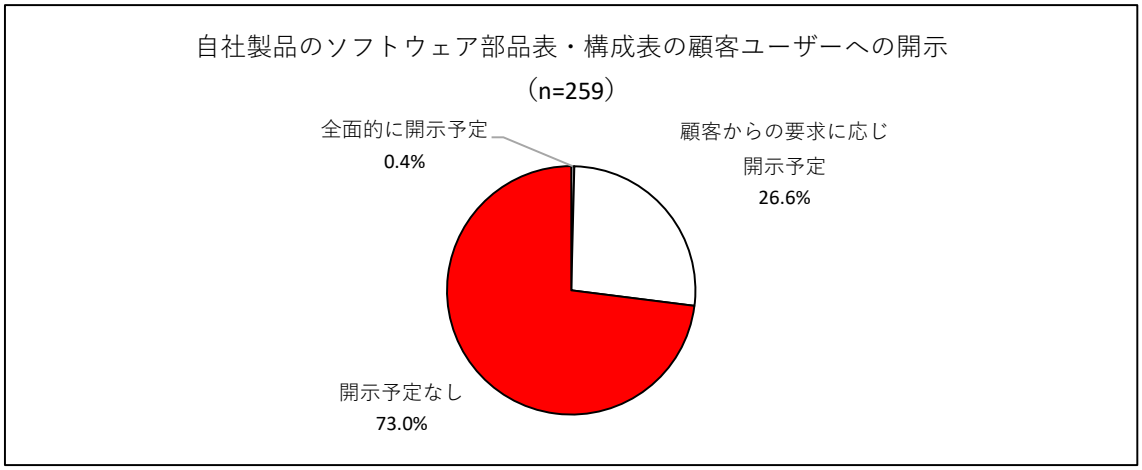
図表 3-1-18.



製品のソフトウェア部品表・構成表の顧客への開示

図表 3-1-19 は、自社製品のソフトウェア部品表・構成表の顧客への開示状況を示している。開示予定なしとの割合は 73.0%であった。

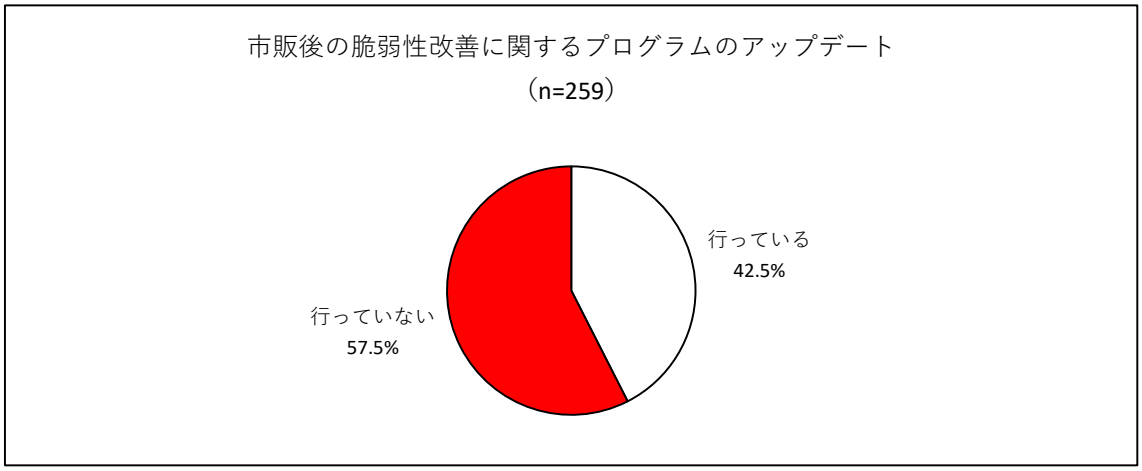
図表 3-1-19.



市販後の脆弱性改善プログラムのアップデート

図表 3-1-20 は、自社製品市販後の脆弱性改善に関するプログラムのアップデートの状況について示している。アップデートを行っていないとの割合は 57.5%であった。

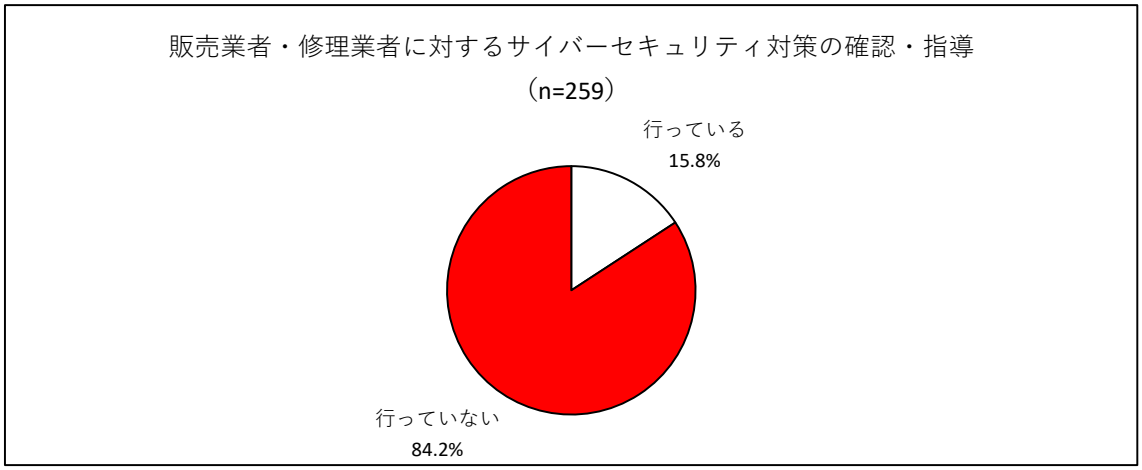
図表 3-1-20.



販売業者・修理業者に対する対策の確認・指導

図表 3-1-21 は、自社製品の販売業者（卸業者）や修理業者に対するサイバーセキュリティ対策の確認・指導の状況について示している。対策の確認・指導を行っていないとの割合は 84.2%であった。

図表 3-1-21.



（２）病院・診療所向け調査結果

①調査の基本情報

ここでは、全国の病院・診療所を対象とした実態調査についての基本情報を記しておく。

同調査は 2021 年 1 月～2 月にかけて、日本全国の病院 5,000 施設、診療所 5,000 施設の合計 10,000 施設を対象に実施し、2,989 件の回答を得た（回収率 30.4%、未達 175 件)。実施主体は公益社団法人日本医師会と公益財団法人医療機器センターの 2 団体であり、実施にあたっては、国立研究開発法人日本医療研究開発機構(AMED)の研究資金を活用し、ウェブ・アンケートを行った。

主要な調査項目は、(1) 情報セキュリティ・サイバーセキュリティに関する組織体制、(2) 行政の取り組みの認知度、(3) インシデントへの対応と実際の経験、(4) 医療機器のサイバーセキュリティに関する医療現場の認識の 4 点である。これら主要な調査項目のうち、(1) ～ (3) については、堤・坂口（2021）[22]および坂口・堤（2021）[23]にて詳細な分析と考察を行ったため本稿では分析の対象外とし、本節では医療機器のサイバーセキュリティに関する医療機器のユーザーであるの認識についての分析結果を示すこととした。下記の図表 3-2 に、同調査の回答者属性を示す。

図表 3-2. 回答者属性

		n	%
開設主体	個人	616	20.6%
	医療法人	1661	55.6%
	国公立・公的	443	14.8%
	その他の法人	269	9.0%
病床規模	無床診療所	1289	43.1%
	有床診療所	111	3.7%
	病院　20～99床	468	15.7%
	病院　100～199床	511	17.1%
	病院　200～499床	463	15.5%
	病院　500床以上	147	4.9%

		n	%
院長の年齢	３０歳代以下	25	0.8%
	４０歳代	285	9.5%
	５０歳代	790	26.4%
	６０歳代	1355	45.3%
	７０歳代	457	15.3%
	８０歳代以上	77	2.6%
回答者職位	理事長	297	9.9%
	院長	709	23.7%
	システム担当	986	33.0%
	事務長	515	17.2%
	その他	482	16.1%

[22] 堤信之、坂口一樹（2021）「オンライン資格確認導入に係るサイバーリスクの実態に関する調査結果の分析と考察」日医総研リサーチエッセイ No.103.
[23] 坂口一樹、堤信之（2021）「病院・診療所のサイバーセキュリティ：医療機関の情報システムの管理体制に関する実態調査から」日医総研ワーキングペーパーNo.453.

②調査結果

サイバーセキュリティ対策が必要な医療機器の存在の認知度

図表 3-2-1 は、サイバーセキュリティ対策が必要な医療機器の存在について、全体および病床規模別の認知度の状況を示している。「知らない」(28.8%) と「あまり知らない」(28.1%) を合わせると、不認知の割合が 5 割を超える。病床規模別にみると、規模が大きくなるほど認知している割合が高くなっていた。

図表 3-2-1. 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の認知度

		n	よく知っている	知っている	あまり知らない	知らない
全体		2,989	251 8.4	1038 34.7	839 28.1	861 28.8
病床規模	診療所	1,400	87 6.2	370 26.4	398 28.4	545 38.9
	病院　20～199床	979	90 9.2	383 39.1	294 30.0	212 21.7
	病院　200～499床	463	46 9.9	204 44.1	121 26.1	92 19.9
	病院　500床以上	147	28 19.0	81 55.1	26 17.7	12 8.2

医療機器のサイバーセキュリティ情報の入手先

図表 3-2-2 は、医療機器のサイバーセキュリティ情報の入手先について、全体および病床規模別に示している。「医療機器のメーカ」(50.3%) が最も多く、次いで、「医療機器の販売業者」(41.3%)、「医療情報システム会社」(23.6%) と続く。この状況は、病床規模別にみても、ほぼ変わらない。なお、「入手していない」という割合が、病床規模に関わらず、1 割を超えていた。

図表 3-2-2. 医療機器のサイバーセキュリティ情報の入手先【複数回答】

		n	医療機器のメーカ	医療機器の販売業者	セキュリティ会社	医療情報システム会社	医師会	所属する病院団体	行政	入手していない	わからない	その他
全体		2,128	1070 50.3	878 41.3	158 7.4	503 23.6	191 9.0	144 6.8	153 7.2	291 13.7	173 8.1	74 3.5
病床規模	診療所	855	409 47.8	330 38.6	58 6.8	162 18.9	103 12.0	11 1.3	24 2.8	138 16.1	68 8.0	22 2.6
	病院　20～199床	767	403 52.5	330 43.0	60 7.8	200 26.1	72 9.4	77 10.0	79 10.3	92 12.0	59 7.7	21 2.7
	病院　200～499床	371	187 50.4	162 43.7	21 5.7	111 29.9	12 3.2	36 9.7	33 8.9	45 12.1	40 10.8	18 4.9
	病院　500床以上	135	71 52.6	56 41.5	19 14.1	30 22.2	4 3.0	20 14.8	17 12.6	16 11.9	6 4.4	13 9.6

入手したサイバーセキュリティ情報の理解度

図表 3-2-3 は、入手したサイバーセキュリティ情報の理解度について、全体および病床規模別に示している。「対策・対応の必要性の判断ができるレベルで理解している」との割合は 42.1%であった。病床規模が大きくなるほど、理解している割合も高かったが、500 床以上の病院でも、その割合は 6 割に満たない。

図表 3-2-3. 入手したサイバーセキュリティ情報の理解度

		n	対策・対応の必要性の判断ができるレベルで理解している	用語は理解できているが、対策・対応の必要性の判断はできない	用語についても理解できない
全体		1,664	701 42.1	799 48.0	164 9.9
病床規模	診療所	649	220 33.9	325 50.1	104 16.0
	病院　20～199床	616	261 42.4	311 50.5	44 7.1
	病院　200～499床	286	153 53.5	120 42.0	13 4.5
	病院　500床以上	113	67 59.3	43 38.1	3 2.7

販売業者からのサイバーセキュリティに関する説明の有無と理解度

図表 3-2-4 は、医療機器販売業者からのサイバーセキュリティに関する説明の有無とその理解度について、全体および病床規模別に示している。「説明はなかった」との割合が 37.9%、病床規模別にみても、4 割前後が「説明はなかった」との回答であった。

図表 3-2-4. 販売業者からのサイバーセキュリティに関する説明の有無と理解度

		n	説明があり、内容も十分に理解できた	説明はあったが、内容は理解できなかった	説明はなかった	わからない
全体		2,989	572 19.1	310 10.4	1134 37.9	973 32.6
病床規模	診療所	1,400	220 15.7	170 12.1	566 40.4	444 31.7
	病院　20～199床	979	212 21.7	107 10.9	340 34.7	320 32.7
	病院　200～499床	463	101 21.8	30 6.5	165 35.6	167 36.1
	病院　500床以上	147	39 26.5	3 2.0	63 42.9	42 28.6

サイバーセキュリティに関する情報が必要なタイミング

図表 3-2-5 は、サイバーセキュリティに関する情報が必要なタイミングについて、全体および病床規模別に示している。「購入検討時に必要」との回答が、病床規模に関わらず、最も多数派であった。一方、「わからない」との回答割合が少なくなく（23.9%）、病床規模が小さくなる程その割合が高かった。

図表 3-2-5. サイバーセキュリティに関する情報が必要なタイミング【複数回答】

		n	購入検討時に必要	購入時に必要	購入後、契約更新に応じて必要	購入後、求めに応じて必要	必要ない	わからない
全体		2,989	1353 45.3	743 24.9	611 20.4	593 19.8	77 2.6	713 23.9
病床規模	診療所	1,400	554 39.6	381 27.2	295 21.1	262 18.7	39 2.8	381 27.2
	病院　20～199床	979	470 48.0	210 21.5	188 19.2	201 20.5	23 2.3	221 22.6
	病院　200～499床	463	242 52.3	113 24.4	90 19.4	85 18.4	11 2.4	94 20.3
	病院　500床以上	147	87 59.2	39 26.5	38 25.9	45 30.6	4 2.7	17 11.6

“レガシーメディカルデバイス”の認知度

図表 3-2-6 は、“レガシーメディカルデバイス”という用語の認知度について[24]、全体および病床規模別に示している。「知らない」との割合が 91.3%であった。病床規模が大きくなるほど、知っている割合は高かったが、500 床以上の病院でも 75.5%が「知らない」との回答であった。

図表 3-2-6. “レガシーメディカルデバイス”という用語の認知度

		n	知っている	知らない
全体		2,989	261 8.7	2728 91.3
病床規模	診療所	1,400	55 3.9	1345 96.1
	病院　20～199床	979	97 9.9	882 90.1
	病院　200～499床	463	73 15.8	390 84.2
	病院　500床以上	147	36 24.5	111 75.5

[24] レガシーメディカルデバイス（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を指す用語である。たとえば、システムの脆弱性を排除または十分に低減する方法として、プログラムの更新またはパッチを当てることができなくなった機器のことである。
https://www.mhlw.go.jp/hourei/doc/tsuchi/T200521I0040.pdf

４．考察と提言

（１）議論の総括

本稿では、医療機器のサイバーセキュリティに関連するこれまでの政策や欧米の状況、主要な関連団体とその取り組みを整理したうえで、製造販売業者と医療現場（病院・診療所）のそれぞれを対象とした調査結果を確認した。

わが国では、2014 年のサイバーセキュリティ基本法の制定を嚆矢として取り組みが進み、内閣府に本部機能を置き、戦略と行動計画が定められている。この戦略と計画において、医療は、国家機能の中枢を担う重要インフラのひとつとの位置づけであり、医療機器のサイバーセキュリティに関わる個別規制もかかる文脈で進められてきた。関連して重要な行政文書は、厚生労働省が所管する「医療情報システムの安全管理に関するガイドライン」と「医療機器のサイバーセキュリティ確保に関するガイダンス」である。あわせて、現下のサイバーリスクに適切な対策をとるよう、製造販売業者向けに行政通知を発出することで、随時、具体的な施策が行われている。

現状、医療機器のサイバーセキュリティに関わる市販前の規制は、医機法第 41 条第 3 項に基づく「基本要件基準」に定められている。市販後には、法令により製造販売業者に課せられた「安全管理情報の収集」と「安全確保業務」という 2 つの責務が対策のポイントとなっている。

開発やサプライチェーン、資本構成等がグローバルに跨る同産業のサイバーセキュリティ確保にあたっては、規制や対処方針について、可能な限りの国際協調が求められる。そこで現在、日本では行政と業界団体が主導して、国際医療機器規制当局フォーラム（IMDRF）のガイダンスの導入と運用の準備を進めている。欧米においても、日本とほぼ同時期に（2014～2016 年）、医療機器に関するサイバーセキュリティ確保の基本的な法整備がなされている。

製造販売業者を対象とした実態調査からは、製造販売業者の組織体制の整備が発展途上である現状とユーザーである医療機関への情報提供や説明責任にも課題があることが明らかになった。直近 3 年間にインシデントを経験した割合は 2.7%だった[25]。一方、86.5%の企業がサイバーセキュリティ・ポリシーの社外公開をしておらず、28.6%に組織体制がなく、41.3%が社員教育を行っていな

[25] 調査では具体的なインシデント事例については収集していない。参考までに、これまで医療機器センターが収集した医療機器に関わるインシデント事例について、別添資料にまとめた。

かった。また、86.4%の企業に対応規定の文書がなく、79.2%が事案発生時の手順の文書化をしていなかった。加えて、79.5%の企業が販売時にサイバーセキュリティに関わる情報提供をしておらず、84.2%が市販後の情報提供をしていなかった。さらに、44.0%の企業がサイバーリスクのある医療機器の使用環境を特定しておらず、47.9%の企業ではインシデント情報を入手できるような体制になっていなかった。また、20.5%の企業が製品の寿命や使用期限、サポート終了についてユーザーへ告知しておらず、73.0%が製品のソフトウェア部品表の開示予定なし、57.5%が市販後の脆弱性改善プログラムのアップデートを行っていない、84.2%が販売業者や修理業者へのサイバーセキュリティ対策の確認・指導を行っていない、との結果であった。

病院・診療所を対象とした実態調査からは、医療機器のサイバーセキュリティという課題自体の認知度の低さが明らかになった。サイバーセキュリティ対策が必要な医療機器の存在を知らない割合（56.9%）、入手した情報を十分理解できていない割合（57.9%）はともに半数を超えており、そもそも「販売業者からサイバーセキュリティについての説明がなかった」との割合が、病床規模に関わらず、4割前後であった。既に、サイバーリスクに対応できなくなった医療機器のことを指す“レガシーメディカルデバイス”という用語に至っては、9割超が知らないとの結果であった。

以上を踏まえて、医療機器のサイバーセキュリティ確保に関わる主要なステークホルダーの役割分担と責任分界に留意しつつ、考察を加え、提言を行う。

（２）医療機器業界への期待

医療機器の使用・維持管理において、サイバーセキュリティに関わる法的な管理責任は、医療機関の管理者にあるが、行政ガイダンスが示している製造販売業者の責務（Box.4-2-1）に照らせば、次に挙げる 2 点が、その前提となる。

1. **製造販売業者から提供される医療機器やその付帯サービスについて、情報セキュリティおよびサイバーセキュリティ対応が十分なされていること。**
2. **製造販売業者からユーザーである医療機関に対して、医療機器の管理に必要な情報が、医療現場に理解できる形で、適時適切に提供されていること。**

Box. 4-2-1. 製造販売業者と医療機関それぞれの責務

○ 製造販売業者の責務

有効性及び安全性を確保した医療機器を設計・製造して供給することを責務としており、加えて、医薬品、医薬部外品、化粧品、医療機器及び再生医療等製品の製造販売後安全管理の基準に関する省令（平成 16 年厚生労働省令第 135 号）に基づき、販売後の使用における医療機器の有効性、安全性等に関する情報収集・分析、必要に応じた対策等、適切な対応が求められている。製造販売業者は医療機器への悪意を持ったサイバー攻撃に対しても、使用環境を含めた医療機器の特徴に応じて、サイバーセキュリティ対応にも取り組んでいく必要がある。

○ 医療機関の責務

医療機器に係るサイバーセキュリティへの対応については、使用者である医療機関側における当該医療機器の適切な使用、維持管理、「安全管理ガイドライン」に基づく情報システムの維持管理等日常の適切な管理が重要である。納入後の医療機器のサイバーセキュリティに関する日常の管理は、医療機関等の使用者にて実施する必要がある。また、医療機器から医療機関等の情報システムへ転送されたデータに関するサイバーリスクについては、システムの管理者である医療機関による対応が必要である。

資料：厚生労働省（2018）「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」
（厚生労働省通知 薬生機審発 0724 第 1 号・薬生安発 0724 第 1 号　別添資料）
https://www.mhlw.go.jp/content/11121000/000346114.pdf

他方で、第 3 章において示した調査結果を見る限り、上記「1. セキュリティ対応」においても「2. 医療機関への情報提供」においても、製造販売業者の対応が不十分な点が、多々あるように見受けられる。サイバー事故が発生した場合、たとえ製造販売業者側に問題があったとしても、対外的には、医療機関側にも管理責任が及ぶ可能性がある。現実的には、企業規模や予算制約等の問題から、個別の製造販売業者では十分な対応が難しいケースもあろう。ここでは、医療機器の業界団体を念頭に置き、今後期待される支援策について、要点を列挙する。

①セキュリティ・ポリシーの社外公開の促進

サイバーセキュリティ対策が必要な製品を取り扱っている企業の９割近く（86.5%）がサイバーセキュリティ・ポリシーの社外公開を行っていない現状は問題である。対外的な説明責任の強化という視点から、業界を挙げて同ポリシーの社外公開の推進（あるいは義務化）を検討してはどうだろうか。同ポリシーの社外公開がなされることで、その他の対策も並行して進むことが期待される。

②医療現場や関連業者への情報提供支援

医療機器のサイバーセキュリティに関する情報提供の現状にも課題がある[26]。個々の医療機器のセキュリティ確保に必要な情報を製造販売業者が各自管理し、医療現場や関連業者に伝達するというやり方は非効率に思える。たとえば、業界団体が加盟各社の医療機器に関する情報を一元管理し、必要に応じて参照可能にするといったやり方のほうが効率的かつ実効性が高いのではないだろうか。

③医療情報システム業界との連携

医療現場では、電子カルテやオーダリングシステム等の医療情報システムと医療機器とが接続されているようなケースが多いと思われる。医療機器のサイバーリスクへの対処にあたっては、医療情報システム業界と連携した取り組みも重要である。調査では、サイバーリスクのある医療機器の使用環境を特定していない企業が多かった（44.0%）。まずはその実態把握から始めるべきだろう。

④相談窓口機能の設置・強化

業界内に、個別の製造販売業者では対応が難しい案件発生時の相談窓口機能を設置・強化することが望ましい。内外の専門家につなぐことによる問題解決の体制構築とインシデントやアクシデントの事例を蓄積し、それらを分析することで次なるリスクに備えるリスクマネジメントの体制構築が求められる。

---

[26] 今回の調査によれば、対象企業の 79.5%が販売時にサイバーセキュリティに関わる情報提供をしておらず、84.2%が市販後の情報提供をしていなかった。84.2%が販売業者や修理業者へのセキュリティ対策の確認・指導を行っていなかった。

（３）行政・政治への提言

最後に、行政・政治向けの提言を列挙して、結びに代えたい。医療機器をはじめとする健康・医療分野のサイバーセキュリティの確保とは、換言すれば、サイバー空間における人々の健康と生命の安全保障に他ならない。医療ＤＸが進展し、サイバー空間と物理空間との融合が一層進む未来を見据えて、高い優先順位を持って取り組むべき政策課題であると考える。

①府省庁間の連携と協働

関係する政府機関のさらなる連携が求められる。医療機器のサイバーセキュリティ確保に関して言えば、日本政府のサイバーセキュリティ政策全体を統括する**「内閣府」**、薬機法をはじめとする諸規制の監督官庁である**「厚生労働省」**、医療機器産業の産業振興をあずかる**「経済産業省」**、サイバー空間におけるインフラである情報通信網を所管する**「総務省」**、実際にサイバー攻撃が発生した場合の犯罪捜査を主導する**「警察庁」**、そして 2021 年に新設され、デジタル技術を活用した各種施策の牽引役が期待されている**「デジタル庁」**という、少なくとも 6 府省庁にまたがる政策課題である。これら府省庁間の連携と協働が、有効な施策のカギである。

②ステークホルダー別の啓発活動

サイバーセキュリティ確保の要諦について、さらなる啓発活動が求められる。医療機器のサイバーセキュリティに関して言えば、(1)製造販売業者向け、(2)医療現場向け、に加えて(3)一般国民・患者向け、という少なくとも３つの対象に向けて、啓発活動を考えてゆく必要があろう。(1)製造販売業者向けに啓発活動では医機連、(2)医療現場向け啓発活動では医師会や病院団体と、関係団体と適宜協力・連携するのが望ましい。(3)一般国民・患者向け啓発活動にあたっては、米国の事例（サイバーリスクの一般向け啓発キャンペーンや具体的手法の好事例の共有）が参考になるだろう。

③国際協調と日本からの情報発信

すでに研究開発が国際的になされ、サプライチェーンがグローバルに拡がっている医療機器のサイバーセキュリティの確保にあたっては、規制の国際協調とあわせて、日本からも積極的な情報発信が求められる。そのためには、行政が主導して、業界団体や医療現場のみならず、国内外のサイバーセキュリティの専門家やリスク対応の専門家、さらには関係するアカデミアを巻き込んで、継続的に議論する場をつくることが、まずは重要である。

④人材育成のプログラム提供

中長期的視点に立てば、医療機器のサイバーセキュリティを担う人材の育成が最も重要である。かかる人材育成のためのプログラムの開発と提供は、業界やアカデミアとも協力して、行政が主導することが望ましいのではないか。たとえば、現在、内閣サイバーセキュリティセンター（NISC）の普及啓発・人材育成専門調査会でなされている議論を業界に特化させる形で、具体化させる方法が考えられる。

⑤社会実装のための財源確保

より高度なセキュリティを実現する技術やノウハウがあったとしても、医療現場にある個別の医療機器や個々の医療従事者の意識と行動に反映され初めて、現実的な意味を持つ。その社会実装のためには、新たな財源確保が欠かせない。財源の検討にあたっては、導入時にかかるイニシャルコストとその後の運用・維持にかかるランニングコストに分けて、財源の手当てを考えるべきだろう。その性質上、前者については補助金で、後者については安全確保の体制を診療報酬上評価する等の方法で、費用を賄うのが望ましいのではないか。