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