【報告様式Ａ】

課題管理番号: 21mk0102147h0003　作成／更新日:令和 4 年 5 月 31 日

日本医療研究開発機構　　医薬品等規制調和・評価研究事業
事後評価報告書

公開

I 基本情報

研究開発課題名：（日本語）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
（英　語）Study on Cybersecurity Issues of Medical Devices in Medical Institutions

研究開発実施期間：平成 31 年 4 月 1 日～令和 4 年 3 月 31 日

研究開発代表者　氏名：（日本語）中野　壮陛
（英　語）Shohei NAKANO

研究開発代表者　所属機関・部署・役職：
（日本語）公益財団法人医療機器センター・医療機器産業研究所・所長
（英　語）Japan Association for the Advancement of Medical Equipment・Medical Device Strategy Institute・

II 研究開発の概要

（和文）

製造販売業者におけるサイバーセキュリティ対策の実態調査の結果、2015 年通知から約 5 年が経過するが、未だ多くの企業に十分な組織・責任者が不在で、市販前から市販後までの一貫した具体的取り組みが不足（中小企業は対策の更なる遅れ）していた。また、サイバーセキュリティ対策に関する情報提供・収集が積極的に行われていなかった（インシデントの報告制度や情報共有システムは要検討)。サイバーセキュリティ対策を実施するうえでの課題は、専門人材の確保や社内教育、医療機関との連携、コストなどであることがわかった。

医療機関におけるサイバーセキュリティ対策の実態調査の結果は、上述の製造販売業と類似しており、専門組織の不足、ネットワーク構成図等もないケースが多く、対策資金も十分ではないことに加え、これまで医療機器に関する情報提供が産業界から十分になされていない実態が明らかとなった。また、2005 年に「医療情報システムの安全管理に関するガイドライン第 1 版」が発行されたが、比較的規模の大きい医療機関向けであること、また情報セキュリティが対象となっていることから、医療機器のサイバーセキュリティ対策についてはこれから詳細に検討する必要があると考えられた。

これらの実態調査および研究班会議での議論から、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を我が国へ導入して整備することを目的に、当事業「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」研究班及び、一般社団法人日本医療機器産業連合会において、医療機器のサイバーセキュリティに係る必要な開発目標及び技術要件等を検討し、別添のとおり、「医療機器のサイバーセキ

ュリティ導入に関する手引書」として取りまとめ 12 月 24 日付で厚労省より通知として発出された。また、医療機関向けの手引書についても同様に医機連 TF と連携し、(公社)日本医師会や四病院団体協議会（(公社)全日本病院協会）からの現場目線での意見を踏まえた案を作成した。

当該研究と通して、2015 年通知から約 5 年が経過するが、未だ多くの企業では**具体的取り組みが不足しており、現実のサイバーリスクが顕在化した今、**現状のままサイバーセキュリティ対策を各社の対応に任せるのは**自発性の観点から限界がある**と考えられた。特に、医療機関にてサイバーセキュリティ対策が講じられた医療機器を適切に取り扱っていくためには、**より強制力のある規制政策が必要**であろう。例えば、サイバーセキュリティ対策をライフサイクルを通じて発揮することを設計段階で求めるなど（実現のためには、基本要件基準の改正が必要かもしれない）といった取り組みが必要であろう。また、実際にその取り組みが妥当なものであるかを承認審査において一定の確認を行うなど（実現のためには、SBOM 等の提出を情報公開請求の対象外とした上で市販前に求めることが必要かもしれない）の検討も必要であろう。

市販後の取り組みとしては、現行の不具合報告制度で扱い切れない事象（健康被害はないものの医療機器の脆弱性が検知された事象等）の報告・共有の仕組みの議論（実現のためには、ステークホルダー間での情報共有分析のためスキーム検討が必要かもしれない）が必要であると考えられた。

また、残された SBOM・レガシー機器の扱い、中古・貸与機器の扱い、わが国特有の業許可の考え方（販売、貸与、修理業）なども積極的に議論していくことが必要である。**一方、IMDRF のレガシー医療機器、SBOM が整理**されれば、国際整合の観点やわが国の医療機器を海外展開できるものにしていく観点から**積極的に取り込んでいくべき**（同様に国際規格は積極的に導入していく姿勢が肝要）と考えられた。

さらに、**医療機関と製造販売業者の責任分界点**を決めるという観点からは、**まずは製造販売業者として、販売業者等の流通上のステークホルダーも含めてどのように責任を果たしていくのかを明確にすること**が、医療機関自らの責任を検討するうえでも非常に重要であろう。

最後に**医療分野は国の重要インフラ**に指定されており、また**何か問題があれば生命に直結**することが医療機関におけるサイバーセキュリティ対策の特徴であるので、**医療機器産業もそれを理解した対策を施すべき**であるし、**製造販売業者向けの手引書の普及啓発活動**に取り組むことが重要であると考えられた。

なお、製造販売業者が取り組むべきサイバーセキュリティ対策として、下記のような項目が重要であることを見出した。

- 情報を提供する体制を構築
- 製造、製造販売、販売、修理等の一貫したサイバーセキュリティ体制の構築
- 製造販売業者の情報収集体制を構築
- 医療機関に提供できる文書等の形で整理する必要
- 製造販売業者から提供された資料が医療機関で理解できるようにするためのマニュアルの整備
- 懸念点を解消したうえで製造販売業者が SBOM を開示しやすい環境を構築
- 市販前からサイバーセキュリティに関する情報を整備する必要

(英文)

From the fact-finding investigation about cybersecurity for medical devices on a manufactures and health delivery organizations (HDO), although approximately five years had passed since the 2015 notification, there are still lack of effective cybersecurity. Therefore, there are limitations in terms of spontaneity in terms of responding to cybersecurity by leaving it up to each company. In particular, a more enforceable regulatory policy is needed to ensure that medical devices with cybersecurity measures are properly handled by HDO. For example, it may be necessary to mandate that cybersecurity methods throughout the total product lifecycle be demonstrated at the design stage. It would also be necessary to verify during the approval process whether such measures are in fact appropriate.

As a postmarket management, it was considered necessary to discuss a mechanism for reporting and sharing events that are not fully handled by the current defect reporting system. For example, it may be necessary to discuss how to handle events in which vulnerabilities of medical devices are detected, although no health hazard is involved.

It is also necessary to discuss the handling of SBOM and legacy medical devices, used and loaned medical devices, and the Japan-specific regulations (business licenses: sales, lending, and repair business). The consideration of international harmonization is also important.

Furthermore, it is also important to determine the boundary of responsibility between the HDO and the manufacturer/distributor. First step is to clarify how to perform the responsibility as a manufacturer and distributor, including distributors and other stakeholders in distribution, which will be very important in examining the responsibility of medical institutions themselves.

Finally, the medical field is classified as a critical national infrastructure, and cyber security measures at HDO are characterized by the fact that any problems can directly affect human life. Therefore, the medical device industry should take cybersecurity for medical devices based on an understanding of the benefits and risks, and it is important to promote and educate manufacturers and distributors about the guidance manual prepared by this research group.