

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研究事業)
分担研究報告書

医療機器サイバーセキュリティの市販後安全対策に関する研究

研究分担者 宮島敦子 国立医薬品食品衛生研究所 医療機器部 室長
研究協力者 野村祐介 国立医薬品食品衛生研究所 医療機器部 室長

研究要旨：

我が国では、医療機器分野において令和5年度を目途にIMDRFガイダンスに基づくサイバーセキュリティ（CS）確保に関する規制を国内に導入する方針が示されている。当該ガイダンスには具体的方法が記載されていないため、実現可能な規制方法を早急に構築する必要がある。

本研究では、産官学連携の下に検討班（WG）を設立し、医療機器CS関連の不具合報告事例、海外の規制状況について調査を進めると共に、医療機器CSに関する不具合報告の基本的考え方について検討を行った。医療機器CSの不具合報告事例については、一般社団法人日本医療機器産業連合会、製造販売後調査委員会CS不具合報告サブWGと連携し、海外における不具合事例、脆弱性に関する事例等についての調査結果が共有されたと共に、国立衛研、検討委員によっても調査された。これまでに患者に健康被害があった事例はなく、CSにおいて特化した不具合の考え方はないが、不具合及び脆弱性の情報共有体制が国毎に異なると共に、当該体制構築が重要であることが判明した。個別事例を踏まえ、一般化して提示できる不具合報告事例の整理を進めている。来年度は、海外の規制状況調査を行い、各国でのCSに関連した医療機器の不具合等報告制度、関連団体との情報共有状況、その他情報収集体制についての調査を進め、文書案をとりまとめる。

研究協力者

山本栄一 国立医薬品食品衛生研究所
医療機器部 部長
中岡竜介 国立医薬品食品衛生研究所
医療機器部 室長
岡本吉弘 国立医薬品食品衛生研究所
医療機器部 室長
迫田秀行 国立医薬品食品衛生研究所
医療機器部 主任研究官

A. 研究の背景・目的

近年、科学技術の発展に伴い、IoT医療機器を含む様々な製品のほか、他社製品を組み合わせて使用する可能性のある医療機器等、新しい形態の医療機器が医療現場に導入されつつある。これらの医療機器では、サイバーセキュリティ（CS）や、他社製品を組み合わせる際の留意点等、市

販後安全対策に関する新たな課題が存在する。

本邦における医療機器のCSの確保については、平成27年4月28日付けで厚生労働省大臣官房参事官(医療機器・再生医療等製品審査管理担当)・医薬食品局安全対策課長連名通知「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」が発出され、医療機器の安全な使用の確保のため、医療機器に関するサイバーリスクに対する適切なリスクマネジメントの実施が求められることになった。国際医療機器規制当局フォーラム(IMDRF)において、CS対策の国際的な調和を図ることを目的として、医療機器CSガイドランス N60「Principles and Practices for Medical Device Cybersecurity」(以下「IMDRFガイドランス」という。)が発行されたことを受け、令和2年5月13日に厚生労働省2課長連名通知「国際医療機器規制当局フォーラム(IMDRF)による医療機器CSの原則及び実践に関するガイドランスの公表について(周知依頼)」が発出された。さらに、IMDRFガイドランスの発行を踏まえて、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、国内に導入、整備することを目的として、市販前を中心に医療機器のCSに係る必要な開発目標及び技術的要件等について検討され、令和3年12月24日に厚生労働省2課長連名通知「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」が発出され、別添として医療機器製造販売業者向けの「医療機器のサイバーセキュリティ導入に関する手引書」が示された。国境を超えて行われる医療機器に対するサイバー攻撃への対策を一層強化して医療現場における安全性を確保するため、医療機器のCSに係る開発目標及び評価

基準が策定され、「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年厚生労働省告示第122号 以下「基本要件基準」という。)が改正された。改正後の基本要件基準第12条第3項は、令和5年4月1日から適用され、1年間の経過措置期間が設定されている。IMDRFにおいては、追補ガイダンスが発出され、その内容に基づき、一般社団法人 日本医療機器産業連合会(医機連)の医療機器CS対応ワーキンググループ(WG)において、Software Bill of Materials(SBOM)の取扱いやレガシー医療機器の取扱い、脆弱性の修正、インシデントの対応等を検討し、令和5年3月31日に 厚生労働省2課長連名通知「医療機器のCS導入に関する手引書の改訂について」が発出され、医療機器製造販売業者向けの「医療機器のCS導入に関する手引書(第2版)」が示された。

医療機関等の医療情報システムに関しては、厚生労働省から「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版が平成17年3月に示され、情勢に応じた改定が随時行われ、令和4年3月第5.2版に至っている。以下「安全管理ガイドライン」という。)が発出されている。また、医療機関における医療機器のCSに係る対応については、令和5年3月31日に 厚生労働省3課長連名通知「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」が発出され、「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」(別添)が示された。

本研究では、産官学連携の下にCSWGを設立し、医療機器CSの不具合報告事例、海外の規制状況について調査を進めると共に、

医療機器 CS に関する不具合報告の基本的考え方について検討を行った。本稿では、当該調査と提言案についての進捗状況について報告する。

B. 研究方法

B-1. サイバーセキュリティワーキンググループの設立

IMDRF ガイドランスの国内導入に向け、市販後安全対策等に係る「医療機器サイバーセキュリティに関する不具合報告の基本的考え方について」の提言案を作成するため、本研究班において、CSWG を設立し、検討会議を開催した。医機連及び公益社団法人 日本臨床工学技士会に研究協力と推薦委員の派遣を依頼した。

WG の委員メンバーは、以下の通りである。(敬称略)

- ・ 青木郁香：公益社団法人日本臨床工学技士会
- ・ 新 秀直：東京大学医学部附属病院 企画情報運営部
- ・ 北川智也：富士フイルム株式会社
- ・ 中里俊章：キャノンメディカルシステムズ株式会社
- ・ 中野壮陸：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
- ・ 肥田泰幸：東都大学 幕張ヒューマンケア学部 臨床工学科
- ・ 松元 恒一郎：日本光電工業（株） 技術戦略本部
- ・ 山田晴久：アボットメディカルジャパン合同会社

その他、厚生労働省 医薬・生活衛生局 医薬安全対策課及び医療機器審査管理課の担当者（オブザーバー）、医薬品医療機器総合機構（PMDA）医療機器品質管理・安全対

策部 医療安全情報管理課の担当者（オブザーバー）、そして国立衛研の本研究課題の分担研究者及び研究協力者（会議事務局）により構成した。

B-2. 医療機器サイバーセキュリティの不具合報告事例と海外の規制状況の調査について

医機連 CS の不具合報告サブ WG は、医機連製造販売後調査（PMS）委員会の中のサブ WG で、「不具合報告等の手引書 第 8 版」の改訂に向け、CS の不具合報告の具体的な事例情報収集及び手引書への追加内容について討議を行なっている。本研究班 WG の医機連 PMS 委員会所属委員より、当該サブ WG の情報が提供された。

医療機器CSの不具合報告が必要な事例の整理や定義づけ、報告のスキームが、提言案を作成する上で重要な課題であることから、事務局において、米国及びEUにおける状況について調査した。

海外における医療機器のCSにおける市販後安全対策に関する規制体制や規制当局からの推奨事項等を調査した上で提言案についての検討を進めることとした。当該調査は中野委員及び中里委員が実施し、IMDRF に参加し、医療機器の薬事制度が整えられている国の規制当局を中心に、各国でのCSに関連した医療機器の不具合等報告制度、関連団体との情報共有状況、情報収集体制等について調査を進めた。対象国・地域は日本、米国、カナダ、豪州、欧州、英国の6カ国とした。

B-3. 医療機器サイバーセキュリティに関する不具合報告の基本的考え方について

本研究では、必要に応じて医療機器 CS

の不具合報告事例、海外の規制状況について調査を進め、最終的には「医療機器サイバーセキュリティに関する不具合報告の基本的考え方」についての文書案を作成することを目的としている。事務局において、文書素案を作成したと共に、WG において項目の過不足、記載内容について議論した。

(倫理面への配慮)

本研究は、医療機器 CS の不具合報告事例、海外の規制状況について調査と医療機器 CS に関する不具合報告の基本的考え方についての提言案作成に係る研究であり、倫理申請等は不要である。

C. 結果及び考察

「医療機器サイバーセキュリティの市販後安全対策に関する研究」における CSWG を計 5 回実施した。

第 1 回 CSWG では、本事業の概要説明と、「新しい資本主義のフォローアップ」についての紹介があった。「新しい資本主義のフォローアップ」では、2023 年度までに、薬事承認後の医療機器のサイバーセキュリティに関する情報収集や評価の方法を具体的に検討し、その内容を周知することが閣議決定された。IMDRF ガイダンスの国内導入に向け、市販後安全対策等に係る技術的内容について、医機連 WG と連携しながら進めていくこととした。医機連 WG での活動及び、AMED 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に係る課題抽出等に関する研究」(2019-2022) についての情報提供があった。サイバーセキュリティに関する不具合報告について、必要な事例や考え方の整理が、この研究班における主な課題となる。必要に応じて海外における不具合報告、情報共有、及び収集等に関

する調査等を実施し、関連部署と情報共有をしながら進めていく。

第 2 回 - 第 5 回 CSWG では、問題点整理と提言骨子案についての検討を行なった。検討項目は、医療機器の不具合報告について、医療機器の不具合事例について、医療機関における報告内容と報告先について、協調的な脆弱性の開示 (CVD) 等についてであった。提言作成と並行して、海外の CS に関する規制の状況についての調査も実施し、調査結果を踏まえて議論を行い、提言案に反映させることになった。医療機器の不具合報告については、医機連 PMS 委員会、不具合報告の手引改訂 WG 傘下にある「CS の不具合報告サブ WG」の活動と情報共有することとした。CSWG の主な活動結果は以下の通りである。

C-1. 医療機器サイバーセキュリティの不具合報告事例について

医機連 CS の不具合報告サブ WG では、医機連に所属の製造販売業者を通じて、不具合事例、脆弱性に関する事例についての調査を行った。その結果、日本での不具合に関する個別報告で様式 8 に相当する案件は現時点ではなかった。米国 Food and Drug Administration (FDA) において、市販後管理の不具合報告は、死亡や重篤な被害を受けた場合などリスクを判断の上で報告し、基本的には従来の法規制要件に従って実施されていることが紹介された。外資系企業による調査の結果、海外においても、これまでに患者に健康被害があった事例はないことが判明した。FDA からの注意喚起として代表例が挙げられており、インスリンポンプ及び植込み型除細動器等の植込み医療機器に報告の事例を踏まえ、一般化して

提示できる不具合報告事例の考え方等について議論を行った。本研究における WG では、引き続きサブ WG における整理結果を共有し、提言案に反映させていく。

事務局において、米国及び EU における不具合報告、情報共有、情報収集状況に関する調査を実施し、WG において紹介した。FDA の「Cybersecurity Safety Communications and Other Alerts」、「Postmarket Management of Cybersecurity in Medical Devices - Guidance for Industry and Food and Drug Administration Staff」、「Cybersecurity Vulnerabilities in Certain GE Healthcare Clinical Information Central Stations and Telemetry Servers: Safety Communication」、EU の「MDCG 2019-16 Rev.1 Guidance on Cybersecurity for medical devices」について調査し、これらの簡易翻訳、概要について紹介した。FDA の文書において、これまで CS の事故に関連した患者の負傷や死亡を認識しておらず、CS 上の脆弱性の修正と報告例は、いずれも実際に起こった事例ではなく、パッチ等に対応可能な例が挙げられていた。パッチの適用や緩和策がなされない場合、これらの脆弱性が患者に危害を与える可能性があるとしていた。EU の医療機器規則では、重大な事故の定義は、患者の死亡に繋がる場合、健康状態が一時的または永続的に悪化する場合、公衆衛生上の重大な脅威とされている。CS の観点からのインシデントと重大インシデントの区別について、こちらでも、いくつかの例が示されているのみであった。

当該調査結果は、医機連 CS の不具合報告サブ WG の調査を含めて検討を行う必要がある。WG において、調査対象の候補として、他に英国、カナダ、豪州が挙がっており、米国、EU ともに現在、改訂等が進めら

れている状況であることから、追加調査の必要性が議論された。

C-2. 海外の規制状況の調査について

海外調査結果に関して、情報を深掘りして、米国や EU がどのような考えで CS による不具合や情報整理を実施しているかを調査、整理し、日本の環境に照らし合わせて文章を直していくのが良いとの意見があり、中野委員と中里委員が、日本、米国、カナダ、豪州、欧州、英国を対象として、各国での医療機器の CS における市販後安全対策に関する海外での規制体制や規制当局からの推奨事項等についての調査を進め、第 5 回 WG で紹介した。

<不具合報告等制度について>

一般的な医療機器不具合等報告制度については、各国において本邦と同様の報告対象、報告期限、報告者の取り決めがあることが確認された。医療機器の CS に関連した不具合報告については、一般的な不具合報告制度と区別した特別な報告クライテリアを設けている国はない。

<関係機関での情報共有及び医療機関や関係する企業等への情報発信について>

米国、カナダ、豪州においては、CS に関連した医療機器脆弱性の情報収集について、高い関心を持って情報収集制度が整えられており、重要な脆弱性に関わる問題については、医療機器メーカーが情報を得てから短期間で関係機関に情報共有を行うような仕組みが整備されている。米国においては、医療機器を所管する FDA と、CS に関する情報を管理している規制当局間での情報共有体制が整えられていることが確認された。

また、豪州は通常の不具合報告とは別のホットラインが整備されていた。いずれの国においても、情報共有体制が極めて重要であることが判明した。

今回調査した 6 ヶ国は、医療機器の規制が進んでいて積極的に実施している国を選定しており、現時点では、まだ調査不足である。参考にした情報は、公になっている文書等であり、記載内容について、過不足がないか確認する必要がある。一方で、調査時期の関係上、当該調査においては EU、米国の改訂等の情報は組み込まれており、今後も軽微な変更は考えられるが、骨格は定まった状況であることが判明した。

次年度は、事務局で参考文献の簡易翻訳を作成し、全 51 資料について内容の詳細及び情報の過不足を確認すると共に、文章を完成させてから、研究班で議論を行う。

C-3. 医療機器サイバーセキュリティに関する不具合報告の基本的考え方について

医療機器 CS の不具合報告事例、海外の規制状況について調査を進めると共に、事務局が「医療機器サイバーセキュリティに関する不具合報告の基本的考え方」の素案(たたき台)を作成し、WG において、項目立ての過不足、記載内容について討議を行った。現時点の章立てを、図 1 に示した。

本文書の対象は、医薬品医療機器等法 第 2 条 4 号に定義された医療機器における、無線又は有線により、メディア媒体を含む他の機器、ネットワーク等との接続が可能なプログラム医療機器を含む医療機器及びプログラムを用いた附属品等を対象とした。なお、医療機器のクラス分類を問わないとした。不具合、脆弱性の定義を記載し、脆

弱性の全てが報告の対象ではなく、共通脆弱性スコアリングシステム (Common Vulnerability Scoring System : CVSS) 等の広く採用されている脆弱性スコアリングシステムを採用して評価することとしている。一方で、CVSS スコアは、医療機器として臨床環境や患者安全への影響へ置き換え、再評価する必要があることから、当該部分の記載については、さらなる討議を要する。医療機器 CS に関する不具合報告においては、CS に特化した報告は不要であり、医療機器として実施する。今後、製造販売業者が報告すべき不具合事例に関しては、医療機器 CS の不具合報告サブ WG における討議結果や、海外各国での医療機器の CS における市販後安全対策に関する規制体制や規制当局からの推奨事項等についての調査結果を踏まえて日本の環境に照らし合わせた上で、本提言に反映させていく必要がある。

D. 結論

産官学連携の下に検討班(WG)を設立し、医療機器 CS の不具合報告事例、海外の規制状況について調査を進めると共に、医療機器 CS に関する不具合報告の基本的考え方について検討を行った。各国、情報共有体制は異なるものの、不具合報告は医療機器として実施し、CS に特化した対応はないことが判明した。引き続き海外における CS に関連した調査を進め、「医療機器サイバーセキュリティに関する不具合報告の基本的考え方」についての文書案をとりまとめる。

E. 研究発表

1. 論文発表
なし
2. 学会発表

なし

F. 知的財産権の出願・登録状況

(予定を含む。)

1. 特許取得

なし

2. 実用新案登録

なし

3. その他

なし

提言骨子案

「医療機器サイバーセキュリティに関する不具合報告の基本的考え方」 (案)

1. はじめに
2. 本文書の対象
3. サイバーセキュリティの不具合と脆弱性
 - (1) 不具合
 - (2) 脆弱性
 - (3) 不具合報告における脆弱性
4. 不具合報告の基本的事項
5. 不具合報告
 - (1) 製造販売業者における報告内容と報告先
 - (2) 医療機関における報告内容と報告先
 - (3) 製造販売業者が報告すべき不具合事例
 - (4) EOS及びEOL

図 1. 提言骨子案