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（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。本年度は、CSWG にて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とりまとめた。医機連 CS の不具合報告サブ WG と連携して、医療機器 CS 関連の不具合報告事例として記載すべき内容について検討し、医療機器 CS に関する不具合報告の基本的考え方（案）をまとめ、厚生労働省・医薬安全対策課に提出した。当該成果を受けて、令和 6 年 1 月 15 日付で、医薬安全対策課長通知（医薬安発 0115 第２号）「医療機器サイバーセキュリティに関する不具合等報告の基本的考え方について」が発出された。

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て使用する際の留意点等、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ガイダンス N60「Principles and Practices for Medical Device Cybersecurity」（以下「IMDRFガイダンス」という。）が発行されたことを受け、令和2年5月13日付けで厚生労働省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（周知依頼）」が発出された。さらに、IMDRFガイダ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日付けで厚生労働省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「医療機器のサイバーセキュリティ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 日付けで 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。

続いて、令和 5 年 5 月 23 日付けで厚生労働省 医療機器審査管理課長通知「医療機器の基本要件基準第 12 条第 3 項の適合性の確認について」、令和 5 年 7 月 20 日付け事務連絡「医療機器の基本要件基準第 12 条第

３項の適用に関する質疑応答集（Q＆A）について」が発出された。

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、当該調査と厚生労働省に提出した提言案に向けた検討会の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 ガイダ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：キヤノンメディカルシステムズ株式会社
- 中野壮陛：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。当該サブ WG と連携の下、本研究班 CSWG で、製造販売業者が報告すべき CS の不具合報告の具体的な事例を整理した。

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/地域とした。本年度は、参考文献について、簡易翻訳を作成し CSWG で共有すると共に、事務局で内容について確認し、補足、追加等を行い整理したものについて、

過不足等ないか確認し、討議後、最終案を取りまとめた。

B-3. 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

本研究では、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作成することを目指し、CSWG において議論し、文書をまとめた。

（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 を令和 5 年 8 月 16 日、9 月 27 日の計 2 回実施した。以降はメールにより討議を行なった。

第 1 回 CSWG では、本事業の概要説明があった。本事業では、薬事承認後の医療機器の CS に関する情報収集や評価の方法を具体的に検討し、取りまとめ案を作成することを目指すことを確認した。昨年度より継続している、海外規制状況調査報告書の作成については、事務局で内容について確認し、補足、追加等を行い整理したものについて、過不足等ないか確認し、討議後、最終化とすることとした。

提言骨子案については、海外調査報告書の内容を受けて、まず、全体の構成についての議論を行う。第 2 回 CSWG にて、各項の内容の詳細について議論する。CS の不具合報告については、医機連 CS の不具合報告サブ WG と連携の下、製造販売業者が報告すべき CS の不具合報告の具体的な事例を整理した。第 2 回 CSWG において討議された内容を提言骨子案に反映させ、メール審議を行い 11 月末に最終案を取りまとめ、医薬安全対策課に提出した。

C-1. 医療機器 CS に関する海外規制状況の調査について

昨年度より継続して、日本及び海外各国における規制状況について調査を行い、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 CSWG にてとりまとめた。参考文献の簡易翻訳を作成し委員間で共有した。事務局で内容について確認し、補足、追加等を行い整理したものについて、過不足等ないか確認し、討議後、最終版とした。海外調査報告書は骨子案を整理するための資料とする。

第 1 回 CSWG にて、海外規制状況調査報告書案について討議を行った。主な内容は以下の通りである。

・タイトルを「医療機器に関連したサイバーセキュリティ脆弱性に対する市販後安全対策体制の調査」に修正する。

・不具合報告の報告様式に関して、不具合・感染症症例報告書及び未知非重篤不具合定期報告書に限定し、判断基準と報告期限について概要を表にて掲載する。

・本邦における CS の脆弱性に関して、医機連の医療機器 CS 対応 WG において、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 2 つの通知が発出されたが、脆弱性に対する情報共有体制についてはまだ整っていない。製造販売業者が実施する範囲を明確にする。
・カナダと豪州においては、CS に関して、一般的な不具合報告制度と区別して報告できる体制が整えられていた。しかしながら、その後の情報伝達、情報共有等に関する連携についての情報は得られなかった。
・重大な脆弱性が見つかった場合に、企業内での情報収集、評価、報告などに関する体制の構築が重要である。製造販売業者に着目した内容を追記する。
・自社の医療機器製品の脆弱性が見つかった場合は、製造販売業者が責任を持って情報共有を行う必要がある。重大で共通性が高い脆弱性が見つかった場合には、協調的な脆弱性の開示（Coordinated Vulnerability Disclosure: CVD）実施する。
・欧州において、レジリエンス法はまだ審議の段階なので、全体として適用されるのはもう少し後になると思われる。NIS 2 が、2024 年 10 月 18 日より施行予定であるため、NIS 2 の施行について本文を修正すると共に、不具合等報告の報告期限の部分は NIS 2 の内容に修正する。

第 2 回 CSWG では、第 1 回の討議において出された論点に従って修正案を作成後、委員や関係者からコメントを収集し、さらなる修正を行った案について討議を行った。主な内容は以下の通りである。
・「3. 調査結果 3.1.2 サイバーセキュリティ脆弱性に対する情報収集及び共有体制」において、「企業内においては、脆弱性に関する情報の収集、評価、報告に関する情報共有体制の構築が必要である。」とあるが、製造販売業者が行う事項であるため、「製造販売業者は」に修正する。

第 2 回 CSWG において、討議された内容を反映させ、最終案を取りまとめた。本 CSWG にて取りまとめた「海外規制状況調査報告書」を別紙 1 に示す。

C-2. 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

海外調査報告書の内容を受けて、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。医機連 CS の不具合報告サブ WG と連携して、医療機器 CS 関連の不具合報告事例として記載すべき内容について検討し、提言骨子案をまとめ、厚生労働省・医薬安全対策課に提出した。

第 1 回 CSWG では、全体の構成についての議論を行った。主な内容は以下の通りである。
・本提言骨子は、製造販売業者向けであることから本文において対象を明記すると共に、内容、順番について整理する。
・不具合報告については、不具合によるものと疑われる症例等を知ったとき、または不具合は生じていないが、患者に重篤な健康被害が発生するおそれのある症例等を知った場合、製造販売業者は、各報告様式に関して施行規則に従って不具合報告の義務がある。
・「CS に特化した報告は不要」という記載は、ニュアンスとしては理解できるものの、誤解を招く表現であるため、「この不具合は、医療機器全てに関わるもので、サイバーセキュリティに関しても同様である。」という記載に揃える。

・CS の事例は、現状では実績がないので、報告すべき事例ではなく、CS 上の問題の事例である。あらかじめサブ WG との打合せを実施する。
・医療機関は PC 等のウイルス感染事故の場合、国に報告する。医療機器においては、当該感染事故は報告義務もなく、情報も集まらない。メーカーがリスクを判断した場合はあがってくる可能性はあるが不具合には当てはまらない。医療機関側からの窓口を記載して欲しい。
・医療機関の項目をどの程度記載するかは、検討の必要がある。医政局の窓口は、情報セキュリティや院内 PC 等ウイルス感染による診療のストップ等（医療行為自体への影響）を懸念して設けられているため、医療機関の方からみると、薬機法の不具合との切り分けが難しくなってくる。
・CVD に対して製造販売業者がどのような対応、体制構築が必要かを記載する。
・End of Support（EOS）や End of Life（EOL）、レガシー医療機器について定義を載せた上で、製造販売業者に求められる活動について整理する。
・医療機関からの報告については、現行制度の医療機関報告が前提になるため、今回は無理のない範囲でまとめ、できることなら参考となる事例も加えて欲しい。その後の医療機関における展開については、PMDA や医機連の協力を得ながら各ガイドラインの内容を医療従事者に伝えるのは、職能団体や病院団体等を通じて行うと思われる。従来の医療機関報告も同様だが、制度が十分に活用されていない。医療機関については、制度について正しく理解するための教育が重要であると思われる。

第 1 回の討議において、海外規制状況調査報告書案及び提言骨子案について、論点及び多くの修正点が明らかとなった。

第 2 回 CSWG では、第 1 回の討議において出された論点に従って事務局が各文書の修正案を作成後、委員や関係者からコメントを収集し、さらなる修正を行った提言骨子案について討議した。主な内容は以下の通りである。
・本提言骨子案は製造販売業者向けであることから、医療機関における報告「4.（2）医療機関における報告内容と報告先」、「5.（5）医療機関における報告内容と報告先」は記載しない方向で調整することとした。医療機関における報告については、厚労科研費の報告書にまとめを記載することにした（C-3.）。

提言骨子案の全体の構成を、以下のように修正した。

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
4. 不具合報告の基本的事項
   （1）製造販売業者における報告内容と報告先
5. サイバーセキュリティに関する不具合報告
   （1）製造販売業者における報告内容と報告先
   （2）製造販売業者が報告すべき不具合事例
   （3）脆弱性に関する対応
   （4）医療機器の EOL、EOS 及びレガシー医療機器
6. 情報共有体制について

7. まとめと今後の展望

・「1.はじめに」において「医療機器は、国内外に流通すると共に、国境の枠組みを超えてサイバー攻撃が行われる可能性が高いことから」とあるが、医療機器であることそのものがサイバー攻撃を受ける可能性が高いと受け取れるため、「国境の枠組みを超えてサイバー攻撃が行われる可能性があることから」に修正した。
・「１．はじめに」に、この文書の立ち位置が分かるような文章が追加できると良い。サイバーセキュリティの不具合報告は、基本的には医療機器の不具合報告と同じ考え方であるが、CS の対策は特性を持つので、この点を強調する必要があるために文書を発出したという内容を追記することにした。
・CS の不具合の記載事例は、想定し得る事象が記載されているため、CS の不具合報告サブ WG にて、「CS の不具合報告が必要と想定される事例として討議された事例」に修正することにした。10 月 30 日に医機連 CS の不具合報告サブ WG が開催され、サブ WG における議論を受けて、最終文案とした。
・脆弱性に関する対応に関して、「例えば MITRE 社が策定した医療機器向けのガイド（MITRE Rubric for Applying CVSS to Medical Devices）が参考となる。」とあるが、一部の認証機関からこのガイドがうまく適応できない可能性が指摘されており、例示として残すか討議した。その結果、「参考となる資料の一つに、MITRE 社が策定した医療機器向けのガイド（MITRE Rubric for Applying CVSS to Medical Devices）がある。」に修正し、例示として残すことにした。
・医療機器の EOL、EOS 及びレガシー医療機器の定義については、IMDRF ガイダンス和訳より引用することとし、記載を整備した。
・EOS に関して、「製造販売業者は EOS に至るまでに発生した不具合に関する情報収集義務及び行政報告義務があるだけでなく、EOS 後を含めた医療機器の製品ライフサイクル全体を通して、発生した不具合に関する情報収集義務及び行政報告義務も製造販売業者に残る。」とあるが、発生した不具合に関する情報収集、行政報告義務は、EOS に至るまでと EOS 後を含めた医療機器の製品のライフサイクル全体であることから、内容を整理し修文した。
・「６．情報共有体制について」「情報共有体制の構築・維持が必要であり」としたように、作るだけでは駄目で、それを維持していくことも重要である。「人材育成の増強」の部分は「そこに併せて継続的な人材育成が望まれる」の表現が良い。

第 2 回 CSWG の討議結果を提言骨子案に反映させ、修文案に対して CSWG 委員及び医機連 CS の不具合報告サブ WG よりコメントを収集し、メール審議を行った。主な内容は以下の通りである。
・「1. はじめに」において、この文書の立ち位置が分かるように記載を整備した。CS 対策が十分と思われても、未知の脆弱性は対応することが難しく、サイバー攻撃に起因する不具合等が起こってしまう可能性がある。医療機器においては、未対応の脆弱性を悪用されて侵入を許した、攻撃性の強いマルウェアに感染した等の時点で、その影響は当該機器に留まらず、同様の脆弱性をもつその他の医療機器や医療システム全体へも影響する等、通常の不具合とは異なり、波

及性が非常に大きいことから、CS に特化した速やかな対応が必要であること及び、本文書が製造販売業者向けであることを明らかにした。

・「5. サイバーセキュリティに関する不具合報告」における製造販売業者が報告すべき不具合事例は、医療機器に共通の事例と個別医療機器の事例に分類して記載することとし、医機連 CS の不具合報告サブ WG において了承された。不具合事例の記載は、「不具合報告等の手引書の改訂版における記載と共通である。

・CS に関する不具合事例「脆弱性が認められ、不正アクセスにより悪用の実績（誤動作、機能不全等）が発生した。」については、補足として、「不正アクセスによる悪用の実績がサポート終了（EOS）の前後にかかわらず、製造販売業者は不具合報告の必要性を適切に判断する必要がある。」を追記した。

その他、軽微な修正等を行い、最終案を 11 月末に厚生労働省・医薬安全対策課に提出した。同課においてさらに改訂後、令和 6 年 1 月 15 日付で、医薬安全対策課長通知（医薬安発 0115 第２号）「医療機器サイバーセキュリティに関する不具合等報告の基本的考え方について」（別紙２）が発出された。

C-3. 医療機関における CS に関する不具合報告の内容と報告先について

本 CSWG で作成した提言骨子案は、製造販売業者向けであることから、本文において対象を明記すると共に、医療機関における CS に関する不具合報告の内容と報告先に関する記載部分は削除した。今後、医療機関における報告に関しては、改めて討議がなされ、周知されていく必要があると思われる。本 WG にて検討した、「不具合報告の基本的事項における医療機関における報告内容と報告先」、及び「サイバーセキュリティに関する不具合報における医療機関における報告内容と報告先」を別紙３に示す。

D. 結論

産官学連携の下に検討班（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。本年度は、CSWG にて、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とりまとめた。

医機連 CS の不具合報告サブ WG と連携して、医療機器 CS 関連の不具合報告事例として記載すべき内容について検討し、医療機器 CS に関する不具合報告の基本的考え方（案）をまとめ、厚生労働省・医薬安全対策課に提出した。当該成果を受けて、令和 6 年 1 月 15 日付で、医薬安全対策課長通知（医薬安発 0115 第２号）「医療機器サイバーセキュリティに関する不具合等報告の基本的考え方について」が発出された。

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

１．特許取得

なし

２．実用新案登録

なし

３．その他　　なし

別紙１

医療機器に関連したサイバーセキュリティ脆弱性に対する市販後安全対策体制の調査

1. 調査の目的

国内外に流通する医療機器においては、国境の枠組みを超えてサイバー攻撃が行われる可能性が高いことから、サイバーセキュリティ対応の国際調和を図ることを目的として、 国際医療機器規制当局フォーラム（International Medical Device Regulators Forum：IMDRF）において、医療機器サイバーセキュリティガイダンス N60「Principles and Practices for Medical Device Cybersecurity」（以下「IMDRF ガイダンス」という。）が取りまとめられた[1)]。我が国では、令和 5 年度を目途に IMDRF ガイダンスに基づく対応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。

本報告では、「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」関する文書案を取りまとめるにあたり、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を調査したと共に、国内において求められる製造販売業者を中心とした市販後安全対策体制について考察した。

2. 調査方法

国内、及び国内と同様に、IMDRF に参加している国の中から、医療機器の薬事制度が整えられている米国、カナダ、豪州、欧州、英国の規制当局について、各国でのサイバーセキュリティに関連した医療機器の不具合等報告制度について調査を行った。調査にあたっては、各国規制当局のホームページから不具合報告制度に関する情報を収集した。また、サイバーセキュリティに関連した医療機器の不具合等の情報収集に積極的に取り組んでいる規制当局に関しては、不具合等報告制度に加え、関連団体との情報共有状況等、その他情報収集体制についても調査を行った。

3. 調査結果

3.1 本邦におけるサイバーセキュリティ脆弱性に対する報告制度について

3.1.1 従来の医療機器の不具合等報告制度

医療機器の不具合報告は、医薬品医療機器等法 第 68 条の 10 第 1 項[2)]及び施行規則第 228 条の 20 第 2 項[3)]に従い実施する。この不具合は、医療機器全てに関わるもので、サイバーセキュリティに関する不具合も含まれる。

不具合報告は以下の方法による。

医療機器の製造販売業者等は、「医薬品等の副作用等の報告について」平成 26 年 10 月 2 日付け薬食発 1002 第 20 号厚生労働省医薬食品局長通知[4)]を参照とし、所定の様式により以下の報告書を医薬品医療機器総合機構（PMDA）に提出しなければならない。

- 医療機器不具合・感染症症例報告書（国内／外国）
- 医療機器に係る不具合の発生率変化調査報告書
- 医療機器の研究報告／外国における製造等の中止、回収、廃棄等の措置調査報告書
- 医療機器品目指定定期報告書
- 医療機器未知非重篤不具合定期報告書

不具合等報告書は、報告期限内に、PMDA 医療機器品質管理・安全対策部医療機器安全課に提出する。

なお、国内死亡症例についての全ての症例並びに外国医療機器に係る製造、輸入又は販売の中止等保健衛生上の危害の発生又は拡大を防止するための措置が講じられた場合の全ての措置内容について、PMDA 医療機器品質管理・安全対策部医療機器安全課に対し、ファックス等により速やかに第一報の報告をする。報告期限には、以下の様に生じた健康被害の重篤性に応じて情報入手日からの 15 日、30 日、定期がある。医療機器不具合・感染症症例報告及び未知非重篤不具合定期報告では、下表のように不具合報告の判断基準及び報告期限が定められている。

表 1　不具合報告の判断基準及び報告期限

(1) 不具合報告（不具合の発生であって健康被害が発生するおそれのあるもの）

	重篤度	使用上の注意等からの予測		報告期限
国内症例	重篤	発生予測不能		30日
		発生予測可能	あらかじめ不具合の発生率が把握できない	30日
			あらかじめ不具合の発生率が把握可能。厚生労働大臣が指定	15日/定期
	非重篤	発生予測不能		定期
		発生予測可能		報告不要
外国症例	重篤	発生予測不能		30日
		発生予測可能	あらかじめ不具合の発生率が把握できない	30日
			あらかじめ不具合の発生率が把握可能	15日/定期報告不要
	非重篤	発生予測不能		報告不要
		発生予測可能		報告不要

(2) 不具合報告(健康被害発生のうち医療機器の不具合による影響であると疑われるもの)

	重篤度		使用上の注意等からの予測		報告期限
国内症例	重篤	死亡	発生予測不能		15日
			発生予測可能		15日
		死亡以外	発生予測不能		15日
			発生予測可能	あらかじめ不具合の発生率が把握できない	15日/30日
				あらかじめ不具合の発生率が把握可能。厚生労働大臣が指定	15日/定期
	非重篤		発生予測不能		定期
			発生予測可能		報告不要
外国症例	重篤	死亡	発生予測不能		15日
			発生予測可能	あらかじめ不具合の発生率が把握できない	30日
				あらかじめ不具合の発生率が把握可能	15日/定期報告不要
		死亡以外	発生予測不能		15日
			発生予測可能	あらかじめ不具合の発生率が把握できない	30日
				あらかじめ不具合の発生率が把握可能	15日/定期報告不要
	非重篤		発生予測不能		報告不要
			発生予測可能		報告不要

また、研究論文等学術的に医療機器の有効性及び安全性に関する重要な情報を得た場合や海外において安全性に関する措置が行われたという情報を得た場合についても、30 日以内報告することとされている。

調査を開始する時点では、常に厳しい期限である 15 日を前提に作業を進めると共に、報告期限内に報告すべき事項の調査が完了しない場合でも、報告期限を厳守する。その場合には、それまでに得られた調査結果を未完了報告とし、発生した事象によりその患者・使用者の受けた、または受けるおそれのある障害のレベルを知りうる範囲で報告する。医療機関側からの報告と齟齬のないことが要求されるが、緊急時における第一報の場合にはその精度は問わない。所定様式の今後の対応欄にその旨記載すると共に、次回報告予定日及び調査完了に時間を要する理由を添えて報告期日までに報告する。後日、正式報告時にはその精度を高めるべく企業は努力すべきである。なお、医療機関側の報告との整合はその時点において取られるべきである。

一般社団法人 日本医療機器産業連合会（医機連）製造販売後調査（PMS）委員会 不具合報告の手引き改訂ワーキンググループ（WG）傘下 サイバーセキュリティの不具合報告サブ WG において、「不具合報告等の手引書 第 8 版」の改訂に向け、サイバーセキュリティの不具合報告の具体的な事例の情報収集及び手引書への追加内容について討議を進めている。

3.1.2 サイバーセキュリティ脆弱性に対する情報収集及び共有体制

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、医療機器のサイバーセキュリティ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[5)]。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[6)]。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、医機連の医療機器サイバーセキュリティ対応 WG 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 厚生労働省より「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「医療機器のサイバーセキュリティ導入に関する手引書(第 2 版)」が示された[7)]。その中で、製造販売業者は、市販前には、医療機器のサイバー攻撃に対する耐性が確保されるよう、設計及び開発を行うと共に、市販後には、意図する使用環境における機器の運用、情報共有、脆弱性の修正、インシデントの対応等を適切に行う必要があることが示されている。また、医療現場においても適正な管理がなされるよう、製造販売業者は、医療機関、使用者、規制当局及び脆弱性発見者等と必要な情報共有等を行い、積極的に連携していくことが求められている。

医療機関における医療機器のサイバーセキュリティに係る対応については、令和 2 年 6 月に厚生労働省より、医薬品・医療機器等安全性情報において、「医療機器のサイバーセキュリティの確保に係る最近の動向について」が取り上げられており[8)]、その中で、医療機器のサイバーセキュリティの確保に関するリスク分析の状況や国際的な動向について、諸外国における分析状況、サイバーセキュリティの対応状況、IMDRF ガイダンスについて、国内における IMDRF ガイダンス導入について紹介されている。また、令和 4 年 3 月 28 日に厚生労働省より「医療機関を標的としたランサムウェアによるサイバー攻撃について(注意喚起)」が発出され[9)]、ランサムウェアによるサイバー攻撃について、攻撃の手口の解説

及び、ランサムウェア攻撃への対策として、具体的な対策例、インシデント対応体制の構築、データ・システムのバックアップ、情報窃取とリークへの対策、医療情報システム等のセキュリティ対策、その他医療機器のサイバーセキュリティ対応に係る留意点が示された。さらに、令和 5 年 3 月 31 日に 厚生労働省より「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 [10]。医療機関からのインシデント発生に関する報告は、厚生労働省医政局特定医薬品開発支援・医療情報担当参事官室、都道府県、医療セプター等に対して行う必要があり、必要に応じて医療機器・ 医療情報システムの保守管理委託先、医療機器事業者等に協力を求める。また、実際に保健衛生上の危害が発生し、又は拡大するおそれかがある場合には医療機器に関する安全性情報として PMDA に報告する必要がある。

厚生労働省が令和 4 年 3 月に発行した「医療情報システムの安全管理に関するガイドライン」[11] では、医療機関等がサイバー攻撃を受けた（疑い含む）場合等の際には、厚生労働省等の所管省庁への連絡等、必要な対応を行うほか、そのための体制を整備する必要があることを示しており、医療機関等がサイバー攻撃を受けた場合等の厚生労働省連絡先（医政局特定医薬品開発支援・医療情報担当参事官室）が定められている [12]。一方で、医療機器に特化したサイバーセキュリティに関する報告窓口は整理されておらず、各企業等の判断によって各窓口への報告や相談が行われている。

実際に発生した不具合等については、医薬品医療機器等法に基づく医療機器不具合等報告制度の中で、PMDA への報告が可能な体制となっている。また、医療機器に関連したサイバーセキュリティ脆弱性が見つかった際に、製造販売業者は、当該医療機器の SBOM 及び設計情報等から脆弱性が存在するソフトウェアの存在、使用の有無及び機能性能に関する影響等を評価し、死亡や重篤な健康被害が発生、また発生するおそれがあると判断した場合には、不具合等の報告を実施する。製造販売業者は、脆弱性に関する情報の収集、評価、報告に関する情報共有体制の構築が必要である。

一方で、製造販売業者が、自社の医療機器の脆弱性情報、他社の医療機器にも関係する脆弱性情報やセキュリティアドバイザリーを開示する場合、その緩和策及び補完的対策が立案できていない状況で開示すれば、即座にサイバー攻撃の標的になってしまうこともあるため、脆弱性情報を開示するタイミングは注意を要する。脆弱性の影響が大きく一般的である場合は、自社の対策だけでなく、場合によっては分野を超えた連携が必要な場合がある。この場合、製造販売業者は、規制当局等と連携して、必要な調整を実施する協調的な脆弱性の開示（CVD：Coordinated Vulnerability Disclosure）のプロセスを確立し実施する。

サイバーセキュリティに関しては、内閣府、経済産業省、警察庁、その他独立行政法人や民間の非営利団体によって積極的な情報収集や関係企業等への情報提供が行われていると共に、サイバー攻撃を受けた場合の対応窓口が紹介されている [13]。サイバーセキュリティに対する国内の各関係機関での取り組み状況を表 2 にまとめた。

表 2　サイバーセキュリティに対する国内の各関係機関での取り組み状況

機関名	属種	サイバー攻撃に対する対応業務
内閣サイバーセキュリティセンター（NISC：National center of Incident readiness and	行政（内閣官房所管）	● サイバーセキュリティ戦略本部の事務局としての役割のほか、行政各部の情報システムに対する不正な活動の監視・分析やサイバーセキュリティの確保に関し必要な助言、情報の提供その他の援助、監査等を行うと共に、サイバーセキュリティの確保に関する総合調整役を担っている。

機関名	属種	サイバー攻撃に対する対応業務
Strategy for Cybersecurity）		• 一般国民向けに、情報セキュリティに関する広報啓発活動として、「サイバーセキュリティ・ポータルサイト」「サイバーセキュリティ関係法令 Q&A ハンドブック」「インターネットの安全・安心ハンドブック」、ランサムウェアへの対応に関するコラム等を公開している [14]。
経済産業省	行政（経済産業省所管）	• サイバーセキュリティ政策として、IT に関するシステムやサービス等を供給する企業及び経営戦略上 IT の利活用が不可欠である企業の経営者を対象に、「サイバーセキュリティ経営ガイドライン」を策定し、関連ツールを公開している。 • ランサムウェアや Emotet をはじめとするサイバー攻撃に対して、サイバーセキュリティ対策に関する注意喚起を行っている [15]。
警察庁	行政（警察庁所管）	• サイバー警察局を設置し、官民連携、人材育成等の基盤整備、各国との情報交換、サイバー事案の捜査指導、高度な解析への技術支援等を推進している。 • 個別事案への対策として、ランサムウェア被害防止対策、Emotet 対策、不正アクセス対策、ウェブサイト改ざん対策、サポート詐欺対策等について情報を公開し、都道府県警察本部のサイバー犯罪相談窓口が設けられている [16] 。
独立行政法人情報処理推進機構（IPA：Information-technology Promotion Agency, Japan）	行政（独立行政法人）	• 情報セキュリティ対策の強化や、優れた IT 人材を育成するための活動を行なっており、IPA 注意喚起情報、IPA コンピュータウイルス・不正アクセスの届出事例、対策情報等を掲載している [17] 。
JPCERT コーディネーションセンター（JPCERT/CC ： Japan Computer Emergency Response Team Coordination Center）	民間非営利団体（一般社団法人）	• 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について、日本国内のインシデント等の報告の受付、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っており、「注意喚起情報」、「インターネット定点観測」、「脆弱性対策情報」、「インターネットリスク可視化サービス」等の情報提供を行っている。 • 情報セキュリティ安心相談窓口では、情報セキュリティ対策に関して、不正ログイン対策特集ページ、ランサムウェア対策特設ページ等を公開し、JPCERT/CC の取組み、被害に遭った場合の対応のポイントや留意点などを FAQ 形式で記載している [18, 19]
日本サイバー犯罪対策センター（JC3：Japan Cybercrime Control Center）	民間非営利団体（一般社団法人）	• サイバー空間の脅威の特定・軽減・無効化に向けた活動を行っており、金融犯罪、情報流出、e コマース、マルウェア等に対する情報を提供し、予防対策、復号ツール等を掲載している [20]。

3.2 主要各国における医療機器に関連したサイバーセキュリティ脆弱性に対する市販後安全対策体制の調査

IMDRF に参加している国の中から米国、カナダ、豪州、欧州、英国の規制当局を対象として、各国における医療機器の不具合等報告制度、医療機器のサイバーセキュリティ脆弱性に着目した市販後安全対

策体制、他機関との連携体制について調査した。なお、米国、EU では、現在、法律改正等が進められている状況であることから、今後もフォローアップが必要である。

3.2.1 米国

(1) 一般的な医療機器不具合等報告制度

米国においては、U.S. Food and Drug Administration（以下「FDA」という。）が医療機器の不具合報告情報を収集している。医療機器の不具合等報告については、Federal Regulations TITLE 21--FOOD AND DRUGS CHAPTER I--FOOD AND DRUG ADMINISTRATION DEPARTMENT OF HEALTH AND HUMAN SERVICES SUBCHAPTER H - MEDICAL DEVICES, PART 803 MEDICAL DEVICE REPORTING[21)]において、医療機器に関する不具合報告手続き等が定められており、米国において医療機器を製造販売する製造販売業者、輸入業者、及び医療機器の使用機関に対し、死亡又は重篤事象、又はこれらに繋がる可能性のある不具合に関する情報を得た場合や、公衆衛生に重大な害を及ぼす不当なリスクを防止するための是正措置を必要とする場合に報告するよう義務づけられている。その重篤性や影響の大きさによって報告期限が定められている。また、患者、医療提供者、介護者からの報告も推奨されており、MedWatch システムを通じて FDA へ報告可能とされている。さらに、FDA へ報告された不具合等報告の内容は、MAUDE システムを通じて公開されている。

表 3 米国における医療機器不具合報告制度

調査項目	概要	
規制当局名	U.S. Food and Drug Administration (FDA)	
医療機器の不具合等報告の関連法律	Federal Regulations TITLE 21--FOOD AND DRUGS, CHAPTER I--FOOD AND DRUG ADMINISTRATION, DEPARTMENT OF HEALTH AND HUMAN SERVICES, SUBCHAPTER H - MEDICAL DEVICES, PART 803 MEDICAL DEVICE REPORTING [21)]	
報告対象（Criteria）	• 死亡又は重篤事象、又はこれらに繋がる可能性のある不具合 • 公衆衛生に重大な害を及ぼす不当なリスクを防止するための是正措置を必要とする場合	
報告者と報告期限	医療機器製造販売業者 [21 CFR 803.20, 803.53]	• 死亡又は重篤事象を引き起こした、または引き起こした可能性がある不具合：FDA へ 10 日以内 • 死亡、重篤事象、死亡や重篤事象を引き起こすおそれのある不具合：FDA へ 30 日以内 • 公衆衛生に重大な害を及ぼす不当なリスクを防止するための改善措置を必要とする場合：FDA へ 5 日以内
	医療機器輸入業者 [21 CFR 803.20]	• 死亡と重篤事象：FDA と製版へ 30 日以内
	医療機器使用者 [21 CFR 803.30, 803.33]	• 死亡：FDA へ 10 日以内 • 重篤事象：製版へ 10 日以内 • 年次報告：毎年 1/1 までに FDA へ
	患者	FDA の医療製品安全性報告プログラム「MedWatch」システムを通じた自主報告 [22)]
	※「不具合報告制度」外にて security 研究者又は企業から直接受け取る場合もある。	

調査項目	概要
不具合等報告情報公開	FDA に報告された不具合報告は、MAUDE データベースにて公開されている。（MAUDE: Manufacturer and User Facility Device Experience）[23]

(2) 医療機器のサイバーセキュリティ脆弱性に着目した市販後安全対策体制

1) 医療機器メーカーに求められている安全対策体制

サイバーセキュリティに関連した医療機器の市販後安全対策に関しては、FDA ガイダンス「Postmarket Management of Cybersecurity in Medical Devices」（2016 年）[24]において、悪用可能性と患者への危害の重大度の関係を考慮した脆弱性評価を行うことが推奨されている。特定された脆弱性の悪用可能性とその患者への危害の深刻度は、患者への危害のリスクを決定するのに役立ち、「制御された」（許容可能な残留リスク）又は「制御されていない」（許容されない残留リスク）のいずれかに分類できるとされている。

また、医療機器のサイバーセキュリティに関する懸念に対処するため、2022 年 3 月に The Protecting and Transforming Cyber Healthcare (PATCH) Act [25]が提案された。当法律では、医療機器メーカーが医療機器を監視し、サイバーセキュリティの脆弱性に対処し、脆弱性の開示を調整するための手順を確立することを含め、最小限のサイバーセキュリティ要件を設定することとされている。PATCH 法案についての審議は止まっており、その代わりに、一部の要求事項が後述するオムニバス法に含まれて成立された。2022 年 12 月 21 日に下院と上院の歳出委員会は、2023 年 9 月 30 日まで政府の資金を維持するオムニバス法案文書を公表した。この文書では、医療機器のセキュリティ要件等の規定が含まれている。オムニバス法案のセクション 3305 には、医療機器製造業者が自社の医療機器が特定のサイバーセキュリティ要件を満たしていることを確認することを要求する文言が含まれている。製造業者は市販後のサイバーセキュリティ上の脆弱性や悪用について、監視、特定、対処する計画を適切な時期に長官に提出しなければならず、これには脆弱性の協調的開示や関連手続きも含まれる。さらに、製造業者は、自社の機器及び関連システムの安全性を確保するためのプロセスを設計・開発しなければならず、これには市販後のアップデートやパッチが含まれる。当法律は、法律の制定から 90 日後に有効になる。本法案は、FDA に対し、医療機器のサイバーセキュリティの向上に関するさらなるガイダンスを発行するよう求めており、政府説明責任局（The Government Accountability Office, GAO）も今年中に報告書を発表する予定である [26]。

また、2022 年 3 月に設立された H.R. 2471 Consolidated Appropriations Act [27] の中で DIVISION Y として示された Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) にて、covered entities（organizations in certain critical infrastructure sectors）に対し、医療機器製造業者がサイバーインシデントの発生を認識してから 72 時間以内に the Department of Homeland Security（国土安全保障省）に報告することが要求されている [28]。

さらに、2022 年 6 月には、医療機器のライフサイクル全体を通じて適切なサイバーセキュリティ要件を導入するための法律「H.R.7667 — 117th Congress (2021-2022)」を制定している [29, 30]。この法の第 808 条では、医療機器のサイバーセキュリティを対象としており、サイバー機器の製造業者は、組織的な脆弱性の開示と手順を含め、市販後のサイバーセキュリティの脆弱性と悪用を適切に監視、特定し、合理的な時間で対処する計画を持たなければならない、としている。また、製造業者は、機器と関連システム　のサイバーセキュリティを確保するプロセスと手順を設計、開発、維持することが求められている。

サイバーセキュリティ脆弱性による医療機器への影響については、FDA のホームページでも情報提供

を行っている[31]。

また、2022 年 11 月には、FDA との契約に基づき、米非営利団体 MITRE が医療機器のサイバーセキュリティインシデントに対処するための実践的な考察を提供するプレイブックの改訂第 2 版を公開している。当プレイブックでは、医療提供組織やその他の関係者が、医療機器に関するサイバーセキュリティインシデントに備えて対応し、機器の有効性を確保し、患者の安全を守るためのフレームワークを概説している[32, 33]。

2) FDA と他機関との連携体制

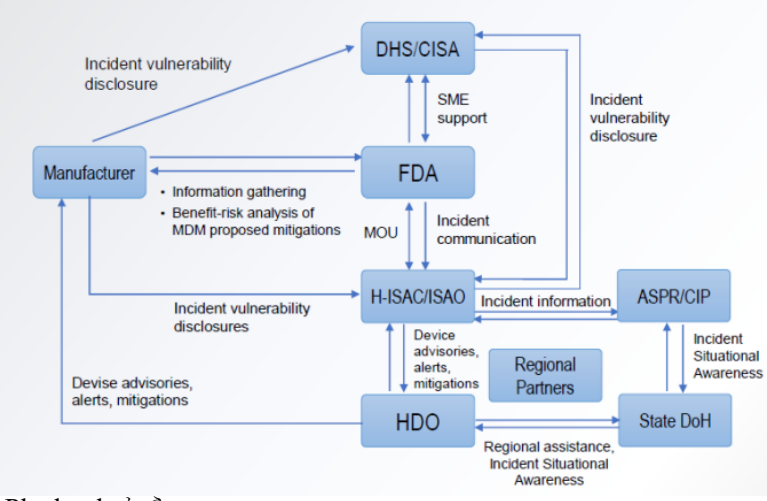
サイバーセキュリティに関しては、FDA ガイダンス「Postmarket Management of Cybersecurity in Medical Devices」（2016 年）によると、2013 年に大統領令により、米国の国家安全保障、経済的安定、公衆衛生と安全を維持するためには、強靭なインフラが不可欠であることや、物理的・サイバー脅威に対する重要インフラのセキュリティとレジリエンスを強化し、脆弱性を軽減し、影響を最小限に抑え、脅威を特定・阻止することを目的とした連邦政府が連携する任務を定めている。FDA と他機関との協力体制については、2015 年に発出された Executive Order - Promoting Private Sector Cybersecurity Information Sharing 13691（以下「EO 13691」という。）[34]において、民間部門及び官民間のサイバーセキュリティ情報共有及び協力のために Information Sharing and Analysis Organizations （ISAOs）の発展を奨励していることが示されている。また、Executive Order 13691 において、ISAO が個人のプライバシーと市民的自由を保護し、ビジネスの機密性を保持し、共有されている情報を保護することを義務付けている。ISAO は、サイバーセキュリティの問題と相互依存性をよりよく理解するために重要なインフラ情報を収集・分析し、サイバーセキュリティの脅威の防止、検知、緩和、影響からの回復を支援するために重要なインフラ情報を伝達・開示し、あるいはサイバーセキュリティの問題の検知と対応に関与するメンバーやその他の関係者に重要なインフラ情報を自発的に伝達する。医療機器に影響を及ぼす脆弱性や脅威を共有する ISAO に製造業者が参加することが推奨されている。FDA は、利害関係者のコラボレーションとコミュニケーションを促進する環境の作成を支援し、医療機器とその周辺の医療 IT インフラストラクチャの安全性、有効性、完全性、及びセキュリティに影響を与える可能性のあるサイバーセキュリティの脅威と脆弱性に関する情報の共有を促進するため ISAO の 1 つである National Health Information Sharing & Analysis Center (NH-ISAC)と覚書を締結した。

現在、FDA が連携している関連機関は下表のとおりである。

表 4 米国での医療機器のサイバーセキュリティ脆弱性等に関する関係機関との連携状況

連携機関	連携状況の概要
National Health Information Sharing & Analysis Center, Inc. (NHISAC) and MediSAO (information sharing analysis organization)（Memorandum of Understanding 205-18-028）	• 利害関係者のコラボレーションとコミュニケーションを促進し、医療機器の安全性、有効性、セキュリティ、及び／又は周囲のヘルスケア IT インフラストラクチャの完全性とセキュリティに影響を与える可能性のあるサイバーセキュリティの脆弱性に関する情報の共有を促進する環境を作成するため、FDA は、サイバーセキュリティの脆弱性と脅威に関する情報を NH-ISAC 及び MedISAO と共有できるメカニズムを確立予定である[35]。 • 当情報共有分析組織の目標は、製造業者に潜在的な脆弱性や新たな脅威に関する情報を FDA と共有する機会を提供し、製造業者がこれらの問題に早期に対処することで患者を保護するのを支援することである。
Health Information Sharing &	• 利害関係者のコラボレーションとコミュニケーションを促進し、医

Analysis Center, Inc. (H-ISAC), formerly known as the National Health Information Sharing & Analysis Center, Inc. (NH-ISAC), and Sensato Critical Infrastructure ISAO（Memorandum of Understanding 225-18-030）	療機器の安全性、有効性、セキュリティ、及び／又は周囲のヘルスケア IT インフラストラクチャの完全性とセキュリティに影響を与える可能性のあるサイバーセキュリティの脆弱性に関する情報の共有を促進する環境を作成するため、FDA は、サイバーセキュリティの脆弱性と脅威に関する情報を H-ISAC 及び Sensato-ISAO と共有できるメカニズムを確立する予定である [36]。 • これらの ISAO の目標は、製造業者に潜在的な脆弱性や新たな脅威に関する情報を FDA と共有する機会を提供し、製造業者がこれらの問題に早期に対処することで患者を保護できるようにすることである。
Department of Homeland Security (DHS)（Memorandum of Understanding 225-19-002）	• 医療機器のサイバーセキュリティを含む医療及び公衆衛生に対する脆弱性及び脅威に関連する情報を共有する際の、役割及び責任を含む両当事者の協力関係を構築する。 • この合意は、潜在的または確認された医療機器のサイバーセキュリティの脆弱性と脅威に関する調整と情報共有を強化するためのフレームワークを実装しています。両機関間のこのコラボレーションは、患者の安全に対する潜在的な脅威に対するより適切でタイムリーな対応につながることを目的としている。



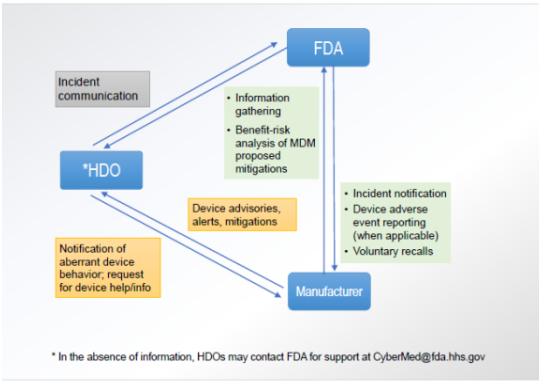


Figure 2. Medical Device Cybersecurity Key Stakeholders Incident Response Interactions

Playbook から
Figure 3. Example of Regional IR Interactions

(3) 実際に発生した事例と対策状況について

FDA は、「Cybersecurity Safety Communications and Other Alerts」[37]において、事例の報告、想定される患者危害、不正アクセスのリスクを軽減するための推奨事項等について、掲載している。

Cybersecurity Safety Communications and Other Alerts の序文において、
「FDA は、各事例において、サイバーセキュリティの事故に関連した患者の負傷や死亡を認識しておらず、臨床で使用されている特定の機器やシステムが意図的に狙われたことも認識していない。しかし、パッチを適用しないまま、あるいはその他の方法で緩和しないまま、これらの脆弱性は、権限のないユーザーが侵害された機器にアクセスし、制御し、コマンドを発行することを可能にし、患者に危害を与える可能性がある。医療施設は、以下に示す安全に関するコミュニケーションやアラートの推奨事項を実施することで、不正アクセスのリスクを軽減することができる。」としている。

以下に、インスリンポンプシステムのサイバーセキュリティリスクに関する報告例を示す。

日付	09/20/2022
安全に関する連絡・注意喚起	Medtronic 社 MiniMed 600 シリーズ インスリンポンプシステムのサイバーセキュリティリスクの可能性について
説明	Medtronic 社 MiniMed 600 シリーズ インスリンポンプシステムの潜在的なサイバーセキュリティリスク FDA は、Medtronic 社 MiniMed 600 シリーズ インスリンポンプシステム (例: MiniMed 630G 及び MiniMed 670G) のサイバーセキュリティリスクについて医療機器ユーザーに警告を発している。 ポンプシステムの通信プロトコルに関連する問題があり、ポンプシステムへの不正アクセスを許す可能性がある。不正アクセスが発生した場合、ポンプの通信プロトコルが侵害され、ポンプのインスリン投与量が過多または過少となる可能性がある。ミニメド 600 シリーズポンプシステムには、無線通信を行うコンポーネント（インスリンポンプ、連続グルコースモニタリング（CGM）トランスミッタ、血糖測定器、ケアリンク USB デバイスなど）がある。不正アクセスが発生するためには、ポンプが他のシステムコンポーネントとペアリングされている間に、近くにいる不正アクセス者（あなたやあなたのケアパートナー以外の人）があなたのポンプにアクセスする必要がある。 FDA は、このサイバーセキュリティの脆弱性に関連する報告を認識していない。 Medtronic 社は、このサイバーセキュリティのリスクについて医療機器ユーザーに知らせるため、緊急医療機器修正（Urgent Medical Device CorrectionExternal Link Disclaimer）を発表し、ユーザーが取るべき行動と推奨事項を示した。 FDA は、このサイバーセキュリティの脆弱性に関連する有害事象を特定し、伝達し、防止するためにメドトロニック社と協働している。FDA は、重要な新情報が入手できた場合、一般市民に情報を提供する。 このサイバーセキュリティリスクに関する追加的な質問については、医療機器ユーザーはメドトロニック社（1-800-646-4633）に問い合わせる必要がある。

3.2.2 カナダ

(1) 一般的な医療機器不具合等報告制度

カナダにおいては、Health Canada （以下「HC」という。）が医療機器の不具合等情報を収集しており、Medical Devices Regulations （SOR/98-282）の 57 条にて、製造業者、輸入業者、販売業者は苦情報告の調査及び時宜を得たリコールが義務付けられている。また、同 59 条において、機器の故障、有効性の低下、またはラベル表示や使用説明書の不備に関連する事象及び患者、使用者、又はその他の人の死亡又は健康状態の深刻な悪化につながった場合、又はそのおそれがある事象について、大臣へのインシデント報告が義務づけられている。消費者等からの報告も推奨されており、MedEffect カナダにて報告が可能となっている [38]。なお、HC に報告された事象については公開されていないが、実施された Recall については公開されている [39]。

表 5　カナダにおける医療機器不具合等報告制度

調査項目	概要
規制当局名	Health Canada (HC)
医療機器の不具合等報告の関連法律	Food and Drugs Act (R.S.C., 1985, c. F-27) [40)] Medical Devices Regulations (SOR/98-282) [41)]
報告対象（Criteria）	• 機器の故障、有効性の低下、またはラベル表示や使用説明書の不備に関連する事象 • 患者、使用者、又はその他の人の死亡又は健康状態の深刻な悪化につながった場合、又はそのおそれがある事象
報告者と報告期限	製造業者、輸入業者： 死亡又は深刻な健康被害の悪化：10 日以内に速報を提出 死亡又は深刻な健康被害の悪化のおそれ：30 日以内に Preliminary report を提出 Preliminary report にて調査及び final report のスケジュールを示し、そのスケジュールまでに最終報告を提出。 病院： 医療機器事故が発生した場合：30 日以内 特別なアクセスのための医療機器（緊急使用等）については、認可を申請した医療専門家が事故に気付いてから 72 時間以内
不具合等報告情報公開	なし

(2)　医療機器のサイバーセキュリティ脆弱性に着目した市販後安全対策体制

カナダのサイバーセキュリティについては、Communications Security Establishment の一組織である Canada Centre for Cyber Security が一元的に監督している。ネットワークに接続する医療機器のサイバーセキュリティについては、2021 年 11 月にガイダンス [42)]が提供されている。当該ガイダンスにおいて、医療機器メーカーに対してはリスク管理、設計段階におけるサイバーセキュリティのコントロール、製品の検証、脆弱性の監視、クラウドの保護等が推奨されている。HC はサイバーセキュリティに関する市販前要件についてはガイダンス [43)]を提供しているが、不具合等報告を含む市販後安全対策については特にガイダンスを示しておらず、サイバーセキュリティ一般に関するインシデントの報告先は Canada Centre for Cyber Security となっている。GC CSEMP（Government of Canada Cyber Security Event Management Plan）Primary レポートはできるだけ早く、発見から 1 時間を超えないようにすること、詳細なレポートは発見から 24 時間以内に報告することとされている。HC と Canada Centre for Cyber Security の連携状況については、情報が得られなかった。

3.2.3　豪州

(1)　一般的な医療機器不具合等報告制度

豪州においては、Therapeutic Goods Administration （以下「TGA」という。） が医療機器に関する不具合等情報を収集している。医療機器の不具合等報告については、Therapeutic Goods (Medical Devices) Regulations 2002）[44)]において報告対象等が定められており（5.7　Conditions applying automatically—period for giving information about adverse events etc (Act s 41FN)）、豪州において医療機器を製造販売する企業に対し、特に、死亡又は重篤事象、予期しない事象や公衆衛生に重大な脅威を与える事象等について報告するよう義務づけられている。その重篤性や影響の大きさによって報告期限が定められてい

る。また、消費者や医療従事者からの報告も推奨されており、consumer online Medical Device Incident Report form[45]や health professional online Medical Device Incident Report form [46]を通じて TGA へ報告可能とされている。なお、TGA に報告された不具合等報告は、Database of Adverse Event Notifications (DAEN) [47]にて公開されている。また、Recall についても公開されている [48] 。医療機器の不具合等報告制度ついては以上のように定められているが、サイバーセキュリティに関連した場合も通常の不具合等報告が適用されるかについては言及されていない。

表 6　豪州における医療機器不具合等報告制度

調査項目	概要
規制当局名	Therapeutic Goods Administration (TGA)
医療機器の不具合等報告の関連法律	Therapeutic Goods (Medical Devices) Regulations 2002 [49]
不具合等報告の対象（Criteria）	有害事象などに関する情報提供期間（Act s 41FN） (a)公衆衛生に対する深刻な脅威を表すイベントまたはその他の出来事に関連している場合：48 時間以内 (b)患者、デバイスのユーザー、または他の人物の死亡、または深刻な健康状態の悪化につながった出来事またはその他の出来事に関連している場合：10 日以内 (c)患者、デバイスのユーザー、または他の人物の死亡または深刻な健康状態の悪化につながる可能性のある事象またはその他の出来事に関連している場合：30 日以内 (d) その他：60 日以内 Report an adverse event for medical devices | Therapeutic Goods Administration (TGA) Meet your ongoing responsibilities as a medical device sponsor | Therapeutic Goods Administration (TGA) [50]
報告者	企業、医療機関、患者
不具合等報告情報公開	Database of Adverse Event Notifications (DAEN) [51]

(2)　医療機器のサイバーセキュリティ脆弱性に着目した市販後安全対策体制

通常の不具合報告とは別ルートにて、医療機器がサイバーセキュリティの問題の影響を受け、健康と安全に直接影響を与える可能性がある場合に使用者が連絡できる TGA の連絡先が用意されていると共に、悪意のあるサイバーセキュリティ事象については、Australian Cyber Security Centre (ACSC) のホットラインにも報告できるように体制が整えられている [52] 。また、注目すべき脆弱性と問題に関連した警告については TGA のホームページにて公開されている [53]。

企業に対しては、2022 年 11 月にガイダンスが発行されており [54]、Total product life cycle (TPLC) アプローチに基づいたリスク評価と管理に関する基本的な要求事項が周知されている。

3.2.4 欧州

(1)　一般的な医療機器不具合等報告制度

欧州においては、EU 各加盟国において医療機器に関する不具合等情報を収集している。基本的に欧州の Regulation (EU) 2017/745 [55]にて医療機器に関する不具合報告手続き等が定められており、欧州各国において医療機器を製造販売する企業や医療機器の使用機関に対し、死亡又は重篤事象、又はこれらに繋

がる可能性のある不具合に関する情報を得た場合や、公衆衛生に重大な害を及ぼす不当なリスクを防止するための是正措置を必要とする場合に報告するよう義務づけられている。報告すべき事象は、死亡・重篤事象、又はこれらに繋がる可能性のある不具合、公衆衛生に重大な害を及ぼす不当なリスクを防止するための是正措置を必要とする事象であり、その重篤性や影響の大きさによって報告期限が定められている。

表 7　欧州における医療機器不具合等報告制度

調査項目	概要
規制当局名	European Medicines Agency (EMA) 及び EU 参加各国規制当局
医療機器の不具合等報告の関連法律	Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (Text with EEA relevance.)[55]
不具合等報告の対象（Criteria）	a) 深刻なインシデントの理解または評価に影響を与える可能性のある関連情報（情報の漏洩、情報の脅威など）を含む、深刻なインシデントの記述。 b) 健康影響（該当する場合)、すなわち臨床徴候、症状、状態及び全体的な健康影響の記述。 製造業者は、IMDRF コードを使用してインデックスを作成 • インシデントに関わる機器の問題。 • 関連する健康への影響。 • サイバーセキュリティ関連のインシデントの根本原因。 （MDCG 2019-16 Guidance on Cybersecurity for medical devices 5.2）[56]
不具合等報告の報告期限	重大なインシデントの定義 • 事業体に重大なサービス運営上の混乱や経済的損失を引き起こすもの。 • 他の自然人又は法人に影響を与えるもの。 報告の流れ • 重大なインシデントを認識してから 24 時間以内に早期警告を行う。 • 重大なインシデントを認識してから 72 時間以内に、上記の早期警告の情報を更新し、 重大なインシデントの重大度・影響・侵害の兆候などについての初期評価を行うためのインシデント通知を行う。 • インシデント通知後 1 か月以内に、インシデントの重大度・影響についての詳細、根本原因、緩和策、国外への影響を含む最終報告書を提出する。 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148」（NIS 2 Directive）[57]
報告者	企業、医療機関、患者
不具合等報告情報公開	なし

(2)　医療機器のサイバーセキュリティ脆弱性に着目した市販後安全対策体制

医療機器のサイバーセキュリティについては、2019 年 12 月に「MDCG 2019-16 Guidance on

Cybersecurity for medical devices」[58]が発行されており、当文書の「5. Post-Market Surveillance and Vigilance」にて市販後対策について述べられているが、従来の医療機器の安全対策体制の中でサイバーセキュリティに関連した事象についても同様に情報収集や市販後対応を行うことが述べられている。

また、European Commission（以下「EC」という。）は、2022 年 9 月にインターネットに接続される機器がサイバーセキュリティの基準を満たすことを製造業者に義務付けた新たな法案「Cyber Resilience Act」[59]を提案した。本法案は、十分に保護されていないデジタル要素を持つすべての製品を EU 市場から排除することを目的としており、デジタル製品を上市する際のルール、製品におけるサイバーセキュリティに関する要求事項、製造業者に課される脆弱性対応の要求事項、当該要求事項への順 守を担保するための市場監督者へのルールが規定されている。製造業者は機器の設計・開発においてサイバーセキュリティを考慮する必要があり、予想される製品の耐用年数（最低 5 年間）は製品のセキュリティに責任を負うことになる[60]。

では以下に示すような内容が求められている。

a. デジタル製品に関する要求事項が含まれており、適用範囲が広い。
  i. 24 時間以内に「悪用された脆弱性」を報告する
    1. 脆弱性が「積極的に悪用」された場合
    2. インシデント
      報告要件に近い
  ii. 悪用可能な既知の脆弱性がない状態で提供される製品
  iii. 最低 5 年間はソフトウェアアップデートを無償で提供すること
  iv. ドキュメントは 10 年間保存されなければならない
  v. セキュリティリスク情報の一般公開
  vi. 一般に公開される実装情報（SBOM を含む）の提供
  vii. 1500 万ユーロ又は世界売上高の 2.5%の罰金。どちらか大きい方
b. MDR の対象製品に除外規定がある。ただし、MDM が作成する可能性のあるもの（例えば SaMD）は必ずしもすべて対象とはならない。
c. 記載されている要件は、他の規制や法律における既存の要件と整合していると思われる。
d. 電子カルテが具体的に記載されている（MDR には該当しない）。
e. この法律を無視することはできないが、MDR が優先される場合は MDR に従う。

表：Cyber Resilience Act法案の要件概要　（情報源：PwCオーストリアの調査結果より）

経過措置		24か月		12か月	24か月	24か月			24か月
義務者		ANNEX I：サイバーセキュリティ必須要件 デジタル要素を含む製品は、設計開発、製造、保守などにおいて特定要件を満たす必要あり		11条：ENISAに対する報告 1.悪用される脆弱性 2.製品のセキュリティに影響するインシデントを知り得てから24時間内	ANNEX V：技術文書 サイバーセキュリティリスク評価を含む	ANNEX VI：適合性評価手順 以下いずれかのモジュールによる			EUサイバーセキュリティ認証フレームワーク (EU) 2019/881 (CSAのこと) による
経済事業者	製品分類	セキュリティ要件	脆弱性管理			(モジュールA) 内部統制手順	(モジュールB) EC 型式審査証明書	(モジュールC) 完全な品質保証	
製造者	デジタル要素を含む製品	●	●	●	●	●	●	●	
	ANNEX IIIクラスIのデジタル要素を含む重要な製品（更新あり）	●	●	●	●		●	●	
	ANNEX IIIクラスIIのデジタル要素を含む重要な製品（更新あり）	●	●	●	●		● (第三者参加必須)	● (第三者参加必須)	
	特定していないデジタル要素を含む高度重要な製品（更新あり）	●	●	●	●		●	●	●
輸入者	すべての製品について、ANNEX Iの要件の実装、適合性評価の実施、技術文書を確認してください。輸入業者が製品のデジタル コンポーネントに変更を加えた場合、製造業者と見なされます。								
販売者	すべての製品について、製品の適合性、エンド ユーザー ドキュメントを確認してください。 輸入業者が製品のデジタル コンポーネントに変更を加えた場合、製造業者と見なされます。								

さらに、EC は 2022 年 12 月に、NIS（ネットワーク情報システム）指令の改訂案（NIS 2）[58]を発表し、2024 年 10 月 18 日より施行予定である。NIS 2 での変更点は、1）大幅な対象の拡大（EU 内でサービスを提供する又は活動を行う中規模(従業員 50 名)以上の主要法人又は重要法人。医療機器分野も対象。）、2）サイバーセキュリティ・リスクマネジメントの強化、3）インシデント報告内容・時限の明確化（24 時間以内に早期警告、72 時間以内にインシデント通知。）、4）厳しい罰則金（違反した場合には、売上げの最大２％又は 1000 万ユーロの罰金。）である。

3.2.5　英国

(1)　一般的な医療機器不具合等報告制度

英国においては、Medicines and Healthcare products Regulatory Agency (MHRA)が医療機器に関する不具合等情報を収集している。医療機器の不具合等報告については、MEDDEV 2.12/1 rev 8 Guidelines on a medical devices vigilance system[61]において報告対象等が定められており、英国において医療機器を製造する製造業者、英国責任者、及び北アイルランドを拠点とする認定代理人に対し、死亡又は重篤事象、又はこれらに繋がる可能性のある不具合に関する情報を得た場合、MHRA に報告するよう義務づけられている。報告すべき事象は、死亡・重篤事象、又はこれらに繋がる可能性のある不具合等であり、その重篤性や影響の大きさによって報告期限が定められている。また、患者や医療提供者等からの報告も推奨されており、Yellow Card システム [62]を通じて MHRA へ報告可能とされている。なお、MHRA へ報告された不具合等情報は公開されていない。

表 8　英国における医療機器不具合等報告制度

調査項目	概要
規制当局名	Medicines and Healthcare products Regulatory Agency (MHRA)
医療機器の不具合等報告の関連法律	MEDDEV 2.12/1 rev 8 [61)] Guidelines on a medical devices vigilance system
不具合等報告の対象（Criteria）	以下の 3 つの報告基準をすべて満たす事象は有害事象とみなされ、MHRA に報告する必要がある。 • 事象が発生した。機器に対して行われた試験、機器に付属する情報の検討、または科学的な情報が事象につながる可能性がある、またはつながった何らかの要因を示している状況が含まれる。 • 製造者の機器が事象の一因であることが疑われる場合。 • 患者、ユーザーまたはその他の人の死亡または健康状態の深刻な悪化につながった、またはつながった可能性がある事象。 すべての有害事象が死亡または深刻な健康状態の悪化につながるわけではない。これらは、他の状況や介入によって防げた可能性がある。以下のような場合でも報告書を送付する必要がある。 • 機器に関連した事故が発生した場合、かつ • 再発した場合、死亡または重大な健康状態の悪化につながる可能性がある。 MEDDEV 2.12/1 rev 8　5.1.1[61)]
不具合等報告の報告期限	1)　医療機器企業 • 重大な公衆衛生上の脅威：2 日以内 • 死亡または予期せぬ深刻な健康状態の悪化：10 日以内 • その他：30 日以内 2)　患者 Yellow Card | Making medicines and medical devices safer (mhra.gov.uk) [62)]
報告者	• 製造業者（義務） • 英国責任者（義務） • 北アイルランドを拠点とする認定代理人（義務） • 患者 Medical devices: guidance for manufacturers on vigilance - GOV.UK (www.gov.uk) [63)]
不具合等報告情報公開	無し

(2)　サイバーセキュリティに特化した医療機器不具合等報告制度

2022 年 6 月に発行された Government response to consultation on the future regulation of medical devices in the United Kingdom [64)]において、Software as a medical device (SaMD) の規制の在り方について示唆されており、サイバーセキュリティについても必須要件とすべきと提言されている。当提言を踏まえ、2022 年 10 月に発行された Software and AI as a Medical Device Change Programme の WP 5 Cyber Secure Medical Devices [65)]にて、サイバーセキュリティと IT 要件を課すための二次的な法律を策定することが予定されている。この二次立法では、コネクテッド医療機器セキュリティ運営グループの原則と整合性をとること、文化・メディア・スポーツ省の製品セキュリティ及び電気通信インフラストラクチャ法案、NHS(国民保健サービス）DCB(データ調整委員会)基準、NHS デジタルテクノロジー評価基準要件などの補完的な要件と一致し、それに基づいて構築すること、国際的なベストプラクティスと調

和していることとしている。また、医療機器と IVD のサイバーセキュリティ及び関連する要件に関するガイダンス、及び、サポート対象外のソフトウェアデバイスの管理に関するガイダンスの作成が予定されており、医療機器に関連するサイバーセキュリティの脆弱性に関する報告体制についても構築を進めようとしている。

さらに、医療機器ソフトウェアに関する申請ガイダンス[66]内 Appendix 4 にて Field Safety Warnings and End-of-Life notification[67]についても言及されている。

3.2.6 まとめ

1) 不具合報告等制度

一般的な医療機器不具合等報告制度については、調査した米国、カナダ、豪州、欧州、英国の各国において、本邦と同様に、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。

一方、医療機器のサイバーセキュリティに関連した不具合報告については、カナダと豪州において一般的な不具合報告制度と区別して報告できる体制が整えられていたが、その後の情報伝達、情報共有等に関する連携についての情報は得られなかった。

2) 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

特に、米国、カナダ、豪州においてはサイバーセキュリティ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提供を行う仕組みが整えられていた。さらに、米国においては、医療機器を所管する FDA と、サイバーセキュリティに関する情報を管理している連携機関と間で、情報共有体制を確立予定であることが確認された。

また、欧州、英国においても、サイバーセキュリティに関連した事象について、情報収集や市販後対応を目指して、法案の改定や体制の構築を進めようとしている。

4. 考察

「3. 調査結果」項での国内外におけるサイバーセキュリティに関連した医療機器不具合等報告制度や情報収集体制に関する調査結果を踏まえ、国内における医療機器のサイバーセキュリティ脆弱性に対する安全対策のあり方について考察した。

4.1 現在の医療機器不具合報告制度における情報収集体制と限界

本邦における現在の医療機器の不具合報告は、医薬品医療機器等法 第 68 条の 10 第 1 項及び施行規則第 228 条の 20 第 2 項に従い実施されている。この不具合は、医療機器全てに関わるもので、サイバーセキュリティも含まれることになる。

不具合等報告書は、報告期限内に、PMDA 医療機器品質管理・安全対策部医療機器安全課に提出する。なお、国内死亡症例についての全ての症例並びに外国医療機器に係る製造、輸入又は販売の中止等保健衛生上の危害の発生又は拡大を防止するための措置が講じられた場合の全ての措置内容について、PMDA 医療機器品質管理・安全対策部医療機器安全課に対し、ファックス等により速やかに第一報の報告をする。報告期限には、生じた健康被害の重篤性に応じて情報入手日からの 15 日、30 日、定期がある。

しかしながら、サイバーセキュリティに関する不具合報告については、これまでに報告例がないこと

から、健康被害の重篤度の判断が難しいと考えられ、的確な情報収集の実施に向けて、医機連 PMS 委員会 不具合報告の手引き改訂 WG 傘下 サイバーセキュリティの不具合報告サブ WG において、「不具合報告等の手引書 第 8 版」の改訂に向け、サイバーセキュリティの不具合報告の具体的な事例の情報収集及び手引書への追加内容について討議を進めている。

4.2 医療機器のサイバーセキュリティ脆弱性に対する安全対策のあり方

サイバーセキュリティを含めた医療機器の不具合報告制度については、各国において類似のクライテリア下にて報告制度が整えられていた。一方、サイバーセキュリティによる医療機器不具合に対して、製造販売業者が、医療機器の脆弱性について広く情報収集し、企業が情報を得てから短期間で行政機関へ情報提供を行う仕組みや、関係機関間で情報を共有し、脆弱性に対応する仕組みが整えられつつある様子が確認できた。これは、一般的な医療機器不具合と異なるサイバーセキュリティ脆弱性の特長を考慮した体制と想定される。従来の医療機器不具合報告制度では、医療機器に重篤な健康被害に繋がる又は繋がる恐れのある何らかの不具合が確認された場合、又は、患者や医療機器の使用者に対する重篤な健康被害等が確認された場合に症例報告の対象とされているが、医療機器のサイバーセキュリティ脆弱性がある場合に、実際に医療機器の不具合や健康被害に繋がるケースが限られていること、また、一般的な医療機器不具合に比べてサイバーセキュリティ脆弱性が医療機関や医療機器に与える影響が広範囲であることから、脆弱性が見つかった場合に、製造販売業者から迅速に特定のサイトへ報告し、行政機関や医療機関へその情報が伝達され、関係者間での情報共有ができるような体制を整えることが求められていた。カナダと豪州においては、サイバーセキュリティによる医療機器不具合に対する特別な報告先が整備されており、その他の国においても体制を整える準備が進められていた。

国内においても、内閣府、経済産業省、警察庁、その他独立行政法人や民間の非営利団体によって積極的な情報収集や関係企業等への情報提供が行われていることが確認されたが、医療機器に関する不具合情報等を管理している厚生労働省や PMDA と、その他機関との間に情報共有を行う仕組みは確認できなかった。以上の各国の取り組みを考慮すると、国内における医療機器のサイバーセキュリティ脆弱性に対する安全対策として、従来の不具合報告制度上において、サイバーセキュリティ脆弱性による医療機器の不具合や健康被害が見つかった場合の報告対象の考え方を整理する必要がある。また、医療機器に関連したサイバーセキュリティ脆弱性が見つかった際に、製造販売業者は、当該医療機器の SBOM 及び設計情報等から脆弱性が存在するソフトウェアの存在、使用の有無及び機能性能に関する影響等を評価し、不具合報告の要否について判断し、必要に応じて不具合等の報告を実施する。したがって、企業内においては、脆弱性に関する情報の収集、評価、報告体制が構築され、具体的な対応手順等が明確化される必要がある。

5. 結語

本調査では、国内における従来の医療機器の不具合等報告制度及び、サイバーセキュリティ脆弱性に対する各関係機関での取り組み状況について確認すると共に、海外での医療機器に関連したサイバーセキュリティ脆弱性に対する市販後安全対策体制について調査し、国内において求められる製造販売業者を中心とした市販後安全対策体制について考察した。サイバーセキュリティを含めた医療機器の不具合報告制度については、各国において類似のクライテリア下にて報告制度が整えられていた。一方、サイバーセキュリティによる医療機器不具合に対して、製造販売業者が、医療機器の脆弱性について広く情報収集し、企業が情報を得てから短期間で行政機関へ情報提供を行う仕組みや、関係機関間で情報を共

有し、脆弱性に対応する仕組みが整えられつつある様子が確認できた。国内においても同様な体制の構築が望まれる。

【参考文献】

1) N60「Principles and Practices for Medical Device Cybersecurity」
https://www.imdrf.org/documents/principles-and-practices-medical-device-cybersecurity

【日本】

2) 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
https://elaws.e-gov.go.jp/document?lawid=335AC0000000145

3) 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施行規則
https://elaws.e-gov.go.jp/document?lawid=336M50000100001_20230428_505M60000100075

4) 医薬品等の副作用等の報告について 厚生労働省
https://www.pmda.go.jp/files/000160021.pdf

5）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
https://www.mhlw.go.jp/web/t_doc?dataId=81aa6953&dataType=0&pageNo=1

6) 医療機器の基本要件基準第 12 条第 3 項の適用について 厚生労働省
https://www.mhlw.go.jp/hourei/doc/tsuchi/T230404I0010.pdf

7）医療機器のサイバーセキュリティ導入に関する手引書の改訂について 厚生労働省
https://www.mhlw.go.jp/hourei/doc/tsuchi/T230404I0050.pdf

8）医療機器のサイバーセキュリティの確保に係る最近の動向について　厚生労働省
医薬品・医療機器等安全性情報ン No.373,
https://www.pmda.go.jp/files/000235278.pdf

9）医療機関を標的としたランサムウェアによるサイバー攻撃について(注意喚起) 厚生労働省
https://www.pref.kagawa.lg.jp/documents/36326/20221115002.pdf

10）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　厚生労働省
https://www.mhlw.go.jp/hourei/doc/tsuchi/T230404G0080.pdf

11) 医療情報システムの安全管理に関するガイドライン 厚生労働省 令和 4 年 3 月
https://www.mhlw.go.jp/stf/shingi/0000516275_00002.html

12) 医療分野のサイバーセキュリティ対策について 厚生労働省
https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryou/iryou/johoka/cyber-security.html

13) NISC 内閣サイバーセキュリティセンター
https://www.nisc.go.jp/tokusetsu/stopransomware/index.html

14) ランサムウエアによるサイバー攻撃に関する注意喚起について
内閣官房内閣サイバーセキュリティセンター 2021 年 4 月 30 日
https://www.nisc.go.jp/pdf/policy/infra/ransomware20210430.pdf

15) サイバーセキュリティの取組の強化に関する注意喚起 経済産業省 2020 年 12 月 18 日
https://www.meti.go.jp/press/2020/12/20201218008/20201218008.html

16) ランサムウェア被害防止対策
警察庁

https://www.npa.go.jp/cyber/ransom/index.html
17）ランサムウェア対策特設ページ
独立行政法人情報処理推進機構 セキュリティセンター　2022 年 11 月 11 日
https://www.ipa.go.jp/security/anshin/ransom_tokusetsu.html
18）ランサムウエア対策特設サイト
一般社団法人 JPCERT コーディネーションセンター　2022 年 10 月 06 日
https://www.jpcert.or.jp/magazine/security/nomore-ransom.html
19) 侵入型ランサムウェア攻撃を受けたら読む FAQ　JPCERT/CC
https://www.jpcert.or.jp/magazine/security/ransom-faq.html
20）ランサムウェア対策について
一般財団法人 日本サイバー犯罪対策センター
https://www.jc3.or.jp/threats/topics/article-375.html
【米国】
21) TITLE 21--FOOD AND DRUGS CHAPTER I--FOOD AND DRUG ADMINISTRATION DEPARTMENT OF HEALTH AND HUMAN SERVICES SUBCHAPTER H - MEDICAL DEVICES PART 803MEDICAL DEVICE REPORTING：FDA　Jan 17, 2023
https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=803&showFR=1
22）The FDA Safety Information and Adverse Event Reporting Program
https://www.fda.gov/safety/medwatch-fda-safety-information-and-adverse-event-reporting-program
23）About Manufacturer and User Facility Device Experience (MAUDE)
MAUDE: Manufacturer and User Facility Device Experience
24）Postmarket Management of Cybersecurity in Medical Devices , December 28, 2016.
https://www.fda.gov/media/95862/downloadd
25）H.R.7084 -PATCH Act of 2022
https://www.congress.gov/bill/117th-congress/house-bill/7084/text
26）Hearth It Security
https://healthitsecurity.com/news/key-medical-device-security-provisions-included-in-omnibus-bill
27）H.R.2471 - Consolidated Appropriations Act, 2022
https://www.congress.gov/bill/117th-congress/house-bill/2471/text
28）FDA Updates Guidance on Cybersecurity Responsibilities for Medical Device Manufacturers, May 11, 2022
https://www.ropesgray.com/en/newsroom/alerts/2022/may/fda-updates-guidance-on-cybersecurity-responsibilities-for-medical-device-manufacturers
29）Legislation that focuses on enhancing medical device cybersecurity passes in US House ,　JUNE 15, 2022
https://industrialcyber.co/regulation-standards-and-compliance/legislation-that-focuses-on-enhancing-medical-device-cybersecurity-passes-in-us-house/
30）H.R.7667 - Food and Drug Amendments of 2022 117th Congress (2021-2022)
https://www.congress.gov/bill/117th-congress/house-bill/7667
31）FDA Cybersecrity playbook
https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity#safety
32）MITRE releases medical device cybersecurity regional incident preparedness, response playbook NOVEMBER

16, 2022
https://industrialcyber.co/medical/mitre-releases-medical-device-cybersecurity-regional-incident-preparedness-response-playbook/
33）Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook
https://www.mitre.org/news-insights/publication/medical-device-cybersecurity-regional-incident-preparedness-and-response
34）The White House Office of the Press, Secretary Executive Order -- Promoting Private Sector Cybersecurity Information Sharing, February 13, 2015
https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari
35）MOU 225-18-028 ; Memorandum of Understanding Between the National Health Information Sharing & Analysis Center, Inc. (NH-ISAC), Medisao and the U.S. Food and Drug Administration Center for Devices and Radiological Health
https://www.fda.gov/about-fda/non-profit-and-other-mous/mou-225-18-028
36）MOU 225-18-030 ; Memorandum of Understanding Between the National Health Information Sharing & Analysis Center, Inc. (NH-ISAC), Medisao and the U.S. Food and Drug Administration Center for Devices and Radiological Health
https://www.fda.gov/about-fda/non-profit-and-other-mous/mou-225-18-030
37）Cybersecurity Safety Communications and Other Alerts
https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity#safety
【カナダ】
38）Government of Canada ; Report a medical device problem
https://www.canada.ca/en/health-canada/services/drugs-health-products/medeffect-canada/adverse-reaction-reporting/medical-device.html
39）Find recalls, advisories and safety alerts.
https://recalls-rappels.canada.ca/en
40）Food and Drugs Act (R.S.C. (Revised Statutes of Canada), 1985, c. F-27)
Food and Drugs Act (R.S.C., 1985, c. F-27
41）SOR/98-282 › Medical Devices Regulations (Canada)
Medical Devices Regulations (SOR/98-282)
42）CYBER SECURITY FOR CONNECTED MEDICAL DEVICES : Canadian Center for Cyber Security
https://cyber.gc.ca/sites/default/files/cyber/2021-11/ITSAP00132_e.pdf
43）Government of Canada , Guidance Document: Pre-market Requirements for Medical Device Cybersecurity Date adopted: 2019/06/17 Effective date: 2019/06/26
https://www.canada.ca/en/health-canada/services/drugs-health-products/medical-devices/application-information/guidance-documents/cybersecurity.html
【豪州】
44）Therapeutic Goods (Medical Devices) Regulations 2002
https://www.legislation.gov.au/Series/F2002B00237
45）consumer online Medical Device Incident Report form [Text→Word]]

https://apps.tga.gov.au/prod/MDIR/UDIR03.aspx?mode=CON&sid=-139515364
46）health professional online Medical Device Incident Report form [Text→Word]]
https://apps.tga.gov.au/prod/MDIR/UDIR03.aspx?mode=HCP&sid=-1569525987
47）Database of Adverse Event Notifications (DAEN) , Last updated: 16 February 2023
https://www.tga.gov.au/safety/safety/safety-monitoring-daen-database-adverse-event-notifications/database-adverse-event-notifications-daen#daen-devices
48）Recall actions database, Last updated: 30 June 2022
https://www.tga.gov.au/recall-actions-database
49）Therapeutic Goods (Medical Devices) Regulations 2002
https://www.legislation.gov.au/Series/F2002B00237
50）Therapeutic Goods (Medical Devices) Regulatisons 2002
https://www.legislation.gov.au/Details/F2023C00032/DownloadReport an adverse event for medical devices | Therapeutic Goods Administration (TGA)Meet your ongoing responsibilities as a medical device sponsor | Therapeutic Goods Administration (TGA)
51）Database of Adverse Event Notifications (DAEN)
https://www.tga.gov.au/safety/safety/safety-monitoring-daen-database-adverse-event-notifications/database-adverse-event-notifications-daen#daen-devices
52）Report potential cyber security issues ; Consumers, 24 November 2022
https://www.tga.gov.au/resources/publication/publications/medical-device-cyber-security-information-users/report-potential-cyber-security-issues
53）Apache Log4j - Cybersecurity vulnerabilities Published: 22 December 2021
https://www.tga.gov.au/news/safety-alerts/apache-log4j-cybersecurity-vulnerabilities
54）Medical device cyber security guidance for industry Version 1.2, November 2022
https://www.tga.gov.au/sites/default/files/medical-device-cyber-security-guidance-industry.pdf
【欧州】
55）Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (Text with EEA relevance.)
https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=uriserv:OJ.L_.2017.117.01.0001.01.ENG
56）MDCG 2019-16 Guidance on Cybersecurity for medical devices December 2019
https://ec.europa.eu/docsroom/documents/41863
57）Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148
https://www.nis-2-directive.com/
58）EU Wants to Toughen Cybersecurity Rules for Smart Devices
https://www.securityweek.com/eu-wants-toughen-cybersecurity-rules-smart-devices
59）Cyber Resilience Act
https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act
60）欧州サイバーレジリエンス法案（EU Cyber Resilience Act）概説～日本の製 造業への影響と最低限

押さえるべき要点 ～ 2022-10-21
https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/eu-cyber-resilience-act.html
【英国】
61）GUIDELINES ON A MEDICAL DEVICES VIGILANCE SYSTEM
MEDDEV 2.12/1 rev 8
62）Yellow Card, Making medicines and medical devices safer
Yellow Card | Making medicines and medical devices safer (mhra.gov.uk)
63）Medical devices: guidance for manufacturers on vigilance
Medical devices: guidance for manufacturers on vigilance - GOV.UK (www.gov.uk)
64）Government response to consultation on the future regulation of medical devices in the United Kingdom 26 June 2022
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1085333/Government_response_to_consultation_on_the_future_regulation_of_medical_devices_in_the_United_Kingdom.pdf
65）Guidance; Software and AI as a Medical Device Change Programme - Roadmap Updated 17 October 2022
https://www.gov.uk/government/publications/software-and-ai-as-a-medical-device-change-programme/software-and-ai-as-a-medical-device-change-programme-roadmap#wp-5-cyber-secure-medical-devices
66）Guidance; Medical devices: software applications (apps)
https://www.gov.uk/government/publications/medical-devices-software-applications-apps
67）Appendix 4 -Field Safety Warnings and End-of-Life notification
Field Safety Warnings and End-of-Life notification

別紙２

医薬安発 0115 第２号
令和６年１月 15 日

各都道府県衛生主管部（局）長　殿

厚生労働省医薬局医薬安全対策課長
（　公　印　省　略　）

医療機器サイバーセキュリティに関する不具合等報告の基本的考え方について

医療機器のサイバーセキュリティの確保については、「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」（平成 27 年４月 28 日付け薬食機参発 0428 第１号・薬食安発 0428 第１号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）において、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を求めています。また、医療機器のサイバーセキュリティに関する具体的なリスクマネジメント並びにサイバーセキュリティ対策及び処置の考え方については、「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」（平成 30 年７月 24 日付け薬生機審発 0724 第１号・薬生安発 0724 第１号・厚生労働省医薬・生活衛生局医療機器審査管理課長・医薬安全対策課長連名通知）として取りまとめられており、製造販売業者は、サイバーリスクに伴う医療機器の不具合等を「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）における安全管理情報として取り扱い、適切な製造販売後安全管理を行う必要があることを示しています。

製造販売業者等が行う不具合等の報告については、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（昭和 35 年法律第 145 号）第 68 条の 10 第 1 項により規定され、その取扱いは「「医薬品等の副作用等の報告について」の一部改正について」（令和３年７月 30 日付け薬生発 0730 第８号厚生労働省医薬・生活衛生局長通知）により示しているところです。

今般、医療機器に対するサイバーセキュリティの確保を一層強化するため、製造販売業者等が行う不具合等の報告について、「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」（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）、研究代表者　国立医薬品食品衛生研究所　医療機器部　室長　宮島敦子）サイバーセキュリティワーキンググループにおいて、別添のとおり「医療機器サイバーセキュリティに関する不具合等報告の基本的考え方」が取りまとめられましたので、御了知の上、医療機器のサイバーセキュリティの更なる確保に向けた医療機器の製造販売後安全管理が円滑に行えるよう、貴管下関係製造販売業者等への周知及び指導等よろしくお願いいたします。

別添

医療機器サイバーセキュリティに関する不具合等報告の基本的考え方

1. はじめに

近年、医療機器の IoT（Internet of Things）化の加速、病院内のイントラネット環境構築に加え、サイバー攻撃の高度化が進んでいることから、医療機器のサイバーセキュリティ（CS）の確保が大きな社会的課題となっている。医療機器は、国内外に流通するとともに、インターネットに接続された医療機器については、国境の枠組みを超えてサイバー攻撃が行われる可能性があることから、CS 対応の国際調和を図ることを目的として、 国際医療機器規制当局フォーラム（International Medical Device Regulators Forum : IMDRF）において、医療機器サイバーセキュリティガイダンス N60「Principles and Practices for Medical Device Cybersecurity（医療機器サイバーセキュリティの原則及び実践）」（以下「IMDRF ガイダンス」という。）が取りまとめられ、令和 2 年 5 月 13 日付け薬生機審発 0513 第 1 号・薬生安発 0513 第 1 号厚生労働省医薬・生活衛生局医療機器審査管理課長・医薬安全対策課長連名通知「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（周知依頼）」によって、我が国においても、医療機器製造販売業者に対して IMDRF ガイダンスを導入することが示された。また、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。

基本的に医療機器の CS は、サイバー攻撃により医療機器の不具合や患者不利益が発生しないように未然に予防することが重要であるため、医療機器 CS の確保に当たり、市販前では、医療機器のサイバー攻撃に対する耐性が確保されるよう、設計及び開発を行い、市販後では、意図した環境での使用、脆弱性の修正（パッチ、アップデート）及びインシデントへの対応等の製造販売業者による適正な管理及び使用者である医療機関内等での適正な管理が相互になされることが必要である。たとえその時点で CS 対策が十分と思われても、将来にわたって未知の脆弱性に対応することは難しく、サイバー攻撃に起因する不具合等が起こってしまう可能性がある。また、既に判明している重大な脆弱性に対して医療機器の CS 対応及び製造販売業者の情報提供が不十分なまま放置されていた場合には、いつでもサイバー攻撃に起因する不具合等が発生し得ると考える必要がある。医療機器においては、未対応の脆弱性を悪用されて侵入を許してしまった、攻撃性の強いマルウェアに感染してしまった等の時点で、その影響は当該機器に留まらず、同様の脆弱性をもつその他の医療機器や医療システム全体へも影響する等、通常の不具合とは異なり、波及性が非常に大きいことから、CS に特化した速やかな対応が必要である。したがって、新たな被害を生じさせないためにも迅速に原因を究明するとともに、適切な安全確保措置を講じる必要がある。本文書では、不具合等報告制度における製造販売業者向けの医療機器 CS の基本的考え方を整理する。

2. 本文書の対象

本文書は、医療機器の製造販売を規制する「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」（昭和 35 年法律第 145 号。以下「医薬品医療機器等法」という。）第 2 条第 4 項に定義された医療機器のうち、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（SaMD ：Software as a Medical Device）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する。なお、医療機器のクラス分類を問わない。

本文書においては、医療機器 CS における不具合等報告制度を中心とした市販後安全対策に関する製造販売業者向けの基本的考え方を整理するとともに、現時点において医薬品医療機器等法に基づいて報告が必要と想定される事例を提示する。市販前を中心とした医療機器 CS に関しては、令和 3 年 12 月 24 日付け薬生機審発 1224 第 1 号・薬生安発 1224 第 1 号厚生労働省医薬・生活衛生局医療機器審査管理課長・医薬安全対策課長通知「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」別添「医療機器のサイバーセキュリティ導入に関する手引書」が参考となる。さらに IMDRF において追補ガイダンスが取りまとめられ、その内容に基づき、令和 5 年 3 月 31 日付け薬生機審発 0331 第 11 号・薬生安発 0331 第 4 号・厚生労働省医薬・生活衛生局医療機器審査管理課長・医薬安全対策課長通知「医療機器のサイバーセキュリティ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「医療機器のサイバーセキュリティ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 5 年 5 月第 6.0 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、国立研究開発法人日本医療研究開発機構医薬品等規制調和・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」（研究開発代表者：公益財団法人医療機器センター専務理事　中野壮陛）」の検討結果が取りまとめられ、令和 5 年 3 月 31 日付け医政参発 0331 第 1 号・薬生機審発 0331 第 16 号・薬生安発 0331 第 8 号・厚生労働省医政局参事官（特定医薬品開発支援・医療情報担当）・医薬・生活衛生局医療機器審査管理課長・医薬安全対策課長通知「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」別添「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」が発出された。

また、本文書の他、一般社団法人 日本医療機器産業連合会が編集している医療機器安全管理情報不具合報告書等の手引書（以下「不具合報告書等の手引書」という。）や、国内外のその他の関連ガイドラインも考慮するべきである。

3. 用語の解説

（1）不具合

「不具合」の事象は広く具合の良くないこと*と定義されており、いわゆる機器自体の故障や「不具合」の原因が機器とは関係なく、使用者側の要因で発生する事象も含まれる。この不具合は、医療機器全てに関わるもので、CS に関する場合も同様である。これらの事象をまとめると次の様になる。

医療機器の「不具合」の種類

- ✓ 仕様上の問題
- ✓ 不良品
- ✓ 故障・破損
- ✓ 添付文書等の不十分な記載
- ✓ 機器による有害事象

「不具合」を上記の 5 種類に分類したが、これらの不具合事象は多様であり、安全性上、対策を施し、他への影響を可及的速やかに最小にとどめる必要のある事象から、対策の緊急性がない軽微な事象や、発生機序や発生頻度が既知の事象まで様々である。「機器による有害事象」は、その他上記 4 つの不具合が原因となる場合や、他の要因で発生する場合もある。

*：「不具合による影響」とは、破損、作動不良等広く具合の良くないことによる影響をいい、設計、製造販売、流通又は使用のいずれの段階によるものであるかを問わない。（平成 26 年 10 月 2 日付け薬食発 1002 第 20 号厚生労働省医薬食品局長通知「医薬品等の副作用等の報告について」）

（2）脆弱性

JIS T 81001-1:2022 3.4.22 において、「ぜい（脆）弱性（vulnerability）」として次のように定義されている。

システムのセキュリティポリシーを破るために悪用される可能性のある、システムの設計、導入又は運用管理における欠陥又は弱み。

医療機器においては、ネットワーク等を介した機能・性能の向上に伴って、サードパーティ製ソフトウェアの使用も増大しており、既知の脆弱性だけでなく、設計検証の過程で発見することが困難な未知の脆弱性が含まれていることを考慮しなければならない。

一般的に、脆弱性を悪用された場合、「機器設定の不正変更」、「診断・治療に対する不正変更又は無効化」、「機密データの喪失又は開示」、「機器の誤動作」、「他の機器・システムへの攻撃・拡散」等が想定され、結果として医療機器の「(1) 不具合」に分類された様々な事象を引き起こす原因となる可能性がある。

(3) EOL、EOS 及びレガシー医療機器

「医療機器のサイバーセキュリティ導入に関する手引書（第 2 版）」において、医療機器の EOL（End of Life）、EOS（End of Support）及びレガシー医療機器は以下のように定義されている。

EOL（End of Life）	製品寿命終了。製品のライフサイクルにおいて、製造業者が定めた有効期間を超えた製品の販売を終了し、製品について正式な EOL プロセス（顧客への通知等）を実施する時点。（IMDRF ガイダンス和訳より）
EOS（End of Support）	サポート終了。製品のライフサイクルにおいて、製造業者が全てのサポート活動を中止する時点。サービスサポートは、この時点を超えない。（IMDRF ガイダンス和訳より）
レガシー医療機器	現在のサイバーセキュリティの脅威に対してアップデート又は補完的対策等の合理的な手段で保護できない医療機器で、販売開始以降の年数にかかわらない。（IMDRF ガイダンス和訳より、一部修正）

4. 製造販売業者における医療機器の不具合等報告

(1) 医療機器の不具合等報告の基本的事項

製造販売業者等は、不具合によるものと疑われる症例等を知ったとき、又は患者に重篤な健康被害が発生するおそれのある不具合を知った場合には、医薬品医療機器等法第 68 条の 10 第 1 項の規定により、令和 3 年 7 月 30 日付け薬生発 0730 第 8 号厚生労働省医薬・生活衛生局長通知「「医薬品等の副作用等の報告について」の一部改正について」を参照し、所定の様式により以下の報告書を独立行政法人医薬品医療機器総合機構医療機器品質管理・安全対策部 医療機器安全対策課（以下「PMDA」という。）に提出しなければならない。

- 様式 8：医療機器不具合・感染症症例報告書（国内／外国）
- 様式 9：医療機器に係る不具合の発生率変化調査報告書
- 様式 10：医療機器の研究報告／外国における製造等の中止、回収、廃棄等の措置調査報告書
- 様式 11：医療機器品目指定定期報告書
- 様式 12：医療機器未知非重篤不具合定期報告書

不具合等報告書は、報告期限内に、PMDA に提出する。なお、国内死亡症例についての全ての症例並びに外国医療機器に係る製造、輸入又は販売の中止等保健衛生上の危害の発生又は拡大を防止するための措置が講じられた場合の全ての措置内容について、PMDA に対し、ファックス等により速やかに第一報の報告をする。報告期限は、医薬品医療機器等法施行規則第 228 条 20 第 2 項に従って、発生もしくは発生のおそれのある健康被害の重篤性に応じて、情報入手日から 15 日、30 日、又は定期報告として、PMDA に報告することが定められている。

調査を開始する時点では、常に厳しい期限である 15 日を前提に作業を進めるとともに、報告期限内に報告すべき事項の調査が完了しない場合でも、報告期限を厳守する。その場合には、それまでに得られた調査結果を未完了報告とし、発生した事象によりその患者・使用者の受けた、又は受けるおそれのある障害のレベルを知りうる範囲で報告する。医療機関側からの報告と齟齬のないことが要求されるが、緊急時における第一報の場合にはその精度は問わない。その場合、所定様式の今後の対応欄に追加報告を行う旨記載し報告期日までに報告する。後日、追加報告時にはその精度を高めるべく報告企業は努力すべきである。なお、医療機関側との整合はその時点において取られるべきである。

(2) サイバーセキュリティに関する不具合等報告

医療機器 CS に関する不具合等報告も、通常の不具合等報告と同様に（1）に示した各種法令、通知等に基づき実施する。

収集した当該医療機器の脆弱性に関する情報に対して、有効性及び安全性等に関する影響等を製造販売業者が評価し、CS に関連して医療機器に不具合が発生し、健康被害が発生した又は健康被害の発生のおそれがある場合や、脆弱性に対し外国医療機器の安全確保措置が実施された場合には、不具合等報告の要否を検討する必要がある。

報告すべき CS に関連して発生する医療機器の不具合としては、以下のような事例が想定される。現時点では CS に関する不具合事例の蓄積が乏しいことから、製造販売業者は、当該例示のみを判断材料とすることなく、使用状況や（想定される）健康被害等を十分に考慮し、医薬品医療機器等法施行規則第 228 条の 20 第 2 項に従って適切に報告要否を判断する必要がある。事例は、一般社団法人日本医療機器産業連合会（以下「医機連」という。）PMS 委員会 不具合報告の手引き改訂 WG 傘下 サイバーセキュリティの不具合報告サブ WG にて、CS の不具合として討議された事例であり、本文書の他、不具合報告書等の手引書の改訂版を参照されたい。レガシー医療機器において発生した事象についても、同様に不具合等報告の必要性を考慮すること。

医療機器全般に共通の事例

- 脆弱性が認められ、不正アクセスにより悪用の実績（誤動作、機能不全等）が発生した*。
- あらかじめ計画されたアップグレードオプションが適用されず（不適切に放置された）、ネットワークに接続されたレガシー医療機器の脆弱性に対し不正アクセスにより悪用の実績（誤動作、機能不全等）が発生した。
- DDoS 攻撃（Distributed Denial of Service attack／分散型サービス拒否攻撃）により、画像診断装置等が意図せず機能停止した。

個別医療機器の事例

- ネットワーク接続された輸液ポンプの未使用ネットワークポートに対する不正アクセスにより設定が変更され、輸液の過剰投与や意図しない停止が起こった。
- インスリンポンプの設定が不正アクセスにより変更され、インスリンの投与量が想定の量より増加し、低血糖に至った。
- 植込み型除細動器の設定が不正アクセスにより変更され、ペーシング不全又はセンシング不全が発生したため、心停止状態の持続や不整脈が誘発された。

*：製造販売業者には EOS に至るまでのみならず EOS 後を含めた医療機器の製品ライフサイクル全体を通して発生した不具合に関する情報収集義務（医薬品医療機器等法 68 条の 2 の 6 第 1 項）及び行政報告義務（医薬品医療機器等法 68 条の 10 第 1 項）が残る。このため、不正アクセスによる悪用の実績が EOS の前後にかかわらず、製造販売業者は不具合等報告の必要性を適切に判断する必要がある。

なお、医薬品医療機器等法第 68 条の 9 第 1 項にあるように、医療機器 CS に関する安全管理体

制において、製造販売業者等は当該医療機器での不具合が発生した際には、適切な措置を講じることが重要である。さらに、通常の安全管理体制において、適時適切かつ積極的に情報収集するとともに、科学的に分析評価した上で、必要な情報を早急に医療機関等へ提供するなど必要な措置を講じ、被害の拡大を防止することも重要である。また、発生原因を調査するとともに、自己検証を行うことで、確実に以後の CS 実施体制を構築する必要がある。安全確保措置には以下のような手段がある。

- 医療機関への情報提供
- 回収・改修等
- 添付文書、取扱説明書の改訂
- 同一製品への処置（販売停止、製造中止、廃棄等）

いずれの作業も重複して実施する場合がある。措置の実施に当たり、適切に記録することなどが必要である。また、措置の実施に当たり都道府県、厚生労働省、PMDA への報告だけでなく、医療機関、患者への連絡等、関係者への報告・情報共有についても検討が必要である。なお、安全確保措置として緊急安全性情報等（イエローレター、ブルーレター）を作成する場合には、平成 26 年 10 月 31 日付け薬食安発 1031 第 1 号厚生労働省医薬食品局安全対策課長通知「緊急安全性情報等の提供に関する指針について」を参照すること。

一方で、製造販売業者が、自社の医療機器の脆弱性情報、他社の医療機器にも関係する脆弱性情報やセキュリティアドバイザリーを開示する場合、その緩和策及び補完的対策が立案できていない状況で開示すれば、即座にサイバー攻撃の標的になってしまうこともあるため、脆弱性情報を開示するタイミングは注意を要する。脆弱性の影響が大きく一般的である場合は、自社の対策だけでなく、場合によっては分野を超えた連携が必要な場合がある。この場合、製造販売業者は、規制当局等と連携して、必要な調整を実施する協調的な脆弱性の開示（CVD：Coordinated Vulnerability Disclosure）のプロセスを確立し実施する。

(3) 脆弱性に関する対応

脆弱性に関しては、全てが報告の対象ではない。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透明性を確保分析・評価を行うことは有用であるが、一般の情報セキュリティにおける使用を想定した CVSS スコア（基本値、現状値）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。参考となる資料の一つに、MITRE 社が策定した医療機器向けのガイド（MITRE Rubric for Applying CVSS to Medical Devices）がある。

製造販売業者は、脆弱性に関して当該医療機器のソフトウェア部品表（SBOM）及び設計情報等から脆弱性が存在するソフトウェアの存在、使用の有無及び機能性能に関する影響等を評価し、使用目的、使用部位、蓋然性等を総合的に判断した結果、当該脆弱性の悪用が原因で、死亡や重篤な健康被害が発生した場合、又は発生するおそれがあると判断した場合には、報告の要否や区分を評価、判断し、医薬品医療機器等法第 68 条の 10 第 1 項の規定により規制当局への不具合等の報告を実施すること。上記評価の結果、当該医療機器において、脆弱性が存在するソフトウェアが使用されていない場合、又はセキュリティパッチ等の対策により問題が除去又は機能性能に影響がない程度にリスクを低減可能で健康被害が発生するおそれがないと判断できる場合は、製造販売業者は、規制当局への不具合等の報告を実施する必要はない。但し、経時的にモニターし、報告の必要が出てきた場合には報告する。

(4) レガシー医療機器に関する対応

医療機器の CS を考える上で、医療機器の製品ライフサイクルと製造販売業者の責任及び情報提供について配慮する必要がある。既知の脆弱性情報等を対策した設計に基づく製品であっても、セキュリティアップデートが提供できなくなる EOS 後も継続して使用される場合、又は新たな緊急

性の高い脆弱性に起因した事象が発生した場合は EOL に達していなくても、即座にレガシー医療機器になることもある。製造販売業者には EOS に至るまでのみならず EOS 後を含めた医療機器の製品ライフサイクル全体を通して発生した不具合に関する情報収集義務（医薬品医療機器等法第 68 条の 2 の 6 第 1 項）及び行政報告義務（医薬品医療機器等法第 68 条の 10 第 1 項）がある。EOS 後の継続した使用に関しては、決して推奨できる状態ではないとともに、継続して使用する責任は医療機関にあることは、全ての関係者が理解しておかねばならず、そのために製造販売業者は、積極的な情報提供を行い、顧客との連携、医療機関と認識を共有することが重要である。

5. 情報共有体制について

医療機器の不具合等については、医薬品医療機器等法に基づく医療機器不具合等報告制度の中で、PMDA へ情報共有される体制となっている。国内における医療機器の CS に関する安全対策として、製造販売業者は、医療機器の CS に関する不具合や健康被害が発生した場合には、当該医療機器の影響等を評価し、不具合等報告の要否について判断し、必要に応じて PMDA に報告する。その際に、製造販売業者は、医療機関、使用者、規制当局及び脆弱性発見者等と必要な情報共有等を行い、連携したアプローチを実施することが求められる。そのために製造販売業者は、脆弱性に関する情報の収集、評価、報告に関する情報共有体制の構築、維持が必要であり、併せて継続的な人材育成が望まれる。

国内において、CS については、内閣府、経済産業省、警察庁、その他独立行政法人や民間の非営利団体によって積極的な情報収集や関係企業等への情報提供が行われている。医療機器の不具合等報告を管轄している厚生労働省においても、令和 3 年 6 月 28 日付け事務連絡「医療機関を標的としたランサムウェアによるサイバー攻撃について（注意喚起）」等により、製造販売業者やその他医療関係者へ、脆弱性に関する情報提供を行っている。

6. まとめと今後の展望

本文書では、国内における医療機器の CS に関する安全対策として、CS に関連して医療機器の不具合や健康被害が発生した場合、又は患者に重篤な健康被害が発生するおそれのある不具合を知った場合の報告対象の考え方を整理した。

一方で、諸外国の取り組みを考慮すると、今後は、医療機器の CS に関する情報を入手した際に、関係者間で情報共有等を行い、連携して対処するための具体的な手順の確立が望まれる。

別紙３

医療機関における CS に関する不具合報告の内容と報告先について

➢ 不具合報告の基本的事項における医療機関における報告内容と報告先

医療機器に不具合が生じた場合、並びに不具合は生じていないが、患者に重篤な被害が発生するおそれのある場合等は、直ちに医療機関内の管理部署（情報管理部門や医療機器管理部門等）や医療安全管理者、医療機器安全管理責任者等及び医療機器の製造販売業者等に連絡する。

一方、製造販売業者を介さずに PMDA に報告する医薬品・医療機器等安全性情報報告制度も利用可能である。当該制度は、日常、医療の現場においてみられる医療機器の使用によって発生する不具合の情報を医薬品医療機器等法第 68 条の 10 第 2 項に基づき、医薬関係者が厚生労働大臣に報告する制度である。現在は、医薬品医療機器等法第 68 条の 13 第 3 項に基づき、PMDA に医薬関係者についての副作用等報告に係る情報の整理を行わせることとしたため、平成 26 年 11 月 25 日より、医療機関等からの不具合は PMDA に報告することとなった。

➢ CS に関する不具合報告における医療機関における報告内容と報告先

医療機器に不具合が生じた場合、並びに不具合は生じていないが、コンピュータウイルスに感染又は感染の疑いがあり、患者に重篤な被害が発生するおそれのある場合等は、直ちに医療機関内の管理部署（情報管理部門や医療機器管理部門等）や医療安全管理者、医療機器安全管理責任者等及び医療機器の製造販売業者等に連絡するとともに、各医療機関が定める手順書等に基づき、管理部署を通じて医療機関内で情報共有すること。当該不具合がサイバー攻撃によるものかどうかについては、見分けをつけるのが困難であると共に、感染源の特定も困難であるため、使用環境や原因と考えられる事象（メールの添付ファイルを開いた、USB メモリ等の機器をつなげた等）と共に、早急に製造販売業者に報告するべきである。特に以下の様な症状が確認された場合は、その症状についても合わせて報告する。

・医療機器設定の不正変更
・治療の不正変更又は無効化
・機密データの喪失又は開示
・医療機器の誤動作
・他の機器・システムへの拡散

一方、製造販売業者を介さずに PMDA に報告する医薬品・医療機器等安全性情報報告制度も利用可能である。当該制度は、日常、医療の現場においてみられる医療機器の使用に

よって発生する不具合の情報を医薬品医療機器等法第 68 条の 10 第 2 項に基づき、医薬関係者が厚生労働大臣に報告する制度である。現在は、医療機関等からの不具合は PMDA に報告する。

報告対象施設はすべての医療機関及び薬局等とし、薬局開設者、病院若しくは診療所の開設者又は医師、歯科医師、薬剤師、登録販売者その他病院等において医療に携わる者のうち業務上医療機器を取り扱う方が報告者となる。報告対象となる情報は、医療機器の使用による不具合の発生（健康被害が発生するおそれのある不具合も含む。）について、保健衛生上の危害の発生又は拡大を防止する観点から報告の必要があると判断した情報（症例）が該当し、医療機器との因果関係が必ずしも明確でない場合であっても報告するべきである。

PMDA に報告された情報については、情報の整理又は調査の結果を厚生労働大臣に通知すると共に、当該医療機器を供給する製造販売業者等へ情報提供する。また、PMDA 又は当該製造販売業者等は、報告を行った医療機関等に対し詳細調査を実施する場合がある。報告された情報については、安全対策の一環として広く情報を公表することがあるが、その場合には、施設名及び患者のプライバシー等に関する部分は公表しない。

報告期限については特に定められていないが、保健衛生上の危害の発生又は拡大防止の観点から、報告の必要性を認めた場合においては、適宜速やかに報告するべきである。

なお、患者からの報告制度は、医療機器においては対象外である。

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対応については、令和 5 年 3 月 31 日付け医政参発 0331 第 1 号 薬生機審発 0331 第 16 号 薬生安発 0331 第 8 号厚生労働省医政局参事官(特定医薬品開発支援・医療情報担当) 医薬・生活衛生局医療機器審査管理課長 医薬・生活衛生局医薬安全対策課長通知（別添）「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」を参照すること。なお、インシデント発生に関する報告は、厚生労働省医政局特定医薬品開発支援・医療情報担当参事官室、都道府県、医療セプター等に対して行う必要がある。実際に保健衛生上の危害が発生し、又は拡大するおそれかがある場合には医療機器に関する安全性情報として PMDA に報告する。また、令和 5 年 5 月 31 日付け産情発 0531 第 1 号厚生労働省の H P に、医療機関等がサイバー攻撃を受けた場合の連絡先として、厚生労働省医政局特定医薬品開発支援・医療情報担当参事官室が示されている。