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。