1

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

1．はじめに

我が国において現在流通している医療機器については，製品自体の品質が担保され，また使用者による適正使用がなされることにより，医療機器の有効性及び安全性が確保され，疾病の診断及び治療等に利用されることになる。

このような医療機器の中には，IoT機器等の通信技術を持つものが多く登場しており，医療機関のネットワーク等に接続され，外部装置と通信しながら使用される，又は，記憶媒体等を介して間欠的にデータの授受が行われながら使用されるものが近年増加している。IoT機器等の基盤となる通信技術の進歩に伴い，今後も医療機器が医療機関のネットワーク，他の医療機器又は電子機器と接続される機会がさらに増加することが想定される。

このように医療機器が外部の装置とデータの授受を行いながら使用される状況では，医療機器がデータ通信による外部からの不正な侵入のリスクに晒される機会が増加することも意味する。例えば，医療機関のネットワーク等に接続された他のコンピュータ等がサイバー攻撃を受けた場合には，ネットワークを介して医療機器がサイバー攻撃を受けるリスクがある。同様に，医療機器がサイバー攻撃を受けた場合には，当該医療機器が接続された医療機関等のネットワークを介して他の医療機器やコンピュータ等もサイバー攻撃を受け，障害が引き起こされる可能性もある。

医療機関において，医療機器のサイバーセキュリティを確保するためには，医療機器が製品としてサイバー攻撃に対する耐性が確保されるよう，市販前に，医療機器メーカーにより設計及び開発がなされた上で医療現場に提供され，市販後に意図する使用環境の運用，情報共有，脆弱性の修正，インシデントの対応などが適切になされることが重要であるが，医療現場において適正な管理がなされることも重要である。

本稿では，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諸外国を含む国際的な動向について紹介する。

2．医療機器のサイバー攻撃に関するリスクに関する諸外国の分析状況

医療機器がサイバー攻撃を受けた場合，検査装置又は診断装置であれば検査の中断や誤った診断につながってしまう可能性が考えられ，治療に用いられる装置であれば，治療の中断等の事象の発生，放射線治療の線量計算プログラムであれば，過量照射や不十分な量の照射が発生する可能性が考えられる。

我が国では，本稿執筆時点において医療機器へのサイバー攻撃が原因となる患者等への健康被害の発生は報告されていない。しかし，海外では，医療機器のサイバーセキュリティを起因としたインシデント事例が複数報告されている。

例の一つとして薬液注入ポンプの脆弱性に関するものが挙げられる。2015年７月，米国FDAはHospira社の薬液注入ポンプであるSymbiq Infusion Systemについて警告通知を発出している。これは，未使用のネットワークポートに対して外部からアクセス可能な状態になっており，通常は管理権限を持たない第三者が，医療機関のネットワークを介して当該製品へ遠隔的にアクセスし，ポンプの注入量を変更することが可能な状況だったというものであった。Hospira社は既に当該製品の製造販売を中止していたものの，米国FDAは，当該製品を使用する医療機関に対し，使用を中止し，他製品へ移行するよう強く推奨する旨等をアナウンスした[1)]。本事例は，医療機器のサイバーセキュリティの不備について，規制当局が有害事象として警告を発信したものである。

また，もう一つの事例として，植込み型心臓ペースメーカのリモート監視デバイスに関する脆弱性に関するものが挙げられる。2017年１月，米国FDAは心臓ペースメーカの遠隔モニタリングシステムについて査察を実施した結果，CFR（Code of Federal Reguration）のパート820に基づく医療機器の品質規制事項に沿った手順通りに，サイバーセキュリティの脆弱性のリスクアセスメントが行われておらず，サイバーセキュリティに関する十分な設計検証が行われていないことが確認した[2)]。この脆弱性は，第三者である攻撃者がペースメーカへ不正にアクセスし，コマンドの実行やペースメーカの設定変更を行う等，ペースメーカの機能を妨害する可能性があるものであり，ペースメーカの製造販売業者は，医療機器のファームウェアをアップデートする等の対応を実施した。本事例については，医療機器の脆弱性に対するサイバー攻撃がなされた際のリスク評価結果を基に，予防的に処置が取られた事例であり，実際にサイバー攻撃による健康被害は生じていない。

３．各国におけるサイバーセキュリティの対応状況について

医療機器のサイバーセキュリティに係る対応として，2000年代に入り，我が国を含む各国において，ガイダンスがまとめられている。

米国FDAにおいては，2005年７月に「Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software」[3)] が取りまとめられ，その後，2014年10月に「Content of Premarket Submissions for Management of Cybersecurity in Medical Devices」[4)]，2016年12月 に「Postmarket Management of Cybersecurity in Medical Devices」[5)] が追加的に取りまとめられている。一方，欧州においては，2018年５月に医療機器のサイバーセキュリティに関する各種の指令が発出されている。この他，カナダ，フランス，ドイツ，オーストラリア，中国において，各国の状況に応じたガイダンスが発行されている状況にある。

我が国においては，医療機器の製造販売業者に対し，医療機器へのサイバー攻撃に対するリスクを適切に評価すると共に，医療機器の特徴に応じてサイバーセキュリティに関する対応を行うよう指示している[6)]。さらに，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及び対策・処置の考え方について，「医療機器のサイバーセキュリティの確保に関するガイダンス」として取りまとめている[7)]。

当該ガイダンスでは，サイバー攻撃によるリスクを想定するために，医療機器を使用する環境を特定し，

使用場所として医療施設又は在宅等の検討を行うこと，そして医療機器を使用する際のネットワーク等への接続方法を特定し，有線又は無線によってネットワークへ接続する場合とUSBメモリ等のような外部記憶媒体を介して外部機器とデータの授受を行う場合とに分け，対応を検討することが必要であるとしている。また，当該ガイダンスにおいては，サイバーセキュリティに係る対応として，医療機器製造販売業者から医療機関等の使用者に対する情報提供を行うこととしており，サイバーセキュリティに関する情報提供の方法として，添付文書や技術資料等について例示している。さらに，医療機器のサイバーセキュリティについては，医療機関との適切な連携が必要であることも留意することとされている。

上述のとおり，我が国を含む各国において，医療機器のサイバーセキュリティに関する各種ガイダンスが取りまとめられているところである。しかし，近年，医療機器が複数国に渡って流通することもあり，また，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。そのため，医療機器のサイバーセキュリティに関する国際整合を図り，一般原則とベストプラクティスを提供す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，「Principles and Practices for Medical Device Cybersecurity」（以下「IMDRFガイダンス」という。）が2020年３月に取りまとめられた[8)]。

４．IMDRFガイダンスについて

IMDRFガイダンスは，各国規制当局の共通概念としてまとめられたものであり，当該ガイダンスでは，行政，医療機器製造販売業者，医療機関関係者等，医療機器のサイバーセキュリティの関係者の間における遅滞のない，積極的な情報共有が重要であることが言及されている。

IMDRFガイダンスにおいて言及されている一般原則としては，国際整合，医療機器の全ライフサイクル，責任の分担と共有（Shared responsibility），情報共有が記載されており，ベストプラクティスの中には，市販後における医療機器のサイバーセキュリティ対応のための考慮事項として，意図する使用環境における医療機器の運用，関係者の間における情報共有，協調的な脆弱性の開示（Coordinated Vulnerability Disclosure：CVD），脆弱性の修正，インシデントへの対応等が挙げられている。

この中でCVDは，サイバーセキュリティを確保するための手段としての情報開示を示し，医療機関の関係者においても重要な意味を持つ。IMDRFガイダンスでは，CVDは，サイバーセキュリティのインシデントへの準備及び対応に関する透明性を強化する１つの手法として位置づけられており，未知の脆弱性等を考慮してセキュアな状態にすることは難しいことから，医療機器の製造販売業者がサイバーセキュリティの脆弱性情報を入手し，それを評価し，緩和策及び補完的対策を開発した上で，医療従事者を含む関係者に対して透明性を持って情報開示することが重要である旨が言及されている。

一方で，IMDRFガイダンスでは，ヘルスケアプロバイダとして医療機関の関係者においても，医療機器の購入から廃棄までの全ライフサイクルを通して，潜在的なサイバーセキュリティリスク及び脅威を継続的に監視，評価，緩和，情報共有及び対応するために，役割分担と医療機器製造販売業者との連携が必要である旨の言及がなされている。

本稿では，IMDRFガイダンスのうち，特に医療機関の関係者において重要と考えられる市販後の情報提供に関係する内容を概説したが，より正確な内容については，国立医薬品食品衛生研究所が作成した邦訳[9)] 及びIMDRFガイダンスの原文を参考にされたい。

５．国内におけるサイバーセキュリティ対応の今後について

医療機器のサイバーセキュリティについて適切に対応するには，医療従事者を含む関係者の協力の下で，医療機器の製造販売業者が個々の医療機器の特性に応じたリスク分析を行った上で，サイバー攻撃によるリスクを低減するための対策を十分に行うことが重要である。

医療機器のサイバーセキュリティに係る安全性を向上させる観点から，我が国においても，今後３年程度を目途に医療機器製造販売業者等の関係業者におけるIMDRFガイダンスの導入に向けて検討を行っている[10)]。そのため，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製造販売業者等との体制確保について，ご理解を頂き，引き続き協力を頂きたい。

＜参考文献＞

１）“Cybersecurity Vulnerabilities of Hospira Symbiq Infusion System: FDA Safety Communication”
https://wayback.archive-it.org/7993/20170404182201/https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm456815.htm（2020年５月20日確認）

２）“Cybersecurity Vulnerabilities Identified in St. Jude Medical's Implantable Cardiac Devices and Merlin@home Transmitter: FDA Safety Communication”
https://www.fda.gov/medical-devices/safety-communications/cybersecurity-vulnerabilities-identified-st-jude-medicals-implantable-cardiac-devices-and-merlinhome（2020年５月７日確認）

３）“Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software”
https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-networked-medical-devices-containing-shelf-ots-software（2020年５月７日確認）

４）“Content of Premarket Submissions for Management of Cybersecurity in Medical Devices”
https://www.fda.gov/regulatory-information/search-fda-guidance-documents/content-premarket-submissions-management-cybersecurity-medical-devices-0（2020年５月７日確認）

５）“Postmarket Management of Cybersecurity in Medical Devices”
https://www.fda.gov/regulatory-information/search-fda-guidance-documents/postmarket-management-cybersecurity-medical-devices（2020年５月７日確認）

６）「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

７）「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

8）“Principles and Practices for Medical Device Cybersecurity”
http://www.imdrf.org/docs/imdrf/final/technical/imdrf-tech-200318-pp-mdc-n60.pdf（2020年５月７日確認）

9）「医療機器サイバーセキュリティの原則及び実践」（原題「Principles and Practices for Medical Device Cybersecurity」）
http://www.nihs.go.jp/index-j.html

10）「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）」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