公募シンポジウム
# シンポジウム10
# IoTにおけるサイバーセキュリティの現状と対策、および対策としてのISAC
2021年11月21日(日) 09:10 〜 11:10 F会場 (2号館2階224)

[4-F-1-03] IoT機器としての医療機器、モバイルヘルスにおけるセキュリティ対策の現状
Current status of security measures for medical devices and mobile health as IoT devices

*松元 恒一郎[1]（1. 日本光電工業株式会社　技術戦略本部）
*Koichiro Matsumoto[1]（1. Nihon Kohden Corp.）
キーワード：IoT Security Guideline, mHealth, IMDRF

近年、医療機器は、有線／無線のネットワークを介しての他の機器やソフトウェアと連携等システム化や USBメモリ等の携帯型メディアを使って医療情報を入出力する機会も増えて来ており、ネットワーク等には医療機器以外の電気機器も接続されており、医療機器の使用環境が常にセキュアであるとは限らない。このため、医療機器の有効性及び安全性を確保するためにサイバーセキュリティの重要性がより増している。本稿では、医療機器を経由して侵入されるセキュリティリスクの事例を説明し、院外を中心としたモバイルヘルスの活用がより推進されること鑑み、平成28年に総務省・経産省から発出された「 IoTセキュリティガイドラン Ver1.0」をベースとして医療機器との特性について論じる。さらに厚生労働省からは、平成27年、「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30年「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」が主として医療機器製造業者に対して発出されている。サイバーセキィリティとしては、他の機器・ネットワーク等と接続して使用する又は他からの不正なアクセス等が想定される医療機器については、サイバーリスクを含む危険性を評価・除去し、リスクマネジメントを行い、使用者に対する必要な情報提供や注意喚起を含めて適切な対策を行うこととしている。2020年4月には、国際医療機器規制当局フォーラム（ IMDRF）から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が公表された。これは、一般原則及びベストプラクティスについて、全ての責任関係者に対して推奨事項を提供するもので、製造業者、医療提供者、使用者、規制当局及び脆弱性報告者を含むすべての利害関係者の共同責任であり、2023年を目途に国内でも導入の検討が進んでいる。さらにモバイルヘルの観点も踏まえて安全管理ガイドラインとサイバーセキュリティガイダンスについても論じる。

IoT 機器としての医療機器、モバイルヘルスにおけるセキュリティ対策の現状

松元 恒一郎[*1]

*1 日本光電工業㈱ 技術戦略本部

Current status of security measures for medical devices and mobile health as IoT devices

Koichiro Matsumoto[*1]

*1 Nihon Kohden Corp.

In recent years, the opportunities to input and output medical information by systematization of medical devices such as linking with other devices and software via wired and wireless networks and portable media such as USB memory sticks are increasing. Electrical devices other than medical devices are connected to the network, and the environment in which medical devices are used is not always secure. Therefore, the importance of cyber security is becoming more and more important to ensure the effectiveness and safety of medical devices. In this paper, we describe an example of a security risk of intrusion through a medical device. Furthermore, we discuss the characteristics of the IoT security guideline based on the "IoT Security Guideline Ver. 1.0" issued by the Ministry of Internal Affairs and Communications and the Ministry of Economy, Trade and Industry in 2016, in comparison with medical devices. Furthermore, The Ministry of Health, Labor and Welfare has issued documents on cybersecurity of medical devices in 2015 and 2018 to medical device manufacturers. In April, 2020, the International Medical Device Regulatory Forum (IMDRF) published guidance on medical device cybersecurity principles and practices. It provides guidance on general principles and best practices that provides recommendations to all responsible parties, is the joint responsibility of all stakeholders, including manufacturers, health care providers, users, regulators and vulnerability reporters, and covers the entire product life-cycle. This guidance will be introduced in Japan until 2023. In addition, I also show cyber security from the perspective of mobile health.

Keywords: IoT Security Guideline, mHealth, IMDRF

1. はじめに

近年、医療機器は、スタンドアロンで使われることより、医療機関のネットワーク等に接続され、又は記憶媒体等を介してデータの授受を行いながら使用されるものが増加している。ネットワーク等には、医療機器以外の電子機器(IoT 機器と考えてもよい)も接続されており、医療機器の使用環境が常にセキュアであるとは限らない。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や不正操作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。また、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。さらにモバイルヘルスを介しての接続も今後需要が拡大しており、このセキュリティ対応も重要となる。

このため、医療機器の本来の目的である、有効性及び安全性を確保するために市販前、市販後となる製品のライフサイクル全般におけるサイバーセキュリティの重要性が増している。医療機器のサイバーセキュリティは、IoT 機器と通ずるところがあり、今や IoT 機器と同じレベルで対応する必要が出てきていると思われる。

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、さらにさらにモバイルヘルスの観点も踏まえて安全管理ガイドラインとサイバーセキュリティガイダンスについても論ずる。

1.1 セキュリティリスクの事例

セキュリティリスクの変遷を含めて代表的ないくつかの事例の概要について述べる。

米国が先行して、2013 年頃からまずは、医療機器の調査というレベルで報告されている。ICS-CERT(Industrial Control Systems Cyber Emergency Response Team:産業制御システムサイバー緊急事態対応チーム)が医療機器の中にハードコードされているパスワードについて注意喚起をしている。また FDA が、医療機器のサイバーセキュリティに関するガイダンスのドラフトを 2013 年 6 月に公開した。2014 年は、医療機器への標的型攻撃の入り口として、ハッキング等報告があり、対象となる機器として薬物注入ポンプや X 線検査装置があげられている。8 月には、米国の病院に中国からサイバー攻撃があり、患者 450 万人のデータが流出したとの報告がされている。狙われたのは、医療機器の開発・研究(治験)データ等の知的財産であった。2015 年には、医療機関への攻撃として医療機器が悪用される事例が報告されている。また 7 月には FDA が、薬物注入ポンプの製品(Hospira 社 Symbiq Infusion System)を特定して、利用中止の指示を行っている [1]。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。

その後も報告事例はあるが、2017 年にはランサムウェア「WannaCry」への大規模感染が発生した。2020 年 6 月 TCP/IP 通信用ライブラリの脆弱性として Ripple20 が報告されている。これが悪用されるとプリンタからデータが盗まれたり、輸液ポンプの動作が変更されたりと重要インフラを含む様々な業界の機器に影響を与えるとされている。これについては医療機器製造販売業者がレポート等出しており、FDA は安全性のレポートは出されていない。さらに 2020 年 9 月にはドイツの病院へのランサムウェア攻撃で初の死者が報告されて

いる。我が国においても 2018 年 10 月の市立病院、2017 年（公表は 2020 年）には大学病院でそれぞれ電子カルテシステム、検査装置へのランサムウェア攻撃が発生している。

1.2 医療機器サイバーセキュリティ各国の規制の状況

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。医療機器サイバーセキュリティの各国の規制状況について、その概要を述べる。

医療機器の主マーケットである米国が、先行しており、FDA においては 2005 年7月に「Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software」[2] 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」[3]、2016 年 12 月に「Postmarket Management of Cybersecurity in Medical Devices」[4]が追加的に取りまとめられている。ヨーロッパ、EU では、一般データ保護規制である General Data Protection Regulation（GDPR）が 2018 年制定され、Medical Device Regulation（MDR）情報セキュリティを含むリスクマネジメントについてはコロナウイルスの影響で、一年延長され、2021 年 5 月となっている。

我が国では、2015 年 4 月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 [5]。さらに、2018 年 7 月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」として取りまとめられている [6]。

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状況にあるが、近年、医療機器が国を渡って流通することや、インターネットに接続されている医療システムについては、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」（医療機器サイバーセキュリティの原則及び実践）が 2020 年 4 月に公開された [7]。我が国も今後これに遵守する動きになっている。

2. IoT セキュリティガイドライン

IoT セキュリティガイドラインは、平成 28 年、2016 年に総務省、経済産業省を中心とした IoT 推進コンソーシアムで検討された [8]。これは、IoT 特有の性質とセキュリティ対策の必要性を踏まえることが重要であると述べている。

関係者が、セキュリティ確保の観点から求められる基本的な取り組みを、セキュリティ・バイ・デザインを基本原則としつつ、明確化することによって、産業界による積極的な開発等の取り組みを促すとともに、利用者が安心して IoT 機器やシステム、サービスを利用できる環境を生み出す。また、関係者が、取り組むべき IoT のセキュリティ対策の認識を促すとともに、その認識のもと関係者間の相互の情報共有を促すための材料を提供する。さらに、守るべきものやリスクの大きさ等を踏まえ、役割・立場に応じて適切なセキュリティ対策の検討が行われることを期待することを目的としている。

2.1 IoT 特有の性質とセキュリティ

IoT 特有の性質として、セキュリティ上の脅威の影響範囲・影響度合いが大きいことがあげられる。つまりネットワークを介して関連する機器・システム、サービス全体に影響が波及しやすくなる。10 年から 20 年程度と長期間に渡って使用される機器が多く、これらの機器のセキュリティ対策が不十分になりえる。さらに機器がどこにあるか等監視が行き届かないことがあげられる。機器側とネットワーク側のコミュニケーション不足があり、相互運用性が確保されておらず、想定外のアクセスが発生する可能性がある。また、開発者が想定しなかった環境で使われたりする可能性があげられる。これは医療機器では、Intended use である「意図する使用」を明確にすることになり、想定していない接続となるので、リスク分析もその部分においては、行われていない状態になる。

2.2 IoT セキリュティガイドラインを医療機器に適用する場合

IoT セキュリティガイドラインでは、方針、分析、設計、構築・接続、運用・保守の工程別に 5 つの指針に基づいて、それぞれ対応することを求めている。「方針」では、IoT の性質を考慮した基本方針を定めること、「分析」では、IoT のリスクを認識すること、「設計」では、セキュリティとして、守るべきものを守る設計を考えること。さらに、「構築・接続」では，ネットワーク上での対策を考えること。最後の工程として「運用・保守」では、安全安心な状態を維持し、情報発信・共有を行うことを指針としている。

医療機器に適用する場合について述べる。IoT 機器・システムは、医療機器、または 医療機器・システムに置き換えることができる。IoT システムは、医療情報システム、IoT 機器・システム提供者は、医療機器・システムの製造販売業者であると言える。システム・サービス提供者は、医療機関，医療情報システムの事業者として置き換えられる。また IoT 機器の一般利用者は、医療機器では、患者及びその家族、医師、技師、看護師と言える。

2.3 医療機器 開発の背景と課題

医療機器の開発背景と課題について述べる。医療機器は、有効性、安全性がより重要となるため、QMS が求められる。また製品寿命が 10 年から 15 年と一般的に長い。その間、必要に応じて、アップグレードが繰り返される。これは、近年重要で、セキュリティの脆弱性による対応のパッチをあてる等必要となっている。スタンドアロンで使われるより、ネットワークを介して接続されることが一般的となっているので、相互運用性が求められる。また、医療機器としては、必須となるユーザビリティも求められる。これらの背景に対して、課題としては、セキュリティに関して、医療機器製造販売業者にエキスパート等人材が不足していることもあるが、対応が後工程になっていることや設計や構成の考え方が十分でないことがあげられる。これらの課題は、製造販売業者の会社全体として取り込む必要があり、筆者が活動している産業界としてもスキルアップのセミナー等教育、啓蒙も充実する必要があると考えている。

3. 安全管理ガイドラインとサイバーセキュリティガイダンス

我が国における、主として医療情報システムを、その適応としている安全管理ガイドラインと、医療機器のサイバーセキュリティガイダンスの関連について述べる。

医療情報システムの安全管理に関するガイドラインは、医療機関が、主体となって医療情報システムの機密性・完全

性・可用性を確保するために医療情報システムの安全管理を行うもので、根拠法は、個人情報保護法、e 文書法となっている。2017 年 4 月に第 5 版が公開され、2021 年 1 月には、サイバー攻撃、二要素認証、クラウドシステム等追記された第 5.1 版が公開された。

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は、2018 年に発出されたガイダンスで、医療機器製造販売業者が主体となって、サイバーリスクに対する医療機器の機能性と患者の安全を保持するものある。医療機関に対して必要な情報提供及び連携を図ることが求められている。根拠法は、医薬品医療機器等法で、省略して、薬機法と呼ばれている。

3.1 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

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は、厚生労働省から、平成 27 年(2015 年)，平成 30 年(2018 年)と発出されており、対象は製造販売業者となっている。

前者が「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」である。基本的な考え方は、サイバーセキュリティが懸念される医療機器について、サイバーセキュリティを確保する必要があることを述べている。医療機器の開発に当たっては、つまり市販前についてサイバーセキュリティのリスク分析を行い、必要な対策を実施することを求めている。今までも医療機器製造販売業者は、製品の開発においてリスクマネジメントを実施しているが、サイバーセキュリティの観点も加えて、実施することになる。既に製造販売している製品、つまり市販後に当たるが、これについても必要であるとしている。

こういった基本的な考えに加えて、他の機器・ネットワーク等と接続して使用する、他の機器から不正なアクセス等が想定される医療機器については、サイバーセキュリティを含む危険性を評価・除去し、リスクマネジメントを行い、使用者である医療従事者等に必要な情報提供や注意喚起を含めて必要な対策を行うように求めている。

後者が、平成 30 年(2018 年)に発出された「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」である。これには、より具体的な実施項目等説明されている。医療機器に関する検討としては、医療機器を使用する環境を特定すること、さらに医療機器のネットワーク等への接続、無線通信、有線通信、USB ポートでの接続等、特定することを求めている。具体的な対応としては、意図される使用環境におけるサイバーリスクに対するリスクマネジメントを実施することとなる。2019 年度 AMED、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わる課題抽出などに関する研究で行われた「製造販売業者が行っている医療機器のサイバーセキュリティ対策に関する実態調査」での設問に「サイバーリスクが懸念される医療機器について、製品の使用環境を特定しているか？」に対して、44%の製造販売業者が全く使用環境を特定していないと回答している。さらに製造販売業者は，必要に応じて医療機関と連携を取ることと求めている。さらに市販後に位置づけられるサイバーリスクに伴う不具合情報の収集、管理等医療機関との連携し、共有することが必要となる。先の実態調査でも、医療機関と情報の連携については、低い数字が出ており、今後も課題である。

ガイダンスの構成の概要を示す。1 項が、目的で市販前・市販後にわたるセキュリティ対応の重要性が述べられている。2 項が、対象となる医療機器及び使用環境の特定、ネットワーク等への接続について項目が述べられている。3 項が、サイバーセキュリティ対応として、リスクマネジメントの実施、キュリティ対応に関する方針、体制の確立、情報開示等製造販売業者、使用者の両面から述べられている。4 項が、市販後の安全性確保となっており、ソフトウェアのアップデート等も対象とされている。5 項が、使用者への情報提供となっており、添付文書への記載事項等が求められている。

4. 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

4.1 国際整合に向けた組織 GHTF/IMDRF

1992 年から 2012 年まで、Global Harmonization Task Force（GHTF）として、日本、オーストラリア、カナダ、ヨーロッパ（EU）、そして米国で構成されて、医療機器規制の基本的なフレームワークに対する多くのガイダンス文書を開発してきた。例えば、基本要件基準、クラス分類ルール等があげられる。各国は、これに基づいて自国の規制に取り込んでいる。

2011 年には、これらの国に加えて、ブラジル、中国、ロシア、シンガポール、韓国が参加し、IMDRF として発足し、現在に至っている。管理委員会は、規制当局となるので、我が国では厚生労働省、PMDA（独立行政法人 医薬品医療機器総合機構）、米国では FDA が参加している。作業グループでは、産業界からも参加可能となっている。

4.2 IMDRF サイバーセキュリティガイダンス

IMDRF のサイバーセキュリティガイダンスである「医療機器サイバーセキュリティの原則と実践」は、各国規制当局の共有概念としてまとめられたものであり、2020 年 4 月に公開された。以下にポイントと示す。

- 医療機器のサイバーセキュリティに対する一般原則及びベストプラクティスについて、全ての責任関係者に対して推奨事項を提供する。
- 患者危害の可能性を検討することに限定し、データプライバシーの侵害に関係するようなその他の危害も重要であるが、この文書の適用範囲とはしていない。規制当局の立場から、患者への危害と患者の安全性を重視し、情報セキュリティを除外し、直接的に医療機器の安全と性能を含むことを明記している。
- サイバーセキュリティは、製造販売業者、医療提供者、ユーザー、規制当局及び脆弱性報告者を含むすべての利害関係者の共同責任であり、製品ライフサイクルの全体を対象としている。
- 設計インプット、リスクマネジメント、セキュリティテスト、市販後管理の戦略、ラベリング規制当局への対応等、市販前の注意事項について述べている。
- 市販後の考慮事項としては、意図する環境における機器の運用や情報共有、さらに協調的な脆弱性の公開（Coordinated Vulnerability Disclosure：CVD）、脆弱性の修正、インシデントへの対応等推奨事項を提供するよう求めている。

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と考えられる。IMDRF ガイダンスにおいて、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ひと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を確保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。

4.3 我が国におけるサイバーセキュリティ対応

国際的な規制調和の推進の観点や国境の枠組みを超えて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、「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）」が令和 2 年（2020 年）5 月に厚生労働省より通知された [9]。2023 年まで3年程度を目途に、医療機器製造販売業者に対して IMDRF ガイダンスの導入に向けて検討することになっている。

産業界では、この方針に基づいて、厚生労働省、PMDA をオブザーバーに迎えて、ワーキンググループをすでに立ち上げ、検討を開始している。

5. 医療機器の資産及び機能性の特定

サイバーセキュリティ対応において、その対象が、遠隔モニタリング等考慮すると医療機関内部、外部となる場合が多く存在する。モバイルヘルスはコロナウイルスの影響もあり、在宅での利活用等その適用は拡大している。その際ネットワークの構成やデータ送信の方法等十分把握、理解しておくことが重要である。

脅威モデル／脅威モデリング（Threat Model/Threat Modeling）は、開発対象のシステム又はソフトウェアがどのようなセキュリティ脅威にさらされており、攻略される可能性を持ちうるかを洗い出す活動である。潜在するセキュリティ脆弱性を上流工程で見つけ出すことによって、より効果的に脆弱性を排除することを狙う。

脅威分析（Threat Analysis & Modeling）への一歩として、侵入可能性の経路分析を行う。例えば医療機器では、USB I/F、SD I/F、CD/DVD IF、専用優先接続、有線 LAN 接続、Wi-Fi、Bluetooth 等汎用無線接続、医用テレメータ等専用無線接続等が考えられる。医療機関では、他の医療機器との接続、電子カルテ、LIS 等院内ネットワーク、医療機関外部を想定するとファイアウォールを介する。医療機関外部は、家庭用環境、診療所等モバイルヘルスの適用が考えられるが、ルータを介してインターネットと接続される。

さらに信頼境界線及びアタックサーフェイスの特定を行い、脅威の特定、脅威の分析、脅威の評価及び対策の特定を行う。機器の機能及びエンドユーザー／患者に対する脅威や脆弱性の影響評価、悪用可能性のある脅威や脆弱性が発生する可能性の評価、リスクレベルと適切な低減戦略の決定、残存リスクとリスク受容基準の評価等対応する必要がある。

6. まとめ

以上、近年の動向、IoT セキュリティガイドライン、医療機器、モバイルヘルスにおけるサイバーセキュリティの確保、IMDRF サイバーセキュリティガイドラインと説明してきた。

まとめとしては、

- 2020 年 4 月、IMDRF サイバーセキュリティガイダンスが公開され、我が国においては 2023 年を目途に、医療機器製造販売業者に対して導入が進められる。
- 製造販売業者は、開発等市販前から保守・廃棄等市販後まで製品のライフサイクル全般にわたって、対応する必要がある。
- 医療機器のサイバーセキュリティは、「規制当局への説明責任」、「ユーザーへの説明責任」、「医療機器の実質的な安全の確保」という側面から、対応する必要がある。
- 安全に影響を及ぼすセキュリティリスクのリスク低減は必須であり、その他のセキュリティリスクについてもユーザーである医療機関から対応が求められる。
- 製造販売業者は、必要に応じて医療機関と連携を取り、保守契約等に基づきサイバーセキュリティの確保を支援することが重要となる。

IMDRF ガイダンスの我が国への導入にあたっては、他の分野に比べ規制に基づく要求事項となることから国際的にも比較的高いレベルのベースラインがあると考えられる。一方、これらの取り組みや技術は、存在する国際規格や一般的に公開されている情報・手法等から構築可能なものが非常に多いと思われる。製造販売業者は、国際整合化の背景を理解し、速やかにサイバーセキュリティベースラインを構築した上で、医療機関、規制当局およびその他のステークホルダーと連携可能な体制を整備する必要がある。本稿の内容が、医療機関、製造販売業者双方にとって、患者安全を確保・維持する活動の一助となれば幸いである。

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 (Cited 2021-Aug-24)].
2) “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 (Cited 2021-Aug-24)].
3) “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 (Cited 2021-Aug-24)].
4) “Postmarket Management of Cybersecurity in Medical Devices” [https://www.fda.gov/regulatory-information/search-fda-guidance-documents/postmarket-management-cybersecurity-medical-devices (Cited 2021-Aug-24)].
5)「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
6)「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
7) “Principles and Practices for Medical Device Cybersecurity” [http://www.imdrf.org/docs/imdrf/final/technical/imdrf-tech-200318-pp-mdc-n60.pdf (Cited 2021-Aug-24)].
8)「IoT セキュリティガイドライン ver 1.0」[https://www.soumu.go.jp/main_content/000428393.pdf (Cited 2021-Aug-24)].
9)「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