JNSA調査研究部会　IoTセキュリティワーキンググループ：
日本におけるソフトウェアサプライチェーンとSBOMのこれから

医療機器におけるサイバーセキュリティ対策とSBOMの活用

一般社団法人 電子情報技術産業協会（JEITA）
ヘルスケアインダストリ部会
医療用ソフトウェア専門委員会 委員長

日本光電工業株式会社　技術戦略本部

松元 恒一郎

2023年8月25日（金）
14:40 ～ 15:10
AP市ヶ谷

自己紹介

- 日本光電工業株式会社入社
  ー生体情報モニタ開発：システム設計・ソフトウェア開発（麻酔関連、薬剤計算処理、アラーム処理等臨床に関連する機能）
  ー心電計開発、ホルター心電計開発
- 2000年頃より医用波形規約の標準化であるMFER（Medical waveform Format Encoding Rules）シリーズ（22077-XX）のISO規格作成
- ISO/TC215 Medical Informatics　WG2/WG4/JWG7/JWG3/TF5　エキスパート
- AAMI/UL 2800-1（Interoperability）プロジェクト　オブザーバー
- DICOM WG32（Neurophysiology Waveforms）オブザーバー
- HL7 Health Care Device WG・Anesthesia WG　メンバー
- 一般社団法人 電子情報技術産業協会（JEITA）ヘルスケアインダストリ部会　医療用ソフトウェア専門委員会　委員長
- 一般社団法人 日本医療機器産業連合会（医機連）
  医療機器サイバーセキュリティ対応WG　副主査、AI/SaMD-WG　副主査、AI活用プログラム医療機器における審査関連研究WG、個人情報取扱対応分科会、プログラム医療機器対応WG規制対応SWG、サイバーセキュリティの不具合報告SWG
- 厚生労働省　「医療情報システムの安全管理に関するガイドライン」改定に向けた調査一式　改定作業班　令和元年～令和2年　構成員
- 経済産業省　産業サイバーセキュリティ研究会WG１『第２層：フィジカル空間とサイバー空間のつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォース　令和元年～令和4年　委員
- 経済産業省　産業サイバーセキュリティ研究会WG1　サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォース　令和3年～　オブザーバー
- AMED 医薬品等規制調和・評価研究事業　データ等の通信機能を有する医療機器開発における相互運用性確保のためのガイダンス策定に関する研究　令和元年～　研究協力者

目次

医療機器に対するサイバーセキュリティ対応も“当たり前の時代”です

○医療機関内の情報通信の高度化が進み、有線・無線を問わず、医療機関のネットワークに医療機器を含む電子機器が接続される状況がさらに増加

医療機器については

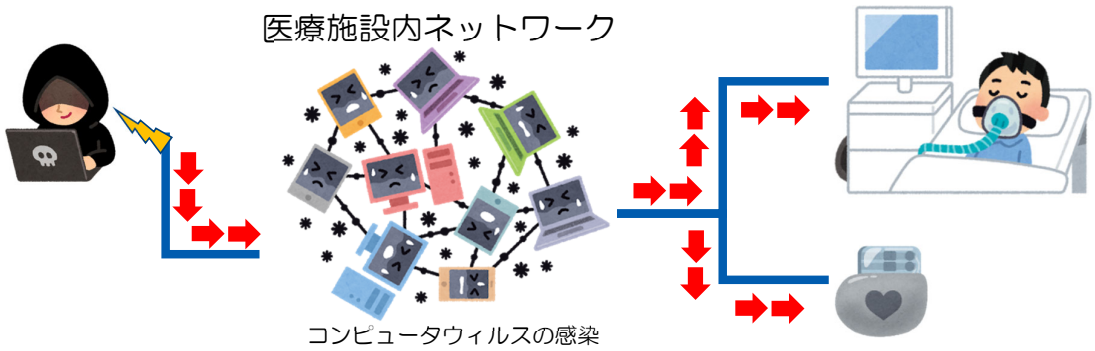
- データアクセスポート（有線・無線・記憶媒体の別を問わない）を持ち、医療情報システム等の外部機器と相互通信する。
- 医療機器の内部で使用されるソフトウェアのライフサイクル（サポート期間）に対して、医療機器自体の製品ライフサイクル（耐久年数）が長く設定されている場合もある。

➢ サイバー攻撃が行われた時には、患者・医療従事者への健康被害にもつながり得る
➢ 医療機器に対しても、不正なデータアクセスやコンピュータウイルス感染の危険性に対する対処が必要。

厚生労働省 医薬・生活衛生局 医療機器審査管理課資料より引用

医療機器へのサイバーリスクとその対応の基本的考え方

事例）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際に、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。



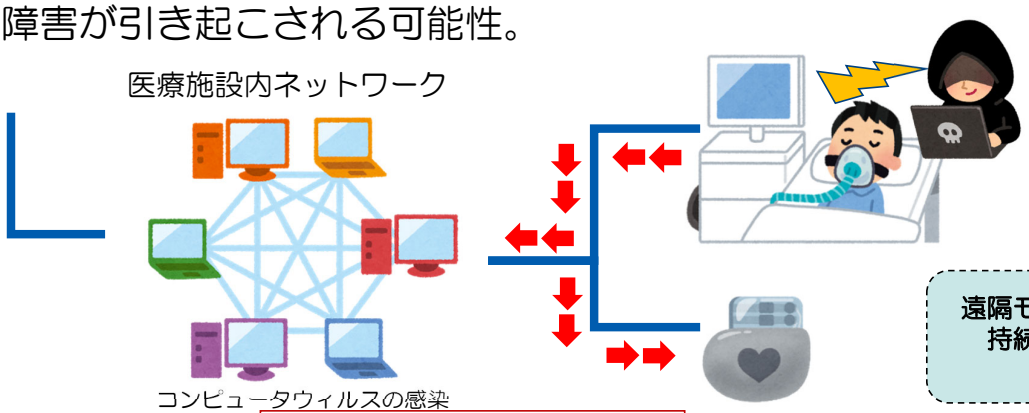
このリスクを低減するために

基本的考え方①
医療機器が<u>サイバー攻撃による影響を受けない</u>ように、<u>製品としての耐性</u>を持ち、かつ、<u>医療施設/医療機関内での管理</u>がなされることが必要。

厚生労働省 医薬・生活衛生局 医療機器審査管理課資料より引用、一部改変

医療機器へのサイバーリスクとその対応の基本的考え方

事例）医療機器がサイバー攻撃を受けた際に、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。



遠隔モニタリング医療
持続的データ通信
RWD

このリスクを低減するために

基本的考え方②
<u>医療機器が感染源にならない</u>ように<u>設計・製造</u>され、かつ、<u>市販後に適正な管理</u>がなされることが必要。

厚生労働省 医薬・生活衛生局 医療機器審査管理課資料より引用

セキュリティリスクの変遷 -1

2012年8月　GAOレポート
- 植え込み型除細動器、インスリンポンプ、無線接続可能医療機器
- FDAはこのような機器の情報セキュリティへの考慮を拡大すべき

GAO: United States Government Accountability Office, 米国政府説明責任局

2013年　**医療機器を調査**
- 米国ICS-CERT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(6月13日)
  (約40ベンダーの約300の医療機器)
- FDAがMedical Device Cybersecurityに関するガイダンスのドラフトを公開(6月14日)

2014年　**医療機器へのサイバー攻撃**（標的型攻撃の入口に）
- 医療機器のハッキングは，容易(4月25日)
  (薬物注入ポンプやX線検査装置が容易にハッキングできる)
- 米国の病院に中国からサイバー攻撃、患者450万人のデータが流出(8月19日)
  (狙われたのは，医療機器の開発・研究（治験）データなどの知的財産)

2015年　**医療機関への攻撃**
- 病院の侵入に医療機器が悪用される(6月8日)
  (医療機器にバックドア)
- GEの複数の医療機器に複数の脆弱性が公開(7月10日)
- FDAがHospira Lifecare PCA Infusion Systemの利用中止を指示(7月31日)
  当該製品が遠隔的に病院のネットワークを通してアクセス可能であり、権限のないユーザーがポンプの注入量を変更することが可能な状況にあることが確認された。

セキュリティリスクの変遷 -2

2017年以降　**ランサムウェア「WannaCry」への大規模感染が始まる**

2020年9月　**医療機関へのサイバー攻撃**
- First death reported following a ransomware attack on a German hospital
  独デュッセルドルフ大学病院が、ランサムウェア攻撃を受けた。同病院が院内の30台以上のサーバに感染したランサムウェア攻撃に対応中に、同病院に救急搬送される予定だった女性患者を受け入れることができず、この患者は30km以上離れた別の病院へ搬送されることになり、死亡。

2021年8月　**BlackBerry OSの脆弱性：車の所有者や病院にとって深刻な悪材料**
- BlackBerry OS vulnerability is seriously bad news for car owners, hospitals
- BlackBerry社、同社の組み込みOSであるQNXにメモリ関数の使用に起因する複数の脆弱性「BadAlloc」が存在することを認めた。
- 今年初めにこの脆弱を発見したMicrosoft社が、米国サイバーセキュリティ・インフラストラクチャセキュリティ庁（CISA）に報告した。
- 数百万台の自動車、病院や工場の重要な機器がハッカーに悪用される可能性がある。
- 厚生労働省からも協調（調整）と情報開示された。

2021年10月　**ランサムウェア攻撃：新生児の死をめぐって**
- 2019年7月に臍帯を首に巻いて生まれ、9ヶ月後に亡くなった大きな脳損傷を引き起こしたと裁判所文書は述べている。
- 2020年6月に提出された法廷文書では、弁護士は、スプリングヒル医療センターとその親会社がサイバー攻撃を防ぐのに十分なことをしておらず、状況の深刻さを隠すために共謀したと非難している。
- この訴訟は、身代金攻撃が電子機器の故障をもたらしたと主張しており、医師は出産中に子供の状態を適切に監視できず、脳損傷を引き起こした。

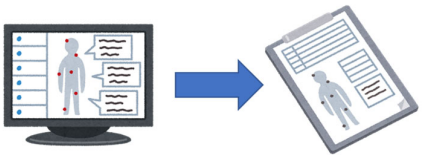
国内のサイバー攻撃の事例

患者，医療従事者へ多大なる影響を及ぼした事例

2018年10月18日　宇陀市立病院（奈良県）

攻撃の内容

- 電子カルテシステムへのランサムウェア攻撃。
- 電子カルテシステムを全面停止して、紙カルテの運用へ切り替え。
- 停止期間は、2日間。
- 個人情報の漏えいや悪用といった被害報告はなし。



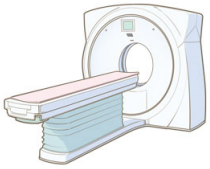
原因

- ウイルスの感染源を特定することはできず。
- しかし、**医療情報システムに私物のパソコンやネットワーク機器を接続しないという基本的なルールが遵守されなかった**ことによって発生した可能性。

2017年8月～2018年1月　福島医大病院（福島県）

攻撃の内容

- 検査装置へのランサムウェア攻撃。
- CT撮影中に端末が再起動を起こし、撮影画像が保存されていなかったことで再撮影を施行。
- 撮影した画像の読み取りができなかったことで再撮影を施行。



原因

- **ランサムウェアに感染していた端末を院内ネットワークに接続した**ことによる感染。

AMEDサイバーセキュリティ研究班資料より引用

2021年6月28日　厚労省通知：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)

- ４月30 日付けで発出された内閣官房内閣サイバーセキュリティセンターからの注意喚起について、改めて貴管内の医療機関に対し周知するとともに、ランサムウェアによるサイバー攻撃の解説及び対策例を参考に関係医療機関に対し注意喚起。

2021年10月　ランサムウェア攻撃：徳島県つるぎ町立半田病院

- 10月31日、電子カルテ他院内システムがランサムウェアに感染し、カルテが閲覧できなくなるなどの大きな被害。
- 調査復旧を請け負った事業者の作業、電子カルテ業者の仮システムの構築、そして、電子カルテより必要に応じて抽出していたデータなどを利用し、令和4年1月4日に通常診療を再開。

2022年10月　ランサムウェア攻撃：大阪急性期・総合医療センター

- 10月31日、電子カルテ他院内システムがランサムウェアに感染し、カルテが閲覧できなくなるなどの大きな被害。
- 通常の外来診療や緊急以外の手術を停止しているほか、救急患者の受け入れもできない状況。
- 11月10日厚生労働省より「医療機関等におけるサイバーセキュリティ対策の強化について（注意喚起）」が発出。
- 攻撃の侵入経路は、医療機関自身のシステムではなく、院外の調理を委託していた事業者のシステムを経由したものである可能性が高いことが判明。
- サプライチェーンリスク全体の確認として、自組織のみならずサプライチェーン全体を俯瞰し、発生が予見されるリスクを医療機関等自身でコントロールできるようにする必要があることから、関係事業者のセキュリティ管理体制を確認した上で、関係事業者とのネットワーク接続点（特にインターネットとの接続点）をすべて管理下におき脆弱性対策を実施する。

医療における情報セキュリティに関する脅威やインシデント

近年、「外的要因」かつ「意図的な事象」に脅威・インシデントの傾向が変化しつつある。

外的要因

外部事業者等によるミス

- 外部事業者の情報紛失
- 外部事業者の設定ミス

(事例)
- 外部事業者の設定ミスにより、患者70人分の個人情報が含まれたファイルがインターネットを経由し、アクセス可能な状態となり、個人情報が漏洩する恐れがあった。

外部からの攻撃

- Webサイト、保守回線等を経由した攻撃
- ランサムウエアやマルウエアなど、
- システムの様々な脆弱性を利用した攻撃

近年、「外部からの攻撃」が増加傾向にあり、医療機関個々での単独対策には限界がある。

偶発的 ― 意図的

医療従事者によるミス

- USBメモリやPCの紛失・盗難
- FAXやメールの誤送信
- 誤操作によるファイルのアップロード

(事例)
- 医師が患者約330人分の手術記録を保存したUSBメモリを紛失した。
- 薬剤師が、糖尿病・内分泌代謝内科を受診した患者3,835人の氏名や生年月日などの個人情報を保存したUSBメモリを紛失した。

内部不正

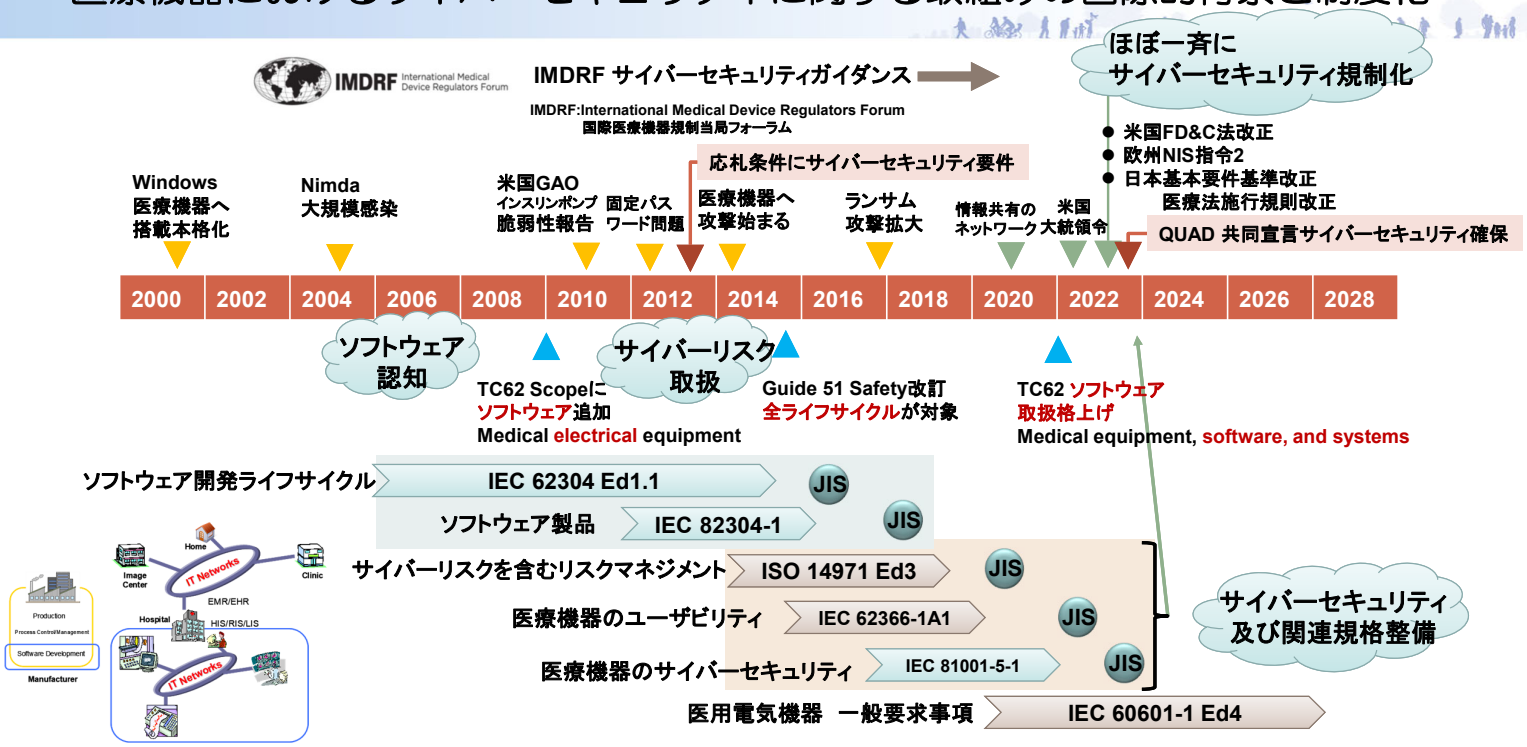
- 職員による、機密情報、個人情報等の持ち出し
- 委託事業者による機密情報、個人情報等の持ち出し

(事例)
- 元職員が、在職中に患者の個人情報を持ち出し、新しく開設する介護事業所の案内状送付に利用した。

内的要因

参照：https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryou/iryou/johoka/cyber-security.html、一部改変

医療機器におけるサイバーセキュリティに関する取組みの国際的背景と制度化



引用：2023年5月31日JIRA政策企画会議「医療機器におけるサイバーセキュリティの取り組みと課題」講演資料

国際整合に向けた組織　GHTF / IMDRF

1992～2012　GHTF（Global Harmonization Task Force）

- 参加者：規制当局及び産業界代表者

日本　オーストラリア　カナダ　ヨーロッパ　アメリカ

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。（基本要件基準、クラス分類ルール等々）

一部、IMDRFが改定

2011～現在　IMDRF（International Medical Device Regulators Forum）

- 参加者：管理委員会は、規制当局
  作業グループは、産業界も参加

（2020/2/19現在）

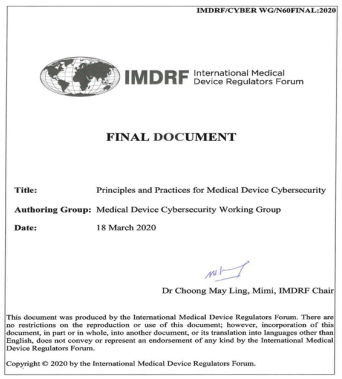
日本　オーストラリア　カナダ　ヨーロッパ　アメリカ

ブラジル　中国　ロシア　シンガポール　韓国

IMDRF サイバーセキュリティガイダンス

Principles and Practices for Medical Device Cybersecurity
（医療機器サイバーセキュリティの原則と実践）

IMDRF/CYBER WG/N60FINAL:2020
2020/03/18付，2020/04/20公開


IMDRF/CYBER WG/N60FINAL:2020

IMDRF International Medical Device Regulators Forum

FINAL DOCUMENT

Title: Principles and Practices for Medical Device Cybersecurity
Authoring Group: Medical Device Cybersecurity Working Group
Date: 18 March 2020

Dr Choong May Ling, Mimi, IMDRF Chair

This document was produced by the International Medical Device Regulators Forum. There are no restrictions on the reproduction or use of this document; however, incorporation of this document, in part or in whole, into another document, or its translation into languages other than English, does not convey or represent an endorsement of any kind by the International Medical Device Regulators Forum.

Copyright © 2020 by the International Medical Device Regulators Forum.

一般原則

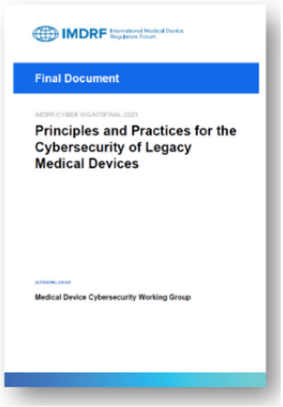
①共同責任
②国際調和
③製品ライフサイクル
④情報共有

- 医療機器（IVD医療機器を含む）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はあるがこの文書の適用範囲ではない。（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**する。**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する。）
- サイバーセキュリティは、**製造業者、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**を対象とする。
- **市販前の考慮事項**として、**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についての推奨事項を提供**する。
- **市販後の考慮事項**として、**意図する環境における機器の運用、情報共有、協調的な脆弱性の公開、脆弱性の修正、インシデントへの対応及びレガシー医療機器についての推奨事項を提供**する。

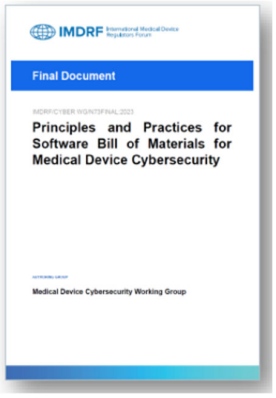
1．はじめに
2．適用範囲
3．定義
4．一般原則
5．医療機器サイバーセキュリティの市販前考慮事項
6．医療機器サイバーセキュリティの市販後考慮事項
7．参考文献
8．附属書

国際医療機器規制当局フォーラム（IMDRF）ガイダンス

原則
基礎概念



応用・実践



2020年4月公開

<N60 原則及び実践概要>
- 各国規制当局の共通概念としてまとめられたもの
- 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、積極的な連携及び情報共有が重要であることを言及

2023年4月公開

<N70 レガシー医療機器概要>
- 老朽化の理由のみでその製品がレガシー医療機器であると判断してはならないことも重要（発売開始直後の医療機器であっても、発生したの脆弱性に対して合理的な手段で保護できない場合等）
- レガシー医療機器の使用を終了又は段階的に使用を終了するための概念フレームワークについても言及

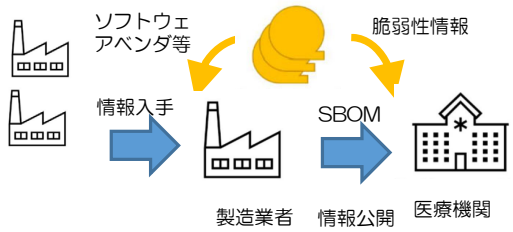
2023年4月公開

<N73 SBOM概要>
- 医療機関等が、医療機器及び接続されるシステムに対する脆弱性の潜在的な影響を理解し、医療機器の安全性及び基本性能を維持することが可能
- 製造販売業者は、医療機器で使用されているコンポーネントを可視化して顧客に提示し、購入決定及び運用保守に必要な情報を提供することが可能

IMDRFガイダンスの3つのキーワード

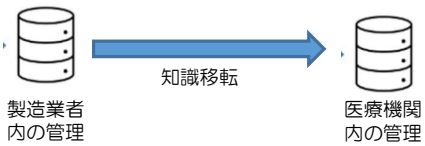
- **Software Bill of Materials（SBOM）**

  医療機器に実装される商用・オープンソース及び市販のソフトウェア部品のサイバーセキュリティに関する情報を提供するための部品表



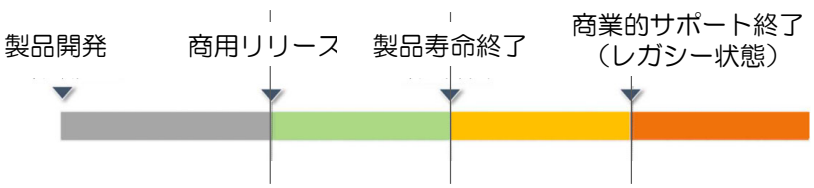
- **Coordinated Vulnerability Disclosure（CVD）「協調的な脆弱性の開示」**

  脆弱性の発見者から情報収集し、関係者間における情報共有などのサイバーセキュリティを確保する各種調整を実施した上で、脆弱性の情報を公開する活動



- **Legacy Medical Device**

  現在のサイバーセキュリティの脅威に対して合理的に保護できない医療機器



※サポートレベルは、顧客との契約に応じて異なる

JEITA医療機器ソフトウェアの最新技術動向セミナー（2022年5月）より引用

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

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では目的や位置付けが異なる事から、主体となる組織や適用範囲が異なるので注意。

【医療情報システムの安全管理に関するガイドライン】
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。

※根拠法：個人情報保護法、e文書法

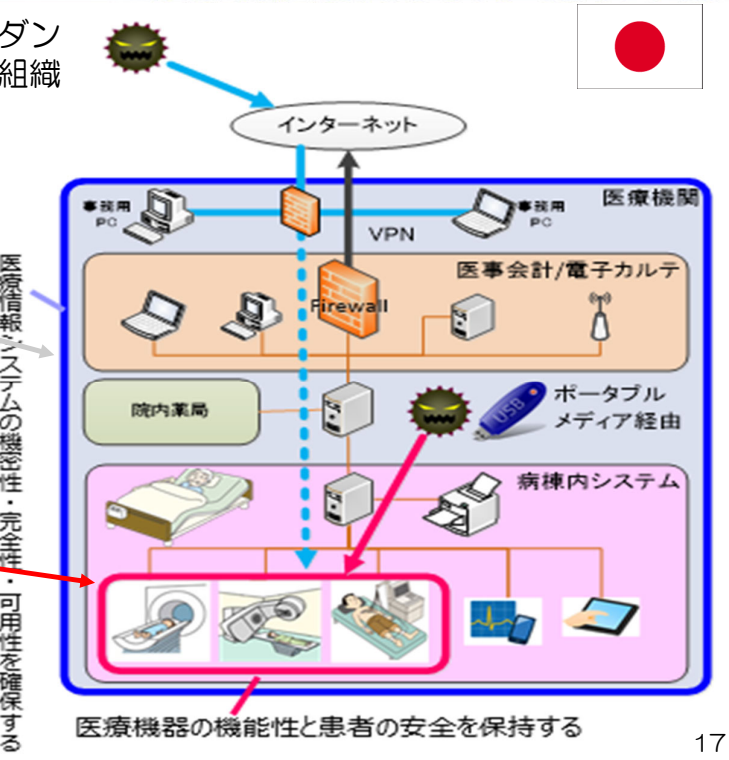
※1 医療情報システムの安全管理に関するガイドライン　第5版（平成29年5月）、第5.2版（令和4年3月）、 第6.0版（令和5年5月）公開

【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】
医療機器製造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。
※医療機関に対して必要な情報提供及び連携を図る。

※根拠法：医薬品医療機器等法

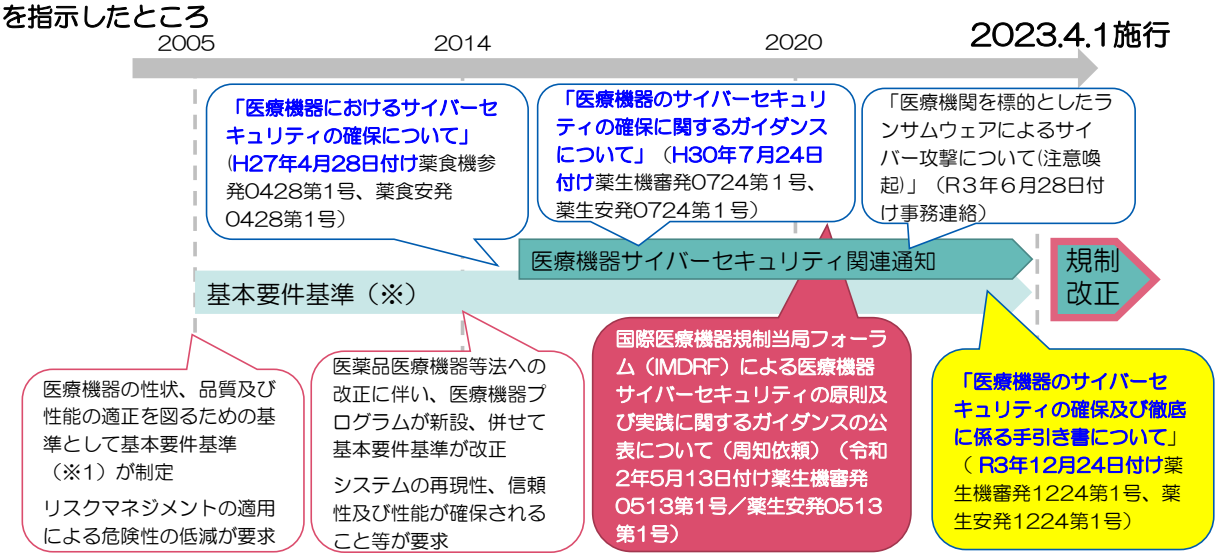
※2 医療機器のサイバーセキュリティの確保に関するガイダンスについて（平成30年7月24日）

JEITA医療機器ソフトウェアの最新技術動向セミナー（2020年2月19日）より引用，一部改変



医療機器を取り巻くサイバーセキュリティの動向 ～日本における医療機器サイバーセキュリティ対応の経緯～

我が国では、平成27年に医療機器に対するサイバーセキュリティ対応を明確化し、製造販売業者に対する対応を指示したところ



※　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、平成26年厚生労働省告示403号一部改正）

令和２年３月、国際医療機器規制当局フォーラム（IMDRF）において、「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」が取りまとめられた

目的

- 国際的な規制調和の観点及び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策定されたIMDRFガイダンスの要求事項を踏襲。
- 医薬品医療機器等法を遵守し、医療機器の品質，有効性及び安全性を確保するために、製造販売業者が、本邦の医療機器に対して導入するための対応及び組織的な取組みを行うための情報を提供。
- 製造販売業者が適切な対応を実施し、製品ライフサイクル全体（Total Product Life Cycle）を通じサイバーセキュリティに関するリスクを低減し、医療機器製品の安全性と基本性能を確保することで、患者への危害の発生及び拡大の防止に繋げる。

製造販売業者の責任の明確化

適用範囲：サイバーセキュリティが求められている医療機器

- 無線又は有線により，他の機器・ネットワーク等との接続が可能なプログラムを用いた医療機器（ソフトウェア単独で医療機器となる医療機器プログラム（Software as a Medical Device：SaMD）を含む）及びプログラムを用いた附属品等に関するサイバーセキュリティを対象。
- 適用の要否は、医療機器のクラス分類（Ⅰ～Ⅳ）だけで判断すべきではなく、意図する使用環境、サイバーリスクに応じた危害等を考慮したリスクベースアプローチによって判断。
- 患者又はユーザーへの危害が発生する可能性のあるサイバーセキュリティリスクに限定。
  - ✓ 製品の性能に悪影響を与える。
  - ✓ 臨床活動に悪影響を与える。
  - ✓ 誤った診断，治療又は予防に繋がる

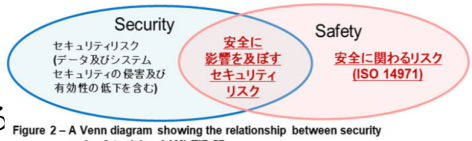
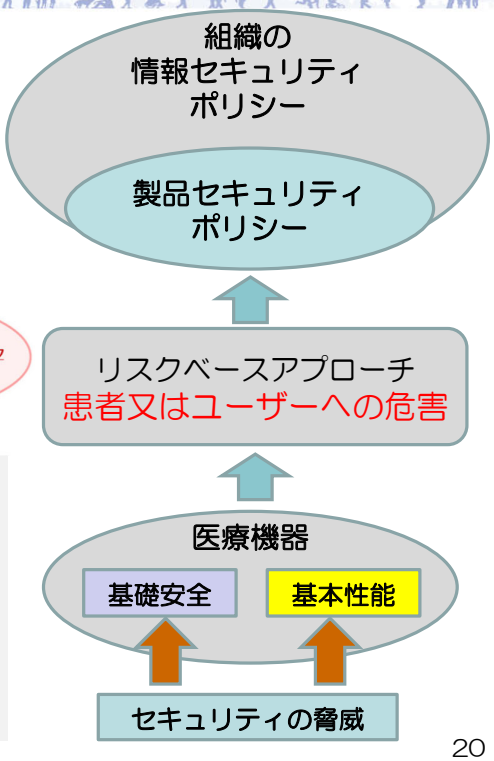


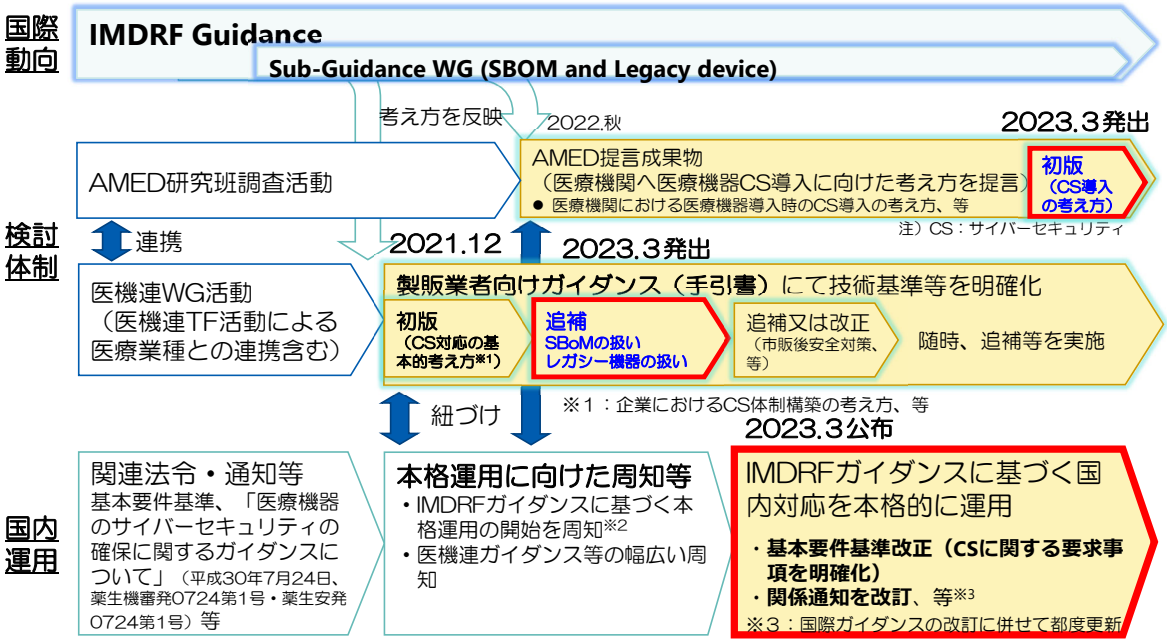
Figure 2 – A Venn diagram showing the relationship between security and safety risks AAMI TIR 57

医療機器は、患者等の個人情報等を扱う医療情報システムの一部としてもみなされるため、データプライバシー等の情報セキュリティに係るリスクへの対応も実施される必要があるが、この文書の適用範囲ではない。情報セキュリティに係る対策については、別途安全管理ガイドライン等を参照する。また、製造販売業者の一般的な企業活動に関するサイバーセキュリティ対応についてもこの文書の適用範囲から除外しているため、医療機器の製造販売業者は、一般的な個人情報の漏洩等の危害についても十分な対応をすることが社会的に求められていることに留意すべきである。



[厚労科研市販後安全対策]サイバーセキュリティに関する研究資料より引用，一部改変

医療機器のサイバーセキュリティについて
～IMDRFガイダンスの国内導入に向けた検討状況～(令和5年3月時点)



※2「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」
（令和３年12月24日薬生機審発1224第１号・薬生安発1224第１号）

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の一部を改正する件（案）について（概要）

■ 改正の趣旨
令和２年３月に国際医療機器規制当局フォーラム（IMDRF）において、「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」が取りまとめられたことに伴い、そのガイダンスの一部の文書（IMDRF N47及びN60文書）の内容を踏まえた医療機器プログラムにおける基本要件基準の改正を行う。

N47:2018-医療機器および IVD 医療機器の安全性と性能に関する基本原則

■ 改正の内容
IMDRF ガイダンスにおいて取りまとめられたサイバーセキュリティを確保するための要件として、次の**３つの観点を基本要件基準に盛り込む改正**を行う。

① **製品の全ライフサイクル**に渡って医療機器**サイバーセキュリティを検討する計画**を備えること。
② **サイバーリスクを低減する設計及び製造**を備えること。
③ 適切な**動作環境に必要となる**ハードウェア、ネットワーク、IT **セキュリティ対策の最低限の要件を設定**すること。

■ 根拠規定
法第41 条第３項

■ 告示日等
告示日：　令和5年3月9日
適用期日：　令和5年4月1日

サイバーリスク対応の基本的考え方①
医療機器が**サイバー攻撃による影響を受けない**ように、**製品としての耐性**を持ち、かつ、**医療施設内での管理**がなされることが必要。

サイバーリスク対応の基本的考え方②
医療機器が感染源にならないように**設計・製造**され、かつ、**市販後に適正な管理**がなされることが必要。

医療機器の基本要件基準（第十二条）改正案

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（昭和三十五年法律第百四十五号） 第四十一条第三項の規定に基づき、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（平成十七年厚生労働省告示第百二十二号）

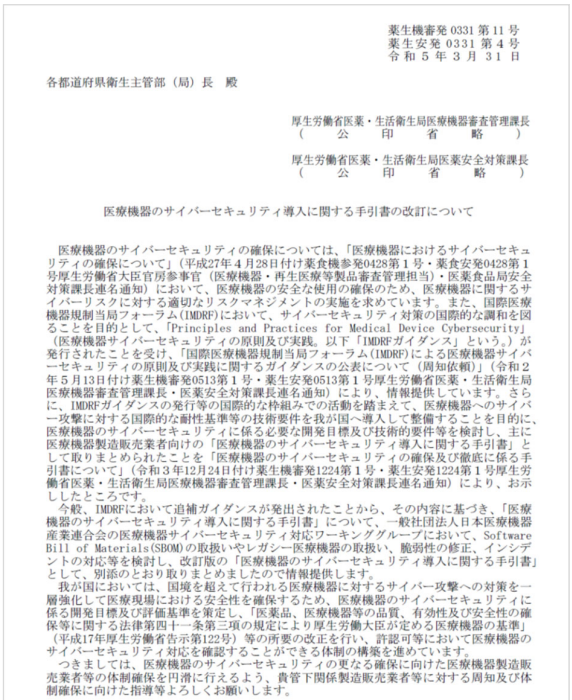
（プログラムを用いた医療機器に対する配慮）
第１２条
１．プログラムを用いた医療機器（医療機器プログラム又はこれを記録した記録媒体たる医療機器を含む。以下同じ。）は、その使用目的に照らし、システムの再現性、信頼性及び性能が確保されるよう設計されていなければならない。また、システムに一つでも故障が発生した場合、当該故障から生じる可能性がある危険性を、合理的に実行可能な限り除去又は低減できるよう、適切な手段が講じられていなければならない。

２．プログラムを用いた医療機器については、最新の技術に基づく開発のライフサイクル、リスクマネジメント並びに当該医療機器を適切に動作させるための確認及び検証の方法を考慮し、その品質及び性能についての検証が実施されていなければならない。

３．プログラムを用いた医療機器のうち、他の機器及びネットワーク等と接続して使用する医療機器又は外部からの不正アクセス及び攻撃アクセス等が想定される医療機器については、当該医療機器における動作環境及びネットワークの**使用環境等を踏まえて適切な要件を特定**し、当該医療機器の機能に支障が生じる又は安全性の懸念が生じるサイバーセキュリティに係る**危険性を特定及び評価**するとともに、当該**危険性が低減する管理**が行われていなければならない。また、当該医療機器は、当該医療機器の**ライフサイクルの全てにおいて、サイバーセキュリティを確保**するための**計画に基づいて設計及び製造**されていなければならない。

新設

製販業向け手引書 - 2023年3月31日 第2版発出



薬生機審発 0331 第 11 号
薬生安発 0331 第 4 号
令 和 5 年 3 月 31 日

各都道府県衛生主管部（局）長　殿

厚生労働省医薬・生活衛生局医療機器審査管理課長
（　公　　印　　省　　略　）

厚生労働省医薬・生活衛生局医薬安全対策課長
（　公　　印　　省　　略　）

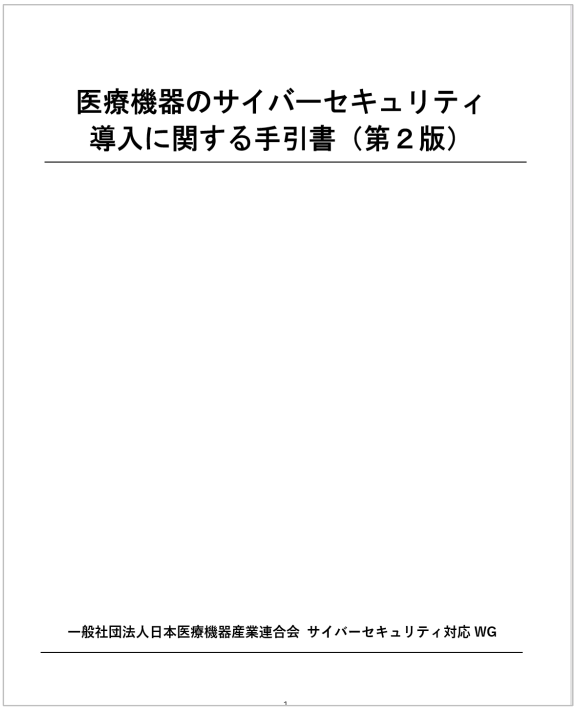
医療機器のサイバーセキュリティ導入に関する手引書の改訂について

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、国際医療機器規制当局フォーラム（IMDRF）において、サイバーセキュリティ対策の国際的な調和を図ることを目的として、「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。以下「IMDRFガイダンス」という。）が発行されたことを受け、「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）により、情報提供しています。さらに、IMDRFガイダンスの発行等の国際的な枠組みでの活動を踏まえて、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我が国へ導入して整備することを目的に、医療機器のサイバーセキュリティに係る必要な開発目標及び技術的要件等を検討し、主に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」として取りまとめられたことを「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」（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・医薬安全対策課長連名通知）により、お示ししたところです。

今般、IMDRFにおいて追補ガイダンスが発出されたことから、その内容に基づき、「医療機器のサイバーセキュリティ導入に関する手引書」について、一般社団法人日本医療機器産業連合会の医療機器サイバーセキュリティ対応ワーキンググループにおいて、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、改訂版の「医療機器のサイバーセキュリティ導入に関する手引書」として、別添のとおり取りまとめましたので情報提供します。

我が国においては、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を策定し、「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）等の所要の改正を行い、許認可等において医療機器のサイバーセキュリティ対応を確認することができる体制の構築を進めています。

つきましては、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の体制確保を円滑に行えるよう、貴管下関係製造販売業者等に対する周知及び体制確保に向けた指導等よろしくお願いします。



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）

一般社団法人日本医療機器産業連合会　サイバーセキュリティ対応 WG

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・生活衛生局医薬安全対策課長連名通知

医療機器のサイバーセキュリティ導入に関する手引書ー追補ー

基本　→　実践

背景
1. 目的
2. 適用範囲
3. 用語及び参考定義
4. 一般原則　（4原則）
5. 市販前考慮事項
   - 5.1. セキュリティ要求事項及びアーキテクチャ設計
   - 5.2. TPLCに関するリスクマネジメント原則
   - 5.3. セキュリティ試験
   - 5.4. TPLCサイバーセキュリティマネジメント計画
   - 5.5. 顧客向け文書
   - 5.6. 規制当局への申請に関する文書
6. 市販後考慮事項
   - 6.1. 意図する使用環境における機器の運用
   - 6.2. 情報共有
   - 6.3. 協調的な脆弱性の開示（CVD）
   - 6.4. 脆弱性の修正
   - 6.5. インシデントへの対応
   - 6.6. レガシー医療機器
7. 業許可に関する考慮事項
   - 7.1. 業許可をもつステークホルダーの役割
   - 7.2. リース医療機器の扱い
   - 7.3. 中古医療機器の扱い

附属書（規定）
A. ソフトウェア部品表（SBOM）の扱い

脆弱性マネジメントの視点から、全体を補充
6.4. 脆弱性の修正
- 脆弱性発見（インシデント未発生）でも不具合報告に至る可能性を示す。

6.5. インシデントへの対応
- 緊急対応、予防的活動、不具合報告、情報共有を具体化

6.6.、6.6.2をIMDRF追補ガイダンスから補充
6.6.3　補完的リスクコントロール追加

- 製販業者：　関連する製造業者、販売業者、貸与業者に対し必要な情報提供
- 販売業者：　販売時に、規則に従い製造販売業者へ確認
- 販売業者：　医療機関（使用者）に情報提供
- 製販業者が定めたEOLを超えた製品の扱い

IMDRFの追補ガイダンスを基本として追加

6.6.　レガシー医療機器
6.6.1.　TPLCとレガシー医療機器
6.6.2.　TPLCにおける責任・考慮事項
6.6.2.1.　設計・開発段階
6.6.2.2.　サポート段階
6.6.2.3.　限定的サポート段階
6.6.2.4.　サポート終了段階
6.6.3.　補完的リスクコントロールに関する考慮事項

A.　ソフトウェア部品表（SBOM）の扱い
A.1　SBOMの生成
A.2　SBOMの要素と推奨フォーマット
A.3　SBOMの提供
A.4　SBOMの事例

医療機関と医療機器製造販売業者で想定される課題

[医療機関]

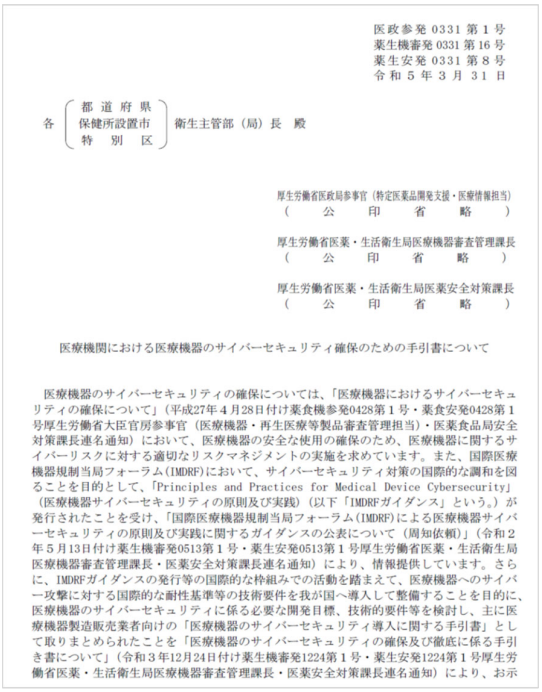
- サイバーセキュリティ対応の重要性は理解するが、具体的に何をすれば良いのか分からない。
- メーカーから十分な情報が提供されない、提供させる情報の内容（意味）が分からない。
- 医療機器の選定にあたり、それぞれのサイバーセキュリティ対応の状況が分からない。
- 稼働中の医療機器のEOSが近づいていると言われたが買い替えは困難。
- 対策を実施するための人材がいない、コストも掛けられない（体制を整備することが困難）。

[医療機器製販業者]

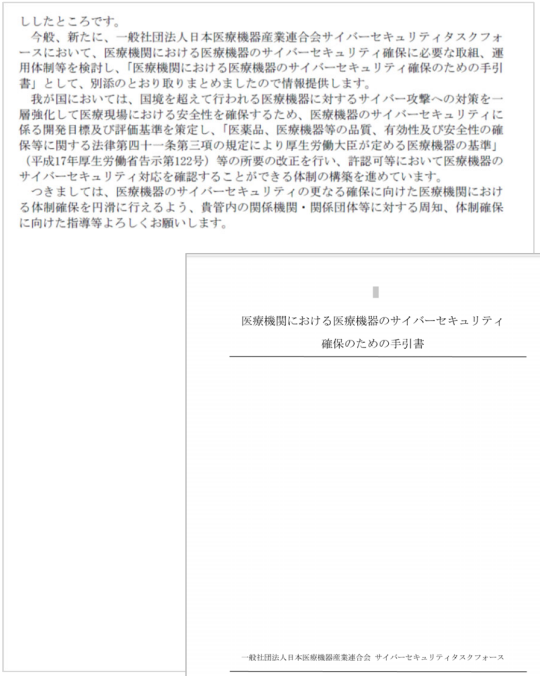
- 医療機関からのインシデント情報などの運用状況についての情報が得られない。
- 保守契約等が無いと、必要な対応が出来ない。
- 医療機関（特に開業医等小規模なところ）の実態把握が困難。
- 情報を提供しても理解、活用してもらえない（理解してもらうのに手間がかかる）。
- どの時期にどこまでの情報を提供すれば良いのか分からない。
- リモートメンテナンスに専用回線を使用するなどでコストがかかることに理解が得られない。

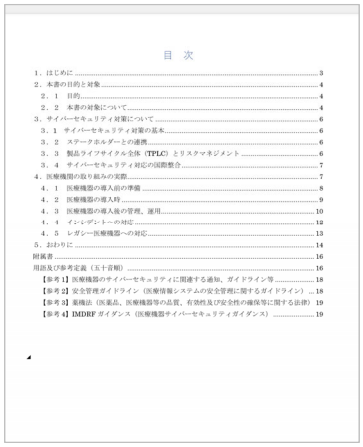
⇨ 医療機関と製造販売業者が、連携して対応する仕組みの構築が必要

医療機関向け手引書 - 2023年3月31日 発出



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
厚生労働省医政局特定医薬品開発支援・医療情報担当参事官室/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連名通知





「医療機関向け手引書」の作成

目的、対象者（読者）、位置付け

- 医療機関等で使用される医療機器のサイバーセキュリティを確保することにより、医療安全が確保された円滑な運用に資することを目的とし、医療機関等で必要となる対応について説明する。
  - 医療機関、医療機器製販業者を中心に、すべてのステークホルダーの役割と連携を明確にする。
  - 患者安全(セーフティ)が中心。情報セキュリティ確保との関係にも触れる。
- 主な対象（読者）は，医療機関等（大規模から小規模）の管理者を想定。
  - 大規模施設：経営者、医療機器安全管理責任者、医療情報システム管理者、医療機器・医療情報システム運用担当者。
  - 小規模施設：経営者（業者等に適切な指示を出すために）。

「医療機関向け手引書」の概要

4．医療機関の取り組みの実際

医療機関と医療機器事業者がサイバーセキュリティ対策・インシデント対応で行うこと（概要）

ステータス		医療機関	医療機器事業者（その他ステークホルダーを含む）
医療機器の導入まで	導入前の準備	●サイバーセキュリティポリシーの確立（医療情報セキュリティ体制の構築等） ●IT インフラの構築・ネットワーク構成図の整備 ●関係者の教育 ●アップデートオプション、保守計画の確認	○提供文書の作成 ・注意事項等情報及び取扱説明書 ・顧客向けセキュリティ文書（システム（ネットワーク）構成図、MDS2、SBOM 等）
	導入時	●医療機器に関する情報の確認 ●保守・サービスに関する役割・責任の明確化、契約締結 ●インシデント発生時の対応手順の確立	○必要情報の提供 ○保守・サービスに関する役割・責任の明確化、契約締結 ○インシデント発生時の連携体制の確認
医療機器の導入後	通常時の管理、運用	●意図する使用環境における機器の運用 ●情報共有 ●協調的な脆弱性の開示（CVD） ●脆弱性の修正	○情報収集、提供 ○脆弱性に関するセキュリティアドバイザリー情報、修正や指示等の提供 ○協調的な脆弱性の開示（CVD）
	インシデント発生時の対応	●インシデント状況の把握 ●関係方面への報告、広報 ●対応手順の実行 ●発生後のインシデントの情報整理、対応手順や通常時の管理、運用へのフィードバック	○医療機関との連携活動 ○規制当局等への報告、情報提供 ○医療機器等の対応
	レガシー状態での対応	●限定的なサポート期間、サポート終了の確認と理解 ●サポート終了後、使用を継続することに対するリスクマネジメントの実施 ●本体では対応が困難な脆弱性の暴露によって、突然レガシー状態となった場合の対応	○限定的なサポート期間、サポート終了の情報提供 ○連携した対応 ○補完的対策を含む緩和策の提供

SBOMに関する検討

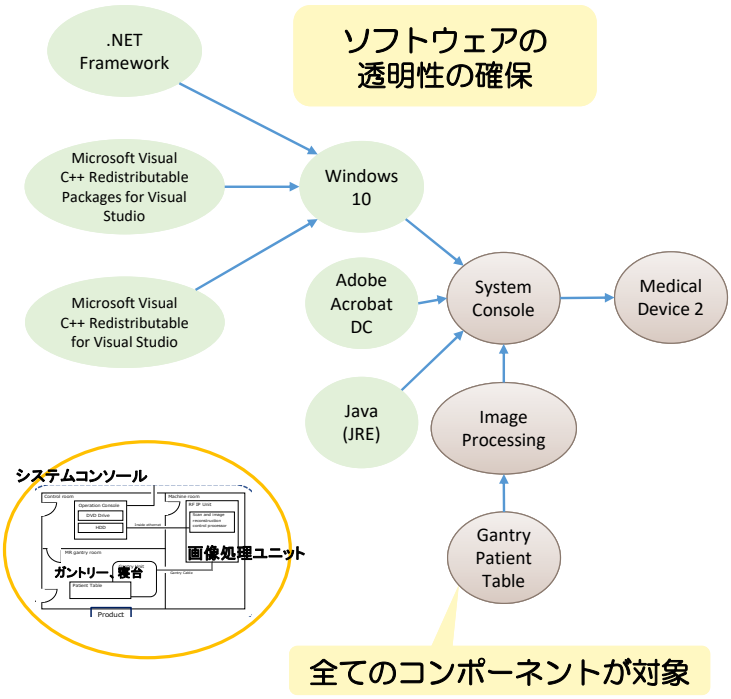
- NTIA“Minimum elements”ベースで検討が進んでいる。
- NTIA：Health Care、Energy Proof　CISA：Sharing、Adoption、Cloud, Tooling
  NTIA：National Telecommunications and Information Adminisration
  CISA：Cybersecurity & Infrastructure Security Agency
- SBOM　製販業　医療機関（ユーザー）共有のためのテンプレート
  電子フォーマット化、契約情報重視のSPDXを標準とする可能性
  -> 直接読込（取込）のためmachine-readableとする
- 製販業者が公開売るアドバイザリーレポートもテンプレートを特定化
  -> 直接読込（取込）のためmachine-readableとする
- VEX（Vulnerability Exploitable eXchange）等ツールによる脆弱性診断の自動化を強く意識
- 2023年7月28日付　経済産業省　産業サイバーセキュリティ研究会WG1　サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォース
  「ソフトウェア管理に向けたSBOMの導入に関する手引」
  https://www.meti.go.jp/press/2023/07/20230728004/20230728004.html

目的：

本手引では、SBOMに関する基本的な情報やSBOMに関する誤解と事実を提供するとともに、企業のSBOM導入を支援するために、SBOM導入に向けた主な実施事項及び導入にあたって認識しておくべきポイントを示す。

SBOMの記載項目

要　素	内　　容
ソフトウェアコンポーネントのサプライヤーの名前	コンポーネントの作成、定義又は識別を行うエンティティ
ソフトウェアコンポーネントの名前	サプライヤーが定義してソフトウェアユニットに割り当てた名称
ソフトウェアコンポーネントのバージョン	以前のバージョンからの変更を特定するためにサプライヤーが用いる識別子
固有識別子	コンポーネントを識別するために使用する、又は関連するデータベースのルックアップキーとして機能する識別子
コンポーネントハッシュ	コンポーネントのバイナリーを識別するために用いる暗号化ハッシュ
関係	上流のコンポーネントXがソフトウェアYに含まれているという関係を特徴づける情報
作成者名	SBOMエントリーの作成者
タイムスタンプ	SBOMデータの集約を行った日時の記録



SBOMの作成・運用方針の確立（脆弱性検知能力）-1

- SBOM作成対象
  - 機器コンポーネント単位で作成
    - OS部分と自製プロプラエタリソフトウェア（proprietary software）部分のSBOM
      商用のソフトウェアか否かを問わず、ソースコードが公開されているオープンソースソフトウェアに対して、非公開のものは、プロプライエタリ」などと呼ばれる。
    - サードパーティ製ソフトウェアは、サプライヤ作成SBOMを入手し、別ファイルとして添付
- SBOMフォーマット
  - 相互変換可能な形式を採用（SPDX Data license: CC0-1.0パブリックドメイン）
    - spdx-json形式、 相互変換可能な xlsx形式等
- SBOM作成方法
  - OS部分のSBOM （パッケージマネージャー等の利用）
  - サードパーティ製ソフトウェアのSBOMの入手、生成
  - 自製プロプラエタリソフトウェアのSBOM
    - ソースコード静的解析、実行ファイルへのバイナリ静的解析等

SBOMの作成・運用方針の確立（脆弱性検知能力）-2

- SBOM管理・提供
  - SBOM情報及び更新情報の入手
    - サードパーティ製ソフトウェアサプライヤーとの契約の締結、充実
      - サプライヤーと契約を結び、SBOM、脆弱性情報の提示を明確にする。
      - 脆弱性情報についてサプライヤーは定期的な情報提供、製販業者は必要に応じて提供を求めるよう進める。
  - SBOM作成
    - 初版確定、バージョンアップ及び他の正式リリース時
    - 脆弱性情報アドバイザリーとしてのSBOM提供

脆弱性情報の共有の必要性
サプライヤーと製販業者との連携・・・
業界の枠を超えて・・・
National DBの構築・・・

継続して取り組む課題

- サイバーセキュリティに関する組織力、リソース拡充（講習会等周知活動）
- 市販後安全対策、保守（ソフトウェアアップデート）
- 国際的な運用検討への参画と導入の検討
  - 脆弱性スキャン、SBOM作成等ツール利用による自動化
  - アドバイザリー文書を含む情報共有の自動化（VEX）

VEX: Vulnerability-ExploitabilityeXchange
https://www.cisa.gov/sites/default/files/publications/VEX_Use_Cases_Document_508c.pdf

ご清聴、有難うございました。

松元　恒一郎
Koichiro_Matsumoto@mb1.nkc.co.jp