医療情報学連合大会共催三菱電機展示ルームセミナー
テーマ：電子文書交換・地域医療連携・セキュリティ

医療機器におけるサイバーセキュリティ対策の最新動向

日本光電工業株式会社　技術戦略本部

一般社団法人　電子情報技術産業協会
医療用ソフトウェア専門委員会　委員長

松元 恒一郎

2023年11月25日
第43回医療情報学連合大会
神戸ファッションマート（六甲アイランド）

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

〇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。

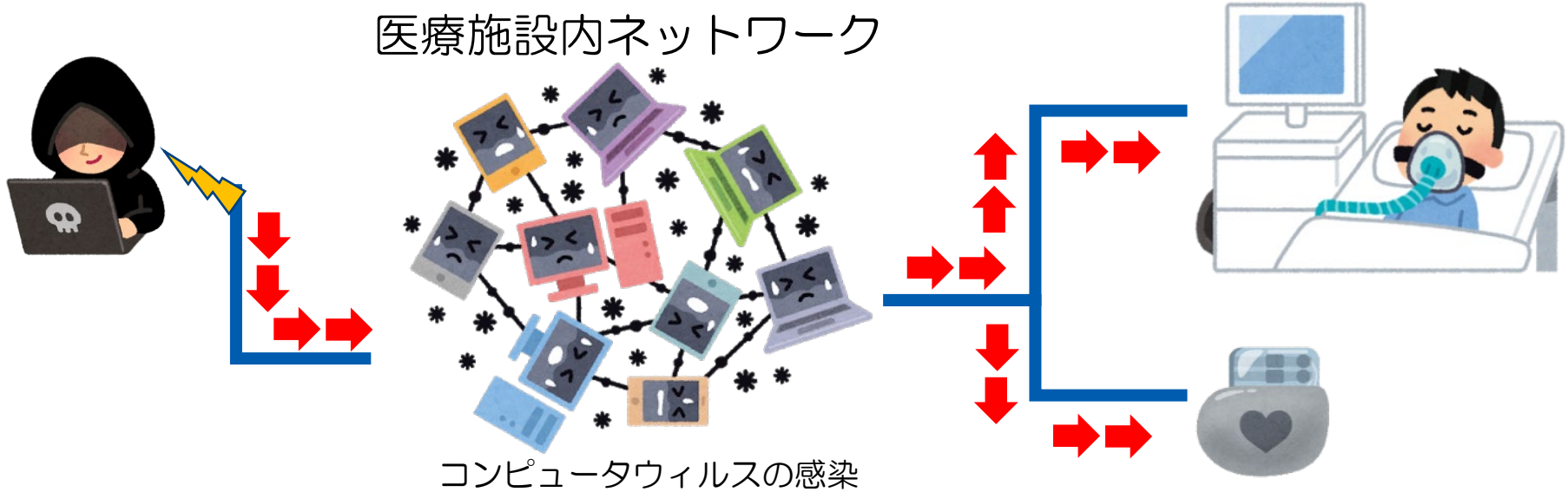
➢ サイバー攻撃が行われた時には、患者・医療従事者への健康被害にもつながり得る。

➢ 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。



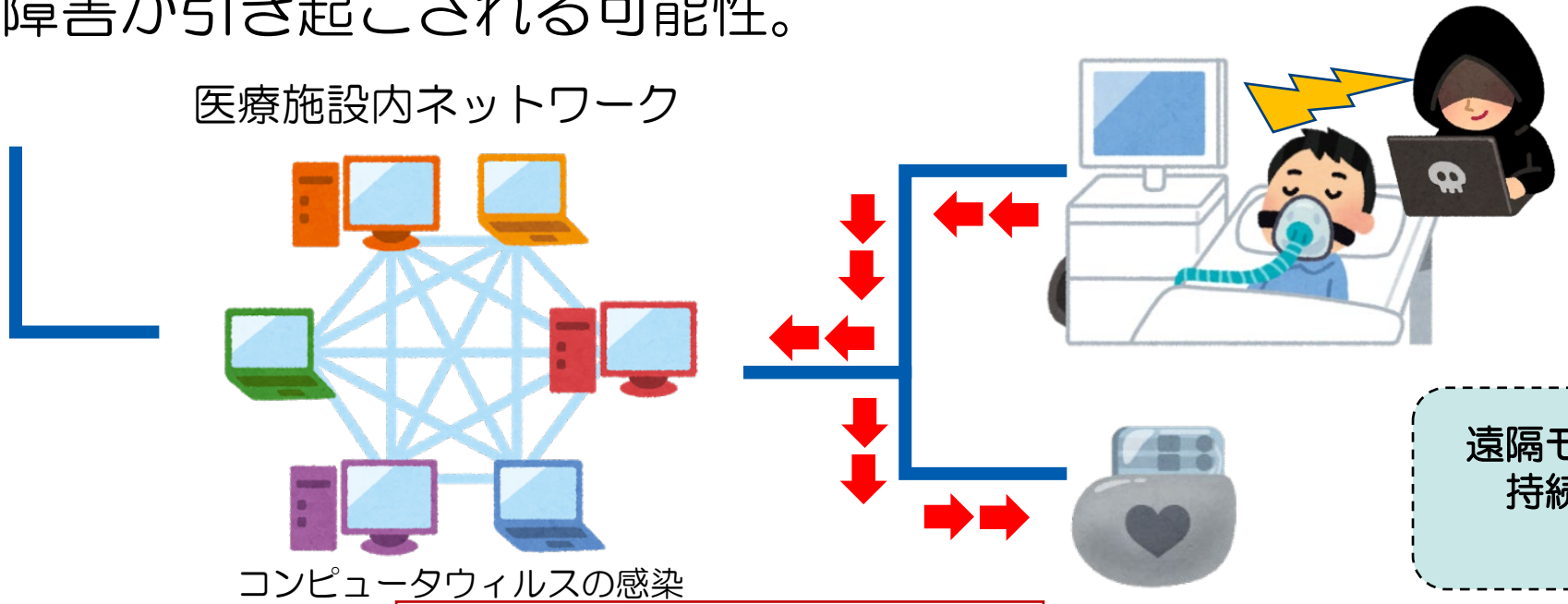
このリスクを低減するために

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
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。

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

目次

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った。

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12月　外来診療所を標的としたサイバー攻撃：

- Cyberattack on BHG opioid treatment network disrupts patient care
  （米国の17州で80以上の外来診療所を運営している外来オピオイド（麻薬性鎮痛薬）治療企業Behavioral Health Group（BHG）、サイバー攻撃を受け、約1週間にわたりITシステムと患者の治療に支障をきたした。自宅で使用するための治療薬をオピオイド依存の治療患者に提供している一部の診療所で、処方箋ラベルが印字できなくなったため、治療薬が提供できなかった）

セキュリティリスクの変遷 -3

2021年12月　医療機関と医療機器メーカー向けの実践ガイダンス：

- HSCA Releases Cybersecurity Guidelines for Medical Device Manufacturers
  （米ヘルスケアサプライチェーン協会（HSCA）、医療機関と医療機器メーカー向けに、サイバーセキュリティと患者のプライバシー保護の実践に関するガイダンスを発表。本ガイダンスは、サイバーセキュリティのトレーニングとソフトウェア、機器の調達基準とリスクの範囲、データの暗号化、情報共有と標準化組織、の4つの主要なカテゴリについて述べられており、医療機関と医療機器メーカが新しいベンダや組織と取引する前に、注意点を特定するためのヒントが示されている）

2022年3月　米Palo Alto Networks社調査レポート：輸液ポンプの75%に悪用可能な脆弱性

- 75% of medical infusion pumps affected by known vulnerabilities
  （米Palo Alto Networks社が、病院やその他の医療機関のネットワーク上にある20万台以上の医療用輸液ポンプを分析した調査レポートによると、75%に攻撃者に悪用される可能性のある既知の脆弱性がある。52%は、2019年に公表された2つの脆弱性の影響を受けやすく、平均的な輸液ポンプの寿命が8～10年であることを考えると、憂慮すべき結果となっている。同社は医療機関に対し、攻撃を防ぐために積極的なセキュリティ戦略を採用することを推奨している）

2022年9月　FBIからの警告：放置されたパッチ未適用の医療機器のリスク

- FBI Warns of Unpatched and Outdated Medical Device Risks
  （米連邦捜査局（FBI）、医療施設に対して、パッチ未適用の古い医療機器のリスクについて警告。病院内の医療機器やその他のIoT機器の半分以上が既知の脆弱性の影響を受けており、中でも除細動器、インスリンポンプ、モバイル心臓テレメトリ、ペースメーカーなどが最も影響を受けている機器の種類に含まれている。FBIは、可能な限りエンドポイント保護を採用すること、医療機器データの暗号化、医療機器ごとにユニークで複雑なパスワードを使用すること、重要な機器を容易に特定できる電子在庫管理システムの保持、定期的な脆弱性スキャンの実施、製造業者と協力して新たに特定された脆弱性へタイムリーにパッチを適用することを推奨している）

セキュリティリスクの変遷 -4

2023年1月　遠隔医療環境におけるリスク

- After targeting water sector, HC3 confirms Clop ransomware attacks against healthcare organizations

（米保健福祉省（HHS）の保健医療セクター・サイバーセキュリティ調整センター（HC3）、ランサムウェア攻撃グループ「Clop」による医療・公衆衛生分野への攻撃について確認されている情報を開示。同グループは、医療文書に見せ掛けたファイルを感染させ、それを標的となる病院に提出した後、それらの悪意のある文書が事前に開かれることを期待して、診療予約をしている。新型コロナウィルスの感染拡大下の遠隔医療環境において、成功する可能性が高くなっている）

2023年6月　米国CISA報告：セキュリティアップデートの欠如->医療機関でも同様・・・

- Hundreds of devices found violating new CISA federal agency directive

（インターネット接続デバイス検察エンジンCensysの研究者ら、米国CISAが発行した拘束力のある運用指令BOD 23-02に従ってセキュア化しなければならないインターネットに公開している機器が、米国連邦政府機関のネットワーク上に数百台あることを発見。インターネットにさらされた13,000以上のホストを発見した。このうち数百台は、様々なネットワークアプライアンスの管理インタフェースへのアクセスを許可していた。また、Microsoft社のWebサーバMicrosoft IIS、SSL/TLSプロトコルを実装したオープンソースライブラリOpenSSL、オープンソースのメール転送ソフト（MTA）Eximがサポート終了となっているサーバ150台も発見し、セキュリティアップデートの欠如によって攻撃対象領域が大幅に増加していた）

2023年9月　医療機関へのサイバー攻撃：大規模医療機関がランサム攻撃を受け、データの一部が公開

- Large Michigan healthcare provider confirms ransomware attack

米ミシガン州の大規模医療機関McLaren HealthCare、ランサムウェア攻撃グループ「BlackCat/ALPHV」による攻撃を受けた。コンピュータネットワーク上で不審な動きを検知し、調査を開始。調査の結果、ランサムウェアによる攻撃を受けたと判断。データの一部がダークウェブ上で入手できる可能性があるという報告も調査している。法執行機関へ通知し、サイバーセキュリティ態勢をさらに強化するため、システムのセキュア化と、患者や地域社会への混乱を抑える対策を講じた。

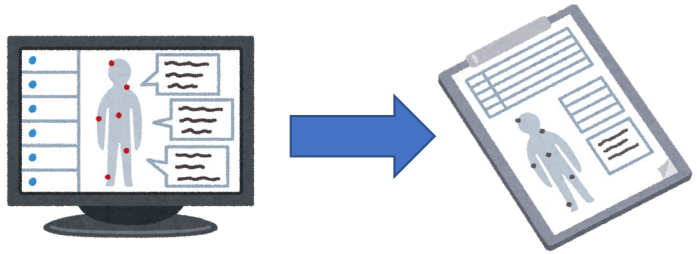
国内のサイバー攻撃の事例

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。



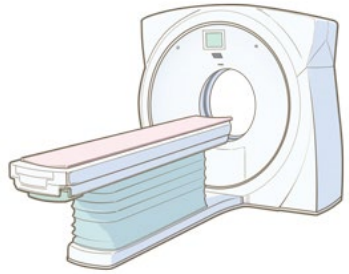
原因

- 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　厚生労働省通知：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

目次

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 ver1.0（平成28年7月）
  IoT推進コンソーシアム、総務省、経済産業省
- 目的
  - IoT特有の性質とセキュリティ対策の必要性を踏まえて、IoT機器やシステム、サービスについて、その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。
  - サイバー攻撃等による被害発生時における関係者間の法的責任の所在を一律に明らかにすることではなく、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こと。
  - 守るべきものやリスクの大きな等を踏まえ、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。

IoTセキュリティガイドライン

■　本ガイドラインは、IoT機器やシステム、サービスの提供にあたってのライフサイクル（方針、分析、設計、構築・接続、運用・保守）における指針を定めるとともに、一般利用者のためのルールを定めたもの。
■　各指針等においては、具体的な対策を要点としてまとめている。

	指針	主な要点
方針	IoTの性質を考慮した基本方針を定める	・経営者がIoTセキュリティにコミットする ・内部不正やミスに備える
分析	IoTのリスクを認識する	・守るべきものを特定する ・つながることによるリスクを想定する
設計	守るべきものを守る設計を考える	・つながる相手に迷惑をかけない設計をする ・不特定の相手とつなげられても安全安心を確保できる設計をする ・安全安心を実現する設計の評価・検証を行う
構築・接続	ネットワーク上での対策を考える	・機能及び用途に応じて適切にネットワーク接続する ・初期設定に留意する ・認証機能を導入する
運用・保守	安全安心な状態を維持し、情報発信・共有を行う	・出荷・リリース後も安全安心な状態を維持する ・出荷・リリース後もIoTリスクを把握し、関係者に守ってもらいたいことを伝える ・IoTシステム・サービスにおける関係者の役割を認識する ・脆弱な機器を把握し、適切に注意喚起を行う
一般利用者のためのルール		・問合せ窓口やサポートがない機器やサービスの購入・利用を控える ・初期設定に気をつける ・使用しなくなった機器については電源を切る ・機器を手放す時はデータを消す

IoT特有の性質とセキュリティ

特有の性質

- セキュリティ上の脅威の影響範囲・影響度合いが大きい。
  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。
- 機器のライフサイクルが長い。
  10～20年程度の長期にわたって使用される機器が多く存在。
  セキュリティ対応が不十分になった機器がネットワークに接続されつづける。
- 機器に対する監視が行き届きにくい。
  パソコンやスマートフォン等のような画面がないことから人目による監視が困難。
- 機器側とネットワーク側の環境や特性の相互理解が不十分である。
  相互の使用環境（意図した条件）が未解決のまま相互運用され、想定外のアクセスが発生。
- 機器の機能・性能が限られている（本来機能と見なされていない）。
  小型のウェラブル（センサー）機器等のリソースが限られている場合、暗号化等のセキュリティ対応を適用できない。
- 開発者が想定していなかった接続（使用環境）が行われる可能性がある。
  無線の影響、新たな機器やシステム、サービスの通信が相互に影響する。

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

- 5つの指針は、医療機器・システムの製造販売業者とその経営者を対象
  - IoT機器・システム → 医療機器　または　医療機器・システム
    （一部、一般IoT機器を示す場合はIoTのまま）
  - IoTシステム → 医療情報システム
    （一部、一般IoTシステムを示す場合はIoTのまま）
  - IoT機器・システム提供者 → 医療機器・システムの製造販売業者
    （製造業者、販売業者、貸与業者、修理業者）
  - システム・サービス提供者 → 医療機関または医療サービスの事業者
    医療情報システムの事業者
    ネットワーク事業者
- 4つのルールは，医療機器・システムの使用者を対象
  - 利用者（一般利用者） → 患者及びその家族、医師、技師、看護師等

目次

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

IMDRF International Medical Device Regulators Forum

IMDRF サイバーセキュリティガイダンス

IMDRF:International Medical Device Regulators Forum
国際医療機器規制当局フォーラム

ほぼ一斉に
サイバーセキュリティ規制化

- 米国FD&C法改正
- 欧州NIS指令2
- 日本基本要件基準改正
  医療法施行規則改正

応札条件にサイバーセキュリティ要件

Windows
医療機器へ
搭載本格化

Nimda
大規模感染

米国GAO
インスリンポンプ
脆弱性報告

固定パス
ワード問題

医療機器へ
攻撃始まる

ランサム
攻撃拡大

情報共有の
ネットワーク

米国
大統領令

QUAD 共同宣言サイバーセキュリティ確保

2000 | 2002 | 2004 | 2006 | 2008 | 2010 | 2012 | 2014 | 2016 | 2018 | 2020 | 2022 | 2024 | 2026 | 2028

ソフトウェア
認知

サイバーリスク
取扱

TC62 Scopeに
ソフトウェア追加
Medical electrical equipment

Guide 51 Safety改訂
全ライフサイクルが対象

TC62 ソフトウェア
取扱格上げ
Medical equipment, software, and systems

ソフトウェア開発ライフサイクル　IEC 62304 Ed1.1　JIS

ソフトウェア製品　IEC 82304-1　JIS

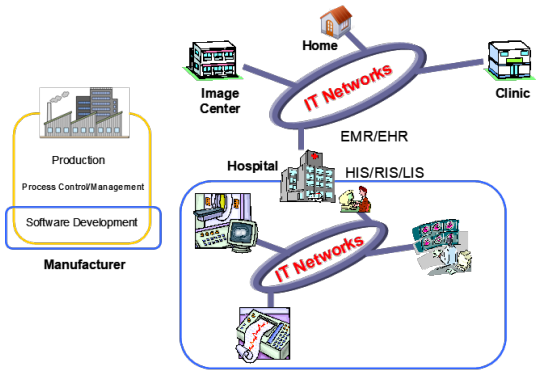
サイバーリスクを含むリスクマネジメント　ISO 14971 Ed3　JIS

医療機器のユーザビリティ　IEC 62366-1A1　JIS

医療機器のサイバーセキュリティ　IEC 81001-5-1　JIS

医用電気機器　一般要求事項　IEC 60601-1 Ed4

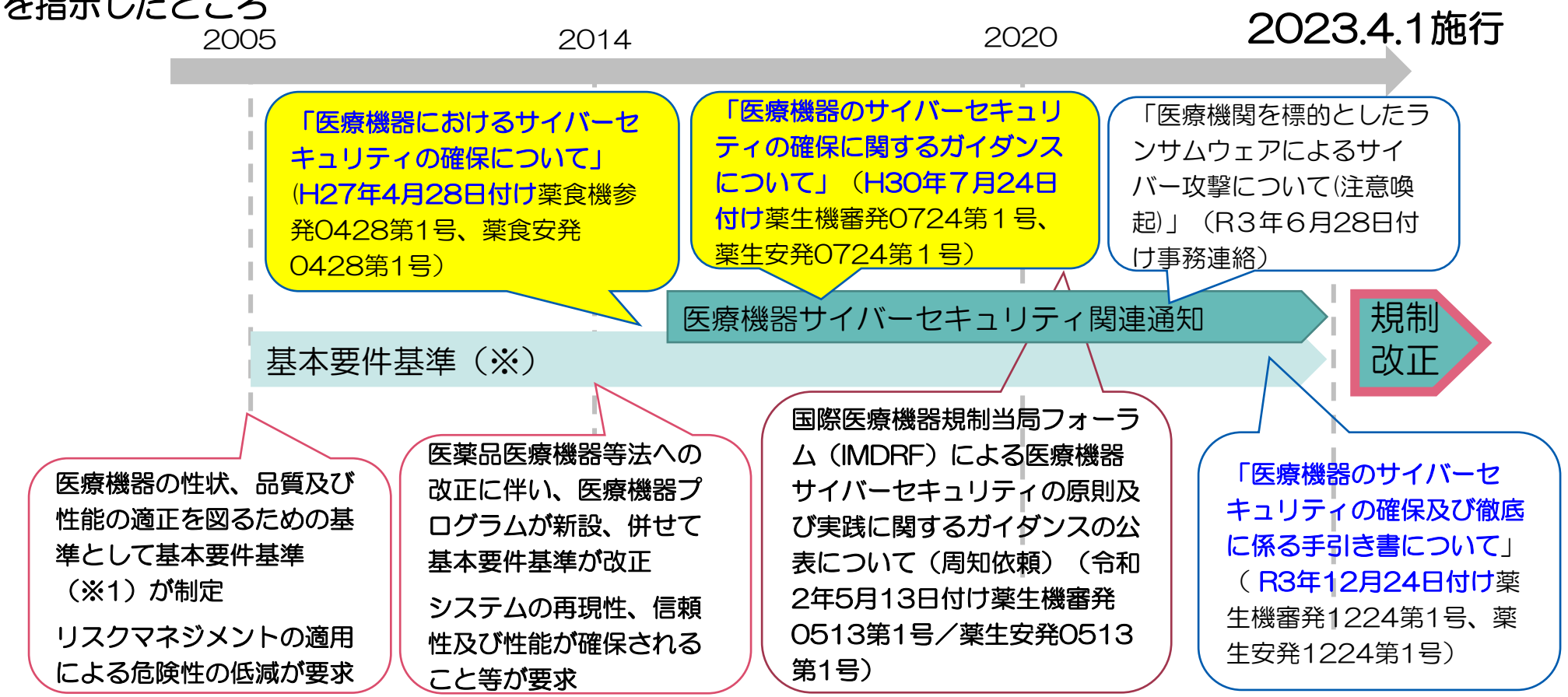
サイバーセキュリティ
及び関連規格整備



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

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

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」　（2015年）
（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）

①基本的考え方

- **製造販売業者は、**サイバーリスク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。
- 医薬品医療機器等法第41条第３項に基づく**基本要件基準（平成17年厚生労働省告示第122号）に基づき、サイバーリスクについても**危険性を評価し、**合理的に実行可能な限り除去することが求められる。**
- サイバーリスクが懸念される**医療機器の開発に当たっては、リスクマネジメントとして必要な対策を実施**し、サイバーセキュリティを確保すること。
- **既に製造販売を行っている医療機器**に関しても、同様に**サイバーセキュリティを確保**することが必要である。

上記が求められている．その上で

②サイバーセキュリティ対応

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。

厚生労働省 医療機器審査管理課
「医療機器のサイバーセキュリティの確保に関する最近の動向」
2020/6/30資料より引用

平成27年4月28日の厚労省通知に書かれた内容

(薬食機参発0428第1号/薬食安発0428第1号)

通知に書かれた具体的な対策①②③	要約
① 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、当該医療機器で想定されるネットワーク使用環境等を踏まえてサイバーリスクを含む危険性を評価・除去し、防護する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。 具体的には、当該医療機器と接続できる範囲を限定する。使用するソフトウェア等は製造販売業者が信頼性を認めたものに限定するなどのような対策が考えられる。	サイバーリスクを評価し、情報提供や注意喚起を含めた対策を行う。
② ①の必要なサイバーセキュリティの確保がなされていない医療機器について、，使用者に対してその旨を明示し、他との接続を行わない又は接続できない設定とするよう必要な注意喚起を行うこと。	サイバーセキュリティの確保がなされていない医療機器は、使用者に明示し、他と接続しないように注意喚起する。
③ 「医療情報システムの安全管理に関するガイドライン」を踏まえ、医療機関における不正ソフトウェア対策やネットワーク上からの不正アクセス対策等のサイバーセキュリティの確保が適切に実施されるよう医療機関に対し、必要な情報提供を行うとともに、必要な連携を図ること。	安全管理ガイドラインを踏まえ、必要な情報を提供し、必要な連携を図る。

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」（2018年）
（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）

①医療機器に関する検討

- 医療機器を使用する環境（医療機関・医療機関の管理が及ばない環境・特定が困難な環境）を特定。
- 医療機器のネットワーク等への接続方法（無線通信、USB 等の外部入出力ポート）の特定。

その上で

②具体的なサイバーセキュリティに関する対応

- 製造販売業者は、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**（リスクが受容可能となるよう、必要な対策を実施）。
- **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。
- 医療機関と連携を取り、サイバーリスクに伴う医療機器の不具合等の情報の収集を実施（**サイバーリスクに伴う医療機器の不具合**等の情報も、**GVP省令における安全管理情報**の一つ）。

厚生労働省 医療機器審査管理課
「医療機器のサイバーセキュリティの確保に関する最近の動向」
2020/6/30資料より引用

ガイダンスの構成

1. 目的
2. 検討が必要となる医療機器及び使用環境の特定
   - 2.1. 対象となる医療機器
   - 2.2. 医療機器の使用環境の特定
     - 2.2.1. 医療機関での使用環境
     - 2.2.2. 医療機関の管理が及ばない使用環境
   - 2.3. 医療機器のネットワーク等への接続
     - 2.3.1. ネットワーク等への接続機器
     - 2.3.2. 無線通信等利用の医療機器
     - 2.3.3. USB等の外部入出力ポート
3. サイバーセキュリティ対応
   - 3.1. 製造販売業者によるサイバーセキュリティ対応
   - 3.2. 使用者によるサイバーセキュリティ対応
4. 市販後の安全性確保について
   - 4.1. 中古医療機器への対応について
5. 使用者等への情報提供
   - 1）添付文書への記載事項

市販前・市販後にわたる
セキュリティ対応

使用環境を特定するなかで
安全管理ガイドラインに基づく
運用を想定

使用環境、接続機器、通信形態、採用技術、
インタフェースを考慮

・リスクマネジメントの実施
・既製品ソフトウェアも考慮
・セキュリティ対応に関する方針 体制
を確立、情報開示

GVP省令に基づく安全管理の実施(情報の集約
と分析、対策)

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

● 適用範囲

サイバーセキュリティに関するリスクが想定される医療機器が対象

- 機器の特性や使用環境からリスクを有するか判断する。
- 医療機器クラス分類（Ⅰ～Ⅳ）は問わない。
- 医療機器の構成品として提供される機器も適用対象。

参照：　2. 検討が必要となる医療機器及び使用環境の特定
2.1. 対象となる医療機器

● 医療機器の使用環境の特定

サイバーリスクを想定するため医療機器の使用環境の特定が必要

- 使用環境，機器構成，機器間接続(機器間通信）。
- 医療機関では安全管理ガイドラインに基づく管理を前提とする。
  個人宅等医療機関管理外で利用するケースも考慮する。
- 通信やネットワークへの接続、有線/無線、利用通信技術や機器、USB等外部デバイス等
  接続環境に応じたリスクを考慮する。

参照：　2.2. 医療機器の使用環境の特定
2.3. 医療機器のネットワーク等への接続

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

- サイバーセキュリティ対応

<u>製造業者によるサイバーセキュリティ対応：</u>

ライフサイクルを通したリスクマネジメント実施と対応方針に基づくセキュリティの維持

- 意図する使用環境に基づくリスクマネジメントの実施と対策。
  - 既製品ソフトウェアの考慮も必要。
- セキュリティに対応する方針と体制の確立。
- 問合せ窓口とサービスに係る取組について開示する事が望ましい。

参照： 3. サイバーセキュリティ対応
3.1. 製造販売業者によるサイバーセキュリティ対応

<u>使用者によるサイバーセキュリティ対応：</u>

ライフサイクルを通したリスクマネジメントの実施と対応方針に基づくセキュリティの維持

- 医療機関と連携しサイバーセキュリティの確保を支援。
- GVP省令に基づき安全管理を実施。

参照： 3. サイバーセキュリティ対応
3.2. 使用者によるサイバーセキュリティ対応

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

● 市販後の安全性確保

GVP省令に基づく市販後の安全管理の実施

- サイバーリスクに伴う医療機器の不具合情報や文献等を収集・調査し、その情報を分析して必要に応じて対策を行う。

中古医療機器への対応

- 中古医療機器においても当該医療機器販売業者に対し適切な指示を行い、サイバーリスクへの対応を実施させる。

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施行規則（昭和 36 年厚生省令第１号） 第 170 条

参照： 4. 市販後の安全性確保について
4.1. 中古医療機器への対応について

● 使用者への情報提供

サイバーセキュリティに関する情報を製造業者から使用者へ提供

- リスクに応じて適切な情報提供を行う。
- 使用環境や運用に関する要件、注意喚起、技術的補足事項。
- 問い合わせ窓口やサイバーセキュリティに対する取り組み情報。

※機器のセキュリティ上の
弱点を取説に書くのは注意！

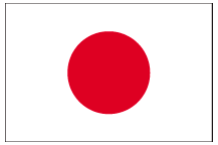
参照： 5. 使用者への情報提供

目次

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　 

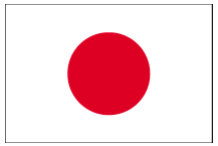
医療機器規制の基本的なフレームワークに対する多くのガイダンス文書を開発。（基本要件基準、クラス分類ルール等々）

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

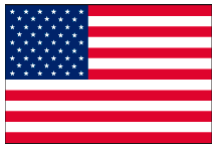
（2020/2/19現在）

日本　 

オーストラリア　 

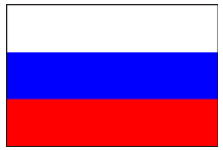
カナダ　 

ヨーロッパ　 

アメリカ　 

ブラジル　 

中国　 

ロシア　 

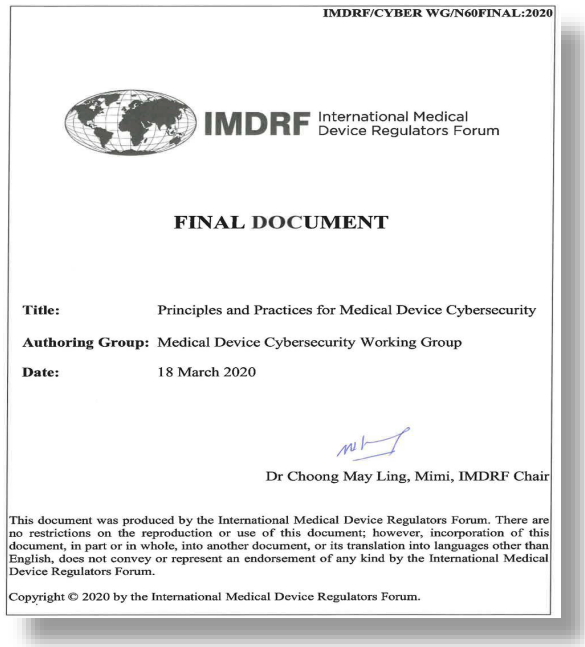
シンガポール　 

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

情報共有の重要性　FDAが示した考慮すべき事項（一部抜粋）

- ユーザー（ヘルスケアプロバイダー、医療提供者（HDO）、医療機関）
  - ネットワーク接続する機器の場合、**購入前に機器の製造業者から保守計画を確実に入手**する。
  - COTSベンダーではなく、サポートのために**機器の製造業者に依頼**する。
  - MedWatchを使用して、**FDAに情報を提供**する。
  - 誤動作が発生し、迅速なサポートが行われない場合は、**機器の製造業者に書面で（又は口頭で）苦情**を申し立てる。

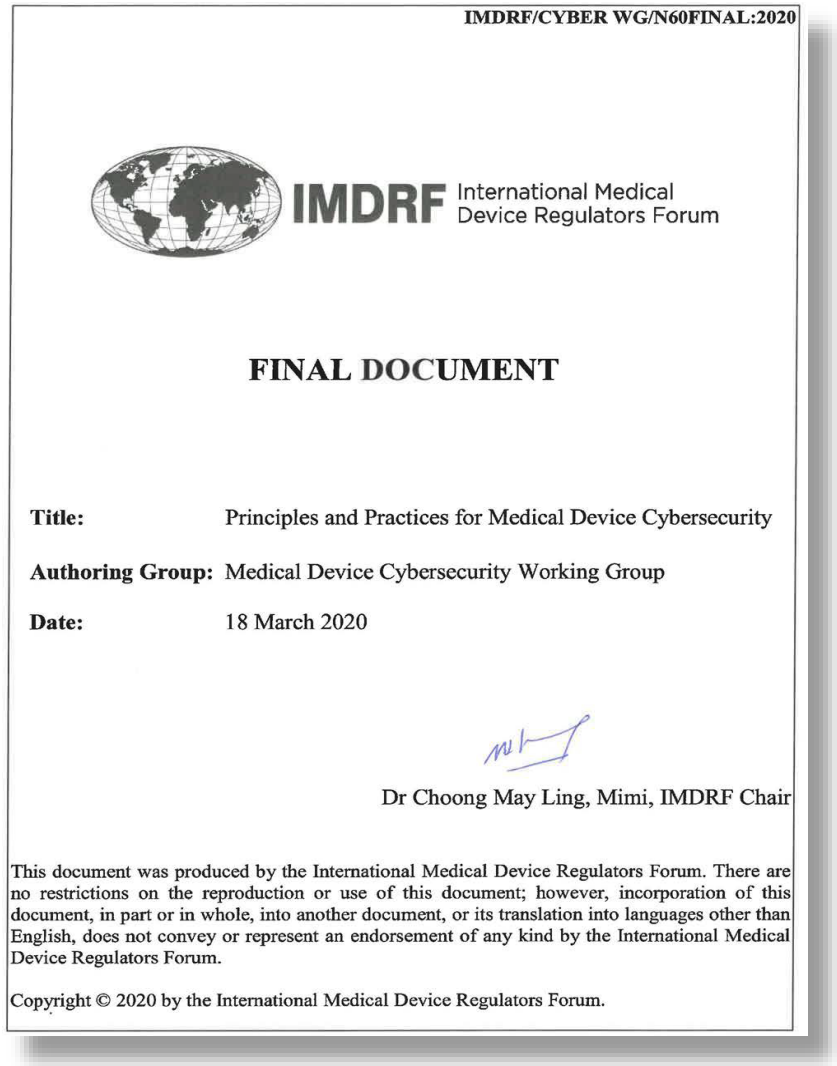
- 製造業者（製販業者）
  - 市販前申請の提出時にCOTS**保守計画の詳細を提供**する。

- COTSベンダー
  - **透明性（Transparency）のあるアップデート**を提供する。
    医療機器の製造業者（製販業者）が、ユーザー（医療機関）に合わせてアップデートを可能にする。

※　COTS：Commercial-off-the-shelf （既製品で一般的に購入などにより入手可能な商用製品）

ガイダンス文書の全体構成

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

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.

1.0 Introduction （はじめに）

2.0 Scope （適用範囲）

3.0 Definition （定義）

4.0 General Principles （一般原則）
- 4.1 Global Harmonization（国際整合）
- 4.2 Total Product Life Cycle（製品ライフサイクルの全体）
- 4.3 Shared Responsibility（共同責任）
- 4.4 Information Sharing（情報共有）

5.0 Pre-Market Considerations for Medical Device Cybersecurity
（医療機器サイバーセキュリティの市販前考慮事項）
主に製造業者

6.0 Post-Market Consideration for Medical Device Cybersecurity
（医療機器サイバーセキュリティの市販後考慮事項）
様々な責任関係者（製造業者，ヘルスケアプロバイダー，患者，規制当局，その他）

ベストプラクティス

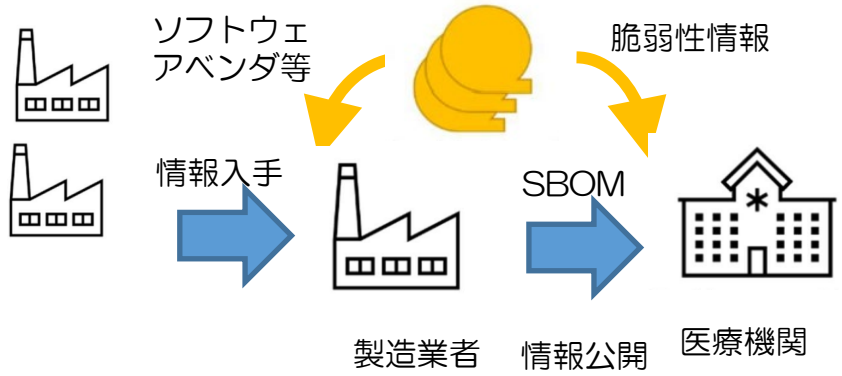
7.0 References （参考文献）

8.0 Appendices （附属書）

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

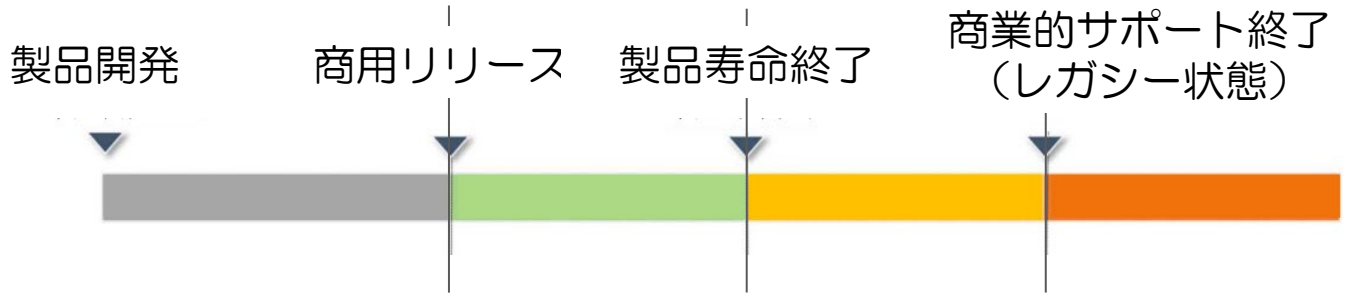


- **Coordinated Vulnerability Disclosure（CVD）「協調的な脆弱性の開示」**

  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

IMDRFガイダンスにおけるポイント（SBOM）

5.0 Pre-Market Considerations for Medical Device Cybersecurity

5.5.2 Customer Security Documentation

A Software Bill of Materials (SBOM) to inform and support operators regarding the cybersecurity of commercial, open source, or off-the-shelf software components which are included in the medical device. An SBOM creates the necessary transparency via a list identifying each software component by its name, origin, version and build. SBOMs enable device operators (including patients and healthcare providers) to effectively manage their [illegible] and related risks, to understand the potential impact of identified vulnerabilities to th[illegible] to maintain the device's safety a[illegible]ate work with the device manuf[illegible]uirements, and performing appro[illegible]g decisions by providing prospec[illegible] determining potential security [illegible] format, syntax and ma[illegible] me[illegible] th[illegible]

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及びサポートを医療機関、顧客に提供するためのソフトウェア部品表

活用：

- 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。
- 医療機関等が、脆弱性が潜んでいる可能性があるソフトウェアの特定、要件の更新及び適切なセキュリティリスクマネジメントの実施を、医療機器製造業者と協力して促進が可能。
- アプリケーション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、購入決定に必要な情報を提供することが可能。

IMDRFガイダンスにおけるポイント（CVD）

6.0 Post-Market Considerations for Medical Device Cybersecurity

6.3 Coordinated Vulnerability Disclosure

Transparency is an essential building block in cybersecurity because it is difficult to secure what is not known. One mechanism that enhances transparency is coordinated vulnerability disclosure (CVD).
CVD establishes formalized processes for obtaining cybersecurity vulnerability information, assessing vulnerabilities, developing mitigations or controls, and disclosing this information to various stakeholders, including cybersecurity information sharing

- 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、医療機関等の関係者においても重要な意味を持つ。
- 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付けられている。

Adopting CVD po impacted technologies to ma tter protect their medical devices, Health IT infrastructure, and patients.

Engaging in CVD is a responsible course of action for raising awareness to security issues and should be vie ma

- 未知の脆弱性を考慮し、セキュアな状態にすることは難易度が高いことから、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、緩和策及び補完的対策を開発・準備した上で、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。

Th
co
fac
should be undertaken as a norm rather than as an exception and medical device stakeholders are encouraged to ask manufacturers about their CVD policies to further catalyze adoption.

IMDRFガイダンスにおけるポイント（レガシーデバイス）

6.0 Post-Market Considerations for Medical Device Cybersecurity

6.6 Legacy Medical Devices

For purposes of this IMDRF guidance, medical devices that cannot be reasonably protected (via updates, and/or compensating controls) against current cybersecurity threats are considered legacy devices. The legacy condition represents an especially complex challenge for the present state of the healthcare ecosystem globally since device cybersecurity may not have been [illegible] the initial device design and maintenance [illegible] ated by the fact that the clinical u [illegible] digital technology within medical de [illegible] within older analog devices. While be [illegible] etwork connectivity in these technologies puts new demands on the device lifetime, which often consists of capital equipment (e.g. scanner hardware) as well as commodity components (e.g. servers, workstations, databases and operating systems).

It is important to note, however, that device age is not a sole determinant of legacy status. In other words, a device that cannot be reasonably protected against current cybersecurity threats may be less than five ye [illegible] ice m [illegible] cy [illegible]

As [illegible] h ar [illegible] re [illegible] e the norm, and the imbalance observed with respect to the multitude of legacy devices in current clinical use -

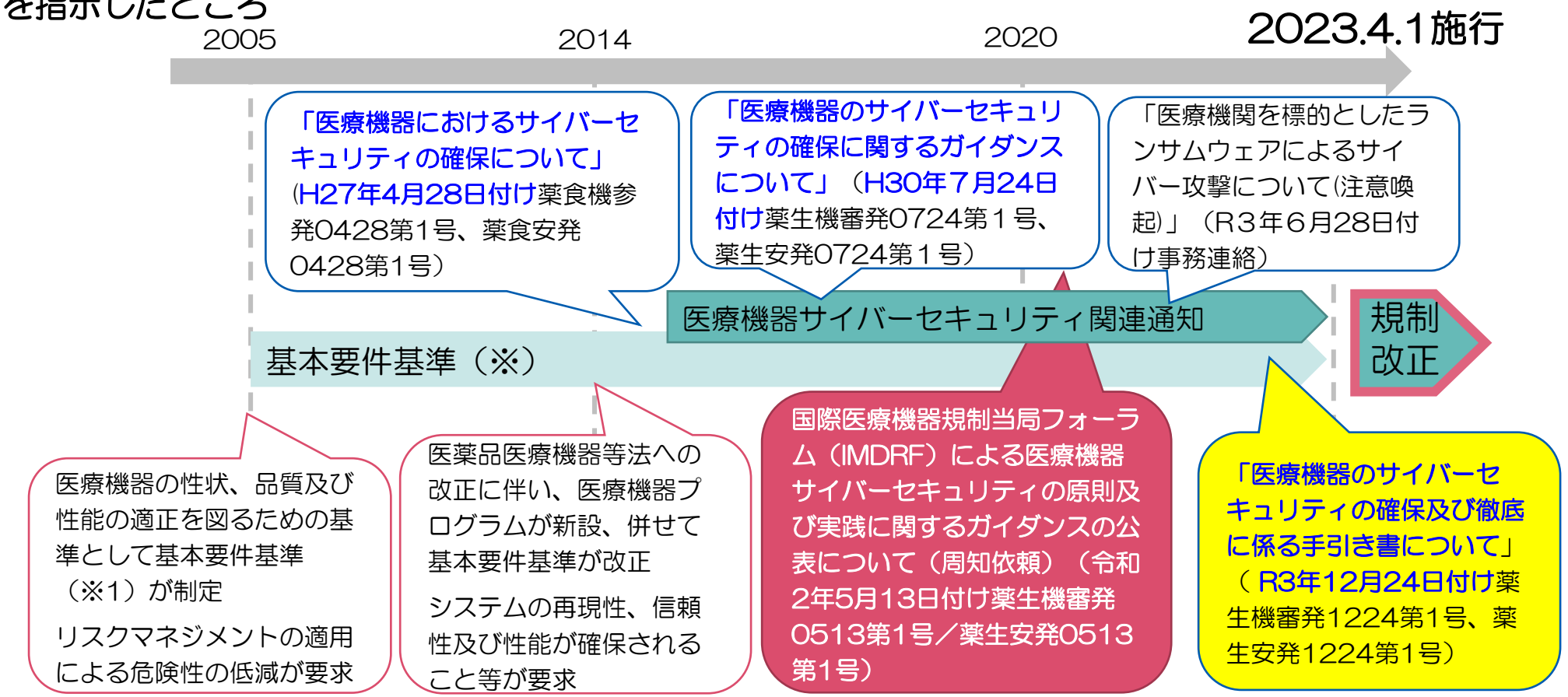
レガシーデバイス：現在のサイバーセキュリティの脅威に対して合理的に保護できない医療機器。

- 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（例えば、発売開始から5年以内の医療機器であっても、現在のサイバーセキュリティの脅威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。

目次

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

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

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
厚生労働省医薬・生活衛生局医薬安全対策課長

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）

医療機器のサイバーセキュリティについては、「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）、厚生労働省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、「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）により、具体的なリスクマネジメント及びサイバーセキュリティ対策を取りまとめたガイダンスを示し、当該ガイダンスを参考に必要な対応を行うよう、関係事業者等に対する周知を依頼してきたところです。

今般、医療機器のサイバーセキュリティ確保の重要性や各国のサイバーセキュリティ対策の実情等を踏まえ、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。）が取りまとめられました。

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、今後３年（2023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を行っているところです。

原文：http://imdrf.org/docs/imdrf/final/technical/imdrf-tech-200318-pp-mdc-n60.pdf
邦訳：http://dmd.nihs.go.jp/cybersecurity/IMDRF_Guidance_Japanese_version.pdf
（国立医薬品食品衛生研究所）

医療機器のサイバーセキュリティ導入に関する手引書
（2021年12月24日）

IMDRF ガイダンス

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
   - 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. ラベリング及び顧客向けセキュリティ文書
   - 5.6. 規制当局への申請に関する文書
6. 医療機器サイバーセキュリティの市販後考慮事項
   - 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
   - 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. 参考文献
8. 附属書

医療機器のサイバーセキュリティ導入に関する手引書

背景
1. 目的
2. 適用範囲
3. 用語及び参考定義
4. 一般原則
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

文献

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

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。

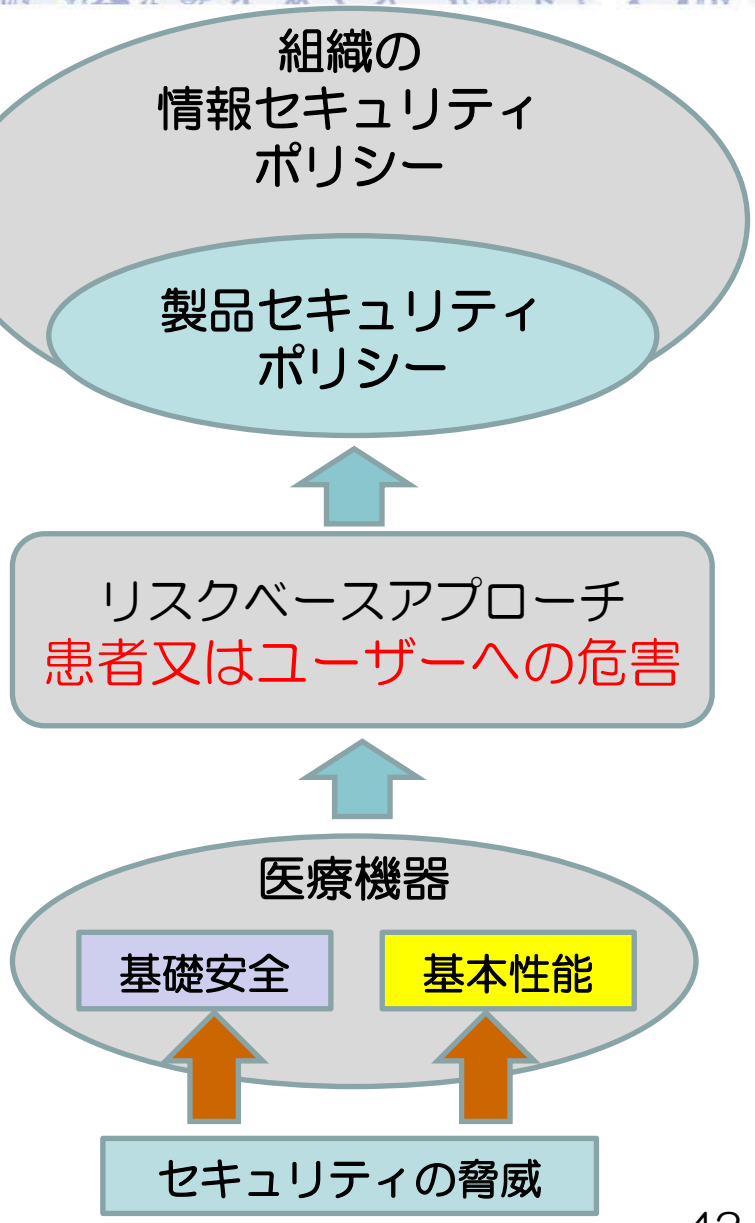
製造販売業者の責任の明確化

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

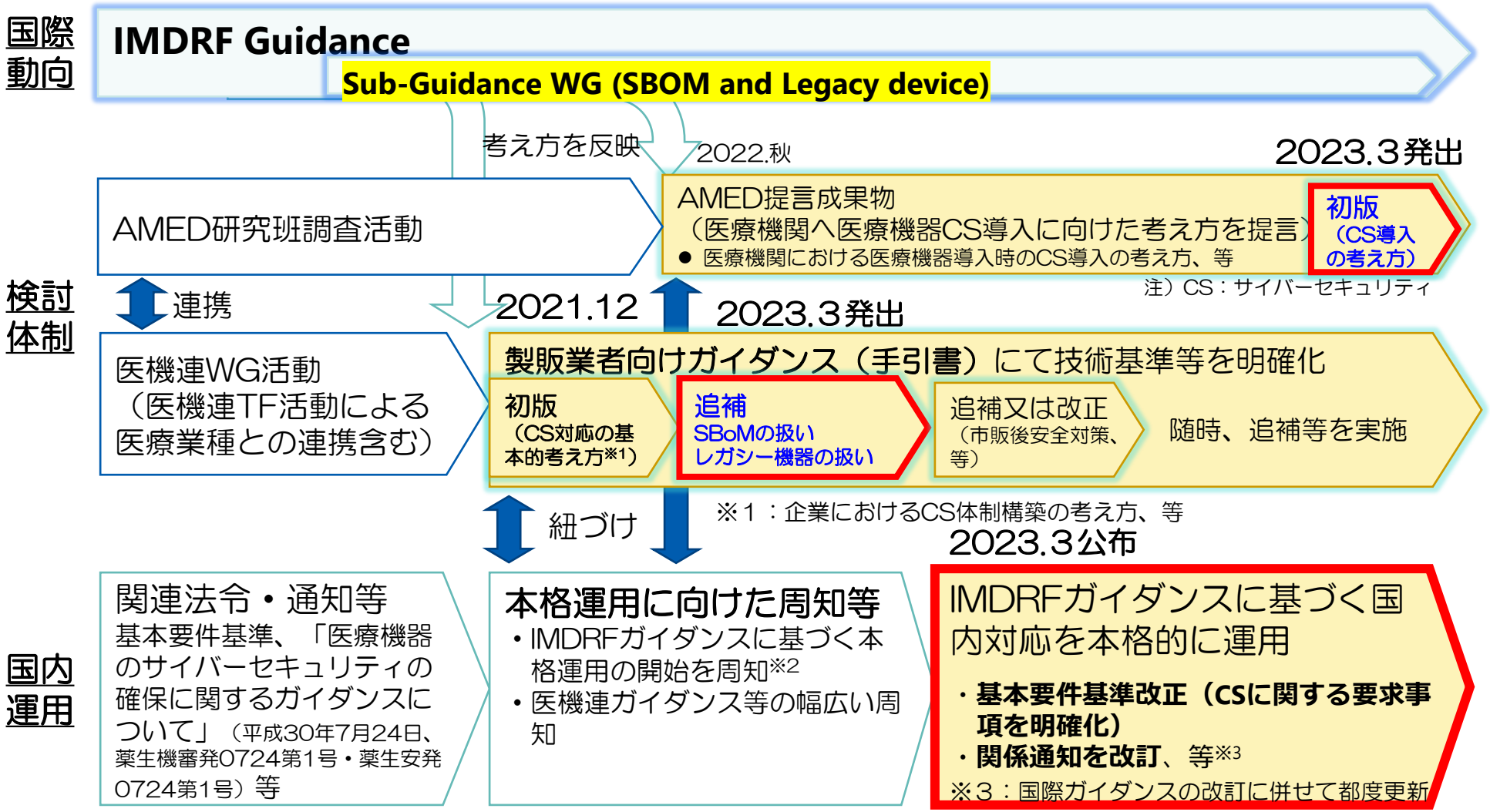
Figure 2 – A Venn diagram showing the relationship between security and safety risks AAMI TIR 57

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）

国際医療機器規制当局フォーラム（IMDRF）ガイダンス


IMDRF/CYBER WG/N60FINAL:202

IMDRF International Medical Device Regulators Forum

FINAL DOCUMENT

Title: Principles and Practices for Medical Device Cybersecurity

Authoring Group: Medical Device Cybersecurity Working Group

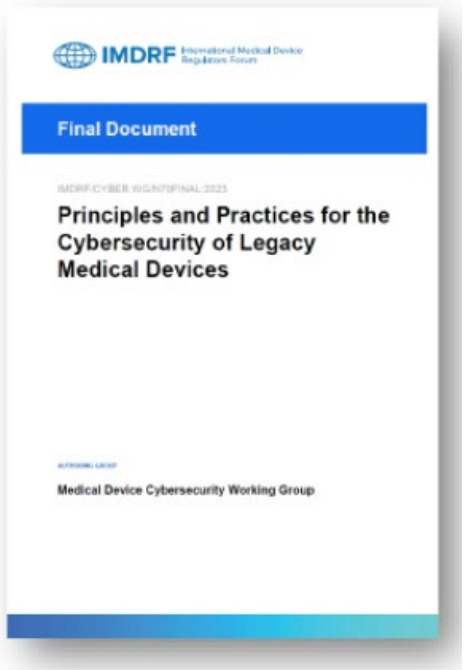
Date: 18 March 2020

Dr Choong May Ling, Mimi, IMDRF Chai

his document was produced by the International Medical Device Regulators Forum. There ar
o restrictions on the reproduction or use of this document; however, incorporation of thi
ocument, in part or in whole, into another document, or its translation into languages other than
nglish, does not convey or represent an endorsement of any kind by the International Medica
evice Regulators Forum.

opyright © 2020 by the International Medical Device Regulators Forum.

原則
基礎概念


IMDRF International Medical Device Regulators Forum

Final Document

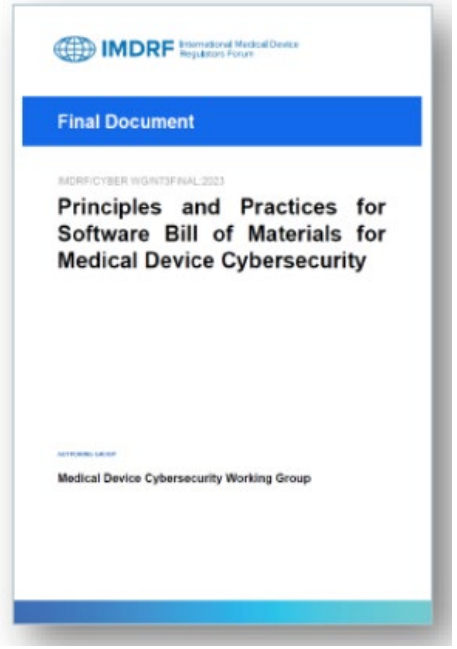
IMDRF/CYBER WG/N70FINAL:2023

Principles and Practices for the Cybersecurity of Legacy Medical Devices

AUTHORING GROUP

Medical Device Cybersecurity Working Group

応用・実践


IMDRF International Medical Device Regulators Forum

Final Document

IMDRF/CYBER WG/N73FINAL:2023

Principles and Practices for Software Bill of Materials for Medical Device Cybersecurity

AUTHORING GROUP

Medical Device Cybersecurity Working Group

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

医療機器の基本要件基準（第12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12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

1

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

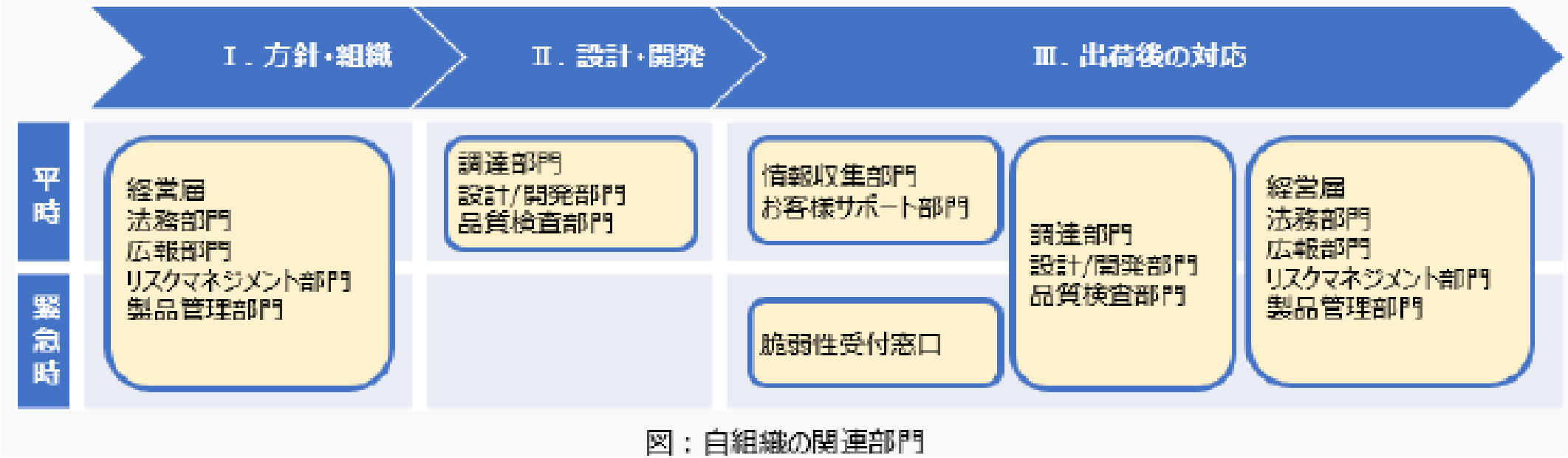
IMDRFの追補ガイダンスを基本として追加

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

PSIRT（Product Security Incident Response Team）

体制：多くの部門に関係する



図：自組織の関連部門

◆ インシデント対応準備

インシデント対応管理ポリシーの確立、詳細な対応計画の策定、インシデント対応チームの設立。
対応の定期的試験及び練習、対応能力の継続的向上。

◆ コミュニケーション

連絡先窓口情報を顧客に提供、状況共有のための日常的な活動体制を確立し、可能な限り早急に適切な情報を顧客に提供、規制当局その他所轄官庁への報告。

脆弱性対処に向けた製品開発者向けガイド（IPA）
https://www.ipa.go.jp/files/000085024.pdf

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

医政参発０３３１第１号
薬生機審発０３３１第16号
薬生安発０３３１第８号
令和５年３月31日

各 都道府県 保健所設置市 特別区 衛生主管部（局）長 殿

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）
（公印省略）

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

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、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き書について」（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、新たに、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タスクフォースにおいて、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に必要な取組、運用体制等を検討し、「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」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関における体制確保を円滑に行えるよう、貴管内の関係機関・関係団体等に対する周知、体制確保に向けた指導等よろしくお願いします。

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

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タスクフォース

目 次

「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）。

-> 改訂に向けて作業中

「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

目次

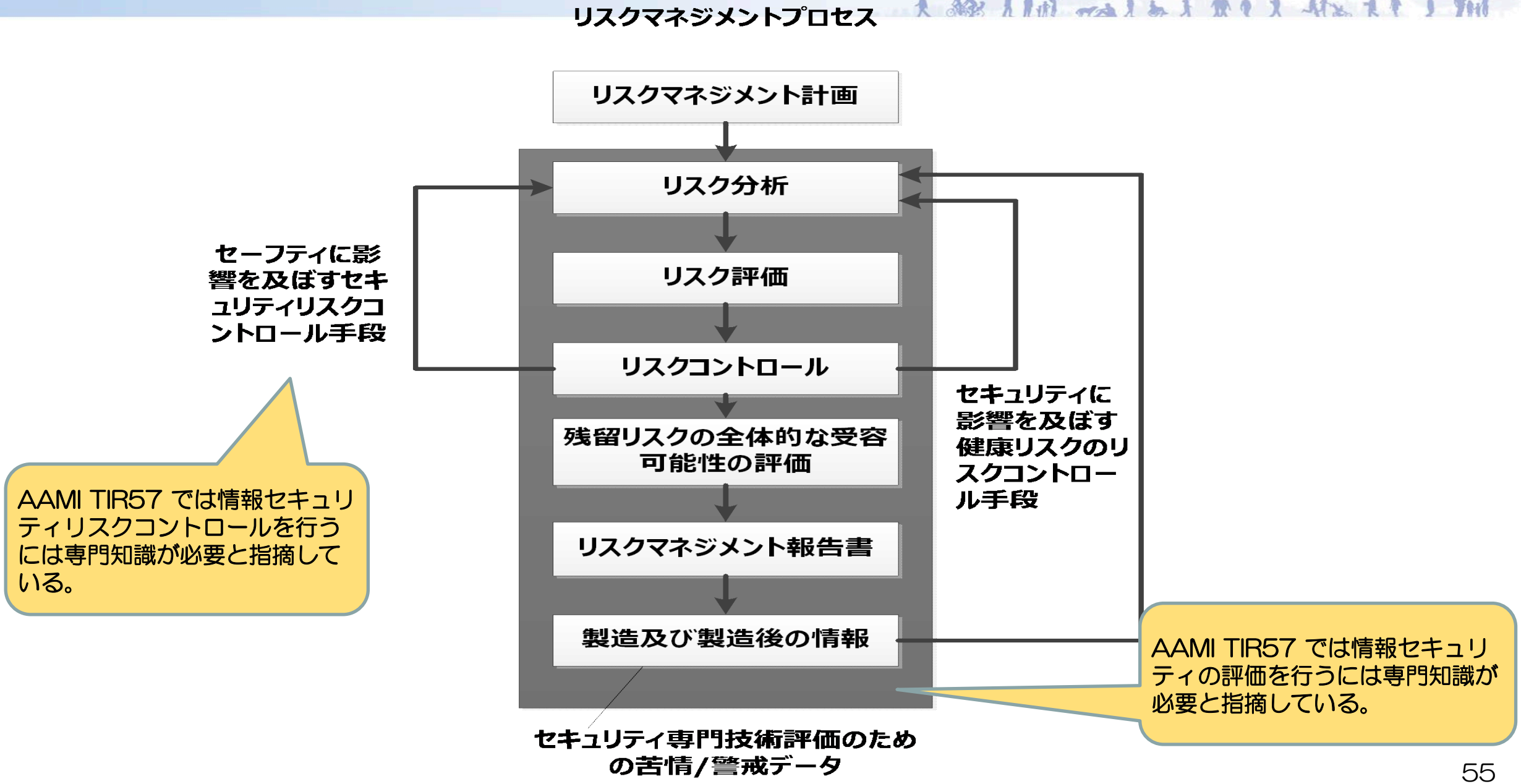
危害にはサイバーセキュリティに起因するものも含まれている

- 危害(harm)の定義
  - 人の受ける~~（身体的）~~傷害若しくは健康障害又は財産若しくは環境の受ける害

ISO/IEC Guide 51:2014の改定で危害(harm)の定義から physical （身体的）が消えた。

サイバー攻撃が原因となりうる傷害や健康被害はもちろんのこと、財産若しくは環境の受ける害に、情報セキュリティのAIC（可用性、完全性、機密性）の侵害により発生する害も含まれると考えれば、患者情報漏洩など機密性の低下も危害に含まれるかもしれない。

リスクマネジメントプロセスに組み込む



サイバーセキュリティリスク分析/報告の項目例

- 医療機器の意図する使用（Intended Use)
- 医療機器や構成品、ポータブルメディア、ネットワーク接続環境の説明
- 保護すべき情報資産の内容
- 侵入経路の分析及び脅威のモデリング
- サイバーセキュリティのリスク分析結果
- サイバーセキュリティリスクコントロール手段検証
- トレーサビリティマトリックス
- サイバーセキュリティ残留リスク判定
- 脆弱性の監視計画
- ペネトレーションテスト（侵入テスト）レポート
- サイバーセキュリティバリデーションのレビューワ資格情報
- サイバーセキュリティバリデーションの結果

リスクコントロールのために必要な外部接続機器等がある場合はそれらも接続環境に含める。

サイバーセキュリティリスクマネジメントのまとめ

- 当該医療機器の意図する使用（Intended Use）を確認する。
- 当該医療機器のネットワークシステム構成図（意図する使用環境）を描く。
- I/Fの一覧（I/F仕様、プトロコル、使用者等）とユースケース（そのI/Fを通して何ができるのか）を分析する。
- サイバーセキュリティのリスク分析及びリスク評価（対策前、対策後）を行う。
- リスク分析は情報セキュリティの可用性、完全性、機密性が低下したときの悪用可能性と危険状態と（患者）危害を分析するとよい。
- 危害の重大さの評価レベルは、従来の評価基準（ISO 14971:2007 表D.3-5）と同じにするか、サイバーセキュリティ用に独自の基準を定義するかを考える。
- 脅威の起こりやすさの評価は「確率」ではなく「悪用可能性」を分析することが望ましい。
- 分析したすべてのリスクが受容可となっていることを確認する。

医療機器の製造業者が行うべき事項（研究・開発，市販前）

- 技術（設計）的始動と製品セキュリティ
  - 米国FISMA、NIST、DHS及びDoDの動向の習得　（RMF: Risk Management Framework）
  - IMDRF、各国規制要求事項、ガイドラインの習得とリスクアセスメント
  - 製品セキュリティポリシー（ベースライン）及び製品セキュリティ要求事項の決定
  - 基本設計（リスクマネジメントと防御対策の確立）の計画と導入
    - ホワイトリスト型プロテクトツールの導入及びブラックリスト型プロテクトツールによる保守方法確立
    - オープンソースを含むOTSソフトウェアの特定（戦略的選択）及び管理とセキュリティ確保
      （SBOM: Software Bill of Materials、software version：UDI）
    - セキュリティの評価手法・手段の確立と継続的運用（開始）
      （悪用可能性：CVSS、脆弱性検出ツール：例Nessus、侵入試験等）
    - 添付資料（MDS2含む）、設計文書
- 仕組み（システム）の構築
  - 企業の情報システムセキュリティマネジメントシステムの適用
    製造所、事業所（ISO 27001： ISMS）
  - 製品セキュリティのための対応組織の設置と継続的運営
    （PSIRT：Product Security Incident Response Team の役割例）
    - セキュリティ情報の収集先の決定（ICS/JPCERT、IPA、サプライヤ等）
    - セキュリティ情報の収集・検知、発見された問題の分類・分析
    - 製品のセキュリティに関連する情報の提供
    - 医療機関を含む社内外の多様なステークホルダとの連携
    - 製品特性に合わせたインシデント対応方針の立案
    - 製品インシデントを発見するための手段・プロセス開発

医療機器の製造業者が行うべき事項（市販後）

- 販売・保守のための技術活動
  - 市販後監視
    - オープンソースを含むOTSソフトウェアの脆弱性管理（PSIRTからの入力）
    - サイバーセキュリティに関連するインシデント等のモニタリング
  - サイバーセキュリティに関する対応
    - セキュリティの評価手法・手段の確立と継続的運用
      （悪用可能性：CVSS、脆弱性検出ツール：例Nessus、侵入試験等）
    - MDS2（Manufacturer Disclosure Statement for Medical Device Security） の提供
    - 米国の主に国防総省（DoD）に関連する施設への納入条件となるATO
      （Authority to Operate：ネットワークにおける運用認定）取得及び取得後の月次報告
      （Nessusによるスキャンを含むSTIG（Security Technical Implementation Guides） の実査による認定で、
      DHA（Defense Health Agency）が実施 （https://health.mil/dha）
    - OS等のプラットフォームの更新技術の開発・評価
- 仕組み（システム）の構築
  - 製品セキュリティのための対応組織の継続的運営（PSIRT：Product Security Incident Response Team）
    - オープンソースを含むOTSソフトウェアの脆弱性管理のための契約管理
    - GDPRに基づくSCC（標準契約条項）の締結（欧州）
    - セキュリティ情報の収集・検知、発見された問題の分類・分析
    - 製品のセキュリティに関連する情報の提供
    - 医療機関を含む社内外の多様なステークホルダとの連携
    - 製品特性に合わせたインシデント対応方針の立案
    - 製品インシデントを発見するための手段・プロセスの保守
  - 情報共有の仕組み　ISAO参加と活動（米国）

SBOMに関する検討

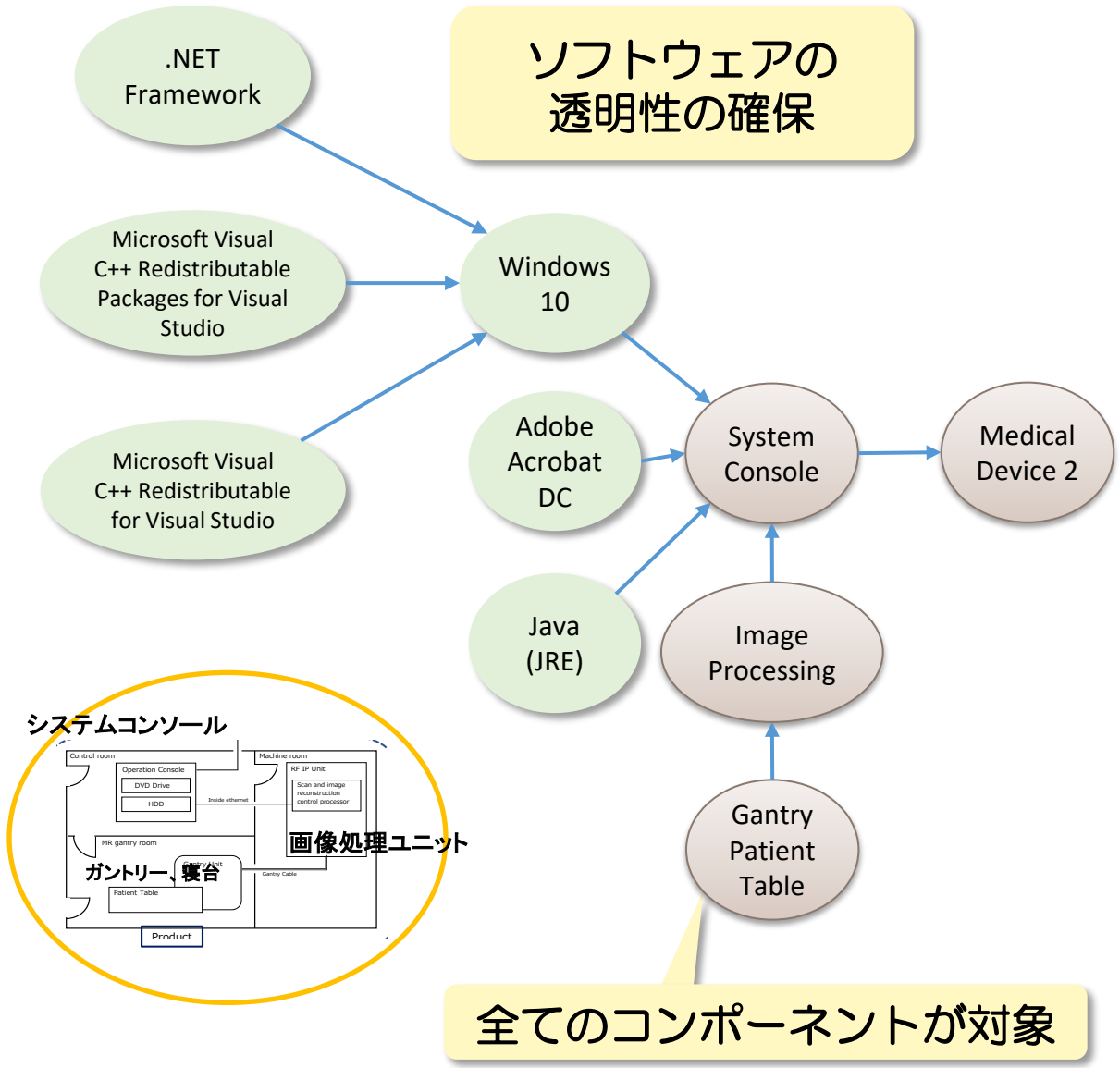
- NTIA：Health Care、Energy Proof　CISA：Sharing、Adoption、Cloud, Tooling
  NTIA：National Telecommunications and Information Adminisration
  CISA：Cybersecurity & Infrastructure Security Agency
- SBOM　製販業　医療機関（ユーザー）共有のためのテンプレート
  電子フォーマット化、契約情報重視のSPDXを標準とする可能性
  -> 直接読込（取込）のためmachine-readableとする
- 製販業者が公開す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
- NTIA“Minimum elements”ベースで検討が進んでいる。
- 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・・・

目次

まとめ

- 厚生労働省は、平成27年(2015年） 医療機器のサイバーセキュリティに関する通知を発行し、平成30年（2018年）通知に対応するガイダンスを発行した。これが基本となっている。
- 令和2年（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、日本では、2023年3月を目途に、医療機器製造販売業者に対して導入が進めら、2023年3月31日に厚生労働省より発出された。
- 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を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（規制要求）」「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。

NIHON KOHDEN

ご清聴，有難うございました。

松元　恒一郎
koi_matsu@ae.auone-net.jp