チュートリアル3：
医療機関におけるサイバーセキュリティへの課題と対応
座長：山下芳範先生、高井康平先生

医療機器における
サイバーセキュリティ対応の現状

日本光電工業株式会社　技術戦略本部
松元 恒一郎

6月30日（木）13:00～15:00　第2会場
第26回日本医療情報学会春季学術大会
シンポジウム2022 in せとうち
岡山コンベンションセンター

第26回日本医療情報学会春季学術大会
COI開示

演題名：医療機器におけるサイバーセキュリティ対応の現状

演　者：松元　恒一郎

私が発表する今回の演題について開示すべきCOIはありません.

目次

医療機器のサイバーセキュリティ対応の必要性

- 医療機器の中には，IoT機器として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.
- 医療機関のネットワークにおいては，医療情報システムに関するガイドラインとして取りまとめられた「医療情報システムの安全管理に関するガイドライン第5.2版」(令和4年3月)に従って，医療情報システムの適正な運用等を行うことが重要である.
- 医療機関のネットワークに接続される医療機器が，直接又は二次的に攻撃を受けた場合，その医療機器自体が機能を失う等の障害だけでなく，当該医療機器が接続された医療機関のネットワーク等を介して同様の障害が拡大する可能性が想定される．これらの事象は，診断・治療の遅れ又は誤り等の結果として，患者に健康危害を及ぼすことがある.

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増し，持続的な対応が必要

医療機器を経由して侵入されるセキュリティリスク

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)

Hospira は 2013年に Symbiq Pumpの生産を終了しているが，未使用のネットワークポート(ポート20/FTP, ポート 23/TELNET)に対してアクセス可能になっていることが分かった.

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6月　Ripple20 （IoTデバイス・ネットワーク機器等に影響する脆弱性）
- 米国のTreck社が開発したTCP/IP通信用ライブラリに存在する19個の脆弱性の総称
- 通信・小売・商社・医療・輸送・工業・エネルギー等広範囲の業界で使用されているとみられている
- 医療機器に影響がある可能性

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，9月10日に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．警察が現在捜査中で，ランサムウェア攻撃と病院の稼動停止時間が患者の死亡の直接的な原因であることが判明した場合，捜査を殺人事件に切り替える予定．病院関係者のSNS投稿によると，ランサムウェア感染の原因は，広く使われている商用ソフトウェアの脆弱性で，BSI（ドイツ連邦政府情報セキュリティ局）にインシデントについて報告.
- Massachusetts Hospital Investigates　'Data Security Incident'
  米マサチューセッツ州の病院Lawrence General Hospital，9月19日にデータセキュリティインシデントが発生し，同病院のシステムが，36時間オフラインとなった．その間，救急車で搬送されて来た患者は他の病院へ搬送され，病院スタッフは医療フォームに手書きで記入し，電話や対面のミーティングで連絡を取り合った．同病院は現在，フォレンジック会社と協力してインシデントの詳細を調査中で，主要な臨床関連のシステムは復旧し，患者のケアを引き続き行っている.

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.

国内では・・・

2017年（公表は2020年）患者，医療従事者へ多大なる影響を及ぼした

- 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.
- 原因は，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.

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.
- 2022年1月4日，通常診療再開.

従来のウイルスは不特定多数を無差別に攻撃するものが多かったが，標的型攻撃は情報の窃取や破壊などを目的として，特定の企業や組織に向けた攻撃を行う.

標的型攻撃のプロセス：

- 興味を引く内容のメールで添付ファイルやURLを開かせる.
- 添付ファイルやURLからウイルスを送り込む.
- 送り込んだウイルスを利用して攻撃を実施する.

さらに，

- 端末を遠隔コントロールする別のウイルスを送り込む.
- 接続可能なマシンにウイルスをばらまく.
- アクセス可能なファイルをコピーして外部に送信する.

さらにひどいものだと，

- ルート権限を奪取する.
- 管理者に成りすましてさまざまな重要機密にアクセスする.
（民間企業などで複数の被害が確認されている）

医療機器規制と個人情報保護

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づけが異なる事から，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

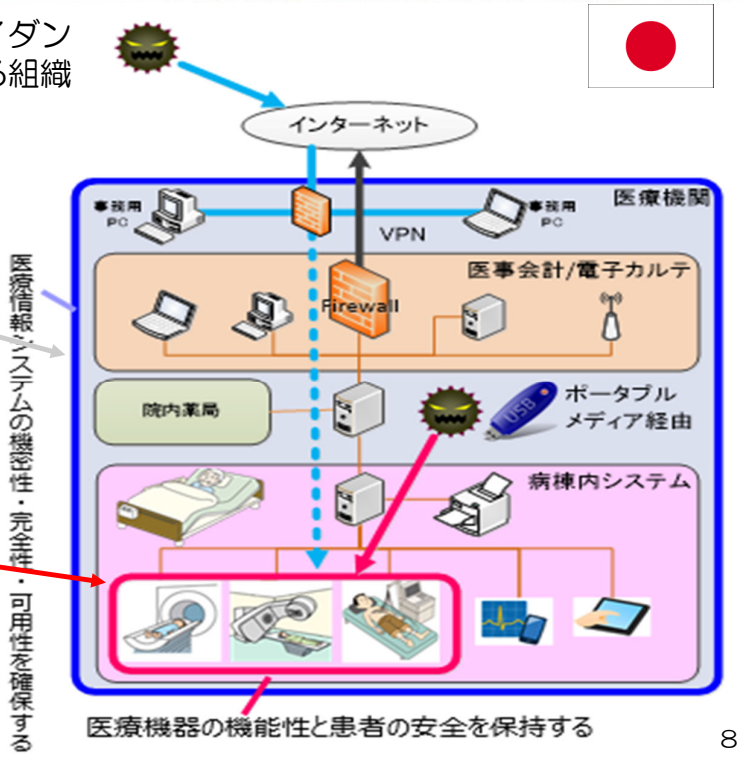
※1 医療情報システムの安全管理に関するガイドライン　第5版（平成29年5月），第5.2版（令和4年3月）公開

【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）

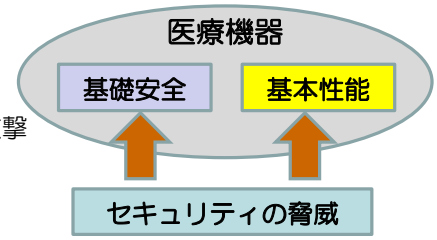
JEITA医療機器ソフトウェアの最新技術動向セミナー（2020年2月19日）より引用，一部改変



医療機器のサイバーセキュリティ（リスクマネジメントの課題解決）

- 2001年～2006年コンピュータワームNimda問題発覚

（Microsoft社のWindowsシリーズのOSを搭載したコンピュータに感染する．
医療機器はWindows採用が遅れたため，問題発覚も遅れた．
JavaScript, IE, Internet Information Server（IIS）のセキュリティホールに対する攻撃
->悪意のある攻撃：それまでのリスクマネジメントでは解決できない



共同責任
Shared
Responsibility

ITインフラ
ベンダー

医療機器
製造販売業者

医療機関

（HDO：Healthcare Delivery Organization）

2005年FDA医療機関向けキャンペーン資料より

- 医療機器の脆弱性を不正利用
  - 機器設定の不正変更
  - 治療の不正変更または無効化
  - 機密データの喪失または開示
  - 機器の誤動作
  - 他の機器・システムへの拡散

共同責任
医療機器のセキュリティは，医療施設，患者，医療従事者，および医療機器の製造業者などの関係者の間での共同責任であると認識している．サイバーセキュリティを維持できない場合，結果として，機器の機能性障害，データ（医療上または個人的な）の真正性，可用性や完全性の損失，あるいは他の接続した機器またはネットワークをセキュリティの脅威へ暴露する可能性がある．これにより，患者の疾患，傷害，または死亡に至る可能性がある．

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．
- 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．
- 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：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）

脅威分析，脆弱性マネジメントの必要性

脆弱性から生じるさまざまなコスト（例）

➢ 製品開発者のコスト

- 製品設計見直し
- セキュリティパッチ開発，配布
- ユーザー対応
- メディア対応
- 株価への影響

➢ 製品ユーザーのコスト

- セキュリティパッチ適用作業
- 攻撃への対応
- セキュリティ強化
- 患者様への対応
- メディア対応

➢ 社会のコスト

- 重要インフラへの攻撃対応
- 製品サプライチェーンへの影響

サイバーセキュリティを取り巻くわが国の取り組み等

- 医療情報システムに関する**全体構成図（ネットワーク構成図，システム構成図等），及びシステム責任者一覧（設置事業者等含む）を整備**
- 利用者の**認証・認可**
- ランサムウェアによる攻撃への対応としての**バックアップのあり方**

対象としては広義

医療機関

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
2017年（第1版は，2005年）

医療に関わる情報を扱う全ての情報システムと，それらのシステムの導入，運用，利用，保守及び廃棄に関わる人又は組織が対象．

第5.2版　2022年3月

対象としては狭義

医療機器の製造販売業者（医療機器企業）

「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，薬食機参発0428第１号・薬食安発0428第１号） 2015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」（平成30年7月24日，薬生機審発0724第1号・薬生安発0724第1号） 2018年

⇩

「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，薬生機審発0513第1号・薬生安発0513第1号） 2020年　※IMDRFガイダンス

国内導入へ 2023年

※規制（ガイダンス等）以外の取り組み

重要インフラ事業者等の情報共有・分析機能及び当該機能を担う組織

内閣サイバーセキュリティセンター（NISC）関連
サイバーセキュリティ重要インフラ
医療セプター
事務局：日本医師会情報システム課

AMEDサイバーセキュリティ研究班資料より引用

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）

一部は，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）

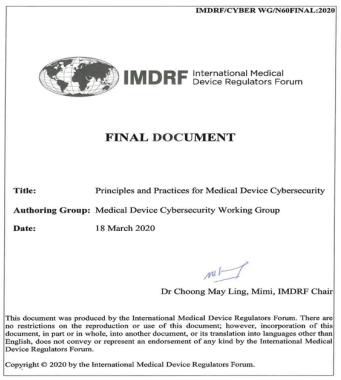
日本　オーストラリア　カナダ　ヨーロッパ　アメリカ

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.

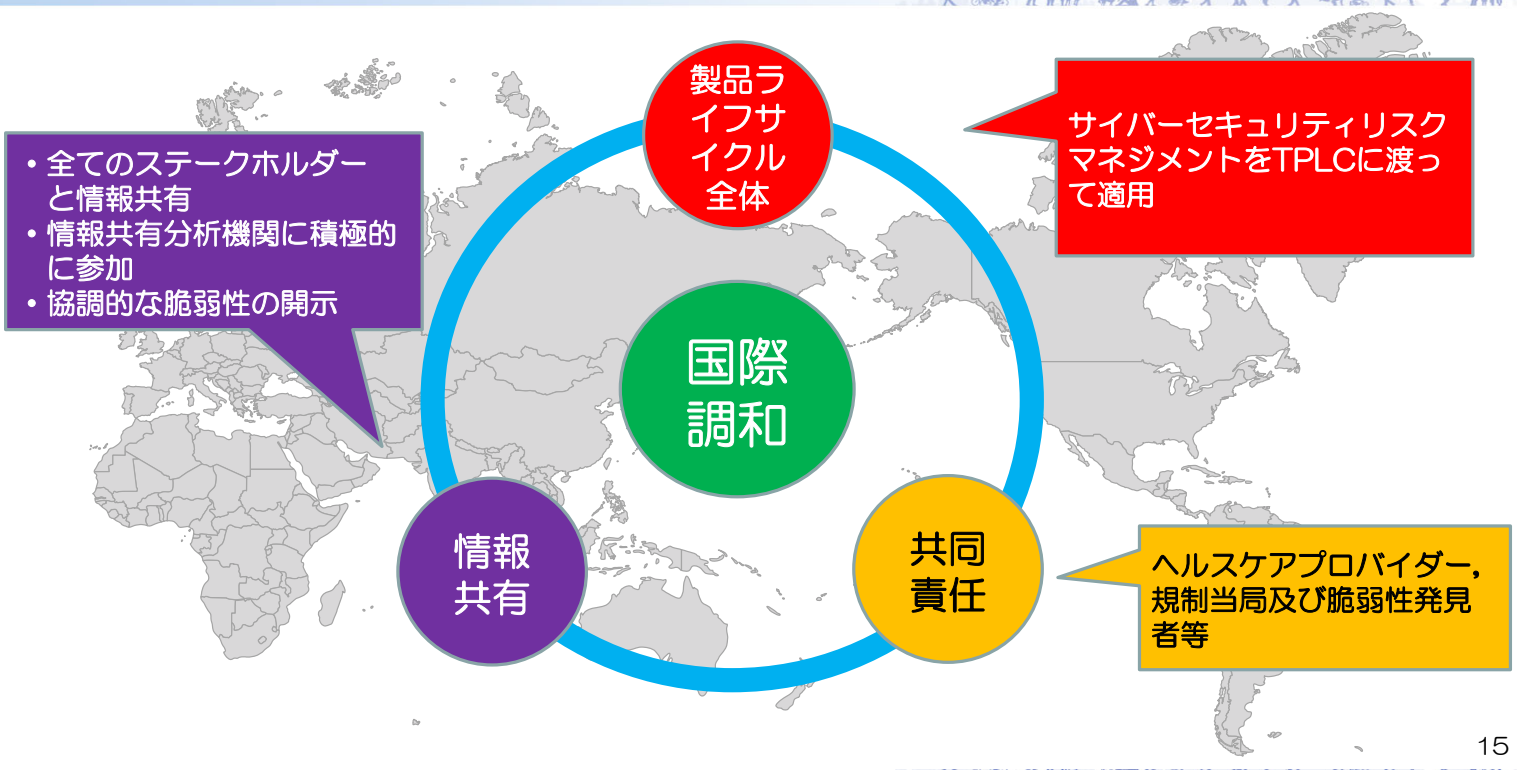
一般原則

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

IMDRFガイダンスの一般原則



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

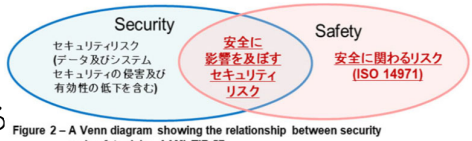
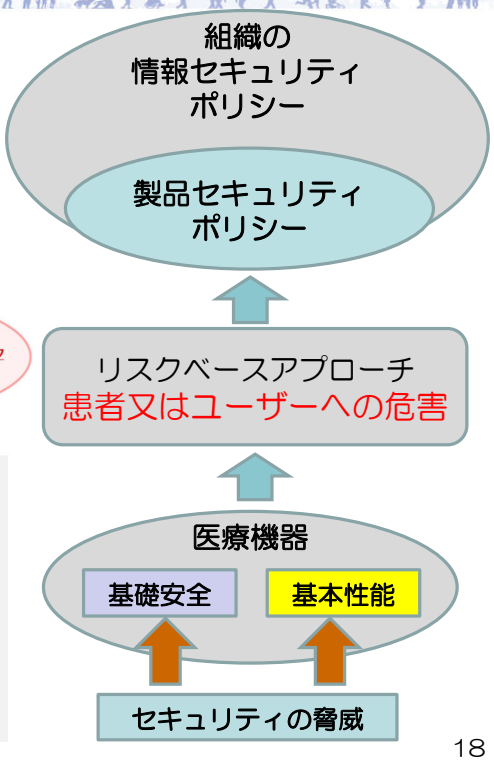


Figure 2 – A Venn diagram showing the relationship between security and safety risks AAMI TIR 57

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

製造販売業者が取り組むべきサイバーセキュリティ課題

①企業体制の考え方の明確化・ガイドライン化

（体制）
- 何をするべきか，文書管理等
- サイバーセキュリティの対象
- 人材不足，教育不足（中小企業ではより深刻？）
- 相談窓口が明確化されていない

②サイバー攻撃への耐性を持つ医療機器の設計・開発の考え方の整理

（審査関係）
- 開発者にとって分かりやすい，サイバーリスクの評価方法
- 薬機法の要求水準（評価の考え方）
- 試験・評価系で参考となる規格
- 併用機器のサイバー対策の考え方，責任の範囲

③個別相談・指導審査の明確化

（審査関係）
- 申請時の添付資料（例えば，SBOMやMDS2の取扱い）
- 添付資料の妥当性の考え方
- 相談するべき内容・相談窓口

④医療機関との情報共有・導入時留意点の明確化

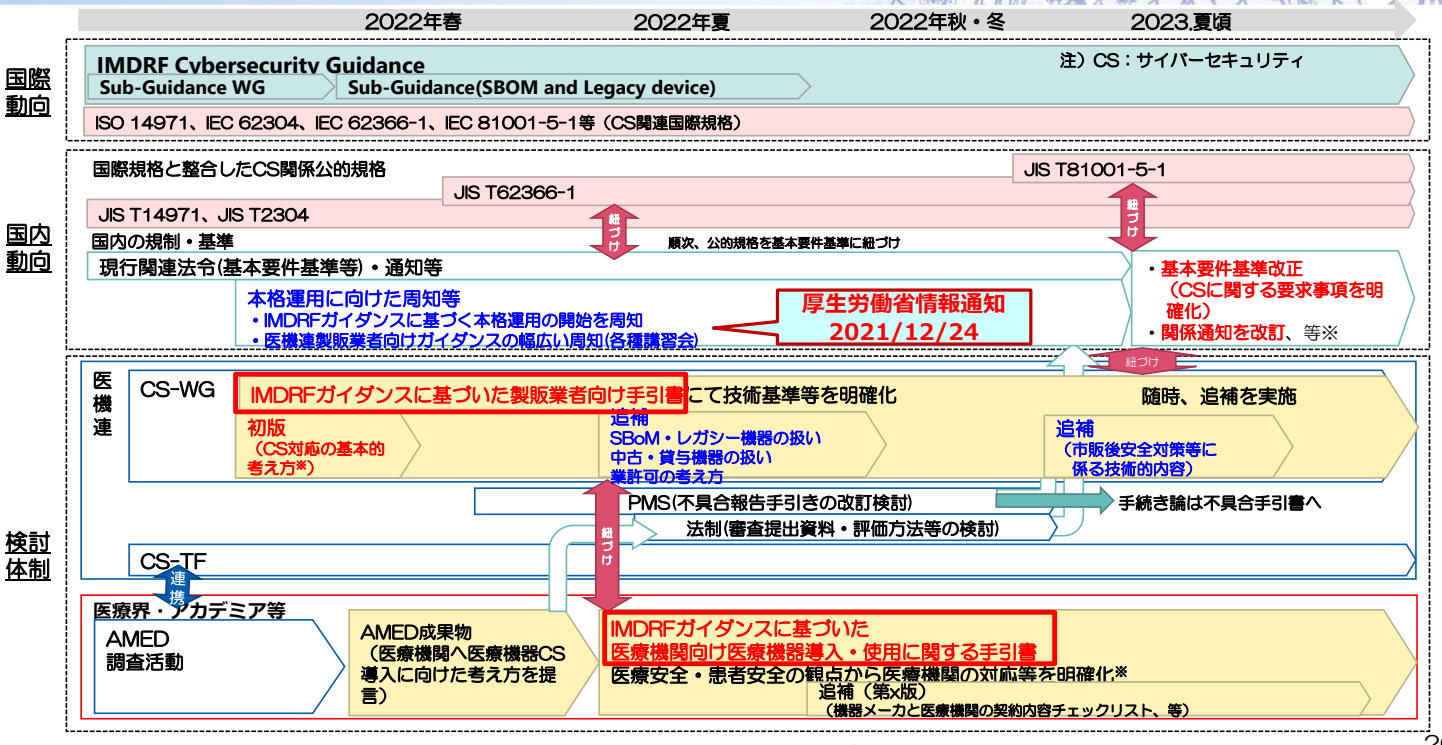
（市販後）
- 使用者への情報提供（SBOMやMDS2，等）
- CVDとして何をすればよいか
- 医療機関では何をするのか
- 医療機関との責任範囲のあり方
- 電子情報システム関連業者との連携

⑤市販後の適正使用・管理の明確化及びガイドライン化

（市販後）
- 各インシデント事例の報告先
- 不具合の考え方の明確化
- インシデント対応の方法
- レガシーデバイスの対応
- 製品寿命年数（EOL）を過ぎた製品のサイバーセキュリティの責任のあり方

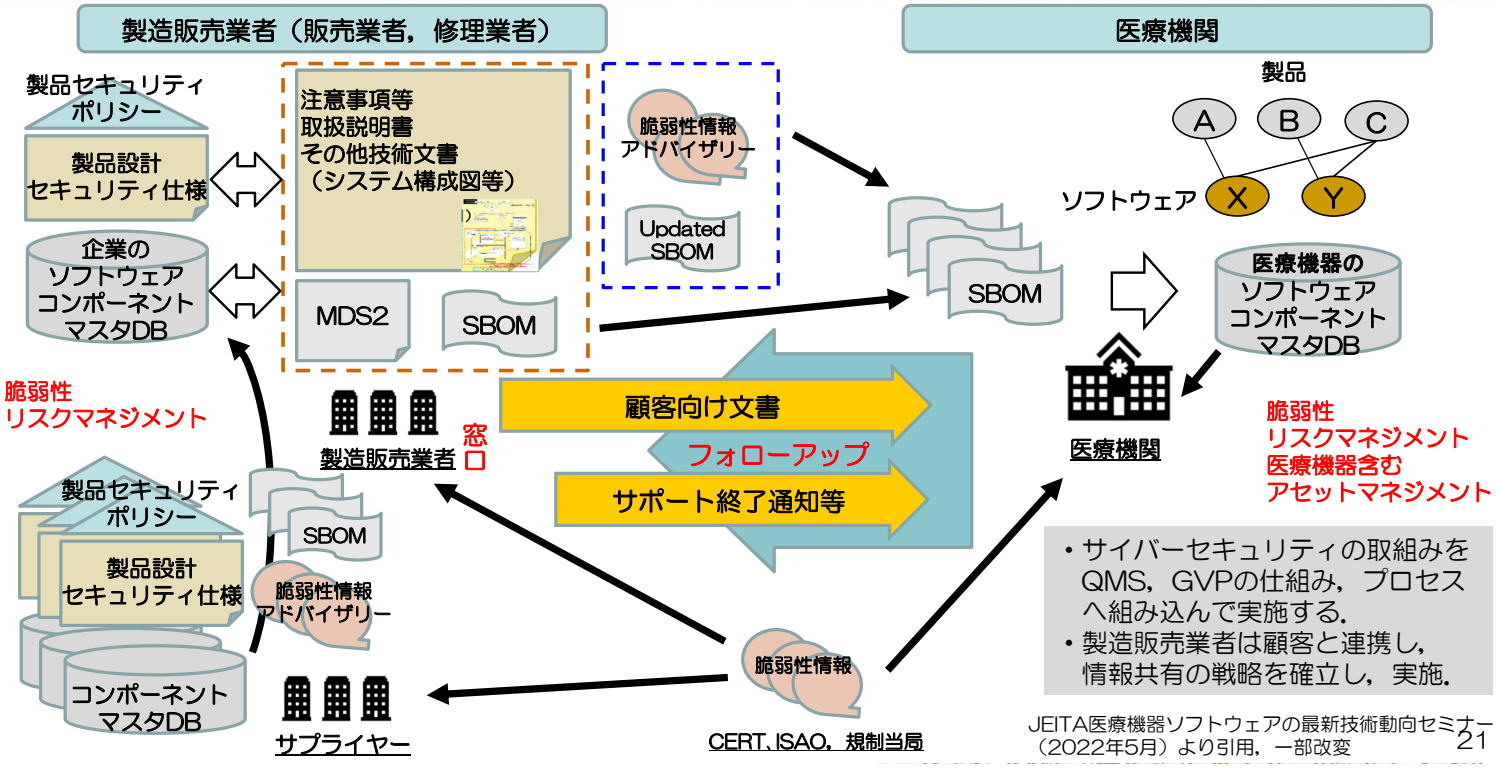
医機連サイバーセキュリティ対応WG資料より

IMDRFガイダンスの国内導入に向けた検討状況
ー今後の予定（2022/3月時点）



※　医政局の医療情報システムの安全管理ガイドラインは患者等の情報保護を目的としたもの

製造販売業者と医療機関との情報共有

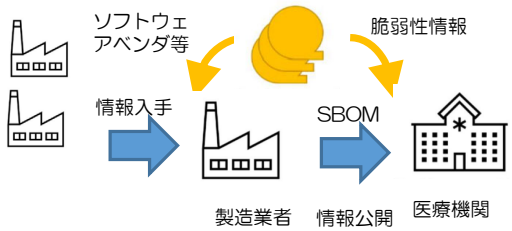


JEITA医療機器ソフトウェアの最新技術動向セミナー（2022年5月）より引用，一部改変

IMDRFガイダンスの3つのキーワード

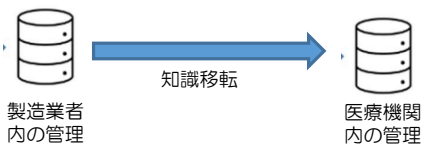
- **Software Bill of Materials（SBOM）**

  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



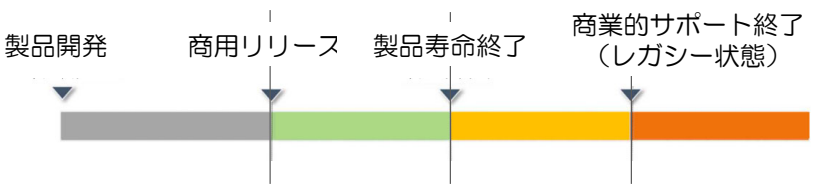
- **Coordinated Vulnerability Disclosure（CVD）「協調的な脆弱性の開示」**

  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

まとめ

- 日本の厚生労働省は，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，2023年夏を目途に，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
Koichiro_Matsumoto@mb1.nkc.co.jp