令和6年度医療機器製造販売業者のサイバーセキュリティ対策周知事業

医療機器サイバーセキュリティの実践

一般社団法人　日本医療機器産業連合会
医療機器サイバーセキュリティ対応WG

Ministry of Health, Labour and Welfare of Japan

令和6年度医療機器製造販売業者のサイバーセキュリティ対策周知事業

■ 医療機器サイバーセキュリティにおける、医療機関との連携に向けた取組と諸課題

1. 医療機器のサイバーセキュリティに関する国内規制の動向

2. 医療機器サイバーセキュリティの実践

- 医療機器のサイバーセキュリティについて
- サイバーセキュリティに係る規格について
  （IEC 81001-5-1:2021）
- 医療機器のサイバーセキュリティ要件に対する
  JIS T 81001-5-1の適用について
  https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/0000179749_00009.html
  https://www.pmda.go.jp/review-services/drug-reviews/about-reviews/devices/0051.html

3. 医療機関との連携及びPSIRTの実践

4.「製造業者/サービス事業者による医療情報セキュリティ開示書」の概要

5. ソフトウェア部品表（SBOM）の作成と運用

医療機器
製造販売業者等

連携

医療機関、
医療情報システム製造業者等

令和6年度医療機器製造販売業者のサイバーセキュリティ対策周知事業

■ 医療機器サイバーセキュリティにおける、医療機関との連携に向けた取組と諸課題

1. 医療機器のサイバーセキュリティに関する国内規制の動向

2. 医療機器サイバーセキュリティの実践
- 医療機器のサイバーセキュリティについて
- サイバーセキュリティに係る規格について（IEC 81001-5-1:2021）
- 医療機器のサイバーセキュリティ要件に対するJIS T 81001-5-1の適用について

3. 医療機関との連携及びPSIRTの実践

4. 「製造業者/サービス事業者による医療情報セキュリティ開示書」の概要

5. ソフトウェア部品表（SBOM）の作成と運用

医療機器
製造販売業者等

連携

医療機関、
医療情報システム製造業者等

目　次

米国の医療機関を中心に2004年から2005年にかけてマルウェアNimdaの大規模感染が発生し、製造販売業者等には、医療機関との連携及び医療機器に導入されたソフトウェアとその保守計画に関する情報提供が求められるようになった。

このための一連の取組み、必要な技術的要件は、国際調和が図られ、国際医療機器規制当局フォーラム（IMDRF）のサイバーセキュリティガイダンスとしてまとめられ、各国又は地域で規制化された。

ここでは、IMDRFガイダンス等に基づいて国際的に求められているサイバーセキュリティ対策の基本的アプローチ、情報共有等に係る取組等について紹介する。

※本資料中の英文の和訳は参考訳です。正確な表現が必要な場合は、元となる英文を参照してください。
※本資料中の記述は、発表者の個人的解釈が含まれており、IMDRFや各国規制当局が認めた内容ではない事を了承ください。
※本資料中には、各社の商標が含まれている場合があります。

1. はじめに

医療機器のサイバーセキュリティ（最初の拡散型大規模感染）

- **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
  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

FDAが示した考慮すべき事項 – 情報共有

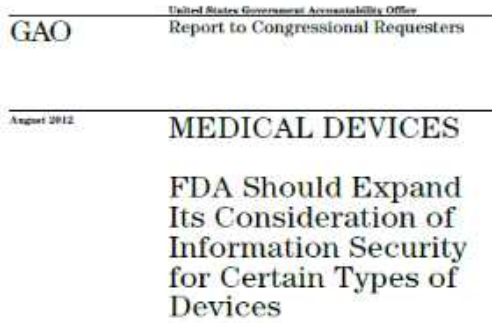
- **医療機関**
  - 購入前に製販業者からCOTS保守計画を入手
  - 機器の製販業者に保守を依頼する
  - MedWatchを使用して、FDAに情報提供
  - 迅速なサポートが行われない場合は、機器の製造業者に書面で（又は口頭で）苦情
- **COTS（サードパーティ）ベンダー**
  - 透明性（Transparency）のあるアップデート提供
    医療機器の製販業者が、医療機関にアップデート提供を可能にする
- **製造販売業者**
  - 市販前申請の提出時にCOTS保守計画を提供

共同責任

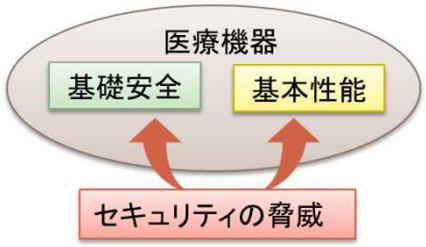
医療機器のセキュリティは、医療施設、患者、医療従事者、および医療機器の製造業者などの関係者の間での共同責任であると認識している。サイバーセキュリティを維持できない場合、結果として、機器の機能性障害、データ（医療上または個人的な）の真正性、可用性や完全性の損失、あるいは他の接続した機器またはネットワークをセキュリティの脅威へ暴露する可能性がある。これにより、患者の疾患、傷害、または死亡に至る可能性がある。

医療機器　サイバーセキュリティに関する脆弱性に関する検討

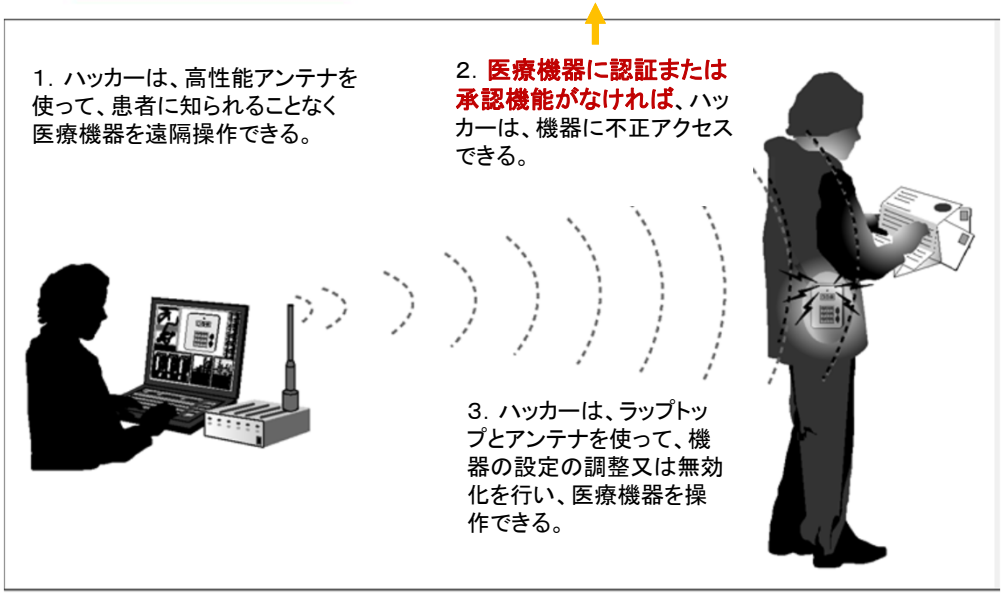
- 医療機器の脆弱性を不正利用
  - 機器設定の不正変更
  - 治療の不正変更または無効化
  - 機密データの喪失または開示
  - 機器の誤動作
  - 他の機器・システムへの拡散


GAO
United States Government Accountability Office
Report to Congressional Requesters
August 2012
MEDICAL DEVICES
FDA Should Expand Its Consideration of Information Security for Certain Types of Devices

2011年
セキュリティ専門家が
遠隔操作で不正利用し、
インスリンポンプの投与量を
変更可能であることを実証



進入路の防御の重要性
“ハードコードされた資格（認証）情報の利用”の悪用がきっかけ



Source: GAO.

遠隔操作によるインスリンポンプの不正アクセスの例
（会計検査院GAOレポート　http://www.gao.gov/products/GAO-12-816）

2013年　医療機器を調査
- 米国ICS-CERT
  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)
  https://ics-cert.us-cert.gov/alerts/ICS-ALERT-13-164-01
  （約40社の300の医療機器）

2014年　医療機器への攻撃
- 医療機器への侵入・拡散は容易と判断される
  （標的型攻撃の入口に）
  http://www.wired.com/2014/04/hospital-equipment-vulnerable/

2015年　医療機関への攻撃

2017年～　ランサムウェア感染多発
「WannaCry」他

2022年
AI利用したランサムウェア

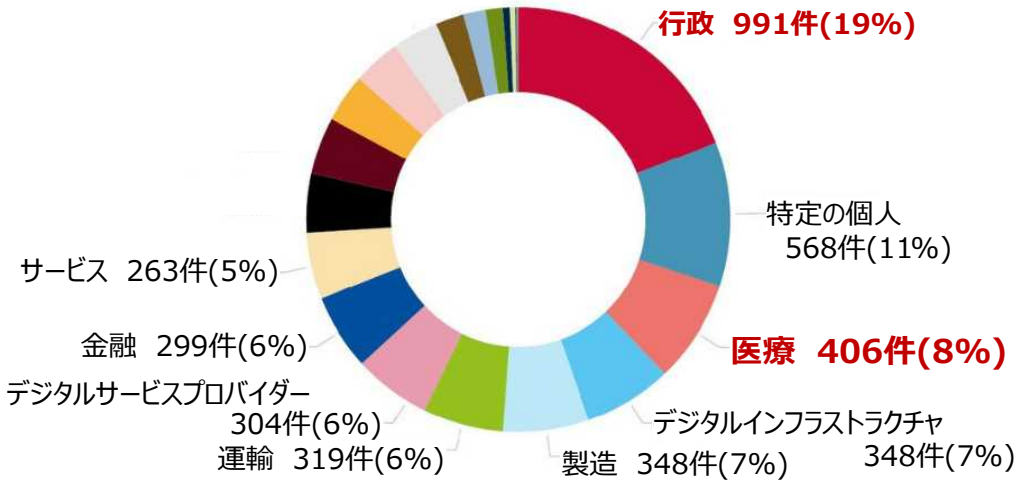
EU動向　ENISA　2023/11

◆ENISA Threat Landscape 2023 <ENISA脅威展望 2023>

URL:　https://www.enisa.europa.eu/news/eu-elections-at-risk-with-rise-of-ai-enabled-information-manipulation

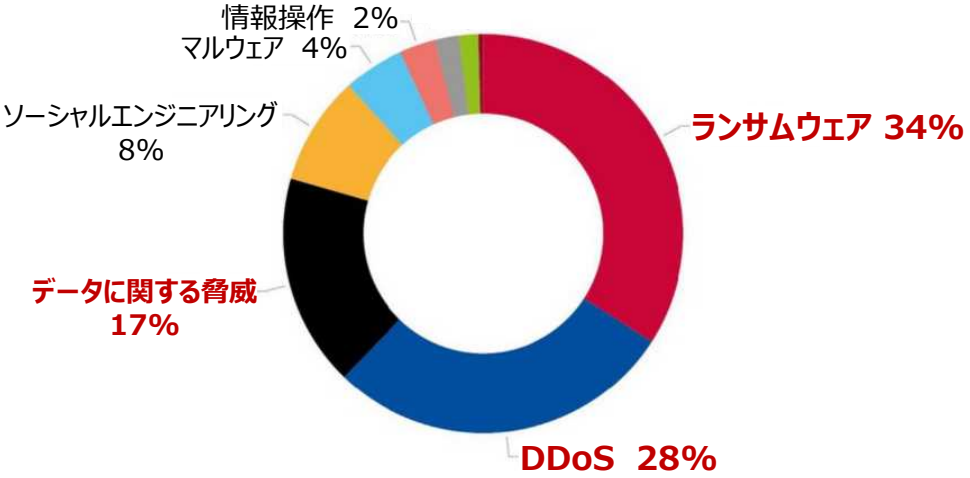
■ **2022年7月～2023年7月までの期間に発見された脅威**について、ENISA Threat Landscape 2023を発行した。

① 主に標的となったのは、行政(19%)、特定の個人(11%)、医療(8%) 。



- 脅威アクターの活動は、地政学的な影響を受け、特定の個人（重要な地位にある個人、政治家など）がますます標的になっている。
- リモート監視および管理ソフトウェアに侵入する、セキュリティ製品の不具合を悪用する、クラウドの設定ミスを悪用する等による危害が加えられている。

② **主な脅威は、ランサムウェアが全体の34%を占め、次にDDoS攻撃が28%**となっている。



- **ランサムウェアは、全業種にを標的としており、製造業(14%)、医療(13%)、サービス業(9%)の順**になっている。
- DDoS攻撃は、行政(34%)を標的としている。次いで、交通機関(17%)、金融機関(9%)の順になっている。

JEITA MEソフトウェア技術専門委員会資料より引用

EU動向　ENISA　2024/11

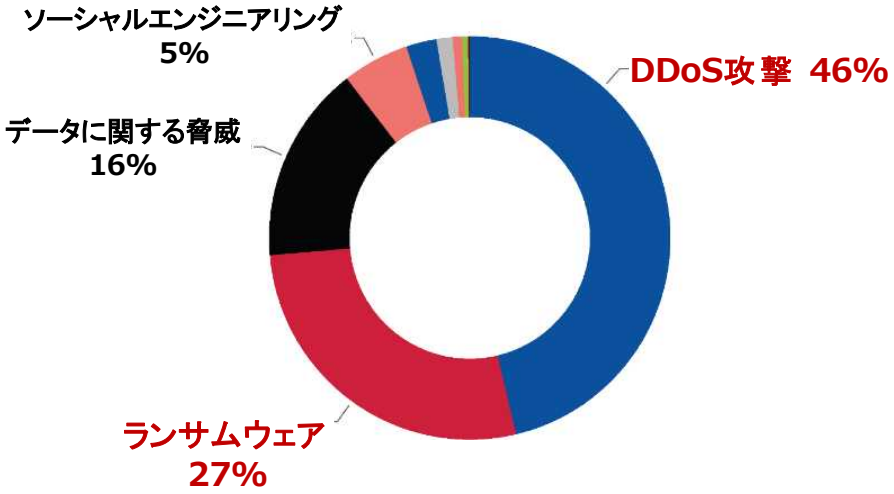
◆ENISA Threat Landscape 2024 ＜ENISA脅威状況2024＞

URL:　https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

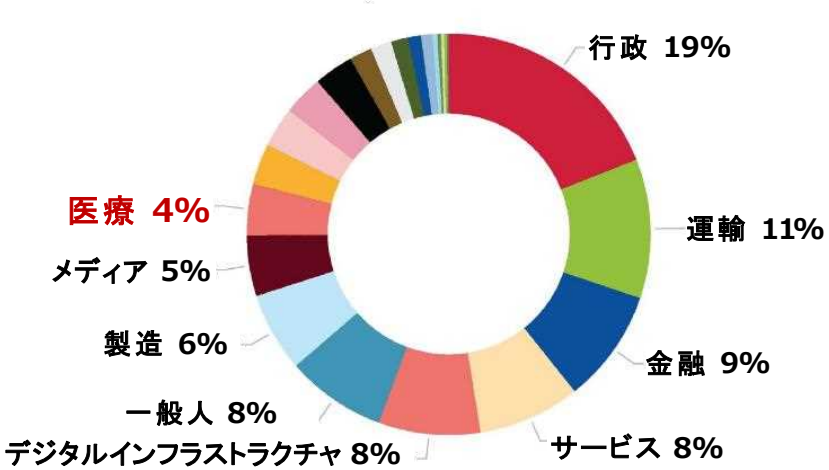
日本国内でもDDoS攻撃が増加
状況は変化

■ 2023年7月～2024年6月までの期間に発見された脅威について、ENISA Threat Landscape 2024を発行した。

① ランサムウェアとDDoS攻撃が多数を占め、次いでデータに関する脅威が続いている。



② 主に標的は、行政(19%)、運輸(11%)、金融(9%)。一般市民を標的にしたソーシャルエンジニアリング、情報操作も確認された。



- 昨年の調査結果と比較すると、DDoS攻撃が1位、ランサムウェアが2位と逆転している。
- DDoS-for-Hireサービスや DDoS攻撃の労力を軽減するツールにより、容易にDDoS攻撃ができるようになり、規模が拡大している。

- DDoS攻撃は、全業種を標的にしている。行政(DDoS攻撃の33%)、運輸(同21%)、金融(同12%) の順になっている。
- ランサムウェアは、サービス(ランサムウェアの18%) 、製造(同17%) 、医療(同8%)の順になっている。

Ministry of Health, Labour and Welfare of Japan

2. インシデント等から得られた医療機器の諸課題

脅威分析、脆弱性マネジメントの必要性 – 大阪急性期・総合医療センターの事例

大阪急性期・総合医療センター 情報セキュリティインシデント調査報告書より抜粋 （2023/3/28 調査委員会）

https://www.gh.opho.jp/pdf/reportgaiyo_v01.pdf

◆ **被害状況** （調査報告書11頁、21頁、28頁、40～41頁）

No	項目	被害内容
1	電子カルテ含む総合情報システム	基幹システムサーバーの大部分がランサムウェアにより暗号化。 PC端末（院内に約2,200台）も不正アクセスの痕跡あり ⇒全てのサーバー、端末をクリーンインストール 基幹システムサーバー再稼働に43日間、 部門システム含めた全体の診療システム復旧に73日間を要す
2	診療制限	2022年11月の診療実績　（前年同月対比）　※2022年12月は現在計算中 新入院患者数:　558人　（前年同月比 33.3%） 延入院患者数:10,191人　（前年同月比 52.9%） 初診患者数　:　465人　（前年同月比 17.9%） 延外来患者数:15,744人　（前年同月比 61.6%）
3	被害額	現在精査中　調査・復旧費用で数億円以上 診療制限に伴う逸失利益として十数億円以上を見込んでいる

◆ 組織的発生要因と予防に向けた提案 （調査報告書15～17頁）

② 契約に関する諸問題

契約の段階で、役割分担や責任分界点などが明示されておらず、保守の範囲や機器の管理方法が曖昧であったため、脆弱性の管理が不十分であったり、外部接続の管理が不十分であった。

【契約段階でのリスクを回避するための措置】
1）共通したセキュリティポリシーによる調達
2）契約時のガイドラインに基づく文書確認（責任分界点（信頼境界）や役割分担の確認）
3）医療情報部門との情報共有による情報資産管理の徹底
4）複数のベンダーによる保守を含んだ契約の場合のプロジェクトマネジメント体制の確認
5）保守を含んだ契約の場合の保守方法の確認

◆ 技術的要因 （調査報告書18～19頁）

① 外部接続（リモートメンテナンス）の管理不備

No	発生原因	発生要因
1	サプライチェーンのVPN機器の脆弱性が放置されていた。	VPN機器やファイアウォール等外部通信機器の保守や脆弱性管理など役割分担が曖昧だった
2	リモートデスクトップ通信（RDP）接続が常時接続となっていた。	リモート保守を許可するための基準が曖昧で、またリモート保守を行う側のセキュリティ環境の確認が不十分だった。
		外部接続（リモート保守）を許可した後に、その利用状況を確認していなかった。

② 内部のセキュリティが脆弱

No	横展開を許した初期設定
1	ユーザーすべてに管理者権限を与えていたため、攻撃者に管理者権限を利用され、ウイルス対策ソフトをアンインストールされた。
2	Windowsのパスワードが、サーバー、端末毎にすべて共通であり、一つのパスワードが窃取されると、他のすべてのサーバー（端末）が乗っ取り可能な状態
3	アカウントロックアウトの設定が無く、パスワード総当たり攻撃や辞書攻撃によりパスワードを数多く試行されログオンが成功した。
4	電子カルテシステムサーバーにウイルス対策ソフト未設定のため、容易に侵入され、ランサムウェアを実行された（他のサーバーや端末にはウイルス対策インストール済み）。

最近のインシデントから得られた教訓について

- インシデントから得られた教訓

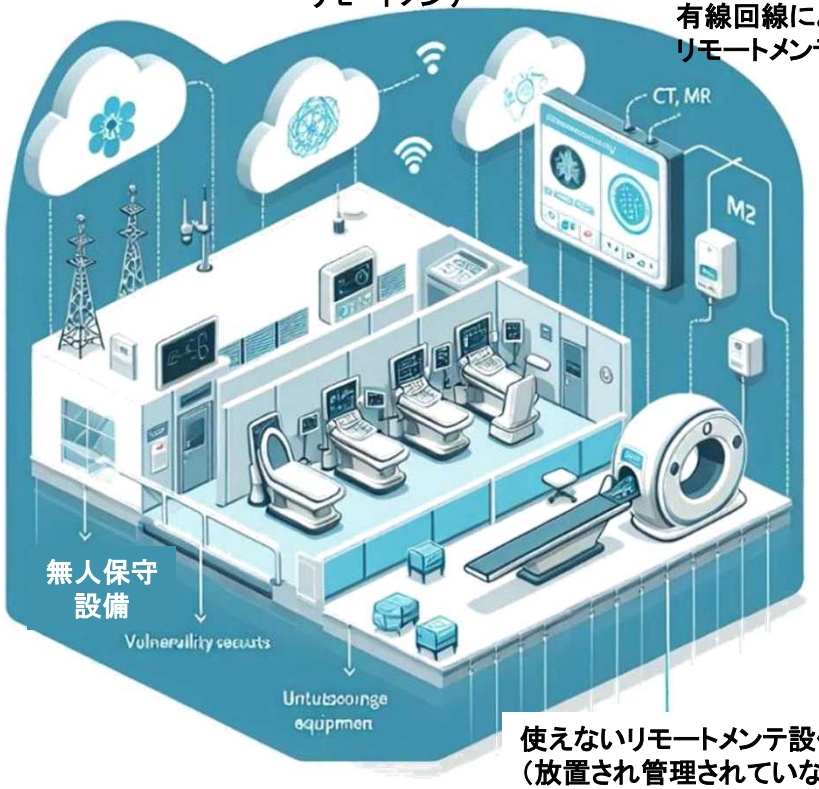
（医療セプターAMBER【全分野】:最近のインシデントから得られた教訓について 2024/10/17）

(1) **サプライチェーン全体でのサイバーセキュリティ向上の取組**が必要
(2) 攻撃を想定したシステム設計と**障害発生時における適切な広報の実施**が必要
(3) **認証手段の高度化の実施**と**認証情報の適切な管理・運用**が必要
(4) **ユーザーリテラシー向上に加えシステム的な対策**が必要

医療セプター（2024年10月17日）情報より

- 製品セキュリティポリシー
- 設計段階からのセキュリティ確保（Secure by Design）
- 協調的脆弱性開示（CVD）

契約等に基づくセキュリティ情報の透明性確保
- **責任分界点（信頼境界）**や**役割分担**の確認

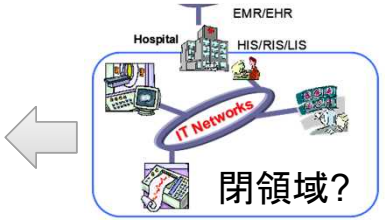


多くの医療機器に独立したリモートメンテ回線が接続された施設のイメージ図（AI利用）

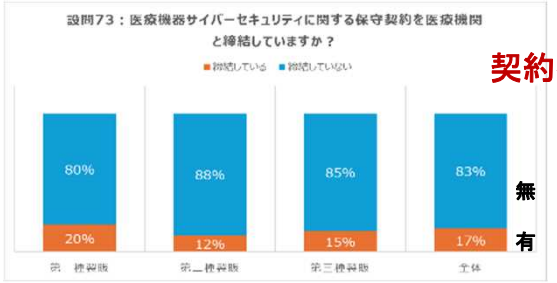
最近のインシデントから得られた教訓について　続き

■ **医療機器及び関連事業者（サプライチェーン）に対する指摘**
（インシデント対応時の復旧作業及び再発防止処置等について：複数のセキュリティ関連団体から指摘）

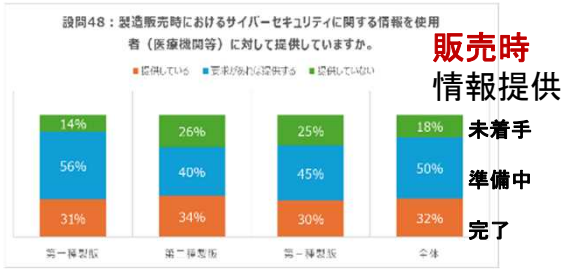
- **古いOS（EOS間近）を使用した医療機器の販売**
（例えば、2010年以降のWindows2000の使用等）
- 薬機法の誤った解釈による**セキュリティパッチ等の適用拒否**
- **リモートメンテ用機材**に関するサイバーセキュリティに関する**情報の非開示**
- 責任分解（信頼境界）、役割や保守を明示した**契約書が皆無**
- MDS/SDS、SBOM等の**セキュリティ関連情報の提出依頼に対する未回答**
（医療機関との間に入る**業者に対して、指導・教育**ができていない。）
- 医療機関等の**求めに応じて情報を提供する体質は不適切**



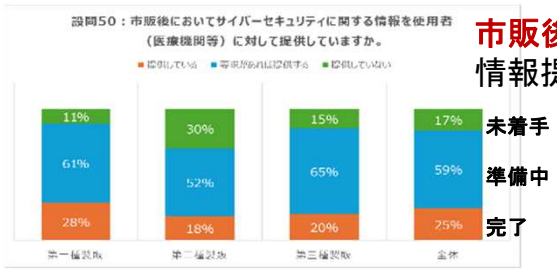
- 製品の基本的サイバーセキュリティ対策及び説明（取説他含む）の実施、設置（実使用）環境に沿った責任分界等調整、契約等の文書化という当たり前の事を確実に実施すべきである。



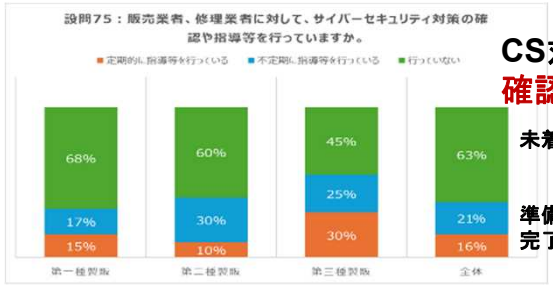
契約有無



販売時
情報提供



市販後
情報提供



CS対策の確認、指導

厚生労働科学研究「医療機関における医療機器のサイバーセキュリティの確保に関する研究」
医療機器製造販売業者等に対する令和６年度アンケート実施結果（2025/1）参照

Ministry of Health, Labour and Welfare of Japan

3. 医療機器サイバーセキュリティの国際的な取組

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NIS2指令
- 日本基本要件基準改正

国際協力の枠組み

米国政府調達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 固定パス
脆弱性報告 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

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

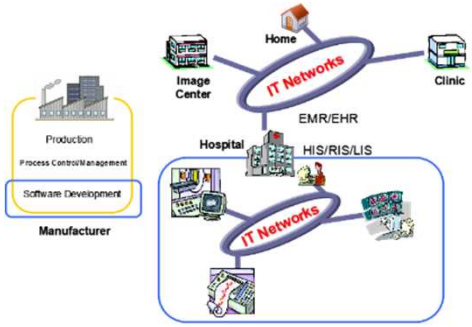
サイバーリスクを含むリスクマネジメント　ISO 14971 Ed3　JIS

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



（参考） 医療機器に対する各国セキュリティ関連規制ガイダンス （2024/12/1現在）

地域	セキュリティ関連規制	発行日
米国	Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions (Final)	2023-09-27
	Select Updates for the Premarket Cybersecurity Guidance: Section 524B of the FD&C Act（上記一部更新）	2024-03-13
	Postmarket Management of Cybersecurity in Medical Devices	2016-12-27
	FDA Content of Premarket Submissions for Device Software Functions (Final)	2023-06-14
	Off-The-Shelf Software Use in Medical Devices	2023-08-11
カナダ	Pre-market Requirements for Medical Device Cybersecurity	2019-06-26
オーストラリア	Medical device cyber security guidance for industry	2021-03
シンガポール	Cybersecurity Labelling Scheme v1.3	2023-09
中国	医療機器ソフトウェア登録審査ガイドライン（2022年改訂版） 医療機器のサイバーセキュリティ登録審査ガイドライン（2022年改訂版）	2022-03-09 2022-03-09
韓国	医療機器のサイバーセキュリティ 許可審査ガイドライン	2019-11-28
フランス	Guideline on Cybersecurity from ANSM	2019-07-26
欧州	MDCG 2019-16 Guidance on Cybersecurity for medical devices	2020-01-07
日本	医療機器のサイバーセキュリティ導入に関する手引書（Ed.2）	2023-03-31
IMDRF	N60 Principles and Practices for Medical Device Cybersecurity	2020-03-18
IMDRF	N70 Principles and Practices for the Cybersecurity of Legacy Medical Devices（レガシー医療機器）	2023-03-28
IMDRF	N73 Principles and Practices for the Software Bill of Materials for Medical Devices（SBOM）	2023-03-28

国際的なサイバーセキュリティの動向　ー　“Secure by Design Guidance”改訂（2023/10/16）

- Hardening Guide（セキュアな環境での使用を前提の設計）から
  Loosening Guide（Internetに直接接続されていてもセキュアな状態を確保する設計）の提供へ
  これまで、医療機器のような製品は、隔離したネットワークやInternetから隔離したネットワークでの使用を前提として提供や設計を行ってきたかもしれません。（未だに取説等に記載しているケースもあり）
  それが、今後は、顧客に提供する文書がセキュアに利用するためのHardening Guideから利便性の為に既定のセキュリティを緩和するためのLoosening Guideの提供の方向になっていく、つまり**製品そのものがデフォルトでセキュアな状態を維持できる設計でなければならないということが求められる**ということ。

https://www.cisa.gov/news-events/alerts/2023/10/16/cisa-nsa-fbi-and-international-partners-release-updated-secure-design-guidance
https://www.cisa.gov/resources-tools/resources/secure-by-design
https://www.itmedia.co.jp/enterprise/articles/2310/19/news065.html

医療機関=閉領域=セキュアな環境

古い製品も継続使用可能？
- サポート期間が終了したOSを使用
- 機器側で脆弱性対策不要

日本のサイバーセキュリティ戦略等も参照
Japan’s National Center of Incident Readiness and Strategy for Cybersecurity (NISC)
» https://www.nisc.go.jp/eng/pdf/cs-strategy-en-pamphlet.pdf
Japan’s Ministry of Economy, Trade and Industry (METI)
» Guide of Introduction of Software Bill of Materials (SBOM) for Software Management
https://www.meti.go.jp/english/press/2023/0728_001.html
» Collection of Use Case Examples Regarding Management Methods for Utilizing OSS and Ensuring Its Security
https://www.meti.go.jp/english/press/2021/0421_003.html

サイバー対策、日米英など13か国が国際協力枠組み発足（2023/10/17）

河野デジタル相は17日の記者会見で、**サイバー対策の一環としてソフトウェア事業者らに安全対応の負担と責任を求めるため、日米英やイスラエルなど計13か国が同日、国際協力枠組みを発足させたと発表**した。参加国は製造物責任の観点を重視し、**事業者らにユーザー保護を促すための国際指針作り**に乗り出す。

枠組みには米連邦捜査局（FBI）や英国家サイバーセキュリティセンターなど各国のサイバー当局が参加し、日本からは内閣サイバーセキュリティセンター（NISC）などが加わった。日本政府は指針作りを通じて各国との連携を深め、サイバー対策の強化につなげることを目指している。

指針では、**事業者が製品の開発段階から取り組むべき原則として、▽顧客のセキュリティー上の結果に責任を負う▽徹底的な透明性と説明責任を受け入れる▽セキュリティー向上を経営の優先事項とする** の3点を掲げる方針だ。指針は法的拘束力を持たないが、事業者にとって「製品の安全を確保するロードマップ」と位置付ける。

〈1〉ウイルスをシステム全体に広げないための多層防御を導入する
〈2〉システムの初期設定で簡単なパスワードを導入しないようにする
〈3〉システムに入る際は複数の認証プロセスを経る
〈4〉セキュリティー対策の責任者を公表する

枠組みに参加する各国は、**指針策定に関して、顧客であるユーザーの負担を軽減し、事業者側にサイバー対策を巡る負担や責任**を求めることを柱とする考えだ。

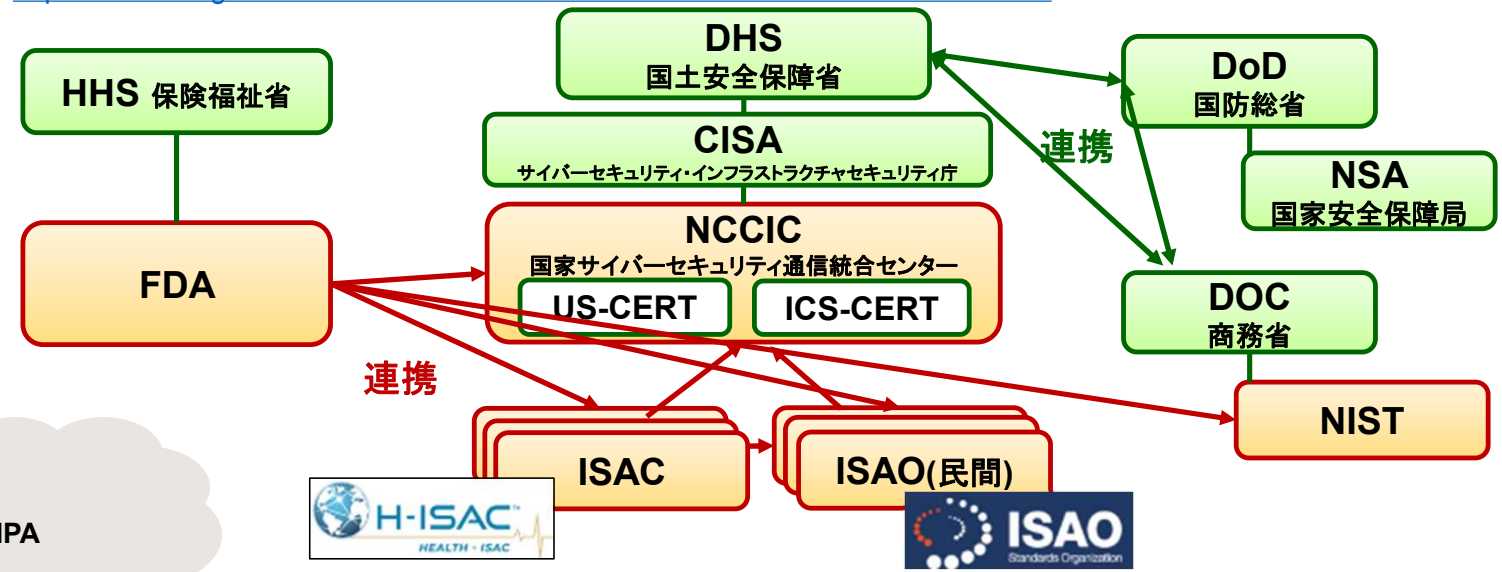
サイバー攻撃に対して脆弱な製品を販売し、購入したユーザーがサイバー被害に遭った場合、**「製品を開発した事業者にも責任の一端がある」との認識**が広がっていることが背景にある。（← “Secure by Design Guidance” ）

サイバー対策、日米英など13か国が国際協力枠組み発足…事業者の責任重視する指針作成へ https://www.yomiuri.co.jp/politics/20231017-OYT1T50133/
※強調表示は本資料作成者にて実施

国際的なサイバーセキュリティに関連する組織及び連携 ー 国家安全保障戦略

- **CERT, ISAC, ISAO: 脅威・脆弱性に関する情報共有（分析）組織**
  - 業界セクター毎に**ISAC**設置　※医療では H-ISAC（国際）
  - 大統領令13691より ISACと連携支援する**ISAO**設置が分野地域毎に進む

FDAはISAOとの連携を通した情報の共有を推奨している。ガイダンスにも記載。
https://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm481968.htm



日本国内
- NISC
- JPCERT/CC / IPA
- 医療セプター
- 医療分野のISAC設立

民間企業と連携し脆弱性やインシデント情報を収集・分析・共有

ISAO: Information Sharing and Analysis Organizations
H-ISAC: Health Information Sharing and Analysis Center
https://h-isac.org/

JEITA 医療用ソフトウェア専門委員会提供

Ministry of Health, Labour and Welfare of Japan

4. 医療機器サイバーセキュリティの法規制及び規格の動向

医療機器に関するセキュリティ－医療機器規制と個人情報保護

医療法施行規則第14条第２項と基本要件基準第12条第3項では、
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。

【医療法施行規則第１条第11項】
病院等の管理者は、法第６条の12の規定に基づき、次に掲げる**安全管理のための体制を確保**しなければならない。一　医療に係る安全管理のための指針を整備すること。

【医療法施行規則第１４条第１項】
病院又は診療所の管理者は、その病院又は診療所に存する医薬品、医療機器及び再生医療等製品につき**医薬品医療機器等法の規定に違反しないよう必要な注意**をしなければならない。

【医療法施行規則第14条第２項】
病院、診療所又は助産所の管理者は、医療の提供に著しい支障を及ぼすおそれがないように、**サイバーセキュリティ（サイバーセキュリティ基本法第２条に規定するサイバーセキュリティをいう。）を確保するために必要な措置**を講じなければならない。

【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**　https://www.mhlw.go.jp/content/12301000/001084098.pdf

製造業者/サービス事業者による医療情報セキュリティ開示書」ガイド　https://www.jahis.jp/standard/detail/id=779
（MDS: 医療情報を扱う医療機器、SDS：リモートサービスを利用する医療機器）
5.2版のチェックリストをそのまま使用する。https://www.jahis.jp/standard/detail/id=987

【基本要件基準第12条第3項】
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**

【医療機器のサイバーセキュリティ導入に関する手引書】
IMDRFガイダンスを踏まえて、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、製造販売業者が実施する、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要件等を取りまとめている。 https://www.mhlw.go.jp/content/11120000/001167217.pdf

製造業者による医療機器セキュリティ開示書（MDS2）　https://www.jira-net.or.jp/publishing/security.html

医療機器製造販売業者は、ISMS等に基づく企業としてのセキュリティ対応を実施することは、他分野と同様である。

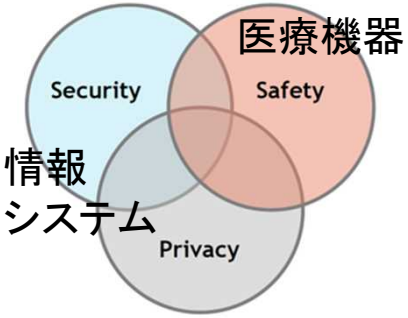
医療情報システムの機密性・完全性・可用性を確保する

医療機器の有効性と安全性を確保し、患者安全に繋げる

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

医療情報システムの安全管理に関するガイドライン第 6.0 版 （2023/5）

- 医療情報システムの安全管理に関するガイドライン 第 6.0 版
  概説編（Overview）と、医療情報システムの安全管理を実施するための統制・管理について各編で想定する読者類型ごとに整理した、経営管理編（Governance）、企画管理編（Management）、システム運用編（Control）の４編から構成する。
- 医療情報システムの安全管理に関するガイドライン第6.0 版（令和５年５月） https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html
- 医療機関におけるサイバーセキュリティ対策チェックリスト（令和５年６月） https://www.mhlw.go.jp/content/10808000/001104308.pdf



医療機関におけるサイバーセキュリティ対策チェックリスト

事業者確認用

○ 令和５年度中

*以下項目は令和５年度中にすべての項目で「はい」にマルが付くよう取り組んでください。
*１回目の確認で「いいえ」の場合、令和５年度中の対応目標日を記入してください。

	チェック項目	確認結果（日付） 1回目	目標日	2回目	備考
1 体制構築	（1） 事業者内に、医療情報システム等の管理に係る管理責任者を設置している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）	
2 医療情報システムの管理・運用	医療情報システム全般について、以下を実施している。				
	（2） リモートメンテナンス（保守）している機器の有無を確認した。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）	
	（3） 医療機関に製造業者/サービス事業者による医療情報セキュリティ開示書（MDS/SDS）を提出した。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）	
	サーバについて、以下を実施している。				
	（4） 利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）	
	（5） 退職者や使用していないアカウント等、不要なアカウントを削除している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）	
	（6） アクセスログを管理している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）	
	ネットワーク機器について、以下を実施している。				
	（7） セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）	
	（8） 接続元制限を実施している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）	

医療機関におけるサイバーセキュリティ対策チェックリスト

事業者確認用

○ 参考項目（令和６年度中）

*以下項目について、令和６年度中にすべての項目で「はい」にマルが付くよう取り組んでください。

	チェック項目	確認結果（日付） 1回目	目標日	2回目	備考
2 医療情報システムの管理・運用	サーバについて、以下を実施している。				
	（7） セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）	
	（9） バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）	
	端末 PC について、以下を実施している。				
	（4） 利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）	
	（5） 退職者や使用していないアカウント等、不要なアカウントを削除している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）	
	（7） セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）	
	（9） バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）	

医療情報システムの安全管理に関するガイドライン第 6.0 版 （2024/5）

- 令和6年度版「医療機関におけるサイバーセキュリティ対策チェックリスト」及び「医療機関におけるサイバーセキュリティ対策チェックリスト マニュアル　～医療機関・事業者向け～」について
- 医療機関におけるサイバーセキュリティ対策チェックリスト（令和6年5月）
  https://www.mhlw.go.jp/content/10808000/001253950.pdf

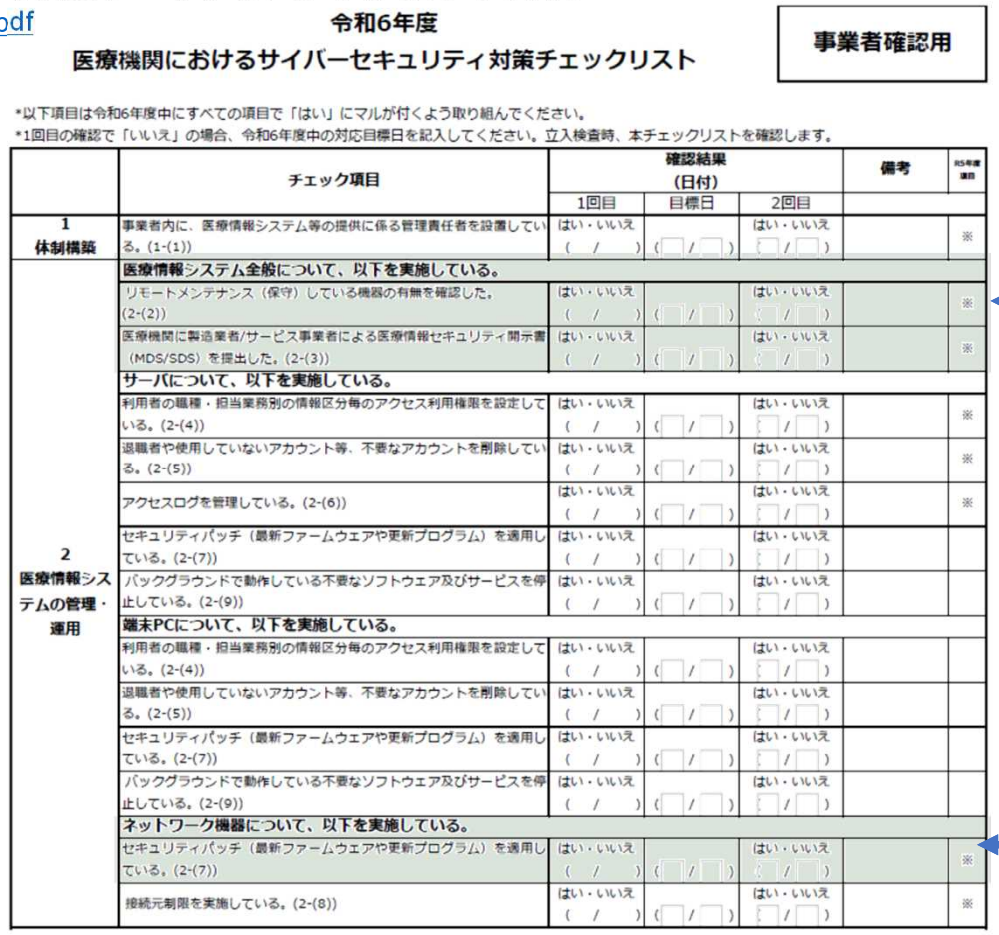
令和6年度版
医療機関におけるサイバーセキュリティ対策チェックリスト

医療機関確認用

	チェック項目	確認結果（日付）	備考
医療情報システムの有無	医療情報システムを導入、運用している。 （「いいえ」の場合、以下すべての項目は確認不要）	はい・いいえ （　/　）	

*以下項目は令和6年度中にすべての項目で「はい」にマルが付くよう取り組んでください。
*1回目の確認で「いいえ」の場合、令和6年度中の対応目標日を記入してください。立入検査時、本チェックリストを確認します。

	チェック項目	確認結果（日付） 1回目	目標日	2回目	備考	R5年度項目
1 体制構築	医療情報システム安全管理責任者を設置している。(1-(1))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		※
2 医療情報システムの管理・運用	**医療情報システム全般について、以下を実施している。**					
	サーバ、端末PC、ネットワーク機器の台帳管理を行っている。(2-(1))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		※
	リモートメンテナンス（保守）を利用している機器の有無を事業者等に確認した。(2-(2)) ※事業者と契約していない場合には、記入不要	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		※
	事業者から製造業者/サービス事業者による医療情報セキュリティ開示書（MDS/SDS）を提出してもらう。(2-(3)) ※事業者と契約していない場合には、記入不要	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		※
	サーバについて、以下を実施している。					
	利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。(2-(4))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		※
	退職者や使用していないアカウント等、不要なアカウントを削除している。(2-(5))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		※
	アクセスログを管理している。(2-(6))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		※
	セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。(2-(7)	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		
	バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。(2-(9))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		
	端末PCについて、以下を実施している。					
	利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。(2-(4))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		
	退職者や使用していないアカウント等、不要なアカウントを削除している。(2-(5))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		
	セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。(2-(7))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		
	バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。(2-(9))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		
	ネットワーク機器について、以下を実施している。					
	セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。(2-(7))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		※
	接続元制限を実施している。(2-(8))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		※
3 インシデント発生に備えた対応	インシデント発生時における組織内と外部関係機関（事業者、厚生労働省、警察等）への連絡体制図がある。(3-(1))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		※
	インシデント発生時に診療を継続するために必要な情報を検討し、データやシステムのバックアップの実施と復旧手順を確認している。(3-(2))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		
	サイバー攻撃を想定した事業継続計画（BCP）を策定している。(3-(3))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		



令和6年度
医療機関におけるサイバーセキュリティ対策チェックリスト

事業者確認用

*以下項目は令和6年度中にすべての項目で「はい」にマルが付くよう取り組んでください。
*1回目の確認で「いいえ」の場合、令和6年度中の対応目標日を記入してください。立入検査時、本チェックリストを確認します。

	チェック項目	確認結果（日付） 1回目	目標日	2回目	備考	R5年度項目
1 体制構築	事業者内に、医療情報システム等の提供に係る管理責任者を設置している。(1-(1))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		※
2 医療情報システムの管理・運用	**医療情報システム全般について、以下を実施している。**					
	リモートメンテナンス（保守）している機器の有無を確認した。(2-(2))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		※
	医療機関に製造業者/サービス事業者による医療情報セキュリティ開示書（MDS/SDS）を提出した。(2-(3))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		※
	サーバについて、以下を実施している。					
	利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。(2-(4))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		※
	退職者や使用していないアカウント等、不要なアカウントを削除している。(2-(5))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		※
	アクセスログを管理している。(2-(6))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		※
	セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。(2-(7))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		
	バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。(2-(9))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		
	端末PCについて、以下を実施している。					
	利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。(2-(4))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		
	退職者や使用していないアカウント等、不要なアカウントを削除している。(2-(5))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		
	セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。(2-(7))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		
	バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。(2-(9))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		
	ネットワーク機器について、以下を実施している。					
	セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。(2-(7))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		※
	接続元制限を実施している。(2-(8))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		※

← リモートメンテ追加

← ネットワーク機器追加

令和6年度医療機器製造販売業者のサイバーセキュリティ対策周知事業

■ 医療機器サイバーセキュリティにおける、医療機関との連携に向けた取組と諸課題

1. 医療機器のサイバーセキュリティに関する国内規制の動向

2. 医療機器サイバーセキュリティの実践

- 医療機器のサイバーセキュリティについて
- サイバーセキュリティに係る規格について（IEC 81001-5-1:2021）
- 医療機器のサイバーセキュリティ要件に対するJIS T 81001-5-1の適用について

3. 医療機関との連携及びPSIRTの実践

4.「製造業者/サービス事業者による医療情報セキュリティ開示書」の概要

5. ソフトウェア部品表（SBOM）の作成と運用

医療機器
製造販売業者等

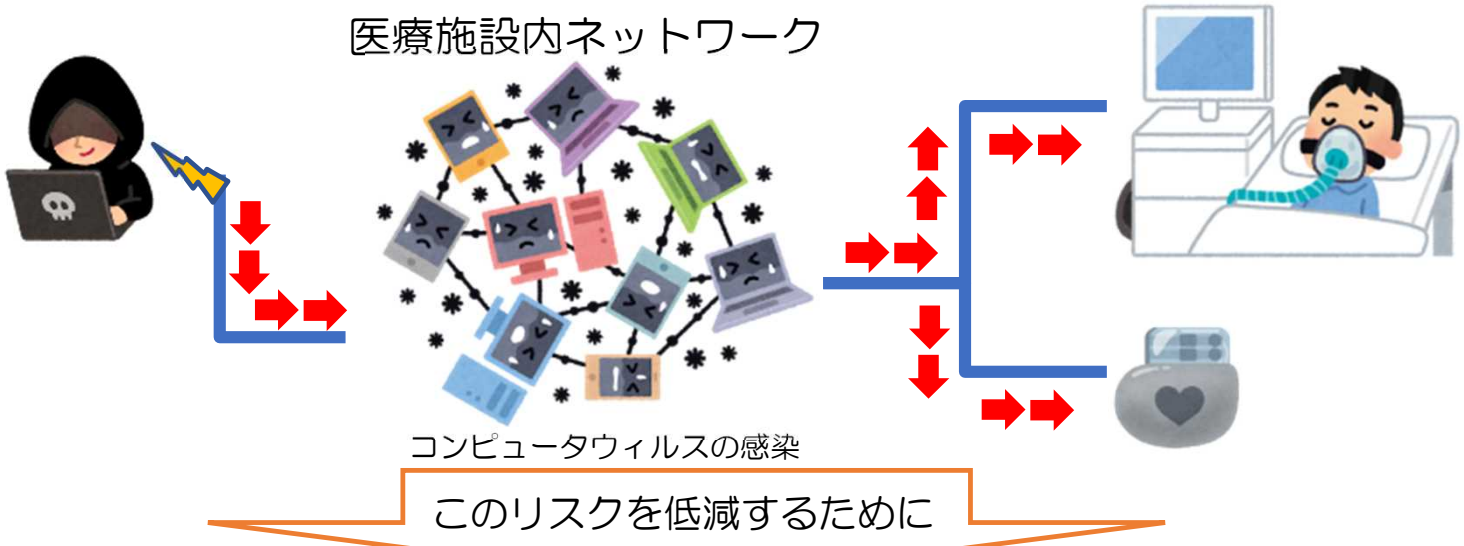
連携

医療機関、
医療情報システム製造業者等

- 基本要件基準第12条第3項について（おさらい）

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



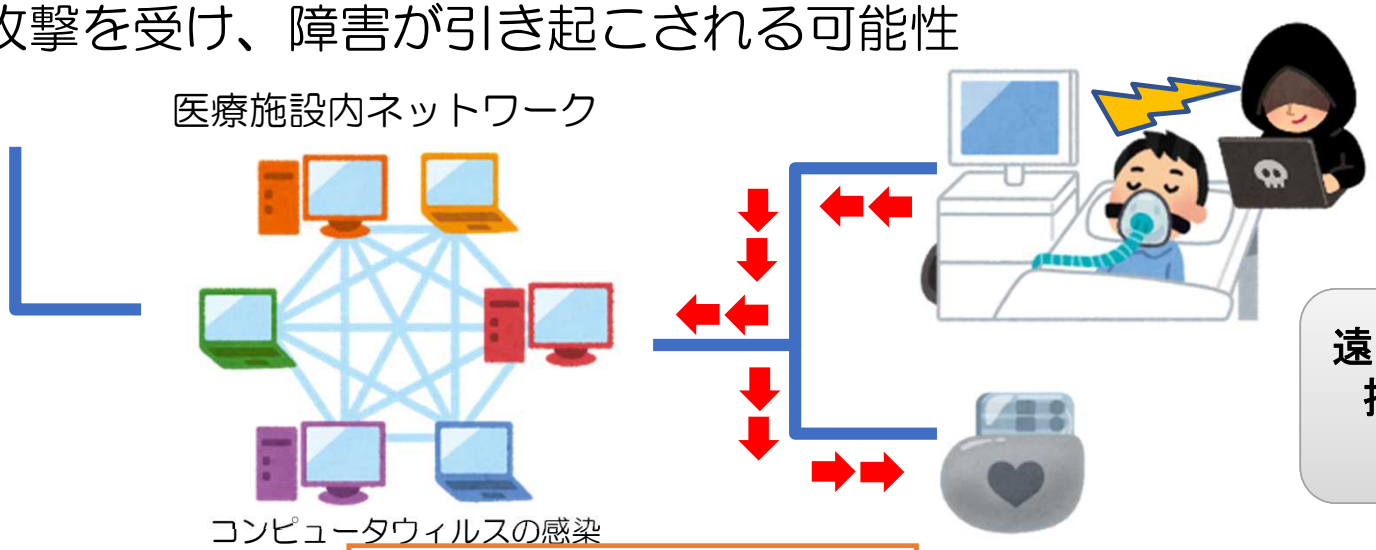
このリスクを低減するために

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

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

製品ライフサイクル全体を見据えた開発・設計

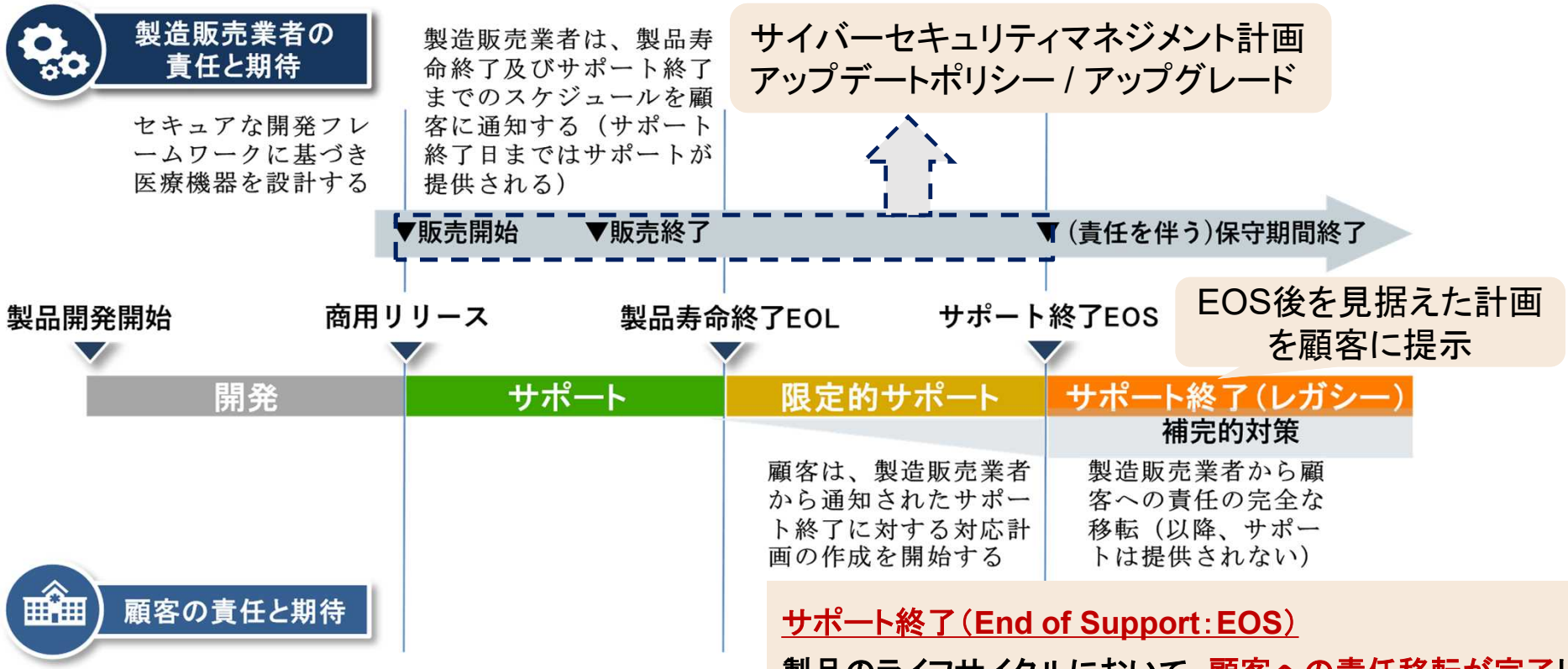


図　製品ライフサイクルにおけるレガシー医療機器の概念フレームワーク

サポート終了（End of Support：EOS）

製品のライフサイクルにおいて、顧客への責任移転が完了し、製造販売業者が、全てのサポート活動を終了する時点。

レガシー医療機器

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は、販売開始以降の年数にかかわらずレガシーであるとみなされる。

基本要件基準第12条第3項について

厚労省医療機器審査管理課資料引用

基本要件基準第12条第3項

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。

他の医療機器、IoT機器、外部記憶媒体、電子カルテや病院内外のネットワーク等に接続する医療機器

サイバーセキュリティ取扱い通知

悪意をもった不正アクセス、過剰な負荷を与える攻撃、マルウェア感染などが想定される医療機器

対象となる医療機器の明確化

ソフトウェアを意図したとおりに動作させるために必要最低限な要件（動作環境及び使用環境)の特定 ← IMDRF N47文書の5.8.4及びサイバーセキュリティ確保通知

サイバーリスクを適切に低減する設計及び製造（サイバーリスクの特定及び評価） ← IMDRF N47文書の5.5.6及びサイバーセキュリティ確保通知

製品の全ライフサイクルにわたって、適切なレベルのサイバーセキュリティを提供する設計、製造及び保守 ← IMDRF N47文書の5.8.5及びIMDRF N60文書の4．2

- サイバーセキュリティ確保通知：「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）
- サイバーセキュリティ取扱い通知：「医療機器の基本要件基準第12条第3項の適用について」（令和5年3月31日付け薬生機審発0331 第8号）
- IMDRF N47文書： IMDRF/GRRP WG/N47 FINAL:2018 “Essential Principles of Safety and Performance of Medical Devices and IVD Medical Devices”
- IMDRF N60文書：IMDRF/CYBER WG/N60 FINAL:2020 “Principles and Practices for Medical Device Cybersecurity”

基本要件基準第12条第3項の適合性の確認について

厚労省医療機器審査管理課資料引用

基本要件基準第12条第3項

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。

対象となる医療機器の明確化

JIS T 81001-5-1:2023

ヘルスソフトウェア及びヘルスITシステムの安全、有効性及びセキュリティー第5-1部：セキュリティー製品ライフサイクルにおけるアクティビティ）

JIS T 81001-5-1は、ソフトウェアのサイバーセキュリティを強化するために、ライフサイクルにおいて実行するアクティビティを規定し、品質マネジメントシステム及びリスクマネジメントシステムの下でソフトウェアを開発・保守することを規定している。

JIS T 81001-5-1等への適合性を確認することによって、これらへの適合を示す。

それぞれの要件に対して、文書番号等の社内文書を特定する情報を示す（Q&A＃2）

この際の留意事項として、
JISに関連する要求事項及び
JISに関連する既存通知等の要求事項
を具体的に示している。

「医療機器の基本要件基準第12条第3項の適合性の確認について」
（令和5年5月23日付け薬生機審発0523第1号）（適合性確認通知）

また、「医療機器の基本要件基準第12条第3項の適用に関する質疑応答集（Q&A）について」（令和5年7月20日付け事務連絡）も発出されている。（以下、**Q&A**）

PMDA 医療機器のサイバーセキュリティについて https://www.pmda.go.jp/review-services/drug-reviews/about-reviews/devices/0051.html
解説資料及びセミナー動画 「医療機器のサイバーセキュリティ要件に対するJIS T 81001-5-1の適用について」参照

医療機器の基本要件基準第12 条第3項の適合性の確認について

薬生機審発0523 第1号
令和5 年5 月23 日

箇条	1. JISに関連する要求事項	2. JISに関連する既存通知等の要求事項
4 （一般要求事項）	サイバーセキュリティの確保に係る活動は、品質マネジメントシステムに基づいて行われていること。	
	規制当局及び顧客に対して脆弱性を適時に通知する活動を確立すること。	品質マネジメントシステムにおいて、セキュリティに対する対応方針、セキュリティに対する問い合わせ窓口を明確化し、顧客に対する脆弱性等の開示手順が定められていることによって確認すること。
	医療機器のリスクマネジメントは、セキュリティの脆弱性、脅威等を考慮したものであること。	
5 （開発プロセス）	開発計画において、セキュリティ更新や開発環境等のセキュリティについて考慮すること。	
	製品のセキュリティ機能を含むセキュリティ要求事項を特定すること。	
	意図する使用環境、信頼境界、多層防御等を考慮してアーキテクチャー設計を行うこと。	意図する使用環境をシステム構成図やネットワーク構成図等を用いて明示することで確認すること。
	セキュリティ設計のベストプラクティスを考慮した設計及び実装を行うこと。	
	ソフトウェアシステム試験を行って、セキュリティ要求事項が満たされ、リスクマネジメントプロセスで特定した脅威に対応する方法が設計に実装され、有効であることを確認すること。	
6 （保守プロセス）	顧客に対するセキュリティ更新の通知方針について定めておくこと。	ソフトウェア保守計画において、サポート終了等の製品寿命に対して計画し、脆弱性の監視、セキュリティ更新等の将来的な脆弱性対策の実施計画をあらかじめ定めておき、その一環として顧客に対するセキュリティ更新の通知方法を明確化すること。
7 （リスクマネジメント）	医療機器のリスクマネジメントにおいて、医療機器の意図する使用及び使用環境を考慮して、関連する脆弱性を特定し、関連する脅威を推定して評価し、リスクコントロール手段によって脅威をコントロールし、その有効性を監視すること。	
8 （構成管理）	医療機器の開発、保守及びサポートのための、変更管理及び変更履歴を伴う構成管理プロセスを確立すること。	構成管理プロセスは、当該医療機器のソフトウェア部品表（SBOM）を適切に作成することによって確認すること。
9 （問題解決）	セキュリティの脆弱性に関する情報伝達及び処理の手順を定め、セキュリティ問題に対して、情報開示を含めて手順に従って実施すること。	

医療機器の基本要件基準第12 条第3項の適合性の確認について

薬生機審発0523 第1号
令和5 年5 月23 日

箇条	1. JISに関連する要求事項	2. JISに関連する既存通知等の要求事項
4 （一般要求事項）	サイバーセキュリティの確保に係る活動は、品質マネジメントシステムに基づいて行われていること。	
	規制当局及び顧客に対して脆弱性を適時に通知する活動を確立すること。	品質マネジメントシステムにおいて、セキュリティに対する対応方針、セキュリティに対する問い合わせ窓口を明確化し、顧客に対する脆弱性等の開示手順が定められていることによって確認すること。
	医療機器のリスクマネジメントは、セキュリティの脆弱性、脅威等を考慮したものであること。	
5 （開発プロセス）	開発計画において、セキュリティ更新や開発環境等のセキュリティについて考慮すること。	
	製品のセキュリティ機能を含むセキュリティ要求事項を特定すること。	
	意図する使用環境、信頼境界、多層防御等を考慮してアーキテクチャー設計を行うこと。	意図する使用環境をシステム構成図やネットワーク構成図等を用いて明示することで確認すること。
	セキュリティ設計のベストプラクティスを考慮した設計及び実装を行うこと。	
	ソフトウェアシステム試験を行って、セキュリティ要求事項が満たされ、リスクマネジメントプロセスで特定した脅威に対応する方法が設計に実装され、有効であることを確認すること。	
6 （保守プロセス）	顧客に対するセキュリティ更新の通知方針について定めておくこと。	ソフトウェア保守計画において、サポート終了等の製品寿命に対して計画し、脆弱性の監視、セキュリティ更新等の将来的な脆弱性対策の実施計画をあらかじめ定めておき、その一環として顧客に対するセキュリティ更新の通知方法を明確化すること。
7 （リスクマネジメント）	医療機器のリスクマネジメントにおいて、医療機器の意図する使用及び使用環境を考慮して、関連する脆弱性を特定し、関連する脅威を推定して評価し、リスクコントロール手段によって脅威をコントロールし、その有効性を監視すること。	
8 （構成管理）	医療機器の開発、保守及びサポートのための、変更管理及び変更履歴を伴う構成管理プロセスを確立すること。	構成管理プロセスは、当該医療機器のソフトウェア部品表（SBOM）を適切に作成することによって確認すること。
9 （問題解決）	セキュリティの脆弱性に関する情報伝達及び処理の手順を定め、セキュリティ問題に対して、情報開示を含めて手順に従って実施すること。	不具合等報告（2024/1/15）、脆弱性の管理等（2024/3//28）、一部変更に伴う軽微変更手続き等の取扱い（2024/4/23）

販売、製造等の禁止

厚労省医療機器審査管理課資料引用

■ 基本要件基準に適合しない医療機器は、販売、製造等を禁止。

（販売、製造等の禁止）
第65条　次の各号のいずれかに該当する医療機器は、販売し、貸与し、授与し、若しくは販売、貸与若しくは授与の目的で製造し、輸入し、貯蔵し、若しくは陳列し、又は医療機器プログラムにあつては電気通信回線を通じて提供してはならない。
一　第41条第3項の規定によりその基準が定められた医療機器であつて、その性状、品質又は性能がその基準に適合しないもの

基本要件基準

二　第23条の2の5若しくは第23条の2の17の厚生労働大臣の承認を受けた医療機器又は第23条の2の23の認証を受けた医療機器であつて、その性状、品質又は性能がその承認又は認証の内容と異なるもの（第23条の2の5第16項（第23条の2の17第5項において準用する場合を含む。）又は第23条の2の23第8項の規定に違反していないものを除く。）
三　第42条第2項の規定によりその基準が定められた医療機器であつて、その基準に適合しないもの
四　その全部又は一部が不潔な物質又は変質若しくは変敗した物質から成つている医療機器
五　異物が混入し、又は付着している医療機器
六　病原微生物その他疾病の原因となるものにより汚染され、又は汚染されているおそれがある医療機器
七　その使用によつて保健衛生上の危険を生ずるおそれがある医療機器

厚生労働省　医療機器におけるサイバーセキュリティに関する通知、資料等

- 医療機器におけるサイバーセキュリティについて
  https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/0000179749_00009.html
  https://www.pmda.go.jp/review-services/drug-reviews/about-reviews/devices/0051.html

JIS T 2304のソフトウェアライフサイクルプロセス

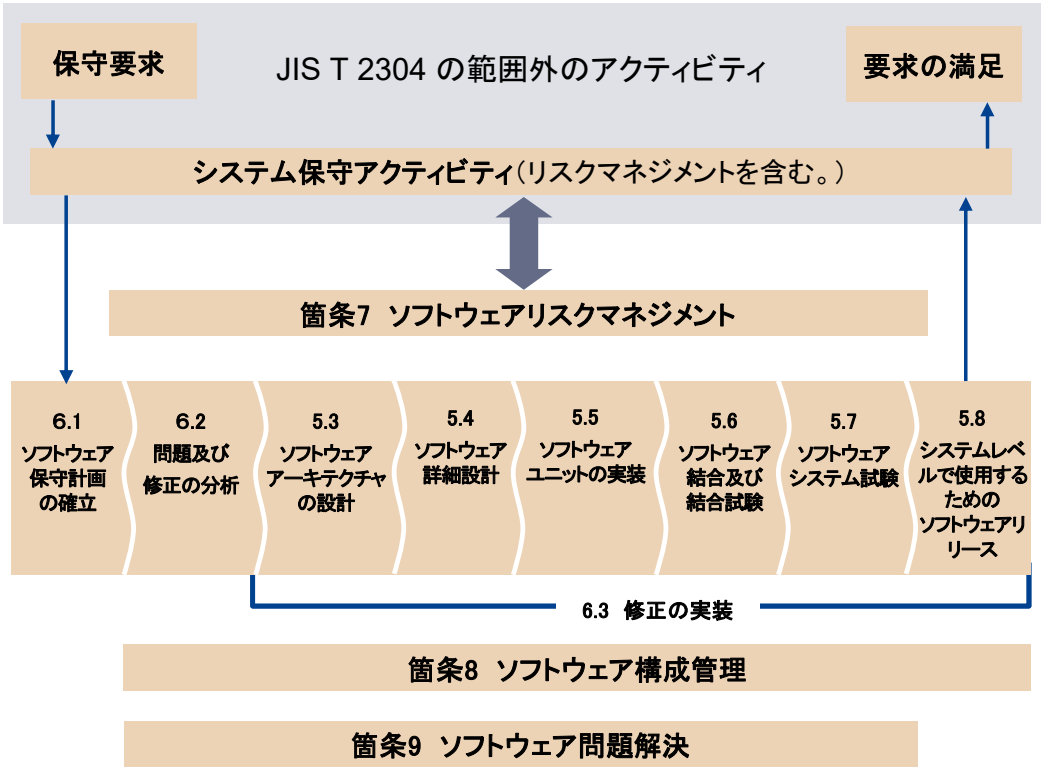
PMDA資料引用

安全なソフトウェアを実現するためには、試験を実施するだけではなく、次が必要

- ハザードを特定し、関連するリスクが受容可能なレベルにまで低減されている。（リスクマネジメント）
- 適切なプロセスを規定し、それが効果的に実施されている。（ライフサイクルプロセス）

基本要件基準第12条第2項への適合は、JIS T 2304への適合によって確認する。基本要件基準第12条第3項への適合は、JIS T 2304のライフサイクル要求事項の構成でセキュリティ対応を規定するJIS T 81001-5-1への適合によって確認する。

JIS T 2304:2017 図1－ソフトウェア開発プロセス及びアクティビティの関連図より



JIS T 2304:2017 図2－ソフトウェア保守プロセス及びアクティビティの関連図より

規格の構成

PMDA資料引用

ヘルスソフトウェアのサイバーセキュリティを強化するために、ライフサイクルにおいて実行するアクティビティを**JIS T 2304の順序で記載**している

	JIS T 2304
4	一般要求事項
5	ソフトウェア開発プロセス
6	ソフトウェア保守プロセス
7	ソフトウェアリスクマネジメントプロセス
8	ソフトウェア構成管理プロセス
9	ソフトウェア問題解決プロセス

	JIS T 81001-5-1
4	一般要求事項
5	ソフトウェア開発プロセス
6	ソフトウェア保守プロセス
7	セキュリティに関連するリスクマネジメントプロセス
8	ソフトウェア構成管理プロセス
9	ソフトウェア問題解決プロセス

製造業者が品質マネジメントシステム及びリスクマネジメントシステムの下で，ヘルスソフトウェアを開発し保守することを規定

製造業者が実施するソフトウェアライフサイクルプロセスの一部として，アクティビティ及びその結果のアウトプットを規定

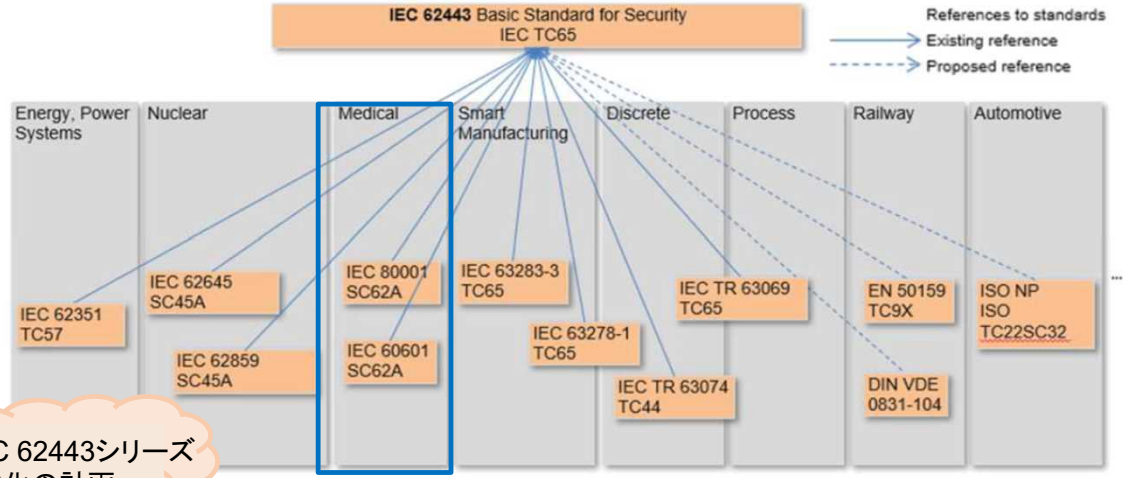
製造業者が実施する問題解決プロセスの一部として，アクティビティ及びその結果のアウトプットを規定

医療機器の場合は、ソフトウェアライフサイクルプロセスやリスクマネジメントプロセスが求められていて、各製造業者においてすでに実装されていると考えられるので、この規格では、セキュリティライフサイクルプロセスそのものを別途規定するのではなく、既存のプロセスの枠組みに追加するアクティビティを規定している。

IEC 81001-5-1（JIS T 81001-5-1）:
PMDA 医療機器のサイバーセキュリティについて https://www.pmda.go.jp/review-services/drug-reviews/about-reviews/devices/0051.html
解説資料及びセミナー動画 「サイバーセキュリティに係る規格について（IEC 81001-5-1:2021）」 参照

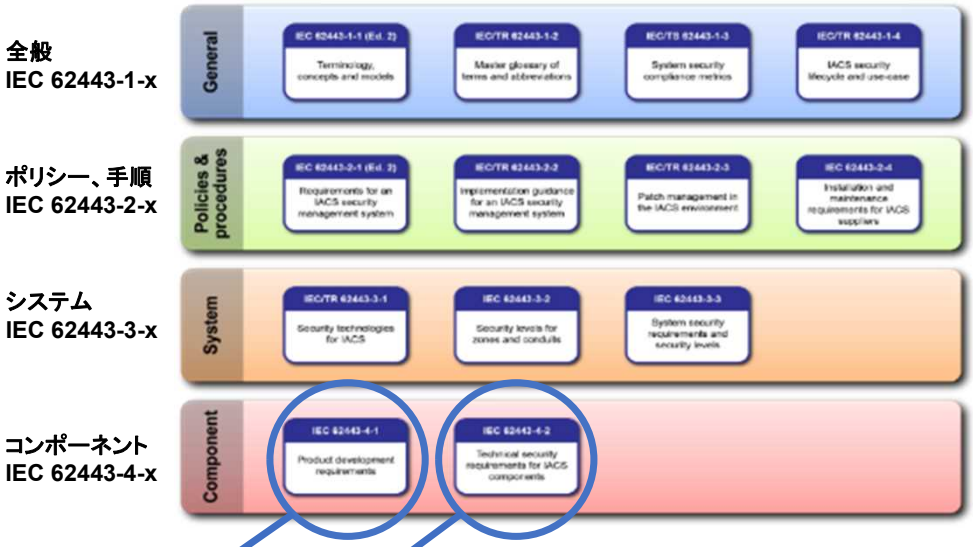
IEC 62443-4-1 と IEC 81001-5-1 との関係

水平規格（horizontal standard）にするための役割を担う委員会
IEC 62443 シリーズを 水平規格にするための 調整役を担う委員会を TC65 に割り当て、作業を開始した。
既にCAB(Conformity Assessment Board)からSMB(Standardization Management Board)に、この規格を Base Standardsとして扱うよう勧告がでている。



他領域からの参照状況[1]

IEC 62443シリーズ
JIS化の計画



（ACSEC 古原分科会長 2020年11月20日 Web 会議出席報告書　成果及び所感 より引用）

IEC TC62（医用電気機器）では、2つの文書で参照している。
- IEC 81001-5-1（IS）:　　製品ライフサイクルにおけるアクティビティ
- IEC TR 60601-4-5（TR）:　　医療機器の安全に関する技術的セキュリティ仕様

OT(Operational Technologies)の定義

"Hardware and software that detects or causes a change through the direct monitoring and/or control of real-world assets and processes."

JIS T 81001-5-1 リスクマネジメントプロセスと他のプロセスとの関連

PMDA資料引用

箇条4　一般要求事項
- 4.2　セキュリティに関連するリスクマネジメント
- 4.3　リスク移転に関連するソフトウェアアイテムの分類

詳細を箇条7に規定

リスクマネジメントプロセスは、脅威モデリングの手法を用いて行い、
その結果を文書化した脅威モデルは、開発プロセスや問題解決プロセスで
参照して、対処する

箇条5　ソフトウェア開発プロセス
- 5.3　ソフトウェアアーキテクチャー設計
- 5.4　ソフトウェア設計
- 5.7　ソフトウェアシステム試験

特定した脅威に対応する方法を設計に含めて、
システム試験で有効性を確認する

セキュリティコンテキストは、
製品レベルの意図する使用環境
から導き出し、設計に反映する

多層防御を考慮し、
信頼境界を文書化

脅威モデル：
脅威モデリングのアクティビティを文書化した結果

脅威モデル

特定したすべての問題を対処する

箇条7　セキュリティに関連するリスクマネジメントプロセス
- 7.1　リスクマネジメントのコンテキスト
- 7.2　ぜい(脆)弱性、脅威及び関連する悪影響の特定
- 7.3　セキュリティに関連するリスクの推定及び評価
- 7.4　セキュリティに関連するリスクのコントロール
- 7.5　リスクコントロールの有効性の監視

脅威モデリング

箇条9　ソフトウェア問題解決プロセス
- 9.4　ぜい(脆)弱性の分析
- 9.5　セキュリティ関連の問題への対応

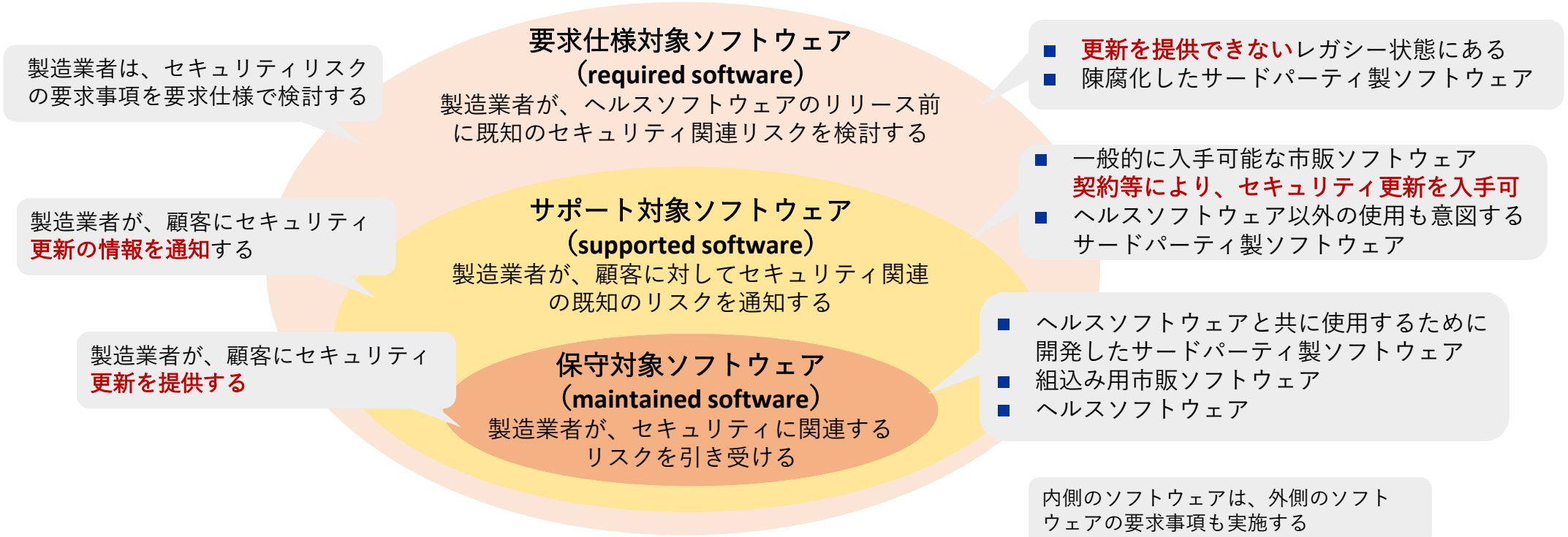
医療機器のリスクマネジメントにおいて、医療機器の意図する使用及び使用環境を考慮して、関連する脆弱性を特定し、関連する脅威を推定して評価し、リスクコントロール手段によって脅威をコントロールし、その有効性を監視すること。(適合性確認通知の1.の(4))

セキュリティの脆弱性に関する情報伝達及び処理の手順を定め、セキュリティ問題に対して、情報開示を含めて手順に従って実施すること。(適合性確認通知の1.の(6))

4.3 リスク移転に関連するソフトウェアアイテムの分類

- ソフトウェアアイテムの分類（保守対象ソフトウェア、サポート対象ソフトウェア、要求仕様対象ソフトウェアのうち、どれか）を文書化する。
- 分類は、リスク移転の観点から整理されている。
  - JIS Q 13485の7.4（購買）の一部として実施可能。

サイバーセキュリティのリスク評価に必要なソフトウェア部品の分類の基礎
IEC 81001-5-1 ISH（解説書：Interpretation SHeet）



Ministry of Health, Labour and Welfare of Japan

5. 医療機器サイバーセキュリティ対応のフレームワーク

IMDRF（International Medical Device Regulators Forum）の動向

- 医療機器のサイバーセキュリティに関して、2019年1月にWGキックオフ → 2020年4月公開
  - 医療機器サイバーセキュリティの原則及び実践：Principles and Practices for Medical Device Cybersecurity
    原文：http://imdrf.org/docs/imdrf/final/technical/imdrf-tech-200318-pp-mdc-n60.pdf
    邦訳：https://dmd.nihs.go.jp/cybersecurity/IMDRF_Guidance_Japanese_version.pdf
    - 医療機器規制当局としての対応指針（ハイレベルで包括的な国家ルール）

一般原則
① 国際調和
② 製品ライフサイクル
③ 共同責任
④ 情報共有
⇒ 市販前の考慮事項 ⇒ 市販後の考慮事項

- SBOM及びレガシー医療機器に関するNWIE(Extension)についてガイダンス追補の策定のため、2021年2月にWG作業を再開 → 2023年4月公開
  - レガシー医療機器：Principles and Practices for the Cybersecurity of Legacy Medical Devices
    https://www.imdrf.org/documents/principles-and-practices-cybersecurity-legacy-medical-devices
  - ソフトウェア部品表（SBOM）：Principles and Practices for the Software Bill of Materials for Medical Devices
    https://www.imdrf.org/documents/principles-and-practices-software-bill-materials-medical-device-cybersecurity

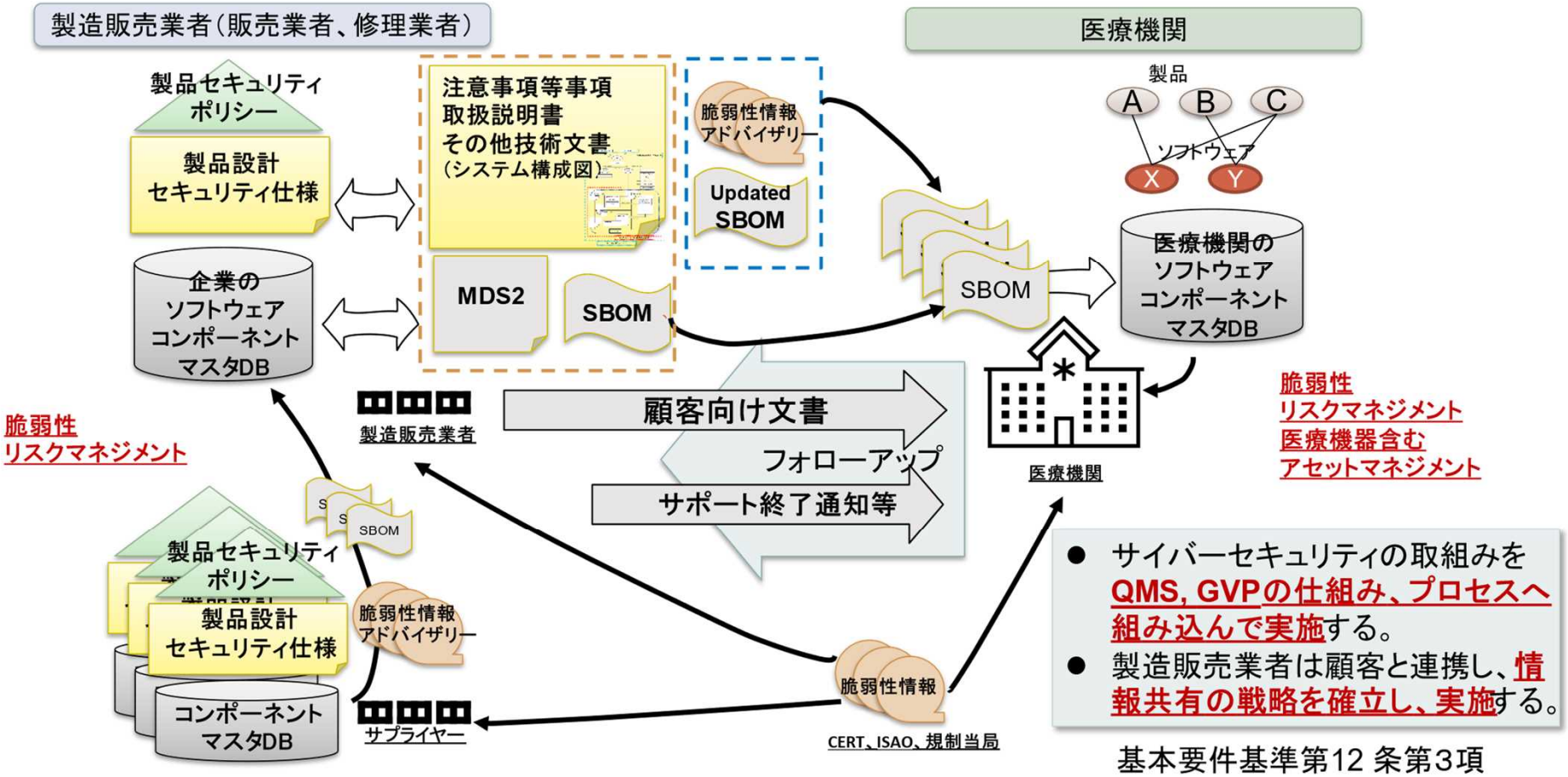
「国際医療機器規制当局フォーラム(IMDRF)による医療機器サイバーセキュリティの原則及び実践に関するガイダンスの公表について（周知依頼）」
（令和2年5月13日、薬生機審発0513第1号・薬生安発0513第1号）
2020年 ※IMDRFガイダンス

「医療機器のサイバーセキュリティ導入に関する手引書」
・初版：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
・改訂：令和5年 3月31日、薬生機審発0331第11号 薬生安発 0331第4号
2023年改訂 にて通知された

国内導入へ 2023年

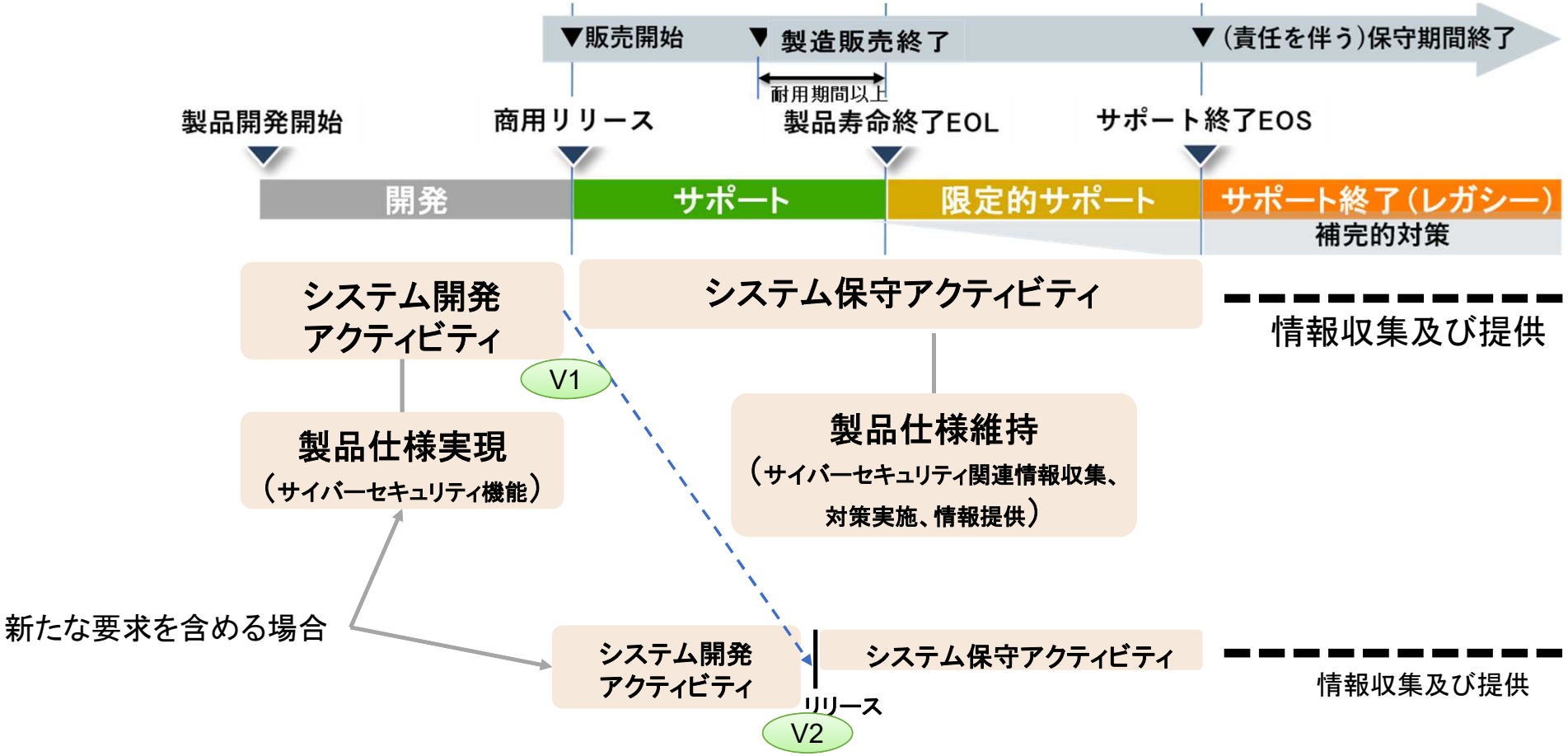
IMDRFガイダンス 一般原則、国際規格（IEC 81001-5-1）一般要求事項

- 製造販売業者が品質マネジメントシステム及びリスクマネジメントシステムの下でヘルスソフトウェアを開発し保守すること、セキュリティに関連して必要な要件の実施が規定されている。



基本要件基準第12 条第3項

製品のライフサイクル（EOL、EOS）



製造販売業者と医療機関との連携（概要）例

製造販売業者		製造販売業者のアクティビティ	医療機関のアクティビティ	医療機関	
医療機器の開発，販売に向けた準備		○製品セキュリティポリシーの作成と開示 ○保守計画の作成 ○医療機関向け文書の作成・提示 ・注意事項等情報及び取扱説明書 ・セキュリティ関連文書（ネットワーク構成図，信頼境界，MDS2，SBOM，MDS，SDS等） ・製品保守計画及び契約案 ○必要なトレーニングの準備	●医療機器の使用環境の特定及びセキュリティ仕様の特定 ●医療機器の医療機関のセキュリティ管理体制への組込み及びネットワーク構成更新 ●必要なセキュリティ関連文書の整備 ●保守計画の確認及び契約等準備	医療情報システムの構築に向けた準備 ・セキュリティ、プライバシーポリシー確立 ・導入IoTの選定 ・導入医療機器の選定 ・責任境界・役割の調整	
医療機器の設置，運用開始		○使用環境（設置環境）に応じたセキュリティ文書（更新）等の提示 ○保守に関する範囲・役割・責任・連携等に関する契約条項の調整	●医療機器を含めた医療情報システムのセキュリティ状態の確認 ●保守に関する契約締結	システム・機器導入 システムバリデーション システム運用開始	
医療機器の運用	製品ライフサイクルにおける対応（レガシー医療機器に関する対応含む）	○製品寿命終了（EOL），サポート終了（EOS）の通知 ○製品保守計画に従った具体的な実施計画の提示 ○情報収集，セキュリティ関連文書の更新 ○脆弱性に関するセキュリティアドバイザリー情報開示，セキュリティ対策又は補完的対策を含む緩和策の提示 ○協調的な脆弱性開示（CVD）の対応として，調査又は関係部門へ注意喚起	●製品ライフサイクルの理解及びEOS後の対応計画 ●保守実施計画の理解と実施の調整 ●医療機器の使用環境におけるセキュリティ情報収集 ●セキュリティ関連文書の更新確認 ●医療機器の脆弱性対策実施 ●医療機関内の情報共有 ●レガシー医療機器への対策 ●協調的な脆弱性の開示（CVD）の対応	システムの維持・更新	医療情報システムの運用
	インシデント発生時の対応	○医療機関との連携活動 ○規制当局等への報告，情報提供 ○医療機器等の回復・復帰のための措置及び支援	●インシデント状況の把握及び対応実施 ●関係方面への報告，広報 ●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	インシデント発生時の対応	

医療機器のサイバーセキュリティに関する 質疑応答集（Q＆A） 第2弾（2024/1/31）

■ 市販後のサイバーセキュリティの確保について

Q	A
Q11 **市販後のサイバーセキュリティの確保は、製造販売後安全管理において実施する**ことで良いか。	A11 貴見のとおり。製造販売業者は医薬品、医薬部外品、化粧品、医療機器及び再生医療等製品の製造販売後安全管理の基準に関する省令（平成16年厚生労働省令第135号）に則り製造販売後安全管理を行う必要がある。当該省令第七条から九条に規定されるとおり、**サイバーセキュリティを確保するために必要な情報を収集し、遅滞なく検討した結果、必要があると認める時は、安全確保措置（医療関係者への情報提供、脆弱性対策（市販後のアップデート等を含む）等）を実施する必要**がある。 なお、安全管理情報の収集にあたっては、安全管理責任者は国内品質業務運営責任者等、その他の製造販売後安全管理に関係する部門の責任者と密接な連携を図り、国内品質業務運営責任者等が入手した情報のうち、**品質に関する情報については引き続きQMS省令に基づき国内品質業務運営責任者等が必要な検討・措置を行う**こと。

市販後におけるリスクマネジメント

i. 顧客苦情の収集、文書化及び対応（附帯サービスを含む）

ii. 規制当局が要求する有害事象・事故の報告（例えば、機器の不具合により、死亡、重傷に至った事象又は再発した場合に死亡、重傷に至る可能性のある事象）

iii. 必要な場合、市場安全是正処置の実施（例えば、リコール、修正、IFUの変更等）
場合によっては（例えば、ライフサイクルの段階によっては）、製造販売業者は正式な処置を行わず、単に情報共有を行うだけかもしれない。

iv. 脆弱性マネジメントを含むプロアクティブなリスクマネジメントへの取組（例えば、ツール、リソース、人員を使用して、機器のセキュリティ及び安全に関連するリスクに影響を与えるセキュリティ問題を継続的に監視、対処及び情報共有）

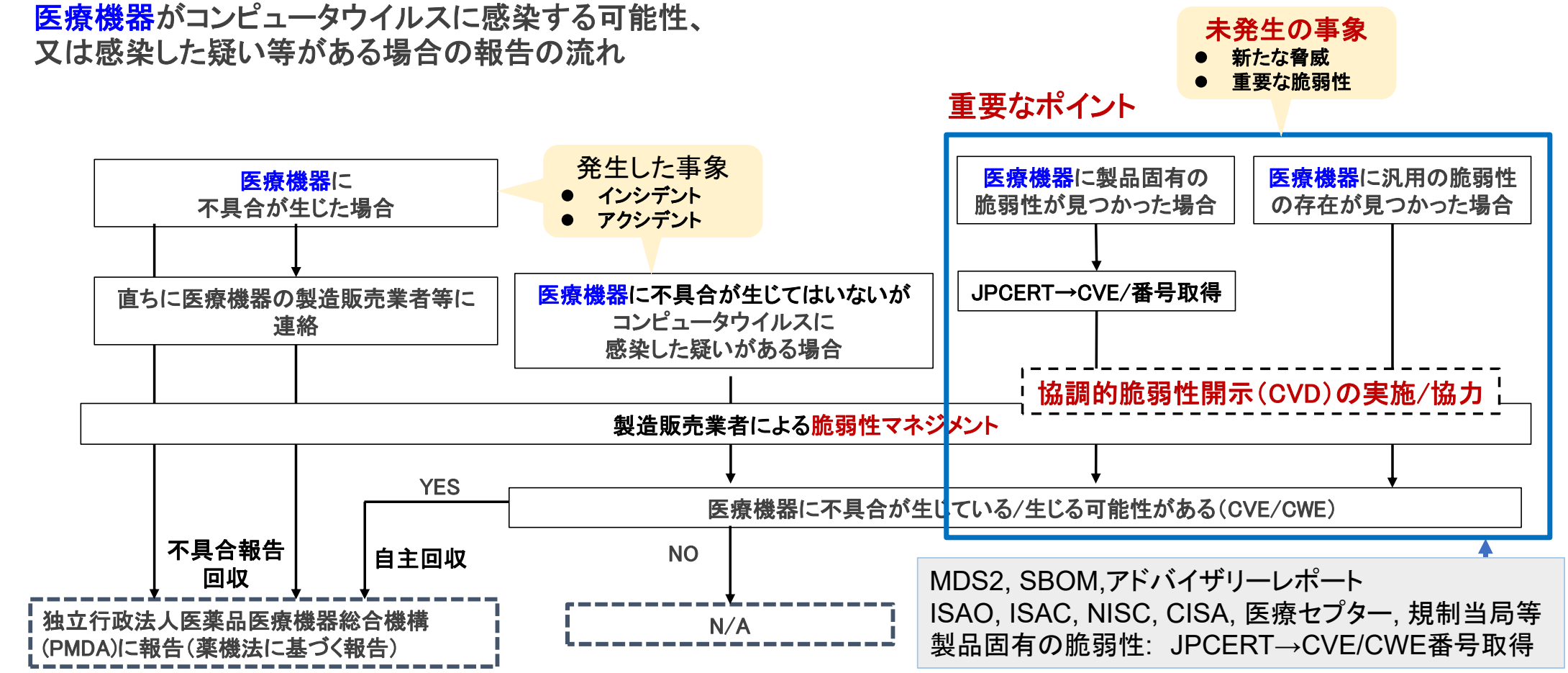
v. 脆弱性マネジメントを含むリアクティブなリスクマネジメントへの取組（例えば、必要に応じて集められたツール、リソース及び人員を使用して、重要なセキュリティ及び安全に関連するリスクに対処し、情報共有）

GVPプロセスに導入

詳細 JIS T 81001-5-1参照

医療機器のサイバーセキュリティに関する脆弱性マネジメント　―　製造販売業者の視点

医療機器がコンピュータウイルスに感染する可能性、
又は感染した疑い等がある場合の報告の流れ



医療機器サイバーセキュリティに関する不具合等報告の基本的考え方について（医薬安発0115第2号）

医療機器のサイバーセキュリティを確保するための脆弱性の管理等について（医薬機発0328第1号、医薬案発0328第3号）

（参考） PSIRT（製販業者における製品セキュリティインシデント対応チーム）の設置

◆ 組織が開発・販売する製品等の脆弱性リスクの特定、評価、対処を行う組織内のエンティティ

Product Security Incident Response Team (PSIRT) Maturity Document　日本語版　2022/7

https://www.nca.gr.jp/activity/pub_doc/first_psirt_maturity_document.html

- FIRSTの製品セキュリティコミュニティによってまとめられた「製品セキュリティインシデント対応チーム（PSIRT）成熟度ドキュメント運用能力と成熟度レベル」の日本語訳が公開されています。
  FIRST (Forum of Incident Response and Security Teams)： http://www.first.org/
- 本書ではProduct Security Incident Response Team (PSIRT)が成熟度レベル毎に選択する一連のユースケースとサービスの概要を紹介しています。
- 日本語訳は日本シーサート協議会と Software ISAC によって翻訳された後、JPCERT/CC とPanasonic PSIRT とTOSHIBA-SIRTによってレビューされています。

図：自組織の関連部門

PSIRT = 構え

この部門の協力がなければ
情報共有が進まない

図 3：成熟度レベル 3 の望ましいサービスレベルとサービスの一覧

医療機器サイバーセキュリティに関する不具合等報告の基本的考え方について

（医薬安発0115第2号）

医薬安発0115 第２号
令和６年１月15 日

各都道府県衛生主管部（局）長 殿

厚生労働省医薬局医薬安全対策課長
（ 公印省略）

医療機器サイバーセキュリティに関する不具合等報告の基本的考え方について

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、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並びにサイバーセキュリティ対策及び処置の考え方については、「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）として取りまとめられており、製造販売業者は、サイバーリスクに伴う医療機器の不具合等を「医薬品、医薬部外品、化粧品、医療機器及び再生医療等製品の製造販売後安全管理の基準に関する省令」（平成16 年厚生労働省令第135 号）における安全管理情報として取り扱い、適切な製造販売後安全管理を行う必要があることを示しています。

製造販売業者等が行う不具合等の報告については、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35 年法律第145 号）第68 条の10 第1 項により規定され、その取扱いは「「医薬品等の副作用等の報告について」の一部改正について」（令和３年７月30 日付け薬生発0730 第８号厚生労働省医薬・生活衛生局長通知）により示しているところです。

今般、医療機器に対するサイバーセキュリティの確保を一層強化するため、製造販売業者等が行う不具合等の報告について、「新たな形態の医療機器等をより安全かつ有効に使用するための市販後安全対策のあり方に関する研究」（厚生労働行政推進調査事業費補助金（医薬品・医療機器等レギュラトリーサイエンス政策研究事業）、研究代表者 国立医薬品食品衛生研究所 医療機器部 サイバーセキュリティワーキンググループにおいて、別添のとおり「医療機器サイバーセキュリティに関する不具合等報告の基本的考え方」が取りまとめられましたので、御了知の上、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の製造販売後安全管理が円滑に行えるよう、貴管下関係製造販売業者等への周知及び指導等よろしくお願いいたします。

医療機器サイバーセキュリティに関する不具合等報告の基本的考え方　別添

1. はじめに
2. 本文書の対象
3. 用語の解説
4. 製造販売業者における医療機器の不具合等報告
   (1) 医療機器の不具合等報告の基本的事項
   不具合等報告書は、報告期限内に、PMDA医療機器品質管理・安全対策部 医療機器安全対策課に提出する。
   (2) サイバーセキュリティに関する不具合等報告
   レガシー医療機器において発生した事象についても、同様に不具合等報告の必要性を考慮すること。
   (3) 脆弱性に関する対応
   当該脆弱性の悪用が原因で、死亡や重篤な健康被害が発生した場合、又は発生するおそれがあると判断した場合には、報告の要否や区分を評価、判断し、医薬品医療機器等法第68条の10第1項の規定により規制当局への不具合等の報告を実施する。
   (4) レガシー医療機器に関する対応
   EOS 後の継続した使用に関しては、決して推奨できる状態ではないとともに、継続して使用する責任は医療機関にあることは、全ての関係者が理解しておかねばならず、そのために製造販売業者は、積極的な情報提供を行い、顧客との連携、医療機関と認識を共有することが重要である。
5. 情報共有体制について
   製造販売業者は、医療機器のCS に関する不具合や健康被害が発生した場合には、当該医療機器の影響等を評価し、不具合等報告の要否について判断し、必要に応じてPMDA に報告する。その際に、製造販売業者は、医療機関、使用者、規制当局及び脆弱性発見者等と必要な情報共有等を行い、連携したアプローチを実施することが求められる。そのために製造販売業者は、脆弱性に関する情報の収集、評価、報告に関する情報共有体制の構築、維持が必要であり、併せて継続的な人材育成が望まれる。
6. まとめと今後の展望
   今後は、医療機器のCS に関する情報を入手した際に、関係者間で情報共有等を行い、連携して対処するための具体的な手順の確立が望まれる。

医療機器のサイバーセキュリティを確保するための脆弱性の管理等について

（医薬機発0328第１号、医薬安発0328第３号）

医薬機審発0328第１号
医薬安発0328第３号
令和６年３月28日

各都道府県衛生主管部（局）長 殿

厚生労働省医薬局医療機器審査管理課長
（公印省略）
厚生労働省医薬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における、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た「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。）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、情報提供しています。

さらに、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、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、「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」（令和５年３月31日付け薬生機審発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・医薬安全対策課長連名通知）により、お示ししたところです。

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号の改正を行い、許認可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進めています。

今般、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、脆弱性の管理等に関する留意事項を下記のとおりまとめたので、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。

情報セキュリティ早期警戒パートナーシップガイドライン 2019 年版第2刷
「5. 製品開発者の対応」
https://www.ipa.go.jp/security/guide/vuln/partnership_guide.html

医療機器のサイバーセキュリティを確保するための脆弱性の管理等について

（医薬機発0328第１号、医薬安発0328第３号）

- 脆弱性の管理

  脆弱性は、システムのセキュリティポリシーを破るために悪用される可能性のある、システムの設計、導入又は運用管理における欠陥又は弱みであることから（JIS T 81001-1:2022 3.4.22）、医療機器のサイバーセキュリティを確保するため、**医療機器製造販売業者等は、当該医療機器の脆弱性について、特定、評価、開示、修正等を行う必要**ある。

- **医療機器に製品固有の脆弱性が見つかった場合**
- **医療機器に汎用の脆弱性の存在及び悪用により受容できないリスクが発生する可能性がある場合**

＜IPA＞
以下ウェブサイトを参照の上、脆弱性関連情報を届出すること。
参考：https://www.ipa.go.jp/security/todokede/vuln/uketsuke.html
なお、IPAは脆弱性関連情報の届出の受付機関であり、医療機器製造販売業者等への連絡及び公表に係る調整はJPCERT/CCにて実施される。

脆弱性情報の届出と対応について

経済産業省告示に基づき運用されている「情報セキュリティ早期警戒 パートナーシップガイドライン」（2022年5月）

- 自らが**発見者**の場合
  脆弱性関連情報の**届出の受付機関**： 独立行政法人情報処理推進機構（IPA）
  https://www.ipa.go.jp/security/todokede/vuln/uketsuke.html
- 脆弱性関連情報に関して**製品開発者への連絡および公表に係る調整機関**
  一般社団法人JPCERTコーディネーションセンター（JPCERT/CC）

製品開発者登録
https://www.jpcert.or.jp/vh/register.html

必要な社内プロセス例

① 最上位のCVDに基づく調査対応

国際的にも一般的で極めて緊急性の高い脆弱性（例えばBluetoothに関する脆弱性）が発見された場合、CISA等の調整機関に報告され、一般公開する前に、世界各地のCERTをとおして事前確認・対応が確認されて後、公開される。
日本の場合、内閣サイバーセキュリティセンター（NISC）経由で省庁→工業会→企業、又はJP-CERT/CC経由で各分野団体に伝えられ、確認作業が必要な場合は、情報収集を伴う場合もある。医療機器の場合、厚労省機器課・安対課から届いた調査・確認であれば、社内において、全ての稼働製品及び設計開発中の製品について調査し、影響の有無等を回答し、対策が必要ならば即座に計画することになる。

② 製販業自らが自社製品（サードパーティ製ソフトウェア部品含む）に新たな脆弱性を発見した場合

自社内の影響を即座に調査し、他機器にも影響するような汎用性の高い脆弱性であった場合は、IPAに脆弱性報告し、自身で一般公開及び開示しないようにする。顧客に対してもIPAの許可を得てから開示する。ここから先のCVD手順はJPCERT/CCが管理する。リスクの低い脆弱性であれば、単純な脆弱性報告で完了する。

③ 社外の発見者からの脆弱性報告の窓口設置及びプロセス確立

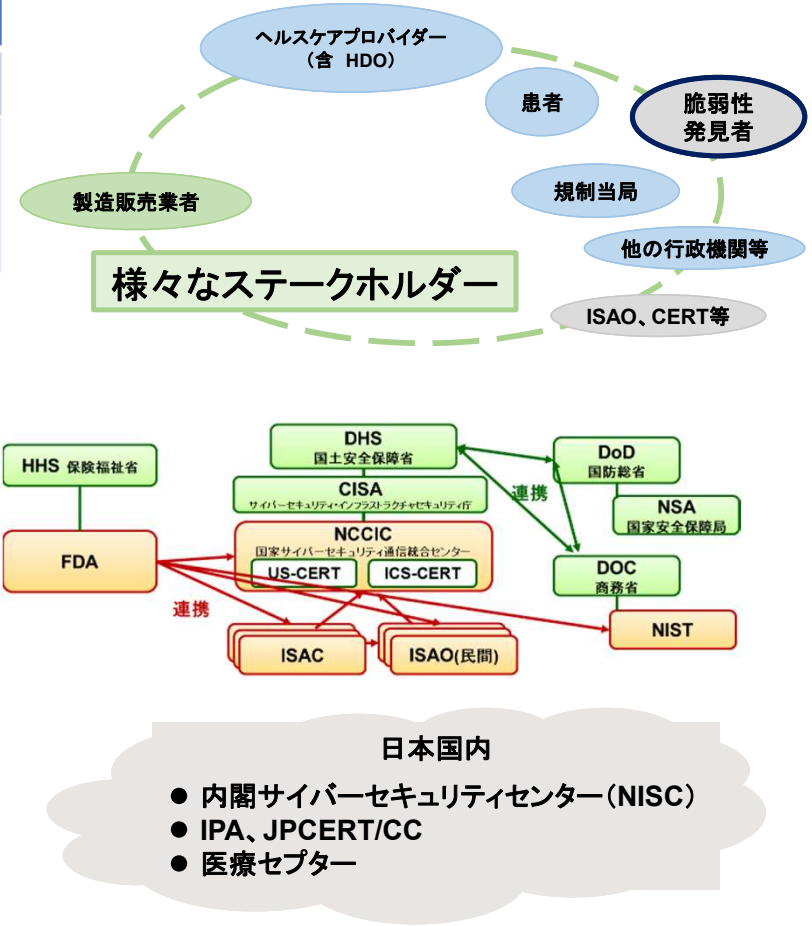
報告された脆弱性のリスクを判定し、製品に関連する新たな脆弱性であった場合は、発見者にCVDプロセスを開始することを伝え、脆弱性の公開・開示を控えてもらい、社内CVDプロセス上記②へ移行する。一連の処理が終わった後、必ず発見者に連絡する。
製品に関連する既知の脆弱性（対応済み）、又は製品に関係しない（影響しない）脆弱性であった場合は、発見者と、IPAへの報告等について協議する等々。（ここは自由）

ぜい(脆)弱性についての通知の受領 （JIS T 81001-5-1 箇条9.2）

9.2	ぜい(脆)弱性についての通知の受領
	ぜい(脆)弱性に関する情報を製造業者へ報告可能にする （サプライチェーン）
	ヘルスソフトウェアのセキュリティ関連の問題についてのレポートを入手し，問題解決まで追跡可能な情報源を、社内外又は苦情処理システム等から定め、情報が入手可能な仕組みを構築する

a) セキュリティの検証及びバリデーションの試験担当者
b) 製品で使用するサードパーティ製コンポーネントの供給者
c) 製品の開発担当者及び試験担当者
d) インテグレーター、操作者、管理者及び保守要員を含む製品のユーザー
e) 監査イベントログ情報から得られたデータ
f) セキュリティの研究者[セキュリティのぜい(脆)弱性報告者]
ISO/IEC 29147 (情報技術— セキュリティ技術 — 脆弱性開示)も参照
g) ヘルスソフトウェアに影響する可能性がある広範囲のぜい(脆)弱性についてのデータ又は通知

9.1 概要 | 9.2 ぜい(脆)弱性，脅威及び関連する悪影響の特定 | 9.3 ぜい(脆)弱性のレビュー | 9.4 ぜい(脆)弱性の分析 | 9.5 セキュリティ関連の問題への対応



情報共有の仕組み

医療機器のサイバーセキュリティ対策に関連する一部変更に伴う軽微変更手続き等の取扱いについて

（医薬機審発0423第１号）

医薬機審発０４２３第１号
令和６年４月２３日

各都道府県衛生主管部（局）長 殿

厚生労働省医薬局医療機器審査管理課長
（公印省略）

「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41条第３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」（令和５年厚生労働省告示第67号）による改正後の「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41条第３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。以下「基本要件基準」という。）第12条第３項については、「医療機器の基本要件基準第12条第３項の適用について」（令和５年３月31日付け薬生機審発0331第８号）等により示しているところです。

今般、医療機器のサイバーセキュリティ対策に関連する一部変更に伴う軽微変更手続き等の取扱いについて別添のとおりとりまとめましたので、御了知の上、貴管内の製造販売業者において内容につき浸透が図られるよう、周知方御配慮願います。

ここで示すのは、製品の有効性及び安全性に関わる機能に影響しない場合に限るものであり、例えば、ペースメーカや植込み型除細動器等で医療機関側が遠隔モニタリングを行う目的でネットワークに接続している医療機器は、ネットワークへの接続の可否が当該医療機器の有効性及び安全性の根幹に関わるため、本事例の対象外となる。

また、本来の使用方法ができなくなる変更も本事例の対象外であることに留意すること。

医療機器全体に関する一部変更に伴う軽微変更手続き等については、「医療機器の製造販売承認申請の作成に際し留意すべき事項について」（平成26年11月20日付け薬食機参発1120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）通知）、「医療機器の一部変更に伴う手続について」（平成20年10月23日付け薬食機発第1023001号厚生労働省医薬食品局審査管理課医療機器審査管理室長通知）及び「医療機器の一部変更に伴う軽微変更手続き等の取扱いについて」（平成29年7月31日付け薬生機審発0731第5号厚生労働省医薬・生活衛生局医療機器審査管理課長通知）に示した取扱い等を参考とすること。

なお、以下は事例を示すものであり、軽微変更届の対象となる事例並びに承認(認証)事項一部変更承認(認証)申請(以下「一変申請」という。)及び軽微変更届のいずれも必要でない事例はこれらに限るものではない。

個別の事例における取扱いについては、必要に応じ、独立行政法人医薬品医療機器総合機構又は登録認証機関に相談されたい。

医療機器のサイバーセキュリティ対策に関連する一部変更に伴う軽微変更手続き等の取扱いについて（別添）

1. 軽微変更届の対象となる事例

（変更等に伴う医療機器としての機能の追加・変更等がない場合に限り、軽微変更届の対象）

1. 使用方法欄における動作環境であるOS の種類やクラウド動作の追加・変更・削除

   以下①＆②の事例のうち、動作環境であるOS 等の種類の変更において、医療機器としての使用目的又は効果及びその性能に影響を与えない場合。

   ①汎用PCで動作する製品について、クラウド環境での動作を追加する場合

   （事例） 汎用PC（Windows 11）で動作する製品について、クラウド環境における動作も提供していることを追加。（なお、この場合は、クラウド環境で使用するための操作方法の変更も含む。）

   ②異なる種類の動作環境であるOS への変更・追加

   （事例） iOS 17 で動作する製品に対して、異なる種類のOS であるAndroid 13 を動作環境として追加。

2. 一変申請及び軽微変更届のいずれの手続きも要さない事例

（変更等に伴い医療機器としての機能の追加・変更等がない場合に限り、一変申請及び軽微変更届のいずれの手続きも必要ではない。次回の一変申請時には記載整備を要することに留意。）

1. 形状、構造及び原理欄又は使用方法欄の動作環境等に記載されたネットワークポート（物理的なインタフェースと論理的なIP ポートの双方を含む。）の削除

   （事例）ネットワーク接続できるハードウェア医療機器であり、ネットワークポートの説明が申請書に書かれている場合。（削除を行うことで製品の有効性及び安全性に関わる機能に影響する場合は含まない。）

2. 形状、構造及び原理欄又は使用方法欄における動作環境等におけるネットワーク接続の禁止又は接続要件の厳格化に対する変更又は追加

   （事例）ネットワークに接続できる医療機器(プログラム医療機器(以下SaMD という。)を含む。)に対して、SSL通信に限定することや接続相手を限定すること等の場合。

医療機器のサイバーセキュリティ対策に関連する一部変更に伴う軽微変更手続き等の取扱いについて（別添）

2. 一変申請及び軽微変更届のいずれの手続きも要さない事例

（変更等に伴い医療機器としての機能の追加・変更等がない場合に限り、一変申請及び軽微変更届のいずれの手続きも必要ではない。次回の一変申請時には記載整備を要することに留意。）

3. 形状、構造及び原理欄又は使用方法欄における動作環境等に対する、セキュリティ機能（認証、認可、暗号化、セキュリティイベント検出機能・通知、ログ、リモートソフトウェア更新等）又は補完的対策（ファイアウォール、マルウェア対策ソフト等）の変更又は追加

   （事例）ネットワークに接続できる医療機器(SaMD を含む。)に対し、セキュリティ機能・補完的対策のうち、使用方法の追加やアクセスレベルの強化等の製品安全性に関わらないものを実施する場合。（システム可用性・データ完全性等に関連し患者安全の確保に影響するものは含まない。）

   （事例）ネットワーク接続を必要としているが、補完的対策を追加又は変更しないとリスクをコントロールしきれない製品に補完的対策やセキュリティ機能を同梱する場合。

4. 使用方法欄における動作環境であるOS 等の変更・追加・削除（医療機器としての使用目的又は効果及びその性能に影響を与えない場合に限る。）

   ①動作環境であるOS バージョン等の追加・変更・削除

   （事例） Windows 10 での動作を指定している製品に対して、Windows 11 を追加する場合。

   （事例） OS 供給元のサービス終了に伴い動作環境のOS 指定からWindows 8 を削除する場合。

   セキュリティパッチ（回収の該当性の判断）

   ②動作環境として用いるデータベース等のバージョンの追加・変更

   （事例）MS SQL Server2019 までのバージョンを動作環境として指定している製品について、その後継バージョンを追加する場合。

   （事例）データベースの動作環境としてJava14 を指定していた製品にJava16 を追加又は変更する場合。

5. 使用方法欄における操作方法や注意事項の変更

   （事例）併用医療機器を特定させることにより、サポート終了（EOS）となった製品を使用不可としてリスク軽減を図る場合。

注意喚起：医療機器のサイバーセキュリティ対策の実施について

■ 医療機器のサイバーセキュリティ対策の実施について

「販売終了又はEOL後の医療機器に対するセキュリティパッチの適用について」

- 2019～2020年（サイバーセキュリティ対応WG活動初期の頃）には、
「薬機法の規則によって医療機器にはセキュリティパッチが適用できない」として、
ライフサイクルに関わらず、薬機法を理由に、医療機関のセキュリティに関する
問合せ、パッチ適用の依頼を拒否する業者が相当数いた。（問合せあり）

通知（医薬機審発0423第1号）に従い、
脆弱性の緊急性、重要性に応じて速やかに対応する。

医機連QA（2019年3月26日）を念頭におきつつ、事象により回収の該当性の判断が必要だが、
パッチ適用は回収通知に照らして判断しても、改修には該当しないケースもあると思われる。

Q4-2：医療機器（機械器具）において、サイバーセキュリティ対応として、OS 等のアップデートを行う行為は、回収（改修）に該当しないと考えてよいか？

A4-2：発生する事象により回収への該当性を判断すること。
また、平成27年9月1日 薬食監麻発0901 第5号 医療機器及び体外診断用医薬品の製造管理及び品質管理の基準等に係る質疑応答集（Q&A）について（その3）通知の“医療機関等でのバージョンアップ関係”Q9～Q12 を参照すること。

医療機器の基本要件基準第12条第3項の適用について

令和5年3月31日付
薬生機審発0331 第8号

- 基本要件基準第12条第3項が適用されない機器について

なお、令和6年4月1日以降に製造販売する医療機器は、改正後の基本要件基準への適合を確認した上で、改正後の基本要件基準への適合に関する資料を求めに応じて提示できるようにしておくこと。
令和6年3月31日以前に製造販売された医療機器に関する取扱いについては追って通知するものとする。

- 令和6年3月31日以前に製造販売された医療機器のサイバーセキュリティ対応

「基本要件基準」
第12条第3項を適用して設計開発・保守を継続している医療機器

＋

医療現場に存在し、「基本要件基準」第12条第3項への適合が確認できない医療機器

医療機器のサイバーセキュリティ対策に関連する情報提供について

令和６年３月31日以前に製造販売された医療機器のうち、医療機関に存在し、「基本要件基準」第12条第３項への適合が確認されていない医療機器については、設計及び開発におけるサイバーセキュリティ対応が十分とは限らず、サイバー攻撃に対して脆弱である場合がある。医療現場における患者の安全性を確保するため、医療機器の製造販売業者、外国製造医療機器等特例承認取得者又は外国指定高度管理医療機器製造等事業者（以下「製造販売業者等」という。）は、当該医療機器のサイバーリスクに関する評価を実施し、医療機関等に対し、運用、意図する使用環境におけるサイバーリスク等の情報共有、脆弱性の管理等を適切に行う必要がある。従って、令和６年３月31日以前に製造販売された医療機器のうち、医療機関において稼働している可能性のある医療機器のサイバーセキュリティ対応について、以下に留意すること。

（1） 製造販売業者等は、医療現場における患者の安全性を確保するため、当該医療機器のサイバーリスク等に関する評価及び対策等を適切に実施し、意図する使用環境におけるサイバーリスク等に関する情報を医療機関等に提供すること。また、医療機関等の求めに応じてソフトウェア部品表（SBOM）を提示できるように準備しておくこと。

（2） 製造販売業者等は、医療機器のライフサイクルを特定し、製品寿命終了（EOL）及びサポート終了（EOS）に関する情報を医療機関等に提供すること。

① 医療機器がEOLを越えていない場合、製造販売業者等は、サポート（適用可能なセキュリティパッチ、セキュリティ確保に必要なアップグレード等）に関する情報を含めて提供すること。

② 医療機器がEOLを越えている場合、製造販売業者等は、EOSまでの期間は、限定的サポート（セキュリティパッチ、必要に応じて補完的対策等）に関する情報を含めて提供すること。

③ 医療機器がEOSを越えている場合、医療機器製造販売業者等は、速やかに補完的対策等の情報を含め、EOSに関する情報を提供すること。

（3） 製造販売業者等は、医療機器がEOSに達していない（(2)の①又は②）場合、医療機関等に提供したセキュリティパッチ等の情報について、医療機器に適用する計画等を医療機関等へ示し、医療機関等と連携して定期点検等の適切な時期に適用すること。医療機器に適用するセキュリティパッチ等の評価等に時間を要する場合は、ファイアウォール等の補完的対策を先行してリスク緩和策として適用する等の段階的な計画としてもよい。

（4） 製造販売業者等は、医療機器がEOSを越えて使用されている場合においても、有効性及び安全性に関する事項その他製品の適正な使用のために必要なサイバーセキュリティに関する情報を収集し、医療機関等への情報提供を行うこと。また、サイバーセキュリティに関連して医療機器に不具合が発生し、健康被害が発生した又は健康被害の発生のおそれがある場合や、脆弱性に対し外国医療機器の安全確保措置が実施された場合には、不具合等報告の要否を検討し適切な対応をとること。

（5） 製造販売業者等は、中古医療機器を取扱う販売業者等の求めに応じて上記（1）～(4)と同様に提供すること。

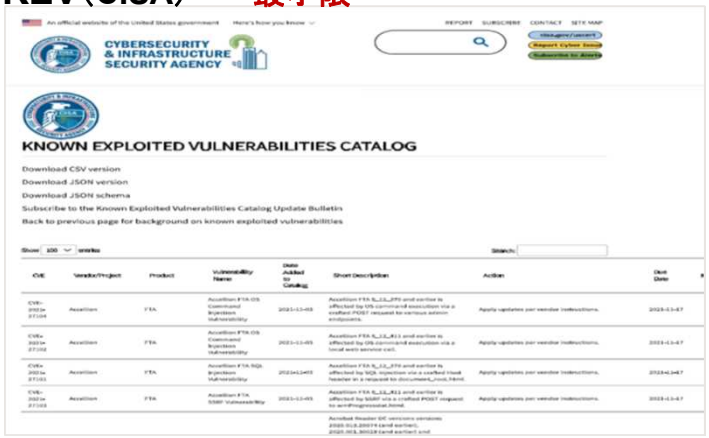
注意： 発出された通知で確認してください。

医療機器のサイバーセキュリティ対策に関連する情報提供について　その1

令和6年3月31日以前に製造販売された医療機器のうち、医療機関に存在し、「基本要件基準」第12条第3項への適合が確認されていない医療機器については、設計及び開発におけるサイバーセキュリティ対応が十分とは限らず、サイバー攻撃に対して脆弱である場合がある。医療現場における患者の安全性を確保するため、医療機器の製造販売業者、外国製造医療機器等特例承認取得者又は外国指定高度管理医療機器製造等事業者（以下「製造販売業者等」という。）は、当該医療機器のサイバーリスクに関する評価を実施し、医療機関等に対し、運用、意図する使用環境におけるサイバーリスク等の情報共有、脆弱性の管理等を適切に行う必要がある。従って、令和6年3月31日以前に製造販売された医療機器のうち、医療機関において稼働している可能性のある医療機器のサイバーセキュリティ対応について、以下に留意すること。

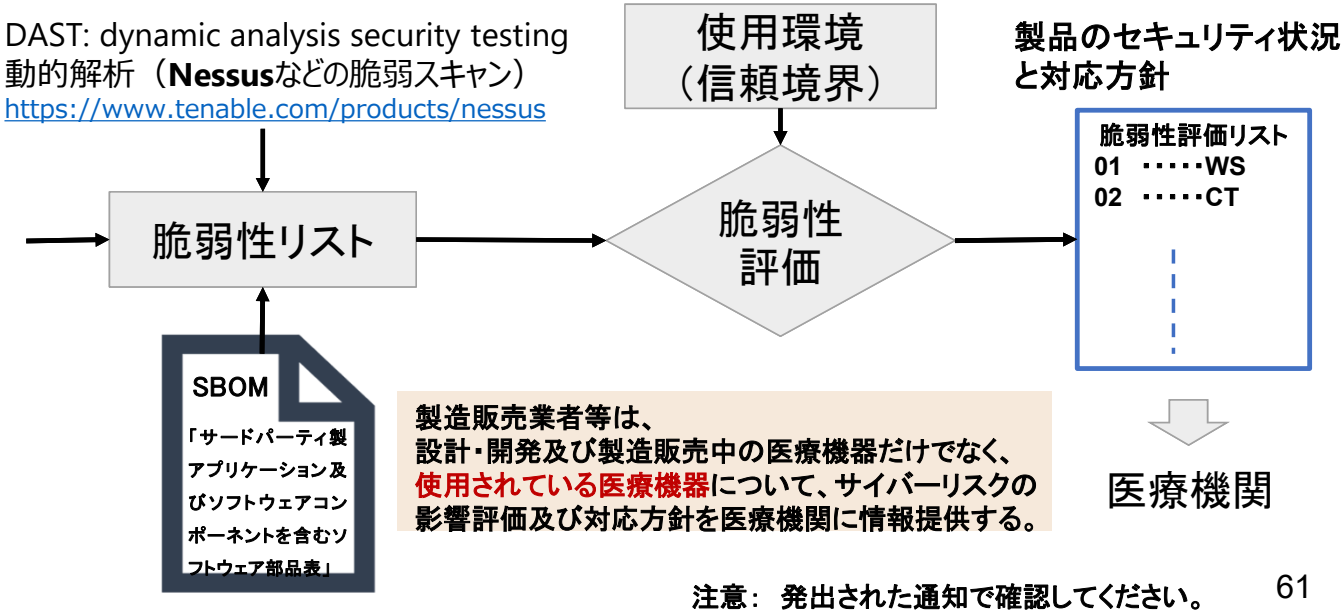
（1） 製造販売業者等は、医療現場における患者の安全性を確保するため、当該医療機器のサイバーリスク等に関する評価及び対策等を適切に実施し、意図する使用環境におけるサイバーリスク等に関する情報を医療機関等に提供すること。また、医療機関等の求めに応じてソフトウェア部品表（SBOM）を提示できるように準備しておくこと。

既知の悪用された脆弱性カタログ
KEV（CISA）　ー 最小限 ー



Known Exploited Vulnerabilities catalog
https://www.cisa.gov/known-exploited-vulnerabilities-catalog

DAST: dynamic analysis security testing
動的解析（**Nessus**などの脆弱スキャン）
https://www.tenable.com/products/nessus



注意：　発出された通知で確認してください。

医療機器のサイバーセキュリティ対策に関連する情報提供について　その2

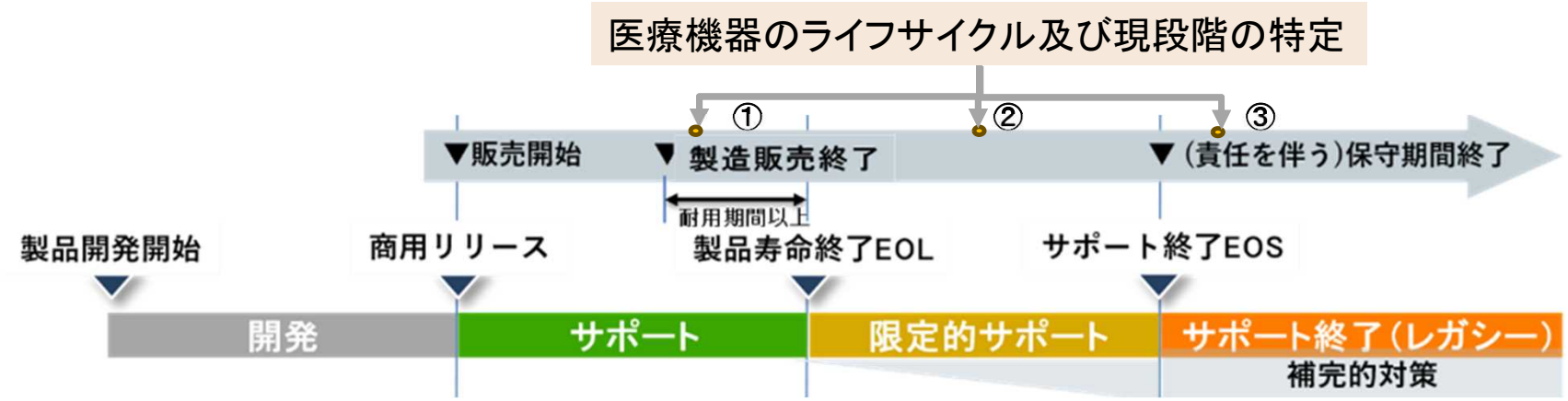
（2） 製造販売業者等は、医療機器のライフサイクルを特定し、製品寿命終了（EOL）及びサポート終了（EOS）に関する情報を医療機関等に提供すること。

① 医療機器がEOLを越えていない場合、製造販売業者等は、サポート（適用可能なセキュリティパッチ、セキュリティ確保に必要なアップグレード等）に関する情報を含めて提供すること。

② 医療機器がEOLを越えている場合、製造販売業者等は、EOSまでの期間は、限定的サポート（セキュリティパッチ、必要に応じて補完的対策等）に関する情報を含めて提供すること。

③ 医療機器がEOSを越えている場合、医療機器製造販売業者等は、速やかに補完的対策等の情報を含め、EOSに関する情報を提供すること。

（3） 製造販売業者等は、医療機器がEOSに達していない（(2)の①又は②）場合、医療機関等に提供したセキュリティパッチ等の情報について、医療機器に適用する計画等を医療機関等へ示し、医療機関等と連携して定期点検等の適切な時期に適用すること。医療機器に適用するセキュリティパッチ等の評価等に時間を要する場合は、ファイアウォール等の補完的対策を先行してリスク緩和策として適用する等の段階的な計画としてもよい。



注意： 発出された通知で確認してください。

（参考）補完的リスクコントロールに関する考慮事項

- 補完的リスクコントロール手段は、医療機器の設計の一部として実装されたリスクコントロール手段の代わりに又はそれがない場合に適用される、特定のタイプのリスクコントロール手段である（AAMI TIR97: 2019）。**健康及び安全に関連するリスクが特定された場合又はその他の不適合がある場合に、製造販売業者は、機器を適合状態にするために、更なる修正、是正処置を実施し、適用可能な場合は、予防処置を実施する。**

- 機器が、製造販売業者によって通知されたようにEOSに到達した際、ヘルスケアプロバイダーは、レガシーな技術を使うことで引き起こされるリスクがあるのに製造販売業者の（セキュリティに関する）サポートがない状態であるにもかかわらず、機器の運用を継続するという決定を行う可能性がある。継続使用の理由としては、機器を臨床使用可能な期間がサポート期間を超えている、市場に現実的な代替策がない、予算の限界などが挙げられるが、これらには限られない。

- 機器の運用継続を決定したら、ヘルスケアプロバイダーは、限定的サポート段階及びEOS段階に製造販売業者が提供する製品の顧客向けセキュリティ文書を調べることが望ましい。この文書には、機器それ自身及び運用するIT環境に対して適用可能な、最低限の補完的リスクコントロール手段が含まれている。

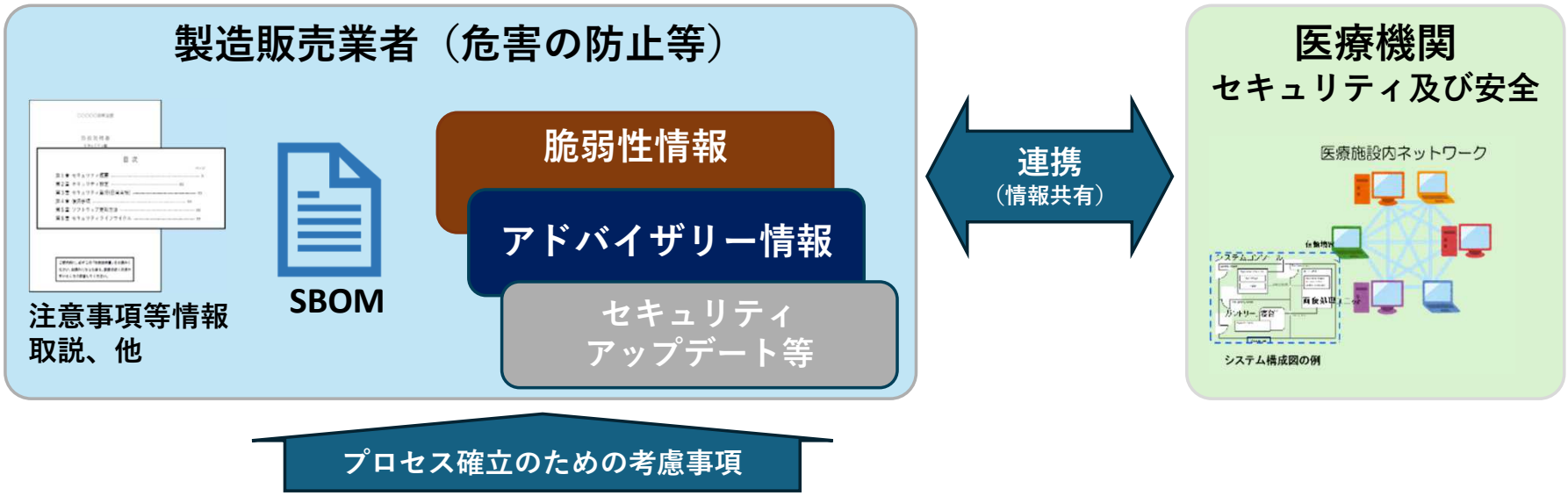
補完的リスクコントロールに関する考慮事項

- 補完的リスクコントロール手段の例

コントロールのタイプ	補完的リスクコントロール手段
物理的アクセス	単に機器を物理的に制限された領域に置いて、物理的な入室管理を適切に行うことによって、機器への物理的アクセスを、許可した要員だけに制限する。
リムーバブルメディア	USBドライブなどのリムーバブルメディアの使用を、システムのBIOS/UEFIポリシーによって、OSのポリシー又は物理的手段を通して制限する。
ネットワークの分離	機器を病院ネットワークから分離する。
ネットワークのセグメント化	機器のVLAN並びに機器が通信するその他のインフラストラクチャー及びサービスをセットアップする。
監視	侵入検知システム（IDS）、侵入予防システム（IPS）又はセキュリティ情報及び事象マネジメント（SIEM）を用いて、機器及びネットワークの疑わしい活動を監視する。
リモートアクセス	機器からリモートアクセス機能を削除する。
ファイアウォール	機器を物理的又は仮想的なファイアウォールの背後に配置し、厳密に必要なネットワーク通信のファイアウォールポートだけを開放する。
アンチマルウェア	機器にマルウェア対策ソフトウェアをインストールする。ネットワークから分離された機器（スタンドアローン）については、定義の更新を必要としないソフトウェアを用いる。例えば、AIを用いたマルウェア対策ソフトウェア。
バックアップ及び復元	災害時のデータ損失に対して保護するために、バックアップ及び復元の手順を実装する。

医療機器のサイバーセキュリティに関する脆弱性マネジメント　―　プロセス確立

■ 製品セキュリティの透明性を確保し、医療機関との情報共有を重視した
サイバーセキュリティ対策の確立・実施



- 医療機器のサイバーセキュリティを確保するための**脆弱性の管理**等について
（医薬機発0328第1号、医薬安発0328第3号）
- 医療機器サイバーセキュリティに関する**不具合等報告の基本的考え方**について
（医薬安発0115第2号）
- 医療機器の**サイバーセキュリティ対策**に関連する一部変更に伴う軽微変更手続き等の取扱いについて
（医薬機審発0423第1号）
- 医療機器のサイバーセキュリティ対策に関連する情報提供について

Ministry of Health, Labour and Welfare of Japan

6. 医療機器サイバーセキュリティに関する情報共有の取組

サイバーセキュリティに関する情報共有　ー　基本情報　ー

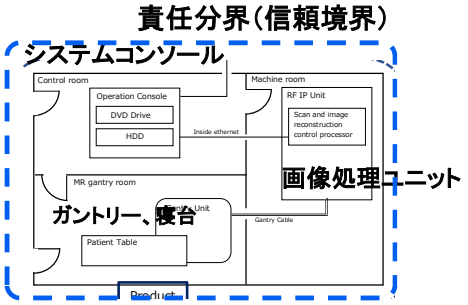
■ 注意事項等情報及び取扱説明書（例）

- 意図する使用環境、ユーザーの遵守事項（概要）、要求された環境外で使用した場合のリスク等
- サイバーセキュリティに関連する問合せ窓口及びサイバーセキュリティに関連するサービスの照会先
- アンチマルウェアソフトウェア、ネットワーク接続設定、ファイアウォールの使用等、意図する使用環境に適した推奨されるサイバーセキュリティに関連する医療機器の使用方法及び製品仕様
- 正常な機能を回復するためのバックアップ並びに復元の機能及び手順の説明
- データを送受信するネットワークポート及びその他のインタフェースのリスト並びにポート機能、着信・発信ポートの説明。但し、未使用ポートは無効化することに留意する。
- エンドユーザー向けのシステム構成図（ネットワーク構成図）

ー 既知の脆弱性等に対する対策 ー

- ファイアウォールなど補完的対策に関連する装置の設置・設定に関する情報

※ 必要に応じて更新する。



システム構成図の例

サイバーセキュリティに関する情報共有 ― 透明性 ―

その他のセキュリティ文書

- 医療機器の製品寿命（EOL）、サポート終了（EOS）や保守計画に関する情報
- 医療機器製品に実装されているオープンソース及び市販のソフトウェア部品（製品コンポーネント）の透明性を確保するためのSBOM
- 医療機器の意図する使用及び使用環境に対する設計を俯瞰可能な、製造販売業者による医療機器セキュリティ開示書（Manufacturer Disclosure Statement for Medical Device Security：MDS2）

- 必要に応じて、セキュアなネットワーク接続の展開及びサービスを可能にするための技術的指示
  - 意図したとおりの医療機器の動作を確保するための、医療機器周辺の一般IT機器等の支援インフラの要求事項に関するユーザーへの具体的なガイダンス
  - セキュアな設定を用いた機器の強化あるいは強化可能性に関する説明（マルウェア対策、ファイアウォール/ファイアウォール規則、ホワイトリスト等）

- サイバーセキュリティ脆弱性又はインシデントが検知された際の対応方法に関するユーザーへの指示
- 医療機器に係るセキュリティ事象が検出された場合に、医療機器又は支援システムがユーザーに異常を通知する方法に関する説明

アドバイザリー情報

- 必要に応じて、認証された特権ユーザーが、医療機器の設定を保存し、回復するための方法の説明
- 許可されたユーザーが、製造販売業からアップデートをダウンロードしてインストールするための体系的な手順の説明

注記　SBOM及びMDS2は、医療機器のセキュリティ設計及びリスクマネジメント計画を踏まえたTPLC並びに顧客向け文書に関する網羅的な文書となる。SBOM及びMDS2は製品導入の検討にあたって開示を求められる場合もある。

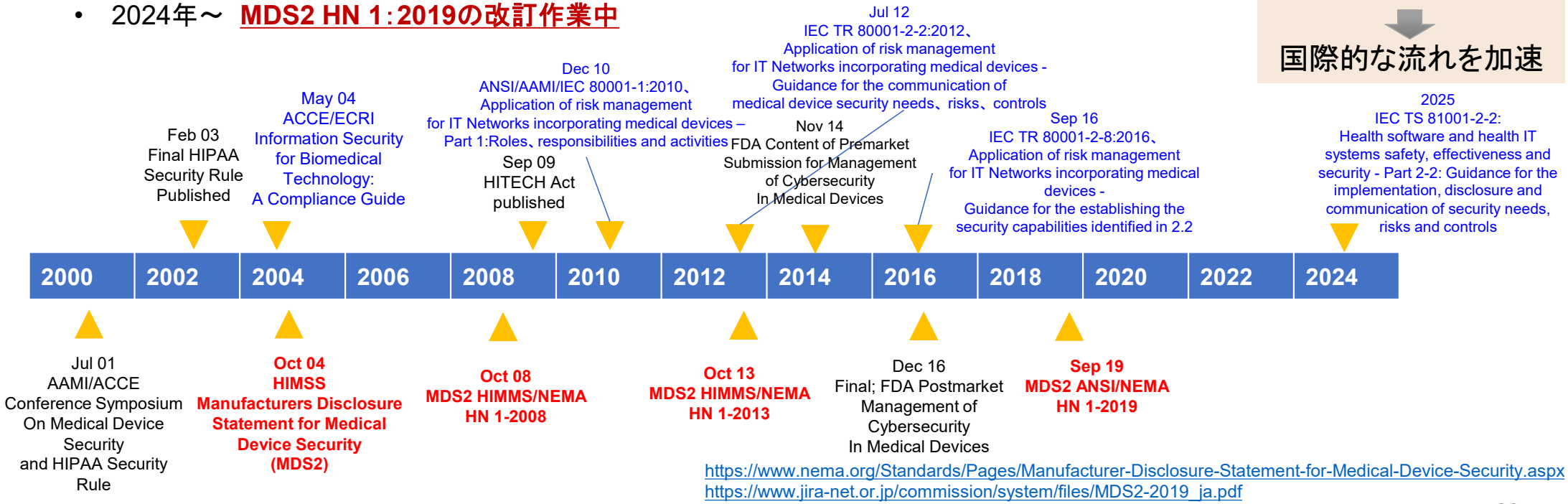
MDS2の背景

MDS2: Manufacturer Disclosure Statement for Medical Device Security
（医療機器セキュリティに関する製造業者の情報開示説明書）

MDS2は米国HIPAA法への適合チェックのツールの位置付けで導入された。

- 2003年 「HIPAA（医療保険の相互運用性と説明責任に関する法令）法」発効（Health Insurance Portability and Accountability Act）
- 2004年 **「MDS2 v.1.0(2004-11-01)」**として公表
- 2008年 HIMSS/NEMA合同規格**「HIMSS/NEMA Standard HN 1-2008」**として公表
- 2013年 **IEC TR 80001-2-2のセキュリティカテゴリーに合わせするために、改訂作業**を行い、**「HIMSS/NEMA Standard HN 1-2013」**を公表
- 2017年 NEMAは文書の機能性をさらに改善し技術の進歩を取り入れるために、2013-MDS2の改訂作業に着手
- 2019年10月に**「ANSI/NEMA HN 1-2019」**を公表
- 2022年～ **IEC TS 81001-2-2として、HN 1-2019 のセキュリティカテゴリーに対応する国際標準化**
- 2024年～ **MDS2 HN 1：2019の改訂作業中**

医療機器の
セキュリティ機能開示
⇩
国際的な流れを加速



https://www.nema.org/Standards/Pages/Manufacturer-Disclosure-Statement-for-Medical-Device-Security.aspx
https://www.jira-net.or.jp/commission/system/files/MDS2-2019_ja.pdf

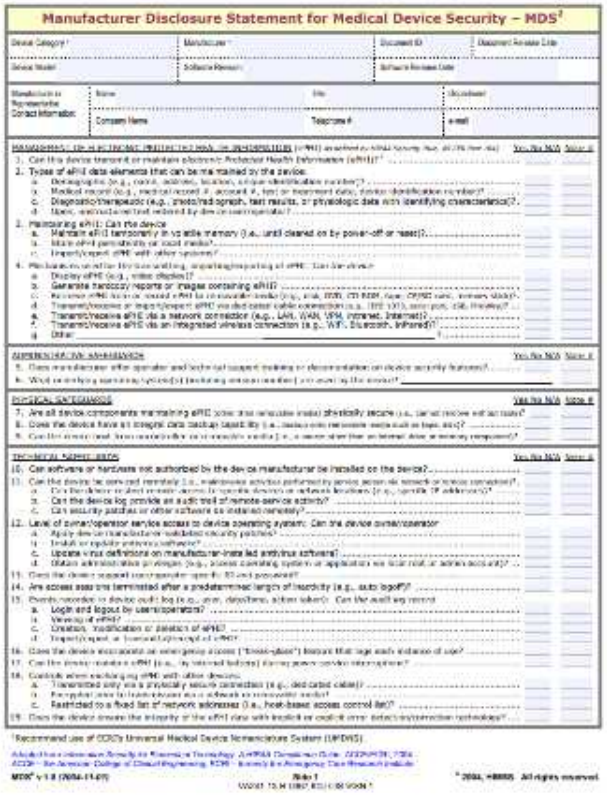
MDS2 － 透明性（Transparency）強化

- **MDS2: Manufacturer Disclosure Statement for Medical Device Security**
  （医療機器セキュリティに関する製造業者の情報開示説明書）

セキュリティ機能の説明

MDS2カテゴリ	コメント
MPII	個人を特定できる情報の管理
ALOF	自動ログオフ
AUDT	監査コントロール
AUTH	認証
CSUP	サイバーセキュリティ製品の更新
DIDT	健康データの匿名化
DTBK	データのバックアップと災害復旧
EMRG	緊急アクセス
IGAU	健康データの完全性と真正性
MLDP	マルウェアの検出/保護
NAUT	ノードの認証
CONN	接続能力
PAUT	個人認証
PLOK	物理的ロック
RDMP	機器のライフサイクルにおけるサードパーティアプリケーション及びソフトウェアコンポーネントのロードマップ
SBOM	ソフトウェア部品表（SBOM）
SAHD	システムとアプリケーションの堅牢化
SGUD	セキュリティガイド
STCF	健康データストレージの機密性
TXCF	送信の機密性
TXIG	送信の完全性
RMOT	リモートサービス及び管理
OTHR	他のセキュリティ考察

MDS2 Form（HN 1-2019 ）



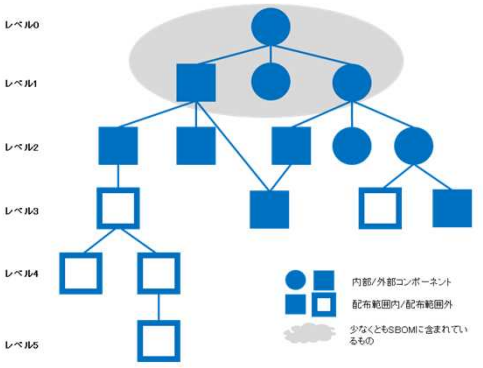


図9 トップレベルSBOM

附属書 SBOM（規定がない）

- トップレベルSBOM
- ネットワーク接続したシステムユニットに限定

SBOMは独立して進化

MDS2とSBOMの分離に関する議論

ソフトウェア部品表（SBOM）の変遷

IEC 62304 にみるSBOMの基礎情報

8 ソフトウェア構成管理プロセス
8.1 構成識別（クラス A、B、C）
8.1.2 SOUP の特定（クラス A、B、C）
現在使用中の SOUP 構成アイテム（標準ライブラリを含む）のそれぞれについて、次を文書化
a) 名称
b) 提供業者（サプライヤー）
c) SOUP を特定する識別子
識別子の例: バージョン、リリース年月日、パッチ番号、アップグレードの識別子など

3要素

8.1.3 システム構成文書の特定（クラス A、B、C）
構成アイテム及びそのバージョン一式の文書化

ただし、ここでは、SOUPはサードパーティ製コンポーネントとする。

OTS（サードパーティ製）
ソフトウェアの透明性確保

手引書改定案 表A-2 SBOMの最小限の要素

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（オプション）	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
依存関係	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

7要素

MDS2の附属書　SBOM
（機械可読を目的としていない）

Software Name	Version	Creator
Windows 10 IoT enterprise 2019 LTSC	1809	Microsoft
Microsoft Visual C++ 2017 Redistributable (x64)	14.14.26429.4	Microsoft
SQL Server Browser for SQL Server 2014	12.2.5000.9	Microsoft

SQL Server、Visual C++、Visual Studio、Windows、Microsoftはマイクロソフトグループ企業の商標です。

サプライヤーのSBOM提供

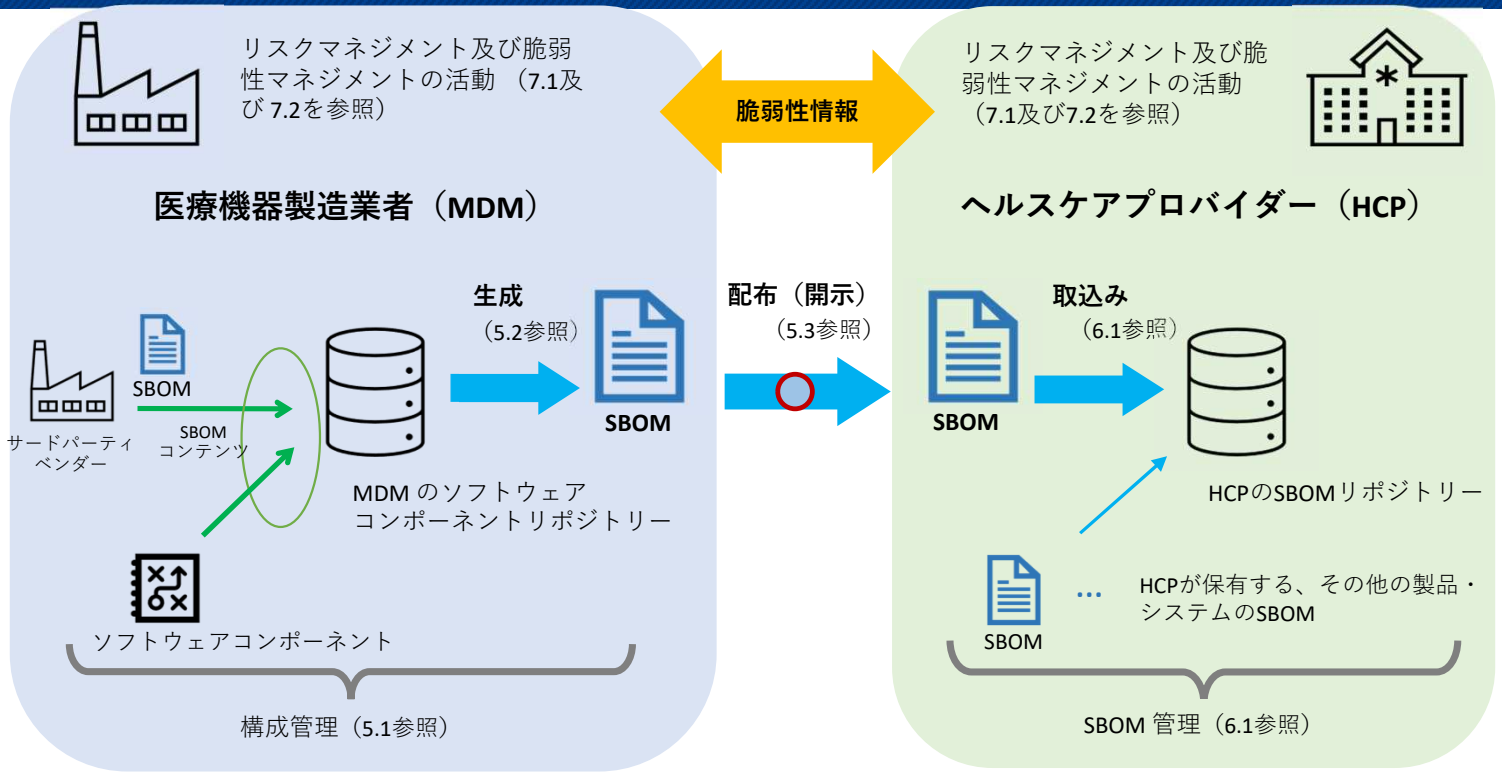
製販業者のツール等を利用した探索

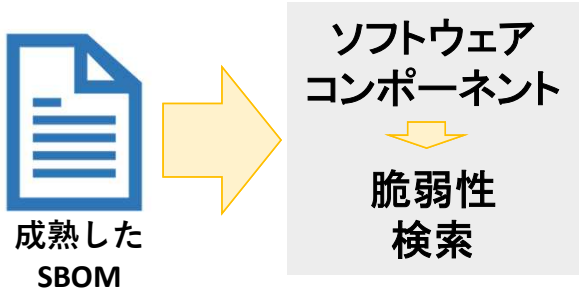
SBOMのフォーマットの例（機械可読の電子ファイル）

(1) SPDX（Software Package Data Exchange）ISO/IEC 5962:2021
・ライセンス情報含む）
・Tag-Value(txt)形式、RDF形式、xls形式、json形式、xml形式等
(2) CycloneDX　（セキュリティに特化）
(3) SWIDタグ（Software Identificationタグ）　ISO/IEC 19770-2:2015

id	サプライヤーの名前	コンポーネントの名前	コンポーネントのバージョン	固有識別子	関係	作成者	タイムスタンプ
1	Microsoft	Windows 10 IoT enterprise 2019 LTSC	1809	cpe:2.3:o:microsoft:windows_10:2019:*:*:*:enterprise_ltsc:*:*:* 0402EE03-3BF6-4243-A257-7FFFC088EEFF	Included in System Console	IKIREN	2023-08-19 T08:14:01Z
2	Microsoft	Microsoft Visual C++ 2017 Redistributable (x64)	14.14.26429.4	cpe:2.3:a:microsoft:visual_studio:2017:*:*:*:*:*:*:* or cpe:2.3:a:microsoft:visual_c++:*:*:*:*:*:*:*	Included in id#1	IKIREN	2023-01-21 T03:14:07Z
3	Microsoft	SQL Server Browser for SQL Server 2014	12.2.5000.9	cpe:2.3:a:microsoft:sql_server:2014:sp2:*:*:*:*:*:*	Included in System Console	IKIREN	2023-01-13 T05:54:00Z

ソフトウェア部品表（SBOM）の作成・運用の確立（脆弱性検知）



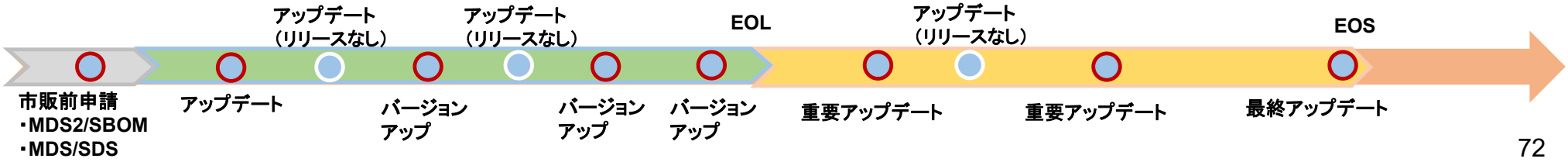


全分野対象に進められている脆弱性マネジメント自動化のフロー（SBOM起点）

SBOM導入・運用の手引き（2024/12）
https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2024/sbn8o10000001y6j-att/sbn8o10000001zcl.pdf

IMDRF N73 図1—SBOMフレームワークの概要を引用

参考）ソフトウェア管理に向けたSBOM（Software Bill of Materials）の導入に関する手引 Ver. 2.0
https://www.meti.go.jp/policy/netsecurity/wg1/SBOMv2.pdf



SBOM関連の課題（例）

- 課題を理解した上で、一貫した命名法とデータ形式を用いて正規化されたルールを利用する必要

ソフトウェア部品表（SBOM）処理におけるデータ正規化の課題と緩和策 （MITRE）

https://www.mitre.org/sites/default/files/2024-10/PR-24-2647-Data-Normalization-Challenges-Mitigations-Software-Bill-Of-Materials-Processing.pdf

ID	サプライヤー名	コンポーネント名	コンポーネントのバージョン	その他の一意の識別子	依存関係	SBOM作成者	タイムスタンプ
1	Company A	Application	1.1	234	Primary	Company A	05-09-2022 13:00:00
2	Company B	Browser	2.1	334	Included in **#1**	Company B	04-18-2022 15:00:00
3	Mr. C	Compression Engine	3.1	434	Included in **#2**	Company A	05-09-2022 13:00:00
4	Community P	Protocol	2.2	534	Included in **#1**	Company A	05-09-2022 13:00:00

Naming Rule

作成の単位で割りつけられる

CPEの問題は未解決
（この例は、serialNumber、component/cpe）

多数の言い回しがある
マージした場合にID＃の
リンクが壊れないように注意

※ CPEの命名規則

- **CPE：Common Platform Enumeration**、共通プラットフォーム一覧
  - CPEは、米国政府が推進している情報セキュリティにかかわる技術面での自動化と標準化を実現する技術仕様SCAP(Security Content Automation Protocol)(*2)の構成要素のひとつ　IPAの解説：https://www.ipa.go.jp/security/vuln/scap/cpe.html
- cpe:/{種別}:{ベンダ名}:{製品名}:{バージョン}:{アップデート}:{エディション}:{言語}
  - 大文字と小文字の区別はない
  - 基本構成のそれぞれの箇所が空白の場合、「全て」を意味する。例えばバージョンが空白の場合、全てのバージョンの意味。

CPE例
microsoft:windows_2000::sp4:pro

Windows、Microsoftはマイクロソフトグループ企業の商標です。

ソフトウェア利用者が所有するSBOMの事例 ー 羅層構造

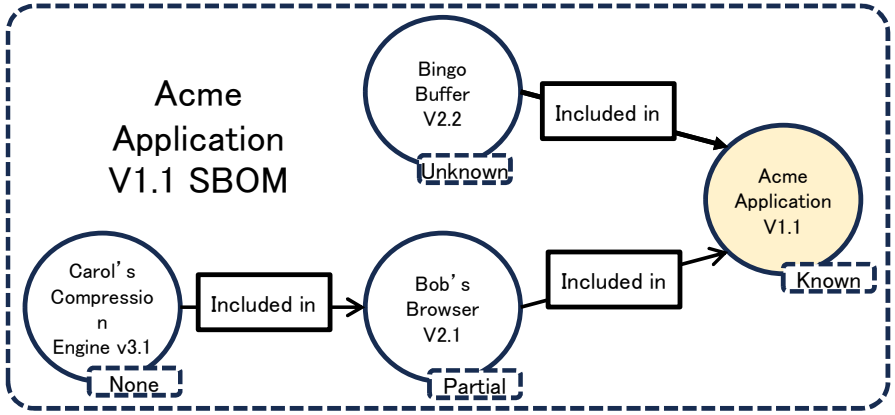


図6 のサプライチェーンのSBOM図（一つのSBOM）

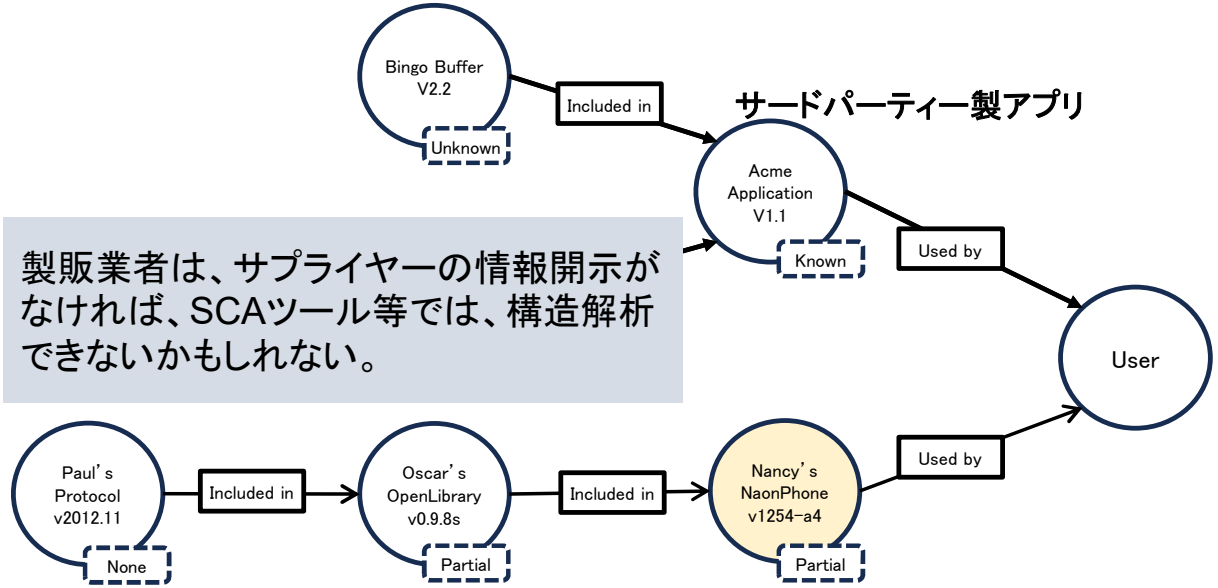


図7 2つのサプライチェーンを含むSBOM図（説明のため一部加工）

表9 NancyのNanoPhoneの概念的なSBOM表の例

コンポーネント名	サプライヤー名	バージョン文字列	作成者	ハッシュ	個別識別子	依存関係	依存関係の完全性
NanoPhone	Nancy	v1254-a4	Nancy	0x523	237	Primary	Partial
|--OpenLibrary	Oscar	0.9.8s	Nancy	0xA23	394	Included in	Partial
|--Protocol	Paul	2012.11	Nancy	0xB53	934	Included in	None

*表は例示のために、タイムスタンプ属性は省略され、他の属性名は短縮されていることに注意する。

CISA: Framing Software Component Transparency: Establishing a Common Software Bill of Materials (SBOM) September 3, 2024
https://www.cisa.gov/sites/default/files/2024-10/SBOM%20Framing%20Software%20Component%20Transparency%202024.pdf

ソフトウェア利用者が所有するSBOMの事例 ー 羅層構造

サプライヤー提供の
SBOM活用

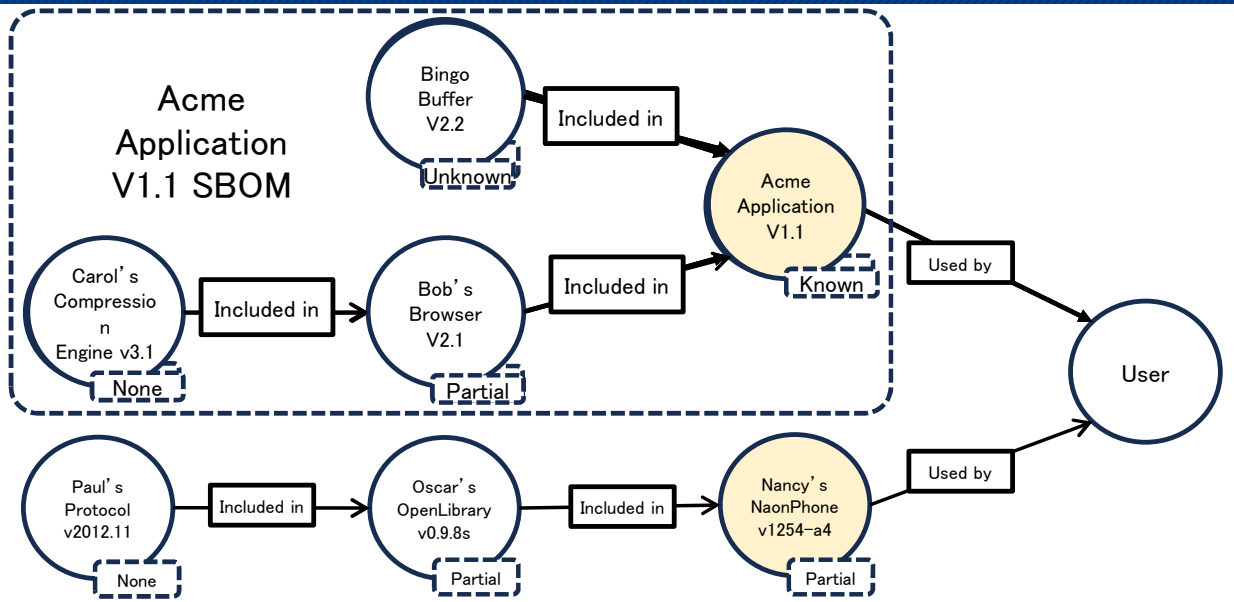


図7 2つのサプライチェーンを含むコンポーネント図

表9 NancyのNanoPhoneの概念的なSBOM表の例

コンポーネント名	サプライヤー名	バージョン文字列	作成者	ハッシュ	個別識別子	依存関係	依存関係の完全性
NanoPhone	Nancy	v1254-a4	Nancy	0x523	237	Primary	Partial
|--OpenLibrary	Oscar	0.9.8s	Nancy	0xA23	394	Included in	Partial
|--Protocol	Paul	2012.11	Nancy	0xB53	934	Included in	None

*表は例示のために、タイムスタンプ属性は省略され、他の属性名は短縮されていることに注意する。

CISA: Framing Software Component Transparency: Establishing a Common Software Bill of Materials (SBOM) September 3, 2024
https://www.cisa.gov/sites/default/files/2024-10/SBOM%20Framing%20Software%20Component%20Transparency%202024.pdf

医療機器の範囲、信頼境界の明確化、図化とSBOM

- SBOMの対象範囲： **医療機器の構成に含まれる全てのコンポーネントが対象**
  データ（情報）の流れを踏まえて図化

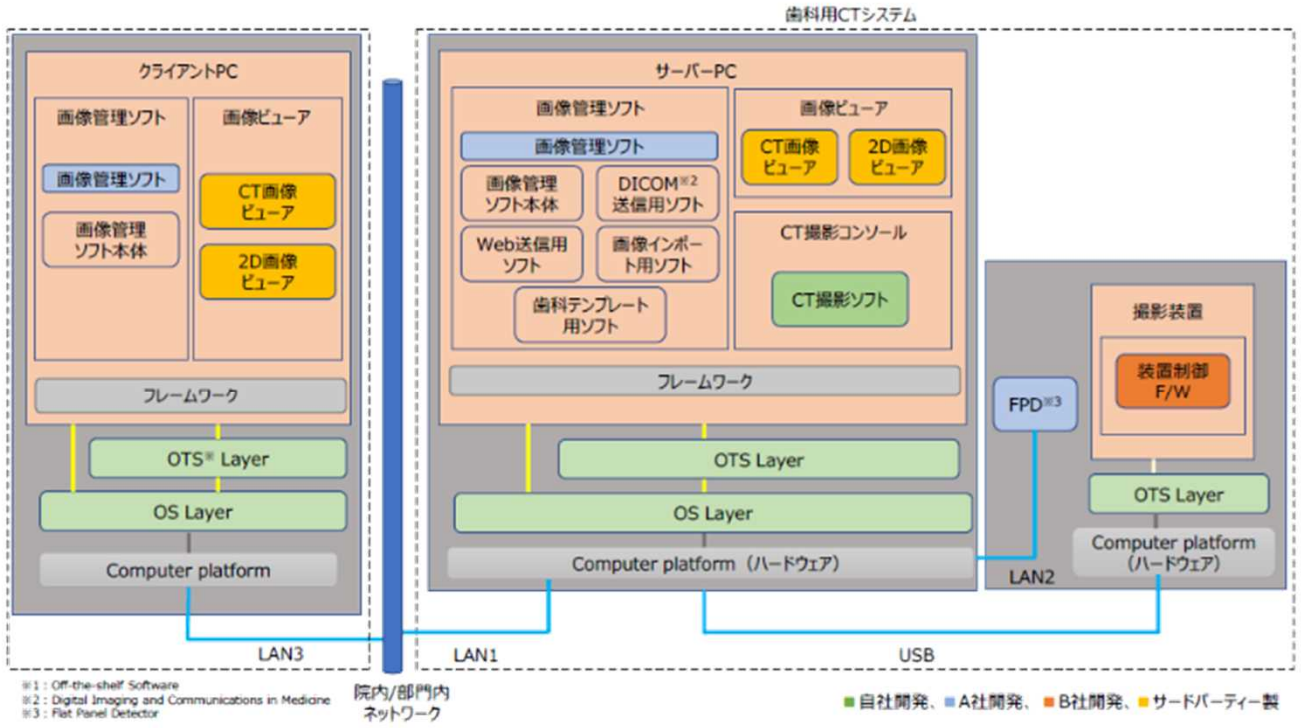


図 4-1 システム構成図の例（歯科用 CT の例）　経産省資料より

複数の製品（ユニット）からなる製品のSBOM作成

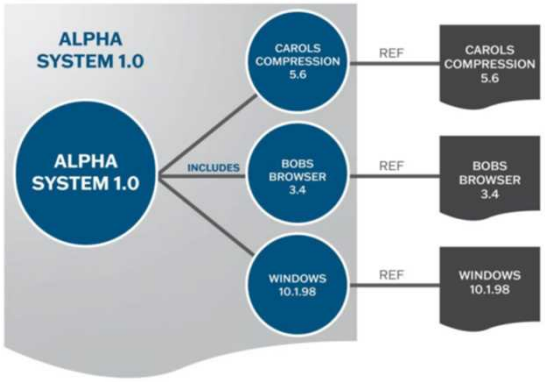


Figure 1: Sample graphical representation of a PLB-SBOM for “Alpha System 1.0”

Assembling a Group of Products
https://www.cisa.gov/sites/default/files/2024-01/Assembling-a-Group-of-Products_508c_0.pdf

SBOMとソフトウェア・ライセンシング・ガバナンス
— ソフトウェア構成管理の完全性及び透明性の保証
（SBOM非準拠のソフトウェアの排除を推奨）

FDA Medical Device Cybersecurity And SBOMs: Compliance And Potential
https://www.forbes.com/sites/forbestechcouncil/2024/07/22/fda-medical-device-cybersecurity-and-sboms-compliance-and-potential/

国際的なサイバーセキュリティの動向　ー　“CISA: Secure by Demand Guidance”（2024/8/6）

このガイダンスでは、ソフトウェアを購入する組織が、ソフトウェア製造者のサイバーセキュリティに対するアプローチをよりよく理解し、製造者がセキュア・バイ・デザインを中核的な検討事項としていることを確認するために使用できる質問とリソースを示す。このガイダンスは、CISA が技術メーカー向けに提供している「Secure by Design」ガイダンスと対をなし、「Secure by Design」の 3 つの原則を提示している。

1. 顧客のセキュリティ成果を所有する。
2. 抜本的な透明性と説明責任を受け入れる。
3. これらの目標を達成するための組織構造とリーダーシップを構築する。

サイバーセキュリティに関する
QMSの指標

- 顧客はメーカーが製品セキュリティにどのように取り組んでいるかにも注目する必要がある。
- 製品セキュリティとは、ソフトウェア・メーカーが提供する製品が攻撃者に対して安全であることを保証するために取る行動を指す。
- このガイダンスは、製品セキュリティの成熟度や、製造者がセキュアバイデザインの原則に従っているかどうかを評価するために組織が活用できるリソースを提供する。

組織は、製品セキュリティへの配慮を調達ライフサイクルの様々な段階に組み込むことができる：
調達前に、候補となる各ソフトウェアメーカの製品セキュリティに対する取り組みを理解するための質問を行う。
調達中に、適宜、製品セキュリティ要件を契約文言に組み込む。
調達後、ソフトウェアメーカーの製品セキュリティとセキュリティ成果を継続的に評価する。

https://www.cisa.gov/resources-tools/resources/secure-demand-guide

ソフトウェア部品表（SBOM）関連の課題　ー　共有方法の確立

- SBOMシェアリング入門　SBOM Sharing Primer

本文書は、ソフトウェア部品表（SBOM）をソフトウェアサプライチェーンの異なる関係者間で共有する方法の例を示す。**ある当事者がSBOMを作成し、別の当事者がそのSBOMにアクセスしたいと仮定した場合の、SBOM共有のプロセスとメカニズムに焦点**を当てている。例として、プロプライエタリなソフトウェアベンダーが電子メールでSBOMを共有するものから、オープンソースプロジェクトが集中型リポジトリでSBOMを公開するものまで、現在使用されている**SBOM共有方法**を示す。

ライフサイクル段階	洗練度　低	洗練度　中	洗練度　高
開示	● 消費者主導 ● 著者または販売業者によるガイダンスが限定的、または存在しない。	● ソフトウェアのソースコードに配置されたSBOM - 時点（単数バージョン） -メーカー使用説明書（MUD） ● 既知の中央リポジトリ ● ウェブサイト	● 利用可能なSBOMの自動伝播 ● 関係者への継続的な更新 ● 発行/購読パターン ● 分散台帳
アクセス	● 制御不能 ● 手動制御 ● ケースバイケース	● 要認証 ● アクセス制御の粒度に制限 ● プライベート/ブロードキャスト/パブリックチャネル、ロール ● プライベートチェーン/コンセンサスアルゴリズム	● 認証とアクセス制御の委譲 ● 完全なアクセス制御の粒度
トランスポート	● 人間主導のプロセス ● ポイントツーポイント ● 言葉による伝達	● 一貫性のない、多様な方法または文書 ● アドホックな自動化	● ドキュメント ● 再現性 ● 自動アクセス ● よく知られたプロトコル（REST/RESTful/SOAP APIなど） ● 分散台帳の同期

表1：SBOM共有ライフサイクルの段階と洗練度

共有方法の段階的移行（目標・計画）

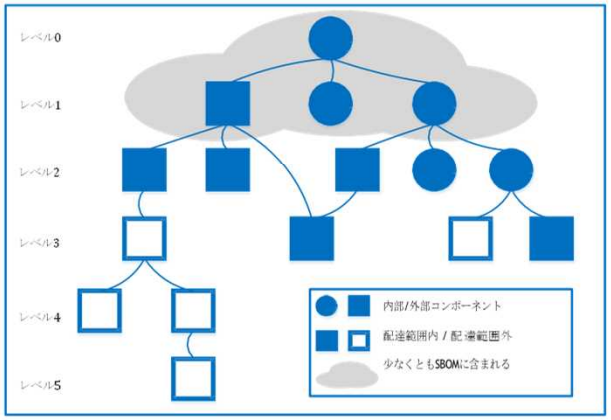
SBOMの共有は、さまざまな洗練されたメカニズムを使用して、今日すでに行われていることを実例で示した。本稿が示すように、さまざまな共有アプローチにはトレードオフがある。より手作業的な手法では、アクセスの制御をより大きくすることができるが、拡張性に欠ける。自動化された共有方法は、規模に応じた発見可能性と転送をサポートするが、より高度なアクセス制御を必要とする場合がある。**最終的に、適切な SBOM 共有メカニズムを選択するかどうかは、ソフトウェア・ライセンス、業界の慣行、組織の優先事項、対象消費者、リスク許容度などの要因によって決まる。**

例 1：電子メール経由で共有される独自ソフトウェアの SBOM
例 2：ベンダーのポータルを介して共有される独自ソフトウェアの SBOM
例 3：ベンダーのポータルで共有される独自ソフトウェアのSBOM
例 4：ツールを経由したOpen Source Software（OSS）の SBOMの共有
例 5：プラットフォーム経由で共有されるOSSのSBOM
例 6：サプライチェーンを介して共有される独自ソフトウェアのSBOM

https://www.cisa.gov/sites/default/files/2024-05/SBOM%20Sharing%20Primer.pdf

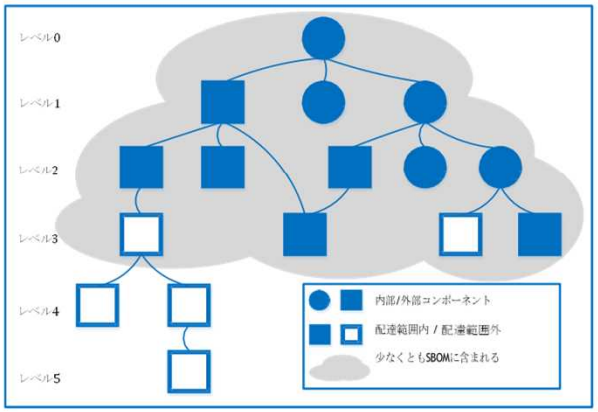
ソフトウェア部品表（SBOM）関連の課題　ー　SBOMの粒度（詳細レベル）

- **BSI TR-03183: Cyber Resilience Requirements for Manufacturers and Products**
  製造業者及び製品に対するサイバーレジリエンス要求事項
  ドイツBSIが、来るサイバーレジリエンス法に向けて、製造業者および製品に対するサイバーレジリエンス要求事項に関する多くの文書を発表した。**第2部では、SBOMの形式的・技術的要件が記述**されている。他の2つのパート（一般要求事項と脆弱性の取扱い）はコミュニティドラフトであり、11月末まで協議が可能である。
  https://www.bsi.bund.de/dok/TR-03183-en
  Part-1 General requirements　2024/9/20 Draft
  Part-2 Software Bill of Materials (SBOM) 2024/9/20 V2.0
  Part-3 Vulnerability Reports and Notifications （CVD手順等） 2024/9/20 Draft
- **SBOMの詳細レベル**



主要コンポーネントの完全な記述に加えて、SBOMには主要コンポーネントが直接依存するすべてのコンポーネントの完全な記述が含まれる。

図1：トップレベルSBOM



主要コンポーネントの完全な記述に加えて、SBOMは、納入範囲に属し、主要コンポーネントによって直接または移行的に依存される、少なくともすべてのコンポーネントの完全な記述を含む。コンポーネントとその依存関係の完全な記述と再帰的解決は、少なくとも納入範囲外の最初のコンポーネントまでの各パスで実行される。このコンポーネントも、このコンポーネントの依存関係を除き、SBOMに完全に記述されなければならない；

図4：納入品目SBOM

したがって、これらの依存関係を解決する必要はない。

アドバイザリー情報の開示

- 情報開示の目的：**製造販売業者の責任**
  ユーザーに求められた際に必ず提供
  - 脆弱性に関係する製品と対策
  - 製品に直接関係（影響）しない脆弱性に対する情報
  - EOS後の緊急性が高い脆弱性に対する情報

セキュリティ アドバイザリー報告の例

- 協調的な脆弱性の開示（CVD）実現の上で必須
  例） 脆弱性 “Ripple20”
  「Ripple20」と名付けられたこれらの脆弱性が悪用されると、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、産業用制御機器が誤作動したりと、重要インフラを含む様々な業界で使用される数億台もの機器に影響を与えるという。
  2020/6/16 （IPA CIPセキュリティニュース 2020年6月第3週号より）
  https://www.infosecurity-magazine.com/news/ripple20-vulnerabilities-discovered/

- 公開されているアドバイザリーレポート（H-ISAC 2020年6月19日）

Manufacturer	Public Advisory
B. Braun	https://www.bbraunusa.com/en/products-and-therapies/customer-communications.html
Baxter	https://www.baxter.com/product-security
Carestream	https://www.carestream.com/en/us/services-and-support/cybersecurity-and-privacy
GE Healthcare	https://www.gehealthcare.com/security
Medtronic	https://global.medtronic.com/xg-en/product-security/security-bulletins.html

https://h-isac.org/

脆弱性関連情報（セキュリティ アドバイザリー） ー 製造販売業者と医療機関との連携

Windows DNS サーバーのリモートでコードが実行される脆弱性(CVE-2020-1350)

2020年7月14日、Microsoft社は「パッチチューズデイ」と呼ばれるWindowsの定期アップデート「2020 年 7 月のセキュリティ更新プログラム」（**緊急：CVSS 10.0**）を公開しました。中でも、Windows DNSサーバのRCE（リモート遠隔コード実行）脆弱性「CVE2020-1350」は発見者のCheck Point社により**「SIGRed」と命名され「ワーム活動に利用可能」**な脆弱性として注視されています。（トレンドマイクロ社）
https://blog.trendmicro.co.jp/archives/25567

製造販売業者（SBOM提供済み）

■ セキュリティアドバイザリーの開示

影響を受けるのはDNSサーバだけであり、クライアントに影響はないので、影響範囲は大きくないと判断している。

2020年7月21日　CVE-2020-1350| Windows DNS Server Remote Code Execution Vulnerability

MITRE CVE-2020-1350

概要

弊社は、弊社が製造する医用画像機器への本脆弱性の適用可能性の調査を継続しています。

- **対象となる可能性のある製品**
- **該当なし**
- **該当しない製品**
- **すべてのコンピュータ断層撮影装置**
- **すべての超音波画像診断装置**
- **調査中の製品**
  - **なし**

注：この脆弱性は、現在更新された分析を待っているものであり、最新の改訂版の時点での当社の最善の知見を示したものです。そのため、更なる解析が行われ、その結果が更新された場合には、内容が変更される可能性があります。

本件の問合せ先

……..

医療機関（医療機器のソフトウェアを管理）

■保有する医療機器のSBOM情報を確認

医療機器を構成するOS、ソフトウェアを確認

■ 公開CVE情報からNVD脆弱性情報を確認

影響を受けるOS,ソフトウェアの構成を確認
＞　影響を受ける可能性がある医療機器を確認

■製販業者のアドバイザリー情報で検証

影響を受ける医療機器を確認
＞　リスクアセスメントを実施し、至急対応、問合せ等

対応の実施

Windowsはマイクロソフトグループ企業の商標です。

脆弱性関連情報（セキュリティ アドバイザリー）のフレームワーク

3.2 脆弱性の概要

3.2.1 CVE-2018-8444　Windows SMB の情報漏えいの脆弱性

Microsoft Server Message Block 2.0 (SMBv2) サーバーが特定の要求を処理する方法に、情報漏えいの脆弱性が存在します。この脆弱性の悪用に成功した攻撃者は、特別に細工されたパケットを作成し、サーバーから情報を漏えいさせる可能性があります。
CVE-2018-8444 がこの脆弱性に割り当てられています。
CVSS v3 ベーススコアは、7.0 と計算されています。 CVSSベクタ文字列は、(AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C) です。

3.3 背景

- 重要インフラストラクチャ分野: ヘルスケアと公衆衛生
- 導入国/地域: 世界

4. 緩和策

影響を受ける製品のセキュリティアップデートを用意していますので、適用することを推奨します。下記、連絡先までお問い合わせ下さい。
セキュリティアップデートが適用されるまでは、またサポート終了製品については、影響を受ける製品をそれぞれのネットワークセグメント内の感染したシステム全てから隔離することを推奨します（例えば、ファイアウォールによって上記のネットワークポートへのアクセスをブロックします）。
この脆弱性に対する暫定的な緩和策として、以下を推奨致します。

- 管理されたネットワーク環境には、許可された担当者だけが接続することを確実なものとしていただく。
- 患者の安全と治療がリスクにさらされていない場合は、未感染の製品をネットワークから切り離し、スタンドアロンモードで使用してください。
- 提供されるパッチまたは修正がシステムにインストールされた後でのみ、製品を再接続します。

連絡先

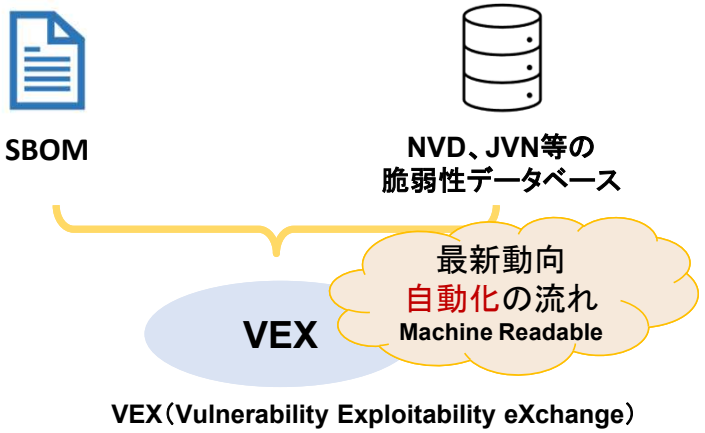
ご質問等に関しましては、サービス窓口までお問い合わせ下さい。
〇〇〇〇〇〇

a) ぜい（脆）弱性の潜在的影響
b) 公知のぜい（脆）弱性
c) ぜい（脆）弱性に対して既知の悪用情報が存在するか

d) 影響を受ける運用中の製品の数量
e) 効果的な補完的対策の利用可能性

対象にあわせた平易な言葉で

脆弱性情報の授受の自動化
Vulnerability-Exploitability eXchange (VEX)
https://www.ntia.gov/files/ntia/publications/vex_one-page_summary.pdf



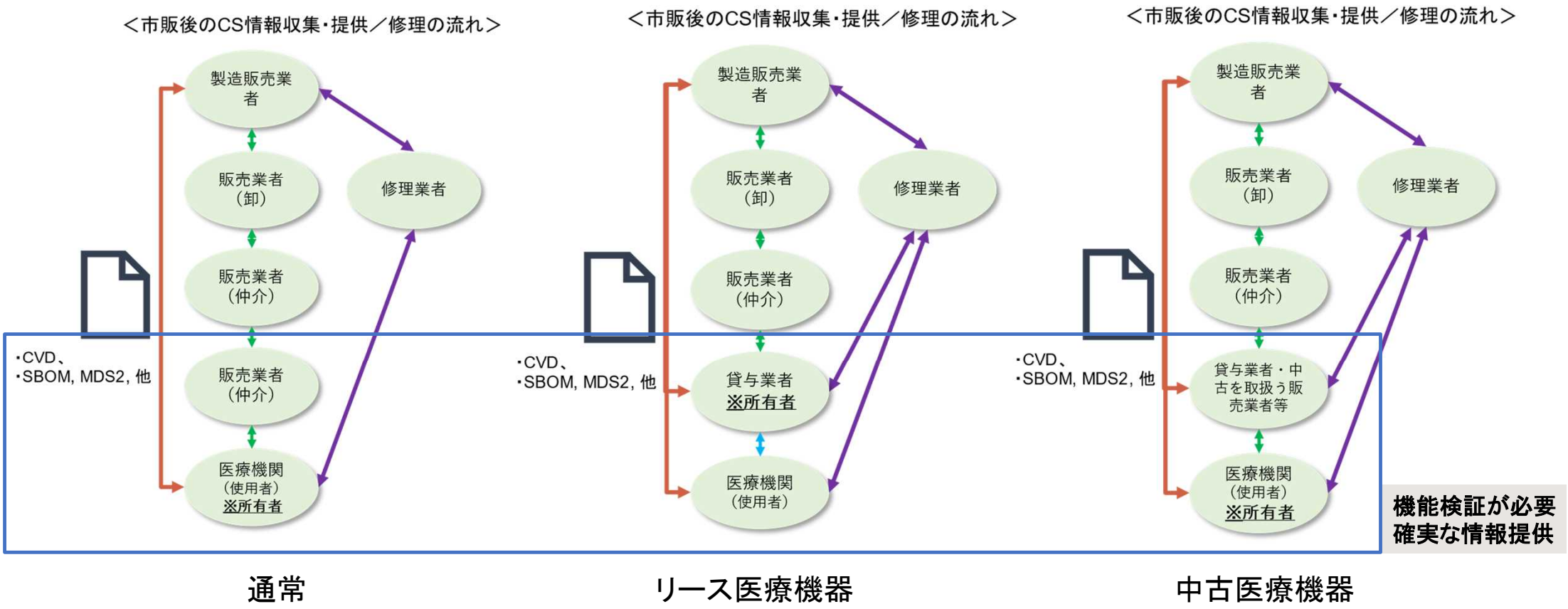
VEX（Vulnerability Exploitability eXchange）

- Not Affected（影響なし）　：修正不要
- Affected（影響あり）　：修正、対応を推奨
- Fixed（修正済み）
- Under Investigation（調査中）

参考：NTIA “Vulnerability-Exploitability eXchange (VEX) – An Overview (2021)”

情報共有の戦略・仕組みの確立

- サイバーセキュリティ対応における各ステークホルダーの連携
  SBOM、脆弱性情報、アドバイザリー等情報の性格上、確実性に加え即時性が必要



令和6年度医療機器製造販売業者のサイバーセキュリティ対策周知事業

■ 医療機器サイバーセキュリティにおける、医療機関との連携に向けた取組と諸課題

1. 医療機器のサイバーセキュリティに関する国内規制の動向

2. 医療機器サイバーセキュリティの実践

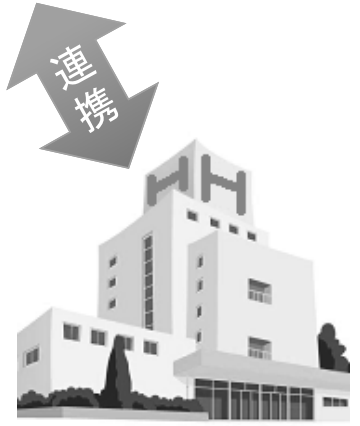
- 医療機器のサイバーセキュリティについて
- サイバーセキュリティに係る規格について（IEC 81001-5-1:2021）
- 医療機器のサイバーセキュリティ要件に対するJIS T 81001-5-1の適用について

3. 医療機関との連携及びPSIRTの実践

4. 「製造業者/サービス事業者による医療情報セキュリティ開示書」の概要

5. ソフトウェア部品表（SBOM）の作成と運用

医療機器
製造販売業者等



医療機関、
医療情報システム製造業者等

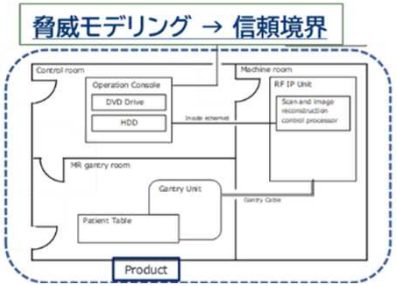
Ministry of Health, Labour and Welfare of Japan

7. まとめ

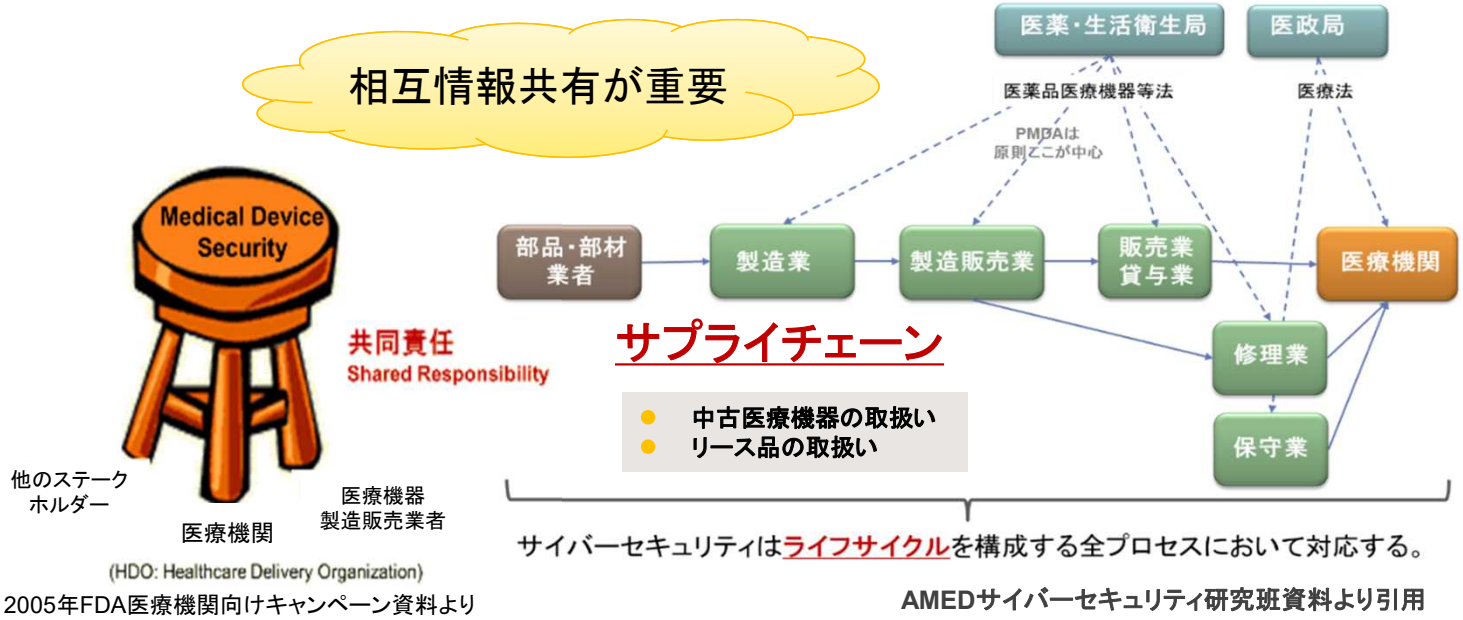
医療機器ソフトウェアのサイバーセキュリティに関連するリスク

- 製造販売業者は、**全ての要求仕様対象ソフトウェアのセキュリティに関連するリスクを特定し、マネジメントするアクティビティを確立**する。

全てのソフトウェア部品（の素性）の明確化 ➡ ソフトウェア部品表（SBOM）

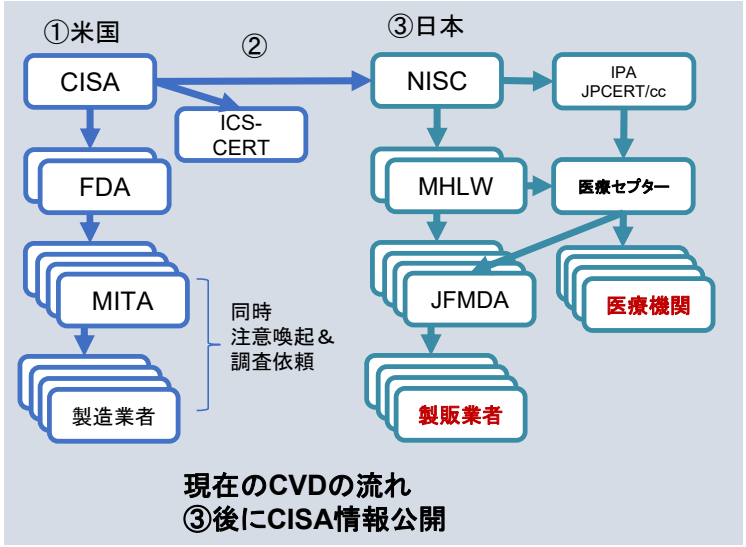


未知の脆弱性を考慮することは難しい　ー 透明性の強化が必要 ー



2005年FDA医療機関向けキャンペーン資料より

AMEDサイバーセキュリティ研究班資料より引用



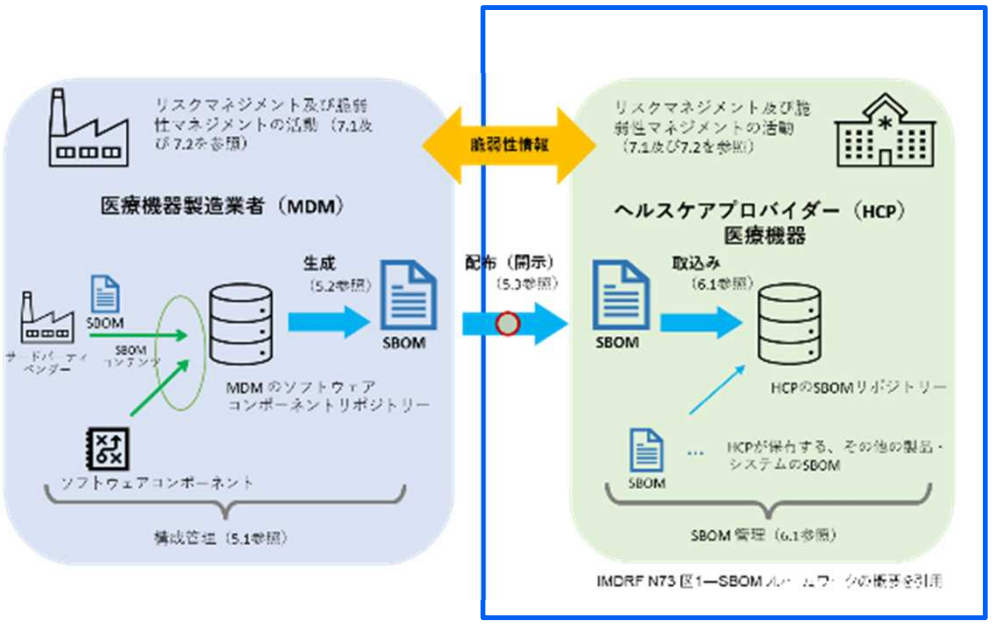
規制当局やISAO/CERTとの連携が重要
IPA、JPCERT/CC、医療セプター（医機連加盟団体経由）

製造販売業者が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（情報の透明性）
  - ソフトウェアの管理強化
  - **セキュリティポリシーの開示**
  - **契約（責任分界（信頼境界）及び役割）**
  - **修理・保守方法の確立**
  - **医療機関との連携及び積極的な情報提供**
- 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（ソフトウェア部品表）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）
    → 網羅性+効率の追求

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

仕組みの構築及び確立



Ministry of Health, Labour and Welfare of Japan

医療機器サイバーセキュリティの実践

ご清聴ありがとうございました。