

SaMD含む医療機器ソフトウェアの サイバーセキュリティ関連規格・規制の動向

※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。
※本資料中では、便宜上JIS規格表記をしている箇所がありますが、必要に応じて対応国際規格に読替えてください。
※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。



2026年2月3日

医機連サイバーセキュリティ対応WG主査

IEC TC62 SC62A/JWG7、MT49 Expert

ISO TC210/JWG1、JWG3 Expert

中里 俊章

重要インフラのひとつである「医療機関」のサイバーセキュリティ確保は、医療情報の信頼性だけでなく、患者安全の向上のため必要であり、このため、この構成要素である「医療機器」のサイバーセキュリティ確保も、確実に実施し、維持しなくてはならない。

1. はじめに
2. 国際規格制定及び規制の動向
3. サイバーセキュリティ対策の基本的考え方
4. まとめ

1. はじめに

◆ ENISA 脅威状況2023, 2024及び2025

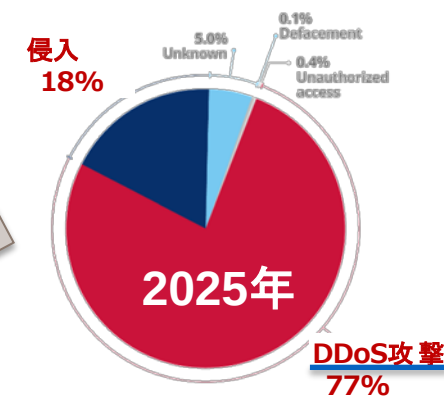
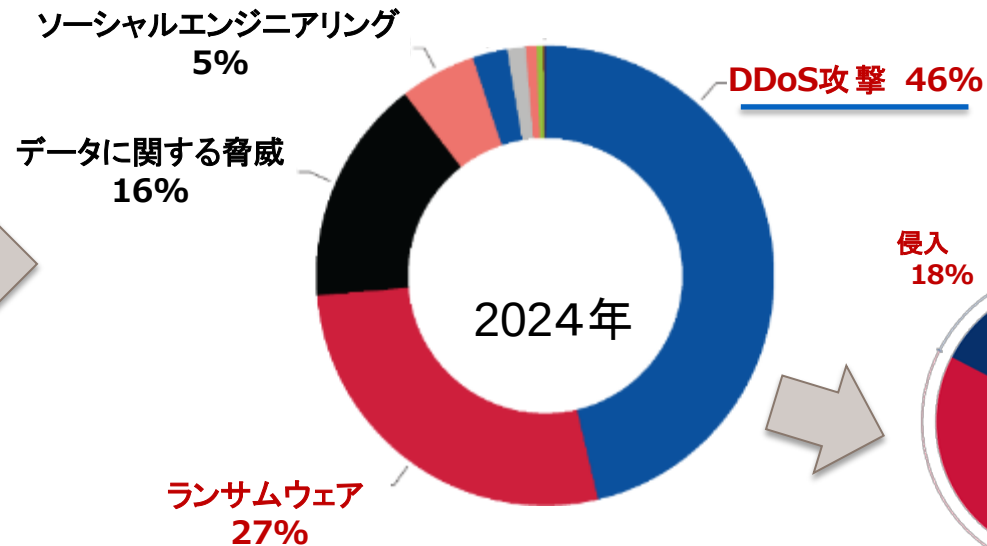
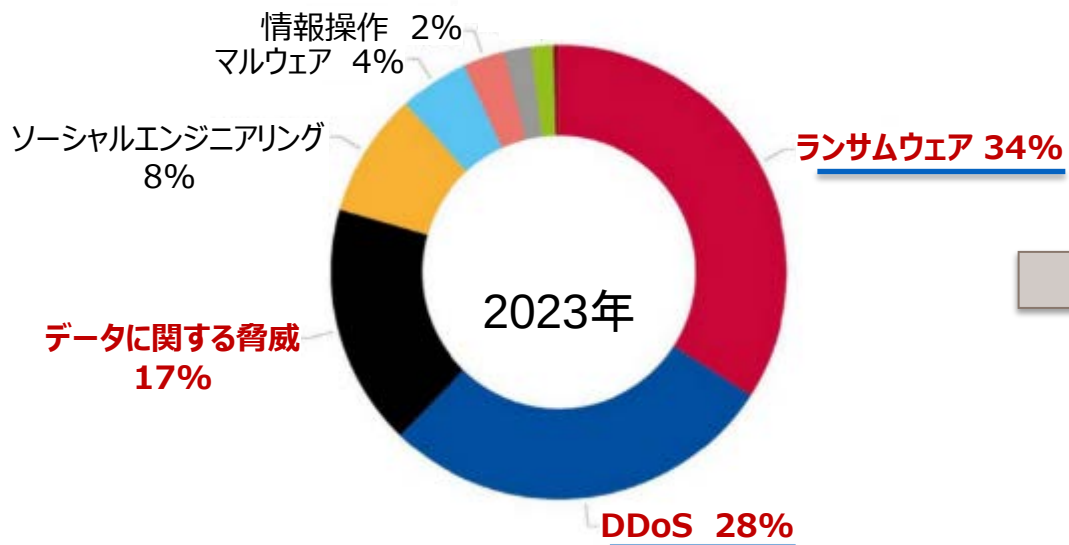
2023: <https://www.enisa.europa.eu/news/eu-elections-at-risk-with-rise-of-ai-enabled-information-manipulation>

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

2025: https://www.enisa.europa.eu/sites/default/files/2025-11/ENISA%20Threat%20Landscape%202025_0.pdf

- 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。
- 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。
- 2024年7月～2025年6月までの期間に発見された脅威について、ENISA Threat Landscape 2025を発行した。

- ① 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。
- ② 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。



- 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。

- 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。

■ 報告書「Update Critical」(WPI StrategyがCiscoの委託を受けて作成)

重要国家インフラ(CNI)におけるサポート終了(End-of-Life: EoL、IMDRFでいうEOS)技術がもたらす、増大し、コストがかさみ、見過ごされがちなサイバーセキュリティリスクに警鐘を鳴らしている。攻撃者は高度な「ゼロデイ」脆弱性を悪用するよりも、パッチが適用されていない、あるいは古すぎてパッチを適用できないネットワーク機器といった単純な手段で侵入することが多いのが実情である。

多くの政府やCNI事業者は、旧式システムの維持にIT予算の大部分を費やしており、これは「技術的負債」として知られている。この負債を返済(修正)するのではなく、利払い(維持)に終始する現在の資金調達モデルは、根本的な脆弱性を放置し、リスクを増大させている。

国	EoLリスクスコア
英国	92.0
米国	88.0
ドイツ	87.8
フランス	83.0
日本	65.0

情報利活用が
進んでいないだけ

脆弱なセクター:
評価対象となった全ての国において、医療セクターが特に脆弱な分野として際立っています。これは、医療システムへのサイバー攻撃がもたらす深刻な影響と、同セクターにおけるEoL技術への高いリスクの露呈を反映しています。例えば、2022年の調査では、フランスの病院の60%が、2020年にセキュリティ更新が終了したWindows 7を使用していた。

1. CNI事業者に対し、EoL技術の管理に関するより積極的な要件を課す必要がある。
2. 旧式技術への資金調達モデルを、技術的負債の「維持」から「修正」へと転換する必要がある。
3. 技術ライフサイクル管理に関するガイダンスをより明確にし、EoLの課題に明示的に取り組むべきである。
4. 脅威と脆弱性への意識と積極的な対応を促すため、情報共有と透明性を向上させるべきである。

■ 医療機器 (SaMDの場合を除き) は、組込み契約に基づくOSを使用

- Microsoftは2023年1月10日、「Windows 7」「Windows 8.1」のサポートを終了
つまり、これらのOSに対するセキュリティ更新プログラムとテクニカルサポートは今後提供されない。
Windows 7のサポートは2020年に終了したが、一部のProfessionalおよびEnterpriseユーザーを対象に拡張セキュリティ更新プログラム (ESU) がサポート終了日から最大3年間提供されていた。同プログラムは、Windows 8.1に対しては提供されない。
<https://japan.zdnet.com/article/35198418/>
<https://msrc-blog.microsoft.com/2016/10/11/more-on-windows-7-and-windows-8-1-servicing-changes/>
- 「Windows 10のサポート終了日は2025年10月14日 (22H2版)」 (汎用PCのOS通常ライセンスの場合: SaMD)
<https://it.impress.co.jp/articles/-/27034>

マイクロソフト製品のサポートライフサイクル

製品名	製品発売日	メインストリーム サポート終了日 (発売日から5年)	延長サポート終了日 (セキュリティパッチ提供終了) (発売日から10年)
Windows 2000 Professional	2000 年 3 月 31 日	2005 年 6 月 30 日	2010 年 7 月 13 日
Windows XP Professional	2001 年 12 月 31 日	2009 年 4 月 14 日	SP2 : 2010 年 7 月 13 日 SP3 : 2014 年 4 月 8 日
Windows 7	2009 年 10 月 22 日	2015 年 1 月 13 日	2020 年 1 月 14 日
Windows 8.1	2013 年 11 月 13 日	2018 年 1 月 9 日	2023 年 1 月 10 日
Windows 10 IoT Enterprise 2015 LTSC	2015 年 7 月 29 日	2020 年 10 月 13 日	2025 年 10 月 14 日
Windows 10 IoT Enterprise 2016 LTSC	2016 年 8 月 2 日	2021 年 10 月 12 日	2026 年 10 月 13 日
Windows 10 IoT Enterprise 2019 LTSC	2018 年 11 月 13 日	2024 年 1 月 9 日	2029 年 1 月 9 日
Windows 10 IoT Enterprise 2021 LTSC	2021 年 11 月 16 日	2027 年 1 月 12 日	2032 年 1 月 13 日
Windows 11 IoT Enterprise 2024 LTSC	2024 年 10 月 1 日	2029 年 10 月 9 日	2034 年 10 月 10 日

ソフトウェア・ライセンスの認識

② レガシー医療機器として、最低限の補完的対策、ネットワーク分離等のリスク軽減策を医療機関に提示する

ESUによってEOS後も有償延長サポート (国際的に影響大)

今回は、ESUなしに即座にサポート打切り

*ESU: Extended Security Updates

① 医療機器の組込ライセンスにおけるWindows10を最新にする、又はWindows11に更新する等の保守計画を立て、医療機関に提示する

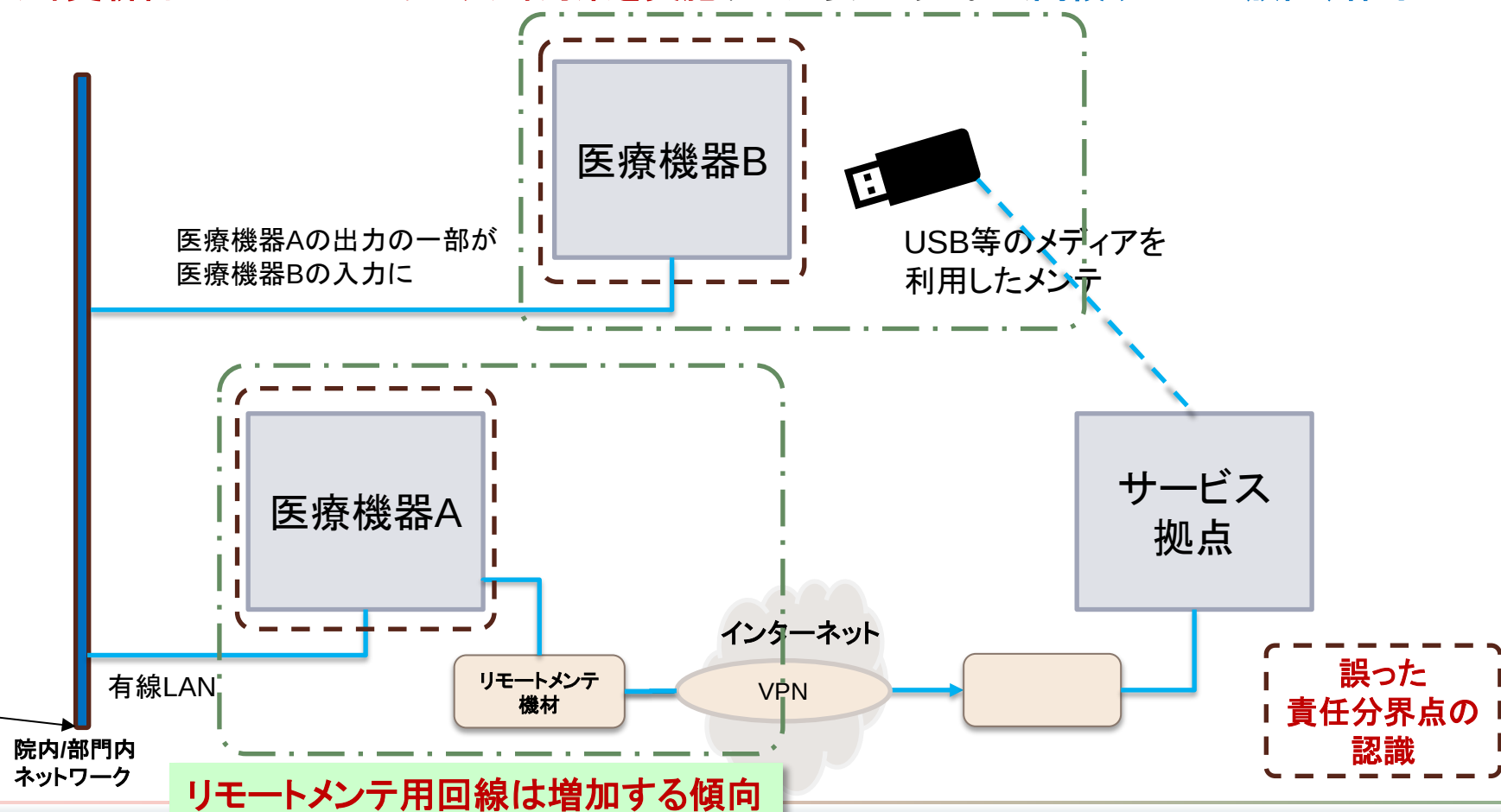
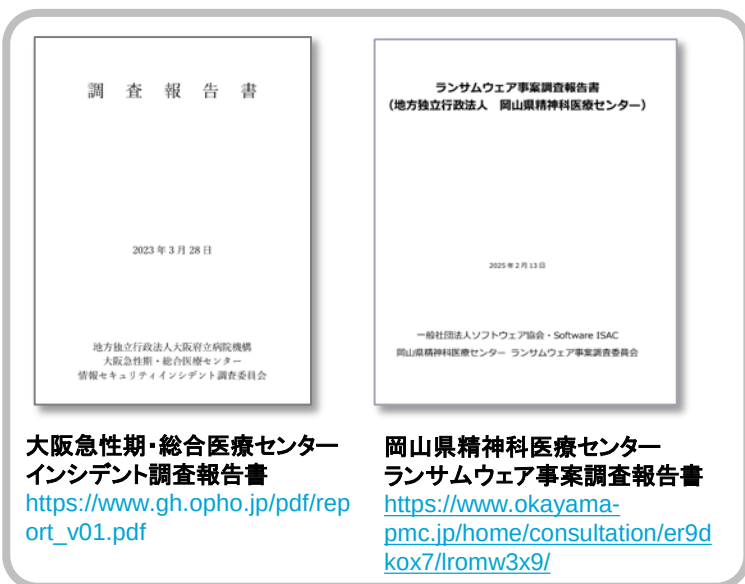
Windowsはマイクロソフトグループ企業の商標です。

医療機器のサイバーセキュリティ対策の実態と課題

製造販売業者の誤った認識
外部接続に関する不備

■ 外部接続(リモートメンテナンス)の管理不備 / 契約に関する諸問題 / 内部のセキュリティが脆弱

- 製造販売業者は、**医療機器の信頼境界(責任分界点)**を契約等により明確にし、**医療機関との責任分担及び作業等の管理を確立**する。**(妥当な契約締結は3%程度)**
- 製造販売業者は、医療機関内に設置する医療機器以外のリモートメンテナンス等のネットワーク機材についても**情報開示し、医療機器同様に遅滞なくセキュリティ更新含むサイバーセキュリティ対策を実施**する必要がある。**(閉領域だから放置、保守不要という誤認識)**

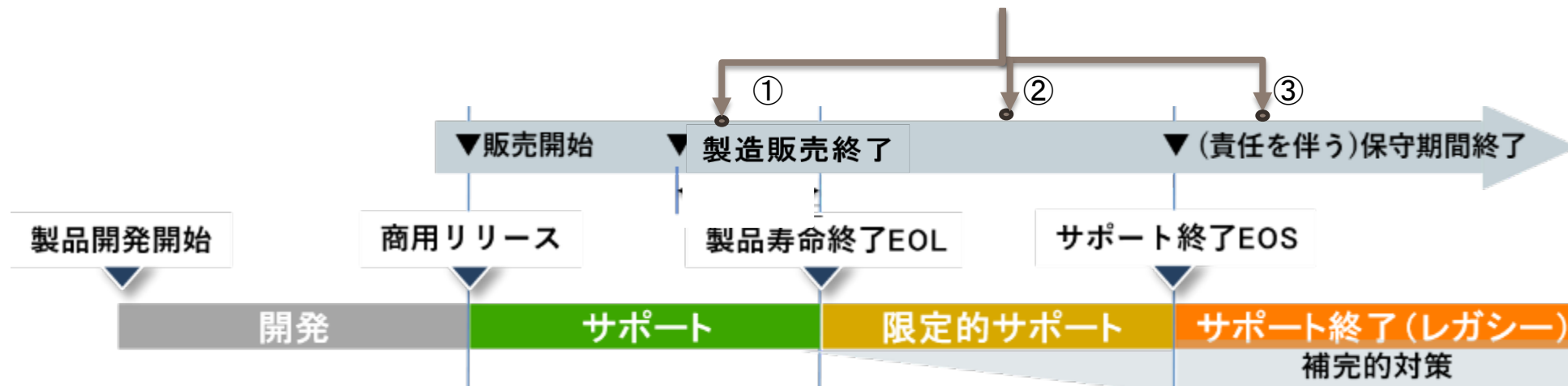


院内/部門内ネットワークは
閉領域でセキュアだとする
誤った認識

- ・ 固定パスワード
- ・ サポート終了した機器の販売
- ・ セキュリティ情報の未提供
- ・ セキュリティ更新の未実装、他

医薬機審発0417 第1号
医薬安発0417 第1号
令和7年4月17日

医療機器のライフサイクル及び現段階の保守計画特定



2024年3月31日

「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
(稼働中の医療機器の80%以上)

医療機器は実使用期間が長いため、
この割合はあまり変化しない

医療機関内の医療機器

医療機器のサイバーセキュリティ対策に関する情報提供について

医薬機審発0417 第1号
医薬安発0417 第1号
令和7年4月17日

「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項の取扱いについては、「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。以下「取扱い通知」)等により示しているところです。

取扱い通知4(1)において、追って通知するとしていた令和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、今般、その一部として、医療機器のサイバーセキュリティ対策の更なる確保に向けた医療機器製造販売業者、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。)の体制確保を円滑に行えるよう、サイバーリスク等に関する情報提供における留意事項を下記のとおりまとめました。

製造販売業者等は、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。以下「法」という。)第68条の2の6第1項に基づき、医療機器の適正な使用のために必要な情報を収集し、及び検討するとともに、これを医療機関等に提供するよう努めなければならないとされていること、法第68条の9第1項に基づき必要な措置を講じなければならないとされていることに加え、法第68条の10第1項に基づき不具合等を厚生労働大臣に報告しなければならないとされているところ、引き続き、本通知における留意事項に基づき、適切な対応を進めるよう、貴管下関係製造販売業者等に対する周知及び体制確保に向けた指導等よろしく願います。

なお、本通知の写しを独立行政法人医薬品医療機器総合機構理事長、一般社団法人日本医療機器産業連合会会長、一般社団法人米国医療機器・IVD工業会会長、欧州ビジネス協会医療機器・IVD委員会委員長、一般社団法人日本臨床検査薬協会会長及び医薬品医療機器等法登録認証機関協議会代表幹事宛て送付することを申し添えます。

医療機器のサイバーセキュリティ対策に関する情報提供について

医薬機審発0417 第1号

医薬安発0417 第1号

令和7年4月17日

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、医療機関等に存在し、「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、及び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、医療機関等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。**なお、サポート終了(EOS)を過ぎたものと製造販売業者等が判断した医療機器については、納入先である医療機関等に対し、既にEOSなどに関する必要な情報提供をしている場合、SBOMの作成及び提示を要しない。
- (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EOSに関する情報を医療機関等に提供していない場合は、医療機器のライフサイクル(①～③)に応じて医療機関等に提供すること。**なお、EOL、EOSを設定する時期については、製品のライフサイクルに応じて各製造販売業者等にて設定されるべきものであるが、**EOL、EOSを設定した場合は適宜、医療機関等へ情報提供を行うこと。**
 - 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、製造販売業者等は、補完的対策等の情報を含め、EOSに関する情報を速やかに提供すること。
- (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)と同様の対応をすること。

- 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)
- 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>



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

「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

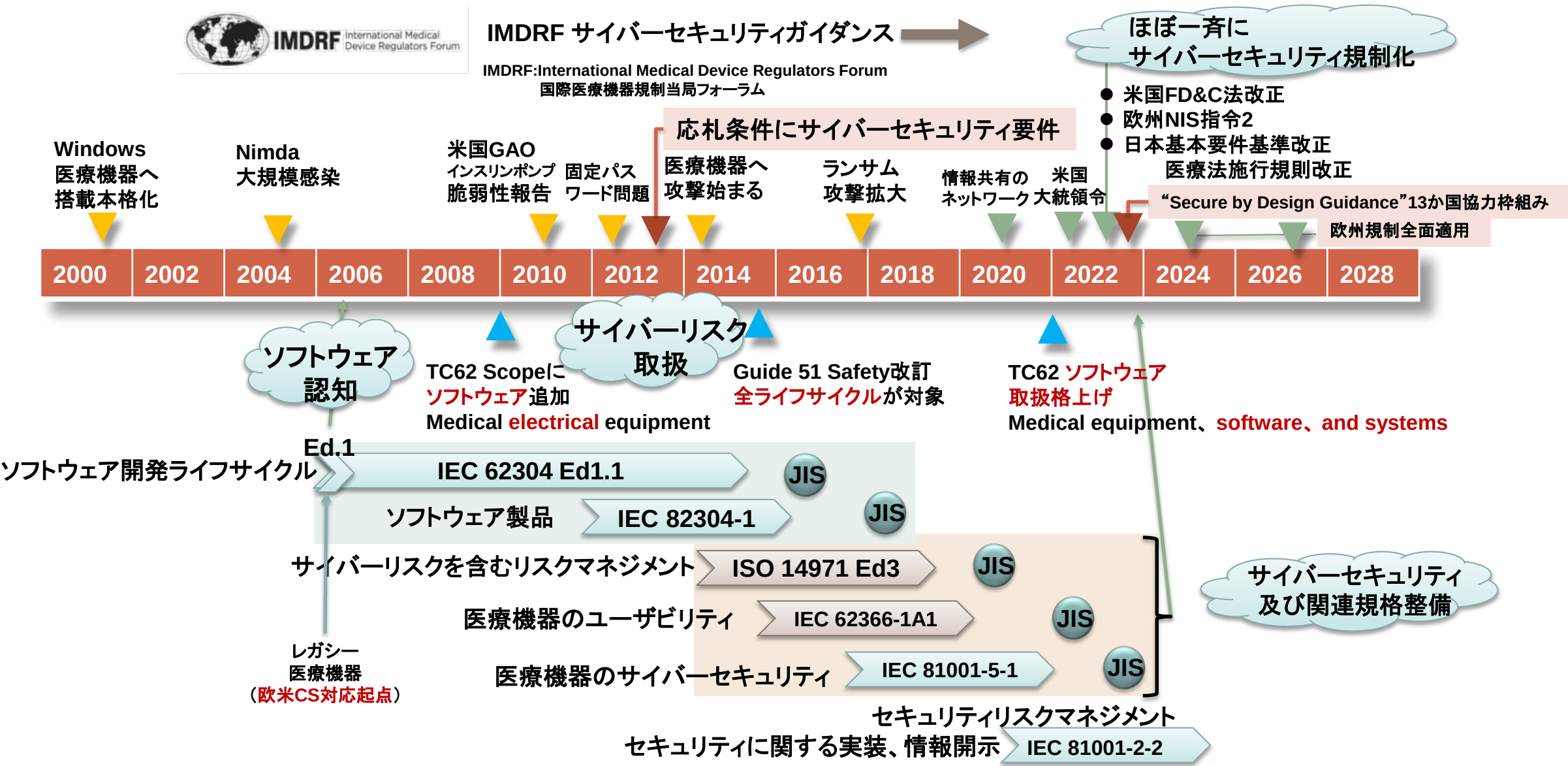
「医療機器のサイバーセキュリティ導入に関する手引書」

- ・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

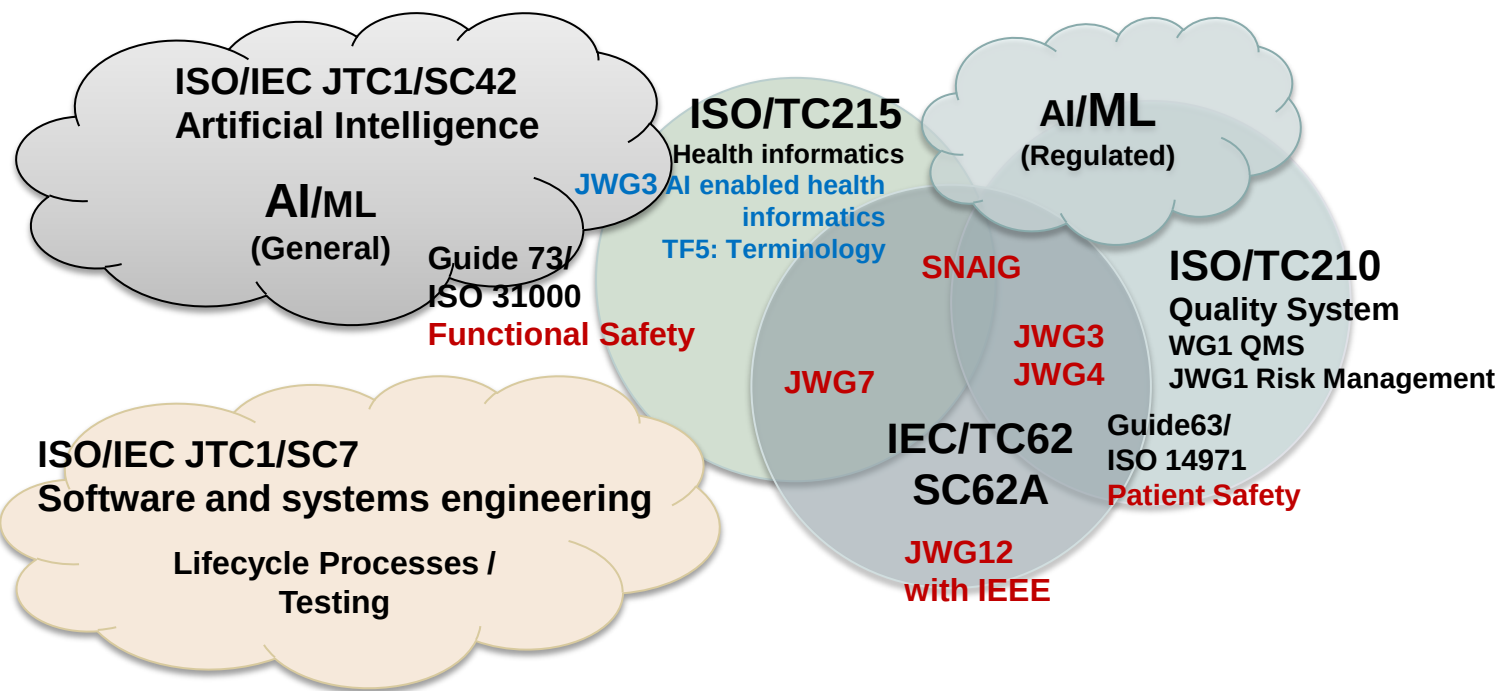
国内
導入へ
2023年

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背景と制度化

実力を問われる規制化
欧州は2006年まで遡って対策



2. 国際規格制定及び規制の動向



IEC TC62 : 医用電気機器、ソフトウェア及びシステム
 SNAIG : ソフトウェア、ネットワーク及び人工知能 (AI) に関する諮問委員会
 JWG12 (IEEEとのジョイント) : 機械学習活用医療機器の市販後監視
 SC62A : 医用電気機器の共通事項 (リスクマネジメント、ユーザビリティエンジニアリング、ソフトウェア等)
 JWG1 (ISO TC210とのジョイント) : 医療機器へのリスクマネジメントの適用
 JWG3 (ISO TC210とのジョイント) : 医療機器ソフトウェアソフトウェアライフサイクル
 JWG4 (ISO TC210とのジョイント) : 医療機器ユーザビリティ
 JWG7 (ISO TC215とのジョイント) : ヘルスソフトウェア

ISO TC210 : 医療機器を含む健康目的の製品の品質管理と関連する一般事項 (ISO 13485, ISO 14971, 他)
 ISO TC215 : 医療情報 Health Informatics (ISO/HL7 27931, ISO 27799, 他)

ISO/IEC JTC1/SC42 : 人工知能
 JWG3 (ISO TC215とのジョイント) : AI活用医療情報
 ISO/IEC JTC1/SC7 : ソフトウェア及びシステムエンジニアリング

■ ヘルスソフトウェアの定義の議論

ヘルスソフトウェア(health software) IEC 880-20-07

次のいずれかであるソフトウェア

- 個人の健康(880-10-05)を管理, 維持若しくは改善するために又はケアを提供するために特に使用することを意図するソフトウェア
- 医用機器(880-09-24)に組み込むことを目的に開発されたソフトウェア
- MES(880-09-27)に組み込むことを目的に開発されたソフトウェア

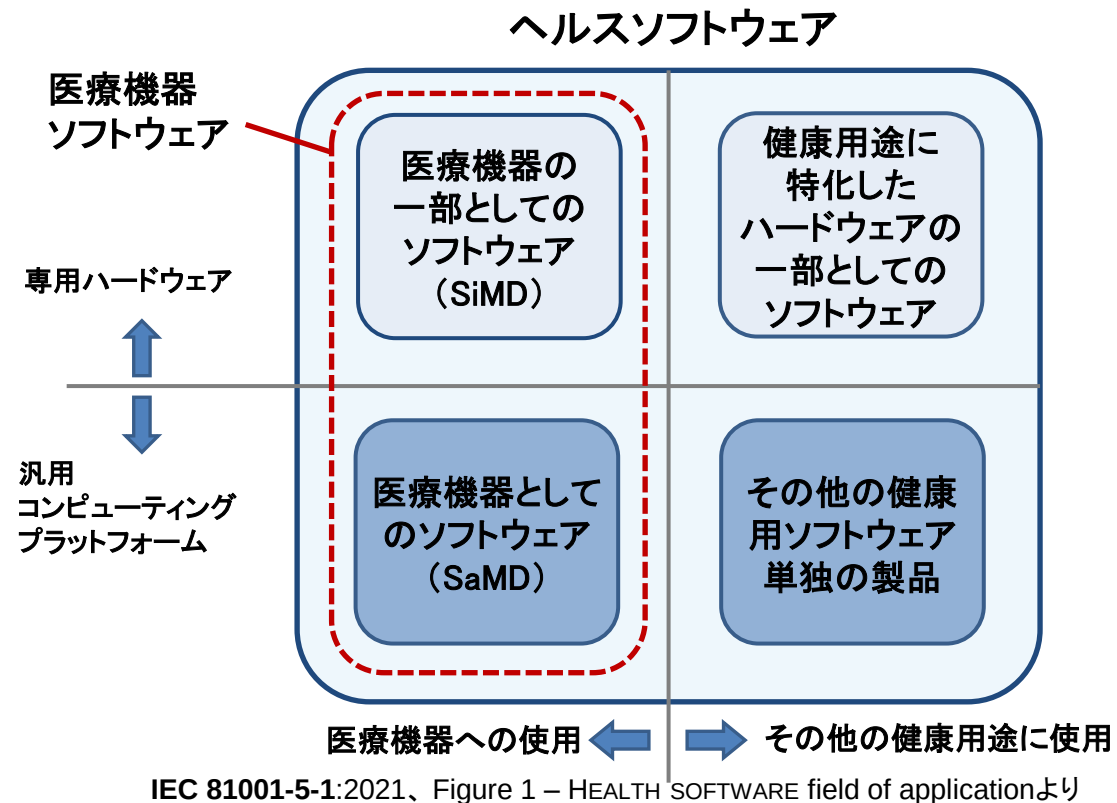
注釈1 ヘルスソフトウェアは, 医療機器ソフトウェアを全て含んでいる。

注釈2 MESに組み込まれるが, その目的で開発されていないソフトウェア [例えば, 商用OTS(off-the-shelf, 既製品)ソフトウェア, すなわちCOTSソフトウェア] は, ヘルスソフトウェアとはみなされない。

(出典: JIS T 81001-1:2022の3.3.9の書式を変更し, 第3項を追加し, 注釈1を置換え, 注釈2を追加)

■ IEC 82304-1改訂に向けて

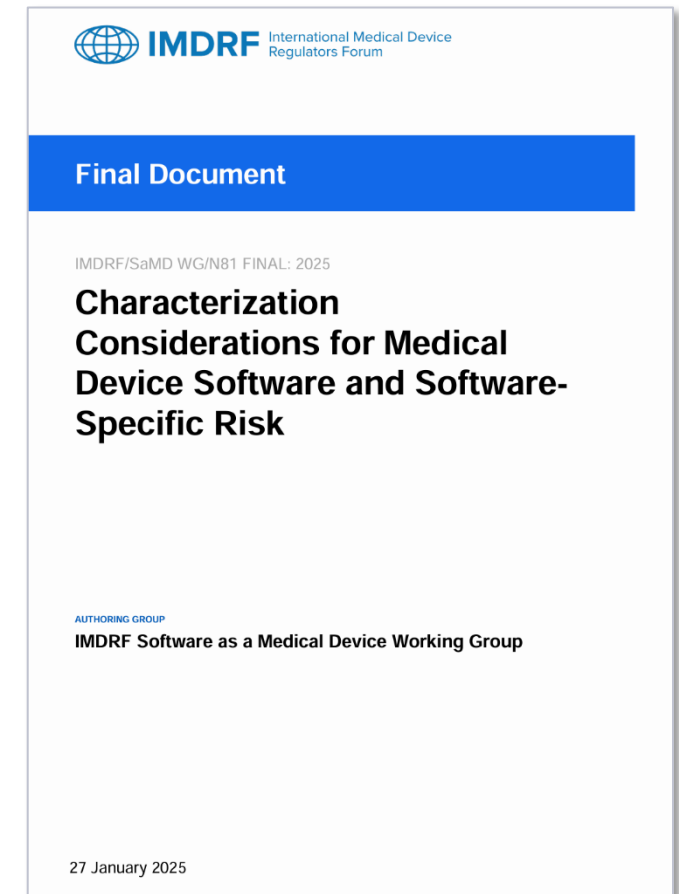
- 製品規格としての要件を規定する。(IEC 62304 Ed.2との関係)
- SaMDに関わる環境は大きく変化している。欧州では、2024年11月から**CRAによりほとんどの機器が規制対象**となる。
- 2026年4月JWG7会議から検討を始める。



MDR及びIVDR製品は、CRAの対象から除外されている。
非医療機器である医療情報システムは、CRA対象であり、
接続して使用される医療機器は、医療機関等からSBOM等の情報提供が求められる可能性が高い。

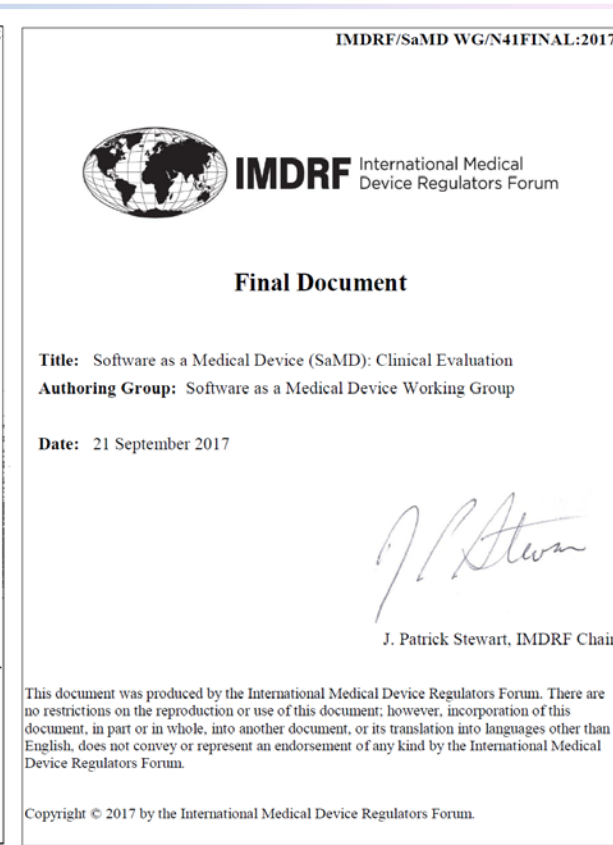
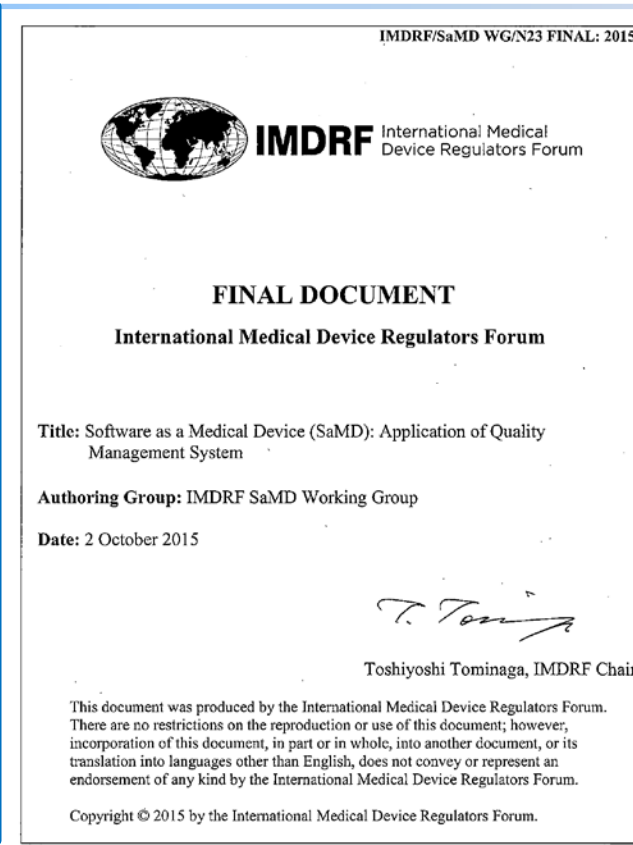
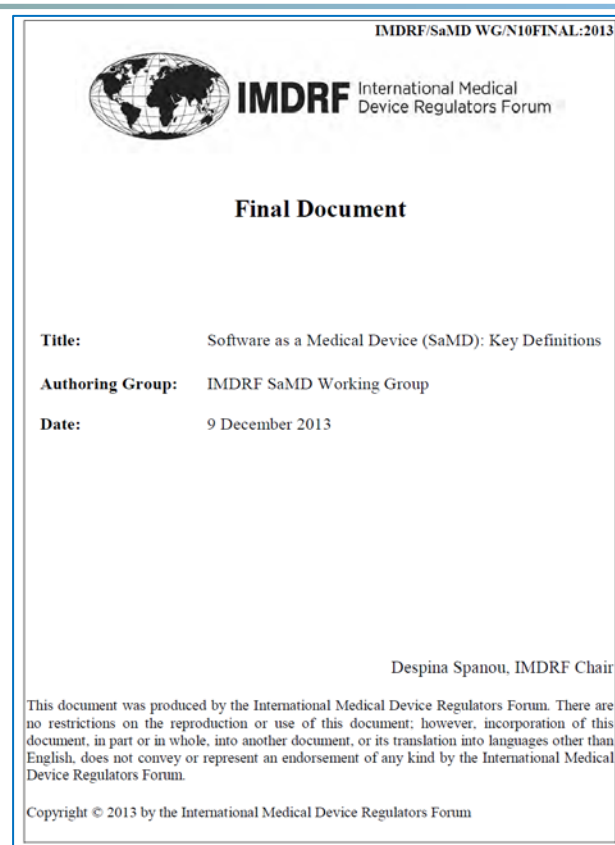
■ IMDRF SaMD-WG

N81: Characterization Considerations for Medical Device Software and Software Specific Risk (米、加共同提案)



https://www.imdrf.org/sites/default/files/2025-01/IMDRF_SaMD%20WG_Software-Specific%20Risk_N81%20Final_0.pdf

IMDRF SaMD-WGの活動



N10 Software as a Medical Device(SaMD): Key Definitions

<https://www.imdrf.org/documents/software-medical-device-samd-key-definitions>

N10 SaMD: 主要な定義 (2013/12/9)

N12 "Software as a Medical Device": Possible Framework for Risk Categorization and Corresponding Considerations

<https://www.imdrf.org/documents/software-medical-device-possible-framework-risk-categorization-and-corresponding-considerations>

N12 SaMD: リスク分類の可能な枠組みと対応する考察事項 (2014/9/18)

N23 Software as a Medical Device (SaMD): Application of Quality Management System

<https://www.imdrf.org/documents/software-medical-device-samd-application-quality-management-system>

N23 SaMD: QMSの適用 (2015/10/2)

N41 Software as a Medical Device (SaMD): Clinical Evaluation

<https://www.imdrf.org/documents/software-medical-device-samd-clinical-evaluation>

N41 SaMD: 臨床評価 (2017/9/12)

■ MDRの規則11aの適用結果として自社製品に適用されるリスククラスについて、EU市場に**医療機器ソフトウェア(MDSW)**を流通させる事業者には有用な目安を提供(説明目的)

SaMDではなく、医療機器ソフトウェアとして扱う方向

ISO 24973(DTx)は、SaMDとして開発をしていたが、CD段階でプロジェクト中断。

MDSWが提供する情報が、診断・治療に関連する医療状況において持つ重要性				
医療状況または患者状態	高	中	低	
	治療または診断 ~IMDRF 5.1.1	臨床管理を推進する ~IMDRF 5.1.2	臨床管理に情報を提供する（その他すべて）	
	緊急事態または患者の状態 ~IMDRF 5.2.1	クラス III カテゴリー IV.i	クラス IIb カテゴリー III.i	クラス IIa カテゴリー II.i
	深刻な状況または患者の状態 ~IMDRF 5.2.2	クラス IIb カテゴリー III. ii	クラス IIa カテゴリー II.ii	クラス IIa カテゴリー I.ii
	軽度な状況または患者の状態（その他すべて）	クラス IIa カテゴリー II.iii	クラス IIa カテゴリー I.iii	クラス IIa カテゴリー I.i

表1：規則11に関する分類ガイダンス

IMDRF N12 7.1 SaMDカテゴリー(オリジナル)

医療場面や病態の現状	医療上の決定に対する SaMD 提供情報の意義		
	治療または診断	臨床管理の運用	臨床管理に関する情報提供
危機的 (Critical)	IV	III	II
深刻 (Serious)	III	II	I
深刻でない (Non-serious)	II	I	I

IMDRF SaMD-WG
N12 Software as a Medical Device: Possible Framework for Risk 13 Categorization and Corresponding Controls 参照
<https://www.imdrf.org/documents/software-medical-device-possible-framework-risk-categorization-and-corresponding-considerations>

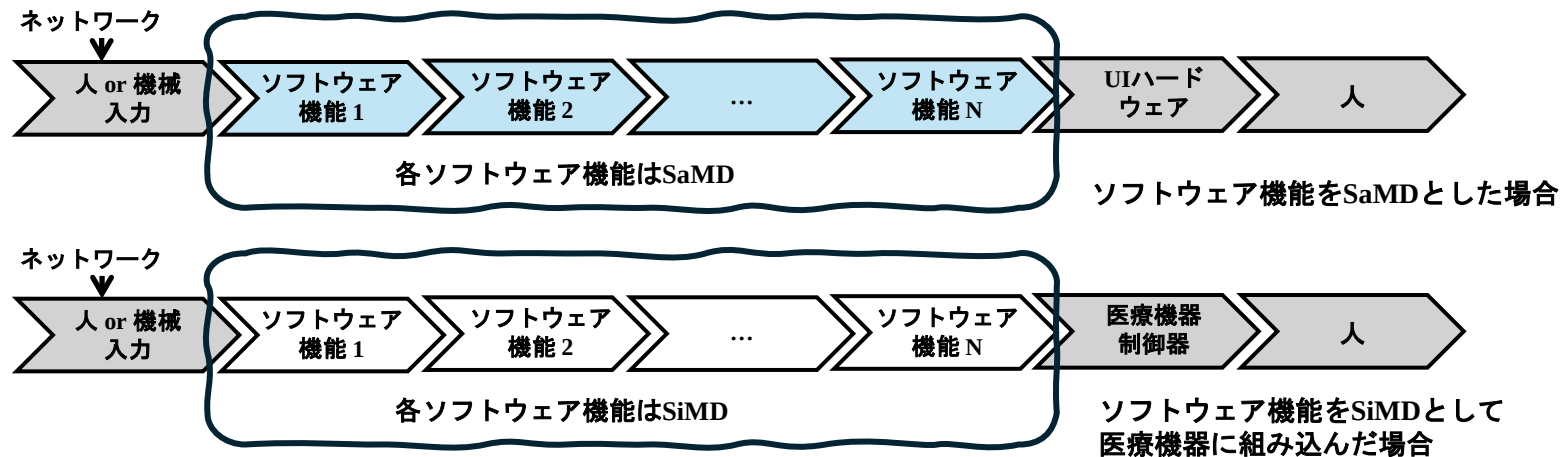
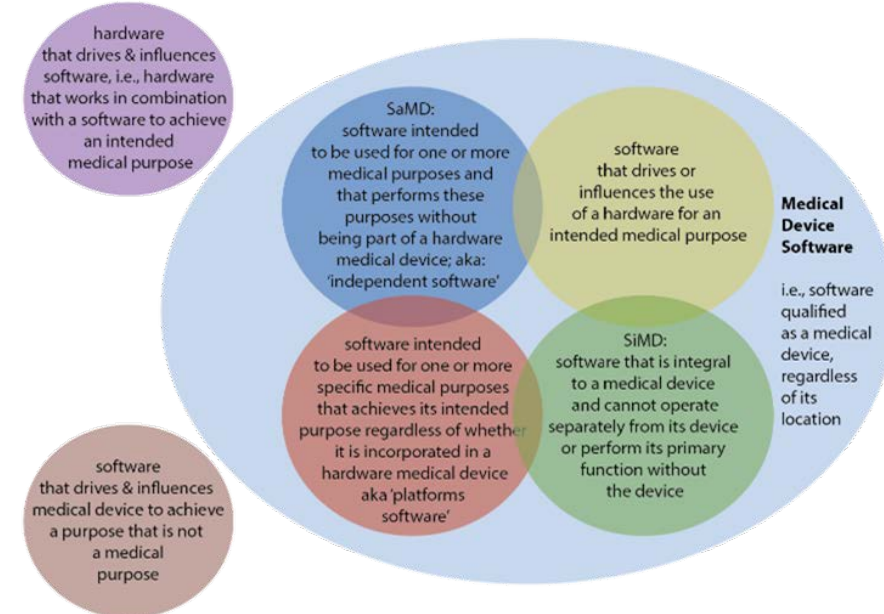
N81 医療機器ソフトウェアおよびソフトウェア固有リスクの特性評価に関する考慮事項

■ SaMDのリスク分類の考え方(N12)について、SaMDに限定せずに検討

医療機器ソフトウェア

- 1つ以上の医療目的の達成に使用するための情報を生成することを意図したソフトウェア
- ハードウェア医療機器の一部であるソフトウェア
- ハードウェア医療機器の一部ではなく、他の医療機器から独立しているソフトウェア)
- ハードウェア医療機器がその意図された使用／目的を達成するために必要なソフトウェア
- 他の医療機器によって駆動又は影響されるソフトウェア
- 人間の使用者、医療機器及び／又は非医療機器向けの出力を有するソフトウェア
- 人間、医療機器及び／又は医療機器ではない製品からの入力を使用するソフトウェア

SaMDにおけるパイプラインの考慮

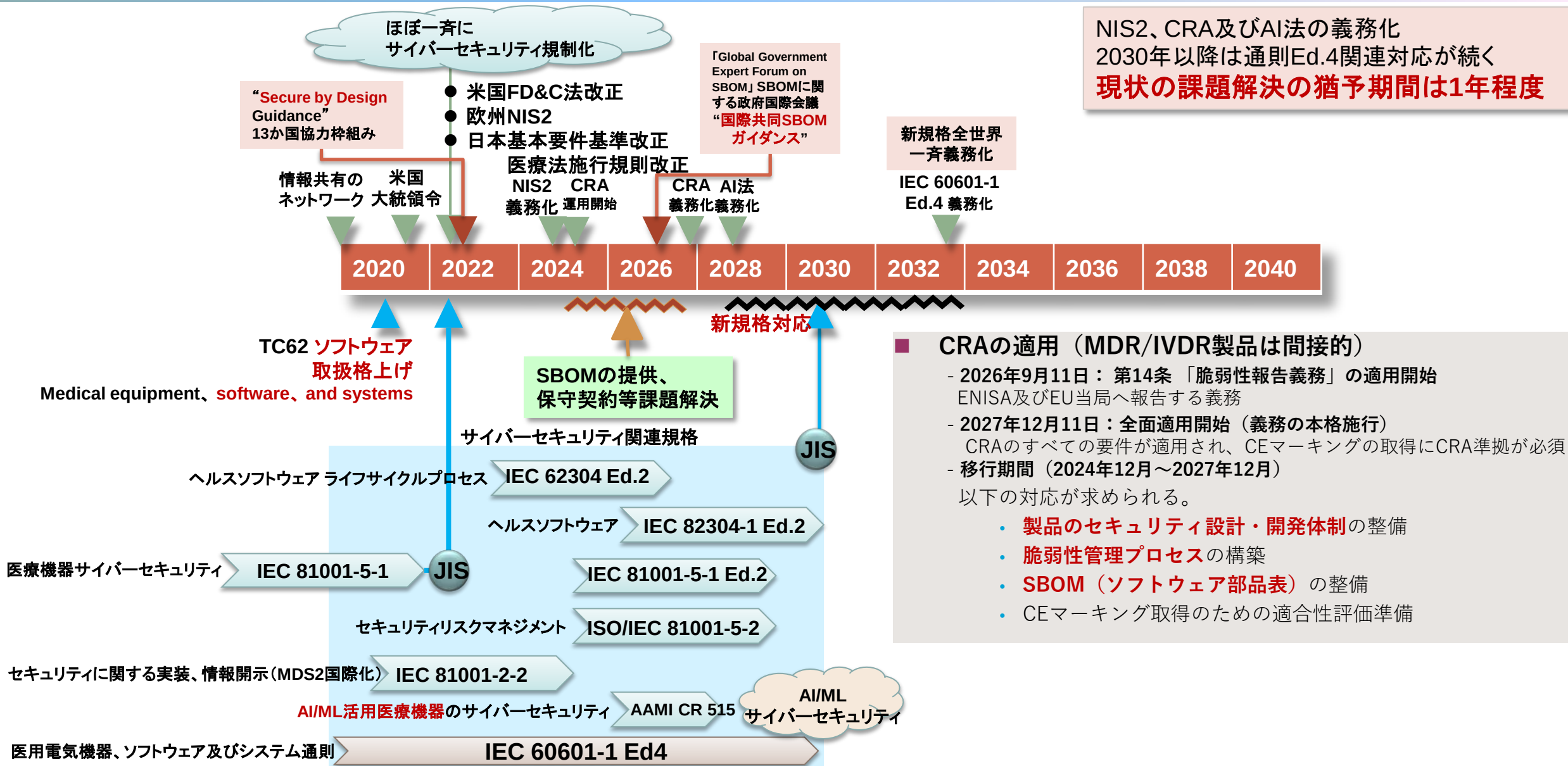


パイプラインの考え方 (IMDRF SaMD-WGでの検討より)

サイバーデバイスの考え方

「インターネットに接続する能力」に関連して、サイバー攻撃がコンポーネントに到達する可能性のある医療機器は「サイバーデバイス」とみなされる。例えば、ネットワークに接続する機能を持たないSaMDがネットワークに接続するプラットフォーム上に存在する場合、パイプラインの考え方により、これらのSaMDもサイバーデバイスとみなされることになる(左図上)。サイバー脅威の「起源」(意図的な攻撃、ユーザーの過失/エラー等)は重要ではない。

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



NIS2指令 改正ネットワーク及び情報システム指令

- 2020年12月、欧州委員会がNIS（ネットワーク情報システム）指令の改正案（NIS2）を発表。
- NIS2での変更点は、①大幅な対象拡大、②サイバーセキュリティ・リスクマネジメントの強化、③インシデント報告内容・時限の明確化、④厳しい罰則金。
- 2022年12月、NIS2指令官報掲載。2024年10月18日より施行。<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555&qid=168413649719>

	NIS	NIS2
スコープ	ヘルスケア、交通、金融、デジタルインフラ、水道、エネルギー、デジタルサービスプロバイダー	＜主要エンティティ＞ エネルギー、運輸、銀行、金融市場インフラ、ヘルスケア、飲料水、下水、デジタルインフラ、ICTサービスマネジメント、公的サービス、宇宙 ＜重要エンティティ＞ 郵便・宅配、廃棄物管理、化学品、食品、製造業（医療機器、コンピュータ・電気電子・光学製品、機械、自動車・トレーラー、輸送機器）、デジタルプロバイダー、研究
要件	・各社のサイバーセキュリティ対策 ・重大事件が起きた際の当局への通報 等	＜リスクマネジメント（21条）＞ ・リスクマネジメント及び情報セキュリティ対策 ・インシデントハンドリング ・ビジネス継続性 ・サプライチェーンセキュリティ ・ネットワークやシステムのセキュリティ ・サイバーセキュリティリスクマネジメントの効率性評価 ・サイバー衛生の実施及びサイバーセキュリティ教育 ・暗号技術の活用 ・アクセスコントロール等の人的セキュリティ ・多要素認証の活用 ＜報告義務（23条）＞ 重大なインシデント（24時間以内に早期警告、72時間以内にインシデント通知、1か月以内の最終報告） ＜その他＞サイバーセキュリティ認証制度（EUCC）の活用等 違反した場合には、売上げの最大2%又は1000万ユーロの罰金
罰則	罰則額は加盟国の裁量	

NIS2
CRA

FDA サイバーセキュリティ市販前ガイダンス改訂最終版 (2025/6/27)

■ 医療機器におけるサイバーセキュリティ: 品質システムに関する考慮事項と市販前申請の内容

- I. 序文
- II. 適用範囲
- III. 背景
- IV. 一般原則
 - A. サイバーセキュリティは、機器安全及び品質システム規則の一部
 - B. セキュリティ設計
 - C. 透明性
 - D. 提出書類
- V. SPDFを使用したサイバーセキュリティリスクの管理
 - A. セキュリティリスクマネジメント
 - 1. 脅威モデリング
 - 2. サイバーセキュリティリスクアセスメント
 - 3. 相互運用性に関する考慮事項
 - 4. サードパーティ・ソフトウェアコンポーネント
 - 5. 未解決異常のセキュリティアセスメント
 - 6. TPLCセキュリティリスクマネジメント
 - B. セキュリティアーキテクチャー
 - 1. セキュリティコントロールの実施
 - 2. セキュリティアーキテクチャーの考え方
 - (a) グローバルシステム
 - (b) 複数の患者への危害
 - (c) 更新可能性及びパッチ可能性
 - (d) セキュリティユースケース
 - C. サイバーセキュリティ試験
- VI. サイバーセキュリティの透明性
 - A. サイバーセキュリティリスクのある機器のラベリング
 - B. サイバーセキュリティマネジメント計画

- VII. サイバーデバイス (524Bに基づく要件)
 - A. FD&C 法第 524B 条に準拠する必要がある者
 - B. FD&C法セクション524Bの対象となるデバイス
 - C. FD&C 法第 524B 条に準拠するための文書化の推奨事項
 - 1. 計画及び手順 (第 524B 条(b)(1))
 - 2. サイバーセキュリティの保証を (第 524B 条(b)(2))
合理的な提供するためのプロセス及び手順の設計、開発及び維持
 - 3. ソフトウェア部品表 (SBOM) (第 524B 条(b)(3))
 - D. 修正
 - 1. サイバーセキュリティに影響を与える可能性のある変更
 - 2. サイバーセキュリティに影響を与える可能性の低い変更
 - E. サイバー機器のサイバーセキュリティの合理的保証

附属書1. セキュリティコントロール区分と関連する推奨事項

- A. 認証
- B. 認可
- C. 暗号
- D. コード、データ及び実行の完全性
- E. 秘密保持
- F. イベント検出及びロギング
- G. 回復力
- H. ファームウェアとソフトウェア更新

附属書2. セキュリティ・アーキテクチャー・フローの提出文書

- A. ダイアグラム
- B. アーキテクチャビューの情報の詳細

附属書3. 治験機器申請のための提出書類

附属書4. 一般的な市販前申請文書の要素とリスクに応じた対応

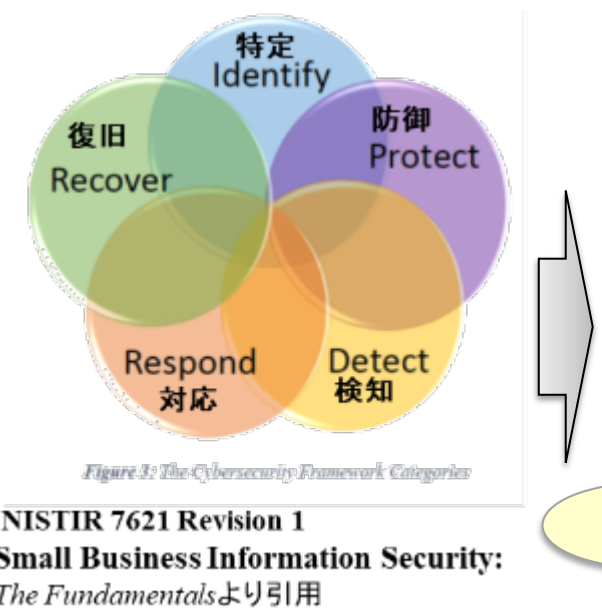
附属書4. 用語

<https://www.fda.gov/media/119933/download>

V. SPDFを使用したサイバーセキュリティリスクの管理

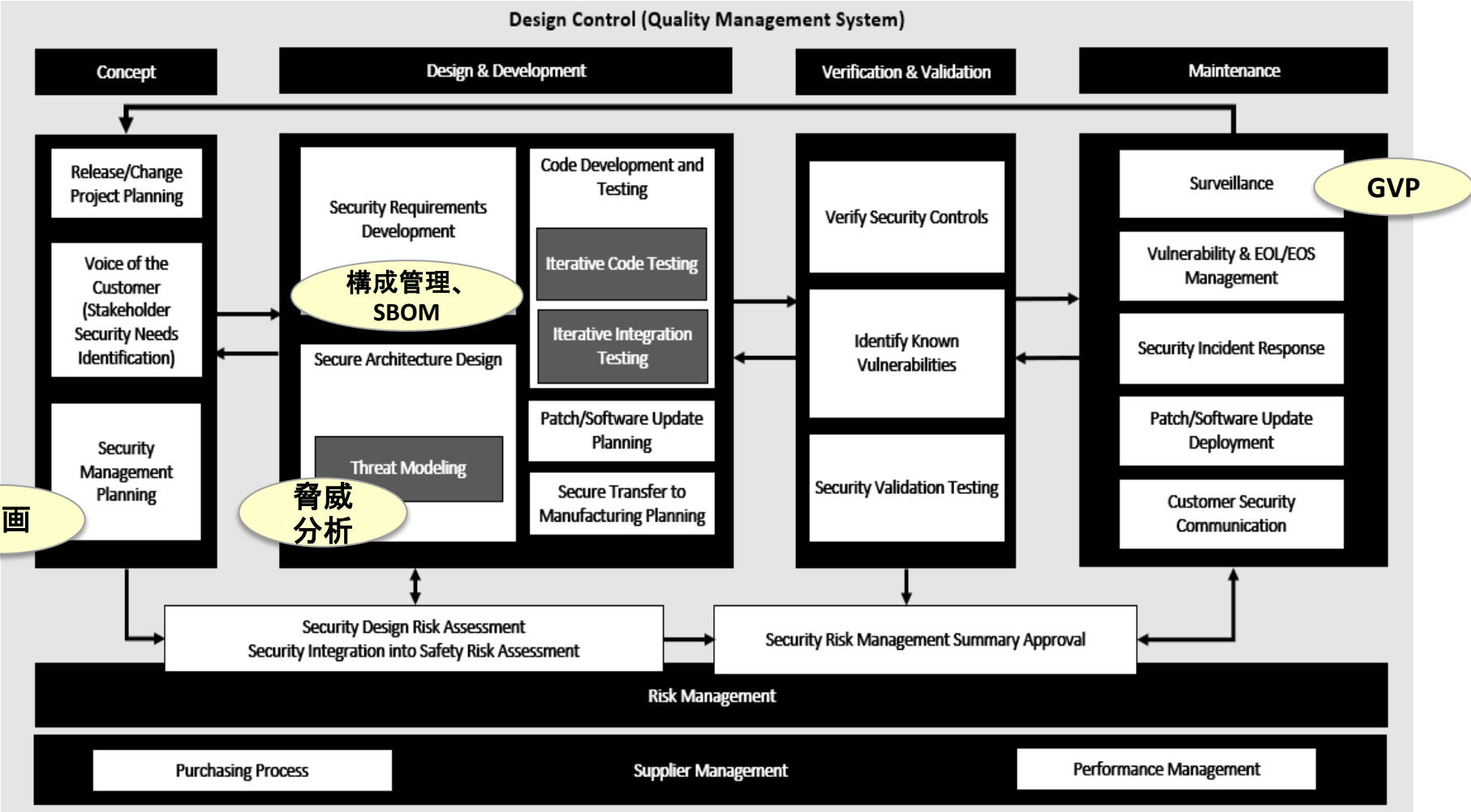
■ セキュリティ対応フレームワーク（JSP V2）

SPDF:セキュア製品開発フレームワーク



リスクコントロール策のベース

NIST SP-800 53B Revision 5
組織と情報システムのための
セキュリティ及びプライバシー管理策



出典: MEDICAL TECHNOLOGY AND HEALTH IT JOINT SECURITY PLAN V2
<https://healthsectorcouncil.org/wp-content/uploads/2024/03/Medical-Technology-and-Health-IT-Joint-Security-Plan-v2.pdf>

■ VII. サイバーデバイス (FD&C法第524B条による)

ネットワークの物理的接続手段に寄らない

A. FD&C法第524B条に準拠する必要がある者

FD&C法第524B条(a)に基づき製造業者を含む者は、524B条(c)に定義される「サイバーデバイス」の定義を満たすデバイスについて、510(k)、PMA、PDP、De Novo、又はHDEのいずれかの経路で**市販前申請又は提出を行う場合、サイバーデバイスが524B条(b)に基づくサイバーセキュリティ要件を満たすことを保証するためにFDAが要求する情報を含める必要がある。**

B. FD&C法第524B条の対象となるデバイス

FD&C法第524B条とその要件は、“サイバーデバイス”に適用される。FD&C法第524B条(c)は、“サイバーデバイス”を、以下の基準をすべて満たすデバイスと定義している。“(1)デバイスとして、又はデバイス内に、スポンサーによって検証、インストール、又は認可されたソフトウェアを含む、(2)インターネットに接続する機能を有する、(3)スポンサーによって検証、インストール、又は認可された、サイバーセキュリティの脅威に脆弱である可能性のあるそのような技術的特性を含む”。

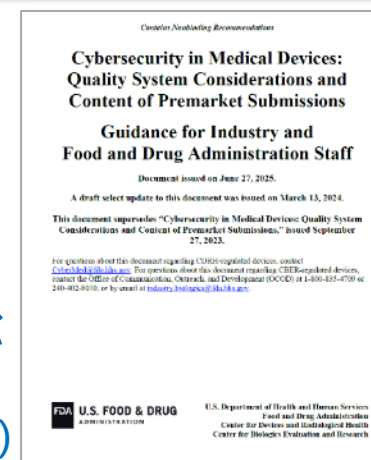
FDAはまた、「インターネットに接続する能力」を、**意図的であるか否かにかかわらず、あらゆる手段(機器の脅威面および使用環境の評価で特定されたあらゆる時点を含む)を通じてインターネットに接続できる機器を含むもの**と考えている。デバイスに以下の能力があることは、十分に実証されている。

インターネットに接続する場合、そのような接続が機器スポンサーによって意図されたかどうかにかかわらず、インターネットに接続できる可能性がある。

FDAは、以下のいずれかの機能を含む機器を、インターネットに接続する能力を有するとみなしている。以下のリストは例示であり、網羅的なものではない:

- ネットワーク、サーバー又はクラウドサービスプロバイダーとの接続
- 無線周波数通信(Wi-Fi、携帯電話、Bluetooth、Bluetooth Low Energyなど)
- 磁気誘導通信
- インターネットに接続可能なハードウェアコネクタ(USB、イーサネット、**シリアルポート**等)

<https://www.fda.gov/media/119933/download>



■ FDA ホワイトペーパー 医療製品製造に使用される技術と設備のセキュリティ確保(OT技術) QMSソフトウェアのセキュリティ

保健福祉省とFDAは、医療製品、米国の医療インフラ、公衆衛生のサプライチェーン全般(製造と出荷を含む)のサイバーセキュリティに特に力を入れている。

製造インフラは、コネクテッド・デバイス、モノのインターネット(IoT)、スマート・テクノロジーがユビキタスになっているため、特に脆弱になりやすい。**これらのコネクテッド・テクノロジーはオペレーショナル・テクノロジー(OT)と呼ばれ、これまでサイバーセキュリティよりも一貫した機能を優先するように設計されてきた。**

その結果、いつ、どこで、どのような通信が行われているのかを把握することが難しくなり、サイバーセキュリティ・インシデントのリスクが高まる可能性がある。



標準技術局(NIST)の連邦情報製品規格(FIPS)、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・エージェンシー(CISA)のガイドラインには、厳格なネットワーク・ルーティング要件等が規定されているが、**残念ながら、多くの市販(COTS)製品は、これらのセキュリティ要件にネイティブに準拠しておらず、再構成が必要な場合がある。**これらのガイドラインが業界の標準的な慣行となるまでは、多くの OT構成にかなりの脆弱性が内在する可能性がある。

FDAの最近の経験は、ネットワーク対応技術やスマート運用技術を導入し、安全性を確保する際の潜在的な考慮事項、脆弱性、リスクを特定する機会となる。これらの考慮事項は3つのカテゴリー(技術的情報交換、セキュリティ標準とコンプライアンス、セキュリティ・バイ・デザイン)に分類される。

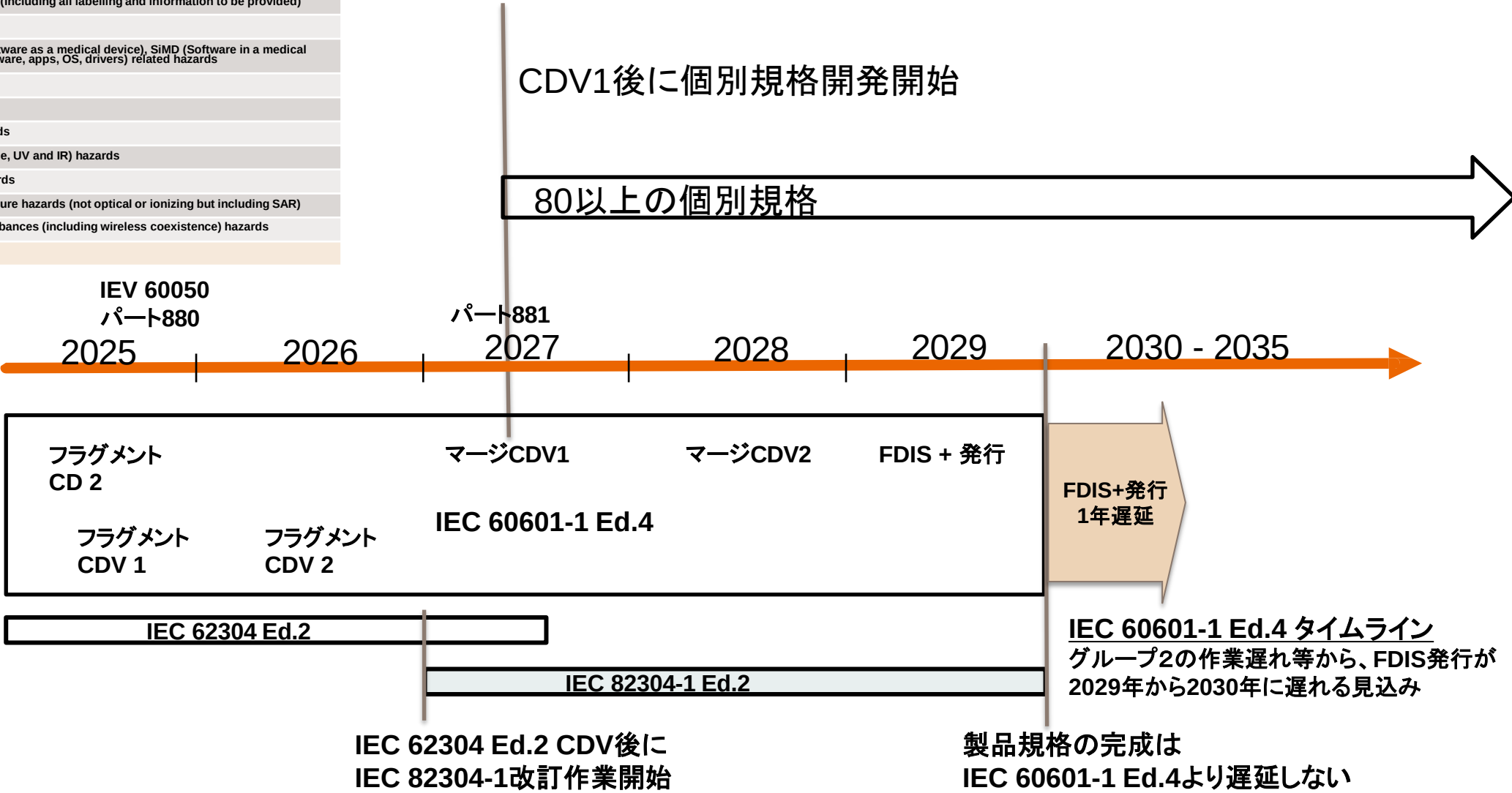
使いやすい運用環境の構築と、可能な限り多くの脅威に対する運用の安全性確保との間で、バランスを取る必要がある。セキュリティと使いやすさのどちらかを重視しすぎると、公衆衛生、患者の治療へのアクセス、最先端製品の利用可能性、パンデミック対策に深刻な影響を及ぼす可能性がある。品質保証プログラムと同じように、**強力なサイバーセキュリティ・プロセスは、「安全で、効果的で、信頼できる医療製品の生産」の課題を解決するための支柱の一つ**である。

<https://www.fda.gov/media/187159/download>

IEC 60601-1 Ed.4に関連する規格のタイムライン 2025

WG	フラグメント	タイトル
WG 37	Frag.1	General requirements
WG 38	Frag.2	Physical environment hazards
WG 39	Frag.3	User interface aspects (including all labelling and information to be provided)
WG 40	Frag.4	Materials hazards
WG 41	Frag.5	PEMS (e.g., SaMD (Software as a medical device), SIMD (Software in a medical device), firmware, Software, apps, OS, drivers) related hazards
WG 42	Frag.6	Electrical hazards
WG 43	Frag.7	Mechanical hazards
WG 44	Frag.8	Thermal and fire hazards
WG 45	Frag.9	Optical radiation (visible, UV and IR) hazards
WG 46	Frag.10	Ionizing radiation hazards
WG 47	Frag.11	Electromagnetic exposure hazards (not optical or ionizing but including SAR)
WG 48	Frag.12	Electromagnetic disturbances (including wireless coexistence) hazards
MT49		IEC 62304 Ed.2

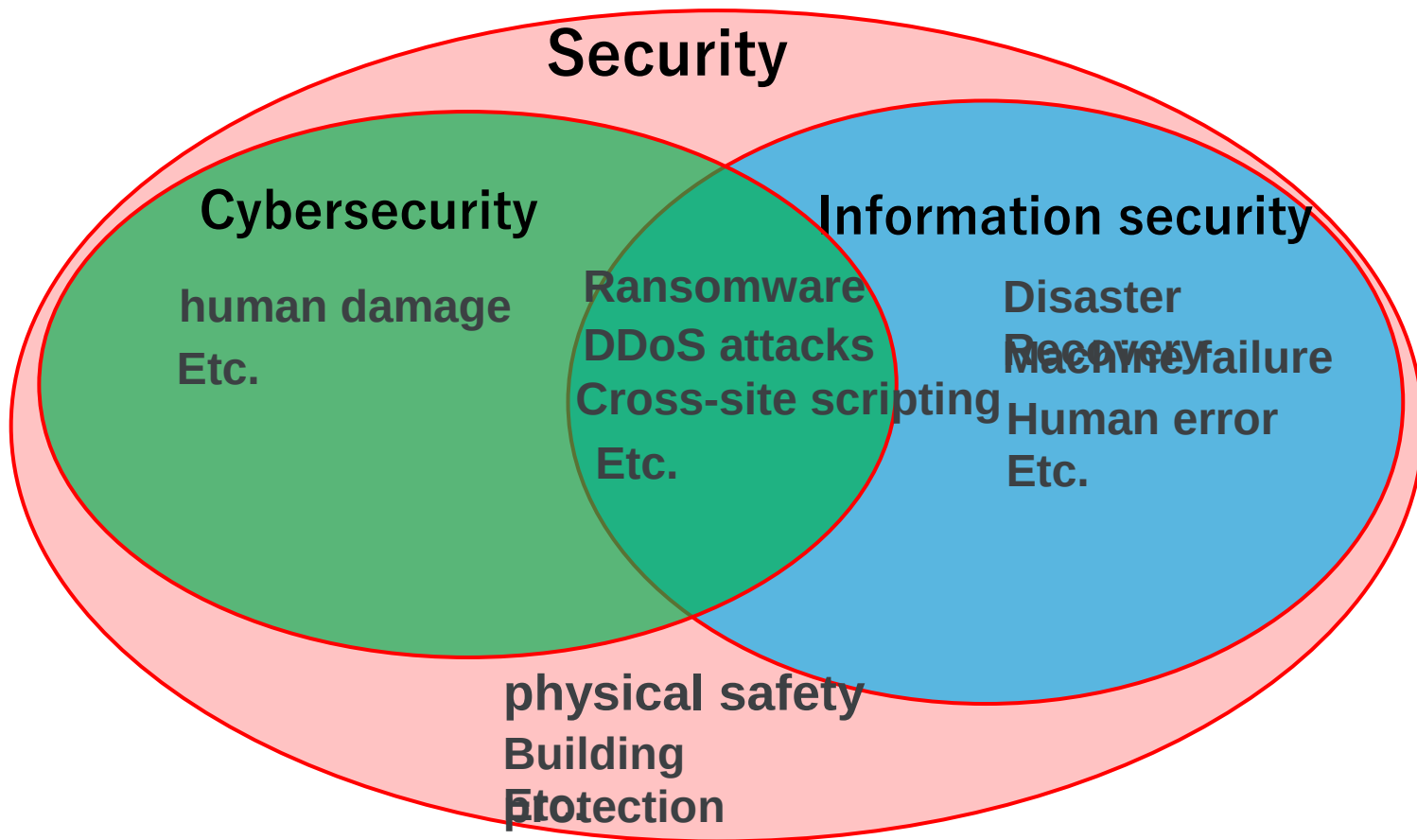
12WGで活動
Group1: Frag 1,2,3,4,11
Group2: Frag 5,6,7,8,9,10,12
MT49: IEC 62304 Ed.2



用語“security”, “information security”, “cybersecurity”の関係 (ISO TC215)

■ ISO 81001-1における定義とその背景(ISO TC215)

Security/Cybersecurity – state where information and systems are protected from unauthorized activities, such as access, use, disclosure, disruption, modification, or destruction to a degree that the risks related to violation of confidentiality, integrity, and availability are maintained at an acceptable level throughout the life cycle



“サイバーセキュリティ”の定義

Security is defined in IEC Guide 120

Security is the collection of physical, technical and organizational measures to protect assets in the electrotechnical domain — including equipment, systems, services, information and operational procedures, and people — from threats and risks so as to maintain their functionality, safety, reliability, availability, integrity and confidentiality

Information security is defined in ISO/IEC 27000

information security
Preservation of *confidentiality*, *integrity* and *availability* of information
Note 1 to entry: In addition, other properties, such as *authenticity*, *accountability*, *non-repudiation*, and *reliability* can also be involved.

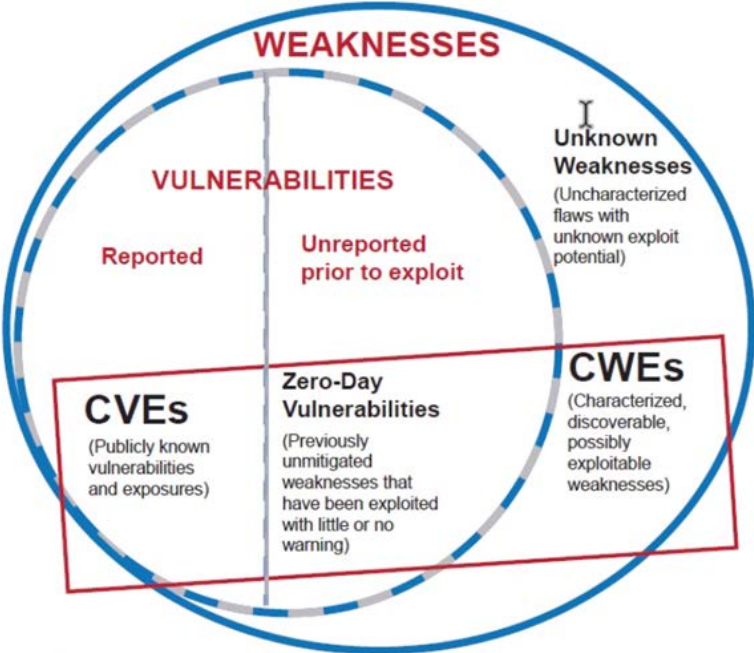
ISMS適合

Cybersecurity is defined in ISO/IEC TS 27100

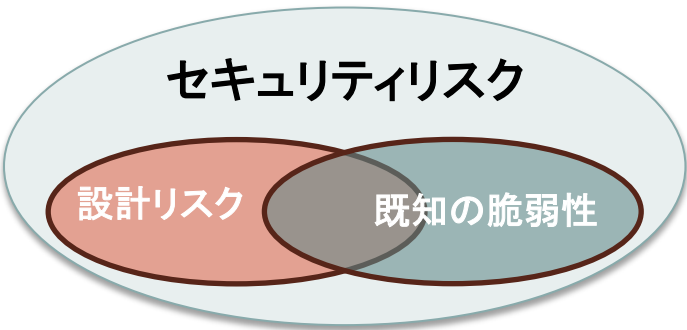
cybersecurity
safeguarding of people, society, organizations and nations from cyber *risks*
Note 1 to entry: Safeguarding means to keep cyber risks at a tolerable level.

- 脅威モデリング
脅威モデリング関連をプロセス要求事項として含める。
国際的に利用されているSTRIDE 等の脅威モデリングを
ベースに攻撃パターン(ベクトル)、CWE(弱み)、事例等を
基に設計及び市販後監視に関する要求事項をまとめる。
脅威分析に関する部分はAnnexで解説を加える。

Figure A1
Weaknesses and Vulnerabilities

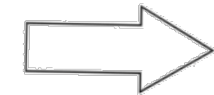


su4668



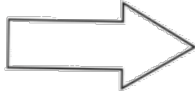
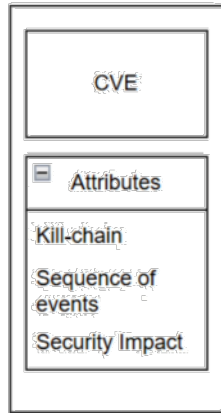
セキュリティリスク関連図

Weaknesses (弱み)



Weaknesses in code can be caused by many different elements. These are security/safety agnostic currently.

Vulnerabilities (脆弱性)



Given a sequence of events, a security impact is proven to make a weakness vulnerable to security attacks. This asserts the security context for a weakness.

Exploits (悪用)



From analysis an exploit is found to be present in a product. This means that the deployment environment has been proven to be exploitable using the vulnerability sequence. The exploit is evaluated with company specific context for its impact rating on an asset, along with an exploitability rating, providing a risk.

(参考) サイバーセキュリティに関するリスク評価の手順 - 脅威分析

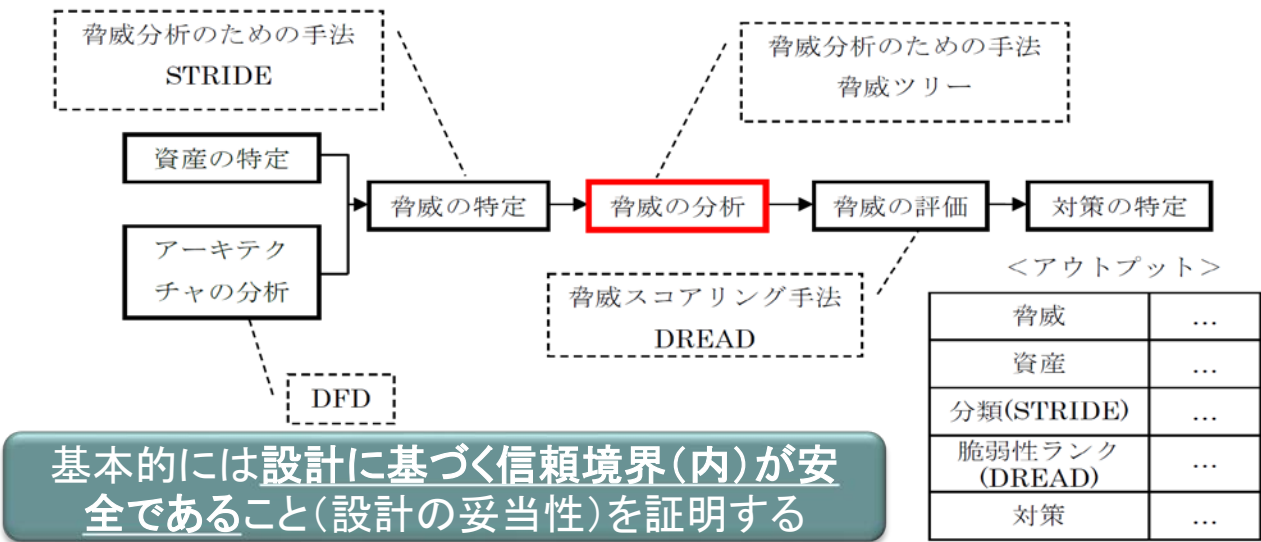
■ 一般的なリスク評価手順とFDA市販前ガイダンスの推奨

- 1. 資産の特定
- 2. アーキテクチャの分析
- 3. 脅威の特定
- 4. 脅威の分析
- 5. 脅威の評価
- 6. 対策の特定

- 1. 資産、脅威、脆弱性の特定
- 2. 機器の機能及びエンドユーザ／患者に対する脅威や脆弱性の影響評価
- 3. 悪用可能性のある脅威や脆弱性が発生する可能性の評価
- 4. リスクレベルと適切な低減戦略の決定
- 5. 残存リスクとリスク受容基準の評価

FDA市販前ガイダンス(V.A.1.)では、脅威モデリングには幾つかの手法及び／又は手法の組み合わせがあり、製造業者はそれらを選択できると説明している。また、選んだ手法について、製造業者が根拠を脅威モデリングの文書に含めるように求めている。

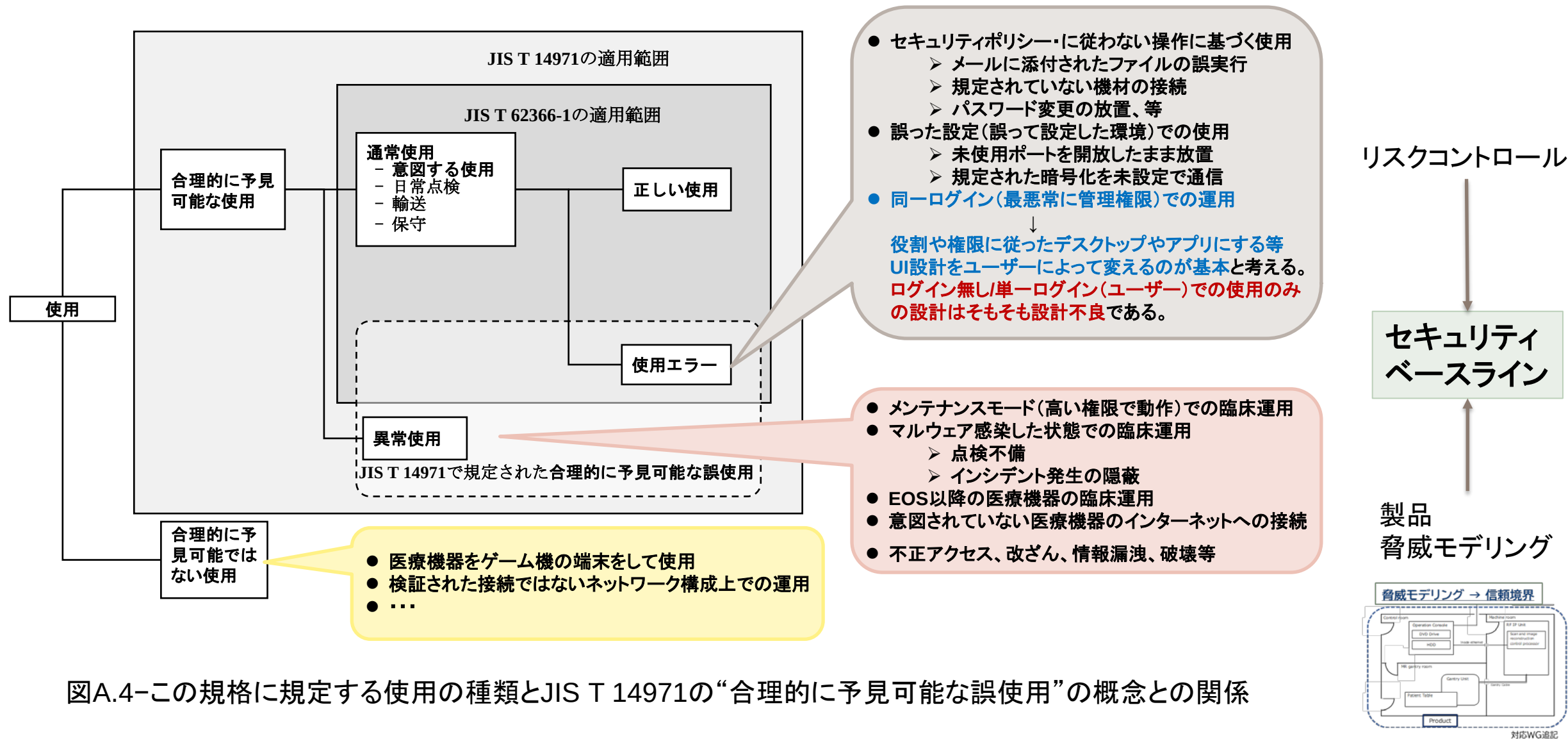
■ 一般的なサイバーセキュリティに関するリスク評価の手順の例



STRIDE の脅威例	脅威	脅威例
	Spoofing (なりすまし)	正規ユーザのなりすまし
	Tampering (改ざん)	データの改変
	Repudiation (否認)	ログの消去
	Information Disclosure (情報漏えい)	パスワードの奪取
	Denial of Service (サービス拒否)	通信の妨害
	Elevation of Privilege (権限昇格)	root 権限の奪取

DREAD の概要	観点	概要
	Damage	リスクが発生した場合の影響の度合い
	Reproductivity	リスクを再現させるための容易性
	Exploitability	攻撃に利用されうる可能性
	Affected users	影響を受けるユーザの規模
	Discoverability	リスクの発見容易性

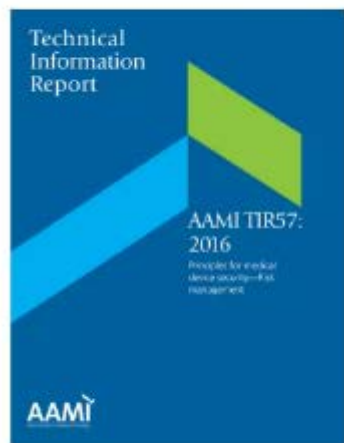
機器のサイバーセキュリティ確保のための セキュリティ検証の手引き (令和 6 年度 改定版)
https://www.meti.go.jp/policy/netsecurity/wg3/kensyou_tebiki_r6kaitei.pdf



図A.4-この規格に規定する使用の種類とJIS T 14971の“合理的に予見可能な誤使用”の概念との関係

■ ISO/IEC 81001-5-2 Health software and HIT system safety, effectiveness and security - Part 5-2 Security Risk Management for Manufacturers

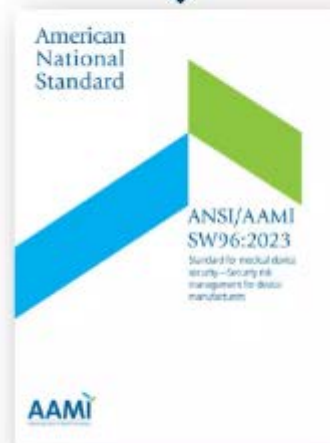
本文書は、ISO14971 で定義されたリスクマネジメントの枠組みの中で、ライフサイクルを通じて**設計、製造及び製造後のセキュリティリスクマネジメントに取り組む際の要求事項及びガイダンスを提供**する。



AAMI TIR57:2016
市販前のCS-RM



AAMI TIR97:2019
市販後のCS-RM



AAMI SW96:2023
ライフサイクル全体のCS-RM

Expanding upon security-related harm

AAMI TIR57:2016 defines several supporting terms necessary to define security-related harm



TIR 57とISO 14971のギャップ

→ **ISO 14971:2019に整合**

■ IEC 81001-5-1との関係

- 製品ライフサイクル全体のリスクマネジメントに関連した規格とし、IEC 81001-5-1を補完する。

■ Ed.2の変更点(仕様検討中) 開発期間:36 か月 (CD:2026/9, DIS/CDV 2027/9, IS 2028/9)

① ライフサイクルに関する根本的な課題について (Scope の検討)

この規格では、「ヘルスソフトウェアの開発及び保守に関わるセキュリティライフサイクルアクティビティ」を規定すると修正し、「**IEC 62443-4-1 への適合を支援する**」という部分は削除される。さらに、IEC 62304 の範囲だけでなく、全製品ライフサイクルを対象とすることを意図する図としてIMSDRF やFDA が参照しているJSP (Joint Security Plan) V2 のフレームワークが紹介された。

JSP2: <https://healthsectorcouncil.org/jsp2/>

また、プロセス規格の要求事項に関する記載部分は削除した。以下を改訂後のScope 案とした。

This document defines the security LIFE CYCLE requirements for development and maintenance of HEALTH SOFTWARE – taking the specific needs for HEALTH SOFTWARE into account. The PROCESSES, ACTIVITIES, and TASKS described in this document establishes a common framework for secure HEALTH SOFTWARE.

This document excludes specification of ACCOMPANYING DOCUMENTATION contents.

② ソフトウェアアイテム(コンポーネント)分類(4.3)の扱い

Ed.1 のISH(解説文)にある表に沿って、**Ed.2 のアクティビティについて(IEC 62304 のレベルI, II のように)該当する分類を示す方式に変更**する。

また、製品ライフサイクルに従って、“REQUIRED SOFTWARE”、“SUPPORTED SOFTWARE”及び“MAINTAINED SOFTWARE”分類に関する要求事項をより明確にする。

今後この必要に応じて分類名の変更も考慮する。

Activity Category	Clause	MAINTAINED	SUPPORTED (includes MAINTAINED)	REQUIRED (includes SUPPORTED)
Quality Management	4.3 Software Item classification related to risk transfer (Note: clarifying roles and responsibilities in support)	X	X	X
Software development	5.2.3 Security Risks for REQUIRED SOFTWARE	X*	X*	X
Software maintenance	6.3.1 SUPPORTED SOFTWARE update documentation	X*	X	
	6.3.2 MAINTAINED SOFTWARE security update delivery	X		
	6.3.3 MAINTAINED SOFTWARE security update INTEGRITY	X		

③ 製品ライフサイクルに関する検討

厚労省通知内で使用した図にある**販売終了 (End of Sales)**及び(責任を負う)**保守期間終了 (End of Guaranteed Support: EOGS)**の考え方の重要性が紹介された。

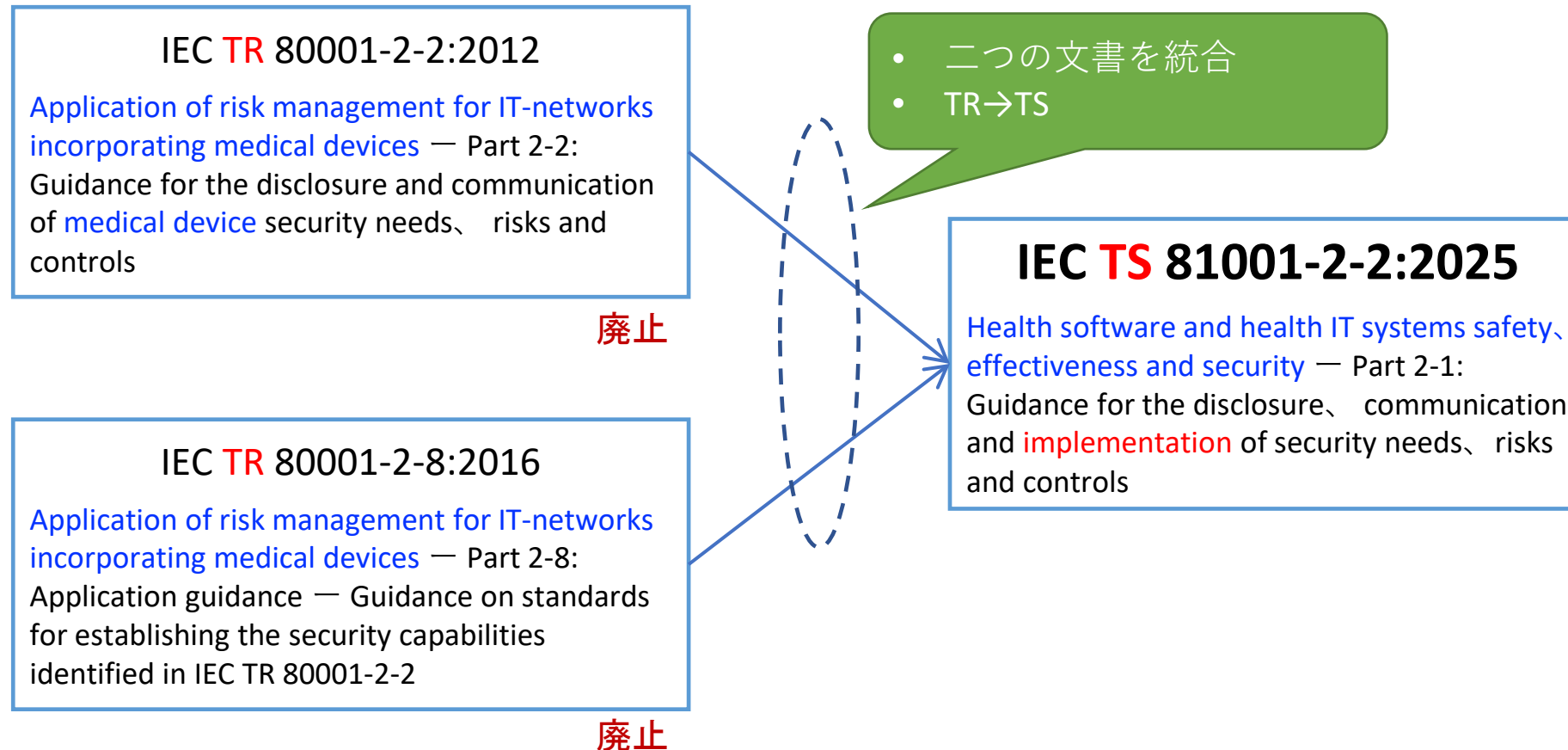


令和7年4月17日付厚労省通知“医療機器のサイバーセキュリティ対策に関連する情報提供について”いわゆる“追って通知”にある図

- IEC TR 80001-2-2(セキュリティ機能の開示)及び80001-2-8(セキュリティ機能の実装指針)を
IEC TS 81001-2-2(技術仕様書:TS)として統合して改訂 (**2025/10/1発行**)

HEALTH SOFTWARE AND HEALTH IT SYSTEMS SAFETY、EFFECTIVENESS AND SECURITY –

Part 2-2: Guidance for the disclosure、communication and implementation of medical device security needs、risks and controls



IEC TS 81001-2-2:2025 (MDS2との連携強化及び国際化)- 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

IEC TS 81001-2-2	MDS2カテゴリー	類型3：汎用画像診断装置WS	コメント
5.2	ALOF	要	自動ログオフ
5.3	AUDT	要	監査コントロール
5.4	AUTH	要	認証
5.5	CSUP	要	サイバーセキュリティ製品の更新
5.6	DIDT	要	健康データの匿名化
5.7	DTBK	要	データのバックアップと災害復旧
5.8	EMRG	要	緊急アクセス
5.9	IGAU	要	健康データの完全性と真正性
5.10	MLDP	要	マルウェアの検出/保護
5.11	NAUT	要	ノードの認証
5.12	PAUT	要	個人認証
5.13	PLOK	一部要	物理的ロック
5.15	SAHD	要	システムとアプリケーションの堅牢化
6.2	SGUD	要	セキュリティガイド
5.16	STCF	要	健康データストレージの機密性
5.17	TXCF	要	送信の機密性
5.18	TXIG	一部要	送信の完全性
6.3	RMOT	—	リモートサービス及び管理
6.4	SBOM	要	ソフトウェア部品表 (SBOM)
6.5	CONN	—	接続能力
5.14	RDMP	要	製品リスクに依存。単体プログラムは、その動作環境の情報、対応が必要
6.6	MPPI	—	個人を特定できる情報の管理



MDS2 Form (HN 1-2019)

Manufacturer Disclosure Statement for Medical Device Security – MDS²

Device Category 1	Manufacturer 1	Document ID	Document Release Date
Device Model	Software Version	Software Release Date	
Manufacturer or Representative Contact Information	Name	Title	Department
	Company Name	Telephone #	e-mail

MANUFACTURER'S DISCLOSURE STATEMENT FOR MEDICAL DEVICE SECURITY (MDS²) (MDS² is defined by IEC TS 81001-2-2:2025)

1. Can the device transmit or maintain electronic Protected Health Information (ePHI)?

2. Types of ePHI data elements that can be maintained by the device:

3. Maintaining ePHI: Can the device:

4. Mechanisms used for the transmission, import/export of ePHI: Can the device:

ADMINISTRATIVE SAFEGUARDS

5. Does manufacturer offer operator and technical support training or documentation on device security features?

6. What underlying operating system(s) (including version number) are used by the device?

PHYSICAL SAFEGUARDS

7. Are all device components maintaining ePHI (other than removable media) physically secure (i.e., cannot remove without notice)?

8. Does the device have an integral data backup capability (i.e., backup into removable media such as tape, disk)?

9. Can the device boot from non-volatile or removable media (i.e., a server other than an internal drive or memory component)?

TECHNICAL SAFEGUARDS

10. Can software or hardware not authorized by the device manufacturer be installed on the device?

11. Can the device be serviced remotely (i.e., maintenance activities performed by service personnel via network or remote connection)?

12. Level of supervisor/service access to device operating system: Can the device device/operator:

13. Does the device segment user/operator specific ID and password?

14. Are access sessions terminated after a predetermined length of inactivity (e.g., auto logoff)?

15. Events recorded in device audit log (e.g., user, date/time, action taken): Can the audit log record:

16. Does the device incorporate an emergency access ("bypass-glass") feature that logs each instance of use?

17. Can the device maintain ePHI (e.g., by internal history) during power service interruptions?

18. Can the device exchange ePHI with other devices:

19. Does the device ensure the integrity of the ePHI data with block or end-to-end error detection/correction technology?

セキュリティ機能の実装

~~出来上がったコードにセキュリティ機能を後付けで追加する~~

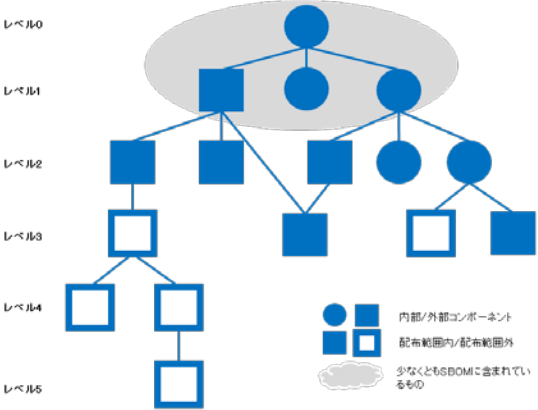


図9 トップレベルSBOM

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

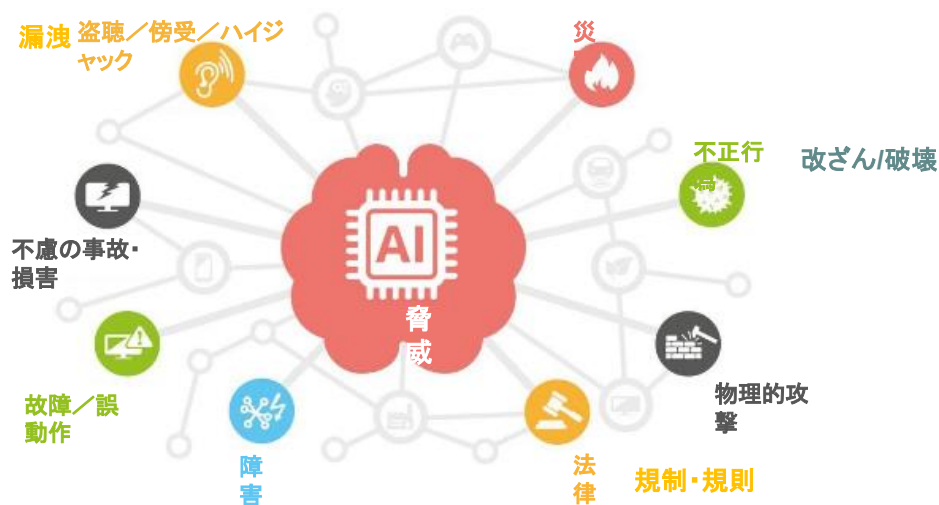


SBOMは独立して進化

IEC TS 81001-2-2はSBOM含まず
MDS2はSBOMを分離する議論

■ 欧州Team-NB (Notified Body) 医療機器における人工知能に関する質問 2024/11

- FDAのAIガイダンスが、メーカーに対し医療機器の設計・検証・監視方法を提示するアプローチに対し、Team-NBのAIチェックリストは実施状況を確認するアプローチを取る。つまりTeam-NBのアプローチは「実施方法を提示せよ」というもの。
- 両アプローチは本質的に同等で、最終的にはFDAも製造者の実施内容を審査する。
ただし、FDAのアプローチは「実施方法の共通基盤を設定する」点でより教示的である。
- FDAのAI医療機器ガイダンスに従うことは、ある意味でTeam-NBのチェックリストへの回答を可能にする
 - IG-NB: 2024_Joint-Team-NB-IG-NB-PositionPaper-AI-in-MDQuestionnaire-Version 1
<https://www.ig-nb.de/veroeffentlichungen>
 - Team-NB: Joint-Team-NB-IG-NB-PositionPaper-AI-in-MD-Questionnaire-V1-20241125
<https://www.team-nb.org/wp-content/uploads/2024/11/Joint-Team-NB-IG-NB-PositionPaper-AI-in-MD-Questionnaire-V1-20241125.pdf>

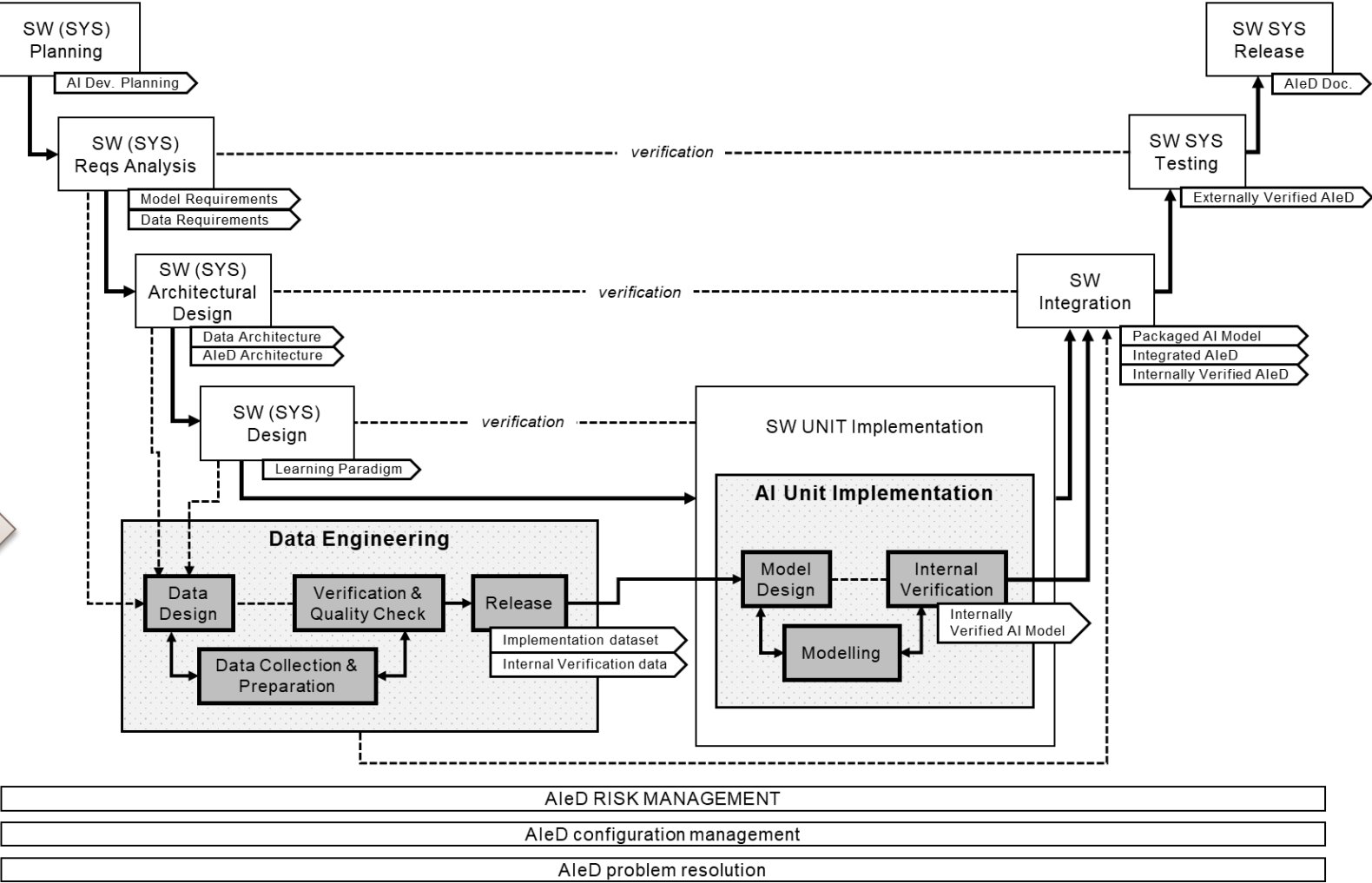


- AI システムにおいてセキュリティを確保するには、CRAに定められたセキュリティ要件に準拠するだけでは不十分
- AI特有のセキュリティ課題への対策は未成熟状態

<https://www.enisa.europa.eu/publications/cybersecurity-of-ai-and-standardisation>

<https://op.europa.eu/en/publication-detail/-/publication/e52bf2d7-4017-11eb-b27b-01aa75ed71a1/language-en>

■ Vモデルに含まれるAI活用デバイス固有のアクティビティ及びタスク(案)



IEC 63621
Artificial intelligence
enabled medical
devices - Data
management
AIデータマネジメント

Figure 4 – AI-enabled Device-specific Activities and Tasks included in Traditional V-Model

6.2.4 人工知能のセキュリティ・リスク

注:ソフトウェア支援医療機器やソフトウェア医療機器のサイバーセキュリティリスクはすでに知られているが(IG-NBの「医療機器のサイバーセキュリティに関するアンケート」やTeam-NBの「サイバーセキュリティに関するポジションペーパー」を参照)、それに加えてAI特有の攻撃もある。これらは、コード内の「バグ」や人為的ミスが主な原因である従来のサイバー攻撃とは根本的に異なる。AIに対するサイバー攻撃は通常、基礎となるアルゴリズムに内在する脆弱性を狙ったもので、これは修正できないか、修正が困難なものに限られる。いわゆる敵対的攻撃は、AIの判断／分類を操作することを目的としている。

1. 製造業者は、**ポイズニング攻撃、回避攻撃、トレーニングデータやモデルの抽出など、AIに適用されるサイバーセキュリティリスクを特定**しているか。 規則(EU)2017/745、附属書 I 3.)、規則(EU)2017/746 附属書 I 3.)、EN ISO 13485 第 7.1 項
2. 製造業者は、**AIモデルに対する脅威を特定するための情報源(Adversarial ML Threat Ma-trix、FDA MAUDEデータベースなど)を検索し、文書化**しているか。 規則(EU)2017/745 附属書 I 3.)、規則(EU)2017/746 附属書 I 3.)、EN ISO 13485、条項 8.2, 8.4, EN ISO 14971、条項 5.3、5.4、7.2、10, MDCG 2019-16, EN 62304、9.6項、EN 82304-1、条項8
3. 製造業者は、**リスクマネジメントにおいて、特定されたセキュリティリスクを考慮し、評価**しているか。
規則(EU 2017/745)附属書 I 3. c), 17.2, 17.3, 規則(EU)2017/746 附属書 I 3.)、EN ISO 13485、条項 7.3.3 c.)、EN ISO 14971、5.3項
4. 製造業者は、**特定されたリスクに対するリスク軽減策を定義**しているか？
規則(EU)2017/745、附属書 I 3. 規則(EU)2017/746 附属書 I 3.)、EN ISO 14971、7.2項
5. **AIのライフサイクルは、適切なセキュリティ・ライフサイクルを考慮**しているか。
規則(EU)2017/745、附属書 I 17.2.、規則(EU)2017/746、附属書 I 16.2.、MDCG 2019-16、EN 62304、節 4.3, 5.1.1 e)、IEC 81001-5-1:2021
6. **敵対的攻撃に対してアルゴリズムを強化する対策が実施され、考慮**されているか？
規則(EU)2017/745、附属書 I 1.、4. 規則(EU)2017/746、附属書 I 1.、4.、EN ISO 14971 第10.2項
7. 製造業者は、**AIモデルとその展開戦略に関するセキュリティリスク評価において、インフラとサプライチェーン全体を考慮**しているか。
(例えばクラウド上で動作するバックエンド・ソフトウェアや、開発・製品ライフサイクル中の特定の機能にクラウドベースのサービスを利用する) 規則(EU)2017/745、附属書 I 1.、4.、規則(EU)2017/746、附属書 I 1.、4.、EN 62304、5.1.1項、4.3項

<https://www.team-nb.org/wp-content/uploads/2024/11/Joint-Team-NB-IG-NB-PositionPaper-AI-in-MD-Questionnaire-V1-20241125.pdf>

■ 機械学習(ML)活用医療機器に特有のサイバーセキュリティの考慮事項 (AAMI CR 指針文書)

MLを活用した医療機器の特有の脅威

- データ中心の開発プロセスが特徴であり、高品質なデータの収集と準備が重要。
- MLモデルは、トレーニング中にデータ漏洩や予期しない結果を生じるリスクがある。
- サイバー攻撃の新たなベクトルが存在し、特に医療分野ではその影響が深刻。

サイバーセキュリティのリスク評価

- 各脅威の影響分析を行い、患者の安全やデバイスの性能に与える影響を評価。
- 脅威の発生可能性を評価し、攻撃の複雑さやターゲットの価値を考慮。
- リスクを軽減するための戦略を特定し、実施することが重要。

データマネジメントの重要性

- データの収集、クリーニング、保存、ガバナンスを含む。
- データのセキュリティは、すべてのデータ管理活動において重要。
- データの品質管理は、ライフサイクル全体を通じて維持されるべき。

モデルの設計と実装

- アルゴリズムの選択や特徴エンジニアリングを含む。
- 初期テストを通じてモデルが意図した通りに機能することを確認。

モデルのトレーニングと評価

- トレーニングデータを使用してモデルを開発し、パターンを学習。
- モデルのチューニングと評価を行い、性能を最適化。

モデルのデプロイメントと監視

- トレーニングされたモデルを新しいデータに対して使用。
- 定期的に性能を監視し、必要に応じて更新や再トレーニングを行う。

モデルの退役と廃止

- 現在のビジネスニーズやデータ環境に合わせてモデルを維持。
- 効率的な運用を確保するために、価値を提供しないモデルは削除。

医療機器における機械学習の脅威

バックドア攻撃: 特定の入力によってトリガーされる隠れたバックドア注入

- 攻撃は、訓練データの一部に特定のパターンを追加
- 緩和策: 特定の入力トリガーの動作をテストすること等

バイアス悪用攻撃: モデル内の既知のバイアスを利用して不公正な結果を出力する

- 例として、主に白人患者のデータで訓練された皮膚癌診断モデル等
- 緩和策: バイアス評価とデータの再訓練等

データ漏洩攻撃: データ漏洩攻撃は、訓練データに本来利用できない情報が含まれる

- これにより、モデルは不正確な予測を行う可能性があります。
- 緩和策: データの検証とアクセス制御等

回避攻撃: 回避攻撃は、AI/MLモデルを誤解させるために設計された入力を使用

- 攻撃者は、医療画像に微妙な変更を加えることで、モデルの誤解を引き起こす
- 緩和策: 誤分類の監視と敵対的訓練等

内部攻撃: 内部攻撃は、AI/MLシステムにアクセスできる悪意のある内部者による

- 例として、医療機器メーカーの不満を持つエンジニア等
- 緩和策: 厳格なアクセス制御と定期的なセキュリティトレーニング

モデル盗難攻撃: モデル盗難攻撃は、機械学習モデルの機能を複製

- 攻撃者は、モデルのパラメータに不正にアクセスし、独立して使用可能な複製を作成
- 緩和策: 暗号化と厳格なアクセス制御等

出力整合性攻撃: 出力整合性攻撃は、機械学習モデルの出力を変更又は操作

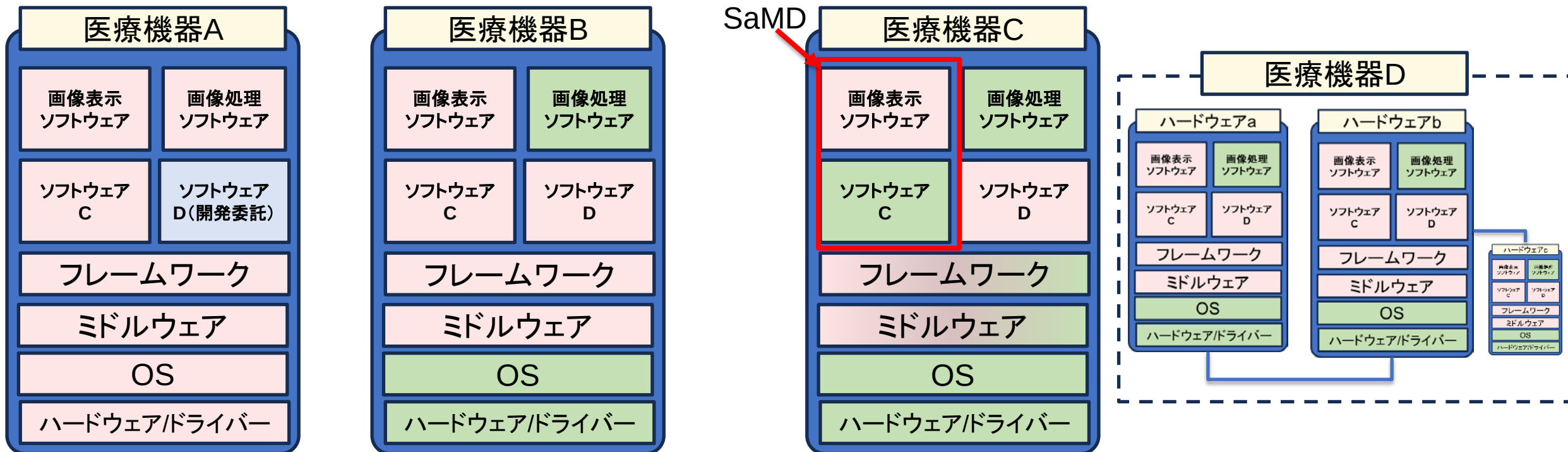
- 攻撃者は、モデルの出力を傍受し、変更することが可能
- 緩和策: 暗号化手法とデータ検証等

3. サイバーセキュリティ対策の基本的考え方

ソフトウェア構成管理とSBOM作成

汎用プラットフォーム上のアプリ(SaMD)
には、単独で必要な配慮事項

■ ソフトウェアの種類、開発方法によって、4つに分類できる。



ケース1（自製ソフトウェア）

OS: 自製RTOS, ソース
コード管理されたLinux 等

ケース2（自製+OTSソフトウェア）

OS: RTOS, Linux, Windows 等

ケース3（SaMD）

OS: RTOS, Linux, Windows,
Android, iOS等

ケース4（複数ハードウェア機器）

OS: ケース1, 2, 3の組合せ

自製ソフトウェア

開発委託ソフトウェア

OTSソフトウェア

SaMD（Android, iOSの場合）
開発のルールとストア審査・登録が必要
セキュリティプライバシーに特別な配慮が必要

Windowsはマイクロソフトグループ企業の商標です。AndroidはGoogle LLCの商標です。iOSはCisco Systems, Inc.の商標です。

医療機器のセキュリティリスク評価におけるCVSSの活用 — 医療機器のフォーカス

CMS ALLIANCE TO MODERNIZE HEALTHCARE May 18, 2017

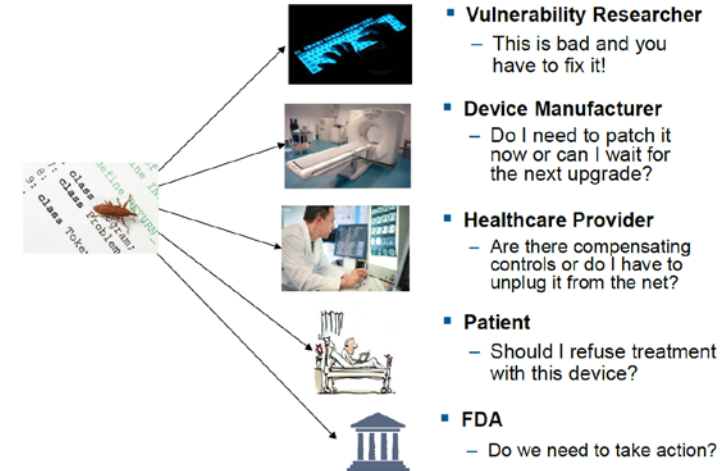
Using CVSS in Medical Device Security Risk Assessment

Penny Chase, The MITRE Corporation
Steve Christey Coley, The MITRE Corporation

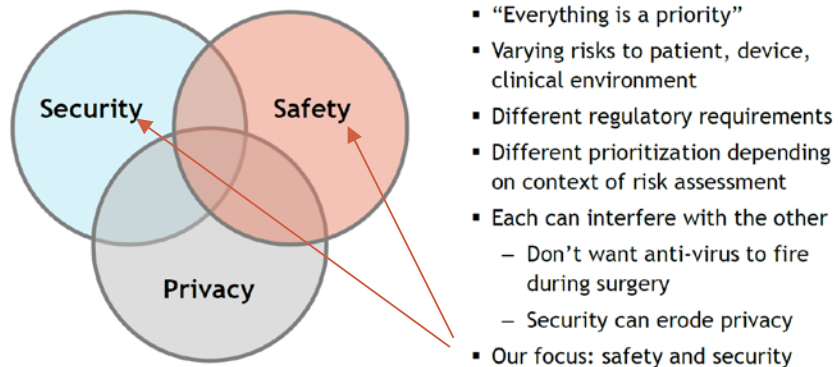


Approved for Public Release; Distribution Unlimited. 17-2078 © 2017, The MITRE Corporation. All Rights Reserved.

Problem: Different Perspectives of Vulnerabilities and Their Severity



The Delicate Balance of Safety, Security, and Privacy



Approach

- Set up a cross-stakeholder working group
 - Medical device manufacturers
 - Health care delivery organizations
 - Cybersecurity researchers
 - FIRST CVSS SIG
- Interact via telecons, listserv, collaboration group
- Reviewed how some manufacturers and healthcare delivery organizations currently use CVSS
- Came to consensus on approach
 - Provide scoring guidance in form of a rubric and examples of use
 - Recognize that there are multiple use cases
- Next steps
 - Form subgroups to work on rubric for base and environmental groups
 - Get feedback from broader stakeholder community
 - Develop Medical Device Development Tool qualification package

ステークホルダ間ワーキンググループ

Rubric for Applying CVSS to Medical Devices (2020/10/27更新)

<https://www.mitre.org/sites/default/files/2021-11/pr-18-2208-rubric-for-applying-cvss-to-medical-devices.pdf>

セーフティ(安全)とサイバーセキュリティ ISO 14971:2019 (AAMI TIR57:2016)

■ 危害(harm)の定義の改訂

physical injury or damage to the health of people、or damage to property or the environment

injury or damage to the health of people、or damage to property or the environment

データ及びシステムのセキュリティ侵害

人の受ける健康障害及び被害

財産若しくは環境の受ける害

危害の定義に財産及び環境への害が含まれている。その上で、“人の安全”を重視している。

■ セキュリティリスクは、

安全に影響を及ぼす場合と、有効性の低下など財産や環境に影響を及ぼす場合がある。

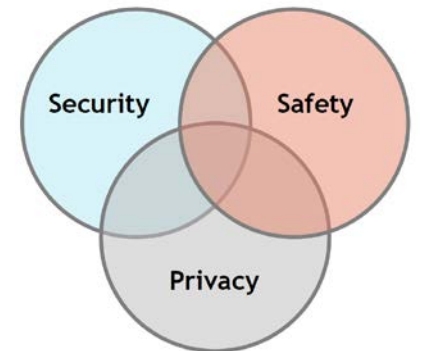
安全に影響を及ぼすセキュリティリスクは従来のリスクマネジメントと同様にマネジメントできる。

セキュリティリスクは、一般的な情報セキュリティの考え方と同じであるため、個人情報保護等の概念も含まれている。



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

人の安全を重視



一般的には...

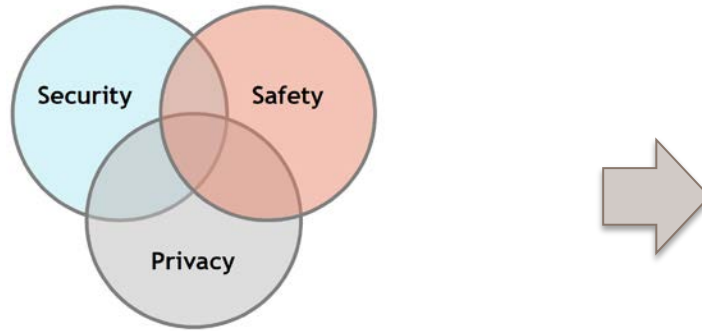
■ FDA、IMDRFガイダンスでは、患者安全という指針を示し、「人の安全」を重視している。

医療機器の設計における基本的考慮事項

汎用プラットフォーム上のアプリ(SaMD)は、OS依存性低減の取組が必要

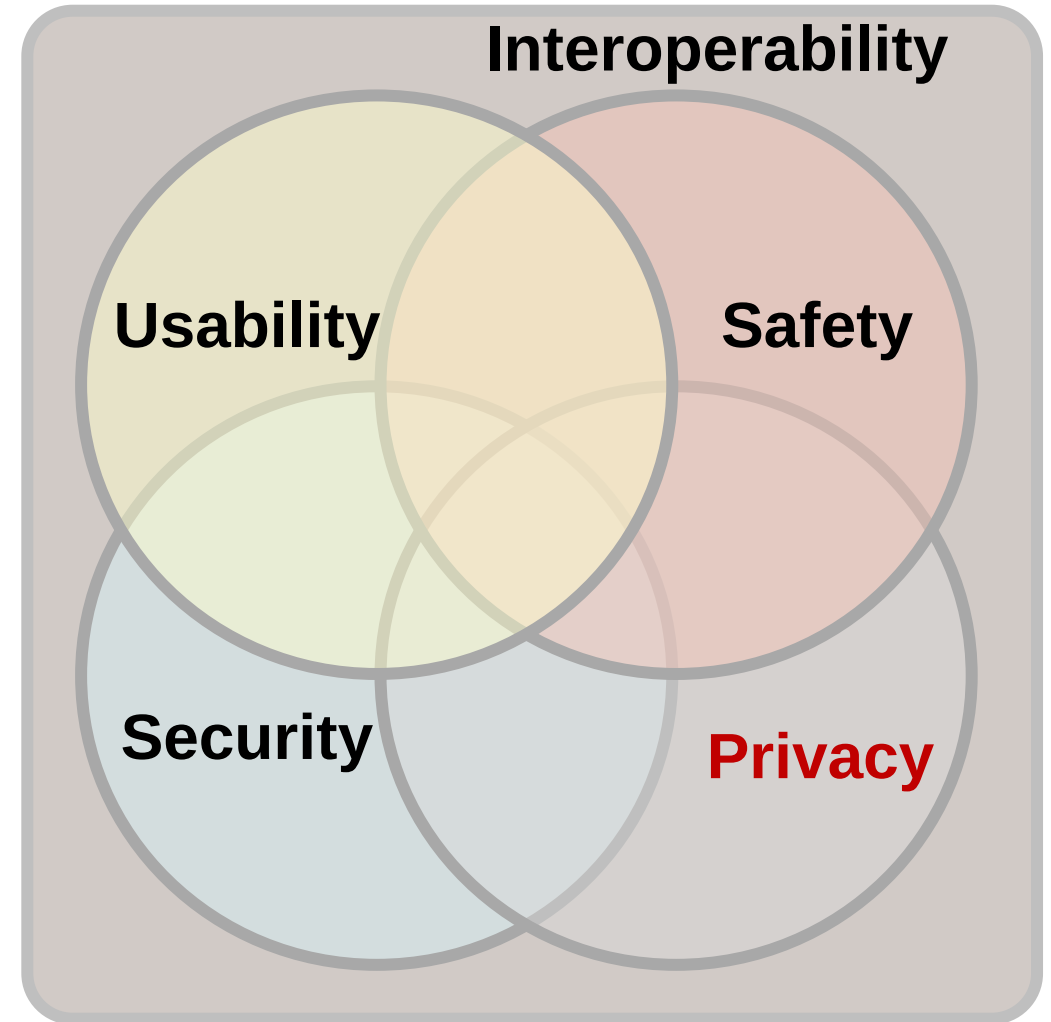
■ 医療機器ソフトウェア(SaMD含む)

- 医療機器全体で安全(セーフティ)とセキュリティを確保
- ユーザビリティエンジニアリングの考慮は必須
- 相互運用性(Interoperability)も必須の考慮事項



■ 汎用IoT機器上のSaMD(Android、iOS/iPadOS)

- OWASP MASVS(Mobile Application Security Verification Standard)L2(高セキュリティ)の適用を求められる可能性(ストア審査要件)
- 個人識別情報(PII)や医療データが含まれるならば、プライバシーも重要な考慮事項(プライバシーポリシー、ISMS適合他)
- OS依存性の低減: OS アップデート影響評価フロー確立
製造業者は、OSアップデートのタイミングを制御できない



医療機器の設計における基本的考慮事項

AndroidはGoogle LLCの商標です。iOSはCisco Systems, Inc.の商標です。iPadOSはApple Inc.の商標です。

→ 保守計画の基本的アプローチが異なる

汎用プラットフォーム上のアプリ (SaMD)
は、SiMDより厳しい使用環境を想定

領域	MASVS	FDA(Cybersecurity / SaMD)	IEC 62304 / IEC 81001-5-1	ISO 14971
アーキテクチャ設計	V1	脅威モデリング, DFD, アーキテクチャーレビュー	ソフトウェア設計(5.3)	リスク分析(4.4)
データ保護	V2	PHI/PII 保護、データ最小化	データ管理	リスクコントロール
暗号化	V3	暗号化、鍵の管理	実装(5.5)	リスク低減策
認証・セッション	V4	アクセス制御、認証	ソフトウェア要求(5.2)	誤使用リスク
通信セキュリティ	V5	安全な通信、完全性	インタフェース設計	ハザード識別
プラットフォーム相互作用	V6	OS 依存性、アップデート管理	ソフトウェア構成管理(8)	変更管理
コード品質	V7	SBOM, 脆弱性管理	検証・妥当性確認(5.7)	残留リスク評価
逆コンパイル耐性	V8	改ざん防止	ソフトウェア保護	リスクコントロール



基本的な開発ライフサイクルプロセスはIEC 62304、IEC 81001-5-1を適用できる。しかしながら、**SiMDやSiMDの一部であるSaMDより厳しい使用環境に曝される**ため、デフォルトでセキュアな状態を維持できる設計(Secure by Design)の徹底が必須である。また、**プラットフォームのアップデート等に対する対策はSiMDより重要**である。

AndroidはGoogle LLCの商標です。iOSはCisco Systems, Inc.の商標です。iPadOSはApple Inc.の商標です。

- 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/2022/0510_003.html

(日本語) <https://www.meti.go.jp/press/2022/05/20220510001/20220510001.html>

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

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。 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。

サプライチェーン・マネジメント



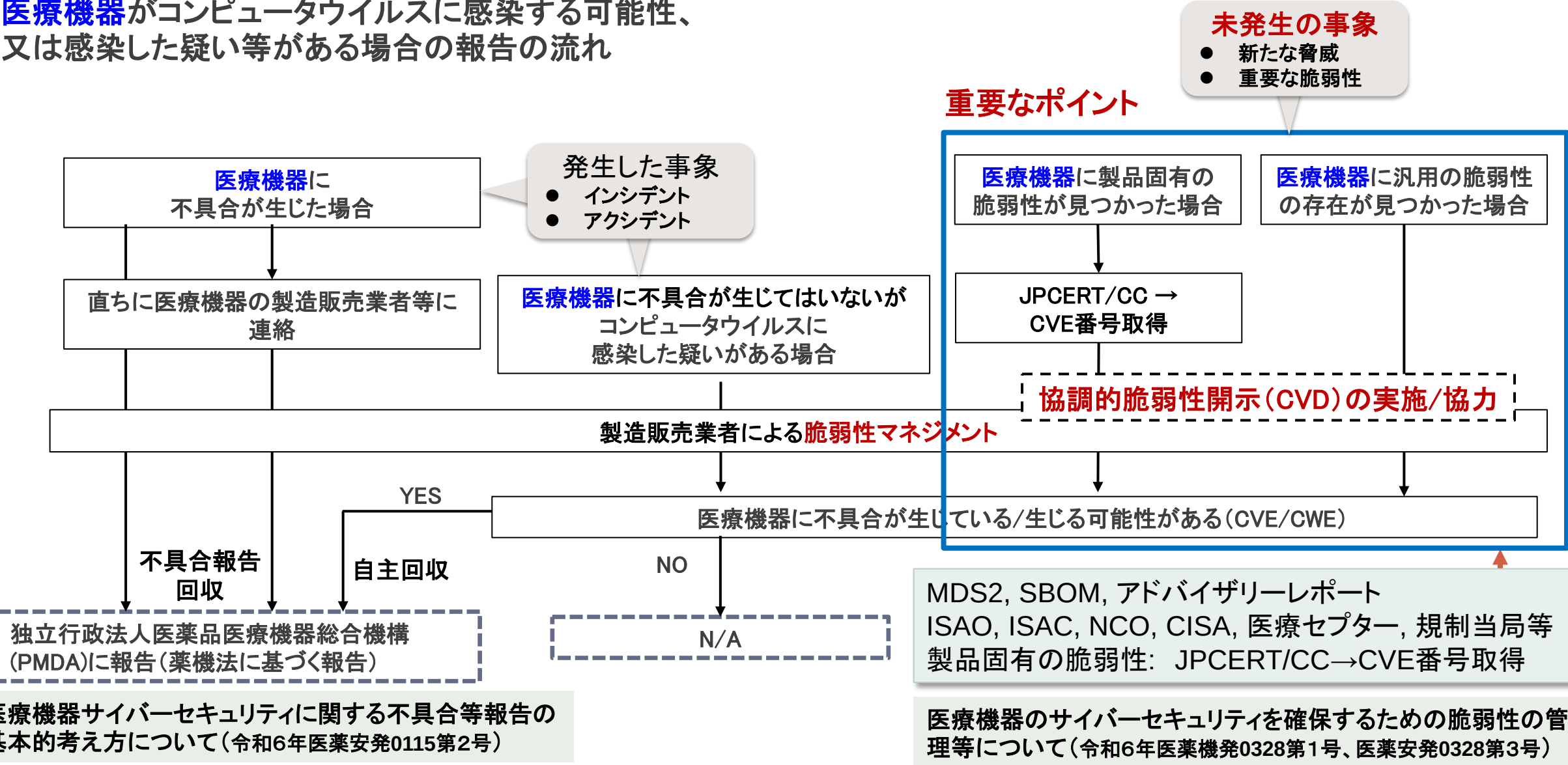
サイバーセキュリティに関する
QMSの指標

- ・ 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サプライチェーン・ライフサイクルの様々な段階に組み込む：
調達前に、候補となる各ソフトウェアメーカー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>

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



JPCERT/CCの早期警戒情報の提供フレームワーク

- 提供対象
国民の社会活動に大きな影響を与えるインフラ、サービス及びプロダクトを提供されている組織及び団体における情報セキュリティ関連部署もしくは組織内 CSIRT

サイバーセキュリティインシデント発生時の相談窓口

- サイバー攻撃又はその疑いにより、情報漏えい、ウイルス感染、システム停止などのインシデントが発生した場合、迅速な対応が必要です。
- 金銭被害、信用低下、事業停止等や関係者（顧客、取引先、従業員等）への被害拡大を最小限に抑えられよう、警察への相談に加え、初動対応を支援する以下の専門機関の活用を検討ください。

独立行政法人情報処理推進機構（IPA）

企業・組織のためのインシデントの相談・届出・情報提供窓口

不正アクセス等のインシデントに関する相談や届出、情報提供の受付：
<https://www.ipa.go.jp/security/todokede/incidentportal.html>

(相談例)

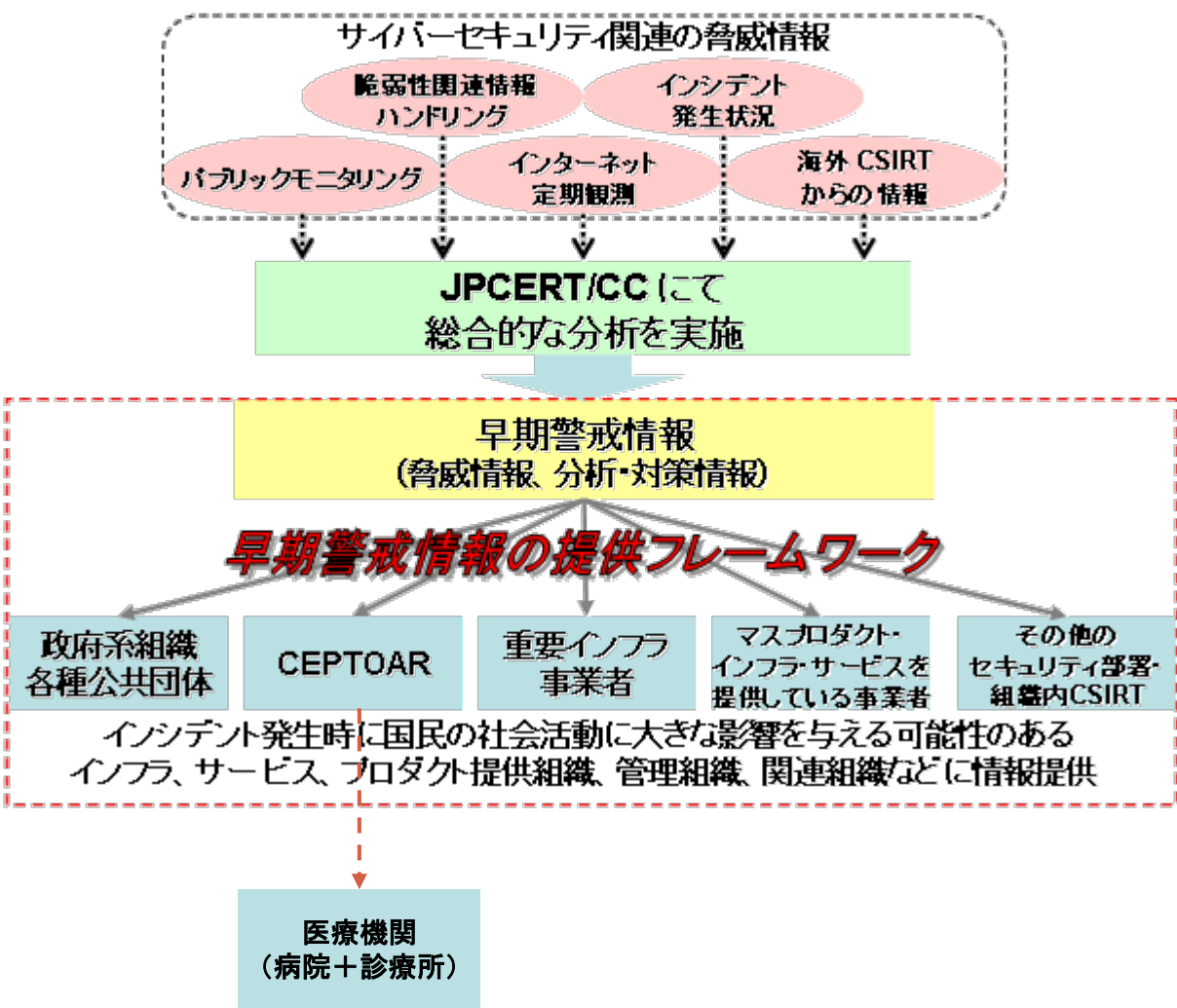
- ランサムウェアに感染したため、対処方法について相談したい
- 普段の情報セキュリティの対策やIPAのセキュリティ施策について知りたい
- サイバー攻撃被害について、サイバー保険の適用を受けるために公的機関への届出を行いたい

一般社団法人JPCERTコーディネーションセンター

インシデントを報告したい
発生元に調整を依頼したい

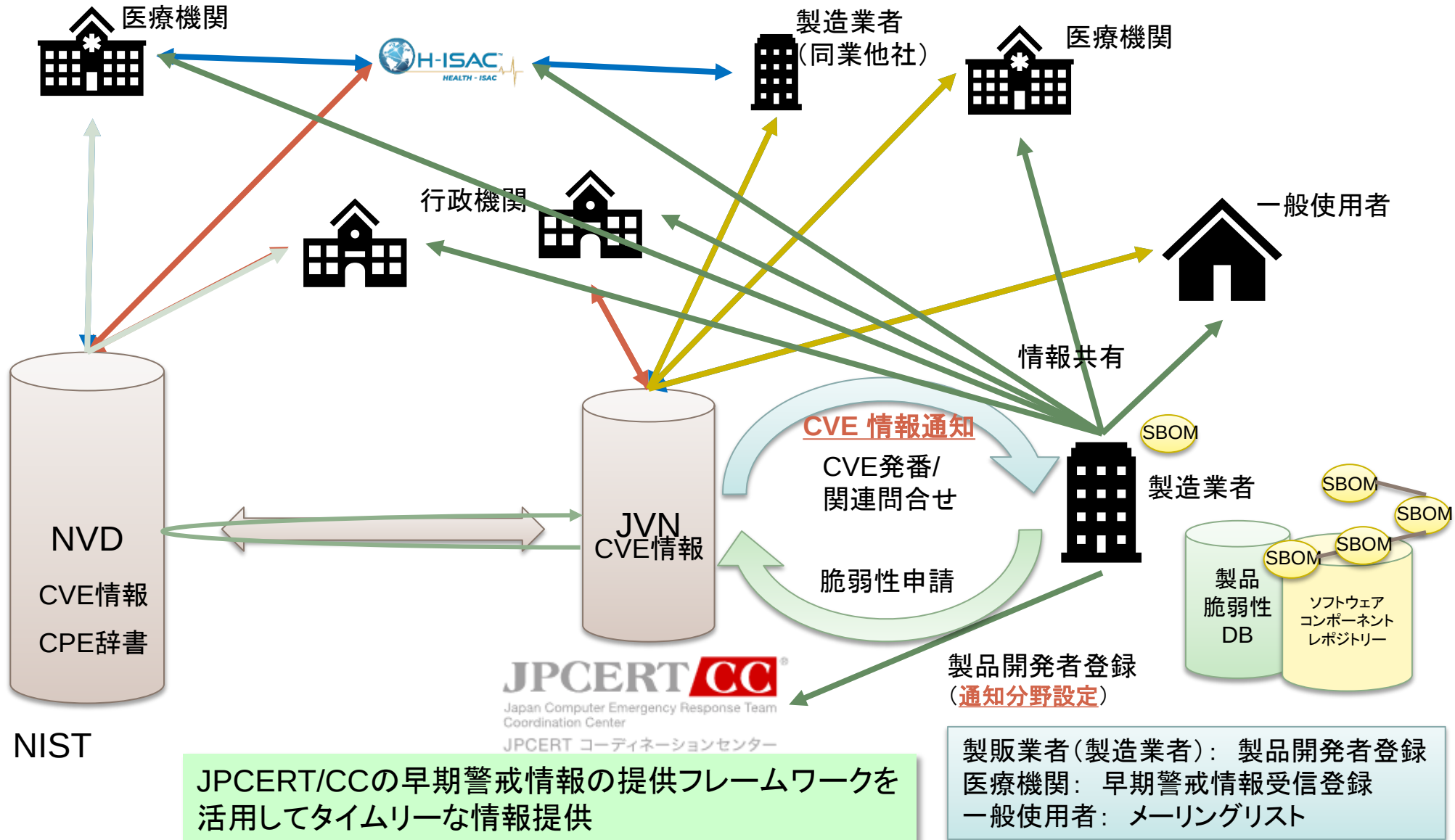
インシデント 対応・調整 依頼

- インシデント初動対応（必要な調査、対応方針の検討、被害箇所の特定等）のサポートなどの依頼相談：
<https://www.jpcert.or.jp/form/>
- インシデント対応に関する様々な相談、情報提供の受付：
<https://www.jpcert.or.jp/ir/consult.html>



<https://www.jpcert.or.jp/ics/ics-community.html>

脆弱性に関する情報共有の仕組み（脆弱性登録・共有フロー）



1. 概要

セントラルモニタ CNS-6201(該当バージョン:01-03,01-04,01-05,01-06,02-10,02-11,02-40)は、**サービス拒否(DoS)の脆弱性により、動作の低下を招いたり、機能不全が生じたりする可能性**があります。

2. 脆弱性ID

CVE: CVE-2025-59668

JVN: JVN#96989989

3. 説明

- 脆弱性を含む製品/ソフトウェア

製品名: セントラルモニタ

製品型式: CNS-6201

バージョン: 01-03,01-04,01-05,01-06,02-10,02-11,02-40

- 脆弱性の種類

CWE-476: NULL Pointer Dereference

- 脆弱性の説明

セントラルモニタ CNS-6201の該当バージョンにおけるUDPパケット処理において、**攻撃者が特別に細工したパケットを送信すると**、受信処理でNULLポインタ参照が発生し、プロセスが異常終了して**サービス拒否(DoS)に至ります**。本脆弱性の悪用に認証は不要で、UDPサービスにネットワーク上、到達可能であれば再現します。

4. インパクト

本脆弱性が悪用されると、サービス拒否(DoS)に至り、可用性が低下する可能性があります。影響は可用性に限定され、機密性および完全性への直接的な影響はありません。現時点で任意コード実行や権限昇格は確認されておらず、本脆弱性に起因する健康被害や可用性低下の報告は受けていません。

5. CVSSスコア

CVSS v4.0 Base Score: 8.7 / HIGH

CVSS v4.0 Vector: CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N

CVSS v3.1 Base Score: 7.5 / HIGH

CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

5. 解決

本製品で特定された脆弱性は、サポート終了を迎えたバージョンに存在します。**本製品については、米国では保守体制を2024年9月に終了(EOS)、それ以外の国でも該当バージョンについては保守対応期間を終了**しており、後継品への移行をお願いしています。継続使用される場合は、ネットワーク管理者の責任のもとで下記の代替えコントロールの徹底をお願いします。

- 影響を受ける製品をインターネットおよび信頼できないシステムから分離してください。
- 影響を受ける製品に到達しようとするすべてのネットワークトラフィックを監視し、疑わしいアクティビティがないか記録してください。
- HIS等との連携が必要な場合は、物理的に分離されたモニタネットワークと他ネットワークの間に境界装置(ファイアウォールまたはルータ)を設け、必要最小限の通信のみを明示的に許可してください。
- ベッドサイドモニタもしくは、医用テレメータによる、測定の間隔を延長をお願いします。サービス拒否(DoS)状態に至った場合は、本体正面にあるパワースイッチを長押し(5秒以上)して強制終了のうえ、再度、パワースイッチを押して電源をオンにしてください。

6. 謝辞

QuinnTech.aiのJared P. Quinnがこの脆弱性を発見し、日本光電およびCISAに報告しました。CISAと協力して、JPCERT/CCが報告者と日本光電の間の調整を行いました。

7. 改訂履歴

Revision	日付	説明
1	2025-09-30	初版公開
2	2025-10-06	JVNアドバイザのリンクを追加

本脆弱性に関するご不明な点やご質問がございましたら、当社ウェブサイトお問い合わせフォーム <https://www.nihonkohden.co.jp/feedback.html> に、お問い合わせください。

<https://jvn.jp/vu/JVNVU96989989/index.html>

レガシー医療機器に対するベストプラクティス事例

4. まとめ

SaMDに関する国際的な扱い

■ 考え方

- **基本的に医療機器ソフトウェア**の要求事項を適用
 - SaMDは医療機器ソフトウェアのひとつの(特殊な)製品形態
- AI/ML、サイバーセキュリティ関連ベース規格は医療機器ソフトウェアが適用範囲

■ 汎用IoT機器(プラットフォーム: Android、iOS/iPadOS)上のSaMD

- 販売終了後**サポート期間が短い**
製品が多いことが指摘(US)

↓
OS等の実行環境のアップデート対応
(今後の課題)

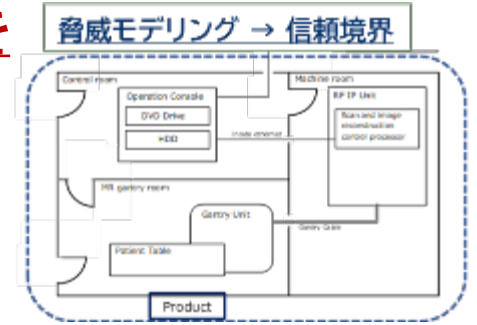


- **より厳しい使用環境に曝されるため、**
デフォルトでセキュアな状態を維持できる設計(Secure by Design)の徹底が必須

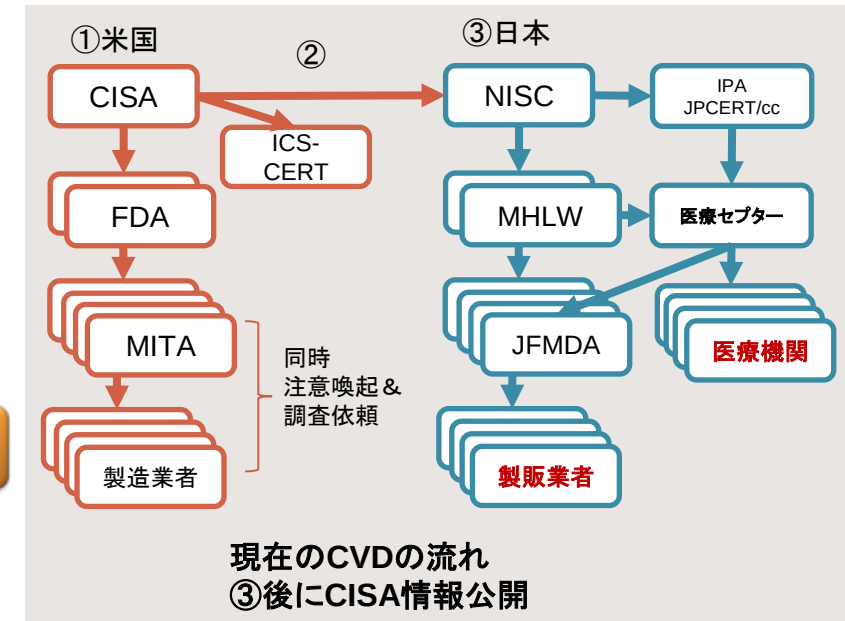
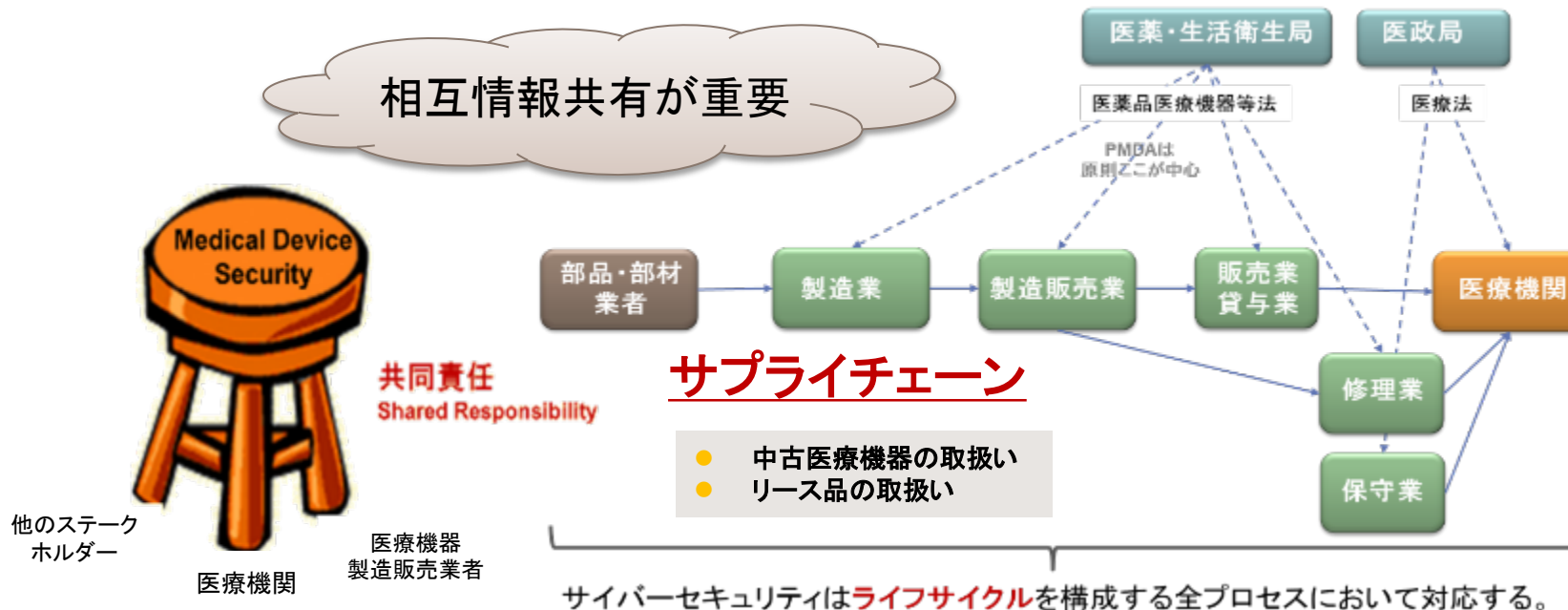
医療機器ソフトウェアのサイバーセキュリティに関連するリスク

- 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 — 透明性の強化が必要 —



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)

他のステークホルダー
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

AMEDサイバーセキュリティ研究班資料より引用

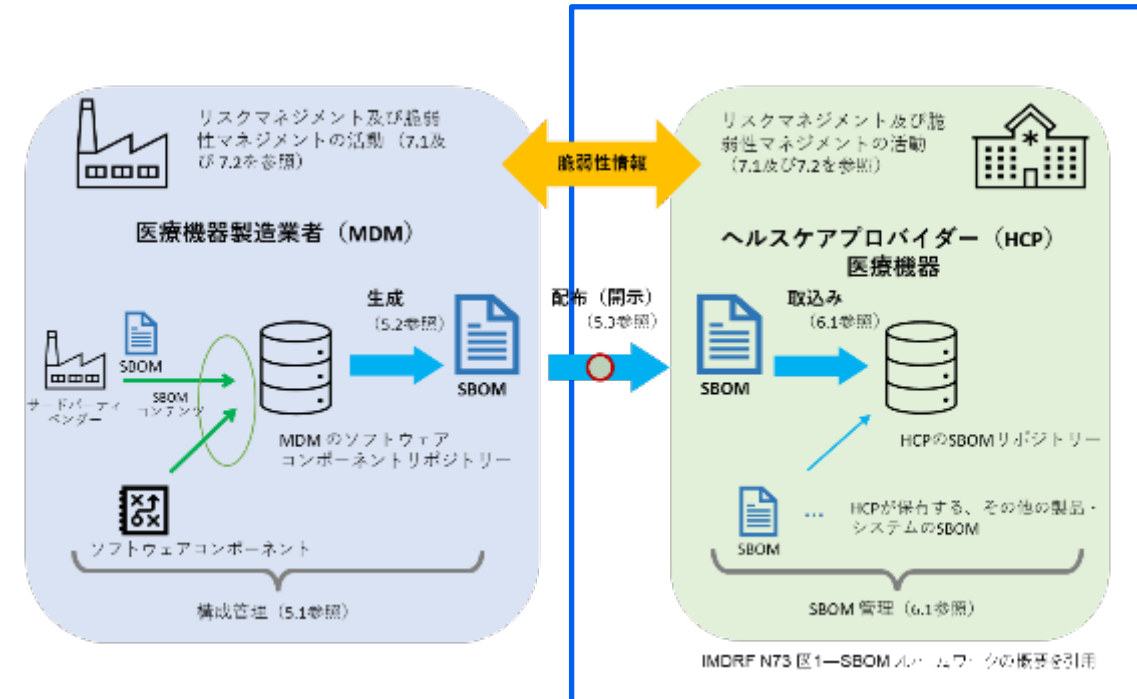
製造販売業者が継続して取り組む課題

- 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） → 2026年中に実施又は実施計画
 - セキュリティポリシーの開示（必要に応じてプライバシーポリシー、ISMS適合他）
 - ソフトウェアの管理、脆弱性対策強化
 - 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



SAMD含む医療機器ソフトウェアの
サイバーセキュリティ関連規格・規制の動向
ご清聴ありがとうございました。