2026年度 JIRA-JAHIS合同報告会
― 医療機器におけるサイバーセキュリティ対策 ―

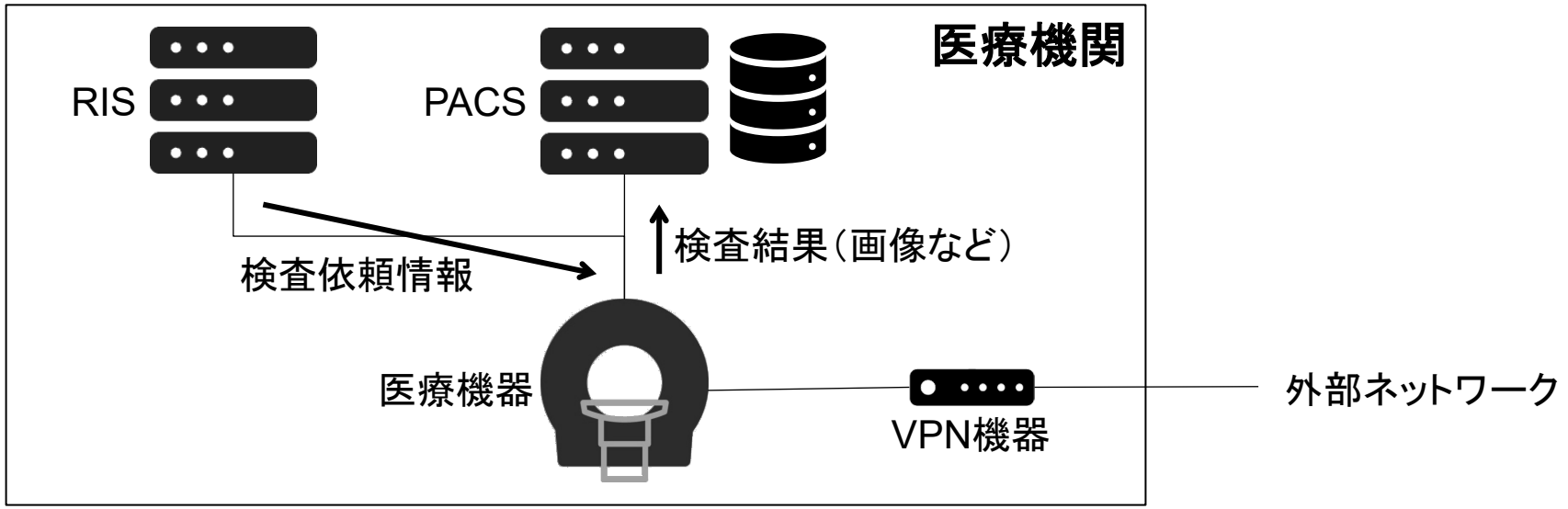
「SBOM対応を含む医療機器サイバーセキュリティ関連規制・ガイドラインの動向」



一般社団法人 日本画像医療システム工業会（JIRA)
医用画像システム部会　セキュリティ委員会　委員　花石　昌文

サイバーセキュリティ管理の対象となる医療機器等

- 医療情報システムや外部ネットワークと接続される医療機器
- 医療機器の運用保守に必要な周辺機器（医療機器でなくても、医療機器の安全性確保やサイバーセキュリティ維持に不可欠であれば対象）
- サイバーセキュリティ管理の対象となる医療機器は、医療情報システムにカテゴライズされる

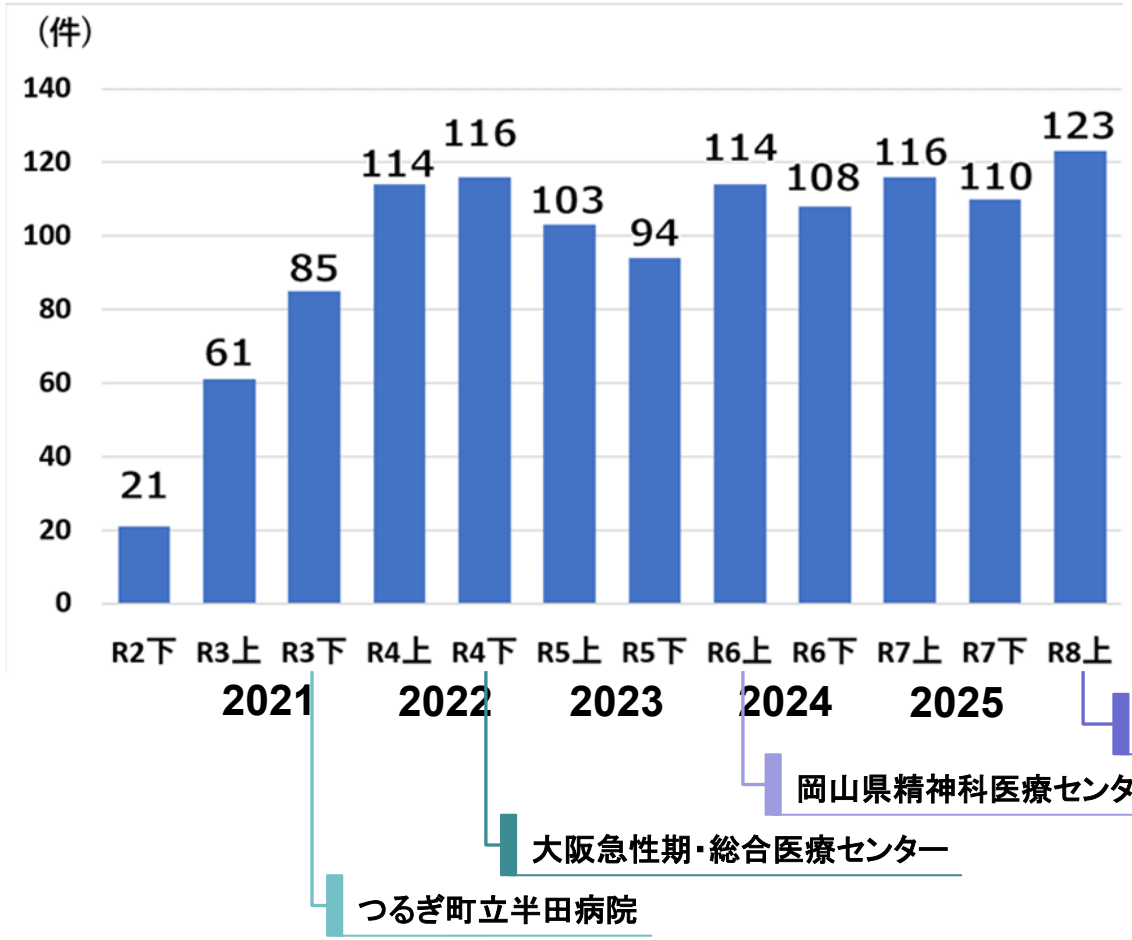


※ 参考：厚生労働省「医療機関における医療機器のサイバーセキュリティ確保のための手引書（第2版）」

医療機器サイバーセキュリティを取り巻く環境変化 1/2

- ランサムウェア被害の増加に伴い、医療機関で深刻な事案発生

【図表４：ランサムウェア被害報告件数】※



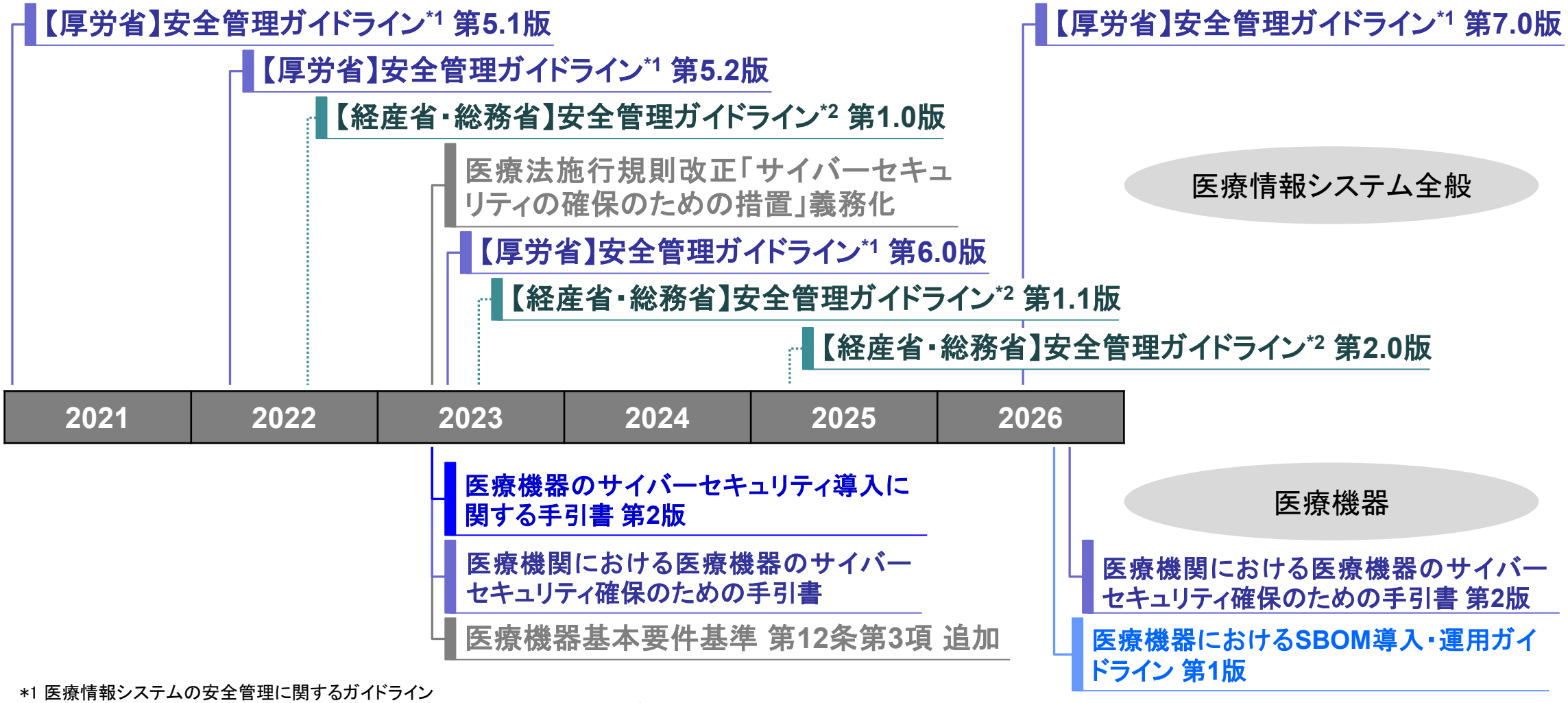
■ 医療機関のランサムウェア被害の共通要因

- 侵入経路
  - VPN装置の脆弱性への未対策
  - VPNアカウント管理の不備
- 被害拡大要因
  - 管理者権限の過剰付与
  - パスワードの使い回し
  - システム間の分離不足

※ 出典：警察庁「サイバー空間をめぐる脅威の情勢等（令和8年上半期）」

医療機器サイバーセキュリティを取り巻く環境変化 2/2

- 医療分野におけるサイバーセキュリティ要求が継続的に強化



*1 医療情報システムの安全管理に関するガイドライン
*2 医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン

医療機器におけるサイバーセキュリティ関連の規制と文書の整理

- 医療機器のサイバーセキュリティ対応は、法令や技術規格を踏まえ、各種手引書やガイドラインにより実務へ展開

	規制・文書	説明
1	薬機法	委任法令として基本要件基準を規定
2	医療機器基本要件基準	薬機法第41条第3項に基づく基準。サイバーセキュリティ要求は第12条第3項に規定
3	JIS T 81001-5-1	基本要件基準（第12条第3項など）の要求に対応するための重要な技術規格・参照規格
4	医療機器のサイバーセキュリティ導入に関する手引書	規制対応やサイバーセキュリティ実務の考え方を整理した、製造販売業者向けの解説文書
5	医療機関における医療機器のサイバーセキュリティ確保のための手引書	医療機関と医療機器事業者の役割分担や連携方法に加えて、MDS2やSBOM等のセキュリティ情報活用について整理した、主に医療機関向けの実務手引書
6	医療機器におけるSBOM導入・運用ガイドライン	SBOM導入をこれから開始する、または試行段階の製造販売業者向けにSBOMの作成・運用を具体化したガイドライン

MDS2とSBOMの役割

- 「医療機関における医療機器のサイバーセキュリティ確保のための手引書」では、製造販売業者に対し、MDS2やSBOM等のセキュリティ文書の提供／継続的な更新を求めている
  - MDS2：医療機器のセキュリティ機能を標準書式で開示する文書
  - SBOM：医療機器に含まれるソフトウェア構成要素を開示する文書

医療機関はMDS2やSBOMなどを活用して、医療機器のリスク評価・脆弱性管理を実施することが求められる

MDS2の概要

- **M**anufacturer **D**isclosure **S**tatement for **M**edical **D**evice **S**ecurity, ANSI/NEMA HN 1-2019
  - 認証、アクセス制御、監査、データ保護、通信など、医療機器のセキュリティ機能を標準様式で開示する文書
  - MDS2のセキュリティ機能体系はIEC TS 81001-2-2:2025（国際技術仕様）に継承・発展
  - MDS2のセクション構成／概要

No.	ID	セクション	設問概要	No.	ID	セクション	設問概要
1	DOC	機器の説明	機器情報・用途説明／脆弱性開示	14	PAUT	個人の認証	ユーザー認証（ID・パスワード等）
2	MPII	個人識別可能情報の管理	個人情報の保存有無と管理方法	15	PLOK	物理的ロック	機器の物理的な保護対策
3	ALOF	自動ログオフ	一定時間未操作時の自動ログオフ	16	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およびソフトウェアコンポーネントのロードマップ	サードパーティーアプリケーション及びソフトウェアコンポーネントのセキュリティサポートに関する製造業者の計画
4	AUDT	監査コントロール	操作履歴・監査ログの記録				
5	AUTH	認証	認証機能とアクセス制御				
6	CSUP	サイバーセキュリティ製品の更新	セキュリティパッチやソフト更新対応	17	SBOM	ソフトウェア部品表	SBOMの有無及び標準形式での提供
7	DIDT	健康データの非識別化	健康データの匿名化・非識別化機能	18	SAHD	システムとアプリケーションの堅牢化	不要機能無効化などのセキュリティ強化対応
8	DTBK	データのバックアップと災害復旧	バックアップおよび災害復旧機能				
9	EMRG	緊急アクセス	緊急時のアクセス機能の組み込み	19	SGUD	セキュリティガイダンス	顧客向けセキュリティ情報・ガイダンス
10	IGAU	健康データの完全性と信頼性	データ改ざん検知・完全性確認	20	STCF	健康データストレージの機密性	保存データの暗号化・保護
11	MLDP	マルウェアの検出/保護	マルウェア対策機能	21	TXCF	通信の機密性	通信データの暗号化・保護
12	NAUT	ノードの認証	システム間・ノード間の認証	22	TXIG	通信の完全性	通信データの改ざん防止
13	CONN	接続能力	ネットワーク接続および通信機能	23	RMOT	リモートサービス	リモート保守・遠隔サービス機能

※ 出典：JIRA ANSI/NEMA規格MDS2「医療機器セキュリティのための製造業者開示説明書」

MDSとMDS2のマッピング例 1/3（ご参考）

MDS 5.0		MDS2（ANSI/NEMA HN 1-2019）	
項	質問	ID	質問
1	扱う情報のリストを医療機関等に提示できるか？	MPII-1	この機器は、個人識別可能情報（例：保護対象電子医療情報［ePHI］）を表示、通信、保存、または修正できるか? ガイダンス：　機器が保持できるPII要素（例：患者名、患者ID、社会保障番号、生体データ）を「Note」に記載するか、完全なリストについて製品文書の参照先を示す。
2	個人情報が入力・参照できる端末の覗き見防止の機能があるか？		
3	離席時の不正入力防止の機能があるか？	ALOF-1	操作していない時間があらかじめ決めた一定の長さを超えると、ログインしているユーザーの再認証を強制するように機器を設定できるか（例：自動ログオフ、セッションロック、パスワードで保護されたスクリーンセーバ）？
4	アクセス管理の機能があるか？	AUTH-1	機器はユーザーログイン要件又はその他のメカニズムを使って許可されていないユーザーのアクセスを禁止できるか？
4.1	利用者の認証方式は？	PAUT-1	機器は、すべてのユーザーおよび役割（サービスアカウントを含む）に固有のIDおよびパスワードをサポートし、実施しているか?
	• 記憶（ID・パスワード等）	PAUT-1.1	機器は、すべてのユーザー及び役割（サービスアカウントを含む）に対して固有のID及びパスワードの認証を行っているか?
	• 生体認証（指紋等）	PAUT-11	機器は生体認証をサポートしているか?
	• 物理媒体（ICカード等）	PAUT-12	機器は物理的なトークン（例：バッジアクセス）をサポートしているか?
	• 上記のうちの二要素を組み合わせた認証（具体的な組み合わせを備考に記入してください）	PAUT-8	多要素認証をサポートしているか?
	• その他（具体的な認証方式を備考に記入してください）		
4.1.1	パスワードを利用者認証手段として利用している場合、パスワード管理は可能か？	PAUT-6	確立されている（組織固有の）複雑なルールを満たすユーザーアカウントのパスワードを強制的に作成するように機器を設定できるか？
4.1.2	セキュリティ・デバイスを用いる場合に破損等で本人の識別情報が利用できない際の代替機能があるか？		
4.2	利用者の職種・担当業務別の情報区分ごとのアクセス管理機能があるか？	AUTH-2	ユーザーは、「役割」（例：ユーザー、管理者、サービス等）に基づき、異なる権限レベルを割り当てることができるか?

MDSとMDS2のマッピング例 2/3（ご参考）

MDS 5.0		MDS2（ANSI/NEMA HN 1-2019）	
項	質問	ID	質問
4.3	アクセス記録（アクセスログ）機能があるか？	AUDT-1	医療機器は、標準的なオペレーティングシステムログ以外に追加の監査ログや監査レポートを作成することができるか?
4.3.1	アクセスログを利用者が確認する機能があるか？	AUDT-6	監査ログは所有者/操作者が監視/レビューできるか?
4.3.2	アクセスログへのアクセス制限機能があるか？	AUDT-7	監査ログは変更から保護されているか?
		AUDT-7.1	監査ログはアクセスから保護されているか?
5	時刻情報の正確性を担保する機能があるか？	AUDT-4.1.1	日時はネットワーク時刻プロトコル（NTP）または同等の時刻ソースによって同期できるか?
6	不正ソフトウェア対策機能を有しているか？	MLDP-2	機器はマルウェア対策ソフトウェア（またはその他のマルウェア対策メカニズム）の使用をサポートしているか？
		MLDP-4	機器は、機器上での実行が許可されているソフトウェアおよびサービスを制限するアプリケーションのホワイトリストを使用しているか?
7	無線LANを利用する場合のセキュリティ対策機能はあるか？	CONN-1.1.1	機器はWi-Fiをサポートしているか?
8	持ち出し機器において、ソフトウェアのインストールを制限する機能があるか？	CSUP-10.1	システムには、未承認ソフトウェアのインストールを防止するためのメカニズムがあるか?
9	持ち出し機器において、外部入出力装置の機能を無効にすることができるか？	MPII-3.3	機器は、個人識別可能情報をリムーバブルメディアから取得、またはリムーバブルメディアへ記録するか（例：リムーバブル-HDD、USBメモリ、DVD-R/RW、CD-R/RW、テープ、CF/SDカード、メモリスティックなど）?
		CONN-1	機器にはハードウェア接続機能があるか?
		※ *無効にすることができるか、に関する直接的な質問はない*	
10	管理区域外への持ち出しの際、起動パスワード等のアクセス制限機能または暗号化機能があるか？	STCF-1	機器は保存されているデータを暗号化できるか？

MDSとMDS2のマッピング例 3/3（ご参考）

MDS 5.0		MDS2（ANSI/NEMA HN 1-2019）	
項	質問	ID	質問
11	非常時アカウント又は、非常時機能を持っているか？	EMRG-1	機器には緊急アクセス（「ブレイクグラス」）機能が組み込まれているか？
12	「外部と個人情報を含む医療情報を通信する機能」や「リモートメンテナンス機能」を有するか？	MPII-3.7	機器は、外部ネットワーク（例：インターネット）上で個人識別可能情報を送信/受信するか?
		RMOT-1	機器は、機器の分析または修理のためのリモートサービス接続を許可するか?
12.1	なりすましの対策（認証）機能を有するか？		
12.2	データの暗号化が可能か？		
12.3	ネットワークの経路制御・プロトコル制御に関わる機能を有しているか？		
12.3.1	ネットワークの経路制御・プロトコル制御に関わる機能は、安全管理ガイドラインを満たす設定が可能か？		*MDS2は医療機器セキュリティのための製造業者開示説明書であるため、リモートサービスの具体的な実装に関する質問は含まれておらず、相当する質問はない。*
12.3.1.1	対応している通信方式はいずれか？		
	• 専用線，公衆網，IP-VPN，IPsec-VPN，TLS1.2以上　高セキュリティ型、クライアント認証		
12.3.1.2	ネットワークの経路制御・プロトコル制御に関わる機能の適正さ（回り込み対策を含む）を証明できる文書があるか？		
12.4	リモートメンテナンス機能を有するか？	RMOT-1	機器は、機器の分析または修理のためのリモートサービス接続を許可するか?
12.4.1	リモートメンテナンスサービスに関し、不必要なリモートログインを制限する機能があるか？	RMOT-1.1	機器は、所有者/操作者が機器の分析や修理のためのリモートサービスセッションを主導できるようにしているか?

SBOMの概要

- SBOM（Software Bill of Materials）とは、どのようなソフトウェアが入っているかを示す一覧
  - 医療機器に組み込まれたソフトウェアを構成するコンポーネント（OSS*3、OTSソフトウェア*4、自社開発モジュールなど）の一覧と、その属性情報を体系的に記録したもの
  - 脆弱性管理、ライセンス管理、ライフサイクル管理などのリスクベースアプローチの根拠となる情報
  - FDAは、サイバーセキュリティ対象となる「サイバーデバイス」の申請において、SBOMを含むサイバーセキュリティ関連文書の提出を要求

*3 Open Source Software
*4 Off-The-Shelf（既製品）ソフトウェア

※ 出典：厚生労働省「医療機器におけるSBOM導入・運用ガイドライン（第1版）」

なぜSBOMが必要なのか

- ソフトウェアの複雑化に伴い、利用ソフトウェアの把握が困難に
  - 医療機器は多数のソフトウェア部品から構成される
    - OS、ミドルウェア、各種ライブラリ、オープンソースソフトウェア、自社開発ソフトウェア
  - ソフトウェア脆弱性の公表件数は大幅に増加する傾向
  - 利用しているソフトウェアを把握していなければ迅速な影響評価が困難

SBOMを用いた脆弱性影響評価の流れ（医療機器製販業者の例）

- オープンソースや市販ソフトウェアの脆弱性が公開された場合

	ステップ	例／説明
1	脆弱性情報公開	• CVE-2026-109618, 109619：PHP2shell 公開 • 影響を受けるシステム - PHP 8.2.35より前の8.2系バージョン - PHP 8.3.36より前の8.3系バージョン - PHP 8.4.27より前の8.4系バージョン - PHP 8.5.12より前の8.5系バージョン
2	SBOMで利用コンポーネントを確認	SCA（Software Composition Analysis）ツールなどを用いてSBOMを確認し、対象製品を特定
3	影響の有無を評価	利用方法や設定が特定の発生条件に合致するか、影響評価を実施
4	セキュリティアドバイザリーの発行・対策実施	影響を受ける製品が発見された場合、その対策の立案から検証までを行い、セキュリティアドバイザリーを発行

SBOMのイメージ

- SBOMの例（イメージ）

	サプライヤー名	コンポーネント名	バージョン
1	Medical Device Co.	Medical-Application	1.1
2	Microsoft	Microsoft Windows 10 Enterprise LTSC 2019	10.017763.5329
3	Microsoft	Microsoft .NET Framework	4.8.03761.0
4	Microsoft	Microsoft SQL Server Express	14.0.1000
5	OpenCV.org	OpenCV	3.3.0
6	Google	Google Protobuf	2.0.0.668
	...	.....	.....

【SBOM活用上の留意点】

- SBOMは医療機器のソフトウェア構成を詳細に示す情報であるため、機密情報として適切な管理が必要
- SBOMは使用されているソフトウェアコンポーネントを示すものであり、脆弱性の影響有無は利用状況や設定、構成等を踏まえて別途評価が必要

SBOMの最小要素と提供フォーマット

- SBOMの最小限の要素

	要素	内容
1	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
2	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
3	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
4	その他の固有識別子	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
5	コンポーネントハッシュ	コンポーネントのバイナリを識別するために用いる暗号学的ハッシュ（オプション）
6	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ソフトウェアアーキテクチャー上の関係を特徴づける情報
7	SBOMの作成主体	SBOMエントリーの作成者
8	タイムスタンプ	SBOM データの集約を行った日時の記録(ISO 8601形式)

- SBOM導入・運用ガイドライン推奨するSBOMフォーマット
  - SPDX 2.2以上, CycloneDX 1.6以上

医療機関と医療機器事業者の継続的な情報共有

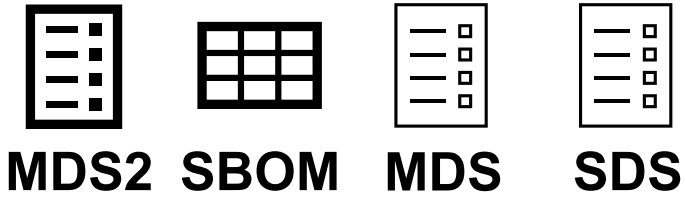
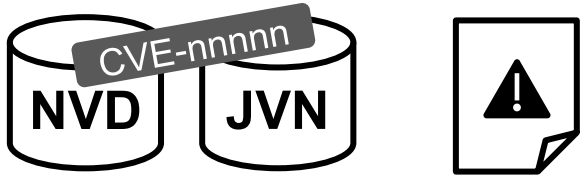
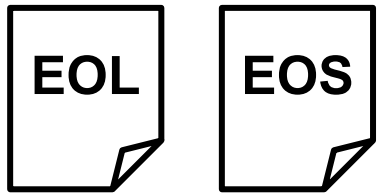
- 医療機器事業者から医療機関へ行うサイバーセキュリティ対策概要例

導入準備	運用	
	製品ライフサイクルにおける対応	インシデント発生時の対応
○ 製品セキュリティポリシーの作成と開示 ○ 製品保守計画の作成 ○ 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 ・ **セキュリティ文書**の作成・提示 – システム（ネットワーク）構成図 – 信頼境界 – MDS2 – SBOM – MDS – SDS	○ 製品寿命終了（EOL）、サポート終了（EOS）の通知 ○ 医療機関のEOS後の対応計画作成に関する支援・協力 ○ 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、**セキュリティ文書（MDS2, SBOMなど）**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	○ 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

※ 出典：厚生労働省「医療機関における医療機器のサイバーセキュリティ 確保のための手引書（第2版）」

まとめ

- 医療機関と医療機器事業者との情報共有と役割

医療機関	文書／情報	医療機器事業者
• セキュリティ文書を活用した医療機器のリスク評価	セキュリティ文書  	• MDS2やSBOMなどのセキュリティ文書の提供 • セキュリティ文書の継続的な更新
• 脆弱性情報やセキュリティアドバイザリーを活用した継続的な管理	脆弱性情報　アドバイザリー  	• 脆弱性評価結果やセキュリティアドバイザリーの提供
• EOL/EOSを考慮したライフサイクル管理	 	• EOL/EOS情報の提供

御清聴 ありがとうございました。