2026年度 JIRA-JAHIS合同報告会
2026.11.10

医療現場から見た
医療機器におけるサイバーセキュリティ対策

厚生労働省 政策統括官付 医療情報連携担当参事官室
大阪国際がんセンター
川眞田実

利益相反（COI）の開示

私は今回の演題に関連して、
開示すべき利益相反はありません。

本日の講演内容は私見を含むものであり、厚生労働省の公式見解をすべからく述べたものではありません

本日の内容

- 現在のサイバーリスクと医療DXについて
- 医療機関に求められる管理とは
- 医療現場の実態と構造的課題

高性能AIにより、脆弱性の発見から悪用までが高速化

01

探索

脆弱性の発見を高速化
AIがソフトウェアの解析や既知の脆弱性情報の分析が可能

02

侵入

未対策の外部接続点を悪用
未更新のVPN機器や遠隔保守用の接続経路などが侵入口に

03

被害拡大

院内の他システムへ波及
電子カルテ・PACS等への影響と個人情報の漏洩

求められる対応

①外部接続点の把握　**②脆弱性への迅速な対応**
③認証とアクセス制御　**④継続監視**

出典：政府8府省庁などによる注意喚起
「AI性能の高度化を踏まえたサイバーセキュリティ対策の強化について」（2026年5月18日）

外部接続点の適正化と維持管理の支援事業

外部接続点の「見える化」から、集約・アクセス制御・継続監視へ

医療機器の遠隔保守回線も含め、病院全体で接続を管理する体制へ（可能な範囲で）

01　支援対象

314病院

都道府県枠94施設＋国選定220施設

※支援対象
・電子カルテを導入している
・ネットワーク構成図や機器管理台帳を作成している

02　具体的な整備内容

接続点の適正化と維持管理体制作りの支援

物理的集約：
接続回線・境界機器の削減、集約

論理的集約：
通信経路・アクセス権限の一元管理

維持管理：
監視・設定管理・セキュリティ対策の継続

03　国による支援

計画＋設備補助

技術支援：委託事業者によるネットワーク統合計画の策定支援
設備補助：計画に基づく設備購入・構築費用を補助
400床以上350万円／399床以下200万円（当初予定額・補助率10/10）

外部接続点を病院全体で統制・維持管理することが目的

医療情報化推進方針

厚労省「医療DXで、より良い医療を、これからも。」



医療DXで、より良い医療を、これからも。

医療DX（デジタルトランスフォーメーション）とは、デジタル技術を活用して、
みなさん一人ひとりの医療や健康をよりよくする取組です。
より質の高い、安全で便利な医療を全国で実現し、未来の医療の発展にもつなげていきます。



今後の医療DXの推進方針・取り組むべき事項

❶ 全国で医療情報を共有できる基盤を整えます

マイナ保険証で より便利で安全に

マイナ保険証を使って、医療サービスをもっと便利で安全にします



全国で医療情報を共有できる基盤を整えます

患者さんの医療情報を医療機関などで安全に共有できる仕組みを全国に広げます



医療等の提供に必要な情報を、より安心・便利に共有し、
いつでもどこでも必要な医療を受けられるようにします

❷医療機関などのセキュリティを守ります

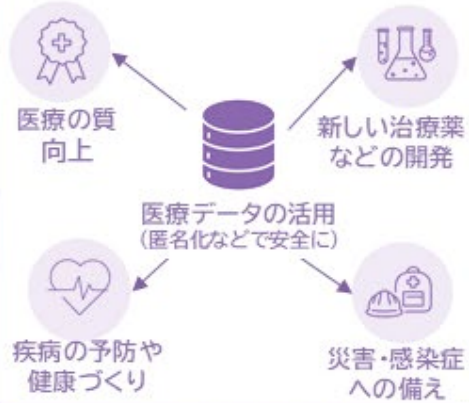
医療機関の情報システムをクラウド化することで、サイバーセキュリティ対策を強化します。



現場の負担を減らし、安心して医療DXを進められる環境をつくります

❸データを活かしてより良い医療と研究へ

医療の質の向上や、新しい治療法・医薬品の開発などにつなげます



データの力で未来の医療とみんなの健康を支えます

医療DXで期待できること

待ち時間の短縮・効率的な受診
手続がスムーズになり
待ち時間の短縮につながります

より良い医療を、どこでも
引越し後や旅行先でも今までの情報に基づいた医療が受けられます

安心安全な受診
本人確認や情報の共有で、誤りや重複を防ぎ、より安全な医療へ

未来の医療の発展
データの活用で、医療が進歩し、みんなの健康を支えます

医療情報化推進方針　概要

1．医療情報化推進の意義及び基本的な方向に関する事項

医療情報化推進の意義

「点で進んできたDXを、国がハブとなって“線”につなぎ、やがて“面”へ。」

個々の医療機関等の業務運用に即して構築してきた多様なデジタル基盤を、国が共通ルールや共通プラットフォームで束ね直し、民間の創意工夫を組み合わせ、日本全体で「つながるDX」へ再構築する。この再構築を通じて、以下の5点を実現する。

1. 医療等の現場におけるDXによる生産性向上やセキュリティ対策の徹底による **医療等サービスの安定的な提供**
2. 全国的な医療等情報の共有体制の整備による **医療等サービスの質の向上と患者の利便性向上**
3. 医療等情報の共有等による効率的なサービス提供とモダンな技術を活用したシステムへの刷新、医療費適正化に資する取組等による **制度の持続可能性の確保と国民負担の軽減**
4. PHRの一元的な把握を可能とすることによる **個人の健康増進への寄与**
5. 安全保障や危機管理の観点から自然災害や感染症危機に対応する **サービス提供体制の強靭化**

「国民一人ひとりにとって最適で質の高い医療等サービスが安定的・持続的に受けられる社会」を目指す。

医療情報化推進の基本的な方向

クラウド移行で3つを実現

「オンプレミスのたこつぼ化を越え、クラウドで基盤をつなぎ直す。」

「つながるDX」を実現するために、オンプレミスによるたこつぼ型の構造をつむぎ直し、共通ルールのもとで相互接続が可能なクラウド型基盤へと再構築していく。

業務効率化・生産性向上

医療情報システムのクラウド化により、AIを活用した業務効率化ツール等の導入を容易にし、業務効率化と生産性向上を実現

セキュリティ対策

クラウド化によりセキュリティ監視を強化し、サイバー攻撃への対応力を向上

データの共有

データ連携基盤の構築により、医療機関等との情報共有の円滑化、PHRの個人への還元、データの二次利用を促進

全国医療等情報プラットフォームの構築

医療機関や薬局、介護事業者、保険者、救急隊、自治体などが医療等情報を共有できるようにするとともに、国民もマイナポータル等で情報を閲覧・活用できる環境を実現する。

構築に当たっては、以下の点に留意して推進していく。

- ✓ DXサービス利用を効率的・計画的に行うための部局間連携の強化
- ✓ 電子カルテの認証制度活用によるベンダーへの改修要請
- ✓ 費用対効果を踏まえたシステムの導入判断
- ✓ ダッシュボードによる進捗・効果の見える化、国民の理解醸成

対象期間

※医療計画や介護保険事業計画のスケジュールを踏まえ、第1期は3年半、その後当面は3年ごととする予定。

目標

（2028年度までに）

- 電子カルテ普及率100%
  - 200床以上の病院（療養病床等が中心の病院を除く）の電子カルテ

（2030年末までに）

- 電子カルテ普及率約100%
  - 必要な患者の医療情報共有が可能な電子カルテ
- サイバーセキュリティ対策100%
  - 地域の拠点となる病院の対策100%実施
- クラウドネイティブ型の環境整備
  - 大病院向けのクラウドネイティブ型製品の提供

厚労省「医療情報化推進方針の概要について」。2026年10月1日

医療情報化推進方針(第1期:2026年10月～2030年3月)に基づき予定している主な取組



2029年度

- 【データ共有】 電子カルテ情報共有サービスで共有する情報を「歯科情報」に拡大
- 【自治体】 自治体検診情報を共有する仕組みについて全国展開 (※2029年度以降)

2028年度

- 【セキュリティ】 基幹インフラ制度の対象となる病院(特定機能病院を念頭)について、セキュリティ対策状況の点検等の対応を完了
- 【データ共有】 救急隊と医療機関が傷病者情報を共有するための「救急医療情報連携プラットフォーム」の全国展開 (※2028年度以降)
- 【医療】 200床以上の病院(療養病床等が中心の病院を除く)の電子カルテ普及率約100%
- 【医療】 医科・DPC向け共通算定モジュールのレセプト作成・請求事務を支援する機能や労災版モジュールを運用開始
- 【医療】 医療用医薬品の流通分野のキーコード(GS1コード)とYJコードを含む公的なデータベースの公開
- 【介護】 介護情報基盤について、全ての自治体で利用を開始(※2028年度を目処に目指す)
- 【二次利用】 公的データベースにおける仮名化情報や情報連携基盤の利用・提供の開始
- 【二次利用】 電子カルテ情報データベースの運用開始

2027年度

- 【電子カルテ】 電子カルテ情報共有サービス等に対応する認証クラウドネイティブ型電子カルテの普及開始
- 【電子カルテ】 標準型電子カルテ(導入版)の医療機関による導入を開始
- 【セキュリティ】 基幹インフラ制度の対象となる病院(特定機能病院を念頭)について、セキュリティ対策状況の点検等の対応を開始
- 【データ共有】 電子カルテ情報共有サービスで共有する情報を「訪問看護指示書・計画書・報告書等」に拡大

2026年度

- 【データ共有】 電子カルテ情報共有サービスについて、冬を目途に全国での運用開始
- 【医療】 医療費助成のオンライン資格確認について、全国規模での導入
- 【介護】 介護情報基盤について、介護保険システムの標準化対応が完了した自治体から、順次、利用を開始
- 【自治体】 予防接種事務について、予診情報・予防接種記録管理/請求支払システムの運用を開始し、デジタル化を順次開始
- 【自治体】 乳幼児健診等(特に集団健診)について、母子保健DXを環境が整った自治体から順次開始

本日の内容

- 現在のサイバーリスクと医療DXについて
- 医療機関に求められる管理とは
- 医療現場の実態と構造的課題

大阪急性期・総合医療センターのサイバー攻撃事例

2022/10/31 大規模システム障害

段階的に 手術・救急等を再開

12/12 基幹システム再稼働

2023/1/11 診療体制が完全復旧

43日 基幹システム再稼働まで

73日 部門システムを含む診療システム復旧まで

事例から見えた課題（調査報告書より引用）

01 外部接続の把握と管理
委託先・保守事業者の接続経路やアクセス権限を把握する

02 院内ネットワークの被害拡大防止
システム間の接続や通信を制御し、侵害の波及を抑える

03 診療継続と復旧への備え
システム停止を想定した代替運用と復旧手順を整備する

医療機器への示唆

機器単体ではなく、
接続環境を含めた管理が必要
医療機器単体に加え、電子カルテ・PACS・ネットワーク・外部保守を含む使用環境全体を管理する。だれが？

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 概要」（2023年3月28日）

被害に遭うということ

- ✓長期間の診療停止（患者）
- ✓多大な金銭的負担（病院）
- ✓個人情報の漏洩の可能性
- ✓社会的な信用喪失

初動対応調査：約１億円
被害額：復旧費用で数億円以上
診療制限などの損益は数10億円以上

医療情報の信頼性について

01
システム停止
必要な情報を利用し、診療を継続できるか

02
改ざん・混同
表示された情報を信じて診療してよいか

03
情報漏洩
患者のプライバシーと情報を守れるか

04
信頼喪失
何が変更されどの情報が正しいと判断できるのか

AIによりシステム侵入 → 改ざんの可能性
→ 情報の真正性が保証できなくなる → ？

保存された情報の真正性についてバックアップなど検討しましたが、
医療機器については少し観点が異なっていて、
情報の発生源は機器であるという事、つまり、生成された所から利用・復旧についての信頼性を考えていく必要があると考えています。

病院全体で確認すべき安全管理対策

01 資産管理・脆弱性

誰が対応するかを明確化
・OS・ソフトウェア等の更新とサポート期限を確認
・脆弱性修正、ウイルス対策の実施状況を把握など

02 認証・接続管理

どこから接続できるかを把握
・管理者権限、パスワード、ソフト導入制限
・外部接続、リモート保守経路と接続条件の管理

03 バックアップ・復旧

被害が発生しても復旧できるか
・オフラインバックアップの取得と保護
・復旧手順の整備、復元できることの確認

04 監視・初動体制

異常に気づき、被害拡大を防げるか
・ログの取得／管理、異常検知時の対応
・連絡体制、初動対応手順、証拠保全を整備

個別システムの対策だけでなく、病院全体で管理する仕組みが必要

医療機器においては、契約 接続 資産 運用の一体管理

01 契約・責任分界

誰が対応するかを明確化
・VPN・OS等の保守・更新担当を明記
・脆弱性情報の通知、障害時の対応を契約・SLAで規定
・サポート終了時の対応

02 外部接続・保守管理

どこから接続できるかを把握
・VPN・リモート保守経路を一覧化
・接続許可、利用者、接続時間、ログを管理
・作業記録などの管理も

03 医療機器・資産管理

部門調達の機器も一元的に把握
・CT・MRI・保守端末等を台帳管理
・接続先、OS、保守期限、構成変更を把握
・PACSとの接続機器一覧の把握

04 運用・点検体制

決めた対策が守られているか確認
・管理者権限、認証設定、通信制御を点検
・ログ監視、更新状況、是正結果を確認
・脆弱性発見時の対応、代替策の準備

医療機関と事業者が、それぞれの情報と役割を共有して管理する

医療機関と医療機器ベンダーの役割

医療機関側の対応

医療法施行規則　第14条第2項
サイバーセキュリティ確保のための必要な措置

医療情報システムの安全管理ガイドライン 第7.0版
組織管理体制、運用管理、技術対策など

チェックリスト／保健所の立入検査
対策の実施状況を確認

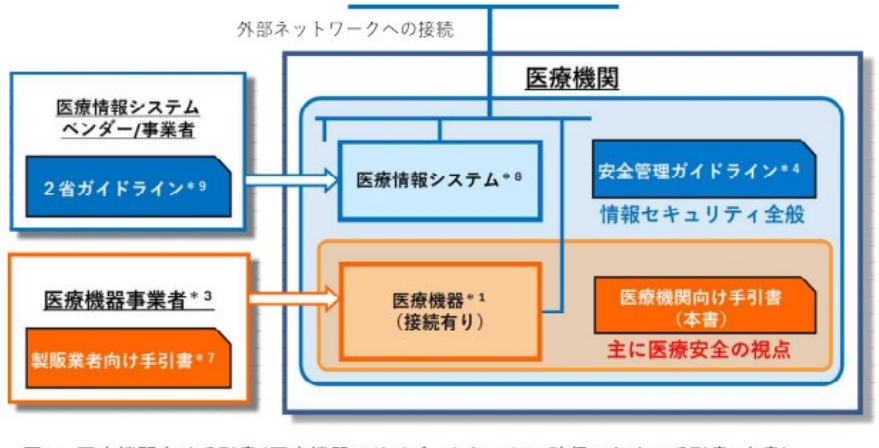
医療機器ベンダー側の対応

薬機法 基本要件基準 第12条第3項
ライフサイクル管理を通じたサイバーリスク対応

関連通知・製造販売業者向け手引書
安全な設計・製造、脆弱性への対応

市販後の脆弱性管理
脆弱性情報の提供、更新、サポート終了対応

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）



サイバーセキュリティ対策チェックリストについて

01 管理台帳

サーバ・端末・ネットワーク機器の台帳を整備し，管理対象を把握する

02 リモート保守

医療機関と事業者が、遠隔保守を利用する機器の有無を相互に確認する

03 MDS/SDS

事業者がセキュリティ開示書を提示し、医療機関が内容を確認する

04 BCP

医療機関は連絡体制・バックアップ・復旧手順を確認し、事業者も自社のBCPを整備する

本チェックリストの位置づけ

厚生労働省は、2023年4月1日から医療法施行規則第14条第2項を施行し、同時に医療法第25条第1項に基づく立入検査の項目へサイバーセキュリティ対策の実施状況を追加しました。つまり、法令上の義務を、立入検査においてチェックリスト等で確認する仕組みを設けている。医療機関では最重要項目。

本チェックリストにはMDS/SDSの記載があるものの、SBOMの取得・確認については記載がない。
現在、医療機器向け手引書（第2版）を踏まえ、MDS2・SBOM等の提供・確認や継続的な情報更新についても、今後の改訂での整理を期待したい。

医療機関側でもライフサイクル全体で管理が必要

医療機器のライフサイクルマネジメント

1.導入時（契約・責任分界の明確化）

接続環境などの必要情報（MDS2・MDS・SDS・SBOM等）を収集し想定されるリスクを把握し、受容可能なレベルまで低減するというマネジメント

2.運用時（継続的なリスク評価と対策）

脆弱性情報や使用環境の変化を継続的に把握し、診療への影響を踏まえてリスクの再評価が必要。リスクの変化を把握し、対策を継続的に見直すマネジメントが求められる。

令 和 8 年 9 月 2 4 日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の改定についてより引用

医療機器のライフサイクルマネジメント

導入前｜安全に利用できる環境を整える

- ✓ 使用環境・接続要件・セキュリティ仕様の確認
- ✓ MDS2等の製品情報、保守条件、EOL・EOSの確認
- ✓ 導入時のリスク評価と保守・更新の責任分界の協議

導入時｜構成と管理責任を明確にする

- ✓ 機器台帳・ネットワーク構成図・接続経路の更新
- ✓ 認証設定、リモート保守経路、実際の稼働状況の確認
- ✓ 保守契約、連絡窓口、インシデント対応手順の確定

運用中｜変化への必要な対策を実施する

- ✓ 構成変更、脆弱性情報、更新・保守状況を継続的に確認
- ✓ 該当機器・診療影響を踏まえたリスク評価
- ✓ 事業者と調整して更新・補完的対策を実施・記録

更新・終了｜サポート終了後への対応

- ✓ EOL・EOSを踏まえた更新・廃止・ネットワーク分離の計画と実施
- ✓ 継続使用が避けられない場合の補完的対策とリスク評価
- ✓ 機器廃止時のデータ消去・接続解除・台帳更新

医療機関とベンダーが連携して導入から更新まで、継続的にリスクを評価・管理する

医療機器事業者も積極的にリスクマネジメントを実施し、脆弱性情報を開示して、相互に連携して対策を実施する必要があります

令和８年９月２４日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の改定についてより引用

SBOMは医療機器の脆弱性を把握するための情報

2026年8月25日 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）」

SBOM

ソフトウェア構成の把握
製品に含まれるソフトウェアの名称・バージョン・依存関係等を把握し、脆弱性の影響調査に活用する情報

MDS2/MDS/SDS

セキュリティ機能・対策を把握
製品・サービスのセキュリティ機能、設定条件、運用上の注意事項などを確認するための開示資料

◆**ベンダー**はSBOMを作成・更新し、販売時・変更時の提供を基本とするとともに、脆弱性情報を継続的に収集・評価する。医療機関に必要な情報と対策を主体的に提供し、SBOMの提示要請にも対応できる体制を整える。

第3.2節「SBOM導入・運用体制およびプロセス」第6.2.1～6.2.2節「脆弱性情報の収集・照合、影響評価」

◆**医療機関**は使用機器と接続環境を把握し、SBOMや事業者から提供される脆弱性情報を基に、診療への影響を評価し、必要な対策を協議する。

医療機関向け手引書（第2版）第4.3節（1）③「医療機器の使用環境全体のセキュリティ情報収集」

SBOMだけでは、医療機関は対応の必要性を判断できません

例えば、CT装置に含まれるソフトウェア部品に脆弱性が公表された場合

- ◆ 医療機関は、SBOMによって該当部品の存在は把握できても、その脆弱性が医療機器にどのような影響を与えるのか、実際に悪用可能なのかを医療機関だけで判断することは難しい（この情報が欲しいです）。
- ◆ SBOM導入・運用ガイドラインでは**将来的**に、VEX（Vulnerability Exploitability eXchange）等を組み合わせ、製品への影響の有無を提供する事にも言及しています。
- ◆ 医療機関が求めているのは、製品への影響、対応の緊急度、更新方法や対策方法など、実際の対応を判断できる情報である。

ベンダーは製品への影響と必要な対策を示し、医療機関は診療への影響を評価する
双方の継続的な情報共有と連携が不可欠。

SBOM導入・運用ガイドライン第1版、第5.3.3節

医療機関のSBOM認知と課題

01 認知・依頼時期

導入時に求めていない例が多い
導入後に要望するケースはまだ少ない

02 用語・窓口

SBOMという用語や目的が十分共有出来ていないケースが見られる。
窓口でも通じないケースもある。

03 回答状況

一部では依頼しても、返信なし・未提出など入手できない事例もある

04 提出条件

NDA等を求めるケースもある
対象範囲、更新方法等異なる例もある

本日の内容

- 現在のサイバーリスクと医療DXについて
- 医療機関に求められる管理とは
- 医療現場の実態と構造的課題

管理情報は分断されやすい（大変なこと）

ネットワークを介して連携している

電子カルテ	RIS	医療機器	PACS

医療情報システムは相互に接続されている一方、導入・接続・保守を担う関係者は院内の複数部門で分担

事務部門
機器購入・保守契約・予算管理など

医療情報部門
システム運用管理・ネットワーク管理など

診療部門
日常運用・検査品質・機器選定など

ベンダー・卸業者
定期点検・故障対応など

管理境界で生じる問題
外部保守接続の把握・承認部門はどこなのか
脆弱性が通知されたとき、対象機器・担当者など特定が困難な場合もある

診療を続けながら、脅威の変化への対応の難しさ

- **診療が優先**
  CT・MRIなどは日中稼働しており、設定変更や更新作業は診療終了後になりやすい
- **管理している機器やシステムが多い**
  多数の装置について、構成情報、接続先、脆弱性情報、更新状況を把握する必要がある。
- **限られた人員での対応**
  診療業務と並行して、情報収集、メーカーへの確認、院内調整、記録まで担っている。
- **対応の判断が難しい**
  更新による機能への影響や装置停止の可否は、現場だけで判断できないことがある。

継続的な安全管理には、医療機関の人材育成・体制整備と、事業者の支援が必要

放射線部門で起きやすい構造的問題

1. 放射線部門の組織・教育体制
   - 部門内のITリテラシー・セキュリティの知識や経験に差がある
2. 機器導入は一大イベント
   - 高機能・高性能な機器を求めるため、導入コストが高くなる
   - 調達時は様々な事柄に注視（購入後は機能面・運用面に意識）
   - 導入後の安全管理を行う体制が検討・構築されない
3. 医療機器に関しては責任の所在が分散しやすい
   - 調達は事務、装置は放射線部、保守も放射線部門
   - ネットワークも放射線部門・・・曖昧？
4. 医療機器であると同時にIT機器であるという認識はない

個人の意識だけでなく、導入時に運用・保守・更新まで決める仕組みが必要

診療技術への関心と、運用管理にむけて

セキュリティ管理も製品選定時から考えて行くために、

01

教育

育成校において一定の情報セキュリティ教育を受けているものの、機器の運用管理などにおけるセキュリティ教育は受けていない

02

導入

最善の医療を提供するという観点から、画質・被ばく・性能・使いやすさにおいて熱心に検討をする。

03

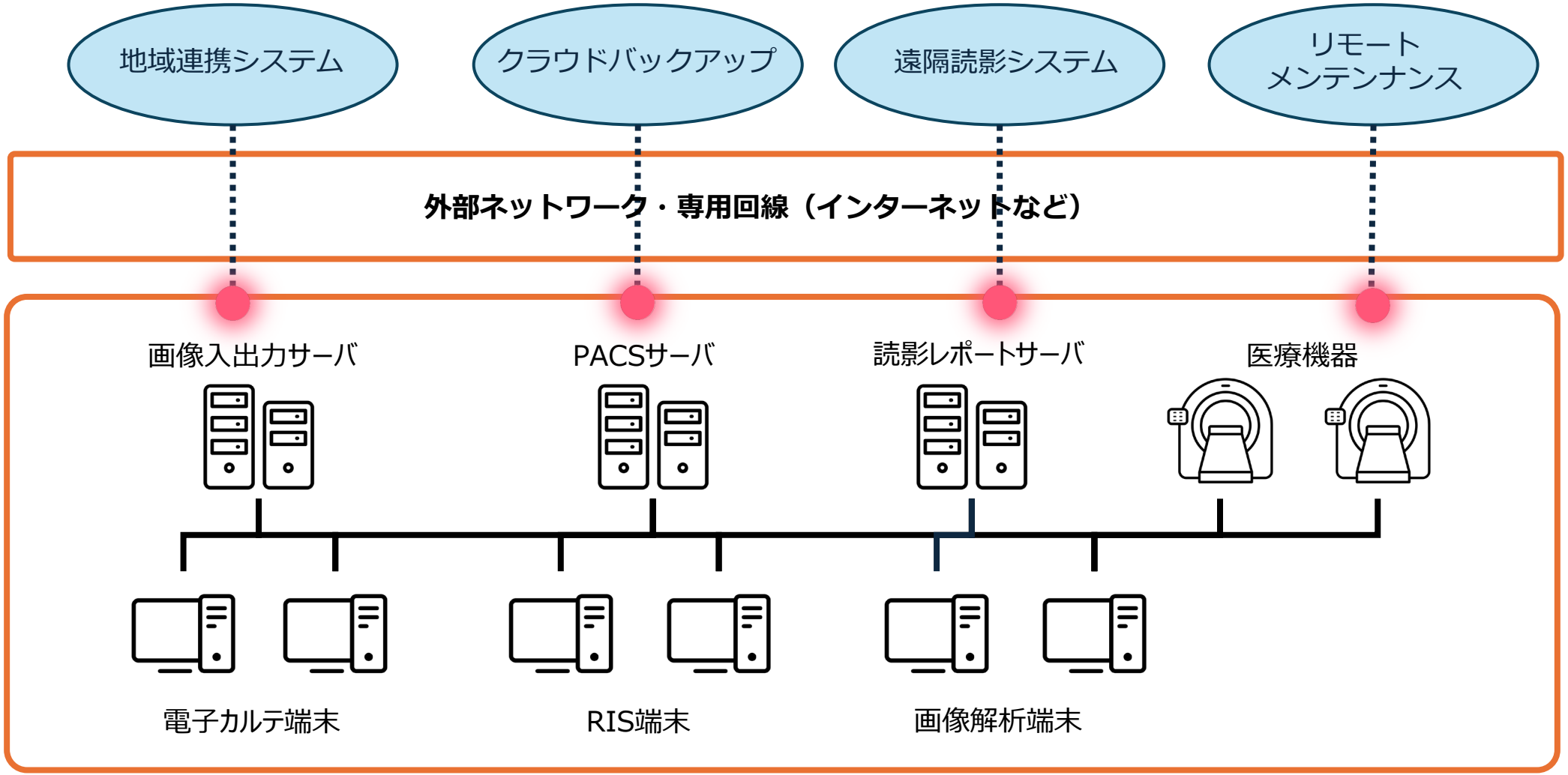
導入後

接続管理・更新・脆弱性対応等は導入後に個別対応となる場合が多い

医療従事者個人の問題ではなく、教育・調達・運用をつなぐ仕組みの課題であり、

今後は、技術向上への熱心さと、調達時からの運用設計につなげたい。

放射線部門には多様な外部接続経路が存在する



多くの院外接続部分が存在しており、全体把握と統制が必要

リモート保守で確認すべき項目

01 対象・所在

対象機器とその設置場所
保守事業者と接続元環境
ネットワーク機器

02 接続・認証

回線種別
接続方式と認証・権限
接続許可と停止方法

03 監視・記録

作業申請と実施記録
不正通信監視
ログ保存先・期間

04 契約・継続管理

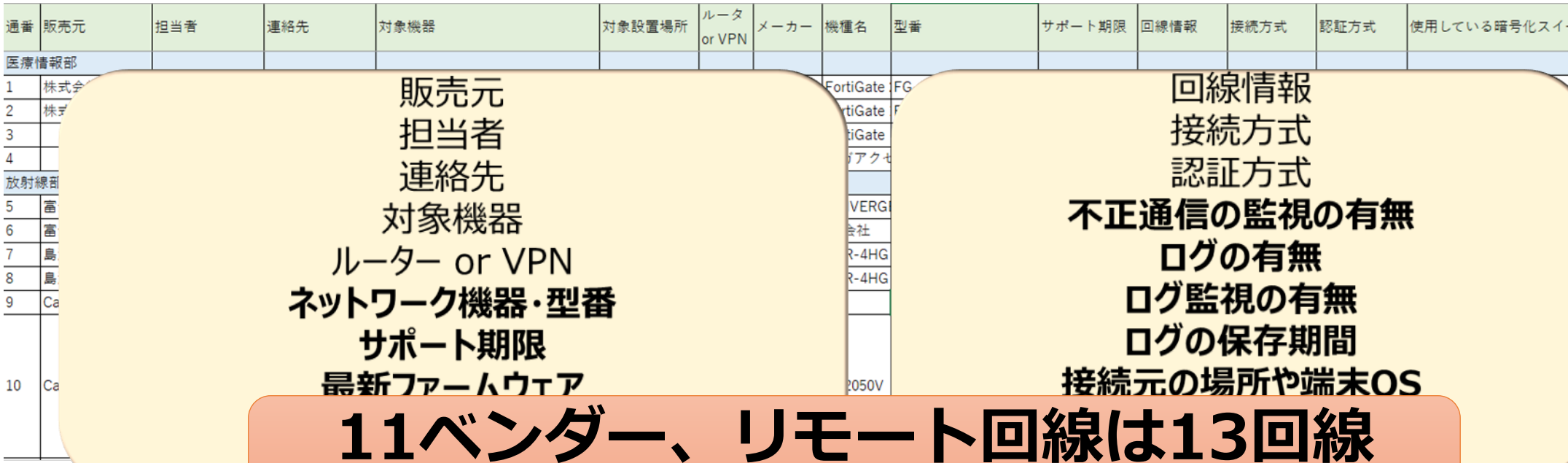
SDS/SLA
ファームウェア／脆弱性更新日
サポート期限／緊急対応

実調査で明らかになった管理対象の広がり

放射線部門における医療機器（32台）

一般撮影系装置：10台、CT：5台、MRI：3台、TV透視装置：5台

血管撮影装置：3台、PET/SPECT装置：2台、放射線治療装置：4台



11ベンダー、リモート回線は13回線

薬剤部門：3回線、臨床工学部門：6回線、臨床検査部門：7回線

放射線技師の教育カリキュラム（102）

Ⅰ.　基礎分野（14）

Ⅱ.　専門基礎分野（31）

1.　人体の構造と機能及び疾患の成り立ち

2.　保健医療福祉における理工学的基礎並びに放射線の科学及び技術

Ⅲ.　専門科目

1.　診療画像技術学・臨床画像学（18）

2.　核医学検査技術学（6）

3.　放射線治療技術学（7）

4.　医療画像情報学（6）

5.　放射線安全管理学（4）

6.　医療安全管理学（2）

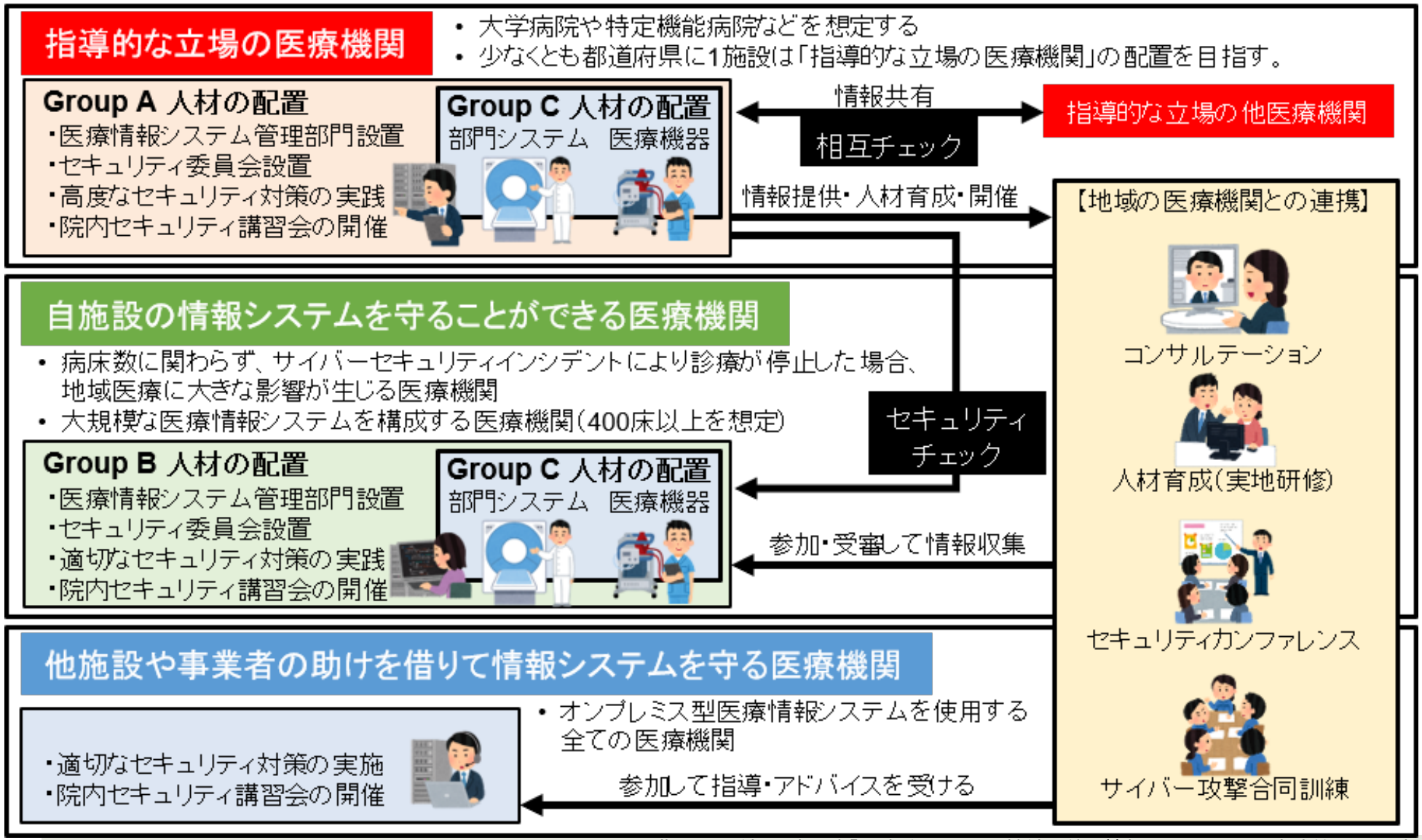
7.　実践臨床画像学（2）

Ⅳ. 臨床実習（12）

令和3年4月 カリキュラムの改定
新たな知識・働き方改革・医療DX

診療放射線技師学校養成所指定規則より抜粋・改変

医療機関の機能に応じたサイバーセキュリティ人材の配置



出典：厚労科研・武田班「医療分野における持続可能な情報セキュリティ人材育成等に関する提言」図1（2025年5月30日）

まとめ

- ◆医療DXの進展に伴い、医療機器は接続環境も含めた継続的なリスク管理が必要
- ◆医療現場では、管理情報と責任が分散し、診療と両立した対応が難しい
- ◆ベンダーの方々の協力を得ながらの診療継続を目指したい
- ◆導入時から運用・保守・更新が設計できる組織体制と、人材育成を共に進める必要があると考える