2026年度 JIRA-JAHIS合同報告会

「医療機器・医療情報システムにおける サイバーセキュリティ対策の重要性再認識」
― 患者安全と医療継続性を支えるために ―

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　委員長　堀野誠人



本日お伝えしたいこと

医療機器・医療情報システムにおけるサイバーセキュリティで第一に考えるべきことは

- 医療継続性への対策
- 患者安全への対策

医療現場を守るためには、関係者全ての連携が必要

- 医療機関、医療機器／医療情報システムベンダー、保守委託事業者等

厚労省安全管理ガイドライン7.0版（以降、安全管理GL7.0と略記）や医療機器規制も、この方向性を強く示している。

医療機関を取り巻く脅威の変化

近年の特徴

- ランサムウェア攻撃の増加
- VPN装置の脆弱性悪用
- リモート保守経路の侵害
- サプライチェーン攻撃
- クラウドサービスを狙う攻撃

被害が発生すると

- 電子カルテ停止
- 画像配信停止
- 検査停止
- 診療制限

発生時期	医療機関	被害概要	診療への影響	主な原因・特徴
2021年10月	つるぎ町立半田病院（徳島県）	LockBitによるランサムウェア被害	約2か月診療制限	VPN脆弱性、セキュリティ対策不足
2022年10月	大阪急性期・総合医療センター	電子カルテ等基幹システム暗号化	全面復旧まで約73日	給食業者経由のサプライチェーン攻撃、VPN脆弱性、責任分界不明確
2024年3月	国分生協病院（鹿児島県）	ランサムウェア被害	救急・新規外来を約10日停止	リモート保守用回線の設定不備、対象サーバーのウイルス対策不足
2024年5月	岡山県精神科医療センター	電子カルテ停止、約4万人分の患者情報漏えいの可能性	約3か月で全面復旧	VPN脆弱性放置、弱いパスワード、管理者権限乱用
2026年2月	日本医科大学武蔵小杉病院	ナースコールサーバー3台が被害。約13万件の患者情報漏洩の可能性	診療停止は無し	リモート保守用回線の設定不備、VPN脆弱性

活動中の81ランサムウエアのうち、約50が医療機関を標的としている※

※ 出典：Cyfirma社レポート（シンガポールのサイバーセキュリティ企業）

サイバー攻撃がもたらすリスク

Confidentiality（機密性）へのリスク　…　患者情報の漏えい
Integrity（完全性）へのリスク　…　データ改ざん
Availability（可用性）へのリスク　…　システム停止

患者安全への影響

「診断遅延」「治療遅延」「医療提供停止」につながる可能性がある。

行政・業界の方向性

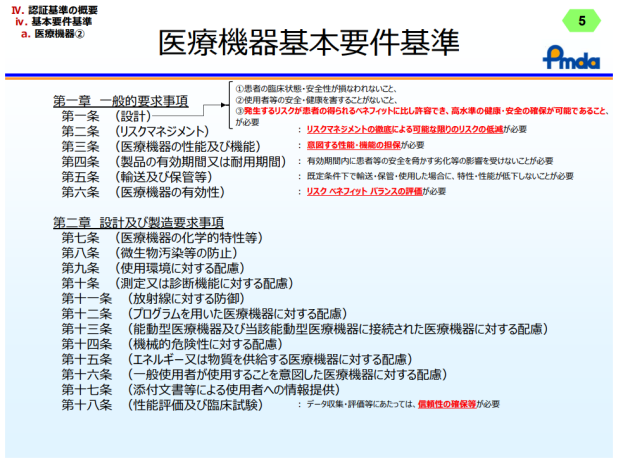
- 医療情報システム事業者
  - ➢二省GL（経産省・総務省）
- 医療機関、事業者
  - ➢安全管理GL7.0（厚労省）
- 医療機器業界
  - ➢医療機器基本要件基準
  - ➢IMDRF
  - ➢JIS T 81001-5-1



二省ガイドライン（出典：経済産業省）
https://www.meti.go.jp/policy/mono_info_service/healthcare/teikyoujigyousyagl.html



医療情報システムの安全管理に関するガイドライン第7.0版（令和8年6月）｜厚生労働省
出典：厚生労働省



https://www.pmda.go.jp/files/000240068.pdf
出典：独立行政法人 医薬品医療機器総合機構

全てが「サイバーセキュリティを前提とした医療提供体制」へ向かっている

二省GL2.0版のポイント

① 対象事業者の明確化
② 合意内容の明確化
③ リスクコミュニケーション
④ 安全管理対策の開示
⑤ SLA・責任分界

対策内容を開示し、
医療機関と合意し、
継続的に共有する

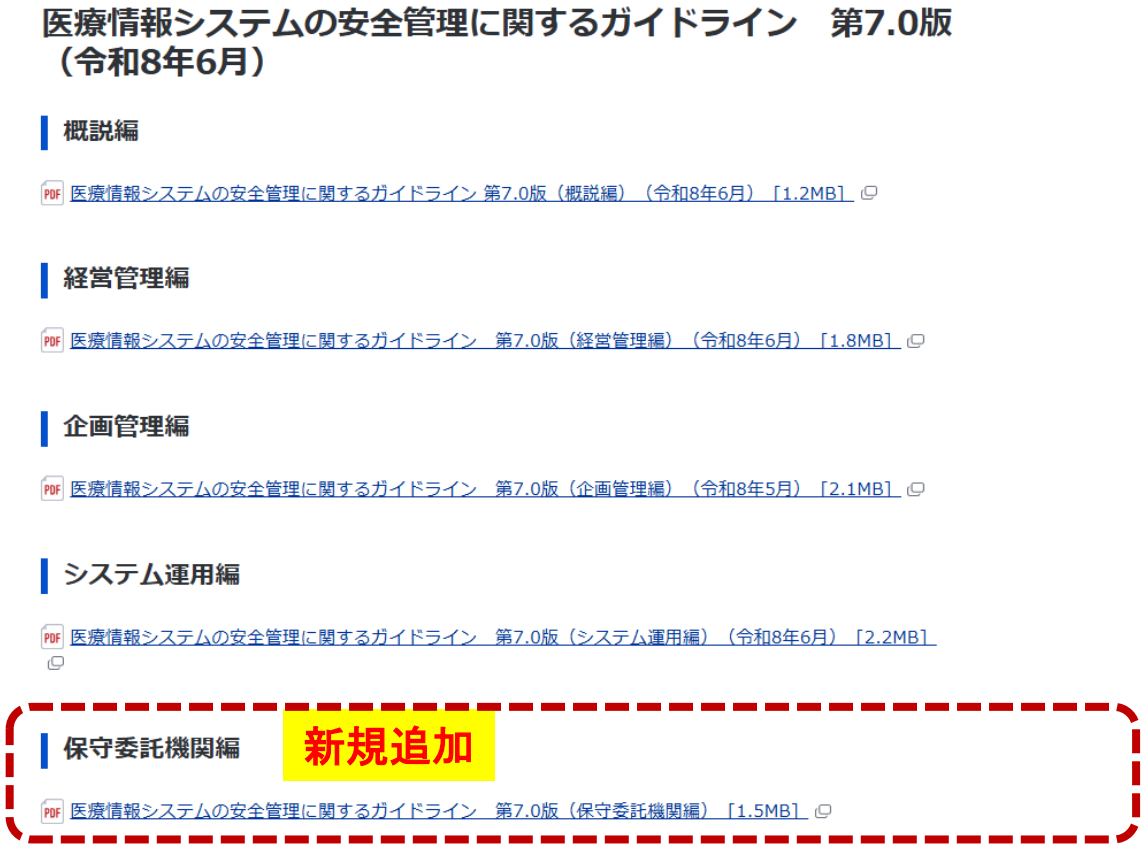


二省GLの考え方は、厚労省の安全管理GLへ引き継がれる
医療の安全は医療機関と関係事業者が共同で守ることがより明確化

厚労省安全管理GL7.0版のポイント

改定のキーワード

- 保守委託機関編の新設
- 二要素認証の明確化
- クラウド利用の整理
- サプライチェーンリスクへの対応
- 責任分界の明確化
- 医療の継続計画強化



医療情報システムの安全管理に関するガイドライン　第7.0版
（令和8年6月）

概説編

医療情報システムの安全管理に関するガイドライン 第7.0版（概説編）（令和8年6月）［1.2MB］

経営管理編

医療情報システムの安全管理に関するガイドライン　第7.0版（経営管理編）（令和8年6月）［1.8MB］

企画管理編

医療情報システムの安全管理に関するガイドライン　第7.0版（企画管理編）（令和8年5月）［2.1MB］

システム運用編

医療情報システムの安全管理に関するガイドライン　第7.0版（システム運用編）（令和8年6月）［2.2MB］

保守委託機関編　新規追加

医療情報システムの安全管理に関するガイドライン　第7.0版（保守委託機関編）［1.5MB］

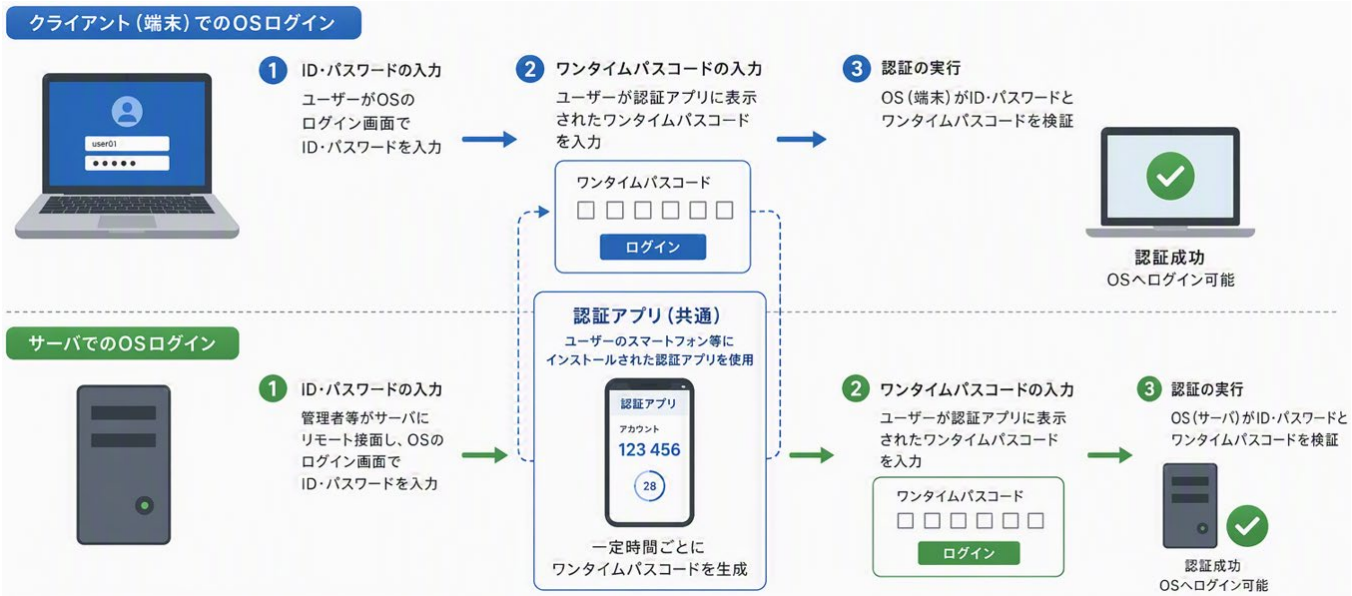
医療情報システムの安全管理に関するガイドライン　第7.0版（令和8年6月）｜厚生労働省
出典：厚生労働省

「医療機関単独で守る」から「関係事業者と共同で守る」へ

特に重要なポイント① 二要素認証

安全管理GL7.0では二要素認証対応を明確化

- クライアント端末
- サーバ機



医療機器やレガシーシステムでは課題が存在

- 医療機関特有の理由
  - ✓ マスク・手袋等で生体認証が使えない等
- 技術的制約
  - ✓ 環境が古くソフトウェアの改修が困難等

例）個人スマホ等への認証アプリ導入による二要素認証
・ ID/パスワード（記憶）＋スマホ認証アプリ（物理）

※次期7.1版では、一時的も含め医療データを保持している装置を含めてサーバと位置付け、アクセス時の二要素認証を求める方向へ議論が進んでいる

医療機関とベンダーの協議が重要

特に重要なポイント② 責任分界

これまで．．．

- ベンダーに任せている

これから．．．

- ベンダーが対応する内容
- 医療機関が対応する内容

を明確化

チェックリストで責任分界に認識の齟齬が無いかを確認

令和8年度

医療機関・薬局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8年度中にすべての項目で「はい」または「対象外」にマルが付くよう取り組んでください。

・「はい」　：医療機関・薬局との保守契約範囲に含まれる項目であり、事業者側の責任で対応できていることを指します。
・「いいえ」：医療機関・薬局との保守契約範囲に含まれる項目であるが、事業者側が対応できていない項目となります。
　事業者としての令和8年度中の対応目標日を記入してください。
・**「対象外」：医療機関・薬局との保守契約範囲外となり、当該項目の責任を医療機関・薬局が負います。**
　医療機関・薬局に対して、責任分界の認識齟齬がないか、事業者側から必ず確認して下さい。

	チェック項目	（日付） 確認日	（日付） 目標日	備考
1 体制構築	①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。	はい・いいえ (/)	(/)	
	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医療機関等に伝えた。	はい・いいえ (/)	(/)	
	③医療機関等に製造業者/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 (/)	(/)	
	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。※管理者権限対象者の明確化を行っている。	はい・いいえ・対象外 (/)	(/)	
	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または無効化している。	はい・いいえ・対象外 (/)	(/)	
	⑥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・対象外 (/)	(/)	
	⑦パスワードは英数字の混在した8桁以上としている。 ※二要素認証を採用するまでの期間は13桁以上としている。	はい・いいえ (/)	(/)	
2 医療情報シス	⑧パスワードの使い回しを禁止している。	はい・いいえ (/)	(/)	

安全管理GL7.0では責任分界の確認を重視

特に重要なポイント③ 医療の継続計画（BCP）

サイバー攻撃を想定したBCP

- 予防だけでは不十分
- 被害発生を前提

求められる内容

① バックアップ
② 復旧手順
③ 連絡体制
④ 訓練



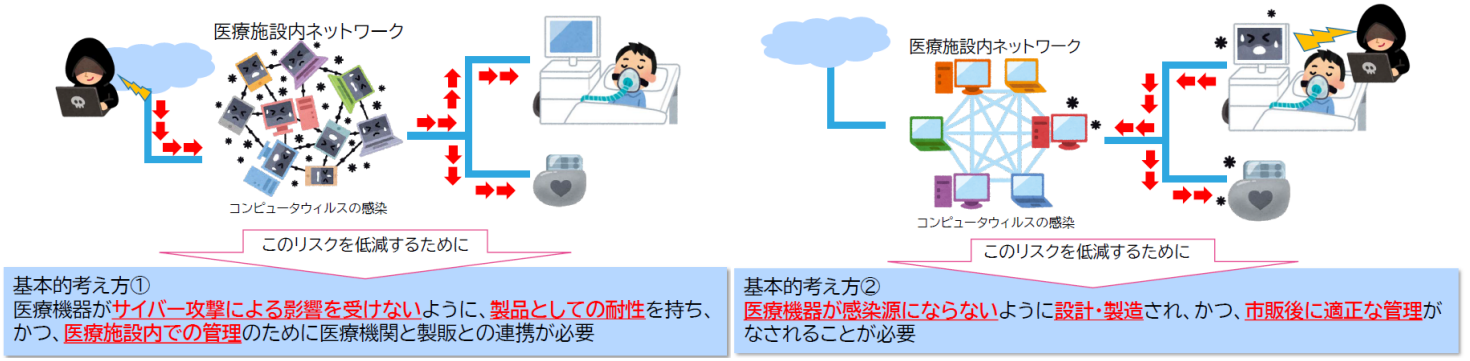
「止めない」だけでなく「復旧できる」が重要

医療機器基本要件基準改正（2023年）

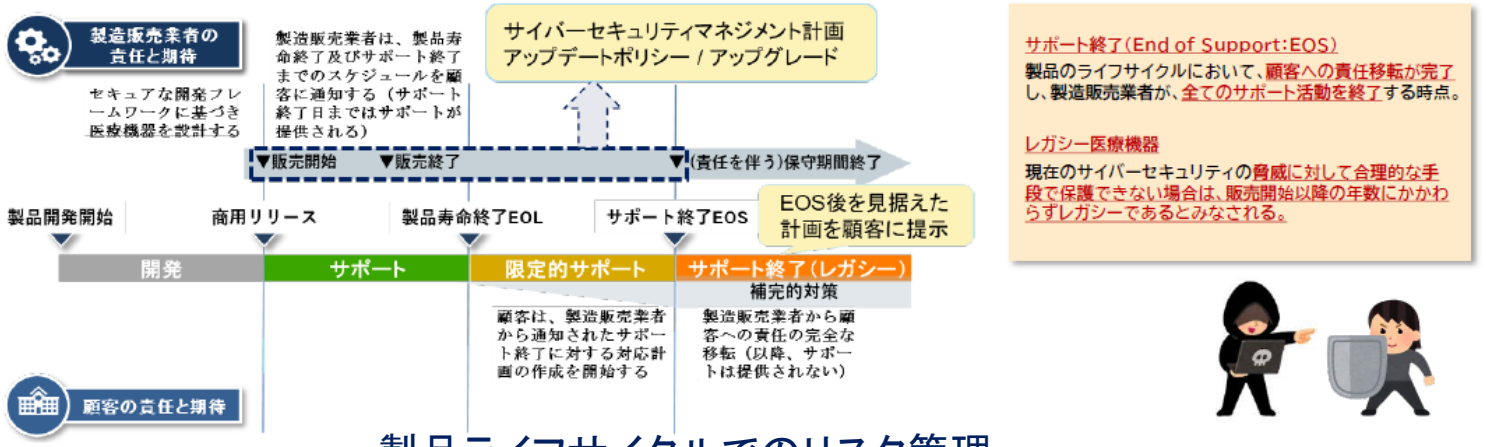
要求事項（第12条3項）

- サイバーリスク評価
- リスク低減措置
- ライフサイクル全体での管理

が求められるようになった



サイバーリスクの評価・リスクの低減措置



製品ライフサイクルでのリスク管理

Copyright © Ministry of Health, Labour and Welfare of Japan and Pharmaceuticals and Medical Devices Agency, All Rights Reserved.

医療機器サイバーセキュリティの考え方

医療機器はネットワークにつながることで利便性が向上する一方
攻撃対象にもなる

【重要な考え方】

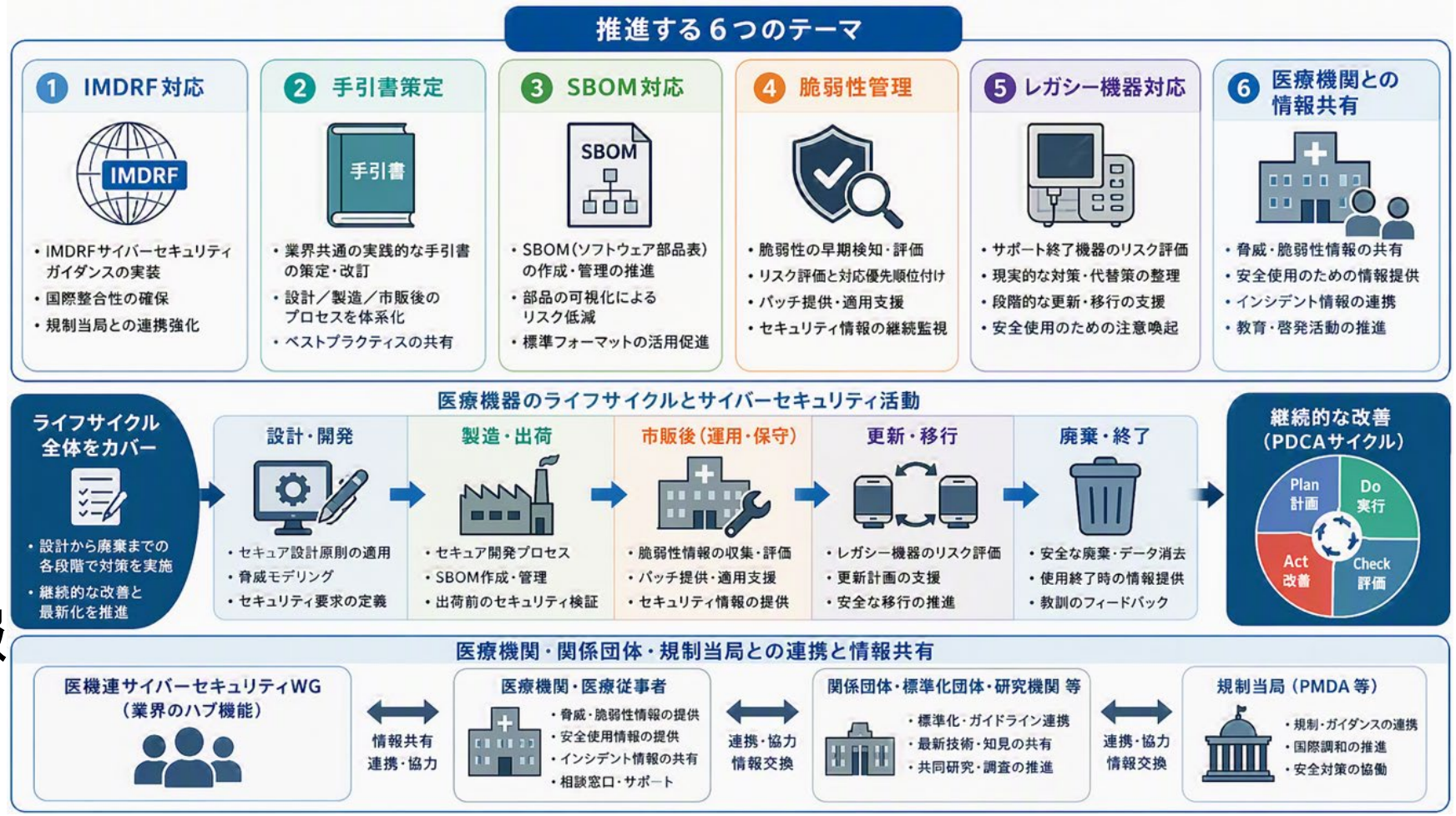
- TPLC（Total Product Life Cycle）
  - ➢設計、製造、市販後保守、廃止まで含めて管理する



医機連サイバーセキュリティWGの取り組み

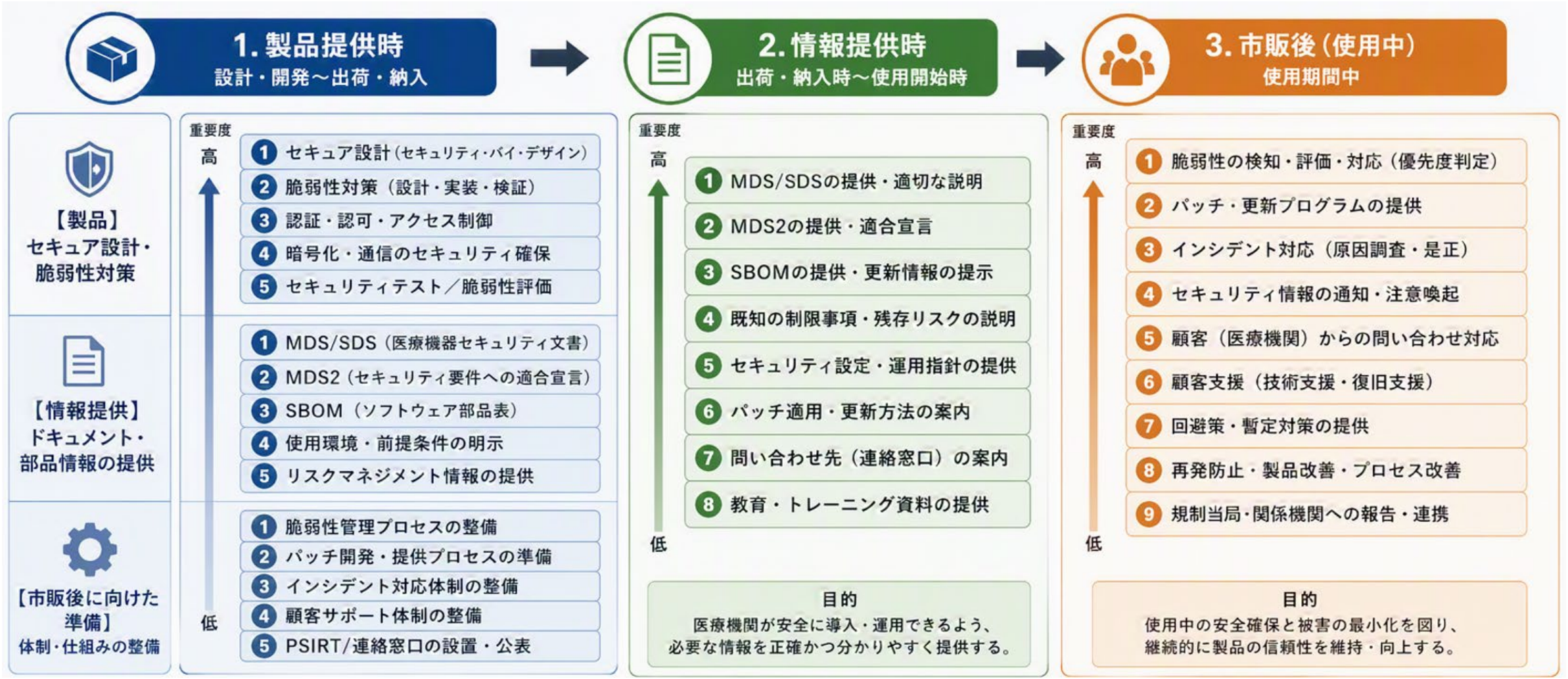
JIRAが参加する医機連CS-WGでは以下を推進

① IMDRF対応
② 手引書策定
③ SBOM対応
④ 脆弱性管理
⑤ レガシー機器対応
⑥ 医療機関との情報共有



キーワードは「共同での取り組み」「情報共有」「継続的改善」

医療機器ベンダーに求められること



製品のライフサイクル全体を通じて、医療の安全・安心を支える責任を果たすことが重要

医療情報システムベンダーに求められること

システム提供
安全・安心なシステムを提供

運用支援（継続的なセキュリティ確保）
導入後も安全に運用できるよう支援

安心・安全な医療の実現
医療の質向上と信頼確保に貢献

システムベンダーが提供・支援する主な内容

医療機関（利用者）



医療従事者・事務職員



院内ネットワーク・端末

多要素認証（MFA）対応
- 多要素認証の仕組みを提供
- 設定支援・導入支援
- 利用方法の周知・教育支援



ログ管理
- ログ取得・保存の仕組み提供
- 保管ポリシーの設定支援
- ログの監視・分析支援
- インシデント調査への活用支援

リモート保守管理
- 安全なリモート接続環境の提供
- アクセス制御・操作記録
- 保守作業の事前承認・通知
- 定期的な接続点検

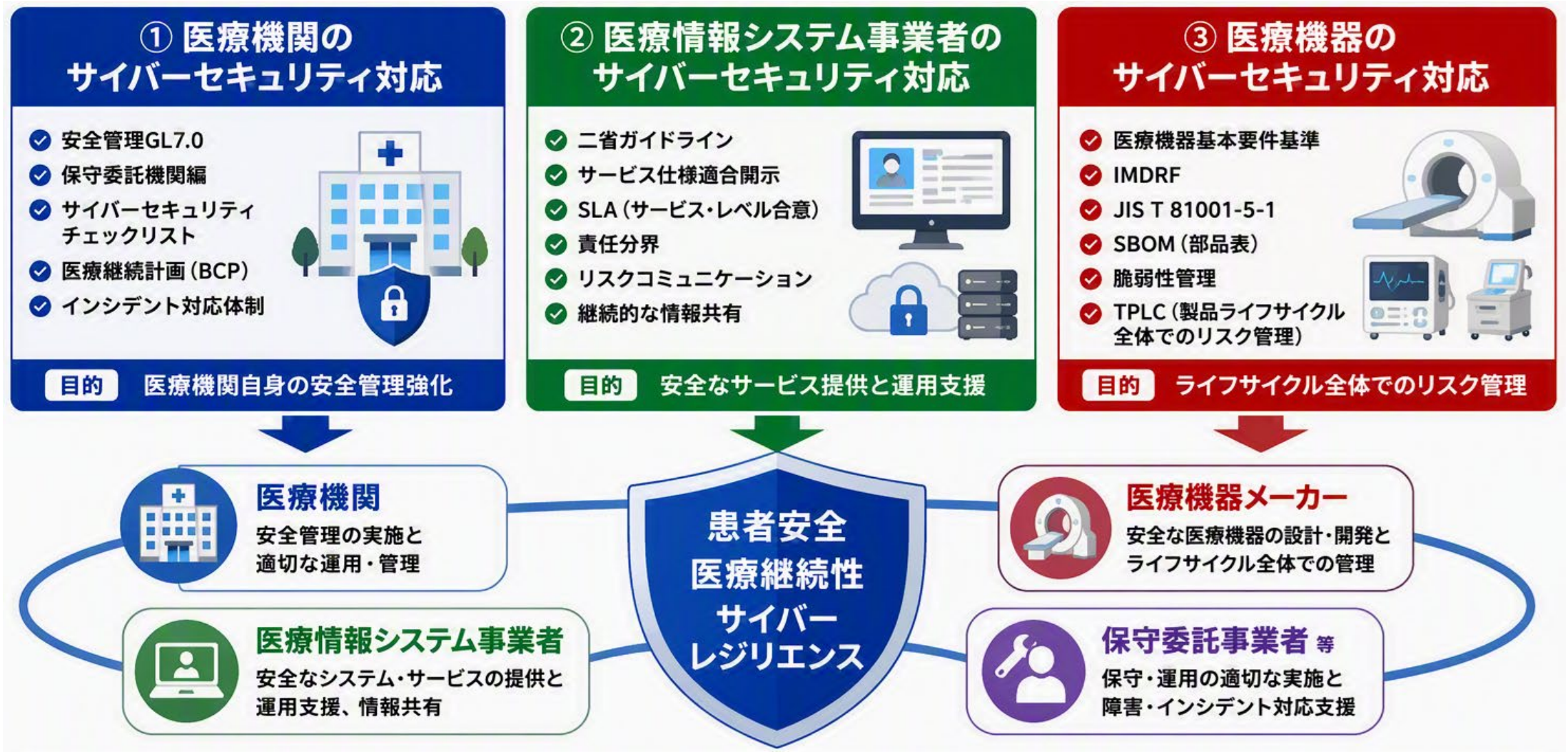
クラウドセキュリティ
- 安全なクラウド基盤の提供
- データの暗号化・アクセス制御
- 脆弱性管理・パッチ適用
- 可用性・バックアップ確保
- クラウド設定の最適化支援

運用・監視・サポート
- 24/7監視（障害・セキュリティ）
- アラート通知・一次対応
- 問合せ対応（ヘルプデスク）
- インシデント対応支援
- 定期レポート・改善提案

アップデート・脆弱性対応
- セキュリティ更新の提供
- 適用計画の案内・支援
- 影響調査・検証
- 適用作業の実施支援
- 既知の脆弱性情報の提供

責任分界点を明確にし、システム提供だけでなく運用まで含めた支援が必要

JIRA・JAHISが関わる活動の方向性



JIRA・JAHISはそれぞれの方向からの患者安全、医療継続性の確保を支援します。

御清聴 ありがとうございました。