独立行政法人 医薬品医療機器総合機構
Pharmaceuticals and Medical Devices Agency

IMDRF活動報告会：Cybersecurity WG

独立行政法人　医薬品医療機器総合機構
医療機器調査・基準部　医療機器基準課
関水 英正

内容

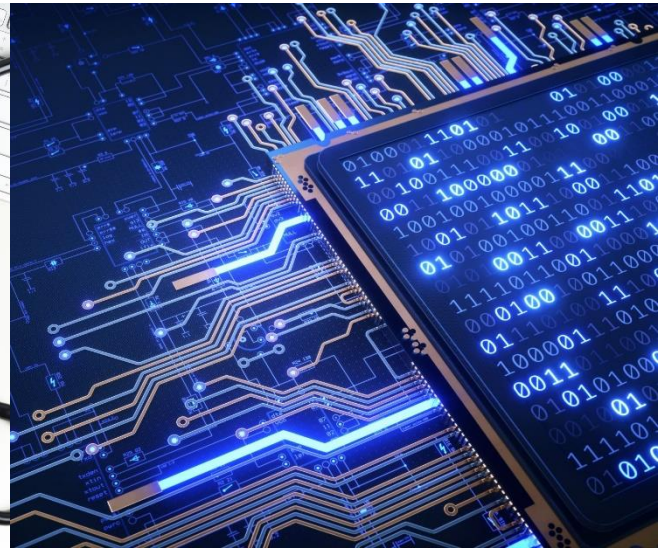
- IMDRF Cybersecurity WGの目標
- IMDRF Cybersecurity WGの活動経緯、予定
- サイバーセキュリティガイダンスの概要
- 追補ガイダンスの開発について

本講演の意見に係る部分は、演者の個人的見解であり、
PMDAの公式見解ではありません。

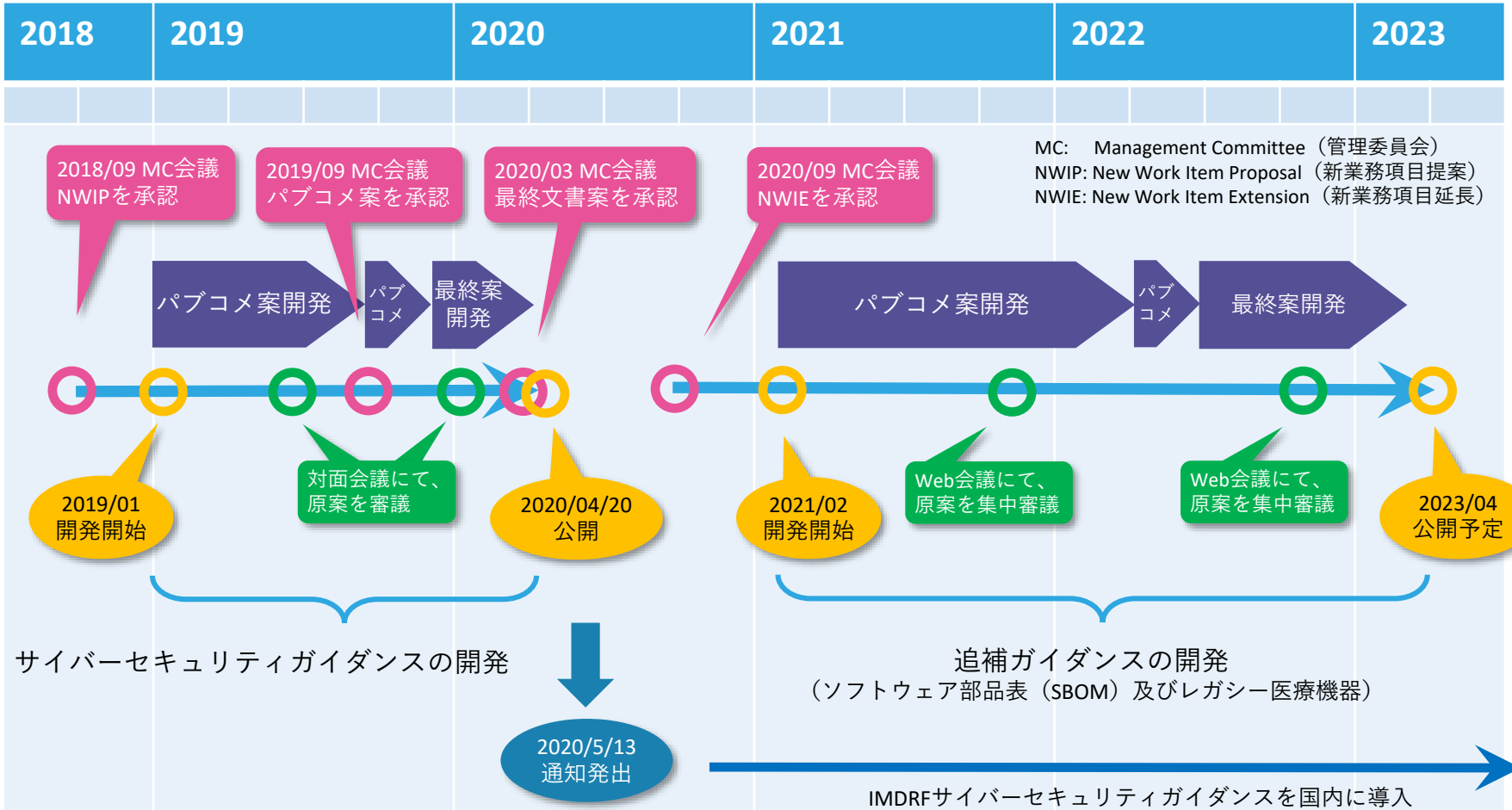
IMDRF Cybersecurity WGの目標

- **医療機器のサイバーセキュリティ**に関する国際的な**規制の整合化**を促進するために、オープンな議論を行い、全ての関係者にとって理解しやすく、実現可能な**ベストプラクティスを共有**すること。
- 具体的には、製造業者、ヘルスケアプロバイダ、規制当局、医療機器のライフサイクル全体にわたるユーザなど、責任関係者の全てに向けた、医療機器の**サイバーセキュリティに関する指針**を提供する文書を作成することを目標とする。





IMDRF Cybersecurity WGの活動経緯、予定



令和2年5月13日付け薬生機審発0513第１号・薬生安発0513第1号通知
「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）」
（https://www.mhlw.go.jp/hourei/doc/tsuchi/T200521I0040.pdf）

サイバーセキュリティガイダンスの概要

産業界代表者を含む作業グループで原案作成、
IMDRF管理委員会（MC）の承認を受け、
2020年3月18日発行

IMDRF/CYBER WG/N60FINAL:2020

IMDRF International Medical Device Regulators Forum

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）

Title: Principles and Practices for Medical Device Cybersecurity

Authoring Group: Medical Device Cybersecurity Working Group

Date: 18 March 2020

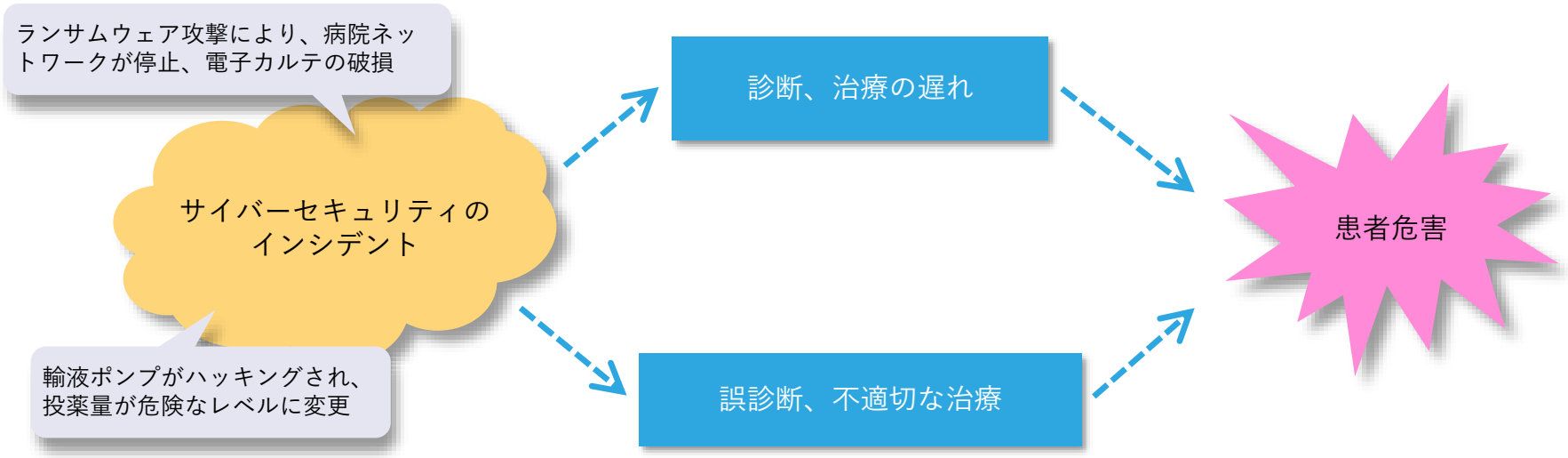
Dr Choong May Ling, Mimi, IMDRF Chair

This document was produced by the International Medical Device Regulators Forum. There are no restrictions on the reproduction or use of this document; however, incorporation of this document, in part or in whole, into another document, or its translation into languages other than English, does not convey or represent an endorsement of any kind by the International Medical Device Regulators Forum.

Copyright © 2020 by the International Medical Device Regulators Forum.

1.0　はじめに

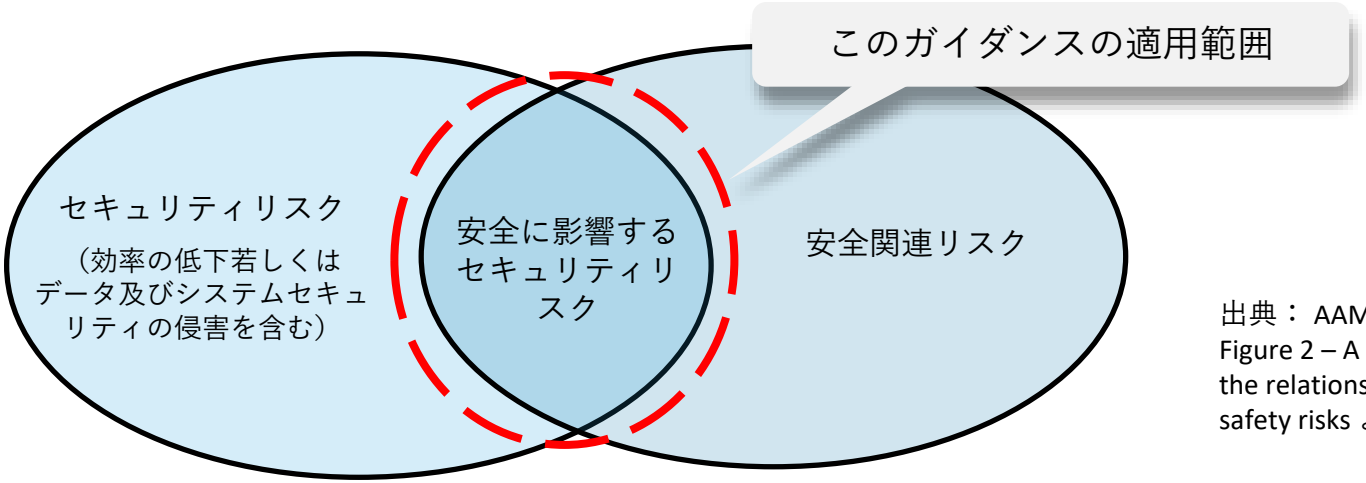
サイバーセキュリティのインシデントは、**診断及び治療介入の遅延**、**誤診断又は不適切な治療介入等の発生**により、**患者危害に至る可能性**がある。



本IMDRFガイダンスは、医療機器のサイバーセキュリティに関する国際整合を図るための**一般原則**と**ベストプラクティス**を提供することを目的とする。

2.0　適用範囲

本文書の適用範囲は、**患者への危害が発生する可能性**に関する検討に限定されていることに留意する必要がある。**データプライバシーの侵害等**、その他の危害も重要であるが、本文書では**適用範囲から除外**する。



出典： AAMI TIR57:2016
Figure 2 – A Venn diagram showing the relationship between security and safety risks より

本ガイダンスで述べるヘルスケアプロバイダには、医療機関が含まれる。

本文書の“ヘルスケアプロバイダ”

医療従事者

HDO (Healthcare Delivery Organization)、医療機関等

4.0 一般原則

4.1 国際整合

責任関係者は、医療機器のサイバーセキュリティの全ライフサイクルについて、国際整合したアプローチをとることが奨励されている。

4.2 製品ライフサイクルの全体（TPLC）

サイバーセキュリティの脅威及び脆弱性に関連する**リスクを、医療機器の全ライフサイクルにわたって**検討することが望ましい。

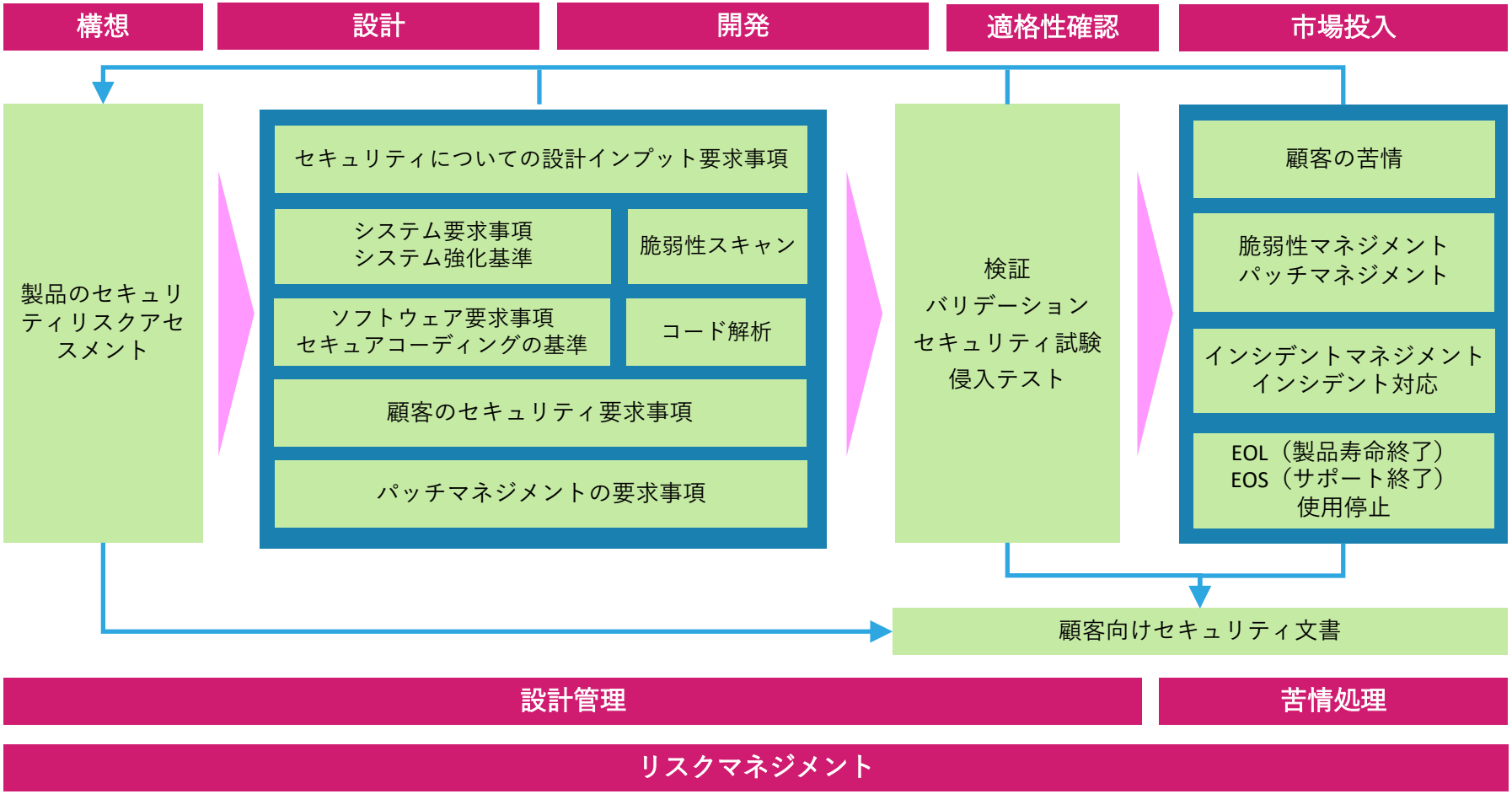
4.3 共同責任

医療機器のサイバーセキュリティは、共同責任である。製品ライフサイクルの全体にわたってサイバーセキュリティのリスク及び脅威に対応するために、全ての責任関係者が、**それぞれの責任を理解し、他の責任関係者と密接に連携**しなければならない。

4.4 情報共有

責任関係者は、医療機器の安全で有効な使用を可能にするために、透明性及び連携を高めるための情報共有が奨励されている。

4.2 製品ライフサイクルの全体（TPLC）



出典： Medical Device and Health IT Joint Security Plan (January 2019)
Figure 1. Product Security Framework.

5.0　医療機器サイバーセキュリティの市販前の考慮事項

医療機器のサイバーセキュリティは、製品の全ライフサイクルに渡って検討することが望ましく、製造業者が医療機器の**市販前の**設計段階及び開発中に対応すべき**重要な要素**がある。

重要な要素は、次である。

- セキュリティ機能を製品に組込む
- 受容できるリスクマネジメント手法を適用する
- セキュリティ試験を行う
- ユーザに対する情報提供を計画する
- 市販後活動を計画する

5.1　セキュリティ要求事項及びアーキテクチャ設計
5.2　TPLCに関するリスクマネジメント原則
5.3　セキュリティ試験
5.4　TPLCサイバーセキュリティマネジメント計画
5.5　ラベリング及び顧客向けセキュリティ文書
5.6　規制当局への申請に関する文書

主に製造業者向け

意図する使用環境に加え、合理的に予見可能な誤使用のシナリオの検討が望ましい。

5.2 TPLCに関するリスクマネジメント原則

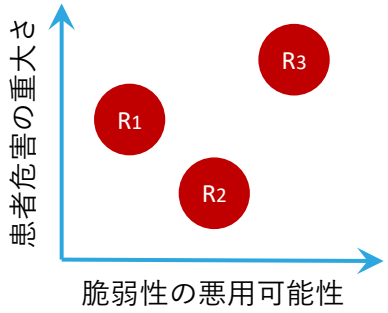
リスクマネジメントプロセスの一環として以下のステップを踏むことが望ましい。

- サイバーセキュリティの**脆弱性を特定**する
- 関連する**リスクを推定し、評価**する
- リスクを**受容可能なレベルまでコントロール**する
- リスクコントロールの**有効性を評価・監視**する
- 重要な責任関係者に対する協調的な情報開示を通じて、リスクに関する**情報を提供**する

既存のリスクマネジメントプロセスに**並行**してもよいし、**統合**してもよい

脅威モデリング、脆弱性スコアリングなどのセキュリティ関連のアクティビティを考慮する

医療機器の規制に関するサイバーセキュリティのリスク分析は、サイバーセキュリティの**脆弱性の悪用可能性**、脆弱性が悪用された場合の**患者危害の重大さ**を考慮して、患者危害のリスク評価に注力することが望ましい。この分析においては、補完的対策及びリスク緩和策について検討することが望ましい。



5.3　セキュリティ試験

製造業者は、設計開発プロセスの検証及びバリデーションの段階において、様々な種類の**セキュリティ試験**を採用することにより、重大な既知の**脆弱性がコードに含まれていない**ことを証明すると共に、**セキュリティコントロールが効果的**に実施されていることを証明することが望ましい。

下記を考慮する。

- 既知の脆弱性又はソフトウェアの弱点についての、ソフトウェアコンポーネントとモジュールのターゲット検索
- 定期的なセキュリティ試験（静的コード解析、動的解析、堅牢性試験、脆弱性スキャン、ソフトウェアコンポジション解析等）
- 技術的なセキュリティ分析（侵入テスト等。未知の脆弱性の特定又は代替エントリポイントのチェック等を含む）
- 脆弱性評価（自社の他の製品に対する脆弱性の影響分析（バリアント解析）、対抗手段の特定、脆弱性の修正又は緩和等）

5.4　TPLCサイバーセキュリティマネジメント計画

製造業者は、製品ライフサイクルの全体を通じたサイバーセキュリティマネジメント計画の一環として、**脆弱性及び悪用を積極的に監視、特定、対応**することが望ましい。製品開発の**市販前段階で計画を作成**することが望ましい。

計画では、次を取り扱うことが望ましい。

- TPLCを通じた監視（新たに発見された脆弱性への対応）
- 脆弱性の開示（脆弱性の存在及び緩和又は修正方法の開示）
- アップデート及び脆弱性の修正
  （定期的又は特定の脆弱性に対するソフトウェア・アップデートの実施）
- 復旧（インシデント後に通常の運用状態に戻す）
- 情報共有（情報共有分析機関ISAO等への参加）

5.5　ラベリング及び顧客向けセキュリティ文書

5.5.1　ラベリング

ラベリングは、関連するサイバーセキュリティリスクを考慮して該当する**セキュリティ情報**を**エンドユーザに伝達**するものである。

■ 推奨のサイバーセキュリティコントロールに関連する医療機器の使用方法及び製品仕様、 ■ バックアップ及び復元の機能及び手順、 ■ ネットワークポート及び他のインターフェイスのリスト、 ■ ユーザ向けシステム構成図

5.5.2　顧客向けセキュリティ文書

取扱説明書に加えて、製造業者が提供する医療機器の**インストール及び設定に係る技術文書**、並びに**運用環境のための技術的要求事項**は、ユーザが医療機器を安全でセキュアに使用する上で特に重要である。

■インフラについてのガイダンス、 ■ 設定によるセキュリティ強化の説明、 ■ セキュリティ対応のネットワーク接続のための技術的指示、 ■ 脆弱性・インシデントが検知された際の対応方法、 ■ 医療機器又は支援システムがユーザに異常を通知する方法、 ■ 設定の保存、回復方法、■ アップデートのダウンロード及びインストール方法、 ■ ソフトウェア部品表（SBOM：Software Bill of Materials）

5.5　ラベリング及び顧客向けセキュリティ文書

SBOM（ソフトウェア部品表）は、
製造業者とヘルスケアプロバイダ等との
コミュニケーションツールである

- 資産、関連するリスクを管理
- 脆弱性の影響を理解
- 安全性、基本性能の維持

医療機器製造業者

使用部品を見える化
（購入決定にも必要な情報）

SBOM

名称、作成元、
バージョン、
ビルド番号等々の
ソフトウェア部品
に関する情報

信頼できるコミュニケーションチャネルを通じて提供

ヘルスケアプロバイダ

- 脆弱なソフトウェア、更新の要件を特定
- セキュリティリスクマネジメントの実施

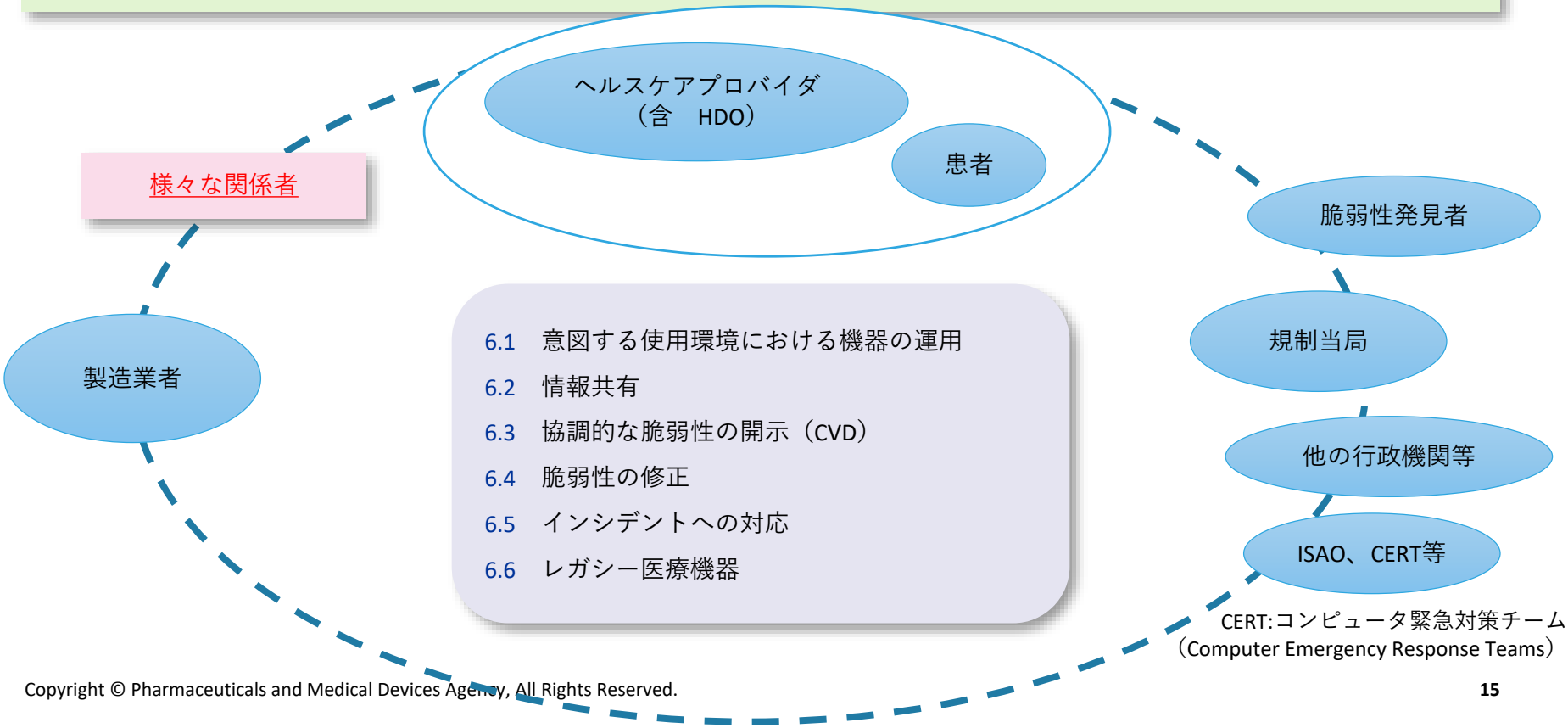
形式、構文、マークアップについて
業界のベストプラクティスの活用

補完的対策に用いる追加ハードウェアの
情報も含める（6.6.2より）

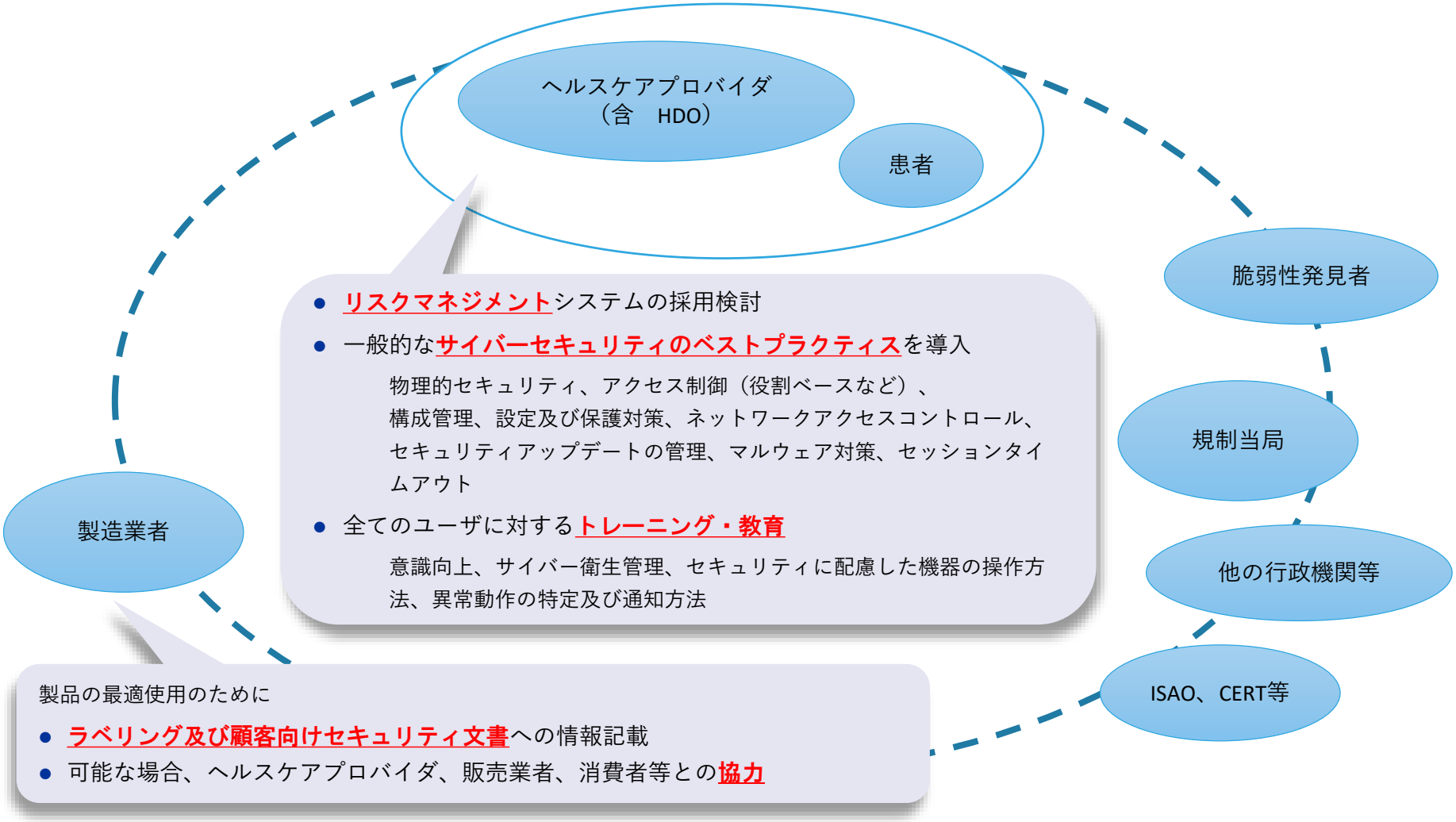
MDS2（医療機器セキュリティのための製造業者開示説明書：Medical Device Security Manufacturer Disclosure Statement）では、例として、XMLベースのソフトウェア識別タグ（SWID）である、ISO/IEC 19770-2やNISTIR 8060を提示

6.0　医療機器サイバーセキュリティの市販後考慮事項

脆弱性は時間経過に伴って変化するため、市販前の設計段階で実施したセキュリティ対応は、リスクが受容可能な状態を適切に維持できない可能性がある。そのため、**様々な責任関係者がそれぞれの役割を果たす市販後のアプローチ**が必要になる。



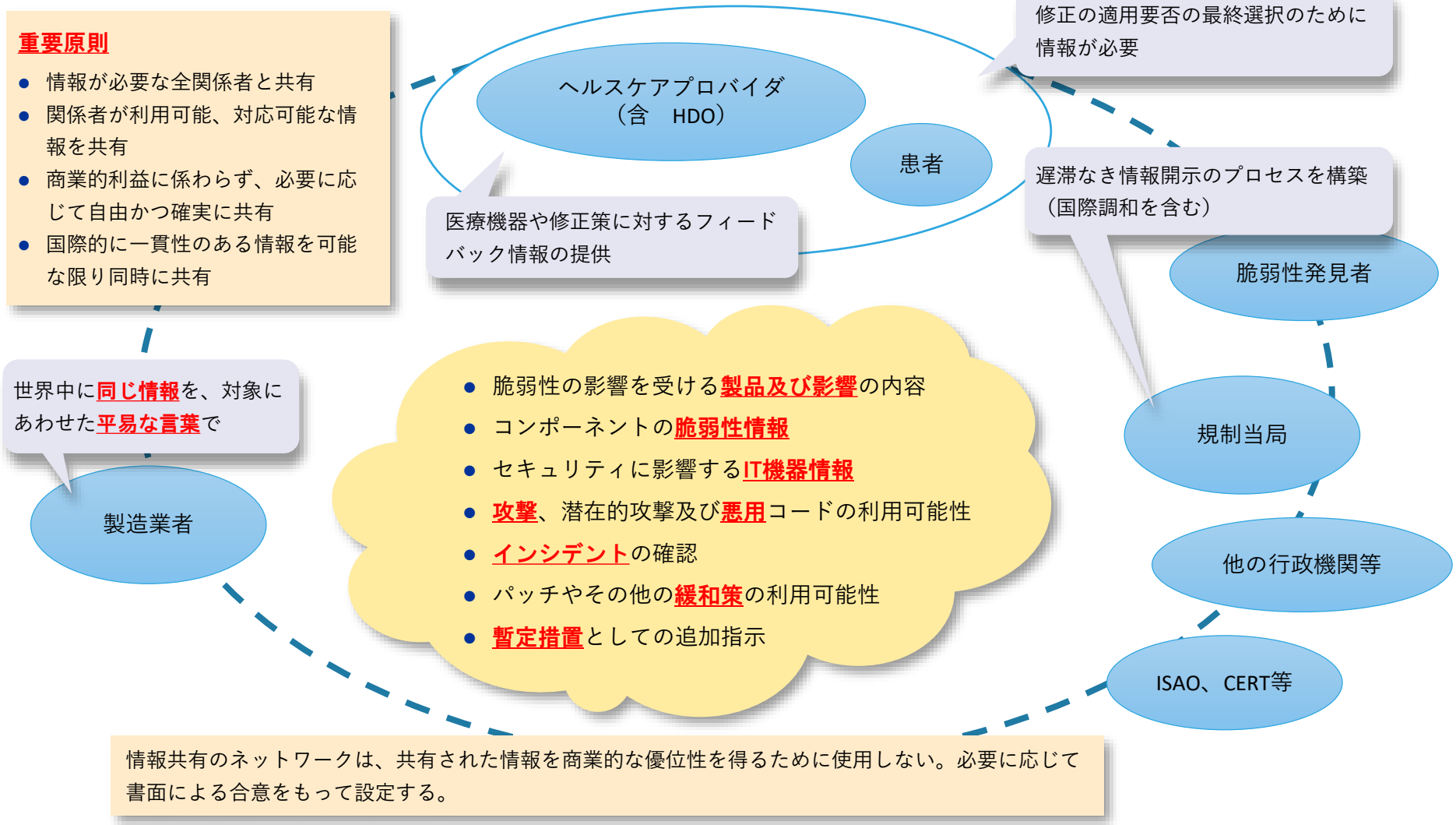
6.1　意図する使用環境における機器の運用



6.1　情報共有

重要原則

- 情報が必要な全関係者と共有
- 関係者が利用可能、対応可能な情報を共有
- 商業的利益に係わらず、必要に応じて自由かつ確実に共有
- 国際的に一貫性のある情報を可能な限り同時に共有

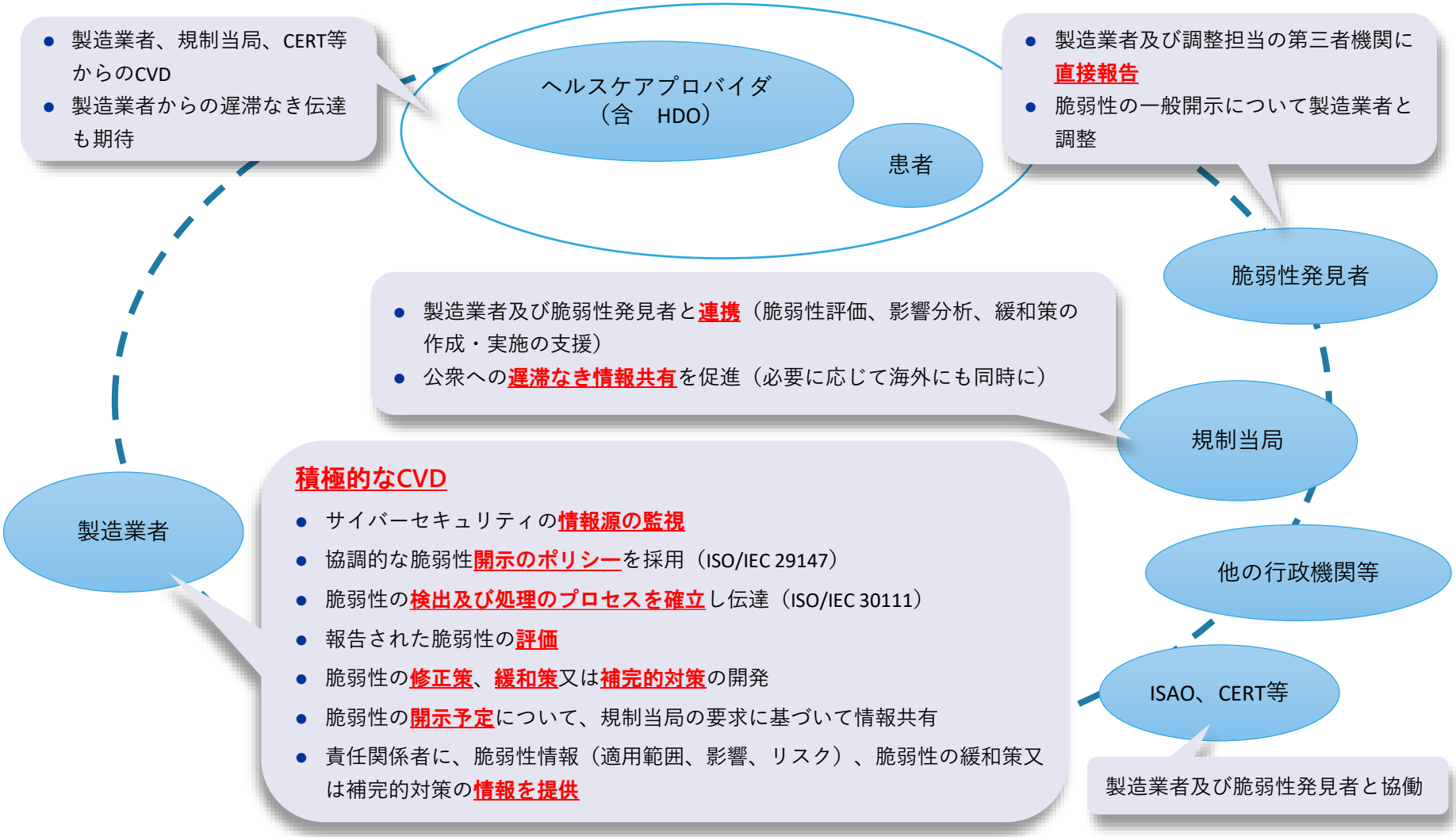


情報共有のネットワークは、共有された情報を商業的な優位性を得るために使用しない。必要に応じて書面による合意をもって設定する。

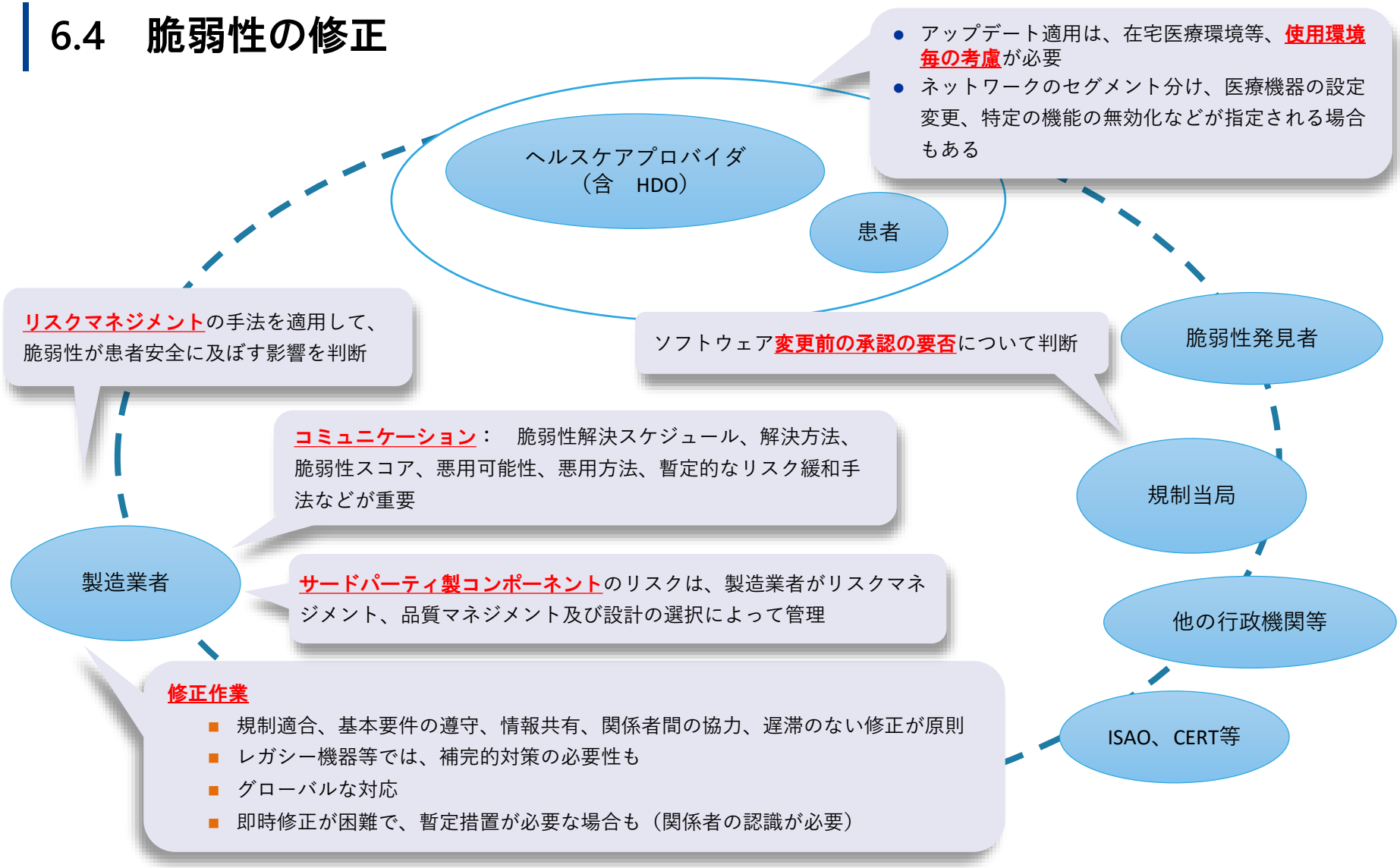
6.3　協調的な脆弱性の開示（CVD）

- CVDは、脆弱性情報を入手、評価し、緩和策及び補完的対策を**開発した上で**、責任関係者に**当該情報を開示するための正式なプロセス**を確立する。
  - 責任関係者には、顧客、同業他社、規制当局、サイバーセキュリティ情報共有組織及び一般人を含む。
  - CVDは、サイバーセキュリティのインシデントへの準備・対応に不可欠な、**透明性強化の一手法**である。
- CVDの採用は、**エンドユーザへの積極的なアプローチ**となる。
- CVDへの取り組みが、製造業者の**成熟度の判断基準**となる。
- CVDを**例外なく実施**することが望ましい。
  （製造業者に対し、CVDポリシーを照会することで、導入促進。）

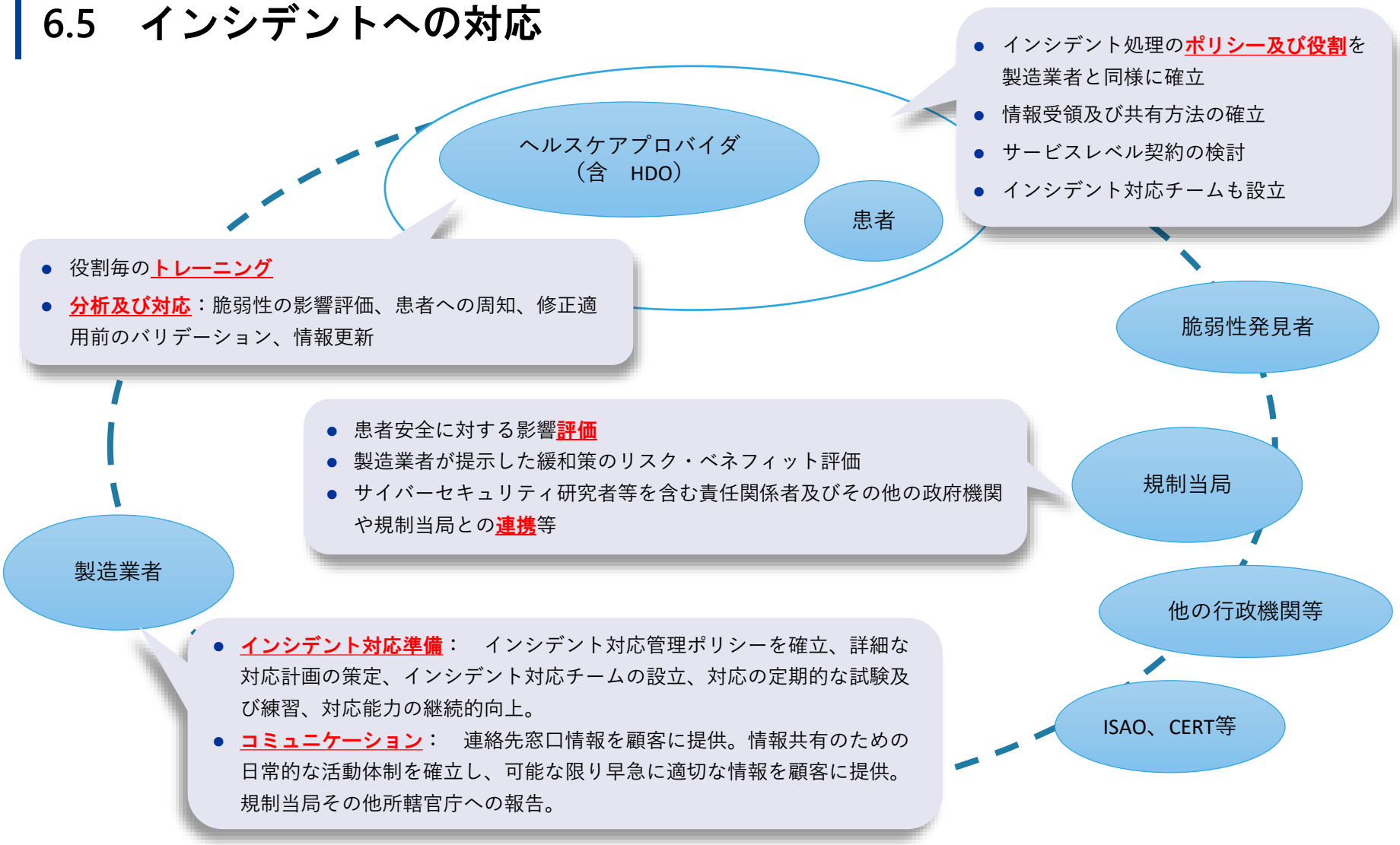
6.3　協調的な脆弱性の開示（CVD）



6.4　脆弱性の修正



6.5　インシデントへの対応



6.6　レガシー医療機器

- レガシー医療機器とは、**現在のサイバーセキュリティの脅威に対して**アップデート又は補完的対策等の**合理的な手段で保護できない**医療機器をいう。
- 医療機器の臨床的有用性が、**セキュリティ対応のサポート期間を超える**ことが多く、問題である。
- **老朽化**の理由**だけで**、レガシー医療機器であると**判断してはならない**。

（発売開始から5年以内でも、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ければ、レガシー、15年以上経っていても、合理的な手段で保護できれば、レガシーではない。）

理想的将来像

- 事業の継続が計画できるように、ヘルスケアプロバイダに対して**事前に適切な通知**を行った上で、**レガシー医療機器を段階的に使用停止**にしていく。

それに向けた**概念フレームワーク**を説明

6.6　レガシー医療機器

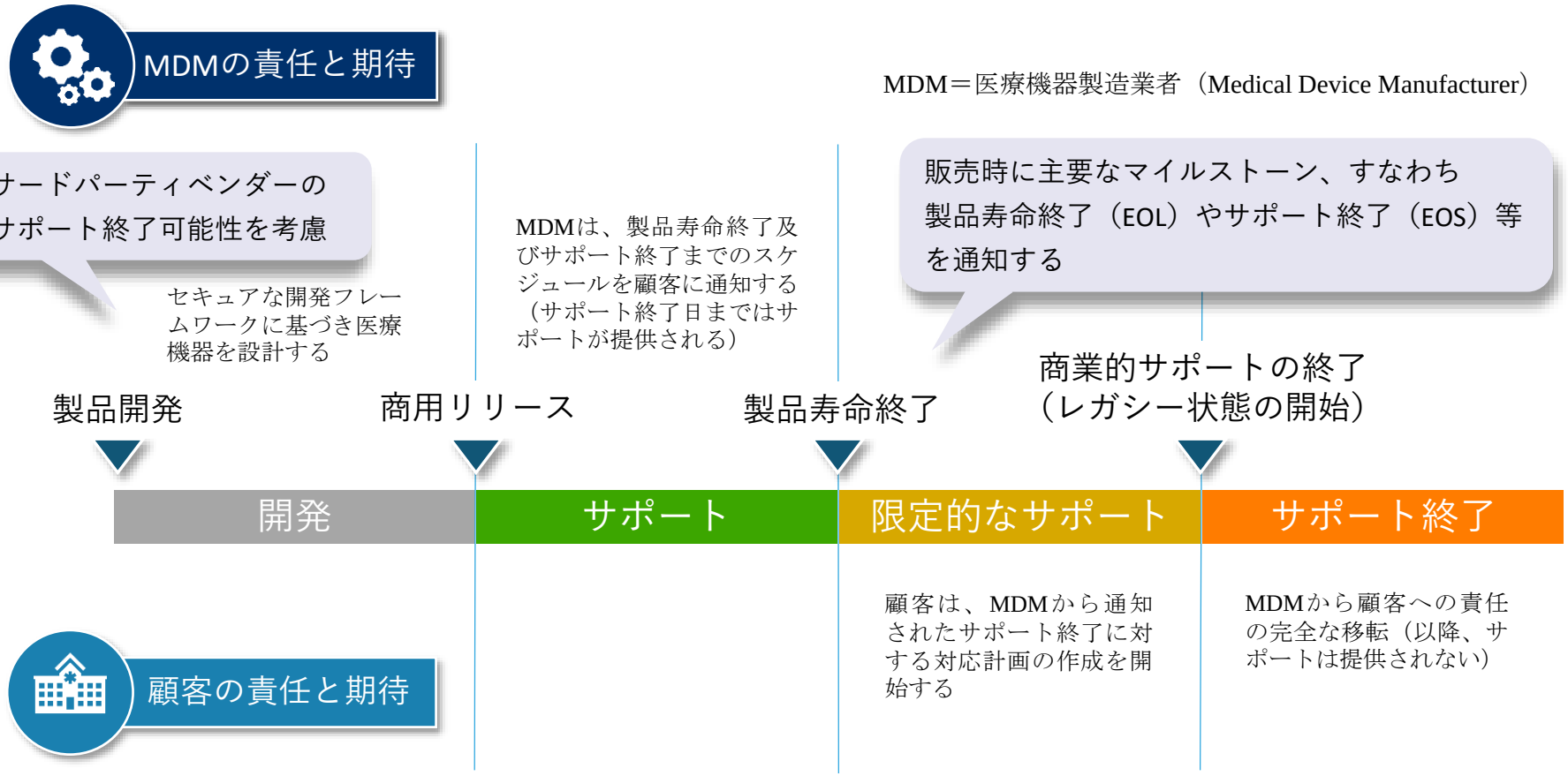


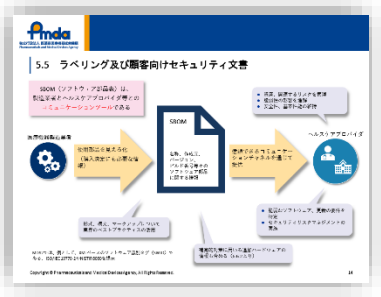
図2　サイバーセキュリティに関する製品ライフサイクルの機能として表現した
レガシー医療機器の概念フレームワーク

追補ガイダンスの開発について

- 2020年9月のMC（管理委員会）会議で、NWIE（新業務項目延長）を承認

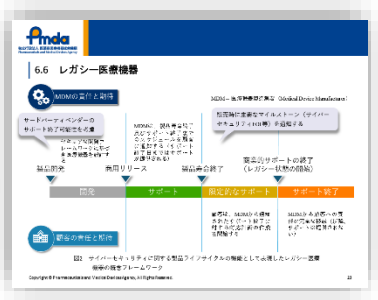
Medical Device Cybersecurity **Deeper Dive**: Legacy Devices and Transparency of Software Components Including Use of Third-Party Software

（医療機器サイバーセキュリティの**深掘り**：レガシー機器及びサードパーティ製ソフトウェアを含むソフトウェアコンポーネントの透明性について）

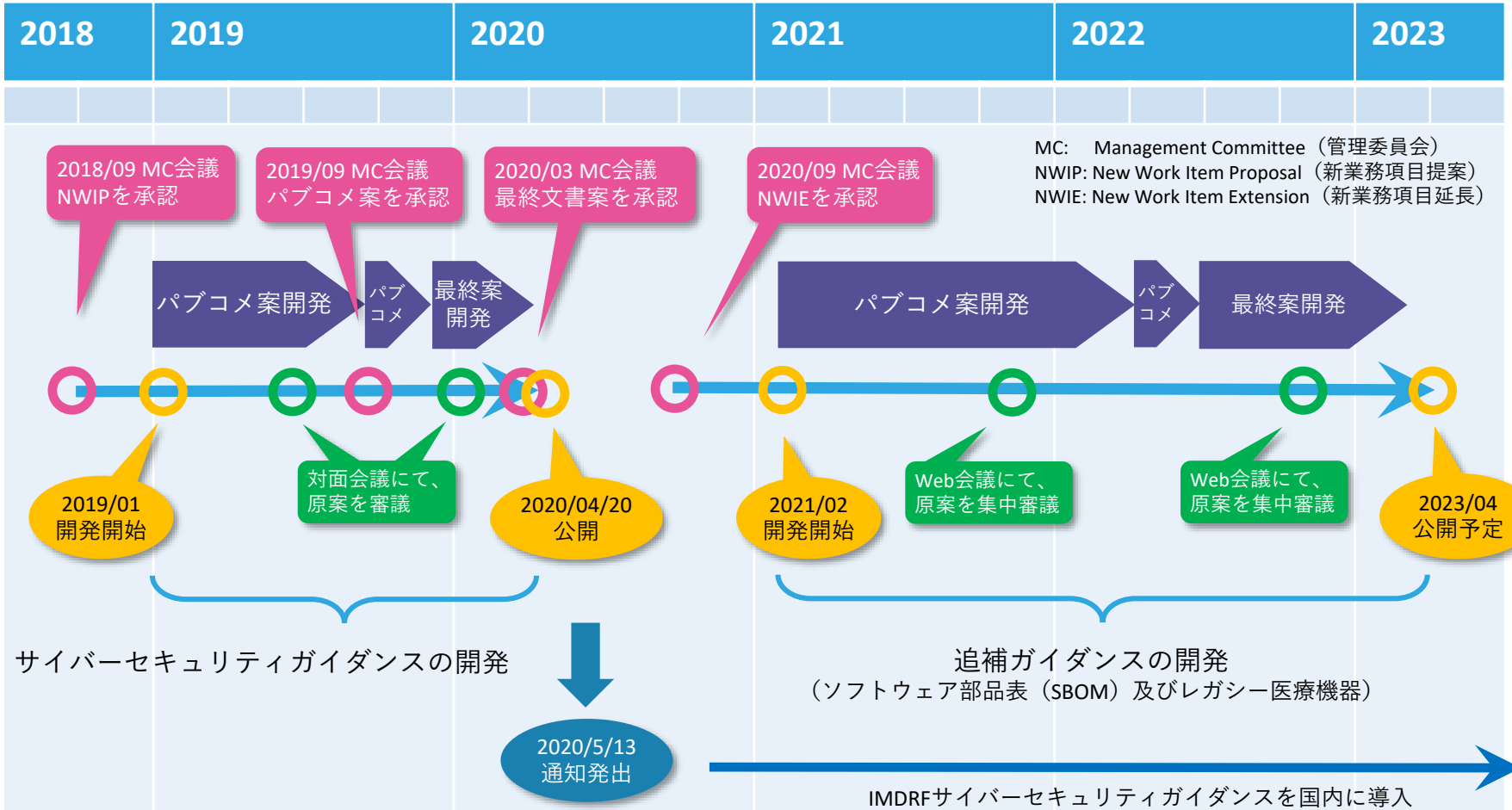


ソフトウェア部品表（SBOM）の実装並びにサードパーティ製ソフトウェアの使用及びサポートの透明性に取り組む

IMDRF サイバーセキュリティガイダンスに記載の**レガシー機器の概念フレームワークを、運用可能な形で**別文書としてまとめる



IMDRF Cybersecurity WGの活動経緯、予定



令和2年5月13日付け薬生機審発0513第１号・薬生安発0513第1号通知
「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）」
（https://www.mhlw.go.jp/hourei/doc/tsuchi/T200521I0040.pdf）

まとめ

- IMDRF Cybersecurity WGの目標
- IMDRF Cybersecurity WGの活動経緯、予定
- サイバーセキュリティガイダンスの概要
- 追補ガイダンスの開発について