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

IMDRF サイバーセキュリティWG活動報告

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

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

はじめに

- IMDRFサイバーセキュリティWGの活動の概要
- レガシー医療機器のサイバーセキュリティの原則及び実践
  （IMDRF/CYBER WG/N70FINAL:2023）
- 医療機器サイバーセキュリティのためのソフトウェア部品表の原則及び実践
  （IMDRF/CYBER WG/N73FINAL:2023）

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。

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

IMDRFサイバーセキュリティWGの活動の概要

WGの目標：

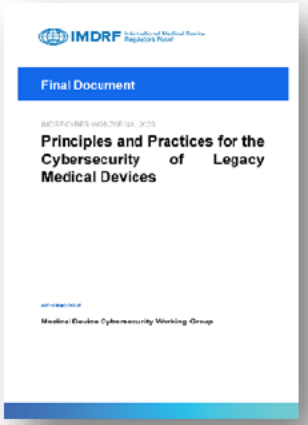
- 医療機器のサイバーセキュリティに関する国際的な規制の整合化の促進のために、ベストプラクティスを共有する
- そのため、製造業者、ヘルスケアプロバイダー、規制当局、ユーザー等の関係者すべてに向けた、医療機器のサイバーセキュリティに関する指針を提供する文書を作成する

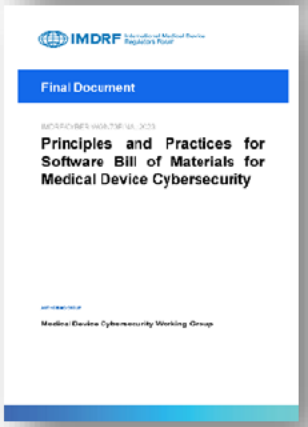
（日本からは、厚労省、PMDA、キヤノンメディカルシステムが参画）

IMDRF サイバーセキュリティWGの発行文書

6.6「レガシー医療機器」について深堀り

5. 5. 2「顧客向けセキュリティ文書」に記載のソフトウェア部品表について、深堀り





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）

IMDRF/CYBER WG/N60FINAL:2020（2020年4月発行）

https://www.imdrf.org/documents/principles-and-practices-medical-device-cybersecurity

（以下、「サイバーセキュリティガイダンス」）

Principles and Practices for the Cybersecurity of Legacy Medical Devices

（レガシー医療機器のサイバーセキュリティの原則及び実践）

IMDRF/CYBER WG/N70FINAL:2020（2023年4月発行）

https://www.imdrf.org/documents/principles-and-practices-cybersecurity-legacy-medical-devices

（以下、「レガシーガイダンス」）

サイバーセキュリティガイダンスのパブコメにおいて、実装の詳細が知りたいとの声が多かった二つのテーマについて、新たにガイダンスを開発した

Principles and Practices for Software Bill of Materials for Medical Device Cybersecurity

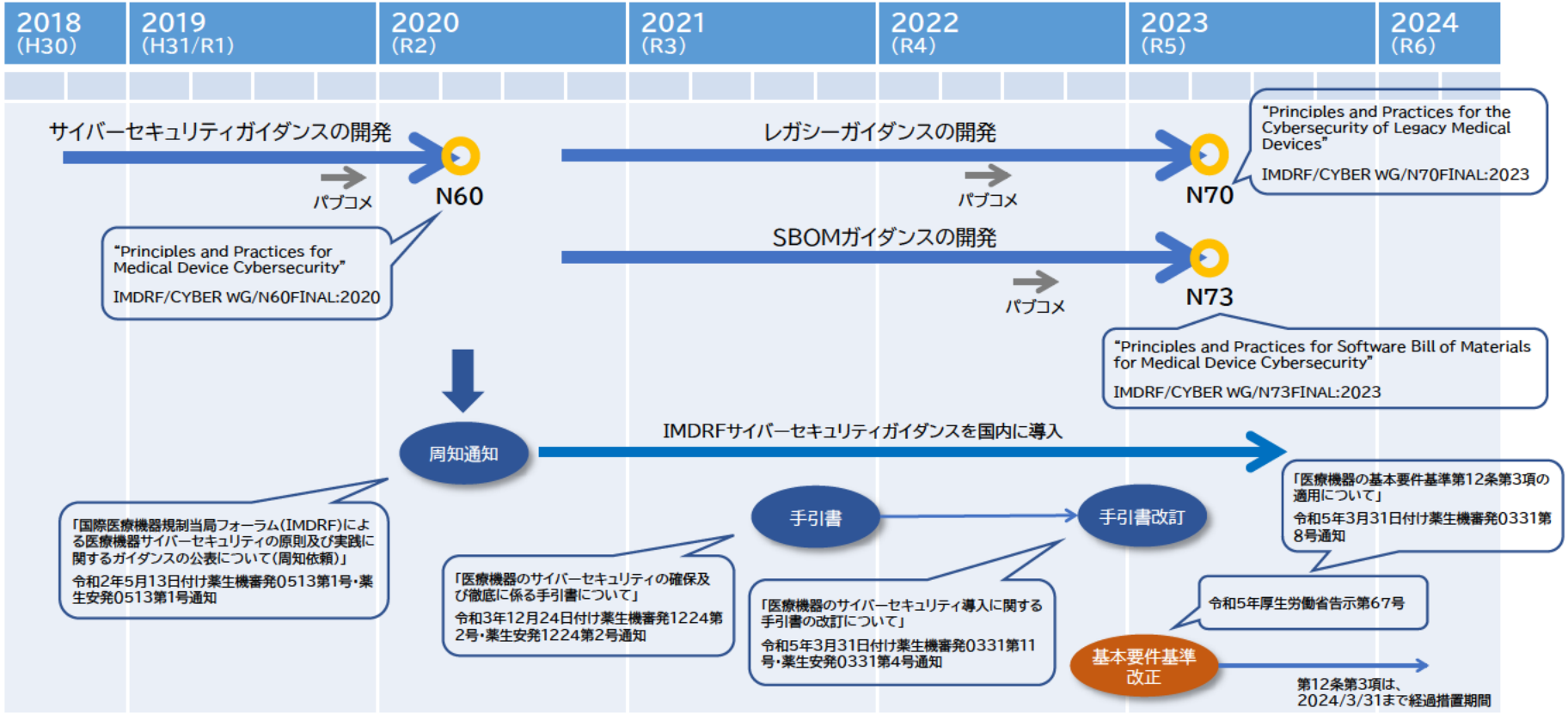
（医療機器サイバーセキュリティのためのソフトウェア部品表の原則及び実践）

IMDRF/CYBER WG/N73FINAL:2020（2023年4月発行）

https://www.imdrf.org/documents/principles-and-practices-cybersecurity-legacy-medical-devices

（以下、SBOMガイダンス」）

IMDRF Cybersecurity WGの活動の経緯



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

レガシー医療機器のサイバーセキュリティの原則及び実践
（IMDRF/CYBER WG/N70FINAL:2023）

レガシーガイダンスのあらまし

- 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合理的に保護できない医療機器”

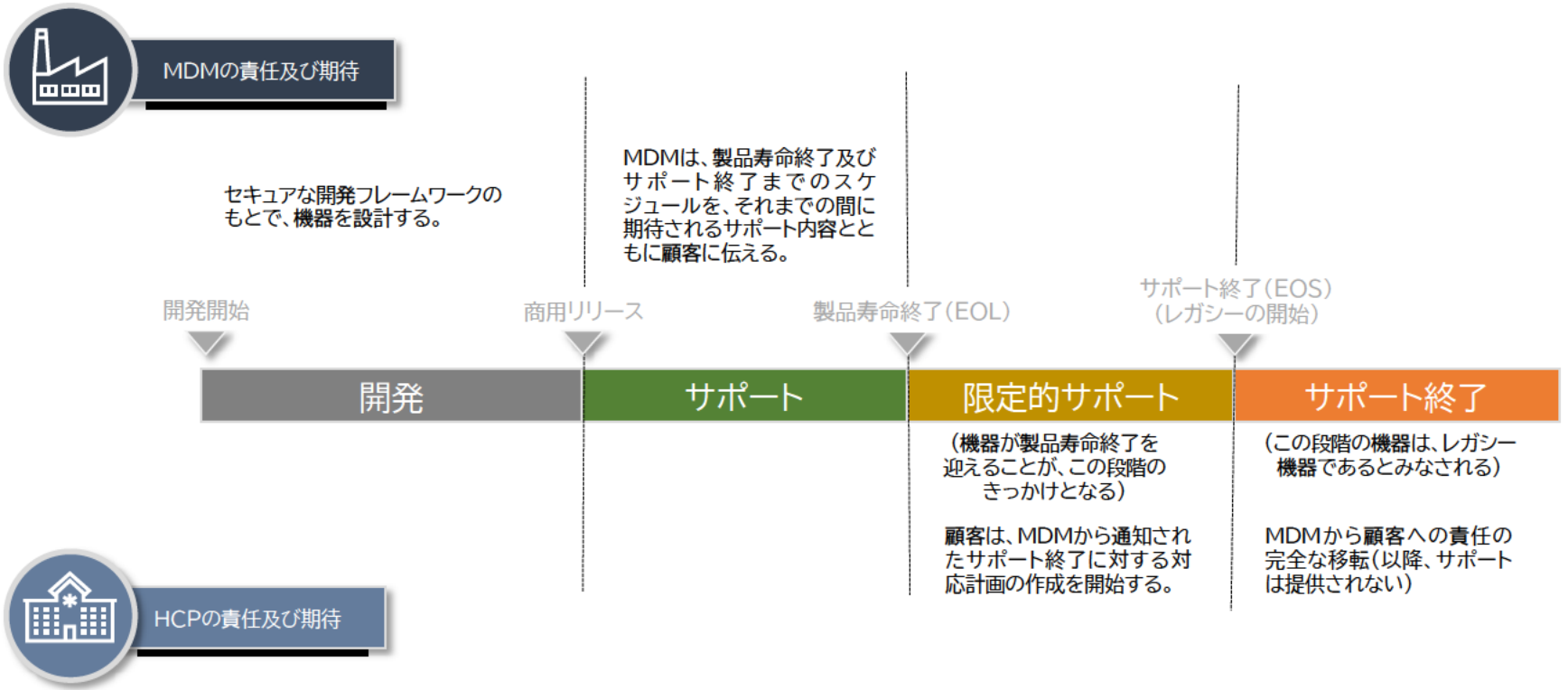
- ガイダンス開発の背景:
  - レガシー医療機器が引き続き医療の現場で使用されており、患者安全に対する重大な脅威が生み出されかねない
  - ヘルスケアプロバイダーに対して製品寿命終了やサポート終了を事前に通知する、事業継続計画をたてて、プロバイダーがレガシーでない医療機器へアップグレードしたり、使用停止するとケアの継続に影響が出る場合はリスク管理を改善する、といったことに必要な情報を与えるために指針が必要
  - サイバーセキュリティガイダンスのパブコメで、実装の詳細が知りたいとの声が多かった

- レガシーガイダンスの目的:

サイバーセキュリティガイダンスに示されたレガシー医療機器の(概念的)フレームワークを実装する際の推奨事項をライフサイクルの各段階に対して示す。

- 主な関係者:
  - 医療機器製造業者(MDM、Medical Device Manufacturer)
  - ヘルスケアプロバイダー(HCP、Healthcare Provider)

レガシー医療機器のフレームワークの概要



*医療機器製造業者(MDM)は、医療機器の責任に関する各地域のガイダンスに従う。サポートレベルは、顧客との契約に応じて異なる可能性がある。なお、この図の顧客とは、ヘルスケアプロバイダー(HCP)を意味する。

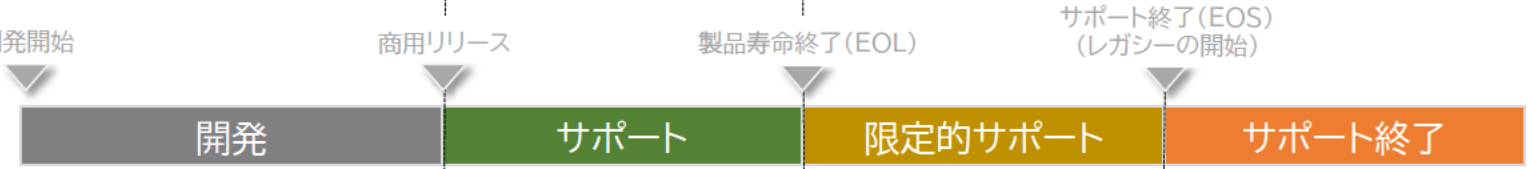
レガシー医療機器のフレームワークの概要

ライフサイクルのそれぞれの段階において、
コミュニケーション、リスクマネジメント、責任移転の観点から、
製造業者及びヘルスケアプロバイダーのそれぞれに対する推奨事項を示している

MDMの責任及び期待

セキュアな開発フレームワークのもとで、機器を設計する。

MDMは、製品寿命終了及びサポート終了までのスケジュールを、それまでの間に期待されるサポート内容とともに顧客に伝える。



(機器が製品寿命終了を迎えることが、この段階のきっかけとなる)

顧客は、MDMから通知されたサポート終了に対する対応計画の作成を開始する。

(この段階の機器は、レガシー機器であるとみなされる)

MDMから顧客への責任の完全な移転(以降、サポートは提供されない)

HCPの責任及び期待

使用しているサードパーティ製コンポーネントが、突然EOSを迎える等の事情で、予期しないレガシー(Unplanned Legacy)が起こる可能性がある。

別のライフサイクル段階に移行するきっかけになるようなリスクを評価するフレームワークについても5. 5に示されている。

*医療機器製造業者(MDM)は、医療機器の責任に関する各地域のガイダン
契約に応じて異なる可能性がある。なお、この図の顧客とは、ヘルスケアプロ

コミュニケーションの観点

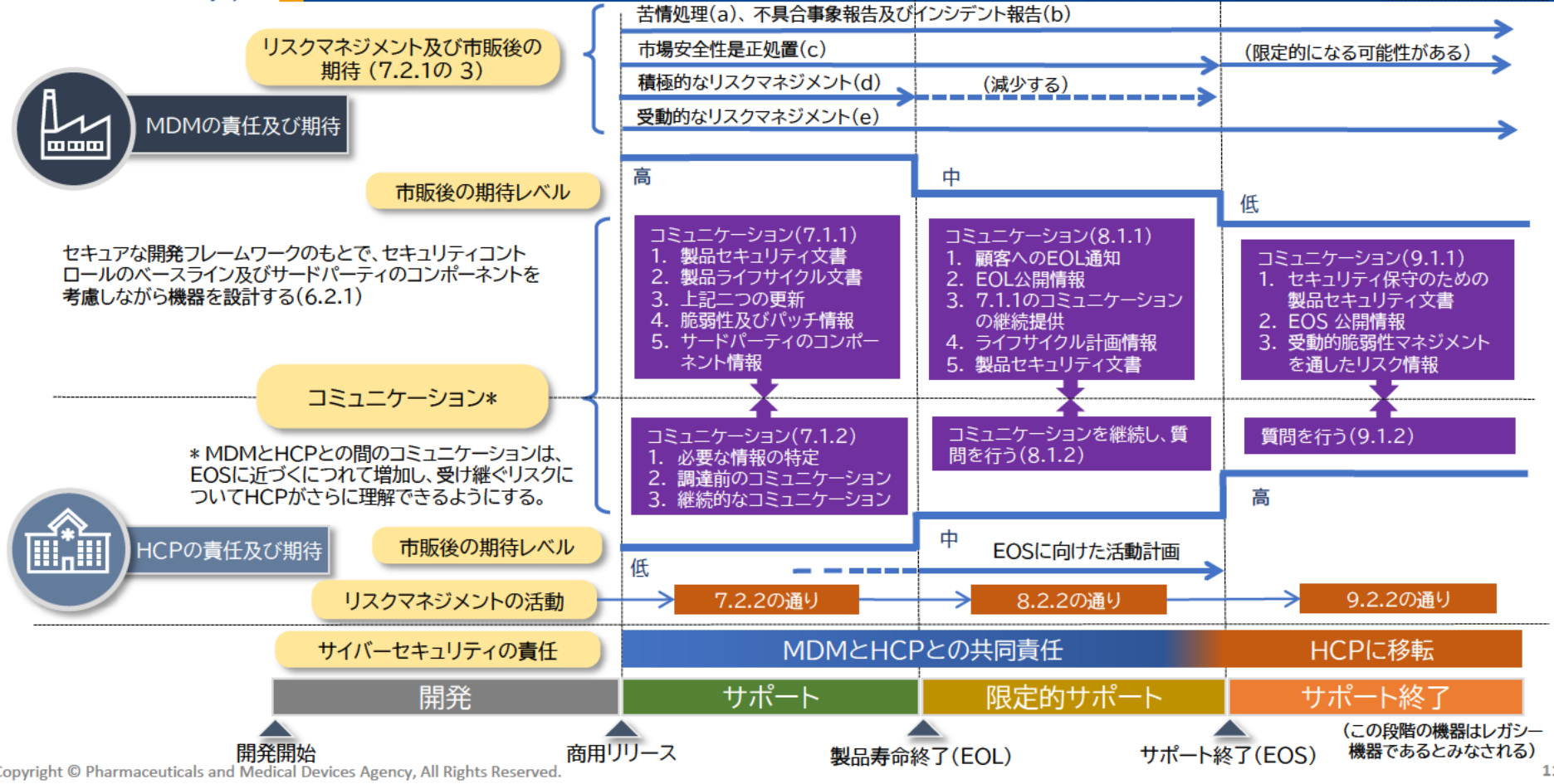
- レガシーについては、医療機器に関する情報の欠落が重要課題なので、製造業者とヘルスケアプロバイダーとの間のコミュニケーションは極めて重要
- 製造業者は、ベストプラクティスとして、少なくとも2～3年前に、EOLやEOSの期日を情報提供することが望ましい
- 製造業者からは、製品セキュリティ文書、ライフサイクルの段階が移行することの通知、脆弱性・パッチの情報を提供する
- ヘルスケアプロバイダーは、受け取った情報に関する疑問について、製造業者に質問する
- ヘルスケアプロバイダーと製造業者との間のコミュニケーションは、EOSに近づくにつれて増加する

リスクマネジメント及び責任移転の観点

- 医療機器がEOSに近づくにつれ、製造業者の責任が減少し、ヘルスケアプロバイダーの責任が増加する
- EOS後も、製造業者は、地域の規制に従って、苦情処理や不具合事象報告、インシデント報告等の市販後活動を行う責任がある

	製造業者側の推奨事項	ヘルスケアプロバイダー側の推奨事項
リスクマネジメント	■ 製品開発においては、設計によってセキュリティを組み込む ■ サードパーティのサポート終了等に対してリスクマネジメントを行う ■ EOL及びEOS期日についてコミュニケーションする	■ 医療機器の設計及び運用環境を考慮する ■ 自身のリスク管理の能力を評価する ■ 必要な文書及び要求事項を確実にする ■ EOSを超えた機器使用を評価するために、自身の能力及びリスクを検討する
責任移転	■ 地域の規制要求に従った市販後の期待に適合する ■ 必要な文書及び要求事項をヘルスケアプロバイダーに対して提供する ■ 医療機器のアップグレードの選択肢を提供する ■ EOSにおいて、責任移転を完了する	■ 医療機器のアップグレードの選択肢を検討する ■ EOSにおけるリスクを受容するか、又は新たな若しくはアップグレードした医療機器へ移行する

レガシー医療機器のフレームワークの詳細



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

医療機器サイバーセキュリティのためのソフトウェア部品表の原則及び実践（IMDRF/CYBER WG/N73FINAL:2023）

SBOMガイダンスのあらまし

- SBOM(ソフトウェア部品表)とは:

“一つ又は複数の識別したコンポーネント、それらの関係及びその他の関連する情報のリスト”

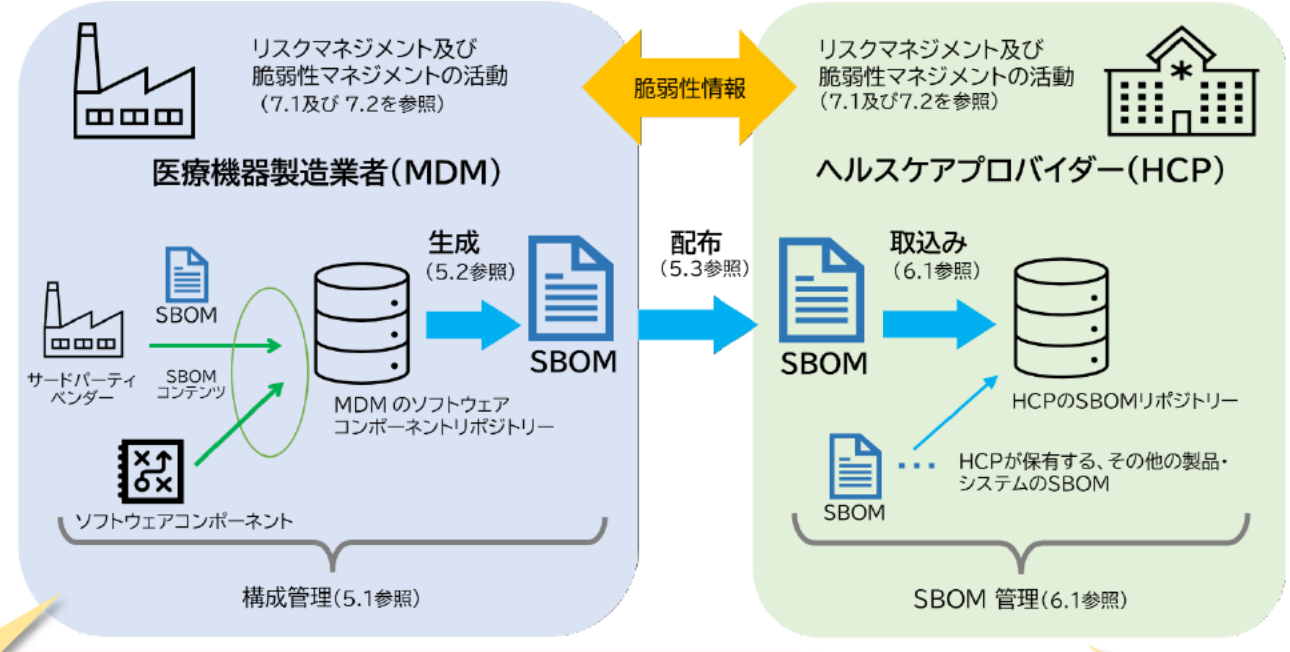
- ガイダンス開発の背景:
  - 今日の医療機器には、非常に多くのソフトウェアコンポーネント(自製、市販、オープンソース等)が組み込まれている
  - それらのコンポーネントに対する脆弱性が後から見つかったり、コンポーネントがサポート終了したりすることが、患者へのリスクの源になる可能性がある
  - SBOMは、サイバーセキュリティのリスクマネジメントプロセスを全ライフサイクルに渡って改善するために利用可能なリソースである
  - サイバーセキュリティガイダンスのパブコメで、実装の詳細が知りたいとの声が多かった

- SBOMガイダンスの目的:

SBOMの実装についての推奨事項を提供し、医療機器におけるソフトウェア使用の透明性を高める。

- 主な関係者:
  - 医療機器製造業者(MDM、Medical Device Manufacturer)
  - ヘルスケアプロバイダー(HCP、Healthcare Provider)

SBOMフレームワークの概要

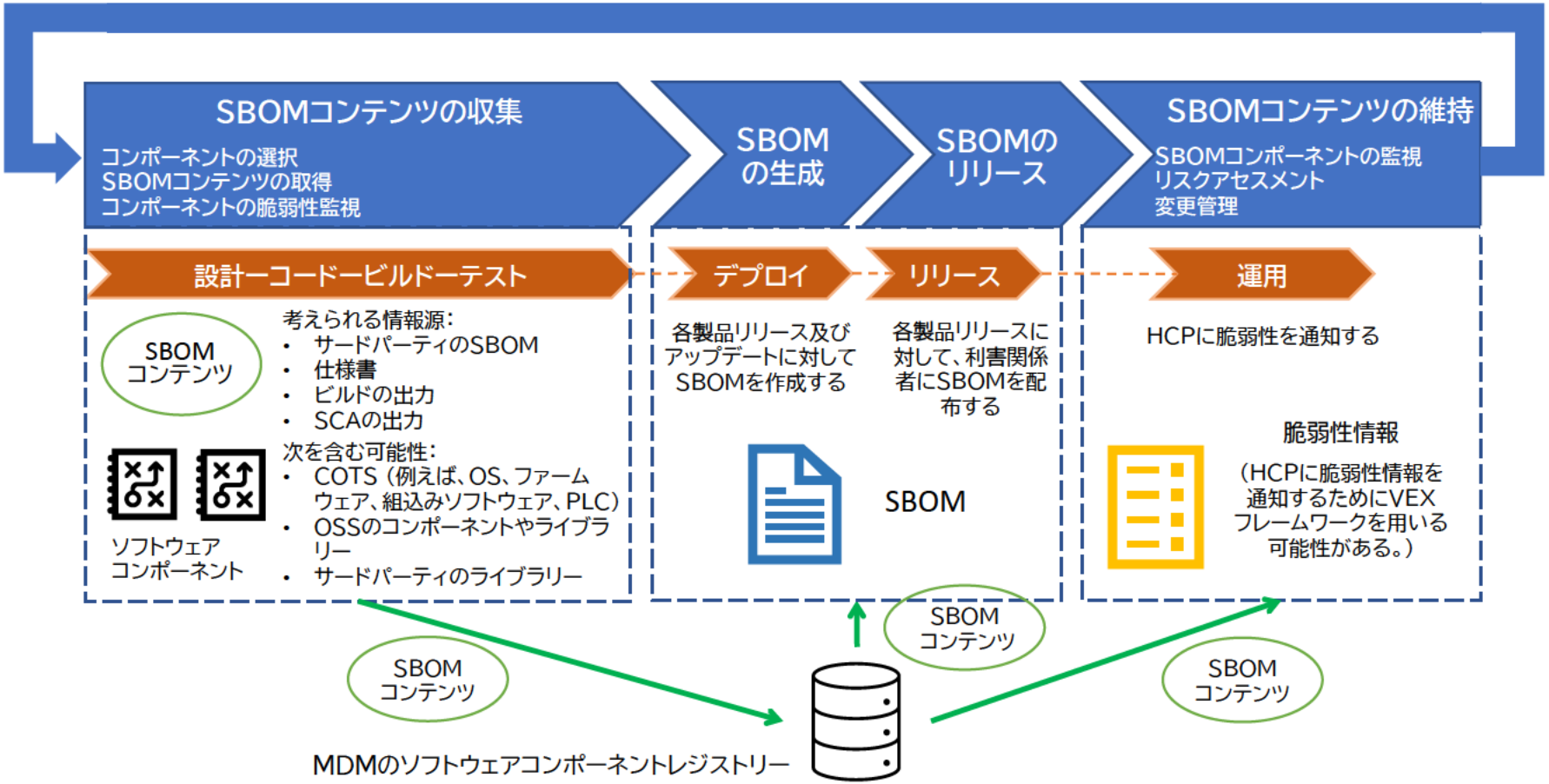


当該医療機器のSBOMは、製造業者及びヘルスケアプロバイダーの双方において、リスクマネジメント活動及び脆弱性マネジメント活動のために活用する

- 医療機器には、サードパーティー製、オープンソース、自製等様々なソフトウェアコンポーネントが組み込まれる
- 製造業者は、医療機器に組み込むソフトウェアコンポーネントの情報を、開発工程における構成管理の一環としてデータベース等で管理する
- 製造業者は、そのデータから必要な情報を抽出してSBOMを生成し、ヘルスケアプロバイダーに配布する

ヘルスケアプロバイダーは、その他の製品・システムのSBOMとともに、配布されたSBOMをヘルスケアプロバイダーのデータベース等に取り込んで管理して活用する

製造業者の考慮事項の概要



SBOMの要素及びフォーマット

- SBOMには、最低限次の要素を含めることが望ましい （NTIA（米国電気通信情報管理局）の推奨事項に一致）

要素	説明
作成者名	SBOMファイルを作成したエンティティ（すなわち、個人、組織又はそれに類するもの）
タイムスタンプ	SBOMデータの構築を行った日時の記録
ソフトウェアコンポーネントのベンダー（サプライヤー）	コンポーネントを作成、定義、識別するエンティティ。ソフトウェアコンポーネントのベンダー名は、一般に、商用ソフトウェアの法的なビジネス名を参照することが望ましい。
ソフトウェアコンポーネントの名称	元のサプライヤーが定義した、ソフトウェアユニットに割り当てられた名称
ソフトウェアコンポーネントのバージョン	以前に識別した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
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
関係	上流コンポーネントXがコンポーネントYに含まれるという関係の説明

- SBOMのフォーマット（自動化可能なもの）
  - CycloneDX
  - SPDX（Software Package Data Exchange）
  - SWID（Software Identification）

ヘルスケアプロバイダーの考慮事項の概要

- SBOMの取り込み及び管理
  - 資産の在庫管理を完全かつ正確に行うことが極めて重要
  - 有効性を最大限に高めるためには、SBOMは機械可読性があること
  - ヘルスケアプロバイダーと製造業者との間のコミュニケーションは、機密性があること
  - ヘルスケアプロバイダーがSBOMをデータベース等で管理する場合は、次を考慮することが望ましい：
    - 検索・照会機能　（医療機器のリスクを特定し、管理するため）
    - 更新及び保守　（情報が最新で正確であることを確実にする）
    - セキュリティ　（悪意をもって改ざんされたり、攻撃のロードマップにされないようにする）

SBOMのユースケース

- リスクマネジメント
  - 全製品ライフサイクルにわたり、製造業者及びヘルスケアプロバイダーの双方に対してSBOMのベネフィットがある
  - 製造業者は、サイバーセキュリティのリスクを評価し、コントロールし、監視するためにSBOMを使用できる
  - ヘルスケアプロバイダーは、調達時点からリスクマネジメントを開始するが、それにSBOMを使用できる
- 脆弱性マネジメント
  - SBOMは、新たな脆弱性の出現を監視し、現時点におけるサポート及び非サポートソフトウェアを理解する助けにすることができる
  - SBOMは、脆弱性の影響及びそれに対する改善策を決定する際の管理を支援する
- インシデントマネジメント
  - SBOMは、影響の可能性がある機器を特定する手助けにできる

ソフトウェア部品表とレガシー医療機器

- 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合理的に保護できない医療機器である
- レガシー医療機器に対するSBOMをもつことは、有益である
- レガシー医療機器のSBOMを作成するのは、難しいかもしれない
  - 製造業者は、レガシー機器のSBOMを作成するために最大限に努力することが望ましい
  - ソフトウェアコンポジション解析などのツールが役立つかもしれない。範囲、深さ、正確性は減少する可能性がある。

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

おわりに

IMDRFサイバーセキュリティWGの活動について、その概要、最近発行された二つのガイダンス文書について説明しました。

ご清聴ありがとうございました。