医療機器ソフトウェア部品表による構成管理・情報連携体制の確立

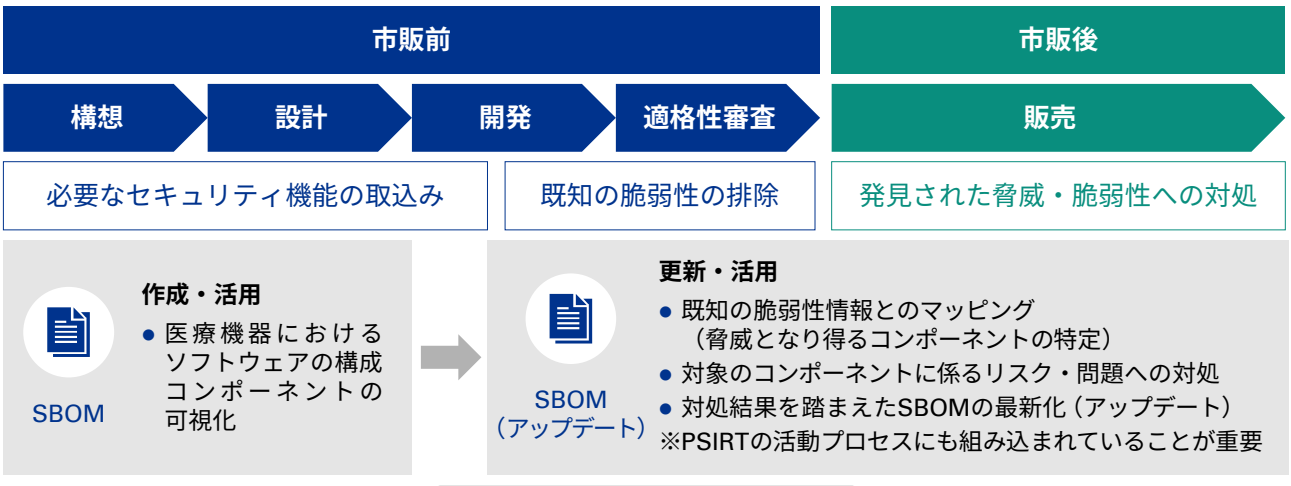
薬機法に基づく基本要件基準に準拠したサイバーセキュリティ対応

医療分野における急速な情報化・ネットワーク化に伴い、医療安全の確保に向けた医療機器のサイバーセキュリティ対応が重要な課題となっています。日本では2023年4月1日より、薬機法（医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律）に基づき、医療機器の新たな基本要件基準が適用されています。当該基準の一部として、構成管理プロセスおよび情報連携体制を確立するために、ソフトウェア部品表（SBOM）の作成・活用が求められるようになり、2024年4月1日までに企業は当該基準を満たしていることを示す必要があります。KPMGでは、こうした背景を踏まえ、本規制への対応の一環として、SBOMの作成やPSIRT（Product Security Incident Response Team）等の情報連携体制構築を含めたSBOMの作成・活用に係る施策の立案および推進を支援します。

SBOMの作成・活用による医療機器における構成管理プロセスの確立

薬機法に基づく基本要件基準の改正により、他の機器およびネットワーク等と接続して使用する医療機器（SaMD*含む）を対象に、開発・保守・サポートのための変更管理および構成管理プロセスを確立することが必須となりました。具体的には、当該医療機器のSBOMを適切に作成することが、プロセス確立のための要件であるとされ、許認可申請時にはSBOMを提示できるよう準備が求められます。市販前においては、必要なセキュリティ機能の取込みや、既知の脆弱性の排除のためにSBOMを作成・活用します。加えて、市販後においては発見された脅威・脆弱性に適時に対処するために、SBOMを最新の状態に維持したうえで、引き続き活用することが重要です。

* SaMD（Software as a Medical Device）：プログラム医療機器

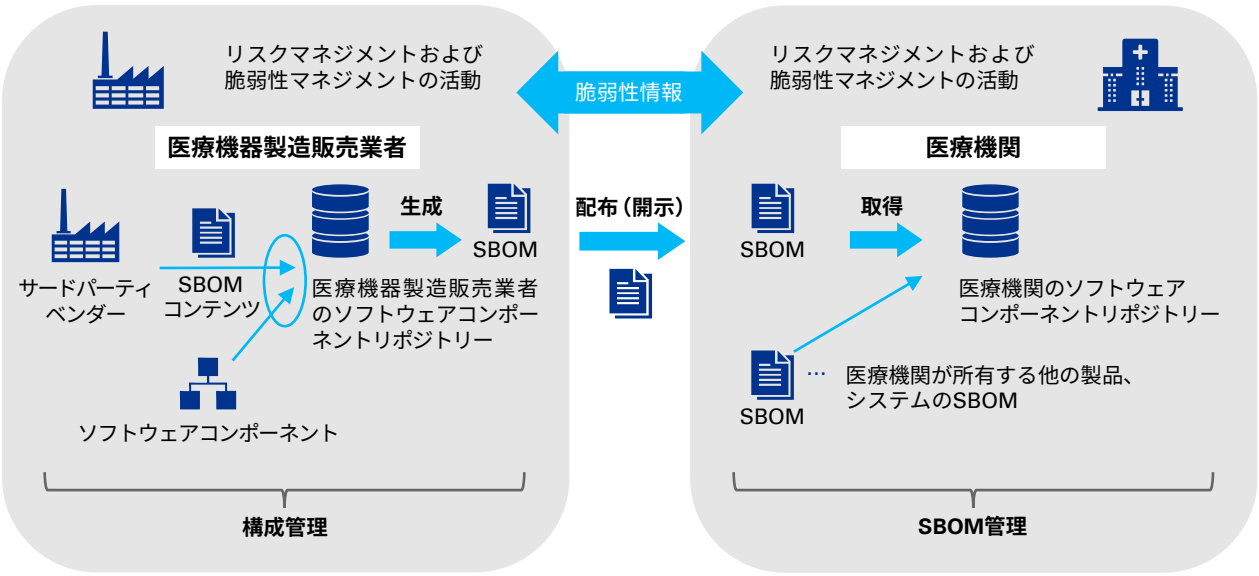


医療機器の安全確保に向け、ソフトウェアの構成コンポーネントレベルでの管理および適切な対処が必要

ソフトウェア部品表（SBOM）

SBOMは、医療機関、医療機器の使用者が、その資産を効率的に管理して、識別された脆弱性が機器の安全性および性能に与える影響を把握し、その対応を可能にするものと位置づけられています。そのため、医療機器の製造販売業者は、サードパーティベンダーの最新のSBOM、EOL／EOS[*1]の把握が求められます。また、当該医療機器のSBOMには特定可能な構成情報とともに、製品のアップグレード等の管理計画の根拠となる情報を保持しなければなりません。SBOMは製品のTPLC[*2]に関する網羅的な文書となり、製品導入にあたり顧客から開示を求められることを想定した内容にする必要があります。

*1 EOL (End of Life)：有効期間を超えた製品の販売を終了する時点を指す／EOS (End of Support)： 製造業者が全てのサポート活動を中止する時点を指す
*2 TPLC (Total Product Life Cycle)：製品ライフサイクル全体



SBOMの構想検討

薬機法で求められるSBOMは、ソフトウェア管理の一手法であり、導入の際には、組織の現状に適合させることが重要です。そのため、SBOM構想検討の段階で、適用範囲を薬機法の要求と自社の現況に合わせて検討し、具体的な計画に落とし込むことが肝要です。KPMGは、効果的なSBOMの活用に向けた環境構築、体制整備の構想検討を支援します。

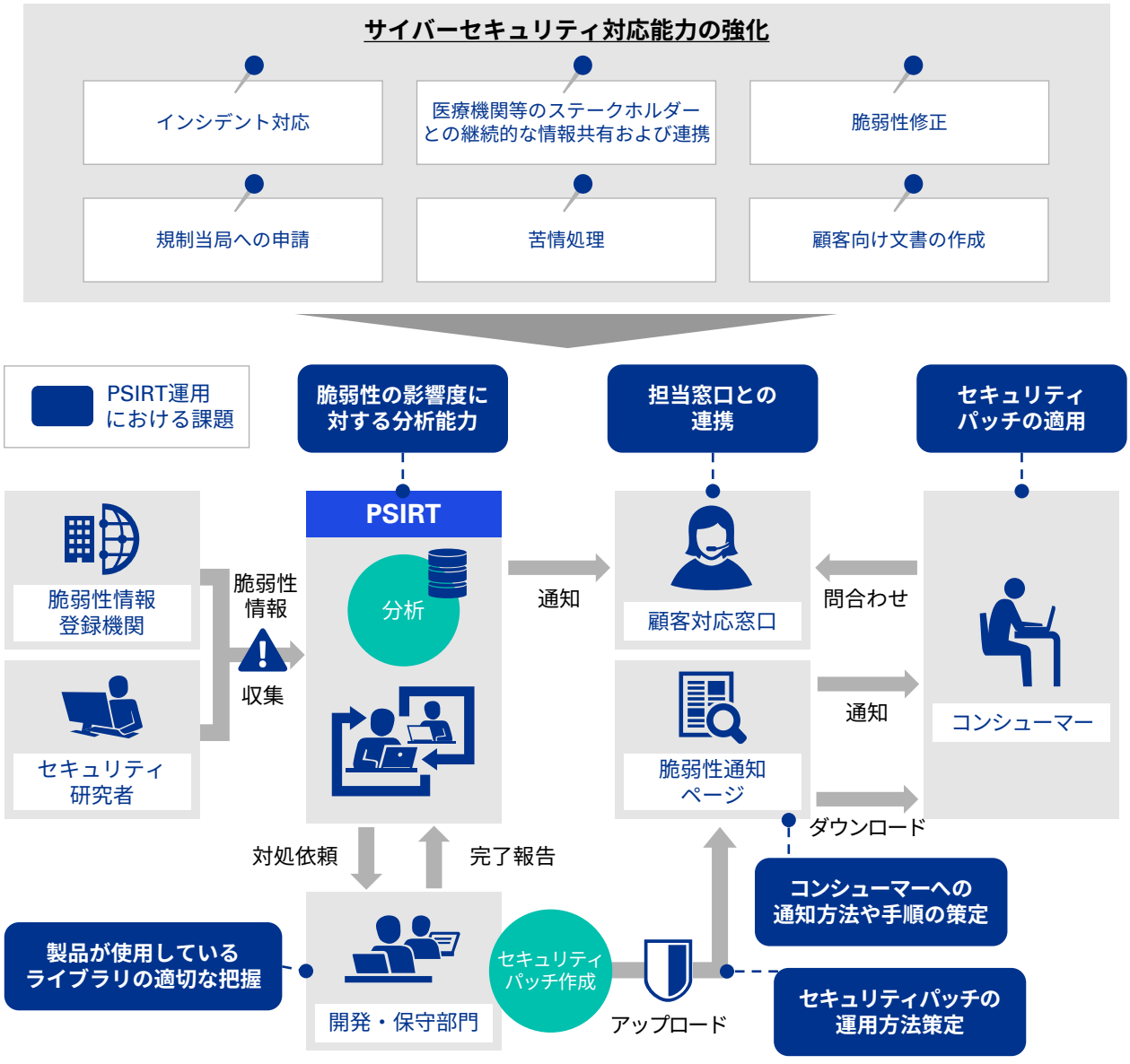
SBOM導入の観点と適用範囲（5W1H）

観点	主な適用項目
作成主体（Who）	■ 自組織で作成 ■ 取引契約のあるサプライヤーにて作成 ■ 取引契約のないサプライヤー（OSS[*3]コミュニティ等）にて作成
作成タイミング（When）	■ 製品計画時または開発計画時、プログラム開発時、ソフトウェアビルド時 ■ ソフトウェア納入時、コンポーネントのバージョンアップ時
活用主体（Who）	■ ソフトウェア利用者、最終製品ベンダー、開発ベンダー、最終製品ユーザー
対象とするコンポーネントの範囲（What、Where）	■ 開発主体が直接利用するコンポーネントのみ ■ 既製品等開発委託契約のないコンポーネントから再帰的に利用されるコンポーネントも含める
作成手段（How）	■ 構成管理情報を踏まえて手動で作成 ■ ツールを用いて自動で作成 ■ 一部は構成管理情報を踏まえて手動で作成、一部はツールを用いて自動で作成等、手動と自動を併用
活用範囲（Why）	■ 脆弱性管理、ライセンス管理、開発生産性の向上 ■ 資産管理、トレーサビリティ ■ 利用者や納入先に対するコンポーネントに関する情報の共有
フォーマット・項目（What）	■ 標準フォーマット（SPDX[*4]、SWID[*5]タグ） ■ 米国大統領令におけるデータフィールドの最小要素 ■ 規制・要求事項や業界の慣行として使用される独自のフォーマット

*3 OSS：オープンソースソフトウェア
*4 SPDX (Software Package Data Exchange)：システムを構成するソフトウェアについての情報を収集して管理するためのデータ形式の標準の1つ
*5 SWID (Software Identification) タグ：ソフトウェア製品の構成要素を識別するための標準化されたXMLフォーマット

PSIRT等の製品セキュリティ体制におけるSBOM活用

厚生労働省発行の「医療機器のサイバーセキュリティ導入に関する手引書」では、医療機器製造販売業者は医療機関、医療機器の使用者、規制当局または脆弱性発見者等のステークホルダーとの連携可能な体制（PSIRT）の構築が求められています。PSIRTを構築することで、ステークホルダーとサイバーセキュリティに関する情報を遅滞なく情報共有することが可能となります。また、医療機器製造販売業者のなかで脅威を特定し、関連するリスクを評価して、それを適宜対応するための能力を最大化することが期待されています。SBOMは、製品リスクを評価・共有するうえで、ベースとなる情報を提供する重要なツールとして、PSIRTが実現するセキュリティ機能のプロセスに組み込まれていることが重要です。KPMGは、PSIRT構築にあたり、関連部門とのシームレスな連携、SBOMの適切な管理、コンシューマーへの通知プロセスの確立などを支援します。



PSIRT構築によるステークホルダーとの連携

本リーフレットで紹介するサービスは、公認会計士法、独立性規則及び利益相反等の観点から、提供できる企業や提供できる業務の範囲等に一定の制限がかかる場合があります。詳しくはKPMGコンサルティング株式会社までお問い合わせください。

KPMGコンサルティング株式会社

T: 03-3548-5111
E: kc@jp.kpmg.com

kpmg.com/jp/kc