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

医療機器のセキュリティ規格 IEC 81001-5-1について

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

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

医療機器のセキュリティについての規格である、IEC 81001-5-1について、この規格でどのようなことが規定されているのか、その概略を次の流れで説明します。

- 全体の概要
- 箇条4から箇条9の概要
- トランジションヘルスソフトウェアについて

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

全体の概要

まず、全体の概要として、IEC 81001-5-1の概要や規格の構成について説明します。

規格の概要

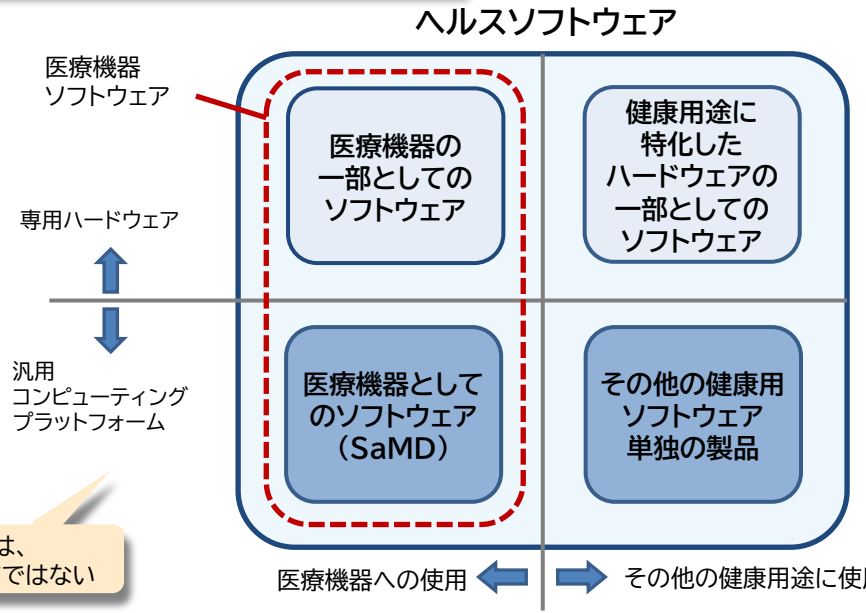
IEC 81001-5-1:2021

Health software and health IT systems safety, effectiveness and security – Part 5-1: Security – Activities in the product life cycle

(ヘルスソフトウェア及びヘルスITシステムの安全，有効性及びセキュリティ－第5-1部:セキュリティ－製品ライフサイクルにおけるアクティビティ)

現在JISを開発中で、
JIS T 81001-5-1として公示予定

- ISO/TC215(医療情報)及びIEC SC62A(医用電気機器)の合同作業班 JWG7(Safe, effective and secure health software and health IT systems, including those incorporating medical devices:安全、有効かつセキュアなヘルスソフトウェア及びヘルスITシステム、医療機器に組込むものを含む)で開発
- State of the art(最新の技術水準)と考えられる、IEC 62443-4-1(産業用自動制御システムの製品ライフサイクルのセキュリティ要求事項)への適合をサポートするために必要な、ヘルスソフトウェアの開発及び保守のライフサイクルの要求事項を規定
- ヘルスソフトウェアのサイバーセキュリティを強化するために、ライフサイクルにおいて実行するアクティビティをJIS T 2304の順序で記載



ヘルスソフトウェアは、
規制対象外のソフトウェアではない

IEC 81001-5-1:2021, Figure 1 – HEALTH SOFTWARE field of applicationより

規格の構成

ヘルスソフトウェアのサイバーセキュリティを強化するために、ライフサイクルにおいて実行するアクティビティをJIS T 2304の順序で記載している

	JIS T 2304
4	一般要求事項
5	ソフトウェア開発プロセス
6	ソフトウェア保守プロセス
7	ソフトウェアリスクマネジメントプロセス
8	ソフトウェア構成管理プロセス
9	ソフトウェア問題解決プロセス

	IEC 81001-5-1
4	一般要求事項
5	ソフトウェア開発プロセス
6	ソフトウェア保守プロセス
7	セキュリティに関連するリスクマネジメントプロセス
8	ソフトウェア構成管理プロセス
9	ソフトウェア問題解決プロセス

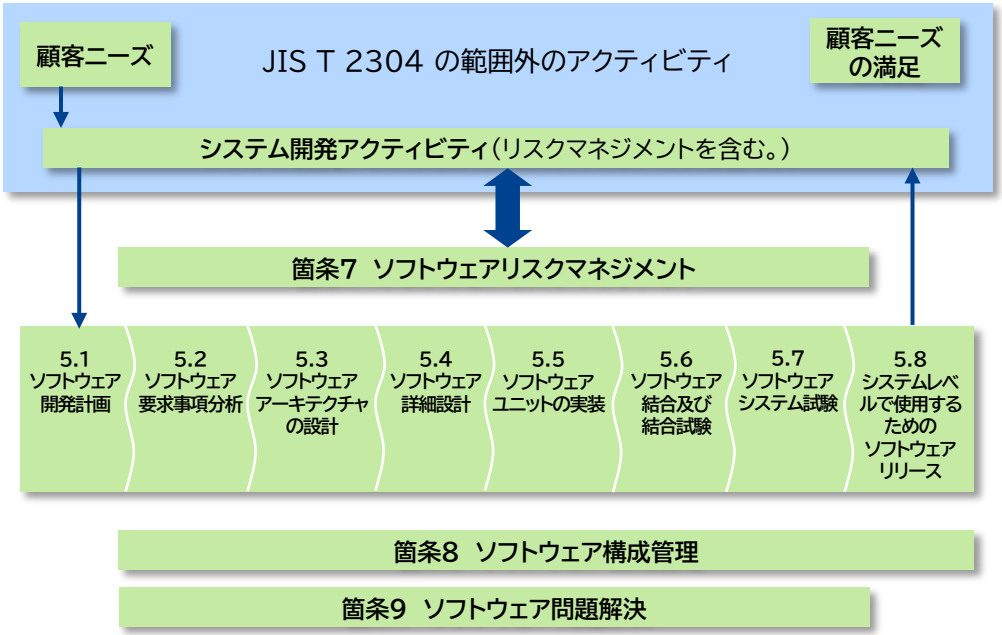
製造業者が品質マネジメントシステム及びリスクマネジメントシステムの下で，ヘルスソフトウェアを開発し保守することを規定

製造業者が実施するソフトウェアライフサイクルプロセスの一部として，アクティビティ及びその結果のアウトプットを規定

製造業者が実施する問題解決プロセスの一部として，アクティビティ及びその結果のアウトプットを規定

医療機器の場合は、ソフトウェアライフサイクルプロセスやリスクマネジメントプロセスが求められていて、各製造業者においてすでに実装されていると考えられるので、この規格では、セキュリティライフサイクルプロセスそのものを別途規定するのではなく、既存のプロセスの枠組みに追加するアクティビティを規定している。

JIS T 2304 ソフトウェアライフサイクルプロセスのおさらい



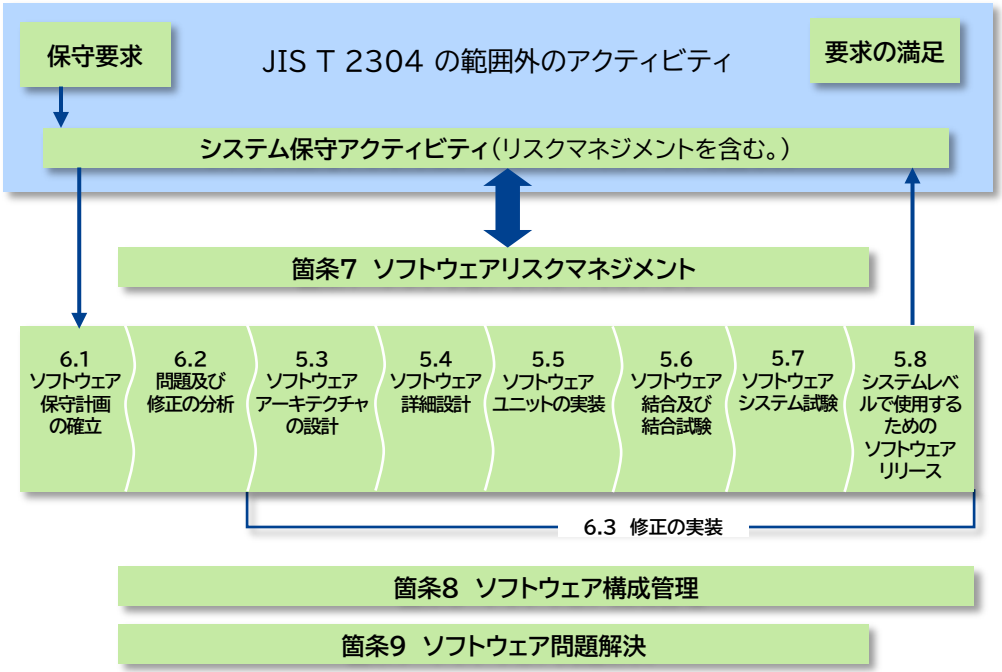
JIS T 2304:2017 図1－ソフトウェア開発プロセス及びアクティビティの関連図より

安全なソフトウェアを実現するためには、試験を実施するだけではなく、次が必要

- ハザードを特定し、関連するリスクが受容可能なレベルにまで低減されている。（リスクマネジメント）
- 適切なプロセスを規定し、それが効果的に実施されている。（ライフサイクルプロセス）

特定のライフサイクルモデルを規定するものではない

JIS T 2304 ソフトウェアライフサイクルプロセスのおさらい



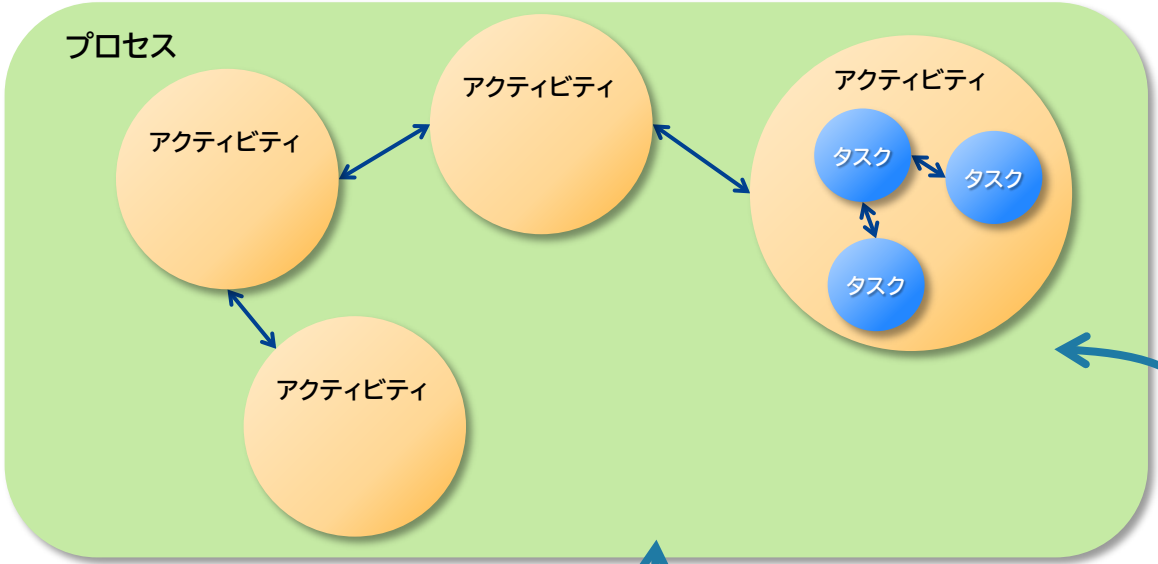
JIS T 2304:2017 図2－ソフトウェア保守プロセス及びアクティビティの関連図より

安全なソフトウェアを実現するためには、試験を実施するだけではなく、次が必要

- ハザードを特定し、関連するリスクが受容可能なレベルにまで低減されている。(リスクマネジメント)
- 適切なプロセスを規定し、それが効果的に実施されている。(ライフサイクルプロセス)

特定のライフサイクルモデルを規定するものではない

IEC 81001-5-1の構成のイメージ



JIS T 2304のライフサイクルプロセスや
JIS T 14971のリスクマネジメントプロセスに対して、
セキュリティに必要なアクティビティを追加するイメージ

アクティビティ

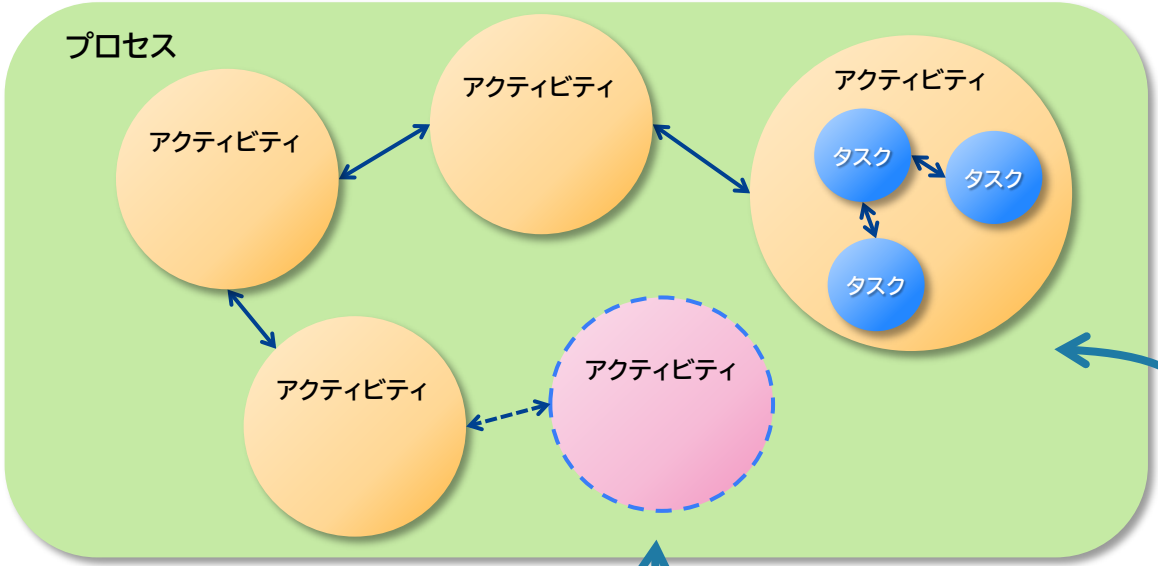
追加するアクティビティは、
IEC 62443-4-1の各箇条
の要求事項に由来

4. セキュリティマネジメント(SM)
5. セキュリティ要求事項の仕様(SR)
6. 設計によるセキュリティ(SD)
7. セキュアな実装(SI)
8. セキュリティの検証及びバリデーション試験(SVV)
9. セキュリティ関連問題の管理(DM)
10. セキュリティ更新の管理(SUM)
11. セキュリティのガイドライン(SG)

アクティビティ

「この規格においては, “アクティビティを確立する”とは, 製造業者がこのアクティビティを文書化し, 有効かつ完全に行うことを確実にすることを意味している。」

IEC 81001-5-1の構成のイメージ



JIS T 2304のライフサイクルプロセスや
JIS T 14971のリスクマネジメントプロセスに対して、
セキュリティに必要なアクティビティを追加するイメージ

アクティビティ

追加するアクティビティは、
IEC 62443-4-1の各箇条
の要求事項に由来

4. セキュリティマネジメント(SM)
5. セキュリティ要求事項の仕様(SR)
6. 設計によるセキュリティ(SD)
7. セキュアな実装(SI)
8. セキュリティの検証及びバリデーション試験(SVV)
9. セキュリティ関連問題の管理(DM)
10. セキュリティ更新の管理(SUM)
11. セキュリティのガイドライン(SG)

アクティビティ

「この規格においては, “アクティビティを確立する”とは, 製造業者がこのアクティビティを文書化し, 有効かつ完全に行うことを確実にすることを意味している。」

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

箇条4：一般要求事項

箇条4は、製造業者が品質マネジメントシステム及びリスクマネジメントシステムの下でヘルスソフトウェアを開発し保守することを規定しており、セキュリティに関連して必要なアクティビティを規定しています。

4.1 品質マネジメント

- 4.1は、品質マネジメントについてのセキュリティ関連事項を規定
- 品質マネジメントシステムは、JIS Q 13485又は同等の規格に従って実施可能(4.1.1)
- 一部の細分箇条については、JIS Q 13485の相応する規定の一部として実施可能と示されている。

4.1	品質マネジメント	(JIS Q 13485の一部として実施可能)	
4.1.1	品質マネジメントシステム		
4.1.2	責任の特定		
4.1.3	適用可能性の特定		
4.1.4	セキュリティの専門知識	6.2	人的資源
4.1.5	サードパーティの供給者からのソフトウェアアイテム		
4.1.6	継続的改善	8.5	改善
4.1.7	セキュリティ関連の問題の開示	7.2.3	コミュニケーション
4.1.8	セキュリティ欠陥マネジメントの定期的なレビュー	5.6	マネジメントレビュー
4.1.9	附属資料のレビュー	7.3	設計・開発

JIS T 2304とは異なり、アクティビティの選択は、ソフトウェア安全クラス分類にはよらないことに注意

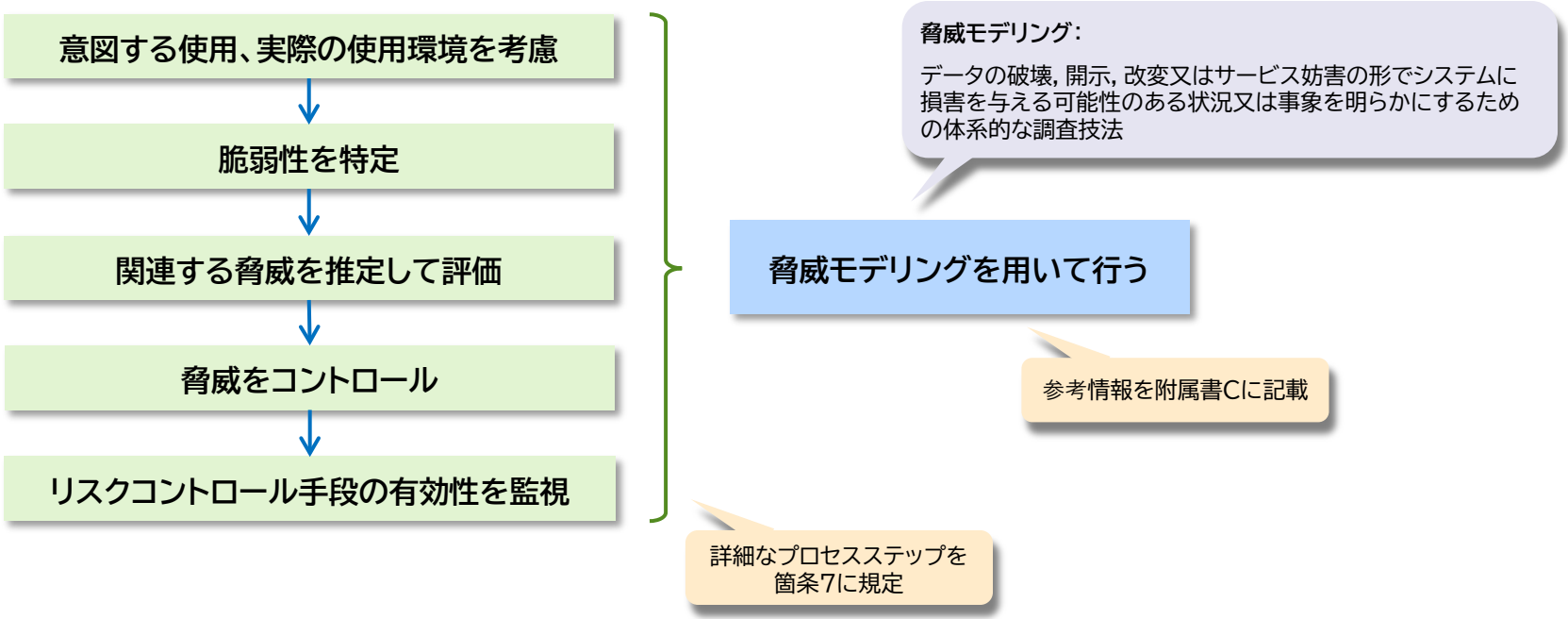
セキュリティに関連するソフトウェアアイテムを開発委託する場合には、委託先にもセキュリティのライフサイクルアクティビティを求める

規制当局及びユーザーに脆弱性を適時に開示する → 協調的な脆弱性の開示(CVD)

ソフトウェア問題解決プロセスの定期的レビュー

4.2 セキュリティに関連するリスクマネジメント

- セキュリティに関連するリスクマネジメントのプロセスを確立する

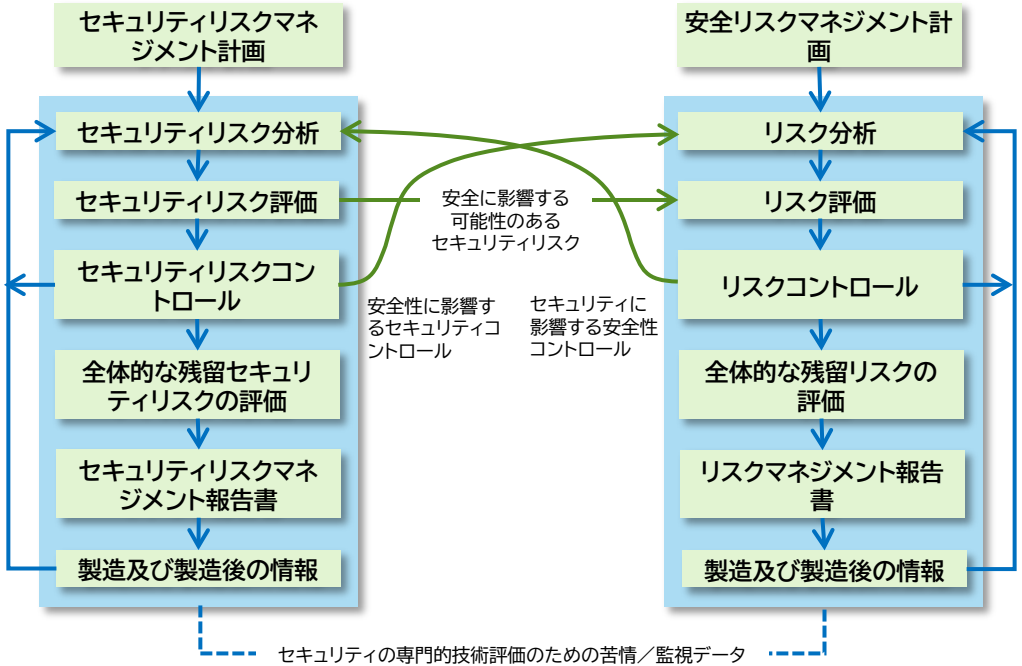


- 各脆弱性に対応するための適切な方法を決定する際に適用するリスクの受容可能性の判断基準を確立する

JIS T 14971とセキュリティ

これまで、JIS T 14971（ISO 14971）ではセキュリティのリスクマネジメントは対応しきれないとする考えもあったが、第3版となるJIS T 14971:2020（ISO 14971:2019）では、「この規格に規定するプロセスは，医療機器に関連する，生体適合性，データ及びシステムの**セキュリティ**，電気，動く部分，放射線，ユーザビリティなどに関するリスクに適用する。」と明確に規定している。

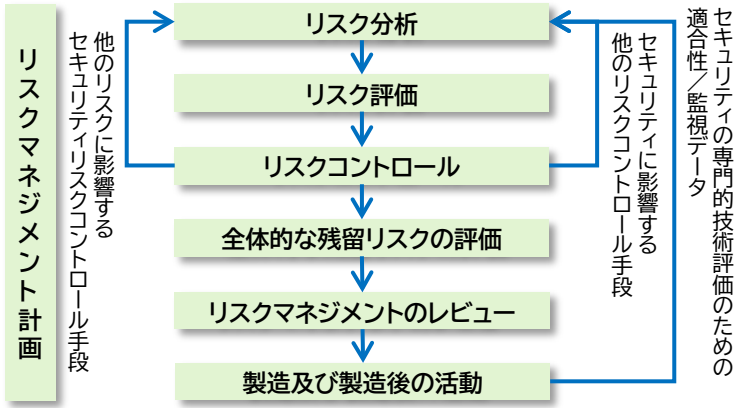
推奨するセキュリティリスクプロセス



ISO 14971:2007の安全リスクプロセス

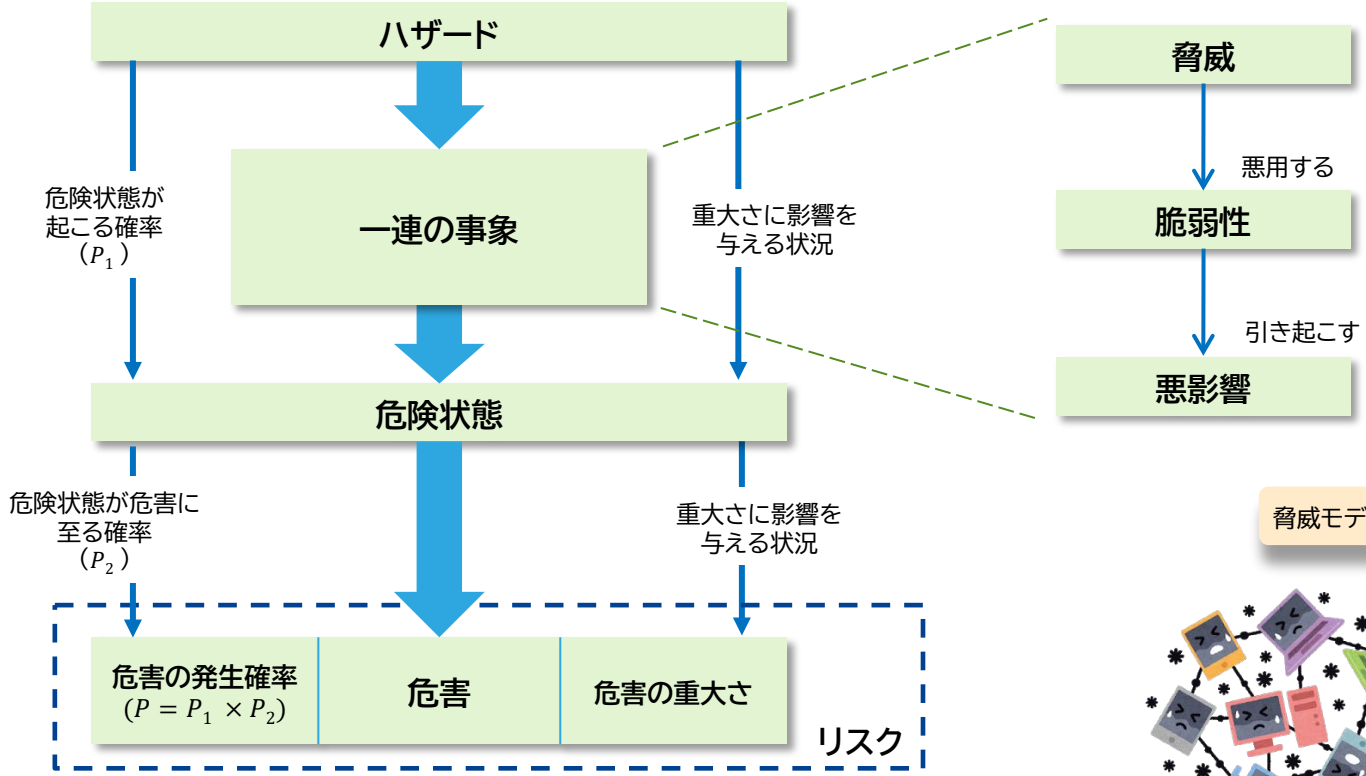
AAMI TIR57:2016の“Figure 4 – Relationships between the security risk and safety risk management process.”より

JIS T 14971のリスクマネジメントの枠組みで、セキュリティに対しても対応できるが、適切に行うためには、脆弱性、脅威及び他のセキュリティ関連の用語の適切なマッピングを行い、セキュリティ関連のアクティビティを追加することが必要である。



TR T 24971:2020の“図F.2 – セキュリティのリスクコントロール手段と他のリスクコントロール手段との相互作用”より

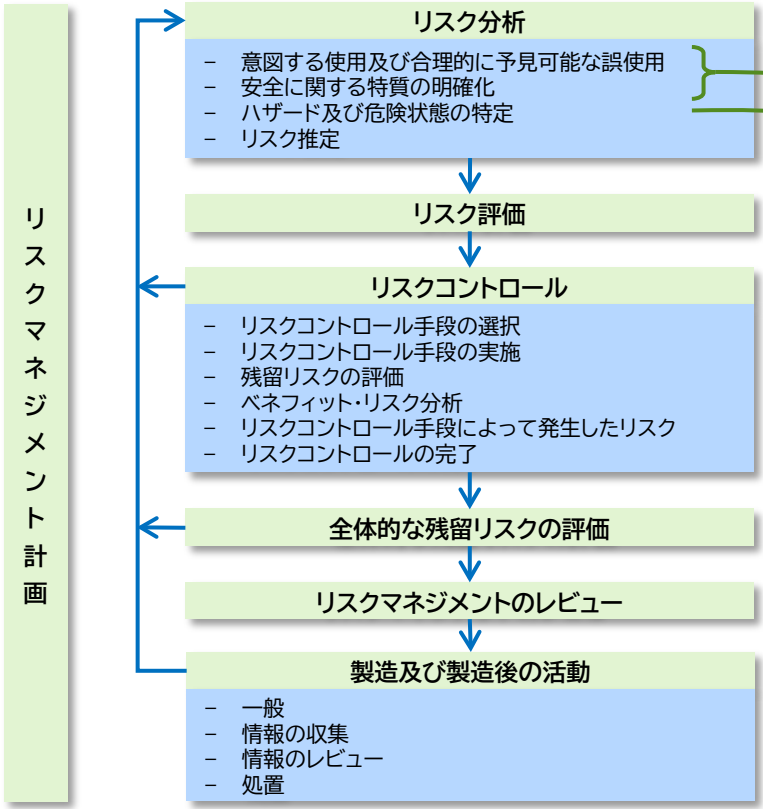
脆弱性、脅威及び他のセキュリティ関連の用語のマッピングの例



JIS T 14971:2020, 図C.1－ハザード, 一連の事象, 危険状態及び危害の関係の図解例より

JIS T 14971のリスクマネジメントプロセスと箇条7との対応

JIS T 14971のリスクマネジメントプロセスの概略



IEC 81001-5-1の箇条7に規定するリスクマネジメントプロセス

製造業者は，ヘルスソフトウェアに関連するセキュリティに関連するリスクをマネジメントするプロセスを，その製品リスクマネジメントのアプローチの一部として確立し，維持する。(7.1.1より)

- 7.1 リスクマネジメントのコンテキスト
- 7.2 ぜい(脆)弱性，脅威及び関連する悪影響の特定
- 7.3 セキュリティに関連するリスクの推定及び評価
- 7.4 セキュリティに関連するリスクのコントロール
- 7.5 リスクコントロールの有効性の監視

このプロセスは，既存の一般的なリスクマネジメントプロセスの一部とすることが可能である。(4.2 注記2より)

リスクマネジメントプロセスと他のプロセスとの関連

箇条4　一般要求事項

4.2　セキュリティに関連するリスクマネジメント

詳細を箇条7に規定

リスクマネジメントプロセスは、脅威モデリングの手法を用いて行い、
その結果を文書化した脅威モデルは、開発プロセスや問題解決プロセスで
参照して、対処する

箇条5　ソフトウェア開発プロセス

5.3　ソフトウェアアーキテクチャー設計

5.4　ソフトウェア設計

5.7　ソフトウェアシステム試験

セキュリティコンテキストは、
製品レベルの意図する使用環境
から導き出し、設計に反映する

多層防御を考慮し、
信頼境界を文書化

特定した脅威に対応する方法を設計に含めて、
システム試験で有効性を確認する

脅威モデル:
脅威モデリングのアクティビティを文書化した結果

脅威モデル

特定したすべての問題を対処する

箇条7　セキュリティに関連するリスクマネジメントプロセス

7.1　リスクマネジメントのコンテキスト

7.2　ぜい(脆)弱性，脅威及び関連する悪影響の特定

7.3　セキュリティに関連するリスクの推定及び評価

7.4　セキュリティに関連するリスクのコントロール

7.5　リスクコントロールの有効性の監視

脅威モデリング

箇条9　ソフトウェア問題解決プロセス

9.4　ぜい(脆)弱性の分析

9.5　セキュリティ関連の問題への対応

4.3 リスク移転に関連するソフトウェアアイテムの分類

- ソフトウェアアイテムの分類（保守対象ソフトウェア、サポート対象ソフトウェア、要求仕様対象ソフトウェアのうち、どれか）を文書化する。
- 分類は、リスク移転の観点から整理されている。
- JIS Q 13485の7.4（購買）の一部として実施可能。

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

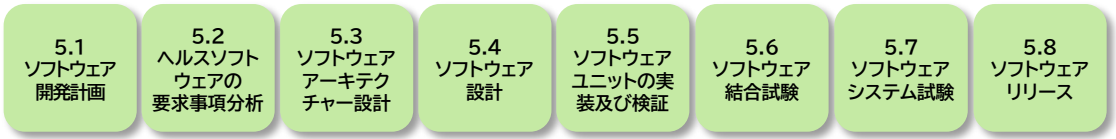
箇条5～9の説明

箇条4の一般要求事項の説明に続いて、下記の箇条5～9の各プロセスについて説明します。

- 箇条5：ソフトウェア開発プロセス
- 箇条6：ソフトウェア保守プロセス
- 箇条7：セキュリティに関連するリスクマネジメントプロセス
- 箇条8：ソフトウェア構成管理プロセス
- 箇条9：ソフトウェア問題解決プロセス

箇条5　ソフトウェア開発プロセス

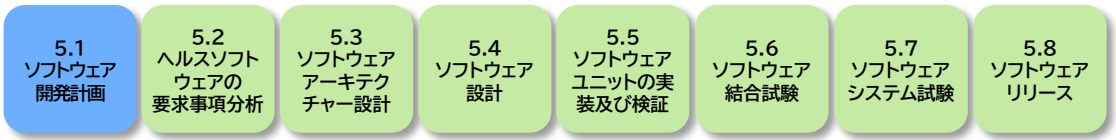
- 5.1　ソフトウェア開発計画
- 5.2　ヘルスソフトウェアの要求事項分析
- 5.3　ソフトウェアアーキテクチャー設計
- 5.4　ソフトウェア設計
- 5.5　ソフトウェアユニットの実装及び検証
- 5.6　ソフトウェア結合試験
- 5.7　ソフトウェアシステム試験
- 5.8　ソフトウェアリリース



5.1 ソフトウェア開発計画

要求事項の内容	説明
構想から使用停止に至る全般的なライフサイクルのアクティビティを確立する	JIS T 2304のソフトウェアライフサイクルプロセスの計画に加えて、セキュリティ関連のアクティビティとして、セキュリティ更新及びパッチに関連したアクティビティを追加して計画する。追加アクティビティについても、文書化したうえで、有効かつ完全に実施する。
この規格の要求事項を実施しない正当性について文書化する	ソフトウェアが含まれる医療機器だとしても、外部接続が全くないということであれば、この規格を適用する必要はない。セキュリティの専門知識を持つ人がレビューして承認し、きちんと文書化しておく。
開発環境のセキュリティを考慮する	開発環境が攻撃されて、例えば、怪しいコードが製品のプログラムに混入されたとしたら、市場に出荷される製品が最初からマルウェア等に感染してしまうことになる。
セキュアコーディングの規約を確立する	セキュリティの弱みが知られているデザインパターンを避ける、避けるべきソフトウェア機能（使用禁止関数など）を用いないなど、具体例が附属書A.4に示されている。

※JIS T 2304の開発計画においても、単に日程計画にとどまらず、開発手法やツールについても計画することが求められており、セキュリティに対応するためには、開発環境のセキュリティやセキュアコーディングの規約等を考慮する。



5.2 ヘルスソフトウェアの要求事項分析

要求事項の内容	説明
セキュリティ要求事項の文書化を行う（据付け、運用、保守及び使用停止に関連するセキュリティ機能の要求事項を含む）	セキュリティ機能については、IEC/TR 60601-4-5やIEC 80001-2-2などが参考になる。
セキュリティ要求事項のレビューを行う。レビュー担当者の独立性レベルを文書化する	レビューの担当には、開発担当、試験担当、機能横断的エキスパート（臨床知識をもつ人など）、セキュリティのアドバイザーの各分野の人を含める。
要求仕様対象ソフトウェアのセキュリティリスクを特定し、マネジメントする	セキュリティ更新の提供や情報提供をしないソフトウェアコンポーネントに対しても、要求事項分析の段階では、セキュリティのリスクマネジメントを行う。

5.3 ソフトウェアアーキテクチャー設計

要求事項の内容	説明
セキュアなアーキテクチャーを定める（多層防御の考慮が望ましい）。 セキュリティのリスクコントロールは、安全又は性能の要求事項を考慮する	多層防御とは、一連の防御メカニズムを積み重ね、一つのメカニズムが失敗した場合でも、もう一つの層が攻撃を防ぎ、全体としてセキュリティを強化することである。多層防御には、ユーザー側で実施するセキュリティ保護を含めることがある。セキュリティのリスクコントロールは、安全や性能の要求事項とバランスの取れたものであることが必要。
セキュアな設計のベストプラクティスを特定し、実行し、維持する。 ベストプラクティスは文書化する。 多重防御の一部としてセキュリティアーキテクチャーを定める	セキュアな設計のベストプラクティスとしては、信頼境界を全て文書化する、最小権限、シンプルな設計、セキュアな設計パターンの使用、攻撃対象領域の削減、デバッグ用ポートやデバッグ情報の除去などがある（これには限定しない）。これらを、アーキテクチャー設計においても考慮する。（5.4のソフトウェア設計においても同様に考慮する。）
悪条件における動作に関して、アーキテクチャーのレビューを行う（文書化し、実施する）	他のソフトウェアアイテムから意図しない影響を受けないように、アーキテクチャ設計で分離を考慮する、アーキテクチャーがセキュリティの欠陥をもたらさないようにする。

5.4 ソフトウェア設計

要求事項	説明
セキュアなヘルスソフトウェアを設計・開発し、文書化し、ベストプラクティスの使用を維持する	アルゴリズムなどのソフトウェア技術、プログラミング言語、5.3で示した設計のベストプラクティスを考慮して行う。
ヘルスソフトウェアの設計には、脅威モデルにおいて特定した脅威に対応する方法を含める	リスクコントロールを多層防御の様々なレイヤーで実施するよう設計する。
物理的及び論理的インターフェイスを含む、ヘルスソフトウェアのインターフェイスを特定し、特性を明確化する	インターフェイスは、様々な構成要素間のLAN、Wi-Fi、その他のネットワーク接続の他、ソフトウェアコンポーネント間のメッセージングやAPI、通信プロトコルなどを考慮する。どんなインターフェイスがあり、データフローやコントロールフローは何か、信頼境界を超えるアクセスの有無、保護方法、アクセスコントロール、影響を受ける資産などを特定する。
詳細設計の検証を行う（関連する弱みを特定し、特性を明確化し、問題解決まで追跡する）	脅威モデリングで検討した、脅威ー脆弱性ー悪影響について、詳細設計で考慮されているか、問題解決プロセスでの対応にトレーサビリティがあるかどうか確認する。

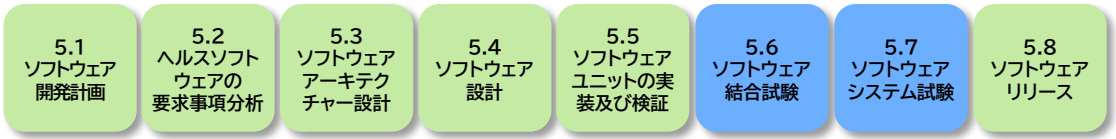
5.5 ソフトウェアユニットの実装及び検証

要求事項の内容	説明
セキュアコーディングの規約に従って実装する	セキュアコーディングのベストプラクティスとしては、セキュリティの弱みが知られているデザインパターンや使用禁止関数を避ける、静的解析ツールなどの自動化ツールを使用する、MISRA-Cなどの一般的なコーディング規約を用いる、信頼境界を超えるインプットは正当性確認をする、などがある。
実装レビューを行い、実装に係るセキュリティ関連の問題を特定し、特性を明確化し、問題解決プロセスに取り込む	適切に実装されていないセキュリティ要求事項がないか、従っていないセキュアコーディングの規約はないか、セキュリティ設計に対するセキュリティ機能の実装とトレーサビリティのレビュー、実装したインターフェイス、信頼境界、資産が脅威によって侵害されるかどうかを調べる。

5.6 ソフトウェア結合試験、5.7 ソフトウェアシステム試験

- 5.6は、ソフトウェアシステム試験の一部を，ソフトウェア結合試験の一部として実施することができることを規定。5.7は次の通り。

要求事項の内容	説明
セキュリティ要求事項試験：セキュリティの機能が、セキュリティ要求事項を満たしており、エラーのシナリオや不正な入力に対応していることを検証する	意図する使用環境に基づいて、機能試験、性能及びスケーラブル試験、境界・エッジ試験、クラウド等のサービスに対する試験など。
脅威軽減試験：脅威モデルで特定し、評価した脅威について、軽減策の有効性を試験する	例えば、不正データや過大負荷に対する振る舞いを検出するための入力バリデーション試験。
脆弱性試験：潜在的なセキュリティ脆弱性を特定し、特性を明確化する試験を実施する	ぜい(脆)弱性スキャンによって、既知のぜい(脆)弱性を自動検出する。
侵入試験：セキュリティ脆弱性を発見し悪用する試験を行って、弱みを特定し、特性を明確化する	攻撃者のアプローチで、機密性、完全性、可用性の侵害を試みる試験。
試験担当者と開発担当者との間の利益相反を管理して、試験の客観性を確実にする	(準)独立の内部試験チームあるいはセキュリティ試験組織の導入などを検討する。



5.8 ソフトウェアリリース

要求事項の内容	説明
システム試験で見つかった全ての事項が問題解決プロセスで対処されたことを確実にする	JIS T 2304の5.8.1 ソフトウェア検証の完了確認とほぼ同等。
附属資料の要求事項を確立する	セキュアな運用の指針、アカウント管理の指針、セキュリティ上の残留リスクについての情報などをユーザーに提供する。
関連するファイル(スクリプト、実行ファイル含む)の完全性の検証メカニズムを提供する	ユーザーが提供されたファイルが改変されていないか、確認できるようにする。暗号化ハッシュ、デジタル署名など。
コード署名に用いる秘密鍵を不正アクセス又は改変から保護する	手順、技術的コントロールを行って、確実に保護できるようにする。
セキュリティ関連問題の対処、追跡が完了してからリリースする	開発中に見つかった問題を適切に対応してからリリースする。
リリース前に全てのプロセスが完了したことを文書化し、それを検証する	JIS T 2304の5.8.6 アクティビティ及びタスクの完了確認とほぼ同等。
ヘルスソフトウェアの使用を終了する際の指針を含む製品ユーザー文書を作成する	機微情報や所有権のあるソフトウェア等を適切に取り除く手順を示す。

5.1 ソフトウェア開発計画 | 5.2 ヘルスソフトウェアの要求事項分析 | 5.3 ソフトウェアアーキテクチャー設計 | 5.4 ソフトウェア設計 | 5.5 ソフトウェアユニットの実装及び検証 | 5.6 ソフトウェア結合試験 | 5.7 ソフトウェアシステム試験 | 5.8 ソフトウェアリリース

箇条6　ソフトウェア保守プロセス

細分箇条	内容
6.1　ソフトウェア保守計画の確立	セキュリティ更新をどれくらいの時間で確認してユーザーに配送するかについて、組織としての対応方針を定める
6.2　問題及び修正の分析	セキュリティ更新を提供又は情報提供するソフトウェアアイテムについて、関連情報を収集し、レビューする。
	セキュリティ更新が脆弱性に対応できていることを検証する
6.3　変更の実装	セキュリティ更新について文書化する
	セキュリティ更新を提供するソフトウェアについて、更新をユーザーに配送する
	ユーザーが正しいパッチを確実に入手できるようにする（ユーザーがパッチが正しいものであるか確認できるようにする）

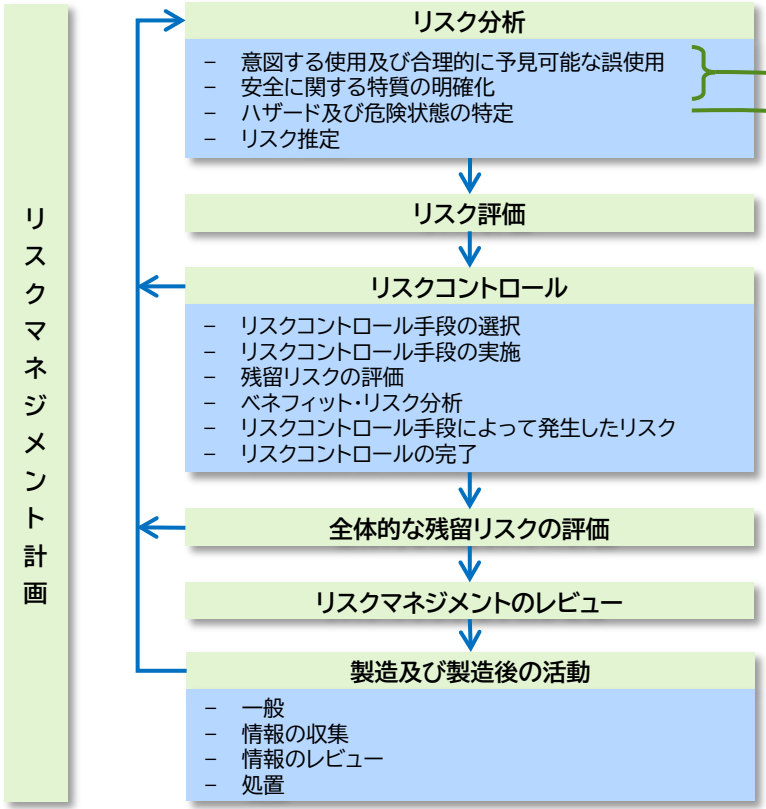
JIS T 2304の箇条6の要求事項に加えて、これらを行う。

JIS T 2304の箇条6の細分箇条の構成（参考）

6.1　ソフトウェア保守計画の確立			
6.2　問題及び修正の分析	6.2.1　フィードバックの文書化及び評価	6.3　修正の実装	6.3.1　確立したプロセスを使用した修正の実装
	6.2.2　ソフトウェア問題解決プロセスの使用		6.3.2　修正ソフトウェアシステムの再リリース
	6.2.3　変更要求の分析		
	6.2.4　変更要求の承認		
	6.2.5　ユーザー及び規制当局への通知		

箇条7　セキュリティに関連するリスクマネジメントプロセス（再掲）

JIS T 14971のリスクマネジメントプロセスの概略



IEC 81001-5-1の箇条7に規定するリスクマネジメントプロセス

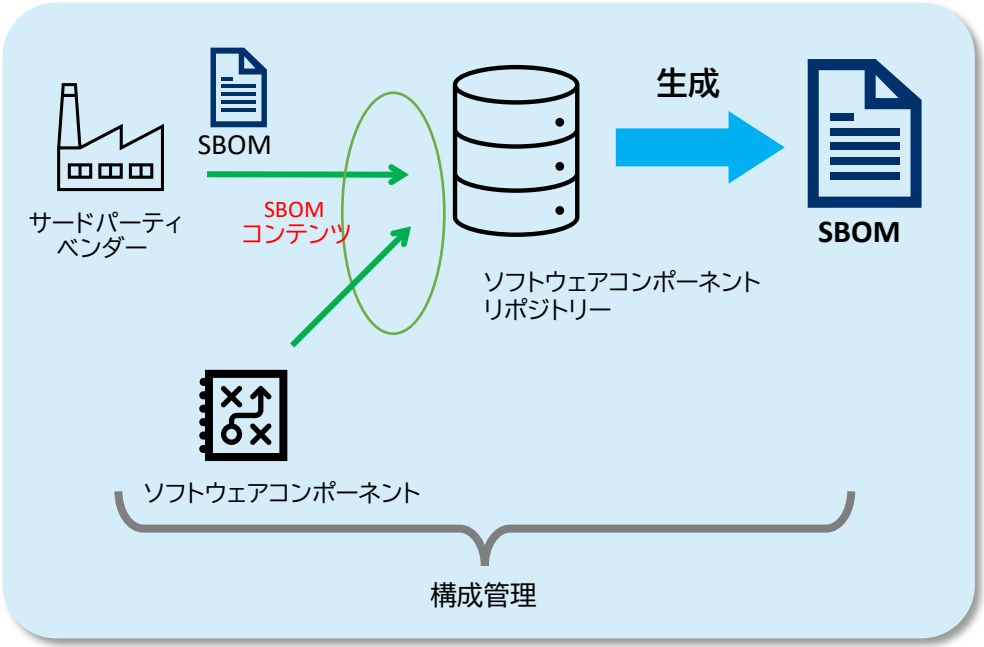
製造業者は，ヘルスソフトウェアに関連するセキュリティに関連するリスクをマネジメントするプロセスを，その製品リスクマネジメントのアプローチの一部として確立し，維持する。（7.1.1より）

- 7.1 リスクマネジメントのコンテキスト
- 7.2 ぜい（脆）弱性，脅威及び関連する悪影響の特定
- 7.3 セキュリティに関連するリスクの推定及び評価
- 7.4 セキュリティに関連するリスクのコントロール
- 7.5 リスクコントロールの有効性の監視

このプロセスは，既存の一般的なリスクマネジメントプロセスの一部とすることが可能である。（4.2 注記2より）

箇条8　ソフトウェア構成管理プロセス

既にリリースした又は市場にあるヘルスソフトウェアに対しても，セキュリティの責務として，構成管理を行い，ぜい(脆)弱性の影響を受けやすい，又は受ける可能性がある，含まれる外部コンポーネントのリストを再現可能とする。



SBOM(ソフトウェア部品表)を作成できるように構成管理を行うことを求めている。

箇条9　ソフトウェア問題解決プロセス

セキュリティ関連の問題を取り扱うために使用するアクティビティが規定されている。

- 脆弱性については、通知を受け、レビューし、分析する
- セキュリティ問題への対応は、次によって行う
  - 対応するアクティビティを確立し、4.1.7（セキュリティ関連の問題の開示）に従って、開示するかどうかを決定する
  - セキュリティ関連リスクに対して、対処するかどうか、どのように対処するかを決定する（対処は、ソフトウェア問題解決プロセスで行うか、意図する使用環境に関する仕様変更によって行う）
  - 設計又は実装に対する全ての変更をレビューする
  - 他のプロセスに対して情報提供する
  - サードパーティ製ソースコードの問題は、サードパーティに通知する
  - 未解決問題については、定期的にレビューする

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

トランジションヘルスソフトウェアについて

この規格の発行前にリリースされ、この規格の箇条4～箇条9に規定する全ての要求事項には適合していないヘルスソフトウェアについて、どのように規定されているか説明します。

トランジションヘルスソフトウェアについて

トランジションヘルスソフトウェア：
この規格の発行前にリリースされ、この規格の箇条4～箇条9に規定する全ての要求事項には適合していないヘルスソフトウェアのこと

再開発する

セキュリティを改善する

- セキュリティ運用ガイドラインの更新
- 補完的コントロールの義務づけ
- 一部のソフトウェアの書直し、等々

そのためのアクティビティを、F.2～F.4に規定

附属書Fへの適合宣言

- JIS T 2304のレガシーソフトウェアの考え方は、セキュリティ対応には不十分
- IMDRFガイダンスのレガシー医療機器も考慮して、レガシーではなく、トランジション（過渡的）ヘルスソフトウェアと呼んでいる

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

IEC 81001-5-1の概要及び内容の考え方について、説明しました。詳細については、今後公示される予定のJIS T 81001-5-1も併せてご参照ください。

ご清聴ありがとうございました。