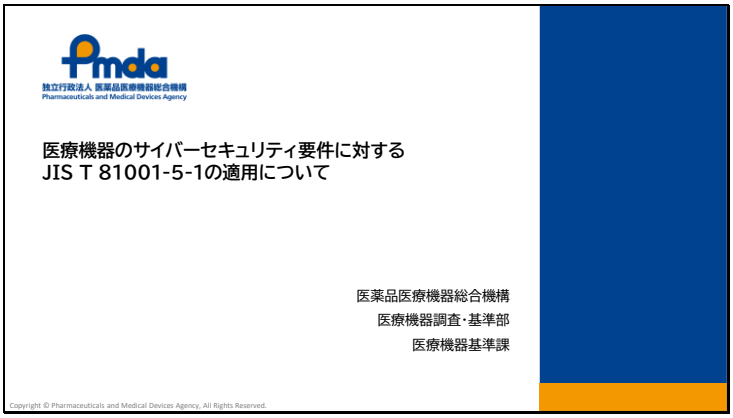
医療機器のサイバーセキュリティ要件に対する JIS T 81001-5-1 の適用について

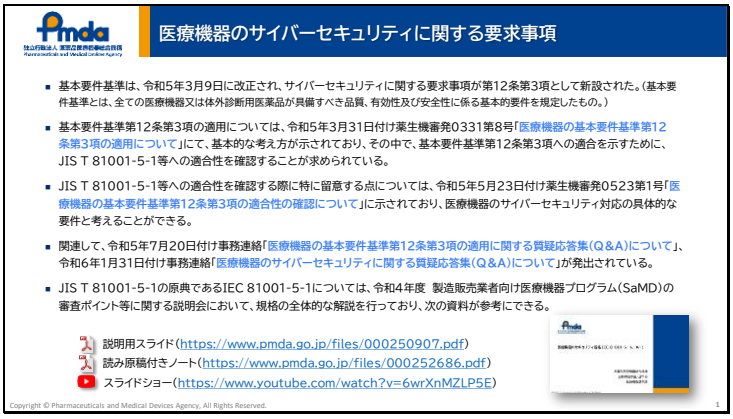
（2023 年度 登録認証機関向けトレーニング資料）

Slide 0



医療機器のサイバーセキュリティ要件に対して、JIS T 81001-5-1をどのように適用するかについて説明します。

Slide 1



医療機器の基本要件基準は、令和5年3月9日に改正され、サイバーセキュリティに関する要求事項が第12条第3項として新設されました。

この第12条第3項の適用については、令和5年3月31日付の通知で、基本的な考え方が示されており、適合を示すためにJIS T 81001-5-1等への適合性を確認することが求められています。

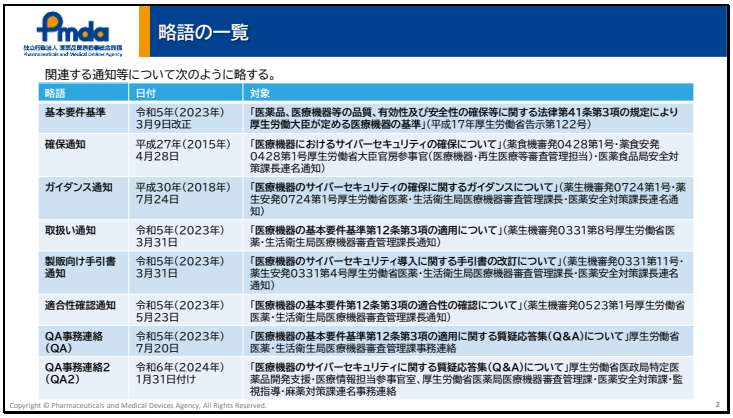
また、JIS T 81001-5-1等への適合性を確認する際に特に留意する点については、令和5年5月23日付通知に示されており、医療機器のサイバーセキュリティ対応の具体的な要件であると考えることができます。

これに関連して、令和5年7月20日付けで事務連絡「医療機器の基本要件第12条第3項の適用に関する質疑応答集（Q&A）について」、また令和６年1月31日付け事務連絡で、「医療機器のサイバーセキュリティに関する質疑応答集（Q&A)について」も出ています。

JIS T 81001-5-1は、IEC 81001-5-1と同じ内容の日本産業規格ですが、IECについては、令和4年度 製造販売業者向け医療機器プログラムの審査ポイント等に関する説明会で、規格の全体的な解説を行っています。ここに説明資料やYouTubeのリンクを示しますので、これらの資料を参考にしていただければ、と思います。

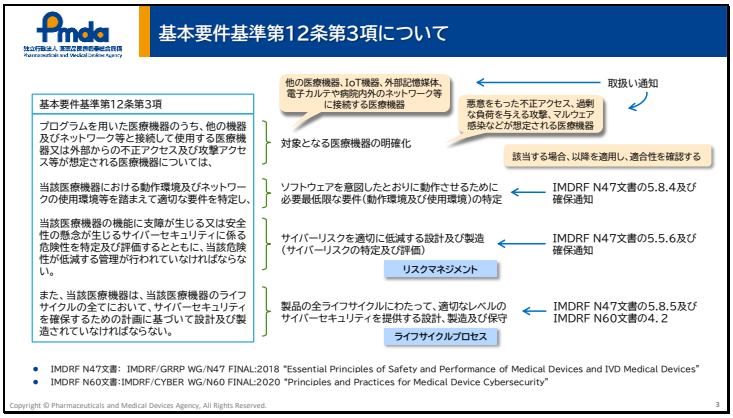
今回の説明では、令和5年5月23日付で発出された「医療機器の基本要件基準第12条第3項の適合性の確認について」で示されている、確認の上での留意点を考慮して、質疑応答集の内容も踏まえて、JIS T 81001-5-1の要点を解説します。

Slide 2



この資料においては、関連する通知等について、次のように略しています。

Slide 3



まず、基本要件基準第12条第3項の内容についてですが、ここに示しているような内容になっています。

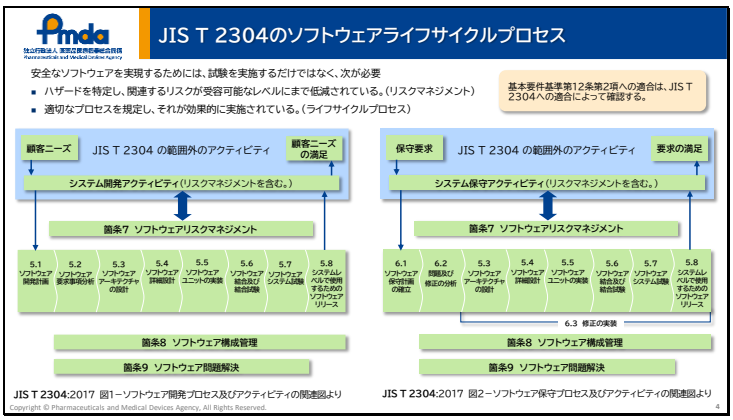
最初のパートでは、対象となる医療機器の明確化を行い、
次に、ソフトウェアを意図したとおりに動作させるための必要最低限な要件（動作環境や使用環境）を特定すること、
そして、サイバーセキュリティのリスクを適切に低減する設計及び製造を行うこと、製品の全ライフサイクルにわたって、適切なレベルのサイバーセキュリティを提供するような設計、製造及び保守を行うこと、
を求めています。

この内容については、確保通知の内容と、IMDRFで定めた、医療機器の基本要件についてのN47文書及びサイバーセキュリティについてのN60文書を踏まえたものになっています。

なお、対象となる医療機器については、取扱い通知ではこのように解説されていますが、ネットワークに対する接続だけでなく、USBメモリ等の外部記憶媒体経由でのマルウェア感染等も想定し、また、その医療機器自身がサイバー攻撃を受ける他、医療機器が踏み台となる場合も含め、サイバーセキュリティの危険性を生じるかどうかを考慮して判断していただければ、と思います。

取扱い通知に示されている対象の医療機器に該当する場合は、動作環境、使用環境の特定を行ったうえで、リスク分析をして対応・管理することが必要になります。クラウドにアクセスして用いる医療機器プログラムにおいても、医療機器であるプログラム部分について同様の対応が必要です。

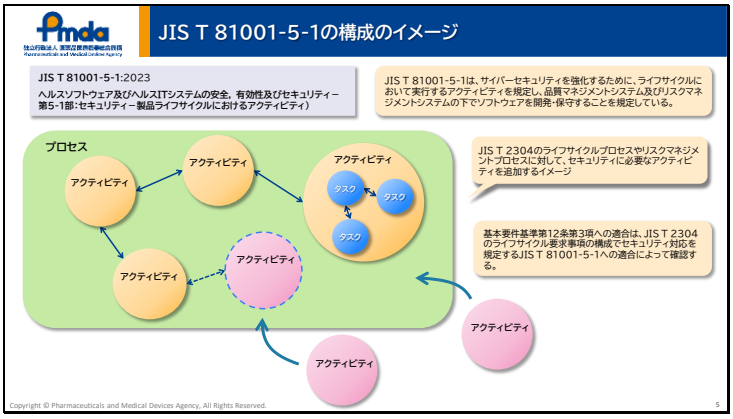
Slide 4



基本要件基準の第12条第3項では、リスクマネジメントやライフサイクルプロセスについて示されています。
安全なソフトウェアを実現するためには、ハザードを特定し、関連するリスクが受容

可能なレベルまで低減されているというリスクマネジメントの考え方と、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というライフサイクルプロセスの考え方が必要です。JIS T 2304においては、開発及び保守について、ライフサイクルプロセス及びそれを支援するリスクマネジメント、構成管理、問題解決のプロセスが規定されていて、第12条第2項の適合のために、すでに各製販においては、これらが実装されています。

Slide 5

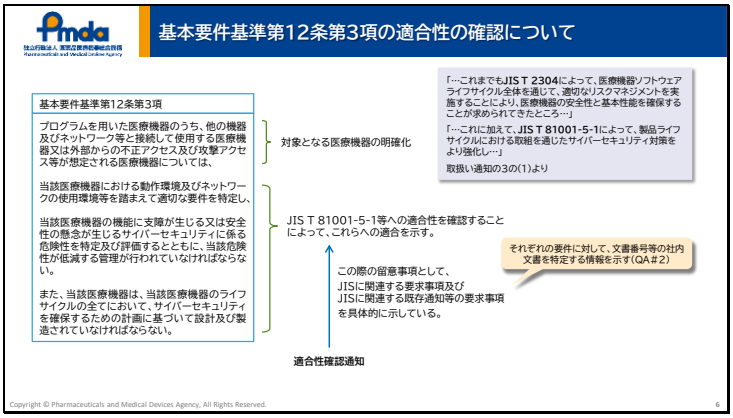


JIS T 81001-5-1は、サイバーセキュリティを強化するために、ライフサイクルにおいて実行するアクティビティを規定し、品質マネジメントシステム及びリスクマネジメントシステムの下でソフトウェアを開発・保守することを規定する規格です。

JIS T 81001-5-1の構成は、ここにあるとおり、JIS T 2304の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に対して、サイバーセキュリティに必要なアクティビティを追加するようなイメージです。

第12条第3項のサイバーセキュリティについては、JIS T 2304のライフサイクルの構成でセキュリティ対応を規定するJIS T 81001-5-1を用いて、先ほど示したようなJIS T 2304に規定するプロセスに対して、アドオンする形でセキュリティのためのアクティビティを実施するということになります。

Slide 6

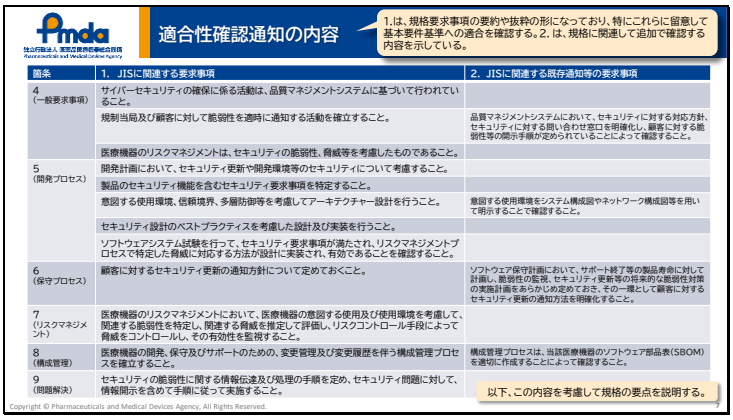


取扱い通知には、このような（右上）説明があり、基本要件基準第12条第3項の適合性の確認は、JIS T 81001-5-1等への適合性を確認することによって示す、とされています。

令和5年5月23日に発出された適合性確認通知では、基本要件基準第12条第3項への適合を示すために、規格への適合を確認する際の留意事項として、JISに関連する要求事項及びJISに関連する既存通知等の要求事項を具体的に示しています。

また、7月20日付で出されている、質疑応答集、Q&Aの事務連絡の第2項によれば、適合性を示す際には、適合性確認通知で示されているそれぞれの要件に対して、文書番号等の社内文書を特定する情報を示すということになっています。

Slide 7

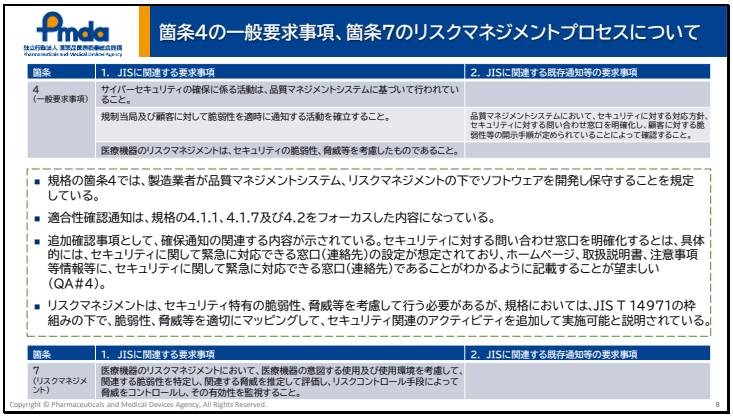


適合性確認通知の内容ですが、JIS T 81001-5-1の箇条4～9に対して、各箇条の要求事項の要約や抜粋の形で、1.のJISに関連する要求事項がまとめられており、特にこれらに留意して基本要件への適合を確認します。

2.には、既存の通知ですでに要求されていた内容や規格への適合状況を端的に示す内容など、規格に関連して追加で確認すべき内容が示されています。

以下、この内容を考慮して、規格の要点を説明します。

Slide 8



規格の箇条4　一般要求事項では、製造業者が品質マネジメントシステム、リスクマネジメントの下でソフトウェアを開発し、保守することを規定しています。

適合性確認通知では、規格の4.1.1 品質マネジメントシステム、4.1.7 セキュリティ関連の問題の通知、4.2 セキュリティに関連するリスクマネジメントについてフォーカスした内容となっています。

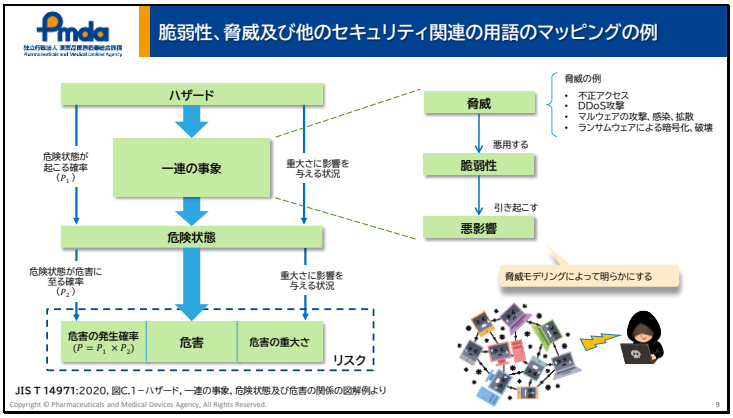
つまり、サイバーセキュリティ関連の活動は、品質マネジメントシステムに基づいて行うこと、脆弱性を適時に通知する活動を確立すること、リスクマネジメントは、セキュリティの脆弱性、脅威等を考慮することです。

追加の確認事項としては、平成27年の確保通知の関連する内容が示されています。品質マネジメントシステムにおいて、セキュリティに対する対応方針、セキュリティに対する問い合わせ窓口を明確化し、顧客に対する脆弱性等の開示手順が定められていることですが、方針等を明確化し、手順に基づいて行うという品質マネジメントシステムの考え方をベースにしています。

ここでセキュリティに対する問い合わせ窓口を明確化するとは、具体的には、セキュリティに関して緊急に対応できる窓口の設定が想定されており、ホームページ、取扱説明書、注意事項等表示などで、緊急対応窓口であることがわかるような形で記載することが望ましいとQ&Aでは解説されています。

また、リスクマネジメントについては、セキュリティ特有の脆弱性、脅威等を考慮して行うことが必要で、箇条7に関連する要求事項として、医療機器の意図する使用及び使用環境を考慮して、関連する脆弱性を特定し、関連する脅威を推定して評価し、リスクコントロール手段によって脅威をコントロールし、その有効性を監視することとされていますが、規格においては、これはJIS T 14971の枠組みの下で、脆弱性、脅威等を適切にマッピングして、セキュリティ関連のアクティビティを追加して行うことができると説明されています。

Slide 9



脆弱性や脅威などのセキュリティ用語のマッピングの例を示します。

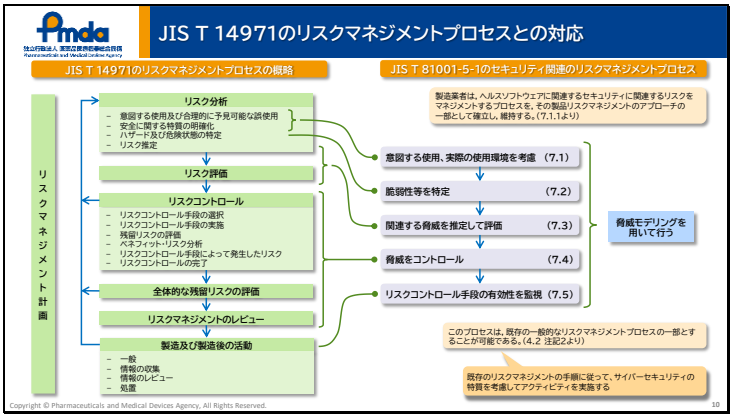
左側に示しているのが、JIS T 14971に示している、ハザード、一連の事象、危険状態及び危害の関係図です。一連の事象によって、ハザードにさらされ、危険状態が起こり、危害につながるという関係によってリスクを考えていくということです。

セキュリティ関係については、一連の事象において、脅威が脆弱性を悪用し、悪影響を引き起こす、というふうに対応させることができます。対応付けについては、この他にもいろいろな考え方がありますが、これは、その中の一例を示しています。

ここで、脅威の例としては、不正アクセス、DDoS攻撃、マルウェアの攻撃、感染、拡散、ランサムウェアによる暗号化、破壊などがあり、それらがシステムの脆弱性を悪用して、悪影響を引き起こす、これによってハザードにさらされ、危険状態が起こり、危害につながる、というように考えると理解しやすいかと思います。

そして、脅威が脆弱性を悪用し、悪影響を引き起こす、という一連の流れについて、脅威モデリングの様々なアプローチを使って、体系的に調査して、明らかにしていく、ということが、IEC 81001-5-1でセキュリティのリスクマネジメントで求めている内容です。

Slide 10

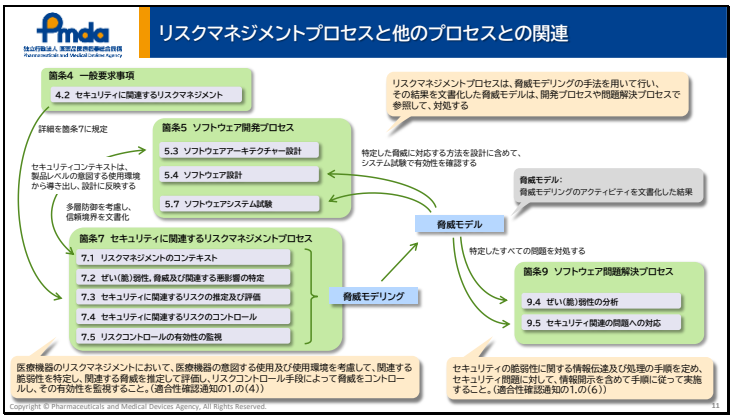


JIS T 81001-5-1の箇条7では、リスクマネジメントプロセスのステップを7.1～7.5にわたって規定しています。

つまり、意図する使用、実際の使用環境を考慮し、脆弱性等を特定し、関連する脅威を推定して評価し、脅威をコントロールし、リスクコントロール手段の有効性を監視する、という流れになります。

これは、それぞれJIS T 14971のリスクマネジメントプロセスのステップに対して、このような形でマッピングできますから、既存のリスクマネジメントプロセスに対して、JIS T 81001-5-1で規定するアクティビティを追加して実行する、つまり、既存のリスクマネジメントの手順に従って、サイバーセキュリティの特質を考慮してアクティビティを実施すると考えればよいと思います。

Slide 11



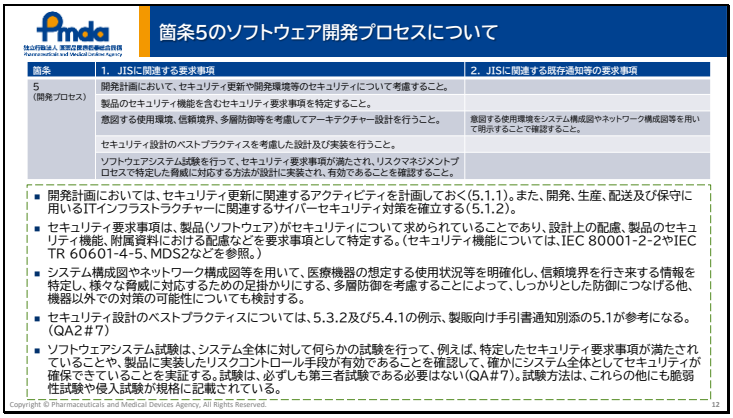
箇条7のセキュリティに関連するリスクマネジメントプロセスについては、先ほど箇条4でも示した通り、リスクマネジメントに対する一般要求事項の詳細がこのような形で箇条7に規定されています。

リスクマネジメントのプロセスは、その他のライフサイクルプロセスにもいろいろな関連があり、開発プロセスにおいては、リスクマネジメントで特定した脅威に対応する方法を設計に含め、システム試験で有効性を確認する、問題解決プロセスでは、リスクマネジメントで特定した全ての問題を対処するようにする、ということになります。

また、意図する使用、使用環境は、リスクマネジメントの出発点であると同時に、ソフトウェアアーキテクチャ設計の前提にもなるものです。

したがって、リスクマネジメントプロセスだけを行うということではなく、このように関連する各プロセスについてもしっかり実施することが必要です。

Slide 12



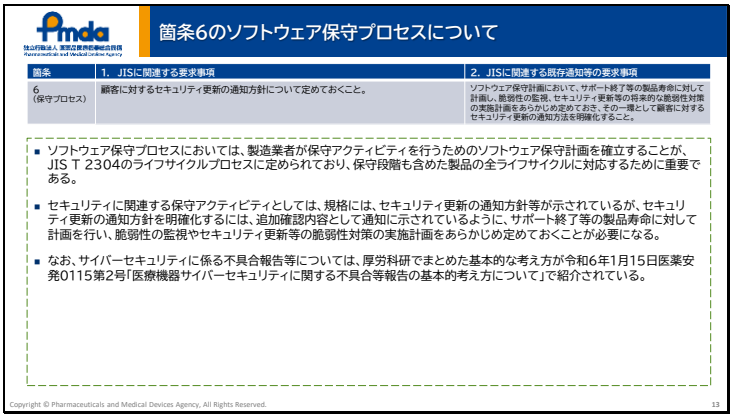
箇条５のソフトウェア開発プロセスについては、全体のエッセンスをいくつかの段階に分けて要約して記載しているという格好になります。

開発計画においては、セキュリティ更新に関連するアクティビティを計画しておくこと、また開発、生産、配送及び保守に用いるITインフラストラクチャーに関連するサイバーセキュリティ対策を確立することが規格では求められています。後者については、例えば工場で製品にソフトウェアをインストールする設備がウイルス感染していることのないように、計画的に対応していくということも考慮が必要です。

全体のアーキテクチャー設計においては、医療機器の想定する使用状況等を明確化し、信頼境界を行き来する情報と特定し、それを様々な脅威に対応するための足掛かりにする、多層防御を考慮することで、しっかりとした防御につなげる他、機器以外での対策の可能性についても検討するといったことを行います。これらをシステム構成図やネットワーク構成図を用いて説明できるようにしておくことで、規格の適合状況をはっきりと示すことができ、さらには、将来的な医療機関等からの問合せに対しても、それを活用することができます。

ソフトウェアシステム試験は、ソフトウェアシステム全体に対する試験ということですが、システム全体に対して何らかの試験を行って、例えば、上記で特定したセキュリティの要求事項が満たされていることや、実装したリスクコントロール手段が有効であることを確認して、確かにセキュリティが確保できていることを示します。試験は、必ずしも第三者試験である必要はありません。また、試験方法としてもこれらの他にも脆弱性試験や侵入試験が規格に規定されており、これらによってセキュリティの確保を示すといったことも可能です。

Slide 13

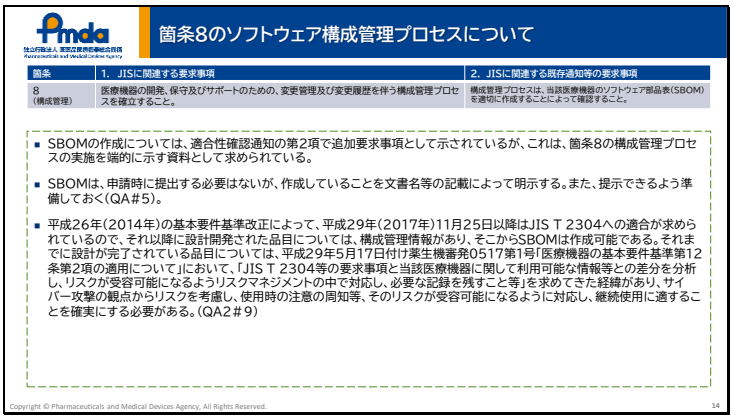


ソフトウェア保守プロセスにおいては、製造業者が保守アクティビティを行うためのソフトウェア保守計画を確立することがJIS T 2304のライフサイクルプロセスに定められており、保守段階も含めた製品の全ライフサイクルに対応するために、あらかじめ計画しておくことが重要になります。

セキュリティに関連する保守アクティビティとしては、規格には、セキュリティ更新の通知方針等が示されていますが、セキュリティ更新を将来にわたってずっと通知し続けるというのは現実的ではありません。追加確認内容として適合性確認通知に示されてるように、サポート終了等の製品寿命に対して計画を行い、脆弱性の監視やセキュリティ更新等の脆弱性対策の実施計画をあらかじめ定めておくことが必要になります。

なお、サイバーセキュリティに係る不具合報告等については、厚労科研でまとめた基本的考え方が、ここにしめした通知で紹介されているので、参考にしてください。

Slide 14



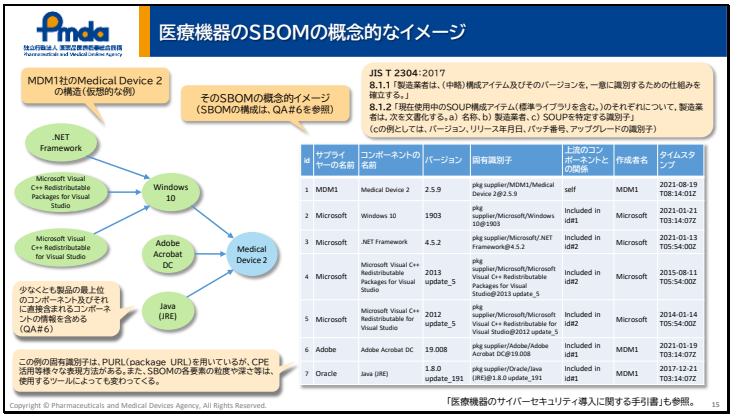
箇条８については、変更管理及び変更履歴を伴う構成管理プロセスを確立することを、規格ではシンプルに求めていますが、それによって脆弱性の影響を受けるコンポーネントのリストを明確にすることができることから、構成管理プロセスの実施を端的に示す資料として、ソフトウェア部品表（SBOM）を作成することが、サイバーセキュリティ

に関して追加要求事項として示されています。

Q&Aにあるとおり、SBOMは申請時に提出する必要はありませんが、作成していることを文書名等の明示によって明確化し、提示できるよう準備しておくことが必要です。

基本要件基準第12条第２項で求められているJIS T 2304においても構成管理プロセスが規定されていますので、平成29年11月25日以降に設計開発された品目については、構成管理情報があり、そこからSBOMは作成可能です。それまでに設計が完了している品目については、平成29年5月17日付けの通知で、差分を分析し、リスクが受容可能になるように対応して必要な記録を残すことなどが求められていることも考慮して対応を検討する必要があります。

Slide 15



SBOMについては、例えば、このような構造のソフトウェアの場合、右のような表形式の概念的なイメージとなります。

SBOMの各要素の粒度や深さ等は、使用するツールによっても変わってきますが、Q&Aでは、少なくとも最上位のコンポーネント及びそれに直接含まれるコンポーネントの情報を含めることが示されています。また、各コンポーネントについて明示する情報については、JIS T 2304の構成管理プロセスの規定にある、構成アイテム及びそのバージョンを一意に識別するための仕組み、SOUP構成アイテムのそれぞれについて文書化すべき情報を活用して、特定することが可能です。

なお、この例の固有識別子は、Package URLを用いていますが、その他CPEの活用等様々な表現方法があります。

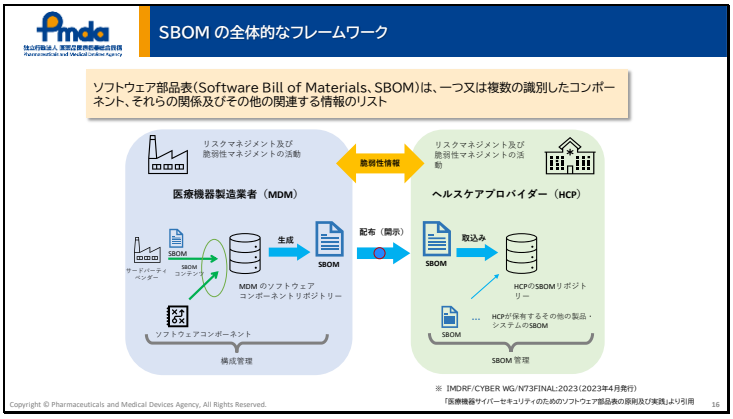
審査等においては、構成管理プロセスの確認としての位置づけでSBOMを特定するということで、特にSBOMの形式等の指定はありません。

今後、医療機関等がサイバーセキュリティ対応のためにSBOM等の資料を製造業者に求めることも想定されますが、その場合は、病院等の指定のフォーマットで、ということになるかと思います。

SBOMに限らず、サイバーセキュリティの対応においては、医療機関等の相手先と十

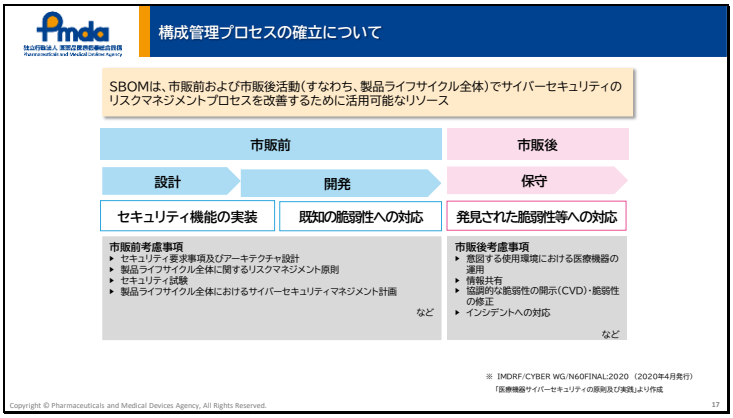
分なコミュニケーションをとって行っていくということが重要です。

Slide 16



IMDRFガイダンスでは、SBOMの全体的なフレームワークがこのような図で説明されています。医療機関と医療機器製造業者の間においては、SBOMの生成・取得を通じて、脆弱性情報等の共有が可能で、ソフトウェア透明性が高まることが期待されています。そのため、今後、製品導入にあたり顧客である医療機関から、SBOMの開示を求められるケースが増えてくることが想定されます。

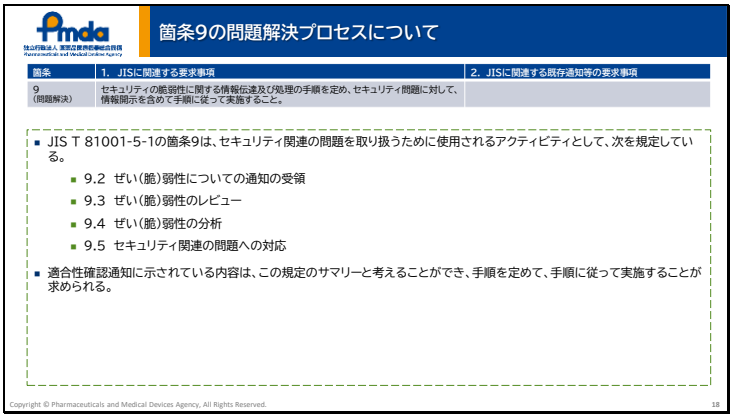
Slide 17



また、構成管理の観点からのSBOMの必要性については、この図のように整理されています。

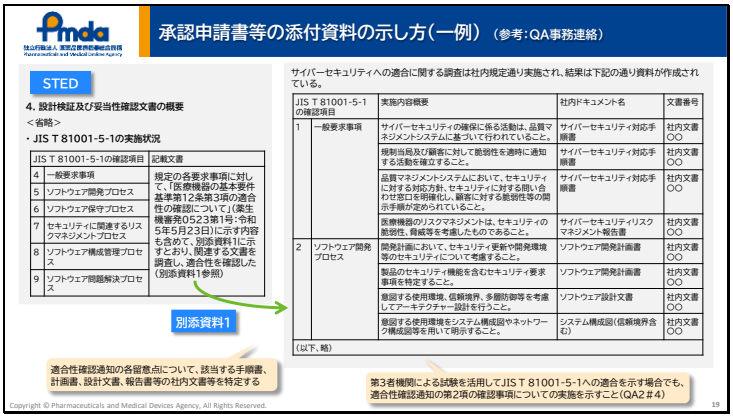
SBOMは、市販前においては、必要なセキュリティ機能の実装や、既知の脆弱性の排除のためにSBOMを作成・活用し、市販後においては脆弱性監視プロセスを補助するリソースとして、市場にあるリスクのある機器を特定するために、SBOMを活用することが重要です。

Slide 18



JIS T 81001-5-1の箇条９の問題解決プロセスでは、ここに示したアクティビティをセキュリティ問題を取り扱うために使用するとして規定していますが、適合性確認通知に示されている内容は、この箇条の規定のサマリーと考えることができ、セキュリティ問題への対処について、手順を定めて、手順に従って実施することが求められています。

Slide 19

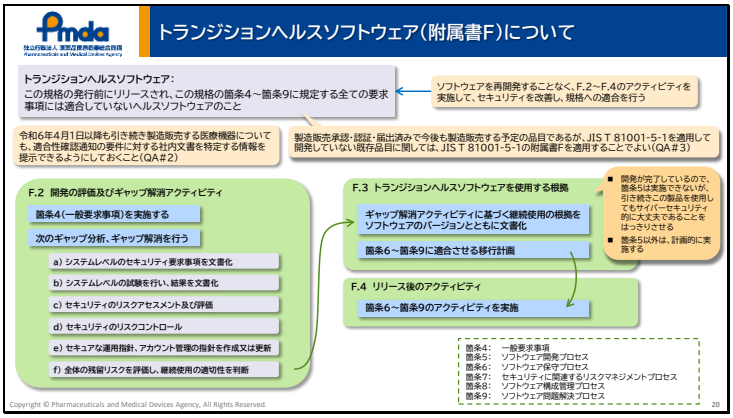


このスライドには、QA事務連絡の別添の記載事例を参考に、STED等の記載例を示しています。

STEDの４項に、JIS T 81001-5-1の実施状況として、適合性確認通知の内容を含めてJIS T 81001-5-1の適合性確認について示し、別添資料において、適合性郭に通知の各留意点について、該当する手順書、計画書、設計文書、報告書等の社内文書等を特定することになります。

第三者機関による試験を活用して、JIS T 81001-5-1への適合を示す場合でも、適合性郭に通知の第２項の確認事項についての実施を示すことが必要です。

Slide 20



最後に、附属書Fに規定されているトランジションヘルスソフトウェアについて説明します。

トランジションヘルスソフトウェアとは、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ソフトウェアのことをいいますが、開発等が終了したソフトウェアについてもセキュリティ確保について示す必要が生じることがあるため、ソフトウェアを再開発することなく、F.2～F.4のアクティビティを実施してセキュリティを改善し、規格への適合を示すという内容になります。

国内のサイバーセキュリティ対応においては、経過措置期間終了日の翌日令和６年４月１日以降も引き続き製造販売する医療機器についても、適合性確認通知の要件に対する社内文書を特定する情報を提示できるようにしておくことが必要ですが、製造販売承認、認証、届出済みで今後も製造販売をする予定の品目であるが、JIS T 81001-5-1を適用して開発していない既存品目については、このトランジションヘルスソフトウェアを適用することでもよいとされています。

F.2～F.4のアクティビティですが、まず、箇条４の一般要求事項の内容を実施し、次のような内容でギャップ分析、ギャップ解消を行います。

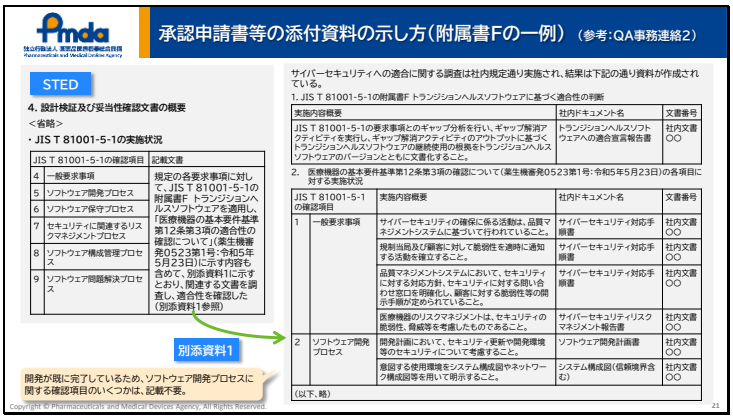
システムレベルでセキュリティ要求事項を文書化し、システムレベルの試験を行い、結果を文書化します。セキュリティのリスクアセスメント及び評価、リスクコントロールを行い、セキュリティ確保のための運用指針、アカウント管理の指針を作成又は更新します。そして、全体の残留リスクを評価し、継続使用の適切性を判断します。

こうしたギャップ解消アクティビティに基づく継続使用の根拠をバージョンごとに文書化し、箇条６の保守プロセスから箇条９の問題解決プロセスまでに適合するための移行計画を策定し、それに従って、開発プロセス以外の箇条６から９を実施していきます。

まとめますと、開発が完了しているので、箇条5については実施できないが、引き続きこのソフトウェアあるいは製品を使用してもサイバーセキュリティ的に大丈夫だということをはっきりさせる、箇条5以外のプロセスについては、計画的に実施していく、

ということが規格がトランジションソフトウェアについて求めている内容だということになります。

Slide 21



附属書Fを用いた場合の添付資料等の記載事例について示します。

先ほど示した例と異なる点は、STEDにおいては、附属書Fのトランジションヘルスソフトウェアを適用していることを明記し、別添資料においては、附属書Fに基づく適合性の判断について、ソフトウェアの継続使用の根拠及びソフトウェアのバージョン等を示す文書を特定する情報を示します。

また、トランジションヘルスソフトウェアの場合は、箇条５のソフトウェア開発プロセスについては、完全には実施できないが、それ以外の箇条４，箇条6～箇条９については計画的に実施するということですので、ソフトウェア開発プロセスに関連する確認項目のいくつかについては、記載しませんが、それ以外については同様に該当する社内文書等を特定するようにします。

Slide 21

以上、適合性確認通知や質疑応答集の内容を踏まえ、JIS T 81001-5-1の要点を解説しました。

ご清聴ありがとうございました。

以上