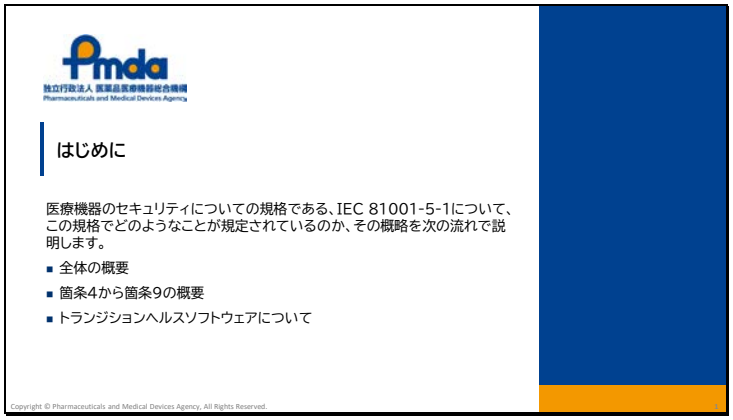
４　医療機器プログラム（SaMD）に使われる規格解説
ii. サイバーセキュリティに係る規格（IEC 81001-5-1:2021）

（令和４年度 製造販売業者向け医療機器プログラム（SaMD）の審査ポイント等に関する説明会資料）

Slide 0

医療機器のセキュリティの規格である、IEC 81001-5-1 について説明します。

Slide 1



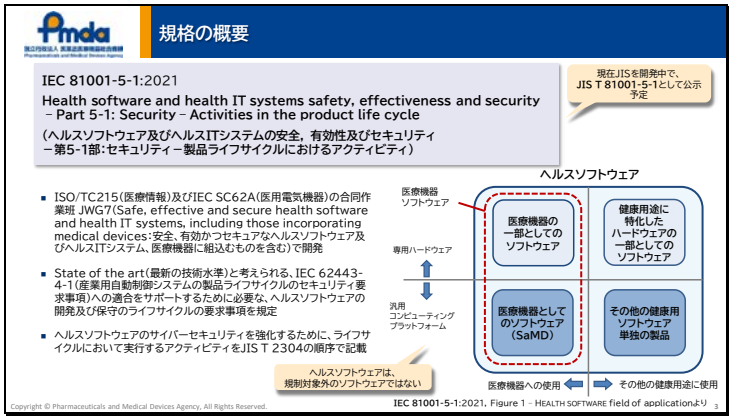
この規格でどのようなことが規定されているのか、その概略を次の流れで説明します。

まず、全体の概要について、次に箇条４から箇条９の概要について、最後に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。

Slide 2

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。

Slide 3



規格の名称は、ここに示した通り、「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ー第 5-1 部：セキュリティー製品ライフサイクルにおけるアクティビティ」です。

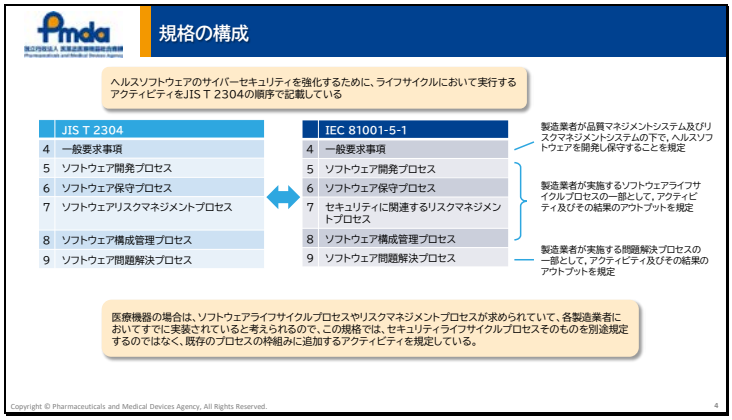
この規格は、ISO/TC215（医療情報）及び IEC SC62A（医用電気機器）という ISO、IEC の二つの委員会の合同作業班 JWG7 で開発されました。規格の名称の前半は、JWG7 が開発するヘルスソフトウェア関連の規格である IEC 81001 シリーズに共通のもので、名称の後半が、個々の規格のテーマを示しています。つまり、この規格は、第 5 の１部として、セキュリティの製品ライフサイクルにおけるアクティビティを規定しているということです。この規格は、現在 JIS を開発中で、JIS T 81001-5-1 として公示される予定になっています。

ここで、規格の対象はヘルスソフトウェアということになりますが、ヘルスソフトウェアは、この図に示す通り、規制対象である医療機器ソフトウェアを含む、健康関連のソ

フトウェア全般を指しています。規制対象外のソフトウェアのことをヘルスソフトウェアと呼ぶわけではないことに注意してください。

この規格は、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しています。その内容としては、産業用自動制御システムのセキュリティ要求事項を規定した、IEC 62443-4-1 の要求事項を参考に作られており、IEC 81001-5-1 に適合すれば、IEC 62443-4-1 に対する適合も容易に行うことができる、ということを狙ったものになっています。

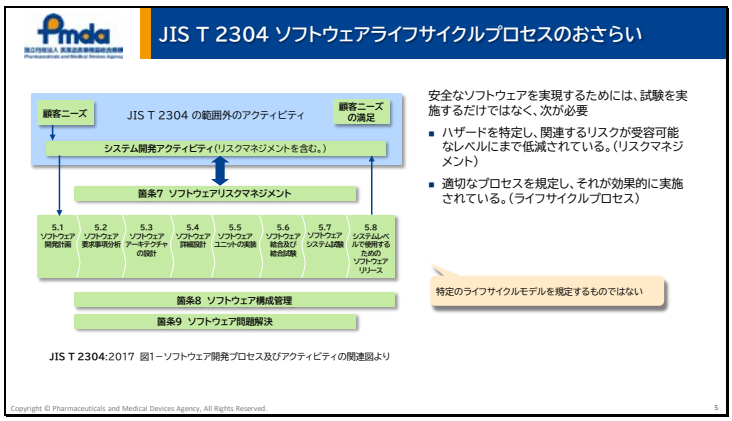
Slide 4



IEC 81001-5-1 では、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 と同じ並びで規定しています。この表で、左側が、JIS T 2304 のソフトウェアライフサイクルの規格の箇条の構成、右側が、この規格の箇条の構成を示しています。ほとんど同じ内容のものが同じ順序で並んでいます。

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は、それらがすでに実装されていると考えられるので、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、既存のソフトウェアライフサイクル等の枠組みに追加するアクティビティを規定しているというわけです。

Slide 5



ここで、JIS T 2304 のソフトウェアライフサイクルプロセスについて、少しおさらいをしたいと思います。

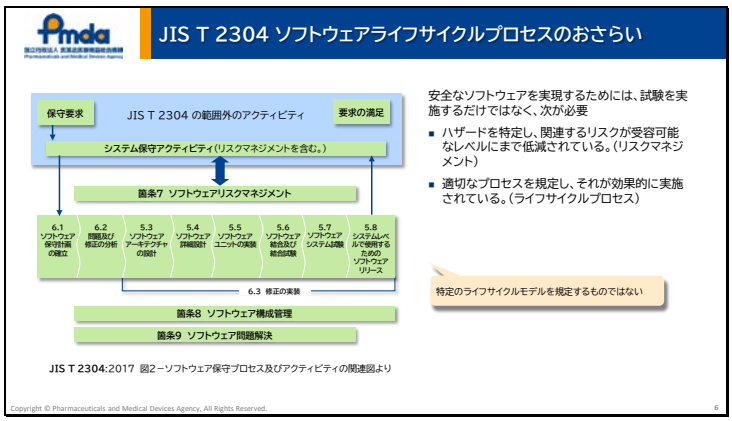
医療機器においては、ソフトウェアの役割がますます大きくなってきていており、また、ソフトウェアを使用することによって、医療機器の複雑さのレベルが増えています。ソフトウェアの試験を実施して、問題をつぶしていくことで、ある程度の品質向上は図れるものの、本当に安全なソフトウェアを実現しようとした場合は、試験の実施だけでは不十分で、次のようなことが求められます。

一つは、ハザードを特定して、関連するリスクが受容可能なレベルにまで低減されること、これはリスクマネジメントの要求です。
もう一つは、適切なプロセスを規定して、それが効果的に実施されていることで、これがライフサイクルプロセスの要求になります。

JIS T 2304 では、この観点から、開発プロセスや保守プロセスに加え、リスクマネジメントプロセス、さらにはこれらに不可欠な、構成管理プロセス、問題解決プロセスといったソフトウェアのライフサイクルプロセスを規定した規格です。

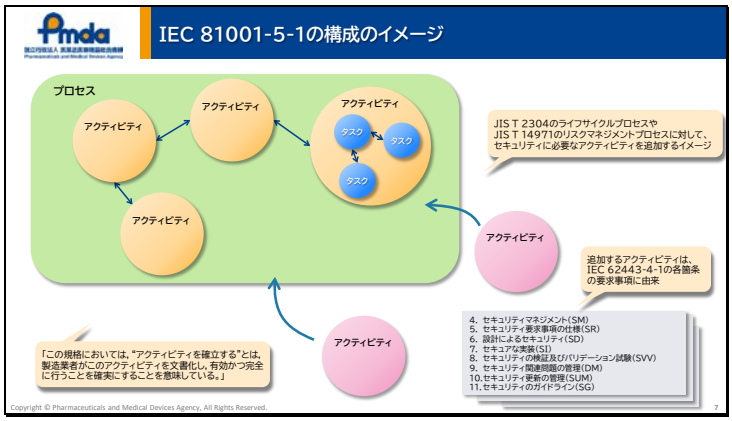
この図は、ソフトウェア開発プロセスの関連図を示したものです。ソフトウェア開発プロセスは、5.1～5.8 に規定されています。一見、ウォーターフォールモデルを想定しているように見えますが、規格自体は、特定のライフサイクルモデルを規定するものではありません。Agile に適用するためには、JIS T 2304 の規格のプロセス、アクティビティ、タスクを Agile 開発モデルに割り付けて行うということになります。

Slide 6



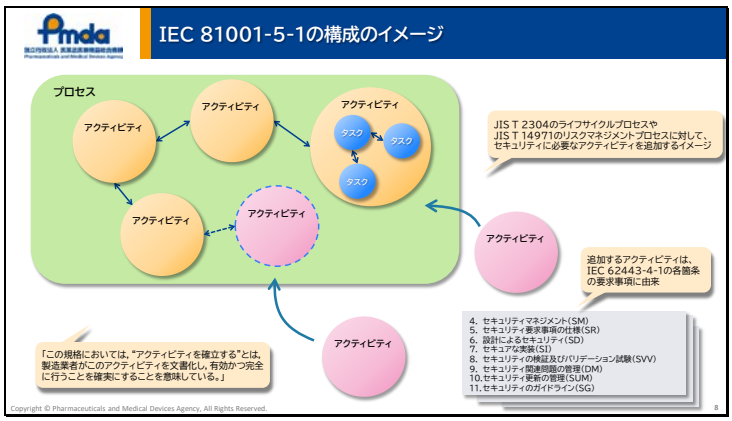
ソフトウェア保守プロセスの関連図についても、JIS T 2304 には、このように示されています。保守プロセスにおいては、保守計画を確立し、問題及び修正を分析して、修正を実装しますが、修正の実装そのものは、開発プロセスの設計や試験等の同様のアクティビティを実施していくことになります。

Slide 7



このスライドは、この規格がどんなイメージで構成されているかを示したものです。相互に関係する又は相互に作用するタスクの集まりがアクティビティであり、そのアクティビティの集まりがプロセスである、というのが JIS T 2304 に規定するタスク、アクティビティ、プロセスの階層関係ですが、IEC 81001-5-1 は、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している、というイメージになります。

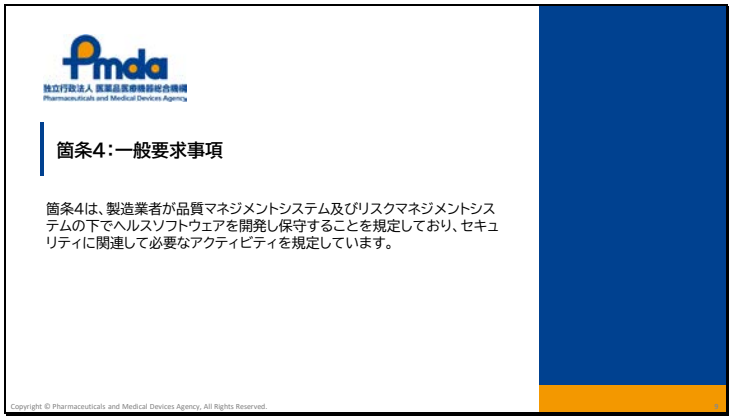
Slide 8



そして、追加するアクティビティについては、先ほど示した IEC 62443-4-1 の箇条 4 から箇条 11 に規定されている要求事項に由来しています。これによって、IEC 62443-4-1 への適合を支援しているということになります。

なお、規格の随所に、「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。」とありますので、アクティビティについては、文書化して、確実に行いなさいということになります。

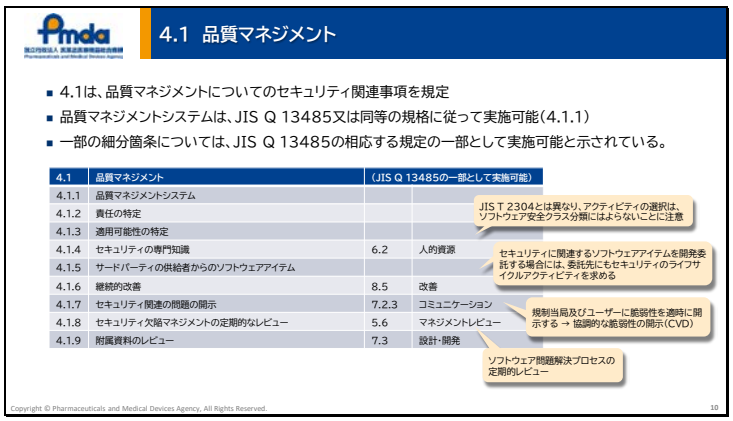
Slide 9



ここからは、箇条 4 から箇条 9 について、どういう内容が規定されているのかを説明します。

まず、箇条 4 ですが、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、それらに必要なアクティビティを規定しています。

Slide 10



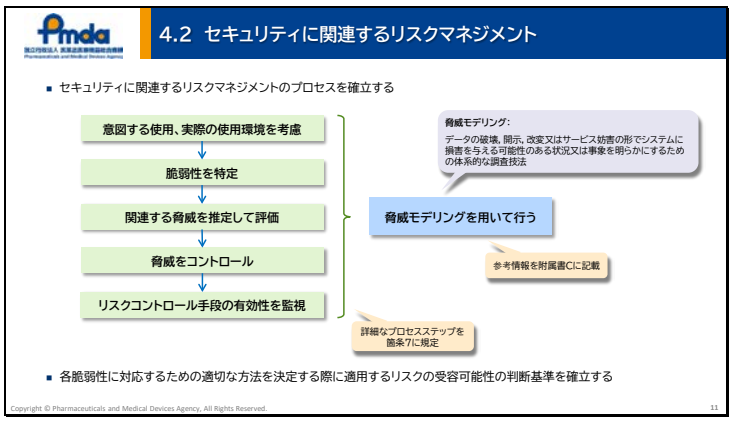
4.1 は、品質マネジメントについてのセキュリティ関連事項を規定しています。品質マネジメントシステム自体は、JIS Q 13485 又は同等の規格に従って実施可能とあり、さらに一部の細分箇条については、JIS Q 13485 の相応する規定の一部として実施可能と示されているので、実際の内容については、細分箇条の見出し等で、おおよその内容はお分かりいただけるものと思いますが、一部注意の必要な箇所について説明します。

まず、4.1.3 の適用可能性の特定に関連した話ですが、アクティビティを実施するかどうかの選択については、JIS T 2304 とは異なり、ソフトウェア安全クラス分類にはよらないことに注意が必要です。

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については、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ていくことが必要とされています。

4.1.7 は、規制当局及びユーザーに対して、脆弱性を適時に開示するという要求ですが、これは、協調的な脆弱性の開示（CVD）に関係する内容です。組織としての対応方針や手順を定めておく必要があります。

Slide 11

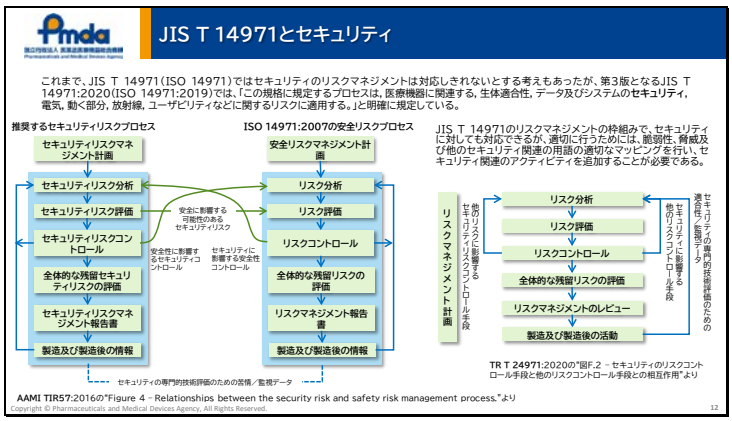


4.2 は、セキュリティに関連するリスクマネジメントプロセスを確立すること、リスクの受容可能性の判断基準を確立することを要求しています。

セキュリティに関連するリスクマネジメントプロセスは、意図する使用、実際の使用環境を考慮し、脆弱性を特定し、関連する脅威を推定して評価し、脅威をコントロールして、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が、これらを脅威モデリングを用いて行うと規定しています。詳細なプロセスステップは箇条 7 に規定されており、脅威モデリングについての参考情報は、附属書 C に記載されています。

さて、リスクマネジメントといえば、JIS T 14971 に基づいて行われていると思いますが、ここに規定している内容は、どのように考えたらよいでしょうか。

Slide 12

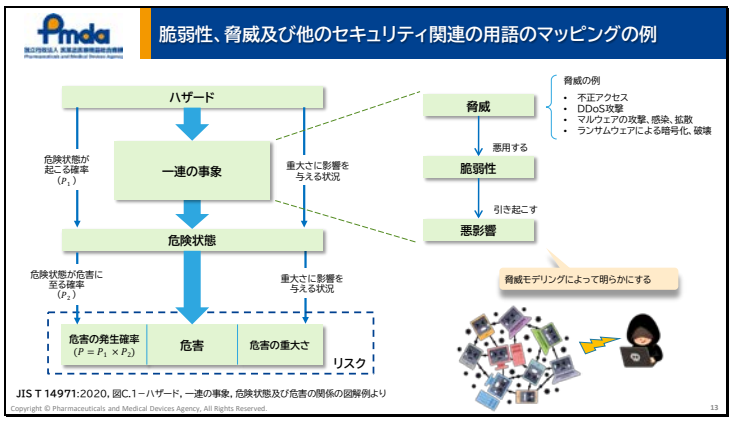


これまで、JIS T 14971 又はその原典である ISO 14971 では、セキュリティのリスクマネジメントは対応しきれないとする考え方がありました。AAMI の TIR57 という技術報告書では、この図に示しているように、セキュリティリスクのプロセスと安全リスクのプロセスの二つを走らせ、お互いのリスクコントロールが影響することを考慮する、という考え方が示されています。

一方、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。」とセキュリティも含めて明確に規定し、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ことを示しています。

IEC 81001-5-1 でも同様に、セキュリティのリスクマネジメントは、JIS T 14971 の枠組みで実施可能である、としていますが、そのためには、脆弱性や脅威といったセキュリティ用語を適切にマッピングするということも記載されています。

Slide 13

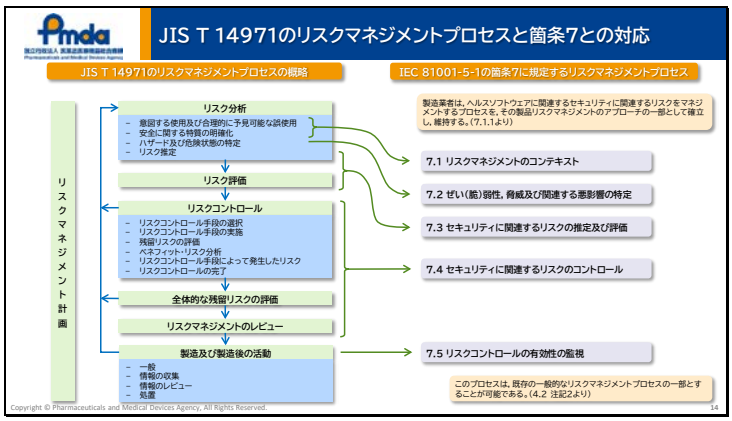


脆弱性や脅威などのセキュリティ用語のマッピングの例を示します。左側に示しているのが、JIS T 14971 に示している、ハザード、一連の事象、危険状態及び危害の関係図です。一連の事象によって、ハザードにさらされ、危険状態が起こり、危害につながるという関係によってリスクを考えていくということです。

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、先に示した AAMI TIR57 にいろいろ説明されていますが、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や破壊などがあり、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 14

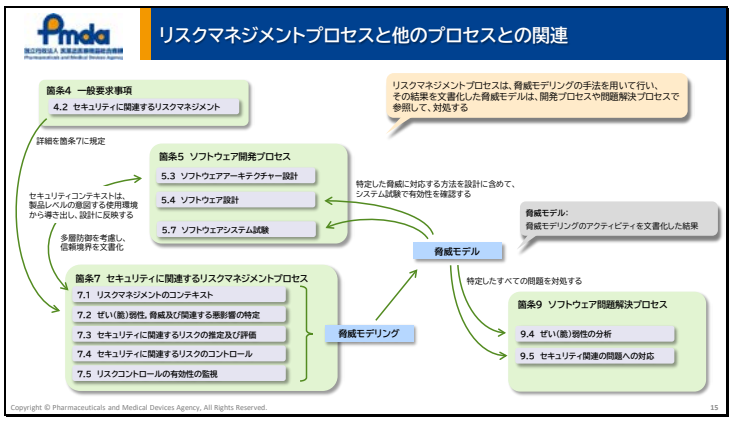


以上を考慮すると、IEC 81001-5-1 の箇条７に規定されている 7.1～7.5 のプロセスステップは、JIS T 14971 のリスクマネジメントプロセスのフローに対して、このような対応付けができることになります。

つまり、7.1 のリスクマネジメントのコンテキストは、意図する使用及び合理的に予見可能な誤使用、及び　安全に関する特質の明確化に、
7.2 の脆弱性、脅威及び関連する悪影響の特定は、ハザード及び危険状態の特定に、
7.3 のセキュリティに関連するリスクの推定及び評価は、そのまま、リスク推定及びリスク評価に、
7.4 のセキュリティに関連するリスクのコントロールについては、リスクコントロールに加えて、全体的な残留リスクの評価、リスクマネジメントのレビューに、
7.5 のリスクコントロールの有効性の監視が製造及び製造後の活動に
それぞれ対応するということになります。

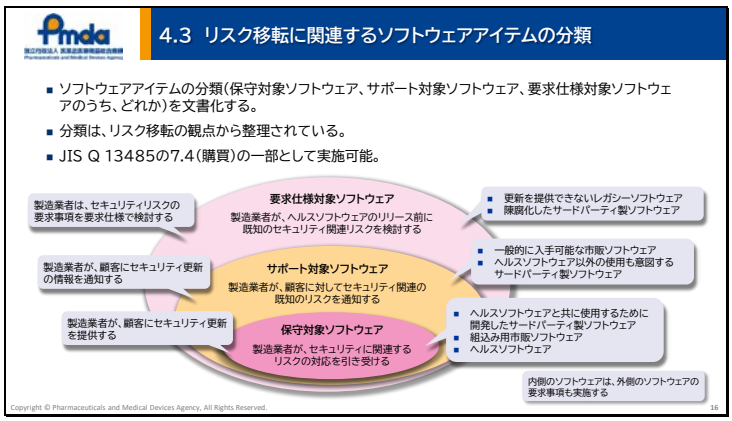
この対応関係を参考にして、この規格に規定されているセキュリティのアクティビティを、既存のリスクマネジメントプロセスに追加していくというふうに考えるとよいと思います。

Slide 15



セキュリティに関連するリスクマネジメントについては、箇条 4 に要求事項が記載され、詳細なプロセスは箇条 7 で規定されています。
箇条 7 では、7.1 から 7.5 に渡ってプロセスステップが規定されており、すでに説明した通り、これを脅威モデリングを用いて行うということになります。
脅威モデリングの結果を文書化したものが、脅威モデルであると定義されていますが、他のプロセスでは、この脅威モデルを参照して対処することが求められています。
開発プロセスにおいては、脅威モデルで特定した脅威に対応する方法を設計に含め、システム試験でその有効性を確認する、
問題解決プロセスでは、脅威モデルで特定した全ての問題を対処するようにする、ということです。
脅威や脆弱性といったセキュリティ特有のものを適切に扱うことによって、JIS T 14971 の枠組みでセキュリティのリスクマネジメントに対応できるということですので、脅威モデルの参照についても、リスクマネジメントの結果を適切に考慮するというふうに考えると、規格の理解に役立つものと思います。
なお、7.1 のリスクマネジメントのコンテキストにおいては、製品がどのような環境でどのように用いられるかといった、セキュリティ的な条件をセキュリティコンテキストとして明確にすることを求めており、これは、製品の意図する使用から導き出して、設計に反映していくことが必要です。また、アーキテクチャー設計においては、多層防御を考慮し、信頼境界を文書化しますが、こうしたことが脅威モデリングの出発点としても要求されますので、この点からもリスクマネジメントと開発プロセスのかかわりが出てきます。

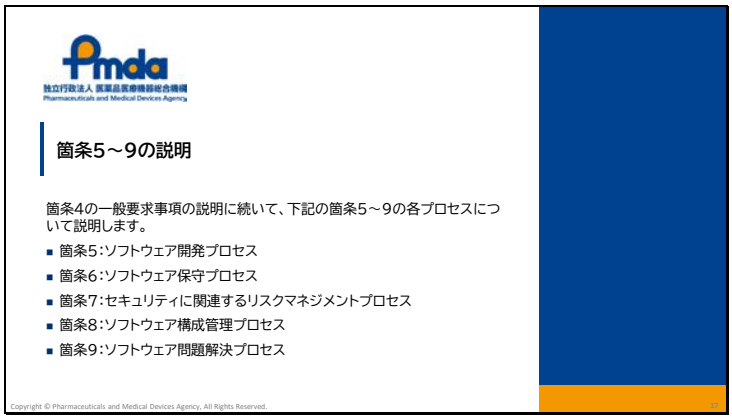
Slide 16



箇条４の一般要求事項の最後のパートは、ソフトウェアアイテムをリスク移転の観点から分類しなさいという要求事項です。

ヘルスソフトウェアの意図する使用を実現するために必要なソフトウェアアイテムについては、全て、市販前の段階でセキュリティリスクを特定して対応しておく必要があるが、そのすべてが市販後にセキュリティ更新を提供したり、更新情報をユーザーに知らせたりするわけではない、ということから、要求仕様対象ソフトウェア、サポート対象ソフトウェア、保守対象ソフトウェアに分類して整理する、ということが規定されています。

Slide 17



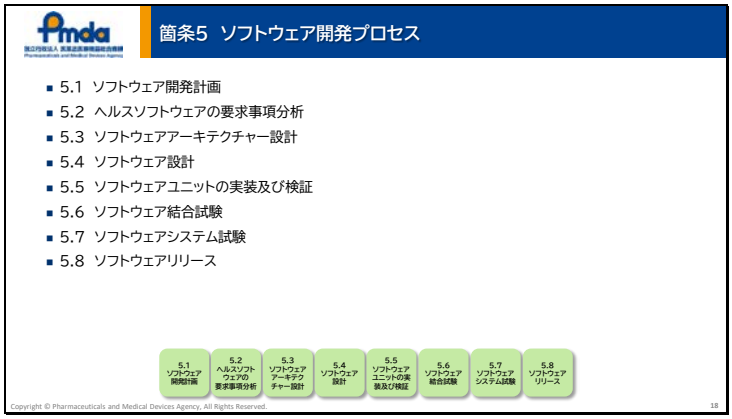
箇条 4 の一般要求事項の説明に続いて、ここに示した箇条 5～9 の各プロセスについて説明します。

IEC 81001-5-1 についても、安全で有効な医療機器のための枠組みを示したプロセス規格であると考えられますので、プロセスの枠組みを規定する、つまりプロセスで行うべき要求事項を淡々と規定しており、規格に適合するためには、これらの要求事項を

実施していくということになります。

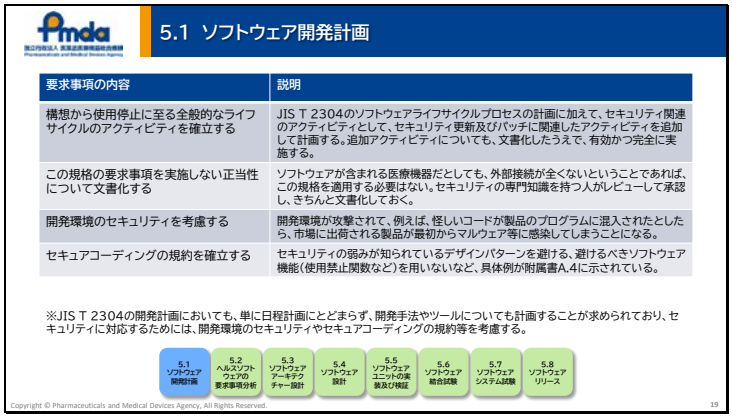
今回の説明では、資料のうち、ポイントだけを説明します。

Slide 18



まず、箇条５のソフトウェア開発プロセスです。5.1～5.8 について、順に説明します。

Slide 19

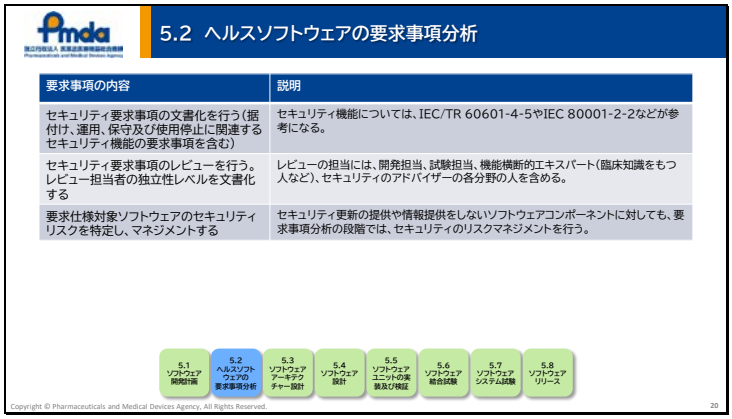


5.1 のソフトウェア開発計画においては、JIS T 2304 におけるライフサイクルプロセスの計画に加えて、セキュリティ関連として、セキュリティ更新及びセキュリティパッチに関連したアクティビティを追加して計画します。

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ありません。しかし、ネットワーク接続がなくても、USB メモリーが接続可能で、何らかのデータやり取りが可能になっている等の場合は、セキュリティを検討する必要があります。適用しない正当性は、きちんとレビューし文書化しておく必要があります。

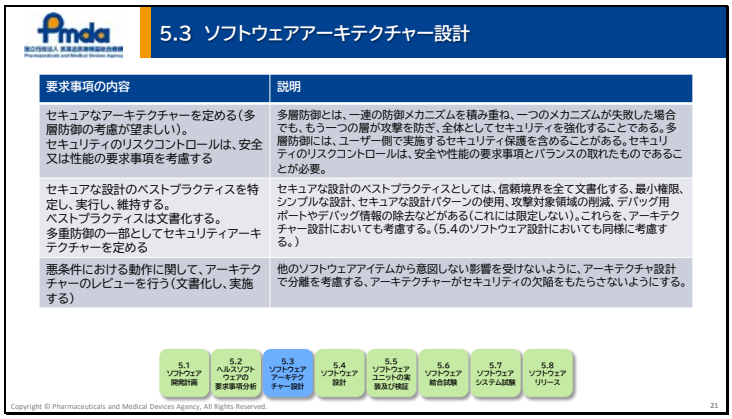
また、JIS T 2304 の開発計画の規定も、単に日程計画だけにとどまらず、開発手法やツールに関しても計画を求めていますので、この規格においても、開発環境やコーディング規約等について開発計画の中で規定されています。

Slide 20



要求事項分析では、セキュリティの要求事項を文書化し、レビューを行います。要求事項には、据付、運用、保守及び使用停止といった、製品の全ライフサイクルに関連するセキュリティ機能についても含めます。この規格は、開発や保守といったライフサイクルにおいて何をするかということを規定していますが、セキュリティ機能、すなわち、セキュリティ対応のために製品でどんなことを行うのか、といった点については、IEC/TR 60601-4-5 や IEC 80001-2-2 などの規定が参考になりますので、それらを活用して明確化します。

Slide 21

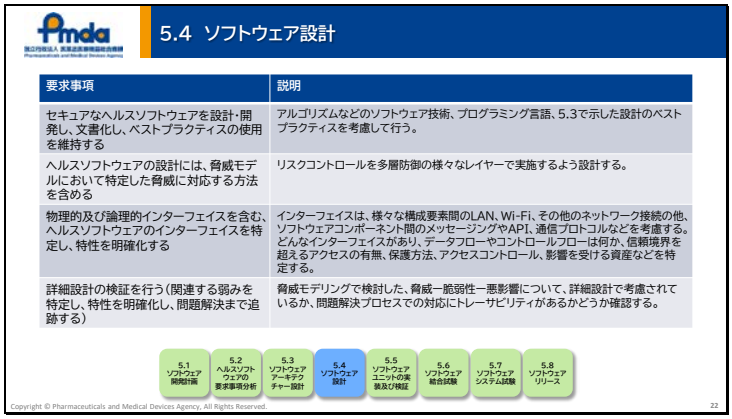


セキュリティのアーキテクチャー設計においては、多層防御を考慮することが望ましいと規定されています。多層防御とは、防御メカニズムを何層にも積み重ねることによって、仮に一つのメカニズムが破られても、別の層が攻撃を防いで全体的にセキュリティを保つようにすることです。これには、ユーザー側で実施するセキュリティ保護を含め

ることがあります。こうしたアーキテクチャーを設計するためには、脅威モデリング、つまりセキュリティのリスクマネジメントの最初の段階として、ネットワーク構成図を作成して、信頼境界を文書化するなどによって、セキュリティコンテキストを明確化する必要があります。

またセキュリティに対するリスクコントロール手段は、安全や性能とのバランスが取れたものであることが必要です。例えば、一刻を争う救急の現場で使用する機器においては、ユーザー認証が非常に煩雑なものであってはなりませんし、アンチウィルスソフトウェアの処理が非常に重くて、医療機器の本来の処理に影響を及ぼすようなことがあってはなりません。こうしたこともアーキテクチャーとして配慮します。

Slide 22

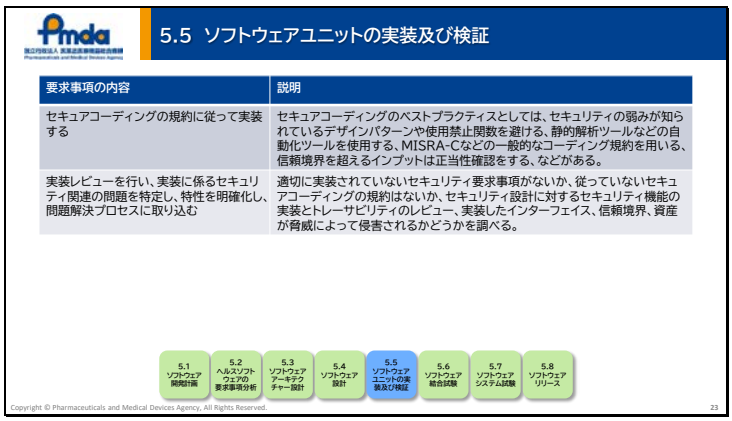


セキュアな設計を行うためには、アルゴリズムなどのソフトウェア技術やプログラミング言語のほかに、最小権限の原則、シンプルな設計、セキュアな設計パターンの使用、攻撃対象領域の削減といった、（5.3 に記載されている）様々なベストプラクティスを考慮して行います。

インターフェイスの明確化は、ネットワーク接続の他、コンポーネント間のインターフェイスも考慮して、データフロー、コントロールフローを検討して行います。

脅威モデリングで検討した、脅威が脆弱性を悪用して悪影響を及ぼす一連の事象に対しては、詳細設計においてリスクコントロール手段を組み込んで、トレーサビリティが取れるようにしておきます。

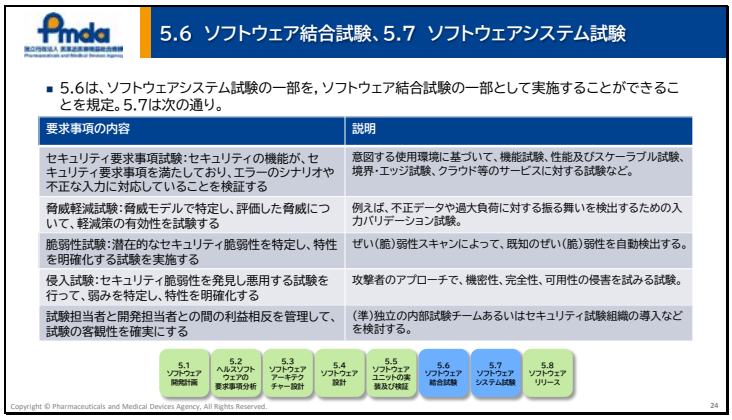
Slide 23



ソフトウェアの実装においても、セキュリティの弱みが知られているような設計パターンや使用禁止関数を避ける、静的解析ツールを用いる、MISRA-C など一般的なコーディング規約を採用する、信頼境界を超えるインプットは正当性チェックをするなどといった、ベストプラクティスを使って行います。

実装のレビューにおいては、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を確認する、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を検証する、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などを行います。

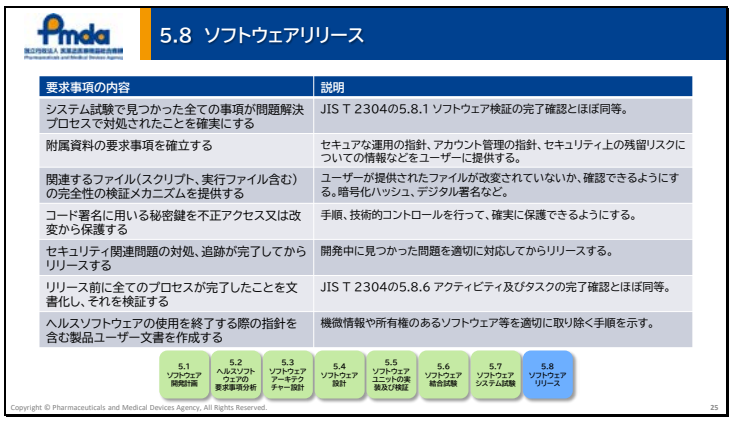
Slide 24



セキュリティに関連するソフトウェアシステム試験としては、５．７にセキュリティ要求事項試験、脅威軽減試験、脆弱性試験、侵入試験を規定して、説明されています。

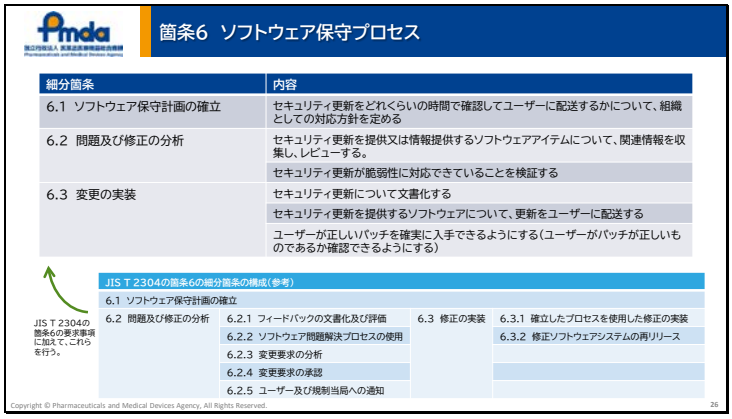
また、試験担当者と開発担当者との利益相反を管理することで、試験の客観性が担保できるということから、独立した内部試験チームやセキュリティ試験組織の導入について検討するとよいとも記載されています。

Slide 25



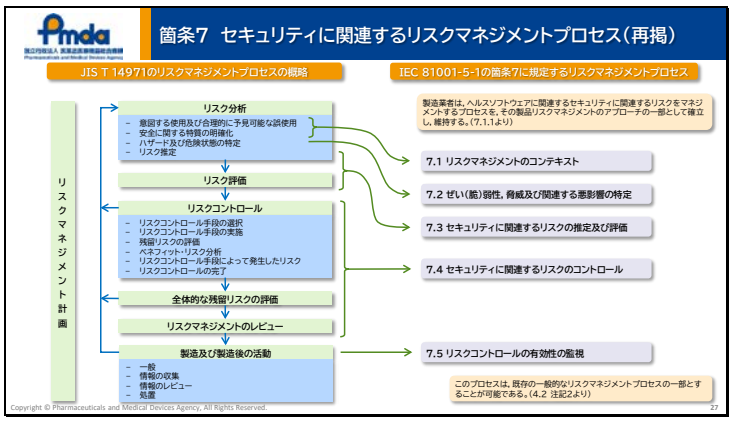
5.8 のソフトウェアリリースでは、JIS T 2304 の要求事項と類似の内容に加えて、セキュアな運用の指針、アカウント管理の指針、機微情報の取り扱いなどの使用終了の際の指針といった内容をユーザーに提供すること、ファイルの完全性や秘密鍵の保護を行うことなどが規定されています。

Slide 26



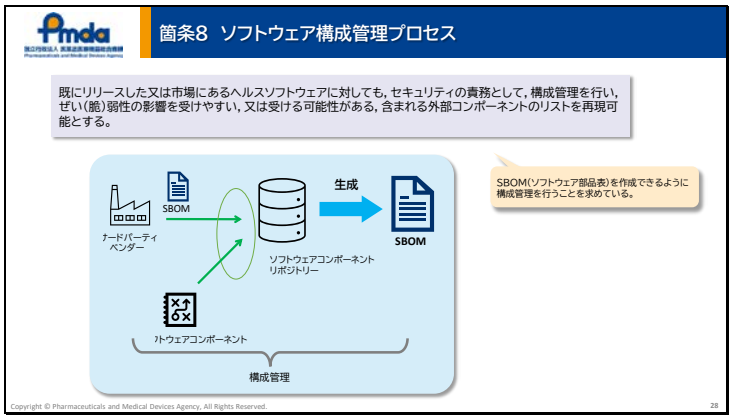
ソフトウェア保守プロセスは、基本的に JIS T 2304 の箇条 6 に従って行いますが、IEC 81001-5-1 では、保守全体において、セキュリティ更新やセキュリティパッチをどのように扱うか、という点を追加で規定しています。

Slide 27



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、すでに説明した通り、JIS T 14971 のリスクマネジメントプロセスとの対応付けを行って、製品リスクマネジメントの一部として行うことができる、となっています。

Slide 28



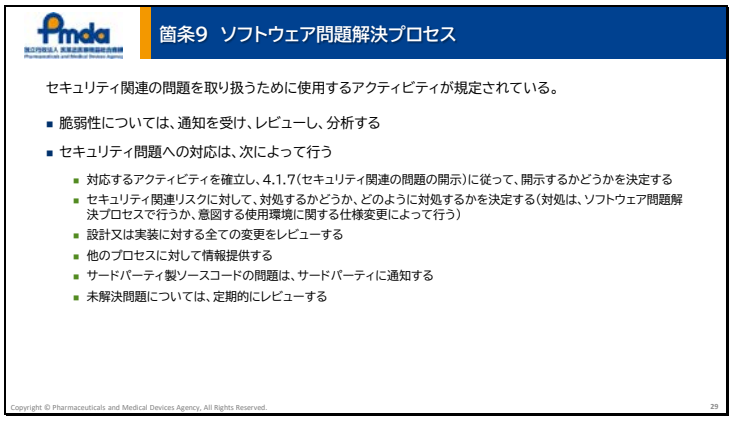
ソフトウェア構成管理プロセスについては、JIS T 2304 に規定する通り、一般的な構成管理プロセスを確立するということになりますが、セキュリティに特化した要求事項として、脆弱性が影響する可能性がある外部コンポーネントについては、すでにリリースした、あるいは、市場にあるヘルスソフトウェアに対しても、そのコンポーネントのリストを作れるようにしておく、という要求があります。

これは、いわゆる SBOM（ソフトウェア部品表）が作成できるように構成管理を行ってくださいということになります。

ソフトウェアを構成するいろいろなコンポーネント、つまり、サードパーティベンダーからのコンポーネントや自製のコンポーネントについては、構成管理プロセスの中でいろいろなデータが集められていることになると思います。

SBOM は、そうしたデータを活用して作成するということになります。

Slide 29

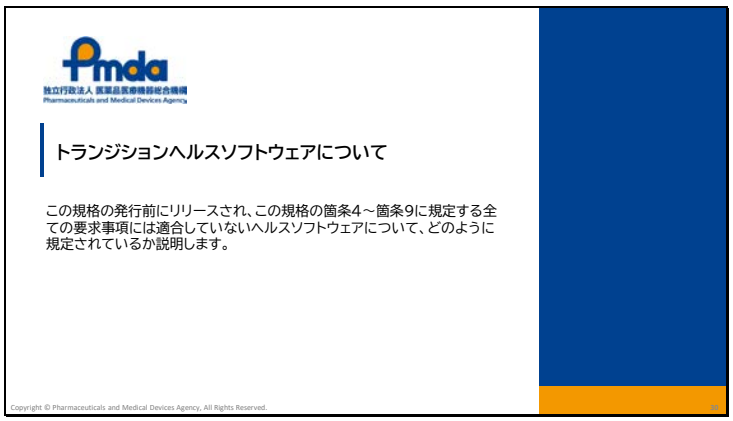


箇条 9 のソフトウェア問題解決プロセスにおいては、セキュリティ関連の問題を取り扱うためのアクティビティが規定されています。

まず、脆弱性への対応としては、脆弱性についての通知を受け、レビューし、分析することが規定されています。

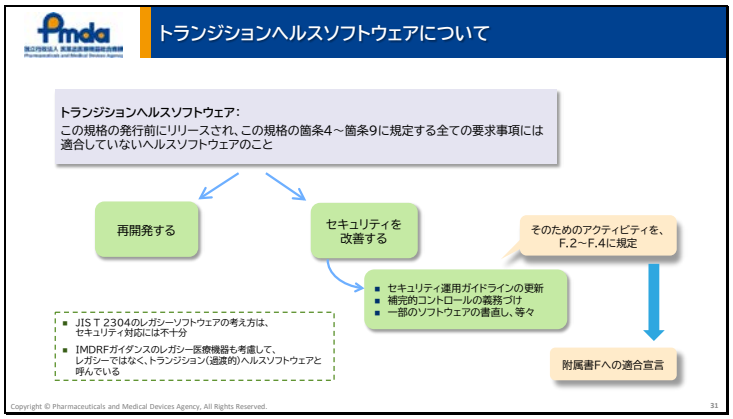
また、セキュリティ問題への対応については、対処するかどうか、どのように対処するか、どのようにそれを開示するかを決めて行います。
対処する場合は、JIS T 2304 の問題解決プロセスを通じて行うか、あるいは意図する使用環境に関する仕様変更などによって行います。
対応のために設計や実装の変更を行った場合は、安全、有効性及びセキュリティへの影響についてレビューを行います。他のプロセスに対して問題報告の形で情報提供したり、サードパーティ製ソースコードの問題については、サードパーティに通知します。未解決問題は、少なくとも製品のリリースごとに定期的にレビューすることが必要です。

Slide 30



最後に、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、つまりトランジション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。

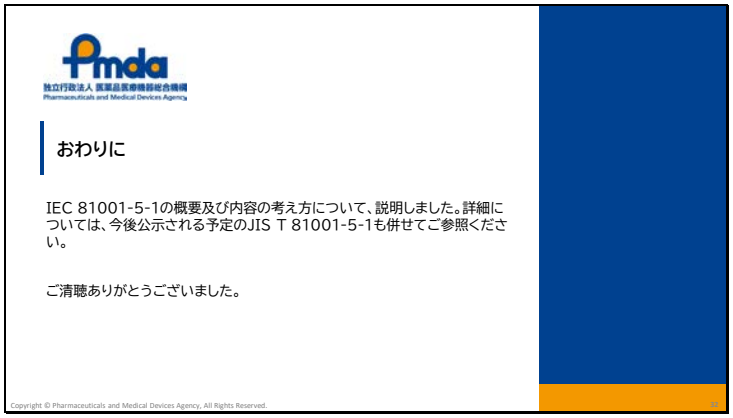
Slide 31



この規格は、プロセス規格であり、開発プロセス等を規定しているので、この規格の発行前にリリースしたソフトウェアについては、この規格の要求事項の全てに対して適合していないケースが考えられます。
そのようなソフトウェアを、この規格ではトランジションヘルスソフトウェアと呼び、そうした場合に、この規格への適合をどう考えたらよいかが、附属書 F に規定されています。
JIS T 2304 にも同様の考えがあり、レガシーソフトウェアとして、そのための適合方法が規定されていますが、セキュリティ対応においては、JIS T 2304 のレガシーソフトウェアでは不十分であること、セキュリティ関係では、IMDRF のガイダンスでレガシー医療機器という考え方が示されていることから、レガシーソフトウェアではなく、トランジションヘルスソフトウェアと呼んでいます。
トランジションヘルスソフトウェア、つまり、この規格の発行前にリリースされ、この

規格の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は、二つのやり方があり、
一つは、再開発する、
もう一つが、セキュリティを改善する、つまり、セキュリティ運用ガイドラインを更新する、補完的コントロールを義務づける、一部のソフトウェアを書き直すなどを行う、ということになります。
セキュリティの改善方法について、附属書の F.2～F.4 に規定されていますが、これらによってセキュリティを改善した場合は、この規格に対する完全な適合とはならず、附属書 F による適合となります。
なお、JIS T 2304 のレガシーソフトウェアでは不十分であるという理由は、フィードバックの評価やリスクコントロール手段の継続的有効性を確認すること等で、ソフトウェアの変更なしで適合としてしまうと、変化の速いサイバーセキュリティに対して対応しきれないので、何らかの形で改善を求めるというのが、トランジションヘルスソフトウェアの考え方ということになります。

Slide 32



以上、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。

以上