サイバーセキュリティ手順書

＊ご留意いただきたい事項＊

青字で記載されている文章はインストラクションです。文書発効時には削除ください。

黄色マーカーの付されている箇所は、貴社の事情に合わせご自由にご変更ください。

なお、文書中には当社の関連するひな形を参照させている箇所がございます。

当該箇所は貴社の適切な文書に置き換えてください。当社ひな形のご用意もございますのでお気軽にお問い合わせください。

役　割	役職／所属部門	氏　名	日付
作成者			年　月　日
確認者			年　月　日
承認者			年　月　日

※下記「〇〇株式会社」の変更は、Word の「ファイル>情報>プロパティ>会社」の会社名の欄をご変更後、「〇〇株式会社」部分を右クリックし、「フィールド更新」を選択してください。

〇〇株式会社

改訂履歴

Ver.	発効日 制定／改訂内容（変更理由、変更内容、影響を与える関連文書） 作成者/審査者/承認者			
バージョン 1.0	発 効 日	20XX 年 00 月 00 日		
	理　　由	初版制定（※次版以降、改訂の理由をここに記載してください）		
	内　　容	初版制定（※次版以降、改訂の内容をここに記載してください）		
	改訂の影響を受ける文書	N/A （※次版以降、本文書の改訂により影響を受ける文書をここに記載してください）		
	役　　割	作成者	審査者	承認者
	所属部門	XXX	XXX	XXX
	役　　職	XXX	XXX	XXX
	氏　　名	XXX	XXX	XXX

目 次

【留意事項】

IEC 81001-5-1（JIS T 81001-5-1）「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」のみでは、単独の手順書を作成することは出来ません。

IEC 81001-5-1 は、IEC 62304（JIS T 2304）「医療機器ソフトウェアーソフトウェアライフサイクルプロセス」に則った手順書に IEC 81001-5-1 の要求事項を加えることを要求しています。

従い、本手順書は IEC 62304 および IEC 81001-5-1 の両方を遵守することが出来ます。

IEC 81001-5-1 は IEC 62304 の対応する章番号を合わせてあります。しかしながら、細箇条番号までは一致しておりません。そのため、当社のノウハウにより、適切な位置に IEC 81001-5-1 の要求事項を挿入しております。また一部、順序を入れ替えております。

本手順書では、IEC 81001-5-1 の要求事項は赤字で示しています。また出典元の箇条番号およびタイトルを記載してあります。

箇条番号のみ記載しているものは、IEC 62304 の番号を表します。

IEC 81001-5-1 と IEC 62304 はプロセス規格です。実施すべきプロセスを定義しているのみで、具体的な方法論等（ウォータフォールモデルまたはアジャイル開発など）は示していません。プロセスはアクティビティで構成され、アクティビティはタスクで構成されます。

IEC 81001-5-1、IEC 62304 共に、要求されているアクティビティを中心に、手順書等で確立すること要求しています。本手順書（ひな形）は、要求されているアクティビティを手順化したものです。

IEC 62304 は、ソフトウェア安全性クラス A、B、C に応じて、必須アクティビティを定義しています。しかしながら、IEC 81001-5-1 の要求事項はソフトウェア安全性クラス A、B、C に依存しません（すべて遵守が必須です）。

IEC 81001-5-1 はヘルスソフトウェア（医療機器ソフトウェア＋非医療機器ソフトウェア）を対象としていますが、本手順書は医療機器ソフトウェアのみを対象としています。

本手順書に記載されている成果物は本手順書には付属しません。必要に応じて別途お買い求めください。

SaMD（単体プログラム）の場合（つまりハードを持たない医療機器ソフトウェア、エンベデッドソフトウェアではない場合）は、ソフトウェアシステム要求事項とシステム要求事項とに差異がないため、どちらかを削除する必要があります。

また同様に SaMD（単体プログラム）の場合、結合試験とシステム試験は統合することが可能です。

SaMD（単体プログラム）の場合、青字で示していますので、適切に修正してください。

役割名（開発担当者、検証担当者等）は貴社の組織に合わせて修正してください。

IEC 81001-5-1 と IEC 62304 は非常に難解です。まずは当社の発信するセミナー（YouTube、有償セミナー）などを視聴頂くことを強く推奨いたします。

【Rev 2.0 への変更点】

「IEC 81001-5-1 対応版」と「医療機器のサイバーセキュリティ導入に関する手引書（第 2 版）対応版」を統合しました。

その結果、下記の変更を行いました。

1. **適用範囲の更新**
2. **章タイトルの更新**
   - **7. ソフトウェア開発およびサイバーセキュリティ確保手順（市販前）（5.）**
   - **8. ソフトウェア保守プロセスおよびサイバーセキュリティ確保手順（市販後）（6.）**
3. **下記の章を追加**
   - **7.2 リスクアセスメント**
   - **7.5 リスクコントロール策の検討**
   - **7.10.3 セキュリティ試験計画書**
   - **7.10.4 セキュリティ試験**
   - **7.12.10 サイバーセキュリティマネジメント計画書の作成**
   - **7.12.11 顧客向け文書の作成**
   - **7.12.12 規制当局への申請**

1. 目的

本文書の目的は、〇〇株式会社（以下、当社）において、医療機器ソフトウェアにおけるサイバーセキュリティ対応手順を明確にすることである。

2. 適用範囲

2.1 適用範囲

本文書は、無線または有線により、メディア媒体を含む他の機器、ネットワーク等との接続が可能なプログラムを用いた医療機器（ソフトウェア単独で医療機器となる医療機器プログラム（Software as a Medical Device：SaMD）を含む）およびプログラムを用いた附属品（医療機器の薬事承認等範囲内の構成品）等に関するサイバーセキュリティを対象とする。

また、医療機器の保守を目的として構成されるプログラムを用いた周辺機器についても契約等に応じて対象とする。

ただし、下記のような患者またはユーザーへの危害が発生する可能性のあるサイバーセキュリティリスクに限定する。

1) 製品の性能に影響を与える
2) 臨床活動に影響を与える
3) 誤った診断、治療または予防に繋がる

2.2 非適用範囲

本文書は下記には適用しない。

1) 情報セキュリティに係るリスク
2) 企業活動に関するサイバーセキュリティ対応
3) 当社の企業活動に関するサイバーセキュリティのための CSIRT（Computer Security Incident Response Team）活動

SaMD の場合、ソフトウェアシステム要求事項とシステム要求事項とに差異がないため、IEC 62304 の下記事項については、非適用とする。

1) IEC 62304 5.1.3 a) ソフトウェア開発計画におけるシステム設計およびシステム開発の引用
2) IEC 62304 5.2.1 システム要求事項からのソフトウェア要求事項の定義および文書化

本手順書は、レガシーソフトウェアを取り扱わない。

1) 4.4 レガシーソフトウェア

3. 用語の定義

用　語	定　義
附属資料（accompanying documentation）	ヘルスソフトウェア若しくはヘルス IT システムまたは附属品に使用することを意図する、責任部門または操作者のための情報を記載した資料
SaMD	Software as a Medical Device の略 デジタルヘルスに含まれる概念であり、医療目的で用いられる単体のソフトウェア（単体プログラム）のこと。
プロセス（PROCESSES）	入力を出力に変換する、相互関連または相互作用アクティビティのセット インプットを使用して意図する結果（成果）を生み出す、相互に関連するまたは相互に作用する一連のアクティビティ
アクティビティ（ACTIVITIES）	相互関連または相互作用タスクのセット 一組以上の相互関係または相互作用のあるタスク （出典：JIS T 2304:2017 の 3.1）
タスク（TASKS）	プロセスの構成要素
リスクマネジメントファイル（RISKMANAGEMENT FILE）	必ずしも連続的でないが、リスク管理プロセスによって生成される記録または他の文書のセット
ソフトウェアシステム	特定の機能または特定の機能群を達成するために組む、複数のソフトウェアアイテムを結合した集合体
ソフトウェアアイテム（SOFTWARE ITEM）	識別可能なコンピュータープログラムの一部、すなわち、ソースコード、オブジェクトコード、制御コード、制御データまたはこれらアイテムの集合体。 3 つの用語がソフトウェアの分解を示す。 トップレベルがソフトウェアシステムである。 それ以上分解されない最低レベルが、ソフトウェアユニットである。 トップおよびボトムレベルを含む、分解の全レベルは、ソフトウェアアイテムと呼ばれる。 ソフトウェアシステムは、1 またはそれ以上のソフトウェアアイテムで構成され、各ソフトウェアアイテムは、1 またはそれ以上のソフトウェアユニットまたは分解可能なソフトウェアアイテムで構成される。 ソフトウェアアイテムおよびソフトウェアユニットの定義および程度を供給する責任は、製造者にゆだねられている。 コンピュータープログラムの識別可能な部分（例えば、ソースコード、オブジェクトコード、制御コード、制御データまたはこれらのアイテムの集まり） （出典：JIS T 2304:2017 の 3.25 を変更し、注記を削除）
ソフトウェアユニット	他のアイテムに分割できないソフトウェアアイテム。
ソフトウェア保守（software maintenance）	リリースした後に行う、ヘルスソフトウェアに対する変更 （出典：JIS T 82304-1:2018 の 3.21 を変更し、“ヘルスソフトウェア製品”を“ヘルスソフトウェア”に置換え、保守の目的を注釈 1 に記載し、注記を注釈 2 とした。）
保守対象ソフトウェア（maintained software）	製造業者が、セキュリティに関連するリスクへの対応を引き受けるソフトウェアアイテム
サポート対象ソフトウェア（supported software）	製造業者が、顧客に対しセキュリティ関連の既知のリスクを通知するソフトウェアアイテム
SOUP（Software Of Unknown Provenance）	開発過程が不明なソフトウェア。 すでに開発されていて一般に利用できるが、医療機器に組み込むことを目的に開発したものではないソフトウェアアイテムまたは以前開発されたソフトウェアア

4. 役割と責任

役　割	責　任
設計開発責任者	・ソフトウェア開発プロセスおよびソフトウェア保守プロセスにおける期間、コストに関する責任を負う ・ソフトウェア開発プロセスにおけるすべての成果物の作成の責任を負う ・ソフトウェア開発プロセスおよびソフトウェア保守プロセスにおける成果物に関して、製品開発を行う上での妥当性の観点からレビュし、確認する責任を負う ・変更の承認権を持ち、変更要求の影響による制御レベルに応じて選定される
設計開発担当者	・ソフトウェア開発プロセスにおける全ての成果物の作成を担当する ・ソフトウェア開発プロセスおよびソフトウェア保守プロセスにおける成果物に関して、製品開発を行う上での妥当性の観点でのレビュを担当する ・構成管理を行う
検証責任者	・ソフトウェア検証計画書およびシステムテスト関連文書の作成の責任を負う
検証担当者	・ソフトウェア検証計画書およびシステムテスト関連文書の作成を担当する ・システムテスト計画書に基づきセキュリティ要求事項試験を実施する ・システムテスト計画書に基づき脅威軽減試験を実施する ・システムテスト計画書に基づき脆弱性試験を実施する ・システムテスト計画書に基づき侵入試験を実施する
品質保証責任者	・ソフトウェアの品質に関する責任を負う
品質保証担当者	・ソフトウェアの品質保証の観点で、成果物のレビュを担当する
保守チーム	・ソフトウェア保守プロセスのタスクを担当する
保守チーム責任者	・ソフトウェア保守プロセスにおける責任を負う

5. 設計開発ステージとソフトウェア開発プロセスの対応（5.1.3 b)）

設計開発ステージ	ソフトウェア開発プロセス	
ステージ	プロセス	セクション
設計開発計画	ソフトウェア開発計画	7.1
設計インプット	ソフトウェア要求分析	7.3
設計アウトプット/設計検証	ソフトウェアアーキテクチャ設計	7.5
	ソフトウェア詳細設計	7.7
	ソフトウェアユニットの実装	7.8.2
	ソフトウェアユニットの検証	7.8.3
	ソフトウェア結合および結合試験	7.9
	ソフトウェアシステム試験（SaMD の場合ソフトウェアシステム試験を統合する）	7.10
	リリース	7.12
設計の妥当性確認	ソフトウェア結合試験（SaMD の場合ソフトウェアシステム試験を統合する）	7.10

6. 成果物

当社では、製品向けソフトウェアの開発に際して、以下の成果物を作成する。

項	プロセス	成果物	安全性クラス	作成者	レビュ	承認者
7.1	ソフトウェア開発計画（5.1）	ソフトウェア開発計画書	ABC	設計開発担当者	品質保証担当者	設計開発責任者
		ソフトウェア検証計画書	ABC	検証担当者	品質保証担当者	検証責任者
		リスクマネジメント計画書	ABC	設計開発担当者	品質保証担当者	設計開発責任者
		ソフトウェア文書管理計画書	ABC	設計開発担当者	品質保証担当者	設計開発責任者
		ソフトウェア構成管理計画書	ABC	設計開発担当者	品質保証担当者	設計開発責任者
		ソフトウェア結合試験計画書	BC	設計開発担当者	品質保証担当者	設計開発責任者
7.2	ソフトウェア要求分析（5.2）	ソフトウェア要求分析シート	ABC	設計開発担当者	品質保証担当者	設計開発責任者
		ソフトウェア要求仕様書	ABC	設計開発担当者	品質保証担当者	設計開発責任者
		トレーサビリティマトリックス	ABC	設計開発担当者	品質保証担当者	
		リスクマネジメントワークシート（更新）	ABC	設計開発担当者	-	-
		ソフトウェア要求事項検証記録	ABC	品質保証担当者	-	-
		ソフトウェア要求分析シートレビュ記録	ABC	品質保証担当者		
		リスクマネジメントファイル				
7.3	ソフトウェアアーキテクチャの設計（5.3）	ソフトウェアアーキテクチャ仕様書	BC	設計開発担当者	品質保証担当者	設計開発責任者
		ソフトウェアアーキテクチャ仕様書検証記録	BC	品質保証担当者	-	-
		トレーサビリティマトリックス	BC	設計開発担当者	品質保証担当者	-
7.4	ソフトウェア詳細設計（5.4）	ソフトウェア詳細設計書	BC	設計開発担当者	品質保証担当者	設計開発責任者
		ソフトウェア詳細設計書検証記録	C	品質保証担当者	-	-
		トレーサビリティマトリックス	BC	設計開発担当者	品質保証担当者	-
7.5.2	ソフトウェアユニットの実装（5.5）	ソースコード	BC	設計開発担当者	品質保証担当者	設計開発責任者
		ソフトウェアユニット検証計画書	BC	設計開発担当者	品質保証担当者	設計開発責任者
		ソフトウェアユニットテスト仕様書	BC	設計開発担当者	品質保証担当者	設計開発責任者

7. ソフトウェア開発およびサイバーセキュリティ確保手順（市販前）（5.）

以下手順においては、特記がない限り当該アクティビティはソフトウェア安全性クラス A、B、C すべてにおいて適用される。

7.1 ソフトウェア開発計画（5.1）

7.1.1 プロセスのインプットおよびアウトプット

インプット	アウトプット
➢ソフトウェア要求	➢「ソフトウェア開発計画書」 ➢「ソフトウェア検証計画書」 ➢「リスクマネジメント計画書」 ➢「ソフトウェア文書管理計画書」 ➢「ソフトウェア構成管理計画書」 ➢「ソフトウェア結合試験計画書」

7.1.2 ソフトウェア開発計画書の作成

開発するソフトウェアシステムの適用範囲、規模およびソフトウェア安全クラス分類に適した、ソフトウェア開発プロセスのアクティビティを実施するために、（一つまたは複数の）ソフトウェア開発計画を確立する。

ソフトウェア開発ライフサイクルモデルは、その計画の中に全てを定義するか、または引用するかのいずれかとする。計画は、次の事項を扱った内容とする。（クラス A、B、C）

安全性クラス分類が決定するまで、全てのソフトウェアアイテムはクラス C であると想定すること。

したがって、全てのクラスが対象でない項目についても計画書内に項目の記載を設け、安全性クラス分類決定後に詳細事項を記載すること。

役　割	実施内容	成果物	留意事項
設計開発担当者	ソフトウェア開発の計画を策定し、「ソフトウェア開発計画書」を作成する。（5.1.1）	「ソフトウェア開発計画書」（MD-SW-01）	・ソフトウェア開発計画書には以下の事項を含むこと： ➢ソフトウェアシステムの開発に使用するプロセス ➢アクティビティおよびタスクの成果物（文書化を含む。） ➢システム要求事項、ソフトウェア要求事項、結合試験（ソフトウェアシステム試験）およびソフトウェアに実装するリスクコントロール手段の間のトレーサビリティ ➢SOUP 構成アイテムおよび開発支援用ソフトウェアを含む、ソフトウェア構成管理および変更管理 ➢ライフサイクルの各段階で発見される、医療機器ソフトウェア、成果物およびアクティビティの問題に対処するためのソフ

役　割	実施内容	成果物	留意事項
			トウェア問題解決
設計開発担当者	（IEC 81001-5-1 5.1.1 ライフサイクルプロセスにおけるアクティビティ） 「ソフトウェア開発計画書」には、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含める。	「ソフトウェア開発計画書」（MD-SW-01） または 「サイバーセキュリティマネジメント計画書」（MD-QMS-F85）	ライフサイクルのアクティビティは、通常受け入れられている製品開発プロセスと一貫性があり、それと統合されたもので、次を含むが、これらには限らない。 a) 変更管理および変更履歴を伴う、構成管理 b) 製品の説明およびトレーサビリティを伴う要求事項の定義 c) モジュラー設計などの、ソフトウェアまたはハードウェアの設計および実装の実践 d) 再現性のある試験による検証およびバリデーションのプロセス e) 全ての開発プロセス記録のレビュおよび承認 f) 製品のサポート g) ソフトウェアのセキュリティ更新およびパッチ
設計開発担当者	（IEC 81001-5-1 5.1.2 開発環境のセキュリティ） 開発、生産、配送および保守に用いる IT インフラストラクチャーを、不正アクセス、破損および削除から保護するためのリスクベースの手続的および技術的なコントロールを「ソフトウェア開発計画書」に明記する。	「ソフトウェア開発計画書」（MD-SW-01） または 「サイバーセキュリティマネジメント計画書」（MD-QMS-F85）	・設計、実装、更新、試験およびリリースを実施中のソフトウェアを保護することを含む。
設計開発担当者	（IEC 81001-5-1 5.1.3 セキュアコーディングの規約） セキュアなソフトウェアシステムの設計および実装に関連する現時点でのベストプラクティスに合致するセキュアコーディングの規約を「ソフトウェア開発計画書」に明記する。	「ソフトウェア開発計画書」（MD-SW-01） または 「サイバーセキュリティマネジメント計画書」（MD-QMS-F85）	
設計開発担当者	「ソフトウェア開発計画書」に、ソフトウェアアイテムの開発に関連する次の項目を示すかまたは引用する。（5.1.4） 4) 規格 5) 方法 6) ツール	「ソフトウェア開発計画書」（MD-SW-01）	・クラス C の場合
設計開発担当者	管理が必要な支援アイテムを特定し、「ソフトウェア開発計画書」に明記する。（5.1.10）	「ソフトウェア開発計画書」（MD-SW-01）	・クラス B、C のソフトウェアの場合 ・管理が必要な支援アイテムには、医療機器ソフトウェアに影響を及ぼす可能性のある、医療機器ソフトウェアの開発に使用するツー

役　割	実施内容	成果物	留意事項
			ル、アイテムまたは設定を含めること。
設計開発担当者	ソフトウェア構成アイテムが、その検証前に、構成マネジメント管理下に置かれるように計画し、「ソフトウェア開発計画書」に記載する。（5.1.11）	「ソフトウェア開発計画書」（MD-SW-01）	・クラス B、C のソフトウェアの場合
設計開発担当者	次のための手順を「ソフトウェア開発計画書」に含める（5.1.12）： a) 選択されたプログラミング技術に基づいて取り入れられたかもしれない、ソフトウェアシステムに関する欠陥のカテゴリーの特定 b) これらの欠陥が許容できないリスクを誘発しないことを実証する証拠の文書化	「ソフトウェア開発計画書」（MD-SW-01）	・クラス B、C のソフトウェアの場合 ・基準とすることでも良い。
品質保証担当者	「ソフトウェア開発計画書」をレビュする。	「ソフトウェア開発計画書」（MD-SW-01）	
設計開発責任者	「ソフトウェア開発計画書」の記載内容を確認し、承認する。	「ソフトウェア開発計画書」（MD-SW-01）	・「ソフトウェア開発計画書レビュ記録」を参照すること。

7.1.3　ソフトウェア結合および結合試験計画書（5.1.5）

役　割	実施内容	成果物	留意事項
検証担当者	「ソフトウェア結合試験計画書」を作成する。	「ソフトウェア結合試験計画書」（MD-SW-05）	・クラス B、C の場合 ・結合試験およびソフトウェアシステム試験は、一つの計画および一連のアクティビティに結合することとする。 ・「ソフトウェア開発計画書」から本計画書を引用すること。 ・「ソフトウェア開発計画書」に直接記載しても良い。
品質保証担当者	「ソフトウェア結合試験計画書」をレビュし、レビュ結果を文書化する。	「ソフトウェア結合試験計画書」（MD-SW-05）	
検証責任者	「ソフトウェア結合試験計画書」の記載内容を確認し、承認する。	「ソフトウェア結合試験計画書」（MD-SW-05）	

7.1.4　ソフトウェア検証計画書の作成（5.1.6）

役　割	実施内容	成果物	留意事項
検証担当者	「ソフトウェア開発計画書」（最新版）を参照し、「ソフトウェア検証計画書」を作成する。	「ソフトウェア検証計画書」（MD-SW-02）	・「ソフトウェア開発計画書」から本計画書を引用すること。 ・「ソフトウェア開発計画書」に直

			接記載しても良い。 ・「ソフトウェア検証計画書」（MD-SW-02）には以下の事項を含めること： ➢検証が必要な成果物 ➢各ライフサイクルアクティビティに必要な検証タスク ➢成果物を検証するマイルストーン ➢成果物検証の合否判定基準
品質保証担当者	「ソフトウェア検証計画書」をレビュし、レビュ結果を文書化する。	「ソフトウェア検証計画書」（MD-SW-02）	
検証責任者	「ソフトウェア検証計画書」の記載内容を確認し、承認する。	「ソフトウェア検証計画書」（MD-SW-02）	

7.1.5 リスクマネジメント計画書の作成（5.1.7）

本文書で定義したドキュメントはすべてソフトウェア文書管理の対象とする。

すべての成果物を「リスクマネジメント規程」（MD-QMS-K5）に従って RMF にファイリングし、管理すること。

役　割	実施内容	成果物	留意事項
リスクマネジメント担当者	「リスクマネジメント計画書」を作成する。	「リスクマネジメント計画書」（MD-QMS-F503）	・「リスクマネジメント規程」（MD-QMS-K5）に従う。 ・「ソフトウェア開発計画書」から本計画書を引用すること。 ・「ソフトウェア開発計画書」に直接記載しても良い。
品質保証担当者	「リスクマネジメント計画書」をレビュし、レビュ結果を文書化する。	「リスクマネジメント計画書」（MD-QMS-F503）	
設計開発責任者	「リスクマネジメント計画書」の記載内容を確認し、承認する。	「リスクマネジメント計画書」（MD-QMS-F503）	

7.1.6 ソフトウェア文書管理計画書の作成（5.1.8）

ソフトウェア開発プロセスにて作成するドキュメント、文書作成に関わる作業標準の識別、発行に関わる計画を作成し、文書化する。

本文書で定義したドキュメントはすべてソフトウェア文書管理の対象とする。

すべての成果物を「設計管理規程」（MD-QMS-K4）に従って DHF にファイリングし、管理すること。

役　割	実施内容	成果物	留意事項
設計開発担当者	「ソフトウェア文書管理計画書」を作成する。	「ソフトウェア文書管理計画書」（MD-SW-	・「ソフトウェア開発計画書」から本計画書を引用すること。 ・「ソフトウェア開発計画書」に直

		03）	接記載しても良い。 ・ 記載した文書または文書のタイプそれぞれについて、次の情報を示すかまたは引用すること。 ➢題名、名称または命名規則（naming convention） ➢目的 ➢開発、レビュ、承認および修正のための手順並びに責任
品質保証担当者	「ソフトウェア文書管理計画書」をレビュし、レビュ結果を文書化する。	「ソフトウェア文書管理計画書」（MD-SW-03）	
設計開発責任者	「ソフトウェア文書管理計画書」の記載内容を確認し、承認する。	「ソフトウェア文書管理計画書」（MD-SW-03）	

7.1.7 ソフトウェア構成管理計画書の作成（5.1.9）

エンベデッド SOUP を含む、ソフトウェアの構成アイテムの保管、アクセス、リリースおよび変更制御に関わる計画を作成し、文書化する。

開発が進むにつれて、必要に応じてソフトウェア構成管理計画書を更新すること。

役　割	実施内容	成果物	留意事項
設計開発担当者	「ソフトウェア構成管理計画書」を作成する。	「ソフトウェア構成管理計画書」（MD-SW-04）	・「ソフトウェア開発計画書」から本計画書を引用すること。 ・「ソフトウェア開発計画書」に直接記載しても良い。 ・以下のソフトウェア構成管理情報を記載または引用すること： ➢管理対象アイテムのクラス、タイプ、カテゴリーまたはリスト ➢ソフトウェア構成管理アクティビティおよびタスク ➢ソフトウェア構成管理活動の実行に責任を負う組織 ➢それらの組織と他の組織（例えばソフトウェア開発または保守など）との関係 ➢アイテムを構成管理下に置く時期 ➢問題解決プロセスを使用する時期
品質保証担当者	「ソフトウェア構成管理計画書」をレビュし、レビュ結果を文書化する。	「ソフトウェア構成管理計画書」（MD-SW-04）	
設計開発責任者	「ソフトウェア構成管理計画書」の記載内容を確認し、承認する。	「ソフトウェア構成管理計画	

		書」（MD-SW-04）	

7.2 リスクアセスメント

実施者	実施内容	成果物	留意事項
リスクマネジメント担当者	既知の脆弱性に対する最新のアップデートを調査する		・脆弱性検査・診断ツール等を利用して定量的に対応度合いを把握・記録すること ・共通脆弱性スコアリングシステム（Common Vulnerability Scoring System：CVSS）等の広く採用されている脆弱性スコアリングシステムを採用して透明性を確保し分析・評価を行うこと ・必要に応じて、CVSS スコア（基本値、現状値）を再評価すること ・再評価に関して MITRE Rubric for Applying CVSS to Medical Devices を参照すること ・サードパーティ製ソフトウェアの提供業者の倒産や買収による突然のサポート停止等を含め、脆弱性発生によるリスクがあることを理解すること
リスクマネジメント担当者	サイバーセキュリティに関する脆弱性を特定する	リスクマネジメントワークシート	・最新の技術に基づくリスクマネジメント手法を適用すること ・医療機器の意図する使用環境を評価すること ・合理的に予見可能な誤使用のシナリオを評価すること
リスクマネジメント担当者	関連するリスクの推定および評価を実施する	リスクマネジメントワークシート	・MD-QMS-K5「リスクマネジメント規程」に従うこと ・JIS T 14971:2020 および TR T 24971:2020 によって最新の技術に基づくリスクマネジメントを TPLC に渡って実施すること
リスクマネジメント担当者	脅威分析を行い、第三者による攻撃、脆弱性の悪用可能性を評価する		・脅威モデリング等を用いること
リスクマネジメント担当者	攻撃対象領域（アタックサーフェイスともいう）を特定する	システム構成（アーキテクチャ）図	・システム構成図は顧客向け文書に記載すること ・「サイバーセキュリティ規程」の「セキュリティ要求事項およびアーキテクチャ設計の設計原則」を参照すること

7.4 ソフトウェア要求分析（5.2）

7.4.1 プロセスのインプットおよびアウトプット

インプット	アウトプット
➢ 「ソフトウェア開発計画書」	➢ 「ソフトウェア要求仕様書」 ➢ 「ソフトウェア開発計画書」等の各種計画書（更新） ➢ 「トレーサビリティマトリックス」 ➢ 「ソフトウェア要件分析シート」（任意） ➢ 「リスクマネジメントワークシート」（更新） ➢ 「ソフトウェア要求仕様書チェックリスト」 ➢ 「ソフトウェア要求事項検証記録」 ➢ 上記文書のレビュ記録

7.4.2 ソフトウェア要求仕様書作成準備

役　割	実施内容	成果物	留意事項
設計開発責任者	提案されたプロジェクトの製品の要件を理解する。		・ 下記のことで達成できる。 ➢商品担当部門または設計開発担当者とのブレーンストーミングセッション ➢プロジェクトチームとの議論 ➢質問票 など ・ 必要であれば、要件理解の妥当性を確認するために、適切な利害関係者と共同でソフトウェアの要件として割り当てられた要件をレビュすること。 ・ 割り当てられた要件のレビュ結果を基にコミットメントが実現可能かどうかを利害関係者と協議すること。
設計開発担当者	必要に応じ、要件を分析し、「ソフトウェア要求分析シート」（MD-SW-10）を作成する。	「ソフトウェア要求分析シート」（MD-SW-10）	・ 下記の要素に対して要件を分析し文書化する。 ➢タイプ（機能または非機能） ➢優先度 ➢検証／テスト方法 ➢テストレベル ・ 要件に関する不明な点は、設計開発担当者または商品担当部門に確認して解決すること。
品質保証担当者	「ソフトウェア要求分析シート」をレビュし、レビュ結果を文書化する。	「ソフトウェア要求分析シート	

役　割	実施内容	成果物	留意事項
		レビュー記録」（MD-SW-11）	
設計開発責任者	「ソフトウェア要求分析シート」の記載内容を確認し、承認する。		
設計開発担当者	リスク分析を行う。	「リスクマネジメントワークシート」（MD-QMS-F505）	・「リスクマネジメント規程」（MD-QMS-K5）に従う。
設計開発担当者	サイバーセキュリティについて検討する。	「リスクマネジメントワークシート」（MD-QMS-F505）	・「サイバーセキュリティ規程」（MD-QMS-K85）に従う。
設計開発担当者	ユーザビリティエンジニアリング評価を行う。	「リスクマネジメントワークシート」（MD-QMS-F505）	・「ユーザビリティエンジニアリング規程」（MD-QMS-K4U）に従う。

7.4.3　ソフトウェア要求仕様書の作成（5.2.2）

役　割	実施内容	成果物	留意事項
設計開発担当者	「ソフトウェア要求仕様書」を作成する。	「ソフトウェア要求仕様書」（MD-SW-12）	・ソフトウェア開発の初期に要求事項のすべてが明らかになっているとは限らないため、T.B.D 項目を含んでいても良い。ただし、すべての T.B.D 項目を終結まで追跡すること。 ・ソフトウェア要求事項の定義に役立つ品質特性に関する情報については、ISO/IEC9126-1 に記載されているため、要求仕様作成の際の参考情報として用いて良い。 ・必要に応じてシステム要求事項を含めた既存の要求事項の再評価を行い、その要求事項を更新すること。 ・以下を特定し、文書化すること。 ➢ 機能および能力についての要求事項 ➢ ソフトウェアシステムのインプットおよびアウトプット ➢ ソフトウェアシステムと他のシステムとの間のインターフェース ➢ ソフトウェアによる警報、

役　割	実施内容	成果物	留意事項
			警告および操作者へのメッセージ ➢ い ➢ ソフトウェアが要求するユーザインタフェース要求事項 ➢ データ定義およびデータベース要求事項 ➢ 納入した医療機器ソフトウェアの、操作現場および保守現場におけるインストールおよび検収の要求事項 ➢ 操作および保守の方法に関わる要求事項 ➢ ITネットワーク側面に関する要求事項 ➢ ユーザー保守要求事項 ➢ 規制要求事項
設計開発担当者	(IEC 81001-5-1 5.2.1 ヘルスソフトウェアのセキュリティ要求事項) 据付け、運用、保守およ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、ソフトウェアのセキュリティ要求事項を「ソフトウェア要求仕様書」に明記する。	「ソフトウェア要求仕様書」（MD-SW-12）	
設計開発担当者	ソフトウェアシステムの安全性クラス分類を行う。（4.3）	「リスクマネジメントファイル」（MD-QMS-F507）	
設計開発担当者	ソフトウェアに実装するリスクコントロール手段を、医療機器ソフトウェアの要求事項に含める。（5.2.3）	「ソフトウェア要求仕様書」（MD-SW-12）	ソフトウェアクラス B、C の場合

7.4.4　ソフトウェアリスク分析の再評価（5.2.4）

役　割	実施内容	成果物	留意事項
設計開発担当者	ソフトウェア要求事項の確定後、医療機器のリスク分析を再評価し、「リスクマネジメントワークシート」（MD-QMS-F502）を更新する。	「リスクマネジメントワークシート」（MD-QMS-F505）	・ソフトウェア要求事項をインプットとして、特にソフトウェアに起因する危害に着目して医療機器のリスク分析を再評価し、更新すること。
設計開発担当者	（IEC 81001-5-1 5.2.3 要求仕様対象ソフトウェアのセキュリティに関連するリスク） 全ての要求仕様対象ソフトウェアのセキュリティに関連するリスクを特定し、「ソフトウェア要求仕様書」に明記す	「ソフトウェア要求仕様書」（MD-SW-12）	

役　割	実施内容	成果物	留意事項
	る。		

7.4.5　要求事項の更新（5.2.5）

役　割	実施内容	成果物	留意事項
設計開発担当者	要求事項分析の結果を受け、必要に応じてシステム要求事項等の既存の要求事項を再評価し、更新する。	「ソフトウェア要求仕様書」（MD-SW-12）	

7.4.6　ソフトウェア要求事項の検証（5.2.6）

役　割	実施内容	成果物	留意事項
品質保証担当者	ソフトウェア要求事項を検証し、「ソフトウェア要求事項検証記録」を作成する。	「ソフトウェア要求事項検証記録」（MD-SW-13）	・以下について検証すること。 ➢ システム要求事項（リスクコントロールに関わるものを含む。）を実装している。 ➢ 相互に矛盾しない。 ➢ 曖昧さを回避した用語で表現している。 ➢ 試験基準を確立することができる用語で表現していて、試験が実施できる用語で表現している。 ➢ 一意に識別できる。 ➢ システム要求事項または他の要求事項を追跡できる。
各レビュ担当者	（IEC 81001-5-1 5.2.2 セキュリティ要求事項のレビュ） セキュリティ要求事項を確実にするため「ソフトウェア要求仕様書」をレビュする。	「ソフトウェア要求事項検証記録」（MD-SW-13）	下記をレビュすること。 a)　リスクコントロールに関連するものを含む製品要求事項を実装している。 b)　相互に矛盾しない。 c)　曖昧さを回避した用語で表現している。 d)　試験基準を確立して、試験が行える表現で記載している。
各レビュ担当者	レビュ担当者の独立性のレベルを示すために「ソフトウェア要求事項検証記録」にレビュ担当者の氏名・所属部署・役職・本プロジェクトにおける役割と責任等を明記する。	「ソフトウェア要求事項検証記録」（MD-SW-13）	次の代表的な分野の各々が、このアクティビティに参加すること。 a)　IT アーキテクト・開発担当者（要求事項を実装する人） b)　試験担当者（要求事項に適合していることを確認する人）

役　割	実施内容	成果物	留意事項
			c)　機能横断的なエキスパート（臨床知識をもつ人を含むことが可能である。） d)　セキュリティのアドバイザー
設計開発責任者	「ソフトウェア要求事項検証記録」の記載内容を確認し、問題がなければ「ソフトウェア要求仕様書」を承認する。	「ソフトウェア要求仕様書」（MD-SW-12）	

7.4.7　ソフトウェア開発計画書の更新（5.1.2）

役　割	実施内容	成果物	留意事項
設計開発担当者	・ 安全性クラス分類の結果を受け、7.1 項で作成した「ソフトウェア開発計画書」およびその他の計画書を更新する。	「ソフトウェア開発計画書」（MD-SW-01） 「ソフトウェア検証計画書」（MD-SW-02） 「リスクマネジメント計画書」（MD-QMS-F503） 「ソフトウェア文書管理計画書」（MD-SW-03） 「ソフトウェア構成管理計画書」（MD-SW-04） 「ソフトウェア結合試験計画書」（MD-SW-05）	・ ソフトウェアアイテムをグループ分けし、各グループに対して適用するプロセスを設定すること。 ・ 各グループに適用するプロセスは、各グループに含まれるソフトウェアアイテムの中で最も高い安全性クラスをもとに設定すること。 ・ より低い安全性クラスを設定する場合は、根拠を記載すること。 ・ 「文書管理規程」（MD-QMS-K4）に従うこと。
品質保証担当者	更新された「ソフトウェア開発計画書」等をレビュし、レビュ結果を文書化する。		
設計開発責任者	更新された「ソフトウェア開発計画書」等の記載内容を確認し、承認する。		

7.5　リスクコントロール策の検討

実施者	実施内容	成果物	留意事項
設計開発担当者	リスクコントロール策を検討する	リスクマネジメントワークシート	・医療機器製品の品質、有効性および安全性が確保されるよう、当社の責任によって必要な対策を設計段階で講じること ・リスクを受容可能なレベルまで低減すること ・開発環境については、JIS T 2304 の「管理が必要な支援アイテム」の規定に従って管理すること ・MD-QMS-K85「サイバーセキュリティ規程」に従い、補完的リスクコントロールについても考慮すること。
設計開発担当者	セキュリティ機能を組込む	設計仕様書	・MD-QMS-K4「設計管理規程」に従うこと ・製品に導入したソフトウェアに駆除できない既知の脆弱性が存在した場合、それが如何なる手段を持っても悪用されないという妥当な証拠があれば、これを設計仕様書に記載すること ・市販後に合理的手段によってアップデートを導入できるユーザビリティが考慮された手段を機能として組み込むこと ・医療機器がレガシー状態になった場合を想定して、適用可能なファイアウォール等の補完的対策の仕様および利用可能性等についてあらかじめ検討しておくこと

7.6　ソフトウェアアーキテクチャの設計（5.3）

7.6.1　プロセスのインプットおよびアウトプット

インプット	アウトプット
➢「ソフトウェア要求仕様書」	➢「ソフトウェアソフトウェアアーキテクチャ仕様書」 ➢「ソフトウェアアーキテクチャ仕様書検証記録」 ➢レビュ記録 ➢「トレーサビリティマトリックス」

7.6.2　ソフトウェアアーキテクチャ仕様書の作成

役　割	実施内容	成果物	留意事項

設計開発担当者	医療機器ソフトウェアの要求事項を、文書化したアーキテクチャ（ソフトウェアの構造の説明およびソフトウェアアイテムの特定をしているもの）に変換する。（5.3.1）	「ソフトウェアアーキテクチャ仕様書」（MD-SW-20）	・クラス B、C の場合 ・以下の事項を記載する。 ➢ソフトウェアの要求事項のソフトウェアの構造およびソフトウェアアイテムを明示したアーキテクチャへの変換 ➢ソフトウェアアイテムとソフトウェアアイテム外部のコンポーネント（ソフトウェアおよびハードウェア）との間、およびソフトウェアアイテム間のインターフェースについて開発したアーキテクチャ
設計開発担当者	（IEC 81001-5-1 5.3.1 多層防御アーキテクチャ） 設計セキュアなアーキテクチャを定め「ソフトウェアアーキテクチャ仕様書」に明記する。	「ソフトウェアアーキテクチャ仕様書」（MD-SW-20）	・開発の各段階で、多層防御を考慮し、各階層の防御に対して技術的要求事項を割り当てることが望ましい。 ・技術的なセキュリティに関連するリスクコントロールを特定する際、ソフトウェアの安全または性能に関する要求事項を考慮に入れる。
設計開発担当者	ソフトウェアアイテムとソフトウェアアイテム外部のコンポーネント（ソフトウェアおよびハードウェア）との間、およびソフトウェアアイテム間のインターフェースについて、アーキテクチャを開発し、「ソフトウェアアーキテクチャ仕様書」に記載する。（5.3.2）	「ソフトウェアアーキテクチャ仕様書」（MD-SW-20）	・クラス B、C の場合
設計開発担当者	（IEC 81001-5-1 5.3.2 セキュアな設計のベストプラクティス） セキュアな設計のベストプラクティスを特定し「ソフトウェアアーキテクチャ仕様書」に明記する。	「ソフトウェアアーキテクチャ仕様書」（MD-SW-20）	セキュアな設計のベストプラクティスを文書化する。 これには、次を含めることが望ましいが、これらには限らない。 a) 設計の一部として、全ての信頼境界を文書化 b) 最小権限（意図する操作を実行するために必要な権限だけをユーザーまたはソフトウェアに許可） c) 可能な場合、セキュアであることが証明されたソフトウェアアイテムまたは設計の使用 d) メカニズムの経済性（シンプルな設計の追求） e) セキュアな設計パターンの使用

			f) 攻撃対象領域の削減 g) 開発中に用いた、バックドア、デバッグ用のアクセス手段およびデバッグ情報の除去、またはそれらの存在および不正アクセスからの保護の必要性の文書化 h) 不正アクセスからの、残ったデバッグ情報の保護 必要に応じて、上記のベストプラクティスを含めて、多層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。
設計開発担当者	SOUP アイテムについて、その意図した用途に必要な機能性能要求事項を明確にし、「ソフトウェアアーキテクチャ仕様書」に記載する。（5.3.3）	「ソフトウェアアーキテクチャ仕様書」（MD-SW-20）	・ クラス B、C の場合 ・ ソフトウェアアイテムを SOUP と特定している場合
設計開発担当者	SOUP アイテムの正常な動作に必要なシステムハードウェアおよびシステムソフトウェアを明確にし、「ソフトウェアアーキテクチャ仕様書」に記載する。（5.3.4）	「ソフトウェアアーキテクチャ仕様書」（MD-SW-20）	・ クラス B、C の場合 ・ ソフトウェアアイテムを SOUP と特定している場合
設計開発担当者	リスクコントロールに必要なソフトウェアアイテム間の分離を明確化し、分離が有効であることを確実にする方法を「ソフトウェアアーキテクチャ仕様書」に記載する。（5.3.5）	「ソフトウェアアーキテクチャ仕様書」（MD-SW-20）	・ クラス C の場合
設計開発担当者	各ソフトウェアアイテムに対して安全性クラスを分類し、文書化する。（4.3 d)、e)）	「ソフトウェアアーキテクチャ仕様書」（MD-SW-20）	・ 患者、操作者、その他の人々に対する影響を考慮する。 ・ 各ソフトウェアアイテムは基本的にソフトウェアシステムの安全性クラスを引き継ぐ形で安全性クラスを設定する。 ・ ただし、論理的根拠を明示できる場合は、引き継いだ安全性クラスと異なる安全性クラスを設定しても良い。
設計開発担当者	「トレーサビリティマトリックス」を更新する。	「トレーサビリティマトリックス」（MD-SW-21）	
品質保証担当者	「トレーサビリティマトリックス」をレビュし、レビュ結果を文書化する。	「トレーサビリティマトリックス」（MD-SW-21）	

7.6.3 ソフトウェアアーキテクチャ仕様書の検証（5.3.6）

役　割	実施内容	成果物	留意事項
検証担当者	ソフトウェア要求事項を検証し、「ソフトウェアアーキテクチャ仕様書検証記録」に文書化する。	「ソフトウェアアーキテクチャ仕様書検証記録」（MD-SW-22）	・クラス B、C の場合 ・以下の事項を検証すること。 ➢ ソフトウェアのアーキテクチャが、リスクコントロールに関わる要求事項を含む、システムおよびソフトウェアの要求事項を実装している。 ➢ ソフトウェアアーキテクチャ仕様書が、ソフトウェアアイテム間およびソフトウェアアイテムとハードウェアとの間のインターフェースを支援できる。 ➢ 医療機器アーキテクチャが、全ての SOUP アイテムの正常な動作を支援している。
検証担当者	（IEC 81001-5-1 5.3.3 セキュリティアーキテクチャー設計のレビュ） 悪条件における動作に関して、ソフトウェアのアーキテクチャのレビュを実施し「ソフトウェアアーキテクチャ仕様書検証記録」に文書化する。	「ソフトウェアアーキテクチャ仕様書検証記録」（MD-SW-22）	次に示すソフトウェアのアーキテクチャのレビュを実施する。 a) ソフトウェアアイテムの効果的な分離 b) セキュアな設計のベストプラクティス（5.3.2 参照） c) アーキテクチャによってもたらされる可能性があるセキュリティの欠陥
設計開発責任者	「ソフトウェアアーキテクチャ仕様書検証記録」の記載内容を確認し、「ソフトウェアアーキテクチャ仕様書」を承認する。	「ソフトウェアアーキテクチャ仕様書」（MD-SW-20）	

7.7　ソフトウェア詳細設計（5.4）

エンベデッド SOUP は本章を実施しない。

7.7.1　プロセスのインプットおよびアウトプット

インプット	アウトプット
➢「ソフトウェア開発計画書」 ➢「ソフトウェア要求仕様書」 ➢「ソフトウェアアーキテクチャ仕様書」	➢「ソフトウェア詳細設計書」 ➢「トレーサビリティマトリックス」 ➢「ソフトウェア詳細設計検証記録」（クラス C の場合）

7.7.2　リスクマネジメントワークシートの更新

役　割	実施内容	成果物	留意事項
リスクマネジメント担当者	リスクマネジメントファイルに文書化した、ソフトウェアアイテムが危険状態の一因となるケースのそれぞれについて、リスクコントロール手段を選択し、文書化する。（7.2.1）	「リスクマネジメントワークシート」（MD-QMS-F505）	・クラス B、C の場合 ・リスクコントロール手段は、ソフトウェア若しくは動作環境において実施するか、または取扱説明書への記載による。
リスクマネジメント担当者	（IEC 81001-5-1 7.2 脆弱性、脅威および関連する悪影響の特定） 資産の機密性、完全性および可用性に影響を及ぼす脆弱性、脅威および関連する悪影響を特定し「リスクマネジメントワークシート」に文書化する。	「リスクマネジメントワークシート」（MD-QMS-F505）	・このアクティビティでは、セキュリティコンテキストに関して、意図する使用および意図する使用環境を考慮する。 ・これらのアクティビティは、全ての製品が、（該当する場合）次の特性について、製品の現在の開発範囲に特有の脅威モデルをもつことを確実にするために採用する。 a) システム全体について、分類された情報の正しいフロー b) 信頼境界 c) プロセス d) データストア e) 相互作用する外部エンティティ f) 製品に実装されている内部および外部の通信プロトコル g) デバッグポートを含む、外部からアクセス可能な物理的ポート h) ハードウェアを攻撃するために用いられる可能性がある、JTAG（Joint Test Action Group）などの回路基板のコ

			ネクターまたはデバッグヘッダー i) （意図する）ハードウェアに対する攻撃を含む、潜在的な攻撃ベクター※) j) 潜在的な脅威 k) 特定したセキュリティ関連の問題 l) ドライバーまたはサードパーティ製のアプリケーション（供給者によって開発されていないコード）がアプリケーションにリンクされているという形をとった外部的な依存性 ・脅威モデルは、内容が正しく、かつ、理解していることを確実にするために、開発チームがレビュおよび検証する。 ・脅威モデルは、リリースした製品に対し、（少なくとも年に一度）定期的なレビュを行い、設計変更がされていない場合でも、製品への新たな脅威の発生に対応する必要に応じて更新する。 ・脅威モデルで特定された全ての問題は、9.4 および 9.5 の規定に従って対応する。
リスクマネジメント担当者	次の事項を実施する。（7.2.2） a) リスクコントロール手段をソフトウェア要求事項に含める。 b) リスクコントロール手段の実施に寄与する各ソフトウェアアイテムに対して、そのリスクコントロール手段によってコントロールしているリスクに基づいて、ソフトウェア安全クラスの分類を行う。	「ソフトウェア要求仕様書」（MD-SW-12）（更新） 「ソフトウェアアーキテクチャ仕様書」（MD-SW-20）（更新）	・クラス B、C の場合 ・リスクコントロール手段をソフトウェアアイテムの機能の一部として実装する場合
リスクマネジメント担当者	（IEC 81001-5-1 7.3 セキュリティに関連するリスクの推定および評価） セキュリティに関連するリスクの推定および評価を「リスクマネジメントワークシート」に文書化する。	「リスクマネジメントワークシート」（MD-QMS-F505）	次を行うアクティビティを確立する。 a) 7.2 で特定した脆弱性のリスクを推定する。リスク推定は、脆弱性がサイバーセキュリティに及ぼす悪影響を考慮して行う。リスク推定は、CVSS、MITRE による医療機器用スコアリングなどの脆弱性スコアリングを用いてサポートすることが可能である。スコアリング

			システムは、他のリスクに対して当社が用いる発生確率・重大さのスキーム（例えば、JIS Z 8051 または JIS T 14971 を参照）に基づくことも可能である。 b) 推定したリスクを評価し、スコアリングに基づいて、リスクが受容可能かどうかを判断する。 c) 脅威モデルに対する全ての更新について、製品のリスクマネジメントプロセスに情報提供する。

※ “攻撃ベクター”とは、攻撃者が悪意のある結果をもたらすために機器またはネットワークにアクセスするための手段または経路をいう。

7.7.3 ソフトウェア詳細設計書

役　割	実施内容	成果物	留意事項
設計開発担当者	ソフトウェアがソフトウェアユニットによって表現できるまでそのソフトウェアを分割し、「ソフトウェア詳細設計書」に文書化する。（5.4.1）	「ソフトウェア詳細設計書」（MD-SW-30）	・クラス B、C の場合
設計開発担当者	（IEC 81001-5-1 5.4.1 ソフトウェア設計のベストプラクティス） セキュアなソフトウェアの設計（セキュアな設計のベストプラクティスの使用）を「ソフトウェア詳細設計書」に明記する。	「ソフトウェア詳細設計書」（MD-SW-30）	次を考慮する。 a) アプリケーションレベルのソフトウェア技術（例えば、アルゴリズム、手法） b) 使用するプログラミング技術（例えば、プログラミング言語） c) セキュアな設計のベストプラクティス
設計開発担当者	各ソフトウェアユニットを正しく実行できるように、十分な詳細さで「ソフトウェア詳細設計書」を記載すること。（5.4.2）	「ソフトウェア詳細設計書」（MD-SW-30）	・クラス C の場合
設計開発担当者	（IEC 81001-5-1 5.4.2 セキュアな設計） 「ソフトウェア詳細設計書」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。	「ソフトウェア詳細設計書」（MD-SW-30）	

設計開発担当者	ソフトウェアユニットと外部コンポーネント（ハードウェアまたはソフトウェア）との間のインターフェース、並びに、ソフトウェアユニット間の全てのインターフェースに対して、各ソフトウェアユニットおよびそのインターフェースを正しく実行できるだけの十分な詳細さでインターフェースを設計し、「ソフトウェア詳細設計書」に記載する。（5.4.3）	「ソフトウェア詳細設計書」（MD-SW-30）	・クラス C の場合
設計開発担当者	（IEC 81001-5-1 5.4.3 セキュアなヘルスソフトウェアのインターフェース） 「ソフトウェア詳細設計書」には、物理的および論理的インターフェースを含む、ソフトウェアの各インターフェースを特定し、特性を明確化したうえで文書化する。	「ソフトウェア詳細設計書」（MD-SW-30）	必要に応じて、設計の一部として次を明確にする。 a) インターフェースが、外部から（他の製品によって）アクセス可能か、若しくはソフトウェアのソフトウェアアイテムとの間で内部的にアクセス可能か、またはその両方か b) 外部インターフェース上の、ソフトウェアセキュリティコンテキストのセキュリティへの影響 c) インターフェースの潜在的なユーザーおよびインターフェースを介して（直接的または間接的に）アクセス可能な資産 d) 静的設計が、信頼境界を越えるインターフェースへのアクセスを含むかどうか e) 関連する脅威を含む、ソフトウェアのセキュリティコンテキスト内でのインターフェースの使用に関連する、セキュリティの考慮事項、想定および／または制約事項 f) インターフェースの使用および c)で明確にした資産のアクセスに必要な、セキュリティ上の役割、権限・権利およびアクセスコントロールの許可 g) インターフェースおよび c)で特定した資産を保護するために用いる、実行時の入力バリデーション、アウトプット処理およびエラー処理を含む、セキュリティ機能および／または補完的メ

			カニズム h) インターフェースを実装するためのサードパーティ製ソフトウェアアイテムの使用およびそのセキュリティ機能 i) インターフェースが外部からアクセス可能な場合は、その使用方法を記載した文書 j) 脅威モデルで特定した脅威を、設計でどのように軽減しているかの説明
設計開発担当者	「トレーサビリティマトリックス」を更新する。	「トレーサビリティマトリックス」（MD-SW-21）	
品質保証担当者	「トレーサビリティマトリックス」をレビュし、レビュ結果を文書化する。	「トレーサビリティマトリックス」（MD-SW-21）	

7.7.4 詳細設計の検証（5.4.4）

役　割	実施内容	成果物	留意事項
検証担当者	ソフトウェアの詳細設計を検証し、「ソフトウェア詳細設計検証記録」に文書化する。	「ソフトウェア詳細設計検証記録」（MD-SW-31）	・クラス C の場合 ・次によることを検証する。 1) ソフトウェアアーキテクチャ仕様書を実装している。 2) ソフトウェアアーキテクチャ仕様書との矛盾がない。
検証担当者	リスクコントロール手段を全て実施していることを検証し、その検証結果を文書化する。（7.3.1）	「ソフトウェア詳細設計検証記録」（MD-SW-31）	・「リスクマネジメントワークシート」を参照すること。
検証担当者	（IEC 81001-5-1 5.4.4 セキュリティに対する詳細設計の検証） セキュアな設計の重大な各改訂に関連する弱みについて、特定し、特性を明確化し「ソフトウェア詳細設計検証記録」に文書化する。	「ソフトウェア詳細設計検証記録」（MD-SW-31）	・これは、次を含むが、これらには限らない。 a) 設計で適切に対応されなかったセキュリティ要求事項 b) 製品のインターフェース、信頼境界および資産における、脅威および脅威が脆弱性を悪用する能力 c) 従わなかった詳細設計のベストプラクティス（5.3.2 および 5.4.1）の特定、文書化および特性の明確化 ・問題解決まで追跡すること

リスクマネジメント担当者	リスクコントロール手段をレビュし、それによって新たな危険状態に至ることがないか判断する。（7.3.1）	「ソフトウェア詳細設計検証記録」（MD-SW-31）	・
設計開発責任者	「ソフトウェア詳細設計検証記録」の記載内容を確認し、「ソフトウェア詳細設計書」を承認する。	「ソフトウェア詳細設計書」（MD-SW-30）	・「ソフトウェア詳細設計書」のレビュ記録を参照すること。
設計開発担当者	「トレーサビリティマトリックス」を更新する。	「トレーサビリティマトリックス」（MD-SW-21）	
品質保証担当者	「トレーサビリティマトリックス」をレビュし、レビュ結果を文書化する。	「トレーサビリティマトリックス」（MD-SW-21）	

7.8　ソフトウェアユニットの実装（5.5）

エンベデッド SOUP は本章を実施しない。

7.8.1　プロセスのインプットおよびアウトプット

インプット	アウトプット
➢「ソフトウェア開発計画書」 ➢「ソフトウェアアーキテクチャ仕様書」 ➢「ソフトウェア詳細設計書」	➢ ソースコード ➢ コードレビュチェックリスト ➢ 「ソフトウェアユニットテスト仕様書」 ➢ すべてのテストケースが合格するまで繰り返した「ソフトウェアユニットテスト記録」 ➢ 「ソフトウェアユニットテスト報告書」 ➢ 「トレーサビリティマトリックス」 ➢ 上記文書のレビュ記録

7.8.2　ソフトウェアユニットの実装（5.5.1）

役　割	実施内容	成果物	留意事項
設計開発担当者	(IEC 81001-5-1 5.5.1 セキュアコーディングの規約) セキュアコーディングの規約を文書化する。	コーディング規約（各言語毎）	
設計開発担当者	「ソースコード」を作成する。	ソースコード	・コーディング規約に従うこと

7.8.3　ソフトウェアユニット検証プロセスの確立（5.5.2）

役　割	実施内容	成果物	留意事項
設計開発担当者	ソフトウェアユニットを検証するための方針、方法および手順を「ソフトウェアユニット検証計画書」に文書化する。	「ソフトウェアユニット検証計画書」（MD-SW-40）	・クラス B、C の場合 ・検証を試験によって実施する場合は、その試験手順の適切性について評価すること。

7.8.4　ソフトウェアユニットの合否判定基準

役　割	実施内容	成果物	留意事項
設計開発担当者	より大きなソフトウェアアイテムに結合する前に、必要に応じて「ソフトウェアユニットの合否判定基準」を確立し、ソフトウェアユニットが合否判定基準を確実に適合するようにする。（5.5.3）	「ソフトウェアユニットテスト仕様書」（MD-SW-41）	・クラス B、C の場合 ・合否判定基準の例は以下の通り： ➢ ソフトウェアコードが、リスクコントロール手段を含む要求事項を実装しているか。 ➢ ソフトウェアコードが、ソフトウェアユニットのイン

			ターフェース設計と矛盾しないか。 ➢ ソフトウェアコードが、プログラミング手順またはコーディング標準に従っているか。
設計開発担当者	設計に当たって、必要に応じて次の事項についての追加の合否判定基準を含める。（5.5.4）	「ソフトウェアユニットテスト仕様書」（MD-SW-41）	・クラス C のソフトウェアユニットについて、必要に応じて以下の事項を追加の合否判定基準に含めること： ➢ 適正なイベントシーケンス ➢ データおよび制御フロー ➢ 計画したリソース配分 ➢ 異常処理（エラーの定義、特定および復帰） ➢ 変数の初期化 ➢ 自己診断 ➢ メモリー管理およびメモリオーバーフロー ➢ 境界条件
品質保証担当者	「ソフトウェアユニットテスト仕様書」をレビュする。	「ソフトウェアユニットテスト仕様書レビュ記録」（MD-SW-42）	・テスト手順の適切性について評価すること。
設計開発責任者	「ソフトウェアユニットテスト仕様書」の記載内容を確認し、承認する。	「ソフトウェアユニットテスト仕様書」（MD-SW-41）	・「ソフトウェアユニットテスト仕様書」のレビュ記録を参照すること。
設計開発担当者	「トレーサビリティマトリックス」を更新する。	「トレーサビリティマトリックス」（MD-SW-21）	・
品質保証担当者	「トレーサビリティマトリックス」をレビュし、レビュ結果を文書化する。	「トレーサビリティマトリックス」（MD-SW-21）	・

7.8.5　ソフトウェアユニットの検証（5.5.5）

エンベデッド SOUP は本章を実施しない。

役　割	実施内容	成果物	留意事項
設計開発担当者	「ソフトウェアユニット検証計画書」に従って、「ソースコード」をレビュし、レビュ結果を文書化する。 必要に応じて「コードレビュチェックリスト」を作成する。	ソースコード 「コードレビュチェックリスト」（MD-SW-43）	・ソースコードを作成した者とは別の設計開発担当者が実施すること。
設計開発担当者	（IEC 81001-5-1 5.5.2 セキュリティの実装レビュ） セキュアな設計の実装に関連する全ての	ソースコード 「コードレビュチェックリス	これは、次を含む。 a)　実装で適切に対応されなかったセキュリティ要求事項

	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ための実装レビュを行う。	ト」（MD-SW-43）	（5.2 参照）の特定 b) 使用したセキュアコーディングの規約を特定し、セキュアコーディングの規約のうち、従わなかった部分を文書化する（例えば、使用禁止関数の使用、または最小権限の原則の不適用）。 c) 5.1.3 で確立した、サポートするプログラミング言語に対するセキュアコーディングの規約を使用した、セキュアコーディングのエラーを判断するためのソースコードの静的コード解析（Static Code Analysis、SCA）。静的コード解析は、通常、ツールを使用して行うが、コードインスペクションおよびコードウォークスルーによって行うことも可能である。 d) セキュリティ設計（5.3 および 5.4 を参照）をサポートするために定義したセキュリティ機能に対する実装およびそのトレーサビリティのレビュ e) 脅威の調査およびその脅威が実装インターフェース、信頼境界および資産を侵害する能力の調査（5.3 および 5.4 参照）
設計開発担当者	「ソフトウェアユニットテスト仕様書」に従って、ソフトウェアユニットテストを実施し、テスト結果を記載して「ソフトウェアユニットテスト記録」を作成する。	「ソフトウェアユニットテスト記録」（MD-SW-44）	・「ソフトウェアユニットテスト仕様書」のコピーを用意し、テスト結果を記載したものをテスト記録とすること。 ・テスト結果が期待される結果と相違する場合、再試験を実施するために十分に詳細な情報を記入すること。
設計開発担当者	テスト結果を評価する。	「ソフトウェアユニットテスト記録」（MD-SW-44）	・必要に応じてソフトウェア変更管理手順書に則って該当する成果物の変更を行うこと。
設計開発担当者	テストの実施条件や評価結果を記載する。	「ソフトウェアユニットテスト記録」（MD-SW-44）	・ソフトウェアユニットテストの実施者、実施日、テストサイクル、エラーレートなど。
設計開発担当者	すべてのテストケースが合格（エラーレートが 0%）となるまでテストを繰り返	「ソフトウェアユニットテスト	・バグ収束曲線等を作成し、残存バグ数を推定すること。

7.10　ソフトウェアシステム試験（5.7）

SaMD 開発の場合、ソフトウェアシステム試験を結合試験に統合することとする。

ソフトウェアシステム試験中に異常が発見された場合、10. ソフトウェア問題管理（9.）に従って処理すること。

7.10.1　プロセスのインプットおよびアウトプット

インプット	アウトプット
➢「ソフトウェア開発計画書」 ➢「ソフトウェア要求仕様書」 ➢「ソフトウェア検証計画書」 ➢「ソフトウェア結合試験報告書」 ➢「ソフトウェア要求仕様書」	➢「ソフトウェアシステム試験計画書」 ➢「ソフトウェアシステム試験仕様書」 ➢「ソフトウェアシステム試験スクリプト」 ➢「ソフトウェアシステム試験記録」 ➢「ソフトウェアシステム試験検証記録」 ➢「ソフトウェアシステム試験報告書」 ➢「トレーサビリティマトリックス」 ➢レビュ記録

7.10.2　ソフトウェアシステム試験計画書（5.7.1）

役　割	実施内容	成果物	留意事項
検証担当者	「ソフトウェア検証計画書」および「ソフトウェア要求仕様書」に基づき「ソフトウェアシステム試験計画書」を作成する。	「ソフトウェアシステム試験計画書」	・エンベデッド SOUP を含める。 ・個々のソフトウェア要求事項を対象として、インプット内容、予想する結果、合否判定基準および手順を規定した一連の試験を確立すること。
品質保証担当者	「ソフトウェアシステム試験計画書」をレビュする。	「ソフトウェアシステム試験計画書」	・検証戦略および試験手順の適切性を評価すること。
検証責任者	「ソフトウェアシステム試験計画書」の記載内容を確認し、承認する。	「ソフトウェアシステム試験計画書」	・「ソフトウェアシステム試験計画書」のレビュ記録を参照すること。

7.10.3 セキュリティ試験計画書

役　割	実施内容	成果物	留意事項
検証担当者	「ソフトウェア検証計画書」および「ソフトウェア要求仕様書」に基づき「セキュリティ試験計画書」を作成する。	「セキュリティ試験計画書」	・（IEC 81001-5-1 5.7.5 試験担当者と開発担当者との間の利益相反の管理）攻撃対象領域解析、セキュリティ要求事項試験、脅威軽減試験、脆弱性試験、既知の脆弱性スキャン、侵入試験を実施する検証担当者は、設計開発担当者とは異なる者とすること
検証担当者	（IEC 81001-5-1 5.7.1 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、エラーのシナリオおよび不正な入力に対応していることを検証する試験を計画し「セキュリティ試験計画書」に文書化する。	「セキュリティ試験計画書」	・意図する使用環境に基づき、次の種類の試験を含める。 a) セキュリティ要求事項の機能試験 b) 性能およびスケーラビリティ試験 c) セキュリティに影響する可能性のある、境界・エッジ条件、ストレスおよび不正な形式または予期しないインプットの試験 d) サービスプロバイダー、当社および操作者の間の責任協定取決書に基づく、ソフトウェアが意図する機能を実現するために用いるソフトウェアサービスに対する試験。ソフトウェアサービスは、例えば、クラウドサービス、サービスとしてのソフトウェア（SaaS）、サービスとしてのインフラストラクチャー（IaaS）、サービスとしてのプラットフォーム（PaaS）である。
検証担当者	（IEC 81001-5-1 5.7.2 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、その軽減策の有効性を試験する計画を「セキュリティ試験計画書」に文書化する。	「セキュリティ試験計画書」	アクティビティには、次を含める。 a) 特定の脅威に対応するために実装した各軽減策が、設計どおりに動作することを確実にするために、適切な試験内容を策定し、実行する。 b) 各軽減策を妨害する計画を作成し、実行する。 c) 軽減策が、設計にその他の

			脆弱性を生じさせないことを確実にする。
検証担当者	（IEC 81001-5-1 5.7.3 脆弱性試験） ソフトウェアの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ことに焦点を当てた試験を実施する計画を「セキュリティ試験計画書」に文書化する。	「セキュリティ試験計画書」	a) 既知の脆弱性に対する試験は、少なくとも、確立され業界で認められた、既知の脆弱性の公的な情報源の最近の内容に基づいたものとする。 b) 必要に応じて、試験には、次を含める。 c) セキュリティの問題を見つけることに焦点を当てた、不正なインプットまたは予期しないインプットに対する悪用ケース試験。これには、全ての外部インターフェースおよびプロトコルに対する、手動の悪用ケース試験または自動化した悪用ケース試験および特殊な種類の悪用ケース試験を含める。例としては、ファジング、並びにネットワークトラフィックの負荷試験および容量試験がある。 d) システムへの全ての進入路およびシステムからの全ての退出路並びに一般的な脆弱性［弱いアクセスコントロールリスト（Access-Control-Lists、ACL）、露出ポートおよび昇格された権限で実行されているサービスを含むが、それらには限らない。］を特定するための攻撃対象領域試験 e) （該当する場合）ハードウェア、ホスト、インターフェースまたはソフトウェアアイテムの既知の脆弱性を検出することに焦点を当てた、“クローズドボックス型”の既知の脆弱性スキャン f) ソフトウェアとともに用いるためにサードパーティの供給者から供給された組込み用ファームウェアを含む、全てのバイナリー実行ファイルに対するソフトウェアコンポジション解析。

			この解析は、次を検出するために用いることが可能である。 1) ソフトウェアアイテムの既知の脆弱性 2) 脆弱なライブラリーへのリンク 3) セキュリティルールの違反 4) 脆弱性につながる可能性があるコンパイラー設定 5) 対象のソフトウェアとソフトウェア部品表との比較 g) 例えば、ファジングのような動的セキュリティ試験。静的なコード解析では可視化できない欠陥を検出する。これには、ランタイムハンドルの解放失敗、メモリーリークおよび認証なしでの共有メモリーへのアクセスによるサービス妨害状況を含むが、それらには限らない。この試験は、ツールが利用可能な場合には適用する。
検証担当者	（IEC 81001-5-1 5.7.4 侵入試験） ソフトウェアのセキュリティ脆弱性を発見し悪用することに焦点を当てた試験を通じて、弱みを特定し特性を明確化する侵入試験の実施計画を「ソフトウェアシステム試験計画書」に文書化する。	「セキュリティ試験計画書」	
品質保証担当者	「セキュリティ試験計画書」をレビュする。	「セキュリティ試験計画書」	・検証戦略および試験手順の適切性を評価すること。
検証責任者	「セキュリティ試験計画書」の記載内容を確認し、承認する。	「セキュリティ試験計画書」	・「セキュリティ試験計画書」のレビュ記録を参照すること。

7.10.4 セキュリティ試験

実施者	実施内容	成果物	留意事項
設計開発担当者	下記のセキュリティ試験を実施する ・静的コード解析 ・動的解析 ・堅牢性試験 ・ソフトウェアコンポジション解析 ・ファジング	「セキュリティ試験記録」	・セキュリティコントロールが効果的に実施されていることを証明すること ・セキュリティの対応状況を評価することによって、既知の脆弱性（少なくとも重大（「致命的（Critical）」または「ハイリスク」）と判定された脆弱性）がコードに含まれていないことを証明すること

実施者	実施内容	成果物	留意事項
	等		・医療機器が使用される状況を考慮すること ・医療機器が他の機器・ネットワーク等に接続される環境を考慮すること
設計開発担当者	脆弱性スキャンを実施する	「セキュリティ試験記録」	・STIGs（Security Technical Implementation Guides）基準の達成度を確認すること ・CIS（Center for Internet Security）ベンチマーク等のセキュリティアセスメントツールを利用した定量的セキュリティ評価等を利用して可視化すること
設計開発担当者	必要に応じて侵入試験を実施する	「セキュリティ試験記録」	・意図する使用および予見可能な誤使用に起因する危険性を評価し、合理的に実行可能な限り除去した上でもなお、脆弱性が悪用された場合に予見可能な患者安全に対する影響が大きい製品の場合 ・経済産業省が策定した「情報セキュリティサービス基準」に適合したと認められた事業者の脆弱性診断サービス（IPA 提供）や同省に登録された登録認証機関による第三者試験を利用すること
設計開発リーダー	各「検証報告書」をレビュする。	「セキュリティ試験記録」	・検証報告書のレビュに関しては、MD-QMS-K4「設計管理規程」に従うこと
設計開発責任者	適切なレビュが完了していることを確認し、各「検証報告書」を承認する	「セキュリティ試験記録」	・検証報告書の承認に関しては、MD-QMS-K4「設計管理規程」に従うこと

7.10.5　ソフトウェアシステム試験記録（5.7.5）

役　割	実施内容	成果物	留意事項
検証担当者	「ソフトウェアシステム試験スクリプト」に従って、ソフトウェアシステム試験を実施し、テスト結果を「ソフトウェアシステム試験記録」に記載する。	「ソフトウェアシステム試験記録」	・「ソフトウェアシステム試験スクリプト」のコピーを用意し、「ソフトウェアシステム試験記録」とすること。 ・テスト結果が期待される結果と相違する場合、再試験を実施するために十分に詳細な情報を記入すること。 ・試験の再現性を支持するために、次を文書化しなくてはならない。 a) 要求されている動作および予想結果を示す試験項目手順への言及 b) 試験結果（合否および異常のリスト）

			c) 試験したソフトウェアのバージョン d) 関連するハードウェアおよびソフトウェアの試験構成 e) 関連する試験ツール f) 試験日 g) 試験の実施および試験結果の記録に責任を持つ人の特定
検証担当者	ソフトウェアシステム試験中に発見した異常を、ソフトウェア問題解決プロセスで処理する。（5.7.2）		・
検証責任者	「ソフトウェアシステム試験記録」を参照し、テスト結果を評価する。	・	・「ソフトウェア開発計画書」に則って障害対応を実施すること。 ・必要に応じて該当する成果物の変更を行うこと。
検証担当者	「ソフトウェアシステム試験記録」にソフトウェアシステム試験の実施者と実施日を記載する。	・	・
品質保証担当者	次のことを検証し、「ソフトウェアシステム試験検証記録」を作成する： 1) 全てのソフトウェア要求事項の試験が終了したか、またはその他の方法で検証されている 2) ソフトウェア要求事項と試験、またはその他の検証との間のトレーサビリティが記録されている 3) 試験結果が要求されている合否基準を満たしている。	・	・
品質保証担当者	「ソフトウェアシステム試験記録」をレビュし、レビュ結果を文書化する。	・	・
検証責任者	「ソフトウェアシステム試験記録」の記載内容を確認し、承認サインを記入する。	・	・「ソフトウェアシステム試験記録」のレビュ記録を参照すること。

7.10.6 変更後の再試験（5.7.3）

ソフトウェアを変更した場合には、以下を実施する。

役　割	実施内容	成果物	留意事項
検証担当者	ソフトウェアシステム試験の実施中に変更があった場合、次の処理をする。 a) 必要に応じた試験のやり直し、試験の修正および実施、又は追加試験の実施によって、変更が問題の訂正にどの程度有効かを検証する。 b) 副作用が発生しなかったことを示すための適切な試験を実施する。 c) 関連するリスクマネジメントアクティビティを実行する。		

検証担当者	必要に応じた試験のやり直し、試験の修正および実施、または追加試験の実施によって、変更が問題の訂正にどの程度有効かを検証する。		
検証担当者	副作用が発生しなかったことを示すための適切な試験を実施する。		
検証担当者	関連するリスクマネジメントアクティビティを実行する。		

7.10.7 ソフトウェアシステム試験の評価（5.7.4）

役　割	実施内容	成果物	留意事項
検証担当者	検証戦略および試験手順の適切性を評価する。		
検証担当者	次のことを検証する。 a) 全てのソフトウェア要求事項の試験が終了したか、又はその他の方法で検証された。 b) ソフトウェア要求事項と試験、又はその他の検証との間のトレーサビリティが記録されている。 c) 試験結果が要求されている合否基準を満たしている。		

7.11 トレーサビリティマトリックスの作成および更新（7.3.3）

役　割	実施内容	成果物	留意事項
設計開発担当者/検証担当者	トレーサビリティマトリックスを作成・更新する。	「トレーサビリティマトリックス」（MD-SW-21）	・クラス B、C の場合 ・「ソフトウェア要求トレーサビリティ」シートを記入し、製品要求とソフトウェア要求のトレーサビリティを文書化する。
設計開発担当者/検証担当者	「リスクマネジメントワークシート」を更新する。（7.3.3）	「リスクマネジメントワークシート」（MD-QMS-F505）	・クラス B、C の場合 ・次のソフトウェアに関連する事項のトレーサビリティについて、適宜文書化すること。 a) 危険状態からソフトウェアアイテムまで b) ソフトウェアアイテムから特定のソフトウェアの原因まで c) ソフトウェアの原因からリスクコントロール手段まで d) リスクコントロール手段からリスクコントロール手段の検証まで ・上記は「リスクマネジメント規程」（MD-QMS-K5）に従うこと。
品質保証担当者	トレーサビリティマトリックスをレビュし、レビュ結果を文書化する。	「トレーサビリティマトリックス」（MD-SW-21）	・

トレーサビリティマトリックスの記入要領

フェーズ	実施内容	留意事項
ソフトウェア要求分析	「トレーサビリティマトリックス」（MD-SW-21）を作成し、「ソフトウェア要求トレーサビリティ」シートを記入する。	
ソフトウェアアーキテクチャ仕様書設計	「ソフトウェアトレーサビリティ」シートの「概要設計」までの列を記入する。	
ソフトウェア詳細設計	「ソフトウェアトレーサビリティ」シートの「詳細設計」までの列を記入する。	
ソフトウェアユニットの実装	「ソフトウェアトレーサビリティ」シートの「コード」までの列を記入する。	
ソフトウェアユニットテスト	「ソフトウェアトレーサビリティ」シートの「単体」列および「ソフトウェアトレーサビリティ（詳細設計対ユニットテスト）」シートを記入する。	
ソフトウェア結合試験	「ソフトウェアトレーサビリティ」シートの「結合」列および「ソフトウェアトレーサビリティ（概要設計対都合テスト）」シートを記入する。	

役　割	実施内容	成果物	留意事項
設計開発担当者	検証結果を「ソフトウェア問題報告書」に記録する。	「ソフトウェア問題報告書」（MD-SW-90）	・「ソフトウェア結合試験記録」に次を含めること。（9.8） a) 試験結果 b) 発見した異常 c) 試験したソフトウェアのバージョン d) 関連するハードウェアおよびソフトウェアテスト構成 e) 関連試験ツール f) 試験実施日 g) 試験者の識別

11. 参考

1) 「ソフトウェア開発規程」（MD-SW-A1）
2) 「設計管理規程」（MD-QMS-K4）
3) 「ユーザビリティエンジニアリング規程」（MD-QMS-K4U）
4) 「リスクマネジメント規程」（MD-QMS-K5）

12. 付則

本文書の改廃は、○○○が立案し、×××の承認を得る。

202X 年 00 月 00 日　発効