- 人的故障の可能性は、このアプリケーションにおけるソフトウェア故障の可能性よりも非常に大きかった（大きく見えた）。人間は、誤字、シートの間違った版の使用などをする可能性がある。この例における“ソフトウェア検証”により、プロセスがさらにヒューマンエラーの影響を受けにくくなった。
- この例は、日常的に使用するオフィス生産性ツールでさえもいかに構成管理が重要かを強調している。

注 – これは、あまりうまく処理されなかった実例にもとづいている。事実、スプレッドシートのバージョニングにヒューマンエラーがあった。予期せず、複数の PC の Excel 設定が異なり、それに連動したフォントの版が問題となり、ハードコピーの結果が同一にならなかった（プリンタのフォントもプリンタが異なると問題になりうる）。検証は不要であるとほとんど看過される一見単純なスプレッドシートが、実際には、メッセージ翻訳の破損で問題となった。

例 8：パラメトリック滅菌装置

メアリーは、彼女の勤めるオールウェイズセーフ・メディカルデバイスカンパニー 用にカスタム開発される新しい自動滅菌システムの検証の取り組みを率いる業務を行ってきた。

プロセスの定義

メアリーは、まず、彼女の会社の工場に導入しようとしているこの 100%ETO（エチレンオキサイド）滅菌プロセスについて彼女が知っていることの定義及び文書化を開始する。

- 医療機器を手動で滅菌装置に入れる。
- シリアルナンバー、バッチ情報及び滅菌サイクル情報を DHR に転送する。
- このプロセスには、パラメトリックリリースのための滅菌サイクル変数評価が含まれている。
- 自動滅菌システムのソフトウェアは、滅菌サイクル活動を制御する。
- サイクル完了後、医療機器を手動で取り出し、脱気室に移動する。

プロセスリスクの分析

メアリーは、このプロセスのリスクを非常に懸念している。このプロセスが故障すれば、次のような重大な結果が生じうる。

1. 医療機器の滅菌不良。この故障の結果、未滅菌製品の使用による感染症のため、重大な損傷又は死亡が発生する可能性がある。
2. 医療機器の履歴情報及び製品のトレーサビリティ紛失。
3. 製造施設若しくは環境、又はその両方への有害化学物質の放出。この故障の結果、滅菌装置のオペレータ又は近隣住民の重大な損傷又は死亡が発生する可能性がある。

そこで、メアリーは、このようなリスクを軽減するためにどのリスクコントロール手段を設定し、検証しなければならないかを考える。メアリーは、正確な温度及び相対湿度で適量のガスが、適当な時間使用されるパラメトリック滅菌技法を使用して、リスクを制御できると考えた。さらに、滅菌装置のデータの適切なパラメトリック値を手動で確認して、独自に滅菌が十分であるかを確認する。最後に、彼女は、施設への化学物質の漏れを制御するために、二重安全装置のシャットダウン及び密封構造を採用しなければならないと考えた。

これらのリスクコントロールを実施しても、複数のシステム故障が同時に発生し、医療機器が滅菌されない可能性がある。しかし、これが発生した場合の影響は大きいため、メアリーはこのプロセスの残留リスクは高いと考える。彼女は、このリスクは大きなリスクに変わるため、厳格な検証が適当と考える。

ソフトウェアの目的と意図の定義

メアリーは、このシステムでソフトウェアをどのように使用するのかを詳しく理解したい。まず、彼女は、このソフトウェアが何をすべきかを考える。この場合、ソフトウェアは、DHR に入力する情報の記録及びパラメトリックリリースのための滅菌値の分析など、100% ETO 滅菌槽を用いた医療機器滅菌プロセスを制御する。この新しい滅菌装置は、現行のシステムより大きなバッチを収容できるために購入した。この点は、現在の製品の需要を満たすためには非常に重要である。滅菌のオペレータが QA とともにこのシステムを使用し、医療機器のリリースの受容可能性を判定する。メアリーは、これは、滅菌サイクル中の滅菌槽のリアルタイム制御及び監視並びにデータベースへの情報保管を通じて実行されることを理解する。メアリーは、このシステムが滅菌施設の中に設置され、システムに必要な保守のために使用しないのは通常週 1 日だと知り喜んでいる。

メアリーは、このソフトウェアは、医療機器を手動で滅菌槽に入れる点から手動で滅菌槽から取り出す点までのすべての側面を自動化すると判断する。

メアリーは、目的と意図を次の通り記録する。

この滅菌ソフトウェアは、滅菌プロセスを制御及び監視し、データをプロセスから滅菌済み医療機器の DHR へ転送し、パラメトリックリリースの滅菌サイクル変数を評価する。

検証プランニング

ここで、メアリーは、ソフトウェアが何をするのかを理解したため、高レベルの検証プランニングを作成する準備が整った。彼女は、後で詳細を付け加える必要があることを知っているが、今、検証プランニングを開始し、十分に情報を得た状態でソフトウェアの障害リスクを特定し、それを使用して計画を完了したい。

初期に高い残留リスクが特定されたため、メアリーは検証の取り組みにおいて詳細及び形式を準備する必要があると考える。彼女は、詳細の文書化には高レベルの厳格さを適用し、小規模の取り組みでよくあるように文書を統合するのではなく、ほとんどの文書を独立した文書にしたいと考える。このシステムは高リスクであるため、医療機器のソフトウェア開発と同程度の厳格さで開発することを決定する。その結果、彼

女は、ライフサイクル制御法として、医療機器のソフトウェアに、つまりソフトウェアライフサイクルプロセス（IEC 62304:2006）に従うことを決定し、ソフトウェアリスクマネジメントの指針として AAMI TIR32：医療機器ソフトウェアリスクマネジメントを参照する。さらに、開発の取り組みにソフトウェア障害の木分析の適用を決定し、すべての危害の原因を考慮するようにする。また、彼女は、ユーザービジネスプロセス要求事項及びソフトウェア要求事項を正式に定義及び文書化することも決定する。特に懸念となる機能は特別に識別する。さらにメアリーは正式なソフトウェア要求事項の審査も計画する。QA、滅菌技術者及び滅菌マネージャーの承認が必要である。このシステムの重大度及びリスクから考えて、検証レポートの最終承認には、上級管理職のメンバーも加える。

ソフトウェア要求事項の定義

ここでメアリーは、ソフトウェア要求事項の定義を作成する。彼女は、ソフトウェア要求事項では、警告、エラーの取り扱い及びメッセージ、変数設定の確認、DHR システムのインターフェース、センサー制御及び監視、動作制御及び監視を取り扱わなければならないと決定する。

このシステムは電子データを管理するため、メアリーは、21 CFR 11 の文言から標準的要求事項文書も含める。

信頼の確立及びソフトウェアの制御

すべてを内部で実施するために納入業者の活動が発生する必要がないため、オールウェイズセーフの内部開発制御手順をもとに、メアリーは開発ライフサイクルを通じて内部制御を使用する。

ソフトウェアと他のシステムとの境界の定義

メアリーは、次に、他にどのシステムが新しい滅菌装置とインターフェースする必要があるかを考える。彼女は、唯一のインターフェースは、滅菌サイクル中に発生したデータを保管するオールウェイズセーフの既存の DHR データベースシステムであると判断する。

ソフトウェアの障害リスク分析

メアリーは、既に自動化するビジネスプロセスは高リスクであると判断したが、まだ、ソフトウェアの障害のリスクを分析する必要がある。メアリーは、AAMI TIR を参照

してこの活動に定量的リスクモデルを選択する。彼女は新しいシステムに次の通り順位をつけた。

- このシステムの障害により死亡又は重大な損傷が生じうるため、メアリーは“重大さ”を高い（10）と評価する。
- ソフトウェア自体が滅菌の受容可能性を決定しているため、ソフトウェア自体の障害が危害をもたらす可能性があり、彼女は“可能性”を高い（10）と評価する。
- 彼女はリスクスコアを 20 と計算し、これは高リスクに分類される。

高リスク分類には、厳格な検証方法が適用される。滅菌装置自体が医療機器であるかのように厳格かつ包括的にこの方法を遵守する。

この自動システムの残留リスクは、軽減により合理的に達成可能なできるだけ低い（ALARP）。このシステムによる危害の重大さにより、滅菌は本質的に高リスクのプロセスである。AAMI TIR 32 を使用したリスクに関する追加活動も実施する。

検証プランニングの終了

ここで、メアリーはソフトウェア要求事項の定義を完了し、実施アプローチを決定し、ソフトウェアのリスクを分析したため、検証プランニング終了に十分な情報を得ている。

検証プランニングの初期で、メアリーは既にリスクマネジメントに対する厳格なアプローチを採用すべきと決定し、既に検証の取り組みを高度に正式な方法で取り扱う計画を立てていた。

したがって、彼女は使用予定の AAMI TIR32:2004 で特定されるリスクマネジメントツールを説明する。

リスクマネジメントツール

- ソフトウェア障害の木分析
- リスクマネジメント計画
- 製造/ビジネスプロセスにおけるリスクコントロール手段の特定
- ソフトウェアの障害分析（リスク分析）

メアリーは、次に、ソフトウェアの設計、開発及び設定段階でどのようにソフトウェアに対する信頼を確立するかを考える。彼女は、既に、ライフサイクル制御に IEC 62304 規格の採用を決定している。彼女はここで、このソフトウェアが設計、開発及び設定段階で適切に開発されたことを示す他の関連するツールを特定する。

設計、開発及び設定ツール

- IEC 62304：2006
- アーキテクチャの文書化及び審査
- 設計仕様
- ソフトウェアの詳細の設計及び審査
- ソフトウェアコーディング規約
- トレーサビリティマトリックス
- ソフトウェアシステム設計におけるリスクコントロール手段の特定
- コード審査/コード検証
- 開発及び設計審査

メアリーは、この新しいシステムを広範に検査する必要があると確信している。まず、彼女は、通常の単体テスト、統合テスト及びインターフェーステスト活動以外に正式な試験計画活動が必要と判断する。しかし、このシステムは、最終医療機器をリアルタイムでリリースするため、負荷テスト、性能テスト、及び入力テストを広範に組み合わせて可能な限り多くの操作状況を作り出して、システムの制限を広げなければならないと判断する。

検査ツール

- テスト計画
- 単体テスト
- 統合テスト
- インターフェーステスト
- 回帰テスト（必要な場合）
- ソフトウェアシステムテスト
- 頑健性（負荷）テスト
- 入力テストの組み合わせ
- 性能テスト

最後に、このシステムは、生産環境において完全に実施されるまで完了しないため、メアリーは、導入段階で検討したい検証活動に関心を移す。彼女は、システムの適切な文書化及びユーザーに対する正確な使用についての十分な教育訓練を確実にしたい。また、システムを意図通りに確実に設置したい。そこで、彼女は導入段階の検証プランニングに次の計画を追加する。

導入ツール

- 使用手順の審査
- 内部教育訓練
- 据付時適格性確認
- 操作及び性能の適格性確認
- オペレータの認証

保守計画

メアリーは、残留リスクリスクが高いため、保守について懸念している。彼女は、システム導入以後にソフトウェアの品質を保証するために、ユーザーの教育訓練、システム監視手法、システム出力の正確さの確認及び欠陥の報告の評価などいくつかの保守活動を計画する。また、彼女は、ソフトウェア保守活動に加え、校正など、ハードウェアの保守活動が実施されていることを確認する。

廃用活動

旧システムで作成したデータを DHR 用に記録保管する必要があるが、新しい形式とは互換性がなかったため、メアリーは旧システムの廃用に苦労した。このシステムは、普遍的なデータ形式を採用しており、新システムへの世代交代時に残存データの移動を柔軟に実施できる。

例 9：不適合材料報告システム（NCMRS）– システム全体のアップグレード

アドバンスドメディカルスペシャリティーズコーポレーション（架空の企業）は、不適合材料報告システム（NCMRS）のソフトウェアをアップグレードしている。これは市販のソフトウェア部品ケージであるが、アドバンスドメディカルは、過去の大規模なリリース時にアップグレード をしなかったため、大規模なリリース 2 回分の遅れがある。この会社では現在第 2 版を使用しているが、最新の第 4 版がリリースされている。現行のソフトウェア保守契約を維持するために、アドバンスドメディカルはアップグレードしなければならない。NCMRS-Pro（ソフトウェア）の第 4 版は、現在使用している V2 に比べ大きく変化している。特に、この製品は、通常のクライアント/サーバーアプリケーションからウェブベースのアプリケーションにプラットフォームを変更した。新しいソフトウェアには重大な特性及び機能も入っている。ビジネスプロセスオーナー兼プロジェクトマネージャーはフランクである。フランクは、既存のソフトウェア及びプロセスについて、新しい要求事項はないが、新しいソフトウェアの特性を利用したいと考えている。

フランクは、規制グループに相談し、ERP システムと NCMRS システム間の現行のインターフェースには変更がなくそのままであると判断したが、新版では ERP システムにデータを書き戻すことができ、この拡大インターフェースを検証時に詳細に調べなければならないと認識する。フランク、製造品質技術者及び規制チームが検証の取り組みの適用範囲決定を検討し始める。

プロセスの定義

フランクは、現行の手動プロセスを分析し、新しいソフトウェアによりワークフローのどの要素を自動化するかを決定する。

1) 不適合材料又は製品が発生する可能性を認識（適用範囲外）
2) 不適合材料及びその発見にまつわる状況に関する情報を入力（適用範囲内）
3) その材料の適切な識別、評価、調査及び処分を可能にする情報の経路選択（適用範囲内）
4) 重要な利害関係者並びに財務、購入、計画及び日程計画を適切に取り扱うための他のコンピュータシステムに情報を伝達（適用範囲内）.
5) その材料の物理的処分（適用範囲外）。ただし、処分に関するデータはこのシステムに記録する。

プロセスリスクの分析

フランクは、このプロセス及び補助となるソフトウェア にリスクがあると気づいている。このプロセスで故障が発生すれば、次のような深刻な結果が生じる可能性がある。

- 不注意により不適合材料が製造フロアにリリースされる。
- 不注意により不適合材料が市場にリリースされる。
- スクラップ、作り直しなどによりコスト又は製造が増加するなど。

フランクとチームは、以上のリスクを軽減するためにどのリスクコントロール手段が実施されているかを考える。

- 不適合材料の検知、隔離、制御及び修正の手順制御
- プロセスが適切に制御されていない可能性があるという開発の傾向を特定するための、SPC データ及びその他の手段の管理及び品質審査
- 手順の遵守に関するオペレータの継続的訓練
- 製造プロセス特有でない問題があることを示す材料の使用を特定するための財務報告書

以上のリスクコントロールを実施しても、複数のシステム障害が同時に発生すると、不適合材料又は製品を適切に制御できなくなる。しかし、この種類の障害が発生した場合、品質、規制及び財政上の影響が出る可能性があるため、フランクは、プロセスリスクのために厳格な信頼確立活動を実施し、ソフトウェアの正確な作動及び意図する使用の適合を確実にする必要があると判断する。

ソフトウェアの目的と意図の定義

フランク社、ソフトウェアのアップグレードがどのように彼の会社のユーザー及び組織に影響を与えるかについて詳細に理解したい。フランクは、このソフトウェアは基本的には自動問題追跡及び管理ツールだと結論づける。規格のツール、装置及びその他の手段を用いて業務を行う製造要員は、不適合材料及び製品を認識し、隔離する責任を負う。問題が認識されたら、その状況の詳細をソフトウェアに入力する。次に、ソフトウェアは、ワークフロー、割り当て及び通知を管理し問題を解決し、材料及び製品の処分に必要な様々な活動を記録する。ソフトウェアのアップグレードは、このプロセスを簡素化、効率化するとともに、品質チームに対しより強力なデータ分析及び動向のツールを提供し、品質の問題を見極められるようにしなければならない。フランクは、アップグレードが必要なプロセスの変更は主にワークフロー及び情報伝達であると理解する。ソフトウェア自体は財務上の決定を行わず、他の結果を独自で決定しないが、システムと相互にかかわる人間による決定を受け、記録する。

フランクは、このソフトウェアは、材料の処分の審査及び電子署名を含む不適合プロセスのワークフローの部分を自動化すると決定する。関連する規制には、21 CFR 820.90 がある。また、電子システムであるため、21 CFR Part 11 の条件は閉鎖システム及び電子署名にも適用される。

チームが作成するソフトウェアの目的と意図は次の通りである。

NCMRS ソフトウェアの意図は、21 CFR 820.90 に基づいた不適合材料及び製品の処理の支援である。このシステムは、SOP に定められたプロセスステップの記録に使用し、実行プロセス、実行した日時及び担当者並びに各ステップの結果を記録する。このシステムにより品質モニタリング及び改善活動においてもデータを利用できる。

ソフトウェアと他のシステムとの境界の定義

NCMRS ソフトウェアには2つのインターフェースがある。主インターフェースはERP システムで、副インターフェースは会社の HR システムである。主インターフェースは、1 日 2 回のバッチ処理が予定されており、最終製品、仕掛品、 部品表（BOM）及び工程表（BOO）を更新するよう設計されている。インターフェースは、品質保持、材料の処分や他のトランザクション情報についてのNCMR データをERP に提供する。副インターフェースは HR システムからの片方向性で、日程計画及び割当て目的でNCMR 従業員データを更新する。

初回検証プランニング

フランクは、NCMR プロセス及びソフトウェアを十分に理解し、高レベルの検証プランニングを作成する自信を深めた。計画のプロセスで詳細を追加する。

このチームは、最も“付加価値が高く”、ソフトウェアがすべきことを最も適切に表した文書を特定する。これらの文書は、通常“要求事項”と言われるが、この文書自体は 通常の一連のユーザーの要求事項ではない。代わりに、ソフトウェアがどのように作動することが期待されているかを詳細に説明する。このように、自動及び手動検査の分析は、審査及び結果の点でより定性的になり、特定のユーザー要求事項が満たされない場合に個々のテストを見るのではなく、結果及びシステムが意図通りに作動しているかどうかを全体的に見ている。

この文書一式には次が含まれる。

1) ワークフロー/ビジネス規則文書。ソフトウェアのこの領域は設定可能であるため、チームは一連の望ましい設定を作成し、作業を記述する詳細なプロセスフロー及び論理図を作成する。

2) インターフェース文書。この文書は、ERP 及び HR システムから NCMRS システムへ移動するデータ要素並びにどのデータ要素がいつ NCMRS から ERP に移動するかを記述する。

3) データ移行文書。この一連の文書は、過去のどのデータをアップグレードされたシステムに移行するかを記述する。

4) 電子記録（パート 11）文書。このシステムは電子記録及び署名を管理するため、フランクは検証、安全、監査証跡及び電子署名に関する 21 CFR 11 の文言からの標準要求事項文書を含めた。

検証プランニングには、以上の各文書の審査及び承認結果が含まれる。QA、製造エンジニアリング部門及び情報システムグループの承認が必要になる。このシステムは、重要かつリスクがあるため、検証報告の最終承認には、上級管理職全員が参加する。

ソフトウェア使用の要求事項の定義

フランクとチームは、納入業者が支給したシステム文書及び既存のインターフェースに関する過去の文書にもとづいて、上述の文書をまとめ始める。

信頼の確立及びソフトウェアの制御

フランクは、このソフトウェア及びその納入業者と良好な関係にある。フランクは、ソフトウェアに対する信頼確立のためにチームが使用する主な取り組みをあげる。

1) 納入業者は、アドバンスドメディカルの社内方針及び手順に従い、認定資格を所有している。これまでの監査で、この納入業者には適当な品質システム及び SDLC があるとわかっている。この納入業者は市販のソフトウェアを製造しており、アドバンスドメディカル の意図する使用に類似した使用が、規制産業で使用されてきた経緯がある。納入業者は、定期的に監査を受け、認定資格を維持する。

2) アドバンスドメディカルはある納入業者が供給する自動検査ツールを使用し、ソフトウェアが適切にインストールされ、テストスイートの境界内で機能することを検証する。このツールは、数時間で 8,000 を超えるトランザクションを実施できる。しかし、この企業が取り入れようとする特定の設定オプションは試験しない。

3) チームは、実際の不適合報告の統計学的に有意なサンプリングの並行処理が含まれる紙媒体の付属検査計画を作成する。出力の精確さ、データの完全性及び手順の遵守を確認する。

4) チームは、過去のデータの完全性が維持されるよう、サンプリング手法を用いて既存のシステム記録のデータ変換及び移行を検証する。記録の数値は 100%転換の検証に用いる。

5) データ移行の完全性及び精確さを測定するために、サンプリング手法を用いてデータインターフェースを検証する。

ソフトウェアの障害リスク分析

フランクは AAMI TIR を参考に、必要とされる検証の厳格さを決定する。ソフトウェアの障害により、電子記録の紛失、破損 又は誤った取り扱いが発生する可能性がある。以上のリスクの軽減は、納入業者の内部品質システム、ソフトウェアの据付時適格性確認（自動検査ツール）及び付属ユースケーステスト及び検証で制御されている。このシステムの残留リスクは、下流のプロセス制御があるため、合理的に達成可能なできるだけ低い（ALARP）とみなされる。

最終検証プランニング

この決定は、非常に厳格な検証方法が適用されることを示唆している。使用する方法から、合理的な程度までソフトウェアが意図した通り作動すると保証される。チームは、彼らがこのシステムの要求事項を適切に定義し、実施アプローチを決定し、ソフトウェアのリスクを分析し、詳細な検証プランニングを進めるために十分な情報が得られたと結論づけた。

大規模な試験については、この意図する使用に妥当であるとチームが判断した自動テストスイートを用いて実施する。製造フロアのビジネスケースを使用して、付属のユースケーステストを追加的に実施した。以上の試験の目的は、a）プロセスが意図した通りに作動することを検証し、b）ユーザーの受入及び教育訓練を加速し、c）設定変更がソフトウェアに悪影響を及ぼさないことを検証することである。付属の試験は、過去に監査で検証した納入業者の内部システムの試験にかわるものではない。自動試験が問題なく終了すれば、ソフトウェアが適切にインストールされ、機能的に受入可能であることを示す。

このチームは、残りのインストール、設定、試験、検証およびお検証の取り組みのために AAMI TIR から以下の“ツール”を選択する。

設計、開発及び設定ツール

- アーキテクチャの文書化及び審査
- ソフトウェアシステム設計内のリスクコントロール手段の特定
- 構造設計審査

- 納入業者の“既知の問題”リストの審査
- 納入業者ベースシステムの検証文書化の審査
- “アウトオブザボックス”ソフトウェアワークフロープロセスダイアグラムの審査
- “アウトオブザボックス”標準報告ライブラリの審査
- 標準ワークフロー及びビジネス規則の構造変更のギャップ分析

試験ツール

- テスト計画
- 納入業者が供給する、インストール、検証及び資格認定用自動試験ツールの記述及び結果
- インストール及び性能検査（自動テストスイートの一部）
- 人工的に作成したテストケースではなく実際の不適合記録を用いた、設定変更に関するユースケーステスト
- 移行データ検証用サンプリング計画
- オペレーショナルインターフェースを検証するシステムチェック

導入ツール

- 使用手順の審査
- 内部教育訓練
- オペレータの認証

保守計画

フランクは、システム導入後に使用中のソフトウェアの品質を維持するために、ユーザーの教育訓練、システムモニタリング手法、システム出力の定期的監査及び内部及び納入業者への欠陥報告など複数の保守活動を使用する計画を立てている。フランクは、納入業者との接点を確立しており、バグの通知、保守のリリース及びその他の連絡がアドバンスドメディカルのソフトウェアの保守担当者に入ってくる。

廃用活動

フランクは、現行のシステムを切り替え後も利用して、処理量及び結果を比較し、性能の指標を作成しようと計画している。新しいシステムが６ヵ月間問題なく作動した後に、旧システムを完全に停止する。

例 10：不適合材料報告（NCMR）審査委員会会議日程計画ソフトウェア

従業員 1000 人の企業が、不適合材料報告（NCMR）審査活動に必要な会議日程計画を電子的に補助してもらおうと、新しいソフトウェアソリューションを試すことに決定した。この自動化を実行するために指名されたプロジェクトチームは、新しいソフトウェアプログラムは市販されたばかりであると聞く。納入業者は、このソフトウェアで他のコンピュータ化システムインターフェースからのデータにもとづいて会議の日程を作成できると主張する。チームは、妥当性が確認されている自社の NCMR データベースシステムから NCMR データを収集できれば、このソフトウェアは NCMR 審査委員会の日程計画に役立つと判断する。

プロセスの定義

チームは NCMR 審査委員会会議の日程計画プロセスについて議論し、彼らの NCMR 処理手順を検討する。この結果、以下のプロセスが定義される。

1. 不適合が特定されたら、関連する材料にラベルを添付し、隔離し、妥当性が確認された NCMR データベースに記録する。
2. 不適合に関するすべての調査結果及び推奨される処分活動を審査するための会議を毎週開く。
3. 会議では、審査の準備が整った NCMR リスト並びに結果報告のために出席し、処分活動及び承認に参加すべき個人を特定する。
4. 審査委員会の会議前日、参加が必要な人に会議要請書が送られる。要請書には議論すべき NCMR のリストが記載されている。

プロセスリスク分析

ブレーンストーム活動を通じて、チームはこのプロセスで故障が発生した場合、どのような危害が生じうるかを評価する。

- 会議要請書が送付されない。
- 会議要請書が適当な時間に送付されない。
- 不適当な人物に参加を要請する。
- 審査用に不適当な NCMR リストが特定される。

リリースされた NCMR 処理手順では NCMR 処理マネージャーを一人、選任する必要があることがわかった。この人物は、すべての NCMR を適時処理し、妥当性が確認された NCMR データベースで見つかったデータから NCMR 処理の指標を公表する。特定されたすべてのケースにおける会議日程計画ソフトウェアによる危害は、審査委員会会議の効率の低下及び NCMR 処理マネージャーの時間的負担の増大であった。

したがって、プロセス障害リスク分析で、規制リスク、環境リスク及び人への危害のリスクは低いと判定した。

意図する使用の定義

ソフトウェア使用、規制上の利用及び境界の目的と意図を次の通り定義する。

- ソフトウェアの使用
  - 誰が – ソフトウェアは、主にNCMR処理マネージャーが使用する。
  - 何を – ソフトウェアは、その週の会議に参加すべき個人に会議の電子招待状を自動的に送付する。
  - いつ – ソフトウェアは、NCMR会議を計画すべき時に使用する。
  - どこで – 参加者が会議の会場付近に住んでいる場合、ソフトウェアはLAN上でのみ使用すればよい。
  - どのように – ソフトウェアはNCMR審査委員会が審査すべき公開されたNCMRのリストを検索する。NCMR処理マネージャーは、次の会議で審査すべきNCMRを特定する。ソフトウェアは、次に、NCMR処理マネージャーが作成した表を用いて、特定の会議に参加すべき個人を特定する。会議の日付はNCMR処理マネージャーが特定し、この日の前日にソフトウェアが参加すべき参加者に会議の電子招待状を送付する。
  - なぜ – ソフトウェアは、毎週のNCMR審査委員会会議に参加すべき個人への適時通知を改善するために使用する。
- 境界：
  このソフトウェアの境界は、NCMRデータベースとのインターフェース及びユーザーとのGUIインターフェースである。
- 規制上の使用：
  このソフトウェアは規制上の要求事項遵守を証明するための情報を保存しない。NCMR又はNCMRの処理に関する機器履歴簿情報はすべて 、紙又は妥当性が確認されたNCMRデータベースで記録する。

この目的と意図の作成及び審査後、このソフトウェアは、規制で求められる活動を自動化せず、規制で求められる品質記録を作成しないことがわかった。このソフトウェアは、規制活動（NCMRプロセス）の一部である会議を*補助する*が、規制活動を自動化するわけではない。その結果、チームは、上にあげた意図する使用を記録し、正式な検証は必要でないと明確に述べた。しかし、チームは、保守期間に使用法にわずかな変更があっても、もとの検証の決定に重大な影響を与えうると認識する。例えば、ソフトウェアが議事録保管に使用された場合、又は、規制当局の捜査官により審査会

議に参加した個人のリスト作成に使用された場合、もとの“適用範囲外”の決定が影響を受ける場合がある。したがって、チームは、彼らの品質システム手順を更新し、この意図する使用の定期的な評価及び関連プロセス変更の結果を反映しなければならない。

ツールボックスの使用

ツールボックスから次のツールを使用する。

- 開発-定義
  - プロセス要求事項の定義
  - プロセス障害リスク分析
  - 意図する使用の定義
- 保守
  - 保守計画

考察

このソフトウェアが自動化する特定の使用及び活動の境界を明確にした結果、チームは、このソフトウェアが規制プロセスのソフトウェアの定義を満たしていないために妥当性を確認する必要はないと適切に表明できた。ソフトウェアの実際の使用が、意図する使用の定義に完全に該当するには、この種のソフトウェアの識別を慎重に行わなければならない。また、ライフサイクルの保守期間には、意図する使用は容易に変更され、ソフトウェアの変更なしに行われることもある。このために、保守計画は企業が使用するソフトウェアの適切な制御において重要な役割を果たしている。

例 11：認定納入業者リストシステム

アクメコーポレーションはクラス II の医療機器製造業者である。この企業は、手動の手順で認定納入業者リスト（AVL）を保守してきた。この企業は、ある納入業者が特定の部品供給の認定があるか否かを確認するプロセスを自動化するために AVL システムを開発したい。新しい AVL システムのプロジェクトマネージャーであるジャックは、AVL プロセスが Part 820.50（3）によって規制されたプロセスであると判断する。

820.50 購買制御

各製造業者は、すべての購買した、又はその他の方法で受け取った製品及びサービスが規定した要求事項に適合することを保証する手順を確立及び保守しなければならない。

（3）受入可能な供給者、請負業者及びコンサルタントの記録を作成し、保管する。

従って、導入予定の AVL システムはソフトウェア検証の要求事項が適用される。

プロセスの定義

AVL システム開発の要求事項及びリスクの理解を深めるために、ジャックは、関連するビジネスプロセスを次の通り定義する。

1. エンジニアリング部門が新しい納入業者の認定を求める場合、その納入業者の部品のサンプルを品質グループに提出し、資格認定を受ける。
2. 納入業者の部品のサンプルの資格認定後、品質グループは購買グループに、その納入業者の名称及び認定部品番号及び記述の認定納入業者リスト入力及び購買グループにおける紙媒体での保管を承認する電子メールを送付する。
3. 購買グループは、手動で納入業者の名称が手書きの AVL に正確に追加されたことを確認する。
4. 購買グループが部品を発注するときは、その納入業者が認定を受けており、請求した部品の供給許可を得ているか AVL を参照する。

プロセスリスクの分析

ジャックは、次に、現行のプロセスで発生しうる問題について考える。彼は、このプロセスが故障した場合、未認定の納入業者に部品を注文する可能性があると考えた。これは、非認定納入業者が何らかの理由で認定納入業者リストに追加されている場合

と、購買グループが部品発注前に認定納入業者リストを確認し忘れた場合に発生しうる。

ジャックは、次に、以上のリスクを軽減するためにどのようなリスクコントロール手段が実施されているかを考える。ジャックは、購買グループが納入業者の名称が正確に認定納入業者リストに追加されているかを手動で確認し、リストへのアクセスを許可された従業員に制限する手順を実施していることを知る。さらに、彼は、現行の購買手順では、購入者が発注書を出す前に認定納入業者リストを確認したことを示す署名が必要であることを知る。認定納入業者に発注したかどうかの確認は、納入業者リストを受け取った部品と照合する受入検査で実施する。以上のリスクコントロール手段に基づき、ジャックは、残留リスクは低いと判断する。したがって、新しい AVL システムは恐らく低リスクシステムであろうと考える。

意図する使用の定義

ここで、ジャックは自動化すべきビジネスプロセスを理解しており、導入予定の新しい AVL システムの目的と意図を作成する準備が整った。

彼は、次の通り記載する。

AVL システムは、部品を認定納入業者のみに発注するよう電子 AVL による納入業者及び部品の照合を自動化する。新しいシステムは、既存の PO システムに接続した AVL データベースを採用し、本社のアクメコーポレーション購買グループが納入業者資格認定プロセスに使用し、購入担当者が PO 作成プロセスで使用する。

ジャックは、AVL システムがインターフェースする他のシステム及びプロセスを考え、新システムの境界を明確にするために文書に文言を追加した。

購入プロセスは、AVL システムが自動化したプロセスとインターフェースする。インターフェースは、発注書に記載された納入業者の状態の AVL データベースでの検索になる。購入プロセスは AVL のデータの正確さを確認するのではなく、納入業者評価プロセスとはインターフェースしない。

最後に、ジャックは、導入予定のシステムが遵守すべき FDA 規則について考える。彼は、この重要な事実を反映するために、文章にに一言付け加える。

導入予定のシステムには、21 CFR 11 の要求事項に従い保護すべき電子記録が入っている。これら記録の従前規則は 21 CFR 820.50（3）である。

検証プランニング

ここで、ジャックは自動化すべきビジネスプロセスを理解しており、新システムの目的と意図を決定しており、次に、高レベルの検証プランニングを作成する準備が整った。彼は、後日計画の詳細を肉付けするが、必要な検証の取り組みのレベルを特定できるよう、検証プランニングを今開始したい。

これより前に、ジャックは既存の AVL プロセスのプロセス残留リスクは低いと判断した。したがって、彼は、この検証の取り組みでは多くの詳細又は手続きは不要であると考える。彼は、新システムのユーザービジネスプロセス要求事項及びソフトウェア要求事項の定義が重要であると理解している。しかし、このシステムは低リスクであるため、それぞれ別の署名付文書を作成する必要はない。したがって、彼は、表形式を用いて、ビジネスプロセス要求事項、ソフトウェア要求事項に加えて彼の検査計画も単一文書にすることを決定する。

さらに、このシステムは非常にリスクが低いため、ジャックは、この検証の取り組みには広範な経営者の審査は不要と判断する。彼は、供給者開発マネージャー及び QA 代表者の承認で十分であるとの結論を出した。しかし、ユーザーの要求事項が正確であると確信するにはこの購買グループの代表の確認も必要であると考える。

以上の決定に基づき、ジャックは検証プランニングの作成を開始する。アクメコーポレーションには、検証プランニング用の標準様式がある。検証プランニングには定義されていない項があり、ジャックが初回のシステム設計の承認後に計画を更新する。

ソフトウェア要求事項の定義

ジャックは、ソフトウェア要求事項を作成する。彼は、ソフトウェア要求事項には AVL プロセス／システムがすべきこと、AVL システムと購買システムのインターフェースの仕様、データ辞書及びシステムが取り扱えるべき有効な問い合わせの例を含めるべきだと決定する。

このシステムは、必要な電子記録を支援するため、ジャックは、21 CFR 11 の文言からの標準要求事項文書も、何が“電子記録”かについての詳細なリストとともに入れる。

ソフトウェアと他のシステムとの境界の定義

ジャックは、次に、新しい AVL システムがインターフェースすべき他のシステムについて考える。 彼は、単純な SQL クエリで AVL データベースの問い合わせができるアクメの既存の購買システムが唯一のインターフェースであると判断する。

信頼の確立及びソフトウェアの制御

ジャックは、新システム購入のためにどのアプローチ及びどの技術を使用するか決定しなければならない。ビジネス要求事項が非常に単純であり、処理量は少なく、低リスクシステムであることから、広範に使用されており、使いやすいデータベースアクセスシステムである Microsoft Access を用いてシステムを開発することに決定する。

Microsoft は、外部のソフトウェア開発者であるため、ジャックは、Microsoft Access に対する信頼を確立するためにどのような種類の活動を実施すべきか決定しなければならない。ジャックは、Microsoft Access は広く使用されているツールで、過去に、この製品に関する問題があれば迅速に特定され、インターネットの掲示板に公表されたことを述べた。AVL システムは低リスクであるという事実と合わせて、ジャックは、データベース開発者である Microsoft の納入業者監査は不要と判断する。

新システムには電子記録が入っているため、ジャックは、記録の妥当性を保証するために必要な制御を提供する第三者の“ラッパー”ソフトウェアを MS Access 周辺に使用する決定をした。

ソフトウェアの障害リスク分析

ジャックは、自動化すべきビジネスプロセスは低リスクと既に判断したが、まだ、ソフトウェア障害のリスクを分析する必要がある。彼は、この活動に定量的リスクモデル（1〜10 の尺度）を使用することを決定し、新システムに次の通り順位をつけた。

- ソフトウェアの障害により間接的な危害しか発生しないため、彼は、“重大さ”を中程度（6）と評価した。 彼の評価はプロセスの下流での制御にもとづいている。
- データベースの設計は非常に単純で、検査中に検出できない重大なバグが出てくる可能性は低いと考えたため、可能性は低い（1）と評価した。
- 合わせて考えると、低リスクに分類される。

したがって、ジャックは低リスクに適した検証業務を実施する。

検証プランニングの終了

ここで、ジャックはソフトウェアの要求事項を定義し、実施アプローチを決定し、ソフトウェアのリスクを分析し、検証プランニング終了に十分な情報を得ている。この時点で、ジャックは、このシステム、実施アプローチ及びソフトウェアリスクについて知っていることすべてに照らし合わせて、このシステムがその意図する使用に適しているという信頼を本当に確立できるのはどの検証活動であるか、自問する。

- これは、購入したデータベースツールで、リスクは相対的に低いため、彼が計画した検証活動は適切であるが、オペレーションシステム及びAccessのバージョン変更が適切に記録されるよう、環境要求事項に取り組まなければならない。彼は、検証プランニングを更新し、正式なソフトウェア構造制御を請求する。
- ジャックは、また、このシステムには従前規則（21 3146 CFR 820.50）で必要な電子記録が入っているため、電子記録の安全、精確さ、回復及び保存を制御する必要があると理解する。彼は、ソフトウェア要求事項に文言を加え、以上の点に言及し、テスト計画に入れるようにする。
- 次に、ジャックは、第三者によるこのシステムの開発方法について考え、開発者が、カスタマイゼーション、入力、インターフェース、データ保存及び出力の要求事項を正確に伝えているかを懸念する。このシステムは既存の他のシステムからの入力に依存しているため、彼は、検証プランニングの重要な活動としてインターフェーステスト及び統合システムテストを追加し、開発者の業務の精確さを確認する。

最後に、彼は、開発中の開発者による適切な版制御の継続を確認したいため、“ソフトウェア版制御”を必要な活動として彼の検証プランニングに追加する。

したがって、ジャックの批判的思考により、残りの開発及び検証の取り組みには、次の“ツール”が含まれる。

設計、開発及び設定ツール

- ソフトウェアアーキテクチャの文書化及び審査
- トレーサビリティマトリックス（要求事項の仕様に統合）
- リスクコントロール手段は、ユーザー仕様に記録する。

試験ツール

- 統合テスト（要求事項の仕様に記録）
- インターフェーステスト（要求事項の仕様に記録）
- ソフトウェアシステムテスト（要求事項の仕様に記録）

導入ツール

- ユーザー手順の確認
- アプリケーションの内部教育訓練
- 据付時適格性確認

保守計画

ジャックは、システム導入後に、システムの品質を保証するために適切な活動は何かを前もって考える。このシステムは残留リスクが低いことから、データベースのAVLデータの精確さの品質審査が必要と考える。ジャックは、検証プランニングの項にこの点を記載し、システムが作動したら3ヵ月毎にこの審査を実行するよう手順を開発及び実行するよう請求する。

例 12：校正管理ソフトウェア

XYZ メディカルカンパニーは急成長している。この企業は、欧州及びアジアの企業を買収した。そのために、この会社の校正管理の必要性も高まっている。現在、校正マネージャーがすべての校正情報が記載された帳簿をつけ、毎週、校正済み装置の在庫を確認し、再校正が必要な品目があるかを判断する。会社の成長に伴い、在庫も非常に大きくなり、また世界中に分散しているため、一人の担当者が紙のシステムを利用して管理できなくなってきている。コンピュータ化システムを導入する時期にきている。

プロセスの定義

XYZ メディカルには、 品質システムの一部を自動化するコンピュータ化システムの意図する使用の検証を必要とする SOP がある。この会社は、まず、プロセスに内在するリスクは何かを理解し、ソフトウェアのソリューションで現行のプロセスの一部又は全体を自動化できるかどうかを判断する情報を得るために、校正管理プロセスを定義する。この会社は、次のステップの詳細が記載された校正管理 SOP を確認する。

1. 新しい装置を調達する。
2. 装置に唯一の識別番号をつける。
3. 校正手順を決定する。
4. 装置を校正する。
5. 校正状態を装置に記録する。
6. 校正の要求事項及び状態、有効期限を含む校正記録を保管する。
7. 校正記録は、報告及び校正管理活動に必要である。

プロセスのリスク分析

紙媒体のシステム又は電子システムいずれにおいても、校正管理プロセスにはリスクが内在している。

このプロセスに関するリスクは次の通りである。

- 校正の有効期限が切れた装置を使用し、不正な測定値を記録した。これは、どの装置で発生するか、又は、この装置が使用されるプロセスの段階により、様々な結果を生じうる。
- 校正外の装置に校正済みを示す正確でないラベルが添付されている。これも、どの装置で発生するか、又は、プロセスの段階により様々な結果を生じうる。

- 校正記録を紛失し、装置に校正の有効期限が切れた未処理分が生じる。これにより、作業が遅れる可能性がある。
- 校正状態を誤って記録すると、有効期限が切れた装置が使用される可能性がある。
- 2 つの装置が同一の識別番号を受け取ると、唯一の記録ではなくなる。

校正が正確でない結果、最悪の場合、校正外の装置を使用して最終受入検査を実施し、本来ならば不合格となるべき医療機器が合格となる可能性があるため、このリスクを高リスクと判断する。この問題を低減するために、このグループは SOP を更新して、この装置のユーザーに使用前に装置に添付してある校正の有効期限シールを確認し、校正済み装置を使用するプロトコル実行時には、使用した装置の ID 番号及び校正の有効期限を記録なければならないという指示を入れなければならない。また、校正すべき装置を識別でき、ラベルがない装置又は有効期限を過ぎたラベルのついた装置を使用しないようユーザーを教育訓練しなければならない。この会社は、取扱説明書は適切な手段であるが、リスクを低くするほどの効果はないと考えるため、以上の対策を実施するとシステムの残留リスクは中程度になる。

ソフトウェアの意図する使用の定義

このシステムは校正活動を遂行しない。このシステムは、装置の校正情報及びデータ並びに校正履歴及び状態の入ったデータベースである。これは、校正プロセスのステップ 2、6 及び 7 を制御する。

このグループは、次の目的と意図のためにシステムの妥当性を確認することに合意する。

校正管理システムは、校正を必要とする装置への識別番号交付、校正済み装置のラベル印刷、校正結果のデータ保管、及び装置の校正状態報告に用いる。このシステムは、検査、測定及び試験装置に関する規則 21 CFR Part 820.72 の一部を自動化する。

検証プランニング

検証活動の準備のために、このグループは、成果物の内容及びこのプロセスへの職能を超えたグループの関与について予測し、検証プランニングを始める。

次の文書は、

選択したツールの文書化の厳密さのレベルを定義する。

- このシステムの文書化の厳密さは中程度である。つまり、主要成果物は個別に作成され、承認を受ける。

選択した“ツール”の精査（経営者及び職能を超えた関与及び審査）レベルを定義する。

- このシステムは、世界中で校正管理に使用されることから、グローバルITマネジメント及びオペレーションズマネジメントが、このシステムの検証プランニング及び検証レポートの承認という形式で参加することが適切である。これに加え、新しい施設の装置のマネージャーはすべての文書の審査及び承認に関与する。

ツールボックス から“定義”ツールを選択する。

- ユーザー/ビジネスプロセス要求事項
- ソフトウェア 要求事項
- 正式なソフトウェア要求事項の審査

ソフトウェア要求事項の定義

ソフトウェア要求事項には以下の要素が含まれる。

- 機能的ワークフロー
- 電子記録及び電子署名の要求事項
- データ論理要求事項
- 報告要求事項
- 機器のラベル印刷に特定した要求事項
- ユーザーの安全及び特性
- 性能要求事項
- 能力の定義

信頼の確立及びソフトウェアの制御

このグループは、この種の製品の納入業者3社を調査し、1社に、彼らの計画する意図する使用に最も良く適合する製品があることが判明した。その納入業者は、医療機器業界では広く使用されている。この会社の製品のこの版は相対的に新しい。旧版の追跡記録からある程度の信頼は得られるが、現在報告されている問題に基づいた既知の欠陥分析を実施し、検査開発グループが旧版にはない新機能の精査を実施する。

ソフトウェアと他のシステムとの境界の定義

このソフトウェアには他のソフトウェアシステムとのインターフェースはない。

ソフトウェアのリスク分析

検証チームは、グローバルな校正マネージャーとともに次の質問票を使用してソフトウェアのリスクを判定する。彼らは、まず、リスクを特定してから、そのリスクに対するリスクコントロール手段を特定し、残留リスクの受容可能性を評価する。

リスク分析

	リスク評価アンケート	Yes または No で回答すること Yes の場合はリスク番号を記入すること（例：リスク#1、リスク#2、…..リスク#n）
1.1 **製品の安全性** **（危害）**	ソフトウェアが故障した際に懸念される製品安全性への潜在的なリスクは存在するか？ すべての場合にある。－ソフトウェアが誤って校正外装置を校正装置と識別する可能性がある。 ➢ 患者への危害－ある。校正外装置が測定に使用されれば、校正外装置が患者に使用されうる。 ➢ オペレータへの危害－ある。温度又は力の測定が誤っている場合、オペレータが挟まれたり、負傷する可能性がある。 ➢ 第三者への危害－ある。装置による。 ➢ サービス担当者への危害－ある。温度や力を誤って測定すると、サービス担当者が挟まれたり、負傷する可能性がある。 ➢ 環境への危害―ある。圧力を誤って測定すると容器内に環境への有毒物質が入っている場合、容器に漏れが生じうる。	リスク 1－校正外装置が使用される
1.2 **製品の安全性** **（危害）**	ソフトウェアのユーザーがミスを犯した際に懸念される製品安全性への潜在的なリスクは存在するか？ ユーザーが装置の誤った校正データを入力した場合、すべての場合にある（1.1 参照）。 ➢ 患者への危害－ある。 ➢ オペレータへの危害－ある。 ➢ 第三者への危害－ある。 ➢ サービス担当者への危害－ある。 ➢ 環境への危害－ある。	リスク 1 参照
2.1 **製品クオリティ**	ソフトウェアが故障した際に懸念される製品クオリティへの潜在的なリスク（安全性のリスクを除く）は存在するか？ ある－ソフトウェアが誤って校正外装置を校正装置と識別して、製品が仕様外となりうる。これにより安全上の問題はないが、顧客の不満が生じる可能性がある。	リスク 1 参照

2.2 製品クオリティ	**ソフトウェアのユーザーがミスを犯した際に懸念される製品クオリティへの潜在的なリスク（安全性のリスクを除く）は存在するか？** ある－ユーザーが装置の誤った校正データを入力し、その装置で製品を測定した場合､製品が仕様外となり、安全上の問題はないが、顧客の不満が生じる可能性がある。	リスク 1 参照
3.1 記録の完全性	**記録を保管するシステムに記録の完全性への潜在的なリスクは存在するか？** • 記録の紛失－ある。校正記録が紛失する場合がある。 • 記録損傷－ある。校正記録が破損する場合がある。	リスク 2－校正記録が紛失し、法令遵守の問題になる リスク 3－校正記録が破損し、法令遵守の問題になる
4.1 FDA/ISO 規格の遵守証明	**規格遵守を証明する能力に関する潜在的なリスクは存在するか？** • 記録消失－ある。校正記録が紛失する場合がある。 • 記録損傷－ある。校正記録が破損する場合がある。	リスク 2 及びリスク 3 参照

リスク評価及び制御

リスク番号	説明	重大性	予防策	残留リスク
リスク#1	校正外装置を使用して製品を測定する、又は圧力若しくは力を測定する（ソフトウェアによる装置の誤識別又はユーザーによる誤った装置校正データの入力による）。	• 高レベル	システムは、装置の ID、シリアルナンバー並びに校正状態及び有効期限を記載したラベルを印刷する。手順では、装置使用前に従業員はこの情報を検証するように教育訓練を受けている。校正記録に記録される前に、2 人目が入力データを検証するプロセスがある。	受容可能
リスク#2	記録が紛失し、校正管理活動を擁護できない。	• 中レベル	校正データは、校正業者からの紙のデータで維持管理する	受容可能
リスク#3	記録が破損し、校正管理活動を擁護できない。	• 中レベル	校正データは、校正業者からの紙のデータで維持管理する	受容可能

リスク分析終了後、グループは、軽減後の残留リスクは受容可能であると満足している。

検証プランニングの終了

検証プランニングを終了するために、計画を修正して次に選択したツールを入れた。

インプリメンテーションツール

- トレーサビリティマトリックス
- システム設定の審査

試験ツール

- サイズ分析
- テスト計画
- 納入業者が、計画設定用試験及び旧版のソフトウェアにない新しい機能の試験付のテストスイートを提供。

導入ツール

- アプリケーションの内部教育訓練
- 据付時適格性確認（サーバー及びワークステーション用）

保守計画

何らかの時点で必ず保守を実施するため、グループは、システムの検証に加え、システムの保守計画も有益と考える。システムのモニタリング技術を使用して、欠陥、使用上の問題及び意図する使用の変更を確認する。

システム（ハードウェア、更新、パッチ、安全上の問題）の変更が分類されるように計画を作成し、チームがより効果的に変更を実施できるようにする。

例 13：自動ビジョンシステム

ゲアリーの会社の技術者は非常に優秀である。彼らは、ゲアリーのオートメーション領域で生産された製品である½インチ～1 ½インチの金属製バーについて知っているため、このバーについて 2 つのアプリケーションを見つけた。ひとつは 1 インチ以下のバー用、もうひとつは 1 ¼±¼インチ用である。バーの幅はすべて 1/8 インチである。いずれのアプリケーションも医療機器用で、規定した長さのバーが必要であった。オートメーション領域の技術者であるゲアリーの業務は、部品を選別する自動ビジョンシステムの検証である。

プロセスの記述

いずれのアプリケーションもバーの厚みの仕様は同じで、この寸法は、バー切断機で使用する原材料で確認した。バーの長さ以外の合格基準はすべて上流で確認し、長さはゲアリーの自動ビジョンシステムで測定した。

機械のプロセスは単純であった。バーを容器に入れ、じょうごでひとつずつコンベヤーに乗せた。停止場所までバーが運ばれ、カメラでバーの長さを計測した。次に、結果により、バーは 1 インチ以下用の容器又はそれより長いバー用の容器に運ばれた。

下流では他にバーの長さを確認しなかった。誤ったサイズのバーが使用された場合、製造された装置に漏れが生じるため、患者への危害のリスクが増大する。下流でこの増大リスクを検査する方法はなかったが、バーが規定した寸法の範囲内の正しい長さであれば装置に漏れは生じない。この装置は長年にわたり製造されており、このリスクは十分に理解されている。自動ビジョンシステムは、手動の測定プロセスの代替である。

意図する使用の定義

ゲアリーは自動化するプロセスを理解しているため、目的と意図の定義を始める。

ソフトウェアの意図は、コンベヤー上に金属製のバーが 1 本あることを確認し、その長さを計測することである。

リスク分析

ゲアリーは、施設のリスク分析プロセスを使用して、製品の故障又は破壊試験以外には間違ったサイズのバーが使用された事を検知する方法はなく、故障により患者に危害が加わる可能性があるため、このシステムの障害のリスクは高いと判断した。

このプロセスの重要な変数はバーの長さである。自動化によりこのリスクが増減することはない。

検証プランニング

検証プランニングの最初の検討において、ゲアリーは、 自分のリスク分析で高リスクの結果が出たため、厳格な妥当性確プロセスの使用を計画する。検証ツールのツールボックス確認後、彼は、正式な要求事項の定義の文書を計画し、製造技術者、もう一人のオートメーション技術者及び品質技術者が参加するソフトウェア要求事項の審査を計画する。このシステムのソフトウェアは社内で開発するが、これまでのシステムオートメーションと比べて単純である。

リスクコントロール手段

注目すべきリスク領域が 2 つ特定された。

1. 1 本のバーが測定位置にあることを確認する。機械の狭い経路（幅¼インチ、高さ 3/16 インチ）をバーが下降するため、部品は経路の長さに沿ってのみ通過し、バーが縦に連続していれば経路に入る。しかし、2 つの部品がコンベヤーの中で隣り合う可能性がある。

   このリスクを軽減するために、このソフトウェアが長さの前に幅を確認する。部品の幅が 1/8 インチ（過去に確認した仕様によれば、±1/32 インチ）を超える場合、2 つの部品がコンベヤーの中にあるため、拒否される。この目的のために、機械に 3 個目の容器を追加した。
2. バーが近づきすぎて、1 本目の末端と 2 本目の先端がわからない場合がある。このソフトウェアは、1 ½インチを超えることを確認できない部品をすべて拒否容器に運搬する。

検証業務

次に、ゲアリーは検証業務に進む。彼は、正式な設計文書の必要性を特定し、要求事項を審査したチームとともに設計の各項の正式な査察を計画する。また、コードを作成した場合、ソフトウェアの開発経験のあるオートメーション技術者及び製造技術者が設計に照らし合わせて審査する。このソフトウェアは内部で開発したため、納入業者管理活動は選択しなかった。オートメーション技術者、製造技術者及び品質技術者全員に、ソフトウェアのトレーサビリティの審査及び要求事項の再設計を請求する。技術者は、すべての要求事項の試験が完全に終了したことを確認する試験の後に、同じ試験を行う。

ゲアリーが選んだツールボックスのテストの項には、テスト計画にソフトウェア環境及び予想テスト結果の詳細を含めるテストの計画が入っている。彼は、単体テスト、統合テスト及びシステムテストなど、開発の様々な時点において数種類のテストを計画した。正常及び異常テストケースを、コンベヤーベルトのスピードに関する性能試験とともに使用する。テスト計画は、ゲアリー以外にオートメーション技術者、製造技術者及び品質技術者が審査及び承認しなければならない。予想結果と実際の検査結果の比較、合否の指示、テストの識別並びにあらゆる故障の問題解決及び回帰テストが含まれるテスト結果についても、ゲアリーはこのグループから承認をうけなければならない。

インプリメンテーション、試験及び導入

自動ビジョンシステムの導入について、ゲアリーは、ツールボックスの導入ツールを確認し、据付時適格性確認及びプロセスの検証が必要だと判断する。また、彼は、このシステムのユーザーのためにユーザーの手順を作成し、オペレータの認証が必要だと決定する。

保守

ゲアリーの部門は、部門全体で製造フロアのすべてのシステムの保守を計画する。この領域には特別の計画又は活動は必要でない。

例 14：ピックアンドプレースシステム

アクメコーポレーションは、クラス II の医療機器製造業者である。アクメコーポレーションは、あるステーションから自社で製造する医療機器の一部であるカートリッジに半製品である部品を入れる作業を自動化したい。

新しいピックアンドプレース（P&P）システムのプロジェクトマネージャーであるジャックは、P&P プロセスは医療機器製造の一部であるため、21 CFR Part 820 の規制を受けるプロセスであると判断する。したがって、導入が予定されている P&P システムはソフトウェア検証の要求事項に該当する。

現行プロセスの定義

P&P システム開発の要求事項及びリスクの理解を深めるために、ジャックは関連するビジネスプロセスを次の通り定義する。

1. 製造工程のステーション 11 から来る部品をステーション 12 のカートリッジに入れる（カートリッジ 1 個あたり部品 20 個）。現在、この操作は、オペレータが手動で行っている。
2. オペレータは、次に、ステーション 12 の受入トラックに手動でカートリッジを乗せる。
3. オペレータは手動でカートリッジを検査し、部品の位置が正確であることを確認する（ステップ 2 及び 3 は、カートリッジ 1 個あたり約 3 分）。
4. カートリッジは、それまでのプロセスのステップすべてにおいて異常がないことを確認する目視検査を含む他の組立段階に進む。

プロセスリスクの分析

ジャックは、次に、現行のプロセスで発生しうる問題について考える。彼の分析では、次の通りである。

1. オペレータが半製品である部品を変形させる可能性がある。これは、下流の検査ステーションで検知する。
2. オペレータが誤ってカートリッジに部品を入れる可能性、又はカートリッジのスロットに入れられない可能性がある。これは、現在、手動検査によりステーション 12 で検出する。

リスクコントロール手段に基づき、ジャックはプロセスの残留リスクは低いと判断する。したがって、新しい P&P システムも恐らく低リスクシステムであろうと考える。

新プロセスの定義

ジャックは、プロセスリスクを評価した後、P&P システムの知識から判断して、新しいプロセスを次の通り定義する。

1. P&P システムにカートリッジを搭載する。
2. P&P システムは、ステーション 11 から部品を拾い上げ、カートリッジに挿入する（カートリッジ 1 個あたり部品 20 個）。
3. P&P システムは、カートリッジを目視検査し、すべての部品が正確な位置にあり、カートリッジのすべてのスロットが充填されていることを確認する。不良カートリッジは自動的に拒否する。
4. P&P システムは、 受容可能なカートリッジをステーション 12 に置く。（ステップ 2～4 は 1 分間）。
5. カートリッジは、それまでのプロセスのステップすべてにおいて変形がないことを確認する目視検査を含む他の組立段階に進む。

ソフトウェアの意図する使用の定義

ジャックは、既に自動化すべきプロセスを理解しており、導入予定の新しい P&P システムの目的と意図を作成しようとしている。

彼は、次の通り記載する。

P&P システムは、ステーション 11 から部品を拾い上げ、カートリッジに挿入し、カートリッジのすべてのスロットが正確に充填されていることを確認し、不良カートリッジは拒否し、その後、1 分間にカートリッジ 1 個の速度でカートリッジをステーション 12 の受ラインに乗せる。

また、ジャックは、P&P システムと他のシステムのインターフェースについて考え、他にインターフェースはないと判断する。彼は、ユーザーインターフェースはあるが、ソフトウェア インターフェースはないと判断する。

検証プランニング

ここで、ジャックは自動化すべきビジネスプロセスを理解しており、新システムの目的及び意図を決定し、次に、高レベルの検証プランニングを作成する準備が整った。彼は、後日計画の詳細を肉付けするが、必要な検証の取り組みのレベルを特定できるよう、検証プランニングを今開始したい。

検証プランニングの開始にあたり、ジャックは、導入されるシステムが遵守すべき FDA の規制について考える。彼は、検証プランニングに 21 CFR Part 820 を要求事項

として記入し、このシステムで作成又は維持する電子品質システム記録はなく、電子署名もないため、21 CFR Part 11 は適用されないと判断する。

既に、ジャックは既存の P&P システムのプロセス残留リスクは低いと判断した。したがって、彼は、この検証の取り組みでは多くの詳細又は手続きは不要であると考える。彼は、新システムのユーザービジネスプロセス要求事項及びソフトウェア要求事項の定義が重要であると理解している。しかし、このシステムは低リスクであるため、それぞれ別の署名付文書を作成する必要はない。したがって、彼は、表形式を用いて、ビジネスプロセス要求事項、ソフトウェア要求事項に加えて彼の検査計画も単一文書にすることを決定する。

さらに、このシステムは非常にリスクが低いため、ジャックは、この検証の取り組みには広範な経営者の審査は不要と判断する。彼は、製造マネージャー及び QA 代表者の承認で十分であるとの結論を出した。しかし、ユーザーの要求事項が正確であると確信するにはこのプロセスのオペレータ代表の確認も必要であると考える。

以上の決定に基づき、ジャックは検証プランニングの作成を開始する。アクメコーポレーションには、検証プランニング用の標準様式がある。検証プランニングの一部はまだ空欄となっており、最初のシステム設計が承認された後にジャックが記入する。

システム及びソフトウェア要求事項の定義

ジャックは、ソフトウェア要求事項を作成する。彼は、ソフトウェア要求事項に、P&P プロセス/システムステップとは何か、並びに P&P システムとステーション 11 及び 12 とのインターフェースの仕様が含まれることを決定する。このシステム要求事項は、P&P システムの動きの速さ及び精確さが含まれる。危害のリスクを低減するために、ジャックは、オペレータとピックアンドプレースのアームの間に物理的な壁を設置する安全に関する要求事項を追加する。

信頼の確立及びソフトウェアの制御

ジャックは、新システム購入のためにどのアプローチ及びどの技術を使用するか決定しなければならない。ビジネス要求事項が非常に単純である、処理量は少なく、低リスクシステムであることから、彼は第三者の P&P システム購入を決定する。彼は、価格と品質を考慮して、P&P システム業界のリーダーであるコントロルシス株式会社の P&P システム購入を決定する。

コントロルシスは外部のシステム納入業者であるため、この納入業者に対する信頼を確立するためにどのような種類の活動を行うべきか決定しなければならない。ジャックは手持ちのコントロルシスに関する情報を評価し、コントロルシスの製品は広範に

使用されており、過去に、この製品に関する問題があれば迅速に特定し、インターネットの掲示板に公表されたことを知った。また、コントロルシスは自動 IQ/OQ/PQ テストスイートを提供している。P&P システムは低リスクであるという事実と合わせて、ジャックは、コントロルシスの納入業者監査は不要と判断し、この納入業者を承認する。

ソフトウェアの障害リスク分析

ジャックは、自動化すべきビジネスプロセスは低リスクと既に判断したが、まだ、ソフトウェア障害のリスクを分析する必要がある。彼は、この活動に定量的リスクモデルを使用することを決定し、新システムに次の通り順位をつけた。

- ソフトウェアの障害は下流の活動で検知されるため、彼は、“重大さ”を 1～10 の尺度で低い（3）と評価した。
- システムの設計は非常に単純で、検査中に検出できない重大なバグが出てくる可能性は低いと考えたため、可能性は低い（1）と評価した。
- 彼は、リスクスコアを 4 と算出した。これは、低リスクに分類される。

したがって、ジャックは低リスクに適した検証業務を実施する。

検証プランニングの終了

ここで、ジャックはソフトウェアの要求事項を定義し、実施アプローチを決定し、ソフトウェアのリスクを分析し、検証プランニング終了に十分な情報を得ている。

導入予定のシステムは残留が少ないことから、ジャックは今後の開発及び検証の取り組みに次の“ツール”を選択する。

設計、開発及び設定ツール

- ソフトウェアアーキテクチャの文書化及び審査
- トレーサビリティマトリックス（要求事項の仕様に統合）
- リスクコントロール手段は、ユーザー仕様に記録する。

試験ツール

- 統合テスト（要求事項の仕様に記録）
- インターフェーステスト（要求事項の仕様に記録）
- ソフトウェアシステムテスト（要求事項の仕様に記録）

導入ツール

- ユーザー手順の確認

- アプリケーションの内部教育訓練
- 納入業者供給テストスイート（コントロルシスより）

保守計画

ジャックは、システム導入後に、システムの品質を保証するために適切な活動は何かを前もって考える。このシステムは残留リスクが低いことから、ジャックは校正スケジュールに移動機構の校正を追加する時に製造業者の助言に従い、このシステムをこの会社の最長検証審査サイクル（3 年）とする。

批判的思考審査

最終的に、ジャックは、すべての要求される要素を考慮し、自分の検証のアプローチを信頼できるかを自問する。ジャックは、選択した検証活動が完了すればソフトウェアが意図した通りに作動する信頼が生じると結論づけた。

附属書 D
定義

変更管理：適当な分野の資格認定を受けた代表者が、制御された、又は妥当性が確認された実体（例えば、製品、ソフトウェア又は文書）の変更の問題及び変更の請求を記録、評価、実施及び配置する、制御された方法。変更管理プロセスは、故障報告、変更請求、変更請求の評価並びに変更の承認、実施及び導入を含む。評価には、ソフトウェアの安全かつ有効な操作に対する変更の影響評価、変更後の正確な操作検証に必要な回帰テストのレベル、及びソフトウェアがその意図する使用に従い実行を継続するという信頼を得るために必要なその他の活動の定義を含まなければならない。

変更制御：変更管理の一部で、設定の定義及び構成要素を含むすべての文書及び成果物の変更を処理する制御された方法。

コンピュータ:（1）作動中に人間の介入なく多くの算術演算又は論理演算など重要な計算を実行する機能単位。（2）内蔵プログラムが制御する関連処理装置及び周辺装置のひとつ、又はそれ以上から構成する、人間の介入なく多くの算術演算又は論理演算など重要な計算を実行するプログラム可能な機能単位。（IEEE）

構成制御：変更制御の一部で、構成（設計、仕様、製図など）及び構成要素を定義する文書の変更を処理する制御された方法。

構成品目：特定の基準点においてのみ識別できるエンドユーザー機能を満たす構成内の実体。（ISO/IEC 12207）

批判的思考（クリティカルシンキング）：ソフトウェアが妥当性を確認された状態であるという信頼を獲得し、維持するための適切な活動の特定及び選択に使用する、ソフトウェア及び環境の多様な側面を分析し、評価するプロセス。

導入：ソフトウェアを使用可能にするすべての活動。

動的分析：動的分析とは、プログラムコードの実行により実施する試験である。

危害：人の受ける身体的障害もしくは健康障害、又は財産若しくは環境の受ける害。本 TIR では法令遵守への影響も含む。詳細は附属書 B 参照。

ハザード：危害の潜在的な源（ANSI/AAMI/ISO 14971）

危険事象：あらゆるハザードの発生（ISO ガイド 51）

危険状態：潜在的ハザード発生防止の制御が不十分な一連の状況。

意図する使用：4.3.1.4 項参照

医療機器ソフトウェア：医療機器の構成要素、部品若しくは附属品として使用するソフトウェア、又はそれ自体が医療機器であるもの。

プロトコル：コミュニケーション実現において機能単位の行動を決定する一連の意味規則及び構文規則。（FDA コンピュータ化システム及びソフトウェア開発技術用語集）

プロセス障害：医療機器の安全及び有効性、製造要員、環境又は品質システムに対するプロセス障害の影響の測定。

品質システム： 品質管理を実施するための組織構造、責任、手順、プロセス及び資源。（21 CFR 820）

規制プロセス：医療機器製造業者が実施する、品質システム規則で定められた一連の活動。（21 CFR 820）

リスク：危害の発生確率とその危害の重大さとの組み合わせ。（ANSI/AAMI/ISO 14971）

リスク分析：適切な情報をまとめ、統合すること。これは、リスクを管理するためのその情報の使い方の指針となる。

リスクアセスメント:リスク分析及びリスク評価からなる全体プロセス。（ANSI/AAMI/ISO 14971）（DOD）リスクとその影響に関する包括的な評価。（FDA コンピュータ化システム及びソフトウェア開発技術用語集）

リスクコントロール手段：危害の発生確率の重大さを低減するための方法。

リスクマネジメント：リスクの分析、評価及びコントロール業務に対して、管理方針、手順及び実施を体系的に適用すること。（ANSI/AAMI/ISO 14971）

ソフトウェアのリスク：自動化したプロセス及びプロセス障害の分析で特定された関心領域に対してソフトウェア障害の影響を測定すること。

ソフトウェア開発プロセス：ユーザーのニーズをソフトウェア製品に変えるプロセス。このプロセスでは、ユーザーのニーズをソフトウェアの要求事項に変え、ソフトウェアの要求事項を設計にし、設計をコードに入れ、コードを試験し、時に操作活動のソフトウェアをインストール及び確認する。注：このような活動は、重複又は反復する場合がある。参照：漸増的開発、ラピッドプロトタイピング、スパイラルモデル、ウォーターフォールモデル。（IEEE）

規制プロセス用ソフトウェア（規制プロセスソフトウェア）:品質システム規則（21 CFR 820）で定められた、機器の設計、試験、部品の受け入れ、製造、ラベリング、包装、販売及び苦情処理の自動化に使用するソフトウェア又は品質システムの他の側面の自動化に使用するソフトウェア。また、電子記録の作成、修正及び保管に使用するソフトウェア並びに検証の要求事項の対象となる電子署名の管理に使用するソフトウェアにも適用される。(21 CFR 11)

静的解析：静的解析は、プログラムの実行を伴わずに実施する評価で、ソフトウェアの形状、構造、内容及び記録にもとづいてソフトウェアを評価するプロセスが含まれる。

試験:（IEEE）（1）規定された条件においてシステム又は構成要素を操作し、結果を観察又は記録し、そのシステム又は構成要素のある側面を評価するプロセス。（2）既存の条件と必要とされる条件の差を検出し（バグなど）、ソフトウェアの特性を評価するソフトウェアの分析プロセス。参照：動的分析、静的分析、ソフトウェア工学。（FDA コンピュータ化システム及びソフトウェア開発技術用語集）

トレーサビリティ:（IEEE）（1）開発プロセスの 2 つ又はそれ以上の製品の間に確立される関係の程度。特に相互に先任－後任関係又は主従関係がある製品について言う。例えば、特定のソフトウェアの構成要素の要求事項と設計が適合する程度。（2）ソフトウェア開発製品の各要素が存在理由を確立する程度。例えば、風船図の各要素が、それが満たす要求事項を参照する程度。（FDA コンピュータ化システム及びソフトウェア開発技術用語集）

妥当性が確認された状態：意図する使用の妥当性が確認されたソフトウェアを確立するために、十分な信頼獲得活動が実施された状態。

検証： 所定の意図する使用の特定の要求事項が一貫して実施されたことの検討及び客観的証拠の提出による確認。（21 CFR 820）

納入業者管理：購入したソフトウェア及びソフトウェア関連サービス（又はその両方）の納入業者を評価するプロセス。この納入業者の製品及び購入したソフトウェアが規制プロセスでの使用中に妥当性が確認された状態を継続するために必要な継続的関係にどのような信頼獲得活動が実施されたかを判断する。

版制御：構成制御の一部で、構成要素及び版変更を処理する制御された方法。

ウォッチドッグタイマー：ハングなどの故障状況によりメインプログラムが通常のウォッチドッグサービスを実行しない場合（“サービスパルス”を書き込む）、コンピュータハードウェアの時間計測器がシステムをリセットする。目的は、ハング状態から正常の運転にシステムを戻すことである。

附属書 E
参考資料

21 CFR 820, *21 FDA Code of Federal Regulations, part 820 - Quality Systems*

21 CFR 11, *21 FDA Code of Federal Regulations, part 11 - Electronic Records / Signatures*

AAMI TIR32, *Medical device software risk management*

CMMI, *Capability Maturity Model Integration, Software Engineering Institute*

IEEE, *Institute of Electrical and Electronics Engineers, Inc. Software Standards*

GCSSDT, *FDA Glossary of Computerized System and Software Development Terminology*

GPSV, *General Principles of Software Validation; Final Guidance for Industry and FDA Staff; (FDA/CDRH 938:2002)*

ISO 14971, *International Organization for Standardization (ISO), Medical devices - Application of risk management to medical devices (ISO 14971:2000)*

ISO 13485, *International Organization for Standardization (ISO), Quality management systems -Requirements for regulatory purposes (ISO 13485:2003)*

ISO 9000, *International Organization for Standardization (ISO), Quality management systems -Fundamentals and vocabulary (ISO 9000:2005)*