2023 年 8 月 8 日　医療機器 QMS コンサルタント　矢部久雄

Appendix A. Examples

The examples in this section outline possible application of the principles in this draft guidance to various software assurance 605 situations cases.
このセクションの例は、さまざまなソフトウェア アシュアランスのケースに対するこのドラフト ガイダンスの原則の可能な適用の概要を示しています。

Example 1: Nonconformance Management System

A manufacturer has purchased COTS software for automating their nonconformance process and is applying a risk-based approach for computer software assurance in its implementation. The software is intended to manage the nonconformance process electronically. The following features, functions, or operations were considered by the manufacturer in developing a risk-based assurance strategy:
製造業者は、不適合プロセスを自動化するために COTS ソフトウェアを購入し、その実装におけるコンピューター ソフトウェア保証のためにリスクベースのアプローチを適用しています。 このソフトウェアは、不適合プロセスを電子的に管理することを目的としています。 以下の特徴、機能、または操作は、リスクベースの保証戦略を開発する際に製造業者によって考慮されました。

Table 2. Computer Software Assurance Example for a Nonconformance Management System

Features, Functions, or Operations	Intended Use of the Features, Functions or Operations	Risk-Based Analysis	Assurance Activities	Establishing the appropriate record
Nonconformance (NC) Initiation Operations: · A nonconforming event results in the creation of an NC record. · The necessary data for initiation are recorded prior to completion of an NC initiation task.	The intended uses of the operations are to manage the workflow of the nonconformance and to error-proof the workflow to facilitate the work and a complete quality record. These operations are intended to supplement	Failure of the NC initiation operation to perform as intended may delay the initiation workflow, but would not result in a quality problem that foreseeably compromises safety, as the manufacturer has additional processes in place for	The manufacturer has performed an assessment of the system capability, supplier evaluation, and installation activities. In addition, the manufacturer supplements these activities with exploratory testing of the operations. High level	The manufacturer documents: · the intended use · risk determination, · summary description of the features, functions, operations tested · the testing objectives and if they passed or failed

· An NC Owner is assigned prior to completion of the NC initiation task.	processes established by the manufacturer for containment of non-conforming product.	containment of non-conforming product. As such, the manufacturer determined the NC initiation operations did not pose a high process risk.	objectives for testing are established to meet the intended use and no unanticipated failures occur.	· any issues found and their disposition · a concluding statement noting that the performance of the operation is acceptable · the date testing was performed, and who performed the testing.
<u>Electronic Signature Function:</u> · The electronic signature execution record is stored as part of the audit trail. · The electronic signature employs two distinct identification components of a login and password. · When an electronic signature is executed, the following information is part of the execution record: o The name of the person who signs the record o The date (DD-MMYYYY) and time (hh:mm) the signature was executed. o The meaning associated with the signature (such as	The intended use of the electronic signature function is to capture and store an electronic signature where a signature is required and such that it meets requirements for electronic signatures.	If the electronic signature function were to fail to perform as intended, then production or quality system records may not reflect appropriate approval or be sufficiently auditable, or may fail to meet other regulatory requirements. However, such a failure would not foreseeably lead to compromised safety. As such, the manufacturer determined that this function does not pose high process risk.	The manufacturer has performed an assessment of the system capability, supplier evaluation, and installation activities. To provide assurance that the function complies with applicable requirements, the manufacturer performs ad-hoc testing of this function with users to demonstrate the function meets the intended use.	The manufacturer documents: · the intended use · risk determination · testing performed · any issues found and their disposition · a concluding statement noting that the performance of the function is acceptable · the date testing was performed and who performed the testing.

review, approval, responsibility, or authorship).				
Product Containment Function: · When a nonconformance is initiated for product outside of the manufacturer's control, then the system prompts the user to identify if a product correction or removal is needed.	This function is intended to trigger the necessary evaluation and decisionmaking on whether a product correction or removal is needed when the nonconformance occurred in product that has been distributed.	Failure of the function to perform as intended would result in a necessary correction or removal not being initiated, resulting in a quality problem that foreseeably compromises safety. The manufacturer therefore determined that this function poses high process risk.	The manufacturer has performed an assessment of the system capability, supplier evaluation, and installation activities. Since the manufacturer determined the function to pose high process risk, the manufacturer determined assurance activities commensurate with the medical device risk: established a detailed scripted test protocol that exercises the possible interactions and potential ways the function could fail. The testing also included appropriate repeatability testing in various scenarios to provide assurance that the function works reliably.	The manufacturer documents: · the intended use · risk determination · detailed test protocol developed · detailed report of the testing performed · pass/fail results for each test case · any issues found and their disposition · a concluding statement noting that the performance of the operation is acceptable · the date testing was performed and who performed the testing · the signature and date of the appropriate signatory authority.

特徴、機能または操作	特徴、機能または操作の使用目的	リスクベースの分析	保証活動	適切な記録の確立
不適合（NC）開始操作:	操作の使用目的は、不適合のワ	NC 開始操作が意図したとお	メーカーは、システム機能の評	メーカーの文書:

· 不適合イベントにより、NC レコードが作成されます。 · NC 開始タスクの完了前に、開始に必要なデータが記録されます。 · NC 所有者は、NC 開始タスクの完了前に割り当てられます。	ークフローを管理し、ワークフローのエラーを防止して、作業と完全な品質記録を促進することです。 これらの操作は、不適合製品の封じ込めのために製造業者によって確立されたプロセスを補足することを目的としています。	りに実行されない場合、開始ワークフローが遅れる可能性がありますが、製造業者は不適合製品を封じ込めるための追加プロセスを実施しているため、安全性を損なう品質問題は発生しません。 そのため、メーカーは、NC 開始操作が高いプロセス リスクをもたらさないと判断しました。	価、サプライヤーの評価、および設置作業を実施しました。さらに、製造業者はこれらの活動を操作の探索的テストで補足します。 テストの高レベルの目標は、使用目的を満たすように確立されており、予期しない障害は発生しません。	· 使用目的 · リスク決定、 · テストされた特徴、機能、操作の概要説明 · テストの目的と合格または不合格 · 見つかった問題とその処置 · 操作のパフォーマンスが許容できることを示す結論文 · テストが実施された日付、およびテストを実施した人。
<u>電子署名機能:</u> ・電子署名の実行記録は、監査証跡の一部として保存されます。 · 電子署名は、ログインとパスワードという 2 つの異なる識別コンポーネントを使用します。 · 電子署名が実行されると、次の情報が実行記録の一部になります。 o 記録に署名した人の名前 o 署名が実行された日付 (DD-MMYYYY) と時刻 (hh:mm)。 o 署名に関連付けられた意味 (レビュー、承認、責任、作成者	電子署名機能の使用目的は、署名が必要な場合に電子署名を取得して保存し、電子署名の要件を満たすことです。	電子署名機能が意図したとおりに実行されなかった場合、生産または品質システムの記録は適切な承認を反映していないか、十分に監査可能でないか、または他の規制要件を満たしていない可能性があります。しかし、そのような失敗が予見できるほど、安全性が損なわれることはありません。 そのため、メーカーは、この機能が高いプロセス リスクをもたらさないと判断しました。	メーカーは、システム機能の評価、サプライヤーの評価、および設置作業を実施しました。機能が適用される要件に準拠していることを保証するために、製造業者は、ユーザーを対象にこの機能のアドホック テストを実施し、機能が意図した用途を満たしていることを実証します。	メーカーの文書: · 使用目的 · リスク判定 · 実施された試験 · 見つかった問題とその処置 · 機能の性能が許容できることを示す結論文 · テストが実行された日付とテストを実行した人。

など)。				
製品封じ込め機能: · メーカーの管理外で製品の不適合が開始された場合、システムは、製品の修正または削除が必要かどうかを確認するようユーザーに促します。	この機能は、流通した製品に不適合が発生した場合に、製品の修正または削除が必要かどうかについて、必要な評価と意思決定をトリガーすることを目的としています。	機能が意図したとおりに実行されない場合、必要な修正または削除が開始されず、安全性が損なわれることが予測される品質上の問題が発生します。したがって、メーカーは、この機能が高いプロセス リスクをもたらすと判断しました。	メーカーは、システム機能の評価、サプライヤーの評価、および設置作業を実施しました。製造業者は、その機能が高いプロセス リスクをもたらすと判断したため、製造業者は、医療機器のリスクに見合った保証活動を決定しました。つまり、可能性のある相互作用と機能が失敗する可能性のある方法を実行する詳細なスクリプト化されたテスト プロトコルを確立しました。 テストには、機能が確実に機能することを保証するために、さまざまなシナリオでの適切な再現性テストも含まれていました。	メーカーの文書: · 使用目的 · リスク判定 · 詳細な試験プロトコルの開発 · 実施されたテストの詳細なレポート ・各テストケースの合否結果 · 見つかった問題とその処置 · 操作のパフォーマンスが許容できることを示す結論文 · テストが実施された日付と誰がテストを実施したか · 適切な署名機関の署名と日付。

Example 2: Learning Management System (LMS)

A manufacturer is implementing a COTS LMS and is applying a risk-based approach for computer software assurance in its implementation. The software is intended to manage, record, track, and report on training. The following features, functions, or operations were considered by the manufacturer in developing a risk-based assurance strategy:

製造業者は COTS LMS を実装しており、その実装においてコンピュータ ソフトウェア保証のためにリスクベースのアプローチを適用しています。 このソフトウェアは、トレーニングの管理、記録、追跡、およびレポートを目的としています。 以下の機能、機能、または操作は、リスクベースの保証戦略を開発する際に製造業者によって考慮されました。

Table 3. Computer Software Assurance Example for an LMS

Features, Functions, or Operations	Intended Use of the Features, Functions or Operations	Risk-Based Analysis	Assurance Activities	Establishing the appropriate record
*The system provides user log-on features (e.g., username and password) · The system assigns trainings to users per the curriculum assigned by management · The system captures evidence of users' training completion · The system notifies users of training curriculum assignments, completion of trainings, and outstanding trainings · The system notifies users' management of outstanding trainings · The system generates reports on training curriculum assignments, completion of training, and outstanding trainings	All of the features, functions, and operations have the same intended use, that is, to manage, record, track and report on training. They are intended to automate processes to comply with 21 CFR 820.25 (Personnel), and to establish the necessary records.	Failure of these features, functions, or operations to perform as intended would impact the integrity of the quality system record but would not foreseeably compromise safety. As such, the manufacturer determined that the features, functions, and operations do not pose high process risk.	The manufacturer has performed an assessment of the system capability, supplier evaluation, and installation activities. In addition, the manufacturer supplements these activities with unscripted testing, applying errorguessing to attempt to circumvent process flow and "break" the system (e.g. try to delete the audit trail).	The manufacturer documents: · the intended use · risk determination · a summary description of the failure modes tested · any issues found and their disposition · a concluding statement noting that the performance of the operation is acceptable · the date testing was performed, and who performed the testing.

特徴、機能または操作	特徴、機能または操作の使用	リスクベースの分析	保証活動	適切な記録の確立

	目的			
・システムは、ユーザーのログオン機能（ユーザー名とパスワードなど）を提供します。 · システムは、管理者によって割り当てられたカリキュラムに従ってユーザーにトレーニングを割り当てます · システムは、ユーザーのトレーニング完了の証拠を取得します · システムは、トレーニングカリキュラムの割り当て、トレーニングの完了、および優れたトレーニングをユーザーに通知します ・システムは、優れたトレーニングのユーザーの管理に通知します · システムは、トレーニングカリキュラムの割り当て、トレーニングの完了、および優れたトレーニングに関するレポートを生成します。	すべての特徴、機能、および操作の使用目的は同じです。つまり、トレーニングの管理、記録、追跡、およびレポートです。これらは、21 CFR 820.25 (人員)に準拠するためのプロセスを自動化し、必要な記録を確立することを目的としています。	これらの特徴、機能、または操作が意図したとおりに実行されない場合、品質システム記録の完全性に影響を与えますが、予見できるほど安全性が損なわれることはありません。 そのため、メーカーは、特徴、機能、および操作が高いプロセスリスクをもたらさないと判断しました。	メーカーは、システム機能の評価、サプライヤーの評価、および設置作業を実施しました。さらに、製造業者はこれらの活動をスクリプト化されていないテストで補完し、エラー推測を適用してプロセス フローを回避し、システムを「破壊」しようとします (たとえば、監査証跡を削除しようとします)。	メーカーの文書: · 使用目的 · リスク判定 · テストされた故障モードの概要説明 · 見つかった問題とその処置 · 操作のパフォーマンスが許容できることを示す結論文 · テストが実施された日付、およびテストを実施した人。

Example 3: Business Intelligence Applications

A medical device manufacturer has decided to implement a commercial business intelligence solution for data mining, trending, and reporting. The software is intended to better understand product and process performance over time, in order to provide identification of improvement opportunities. The following features, functions, or operations were considered by the manufacturer in developing a risk-based assurance strategy:

ある医療機器メーカーは、データ マイニング、傾向分析、およびレポート作成のための商用ビジネス インテリジェンス ソリューションを実装することを決定しました。 このソフトウェアは、改善の機会を特定するために、製品とプロセスのパフォーマンスを経時的によりよく理解することを目的としています。 以下の特徴、機能、または操作は、リスクベースの保証戦略を開発する際に製造業者によって考慮されました。

Table 4. Computer Software Assurance Example for a Business Intelligence Application

Features, Functions, or Operations	Intended Use of the Features, Functions or Operations	Risk-Based Analysis	Assurance Activities	Establishing the appropriate record
Connectivity Functions: · The software allows for connecting to various databases in the organization and external data sources. · The software maintains the integrity of the data from the original sources and is able to determine if there is an issue with the integrity of the data, corruption, or problems in data transfer.	These functions are intended to ensure a secure and robust capability for the system to connect to the appropriate data sources, ensure integrity of the data, prevent data corruption, modify, and store the data appropriately.	Failure of these functions to perform as intended would result in inaccurate or inconsistent trending or analysis. This would result in failure to identify potential quality trends, issues or opportunities for improvement, which in some cases, may result in a quality problem that foreseeably compromises safety. As such, the manufacturer determined that these functions posed high process risk, necessitating more-rigorous assurance activities, commensurate with the related medical device risk.	The manufacturer determined assurance activities commensurate with the medical device risk and has performed an assessment of the system capability, supplier evaluation, and installation activities. Additionally, the manufacturer establishes a detailed scripted test protocol that exercises the possible interactions and potential ways the functions could fail. The testing also includes appropriate repeatability testing in various scenarios to provide assurance that the functions work reliably.	The manufacturer documents: · the intended use · risk determination · detailed test protocol · a detailed report of the testing performed · pass/fail results for each test case · any issues found and their disposition · a concluding statement noting that the performance of the operation is acceptable · the date testing was performed, and who performed the testing · the signature and date of the appropriate signatory authority.

Usability Feature: · The software provides the user a help menu for the application.	This feature is intended to facilitate the interaction of the user with the system and provide assistance on use of all the system features.	The failure of the feature to perform as intended is unlikely to result in a quality problem that would lead to compromised safety. Therefore, the manufacturer determined that the feature does not pose high process risk.	The feature does not necessitate any additional assurance effort beyond what the manufacturer has already performed in assessing the system capability, supplier evaluation, and installation activities.	The manufacturer documents: · the intended use · risk determination · the date of assessment and who performed the assessment · a concluding statement noting that the performance is acceptable given the intended use and risk.
Reporting Functions: · The software is able to create and perform queries and join data from various sources to perform data mining. · The software allows for various statistical analysis and data summarization. · The software is able to create graphs from the data. · The software provides the capability to generate reports of the analysis.	These functions are intended to allow the user to query the data sources, join data from various sources, perform analysis, and generate visuals and summaries. These functions are intended for collection and recording data for monitoring and review purposes that do not have a direct impact on production or process performance. In this example, the software is not intended to inform quality decisions.	Failure of these functions to perform as intended may result in a quality problem (e.g., incomplete or inadequate reports) but, in this example, would not foreseeably lead to compromised safety because these functions are intended for collection and recording data for monitoring and review purposes that do not have a direct impact on production or process performance. Therefore, the manufacturer determined that these functions do not	The supplier of the reporting software has validated the ability of the software to create and perform queries, join data from various sources to perform data mining, perform statistical analysis and data summarization, create graphs and generate reports. Beyond this, the manufacturer has assessed the system capability and performed supplier evaluation and installation activities. As such, the manufacturer determined	The manufacturer documents: · the intended use · risk determination · the date of assessment and who performed the assessment · a concluding statement noting that the performance is acceptable given the intended use and risk.

		pose high process risk.	that the reporting functions of the software do not necessitate any additional assurance effort beyond these activities.	

特徴、機能または操作	特徴、機能または操作の使用目的	リスクベースの分析	保証活動	適切な記録の確立
接続機能: · このソフトウェアにより、組織内のさまざまなデータベースや外部データ ソースに接続できます。 · ソフトウェアは、元のソースからのデータの整合性を維持し、データの整合性に問題があるかどうか、破損、またはデータ転送の問題があるかどうかを判断できます。	これらの機能は、システムが適切なデータ ソースに接続し、データの整合性を確保し、データの破損を防止し、データを適切に変更および保存するための安全で堅牢な機能を確保することを目的としています。	これらの機能が意図したとおりに実行されない場合、不正確または一貫性のない傾向分析または分析が行われる可能性があります。 これにより、潜在的な品質傾向、問題、または改善の機会を特定できず、場合によっては、安全性を損なうことが予見できる品質問題につながる可能性があります。 そのため、メーカーは、これらの機能が高いプロセス リスクをもたらすと判断し、関連する医療機器のリスクに見合った、より厳格な保証活動が必要であると判断しました。	メーカーは、医療機器のリスクに見合った保証活動を決定し、システム機能の評価、サプライヤーの評価、および設置活動を実施しました。 さらに、メーカーは、可能な相互作用と機能が失敗する可能性のある方法を実行する詳細なスクリプト化されたテスト プロトコルを確立します。 テストには、さまざまなシナリオでの適切な再現性テストも含まれており、機能が確実に機能することを保証します。	メーカーの文書: · 使用目的 · リスク判定 · 詳細な試験プロトコル · 実施されたテストの詳細なレポート ・各テストケースの合否結果 · 見つかった問題とその処置 · 操作のパフォーマンスが許容できることを示す結論文 · テストが実施された日付、およびテストを実施した人 · 適切な署名機関の署名と日付。
使いやすさの特徴: · ソフトウェアは、ユーザーにアプリケーションのヘルプ メニューを提供します。	この機能は、ユーザーとシステムの対話を容易にし、すべてのシステム機能の使用を支援することを目的としています。	機能が意図したとおりに機能しないことで、安全性が損なわれるような品質上の問題が発生する可能性はほとんどあり	この機能は、メーカーがシステム機能の評価、サプライヤーの評価、および設置作業で既に実施した以上の追加の保証作業	メーカーの文書: · 使用目的 · リスク判定 · 評価の日付と誰が評価を行

		ません。 したがって、メーカーは、この機能が高いプロセスリスクをもたらさないと判断しました。	を必要としません。	ったか · 意図された用途とリスクを考慮して、パフォーマンスが許容できることを示す結論文。
レポート機能: · このソフトウェアは、クエリ（質問、特に公式になされた質問）を作成して実行し、さまざまなソースからのデータを結合してデータ マイニングを実行できます。 · ソフトウェアは、さまざまな統計分析とデータの要約を可能にします。 · ソフトウェアは、データからグラフを作成できます。 · ソフトウェアは、分析のレポートを生成する機能を提供します。	これらの機能は、ユーザーがデータ ソースをクエリしたり、さまざまなソースからのデータを結合したり、分析を実行したり、ビジュアルや要約を生成したりできるようにすることを目的としています。 これらの機能は、生産またはプロセスのパフォーマンスに直接影響を与えない監視およびレビュー目的でのデータの収集および記録を目的としています。 この例では、ソフトウェアは品質決定を通知することを意図していません。	これらの機能が意図したとおりに実行されない場合、品質上の問題（不完全または不適切なレポートなど）が発生する可能性がありますが、この例では、これらの機能は監視およびレビュー目的でデータを収集および記録することを目的としているため、安全性が損なわれることは予見できません。 生産やプロセスのパフォーマンスに直接影響を与えないもの。 したがって、メーカーは、これらの機能が高いプロセスリスクをもたらさないと判断しました。	レポート ソフトウェアのサプライヤーは、ソフトウェアがクエリを作成および実行し、さまざまなソースからのデータを結合してデータ マイニングを実行し、統計分析とデータ要約を実行し、グラフを作成し、レポートを生成する機能を検証しました。 さらに、メーカーはシステムの機能を評価し、サプライヤーの評価と設置作業を実施しました。 そのため、製造業者は、ソフトウェアのレポート機能は、これらの活動以外に追加の保証努力を必要としないと判断しました。	メーカーの文書: · 使用目的 · リスク判定 · 評価の日付と誰が評価を行ったか · 意図された用途とリスクを考慮して、パフォーマンスが許容できることを示す結論文。