Contains Nonbinding Recommendations

Computer Software Assurance for Production and Quality System Software

Guidance for Industry and Food and Drug Administration Staff

Document issued on September 24, 2025.

The draft of this document was issued on September 13, 2022.

For questions about this document regarding CDRH-regulated devices, contact the Compliance and Quality Staff at 301-796-5577 or by email at CaseforQuality@fda.hhs.gov. For questions about this document regarding CBER-regulated devices, contact the Office of Communication, Outreach, and Development (OCOD) at 1-800-835-4709 or 240-402-8010, or by email at ocod@fda.hhs.gov.

U.S. FOOD & DRUG ADMINISTRATION

U.S. Department of Health and Human Services
Food and Drug Administration
Center for Devices and Radiological Health
Center for Biologics Evaluation and Research

管理番号: BZLib-141
改訂番号: 2
名称: **Computer Software Assurance for Production and Quality System Software**
ﾍﾟｰｼﾞ数: 全 80ページ

【注記】

本書は、FDA が発行した英語原文を株式会社文善にて和文翻訳したものです。

翻訳文はできるだけ英語原文に忠実になるよう努めましたが、あくまでも英語原文を正とするものです。本書は規制の理解を補助する目的で作成したものであり、株式会社文善は翻訳文に誤りがないことについて保証いたしません。

原文の内容をご自身で必ず確認してください。株式会社文善は、本書を利用したことに起因して、何らかの損害が生じたとしても、これについては一切の責任を負いません。

本書に含まれる内容は、予告なしに変更されることがあります。

本書を含め、株式会社文善のサイト (https://bunzen.co.jp) では、電磁的記録・電子署名等に関する規制やガイダンスの翻訳を掲載しています。

本書、株式会社文善のサービス等への質問、コメント等は info1@bunzen.co.jp にお寄せください。

【本書の表記について】

文脈に応じ説明を補足した場合、〔 〕内にそれを記述しています。
読みやすさのために、論旨を補足するような文は適宜 ( ) に入れています。また”and”で並べられた単語を中黒点「・」、”or”で並べられた単語をスラッシュ「／」で区切る場合があります。なお、原文の「/」はそのまま訳文でも「/」にしています。
【訳注】には、訳又は内容についての説明を記載しています。

目次

Preface (序文)

This guidance represents the current thinking of the Food and Drug Administration (FDA or Agency) on this topic. It does not establish any rights for any person and is not binding on FDA or the public. You can use an alternative approach if it satisfies the requirements of the applicable statutes and regulations. To discuss an alternative approach, contact the FDA staff or Office responsible for this guidance as listed on the title page.	*本ガイダンスは、当該トピックについて、食品医薬品局 (FDA 又は当局) の現在の考えを示す。本ガイダンスは、いかなる者に対しても権利を与えたりするものではなく、FDA 又は公衆を拘束するものではない。適用される法令及び規制の要件を満たす限り、本ガイダンスで示された方法に代わる方法を用いてもよい。代替方法に関する相談については、表紙に挙げた本ガイダンスに責任を持つFDA 職員又はFDA 事務所に連絡されたい。*

I. Introduction[1] (序章 [1])

FDA is issuing this guidance to provide recommendations on computer software assurance for computers and automated data processing systems used as part of medical device production or the quality system. This guidance:	FDA は、医療機器の製造システム／品質システムの一部として使用されるコンピュータ及び自動データ処理システムのコンピュータソフトウェア保証 (computer software assurance) に関する推奨事項を示すために、本ガイダンスを発行する。本ガイダンスは以下のことを意図している。
• Describes “computer software assurance” as a risk-based approach to establish confidence in the automation used for production or quality systems, and identifies where additional rigor may be appropriate; and	• 「コンピュータソフトウェア保証」を、製造システム／品質システムに使用されるオートメーションの信用を確立するためのリスクベースアプローチとして説明するとともに、さらなる厳密さがどこで必要になるのかを明確にする。

[1] This guidance has been prepared by the Center for Devices and Radiological Health (CDRH) and the Center for Biologics Evaluation and Research (CBER) in consultation with the Center for Drug Evaluation and Research (CDER), Office of Combination Products (OCP), and Office of Inspections and Investigations (OII).
[1] 本ガイダンスは、Center for Devices and Radiological Health (CDRH) 及び Center for Biologics Evaluation and Research (CBER) が、Center for Drug Evaluation and Research (CDER)、Office of Combination Products (OCP) 及び Office of Inspections and Investigations (OII)と協議して作成したものである。

• Describes various methods and testing activities that may be applied to establish computer software assurance and provide objective evidence to fulfill regulatory requirements, such as computer software validation requirements in quality system obligations, including requirements in 21 CFR Part 820 (hereafter referred to as "Part 820").[2]	• コンピュータソフトウェア保証を確立し、規制要件を満たす客観的証跡を得るための様々な方法やテスト活動について説明する[2]。ここで、規制要件は、quality system obligations（21 CFR Part 820 (以下、Part 820) 要件を含む）におけるコンピュータソフトウェアバリデーション要件等である。
This guidance supplements FDA's guidance, "General Principles of Software Validation" (hereafter referred to as the "Software Validation guidance") except this guidance supersedes Section 6: Validation of Automated Process Equipment and Quality System Software of the Software Validation guidance.	本ガイダンスは、FDA のガイダンス「General Principles of Software Validation」(以下、Software Validation guidance) を補足するものであるが、Software Validation guidance の第 6 章「自動プロセス機器及び品質システムソフトウェアのバリデーション」 は、本ガイダンスにより置き換えられる。 【訳注】FDA の General Principles of Software Validation の和訳については、https://bunzen.co.jp/ 参照。
For the current edition of the FDA-recognized consensus standard referenced in this document, see the FDA Recognized Consensus Standards Database.[3]	本文書で参照されている FDA の認定合意規格の最新版は、FDA Recognized Consensus Standards Database[3] を参照のこと。

[2] On February 2, 2024, FDA issued a final rule amending the device Quality System Regulation, 21 CFR Part 820, to align more closely with international consensus standards for devices (89 FR 7496, available at https://www.federalregister.gov/d/2024-01709). This final rule will take effect on February 2, 2026. Once in effect, this rule will withdraw the majority of the current requirements in Part 820, including 21 CFR 820.70, and instead incorporate by reference the 2016 edition of the International Organization for Standardization (ISO) 13485, Medical devices - Quality management systems – Requirements for regulatory purposes, in Part 820. As stated in the final rule, the requirements in ISO 13485 are, when taken in totality, substantially similar to the requirements of the current Part 820, providing a similar level of assurance in a firm's quality management system and ability to consistently manufacture devices that are safe and effective and otherwise in compliance with the Federal Food, Drug, and Cosmetic Act (FD&C Act). When the final rule takes effect, FDA will also update this guidance, including the references to provisions in Part 820 in this guidance, to be consistent with the rule.
[2] 2024 年 2 月 2 日、FDA は、医療機器の国際コンセンサス標準にさらに沿うよう医療機器品質システム規制 (21 CFR Part 820) を改正する最終規則を発行した (https://www.federalregister.gov/d/2024-01709 の、89 FR 7496 で入手可能)。この最終規則は 2026 年 2 月 2 日に発効する。この規則の発効により、21 CFR 820.70 を含む、Part 820 の現在の要件の大部分が撤回され、代わりに、Part 820 に International Organization for Standardization (ISO) 13485, Medical devices - Quality management systems – Requirements for regulatory purposes の 2016 年版が参照により組み込まれることになる。最終規則に記載されているように、ISO 13485 の要件は、全体として見ると、現在の Part 820 の要件と実質的に同様であり、企業の品質管理システムと、安全で効果的であり、Federal Food, Drug, and Cosmetic Act (FD&C Act) に準拠した医療機器を一貫して製造する能力について、同様のレベルの保証を提供する。最終規則が発効すると、FDA は、本ガイダンス内の Part 820 の規定への参照を含め、本ガイダンスも規則と一致するように更新される。

[3] Available at https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfStandards/search.cfm

In general, FDA's guidance documents do not establish legally enforceable responsibilities. Instead, guidances describe the Agency's current thinking on a topic and should be viewed only as recommendations, unless specific regulatory or statutory requirements are cited. The use of the word *should* in Agency guidances means that something is suggested or recommended, but not required.	一般的に、FDA のガイダンスは、法的強制力のある責任を確立するものではない。むしろガイダンスは、あるトピックに関する FDA の現在の考え方を説明するものであり、特定の規制又は法的要件が引用されていない限り、単なる推奨事項と見なされるべきものである。FDA のガイダンスで「*should*」【訳注】を用いているときは、何かを提案又は推奨しているものの、必須ではないことを意味する。 【訳注】「should」は「～べきである」「～必要がある」と訳し、「must」は「～なければならない」と訳している。

II. Background (バックグラウンド)

FDA envisions a future state where the medical device ecosystem is inherently focused on device features and manufacturing practices that promote product quality and patient safety. FDA has sought to identify and promote successful manufacturing practices and help device manufacturers raise their manufacturing quality level. In doing so, one goal is to help manufacturers produce high-quality medical devices that align with the laws and regulations implemented by FDA. Compliance with quality system obligations including those in Part 820 is required for manufacturers of finished medical devices to the extent they engage in operations to which those obligations apply. Quality system obligations include requirements for medical device manufacturers to develop, conduct, control, and monitor production processes to ensure that a device conforms to its specifications,[4] including requirements for manufacturers to validate computer software used as part of production or the quality system for its intended use.[5,6] The recommendations on computer software assurance in this guidance are intended to promote product quality and patient safety, and correlate to higher-quality outcomes. This guidance addresses practices relating to computers and automated data processing systems used as part of production or the quality system.	FDA は、医療機器のエコシステムにおいて、医療機器の機能要素や製造慣行が、当たり前のように製品の品質と患者の安全を促進することに重点を置くような未来を思い描いている。FDA は、成功している製造慣行を見つけて広めていくことで医療機器製造業者の製造品質レベル向上を支援しようとしてきた。そこでのゴールの一つは、製造業者を支援し、FDA の施行する法律及び規制に沿った高品質の医療機器を製造できるようにすることである。医療機器最終製品の製造業者は、該当する業務に従事する範囲で、quality system obligations（Part 820 の obligations を含む）に準拠することが求められる。Quality system obligations には、医療機器製造業者が製造プロセスを開発、実施、コントロール及び監視し、医療機器が仕様に適合していることを確実にするという要件[4] があり、そこには製造システム／品質システムの一部として利用されるコンピュータソフトウェアを意図した用途に対してバリデーションを行うことという要件が含まれる[5,6]。本ガイダンスにおけるコンピュータソフトウェア保証に関する推奨事項は、製品の品質と患者の安全を促進し、より高品質の結果につながることを目的としている。本ガイダンスでは、製造システム／品質システムの一部として使用されるコンピュータ及び自動データ処理システムに関する慣行を取り扱う。

[4] See 21 CFR 820.70.
[5] See 21 CFR 820.70(i).
[6] This guidance discusses the “intended use” of computer software used as part of production or the quality system (see 21 CFR 820.70(i)), which is different from the intended use of the device itself (see 21 CFR 801.4).
[6] 本ガイダンスでは、製造システム／品質システムの一部として使用されるコンピュータソフトウェアの「意図した用途」（21 CFR 820.70(i) を参照）について説明する。これは、医療機器自体の意図した用途（21 CFR 801.4 を参照）とは異なる。

In recent years, advances in manufacturing technologies, including the adoption of automation, robotics, simulation, and other digital capabilities, have allowed manufacturers to reduce sources of error, optimize resources, and reduce patient risk. FDA recognizes the potential for these technologies to provide significant benefits for enhancing the quality, availability, and safety of medical devices, and has undertaken several efforts to help foster the adoption and use of such technologies. Specifically, FDA has engaged with stakeholders via the Medical Device Innovation Consortium (MDIC), site visits to medical device manufacturers, and benchmarking efforts with other industries (e.g., automotive, consumer electronics) to keep abreast of the latest technologies and to better understand stakeholders' challenges and opportunities for further advancement. As part of these ongoing efforts, medical device manufacturers have expressed a desire for greater clarity regarding the Agency's expectations for software validation for computers and automated data processing systems used as part of production or the quality system. Given the rapidly changing nature of software, manufacturers have also expressed a desire for a more iterative, agile approach for validation of computer software used as part of production or the quality system.	近年の自動化、ロボティクス、シミュレーション、その他のデジタル能力の採用等を含む製造技術の発展により、製造業者はエラーの発生元を減らし、リソースを最適化し、患者のリスクを軽減できるようになった。FDA は、医療機器の品質・可用性・安全性を向上させるうえで重大な役割を果たすであろう、これらの技術のポテンシャルを認識しており、これらの技術の採用と利用を促進するためにいくつかの取り組みを行ってきた。 具体的には、Medical Device Innovation Consortium (MDIC)、医療機器製造業者へのサイト訪問、及び他業界 (例：自動車、家電) とのベンチマーキングを通じてステークホルダと関わることで、最新技術に遅れを取らないようにするとともに、ステークホルダがさらに発展を遂げるうえでの課題や機会をより深く理解しようとしてきた。これらの継続的な取り組みにおいて、医療機器製造業者は、製造システム／品質システムの一部として使用されるコンピュータ及び自動データ処理システムのソフトウェアバリデーションについての当局の期待を明確化してほしいとの希望を表明していた。また製造業者は、急速に変化していくソフトウェアの性質を踏まえ、製造システム／品質システムの一部として使用されるコンピュータソフトウェアバリデーションにより反復的でアジャイルなアプローチを用いたいとの希望も表明していた。

Traditionally, software validation has often been accomplished via software testing and other verification activities conducted at each stage of the software development life cycle. However, as explained in FDA's Software Validation guidance, software testing alone is often insufficient to establish confidence that the software is fit for its intended use. Instead, the Software Validation guidance recommends that "software quality assurance" focus on preventing the introduction of defects into the software development process, and it encourages use of a risk-based approach for establishing confidence that software is fit for its intended use.	これまでのソフトウェアバリデーションは、多くの場合において、ソフトウェア開発ライフサイクルの各段階で実施されるソフトウェアテストやその他の検証活動を通じて達成されてきた。ただし、FDA の Software Validation guidance で説明しているように、ソフトウェアが意図した用途に適合していることの信用を確立するためには、ソフトウェアのテストだけでは不十分であることが多い。そこで Software Validation guidance は、〔テスト一辺倒でなく〕「ソフトウェア品質保証」においてソフトウェア開発プロセスに欠陥が入り込まないようにすることに重点を置くことを推奨し、リスクベースアプローチを使用してソフトウェアが意図した用途に適合していることの信用を確立するよう奨励している。
FDA believes that applying a risk-based approach to computer software used as part of production or the quality system would better focus manufacturers' quality assurance activities to help ensure product quality while helping to fulfill validation requirements. For these reasons, FDA is providing recommendations on computer software assurance for computers and automated data processing systems used as part of medical device production or the quality system. FDA believes that these recommendations will help foster the adoption and use of innovative technologies that promote patient access to high-quality medical devices and help manufacturers to keep pace with the dynamic, rapidly changing technology landscape, while promoting compliance with laws and regulations implemented by FDA.	製造業者が製造システム／品質システムの一部として使用されるコンピュータソフトウェアにリスクベースアプローチを採用すれば、その品質保証活動において、バリデーション要件を満たしつつ製品の品質を確保することにもっと集中できるようになるであろう。FDA はこのような理由から、医療機器の製造システム／品質システムの一部として使用されるコンピュータ及び自動データ処理システムのコンピュータソフトウェア保証に関する推奨事項を提供するものである。これらの推奨事項が、患者に高品質な医療機器へのアクセスを促進するような革新的な技術の採用と使用を後押しし、製造業者がダイナミックかつ急速に変化する技術情勢に追随することを助け、かつ FDA の施行する法律及び規制への適合を推し進めることに役立つと考えている。

III. Scope (範囲)

This guidance provides recommendations regarding computer software assurance for computers or automated data processing systems used as part of production or the quality system for medical devices.	本ガイダンスは、医療機器の製造システム／品質システムの一部として使用されるコンピュータ又は自動データ処理システムのコンピュータソフトウェア保証に関する推奨事項を提供する。
This guidance is not intended to provide a complete description of all software validation principles. FDA has previously outlined principles for software validation, including managing changes as part of the software life cycle, in FDA's Software Validation guidance. This guidance applies the risk-based approach to software validation discussed in the Software Validation guidance to production or quality system software. This guidance additionally discusses specific risk considerations, acceptable testing methods, and efficient generation of objective evidence for production or quality system software through the life cycle of the medical device.	本ガイダンスは、ソフトウェアバリデーションのすべての原則を完全に説明することは意図していない。FDA は以前 Software Validation guidance で、ソフトウェアライフサイクルの一部として変更を管理することを含め、ソフトウェアバリデーションの原則を説明済みである。本ガイダンスでは、Software Validation guidance で説明されているソフトウェアバリデーションに対するリスクベースアプローチを、製造システム／品質システムのソフトウェアに適用している。本ガイダンスでは、医療機器のライフサイクルを通じて、具体的なリスク検討事項、許容可能なテスト方法、及び製造システム／品質システムのソフトウェアにおける客観的証跡の効率的な取得方法についても説明する。
This guidance does not provide recommendations for the design verification or validation requirements for device software functions, which are software functions that meet the definition of a device under section 201(h) of the Federal Food, Drug, and Cosmetic Act (FD&C Act). For more information regarding FDA's recommendations for the validation of medical device software, see the Software Validation guidance.	本ガイダンスは、医療機器ソフトウェア機能（すなわち Federal Food, Drug, and Cosmetic Act (FD&C Act) Section201(h) における医療機器の定義に該当するソフトウェア機能）の設計検証やバリデーション要件に関する推奨事項を提供するものではない。医療機器ソフトウェアのバリデーションに関する FDA の推奨事項の詳細については Software Validation guidance を参照のこと。

IV. Definitions (定義)

【訳注】この章の定義の訳は独立行政法人 情報処理推進機構 (IPA)の訳（SP 800-145, 2011 年 9 月）を参考にした。

The following definitions apply for the purposes of this guidance.[7]	本ガイダンスでは、以下の定義が適用される [7]。
Cloud Computing (Cloud): Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. The cloud is composed of three service models: software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS). The cloud model is also composed of four deployment models: private cloud, community cloud, public cloud, and hybrid cloud.[8]	**クラウドコンピューティング（クラウド）：**クラウドコンピューティングは、最小限の管理作業やサービスプロバイダとのやり取りで迅速にプロビジョニング及びリリースできる、構成設定可能なコンピューティングリソース（ネットワーク、サーバー、ストレージ、アプリケーション、サービス等）の共有プールへの、ユビキタスで便利なオンデマンドネットワークアクセスを可能にするモデルである。このクラウドモデルは、オンデマンド・セルフサービス、幅広いネットワークアクセス、リソースの共有、スピーディな拡張性、サービスが計測可能であること、という 5 つの重要な特性で構成されている。クラウドは、software as a service (SaaS)、platform as a service (PaaS)、infrastructure as a service (IaaS) の 3 つのサービスモデルで構成される。クラウドモデルは、さらにプライベートクラウド、コミュニティクラウド、パブリッククラウド、ハイブリッドクラウドの 4 つの実装モデルで構成される [8]。

[7] Some of the definitions originate from other FDA sources (e.g., Software Validation guidance) and are applicable in those instances.
[7] 一部の定義は、FDA の他の資料（Software Validation guidance 等）の定義を用いている。
[8] This definition is derived from the National Institute of Standards and Technology's "The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology," available at https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf
[8] この定義は、National Institute of Standards and Technology's "The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology," (https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf)に基づく。

Infrastructure as a service (IaaS): The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).[9]	**インフラストラクチャ・アズ・ア・サービス（サービスの形で提供されるインフラストラクチャ）IaaS:** 利用者に提供される機能は、演算機能、ストレージ、ネットワークその他の基礎的コンピューティングリソースを配置することであり、そこで、ユーザはオペレーティングシステムやアプリケーションを含む任意のソフトウェアを実装し走らせることができる。ユーザは基盤にあるインフラストラクチャを管理したりコントロールしたりすることはないが、オペレーティングシステム、ストレージ、実装されたアプリケーションに対するコントロール権を持ち、場合によっては特定のネットワークコンポーネント機器（例えば、ホストファイアウォール）についての限定的なコントロール権を持つ[9]。
Platform as a service (PaaS): The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider.[10] The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.[11]	**プラットフォーム・アズ・ア・サービス（サービスの形で提供されるプラットフォーム）PaaS:** 利用者に提供される機能は、クラウドのインフラストラクチャ上にユーザが開発したまたは購入したアプリケーションを実装することであり、そのアプリケーションはプロバイダがサポートするプログラミング言語、ライブラリ、サービス、およびツールを用いて生み出されたものである[10]。ユーザは基盤にあるインフラストラクチャを、ネットワークであれ、サーバーであれ、オペレーティングシステムであれ、ストレージであれ、管理したりコントロールしたりすることはない。一方ユーザは自分が実装したアプリケーションと、場合によってはそのアプリケーションをホストする環境の設定についてコントロール権を持つ[11]。

[9] Id.
[10] This capability does not necessarily preclude the use of compatible programming languages, libraries, services, and tools from other sources.
[10] この機能は、他のソースからの互換性のあるプログラミング言語、ライブラリ、サービス、及びツールの使用を必ずしも妨げるものではない。
[11] See footnote 8.
[11] 脚注 8 を参照。

Software as a service (SaaS): The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.[12]	**ソフトウェア・アズ・ア・サービス（サービスの形で提供されるソフトウェア）SaaS:** 利用者に提供される機能は、クラウドのインフラストラクチャ 2 上で稼動しているプロバイダ由来のアプリケーションである。アプリケーションには、クライアントの様々な装置から、ウェブブラウザのようなシンクライアント型インターフェイス（例えば、ウェブメール）、またはプログラムインターフェイスのいずれかを通じてアクセスする。ユーザは基盤にあるインフラストラクチャを、ネットワークであれ、サーバーであれ、オペレーティングシステムであれ、ストレージであれ、各アプリケーション機能ですら、管理したりコントロールしたりすることはない。ただし、ユーザに固有のアプリケーションの構成の設定はその例外となろう[12]。

[12] Id.

V. Computer Software Assurance (コンピュータソフトウェア保証)

Computer software assurance is a risk-based approach for establishing and maintaining confidence that software is fit for its intended use. This approach considers the risk of compromised safety and/or quality of the device (should the software fail to perform as intended) to determine the level of assurance effort and activities appropriate to establish confidence in the software. Because the computer software assurance effort is risk-based, it follows a least-burdensome approach, where the burden of validation is no more than necessary to address the risk. Such an approach supports the efficient use of resources, in turn promoting product quality.	コンピュータソフトウェア保証とは、ソフトウェアが意図した用途に適合しているという信用を確立し、維持管理するためのリスクベースアプローチである。このアプローチでは、（ソフトウェアが意図通りに機能しなくなったときの）医療機器の安全性、及び (又は) 品質が損なわれるリスクを考え、ソフトウェアに対する信用を確立するために適切な保証の取り組み・活動レベルを決定する。コンピュータソフトウェア保証の取り組みはリスクに基づくものであるため、最も負担が少ないアプローチに従う。すなわち、バリデーションの負担はリスクに対処するために必要最低限なものとする。このようなアプローチにより、リソースを効率的に使用できるようになり、結果的に製品の品質が向上する。
In addition, computer software assurance establishes and maintains that the software used in production or the quality system is in a state of control throughout its life cycle (“validated state”). This is important because manufacturers increasingly rely on computers and automated processing systems to monitor and operate production, alert responsible personnel, and transfer and analyze production data, among other uses. By allowing manufacturers to leverage principles such as risk-based testing, unscripted testing, continuous performance monitoring, and data monitoring, as well as validation activities performed by other entities (e.g., developers, suppliers, cloud service providers), the computer software assurance approach provides flexibility and agility in helping to provide assurance that the software maintains a validated state consistent with applicable quality system obligations.	さらに、コンピュータソフトウェア保証により、製造システム／品質システムで使用されるソフトウェアは、ライフサイクル全体にわたって、コントロールされた状態が確立され、維持管理される。製造業者が、製造の監視や操作、担当者への注意喚起、製造データの転送や分析等のためにコンピュータや自動処理システムにますます依存するようになっていることから、これは重要なことである。製造業者がリスクベーステスト、非スクリプトテスト、継続的パフォーマンス監視、データ監視等の考え方、さらに他組織 (例 : 開発者、供給者、クラウドサービスプロバイダ) によるバリデーション活動をうまく活用することでコンピュータソフトウェア保証アプローチは柔軟かつ迅速なものとなり、適用される quality system obligations に沿った、バリデーション済みの状態を維持管理することの保証に役立つであろう。

Software that is fit for its intended use and that maintains a validated state should perform as intended, helping to ensure that finished devices will be safe and effective and in compliance with regulatory requirements (see 21 CFR 820.1(a)(1)). Section V outlines a risk-based framework for computer software assurance.	意図した用途に適合し、バリデーション済みの状態が維持管理されたソフトウェアは、意図通りに動作し、最終製品が安全かつ効果的に規制要件 (21 CFR 820.1(a)(1) を参照) に適合することを確実にするであろう。V 章では、コンピュータソフトウェア保証のためのリスクベースフレームワークについて概説する。

A. Computer Software Assurance Risk Framework (コンピュータソフトウェア保証のリスクフレームワーク)

The following approach is intended to help manufacturers establish a risk-based framework for computer software assurance throughout the software's life cycle. The approach outlined can be applied, but is not limited, to automation tools (e.g., BOTS or automatic workflows), data analytic tools, artificial intelligence/machine learning tools, and cloud computing when used as part of production or the quality system.[13]	以下に示すアプローチは、製造業者がソフトウェアライフサイクル全体にわたってコンピュータソフトウェア保証のリスクベースフレームワークを確立することを支援するためのものである。このアプローチは、以下に適用可能であるが、これらに限定されるものではない[13]。 • 自動化ツール（BOTS や自動ワークフロー等） • データ分析ツール • 人工知能/機械学習ツール、及び • 製造システム／品質システムの一部として使用されるクラウドコンピューティング
Examples of applying this risk framework to various computer software assurance situations are provided in Appendix A.	付録 A に、このリスクフレームワークを、コンピュータソフトウェア保証を行うさまざまな場面に適用する例を示す。

[13] Cloud computing used as part of production or the quality system, including when supporting associated recordkeeping and manufacturing activities, is within the scope of this guidance. Cloud computing used as part of device software functions are not in the scope of this guidance.
[13]クラウドコンピューティングを製造システム／品質システムの一部として使用する場合（関連する記録管理や製造活動のサポートを含む）は、本ガイダンスが適用される。クラウドコンピューティングを医療機器ソフトウェア機能の一部として使用する場合は、本ガイダンスの適用範囲外である。

(1) Identifying the Intended Use (意図した用途の明確化)

The regulation requires manufacturers to validate software **that is used as part of production or the quality system** for its intended use (see 21 CFR 820.70(i)). This includes various cloud computing models related to computerized systems, such as IaaS, PaaS, and SaaS.	規制は、製造業者が、**製造システム／品質システムの一部として使用される**ソフトウェアをその意図した用途に対してバリデーションを行うことを求めている (21 CFR 820.70(i) を参照)。これには、IaaS、PaaS、SaaS といったコンピュータ化システムに関連するさまざまなクラウドコンピューティングモデルが含まれる。
To determine whether the requirement for validation applies, manufacturers must determine whether the software is or will be used as part of production or the quality system (whether directly or to support production or the quality system).	バリデーションが必要かどうかを判断するために、製造業者は、そのソフトウェアが製造システム／品質システムの一部として使用されているか、又は使用予定があるか（直接使用か、それとも製造システム／品質システムへのサポート使用か）を判断する必要がある。
Software with the following intended uses is considered to be used **directly** as part of production or the quality system:	ソフトウェアの意図した用途が以下である場合、製造システム／品質システムの一部としての**直接使用**であると見なされる。
• Software intended for automating production processes, inspection, testing, or the collection and processing of production data; and	• 製造プロセス、検査、テストの自動化、又は製造データの収集や処理を意図したソフトウェア。
• Software intended for automating quality system processes, collection and processing of quality system data, or maintaining a quality record established under applicable quality system obligations.	• 品質システムのプロセスの自動化、品質システムのデータの収集や処理、又は適用される quality system obligations に従って作成された品質記録の維持管理を意図したソフトウェア。
Software with the following intended uses is considered to be used to **support** production or the quality system:	ソフトウェアの意図した用途が以下である場合、製造システム／品質システムへの**サポート使用**であると見なされる。

• Software intended for use as development tools that test or monitor software systems or that automate testing activities for the software used as part of production or the quality system, such as those used for developing and running scripts or software embedded in the production equipment (e.g., firmware); and	• ソフトウェアシステムをテスト又は監視する開発ツールとして使用されるソフトウェア、又は製造システム／品質システムの一部として使用されるソフトウェアのテスト活動を自動化する開発ツールとして使用されるソフトウェア（例：スクリプトの開発・実行に用いられるソフトウェア）、又は（ファームウェア等の）製造設備に組み込まれたソフトウェア。
• Software intended for automating general record-keeping for production or the quality system that is not part of the quality record.	• 品質記録に含まれない、製造システム／品質システムの一般的な記録保管の自動化を意図したソフトウェア。
Both kinds of software are used as part of production or the quality system and must be validated under 21 CFR 820.70(i). However, as further discussed below, supporting software often carries lower risk, such that under a risk-based computer software assurance approach, the effort of validation may be reduced accordingly without compromising safety.	いずれの種類のソフトウェアも、製造システム／品質システムの一部として使用されており、21 CFR 820.70(i) に基づいてバリデーションを行わなければならない。ただし、以下で説明するように、サポートソフトウェアはリスクが低いことが多いため、リスクベースのコンピュータソフトウェア保証アプローチで、安全性を損なうことなく、リスクに応じてバリデーションの労力を低減することができる。
On the other hand, software with the following intended uses generally **is not** considered to be used as part of production or the quality system, such that the requirement for validation in 21 CFR 820.70(i) would not apply:	また、ソフトウェアの意図した用途が以下である場合、一般的に製造システム／品質システムの一部として使用されるとは見なされ**ない**ため、21 CFR 820.70(i) で求めるバリデーションは不要である。
• Software intended for management of general business processes or operations not specific to production or the quality system, such as email or accounting applications; and • Software intended for establishing or supporting infrastructure not specific to production or the quality system, such as networking, user authentication, or continuity of operations (e.g., backup and restore).	• 電子メールや会計アプリケーション等の、製造システム／品質システムに関連しない汎用ビジネスプロセス／業務の管理を意図したソフトウェア。 • 製造システム／品質システム専用ではないインフラストラクチャを確立／サポートするためのソフトウェア。例えば、ネットワーク、ユーザ認証、又は業務継続（バックアップ及びリストア等）。

FDA recommends manufacturers focus on the intended use of the software when considering cloud computing models, as not all cloud computing models are “directly” used as part of production or the quality system. For example, an IaaS cloud storage solution falls into the category of infrastructure, but may be used to store quality records established under applicable quality system obligations, in which case the IaaS cloud storage solution would be considered to be used directly as part of production or the quality system. In this example, FDA recommends manufacturers focus the assurance effort on the features or functions relevant to the integrity of the records and 21 CFR Part 11 requirements applicable to the records intended to be stored.	すべてのクラウドコンピューティングモデルが、製造システム／品質システムの一部として「直接」使用されるわけではないため、FDA は製造業者に対し、クラウドコンピューティングモデルを検討する際にソフトウェアの意図した用途に重点を置くことを推奨する。例えば、IaaS クラウドストレージソリューションは、インフラストラクチャとして分類されるが、関連する quality system obligations 下で作成された品質記録を保存するために使用される場合がある。この場合、IaaS クラウドストレージソリューションは、製造システム／品質システムの一部として直接使用されるものと見なされる。このような場合、FDA は製造業者に対し、記録のインテグリティの確保に有用な機能要素又は機能と、格納対象の記録に適用される 21 CFR Part 11 要件に保証の取り組みを集中させるよう推奨する。
Conversely, an IaaS cloud storage solution may support infrastructure to store production and process data; this would not be considered an established quality system record. In this example, the IaaS cloud storage solution does not support production or the quality system, and the requirement for validation in 21 CFR 820.70(i) would not apply. When storage of data in the cloud is independent of whether or not the data is part of the quality record, it is the manufacturer’s obligation to determine what the appropriate level of risk is for that application. Manufacturers may consider a least-burdensome approach to assuring the IaaS cloud storage solution is adequate for their business.	逆に、IaaS クラウドストレージソリューションのサポートするインフラストラクチャに格納されるデータが製造・プロセスデータである場合、これは確立された品質システム記録とは見なされない。この例では、IaaS クラウドストレージソリューションは製造システム／品質システムをサポートしていないため、21 CFR 820.70(i) で求めるバリデーションは不要となる。データを品質記録の一部であるかどうかとは無関係にクラウドへ格納している場合、アプリケーションのリスクレベルを適切に決定することは製造業者の責務である。製造業者は、IaaS クラウドストレージソリューションが自社のビジネスに適していることを保証するために負担が最も少なくなるアプローチを採用してよい。

FDA recognizes that software used in production or the quality system is often complex and comprised of multiple features, functions, and operations;[14] software may have one or more intended uses depending on the individual features, functions, and operations of that software. In cases where the individual features, functions, and operations of the software have different roles within production or the quality system, they may present different risks with different levels of validation effort. FDA recommends that manufacturers examine the intended uses of the individual features, functions, and operations to facilitate development of a risk-based assurance strategy. Manufacturers may decide to conduct different assurance activities for individual features, functions, or operations as related to the intended use.	FDA は、製造システム／品質システムで使用されるソフトウェアがしばしば複雑であり、複数の機能要素・機能・業務で構成されていることを認識している[14]。ソフトウェアの個々の機能要素・機能・業務に応じて、ソフトウェアには 1 つ又はそれ以上の意図した用途がある。ソフトウェアの個々の機能要素・機能・業務が、製造システム／品質システムにおいて異なる役割を果たす場合、もたらされるリスクはそれぞれで異なったものとなり、バリデーションの取り組みのレベルは異なるものとなるであろう。 FDA は、製造業者が、個々の機能要素・機能・業務の意図した用途を精査し、リスクベースの保証戦略を立案していくことを推奨する。意図した用途に応じて、機能要素／機能／業務ごとに異なる保証活動の実施を決定する場合もあるであろう。

[14] That is, software is often an integration of “features,” that are used together to perform a “function” that provides a desired outcome. Several functions of the software may, in turn, be applied together in an “operation” to perform practical work in a process.
[14]ソフトウェアは多くの場合「機能要素 (feature)」が統合されたものであり、「機能要素 (feature)」が集まって 1 つの「機能（function)」を実行する。「機能（function)」は求められる結果を提供する。ソフトウェアの複数の「機能（function)」が合わさって 1 つの「業務（operation)」に用いられる。「業務（operation)」は 1 つのプロセスにおける実用的な仕事を果たす。

For example, a commercial off-the-shelf (COTS) spreadsheet software may be comprised of various functions with different intended uses. When utilizing the basic input functions of the COTS spreadsheet software for an intended use of documenting the time and temperature readings for a curing process, a manufacturer may not need to perform additional assurance activities beyond those conducted by the COTS software developer and initial installation and configuration. The intended use of the software, "documenting readings," only supports maintaining a record of the process information and poses a low process risk. As such, initial activities such as the successful vendor assessment and software installation and configuration may be sufficient to establish that the software is fit for its intended use and maintains a validated state. However, if a manufacturer also utilizes built-in functions of the COTS spreadsheet to create custom formulas that are directly used in production or the quality system, then additional risks and data integrity considerations may be present. For example, if a custom formula automatically calculates time and temperature statistics to monitor the performance and suitability of the curing process, then additional validation by the manufacturer might be necessary.	例えば、市販 (COTS) 表計算ソフトウェアは、異なる意図した用途を持つ様々な機能から構成される。COTS 表計算ソフトウェアの基本的な入力機能において、その意図した用途が硬化プロセスの時間と温度の測定値を記録することである場合、COTS ソフトウェア開発者による保証活動、及び初期インストール・構成設定の他に追加的な保証活動は必要ないであろう。ソフトウェアの意図した用途である「測定値を記録すること」は、プロセス情報のひとつの記録を維持管理することをサポートするだけであり、それによりもたらされるプロセスリスクは低い。そのため、（成功裡に実施されたベンダアセスメントやソフトウェアのインストール・構成設定等の）初期活動により、ソフトウェアが意図した用途に適合し、バリデーション済みの状態を維持管理していることを十分に立証できるであろう。ただし、製造業者がその COTS 表計算ソフトウェアの組み込み関数を利用して、製造システム／品質システムで直接使用されるカスタム計算式を作成する場合、新たなリスクとデータインテグリティの検討事項が出てくる可能性がある。例えば、硬化プロセスのパフォーマンスと適切さを監視するためにカスタム計算式により時間と温度の統計を自動的に計算するような場合、製造業者は追加のバリデーションを実施する必要があるかもしれない。

For the purposes of this guidance, we describe and recommend a computer software assurance framework where manufacturers examine the intended uses of the individual features, functions, or operations of the software. However, in simple cases where software has only one intended use (e.g., if all of the features, functions, and operations within the software share the same intended use), manufacturers may not find it helpful to examine each feature, function, and operation individually. In such cases, manufacturers may develop a risk-based approach and consider assurance activities based on the intended use of the software overall. FDA recommends that manufacturers document their decision-making process for determining whether a software feature, function, or operation is or will be used as part of production or the quality system through their quality management system.	本ガイダンスでは、製造業者がソフトウェアの個々の機能要素／機能／業務の意図した用途を精査する、コンピュータソフトウェア保証フレームワークを説明し、かつ推奨する。ただし、ソフトウェアの意図した用途が 1 つしかない単純なケース (例：ソフトウェア内のすべての機能要素・機能・業務が、同じ意図した用途を共有している場合) では、機能要素・機能・業務を個別に精査する意味はないかもしれない。このような場合、製造業者は、リスクベースアプローチを実施し、ソフトウェア全体の意図した用途に基づいて保証活動を行うことを検討してもよいであろう。 FDA は、製造業者が自分たちの品質管理システムに沿ってソフトウェアの機能要素／機能／業務が製造システム／品質システムの一部として使用されているか、又は使用される予定であるかどうかを判断するための意思決定プロセスを文書化することを推奨する。

(2) Determining the Risk Based Approach (リスクベースアプローチの決定)

Once a manufacturer has determined that a software feature, function, or operation is or will be used as part of production or the quality system, FDA recommends using a risk-based analysis **to determine appropriate assurance activities**. Broadly, this risk-based approach entails systematically identifying reasonably foreseeable software failures, determining whether such a failure poses a high process risk, and systematically selecting and performing assurance activities commensurate with the medical device or process risk, as applicable. Manufacturers should select an appropriate frequency for performing assurance activities based on their risk-based analysis and accounting for their processes and procedures, as appropriate for the software and assurance activities	ソフトウェアの機能要素／機能／業務が、製造システム／品質システムの一部として使用されているか、又は使用される予定であると判断したら、リスクベース分析により**適切な保証活動を決定すること**を推奨する。大まかに述べると、このリスクベースアプローチとは、 • 合理的に予見可能なソフトウェア故障を体系的に特定し、 • その故障が高いプロセスリスクをもたらすかどうかを判断し、 • 必要に応じて医療機器リスク又はプロセスリスクに応じた保証活動を体系的に選択し、実施する、 というものである。製造業者は、保証活動の適切な実行頻度を、ソフトウェア及び実施される保証活動に応じて、かつリスクベース分析とプ

being performed.	ロセス及び手順の考慮に基づいて、選択する必要がある。
Note that conducting a risk-based analysis for computer software assurance for production or quality system software, as described in this guidance, is distinct from performing a risk analysis for a medical device as described in the International Organization for Standardization (ISO) 14971:2019 – *Medical devices – Application of risk management to medical devices*.	本ガイダンスで説明しているように、製造システム／品質システムソフトウェアのコンピュータソフトウェア保証のためのリスクベース分析は、International Organization for Standardization (ISO) 14971:2019 – *Medical devices – Application of risk management to medical devices* に記載されている医療機器のリスク分析とは異なることに注意すること。
The risk-based analysis for production or quality system software focuses on those factors that may impact or prevent the software from performing as intended, such as proper system configuration and management, security of the system, data integrity, data storage, data transfer, or operation error. A risk-based analysis for production or quality system software should consider which failures are reasonably foreseeable (as opposed to likely) and the risks resulting from each such failure. For example, in a risk-based analysis a manufacturer may consider the risks resulting from a power outage, which may not be likely to occur but is reasonably foreseeable to occur over the life cycle of a production or quality system. This guidance discusses both process risks and medical device risks. A process risk refers to the potential to compromise production or the quality system. A medical device risk refers to the potential for a device to harm the patient or user. When discussing medical device risks, this guidance focuses on the medical device risk resulting from a quality problem that compromises safety.	製造システム／品質システムソフトウェアのリスクベース分析では、ソフトウェアが意図通りに動作することに影響を与えたり、妨げたりするような要因（例えば、適切なシステム構成設定・管理、システムセキュリティ、データインテグリティ、データ格納、データ転送、操作エラー等）に焦点をあてる。製造システム／品質システムソフトウェアのリスクベース分析では、（どの故障が発生する可能性があるか、ではなく）どの故障が合理的に予見できるかを検討し、その故障によりもたらされるリスクを検討する必要がある。例えば、停電は、発生する可能性は低いものの、製造システム／品質システムのライフサイクル全体で発生することが合理的に予見できるため、リスクベース分析で停電によって生じるリスクを考慮するであろう。本ガイダンスでは、プロセスリスクと医療機器リスクの両方について述べている。医療機器リスクとは、機器が患者やユーザに危害を与える可能性を指す。本ガイダンスで医療機器リスクについて述べる場合、安全を損なうような品質問題によりもたらされる医療機器リスクに焦点をあてている。
Specifically, FDA considers a software feature, function, or operation to pose a high **process** risk **when its failure to perform as intended may result**	具体的に言うと、FDA は、ソフトウェアの機能要素／機能／業務が**意図通りに動作しないことにより、安全を損なうような品質問題が発生す**

in a quality problem that foreseeably compromises safety, meaning a medical device risk. This process risk identification step focuses only on the process, as opposed to the medical device risk posed to the patient or user. Examples of software features, functions, or operations that are generally **high process risk** are those that:	**る可能性がある場合（すなわち医療機器リスクが発生する可能性がある場合）**、そのソフトウェアの機能要素／機能／業務に高い**プロセスリスク**があると考える。このプロセスリスク特定ステップでは、患者又はユーザに対する医療機器リスクではなく、プロセスのみを考える。一般的に**プロセスリスクが高い**ソフトウェアの機能要素／機能／業務の例は以下のとおりである。
• Maintain process parameters (e.g., temperature, pressure, or humidity) that affect the physical properties of product or manufacturing processes that are identified as essential to device safety;	• 医療機器の安全に不可欠であると特定された製品又は製造プロセスの物理的特性に影響を与えるプロセスパラメータ (例：温度、圧力、湿度) を維持管理するもの。
• Measure, inspect, analyze and/or determine acceptability of product or process with limited or no additional human awareness or review;	• 製品又はプロセスの受入可能かどうかを測定、検査、分析、及び (又は) 決定を行うもので、人による確認やレビューが限定的か、行われていない場合。
• Perform process corrections or adjustments of process parameters based on data monitoring or automated feedback from other process steps without additional human awareness or review;	• データ監視又は他のプロセスステップからの自動フィードバックに基づいて、プロセスを修正する、又はプロセスパラメータを調整するもので、人による認識又はレビューが行われていない場合。
• Produce instructions for use or other labeling provided to patients and users that are necessary for safe operation of the medical device; and/or	• 医療機器の安全な操作に必要な、患者及びユーザに提供される使用説明書、又はその他のラベルを作成するもの。 及び (又は)
• Automate surveillance, trending, or tracking of data that the manufacturer identifies as essential to device safety (e.g., cybersecurity) and quality.	• 製造業者が医療機器の安全性と品質に不可欠であると特定したデータの監視、傾向分析、又は追跡を自動化するもの（サイバーセキュリティ等）。
In contrast, FDA considers a software feature, function, or operation not to pose a high process risk **when its failure to perform as intended would not result in a quality problem that foreseeably**	対照的に、FDA は、ソフトウェアの機能要素／機能／業務が**意図通りに動作しなくても、安全性を損なうことが予見できる品質問題につながらない**場合、高いプロセスリスクはないと考え

compromises safety. This includes situations **where failure to perform as intended would not result in a quality problem**, as well as situations **where failure to perform as intended may result in a quality problem that does not foreseeably lead to compromised safety**. Examples of software features, functions, or operations that generally are **not high process risk** include those that:	ている。これには、**意図通りに動作しなくても品質問題が生じない場合**、及び**意図通りに動作せず品質問題が引き起こされたとしても安全性を損なうことが予見できない**場合が含まれる。一般的にプロセスリスクが高くないソフトウェアの機能要素／機能／業務の例は以下のとおりである。
• Collect and record data from the process for monitoring and review purposes that do not have a direct impact on production or process performance;	• 監視及びレビューの目的でプロセスからデータを収集・記録するもので、製造又はプロセスのパフォーマンスに直接影響を与えないもの。
• Are used as part the quality system for Corrective and Preventive Actions (CAPA)routing, automated logging/tracking of complaints, automated change control management, or automated procedure management;	• 品質システムの一部として使用されるもの。是正及び予防措置 (CAPA) の回付、自動化された苦情記録/追跡、自動化された変更コントロール管理、自動化された手順管理等。
• Are intended to manage data (process, store, and/or organize data), automate an existing calculation, increase process monitoring, or provide alerts relevant to managing data when an exception occurs in an established process; and/or	• データを管理 (データを処理、格納、及び（又は）整理) するもの、既存の計算を自動化するもの、プロセス監視を強化するもの、確立されたプロセスで例外が発生したときにデータ管理に関連する警報を出すもの。 及び (又は)
• Are used to support production or the quality system, as explained in Section V.A.1 above.	• 上記 V.A.章で説明されているように、製造システム／品質システムをサポートするために使用されるもの。
FDA acknowledges that process risks associated with software used as part of production or the quality system are on a spectrum, ranging from high process risk to low process risk. Manufacturers should determine the risk of each software feature, function, or operation as the risk falls on that spectrum, depending on the intended use of the software. FDA is primarily concerned with the	製造システム／品質システムの一部として使用されるソフトウェアのプロセスリスクは、高いプロセスリスクから低いプロセスリスクまでのスペクトラムのどこかにある。製造業者は、ソフトウェアの意図した用途に照らして、ソフトウェアのそれぞれの機能要素／機能／業務のリスクがスペクトラム上のどこに位置するかを決定する必要がある。FDA の主な関心は、高いプ

review and assurance for those software features, functions, and operations that are high process risk because a failure also poses a medical device risk. For the purposes of this guidance, FDA is presenting the process risks in a binary manner, “high process risk” and “not high process risk.” A manufacturer may still determine that a process risk is, for example, “moderate,” “intermediate,” or even “low” for purposes of determining assurance activities; in such a case, the portions of this guidance concerning “not high process risk” would apply. As discussed in Section V.A.4 below, assurance activities should be conducted for software that is “high process risk” commensurate with the medical device risk and “not high process risk” commensurate with the process risk.	ロセスリスクのソフトウェアの機能要素・機能・業務が、レビューされ、かつ保証されているかどうかである。というのは、故障が医療機器リスクにもつながるためである。本ガイダンスで FDA はプロセスリスクを「高いプロセスリスク」と「高くないプロセスリスク」という 2 つに分けて説明している。製造業者は、保証活動を決定する際に、プロセスリスクを、例えば、「中 (moderate)」、「中間 (intermediate)」、さらに「低 (low)」のように分けてもよく、それらには本ガイダンスの「高くないプロセスリスク」に関する部分が適用される。下記 V.A.4 章で説明するように、ソフトウェアの保証活動は、医療機器リスクに相当する「高いプロセスリスク」と「高くないプロセスリスク」それぞれでプロセスリスクに応じたものとする必要がある。
Example: An Enterprise Resource Planning (ERP) Management system contains a feature that automates manufacturing material restocking. This feature automates material ordering and delivery to appropriate production operations. However, a qualified person checks the materials before their use in production. The failure of this feature to perform as intended may result in a mix-up in restocking and delivery, which would be a quality problem because the wrong materials would be restocked and delivered. However, the delivery of the wrong materials to the qualified person should result in the rejection of those materials before use in production; as such, the quality problem should not foreseeably lead to compromised safety. The manufacturer identifies this as an intermediate (not high) process risk and determines assurance activities commensurate with the process risk. The manufacturer has performed an evaluation of the ERP vendor, the ERP system information, and has	*例* : ERP 管理システムは、製造資材の補充を自動化する機能要素を持つ。この機能要素により、材料の適切な製造オペレーションへの発注と配送が自動化される。ただし、qualified person が製造に使用する前に材料をチェックしている。この機能要素が意図通りに動作しない場合、補充と配送で取り違えが生じる可能性があり、間違った材料が補充・配送されかねないことから、品質問題につながる可能性がある。ただし、間違った材料が qualified person に配送されたとしても、それらの材料は製造に使用される前に却下されるであろう。そのため、品質問題によって安全性が損なわれるとは予見できない。〔この例における〕製造業者は、これを中間の (高くない) プロセスリスクとし、プロセスリスクに応じた保証活動を決定する。当該製造業者は、ERP ベンダ、ERP システム情報の評価、自社の業務に合わせた ERP システムの構成設定を実施済みであることから、材料の発注と配送の自動化に関連する残りの保証活動を実

configured the ERP system for its operations. The manufacturer implements any remaining assurance activities associated with the material order and delivery automation.	施する。
Example: A similar feature in another ERP management system performs the same tasks as in the previous example except that it also automates checking the materials before their use in production. A qualified person does not check the material first. The manufacturer identifies this as a high process risk because the failure of the feature to perform as intended may result in a quality problem that foreseeably compromises safety. As such, the manufacturer will determine assurance activities that are commensurate with the related medical device risk. The manufacturer has previously performed assurance activities on the material identification data system, the automated material scanning systems (barcode scanners), evaluated the ERP vendor/information, and has configured the ERP system for their operations. The manufacturer implements any remaining assurance activities associated with the ordering and delivery automation.	*例*： 別の ERP 管理システムにおける同様の機能要素は、前の例と同じタスクを実行するが、製造で使用する前の材料チェックも自動化している。qualified person は事前に材料をチェックしていない。機能要素が意図通りに動作しないと、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るため、〔この例における〕製造業者はこれを高いプロセスリスクと分類する。そのため、製造業者は、関連する医療機器リスクに応じた保証活動を決定する。当該製造業者は既に材料識別データシステム、自動材料スキャンシステム（バーコードスキャナー）に関する保証活動、ERP ベンダ/情報の評価、業務に合わせた ERP システムの構成設定を実施済みであることから、発注と配送の自動化に関連する残りの保証活動を実施する。
Example: An ERP management system contains a feature to automate product delivery. The medical device risk depends upon, among other factors, the correct product being delivered to the device user. A failure of this feature to perform as intended may result in a delivery mix-up, which would be a quality problem that foreseeably compromises safety; as such, the manufacturer identifies this as a high process risk. Since the failure would compromise safety, the manufacturer will next determine the related increase in medical device risk and identify the assurance activities that are commensurate with	*例：* ある ERP 管理システムには、製品配送を自動化する機能要素が含まれている。医療機器リスクは、（他の要因もあるものの）医療機器の利用者に適切な製品が届けられるかどうかに依存する。この機能要素が意図通りに動作しない場合、誤配送が発生する可能性がある。これは品質問題であり、安全性が損なわれることが予見できる。そのため、製造業者はこれを高いプロセスリスクとして分類する。次に、故障により安全性が損なわれるということで関連する医療機器リスクを引き上げ、その医療機器リスクに応じた保証活動を特定する。〔この例にお

the medical device risk. In this case, the manufacturer has not already implemented any of the identified assurance activities, so the manufacturer implements all of the assurance activities identified in the analysis.	ける〕製造業者が、挙げられた保証活動をいずれも未実施であり、分析で挙げられたすべての保証活動を実施する。
Example: An automated graphical user interface (GUI) function in the production software is used for developing test scripts based on user interactions and to automate future testing of modifications to the user interface of a system used in production. A failure of this GUI function to perform as intended may result in implementation disruptions and software updates to the production system being delayed, but in this case, these errors should not foreseeably lead to compromised safety because the GUI function operates in a separate test environment. The manufacturer identifies this as a low (not high) process risk and determines assurance activities that are commensurate with the process risk. The manufacturer already undertakes some of those identified assurance activities so implements the remaining identified assurance activities.	*例*： 製造ソフトウェアの自動グラフィカルユーザインターフェース (GUI) 機能は、ユーザインターフェースに基づくテストスクリプトを開発し、製造で使用されるシステムのユーザインターフェースに対する変更の（将来の）テストを自動化する目的で使用されている。この GUI 機能が意図通りに動作しない場合、実装が中断され、製造システムのソフトウェア更新が遅延する可能性がある。ただし、この場合 GUI 機能は別のテスト環境では動作するため、エラーにより安全性が損なわれるとは予見できない。〔この例における〕製造業者は、これを低い (高くない) プロセスリスクとして分類し、プロセスリスクに応じた保証活動を決定する。当該製造業者は挙げられた保証活動の一部を既に実施済みであり、残りの保証活動を実施する。

(3) Production or Quality System Software Changes
(製造システム／品質システムのソフトウェアの変更)

For devices with approved premarket approval applications (PMA) or humanitarian device exemptions (HDE), PMA/HDE supplements are not required for changes to the manufacturing procedure or method of manufacturing that do not affect the safety or effectiveness of the device if they are reported to FDA in a periodic report (usually referred to as an annual report).[15] PMA/HDE supplements also are not required for modifications to manufacturing procedures or methods of manufacture that affect the safety and effectiveness of the device; these are submitted in a 30-day notice.[16] Changes to the manufacturing procedure or method of manufacturing may include changes to software used in production or the quality system. For an addition or change to software used in production or the quality system of devices with approved PMAs or HDEs, FDA recommends that manufacturers apply the principles outlined above in Section V.A.2 in determining whether the change may affect the safety or effectiveness of the device. In general, if a change may result in a quality problem that foreseeably compromises safety, then it should be submitted in a 30-day notice. If a change would not result in a quality problem that foreseeably compromises safety, then the change may be appropriate to report in an annual report.[17]	承認された premarket approval applications (PMA) 又は humanitarian device exemptions (HDE) の対象となる医療機器については、製造手順又は製造方法の変更で医療機器の安全性又は有効性に影響を与えないものは定期報告書 (通常、annual report と呼ばれる) で FDA に報告すれば、PMA/HDE supplements は不要である[15]。医療機器の安全性と有効性に影響を与える製造手順又は製造方法を調整 (modification) する場合にも PMA/HDE supplements は不要であり、30-day notice を提出することになる[16]。製造手順又は製造方法の変更には、製造システム／品質システムに使用されるソフトウェアの変更が含まれることがある。PMA／HDE 承認済の医療機器の製造システム／品質システムで使用されるソフトウェアへ追加又は変更する場合、その変更が医療機器の安全性又は有効性に影響する可能性があるかどうかを判断する際に、上記 V.A.2 章の原則を適用することを推奨する。一般的に、変更により、安全性を損なうことが予見できる品質問題が引き起され得るのであれば、30-day notice に含める必要がある。その変更が、安全性を損なうことが予見できる品質問題につながらない場合は、annual report で報告することが適切であろう。

[15] 21 CFR 814.39(b), 814.108, and 814.126(b)(1), and the "Annual Reports for Approved Premarket Approval Applications (PMA)" guidance.
[16] 21 CFR 814.39(f), 814.108, and 814.126(b)(1). Changes in manufacturing/sterilization site or to design or performance specifications do not qualify for a 30-day notice, see 21 CFR 814.39(a).
[16] 21 CFR 814.39(f), 814.108, 及び 814.126(b)(1)。製造/滅菌場所の変更、又は設計や性能仕様の変更については、30-day noice の対象にはならない。21 CFR 814.39(a) を参照のこと。
[17] Manufacturers should also consult the "Enforcement Policy for Certain Supplements for Approved Premarket Approval (PMA) or Humanitarian Device Exemption (HDE) Submissions" guidance…
【訳注】脚注 17 は本書末尾に掲載した。

For example, a Manufacturing Execution System (MES) may be used to manage workflow, track progress, record data, and establish alerts or thresholds based on validated parameters, which are part of maintaining the quality system. Failure of such an MES to perform as intended may disrupt operations but not affect the process parameters established to produce a safe and effective device. Changes affecting these MES operations are generally submitted in annual reports. In contrast, an MES used to automatically control and adjust established critical production parameters (e.g., temperature, pressure, process time) may be a change to a manufacturing procedure that affects the safety or effectiveness of the device. If so, changes affecting this specific operation would be submitted in a 30-day notice.	例えば、製造実行システム (MES) は、品質システムの維持活動の一環として、ワークフローの管理、進捗状況の追跡、データの記録、及びバリデーション済みのパラメータに基づく警報／しきい値の確立に利用できる。このようなMES が意図通りに動作しない場合、業務が中断される可能性はあるものの、安全かつ有効な医療機器を製造するために確立されたプロセスパラメータには影響しない。一般的にこういったMES の運用に影響するような変更は、annual reports で報告すればよいと考えられる。対照的に、確立された重要な製造パラメータ (例：温度、圧力、処理時間) を自動的にコントロール・調節するために使用される MES であれば、医療機器の安全性又は有効性に影響を与える製造手順の変更となる可能性があり、この業務に影響する変更は 30-day notice で提出されるであろう。

(4) Determining the Appropriate Assurance Activities (適切な保証活動の決定)

Once the manufacturer has determined whether a software feature, function, or operation poses a high process risk (a quality problem that may foreseeably compromise safety), the manufacturer should identify the assurance activities commensurate with the medical device risk or the process risk. In cases where the quality problem may foreseeably compromise safety (high process risk), the level of assurance should be commensurate with the medical device risk. In cases where the quality problem may not foreseeably compromise safety (not high process risk), the level of assurance rigor should be commensurate with the process risk. In either case, heightened risks of software features, functions, or operations generally entail greater rigor for assurance efforts (i.e., a greater amount of objective evidence). Conversely, relatively low risk (i.e., not high process	製造業者は、ソフトウェアの機能要素／機能／業務に高いプロセスリスク (安全性を損なうことが予見できる品質問題) があるかどうかを判断した後で、医療機器リスク又はプロセスリスクに応じた保証活動を明らかにする必要がある。品質問題が安全性を損なうことを予見できる(高いプロセスリスク) 場合、保証レベルは医療機器リスクに応じたものにする必要がある。品質問題が安全性を損なうことを予見できない(高くないプロセスリスク) 場合、保証の厳密さのレベルはプロセスリスクに応じたものにする必要がある。いずれの場合も、一般的に、ソフトウェアの機能要素／機能／業務のリスクが高くなると、保証の取り組みはより厳格となり、より多くの客観的な証跡が必要となる。逆に、安全性、及び (又は) 品質を損なうリスクが比較的低い (つまり、高くないプロセスリスク)

risk) of compromised safety and/or quality generally entails less collection of objective evidence for the computer software assurance effort.	場合、一般的に、コンピュータソフトウェア保証の取り組みのために収集すべき客観的な証跡は少なくなる。
A software feature, function, or operation that could lead to severe harm to a patient or user would generally be high medical device risk. In contrast, a feature, function, or operation that would not foreseeably lead to severe harm would likely not be high medical device risk. In either case, the risk of the software's failure to perform as intended is commensurate with the resulting medical device risk.	一般的に、患者又はユーザに重大な危害をもたらす可能性のあるソフトウェアの機能要素／機能／業務は、医療機器リスクが高い。対照的に、深刻な危害をもたらすことが予見できない機能要素／機能／業務は、医療機器リスクが高くないことが多い。いずれの場合も、ソフトウェアが意図通りに動作しない場合のリスクは、その結果として生じる医療機器リスクに比例したものとなる。
If the manufacturer instead determined that the software feature, function, or operation does not pose a high process risk (i.e., it would not lead to a quality problem that foreseeably compromises safety), the manufacturer should consider the risk relative to the process (i.e., production or the quality system). This is because the failure would not compromise safety, so the failure would not introduce additional medical device risk. For example, a function that collects and records process data for review would pose a lower process risk than a function that determines acceptability of product prior to human review.	ソフトウェアの機能要素／機能／業務に高いプロセスリスクがない (つまり、安全性を損なうことが予見できる品質問題につながらない) と判断した場合は、プロセス（すなわち製造システム／品質システム）に関するリスクを〔集中的に〕検討すべきである。これは、故障が安全性を損なわないため、故障による医療機器リスクの増大がないからである。例えば、レビューのためにプロセスデータを収集・記録する機能は、人がレビューする前に製品の合否を判定する機能よりもプロセスリスクが低い。
Types of manual or automated testing that may be considered as part of the assurance activities commonly performed by manufacturers include, but are not limited to, the following:	製造業者が一般的に実施する保証活動の一部として考えられる手動/／自動テストの種類には以下があるが、これらに限定されるものではない。
• **Unscripted testing:** Dynamic testing in which the tester's actions are not prescribed by written instructions in a test case.[18] It includes:	• **非スクリプトテスト：**テスト担当者のアクションが、テストケースの書面による指示に規定されない動的テスト[18]。以下が含まれる。

[18] IEC/IEEE/ISO 29119-1 Second edition 2022-01: Software and systems engineering – Software testing - Part 1: General Concepts, Section 3.133

♦ **Scenario Testing (Also referred to as Ad-Hoc Testing):** A specification-based test case design technique based on exercising sequences of interactions between the test item and other systems.[19] (Users are considered to be other systems in this context.)	♦ **シナリオテスト（アドホックテスト）：** 仕様ベースのテストケース設計手法[19]の一つであり、テスト項目と他システム(ユーザは他システムであると見なされる。) の間のやりとりを順序立てて実行する。
♦ **Experience-based testing:** Class of test case design techniques based on using the experience of testers to generate test cases.[20] Experience-based testing can include concepts such as test attacks, tours, and error taxonomies which target potential problems such as security, performance, and other quality areas,[21] and can include:	♦ **経験ベーステスト：**テストケース設計技法の種類[20]であり、テスト担当者の経験を利用してテストケースを生成する。経験に基づくテストには、セキュリティ、パフォーマンス、他の品質領域の潜在的な問題に焦点を当てた test attacks、tour、エラー分類等の概念[21]概念が含まれる場合がある。また、次のような内容も含まれる場合がある。
- **Error-guessing:** A test design technique in which test cases are derived on the basis of the tester's knowledge of past failures or general knowledge of failure modes. The relevant knowledge can be gained from personal experience, or can be encapsulated in, for example, a defects database or a "bug taxonomy."[22]	- **エラー推測：**テスト設計技法の一つであり、テスト担当者の過去の故障に関する知識、又は故障モードに関する汎用知識に基づいてテストケースを作成する。関連知識は、個人的な経験から得られる場合もあれば、欠陥データベースや「バグ分類」等にまとめられている場合もある[22]。
- **Exploratory testing:** Experience-based testing in which the tester spontaneously designs and executes tests based on the tester's existing relevant knowledge, prior exploration of the test item (including results from previous tests), and heuristic "rules of thumb" regarding common software behaviors and types of	- **探索的テスト：**テスト担当者が自発的にテストを設計及び実行するような経験ベーステストであり、テスト担当者の持っている関連知識、過去のテスト項目の探索(過去のテスト結果を含む)、及び一般的なソフトウェア動作や故障の種類についての自己経験をもとにした「大雑把なルー

[19] Id. at Section 3.72.
[20] Id. at Section 3.36.
[21] Id. at Section 4.4.5.
[22] Id. at Section 3.32.

failure. Exploratory testing looks for hidden properties, including hidden, unanticipated user behaviors, or accidental use situations that could interfere with other software properties being tested and could pose a risk of software failure.[23]	ル」に基づく。探索的テストは、隠れた特性（例えば、他のテスト対象ソフトウェア特性に干渉し、ソフトウェア故障リスクとなるような、表面化していない予想外のユーザ行動又は誤った利用状況）を見つけようとするものである[23]。
• **Scripted testing:** Testing in which test cases are recorded (e.g., document in a test management tool or in a spreadsheet) and can then be executed manually or executed automatically using an automated testing tool. The level of detail required for each test case and the evidence necessary to establish the software feature, function, or operation performs as intended depends on the risk posed by the software feature, function, or operation. For example, depending on the intended use, a more robust scripted testing where the test cases and evidence may include detailed requirements for repeatability, traceability, or auditability may be appropriate.	• **スクリプトテスト：**テストケースが（テスト管理ツール又はスプレッドシートの文書等に）記録され、それをもとに、手動で、又は自動テストツールを使用して自動で、実行できるテスト。ソフトウェアの機能要素／機能／業務が意図した通りに動作することを証明するために必要な各テストケースの詳細レベル、及び必要とされる証跡は、ソフトウェアの機能要素／機能／業務によってもたらされるリスクによって異なる。例えば、使用目的によっては、より堅固なスクリプト化されたテストが適切な場合があり、テストケースと証跡により再現性／追跡可能性／監査可能性に関する詳細な要件を満たすようにする。
This guidance describes a risk-based approach manufacturers may consider in meeting regulatory requirements. It is not an exhaustive list of software testing methods and principles. FDA recognizes that there are software testing methods and approaches, beyond those referenced in the guidance, that manufacturers have the flexibility to consider and utilize, as appropriate.[24]	本ガイダンスでは、製造業者が規制要件を満たすために考慮するリスクベースアプローチについて説明している。これはソフトウェアテストの方法と原則を網羅しているわけではなく、FDA は、本ガイダンスで言及されているもの以外にも、製造業者が必要に応じて検討し活用できる、柔軟性のあるソフトウェアテスト方法とアプローチがあることを認識している[24]。

[23] See id. at Section 3.37.
[24] For additional resources on current software testing methods and validation approaches, manufacturers may refer to various software standards and industry guidance, such as, but not limited to GAMP5 – A Risk-Based Approach to Compliant GxP Computerized Systems (Second Edition).
[24] 製造業者は、現在のソフトウェアテスト方法とバリデーションアプローチに関する追加リソースとして、GAMP5 – A Risk-Based Approach to Compliant GxP Computerized Systems (Second Edition) 等、さまざまなソフトウェア標準と業界ガイダンスを参照されたい。

For example, the "Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submission" guidance, which is applicable to devices with cybersecurity considerations and describes recommendations regarding the cybersecurity information to be submitted for devices under certain premarket submission types, includes recommendations for cybersecurity testing used to demonstrate the effectiveness of design controls. Manufacturers may consider utilizing the cybersecurity testing methods described in that guidance when conducting the assurance activities described in this guidance, as appropriate.	例えば、サイバーセキュリティについて考慮することが求められる医療機器に適用される「Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submission」ガイダンスには、一部の市販前申請において提出が求められるサイバーセキュリティ情報に関する推奨事項が記載されており、そこに設計コントロールの有効性を実証するためのサイバーセキュリティテストに関する推奨事項が含まれている。製造業者は、本ガイダンスに記載されている保証活動を実施する際に、必要に応じて、そのガイダンスに記載されているサイバーセキュリティテスト方法を活用することを検討するとよい。
In general, FDA recommends that manufacturers apply principles of risk-based testing in which the management, selection, prioritization, and use of testing activities and resources are consciously based on corresponding types and levels of analyzed risk to determine the appropriate activities. For high process risk software features, functions, and operations, manufacturers may choose to consider more rigor such as the use of scripted testing or a hybrid approach of scripted testing and unscripted testing, scaled as appropriate, when determining their assurance activities. In contrast, for software features, functions, and operations that are not high process risk, manufacturers may consider using unscripted testing methods such as scenario testing, error-guessing, exploratory testing, or a combination of methods that is suitable for the risk. The testing examples discussed for high process risk and not high process risk are not exclusive to those categories. Manufacturers should apply the principles of risk-based testing to determine the appropriate type of testing to perform. For example, unscripted testing may be better suited to assure the	一般的に、FDA は、製造業者がリスクベーステストの原則を適用することを推奨する。すなわち、適切な活動を決定するためにリスク分析し、そのリスクの種類とレベルに意識的に基づいてテスト活動とリソースを管理し、選択し、優先順位付けし、使用することである。プロセスリスクの高いソフトウェアの機能要素・機能・業務の保証活動を決定する際は、例えば、スクリプトテストを用いる、又はスクリプトテストと非スクリプトテストを、配分を適切に調整し、組み合わせるハイブリッドアプローチを用いる等〔保証活動を〕より厳密にすることを検討する。対照的に、プロセスリスクが高くないソフトウェアの機能要素・機能・業務については（シナリオテスト、エラー推測、探索的テスト、又はリスクに応じたこれらの方法の組み合わせ等の）非スクリプトテスト方法の使用を検討してもよい。プロセスリスクが高い場合と高くない場合について説明したテストの例は、それらのカテゴリに限定されるものではない。製造業者は、リスクベーステストの原則を適用して、実行する適切なテストの種類を決定すべきである。例えば、プロセスリスクの高い機能

software performs as intended even for high process risk features, functions, and operations. Conversely, a manufacturer may find it more effective and efficient to develop scripted testing and automate it for not high process risk features, functions, and operations.	要素・機能・業務の場合であっても、ソフトウェアが意図したとおりに動作することを保証するために非スクリプトテストが適している場合がある。逆に、プロセスリスクが高くない機能要素・機能・業務を、スクリプトテストを開発して自動化する方が効果的かつ効率的である場合もある。

(5) Additional Considerations for Assurance Activities (保証活動に関する追加の考慮事項)

When deciding on the appropriate assurance activities, manufacturers should consider whether there are any additional controls or mechanisms in place throughout the quality system that may decrease the impact of compromised safety and/or quality if failure of the software feature, function or operation were to occur. For example, as part of a comprehensive assurance approach, manufacturers can leverage the following to reduce the effort of additional assurance activities:	適切な保証活動を決定する際に、ソフトウェアの機能要素／機能／業務に故障が発生したときに、損なわれた安全性、及び (又は) 品質の影響を低減するような、追加的なコントロールやメカニズムが品質システム全体を通して設けられているかどうかを考慮する必要がある。例えば、包括的な保証アプローチの一環として、以下を活用することで追加的な保証活動の労力を削減できる。
• Activities and established processes that provide control in production or fully verify processes in which software is involved. Such activities may include procedures to ensure integrity in the data supporting production, subsequent inspection or testing, or software quality assurance processes performed by other organizational units.	• 製造をコントロールしたり、ソフトウェアの関与するプロセスを完全に検証したりするような活動、及び確立されたプロセス。このような活動の例には以下がある。 ◆ 製造をサポートするデータのインテグリティを確実にする手順 ◆ 製造後の検査／テスト、又は ◆ 他部門により実施されるソフトウェア品質保証プロセス

• Established purchasing control processes for selecting and monitoring software vendors. For example, the medical device manufacturer could incorporate the software development practices, validation work, and electronic information already performed by developers of the software as the starting point and determine what additional activities may be needed. For some lower-risk software features, functions, and operations, this may be all the assurance that is needed by the manufacturer.	• ソフトウェアベンダを選定及び監視するための確立された購買コントロールプロセス。例えば、医療機器製造業者は、〔ソフトウェアベンダの〕ソフトウェア開発慣行、バリデーション作業、及びソフトウェア開発者により既に実施された電子情報を最初の段階で〔自社の保証活動に〕組み込み、その上でさらに必要な活動を決定する。リスクの低いソフトウェアの機能要素・機能・業務であれば、医療機器製造業者に必要とされる保証は、これだけで済むかもしれない。
• Additional process controls, including activities to reduce cybersecurity exposure,[25] that have been incorporated throughout production. For example, if a process is fully understood, all critical process parameters are monitored, and/or all outputs of a process undergo verification testing, these controls can serve as additional mechanisms to detect and correct the occurrence of quality problems that may occur if a software feature, function, or operation were to fail to perform as intended. In this example, the presence of these controls can be leveraged to reduce the effort of assurance activities appropriate for the software.	• 製造全体に組み込まれた（サイバーセキュリティのエクスポージャ[25]を減らす活動を含む）追加的なプロセスコントロール。例えば、プロセスが十分に理解されているならば、すべての重要なプロセスパラメータが監視され、及び (又は) プロセスのすべての出力について検証テストが行われるが、これらのコントロールは、ソフトウェアの機能要素／機能／業務が意図通りに動作しないときに引き起こされる品質問題の発生を検出・修正するための追加的なメカニズムとして利用することができる。この例では、これらのコントロールが設けられていることを根拠にして、ソフトウェアに適した保証活動の労力を削減できる。

[25] See the "Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submission" guidance.

• The data and information periodically or continuously collected by the software for the purposes of monitoring or detecting issues and anomalies in the software after implementation of the software. The capability to monitor and detect performance issues or deviations and system errors may reduce the risk associated with a failure of the software to perform as intended and may be considered when deciding on assurance activities.	• ソフトウェア実装後に発生するソフトウェアの課題や異常を監視又は検出する目的で、ソフトウェアにより定期的又は継続的に収集されるデータ・情報。パフォーマンスの課題や逸脱、及びシステムエラーを監視・検出することができれば、ソフトウェアが意図通りに動作しないことによるリスクを低減できる可能性があり、保証活動を決定する際に考慮するとよい。
• The use of tools supporting software development and system life cycle activities (e.g., bug, anomaly tracking, requirement traceability tools) for the assurance of software used in production or as part of the quality system whenever possible.	• ソフトウェア開発やシステムライフサイクル活動をサポートするツール (例：バグ／異常追跡ツール、要件トレーサビリティツール) の利用。これらは、可能な範囲で、製造システム、又は品質システムの一部として使用されるソフトウェアを保証するために利用される。
• The use of testing and results done in iterative cycles and continuously throughout the life cycle of the software used in production or as part of the quality system.	• 製造システム、又は品質システムの一部として使用されるソフトウェアのライフサイクル全体にわたって反復的に、継続的に実施されるテスト及び結果の利用。
FDA recognizes that manufacturers may have limited access to information from the software vendor as part of an assessment and recommends manufacturers establish and apply a risk-based analysis of the software vendor as part of their assurance approach. The manufacturer's assessment may consider various sources of information when deciding the appropriate level of control for the software vendor (e.g., purchasing controls). To evaluate the vendor's capabilities, whether cloud-based, on premise, or a hybrid, the manufacturer may consider activities including but not limited to:	FDA は、〔ソフトウェアベンダの〕アセスメントにおいて、製造業者がソフトウェアベンダからの情報にアクセスできる範囲に限りがあることは認識しており、保証アプローチの一環として、ソフトウェアベンダのリスクベース分析を確立し、適用することを推奨する。ソフトウェアベンダに対する適切なコントロール（購買コントロール等）のレベルを決定する際に、製造業者は、アセスメントでさまざまな情報源を考慮することになるであろう。クラウドベース、オンプレミス、ハイブリッドのいずれであっても、ベンダの能力を評価するために、製造業者は次のような活動（ただし、これらに限定されるものではない）を考慮するとよい。

• Onsite audits of the vendor, if applicable. FDA acknowledges that it may not be feasible or appropriate for a device manufacturer to audit the software vendor. Manufacturers may consider any alternative combination of information, as applicable, in a risk-based analysis of the controls and capabilities of the software vendor;	• ベンダに対して訪問監査を行う（適切な場合のみ）。FDA は、ソフトウェアベンダを監査することが実現可能ではない、又は適切ではない可能性があることを認識している。製造業者は、ソフトウェアベンダのコントロールと機能に関するリスクベース分析では、必要に応じて、〔訪問監査に〕代わる情報の組み合わせを考慮することができる。
• Review of the vendor's accreditations and certifications (e.g., Service Organization Controls reports), and industry standard certifications (e.g., ISO certifications);	• ベンダの認定・認証（Service Organization Controls レポート等）、及び業界標準認証（ISO 認証等）をレビューする。
• Review of the vendor's practices and documentation for software development, software quality assurance, cybersecurity (e.g., security risk assessments, threat modeling, security design reviews, software bill of materials (SBOM), and testing) and risk mitigation; and	• ソフトウェア開発、ソフトウェア品質保証、サイバーセキュリティ（セキュリティリスクアセスメント、脅威モデリング、セキュリティ設計レビュー、ソフトウェア部品表（SBOM）、テスト等）、及びリスク軽減に関するベンダの慣行と文書資料をレビューする。
• Review of the vendor's or software's data integrity capabilities or controls such as, but not limited to: ◆ Retaining records, archiving data, and generating accurate and complete copies of records; ◆ Securing data at rest and in transit (i.e., maintaining secure, computer-generated, time-stamped audit trails of users' actions and changes to data, encrypting data); and/or ◆ Establishing and maintaining access controls, electronic signature controls and authorization checks for users' actions.	• データインテグリティに関するベンダ／ソフトウェアの能力／コントロールをレビューする（以下に限定されるものではない）。 ◆ 記録の保管、データのアーカイブ、記録の正確かつ完全なコピーの生成 ◆ 保存時及び転送時のデータのセキュリティ保護（すなわち、ユーザ操作とデータ変更〔を記録する〕安全な、コンピュータ生成のタイムスタンプ付き監査証跡の安全な維持管理、データの暗号化）、及び（又は） ◆ ユーザのアクションに対するアクセスコントロール、電子署名コントロール、及び承認チェックの確立・維持管理

A manufacturer should establish and maintain within its procedures the requirements it has for suppliers on the basis of their ability to meet specified requirements and define the type and extent of control to be exercised over the product, services, and suppliers. Manufacturers should consider appropriate sources of information regarding the vendor in their evaluation decision. FDA recommends that manufacturers establish a risk-based approach to the evaluation of the vendor of software or service, the evaluation activities, and the appropriate objective evidence to retain.	製造業者は、以下を実施すべきである。 • 自社の手順の一環として（供給者が提示された要件を満たす能力に基づいて）供給者に対する要件を確立・維持管理し、 • 製品、サービス、及び供給者に適用するコントロールの種類と範囲を定義する。 製造業者は、ベンダを評価判定する際に、ベンダに関する情報源が適切であることを考慮する必要がある。FDA は、製造業者に対し、以下についてリスクベースアプローチを確立することを推奨する。 • ソフトウェアベンダ／サービスベンダの評価判定、 • 評価活動、及び • 保管すべき適切な客観的証跡
For example, supporting software, as referenced in Section V.A.1, often carries lower risk, such that the assurance effort may generally be reduced accordingly. Because assurance activities used “directly” in production or the quality system often inherently cover the performance of supporting software, assurance that this supporting software performs as intended may be sufficiently established by leveraging vendor evaluation and validation records, software installation, or software configuration, such that additional assurance activities (e.g., scripted or unscripted testing) may be unnecessary.	例えば、V.A.1 章で参照されているようなサポートソフトウェアは、多くの場合、リスクが低いため、一般的に保証作業を相応に削減できるであろう。往々にして製造システム／品質システムに「直接」使用される保証活動は、ついでにサポートソフトウェアのパフォーマンスもカバーしてしまうことが多く、サポートソフトウェアが意図通りに動作することの保証が、ベンダの評価結果及びバリデーション記録、ソフトウェアのインストール、又はソフトウェアの構成設定を活用するだけで十分に確立できてしまい、追加的な保証活動 (例：スクリプトテスト又は非スクリプトテスト) が不要となる場合がある。

Example: A CAPA automation system is being written in Java script and a debugger tool is used to set up breakpoints and step through the code. Once the code is debugged, all the debugger content is removed prior to implementation. In this situation, the debugger tool is used to assist a software developer during the coding of a quality system but is not subject to quality system obligations because the COTS tool, which is not integrated with production or the quality system, is not used as part of production or the quality system. FDA recommends manufacturers establish a least-burdensome approach to ensure the tool performs as intended.	*例：* CAPA 自動化システムは Java スクリプトで記述されており、デバッガツールを使用してブレークポイントを設定し、コードをステップ実行する。コードがデバッグされた後は、すべてのデバッガコンテンツは実装前に削除される。このような場合、デバッガツールは品質システムのコーディング中にソフトウェア開発者を支援するために使用されるが、quality system obligations の対象にはならない。なぜならば製造システム／品質システムに組み込まれていない COTS ツールは、製造システム／品質システムの一部として使用されていないからである。FDA は、製造業者に対し、ツールが意図したとおりに機能することを確実にするために、最も負担の少ないアプローチを確立することを推奨する。
Example: A manufacturer is using a cloud storage solution for production data. The system has a network load specification, and a parameterization tool is used to simulate anticipated peak load of the production system. The load testing results shows objective evidence that the system can absorb the required user load and becomes part of the validation package. The parameterization tool is not the system of record of the testing result because it does not alter the code within the production system and the testing does not add any data to the production system. FDA recommends manufacturers establish a least-burdensome approach to ensure the tool performs as intended.	*例：*〔この例における〕製造業者は製造データにクラウドストレージソリューションを使用している。システムはネットワーク負荷に関する仕様に基づき、パラメータ化ツールを使用して、製造システムの予想されるピーク負荷をシミュレートする。負荷テストでは、システムが必要なユーザ負荷を吸収できることが客観的な証跡が示された。テスト結果はバリデーションパッケージの一部となる。 〔このような場合〕パラメータ化ツールは、テスト結果を記録するシステムとはみなされない。なぜなら、パラメータ化ツールは製造システム内のコードを変更するものでなく、またテストによって製造システムにデータが追加されるものではないからである。FDA は、製造業者に対し、ツールが意図したとおりに機能することを確実にするために、最も負担の少ないアプローチを確立することを推奨する。

Manufacturers are responsible for determining the appropriate assurance activities for ensuring the software features, functions, or operations maintain a validated state. The assurance activities and considerations noted above are some possible ways of providing assurance and are not intended to be prescriptive or exhaustive. Manufacturers may leverage any of the activities, or a combination of activities, that are most appropriate for risk associated with the intended use.	製造業者は、ソフトウェアの機能要素／機能／業務がバリデーション済みの状態を維持管理することを保証するための適切な保証活動を決定する責任を持つ。上記の保証活動と考慮事項は、保証を提供するための、いくつかの可能な方法であり、作業を細かに規定するものではなく、また網羅的でもない。製造業者は、意図した用途に関連するリスクに最も適した活動を一つ選ぶ、又は組み合わせて活用するとよい。

(6) Establishing the Appropriate Record (適切な記録の作成)

When establishing the record, the manufacturer should capture sufficient objective evidence to demonstrate that the software feature, function, or operation was assessed and performs as intended. In general, FDA recommends the record include the following:	製造業者が記録を作成する際、ソフトウェアの機能要素／機能／業務をアセスメントし、意図通りに動作したことを示す十分な客観的証跡を取得する必要がある。FDA は、一般的に、記録には次の内容を含めることを推奨する。
• The intended use of the software feature, function, or operation;	• ソフトウェアの機能要素／機能／業務の意図した用途。
• The result of the risk-based analysis of the software feature, function, or operation; and	• ソフトウェアの機能要素／機能／業務のリスクベース分析の結果。
• Documentation of the assurance activities conducted, including: ◆ A description of the testing conducted based on the assurance activity. ◆ Issues found during testing (e.g., deviations, defects, and/or failures).	• 実施された保証活動の文書資料。以下を含む： ◆ 保証活動に基づいて実施したテストの説明。 ◆ テスト中に発見された課題 (例：逸脱、故障) 。

• A conclusion statement declaring acceptability of the software for its intended use. If issues were found, FDA recommends including resolution of issues found as part of the conclusion statement. The manufacturer may consider including process controls implemented to address any impact from the issues to the intended use or appropriate risk justification addressing why the issues found will not impact the intended use.	• 意図した用途に対してソフトウェアが受入可能であることを宣言する結論。課題が見つかった場合、FDA は、結論の一部として、見つかった課題の解決策を含めることを推奨する。製造業者は、次のいずれかを含めることを検討する。 - その課題が意図した用途に与える影響に対処するために実装されたプロセスコントロール、又は - なぜ発見された課題が意図した用途に影響しないのかを述べる適切なリスクの合理的な説明
• Record of who performed testing/assessment and date the testing/assessment was performed.	• テスト/アセスメント実施者、及びテスト/アセスメント実施日付の記録。
• Established review and approval when appropriate (e.g., when necessary, a signature and date of an individual with signatory authority).	• 確立されたレビュー・承認 (例：必要に応じて、署名権限者の署名と日付) （適切な場合のみ)。
Documentation of assurance activities need not include more evidence than necessary to show that the software feature, function, or operation performs as intended for the risk identified. FDA recommends the record retain sufficient details of the assurance activity to serve as a baseline for improvements or as a reference point if issues occur.[26]	保証活動の文書資料に含める証跡は、特定されたリスクに対してソフトウェアの機能要素／機能／業務が意図通りに動作することを示すために必要なもの以外は不要である。FDA は、記録に保証活動の十分な詳細を盛り込むようにし、改善のためのベースラインや課題発生時の参照に用いることができるようにすることを推奨する[26]。

[26] For the Quality System regulation's general requirements for records, including record retention period, see 21 CFR 820.180.
[26] 記録保存期間を含む、記録に関する品質システム規則の一般要件については、21 CFR 820.180 を参照のこと。

Advances in digital technology may allow for manufacturers to leverage digital retention of results, automated traceability, automated testing, and electronic capture of work performed as objective evidence, reducing the need for manual or paper-based documentation. As a least-burdensome approach, **FDA recommends incorporating the use of digital records, such as system logs, audit trails, and other data generated and maintained by the software**, as opposed to paper documentation, screenshots, or duplicating results already digitally retained by the software when establishing the record associated with the assurance activities. When using digital records, FDA recommends manufacturers consider the intended use and the need for accuracy, reliability, integrity, availability, and authenticity of the record as part of the risk-based assurance approach established.	デジタル技術の進歩により、製造業者が、結果のデジタル保存、自動トレーサビリティ、自動テスト、及び客観的な証跡としての実施作業の電子キャプチャを活用できるようになり、手作業又は紙ベースの文書化の必要性は減ってきた。**FDA は、**最も負担が少ないアプローチとして、製造業者が保証活動に関連する記録を作成する際に、紙の文書資料、スクリーンショット、又はソフトウェアによって既にデジタル形式で保管されている結果の複製の代わりに、**（システムログ、監査証跡、及びソフトウェアによって生成及び維持管理されるその他のデータ、等の）デジタル記録の使用を〔保証活動に〕組み込むことを推奨する**。デジタル記録を使用する場合、FDA は、確立されたリスクベース保証アプローチの一環として、製造業者がデジタル記録の意図した用途、及び正確性 (accuracy)、信頼性 (reliability)、インテグリティ、可用性 (availability)、真正性 (authenticity) の必要性を考慮することを推奨する。
Table 1 provides some examples of ways to implement and develop the record when using the risk-based testing approaches, including testing approaches identified in Section V.A.4 above. Manufacturers may use alternative approaches and provide different documentation so long as their approach satisfies applicable legal documentation requirements.	表 1 は、上記 V.A.4 章で特定されたテストアプローチを含む、リスクベースのテストアプローチを使用する際に〔テストを〕実施し、記録を作成する方法の例をいくつか示している。製造業者は、該当する文書資料に関する法的要件を満たす限り、以下と異なるアプローチを使用し、以下と異なる文書資料を作成してもよい。 【訳注】見やすさのため、表の中に訳文を記載せずに、元の表の後に訳した表を続けた。Table 1 の訳は「表 1 - 保証活動と記録の例」参照。

Table 1 – Examples of Assurance Activities and Records

Assurance Activity	Test Plan	Test Results	Record (Including Digital)
Scripted Testing: Robust	• Test objectives • Test cases (step-by-step procedure) • Expected results • Independent review and approval of test plan when appropriate	• Result record obtained for each test case • Details regarding any failures/deviations found	• Intended use • Result of risk-based analysis • Detailed report of testing performed • Result for each test case • Issues found • Conclusion declaring acceptability of the software for its intended use, including the resolution or appropriate risk justification of issues found • Record of who performed testing and the date the testing was performed • Established review and approval when appropriate
Scripted Testing: Limited	• Limited test cases (step-by-step procedure) identified • Expected results for the test cases • Identify unscripted testing applied • Independent review and approval of test plan when appropriate	• Result record obtained for each test case • Details regarding any failures/deviations found	• Intended use • Result of risk-based analysis • Summary description of testing performed • Result for each test case • Issues found • Conclusion declaring acceptability of the software for its intended use, including the resolution or appropriate risk justification of issues found • Record of who performed testing and date the testing was performed • Established review and approval when appropriate
Unscripted Testing: Scenario Testing	• Testing of features and functions with no test plan	• Details regarding any failures/deviations found	• Intended use • Result of risk-based analysis • Summary description of features and functions tested, and testing performed • Issues found • Conclusion declaring acceptability of the software for its intended use, including the resolution or appropriate

Assurance Activity	Test Plan	Test Results	Record (Including Digital)
			risk justification of issues found • Record of who performed testing and date the testing was performed • Established review and approval when appropriate
Unscripted Testing: Error guessing	• Testing of failure-modes with no test plan	• Details regarding any failures/ deviations found	• Intended use • Result of risk-based analysis • Summary description of failure-modes tested, and testing performed • Issues found • Conclusion declaring acceptability of the software for its intended use, including the resolution or appropriate risk justification of issues found • Record of who performed testing and date the testing was performed • Established review and approval when appropriate
Unscripted Testing: Exploratory Testing	• Establish high level test plan objectives with pass/fail criteria for each objective (no step-by-step procedure is necessary)	• Details regarding any failures/deviations found	• Intended use • Result of risk-based analysis • Summary description of the objectives tested, and testing performed • Issues found • Conclusion declaring acceptability of the software for its intended use, including the resolution or appropriate risk justification of issues found • Record of who performed testing and date the testing was performed • Established review and approval when appropriate

表 1 - 保証活動と記録の例

保証活動	テスト計画	テスト結果	記録（デジタルを含む）
スクリプトテスト: 堅牢	• テスト目的 • テストケース (ステップバイステップの手順) • 期待される結果 • テスト計画の独立したレビューと承認（適切な場合）	• 各テストケースで得られた結果記録 • 発見された故障/逸脱に関する詳細	• 意図した用途 • リスクベース分析の結果 • 実施したテストの詳細報告 • 各テストケースの結果 • 見つかった課題 • 意図した用途に対してソフトウェアが受入可能であることを宣言する結論（見つかった課題の解決策又は適切なリスクの合理的な説明を含む） • テスト実施者、及び実施日付の記録 • 必要に応じて、確立されたレビューと承認
スクリプトテスト: 限定的	• 特定された、限定的なテストケース (ステップバイステップの手順) • テストケースの期待される結果 • 適用された非スクリプトテストの特定 • テスト計画の独立したレビューと承認（適切な場合）	• 各テストケースで得られた結果記録 • 発見された故障/逸脱に関する詳細	• 意図した用途 • リスクベース分析の結果 • 実施したテストの概要説明 • 各テストケースの結果 • 見つかった課題 • 意図した用途に対してソフトウェアが受入可能であることを宣言する結論（見つかった課題の解決策や適切なリスクの合理的な説明を含む） • テスト実施者、及び実施日付の記録 • 必要に応じて、確立されたレビューと承認

保証活動	テスト計画	テスト結果	記録（デジタルを含む）
非スクリプトテスト: シナリオテスト	• テスト計画なしで機能要素・機能をテストする。	• 発見された故障/逸脱に関する詳細	• 意図した用途 • リスクベース分析の結果 • テストした機能要素・機能、及び実施したテストの概要説明 • 見つかった課題 • 意図した用途に対してソフトウェアが受入可能であることを宣言する結論（見つかった課題の解決策や適切なリスクの合理的な説明を含む） • テスト実施者、及び実施日付の記録 • 必要に応じて、確立されたレビューと承認
非スクリプトテスト: エラー推測	• テスト計画なしで故障モードをテストする。	• 発見された故障/逸脱に関する詳細	• 意図した用途 • リスクベース分析の結果 • テストした故障モード、及び実施したテストの概要説明 • 見つかった課題 • 意図した用途に対してソフトウェアが受入可能であることを宣言する結論（見つかった課題の解決策や適切なリスクの合理的な説明を含む） • テスト実施者、及び実施日付の記録 • 必要に応じて、確立されたレビューと承認

保証活動	テスト計画	テスト結果	記録（デジタルを含む）
非スクリプトテスト: 探索的テスト	• 各目的に対する合/否基準を含む、高レベルのテスト計画における目的を定める (ステップバイステップの手順は必要ない)。	• 発見された故障/逸脱に関する詳細	• 意図した用途 • リスクベース分析の結果 • テスト目的、及び実施したテストの概要説明 • 見つかった課題 • 意図した用途に対してソフトウェアが受入可能であることを宣言する結論（見つかった課題の解決策や適切なリスクの合理的な説明を含む） • テスト実施者、及び実施日付の記録 • 必要に応じて、確立されたレビューと承認

The following is an example of a record of assurance in a scenario where a manufacturer has developed a spreadsheet with the intended use of collecting and graphing nonconformance data stored in a controlled system for monitoring purposes. In this example, the manufacturer has established additional process controls and inspections that ensure non-conforming product is not released. In this case, failure of the spreadsheet to perform as intended would not result in a quality problem that foreseeably leads to compromised safety, so the spreadsheet would not pose a high process risk. The manufacturer conducted rapid exploratory testing of specific functions used in the spreadsheet to ensure that analyses can be created, read, updated, and/or deleted. During exploratory testing, all calculated fields updated correctly except for one deviation that occurred during the testing of the update. In this scenario, the record would be documented as follows:	以下は、スプレッドシートを開発するシナリオの保証記録の例である。この例では、意図した用途は、コントロールされた監視システムに格納されている不適合データを収集してグラフ化することである。この例における製造業者は、不適合製品がリリースされないようにするために追加的なプロセスコントロールと検査を確立している。この場合、スプレッドシートが意図通りに動作しなくても、安全性が損なわれると予見できる品質問題にはつながらないため、スプレッドシートが高いプロセスリスクとなることはない。当該製造業者は、スプレッドシートで使用される特定の機能についてすばやく探索的テストを実施して、分析結果が作成、読み取り、更新、削除されることを確認した。探索的テストでは、更新テスト中に発生した 1 件の逸脱を除いて、すべての計算結果フィールドが正しく更新された。このシナリオの記録は次のように文書化される。

• **Intended Use:** The spreadsheet is intended for use in collecting and graphing nonconformance data stored in a controlled system for monitoring purposes; as such, it is used as part of production or the quality system. Because of this use, the spreadsheet is different from similar software used for business operations such as for accounting.	• **意図した用途：**スプレッドシートは、コントロールされた監視システムに格納されている不適合データを収集してグラフ化するために使用することを意図しており、製造システム／品質システムの一部として使用される。このような用途であることから、スプレッドシートは、会計等のビジネス活動に使用される同様のソフトウェアとは異なる。
• **Risk-Based Analysis:** In this case, the software is only used to collect and display data for monitoring nonconformances, and the manufacturer has established additional process controls and inspections to ensure that nonconforming product is not released. Therefore, failure of the spreadsheet to perform as intended should not result in a quality problem that foreseeably leads to compromised safety. As such, the software does not pose a high process risk, and the assurance activities should be commensurate with the process risk.	• **リスクベース分析：**この例では、ソフトウェアは不適合監視データを収集し、表示するためにのみ使用されており、不適合製品をリリースしないようにするために追加的なプロセスコントロールと検査が確立されている。従って、スプレッドシートが意図通りに動作しなくても、安全性が損なわれることが予測できるような品質問題につながることはない。そのため、ソフトウェアは高いプロセスリスクがあるとはいえず、保証活動はプロセスリスクに応じたものとする必要がある。
• **Tested:** Spreadsheet X, Version 1.2	• **テスト対象：**Spreadsheet X, Version 1.2
• **Test type:** Unscripted testing – exploratory testing	• **テストの種類：**非スクリプトテスト - 探索的テスト
• **Goal:** Ensure that analyses can be correctly created, read, updated, and deleted	• **ゴール：**分析結果が正しく作成・読み取り・更新・削除できることを確認する。

• Testing objectives and activities: ♦ Create new analysis: Passed ♦ Read data from the required source: Passed ♦ Update data in the analysis: Failed due to input error, then passed re-test ♦ Delete data: Passed ♦ Verify through observation that all calculated fields correctly update with changes: Passed with noted deviation	• テスト目的と活動： ♦ 分析結果の新規作成：合格 ♦ 必要なソースからのデータ読み取り：合格 ♦ 分析結果のデータを更新：入力エラーが原因で失敗したが、その後、再テストで合格 ♦ データの削除：合格 ♦ 変更に応じてすべての計算フィールドが正しく更新されていることを観察により検証する：合格、ただし逸脱あり。
• **Deviation:** During the testing of the update, when the user inadvertently input text into an updatable field requiring numeric data, the associated row showed an immediate error.	• **逸脱：**更新のテストにおいて、数値データを入れるべき更新可能フィールドにユーザが誤ってテキストを入力した。関連する行にすぐにエラーが表示された。
• **Conclusion:** The spreadsheet is acceptable for its intended use. Incorrectly inputting text into the field is immediately visible and does not impact the intended use. A new validation rule was placed on the field to permit only numeric data inputs. The testing was performed again with the validation rule and the update passed all testing objectives. No additional errors were observed in the spreadsheet functions after the validation rule was implemented.	• **結論：**スプレッドシートは意図した用途に対して受入可能である。フィールドに誤ってテキスト入力したことはすぐに明らかとなり、意図した用途には影響がない。数値データ入力のみを許可する新たなバリデーションルールをフィールドに設けた。バリデーションルールを使用して再度テストを実施し、更新はすべてのテスト目的に合格した。バリデーションルールが実装された後、スプレッドシート関数で追加のエラーは確認されなかった。
• **When/Who:** July 9, 2024, by Jane Smith	• **テスト日付/テスト者：**July 9, 2024, by Jane Smith

B. Considerations for Electronic Records Requirements (電子記録要件に関する考慮)

Manufacturers have expressed confusion and concern regarding the application of 21 CFR Part 11, Electronic Records; Electronic Signatures, to computers or automated data processing systems used as part of production or the quality system. Manufacturers should refer to the "Part 11, Electronic Records; Electronic Signatures – Scope and Application" guidance (hereafter referred to as the "Electronic Records guidance"), when determining whether and how to apply 21 CFR Part 11 (hereafter referred to as "Part 11").	製造業者は、21 CFR Part 11, Electronic Records; Electronic Signatures の製造システム／品質システムの一部として使用されるコンピュータ又は自動データ処理システムへの適用について混乱と懸念を表明してきた。21 CFR Part 11（以下、「Part 11」）が適用されるのかどうか、またどのように適用されるかを決定する際に、「Part 11, Electronic Records; Electronic Signatures – Scope and Application」（以下、電子記録ガイダンス）を参照すべきである。 【訳注】Part 11 及び Scope and Application ガイダンスの和訳については、https://bunzen.co.jp/ 参照。
The regulations in Part 11 set forth the criteria under which FDA considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper (see 21 CFR 11.1(a)). In general, Part 11 applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted under any records requirements set forth in Agency regulations (see 21 CFR 11.1(b)). Part 11 also applies to electronic records submitted to the Agency under requirements of the FD&C Act and the Public Health Service Act (PHS Act), even if such records are not specifically identified in Agency regulations (see 21 CFR 11.1(b)). The underlying requirements set forth in the FD&C Act, PHS Act, and FDA regulations (other than Part 11) are referred to as "predicate rules." In addition, where electronic signatures and their associated electronic records meet the requirements of Part 11, FDA will generally consider the electronic signatures to be equivalent to full handwritten signatures, initials, and other general	Part 11 規制では、電子記録、電子署名、及び電子記録になされた手書き署名が、信用性 (trustworthy) と信頼性 (reliable) があり、紙の記録及び紙の上の手書き署名と同等のものと FDA が見なす際の一般的判断基準を示している (21 CFR 11.1(a) 参照)。一般的に、Part 11 は、FDA 規制で定められた記録についてのあらゆる要件の下で、作成、修正、維持管理、アーカイブ、取出、又は伝送される電子形式の記録に適用される (21 CFR 11.1(b) を参照)。Part 11 は、FD&C Act 及び Public Health Service Act (PHS) の要件に基づいて FDA に提出される電子記録であれば、たとえその記録が FDA の諸規制で具体的に特定されておらずとも適用される（21 CFR 11.1(b) を参照）。FD&C Act、PHS Act、及び（Part 11 以外の）FDA 規制で定められた、根底となる要件を、「predicate rules」と呼ぶ。さらに、電子署名及びそれに関連する電子記録が Part 11 の要件を満たしている場合、FDA は通常、その電子署名を、FDA の諸規制によって要求される手書きのフルネームの署名、イニシャル、及びその他の一般的な署名と同等のものと見なす(21 CFR 11.1(c)) 。

signings as required by agency regulations (21 CFR 11.1(c)).	
For computer software used as part of production or the quality system, the applicable predicate rules include those under Part 820. A document required under Part 820—including, but not necessarily limited to, a document Part 820 requires to bear a signature—and maintained in electronic form would generally be an "electronic record" under Part 11 (see 21 CFR 11.3(b)(6)). To determine when a record is required under Part 820, manufacturers should consider, among other things, whether the record would be necessary as evidence to document required validation. If a manufacturer maintains in electronic form a document required under Part 820, then Part 11 generally applies.	製造システム／品質システムの一部として使用されるコンピュータソフトウェアの場合、適用される predicate rules には、Part 820 の規則が含まれる。Part 820 で要求される文書（Part 820 で署名が求められる文書を含むが、これに限定されるものではない）で電子形式に維持管理される文書は、通常、Part 11 の「電子記録」である（21 CFR 11.3(b)(6)を参照）。Part 820 に基づいた記録がどこで必要になるかを判断するためには、〔Part 820 で〕要求されるバリデーションを文書化するための証跡として記録が必要となるかどうか等を考慮する必要がある。製造業者が Part 820 で要求される文書を電子形式で維持管理する場合は、通常、Part 11 が適用される。
Example: Documentation demonstrating that a management enterprise system correctly and reliably automates checking materials before use in production would generally be necessary as evidence for a manufacturer to support a validated state. In this example, Part 11 would generally apply to the documentation if in electronic form.	*例*：製造で使用する前の材料チェックが、全社管理システムにより正確かつ確実に自動化されていることを示す文書資料は、通常、製造業者がバリデーションされた状態であることを裏付ける証跡として必要になる。この例では、文書資料が電子形式である場合、通常、Part 11 が適用される。
Example: Upon application startup, a COTS automatically saves routine activity logs. However, in this case, these activity logs are not necessary as evidence for a manufacturer to support a validated state. In this example, Part 11 would not apply to the activity logs.	*例*：アプリケーションの起動時に、COTS が日常的なアクティビティログを自動的に保存する。ただし、この場合、これらのアクティビティログは、製造元がバリデーションされた状態であることを裏付ける証跡として必要ではない。この例では、Part 11 はアクティビティログには適用されない。
As discussed in the Electronic Records guidance, FDA intends to exercise enforcement discretion regarding specific Part 11 requirements for validation of computerized systems used to create, modify, maintain, or transmit electronic records (see 21 CFR 11.10(a) and 11.30). But the enforcement	Electronic Records guidance で説明されているように、FDA は、電子記録の作成、修正、維持管理、又は伝送に使用されるコンピュータ化システムのバリデーションに関する特定の Part 11 要件に対し、執行を裁量する（21 CFR 11.10(a) 及び 11.30 を参照）。しかし、Electronic Records

discretion policy described in the Electronic Records guidance (concerning validation of computerized systems used to create, modify, maintain, or transmit electronic records) expressly does not apply to the validation requirement for computer software used as part of production or the quality system arising under 21 CFR 820.70(i). This guidance recommends that manufacturers base their approach to computer software assurance on a justified and documented risk assessment and a determination of the potential of the system to affect product quality, patient safety, and record integrity. Manufacturers may utilize a least-burdensome, risk-based approach outlined in this guidance to provide assurance that the software that maintains electronic records subject to Part 11 performs as intended.	guidance に記載されている執行裁量ポリシー（電子記録の作成、修正、維持管理、又は伝送に使用されるコンピュータ化システムのバリデーションに関するもの）は、明らかに 21 CFR 820.70(i) で定める製造システム／品質システムの一部として使用されるコンピュータソフトウェアのバリデーション要件には適用されない。 本ガイダンスでは、製造業者がコンピュータソフトウェア保証へのアプローチを、合理的に説明可能で文書化されたリスクアセスメントと、システムが製品の品質、患者の安全性、記録のインテグリティに影響を与える可能性の判断に基づいて行うことを推奨する。製造業者は、このガイダンスで概説されている、負担が最も少ないリスクベースのアプローチを利用して、Part 11 の対象となる電子記録を維持管理するソフトウェアが意図したとおりに動作することを保証することができる。

Footnotes (脚注)

Footnote 17

Manufacturers should also consult the “Enforcement Policy for Certain Supplements for Approved Premarket Approval (PMA) or Humanitarian Device Exemption (HDE) Submissions” guidance, which describes FDA’s general recommendations for limited modifications to devices required to have an approved PMA or HDE to help address manufacturing limitations or supply chain disruptions.	製造業者は「Enforcement Policy for Certain Supplements for Approved Premarket Approval (PMA) or Humanitarian Device Exemption (HDE) Submissions」ガイダンスも参照すべきである。そこでは、製造上の制限やサプライチェーンの混乱に対処するために、承認済み PMA 又は HDE が必要な機器に対する限定的な変更に関する FDA の一般的な推奨事項が説明されている。

Appendix A. Examples (付録 A. 例)

The examples in this section outline possible application of the principles in this guidance to various software assurance situations.	この章で挙げる例は、さまざまなソフトウェア保証を行う場面で、本ガイダンスで示す原則をどのように適用できるかを概説するものである。

Example 1: Nonconformance Management System (例 1：不適合管理システム)

A manufacturer has purchased and configured 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.	ある製造業者は、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、構成設定した。その実装のコンピュータソフトウェア保証においてリスクベースアプローチを適用しようとしている。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意図している。
As part of the assurance activities, the manufacturer performs a thorough assessment of the software vendor that includes: • Evaluation of the vendor's software development life cycle, • Review of the vendor's quality management system and relevant certifications, and • Review of vendor's cybersecurity documentation and life cycle management plans as well as relevant certifications.	製造業者は、保証活動の一環としてソフトウェアベンダに対して次のような綿密なアセスメントを実施する。 • ベンダのソフトウェア開発ライフサイクルの評価 • ベンダの品質管理システムと関連認証のレビュー、及び • ベンダのサイバーセキュリティに関する文書資料とライフサイクル管理計画、及び関連する認証のレビュー

Based on the manufacturer's established SOP for evaluating suppliers, the vendor's capability to meet the manufacturer's requirements are deemed acceptable for the software's intended use. The manufacturer maintains a record of the evaluation according to their established purchasing control procedures. The following features, functions, or operations were considered by the manufacturer in developing a risk-based assurance strategy:	確立された供給者評価の SOP に基づき、ベンダが製造業者の要件を満たす能力は、ソフトウェアの意図した用途に対して受入可能と考えられる。製造業者は、確立された購買コントロール手順に従って評価の記録を維持管理する。 製造業者は、リスクベースの保証戦略を立案する中で以下の機能要素／機能／業務を検討した。 【訳注】見やすさのため、表の中に訳文を記載せずに、元の表の後に訳した表を続けた。Table 2 の訳は 「表 2. 不適合処理管理システムのコンピュータソフトウェア保証の例」参照。

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 Initiation Operations: • A nonconforming event results in the creation of a nonconformance record. • The necessary data for initiation are recorded prior to completion of a nonconformance initiation task. • A Nonconformance Owner is assigned prior to completion of the nonconformance 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 processes established by the manufacturer for containment of non-conforming product.	Failure of the nonconformance 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 containment of non-conforming product, which include separation of affected product, alerting line management, and labeling the affected product. As such, the manufacturer determined the nonconformance initiation operations did not pose a 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 exploratory testing of the operations. High level objectives for testing are established to meet the intended use and no unanticipated failures occur.	The manufacturer documents: • the intended use • result of risk-based analysis • summary description of the operations tested • the testing objectives and if they passed or failed • any issues found • conclusion declaring acceptability including resolution of issues • record of who performed testing and date the testing was performed

Electronic Signature Function: • 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: ♦ The name of the person who signs the record ♦ The date (DD-MM-YYYY) and time (hh:mm) the signature was executed. ♦ The role of the signatory associated with the signature (such as review, approval, responsibility, or authorship).	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.	Failure of the electronic signature function to perform as intended may compromise or delay compliance with regulatory requirements and established SOPs but would not result in a quality problem that foreseeably compromises safety. As such the manufacturer determined that the electronic signature function did not pose a 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 scenario testing of this function with users to demonstrate the function meets the intended use.	The manufacturer documents: • the intended use • result of risk-based analysis • testing performed • any issues found • conclusion declaring acceptability including resolution of issues • record of who performed testing and date the testing was performed
Product Containment Function:	This function is	Failure of the function to	The manufacturer has	The manufacturer documents:

Features, Functions, or Operations	Intended Use of the Features, Functions or Operations	Risk-Based Analysis	Assurance Activities	Establishing the appropriate record
• 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.	intended to trigger the necessary evaluation and decision-making on whether a product correction or removal is needed when the nonconformance occurred in product that has been distributed.	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.	performed an assessment of the system capability, supplier evaluation, and installation activities. The manufacturer determined the function is a high process risk. The manufacturer performed assurance activities commensurate with the medical device risk and established a detailed scripted test protocol to exercise the possible interactions and potential function failures. The testing also included appropriate repeatability testing in various scenarios to provide assurance that the function works reliably.	• the intended use • result of risk-based analysis • a detailed test protocol • detailed report of the testing performed • pass/fail results for each test case • any issues found • conclusion declaring acceptability including resolution of issues • record of who performed testing and date the testing was performed • the signature and date of the signatory authority according to the manufacturer's established SOP

表 2. 不適合処理管理システムのコンピュータソフトウェア保証の例

機能要素／機能／業務	機能要素／機能／業務の意図した用途	リスクベース分析	保証活動	適切な記録の作成
不適合処理開始業務: • 不適合イベントにより、不適合記録が作成される。 • 不適合処理開始タスクの完了前に、開始に必要なデータが記録される。 • 不適合処理開始タスクが完了する前に、Nonconformance Owner が任命される。	この業務の意図した用途は、不適合のワークフローを管理し、ワークフローのエラーを防止することにより、作業及び完全な品質記録を可能にすることである。この業務は、不適合製品の応急措置のために確立されたプロセスを補足することを意図している。	不適合処理開始業務が意図通りに実施されない場合、開始ワークフローが遅れる可能性があるが、不適合製品の応急措置（影響を受けた製品の分離、ライン管理者への注意喚起、影響を受けた製品のラベル付けを含む）のための追加的なプロセスが設けられているため、安全性を損なう品質問題は発生しない。そのため、不適合処理開始業務に高いプロセスリスクはないと判断した。	システム能力のアセスメント、供給者評価、及びインストレーション活動を実施した。さらに、これらの活動の補足として業務の探索的テストを行う。高いレベルのテスト目的を定め、意図した用途を満たし、想定外の故障が発生しないようにした。	製造業者の文書: • 意図した用途 • リスクベース分析の結果 • テストした業務の概要説明 • テスト目的と合否結果 • 見つかった課題 • 受入可能であることを宣言する結論（課題の解決を含む） • テスト実施者、及び実施日付の記録

機能要素／機能／業務	機能要素／機能／業務の意図した用途	リスクベース分析	保証活動	適切な記録の作成
電子署名機能: • 電子署名の実行記録は、監査証跡の一部として保存される。 • 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する。 • 電子署名が実行されると、次の情報が実行記録の一部となる。 ♦ 署名者名 ♦ 署名実行日付 (DD-MM-YYYY) と時刻 (hh:mm) ♦ 署名における署名者の役割 (レビュー、承認、責任、作成者等)。	電子署名機能の意図した用途は、署名が必要なところで電子署名を取得し、保存することであり、かつ電子署名の要件を満たすことである。	電子署名機能が意図通りに動作しなかった場合、規制要件や確立された SOP への準拠が損なわれたり、遅れたりする可能性があるが、安全性が損なわれると予見できるような品質問題に発展することはない。そのため、電子署名機能に高いプロセスリスクはないと判断した。	システム能力のアセスメント、供給者評価、及びインストレーション活動を実施した。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、ユーザがこの機能のシナリオテストを実施し、機能が意図した用途を満たしていることを示した。	製造業者の文書: • 意図した用途 • リスクベース分析の結果 • 実施したテスト • 見つかった課題 • 受入可能であることを宣言する結論（課題の解決を含む） • テスト実施者、及び実施日付の記録

機能要素／機能／業務	機能要素／機能／業務の意図した用途	リスクベース分析	保証活動	適切な記録の作成
製品応急措置機能: • 製造業者のコントロールが及ばないところで製品の不適合が発生した場合、システムは、製品の修正又は撤収が必要かどうかを確認するようユーザに促す。	この機能の意図した用途は、流通した製品に不適合が発生した場合に、製品の修正又は撤収が必要かどうかについて、必要な評価と意思決定を開始することである。	機能が意図通りに動作しない場合、必要な修正又は撤収が開始されず、安全性が損なわれることが予見できる品質問題が発生する。従って、製造業者は、この機能が高いプロセスリスクがあると判断した。	システム能力のアセスメント、供給者評価、及びインストレーション活動を実施した。その機能に高いプロセスリスクがあると判断した。医療機器リスクに応じた保証活動を実施し、起こりうる相互作用や潜在的な機能障害をテストするための詳細なスクリプトテストのプロトコルを作成した。機能が信頼性をもって動作することを保証するために、テストには、さまざまなシナリオにおける繰り返し性テストも含めた。	製造業者の文書: • 意図した用途 • リスクベース分析の結果 • 詳細なテストプロトコル • 実施したテストの詳細報告 • 各テストケースの合/否結果 • 見つかった課題 • テスト実施者、及びテスト実施日付の記録 • 製造業者が定めた SOP に従った署名権限者による署名、及び日付

Example 2: Learning Management System (LMS) (例 2: 学習管理システム (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.	ある製造業者は、COTS LMS を導入しているところであり、その導入にあたってコンピュータソフトウェア保証にリスクベースアプローチを適用しようとしている。このソフトウェアは、トレーニングの管理、記録、追跡、及びレポートを意図している。
As part of the assurance activities, the manufacturer performs a thorough assessment of the software vendor that includes: • Evaluation of the vendor's software development life cycle, and • Review of the vendor's quality management system and relevant certifications.	保証活動の一環として、製造業者はソフトウェアベンダに対して次のような綿密なアセスメントを実施する。 • ベンダのソフトウェア開発ライフサイクルの評価、及び • ベンダの品質管理システムと関連する認証のレビュー
Based on the manufacturer's established SOP for evaluating suppliers, the vendor's capability to meet the manufacturer's requirements are deemed acceptable for the software intended use. The manufacturer maintains a record of the evaluation according to their established purchasing control procedures.	確立された供給者評価の SOP に基づき、ベンダが製造業者の要件を満たす能力は、ソフトウェアの意図した用途に対して受入可能と考えられる。製造業者は、確立された購買コントロール手順に従って評価の記録を維持管理する。
The following features, functions, or operations were considered by the manufacturer in developing a risk-based assurance strategy:	製造業者は、リスクベースの保証戦略を立案する中で以下の機能要素／機能／業務を検討した。 【訳注】見やすさのため、表の中に訳文を記載せずに、元の表の後に訳した表を続けた。Table 3 の訳は「表 3. LMS のコンピュータソフトウェア保証の例」参照。

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
Access Control, User Management, and Notification Functions: • Create and manage user log-on features (e.g., username and password). • Assigns trainings to users per the curriculum assigned by management. • The system notifies users of training curriculum assignments, completion of trainings, and outstanding trainings. • The system notifies users' management of outstanding trainings.	These functions are intended to manage user access, user workflow, and user notifications regarding training.	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 error-guessing to attempt to circumvent process flow and verify the access controls of the system.	The manufacturer documents: • the intended use • result of risk-based analysis • a summary description of the failure modes tested • any issues found • conclusion declaring acceptability including resolution of issues • record of who performed testing and date the testing was performed

Features, Functions, or Operations	Intended Use of the Features, Functions or Operations	Risk-Based Analysis	Assurance Activities	Establishing the appropriate record
Record-keeping and Reporting Functions: • The system captures evidence of users' training completion. • The system generates reports on training curriculum assignments, completion of training, and outstanding trainings.	These functions are intended to capture and maintain evidence and records of user training completion and generate analytic reports on the records for review by the organization as needed.	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 to "break" the system (e.g., try to delete the audit trail), verify record integrity, and the report generating functions.	The manufacturer documents: • the intended use • result of risk-based analysis • a summary description of the failure modes tested • any issues found • conclusion declaring acceptability including resolution of issues • record of who performed testing and date the testing was performed

表 3. LMS のコンピュータソフトウェア保証の例

機能要素／機能／業務	機能要素／機能／業務の意図した用途	リスクベース分析	保証活動	適切な記録の作成
アクセスコントロール、ユーザ管理、及び通知機能: • ユーザログオンに関する機能要素を作成及び管理する (例：ユーザ名とパスワード)。 • 管理者が割り当てたカリキュラムに従って、ユーザにトレーニングを割り当てる。 • システムは、トレーニングカリキュラムの割り当て、トレーニング完了、未受講トレーニングをユーザに通知する。 • システムは、未受講トレーニングをユーザの管理者に通知する。	これらの機能は、トレーニングに関するユーザアクセス、ユーザワークフロー、及びユーザ通知を管理することを目的としている。	これらの機能要素／機能／業務が意図通りに動作しない場合、品質システム記録のインテグリティに影響を与えるが、安全性が損なわれるとは予見できない。そのため、この機能要素・機能・業務には高いプロセスリスクがないと判断した。	システム能力のアセスメント、供給者評価、及びインストレーション活動を実施した。さらに、これらの活動を非スクリプトテストで補足する。エラー推測を適用し、プロセスフローを無視してみることでシステムのアクセスコントロールを検証する。	製造業者の文書: • 意図した用途 • リスクベース分析の結果 • テストした故障モードの概要説明 • 見つかった課題 • 受入可能であることを宣言する結論（課題の解決を含む） • テスト実施者、及びテスト実施日付の記録

記録保持及び報告機能: • システムは、ユーザのトレーニング完了の証跡を取得する。 • 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、未受講トレーニングの報告を生成する。	これらの機能は、ユーザトレーニング完了の証跡と記録を取得して維持管理すること、及び必要に応じて組織がレビューできるような〔トレーニング〕記録の分析レポートを生成することを目的としている。	これらの機能要素／機能／業務が意図通りに動作しない場合、品質システム記録のインテグリティに影響を与えるが、安全性が損なわれるとは予見できない。そのため、この機能要素・機能・業務には高いプロセスリスクはないと判断した。	システム能力のアセスメント、供給者評価、及びインストレーション活動を実施した。さらに、非スクリプトテストにより、システムの「破壊」（例えば、監査証跡を削除しようとする）、記録のインテグリティの検証、レポート生成機能の検証を行うことでこれらの活動を補足する。	製造業者の文書: • 意図した用途 • リスクベース分析の結果 • テストした故障モードの概要説明 • 見つかった課題 • 受入可能であることを宣言する結論（課題の解決を含む） • テスト実施者、及びテスト実施日付の記録

Example 3: Business Intelligence Applications (例 3: ビジネスインテリジェンスアプリケーション)

A medical device manufacturer has decided to implement a commercial business intelligence solution for data mining, analytics, and reporting. The software is intended to better understand product and process performance over time, to identify improvement opportunities.	ある医療機器製造業者は、データマイニング、分析、及び報告書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導入することを決定した。このソフトウェアは、経時的な製品及びプロセスのパフォーマンスをより深く理解し、改善の機会を明らかにすることを意図している。
As part of the assurance activities, the manufacturer performs a thorough assessment of the software vendor that includes: • Evaluation of the vendor's software development life cycle, • Review of the vendor's quality management system and relevant certifications, and • Review of vendor's cybersecurity documentation and life cycle management plans as well as relevant certifications.	保証活動の一環として、製造業者はソフトウェアベンダに対して次のような綿密なアセスメントを実施する。 • ベンダのソフトウェア開発ライフサイクルの評価 • ベンダの品質管理システムと関連認証のレビュー、及び • ベンダのサイバーセキュリティに関する文書資料とライフサイクル管理計画、及び関連する認証のレビュー
Based on the manufacturer's established SOP for evaluating suppliers, the vendor's capability to meet the manufacturer's requirements are deemed acceptable for the software intended use. The manufacturer maintains a record of the evaluation according to their established purchasing control procedures.	確立された供給者評価の SOP に基づき、ベンダが製造業者の要件を満たす能力は、ソフトウェアの意図した用途に対して受入可能と考えられる。製造業者は、確立された購買コントロール手順に従って評価の記録を維持管理する。
In addition to the vendor assessment, the following features, functions, or operations were considered by the manufacturer in developing a risk-based assurance strategy:	ベンダアセスメントに加えて、製造業者は、リスクベースの保証戦略を立案する中で以下の機能要素／機能／業務を検討した。 【訳注】見やすさのため、表の中に訳文を記載せずに、元の表の後に訳した表を続けた。Table 4 の訳は「表 4. ビジネスインテリジェンスアプリケーションのコンピュータソフトウェア保証の例」参照。

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 • result of risk-based analysis • detailed test protocol • a detailed report of the testing performed • pass/fail results for each test case • any issues found • conclusion declaring acceptability including resolution of issues found • record of who performed testing and date the testing was performed • the signature and date of the signatory authority according to the manufacturers established SOP

Features, Functions, or Operations	Intended Use of the Features, Functions or Operations	Risk-Based Analysis	Assurance Activities	Establishing the appropriate record
User help 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.	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 • result of risk-based analysis • record of who performed the assessment and date the assessment was performed • conclusion declaring acceptability including resolution of issues

Features, Functions, or Operations	Intended Use of the Features, Functions or Operations	Risk-Based Analysis	Assurance Activities	Establishing the appropriate record
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 can 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 pose high process risk.	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 that the reporting functions of the software do not necessitate any additional assurance effort beyond these activities.	The manufacturer documents: • the intended use • risk-based analysis • record of who performed the assessment and date the assessment was performed • conclusion declaring acceptability including resolution, justification, and/or process controls implemented addressing the impact of the issues

表 4. ビジネスインテリジェンスアプリケーションのコンピュータソフトウェア保証の例

機能要素／機能／業務	機能要素／機能／業務の意図した用途	リスクベース分析	保証活動	適切な記録の作成
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る。 • ソフトウェアは、元ソースから持ってきたデータインテグリティを維持管理し、データインテグリティの課題、〔データの〕破損、又はデータ転送に問題があるかどうかを判断できる。	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、データインテグリティを確保し、データの破損を防止し、データを適切に変更及び保存するといったシステムの安全で堅牢な能力を確実にすることを意図している。	これらの機能が意図通りに動作しない場合、傾向分析や解析の正確性又は一貫性がなくなってしまう。これにより、潜在的な品質傾向、課題、改善機会を把握できなくなり、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る。そのため、これらの機能に高いプロセスリスクがあると判断し、その医療機器リスクに応じた、より厳格な保証活動が必要であると判断した。	製造業者は、医療機器リスクに応じた保証活動を決定し、システム能力のアセスメント、供給者評価、及びインストレーション活動を実施した。さらに、可能な操作をいろいろ試したり機能がエラーになりそうな方法を試したりする詳細なスクリプトテストのプロトコルを作成する。テストには、機能が信頼性をもって動作することを保証するために、さまざまなシナリオに合わせた再現テストも含めた。	製造業者の文書: • 意図した用途 • リスクベース分析の結果 • 詳細なテストプロトコル • 実施したテストの詳細報告 • 各テストケースの合/否結果 • 見つかった課題 • 受入可能であることを宣言する結論（見つかった課題の解決を含む） • テスト実施者、及びテスト実施日付の記録 • 製造業者が定めた SOP に従った署名権限者による署名、及び日付

機能要素／機能／業務	機能要素／機能／業務の意図した用途	リスクベース分析	保証活動	適切な記録の作成
ユーザヘルプに関する機能要素: • ソフトウェアは、ユーザにアプリケーションのヘルプメニューを提供する。	この機能要素は、ユーザとシステムのインタラクションを助け、システムすべての機能要素の使用を支援することを意図している。	機能が意図通りに機能しないことで、安全性が損なわれるような品質問題が発生する可能性はほとんどない。従って、この機能に高いプロセスリスクはないと判断した。	この機能要素は、既に実施済みのシステム能力のアセスメント、供給者評価、及びインストレーション活動以上の追加の保証作業を必要としない。	製造業者の文書: • 意図した用途 • リスクベース分析の結果 • アセスメント実施者、及びアセスメント実施日付の記録 • 受入可能であることを宣言する結論（課題の解決を含む）

機能要素／機能／業務	機能要素／機能／業務の意図した用途	リスクベース分析	保証活動	適切な記録の作成
<u>レポート機能:</u> • このソフトウェアは、クエリを作成して実行し、さまざまなソースからのデータを結合し、データマイニングを実行できる。 • ソフトウェアは、さまざまな統計解析とデータ要約を可能にする。 • ソフトウェアは、データからグラフを作成できる。 • ソフトウェアは、分析報告を生成する能力を提供する。	これらの機能は、ユーザが、データソースにクエリを実行し、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できるようにすることを意図している。これらの機能は、監視及びレビュー目的でのデータを収集及び記録することを意図しており、製造又はプロセスのパフォーマンスへの直接の影響はない。この例では、ソフトウェアは品質に関する決定を通知することは意図していない。	これらの機能が意図通りに動作しない場合、品質問題 (例：不完全又は不適切なレポート) が発生する可能性があるが、この例では、これらの機能は、製造やプロセスのパフォーマンスに直接影響を与えない監視及びレビュー目的でデータを収集及び記録することを意図しているため、安全性が損なわれるとは予見できない。従って、これらの機能に高いプロセスリスクはないと判断した。	レポートソフトウェアの供給者は、ソフトウェアがクエリを作成及び実行し、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、統計解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バリデーション済みである。さらに、製造業者はシステムの能力をアセスメントし、供給者評価とインストレーション活動を実施した。そのため、ソフトウェアのレポート機能は、これらの活動以上の追加的な保証努力は必要ないと判断した。	製造業者の文書: • 意図した用途 • リスクベース分析の結果 • アセスメント実施者、及びアセスメント実施日付の記録 • 受入可能であることを宣言する結論（解決策、合理的な説明、及び（又は）課題の影響に対処するために実装されたプロセスコントロールを含む）

Example 4: Software as a Service (SaaS) Product Life Cycle Management System (PLM) (Software as a Service (SaaS)

製品ライフサイクル管理システム (PLM))

A medical device manufacturer has decided to implement a SaaS-based Product Life Cycle Management System (PLM). While the PLM SaaS solution has the capability to automate the management of various life cycle stages of a product development, the manufacturer intends to use the solution for broad project management. The SaaS PLM is intended to automate the intake of project requirements, develop project plans, monitor/track project execution, and maintain relevant records, signatures, and deliverables upon project closing. This intended use of the system does not directly impact patient safety or product quality but does maintain a quality system record where integrity of the data is needed. The manufacturer does not need any customization of the "out-of-the-box" capabilities of the SaaS product and only needs to perform basic standard configuration of the SaaS product (e.g., user roles, accounts). As part of the assurance activities, the manufacturer performs a thorough assessment of the SaaS vendor that includes: • Evaluation of the vendor's software development life cycle, • Review of the vendor's quality management system and relevant certifications, • Review of vendor's cybersecurity documentation and life cycle management plans as well as relevant certifications, and • Review of the vendor's infrastructure support including availability and reliability.	ある医療機器製造業者は、SaaS ベースの製品ライフサイクル管理システム (PLM) を導入することを決定した。PLM SaaS ソリューションには、製品開発のさまざまなライフサイクル段階の管理を自動化する機能があるが、製造業者は、このソリューションを幅広いプロジェクト管理に使用することを意図している。SaaS PLM は、プロジェクト要件の取り込みを自動化し、プロジェクト計画を策定し、プロジェクト実行を監視/追跡し、プロジェクトの終了時に関連記録、署名、成果物を維持管理するものである。このシステムの意図した用途は、患者の安全性や製品の品質に直接影響を与えるものではないが、データインテグリティが必要な品質システム記録を維持管理する。SaaS 製品の「out-of-the-box」機能のカスタマイズは不要であり、SaaS 製品の基本的な標準構成設定（ユーザロール、アカウント等）を行うだけで済む。 保証活動の一環として、製造業者は SaaS ベンダに対して次のような綿密なアセスメントを実施する。 • ベンダのソフトウェア開発ライフサイクルの評価 • ベンダの品質管理システムと関連認証のレビュー • ベンダのサイバーセキュリティに関する文書資料とライフサイクル管理計画、及び関連する認証のレビュー、及び • ベンダのインフラストラクチャサポート（可用性と信頼性を含む）のレビュー

Based on the manufacturer's established SOP for evaluating suppliers, the vendor's capability to meet the manufacturer's requirements are deemed acceptable for the software intended use. The manufacturer maintains a record of the evaluation according to their established purchasing control procedures. The manufacturer also establishes a service agreement with the SaaS vendor that includes requirements for security, data integrity, privacy, availability, change management, and business continuity. **Automatic Updates:** The SaaS vendor provides the manufacturer documentation summarizing the changes, testing, and testing results of all automatic updates made to the SaaS system functions identified by the manufacturer as part of the service agreement. The manufacturer performs an assessment of the changes and the effect they may have on the intended use. The manufacturer performs risk-based assurance testing of the changes appropriate to the impact identified. The manufacturer maintains a record summarizing the risk assessment of the change and any assurance activities performed.	確立された供給者評価の SOP に基づき、ベンダが製造業者の要件を満たす能力は、ソフトウェアの意図した用途に対して受入可能と考えられる。製造業者は、確立された購買コントロール手順に従って評価の記録を維持管理する。製造業者は、セキュリティ、データインテグリティ、プライバシー、可用性、変更管理、及びビジネス継続性の要件を含むサービス契約を SaaS ベンダと締結する。 **自動更新:** SaaS ベンダは、サービス契約の一環として、製造業者が指定した SaaS システム機能に対するすべての自動アップデートについての変更、テスト、及びテスト結果を総括する文書資料を製造業者に提供する。製造業者は、変更内容とそれが意図した用途に与える影響をアセスメントする。製造業者は、それぞれの変更について明かになった影響に応じた適切なリスクベースの保証テストを実施する。製造業者は、変更のリスクアセスメントと実施された保証活動を総括した記録を維持管理する。 【訳注】見やすさのため、表の中に訳文を記載せずに、元の表の後に訳した表を続けた。Table 5 の訳は 「表 5. SaaS PLM 向けコンピュータソフトウェア保証の例」参照。

Table 5. Computer Software Assurance Example for SaaS PLM

Features, Functions, or Operations	Intended Use of the Features, Functions or Operations	Risk-Based Analysis	Assurance Activities	Establishing the appropriate record
Project Initiation and Planning Function: • The software allows for the creation of a new project. • The software is able to assign team members and roles to the project as assigned by the manufacturer's management. • The software intakes and updates project requirements and specifications. • The software is able to develop a project plan, with tasks, dependencies, milestones, and deliverables. • The software monitors changes to data maintained by the project record.	These functions are intended to automate the creation of a data record for the project, maintain user roles, assign responsibilities for key project data to team members, intake the key data relevant to the project, maintain the integrity and associations of the project data, and monitor changes or updates to the project information.	Failure of these functions 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 functions do not pose high process risk.	The manufacturer has performed an assessment of the system capability, supplier evaluation, and established service agreements with the SaaS vendor. Based on the risk-based analysis, the manufacturer performs a configuration verification and User Acceptance Testing (UAT) using exploratory unscripted testing.	The manufacturer documents: • the intended use • risk-based analysis • summary description of the objectives tested, and testing performed • any issues found • conclusion declaring acceptability including resolution, justification, and/or process controls implemented addressing the impact of the issues • record of who performed assessment and date the assessment was performed

Features, Functions, or Operations	Intended Use of the Features, Functions or Operations	Risk-Based Analysis	Assurance Activities	Establishing the appropriate record
Electronic Signature Function: • 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: ♦ The name of the person who signs the record ♦ The date (DD-MM-YYYY) and time (hh:mm) the signature was executed. ♦ The meaning associated with the signature (such as review, approval, responsibility, or authorship).	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.	Failure of the electronic signature function to perform as intended may compromise or delay compliance with regulatory requirements and established SOPs but would not result in a quality problem that foreseeably compromises safety. As such the manufacturer determined that the electronic signature function does not pose a high process risk.	The manufacturer has performed an assessment of the system capability, supplier evaluation, and configuration activities. To provide assurance that the function complies with applicable requirements, the manufacturer performs scenario testing of this function with users to demonstrate the function meets the intended use.	The manufacturer documents: • the intended use • risk-based analysis • testing performed • any issues found • record of who performed testing and date the testing was performed • conclusion declaring acceptability including resolution, justification, and/or process controls implemented addressing the impact of the issues

Features, Functions, or Operations	Intended Use of the Features, Functions or Operations	Risk-Based Analysis	Assurance Activities	Establishing the appropriate record
Access Control and Traceability Functions: • The function controls user roles, associated permissions, and system access (e.g., user log-on). • The function monitors and maintains records of access and modifications of the final data records maintained in the system. • The function produces time stamped reports of the system access, authorization, change, and the associated user for modifications made to final data records maintained in the system as established by the manufacturer's procedure for auditing.	These functions are intended to provide appropriate access control, establish user roles, and maintain individual user accounts. The functions are also intended to monitor, maintain, and report a time-stamped logging of access or changes to the training records or electronic signature events to ensure the authenticity, reliability, and integrity of the final records established by the manufacturer to be maintained.	Failure of these functions to perform as intended has a significant impact on the overall intended use and system operations, and as such, may result in a quality system integrity and compliance issue. Since these functions are intended to ensure integrity of the data record for a quality system requirement only, the manufacturer determines that a failure to perform as intended would not foreseeably lead to compromised safety and therefore does not pose a high process risk.	The manufacturer has performed an assessment of the system capability, supplier evaluation, and established service agreements with the SaaS vendor. Based on the risk-based analysis, the manufacturer performs a configuration verification and develops an automated test script that will quickly exercise the access controls to also support verification of future changes. Additionally, the manufacturer performs User Acceptance Testing (UAT) of the reporting capabilities using exploratory unscripted testing.	The manufacturer documents: • the intended use • risk-based analysis • summary of automated test cases in the test script (or electronic version of the test script) and a summary description of the objectives tested, and testing performed • any issues found and results of the automated test script • conclusion declaring acceptability including resolution, justification, and/or process controls implemented addressing the impact of the issues • record of who performed testing and date the testing was performed

表 5. SaaS PLM向けコンピュータソフトウェア保証の例

機能要素／機能／業務	機能要素／機能／業務の意図した用途	リスクベース分析	保証活動	適切な記録の作成
プロジェクト開始及び計画機能: • ソフトウェアは、新しいプロジェクトを作成することができる。 • ソフトウェアは、製造業者の経営層の指示に従って、プロジェクトにチームメンバーと役割を割り当てることができる。 • ソフトウェアは、プロジェクト要件と仕様を取り込み、更新する。 • ソフトウェアは、タスク、依存関係、マイルストーン、成果物を含むプロジェクト計画を作成することができる。 • ソフトウェアは、プロジェクト記録に維持管理されるデータへの変更を監視する。	これらの機能は、プロジェクトのデータ 記録の作成を自動化し、ユーザロールを維持管理し、主要なプロジェクトデータに対する責任をチームメンバーに割り当て、プロジェクトに関連する主要なデータを取り込み、プロジェクトデータのインテグリティと関連付けを維持管理し、プロジェクト情報の変更や更新を監視することを意図している。	これらの機能が意図したとおりに実行されない場合、品質システム記録のインテグリティに影響するが、安全性が損なわれることは予見できない。従って、この機能に高いプロセスリスクはないと判断した。	製造業者は、システム機能のアセスメント、供給者評価を実施し、SaaS ベンダとサービス契約を締結した。リスクベース分析に基づいて、製造業者は探索的な非スクリプトテストにより、構成設定の評価とユーザ受入テスト (UAT) を実施する。	製造業者の文書: • 意図した用途 • リスクベース分析 • テスト目的及び実施したテストの概要説明 • 見つかった課題 • 受入可能であることを宣言する結論（解決策、合理的な説明、及び（又は）課題の影響に対処するために実施されたプロセスコントロールを含む） • アセスメント実施者、及びアセスメント日付の記録、

機能要素／機能／業務	機能要素／機能／業務の意図した用途	リスクベース分析	保証活動	適切な記録の作成
電子署名機能: • 電子署名の実行記録は、監査証跡の一部として保存される。 • 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する。 • 電子署名が実行されると、次の情報が実行記録の一部となる。 ♦ 署名者名 ♦ 署名実行日付 (DD-MM-YYYY) と時刻 (hh:mm) ♦ 署名に関連する意味 (レビュー、承認、責任、作成者等)。	電子署名機能の意図した用途は、署名が必要なところで電子署名を取得し、保存することであり、かつ電子署名の要件を満たすことである。	電子署名機能が意図通りに動作しなかった場合、規制要件や確立された SOP への準拠が損なわれたり、遅れたりする可能性があるが、安全性が損なわれると予見できるような品質の問題に発展することはない。そのため、電子署名機能に高いプロセスリスクはないと判断した。	システム能力のアセスメント、供給者評価、及び構成設定活動を実施した。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、ユーザがこの機能についてシナリオテストを実施し、機能が意図した用途を満たしていることを示した。	製造業者の文書: • 意図した用途 • リスクベース分析の結果 • 実施したテスト • 見つかった課題 • テスト実施者、及び実施日付の記録 • 受入可能であることを宣言する結論（解決策、合理的な説明、及び（又は）課題の影響に対処するために実施されたプロセスコントロールを含む）

機能要素／機能／業務	機能要素／機能／業務の意図した用途	リスクベース分析	保証活動	適切な記録の作成
アクセスコントロール及びトレーサビリティ機能: • この機能は、ユーザの役割、関連する権限、及びシステムアクセス（ユーザログオン等）をコントロールする。 • この機能は、システム内に保持されている最終データ 記録へのアクセスと変更の記録を監視及び維持管理する。 • この機能は、(製造業者の監査手順に基づき確立され）システムに保持されている最終データ記録に対する変更に対する、システムアクセス、承認、変更、及び関連ユーザについてのタイムスタンプ付きレポートを生成する。	これらの機能は、適切なアクセスコントロールを提供し、ユーザロールを確立し、個々のユーザ アカウントを維持管理することを目的としている。 また、これらの機能は、トレーニング記録や電子署名イベントへのアクセスや変更のタイムスタンプ付きログを監視、維持管理、報告し、製造業者が維持管理する最終記録の真正性、信頼性、インテグリティを確保することを目的としている。	これらの機能が意図したとおりに実行されない場合、全体的な意図した用途及びシステム操作に重大な影響を及ぼし、その結果、品質システムのインテグリティ及びコンプライアンスに問題が発生する可能性がある。 これらの機能は、品質システム要件のみに基づいてデータ記録のインテグリティを確実にすることを意図しているため、意図したとおりに機能しない場合でも安全性が損なわれることになるとは予見できず、したがって高いプロセスリスクはないと判断した。	製造業者は、システム機能のアセスメント、供給者評価を実施し、SaaS ベンダとサービス契約を締結した。 リスクベースの分析に基づいて、製造業者は構成設定の検証を実施し、アクセスコントロールを迅速に実行する自動テストスクリプト（これは、将来の変更の検証もサポートする）を開発する。さらに、探索的な非スクリプトテストにより、レポート機能のユーザ受入テスト (UAT) を実施する。	製造業者の文書: • 意図した用途 • リスクベース分析 • テストスクリプト（又はテストスクリプトの電子版）内の自動テストケースの概要と、テストの目的と実行されたテストの概要説明 • 見つかった課題と自動テストスクリプトの結果 • 受入可能であることを宣言する結論（解決策、合理的な説明、及び（又は）課題の影響に対処するために実施されたプロセスコントロールを含む） • テスト実施者、及び実施日付の記録