管理番号: BZLib-124

改訂番号: 0

名称: **Good Practices for Computerized Systems in Regulated "GxP" Environments**

ページ数: 全 84ページ

PHARMACEUTICAL INSPECTION CONVENTION
PHARMACEUTICAL INSPECTION CO-OPERATION SCHEME

PI 011-3
25 September 2007

PIC/S GUIDANCE

GOOD PRACTICES FOR COMPUTERISED SYSTEMS IN REGULATED "GXP" ENVIRONMENTS

Editor: PIC/S Secretariat

e-mail: info@picscheme.org
web site: http://www.picscheme.org

株式会社文善

改 0　　2022 年 6 月 21 日

管理番号: BZLib-124

改訂番号: 0

名称: **Good Practices for Computerized Systems in Regulated "GxP" Environments**

ページ数: 全 84ページ

【注記】

本書は、Pharmaceutical Inspection Convention (PIC) の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】

本文にない言葉を補足した場合、〔 〕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。

【訳注】には、訳又は内容についての説明を記載しています。

【巻末訳注】には、本書内で共通の内容を巻末で説明しています。

目次

1. DOCUMENT HISTORY

1. 文書履歴

Adoption by PIC/S Committee	2-3 June 2003
Entry into force	1 September 2003

PART ONE – PREAMBLE

第一部 — プリアンブル

2. PURPOSE

2. 目的

2.1	The PIC/S Guide to Good Manufacturing Practices is the basis for GMP inspections. In particular its Annex 11, 'Computerised Systems' is used when inspecting such systems.	PIC/S Guide to Good Manufacturing Practices は、GMP 査察の基本となるが、その中でも Annex 11「Computerised Systems」【巻末訳注 1】は、コンピュータ化システムの査察時に使用される。
2.2	The purpose of this document is to provide recommendations and background information concerning computerised systems that will be of assistance to inspectors for training purposes and during the inspection of computerised systems. The document will be of assistance to all 'Good Practice' Inspectors responsible for inspecting applications in the regulated pharmaceutical sector[1]; hence the use of the acronym 'GxP' in the title. It is recognised that not all companies subjected to GLP inspections are linked to the regulated pharmaceutical sector. However, it is considered that the guidance contained within this PIC/S document may also be beneficial to companies subjected to other regulatory frameworks and GLP inspection.	本書の目的は、コンピュータ化システムについての推奨事項と背景情報を示すことで、査察官のトレーニング、及びコンピュータ化システムの査察に役立てることにある。本書は規制対象の製薬セクター[1]のアプリケーションの査察に責任を持つ、全ての「グッドプラクティス」の査察官に有用となると思われ、そのため本書のタイトルに「GxP」の略語を用いた。GLP 査察対象の全ての会社が規制対象の製薬セクターに関連しているわけではないことは承知しているが、本書に示すガイダンスは、他の規制下で GLP 査察を受ける会社にとっても役立つであろう。
2.3	GDP defines the scope of compliance requirements for wholesaling and distribution practice. Where automated systems and electronic records are used for such applications then inspectors will expect such regulated users to have in place the sorts of controls and disciplines outlined in this document, or a best practice alternative. Vertically integrated companies (R&D, manufacturing and distribution) will already apply such controls and	GDP (Good Distribution Practice) では、卸売及び物流のプラクティスについての適合要件の範囲を定義している。このようなアプリケーションで自動化システムと電子記録が用いられる場合、査察官は、規制対象ユーザーが本書で示すようなコントロールと規律を設けるか、又は代替のベストプラクティスを設けることを期待する。（R&D、製造、及び物流が）垂直統合された会社では、既にこのよう

[1] Throughout this document the 'users' (owners of the good practice computerised systems being inspected) are collectively referred to as 'regulated users' for clarity.
[1] 本書を通じて「ユーザー」（査察対象のグッドプラクティスコンピュータ化システムのオーナー）は、明確化を図るために総称して「規制対象ユーザー」という。

	compliance measures.	なコントロールと適合方策を講じているであろう。
2.4	International regulatory agencies have collaborated to produce this harmonised guidance for the implementation, management and operation of computerised systems. It is intended as a reference for regulated users, including their suppliers, in addition to regulatory inspectors and investigators.	各国の規制当局が協力して、コンピュータ化システムの実装、管理、及び運用のための統一的なガイダンスを作成した。本書は、規制の査察官及び調査員だけでなく、規制対象ユーザーやサプライヤ等が参照することを意図している。
2.5	This guidance document is intended to provide a logical explanation of the basic requirements for the implementation, validation and operation of computerised systems. Additionally, the document may be adapted to identify the criteria that would be expected to be considered if a regulated user, or a regulatory agency, were to conduct an inspection of the implemented computerised system(s), against GxP compliance requirements and/or perceived risks.	本書では、コンピュータ化システムの実装、バリデーション、及び運用の基本要件の論理的説明を提供することを意図している。さらに、規制対象ユーザー又は規制当局が、実装されたコンピュータ化システムを GxP 適合要件及び（又は）認識されているリスクに照らして査察する際に、どのような基準を満たすべきかを検討するために本書を利用できる。
2.6	This guidance document provides details of good practices, which should support new technology and technical innovations.	本書は新しい技術や技術革新を支えるグッドプラクティスについての詳細を示す。
2.7	It should be noted that it is important for national legislation to be referred to when determining the extent to which the provisions laid down in this document may be applicable.	本書で示す条項が適用される範囲を判断する際に、その国の法律を参照することが重要であることに留意する必要がある。
2.8	An auditor or an inspector may wish to consider *evidence for compliance* as indicated in *italicised text* throughout this document.	監査者又は査察官は、本書を通じて*斜体表記*されている*適合の証拠*を検討するとよいであろう。
2.9	It is to be hoped that the PIC/S Expert Circle on Computerised Systems will build on this consensus reference document, to deliver simplified training and aide memoires for the inspection of common GxP systems, as well as sector specific applications. As technology continues its relentless advance the Expert Circle could also provide interpretation of GxP and recommend changes, if appropriate. Such materials could provide further sub-set appendices to Section 24 ('Inspection tabulated checklists and aide memoires').	PIC/S Expert Circle on Computerised Systems はこの統一見解の参考書を踏まえ、セクター固有のアプリケーションの査察だけでなく、セクター共通の GxP システムの査察のために、簡略版トレーニング及び覚書を提供したいと考えている。技術の絶え間ない進歩に伴い、Expert Circle も必要に応じて GxP の解釈と推奨事項の変更を提案するかもしれない。こうした情報は、24 章「チェックリストと覚書」のサブセットの付録となっていくであろう。
2.10	Some repetition is inevitable in a document that has evolved over many years and through various working party multinational iterations. It is not intended that this document is read from cover to cover, but should be 'dipped into' as a reference source when needed and for that reason some sections have to stand-alone.	〔本書は〕長年にわたって、作業班（調査委員会）の複数国にまたがった反復により作り上げられた文書であるため、ある程度の繰り返しが出てくるのは仕方がない。本書は、最初から最後までを「通読」するのではなく、参考資料として必要なときに参照することを意図しているため、いくつかの章は独立したものになっている。

3. SCOPE

3. 範囲

3.1	It is acknowledged that the field of computer technology continues to develop at a considerable speed and the regulated user has to ensure that the software and systems have been developed to best engineering practices in a quality assured manner. It will be for regulated users to define relevant applications, impacted business units and corresponding deliverables for such applications. This document sheds some light on the techniques and controls required for this.	コンピュータ技術分野がかなりのスピードで進歩を続けているという認識のもと、規制対象ユーザーは、品質が保証されるやり方でソフトウェアとシステムがベストエンジニアリングプラクティスに沿うように開発されたことを確実にしなければならない。どのアプリケーションが関係するか、どの業務部門が影響を受けるか、アプリケーションに対応する成果物は何か、を定義するのは規制対象ユーザーである。本書では、このために必要な技術とコントロールについて説明する。
3.2	At the time of issue this document reflected the current state of the art. It is not intended to be a barrier to technical innovation or the pursuit of excellence. The advice in this Guidance is not mandatory for industry. However, industry should consider these recommendations as appropriate.	本書は、発行時における最新技術を反映しているが、技術革新や優れたものを阻む意図はない。本書に記載したアドバイスは、業界にとって必須ではない。しかし、業界は必要に応じ本書の推奨事項を検討すべきである。
3.3	For hardware, peripherals, integrated process links and system functionality in general, the controls and testing arrangements are by comparison to software, fairly mature, logically more visible and the failure modes more predictable.	ソフトウェアに比べれば、ハードウェア、周辺機器、統合プロセス接続、及び一般的なシステム機能のコントロールやテストのやり方は、十分成熟しており、論理的に明確であり、故障モードは予測しやすい。
3.4	As a result, we have tried to keep the contents of this document practical and principle-oriented, to ensure that it retains relevance for as long as possible. However, value judgements and consensus between parties can be difficult to achieve at times in this complicated field.	以上のことから、本書の内容を、できるだけ長期にわたり陳腐化しないように、実用的かつ原則を優先したものとなるよう試みた。しかし、この複雑な分野で、価値判断し、関係者間でコンセンサスを得ることは、往々にして困難である。
3.5	The scope of the document is broad, covering necessary steps and the documentation needed for the implementation and validation of a computerised system. Management of such projects requires the linking[2] of important aspects of management policies, documentation and record systems embracing the respective professional disciplines involved in the development and use of the computerised system.	本書の適用範囲はコンピュータ化システムの実装、及びバリデーションに必要なステップと文書をカバーする広範なものになっている。このようなプロジェクトを管理するためには、コンピュータ化システムの開発／利用に関する専門的なやり方を取り入れた管理方針／文書化／記録システムの重要な側面を連携[2]させる必要がある。

[2] For successful project management these links should be established between the supplier(s) [developer(s) and producer(s) of individual components or complete computerised system] and the regulated user [purchaser and user of the computerised system].
[2] プロジェクト管理を成功させるために、サプライヤ（コンピュータ化システムの一部又は全体の開発者兼製造者）と規制対象ユーザー（コンピュータ化システムの購入者兼ユーザー）の間でこのような連携を確立すべきである。

3.6	Of necessity this guidance contains some 'how to' achieve GxP compliance advice for suppliers and developers of software and automated systems, in addition to guidance for the regulated users. This is because of the iterative nature of software development and the requirement for quality and functionality to be built into the software in a disciplined manner, to ensure structural integrity, consistency, robustness and reliability. This will often be outside of the direct control of the regulated user (as purchaser/customer). There will normally be a need to manage and control the split responsibilities of contracted suppliers (whether in-house or external party) and regulated user businesses (customers), for project management, product specifications, quality assurance standards and performance.	本書では、必要に迫られ、規制対象ユーザー向けのガイダンスにとどまらず、ソフトウェアや自動化システムのサプライヤと開発者向けの、GxP 適合の「ハウツー」についてもアドバイスしている。何故ならソフトウェア開発は反復性があるものであり、構造的完全性／一貫性／堅牢性／信頼性を確実にする規律のある方法で、品質と機能に関する要件をソフトウェアに落とし込む必要があるためである。多くの場合、規制対象ユーザーは（購入者／顧客であり）そのことを直接コントロールすることができない。一般的に、受託したサプライヤ（社内／社外を問わず）と規制対象ユーザーのビジネス部門（顧客）の間で、プロジェクト管理、製品の仕様、品質保証の基準と実施状況についての責任を分担し、管理し、コントロールする必要がある。
3.7	This document also identifies the important aspects of validation of computerised systems. Descriptions of strategies that may be used for different categories of computer systems are described as well as identifying the approach that might be taken for the retrospective validation of legacy (old) systems. (see in particular Sections 4.5 and 6.2 (Figure:1) and 16 of this document).	本書では何がコンピュータ化システムバリデーションの重要な側面なのかについても明らかにする。コンピュータシステムの様々なカテゴリに使用できる戦略について説明するとともに、レガシーシステム（既設システム）の回顧的バリデーションで用いるアプローチを明らかにしている（特に本書の 4.5 章、6.2 章 (図:1) 、及び 16 章を参照）。
3.8	PIC/S considers that adoption of the principles, guidance, reporting and life cycle documentation best practices, outlined in this document, will enable users of computerised systems to establish quality assurance systems and records capable of demonstrating compliance with current GxP requirements and related guidance.	PIC/S の考えでは、コンピュータ化システムのユーザーは、本書で示す原則、ガイダンス、報告、及びライフサイクル文書に関するベストプラクティスを採用することで、最新 GxP 要件と関連ガイダンスへの適合を説明できるような品質保証システム及び記録を確立することができる。

4. INTRODUCTION

4. 序文

4.1	The structure of the document is designed to identify discrete subsections and their interrelationship within the principal topics concerning the implementation, validation and operation of computerised systems. A reference section, together with a glossary of terms commonly used in this industry sector will be found at the end of this document. Section 26 'Further Reading' suggests a number of textbooks, technical reports and guidelines that amplify the science, technology and practices underpinning this guideline. The 1994 publication by Stokes et al (Further Reading Ref: 1) provides insight into the requirements for computerised systems in GCP, GLP and GMP, together with a historical perspective on validation and international regulatory requirements.	本書は、コンピュータ化システムの実装、バリデーション、及び運用といった主要トピックごとに記載される章及び相互関係を特定できるように構成されている。本書の最後の部分には、関連文書の章と合わせて、この業界で一般的に用いられる用語集を掲載した。26章「推奨参考資料」には、本ガイドラインを裏付ける科学／技術／慣行について詳述するテキストブック／技術レポート／ガイドラインを数多く掲載している。Stokes らによる1994 年発行の文献（推奨参考資料 1）では、GCP、GLP 及び GMP におけるコンピュータ化システムの要件について考察し、バリデーションと国際的な規制要件について歴史的観点から論じている。
4.2	In recent years there has been an increasing trend to integrate electronic record and business management systems across all operational areas. In the future it is expected that our reliance on computer systems will continue to grow, rather than diminish. The use of validated, effective, GxP controlled computerised systems should provide enhancements in the quality assurance of regulated materials/products and associated data/information management. The extent of the validation effort and control arrangements should not be underestimated and a harmonised approach by industry and regulators is beneficial.	最近、あらゆる業務分野において電子記録システムと経営管理システムを統合する動きが強まってきている。将来的に、コンピュータシステムへの依存は、低くなるというよりは増大し続けるであろう。バリデートされた、効果的な、GxP でコントロールされたコンピュータ化システムを利用すれば、規制対象の原材料／製品の品質保証、及び関連するデータ／情報の管理を強化できるであろう。バリデーションを行い、コントロールを整備する程度を甘く考えるべきではなく、業界と規制当局により統一化されたアプローチが有益である。
4.3	Commercial 'off the shelf', 'standard', or proprietary systems can be particularly difficult to assess from a quality and performance point of view. For GxP regulated applications it is essential for the regulated user to *define a requirement specification* prior to selection and to carry out a properly *documented supplier assessment and risk analysis* for the various system options. Information for such exercises may come from *supplier audits* and research into the supplier's product versions in the user community and literature. This risk-based approach is one way for a firm to demonstrate that they have applied a controlled methodology, to determine the degree of assurance that a computerised system is fit for purpose. It will certainly be useful *evidence for consideration by an inspector*. (Note: What constitutes a 'critical	「市販製品」、「標準製品」、又はサプライヤ独自のシステムを、品質及び性能の観点からアセスメントすることは特に困難である。GxP 規制対象のアプリケーションでは、選定前に、規制対象ユーザーが*要件の仕様を定義*し、システムの様々なオプションに対し適切に*サプライヤアセスメントとリスク分析を実施し、記録すること*が必須である。そのための情報は、*サプライヤを監査*したり、サプライヤの当該製品のバージョンをユーザーコミュニティや文献で調査したりすることで得られる。コンピュータ化システムが利用目的に適していることを保証する程度をコントロールされた手法を用いて判断していることを、〔査察官に〕訴求する方法の一つは、このリスクベースアプローチである。これは*査*

	application' may vary considerably, depending on the situation – perhaps more so in GLP than in other disciplines).	*察官が考慮すべき証拠*として有力であろう（注意：何が「重要なアプリケーション」なのかは、状況に応じてかなり異なり、それはおそらく GLP では他の領域よりもいっそう顕著であろう）。
4.4	Whilst much of the detailed industry guidance relates to 'bespoke' and configured applications there are a number of tools and assessment techniques recommended for commercial packages and standard automated equipment. Complex automated state of the art processing equipment (such as high output tabletting machinery with in-process monitoring and feedback control functionality), or complex analytical instrumentation, for example, is difficult to assess without the supplier's help. The co-operation of the supplier is essential and it is important for suppliers to anticipate the needs of regulated user's for relevant product development life cycle quality and validation information. Such an approach also provides added value for the automated products. The QA and validation aspects for large automation aspects will inevitably be complex and may be subsumed in major engineering projects activated by the potential regulated user. *Inspectors will be interested in the evidence relating to the firm's assessment of the supplier's critical automated features as well as the traditional engineering, qualification and process performance aspects. Much of the guidance given in the GAMP Guide (Ref: 4), for example, is scaleable to complex projects and equipment with sub-contracted features. (Note: The risk assessment described in '4.3' above should identify critical features and functions for both the project team and the inspector).*	詳細な業界ガイダンスには、「カスタム」アプリケーション及び構成設定されたアプリケーションについて述べているものが多いが、市販パッケージ及び標準自動化機器向けにも多くのツールやアセスメント技術が推奨されている。例えば、プロセス内モニタリングとフィードバック制御機能を備えた高出力の打錠機のような最新の複雑な自動処理装置や複雑な分析機器の場合、サプライヤの支援なしにアセスメントすることは困難である。サプライヤの協力は不可欠であり、サプライヤにとって、関連する製品の開発ライフサイクルの品質とバリデーションについて、規制対象ユーザーがどのような情報を求めているのかを理解することは重要である。こうしたアプローチは、オートメーション製品に付加価値をもたらすことにもなる。大規模なオートメーションの QA とバリデーションは、必然的に複雑になり、規制対象ユーザーが行う大規模なエンジニアリングプロジェクトの一部として行われる場合がある。 *査察官は、従来のエンジニアリング、適格性評価、及びプロセス性能の側面だけでなく、サプライヤの重要な自動化機能に対する規制対象ユーザーによるアセスメントの証拠に関心を持っている。例えば、GAMP ガイド(Ref: 4)*【巻末訳注 2】*に掲載されているガイダンスの多くは、複雑なプロジェクトやカスタマイズ機能を持つ機器に対しスケーラブルである（注意：プロジェクトチームと査察官の双方にとって重要な特徴と機能は、上記「4.3 章」で説明したリスクアセスメントにより明らかにされるであろう）。*
4.5	When a GxP inspector has to assess an installed computerised system at a regulated user's site, s/he may consider some, or all, of the elements shown in Figure 1: "Computerised system", (viz.: the ***controlling system*** and the ***controlled process*** in an ***operating environment***). *The inspector will consider the potential risks, from the automated system to product/material quality or data integrity,* ***as identified and documented by the regulated user****, in order to assess the fitness for*	規制対象ユーザーのサイトでインストールされているコンピュータ化システムをアセスメントすることになった場合、GxP 査察官は図 1「コンピュータ化システム」に記載された要素（すなわち、「***運用環境***における***制御システム***及び***制御対象のプロセス***」）の一部又は全てを検討するであろう。*査察官は、特定システムが利用目的に適合しているかアセスメントするために、****規制対象ユーザーが特定***

	purpose of the particular system(s). The company's risk assessment records may also be referred to as part of this process. The inspector's assessment may also involve a consideration of system life cycle, quality assurance measures, validation and operational control evidence for the controlling system, as well as validation and operational experience with the controlled process.	***し、文書化した内容に沿って、****自動化システムへの潜在的リスクだけでなく、製品／原材料の品質又はデータインテグリティへの潜在的リスクも検討する。このプロセスの一環で、会社が実施したリスクアセスメントの記録も参照するかもしれない。この他、査察官によるアセスメントには、システムのライフサイクル、品質保証の方策、制御システムのバリデーション／運用コントロールの証拠、制御対象のプロセスのバリデーション／運用実績が含まれるであろう。*
4.6	*The validation documentation should cover all the steps of the life-cycle with appropriate methods for measurement and reporting, (e.g. assessment reports and details of quality and test measures), as required. Regulated users should be able to justify and defend their standards, protocols, acceptance criteria, procedures and records in the light of their own documented risk and complexity assessments, aimed at ensuring fitness for purpose and regulatory compliance.*	*バリデーション文書は、要求に応じた測定／報告の適切な方式（例：評価報告書、品質及びテスト方策の詳細）により、ライフサイクルの全てのステップをカバーする必要がある。規制対象ユーザーは、利用目的への適合と規制準拠のために、自分たちの基準／実施計画／受入基準／手順／記録が適切であることを、リスクと複雑さのアセスメント記録に照らして、説明／弁護できるようにすべきである。*
4.7	The Pharmaceutical Industry Systems Validation Forum in the UK developed the Good Automated Manufacturing Practice (GAMP) Supplier Guide to assist software suppliers in implementing an appropriate quality management system. *The GAMP Guide (and appendices) has evolved largely to define best practices in specifying, designing, building, testing, qualifying and documenting these systems to a rigorous validation management scheme, largely for the* ***controlling system****.* GAMP Forum is now sponsored by ISPE and has international membership and participation, including 'GAMP Americas'. (Websites: www.gamp.org and www.ispe.org)	英国の Pharmaceutical Industry Systems Validation Forum が、ソフトウェアサプライヤによる適切な品質管理システムの実装を支援するために Good Automated Manufacturing Practice (GAMP) Supplier Guide を作成している。*GAMP ガイド（及びその付録）*【巻末訳注 2】*は、主に****制御システム****について、厳格なバリデーション管理計画に従ってシステムの仕様作成／設計／構築／テスト／適格性評価／文書化するためのベストプラクティスを定義するように発展してきている。*現在 GAMP Forum は ISPE から後援を受けており、「GAMP Americas」を含む国際的な会員／参加者を有している。(Websites: www.gamp.org and www.ispe.org)

4.8	Apart from user acceptance testing (OQ) versus the functional specification, which may include 'Factory Acceptance Testing' (FAT), for example, at the supplier, the regulated user also has responsibility for the (PQ) performance qualification of the system. In this context the PQ *user acceptance test of the system is in its operating environment*[3], *and will again be against a User Requirements Specification (URS) that will include protocols and criteria for the performance and quality acceptance, not only for the* ***controlling system*** *but also for the* ***controlled*** *(pharmaceutical related)* ***process*** *application. Cross- references to any related, relevant process validation documentation should be clearly stated in respect of the latter. The GAMP Guide and PDA technical report No 18 (Further Reading Ref: 6) provide good practice guidance to drafting and using a URS, whereas pharmaceutical process validation guidance is given elsewhere (see PIC/S PI 006 and related EU/USFDA documents).*	機能仕様に対する「ユーザー受入テスト」(OQ) には、例えばサプライヤ施設で実施す「工場受入テスト」(FAT) を含むことがあるが、それとは別に、規制対象ユーザーはシステムの性能適格性評価 (PQ) の責任を持つ。この意味においてシステムの PQ *ユーザー受入テストは運用環境*[3] *において、ユーザー要求仕様書 (URS) に対して行われるものであり、****制御システム****だけでなく、****制御対象の*** *(製薬に関連した)* ***プロセス*** *アプリケーションの性能／品質を受け入れるための実施計画と基準が含まれる。後者については、関連する、重要なプロセスバリデーション文書への相互参照を明確に記述すべきである。GAMP ガイド*【巻末訳注 2】*及び PDA technical report No 18 (推奨参考資料 6) には、URS の作成／利用についてのグッドプラクティスガイダンスが記載されており、また製薬プロセスバリデーションのガイダンスは他の場所 (PIC/S PI 006 及び関連する欧州/米国 FDA の文書を参照) に記載されている。*
4.9	Computerised systems may simplistically be considered to exist as three main application types, i.e.: process control systems, data processing systems, (including data collection/capture) and data record/ storage systems. There may be links between these three types of system, described as 'interfaces'. For critical systems, the inspector should study the user's specifications, reports, data, acceptance criteria and other documentation for various phases of the project. The regulated user should be able to demonstrate through the *validation evidence* that they have a high level of confidence in the integrity of both the processes executed within the ***controlling*** computer ***system*** and in those ***processes controlled*** by the computer system within the prescribed ***operating environment***.	コンピュータ化システムは、単純化すれば、3 つの主要なアプリケーションタイプに分けられる。すなわち、プロセス制御システム、データ処理システム（データ収集／取得を含む）、及びデータ記録／保存システムである。この 3 つのシステム間に「インターフェース」と呼ばれるリンクが存在することもある。査察官は、重要なシステムについて、ユーザーの仕様書、報告書、データ、受入基準、等のプロジェクトの様々なフェーズの文書を調べるべきである。規制対象ユーザーは、***制御***コンピュータ ***システム***内で実行されるプロセス、及び事前に定められた***運用環境***においてそのコンピュータシステムにより ***制御されるプロセス***の両方ついて、そのインテグリティが高度に信頼できるものであることを、*バリデーションの証拠*を用いて、説明できるようにすべきである。
4.10	The simplification of application system types may at first sight seem to be misleading for some readers. For GCP, examples of specific clinical systems have been described in 'Computer	アプリケーションシステムを単純にタイプ分けすることは、一見したところ一部の読者に誤解を与えるかもしれない。GCP については

[3] Large enterprise or MRP-II systems may be tested in a pilot mode environment initially, followed by controlled 'roll-out' to the user environment.
[3] 大規模企業システムや MRP-II システムは最初にパイロットモード環境でテストし、その後コントロール下でユーザー環境に「展開」することがある。

	Systems Validation in Clinical Research' Section 9 (Further Reading Ref: 12). It can be seen that many of these systems have much in common with requirements for other GxP sectors, (e.g. Electronic transfer of data and/or software systems, (clinical) database management systems, statistical systems, derived data systems, electronic document management systems, electronic records and electronic signatures).	具体的な治験システムの例が「Computer Systems Validation in Clinical Research」 (推奨参考資料 12) の 9 章に掲載されている。こうしたシステムの多くは他の GxP セクターの要件とかなりの共通点がある（例：データ及び（又は）ソフトウェアの電子転送システム、（治験）データベース管理システム、統計システム、導出データシステム、電子文書管理システム、電子記録と電子署名）。
4.11	The regulated users of the system have the ultimate responsibility for ensuring that *documented validation evidence is available to GxP inspectors for review.*	システムの規制対象ユーザーは、*文書化されたバリデーションの証拠を GxP 査察官に確実に提供し、レビューできるようにする*最終的な責任を持つ。
4.12	In addition to the validation considerations, the inspector will also be concerned with assessing the basic *operational controls, quality system and security features* for these systems, as indicated in the PIC/S GMP Annex 11 and amplified in the APV Guidance, q.v. For a copy of the APV Guidance, see GAMP 4 Appendix 09 (Further Reading Ref: 15).	査察官は、バリデーションで考慮すべき事項に加えて、基本的な*運用コントロール／品質システム／システムのセキュリティ機能*をアセスメントすることにも関心を持つであろう。これらは PIC/S GMP Annex 11【巻末訳注 1】に記載され、APV Guidance でさらに詳述されている。APV Guidance のコピーは、GAMP4 付録 O9【巻末訳注 2】を参照のこと（推奨参考資料 15）。

PART TWO - IMPLEMENTATION OF SYSTEM
第二部　―　システムの実装

5. IMPLEMENTATION OF COMPUTERISED SYSTEMS
5. コンピュータ化システムの実装

5.1	The assurance of the reliability of a Supplier's software products is attributable to the quality of the software engineering processes followed during development. This should include design, coding, verification testing, integration, and change control features of the development life cycle, (including after sales support). In order for customers to have confidence in the reliability of the products, they should evaluate the quality methodology of the supplier for the design, construction, supply and maintenance of the software[4] . A formal, extensive review of the history of the Supply Company and the software package may be an option to consider where an additional degree of assurance of the reliability of the software is needed. This should be documented in a *Supplier Audit Report*[5]. Prospective purchasers should consider any known limitations and problems for particular software packages or versions and the adequacy of any corrective actions by the Supplier. Appropriate, comprehensive *documented customer acceptance testing* should support the final selection of the software package. Errors often come to light after implementation and it is important for the Supplier to advise/assist the Customer concerning any problems and modifications to resolve errors. For so called 'standard software packages' and COTS (as referenced in the GAMP guide and commercial literature), it is important that purchasers are vigilant in maintaining reliable systems. This may include *documented reviews of their own experiences, (e.g. log books and error reporting and resolution),* from reading relevant literature or from interacting with application 'User Groups' to identify and resolve any serious problems. *Conclusions and recommendations from such activities should be recorded.*	サプライヤの提供するソフトウェア製品に対して信頼性を保証できるかどうかは、開発時に採用されたソフトウェアエンジニアリングプロセスの品質次第である。例えば、開発ライフサイクル（販売後のサポートを含む）における設計／コーディング／検証テスト／統合／変更コントロールの特徴等である。顧客が製品の信頼性について確証を得るためには、ソフトウェアの設計／構築／供給／保守に関するサプライヤの品質手法を評価すべきである[4]。ソフトウェアについてさらに高度な信頼性保証が必要となる場合、サプライヤ会社及びそのソフトウェアパッケージの過去の履歴について、正式な、広範なレビューを実施することも検討すべきである。これは*サプライヤ監査報告書*[5]として文書化すべきである。システムの購入を予定する者は、ソフトウェアパッケージ／バージョンの既知の制約や問題点、及びサプライヤによる是正措置の適切性を検討すべきである。ソフトウェアパッケージの最終選定は、適切かつ包括的な*文書化された、顧客による受入テスト*により裏付けられるべきである。エラーは実装後に発見されることが多いため、サプライヤが顧客に対して問題点やエラー処置のための修正についてアドバイス／支援することが重要である。（GAMP ガイド【巻末訳注 2】及び市販の資料で言及されているような）いわゆる「標準ソフトウェアパッケージ」や市販ソフトウェアについては、システムの信頼性を維持するために、購入者側が絶えず注意を怠らないことが重要である。例えば、深刻な問題を特定し解決するために、自分たちで実施したこと *（例：ログブック、エラー報告と解決）*を関連資料の調査、又はアプリケーション

[4] Refer also to ISO15504 (1998) 'Information Technology Software Process Assessment' and see GAMP 4 Appendix M2 'Guideline for Supplier Audit'.
[5] A minority of suppliers are not responsive to requests for an audit. The need to perform a supplier audit should be linked to the regulated user's risk assessment and quality assurance standards.
[5] ごく一部であるが、監査を要求しても応答を返さないサプライヤも存在する。規制対象ユーザーのリスクアセスメントと品質保証基準に基づいてサプライヤ監査を実施する必要性を判断すべきである。

		「ユーザーグループ」とのやり取りに照らしてレビューし、文書化することが含まれる。こうしたアクティビティから得た結論と推奨事項は記録すべきである。
5.2	Where the reliability and structural integrity of complex software products cannot be directly assessed, or completely evaluated, then it is even more important to assure that a good construction process has been used and has been properly documented. It is recognised that complex commercial proprietary applications can be extremely difficult to assess due to commercial secrecy and rivalry between suppliers, competing for market share[6] . Market research plus focused quality system and product specific audits[7] of the suppliers by the regulated user (or by an accredited third party auditor) may be beneficial here. The business/GxP criticality and risks relating to the application will determine the nature and extent of any assessment of suppliers and software products. GAMP Forum and PDA have provided advice and guidance in the GxP field on these matters.	複雑なソフトウェア製品の信頼性と構造的インテグリティを直接アセスメントできない、又は完全に評価することができない場合は、〔サプライヤが〕グッドコンストラクションプロセス（good construction process）を用い、かつ適切に文書化していることを確認することがさらに重要になる。サプライヤ独自の複雑な市販アプリケーションに対するアセスメントは、商業上の機密や市場シェアを争うサプライヤ同士の競争のために、非常に困難であることは認識されている[6]。このようなときは、市場調査に加えて、規制対象ユーザー（又は認定されたサードパーティーの監査者）による、サプライヤの品質システムと個々の製品に着目した監査[7]が有益であろう。ビジネス／GxP の重要度、及びアプリケーションのリスクによって、サプライヤとソフトウェア製品のアセスメントの性質と範囲が決定される。GAMP Forum 及び PDA は、GxP 分野におけるこのような事項についてアドバイスとガイダンスを提供している。
5.3	*At all times there is a need for complete and accurate documentation and records to cover all aspects of the design phase, implementation & validation of the computerised system(s). Operating and reporting requirements for the important phases of the Software development Life Cycle related qualifications and testing exercises and commissioning should be covered by comprehensive Standard Operating Procedures or quality plans. The need for control and documentation of the development, implementation and operation of computer systems is extremely important for the validation of the system. There needs to be a strong emphasis on quality assurance in the development*	*コンピュータ化システムの設計フェーズ、実装及びバリデーションの全側面をカバーする完全かつ正確な文書と記録が常に必要である。包括的な SOP 又は品質計画に、適格性評価とテストの慣行、及び試運転に関するソフトウェア開発ライフサイクルの重要なフェーズにおける運用及び報告についての要件を記載すべきである。コンピュータシステムの開発／実装／運用をコントロールし、文書化することを要求することはシステムをバリデーションするうえで非常に重要である。特に開発ステージにおける品質保証に重点を置くべきである。品質保証された文書管理システムの下で、システムライフサイクル文書*

[6] The UK Government's Interdepartmental Committee on Software Engineering (ICSE) and the Real Time Engineering Group, have referred to such software as SOUP ('Software of Uncertain Pedigree') (1999).
[6] 英国政府の Interdepartmental Committee on Software Engineering (ICSE) 及び Real Time Engineering Group は、このようなソフトウェアを SOUP (「Software of Uncertain Pedigree」)と呼んでいる。
[7] Audits are not mandatory but are considered 'good practice', and it is for the regulated user to determine any auditing needs, scope and standards.
[7] 監査は必須ではないが、「グッドプラクティス」であると考えられる。監査の必要性、範囲、基準を決定するのは規制対象ユーザーである。

	stages. It is fundamental for system life cycle documents to be controlled and maintained (version, audit trails as appropriate), within a quality assured document management system and available for inspection, if necessary. Regulated users may choose to implement these requirements using either robust paper, electronic or hybrid systems.	*をコントロールし、維持し（バージョン、必要に応じて監査証跡）、必要時に査察で提供できるようにすることは必須である。*規制対象ユーザーは、これらの要件を、紙、電子的、又はハイブリッドのいずれかの方法を選択し、堅牢なシステムを実装することになる。

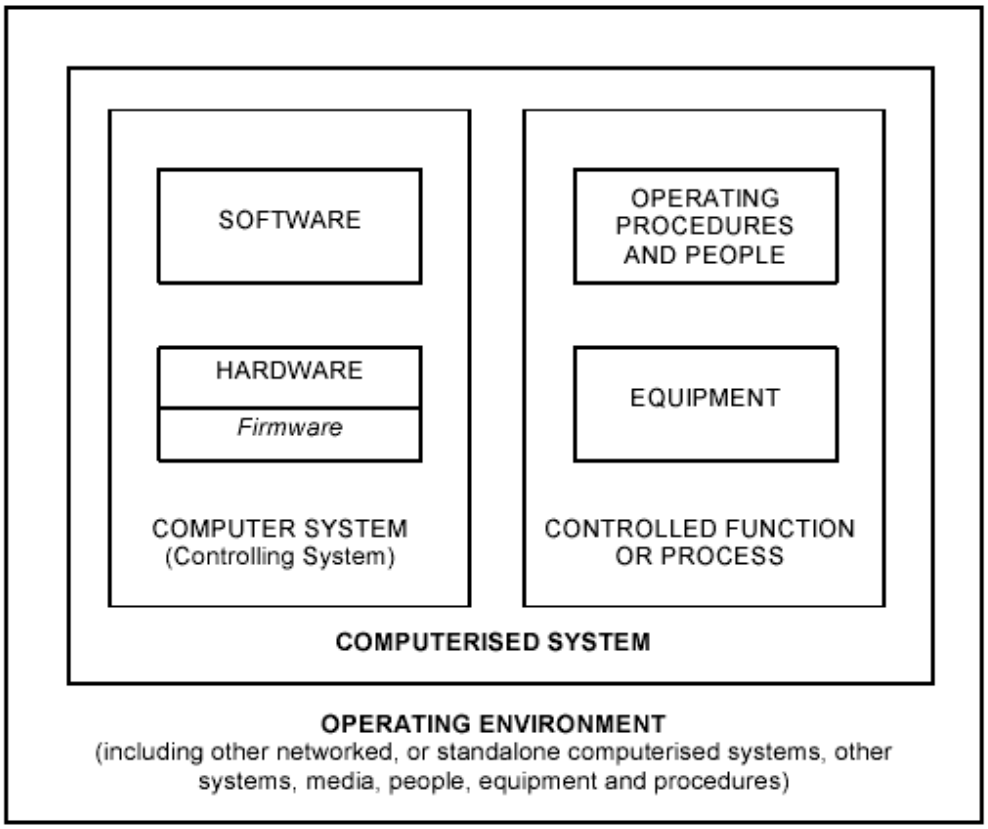
6. THE STRUCTURE AND FUNCTIONS OF THE COMPUTER SYSTEM(S)
6. コンピュータシステムの構造と機能

6.1	A recent USFDA document[8] identifies three premises that constitute the basic principles of quality assurance, which apply to software engineering: • Quality, safety and effectiveness must be designed and built into the software. • Quality cannot be inspected or tested into the finished software. • Each phase of the development process must be controlled to maximise the probability that the finished software meets all quality and design specifications.	最近の米国 FDA の文書[8]【訳注】では、ソフトウェアエンジニアリングに適用される品質保証の基本原則として以下の 3 つの前提を挙げている。 • 品質、安全性、及び有効性を設計し、ソフトウェアに組み込まなければならない。 • 検査又はテストでは、ソフトウェアに品質を作り込むことはできない。 • 開発プロセスの各フェーズをコントロールし、完成したソフトウェアが全ての品質及び設計の仕様を満たす可能性を最大限にしなければならない。 【訳注】FDA の General Principles of Software Validation の和訳については、https://bunzen.co.jp/ 参照。
6.2	A computerised system is composed of the computer system and the controlled function or process. The computer system is composed of all computer hardware, firmware, installed devices, and software controlling the operation of the computer. The controlled function may be composed of equipment[9] to be controlled and operating procedures that define the function of such equipment, or it may be an operation, which does not require equipment other than the hardware in the computer system. Interfaces and networked functions through LAN and WAN are	コンピュータ化システムは、コンピュータシステム、と制御される機能（又はプロセス）から構成される。コンピュータシステムは、全てのコンピュータのハードウェア、ファームウェア、インストールされたデバイス、及びコンピュータの運転を制御するソフトウェアから構成される。制御される機能は、制御される機器[9]とその機器の機能を定義する操作手順により構成される場合もあれば、操作だけで、コンピュータシステムのハードウェア以外の機器を必要としない場合もある。

[8] 'Final Guidance for Industry and FDA Staff: General Principles of Software Validation', CDRH, January 2002 (Further Reading Ref. 5).
[9] e.g. automated equipment and laboratory or process related instrumentation.
[9] 例：自動化機器、及びラボラトリ又はプロセス関連の計装。

	aspects of the computerised system and operating environment potentially linking a multitude of computers and applications. A firm's GxP system environment, functionality and interactions with other system(s) needs to be clearly defined and controlled in respect of GMP Annex 11 (4). It may be necessary to equip personal PC applications and Internet/ e-mail/ personal data filing/ etc., with appropriate security and design measures to protect GxP systems whilst permitting authorised users to control the personal applications on their desktop PCs.	LAN や WAN によるインターフェース及びネットワーク接続された機能は、多数のコンピュータやアプリケーションを接続する可能性のある、コンピュータ化システム及び運用環境の特徴である。会社の GxP システム環境、機能、他のシステムとのやり取りは、GMP Annex 11 (4) 【巻末訳注 1】に基づいて明確に定義し、コントロールする必要がある。許可されたユーザーが自身のデスクトップ PC 上でパーソナルアプリケーションをコントロールすることを許可することは構わないが、個人用 PC のアプリケーション、及びインターネット／電子メール／個人データのファイリング等に対して適切なセキュリティと設計の方策を講じ、GxP システムを保護することが必要であろう。

Figure 1 Schematic (below) identifies the relationship of the various components of a computerised system in its operating environment.
図 1 運用環境におけるコンピュータ化システムの各コンポーネントの関係を示した図（以下）。



6.3	A large variety of computer systems are used in regulated user organisations. These range from the simple standalone to large integrated and complex systems. For example, a significant proportion of programmable electronic systems and proprietary automated equipment for manufacturing, laboratory or clinical use, contains 'firmware' with embedded software in place (for further details on firmware and embedded software refer to the glossary. Also, see Section 15.1 of this document for approaches to be taken with different systems. Firmware and operating systems are usually qualified for the intended use (including version, release or related criteria) as part of performance qualification / process validation. *Regulated users should have an inventory of all their computerised systems, ownership, supplier/developer, functionality, links and validation status. A policy and validation master plan for computerised systems should also be available for inspection.*	規制対象ユーザーの組織では、多種多様なコンピュータシステムが使用されている。これには、単純なスタンドアロンシステムから、大きな統合された複雑なシステムまである。例えば、大部分のプログラマブル電子システム、及び製造、ラボラトリ、治験で用いられるサプライヤ独自の自動化機器には、ソフトウェアが組み込まれた「ファームウェア」が搭載されている（ファームウェア及び組み込みソフトウェアの詳細は、用語集を参照）。また、様々なシステムで講じるべきアプローチについては本書の 15.1 章も参照のこと。ファームウェアとオペレーティングシステムは、意図された利用目的に対する適格性評価（バージョン、リリース、又は関連する基準を含む）は、一般的に性能適格性判定／プロセスバリデーションの一環として行われる。*規制対象ユーザーは、全てのコンピュータ化システム、オーナーシップ、サプライヤ／開発者、機能、リンク、及びバリデーションのステータス〔を管理する〕台帳を用意すべきである。コンピュータ化システムの方針とバリデーションマスター計画書も査察時に提供できるようにすべきである。*

7. PLANNING AND LIFE-CYCLE MANAGEMENT

7. 計画とライフサイクル管理

7.1	A high level of assurance of quality and reliability cannot be attributed to a computerised system based simply on a series of tests solely designed to confirm the correct function of the software and its interaction with hardware. There needs to be a *formal planned approach by the developer* to assure that quality is built into the product. ISO 9001 provides a quality system model for quality assurance in design, development, production, installation and servicing. The objective of testing during software development at the supplier should be to try to break the structural integrity of the software and find any weaknesses through a rigorous testing regime. Audits of suppliers conducted by or on behalf of regulated users should cover these issues when project related risk analyses deem it to be necessary.	ソフトウェアの正常機能とハードウェアとのやり取りを確認するように設計した一連のテストを単純に実施するだけでは、コンピュータ化システムの品質及び信頼性を高度に保証することはできない。品質が製品に組み込まれるように*開発者が正式に計画したアプローチ*が必要である。ISO 9001 は、設計／開発／製造／据付／サービス提供における品質保証のための品質システムモデルを提供している。サプライヤがソフトウェア開発中に行うテストの目的は、厳格なテスト方法により、ソフトウェアの構造的インテグリティを壊して、あらゆる弱点をも見つけ出そうとすることである。プロジェクトにおけるリスク分析の結果で必要と判断された場合、規制対象ユーザー自身又はその代理者によるサプライヤ監査でこれらの課題をカバーすべきである。

7.2	ISO/IEC 12207:1995 provides guidance on acceptable practices for Information Technology - Software life cycle processes and ISO 9004, ISO 10005 and ISO 10007 provide guidance on Quality Management and system elements, including quality plans and configuration management. IEEE 1298 is specific and prescriptive on what should be addressed in planning. ISO 9126 concerns software quality and defines the quality attributes for critical applications. The GAMP Guide also provides relevant guidance for the pharmaceutical sector.	ISO/IEC 12207:1995 は、IT – ソフトウェアライフサイクルプロセスで許容可能な慣行についてのガイダンスを提供している。また、ISO 9004、ISO 10005 及び ISO 10007 は、品質管理、及び品質計画と構成管理を含むシステム要素についてのガイダンスを示している。IEEE 1298 は計画で取り上げるべき事項を具体的に規定している。ISO 9126 は、ソフトウェア品質を対象とし、重要なアプリケーションについての品質属性を定義している。GAMP ガイド【巻末訳注 2】も製薬セクターに対する関連ガイダンスを掲載している。
7.3	*It would be expected that the regulated user's Validation Policy or Validation Master Plan (VMP)[10] should identify the company's approach to validation and its overall philosophy with respect to computerised systems. The VMP[11] should:* • Identify which computerised systems are subject to validation. • Provide brief descriptions of the validation strategies for different categories of computerised systems as well as other validation activities. • Outline protocols and related test procedures for all validation activities including computer systems. • Define reporting requirements to document validation exercises and related results. • Identify key personnel and their responsibilities as part of the Validation Program.	*規制対象ユーザーのバリデーション方針又はバリデーションマスター計画 (VMP)[10] では、会社のバリデーションについてのアプローチとコンピュータ化システムに関する全般的な考え方を示すことが期待される。VMP[11] には以下が必要である。* • バリデーション対象となるコンピュータ化システムを特定する。 • コンピュータ化システムのカテゴリに応じたバリデーション戦略、及び他のバリデーション活動について簡単に説明する。 • コンピュータシステムを含む全てのバリデーション活動について、実施計画及び関連テスト手順の概要を示す。 • バリデーション実施内容とその結果を文書化するための報告要件を定義する。 • バリデーションプログラムの一環として主となる要員とその責任を特定する。

[10] Refer to GMP Annex 15 for more details concerning the VMP requirements.
[10] VMP の要件の詳細については、GMP Annex 15 を参照。
[11] It may be appropriate to refer to established policies, SOPs or individual validation plans to meet these requirements.
[11] これらの要件を満たすには、確立された方針、SOP、又は個々のバリデーション計画を参照することが適切であろう。

8. MANAGEMENT AND RESPONSIBILITIES

8. 管理と責任

8.1	*It is important for a regulated user to have in place a comprehensive policy and procedures for the specification, purchase, development and implementation of computerised systems. Ideally these procedures would cover all computerised systems;* this PIC/S document will only concern itself with those systems that have an impact on GxP requirements.	*規制対象ユーザーがコンピュータ化システムの仕様／購入／開発／実装について包括的な方針と手順を定めておくことは重要である。その手順で全てのコンピュータ化システムをカバーできることが理想ではあるが、*本書は、GxP 要件に影響を及ぼすシステムのみを対象とする。
8.2	The organisation should regard disciplines related to the introduction of a computerised system as in accord with the basic principles of project management. Achieving the quality, performance and reliability objectives for any project requires competence in engineering and design. Where regulated users do not have the resources for engineering and design within their own organisation, there is a heavy reliance on the supplying company's resources.	コンピュータ化システムの導入に必要な規律は、プロジェクト管理の基本原則に合わせるべきである。プロジェクトで品質／性能／信頼性の目標を達成するためには、エンジニアリングと設計の能力が必要である。規制対象ユーザーがその組織内にエンジニアリングと設計のリソースを持たない場合、サプライヤ会社のリソースに大きく依存することになる。
8.3	To satisfy the quality, performance and reliability objectives, the regulated user needs to assure that the supplier's management policies; systems and related procedures will achieve the desired objectives. Enlightened suppliers should provide such evidence and added value to all customers, whether large or small, through the recognition of industry standards from GAMP Forum, Supplier Forum, PDA, ISPE, etc., and also through shared audits, user groups, and product certification arrangements.	規制対象ユーザーが品質／性能／信頼性の目的を達成するためには、サプライヤの管理方針／システム／関連手順が望む目的を達成するものであることを保証する必要がある。十分理解しているサプライヤは、規模の大小を問わず、GAMP Forum、Supplier Forum、PDA、ISPE 等の業界標準を認識すること、及び監査結果の共有／ユーザーグループ／製品の認定証の準備を行うことで、全ての顧客に対して、そういった証拠と付加価値を提供するであろう。
8.4	*It is important to acknowledge that the scope and level of documentation and records needed to formalise and satisfy basic project management requirements for critical systems will be dependent upon:* • *the complexity of the system and variables relating to quality and performance;* • *the need to ensure data integrity;* • *the level of risk associated with its operation;* • *the GxP impact areas involved.*	*重要なシステムについて、どの範囲やレベルで文書や記録を文書化すれば、基本的なプロジェクト管理要件を正式化し、満足することになるのかは、以下に依存することを認識しておくことが重要である。* • *システムの複雑さ、及び品質／性能に関連する変動要素* • *データインテグリティを確実にする必要性* • *運用に関連するリスクレベル* • *GxP に影響のある領域*

8.5	Within the regulated user organisation there should be clearly defined responsibilities for the management of all ICT[12] products, computerised systems and projects. Management should cover the full spectrum, from simple input/output devices and programmable logic controllers (PLCs) through to integrated supervisory or information systems and business management levels. These responsibilities should involve development and administration of policies on purchase of IT products, as well as the introduction, commissioning and maintenance of IT products. The responsibilities should extend to development and implementation of formal monitoring, auditing and servicing of each system and designate the related documentation and records for such activities.	規制対象ユーザー組織内で、全ての ICT[12] 製品、コンピュータ化システム、及びプロジェクトについて管理する責任を明確に定義すべきである。管理対象は、単純な入出力デバイスやプログラマブルロジックコントローラ（PLC）から、統合された監視システム／情報システムやビジネス管理レベルまで、幅広くカバーすべきである。これらの責任には、IT 製品の導入、試運転や保守だけでなく、開発及び購入に関する方針の管理も含まれる。各システムに対する正式な監視／監査／サービスを開発／実装することも責任に含め、こうした活動に関連する文書と記録を定めるべきである。
8.6	*BS 7799: 1999, (13), is issued in two parts (Part 1: Code of practice for information security management, and Part 2: Specification for information security management systems) and provides recommended guidance on a comprehensive set of controls comprising best practices in information security[13] . These controls and measures (or the equivalent) are recommended for adoption within this PIC/S guidance. They will assist in drafting the internal control standards and procedures to be implemented by IT management and administration departments.*	*BS 7799: 1999, (13) は以下の 2 部構成で発行されており、情報セキュリティのベストプラクティスから構成される、包括的なコントロールについての推奨ガイダンス[13] を掲載している。* *Part 1: Code of practice for information security management* *Part 2: Specification for information security management systems* *本書では、このようなコントロールや方策（又は同等のもの）を採用することを推奨している。これらは、IT 管理及び管理部門が実装する内部コントロールの基準や手順を起草するうえで役立つであろう。*

[12] ICT = Information and Communications Technology
[13] Relevant recent guidance is also provided in ISO/IEC17799:2000 on Information Technology － "Code of practice for information security management" and also in the pre-amble to FDA's 21 CFR Part 11【訳注】.
【訳注】ISO17799 は現在では ISO27002 となっている。Part 11 Preamble の和訳については https://bunzen.co.jp/ 参照。

9. USER REQUIREMENT SPECIFICATIONS (URS)

9. ユーザー要求仕様書 (URS)

9.1	When utilising a computerised system within a regulated environment it is appropriate to establish *system control documentation or a system description,* [e.g. as required by GMP Annex 11(4)],[14] giving a written detailed description of the system, also covering development and maintenance.[15] This system control document may include a record of, or a reference to, the documented 'User Requirement Specifications' (URS), or other life-cycle documents. It should also be the definitive statement of what the system must or must not do. This document is also important for legacy systems and those systems under development.[16]	規制環境下でコンピュータ化システムを利用する場合、[例えば、GMP Annex 11(4) 【巻末訳注1】で要求されているように]*システムコントロール文書又はシステム記述書*を作成[14]し、文書にシステム詳細を記述し、開発と保守[15]もカバーするとよい。このシステムコントロール文書には、「ユーザー要求仕様書(URS)」等のライフサイクル文書の記録又は参照が含まれるであろう。〔この文書は〕システムがしなければならないこと、してはいけないことを定める宣言でもある。レガシーシステムや開発中のシステムにおいてもこの文書は重要である[16]。
9.2	*When properly documented, the URS should be complete, realistic, definitive and testable. Establishment and agreement to the requirements for the software is of paramount importance. Requirements also need to define non-software (e.g. SOPs) and hardware.*	*適切に文書化された URS は、完全で、実現可能で、あいまいさがなく、テスト可能なものとなるはずである。ソフトウェア要件を確立し、合意することは最も重要である。要件には、非ソフトウェア要件（例：SOP）やハードウェア要件についても定義する必要がある。*
9.3	*"User Requirement Specifications", (URS), requirements should satisfy the following criteria:* • *Each requirement document should be reviewed, authorised and uniquely catalogued.* • *There should be no conflict between requirements.* • *Each requirement, particularly those to be met to satisfy GxP expectations, should be* specified in a manner such that compliance with the requirements is capable of being verified objectively by an authorised method, e.g. inspection, analysis or test.	*「ユーザー要求仕様書」(URS) の要件は、以下の基準を満たすべきである。* • *各要件文書はレビュー、承認し、一意にリスト化すること。* • *要件同士が矛盾しないようにすること。* • *各要件、特に GxP の期待を満足するために適合すべき要件は、要件への適合が承認された方式（例：検査、分析、又はテスト）により客観的に検証できるように記載すべきである。*

[14] Linked, approved system life-cycle records may very well meet the requirements for the system control documentation/system description.
[14] 関連付けられ、承認されたシステムのライフサイクル記録は、システムコントロール文書／システム記述書の要件を十分満たすであろう。
[15] Development and maintenance information may often be held in separate (referenced) documents for large complex systems.
[15] 大規模で複雑なシステムでは、開発や保守に関する情報は別個の（参照された）文書に記載されることが多い。
[16] Risk assessment in the URS phase also needs to be addressed.
[16] URS フェーズにおけるリスクアセスメントについても対応する必要がある。

	• *The URS, although independent of the supplier should be understood and agreed by both user and supplier[17]. There should be a clear distinction between mandatory regulatory requirements and optional features.* • *The URS should contain functional and non-functional requirements: functionality, effectiveness, maintainability, usability, etc. Requirements should be objectively verifiable.[18]*	• *URS はサプライヤからは独立したものであるが、ユーザーとサプライヤの双方が理解し、合意すべきものである[17]。必須の規制要件とオプション機能は明確に区別すべきである。* • *URS には機能及び非機能要件（機能、有効性、保守性、操作性等）を含むべきである。要件は客観的に検証できる[18]ようにすべきである。*
9.4	Evaluation of the URS and the functional specifications should allow identification of the GxP requirements covered by the system. Additionally the URS will provide information as to where there are important interfaces between the system and manual operations. *The URS should also form the basis for a risk assessment of the system for GxP compliance requirements, in addition to other risks such as safety. The risk analysis may be based on the FS, which is related to the URS, (e.g. for bespoke systems). The risk assessment and the results including the reasons for the ranking as either: 'critical' or 'not critical' should be documented.[19] The nature of any GxP risks should be clearly stated.*	URS 及び機能仕様書を評価する際に、システムがカバーする GxP 要件を特定しておくべきである。さらに、URS には、どこにシステムと手動操作の間の重要なインターフェースがあるのかといった情報も含まれる。*また、URS はシステムの GxP 適合要件に対するリスク及び（例えば、安全性等の）他のリスクをアセスメントする際の基本となる。リスク分析は、（例えば、カスタムシステムでは）URS に関連する FS を用いて行うこともある。リスクアセスメント及びその結果は、「重要」、「非重要」に分類した理由とともに文書化すべきである[19]。GxP に関するすべてのリスクは、その性質を明確に記載する必要がある。*

[17] Note: This is straightforward for a bespoke system. However, for marketed proprietary systems or configurable packages then it is for prospective users, integrators and suppliers to discuss and review proposed user requirements, versus package functionality. It is essential to determine the 'degree of fit' and then control any necessary configuration work, modification, coding, testing and validation requirements in line with this guidance.

[17] 注意：このことはカスタムシステムの場合は明白である。市販されているサプライヤ独自のシステムや構成設定可能なパッケージの場合は、利用を検討しているユーザー、インテグレータ、及びサプライヤが、提案されたユーザー要件をパッケージ機能に照らして討議し、レビューする。「適合性の度合い」を判断し、構成設定作業／修正／コーディング／テスト／バリデーションを行う必要があれば本ガイダンスに添ってコントロールすることが必須である。

[18] When choosing a 'standard product' or component, the URS may be developed compiling required features from the supplier's specifications.

[18]「標準製品」又はコンポーネントを選定するときは、サプライヤの仕様書から必要な機能を編集して URS を作成してもよい。

[19] Risk assessments and analyses can be useful at various stages during the entire system life-cycle and not just for the FS or URS, (see also GAMP 4 'M3').

[19]リスク評価とリスク分析は、単に FS 又は URS のためだけでなく、システムのライフサイクル全体の様々な段階で役立つ（GAMP 4 'M3' も参照）。

9.5	All computerised systems should have been subjected to documented prospective validation or qualification. Readers should refer to Section 15 of this document for validation strategies for different categories of software and systems. However, as user's systems evolve through modification, enhancement or integration and in response to additional regulatory requirements, it may be necessary to conduct additional re-qualification and revalidation work on the existing systems. The URS and 'System Description' document should be correspondingly updated as validation life cycle evidence. *Figure 2 (see Section 11 below) shows the relationship between URS and performance qualification (PQ).*	全てのコンピュータ化システムは、文書化された予測的バリデーションや適格性評価を済ませておく必要がある。様々なカテゴリのソフトウェア／システムのバリデーション戦略については本書の 15 章を参照のこと。ただし、ユーザーのシステムは修正、拡張や統合により、又は新たな規制要件に対応するために進化していくため、既設システムについて新たに再適格性評価や再バリデーションを実施する必要が生じる場合がある。URS と「システム記述書」は、その度にバリデーションライフサイクルの証拠として更新すべきである。 *図 2（以下の 11 章を参照）に URS と性能適格性評価 (PQ) の関係を示す。*

10. FUNCTIONAL SPECIFICATIONS (FS)

10. 機能仕様書 (FS)

10.1	From the URS, the supplier (this would include in-house developer) of the software would be able to develop the functional specifications (in the case of bespoke programs) or clearly identify the functional specifications for selection and purchase of off-the-shelf systems. The functional specifications should define a system to meet the URS, i.e. the customer's needs.	ソフトウェアのサプライヤ（社内開発者を含む）は、URS をもとにして、機能仕様書（カスタムプログラムの場合）を作成したり、又は市販システムの選定／購入のための機能仕様を明確に特定したりできるであろう。機能仕様書は、URS、すなわち顧客のニーズ、を満たすシステムを定義するものである。
10.2	The functional specifications should provide a precise and detailed description of each of the essential requirements for the computer system and external interfaces. This means descriptions of functions, performances and where applicable, design constraints and attributes.	機能仕様書には、コンピュータシステム及び外部インターフェースに不可欠な各要件についての明確かつ詳細な記述を盛り込むべきである。つまり、機能、性能、及び（該当する場合は）設計上の制約と属性について記述する。
10.3	*For particular types and levels of systems it may be appropriate to have a combined URS and FS. Section 14 of this document gives further details of validation strategies for the five different categories for computer software as identified in the GAMP Guide.*	*システムのタイプとレベルによっては、URS と FS をまとめることが妥当な場合がある。本書の 14 章では、GAMP ガイド【巻末訳注 2】に記載されているコンピュータソフトウェアの 5 つのカテゴリに対するバリデーション戦略をさらに詳しく説明する。*
10.4	*The regulated user should be able to provide documentation describing the computer system(s) to include logic flow or block diagrams where practical, also giving an indication of hardware layout, networks and interaction. These basic schematics should align with the functional specification and be traceable to the URS. Within the EU it is logical for this information to be held*	*規制対象ユーザーは、コンピュータシステムを説明する文書を提示できるようにすべきである。その文書には、適切な場合はロジックフロー又はブロック図を含め、ハードウェアのレイアウト、ネットワーク、及びやり取りが分かるようにすべきである。このような基本的な図表は、機能仕様に整合性をもたせる*

	within the controlled 'System Description' document, required by GMP Annex 11 (4).	*ようにし、URS に対してトレースできるようにすべきである。EU 内では、GMP Annex 11 (4)【巻末訳注 1】で要求されているように、このような情報をコントロールされた「システム記述書」に記載することが合理的であろう。*

11. SUPPLIERS, SOFTWARE DEVELOPERS AND QUALITY MANAGEMENT

11. サプライヤ、ソフトウェア開発者、及び品質管理

	Figure 2 below maps the relationships between the key specification and qualification elements as the system is specified, designed, built and tested.	以下の図 2 は、システムの仕様作成／設計／構築、及びテストの各段階に応じた主な仕様と適格性評価の要素の関係を示している。

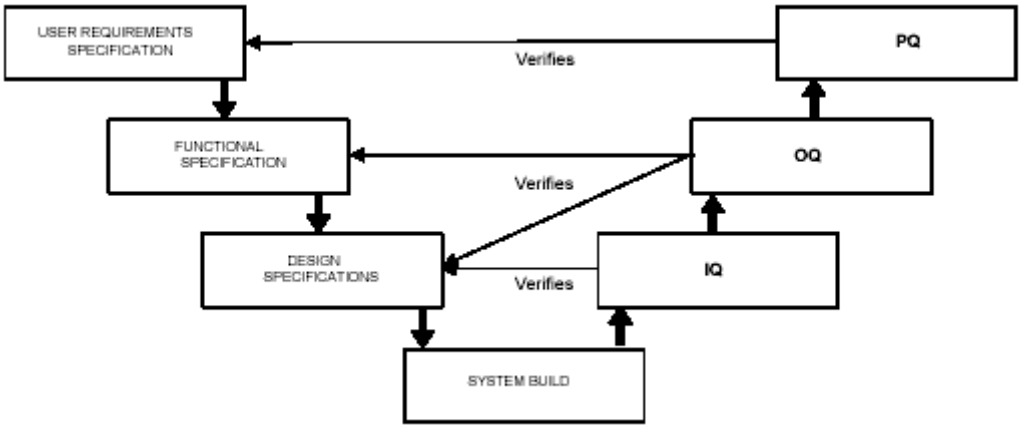


Figure 2. Basic framework for specification and qualification (based on Figure 6.2 of GAMP-4)[20]

図 2 仕様と適格性評価の基本的な枠組み（GAMP4【巻末訳注 2】の図 6.2 に基づく）[20]

[20] This is an example only. Regulated users would be expected to comment on their own particular model. They should also interpret and define the relationships between various life-cycle elements as appropriate.
[20] これはあくまで例である。規制対象ユーザーは自社の〔開発〕モデルについて説明することが期待される。また必要に応じライフサイクルの様々な要素間の関係を解釈し、定義すべきである。

11.1	The quality controls and quality assurance procedures, documentation and records related to the development and production of the software and hardware for computer systems are of critical importance. There are a number of accepted models for software development, e.g. the spiral model of development, the waterfall model and the life cycle model. All models have their own special attributes. As an example the GAMP guide adopts, but does not mandate a "V" framework (see figure 2 above). (Note: The URS and FS may be combined for smaller projects. These are related to the OQ.)	品質コントロールと品質保証の手順、コンピュータシステムのソフトウェアとハードウェアの開発と製造に関わる文書と記録は非常に重要である。ソフトウェア開発には、一般に認められたモデルが数多くある（例：スパイラルモデル、ウォーターフォールモデル、ライフサイクルモデル等）。各モデルにはそれぞれ特徴がある。例として、GAMP ガイド【巻末訳注 2】では "V" フレームワーク（上の図 2 を参照）を採用しているが、これは必須ではない（注意：小規模システムでは URS と FS をまとめてもよく、それらは OQ に対応する）。
11.2	Supplier and developer reputations and trading histories for the software product provide some guidance to the level of reliability that may be assigned to the product supplied. *The pharmaceutical regulated user therefore should have in place procedures and records that indicated how and on what basis suppliers were selected.*	サプライヤと開発者の評判、ソフトウェア製品についての取引履歴は、供給される製品がどの程度信頼できるかを示す一定の指針となる。*従って医薬規制対象ユーザーは、サプライヤ選定の方法と根拠を示す手順と記録を用意すべきである。*
11.3	Compliance with a recognised Quality Management System (QMS) may provide the regulated user and regulatory agencies with the desired confidence in the structural integrity, operational reliability and on-going support for software and hardware products utilised in the system. The accreditation assessment schedule and scope of certification needs to be relevant to the nature of the proposed application. Structural integrity and the application of good software and hardware engineering practices are important for critical systems.	世間で認められた品質管理システム (QMS) に適合することにより、システムで使用されているソフトウェア製品とハードウェア製品の構造的インテグリティ／運用の信頼性／継続的なサポートについて規制対象ユーザーと規制当局の望むような信用を得ることができる。認証アセスメントのスケジュールや対象範囲は、提案されているアプリケーションの性質をアセスメントするうえで意味のあるものとする必要がある。重要なシステムにとって、構造的インテグリティ、及びソフトウェア／ハードウェアにグッドエンジニアリングプラクティスを適用することは重要である。
11.4	Confidence in the structural integrity may be based to some extent on the recognition of relevant certification of a company's software and hardware development methodology and QMS to ISO 9001 standard, such as (for example) TickIT certification and utilisation of ISO 9000 related guidance. However, it is essential that the assessment scope and schedules applied by the certifying auditors for these schemes should cover the engineering quality standards, actual practices, controls and records in place including non-conforming product (error feedback from the market), corrective actions, change management and so forth for particular products and versions. These can be very useful benchmarks for the design engineering, replication and maintenance	会社のソフトウェア／ハードウェアの開発手法が何らかの有効な認証を受けていることが分かれば、構造的インテグリティをある程度信用することができる。また〔会社の〕QMS は（例えば TickIT 認証や ISO9000 関連のガイダンスの利用等の）ISO 9001 規格〔認証を受けていること〕により信用することができる。しかしながら、これらの取り組みにおける認証機関の審査者によるアセスメントの範囲とスケジュールが、会社におけるエンジニアリング品質基準、実際の慣行、コントロール、記録（特定の製品やバージョンについての不適合品（市場からのエラーのフィードバック）、是正措置、変更管理等を含む）を

	standards in place at suppliers of large proprietary packages and can assist pharmaceutical clients with short listing and selection criteria.	カバーしていることが必須である。これら〔の認証〕は、大規模な独自パッケージを提供するサプライヤの持つ設計エンジニアリング／複製／保守の基準を評価するためのベンチマークとして非常に有効であり、医薬品業界の顧客がサプライヤを絞り込み、選定する助けとなる。
11.5	However, an assessment of the supplier's QMS and recognised certification alone is unlikely to be the final arbiter for critical systems. The certification may very well be inadequate, or inappropriate. *In such cases, the regulated user may wish to consider additional means of assessing fitness for purpose against predetermined requirements, specifications and anticipated risks. Techniques such as supplier questionnaires, (shared) supplier audits and interaction with user and sector focus groups can be helpful.* This may also include the specific conformity assessment of existing, as well as bespoke software and hardware products. GAMP and PDA guideline documents identify a need to audit suppliers for systems carrying a high risk and have detailed guidance on supplier auditing procedures/ options.	しかし、サプライヤの QMS アセスメントや認知された認証だけでは、重要なシステムを最終的に選定する要因にはならないであろう。認証が不十分又は不適切であるかもしれない。*このような場合、規制対象ユーザーは、あらかじめ定められた要件／仕様／予測されるリスクについて、利用目的への適合性をアセスメントするための追加的手段を検討してもよいであろう。サプライヤへの質問票、（共有）サプライヤ監査、及びユーザーと業界フォーカスグループとのやり取り等のテクニックは有用である。*これには、カスタマイズされるソフトウェア／ハードウェア製品だけでなく既存のソフトウェア／ハードウェア製品に対する適合性アセスメントも含まれるであろう。GAMP と PDA のガイドライン文書では高リスクのシステムについてサプライヤを監査する必要性を明らかにし、サプライヤ監査の手順／選択肢について詳細なガイダンスを示している。
11.6	Appendix O9 of the GAMP 4 Guide incorporates an independent commentary on PIC/S GMP Annex 11 and provides specific advice on quality and operational matters to help ensure compliance with the PIC/S and EU GMP. Users and suppliers need to ensure that software, hardware and systems are: • quality assured; • fit for their intended purpose; and • *supported by appropriate documentation for quality and validation traceability.*	GAMP 4 Guide【巻末訳注 2】の付録 O9 では、PIC/S GMP Annex 11【巻末訳注 1】に対する独自のコメントを掲載し、PIC/S 及び EU GMP に確実に適合するための品質及び運用の具体的な助言を提供している。ユーザーとサプライヤはソフトウェア／ハードウェア／システムを確実に以下のようにする必要がある。 • 品質が保証されている。 • 意図した利用目的に適合している、及び • *品質及びバリデーションのトレーサビリティが適切な文書によって裏付けられている。*

12. IMPORTANT QMS AND SOFTWARE STANDARDS ATTRIBUTES

12. QMS とソフトウェア規格の重要な属性

12.1	The Standards ISO 9001, ISO 9126 & IEEE 1298 have a number of important features that can be summarised in the following points: • They are structured around a QMS approach to the development, testing and documentation for software design, production and installation. • Compliance with the standard requires formal systems for control, traceability and accountability of product(s) and personnel. • The standard outlines the features and requirements of a life cycle approach to software production ("manufacture"), with emphasis on the importance of a change control procedure. • The need for, and importance of, testing of software product/s is identified by the standard as it requires a tiered approach to testing and identifies three levels of testing for software: - Unit code testing; - Integrated module testing; and - Customer acceptance testing. - The GAMP Guide is also widely used as an industry standard of relevance here.	ISO 9001, ISO 9126、及び IEEE 1298 の規格には多くの重要な部分があり、以下のように要約できる。 • これらの規格はソフトウェアの開発、テスト、及び設計／製作／据付の文書化に対する QMS アプローチを中心に構成されている。 • 規格に適合するためには、製品と要員のコントロール、トレーサビリティ、説明責任に関する正式なシステムが必要である。 • 規格はソフトウェア製造（「生産」）のライフサイクルアプローチの特徴と要件の概要を示し、変更コントロール手順の重要性を強調している。 • 規格でソフトウェア製品のテストの必要性、重要性を明らかにしており、テストに対し階層的なアプローチを要求し、ソフトウェアに対し次の 3 レベルのテストを特定している。 - 単体コードテスト - 統合モジュールテスト - 顧客の受入テスト - GAMP ガイド【巻末訳注 2】も有効な業界規格として広く使用されている。
12.2	There are a number of advantages in organisations utilising a QMS approach for development and changes to software product. It would be expected that this approach if utilised by developers and producers of software should ensure (within the limitations of the quality management system approach) the following: • Management commitment to quality and design control by instituting systems for quality control, documentation and quality assurance. • Development, production and installation based on quality plans, verified by quality records. The QMS requires development, testing and programming standards.	ソフトウェア製品の開発と変更に QMS アプローチを採用する組織には、数多くの利点がもたらされる。このアプローチをソフトウェアの開発者と製造者が利用すれば、（品質管理システムのアプローチの範囲内で）以下が確実になることが期待される。 • 品質コントロール、文書化、品質保証のシステムを設けることによる、品質と設計のコントロールへの経営層のコミットメント。 • 品質計画に基づき、品質記録によって検証される開発／製造／据付。QMS では開発／テスト／プログラミングの基準が必要となる。

	• Adherence to quality assurance disciplines such as internal audits of the processes, corrective & preventative action procedures and control of non-conforming product. • QMS methodology to establish requirements for purchased (subcontracted) software product.	• 品質保証の規律の遵守（例えば、プロセスの内部監査、是正予防措置の手順、不適合品のコントロール等）。 • 購入した（委託した）ソフトウェア製品に対する要件を作成するための QMS 手法。

13. TESTING

13. テスト

13.1	Assurance of reliability of software is achieved by execution of quality plans and testing during the software development process. This involves unit code testing and integration testing in accordance with the principles of ISO 12207, IEEE 1298 and IEEE 829 'Software Test Documentation'[21] . See also the corresponding sections in the GAMP Guide. *The development and testing of hardware and software should be done under a quality assurance system, documented and formally agreed between the various parties. This can ultimately provide evidence in support of GxP quality compliance (e.g. Annex 11(5)). Locations and responsibilities for testing (depending on the category of the software and system) are outlined in the GAMP Guide, qv.*	ソフトウェア開発プロセスにおける品質計画とテストの遂行によりソフトウェアの信頼性に対する保証が得られる。これには、ISO 12207、 IEEE 1298、IEEE 829 「Software Test Documentation」[21] の原則に従った単体コードテストと統合テストが含まれる。GAMP ガイド【巻末訳注 2】の該当する章も参照のこと。*ハードウェア／ソフトウェアの開発及びテストは、品質保証システムのもと行われるべきであり、文書化され、各当事者間で正式に合意される必要がある。これにより最終的に、GxP 品質への適合（例：Annex 11 (5)【巻末訳注 1】）を裏付ける証拠を得ることができる。テストを行う場所及び責任（ソフトウェア／システムのカテゴリに依存する）は、GAMP ガイド【巻末訳注 2】に概要が記載されているので参照のこと。*
13.2	One of the most critical aspects of development of software is the integration testing phase where individual elements of software code (and hardware, where applicable), are combined and tested during or prior to this stage until the entire system has been integrated. Extra benefits may be achieved by code walk-throughs including evaluation of critical algorithms and/or routines, prior to testing. Errors found at the integration testing phase are much cheaper to correct than errors found at a later stage of testing. Code review (walk-through) is best done as early in the process as possible, preferably before submitting	ソフトウェア開発におけるもっとも重要な部分の一つは統合テストフェーズであり、このステージ中又は事前に、ソフトウェアコード（及び該当する場合はハードウェア）の各要素を結合し、テスト行う。これはシステム全体が統合されるまで繰り返す。テスト実施前に重要なアルゴリズム及び（又は）ルーチンの評価を含むコードウォークスルーを行っておくことにより、さらに良い結果が得られるであろう。統合テストフェーズで見つかったエラーは、この後で行われるテストで見つか

[21] This testing is defined as verification of the software element. Verification is defined as the process of determining whether or not the products of a given phase of the software development cycle fulfil the requirements established during the previous phase.
[21] このテストはソフトウェア要素を検証するものである。この場合の検証とは、ソフトウェア開発サイクルにおいて、あるフェーズの成果物が、その前のフェーズで定められた要件を満たしているか否かを判断するプロセスのことである。

	a module to test. Code reviews are best performed before formal unit code testing (i.e. before a unit or module is frozen and enters formal testing).	るエラーよりもかなり低コストで修正できる。コードレビュー（ウォークスルー）は、可能な限りプロセスのなるべく早い段階で行うと効果的であり、できればモジュールをテストに回す前に行うことが望ましい。コードレビューは、正式な単体コードテスト前（すなわち、単体又はモジュールが固定され、正式なテストに入る前）に実施するのが最もよい。
13.3	For some simpler GxP systems, for example certain PLCs and systems based on basic algorithms or logic sets, the functional testing may provide adequate assurance of reliability of the computerised system. For critical and/or more complex systems the verification testing that is conducted at the IQ, OQ & PQ stages provides only a limited level of assurance that the system does what it purports to do, reliably. This level of testing provides only limited assurance of the operation and reliability of hidden functions and code. For complex systems there should also be a high level of assurance that the development of the software has ensured delivery and operation of a quality product that is structurally sound, clearly defined and controlled.	単純な GxP システム（例えば一部の PLC、及び基本アルゴリズム／論理セットに従うシステム）であれば、機能テストによりコンピュータ化システムの信頼性を適切に保証することができる場合がある。重要及び（又は）複雑なシステムでは、IQ／OQ／PQ ステージで実施される検証テストで、システムが信頼性を持って意図したことを実行できることを完全に保証することはできない。このレベルのテストでは、隠れた機能／コードの操作と信頼性に対して得られる保証には限りがある。複雑なシステムでは、ソフトウェア開発〔プロセス〕により、高品質の製品（適切に構造化され、明確に定義／コントロールされている）が確実に引き渡し／運用されていることの高度な保証が必要である。
13.4	*Test scripts should be developed, formally documented and used to demonstrate that the system has been installed, and is operating and performing satisfactorily. These test scripts should be related to the User Requirements Specifications and the Functional specifications for the system.* This schedule of testing should be specifically aimed at demonstrating the validation of the system[22] . In software engineering terms satisfactory results obtained from the testing should confirm design validation.	*システムが据え付けられ、満足に機能／稼動していることを示すために、テストスクリプトを作成し、正式に文書化し、使用すべきである。このようなテストスクリプトはシステムのユーザー要求仕様書と機能仕様書に関係付ける必要がある。*このテストをスケジュールする際は、特にシステムの妥当性を実証することを目的とすべきである[22]。ソフトウェアエンジニアリングでは、テストにおける満足な結果により、設計の妥当性が確認される。
13.5	Any processing equipment and activities related to or controlled by the computer system would require additional IQ, OQ and PQ testing regimes.	コンピュータシステムに関連する、又はコンピュータシステムによってコントロールされ

[22] The supplier/developer should draft test scripts according to the project quality plan to verify performance to the functional specifications. The scripts should stress test the structural integrity, critical algorithms and 'boundary value' aspects of the integrated software. The test scripts related to the user requirements specification are the responsibility of the regulated users.
[22] サプライヤ／開発者は、機能仕様書に対し性能を検証するためにプロジェクトの品質計画に従いテストスクリプトを作成すべきである。このスクリプトでは、統合ソフトウェアの構造的インテグリティ、重要なアルゴリズム、及び「境界値」の側面のテストに重点を置くべきである。ユーザー要求仕様書に関連するテストスクリプトは規制対象ユーザーの責任である。

	It may be appropriate to combine test phases and test scopes for a group of equipment or activities, and this should be defined in a test plan or strategy.	る、処理装置（加工装置）や活動には、追加的な IQ／OQ／PQ のテスト体制が新たに必要となるであろう。一連の装置や活動について、テストフェーズ及びテスト範囲をグループ化することが適切な場合もあり、そのことはテスト計画又は戦略にて定義しておくべきである。
13.6	Regulated Users should be able to demonstrate formal acceptance of systems after testing and controlled transfer into the live operational environment.	規制対象ユーザーは、テスト及び本番稼動環境へのコントロールされた移行の後に、システムを正式に受け入れたことを説明できるようにすべきである。

14. VALIDATION STRATEGIES AND PRIORITIES

14. バリデーション戦略と優先順位

14.1	Regulated users need to be able to provide evidence for their computerised systems to demonstrate their range, complexity, functionality, control and validation status.	規制対象ユーザーは、自社で使用しているコンピュータ化システムについて範囲、複雑さ、機能、コントロール、及びバリデーションステータスを示す証拠を提示できるようにする必要がある。
14.2	For the validation of computerised systems there should be a system in place that assures the ***formal assessment and reporting*** of quality and performance measures for all the life-cycle stages of software and system development, its implementation, qualification and acceptance, operation, modification, re-qualification, maintenance and retirement[23]. This should enable both the regulated user, and competent authority, to have a high level of confidence in the integrity of both the processes executed within the controlling computer system(s) and in those processes controlled by and/or linked to the computer system(s), within the prescribed operating environment(s).[24] (See also Section '4.6')	コンピュータ化システムのバリデーションでは、ソフトウェア／システム開発ライフサイクルの全てのステージの品質と性能の方策、その実装、適格性評価と受入、運用、修正、再適格性評価、保守、リタイアメントについての***正式なアセスメントと報告***を保証するシステムが必要である[23]。これにより、規制対象ユーザーと当局の双方が、事前に定められた運用環境において、制御するコンピュータシステム内で実行されるプロセス及びそのコンピュータシステムに制御及び（又は）リンクされるプロセスの両方のインテグリティについて、高いレベルの確証を持つことができる[24]（「4.6」章も参照）。

[23] Tools and controls within the QMS, such as audits, change controls, configuration management and continuous improvement programmes may feature here.
[23] 監査、変更コントロール、構成管理、継続的な改善プログラム等、QMS 内でのツールとコントロールはここでの重要な一部である。
[24] The italicised-bold part of this definition should be interpreted as requiring controlled documented methodology and records based on best compliance practices. This is to ensure that firms have generated documented evidence (electronic and/ or paper based), that gives a high level of assurance that both the computer system and the computerised system, will consistently perform as specified, designed, implemented and validated. Related validation dossiers for complex integrated projects should be clearly cross-linked for audit purposes.
[24] この定義の斜体太字表記部分は、ベストコンプライアンスプラクティス（best compliance practices）に基づき要求される、コントロールされた、文書化された方法と記録であることを表している。これにより会社

14.3	***The regulated user's range of computerised systems needs to be formally listed in an inventory*** *and the scope/extent of validation for each detailed in a consolidated written Validation programme[25]. Validation scope should include GxP compliance criteria, ranked for product/process quality and data integrity risk criticality, should the system fail or malfunction.* This process represents one of the most important pre-requisites of Validation Master Planning (*see PIC/S doc. PI 006*), in that it is essential to assign priorities and attention to those systems (and features within systems) that represent the highest potential for disaster, should they malfunction or become inoperative. The risk analyses and the results, together with reasoning for ***critical*** or ***non-critical*** classifications, should be documented. Risks potentially impacting on GxP compliance should be clearly identified. There are a number of techniques to help identify and analyse risks and to select risk reduction and control measures. For further information refer to the GAMP Guide appendix and the GAMP Forum special interest group paper on 'Functional Risk Assessment'.	***規制対象ユーザーのコンピュータ化システムは、正式にシステム台帳へリスト化し、****それぞれのバリデーションの範囲／程度を、統合されたひとつのバリデーションプログラム文書を詳細に示す[25]。バリデーション範囲には、システム故障や機能不良が発生した場合の、製品／プロセスの品質とデータインテグリティに及ぼすリスクの重要度に応じてランク付けした GxP 適合基準を含むべきである。*故障又は動作不能時に最大の惨事を招く可能性のあるシステム（及びシステム内の機能）を優先し、関心を向けることが重要であるという意味で、このプロセスはバリデーションマスター計画（*PIC/S doc. PI 006 を参照*）の最も重要な前提条件の１つである。リスク分析とその結果は、***「重要」***又は***「非重要」***に分類した根拠と合わせて文書化すべきである。GxP 適合に影響を及ぼし得るリスクは、明確に特定すべきである。リスクの特定／分析を支援し、リスクを軽減／コントロールする方策を選択するためのテクニックは数多く存在する。詳しい情報については、GAMP ガイド【巻末訳注 2】の付録と GAMP Forum Special Interest Group の「Functional Risk Assessment」に関する文書を参照のこと。
14.4	GxP compliance evidence is essential for the following aspects and activities[26] related to computerised systems: • data input (capture and integrity), data filing, data-processing, networks, process control and monitoring, electronic records, archiving, retrieval, printing, access, change management, audit trails and decisions associated with any automated GxP related activity;	GxP 適合の証拠は、コンピュータ化システムに関わる以下の側面と活動[26]において不可欠である。 • データ入力（収集及びインテグリティ）、データのファイリング、データ処理、ネットワーク、プロセス制御と監視、電子記録、アーカイブ、取出、印刷、アクセス、変更管理、監査証跡、自動化された GxP 関連活動に関わる決定。

は、コンピュータシステムとコンピュータ化システムの両方が、仕様定義され、設計され、実装され、バリデートされたとおりに、一貫して動作することを、高度に保証するための文書化された証拠（電子及び（又は）紙ベース）を作成済みであるか確認する。複雑な統合プロジェクトの関連するバリデーション書類は監査対応のためにわかりやすく相互リンクしておくべきである。

[25] The scope or extent of validation for each system can be detailed in individual validation plans. A hierarchy of linked validation plans may be appropriate as outlined in GAMP 4 guidance Appendix M1: 'Guideline for validation planning'.

[25] 各システムのバリデーション範囲又は程度は、個々のバリデーション計画に詳細に示すことができる。GAMP4 ガイダンス【巻末訳注 2】付録 M1「Guideline for validation planning」に概説されているように、複数のバリデーション計画を相互参照し、階層化することが適している場合もある。

[26] These examples are intended to be illustrative, not exhaustive.

[26] これらの例は、全てを網羅するものではなく、例示を意図したものである。

	• in this context, examples of GxP related activities might include: regulatory submissions, R&D, clinical trials, procurement, dispensing/weighing, manufacturing, assembly, testing, quality control, quality assurance, inventory control, storage and distribution, training, calibration, maintenance, contracts/technical agreements and associated records and reports.	• ここで、GxP 関連活動の例としては、規制上の申請、R&D、治験、調達、調剤／計量、製造、組立、テスト、品質コントロール、品質保証、在庫コントロール、保管／物流、トレーニング、キャリブレーション、保守、契約／技術上の合意、関連する記録と報告書などがある。
14.5	Historically, these systems have relied on manual systems, some electro-mechanical controls and paper based documentation. The introduction of computerised systems does not diminish the need for compliance with GxP requirements and guidelines.	従来は、このようなシステムは、手作業、電気機械的制御、紙ベースによる文書に依存していた。コンピュータ化システムを導入しても、GxP 要件／ガイドラインに適合する必要性が低くなるわけではない。
14.6	The current Good Automated Manufacturing Practice (GAMP) Supplier Guide provides essential guidance to suppliers of software to the Industry. The guide also provides a concise explanation of the interrelationship between various stages of software development and the requirements for Installation, Operational & Performance Qualification. The **GAMP Guide** identifies five different categories of software.	最新の Good Automated Manufacturing Practice (GAMP) Supplier Guide には、業界向けソフトウェアのサプライヤに対する重要なガイダンスが掲載されている。また、ソフトウェア開発の各ステージの相互関係、及び IQ／OQ／PQ の要件についても簡潔に説明している。この **GAMP ガイド**【巻末訳注 2】では、ソフトウェアのカテゴリを 5 つに分類している。

15. GAMP VALIDATION APPROACH BASED ON DIFFERENT CATEGORIES OF SOFTWARE PRODUCTS

15. ソフトウェア製品カテゴリ別の GAMP のバリデーションアプローチ

15.1	The GAMP Guide may be referred to as appropriate for detailed guidance both in the core project management section, the quality narrative and the specific appendices. The following are category summaries from GAMP 4:	GAMP ガイド【巻末訳注 2】は、必要に応じ、核となるプロジェクト管理の章、品質の説明、及び各付録を、詳細なガイダンスとして参照するとよい。以下は GAMP 4 のカテゴリをまとめたものである。

Reproduced from the GAMP 4 Guide (with permission) Appendix M4

GAMP 4 Guide【巻末訳注 2】 **付録 M4 から（許可を得て）再掲**

Table 2.1: Summary of Software Categories
表 2.1　ソフトウェアカテゴリのまとめ

Category **カテゴリ**	**Software Type** **ソフトウェアタイプ**	**Validation Approach** **バリデーションアプローチ**
1	**Operating System** **オペレーティングシステム**	Record version (including service pack). The Operating System will be challenged indirectly by the functional testing of the application. バージョン（サービスパックを含む）を記録する。オペレーティングシステムはアプリケーション機能テストの際に間接的にテストされる。
2	**Firmware** **ファームウェア**【訳注】 【訳注】2008 年に発行された GAMP 5 ではカテゴリ 2 は削除され、欠番となった。	For non-configurable firmware record version. Calibrate instruments as necessary. Verify operation against user requirements. 構成設定できないファームウェアについてバージョンを記録する。必要に応じて機器をキャリブレーションする。ユーザー要件に照らして動作を検証する。
		For configurable firmware record version and configuration. Calibrate instruments as necessary and verify operation against user requirements. 構成設定可能なファームウェアについては、バージョンと構成設定を記録する。必要に応じて機器をキャリブレーションし、動作をユーザー要件に照らして検証する。
		Manage custom (bespoke) firmware as Category 5 software. カスタムファームウェアは、カテゴリ 5 ソフトウェアとして管理する。
3	**Standard Software Packages** **標準ソフトウェアパッケージ**	Record version (and configuration of environment) and verify operation against user requirements. Consider auditing the supplier for critical and complex applications. バージョン（及び環境の構成設定）を記録し、動作をユーザー要件に照らして検証する。重要で複雑なアプリケーションはサプライヤ監査の実施を検討する。
4	**Configurable Software Packages** **構成設定可能ソフトウェアパッケージ**	Record version and configuration, and verify operation against user requirements. Normally audit the supplier for critical and complex applications. バージョンと構成設定を記録し、動作をユーザー要件に対して検証する。 一般的に、重要で複雑なアプリケーションについてサプライヤを監査する。

Category カテゴリ	**Software Type** ソフトウェアタイプ	**Validation Approach** バリデーションアプローチ
		Manage any custom (bespoke) programming as Category 5. カスタムプログラミングがあれば、それはカテゴリ 5 ソフトウェアとして管理する。
5	**Custom (Bespoke) Software** カスタムソフトウェア	Audit supplier and validate complete system. サプライヤを監査し、システム全体をバリデートする。

15.2	However, this pre-defined category approach may be difficult to apply to complex integrated computerised systems where different GAMP category 'levels' are effectively combined. Many systems span the category levels. For all critical systems a holistic risk-based approach is necessary. This should consider the risks from the entire pharmaceutical application. Quality assurance controls, qualification work and risk reduction measures can cascade from this to consider each of the elements comprising the computerised system. GAMP guidance is considered to be scaleable for large, medium and small, complex and simple systems. Where software and systems do not appear to fit readily into this category system then it is for users to apply judgement in determining particular quality measures, validation strategies and acceptance criteria. For instance, under particular circumstances the operating system configuration may contribute to the overall risk of the system and the level of validation should reflect this. *Inspectors will be interested in the company's approach to identifying GxP risks and the criteria for assessing the fitness for purpose of the system application.*	しかし、この事前に定義されたカテゴリを用いたアプローチは、様々な GAMP カテゴリ「レベル」が組み合わされた、複雑で統合されたコンピュータ化システムに適用することは困難であろう。多くのシステムは複数のカテゴリレベルにまたがっている。全ての重要なシステムには、大局的なリスクベースアプローチが必要である。このためには製薬アプリケーションを全体から見たリスクを検討する。続いて品質保証コントロール、適格性評価作業、及びリスク低減方策を実施し、コンピュータ化システムを構成する各要素について検討する。GAMP ガイド【巻末訳注 2】は、大／中／小規模、複雑／単純なシステムに対しスケーラブルであると考えられる。ソフトウェア／システムがこの分類方式にそのまま当てはまらない場合、品質方策／バリデーション戦略／受入基準を決定するのはユーザーである。例えば、状況によっては、オペレーティングシステムの構成設定が、システムの全体的なリスクに影響を与えることがあるが、バリデーションのレベルには、そのことを反映すべきである。*査察官は、会社における、GxP リスクを特定するアプローチ、及びシステムアプリケーションの利用目的への適合性をアセスメントする基準に関心を持っている。*
15.3	There are a number of additional important aspects that would be required in the documentation and records necessary to support a validation exercise. These aspects relate to on-going evaluation and system maintenance. As a result the documentation and records for validation of a computer system would also require information and records for the following aspects of system control:	バリデーション実施を裏付けるために必要な文書／記録には、数多くの重要な追加的事項が求められる。それらは、オンゴーイング評価とシステム保守に関連するものである。結果的に、コンピュータシステムのバリデーション文書／記録には、以下のシステムコントロールについての情報と記録が必要になるであろう。

	• *Evaluation records to demonstrate that the system works as described in the URS (verification stage and on-going monitoring).* • *Records of operator training (introduction and on-going training).* • *Procedure for on-going monitoring, this procedure would interlink the error report system and the deviation reports system with the change control procedure.* • *Maintenance of user manuals and SOPs for all systems.*	• *システムが URS に記載されたとおりに機能することを示す評価記録（検証ステージとオンゴーイングモニタリング）。* • *操作者トレーニングの記録（導入時トレーニングとーニング）。* • *オンゴーイングモニタリングの手順。この手順により、エラー報告システム及び逸脱報告システムを変更コントロール手順にリンクさせる。* • *全てのシステムのユーザーマニュアルと SOP の維持管理。*

16. RETROSPECTIVE VALIDATION

16. 回顧的バリデーション

16.1	Retrospective validation is not equivalent to prospective validation and is not an option for new systems. Firms will be required to justify the continued use of existing computerised systems that have been inadequately documented for validation purposes. Some of this may be based on historical evidence but much will be concerned with re-defining, documenting, re-qualifying, prospectively validating applications and introducing GxP related life-cycle controls. Reference should also be made to GAMP Forum's forthcoming guidance on 'Legacy Systems'. *Inspectors may be interested in seeing whether 'system descriptions' are available and that documented evidence exists that the system has been checked/tested against URS and other specifications. Risk and criticality analysis and assessment of supplier may also be relevant. A documented evaluation of system history i.e. error logs, changes made, evaluation of user manuals and SOPs would also be expected to provide some of the documentation relating to the 'controlled system' in place of formal validation evidence.*	回顧的バリデーションは予測的バリデーションと同等ではないため、〔回顧的バリデーションは〕新しいシステムについては選択肢にはならない。バリデーションのための文書化が不適切な既設コンピュータ化システムを継続して使用するのであれば、その正当理由を示すことを求められるであろう。過去の証拠を利用できるものもあるかもしれないが、多くはアプリケーションを再定義し、文書化し、再適格性評価し、予測的バリデートし、GxP 関連のライフサイクルコントロールを導入することになるであろう。GAMP Forum が近々発行する予定の「レガシーシステム」に関するガイダンスも参照すべきである。*査察官は、「システム記述書」が提供されるかどうか、そしてシステムが URS や他の仕様書に照らしてチェック／テストされた文書化された証拠が存在するかどうか、に関心がある。リスク／重要度の分析、及びサプライヤアセスメントも有効であろう。正式なバリデーションの証拠が無い代わりに、システムの履歴に対する文書化された評価（すなわちエラーのログ／変更記録／ユーザーマニュアルの評価／SOP）も、「コントロールされたシステム」を示す文書の一部となることが期待される。*

16.2	A significant number of legacy systems may operate satisfactorily and reliably, however, this does not preclude them from a requirement for validation. The approach to be taken is to provide data and information to support the retrospective documentation of the system to provide validation and re-qualification evidence. GxPs have required the validation of computerised systems for many years. *It should therefore be noted that a lack of prospective validation evidence for computerised systems would increasingly be seen as a serious deviation from GxPs by a number of regulatory authorities*[27]. *However retrospective validation might be justified if a non-GxP system is newly classified as a GxP system.*	かなりの数のレガシーシステムが、満足に、信頼性をもって動作しているかもしれないが、そのことをもってバリデーションをしなくてもよいということにはならない。取るべきアプローチは、回顧的にシステムを文書化することができるようなデータと情報を用意し、バリデーションと再適格性評価の証拠を示すことである。GxP は長年にわたりコンピュータ化システムバリデーションを要件としてきた。*従って、多くの規制当局が、これからますますコンピュータ化システムの予測的バリデーションの証拠の欠如を深刻な GxP 逸脱とみなすであろうことに留意すべきである*[27]。*ただし、過去に GxP システムではなかったものが、新たに GxP システムに分類し直された場合は、回顧的バリデーションが正当化されることがある。*
16.3	The principles identified above for computer systems validation should be addressed where a retrospective validation approach has been undertaken for a legacy system. For legacy systems, because of their age and unique characteristics, the system development documentation and records appropriate for validation may not be available. As a result the approach taken to establish and document system reliability and on-going assurance based on the "build-in-quality" concept for software development would, of necessity, be different to a current system.	レガシーシステムに対し回顧的バリデーションを行うのであれば、上記で明らかにしたコンピュータシステムバリデーションの原則に対応すべきである。各レガシーシステムは、それぞれ年数と特徴が異なるため、バリデーションに利用できそうなシステム開発文書／記録は入手できないかもしれない。その場合、ソフトウェア開発の「品質の作り込み」の概念に基づいた、システムの信頼性及びオンゴーイング保証を確立／文書化するアプローチは、現行システムとは異なるものとなるであろう。

[27] Compared with 10 to 20 years ago, when GxP related applications were often rudimentary and 'standalone', there are now many more integrated, 'infrastructure' computer systems to consider, especially when regulated users are striving to achieve 'so-called' paperless systems. Some specific national GxP compliance regulations, such as the US FDA's 21 CFR Part 11: 'Electronic Records and Electronic Signatures' have set specific requirements in this field. For legacy systems, firms often have to consider retrospective validation, upgrading or replacement.

[27] GxP 関連のアプリケーションのほとんどが、原始的で「スタンドアロン」であった 10～20 年前に比べて、現在は統合された、「インフラストラクチャ」コンピュータシステムがかなり多くなっている。規制対象ユーザーが「いわゆる」ペーパーレスシステムの実現を目指している場合は特にそうである。国家レベルの GxP 適合規制の中には、FDA 21 CFR Part 11: 「Electronic Records and Electronic Signatures」等のように、この分野で特定の要件を定めているものがある。会社は往々にして、レガシーシステムについて、回顧的バリデーション、アップグレード、リプレースのいずれを行うかを検討しなければならない。

16.4	Nevertheless, the validation strategy would be consistent with the principles established for classic retrospective validation where the assurances are established, based on compilation and formal review of the history of use, maintenance, error report and change control system records and risk assessment of the system and its functions. These activities should be based on documented URS's[28] . If historical data do not encompass the current range of operating parameters, or if there have been significant changes between past and current practices, then retrospective data would not of itself support validation of the current system.	とはいえ、レガシーシステムのバリデーション戦略は、従来の回顧的バリデーションのために確立された原則と一貫したものとなるであろう。その原則とは、使用、保守、エラー報告及び変更コントロールシステムの記録、並びにシステムとその機能のリスクアセスメントの履歴をまとめ、それらをレビューすることにより保証を確立できるというものである。これらの活動は文書化された URS[28] に基づくべきである。履歴データが現行の運用パラメータの範囲をカバーしていない場合、又は過去と現在の運用で大幅な変更があった場合は、回顧的データだけでは現行システムのバリデーションを裏付けることはできない。
16.5	*The validation exercise for on-going evaluation of legacy systems should entail inclusion of the systems under all the documentation, records and procedural requirements associated with a current system. For example, change control, audit trail(s), (where appropriate), data & system security, additional development or modification of software under a QMS,[29] maintenance of data integrity, system back up requirements, operator (user) training and on-going evaluation of the system operations.*	*レガシーシステムをオンゴーイング評価する際のバリデーション作業には、現行システムに関連する全ての文書／記録／手順の要件に示される仕組みを含むべきである。例えば、変更コントロール、（妥当な場合）監査証跡、データ及びシステムのセキュリティ、QMS[29] 下でのソフトウェアの追加開発／修正、データインテグリティの維持、システムのバックアップ要件、操作者（ユーザー）トレーニング、システム運用のオンゴーイング評価である。*
16.6	*Ultimately, regulated users have to be able to demonstrate:* • *Defined requirements* • *System description, or equivalent* • *Verification evidence that the system has been qualified and accepted and that GxP requirements are met*	*規制対象ユーザーは、最終的に以下を示すことができなければならない。* • *定義された要件* • *システム記述書、又は同等のもの* • *システムが適格性評価され、受け入れられ、かつ GxP 要件が満たされたという検証の証拠*
16.7	*In the absence of adequate 'retrospective qualification or validation' evidence this could be a reason to suspend, discontinue or turn-off any legacy system(s).*	*適切な「回顧的適格性評価又は回顧的バリデーション」の証拠がない場合、レガシーシステムを一時停止、運用停止又は運転停止する理由になり得る。*

[28] 'Experience reports' supported by additional testing have reportedly been used to retrospectively derive a URS.
[28] 追加テストによって裏付けられた「Experience reports」を用いて回顧的に URS を作成したことが報告されている。
[29] QMS = Quality Management System
[29] QMS＝品質管理システム

PART THREE - SYSTEM OPERATION / INSPECTION / REFERENCES
第三部 - システムの運用／査察／参考資料

17. CHANGE MANAGEMENT
17. 変更管理

17.1	It is important for proper control that a comprehensive change management system is instituted. This may take two forms in that during the Design phase it may only be necessary to keep records pertaining to the project up-to-date without formal "sign-off" approvals for all changes. However, once the project reaches a point where specifications are under development and conceptual aspects have been finalised, then a formal change control procedure should be established which will require clear, prescriptive and accurate documentation and records. It is important for the responsibilities of participants in the change control procedure to be carefully defined.	適切なコントロールを行うためには、包括的な変更管理システムを設けることが重要である。これは次の 2 つの形式を取り得る。設計フェーズでは、プロジェクトに関する記録を最新に維持するために、全ての変更について、正式な承認の「署名」なしで〔コントロールを〕行う。しかし、仕様が作成され、概念レベルが確定したら、正式な変更コントロール手順を策定し、明確で、詳細で、正確な文書／記録を求めるようにすべきである。変更コントロール手順に関わる者の責任について、注意深く定義することが重要である。
17.2	As discussed previously, it is appropriate for regulated users to have a system control document or some other record system to achieve a documented baseline record for the description of the computerised system. The system control documentation should be the definitive statement of what the system must do. The control document should also provide a record of the User Requirement Specifications. The change control procedure for the computerised system "project" should be integrated with the Master change control procedure for the regulated user organisation[30]. *The change control procedure will need to take account of the corresponding procedures and records used by suppliers, integrators and other parties contracted to support the particular system and applications.* Validated decentralised arrangements for change control may be a feature in large complex regulated user companies.	前述のように、規制対象ユーザーはシステムコントロール文書、又は何等かの記録システムを用意し、コンピュータ化システムを記述するためのベースライン記録を文書化するとよい。システムコントロール文書は、システムが何をしなければならないかを明確に宣言するものである。コントロール文書には、ユーザー要求仕様の記録も含まれる。コンピュータ化システム「プロジェクト」の変更コントロール手順は、規制対象ユーザー組織のマスター変更コントロール手順に統合すべきである[30]。*変更コントロール手順では、そのシステム／アプリケーションのサポートを契約したサプライヤやインテグレータ等の当事者が使用する変更コントロール手順／記録を考慮する必要がある。*大規模で複雑な規制対象ユーザー会社では、変更コントロールをバリデートされた分散体制で行うことが特徴かもしれない。

[30] It is important for regulated users to ensure that change control management is in place during all system life cycle phases, i.e. from design and development through operation, maintenance, modification and retirement. The arrangements should be described in the validation plans for the project. Records should be kept with the project files.
[30] 規制対象ユーザーにとって、システムの全ライフサイクルフェーズにおいて、すなわち設計、開発から運用、保守、修正、リタイアメントに至るまで、変更コントロールの管理を設けるようにすることが非常に重要である。こういった措置はプロジェクトのバリデーション計画に記述すべきである。記録はプロジェクトのファイルと一緒に保存すべきである。

17.3	Common IT infrastructure features may need to be controlled centrally by IT systems and security management. Key roles, responsibilities and procedures need to be clearly documented in relevant internal and external *Service Level Agreements, (SLAs),* or equivalent documents.	共通の IT インフラストラクチャ機能は、IT システム／セキュリティ管理組織が集中的にコントロールする必要があるかもしれない。主要な役割、責任、及び手順は、関連する社内／社外との *サービスレベル合意書 (SLA)*、又は同等の文書により明確に文書化する必要がある。

18. CHANGE CONTROL AND ERROR REPORT SYSTEM

18. 変更コントロールとエラー報告システム

18.1	The formal change control procedure should outline the necessary information and records for the following areas: • *Records of details of proposed change(s) with reasoning.* • *System status and controls impact prior to implementing change(s).* • *Review and change authorisation methods (also see 12.5).* • *Records of change reviews and sentencing (approval or rejection).* • *Method of indicating 'change' status of documentation.* • *Method(s) of assessing the full impact of change(s), including regression analysis and regression testing, as appropriate (IEEE).* • *Interface of change control procedure with configuration management system.*	正式な変更コントロール手順では、以下の領域で必要な情報／記録を概説すべきである。 • *提案された変更の詳細とその理由を示す記録。* • *変更実施前のシステムの状況とコントロール上の影響。* • *レビューと変更承認の方法（12.5 章も参照）。* • *変更のレビューと判定（承認又は却下）の記録。* • *文書が「変更」されたことを示す方法。* • *変更の影響をアセスメントする方法。必要に応じ、機能退行がないことの分析と機能退行テストを含む（IEEE）。* • *変更コントロール手順と構成管理システムとのインターフェース。*
18.2	*The procedure should accommodate any changes that may come from enhancement of the system, i.e. a change to the user requirements specifications not identified at the start of the project. Or alternatively a change may be made in response to an error, deviation or problem identified during use of the system. The procedure should define the circumstances and the documentation requirements for emergency changes ("hot-fixes"). Each error and the authorised actions taken should be fully documented. The records should be either paper based or electronically filed.*	*変更コントロール手順では、システムの機能拡張による変更（すなわちプロジェクト開始時には特定されていなかったユーザー要求仕様への変更）を取り扱うべきである。また、変更は、システム使用中に特定されたエラー／逸脱／問題に対応するために行われることもある。この手順では、緊急変更（「ホットフィクス」）を行うべき状況と文書化の要件を定義すべきである。すべての〔変更実施に伴う〕エラー及び実施した承認済アクションは完全に文書化すべきである。記録は紙ベース、又は電子的にファイルする。*

18.3	Computer systems seldom remain static in their development and use. For documentation and computer system control it should be recognised that there are several areas that would initiate change or a review for change. These are: • a deviation report; • an error report; or • a request for enhancement of the computer system; • hardware and software updates.	コンピュータシステムは、開発時も使用時も静的であり続けることはほとんどない。文書及びコンピュータシステムのコントロールを変更する、又は変更をレビューする契機はいくつかあり、それらは以下である。 • 逸脱報告 • エラー報告、又は • コンピュータシステムの機能拡張依頼 • ハードウェア／ソフトウェアの更新
18.4	The results of periodic reviews may be helpful, e.g. in indicating process drifts and the need for change. *Quality systems procedures should ensure that the changes are clearly documented and closed out after actions have been completed. The change control procedure should complement and link with the deviation and errors report system. Various GAMP 4 'Operation' appendices include guidance in these areas.*	定期レビューの結果は、例えばプロセスが安定せず、変更が必要であることを示すうえで、有用であろう。*品質システム手順により、変更を明確に文書化し、アクション終了後にクローズすることを確実にすべきである。変更コントロール手順は、それを補完し、逸脱／エラー報告システムと連携すべきである。GAMP 4【巻末訳注2】の付録「Operation」にこの領域のガイダンスが記載されている。*
18.5	*The supplier of the software should have its own change control system in place and there should be clear and agreed procedures covering the interrelationship of the suppliers and users change control system. Where changes are made then the modifications of software should be undertaken following formal QMS documentation, records and procedural requirements.*	*ソフトウェアのサプライヤは、自分たちの変更コントロールシステムを設けるべきであり、サプライヤの変更コントロールシステムとユーザーの変更コントロールシステムの相互関係をカバーする明確かつ合意された手順が必要である。変更が行われたら、正式な、QMS の文書／記録／手順の要件に従いソフトウェアの修正を実施すべきである。*
18.6	Any changes to the validated computerised system should not be undertaken without review and authorisation on behalf of all stakeholders responsible for the current user requirements. It may be appropriate for this to be undertaken by the system owner and QA representative. *Test scripts, determined by the project plan, q.v., (of defined test type and extent of tests),* should be used to verify the acceptability of the software element developed in response to a change request. *Integration testing may also be necessary before release of the new software version*[31] .	バリデートされたコンピュータ化システムの変更は、現行のユーザー要件に責任を持つ全てのステークホルダーの代表によるレビューと承認なしに実施すべきではない。これはシステムオーナー及び QA 代表が実施することが適切であろう。*（テストの種類と範囲を記載する）プロジェクト計画で定められたテストスクリプト*を用いて、変更依頼に基づき開発されたソフトウェア要素が受け入れ可能か検証すべきである。*新しいソフトウェアバージョンをリリースする前に統合テストが必要になる場合がある*[31]。

[31] It may be necessary to regard proposed changes to infrastructure as a special case and define a set of stakeholders.
[31] インフラストラクチャに対し提案された変更を特殊ケースと見なし、ステークホルダーを別に定めることが必要となる場合がある。

19. SYSTEM SECURITY, INCLUDING BACK-UP

19. バックアップを含むシステムのセキュリティ

19.1	The security of the system and security of the data is very important and the procedures and records pertaining to these aspects should be based on the IT policies of the regulated user and in conformance with the relevant regulatory requirements. The use of a computerised system does not reduce the requirements that would be expected for a manual system of data control and security. 'System owner's' responsibilities will include the management of access to their systems and for important systems the controls will be implemented through an Information Security Management System (ISMS).	システムのセキュリティとデータのセキュリティは非常に重要であり、これらに関する手順／記録は、規制対象ユーザーの IT 方針に基づくべきであり、かつ関連する規制要件にも適合すべきである。手作業のときに期待されるデータコントロールとセキュリティの要件は、コンピュータ化システムを使用したとしても軽減されるわけではない。「システムオーナー」の責任には、システムアクセス管理が含まれており、重要なシステムのコントロールは情報セキュリティ管理システム (ISMS) により実装されるであろう。
19.2	It is very important for the regulated user to maintain *the procedures and records related to the access to the system(s). There should be clearly defined responsibilities for system security management, suitable for both small and complex systems, including:* • *The implementation of the security strategy and delegation* • *The management and assignment of privileges* • *Levels of access for users* • *Levels of access for infrastructure (firewall, backup, re-booter, etc.).*	*規制対象ユーザーがシステムアクセスに関する手順／記録を維持管理することは非常に重要である。システムのセキュリティ管理について責任を明確に定義すべきである。それは小規模システムにも複雑なシステムにも利用できるようなものとし、以下を含む。* • *セキュリティ戦略の実施と権限委譲* • *特権の管理と割当* • *ユーザーのアクセスレベル* • *インフラストラクチャ（ファイアウォール、バックアップ、リブータ等）のアクセスレベル*
19.3	*The examination of the procedures and records should assure that the following basic requirements are satisfied:* • *Access rights for all operators are clearly defined and controlled, including physical and logical access.* • *Basic rules exist and are documented to ensure security related to personal passwords or pass cards and related system/data security requirements are not reduced or negated.* • *Correct authority and responsibilities are assigned to the correct organisational level.*	*手順／記録をチェックし、以下の基本要件が満たされることを保証すべきである。* • *操作者全員のアクセス権が、物理的及び論理的なアクセスを含めて明確に定義され、コントロールされている。* • *基本ルールが存在し、文書化されており、個人のパスワード又はパスカードのセキュリティ、及びシステム／データのセキュリティ要件が、緩くなっていない又は無効にされていないことを確実にする。* • *正しい権限と責任が正しい組織レベルに割り当てられている。*

	• *Procedures are in place to ensure that identification code and password issuance are periodically checked, recalled or revised.* • *Loss management procedures exist to electronically invalidate lost, stolen or potentially compromised passwords. The system should be capable of enforcing regular changes of passwords. Precise change rates to be justified within the ISMS.* • *Procedures identify prohibited passwords.* • *An audit log of breaches of password security should be kept and measures should be in place to address breaches of password security.* • *The system should enforce revoking of access after a specified number of unsuccessful logon attempts.* • *Measures are needed to ensure the validated recovery of original information and data following back up, media transfer, transcription, archiving, or system failure.* • *Attempted breaches of security safeguards should be recorded and investigated.* • *Some equipment, such as standalone computerised systems and dedicated operator equipment interfaces and instruments may lack logical (password etc.) capabilities. These should be listed, justified and subjected to other procedural controls.*	• *ID コードとパスワードの発行を定期的にチェック／無効化／改訂を確実に行うための手順が実施されている。* • *紛失されたり、盗難されたり、信頼がおけなくなったパスワードを電子的に無効にする紛失管理手順が存在する。パスワードの定期的な変更をシステムによって強制できるようにすべきである。厳密な変更頻度の妥当性は、ISMS で説明する。* • *禁止されたパスワードは、手順により特定する。* • *パスワードセキュリティ違反の監査ログは保持し、パスワードセキュリティ違反に対応する方策を設けるべきである。* • *規定回数を超えてログオンの試みに失敗した場合、システムがアクセス取消を強制すべきである。* • *バックアップ、媒体への転送、転記、アーカイブ又はシステム故障の後で、オリジナルの情報／データの（バリデートされた）リカバリを確実にするような方策が必要である。* • *セキュリティセーフガードに対する違反の試みは記録し、調査すべきである。* • *スタンドアロンのコンピュータ化システム、専用機器の操作者画面／計器には、（パスワード等の）論理機能が欠如している場合がある。これらはリスト化し、合理的な理由を示し、手順によるコントロールを行うべきである。*
19.4	It should be realised that when absolutely necessary Inspectorates of the national competent authorities may need to be able to access a firm's encrypted GxP data. In such circumstances, either keys for decryption would need to be made readily available to the Inspectors working for the competent authorities, or decryption would have to take place under the inspector's supervision.	どうしても必要となった場合、各国の査察官は、会社の暗号化された GxP データにアクセスする必要があることを了解されたい。こうした状況で、当局査察官に復号化の鍵を提供するか、又は査察官が見ている前で復号化する必要がある。

19.5	The *validated back-up procedure* including storage facilities and media should assure data integrity. The frequency of back up is dependent on the computer system functions and the risk assessment of a loss of data. In order to guarantee the availability of stored data, back-up copies should be made of such data that are required to re-construct all GxP-relevant documentation (including audit trail records).	データインテグリティは、*バリデートされたバックアップ手順*（格納施設及び媒体についての記載を含む）により保証すべきである。バックアップ頻度は、コンピュータシステム機能とデータ損失のリスクのアセスメントにより決定する。保存されたデータの可用性を保証するために、バックアップコピーは、全ての GxP 関連資料（監査証跡の記録を含む）を再構築するために必要とされるデータから構成すべきである。
19.6	There should be *written procedures for recovery of the system* following a breakdown; these procedures should include documentation and record requirements to assure retrieval and maintenance of GxP information. *The examination of the procedures and records should assure that the following basic back up and disaster recovery requirements are satisfied:* • *There should be procedures to assure routine back-up of data to a safe storage location, adequately separated from the primary storage location, and at a frequency based on an analysis of risk to GxP data.* • *The back-up procedure including storage facilities and media used should assure data integrity. There should be a log of backed up data with references to the media used for storage. Media used should be documented and justified for reliability.* • *All GxP related data, including audit trails should be backed-up.* • *Procedure for regular testing, including a test plan, for back up and disaster recovery procedures should be in place.* • *A log of back up testing including date of testing and results should be kept. A record of rectification of any errors should be kept.*	システムが故障したときに*システムをリカバリするための文書化された手順*を設けるべきである。この手順には、GxP 情報の取出と維持を保証するための文書／記録の要件を含むべきである。*手順と記録をチェックし、以下のバックアップと災害復旧の基本的な要件を満たすことを確認すべきである。* • *データを、主となるデータ格納場所から十分離れた安全な格納場所に、GxP データのリスク分析に基づく頻度で、日常的にバックアップすることを確実にする手順が設けられている必要がある。* • *格納施設と媒体を記載したバックアップ手順により、データインテグリティを保証すべきである。バックアップデータのログを残すべきであり、ログには保管に使用した媒体を明記すべきである。使用する媒体は文書化し、その信頼性について根拠を示すべきである。* • *全ての GxP 関連データ（監査証跡を含む）のバックアップをとるべきである。* • *バックアップと災害復旧手順に対する定期テストの手順（テスト計画を含む）を設けるべきである。* • *バックアップテストのログ（テスト実施日と結果を含む）を保管すべきである。エラーを訂正した記録もすべて保管すべきである。*
19.7	The *physical security* of the system should also be adequate to minimise the possibility of unauthorised access, wilful or accidental damage by personnel or loss of data.	許可のないアクセス、従業員による故意又は事故による損傷、データ損失の可能性を最小限に抑えるためには、システムの*物理的セキュリティ*も適切なものとすべきである。

20. DATA CHANGES - AUDIT TRAIL/CRITICAL DATA ENTRY

20. データ変更 - 監査証跡／重要データの入力

20.1	Where applicable, the audit trail for the data integrity may need to include functions such as authorised user, creations, links, embedded comments, deletions, modifications/corrections, authorities, privileges, time and date, inter-alia. *All linked components are to be immutably[32] linked in an IT system security controlled audit trail. All original data records and masters and any subsequent alterations, additions, deletions or modifications are to be retained accurately and comprehensively within the retrievable audit trail. The nature and context of transactions logged in the audit trail to be deducible from and in agreement with, the firm's approved Standard Operating Procedures for information security management for the particular computerised applications and user's authorities[33]. Firms will need clearly documented policies, standard operating procedures, validation reports and training records covering such system controls. Information Security Management standards such as ISO/IEC 17799:2000[34] may be of assistance with the design, implementation and control of such systems.*	データインテグリティのために取得する監査証跡が必要な場合、〔操作を行った〕許可されたユーザー、作成、リンク、埋め込みコメント、削除、修正／訂正、権限、特権、日付時刻等の機能を含む必要がある。*全てのリンクされたコンポーネントは、IT システムのセキュリティコントロール下にある監査証跡に永続的に[32] リンクされるべきである。全てのオリジナルのデータ記録／マスター、及びその後の変更、追加、削除、修正は、取出可能な監査証跡内に正確かつ包括的に保持すべきである。どのようなトランザクションを、どのような場面で監査証跡に記録するかは、コンピュータ化アプリケーションとユーザー権限に関する（承認された）情報セキュリティ管理 SOP から導き出し、それと矛盾しないようにする[33]。各社では、こういったシステムコントロールをカバーする明確に文書化された方針、SOP、バリデーション報告書、トレーニング記録が必要になるであろう。ISO/IEC 17799:2000[34] 等の情報セキュリティ管理の規格が、こうしたシステムの設計／実装／コントロールに役立つであろう。*
20.2	Where applicable, there should be *special procedures for critical data entry* requiring a second check, for example the data entry and check for a manufacturing formula or the keying in of laboratory data and results from paper	必要に応じて、ダブルチェックを要求するような*重要データの入力のための特別な手順*を用意すべきである。例えば、製造方法に関するデータの入力やチェック、又は紙の記録からのラボラトリデータや結果のタイプ入力等がある[35]。許可された 2 人目の者が、名前、ID、日時を記録し、キーボードからのデータ入力を検証してもよい。（ディスペンサーのように）データベースやインテリジェント周辺機器に接続され、データを直接収集する自

[32] Penguin English Dictionary: 'Immutable [imewtab'l] adj unchangeable; without variation - immutably adv.
[32] Penguin English Dictionary の Immutable の定義「変化がなく変わらない、不変の」
[33] The systematic contextual 'labelling' of transactions in the electronic audit trail log is recommended as it can have automated functional feedback control links with security validation features.
[33] 電子監査証跡ログには、トランザクションの体系的な、コンテキストに応じた「ラベリング」を行うことを推奨する。これは、セキュリティバリデーション機能との、自動的な機能的フィードバックコントロールリンクを持つためである。
[34] Information Technology - - "Code of practice for information security management" BSI/DISC and national standards bodies. Other guidance will be found in the guidelines supporting FDA's 21 CFR Part 11.
[34] Information Technology - - "Code of practice for information security management" BSI/DISC and national standards bodies. FDA の 21 CFR Part 11 をサポートするガイドラインにもその他のガイダンスが記載されている。

	records[35]. A second authorised person with logged name and identification, with time and date, may verify data entry via the keyboard. For other automated systems featuring direct data capture linked to other databases and intelligent peripherals then the second check may be part of validated system functionality (e.g. in a dispensary). Special access, system control features and/or special devices such as identification code bars, and the inclusion and use of an audit trail to capture the diversity of changes possibly impacting the data may facilitate this check.	動化システムでは、2 つ目のチェックはバリデートされたシステム機能の一部に組み込まれるであろう。このようなチェックを可能にするものには、ID コードバー等の特別なアクセス、システムコントロール機能及び（又は）特殊なデバイス、並びにデータに影響を及ぼし得る様々な変更を記録する監査証跡機能の導入／利用がある。
20.3	*The records pertaining to the audit trail* events should be documented, ideally as features of the operating system, database management system (DBMS), document management system (DMS) and other major applications. Time-linked audit trail records should be available, if required, in a human readable form as required by the inspector[36]. *GxP Inspectors may see evidence for different forms of audit trail depending on the regulations prevailing in the intended regulated markets for the products or data.*	*監査証跡*〔の対象となる〕イベント*に関する記録*は、理想的には、オペレーティングシステム、データベース管理システム (DBMS) 、文書管理システム (DMS) 、他の主要アプリケーションの機能として文書化すべきである。時刻に紐付けられた監査証跡記録を、必要時に、査察官の求めに応じて、人間が読むことができる形式で提供できるようにすべきである [36]。*GxP 査察官は（製品又はデータが対象となる市場の規制に応じた様々な形式の）監査証跡の証拠を見ることができる。*
20.4	It is expected that appropriate controls will exist such as the maintenance of a *register of authorised users, identification codes, scope of authorised actions,* in support of GxP electronic records and electronic signatures.	GxP 電子記録及び電子署名を利用するために、*許可されたユーザー、ID コード、許可されたアクションの範囲の台帳*の維持管理等の適切なコントロールを設けることが期待される。
20.5	There should be *records of checks* that the data/control/monitoring interface(s) between the system and equipment ensure correct input and output transmission.	システムと機器の間のデータ／コントロール／監視に関するインターフェースにおいて、正しい入力及び出力が確実に伝送されたことの*チェック記録*を残すべきである。

[35] This is an established compliance requirement in the GMP discipline.
[35] これは、GMP の規律として確立された適合要件である。
[36] It should be noted that for the USA market it may be a requirement in for audit trails to be available in electronic form, not just paper, but the implementation and enforcement of compliance with 21 CFR Part 11 is under review by FDA in 2003, (see Ref. 11).
[36] 米国市場向けの場合、監査証跡は紙だけでなく電子形式で用意することが要件のようであるが、21 CFR Part 11 への適合の実施と執行については、2003 年時点で FDA は検討中である（参考資料 11 を参照）ことに留意されたい。

21. ELECTRONIC RECORDS AND ELECTRONIC SIGNATURES

21. 電子記録と電子署名

21.1	EC Directive 91/356 sets out the legal requirements for EU GMP. The GMP obligations include a requirement to maintain a system of documentation, (Article 9)[37]. The main requirements here being that the regulated user has validated the system by proving that the system is able to store the data for the required time, that the data is made readily available in legible form and that the data is protected against loss or damage.	EC Directive 91/356 には EU GMP の法的要件が示されている。この GMP には、文書システムを維持することが義務付けられている（Article 9）[37]。この主たる要件は、規制対象ユーザーがシステムをバリデートし、要求される期間データを保管でき、データが見読性のある形式でいつでも利用可能であり、損失又は損傷からデータを保護することである。
21.2	The guidelines relating to documentation in the GMP Guide are in Chapter 4 and there is no requirement here that documents be in writing. Indeed in paragraph 4.9 the section amplifies Article 9.2 (see above). It references electronic data processing (EDP) systems and implies a number of good practice measures that should be in place to protect the data: • access by authorised personnel only • use of passwords • creation of backup copies • independent checking of critical data • safe storage of data for the required time Such systems also require evidence to demonstrate: • (fundamental) the use of validated, secure computerised systems • the systematic use of an accurate, secure, audit trail, (where appropriate)	GMP Guide の文書に関連するガイドラインは Chapter 4 に掲載されており、文書が紙でなければならないという要件はない。実際、この 4.9 項では、Article 9.2（上記を参照）を詳述している。そこでは、電子データ処理（EDP）システムについて述べられており、以下のようなデータ保護のために実施すべき数多くのグッドプラクティスの方策を示している。 • 許可された要員のみによるアクセス • パスワードの使用 • バックアップコピーの作成 • 重要なデータの独立した〔本人以外の〕チェック • 要求される期間におけるデータの安全な格納 こうしたシステムでは、以下を示す証拠も必要になる。 • （基礎的要件）バリデートされた安全なコンピュータ化システムの使用 • （適切な場合）正確、安全な監査証跡の体系的な使用

[37] The main requirements in Article 9.1 are that documents are clear, legible and up to date, that the system of documentation makes it possible to trace the history of manufacture (and testing) of each batch and that the records are retained for the required time. Article 9.2 envisages that this documentation may be electronic, photographic or in the form of another data processing system, rather than written.
[37] Article 9.1 の主な要件は、文書が明確／判読可能／最新であり、文書システムにより、各バッチの製造（及びテスト）の履歴が追跡可能であり、必要期間記録を保持するというものである。Article 9.2 は、文書が手書きというよりは、電子的、写真の利用、又は他のデータ処理形式であることを想定している。

21.3	The central consideration here as in Directive 91/356, is that *records are accurately made and protected against loss or damage or unauthorised alteration so that there is a clear and accurate audit trail throughout the manufacturing process available to the licensing authority for the appropriate time.*	Directive 91/356 にあるように、ここで主に考慮することは、*記録を正確に作成し、損失、損傷、許可のない変更から保護することであり、それにより全製造プロセスの、明確かつ正確な、監査証跡を当局に適宜提供できるようにすることである。*
21.4	The situation for an authorised wholesale distributor is similar for records covering purchases/sales invoices, (on paper or on computer, or any other form[38]). The requirements for records are clear: *"Records should be made… in such a way that all significant activities or events are traceable… and are clear and readily available".*	認可された卸売業者についても、購入／販売の納品書をカバーする記録（紙、コンピュータ上、又はその他の形式）に関する状況は同様である[38]。記録に対する要件は明確であり *「記録は全ての重要な活動又はイベントが追跡可能なように作成されるべきである……そして、明確であり、かつすぐに提供できるようにすべきである。」*
21.5	*Regulated user companies generally have a choice as to whether to use electronic records or electronic signatures instead of paper based records. When regulated users elect to use electronic records for GxP applications then it will be necessary for the companies to identify the particular regulations being applied and whether they are to be considered legally binding and equivalent to their paper-based counterparts. Regulations applicable to particular GxP disciplines may impose specific rules e.g. when electronic records and electronic signatures are used as a primary source of data, records and/or evidence.* *It is for the regulated user to explain and justify the technologies and controls in place.* *An appropriate form of Electronic signature[39] or authentication / identification[40] should be applied where*	*一般的に規制対象ユーザー会社には、紙ベースの記録の代替として電子記録／電子署名を使用する選択肢がある。規制対象ユーザーが GxP アプリケーションに電子記録を使用することを選択した場合、適用される規制を特定し、電子記録が法的拘束力のあるものと考えられるかどうか、そして紙ベースの記録と同等であるかどうか、を明らかにする必要がある。GxP 分野によっては規制が特別な規則を課している場合がある。例えば、電子記録と電子署名を、データ／記録／証拠のプライマリソースとして用いる場合である。* *使用する技術とコントロールを説明し、妥当性を示すことは規制対象ユーザーの責任である。* *以下の場合に、電子署名[39] 又は認証／識別[40] の適切な形式を適用すべきである。*

[38] The relevant EC directive being 92/25, Article 6(e), as amplified in the GDP guidelines (94/C 63/03). Article 8 of 92/25 requires that the documentation system makes it possible to trace the distribution path for every product.
[38] 関連する EC directive92/25, Article 6(e)は GDP ガイドライン (94/C 63/03) で詳述されている。EC directive 92/25 の Article 8 は、文書システムにより、全製品の流通経路の追跡を可能にすることを要求している。
[39] It has been proposed via industry comments that a signature should be unique to the owner of that signature but not necessarily unique to the system. It has also been argued that it may be desirable to issue and maintain only one signature across a multitude of systems. Regulated users may need to explain and justify such arrangements, controls and logic.
[39] 業界からのコメントで、署名はその所有者に対し固有であるべきだが、必ずしもシステムに対して固有である必要はないと提案されていた。また、複数システムに対し署名をひとつだけ発行し、維持することが望ましいという議論もあった。規制対象ユーザーは、こういった措置、コントロール、及び論旨を説明し、妥当性を示す必要がある。
[40] The regulated user is expected to justify the choice of methods to be used to ensure compliance with regulations and GxP, (see glossary 'Advanced Electronic Signature', 'Electronic Signature (3)' etc.
[40] 規制対象ユーザーは、規制及び GxP に確実に適合するために、使用する方式の選択が妥当であったことを示すことが期待される。（用語集の「高度な電子署名」、「電子署名(3)」等を参照。）

	• external access can be made to a computerised GxP system • the system electronically generates GxP regulatory records, or • key decisions and actions are able to be undertaken through an electronic interface.	• GxP コンピュータ化システムに外部からアクセス可能である。 • システムが電子的に GxP 規制対象記録を生成する、又は • 電子インターフェースを介し、主要な決定やアクションを実施できる。
21.6	Generally there is no requirement for records and documents created and maintained, as part of GxP, to be in 'writing',[41] and validated, secure electronic versions are permitted. In the absence of provisions to the contrary this will arguably extend to "electronic signatures". Certainly, **where regulated users have elected to use electronic records in place of paper-based media,** then it can be argued, (from the forgoing requirements) that for accurate, authorised, secure electronic record systems these systems would logically require *an attached immutable audit trail identifying person, time and date and linking to particular transactions. However, some systems may utilise a combination of human actions together with other automated functions and a variety of media for GxP data processing, records and information. Such systems may be described as 'hybrid' and in such cases documented procedural controls with recorded links, by reference and signatures may have to be used to complete the audit trail across, for example, a mixture of paper based records*[42] *and electronic files.*	一般的には GxP のために作成され、維持される記録／文書が、「手書き」[41] でなければならないという要件はなく、バリデートされた、安全な電子バージョンは認められる。このことは、違反とする条項もないことから、おそらく「電子署名」にも当てはまるといえるであろう。**規制対象ユーザーが紙ベースの媒体の代わりに電子記録の使用を選択した場合、**正確な、許可された、安全な電子記録システムには、論理的な帰結として、システムに*付属する、永続的な（操作者と、日付と時刻を特定し、特定のトランザクションに紐づけられる）監査証跡*が必要であると（前述の要件から）いえる。*しかし、システムによっては、GxP データの処理／記録／情報のために、人によるアクションを、自動化機能や各種媒体と組み合わせて使用するものもある。こうしたシステムは「ハイブリッド」と呼ばれる。このような場合には、例えば紙ベースの記録*[42] *と電子ファイルが入り混じる状況で、全体を通した監査証跡を完成させるため、参照と署名により紐づけを記録するような、文書化された手順的コントロールを使用しなければならないであろう。*
21.7	Whilst EC Directive 2001/83[43] requires a Qualified Person to "certify" in a 'register' that batches for release meet the required condition we are not aware of any provisions that would restrict this activity to paper based media and a handwritten certifying signature. Validated and secure electronic data processing systems may therefore be used in this context.	EC Directive 2001/83[43] はバッチがリリースの必要条件を満たしていることを、Qualified Person が「記録簿」において「保証」することを要求しているが、この活動を紙ベースの媒体、及び保証するための手書き署名に限定する条項は見当たらない。従ってこのような状況では、バリデートされた、安全な電子データ処理システムを使用してもよい。

[41] In this context 'writing' meaning 'written by hand and/or signed by hand' on paper media.
[41] ここで、「writing」は紙媒体に「手書きされた、及び（又は）手書き署名された」の意味である。
[42] Including printouts from computerised systems.
[42] コンピュータ化システムによる印字を含む。
[43] Superseding 75/319 Article 22 following codification.
[43] 成文化後、75/319 Article 22 にとって代わる。

21.8	*The key aspects of infrastructure, system and specific application to be controlled and managed are:* • *the authorised user log-on for a specific application* • *a unique combination of user ID and password called for by the computerised system and linked to the user's authorised account for the use of a specific application* • *permitted task functionality for that user* • *the system to have defined time zone(s) and date standard referencing with relative transaction linking, (complex systems may span several time zones)* • *the audit trail*[44] • *other physical and logical system information security infrastructure control features.*	*コントロール／管理されるインフラストラクチャ／システム／アプリケーションの主要な側面を以下に示す。* • *許可されたユーザーがアプリケーションにログオンする。* • *ユーザーID とパスワードのユニークな組み合わせがコンピュータ化システムにより要求され、それが（アプリケーションの使用を許可された）ユーザーアカウントにリンクされている。* • *当該ユーザーに許可されたタスク機能。* • *システムに定義されたタイムゾーンと日付の基準を持たせ、相対的なトランザクションの関連付けに参照する。（複雑なシステムでは複数のタイムゾーンにまたがることがある。）* • *監査証跡*[44] • *他の物理的及び論理的なシステム情報セキュリティのインフラストラクチャコントロール機能。*
21.9	Issues to consider when assessing GxP compliance in the use of electronic signatures include that: • *Documentary evidence of compliance exists* for all aspects of infrastructure, system and specific application.	以下は電子署名を使用する際に GxP 適合性をアセスメントする際に検討すべき課題である。 • *インフラストラクチャ／システム／アプリケーションの全ての側面について適合を示す証拠書類が存在するか。*

[44] See previous Section ('20.1').
[44] 前の章 (「20.1 章」)を参照。

	• *Where risk assessment concludes that the use of a digital signature may be necessary (e.g. Certification to a third party or in GCP field data collection and transmission) that adequate security measures exist to protect the key to a digital signature.* The level of security that is appropriate depends on the sensitivity of the transaction and the possible impact of the unauthorised use of the key. Public Key Infrastructure (PKI) may be appropriate where risk assessment indicates that a high level of security is required.	• *リスクアセスメントにより、(例えば第三者、又はGCPのフィールドデータの収集と伝送に対する保証のために）デジタル署名の使用が必要であると結論付けられた場合、デジタル署名の鍵を保護する適切なセキュリティ方策が設けられているか。*必要なセキュリティレベルは、トランザクションの重要性及び許可なく鍵を使用することによりもたらされる影響によって決まる。リスクアセスメントの結果、高度なセキュリティが必要であることが示された場合、公開鍵認証基盤（PKI）〔の利用〕が適切であろう。
	• *A register of entities* that are authorised is being maintained.	• 許可された*署名者の登録簿*が維持されているか。
	• There are *procedures* that ensure that entities authorised to use electronic signatures are aware of their responsibilities for actions initiated under their electronic signatures.	• 電子署名を使用する許可を与えられた者に対して、自らの電子署名のもと開始したアクションに対する責任を確実に認識させるような*手順*が設けられているか。
	• Personnel administering the systems have *appropriate security clearances, training, skills and knowledge.*	• システムを管理する要員が、*適切なセキュリティクリアランス、トレーニング実績、スキル、知識*を有しているか。
	• *Procedures* are in place to record the printed name, or 'identity', of the signer, the date and time when the signature was executed and the meaning associated with the signature.	• 署名者の活字体名又は「ID」、署名がなされた日付と時刻、及び署名の意味を記録する*手順*が設けられているか。
	• *Procedures* exist to try to detect the unauthorised use of an electronic signature or compromised ID password combinations.	• 認可されていない電子署名の使用、又は危殆化したID／パスワードの組み合わせの利用を検出するための*手順*が設けられているか。
21.10	*Issues to consider where electronic records are used to retain GxP data:*	*以下はGxPデータを保持する目的で電子記録を使用する際に検討すべき課題である。*
	• *Documentary evidence of compliance exists*	• *適合を示す証拠書類が存在するか。*
	• *Archiving procedures* are provided and records of use exist	• *アーカイブ手順*が設けられ、使用した記録が存在しているか。
	• *Procedures exist* to ensure accuracy, reliability and consistency in accordance with the validation exercise reported for the electronic record system	• 電子記録システムのバリデーションにより、正確性／信頼性／一貫性を確実にし、報告する*手順が設けられているか。*

	• *System controls and detection measures (supported by procedures) exist* to enable the identification, quarantining and reporting of invalid or altered records • *Procedures exist* to enable the retrieval of records throughout the retention period • *The ability exists* to generate accurate and complete copies of records in both human readable and electronic form • Access to records is limited to authorised individuals • *Secure, computer-generated, time-stamped audit trails to independently record GxP related actions following access to the system are used*[45].	• 無効な記録、又は変更された記録を、識別／隔離／報告するための*システムコントロールと検出の方策（手順書により裏付けられる）が存在するか。* • 保存期間中の記録の取出を可能にする*手順が設けられているか。* • 正確で完全な記録のコピーを、人間が読むことができる形式と電子形式の両方で、*生成することができるか。* • 記録へのアクセスが、許可された個人に制限されているか。 • *システムへのアクセス時に、GxP 関連のアクションを（操作とは）独立させて記録する、コンピュータにより生成される、安全なタイムスタンプ付の監査証跡を用いているか*[45]*。*
21.11	*Procedures exist* to ensure that change-control and revision (additions, modifications, deletions) transactions are documented in the audit trail.	変更コントロールと改訂（追加／修正／削除）のトランザクションを監査証跡に確実に記録する*手順が設けられている。*
21.12	*Issues to consider when the GxP system has a provision for external access*[46]*:* • The system has a method of ensuring that external access and inputs come o*nly from authorised clients and that they come in the correct format,* for example as encrypted, digitally signed mail or data packets. *A mechanism must exist to quarantine external inputs where security conditions are not met.* The information security management arrangements need to cover the quarantine, notification and the final sentencing of such inputs.	*以下は GxP システムが外部アクセスを提供する場合に検討すべき課題である*[46]*。* • 外部からのアクセスや入力が、*許可されたクライアントからのみ行われ、正しいフォーマット*（例えば暗号化され、デジタル署名されたメール又はデータパケット）であることを確実にするような方策がシステムに備わっているか。*セキュリティ条件が満たされない場合に外部からのインプットを隔離するメカニズムを設けなければならない。*情報セキュリティ管理体制で、こうしたインプットの隔離／通知／最終決定をカバーする必要がある。

[45] A database management system (DBMS) will have this included as an optional feature, but for other systems it may be necessary to ensure that it is an added function. Regulated users will then need to ensure that it is left 'switched' on.
[45] データベース管理システム (DBMS) には、オプション機能としてこの機能が装備されているかもしれないが、他のシステムではそういった機能が追加されていることを確実にする必要があるかもしれない。規制対象ユーザーはその機能が「スイッチオン」されていることを確実にする必要がある。
[46] Sometimes referred to as 'open' systems
[46]「オープン」システムと呼ばれることがある。

	• Mechanisms are in place to ensure that all external access can be tracked. *Each element of the processing stage should incorporate logging and monitoring facilities.* ***However, inspectors may expect to see less onerous tracking for 'read only' access to a suitably secure and protected system.*** • *The capacity should exist to keep copies of data and to re-send them from one stage to another if they get "lost" or corrupted at a later stage of processing.*	• 全ての外部アクセスを確実に追跡できるようにするメカニズムがあるか。*処理ステージの各部分には、ロギングと監視の機能を組み込む。****しかし、十分に安全で保護されたシステムへの「読み取り専用」アクセスであれば、査察官は、より負担の少ない追跡方法を期待するかもしれない。*** • *データのコピーを保持し、後処理のステージでデータが「紛失」したり壊れたりした場合に、そのデータのコピーを再送できるようになっているか。*
21.13	*Additional security arrangements and controls will be needed for GxP computerised systems which electronically generate regulatory records, allow external access, or enable key decisions and actions to be undertaken through electronic interfaces.* These requirements are being determined largely by international initiatives to establish electronic commerce[47]. However, where firms are interfacing such open system (external access) functionality, in whole or in part, with their GxP systems, then *the security, control and validation information will need to be documented and available to GxP inspectors.*	*規制対象の記録を電子的に生成する、外部アクセスを認めている、又は画面から主要な決定やアクションを実施することができる GxP コンピュータ化システムには追加のセキュリティ措置／コントロールが必要になる。*このような要件は、主に電子商取引[47]を確立する国際的イニシアチブによって決められている。しかし、こうしたオープンシステム（外部アクセス）機能の全体又は一部を GxP システムと接続している場合は、*セキュリティ、コントロール、及びバリデーション情報を文書化し、GxP 査察官に提供できるようにする必要がある。*

[47] Including 21 CFR Part 11. Title 21 Code of Federal Regulations Part 11 (21 CFR Part 11), which was issued by the US FDA in 1997 and provides criteria under which that agency considers electronic records and electronic signatures to be equivalent to paper records and hand-written signatures. In Europe EC Directive 1999/93/EC (December 1999) on a community framework for electronic signatures and EC Directive 2000/31/EC (May 2000) on electronic commerce in the internal market are important. These directives were implemented during 2001. It is not the purpose of GxP guides to reproduce such business and commerce requirements.

[47] 21 CFR Part 11 を含む。これは、FDA が 1997 年に発行したもので電子記録／電子署名が紙の記録／手書き署名と同等であると FDA がみなす基準を示すものである。欧州では、電子署名についての欧州地域の枠組みに関する指令 EC Directive 1999/93/EC (1999 年 12 月)、欧州市場内の電子商取引に関する指令 EC Directive 2000/31/EC (2000 年 5 月) が重要である。これらの指令は 2001 年に実施された。GxP ガイドでこうしたビジネス、商取引上の要件を繰り返すつもりはない。

22. PERSONNEL

22. 要員

	Note: 22.1 to 22.7 is based largely on the APV Guideline[48] , q.v., with judicious editing where necessary to fit the context of this document.	注意：22.1 章 から 22.7 章までは主に APV Guideline[48] に基づいたものであり、必要に応じ本書の文脈に合うように慎重な判断のうえ編集している。
22.1	There should be *sufficient, qualified staff with the relevant experience* to carry out tasks for which the regulated user is responsible in connection with the planning, introduction, application (operation), application consultancy on, and regular monitoring of, computerised systems.	規制対象ユーザーが責任を有する、コンピュータ化システムの計画、導入、適用（運用）、アプリケーションのコンサルティング、定期的な監視に係るタスクを遂行するために、*十分な人数の、適切な経験を持つ、適格なスタッフ*を揃えるべきである。
22.2	Ideally staff qualifications should be assessed on the basis of professional training, education and experience in handling and developing computerised systems. The field of work in which the staff will be operating should determine qualification requirements. *Staff should only be deployed in areas suited to their skills and training.*	理想的には、コンピュータ化システムを取り扱い、開発するうえでの専門的なトレーニング／教育／経験に基づいてスタッフの適格性を評価すべきである。スタッフが従事する作業の分野によって適格性の要件を決めるべきである。*スタッフは、そのスキルとトレーニングに見合った領域に限って配置すべきである。*
22.3	The individual *areas of responsibility should be laid down in writing* and be clearly understandable to every member of staff. The fact that computerised systems may take over decision-making functions does not affect the legally prescribed responsibilities of the persons in key positions.	*個々の責任領域は書面で規定し*、各スタッフが明確に理解できるようにすべきである。コンピュータ化システムが〔人の代わりに〕意思決定するとしても、主要な立場にいる者が負う法的に定められた責任に変わりはない。
22.4	Prior to converting a process from manual to automated control (or the introduction of a new automated operation) it is important that project staff consider any quality assurance and safety issues as part of an *impact assessment of risks*. Risk reduction measures may need to be incorporated into the systems design and operation[49]. (Additional risks to the quality of GxP related products/materials should not be introduced as a result of reducing the manual involvement in the process).	手動コントロールから自動コントロール（又は新しい自動化運転の導入）にプロセスを転換する前に、*リスクの影響度アセスメント*の一環として、プロジェクトスタッフが、品質保証と安全性の課題を検討しておくことが重要である。システムの設計や運用にリスク低減策を組み込む必要があるかもしれない[49]。（プロセスにおける手作業を減らした結果、GxP 関連の製品／原材料の品質に新たなリスクが生じないようにすべきである。）

[48] Section 22.4 has been substantially re-worded compared with the original (English language version) APV guidance, for clarity.
[48] 22.4 章はオリジナル（英語版）の APV guidance に比べて、明確化を図るために表現をかなり変更している。
[49] "Account should be taken of the risk of certain aspects of the previous procedures such as quality or safety being lost as a result of reduced operator involvement following the introduction of a computerised system."(to quote the APV document)
[49]「コンピュータ化システムの導入後にオペレータの関与が減ることにより、品質又は安全性等、過去の手順でできていたことが失われるリスクを考慮すべきである。」（APV 文書の引用）

22.5	The regulated user is responsible for ensuring all staff who have to perform tasks in connection with computerised systems are given the *requisite training* and *relevant guidelines* on computerised systems. That should also apply to system developers, maintenance and repair staff and staff whose work could affect the documented operability of the systems.	規制対象ユーザーは、コンピュータ化システムに関わるタスクを遂行するスタッフ全員に、コンピュータ化システムに関する*必要なトレーニングと関連するガイドライン*を確実に提供する責任がある。これは、システム開発者、保守、及び修理のスタッフ、並びに文書化されたシステムの操作性に影響を与えるような作業に関わるスタッフにも適用される。
22.6	Apart from a basic training in computerised systems, newly recruited staff should also be trained in the tasks assigned to them personally. Furthermore, ongoing/awareness training should also be undertaken according to *standard training programs* and the effectiveness of the training assessed periodically following implementation, (through testing).	新規採用スタッフには、コンピュータ化システムの基礎トレーニングとは別に、個人的に割り当てられたタスクについてもトレーニングすべきである。さらに、*標準トレーニングプログラム*に従いオンゴーイング／意識向上トレーニングを実施し、導入後に定期的に（テストを通して）トレーニングの有効性をアセスメントすべきである。
22.7	In connection with training, the GxP and life-cycle concept and all measures to improve understanding and application of the concept should be explained. Training **measures and qualifications** should be documented and stored as part of the life cycle documentation. (Training records may be stored in accordance with regulated user procedures)	トレーニングに関連して、GxP とライフサイクルの概念、及びその概念の理解と応用を改善するためのあらゆる方策を説明すべきである。トレーニングの**方法と適格性**は、ライフサイクル文書の一環として文書化し、保存すべきである（トレーニング記録は規制対象ユーザーの手順に従い保存してもよい）。

23. INSPECTION CONSIDERATIONS

23. 査察についての検討事項

23.1	The attention paid by inspectors to the assessment of the GxP implications of computerised systems on a site (and between sites), will be determined to some extent by the overall *site history* and *risk assessment* carried out by the inspector in preparing for the inspection. Information computer technology management arrangements for the procurement and validation of software and systems may be centralised at the regulated user's headquarter site rather than at the site of inspection. In such circumstances the controls, SOPs and records in place to ensure GxP compliance at inspection sites will need to be made available on site. In some circumstances it may also be necessary to consider an inspection at the HQ site.	査察官が、サイトにある（及びサイトにまたがる）コンピュータ化システムの GxP 部分のアセスメントにどの程度の関心を払うかは、全体的な*サイトの変遷*と査察準備として実施する*リスクアセスメント*によってある程度決まってくる。ソフトウェアやシステムの調達やバリデーションについての情報コンピュータ技術管理体制が、査察対象サイトではなく、本社で集約されている場合がある。こうした状況では、GxP 適合を確実にするためのコントロール内容、SOP、及び記録を、査察対象サイトで閲覧できるようにしておく必要がある。場合によっては、本社で査察することを検討する必要があるかもしれない。

23.2	Clearly where a site has a lot of automation and integrated computerised systems - and manufactures a range of sterile products - (for example), then the **potential** risks from a GxP failure, (whether computer related or otherwise) for the patient are high. However, where such automated systems are well designed, implemented, managed and controlled, then potential risks to product quality (and to patients) may be considerably reduced, compared with labour intensive operations, as the latter carry inherent risks from human variability and errors. Inspectors have to come to a judgement on this by *studying the firm's evidence not just in relation to the technology aspects (through the application of GAMP etc.) but also the GxP risks identified (through PQ[50] reports and such-like).*	サイトに自動化システムや統合されたコンピュータ化システムが多数存在し、例えば様々な滅菌製品を製造している場合、明らかに GxP 逸脱（コンピュータ関連又はそれ以外の逸脱）が患者に及ぼし得る**潜在的**リスクは高い。しかし、こうした自動化システムが適切に設計／実装／管理／コントロールされていれば、製品の品質（及び患者）に及ぼし得るリスクは、労働集約型の運用に比べて相当軽減されている可能性がある。これは労働集約型の運用ではバラツキや誤りという人に特有なリスクがあるためである。査察官は*会社からの証拠を、（GAMP 等を適用した）技術的側面だけではなく、（PQ 報告書等[50]から）特定された GxP リスクの観点からも検討*して、この判断を下さなければならない。
23.3	Humans design, build, test, implement **and change** these complex systems and there is opportunity for critical error with automated systems at any stage in the life-cycle unless properly managed. The GAMP Guide provides relevant guidance on these aspects.	このような複雑なシステムを人間が設計／構築／テスト／実装／**変更**する場合、適切に管理しない限り、ライフサイクルのあらゆるステージで自動化システムに重大なエラーが発生する可能性がある。こうした側面について GAMP ガイド【巻末訳注 2】は有効なガイダンスを提供している。
23.4	It is not intended that this guidance should be used as a 'blunt instrument' for all on-site inspections but inspectors should use it selectively to build up a clear picture of a company's scale and complexity of on-site computerization (or automation) and investigate selectively the critical systems and risks. As stated in '2.7' of this PIC/S guidance, inspectors may wish to consider evidence for compliance with GxP as indicated by italicised text throughout the document. Table 1 (page 34) immediately following this section provides a suggested checklist for information to be considered prior to inspection[51].	本ガイダンスを全てのオンサイト査察に「鈍器」のように使用することは意図していない。査察官は、むしろ本ガイダンスを選択的に用いて、各社のサイトにおけるコンピュータ化（又は自動化）の規模と複雑さについて十分に把握し、重要なシステムとそのリスクについて選択的に調査すべきである。本ガイダンスの「2.7 章」で述べたように、査察官は、本ガイダンス中に斜体字で表記されている GxP 適合の証拠を検討するとよいであろう。本章のすぐ後にある表 1 は、査察前に検討したほうがよい情報のチェックリストになっている[51]。
23.5	Where little is known about computerization on a site, then it may be necessary to use a *pre-inspection questionnaire* to amplify the Site Master File details.	サイトのコンピュータ化の状況についての情報がほとんど無いときは、サイトマスターファイルを補足するために *pre-inspection questionnaire* を用いるとよい。

[50] PQ = Performance Qualification
[50] PQ＝性能適格性評価
[51] An electronic keyword search of GxP documents will reveal specific compliance requirements to assist in preparing for particular topic inspections. Keywords such as:… 【訳注】
【訳注】脚注が長いため、本書末尾に移しました。

23.6	Inspectors should *select the GxP critical computerised systems* from the information provided and consider firstly the *validation evidence* for the selected system(s) and then *the routine operational controls* for maintaining a valid system that is accurate and reliable. Inspectors may find that different departments in pharmaceutical companies will have responsibility for GxP aspects of commercial, or business (IT systems) and lower level process control systems. *Look for evidence of inconsistency, or muddled standards.*	査察官は、提供された情報をもとに*重要な GxP コンピュータ化システムを選定*し、先ずはそのシステムについての*バリデーションの証拠*、次に（正確で信頼できる、有効なシステム維持するための）*日常的な運用コントロール*を調べるべきである。製薬会社において、商業／ビジネス（の IT システム）の GxP 関連部分や低レベルのプロセスコントロールシステムについて異なる部署が責任を持っていることもある。このようなときは、*一貫性が無い、又は基準の適用が混乱している、といった証拠を探す。*
23.7	GxP critical computerised systems are those that can affect product quality and patient safety, either directly (e.g. control systems) or the integrity of product related information (e.g. data/information systems relating to coding, randomisation, distribution, product recalls, clinical measures, patient records, donation sources, laboratory data, etc.). This is not intended as an exhaustive list.	GxP 上重要なコンピュータ化システムとは、製品の品質及び患者の安全に直接的な影響を及ぼすシステム（例：制御システム）、又は製品に関連した情報（例：コーディング／無作為化／物流／製品回収／臨床測定／患者記録／臓器提供者／ラボラトリデータ等に関連するデータ／情報システム）のインテグリティに影響を及ぼし得るものである。なお、ここで挙げた例は全てを網羅したものではない。
23.8	*It is essential that firms have a computerised systems validation policy together with linked SOPs and plans, including a listing, or inventory, of all their computerised systems - classified as to their use, criticality and validation status.* For long standing systems, validation may have been carried out retrospectively and for systems purchased or implemented in the last few years, the validation should have been carried out (and recorded) prospectively. Firms should have plans to complete any outstanding retrospective validation of GxP related computer systems within a reasonable time period depending on the risks and complexity of the systems. The continued use of critical systems that are unsupportable by suppliers and cannot be validated must be justified by regulated users, supported by alternative fail-safe arrangements and considered for urgent phased replacement.	*各社は、コンピュータ化システムバリデーション方針と併せて、関連する SOP 及び計画（全てのコンピュータ化システムを、利用目的、重要度、バリデーション状態で分類したリスト又は台帳を含む）を用意することが必須である。*昔からあるシステムは回顧的にバリデーションされているであろうし、過去数年の間に購入又は導入されたシステムは、バリデーションが同時進行的に実施され（記録され）ているはずである。GxP 関連のコンピュータシステムのバリデーションが未実施であれば、システムのリスクと複雑さに応じて、妥当な期間内に回顧的バリデーションを完了させる計画を持っていて然るべきである。サプライヤによるサポートを受けられずバリデートできていない重要なシステムを継続使用する場合は、規制対象ユーザーはそのことの妥当性を説明できるようにしておくとともに、代替のフェイルセーフ措置を用意し、また直ちに段階的なリプレースを検討しなければならない。

23.9	The firm's validation approach should follow a life-cycle methodology, with management controls and documentation as outlined in this guidance, which contains consensus best practice guidelines.	各社のバリデーションアプローチは、本ガイダンス（ここにはコンセンサスの得られたベストプラクティスガイドラインが含まれている）で概説した管理コントロールと文書を備えたライフサイクル手法に従うべきである。
23.10	Inspectors should review the firm's *Validation Summary Report*[52], (VSR) for the selected system and refer as necessary to the *System Acceptance Test Specification* and lower level documents. They should *look for evidence that the qualification testing has been linked with the relevant specification's acceptance criteria, viz:* • PQ versus URS • OQ versus FS[53] • IQ versus DS or DR[54] • Supplier audit reports • Validation and *quality plans. e.g. Validation Master Plan, (VMP) or Policy. (*For big projects there should be a project quality plan and a QMS for the documentation. For smaller projects established SOPs may suffice)	査察官は、選択したシステムについてバリデーションサマリー報告書（VSR）[52]をレビューし、必要に応じて*システム受入テスト仕様書*及び下位レベルの文書を参照すべきである。査察官は*適格性評価テストが関連する仕様の受入基準とリンクされている証拠を探すべきである。すなわち：* • PQ と URS • OQ と FS[53] • IQ と DS 又は DR[54] • サプライヤ監査報告書 • バリデーション計画と*品質計画（例：バリデーションマスター計画書（VMP）又は方針） （*大規模プロジェクトでは、文書化のために、プロジェクト品質計画や QMS を設けておくべきである。小規模なプロジェクトでは、確立された SOP で十分であろう。）
23.11	*Inspectors should look for the traceability of actions, tests and the resolution of errors and deviations in selected documents. If the firm has **not** got proper change and version controls over its system life-cycle and validation documents, then the validation status is suspect.*	*査察官は、選んだ文書において、関連するアクション、テスト、エラー／逸脱の処置についてトレーサビリティを探すべきである。会社がシステムのライフサイクル文書とバリデーション文書について適切な変更コントロールとバージョンコントロールを行って**いなければ**、そのバリデーション状態は疑わしい。*

[52] VSR=A best practice high level report, summarising the validation exercise, results and conclusions, linking via cross referencing to lower level project records, detailed reports and protocols. This is useful for briefing both senior managers, in regulated user organisations and for reference by auditors/ inspectors.
[52] VSR＝高レベルのベストプラクティスの報告書で、バリデーションの実施内容／実施結果／結論を要約し、下位レベルのプロジェクト記録、詳細報告書、及び実施計画を相互参照することで関連付ける。これは、規制対象ユーザー組織の上級管理者の状況説明用、及び監査者／査察官の参照用として、双方に有用である。
[53] OQ = Operational Qualification; FS = Functional Specification
[53] OQ＝運転時適格性評価、FS＝機能仕様書
[54] IQ = Installation Qualification; DS= Design Specification; DR = Design Review
[54] IQ＝据付時適格性評価、DS＝設計仕様書、DR=デザインレビュー

23.12	*Inspectors should consider all parts of PIC/S GMP Annex 11 for relevance to* particular ***validation projects*** and in particular, the 'Principle' and items 1, 2, 3, 4, 5 and 7.	*査察官は、**バリデーションプロジェクト**に関して PIC/S GMP Annex 11 の全ての部分、特に「原則」と第 1 項、第 2 項、第 3 項、第 4 項、第 5 項及び第 7 項【巻末訳注 1】を考慮すべきである。*
23.13	***The lack of a written detailed description of each system, (kept up-to-date with controls over changes), its functions, security and interactions (A11.4); a lack of evidence for the quality assurance of the software development process (A11.5), coupled with a lack of adequate validation evidence to support the use of GMP related automated systems may very well be either a critical or a major deficiency. The ranking will depend on the inspector's risk assessment judgement for particular cases. (NB. Since 1983, the GMPs have called for validated electronic data-processing systems and since 1992 for the validation of all GMP related computer systems).***	***(変更がコントロールされ最新状態に保たれた) 各システムの詳細な説明、その機能、セキュリティ、及びやり取りを記述した文書が無い (A11.4)、ソフトウェア開発プロセスの品質保証の証拠が無い (A11.5) といった状況で、さらに GMP 関連の自動化システムの使用を裏付ける適切なバリデーションの証拠が無いとなると、Critical 又は Major な欠陥となり得る。〔指摘の〕ランクは各事例に対する査察官のリスクアセスメントの判断によって決まる。(注意 : 1983 年以降、GMP はバリデートされた電子データ処理システムを要求しており、1992 年以降、全ての GMP 関連のコンピュータシステムのバリデーションを要求している)。***
23.14	*If satisfied with the validation evidence, inspectors should then study the system when it is being used and calling for printouts of reports from the system and archives as relevant. All points in Annex 11 (6, 8-19) may be relevant to this part of the assessment. Look for correlation with validation work, evidence of change control, configuration management, accuracy and reliability. Security, access controls and data integrity will be relevant to many of the systems particularly EDP (i.e.: **E**lectronic **D**ata **P**rocessing) systems.*	*バリデーションの証拠が満足できるものであれば、次にシステムの使用状況を調べ、システム及び (該当する場合は) アーカイブされた帳票の印刷を求める。Annex 11 (第 6 項、第 8-19 項)【巻末訳注 1】の全てのポイントがこの部分に関連する。バリデーション作業、変更コントロールの証拠、構成管理、正確性及び信頼性の相互関連を調べること。セキュリティ／アクセスコントロール／データインテグリティ〔を調べること〕は、多くのシステム、特に EDP (電子データ処理) システムにとって有効であろう。*
23.15	*Consider also PIC/S GMP 4.9 and EC Directive 91/356/EEC Article 9(2) for EDP systems.* Guidance on the common industry interpretation of Annex 11 is given in the GAMP Guide, from the German APV.	*EDP システムについては PIC/S GMP 4.9 及び EC Directive 91/356/EEC Article 9(2) も考慮する。*Annex 11【巻末訳注 1】の業界の一般的な解釈は、German APV による GAMP ガイド【巻末訳注 2】に掲載されている。
23.16	***Deficiency ratings applied by Inspectors will be based on the relative risk of the application and their judgement of risk criticality.***	***査察官は、アプリケーションの相対的リスク及びリスクの重要度についての判断に基づいて欠陥の程度を判定する。***

24. CHECKLISTS AND AIDE MEMOIRES
24. チェックリストと覚書

Table 1
表 1

	Table 13.5 in the publication 'Good Computer Validation Practices', (Suggested Further Reading Ref.1), provided a summary of typical information to be made available to an inspector as part of preparation work. As it is still largely relevant, it is reproduced in updated form below, with the author's permission, for information:	表 13.5 は「Good Computer Validation Practices」（推奨参考資料 Ref.1）に掲載されているものであり、査察官が準備作業で入手する代表的な情報をまとめたものである。現在でもほぼ有効であるため、参考として作成者の許可を得て下記の新たな書式で再掲した。

	INSPECTORS - PREPARING FOR AN INSPECTION	**査察官―査察準備のために**
1.	Details of the organisation and management of IT/Computer Services and Project Engineering on Site.	サイトにおける IT／コンピュータサービス、及びプロジェクトエンジニアリングの組織と管理の詳細。
2.	The regulated user's policies on procurement of hardware, software and systems for use in GxP areas.	GxP 分野で使用するハードウェア、ソフトウェア、及びシステムの調達についての規制対象ユーザーの方針。
3.	The regulated user's policy on the validation of GxP computerised systems	GxP コンピュータ化システムのバリデーションについての規制対象ユーザーの方針。
4.	A list of IT/Computer Services Standards and SOPs.	IT／コンピュータサービスの基準／SOP のリスト。
5.	The project management standards and procedures that have been applied to the development of the various applications.	様々なアプリケーションの開発に適用されてきたプロジェクト管理の基準と手順。
6.	Identify work contracted out routinely for systems support and maintenance.	システムのサポートと保守のために日常的に外注している作業の特定。
7.	A list, or inventory, of all Computerised Systems on site by name and application for business, management, information and automation levels. The list should also indicate validation status and risk ranking. (Include basic schematics of installed hardware and networks).	サイトにある全てのコンピュータ化システムを名称、適用業務、管理、情報、自動化レベルについて分類したリスト又は台帳。このリストには、バリデーション状態とリスクのランクも示されるべきである。（据付けたハードウェア及びネットワークの基本的な図を含む。）
8.	Identify and list those systems, sub-systems, modules and/or programs that are relevant to GxP and product quality. Cross-refer to the lists provided for '6' above.	GxP 及び製品品質に関連するシステム、サブシステム、モジュール及び（又は）プログラムの特定とリスト化。上記「第 6 項」のリストと突き合わせる。
9.	For the GxP significant elements and systems identified in '7' please provide additional information as below:	上記「第 7 項」で特定した GxP 上重要な要素及びシステムについて、以下の追加情報を入手する。

	INSPECTORS - PREPARING FOR AN INSPECTION	査察官―査察準備のために
10.	Details of disaster-recovery, back up, change-controls, information security, and configuration management.	災害復旧、バックアップ、変更コントロール、情報セキュリティ、構成管理の詳細。
11.	A summary of documentation that generally exists to provide up-to-date descriptions of the systems and to show physical arrangements, data flows, interactions with other systems and life cycle and validation records. The summary should indicate whether all of these systems have been fully documented and validated and confirm the existence of controlled system description documents as required by EU GMP A11 (4).	通常はシステムの最新の記述を説明するサマリが存在し、物理的配置、データフロー、他のシステムとのやり取り、ライフサイクルの記録、及びバリデーションの記録を示す。このサマリは、これらの全てのシステムが十分に文書化され、バリデートされているかどうかを示し、また EU GMP A11 (4) で要求されるコントロールされたシステム記述書が存在することが確認できるものであること。
12.	A statement on the qualifications and training background of personnel engaged in design, coding, testing, validation, installation and operation of computerised systems, including consultants and sub-contractors, (specifications, job descriptions, training logs).	コンピュータ化システムの設計、コーディング、テスト、バリデーション、据付、運用に従事する要員の適格性とトレーニングについての宣言。コンサルタント及び請負業者も対象とする（仕様書、職務記述書、トレーニング記録）。
13.	State the firm's approach to assessing potential suppliers of hardware, software and systems.	潜在的なハードウェア／ソフトウェア／システムの供給者をアセスメントする際の会社のアプローチを記載する。
14.	Specify how the firm determines whether purchased or "in-house" software has been produced in accordance with a system of QA and how validation work is undertaken.	購入又は「内製」したソフトウェアが、QA システムに従って作成されたかどうかを会社がどのように判断しているか、及び会社がどのようにバリデーション作業を実施しているか、を特定する。
15.	Document the approach that is taken to the validation and documentation of older systems where original records are inadequate.	オリジナル記録が不適切である場合、古いシステムのバリデーションと文書化のために講じたアプローチを記録する。
16.	Summarise the significant computer system changes made since the last inspection and plans for future developments.	前回の査察以降のコンピュータシステムの重要な変更、及び将来の開発計画をまとめる。
17.	Ensure that records relating to the various systems are readily available, well organised, and key staff are prepared to present, discuss and review the detail, as necessary.	様々なシステムの関連記録が、すぐに提供可能であり、適切に構成されており、必要に応じ主要スタッフが詳細について発表、議論、レビューする用意があることを確認する。

Table 2
表 2
Software Related - Inspector's Aide Memoir[55]
ソフトウェア関連の査察官の覚書 [55]

Life Cycle Stage **ライフサイクルステージ**	**Project Stage Activity** **プロジェクトステージのアクティビティ**	**Evidence for Review** **レビューの証拠**
1. Development 開発	Develop URS/FS/DS URS/FS/DS を作成する。	URS/FS/DS Documents URS/FS/DS 文書
1. Development 開発	Plan Testing テストを計画する。	Test plan and test scripts テスト計画とテストスクリプト
1. Development 開発	Plan documentation of Testing テストの文書化を計画する。	Written document describing how testing should be documented. テストの文書化の方法を説明する文書。
2. Implementing 実装	Select programming language and tools プログラミング言語とツールを選択する。	Document recording programming choices プログラミングの選択を記録する文書。
2. Implementing 実装	Write/create software program. ソフトウェアプログラムを記述／作成する。	Documented source code with comments; explanation of function; in-data and expected out-data for each structured module. How modules influence each other. If program is purchased, how is access to source code guaranteed[56]? 作成されたコメント付きソースコード。機能の説明、各構造化モジュールの入力データ及び予測される出力データが記載されている。モジュールが互いにどのように影響しあうか。プログラムを購入する場合、ソースコードへのアクセスはどのように保証されるか。[56]

[55] Some of the details below are not relevant for COTS but it is necessary to have clearly defined the requirements for intended use and to have assessed the application's fitness for purpose.
[55] 以下の詳細の中には、市販ソフトウェアには適用されないものもあるが、用途についての要件を明確に定め、当該アプリケーションが目的に合っているかどうかのアセスメントを済ませている必要がある。
[56] Under some circumstances, access to source code cannot be guaranteed. Regulated users are expected to have assessed the business risks and put in place contingency measures in the event of the business failure of the supplier.
[56] 状況によっては、ソースコードへのアクセスが保証されないことがある。規制対象ユーザーは、ビジネスリスクのアセスメントを行い、サプライヤのビジネスが失敗した場合に非常事態措置を実施することを期待される。

Life Cycle Stage ライフサイクルステージ	Project Stage Activity プロジェクトステージのアクティビティ	Evidence for Review レビューの証拠
3. Testing (Modules) （モジュールの）テスト	Make sure each module only accepts allowed in-data and gives only allowed out-data. Testing should discover incorrect data and logic errors. 各モジュールが認められた入力データのみを受け入れ、認められた出力データのみを出力するようにする。テストにより、誤ったデータと論理エラーを発見すべきである。	Sample reports from testing if possible. Has testing covered boundaries of limits and also the input of invalid data? Have all tests been documented? Have all errors/failures been followed up? テスト報告書のサンプル（可能な場合）。テストは制限の境界、及び無効なデータの入力をカバーしているか。全てのテストは文書化されているか。全てのエラー／故障はフォローアップされているか。
Testing (Integrated Modules). （統合モジュールの）テスト	Same type of tests but applied after integrating the modules. 〔上記と〕同じタイプのテストだが、モジュール統合後に適用される。	Same kind of review of evidence. If the program is purchased, then validation proof needs to have been assessed by regulated user. 〔上記と〕同様の証拠のレビュー。プログラムを購入した場合は、規制対象ユーザーがバリデーションの証明をアセスメントしておく必要がある。
4. Maintenance 保守	Correct errors, update versions when needed. エラーを修正し、必要があればバージョンを更新する。	Formal routines and records for configuration management and change control. Regression testing and periodic evaluation (as a system goes through multiple changes over time) 構成管理と変更コントロールの正式な日常業務と記録。（システムが時間の経過に伴い複数の変更を受けるため）機能退行テストと定期評価。
5. Documentation 文書	System documentation (including software) correct and updated. 正確で、更新されたシステム文書（ソフトウェアを含む）。	User handbook, supporting SOPs, correct versions. ユーザーハンドブック、サポートする SOP、正しいバージョン。
6. Re-validation. 再バリデーション	Re-validate when changes are made to the program. プログラムを変更した場合に再バリデーションを実施する。	Changes are reviewed and decisions documented. Routines and records are in-place, scoped dependent on the size/complexity of the changes 変更がレビューされ、決定が文書化されている。日常業務が定められており、記録が存在し、変更の規模／複雑さに応じて適用範囲が決められている。

Life Cycle Stage ライフサイクルステージ	Project Stage Activity プロジェクトステージのアクティビティ	Evidence for Review レビューの証拠
7. Other matters その他の事項	Alternative routines are put in place for system failure and training includes this. システム故障時に代替の日常業務が実施される。トレーニングにこれが含まれている。	The alternative routines are documented, including training records. 代替の日常業務が文書化されている（トレーニング記録を含む）。

Table 3
表 3
Computer System Validation Related - Inspector's Aide Memoir
コンピュータシステムバリデーション関連についての査察官の覚書

Number 番号	Element 要素	Control Measure Checks コントロール方策のチェック
1	Define 定義	Is the system defined? What should it do? Is there a written validation plan? Are there full specifications? Are there written protocols? (Including acceptance criteria). システムは定義されているか？システムがすべきことは何か？文書化されたバリデーション計画はあるか？仕様は完全か？文書化された実施計画はあるか？（受入基準を含む）
2	Testing テスト	Do the test records show that 'in' and 'out' data meets the specifications? テスト記録が「入力」データと「出力」データが仕様を満たしていることを示しているか？
3	Documented results 文書化された結果	Are the results complete and documented? 結果は完全であり、文書化されているか？
4	Verify correctness 正確さを検証する	Are data and documentation correct and complete? Have these been verified by the regulated user? データと文書は正確かつ完全なものであるか？これらは規制対象ユーザーによって検証されているか？
5	Compare with Acceptance Criteria 受入基準と比較する	Have competent responsible personnel carried out the validation and review work? Is this all documented? 適格な信頼できる要員がバリデーションとレビューの作業を実施しているか？これは全て文書化されているか？

Number 番号	Element 要素	Control Measure Checks コントロール方策のチェック
6	Conclusions 結論	Are conclusions complete, meaningful and based on results? Are acceptance criteria fulfilled? Are there any conditional conclusions? 結論は完全で、意味があり、結果に基づいたものであるか？受入基準を満たしているか？結論に条件があるか？
7	Approval 承認	Has approval been formally recorded? Was there any QA/QC involvement at the regulated user? 承認は正式に記録されているか？規制対象ユーザー側での QA／QC の関与はあるか？
8	On-going evaluation オンゴーイング評価	What is the procedure to ensure on-going evaluation of the system? What are the change control procedures? システムのオンゴーイング評価を確実にする手順はどのようなものか？変更コントロール手順はどのようなものか？

Table 4
表 4
Annex 11 - Inspector's Checklist
Annex 11 -査察官のチェックリスト【巻末訳注 1】

Point ポイント	Requirement 要件	Inspector's Check/Comment 査察官のチェック／コメント
Personnel (1) 要員	Key personnel/computer specialists co-operate. 主要要員／コンピュータスペシャリストが協力している。	
Personnel (1) 要員	Project and user personnel are trained and any necessary experts are involved. プロジェクト及びユーザー要員がトレーニングを受け、必要に応じ専門家が関与している。	
Validation (2) バリデーション	Life-cycle model; formal policy and procedures in place. ライフサイクルのモデル。正式な方針と手順が設けられている。	
System (3) システム	Influence of environment 環境の影響	
(4)	There is a written, up to date, detailed description of the system. 最新の詳細なシステム記述書がある。	
(5)	Software has been produced according to a quality assured system. 品質保証システムに従ってソフトウェアが作成されている。	

Point ポイント	Requirement 要件	Inspector's Check/Comment 査察官のチェック／コメント
(6)	Checks of data and calculations built in. データと演算のチェックが組み込まれている。	
(7)	System tested and validated. Verified against previous/or manual system being replaced. システムがテストされ、バリデートされている。置き換え前のシステム、または手作業のときと比較して検証されている。	
(8)	Data entry and change only by authorised personnel. Password / security management. データの入力と変更は許可された要員に限定されている。パスワード／セキュリティ管理。	
(9)	Critical data (GXP data) verified by a 2nd person, or by a validated electronic method. 重要なデータ（GxP データ）は、当事者とは別の者、又はバリデートされた電子的方式によって検証されている。	
(10)	Audit trail for data entry and processing. データの入力と処理についての監査証跡。	
(11)	Alterations to system and programs subjected to rigorous change controls, including re-validation and approvals. システム及びプログラムに対する変更は、再バリデーションと承認を含む厳格な変更コントロールに従っている。	
(12)	Printed copies of electronically stored data available if needed? 必要な場合、電子的に保存されたデータを印刷したコピーが入手可能である。	
(13) and GMP 4.9	Physical and logical protection of data. Information security management and change management. データの物理的及び論理的保護。情報のセキュリティ管理と変更管理。	
(14)	Data back up procedures; separate and secure media and locations. データのバックアップ手順。離れたところにある安全な媒体と保管場所。	
(15)	Alternative routine arrangements established in the event of system failure. システム故障が発生した場合の代替の日常業務の体制が確立されている。	

Point ポイント	Requirement 要件	Inspector's Check/Comment 査察官のチェック／コメント
(16)	Validated alternative arrangements (15) defined and documented. Records of failures and remediation exist. バリデートされた代替の体制（15）が定義され、文書化されている。故障と対処の記録が存在する。	
(17)	Records show the analysis of errors and corrective actions taken. エラーの分析と講じた是正処置が記録されている。	
(18)	Service level agreements or contracts in place for services provided by outside agencies for computerised systems at regulated user's sites. 規制対象ユーザーのサイトにあるコンピュータ化システムのために外部機関が提供するサービスについてサービスレベル合意書又は契約書が存在する。	
(19)	Responsibilities in chain of release of batches defined and linked to QP. 一連のバッチリリースについての責任が定義され、QP【訳注】にリンクされている。 【訳注】Qualified Person 。	

Table 5
表 5
General Points for Inspectors To Consider On Inspection
査察官が査察時に検討すべき一般事項

Number 番号	Area 領域	Remember 留意点
1.	Personnel 要員	Is there only one key person? (Dependence on only one person may be catastrophic). キーパーソンは 1 名のみか？（1 名のみに依存することは、大惨事を招き得る）
2.	Organisation 組織	Is management involved? 管理職が関与しているか？
3.	Organisation 組織	Is the Quality organisation involved? 品質組織が関与しているか？
4.	Data system データシステム	Early during the inspection, ask for a complete overview of the system(s) including flow of data. 査察の初期にデータフローを含むシステムの完全な概要を要求する。

Number 番号	Area 領域	Remember 留意点
5.	Data system データシステム	The use of 'parallel' systems may indicate 'grey' areas and potential system weaknesses. 「並列」システムを使用しているというときは、「灰色」の領域があるということであり、システムの脆弱性があるかもしれない。
6.	Validation バリデーション	Has terminology actually been defined? Is it used correctly? 実際に用語が定義されているか？用語は正確に用いられているか？
7.	Security セキュリティ	How is access controlled? Information Security Management? アクセスはどのようにコントロールされているか？情報セキュリティ管理〔はどうなっているか〕？
8.	Maintenance 保守	Is there a maintenance manual of each system detailing what to do on a periodic basis? (Daily, weekly, monthly etc). Are there corresponding records of compliance? 各システムの保守マニュアルがあり、定期的（毎日、毎週、毎月等）に行うべきことを詳細に記述しているか？適合を示す記録があるか？
9.	Control of System システムのコントロール	Routines for configuration management, and change control in place? 構成管理、及び変更コントロールの日常業務が定められているか？
10.	Self-inspections 自己査察	Are self-inspection routines in place? 自己査察の日常業務が定められているか？

Table 6
表 6
Overview of User Responsibilities (from GAMP 4 Table 7.1) [57]
ユーザーの責任の概要（GAMP 4【巻末訳 2】の表 7.1 より）[57]

Step ステップ	Task タスク	Description 説明
1.	Identify system システムの特定	Each automated system should be assessed and GxP regulated systems identified. 各自動化システムを評価し、GxP 規制の対象となるシステムを特定する。
2.	Produce URS URS の作成	The URS should define clearly and precisely what the user wants the system to do, state any constraints, and define regulatory and documentation requirements. ユーザーがシステムに期待することを URS に明確かつ正確に定義する。制約があれば記述し、規制と文書化の要件を定義する。

[57] Refer also to Section 15 for context (validation strategy for different systems).
[57] この背景（様々なシステムについてのバリデーション戦略）については第 15 章も参照。

Step ステップ	Task タスク	Description 説明
3.	Determine validation strategy バリデーション戦略の策定	
	• Risk Assessment リスクアセスメント	An initial Risk Assessment should be carried out during validation planning. Further assessments should be performed as specifications are developed. バリデーション計画中に初期リスクアセスメントを実施する。仕様が決定するに従い、更なるアセスメントを行う。
	• Assessment of system components システムコンポーネントのアセスメント	System components should be assessed and categorized to determine the validation approach required. The output from this assessment will feed into the Validation Plan. システムコンポーネントのアセスメントを行い、必要とされるバリデーションアプローチを決定するために分類する。このアセスメント結果のアウトプットはバリデーション計画書に組み込まれる。
	• Supplier assessment サプライヤアセスメント	Suppliers should be formally assessed as part of the process of selecting a supplier and planning for validation. The decision whether to perform a Supplier Audit should be documented and based on a Risk Assessment and categorization of the system components. サプライヤ選定プロセス及びバリデーションの計画策定の一環として、サプライヤを正式にアセスメントする。サプライヤ監査を実施するか否かを決定し、文書化する。決定はリスクアセスメントとシステムコンポーネントの分類に基づいて行う。
4.	Produce Validation Plan バリデーション計画書の作成	The Validation Plan should define the activities, procedures, and responsibilities for establishing the adequacy of the system. It typically defines what Risk Assessments are to be performed. バリデーション計画書では、システムの妥当性を確立するための活動／手順／責任を定める。一般的に、どのようなリスクアセスメントを実施するかを定める。
5.	Review and approve specifications, including the system description システム記述書を含む仕様のレビュー及び承認	The user should review and approve specifications produced by the supplier. ユーザーはサプライヤが作成した仕様のレビュー及び承認を行う。
6.	Monitor development of system システム開発の監視	The user should monitor development and configuration activities against an agreed plan. ユーザーは、開発／構成設定の活動を、合意された計画に照らして監視する。
7.	Review source code ソースコードのレビュー	The user should ensure that source code is adequately reviewed during system development. ユーザーは、ソースコードがシステム開発中に適切にレビューされることを確実にする。

Step ステップ	Task タスク	Description 説明
8.	Review and approve test specifications テスト仕様のレビュー及び承認	The user should review and approve test specifications prior to formal testing. ユーザーは、正式なテストを実施する前に、テスト仕様をレビュー及び承認する。
9.	Perform testing テストの実施	The user may be involved in testing, as a witness during test execution, or as a reviewer of test results. ユーザーは、テスト実施中の立会者、又はテスト結果のレビュー者としてテストに関わる。
10.	Review and approve test reports テスト報告書のレビュー及び承認	The user should approve the test reports and associated test results. ユーザーはテスト報告書と関連するテスト結果を承認する。
11.	Produce Validation Report バリデーション報告書の作成	The Validation Report should summarize all deliverables and activities and provides evidence that the system is validated. バリデーション報告書では、全ての成果物と活動を要約し、システムがバリデートされた証拠を示す。
12.	Maintain System システムの保守	Once the system has been accepted, the user should establish adequate system management and operational procedures. システム受入後、ユーザーはシステムを管理／運用するための適切な手順を確立する。
13.	System Retirement システムリタイアメント	The user should manage the replacement or withdrawal of the automated system from use. ユーザーは自動化システムの置き換え、又は運用停止を管理する。

25. REFERENCES FOR RELEVANT STANDARDS AND GMP GUIDES / CODES

25. 関連規格と GMP ガイド／規則の参考資料

(1) EU Annex 11 to the EU guidelines of Good Manufacturing Practice for Medicinal Products.
(2) Annex 11 to PIC/S Guide to Good Manufacturing Practice for Medicinal Products, Document PH 1/97 (Rev. 3), PIC/S Secretariat, 9-11 rue de Varembe, CH-1211 Geneva 20
(3) GAMP Guide for Validation of Automated Systems, GAMP4 (ISPE (GAMP Forum), 2001)
(4) Australian Code of GMP for Medicinal Products, August 2002.
(5) WHO Guideline for GMP for Manufacture of Pharmaceutical Products.
(6) Relevant CFR sections of the USFDA Register:

Hardware
21 CFR 211.63, 67, 68
21 CFR Part 11 Electronic Records: Electronic Signatures

Software
21 CFR 211.68, 180, 188, 192
21 CFR Part11 Electronic Records: Electronic Signatures

Quality System
21 CFR 820 Quality system regulation

GLP
21 CFR 58 Good laboratory practice for non-clinical laboratory studies

(7) ISO standards:
Quality management and quality assurance
ISO 9000-1 Part 1: Guidelines for selection and use.
ISO 9000-3 Part 3: Guidelines for the application of ISO9001:1994 to the development, supply, installation and maintenance of computer software. See also current Tick-IT Guide for construction, software engineering, assessment and certification (see ref. 12 re:BSI DISC London)

Quality Management and quality system elements
ISO 9004-1 Part 1: Guidelines.
ISO 9004-2 Part 2: Guidelines for Services.
ISO 9004-4 Part 4: Guidelines for quality improvement.
ISO 10005: 1995 Quality management - Guidelines for quality plans.
ISO 10007: 1995 Quality management - Guidelines for Configuration Management

Life cycle management
ISO/IEC 12207:1995 Information Technology - Software Life Cycle processes
ISO/IEC 17799:2000 (BS 7799-1:2000) Information technology － Code of practice for information security management.

(8) IEEE Publications:
IEEE 729 Glossary of Software Engineering Terminology
IEEE 730 Quality Assurance Plan
IEEE 828 Software Configuration Management Plans
IEEE 829 Software Test Documentation
IEEE 830 Guide to Software Requirements Specification
IEEE 983 Guide to Software Quality Assurance Planning
IEEE 1012 Software Verification Plans
IEEE 1298 Software Quality Management System Part 1: Requirements

(9) British Standards:
BS 7799: 1999 "Information Security Management", BSI DISC 389 Chiswick High Road, London W4 4AL (Tel:+44 181 995 7799 Fax:+44 181 996 6411 http://www.bsi.org.uk/disc)
BS 7799: 2000 Information technology － Code of practice for information management

(10) DISC BSI Guides
DISC PD 5000 series of 'Codes for Electronic Documents and e-Commerce Transactions as Legally Admissible Evidence' (including DISC PD 0008:1999 in Pt 1):

Pt 1	Information Stored Electronically
Pt 2	Electronic Communication and e-mail policy
Pt 3	Identity Signature and Copyright
Pt 4	Using Certification Authorities
Pt 5	Using trusted Third Party Archives
DISC PD 3002	Guide to BS 7799 Risk Assessment and Risk Management (ISBN 0 580 29551 6)
DISC PD 3005	Guide on the selection of BS 7799 controls (ISBN 0 580 33011 7)

(11) 'Guidance for Industry, Part 11, Electronic Records; Electronic Signatures - Scope and Application', US Dept. of Health and Human Services and all FDA Centers/ Offices, February 2003. (\\CDS029\CDERGUID\5505dft.doc) - draft guidance for comment【訳注】.

【訳注】Part 11, Electronic Records; Electronic Signatures - Scope and Application'は既に発行済みである。（https://www.fda.gov/media/75414/download）

26. SUGGESTED FURTHER READING

26. 推奨参考資料

1. Good Computer Validation Practices － Common Sense Implementation [Stokes, Branning, Chapman, Hambloch & Trill. Interpharm Press, USA: ISBN: 0-935184-55-4]
2. Computer Systems Validation for the Pharmaceutical and Medical Device Industries [Chamberlain. ISBN 0-9631489-0-8].
3. Validating Automated Manufacturing and Laboratory Applications, [Wingate et al., Interpharm Press, USA: ISBN 1-57491-037-X]
4. Validation of Computerized Analytical Systems, Interpharm Press, L. Huber, ISBN: 0-935184-75-9, 1995
5. General Principles of Software Validation - Final Guidance for Industry and FDA Staff (FDA, CDRH, January 2002)
6. PDA Technical Report No 18, "Validation of Computer-Related Systems", PDA Journal of Pharmaceutical Science and Technology, 1995 Supplement, Vol. 49, No.S1
7. PDA Technical Report No. 32, "Report on the Auditing of Suppliers providing Computer Products and Services for Regulated Pharmaceutical Operations" (PDA, 1999)
8. 'Validation of Process Control Systems: a Guideline by GMA & NAMUR', in Section 5 of GAMP-3 (1998) Vol. 2, Best Practice for Users and Suppliers.
9. PDA Technical Report No. 31: "Validation and Qualification of Computerised Laboratory Data Acquisition Systems", PDA Journal of Pharmaceutical Science and Technology, 1999 Supplement, Vol. 53, No.4
10. Guidance for Industry - 'Computerized systems used in Clinical Trials', US FDA, April 1999
11. GLP Consensus Document 'The Application of the Principles of GLP to Computerised Systems', 1995, OECD/ OCDE/GD (95) 115 (Environment Monograph No.116)
12. Computer Systems Validation in Clinical Research, 1997, ACDM/ PSI Working Party. (ACDM, PO Box 129, Macclesfield, Cheshire SK11 8FG England)
13. ICH Topic E6: 'Guideline for Good Clinical Practice'. (ICH-GCP/CPMP/ICH/135/95)
14. EU GMP Guide Annex 15, 'Qualification and Validation', European Commission, July 2001, (based on PIC/S recommendations)
15. APV Guidance, Appendix 9 to GAMP4 'Guide for Validation of Automated Systems', ISPE (GAMP Forum), 2001

27. GLOSSARY OF TERMS

27. 用語集

This glossary has been extracted predominantly from the (1) EU GMP Annex 15, Qualification and Validation document, [see 'Further Reading Ref:14]; (2) the GAMP Guide; and (3) the PDA Technical Report No 18. The list of definitions has been compiled to reflect the current terminology generally accepted internationally. Inspectors may have to correlate or adapt the terms in the light of internal policies, standards and guidelines used by regulated user's companies and relevant SDLC methodologies. The sources of each of the definitions have been identified in the following manner: • EU GMP Annex 15 PIC/S document definitions are recorded as (1); • GAMP definitions are recorded as (2);	本用語集は主に以下から抜粋した。 (1) EU GMP Annex 15, Qualification and Validation document（推奨参考資料 14 を参照） (2) GAMP ガイド【巻末訳注 2】 (3) PDA Technical Report No 18 この用語集の定義は、一般的に国際的に認められている最新用語を反映するように編集した。査察官は、これらの用語を規制対象ユーザー会社が使用する社内の方針／基準／ガイドライン、及び関連する SDLC 手法を踏まえたうえで、関連付けて理解するか、適応する必要があるかもしれない。定義の出典は、以下のように区別して示した。 • EU GMP Annex 15 PIC/S ドキュメントの定義は (1) • GAMP の定義は (2) 【訳注】

• PDA technical report no. 18 definitions are recorded as (3); • EC Directive 1999/93/EC on a Community framework for electronic signature, (Official Journal of the European Communities, 19.1.2000), (4); • Definitions elaborated in this PIC/S document do not carry a suffix number.	• PDA technical report no. 18 の定義は (3) • EC Directive 1999/93/EC on a Community framework for electronic signature, (Official Journal of the European Communities, 19.1.2000)は (4) • 本書で独自に作成した定義については上記の文末の出典識別番号は記載しない。 【訳注】(2) GAMP 4【巻末訳注 2】については ISPE より和訳が出版されているが、原文から変更されて引用されているため、独自に訳した。
Advanced Electronic Signature (EU) means an electronic signature, which meets the following requirements: (a). it is uniquely linked to the signatory; (b). it is capable of identifying the signatory; (c). it is created using means that the signatory can maintain under his control; and (d). it is linked to the data to which it relates in such a manner that any change of the data is detectable. (4)	***高度な電子署名*** （EU では）以下の要件を満たす電子署名を意味する。 (a) 署名者に固有に紐付けされている。 (b) 署名者を特定できる。 (c) 署名者が自らのコントロールのもと維持管理できる手段を用いて作成される。 (d) 電子署名は当該データへの変更があれば検出できるようなやり方で関連付けられたデータに紐付けされている。(4)
Application-Specific Software A software program developed or adapted to the specific requirements of the application. (3)	***アプリケーション専用ソフトウェア*** 特定のアプリケーション要件のために開発又は採用されたソフトウェアプログラム。(3)
Automated System Term used to cover a broad range of systems, including automated manufacturing equipment, control systems, automated laboratory systems manufacturing execution systems and computers running laboratory or manufacturing database systems. The automated system consists of the hardware, software and network components, together with the controlled functions and associated documentation. Automated systems are sometimes referred to as computerised systems; in this Guide the two terms are synonymous. (2) (GAMP 4 (3) 'Scope' page 14)	***自動化システム*** 幅広いシステムをカバーする用語であり、自動製造機器、制御システム、自動実験システム、製造実行システム、ラボラトリ又は製造のデータベースシステムを実行するコンピュータ、を含む。 自動化システムは、ハードウェア、ソフトウェア、及びネットワークといった部品と、制御される機能、及び関連文書から構成される。自動化システムはコンピュータ化システムとも呼ばれるが、本書では、この 2 つの用語は同義で用いている。) (GAMP 4 (3) 「Scope」 page 14)
Bespoke A system produced for a customer, specifically to order, to meet a defined set of user requirements. (2)	***カスタム*** 定義された一連のユーザー要件を満たすために顧客の注文どおりに製造されたシステム。(2)
Bug A manifestation of an error in software (a fault). (2)	***バグ*** ソフトウェアのエラーが表出したもの（欠陥）(2)

Change Control A formal system by which qualified representatives of appropriate disciplines review proposed or actual changes that might affect a validated status of facilities, systems, equipment or processes. The intent is to determine the need for action that would ensure that the system is maintained in a validated state. (1) [Authors note: FDA may specifically require evidence of pre and post implementation reviews of changes. The latter to detect any unauthorised changes that may have been made despite established procedures. These are quality assurance activities.]	***変更コントロール*** 提案された（又は実際の）バリデートされた施設／システム／機器／プロセスの状態に影響し得る変更を、資格を持つ適切な専門分野の代表者がレビューする正式なシステム。この意図は、バリデートされたシステム状態を維持することを確実にするためのアクションが必要か否かを決定することである。(1) [著者によるメモ ― FDA は変更実施前と実施後の証拠を要求するかもしれない。後者は、確立された手順があるにも拘らず、許可なく行われた変更を検出するためのものである。これは、品質保証の活動である。]
Commercial off-the-shelf (COTS) Configurable Programs- Stock programs that can be configured to specific user applications by "filling in the blanks", without (COTS) altering the basic program. (3)	***市販ソフトウェア*** 構成設定可能なプログラム―基本プログラムを変更せずに「空欄に入力することで」ユーザーの特定のアプリケーションに合わせて構成設定できる作成済みのプログラム。(3)
Computer Hardware Various pieces of equipment in the computer system, including the central processing unit, the printer, the modem, the cathode ray tube (CRT), and other related apparatus. (3) (See also Figure 1, page 8, of this document).	***コンピュータハードウェア*** コンピュータシステムにおける様々な機器。CPU、プリンタ、モデム、CRT、その他の関連機器を含む。(3)（本書 14 ページの図 1 も参照。）
Computer System Computer hardware components assembled to perform in conjunction with a set of software programs, which are collectively designed to perform a specific function or group of functions. (3) (See also Figure 1, page 8, of this document).	***コンピュータシステム*** コンピュータのハードウェア部品を組み立て、一連のソフトウェアプログラムと組み合わせて動作するものであり、一体となって特定の機能又は機能群を実行するように設計される。(3)（本書 14 ページの図 1 も参照。）
Computerised System A computer system plus the controlled function that it operates. (3) [Authors note: Today this may be considered to be rather a narrow definition, especially in the context of integrated computers. The definition should therefore include all outside influences that interface with the computer system in its operating environment. These may typically include monitoring and network links, (to/from other systems or instruments), manual (keypad inputs), links to different media, manual procedures and automation. The term also covers automated instruments and systems. See also the definition for 'automated systems' in this section and Section 26, Reference 11, the GLP OECD consensus document. PIC/S GMP Annex 11(4) is relevant here regarding documenting the scope and interaction of systems.]	***コンピュータ化システム*** コンピュータシステムに当該システムが動かす制御される機能を加えたもの。(3) [著者によるメモ ― 今日では、特に複数のコンピュータが統合される状況を踏まえると、上記は狭義の定義であると言える。従って、この定義には運用環境においてコンピュータシステムとインターフェースする外部からのあらゆる影響を含めるべきである。これらには、一般的に、（他のシステムや機器との間の）監視／ネットワークのリンク、手入力（キーパッド入力）、他の媒体／手作業／自動化とのリンクのつながりを含む。この用語は、自動化機器とシステムもカバーする。本章の「自動化システム」の定義、第 26 章の参考資料 11 GLP OECD consensus document も参照のこと。システムの範

	囲とインタラクションの文書化に関し PIC/S GMP Annex 11(4) 【巻末訳注 1】 が関連する。]
Configuration The documented physical and functional characteristics of a particular item, or system, e.g. software, computerised system, hardware, firmware and operating system. A change converts one configuration into a new one.	***構成設定*** 特定のアイテム、又はシステム（例：ソフトウェア、コンピュータ化システム、ハードウェア、ファームウェア、及びオペレーティングシステム）の文書化された物理特性及び機能特性。 変更を加えると、既存の構成設定が新しい構成設定に変わる。
Configuration Management The process of identifying and defining the configuration items in a system, controlling the release and change of these items throughout the system life cycle, recording and reporting the status of configuration items and change requests, and verifying the completeness and correctness of configuration items. (2)	***構成管理*** システムにおける構成アイテムを特定／定義し、システムライフサイクルを通してアイテムのリリースと変更をコントロールし、構成アイテムと変更要求のステータスを記録／報告し、構成アイテムの完全性と正確性を検証するプロセス。(2)
Debugging (IEEE) The process of locating, analysing, and correcting suspected faults. (2)	***デバッグ (IEEE)*** 疑わしい欠陥を見つけ、分析し、修正するプロセス。(2)
Electronic Signature An electronic measure that can be substituted for a handwritten signature or initials for the purpose of signifying approval, authorisation or verification of specific data entries. See also definition for 'Advanced Electronic Signature', above.	***電子署名*** 特定のデータ入力を承認、許可、又は検証したことを示す目的で行う手書き署名又はイニシャルの代わりとなる電子的手段。上記の「高度な電子署名」の定義も参照のこと。
Electronic Signature (FDA) 21 CFR Part11 defines this as: The computer data compilation of any symbol or series of symbols executed, adopted, or authorised by an individual to be the legally binding equivalent of the individual's hand-written signature.	***電子署名 (FDA)*** 21 CFR Part11 の定義は次の通り。「手書き署名と同等の法的拘束力があるものとして本人が作成、採用、承認する記号をコンピュータデータとして編集したもの。」
Electronic Signature (EU) 1999/93/EC states: 'electronic signature' means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication. (See also 'Advanced Electronic Signature') (4)	***電子署名(EU)*** 1999/93/EC では以下のように述べている。 「「電子署名」とは、他の電子データに付属しているか、論理的に関連付けられている電子形式のデータであり、認証方式としての役割を果たすものを意味する。」 （「高度な電子署名」の項も参照のこと。）(4)
Embedded System A system, usually microprocessor or PLC based, whose sole purpose is to control a particular piece of automated equipment. This is contrasted with a standalone computer system. (2)	***組込型システム*** 通常、マイクロプロセッサ又は PLC をベースとしたシステムであり、用途が自動化機器の特定部分を制御することに限定されている。これは、スタンドアロンのコンピュータシステムと対比される。(2)

Executive Program (ANSI/IEEE/ASO) A computer program, usually part of the operating system, that controls the execution of other computer programs and regulates the flow of work in a data processing system. (2)	***監視プログラム (ANSI / IEEE / ASO)*** 通常は、オペレーティングシステムの一部であるコンピュータプログラムであり、他のコンピュータプログラムの実行を制御し、データ処理システムにおけるワークフローを制御する。(2)
Firmware A software program permanently recorded in a hardware device, such as an EPROM. (3) (Note: EPROM stands for 'Erasable Programmable Read Only Memory')	***ファームウェア*** EPROM 等のハードウェアデバイスに永続的に記録されたソフトウェアプログラム。(3)（注意 — EPROM は「Erasable Programmable Read Only Memory」の略語で、「消去可能な PROM」のこと。）
Functional Requirements (ANSI/IEEE) Statements that describe functions a computer-related system must be capable of performing. (3)	***機能要件 (ANSI /IEEE)*** コンピュータ関連システムが実行できなければならない機能を述べた宣言。(3)
Functional Specifications Statements of how the computerised system will satisfy functional requirements of the computer-related system. (3)	***機能仕様書*** コンピュータ関連システムの機能要件をコンピュータ化システムがどのように満たすかを述べた宣言。(3)
Functional Testing A process for verifying that software, a system, or a system component performs its intended functions. (3)	***機能テスト*** ソフトウェア、システム、又はシステムコンポーネントが意図どおりに機能することを検証するプロセス。(3)
Hardware Acceptance Test Specification Statements for the testing of all key aspects of hardware installation to assure adherence to appropriate codes and approved design intentions and that the recommendations of the regulated user have been suitably considered. (2)	***ハードウェア受入テスト仕様書*** ハードウェア据付の全ての主要な側面をテストすることの宣言であり、該当する規則及び承認された設計の意図に適合し、規制対象ユーザーへの推奨事項が適切に考慮されたことを保証するもの。(2)
Hardware Design Specification (APV) Description of the hardware on which the software resides and how it is to be connected to any system or equipment. (2)	***ハードウェア設計仕様書 (APV)*** ソフトウェアが搭載されるハードウェア、及びハードウェアがシステムや機器にいかに接続されるかについての記述。(2)
Hybrid Systems Refer to Section '21.6' of this document	***ハイブリッドシステム*** 本書の「第 21.6 章」を参照のこと。
Integration testing (IEEE) An orderly progression of testing in which software elements, hardware elements, or both are combined and tested until the entire system has been integrated. (2)	***統合テスト (IEEE)*** 統制されたテスト進行の一部であり、ソフトウェア要素、ハードウェア要素、又は両者が結合されテストされる。これはシステム全体が統合されるまで行われる。(2)
Interface (ANSI/IEEE) A shared boundary. To interact or communicate with another system component. (2)	***インターフェース (ANSI/IEEE)*** 共有される境界部分。他のシステムコンポーネントとやり取り又は通信を行うためのもの。(2)

Legacy Computerised Systems These are regarded as systems that have been established and in use for some considerable time. For a variety of reasons, they may be generally characterised by lack of adequate GMP compliance related documentation and records pertaining to the development and commissioning stage of the system. Additionally, because of their age there may be no records of a formal approach to validation of the system.	***レガシーコンピュータ化システム*** 導入後、かなりの期間使用されてきたシステムのことをいう。一般的に、様々な理由から、適切な GMP 適合を示す関連文書、及びシステムの開発／試運転の段階に関する記録が欠如していることが多い。さらに、時間が経過しているためにシステムバリデーションの正式なアプローチの記録が存在しない場合がある。
Life Cycle Concept An approach to computer system development that begins with (PMA CSVC) identification of the user's requirements, continues through design, integration, qualification, user validation, control and maintenance, and ends only when commercial use of the system is discontinued. (2)	***ライフサイクルの概念*** コンピュータシステム開発のアプローチのひとつであり、ユーザー要件の特定から始まり、設計、統合、適格性評価、ユーザーのバリデーション、コントロール、及び保守に至るまで続く。システムの商用利用が停止した場合にのみ終了する。(2)　(PMA CSVC) 【巻末訳注 3】
Loop Testing Checking the installed combination of elements characterising each type of input/output loop. (2)	***ループテスト*** 据え付けられた要素の組み合わせで、各種のインプット／アウトプットのループの特徴を持つものをチェックすること。(2)
Network (ANSI/IEEE & GAMP) (a). An interconnected, or interrelated group of nodes. (b). An interconnected communications facility. A Local Area Network (LAN) is a high bandwidth (allowing a high data transfer rate) computer network operating over a small area such as an office or group of offices. (2)	***ネットワーク (ANSI/IEEE & GAMP 【巻末訳注 2】)*** (a) 相互接続された、又は相互に関連するノードの集まり。 (b) 相互接続された通信設備。LAN は高帯域幅（高データ転送率を実現）のコンピュータネットワークであり、オフィスや複数のオフィス等の狭い範囲で機能する。(2)
Operating Environment Those conditions and activities interfacing directly or indirectly with the system of concern, control of which can affect the system's validated state. (3)	***運用環境*** 対象システムに直接又は間接的にインターフェースする状態及び活動であり、そのコントロールがシステムのバリデートされた状態に影響を及ぼし得るもの。(3)
Operating System A set of software programs provided with a computer that function as the interface between the hardware and the applications program. (3)	***オペレーティングシステム*** ハードウェアとアプリケーションプログラムの間のインターフェースとして機能する、コンピュータと合わせて提供される一連のソフトウェアプログラム。(3)
Public Key Infrastructure **Public Key Infrastructure (PKI) provides a framework for secure communication, using a combination of public-key cryptography and Digital Certificates.** PKIs can exist within many different domains but essentially there are two types: A Private PKI is deployed by a corporation for the benefit of its business and any related parties (e.g.	***公開鍵認証基盤*** **公開鍵認証基盤 (PKI) は、公開鍵の暗号とデジタル認証の組み合わせを用いて安全な通信の枠組みを提供する。** PKI は、異なる多くの領域で存在しているが、本質的には以下の 2 種類がある。 Private PKI は、会社で用いられ、その会社のビジネスと関連当事者（例：顧客、サプライヤ）の

customers, suppliers). Public PKIs (using 'Trusted Third Parties') are deployed on open systems, such as the Internet and facilitate security between previously unrelated parties.	ために用いられる。 Public PKI（「信頼のおける第三者」を用いる）は、インターネット等のオープンシステムで用いられ、過去に関係を持っていない当事者間のセキュリティを円滑にする。
Raw Data[58] Any work-sheets, records, memoranda, notes, or exact copies thereof, that are the result of original observations and activities and which are necessary for the reconstruction and evaluation of a work project, process or study report, etc. Raw data may be hard/paper copy or electronic but must be known and defined in system procedures. (2)	***生データ***[58] オリジナルの観測及びアクティビティの結果であるワークシート、記録、メモ、覚書、又はその正確なコピーであり、作業計画、プロセス、研究報告書等の再現及び評価に必要なもの。生データはハード／紙のコピー、又は電子的な場合があるが、〔何が生データか、を〕周知し、システム手順で定義しておかなければならない。(2)
Regulated User The regulated Good Practice entity, that is responsible for the operation of a computerised system and the applications, files and data held thereon. (See also 'User')	***規制対象ユーザー*** 規制対象グッドプラクティスの事業体であり、コンピュータ化システム、及びそこに保持されるアプリケーション／ファイル／データのオペレーションに責任を持つ者（「ユーザー」の項も参照）。
Revalidation Repetition of the validation process or a specific portion of it. (2)	***再バリデーション*** バリデーションプロセス、又はその一部を繰り返すこと。(2)
Security (IEEE) The protection of computer hardware and software from accidental or malicious access, use, modification, destruction or disclosure. Security also pertains to personnel, data, communications and the physical protection of computer installations. (2)	***セキュリティ (IEEE)*** コンピュータのハードウェアとソフトウェアの偶発的又は悪意のあるアクセス、使用、変更、破壊、開示からの保護。セキュリティは、要員、データ、通信、及びコンピュータの据付の物理的保護にも関係する。(2)
Source Code (PMA CSVC) An original computer program expressed in human-readable form (programming language), which must be translated into machine-readable form before it can be executed by the computer. (2)	***ソースコード (PMA CSVC*** 【巻末訳注 3】***)*** 人間が読むことができる形式（プログラミング言語）で表現されたオリジナルのコンピュータプログラムであり、コンピュータが解読できる形式に翻訳してからコンピュータによって実行される。(2)
Standalone System A self-contained computer system, which provides data processing, monitoring or control functions but which is not embedded within automated equipment. This is contrasted with an embedded system, the sole purpose of which is to control a particular piece of automated equipment. (2)	***スタンドアロンシステム*** 自己完結型のコンピュータシステムであり、データ処理、監視、又は制御機能を提供するが、自動化機器の中には組み込まれていない。これは、自動化機器の特定部分を制御する用途に限定した組込型システムと対比される。(2)

[58] PIC/S Author's Note on 'Raw Data'- For information: FDA's 21 CFR Part 11 requires the retention of electronic records in electronic form… 【訳注】

【訳注】脚注が長いため、本書末尾に移しました。

Structural Integrity (Software) Software attributes reflecting the degree to which source code satisfies specified software requirements and conforms to contemporary software development practices and standards. (3)	***構造的インテグリティ（ソフトウェア）*** ソースコードが指定されたソフトウェア要件を満たし、ソフトウェア開発の最新の慣行と標準に従っている程度を示すソフトウェアの属性。(3)
Structural Testing Examining the internal structure of the source code. Includes low-level and high-level code review, path analysis, auditing of programming procedures and standards actually used, inspection for extraneous "dead code", boundary analysis and other techniques. Requires specific computer science and programming expertise. (2)	***構造化テスト*** ソースコードの内部構造を調べること。低レベル／高レベルのコードレビュー、パス分析、プログラミング手順と実際に使用された標準の監査、関係のない「dead code」の検査、境界分析、等の技術を含む。情報工学、プログラミングの特定の専門知識を必要とする。(2)
Structural Verification An activity intended to produce documented assurance that software has appropriate structural integrity. (3)	***構造化検証*** ソフトウェアが適切な構造的インテグリティを持つことの文書化された証拠を作成することを意図した活動。(3)
System Acceptance Test Specification (2) The system acceptance test specification is a description of those tests to be carried out to permit acceptance of the system by the user. Typically it should address the following: • System functionality • System performance • Critical parameters • Operating procedures The tests should ensure that the product operates as indicated in the functional specification and meets the user requirements as defined in the URS. The tests typically include limit, alarms and boundary testing. The System Acceptance Test Specification is a contractual document and, as such, should be approved by both the supplier/ developer/ integrator and the end user. An example procedure for producing a System Acceptance Test Specification is given in a GAMP Guide Appendix.	***システム受入テスト仕様書 (2)*** システム受入テスト仕様書は、ユーザーによるシステムの受入を許可するために実施するテストの記述である。 通常、以下を取り扱う。 • システム機能 • システム性能 • 重要なパラメータ • 操作手順 このテストにより製品が機能仕様書に記載されている通りに機能すること、及び URS で定義されているユーザー要件を満たすことを確実にする。このテストには一般的に限界値、アラーム、及び境界値のテストが含まれる。 システム受入テスト仕様書は契約文書であり、サプライヤ／開発者／インテグレータ側とエンドユーザー側の双方によって承認されるべきである。システム受入テスト仕様書の作成手順例は GAMP ガイド 付録【巻末脚注 2】に掲載されている。
System Software Software designed to facilitate the operation and maintenance of a computer system and its associated programs, such as operating systems, assemblers, utilities, network software and ***Executive Program*** programs. System software is generally independent of the specific application. (3)	***システムソフトウェア*** コンピュータシステム及びその関連プログラム（オペレーティングシステム、アセンブラ、ユーティリティ、ネットワークソフトウェア、***監視プログラム***等）の運用と保守を容易にするために設計されたソフトウェア。システムソフトウェアは一般的に個々のアプリケーションからは独立している。(3)

System Specifications (PMA CSVC) Describe how the system will meet the functional requirements. (2)	***システム仕様書 (PMA CSVC【巻末脚注3】)*** システムがどのように機能要件を満たすか記述する。(2)
Unplanned (Emergency) Change (PMA CSVC)[59] An unanticipated necessary change to a validated system requiring rapid implementation, also known as a "hot-fix". (2)	***計画外（緊急）変更 (PMA CSVC【巻末脚注3】)[59]*** バリデートされたシステムに対する想定外の必要な変更であり迅速な実施が求められる。「ホットフィックス」ともいう。(2)
User The company or group responsible for the operation of a system. (3) (see also 'Regulated User'). The GxP customer, or user organisation, contracting a supplier to provide a product. In the context of this document it is, therefore, not intended to apply only to individuals who use the system, and is synonymous with 'Customer'. (2)	***ユーザー*** システムの運用に責任を持つ会社、又はグループ。(3) (「規制対象ユーザー」の項も参照) サプライヤと製品供給の契約を結んでいる GxP〔規制対象の〕顧客、又はユーザー組織。従って、本書では、システムを使用する個人だけでなく、「顧客」とも同義である。(2)
Utility Software (ANSI/IEEE) Computer programs or routines designed to perform some general support function required by other application software, by the operating system, or by system users. (2)	***ユーティリティソフトウェア (ANSI/IEEE)*** 他のアプリケーションソフトウェア、オペレーティングシステム、又はシステムユーザーによって必要とされる一般的なサポート機能を実行するよう設計されたコンピュータプログラム又はルーチン。(2)
Validation of Computerised Systems See text Section '14.2' for definition.	***コンピュータ化システムバリデーション*** 定義については「第 14.2 章」を参照。

28. ABBREVIATIONS USED IN THE DOCUMENT

28. 本書で用いる略語

ANSI:	American National Standards Institute
APV:	Arbeitsgemeinschaft fur Pharmazeutische Verfahrenstechnik E.V.
BSI:	British Standards Institute
DCS:	Distributed Control System
DR:	Design Review
DS:	Design Specification

[59] This can be very risky. 'Fix' testing/ implementation work should ideally not be carried out initially in the live environment. All changes to the live validated system(s) must be subjected to the firm's change control, configuration management and validation procedural controls, to ensure compliance with GMP and the maintenance of a validated state.
[59] 計画外の変更はとてもリスクがある。「修正」のテスト／実装の作業は、最初に本番環境で実施しないことが理想的である。バリデートされた本番システムに加える全ての変更は、会社の変更コントロール、構成管理、及びバリデーション手順のコントロールの対象とし、GMP への適合とバリデートされた状態の維持を確実にしなければならない。

DQ:	Design Qualification
EDP:	Electronic Data Processing
EU:	European Union
FDA:	US Food and Drug Administration
FS:	Functional Specification
GAMP:	Good Automated Manufacturing Practice
GCP:	Good Clinical Practice
GDP	Good Distribution Practice
GLP:	Good Laboratory Practice
GMP:	Good Manufacturing Practice
GxP:	Compliance requirements for all good practice disciplines in the regulated pharmaceutical sector supply chain from discovery to post marketing. 規制対象の製薬セクターにおける、新薬発見から市販後までのサプライチェーンの全グッドプラクティス領域における適合要件。
IEC:	International Electrical Commission
IEEE;	Institute of Electrical and Electronics Engineers, Inc.
IQ:	Installation Qualification
ISMS	Information Security Management System
ISO:	International Standards Organisation
ISPE	International Society for Pharmaceutical Engineering
LIMS:	Laboratory Information Management System
LAN:	Local Area Network
MRP:	Materials Requirements Planning
MRP-II:	Manufacturing Resource Planning
OQ:	Operational Qualification

PDA:	Parenteral Drug Association
PIC/S:	Pharmaceutical Inspection Co-operation Scheme
PKI	Public Key Infrastructure
PLC:	Programmable Logic Controller
PQ:	Performance Qualification
QMS:	Quality Management System
R&D:	Research and Development
SCADA:	Supervisory Control And Data Acquisition
SLA:	Service Level Agreement
SOPs:	Standard Operating Procedures
URS:	User Requirements Specification
VSR:	Validation Summary Report (see footnote to Section '23.10')
WAN:	Wide Area Network

脚注

文末脚注がページ内に収まらないものを以下に転記した。

51	An electronic keyword search of GxP documents will reveal specific compliance requirements to assist in preparing for particular topic inspections. Keywords such as: 'document', 'specification', 'formula', 'procedure', 'record', 'data', 'log book', 'instruction', 'written', 'sign', 'approve', 'writing', 'signature' are particularly helpful for records, data, documentation, authorisation and signature issues.	電子的に GxP 文書のキーワードを検索することにより、特定のトピックについて査察の準備に役立つ具体的な適合要件が見つかるであろう。「文書 (document)」、「仕様 (specification)」、「製法 (formula)」、「手順 (procedure)」、「記録 (record)」、「データ (data)」、「ログブック (log book)」、「指示 (instructions)」、「文書化 (written)」、「署名 (sign)」、「承認 (approve)」、「書面（writing）」、「署名 (signature)」といったキーワードは、特に記録、データ、文書、権限、及び署名に関する問題に有用であろう。

58	PIC/S Author's Note on 'Raw Data'- For information: FDA's 21 CFR Part 11 requires the retention of electronic records in electronic form (thus including raw data electronically captured or recorded). Also, for all good practice disciplines regulated by competent authorities it must be possible to reconstruct studies and reports from raw data and the electronic records may be needed to support any paper printouts.	生データに関する PIC/S の著者のメモ－参考情報：FDA 21 CFR Part 11 では、電子記録（すなわち電子的に収集又は記録された「生データ」を含む）の電子形式での保存を要求している。また、監督官庁が規制する全グッドプラクティス領域〔全 GxP 領域〕では、研究や報告を生データから再現できなければならず、紙の印刷物を裏付ける電子記録が必要となる場合がある。

【巻末訳注】

1. Annex 11

Annex 11 は 2011 年に大幅に改訂されている。
本書で参照されている改訂前の Annex 11 の項目を以下に示す。

Principle
Personnel
1. 要員の協力とトレーニング
Validation
2. バリデーションの実施
System
3. 設置環境
4. システム記述書
5. ソフトウェアの品質確保
6. データ入力／処理のビルトインチェック
7. テスト
8. データ入力／修正者の制限
9. 重要データ入力時の追加チェック
10. 監査証跡
11. 変更コントロール
12. 電子データの印刷
13. 電子データの保存
14. バックアップ
15. システム故障時の運用継続対策
16. システムフェイル時の対応手順
17. エラー発生時の対応手順
18. 外部業者の利用
19. バッチリリース

2. GAMP

本書で参照されている GAMP は ISPE から 2001 年に発行された GAMP 4 である。その後、ISPE は 2008 年に "GAMP 5 A Risk-Based Approach to Compliant GxP Computerized Systems" を発行している。
GAMP 4 の目次は https://www.ispe.gr.jp/ISPE/07_public/subwin07_01_02.html に示されている。

1 序　文
1.1 GAMP 活動開始の経緯
1.2 サプライヤ向けガイダンス

3. PMA CSVC

Pharmaceutical Manufacturers Association の Computer System Validation Committee 。1980 年代から 1990 年代にかけて CSV について先導的な役割を果たした。1990 年代に解散した。