OECD SERIES ON PRINCIPLES OF GOOD LABORATORY PRACTICE AND COMPLIANCE MONITORING
Number 17

Advisory Document of the Working Group on Good Laboratory Practice

Application of GLP Principles to Computerised Systems

GLP 原則及び適合性モニタリングに関する OECD シリーズ

No.17

GLP 原則のコンピュータ化システムへの適用

英文・和訳 対比表

日本 QA 研究会 GLP 部会 第 3 分科会

22-Apr-2016 OECD SERIES ON PRINCIPLES OF GOOD LABORATORY PRACTICE AND COMPLIANCE MONITORING Number 17 Advisory Document of the Working Group on Good Laboratory Practice Application of GLP Principles to Computerised Systems JT03394591	2016 年 4 月 22 日 GLP 原則及び適合性モニタリングに関する OECD シリーズ No.17 GLP 作業部会アドバイサリー文書 GLP 原則のコンピュータ化システムへの適用 JT03394591
FOREWORD The OECD Working Group on Good Laboratory Practice, at its 26th meeting in 2012, established a drafting group under the leadership of Austria's Federal Office for Safety in Health Care (Rd. Ronald BAUER) to update the 1995 OECD GLP Consensus Document number 10 - The Application of the Principles of GLP to Computerised Systems. The drafting group included representatives from Austria, Belgium, Ireland, Italy, Switzerland, the UK and the US EPA. The following Advisory Document replaces the 1995 consensus document. It retains all of the key text from the original Consensus Document number 10, but includes new text to reflect the current state-of-the art in this field. This draft Advisory Document was posted on the GLP public web site on 17 September, 2014 and members of the public were invited to comment by 14 November 2014. This document reflects those comments. This document is published under the responsibility of the Joint Meeting of the Chemicals Committee and the Working Party on Chemicals, Pesticides and Biotechnology of the OECD.	序文 OECD GLP 作業部会は 2012 年の第 26 回会合において、オーストリアの連邦医療安全局（Federal Office for Safety in Health Care（Rd. Ronald BAUER））の指揮の下、1995 年 OECD GLP コンセンサス文書 No. 10、「GLP 原則のコンピュータ化システムへの適用」を更新するための原案検討グループを設置した。この原案検討グループにはオーストリア、ベルギー、アイルランド、イタリア、スイス、イギリス及び米国 EPA の代表者が加わった。 以下のアドバイサリー文書は 1995 年のコンセンサス文書と差し替えられる。オリジナルのコンセンサス文書No. 10 の主要テキストは全てそのまま採用しているが、この分野における最新技術を反映させるために新たなテキストを盛り込んでいる。本アドバイサリー文書草案は 2014 年 9 月 17 日に GLP の公開ウェブサイトで発表され、2014 年 11 月 14 日まで一般からのコメントを募集した。本書はこうしたコメントを反映している。 本書は OECD の化学品委員会及び化学品・農薬・バイオ技術作業部会合同会合の責任の下に発表される。

TABLE OF CONTENTS	目次

1. PREAMBLE	**1. 前文**
1. This document introduces a life cycle approach to the validation and operation of computerised systems. It emphasises risk assessment as the central element of a scalable, economic and effective validation process with a focus on data integrity. The intention of this document is to provide guidance that will allow test facilities to develop an adequate strategy for the validation and operation of any type of computerised system, regardless of its complexity, in a GLP environment.	1. 本書はコンピュータ化システムのバリデーション及び運用に関するライフサイクルアプローチを紹介するものである。データの完全性に焦点を絞ったスケーラブルで経済的かつ効果的なバリデーションプロセスの中心的要素としてリスクアセスメントに重点を置いている。本書の意図しているところは､GLP環境下において、試験施設が、システムの複雑さに関係なく、あらゆる種類のコンピュータ化システムのバリデーションと運用の適切な戦略を策定できるような手引きとなることである。
1.1. Scope and definition of terms 2. Relevant terms are defined in the Glossary in Appendix 2.	**1.1. 範囲及び用語の定義** 2. 関係用語は別紙2の用語解説において定義される。

1.1.1. Computerised System	**1.1.1. コンピュータ化システム**
3. This guidance applies to all types of computerised systems used in GLP regulated activities regardless of their complexity (ranging from simple devices like balances to more complex devices such as stand-alone PCs controlling lab-based instruments and complex systems like laboratory information management systems). The computerised system consists of hardware, software, and interfaces to its operating environment. Hardware consists of the physical components of the computerised system; it includes the computer unit itself and its peripheral components. Software is the program or programs that control the operation of the computerised system. All GLP Principles that apply to equipment therefore apply to both hardware and software. During the planning, conduct, reporting and archiving of studies, there may be several computerised systems in use for a variety of purposes. Such purposes might include the direct or indirect capturing of data from automated instruments, operation/control of automated equipment and the processing, reporting and storage of data. Consequently there should be appropriate procedures to control, maintain and operate computerised systems.	3. 本ガイダンスは、当該システムの複雑さに関係なく（天秤のような単純な装置から、試験室で使用される機器を制御するスタンドアロンPC などのより複雑な装置や、ラボ情報管理システム（LIMS）のような複雑なシステムに至るまで）、GLP の対象となる活動において使用される、あらゆる種類のコンピュータ化システムに適用される。コンピュータ化システムは、ハードウェア、ソフトウェア、そしてその運用環境へのインターフェースで構成される。ハードウェアはコンピュータ化システムの物理的構成要素から成り、コンピュータ装置自体と周辺機器が含まれる。ソフトウェアはコンピュータ化システムの動作を制御する単体又は複数のプログラムである。したがって、機器に適用される全ての GLP 原則はハードウェアとソフトウェアの両方に適用される。試験の計画から実施、報告及びアーカイブまでの間に、複数のコンピュータ化システムが様々な目的で使用される可能性がある。このような目的には、自動化装置からの直接又は間接的なデータ取込み、自動化装置の操作／制御、データの処理、報告及び保存などが含まれるだろう。それゆえにコンピュータ化システムのコントロール、保守、運用のための適切な手順が設けられるべきである。

1.1.2. Validation 4. The demonstration that a computerised system is suitable throughout its life cycle for its intended purpose is of fundamental importance and is referred to as computerised systems validation. All computerised systems used for the generation, measurement, calculation, assessment, transfer, processing, storage or archiving of data intended for regulatory submission or to support regulatory decisions should be validated, and operated and maintained in ways that are compliant with the GLP Principles. The same requirement also applies to computerised systems used to produce other GLP-relevant data such as records of raw data, environmental conditions, personnel and training records, maintenance documentation, etc. The process a computerised system performs should be reliable and fit for purpose. The validation process must provide a high degree of assurance that a computerised system meets its pre-determined specifications. Validation should be undertaken by means of a formal validation plan and performed prior to operational use.	**1.1.2. バリデーション** 4. コンピュータ化システムがそのライフサイクル全体にわたって意図された目的に適ったものであるということの立証は根本的に重要なことであり、これはコンピュータ化システムのバリデーションと呼ばれる。規制当局への申請を目的とするデータの生成、測定、計算、評価、転送、処理、保存又はアーカイブのために、あるいは規制対応のための決定をサポートするために使用される全てのコンピュータ化システムは、GLP原則を遵守した方法でバリデートされ、運用され、保守されるべきである。生データ、環境条件、担当者及び教育訓練の記録、保守管理文書など、他のGLP関連データを作成するときに用いられるコンピュータ化システムにも同じ要件が適用される。コンピュータ化システムによって行われるプロセスは信頼でき、目的に適っているべきである。バリデーションプロセスは、コンピュータ化システムがあらかじめ定められた仕様に適合していることを高度に保証するものでなければならない。バリデーションは正式なバリデーション計画書を用いて行い、運用開始前に実施するべきである。
5. Validation of newly established computerised systems should be done prospectively. Depending on the size, criticality and novelty of the system, testing should be performed if possible in a dedicated validation environment before transfer into the laboratory environment. It must be ensured that the validation environment is equivalent to the laboratory environment for appropriate simulation. Appropriate change control should be applied throughout the system's life cycle including its retirement.	5. 新たに設置されるコンピュータ化システムのバリデーションはプロスペクティブに行うべきである。システムの規模、重要度、新規性に応じて判断するべきだが、可能であれば試験室環境に移す前に専用のバリデーション環境でテストを行うべきである。適切にシミュレーションできるよう、バリデーション環境は試験室環境と同等であることが担保されなければならない。廃止も含め、システムのライフサイクル全体にわたって適切な変更管理を行うべきである。

6. Retrospective validation is not permitted unless the scope of use has changed or an existing system has become GLP-relevant (e.g., the need for compliance with the GLP Principles was not foreseen or specified). Where this occurs there should be a documented justification prior to the use of the system in a GLP study. This should involve a retrospective evaluation to assess suitability that begins with gathering relevant historical records related to the computerised system. These records should be reviewed and a written summary should be produced. This retrospective summary should specify what evidence is available and what additional requirements must be tested during formal acceptance testing to achieve the validated status.	6. レトロスペクティブなバリデーションは、使用範囲が変更されたか、既存システムが GLP 関連システムになった場合（例えば、GLP 原則遵守の必要性が予測若しくは指定されていなかった場合）でない限り、認められない。このような場合には、GLP 試験で当該システムを使用する前に、正当性を文書化するべきである。正当化のために、当該コンピュータ化システムに関するこれまでの関連記録の収集から始まるレトロスペクティブな適合性の評価を行うべきである。これらの記録についてレビューし、要約文書を作成するべきである。このレトロスペクティブな評価の要約においては、どのようなエビデンスが揃っているのか、また、どのような追加要件が、バリデートされた状態となるための正式な受入テストにおいて検証されなければならないかを明記するべきである。
1.1.3. Qualification 7. Formal qualification rather than validation may be acceptable for Commercial Off-The-Shelf systems (COTS), automated equipment of low complexity or small systems. Due to its extensive use, validity of the incorporated software can be assumed in cases where no customisation is performed. Reference is made to respective guidance from the Good Manufacturing Practice (GMP) area, as e.g. Annex 15 of the EU Guidelines for Good Manufacturing Practice for Medicinal Products for Human and Veterinary Use, regarding “Qualification and Validation.”	**1.1.3. 適格性評価** 7. 市販の既製品システム（COTS）、複雑さの低い自動化装置又は小規模システムについてはバリデーションよりも正式な適格性評価の方が手段として良い場合がある。内蔵ソフトウェアについては広範に使用されることから、カスタマイズが行われていない場合にはその正当性を仮定することができる。例えば「適格性評価及びバリデーション」については、Good Manufacturing Practice（GMP）分野の個別のガイダンス（例えば、ヒト用及び動物用医薬品の GMP に関する EU ガイドライン アネックス 15 など）が参考になる。
8. Examples of low complexity COTS, automated equipment or small systems may be: analytical equipment such as electronic pipettes, balances, photometers and storage devices like refrigerators, freezers, etc.	8. 複雑さの低い COTS、自動化装置ないし小規模システムの例として以下のものが挙げられる：電子ピペット、天秤、光度計などの分析装置、及び冷蔵庫、冷凍庫のような保存機器など。

9. Test facility management must decide and define criteria for when to apply computerised system validation and/or qualification approaches. A risk based approach should be applied to define critical process parameters and the actions used to monitor each process to ensure it remains in a state of control throughout the life cycle of the computerised system. Therefore it is expected that stringent calibration and maintenance measures are in place, along with the use of internal references or standards with strict pre-defined specifications. Application of statistical process control tools (e.g., control charts) are recommended and long term traceability of monitoring results is expected. Special focus and monitoring is expected with regard to the control of data flow where interfaces to other systems are established. Standard procedures shall be in place that clearly describe defined process and control steps.	9. 運営管理者は、コンピュータ化システムのバリデーション及び／又は適格性評価アプローチを適用する時期に関する基準を決定し、定義しなければならない。コンピュータ化システムのライフサイクルを通して、コントロールされた状態が確実に維持されるために、重要なプロセスパラメータ及び各プロセスのモニターに用いる措置を定めるときには、リスクベースアプローチを適用するべきである。したがって、事前に規定された厳格な仕様に従った内部基準ないし標準の使用とともに、厳密な校正及び保守方法の整備が期待される。統計的プロセスコントロールツール（例えば、コントロールチャート）の適用が推奨され、モニタリング結果の長期にわたるトレーサビリティが期待される。他のシステムとインターフェースを介して接続されている場合には、データフローの制御に特別に焦点を当ててモニタリングすることが期待される。特定のプロセス及び管理手順を明確に記した標準手順書を配置するべきである。
10. Re-qualification activities should be performed based on pre-defined time periods taking into account identified risks. The qualification approach should be detailed in procedures.	10. 適格性再評価活動は、特定されたリスクに応じて事前に定めた時期に行うべきである。適格性評価アプローチを手順書で詳しく説明するべきである。
11. Existing qualification plans and reports may be referenced when multiple examples of the same equipment are used within the test facility.	11. 試験施設内で複数の同じ装置を使用するときには既存の適格性評価計画や報告書を参照することができる。

1.1.4. Life cycle 12. The validation approach should be risk-based and test facility management has the freedom to choose any appropriate life cycle model. It should ensure validation activities are defined and performed in a systematic way from conception, understanding the requirements, through development, release, operational use, to system retirement. All relevant phases of the life cycle should be documented and defined. This may include the purchase, specification, design, development and testing, implementation, operation and retirement of computerised systems. Life cycle activities should be scaled based on documented risk assessment. Minimal activities may be required for simple processes like weighing on a stand-alone balance; more extensive activities might be required for complex systems like interfaced laboratory information management systems.	**1.1.4. ライフサイクル** 12. バリデーションアプローチはリスクベースとするべきであるが、運営管理者は適切なライフサイクルモデルを自由に選択できる。構想、要件についての理解から開発、リリース、実運用での使用、そしてシステム廃止に至るまで、バリデーション活動を定義し、体系的に実施することを確実にするべきである。ライフサイクルに関連する全ての段階は文書化して定義するべきである。段階としては、コンピュータ化システムの調達、仕様定義、設計、開発及びテスト、実装、運用そして廃止などがあるだろう。ライフサイクル活動の規模は文書化されたリスクアセスメントに基づいて決めるべきである。スタンドアロンの天秤で計量するような単純なプロセスの場合は最小限の活動で構わないだろう。インターフェースを介して接続される LIMS（試験室情報管理システム）のような複雑なシステムの場合は、より広範な活動が必要になるかもしれない。
1.2. Risk management 13. Risk management should be applied throughout the life cycle of a computerised system taking into account the need to ensure data integrity and the quality of the study results. Risk management consists of risk identification, risk assessment, risk mitigation and risk control. Decisions on the extent of validation and data integrity controls should be based on a documented rationale and documented risk assessment. Risk management should link to other relevant procedures (e.g. configuration and change management, management processes for data, business risks, etc.).	**1.2. リスクマネジメント** 13. データの完全性と試験結果の質を確保する必要性を考慮して、リスクマネジメントをコンピュータ化システムのライフサイクル全体にわたって適用するべきである。リスクマネジメントは、リスク特定、リスクアセスメント、リスク軽減及びリスクコントロールから成る。バリデーションの範囲及びデータの完全性をコントロールする範囲に関する決定は文書化された合理的根拠と文書化されたリスクアセスメントに基づくべきである。リスクマネジメントは他の関係手順（例えば、構成マネジメントと変更マネジメント、データとビジネスリスクなどの管理手順）と結び付けるべきである。

14. Risk assessment should be used to develop an adequate validation strategy and to scale the validation efforts. The validation effort should be driven by the intended use of the system and potential risks to data quality and data integrity. The outcome of the risk assessment process should result in the design of appropriate validation activities for computerised systems or computerised system functionalities. The appropriate use of risk assessments is of paramount importance for an effective and efficient validation approach. If risk assessment outcomes are appropriately used they will provide test facility management with an adequate methodology to validate both simple laboratory systems as well as complex laboratory data management systems.	14. 適切なバリデーション戦略を策定し、バリデーション作業の規模を決めるためにリスクアセスメントを実施するべきである。バリデーション作業は、システムの使用目的とデータの品質及びデータの完全性に対する潜在的リスクに基づいて決定するべきである。リスクアセスメントプロセスの結果が、コンピュータ化システム又はコンピュータ化システムの機能にとって適切なバリデーション活動の設計につながるべきである。リスクアセスメントの適切な利用は効果的かつ効率的なバリデーションアプローチにとって最も重要である。リスクアセスメントの結果が適切に利用されれば、運営管理者は、単純なラボシステムと複雑なラボデータ管理システムの両方をバリデートするのに用いることができる適切な方法論を見出すことができるだろう。
15. Risk assessment of computerised systems that are used both for GLP-studies and non-GLP studies should include any potential impact of non-GLP activities on GLP compliant activities. The same requirements for validation apply for such systems as for computerised systems that are used exclusively in GLP studies. There should be a clear differentiation of GLP data from non-GLP data.	15. GLP 試験及び非 GLP 試験両方に使用されるコンピュータ化システムのリスクアセスメントには、GLP を遵守した活動に対する非 GLP 活動が及ぼすあらゆる潜在的影響も含めるべきである。このようなシステムに関しては、GLP 試験専用に使用されるコンピュータ化システムに関するものと同じバリデーション要件が適用される。GLP データと非 GLP データは明確に区別されるべきである。

1.3. Personnel, roles and responsibilities 16. The GLP Principles require that a test facility or a test site have appropriately qualified and experienced personnel and that there are documented task specific training programmes including both on-the-job training and, where appropriate, attendance at external training courses. Records of all such training should be maintained. The same provisions also apply for all personnel involved with computerised systems. Tasks and responsibilities of test facility management, quality assurance, study director and study personnel that use or maintain computerised systems should be defined and described.	**1.3. 担当者、役割、責任** 16. GLP 原則では、試験施設ないし試験場所には適切な資格を有する経験豊富な者を置き、OJT と、必要に応じて外部研修コースへの参加も含む、職務に応じた教育訓練プログラムを文書化することを義務付けている。このような教育訓練の記録は全て保存されるべきである。コンピュータ化システムの関係者全員についても同じ規定が適用される。コンピュータ化システムを使用又は保守管理する運営管理者、信頼性保証部門、試験責任者及び試験従事者の任務と責任を定義して記述するべきである。
17. To validate a system and to operate a validated system, there should be close cooperation between all relevant personnel if possible such as the test facility management, the study director, quality assurance personnel, IT personnel and validation personnel. All personnel should have appropriate qualifications and be provided with appropriate levels of access and defined responsibilities to carry out their assigned duties.	17. システムのバリデーションを行い、バリデートされたシステムを運用するためには、運営管理者、試験責任者、信頼性保証担当者、IT 担当者、バリデーション担当者など、可能であれば全ての関係者間で緊密に協力するべきである。全ての担当者は適切な資格を有しており、適切なレベルのアクセス権限が与えられ、割り当てられた任務を遂行する責任が規定されているべきである。
18. Personnel who validate, operate and maintain computerised systems are responsible for performing their activities in accordance with the GLP Principles and best practice guidance and standards (see "References" in Chapter 5 below).	18. コンピュータ化システムのバリデーション、運用及び保守を行う者は GLP 原則やベストプラクティスガイダンス及び基準に従って活動を行う責任を負う（下記第 5 章の「参考文献」参照）。
19. During validation of computerised systems and the conduct of GLP studies, roles and responsibilities should be defined and controlled via system access privileges, training and general GLP requirements. Training records and system access authorisations of users should be available and demonstrate that personnel have sufficient knowledge and access rights to fulfill their respective roles in a GLP compliant manner.	19. コンピュータ化システムのバリデーション及び GLP 試験の実施においては、役割と責任を明確にし、システムアクセス権、教育訓練及び一般的な GLP 要件を通じて管理するべきである。ユーザの教育訓練記録及びシステムアクセス許可を確認できるようにしておき、これらは担当者が GLP に適合した方法で各自の役割を果たすための十分な知識とアクセス権を有していることの立証となっているべきである。

20. Relevant contracts or service level agreements should detail GLP training requirements for global or corporate IT teams or for external and internal IT service providers who may work in accordance with quality management systems other than GLP.	20. 関連する契約書ないしサービスレベルアグリーメントにおいては、GLP 以外の品質マネジメントシステムに従って作業をする可能性のある、グローバルないし企業 IT チーム、あるいは内外の IT サービスプロバイダ向けの GLP 教育訓練要件を詳述するべきである。
21. Roles and Responsibilities are described in Appendix 1.	21. 役割及び責任については別紙 1 に記す。
1.3.1. Test facility management 22. Test facility management has overall responsibility to ensure that the facilities, equipment, personnel and procedures are in place to achieve and maintain validated computerised systems.	**1.3.1. 運営管理者** 22. 運営管理者は、バリデートされたコンピュータ化システムを実現し､維持するための設備、機器、担当者及び手順書が確実に揃っていることに全般的責任を負う。
23. This includes: a) the responsibility to establish procedures to ensure that computerised systems are suitable for their intended purpose and are operated and maintained in accordance with the Principles of GLP; b) the appointment and effective organisation of an adequate number of appropriately qualified and experienced staff; and c) the obligation to ensure that the facilities, equipment and data handling procedures are of an adequate standard.	23. この責任には以下のことが含まれる。 a) コンピュータ化システムが意図した目的に適ったものであり、GLP 原則に従って運用され､保守管理されることを確実にするための手順を確立する責任 b) 十分な人数の適切な資格を有する経験豊富な者の任命と効果的な組織化 c) 設備、機器及びデータを取り扱う手順が十分な水準のものであることを確保する義務
24. Test facility management should ensure that procedures required to achieve and maintain the validated status of computerised systems are understood and followed, and ensure that effective monitoring of compliance occurs.	24. 運営管理者は、コンピュータ化システムをバリデートされた状態にしてこれを維持するために必要な手順が確実に理解され、守られること、また、法令遵守状況の効果的なモニタリングが確実に行われるようにするべきである。

25. Test facility management should designate personnel with specific responsibility for the development, validation, operation and maintenance of computerised systems. Such personnel should be suitably qualified, with relevant experience and appropriate training to perform their duties in accordance with the GLP Principles.	25. 運営管理者はコンピュータ化システムの開発、バリデーション、操作及び保守管理に対する特定の責任を負う者を指名するべきである。このような者は適切な資格を有し、GLP 原則に従って任務を遂行するための当該経験を有し、適切な教育訓練を受けているべきである。
26. It is the overall responsibility of the local test facility management to ensure that computerised systems provided within a wider company are operated and maintained locally in accordance with the Principles of GLP. Written agreements between the local test facility management and the parent organisation should clearly assign responsibilities for validation and maintaining the validated status and GLP compliant operation of computerised systems. Test facility management can delegate responsibilities fully or partly at an individual system level or collectively to adequately trained personnel (e.g. the overall responsibility for GLP compliance of computerised systems to a system owner or for a specific computerised system to a validation director).	26. 会社内で広く使用されるコンピュータ化システムが当該施設で GLP 原則に従って運用され保守管理されることを確実にすることは、当該施設の運営管理者の全般的責任である。当該施設の運営管理者と親組織との間の合意書は、バリデーション並びにコンピュータ化システムのバリデートされた状態及び GLP に適合した運用の維持に対する責任分担を明確に定めたものにするべきである。運営管理者は個別のシステム単位で、あるいはまとめて、適切に訓練を受けた者に責任の全部又は一部を委譲することができる（例えば、コンピュータ化システムの GLP 適合に対する全般的責任をシステムオーナに委譲する、あるいは特定のコンピュータ化システムに関してバリデーション責任者に委譲する）。
27. The test facility management should define roles and responsibilities for both validation activities and the routine operation of each computerised system regardless of its level of complexity. Potential conflicts of interest associated with roles and responsibilities should be considered to avoid risks to data integrity (e.g. analytical personnel should not be in control of the audit trail settings of the system they are working with).	27. 運営管理者は、その複雑さの程度に関係なく、各コンピュータ化システムのバリデーション活動と日常的操作の両方について役割と責任を定義するべきである。データの完全性に対するリスクを避けるために、役割及び責任に関係する潜在的な利益相反を考慮するべきである（例えば、分析担当者は自らが使用しているシステムの監査証跡の設定内容を管理するべきではない）。

1.3.2. Study Director 28. The study director is responsible for the overall conduct and GLP compliance of the studies. The study director has the responsibility to ensure that all computerised systems used in the studies are validated and used appropriately. The study director's responsibility for electronic data is the same as that for data recorded on paper (data should be attributable, legible, contemporaneous, original, accurate, complete, consistent, enduring, and available). Before the initiation of a GLP study, confirmation of the validation status of all the computerised system(s) that will be used should be verified by the study director.	**1.3.2. 試験責任者** 28. 試験責任者は試験の実施全般と GLP 適合に対する責任を負う。試験責任者は、試験で使用される全てのコンピュータ化システムが適切にバリデートされ、使用されることを確実にする責任を有する。電子データに関する試験責任者の責任は紙に記録されるデータに関するものと同じである（データは帰属が明確で、判読可能で、同時性があり、原本であり、正確で、完全なもので、一貫しており、恒久的なものであり、利用可能であること）。GLP 試験の開始前に、使用される全てのコンピュータ化システムのバリデーション状態が試験責任者によって確認されるべきである。
1.3.3. Quality assurance 29. Quality assurance personnel should be aware of GLP-relevant computerised systems at their test facility or test site. Quality assurance responsibilities for computerised systems should be defined by test facility management and described in written procedures. Quality assurance should be able to verify the valid use of computerised systems. The quality assurance program should include procedures and practices that verify if established standards are met for all phases of a system's life cycle. Tasks to verify standards in validation, operation and maintenance of computerised systems may be delegated to experts or specialist auditors (e.g. system administrators, system owners, external experts etc.). Quality assurance personnel should be provided with an appropriate level of training and access to allow them to inspect specific computer processes if needed (audit trail reviewing, data analysis techniques, etc.). During inspections of studies, quality assurance personnel should have direct read-only access to the data if it is only available within a computerised system.	**1.3.3. 信頼性保証部門** 29. 信頼性保証担当者はその試験施設又は試験場所にある GLP 関連のコンピュータ化システムについて認識しておくべきである。コンピュータ化システムに関する信頼性保証部門の責任は運営管理者によって規定され、手順書に記されているべきである。信頼性保証部門はコンピュータ化システムが正当に使用されていることを確認できるべきである。信頼性保証プログラムには、システムのライフサイクルの全段階において設定基準が満たされているかどうかを検証する手順及び実施基準を盛り込むべきである。コンピュータ化システムのバリデーション、運用及び保守管理における基準を検証する作業は専門家ないしは専門調査者（例えば、システムアドミニストレータ、システムオーナ、外部専門家など）に委託しても構わない。信頼性保証担当者には、必要に応じて特定のコンピュータプロセスを調査できるように、適切な水準の教育訓練を受けさせ、アクセス権を与えるべきである（監査証跡レビュー、データ分析技術など）。試験の調査時、信頼性保証担当者は、コンピュータ化システム内でのみ閲覧可能なデータに対しては、読取り専用で直接アクセスする権限を持っているべきである。

30. Study directors and quality assurance personnel should have sufficient training to understand the relevant procedures in adequate use of GLP-relevant computerised systems.	30. 試験責任者及び信頼性保証担当者はGLP関連のコンピュータ化システムの適切な使用に関連する手順を理解できるだけの十分な教育訓練を受ける必要がある。
1.4. Facility 31. Due consideration should be given to the physical location of computer hardware, peripheral components, communications equipment and electronic storage media. Extremes of temperature and humidity, dust, electromagnetic interference and proximity to high voltage cables should be avoided unless the equipment is specifically designed to operate under such conditions.	**1.4. 施設** 31. コンピュータハードウェア、周辺機器、通信装置及び電子記録媒体の設置環境について十分に配慮するべきである。極端な温度や湿度、埃、電磁干渉及び高圧線との近接を避けるべきである。ただし、装置がこのような条件下で作動するように特別に設計されている場合にはこの限りではない。
32. Consideration must also be given to the electrical supply for computer equipment and, where appropriate, back-up or uninterruptable supplies for computerised systems whose sudden failure would affect the results of a study. Adequate facilities should be provided for the secure retention of electronic storage media.	32. 突発的な障害が試験結果に影響を及ぼす恐れのあるコンピュータ化システムについては、コンピュータ機器の電力供給、必要に応じて、バックアップないし無停電電源装置についても配慮しなければならない。電子記録媒体を安全に保持するために適切な施設が用意されるべきである。
1.5. Inventory 33. An up-to-date listing (inventory) of all GLP-relevant computerised systems and their functionality should be maintained. The list should cover all GLP-relevant computerised systems, regardless of their complexity. Computerised systems used in GLP studies should be traceable from the study plan or relevant method to the inventory. The inventory should contain the validation status, make, model or version as relevant, and business process owner and IT system owner (persons who have responsibility or accountability for the system).	**1.5. インベントリ** 33. 全てのGLP関連のコンピュータ化システムとその機能について、最新の一覧表（インベントリ）を維持するべきである。その複雑さに関係なく、全てのGLP関連のコンピュータ化システムを網羅するべきである。GLP試験で使用されるコンピュータ化システムは、試験計画書ないし当該試験方法からインベントリのシステムが紐づけられるようにするべきである。インベントリには当該システムのバリデーション状態、製造元、型式又はバージョン、並びにビジネスプロセスオーナ及びITシステムオーナ（システムに対して責任又は説明責任を負う者）が記載されているべきである。

1.6. Supplier 34. When suppliers (e.g. third parties, vendors, internal IT departments, service providers including hosting service providers) are used to provide, install, configure, integrate, validate, maintain, modify decommission or retain a computerised system or for services such as data processing, data storage, archiving or cloud services, then written agreements (contracts) should exist between the test facility and the supplier. These agreements should include clear statements outlining the responsibilities of the supplier as well as clear statements about data ownership.	**1.6. サプライヤ** 34. サプライヤ（例えば、サードパーティ、ベンダー、内部 IT 部門、ホスティングサービスプロバイダを含むサービスプロバイダ）を利用してコンピュータ化システムの用意、設置、構成設定、統合、バリデーション、保守管理、変更、運転停止又は保持を行う場合、あるいはデータ処理、データ保存、アーカイブ又はクラウドサービスなどのサービスのために利用する場合、試験施設とサプライヤとの間には書面での合意（契約書）が存在するべきである。こうした合意書にはサプライヤの責任を明確に記載すると同時にデータ所有権についても明記するべきである。
35. The competence and reliability of a supplier should be evaluated by test facility management. The need for, and extent of, vendor assessment should be based upon a risk assessment taking into account the complexity of the computerised system and the criticality of the business process supported by the computerised system. The need for an audit should be based on a documented risk assessment. It is test facility management's responsibility to justify the requirement for and type of audit based on risk.	35. サプライヤの能力と信頼性は運営管理者によって評価されるべきである。ベンダー評価の必要性、並びにその程度は、コンピュータ化システムの複雑さとコンピュータ化システムによってサポートされるビジネスプロセスの重要度を考慮して、リスクアセスメントに基づくものにするべきである。 調査/監査の必要性は文書化されたリスクアセスメントに基づいたものとするべきである。リスクに基づいて調査/監査の要件と種類を正当化するのは運営管理者の責任である。
36. If the evaluation scope includes a technical as well as compliance focus, the involvement of specialist technical personnel as well as quality assurance personnel should be considered. Test facility management should be able to provide inspectors with information about the quality systems of suppliers depending on the services they are providing. Suppliers do not need to conform to GLP regulations, but must operate to a documented quality system verified as acceptable by test facility management with input from the quality assurance unit.	36. 評価範囲に法令遵守の問題と同様に技術的問題も含まれる場合、信頼性保証担当者とともに専門的技術担当者の関与を考慮するべきである。運営管理者は、提供されるサービスに応じてサプライヤの品質システムに関する情報を調査官に提供できるようにするべきである。サプライヤは GLP 規制に従う必要はないが、信頼性保証部門から得た情報を基に運営管理者が容認可能とした、文書化された品質システムに合わせて活動しなければならない。

37. For vendor-supplied systems, it is likely that much of the documentation created during the development is retained at the vendor's site. If documentation is retained at the vendor's site, test facility management should ensure it is securely stored. This may require a formal contract between the vendor and the test facility. In this case, evidence of a formal assessment and/or vendor audits should be available at the test facility. Formal acceptance testing by the test facility of vendor-supplied systems is required.	37. ベンダーから供給されるシステムの場合、開発時に作成された資料の多くはベンダー側で保持される可能性が高い。資料がベンダー側で保持される場合、運営管理者は資料が安全に保存されることを確実にするべきである。このためにはベンダーと試験施設の間で正式な契約を結ぶ必要があるだろう。この場合、正式な評価及び／又はベンダーオーディットのエビデンスを試験施設で確認できるようにするべきである。ベンダーから供給されるシステムについては試験施設による正式な受入テストが必要である。
38. Test facility management should define in written agreements the interfaces between its validation procedures and any activities provided by a supplier. Such interfaces should be applicable to the validation phase and to the operational phase. For example, any testing activities performed by a supplier should be evaluated by the test facility management.	38. 運営管理者は合意書において、そのバリデーション手順とサプライヤによる活動の接点について定義するべきである。このような接点はバリデーション段階及び運用段階に適用できるようにするべきである。例えばサプライヤによって行われるいずれのテストも運営管理者によって評価されるべきである。
39. Hosted services (e.g. platform, software, data storage, archiving, backup or processes as a service) should be treated like any other supplier service and require written agreements describing the roles and responsibilities of each party. It is the responsibility of test facility management to evaluate the relevant service and to estimate risks to data integrity and data availability. Test facility management should be aware of potential risks resulting from the uncontrolled use of hosted services.	39. ホスティングサービス（例えば、プラットフォーム、ソフトウェア、データ保存、アーカイブ、バックアップ又はサービスとしての一連の作業）は他のあらゆるサプライヤサービスと同様に扱われるべきであり、各当事者の役割と責任を記述した合意書を必要とする。関連するサービスを評価し、データの完全性やデータの利用可能性に対するリスクを見積もるのは運営管理者の責任である。運営管理者は、ホスティングサービスの制御されていない利用によって生じる潜在的リスクについて認識しておくべきである。
40. A test facility may include the company's IT department as a part of its GLP facility. In such cases they must have a reporting line to test facility management.	40. 試験施設にはGLP施設の一部として会社のIT 部門が含まれる場合もある。このような場合、IT 部門は、運営管理者に報告する仕組みを持たなければならない。

1.7. Commercial Off-The-Shelf products (COTS) 41. A computerised system may fully or partially rely on COTS products. COTS products may be used without modification, with limited configuration, with heavy configuration or even customised coding. As with any other type of software, COTS products require appropriate validation depending on the risk and the complexity of any customisation. If an application (e.g. a spreadsheet) is not complex, it might be sufficient to verify functions against user requirement specifications.	**1.7. 市販の既製品（COTS）** 41. コンピュータ化システムは COTS 製品に完全に、あるいは部分的に依存することもある。COTS 製品は変更を加えることなく使用される場合もあれば、限定的な構成設定の場合、大掛かりな構成設定の場合、あるいはコーディングをカスタマイズして使用される場合もある。他のあらゆる種類のソフトウェアと同様、COTS 製品もリスクとカスタマイズの複雑さに応じて適切なバリデーションを要する。アプリケーション（例えば、スプレッドシート）が複雑なものでなければ、ユーザ要求仕様書に照らして機能を確認するだけで十分かもしれない。
42. User requirement specifications should be written for any application that is based on a COTS product. Documentation supplied with a Commercial Off-The-Shelf (COTS) product should be verified by test facility management to ensure it is able to fulfill user requirement specifications.	42. ユーザ要求仕様書は COTS 製品をベースにするあらゆるアプリケーションに関して作成するべきである。市販の既製品（COTS）とともに提供される資料は、ユーザ要求仕様を満たせることを確実にするために運営管理者によって確認されるべきである。
43. Spreadsheet templates for calculations using pre-defined formulas, self-written equations, or macros should be regarded as in-house developed applications. The validation requirements for these are described in sections 2 and 3 and will depend on risk and complexity. The underlying COTS product will require an appropriate form of qualification and documentation. Qualification of the underlying COTS product alone is not sufficient.	43. 製品にあらかじめ組み込まれた数式、自作の数式、又はマクロを使用した計算処理のためのスプレッドシートテンプレートは自社開発アプリケーションとみなすべきである。これらに関するバリデーション要件は 2 及び 3 のセクションに記載されており、リスクと複雑さに依存する。ベースになる COTS 製品は適切な形式の適格性評価と文書化が必要となる。ベースになる COTS 製品の適格性評価だけでは不十分である。

1.8. Change and configuration control	**1. 8. 変更管理と構成管理**
44. Any changes to a computerised system should be made in a controlled manner and in accordance with written change control procedures. Change control procedures should cover the validation phase, the operational phase (including archiving) and the phase in which the system is retired. Test facility management should define roles and responsibilities of those involved with change control activities. Decisions on change control requirements should be risk based and will depend on the complexity and criticality of the change to data integrity or the business processes supported by the computerised system. Risk assessment used in change control can utilise software categorisation as described in current ISPE[1] GAMP[2] guidance.	44. コンピュータ化システムに加えられるいずれの変更も、コントロールされた方法で、変更管理手順書に従って行われるべきである。変更管理手順はバリデーション段階、運用段階（アーカイブを含む）並びにシステムの廃止段階に適用されるべきである。運営管理者は変更管理活動に関与する者の役割と責任を定義するべきである。変更管理要件に関する決定はリスクベースでなされるべきで、またデータの完全性又はコンピュータ化システムによってサポートされるビジネスプロセスに対する変更の複雑さと重要度に依存する。変更管理において利用されるリスクアセスメントでは ISPE[1] の最新版 GAMP[2] ガイダンスに記載されるソフトウェア分類を利用することができる。
45. Change control should cover any item that undergoes review, approval and testing and that is relevant for a defined configuration of a computerised system. It should ensure that a system's configuration is accurately described and documented at all times. Study specific activities (e.g. data capturing, data calculation, etc.) should be traceable to a specific configuration of the computerised systems if the configuration is relevant for the results. Change control should be interfaced with risk assessment, testing, release and adequate documentation procedures.	45. 変更管理は、レビュー、承認及びテストに関わる項目並びにコンピュータ化システムの規定の構成に関係する項目を全てカバーするべきである。常にシステムの構成設定が正確に記述され、文書化されるようにするべきである。試験固有の活動（例えば、データ取込み、データ計算など）については、構成設定が結果に関連するのであれば、コンピュータ化システムの特定の構成設定まで追跡可能とするべきである。変更管理はリスクアセスメント、テスト、リリース及び適切な文書化手順と結び付いているべきである。

[1] ISPE - International Society for Pharmaceutical Engineering
[2] GAMP - Good Automated Manufacturing Practice

1.9. Documentation requirements 46. Documentation requirements for computerised systems should be included in the quality management system and should cover all GLP-relevant computerised systems. The depth of documentation necessary will vary dependent on the complexity and validation strategy of the computerised system. For each computerised system there should be documentation typically covering: a) the name and version of the computerised system's software or identification code and a detailed and clear description of the purpose of the computerised system; b) the hardware on which the software operates; c) the operating system and other system software (e.g., tools) used in conjunction with the computerised system; d) the computerised system's programming language(s) and/or data base tools used where appropriate only; e) the major functions performed by the computerised system; f) an overview of the type and flow of data associated with the computerised system; g) file structures, error and alarm messages associated with the use of the computerised system; h) the computerised system's software components with version numbers; and i) configuration and communication links among modules of the computerised system and to equipment and other systems.	**1.9. 文書化が必要な事項** 46. コンピュータ化システムに関して文書化が必要な事項は、品質マネジメントシステムに含まれるべきであり、全ての GLP 関連コンピュータ化システムを対象にするべきである。文書化の必要性の程度はコンピュータ化システムの複雑さやバリデーション戦略に応じて異なる。それぞれのコンピュータ化システムについて、一般に以下を網羅した文書を用意するべきである。 a) コンピュータ化システムのソフトウェアの名称とバージョン又は識別コード及びコンピュータ化システムの目的についての詳細かつ明確な説明 b) ソフトウェアが作動するハードウェア c) コンピュータ化システムと連携して使用されるオペレーティングシステム及びその他のシステムソフトウェア（例えば、ツール） d) コンピュータ化システムのプログラミング言語及び／又はデータベースツール（使用された場合に限る） e) コンピュータ化システムによって実行される主な機能 f) コンピュータ化システムに関係するデータの種類と流れについての概要 g) コンピュータ化システムの使用に関係するファイル構造、エラー及び警告メッセージ h) コンピュータ化システムのソフトウェアコンポーネントとそのバージョン番号 i) コンピュータ化システムのモジュール間の構成設定と通信リンク並びに装置や他のシステムへの構成設定と通信リンク

47. The use of computerised systems should be documented adequately. Such documentation typically covers, but is not limited to: a) procedures for the operation of computerised systems (hardware and software) and the responsibilities of personnel involved; b) procedures for security measures to detect and prevent unauthorised access or changes to data; c) change control procedures describing processes for authorisation, testing and documentation of changes to equipment (hardware and software); d) procedures for the periodic evaluation for correct functioning of the complete system or its component parts and the recording of these tests; e) procedures covering routine preventative maintenance and fault repair (these procedures should clearly detail the roles and responsibilities of personnel involved. For COTS systems, the use of a vendor's own policies and procedures for performing the work where appropriate is acceptable. This should be detailed in a written service level agreement); f) procedures for software development, acceptance testing, and other relevant testing and the recording of all testing; g) back-up and business continuity procedures; h) procedures for the archiving and "retrieval" of all electronic data, software versions and documentation of computer configuration and evidence of all activities; i) procedures for the monitoring and auditing of computerised systems and evidence of all activities; and j) procedures and authorisation for system retirement.	47. コンピュータ化システムの使用について適切な文書を作成するべきである。このような文書には一般に以下の内容が記載されるが、これだけに限定されない。 a) コンピュータ化システム（ハードウェア及びソフトウェア）の操作手順及び関係者の責任 b) データへの不正なアクセス又は変更を検出して防止するためのセキュリティ対策の手順 c) 装置（ハードウェア及びソフトウェア）に加える変更の許可、テスト及び文書化のプロセスを説明する変更管理手順 d) システム全体又はその構成部分が適切に機能していることについての定期的な評価とこれに関わるテストの記録の手順 e) 日常の予防保守及び障害復旧の手順（こうした手順においては関係者の役割と責任を明確に詳しく決めるべきである。COTS システムの場合、必要に応じて作業を遂行するためのベンダー独自の方針及び手順の採用が認められる。このことはサービスレベルアグリーメントに詳しく記述しておくべきである） f) ソフトウェア開発、受入テスト及びその他の関連するテスト並びに全てのテストの記録の手順 g) バックアップ及び事業継続手順 h) 全ての電子データ、ソフトウェアバージョン、コンピュータ構成についての資料並びに全ての活動のエビデンスをアーカイブし、「リトリーブ」するための手順 i) コンピュータ化システム及び全ての活動のエビデンスをモニタリング・調査する手順 j) システム廃止の手順及び許可

48. Further management and validation procedures should be described if relevant and may comprise but not be limited to: acquisition; risk management; service management; validation planning; requirement specification; design specification; installation; system release; traceability; incident management; configuration management; record management; staffing; roles and responsibilities of personnel and document management.	48. 関連する場合には、さらなる管理及びバリデーション手順も記載するべきである。以下のものがあるが、これだけに限定されない。 データ取得、リスクマネジメント、サービス管理、バリデーション計画、要求仕様、設計仕様、設置、システムリリース、トレーサビリティ、インシデント管理、構成管理、記録管理、担当者の配属、担当者の役割と責任、文書管理。
49. Records and procedures should be available that describe in sufficient detail validation and use of the computerised system. Such records may comprise but are not limited to: risk assessment; supplier assessment; service level agreements; requirement specifications; testing; release; personnel and user training; descriptions of incidents and changes; configuration and operation.	49. コンピュータ化システムのバリデーションや使用について十分に詳しく記述している記録や手順書を用意するべきである。このような記録としては以下のものがあるが、これだけに限定されない。 リスクアセスメント、サプライヤアセスメント、サービスレベルアグリーメント、要求仕様書、テスト、リリース、担当者及びユーザの教育訓練、インシデント及び変更の内容、構成設定、運用。
50. The complete documentation of validation and operation of a computerised system should be available as long as study data generated with the system have to be archived according to applicable regulations.	50. システムで生成される試験データを、適用される規制に従ってアーカイブしなければならない期間は、コンピュータ化システムのバリデーション及び運用についての完全な文書を利用可能な状態にしておくべきである。

2. PROJECT PHASE	2. 開発段階
2.1. Validation 51. Computerised systems should be designed and demonstrated to be fit for purpose in a GLP environment and introduced in a pre-planned manner. The validation of a computerised system, its documentation and reports should cover the relevant steps of the life cycle, as defined by test facility management based on the complexity and intended use of a system. The validation effort may be scaled and adapted to the type of system justified by documented risk assessment. Test facility management may rely on best practice guidance when scaling the validation effort. Test facility management should be able to justify the life cycle, the strategy, validation standards, protocols, acceptance criteria, procedures, records and corresponding deliverables based on a risk assessment. For example, test facility management`s validation deliverables may be limited to user requirement specifications, a validation plan, user acceptance testing and a validation report if it can be justified by risk assessment.	**2.1. バリデーション** 51. コンピュータ化システムはGLP環境での目的に適合するように設計され、これが立証され、あらかじめ計画されたとおりに導入されるべきである。コンピュータ化システムのバリデーション、その記録文書及び報告書はライフサイクルの各段階を網羅するべきである。なお、その各段階は、システムの複雑さと使用目的に基づいて運営管理者によって規定される。バリデーション作業は、リスクアセスメント文書によって正当化されるシステムの種類に応じた規模とすることができる。運営管理者はバリデーション作業の規模を決定するときにベストプラクティスに関する指針に依拠することができる。運営管理者は、ライフサイクル、戦略、バリデーション基準、計画書、受入基準、手順、記録及び付随して発生する成果物をリスクアセスメントに基づいて正当化できるべきである。例えば運営管理者のバリデーション成果物は、リスクアセスメントによって正当化できるのであれば、ユーザ要求仕様書、バリデーション計画、ユーザ受入テスト、そしてバリデーション報告書に限定することができる。
52. There should be evidence that the system was adequately tested for conformance with the acceptance criteria set by the test facility prior to being put into routine use. Formal acceptance testing requires the conduct of tests following a pre-defined plan and retention of documented evidence of all testing procedures, test data, test results, a formal summary of testing and a record of formal acceptance.	52. システムが日常的に使用されるようになる前に、試験施設によって設定される受入基準への適合性について十分にテストされたことのエビデンスが必要である。正式な受入テストでは、事前に定められた計画に従ったテストの実施と、全てのテスト手順、テストデータ、テスト結果、テストの正式な要約及び正式な受入の記録についての文書化されたエビデンスを保持する必要がある。

2.2. Change control during validation phase 53. A change control and deviation management process should be in place from the start of the validation process. If change control and deviation records are not considered relevant it should be justified by test facility management based on a risk assessment (e.g. a simplified validation approach of a less complex [i.e. simple] system).	**2.2. バリデーション段階における変更管理** 53. 変更管理と逸脱管理のプロセスをバリデーションプロセスの開始時点から設けておくべきである。変更管理と逸脱の記録が必要ないと考えるのであれば、このことはリスクアセスメントに基づいて運営管理者によって正当化されるべきである（例えば、複雑でない（すなわち単純な）システムの簡易バリデーションアプローチ）。
54. Change control during development and validation of a system should be clearly distinguished from change control during the operation of the system. Validation documentation should include change control records (if applicable) and reports of all deviations observed during the validation process.	54. システムの開発及びバリデーション中の変更管理はシステム運用時のとは明確に区別するべきである。バリデーション文書には、変更管理記録（該当する場合）とバリデーションプロセスにおいて観察された全ての逸脱の報告書を含めるべきである。
2.3. System description 55. A system description detailing the physical and logical arrangements, data flows and interfaces with other systems or processes, any hardware and software prerequisites, and security measures should be available. An up-to-date system description should be maintained throughout the life cycle of the system as described in chapter 1.9. For simple systems with low complexity, a less complex description would be acceptable.	**2.3. システム記述書** 55. 物理的・論理的配置、データフローや他のシステムないしプロセスとのインターフェース、ハードウェア及びソフトウェアの必須条件、セキュリティ対策を詳述したシステム記述書を用意するべきである。1.9 に記載されるとおり、システムのライフサイクルを通して最新版のシステム記述書を維持するべきである。複雑さの低い単純なシステムについては、単純な記述書でも構わないだろう。

2.4. User requirement specifications 56. User requirement specifications are of paramount importance for all validation activities and should be generated for all GLP-relevant computerised systems regardless of the system's complexity. User requirement specifications should describe the functions of a system and should be based on a documented business process for the system, and the applicable regulatory requirements. An initial validation risk assessment should be based upon an understanding of the business processes, user requirement specifications and regulatory requirements.	**2.4. ユーザ要求仕様書** 56. ユーザ要求仕様書は全てのバリデーション活動にとって最も重要なものであり、システムの複雑さに関係なく全ての GLP 関連コンピュータ化システムに関して作成されるべきである。ユーザ要求仕様書にはシステムの機能を記載するべきであり、システムのためのビジネスプロセス文書並びに適用される規制要件に基づいたものとするべきである。バリデーションの最初のリスクアセスメントは、ビジネスプロセス、ユーザ要求仕様書及び規制要件についての理解に基づいているべきである。
57. User requirement specifications should cover all GLP-relevant functions of a system and should be used in the risk assessment to identify critical functions and appropriate testing activities. Depending on a system's complexity, user requirement specifications should be traceable to any further specification documents, if applicable, and test documentation generated throughout the life cycle.	57. ユーザ要求仕様書はシステムの GLP 関連機能を全て網羅するべきであり、重要な機能や適切なテスト活動を特定するためのリスクアセスメントにおいて使用されるべきである。システムの複雑さに応じて、ユーザ要求仕様書は、他の仕様書（該当する場合）及びライフサイクルを通して作成されるテスト文書に追跡可能とするべきである。
58. If a provided system (purchased or hosted by a supplier) contains more functions than needed, only the GLP-relevant functions need to be tested. Validation should also include functions that may be used in non-GLP studies and that might interfere with the use of the computerised system in GLP studies. The other functions and/or functionalities that are out of scope (i.e. not intended to be used) should be identified but do not require testing.	58. 供給されたシステム（購入システム又はサプライヤによってホスティングされたシステム）に必要以上の機能が備わっている場合、GLP 関連機能だけをテストすれば良い。バリデーションでは、非 GLP 試験で使用され、GLP 試験でのコンピュータ化システムの使用の妨げとなるかもしれない機能も対象とするべきである。対象外の（すなわち使用を意図されていない）その他の機能については、特定するべきであるが、テストをする必要はない。

2.5. Quality Management system and support procedures 59. Both the development of a computerised system as well as the validation process should be governed by a quality management system. There should be adequate documentation that a system was developed in a controlled manner and preferably according to recognised quality and technical standards (e.g. ISO 9001). If a system is developed by a vendor, it is the responsibility of test facility management to evaluate the vendor's system development quality management system. The test facility management should rely on risk assessment when defining the evaluation strategy.	**2.5. 品質マネジメントシステムと関係手順** 59. コンピュータ化システムの開発及びバリデーションプロセスは，ともに品質マネジメントシステムによって管理されるべきである。システムが、定められた方法で、できれば広く認められている品質及び技術規格（例えば、ISO 9001）に従って開発されたことが適切に文書に記録されているべきである。システムがベンダーによって開発される場合、ベンダーのシステム開発品質マネジメントシステムを評価するのは運営管理者の責任である。評価方法を決める際、運営管理者はリスクアセスメントに依拠するべきである。
2.6. Customised systems[3] 60. Customised systems are developed for a specific use by a particular test facility (e.g. GLP study specific data capturing systems, spreadsheet templates with formulas or macros, queries, statistical applications or data evaluation systems, etc.). Such computerised systems may also be configured or coded specifically for one or more GLP studies. As no experience from previous or parallel use is available, customised systems bear the highest intrinsic risk. There should be a process in place for the validation of customised computerised systems that ensure the formal assessment and reporting of quality and performance measures for all the life cycle stages of the system.	**2.6. カスタマイズシステム** [3] 60. カスタマイズシステムは特定の試験施設の特定用途のために開発される（例えば、GLP 試験特有のデータ取込みシステム、数式又はマクロ付きスプレッドシートテンプレート、クエリー、統計アプリケーション又はデータ評価システムなど)。このようなコンピュータ化システムは一つないし複数の GLP 試験専用に構成設定又はプログラミングされることもある。カスタマイズシステムは、過去に使用されることはなく、また他の施設でも使用されることはないため、最も高度に内在するリスクを抱えている。カスタマイズされたコンピュータ化システムのバリデーションについては、システムのライフサイクル全段階にわたる品質及び性能指標の正式な評価と報告が確実に行われるプロセスを整えるべきである。

[3] Source code of customised systems (or all software of the computerised system) in some OECD member countries should be retrievable by the test facility management to provide the monitoring authority access to the software code. This can be done by archiving a digital copy of the source code, escrow arrangements, or written agreements.
一部の OECD 加盟国では、カスタマイズシステム（又はコンピュータ化システムの全てのソフトウェア）のソースコードは、査察当局がソフトウェアコードにアクセスできるよう、運営管理者によってリトリーブが可能な状況にされているべきである。これはソースコードのデジタルコピーのアーカイブ、預託協定、又は合意書によって可能である。

61. A written agreement between the supplier of the customised system and test facility management describing roles and responsibilities relevant to the system and its validation is necessary. The validation effort of the test facility management should consider all quality relevant activities of the supplier even at the supplier's business location. Any outsourced activities or in-house supplier activities should be part of the computerised system's life cycle.	61. カスタマイズシステムのサプライヤと運営管理者との間で、システムとそのバリデーションに関する役割と責任を記述した合意書が必要である。運営管理者のバリデーション作業においては、サプライヤがサプライヤの事業拠点で行う品質関連活動を全て考慮するべきである。外部委託活動ないしサプライヤの社内活動のいずれもコンピュータ化システムのライフサイクルの一環とするべきである。
62. If a hosted application is a custom coded or configured application, the system must be addressed both as a customised and a vendor-supplied system.	62. ホスティングアプリケーションがカスタマイズしたプログラムからなる場合又は構成設定されたアプリケーションの場合、そのシステムはカスタマイズシステムとしても、また、ベンダーから供給されるシステムとしても扱われなければならない。

2.7. Testing 63. Testing (e.g. installation testing, user acceptance testing) should be carried out to ensure that a system meets predefined requirements. It is test facility management's responsibility to understand the need for testing and to ensure the completeness of the tests and test documentation. Testing should be based upon business process knowledge and intended use of the system. Procedures should describe how tests are conducted and clearly define roles and responsibilities and documentation requirements. It is the test facility management's responsibility to decide on the depth and breadth of the testing guided by risk assessment. Test facility management should ensure that all systems, including COTS systems, are tested and evaluated. A supplier's testing activity and documentation may assist the test facility management in its validation efforts and may supplement or replace test facility testing. Test facility management should retain evidence of testing regardless of whether the testing is done by the test facility or by a supplier demonstrating appropriate test methods and test scenarios have been employed. In particular, system (process) parameter limits, data limits and error handling should be considered.	**2.7. テスト** 63. システムがあらかじめ定義された要件を満たしていることを確認するためにテスト（例えば、据付テスト、ユーザ受入テスト）を実施するべきである。テストの必要性について理解し、テスト及びテスト文書の完全性を確保するのは運営管理者の責任である。テストはビジネスプロセスの知識とシステムの使用目的に基づいたものとするべきである。手順書に、テストの方法並びに役割と責任及び文書化するべき事項を明確に規定するべきである。リスクアセスメントを指針としてテストの詳細さと範囲を決めるのは運営管理者の責任である。運営管理者は、COTS システムを含む全てのシステムがテストされ、評価されることを確実にするべきである。サプライヤのテスト活動及び記録文書は運営管理者のバリデーション活動に役立ち、試験施設でのテストの補足又は代替となるだろう。運営管理者は、テストが試験施設によって行われるかサプライヤによって行われるかに関係なく、適切なテスト方法及びテストシナリオが用いられたことを明示するテストのエビデンスを持ち続けるべきである。特にシステム（プロセス）パラメータ限界、データ限界及びエラー処理について考慮するべきである。
64. The test facility management should consider a method specific user acceptance testing to demonstrate that the system is fit for performing a specific GLP study (e.g. prove the suitability of a system performing a typical analytical determination including calibration, measurements, calculations and data transfer to a LIMS).	64. 運営管理者は、システムが特定の GLP 試験を行うのに適していることを証明するために特定のユーザ受入テストの方法を考慮するべきである（例えば、校正、測定、計算及び LIMS へのデータ転送を含む典型的な分析測定を実施するためのシステムの適合性の証明）。

65. An interface to change control procedures should exist. When testing leads to system changes these should be managed via change control. Evidence of adequate testing could be provided by maintaining records of internal testing results, or records of vendor auditing.	65. テストは変更管理手順とつながっているべきである。テストの結果、システム変更に至る場合、これを変更管理によって管理するべきである。内部テスト結果の記録又はベンダーオーディットの記録を保管しておくことで適切な試験のエビデンスとすることができる。
2.8. Data migration 66. Data migration may occur in the course of a GLP study or after a study has been finalised. Data migration should be part of the test facility management's validation scope if GLP-relevant data is affected regardless of the status of any GLP study project. If study records are archived in an electronic system, data migration may become relevant.	**2.8. データ移行** 66. GLP 試験の途中で、あるいは試験の終了後にデータ移行が行われる場合がある。データ移行は、GLP 関連データが影響を受けるのであれば、いずれの GLP 試験においても、試験の段階に関係なく運営管理者のバリデーション範囲に含めるべきである。試験記録が電子システムにアーカイブされる場合、データ移行が関係することもある。
67. Where electronic data are transferred from one system to another, the process must be documented. It is test facility management's responsibility to ensure and demonstrating that data are not altered during the migration process. Conversion of data to a different format should be considered as data migration (e.g. from a proprietary data format to PDF). Where data are transferred to another medium, data must be verified as an exact copy prior to any destruction of the original data.	67. 電子データをシステム間で転送する場合、このプロセスを文書化しなければならない。移行プロセスでデータが改ざんされないことを確実にして、このことを立証するのは運営管理者の責任である。異なる形式へのデータ変換はデータ移行とみなされるべきである（例えば、独自のデータ形式から PDF 形式に）。データが別の媒体に転送される場合、オリジナルデータの廃棄前に、データが正確なコピーであることを検証しなければならない。
68. Data migration efforts may vary greatly in complexity and risks. Examples include: a) version upgrades; b) data conversions (from one database to another; to another data format; software upgrade related change of format); c) same system migration (moving application; data from one server to another); and d) migration from a source to a target system.	68. データ移行作業は複雑さやリスクに大きなばらつきがある。例として以下のものがある。 a) バージョンアップグレード b) データ変換（別のデータベースへの移行、別のデータ形式への変換、ソフトウェアアップグレードに関連する形式変更） c) 同じシステム内での移行（アプリケーションの移動、別のサーバへのデータ移行） d) ソースシステムからターゲットシステムへの移行

69. Migrated data should remain usable and should retain its content and meaning. The value and/or meaning of and links between a system audit trail and electronic signatures should be ensured in a migration process. It is the test facility management's responsibility to maintain the link between the readable audit trail or electronic signatures and the audited data.	69. 移行されたデータは引き続き使用できるべきであり、その内容及び意味を保持しているべきである。移行プロセスにおいて、システム監査証跡と電子署名の値及び／又は意味並びにシステム監査証跡と電子署名のリンクが確保されるべきである。判読可能な監査証跡又は電子署名と監査済みデータとのリンクを維持するのは運営管理者の責任である。
2.9. Exchange of data 70. Communications related to computerised systems broadly fall into two categories: between computers or between computers and peripheral components. GLP-relevant data may be transported automatically, uni-directionally or bi-directionally, from one system to another system (e.g. from a remote data capturing system to a central data base, from spreadsheets to a LIMS, from a chromatography data management system to a LIMS, or from a spreadsheet to a statistics software application). All communication links are potential sources of error and may result in the loss or corruption of data. Appropriate controls of interfaces for security and system integrity must be adequately addressed during development, validation, operation and maintenance. Electronic data exchange between systems should include appropriate built-in checks for the correct and secure entry and processing of data. Network infrastructure should be qualified. However, this requirement is not meant to request validation of standard communication infrastructure and its procedures (e.g. the basic communication language of the internet TCP/IP [Transmission Control Protocol / Internet Protocol]).	**2.9. データの交換** 70. コンピュータ化システムに関係する通信は大まかに 2 つに分類される。コンピュータ間の通信又はコンピュータと周辺機器間の通信である。GLP 関連データはシステムから別のシステムに自動的に、一方向に、あるいは双方向に伝送される場合がある（例えば、遠隔データ取込みシステムから中央のデータベース、スプレッドシートから LIMS、クロマトグラフィデータ管理システムから LIMS、あるいはスプレッドシートから統計ソフトウェアアプリケーション）。全ての通信回線は潜在的なエラー発生源であり、データの損失ないし破損に至る可能性がある。開発、バリデーション、操作及び保守管理時には、セキュリティ及びシステム保全のためにインターフェースの適切な管理に的確に取り組まなければならない。システム間の電子データ交換では、データの正確で安全な入力及び処理のための適切なチェック機構が内蔵されているべきである。ネットワークインフラストラクチャは適格性評価を行うべきである。ただしこの要件は、標準的な通信基盤とその手順（例えば、インターネット TCP/IP（伝送制御プロトコル／インターネットプロトコル）の基本的な通信言語）のバリデーションを要求するものではない。

3. OPERATIONAL PHASE	**3. 運用段階**
71. All computerised systems should be operated and maintained in a manner which ensures the continuity of the validated state.	71. 全てのコンピュータ化システムはバリデートされた状態の維持を確保する方法で運用され、維持されるべきである。
3.1. Accuracy checks 72. Test facility management should be aware of all GLP-relevant data entered manually into electronic systems. It is test facility management's responsibility to adequately control any electronic data entry system regardless of its complexity. Risk assessment should be applied to identify the potential for erroneous data entry and to evaluate the criticality and consequences of erroneously or incorrectly entered data. Risk mitigation strategies should be described and implemented. This may result in the need for additional manual and/or electronic checks for the accuracy of entered data by a second operator or electronic system. When used, automated checks on data entry should be included in the validation of a computerised system (e.g. automatically applied validation scripts during manual data entry), the depth of validation efforts should be scaled based on risk assessment. The use of invalidated data entry systems should be excluded (e.g. uncontrolled use of spreadsheets). If manual control procedures are applied for manual data entry, the procedure should be assured by adequate documentation which will facilitate reconstruction of activities.	**3.1. 正確性チェック** 72. 運営管理者は電子システムに手動で入力される GLP 関連データを全て把握しておくべきである。その複雑さに関係なく、あらゆる電子データ入力システムを適切にコントロールするのは運営管理者の責任である。データ入力ミスの起こる可能性を特定し、誤入力又は入力が不正確なデータの重要度や影響を評価するためにリスクアセスメントを適用するべきである。リスク軽減戦略を示し、実行するべきである。リスク軽減戦略に基づき、入力されたデータの正確性のために別のオペレータによる追加のマニュアルチェック及び／又は電子システムによる電子的なチェックを実施する必要性が生じる場合がある。データ入力の自動チェックを採用する場合、コンピュータ化システムのバリデーションに含めるべきであり（例えば、手動によるデータ入力時に自動的に適用される検証スクリプト)、バリデーション作業の詳細さはリスクアセスメントに基づいて決めるべきである。バリデートされていないデータ入力システムの使用は排除するべきである（例えば、スプレッドシートの制御されない使用)。手動データ入力に対して、手動でコントロールする手順を適用するのであれば、作業の再構築を容易にする適切な文書を作成することによってその手順を確実なものにするべきである。

3.2 Data and storage of data 73. When data (raw data, derived data or metadata) are stored electronically, requirements for back-up and archiving purposes should be defined. Back-up of all relevant data should be carried out to allow recovery following failure which compromises the integrity of the system.	**3.2 データ及びデータの保存** 73. データ（生データ、派生データ又はメタデータ）が電子的に保存される場合、バックアップ及びアーカイブのための要件を定義するべきである。システムの完全性を損なう障害が発生した後の復旧を可能にするために、全ての関連するデータのバックアップを行うべきである。
74. Stored data should be secured by both physical and electronic means against loss, damage and/or alteration. Stored data should be verified for restorability, accessibility, readability and accuracy. Verification procedures of stored data should be risk based. Access to stored data should be ensured throughout the retention period.	74. 保存データは、物理的手段及び電子的手段の両方によって、損失、損傷及び／又は改ざんから保護されるべきである。保存データの復旧可能性、アクセス性、見読性、正確性について検証するべきである。保存データの確認手順はリスクベースで検討するべきである。データの保存期間全体を通じて保存データへのアクセスを確保するべきである。
75. Hardware and software system changes must allow continued access to, and retention of, the data without any risk to data integrity. When a system or software is updated, it must be possible to read data stored by the previous version or other methods must be available to read the old data. Supporting information (e.g. maintenance logs, calibration records, configuration etc.) which is necessary to verify the validity of raw data or to reconstruct a whole study or parts of it should be backed-up and retained in the archives. Software should be retained in the archive if necessary to read or reconstruct data.	75. ハードウェア及びソフトウェアのシステム変更があっても、データの完全性にいかなるリスクを及ぼすことなく、データへの継続的なアクセスとデータの保持が可能でなければならない。システム又はソフトウェアが更新される場合、以前のバージョンで保存されたデータを読み取ることが可能でなければならず、そうでなければ旧データを読み取るための他の方法がなければならない。生データの正当性の確認あるいは試験全体又はその一部の再構築に必要な補足情報（例えば、保守管理記録、校正記録、構成設定など）はバックアップを行い、また、資料保存施設に保存するべきである。データの読取りないし再構築のために必要なソフトウェアは資料保存施設に保存するべきである。

76. Regarding electronic records, test facility management should have: a) identified any study relevant electronic records (e.g. raw data, derived data). It is necessary that raw data are identified for each computerised system no matter how raw data are associated with it (e.g. by storage on an electronic storage medium, by computer or instrument printouts etc.); b) assessed the criticality of the electronic records for the quality of study results; c) assessed potential risks to the electronic records; d) established risk mitigation procedures; and e) monitored the effectiveness of risk mitigation throughout the life cycle.	76. 電子記録に関して、運営管理者は以下のことを行っているべきである。 a) 全ての試験関連の電子記録を特定している（例えば、生データ、派生データ）。コンピュータ化システムごとに生データを特定する必要がある。それは、生データがコンピュータ化システムとどのように関連しているかを問わない（例えば、電子記録媒体への保存、コンピュータ又は機器によるプリントアウトなどの形で） b) 試験結果の品質における電子記録の重要度を評価している c) 電子記録への潜在的リスクを評価している d) リスク軽減手順を確立している e) ライフサイクル全体にわたってリスク軽減の効果をモニターしている

77. Regarding procedures, the test facility management should describe how electronic records are stored, how record integrity is protected and how readability of records is maintained. For any GLP-relevant time period, this includes, but may not be limited to: a) physical access control to electronic storage media (e.g. measures for controlling and monitoring access of personnel to server rooms, etc.); b) logical (electronic) access control to stored records (e.g. authorisation concepts for computerised systems as part of computerised system validation which defines roles and privileges in any GLP-relevant computerised system); c) physical protection of storage media against loss or destruction (e.g. fire, humidity, destructive electrical faults or anomalies, theft, etc.); d) protection of stored electronic records against loss and alteration (e.g. validation of back-up procedures including the verification of back-up data and proper storage of back-up data; application of audit trail systems); and e) ensuring accessibility and readability of electronic records by providing an adequate physical environment as well as software environment.	77. 手順書に関して、運営管理者は電子記録がどのように保存され、記録の完全性がどのように保護され、記録の見読性がどのように維持されるのかを記述するべきである。GLP 関連の期間において以下の手順が含まれるが、これだけに限定されない。 a) 電子記録媒体への物理的アクセスコントロール（例えば、担当者のサーバルームへのアクセスに対する制御及びモニタリングの方法など） b) 保存された記録への論理的（電子的）アクセスコントロール（例えば、全ての GLP 関連コンピュータ化システムにおける役割と権限を規定する、コンピュータ化システムのバリデーションの一環としてのコンピュータ化システムに関する権限の認定コンセプト） c) 記録媒体の損失ないし破壊に対しての物理的保護（例えば、火災、湿度、破壊的な電気的障害ないし異常、盗難など） d) 保存された電子記録の損失及び改ざんに対する保護（例えば、バックアップデータの確認及びバックアップデータの適切な保存を含むバックアップ手順のバリデーション、監査証跡システムの利用） e) 適切な物理的環境及びソフトウェア環境を用意することによる、電子記録のアクセス性及び見読性の確保
78. Data storage should be considered for each computerised system used to perform GLP studies during the study phase and archiving period. It is not necessary to include the evaluation in the study documentation. However, test facility management should have a policy to explain how data are stored and how storage requirements are satisfied. This information should be part of the system validation documentation set. If the test facility hands over the electronic study data to a sponsor, the responsibility for the data transfers to the sponsor.	78. GLP 試験を行うために使用される各コンピュータ化システムに関して、試験期間及びアーカイブ期間におけるデータ保存について考慮するべきである。試験関連の文書にその評価を盛り込む必要はない。しかしながら運営管理者は、データがどのように保存され、保存要件がどのように満たされるのかについて説明できる方針を持つべきである。この情報は一連のシステムバリデーション文書に含めるべきである。試験施設が試験委託者に試験の電子データを引き渡す場合、データに関する責任は試験委託者に移る。

3.3. Printouts 79. If data are printed to represent raw data, all electronic data including derived data as well as metadata and (information about data changes if such changes are necessary to maintain the correct content and meaning of the data) should be printed. Alternatively all electronic records should be verifiable on screen in human-readable format and retained. This includes all information about changes made to records, if such changes are relevant for the correct content and meaning.	**3.3. プリントアウト** 79. データをプリントアウトして生データとする場合には、派生データやメタデータ（及び、データの正確な内容と意味を維持するために変更が必要な場合はデータ変更に関する情報）を含む全ての電子データを印刷するべきである。あるいは、全ての電子記録を画面上で人が読める形式で確認できるようにし、保存するべきである。これには記録に対して行われた変更に関する全ての情報も、当該変更が記録の正確な内容と意味に関連するのであれば、含まれる。
3.4. Audit trails 80. An audit trail provides documentary evidence of activities that have affected the content or meaning of a record at a specific time point. Audit trails need to be available and convertible to a human readable form. Depending on the system, log files may be considered (or may be considered in addition, to an audit trailing system) to meet this requirement. Any change to electronic records must not obscure the original entry and be time and date stamped and traceable to the person who made the change.	**3.4. 監査証跡** 80. 監査証跡は、特定の時点における記録の内容ないし意味に影響を及ぼした活動のエビデンスを文書化したものである。監査証跡は人が読める形式か、又は人が読める形式に変換できる必要がある。システムによってはログファイルがこの要件を満たすとみなすことができる（あるいは監査証跡システムとログファイルの組合せによりこの要件を満たすとみなせるかもしれない）。電子記録の変更によって元の入力内容が分からなくなってはならず、変更の時刻及び日付スタンプを付けなければならず、変更を行った人物まで追跡可能でなければならない。
81. Audit trail for a computerised system should be enabled, appropriately configured and reflect the roles and responsibilities of study personnel. The ability to make modifications to the audit trail settings should be restricted to authorised personnel. Any personnel involved in a study (e.g. study directors, heads of analytical departments, analysts, etc.) should not be authorised to change audit trail settings.	81. コンピュータ化システムの監査証跡は有効で、適切に構成設定され、試験従事者の役割と責任を反映しているべきである。監査証跡の設定を変更できるのは許可を受けた者に限定するべきである。試験に関与する者（例えば、試験責任者、分析部門の責任者、分析担当者など）に対しては監査証跡の設定変更を許可するべきではない。

82. A system should be in place that can ensures a risk based review of the audit trail functions, its settings and the recorded information. The test facility management may consider, but should not be limited to, individual events (e.g. user behavior, suspected data integrity issues) to review the audit trail records. Completeness and suitability of the audit trail functions and settings may be considered. GLP quality assurance personnel should be involved. A review of the audit trail functions should be based upon an understanding of the use of the system, the ability to modify the record and the controls preventing malicious alterations of the records.	82. システムは、監査証跡機能とその設定値及び記録された情報についてリスクベースレビューが確実に行えるようになっているべきである。運営管理者は、監査証跡記録をレビューするときに、個別事象（例えば、ユーザの行動、データの完全性が疑われる問題）を考慮することになるであろうが、これだけに限定するべきではない。監査証跡機能及びその設定値の完全性と適切性について検討することになるかもしれない。GLP の信頼性保証担当者が関与するべきである。監査証跡機能のレビューは、システムの使用、記録修正の可能性、悪意のある記録改ざんを防止するための仕組みに関する理解に基づいて行うべきである。
83. The system should be able to highlight alterations made to previously entered data both on the screen and in any printed copies. The original and modified entries should be retained by the system. Audit trails may exist in some systems as a record of changes supplemental to the view to the data (on screen or printed). The original data should be stored together with the modified data. For example, any re-integrated chromatogram modified for the purpose of recalculation should be marked irrevocably.	83. システムは、以前に入力されたデータに対する変更を画面上でもプリントアウトにおいても強調できるようにするべきである。変更前と変更後の入力内容がシステムに保持されているべきである。一部のシステムでは、データ表示（画面上又はプリントアウト）の補足的な変更記録として監査証跡が存在する場合もある。オリジナルデータは変更されたデータとともに保存されるべきである。例えば再計算のために変更された再積分クロマトグラムには取消し不能な形式でマークを付けるべきである。

3.5. Change management and configuration management 84. Test facility management should have appropriate procedures for configuration management and change management in the operational phase. Both change and configuration management should be applied to hardware and software. Change control measures should ensure that changes to the configuration of the computerised system that may affect the validation status are introduced in a controlled manner. A change should be traceable to appropriate change and configuration control records. Procedures should describe the method of evaluation used to determine the extent of retesting necessary to maintain the validated status of the system.	**3.5. 変更マネジメントと構成マネジメント** 84. 運営管理者は運用段階における構成マネジメントと変更マネジメントのための適切な手順を設けるべきである。変更マネジメントと構成マネジメントの両方をハードウェア及びソフトウェアに適用するべきである。変更管理措置によって、確実に、バリデーション状態に影響を及ぼす可能性のあるコンピュータ化システムの構成設定変更が制御された方法で行われるようにするべきである。変更は当該変更管理及び構成管理の記録まで追跡可能とするべきである。手順書には、システムのバリデートされた状態を維持するために必要な再テストの範囲を決定するときに使用される評価方法を記載するべきである。
85. Change control procedures should clearly define roles and responsibilities for accessing and approving changes and detail procedures for assessing the change. Irrespective of the origin of the change (supplier or in-house developed system), appropriate information needs to be provided as part of the change control process. Change control procedures should ensure data integrity.	85. 変更管理手順書では、変更へのアクセス及び承認のための役割と責任、並びに変更を評価するための詳細手順を明確に定めるべきである。変更の起源（サプライヤか、自社開発システムか）に関係なく、変更管理プロセスの一環として適切な情報提供が必要である。変更管理手順によってデータの完全性を確保するべきである。
86. The configuration of a computerised system should be known at any point during its life cycle, from the initial steps of development through to retirement. The documented compliance of an analytical instrument's configuration with the provisions of method validation is required to demonstrate the adequate use of a computerised system in a GLP study – regardless of its complexity. Any GLP study result should be traceable to the relevant and validated system configuration to allow the verification of settings as provided by the study plan or the relevant method.	86. コンピュータ化システムの構成設定は、開発の初期段階から廃止に至るまで、そのライフサイクルのあらゆる時点で理解されているべきである。分析装置の構成設定がメソッドバリデーションの条件に適合していることを文書化することが、GLP 試験におけるコンピュータ化システム（複雑さに関係なく）の適切な使用を証明するために必要である。いかなる GLP 試験の結果も、試験計画又は関連する試験方法で規定された設定で得られたことが確認できるように、試験に関連する、バリデートされたシステムの構成設定まで追跡可能とするべきである。

87. Changes may be required in response to incidents or to facility/study specific purposes. After modification or repair, the validation status of the system should be verified and documented.	87.インシデントへの対処として、又は施設／試験固有の目的に応じるため、変更が必要となる場合がある。変更又は修復後、システムのバリデーション状態を検証し、文書化するべきである。
88. Modifications implemented by routine automation (e.g. virus protection or operating system patches) should be part of formal change control or configuration management. The absence of change management for a computerised system should be justified and based on risk assessment.	88. 日常的な自動処理で行われる修正（例えば、ウィルスからの保護又はオペレーティングシステムのパッチ）は、正式な変更管理又は構成マネジメントの一環とするべきである。コンピュータ化システムの変更マネジメントが行われない場合は、リスクアセスメントに基づき、正当であることを証明するべきである。

3.6. Periodic review 89. Computerised systems should be periodically reviewed to confirm that they remain in a validated state, are compliant with GLP and continue to meet stated performance criteria (e.g. reliability, responsiveness, capacity etc.). The review should include, where appropriate, the current range of functionality, deviation records, incidents, upgrade history, performance, reliability and security that may have affected the validation status of the system. The frequency and depth of the periodic review should be determined based on a risk assessment considering complexity and GLP criticality. The periodic review should take into account any reported unexpected event that may have affected the validation status of a system. The suitability of the review activities and the involvement of specialist personnel as well as GLP-relevant personnel (e.g. test facility management, quality assurance, IT support personnel, supplier etc.) should be justified. Responsibilities of personnel involved in periodic reviews of the validation status of computerised systems should be defined. The need for an interaction between the periodic review activities and the incident reporting system may be considered depending on a risk assessment. Results of periodic review activities and, when applicable, remedial actions should be documented.	**3.6. 定期的レビュー** 89. コンピュータ化システムを定期的にレビューし、バリデートされた状態にあること、GLP に適合していること、そして規定のパフォーマンス基準（例えば、信頼性、応答性、能力など）を満たし続けていることを確認するべきである。レビュー対象は、必要に応じて、システムのバリデーション状態に影響を及ぼした可能性のある、現在の機能範囲、逸脱記録、インシデント、アップグレード履歴、パフォーマンス、信頼性及びセキュリティなどとするべきである。定期的レビューの頻度及び詳細さは、複雑さや GLP 上の重要度を考慮して、リスクアセスメントに基づいて決定するべきである。定期的レビューにおいては、システムのバリデーション状態に影響を及ぼした可能性のある、報告された全ての予期せぬ事象を考慮に入れるべきである。 レビュー活動の適切性と、専門要員及び GLP 関連職員（例えば、運営管理者、信頼性保証部門、IT サポート担当者、サプライヤなど）の関与について、正当であることを証明するべきである。コンピュータ化システムのバリデーション状態の定期的レビューに関与する者の責任を定めるべきである。リスクアセスメントに応じて定期的レビュー活動とインシデント報告システムとの連係の必要性が検討される場合もある。定期的レビュー活動の結果並びに該当する場合には改善措置について、文書化するべきである。

90. Computerised systems of less criticality and less complexity may be excluded from the review if the exclusion is justified based on risk. A periodic review may be unnecessary when major (re-)validation activities have recently occurred and could therefore be postponed. If no unexpected events that may have affected the validated status were reported, automated COTS systems may be excluded from the review. A periodic user review should be done when required (e.g. in the event of organisational changes) or at least yearly as persons and access roles may change. The user review should also be done for COTS.	90. 重要度の低い、あまり複雑でないコンピュータ化システムについては、リスクに基づいて正当化されるのであれば、レビューから除外することができる。重要な（再）バリデーション活動が最近行われている場合には定期的レビューは不要となる可能性があり、それゆえに延期できる。バリデートされた状態に影響を及ぼした可能性のある予期せぬ事象が報告されなかった場合、自動化 COTS システムをレビュー対象から除外することができる。定期的なユーザレビューは必要に応じて（例えば、組織変更があった場合）、又は人やアクセス上の役割が変更になれば少なくとも年 1 回、行うべきである。ユーザレビューは COTS についても行うべきである。
3.7. Physical, logical security and data integrity 91. Documented security procedures authorised by test facility management should be in place for the protection of hardware, software and data from corruption or unauthorised modification, or loss. Appropriate physical and/or logical controls should be implemented depending on the complexity and criticality of a system and the requirements of the organisation in which the system is operated.	**3.7. 物理的、論理的セキュリティ及びデータの完全性** 91. ハードウェア、ソフトウェア及びデータを破損ないし不正な変更、又は損失から保護するために、運営管理者によって承認されたセキュリティ手順書を用意するべきである。システムの複雑さや重要度、並びにシステムが運用される組織の要件に応じて適切な物理的及び／又は論理的コントロールを実現するべきである。

92. Suitable control methods for preventing unauthorised physical access to the system (e.g. computer hardware, communications equipment, peripheral components and electronic storage media) may include the use of keys, pass cards, personal codes with passwords, biometrics, or restricted access to specific computer equipment (e.g. data storage areas, interfaces, computers, server rooms, etc.). Creation, change, and cancellation of access authorisations should be recorded. Authorisation records should be periodically reviewed based upon the criticality of the process supported by the computerised system and in case of relevant organisational changes in the test facility.	92. システム（例えば、コンピュータハードウェア、通信装置、周辺機器、電子記録媒体）への不正な物理的アクセスを防止するための適切なコントロール方法としては、鍵、パスカード、パスワード付きの個人コード、バイオメトリクスの利用、又は特定のコンピュータ装置へのアクセス制限（例えば、データ保存区域、インターフェース、コンピュータ、サーバルームなど）などがある。アクセス権限の付与、変更及び取消について記録するべきである。権限の記録は当該コンピュータ化システムによってサポートされているプロセスの重要度に基づいて、定期的に、また試験施設において関係組織変更があった場合にレビューを行うべきである。
93. As maintaining data integrity is a primary objective of the GLP Principles, test facility management should ensure that personnel are aware of the importance of data security, the procedures and system features that are available to provide appropriate security and the consequences of security breaches. Such system features could include routine surveillance of system access, the implementation of file verification routines and exception and/or trend reporting.	93. データの完全性の維持はGLP原則の最上位の目的であるため、運営管理者は、担当者にデータセキュリティの重要性、適切なセキュリティを保証できる手順やシステム機能、セキュリティ侵害の影響を認識させるべきである。このようなシステム機能には、システムアクセスの日常的監視、ファイル検証ルーチンの実装、例外及び／又はトレンド報告などがある。
94. For equipment not held within specific “computer rooms” (e.g. personal computers and terminals), there should be access controls to the area where the hardware is located (e.g. access control to a building, a laboratory area, or a specific room). Where such equipment is located remotely (e.g. portable components and modem links) additional measures may be taken that should be justified and risk based (e.g. cryptographic control).	94. 特定の「コンピュータルーム」内に置かれていない装置（例えば、パーソナルコンピュータや端末）については、ハードウェアが置かれている区域へのアクセスコントロールが行われるべきである（例えば、建物、試験操作区域、又は特定の部屋の入退室管理）。このような装置が遠隔地にある場合（例えば、携帯機器やモデム接続機器）、追加的対策を講じることになるかもしれないが、これは正当化され、リスクベースで検討するべきである（例えば、暗号化制御）。

95. It is essential that only qualified and approved versions of software are in use. Any introduction of data or software from external sources should be controlled. These controls may be provided by the computer operating system, by specific security routines, by routines embedded into the applications or by combinations of the above. Systems for data and for document storage should be designed to record the date, time and identity of operators entering, changing, confirming or deleting data.	95. ソフトウェアは適格性評価を受けた承認済みのバージョンのみ使用することが必須である。全ての外部からのデータないしソフトウェアの取込みをコントロールするべきである。こうしたコントロールはコンピュータのオペレーティングシステム、特定のセキュリティルーチン、アプリケーションに埋め込まれたルーチン、あるいはこれらの組合せによって行うことができる。データ及び文書保存用のシステムは、日付、時刻並びにデータを入力、変更、確認又は削除するオペレータの身元を記録するように設計されるべきである。
96. The potential for corruption of data by a malignant code or other agents should be addressed if considered necessary. Security measures should be taken to ensure data integrity in the event of both short term and long term system failure.	96. 悪意のあるコード又はその他の手段によるデータ破損の可能性について必要とみなされるのであれば対処するべきである。短期的及び長期的なシステム障害が発生した場合にデータの完全性を確保するためのセキュリティ対策を講じるべきである。
97. An appropriate and well maintained authorisation policy should specify logical access rights to domains, computers, applications and data. User privileges should be defined for operating systems and applications, and should be adapted as required by the organisation of the test facility and in combination with the requirements of a particular GLP study. Roles and responsibilities of personnel granting user privileges should be defined.	97. 適切かつよく維持された権限付与のポリシーによって、ドメイン、コンピュータ、アプリケーション及びデータへの論理的アクセス権を規定するべきである。オペレーティングシステム及びアプリケーションに関してユーザ権限を定義するべきであり、ユーザ権限は、試験施設の組織で必要とされるとおりに、所定の GLP 試験の要件と組み合わせて適応させるべきである。ユーザ権限を付与する者の役割と責任を定義するべきである。

98. User privileges within a computerised system should not interfere with the requirements for data integrity. The activities of any GLP study personnel should be traceable to the user privileges and activities within all relevant computerised systems and should be reflected in user privilege control documents. Administrator rights should not be given to persons with a potential interest in the data (e.g. the laboratory role 'analyst' is not compatible with the system role 'administrator' in a chromatography data management system). A user should not have a second role in a particular system that could interfere with the requirements for data integrity.	98. コンピュータ化システムにおけるユーザ権限はデータの完全性に関する要件の妨げとなってはならない。GLP 試験従事者の活動は、全ての関連するコンピュータ化システム内のユーザ権限と活動まで追跡可能とするべきで、ユーザ権限管理文書に反映させるべきである。管理者権限はデータに関して潜在的な利害関係を持つ可能性のある者に与えてはならない（例えば、「分析者」という実験上の役割は、クロマトグラフィデータ管理システムにおける「アドミニストレーター」というシステム上の役割と両立することはできない)。ユーザは所定のシステムにおいてデータの完全性に関する要件の妨げとなるような第二の役割を持つべきではない。
3.8. Incident Management 99. During the daily operation of the system, records should be maintained of any problems or inconsistencies detected and any remedial action taken. The study director, test facility management, quality assurance and, if appropriate, the sponsor should be informed about incidents requiring remedial action. The study director is responsible for defining the criticality of incidents and for assessing the impact on the study. The root cause of an incident requiring remedial action should be identified and should form the basis of corrective and preventive actions. The priority for corrective and preventative actions should be determined. It should be possible to trace all incidents requiring remedial action reported for a computerised system to the affected GLP studies and vice versa.	**3.8. インシデント管理** 99. 日常のシステム運用において、検出された全ての問題ないし矛盾点及び講じられた全ての改善措置の記録を残すべきである。試験責任者、運営管理者、信頼性保証部門、及び適切であれば試験委託者は、改善措置を要するインシデントについて連絡を受けるべきである。試験責任者はインシデントの重大さの明示と試験への影響の評価に責任を負う。改善措置を要するインシデントについては根本原因を特定するべきであり、是正措置及び予防措置はこれに基づいたものにするべきである。是正措置及び予防措置の優先順位を決定するべきである。コンピュータ化システムに関して報告された、改善措置を要するインシデントは全て、影響を受けた GLP 試験まで追跡可能とするべきであり、これの逆も追跡可能とするべきである。

100. Incident records should be maintained with the system documentation and periodically archived. Incident records should be archived and stored with the system relevant (validation) documentation as incident reports are needed for monitoring and periodic review. Test facility management should have incident management interfaced or integrated with change management, configuration management, periodic review and training. Incident review should be part of a periodic system evaluation.	100. インシデント記録をシステム記録文書とともに維持し、定期的にアーカイブするべきである。インシデント報告書はモニタリングと定期的レビューのために必要であるため、インシデント記録をアーカイブして、システム関係の（バリデーション）記録文書とともに保存するべきである。運営管理者はインシデント管理を変更マネジメント、構成マネジメント、定期的レビュー及び訓練と結び付けるか、これらと統合するべきである。インシデントレビューを定期的なシステム評価の一環とするべきである。
3.9. Electronic signature 101. Electronic records may be signed electronically by applying an electronic signature.	**3.9. 電子署名** 101. 電子記録には電子署名を適用することによって電子的に署名された状態にすることができる。
102. Electronic signatures are expected to: a) have the same legal consequences as a hand-written signature at least within the boundaries of the test facility; b) be permanently linked to their respective record(s); c) include the time and date that they were applied; and d) allow the identification of the signatory and the meaning of the signature.	102. 電子署名に対しては以下のことが期待される。 a) 少なくとも試験施設の区域内では手書きの署名と同じ法的効果を持つ b) それぞれの記録と恒久的に結び付けられる。 c) 適用された日時が含まれている d) 署名者の特定及び署名の意味を与える
103. An electronic signature function of a computerised system should be addressed in the requirements for the system and validated and described in the system procedures. The test facility management should have identified those records which require a hand-written or an electronic signature. It is test facility management's decision to rely on an electronic signature function if other means are possible (e.g. printing and signing by hand). The applied procedure should be described adequately.	103. コンピュータ化システムの電子署名機能について、システム要求事項に取り上げ、バリデーションを行い、システム手順書に記述するべきである。運営管理者は手書き又は電子署名を必要とする記録を特定しておくべきである。他の手段が可能である場合（例えば、印刷して手書きで署名する）、電子署名機能を使用するかどうかを決定するのは運営管理者である。適用手順を十分に記述するべきである。

104. Test facility management should ensure the establishment of an electronic signature policy in order to ensure the adequate use and maintenance of electronic signature functions of a computerised system. Personnel authorised to sign electronically should be clearly identified by name and bound by name to the electronic signature policy. A person's role in a GLP study should be reflected by the meaning of the corresponding electronic signature applied by a study relevant computerised system and should be traceable to the system's authorisation policy. It might be necessary to adapt a computerised system's authorisation concept to study specific requirements.	104. 運営管理者は、コンピュータ化システムの電子署名機能の適切な使用と維持を確保するために、電子署名ポリシーを確実に規定するべきである。電子署名の使用が許可されている者は、名前で明確に特定され、名前により電子署名ポリシーに結び付けられているべきである。 GLP 試験における担当者の役割は、試験関連のコンピュータ化システムによって適用される当該電子署名の意味に反映され、システムの権限認定ポリシーまで追跡可能とするべきである。 コンピュータ化システムの権限の認定コンセプトを試験固有の要件に適応させる必要があるかもしれない。
105. Test facility management should ensure that the electronic signature is equivalent to the handwritten signature and its authenticity is undisputable at least within the boundaries of the test facility or test site. Password re-entry should be considered as a minimum requirement for an electronic signature. The actuation of a function key by a person logged into a system should not be considered as an electronic signature.	105. 運営管理者は、少なくとも試験施設ないし試験場所の区域内では、電子署名が手書き署名と同等であり、真正であることに疑問の余地がないことを確実にするべきである。パスワードの再入力を電子署名の最低要件とするべきである。システムにログインしている者によるファンクションキーでの作動は電子署名とみなされるべきではない。

106. Metadata which are associated with the electronically signed record should be clearly identified (e.g. method settings and system configuration if relevant for the electronically signed analytical result etc.). The computerised system's signature function should ensure the timeliness of the linkage between the electronically signed record and the supporting metadata. It should not be possible for the user to change an applied electronic signature nor the link to the associated metadata. If a change to an electronically signed record or the supporting metadata occurs it should be explained, (electronically) signed and dated by the person responsible for the change. The impact of the change to an electronically signed record or the supporting metadata on the electronic signature should be evaluated as the change invalidates the electronic signature.	106. 電子署名された記録に関連付けられるメタデータを明確に特定するべきである（例えば、電子署名された分析結果に関連するメソッド設定値やシステム構成設定など）。コンピュータ化システムの署名機能によって電子署名された記録と補助メタデータとが瞬時にリンクされることを確実にするべきである。付与された電子署名と関連メタデータとのリンクをユーザが変更することを可能とするべきではない。電子署名された記録又は補助メタデータの変更が行われる場合、その変更に責任を有する者によって説明され、（電子的に）署名され、日付が記録されるべきである。変更が電子署名を無効にしてしまうため、電子署名された記録又は電子署名の補助メタデータを変更することのインパクトについて評価するべきである。

107. Test facility management may apply a “paper-based” procedure to sign records that are printed from the electronic system. It should be noted that paper printouts of an electronic record may not contain all of the information that is necessary to fully reconstruct the activities or provide the full meaning of the data. Certain supporting metadata relevant for the printed/signed record may be kept electronically in a hybrid solution. The use of such a hybrid system should be fully explained in facility procedures and justified via risk assessment. Based upon a risk assessment, printing has to be done on a clear understanding of the process and the information that will not be captured in the printout. The hybrid solution should be described clearly to identify all additional electronic records or supporting metadata which are represented by the printed and signed version of a record. An appropriate system for version control should ensure the timeliness of the linkage between the printed/signed record and the electronically maintained records. Access to modified or superseded records for traceability of changes and documentation of invalid results should be possible. However those records should be excluded from routine use. If a complete set of electronic records and its printed analogue are maintained in parallel, the test facility management should specify the regulated record type in order to apply the appropriate control procedure (e.g. if the complete set of information of an analytical system is printed and maintained electronically in parallel it should be define which set of information is the regulated one).	107. 運営管理者は電子システムから出力される記録に署名するための「紙ベース」の手順を適用することができる。電子記録の紙へのプリントアウトには、活動の完全な再構築又はデータの完全な意味の提示に必要な情報が全て含まれているわけではないことに注意するべきである。印刷／署名された記録に関連するある種の補助メタデータはハイブリッドソリューションによって電子的に保つことができる。このようなハイブリッドシステムの使用については施設の手順書において十分に説明し、リスクアセスメントを通じて正当化するべきである。リスクアセスメントに基づいて、プリントアウトには表示されないプロセスと情報について明確に理解した上で、印刷が行われなければならない。ハイブリッドソリューションについては、記録の印刷・署名版で示される全ての追加電子記録ないし補助メタデータが特定できるよう明確な説明がなされるべきである。バージョン管理のための適切なシステムによって、印刷／署名された記録と電子的に維持される記録とが瞬時にリンクされることを確実にするべきである。変更及び無効な結果の記録文書のトレーサビリティのために、変更された又は取って代わられた記録へのアクセスを可能とするべきである。ただし、これらの記録は日常的な使用からは除外するべきである。電子記録とその印刷版の一式を同時に維持する場合、運営管理者は適切なコントロール手順を適用するために規制対象記録の種類を指定するべきである（例えば、分析システムの完全な情報が印刷されると同時に電子的にも維持される場合、どちらの情報が規制対象であるのかを明確にするべきである）。

3.10. Data approval 108. If a procedure includes an electronic data approval process, the data approval functionality should be included as part of the system validation. The approval process should be described in facility procedures and be performed electronically within the system.	**3.10. データ承認** 108. 手順に電子的なデータ承認プロセスが含まれる場合、データ承認機能をシステムバリデーションの対象に含めるべきである。承認プロセスを施設の手順書に記述し、システム内で電子的に実行するべきである。
3.11. Archiving 109. With regards to archiving, this advisory document supplements OECD GLP Advisory Document Number 15 “Establishment and Control of Archives that Operate in Compliance with the Principles of GLP”.	**3.11. アーカイブ** 109. アーカイブに関して、本アドバイサリー文書は OECD GLP アドバイサリー文書 No. 15「GLP 原則遵守下に運営される資料保存施設の設置及び管理」を補足するものである。
110. Any GLP-relevant data may be archived electronically. The GLP Principles for archiving must be applied consistently to electronic and non-electronic data. It is therefore important that electronic data is stored with the same levels of access control, indexing and expedient “retrieval” as non-electronic data.	110. GLP 関連データは全て電子的にアーカイブすることができる。電子データ及び非電子データに対し、一貫して、アーカイブに関する GLP 原則を適用しなければならない。それゆえに電子データは、アクセスコントロール、見出し付け、適切な「リトリーブ」に関して非電子データと同じ水準で保存されることが重要である。
111. Viewing electronic records without the possibility of alteration or deletion of the archived electronic records or replicating within a computerised system or to another computerised system does not constitute “retrieval” of records. Only when the possibility of alteration or deletion of the archived record exists, should that be considered access, withdrawal, “retrieval”, or removal of records and materials. The archivist should be able to control the assignment of "view only" access to archived electronic data in order to verify that the requirements for archived data are met.	111. アーカイブされた電子記録を変更や削除する可能性のない状況で、あるいはコンピュータ化システム内又は別のコンピュータ化システムに複写する可能性のない状況で、電子記録を閲覧することは、記録の「リトリーブ」には該当しない。アーカイブされた記録の変更又は削除の可能性が存在する場合のみ、記録や資料のアクセス、引き出し、「リトリーブ」、又は移動とみなすべきである。資料保存施設管理責任者はアーカイブされたデータに関する要件が満たされていることを確認するために、アーカイブされている電子データへの「閲覧専用」アクセス権の割当を制御できるべきである。

112. Electronic data should be accessible and readable, and its integrity maintained, during the archiving period. If a hybrid solution is chosen (i.e. “paper-based” data and electronic data maintained in parallel) the test facility management should specify the regulated records for relevance in archiving.	112. 電子データはアーカイブ期間中、アクセス可能かつ読取り可能で、その完全性が維持されているべきである。ハイブリッドソリューションが選択される場合（すなわち、「紙ベース」のデータと電子データが同時に維持される場合）、運営管理者はアーカイブ時に関連する規制対象記録を指定するべきである。
113. Electronic archiving should be regarded as an independent procedure which should be validated appropriately. A risk assessment should be applied when designing and validating the archiving procedure. Relevant hosting systems and data formats should be evaluated regarding accessibility, readability and influences on data integrity during the archiving period. Consideration may have to be given to archiving electronic data in an open format that is independent from proprietary file format e.g. from an instrument manufacturer. Where data conversion is needed, the requirements from section 2.8 apply. The archivist, who holds sole responsibility, may delegate tasks during the management of electronic data to qualified personnel or automated processes (e.g. access control). For roles and responsibilities in the archiving process refer to OECD GLP Advisory Document Number 15.	113. 電子的アーカイブは、適切にバリデーションが行われる必要のある独立した手順とみなすべきである。アーカイブ手順の策定とバリデーションにはリスクアセスメントを適用するべきである。アーカイブ期間中のアクセスし易さ、見読性及びデータの完全性に対する影響に関して、関連するホスティングシステム及びデータ形式を評価するべきである。商標で守られたファイル形式、例えば装置製造業者のものとは別の、オープンフォーマットでの電子データの保管を検討する必要があるかもしれない。データ変換が必要な場合は2.8項の要件が適用される。単独で責任を負っている資料保存施設管理責任者は、電子データの管理において、資格のある者に職務を委託するか、自動化プロセスに委ねることができる（例えば、アクセスコントロール）。アーカイブプロセスにおける役割と責任についてはOECD GLPアドバイサリー文書No. 15を参照。

114. Procedures have to be implemented to ensure that the long-term integrity of data stored electronically is not compromised. If data media, data formats, hardware or software of archiving systems (not the data collection systems) change during the archiving period, the test facility management should ensure that there is no negative influence on the accessibility, readability and integrity of the archived data. The continuing ability to retrieve the data should be ensured and tested. Where problems with long-term access to data are envisaged or when computerised systems have to be retired, procedures for ensuring continued readability of the data should be established. This may, for example, include producing hard copy printouts or converting data to a different format or transferring data to another system. If migration of data including conversion to a different data format or printing is relevant, the requirements of this guidance for data migration should be met. Risk assessment, change control, configuration management and testing regime should be considered as relevant standard procedures when changes in the archiving system are required. As content and meaning of any electronic data should be preserved during the archiving period, the complete information package should be identified and archived (e.g. raw data, meta-data necessary to understand correctly the meaning of a record or to reconstruct its source, electronic signatures, audit trails, etc.).	114. 電子的に保存されるデータの完全性が長期にわたって損なわれることのないようにするための手順を設定しなければならない。アーカイブシステム（データ収集システムではない）のデータ媒体、データ形式、ハードウェア又はソフトウェアがアーカイブ期間中に変更される場合、運営管理者は、保管されているデータのアクセスしやすさ、見読性及び完全性に悪影響が及ばないことを確実にするべきである。データが継続的にリトリーブできることを確実にし、これをテストするべきである。データへの長期間にわたるアクセスに関する問題が予想される場合、あるいはコンピュータ化システムを廃止しなければならない場合､データが確実に、継続的に読み取れるように手順を設定しなければならない。例えば、ハードコピープリントアウトの作成、データ形式の変換、別のシステムへのデータ転送などがある。異なるデータ形式への変換や印刷を含むデータの移行が関係する場合、データ移行に関する本ガイダンスの要件を満たすべきである。アーカイブシステムにおける変更が必要になる場合、リスクアセスメント、変更管理、構成マネジメント及びテスト実施体制を関係標準手順として考慮するべきである。アーカイブ期間中に電子データの内容と意味が失われないようにするべきなので、情報一式を特定し､保管しなければならない（例えば、生データ、記録の意味を正確に理解するため、又はその出所、電子署名、監査証跡などを復元するために必要なメタデータ）。

115. If an electronically signed record is archived electronically, its integrity should be ensured for the relevant time period. The verification of the integrity of the signed record, the supporting metadata and the electronic signature should be possible and subjected to evaluation within the archiving period. The periodicity of the evaluation should be justified by the test facility management based on risk assessment.	115. 電子的に署名された記録が電子的にアーカイブされる場合、その完全性がアーカイブ期間中確保されるべきである。署名された記録、補助メタデータ及び電子署名の完全性についての確認を可能とすべきであり、その確認結果はアーカイブ期間内に評価されるべきである。評価の頻度は運営管理者がリスクアセスメントに基づいて正当化するべきである。
116. In the study report, the study director should identify all GLP-relevant electronic data which are subject to electronic archiving and the location of the electronic archive.	116. 試験報告書において、試験責任者は電子アーカイブの対象となる全ての GLP 関連電子データと電子的アーカイブの区域を特定するべきである。
117. Any data held in support of relevant computerised systems, such as source code, development, validation, operation, maintenance and monitoring records, should be held for at least as long as study records associated with these systems.	117. ソースコード、開発、バリデーション、操作、保守管理及びモニター記録など、当該コンピュータ化システムをサポートするために保持されている全てのデータは、少なくとも当該システムと関係する試験記録と同じ期間は保持されるべきである。
118. No electronically stored data should be destroyed without test facility management and, where applicable, the sponsor's authorisation and relevant documentation.	118. 電子的に保存されていないデータは、運営管理者並びに該当する場合には試験委託者の許可なしに、また関連する文書記録なしに廃棄してはならない。
3.12 Business continuity and disaster recovery 119. Provisions should be made to ensure the continuity of support for computerised systems which are used for GLP-relevant processes in the event of a system breakdown (e.g. a manual data entry or alternative computerised system). The time required to bring the alternative arrangements into use should be based on a risk assessment which should be appropriate for a particular system and the business process it supports. These arrangements should be adequately documented and tested.	**3.12 事業継続と災害復旧** 119. システム故障発生の際、GLP 関連プロセスに使用されているコンピュータ化システムのサポートが確実に継続できる対策がとられているべきである（例えば、手動データ入力や代替コンピュータ化システム）。代替手段を発動させるために要する時間は、所定のシステムとこれがサポートするビジネスプロセスに適したリスクアセスメントに基づいて検討するべきである。こうした手段については適切に文書化し、テストするべきである。

120. Procedures should be in place describing the measures to be taken in the event of partial or total failure of a computerised system. Measures may range from planned hardware redundancy to transition back to an alternative system. All contingency plans need to be well documented and validated and they should ensure continued data integrity and that the study is not compromised in any way. GLP personnel should be aware of such contingency plans.	120. コンピュータ化システムの部分的障害又は全面的障害が発生した場合に講じられる対策を説明した手順書を用意しておくべきである。この対策はハードウェアの冗長性計画から代替システムへの移行まで多岐にわたる。全ての緊急時対応計画は、十分に文書化してバリデートされる必要があり、データの継続的な完全性を確保し、決して試験に支障を来すことのないものでなければならない。GLP 職員はこのような緊急時対応計画について認識しておくべきである。
121. Procedures for the recovery of a computerised system should depend on the criticality of the system, but it is essential that original or back-up copies of all software in the version relevant for the validated computerised system are maintained, escrowed, or available by service level agreement. If recovery procedures entail changes to hardware or software, the validation requirements of this guidance apply.	121. コンピュータ化システムの復旧手順はシステムの重要度に応じたものにするべきであるが、バリデートされたコンピュータ化システムに関係するバージョンの全てのソフトウェアのオリジナルないしバックアップコピーが、サービスレベルアグリーメントによって維持されるか、預託されるか、あるいは利用可能であることが必須である。復旧手順がハードウェア又はソフトウェアの変更を伴うものである場合、本ガイダンスのバリデーション要件が適用される。
122. Where an alternative data capturing procedure is applied, if the manually recorded data is subsequently entered into the computer it should be clearly identified as such. The data entry process should be validated and there should be a statement that entered data is equivalent to the manually recorded raw data. The manually recorded raw data should be retained as the original record and archived as such. The full retention period of the manually recorded raw data is required. Alternative back-up procedures should serve to minimise the risk of any data loss and ensure that these alternative records are retained.	122. 代替データ取込み手順が適用され，手作業で記録されたデータがその後コンピュータに入力された場合は、このことを明確にしておくべきである。データ入力プロセスはバリデートされ、入力されたデータは手作業で記録された生データと同じであるという陳述書が必要である。手作業で記録された生データはオリジナルの記録として扱われ、オリジナルの記録としてアーカイブされるべきである。手作業で記録された生データの十分な保存期間が必要である。代替バックアップ手順によってデータ損失のリスクを最小限に抑えられるようにし、代替記録が確実に保存されるようにするべきである。

4. RETIREMENT PHASE	4. 廃止段階
123. The system retirement should be considered as a system life cycle phase. It should be planned, risk based and documented. If migration or archiving of GLP-relevant data is necessary, risks to data should be excluded and the requirements of this guideline apply.	123. システム廃止をシステムのライフサイクルの一つの段階とみなすべきである。廃止は計画され、リスクベースで検討され、文書化されるべきである。GLP 関連データの移行又はアーカイブが必要な場合はデータへのリスクを排除するべきであり、本ガイダンスの要件が適用される。

5. REFERENCES	5. 参考文献
"Good Practices for Computerised Systems in Regulated GxP Environments" [effective 25.09.2007] PIC/S PI 11-3	規制対象GxP環境におけるコンピュータ化システムのための適正実施基準［2007 年 9 月 25 日発効］PIC/S PI 11-3
"Computerised Systems used in Nonclinical Safety Assessment: Current Concepts in Validation and Compliance" [published 2008, DIA, Red Apple II]."	非臨床安全性評価において使用されるコンピュータ化システム：バリデーション及び規制適合における最新概念［2008 年発行、DIA, Red Apple II］
"GAMP 5 - A Risk Based Approach to Compliant GxP Computerised Systems" ISPE Good Automated Manufacturing Practice © ISPE 2007	GAMP 5 -コンピュータ化システムの GxP 適合へのリスクベースアプローチ)" ISPE Good Automated Manufacturing Practice © ISPE 2007
"Establishment and Control of Archives that Operate in Compliance with the Principles of GLP", [ENV/JM/MONO(2007)10], OECD GLP Advisory Document Number 15.	GLP 原則遵守下に運営される資料保存施設の設置及び管理［ENV/JM/MONO(2007)10］, OECD GLP アドバイサリー文書 No. 15
The rules governing medicinal products in the European Union. Volume 4 - Guidelines for good manufacturing practices for medicinal products for human and veterinary use. Annex 15 to the EU Guide of GMP "Qualification and Validation" October 2015.	欧州連合で医薬品に適用される規則。Volume 4 - 人体用及び動物用医薬品の GMP に関するガイドライン。EU GMP「適格性評価及びバリデーション」ガイド、アネックス 15）2015 年 10 月。

Appendix 1: Roles and Responsibilities

Role	Responsibility
Business Process Owner	The individual or organisation responsible for providing the resources for a business process (e.g. a preclinical trial)
IT Personnel	Personnel involved in the purchase, installation and maintenance of a computerised system. Responsibility includes, for example, operating and maintaining the hardware and software, conducting backups, resolving problems, etc.
Personnel	Any person involved in validation, operation or support of a computerised system.
Quality Assurance	(See ENV/MC/CHEM(98)17 "OECD Principles of GLP", (1997), 2.2.8.)
Sponsor	(See ENV/MC/CHEM(98)17 "OECD Principles of GLP", (1997), 2.2.5.)
Study Director	(See ENV/MC/CHEM(98)17 "OECD Principles of GLP", (1997), 2.2.6.)
Supplier	Third parties, vendors, internal IT departments, service providers including hosted service providers, etc.

別紙 1：役割と責任

役割	責任
ビジネスプロセスオーナ	ビジネスプロセス（例えば、前臨床試験）のための資源提供の責任を負う個人又は組織。
IT 担当者	コンピュータ化システムの購入、据付及び保守管理に携わる担当者。責任には例えば、ハードウェア及びソフトウェアの運用・保守、バックアップの実施、問題解決などが含まれる。
担当者	コンピュータ化システムのバリデーション、運用又はサポートに携わる人。
信頼性保証	（ENV/MC/CHEM(98)17「OECD GLP 原則」、(1997 年)、2.2.8.参照）
試験委託者	（ENV/MC/CHEM(98)17「OECD GLP 原則」、(1997 年)、2.2.5.参照）
試験責任者	（ENV/MC/CHEM(98)17「OECD GLP 原則」、(1997 年)、2.2.6.参照）
サプライヤ	サードパーティ、ベンダー、内部 IT 部門、ホスティングサービスプロバイダを含むサービスプロバイダなど。

System Owner / IT Owner	The individual who is responsible for the availability, support and maintenance of a system and for the security of the data residing on that system. The system owner is responsible for ensuring that the computerised system is supported and maintained in accordance with applicable procedures. The System Owner acts on behalf of the test facility management. Global IT systems may have a global system owner and local system owners to manage local implementation (see GAMP 5).	システムオーナ／IT オーナ	システムの利用可用性、サポート、保守管理に対して、並びに当該システムにあるデータのセキュリティに対して責任を負う個人。システムオーナは、コンピュータ化システムが適用手順書に従ってサポートされ保守されることを確実にする責任を負う。システムオーナは運営管理者の代理を務める。グローバル IT システムの場合、グローバルシステムオーナとローカルの実装を管理するローカルシステムオーナが置かれることもある（GAMP 5 参照）。
Test facility management	(See ENV/MC/CHEM(98)17 “OECD Principles of GLP”, (1997), 2.2.3.)	運営管理者	（ENV/MC/CHEM(98)17「OECD GLP 原則」、(1997 年)、2.2.3.参照）
User	The personnel operating the computerised system in a GLP study.	ユーザ	GLP 試験においてコンピュータ化システムを操作する者。
Validation Director	A delegated person responsible for a validation project.	バリデーション責任者	バリデーションプロジェクトの責任者。

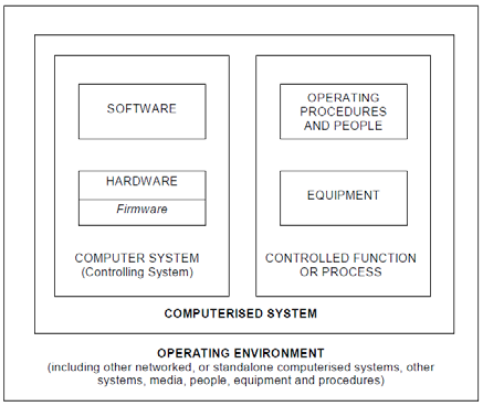
Appendix 2: Glossary

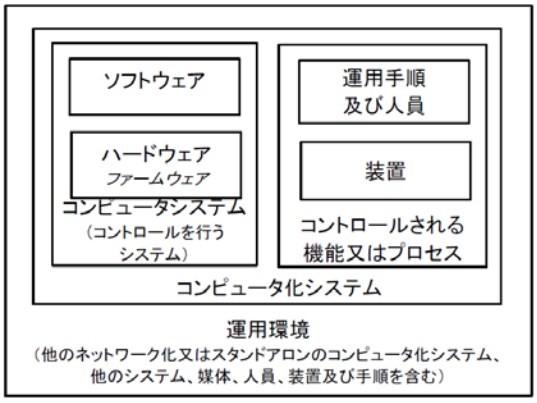
Term	Definition
Acceptance Criteria	The documented criteria that should be met to successfully complete a test phase or to meet delivery requirements.
Acceptance testing	Formal testing of a computerised system in its anticipated operating environment to determine whether all acceptance criteria of the test facility have been met and whether the system is acceptable for operational use.
Authorisation concept	An authorisation concept is a formal procedure to define and control access rights to and privileges in a computerized system.
Back-up	Provisions made for the recovery of data files or software, for the restart of processing, or for the use of alternative computer equipment after a system failure or disaster.
Change Control	Ongoing evaluation and documentation of system operations and changes to determine whether a validation process is necessary following any changes to the computerised system.

別紙 2：用語解説

用語	定義
受入基準	テスト段階を正常に完了させるために、又は引渡し要件を満たすために、満たすべき文書化された基準。
受入テスト	コンピュータ化システムについての、試験施設の受入基準が全て満たされているかどうか、並びにシステムが実運用での使用にふさわしいかどうかを判定するための、予想される運用環境での正式なテスト。
権限の認定コンセプト	権限の認定コンセプトとはコンピュータ化システムへのアクセス権及びコンピュータ化システムにおける権限を定義し、管理するための正式な手順である。
バックアップ	システム障害又は災害発生後の、データファイル又はソフトウェアの復旧、処理の再開、又は代替コンピュータ装置の使用のために行われる準備。
変更管理	コンピュータ化システムの変更に伴い、バリデーションプロセスが必要かどうか判定するための、システム運用及び変更についての継続的な評価と文書化。

Change Management	Change management is the process of controlling the life cycle of changes.	変更マネジメント	変更マネジメントは変更のライフサイクルを管理するプロセスである。
Commercial off-the-shelf (COTS) product	Software or hardware is a commercial off-the-shelf (COTS) product if provided by a vendor to the general public, if available in multiple and identical copies, and if implemented by the test facility management without or with some customization.	市販の既製品（COTS）	ソフトウェア又はハードウェアで、ベンダーによって一般の人々に提供される場合、同一のものが複数入手できる場合、またカスタマイズなし若しくは少しマスタマイズして運営管理者によって実装される場合は、市販の既製品（COTS）である。
Computerised System	“A computerized system is a function (process or operation) integrated with a computer system and performed by trained personnel. The function is controlled by the computer system. The controlling computer system is comprised of hardware and software. The controlled function is comprised of equipment to be controlled and operating procedures performed by personnel.” *PIC/S PI 11-3 “Good Practices for Computerised Systems in Regulated GxP Environments*”	コンピュータ化システム	「コンピュータ化システムとは、コンピュータシステムと一体化し、訓練を受けた者によって実行される機能（プロセス又は操作）である。その機能はコンピュータシステムによってコントロールされる。コントロールを行うコンピュータシステムはハードウェアとソフトウェアで構成される。コントロールされる機能はコントロールされる装置と担当者によって実行される運用手順で構成される。」PIC/S PI 11-3 規制対象GxP環境におけるコンピュータ化システムのための適正実施基準





Configuration	A configuration is an arrangement of functional units and pertains to the choice of hardware, software and documentation. It affects function and performance of the system.	構成設定	構成設定とは機能単位の配置であり、ハードウェア、ソフトウェア及び文書の選択に関係する。システムの機能や性能に影響する。
Configuration Management	Configuration management comprises those activities necessary to be able to precisely define a computerised system at a certain time point.	構成マネジメント	構成マネジメントは所定の時点におけるコンピュータ化システムを正確に定義できるようにするために必要な活動から成る。
Controlled function	Is a process or operation integrated with a computer system and performed by trained people.	コントロールされる機能	コンピュータシステムと一体化した、訓練を受けた人によって実行されるプロセス又は操作である。
Corrective and Preventive Actions	The concept of corrective and preventive actions focusses on the systematic investigation of the root causes of identified problems or risks in an attempt to prevent their recurrence or to prevent occurrence.	是正措置及び予防措置	是正措置及び予防措置の概念は、特定された問題ないしリスクの発生や再発を防止するために、その根本原因の体系的調査に焦点が絞られる。
Customized computerised system	A computerised system individually designed to suit a specific business process.	カスタマイズされたコンピュータ化システム	特定のビジネスプロセスに合わせて個別に設計されたコンピュータ化システム。

Data (derived data)	Derived data depend on raw data and can be reconstructed from raw data (e.g., final concentrations as calculated by a spreadsheet relying on raw data, result tables as summarized by a LIMS, etc.).	データ（派生データ）	派生データは生データに依存し、生データから再構築することができる（例えば、生データに依存してスプレッドシートによって計算された最終濃度、LIMS によって要約された結果表など）。
Data (raw data)	Data (raw data) may be defined as measurable or descriptive attribute of a physical entity, process or event. The GLP Principles define raw data as all laboratory records and documentation, including data directly entered into a computer through an automatic instrument interface, which are the results of primary observations and activities in a study and which are necessary for the reconstruction and evaluation of the report of that study.	データ（生データ）	データ（生データ）は物理的実体、プロセス又は事象の測定可能な特性又は説明的特性として定義することができる。GLP 原則では生データについて、試験における主要な観察及び活動の結果であり、当該試験の再現及び報告書評価のために必要な、自動装置インターフェースを通じてコンピュータに直接入力されるデータを始めとする、全ての試験室記録及び文書として定義している。
Data approval	Data approval means locking data after collection, verification and e.g. transformation to make data suitable for use in records.	データ承認	データ承認とは、収集、確認、そして例えば、データを記録として使用するのに適したものにするための変換後に、データをロックすることを意味する。
Data capture	Data capture are actions that typically take place to plan, collect, and verify data and associated metadata elements.	データ取込み	データ取込みとは、データと関連メタデータ要素を計画し、収集し、確認するために一般に行われる活動である。

Data migration	Data migration is the activity of e.g. transporting electronic data from one computer system to another, transferring data between storage media or simply the transition of data from one state to another [e.g. conversion of data to a different format]. The term “data” refers to “raw data” as well as “metadata”.	データ移行	データ移行とは、例えば、あるコンピュータシステムから別のコンピュータシステムへの電子データの伝送、記録媒体間のデータの転送という活動、若しくはある状態から別の状態へのデータの単純な推移（例えば、異なる形式へのデータの変換）である。「データ」という語は「生データ」及び「メタデータ」のことを指す。
Deviation (incident) management	Deviation (incident) management comprises those activities to identify, document, evaluate and when appropriate, investigate in order to determine the originating causes of deviation (incident) to prevent recurrence.	逸脱（インシデント）管理	逸脱（インシデント）管理は、逸脱（インシデント）の発生原因を判定して再発を防止するために、特定、文書化、評価及び必要に応じて、調査を行う活動から成る。
Electronic record	Any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.	電子記録	コンピュータシステムによって作成、修正、維持、アーカイブ、リトリーブ、又は配布される、デジタル形式でのテキスト、グラフィクス、データ、音声、画像、又はその他の情報表現のあらゆる組合せ。
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.	電子署名	特定のデータ入力の承認、許可又は確認を示すために手書きの署名又はイニシャルに代えることのできる電子的手段。

Hybrid solution (system)	Co-existence of paper and electronic record and signature components. Examples include combinations of paper (or other non-electronic media) and electronic records, paper records and electronic signatures, or handwritten signatures linked to electronic records.	ハイブリッドソリューション（システム）	紙の記録と電子記録及び署名要素の共存。例として、紙（又はその他の非電子媒体）の記録と電子記録、紙の記録と電子署名の組合せ、又は電子記録に関連付けられる手書き署名などがある。
Life cycle	An approach to computerised system development that begins with identification of the user's requirements, continues through design, integration, qualification, user validation, control and maintenance, and ends when use of the system is retired.	ライフサイクル	コンピュータ化システムの開発に対するアプローチで、ユーザの要求事項の特定から始まり、設計、統合、適格性評価、ユーザバリデーション、コントロール及び保守管理と続き、システムが廃止される時点で終了する。
Life cycle model	A life cycle model describes the phases or activities of a project from conception until the product is retired. It specifies the relationships between project phases, including transition criteria, feedback mechanisms, milestones, baselines, reviews, and deliverables.	ライフサイクルモデル	ライフサイクルモデルとは、構想から製品のリタイアまでのプロジェクトの諸段階又は活動を表すものである。移行基準、フィードバックメカニズム、マイルストン、ベースライン、レビュー及び成果物を始めとする、各プロジェクト段階の関係性が定められる。

Metadata	Metadata is data about data. Metadata is any information used for the identification, description, and relationships of electronic records or their elements. Metadata gives data meaning, provides context, defines structure, and enables retrievability across systems, and usability, authenticity, and auditability across time.	メタデータ	メタデータとはデータに関するデータである。メタデータは電子記録又はその要素の識別、説明及び関係性のために使用される情報である。メタデータはデータに意味を与え、コンテキストを提供し、構造を規定し、システム横断的に検索を可能にし、時間を越えて使用でき、真正であることを確実にし、監査を可能にする。
Operating System	A programme or collection of programmes, routines and sub-routines that controls the operation of a computer. An operating system may provide services such as resource allocation, scheduling, input/output control, and data management.	オペレーティングシステム	コンピュータの動作をコントロールする、プログラム又はプログラム、ルーチン及びサブルーチンの集合。オペレーティングシステムはリソース配分、スケジューリング、入出力制御、データ管理などのサービスを提供できる。
Peripheral Components	Any interfaced instrumentation, or auxiliary or remote components such as printers, modems and terminals, etc.	周辺機器	インターフェース接続された計測機器、又はプリンタ、モデム、端末などの補助機器ないし通信回線を介して利用可能なコンポーネントなど。
Process	A process is a series of actions designed to produce a specified result. A process defines required activities and the responsibilities of the personnel assigned to do the work. Appropriate tools and equipment, procedures and methods define the tasks and relationships between the tasks.	プロセス	プロセスとは指定の結果を出すために策定される一連の行動である。プロセスでは必要な活動と作業を担当する者の責任が規定される。適切なツール、手順及び方法によって任務及び各任務の関係性が決まる。

Qualification	Action of proving that any equipment including software operates correctly and is fit for its purpose.	適格性評価	ソフトウェアを含む設備が正確に稼働し、その目的に適合していることを証明する活動。
Recognised Technical Standards	Standards as promulgated by national or international standard setting bodies (ISO, IEEE, ANSI, etc.)	認証技術規格	国家ないし国際基準策定機関（ISO、IEEE、ANSIなど）によって公布される規格。
Regulated record	Is one required to be maintained or submitted by GLP regulations. A regulated record may be held in different formats, for example, electronic, paper, or both.	規制対象記録	GLP 規制によって維持又は提出を義務付けられるもの。規制対象記録は様々な形で、例えば電子形式、紙、又は両方の形式で保持することができる。
Risk	Combination of the probability of occurrence of harm and the severity of that harm.	リスク	危害の発生する確率とそれが顕在化した場合の重大性の組合せ。
Risk analysis	Estimation of the risk associated with the identified hazards. It is the qualitative or quantitative process of linking the likelihood of occurrence and severity of harms.	リスク分析	特定されたハザードに関係するリスクの推定。危害の発生する可能性と重大性を結び付ける定性的ないし定量的プロセスである。
Risk assessment	Risk assessment consists of the identification of hazards and the analysis and evaluation of risks associated with exposure to those hazards. Risk assessment is followed by risk control.	リスクアセスメント	リスクアセスメントは、ハザードの特定と、そのハザードへの曝露に伴うリスクの分析及び評価で構成される。リスクアセスメントに続いてリスクコントロールが行われる。
Risk control	Process through which decisions are reached and protective measures are implemented for reducing risks to, or maintaining risks within, specified levels.	リスクコントロール	リスクを指定の水準まで下げるか、指定の水準の範囲内に維持するための決定に至り、保護対策が実施されるプロセス。

Risk identification	A systematic use of information to identify hazards referring to the risk question or problem description. Information can include historical data, theoretical analysis, informed opinions, and the concerns of stakeholders.	リスク特定	リスクに関する質問又は問題点の記述を参照してハザードを特定するために情報を体系的に使用すること。情報には履歴データ、理論的分析、情報に基づいた意見、ステークホルダの懸念事項などがある。
Risk management	The concept of quality risk management is described as “a systematic process” for the assessment, control, communication and review of risks to the quality.	リスクマネジメント	品質リスクマネジメントという概念は、品質に対するリスクのアセスメント、コントロール、コミュニケーション及びレビューのための「系統的プロセス」として表される。
Risk mitigation	Actions taken to lessen the probability of occurrence of harm and the severity of that harm.	リスク軽減	危害の発生する確率とそれが顕在化した場合の重大性を低下させるためにとられる活動。
Security	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 and logical protection of computer installations.	セキュリティ	コンピュータのハードウェア及びソフトウェアを、偶発的又は悪意のあるアクセス、使用、変更、破壊又は開示から保護すること。セキュリティは担当者、データ、通信、並びにコンピュータ装置の物理的及び論理的保護にも関係する。
Software	A programme acquired for or developed, adapted or tailored to the test facility requirements for the purpose of controlling processes, data collection, data manipulation, data reporting and/or archiving.	ソフトウェア	プロセス制御、データ収集、データ操作、データ報告及び／又はアーカイブを目的として、試験施設のために取得され、試験施設の要件に合わせて開発又は適合させたプログラム。

Source Code	An original computer programme expressed in human-readable form (programming language) which must be translated into machine-readable form before it can be executed by the computer.	ソースコード	機械可読形式に変換してからでないとコンピュータによって実行することのできない、人が読める形式（プログラミング言語）で表現されたオリジナルコンピュータプログラム。
User requirement specifications	User requirement specifications define in writing what the user expects the computerised system to be able to do.	ユーザ要求仕様書	ユーザ要求仕様書は、ユーザが期待する、コンピュータ化システムが可能とすることを書面で定義したものである。
User review	Review of user access rights and privileges	ユーザレビュー	ユーザのアクセス権及び特権についてのレビュー。
Validation	Action of proving that a process leads to the expected results. Validation of a computerised system requires ensuring and demonstrating the fitness for its purpose.	バリデーション	プロセスが期待される結果に至ることを証明する活動。コンピュータ化システムのバリデーションにおいては、その目的への適合を確保し、証明することが必要になる。
Validation strategy	The validation strategy defines in a document the process and all activities related to each stage of validation of computerised system.	バリデーション戦略	バリデーション戦略は、コンピュータ化システムのバリデーションの各段階に関係するプロセスと全ての活動を文書で定義したものである。
Further definitions of terms can be found in the "OECD Principles of Good Laboratory Practice."		用語についてのさらなる定義は「OECD GLP 原則」に記載されている。	

一般社団法人日本 QA 研究会 GLP 部会
第 3 分科会

2016 年 8 月作成

GLP 原則及び適合性モニタリングに関する OECD シリーズ
No.17
GLP 原則のコンピュータ化システムへの適用
英文・和訳 対比表

原著（英語）は OECD から以下のタイトルで公開されている。
OECD (2016), Application of GLP Principles to Computerised Systems, OECD Series on Principles of Good Laboratory Practice (GLP) No. 17,
http://www.oecd.org/chemicalsafety/testing/oecdseriesonprinciplesofgoodlaboratorypracticeglpandcompliancemonitoring.htm

一般社団法人日本 QA 研究会
〒108-0073　東京都港区三田 1-4-28
三田国際ビル 6 階
TEL：03-6435-2118　FAX：03-6435-2119