OECD Series on Principles of Good Laboratory Practice and Compliance Monitoring

No. 10　The Application of the Principles of GLP to Computerised Systems (1995)

GLP 原則のコンピュータ・システムへの適用

英文・和訳　対比表

英文	和訳
Throughout recent years there has been an increase in the use of computerised systems by test facilities undertaking health and environmental safety testing. These computerised systems may be involved with the direct or indirect capture of data, processing, reporting and storage of data, and increasingly as an integral part of automated equipment. Where these computerised systems are associated with the conduct of studies intended for regulatory purposes, it is essential that they are developed, validated, operated and maintained in accordance with the OECD Principles of Good Laboratory Practice (GLP).	近年、健康および環境に関わる安全性試験を行う試験施設によって、コンピュータ・システムの利用が増加している。これらのコンピュータ・システムは、直接的あるいは間接的なデータ収集、処理、報告、データ保管に関わっており、自動化された機器の不可分の一部として急速に普及してきている。コンピュータ・システムは、規制目的を対象とした試験の実施に関連する場合、OECD の GLP 原則に従って開発、検証、操作、保守管理されることが必要である。
Scope All computerised systems used for the generation, measurement or assessment of data intended for regulatory submission should be developed, validated, operated and maintained in ways which are compliant with the GLP Principles. During the planning, conduct and reporting of studies there may be several computerised systems in use for a variety of purposes. Such purposes might include the direct or indirect capture of data from automated instruments, operation/control of automated equipment and the processing, reporting and storage of data. For these different activities, computerised systems can vary from a programmable analytical instrument, or a personal computer to a laboratory information management system (LIMS) - with multiple functions. Whatever the scale of computer involvement, the GLP Principles should be applied.	範囲 当局への提出を目的としたデータの作成、測定あるいは評価に使用されるコンピュータ・システムはすべて、GLP 原則に準拠した方法で開発、検証、操作、保守管理されなければならない。 試験の計画、実施、報告において、種々の目的のためにいくつかのコンピュータ・システムが使用されることがある。そのような目的には、自動機器からの直接的あるいは間接的なデータの取り込み、自動機器の操作・管理およびデータの処理、報告、保管などがある。このように業務は多岐にわたるため、コンピュータ・システムは、プログラム可能な分析機器もしくはパーソナルコンピュータから多機能の実験室情報管理システム（LIMS）まで多彩である。コンピュータが関わる規模に関係なく、GLP 原則は適用されなければならない。
Approach Computerised systems associated with the conduct of studies destined for regulatory submission should be of appropriate design, adequate capacity and suitable for their intended purposes. There should be appropriate procedures to control and maintain these systems, and the systems should be developed, validated and operated in a way which is in compliance with the GLP Principles. The demonstration that a computerised system is suitable for its intended purpose is of fundamental importance and is referred to as computer validation.	取り組み 当局への提出を予定した試験の実施に関わるコンピュータ・システムは、適切に設計され、十分な能力を持ち、意図した目的に適したものでなければならない。これらのシステムを管理し維持するための適切な手順がなければならないし、また、これらのシステムは GLP 原則に準拠した方法で開発、検証、操作されなければならない。 コンピュータ・システムが、意図した目的に適していると示すことが重要な基本原則であり、それをコンピュータによる検証という。

The validation process provides 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.	一連の検証行為は、コンピュータ・システムが所定の仕様に適合していることを高度に保証するものである。検証は、正式な検証計画書に基づき、実際の使用に先立って実行されなければならない。
The Application of the GLP Principles to Computerised Systems The following considerations will assist in the application of the GLP Principles to computerised systems outlined above : 1. Responsibilities a) *Management* of a test facility has the overall responsibility for compliance with the GLP Principles. This responsibility includes the appointment and effective organisation of an adequate number of appropriately qualified and experienced staff, as well as the obligation to ensure that the facilities, equipment and data handling procedures are of an adequate standard. Management is responsible for ensuring that computerised systems are suitable for their intended purposes. It should establish computing policies and procedures to ensure that systems are developed, validated, operated and maintained in accordance with the GLP Principles. Management should also ensure that these policies and procedures are understood and followed, and ensure that effective monitoring of such requirements occurs. Management should also 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. b) *Study Directors* are responsible under the GLP Principles for the overall conduct of their studies. Since many such studies will utilise computerised systems, it is essential that Study Directors are fully aware of the involvement of any computerised systems used in studies under their direction. The Study Director's responsibility for data recorded electronically is the same as that for data recorded on paper and thus only systems that have been validated should be used in GLP studies.	GLP 原則のコンピュータ・システムへの適用 以下は、上記で概要を述べたコンピュータ・システムへのGLP原則の適用に役立つ事項である。 1. 責任 a) 試験施設の運営管理者は、GLP 原則の準拠に全般的な責任を持つ。この責任には、施設、機器、データの取り扱い手順が十分な水準にあることを保証する責任と共に、適切な資格を持った経験のある職員を十分な人数任命し、効果的に組織化することも含まれる。 運営管理者は、コンピュータ・システムが、意図した目的に適したものであることを保証する責任がある。運営管理者は、コンピュータに関する方針と手順を確立し、システムがGLP原則どおりに開発、検証、操作、保守管理されることを保証しなければならない。運営管理者はまた、これらの方針や手順が理解され遵守されていること、および、当該必要事項が効果的に監視されていることを保証しなければならない。 さらに運営管理者は、コンピュータ・システムの開発、検証、操作、保守管理について特定の責任を持つ職員を指名しなければならない。それらの職員は業務に関連した経験を持ち、GLP 原則に準拠して業務を行うべく適切な訓練を受けた適当な有資格者でなければならない。 b) 試験責任者はGLP原則の下、試験実施の全般的な責任を負う。これらの試験の多くはコンピュータ・システムを使用しているので、試験責任者は、自らの指示の下に行われる試験で使用されるすべてのコンピュータ・システムの関与について、熟知していることが重要である。 電子的に記録されたデータに関する試験責任者の責任は、紙に記録されたデータに関する責任と同じであり、したがってGLP試験では、検証されたシステムだけを使用しなければならない。

c) *Personnel*. All personnel using computerised systems have a responsibility for operating these systems in compliance with the GLP Principles. Personnel who develop, validate, operate and maintain computerised systems are responsible for performing such activities in accordance with the GLP Principles and recognized technical standards.	c) 職員。 コンピュータ・システムを使用する職員はすべて、それらのシステムを GLP 原則に準拠して操作する責任を負う。コンピュータ・システムを開発、検証、操作、保守管理する職員は、それらの業務を GLP 原則および認知されている技術水準に従って実施する責任がある。
d) *Quality Assurance* (QA) responsibilities for computerised systems must be defined by management and described in written policies and procedures. The quality assurance programme should include procedures and practices that will assure that established standards are met for all phases of the validation, operation and maintenance of computerised systems. It should also include procedures and practices for the introduction of purchased systems and for the process of in-house development of computerised systems. Quality Assurance personnel are required to monitor the GLP compliance of computerised systems and should be given training in any specialist techniques necessary. They should be sufficiently familiar with such systems so as to permit objective comment; in some cases the appointment of specialist auditors may be necessary. QA personnel should have, for review, direct read-only access to the data stored within a computerised system.	d) コンピュータ・システムに対する信頼性保証（QA）の責任は、運営管理者によって定義され、文書化された方針および手順の中で示されなければならない。信頼性保証プログラムには、コンピュータ・システムの検証、操作、維持のすべての段階において、確立された基準を満たしていることを保証する手順と実行を含むべきである。また、その信頼性保証計画の中には、購入したシステムの導入およびシステムを自社で開発する過程についての手順や実行を含めるべきである。 信頼性保証担当者は、コンピュータ・システムの GLP 適合性を調査することを求められ、専門家として必要な技術に関し訓練を受けなければならない。信頼性保証担当者は、客観的な意見ができるよう、そのシステムに十分に習熟していなければならない。場合によっては専門監査員の任命が必要である。 信頼性保証担当者は、調査のため、コンピュータ・システムに保存されたデータに、読み取り専用で直接にアクセスできなければならない。
2. <u>Training</u> The GLP Principles require that a test facility has appropriately qualified and experienced personnel and that there are documented 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 above provisions should also apply for all personnel involved with computerised systems.	2. <u>訓練</u> 試験施設には適切な資格と経験を持った職員がおり、実地訓練および必要であれば外部の訓練コースへの参加を含む文書化された訓練プログラムが存在することを GLP 原則で求めている。それらの訓練の記録はすべて保存されなければならない。 上記の規定は、コンピュータ・システムに関与するすべての職員にも適用される。
3. <u>Facilities and Equipment</u> Adequate facilities and equipment should be available for the proper conduct of studies in compliance with GLP. For computerised systems there will be a number of specific	3. <u>施設および機器</u> GLP に適合した試験を適切に実施するために、十分な施設と機器が具備されていなければならない。コンピュータ・システムに関しては、いくつかの特別な

considerations: a) *Facilities* 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. 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. b) *Equipment* i) *Hardware and Software* A computerised system is defined as a group of hardware components and associated software designed and assembled to perform a specific function or group of functions. Hardware is the physical components of the computerised system; it will include the computer unit itself and its peripheral components. Software is the programme or programmes that control the operation of the computerised system. All GLP Principles which apply to equipment therefore apply to both hardware and software. ii) *Communications* Communications related to computerised systems broadly fall into two categories: between computers or between computers and peripheral components.	配慮が必要である。 a) 施設 コンピュータのハードウェア、周辺機器、通信機器および電子記憶媒体の物理的な設置場所に対して、十分な配慮がなされなければならない。極端な温度、湿度、塵埃、電磁気的干渉および高圧ケーブルへの近接は、その装置がそのような条件下で作動するように特別に設計されたものでない限り避けるべきである。 コンピュータ機器への電力供給、および、必要に応じてコンピュータ・システムのバックアップや無停電装置にも配慮しなければならない。コンピュータ・システムの突然の停止は、試験の結果に影響するからである。 電子的保存媒体の安全な保管に対しても、適切な施設が用意されなければならない。 b) 機器 i) ハードウェアおよびソフトウェア コンピュータ・システムは、特定の、または一連の機能を実行するために設計・組み立てられた、ハードウェアの構成部分と関連するソフトウェアの一群であると定義される。 ハードウェアは、コンピュータ・システムの物理的な構成部分であり、コンピュータ本体および周辺機器を含む。 ソフトウェアは、コンピュータ・システムの操作を統御するプログラムまたはプログラム群である。 したがって、機器に適用される GLP 原則はすべてハードウェアとソフトウェアの両者に適用される。 ii) 通信 コンピュータ・システムに関連する通信は、大きく二つに分けられる。一つはコンピュータ間の通信であり、もう一つはコンピュータと周辺機器との通信であ

All communication links are potential sources of error and may result in the loss or corruption of data. Appropriate controls for security and system integrity must be adequately addressed during the development, validation, operation and maintenance of any computerised system.	る。 すべての通信回線は、エラーの発生源になる可能性があり、データの損失や破損につながる恐れがある。いかなるコンピュータ・システムの開発、検証、操作、維持においても、安全性およびシステムの完全性のための適切な管理が十分になされなければならない。
4. Maintenance and Disaster Recovery Al computerised systems should be installed and maintained in a manner to ensure the continuity of accurate performance.	4. 保守管理および障害修復 すべてのコンピュータ・システムは、継続する正確な作動が保証されるように導入、設置および保守されなければならない。
a) *Maintenance* There should be documented procedures covering both routine preventative maintenance and fault repair. These procedures should clearly detail the roles and responsibilities of personnel involved. Where such maintenance activities have necessitated changes to hardware and/or software it may be necessary to validate the system again. During the daily operation of the system, records should be maintained of any problems or inconsistencies detected and any remedial action taken.	a) 保守管理 日常の予防的な保守管理および障害修復の両者を対象とする文書化された手順が必要である。これらの手順では、関係者の役割と責任を明確に詳述しなければならない。このような保守行為によりハードウェアおよび(または)ソフトウェアの変更が必要とされた場合には、システムの検証が再度必要となる場合もあるであろう。日常のシステム操作において、発見されたいかなる問題あるいは矛盾、また取られたすべての改善措置についても、記録を保存しなければならない。
b) *Disaster Recovery* 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 a paper-based system. All contingency plans need to be well documented, validated and should ensure continued data integrity and should not compromise the study in any way. Personnel involved in the conduct of studies according to the GLP Principles should be aware of such contingency plans.	b) 障害修復 コンピュータ・システムの部分的あるいは全体的な障害に際して取るべき対策を述べた手順書がその場に存在しなければならない。その対策には、ハードウェアを二重に備える方法や紙を使用した方式に逆戻りする方法などがあるであろう。不慮の事態への対応策は、すべて十分に文書化され、検証されていなければならず、データの完全性を引き続き保証し、決して試験に影響を及ぼしてはならない。GLP 原則に従って実施される試験の従事者は、そのような不慮の事態に対する対策について周知していなければならない。
Procedures for the recovery of a computerised system will depend on the criticality of the system, but it is essential that back-up copies of all software are maintained. If recovery procedures entail changes to hardware or software, it may be necessary to validate the system again.	コンピュータ・システムの復旧の手順は、システムの危急性によって様々であるが、すべてのソフトウェアの予備用コピーを取っておくことは重要である。もし復旧の手順がハードウェアまたはソフトウェアの変更を必要とする場合は、システムの検証が再度必要である。

5. Data The GLP Principles define raw data as being all original laboratory records and documentation, including data directly entered into a computer through an instrument interface, which are the results of original observations and activities in a study and which are necessary for the reconstruction and evaluation of the report of that study.	5. データ GLP 原則では、生データを「実験の記録・文書の原本すべてであり、機器のインターフェースを通してコンピュータに直接入力されるデータを含む。それらは、試験における原観察と原活動の結果であり、その試験の報告書の評価と再構築に必要なものである」と定義している。
Computerised systems operating in compliance with GLP Principles may be associated with raw data in a variety of forms, for example, electronic storage media, computer or instrument printouts and microfilm/fiche copies. It is necessary that raw data are defined for each computerised system.	GLP 原則に準拠して操作されるコンピュータ・システムは、様々な形で生データに関わる。たとえば、電子記憶媒体、コンピュータあるいは機器のプリントアウト、マイクロフィルム/マイクロフィッシュのコピーなどである。各コンピュータ・システムにおいて、生データを定義することが必要である。
Where computerised systems are used to capture, process, report or store raw data electronically, system design should always provide for the retention of full audit trails to show all changes to the data without obscuring the original data. It should be possible to associate all changes to data with the persons making those changes by use of timed and dated (electronic) signatures. Reasons for change should be given.	コンピュータ・システムが、生データを電子的に捕獲、処理、報告、保管するために使用される場合は、すべてのデータの変更が原データを損なうことなく行われたことを示すための追跡調査ができるようなシステム設計にしなければならない。日時を示した（電子）署名によって、すべてのデータ変更を、その変更を行った人物に結びつけることが可能でなければならない。変更の理由も示されなければならない。
When raw data are held electronically it is necessary to provide for long term retention requirements for the type of data held and the expected life of computerised systems. Hardware and software system changes must provide for continued access to and retention of the raw data without integrity risks.	生データが電子的に保存される場合は、保存されるデータの型およびコンピュータ・システムの予想耐用年数に応じて、長期保存の要件に備えることが必要である。ハードウェアおよびソフトウェアのシステム変更においては、データの完全性を損なうことなく、継続的な生データへのアクセスとその保管が可能でなければならない。
Supporting information such as maintenance logs and calibration records that are necessary to verify the validity of raw data or to permit reconstruction of a process or a study should be retained in the archives.	保守管理記録や校正記録等、生データの正当性の証明あるいは過程や試験の再構築を可能にするために必要な支援情報は、資料保管施設に保存されなければならない。
Procedures for the operation of a computerised system should also describe the alternative data capture procedures to be followed in the event of system failure. In such circumstances any manually recorded raw data subsequently entered into the computer should be clearly identified as such, and should be retained as the original record. Manual back-up procedures should serve to minimise the risk of any data loss and ensure that these alternative records are retained.	コンピュータ・システムの操作手順書には、システムの故障の際に従うべきデータ収集の代替手順が記載されていなければならない。そのような状況下で手作業によって記録される生データで、その後コンピュータに入力されるものについては、どれも明確にそれとわかるようにしなければならない。また、その生データは原記録として保管されなければならない。手作業によるバックアップ手

	順は、いかなるデータ損失の危険性も最小にし、これらの代替手順による記録が保管されることを保証するものでなければならない。
Where system obsolescence forces a need to transfer electronic raw data from one system to another then the process must be well documented and its integrity verified. Where such migration is not practicable then the raw data must be transferred to another medium and this verified as an exact copy prior to any destruction of the original electronic records.	システムの老朽化により、電子的生データを一つのシステムから別のシステムへ移動しなければならない場合は、その過程を十分に文書化し、その完全性を証明しなければならない。そのような移動が実行できない場合は、生データを他の媒体に移動しなければならないが、電子的原記録を破棄する前に、これが正確なコピーであることを立証しなければならない。
6. Security Documented security procedures should be in place for the protection of hardware, software and data from corruption or unauthorised modification, or loss. In this context security includes the prevention of unauthorised access or changes to the computerised system as well as to the data held within the system. The potential for corruption of data by viruses or other agents should also be addressed. Security measures should also be taken to ensure data integrity in the event of both short term and long term system failure.	6. 安全性 ハードウェア、ソフトウェアおよびデータを破損、権限のない変更あるいは損失から守るための安全性に関する手順書が備えられていなければならない。この意味で、安全性にはシステム内に保存されているデータのみならずコンピュータ・システムへの権限のないアクセスや変更を予防することも含まれる。ウィルスやその他の要因によるデータの破損の可能性についても検討しなければならない。また、短期および長期のシステム故障の際に、データの完全性を保証するための安全対策が講じられなければならない。
a) *Physical Security* Physical security measures should be in place to restrict access to computer hardware, communications equipment, peripheral components and electronic storage media to authorised personnel only. For equipment not held within specific 'computer rooms' (e.g., personal computers and terminals), standard test facility access controls are necessary as a minimum. However, where such equipment is located remotely (e.g., portable components and modem links), additional measures need to be taken.	a) 物理的安全性 権限を有する者のみがコンピュータのハードウェア、通信機器、周辺機器および電子記憶媒体にアクセスできるよう、適切な物理的安全対策が取られていなければならない。特定の「コンピュータ室」に設置されていない機器（たとえば、パーソナルコンピュータや端末機）に対しても、最小限、試験施設における標準的なアクセス管理が必要である。しかし、そのような機器が離れたところに設置されている場合（たとえば、携帯機器やモデムの接続）には、さらに別な対策が必要である。
b) *Logical Security* For each computerised system or application, logical security measures must be in place to prevent unauthorised access to the computerised system, applications and data. It is essential to ensure that only approved versions and validated software are in use. Logical security may include the need to enter a unique user identity with an associated password. Any introduction of data or software from external sources should be controlled. These controls may be	b) 論理的安全性 各コンピュータ・システムあるいはアプリケーション・ソフトに関して、コンピュータ・システムやアプリケーション・ソフトおよびデータへの権限のないアクセスを予防するため、論理的安全対策が講じられなければならない。承認された版、検証されたソフトウェアだけが使用されていることを保証することが重要である。論理的安全性には、使用者固有の身分証明と関連する暗証番号の入力を求

provided by the computer operating system software, by specific security routines, routines embedded into the applications or combinations of the above.	める方法などがある。外部からのデータやソフトウェアの導入はすべて管理されなければならない。これらの管理には、コンピュータの基本ソフトによるもの、特定の安全プログラムによるもの、アプリケーション・ソフトに組み込まれたプログラムまたはこれらの組み合わせによるものなどがある。
c) *Data Integrity* Since maintaining data integrity is a primary objective of the GLP Principles, it is important that everyone associated with a computerised system is aware of the necessity for the above security considerations. 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.	c) データの完全性 データの完全性の維持はGLP原則の主要な目的であるため、コンピュータ・システムに関係しているすべての者が、上記の安全性への配慮の必要性を知っていることが重要である。運営管理者は、職員がデータの安全性の重要性、適切な安全性を与えることができる手順やシステムの特徴、および機密保護違反の重大さについて理解していることを保証しなければならない。そのようなシステム機能としては、システムへのアクセスの日常的な監視、ファイル検査プログラムの履行、除外および(または)傾向報告などがある。
d) *Back-up* It is standard practice with computerised systems to make back-up copies of all software and data to allow for recovery of the system following any failure which compromises the integrity of the system e.g., disk corruption. The implication, therefore, is that the back-up copy may become raw data and must be treated as such.	d) バックアップ システムの完全性を脅かすような故障(たとえば、ディスクの破損)の後にシステムを復旧させるため、すべてのソフトウェアやデータの予備用コピーを取ることは、コンピュータ・システムにおける標準的な慣行である。これはつまり、予備用コピーが生データとなる可能性があるということであり、そのように取り扱われなければならないということを示唆するものである。
7. <u>Validation of Computerised Systems</u> Computerised systems must be suitable for their intended purpose. The following aspects should be addressed:	7. <u>コンピュータ・システムの検証</u> コンピュータ・システムは、それらの意図した目的に合致したものでなければならない。以下の点が検討されなければならない。
a) *Acceptance* Computerised systems should be designed to satisfy GLP Principles and introduced in a pre-planned manner. There should be adequate documentation that each system was developed in a controlled manner and preferably according to recognised quality and technical standards (e.g. ISO/9001). Furthermore, there should be evidence that the system was adequately tested for conformance with the acceptance criteria by the test facility prior to being put into routine use. Formal acceptance testing requires the conduct of tests following a	a) 受け入れ コンピュータ・システムは、GLP原則を満たすように設計され、あらかじめ計画された方法により導入されなければならない。管理された方法で、そしてできれば広く認められた品質および技術標準(たとえば、ISO/9001 など)に従って各システムが開発されたことを十分に示す文書が必要である。さらに、日常的な使用に先立ち、そのシステムが受け入れ基準に適合していることを試験施設において十分に検査したという証拠も必要である。正式な受け入れ検査には、あ

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.	らかじめ定義された計画に従った検査の実施、およびすべての検査手順、検査データ、検査結果、検査の正式な要約および正式な受け入れの記録についての証拠文書の保管が必要である。
For vendor-supplied systems it is likely that much of the documentation created during the development is retained at the vendor's site. In this case, evidence of formal assessment and/or vendor audits should be available at the test facility.	業者によって供給されるシステムでは、開発中に作成された記録文書の多くが業者側に保管されていると思われる。この場合は、正式な評価および(または)その業者の監査についての証拠は試験施設で入手できなければならない。
b) *Retrospective Evaluation* There will be systems where the need for compliance with GLP Principles was not foreseen or not specified. Where this occurs there should be documented justification for use of the systems; this should involve a retrospective evaluation to assess suitability.	b) 遡及的評価 GLP 原則の準拠要求が予見または特定されなかったというシステムがあるであろう。このような場合、そのシステムの使用を正当化する文書記録がなければならない。その中には、システムの適合性を評価するための遡及的評価が含まれている。
Retrospective evaluation begins by gathering all historical records related to the computerised system. These records are then reviewed and a written summary is produced. This retrospective evaluation summary should specify what validation evidence is available and what needs to be done in the future to ensure validation of the computerised system.	遡及的評価は、まずコンピュータ・システムに関する過去のすべての記録を収集することから始まる。これらの記録は、その後調査され、要約文書が作成される。この遡及的評価の要約では、どのような検証の証拠が利用できるのか、そのコンピュータ・システムの検証を保証するために将来何がなされなければならないかを特定しなければならない。
c) *Change Control* Change control is the formal approval and documentation of any change to the computerised system during the operational life of the system. Change control is needed when a change may affect the computerised system's validation status. Change control procedures must be effective once the computerised system is operational.	c) 変更管理 変更管理とは、運用期間中のコンピュータ・システムへのあらゆる変更についての正式な承認と文書化のことである。コンピュータ・システムの検証状況に影響を与える場合は、変更管理が必要である。コンピュータ・システムがひとたび運用段階に入ると、変更管理の手順が有効でなければならない。
The procedure should describe the method of evaluation to determine the extent of retesting necessary to maintain the validated state of the system. The change control procedure should identify the persons responsible for determining the necessity for change control and its approval.	手順書には、システムの検証状況の維持に必要な再検査の範囲を決定するための評価方法が記載されなければならない。変更管理の手順書では、変更管理の必要性の決定、およびその承認を行う責任者を特定しなければならない。
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	変更の由来(業者あるいは自社開発のシステム)に関係なく、変更管理の過程の一部として、適切な情報が提供される必要がある。変更管理手順は、データ

procedures should ensure data integrity.	の完全性を保証しなければならない。
d) *Support Mechanism* In order to ensure that a computerised system remains suitable for its intended purpose, support mechanisms should be in place to ensure the system is functioning and being used correctly. This may involve system management, training, maintenance, technical support, auditing and/or performance assessment. Performance assessment is the formal review of a system at periodic intervals to ensure that it continues to meet stated performance criteria, e.g., reliability, responsiveness, capacity.	d) 支援機構 コンピュータ・システムが、意図した目的に対し常に適正であることを保証するため、システムが機能し正常に使用されていることを保証するための支援機構が整備されていなければならない。これには、システム管理、訓練、保守管理、技術支援、監査および(または)性能評価などが含まれる。性能評価は、定期的に行われる正式な検査であり、システムが、定められた性能基準(たとえば、信頼性、反応性、容量)を常に満たしていることを保証するためのものである。
8. Documentation The items listed below are a guide to the minimum documentation for the development, validation, operation and maintenance of computerised systems.	8. 文書化 以下の項目は、コンピュータ・システムの開発、検証、保守管理のために最低限必要な文書化についての指針である。
a) *Policies* There should be written management policies covering, *inter alia*, the acquisition, requirements, design, validation, testing, installation, operation, maintenance, staffing, control, auditing, monitoring and retirement of computerised systems.	a) 方針 コンピュータ・システムについて、とりわけ、取得、要件、設計、検証、検査、設定、操作、保守管理、職員の配属、管理、監査、監視および廃止を含む文書化された管理方針が存在しなければならない。
b) *Application Description* For each application there should be documentation fully describing:	b) アプリケーションに関する記述 各アプリケーションについて、以下のことを十分に記述した文書がなければならない。
*The name of the application software or identification code and a detailed and clear description of the purpose of the application. *The hardware (with model numbers) on which the application software operates. *The operating system and other system software (e.g., tools) used in conjunction with the application. *The application programming language(s) and/or data base tools used. *The major functions performed by the application *An overview of the type and flow of data/data base design associated with the application. *File structures, error and alarm messages, and algorithms associated with the application.	*アプリケーション・ソフトの名称または識別コード、およびそのアプリケーションの目的に関する詳細で明瞭な記述。 *アプリケーション・ソフトが作動するハードウェア(型番号を記す)。 *アプリケーションと連動して使用される基本ソフトおよびその他のシステムソフト(たとえば、種々のツール)。 *アプリケーションのプログラム言語および(または)使用されているデータベースのツール。 *アプリケーションによって実行される主要な機能 *アプリケーションに関連したデータ(データベース)設計の種類や流れの概説。 *アプリケーションに関連したファイル構造、エラー・警告メッセージおよびアルゴ

*The application software components with version numbers. *Configuration and communication links among application modules and to equipment and other systems.	リズム。 *アプリケーション・ソフトの構成（版の番号を記す）。 *アプリケーション・モジュール間の、および機器や他のシステムへの設定および通信接続。
c) *Source Code* Some OECD Member countries require that the source code for application software should be available at, or retrievable to, the test facility.	c) ソースコード OECD 加盟国の中には、アプリケーション・ソフトのソースコードが試験施設にあること、または試験施設へ回収できることを要求している国もある。
d) *Standard Operating Procedures (SOPs)* Much of the documentation covering the use of computerised systems will be in the form of SOPs. These should cover but not be limited to the following: *Procedures for the operation of computerised systems (hardware/software), and the responsibilities of personnel involved. *Procedures for security measures used to detect and prevent unauthorised access and programme changes. *Procedures and authorisation for programme changes and the recording of changes. *Procedures and authorisation for changes to equipment (hardware/software) including testing before use if appropriate. *Procedures for the periodic testing for correct functioning of the complete system or its component parts and the recording of these tests. *Procedures for the maintenance of computerised systems and any associated equipment. *Procedures for software development and acceptance testing, and the recording of all acceptance testing. *Back-up procedures for all stored data and contingency plans in the event of a breakdown. *Procedures for the archiving and retrieval of all documents, software and computer data. *Procedures for the monitoring and auditing of computerised systems.	d) 標準操作手順書（SOP） コンピュータ・システムの使用に関する文書の多くは、SOP の形式になるであろう。それらは以下の項目を含むべきであるが、これに限定されるものではない。 *コンピュータ・システム（ハードウェア/ソフトウェア）の操作手順および関係者の責務。 *非権限者のアクセスおよびプログラム変更を検出または防止するための安全対策の手順。 *プログラム変更の手順と承認および変更記録。 *機器（ハードウェア/ソフトウェア）の変更の手順と承認、適切であれば使用前の検査を含む。 *全システムあるいはその構成要素が正しく機能していることを定期的に検査する手順とこれらの検査の記録の手順。 *コンピュータ・システムおよび関連しているあらゆる機器の保守管理の手順。 *ソフトウェアの開発と受け入れ検査の手順およびすべての受け入れ検査の記録。 *全保存データのバックアップの手順および破綻時の危機管理計画。 *すべての文書、ソフトウェアおよびコンピュータ・データの保管と検索に関する手順。 *コンピュータ・システムの監視と監査の手順。
9. <u>Archives</u> The GLP Principles for archiving data must be applied consistently to all data types. It is therefore important that electronic data are stored with the same levels of access control, indexing and expedient retrieval as other types of data.	9. <u>保管施設</u> データ保管に関する GLP 原則は、あらゆる種類のデータに一貫性を持って適用されなければならない。したがって、出入管理、索引付け、適切な検索に関して、電子的データを他の種類のデータと同様なレベルで保管することが重要

	である。
Where electronic data from more than one study are stored on a single storage medium (e.g., disk or tape), a detailed index will be required.	複数の試験の電子的データが単一の保存媒体（たとえば、ディスクやテープ）に保存される場合は、詳細な索引が求められる。
It may be necessary to provide facilities with specific environmental controls appropriate to ensure the integrity of the stored electronic data. If this necessitates additional archive facilities then management should ensure that the personnel responsible for managing the archives are identified and that access is limited to authorised personnel. It will also be necessary to implement procedures to ensure that the long-term integrity of data stored electronically is not compromised. Where problems with long-term access to data are envisaged or when computerised systems have to be retired, procedures for ensuring that continued readability of the data should be established. This may, for example, include producing hard copy printouts or transferring the data to another system.	保存されている電子的データの完全性を保証するのに適した、特別に環境制御された施設を設けることが必要な場合もある。そのために新しい保管施設が必要とされる場合は、保管施設の管理責任者が特定されていること、出入が権限のある者に限定されていることを運営管理者は保証しなければならない。さらに、電子的に保管されているデータの長期にわたる完全性が損なわれないことを保証するための手段を講じることも必要である。データへの長期間のアクセスに関して問題が予想される場合、またはコンピュータ・システムを廃止しなければならない場合は、データを引き続き読み取れることを保証する手順を確立しなければならない。これには、たとえばハードコピーの印字や別のシステムへのデータ移動などが含まれる。
No electronically stored data should be destroyed without management authorization and relevant documentation. Other data held in support of computerised systems, such as source code and development, validation, operation, maintenance and monitoring records, should be held for at least as long as study records associated with these systems.	保存されているいかなる電子的データも、運営管理者の承認および関連する文書記録なしに破壊されてはならない。コンピュータ・システムを支援するための他のデータ、たとえばソースコードや開発、検証、操作、保守管理および監視の記録などは、少なくとも、それらのシステムが関与した試験記録と同じ期間保存されなければならない。
Definition of terms[1] [1]Further definitions of terms can be found in the "OECD Principles of Good Laboratory Practice".	用語の定義[1] [1]“OECD Principles of Good Laboratory Practice”には、用語のさらなる定義が掲載されている。
Acceptance Criteria: The documented criteria that should be met to successfully complete a test phase or to meet delivery requirements.	受け入れ基準：検査段階を完了し、または希望納期に間に合うことを満たすべく文書化された基準。
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	受け入れ検査：コンピュータ・システムが試験施設のすべての受け入れ基準に適合しているかどうか、またシステムが実際の使用に適しているかを、予想され

whether the system is acceptable for operational use.	る操作環境で調べる正式な検査。
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.	バックアップ:システムの故障や障害の後の、データ・ファイルやソフトウェアの復旧、データ処理の再開または代替コンピュータ機器の使用のための備え。
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.	変更管理:コンピュータ・システムの変更後、検証が必要かどうかを決定するための、システムの運用と変更に関する継続的な評価と文書化。
Computerised System: A group of hardware components and associated software designed and assembled to perform a specific function or group of functions.	コンピュータ・システム:特定の、または一連の機能を遂行するために設計され組み立てられたハードウェア部品の一群と関連ソフトウェア。
Electronic Signature: The entry in the form of magnetic impulses or computer data compilation of any symbol or series of symbols, executed, adapted or authorized by a person to be equivalent to the person's handwritten signature.	電子署名:磁気信号の形式、あるいは一つまたは一連の記号のコンピュータ・データ編集の形式での登録をいい、手書きの署名と同等に個人によって実行され、改変され、承認を与えられるもの。
Hardware: The physical components of a computerised system, including the computer unit itself and its peripheral components.	ハードウェア:コンピュータ・システムの物理的な構成要素で、コンピュータ装置自体とその周辺機器を含む。
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の機器、あるいは補助的または遠隔の接続機器で、印刷機やモデム、端末機などのこと。
Recognised Technical Standards: Standards as promulgated by national or international standard setting bodies (ISO, IEEE, ANSI, etc.)	認定された技術標準:国内または国際的基準設定機関によって推奨された標準(ISO、IEEE、ANSIなど)。
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.	安全性:偶発的な、または悪意のあるアクセス、使用、改変、破壊、開示からのコンピュータのハードウェアおよびソフトウェアの保護。さらに安全性は、職員、データ、通信、コンピュータ装置の物理的および論理的保護にも関係している。
Software (Application): 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(アプリケーション):各過程やデータの収集、操作、報告および(または)保管を管理するために入手された、または試験施設の要求にあわせて開発、改変、調整されたプログラム。

Software (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. 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. Validation of a Computerised System: The demonstration that a computerised system is suitable for its intended purpose.	ソフトウェア（基本ソフト）：コンピュータの操作を管理するプログラムまたはプログラム群、ルーチン、サブ・ルーチンのこと。基本ソフトは、資源配分、日程計画、入力/出力管理、およびデータ管理などのサービスを提供するものである。 ソースコード：人が読める形式（プログラム言語）で書かれた、コンピュータの原プログラムで、コンピュータによってそれを実行する前に機械が読み取れる形に翻訳する必要があるもの。 コンピュータ・システムの検証。コンピュータ・システムが、その意図した目的に適していることを立証すること。