OECD SERIES ON PRINCIPLES OF GOOD LABORATORY PRACTICE AND COMPLIANCE MONITORING

Number 22

Advisory Document of the Working Party on Good Laboratory Practice on GLP Data Integrity

GLP 原則及び適合性モニタリングに関する OECD シリーズ

No. 22

GLP データインテグリティに関する GLP 作業部会のアドバイザリー文書

英文・和訳対比表

日本 QA 研究会 GLP 部会 第 1 分科会

本対訳は、OECD 文書の理解を深めるために、日本 QA 研究会 GLP 部会 第 1 分科会が、第 3 分科会の協力の下で、第 15 期の活動の一環として作成したものであり、公開にあたり、OECD の監修は受けておらず、本書を利用したことに起因して何らかの損害が生じたとしても本会は一切の責任は負いません。原著と対訳の間に明らかな矛盾や不一致が認められた場合は、原著を優先して利用してください。

英文	和訳
Table of Contents	目次
1. Background 10	1. 背景 10
2. Introduction 10	2. はじめに 10
3. Definitions and terms 11	3. 定義と用語 11
3.1. Data 11	3.1. データ 11
3.2. Data structure 13	3.2. データ構造 13
3.3. Electronic signature 14	3.3. 電子署名 14
3.4. Data integrity 14	3.4. データインテグリティ 14
3.5. Data quality 14	3.5. データ品質 14
3.6. Data life cycle..... 14	3.6. データのライフサイクル 14
3.7. Data governance..... 15	3.7. データガバナンス 15
4. GLP responsibilities for data, from generation to archive..... 15	4.データに対する GLP の責務、データの生成から保存まで ..15
5. Principle actions to ensure data integrity 16	5. データインテグリティ確保のための基本事項 16
6. Data integrity requirements through the data life cycle 18	6. データライフサイクルでのデータインテグリティ要件 18
6.1. General requirements on data 18	6.1. データに関する一般的な要件 18
6.2. Generation, capture or recording of raw data 19	6.2. 生データの生成､収集､記録 19
6.3. Metadata 21	6.3. メタデータ 21
6.4. Electronic Signatures 21	6.4. 電子署名 21

英文	和訳
1. Background One of the fundamental purposes of the Principles of Good Laboratory Practice (GLP) is to ensure the quality and integrity of test data related to non-clinical safety studies. The way in which study data, supporting human, animal and environmental safety assessment, is generated, handled, reported, retained and archived has continued to evolve in line with the introduction and ongoing development of supporting technologies. This includes the increasing use of electronic data capture, integration and automation of systems and other technologies. Systems can range from manual processes with paper records to the use of complex computerised systems. However, the main purpose of the requirements of the Principles of GLP remains the same in having confidence in the quality, the integrity of the data and being able to reconstruct activities performed during the conduct of non-clinical safety studies.	**1. 背景** GLP 原則の基本的な目的の一つは、非臨床安全性試験に関連する試験データの品質と完全性を確保することである。 ヒト、動物、環境の安全性評価を支える試験データの作成、取扱い、報告、保持及び保管の方法は、支援技術の導入と継続的な開発に合わせて進化し続けている。これには、電子データ収集、システムの統合と自動化、その他の技術の使用の増加が含まれる。システムは、紙の記録による手作業から複雑なコンピュータ化システムの使用まで様々である。しかし、GLP 原則の要求事項の主な目的は、品質、データの完全性に確信を持ち、非臨床安全性試験の実施中に行われた活動を再構築できるようにすることに変わりはない。
2. Introduction The following overarching aspects apply to this document: 1. This document provides guidance for test facilities or test sites that conduct GLP studies or GLP study phases.	**2. はじめに** このドキュメントには、以下のような包括的な側面がある。 1. 本文書は、GLP 試験又は GLP 試験段階を実施する試験施設又は試験場所に対するガイダンスである。

英文	和訳
For the purposes of this document, the term ‘test facility’ includes test sites; the term ‘study’ includes study phases; and the term ‘study director’ is extended to cover the responsibilities of principal investigator where this is appropriate.	本文書では、「試験施設」という用語には試験場所が含まれ、「試験」という用語には試験段階が含まれ、「試験責任者」という用語は、必要に応じて試験主任者の責任をカバーするために拡大して用いる。
2. The guidance aims to promote a risk-based approach to the management of data that includes data risk, criticality and life cycle. Users of this document need to understand the data flows they are responsible for or involved in (as a life cycle) in order to identify data that are likely to have impact on GLP compliance. In turn, this will support the identification and the implementation of the most effective and efficient risk-based controls.	2. 本ガイダンスは、データの管理において、データのリスク、重要性、ライフサイクルを含むリスクベースのアプローチを促進することを目的としている。この文書の利用者は、GLP 遵守に影響を与える可能性のあるデータを特定するために、自分が責任を負う、あるいは関与するデータの流れ（ライフサイクルとして）を理解する必要がある。その結果、最も効果的かつ効率的なリスクベースの管理方法を特定し、実施を可能にするであろう。
3. Data integrity is the degree to which data are complete, consistent, accurate, trustworthy and that these characteristics of the data are maintained throughout the data life cycle. Data should be collected and maintained in a secure manner, such that they are attributable, legible, contemporaneously recorded and accurate, whether raw data or a verified copy.	3. データインテグリティとは、データが完全で、一貫性があり、正確で、信頼できるものであり、 データのこれらの特性がデータのライフサイクルを通じて維持されている度合いをいう。データは、生データであれ検証済みコピーであれ、帰属性、可読性、同時記録性、正確性を持って、安全な方法で収集・維持されなければならない。
4. The guidance refers to the acronym ALCOA being Attributable, Legible, Contemporaneous, Original and Accurate. ALCOA has historically been regarded as the attributes of data that are suitable for	4. 本ガイダンスでは、Attributable, Legible, Contemporaneous, Original and Accurate の頭文字をとった ALCOA について述べている。ALCOA は歴史的に、規制目的に適したデータの属性と

英文	和訳
regulatory purposes. ALCOA+ has been referred to in more recent times to emphasise the additional attributes Complete, Consistent, Enduring and Available. There is no difference between the expectations related to data integrity for both these terms since data governance measures should ensure that data are complete, consistent, enduring and available throughout the data life cycle.	みなされてきた。最近、ALCOA+と呼ばれるようになり、Complete（完全な）、Consistent（一貫性のある）、Enduring（永続的な）、Available（入手可能な）という追加属性が強調されるようになった。データガバナンス対策は、データのライフサイクルを通じて、データが完全で、一貫性があり、永続的で、利用可能であることを保証する必要があるため、これらの用語はいずれもデータインテグリティに関する要件であることに違いはない。
5. The guidance addresses data integrity and not data quality since the controls required for integrity do not guarantee the quality of the data (see also definitions in section 3.4 and 3.5). Data integrity provides control over the data (i.e. whether it can be trusted), whereas data quality refers to the data characteristics that assure that data produced are generated in compliance with applicable standards and can be used for its intended purpose.	5. 本ガイダンスはデータの完全性について述べており、データの品質については述べておらず、完全性のために要求される管理は、データの品質を保証するためのものではない（3.4 節及び 3.5 節の定義も参照）。データインテグリティは、データに対する管理（信頼できるかどうか）を提供するものであり、一方、データ品質は、生成されたデータが適用される基準に準拠して生成され、意図された目的に使用できることを保証するデータ特性を意味する。
6. This guidance should be equally applied to the control of all data types and formats. Some points are nevertheless focused, and specifically applicable, to electronic data and electronic systems.	6. このガイダンスは、全てのデータタイプ及びフォーマットの管理に等しく適用されるべきである。しかしながら、いくつかのポイントは、電子データ及び電子システムに焦点を当てている。
7. This guidance should be read in conjunction with OECD Documents No 1 (OECD Principles on Good Laboratory Practice)	7. 本ガイダンスは、OECD 文書 No.1（OECD Principles on Good Laboratory Practice）（OECD, 1997[1]）、No.15（Establishment

英文	和訳
(OECD, 1997[1]), No 15 (Establishment and Control of Archives that Operate in Compliance with the Principles of GLP) (OECD, 2007[2]), No 16 (Guidance on the GLP Requirements for Peer Review of Histopathology) (OECD, 2014[3]) and No 17 (Application of GLP Principles to Computerised Systems) (OECD, 2016[4]) and applicable national regulations. The GLP Principles that reference data integrity can be found in Section II, 1.1.2.b to e, 1.1.2.l, 1.1.2.q, 1.2.2.f, 1.2.2.g, 1.2.2.i, 1.4.3, 2.1.1.c, 3.4, 7.1, 7.4.3, 8.2.6, 8.3.3, 8.3.4, 8.3.5, 10.1 of OECD Document No 1. Where relevant complementary information is contained in this document and other documents, reference is made within the text.	and Control of Archives that Operate in Compliance of the Principles of GLP）（OECD, 2007[2]）、No.16（Guidance on the GLP Requirements for Peer Review of Histopathology）（OECD, 2014[3]）、No.17（Application of GLP Principles to Computerised Systems）（OECD, 2016[4]）、及び適用される国内規制と併せて読まれるべきものである。データインテグリティについて言及している GLP 原則は、OECD Document No 1 のセクション II、1.1.2.b～e、1.1.2.l、1.1.2.q、1.2.2.f、1.2.2.g、1.2.2.i、1.4.3、2.1.1.c、3.4、7.1、7.4.3、8.2.6、8.3.3、8.3.4、8.3.5、10.1 に記載されている。本文書及びその他の文書に関連する補足情報が含まれている場合には、本文中で言及している。
3. Definitions and terms **3.1. Data** Data are quantitative or qualitative facts, figures and statistics collected for reference or analysis. These include all original records and verified copies of original records, including raw data and metadata and all subsequent transformations that are generated or recorded at the time of the GLP activity, and allow complete reconstruction and evaluation of the GLP activity. Data can have different formats (e.g. analogue, digital) and structure,	**3. 定義及び用語** **3.1. データ** データとは、参照又は分析のために収集された定量的又は定性的な事実、数値及び統計のことである。これらには、GLP 活動の時点で生成又は記録された生データ及びメタデータ、並びにその後の全ての変換を含む、全ての原記録及び原記録の検証済みコピーが含まれ、GLP 活動の完全な再構築及び評価を可能にするものである。 データは、異なる形式（例：アナログ、デジタル）や構造、レイ

英文	和訳
layouts (e.g. on paper or on screen), sources (e.g. chromatography charts, text, image, video, etc.), and media used to store or present (paper, DVD, photo film, tape, electronic files, etc.).	アウト（例：紙上、画面上)、ソース（例：クロマトグラフ、テキスト、画像、ビデオなど)、保存又は提示に使用されるメディア（紙、DVD、写真フィルム、テープ、電子ファイルなど）が存在する。
Data may be captured or recorded: i. by manual recording, on paper or in an electronic system, of an observation or of an activity; ii. by automatic recording, on paper (by automatic printing) or in an electronic system, using equipment that range from simple instruments through to complex highly configurable computerised systems; iii. using a hybrid system where combinations of paper (or other non-electronic media) and electronic records constitute the raw data; iv. on other means of media such as photography, imaging methodologies and technologies, chromatography plates, etc. that could be generated manually, or automatically or using a hybrid system.	データは下記のように収集又は記録される。 i. 観察又は活動を紙又は電子システムに手動で記録 ii. 単純な機器から高度に構成可能な複雑なコンピュータ化システムまで、さまざまな機器を用いて、紙面上（自動印刷）又は電子システムに自動記録 iii. 紙（又はその他の非電子媒体）と電子記録の組み合わせが生データを構成するハイブリッドシステムを使用 iv. 写真、画像処理方法及び技術、クロマトグラフィープレートなどその他の媒体上で手動、自動、又はハイブリッドシステムによって生成
Raw data The Principles of GLP define raw data as all original test facility records and documentation, or verified copies thereof, which are the	***生データ*** GLP 原則では、「生データ」とは、試験における最初の観察及び活動の結果であり、GLP 活動の完全な再現及び評価を可能にす

英文	和訳
result of the original observations and activities in a study and allow complete reconstruction and evaluation of the GLP activities. Raw data also may include, for example, photographs, microfilm or microfiche copies, computer readable media, dictated observations, recorded data from automated instruments, or any other data storage medium that has been recognised as capable of providing secure storage of information for a time period.	る、試験施設の記録及び文書のオリジナル、又はその検証済みコピーと定義されている。また、生データには、例えば、写真、マイクロフィルム又はマイクロフィッシュのコピー、コンピュータで読み取り可能な媒体、口述した観察結果、自動化された機器からの記録データ、又は一定期間情報を安全に保存できると認められたその他のデータ記憶媒体が含まれることがある。
Record A record is a piece of information (e.g. data). The term original record is used to describe the first source of information or data capture. Original records are generally raw data. If an original record meets the definition of raw data, but is not considered as such, this must be justified.	***レコード*** レコードとは、情報（データなど）の断片である。オリジナルレコードという言葉は、情報やデータの最初の収集源を表すのに使われる。オリジナルレコードは一般的に生データである。オリジナルレコードが生データの定義を満たしているにもかかわらず、生データとみなされない場合は、その正当性を示す必要がある。
Verified copy A verified copy is a faithful representation of the original at the time the copy is generated. A verified copy may be stored in a different format or document type to the original. Verified copies can be generated to: ・ make a duplicate of the originals to include them in different files (for example, experimental raw data common to several studies);	***検証済みコピー*** 検証済みコピーは、コピーが生成された時点でのオリジナルの忠実な複写である。検証済みコピーは、オリジナルとは異なる形式又は文書タイプで保存することができる。 検証済みコピーは以下の目的で生成される。 ・ オリジナルを別のファイルに入れるために複製を作成する場合（例えば、複数の試験に共通する実験の生データ）。

英文	和訳
・ extend the retention period of some data whose format does not allow preservation (e.g. thermal printouts); ・ allow the retention of the data if the original cannot be kept without causing a risk to other archived materials (for example, paper raw data stained with animal fluids, chemicals etc.); ・ facilitate the exchange of data; ・ support archiving activities. The most common processes to generate verified copies from static records are: ・photocopy of a paper record (paper to paper); ・scan of a paper record (paper to electronic); ・picture of a paper record (paper to picture); ・screen shot and printout of an electronic record (electronic to paper).	・ 保持できない形式のデータの保存期間を延長する場合（例：感熱紙の印刷物）。 ・ 他の保存資料にリスクを与えずにオリジナルを保存できずコピーの保持が認められる場合（例：動物の体液や化学物質で汚れた紙の生データなど） ・ データの交換を円滑に行う場合 ・ 資料保存活動をサポートするため 静的記録から検証済みコピーを生成する最も一般的なプロセスは以下の通りである。 ・ 紙の記録のコピー（紙から紙） ・ 紙の記録のスキャン（紙から電子） ・ 紙の記録の写真（紙から写真） ・ 電子記録のスクリーンショットとプリントアウト（電子から紙）
Derived data Derived data are obtained and reconstructed from raw data (e.g. final concentrations as calculated by a spreadsheet relying on raw data obtained from an instrument; result tables as summarised by a Laboratory Information Management System (LIMS), etc.). Derived data are obtained by data processing.	***派生データ*** 派生データとは、生データから得られ、再構成されたデータ（例えば、機器から得られた生データに基づいてスプレッドシートで計算された最終濃度、Laboratory Information Management System（LIMS）でまとめられた結果表など）をいう。派生データとは、データ処理によって得られるデータのことである。

英文	和訳
Metadata Metadata are data providing information used for the identification, description, and relationships of data. Metadata give data meaning, provide context, define structure, and enable retrievability across systems, and usability, authenticity, and auditability across time. For electronic data, parts of the metadata can be generated in audit trails. Metadata form an integral part of the data. Without the context provided by metadata, the data have no or limited meaning. The degree of metadata missing reduces the ability to interpret the data.	***メタデータ*** メタデータとは、データの識別、説明、関係性を示す情報を提供するデータのことである。メタデータは、データに意味を与え、背景情報を提供し、構造を定義し、システム間の取り出しと移動を可能にし、時間を超えた有用性、信頼性、監査性を実現する。電子データの場合、メタデータの一部は監査証跡として生成される。 メタデータは、データの不可欠な部分を形成する。メタデータによって提供される背景情報がなければ、データは意味を持たないか、限られた意味しか持たない。メタデータの欠落の程度によって、データを解釈する能力が低下する。
Audit trail The audit trail is a form of metadata that contains information associated with actions that relate to the creation, modification or deletion of electronic data. An audit trail provides an automated secure way of recording life cycle details such as creation, additions, deletions or alterations of information in an electronic record without obscuring or overwriting the original record. An audit trail facilitates the reconstruction of the history of such events relating to the record, including the 'who, what, when and why' of the action.	***監査証跡*** 監査証跡とは、電子データの作成、変更、削除に関連するアクションに紐づいた情報を含むメタデータの一形態である。監査証跡は、電子記録の情報の作成、追加、削除、変更などのライフサイクルの詳細を、元の記録を不明瞭にしたり上書きしたりすることなく自動的に安全に記録する方法を提供する。監査証跡は、記録に関連するこのような出来事の履歴の再構築を容易にし、活動の「誰が、何を、いつ、なぜ」を含む。

英文	和訳
3.2. Data structure Data can have different structures. *Static format* A static record format, such as a paper or electronic record, is one that is fixed and allows no interaction between the user and the record content. For example, all paper records are static records. Electronic records that do not contain any link to other records that allow interaction are also static records. A printout from a basic electronic balance, where no electronic data is stored, is an example of a static record from an electronic system.	**3.2. データ構造** データには様々な構造がある。 静的形式 静的記録形式は、紙又は電子記録のように、固定されており、ユーザーと記録内容の間に相互作用がないものである。例えば、紙の記録は全て静的記録である。相互作用を可能にする他の記録へのリンクを含まない電子記録も静的記録である。電子データが保存されていない基本的な電子天秤からの印刷物は、電子システムからの静的記録の一例である。
Dynamic format Records in a dynamic state are mostly electronic records that allow for an interactive relationship between the user and the record content. Examples of a dynamic format include chromatography data maintained as electronic records to allow the user to zoom on the baseline, to view the integration more clearly, or to have direct access via electronic links to the sequence of analysis, the table of results, the audit trails and the methods of acquisition and integration. Records electronically signed are also dynamic records as they contain a link with the authentication of the signature.	動的形式 動的な状態の記録は、ほとんどが電子記録であり、ユーザーと記録内容との間の相互作用を可能にする。動的形式の例には、電子記録として保持されているクロマトグラフィーデータがあり、ユーザーはベースラインを拡大したり、積分をより明確に表示したり、分析の順序、結果の表、監査証跡、収集及び積分の方法などに電子リンクを介して直接アクセスすることができる。電子署名された記録は、署名の認証とのリンクを含むため、動的な記録である。

英文	和訳
File structure The way in which most of the electronic data are structured within the GLP environment will depend on what the data will be used for and the end user will almost always have this dictated to them by what software / computerised system is available.	*ファイル構造* GLP 環境下でのほとんどの電子データの構築方法は、そのデータが何に使用されるかに依存し、エンドユーザーにとっては、ほとんどの場合、利用可能なソフトウェアやコンピュータ化システムによって決められることになる。
Flat files A flat file consists of a single table of data, has no internal hierarchy and allows the user to specify data attributes i.e. its data structure is self-contained and limited. Flat files can be thought of as being similar to the files in a file cabinet drawer, a collection of single records each containing standalone data. The most commonly known flat file would be a .csv or .xls file or a Microsoft Word™ text only document.	*フラットファイル* フラットファイルは、単一のデータテーブルで構成され、内部に階層がなく、ユーザーがデータの属性を指定することができる。すなわち、そのデータ構造は自己完結的で限定的である。 フラットファイルは、ファイルキャビネットの引き出しに入っているファイルのようなもので、それぞれが独立したデータを含む単一の記録の集まりと考えることができる。最も一般的に知られているフラットファイルは、.csv 又は.xls ファイル、あるいは Microsoft Word™のテキストのみの文書である。
Relational databases Relational databases are a collection of tables linked together using a common piece of data, such as a study number, and can be arranged to highlight specific information for ad hoc queries. A relational database is a scalable and query friendly tool that provides the ability to capture a wide variety of data types. Relational databases are	*リレーショナルデータベース* リレーショナルデータベースは、試験番号などの共通データを使用してリンクされたテーブルの集合体であり、任意のクエリによって特定の情報を強調するように配置することができる。リレーショナルデータベースは、拡張性が高く、クエリに適したツールであり、様々な種類のデータを取り込むことができる。リレーシ

英文	和訳
usually not used to record raw data. Relational databases store different components of associated data and metadata in different places. Each individual record is created and may be retrieved by compiling the data and metadata for review using a database reporting tool. For example, electronic records in a database format allows the user to track, trend and query data.	ョナルデータベースは通常、生データの記録には使用されない。 リレーショナルデータベースは、関連するデータとメタデータの異なるコンポーネントを異なる場所に保存する。作成された個々の記録は、データとメタデータをコンパイルすることにより、データベースのレポートツールを使用して、レビューするためのリトリーブをすることができる。 例えば、データベース形式の電子記録は、ユーザーがデータを追跡し、傾向を調べ、絞り込みをすることを可能にする。
3.3. Electronic signature An electronic signature is a signature in digital form that represents the hand-written (‘wet’) signatory. Different types of systems exist from simple ones (e.g. internal user identification with password) to complex systems of signatures (e.g. with an external, certified electronic signature service that provides with timestamp and encrypted information behind the signature). To be considered as an electronic signature in legal terms, the associated level of control required is defined where relevant by local regulation.	**3.3. 電子署名** 電子署名とは、手書きの（「ウェットな」）署名に相当するデジタル形式の署名である。 単純なもの（例：パスワードによる内部ユーザーの識別）から、複雑な署名システム（例：タイムスタンプと署名の背後にある暗号化された情報を提供する外部の認証された電子署名サービスを使用する）まで、様々なタイプのシステムが存在する。法的に電子署名とみなされるためには、必要とされる関連する管理レベルが現地の規制によって定義されている必要がある。
3.4. Data integrity Data integrity is the degree to which data are complete, consistent, accurate, trustworthy and reliable and that these characteristics of the	**3.4. データインテグリティ** データインテグリティとは、データが完全で、一貫し、正確で、信用でき、信頼できるかどうか、またその性質がデータのライフ

英文	和訳
data are maintained throughout the data life cycle. Assuring data integrity requires appropriate quality and risk management systems, including adherence to sound scientific principles, good documentation practices and training of personnel.	サイクル全体にわたって維持されるのかどうかの度合いのことである。データインテグリティを確保するためには、健全な科学的原則の遵守、適切な文書化の実施、人員の訓練など，適切な品質及びリスク管理システムが必要である。
3.5. Data quality Data quality is the assurance that the data produced are generated according to applicable standards and fit for intended purpose. Data quality is assured by appropriate study design that accurately and scientifically addresses the experimental question and hypotheses being studied and by the availability of adequate resources. Data quality affects the value and overall acceptability of the data in regard to decision-making or onward use.	**3.5. データ品質** データの品質とは、生成されたデータが適用可能な基準に従って生成され、意図された目的に適合していることを保証するものである。データの品質は、研究されている実験的な疑問及び仮説に正確かつ科学的に対処する適切な試験デザインと、適切な資源の利用によって保証される。データの品質は、意思決定や以降の使用に関して、データの価値と全体的な受容性に影響を与える。
3.6. Data life cycle The data life cycle includes all phases in the life of the data from generation and recording through processing (including analysis, transformation or migration), use, data retention, archive, retrieval and destruction.	**3.6. データライフサイクル** データライフサイクルには、データの生成及び記録から、処理（分析、変換又は移行を含む）、使用、データの保持、資料保存、リトリーブ及び廃棄に至るまでのデータのライフサイクルにおける全ての段階が含まれる。
・ Data approval: Data approval is the act of authorising data after collection, processing or verification to record that data are suitable for their intended use.	・ データの承認：データ承認とは、データが意図された使用に適していることを記録するために、収集、処理、又は検証の後にデータの正当性を認める行為をいう。

英文	和訳
・ Transcription: Transcription is the process where data are manually copied from a source into another record of data set. Transcription can occur when: ◦ the same information is recorded in different records (for example, the date of arrival of the test item is recorded in multiple records such as logbooks or proformas); ◦ data are entered into a computerised system for calculations. Transcription of manual records into an electronic system constitutes an example of a hybrid system.	・ 転記：転記とは、データをソースから別のデータセットの記録に手動でコピーするプロセスである。 転記は以下のような場合に行われる。 ◦ 同一の情報を異なる記録に記録する場合（例えば、被験物質の到着日を使用記録や作業記録などの複数の記録に記録） ◦ データをコンピュータ化システムに入力して計算する場合手動記録を電子システムに転記することは、ハイブリッドシステムの一例である。
・ Data processing: Data processing is a sequence of operations performed on data in order to extract, present, calculate or obtain derived data in a defined format. Examples might include calculations in a spreadsheet, statistical analysis of individual test system data to present trends, or conversion of a raw electronic signal to a chromatogram and subsequently a calculated numerical result.	・ データ処理：データ処理とは、定義された形式でデータを抽出、表示、計算、又は派生データを得るためにデータに対して行われる一連の操作のことである。例えば、スプレッドシートでの計算、個々の試験システムのデータを統計的に分析して傾向を示すこと、生の電子信号をクロマトグラムに変換し、その後、計算された数値結果を得ることなどが挙げられる。
・ Data migration: Data migration is the process of moving electronic data between different data storage types, computerised systems, or simply the transition of data from one format to another. This may include changing the format of data, but not the content or	・ データ移行：データ移行とは、電子データを異なるデータストレージタイプやコンピュータ化システム間で移動させるプロセス、又は単にデータをある形式から別の形式に移行させることである。これには、データの形式を変更することが含

英文	和訳
meaning, to make it usable or visible on an alternative computerised system.	まれるが、内容や意味は変更せず、別のコンピュータ化システムで使用可能又は表示可能にすることもある。
・ Computerised system transaction: A computerised system transaction is a single operation or sequence of operations performed as a single logical unit of work. The operation(s) that constitute(s) a transaction may not be saved as a permanent record on durable storage until the user commits the transaction through a deliberate act (e.g. pressing a save button, see also “data approval”), or until the system forces the saving of data.	・ コンピュータ化システムトランザクション：コンピュータ化システムトランザクションとは、単一の論理的作業単位として実行される単一の操作又は一連の操作をいう。トランザクションを構成する操作は、ユーザーが意図的な行為（例：保存ボタンを押す、「データ承認」も参照）によってトランザクションを確定するまで、又はシステムがデータの保存を実行するまで、永続的な記録として耐久性のある記憶装置に保存されることはない。
・ Data retention: Data retention is the storage of data which may be for the purpose of archiving (protected data for long-term storage) or back-up (electronic data or for the purposes of disaster recovery).	・ データの保持：データの保持とは、資料保存の目的のデータ（長期保存のための保護されたデータ）又はバックアップ(電子データ又は災害復旧のためのデータ）を保存することである。
・ Back-up: A data back-up is a copy of current data, metadata and system configuration settings maintained for the purpose of recovery including disaster recovery. Back-up allows for provisions made for the recovery of data files or software, for the restart of processing, or for the use of alternative computer equipment following a system failure or disaster.	・ バックアップ：データのバックアップとは、最新のデータ、メタデータ、システム構成設定のコピーで、災害復旧を含む回復を目的として維持されるものである。 バックアップにより、システム障害や災害時に、データファイルやソフトウェアの復旧、処理の再開、代替のコンピュータ機器の使用などの対策ができる。

英文	和訳
・ Archive: Archive means a designated area or facility (e.g. cabinet, room, building or computerised system) for the secure storage and retention of records and materials.	・ 資料保存施設：資料保存施設とは、記録や資料を安全に保存・保持するために指定された区域や施設（キャビネット、部屋、建物、コンピュータ化システムなど）をいう。
3.7. Data governance Data governance is the sum total of arrangements to ensure that data (irrespective of the format in which they are captured, generated, recorded, processed, retained, archived and used) are attributable, legible, contemporaneous, original (or verified copy), accurate, complete, consistent, enduring and accurate (ALCOA+) throughout their life cycle. These arrangements can consist of a single standalone system or across a combination of systems within a test facility.	**3.7. データガバナンス** データガバナンスとは、データ（収集、生成、記録、処理、保持、保存、使用での形式に関わらず）が、そのライフサイクルを通じて、帰属性、可読性、同時性、オリジナルの記録（又は検証済みコピー）、正確性、完全性、一貫性、永続性、正確性（ALCOA+）を確保するための取り決めの総称である。 これらの設定は、単一の独立したシステムで構成されることもあれば、試験施設内の複数のシステムの組み合わせで構成されることもある。
4. GLP responsibilities for data, from generation to archive ***Study Personnel*** All study personnel are responsible for recording raw data promptly and accurately and in compliance with the Principles of GLP.	**4. データに関する GLP の責務、生成から保存まで** ***試験担当者*** 全ての試験担当者は、生データを迅速かつ正確に記録し、「GLP の原則」を遵守する責任がある。
Study Director The study director should ensure that: ・ all raw data are fully documented and recorded; ・ computerised systems used in the study have been validated,	***試験責任者*** 試験責任者は以下のことを確保する必要がある。 ・ 全ての生データが完全に文書化され、記録されていること ・ 試験に使用されるコンピュータ化システムが、データインテ

英文	和訳
including requirements associated with data integrity; and ・ after completion (including termination) of the study, the study plan, the final report, raw data and supporting material are archived so that all the material, including data, needed to reconstruct the study remain available.	グリティに関する要件を含めて、検証されていること ・ 試験の完了（終了を含む）後、試験計画書、最終報告書、生データ及び補助資料を保存し、試験の再構築に必要なデータを含む全ての資料を利用できるようにすること
Archivist The archivist is the individual responsible for the management, operations and procedures for archiving in accordance with the Principles of GLP, including archiving of data, physically and electronically.	***資料保存施設管理責任者*** 資料保存施設管理責任者とは、「GLP の原則」に従って、物理的及び電子的なデータの資料保存を含む、資料保存の管理、運営、手順に責任を持つ人のことである。
Test Facility Management Test Facility Management (TFM) is responsible for the organisation and functioning of the facility where data are generated. TFM should: ・ ensure that a sufficient number of qualified personnel, appropriate facilities, equipment, and materials are available for the timely and proper conduct of the study, including resources to ensure data governance; ・ ensure the maintenance of a record of the qualifications, training, experience and job description for each professional and technical individual;	***運営管理者*** 運営管理者（TFM）は、データが生成される施設の組織及び機能に責任を負う。TFM は以下を行うべきである。 ・ データガバナンスを確保するためのリソースを含め、試験を適時かつ適切に実施するために、十分な数の有資格者、適切な施設、設備、及び資材が利用可能であることを確実にすること ・ 各専門家及び技術者の資格、トレーニング、経験及び職務内容の記録を確実に維持すること ・ 職員が自分の果たすべき機能を明確に理解し、必要に応じて、

英文	和訳
・ ensure that personnel clearly understand the functions they are to perform and, where necessary, provide training for these functions, including training on data integrity; ・ ensure that appropriate and technically valid standard operating procedures (SOPs) are established and followed, and approve all original and revised SOPs, including those relating to the data governance system; ・ ensure that an individual is identified as responsible for the management of the archives, including data, paper and electronic archiving; ・ establish procedures to ensure that computerised systems are suitable for their intended purpose, and are validated, operated and maintained in accordance with the Principles of GLP, including functionalities associated with data integrity; ・ implement systems that comply with current regulatory expectations; and ・ ensure that residual risks associated with data integrity are identified and mitigated.	データインテグリティに関するトレーニングを含め、これらの機能に関するトレーニングを提供することを保証すること ・ 適切かつ技術的に有効な標準操作手順書（SOP）が確立され、遵守されていることを確認し、データガバナンスシステムに関連するものを含む全てのオリジナル及び改訂された SOP を承認すること ・ データ、紙及び電子アーカイブを含む資料保存施設の管理に責任を負う個人が確実に特定されていること ・ コンピュータ化システムが意図された目的に適しており、データインテグリティに関連する機能を含め、GLP の原則に従って検証、運用及び維持されていることを確認するための手順を確立すること ・ 現在の規制当局の期待に適合するシステムを導入すること。 ・ データインテグリティに関連する残存リスクを確実に特定し、軽減すること
Quality Assurance Personnel Quality Assurance (QA) Personnel should conduct inspections to	***信頼性保証担当者*** 信頼性保証担当者は、全ての試験が GLP の原則に従って実施さ

英文	和訳
determine if all studies are conducted in accordance with the Principles of GLP. This may include data collection, data capture systems, implemented data governance measures and associated SOPs and should be included in the QA Programme of the test facility.	れているかどうかを判断するための調査を行うべきである。これには、データ収集、データ収集システム、実施されたデータガバナンス対策及び関連する SOP が含まれる場合があり、試験施設の QA プログラムに含まれるべきである。
5. Principle actions to ensure data integrity 1. TFM should ensure that systems implemented within the test facility produce data that are attributable, legible, contemporaneous, original, accurate, complete, consistent, enduring and available (ALCOA+) in all its forms, i.e. paper and electronic. The study director should verify that the implemented systems are fit for the integrity of the study data.	**5. データインテグリティ確保のための基本事項** 1. TFM は試験施設に導入したシステムについて、作成されるあらゆる形態のデータ（すなわち紙媒体や電子媒体）の帰属性、判読性、同時性、オリジナルの記録、正確性、完全性、一貫性、永続性、利用可能性（ALCOA+）を保証するべきである。試験責任者は導入されたシステムが試験データの完全性に適合していることを確認するべきである。
2. TFM is expected to implement a fully documented system with supporting rationale that provides an acceptable state of control based on the data integrity risk. An example of a suitable approach is to perform a data integrity risk assessment where the processes that produce, process and/or store data are mapped out and each of the formats and their controls are identified and the data criticality, inherent risks and appropriate mitigations documented. Other documented approaches to the identification and control of data integrity risks can be acceptable.	2. TFM には、データインテグリティのリスクが許容され得る管理状態にあることが文書化されたシステムを導入することが期待される。適切なアプローチの例としては、データが生成され、処理され、保存される過程を正確に規定し、データ形式とその管理法を特定すること、データの重要性、データに内在するリスクとその軽減策を文書化するデータインテグリティのリスクアセスメントを行うことである。データインテグリティのリスクの特定と管理には、これ以外の方法を用いることも許容される。

英文	和訳
3. Arrangements in place within the test facility with respect to organisation and personnel, systems and facilities should be designed, operated and where appropriate adapted to support a suitable working environment, i.e. providing an appropriate environment to enable the function of effective data integrity controls.	3. 試験施設内で用いている組織と職員、体制、施設に関する規定は、適切な作業環境を作り出すために設計、運用し、必要ならば変更する。すなわち、適切な作業環境として、データインテグリティに関する管理が効果的に機能する環境を作る。
4. Data governance must be applied across the whole data life cycle to provide assurance of data integrity. Data governance should address data ownership and accountability and consider the design, operation and monitoring of processes/systems in order to comply with data integrity requirements, including control over all changes to data. Data governance systems should also ensure that data are readily available and accessible. Electronic data should be available in human-readable form.	4. データインテグリティを保証するために、データガバナンスをデータのライフサイクル全体に対して適用する。データガバナンスはデータの所有権と説明責任に関わる事項であり、データインテグリティの要求を満たすためのシステムあるいは作業過程（これら全ての変更管理を含む）の設計、運用、監視を検討する。データガバナンスのためのシステムは、データが使いやすく、容易に入手できることを保証すべきである。電子データは、人間が読める形で利用可能でなければならない。
5. The approaches used for the management of data governance should use risk management techniques to detect risks for data integrity failures within the test facility's systems, to minimise the potential risk to data integrity and to identify any residual risk. Approaches used for the management of data governance (e.g. SOPs) should always be approved by TFM. The effectiveness of the data governance approach should be monitored and assessed on a regular basis as defined by	5. データガバナンスの管理手法はリスクマネジメントの考え方を用い、試験施設の体制が内包しているデータインテグリティの過誤を検出すると共に、データインテグリティに関する潜在リスクを最小化し、残存リスクを特定する手法であるべきである。データガバナンスの管理のために利用するものは（例えば SOP）、必ず TFM の承認を受ける。データガバナンスの管理手法の有効性は、TFM の取り決めた通り、定期的に監視及び評価する。

英文	和訳
TFM.	
6. TFM is expected to ensure appropriate resources and training. Data governance systems should include staff training in the importance of data integrity concepts and the creation of a working environment that enables transparency, and actively encourages reporting of errors, omissions and aberrant results.	6. TFM には適切な経営資源の確保と訓練の実施が期待される。データガバナンスの体制には、データインテグリティの概念の重要性を職員に教育すること、透明性を実現する作業環境を構築することで、過失や見落とし、異常の報告を積極的に促すことも含まれている。
7. The risks to data are reflected in their potential to be deleted either unintentionally or intentionally, amended, altered or excluded without authorisation or without the ability to detect such activities and events. The risks to data may be increased by complex or inconsistent or missing processes, with open-ended and subjective outcomes. Simple, well-defined tasks that are undertaken consistently and have a clear objective should be established to mitigate such risks.	7. データに対するリスクには、意図したかどうかによらず、データが削除されたり、権限がないにもかかわらずデータを修正、部分的に変更、除外したり、それらの行動や出来事を検出できない可能性が反映されている。データのリスクは、複雑で、一貫性がない、又は不明瞭であるプロセスによって、また形式が自由な場合や主観的な結果の場合に増大することがある。そのようなリスクを軽減するには、明確な目的を持って常に実施される単純で明確に定義された作業を確立することが必要である。
8. A data integrity risk assessment (or equivalent) should consider all factors required to follow a process or perform an activity. TFM should nominate personnel to conduct the risk assessment and it is advised to be performed by a multidisciplinary team of subject matter experts that may include members with knowledge of the process, study directors, specialists in information technology (IT), QA and all	8. データインテグリティリスクアセスメント（あるいはそれと同等のもの）では、プロセスの追跡、又は業務の遂行に必要な全ての要素を念頭に置くべきである。TFM がリスクアセスメントを行う者を指名し、リスクアセスメントはプロセスに関する知識を持つ者、試験責任者、IT 専門家、QA、その他の関連する分野の専門家を加えた多くの専門分野にわたるチームによって実施

英文	和訳
other relevant functions. It is expected to consider not only the system in isolation but also all supporting activities and functions such as regulations, processes, interfaces to other systems, human intervention, training and quality systems. Automation or the use of a validated system may lower but not eliminate the risk to data integrity. Where there is human intervention, particularly influencing how or what data are recorded or reported, there may be an increased risk from poor organisational controls or data verification due to overreliance on the system's validated state.	することが推奨される。その評価にはシステム単体のみならず、規制、プロセス、他のシステムとのインターフェース、人による介入、訓練、品質体制といった、全ての支援的な活動や機能も含めることが期待される。自動化されたシステムや検証されたシステムは、データインテグリティのリスクは低くなっているがリスクそのものは消えてはいない。人による介入がある場合、特にその介入がデータの記録や報告の方法、並びにその内容に影響を及ぼす時には、バリデートされた状態への過信がもたらす組織的管理の不十分さやデータの検証不足が要因となって、データインテグリティのリスクが増大することがある。
9. Where the data integrity risk assessment (or equivalent) has highlighted areas for remediation, then the prioritisation of actions, including acceptance of an appropriate level of residual risk, should be documented by the designated team and communicated for approval to TFM. Periodic reviews of the risk assessment should be performed to take into account the implemented actions and the possible changes in processes. In situations where long-term remediation actions are identified, risk-reducing short-term measures should be identified, documented, communicated for approval to TFM and implemented to provide an acceptable level of control in data	9. データインテグリティリスクアセスメント（あるいはそれと同等のもの）にて改善を要するとされた領域は、指名されたチームが残存リスクをどの程度受け入れるのかの適切な基準を含めた改善活動の優先順位付けを文書化し、承認に向けて TFM へ連絡する。リスクアセスメントに関する定期的なレビューは、そのプロセスにおいて実行された行為と起き得る変更を考慮して実施する。長期的な改善活動が必要となった場合、短期的なリスク軽減処置を策定し、これを文書化して TFM へ承認に向けて連絡し、より恒久的な改善処置が実施されるまでの間、データガバナンスとして受容できる程度の管理を行う。

英文	和訳
governance until a more permanent solution is implemented.	
10. Regulatory decision-making requires study data to be relevant and reliable. Data criticality may be determined by considering how the data impacts on the objectives, validity and GLP compliance of a study.	10. 規制当局の意思決定には、適切で信頼性のある試験データが必要となる。データの重要性は、そのデータが試験の目的、妥当性、GLP 遵守へ与えている影響を考慮して決定される。
11. The effort and resource applied to assure data integrity should be commensurate with the risk and the impact of the associated data integrity failure.	11. データインテグリティを保証するために投入される労力や経営資源は、データインテグリティの過誤のリスクや過誤が発生した場合の影響度に相応のものとする。
12. Test facilities should be aware that appropriate data integrity controls are necessary for computerised systems as well as paper-based manual systems, although the controls may not be the same. Hybrid systems may be used if their ability to ensure data integrity is demonstrated (see also in section 7.3 “Review of data from hybrid systems”).	12. 試験施設は、全く同じではないにしてもコンピュータ化システムと紙ベースの人の手によるシステムのいずれもが適切なデータインテグリティの管理を求められていると理解するべきである。ハイブリッドシステムは、データインテグリティを保証する能力が実証されていれば利用しても良い (7.3「ハイブリッドシステムで収集したデータのレビュー」も参照のこと)。
6. Data integrity requirements through the data life cycle **6.1. General requirements on data** Test facilities should have an appropriate level of process understanding and technical knowledge of systems used for data recording, including their capabilities, limitations and vulnerabilities. The provision of a work environment that permits performance of	**6. データライフサイクルを通じたデータインテグリティ要件** **6.1. データに関する一般的な要求事項** 試験施設は、適切なレベルのプロセス理解と、データ記録に使用するシステムの機能、制約、脆弱性などの技術的知識を有していなければならない。 必要とされるタスクの実行とデータの記録を可能にする作業環

英文	和訳
tasks and recording of data as required is essential. Examples include adequate space, sufficient time for tasks and properly functioning equipment. The following requirements are applicable to all data. Data should be: A - attributable to the person generating/modifying/reviewing the data L - legible C - contemporaneous O - original record (or verified copy of it) A - accurate Data governance measures should also ensure that data are complete, consistent, enduring and available throughout the life cycle (ALCOA+), where: Complete - the data must be whole, a complete set Consistent - the data must be self-consistent and free from self-contradiction Enduring - permanent, lasting throughout the data life cycle Available - readily available Data generated should be identified at the time of recording by the individual(s) responsible for the data entry.	境の提供は不可欠である。例えば、適切な空間、作業のための十分な時間、適切に機能する機器などである。 以下の要件は、全てのデータに適用される。 データは以下のものでなければならない。 A - データを作成／修正／レビューした人に帰属すること L – 判読性があること C - 同時性があること O - オリジナルの記録（又はその検証済みコピー）であること A - 正確であること また、データガバナンス対策は、データがライフサイクルを通じて完全であり、一貫性があり、永続的であり、利用可能であることを保証する必要がある（ALCOA+）。 Complete - データが完全であること、完全なセットであること Consistent - データは自己矛盾のないものでなければならない Enduring - 恒久的で、データのライフサイクルを通じて持続すること Available – 利用可能性があること 生成されたデータは、記録時にデータ入力の責任者によって識別されるべきである。 コンピュータ化システムの設計では、元の記録を不明瞭にするこ

英文	和訳
Computerised system design should always provide for the retention of full audit trails to show all changes to the data without obscuring the original record. It should be possible to associate all changes to data with the person having made those changes and the date they were made, for example, by use of a data audit trail or equivalent mechanisms, or timed and dated (electronic) signatures. Reason for changes must be given.	となく、データへの全ての変更を示す完全な監査証跡の保持を常に提供する必要がある。データへの全ての変更は、その変更を行った人及び変更が行われた日付と関連付けることができなければならない。例えば、データの監査証跡又は同等の仕組み、又は時間と日付の入った（電子）署名を使用することである。変更の理由が示されていなければならない。
6.2. Generation, capture or recording of raw data Raw data generated during the conduct of the study should be recorded directly, promptly, legibly and accurately. All the raw data should be signed and dated, either electronically or on paper or on other media. Where raw data are generated as a result of direct computer input (e.g. typing a value), raw data should be identified by the identity of the person responsible for the recording and by the time of entry. When the original electronic captured data are not considered as the raw data, this should be justified and documented.	**6.2. 生データの生成、収集、記録** 試験の実施中に発生した生データは、直接、迅速に、判読可能かつ正確に記録されるべきである。全ての生データは、電子的に、又は紙やその他の媒体に署名し、日付を記入すべきである。生データがコンピュータへの直接入力（値の入力など）で生成された場合、生データは記録の責任者の ID と入力時刻によって識別されるべきである。 電子的に収集されたオリジナルのデータを生データとみなさない場合は、その正当性を証明し、文書化しなければならない。
Manual recording Data recorded manually may require independent verification based on a data integrity risk assessment or by other requirements. Examples can include contemporaneous (or timely manner) second person	***手書きの記録*** 人の手によって記録されたデータは、データインテグリティに関するリスクアセスメントやその他の要件に基づいて、独立した検証が必要な場合がある。例としては、データ入力と並行した（又

英文	和訳
verification of data entry or cross-checks of related information sources (for example, equipment logbooks, test system data, etc.) or data review. The level of control should be commensurate with the identified risk of error in the manual recording. Manual observations should be directly and simultaneously recorded by the observer. If there is an exceptional need to confirm the manual observations (e.g. because of its high level of criticality on the validity of the study), additional actions might be considered to demonstrate data integrity (such as image capture or presence of a witness to confirm the observation). Records of the additional actions undertaken by the observer, and where relevant a witness, must be kept as additional data with the raw data recorded by the observer. The use of scribes to contemporaneously record the activity on behalf of another operator can be considered where justified, for example: ・ The act of contemporaneous recording compromises the activity (e.g. documenting test item preparation under sterile conditions by study personnel). ・ In-life examination of test systems. The recording by the second person should be contemporaneous with the task being performed and the records should identify both the	は適時の）二人目によるデータ入力の確認や、関連する情報源（例：機器の使用記録、試験システムのデータなど）とのクロスチェック、データレビューなどが挙げられる。管理のレベルは、人の観察記録におけるエラーの特定されたリスクに見合ったものであるべきである。 人による観察は、観察者によって直接かつ同時に記録されるべきである。人による観察を確認する例外的な必要性がある場合（例：試験の有効性に対する重要性が高いため）、データインテグリティを実証するために追加のアクションが検討されるかもしれない（画像の取り込み又は観察を確認するための証人の存在など）。観察者及び必要に応じて立会人が行った追加行為の記録は、観察者が記録した生データと一緒に追加データとして保存しなければならない。 他のオペレータに代わって活動を同時に記録する書記の利用は、正当化される場合に考慮することができる。例えば、 ・ 同時記録する行為が活動を危険にさらす場合（例：試験担当者により無菌状態での被験物質の準備を記録する場合） ・ 動物実験中の試験システムへの入力 第二者による記録は、実施されている作業と同時に行われるべきであり、記録には、作業を行っている試験担当者と記録を行って

英文	和訳
study personnel performing the task and the person completing the record. The study personnel performing the task should countersign the record when possible to formalise the fact they performed the action (not the acceptance of the recorded data). The process for scribe documentation completion should be described in SOP, which should also specify the activities to which the process applies.	いる者の両方を明記すべきである。作業を実施する試験担当者は、可能な場合には記録に連署して、作業を実施した事実を正式に示すべきである（記録されたデータを受け入れることではない）。書記が記録文書を完成するためのプロセスは、SOP に記述すべきであり、SOP にはプロセスが適用される活動も特定すべきである。
Access to the current version of templates or forms used to record the raw data, should be available at locations where activities take place so that data can be recorded promptly. The number of used templates compared to the number of available copies should be controlled to avoid duplication and to support the identification of data integrity issues, such as the detection of recreation or transcription of a record. If templates or forms to record data are available by printing, the number of printouts should be controlled.	生データを記録するために使用する雛型又は記録用紙の最新版を作業が行われる場所で利用できるようにし、データを迅速に記録できるようにする。使用可能なコピーの数と比較して、使用される雛型の数は、重複を避けるために管理されるべきであり、また、記録の再現や転記の検出など、データインテグリティに関する問題の特定を支援するために管理されるべきである。データを記録するための雛型や記録用紙が印刷して利用できる場合は、印刷枚数を管理するべきである。
Risk assessment should identify the level of control needed and the absence of full control and reconciliation should be justified by risk assessment to determine why some situations are exempt from this requirement.	リスクアセスメントにより、必要な管理レベルを特定し、完全な管理と照合が行われない場合は、なぜ一部の状況がこの要件から除外されるのか、リスクアセスメントにより正当化されるべきである。
The use of blank paper proformas for raw data recording should be limited and controlled but should also be available to allow the	生データの記録のための空欄のある作業記録の使用は、制限して管理すべきであるが、予期せぬ出来事を直ちに記録できるように

英文	和訳
contemporaneous recording of unexpected events. The reconciliation between the available sets of blank forms at the beginning and upon completion of all issued forms should be implemented. The use of paginated books can be an appropriate solution, so that the deletion of pages could be detected. Risk assessment should identify the level of control needed and the absence of full control and reconciliation should be justified. Nevertheless, the system implemented for controlling access to forms should allow an easy availability of the proper document to avoid the potential use of improper recording of data on an unapproved form and any subsequent transcription. Data generated as a direct computer input should be identified at the time of data input by the individual(s) responsible for direct data entries. For electronic data, access to applications should not hamper the contemporaneous recording of data. User access rights should prevent unauthorised data entries.	しておく必要がある。発行された全ての記録用紙の開始時及び完了時に、利用可能な記録用紙のセット間の照合を実施する必要がある。ページ付けされたブックの使用は、ページの削除が検出されるような適切な解決策となりうる。リスクアセスメントでは、必要な管理レベルを特定し、完全な管理と照合が行われない場合には、その正当性を示す必要がある。 それでもなお、記録用紙へのアクセスを管理するためのシステムは、承認されていない記録用紙へのデータの不適切な記録やその後の転記に使用される可能性を避けるために、適切な文書を容易に入手できるようにすべきである。 コンピュータへの直接入力で生成されたデータは、データ入力時に、直接入力を担当する個人によって識別されるべきである。 電子データの場合、アプリケーションへのアクセスがデータの同時記録を妨げてはならない。ユーザーのアクセス権は、不正なデータ入力を防止するものとする。
Automatic recording External devices or system interfacing methods that eliminate manual data entries and human interaction with the computerised system, such	***自動記録*** バーコードリーダー、ID カードリーダ、プリンタなど、手動でのデータ入力やコンピュータ化システムとの人間のやりとりを排

英文	和訳
as barcode scanners, ID card readers, or printers, can be used when validated. The risks related to data integrity may depend on the degree to which equipment or computerised systems that automatically capture, record, or generate data can be configured and validated, and the potential for manipulation or loss of data within the system.	除する外部機器やシステムのインターフェースの利用は、検証された場合に使用することができる。 データインテグリティに関するリスクは、データを自動的に収集、記録、又は生成する機器やコンピュータ化システムがどの程度構成され、検証されるか、及びシステム内でのデータの操作又は損失の可能性があるかによって異なる。
Hybrid systems In the case of basic electronic equipment that does not store electronic data or provides only a printed data output (e.g. certain balances or pH meters), then the printout can constitute the raw data. Where the electronic equipment does store electronic data but only holds a certain volume before overwriting it, all efforts should be made to extract and control the data and metadata as electronic data. Printing it to paper if immediately signed and dated or transforming it into another format is acceptable if no information is lost. Data (including metadata) in their retained format, should be verified prior to deletion from electronic equipment.	***ハイブリッドシステム*** 電子データを保存しない、又は印刷されたデータ出力のみを提供する基本的な電子機器の場合(例:ある種の天秤やpHメーター)、印刷出力が生データを構成することができる。 電子機器が電子データを保存していても、上書きする前の一定量しか保持していない場合は、データとメタデータを電子データとして抽出し、管理するためにあらゆる努力をしなければならない。直ちに署名と日付が入っていれば、紙に印刷したり他の形式に変換したりしても情報が失われなければ問題ない。保存形式のデータ（メタデータを含む）は、電子機器から削除する前に検証する必要がある。
Other media Data can be captured by a photograph or imaging methodologies and technologies (or other media), the requirements for traceability of the	***その他のメディア*** データは、写真や画像処理の方法や技術(又はその他のメディア)で収集することができるが、記録のトレーサビリティに関する要

英文	和訳
recording stay the same.	件は同じである。
Recording in flat files Most flat files do not allow the traceability of the identity of the person recording the data and the date and time of the record. Some flats files may carry basic metadata relating to file creation and date of the last amendment but do not provide an adequate data audit trail. Flat files should generally not be used for direct data capture or storing raw data. Where the use of flat files is necessary, and control of the data cannot be achieved by an alternative method, then risk mitigations must be established that take into account the use of such files. Examples of possible mitigations could include encryption, document location access controls, or technical safeguards that can detect modifications made to the file outside of the originating software.	***フラットファイルへの記録*** ほとんどのフラットファイルでは、データを記録した人の身元や記録した日時を追跡することができない。フラットファイルの中には、ファイルの作成日や最終修正日に関する基本的なメタデータを記録しているものもあるが、十分なデータ監査証跡にはならない。フラットファイルは、通常、データの直接収集や生データの保存には使用すべきではない。 フラットファイルの使用が必要であり、データの管理が他の方法で達成できない場合は、そのようなファイルの使用を考慮に入れたリスク軽減策を確立しなければならない。考えられる軽減策の例としては、暗号化、文書の場所へのアクセス制御、又は元のソフトウェアの外でファイルに加えられた変更を検出できる技術的な保護手段がある。
6.3. Metadata For raw data to have full meaning the data requires metadata and should be considered as part of the data (see also section 6.13 “Data audit trail”). Metadata should be generated contemporaneously with the data and should be retained with the associated data.	**6.3. *メタデータ*** 生データが完全に意味を持つためにはメタデータが必要であり、それらはデータの一部と考えるべきである（6.13 項「データの監査証跡」も参照)。 メタデータはデータと同時に生成され, 関連するデータと共に保持されるべきである。

英文	和訳
6.4. Electronic Signatures An electronic signature should be equivalent to the handwritten signature of the signatory and may be used to signify approval, authorisation or verification of specific data entries. In order to ensure data integrity, the use of electronic signatures should be appropriately controlled with consideration given to: ・ how the signature is attributable to an individual and to the purpose it is being used for (e.g. approval, verification, acknowledgement); ・ how the act of signing is recorded within the system so that it cannot be altered or manipulated without invalidating the signature or status of the entry; ・ how the time and date of the signature is recorded along with the name of the owner and the meaning of the signature; ・ how the record of the signature will be associated with the entry made and how this can be verified; and ・ how the security of the electronic signature is ensured i.e. so that it can only be applied by the owner of that signature. An inserted image of a signature or a footnote indicating that the document has been electronically signed (where this has been entered by a means other than the validated electronic signature process) is not	**6.4. 電子署名** 電子署名は、署名者の手書き署名と同等のものでなければならず、特定のデータエントリの承認，認可又は検証を示すために使用することができる。 データインテグリティを確保するために、電子署名の使用は以下の点を考慮して適切に管理されなければならない。 ・ 署名の個人や使用目的（承認、検証、確認など）への帰属方法。 ・ 署名の行為をシステム内に記録し、署名や入力の状態を無効にすることなく改ざんや操作ができないようにする方法 ・ 署名の日時を所有者の名前と署名の意味と共に記録する方法 ・ 署名の記録と入力した項目との関連付方法や検証方法 ・ 電子署名のセキュリティの確保方法（署名の所有者のみが適用できるようにする方法） 挿入された署名の画像や文書が電子的に署名されていることを示す脚注（有効な電子署名プロセス以外の手段で入力されている場合）だけでは十分ではない。 電子署名機能に関連して、ユーザーID と秘密パスワードからなる従来の認証をバイオメトリクス認証（例：指紋、手、顔、又は虹彩スキャナ）に置き換える場合、実装された解決策を徹底的に

英文	和訳
sufficient. If, in connection with an electronic signature functionality, a traditional authentication consisting of a user ID and a secret password is replaced by biometric authentication (e.g. fingerprint, hand, face or iris scanner), the implemented solution should be thoroughly validated and documented. (See also section 3.9 of OECD Document No 17 (OECD, 2016[4]))	検証し、文書化する必要がある。 (OECD Document No 17 (OECD, 2016[4])の 3.9 節も参照)
6.5. Generation of verified copies A verified copy (irrespective of the type of media used) of data should be confirmed (i.e. documented with dated signature or by generation through a validated process) to have the same information, including data that describe the context, content, and structure, as the original. Original and verified copies must preserve the integrity (accuracy, completeness, content and meaning) of the data. Verification must be attributable to the individual who performs the verification. The date (and time if relevant) of the generation of the verified copy should be retained with the relevant copy. An electronic verified copy of data recorded in paper format can be generated, provided that there is a documented process, in place to ensure that the outcome is a verified copy.	**6.5. 検証済みコピーの生成** データの検証済みコピー（使用するメディアの種類は問わない）は、オリジナルと同じ情報（背景、内容、構造を記述するデータを含む）を持つことが確認されなければならない（日付入りの署名で文書化又は検証されたプロセスで作成）。 オリジナル及び検証済みコピーは、データインテグリティ（正確性、完全性、内容及び意味）を保持しなければならない。 検証は、検証を行った個人に帰属するものでなければならない。検証済みコピーを作成した日付（関連性がある場合は時刻も）は、該当するコピーと共に保持する必要がある。 紙媒体に記録されたデータの電子的な検証済みコピーは、結果が検証済みコピーであることを確実にするためのプロセスが文書化されていれば、作成することができる。

英文	和訳
6.6. Correction or amendment of data Any change in the raw data should be made so as not to obscure the previous entry, should indicate the reason for change and should be dated and signed or initialled by the individual making the change. For data generated as a direct computer input, computerised system design should always provide for the retention of full audit trails to show all changes to the data without obscuring the original record. It should be possible to associate all changes to data with the persons having made those changes, for example, by use of timed and dated (electronic) signatures (see also section 6.13 “Data audit trail”). Reason for changes should be given and recorded.	**6.6. データの訂正又は修正** 生データに変更を加える場合は、前回の入力内容が見えなくならないように行い、変更の理由を示し、変更を行った個人が日付と署名又は記名を行うものとする。 コンピュータへの直接入力で生成されたデータについては、コンピュータ化システムの設計において、元の記録を不明瞭にすることなくデータへの全ての変更を示す完全な監査証跡を常に保持するようにすべきである。データへの全ての変更を、時間と日付の入った（電子）署名などにより、変更を行った人と関連付けることが可能でなければならない（6.13 項「データ監査証跡」も参照）。変更の理由を示し、記録されるべきである。
6.7. Transcription Transcriptions should be avoided as they increase the risks of errors and inconsistencies. Where transcriptions cannot be avoided, they should be verified by a second person or operated by a validated system. The original records should be regarded as raw data and should be retained.	**6.7. 転記** 転記は、エラーや不整合のリスクを高めるため、避けるべきである。転記が避けられない場合は、第二の人物によって検証されるか、検証されたシステムによって実施されるべきである。オリジナルの記録は生データとみなし、保持すべきである。
6.8. Invalidating or Excluding Data Data may only be invalidated or excluded where it can be demonstrated through sound scientific or technical justification or	**6.8. データの無効化又は除外** データの無効化又は除外は、データが記録された事象を示していないことが、科学的・ 技術的に正当化されるか、又は論理的に証

英文	和訳
logical sense that the data are not representative of the recorded event. The rejection of analytical results due to equipment malfunction, or the invalidation of a clinical observation monitored from a dead animal are relevant examples. Investigations to find the cause of the generation of data that must be invalidated or excluded are essential. In all cases, the justification of the invalidation or exclusion should be documented and considered during data review and reporting. For common cases (e.g. incoherent analytical results for a single sample, or failure to meet acceptance criteria), the rules to exclude or invalidate data should be defined in advance in the study plan or in SOPs. All data (even if invalidated) should be retained with the data set and be available for review in a format that allows the validity of the decision to invalidate or exclude the data to be confirmed.	明された場合にのみ行われる。例えば、機器の故障による分析結果の不採用や、死亡動物から得られた臨床観察結果の無効化などが挙げられる。 無効又は除外しなければならないデータが発生した原因を突き止めるための調査は不可欠である。どのような場合でも、無効又は除外の正当な理由を文書化し、データレビューや報告の際に考慮する必要がある。一般的なケース（例：単一サンプルの矛盾する分析結果、又は許容基準を満たさない場合）については、データを除外又は無効にするルールを試験計画又は SOP で事前に定義しておくべきである。全てのデータ（無効化された場合も含む）はデータセットと一緒に保管し、データを無効化又は除外する決定の妥当性を確認できる形式でレビューに利用できるようにしておく。
6.9. Data Processing There should be adequate traceability of any user-defined parameters within data processing activities, including attribution to who performed the activity. Examples include calculations or (with proper access permissions) the selection and application of chromatography integration parameters or selection of gating parameters for analysis	**6.9. データ処理** データ処理作業におけるユーザーが定義したパラメータについては、誰がその作業を行ったかの帰属を含め、適切なトレーサビリティが必要である。例としては、計算、（適切なアクセス許可を得た上での）クロマトグラフィー積分パラメータの選択及び適用、フローサイトメトリーアッセイの分析のためのゲーティング

英文	和訳
of a flow cytometry assay. Processing data rules should be clearly defined and controlled by SOPs. The raw data and available audit trails of the process should be retained. Retained records should allow reconstruction of all data processing activities regardless of whether the output of that processing is subsequently reported. If data processing has been repeated with progressive modification of processing parameters, this should be visible with documented justification to ensure that the processing parameters are not being manipulated to achieve a more desirable end point.	パラメータの選択などが挙げられる。データ処理のルールは明確に定義し、SOP で管理すべきである。 処理に関する生データ及び利用可能な監査証跡を保持しなければならない。その処理の出力が後に報告されるかどうかにかかわらず、全てのデータ処理活動は、保持された記録により再構築できなければならない。処理パラメータを段階的に変更しながらデータ処理を繰り返している場合は、より望ましいエンドポイントを達成するために処理パラメータを操作していないことを保証するために、文書化された正当な理由と共にこのデータ処理を可視化しなければならない。
6.10. Data Migration Data migration procedures should include a rationale and be robustly designed and validated to ensure that data integrity is maintained during the data life cycle. Careful consideration should be given to understanding the data format and the potential for alteration at each stage of data generation, migration and subsequent storage. Measures to ensure and demonstrate that data are not altered during each step of the process should be in place. The challenges of migrating data are often underestimated, particularly regarding maintaining the full meaning and integrity of	**6.10. データ移行** データ移行手順は、データライフサイクルを通してデータインテグリティが維持されることを保証するために、根拠を含み、強固に設計され、検証されるべきである。データの生成、移行、及びその後の保管の各段階におけるデータ形式及び変更の可能性を、慎重に検討して理解しなければならない。プロセスの各段階でデータが改変されていないことを保証し、実証するための対策を講じる必要がある。 データを移行する際の課題、特に記録の完全な意味及び整合性を、関連するメタデータを含めて維持することについては過小評

英文	和訳
the records, including associated metadata. In case of migration from a party (the "sender") to another (the "receiver"), the data, and the associated metadata, date/time of migration, expected format and specification of a transfer protocol or agreement used to migrate the data should be defined before migration. Mechanisms of communication and coordination between the sender and the receiver should be in place to ensure that the received data have the same attributes as the sent data. (See also section 2.8 of OECD Document No 17 (OECD, 2016[4]))	価されがちである。 ある当事者（「送信者」）から別の当事者（「受信者」）への移行の場合、データ、及び関連するメタデータ、移行の日時、想定する形式、及びデータを移行するために使用する転送プロトコル又は契約の仕様は、移行前に定義しなければならない。受信したデータが送信したデータと同じ属性を持つことを保証するために、送信者－受信者間のコミュニケーション及び調整の方法が整備されていなければならない。 (OECD Document No 17 (OECD, 2016[4])の 2.8 節も参照)
6.11. Relational Database Retrieval of information from a relational database requires a database reporting tool or the original application that created the record. Amendments to data should not be performed directly into the database fields but should be via the originator software package, so that appropriate audit trail entries and controls remain in place. Nevertheless, if a data change by a system administrator is required directly into the database, this should be justified, controlled, documented, have the study director's approval and the process should be described in an SOP. Access rights for database entry or amendment should be controlled,	**6.11. リレーショナルデータベース** リレーショナルデータベースからの情報のリトリーブには、データベースレポートツール又はレコードを作成したオリジナルのアプリケーションが必要である。 データの修正は、データベースのフィールドに直接行われるべきではなく、適切な監査証跡の入力及び管理が保持されるように、データ生成元となるソフトウェアパッケージを介して行われるべきである。それにもかかわらず、システム管理者によるデータベースへの直接のデータ変更が必要な場合には、これは正当化され、管理され、文書化され、試験責任者の承認を得ていなければならず、そのプロセスは SOP に記述されるべきである。

英文	和訳
and consistent with the requirements for computerised system user access/system administrator roles (see also section 8.2 “Computerised system access and roles”).	データベースへの入力又は修正のためのアクセス権は管理されるべきであり、コンピュータ化システムのユーザーアクセス／システム管理者の役割の要件と一致しなければならない（8.2 「コンピュータ化システムへのアクセス及び役割」の項も参照)。
6.12. Computerised System Transactions A computerised system transaction where a parameter must be within a defined limit, range, or distribution to ensure quality of the data should be considered as critical. Computerised systems should be designed to ensure that the execution of such transactions are recorded contemporaneously. Where transactional systems are used, the combination of multiple unit operations into a combined single transaction should be avoided (e.g. multiple data entry before saving), and the time intervals before saving of data should be minimised. Systems should be designed to require saving data to permanent memory before prompting users to make changes. Exceptions to these requirements should be justified. TFM should define during the development of the system (e.g. via the user requirements specification) what critical transactions are linked to that system based on the functionality and the level of risk associated with the system. Critical transactions should be	**6.12. コンピュータ化システムトランザクション** あるパラメータが既定の限界値、範囲、又は分布内に収まっていることを以ってデータの品質を確保するコンピュータ化システムのトランザクションは、重要とみなされるべきである。コンピュータ化システムは、そのようなトランザクションの実行が同時に記録されるように設計されるべきである。トランザクションシステムを使用する場合、複数のユニット操作を組み合わせて単一のトランザクションにすることは避けるべきであり（例：保存前の複数のデータ入力)、データの保存までの時間間隔は最小限にすべきである。システムは、ユーザーに変更を促す前に、データを恒久的なメモリに保存するように設計されるべきである。これらの要件に対する例外事項は、正当化しなければならない。 TFM は、そのシステムに関連する機能及びリスクのレベルに基づき、どのような重要なトランザクションがそのシステムに関連付けられているかをシステムの開発中に（例えば、ユーザー要求仕様書を通じて）定義すべきである。重要なトランザクションは、

英文	和訳
documented with process controls that consider system design (prevention), together with monitoring and review processes. Oversight of activities should alert to failures that are not addressed by the process design. Surveillance activities of critical transactions should be considered as part of the QA programme.	プロセスの監視・レビューと共にシステム設計（防止）を検討するプロセスコントロールと合わせて文書化する必要がある。活動の監視により、プロセス設計によって対処されていない障害を警告しなければならない。重要なトランザクションの監視活動は、QA プログラムの一部として考慮されるべきである。
6.13. Data Audit Trail Where computerised systems are used to capture, process, modify, report, store or archive data electronically, system design should always provide for the retention of audit trails to show all changes to, or deletion of the data while retaining previous data. It should be possible to associate all data and changes to data with the persons making those changes, and changes should be dated and time stamped (time and including, where applicable, the time zone). The reason for the change should also be recorded. The items included in the audit trail should be those of relevance to permit reconstruction of the process or activity. Audit trails should always be switched on during GLP activities. Any personnel with a direct interest in the data (study directors, heads of analytical departments, study personnel etc.) should not have the ability to amend or switch off the audit trail functionality. Where a	**6.13. データ監査証跡** コンピュータ化システムを使用してデータを電子的に収集、処理、修正、報告、保管又は 保存する場合、過去のデータを保持しつつ、データへの全ての変更又は削除を示す監査証跡の保持を、システム設計で常に規定する必要がある。全てのデータ（生成）及びデータへの変更を、その変更を行った者と関連付けることが可能でなければならず、変更には日付とタイムスタンプ（時間と、該当する場合はタイムゾーンを含む）が必要である。変更の理由も記録しなければならない。監査証跡には、プロセス又は活動の再構築を可能にする関連項目が含まれていなければならない。 監査証跡は、GLP 活動中は常にオンにしておくべきである。データに直接関わりを持つ職員（試験責任者、分析部門の責任者、試験担当者など）は、監査証跡の機能を修正したり、オフにしたりする権限を持つべきではない。システム管理者が監査証跡機能を修正又はオフにした場合には、監査証跡は自動的にこの活動を記

英文	和訳
system administrator amends or switches off the audit trail functionality, the audit trail should record this automatically and it should also be recorded automatically when the audit trail functionality is switched on again. Where relevant audit trail functionality does not exist or systems do not meet the audit trail and individual user account expectations (e.g. within legacy systems), demonstrated progress should be available to address these shortcomings. This should either be through add-on software that provides these additional functions or by an upgrade to a compliant system. Remediation has to be identified and implemented in a timely manner. If a system has no audit trail capability and review of available systems cannot identify alternatives and technological adaptations or additions to the existing system (i.e. remediation is not possible), this should be justified by evidence that a compliant solution is being worked upon and what mitigation activities, such as alternative level of control, temporarily supports the continued use. Alternative levels of control may be achieved by, for example, the use of manual logbooks or the definition of strict restricted access rights to the system. The printouts of the data could be also considered if integrity of data, including	録し、監査証跡機能が再びオンになったときにも自動的に記録しなければならない。 関連する監査証跡機能が存在しない場合、又はシステムが監査証跡及び個々のユーザーアカウントの期待値を満たしていない場合（レガシーシステム内など)、これらの欠陥への対処を実施して進展していることを示すことができなければならない。これは、これらの追加機能を提供するアドオンソフトウェアによるものか、準拠したシステムへのアップグレードによるものでなければならない。改善策は、適時に特定し、実施しなければならない。 システムに監査証跡機能がなく、利用可能なシステムを検討しても代替システム及び技術的な適合システム、あるいは既存システムへの追加ができない場合（すなわち、改善が不可能な場合）は、適合した解決策を検討していること、及び、どのような（リスク）低減策で一時的に継続使用をサポートしているのか、例えば代替となる管理レベルを根拠として示し、その正当性を示さなければならない。代替となる管理レベルは、例えば、手書きの使用記録の利用やシステムへの厳重な制限付きアクセス権の定義などによって達成することができる。メタデータを含むデータの完全性が保証されていれば、データのプリントアウトも考慮できる。代替管理策は、効果的であり、リスクに基づいており、SOP で規定

英文	和訳
metadata, is ensured. Alternative controls measures should be proven to be effective, risk-based, defined within an SOP and periodically reviewed for reassessment. Some GLP Compliance Monitoring Authorities may not accept systems without audit trail functionality including those with alternative control measures. (See also section 3.4 of OECD Document No 17 (OECD, 2016[4]))	されており、再評価のために定期的に見直されていることが立証されなければならない。 GLP 適合性査察機関の中には、代替管理策を含む監査証跡機能のないシステムを受け入れないところもある。 (OECD Document No 17 (OECD, 2016[4])のセクション 3.4 も参照)
6.14. Data retention Data required to allow the full reconstruction of activities of the studies should be collected and retained. Data should be retained with the associated metadata when applicable. Derived data should be retained with their raw data when necessary for the reconstruction of the study. Data and document retention arrangements should ensure the protection of records from intended or unintended alteration or loss. Secure controls must be in place to ensure the data integrity of the record throughout the retention period. The selected method for retention should ensure that data of appropriate accuracy, completeness, content and meaning are collected and retained for its intended use.	**6.14. データの保持** 試験の活動を完全に再構築するために必要なデータを収集し、保持するべきである。データは、該当する場合、関連するメタデータと共に保持されるべきである。派生したデータは、試験の再構築に必要な場合、生データと共に保持されるべきである。 データ及び文書の保持に関する取り決めでは、意図的又は非意図的な改変や損失から記録が保護されることを確実にしておく。保持期間中、記録のデータインテグリティを確保するための安全な管理が行われなければならない。 保持のために選択された方法は、意図された用途のために適切な正確性、完全性、内容及び意味を持つデータが収集され、保持されることを保証するものでなければならない。

英文	和訳
Retention of dynamic data Information that is captured in a dynamic state should remain available in that state. For example, video recordings used to demonstrate an activity cannot be reduced to a single static image or to a series of single images. Computerised systems that generate dynamic records should allow the dynamic nature of the data to be retained. It may be a challenge to print on paper dynamic records without losing the interactive relationship between the user and the record content. Any printouts should comprise of all associated available metadata, and should keep the link that binds them to the raw data. For example, if the associated metadata are printed in another page from the raw data, the integrity of the link is not ensured and the relationship to the raw data questionable. When electronic raw data cannot be converted to verified copies (e.g. to prints on paper or pdf) without a loss of information (e.g. associated metadata), they should remain available in the original state. If the computerised system cannot be maintained, e.g. if it is no longer supported, then records will be archived according to a documented archiving strategy prior to decommissioning the computerised system.	***動的なデータの保持*** 動的な状態で収集された情報は、その状態のまま利用可能でなければならない。例えば、ある活動を示すために使用されるビデオ録画は、単一の静止画像又は一連の単一画像として情報を減じることはできない。 動的な記録を生成するコンピュータ化システムでは、データの動的な性質を保持できるようにする必要がある。 ユーザーと記録内容の間の相互作用的な関係を失うことなく、動的な記録を紙に印刷することは難しいかもしれない。 印刷物には、関連する全ての利用可能なメタデータが含まれていなければならず、生データとの関連性を維持しなければならない。例えば、関連するメタデータが生データとは別のページに印刷されている場合、関連性の完全性が確保されず、生データとの関係が疑わしいものとなる。 電子的な生データが，情報（関連するメタデータなど）を失うことなく，検証済みのコピー（紙への印刷や pdf など）に変換できない場合は，オリジナルの状態で利用可能なままにしておくべきである。 コンピュータ化システムがサポートされなくなるなどして維持できなくなった場合は、 コンピュータ化システムを廃止する前

英文	和訳
It is conceivable for some data generated by electronic means to be retained in an acceptable paper or electronic format, where it can be justified that a static record maintains the integrity of the raw data. However, the data retention process must be shown to include verified copies of all raw data, metadata, relevant audit trail and result files, any variable software/system configuration settings specific to each record, and all data processing runs (including methods and audit trails) necessary for reconstruction of a given raw data set. When printing on paper is the chosen solution, it would require a validated means to verify that the printed records were an accurate representation of the data set. All information should be retained. Any loss of information should be identified and the risk on the integrity of the data set should be assessed and documented.	に、文書化された資料保存戦略に従って記録を資料保存する。電子的な手段で生成されたデータは、静的な記録によって生データの完全性が維持されていることが正当化される場合には、受け入れ可能な紙又は電子形式で保持することが考えられる。しかし、データ保持プロセスは、特定の生データセットの再構築に必要な全ての生データ、メタデータ、関連する監査証跡及び結果ファイルの検証済みコピー、各記録に固有の可変ソフトウェア／システム構成設定、及び全てのデータ処理実行（方法及び監査証跡を含む）を含むことを示さなければならない。 紙に印刷することが選択された場合、印刷された記録がデータセットの正確な複写であることを検証するためのバリデートされた手段が必要である。 全ての情報は保持されるべきである。情報の損失を特定し、データセットの完全性に対するリスクを評価し、文書化する必要がある。
Retention of electronic signature An electronically signed document is generally a dynamic record. Where a document is electronically signed, the metadata associated with the signature (i.e., printed name of the signer, meaning of signature, and date and time of the signature) should be electronically	***電子署名の保持*** 電子的に署名された文書は、一般的に動的な記録である。文書が電子的に署名されている場合、署名に関連するメタデータ（すなわち、署名者の印刷された名前、署名の意味、及び署名の日付と時刻）は電子的に保持されるべきである。電子的に署名された文

英文	和訳
retained. A document that is signed electronically is only valid when retained electronically unless the paper print out or the pdf copy retains all the traceability to the signers identity, date and time and meaning of signature.	書は、紙に印刷されたものや PDF コピーが署名者の身元、署名の日時、署名の意味に対する全てのトレーサビリティを保持していない限り、電子的に保持された場合にのみ有効である。
Retention of electronic communications Electronic communications are another example of records in a dynamic state. Where data are supported by electronic communication methods such as email and electronic messaging (e.g. allowing verification of GLP activities and responsibilities), processes for ensuring retention and the collation of electronic communications should be established (including ensuring that the records are complete and integrity is intact). Such mechanisms should be designed to maintain the attributability and integrity of those relevant electronic communications such as ensuring that the sender and receiver can be determined alongside appropriate dates and times. Any attachments should remain associated with the corresponding message and message chains should be preserved. Where possible, these should be retained in their original format but if this is not possible, TFM should implement processes for faithful	***電子通信の保持*** 電子通信もまた、動的な状態にある記録の一例である。 データが電子メールや電子メッセージなどの電子的な通信手段でサポートされている場合（例：GLP 活動と責任の確認が可能）、電子通信の保持と照合を確実にするためのプロセスを確立する必要がある（記録が完全であり、完全性が損なわれていないことの確認を含む）。このような仕組みは、適切な日時と共に送信者と受信者を確実に特定できるようにするなど、関連する電子通信の帰属性と完全性を維持するように設計されるべきである。全ての添付ファイルは、対応するメッセージとの関連性を維持し、メッセージチェーンを保存する必要がある。 可能であれば、これらは元の形式で保持されるべきだが、それが不可能な場合、TFM は保持可能な形式での忠実な転写及び検証のためのプロセスを組み込む必要がある。 電子通信の紙への印刷又は単純な PDF ファイルへの移行では、必要な完全性を確保することはできない。

英文	和訳
transcription and verification in a retainable format. The printout on paper or the migration in a flat pdf file of electronic communication cannot ensure the required integrity.	
Retention of verified copies Verified copies from electronic dynamic records (generated by migration) should be retained in dynamic state, so that the verified copy could include the metadata required to ensure that the full meaning of the data (e.g. date formats, context, layout, electronic signatures and authorisations) is kept and its history, including the creation of the verified copy, may be reconstructed. Verified copies may be retained in place of the original, provided that a documented system is in place to verify and record the integrity of the copy. Consideration should be given to any risk associated with the destruction of original records. It should be recognised that some regulatory authorities require originals to be retained.	***検証済みコピーの保持*** 電子的な動的記録からの検証済みコピー（移行によって生成される）は、動的な状態で保持されるべきであり、検証済みコピーには、データの完全な意味（例えば、日付形式、背景情報、レイアウト、電子署名及び認証）を保持し、検証済みコピーの作成を含むその履歴を再構築することを保証するために必要なメタデータが含まれる。 検証済みコピーは、コピーの完全性を検証し記録するための文書化されたシステムが整備されていれば、オリジナルの代わりに保持することができる。オリジナルの記録の破損に関連するあらゆるリスクを考慮する必要がある。一部の規制当局はオリジナルの保持を要求していることを認識すべきである。
Retention of data from hybrid systems Where hybrid systems are required to be used, this should be clearly documented as to what constitutes the whole data set and SOP should define which records should be retained.	***ハイブリッドシステムからのデータの保持*** ハイブリッドシステムを使用する必要がある場合は、何が全データセットを構成するかを明確に文書化し、SOP はどの記録を保持すべきかを定義すべきである。
Retention of data on other media	***他のメディア上のデータの保持***

英文	和訳
Where data are captured by a photograph or imaging methodologies and technologies (or other media), the requirements for storage of that format throughout its life cycle should follow the same considerations as for all data, considering any additional controls required for that format. Where the original format cannot be retained due to degradation issues, alternative mechanisms for recording including verification of the faithfulness of the process (e.g. photography or digitalisation) and subsequent storage may be considered, and the selection rationale documented.	データが写真又は画像処理技術（又は他のメディア）によって収集される場合、その形式のライフサイクル全体にわたる保存に関する要件は、その形式に必要な追加管理を考慮した上で、全てのデータと同じ考えとなる。劣化の問題で元の形式を保持できない場合は、プロセス（写真やデジタル化など）の忠実性の検証とその後の保存を含む記録のための代替メカニズムを検討し、その選択の根拠を文書化する。
6.15. Back-up Mechanisms for ensuring that back-ups have completed successfully should be considered. The systems used should be validated and each back-up can be verified to ensure that it has functioned correctly e.g. by confirming that the data size and other copied properties matches that of the original record. Back-up and recovery processes for electronic data should be tested where appropriate. Such as when changes occur to either the process or tools or applications used during back-up or restore. Moreover, the sustainability of some electronic media used for back-up (such as CDs, DVDs, etc.) needs to be verified periodically.	**6.15. バックアップ** バックアップが正常に完了したことを確認するための仕組みを検討する必要がある。使用されるシステムは検証されるべきであり、各バックアップは、データのサイズやその他のコピーされた特性が元の記録のものと一致することを確認するなどにより、正しく機能したことを確認することができる。 電子データのバックアップとリカバリーのプロセスは、必要に応じてテストされるべきである。例えば、バックアップや復元の際に使用するプロセスやツール、アプリケーションに変更が生じた場合などである。さらに、バックアップに使用される一部の電子メディア（CD、DVD など）の持続性も定期的に検証する必要が

英文	和訳
The back-up procedures should be described in an SOP, and back-up activities should be documented. Back-ups for recovery purposes do not replace the need for archiving of data and metadata for the purposes of reconstruction of the study activity.	ある。 バックアップの手順は SOP に記述し、バックアップ活動を文書化する必要がある。 復旧目的のバックアップは、試験活動の再現を目的としたデータ及びメタデータの資料保存の要求に代わるものではない。
6.16. Archive Data should be archived securely, under the control of the unique archivist, including, where relevant, an appropriate electronic repository whether this is on the original system or elsewhere, subject to suitable controls or in a stand-alone electronic archive. All archive sites (physical as well as electronic) associated with the archived data should be identified and documented. The Principles of GLP for archiving must be applied consistently to electronic and non-electronic data. It is therefore important that electronic data are stored with the same levels of access control and indexing as non-electronic data. Archived records may be the original record and/or a verified copy (see also in section 6.14 “Retention of verified copies”) and should be protected such that they cannot be altered or deleted without detection. Archive arrangements must be designed to permit retrieval and	**6.16. 資料保存** データは、固有の資料保存施設管理責任者の管理下で、安全に資料保存されるべきであり、関連する事項として、独自のシステムなのか、適切な管理下にあるその他のものなのか、スタンドアローンの電子アーカイブであるかを問わず、適切な電子収納場所であることも含まれる。 資料保存されたデータに関連する全ての資料保存場所（物理的及び電子的）を特定し、 文書化する必要がある。 資料保存のための GLP の原則は、電子データ及び非電子データに一貫して適用されなければならない。そのため、電子データは非電子データと同じレベルのアクセス制御と索引を付けて保存することが重要である。 資料保存される記録は、オリジナルの記録及び／又は検証済みコピー（6.14「検証済みコピーの保持」も参照）であり、知らない間に変更又は削除できないように保護されなければならない。

英文	和訳
readability of data and metadata throughout the required retention period. When legacy systems can no longer be supported, consideration should be given to the importance of the data, and if required, to maintaining the software for data accessibility purposes. This may be achieved by maintaining software in a virtual environment. Where this is not possible, data should be migrated before archiving in a controlled, tested, and verified way to a system that can continue to be accessed. Migration to an alternative file format that retains the verified copy attributes of the data may be necessary with increasing age of the legacy data. Where migration with full original record functionality is not technically possible, selection from the options available would have to be based on risk and importance of data over time. The migration file format should be selected taking into account the balance of risk between long-term accessibility versus the possibility of reduced dynamic data functionality (e.g. data interrogation, trending, re-processing etc.). It is recognised that the need to maintain accessibility may require migration to a file format that loses some attributes and/or dynamic data functionality. It is the TFM's responsibility to assess the	資料保存施設の配置は、要求された保存期間中、データ及びメタデータのリトリーブ及び読み取りが可能なように設計されなければならない。 レガシーシステムのサポートができなくなった場合、データの重要性を考慮し、必要であれば、データへのアクセス性のためにソフトウェアを維持することを検討しなければならない。これは、仮想環境でソフトウェアを維持することで実現できるかもしれない。これが不可能な場合は、データを資料保存する前に、制御され、テストされ、検証された方法で、引き続きアクセス可能なシステムに移行する必要がある。レガシーデータの経年変化に伴い、データの属性を保持する検証済みコピーを別のファイル形式に移行することが必要になる場合がある。 完全なオリジナルレコードの機能を備えた移行が技術的に不可能な場合、利用可能な選択肢からの選択は、リスク及び経時的なデータの重要性に基づいて行わなければならない。移行ファイルの形式は、長期的なアクセスのし易さと動的なデータ機能（データの照会、傾向、再処理など）が低下する可能性との間のリスクバランスを考慮して選択する必要がある。アクセス性を維持する必要性から、一部の属性及び／又は動的データ機能を失ったファイル形式への移行が必要となる場合があることは認識されてい

英文	和訳
impact of such losses and maintain the link between the readable audit trail or electronic signatures and the audited data to an acceptable level. (See also section 3.11 of OECD Document No 17 (OECD, 2016[4]))	る。このような欠損の影響を評価し、読み取り可能な監査証跡又は電子署名と監査対象データとの間のリンクを許容可能なレベルに維持することは TFM の責任である。 (OECD Document No. 17 (OECD, 2016[4])の 3.11 項も参照)
7. Data review **7.1. General considerations** Data review consists of appropriate verifications of critical data for quality control which can be conducted by study directors or other personnel. The objectives of data review are: ・ to detect any deletion, amendment, alteration or exclusion; ・ for the study directors, to check that all raw data generated are fully documented and recorded; and ・ to assess the efficiency of data governance measures by review of a complete data set generated through processes throughout the data life cycle. To be effective, the level of data review and the scope of it should be defined by a risk assessment. Identified critical data should be reviewed through the critical steps of their data life. Data review should also include a review of relevant metadata, including audit	**7. データレビュー** **7.1. 一般的な考慮事項** データレビューは、品質管理のために重要なデータを適切に検証することであり、試験責任者又は他の職員が実施することができる。 データレビューの目的は以下の通りである。 ・ 削除、修正、変更、除外を検出すること。 ・ 試験責任者は、生成された全ての生データが完全に文書化され、記録されていることを確認する。 ・ データのライフサイクル全体のプロセスを通じて生成された完全なデータセットをレビューすることにより、データガバナンス対策の効率性を評価する。 効果的に行うためには、データレビューのレベルとその範囲はリスク評価によって定義されるべきである。特定された重要なデータは、そのデータのライフサイクルの重要なステップとしてレビューされるべきである。データレビューには、監査証跡又はその

英文	和訳
trails or elements of them. Data review should be documented. The record of the review should include any deviations to the Principles of GLP, study plans or SOPs detected by the review, the date that review was performed and the signatures of those performing the review. There should be a procedure that describes the process for the data review. A procedure should also describe the actions to be taken if data review identifies deviations. This procedure should enable data corrections or clarifications to provide visibility of the original record, and audit trailed traceability of the correction. Many software packages allow configuration of customised reports to support data review. Changes to report configuration should be controlled to prevent unauthorised changes. The system should be validated and where relevant the report outputs should be verified. Note: The data review conducted by QA aims to support the statement that the reported results accurately and completely reflect the raw data of the studies. It may also be effective when auditing data integrity governance procedures. The level of review should be linked with the criticality of the data.	要素を含んだ関連するメタデータのレビューも含まれるべきである。 データレビューは文書化されるべきである。レビューの記録には、レビューによって検出された GLP の原則、試験計画書又は SOP に対する逸脱、レビューが行われた日付及びレビューを行った者の署名を含めるべきである。 データレビューのプロセスを記載した手順書が必要である。手順書には、データレビューで逸脱が見つかった場合の処置についても記述されているべきである。この手順書では、データの修正又は元の記録の可読性の明確化や修正の監査証跡での追跡調査を可能にする必要がある。 多くのソフトウェアパッケージでは、データレビューを支援するためにカスタマイズされたレポートの設定が可能である。レポート設定の変更は、不正な変更を防ぐように管理されるべきである。システムを検証し、必要に応じてレポート出力を検証するべきである。 注：QA が行うデータレビューは、報告された結果が試験の生データを正確かつ完全に反映しているという陳述を裏付けることを目的としている。また、データインテグリティガバナンスの手順を監査する際にも有効である。レビューのレベルは、データの

英文	和訳
	重要性と連動させる必要がある。
7.2. Review of data audit trail It is not necessary for audit trail review to include every system activity. The relevant data among all the retained data in audit trails should be identified to permit robust data review/verification. The review should be conducted according to a documented risk-based process identifying the criticality of the data subject to the review and the criticality of transactions identified through the data flow. The review may be achieved by direct access to the system audit trail or by use of appropriately designed and validated system reports. Routine data review should include a documented audit trail review as determined by the risk assessment. When designing a system for review of audit trails, this may be limited to those activities with GLP relevance (e.g. relating to data creation, processing, compliance with procedures, modification and deletion etc.). Audit trails may be reviewed as a list of relevant data, or by an 'exception reporting' process. An exception report is a validated search tool that identifies and documents predetermined 'abnormal' data or actions, which requires further attention or investigation by the data reviewer.	**7.2. データ監査証跡のレビュー** 監査証跡のレビューでは、全てのシステム活動を含める必要はない。 監査証跡の全ての保持データの中から関連するデータを特定し、堅牢なデータレビュー／検証を可能にする必要がある。レビューは、レビューの対象となるデータの重要性と、データフローを通じて特定されるトランザクションの重要性を特定する、文書化されたリスクに基づくプロセスに従って実施されるべきである。レビューは、システムの監査証跡に直接アクセスするか、適切に設計され検証されたシステムのレポートを使用することによって達成することができる。 定期的なデータレビューには、リスクアセスメントによって決定された、文書化された監査証跡のレビューを含めるべきである。監査証跡のレビューのためのシステムを設計する際には、GLPに関連する活動（データの作成、処理、手順の遵守、変更及び削除などに関するもの）に限定することができる。監査証跡は、関連するデータのリストとして、又は「例外報告」プロセスによってレビューされる。例外レポートとは、データレビュー担当者がさらなる注意や調査を必要とする、事前に設定された「異常な」

英文	和訳
Reviewers should have sufficient knowledge and system access to review relevant audit trails, raw data and metadata.	データ又はアクションを特定して文書化する、検証された検索ツールである。 レビュー担当者は、関連する監査証跡、生データ及びメタデータをレビューするための十分な知識とシステムアクセスを有していなければならない。
7.3. Review of data from hybrid systems Increased data review is likely to be required for hybrid systems because they are vulnerable to non-attributable data changes. All records from hybrid systems that are defined by the data set should be reviewed by a qualified person. The level of this control should be adapted to the processes used in the hybrid system. Review of data from hybrid systems should be clearly defined and described so that it is possible to determine the actual data sources reviewed.	**7.3. ハイブリッドシステムからのデータのレビュー** ハイブリッドシステムは、帰属しないデータ変更に対して脆弱なため、データのレビューを増やす必要があると思われる。データセットによって定義されるハイブリッドシステムからの全ての記録は、有資格者によってレビューされるべきである。この管理のレベルは、ハイブリッドシステムで使用されているプロセスに合わせるべきである。ハイブリッドシステムからのデータのレビューは、明確に定義され、レビューされた実際のデータソースを判断できるように記述されるべきである。
8. Access to data **8.1. General considerations** Access rights to data and records should be always created based on the risk assessment of each phase of the data lifecycle. Access right should be defined to allow the personnel to fulfil their GLP responsibilities.	**8. データへのアクセス** **8.1. 一般的な考慮事項** データ及び記録へのアクセス権は、常にデータライフサイクルの各段階におけるリスク評価に基づいて設定されるべきである。 アクセス権は、職員が GLP の責任を果たすために限定されるべきである。

英文	和訳
Access to records for personnel performing data review activities should be maintained. The necessary access (including to records, audit trails and system functionality), permissions and training should be available to support QA inspection to verify if all studies are conducted in compliance with the Principles of GLP.	データレビュー活動を行う職員の記録へのアクセス権は維持されるべきである。 全ての試験が GLP 原則に準拠して実施されているかどうかを検証するための QA 調査を支援するために、必要なアクセス権（記録、監査証跡、システム機能を含む）、権限、トレーニングが利用可能であるべきである。
8.2. Computerised system access and roles ***User access*** Full use should be made of access controls to ensure that personnel have access only to functionality that is appropriate for their job and study role, and that actions are attributable to a specific individual. TFM must be able to demonstrate the access levels granted to individual staff members and ensure that historical information regarding user access level is available. Where the system does not capture these data, then a paper record should be available. Controls should be applied to both the operating system and application levels. Individual login at operating system level may not be required if appropriate controls are in place to ensure data integrity (e.g. individual login at application level should be sufficient if modification of data outside the application is not possible).	**8.2. コンピュータ化システムへのアクセスと役割** ***ユーザーアクセス*** 職員がその職務及び試験上の役割に適した機能にのみアクセスできること、及びアクションが特定の個人に帰属することを保証するために、アクセス制御を十分に活用すべきである。TFM は、個々のスタッフに与えられたアクセスレベルを実証し、ユーザーのアクセスレベルに関する履歴情報が利用可能であることを保証できなければならない。システムがこれらのデータを収集しない場合は、紙の記録が利用可能でなければならない。制御は、オペレーティングシステムレベルとアプリケーションレベルの両方に適用されるべきである。データインテグリティを確保するための適切な制御が行われている場合、オペレーティングシステムレベルでの個別のログインは必要ないかもしれない（例えば、アプリケーション外でのデータの変更が不可能である場合、アプリ

英文	和訳
For systems generating, amending or storing GLP data, shared logins or generic user access should not be used. Where the computerised system design supports individual user access, this function must be used. This may require the purchase of additional licences. Systems that are not used in their entirety for GLP purposes but do have elements within them, such as approved suppliers, stock status, location and transaction histories that are GLP applicable require appropriate assessment. It is acknowledged that some computerised systems support only a single user login or limited numbers of user logins. Where no suitable alternative computerised system is available, equivalent control may be provided by third-party software or a paper-based method of providing traceability (with version control). The suitability of alternative systems should be justified and documented.	ケーションレベルでの個別のログインで十分である)。 GLP データを生成、修正又は保存するシステムでは、共有ログイン又は一般的なユーザーアクセスを使用してはならない。コンピュータ化システムの設計上、個々のユーザーのアクセスをサポートすることが可能な場合は、この機能を使用しなければならない。この場合、追加ライセンスの購入が必要となることがある。 システムが完全に GLP 目的で使用されているわけではないが、承認された供給者、在庫状況、場所、トランザクションの履歴など、GLP に適用可能な要素を持つシステムについては、適切な評価が必要である。 コンピュータ化システムの中には、1 人のユーザーによるログインのみ、又は限られた数のユーザーによるログインしかサポートしていないものがあることが知られている。適切な代替コンピュータ化システムが利用できない場合には、サードパーティ製のソフトウェアや紙ベースのトレーサビリティー (バージョン管理を含む) によって同等の制御を提供することができる。代替システムの適合性は、正当化され、文書化されなければならない。
System administrator access System administrator access should be restricted to the minimum number of people possible taking account of the size and nature of the	***システム管理者のアクセス*** システム管理者へのアクセスは、試験施設の規模や性質を考慮して、可能な限り最小限の人数に制限されるべきである。一般的な

英文	和訳
test facility. The generic system administrator account should not be available for routine use. Personnel with system administrator access should log in with unique credentials that allow actions in the audit trail(s) to be attributed to a specific individual. The intent of this is to prevent giving access to users with a potential conflict of interest to prevent unauthorised changes that would not be traceable to that person. System administrator rights (permitting activities such as data deletion, database amendment or system configuration changes) should not be assigned to individuals with a direct interest in the data (data generation, amendment, deletion, review or approval). Any changes to study data performed by a system administrator must only be done after receiving prior permission from the study director. Where an independent system administrator cannot be assigned (e.g. in small test facilities), a similar level of control may be achieved using dual user accounts with different privileges with all changes performed under system administrator access subject to appropriate review and approval. The individual should log in using the account with the appropriate access rights for the given task e.g. a laboratory technician performing	システム管理者アカウントは、日常的に使用できないようにするべきである。システム管理者へのアクセス権を持つ職員は、監査証跡のアクションを特定の個人に帰属させることができるよう、固有の認証情報を用いてログインする必要がある。これは、利益相反の可能性があるユーザーにアクセス権を与えて、その人物にたどり着けないような不正な変更を防ぐことを目的としている。 システム管理者の権利（データの削除、データベースの修正、システム構成の変更などの活動を許可する）は、データ（データの生成、修正、削除、レビュー又は承認）に直接利害関係を持つ個人に割り当ててはならない。システム管理者が行う試験データの変更は、試験責任者の事前の許可を得てから行わなければならない。 独立したシステム管理者を置くことができない場合（小規模な試験施設など）は、異なる権限を持つ二重のユーザーアカウントを使用して同様のレベルの管理を行うことができ、システム管理者のアクセス下で行われた全ての変更は、適切なレビューと承認の対象となる。 個人は与えられたタスクに応じた適切なアクセス権を持つアカウントを使用してログインしなければならない。例えば、データチェックを行う実験室の技術者は、そのタスクに対してより適切

英文	和訳
data checking should not log in as system administrator where a more appropriate level of access exists for that task. The suitability of such an arrangement should be periodically reviewed. (See also sections 1.3.1 and 3.7 of OECD Document No 17 (OECD, 2016[4]))	なレベルのアクセス権がある場合、システム管理者としてログインすべきではない。このような取り決めの適切性は、定期的に見直されるべきである。 (OECD Document No 17 (OECD, 2016[4])の 1.3.1 項及び 3.7 項も参照)

一般社団法人日本 QA 研究会 GLP 部会 第 1 分科会

2022 年 1 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. 22
GLP データインテグリティに関する GLP 作業部会のアドバイザリー文書
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 SERIES ON PRINCIPLES OF GOOD LABORATORY PRACTICE AND COMPLIANCE MONITORING Number 22
Advisory Document of the Working Party on Good Laboratory Practice on GLP Data Integrity
https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=ENV-CBC-MONO(2021)26%20&doclanguage=en

一般社団法人日本 QA 研究会
〒103-0023 東京都中央区日本橋本町 2-3-11
日本橋ライフサイエンスビルディング 4 階
TEL：03-6435-2118 FAX：03-6435-2119