

OECD SERIES ON PRINCIPLES OF GOOD LABORATORY PRACTICE AND COMPLIANCE MONITORING

Advisory Document on GLP & Cloud Computing

Supplement 1 to Document Number 17 on Application of GLP Principles to computerised Systems

GLP 原則及び適合性モニタリングに関するOECD シリーズ

No.17 Supplement 1

GLP原則のコンピュータ化システムに対する適用

英文・和訳対比表

日本QA研究会 GLP 部会 第3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3分科会が、第16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より何らかの損害が生じたとしても本会は一切の責任を負いません。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。

なお、本文書に記載されている専門用語について網羅して解説することができませんでした。それらの用語につきましてはお手数ですが、ご自分で検索され、さらに理解を深めていただければ幸いです。

英文		和訳	
Table of contents		内容	
1. Background	3	1. 背景	3
2. Introduction	4	2. はじめに	4
3. Scope	5	3. 範囲	5
4. Overview of cloud computing	6	4. クラウドコンピューティング概論	6
4.1. Definition	6	4.1 定義	6
Figure 1 Cloud computing characteristics, deployment and service models	7	図1. クラウドコンピューティングの特徴、デプロイメントモデル、サービスモデル	7
4.2. Characteristics	8	4.2 特徴	8
4.3. Deployment models	10	4.3 デプロイメントモデル	10
Figure 2 Cloud computing deployment models	14	図2. クラウドコンピューティングデプロイメントモデル	14
4.4. Service models	15	4.4 サービスモデル	15
Figure 3 Shared management of the main components of a cloud computing service between the GLP test facility and the cloud service provider	19	図3. GLP試験施設とクラウドサービスプロバイダー間でのクラウドコンピューティングサービスの主要コンポーネントの共有管理	19

英文		和訳	
5. Cloud computing in GLP environment	20	5. GLP環境下でのクラウドコンピューティング	20
5.1. Responsibilities of the test facility	20	5.1 試験施設の責務	20
5.2. Requirements	23	5.2 要求事項	23
Table 1 GLP requirement management within different cloud service models	23	表1. 異なるクラウドサービスモデル内のGLP要求事項マネジメント	23
5.3 Implementation of cloud-based solution in GLP	28	5.3 GLPにおけるクラウドベースドソリューションの実装	28
5.3.1 Risk assessment and selection of the cloud-based services	29	5.3.1 クラウドベースドサービスのリスク評価と選別	29
5.3.2 Cloud service provider assessment	34	5.3.2 クラウドサービスプロバイダーの評価	34
5.3.3 Service Level Agreement (SLA)	38	5.3.3 サービスレベルアグリーメント	38
5.3.4 Validation of the computerised systems in the cloud-based service	44	5.3.4 クラウドベースドサービスにおけるコンピュータ化システムのバリデーション	44
6. Expectations of the GLP compliance monitoring authorities when inspecting cloud – based solutions	46	6. クラウドベースドソリューションを調査する際の GLP 適合性規制当局への期待	46
6.1. Implementation of the cloud solution	46	6.1 クラウドソリューションの実装	46
6.2. Life cycle of the cloud service application	48	6.2 クラウドサービスアプリケーションのライフサイクル	48
6.3. Electronic archives in cloud solution	49	6.3 クラウドソリューションにおける電子データアーカイブ	49
7. Conclusion	51	7. 結論	51
8. Glossary	52	8. 用語	52

英文	和訳
<p>1. Background</p> <p>The Good Laboratory Practice (GLP) Principles require that records and materials, including electronic records and data, necessary to reconstruct non-clinical safety studies meet the requirements for data quality, data integrity and data availability and are properly retained and archived.</p> <p>An increasing number of GLP test facilities use cloud applications to accommodate these requirements. However, the potential impact on GLP compliance should be considered when using cloud solutions. GLP test facilities have the ultimate responsibility for GLP compliance to assess risks to data integrity, data quality, data availability, data retention and data archiving. Cloud refers to delivery of on-demand network access to a shared pool of configurable computing resources to users and can include software, networks/platforms or infrastructure. Cloud-based solutions in GLP could cover the external development, maintenance and hosting, inside or outside of the premises of the test facility, of computing resources such as:</p> <ol style="list-style-type: none"> 1. Hardware or servers connected by networks. 2. Software or applications that capture, generate, analyse, migrate, store, archive data. 3. Interfaces between applications. 4. Databases. 	<p>1. 背景</p> <p>Good Laboratory Practice (GLP) 原則では、非臨床安全性試験の再構築に必要な記録と資料(電子記録やデータを含む)がデータの品質、データインテグリティ、データの可用性の要件を満たし、適切に一時保管及びアーカイブされることが求められている。これらの要件に対応するためにクラウドアプリケーションを使用するGLP試験施設が増えている。ただし、クラウドソリューションを使用する場合は、GLP適合性への潜在的な影響を考慮する必要がある。GLP試験施設は、データインテグリティ、データの品質、データの可用性、データの一時保管及びデータのアーカイブに対するリスクを評価するというGLP適合性に対する最終的な責任を負う。クラウドとは、構成可能なコンピューティングリソースの共有プールへのオンデマンドネットワークアクセスをユーザーに提供することを指し、ソフトウェア、ネットワーク/プラットフォーム、又はインフラストラクチャが含まれる場合がある。GLPのクラウドベースのソリューションは、試験施設の敷地の内外で、次のようなコンピューティングリソースの外部開発、メンテナンス、ホスティングをカバーする。</p> <ol style="list-style-type: none"> 1. ネットワークで接続されたハードウェア又はサーバー。 2. データを収集、生成、分析、移行、一時保管、アーカイブするソフトウェア又はアプリケーション。 3. アプリケーション間のインターフェース 4. データベース






英文	和訳
<p>2. Introduction</p> <p>This document describes the expectations that GLP Compliance Monitoring Authorities have of GLP test facilities which use cloud-based solutions. Cloud service may be involved in GLP data capture, processing, storage and archiving.</p> <p>This document focuses on the specific characteristics of cloud-based solutions, especially the co-operation between the test facility and the cloud service provider, and clarifies the requirements of the GLP Principles to be applied.</p> <p>This document is considered a supplement to Document No. 17 (Application of GLP Principles to Computerised Systems) (OECD, 2016[1]) and should be read and applied in conjunction with OECD Documents No. 1 (OECD Principles on Good Laboratory Practice) (OECD, 1997[2]), No. 15 (Establishment and Control of Archives that Operate in Compliance with the Principles of GLP) (OECD, 2007[3]), No. 5 (Compliance of laboratory suppliers with GLP principles) (OECD, 2002[4]) and No. 22 (GLP Principles and Data Integrity) (OECD, 2021[5]) and applicable national regulations.</p>	<p>2. はじめに</p> <p>この文書では、GLP 適合性規制当局がクラウドベースのソリューションを使用する GLP 試験施設に対して期待することについて説明する。クラウドサービスは、GLP データの収集、処理、一時保管及びアーカイブに関与する場合がある。この文書は、クラウドベースのソリューション固有の特徴、特に試験施設とクラウドサービスプロバイダーの間の協力を焦点を当て、適用されるGLP原則の要件を明確にする。この文書は、文書No.17 (GLP原則のコンピュータ化システムへの適用) (OECD、2016 [1]) の補足とみなされ、OECD 文書No.1 (OECD GLP 原則) (OECD、1997 [2])、No.15 (GLP 原則遵守下に運営される資料保存施設の設置及び管理) (OECD、2007 [3])、No. 5 (試験施設供給業者のGLP原則適合性) (OECD、2002年 [4]) 及び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) (OECD、2021年 [5]) 及び該当する国内規制と併せて読み、適用する必要がある。</p>

英文	和訳
<p>3. Scope</p> <p>Cloud services can be internally provided services of the test facility or of the company the test facility belongs to, or outsourced services by contracted IT service providers. When contracted, the service can be provided directly by a cloud service provider or via a vendor. Service providers may also have sub-contractors for all or part of the service. This document is applicable to all types of services.</p> <p>Note: the term “cloud service provider” will be used for all types of providers of cloud services including internal IT, external IT, hosted service provider, vendor (usually an individual or entity, who sells the services), supplier (usually the one whose work is to provide the requested services) or cloud provider in the rest of this document.</p> <p>The document applies to all cloud-based solutions, including the ones already in use.</p> <p>The expectations in this document for “test facilities” and “Test Facility Management (TFM)” would equally apply to “test sites” and “Test Site Management”.</p>	<p>3. 範囲</p> <p>クラウドサービスには、試験施設又は試験施設が所属する企業の内部で提供されるサービス、又は契約したITサービスプロバイダーによる外部委託サービスがある。契約すると、クラウドサービスプロバイダーから直接サービスを受けることも、ベンダー経由でサービスを受けることもできる。サービスプロバイダーは、サービスの全部又は一部を（下請け）業者に委託する場合もある。この文書はあらゆる種類のサービスに適用される。</p> <p>注: 本ガイダンスにおいては、「クラウドサービスプロバイダー」という用語は、社内IT、社外IT、ホスト型サービスプロバイダー、ベンダー（通常は、サービスを提供する個人又は法人）、サプライヤ（通常は1社でその仕事は要求されたサービスを提供するもの）を含む、あらゆる種類のクラウドサービスのプロバイダーを指す。</p> <p>このドキュメントは、すでに使用されているものも含め、すべてのクラウドベースのソリューションに適用される。この文書における「試験施設」及び「運営管理者」に対する期待は、「試験場所」及び「試験場所管理責任者」にも同様に当てはまる。</p>

英文	和訳
<p>4. Overview of cloud computing</p> <p>4.1. Definition</p> <p>In general terms, cloud computing can be defined as a model that enables on demand network access to a shared pool of configurable computing resources. The US National Institute of Standards and Technology (NIST) (Peter Mell, 2011[6]) defines cloud computing as “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.” According to NIST, cloud computing has five essential characteristics, four deployment models and three service models as described in Figure 1.</p>	<p>4. クラウドコンピューティングの概要</p> <p>4.1. 定義</p> <p>一般的にクラウドコンピューティングは、構成可能なコンピューティングリソースの共有プールへのオンデマンド ネットワーク アクセスを可能にするモデルとして定義できる。米国国立標準技術研究所 (NIST) (Peter Mell, 2011[6]) は、クラウドコンピューティングを「最小限の管理労力やサービスプロバイダーとのやり取りで迅速なプロビジョニング（割り当て）とリリース（提供）が可能な、構成可能なコンピューティングリソース（ネットワーク、サーバー、ストレージ、アプリケーション、サービスなど）の共有プールへのユビキタスで便利に必要な時にネットワークアクセスを可能にするモデル」と定義している。NISTによると、図1に示すように、クラウドコンピューティングには5つの重要な特徴、4つのデプロイメントモデル、及び3つのサービスモデルがある。</p>

Figure 1 Cloud computing characteristics, deployment and service models

図1 クラウドコンピューティングの特徴、デプロイメントモデル、サービスモデル

 <p>CHARACTERISTICS</p>	 <p>DEPLOYMENT MODELS</p>	 <p>SERVICE MODELS</p>
<p>On-demand self-service Network access Resource-pooling Rapid elasticity Measured service</p>	<p>Private cloud Community cloud Public cloud Hybrid cloud</p>	<p>Infrastructure as a Service Platform as a Service Software as a Service</p>
 <p>CHARACTERISTICS</p>	 <p>DEPLOYMENT MODELS</p>	 <p>SERVICE MODELS</p>
<p>オンデマンドセルフサービス ネットワークアクセス リソースプーリング 迅速な弾力性 計測可能サービス</p>	<p>プライベートクラウド コミュニティクラウド パブリッククラウド ハイブリッドクラウド</p>	<p>IaaS PaaS SaaS</p>

英文	和訳
<p>These characteristics, deployment models and service models as defined by NIST are reproduced or paraphrased below. Possible GLP examples are provided in the following paragraphs (see section 4.3 and section 4.4).</p>	<p>NIST によって定義されたこれらの特徴、デプロイメントモデル、及びサービスモデルを以下の項で改めて説明する。また、考えられるGLPの例を提示する（セクション4.3及びセクション 4.4 を参照）。</p>
<p>4.2 Characteristics</p> <p>The essential characteristics of cloud computing are on-demand self-service, broad network access, resource pooling, rapid elasticity (i.e., easily adaptable and flexible) and measured service.</p> <ol style="list-style-type: none"> 1. On-demand self-service: Users are provided with computing resources without any human interaction with the service provider. 2. Network access: Computing resources are accessible over the network, supporting heterogeneous client platforms (e.g. mobile devices and workstations). 3. Resource-pooling: The provider’s computing resources are pooled to serve multiple users under a single or multi-tenant model, with different physical and virtual resources (e.g., storage, processing, memory, and network bandwidth) dynamically assigned and reassigned according to user demand. 	<p>4.2 特徴</p> <p>クラウドコンピューティングの重要な特徴は、オンデマンドのセルフサービス、広範なネットワーク アクセス、リソースプーリング、迅速な弾力性（つまり、容易に適応でき柔軟であること）、及び計測可能なサービスである。</p> <ol style="list-style-type: none"> 1. オンデマンドのセルフサービス: ユーザーには、サービスプロバイダーとの人的対話なしでコンピューティングリソースが提供される。 2. ネットワークアクセス: コンピューティングリソースはネットワーク経由でアクセスでき、異種クライアントプラットフォーム（モバイルデバイスやワークステーションなど）をサポートする。 3. リソース プーリング: プロバイダーのコンピューティングリソースは、シングルテナントモデル又はマルチテナントモデルの下で複数のユーザーにサービスを提供するためにプールされ、さまざまな物理リソース及び仮想リソース（ストレージ、処理、メモリ、ネットワーク帯域幅など）がユーザーの要求に応じて動的に割り当てられ、再割り当てされる。

<p>4. Rapid elasticity (scalability): Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward, commensurately with demand.</p> <p>5. Measured service: Cloud systems optimise resource use by leveraging and metering their capabilities appropriately according to the type of service (e.g., active user accounts). Resource usage can be monitored, measured, controlled and reported, providing transparency for the provider and user (pay-by-use).</p>	<p>4. 迅速な弾力性（拡張性）：機能は弾力的にプロビジョニング及びリリースされ、場合によっては自動的に、需要に応じて拡大または縮小できる。</p> <p>5. 計測可能なサービス：クラウドシステムは、サービスの種類（アクティブなユーザーアカウントなど）に応じてその機能を適切に活用及び測定することで、リソースの使用を最適化することができる。リソースの使用状況を監視、測定、制御及び報告することができ、プロバイダーとユーザー間の透明性が提供される（従量課金制）</p>
---	---

英文	和訳
<p>4.3 Deployment models</p> <p>Cloud computing can be deployed in different models according to the type of use. There are four types of deployment models: private, public, community and hybrid (Figure 2). The main differences between these deployment models relate to the availability of the cloud infrastructure:</p> <p>1. Private cloud: The cloud infrastructure is provisioned for exclusive use by a single organisation comprising multiple users (e.g. business units). It may be owned, managed, and operated by the organisation, a third party, or some combination of them. The cloud infrastructure is generally hosted out of the premises of the organisation but the data location is under the organisation control.</p> <p>In GLP, a private cloud means hosting of computing resources solely for the use of the contracting test facility or the organisation where it belongs to. This occurs within a private internal network or where the infrastructure is dedicated to the contracting test facility with completely isolated access regardless of whether it is provided by an external or internal cloud service provider.</p>	<p>4.3 デプロイメントモデル</p> <p>クラウドコンピューティングは、用途に応じてさまざまなモデルを導入可能である。導入モデルには、プライベート、パブリック、コミュニティ及びハイブリッドの 4 種類がある（図 2）。これらのデプロイメントモデルの主な違いは、クラウドインフラストラクチャの可用性に関連している。</p> <p>1. プライベートクラウド: クラウドインフラストラクチャは、複数のユーザーで構成される単一の組織（ビジネスユニットなど）による排他的使用のためにプロビジョニングされる。組織、サードパーティ、又はそれらの組み合わせによって所有、管理及び運用される場合がある。クラウドインフラストラクチャは通常組織の敷地外でホストされるが、データロケーションは組織の管理下にある。</p> <p>GLPでは、プライベートクラウドとは、契約を結んでいる試験施設又はその試験施設が所属する組織のみが使用するためのコンピューティングリソースのホスティングを意味する。これは、プライベート内部ネットワーク内、又は外部もしくは内部のクラウドサービスプロバイダーによって提供されるかどうかに関係なく、完全に分離されたアクセスを持つ契約試験施設専用のインフラストラクチャで発生する。</p>

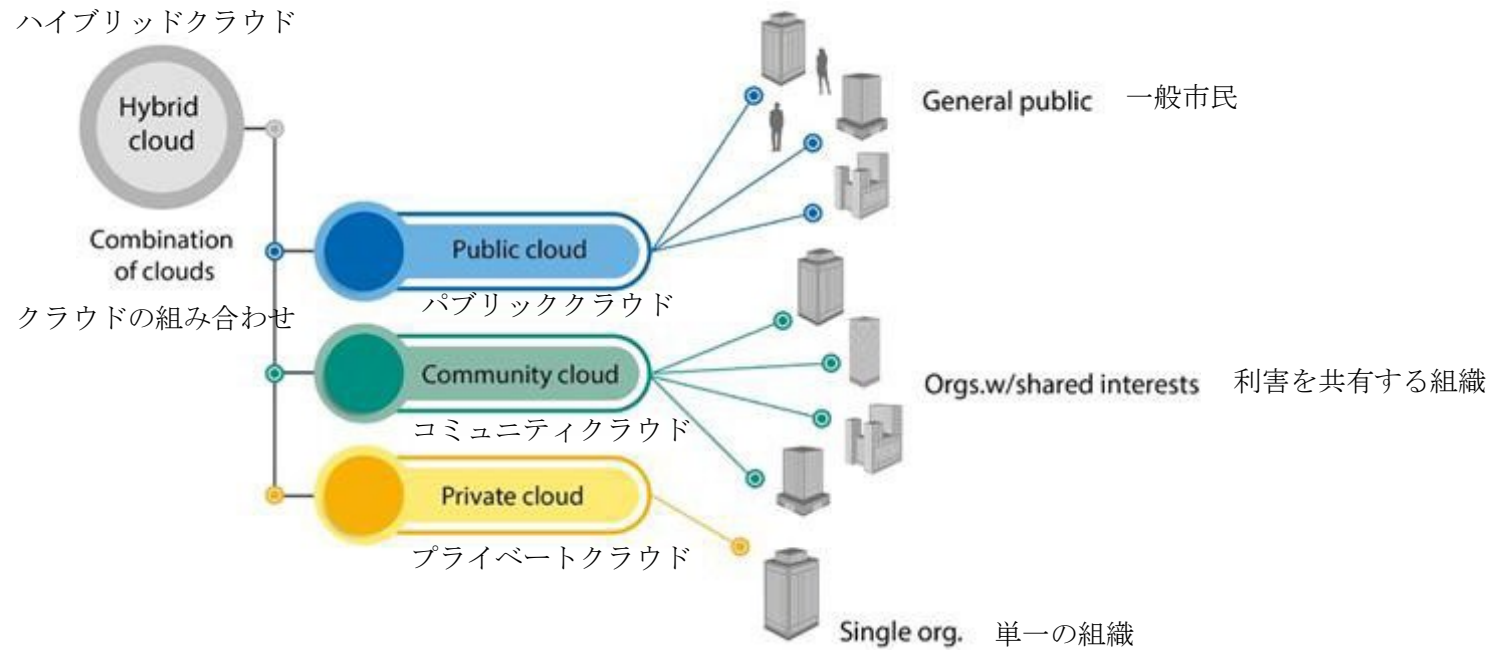
英文	和訳
<p>2. Community cloud: The cloud infrastructure is provisioned for exclusive use by a specific community of users from organisations that have shared requirements (e.g., mission, security requirements, policy, compliance considerations for test facilities). It may be owned, managed, and operated by one or more of the organisations in the community, a third party, or some combination of them. The cloud infrastructure is generally hosted off premises.</p> <p>In GLP, in a community cloud, the cloud infrastructure is shared by several test facilities that have similar interests (e.g., regarding security, compliance). Access is not public but only accessible for a defined group of users with joint requirements. Such a cloud can be operated by one of these institutions or a third party.</p>	<p>2. コミュニティクラウド: クラウドインフラストラクチャは、共通の要件（ミッション、セキュリティ要件、ポリシー、試験施設のコンプライアンスの考慮事項など）を持つ複数の組織の特定のユーザーコミュニティによる排他的使用のためにプロビジョニングされる。これはコミュニティ内の1つ以上の組織、サードパーティ、又はそれらの組み合わせによって所有、管理及び運用される場合がある。クラウドインフラストラクチャは通常、オフプレミスでホストされる。</p> <p>GLPでは、コミュニティクラウドで、同様の利害（セキュリティ、コンプライアンスなど）を持つ複数の試験施設によってクラウドインフラストラクチャが共有される。アクセスは公開されていないが、共通の要件を持つ定義されたユーザーのグループのみがアクセスできる。このようなクラウドは、これらの機関のいずれか又はサードパーティによって運用される。</p>

英文	和訳
<p>3. Public cloud: The cloud infrastructure is provisioned for use by the general public. It may be owned, managed, and operated by a business, academic, or government organisation, or some combination of them. It exists on the premises of the cloud provider. The exact location of the physical infrastructure on which the data is stored, or the applications run, is generally unknown to the users.</p> <p>In GLP, public cloud means hosting of computing resources that can be used by the general public or a large group, such as an entire industry sector; these services are provided by the respective cloud service provider in its facilities/data centres.</p>	<p>3. パブリッククラウド: クラウドインフラストラクチャは、一般の人々が使用できるようにプロビジョニングされている。企業、学術機関、政府機関、あるいはそれらの組み合わせによって所有、管理及び運用されている場合がある。インフラストラクチャはクラウドプロバイダーの敷地内に存在するが、データが保存されている、又はアプリケーションが実行されている物理インフラストラクチャの正確な場所は、通常、ユーザーにはわからない。</p> <p>GLPでは、パブリッククラウドとは、一般大衆又は業界全体などの大規模なグループが使用できるコンピューティングリソースのホスティングを意味する。これらのサービスは、各クラウドサービスプロバイダーの施設/データセンターで提供される。</p>

英文	和訳
<p>4. Hybrid cloud: The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds). As examples of mixed cloud-based solutions, an application is hosted in a part of a public cloud whose accessibility and management are designed as in a private cloud by security measures and access restrictions (“private cloud in public cloud”). Or, the application is hosted in a public cloud, and the generated data are stored and saved in the servers of the test facility (mix of public cloud and traditional IT infrastructure).</p> <p>In GLP, hybrid cloud means a combination of public and private clouds. The test facility uses the public cloud but also has its own private cloud and can create a connection between the two to work as one system.</p>	<p>4. ハイブリッドクラウド: クラウドインフラストラクチャは、2つ以上の異なるクラウドインフラストラクチャ（プライベート、コミュニティ、又はパブリック）で構成されており、それぞれが固有の管理下で存在するが、データとアプリケーションのポータビリティを可能にする標準化又は独自のテクノロジーによって結合されている（例：クラウド間の負荷分散のためのクラウドバースティング）。ハイブリッドクラウドベースのソリューションの例として、アプリケーションは、セキュリティ対策とアクセス制限によってプライベートクラウドと同様にアクセシビリティと管理が設計されたパブリッククラウドの一部でホストされる（「パブリッククラウド内のプライベートクラウド」）。又は、アプリケーションはパブリッククラウドでホストされ、生成されたデータは試験施設（パブリッククラウドと従来のITインフラストラクチャの混合）のサーバーに保存される。</p> <p>GLPでは、ハイブリッドクラウドはパブリッククラウドとプライベートクラウドの組み合わせを意味する。試験施設はパブリッククラウドを使用するが、独自のプライベートクラウドも備えており、2つのクラウド間の接続を作成して1つのシステムとして動作させることができる。</p>

Figure 1 Cloud computing deployment models

図2 クラウドコンピューティングデプロイメントモデル



Source: FSI Insights on policy implementation No. 13, Regulating and supervising the clouds: emerging prudential approaches for insurance companies (Crisanto et al., 2018[7]).

英文	和訳
<p>4.4 Service models</p> <p>Service models refer to the type of computing resource that is offered. There are three main types of service model: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS):</p> <p>1. Infrastructure as a Service (IaaS): The capability provided to the user is to provide processing, storage, networks, and other fundamental computing resources where the user is able to deploy and run arbitrary software, which can include operating systems and applications. The user does not manage or control the underlying cloud infrastructure (e.g. hardware) and has limited to full control over operating systems, storage, deployed applications and networking components (e.g., host firewalls).</p> <p>For GLP test facilities, the IaaS solution offers hosting and maintenance of hardware and network (both physical and virtual components) and the availability of storage and computing capacity and resources.</p>	<p>4.4 サービスモデル</p> <p>サービスモデルは、提供されるコンピューティングリソースのタイプを指す。サービスモデルには、主に3つのタイプがある； サービスとしてのインフラストラクチャ（IaaS）、サービスとしてのプラットフォーム（PaaS）、及びサービスとしてのソフトウェア（SaaS）：</p> <p>1. Infrastructure as a Service (IaaS): ユーザーに提供される機能は、ユーザーがオペレーティングシステムやアプリケーションを含む任意のソフトウェアをデプロイメントして実行できる、処理、ストレージ、ネットワーク及びその他の基本的なコンピューティングリソースを提供することである。ユーザーは、基盤となるクラウドインフラストラクチャ（ハードウェアなど）を管理又は制御せず、オペレーティングシステム、ストレージ、展開されたアプリケーション及びネットワークコンポーネント（ホストファイアウォールなど）の完全な制御に限定される。</p> <p>GLP試験施設の場合、IaaSソリューションは、ハードウェアとネットワーク（物理コンポーネントと仮想コンポーネントの両方）のホスティングとメンテナンス及びストレージとコンピューティングの容量とリソースの可用性を提供する。</p>

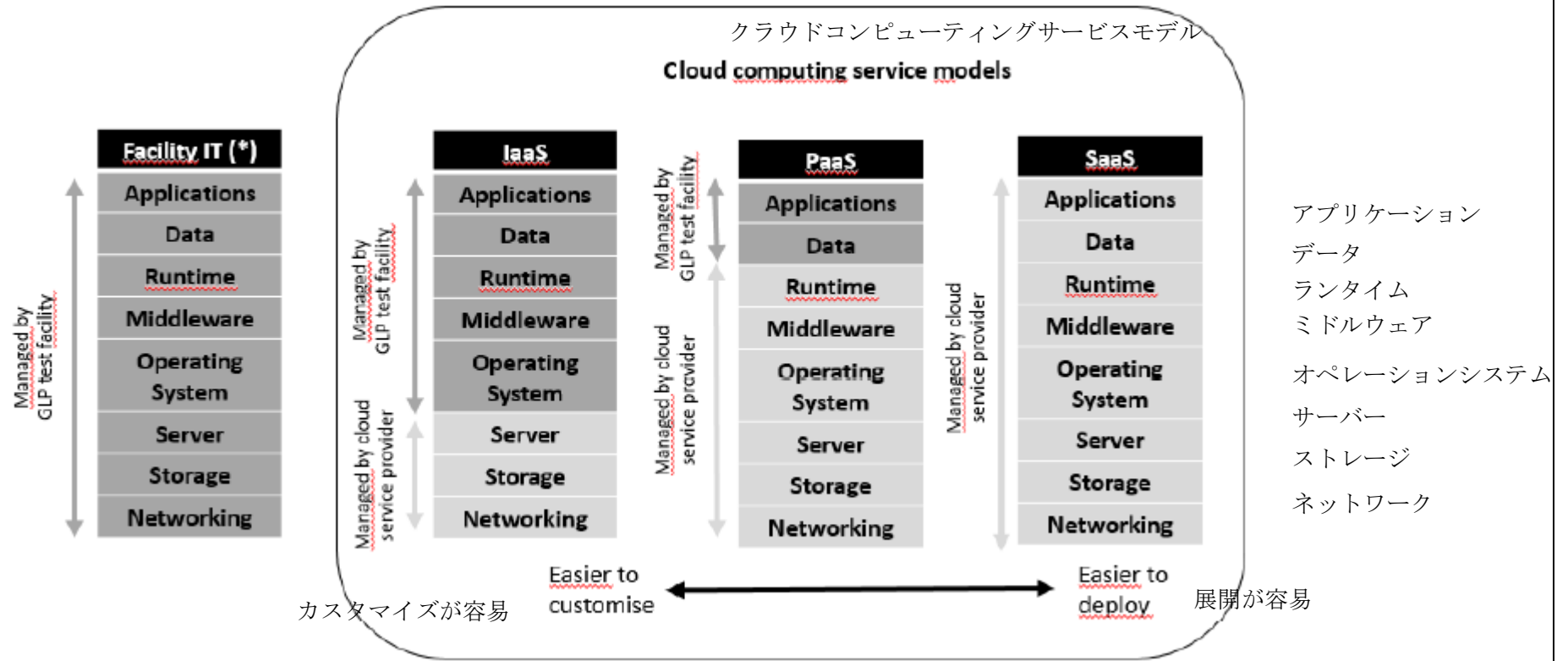
英文	和訳
<p>2. Platform as a Service (PaaS): The capability provided to the user is to deploy onto the cloud infrastructure user-created or acquired applications developed using programming languages, libraries, services, and tools supported by the cloud service provider. Platform as a service is where an external vendor supplies a platform for developing applications on the cloud such as an operating system, a middleware, a database, etc. in addition to the infrastructure. The provision of this service includes managing the infrastructure and basic application software. The user would be responsible for configuration of the application and its fitness for its intended use.</p> <p>In GLP test facilities, hardware and the environment are provided. The platform offers the possibility to manage data and documentation. Operations such as migration, classification, storage are also often included in such services. The GLP test facility remains responsible for the configuration of the systems and the management of software.</p> <p>– Example: The cloud service provider provides an application server and a database to allow the implementation of a Laboratory Information Management System (LIMS).</p>	<p>2. Platform as a Service (PaaS): ユーザーに提供される機能は、クラウドサービスプロバイダーがサポートするプログラミング言語、ライブラリ、サービス、ツールを使用して開発された、ユーザーが作成又は取得したアプリケーションをクラウドインフラストラクチャに展開することである。PaaSとは、インフラストラクチャに加えて、クラウド上でアプリケーションを開発するためのオペレーティングシステム、ミドルウェア、データベースなどのプラットフォームを外部ベンダーが提供するものである。このサービスの提供には、インフラストラクチャと基本的なアプリケーションソフトウェアの管理が含まれる。ユーザーは、アプリケーションの構成とその意図された用途への適合性について責任を負う。</p> <p>GLP試験施設では、ハードウェアと環境が提供される。このプラットフォームは、データとドキュメントの管理を提供する可能性がある。多くの場合、移行、分類、保存などの操作もこのようなサービスに含まれる。GLP 試験施設は引き続きシステムの構成とソフトウェアの管理を担当する。</p> <p>– 例: クラウドサービスプロバイダーは、ラボラトリーデータ管理システム (LIMS) の実装を可能にするアプリケーションサーバーとデータベースを提供する。</p>

英文	和訳
<p>4. Software as a Service (SaaS): The capability provided to the user is to use the provider’s applications running on a cloud infrastructure. The applications are accessible from various client devices through an interface, such as a web browser or a programme interface. The user does not manage or control the underlying cloud infrastructure including applications, network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.</p> <p>In GLP, the SaaS model provides the test facility with applications which generate or analyse data as well as manage documentation and which are developed, installed, maintained and updated by a cloud service provider. The hardware is typically located in a data centre (mostly in public cloud to allow high amount of users). This hosting in a data centre is generally subcontracted by the vendor of the software to a third party. All the security design is ensured by the cloud service provider (usually via other subcontractors). The GLP test facility has to connect via a common or shared platform with specific access rights to use the software. Training is often part of the service provided.</p>	<p>3. Software as a Service (SaaS): ユーザーに提供される機能は、クラウドインフラストラクチャ上で実行されるプロバイダーのアプリケーションを使用することである。アプリケーションは、Web ブラウザーやプログラムインターフェイスを通じて、さまざまなクライアントデバイスからアクセスできる。ユーザーは、限られたユーザー固有のアプリケーション構成設定を除き、アプリケーション、ネットワーク、サーバー、オペレーティングシステム、ストレージ、さらには個々のアプリケーション機能を含む基盤となるクラウドインフラストラクチャを管理又は制御することはない。</p> <p>GLPでは、SaaSモデルは、データの生成や分析、ドキュメントの管理を行うアプリケーションを試験施設に提供し、クラウドサービスプロバイダーによって開発、インストール、保守、更新される。ハードウェアは通常、データセンターに配置される（多くの場合、大量のユーザーを受け入れるためにパブリッククラウドに配置される）。データセンターでのこのホスティングは通常、ソフトウェアのベンダーからサードパーティに外注される。すべてのセキュリティ設計は、クラウドサービスプロバイダー（通常は他の外注業者を通じて）によって保証される。GLP試験施設は、ソフトウェアを使用するために特定のアクセス権を持つ一般の又は共有のプラットフォームを介して接続する必要がある。多くの場合、サプライヤーが実施するトレーニングはユーザーに提供されるサービスの一部である。</p>

英文	和訳
<p>The level of computing intervention of the GLP test facility is limited to internally defining user access to the system. It includes also the configuration of the application to the test facility's intended use, including security in the implementation phase. The use of SaaS consists of a connection with authentication mechanism and the entry of data.</p> <p>– Example: an electronic laboratory notebook system may be hosted in the public cloud allowing the capture of raw data on electronic devices. The data are directly transmitted from the devices via a secured network to be stored in a private (secured) area also hosted in a public cloud.</p> <p>5. Desktop as a Service (DaaS): compared to the SaaS model, this technology supplies also the desktop environment. In this model, all the components of the desktop are virtualized, and only a device is necessary to access the virtual desktop.</p> <p>Figure 3 provides an overview of how the management of the main components of a cloud- based solution is typically shared between the test facility and the cloud service provider depending on the selected cloud computing service models.</p>	<p>GLP試験施設へのコンピュータの介入レベルは、システムに対するユーザーアクセスを内部的に定義することに限定される。これには、実装段階でのセキュリティを含む、試験施設の使用目的に合わせたアプリケーションの構成も含まれる。SaaSの使用は、認証メカニズムとの接続とデータの投入で構成される。</p> <p>– 例: 電子実験ノートシステムをパブリッククラウドでホストし、電子デバイス上で生データを取り込むことができる。データは、安全なネットワークを介してデバイスから直接送信され、パブリッククラウドでホストされているプライベート（安全な）エリアに保存される。</p> <p>4. Desktop as a Service (DaaS): SaaSモデルと比較して、このテクノロジーはデスクトップ環境も提供する。このモデルでは、デスクトップのすべてのコンポーネントが仮想化されており、仮想デスクトップにアクセスするために必要なのはデバイスのみである。</p> <p>図3は、選択したクラウドコンピューティングサービスモデルに応じて、クラウドベースのソリューションの主要コンポーネントの管理が試験施設とクラウドサービスプロバイダーの間で通常どのように共有されるかの概要を示している。</p>

Figure 2 Shared management of the main components of a cloud computing service between the GLP test facility and the cloud service provider

図3 GLP試験施設とクラウドサービスプロバイダー間でのクラウドコンピューティングサービス主要コンポーネントの共有管理



(*) Facility IT: means test facility IT systems without any use of cloud solutions.

(*) 施設IT：クラウドソリューションを一切利用しない試験施設のITシステム。

Legend:

- Managed by GLP test facility GLP試験施設による管理
- Managed by cloud service provider クラウドサービスプロバイダーによる管理

英文	和訳
<p>5. Cloud computing in GLP environment</p> <p>5.1 Responsibilities of the test facility</p> <p>TFM is responsible for GLP compliance within the GLP test facility and the systems that support GLP activities. If IT operations are moved from locally controlled servers to a cloud-based solution, it is essential that appropriate knowledge, awareness and oversight of the systems and practices remain with the test facility and control is exercised. This is regardless of whether this is an internally managed cloud (as part of the test facility or as part of the organisation to which the test facility belongs) or outsourced via an external cloud service provider.</p> <p>Due to the complexity of the offered service, it is also recognized that TFM may delegate contracting and managing such services to specialists or internal specialized departments responsible for general vendor selection, contracting and supervision. Transparency on agreements and obligations of all involved parties is therefore key elements, allowing scalable level on details depending on service provided. Nevertheless, even if the tasks are delegated, TFM is still responsible for the GLP compliance of the systems used in the test facility.</p>	<p>5. GLP環境下でのクラウドコンピューティング</p> <p>5.1 試験施設の責務</p> <p>運営管理者は、GLP試験施設及びGLP活動をサポートするシステム内のGLP遵守に責任を負う。IT運用がローカルで制御されるサーバーからクラウドベースのソリューションに移行される場合、システムに対する適切な知識、認識及び監視を試験施設に課せられ、その制御が実行されることが不可欠である。これは内部管理されたクラウド（試験施設の一部として、又は試験施設が属する組織の一部として）であるか、外部のクラウドサービスプロバイダーを介してアウトソーシングされたものであるかは関係ない。</p> <p>提供されるサービスが複雑であるため、運営管理者はそのようなサービスの契約と管理を、一般的なベンダーの選択、契約、監督を、外部の専門家又は社内の専門部門に委託する場合があることも認識されている。この場合、関係者全員の合意と義務の透明性が重要な要素であり、提供されるサービスに応じて詳細レベルの拡張が可能になる。それにもかかわらず、タスクが委任されている場合でも、運営管理者は試験施設で使用されるシステムのGLP遵守に対する責任を負う。</p>

英文	和訳
<p>The system administrator has access to live and archived data and documents. The circumstances of access and actions taken on the data need to be defined and clarified when data are hosted by a cloud service provider. Administrator rights should not be given to persons with a potential interest in the data and/or documentation. Clear risk mitigation strategies and controlled procedures should be developed and applied to ensure data integrity, quality and availability, independently on where the system administrator is located (test facility or vendor).</p> <p>The study director should ensure that computerised systems (including virtual components that might be hosted locally or in a cloud) used in studies have been validated.</p>	<p>システム管理者は、ライブ及びアーカイブされたデータ及びドキュメントにアクセスできる。データがクラウドサービスプロバイダーによってホストされる場合、アクセスの状況とデータに対して実行されるアクションを定義し、明確にする必要がある。管理者権限は、データやドキュメントに潜在的に利害関係を有する人に与えてはならない。システム管理者の所在地（試験施設又はベンダー）に関係なく、データインテグリティ、品質、可用性を確保するために、明確なリスク軽減戦略と管理された手順を開発及び適用する必要がある。</p> <p>試験責任者は、試験で使用されるコンピュータ化システム（ローカル又はクラウドでホストされる可能性のある仮想コンポーネントを含む）が検証されていることを確認する必要がある。</p>

英文	和訳
<p>The archivist is responsible for the management of archives. If GLP archives are stored in a cloud-based solution, the archivist may need to use the assistance of specialists to look at technical aspects. Nevertheless, the archivist remains responsible and should still ensure that:</p> <ol style="list-style-type: none"> 1. The archiving conditions ensure the integrity of the archived electronic records. 2. Access to the archives is controlled. 3. A system of indexing allows orderly storage and retrieval of records. 4. Migrations of archived electronic records are properly controlled and documented. 5. A process is implemented for periodic readability and data integrity checks. 6. A process is implemented to ensure the readability of data after being migrated from the cloud environment to the test facility (exit strategy). <p>The Quality Assurance (QA) programme should ensure that GLP compliance is preserved. The use of cloud-based solutions in GLP studies should be verified for their GLP compliance by QA as any other computerised systems.</p>	<p>資料保存施設管理責任者はアーカイブの管理に責任を負う。GLPアーカイブがクラウドベースのソリューションに保存されている場合、アーカイビストは技術的な側面を調べるために専門家の支援を利用する必要がある場合がある。そのような場合であっても、資料保存施設管理責任者は引き続き責任を負い、次のことを保証する必要がある：</p> <ol style="list-style-type: none"> 1. アーカイブ条件により、アーカイブされた電子記録の完全性が保証されること。 2. アーカイブへのアクセスは制御されること。 3. インデックス付けシステムにより、記録の秩序ある保存とリトリブが可能であること。 4. アーカイブされた電子記録の移行は適切に管理され、文書化されること。 5. 定期的な見読性とデータインテグリティチェックのためのプロセスが実装されること。 6. クラウド環境から試験施設に移行した後、データの見読性を確保するためのプロセスが実装されること（出口戦略）。 <p>品質保証（QA）プログラムは、GLP遵守が維持されていることを確実にする必要がある。GLP試験におけるクラウドベースソリューションの使用は、他のコンピュータ化システムと同様に、QAによってGLP遵守を検証される必要がある。</p>

英文	和訳
<p>5.2 Requirements</p> <p>GLP requirements for computerised systems and hosted services (or cloud services) are described mainly in OECD Documents No. 1, No. 15 and No. 17. Table 1 provides an overview of GLP requirements as specified in OECD Document No. 1 in relation to the different cloud computing service models.</p> <p>Table 1 GLP requirement management within different cloud service models</p> <p>Legend of the Table:</p> <p>Light Grey: under the full management and intervention of the test facility.</p> <p>Dark Grey: management and interventions shared among the test facility and the cloud service provider and its subcontractors, if any.</p> <p>Black: under the full management of the cloud service provider.</p> <p>Note: it is the ultimate responsibility of the test facility to assess and demonstrate whether the cloud-based services can ensure data quality, data integrity and data availability and do not affect GLP compliance of the test facility.</p> <p>(*) Traditional IT: means test facility IT systems without any use of cloud solutions.</p>	<p>5.2 要求事項</p> <p>コンピュータ化システム及びホスト型サービス（又はクラウドサービス）に関するGLP要求事項は、主にOECD文書No.1、No.15、及び No.17に記載されている。表1は、さまざまなクラウドコンピューティングサービス モデルに関連して、OECD文書No.1に指定されているGLP要件の概要を示している。</p> <p>表1 異なるクラウドサービスモデル内のGLP要求事項マネジメント</p> <p>表の凡例</p> <p>明るい灰色：試験施設の完全な管理と介入の下で実施される。</p> <p>暗い灰色：管理と介入は、試験施設とクラウドサービスプロバイダー及びその下請け業者（存在する場合）の間で共有される。</p> <p>黒：クラウドサービスプロバイダーの完全な管理下にある。</p> <p>注：クラウドベースのサービスがデータの品質、データインテグリティ、及びデータの可用性を確保できるかどうか、また試験施設のGLP適合性に影響を与えないかどうかを評価及び実証することは、試験施設の最終的な責任である。</p> <p>(*)従来の IT: クラウド ソリューションを使用しない試験施設の IT システムを意味する。</p>

Computing resources (コンピューティングリソース)	Traditional IT (*) 従来のIT	GLP Principles requirements (GLP原則要求事項)	Cloud service models		
			IaaS	PaaS	SaaS
Raw Data (including metadata) 生データ (メタデータを含む)		1.2.2.f, 1.4.3, 8.3.5			
Data generation データ発生					
Data classification and accountability データの階層化と責任					
Protection 保護					
User access management ユーザーアクセス管理					
Encryption 暗号化					
Metadata, audit trail generation and management メタデータ、監査証跡の発生と管理					
Migration マイグレーション		1.2.2.f, 1.4.3, 8.3.5			
Physical security measures for raw data 生データに対する物理的セキュリティ確保方法		1.2.2.i			
Applications and software アプリケーションとソフトウェア		1.1.2.b, 1.1.2.q, 1.2.2.g, 4.1			
Application level controls (access, rights) アプリケーションレベルでの制御 (アクセス、権限)					
Physical security measures for hosting of applications アプリケーションのホスティングのための物理的セキュリティ確保方法					
Runtime (databases) ランタイム (データベース)		1.1.2.q			
Middleware (interface between applications) ミドルウェア (アプリケーション間のインターフェース)		1.1.2.q			
Operating systems (Windows, Linux, etc.) OS (ウインドウズ、リナックスなど)		1.1.2.b			

Computing resources (コンピューティングリソース)	Traditional IT (*) 従来のIT	GLP Principles requirements (GLP原則要求事項)	Cloud service models		
			IaaS	PaaS	SaaS
Virtualisation 仮想化		1.1.2.b			
Servers (account, application and data servers) サーバー (アカウント、アプリケーション、データサーバー)		1.1.2.b, 3.1.1			
Storage 保存		1.1.2.b, 1.2.2.i, 3.1.1			
Backup and restore バックアップとリストア		1.1.2.b, 1.2.2.i, 3.1.1			
Data archiving データアーカイブ		1.1.2.b, 1.1.2.l,			
Host infrastructure ホストインフラ		1.1.2.q, 3.4, 9.2.7,			
Physical security measures for hosting of archives アーカイブのホスティングにおける物理的セキュリティ対策		10			
Networking (web browser, web server) ネットワーク (ウェブブラウザ、ウェブサーバ)		1.1.2.b			
VPN, firewall, and network security VPN、ファイアウォール、ネットワークセキュリティ					
Network control ネットワークコントロール					
Disaster Recovery Plan (DRP) 災害復旧計画 (DRP)		1.1.2.b, 3.1.1, 3.4			
Retirement リタイアメント		1.1.2.q, 10.4			
IT personnel IT担当者		1.1.2.b, c, d, 1.4.1			
Computerised systems validation (and periodic review, change control) (コンピュータ化システムバリデーション (CSV) (及び定期レビュー、変更管理)		1.1.2.q, 1.2.2.g			

Computing resources (コンピューティングリソース)	Traditional IT (*) 従来のIT	GLP Principles requirements (GLP原則要求事項)	Cloud service models		
			IaaS	PaaS	SaaS
Quality Assurance (QA) 信頼性保証		1.1.2.f, 2.1.1, 2.1.2			

英文	和訳
<p>All requirements indicated in OECD Document No. 17, section on “supplier” (section 1.6, paragraphs 34 to 40) should be fulfilled by the test facility to manage the cloud service providers.</p> <p>Document No. 17 states that (paragraph 39) cloud or hosted services (e.g. platform, software, data storage, archiving, backup or processes as a service) should be treated like any other supplier service and require written agreements describing the roles and responsibilities of each party.</p> <p>It is the responsibility of TFM to evaluate the relevant service and to estimate risks to data quality, data integrity and data availability.</p> <p>TFM should be aware of potential risks resulting from the uncontrolled use of cloud services and should have the means to be made aware of these risks and its impacts on GLP compliance. Appropriate risk mitigation measures should be in place and documented.</p>	<p>クラウドサービスプロバイダーを管理する試験施設は、OECD 文書 No.17「サプライヤ」の項（1.6、段落34～40）に示されるすべての要件を満たさなければならない。クラウドサービスプロバイダーを管理するために、試験施設が満たす必要がある。</p> <p>OECD文書17では、（段落39で）クラウド又はホスト型サービス（例：サービスとしてのプラットフォーム、ソフトウェア、データストレージ、アーカイブ、バックアップ、又はプロセス）は、他のサプライヤサービスと同様に扱われ、各当事者の役割と責任を説明する書面による合意が必要と述べている。関連するサービスを評価し、データ品質、データインテグリティ、及びデータの可用性に対するリスクを推定するのは運営管理者の責務である。</p> <p>運営管理者は、管理が不十分なクラウドサービスの使用による潜在的なリスクを認識し、これらのリスクとそのGLPコンプライアンスへの影響を認識する手段を備える必要がある。また、適切なリスク軽減策を実施し、文書化する必要がある。</p>
<p>Cloud service providers can interact directly or as a subcontractor from another supplier. TFM should appropriately control all GLP relevant suppliers and subcontractor activities should be transparent to TFM. Written agreements between the test facility and the cloud service provider should mention if parts of the service may be subcontracted (see section on “Service Level Agreement”).</p>	<p>クラウドサービスプロバイダーは、直接やり取りすることも、別のサプライヤの委託業者としてやり取りすることもできる。運営管理者はすべてのGLP関連サプライヤを適切に管理する必要があり、委託業者の活動は運営管理者に対して透明である必要がある。試験施設とクラウドサービスプロバイダーの間の書面による契約には、サービスの一部が下請けに委託される可能性があるかどうかについて言及する必要がある（「サービスレベルアグリーメント」のセクションを参照）。</p>

英文	和訳
<p>5.3 Implementation of cloud-based solution in GLP</p> <p>Where cloud services are used to provide, install, configure, integrate, qualify, maintain, modify or retain a computerised system, the following four key elements will play a crucial role in ensuring whether a GLP test facility can demonstrate compliance to the GLP Principles.</p> <ol style="list-style-type: none"> 1. Detailed risk assessment (with the description of the cloud solution as prerequisite). 2. Thorough cloud service provider assessment, including audits when relevant, prior to use and periodic review. 3. Clearly defined service level agreements directly related to the operational activities and services to be provided. 4. Validation of the computerised systems hosted in cloud-based services. <p>Note: the same requirements are valid for physical and virtual servers.</p>	<p>5.3. GLPにおけるクラウドベースソリューションの実装</p> <p>クラウドサービスを使用してコンピュータ化システムを提供、インストール、構成、統合、認定、保守、変更、又は保持する場合、GLP試験施設がGLP原則へのコンプライアンスを実証できるかどうかを確認する上で、次の4つの要素が重要な役割を果たす。</p> <ol style="list-style-type: none"> 1. 詳細なリスク評価（前提条件としてクラウドソリューションの説明付き）。 2. 使用前及び定期的なレビューに関連する監査を含む、クラウドサービスプロバイダーの徹底的な評価。 3. 提供される運用活動とサービスに直接関連する、明確に定義されたサービスレベルアグリーメント。 4. クラウドベースのサービスでホストされているコンピュータ化システムの検証。 <p>注: 同じ要件が物理サーバーと仮想サーバーに当てはまる。</p>

英文	和訳
<p>5.3.1. Risk assessment and selection of the cloud-based services</p> <p>Risk management should be applied throughout the lifecycle of any computerised system, taking into account data quality, data integrity and data availability.</p> <p>Prior to committing to a cloud-based solution, TFM should identify and describe potential failure modes, assess the associated risks for GLP compliance, including the likelihood and impact, and where applicable, come up with effective mitigating actions. Cloud-based services should be developed, released and managed to ensure data quality, data integrity and data availability without jeopardizing GLP compliance of the test facility.</p> <p>A detailed description of the expectations to the use of the cloud solution and the associated impacts should be available before any choice is made. The steps of the risk assessment include (but are not limited to):</p>	<p>5.3.1 リスク評価とクラウドサービスの選択</p> <p>リスク管理は、データの品質、データインテグリティ、及びデータの可用性を考慮して、コンピュータ化システムのライフサイクル全体にわたって適用される必要がある。</p> <p>クラウドベースのソリューションの適用に取り組む前に、運営管理者は潜在的な障害モードを特定及び記述し、可能性及び影響を含むGLPコンプライアンスに関連するリスクを評価し、該当する場合は効果的な軽減措置を考え出す必要がある。運営管理者は、潜在的な障害モードを特定して説明し、可能性と影響を含む GLP コンプライアンスに関連するリスクを評価し、該当する場合は効果的な緩和措置を考え出す必要があります。クラウドベースのサービスは、試験施設のGLPコンプライアンスを危険にさらすことなく、データ品質、データインテグリティ、及びデータの可用性を確保するために開発、リリース、管理される必要がある。</p> <p>選択を行う前に、クラウドソリューションの使用に対する期待とそれに伴う影響についての詳細な説明を明らかにする必要があります。リスク評価の手順には次が含まれる（ただし、これらに限定されない）。</p>
<p>1. Expected objectives and functionalities including system requirements, user requirements and constraints for the system.</p>	<p>1. システム要件、ユーザー要件、システムの制約など、期待される目的と機能。</p>
<p>2. Infrastructure and applications: the extent to which infrastructure, network/platforms and applications are expected to be provided.</p>	<p>2. インフラストラクチャとアプリケーション: インフラストラクチャ、ネットワーク/プラットフォーム、及びアプリケーションの提供が期待される範囲。</p>

英文	和訳
<p>3. Impact on GLP compliance, especially regarding data migration and storage, resulting from adopting the system provided by the cloud service (non-exhaustive list):</p> <ul style="list-style-type: none"> a. Expected new data process and changes from the current system: in particular, steps for data migration should be carefully identified and described. b. Associated new risks on data quality: risks linked to newly supplied applications to capture, generate or analyse data (reliability, availability of system and data, backup plans for system failure). c. Associated new risk on data integrity and data availability: level of control of remote access to the data, level of protection of the data, secure location for the physical storage of the data (physical infrastructure access, disaster recovery strategy, recovery time objectives and recovery point objectives, location of the data hosting servers, long term integrity of electronically archived data). For SaaS, as the test facility has generally no access to the software itself in case of release event, impacts on data integrity and data availability should be carefully considered by end user when anticipating the business continuity plan, the disaster recovery plan and the exit strategy of the GLP test facility. d. Impacts on systems architecture (both the test facility systems architecture and the systems architecture of the cloud service provider), organisation and operating model. e. Impacts on protection of data ownership. 	<p>3. クラウドサービスによって提供されるシステムの採用によって生じる、特にデータの移行とストレージに関する GLP コンプライアンスへの影響（以下はすべてを網羅しているわけではない）：</p> <ul style="list-style-type: none"> a. 予想される新しいデータプロセスと現在のシステムからの変更：特に、データ移行の手順を慎重に特定し、説明する必要がある。 b. データ品質に関連する新たなリスク：データを取得、生成、又は分析するために新たに提供されたアプリケーションに関連するリスク（信頼性、システムとデータの可用性、システム障害のバックアップ計画）。 c. データインテグリティとデータの可用性に関連する新たなリスク：データへのリモートアクセスの制御レベル、データの保護レベル、データの物理ストレージの安全な場所（物理インフラストラクチャアクセス、災害復旧戦略、目標復旧時点と目標復旧時間、データホスティングサーバーの場所、電子的にアーカイブされたデータの長期的な完全性）。SaaSの場合、通常、リリースイベントの場合、試験施設はソフトウェア自体にアクセスできないため、エンドユーザーは事業継続計画、災害復旧計画、GLP試験施設の出口戦略を予測する際に、データインテグリティとデータの可用性への影響を慎重に考慮する必要がある。 d. システムアーキテクチャ（試験施設のシステムアーキテクチャとクラウドサービスプロバイダーのシステムアーキテクチャの両方）、組織、運用モデルへの影響。 e. データ所有権の保護への影響。

英文	和訳
f. Impacts on competence of the study personnel, study directors, QA personnel and archivist, especially need for training.	f. 試験担当者、試験責任者、QA 担当者、資料保存施設管理責任者の能力への影響、特にトレーニングの必要性。
4. Expected measures to mitigate the identified risks, including (non-exhaustive list): a. Need for adequate controls to maintain or verify data quality, data integrity and data availability and the need for data review. b. Existence of audit trails, where appropriate.	4. 特定されたリスクを軽減するために期待される対策には、以下が含まれる（以下はすべてを網羅しているわけではない）。 a. データ品質、データインテグリティ、データの可用性を維持又は検証するための適切な管理とデータのレビュー。 b. 必要に応じて、監査証跡の存在。
5. Established criteria for selection of the cloud service provider including compliance with specific quality standards and the availability of contingency plans for provider failure such as disaster recovery, security of the cloud service provider etc. (see also section on “cloud service provider assessment”).	5. 特定の品質基準へのコンプライアンスや、災害復旧、クラウドサービスプロバイダーのセキュリティ、プロバイダーの障害に対する緊急時対応計画の可用性などからクラウドサービスプロバイダーの選択基準を確立する。（「クラウドサービスプロバイダーの評価」のセクションも参照すること）。
6. Service migration plan for provider end of service.	6. プロバイダーのサービス終了に伴うサービス移行計画。
7. Archiving (when applicable).	7. アーカイブ（該当する場合）。
When a cloud solution is being selected for use, a clear and complete description and implementation plan should be generated. This should include:	クラウドソリューションの使用を選択する場合は、明確かつ完全な説明と実装計画を作成する必要がある。これには以下を含める必要がある。
1. Cloud service provider(s): name(s) and address(es) of the company (if known, address(es) of the data centres) and contacts, reference to the contract(s).	1. クラウドサービスプロバイダー：会社名、住所（判明している場合は、データセンターの住所）、連絡先、契約書の参照先。
2. Details of any subcontractors of the cloud service provider(s) relevant to GLP compliance: technical role, names and addresses, reference to the contracts.	2. GLP 遵守に関連するクラウドサービスプロバイダーの委託業者の詳細：技術的役割、名前と住所、契約書の参照先。

英文	和訳
3. Overview of the solution selected with detailed description, gaps between expected and provided functionalities, services/products selected, parties involved and delivery location(s).	3. 選択されたソリューションの概要（詳細な説明、期待される機能と提供される機能の間のギャップ、選択されたサービス/製品、関係者、及び提供場所など）。
4. Detailed specifications of activities performed by the cloud service provider (see Table 1), especially sharing of technical tasks, roles and responsibilities between the cloud service provider, its subcontractors and the test facility (see also section on “service level agreement”).	4. クラウドサービスプロバイダーによって実行されるアクティビティの詳細な仕様（表 1 を参照）、特にクラウドサービスプロバイダー、その委託業者及び試験施設の間での技術的なタスク、役割、及び責任の共有（「サービス レベルアグリーメント」のセクションも参照）。
5. Detailed process of validation, including tasks and means provided by the cloud service provider (including possible access when relevant to a test environment where the system can be tested before being put into production).	5. クラウドサービスプロバイダーによって提供されるタスクと手段を含む、検証の詳細なプロセス（実稼働前にシステムをテストできるテスト環境に関連する場合のアクセスの可能性を含む）。
6. Detailed specification ensuring control of access to the data (remote access, cloud service providers’ access to systems and data, cloud service providers’ access to perform changes directly within database where applicable), level of protection of the data, (including IT security activities, e.g., management and review of user accesses, management of passwords, management of firewalls, backup and restore, handling of security incidents, maintenance and security patching of platforms (databases and operating systems), intrusion detection and protection).	6. データへのアクセス制御（リモート アクセス、クラウドサービスプロバイダーによるシステムとデータへのアクセス、クラウドサービスプロバイダーによるデータベース内で直接変更を実行するアクセス（該当する場合））、データ保護レベル（IT セキュリティ活動（例えば、ユーザーアクセスの管理とレビュー、パスワードの管理、ファイアウォールの管理、バックアップとリストア、セキュリティインシデントの処理、プラットフォーム（データベースとオペレーティングシステム）のメンテナンスとセキュリティパッチの適用、侵入の検出と保護）を含む）を確実にする詳細な仕様。
7. Determining the type of service model to implement –IaaS, PaaS or SaaS.	7. 実装するサービスモデルのタイプ（IaaS、PaaS又はSaaS）の決定。

<p>8. Determining the type of deployment model – private, public, community or hybrid.</p>	<p>8. 導入モデルのタイプ（プライベート、パブリック、コミュニティ又はハイブリッド）の決定。</p>
<p>9. SOPs required to govern the routine use, administration and maintenance of the system.</p>	<p>9. システムの日常的な使用、管理及びメンテナンスを統括するために必要なSOP。</p>
<p>10. Training of the test facility personnel if required.</p>	<p>10. 必要に応じて、試験施設担当者のトレーニング</p>
<p>11. Means of control of the solution by the test facility: these controls should be planned to verify that the system is maintained in a validated state to ensure data quality, data integrity and data availability. These controls should be implemented independently from the cloud service provider (internal or external provider), be monitored and the documentation retained. The effort of control should be linked to the functionalities ensured by the cloud-based solution. For example:</p> <p>a. If the cloud-based solution is used for archiving data, periodic controls should be implemented to verify the data integrity and data availability of the archives. The frequency of such controls should be risk-based.</p> <p>b. If the cloud-based solution is a SaaS, data quality, data integrity and data availability can be verified by electronic controls in each run or periodically, check-sums, review of audit trails or of the accesses, or any other solutions. The frequency of such controls should be risk-based. Periodic SaaS application reports which can be provided by the cloud service provider cannot replace independent controls.</p>	<p>11. 試験施設によるソリューションの制御手段: これらの制御は、データの品質、データインテグリティ及びデータの可用性を確保するために、システムが検証済みの状態に維持されていることを検証するために計画する必要がある。これらの制御は、クラウドサービスプロバイダー（内部又は外部プロバイダー）から独立して実装され、監視され、文書が保持される必要がある。制御の取り組みは、クラウドベースのソリューションによって保証される機能に関連付けられる必要がある。例えば:</p> <p>a. データのアーカイブにクラウドベースソリューションを使用する場合、アーカイブのデータインテグリティとデータの可用性を検証するために定期的な制御を実装する必要がある。このような管理の頻度はリスクに基づいて行う必要がある。</p> <p>b. クラウドベースソリューションがSaaSの場合、データ品質、データインテグリティ、及びデータの可用性は、実行ごと又は定期的に電子制御、チェックサム、監査証跡やアクセスのレビュー、又はその他のソリューションによって検証できる。このような管理の頻度はリスクに基づいて行う必要がある。クラウドサービスプロバイダーによって提供される定期的なSaaSアプリケーションレポートは、独立したコントロールに代わるものではない。</p>

英文	和訳
<p>5.3.2. Cloud service provider assessment</p> <p>Note: The management of the cloud service provider plays a vital role to ensure the quality and compliance of the services. The expectations of the test facility from the cloud service provider to ensure a level of service that is fit for purpose for GLP use should be defined in the service level agreement (see section on “service level agreement”).</p>	<p>5.3.2. クラウドプロバイダー評価</p> <p>注: クラウドサービスプロバイダーの管理は、サービスの品質とコンプライアンスを確保するために重要な役割を果たす。クラウドサービスプロバイダーがGLP使用の目的に適したサービスレベルを保証するというクラウドサービスプロバイダーからの試験施設への期待は、サービスレベル契約で定義する必要があります。（「サービスレベルアグリーメント」のセクションを参照）。</p>
<p>The established criteria for the selection of cloud service providers should be documented.</p> <p>The competence and reliability of a cloud service provider are key factors when selecting a product or service provider. A cloud service provider audit may be appropriate and the decision to conduct an audit or not of the cloud service provider should be based upon documented risk assessment. The audit team could also include users, QA personnel, IT experts and/or external experts. Activities of cloud service providers may be subcontracted to other suppliers. In case of any subcontracting, it is the ultimate responsibility of the test facility to assess and demonstrate that the cloud-based services do not affect GLP compliance of the test facility.</p>	<p>クラウドサービスプロバイダーの選択に関して確立された基準を文書化する必要がある。</p> <p>クラウドサービスプロバイダーの能力と信頼性は、製品又はサービスプロバイダーを選択する際の重要な要素である。クラウドサービスプロバイダーの監査が適切な場合があり、クラウドサービスプロバイダーの監査を実施するかどうかの決定は、文書化されたリスク評価に基づいて行われるべきである。監査チームには、ユーザー、QA担当者、IT専門家及び/又は外部専門家が含まれる場合もある。</p> <p>クラウドサービスプロバイダーの活動は、他のサプライヤに委託される場合がある。委託の場合、クラウドサービスが試験施設のGLP適合性に影響を与えないことを評価し実証するのは試験施設の最終的な責任である。</p>

英文	和訳
<p>During cloud service provider assessment, it is essential to verify which (if any) quality system is in place at cloud service provider (including systems of relevant subcontractors).</p> <p>Cloud service provider (and subcontractor) may hold certified quality systems. These may be considered by the test facility, if they support GLP compliance of the test facility.</p> <p>Note: some national regulations (non GLP) may require that the cloud service providers have defined certifications on the level of security they provide prior to ensure the hosting of some specific data (e.g., personal data, medical data, health data). Responsibility of TFM is limited to GLP compliance issues.</p>	<p>クラウドサービスプロバイダーの評価中に、クラウドサービスプロバイダー（関連する委託業者のシステムを含む）にどのような品質システムが導入されているか（存在する場合）を確認することが不可欠である。クラウドサービスプロバイダー（及び委託業者）は、認定された品質システムを保持している場合がある。試験施設のGLPコンプライアンスをサポートする場合、試験施設によって以上の事項が考慮される場合がある。</p> <p>注: 一部の国内規制（非GLP）では、特定のデータ（個人データ、医療データ、健康データなど）のホスティングを保証する前に、クラウドサービスプロバイダーは提供するセキュリティレベルに関する定義済みの認定を取得することが求められる場合がある。運営管理者の責任はGLPコンプライアンス問題に限定される。</p>
<p>Test facility can also choose to outsource the assessment of the cloud service provider to an external expert and the appropriateness of this should be assessed by TFM, with the support of QA.</p>	<p>試験施設は、クラウドサービスプロバイダーの評価を外部の専門家に委託することも選択でき、その適切性は QA のサポートを受けて運営管理者によって評価される必要がある。</p>
<p>Following general items may be addressed during the assessment (non-exhaustive list):</p> <ol style="list-style-type: none"> 1. Quality system of the cloud service provider if any (including subcontractor(s) and standard operating procedure management). 2. Documentation process. 3. Personnel management (including training). 	<p>評価の際に次の一般的な項目を確認可能と思われる（以下はすべてを網羅しているわけではない）。</p> <ol style="list-style-type: none"> 1. クラウドサービスプロバイダーの品質システム（委託業者及び標準的な運用手順管理を含む）。 2. 文書化プロセス。 3. 人事管理（トレーニング含む）。

英文	和訳
<ol style="list-style-type: none"> 4. Confidentiality and security. 5. Control of access to data. 6. Premises and used technology. 7. Qualification of equipment involved in system in scope. 8. Qualification of system in scope (to verify that the required functionalities are successfully tested). 9. Understanding and policy of data integrity. 10. Backup and restore tests. 11. Disaster recovery processes. 12. Exit strategy. 13. Technical assistance resources. 	<ol style="list-style-type: none"> 4. 機密保持とセキュリティ。 5. データへのアクセスの制御 6. 設備と使用されるテクノロジー。 7. 範囲内のシステムに関与する機器の認定。 8. 範囲内のシステムの認定（必要な機能が正常にテストされていることを確認するため）。 9. データインテグリティの理解とポリシー。 10. バックアップとリストアのテスト。 11. 災害復旧プロセス。 12. 出口戦略。 13. 技術支援リソース。
<p>With regards to the cloud-based solution itself and the associated service, the test facility should assess if the provisions of cloud-based services meet the predefined expectations. The cloud service provider needs to have the systems and information readily in place which are commensurate to the activities they perform to support GLP compliance. The cloud service providers should have (considering the service they provide):</p>	<p>クラウドベースのソリューション自体と関連サービスに関して、試験施設はクラウドベースのサービスの規定が事前に定義された期待を満たしているかどうかを評価する必要がある。クラウドサービスプロバイダーは、GLP遵守をサポートするために実行する活動に見合ったシステムと情報をすぐに提示できるよう整備している必要があります。クラウドサービスプロバイダーは、(提供するサービスを考慮して) 以下を備えている必要がある。</p>

英文	和訳
<p>1. Personnel records of all employees directly involved in the services provided to the test facility including:</p> <ul style="list-style-type: none"> a. Records describing the basic education/training and professional experience. b. Training records of continuing education, IT and Quality Management related, appropriate to perform their duties. c. Description of the current responsibilities and roles (e.g. job description, organisational chart). 	<p>1. 試験施設に提供されるサービスに直接関与するすべての従業員の人事記録。以下が含まれる。</p> <ul style="list-style-type: none"> a. 基本的な教育/訓練及び専門的経験を説明する記録。 b. 職務遂行に適切な継続教育、IT、品質管理関連のトレーニング記録。 c. 現在の責任と役割の説明（職務内容、組織図など）。
<p>2. GLP awareness training. This may be a risk mitigation strategy of TFM to ensure key personnel understands the GLP regulations and requirements applicable to the services being provided, in particular data security and storage.</p>	<p>2. GLP意識向上トレーニング。これは、主要担当者が提供されるサービス、特にデータセキュリティとストレージに適用されるGLP規制と要件を確実に理解するための運営管理者のリスク軽減戦略である可能性がある。</p>
<p>3. Specific provisions in relation to cloud services including, for example:</p> <ul style="list-style-type: none"> a. Documentation about the life cycle of the provided system. b. Data integrity understanding of data flows, data processing. c. Back-up and restoring of electronic data and records. d. Archiving of electronic data and records. e. Electronic data ownership and access rights. f. Change and release management. g. Management of the subcontractors, if applicable. 	<p>3. クラウドサービスに関連する具体的な規定には、例えば次のようなものがある。</p> <ul style="list-style-type: none"> a. 提供されたシステムのライフサイクルに関するドキュメント。 b. データフロー、データ処理のデータインテグリティの理解。 c. 電子データと記録のバックアップと復元。 d. 電子データと記録のアーカイブ。 e. 電子データの所有権とアクセス権。 f. 変更及びリリース管理。 g. 該当する場合、委託（外注）業者の管理。

英文	和訳
<p>4. Documentation about all activities performed on behalf of the test facility that ensures the traceability of these activities.</p> <p>5. Provided access to documents as requested for inspections or QA audits.</p> <p>6. Have qualified equipment/hardware in place.</p>	<p>4. 試験施設に代わって実行されるすべての活動に関する文書。これらの活動のトレーサビリティの保証。</p> <p>5. 調査又は QA 監査の要求に応じたドキュメントへのアクセス提供。</p> <p>6. 認定された機器/ハードウェアの設置。</p>
<p>Test facility should verify that the documentation and procedures of the cloud service provider are adequate to ensure a suitable qualification and validation approach for the services provided.</p>	<p>試験施設は、クラウドサービスプロバイダーの文書と手順が、提供されるサービスに対する適切な認定と検証のアプローチを確保するのに適切であることを検証する必要がある。</p>
<p>5.3.3. Service Level Agreement (SLA)</p> <p>Note: Different terms are used to describe document(s) in which operating clauses for cloud service are described: contracts, quality (assurance) agreements, technical specifications, etc. The term Service Level Agreement (SLA) is used in this document.</p>	<p>5.3.3 サービスレベルアグリーメント</p> <p>注: クラウドサービスの運用条項が記載されている文書を説明するには、契約、品質（保証）契約、技術仕様など、さまざまな用語が使用される。この文書では、サービスレベルアグリーメント（SLA）という用語が使用される。</p>
<p>Risk assessment, validation of the system, cloud service provider assessment and service level agreement should clearly indicate that the relevant aspects to data quality, data integrity and data availability are covered when cloud computing is implemented at the test facility. Formal agreements should exist between the GLP test facility and the cloud services providers. These agreements should include clear responsibilities of the cloud services providers' subcontractors, with statements of the responsibilities for the data of any third party(ies) involved in the service.</p>	<p>リスク評価、システムの検証、クラウドサービスプロバイダーの評価、及びサービスレベルアグリーメントは、試験施設でクラウドコンピューティングを実装する際、データ品質、データインテグリティ、及びデータの可用性に関する側面がカバーされていることを明確に示す必要がある。GLP試験施設とクラウドサービスプロバイダーの間には、正式な契約が存在する必要がある。これらの契約には、サービスに関与するサードパーティのデータに対する責任の記述とともに、クラウドサービスプロバイダーの委託業者の明確な責任が含まれている必要がある。</p>

英文	和訳
<p>The SLA is the central document defining all aspects of collaboration between the GLP test facility and the cloud service provider. The SLA should address all relevant aspects including, but not limited to, responsibilities, the use of subcontractors, documentation, performance, archiving, training, communication, reporting lines, audits, validation.</p>	<p>SLAは、GLP試験施設とクラウドサービスプロバイダー間のコラボレーションのあらゆる側面を定義する中心的な文書である。SLAは、責任、委託業者の使用、文書化、パフォーマンス、アーカイブ、トレーニング、コミュニケーション、レポートライン、監査、バリデーションを含むがこれらに限定されない、関連するすべての側面に対処する必要がある。</p>
<p>The use of subcontractors by the cloud service provider should not affect the data quality, data integrity and data availability or overall GLP compliance of the test facility. Appropriate arrangements should be in place for the orderly transfer of the activity, data or services from the contractor to subcontractor. Subcontracting should be authorised in the service level agreement between the test facility and the cloud service provider. Although there is no general requirement for the supplier to be GLP compliant itself, all requirements relevant to ensure data quality, data integrity and data availability should be included in the SLA. SLA should allow the cloud service provider to understand and assume its responsibilities on the data and those entrusted to its subcontractor(s). The test facility should conduct due diligence to ensure the provided service does not compromise data integrity and supports GLP compliance in general.</p>	<p>クラウドサービスプロバイダーによる委託業者の使用は、データ品質、データインテグリティ、データの可用性、又は試験施設全体のGLP適合性に影響を与えてはならない。請負業者から委託業者への活動、データ、又はサービスの秩序ある委託のために、適切な取り決めが整備されている必要がある。委託業者は、試験施設とクラウドサービスプロバイダー間のサービスレベルアグリーメントで許可される必要がある。サプライヤ自体のGLPコンプライアンスに対して一般的な要件はないが、データ品質、データインテグリティ、及びデータの可用性を確保するために関連するすべての要件がSLAに含まれている必要がある。SLAにより、クラウドサービスプロバイダーは、データ及び業者に委託されたデータに対する責任を理解し、引き受けることができるようにする必要がある。試験施設は、提供されるサービスがデータインテグリティを侵害せず、一般的にGLPコンプライアンスをサポートしていることを確認するために評価する必要がある。</p>

英文	和訳
<p><i>Roles and responsibilities</i></p> <p>Roles and responsibilities of test facility and cloud service provider should be clearly described.</p> <p>TFM has the overall responsibility for GLP compliance of the life cycle of their computerised systems and for IT supporting services, even if cloud service providers provide these services.</p> <p>The cloud service provider is responsible for the delivery of cloud-based services that enables the test facility to fulfil all applicable GLP requirements, as specified in the SLA.</p> <p>If activities from the cloud service provider are subcontracted to other suppliers, this should be addressed. A list of subcontractors, subcontracted activities and associated responsibilities should be present in the SLA.</p> <p>It is highly recommended that draft SLAs are reviewed by QA in order to ensure all aspects of GLP compliance are met, however, final responsibility for SLA approval remains at TFM.</p> <p>Modalities of periodic review of existing SLAs should be defined in the SLA.</p> <p>The possibility of cloud service provider audits should be defined in the SLA and scheduled in the QA programme of the test facility.</p> <p>Documentation such as SOPs, personnel records, reports, change control documentation of both partners should reflect respective information from the SLA. Each party should maintain the specific documentation required by the SLA.</p>	<p><i>役割と責任</i></p> <p>試験施設とクラウドサービスプロバイダーの役割と責任を明確に説明する必要がある。</p> <p>運営管理者 は、クラウドサービスプロバイダーがサービスを提供している場合でも、コンピュータ化システムのライフサイクルにおけるGLPコンプライアンスと ITサポートサービスに対する全体的な責任を負う。</p> <p>クラウドサービスプロバイダーは、SLAで指定されているとおり、試験施設が該当するすべてのGLP要件を満たすことができるクラウドベースサービスの提供に責任を負う。</p> <p>クラウドサービスプロバイダーからの活動が他のサプライヤに下請けされている場合は、これに対処する必要がある。委託業者、委託活動、及び関連する責任のリストが SLA に記載されている必要がある。</p> <p>GLP 遵守のすべての側面が満たされていることを確認するために、QAによって SLA 草案をレビューすることを強く推奨する。ただし、SLA承認の最終責任は運営管理者にある。</p> <p>既存のSLAの定期的なレビューの方法をSLAで定義する必要がある。クラウドサービスプロバイダーの監査の可能性はSLAで定義され、試験施設のQAプログラムでスケジュール化される必要がある。</p> <p>両パートナーのSOP、人事記録、報告書、変更管理文書などの文書には、SLAからのそれぞれの情報が反映されている必要がある。各当事者は、SLAで要求される特定の文書を維持する必要がある。</p>

<p><i>System life cycle</i></p> <p>The SLA should describe the duties of the cloud service provider (and any subcontractor(s)) and the test facility during the life cycle of the supported systems. This may include installation, configuration, integration, validation, maintenance (e.g. via remote access), modification, retention or retirement of the system. As a minimum, following points should be covered:</p> <ol style="list-style-type: none"> 1. Data storage. 2. Security. 3. Change control (including application/software updates) and configuration management. A period of time should be discussed with the cloud service provider and defined in the SLA to allow the test facility to conduct testing before implementing changes on the cloud services. The SLA should also state that details about the modifications of the new version and documentation about validation, when applicable, should be provided to the test facility. Access when relevant to a test environment where the new version of the system can be tested before being put into production should be available. 4. Incident management. 5. Business continuity (including back-up and recovery, especially back-up intervals, details on possible locations of mirroring, expected documented confirmations about back-up and mirroring, time for recovery, etc). 6. Qualified infrastructure. 7. Data management. 8. Data integrity maintained throughout record retention period. 	<p>システムのライフサイクル</p> <p>SLAには、サポートされるシステムのライフサイクル中のクラウドサービスプロバイダー（及び下請け業者）と試験施設の義務を記述する必要がある。これには、システムのインストール、構成、統合、検証、メンテナンス（リモートアクセスなどによる）、変更、保持、又はリタイアメントが含まれる場合がある。少なくとも次の点をカバーする必要がある。</p> <ol style="list-style-type: none"> 1. データストレージ 2. セキュリティ 3. 変更管理（アプリケーション/ソフトウェアの更新を含む）と構成管理。クラウドサービスに変更を実装する前に試験施設がテストを実施できるよう、クラウドサービスプロバイダーと一定期間を話し合っ てSLAで定義する必要がある。SLAには、新しいバージョンの変更に関する詳細と、該当する場合には検証に関する文書を試験施設に提供する必要があることも明記する必要がある。システムの新しいバージョンを運用環境に導入する前にテストできるテスト環境に関連する場合は、アクセスが利用可能である必要があります。 4. インシデント管理 5. ビジネス継続性（バックアップとリカバリ、特にバックアップ間隔、ミラーリングの可能な場所の詳細、バックアップとミラーリングに関する予想される文書化された確認、リカバリの時間など） 6. 認定されたインフラストラクチャ 7. データ管理 8. 記録保持期間全体にわたるデータインテグリティの維持
--	--

<p>9. Periodic evaluation by the test facility.</p>	<p>9. 試験施設による定期的な評価</p>
<p><i>Security and Access Control</i></p> <p>Appropriate technical and organisational measures should ensure the logical and physical security and availability of both the data and systems. Maintenance of the systems and incident management should be addressed in the SLA.</p> <p>The SLA should also cover the management of access privileges, including the periodic review of accesses, and these should be restricted to authorised personnel regardless of how the system is accessed.</p> <p>It should be clearly stated that data should not be accessed, migrated (manually, not by storage controller), changed, modified or deleted by the cloud service provider or its subcontractor without prior formal written authorisation by TFM.</p> <p>Procedures on how to prevent cyber-attacks, including, but not limited to, access to electronic data during attacks, and how to restore data and ensure integrity of raw data once it is available again, should be defined.</p>	<p><i>セキュリティとアクセス制御</i></p> <p>適切な技術的及び組織的対策により、データとシステムの両方の論理的及び物理的セキュリティと可用性が確保される必要がある。システムの保守とインシデント管理はSLAで扱う必要がある。</p> <p>SLAは、アクセスの定期的なレビューを含むアクセス権限の管理もカバーする必要があり、これらはシステムへのアクセス方法に関係なく、権限のある担当者に制限される必要がある。</p> <p>運営管理者による事前の正式な書面による許可がない限り、クラウドサービスプロバイダー又はその委託業者によるデータへのアクセス、移行(ストレージ コントローラーではなく手動)、変更、修正、削除を行ってはいけないことを明確に記載する必要がある。</p> <p>攻撃されているデータへのアクセスを含むがこれに限定されないサイバー攻撃を防ぐ方法、及びデータを復元し、再び利用可能になった後に生データインテグリティを確保する方法に関する手順を定義する必要がある。</p>
<p><i>Documentation of the cloud service provider on the systems</i></p> <p>The SLA should define which records are to be retained and archived. The physical and/or logical location of archiving and the retention period should also be defined. The test facility should define documents and records of the cloud service provider that ensure the required traceability of the provided system and verify the availability of such documentation. All defined documents should be accessible by the test facility and GLP compliance monitoring authority inspectors.</p>	<p><i>システムに関するクラウドサービスプロバイダーの文書化</i></p> <p>SLA では、どのレコードを保持及びアーカイブするかを定義する必要がある。アーカイブの物理的及び／又は論理的な場所と保存期間も定義する必要がある。試験施設は、提供されたシステムに必要なトレーサビリティを確保し、そのような文書の可用性を検証するクラウドサービスプロバイダーの文書と記録を定義する必要がある。定義されたすべての文書は、試験施設及びGLP適合性規制当局の調査官がアクセスできる必要がある。</p>

英文	和訳
<p><i>Communication</i></p> <p>The communication lines between the test facility and the cloud service provider should be described in the SLA. The means of communication such as physical or virtual meetings, phone, email, hot line should be defined. There should be an agreement as to which information is to be shared (incident management, change control, access to the data by the vendor etc.). Both parties should cooperate to ensure the compliant and valid operation of the system and to maintain the qualified and validated state of the system.</p>	<p>コミュニケーション</p> <p>試験施設とクラウドサービスプロバイダー間の通信回線はSLAに記載する必要がある。物理的又は仮想的な会議、電話、電子メール、ホットラインなどのコミュニケーション手段を定義する必要がある。また、どの情報（インシデント管理、変更管理、ベンダーによるデータへのアクセスなど）を共有するかについて合意する必要がある。両当事者は、システムのコンプライアンス及び有効な運用を保証し、システムの適格でバリデートされた状態を維持するために協力する必要がある。</p>
<p><i>Exit strategy</i></p> <p>The SLA should clearly describe the test facility’s right to obtain all data and meta-data (including audit trails) in a readable and convertible format, in case the contract with the cloud service provider is terminated (see also OECD document No. 22 chapter 6).</p>	<p>出口戦略</p> <p>SLA には、クラウドサービスプロバイダーとの契約が終了した場合に備えて、すべてのデータ及びメタデータ（監査証跡を含む）を読み取り可能かつ変換可能な形式で取得する試験施設の権利を明確に記載する必要がある（OECD 文書 No. 22 第 6 章も参照）。</p>
<p><i>Final destruction of data</i></p> <p>The SLA should define the process of destruction of data after termination of the contract. The SLA should state that the cloud service provider shall effectively and irreversibly remove and destroy all the data belonging to the test facility after recovery. The cloud service provider should upon test facility’s request provide documentation for certification of such removal and destruction.</p>	<p>データの最終的な破棄</p> <p>SLAでは、契約終了後のデータ破棄のプロセスを定義する必要がある。SLAには、ユーザーのリトリブ後にクラウドサービスプロバイダーが、試験施設に属するすべてのデータを効果的かつ不可逆的に削除及び破壊することを明記する必要がある。クラウドサービスプロバイダーは、試験施設の要求に応じて、そのような排除と破壊の証明のための文書を提供する必要がある。</p>

英文	和訳
<p>5.3.4. Validation of the computerised systems in the cloud-based service</p> <p>As a requirement of the use of computerised systems in GLP, the test facility should use validated systems only, regardless of whether they are SaaS or hosted on IaaS/PaaS.</p> <p>All requirements concerning the computerised system validation should be met. Decisions on the extent of validation activities and data integrity controls, performed under the responsibility of TFM, should be based on a justified and documented risk assessment on the computerised system.</p> <p>The test facility should ensure that all computerised systems are properly validated. The test facility should clearly define the user requirement specifications (even if they may originate from the cloud service provider validation documentation).</p> <p>The test facility should understand what needs to be validated (the application as fit for its intended use within the process), who is responsible to ensure all requirements for computerised system validation are met.</p> <p>If part of the validation documentation is supplied by the cloud service provider, it should be assessed by the test facility for its relevance in the validation process. In case validation documentation from the cloud service provider is used, this should be readably available at the test facility.</p>	<p>5.3.4 クラウドベースのサービスにおけるコンピュータ化システムのバリデーション</p> <p>GLPにおけるコンピュータ化システムの使用要件として、試験施設は、SaaSであるか IaaS/PaaS でホストされているかに関係なく、検証されたシステムのみを使用する必要がある。コンピュータ化システムの検証に関するすべての要件が満たされる必要がある。運営管理者 の責任の下で実行される検証活動とデータ整合性管理の範囲に関する決定は、コンピュータ化システムに関する正当かつ文書化されたリスク評価に基づいて行われるべきである。試験施設は、すべてのコンピュータ化システムが適切に検証されていることを確認する必要がある。試験施設は、ユーザー要求仕様を明確に定義する必要がある（たとえそれがクラウドサービスプロバイダーの検証ドキュメントに由来する場合でも）。試験施設は、何を検証する必要があるか（プロセス内での使用目的に適したアプリケーション）を理解する必要がある、コンピュータ化システム検証のすべての要件が満たされていることを確認する責任がある。</p> <p>バリデーション文書の一部がクラウドサービスプロバイダーによって提供される場合、バリデーションプロセスにおける関連性について試験施設によって評価される必要がある。クラウドサービスプロバイダーからのバリデーション文書が使用される場合、これは試験施設で読み取れるようにする必要がある。</p>

<p>For example, in the case of a SaaS:</p> <ol style="list-style-type: none"> 1. The cloud service provider can provide evidence that the successful installation and management of the application, such as application functional testing, automated testing, unit testing, application programming interface (API) testing, have been performed; even though this may have happened independently of the test facility involvement. The cloud service provider can qualify the hosting infrastructures. SOP for the lifecycle of the application are generally issued by the cloud service provider. TFM should assess the work of the cloud service provider to confirm it has been performed properly for the system in use in the test facility and to detect what is missing. TFM should document and approve this assessment. 2. The test facility should conduct any additional testing that needs to be completed, especially testing in the test facility environment, and the controls needed for the ongoing compliant use of the system (including training of the users, issuance of SOP for the use of the application in a GLP environment). 	<p>例えば、SaaSの場合、</p> <ol style="list-style-type: none"> 1. クラウドサービスプロバイダーは、アプリケーションの機能テスト、自動テスト、単体テスト、アプリケーションプログラミングインターフェース (API) テストなど、アプリケーションのインストールと管理が正常に実行されたことを示す証拠を提供できる。たとえこれが試験施設の関与とは無関係に起こったとしても。クラウドサービスプロバイダーは、ホスティングインフラストラクチャを認定できる。アプリケーションのライフサイクルに関するSOPは通常、クラウドサービスプロバイダーによって発行される。運営管理者は、クラウドサービスプロバイダーの作業を評価して、試験施設で使用されているシステムに対して作業が適切に実行されていることを確認し、何が欠けているかを検出する必要がある。運営管理者はこの評価を文書化して承認する必要がある。 2. 試験施設は、完了する必要がある追加のテスト、特に試験施設環境でのテスト、及びシステムの継続的な準拠使用に必要な制御 (ユーザーのトレーニング、GLP環境でのアプリケーション使用のためのSOPの発行を含む) を実施する必要がある。
<p>As for all computerised systems, the test facility should also make proper arrangements and have procedures in place in case the agreement with the cloud service provider ends or the system is retired, to ensure all data and metadata (including all audit trails) are archived or migrated throughout the duration of the required retention period. Provisions for exit strategy to ensure the data recovery should be tested where possible during the validation of the system.</p>	<p>すべてのコンピュータ化システムに関して、試験施設は、クラウドサービスプロバイダーとの契約が終了するか、システムが廃止された場合に備えて、すべてのデータとメタデータ (すべての監査証跡を含む) が必要な保存期間全体にわたってアーカイブ又は移行されることを確実にするために、適切な手配をし、手順を整備する必要がある。システムの検証中に可能な限り、データの回復を保証する出口戦略規程はテストされるべきである。</p>

英文	和訳
<p>6. Expectations of the GLP compliance monitoring authorities when inspecting cloud – based solutions</p> <p>GLP systems should be validated and operated in a way which ensures the outcome and integrity of GLP data regardless of whether they are installed locally or provided as a cloud service.</p>	<p>6. クラウドベースのソリューションを調査する際のGLP適合性規制当局への期待</p> <p>GLPシステムは、ローカルにインストールされているかクラウドサービスとして提供されているかに関係なく、GLPデータの結果と整合性を保証する方法で検証及び運用される必要がある。</p>
<p>6.1 Implementation of the cloud solution</p> <p>The following documentation should be available to allow verification of the cloud services by GLP inspectors:</p> <ol style="list-style-type: none"> 1. Records of the implemented systems, including the rationale for the selection of the systems, the risk assessment on data quality and integrity and the description of the implemented systems. 2. Documentation on the validation process: <ol style="list-style-type: none"> a. The documentation of the qualification activities performed by the cloud service provider should be available at the test facility. b. The evidence that the qualification activities by the cloud service provides have been assessed as complete and adequate should be provided during the inspection either by the test facility itself, or with help from the cloud service provider where the test facility relies partially on qualification documentation provided by the supplier. c. The documentation of additional qualification/validation activities based on a documented risk assessment that is performed by the test facility should also be available. 	<p>6.1 クラウドソリューションの実装</p> <p>GLP 調査官によるクラウドサービスの検証を可能にするために、次のドキュメントが利用可能である必要がある。</p> <ol style="list-style-type: none"> 1. システム選択の理論的根拠、データの品質と完全性に関するリスク評価、実装されたシステムの説明を含む、実装されたシステムの記録。 2. 検証プロセスに関するドキュメント: <ol style="list-style-type: none"> a. クラウドサービスプロバイダーが実行した適格性評価活動の文書は、試験施設で入手できる必要がある。 b. クラウドサービスが提供する適格性評価活動が完全かつ適切であると評価されたという証拠は、試験施設自体によって、又は試験施設がサプライヤから提供された認定文書に部分的に依存している場合にはクラウドサービスプロバイダーの支援を受けて調査中に提供される必要がある。 c. 試験施設によって実行される文書化されたリスク評価に基づく追加の認定/検証活動の文書も入手可能である必要がある。

英文	和訳
<p>3. The rationale for the choice of the cloud service provider (see also section on “cloud service provider assessment”), even if internal, should be available and include documented assessment/audit of the cloud service providers quality system and qualification and validation processes. Any shortcomings identified should be mitigated by the test facility.</p> <p>4. The service level agreement between the test facility and the cloud service provider, with clear descriptions of the shared activities and responsibilities on the system.</p>	<p>3. クラウドサービスプロバイダーの選択の根拠（「クラウドサービスプロバイダーの評価」のセクションも参照）は、プロバイダー内部のものであっても利用可能であり、クラウドサービスプロバイダーの品質システムと認定及び検証プロセスの文書化された評価/監査が含まれている必要がある。特定された欠点のすべては、試験施設によって軽減されるべきです。</p> <p>4. システム上で共有される活動と責任が明確に説明されている試験施設とクラウドサービスプロバイダーの間のサービスレベルアグリーメント</p>

英文	和訳
<p>6.2 Life cycle of the cloud service application</p> <p>Evidence of the measures implemented by the test facility to ensure continuous validity of the cloud-based solution should be available (by the test facility itself or enforced through the SLA with the cloud service provider). This includes provisions to ensure (list non exhaustive):</p> <ol style="list-style-type: none"> 1. Availability, maintenance, updates, business continuity, disaster recovery plan and migration plan of the system. 2. Data integrity throughout the life cycle. 3. Data quality throughout the life cycle. 4. Data availability. 5. An independent plan of controls implemented and conducted by the test facility to ensure that the cloud-based system stays in a validated state through its life cycle. 6. Documentation about remote access and authentication. 7. The exit strategy, when the contract is ended, should clearly describe how the test facility will obtain all data and meta-data (including audit trails) in a readable and convertible format, in case the contract with the cloud service provider is terminated. <p>In addition to the documentation, demonstration of how a system works can be requested by inspectors to verify its compliance. The test facility should have available details of the functional tests of the system for the inspectors.</p>	<p>6.2 クラウドサービスアプリケーションのライフサイクル</p> <p>クラウドベースのソリューションの継続的な有効性を確保するために試験施設が実施した対策の証拠が入手可能である必要がある（試験施設自体によって、又はクラウドサービスプロバイダーとの SLA を通じて施行される）。これには、以下を保証するための規定が含まれる（これだけに限らない）。</p> <ol style="list-style-type: none"> 1. システムの可用性、メンテナンス、アップデート、事業継続性、災害復旧計画、及び移行計画。 2. ライフサイクル全体にわたるデータインテグリティ。 3. ライフサイクル全体にわたるデータ品質。 4. データの可用性。 5. クラウドベースのシステムがライフサイクルを通じて検証済みの状態に維持されることを保証するために、試験施設によって実装及び実施される独立した制御計画。 6. リモートアクセスと認証に関するドキュメント。 7. 契約終了時の出口戦略（リスクを最小限に抑える方法）では、クラウドサービスプロバイダーとの契約が終了した場合に、試験施設がすべてのデータとメタデータ（監査証跡を含む）を読み取り可能かつ変換可能な形式で取得する方法を明確に説明する必要がある。 <p>調査官は、文書化に加えて、システムがどのように動作するかのデモンストレーションを要求して、そのコンプライアンスを検証することができる。試験施設は、調査官が利用できるシステムの機能テストの詳細を備えている必要がある。</p>

英文	和訳
<p>6.3. Electronic archives in cloud solution</p> <p>Cloud service providers may act as a contract archive by providing services or components to retain and archive GLP relevant data and records.</p> <p>GLP compliance monitoring authorities have different approaches concerning contract archives. Some include them in their monitoring programmes as GLP archive providers; others consider them during the inspection of a test facility. Electronic archives should comply with the applicable GLP Principles (including OECD Document No. 15) and TFM must ultimately ensure that this occurs. Cloud service providers may also be inspected for the GLP compliance by the monitoring authorities.</p> <p>Inspection of the location of servers used for archiving (e.g. buildings, rooms and cabinets) to verify the physical security of the hosting facilities is not always possible, especially if the location is unknown. However, it is noted that some GLP compliance monitoring authorities require details on location of a cloud archive for physical verification, which excludes the use of servers with unknown location for the hosting of electronic archives.</p>	<p>6.3 クラウドソリューションでの電子アーカイブ</p> <p>クラウドサービスプロバイダーは、GLP関連のデータと記録を保持及びアーカイブするためのサービス又はコンポーネントを提供することで、契約アーカイブとして機能する場合がある。</p> <p>GLP適合性調査当局は、契約アーカイブに関してさまざまなアプローチをとっている。一部のGLP適合性規制当局は、GLPアーカイブプロバイダーとして調査プログラムにそれらを含めている。試験施設の調査中にそれらを検討するGLP適合性規制当局もある。電子アーカイブは、適用される GLP 原則（OECD 文書 No. 15 を含む）に準拠する必要があり、運営管理者は最終的にこれが確実に行われるようにする必要がある。クラウドサービスプロバイダーは、規制当局によるGLP適合性の調査を受ける場合もある。</p> <p>ホスティング施設の物理的なセキュリティを検証するために、アーカイブに使用されるサーバーの場所（建物、部屋、キャビネットなど）を調査することは、特に場所が不明な場合には常に可能であるとは限らない。ただし、一部のGLP適合性規制当局は、物理的な検証のためにクラウドアーカイブの場所に関する詳細を要求していること、すなわち電子アーカイブのホスティングに場所が不明なサーバーの使用の除外を求めることに留意すること。</p>

英文	和訳
<p>The test facility should be able to provide documented evidence of GLP compliance for the archive such as the service level agreement and assessment/audit of both the cloud service provider and of the system.</p> <p>Information on the computerised systems and cloud service providers that support logical and technical integrity should be available. This would include proves of full control by archivist, access control, inventory for indexed orderly storage, record retrievability, evidence of record integrity and traceability from raw data to final report.</p> <p>The relevance of all measures to ensure logical, technical and physical integrity should be documented in a risk-based rationale.</p> <p>Measures such as a risk-based back up policy are important. Documented evidence of relevant and efficient back-up and mirroring measures and restoration protocols and a control over those processes by the test facility should be available</p>	<p>試験施設は、クラウドサービスプロバイダーとシステムの両方のサービスレベルアグリーメントや評価/監査など、アーカイブの GLP遵守の文書化された証拠を提供できる必要がある。</p> <p>論理的及び技術的完全性をサポートするコンピュータ化システム及びクラウドサービスプロバイダーに関する情報が入手可能である必要がある。これには、資料保存施設管理責任者による完全な管理の証明、アクセス制御、インデックス付きの整然とした保管場所の目録、記録のリトリート、記録の完全性の証拠、及び生データから最終報告書までのトレーサビリティが含まれる。</p> <p>論理的、技術的、物理的な完全性を確保するためのすべての対策の関連性は、リスクベースの根拠として文書化される必要がある。</p> <p>リスクベースのバックアップポリシーなどの対策が重要である。関連する効率的なバックアップ、ミラーリングの手段、復元プロトコル、及び試験施設によるそれらのプロセスの制御に関する文書化された証拠が利用可能である必要がある。</p>

英文	和訳
<p>7. Conclusion</p> <p>Cloud service providers can offer various solutions that allow acquisition of data for the safety of humans, animals and environment. Implementation of cloud-based solution should not jeopardize the compliance of the GLP activities so that data quality, integrity and availability are assured.</p> <p>When conducting an inspection with cloud-based services involved in the test facility processes, GLP inspectors expect TFM to be able to demonstrate that GLP compliance is still ensured with the implemented cloud service and that TFM has adequate means to control it.</p>	<p>7. 結論</p> <p>クラウドサービスプロバイダーは、人、動物、環境の安全のためのデータを取得できるさまざまなソリューションを提供できる。クラウドベースソリューションの実装が、データの品質、完全性、可用性が保証されるGLP 活動のコンプライアンスを脅かしてはならない。</p> <p>試験施設のプロセスに関与するクラウドベースのサービスの調査を実施する場合、GLP 調査官は、実装されたクラウドサービスでGLP遵守が引き続き確保されていること、及び運営管理者がそれを制御する適切な手段を備えていることを運営管理者が実証できることを期待する。</p>

英文	和訳
8. Glossary	8. 用語集
Back-up (see document No. 17).	<p>バックアップ（ドキュメントNo.17参照）</p> <p>【注釈】 システム障害又は災害発生後の、データファイル又はソフトウェアの復旧、処理の再開、又は代替コンピュータ装置の使用のために行われる準備（例えば別媒体への保存あるいは施設外にバックアップを保存すること）。</p>
Change control (see document No. 17).	<p>変更管理（ドキュメントNo.17参照）</p> <p>【注釈】 コンピュータ化システムの変更に伴いバリデーションプロセスが必要かどうか判定するための、システム運用及び変更についての継続的な評価と文書化。</p>
Computerised system (see document No. 17).	<p>コンピュータ化システム（ドキュメントNo.17参照）</p> <p>【注釈】 「コンピュータ化システムとは、コンピュータシステムと一体化し、訓練を受けた者によって実行される機能（プロセス又は操作）である。その機能はコンピュータシステムによってコントロールされる。コントロールを行うコンピュータシステムはハードウェアとソフトウェアで構成される。コントロールされる機能はコントロールされる装置と担当者によって実行される運用手順で構成される。」 PIC/S PI 11-3規制対象GxP環境におけるコンピュータ化システムのための適正実施基準より引用</p>

英文	和訳
<p>Data (see document No. 17 or 22).</p>	<p>データ（ドキュメントNo.17参照）</p> <p>【注釈】データ（生データ）は物理的実体、プロセス又は事象の測定可能な特徴又は説明的特徴として定義することができる。GLP原則では生データについて、試験における主要な観察及び活動の結果であり、当該試験の再現及び報告書評価のために必要な、自動装置インターフェースを通じてコンピュータに直接入力されるデータを始めとする、全ての試験室記録及び文書として定義している。</p> <p>派生データは生データに依存し、生データから再構築することができる（例えば、生データに依存してスプレッドシートによって計算された最終濃度、LIMSによって要約された結果表など）。</p> <p>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。</p> <p>データは、異なる形式（例：アナログ、デジタル）や構造、レイアウト（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。</p>

英文	和訳
<p>Database : a database is information that is set up for easy access, management and updating. Computer database is an organised collection of data stored, maintained and accessed electronically. Small databases can be stored on a file system, while large databases are hosted on computer clusters or cloud storage.</p>	<p>データベース : データベースは、簡単にアクセス、管理、更新できるように設定された情報である。コンピュータデータベースは、電子的に保存、維持、アクセスされるデータの組織化されたコレクションである。小規模なデータベースはファイル システムに保存できるが、大規模なデータベースはコンピュータクラスター又はクラウドストレージでホストされる。</p>
<p>Data centre: a data centre is a physical facility which is used to house electronic applications and data. A data centre's design is based on a network of computing and storage resources that enable the delivery of shared applications and data. The key components of a data centre's design include routers, switches, firewalls, storage systems, servers and application-delivery controllers.</p>	<p>データセンター : データセンターは、電子アプリケーションとデータを収容するために使用される物理施設である。データセンターの設計は、共有アプリケーションとデータの配信を可能にするコンピューティングリソースとストレージ リソースのネットワークに基づいている。データセンター設計の主要コンポーネントには、ルーター、スイッチ、ファイアウォール、ストレージ システム、サーバー、アプリケーション配信コントローラーが含まれる。</p>
<p>Data protection: data protection is the process of safeguarding data from corruption, compromise or loss and providing the capability to restore the data to a functional state when something happens to render the data inaccessible or unusable.</p>	<p>データ保護 : データ保護は、データを破損、侵害、損失から保護し、何かが起こってデータにアクセスできなくなったり使用できなくなったりしたときに、データを機能的な状態に復元する機能を提供するプロセスである。</p>
<p>Encryption: data encryption converts data from a readable, plaintext format into an unreadable, encoded format. Users and processes can only read and process encrypted data after it is decrypted. The decryption key is secret to be protected against unauthorized access.</p>	<p>暗号化 : データ暗号化は、データを読み取り可能なプレーンテキスト形式から読み取り不可能なエンコードされた形式に変換することである。ユーザーとプロセスは、暗号化されたデータを復号化した後にのみ読み取り、処理できる。復号化キーは、不正アクセスから保護されるために秘密にされる。</p>

英文	和訳
<p>Hardware: hardware refers to the computer's tangible components or delivery systems that store and run the written instructions provided by the software.</p>	<p>ハードウェア：ハードウェアとは、ソフトウェアによって提供される書面による指示を保存及び実行する、コンピュータの有形コンポーネント又は配信システムを指す。</p>
<p>Qualification (see document No. 17).</p>	<p>適格性評価（ドキュメントNo.17参照）</p> <p>【注釈】 ソフトウェアを含む設備が正確に稼働し、その目的に適合していることを証明する活動。</p>
<p>Qualified/verified infrastructure: IT infrastructure qualification is the process of demonstrating that IT components are developed to be fit for their intended use, meet specified requirements and that the system's fitness state is maintained throughout each point in the system's life cycle. Life cycle (see document No. 17 for computerised system life cycle and document No. 22 for data life cycle).</p>	<p>インフラストラクチャ適格性評価／保護：IT インフラストラクチャの適格性評価とは、IT コンポーネントが意図された用途に適合するように開発され、指定された要件を満たしていること、及びシステムのライフサイクルの各時点を通じてシステムの適合状態が維持されていることを実証するプロセス。</p>
<p>Life cycle (see document No. 17 for computerised system life cycle and document No. 22 for data life cycle).</p>	<p>ライフサイクル（コンピュータ化システムのライフサイクルについてはドキュメントNo.17を、データのライフサイクルについてはドキュメントNo.22を参照）</p> <p>【注釈】コンピュータ化システムの開発に対するアプローチで、ユーザーの要求事項の特定から始まり、設計、統合、適格性評価、ユーザーバリデーション、コントロール及び保守管理と続き、システムが廃止される時点で終了する。</p>

英文	和訳
<p>Network: a computer network is a set of computers sharing resources located on or provided by network nodes. The computers use common communication protocols over digital interconnections to communicate with each other.</p>	<p>ネットワーク：コンピュータ ネットワークは、ネットワークノード上にある、又はネットワーク ノードによって提供されるリソースを共有する一連のコンピュータである。コンピュータは、デジタル相互接続を介して共通の通信プロトコルを使用して相互に通信する。</p>
<p>Operating system (see document No. 17).</p>	<p>オペレーティングシステム（ドキュメントNo.17参照）</p> <p>【注釈】 コンピュータの動作をコントロールする、プログラム又はプログラム、ルーチン及びサブルーチンの集合。オペレーティングシステムはリソース配分、スケジューリング、入出力制御、データ管理などのサービスを提供できる。</p>
<p>Recovery time objectives: recovery time objective is the goal an organisation sets for the maximum length of time it should take to restore normal operations following an outage or data loss.</p>	<p>目標復旧時間：目標復旧時間は、停止又はデータ損失の後に通常の運用を復元するために組織が設定する最大時間の目標。</p>
<p>Recovery point objectives: recovery point objectives is the goal for the maximum amount of data the organisation can tolerate losing. This parameter is measured in time: from the moment a failure occurs to the last valid data backup.</p>	<p>目標復旧時点：目標復旧時点は、組織が損失を許容できるデータの最大量の目標。このパラメータは、障害が発生した瞬間から最後の有効なデータ バックアップまでの時間で測定される。</p>
<p>Risk (see document No. 17).</p>	<p>リスク（ドキュメントNo.17参照）</p> <p>【注釈】 危害の発生する確率とそれが顕在化した場合の重大性の組合せ。</p>
<p>Risk assessment (see document No. 17).</p>	<p>リスクアセスメント（ドキュメントNo.17参照）</p> <p>【注釈】 リスクアセスメントは、ハザードの特定と、そのハザードへの曝露に伴うリスクの分析及び評価で構成される。リスクアセスメントに続いてリスクコントロールが行われる。</p>

英文	和訳
<p>Risk mitigation (see document No. 17).</p>	<p>リスク軽減（ドキュメントNo.17参照）</p> <p>【注釈】 危害の発生する確率とそれが顕在化した場合の重大性を低下させるためにとられる活動。</p>
<p>Security (see document No. 17).</p>	<p>セキュリティ（ドキュメントNo.17参照）</p> <p>【注釈】 コンピュータのハードウェア及びソフトウェアを、偶発的又は悪意のあるアクセス、使用、変更、破壊又は開示から保護すること。セキュリティは担当者、データ、通信、並びにコンピュータ装置の物理的及び論理的保護にも関係する。</p>
<p>Server: a server is a software or hardware device that accepts and responds to requests made over a network. The device that makes the request, and receives a response from the server, is called the client.</p>	<p>サーバー：サーバーは、ネットワーク経由で行われたリクエストを受け入れて応答するソフトウェア又はハードウェア デバイスである。リクエストを発行し、サーバーからの応答を受信するデバイスはクライアントと呼ばれる。</p>
<p>Software (see document No. 17).</p>	<p>ソフトウェア（ドキュメントNo.17参照）</p> <p>【注釈】 プロセス制御、データ収集、データ操作、データ報告及び／又はアーカイブを目的として、試験施設のために取得され、試験施設の要件に合わせて開発又は適合させたプログラム。</p>
<p>Validation (see document No. 17).</p>	<p>バリデーション（ドキュメントNo.17参照）</p> <p>【注釈】 プロセスが期待される結果に至ることを証明する活動。コンピュータ化システムのバリデーションにおいては、その目的への適合を確保し、証明することが必要になる。</p>

英文	和訳
<p>Virtual Private Network (VPN): a virtual private network, or VPN, is an encrypted connection over the internet from a device to a network or between two networks. The encrypted connection ensures that sensitive data is safely transmitted. It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely.</p>	<p>仮想プライベート ネットワーク (VPN) : 仮想プライベート ネットワーク (VPN) は、デバイスからネットワークへ、又は 2 つのネットワーク間の、インターネットを介した暗号化された接続である。暗号化された接続により、機密データが安全に送信される。これにより、許可されていない人によるトラフィックの盗聴が防止され、ユーザーはリモートで作業を行うことができる。</p>

一般社団法人日本QA研究会 GLP部会 第3分科会

2024年4月 作成

GLP 原則及び適合性モニタリングに関するOECD シリーズNo. 17 Supplement 1

GLP原則のコンピュータ化システムに対する適用

英文・和訳 対比表

原著（英語）はOECDから以下のタイトルで公開されている。

OECD SERIES ON PRINCIPLES OF GOOD LABORATORY PRACTICE AND COMPLIANCE MONITORING

Advisory Document on GLP & Cloud Computing

Supplement 1 to Document Number 17 on Application of GLP Principles to computerised Systems

[https://one.oecd.org/document/ENV/CBC/MONO\(2023\)27/en/pdf](https://one.oecd.org/document/ENV/CBC/MONO(2023)27/en/pdf)（こちらのアドレスをブラウザのアドレス欄に張り付けて利用ください）

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

本資料は一般社団法人日本QA研究会の成果物です。

私的使用又は引用等を除き、無断複製、無断転載することを禁じます。