OECD SERIES ON PRINCIPLES OF GOOD LABORATORY PRACTICE AND COMPLIANCE MONITORING

Number 25

OECD Position Paper on Good Laboratory Practice and IT Security

GLP　原則及び適合性モニタリングに関する OECD　シリーズ

No. 25

GLPとITセキュリティに関する OECD の見解

英文・和訳対比表

日本 QA 研究会 GLP　部会 第 3 分科会

英文	和訳
About the OECD The Organisation for Economic Co-operation and Development (OECD) is an intergovernmental organisation in which representatives of 38 countries in North and South America, Europe and the Asia and Pacific region, as well as the European Union, meet to coordinate and harmonise policies, discuss issues of mutual concern, and work together to respond to international problems. Most of the OECD's work is carried out by more than 200 specialised committees and working groups composed of member country delegates. Observers from several Partner countries and from interested international organisations attend many of the OECD's workshops and other meetings. Committees and working groups are served by the OECD Secretariat, located in Paris, France, which is organised into directorates and divisions. The Environment, Health and Safety Division publishes free-of-charge documents in twelve different series: Testing and Assessment; Good Laboratory Practice and Compliance Monitoring; Pesticides; Biocides; Risk Management; Harmonisation of Regulatory Oversight in Biotechnology; Safety of Novel Foods and Feeds; Chemical Accidents; Pollutant Release and Transfer Registers; Emission Scenario Documents; Safety of Manufactured Nanomaterials; and Adverse Outcome Pathways. More information about the Environment, Health and Safety Programme and EHS publications is available on the OECD's World Wide Web site (https://www.oecd.org/en/topics/chemical-safety-and-biosafety.html).	OECDについて 経済協力開発機構（OECD）は、南北アメリカ、ヨーロッパ、アジア太平洋地域および欧州連合（EU）の38か国の代表者が、政策の調整と調和、相互の関心事に関する議論、国際問題への共同対応を目的として集まる政府間組織である。OECDの活動のほとんどは、加盟国の代表者で構成される200以上の専門委員会や作業部会によって実施されている。OECDのワークショップやその他の会議の多くには、パートナー諸国や関心のある国際機関からのオブザーバーが参加している。委員会や作業部会は、フランスのパリにあるOECD事務局によって運営されており、事務局は局と部に分かれている。環境・衛生・安全局は、12種類の異なるシリーズで無償の文書を発行している。そのシリーズとは、試験および評価、優良試験所基準および適合性モニタリング、農薬、殺生物剤、リスク管理、バイオテクノロジーにおける規制当局による監査の調和、新規食品および飼料の安全性、化学物質による事故、化学物質排出・移動量届出（PRTR）制度、排出シナリオ文書、製造ナノ材料の安全性、有害性発現経路である。環境（E）・健康（H）・安全（S）プログラムおよびEHSに関する刊行物に関する詳細は、OECDのウェブサイト（https://www.oecd.org/en/topics/chemical-safety-and-biosafety.html）を参照。

英文	和訳
Foreword This position paper was developed by the OECD Working Party on Good Laboratory Practice (GLP) via a drafting group led by Denmark (Medical Products) and consisting of Austria, Belgium, Canada, France (Medical Products), Germany and Switzerland. The document draws upon a publication developed on cyber security and Good Clinical Practice (GCP) at the level of the European Union. The document was reviewed and endorsement by the Working Party on Good Laboratory Practice. This document is published under the responsibility of the Chemicals and Biotechnology Committee which agreed to its declassification.	序文 本ポジションペーパーは、デンマーク（医薬品／医療機器）が主導し、オーストリア、ベルギー、カナダ、フランス（医薬品／医療機器）、ドイツ、スイスで構成される起草グループを通じて、OECDの優良試験所基準（GLP）作業部会が作成したものである。本文書は、欧州連合（EU）レベルでサイバーセキュリティと医薬品の臨床試験実施に関する基準（GCP）に関して作成された文書を参考にしている。本文書は、GLP作業部会により検討および承認された。この文書は、機密解除に同意した化学品・バイオ技術委員会の責任において発行されている。
Table of contents	目次
About the OECD 3	OECDについて 3
Foreword 4	序文 4
Considerations regarding IT security and GLP test facilities 6	ITセキュリティとGLP試験施設に関する考察 6
1. Introduction 6	1. はじめに 6
2. Scope 6	2. 範囲 6
3. Ongoing security measures and GLP responsibilities 6	3. 継続的なセキュリティ対策とGLPの責任 6
4. Physical security 7	4. 物理的セキュリティ 7
5. Firewalls 7	5. ファイアウォール 7
6. Vulnerability management 7	6. 脆弱性管理 7
7. Platform Management 8	7. プラットフォーム管理 8
8. Bidirectional devices (e.g. USB) 8	8. 双方向デバイス（USBなど） 8
9. Anti-virus software 8	9. アンチウィルスソフトウェア 8

英文		和訳	
10. Penetration testing	8	10. ペネトレーションテスト	8
11. Intrusion detection and prevention	8	11. 侵入検知と防止	8
12. Internal activity monitoring	9	12. 内部活動モニタリング	9
13. Security incident management	9	13. セキュリティインシデント管理	9
14. Authentication method	9	14. 認証方法	9
15. Remote authentication	9	15. リモート認証	9
16. Password policies	9	16. パスワードポリシー	9
17. Password confidentiality	10	17. パスワードの機密性	10
18. Inactivity logout	10	18. 非アクティブ時のログアウト	10
19. Remote connection	10	19. リモート接続	10
20. Protection against unauthorised back-end changes	10	20. バックエンドの不正変更からの保護	10
21. Backup	10	21. バックアップ	10
22. Standard Operating Procedures (SOP)	11	22. 標準操作手順書（SOP）	11

1. Introduction GLP data are more and more generated and retained in electronic format. Measures of IT security aim to protect electronic GLP data and applications against the specific hazards encountered in the computerized environment. Threats and attacks on systems containing GLP data and corresponding measures to ensure security of such systems are constantly evolving, especially for systems and services being provided over or interfacing the internet. Handling of IT security may be outsourced by test facilities to external service providers. However, the responsibility remains with the test facility. The recommendation	1. はじめに GLPデータはますます電子形式で作成・保存されるようになってきている。ITセキュリティ対策は、電子形式のGLPデータおよびアプリケーションを、コンピュータ化された環境で遭遇する特定の危険から保護することを目的としている。GLPデータを含むシステムに対する脅威や攻撃、およびそのようなシステムのセキュリティを確保するための対応策は、特にインターネット上で提供されるシステムやサービスにおいて、常に進化している。ITセキュリティの対応は、試験施設が外部のサービスプロバイダーに委託することができる。ただし、責任は試験

英文	和訳
and advice of vendors of operating systems and platforms should be carefully considered and applied where appropriate.	施設にある。オペレーティングシステム（OS）およびプラットフォームのベンダーによる推奨事項および助言は、慎重に検討し、必要に応じて適用すべきである。
2. Scope This position paper concerns electronic GLP data and linked computerised systems hosted in servers and subject to computerised corruptions. The concepts in this document for “test facilities”, “Test facility management” and “study directors”, would equally apply to “test sites”, “test site management” and “principal investigators”, where delegated study phases are conducted as part of a multisite study (these terms are defined in the GLP Principles).	2. 適用範囲 本ポジションペーパーは、電子形式のGLPデータのものであり、ホスティングされたサーバーまたは連結されたコンピュータ化システムの電子的な改ざんに関するものである。この文書における「試験施設」、「運営管理者」、「試験責任者」の概念は、委任された試験段階が複数場所試験の一部として実施される「試験場所」、「試験場所管理責任者」、「試験主任者」にも同様に適用される（これらの用語はGLP原則で定義されている）。
3. Ongoing security measures and GLP responsibilities Test facility management should maintain a security system that prevents unauthorised access and ensures availability to GLP data. Procedures and measures to ensure IT security should be based on the risk and consequence of system malfunctions or internal or external deliberate or undeliberate actions that might adversely affect the integrity of GLP data.	3. 継続的なセキュリティ対策とGLP上の責務 運営管理者は、不正アクセスを防止し、GLPデータへのアクセスを確保するセキュリティシステムを維持すべきである。ITセキュリティを確保するための手順と対策は、GLPデータのインテグリティに悪影響を及ぼす可能性のあるシステム不具合や内部もしくは外部の故意または過失による行為のリスクと結果に基づいて策定すべきである。
4. Physical security Servers, computers, infrastructure and media hosting GLP data and computerised systems relevant to GLP should be physically protected against unauthorised access, damage and loss. The extent of security measures depends on the criticality of the data. Test Facility management should ensure an adequate level of security for data	4. 物理的セキュリティ GLPデータをホスティングするサーバー、コンピュータ、インフラ、メディアとGLPに関連するコンピュータ化システムは、不正アクセス、損傷、紛失から物理的に保護されなければならない。セキュリティ対策の程度はデータの重要度によって異なる。 運営管理者は、データセンターだけでなく、サーバー、コンピュー

英文	和訳
centres as well as for local hardware such as servers, computers, tablets, phones, hard disks and USB drives. At data centres hosting GLP data and applications, physical access should be limited to the necessary minimum. A two-factor authentication can be used. Data centres should be constructed to minimise the risk and impact of natural disasters, there should be pest control and effective measures against fire (e.g. cooling, fire detection and fire suppression), flooding and any other cause that could alter data. There are generally emergency generators and uninterruptible power supplies (UPS) together with redundant internet protocol providers. In case the data centre is of type `co-location´, the servers should be locked up and physically protected (e.g. in cages) to prevent access from other users (`co-location´ means date centres where the hosted hardware belongs to several organisations that have access to the server rooms). Preferably, data are replicated at an appropriate frequency from a primary data centre to a secondary failover site at an appropriate physical distance to minimise the risk that the same fire or natural disaster destroys both data centres. A disaster recovery plan should be in place and tested.	タ、タブレット、電話、ハードディスク、USBドライブなどのローカルハードウェアに対しても、適切なレベルのセキュリティを確保すべきである。 GLPデータおよびアプリケーションをホスティングするデータセンターでは、物理的なアクセスは必要最低限に制限されるべきである。2要素認証を使用することができる。データセンターは自然災害のリスクと影響を最小限に抑えるように構築されるべきであり、ペストコントロールや、火災（冷却、火災検知、消火など）、洪水、その他データに影響を与える可能性のある要因に対する効果的な対策が講じられるべきである。一般的に、非常用発電機や無停電電源装置（UPS）に加え、予備のインターネットプロトコルプロバイダーの冗長性が確保されている。データセンターが「コロケーション」タイプの場合は、他のユーザーからのアクセスを防ぐために、サーバーを施錠し、物理的に保護（例：ケージ内）する必要がある（「コロケーション」とは、サーバー室にアクセスできる複数の組織が所有するハードウェアを収容するデータセンターを意味する）。 理想的には、同じ火災や自然災害によって両方のデータセンターが破壊されるリスクを最小限に抑えるため、プライマリデータセンターから適切な物理的距離にあるセカンダリフェールオーバーサイトに適切な頻度でデータを複製する。災害復旧計画を策定し、テストしておく必要がある。

英文	和訳
5. Firewalls In order to provide a barrier between a trusted internal network and an untrusted external network and to control incoming and outgoing network traffic (from certain IP addresses, destinations, protocols, applications, or ports etc.), effective firewalls are implemented. Firewall rules should be defined as strict as practically feasible, only allowing necessary and permissible traffic. As firewall rules tend to be changed or become insufficient over time (e.g. as software vendors and IT technicians need certain ports to be opened due to installation or maintenance of applications, or as cyber threats evolve), they are periodically reviewed. This review should ensure that actual firewall rules continue to be set as tight as possible.	5. ファイアウォール 信頼できる内部ネットワークと信頼できない外部ネットワークの間に障壁を設け、特定のIPアドレス、デスティネーション、プロトコル、アプリケーション、ポートなどからのネットワークトラフィックの送受信を制御するために、効果的なファイアウォールが実装されている。ファイアウォールのルールは、必要かつ許可されたトラフィックのみを可能とするよう、現実的に可能な限り厳格に定義されるべきである。 ファイアウォールのルールは、時間の経過とともに変更されたり、不十分になったりしがちである（例えば、ソフトウェアベンダーやIT技術者がアプリケーションのインストールやメンテナンスのために特定のポートを開く必要がある場合や、サイバー攻撃が進化する場合など）。そのため、定期的にレビューを行う。このレビューでは、実際のファイアウォールルールが可能な限り厳しく設定され続けていることを確認すべきである。
6. Vulnerability management Critical vulnerabilities in operating systems and platforms can be exploited to give unauthorised individuals privileged access to systems, and to modify or delete data and make data inaccessible to legitimate users. Such exploits are seen in operating systems for servers, computers, tablets, mobile phones and routers as in platforms for databases etc. While these operating systems and platforms are under support, the vendors frequently release security patches to close these vulnerabilities. Consequently, relevant critical security patches for platforms and	6. 脆弱性管理 OSやプラットフォームの重大な脆弱性は、不正な個人に特権的なアクセス権限を与え、データの変更や削除、または正規ユーザーによるデータへのアクセスを不可能にするために悪用される可能性がある。このような悪用は、サーバー、コンピュータ、タブレット、携帯電話、ルーター用のOSや、データベースなどのプラットフォームで発生している。これらのOSやプラットフォームがサポートされている間、ベンダーはこれらの脆弱性を修正するためのセキュリティパッチを頻繁に

英文	和訳
operating systems have to be applied in a timely manner (immediately is recommended). Systems which are not security patched in a timely manner constitute a major risk for loss of data integrity. Where relevant, such systems have to be isolated from computer networks and the internet.	リリースする。したがって、プラットフォームやOSに関連する重要なセキュリティパッチは、適時に適用しなければならない（即時適用が推奨される）。 セキュリティパッチを適時に適用していないシステムは、データインテグリティを損なう大きなリスクとなる。該当する場合は、そのようなシステムをコンピュータネットワークやインターネットから隔離しなければならない。
7. Platform Management Operating systems and platforms for critical applications and components should be updated in a timely manner, in order to prevent their use in an unsupported state. Unsupported platforms and operating systems, for which no security patches are available, are exposed to a higher risk of vulnerability. Validation of applications on new operating systems and platforms and of the migration of data should be planned ahead and completed in due time. Unsupported platforms and operating systems should be isolated from computer networks and the internet.	7. プラットフォーム管理 重要なアプリケーションおよびコンポーネントのOSおよびプラットフォームは、サポートされていない状態で使用されることを防ぐため、適時に更新されるべきである。 セキュリティパッチが利用できないサポートされていないプラットフォームおよびOSは、脆弱性のリスクが高くなる。新しいOSおよびプラットフォーム上のアプリケーションとデータの移行のバリデーションは、事前に計画し、適時に完了すべきである。 サポートされていないプラットフォームおよびOSは、コンピュータネットワークおよびインターネットから隔離すべきである。
8. Bidirectional devices (e.g. USB) Bidirectional devices (e.g. USB) or other portable media or devices may have been used outside the test facility and could possibly compromise the system. Therefore, they should be strictly controlled as they may intentionally or unintentionally introduce malware and impact data integrity and availability.	8. 双方向デバイス（USBなど） 双方向デバイス（USBなど）やその他のポータブルメディアやデバイスは、試験施設外で使用された可能性があり、システムに悪影響を及ぼす可能性がある。したがって、意図的または非意図的にマルウェアを導入し、データのインテグリティと可用性に影響を及ぼす可能性があるため、厳格に管理する必要がある。

英文	和訳
9. Anti-virus software Anti-virus software should be installed and activated on systems used in GLP, as appropriate. The anti-virus software should be continuously updated with the most recent virus definitions in order to identify, quarantine, and remove known computer viruses. This process should be monitored.	9. アンチウィルスソフトウェア GLPで使用されるシステムには、必要に応じてアンチウィルスソフトウェアをインストールし、起動しておくべきである。既知のコンピュータウイルスを特定し、隔離し、除去するために、アンチウィルスソフトウェアは最新のウイルス定義で継続的に更新すべきである。このプロセスは監視すべきである。
10. Penetration testing For systems facing the internet, penetration testing have to be conducted at regular intervals in order to evaluate the adequacy of security measures taken and to identify vulnerabilities in system security, including the potential for unauthorised parties to gain access to and control the system and its data. Vulnerabilities identified, especially those related to a potential loss of data integrity, should be addressed and mitigated in a timely manner.	10. ペネトレーションテスト インターネットに接続されたシステムでは、セキュリティ対策の妥当性を評価し、システムセキュリティの脆弱性を特定するために、定期的にペネトレーションテストを実施する必要がある。これには、不正な第三者がシステムおよびそのデータにアクセスし、制御する可能性も含まれる。特に、データインテグリティが損なわれる可能性に関連する脆弱性は、適時に特定し、対処および緩和されるべきである。。
11. Intrusion detection and prevention An effective intrusion detection and prevention system has to be implemented on systems facing the internet in order to monitor the network for intrusion attempts from external parties and for the design and maintenance of effective preventive measures. Threats via wireless connections have to be considered risk-based and may require a similar approach.	11. 侵入検知と防止 外部からの侵入の試みを監視し、効果的な防止策を設計・維持するためには、インターネットに接続されたシステムに効果的な侵入検知および防止システムを導入する必要がある。 無線接続を介した脅威はリスクベースで考慮する必要があり、同様のアプローチが必要となる場合がある。

英文	和訳
12. Internal activity monitoring An effective system, within the framework given by national labour legislation, for detecting unusual or risky user activities (e.g. shift in activity pattern) have to be in place.	12. 内部行動のモニタリング 国内の労働法規で定められた枠組み内で、異常なユーザー行動やリスクの高いユーザー行動（行動パターンの変化など）を検出するための効果的なシステムを導入しなければならない。
13. Security incident management Test facilities should work according to a procedure that defines and documents security incidents. Such incidents could be addressed in terms of criticality, and where applicable, implements effective corrective and preventive actions to prevent recurrence. In cases where data have been, or may have been, compromised, the procedures should include requirements to report security incidents to relevant parties where applicable. When using a service provider, the service level agreement should ensure that incidents are escalated to the Test Facility Management in a timely manner in order for the Test facility Management to be able to report serious breaches to all relevant parties (study directors, sponsors, archivist …).	13. セキュリティインシデント管理 試験施設は、手順書に従って、セキュリティインシデントを定義し文書化すべきである。このようなインシデントは、その重要度に応じて対処され、必要に応じて、再発防止のための効果的な是正措置および予防措置が実施されるべきである。データが漏洩した、または漏洩した可能性がある場合、手順には、必要に応じて関係者にセキュリティインシデントを報告する要件を含めるべきである。サービスプロバイダーを利用する場合、サービスレベル契約により、インシデントが適時に運営管理者へのエスカレーションを確実にし、運営管理者が重大な違反をすべての関係者（試験責任者、スポンサー、資料保存施設管理責任者など）に報告できるようにすべきである。
14. Authentication method The method of authentication in systems should identify users with a high degree of certainty. A minimum acceptable method would be by means of a user identification and password. The need for more stringent authentication methods should be determined based on a risk assessment of the criticality of the data, and might include authentication methods, such as two factor authentication.	14. 認証方法 システムにおける認証方法は、高い確度でユーザーを識別できるものでなければならない。最低限の許容可能な方法は、ユーザーIDとパスワードによる方法である。より厳格な認証方法の必要性は、データの重要度に関するリスク評価に基づいて決定されるべきであり、2要素認証などの認証方法を含む場合がある。

英文	和訳
Two-factor authentication implies that two of the following three factors be used: • something you know, e.g. a user identification and password • something you have, e.g. a security token, a certificate or a mobile phone and an SMS pass code • something you are, e.g. a fingerprint or an iris scan (biometrics) User accounts are automatically locked after a pre-defined number of successive failed authentication attempts, either for a defined period of time, or until they are re-activated by a system administrator after appropriate security checks.	2要素認証とは、以下の3つの要素のうち2つを使用することを意味する。 • 知っているもの、例えばユーザーIDとパスワード • 持っているもの、例えばセキュリティトークン、証明書、または携帯電話とSMSパスコード • 本人であるもの、例えば指紋または虹彩スキャン（バイオメトリクス） ユーザーアカウントは、事前に設定された回数を連続して認証に失敗すると、自動的にロックされる。ロックは、一定期間継続するか、適切なセキュリティチェックを行った上でシステムアドミニストレータによって再有効化されるまで継続される。
15. Remote authentication Remote access to GLP data and application, e.g. to cloud-based systems, raises specific challenges. The level of security should be proportionate to the criticality of the data (e.g. data required to reconstruct the GLP studies) and to the access rights to be granted (read-only, write or even 'admin' rights). A risk-based approach should be used to define the type of access control required, depending on the level of risk.	15. リモート認証 GLPデータやアプリケーションへのリモートアクセス、例えばクラウドベースのシステムへのアクセスには、特有の課題が浮上する。セキュリティのレベルは、データの重要度（GLP試験の再構築に必要なデータなど）や付与されるアクセス権（読み取り専用、書き込み、あるいは「アドミニストレータ」権限）に比例すべきである。リスクのレベルに応じて、必要なアクセスコントロールの種類を定義するために、リスクベースのアプローチを使用すべきである。
16. Password policies Formal procedures for password policies should be implemented. The policies should include but not necessarily be limited to length, complexity, expiry, login attempts, and logout reset. The policies should be enforced by systems, verified	16. パスワードポリシー パスワードポリシーに関する正式な手順を実施すべきである。ポリシーには、長さ、複雑性、有効期限、ログイン試行回数、ログアウト後のリセットなどを含めるべきであるが、これらに限定されるものでは

英文	和訳
during system validation, included in periodic reviews of the system validation and specifically addressed after detection of intruders. The password rules aim to prevent intrusion.	ない。ポリシーはシステムによって強制的に実行され、システムバリデーション時に検証され、システムバリデーションの定期的レビューに含められ、侵入者の検知後に特に対処されるべきである。パスワードの規則は、侵入を防止することを目的としている。
17. Password confidentiality Passwords should be kept confidential. Passwords initially received from the system or from a manager or system administrator have to be changed by the user on their first connection to the system. This should be mandated by the system.	17. パスワードの機密性 パスワードは機密として扱われるべきである。システムまたはマネージャーやシステムアドミニストレータから最初に受け取ったパスワードは、ユーザーがシステムに初めて接続した際に変更しなければならない。これはシステムによって義務付けられるべきである。
18. Inactivity logout Systems including an automatic inactivity, which logs out a user after a defined period of inactivity, could be considered. In such a case, the user should not be able to set the inactivity logout time (outside defined and acceptable limits) or deactivate the functionality. Upon inactivity logout, a full re-authentication is required (e.g. password entry).	18. 無操作ログアウト 定義された無操作期間が経過するとユーザーをログアウトさせる自動無操作ログアウト機能を含むシステムを検討することもできる。このような場合、ユーザーが無操作ログアウト時間（定義された許容範囲外）を設定したり、機能を無効化したりすることはできないようにすべきである。無操作ログアウト時には、完全な再認証（パスワード入力など）が必要である。
19. Remote connection When remotely connecting to systems over the internet, a secure and encrypted protocol (virtual private network (VPN) and/or hypertext transfer protocol secure (HTTPS)) have to be used.	19. リモート接続 インターネット経由でシステムにリモート接続する場合は、安全な暗号化プロトコル（仮想プライベートネットワーク（VPN）および/またはハイパーテキスト転送プロトコルセキュア（HTTPS））を使用しなければならない。

英文	和訳
20. Protection against unauthorised back-end changes The integrity of data has to be protected against unauthorised back-end changes made directly on a database by a database administrator. A method to prevent such changes could be by setting the application up to encrypt its data on the database or by storing data un-encrypted with an encrypted copy. In either case, the database administrator cannot be identical to the administrator of the application.	20. バックエンドの不正な変更に対する保護 データのインテグリティのためには、データベース管理者によるデータベースへの直接的な不正なバックエンドの変更から保護する必要がある。このような変更を防止する方法としては、データベース上のデータを暗号化するようにアプリケーションを設定するか、暗号化されていないデータを暗号化されたコピーとともに保存する方法が考えられる。いずれの場合も、データベース管理者とアプリケーションの管理者を同一人物にすることはできない。
21. Backup Backups are made, retained and stored following established procedures to ensure that GLP data can be restored in case data has been accidentally or deliberately changed or deleted, lost as the result of a hardware malfunction or corrupted, e.g. as the result of a cyber-attack. The frequency, retention and safe storage of backups is critically important to the effectiveness of the process to mitigate these incidents. Backups are made at suitable intervals (e.g. hourly, daily, weekly and monthly) and their retention (e.g. a week, a month, a quarter, forever) should be determined through a risk-based approach. Backups are not be stored at the same physical location, on the same logical network or behind the same firewall as the original data in order to avoid simultaneous destruction or alteration. Depending on the timely requirements for disaster recovery after an incident, applications and system configurations may also need to be backed up, as it may otherwise take a long time to re-establish services.	21. バックアップ データが誤ってまたは故意に変更、削除された場合、ハードウェアの故障の結果としてデータが損失した場合、あるいは例えばサイバー攻撃の結果としてデータが破損した場合に、GLPデータをリストアできるように、バックアップは確立された手順に従って作成、保持、保存される。バックアップの頻度、保持期間、安全な保存は、これらのインシデントを緩和するプロセスの有効性にとって極めて重要である。 バックアップは適切な間隔（例えば、毎時、毎日、毎週、毎月）で作成され、その保持期間（例えば、1週間、1か月、四半期、永久）はリスクベースのアプローチによって決定されるべきである。同時に破壊または改ざんされることを避けるため、元のデータと同じ物理的な場所、同じ論理ネットワーク上、または同じファイアウォールの背後にバックアップを保存してはならない。 また、インシデント後の災害復旧のタイムリーな要件によっては、アプリケーションやシステム構成もバックアップする必要がある。そう

英文	和訳
Restoration of data and potentially applications and configurations from backup should be tested.	でないと、サービスの再開に長い時間がかかる可能性があるためである。 バックアップからのデータ、および場合によってはアプリケーションや構成のリストアは、テストされるべきである。
22. Standard Operating Procedures (SOP) Procedures/policies should be in place describing what IT security measures are in place and taken by the test facility. It should also be clearly described how the facility will handle any IT security breach and the facility should alert its national GLP compliance monitoring authority in case of any IT security issues and data loss/hacks.	22. 標準操作手順書（SOP） 手順/ポリシーには、試験施設で実施されているITセキュリティ対策について記載すべきである。また、ITセキュリティ違反が発生した場合の対応についても明確に記載すべきである。さらに、ITセキュリティ上の問題やデータ損失/ハッキングが発生した場合は、国のGLP遵守監視当局に通知すべきである。

一般社団法人日本 QA 研究会 GLP 部会 第 3 分科会

2025 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. 25
品質改善ツールと GLP に関する OECD の見解
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 25
OECD Position Paper on Good Laboratory Practice and IT Security
https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/12/oecd-position-paper-on-good-laboratory-practice-and-it-security_9772eecf/910b7bd2-en.pdf

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