



PHARMACEUTICAL INSPECTION CONVENTION
PHARMACEUTICAL INSPECTION CO-OPERATION SCHEME

PI 041-1
1 July 2021

PIC/S GUIDANCE

GOOD PRACTICES FOR DATA MANAGEMENT AND INTEGRITY IN REGULATED GMP/GDP ENVIRONMENTS

法規制を受けるGMP/GDP環境における
データマネジメントと完全性の適正規範

© PIC/S 2021

Reproduction prohibited for commercial purposes.
Reproduction for internal use is authorised, provided that
the source is acknowledged.

営利目的の複製は禁止されています。
社内での使用を目的とした複製は許可されています。
ただし、出典が明記されている場合に限りです。

Editor: PIC/S Secretariat

e-mail: info@picscheme.org

web site: <https://www.picscheme.org>



目 次

| | |
|--|----|
| 1. DOCUMENT HISTORY 文書履歴 | 5 |
| 2. INTRODUCTION はじめに | 5 |
| 3. PURPOSE 目的 | 7 |
| 4. SCOPE 適用範囲 | 9 |
| 5. DATA GOVERNANCE SYSTEM データガバナンスシステム | 11 |
| 5.1 What is data governance? データガバナンスとは何か? | 11 |
| 5.2 Data governance systems データガバナンスシステム | 12 |
| 5.3 Risk management approach to data governance データガバナンスに対するリスクマネジメントアプローチ | 14 |
| 5.4 Data criticality データの重要性 | 16 |
| 5.5 Data risk データのリスク | 16 |
| 6. ORGANISATIONAL INFLUENCES ON SUCCESSFUL DATA INTEGRITY MANAGEMENT データ完全性のマネジメントの成功への組織の影響 | 21 |
| 6.1 General 一般的事項 | 21 |
| 6.2 Policies related to organisational values, quality, staff conduct and ethics 組織の価値観、品質、スタッフの行動および倫理に関する方針 | 24 |
| 6.3 Quality culture 品質文化 | 27 |
| 6.4 Modernising the Pharmaceutical Quality System 医薬品品質システムの近代化 | 28 |
| 6.5 Regular management review of performance indicators (including quality metrics) パフォーマンス指標（品質メトリクス：品質計量化指標を含む）の 定期的なマネジメント・レビュー | 30 |
| 6.6 Resource allocation 資源の配分 | 30 |
| 6.7 Dealing with data integrity issues found internally 組織内部で発見された完全性問題への対処 | 32 |
| 7. GENERAL DATA INTEGRITY PRINCIPLES AND ENABLERS 一般的なデータ完全性の原則と実現化 | 33 |
| 7.7 True copies 真正コピー | 37 |
| 7.8 Limitations of remote review of summary reports 要約報告書の遠隔レビューの限界 | 42 |



8 SPECIFIC DATA INTEGRITY CONSIDERATIONS FOR PAPER- BASED SYSTEMS

| | |
|---|----|
| 紙ベースシステムに固有なデータ完全性の考慮事項 | 44 |
| 8.1 Structure of Pharmaceutical Quality System and control of blank forms/templates/records | |
| PQSシステムの構造と、ブランクの様式／テンプレート／記録書..... | 44 |
| 8.2 Importance of controlling records 記録を管理することの重要性 | 45 |
| 8.3 Generation, distribution and control of template records | |
| テンプレート記録書の生成、配布および管理..... | 46 |
| 8.4 Expectations for the generation, distribution and control of records | |
| 記録の作成、配布、管理に関する期待事項 | 46 |
| 8.5 Use and control of records located at the point-of-use | |
| 使用箇所に置かれる記録の、使用と管理..... | 52 |
| 8.6 Filling out records 記録の記入 | 53 |
| 8.7 Making corrections on records 記録についての修正の実施 | 56 |
| 8.8 Verification of records (secondary checks) 記録の検証（二次チェック） | 57 |
| 8.9 Direct print-outs from electronic systems 電子システムからの直接プリントアウト | 60 |
| 8.10 Document retention (Identifying record retention requirements and archiving records) | |
| 文書の保存（記録保存要件の特定と記録のアーカイブ化） | 60 |
| 8.11 Disposal of original records or true copies 記録原本または真正コピーの廃棄 | 64 |

9. SPECIFIC DATA INTEGRITY CONSIDERATIONS FOR COMPUTERISED SYSTEMS

| | |
|--|-----|
| コンピュータ化されたシステムにおける具体的なデータ完全性に関する考慮事項 | 64 |
| 9.1 Structure of the Pharmaceutical Quality System and control of computerised systems | |
| 医薬品品質システムの構造とコンピュータシステムの管理 | 64 |
| 9.2 Qualification and validation of computerised systems | |
| コンピュータ化されたシステムの適格性およびバリデーション | 68 |
| 9.3 Validation and Maintenance バリデーションとメンテナンス | 69 |
| 9.4 Data Transfer データ転送 | 80 |
| 9.5 System security for computerised systems | |
| コンピュータ化されたシステムのシステムセキュリティ | 84 |
| 9.6 Audit trails for computerised systems コンピュータシステムの監査証跡..... | 96 |
| 9.7 Data capture/entry for computerised systems | |
| コンピュータ化システムの捕捉／エントリ | 101 |
| 9.8 Review of data within computerised systems | |



| | |
|--|-----|
| コンピュータ化されたシステム内のデータのレビュー | 104 |
| 9.9 Storage, archival and disposal of electronic data | |
| 電子的データの保管、アーカイビング、および廃棄 | 107 |
| 9.10 Management of Hybrid Systems ハイブリッドシステムのマネジメント | 111 |
| 10. DATA INTEGRITY CONSIDERATIONS FOR OUTSOURCED ACTIVITIES | |
| 外部委託活動におけるデータ完全性の考慮事項 | 114 |
| 10.1 General supply chain considerations | |
| サプライチェーンに関する一般的な考慮事項 | 114 |
| 10.2 Routine document verification 日常的な文書確認..... | 115 |
| 10.3 Strategies for assessing data integrity in the supply chain | |
| サプライチェーンでのデータ完全性の評価戦略 | 115 |
| 11. REGULATORY ACTIONS IN RESPONSE TO DATA INTEGRITY FINDINGS | |
| データ完全性に関する調査結果に対応する規制措置 | 118 |
| 11.1 Deficiency references 欠陥状態の参照 | 118 |
| 11.2 Classification of deficiencies 欠陥のクラス分類 | 119 |
| 12 REMEDIATION OF DATA INTEGRITY FAILURES データ完全性の欠陥の改善..... | 123 |
| 12.1 Responding to Significant Data Integrity issues | |
| 重要なデータ完全性問題への対応 | 123 |
| 12.2 Indicators of improvement 改善の指標 | 126 |
| 13. Glossary 用語集 | 128 |
| 14 REVISION HISTORY 改定履歴..... | 132 |

1. DOCUMENT HISTORY 文書履歴

| | |
|-----------------------------------|-------------|
| Adoption by Committee of PI 041-1 | 1 June 2021 |
| Entry into force of PI 041-1 | 1 July 2021 |

2. INTRODUCTION はじめに

2.1 PIC/S Participating Authorities regularly undertake inspections of manufacturers and distributors of Active Pharmaceutical Ingredient (API) and medicinal products in order to determine the level of compliance with Good Manufacturing Practice (GMP) and Good Distribution Practice (GDP) principles. These inspections are commonly performed on-site however maybe performed through the remote or off-site evaluation of documentary evidence, in which case the limitations of remote review of data should be considered.

PIC/S 参加機関は、原薬（Active Pharmaceutical Ingredient : API）及び医薬品（medicinal products）の製造業者及び販売業者に対し、GMP（Good Manufacturing Practice : 適正製造規範）及び GDP（Good Distribution Practice : 適正流通規範）の遵守状況を確認するための査察を定期的に行う。これらの査察は一般的に現場（on-site）で行われるが、証拠書類の遠隔評価や現場外（オフサイト : off-site）で行われることもあり、その場合にはデータの遠隔レビューの限界を考慮する必要がある。

2.2 The effectiveness of these inspection processes is determined by the reliability of the evidence provided to the inspector and ultimately the integrity of the underlying data. It is critical to the inspection process that inspectors can determine and fully rely on the accuracy and completeness of evidence and records presented to them.

これらの査察プロセスの有効性は、査察官に提供された証拠の信頼性、ひいては基礎となるデータの完全性によって決定される。査察官は、提示された証拠や記録の正確性と完全性を判断し、十分に信頼できることが、査察プロセスにとって極めて重要である。

2.3 Data management refers to all those activities performed during the handling of data including but not limited to data policy, documentation, quality and security. Good data management practices influence the quality of all data generated and recorded by a manufacturer. These practices should ensure that data is attributable, legible, contemporaneous, original, accurate, complete, consistent, enduring, and available. While the main focus of this document is in relation to GMP/GDP expectations, the principles herein should also be considered in the wider context of good data management such as data included in the registration dossier based on which API and drug product control strategies and specifications are set.

データマネジメントとは、データを取り扱う際に行われるすべての活動をいうものであり、これにはデータポリシー（data policy）、文書化（documentation）、品質（quality）およびセキュリティ（security）を含むが、これに限定されるものではない。適正データマネジメント規範（good data management practices）は、製造業者が生成・記録するすべてのデータの品質に影響を与える。これらの規範は、データの帰属性（attributable）、可読性（legible）、同時性（contemporaneous）、原本性（original）、正確性（accurate）、完全性（complete）、一貫性（consistent）、永続性（enduring）、耐久性（enduring）及び利用可能性（available）を確保すべきである（訳注参照）。この文書の主眼はGMP/GDPに関連したものであるが、ここに示した原則は、原薬及び製剤の管理戦略及び規格が設定される際の基本となる所の、登録書類の添付書類（registration dossier）に含まれるデータなどの、適正データマネジメント（good data management）のより広い文脈においても考慮されるべきである。

（訳注）この文章は、「ALCOA plus」（“ALCOA+”あるいは“ALCOA-C”）についての記載である。

「ALCOA plus」はデータが持つべき特性であって、下記の表のようにまとめられる。なお、用語や説明の日本語は資料によって多少の異同がある。

表：“ALCOA+”の概要（データの求められる属性）

| | 用語 | 訳語（代表例） | 用語の説明 |
|-------|-----------------------|----------|---|
| ALCOA | Attributable | 帰属性 | データの所有者・帰属・責任が明確であること attributable to the person generating the data |
| | Legible | 判読性 | データが判読できこと・理解できること legible and permanent |
| | Contemporaneous | 同時性 | データの生成と記録が同時であること contemporaneous |
| | Original | 原本性 | データが原本であること・複製や転記ではないこと original record (or certified true copy) |
| | Accurate | 正確性 | データが正確であること accurate |
| CEA | Complete | 完全性 | データが完全であること；完全なセット the data must be whole; a complete set |
| | Consistent | 一貫性 | データが一貫して矛盾がないこと the data must be self-consistent |
| | Enduring | 耐久性／普遍性 | データがそのサイクルを通して永続的であること durable; lasting throughout the data lifecycle |
| | Available when needed | 要時取出し可能性 | データが必要なときに利用可能であること readily available for review or inspection purposes |

なお、望月清、「製薬業界に求められるデータインテグリティ実務対応」、ケミカルタイムス、2020年1月号に、簡潔にまとめられた記事が掲載されている。https://www.kanto.co.jp/dcms_media/other/CT_255_03.pdf

2.4 Good data management practices apply to all elements of the Pharmaceutical Quality System and the principles herein apply equally to data generated by electronic and paper-based systems.

適正なデータマネジメントの実践は、医薬品品質システム（PQS: Pharmaceutical Quality System）のすべての要素に適用され、ここに記載された原則は、電子および紙ベースのシステムで生成されたデータに等しく適用される。



2.5 Data Integrity is defined as “the degree to which data are complete, consistent, accurate, trustworthy, and reliable and that these characteristics of the data are maintained throughout the data life cycle”.¹ This is a fundamental requirement for an effective Pharmaceutical Quality System which ensures that medicines are of the required quality. Poor data integrity practices and vulnerabilities undermine the quality of records and evidence, and may ultimately undermine the quality of medicinal products.

データの完全性とは、「データが完全であり、一貫性があり、正確であり、原本性があり（訳注参照）、信頼性があり、データのこれらの特性がデータのライフサイクルを通じて維持される度合い」と定義される¹。これは、医薬品が要求される品質を持つこと保証する効果的な医薬品品質システムの基本要件である。データの整合性に欠ける行為や脆弱性（vulnerabilities）は、記録や証拠の質をむしろ、最終的には医薬品の品質をむしろ可能性がある。

1. ‘GXP’ Data Integrity Guidance and Definitions, MHRA, March 2018

訳注：“trustworthy”は、“deserving of trust, or able to be trusted”（信頼に値する、または信頼できる）との意味であり、「原本性」の用語をあてた。

2.6 The responsibility for good practices regarding data management and integrity lies with the manufacturer or distributor undergoing inspection. They have full responsibility and a duty to assess their data management systems for potential vulnerabilities and take steps to design and implement good data governance practices to ensure data integrity is maintained.

データマネジメントおよび完全性に関する適正な実践の責任は、査察を受ける製造業者または販売業者にある。彼らは「可能性のある脆弱性（vulnerabilities）についてのそのデータマネジメントシステムを評価すること」、及び「データの完全性を確実に維持するために適正なデータガバナンスを設計・実施するための手段を講じる」ことの全ての責任と義務を負っている。

3. PURPOSE 目的

3.1 This document was written with the aim of: この文書は以下の目的を以って書かれている。

3.1.1 Providing guidance for Inspectorates in the interpretation of GMP/GDP requirements in relation to good data management and the conduct of inspections.

適正なデータマネジメントに関連したGMP/GDP要求事項の解釈及び査察の実施について、査察当局にガイダンスを提供する。

3.1.2 Providing consolidated, illustrative guidance on risk-based control strategies which enable the existing requirements for data to be valid, complete and reliable as described in PIC/S Guides for GMP² and GDP³ to be implemented in the context of modern industry practices

and globalised supply chains.

PIC/SガイドGMP²及びGDP³に記載されているデータの妥当性、完全性及び信頼性に関する既存の要求事項を、リスクベースの管理戦略に関する統合された例示的なガイダンスを提供する。これは、現在の業界慣行（modern industry practices）及びグローバル化したサプライチェーンの中で実施できるようにするために行うものである。

2. PIC/S PE 009 Guide to Good Manufacturing Practice for Medicinal Products, specifically Part I chapters 4, 5, 6, Part II chapters 5, 6 & Annex 11

3. PIC/S PE 011 Guide to Good Distribution Practice for Medicinal Products, specifically sections 3, 4, 5 & 6

3.1.3 Facilitating the effective implementation of good data management elements into the routine planning and conduct of GMP²/GDP³ inspections; to provide a tool to harmonise GMP/GDP inspections and to ensure the quality of inspections with regards to data integrity expectations.

GMP/GDP査察の日常的な計画および実施において、適正なデータマネジメントの要素の効果的な導入を促進する；GMP/GDP査察を調和させるためのツールを提供すること、及びおよびデータの完全性に関する期待に関して査察の質を確保すること。

3.2 This guidance, together with Inspectorate resources such as aide memoire, should enable the inspector to make an optimal use of the inspection time and an optimal evaluation of data integrity elements during an inspection.

このガイダンスは、“aide memoire（備忘録）”などの査察当局の資源（リソース）と合わせて活用し、査察中にデータ完全性の要素を最適に評価できるであろう。

3.3 Guidance herein should assist the Inspectorate in planning a risk-based inspection relating to good data management practices.

ここに記載されているガイダンスは、検査当局が適正データマネジメント規範に関連するリスクベースの査察を計画する際に役立つであろう。

3.4 Good data management has always been considered an integral part of GMP/GDP. Hence, this guide is not intended to impose additional regulatory burden upon regulated entities, rather it is intended to provide guidance on the interpretation of existing GMP/GDP requirements relating to current industry data management practices.

適正なデータマネジメントは、常に GMP/GDP の不可欠な要素と考えられている。したがって、このガイドは、規制対象となる企業に新たな規制負担を課すことを意図したものではなく、むしろ、現在の業界のデータマネジメントの慣行に関連する既存のGMP/GDP要求事項の解釈に関するガイダンスを提供することを意図したものである。

3.5 The principles of data management and integrity apply equally to paper- based, computerised and hybrid systems and should not place any restraint upon the development or adoption of new concepts or technologies. In accordance with ICH Q10 principles, this guide should facilitate the adoption of innovative technologies through continual improvement.

データマネジメントとデータ完全性の原則は、紙ベースのシステム、コンピュータ化されたシステム、ハイブリッドシステムに等しく適用され、新しい概念や技術の開発や採用を制限するものであってはならない。ICH Q10 の原則に従い、本ガイドは継続的な改善を通じて革新的な技術の採用を促進すべきである。

3.6 The term “Pharmaceutical Quality System” is predominantly used throughout this document to denote the quality management system used to manage and achieve quality objectives. While the term “Pharmaceutical Quality System” is used predominantly by GMP regulated entities, for the purposes of this guidance, it should be regarded as interchangeable with the term “Quality System” used by GDP regulated entities.

「医薬品品質システム」（“Pharmaceutical Quality System” : PQS）という用語は、主として、品質目標（quality objectives）をマネジメントし、それを達成するために使用される品質のマネジメントのシステムを示すために、この文書で使用されている。「医薬品品質システム」という用語は、主にGMP規制対象企業で使用されているが、本ガイダンスでは、GDP規制対象企業で使用されている「品質システム」（“Quality System”）という用語と互換性があるとみなすべきものである。

3.7 This guide is not mandatory or enforceable under law. It is not intended to be restrictive or to replace national legislation regarding data integrity requirements for manufacturers and distributors of medicinal products and active substances (i.e. active pharmaceutical ingredients). Data integrity deficiencies should be referenced to national legislation or relevant paragraphs of the PIC/S GMP or GDP guidance.

このガイドは、法律に基づく義務的事項や強制力はない。このガイドは、医薬品及び活性物質（原薬）の製造業者及び販売業者のデータ完全性要件に関する国内法を制限したり、代替したりすることを意図していない。データ完全性の不備は、国内法またはPIC/S GMPもしくはGDPガイダンスの関連パラグラフを参照する必要がある。

4. SCOPE 適用範囲

4.1 The guidance has been written to apply to on-site inspections of those sites performing manufacturing (GMP) and distribution (GDP) activities. The principles within this guide are applicable for all stages throughout the product lifecycle. The guide should be considered as

a non-exhaustive list of areas to be considered during inspection.

このガイダンスは、製造（GMP）及び流通（GDP）活動を行っている製造所の現場査察に適用するように作成されている。このガイドの原則は、製品のライフサイクルのすべての段階に適用される。本ガイドは、査察の際に考慮すべき分野を全ては網羅していないリストと考えること。

4.2 The guidance also applies to remote (desktop) inspections of sites performing manufacturing (GMP) and distribution (GDP) activities, although this will be limited to an assessment of data governance systems. On-site assessment is normally required for data verification and evidence of operational compliance with procedures.

この指針は、製造（GMP）及び流通（GDP）活動を行っている事業所の遠隔（desktop：デスクトップ）査察にも適用されるが、これはデータガバナンスシステムの評価に限定されるものとなるだろう。通常、データの検証及び業務上の手順遵守の証明のために、現場での評価（on-site assessment）が必要である。

4.3 Whilst this document has been written with the above scope, many principles regarding good data management practices described herein have applications for other areas of the regulated pharmaceutical and healthcare industry.

この文書は上記の適用範囲を念頭に作成されているが、この文書に記載されている適正データマネジメントの実践に関する多くの原則は、法的規制を受けている製薬業界およびヘルスケア業界の他の分野にも適用できる。

4.4 This guide is not intended to provide specific guidance for “for-cause” inspections following detection of significant data integrity vulnerabilities where forensic expertise may be required.

このガイドは、犯罪科学の専門知識（forensic expertise）が必要となるような重大なデータ完全性の脆弱性が検出された後の“for-cause”査察（原因を究明するための、特別な査察：訳注参照）について、特定のガイダンスを提供することを意図していない。

訳注：「“for-cause” inspections」は、下記のWeb資料に次のような説明がある：

“For Cause” Inspections investigate a specific problem that has been reported to FDA. The source of the report can be the manufacturer (e.g., resultant of a recall, MDR), consumer/user complaints, or even a disgruntled employee. A “for cause” inspection will focus on the particular issue, but can branch out to cover unrelated elements of the firm’s operations. This inspection usually is initiated at the request of CDRH, ORA, or regional directive.

These inspections typically are more in-depth than routine inspections, and they may not follow a QSIT approach.

（参考訳）

「原因究明のための査察」は、FDAに報告された特定の問題を調査するものである。報告の出所は、メーカー（例：回収やMDRの結果）、消費者／ユーザからの苦情、あるいは不満を持った従業員であることもある。原因究明のための査察は、特定の問題に焦点を当てるが、会社の業務の関連性のない要素にまで及ぶこともある。この検査は、通常、CDRH（医療機器・放射線保健センター）、ORA（法規制遵守部）、または米国各区域の指令の要請により開始される。



これらの検査は、通常の検査よりもより詳細なものであり、QSITのアプローチに従わない場合もある。

出典：[Peter Ohanian, "Understanding The 4 Types Of FDA Inspection," MED Device Online, October 3, 2016,](#)

(リンク先は上記に埋め込み)

なお、上記の“MDR”は、欧州で流通する医療機器に関する規制「欧州医療機器規則：Medical Device Regulation」を意味する。また、IVDRというものもあり、これは「体外診断用医療機器規則：In Vitro Diagnostic Regulation」を意味する。

5. DATA GOVERNANCE SYSTEM データガバナンスシステム

5.1 What is data governance? データガバナンスとは何か？

5.1.1 Data governance is the sum total of arrangements which provide assurance of data integrity.

These arrangements ensure that data, irrespective of the process, format or technology in which it is generated, recorded, processed, retained, retrieved and used will ensure an attributable, legible, contemporaneous, original, accurate, complete, consistent, enduring, and available record throughout the data lifecycle. While there may be no legislative requirement to implement a ‘data governance system’, its establishment enables the manufacturer to define, prioritise and communicate their data integrity risk management activities in a coherent manner. Absence of a data governance system may indicate uncoordinated data integrity systems, with potential for gaps in control measures.

データガバナンスとは、データの完全性を保証するための取り決めの総体 (sum total of arrangements) である。これらの取り決めは、データが生成され、記録され、処理され、保持され、検索され、使用されるプロセス、フォーマット、または技術にかかわらず、データのライフサイクルを通じて、帰属性 (attributable)、判読性 (legible)、同時期性 (contemporaneous)、オリジナル性 (original)、正確性 (accurate)、完全性 (complete)、一貫性 (consistent)、耐久性 (enduring)、および要事取出し可能性 (available) をもつ記録を確実にするものである (訳注：ALCOA+の各事項)。「データガバナンスシステム」を導入するとの法的要件はないが、このシステムを構築することで、製造業者はデータ完全性マネジメント活動を一貫した方法で定義し、優先順位をつけ、伝達することができる。データガバナンスシステムがないことは、データ完全性システムが一貫性のない対応をしていることを意味し、管理手段にギャップが生じる可能性がある。

5.1.2 The data lifecycle refers to how data is generated, processed, reported, checked, used for decision-making, stored and finally discarded at the end of the retention period. Data relating to a product or process may cross various boundaries within the lifecycle. This may include data transfer between paper-based and computerised systems, or between different organisational boundaries; both internal (e.g. between production, QC and QA) and external (e.g. between service providers or contract givers and acceptors).



データのライフサイクルは、データがどのように生成され、処理され、報告され、確認され、意思決定に使用され、保存され、最終的に保存期間の終了時に廃棄されるかを意味する。製品やプロセスに関連するデータは、ライフサイクルの中で様々な境界を越える可能性がある。これには、紙ベースのシステムとコンピュータ化されたシステムとの間でのデータ転送や、社内（例：製造、QC、QAの間）および社外（例：サービスプロバイダー、契約の授受など）の異なる組織の境界が含まれることがある。

5.2 Data governance systems データガバナンスシステム

5.2.1 Data governance systems should be integral to the Pharmaceutical Quality System described in PIC/S GMP/GDP. It should address data ownership throughout the lifecycle, and consider the design, operation and monitoring of processes and systems in order to comply with the principles of data integrity, including control over intentional and unintentional changes to, and deletion of information.

データガバナンスシステムは、PIC/S GMP/GDPに記載されている医薬品品質システムと一体でなければならない。データガバナンスシステムは、ライフサイクルを通してデータの所有権(ownership)に対処し、そしてデータ完全性の原則に法的な適合をさせるために、プロセスおよびシステムの設計、運営、及びモニタリングを考慮すべきである。これには情報の意図的・非意図的な変更及び削除の管理を含むものである。

5.2.2 Data governance systems rely on the incorporation of suitably designed systems, the use of technologies and data security measures, combined with specific expertise to ensure that data management and integrity is effectively controlled. Regulated entities should take steps to ensure appropriate resources are available and applied in the design, development, operation and monitoring of the data governance systems, commensurate with the complexity of systems, operations, and data criticality and risk.

データガバナンスシステムは、データのマネジメントおよび完全性が、効果的に制御されることを保証するために、特定の専門家が関与した上での「適切に設計されたシステムの組み込み」、および「技術およびデータセキュリティ対策の使用」に依存している。規制対象となる企業は、次のことが保証されるようなステップをとること：

- (1) データガバナンスシステムの設計、開発、運用および監視において、適切なリソースが利用可能であり、適用されること；
- (2) システム、運用の複雑さ、及びデータの重要性およびリスクが見合っていること。

5.2.3 The data governance system should ensure controls over the data lifecycle which are commensurate with the principles of quality risk management. These controls may be:

データガバナンスのシステムは、品質リスクマネジメントの原則に見合った、データライフ

サイクルにわたっての管理を確保すべきである。これらの管理は以下のようなものが考えられる。

□ Organisational 組織的なもの

- procedures, e.g. instructions for completion of records and retention of completed records;
手順、例えば、記録の記入方法や、記入済み記録の保管方法など；
- training of staff and documented authorisation for data generation and approval;
要員の訓練、及びデータの生成と承認に関する文書化された権限；
- data governance system design, considering how data is generated, recorded, processed, retained and used, and risks or vulnerabilities are controlled effectively;
データがどのように生成、記録、処理、保持、使用され、リスクや脆弱性が効果的に管理されているかを考慮した、データガバナンスシステムの設計；
- routine (e.g. daily, batch- or activity-related) data verification;
日常的な（例：毎日、バッチまたは活動に関連する）データ検証；
- periodic surveillance, e.g. self-inspection processes seek to verify the effectiveness of the data governance system; or
定期的なサーベイランス。例えばデータガバナンスシステムの有効性を検証するための自己点検プロセスを行う；または
- the use of personnel with expertise in data management and integrity, including expertise in data security measures.
データマネジメントおよび完全性の専門知識を有する人材の活用。これには、データセキュリティ対策の専門知識を含む。

□ Technical 技術的な面

- computerised system validation, qualification and control;
コンピュータ化システムのバリデーション、適格性評価、及び管理；
- automation; or 自動化；または
- the use of technologies that provide greater controls for data management and integrity.
データのマネジメントと完全性のためのコントロールを強化する技術の使用。

5.2.4 An effective data governance system will demonstrate Senior management's understanding and commitment to effective data governance practices including the necessity for a combination of appropriate organisational culture and behaviours (section 6) and an



understanding of data criticality, data risk and data lifecycle. There should also be evidence of communication of expectations to personnel at all levels within the organisation in a manner which ensures empowerment to report failures and opportunities for improvement. This reduces the incentive to falsify, alter or delete data.

効果的なデータガバナンスシステムは、効果的なデータなデータガバナンスの実践に対する上級管理者の理解とコミットメント（訳注：強い意志を持った誓約）を示すものである。これには、次のものを含んでいる：

- ・適切な組織文化及び行動（Section 6参照）の組み合わせの必要性；及び
- ・データの重要性、データリスク、及びデータライフサイクルの理解。

また、組織内のすべてのレベルの担当者に期待事項を伝えている証拠が存在すべきであり、この方法は、失敗と改善の機会を報告する権限を付与することを、保証するものであること。これにより、データを改ざん、変更、または削除する動機が減少する。

5.2.5 The organisation's arrangements for data governance should be documented within their Pharmaceutical Quality System and regularly reviewed.

データガバナンスに関する組織の取り決めは、その医薬品品質システム（PQS）の中で文書化し、定期的に見直すべきである。

5.3 Risk management approach to data governance

データガバナンスに対するリスクマネジメントアプローチ

5.3.1 Senior management is responsible for the implementation of systems and procedures to minimise the potential risk to data integrity, and for identifying the residual risk, using the principles of ICH Q9. Contract Givers should perform a review of the contract acceptor's data management policies and control strategies as part of their vendor assurance programme. The frequency of such reviews should be based on the criticality of the services provided by the contract acceptor, using risk management principles (refer to section 10).

上級経営陣は、ICH Q9 の原則を用いて、データの完全性に対する潜在的なリスクを最小限に抑えるためのシステム及び手順の実施、並びに残留リスクの特定に責任を負う。業務委託者（Contract Givers）は、そのベンダー保証プログラムの一部として、業務受託者のデータマネジメント方針（contract acceptor's data management policies）と管理戦略のレビューを行うべきである。このようなレビューの頻度は、リスクマネジメントの原則（Section 10 参照）を用いて、業務受託者（contract acceptor）が提供するサービスの重要性に基づくべきである。

5.3.2 The effort and resource assigned to data governance should be commensurate with the risk to product quality, and should also be balanced with other quality resource demands. All entities regulated in accordance with GMP/GDP principles (including manufacturers,



analytical laboratories, importers and wholesale distributors) should design and operate a system which provides an acceptable state of control based on the data quality risk, and which is documented with supporting rationale.

データガバナンスに割り当てられる労力と資源は、製品品質に対するリスクに見合うものとすべきであり、かつ他の品質資源の需要とのバランスをとる必要がある。GMP/GDPの原則に従って規制されている全ての事業者（製造業者、分析機関、輸入業者、卸売販売業者を含む）は、データ品質のリスクに基づいて許容可能な管理状態を提供し、かつ裏付けとなる根拠を文書化した所の、システムを設計し、運用するべきである。

5.3.3 Where long term measures are identified in order to achieve the desired state of control, interim measures should be implemented to mitigate risk, and should be monitored for effectiveness. Where interim measures or risk prioritisation are required, residual data integrity risk should be communicated to senior management, and kept under review. Reverting from automated and computerised systems to paper-based systems will not remove the need for data governance. Such retrograde approaches are likely to increase administrative burden and data risk, and prevent the continuous improvement initiatives referred to in paragraph 3.5.

望ましい管理された状態を達成するために長期的な対策が特定されている場合、リスクを軽減するために暫定的な対策を実施し、その有効性を監視すべきである。暫定措置またはリスクの優先順位付けが必要な場合は、残存するデータ完全性のリスクを上級経営陣に伝え、常に見直しを行うべきである。自動化された、そしてコンピュータ化システムから紙ベースのシステムに戻しても、データガバナンスの必要性は消滅しない。そのような逆行するアプローチは、管理負担とデータリスクを増大させ、3.5項で言及されている継続的な改善のイニシアチブを妨げる可能性が高い。

5.3.4 Not all data or processing steps have the same importance to product quality and patient safety. Risk management should be utilised to determine the importance of each data/processing step. An effective risk management approach to data governance will consider:

全てのデータや処理ステップが、製品の品質や患者の安全性に対して同じ重要性を持つわけではない。各データ／処理のステップの重要性を判断するために、リスクマネジメントを活用すべきである。データガバナンスに対する効果的なリスクマネジメントアプローチは以下を考慮する：

- Data criticality (impact to decision making and product quality) and
データの重要性（意思決定及び製品品質への影響）；及び
- Data risk (opportunity for data alteration and deletion, and likelihood of detection /
visibility of changes by the manufacturer's routine review processes).



データのリスク（データの変更及び削除の機会、製造者の日常的なレビュープロセスによる変更の検出及び可視性の可能性）。

From this information, risk proportionate control measures can be implemented.

Subsequent sections of this guidance that refer to a risk management approach refer to 'risk' as a combination of data risk and data criticality concepts.

これらの情報から、リスクに応じた管理策を実施することができる。本ガイダンスの後続の章では、リスクマネジメントのアプローチに言及しているが、「リスク」とはデータリスクとデータ重要性の概念を組み合わせたものである。

5.4 Data criticality データの重要性

5.4.1 The decision that data influences may differ in importance and the impact of the data to a decision may also vary. Points to consider regarding data criticality include:

データが影響を与える意思決定は、重要性が異なる場合があり、意思決定に対するデータの影響度も異なる場合がある。データの重要性について考慮すべき点は、以下が含まれる。

- Which decision does the data influence?

そのデータはどの意思決定に影響を与えるのか？

For example: when making a batch release decision, data which determines compliance with critical quality attributes is normally of greater importance than warehouse cleaning records.

例えば、バッチ出荷を決定する際には、通常、倉庫の清掃記録よりも、重要な品質特性が、法令（訳注：この場合は製品規格）への適合性を決定するデータの方が重要である；

- What is the impact of the data to product quality or safety?

何が、製品の品質や安全性に対するデータの影響は何か？

For example: for an oral tablet, API assay data is of generally greater impact to product quality and safety than tablet friability data.

例えば：経口錠剤の場合、原薬の定量データは、錠剤の摩損度データよりも製品の品質や安全性に対する影響が一般的に大きい。

5.5 Data risk データのリスク

5.5.1 Whereas data integrity requirements relate to all GMP/GDP data, the assessment of data criticality will help organisations to prioritise their data governance efforts. The rationale

for this prioritisation should be documented in accordance with quality risk management principles.

データの完全性に関する要求事項はすべてのGMP/GDPデータに関連するが、データの重要性を評価することは、組織がデータガバナンスの取り組みに優先順位をつけるのに役立つ。この優先順位付けの根拠は、品質リスク管理の原則に基づいて文書化すべきである。

5.5.2 Data risk assessments should consider the vulnerability of data to involuntary alteration, deletion, loss (either accidental or by security failure) or re-creation or deliberate falsification, and the likelihood of detection of such actions. Consideration should also be given to ensuring complete and timely data recovery in the event of a disaster. Control measures which prevent unauthorised activity, and increase visibility / detectability can be used as risk mitigating actions.

データリスクの評価は、不本意な変更 (involuntary alteration)、削除、消失 (偶発的またはセキュリティ障害による)、あるいは再作成 (re-creation) または意図的な改竄 (deliberate falsification)、そしてそのような行為の発見の可能性を考慮すべきである。また、災害時に完全かつタイムリーにデータを回復することも考慮すべきである。不正な活動を防止し、可視性／検出性を高める管理策は、リスクを軽減するための措置として利用することができる。

5.5.3 Examples of factors which can increase risk of data failure include processes that are complex, or inconsistent, with open ended and subjective outcomes. Simple processes with tasks which are consistent, well defined and objective lead to reduced risk.

データ障害のリスクを増大させる要因の例としては、変更が可能 (open ended) で、複雑性や一貫性のないというプロセスなどが挙げられる。一貫性があり、良く定義され、客観的なリスクを持つ単純なプロセスは、リスクの低減につながる。

5.5.4 Risk assessments should focus on a business process (e.g. production, QC), evaluate data flows and the methods of generating and processing data, and not just consider information technology (IT) system functionality or complexity. Factors to consider include:

リスクアセスメントは、情報技術 (IT) システムの機能性や複雑性だけを考慮するのではなく、ビジネスプロセス (製造、品質管理など) に焦点を当て、データの流れ及びデータの生成・処理方法を評価するものとする。考慮すべき要素は以下の通りである：

- process complexity (e.g. multi-stage processes, data transfer between processes or systems, complex data processing);
プロセスの複雑性 (例えば、多段階のプロセス、プロセスまたはシステム間のデータ転送、複雑なデータ処理) ；
- methods of generating, processing, storing and archiving data and the ability to assure data quality and integrity;



データの生成、処理、保存、保管の方法、およびデータの品質と整合性を保証する能力；

- process consistency (e.g. biological production processes or analytical tests may exhibit a higher degree of variability compared to small molecule chemistry);

プロセスの一貫性（例えば、生物学的生産のプロセスや分析試験は、低分子化学と比較して、より高度な変動性を示す可能性がある）。

- degree of automation / human interaction;

自動化／ヒトの相互作用の度合い；

- subjectivity of outcome / result (i.e. is the process open-ended vs well defined);

成果（outcome）／結果（result）の主観性（プロセスがオープンエンド（任意に変更可能）であるか、明確に定義されているかなど）；

- outcomes of a comparison between electronic system data and manually recorded events (e.g. apparent discrepancies between analytical reports and raw-data acquisition times); and

電子システムのデータと手動で記録された事象との比較の結果（例：分析報告書と生データの取得時間との間の明らかな不一致）。そして

- inherent data integrity controls incorporated into the system or software.

システムまたはソフトウェアに組み込まれている固有のデータ完全性管理。

5.5.5 For computerised systems, manual interfaces with IT systems should be considered in the risk assessment process. Computerised system validation in isolation may not result in low data integrity risk, in particular, if the user is able to influence the reporting of data from the validated system, and system validation does not address the basic requirements outlined in section 9 of this document. A fully automated and validated process together with a configuration that does not allow human intervention, or reduces human intervention to a minimum, is preferable as this design lowers the data integrity risk. Appropriate procedural controls should be installed and verified where integrated controls are not possible for technical reasons.

コンピュータ化されたシステムの場合、ITシステムとの手動によるインターフェースは、リスクアセスメントのプロセスにおいて考慮すべきである。コンピュータ化されたシステムのバリデーションを単独で実施した場合、特に、ユーザがバリデーションされたシステムからのデータの報告に影響を与えることができ、システムのバリデーションが本文書のSection 9に概説されている基本的な要件に対応していない場合には、データ完全性へのリスクが低くならない可能性がある。ヒトの介入を許さないか、あるいは人の介入を最小限にまで減らした形態を持つ、完全に自動化され、バリデートされたプロセスは、データ完全性に対するリスクを低くした設計として望ましいものである。技術的な理由から、統合化された制御が不可能な場合は、適切な手続き的な管理を導入し、それを確認する必要がある。



5.5.6 Critical thinking skills should be used by inspectors to determine whether control and review procedures effectively achieve their desired outcomes. An indicator of data governance maturity is an organisational understanding and acceptance of residual risk, which prioritises actions. An organisation which believes that there is 'no risk' of data integrity failure is unlikely to have made an adequate assessment of inherent risks in the data lifecycle. The approach to assessment of data lifecycle, criticality and risk should therefore be examined in detail. This may indicate potential failure modes which can be investigated during an inspection.

査察官は、管理とレビューの手順が望ましい結果を効果的に達成しているかどうかを判断するために、批判的な思考スキルを使用すべきである。データガバナンスの成熟度を示す指標は、残存リスクに対する組織の理解と受容であり、これにより行動の優先順位が決まる。データの完全性が損なわれるリスクは「ない」と信じている組織は、データライフサイクルに内在するリスクを十分に評価していない可能性が高い。したがって、データのライフサイクル、重要性及びリスクの評価に対するアプローチを詳細に検討する必要がある。これにより、査察の際に調査可能な潜在的な欠陥モードが示される可能性がある。

5.6 Data governance system review データガバナンスシステムのレビュー

5.6.1 The effectiveness of data integrity control measures should be assessed periodically as part of self-inspection (internal audit) or other periodic review processes. This should ensure that controls over the data lifecycle are operating as intended.

データ完全性の管理手段の有効性は、自己点検（内部監査）またはその他の定期的なレビュープロセスの一環として定期的に評価されるべきである。これにより、データのライフサイクルわたっての管理が、意図したとおりに機能していることを確認すべきである。

5.6.2 In addition to routine data verification checks (e.g. daily, batch- or activity- related), self-inspection activities should be extended to a wider review of control measures, including:

日常的なデータ検証チェック（毎日、バッチ毎、または活動に関連づけて）に加えて、自己点検活動は以下のような管理方法の広範なレビューにまで拡張するべきである：

- A check of continued personnel understanding of good data management practice in the context of protecting of the patient, and ensuring the maintenance of a working environment which is focussed on quality and open reporting of issues (e.g. by review of continued training in good data management principles and expectations).

患者を保護するという観点から、適正データマネジメント規範を職員が継続的に理解しているかのチェック。そして、品質とその問題のオープンな報告に焦点を当てた作業環境を、確実に維持しているかどうかを確認する（例えば、継続的な適正データマネジ



ントの原則をレビューすることによって行う) ;

- A review for consistency of reported data/outcomes against raw entries.

報告されたデータ／結果と生データの記録との整合性を確認すること。

This may review data not included during the routine data verification checks (where justified based on risk), and/or a sample of previously verified data to ensure the continued effectiveness of the routine process. ;

これは日常的なデータ確認のチェック中に含まれない（リスクに基づき、その論理的妥当性の説明がされている所の）データを、レビュー対象にする可能性があり、そして／または、ルーチンプロセスの継続的な有効性を保証するために以前に検証されたデータのサンプル（訳注：を用いての比較）を行う可能性がある。

- A risk-based sample of computerised system logs / audit trails to ensure that information of relevance to GMP/GDP activity is reported accurately. This is relevant to situations where routine computerised system data is reviewed manually or by a validated 'exception report'⁴. ;

GMP/GDP活動に関連する情報が正確に報告されていることを確認するために、コンピュータ化システムのログ／監査証跡（audit trails）のリスクベースのサンプル。これは、ルーチンのコンピュータシステムデータを手動でレビューする場合や、バリデート済みの「例外報告書」（exception report）によってレビューする場合に関連する⁴。

- 4** An 'exception report' is a validated search tool that identifies and documents predetermined 'abnormal' data or actions, which requires further attention or investigation by the data reviewer.

「例外レポート」（exception report）とは、事前に設定した「異常」（'abnormal'）なデータやアクションを特定し、それを文書化するためのバリデートされた調査ツール（validated search tool）であり、データのレビュー担当者が、さらなる注意を向けたり、調査を必要としたりするものである。

（訳注）：IT用語として「例外処理」（exception handling）という用語があり、この報告書のことであろう。

詳細は下記サイト参照のこと（2021.08.03アクセス）

<https://e-words.jp/w/%E4%BE%8B%E5%A4%96%E5%87%A6%E7%90%86.html>

- A review of quality system metrics (i.e. trending) that may also be indicators of data governance effectiveness. ;

データガバナンスの有効性の指標となる可能性をもつ品質システムの計量化指標（quality system metrics）のレビュー（例：トレンドニング：訳注 通常はトレンドグラフ化して管理）。

5.6.3 An effective review of the data governance system will demonstrate understanding regarding importance of interaction of company behaviours with organisational and technical controls. The outcome of the review should be communicated to senior



management, and be used in the assessment of residual data integrity risk.

データガバナンスシステムの効果的なレビューは、組織的及び技術的な管理をもつての「企業の行動との相互作用の重要性に関する理解」を示すものとなる。レビューの結果は、上級管理者に伝えて、残存するデータ完全性のリスクの評価に使用されるべきである。

6. ORGANISATIONAL INFLUENCES ON SUCCESSFUL DATA INTEGRITY MANAGEMENT データ完全性のマネジメントの成功への組織の影響

6.1 General 一般的事項

6.1.1 It may not be appropriate or possible to report an inspection deficiency relating to organisational behaviour. An understanding of how behaviour influences (i) the incentive to amend, delete or falsify data and (ii) the effectiveness of procedural controls designed to ensure data integrity, can provide the inspector with useful indicators of risk which can be investigated further.

組織上の動態（organisational behaviour）に関する査察で見られた欠陥（inspection deficiency）を告げることは、適切ではないか、または可能ではない場合がある。次の事についての影響が、その企業どの様な行動をとらせたかを理解することは、査察官に更なる調査が出来るリスクの有用な指標を提供するものである：

(i) データの修正、削除又は改ざんを行う動機；

(ii) データの完全性を確保するために設計された手続き上の管理の有効性にどのような影響を与えるか。

6.1.2 Inspectors should be sensitive to the influence of culture on organisational behaviour, and apply the principles described in this section of the guidance in an appropriate way. An effective ‘quality culture’ and data governance may be different in its implementation from one location to another. However, where it is apparent that cultural approaches have led to data integrity concerns; these concerns should be effectively and objectively reported by the inspector to the organisation for rectification.

査察官は、組織の動態（organisational behaviour）に関して文化（訳注：企業文化）の影響に対して感度を高く（sensitive）すべきであって、ガイダンスのこのセクションに記載されている原則を適切に応用する必要がある。効果的な「品質文化」（quality culture）とデータガバナンスは、場所によって（訳注：事業者ごとに）その実施方法が異なる場合がある。しかし、文化的なアプローチ（cultural approaches）が、データ完全性の懸念につながっていることが明らかな場合、これらの懸念は、その是正（rectification）のために、査察官からその組織に効果的かつ客観的に報告するべきである。



6.1.3 Depending on culture, an organisation's control measures may be:

企業文化に応じて、組織の管理手段は以下のようなになるであろう：

- 'open' (where hierarchy can be challenged by subordinates, and full reporting of a systemic or individual failure is a business expectation)
「オープン」（上下関係（hierarchy）に係りなく異議を述べることができ、組織的または個人的な失敗を完全に報告することがビジネス上で期待される場合）
- 'closed' (where reporting failure or challenging a hierarchy is culturally more difficult)
「クローズド」（失敗の報告や、上下関係を越えて異議を唱えることが文化的により困難である場合）

6.1.4 Good data governance in 'open' cultures may be facilitated by employee empowerment to identify and report issues through the Pharmaceutical Quality System. In 'closed' cultures, a greater emphasis on oversight and secondary review may be required to achieve an equivalent level of control due to the social barrier of communicating undesirable information. The availability of a confidential escalation process to senior management may also be of greater importance in this situation, and these arrangements should clearly demonstrate that reporting is actively supported and encouraged by senior management.

「開かれた」文化での適正なデータガバナンスは、医薬品品質システム（PQS）を通じて従業員が問題を特定し報告する権限を持つことで、促進されるかもしれない。「閉鎖的」な文化（'closed' cultures）では、望ましくない情報を伝えることが社会的障壁（social barrier）となるため、同等の管理レベルを達成するためには、監視と二次レビューを、より重視することが必要となる可能性がある。このような状況では、上級管理者への機密の上申プロセスを利用できることがより重要をもち、これらの取り決めは、報告が上級管理者によって積極的に支援され、奨励されていることを、明確に証明すべきである。

6.1.5 The extent of Management's knowledge and understanding of data integrity can influence the organisation's success of data integrity management. Management should know their legal and moral obligation (i.e. duty and power) to prevent data integrity lapses from occurring and to detect them, if they should occur. Management should have sufficient visibility and understanding of data integrity risks for paper and computerised (both hybrid and electronic) work flows.

データ完全性に関する経営陣の知識（Management's knowledge）と理解の程度は、当該組織のデータ完全性マネジメントの成功に影響を与える。経営陣は、データ完全性の喪失の発生を防ぎ、万一発生した場合にはそれを検知するという、法的および道徳的な義務（すなわち義務と権限）を知っておくべきである。経営者は、紙とコンピュータ（ハイブリッドと電子の両方）の業務フローについて、データ完全性のリスクを十分に可視化し、理解する必要がある。



6.1.6 Lapses in data integrity are not limited to fraud or falsification; they can be unintentional and still pose risk. Any potential for compromising the reliability of data is a risk that should be identified and understood in order for appropriate controls to be put in place (refer sections 5.3 - 5.5). Direct controls usually take the form of written policies and procedures, but indirect influences on employee behaviour (such as undue pressure, incentives for productivity in excess of process capability, opportunities for compromising data and employee rationalisation of negative behaviours) should be understood and addressed as well.

データの完全性の欠落は、不正 (fraud) や改ざん (falsification) に限らない ; 意図しないものであってもリスクとなる。データの信頼性が損なわれる可能性は、適切な管理を実施するためにそれを特定し、理解をすべきリスクである (5.3~5.5項を参照)。直接的な管理は通常、文書化された方針と手順の形をとるが、従業員の行動に対する間接的な影響 (不当な圧力 (undue pressure))、プロセス能力を超える生産性への誘因 (incentives for productivity in excess of process capability)、データの危険化の機会 (opportunities for compromising data)、否定的な行動の従業員による正当化 (employee rationalisation of negative behaviours) など) についても理解し、同じように対処する必要がある。

6.1.7 Data integrity breaches can occur at any time, by any employee, so management needs to be vigilant in detecting issues and understand reasons behind lapses, when found, to enable investigation of the issue and implementation of corrective and preventive actions.

データ完全性の綻びは、いつでも、どのような従業員でも発生する可能性がある。そのため、経営陣は、問題を検知するための注意を怠らず、問題が見つかった場合にはその理由を理解し、問題の調査と是正・予防措置の実施を可能にする必要がある。

6.1.8 There are consequences of data integrity lapses that affect the various stakeholders (patients, regulators, customers) including directly impacting patient safety and undermining confidence in the organisation and its products. Employee awareness and understanding of these consequences can be helpful in fostering an environment in which quality is a priority.

データ完全性の喪失が発生することは、様々な利害関係者 (患者、規制当局、顧客) に影響を与える。これには、患者安全性に対する直接的なインパクトを与えるのみならず、組織とその製品に対する信頼性の喪失も含まれる。これらの結末についての従業員の自覚と理解は、品質を最優先する所の環境を醸成させることに役立つ。

6.1.9 Management should establish controls to prevent, detect, assess and correct data integrity breaches, as well as verify those controls are performing as intended to assure data integrity. Sections 6.2 to 6.7 outline the key items that Management should address to achieve success with data integrity.



経営陣は、データの完全性に関する違反を防止し、検出し、評価し、そして是正するための管理を確立すべきである。もちろん、それらの管理がデータの完全性を保証するために意図されたとおりに機能していることを確認することも含まれる。Sections 6.2から6.7では、経営陣がデータ完全性を成功させるために、取り組むべき重要事項を概説している。

6.1.10 Senior Management should have an appropriate level of understanding and commitment to effective data governance practices including the necessity for a combination of appropriate organisational culture and behaviours (section 6) and an understanding of data criticality, data risk and data lifecycle. There should also be evidence of communication of expectations to personnel at all levels within the organisation in a manner which ensures empowerment to report failures and opportunities for improvement. This reduces the incentive to falsify, alter or delete data.

上級経営陣は、次の点について適切なレベルでの理解とコミットメントを持つべきである：

- (1) 効果的なデータガバナンスについての理解とコミットメント。
これには、適切な組織文化及び行動（セクション6）が含まれる；
- (2) データの重要性、データのリスク、及びデータライフサイクルの理解。

また、失敗や改善の機会を報告する権限を保証する方法で、組織内のすべてのレベルの担当者に期待事項を伝えている証拠が存在するべきである。これにより、データを改ざん、変更、または削除する動機が減少する。

6.2 Policies related to organisational values, quality, staff conduct and ethics

組織の価値観、品質、スタッフの行動および倫理に関する方針

6.2.1 Appropriate expectations for staff conduct, commitment to quality, organisational values and ethics should clearly communicated throughout the organisation and policies should be available to support the implementation and maintenance of an appropriate quality culture. Policies should reflect Management's philosophy on quality, and should be written with the intent of developing an environment of trust, where all individuals are responsible and accountable for ensuring patient safety and product quality.

スタッフの行動、品質へのコミットメント(強い意志をもった誓約)、組織の価値、及び倫理(ethics)に対する適切な期待は、組織全体に明確に伝えられるべきであり、適切な品質文化の実施及び維持を支援するための方針が、利用可能であるべきである。その方針は、品質に関する経営者の哲学を反映し、すべての職員が患者の安全と製品の品質を確保することに責任と責任を持ち、信頼の環境を構築する意図で書かれるべきである。

6.2.2 Management should make personnel aware of the importance of their role in ensuring data quality and the implication of their activities to assuring product quality and

protecting patient safety.

経営陣は、データの質を確保する上での自分の役割の重要性、および製品の品質を保証し患者の安全を守る上での自分の活動の意味を、各人に認識させるべきである。

- 6.2.3 Policies should clearly define the expectation of ethical behaviour, such as honesty. This should be communicated to and be well understood by all personnel. The communication should not be limited only to knowing the requirements, but also why they were established and the consequences of failing to fulfil the requirements.

方針は、正直さなどの倫理的行動の期待値を明確に定義すべきである。これは、すべての職員に伝えられ、よく理解されるべきである。このコミュニケーションは、要求事項を知ることだけにとどまらず、なぜその要求事項が設定されたのか、要求事項を満たせなかった場合はどうなるかの結果も含めて行われるべきである。

- 6.2.4 Unwanted behaviours, such as deliberate data falsification, unauthorised changes, destruction of data, or other conduct that compromises data quality should be addressed promptly. Examples of unwanted behaviours and attitudes should be documented in the company policies. Actions to be taken in response to unwanted behaviours should be documented. However, care should be taken to ensure that actions taken, (such as disciplinary actions) do not impede any subsequent investigation into the data integrity issues identified, e.g. severe retribution may prevent other staff members from disclosing information of value to the investigation.

意図的なデータの改ざん (deliberate data falsification)、不正な変更 (unauthorised changes)、データの破壊、またはその他のデータの品質を損なうような望ましくない行動は、速やかに対処する必要がある。望ましくない行動や態度の例は、会社の方針に文書化をするべきである。ただし（懲戒処分などの）措置が、特定されたデータの完全性の問題に関するその後の調査を妨げないように注意する必要がある。例えば、厳しい懲罰は、他のスタッフが調査に価値のある情報を開示するのを妨げる可能性がある。

- 6.2.5 The display of behaviours that conform to good practices for data management and integrity should be actively encouraged and recognised appropriately.

データのマネジメント及び完全性に関する適正な実践にかなった行動を示すことは、積極的に奨励され、そして適切に評価されるべきである。

- 6.2.6 There should be a confidential escalation program supported by company policies and procedures whereby it encourages personnel to bring instances of possible breaches of policies to the attention of senior management without consequence for the informer/employee. The potential for breaches of the policies by senior management should be recognised and a suitable reporting mechanism for those cases should be available.



企業のポリシーおよび手順に裏付けられた部外秘のエスカレーションプログラム（訳注：上申して行く手続文書）が存在するべきである。これにより、情報提供者／職員に影響を与えることなく、ポリシー違反の可能性がある事例を上級管理者に知らせることを従業員に奨励するべきである。上級管理者によるポリシー違反の可能性を認識し、そのような事例のための適切な報告メカニズムを利用可能にすべきである。

6.2.3 Where possible, management should implement systems with controls that by default, uphold the intent and requirements of company policies.

可能であれば、経営陣はデフォルト（訳注：規定済の方針として）で、企業の方針の意図と要件を維持する管理を備えたシステムを、導入すべきである。

6.2.4 Unwanted behaviours, such as deliberate data falsification, unauthorised changes, destruction of data, or other conduct that compromises data quality should be addressed promptly. Examples of unwanted behaviours and attitudes should be documented in the company policies. Actions to be taken in response to unwanted behaviours should be documented. However, care should be taken to ensure that actions taken, (such as disciplinary actions) do not impede any subsequent investigation into the data integrity issues identified, e.g. severe retribution may prevent other staff members from disclosing information of value to the investigation.

意図的なデータの改ざん（deliberate data falsification）、不正な変更（unauthorised changes）、データの破壊（destruction of data）など、データの品質を損なうような望ましくない行動には、速やかに対処する必要がある。望ましくない行動や態度の事例は、会社の方針の中に文書化を行うべきである。望ましくない行動に対応するための措置は、これを文書化する必要がある。ただし、とられる（懲戒処分などの）措置が、特定されたデータの完全性の問題に関するその後の調査を妨げないように注意する必要がある。例えば、厳しい懲罰により、他のスタッフが調査に価値のある情報の開示を妨げる可能性がある。

6.2.5 The display of behaviours that conform to good practices for data management and integrity should be actively encouraged and recognised appropriately.

「データマネジメントと完全性に関する適正な規範（good practices）に適合した行動をとる」べきことを指し示し、適切に認識をさせるべきである。

6.2.6 There should be a confidential escalation program supported by company policies and procedures whereby it encourages personnel to bring instances of possible breaches of policies to the attention of senior management without consequence for the informer/employee. The potential for breaches of the policies by senior management should be recognised and a suitable reporting mechanism for those cases should be available.

会社の方針と手順に支えられた秘密のエスカレーションプログラム（訳注参照）が存在すべき

である。これにより、情報提供者／従業員に影響を与えることなく、方針違反の可能性がある事例を上級管理者に知らせることを、従業員に奨励することができる。上級管理者（senior management）によるポリシー違反の可能性は認識しておくべきであり、そのような場合のための適切な報告メカニズムを用意しておくべきである。

訳注：ここで使用している“escalation program”とは、ITの分野の用語ではなく、それに準じた意味で、使用していると思われる。ネットの記載によれば、次の通りである。；ITの分野では、「より大きな範囲に対象を広げること」「発生した問題などに対処できず、より上位の存在に対応を要請すること」という意味で用いられることが多い。

6.2.7 Where possible, management should implement systems with controls that by default, uphold the intent and requirements of company policies.

可能であれば経営陣は、デフォルト（訳注：初期設定として既にもっている機能）で、企業ポリシーの意図と要件を維持する所の管理を備えたシステムを導入すべきである。

6.3 Quality culture 品質文化

6.3.1 Management should aim to create a work environment (i.e. quality culture) that is transparent and open, one in which personnel are encouraged to freely communicate failures and mistakes, including potential data reliability issues, so that corrective and preventive actions can be taken. Organisational reporting structure should permit the information flow between personnel at all levels.

経営陣は、透明でオープンな職場環境（すなわち品質文化）の構築を目指すべきであり、これは職員の失敗やミスを自由に伝えることが奨励されるようなものであり、これにはデータの信頼性に関する潜在的な問題も含まれる。そのようにして、是正措置および予防措置を講じることが可能なようにするべきである。組織の報告を行う体制は、あらゆるレベルの職員間の情報の流れを可能にすべきである。

6.3.2 It is the collection of values, beliefs, thinking, and behaviours demonstrated consistently by management, team leaders, quality personnel and all personnel that contribute to creating a quality culture to assure data quality and integrity.

品質文化とは、データの品質及び完全性を保証するために、品質文化の創造に貢献する、経営陣、チームリーダー、品質担当職員、及び全ての担当が一貫して示される価値観（values）、信念（beliefs）、考え方（thinking）、及び行動（behaviours）の集合体である。

6.3.3 Management can foster quality culture by:

経営陣は以下の方法で品質文化を醸成することができる：

- Ensuring awareness and understanding of expectations (e.g. Code of Values and Ethics and Code of Conduct),

期待される事項（価値観・倫理規範、行動規範など）の認識と理解を確保すること。

- Leading by example, management should demonstrate the behaviours they expect to see,
模範を示すことで、経営陣は期待する行動を示すべきである；
- Being accountable for actions and decisions, particularly delegated activities, ;
行動と決定に責任を持つこと。特に委任された活動に責任を持つ；
- Staying continuously and actively involved in the operations of the business,
事業運営に継続的、かつ積極的に関与する；
- Setting realistic expectations, considering the limitations that place pressures on employees, ;
従業員にプレッシャーを与えることの限界を回避し、現実的な期待値を設定する；
- Allocating appropriate technical and personnel resources to meet operational requirements and expectations, ;
業務上の要求と期待に応えるために、適切な技術的および人的資源を割り当てる；
- Implementing fair and just consequences and rewards that promote good cultural attitudes towards ensuring data integrity, and
データの完全性を確保するために、適正な文化的姿勢を促進させる所の公平で公正な結果（fair and just consequences）と恩恵（rewards）を導入する；
- Being aware of regulatory trends to apply “lessons learned” to the organisation.
組織に「学んだ教訓」（“lessons learned”）を適用するために、規制の動向を認識し続ける。

6.4 Modernising the Pharmaceutical Quality System 医薬品品質システムの近代化

6.4.1 The application of modern quality risk management principles and good data management practices to the current Pharmaceutical Quality System serves to modernize the system to meet the challenges that come with the generation of complex data.

現在の医薬品品質システム（Pharmaceutical Quality System : PQS）に、最新の品質リスクマネジメントの原則と、優れたデータマネジメントの手法を適用することは、複雑なデータの生成に伴う課題に対応するシステムの近代化を図ることに役立つ。

6.4.2 The company’s Pharmaceutical Quality System should be able to prevent, detect and correct weaknesses in the system or their processes that may lead to data integrity lapses. The company should know their data life cycle and integrate the appropriate controls and procedures such that the data generated will be valid, complete and reliable. Specifically,



such control and procedural changes may be in the following areas:

企業の医薬品品質システムは、データの完全性の喪失につながる可能性のあるシステムまたはそのプロセスの弱点を防止し、検出し、修正を可能とすべきである。企業は、データのライフサイクルを把握し、生成されるデータが有効かつ完全で信頼性のあるものとなるように、適切なコントロールと手順を統合すべきである。具体的には、このような管理や手順の変更は、以下の分野で行われる可能性がある：

- Quality Risk Management, 品質リスクマネジメント；
- Investigation programs, 調査プログラム；
- Data review practices (section 9), データ照査の規範（第9項）；
- Computerised system validation, コンピュータ化システムバリデーション；
- IT infrastructure, services and security (physical and virtual),
ITインフラ、サービス、セキュリティ（物理的および仮想的なもの）；
- Vendor/contractor management, ベンダー・委託先の業者のマネジメント；
- Training program to include company's approach to data governance and data governance SOPs,
データガバナンスと、データガバナンスSOPsに対する企業のアプローチを含む研修プログラム；
- Storage, processing, transfer and retrieval of completed records, including decentralised/cloud-based data storage, processing and transfer activities,
完了した記録の保管・処理・転送・検索。これには分散型（decentralised）／クラウド型（cloud-based）のデータ保管・処理・転送活動を含む；
- Appropriate oversight of the purchase of GMP/GDP critical equipment and IT infrastructure that incorporate requirements designed to meet data integrity expectations, e.g. User Requirement Specifications, (Refer section 9.2)
データの完全性に関する期待を満たすように設計された要件（例えば、ユーザ要求仕様書）を組み込んだ GMP/GDP の重要機器および IT インフラ（infrastructure）の購入を適切に監視すること（9.2 項参照）；
- Self-inspection program to include data quality and integrity, and
データの品質と完全性を含む自己点検プログラム； および
- Performance indicators (quality metrics) and reporting to senior management.
パフォーマンス指標（品質メトリクス：品質計量化指標）と上級経営陣への報告。



6.5 Regular management review of performance indicators (including quality metrics)

パフォーマンス指標（品質メトリクス：品質計量化指標を含む）の定期的なマネジメント・レビュー

6.5.1 There should be regular management reviews of performance indicators, including those related to data integrity, such that significant issues are identified, escalated and addressed in a timely manner. Caution should be taken when key performance indicators are selected so as not to inadvertently result in a culture in which data integrity is lower in priority.

パフォーマンス指標（performance indicators）の定期的なマネジメントレビューを行うべきである。これには、データ完全性に係る重要な問題が特定され、タイムリーに段階的に対応レベルが高められ、かつ対応するようにすべきである。重要なパフォーマンス指標（key performance indicators）を選定する場合には注意を要する。それは、データの完全性は、その優先順位が低いという文化を不用意に生まないようにすべきである。

6.5.2 The head of the Quality unit should have direct access to senior management in order to directly communicate risks so that senior management is aware and can allocate resources to address any issues.

品質部門（the Quality unit）の責任者は、リスクを直接伝えるために上級経営陣への直接アクセス権を持つべきであって、それによって、上級経営陣が問題を認識し、問題に対処するためにリソースを割り当てることができるようにする。

6.5.3 Management can have an independent expert periodically verify the effectiveness of their systems and controls.

経営陣は、そのシステムと管理の有効性を、独立した専門家に定期的に検証してもらうことが出来る。

6.6 Resource allocation 資源の配分

6.6.1 Management should allocate appropriate resources to support and sustain good data integrity management such that the workload and pressures on those responsible for data generation and record keeping do not increase the likelihood of errors or the opportunity to deliberately compromise data integrity.

経営陣は、適正なデータ完全性マネジメントを支援し、そして維持するために、適切な資源を割り当てべきである。これにより、データ生成および記録保持を担当する職員の作業量やプレッシャーが、エラーの可能性やデータの完全性を意図的に損なう機会を、増大させないようにする。



6.6.2 There should be sufficient number of personnel for quality and management oversight, IT support, conduct of investigations, and management of training programs that are commensurate with the operations of the organisation.

品質及び管理の監督、ITサポート、調査の実施、研修プログラムのマネジメントのために、当該組織の運営に見合った十分な数の人員を配置するべきである。

6.6.3 There should be provisions to purchase equipment, software and hardware that are appropriate for their needs, based on the criticality of the data in question. Companies should implement technical solutions that improve compliance with ALCOA+⁵ principles and thus mitigate weaknesses in relation to data quality and integrity.

問題となっているデータの重要性に基づいて、そのニーズに適した機器、ソフトウェア、ハードウェアを購入するための規定を持つべきである。企業は、ALCOA+⁵の原則への準拠を向上させ、それによってデータの品質と完全性に関連する弱点を緩和する技術的解決手段を導入すべきである。

⁵ : EMA guidance for GCP inspections conducted in the context of the Centralised Procedure

Centralised Procedure（中央審査方式）方式で行われるGCP査察のためのEMAガイダンス

6.6.4 Personnel should be qualified and trained for their specific duties, with appropriate segregation of duties, including the importance of good documentation practices (GdocPs). There should be evidence of the effectiveness of training on critical procedures, such as electronic data review. The concept of good data management practices applies to all functional departments that play a role in GMP/GDP, including areas such as IT and engineering.

職員は、適切に職務の分離を行い、それぞれの職務に応じた資格と訓練を受けるべきである。これには、これには適正文書化規範（GdocPs）の重要性も含まれる。また、電子データのレビュー（electronic data review）などの重要な手順に関する訓練の有効性を示す証拠が必要である。適正なデータマネジメント規範の概念は、ITやエンジニアリングなどの分野を含め、GMP/GDPにおいてその役割を果たしている、全ての機能を果たしている部門に適用される。

6.6.5 Data quality and integrity should be familiar to all, but data quality experts from various levels (SMEs, supervisors, team leaders) may be called upon to work together to conduct/support investigations, identify system gaps and drive implementation of improvements.

データの品質と整合性は、誰もが慣れ親しむべきであるが、様々なレベルのデータ品質専門家（SME、監督者、チームリーダー）が協力して調査を実施／支援し、システム上のギャップを特定し、改善策の実施を推進することが求められる場合がある。

6.6.6 Introduction of new roles in an organisation relating to good data management such as a



data custodian might be considered.

データ管理者（data custodian：訳注参照）のような、適正データマネジメントに関連する組織の新しい役割の導入が、検討されるかもしれない。

訳注（ネットよりの引用）：[データ管理者（data custodian）とは、データが保護を目的としたタスクを日々完了できるように操作する者である。](#)

6.7 Dealing with data integrity issues found internally

組織内部で発見されたデータ完全性問題への対処

6.7.1 In the event that data integrity lapses are found, they should be handled as any deviation would be according to the Pharmaceutical Quality System. It is important to determine the extent of the problem as well as its root cause, then correcting the issue to its full extent and implement preventive measures. This may include the use of a third party for additional expertise or perspective, which may involve a gap assessment to identify weaknesses in the system.

データ完全性の欠落が発見された場合は、医薬品品質システム（PQS）に従って、逸脱と同様に対処する。根本原因は勿論のことであるが、その問題の範囲を特定することが重要である。次に、その問題の全範囲に対して是正を行い（correcting）、予防措置を講じる。これには、追加の専門知識や見解を得るために、第三者を利用することも含まれ、システムの弱点を特定するためにギャップ評価（gap assessment）を行うこともある。

6.7.2 When considering the impact on patient safety and product quality, any conclusions drawn should be supported by sound scientific evidence.

患者への安全性や製品の品質への影響を考慮する場合、導き出された結論は、妥当な科学的証拠（sound scientific evidence）によって裏付けられるべきである。

6.7.3 Corrections may include product recall, client notification and reporting to regulatory authorities. Corrections and corrective action plans and their implementation should be recorded and monitored.

是正は、製品の回収、顧客への通知及び規制当局への報告が含まれる場合がある。是正と是正措置計画、及びその実施状況は記録し、モニターする必要がある。

6.7.4 Further guidance may be found in section 12 of this guide.

更なるガイダンスは、このガイドのSection 12 に述べられている。



7. GENERAL DATA INTEGRITY PRINCIPLES AND ENABLERS

一般的なデータ完全性の原則と実現化

- 7.1 The Pharmaceutical Quality System should be implemented throughout the different stages of the life cycle of the APIs and medicinal products and should encourage the use of science and risk-based approaches.

医薬品品質システム（PQS）は、原薬及び医薬品のライフサイクルの様々な段階を通じて実施されるべきであり、科学的及びリスクベースのアプローチの使用を奨励すべきである。

- 7.2 To ensure that decision making is well informed and to verify that the information is reliable, the events or actions that informed those decisions should be well documented. As such, Good Documentation Practices are key to ensuring data integrity, and a fundamental part of a well-designed Pharmaceutical Quality System (discussed in section 6).

意思決定十分な情報に基づくことを保証し、その情報が信頼できることを確認するために、それらの意思決定に影響を与えた事象（events）又は行為（actions）は、十分に文書化されるべきである。そのため、適正文書化規範（Good Documentation Practices : GdocPs）は、データの完全性を確保するための鍵であり、適切に設計された医薬品品質システム（Section 6で議論）の基本的な部分である。

- 7.3 The application of GdocPs may vary depending on the medium used to record the data (i.e. physical vs. electronic records), but the principles are applicable to both. This section will introduce those key principles and following sections (8 & 9) will explore these principles relative to documentation in both paper-based and electronic-based recordkeeping.

GdocPs の適用は、データを記録する媒体（物理的な記録と電子的な記録）によって異なるが、その原則はどちらにも適用できる。このセクションでは、これらの重要な原則を紹介し、次のセクション（8 と 9）では、紙ベースと電子ベースの両方の記録管理における文書化に関連して、これらの原則を探る。

- 7.4 Some key concepts of GdocPs are summarised by the acronym ALCOA: Attributable, Legible, Contemporaneous, Original, And Accurate. The following attributes can be added to the list: Complete, Consistent, Enduring and Available (ALCOA+⁶). Together, these expectations ensure that events are properly documented and the data can be used to support informed decisions.

GdocPs のいくつかの重要な概念は、ALCOA という頭字語（acronym）でまとめられている：これは、帰属性（Attributable）、判読性（Legible）、同時性（Contemporaneous）、原本性（Original）及び正確性（Accurate）である。これに次のような属性を加えることができる：完全性（Complete）、一貫性（Consistent）、耐久性／普遍性（Enduring）及び要時取出し可能性



(Available when needed) である。つまり「ALCOA+」⁶である。これらの期待事項を組み合わせることで、事象が適切に文書化され、そのデータは、行われた決定裏付けのために、使用することが出来る。

⁶ EMA guidance for GCP inspections conducted in the context of the Centralised Procedure
EMAによる中央審査方式で実施されるGCP査察のガイダンス

7.5 Basic data integrity principles applicable to both paper and electronic systems (i.e. ALCOA +):

紙 及び 電子のシステムの両方に適用可能な、基本的なデータ完全性の原則：

| Data Integrity Attribute データ完全性の属性 | Requirement 要求内容 |
|---------------------------------------|---|
| Attributable 帰属性 | <p>It should be possible to identify the individual or computerised system that performed a recorded task and when the task was performed. This also applies to any changes made to records, such as corrections, deletions, and changes where it is important to know who made a change, when, and why.</p> <p>記録されたタスクを実行した個人またはコンピュータ化システムと、そのタスクが、いつ実行されたかを特定可能にすべきである。これはまた、「誰が、何時、何のために変更を行ったか」を知ることが重要である、「修正」、「削除」、「変更」などの、記録に加えられた変更にも適用される。</p> |
| Legible 判読性 | <p>All records should be legible – the information should be readable and unambiguous in order for it to be understandable and of use. This applies to all information that would be required to be considered Complete, including all Original records or entries. Where the ‘dynamic’ nature of electronic data (the ability to search, query, trend, etc.) is important to the content and meaning of the record, the ability to interact with the data using a suitable application is important to the ‘availability’ of the record.</p> <p>すべての記録は読みやすくなければならない。－ 情報を理解し、それを利用するためには、読みやすく、明確なものとすべきである。これは、これは、Original (オリジナル) の記録またはエントリー (entries: 訳注 入力) を含め、「完全 (Complete)」とみなされるために必要な、すべての情報に適用される。電子データの「動的 (‘dynamic’)」な性質 (検索 (search)、照会 (query)、傾向分析 (trend) などの機能) が記録の内容と意味にとって重要である場合、適切なアプリケーションを使用してデータと対話できることが記録の「利用可能性 (‘availability’)」にとって重要である。</p> |



| Data IntegrityAttribute データ完全性の属性 | Requirement 要求内容 |
|--------------------------------------|---|
| Contemporaneous 同時性 | <p>The evidence of actions, events or decisions should be recorded as they take place. This documentation should serve as an accurate attestation of what was done, or what was decided and why, i.e. what influenced the decision at that time.</p> <p>行動 (actions)、出来事 (events) あるいは決定 (decisions) の証拠は、それらが行われた時に記録されるべきである。この文書は、何が行われたか、何が決定されたか、そしてその理由、すなわちその時の決定に何が影響したかを正確に証明するものとするべきである。</p> |
| Original 原本性 | <p>The original record can be described as the first-capture of information, whether recorded on paper (static) or electronically (usually dynamic, depending on the complexity of the system). Information that is originally captured in a dynamic state should remain available in that state.</p> <p>オリジナルの記録は、紙に記録されているか（静的）、電子的に記録されているか（システムの複雑さにもよるが、通常は動的）を問わず、情報の最初の取得（first-capture of information）と表現することができる。動的な状態で最初に取得された情報は、その状態で利用可能でなければならない。</p> |
| Accurate 正確性 | <p>Records need to be a truthful representation of facts to be accurate. Ensuring records are accurate is achieved through many elements of a robust Pharmaceutical Quality System. This can be comprised of:</p> <p>記録は、正確であるためには、事実を正確に表現している必要がある。記録が正確であることは、堅牢な医薬品品質システムの多くの要素を通して達成される。これは、次のようなものからなっている。：</p> <ul style="list-style-type: none"> • equipment related factors such as qualification, calibration, maintenance and computer validation. <p>機器関連の要素。例えば適格性評価、校正、保全、及びコンピュータバリデーション；</p> <ul style="list-style-type: none"> • policies and procedures to control actions and behaviours, including data review procedures to verify adherence to procedural requirements； <p>行動および行為を管理するための方針および手順。これには、手続き上の要求事項の遵守を検証するためのデータレビュー手順を含む；</p> <ul style="list-style-type: none"> • deviation management including root cause analysis, impact assessments and |



| Data IntegrityAttribute データ完全性の属性 | Requirement 要求内容 |
|--------------------------------------|---|
| | <p>CAPA</p> <p>逸脱に対するマネジメント。これには根本原因分析、インパクトアセスメント（訳注：ネガティブな影響に対する評価）、およびCAPA（是正措置・予防措置）</p> <ul style="list-style-type: none"> trained and qualified personnel who understand the importance of following established procedures and documenting their actions and decisions. <p>確立された手順に従い、その行動と決定を文書化することに理解をしている、訓練された、かつ適格性を評価された職員。</p> <p>Together, these elements aim to ensure the accuracy of information, including scientific data that is used to make critical decisions about the quality of products.</p> <p>全体として、これらの要素は、情報の正確性を確保することを目的としている。それには、製品の品質に関する重要な意思決定に使用する科学的データを含むものである。</p> |
| Complete 完全性 | <p>All information that would be critical to recreating an event is important when trying to understand the event. It is important that information is not lost or deleted. The level of detail required for an information set to be considered complete would depend on the criticality of the information (see section 5.4 Data criticality). A complete record of data generated electronically includes relevant metadata (see section 9).</p> <p>ある出来事を再現するために必須（critical）な全ての情報は、その出来事を理解しようとするときに重要である。情報が失われたり削除されたりしないことが重要である。情報セットが完全であるとみなされるために必要な詳細度のレベルは、その情報の重要性に依存する（Section 5.4のデータの重要性を参照）。電子的に生成されたデータの完全な記録には、関連するメタデータ（metadata）が含まれる（セクション9参照）。</p> |
| Consistent 一貫性 | <p>Information should be created, processed, and stored in a logical manner that has a defined consistency. This includes policies or procedures that help control or standardize data (e.g. chronological sequencing, date formats, units of measurement, approaches to rounding, significant digits, etc.).</p> <p>情報は、定義された一貫性を持つ論理的方法で作成し、処理し、保存すべきである。これには、データの管理や標準化に役立つポリシーや手順が含まれる（例：時系列の順序、日付のフォーマット、測定単位、丸め方のアプローチ、有効数字など）。</p> |



| Data Integrity Attribute データ完全性の属性 | Requirement 要求内容 |
|---------------------------------------|--|
| Enduring 耐久性／普遍性 | <p>Records should be kept in a manner such that they exist for the entire period during which they might be needed. This means they need to remain intact and accessible as an indelible/durable record throughout the record retention period.</p> <p>記録は、それが必要とされる可能性のある全期間にわたって存在するような方法で保管すべきである。これは、その記録保持期間中、消えない／耐久性のある記録（indelible /durable record）として、そのままの状態で、かつアクセス（訳注：取出しが可能な）できる必要があることを意味する。</p> |
| Available 要時取出し可能性 | <p>Records should be available for review at any time during the required retention period, accessible in a readable format to all applicable personnel who are responsible for their review whether for routine release decisions, investigations, trending, annual reports, audits or inspections.</p> <p>記録は、必要とされる保存期間中、いつでも閲覧できて、該当する全ての該当する職員が読み易い書式でアクセスできるようにしておかなければならない。ここで、「該当する職員」とは、日常的な出荷判定、調査、トレンドの監視、年次報告、監査あるいは査察などのレビューに関係する職員である。</p> |

7.6 If these elements are appropriately applied to all applicable areas of GMP and GDP related activities, along with other supporting elements of a Pharmaceutical Quality System, the reliability of the information used to make critical decisions regarding drug products should be adequately assured.

もしこれらの要素が、GMPおよびGDPに関連する活動のすべての領域に適切に適用され、医薬品品質システムの他の支援要素と共に適用されるならば、医薬品に関する重要な決定を行うための情報の信頼性は、十分に保証されるはずである。

7.7 True copies 真正コピー

7.7.1 Copies of original paper records (e.g. analytical summary reports, validation reports, etc.) are generally very useful for communication purposes, e.g. between companies operating at different locations. These records should be controlled during their life cycle to ensure that the data received from another site (sister company, contractor, etc.) are maintained as “true copies” where appropriate, or used as a “summary report” where the requirements of a “true copy” are not met (e.g. summary of complex analytical data).

オリジナルの紙の記録（例：分析要約報告書、バリデーションレポートなど）のコピーは、

一般的に例えば、異なる場所で活動する企業間などのコミュニケーション目的で非常に有用である。これらの記録は、別のサイト(site : 事業所) (姉妹会社、請負業者など) から受領したデータが、それが適切な場合は「真正コピー」 (“true copies”) として維持されるか、あるいは、「真正コピー」の要件が満たされない場合(複雑な分析データの要約報告書など) には、「要約レポート」 (“summary report”) として使用されることが、確実となるように、そのライフサイクルにわたって管理するべきである。

7.7.2 It is conceivable for raw data generated by electronic means to be retained in an acceptable paper or pdf format, where it can be justified that a static record maintains the integrity of the original data.

静的な記録 (static record) が、元のデータ (original data) の完全性を維持していることを正当化できる場合には、容認可能な「紙」や「pdf」の形式で保持することが考えられる。

However, the data retention process should record all data, (including metadata) for all activities which directly or indirectly impact on all aspects of the quality of medicinal products,(e.g. for records of analysis this may include: raw data, metadata, relevant audit trail and result files, software / system configuration settings specific to each analytical run, and all data processing runs (including methods and audit trails) necessary for reconstruction of a given raw data set).

しかしながら、データ保持プロセスでは、医薬品の品質のあらゆる側面に、直接または間接的に影響を与えるすべての活動に関するすべてのデータ (メタデータを含む) を記録しなければならない (例えば、分析の記録では、次のものが含まれるであろう : 原資 (生) データ、関連するメタデータ、関連する監査証跡とその結果ファイル (relevant audit trail and result files) 、各分析ラン (analytical run) 、及びあるデータセットの再構成に必要な全てのデータ処理ラン (方法および監査証跡を含む)) 。

It would also require a documented means to verify that the printed records were an accurate representation. This approach is likely to be onerous in its administration to enable a GMP/GDP compliant record.

また、印刷された記録が正確に表現されていることを検証するための、文書化された手段も必要となる。このアプローチは、GMP/GDPに準拠した記録を可能にするための管理において、負担が大きいと思われる。

7.7.3 Many electronic records are important to retain in their dynamic format, to enable interaction with the data. Data should be retained in a dynamic form where this is critical to its integrity or later verification. Risk management principles should be utilised to support and justify whether and how long data should be stored in a dynamic format.

多くの電子記録は、データとのインタラクション (相互の確認) を可能にするために、動的な形式で保持することが重要である。データの完全性や、後の検証が不可欠な場合は、デー

データを動的な形式で保持すべきである。データを動的形式で保存すべきかどうか、またどのくらいの期間保存すべきかを裏付け、正当化するために、リスクマネジメントの原則を利用すべきである。

7.7.4 At the receiving site, these records (true copies) may either be managed in a paper or electronic format (e.g., PDF) and should be controlled according to an approved QA procedure.

受領側のサイト（事業所）では、これらの記録（真正コピー）は、紙または電子フォーマット（PDFなど）のいずれかで管理され、承認されたQAの手順に従って管理される必要がある。

7.7.5 Care should be taken to ensure that documents are appropriately authenticated as “true copies” in a manner that allows the authenticity of the document to be readily verified, e.g. through the use of handwritten or electronic signatures or generated following a validated process for creating true copies.

文書の真正性（authenticity）を容易に検証できる方法、例えば、手書き署名または電子署名（handwritten or electronic signatures）の使用、または真正コピーを作成するための有効なプロセスに従って生成された文書は、「真正なコピー」として適切に認証されることが保証されるように、注意を払う必要がある。

| Item | How should the “true copy” be issued and controlled? 如何にして真正コピーを発行し、管理すべきか？ |
|------|---|
| 1. | <p>Creating a “true copy” of a paper document. 紙の文書の「真正コピー」（“true copy”）を作成する。</p> <p>At the company who issues the true copy: 真正コピーを発行する企業では：</p> <ul style="list-style-type: none"> - Obtain the original of the document to be copied コピーする文書の原本を入手する； - Photocopy the original document ensuring that no information from the original copy is lost; 原本の情報が失われないことを保証するために、原本を写真撮影する； - Verify the authenticity of the copied document and sign and date the new hardcopy as a “true copy”; コピーした文書の真正性(authenticity)を確認し、新たなハードコピーを「真正コピー」（“true copy”）として署名し、日付を記入する。 <p>The “True Copy” may now be sent to the intended recipient. その「真正コピー」を、このようにして、目的とする受領者に送信することができる。</p> <p>Creating a “true copy” of an electronic document. 電子文書の「真正コピー」の作成</p> |



| | |
|--|--|
| | <p>A 'true copy' of an electronic record should be created by electronic means (electronic file copy), including all required metadata. Creating pdf versions of electronic data should be prohibited, where there is the potential for loss of metadata.</p> <p>電子記録の「真正コピー」は、必要なメタデータをすべて含んだ電子的手段（電子ファイルコピー）で作成すべきである。メタデータが失われる可能性がある場合は、電子データのpdfバージョンを作成することは、禁止すべきである。</p> <p>The "True Copy" may now be sent to the intended recipient.</p> <p>「真正コピー」(True Copy)は、このようにして意図した受領者に送信することができる。</p> <p>A distribution list of all issued "true copies" (soft/hard) should be maintained.</p> <p>発行した全ての「真正コピー："True Copy"」(ソフト/ハード)の配布リストは、これを保持すべきである。</p> |
| | <p>Specific elements that should be checked when reviewing records:</p> <p>記録をレビューする際にチェックすべき具体的な要素。</p> <ul style="list-style-type: none"> • Verify the procedure for the generation of true copies, and ensure that the generation method is controlled appropriately. 真正コピーの作成手順を確認し、作成方法が適切に管理されていることを確認する。 • Check that true copies issued are identical (complete and accurate) to original records. Copied records should be checked against the original document records to make sure there is no tampering of the scanned image. 発行された真正コピーが原本の記録と同一（完全かつ正確）であることを確認する。複写された記録は、原本の文書記録と照合し、スキャン画像の改ざんがないことを確認する。 • Check that scanned or saved records are protected to ensure data integrity. スキャンまたはセーブした記録がデータ完全を保証しているように、保護されているかをチェックする。 • After scanning paper records and verifying creation of a 'true copy': 紙の記録をスキャンしたのち、「真正コピー」が作成されたことを確認する。 <ul style="list-style-type: none"> — Where true copies are generated for distribution purposes, e.g. to be sent to a client, the original documents from which the scanned images have been created should be retained for the respective retention periods by the record owner. <p>(訳者注：原文において、上記の二重線で示した部分が挿入されているが、これは、その前の文と同一の文章であり、原文作成の際の編集ミスと思われる。)</p> <p>真正コピーが配布目的で生成された場合、例えば、クライアントに送付する場合は、オリジナル文書（スキャンされてイメージが作成された元の文書）は、その記録のオーナーにより、当該保持期間を保持する必要がある。</p> — Where true copies are generated to aid document retention, it may be possible to retain the copy in place of the original records documents from which the scanned |

| | |
|----|--|
| | <p>images have been created.</p> <p>文書の保存を助けるために真正コピーを作成した場合、スキャンした元の記録文書の代わりに、当該真正コピーを保存することが可能な場合がある。</p> |
| | <p>At the company who receives the true copy:</p> <p>真正コピーを受け取った企業では：</p> <ul style="list-style-type: none"> - The paper version, scanned copy or electronic file should be reviewed and filed according to good document management practices. <p>紙の版、スキャンしたコピー、または電子ファイルは、適正な文書管理の慣行に従って確認し、ファイルする必要がある。</p> <p>The document should clearly indicate that it is a true copy and not an original record.</p> <p>文書は、それが原本の記録ではなく真正コピーであることを明確に示すべきである。</p> |
| 2. | <p>Specific elements that should be checked when reviewing records:</p> <p>記録をレビューする際に確認すべき具体的な要素：</p> <ul style="list-style-type: none"> • Check that received records are checked and retained appropriately. <p>受け取った記録がチェックされ、適切に保管されていることを確認する；</p> <ul style="list-style-type: none"> • A system should be in place to verify the authenticity of “true copies” <p>「真正コピー」の真偽を確認する仕組みがあること；</p> <p>e.g. through verification of the correct signatories.</p> <p>例えば、正しい署名者を確認するなどにより。</p> |

7.7.6 A quality agreement should be in place to address the responsibilities for the generation and transfer of “true copies” and data integrity controls. The system for the issuance and control of “true copies” should be audited by the contract giver and receiver to ensure the process is robust and meets data integrity principles.

「真正コピー」の生成及び転送およびデータ完全性の管理について、その責任に関する適切な品質合意書（quality agreement）が存在すべきである。「真正コピー」の発行及び管理のシステムは、堅牢であり、データ完全性の原則に合致していることを保証するために、委託および受託契約者（contract giver and receiver）により監査すべきである。

7.8 Limitations of remote review of summary reports

要約報告書の遠隔レビューの限界

7.8.1 The remote review of data within summary reports is a common necessity; however, the limitations of remote data review should be fully understood to enable adequate control of data integrity.

要約報告書内のデータの遠隔監査は、一般的に必要とされている；しかしながら、データ完全性の適切な管理を可能にすることに対する遠隔によるデータのレビューの限界は、十分に理解する必要がある。

7.8.2 Summary reports of data are often supplied between physically remote manufacturing sites, Market Authorisation Holders and other interested parties. However, it should be acknowledged that summary reports are essentially limited in their nature, in that critical supporting data and metadata are often not included and therefore original data cannot be reviewed.

データの要約報告書は、物理的に離れた場所にある製造施設、販売承認保持者、その他の関係者の間に提供されることが多い。しかし、要約報告書はその性質から、重要な裏付けデータやメタデータが含まれていないことが多いため、オリジナルのデータをレビューすることができないという点で、本質的に限定された性質のものであることを認識する必要がある。

7.8.3 It is therefore essential that summary reports are viewed as but one element of the process for the transfer of data and that interested parties and Inspectorates do not place sole reliance on summary report data.

それゆえに、要約報告書はデータ転送プロセスの一つの要素であると考え、利害関係者や査察当局が要約報告書のデータのみに依存しないようにすることが重要である。

7.8.4 Prior to acceptance of summary data, an evaluation of the supplier’s quality system and compliance with data integrity principles should be established. It is not normally



acceptable nor possible to determine compliance with data integrity principles through the use of a desk-top or similar assessment.

要約されたデータを受領する前に、サプライヤの品質システムとデータ完全性の原則の順守の評価を確立すべきである。データ完全性の原則への準拠を、机上の評価あるいは同様な評価の適用で判断することは、通常、許容されず、また不可能である。

- 7.8.4.1 For external entities, this should be determined through on-site audit when considered important in the context of quality risk management. The audit should assure the veracity of data generated by the company, and include a review of the mechanisms used to generate and distribute summary data and reports.

外部機関の場合は、品質リスクマネジメントの関連から重要と考えられる場合には、実地監査（on-site audit）によって判断すべきである。監査では、その企業が作成したデータの信憑性（veracity）を確証し、要約されたデータや報告書を作成・配布するために使用される仕組み（メカニズム）の観点のレビューを含めるである。

- 7.8.4.2 Where summary data is distributed between different sites of the same organisation, the evaluation of the supplying site's compliance may be determined through alternative means (e.g. evidence of compliance with corporate procedures, internal audit reports, etc.).

要約されたデータが同一組織の異なる部署間に配布されている場合、その提供元の部署の（訳注：データ完全性についての）コンプライアンスの評価は、別の手段（企業内の手順に準拠している証拠、内部監査報告書など）によって決定することができる。

- 7.8.5 Summary data should be prepared in accordance with agreed procedures and reviewed and approved by authorised staff at the original site. Summaries should be accompanied with a declaration signed by the Authorised Person stating the authenticity and accuracy of the summary. The arrangements for the generation, transfer and verification of summary reports should be addressed within quality/technical agreements.

要約されたデータは、合意された手順に従って作成し、そのオリジナルの部署での権限を有するスタッフ（authorised staff）がレビューして承認する。その要約は、当該要約書の信頼性と正確性を述べたオーソライズド・パーソン（Authorised Person：訳注：単語の最初の文字が大文字であることに要注意）が署名した宣誓書（declaration）を添付すること。要約報告書のサマリーレポートの作成、転送及び検証（verification）に関する取り決めは、品質／技術協定（quality/technical agreements）の中で取り扱うべきである。



8 SPECIFIC DATA INTEGRITY CONSIDERATIONS FOR PAPER- BASED SYSTEMS

紙ベースシステムに固有なデータ完全性の考慮事項

8.1 Structure of Pharmaceutical Quality System and control of blank forms/templates/records

PQSシステムの構造と、ブランクの様式／テンプレート（訳注：定型的書式の文書）／記録書

8.1.1 The effective management of paper based documents is a key element of GMP/GDP. Accordingly the documentation system should be designed to meet GMP/GDP requirements and ensure that documents and records are effectively controlled to maintain their integrity.

紙ベースの文書を効果的に管理することは、GMP/GDPの重要な要素である。従って、文書システムは GMP/GDP の要求事項を満たすように設計し、文書及び記録がその完全性を維持するために効果的に管理されることを確実にすべきである。

8.1.2 Paper records should be controlled and should remain attributable, legible, contemporaneous, original and accurate, complete, consistent enduring (indelible/durable), and available (ALCOA+) throughout the data lifecycle.

紙媒体の記録は管理され、データのライフサイクルを通して、帰属性 (attributable)、判読可能性 (legible)、同時性 (contemporaneous)、原本性 (original) かつ正確性 (accurate)、完全性 (complete)、一貫した永続性 (消去不可能性／耐久性) (consistent enduring : indelible/durable)、及び利用可能性 (available) (ALCOA+) を維持すること。

8.1.3 Procedures outlining good documentation practices and arrangements for document control should be available within the Pharmaceutical Quality System. These procedures should specify how data integrity is maintained throughout the lifecycle of the data, including:

適正な文書化規範および文書管理の取り決めに概説した手順書が、医薬品品質システム (PQS) 内で利用可能とする。これらの手順には、データのライフサイクルを通じてデータの整合性を維持する方法を明記すること。これには、次の事項が含まれる：

- creation, review, and approval of master documents and procedures;
マスター文書や手順書の作成、レビュー、承認；
- generation, distribution and control of templates used to record data (master, logs, etc.);
データ記録のために使用するテンプレート（マスター、ログなど）の作成、配布、管理。
- retrieval and disaster recovery processes regarding records;
記録の検索 (retrieval) 及び災害時の回復 (disaster recovery) のプロセス



- generation of working copies of documents for routine use, with specific emphasis on ensuring copies of documents, e.g. SOPs and blank forms are issued and reconciled for use in a controlled and traceable manner;
日常的に使用する文書の作業用コピー（複写物）の生成。これは、文書のコピーを保証することに、特に強調したものであること。例えば、SOP やブランクフォーム（空の様式）が、発行され、その枚数の照合（reconciled）が可能であること。
- completion of paper based documents, specifying how individual operators are identified, data entry formats, recording amendments, and routine review for accuracy, authenticity and completeness; and
個々のオペレータの特定方法、データ入力フォーマット、修正の記録、および正確性（accuracy）、信憑性（authenticity）、完全性（completeness）をどの様に行うか規定した、紙ベースの文書の完全性； 及び
- filing, retrieval, retention, archival and disposal of records.
記録のファイリング、検索、保管、アーカイブ、廃棄。

8.2 Importance of controlling records 記録を管理することの重要性

8.2.1 Records are critical to GMP/GDP operations and thus control is necessary to ensure:

記録は GMP/GDP 運用に不可欠であり、それ故、以下を確実にするための管理が必要である：

- evidence of activities performed; 行われた活動の証拠；
- evidence of compliance with GMP/GDP requirements and company policies, procedures and work instructions;
GMP/GDP の要求事項、及び企業の方針、手順及び作業指示への適合性の証拠。
- effectiveness of Pharmaceutical Quality System;
医薬品品質システム（PQS）の有効性
- traceability; トレーサビリティ（遡及可能性）
- process authenticity and consistency; プロセスの信頼性及び一貫性
- evidence of the good quality attributes of the medicinal products manufactured;
製造された医薬品の適正な品質特性の証明；
- in case of complaints or recalls, records could be used for investigational purposes; and
苦情やリコールが発生した場合、記録は調査目的で使用される可能性がある；及び



- in case of deviations or test failures, records are critical to completing an effective investigation.

逸脱や試験不適合の場合、記録は効果的な調査を完了するために重要である。

8.3 Generation, distribution and control of template records

テンプレート記録書の生成、配布および管理

8.3.1 Managing and controlling master documents is necessary to ensure that the risk of someone inappropriately using and/or falsifying a record 'by ordinary means' (i.e. not requiring the use of specialist fraud skills) is reduced to an acceptable level. The following expectations should be implemented using a quality risk management approach, considering the risk and criticality of data recorded (see section 5.4, 5.5).

マスター文書の管理および制御は、「通常的手段」（すなわち、専門的な不正技術を必要としない）によって、誰かが記録を不適切に使用したり、あるいは改ざん（falsifying）したりするリスクを、許容されるレベルまで下げることを保証するために必要である。以下に述べる期待事項は、記録されたデータのリスクと重要性を考慮した品質リスクマネジメントアプローチを使用して実施すべきである。（5.4、5.5項参照）。

8.4 Expectations for the generation, distribution and control of records

記録の作成、配布、管理に関する期待事項

| Item | Generation 作成 |
|------|--|
| 1. | <p>Expectation 期待される事項</p> <p>All documents should have a unique identifier (including the version number) and should be checked, approved, signed and dated.</p> <p>すべての文書には一意の識別子（バージョン番号を含む）を付け、チェック、承認、署名、日付を入れるべきである。</p> <p>The use of uncontrolled documents should be prohibited by local procedures. The use of temporary recording practices, e.g. scraps of paper should be prohibited.</p> <p>管理されていない文書の使用は、ローカルな手順によって禁止されるべきである。紙切れなどの一時的な記録方法の使用は禁止すること。</p> <p>Potential risk of not meeting expectations/items to be checked 期待に一致しない潜在的リスク／チェックすべき事項</p> <ul style="list-style-type: none"> • Uncontrolled documents increase the potential for omission or loss of critical data as these documents may be discarded or destroyed without trace ability. In addition, uncontrolled records may not be designed to correctly record critical data. <p>管理されていない文書は、重要なデータの漏れや紛失の可能性が高まる。という</p> |



| | |
|----|--|
| | <p>のは、追跡の可能性がない状態で廃棄または破棄される可能性が存在するからである。更に、管理されていない記録は、重要なデータを正しく記録するように設計されていない可能性がある。</p> <ul style="list-style-type: none"> • It might be easier to falsify uncontrolled records. 管理されていない記録は、改ざんが容易な場合がある。 • Use of temporary recording practices may lead to data omission, and these temporary original records are not specified for retention. 一時的な記録方法は、データの漏れが発生する可能性があり、このような一時的な原本の記録は、のために指定されていない。 • If records can be created and accessed without control, it is possible that the records may not have been recorded at the time the event occurred. 管理されていない記録が作成され、アクセスできる場合、ある事象発生した時点で記録されていない可能性がある。 • There is a risk of using superseded forms if there is no version control or controls for issuance. バージョン管理や発行管理が行われていない場合、古い帳票を使用する危険性がある。 |
| 2. | <p>Expectation 期待されること</p> <p>The document design should provide sufficient space for manual data entries. ドキュメントのデザインには、手書きのデータを書き入れるための十分なスペースが必要である。</p> <p>Potential risk of not meeting expectations/items to be checked 期待を満たさない場合の潜在的なリスク／チェックすべき項目</p> <ul style="list-style-type: none"> • Handwritten data may not be clear and legible if the spaces provided for data entry are not sufficiently sized. 手書きのデータは、入力スペースが十分に確保されていないと、明瞭で読みやすいものにならない。 • Documents should be designed to provide sufficient space for comments, e.g. in case of a transcription error, there should be sufficient space for the operator to cross out, initial and date the error, and record any explanation required. 例えば、転記ミスがあった場合、作業者がそのミスを消し、イニシャルと日付を記入し、必要な説明を記録するための十分なスペースが必要である。 • If additional pages of the documents are added to allow complete documentation, the number of, and reference to any pages added should be clearly documented on the main record page and signed. 完全な文書化のために文書のページを追加する場合は、追加したページの数と参照先を主記録ページ (main record page) に明確に記録し、署名する。 • Sufficient space should be provided in the document format to add all necessary data, |


| | |
|----|--|
| | <p>and data should not be recorded haphazardly on the document, for example to avoid recording on the reverse of printed recording on the reverse of printed pages which are not intended for this purpose.</p> <p>必要な全てのデータを追加するための十分なスペースが、文書フォーマットに用意されているべきである。そしてデータは、やみくもに、その文書に記録すべきではない、例えば、この目的外のためにプリントされている頁の裏面に記録することなどを避けるようにする。</p> |
| 3. | <p>Expectation 期待されること</p> <p>The document design should make it clear what data is to be provided in entries. 文書の設計では、エントリー（入力）で与えられるデータが何であることを明確にする必要がある。</p> <p>Potential risks of not meeting expectations/items to be checked 期待を満たさない場合の潜在的なリスク／チェックすべき項目</p> <ul style="list-style-type: none"> • Ambiguous instructions may lead to inconsistent/incorrect recording of data. 曖昧な指示は、データの一貫性のなく／間違った記録につながる可能性がある。 • Good design ensures all critical data is recorded and ensures clear, contemporaneous and enduring (indelible/durable) completion of entries. 優れたデザインは、すべての重要なデータが記録され、明確に、同時的に、そして永続的（消えない/壊れない）な記入を保証する。 • The document should also be structured in such a way as to record information in the same order as the operational process and related SOP, to minimize the risk of inadvertently omitting critical data. 文書は、重要なデータを誤って取り除かれるリスクを最小限にするために、運用手順および関連する SOP と同じ順序で情報を記録するように構成すべきである。 |
| 4. | <p>Expectation 期待されること</p> <p>Documents should be stored in a manner which ensures appropriate version control. 文書は、適切なバージョン管理を確実にする方法で保管すること。</p> <p>Master documents should contain distinctive marking so to distinguish the master from a copy, e.g. use of coloured papers or inks so as to prevent inadvertent use. マスター文書は、マスターとコピーを区別するための特徴的なマーキングを施すべきである。例えば、不用意な使用を防ぐために、色付きの紙やインクを使用するなど。</p> <p>Master documents (in electronic form) should be prevented from unauthorised or inadvertent changes. マスター文書（電子形式）は、無許可または不注意による変更を防止すべきである。</p> <p>E.g.: For the template records stored electronically, the following precautions should be in place: — access to master templates should be controlled;</p> |



| | |
|--|--|
| | <p>— process controls for creating and updating versions should be clear and practically applied/verified; and</p> <p>— master documents should be stored in a manner which prevents unauthorised changes.</p> <p>例えば：電子的に保存されたテンプレート（訳注：定型的書式の文書）記録は、以下の予防措置を講じること。</p> <p>— マスターのテンプレートへのアクセスは、管理すること。</p> <p>— 作成及びバージョンの更新のためのプロセス管理は、特に実際の適用／検証が明確であること；及び</p> <p>— 作成マスターの文書は、無許可の変更を防止する方法で保存すること。</p> |
| | <p>Potential risk of not meeting expectations/items to be checked 期待を満たさない場合の潜在的なリスク / チェックすべき項目</p> <ul style="list-style-type: none"> • Inappropriate storage conditions can allow unauthorised modification, use of expired and/or draft documents or cause the loss of master documents. <p>不適切な保管状態は、無許可の変更、期限切れ及び/又はドラフト文書の使用、又はマスター文書の紛失を可能にする。</p> <ul style="list-style-type: none"> • The processes of implementation and the effective communication, by way of appropriate training prior to implementation when applicable, are just as important as the document. <p>該当する場合は、実施のプロセスと、実施する前の適切な訓練による効果的なコミュニケーションは、文書と同様に重要である。</p> |

| Item | Distribution and Control 配布および管理 |
|------|--|
| 1. | <p>Expectations 期待されること</p> <p>Updated versions should be distributed in a timely manner.</p> <p>更新されたバージョンは、タイムリーに配布すべきである。</p> <p>Obsolete master documents and files should be archived and their access restricted.</p> <p>旧版となったマスター文書やファイルはアーカイブ化し、そのアクセスを制限すること。</p> <p>Any issued and unused physical documents should be retrieved and reconciled.</p> <p>発行され、そして使用されなくなった全ての文書は回収し、（訳注：回収されたかを）照合すること。</p> <p>Where authorised by Quality, recovered copies of documents may be destroyed. However, master copies of authorised documents should be preserved.</p> <p>Quality（品質保証部門？）が許可した場合、文書の回収された写し（recovered copies of documents）を廃棄することが可能である。ただし、承認された文書のマスターコピー</p> |



| | |
|----|--|
| | <p>ーは保存するべきである。</p> <p>Potential risk of not meeting expectations/items to be checked</p> <p>期待に合致しない場合の潜在的なリスク／チェックすべき項目</p> <ul style="list-style-type: none"> • There may be a risk that obsolete versions can be used by mistake if available for use. <p>もし旧版が使用可能な場合、誤って使用されるリスクが存在する。</p> |
| 2. | <p>Expectation 期待されること</p> <p>Document issuance should be controlled by written procedures that include the following controls:</p> <p>文書の発行は、以下の管理を含む書面による文書化された手順によって管理するべきである：</p> <ul style="list-style-type: none"> - details of who issued the copies and when they were issued; 誰がコピーを発行したか、いつ発行されたかの詳細 - clear means of differentiating approved copies of documents, e.g. by use of a secure stamp, or paper colour code not available in the working areas or another appropriate system; 承認された文書のコピーを区別する明確な手段。例えば、セキュア・スタンプ（訳注：例えば右の図）の使用、作業区域で利用できない紙製のカラーコード、あるいは、その他の適切なシステムの使用）；  - ensuring that only the current approved version is available for use; 最新の承認済みバージョンのみが使用可能であることを保証すること； - allocating a unique identifier to each blank document issued and recording the issue of each document in a register ; 発行された各ブランク文書（blank document）に一意の識別子（unique identifier）を割り当て、各文書の発行を登録簿に記録すること。 - numbering every distributed copy (e.g.: copy 2 of 2) and sequential numbering of issued pages in bound books; 配布されたすべてのコピーへの番号付け（例：コピー2／2）、製本された書籍の発行ページに連番を付ける。 - where the re-issue of additional copies of the blank template is necessary, a controlled process regarding re-issue should be followed with all distributed copies maintained and a justification and approval for the need of an extra copy recorded, e.g.: “the original template record was damaged” ; 空白（ブランク）のテンプレート（訳注：定型書式の文書）を追加で発行する必要がある場合は、再発行に関する管理されたプロセスは、配布した全てのコピーを保持し、そして特別にコピーを配布した必要性について、その理由の説明と承認をする（例：元のテンプレートの記録書がダメージを受けた）； - critical GMP/GDP blank forms (e.g.: worksheets, laboratory notebooks, batch |

records, control records) should be reconciled following use to ensure the accuracy and completeness of records; and

重要なGMP/GDPブランクの書式（例えば、ワークシート、ラボ用ノート、バッチ記録書、管理記録）は、記録の正確性と完全性を保証するために、使用後に照合を行う（be reconciled）べきである；および

- where copies of documents other than records, (e.g. procedures), are printed for reference only, reconciliation may not be required, providing the documents are time-stamped on generation, and their short-term validity marked on the document.

記録書以外の文書（例：手順書）のコピーを、参照するためにのみ印刷する場合は、照合（reconciliation: 訳注 部数の照合）は必要でないかもしれない。ただし、その文書を生成した時に、タイムスタンプがされ（time-stamped）、その文書が短期間のみ有効であることが記されていることが必要である。

Potential risk of not meeting expectations/items to be checked

期待に合致しない場合の潜在的なリスク／チェックすべき項目

Without the use of security measures, there is a risk that rewriting or falsification of data may be made after photocopying or scanning the template record (which gives the user another template copy to use).

セキュリティ対策がなされていないと、テンプレート記録（訳注：定型書式の文書）をコピー又はキャンした後に、データの書き換えや改ざんが行われるリスクがある（これは、ユーザに別のテンプレート（訳注：定型書式の文書）コピーを与えることになる）。

Obsolete versions can be used intentionally or by error.

旧版の文書は、意図的にまたは誤って使用される可能性がある。

A filled record with an anomalous data entry could be replaced by a new rewritten template.

変則的なデータ入力が行われた記入済みの記録は、新たに書き換えられたテンプレートに置き換えられる可能性がある。

All unused forms should be accounted for, and either defaced and destroyed, or returned for secure filing.

未使用のフォーム（訳注：様式文書）はすべてその要否を説明し、棄損させて、破棄する。あるいは、安全なファイリングのために返却する必要がある。

Check that (where used) reference copies of documents are clearly marked with the date of generation, period of validity and clear indication that they are for reference only and not an official copy, e.g. marked 'uncontrolled when printed'.

文書の参照用のコピーを使用する場合は、作成日、有効期間、および参照用のみであって、正式なコピーでないことを明確に示すマーク（例：「印刷時に管理されていない」というマーク）が付けられていることを確認する。

8.4.1 An index of all authorised master documents, (SOP's, forms, templates and records) should be maintained within the Pharmaceutical Quality System. This index should mention for each type of template record at least the following information: title, identifier including version number, location (e.g. documentation database, effective date, next review date, etc.).

承認されたすべてのマスター文書（SOP、様式文書、テンプレート（訳注：定型書式の記録書）及び記録）の索引は、医薬品品質システム内で維持されるべきである。この索引には、テンプレート記録の種類ごとに、少なくとも次の情報を記載すること：題目、制改訂番号を含む識別子、位置づけ（location）（例：文書データベース、発効日、次回レビュー日など）。

8.5 Use and control of records located at the point-of-use

使用箇所に置かれる記録の、使用と管理

8.5.1 Records should be available to operators at the point-of-use and appropriate controls should be in place to manage these records. These controls should be carried out to minimize the risk of damage or loss of the records and ensure data integrity. Where necessary, measures should be taken to protect records from being soiled (e.g. getting wet or stained by materials, etc.).

記録書は使用箇所の作業者が利用できるようにし、これらの記録を管理するために適切なマネジメントを行うべきである。これらの管理は、記録の棄損または紛失のリスクを最小限に抑え、データの完全性を確保するように実施されるべきである。必要に応じて、記録が汚されないように保護する手段を講じるべきである（例えば、水に濡れる、物質で汚れるなどからの保護）。

8.5.2 Records should be appropriately controlled in these areas by designated persons or processes in accordance with written procedures.

記録は、これらの区域において、指定された職員またはプロセスにより、文書化された手順に基づいて適切に管理されるべきである。

8.6 Filling out records 記録の記入

8.6.1 The items listed in the table below should be controlled to assure that a record is properly filled out.

以下の表にリストした項目は、記録が正しく記入されていることを確認するために、管理すべき事項である。

| Item | Completion of records 記録の完了 |
|------|---|
| 1. | <p>Expectations 期待されること</p> <p>Handwritten entries should be made by the person who executed the task⁷. 手書きの記入は、その業務を実行した人が行うべきである⁷。</p> <p>⁷ : Scribes may only be used in exceptional circumstances, refer footnote 8. 代筆者（scribes）例外的な状況下でのみ利用できる。脚注 8 参照</p> <p>Unused, blank fields within documents should be voided (e.g. crossed-out), dated and signed. 文書内の未使用の空欄は無効にし（例：消去線を引く）、日付を記入し、署名する。</p> <p>Handwritten entries should be made in clear and legible writing. 手書きでの記入は、明確で読みやすい文字で行うこと。</p> <p>The completion of date fields should be done in an unambiguous format defined for the site. E.g. dd/mm/yyyy or mm/dd/yyyy. 日付欄の記入は、当該製造所で定義された曖昧さのないフォーマットで行うこと。 例：dd/mm/yyyyまたはmm/dd/yyyy。</p> <p>Potential risk of not meeting expectations/items to be checked 期待に合致しない場合の潜在的なリスク／チェックすべき項目</p> <p>Check that handwriting is consistent for entries made by the same person. 手書きの場合は、同一人物によって行われていることをチェックする。</p> <p>Check the entry is legible and clear (i.e. unambiguous; and does not include the use of unknown symbols or abbreviations, e.g. use of ditto(" ") marks. 記入内容が読みやすく明確であることを確認する（曖昧さがなく、不明な記号や略語（例：ditto (" ") : いわゆる「チヨ・チヨ」）マークの使用）が含まれていない）。</p> <p>Check for completeness of data recorded. 記録されたデータが完全であるかどうかを確認する。</p> <p>Check correct pagination of the records and are all pages present. 記録が正しく頁順になっているか（pagination）、すべてのページが存在するかを確認する。</p> |
| 2. | <p>Expectation 期待されること</p> <p>Records relating to operations should be completed contemporaneously⁸. 操作に係る記録は、同時的に完了するべきである⁸。</p> |



| | |
|--|---|
| | <p>8. The use of scribes (second person) to record activity on behalf of another operator should be considered 'exceptional', and only take place where:</p> <p>他の作業員になり替わっての活動を記録することの代筆者（第二者）の利用は、「例外的」なものと考え、以下の場合にのみ行うべきである。</p> <ul style="list-style-type: none"> • The act of recording places the product or activity at risk e.g. documenting line interventions by sterile operators. 記録の行為が製品または活動を危険にさらす場合（例：無菌作業を行う者によるライン介入の記録）。 • To accommodate cultural or staff literacy / language limitations, for instance where an activity is performed by an operator, but witnessed and recorded by a scribe. In these cases, bilingual or controlled translations of documents into local languages and dialect are advised. 文化的な、またはスタッフの能力／言語の制限的事項に対応するため、例えば、ある活動が作業員によって行われるが、代筆者によって立ち合い、記録する場合など。このような場合には、現地の言語や方言への文書の二ヶ国語翻訳または管理された翻訳が推奨される。 <p>In both situations, the scribe recording should be contemporaneous with the task being performed, and should identify both the person performing the observed task and the person completing the record. The person performing the observed task should countersign the record wherever possible, although it is accepted that this countersigning step will be retrospective. The process for a scribe to complete documentation should be described in an approved procedure, which should; specify the activities to which the process applies and assesses the risks associated.</p> <p>いずれの状況においても、代筆者による記録は、行っている業務と同時的に行われるべきであり、観察されたタスクを実施する人及び記録を記入する人の両方を特定すべきである。観察される業務を行っている人は、可能な限り記録に連署すべきであるが、この連署のステップは遡及的であることは、認められている。代筆者が文書を完成させるためのプロセスは、承認された手順書に記載されるべきであり、その手順書は、プロセスが適用される活動を特定し、関連するリスクを評価すべきである。</p> |
| | <p>Potential risk of not meeting expectations/items to be checked 期待に合致しない場合の潜在的なリスク / チェックすべき項目</p> <p>Verify that records are available within the immediate areas in which they are used, i.e. Inspectors should expect that sequential recording can be performed at the site of operations. If the form is not available at the point of use, this will not allow operators to fill in records at the time of occurrence.</p> <p>記録が、それを使用される直接のエリア内で利用可能であることを検証する。すなわち、査察官は、作業の現場で逐次記録ができることを期待すべきである。もし使用する場所で、記入すべき記録書フォームが利用できない場合、それでは作業員が（操作を行った時点で）記録を記入することができない。</p> |

| | |
|----|--|
| 3. | <p>Expectation 期待されること</p> <p>Records should be enduring (indelible). 記録は永続的な（消せない）ものでなければならない。</p> |
|----|--|



| | |
|----|--|
| | <p>Potential risk of not meeting expectations/items to be checked 期待に合致しない場合の潜在的なリスク / チェックすべき項目</p> <p>Check that written entries are in ink, which is not erasable, and/or will not smudge or fade (during the retention period).</p> <p>記入された記録はインクで書かれるが、それが消せないこと、（保存期間中に）汚れたり消えたりしないことをチェックする。</p> <p>Check that the records were not filled out using pencil prior to use of pen (overwriting).</p> <p>記録は、ペンを使う前に鉛筆で記入されていないか（上書きがされていないことの確認）。</p> <p>Note that some paper printouts from systems may fade over time, e.g. thermal paper. Indelible signed and dated true copies of these should be produced and kept.</p> <p>システムから出力された紙の中には、時間が経過すると共に退色してしまうものがある。例えば、感熱紙である。これらの消去ができない署名と日付の入った真正コピー（true copies）を作成し、保管すべきである。</p> |
| 4. | <p>Expectation 期待されること</p> <p>Records should be signed and dated using a unique identifier that is attributable to the author.</p> <p>記録書は、その記録者（author）に帰属する固有の識別子（訳注参照）を用いて署名し、日付を記入すること。</p> <p>訳注：ここでいう「固有の識別子」（unique identifier）とは、コンピュータのログインコードのようなものではなく、簡略化した署名や「花押的な記号」のような、他者が真似できない識別子と考えられる。</p> <p>Potential risk of not meeting expectations/items to be checked 期待に合致しない場合の潜在的なリスク / チェックすべき項目</p> <p>Check that there are signature and initials logs, that are controlled and current and that demonstrate the use of unique examples, not just standardized printed letters.</p> <p>次のことをチェックする：</p> <ul style="list-style-type: none"> ① 署名とイニシャルのログがある； ② 上記①が管理され、最新のものであることを確認する； ③ 標準化された印刷された文字だけでなく、独自の例を使用していることを明らかにする。 <p>Ensure that all key entries are signed & dated, particularly if steps occur over time, i.e. not just signed at the end of the page and/or process.</p> <p>すべての主要なエントリ（入力事項）に署名と日付が入っていることを確認する。特に、時間をかけてステップが行われる場合は、ページの終わりや、プロセスの最後の時点で署名するだけではないことを確認する。</p> <p>The use of personal seals is generally not encouraged; however, where used, seals should be controlled for access. There should be a log which clearly shows traceability between an</p> |



individual and their personal seal. Use of personal seals should be dated (by the owner), to be deemed acceptable.

個人的な印鑑（personal seals）の使用は、一般的に推奨されていない；それを使用する場合は、その印鑑を得るための手段について管理されていること。私的用印鑑（individual seal）と職員業務用印鑑（personal seal）は、そのトレーサビリティを明確に示すログが存在するべきである。職員業務用印鑑（personal seal）の使用は、（所有者による）日付が入ったものが許容されると考えられる。

8.7 Making corrections on records 記録についての修正の実施

Corrections to the records should be made in such way that full traceability is maintained.

記録の修正は、十分なトレーサビリティが維持される方法で行うこと。

| Item | How should records be corrected? |
|------|---|
| 1 | <p>Expectation 期待されること</p> <p>Cross out what is to be changed with a single line. 変更する部分を一本の線で抹消する。</p> <p>Where appropriate, the reason for the correction should be clearly recorded and verified if critical. 必要に応じて、修正の理由を明確に記録し、重要な場合は検証する。</p> <p>Initial and date the change made. 変更した箇所にイニシャルと日付を記入する。</p> <p>Specific elements that should be checked when reviewing records:</p> <p>記録を確認する際にチェックすべき具体的な要素。</p> <p>Check that the original data is readable not obscured (e.g. not obscured by use of liquid paper; overwriting is not permitted). 元のデータが読めて、不明瞭でないことを確認する（例：修正液（liquid paper）を使って不明瞭になっていないか；上書きは許されない）。</p> <p>If changes have been made to critical data entries, verify that a valid reason for the change has been recorded and that supporting evidence for the change is available. 重要なデータのエントリ（訳注：入力された事項）に変更が加えられている場合は、変更の正当な理由が記録されているか、また、変更の裏付けとなる証拠があるかを確認する。</p> <p>Check for unexplained symbols or entries in records. 記録書に説明のつかない記号や記入がないか、確認する。</p> |
| 2. | <p>Expectation 期待される事項</p> <p>Corrections should be made in indelible ink.</p> |



| | |
|--|--|
| | <p>訂正は消えないインク (indelible ink) で行うべきである。</p> <p>Specific elements that should be checked when reviewing records:</p> <p>記録書を確認する際にチェックすべき具体的な要素。</p> <p>Check that written entries are in ink, which is not erasable, and/or will not smudge or fade (during the retention period).</p> <p>書かれた事項 (written entries) が、インクで書かれていること、そして／または (保存期間中は) 鮮明かどうか、退色しないかどうかをチェックする。</p> <p>Check that the records were not filled out using pencil prior to use of pen (overwriting).</p> <p>記録は、ペンを使う前に鉛筆で記入されていないか (上書きされていないかどうか) をチェックする。</p> |
|--|--|

8.8 Verification of records (secondary checks) 記録の検証 (二次チェック)

| Item | When and who should verify the records? 記録書は誰が何時確認するのか? |
|------|--|
| 1. | <p>Expectation 期待されること</p> <p>Records of critical process steps, e.g. critical steps within batch records, should be:</p> <p>重要なプロセスステップの記録、例えば、バッチ記録書内の重要なステップは、以下のようすべきである。</p> <p>reviewed/witnessed by independent and designated personnel at the time of operations occurring; and</p> <p>作業が発生した時点で、独立した、そして指名された職員がレビューし／署名する ;</p> <p>reviewed by an approved person within the production department before sending them to the Quality unit ; and</p> <p>品質部門 (Quality unit) に送付する前に、製造部門内の承認された者がレビューする ;</p> <p>reviewed and approved by the Quality Unit (e.g. Authorised Person / Qualified Person) before release or distribution of the batch produced.</p> <p>製造されたバッチを出荷又は配送する前に、品質部門 (Quality Unit) (例 : オーソライズド・パーソン / 有資格者) がレビューし、承認する。</p> <p>Batch production records of non-critical process steps is generally reviewed by production personnel according to an approved procedure.</p> <p>重要でないプロセスステップのバッチ製造記録書 (batch production records of non-critical process steps) は、通常、承認された手順に従って製造担当者がレビューする。</p> <p>Laboratory records for testing steps should also be reviewed by designated personnel</p> |



(e.g.: second analysts) following completion of testing. Reviewers are expected to check all entries, critical calculations, and undertake appropriate assessment of the reliability of test results in accordance with data-integrity principles.

試験段階での実験室記録も、試験の完了後に指定された職員（例：第二分析者；second analysts）によってレビューするべきである。レビュー担当者は、データ完全性の原則に従って、すべての記入事項、重要な計算を確認し、試験結果の信頼性について適切な評価を行うことが期待される。

Additional controls should be considered when critical test interpretations are made by a single individual (e.g. recording of microbial colonies on agar plates). A secondary review may be required in accordance with risk management principles. In some cases this review may need to be performed in real-time. Suitable electronic means of verifying critical data may be an acceptable alternative, e.g. taking photograph images of the data for retention.

重要な試験の解釈が、ただ一人の職員によって行われる場合（例：寒天培地平板の微生物のコロニーの記録）には、追加の管理を考慮する必要がある。二次レビュー（secondary review）が、リスクマネジメントの原則に従い、必要となる可能性がある。場合によっては、このレビューをリアルタイムで行う必要があるかもしれない。重要なデータを検証するための適切な電子的手段は、その代替法として容認が可能であろう。例えば、保存用にデータの写真画像を撮影するという方法である。

This verification should be conducted after performing production-related tasks and activities and be signed or initialled and dated by the appropriate persons.

この検証（verification）は、製造に関連する業務および活動を行った後に実施し、適切な人が署名（またはイニシアルを記入）して日付を記載すること。

Local SOPs should be in place to describe the process for review of written documents.

ローカルSOP（訳注：SOPの適応範囲が当該部署内に限定される作業手順書）は、文書化された文書のレビューの手順（process）を、適切に述べるべきである。

Specific elements that should be checked when reviewing records:

記録を確認する際にチェックすべき具体的な要素。

- Verify the process for the handling of production records within processing areas to ensure they are readily available to the correct personnel at the time of performing the activity to which the record relates.

製造プロセスを行っている区域内での製造記録書の取り扱いのプロセスを検証する。これは、その記録書が関連する活動を行う時点で、適切な担当職員がすぐにその記録書を利用できるようになっているかを確認するためである。

- Verify that any secondary checks performed during processing were performed by appropriately qualified and independent personnel, e.g. production supervisor or QA.

プロセス作業中に行われる全ての第三者によるチェック（any secondary checks）が、

| | |
|--|---|
| | <p>適切な資格を持ち、かつ独立した職員（製造部門の監督者やQAなど）によって行われたことを確認する。</p> <ul style="list-style-type: none"> • Check that documents were reviewed by production personnel and then quality assurance personnel following completion of operational activities <p>文書が製造作業の完了後に、製造部門の職員によってレビューされ、次いで品質保証部門の職員によってレビューされたことを、チェックする。</p> |
|--|---|

| Item | How should records be verified? 記録書をどの様に確認すべきか？ |
|------|--|
| 2. | <p>Expectation 期待されること</p> <p>Check that all the fields have been completed correctly using the current (approved) templates, and that the data was critically compared to the acceptance criteria.</p> <p>最新の（承認された）テンプレートを使用して、すべてのフィールドが正しく記入されていること及び、そのデータが受入れ可能な判断基準（acceptance criteria）に対して、批判的に比較されている（critically compared）ことを確認する。</p> <p>Check items 1, 2, 3, and 4 of section 8.6 and Items 1 and 2 of section</p> <p>セクション8.6項の項目1、2、3、4、及びセクション8.7項の項目1、2を、チェックする。</p> <p>Specific elements that should be checked when reviewing records:</p> <p>記録を確認する際にチェックすべき具体的な要素：</p> <p>Inspectors should review company procedures for the review of manual data to determine the adequacy of processes.</p> <p>査察官は、プロセスの適切性を判断するために、手書きデータ（manual data）についての、企業の手順をレビューすべきである。</p> <p>The need for, and extent of a secondary check should be based on quality risk management principles, based on the criticality of the data generated.</p> <p>二次チェックの必要性とその程度は、生成されたデータの重要性に基づいて、品質リスクマネジメントの原則に基づくべきである。</p> <p>Check that the secondary reviews of data include a verification of any calculations used.</p> <p>データの二次レビューは、使用された全ての計算の確認を含む。</p> <p>View original data (where possible) to confirm that the correct data was transcribed for the calculation.</p> <p>正しいデータが、計算のために転記されたことを確認するために、元のデータを参照する（可能な場合）。</p> |

8.9 Direct print-outs from electronic systems 電子システムからの直接プリントアウト

8.9.1 Some very simple electronic systems, e.g. balances, pH meters or simple processing equipment which do not store data, generate directly-printed paper records. These types of systems and records provide limited opportunity to influence the presentation of data by (re-)processing, changing of electronic date/time stamps. In these circumstances, the original record should be signed and dated by the person generating the record and information to ensure traceability, such as sample ID, batch number, etc. should be recorded on the record. These original records should be attached to batch processing or testing records.

幾つかの非常に単純な電子的なシステム、例えば、データを保存しない天秤、pHメーター、単純な処理装置などは、直接印刷された紙の記録（directly-printed paper records）が生成される。このようなタイプのシステムおよび記録は、（再）処理や電子的な日付／時間スタンプの変更など、データの表示に影響を与える機会が限られている。このような状況では、記録の原本には記録を作成した人の署名と日付を入れ、サンプルID、バッチ番号などのトレーサビリティを確保するための情報を、記録に書き入れるべきである。これらの原本の記録は、バッチ処理または試験の記録に添付するべきである。

8.9.2 Consideration should be given to ensuring these records are enduring (see section 8.6.1).

これらの記録が永続性を有すること確実にすることを考慮すべきである（8.6.1項参照）。

8.10 Document retention (Identifying record retention requirements and archiving records) 文書の保存（記録保存要件の特定と記録のアーカイブ化）

8.10.1 The retention period of each type of records should (at a minimum) meet those periods specified by GMP/GDP requirements. Consideration should be given to other local or national legislation that may stipulate longer storage periods.

各種の記録の保存期間は、（最低でも）GMP/GDPの要求で指定された期間を満たすべきである。より長い保存期間を規定している可能性のある他の地域または国の法律を考慮するべきである。

8.10.2 The records can be retained internally or by using an outside storage service subject to quality agreements. In this case, the data centre's locations should be identified. A risk assessment should be available to demonstrate retention systems/facilities/services are suitable and that the residual risks are understood.

記録の保管は、社内で行うこともできるし、品質協定に基づいて外部の保管サービスを利用することもできる。この場合、データセンターの所在地を特定する必要がある。保管シ



システム／設備／サービスが適切であること、および残存するリスクが理解されていることを示すために、リスクアセスメントを利用すべきである。

| Item | Where and how should records be archived? どこに、そしてどの様に記録をアーカイブすべきか？ |
|------|---|
| 1. | <p>Expectation 期待されること</p> <p>A system should be in place describing the different steps for archiving records (identification of archive boxes, list of records by box, retention period, archiving location, etc.).</p> <p>記録をアーカイブするためのさまざまな手順（アーカイブボックスの識別、ボックスごとの記録のリスト、保存期間、アーカイブ場所など）を記述したシステムを導入すること。</p> <p>Instructions regarding the controls for storage, as well as access and recovery of records should be in place.</p> <p>記録の保管、アクセスと共に、回収の管理に関する指示がなされていること。</p> <p>Systems should ensure that all GMP/GDP relevant records are stored for periods that meet GMP/GDP requirements⁹.</p> <p>システムは、GMP/GDPに関連するすべての記録が、GMP/GDPの要件を満たす期間、保存されることを保証すること⁹。</p> <p>9. Note that storage periods for some documents may be dictated by other local or national legislation.</p> <p>なお、幾つかの文書の保管期間は、ドキュメントによっては、地域や各国の法令によって保管期間を述べている可能性もある。</p> <p>Specific elements that should be checked when reviewing records: 記録をレビューする際にチェックすべき具体的な要素。</p> <ul style="list-style-type: none"> • Check that the system implemented for retrieving archived records is effective and traceable. アーカイブされた記録を検索するために実施するシステムが、効果的で追跡可能であるかどうかを確認する。 • Check if the records are stored in an orderly manner and are easily identifiable. 記録が整然と保管されており、容易に識別できるかどうかを確認する。 • Check that records are in the defined location and appropriately secured. 記録が定められた場所にあり、適切に保護されているかを確認する。 • Check that access to archived documents is restricted to authorised personnel ensuring integrity of the stored records. アーカイブされた文書へのアクセスは、保存された記録の完全性を確保するために、権限のある担当者に制限されていることを確認する。 |

| | |
|---|--|
| | <ul style="list-style-type: none"> • Check for the presence of records of accessing and returning of records. 記録へのアクセスおよび返却の記録があるかどうかを確認する。 • The storage methods used should permit efficient retrieval of documents when required. 使用される保管方法は、必要なときに文書を効率的に取り出すことができるものであること。 |
| 2 | <p>Expectation 期待されること</p> <p>All hardcopy quality records should be archived in:</p> <p>全てのハードコピーの品質に係る記録は、以下のように保管すること：</p> <ul style="list-style-type: none"> • secure locations to prevent damage or loss, 損傷や紛失を防ぐために安全な場所； • such a manner that it is easily traceable and retrievable, and 簡単に追跡でき、検索できるような方法； • a manner that ensures that records are durable for their archived life. 記録がそのアーカイビングの期間中の耐久性を確保できる方法。 <p>Specific elements that should be checked when reviewing records:</p> <p>記録を確認する際にチェックすべき具体的な要素：</p> <ul style="list-style-type: none"> • Check for the outsourced archived operations if there is a quality agreement in place and if the storage location was audited. 外部に委託したアーカイブ業務に関しては、品質合意書（quality agreement）に関する契約が結ばれているか、保管場所が監査されているかをチェックする。 • Ensure there is some assessment of ensuring that documents will still be legible/available for the entire archival period. 文書がアーカイブの全期間中も読みやすく、利用できることを保証するための評価がされているかを確認する。 • In case of printouts which are not permanent (e.g. thermal transfer paper) a verified ('true') copy should be retained. 永久的ではないプリントアウト（熱転写紙など）の場合は、検証された（「真正の」）コピーを保持すること。 • Verify whether the storage methods used permit efficient retrieval of documents when required. 使用されている保管方法が、必要なときに文書を効率的に取り出せるかどうかを検証する。 |

| | |
|---|--|
| 3 | <p>Expectation 期待されること</p> <p>All records should be protected from damage or destruction by: 全ての記録は、以下の原因による損傷や破壊から保護されているべきである：</p> <p>fire; 火災；</p> <p>liquids (e.g. water, solvents and buffer solution); 液体（例：水、溶剤、緩衝液）；</p> <p>rodents; 齧歯類</p> <p>humidity etc; and. 湿度など； および</p> <p>unauthorised personnel access, who may attempt to amend, destroy or replace records. 記録を修正、破壊、交換しようとする可能性がある、権限のない人のアクセス。</p> |
| | <p>Specific elements that should be checked when reviewing records: 記録を確認する際にチェックすべき具体的な要素：</p> <p>Check if there are systems in place to protect records (e.g. pest control and sprinklers). 記録を保護するためのシステムがあるかどうかをチェックする（例：防虫管理、スプリンクラー）。</p> <p>Note: Sprinkler systems should be implemented according to local safety requirements; however, they should be designed to prevent damage to documents, e.g. documents are protected from water. スプリンクラーシステムは、当該地域の安全要件に従って導入するべきであるが、ドキュメントが水から保護されるなど、ドキュメントへのダメージを防ぐように設計されている必要がある。</p> <p>Check for appropriate access controls for records. 記録に対する適切なアクセスコントロールを確認する。</p> |



8.11 Disposal of original records or true copies 記録原本または真正コピーの廃棄

- 8.11.1 A documented process for the disposal of records should be in place to ensure that the correct original records or true copies are disposed of after the defined retention period. The system should ensure that current records are not destroyed by accident and that historical records do not inadvertently make their way back into the current record stream (e.g. historical records confused/mixed with existing records.)

記録の廃棄のための文書化されたプロセスは、正しいオリジナルの記録または真正コピーが、定義された保存期間後に廃棄されることを確実にすることに適切であること。このシステムは、次のことが確実にとなるようなものであること：

- ・ 現在の記録が誤って破壊されないこと；
- ・ 過去の記録（historical records）が誤って現在の記録の流れに戻ってこないこと。（例えば、過去の記録が既存の記録と混同／混合される）。

- 8.11.2 A record/register should be available to demonstrate appropriate and timely archiving or destruction of retired records in accordance with local policies.

ローカルポリシー（訳注参照）に従って、退色した記録を適切かつタイムリーにアーカイブまたは破棄することを証明する記録/登録が利用可能であること。

訳注：ここでいう「ローカルポリシー」がコンピュータの用語としての位置づけで使用されていることも考えられる。明確な判断が出来ないので、この訳文では「各事業所／各コンピュータ・システム」と考えたい。

- 8.11.3 Measures should be in place to reduce the risk of deleting the wrong documents. The access rights allowing disposal of records should be controlled and limited to few persons.

間違った文書（wrong documents：訳注 削除対象ではない文書）を削除してしまうリスクを低減するための対策が講じられていること。記録の廃棄を許可するアクセス権は管理され、少数の人限定すべきである。

9. SPECIFIC DATA INTEGRITY CONSIDERATIONS FOR COMPUTERISED SYSTEMS

コンピュータ化されたシステムにおける具体的なデータ完全性に関する考慮事項

9.1 Structure of the Pharmaceutical Quality System and control of computerised systems 医薬品品質システムの構造とコンピュータシステムの管理

- 9.1.1 A large variety of computerised systems are used by companies to assist in a significant



number of operational activities. These range from the simple standalone to large integrated and complex systems, many of which have an impact on the quality of products manufactured. It is the responsibility of each regulated entity to fully evaluate and control all computerised systems and manage them in accordance with GMP¹⁰ and GDP¹¹ requirements.

企業では、多くの業務活動を支援するために、様々なコンピュータ・システムが使用されている。それらは、これらは、単純なスタンドアローン（訳注：単体のパソコン）から大規模な統合された複雑なシステムまで多岐にわたり、その多くが製造される製品の品質に影響を与えています。すべてのコンピュータ化されたシステムを十分に評価・管理し、GMP¹⁰およびGDP¹¹の要求事項に従ってマネジメントすることは、各規制対象企業の責任である。

10 PIC/S PE 009 Guide to Good Manufacturing Practice for Medicinal Products, specifically Part I chapters 4, Part II chapters 5, & Annex 11

PIC/S PE 009 Guide to Good Manufacturing Practice for Medicinal Products, 特に、Part I chapters 4, Part II chapters 5, 及び Annex 11の記述。

11 PIC/S PE 011 GDP Guide to Good Distribution Practice for Medicinal Products, specifically section 3.5

PIC/S PE 011 GDP Guide to Good Distribution Practice for Medicinal Products, 特に、section 3.5。

9.1.2 Organisations should be fully aware of the nature and extent of computerised systems utilised, and assessments should be in place that describe each system, its intended use and function, and any data integrity risks or vulnerabilities that may be susceptible to manipulation. Particular emphasis should be placed on determining the criticality of computerised systems and any associated data, in respect of product quality.

組織は、利用されているコンピュータ化システムの性質と範囲を十分に認識すべきであり、かつ、各システム、その意図された用途と機能、操作される可能性のあるデータ完全性のリスクまたは脆弱性を説明する評価を実施すること。特に、製品の品質に関わるコンピュータ化システム及び関連データの重要性を判断することに重点を置くこと。

9.1.3 All computerised systems with potential for impact on product quality should be effectively managed under a Pharmaceutical Quality System which is designed to ensure that systems are protected from acts of accidental or deliberate manipulation, modification or any other activity that may impact on data quality and integrity.

製品の品質に影響を与える可能性のあるすべてのコンピュータ化されたシステムは、偶発的または意図的な操作、変更、またはデータの品質および、完全性に影響を与える可能性のあるその他の行為から、当該システムが確実に保護されるように設計された医薬品品質システムの下で効果的に管理されるべきである。

9.1.4 The processes for the design, evaluation, and selection of computerised systems should include appropriate consideration of the data management and integrity aspects of the

system. Regulated users should ensure that vendors of systems have an adequate understanding of GMP/GDP and data integrity requirements, and that new systems include appropriate controls to ensure effective data management. Legacy systems are expected to meet the same basic requirements; however, full compliance may necessitate the use of additional controls, e.g. supporting administrative procedures or supplementary security hardware/software.

コンピュータ化されたシステムの設計、評価、選定のプロセスには、当該システムのデータのマネジメントと完全性の（訳注：2つの）側面についての適切な検討が含まれるべきである。規制対象となるユーザは、システムのベンダーが次のことの理解を確実なものとする。

- ・ GMP/GDP およびデータ完全性の要求事項を十分に理解している」
- ・ 「新しいシステムには効果的なデータ管理を保証するための適切なコントロールが含まれていること」

従来のシステムも同様の基本的要件を満たすことが期待される；しかしながら、完全に準拠するためには、管理手順（administrative procedures）のサポートや補助的なセキュリティハードウェア／ソフトウェアなど、追加的なコントロールの使用が必要となる場合がある。

9.1.5 Regulated users should fully understand the extent and nature of data generated by computerised systems, and a risk based approach should be taken to determining the data risk and criticality of data (including metadata) and the subsequent controls required to manage the data generated. For example:

規制の対象となるユーザは、コンピュータ化されたシステムによって生成されるデータの範囲と性質を十分に理解する必要がある。そして、データリスクとデータ（メタデータを含む）の重要性、及び生成されたデータを管理（マネージ）するために必要なそれに続く管理を決定するために、リスクベースのアプローチを取る必要がある。例えば、

9.1.5.1 In dealing with raw data, the complete capture and retention of raw data would normally be required in order to reconstruct the manufacturing event or analysis.

生データ（raw data）の取り扱いにおいて、製造面のイベント（事象）や分析を再現するためには、通常、生データの完全な捕捉と保持が必要となる。

9.1.5.2 In dealing with metadata, some metadata is critical in reconstruction of events, (e.g. user identification, times, critical process parameters, units of measure), and would be considered as ‘relevant metadata’ that should be fully captured and managed. However, non-critical meta-data such as system error logs or non-critical system checks may not require full capture and management where justified using risk management.

メタデータを扱う場合、メタデータの中にはイベントを再現する上で重要なものがあり（例：ユーザの識別、時刻、重要なプロセスパラメータ、測定単位）、完全に捕捉して管理すべき「関連メタデータ（‘relevant metadata’）」とみなされる。しかし、システム・エラー



ー・ログ (system error logs) や重要でないシステム・チェック (non-critical system checks) などの重要でないメタデータは、リスクマネジメントを用いて正当化される場合には、完全な捕捉と管理が必要でない可能性をもっている。

9.1.6 When determining data vulnerability and risk, it is important that the computerised system is considered in the context of its use within the business process. For example, the integrity of results generated by an analytical method utilising an integrated computer interface are affected by sample preparation, entry of sample weights into the system, use of the system to generate data, and processing / recording of the final result using that data. The creation and assessment of a data flow map may be useful in understanding the risks and vulnerabilities of computerised systems, particularly interfaced systems.

データの脆弱性及びリスクを判断する場合には、コンピュータ化されたシステムをビジネスプロセスの中で使用するという観点から検討することが重要である。例えば、統合されたコンピュータインターフェースを利用する分析方法によって生成された結果の完全性は、サンプルの準備、システムへのサンプル重量の入力、データを生成するためのシステムの使用、およびそのデータを使用した最終結果の処理/記録によって影響を受ける。データフローマップ (data flow map) の作成と評価は、コンピュータ化されたシステム、特にインターフェイス化されたシステムのリスクと脆弱性を理解するのに役立つであろう。

9.1.7 Consideration should be given to the inherent data integrity controls incorporated into the system and/or software, especially those that may be more vulnerable to exploits than more modern systems that have been designed to meet contemporary data management requirements. Examples of systems that may have vulnerabilities include: manual recording systems, older electronic systems with obsolete security measures, non-networked electronic systems and those that require additional network security protection e.g. using firewalls and intrusion detection or prevention systems.

システムおよび／またはソフトウェアに組み込まれている固有のデータ完全性マネジメントについて、考慮を払うべきである。特に、同時的データマネジメント要求 (contemporary data management requirements) に合致するように設計されている最新のシステムよりも、エクスプロイト (exploits: ネットより「ソフトウェアやシステムが内包しているセキュリティの脆弱性」) に対して脆弱な可能性がある。脆弱である可能性をもつかもしれないシステムの事例は、次のものが含まれる:

- ・手動による記録システム (manual recording systems) ;
- ・旧式のセキュリティ対策が施された古い電子システム
(older electronic systems with obsolete security measures) ;
- ・ネットワーク化されていない電子システム (non-networked electronic systems) ;
- ・ファイアウォールや侵入検知・防止システムなどを使用して追加のネットワークセキュリティ保護を必要とするシステム ;



9.1.8 During inspection of computerised systems, inspectors are recommended to utilise the company's expertise during assessment. Asking and instructing the company's representatives to facilitate access and navigation can aid in the inspection of the system.

コンピュータ化されたシステムの査察では、査察官は評価の際に当該企業の専門知識を活用することを推奨する。企業の代表者に、アクセス (access) とナビゲーション (navigation : 運営) を容易にするように求め、指示することは、システムの査察に役立つ。

9.1.9 The guidance herein is intended to provide specific considerations for data integrity in the context of computerised systems. Further guidance regarding good practices for computerised systems may be found in the PIC/S Good Practices for Computerised Systems in Regulated "GxP" Environments (PI 011).

ここに記載されているガイダンスは、コンピュータ化されたシステムにおけるデータの完全性に関する具体的な考慮事項を提供することを目的としている。コンピュータ化したシステムの適正規範に関する更なるガイダンスは、PIC/S Good Practices for Computerised Systems in Regulated "GxP" Environments (PI 011)に記載されている。

9.1.10 The principles herein apply equally to circumstances where the provision of computerised systems is outsourced. In these cases, the regulated entity retains the responsibility to ensure that outsourced services are managed and assessed in accordance with GMP/GDP requirements, and that appropriate data management and integrity controls are understood by both parties and effectively implemented.

ここでの原則は、コンピュータ化システムの提供を外部に委託する場合にも、同様に適用される。このような場合、規制対象となる企業は、外部委託されたサービスがGMP/GDPの要求事項に従って管理・評価されていること、また、適切なデータマネジメントおよび完全性管理 (integrity controls) が双方で理解され、効果的に実施されていることを保証する責任を有する。

9.2 Qualification and validation of computerised systems

コンピュータ化されたシステムの適格性およびバリデーション

9.2.1 The qualification and validation of computerised systems should be performed in accordance with the relevant GMP/GDP guidelines; the tables below provide clarification regarding specific expectations for ensuring good data governance practices for computerised systems.

コンピュータ化したシステムの適格性評価およびバリデーションは、関連するGMP/GDPガイドラインに従って実施するべきである；以下の表は、コンピュータ化したシステムの適正なデータガバナンスを確保するための具体的な期待事項を明確にしたものである。



- 9.2.2 Validation alone does not necessarily guarantee that records generated are necessarily adequately protected and validated systems may be vulnerable to loss and alteration by accidental or malicious means. Thus, validation should be supplemented by appropriate administrative and physical controls, as well as training of users.

バリデーションのみでは、生成された記録が適切に保護されていることを必ずしも保証するものではなく、バリデーションされたシステムは、偶発的または悪意のある手段（malicious means）による損失や改ざんに対して脆弱である可能性が存在している。したがって、バリデーションはユーザのトレーニングのみならず、適切な管理および物理的コントロール（appropriate administrative and physical controls）によって補完されるべきである。

9.3 Validation and Maintenance バリデーションとメンテナンス

| Item: | System Validation & Maintenance システムのバリデーションとメンテナンス |
|-------|---|
| 1. | <p>Expectation 期待されること</p> <p>Regulated companies should document and implement appropriate controls to ensure that data management and integrity requirements are considered in the initial stages of system procurement and throughout system and data lifecycle.</p> <p>For regulated users, Functional Specifications (FS) and/or User Requirement Specifications (URS) should adequately address data management and integrity requirements.</p> <p>規制対象となる企業は、システム調達初期段階、およびシステムとデータのライフサイクル全体を通じて、データ管理および完全性の要件が考慮されていることを保証するために、適切な管理を文書化し、実施しなければならない。</p> <p>規制対象となるユーザに対しては、機能仕様書（Functional Specifications : FS）および／またはユーザ要求仕様書（User Requirement Specifications : URS）が、データマネジメント及びデータ完全性の要件を適切に言及すべきである。</p> <p>Specific attention should be paid to the purchase of GMP/GDP critical equipment to ensure that systems are appropriately evaluated for data integrity controls prior to purchase.</p> <p>購入に先立ち、システムがデータ完全性の管理について適切に評価されることを確実にするために、GMP/GDPにとって重要な機器の購入に特に注意を払うべきである。</p> <p>Legacy systems (existing systems in use) should be evaluated to determine whether existing system configuration and functionality permits the appropriate control of data in accordance with good data management and integrity practices. Where system functionality or design of these systems does not provide an appropriate level of control, additional controls should be considered and implemented.</p> <p>レガシー (legacy) システム（使用中の既存システム）は、既存のシステム構成と機能</p> |



性が、適正データマネジメントと完全性の規範に従ったデータの適切な管理を可能にするかどうかを判断するために、評価を行うべきである。これらのシステムの機能や設計が適切なレベルの管理を提供しない場合は、追加の管理を検討し、実施する必要がある。

Potential risk of not meeting expectations/items to be checked

期待に合致しない場合の潜在的なリスク / チェックすべき項目

- Inadequate consideration of DI requirements may result in the purchase of software systems that do not include the basic functionality required to meet data management and integrity expectations.

DI要件の不適切な考慮は、データマネジメントや完全性に関する期待に合致させることが必要な基本的機能を含んでいないソフトウェアシステムを購入することになる可能性が生じる可能性がある。

- Inspectors should verify that the implementation of new systems followed a process that gave adequate consideration to DI principles.

査察官は、新しいシステムの導入が、DIの原則を適切に考慮したプロセスに従っていることを確認すべきである。

- Some legacy systems may not include appropriate controls for data management, which may allow the manipulation of data with a low probability of detection.

レガシーシステム（訳注：現在運用中のシステム）の中には、データマネジメントのための適切な管理が含まれていないものがある。これによって、発見される確率の低いデータ取り扱いが可能となる場合がある。

- Assessments of existing systems should be available and provide an overview of any vulnerabilities and list any additional controls implemented to assure data integrity. Additional controls should be appropriately validated and may include:

既存システムの評価を入手し、脆弱性の概要を示し、データの完全性を保証するために実施されるべき追加の管理策を列挙すべきである。追加の管理策は適切に検証されるべきであり、次のようなものが考えられる。

- Using operating system functionality (e.g. Windows Active Directory groups) to assign users and their access privileges where system software does not include administrative controls to control user privileges;

システムソフトウェアが、ユーザ権限 (user privileges) を制御するための管理コン

トロールを含んでいない場合に、ユーザとそのアクセス権限 (access privileges) を割り当てるために、オペレーティングシステムの機能 (Windows Active Directoryのグループなど) を使用する。

- Configuring operating system file/folder permissions to prevent modification/deletion of files when the modification/deletion of data files cannot be controlled by system software; or

データファイルの変更／削除をシステムソフトウェアで制御できない場合に、ファイルの変更／削除を防止するためにオペレーティングシステムのファイル／フォルダの権限を設定すること。

- Implementation of hybrid or manual systems to provide control of data generated.

生成されたデータの制御を行うためのハイブリッドシステムまたは手動システムの導入。

Expectation 期待されること

Regulated users should have an inventory of all computerised systems in use. The list should include reference to:

法的規制を受けるユーザは、使用中のすべてのコンピュータシステムの一覧表を持つべきである。このリストには以下の事項を含むべきである。

- The name, location and primary function of each computerised system;
各コンピュータシステムの名称、設置場所および主要機能。
- Assessments of the function and criticality of the system and associated data; (e.g. direct GMP/GDP impact, indirect impact, none)

当該システムおよび関連データの機能および重要性の評価 (例: GMP/GDPへの直接的な影響、間接的な影響、影響なし)

- The current validation status of each system and reference to existing validation documents.

各システムの現在のバリデーション状況 (status)、及び既存のバリデーション文

書への参照。

Risk assessments should be in place for each system, specifically assessing the necessary controls to ensure data integrity. The level and extent of validation of controls for data integrity should be determined based on the criticality of the system and process and potential risk to product quality, e.g. processes or systems that generate or control batch release data would generally require greater control than those systems managing less critical data or processes.

リスクアセスメントは各システムに対して適切に実施すべきであり、特にデータの完全性を確保するために必要なコントロールを評価する。データの完全性を確保するための管理のレベル及びバリデーションの程度は、「システム及びプロセスの重要性」及び「製品品質に対する潜在的なリスク」に基づいて決定すべきである。例えば、バッチ出荷データを生成する、又は管理するプロセス又はシステムは、一般的に重要性の低いデータ又はプロセスを管理するシステムよりも大きな管理を必要とするであろう。

Consideration should also be given to those systems with higher potential for disaster, malfunction or situations in which the system becomes inoperative.

また、災害 (disaster) や誤動作 (malfunction)、あるいは「システムが機能しなくなる状況」についても考慮する必要がある。

Assessments should also review the vulnerability of the system to inadvertent or unauthorised changes to critical configuration settings or manipulation of data. All controls should be documented and their effectiveness verified.

評価では、重要な（訳注：機器やシステムの）構成設定に対する不注意な (inadvertent) または無許可 (unauthorised) の変更、あるいはデータの操作 (manipulation) に対するシステムの脆弱性 (vulnerability) についても検討する必要があります。すべての管理は文書化され、その有効性が検証すべきである。

2.

Potential risk of not meeting expectations/items to be checked

期待を満たさない場合の潜在的なリスク / チェックすべき項目

- Companies that do not have adequate visibility of all computerised systems in place may overlook the criticality of systems and may thus create vulnerabilities within the data lifecycle.

導入されているすべてのコンピュータ・システムを適切に見通す (visibility) ことができていない企業は、システムの重要性を見落とし、データ・ライフサイクルの中で脆弱性を生み出す可能性がある。

- An inventory list serves to clearly communicate all systems in place and their criticality, ensuring that any changes or modifications to these systems are controlled.

インベントリリスト (inventory list : 訳注参照) は、設置されている全てのシステムとその重要性を明確に伝え、これらのシステムへの変更や修正が確実に管理されるようにする。

訳注：訳語としては「資産台帳」になる。



| | |
|---|---|
| | <ul style="list-style-type: none"> • Verify that risk assessments are in place for critical processing equipment and data acquisition systems. A lack of thorough assessment of system impact may lead to a lack of appropriate validation and system control. Examples of critical systems to review include: 重要な処理装置およびデータ収集システムについて、リスクアセスメントが実施されていることを確認する。システムへの影響（インパクト）の十分なアセスメントを行わないことの欠陥は、適切なバリデーションやシステム管理の欠陥を導く可能性をもっている。レビューすべき重要なシステムの例は以下の通りである： <ul style="list-style-type: none"> - systems used to control the purchasing and status of products and materials; 製品や物品の購入や状態を管理するためのシステム； - systems for the control and data acquisition for critical manufacturing processes; 重要な製造プロセスの制御およびデータ取得のためのシステム； - systems that generate, store or process data that is used to determine batch quality; バッチの品質を決定するために使用されるデータを生成、保存、または処理するシステム。 - systems that generate data that is included in the batch processing or packaging records; and バッチ処理または包装の記録に含まれるデータを生成するシステム；および - systems used in the decision process for the release of products. 製品の出荷に関する意思決定プロセスに使用されるシステム。 |
| 3 | <p>Expectation 期待されること</p> <p>For new systems, a Validation Summary Report for each computerised system (written and approved in accordance with Annex 15 requirements) should be in place and state (or provide reference to) at least the following items:</p> <p>新規システムについては、各コンピュータ化システムのバリデーション概要報告書（PIC/S GMPの付属書15の要求事項に従って作成され、承認されたもの）が整備され、少なくとも以下の項目が記載されている（または参照されている）必要がある。</p> <ul style="list-style-type: none"> - Critical system configuration details and controls for restricting access to configuration and any changes (change management). 重要なシステム構成の詳細と、構成および変更点へのアクセスを制限するための管理（変更マネジメント）。 - A list of all currently approved normal and administrative users specifying the username and the role of the user. 現在承認されているすべての通常ユーザおよび管理権限を持つユーザ（administrative users）のリスト（ユーザ名およびユーザの役割を明記する）； - Frequency of review of audit trails and system logs. 監査証跡（audit trails）およびシステムログ（system logs）のレビューの頻度。； |

| | |
|--|--|
| | <p>- Procedures for: 以下の手順 ;</p> <ul style="list-style-type: none"> • creating new system user; 新しいシステムユーザの作成 ; • modifying or changing privileges for an existing user; 既存のユーザの特権を修正または変更する ; • defining the combination or format of passwords for each system 各システムのパスワードの組み合わせまたは形式の定義 ; • reviewing and deleting users; ユーザについてのレビューおよび削除 ; • back-up processes and frequency; バックアップのプロセスおよび頻度 ; • disaster recovery; 障害回復 ; • data archiving (processes and responsibilities), including procedures for accessing and reading archived data; データのアーカイブ（プロセスおよび責任）。これには、アーカイブされたデータへのアクセスおよび読み取りの手順を含む ; • approving locations for data storage. データ保管場所の承認; <p>- The report should explain how the original data are retained with relevant metadata in a form that permits the reconstruction of the manufacturing process or the analytical activity. 報告書は、製造プロセスまたは分析活動の再構成を可能にする形で、オリジナルデータが、関連するメタデータとともにどのように保持されているかを説明すべきである。</p> <p>For existing systems, documents specifying the above requirements should be available; however, need not be compiled into the Validation Summary report. These documents should be maintained and updated as necessary by the regulated user.</p> <p>既存のシステムは、上記の要求事項を明記した文書が、利用可能性であること ; しかしながら、バリデーション要約報告書にまとめる必要はない。これらの文書は、法規制を受けるユーザが、必要に応じて維持・更新する必要がある。</p> |
| | <p>Potential risk of not meeting expectations/items to be checked 期待を満たさない場合の潜在的なリスク / チェックすべき項目</p> <ul style="list-style-type: none"> • Check that validation systems and reports specifically address data integrity requirements following GMP/GDP requirements and considering ALCOA principles. バリデーションシステム及び報告書が、GMP/GDP の要求事項に従い、かつ ALCOA の原則を考慮した上で、データの完全性に関する要求事項を明確に扱っていることを確認する。 • System configuration and segregation of duties (e.g. authorisation to generate data should be separate to authorisation to verify data) should be defined prior to validation, and verified as effective during testing. システム構成及び職務の分離（例：データを生成する権限とデータを検証する権限 |

| | |
|--|--|
| | <p>は別であること) は、バリデーションに先立って定義され、テストの間に有効であることを確認するべきである。</p> <ul style="list-style-type: none"> • Check the procedures for system access to ensure modifications or changes to systems are restricted and subject to change control management. <p>システムへの修正または変更が制限され、変更管理マネジメントの対象となっていることを確認するために、システムアクセスの手順を確認する。</p> <ul style="list-style-type: none"> • Ensure that system administrator access is restricted to authorised persons and is not used for routine operations. <p>システム管理者のアクセス権は、権限のある人に制限されており、日常業務に使用されていないことを確認する。</p> <ul style="list-style-type: none"> • Check the procedures for granting, modifying and removing access to computerised systems to ensure these activities are controlled. Check the currency of user access logs and privilege levels, there should be no unauthorised users to the system and access accounts should be kept up to date. <p>コンピュータ化システムへの、アクセスを許可すること (granting)、変更すること (modifying)、削除すること (removing) のための手順をチェックする。これは、それらの活動が確実に管理されていることを確認するためである。ユーザのアクセスログ (user access logs) と権限レベル (privilege levels) の最新性をチェックし、システムに無許可のユーザが存在しないようにし、アクセスアカウントが最新の状態に保たれていること。</p> <ul style="list-style-type: none"> • There should also be restrictions to prevent users from amending audit trail functions and from changing any pre-defined directory paths where data files are to be stored. <p>また、ユーザが監査証跡の機能を修正したり、データファイルを保存するために事前に設定されたディレクトリパスを変更したりすることができないような、制限を設ける必要がある。</p> |
| | <p>Expectation 期待されること</p> <p>Companies should have a Validation Master Plan in place that includes specific policies and validation requirements for computerised systems and the integrity of such systems and associated data.</p> <p>企業は、コンピュータ化されたシステムに対する具体的な方針とバリデーション要件、及びそのようなシステムと関連するデータの整合性を含むバリデーションマスタープランを持つべきである。</p> <p>The extent of validation for computerised systems should be determined based on risk. Further guidance regarding assessing validation requirements for computerised systems may be found in PI 011.</p> <p>コンピュータ化されたシステムのバリデーションの範囲は、リスクに基づいて決定するべきである。コンピュータ化されたシステムのバリデーション要件の評価に関する詳細なガイダンスは、PI 011 (GOOD PRACTICES FOR COMPUTERISED SYSTEMS IN REGULATED "GXP" ENVIRONMENTS) に記載されている。</p> |

Before a system is put into routine use, it should be challenged with defined tests for conformance with the acceptance criteria.

システムを日常的に使用する前に、受け入れ基準に適合しているかどうかを定義されたテストで確認する必要がある。

It would be expected that a prospective validation for computerised systems is conducted. Appropriate validation data should be available for systems already in-use.

コンピュータ化されたシステムの予測的バリデーションを実施することが期待される。既に使用されているシステムについては、適切なバリデーションデータを利用可能とすること。

Computerised system validation should be designed according to GMP Annex 15 with URS, DQ, FAT, SAT, IQ, OQ and PQ tests as necessary.

コンピュータ化されたシステムのバリデーションは、必要に応じてURS（ユーザ要求仕様書）、DQ（設計時の適格性評価）、FAT（Factory Acceptance Testing；工場出荷試験）、SAT（Site acceptance testing；現場受入試験）、IQ（設備据付時の適格性評価）、OQ（運転時適格性評価）及びPQ（稼働時適格性評価）の試験を伴うGMP付属書15に従って設計されるべきである。

The qualification testing approach should be tailored for the specific system under validation, and should be justified by the regulated user. Qualification may include Design Qualification (DQ); Installation qualification (IQ); Operational Qualification (OQ); and Performance Qualification (PQ). In particular, specific tests should be designed in order to challenge those areas where data quality or integrity is at risk.

適性評価の試験の方法は、バリデーションの対象となる特定のシステムに合わせて調整すべきであり、それは規制対象となるユーザがその論理的正当性の説明をすべきである。適格性評価には、DQ、IQ、OQ、PQが含まれるであろう。特に、それらの試験は、データの品質または完全性がリスクにさらされている領域に対してチャレンジするように、設計する必要すべきである。

Companies should ensure that computerised systems are qualified for their intended use. Companies should therefore not place sole reliance on vendor qualification packages; validation exercises should include specific tests to ensure data integrity is maintained during operations that reflect normal and intended use.

更に、企業は、コンピュータ化されたシステムが、その意図された用途に適合していることを確認すべきである。したがって企業は、ベンダーの適格性評価パッケージのみに依存すべきではない；バリデーション作業には、通常の使用および意図した使用を反映させた操作中に、データの整合性が維持されることを確認するための特定のテストを含むべきである。

The number of tests should be guided by a risk assessment but the critical functionalities should be at least identified and tested, e.g., certain PLCs and systems based on basic algorithms or logic sets, the functional testing may provide adequate assurance of reliability of the computerised system. For critical and/or more complex systems, detailed verification testing is required during IQ, OQ & PQ stages.

| | |
|----|--|
| | <p>テストの数は、リスクアセスメントによって導かれるべきである。しかし、重要な機能性は少なくとも、それに特定してテストする必要があります。例えば、基本的なアルゴリズムや、ロジックセットに基づくPLCやシステムは、その機能テスト (functional testing) は、コンピュータ化されたシステムの信頼性を十分に保証することができるであろう。重要なシステム及び／又は、より複雑なシステムについては、IQ、OQ、PQの段階で詳細な検証試験 (detailed verification testing) が必要である。</p> |
| 4. | <p>Potential risk of not meeting expectations/items to be checked 期待を満たさない場合の潜在的なリスク / チェックすべき項目</p> <ul style="list-style-type: none"> • Check that validation documents include specific provisions for data integrity; validation reports should specifically address data integrity principles and demonstrate through design and testing that adequate controls are in place. バリデーション文書にデータの完全性に関する具体的な規定が含まれていることをチェックする；バリデーション報告書は、データの完全性の原則を具体的に取り上げ、適切な管理が行われていることを設計とテストによって示すべきである。 • Unvalidated systems may present a significant vulnerability regarding data integrity as user access and system configuration may allow data amendment. バリデーションが行われていないシステムは、ユーザのアクセスやシステム構成によってデータの修正が可能となるため、データの完全性に関して重大な脆弱性をもたらす可能性がある。 • Check that end-user testing includes test-scripts designed to demonstrate that software not only meets the requirements of the vendor, but is fit for its intended use. エンドユーザのテストには、ソフトウェアがベンダーの要求事項を満たしているだけでなく、意図した用途に適合していることを実証するために設計されたテストスクリプト (訳注参照) が含まれていることを確認する。 <p>訳注 (ネットより) : アプリケーションを自動的にテストするための一連の命令のこと。 テストスクリプトは自動化テスト環境で使用される。</p> |

5.

Expectation 期待されること**Periodic System Evaluation 定期的なシステム評価**

Computerised systems should be evaluated periodically in order to ensure continued compliance with respect to data integrity controls. The evaluation should include deviations, changes (including any cumulative effect of changes), upgrade history, performance and maintenance, and assess whether these changes have had any detrimental effect on data management and integrity controls.

コンピュータ化されたシステムは、データ完全性管理に関する継続的なコンプライアンス（法令順守）を確保するために、定期的に評価すべきである。評価には、逸脱、変更（変更の如何なる累積的影響（cumulative effect）も含む）、アップグレードの履歴、性能及びメンテナンスを含み、これらの変更がデータ管理および完全性の管理に有害な影響を与えていないかどうかを評価すべきである。

The frequency of the re-evaluation should be based on a risk assessment depending on the criticality of the computerised systems considering the cumulative effect of changes to the system since last review. The assessment performed should be documented.

再評価の頻度は、前回のレビュー以降に行われたシステムへの変更の累積的影響を考慮し、コンピュータ化したシステムの重要性に応じたリスク評価に基づくべきである。実施した評価は文書化すべきである。

Potential risk of not meeting expectations/items to be checked**期待を満たさない場合の潜在的なリスク / チェックすべき項目**

- Check that re-validation reviews for computerised systems are outlined within validation schedules.

コンピュータ化されたシステムの再バリデーションのレビューは、バリデーションのスケジュールに概説されていることを確認する。

- Verify that systems have been subject to periodic review, particularly with respect to any potential vulnerabilities regarding data integrity.

システムが定期的なレビューを受けていること、特にデータの完全性に関する潜在的な脆弱性について確認すること。

- Any issues identified, such as limitations of current software/hardware should be addressed in a timely manner and corrective and preventive actions, and interim controls should be available and implemented to manage any identified risks.

現行のソフトウェア/ハードウェアの限界などの、特定された問題は、適時に対処し、是正措置および予防措置を行い、そして特定されたリスクを管理するための暫定的な管理が利用可能であり、かつ実施するべきである。



6.

Expectation 期待されること

Operating systems and network components (including hardware) should be updated in a timely manner according to vendor recommendations and migration of applications from older to newer platforms should be planned and conducted in advance of the time before the platforms reach an unsupported state which may affect the management and integrity of data generated by the system.

オペレーティングシステムおよびネットワークコンポーネント（ハードウェアを含む）は、ベンダーの推奨に従って適時に更新するべきである。古いプラットフォームから新しいプラットフォームへのアプリケーションの移行（migration）は、システムで生成されたデータの管理および完全性に影響を与える可能性のあるプラットフォームがサポートされない状態になる前に、事前に計画し、実施するべきである。

Security patches for operating systems and network components should be applied in a controlled and timely manner according to vendor recommendations in order to maintain data security. The application of security patches should be performed in accordance with change management principles.

データのセキュリティを維持するために、オペレーティングシステム及びネットワークコンポーネントのセキュリティパッチ（security patches）は、ベンダーの推奨に従い、管理された方法でタイムリーに適用するべきである。セキュリティパッチの適用は、変更管理の原則に基づいて実施するべきである。

訳注（ネットより）：「セキュリティパッチ」とは、プログラムに脆弱性やセキュリティホールなどが発見された際に、それらの問題を修正するためのプログラムのことである。

Where unsupported operating systems are maintained, i.e. old operating systems are used even after they run out of support by the vendor or supported versions are not security patched, the systems (servers) should be isolated as much as possible from the rest of the network. Remaining interfaces and data transfer to/from other equipment should be carefully designed, configured and qualified to prevent exploitation of the vulnerabilities caused by the unsupported operating system.

サポートされていないオペレーティングシステムが維持されている場合、すなわち、ベンダーのサポートが終了した後も、古いオペレーティングシステムを使用している場合、サポートされているバージョンにセキュリティパッチが適用されていない場合は、そのシステム（サーバ）をネットワークのレスト（rest ; REST; Representational State Transfer : 訳注参照）から可能な限り隔離する必要がある。残りのインターフェースや他の機器との間のデータ転送は、サポートされていないOSに起因する脆弱性が悪用されないように、慎重に設計、設定、適格性を確保する必要がある。

訳注（ネットより）：フィールディング氏が示した（本来の）RESTの設計原則は主として以下の4つの項目から成る。

- ① 「セッションなどの状態管理を行わず、やり取りされる情報はそれ自体で完結して解釈することができる」（WebではHTTP自体にはセッション管理の機構はない）、
- ② 「情報を操作する命令の体系が予め定義・共有されている」（WebではHTTPメソッドに相当）



| | |
|--|---|
| | <p>③ 「すべての情報は汎用的な構文で一意に識別される」 (URL/URIに相当)</p> <p>④ 「情報の一部として、別の状態や別の情報への参照を含めることができる (ハイパーメディア的な書式で情報を表現する)」 (HTMLやXMLに相当)</p> <p>の4つである。</p> <p>Remote access to unsupported systems should be carefully evaluated due to inherent vulnerability risks.</p> <p>サポートされていないシステムへのリモートアクセスは、固有の脆弱性のリスクがあるため、慎重に評価する必要がある。</p> |
| | <p>Potential risk of not meeting expectations/items to be checked 期待を満たさない場合の潜在的なリスク / チェックすべき項目</p> <ul style="list-style-type: none"> • Verify that system updates are performed in a controlled and timely manner. Older systems should be reviewed critically to determine whether appropriate data integrity controls are integrated, or, (where integrated controls are not possible) that appropriate administrative controls have been implemented and are effective. <p>システムの更新が、管理された方法でタイムリーに行われていることを確認する。古いシステムは、適切なデータ完全性管理が統合されているかどうか、または（統合された管理が不可能な場合）適切なアドミニ管理（administrative controls）が実施され、有効であるかどうかを判断するために、批判的にレビューする必要がある。</p> |

9.4 Data Transfer データ転送

| Item: | Data transfer and migration データ転送とマイグレーション |
|-------|---|
| 1. | <p>訳者注（ネットより）：マイグレーション（Migration）は、IT用語としては既存システムやソフトウェア、データなどを別の環境に移転したり、新しい環境に移行しつてりすることを意味する。</p> <p>Expectation 期待されること</p> <p>Interfaces should be assessed and addressed during validation to ensure the correct and complete transfer of data.</p> <p>インターフェースは、データが正しく、かつ完全に転送されることを保証するために、バリデーションにおいて評価し、対処すべきである。</p> <p>Interfaces should include appropriate built-in checks for the correct and secure entry and processing of data, in order to minimise data integrity risks. Verification methods may include the use of:</p> <p>インターフェースは、データの完全性に関するリスクを最小限にするために、データを正しく安全に入力及び処理するための適切なチェック機能を組み込むべきである。検証方法には以下のようなものがある：</p> |



| | |
|----|---|
| | <p>Secure transfer 安全な転送（? : 訳語不明）；</p> <p>Encryption 暗号化；</p> <p>Checksums チェックサム；</p> <p>Where applicable, interfaces between systems should be designed and qualified to include an automated transfer of GMP/GDP data.</p> <p>該当する場合、システム間のインターフェースは、GMP/GDP データの自動転送を含むように設計され、適格性評価をするべきである。</p> <p>Potential risk of not meeting expectations/items to be checked 期待を満たさない場合の潜在的なリスク / チェックすべき項目</p> <ul style="list-style-type: none"> • Interfaces between computerised systems present a risk whereby data may be inadvertently lost, amended or transcribed incorrectly during the transfer process. コンピュータシステム間のインターフェースは、転送プロセス中にデータが誤って失われたり、修正されたり、誤って転記されたりするリスクがある。 • Ensure data is transferred directly to the secure location/database and not simply copied from the local drive (where it may have the potential to be altered). データが安全な場所/データベースに直接転送され、（改ざんされる可能性のある）ローカルドライブからたやすくコピーされないことを確認する。 • Temporary data storage on local computerised systems (e.g. instrument computer) before transfer to final storage or data processing location creates an opportunity for data to be deleted or manipulated. This is a particular risk in the case of ‘standalone’ (non-networked) systems. Ensure the environment that initially stores the data has appropriate DI controls in place. 最終的な保存場所またはデータ処理場所に移動する前に、ローカルのコンピュータシステム（機器のコンピュータなど）に一時的にデータを保存すると、データが削除されたり、または操作されたりする可能性がある。これは「スタンドアロン」（非ネットワーク型）システムの場合には特にリスクが高い。データを最初に保存する環境に、適切なDI管理が存在していることを確認する。 • Well designed and qualified automated data transfer is much morereliable than any manual data transfer conducted by humans. 十分に設計され、適格性評価をされた自動データ転送は、ヒトが行う手動のデータ転送よりもはるかに信頼性が高い。 |
| 2. | <p>Expectation 期待されること</p> <p>Where system software (including operating system) is installed or updated, the user should ensure that existing and archived data can be read by the new software. Where necessary this may require conversion of existing archived data to the new format.</p> <p>システム・ソフトウェア（オペレーティング・システムを含む）をインストールまたは更新する場合、ユーザは、既存のデータ及びアーカイブされたデータが、新しいソフトウェアで読み取れることを確認すべきである。必要に応じて、既存のアー</p> |



| | |
|----|---|
| | <p>カイク・データを新しいフォーマットに変換する必要がある。</p> <p>Where conversion to the new data format of the new software is not possible, the old software should be maintained, e.g. installed in one computer or other technical solution, and also available as a backup media in order to have the opportunity to read the archived data in case of an investigation.</p> <p>新しいソフトウェアの新しいデータ形式への変換が不可能な場合は、古いソフトウェアを維持する必要がある。例えば、1台のコンピュータ又は、その他の技術的ソリューションにインストールし、調査の際にアーカイブされたデータを読み取る機会を持てるように、バックアップメディアとしても利用できる。</p> <p>Potential risk of not meeting expectations/items to be checked 期待を満たさない場合の潜在的なリスク / チェックすべき項目</p> <ul style="list-style-type: none"> It is important that data is readable in its original form throughout the data lifecycle, and therefore users should maintain the readability of data, which may require maintaining access to superseded software. <p>データはそのデータライフサイクルを通して、元の形式 (original form) で読み取れることが重要である。それゆえ、ユーザは、既存のデータおよびアーカイブされたデータが新しいソフトウェアで読み取れることを確認する必要がある。場合によっては、差し替えたソフトウェアへのアクセスを維持できる必要が生じる可能性がある (訳注: フォーマットを変換するなどして)。</p> <ul style="list-style-type: none"> The migration of data from one system to another should be performed in a controlled manner, in accordance with documented protocols, and should include appropriate verification of the complete migration of data. <p>あるシステムから他のシステムへのデータの変換 (migration) が、文書化されたプロトコルに従って、管理された方法で行えないのであれば、データの変換の適切な確認 (verification) を含めるべきである。</p> |
| 3. | <p>Expectation 期待されること</p> <p>When legacy systems software can no longer be supported, consideration should be given to maintaining the software for data accessibility purposes (for as long possible depending upon the specific retention requirements). This may be achieved by maintaining software in a virtual environment.</p> <p>レガシーシステム (訳注: 現在使用しているシステム) のソフトウェアがサポートされなくなった場合、データアクセシビリティの目的で、そのソフトウェアを維持することを考慮しなければならない (特定の保存要件に応じて可能な限り長く)。これは、仮想環境 (virtual environment) でソフトウェアを維持することで実現できる。</p> <p>Migration to an alternative file format that retains as much as possible of the 'true copy' attributes of the data may be necessary with increasing age of the legacy data.</p> <p>レガシーデータの年代が上がるにつれて、データの「真正コピー」属性を可能な限り維持する代替ファイル形式への移行が必要になる場合がある。</p> <p>Where migration with full original data functionality is not technically possible, options</p> |

| | |
|--|---|
| | <p>should be assessed based on risk and the importance of the data over time. The migration file format should be selected considering the balance of risk between long-term accessibility versus the possibility of reduced dynamic data functionality (e.g. data interrogation, trending, re- processing, etc.) The risk assessment should also review the vulnerability of the system to inadvertent or unauthorised changes to critical configuration settings or manipulation of data. All controls to mitigate risk should be documented and their effectiveness verified. It is recognised that the need to maintain accessibility may require migration to a file format that loses some attributes and/or dynamic data functionality.</p> <p>元のデータの機能を完全に維持したまま移行することが技術的に不可能な場合は、選択肢の一つは、リスク及び時間的なデータの重要性に基づいて評価することである。その移行のためのファイル形式は、「長期的なアクセス性」と「動的なデータ機能（例えば、データの照会、トレンド、再加工（re-processing）など）が低下する可能性」との間のリスクのバランスを考慮して選択するべきである。また、リスクアセスメントは、重要な構成設定に対する不注意または不正な変更、あるいはデータの操作に対するシステムの脆弱性を検討する必要がある。リスクを軽減するためのすべての管理は、これを文書化し、その有効性を検証すること。アクセシビリティ（訳注参照）を維持する必要性から、一部の属性や動的データ機能を失ったファイル形式への移行が必要となる場合があることを認識する。</p> <p>訳注（ネットより）：利用者が機器・サービスを円滑に利用できること。</p> |
| | <p>Potential risk of not meeting expectations/items to be checked</p> <p>期待を満たさない場合の潜在的なリスク／確認すべき項目</p> <p>When the software is maintained in a virtual environment, check that appropriate measures to control the software (e.g. validation status, access control by authorised persons, etc.) are in place. All controls should be documented and their effectiveness verified.</p> <p>ソフトウェアが仮想環境で管理されている場合、ソフトウェアを管理するための適切な手段（バリデーションの状態、権限のある者によるアクセス制御など）が実施されていることを確認する。すべての管理を文書化し、その有効性を検証すること。</p> |

9.5 System security for computerised systems

コンピュータ化されたシステムのシステムセキュリティ

| Item: | System security システムセキュリティ |
|-------|--|
| 1. | <p data-bbox="325 383 695 416">Expectation 期待されること</p> <p data-bbox="325 448 1374 577">User access controls shall be configured and enforced to prohibit unauthorised access to, changes to and deletion of data. The extent of security controls is dependent on the criticality of the computerised system. For example:</p> <p data-bbox="325 607 1369 781">ユーザアクセス管理は、データへの不正アクセス、データの変更およびデータの削除を抑制するために、これを設定し、実施すること。セキュリティ管理の程度は、コンピュータ化されたシステムの重要性に依存する。例えば、以下のようなものがある：</p> <ul data-bbox="325 813 1374 1133" style="list-style-type: none"> - Individual Login IDs and passwords should be set up and assigned for all staff needing to access and utilise the specific electronic system. Shared login credentials do not allow for traceability to the individual who performed the activity. For this reason, shared passwords, even for reasons of financial savings, should be prohibited. Login parameters should be verified during validation of the electronic system to ensure that login profiles, configuration and password format are clearly defined and function as intended. <p data-bbox="384 1164 1382 1581">個別のログインIDおよびパスワードは、特定の電子システムへのアクセスおよび利用を必要とするすべてのスタッフに対して、これを設定し、かつ割り当てるべきである。共有のログイン認証 (shared login credentials : 訳注参照) は、アクティビティを実行した個人への追跡ができない。この理由から、共用パスワードは、パスワードの共有は、たとえ経済的な節約のためであっても、禁止すべきである。ログインパラメータ (login parameters) は、ログインプロファイル (login profiles)、構成 (configuration) 及びパスワードの形式が明確に定義され、意図された通りに機能することを確実にするために、電子システムのバリデーション中に検証するべきである。</p> <p data-bbox="384 1610 1358 1718">訳注 (ネットより) : クレデンシャル (credentials) とは、資格、経歴、認定証、信任状などの意味を持つ英単語。情報セキュリティの分野では、認証などに用いられるID、ユーザ名、暗証番号、パスワード、生体パターンなどの識別情報の総称を指す。</p> <ul data-bbox="325 1749 1382 1879" style="list-style-type: none"> - Input of data and changes to computerised records should be made only by authorised personnel. Companies should maintain a list of authorised individuals and their access privileges for each electronic system in use. <p data-bbox="384 1908 1366 2031">データの入力およびコンピュータ記録の変更は、権限のある担当者のみが行うべきである。企業は、使用している電子システムごとに、権限を有する者のリストとそのアクセス権限を管理すべきである。</p> |



- Appropriate controls should be in place regarding the format and use of passwords, to ensure that systems are effectively secured.

システムが効果的に保護されていることを保証するために、パスワードの形式と使用に関して適切な管理を行うべきである。

- Upon initially having been granted system access, a system should allow the user to create a new password, following the normal password rules.

システムへのアクセスが最初に許可されたとき、システムは、通常のパスワード規則に従って、当該ユーザが新しいパスワードを作成できるようにすべきである。

- Systems should support different user access roles (levels) and assignment of a role should follow the least-privilege rule, i.e. assigning the minimum necessary access level for any job function. As a minimum, simple systems should have normal and admin users, but complex systems will typically requires more levels of users (e.g. a hierarchy) to effectively support access control.

システムは、異なるユーザアクセスの役割（レベル）をサポートし、役割の割り当ては、最小権限の原則（least-privilege rule : 訳注参照）に従うべきである。すなわち、全てのジョブ機能（job function）について、最小限必要なアクセスを割り当てる。少なくとも、単純なシステムには通常、ユーザと管理者ユーザがいるべきであるが、複雑なシステムでは、アクセス制御を効果的にサポートするために、より多くのレベルのユーザ（例：階層；ヒエラルキー）が必要となる。

訳注（ネットより）：最小権限の原則とは、情報セキュリティや計算機科学などの分野において、コンピューティング環境の特定の抽象化レイヤー内で全てのモジュールがその正当な目的に必要とされる情報と計算資源のみにアクセスできるように制限する設計原則である。（ウィキペディア）

- Granting of administrator access rights to computerised systems and infrastructure used to run GMP/GDP critical applications should be strictly controlled. Administrator access rights should not be given to normal users on the system (i.e. segregation of duties).

GMP/GDP にとって重要なアプリケーションを実行するために使用されるコンピュータ化されたシステムおよびインフラストラクチャ（基盤設備など）への管理者アクセス権の付与は、厳密に管理すべきである（すなわち職務の分離）。

- Normal users should not have access to critical aspects of the computerised system, e.g. system clocks, file deletion functions, etc.

通常のユーザは、コンピュータ化したシステムの重要な側面、例えばシステム時計やファイル削除機能などにアクセスしてはならない。

- Systems should be able to generate a list of users with actual access to the system, including user identification and roles. User lists should include the names or



unique identifiers that permit identification of specific individuals. The list should be used during periodic user reviews.

システムは、システムに実際にアクセスしているユーザのリストを、作成できるべきである。これには、ユーザの識別と役割が含まれる。ユーザ・リストには、特定の個人の識別を可能にする名前または一意の識別子 (unique identifier) を含めるべきである。このリストは、定期的なユーザレビューの際に使用すべきである。

- Systems should be able to generate a list of successful and unsuccessful login attempts, including:

システムは、成功したログイン試行と失敗したログイン試行のリストを生成することができる。それには以下のものが含まれる：

- User identification ユーザの識別
- User access role ユーザアクセスロール (訳注：日本語のIT用語不明)
- Date and time of the attempted login, either in local time or traceable to local time ログインが試みられた日時、現地時間または現地時間から追跡可能な時間のいずれか、とする
- Session length, in the case of successful logins
ログインに成功した場合のセッションの長さ
- User access controls should ensure strict segregation of duties (i.e. that all users on a system who are conducting normal work tasks should have only normal access rights). Normally, users with elevated access rights (e.g. admin) should not conduct normal worktasks on the system.
ユーザのアクセス管理は、厳密な職務分離を保证する必要がある (すなわち、システム上で通常の作業タスクを行っているすべてのユーザは、通常のアクセス権のみを持つべきである)。通常、高められたアクセス権を持つユーザ (例えば、admin) は、システム上で通常の作業タスクを行うべきではない。
- System administrators should normally be independent from users performing the task, and have no involvement or interest in the outcome of the data generated or available in the electronic system. For example, QC supervisors and managers should not be assigned as the system administrators for electronic systems in their laboratories (e.g. HPLC, GC, UV-Vis). Typically, individuals outside of the quality and production organisations (e.g. Information Technology administrators) should serve as the system administrators and have enhanced permission levels.

システム管理者 (system administrators) は通常、タスクを実行するユーザから独立しているべきであり、電子システムで生成または利用可能なデータの結果に関与または関心を持つべきではない。例えば、QC部門の監督者 (supervisors) 及び管理者 (managers) は、各自のラボの電子システム (HPLC、GC、UV-Visなど)



のシステム管理者として割り当てられるべきではない。一般的に、品質（訳注：QA・QC）及び生産の組織外部の個人（例えば、情報技術管理者；Information Technology administrators）がシステム管理者としてその任を務め強化された権限レベル（enhanced permission levels）を持つべきである。

- For smaller organisations, it may be permissible for a nominated person in the quality unit or production department to hold access as the system administrator; however, in these cases the administrator access should not be used for performing routine operations and the user should hold a second and restricted access for performing routine operations. In these cases all administrator activities conducted should be recorded and approved within the quality system.

小規模な組織では、品質部門（quality unit：訳注 QA+QC）または生産部門で指名された人がシステム管理者としてアクセス権を持つことが許される可能性がある。しかしながら、このような場合、管理者アクセス（administrator access）は日常業務の実行に使用すべきではなく、そのユーザは日常業務を実行するために2番目の制限されたアクセス権（second and restricted access）を持つべきである。このような場合、実施されたすべての管理者活動（administrator activities）は、品質システム（quality system）内に記録され、承認されるべきである。

- Any request for new users, new privileges of users should be authorised by appropriate personnel (e.g. line manager and system owner) and forwarded to the system administrator in a traceable way in accordance with a standard procedure.
- 新しいユーザやユーザの新しい権限（privileges）の要求は、適切な担当者（ラインマネージャ（訳注参照）やシステム所有者など）によって承認され、標準的な手順に従って追跡可能な方法でシステム管理者に転送するべきである。

訳注（ネットより）：「ラインマネージャ」とは、現場の管理職であり、意思決定権を持つ人。

- Computerised systems giving access to GMP/GDP critical data or operations should have an inactivity logout, which, either at the application or the operating system level, logs out a user who has been inactive longer than a predefined time. The time should be shorter, rather than longer and should typically be set to prevent unauthorised access to systems. Upon activation of the inactivity logout, the system should require the user to go through the normal authentication procedure to login again.

GMP/GDPに関わる重要なデータや業務にアクセスを与えられるコンピュータ化したシステムは、非活動時のログアウト機能（inactivity logout）を設けること。この機能は、アプリケーションレベルまたは、オペレーティングシステムレベルで、非活動時の時間があらかじめ設定された時間を超えたユーザをログアウトさせるものである。この時間は長くするのではなく、むしろ短くし、通常はシステムへの不正なアクセス（unauthorised access）を防ぐように設定する。



| | |
|--|---|
| | <p>非活動時のログアウトが有効になると、そのシステムはユーザに対して通常の認証手続きを経て、再度ログインすることを求めるべきである。</p> |
| | <p>Potential risk of not meeting expectations/items to be checked 期待を満たさない場合の潜在的なリスク／確認すべき項目</p> <ul style="list-style-type: none"> • Check that the company has taken all reasonable steps to ensure that the computerised system in use is secured, and protected from deliberate or inadvertent changes. 企業が、使用中のコンピュータシステムのセキュリティを確保し、故意（deliberate）または不注意（inadvertent）による変更から保護するために、あらゆる合理的な手段を講じていることを確認する。 • Systems that are not physically and administratively secured are vulnerable to data integrity issues. Inspectorates should confirm that verified procedures exist that manage system security, ensuring that computerised systems are maintained in their validated state and protected from manipulation. 物理的・管理的（physically and administratively）にセキュリティが確保されていないシステムは、データの完全性の問題に対して脆弱である。査察当局は、システムのセキュリティを管理し、コンピュータ化されたシステムが、有バリデートされた状態で維持され、改ざん（manipulation）から保護されていることを保証するバリデートされた手順が存在することを確認すること。 • Check that individual user log-in IDs are in use. Where the system configuration allows the use of individual user log-in IDs, these should be used. 個別のユーザログインIDが使用されているかどうかを確認する。そのシステムの構成が、個別のユーザログインIDの使用が可能な場合には、それらを使用する必要がある。 • It is acknowledged that some legacy computerised systems support only a single user login or limited numbers of user logins. Where no suitable alternative computerised system is available, equivalent control may be provided by third party software, or a paper based method of providing traceability (with version control). The suitability of alternative systems should be justified and documented. Increased data review is likely to be required for hybrid systems. 幾つかのレガシー（訳注：「現在運用している」の意味）のコンピュータシステムは、単一のユーザログインまたは限られた数のユーザログインしかサポートしていないものがあることが認識されている。適切な代替コンピュータシステムが利用できない場合は、サードパーティ製のソフトウェア、または紙ベースのトレーサビリティ（バージョン管理を含む）の方法により、同等の管理を行うことができる。代替システムの適合性は、その論理的妥当性の説明がされ（justified）、文書化されなければならない。ハイブリッドシステムでは、データのレビューを強化する（increased data review）必要があると思われる。 • Inspectors should verify that a password policy is in place to ensure that systems |

| | |
|----|---|
| | <p>enforce good password rules and require strong passwords. Consideration should be made to using stronger passwords for systems generating or processing critical data.</p> <p>査察官は、システムが適切なパスワード規則を実施し、強力なパスワードを要求することを保証するために、パスワードポリシー（password policy：訳注参照）が実施されていることを確認すること。重要なデータを生成または処理するシステムは、より強力なパスワードを使用することを検討すべきである。</p> <p>訳注（ネットより）：パスワードポリシーとは、ユーザーアカウントのパスワードに使用できる文字数や、文字の組み合わせなどに関する条件のことを指します。... これにより、推測されやすい文字列をパスワードに設定することを防ぎ、セキュリティレベルを向上させられる</p> <ul style="list-style-type: none"> • Systems where a new password cannot be changed by the user, but can only be created by the admin, are incompatible with data integrity, as the confidentiality of passwords cannot be maintained. <p>新しいパスワードをユーザが変更できず、管理者のみが作成できるようなシステムは、パスワードの機密性（confidentiality）が維持できないため、データの完全性とは相容れない。</p> <ul style="list-style-type: none"> • Check that user access levels are appropriately defined, documented and controlled. The use of a single user access level on a system and assigning all users this role, which per definition will be the admin role, is not acceptable. <p>ユーザのアクセスレベルが適切に定義され、文書化され、管理されていることを確認する。システムで単一のユーザ・アクセス・レベルを使用し、すべてのユーザにこのロール（定義上は管理者ロール（admin role））を割り当てることは認められない。</p> <ul style="list-style-type: none"> • Verify that the system uses authority checks to ensure that only authorised individuals can use the system, electronically sign a record, access the operation or computerised system input or output device, alter a record, or perform the operation at hand. <p>権限のある者のみが、以下のことが出来ることを保証するために、目の前で操作を実行させ、システム使用権限（system uses authority）を確認する：</p> <ul style="list-style-type: none"> • そのシステムを使用できる； • 記録に電子署名ができる； • 操作やコンピュータ化されたシステムの入力または出力デバイスにアクセスが出来る • 記録を変更する。 |
| 2. | <p>Expectation 期待されること</p> <p>Computerised systems should be protected from accidental changes or deliberate manipulation. Companies should assess systems and their design to prevent unauthorised changes to validated settings that may ultimately affect data integrity. Consideration should be given to:</p> <p>コンピュータシステムは、偶発的な変更や意図的な操作（deliberate manipulation）から</p> |

保護されること。企業は、最終的にデータの完全性に影響を与える可能性のある、バリデートされた設定に対する不正な変更を防止するために、システムとその設計を評価すべきである。以下の点を考慮すべきである：

- The physical security of computerised system hardware:
コンピュータシステムのハードウェアの物理的なセキュリティ；
 - Location of and access to servers;
サーバーの設置位置とアクセス；
 - Restricting access to PLC modules, e.g. by locking access panels.
例えば、アクセスパネルのロックなどによる、PLC モジュールへのアクセスの制限。
 - Physical access to computers, servers and media should be restricted to authorised individuals. Users on a system should not normally have access to servers and media.
コンピュータ、サーバー、メディア（訳注：記憶媒体？）への物理的なアクセスは、許可された個人に限定すべきである。システム上のユーザは、通常、サーバーおよびメディアへのアクセスを持つべきではない。
- Vulnerability of networked systems from local and external attack;
ローカルおよび外部からの攻撃によるネットワークシステムの脆弱性。
- Remote network updates, e.g. automated updating of networked systems by the vendor.
リモートによるネットワークの更新。例えば、ベンダーによるネットワークシステムの自動更新など。
- Security of system settings, configurations and key data. Access to critical data/operating parameters of systems should be appropriately restricted and any changes to settings/configuration controlled through change management processes by authorised personnel.
システムの設定、構成および主要データのセキュリティ。システムの重要なデータや動作パラメータへのアクセスは適切に制限されるべきであり、設定や構成の変更は、権限のある担当者による変更管理プロセスを通じて制御されるべきである。
- The operating system clock should be synchronized with the clock of connected systems and access to all clocks restricted to authorised personnel.
オペレーティングシステムのクロックは、接続されているシステムのクロックと同期させ、すべてのクロックへのアクセスを権限のある担当者に制限すること。
- Appropriate network security measures should be applied, including intrusion prevention and detection systems.



| | |
|--|--|
| | <p>適切なネットワークセキュリティ対策を施すこと。これには、侵入防止及び検知システムが含まれる。</p> <ul style="list-style-type: none"> - Firewalls should be setup to protect critical data and operations. Port openings (firewall rules) should be based on the, making the firewall rules as tight as possible and thereby allowing only permitting traffic. <p>ファイアウォールを、重要なデータやオペレーションを保護するために設定すること。ポートオープン（ファイアウォールのルール）は、最小特権ポリシー（least privilege policy）に基づき、ファイアウォールのルールを可能な限りタイトにする（訳注：締め付ける）ことで、許可されたトラフィック（訳注参照）のみを許可するようにする。</p> <p>訳注（ネットより）：トラフィック（traffic）とは、交通（量）、通行（量）、往来などの意味を持つ英単語。ITや通信の分野では、通信回線やネットワーク上で送受信される信号やデータのことや、その量や密度のことをトラフィックということが多い。</p> <p>Regulated users should conduct periodic reviews of the continued appropriateness and effectiveness of network security measures, (e.g. by the use of network vulnerability scans of the IT infrastructure to identify potential security weaknesses) and ensure operating systems are maintained with current security measures.</p> <p>規制対象となるユーザは、ネットワークセキュリティ対策の継続的な適切性と有効性について、定期的なレビューを行うべきである（例：ネットワーク脆弱性スキャンを使用して、潜在的なセキュリティの弱点を特定する）。例えば、ITインフラのネットワーク脆弱性スキャンを使用して潜在的なセキュリティ上の弱点を特定するなど）、オペレーティングシステムが最新のセキュリティ対策で維持されていることを確認する。</p> |
| | <p>Potential risk of not meeting expectations/items to be checked 期待を満たさない場合の潜在的なリスク／確認すべき項目</p> <ul style="list-style-type: none"> • Check that access to hardware and software is appropriately secured, and restricted to authorised personnel. <p>ハードウェアおよびソフトウェアへのアクセスが適切に保護されており、権限のある担当者に制限されていることを確認する。</p> <ul style="list-style-type: none"> • Verify that suitable authentication methods are implemented. These methods should include user IDs and passwords but other methods are possible and may be required. However, it is essential that users are positively identifiable. <p>適切な認証方法（authentication methods）が実施されていることを確認すること。これらの方法にはユーザIDとパスワードが含まれるべきであるが、他の方法も可能であり、必要となる場合がある。ただし、ユーザが明確に識別できることが重要である。</p> |

| | |
|----|--|
| | <ul style="list-style-type: none"> • For remote authentication to systems containing critical data available via the internet; verify that additional authentication techniques are employed such as the use of pass code tokens or biometrics. <p>インターネット経由で利用可能な重要データを含むシステムへのリモート認証（remote authentication）について； パスコード・トークン（訳注参照）や生体認証などの追加の認証技術が採用されていることを確認する。</p> <p>訳注（ネットより）： トークンは、ワンタイムパスワードを生成するツールの総称です。ユーザーがオンライン上で取引する際、本人認証として使用することが可能です。パスワードを生成するボタンを押すとワンタイムパスワードが発行されます。トークンの液晶画面にパスワードが表示されますが、一定時間経過すると消えてしまいます。そして新たなパスワードがトークン上に表示される仕組みです。トークンのみでは銀行のログインIDや支店番号はわかりません。しかし、トークンが紛失したり盗難の被害に遭ったりすると、悪意ある第三者により不正ログインされる可能性があります。トークンは、ハードウェアタイプとソフトウェアタイプに大別されます。</p> <ul style="list-style-type: none"> • Verify that access to key operational parameters for systems is appropriately controlled and that, where appropriate, systems enforce the correct order of events and parameters in critical sequences of GMP/GDP steps. <p>システムの主要な動作パラメータへのアクセスが適切に制御されていること、また、必要に応じて、システムが GMP/GDP ステップの重要なシーケンスにおけるイベントおよびパラメータの正しい順序（の実施）を強制することを検証すること。</p> |
| 3. | <p>Expectation 期待されること</p> <p><u>Network protection</u> ネットワークの保護</p> <p>Network system security should include appropriate methods to detect and prevent potential threats to data.</p> <p>ネットワークシステムのセキュリティは、データに対する潜在的な脅威を検出し、防止するための適切な方法が含まれている必要がある。</p> <p>The level of network protection implemented should be based on an assessment of data risk.</p> <p>実施するネットワーク保護のレベルは、データリスクの評価に基づくこと。</p> <p>Firewalls should be used to prevent unauthorised access, and their rules should be subject to periodic reviews against specifications in order to ensure that they are set as restrictive as necessary, allowing only permitted traffic. The reviews should be documented.</p> <p>不正なアクセスを防止するために、ファイアウォールを使用し、その規則は、必要に応じて制限的に設定し、許可されたトラフィックのみを許可することを保証するように、仕様（specifications）に照らして定期的なレビューを行うべきである。この</p> |

| | |
|----|---|
| | <p>レビューは文書化すべきである。</p> <p>Firewalls should be supplemented with appropriate virus-protection or intrusion prevention/detection systems to protect data and computerised systems from attempted attacks and malware.</p> <p>ファイアウォールは、攻撃の試み（attempted attacks）やマルウェア（訳注参照）からデータやコンピュータシステムを保護するために、適切なウイルス保護システムや侵入防止／検出システムで補完すべきである。</p> <p>訳注（ネットより）：マルウェア（malware）とは、不正かつ有害な動作を行う意図で作成された悪意のあるソフトウェアや悪質なコードの総称です。</p> <p>マルウェアには次のようなものがあります。</p> <p>ウイルス</p> <p>他のプログラムに寄生して、そのプログラムの動作を妨げたり、ユーザの意図に反する、有害な作用を及ぼすためのプログラムで、感染機能や自己拡散機能を持つ</p> <p>ワーム</p> <p>独立のファイルで、他のプログラムの動作を妨げたり、ユーザの意図に反する、有害な作用を及ぼすためのプログラムで、感染機能や自己拡散機能を持つ</p> <p>トロイの木馬</p> <p>ユーザの意図に反し、攻撃者の意図する動作を侵入先のコンピュータで秘密裏に行うプログラム</p> <p>スパイウェア</p> <p>感染したパソコンの内部情報を外部に勝手に送信する</p> <p>キーロガー</p> <p>ユーザのキーボード操作をそのまま外部に送信する。スパイウェアの一種</p> <p>バックドア</p> <p>攻撃者が侵入するためのネットワーク上の裏口を開ける</p> <p>ボット</p> <p>攻撃者からの指令により、他のコンピュータやネットワークへの攻撃や、サーバからのファイルの盗み出しなど有害な動作を行うプログラム</p> |
| 3. | <p>Potential risk of not meeting expectations/items to be checked</p> <p>期待を満たさない場合の潜在的なリスク／確認すべき項目</p> <p>Inadequate network security presents risks associated with vulnerability of systems from unauthorised access, misuse or modification.</p> <p>不十分なネットワークセキュリティは、不正なアクセス、誤用（misuse）、改変によるシステムの脆弱性に関連するリスクがある。</p> <p>Check that appropriate measures to control network access are in place. Processes should be in place for the authorisation, monitoring and removal of access.</p> <p>ネットワークへのアクセスを制御するための適切な手段が実施されていることを確認する。アクセスの承認、監視、削除のためのプロセスが適切に整備されていること。</p> <p>Systems should be designed to prevent threats and detect attempted intrusions to the</p> |

| | |
|----|---|
| | <p>network and these measures should be installed, monitored and maintained.</p> <p>システムは、ネットワークへの脅威（threats）を防ぎ、侵入の試みを検知するように設計されていること。これらの対策はインストールし、監視（モニタリング）し、維持されるべきである。</p> <p>Firewall rules are typically subject to changes over time, e.g. temporary opening of ports due to maintenance on servers etc. If never reviewed, firewall rules may become obsolete permitting unwanted traffic or intrusions.</p> <p>ファイアウォールのルールは通常、時間の経過とともに変更を受ける。例えば、サーバーのメンテナンスなどにより一時的にポートが開かれることがある。もし見直しをしないと、ファイアウォール・ルールが時代遅れになり、望ましくないトラフィックや侵入を許してしまう可能性がある。</p> |
| 4. | <p>Electronic signatures used in the place of handwritten signatures should have appropriate controls to ensure their authenticity and traceability to the specific person who electronically signed the record(s).</p> <p>手書きの署名の代わりに使用される電子署名は、その信頼性（authenticity）と、電子署名を行った特定の人物へのトレーサビリティを確保するための適切な管理を持つべきである。</p> <p>Electronic signatures should be permanently linked to their respective record, i.e. if a later change is made to a signed record; the record should indicate the amendment and appear as unsigned.</p> <p>電子署名は、それぞれの記録に恒久的にリンクされるべきである。すなわち、署名された記録に後から変更が加えられた場合、その記録は修正を示し、署名されていないものとして表示されるべきである。</p> <p>Where used, electronic signature functionality should automatically log the date and time when a signature was applied.</p> <p>電子署名機能を使用する場合は、署名が行われた日時を自動的に記録する必要がある。</p> <p>The use of advanced forms of electronic signatures is becoming more common (e.g. the use of biometrics is becoming more prevalent by firms). The use of advanced forms of electronic signatures should be encouraged.</p> <p>高度な形式の電子署名の使用が一般的になってきている（例：バイオメトリクスの使用が企業に浸透してきている）。高度な形式の電子署名の使用を奨励すべきである。</p> <p>Potential risk of not meeting expectations/items to be checked 期待を満たさない場合の潜在的なリスク／確認すべき項目</p> <p>Check that electronic signatures are appropriately validated, their issue to staff is controlled and that at all times, electronic signatures are readily attributable to an individual.</p> <p>電子署名が適切にバリデーションされ、スタッフへの発行が管理され、そして、常に（at</p> |

| | |
|----|---|
| | <p>all times) 、電子署名が個人に容易に帰属していることを確認する。</p> <p>Any changes to data after an electronic signature has been assigned should invalidate the signature until the data has been reviewed again and re-signed.</p> <p>電子署名を付与した後にデータに変更があった場合、データを再度確認して再署名するまで署名は無効とする。</p> |
| 5. | <p><u>Restrictions on use of USB devices</u> USBメモリの使用の制限</p> <p>For reasons of system security, computerised systems should be configured to prevent vulnerabilities from the use of USB memory sticks and storage devices on computer clients and servers hosting GMP/GDP critical data. If necessary, ports should only be opened for approved purposes and all USB devices should be properly scanned before use.</p> <p>システムセキュリティの観点から、コンピュータシステムは、GMP/GDPの重要なデータを有するコンピュータクライアントやサーバー上でのUSBメモリや記憶装置の使用による脆弱性を防ぐように設定すべきである。必要に応じて、許可された目的のためにのみポートを開き、すべてのUSBデバイスは使用前に適切にスキャンするべきである。</p> <p>The use of private USB devices (flash drives, cameras, smartphones, keyboards, etc.) on company computer clients and servers hosting GMP/GDP data, or the use of company USB devices on private computers, should be controlled in order to prevent security breaches.</p> <p>GMP/GDPのデータを保管している会社のコンピュータのクライアントやサーバーで、私的なUSBデバイス（フラッシュドライブ、カメラ、スマートフォン、キーボードなど）を使用したり、私的なコンピュータで会社のUSBデバイスを使用したりすることは、セキュリティの破れを防止するために、これを管理するべきである。</p> <p>Potential risk of not meeting expectations/items to be checked 期待を満たさない場合の潜在的なリスク／確認すべき項目</p> <p>This is especially important where operating system vulnerabilities are known that allow USB devices to trick the computer, by pretending to be another external device, e.g. keyboard, and can contain and start executable code.</p> <p>これは、USBデバイスがキーボードなどの外部デバイス（例えばキーボード）を装ってコンピュータを騙し、実行可能なコードを含んで起動することを可能にするというような、オペレーティングシステムの脆弱性が知られている場合、特に重要である。</p> <p>Controls should be in place to restrict the use of such devices to authorised users and measures to screen USB devices before use should be in place.</p> <p>このようなデバイスの使用を許可されたユーザにを限定するための管理を行い、使用前にUSBデバイスをスクリーニングする対策を講じる必要がある。</p> |

9.6 Audit trails for computerised systems コンピュータシステムの監査証跡

| Item: | Audit Trails 監査証跡 |
|-------|---|
| 1. | <p>Expectation 期待されること</p> <p>Consideration should be given to data management and integrity requirements when purchasing and implementing computerised systems. Companies should select software that includes appropriate electronic audit trail functionality.</p> <p>コンピュータシステムを購入し、それを実行しようとする場合は、データマネジメント及びデータ完全性の要件を考慮する必要がある。企業は、適切な電子監査証跡機能を含むソフトウェアを選択すべきである。</p> <p>Companies should endeavour to purchase and upgrade older systems to implement software that includes electronic audit trail functionality.</p> <p>企業は、電子的な監査証跡機能を含むソフトウェアを導入するために、<u>その様なシステムの購入を行い、古いシステムアップグレードに努めるべきである。</u></p> <p>(訳注：下線部は原文に忠実に翻訳していない。原文を検討が必要である。)</p> <p>It is acknowledged that some very simple systems lack appropriate audit trails; however, alternative arrangements to verify the veracity of data should be implemented, e.g. administrative procedures, secondary checks and controls. Additional guidance may be found under section 9.10 regarding hybrid systems.</p> <p>非常に単純なシステムの中には、適切な監査証跡がないものがあることは認識されている。しかしながら、データの真実性 (veracity) を検証するための代替手段を実施すべきである。例えば、管理手順 (administrative procedures)、二次的なチェック (secondary checks) とコントロールなどである。ハイブリッドシステムに関する追加ガイダンスは、9.10 項に記載されている。</p> <p>Audit trail functionality should be verified during validation of the system to ensure that all changes and deletions of critical data associated with each manual activity are recorded and meet ALCOA+ principles.</p> <p>監査証跡の機能は、システムのバリデーションの際に検証すべきであり、各手作業に関連する重要なデータのすべての変更及び削除は、これを記録し、ALCOA+の原則を満たしていることを確認する。</p> <p>Regulated users should understand the nature and function of audit trails within systems, and should perform an assessment of the different audit trails during qualification to determine the GMP/GDP relevance of each audit trail, and to ensure the correct management and configuration of audit trails for critical and GMP/GDP relevant data. This exercise is important in determining which specific trails and which entries within trails are of significance for review with a defined frequency established. For example, following such an assessment audit trail reviews may focus on:</p> <p>法規制対象となっているユーザは、システム内の監査証跡の性質と機能を理解すべきであり、そして各監査証跡の GMP/GDP 関連性を判断し、重要かつ GMP/GDP 関連のデー</p> |



タに対する監査証跡の正しい管理と設定を確実にするために、適格性確認中に様々な監査証跡の評価を行うべきである。この作業は、どの特定の証跡が、そしてその証跡内のどの項目が、定義された頻度でレビューするために重要であるかを決定する上で大切である。例えば、このような評価の後、監査証跡のレビューは、以下の点に焦点を当てることができる：

- Identifying and reviewing entries/data that relate to changes or modification of data.
データの変更または修正に関連するエントリ/データを特定してレビューすること；
- Review by exception – focusing on anomalous or unauthorized activities.
例外についてのレビュー – 異常または不正な活動に焦点を当てる；
- Systems with limitations that allow change of parameters/data or where activities are left open to modification
パラメータ/データの変更を可能にする限界のあるシステム、または活動が修正可能な状態になっているシステム；
- Note: Well-designed systems with permission settings that prevent change of parameters/data or have access restrictions that prevent changes to configuration settings may negate the need to examine related audit trails in detail ;
注：パラメータ/データの変更を防止する権限設定や、構成設定の変更を防止するアクセス制限を備えた適切に設計されたシステムでは、関連する監査証跡を詳細に調査する必要性がない場合がある。

Audit trail functionalities should be enabled and locked at all times and it should not be possible to deactivate, delete or modify the functionality. If it is possible for administrative users to deactivate, delete or modify the audit trail functionality, an automatic entry should be made in the audit trail indicating that this has occurred.

監査証跡の機能は常に有効であり、（訳注：変更できないように）ロックされていなければならない。機能の無効化、削除、修正を、出来ないようにすべきである。管理者ユーザ（administrative users）が監査証跡機能を無効化、削除又は修正することが可能な場合には、監査証跡にそのような事態が発生したことを示す自動的なエントリが作成されるべきである。

Companies should implement procedures that outline their policy and processes to determine the data that is required in audit trails, and the review of audit trails in accordance with risk management principles. Critical audit trails related to each operation should be independently reviewed with all other records related to the operation and prior to the review of the completion of the operation (e.g. prior to batch release) so as to ensure that critical data and changes to it are acceptable. This review should be performed by the originating department, and where necessary verified by the quality unit, e.g. during self-inspection or investigative activities.

企業は、「監査証跡に必要とされるデータを決定するための方針とプロセス」及び「リスクマネジメントの原則に従った監査証跡のレビュー」を行うべきである。各操作に関連する重要な監査証跡は、操作に関連する他のすべての記録と一緒に、重要なデータ及びその変更が許容されることを確実にするために、操作の完了のレビューの前に（例え



| | |
|--|--|
| | <p>ば、バッチリリースの前に) 独立してレビューするべきである。このレビューは、起点となる部門 (originating department) が行うべきであり、必要に応じて、自己点検や調査活動などの際に品質部門が検証する。</p> <p>Non-critical audit trails reviews can be conducted during system reviews at a pre-defined frequency. This review should be performed by the originating department, and where necessary verified by the quality unit (e.g. during batch release, self-inspection or investigative activities).</p> <p>重要でない監査証跡のレビューは、事前に定義された頻度でシステムレビュー中に実施することが可能である。このレビューは、起点となる部門が実施し、必要に応じて品質部門が検証することが望ましい (例: バッチ出荷時、自主検査又は調査活動時)。</p> |
| | <p>Potential risk of not meeting expectations/items to be checked 期待を満たさない場合の潜在的なリスク／確認すべき項目</p> <ul style="list-style-type: none"> • Validation documentation should demonstrate that audit trails are functional, and that all activities, changes and other transactions within the systems are recorded, together with all relevant metadata. <p>バリデーション文書は、監査証跡が機能していること、そして、システム内の全ての活動、変更、およびその他のトランザクション (訳注参照) が、関連するすべてのメタデータと共に記録されていることを示すべきである。</p> <p>訳注 (ネットより) : IT用語で「複数の処理をひとつにまとめたもの」の意味である。トランザクションでは、複数の処理を一括して実施する。一連の全の処理が問題なく行われた場合にだけ成功とみなされる。どこかに問題があった場合には失敗とみなされる。処理が部分的に実行されることがなく、処理の同時実行制御に適している。</p> <ul style="list-style-type: none"> • Verify that audit trails are regularly reviewed (in accordance with quality risk management principles) and that discrepancies are investigated. <p>監査証跡が (品質リスク管理の原則に従って) 定期的にレビューされ、矛盾 (discrepancies) が調査されていることを検証すること。</p> <ul style="list-style-type: none"> • If no electronic audit trail system exists a paper based record to demonstrate changes to data may be acceptable until a fully audit trailed (integrated system or independent audit software using a validated interface) system becomes available. These hybrid systems are permitted, where they achieve equivalence to integrated audit trail, such as described in Annex 11 of the PIC/S GMP Guide. <p>電子的な監査証跡システムが存在しない場合は、完全な監査証跡 (統合化されたシステムまたはバリデートされたインターフェースを使用した独立した監査ソフトウェア) のシステムが利用可能になるまで、データへの変更を証明する紙ベースの記録が許容される。このようなハイブリッドシステムは、PIC/S GMPガイドの附属書 11に記載されているような統合された監査証跡と同等のものを実現する場合には認められる。</p> <ul style="list-style-type: none"> • Failure to adequately review audit trails may allow manipulated or erroneous data |

| | |
|----|--|
| | <p>to be inadvertently accepted by the Quality Unit and/or Authorised Person.</p> <p>監査証跡を適切にレビューできないことは、操作されたデータや誤ったデータが、品質管理部門や認定者に誤って受け入れられてしまう可能性がある。</p> <ul style="list-style-type: none"> • Clear details of which data are critical, and which changes and deletions should be recorded (audit trail) should be documented. <p>どのデータが重要で、どのような変更や削除が記録されるべきか（監査証跡）の明確な詳細を文書化すること。</p> |
| 2. | <p>Expectation 期待されること</p> <p>Where available, audit trail functionalities for electronic-based systems should be assessed and configured properly to capture any critical activities relating to the acquisition, deletion, overwriting of and changes to data for audit purposes.</p> <p>利用可能な場合は、電子ベースのシステムの監査証跡機能（audit trail functionalities）を評価し、監査目的でデータのための取得、削除、上書き、変更に関連する重要な活動を記録するよう適切に設定する必要がある。</p> <p>Audit trails should be configured to record all manually initiated processes related to critical data.</p> <p>監査証跡は、重要なデータに関連する全ての手動で開始されたプロセス（all manually initiated processes）を記録するように設定するべきである。</p> <p>The system should provide a secure, computer generated, time stamped audit trail to independently record the date and time of entries and actions that create, modify, or delete electronic records.</p> <p>システムは、電子記録を作成、変更、または削除するエントリおよびアクションの日時を独立して記録するために、コンピュータで生成された安全なタイムスタンプ付きの監査証跡を提供すべきである。</p> <ul style="list-style-type: none"> - The audit trail should include the following parameters: 監査証跡には、以下のパラメータを含める必要がある： - details of the user that undertook the action; アクションを実行したユーザの詳細； - what action occurred, was changed, incl. old and new values; どのようなアクションが発生したか、変更されたか （古い値と新しい値を含む） - when the action was taken, incl. date and time ; アクションが実行された日付と時刻； - why the action was taken (reason); and なぜそのアクションが行われたのか（理由）；および - in the case of changes or modifications to data, the name of any person authorising the change. |

| | |
|--|--|
| | <p>データの変更または修正の場合は、その変更を承認した者の名前。</p> <p>The audit trail should allow for reconstruction of the course of events relating to the creation, modification, or deletion of an electronic record.</p> <p>監査証跡は、電子記録の作成、変更、または削除に関連するイベントの経過を再構築が可能とすべきである。</p> <p>The system should be able to print and provide an electronic copy of the audit trail, and whether viewing in the system online or in a hardcopy, the audit trail should be available in a meaningful format.</p> <p>システムは、監査証跡の電子コピーを印刷して提供することができること。また、システムをオンラインで閲覧する場合でも、ハードコピーで閲覧する場合でも、監査証跡を意味のある形式で利用できるようにすること。</p> <p>If possible, the audit trail should retain the dynamic functionalities found in the computerised system, (e.g. search functionality and ability to export data such as to a spreadsheet).</p> <p>可能であれば、監査証跡は、コンピュータ化システムに見られる動的な機能（dynamic functionalities）（例：検索機能、スプレッドシートなどへのデータのエクスポート機能）を保持するべきである。</p> <p>Note: An audit trail should not be confused with a change control system where changes may needed to appropriately controlled and approved under a PQS.</p> <p>監査証跡を、PQS（医薬品品質システム）に基づいて変更を適切に管理・承認する必要がある場合の変更管理システムと混同してはならない。</p> |
| | <p>Potential risk of not meeting expectations/items to be checked</p> <p>期待を満たさない場合の潜在的なリスク／確認すべき項目</p> <p>Verify the format of audit trails to ensure that all critical and relevant information is captured.</p> <p>すべての重要かつ関連する情報が捕捉されていることを確実なものとするために、監査証跡の形式を確認する。</p> <p>The audit trail should include all previous values and record changes should not overwrite or obscure previously recorded information.</p> <p>監査証跡には以前のすべての値が含まれるべきであり、記録の変更が、以前に記録された情報を上書したり、不明瞭にするものであってはならない。</p> <p>Audit trail entries should be recorded in true time and reflect the actual time of activities.</p> <p>監査証跡のエントリは、リアルタイムで記録され、活動の実際の時間を反映すること。</p> <p>Systems recording the same time for a number of sequential interactions, or which only make an entry in the audit trail, once all interactions have been completed, may not be in compliance with expectations to data integrity, particularly where each discrete interaction or sequence is critical, e.g. for the electronic recording of addition of 4 raw materials to a mixing vessel. If the order of addition is a critical process parameter (CPP), then each addition should be recorded individually, with time stamps. If the order of addition is not a CPP then the addition of all 4 materials could be recorded as a single timestamped activity.</p> <p>多数の連続した相互作用に対して同じ時間を記録してしまうシステムや、すべての相互</p> |



| | |
|--|--|
| | <p>作用が完了した後に監査証跡に記入するだけのシステムは、データ完全性に対する期待に 応えていない可能性がある。特に、例えば混合容器への4つの原材料の添加を電子的に 記録する場合など、個別の相互作用や一連の作業が重要であるといった場合には、注意 が必要である。もし、添加の順番が重要なプロセスパラメータ（CPP）である場合、各 添加はタイムスタンプ付きで個別に記録されるべきである。もし添加の順番がCPPでな い場合は、4つの物質の添加を、1つのタイムスタンプ付きのアクティビティとして記録 することができる。</p> |
|--|--|

9.7 Data capture/entry for computerised systems

コンピュータ化システムの捕捉／エントリ

| Item: | Data capture/entry データの捕捉／エントリ |
|-------|--|
| 1. | <p>Expectation 期待されること</p> <p>Systems should be designed for the correct capture of data whether acquired through manual or automated means.</p> <p>システムは、手動または自動のいずれの方法でデータを取得するかにかかわらず、デ ータを正しく取り込むように設計されなければならない。</p> <p>For manual entry: 手動入力の場合</p> <ul style="list-style-type: none"> - The entry of critical data should only be made by authorised individuals and the system should record details of the entry, the individual making the entry and when the entry was made. <p>重要なデータの入力は、権限のある個人によってのみ行われるべきであり、当該シ ステムは、入力の詳細、入力を行った個人、および入力が行われた時点を記録する べきである。</p> |
| | <ul style="list-style-type: none"> - Data should be entered in a specified format that is controlled by the software, validation activities should verify that invalid data formats are not accepted by the system. <p>データはソフトウェアによって制御される指定のフォーマットで入力されるべきで あり、バリデーション活動では「無効なデータフォーマット（invalid data formats）が システムによって受け入れられないことを確認するべきである。</p> <ul style="list-style-type: none"> - All manual data entries of critical data should be verified, either by a second operator, or by a validated computerised means. <p>重要なデータの全ての手動による入力は、第二者（second operator）か、あるいはバリ デートされたコンピューターによる方法によって検証するべきである。</p> <ul style="list-style-type: none"> - Changes to entries should be captured in the audit trail and reviewed by an appropriately authorised and independent person. <p>入力内容の変更は監査証跡に記録し、適切な権限を持つ独立した者がレビューす る。</p> |



For automated data capture: (refer also to table 9.3)

自動データ取り込みのために (表9.3も参照)

The interface between the originating system, data acquisition and recording systems should be validated to ensure the accuracy of data.

データの正確性を確保するために、発信システム(originating system)、データ収集システム(data acquisition)、記録システムの間のインターフェースをバリデートすること。

Data captured by the system should be saved into memory in a format that is not vulnerable to manipulation, loss or change.

システムによって取り込まれたデータは、操作(manipulation)、紛失、変更に対して脆弱ではない形式でメモリに保存されること。

The system software should incorporate validated checks to ensure the completeness of data acquired, as well as any relevant metadata associated with the data.

システムソフトウェアは、データに関連するメタデータは勿論のこと、取得したデータの完全性を保証するためのバリデートされたチェック機能が組み込まれていること。

Potential risk of not meeting expectations/items to be checked

期待を満たさない場合の潜在的なリスク／確認すべき項目

Ensure that manual entries of critical data made into computerised systems are subject to an appropriate secondary check.

コンピュータ化されたシステムへの重要データの手動入力、適切な二次チェック(secondary check)を受けていることを確認する。

Validation records should be reviewed for systems using automated data capture to ensure that data verification and integrity measures are implemented and effective, e.g. verify whether an auto save function was validated and, therefore, users have no ability to disable it and potentially generate unreported data.

自動的なデータ収集を使用しているシステムのバリデーションをレビューすべきである。これはデータの確認(verification)と完全性(integrity)の計測を実施、効果的であることを確認するためである。例えば、自動保存機能がバリデートされているため、ユーザがこの機能を無効にすることができず、報告されないデータを生成する可能性がないかどうかを確認する。



2.

Expectation 期待されること

Any necessary changes to data should be authorised and controlled in accordance with approved procedures.

データへの必要な変更は、承認された手順に従って認可され、管理されること。

For example, manual integrations and reprocessing of laboratory results should be performed in an approved and controlled manner. The firm's quality unit should establish measures to ensure that changes to data are performed only when necessary and by designated individuals. Original (unchanged) data should be retained in its original context.

例えば、検査結果の手動による統合及び再処理は、承認され管理された方法で行われるべきである。企業の品質部門は、データへの変更が必要な場合にのみ、指定された個人によって行われることを確実にするための手段を確立すべきである。オリジナル（変更されていない）データは、元の状況で保持されるべきである。

Any and all changes and modifications to raw data should be fully documented and should be reviewed and approved by at least one appropriately trained and qualified individual.

生データに対するすべての変更および修正は、完全に文書化されるべきであり、少なくとも1人の適切な訓練を受けた有資格者によってレビューおよび承認されるべきである。

Potential risk of not meeting expectations/items to be checked

期待値を満たさない場合の潜在的リスク／チェックすべき項目

Verify that appropriate procedures exist to control any amendments or re-processing of data. Evidence should demonstrate an appropriate process of formal approval for the proposed change, controlled/restricted/defined changes and formal review of the changes made.

データの修正または再処理を管理するための適切な手順が存在することを検証する。提案された変更に対する正式な承認、管理された／制限された／定義された変更、および行われた変更の正式なレビューの適切なプロセスを示す証拠を示すこと。



9.8 Review of data within computerised systems

コンピュータ化されたシステム内のデータのレビュー

| Item: | Review of electronic data 電子的データのレビュー |
|-------|---|
| 1. | <p data-bbox="308 376 686 412">Expectation 期待されること</p> <p data-bbox="308 443 1362 763">The regulated user should perform a risk assessment in order to identify all the GMP/GDP relevant electronic data generated by the computerised systems, and the criticality of the data. Once identified, critical data should be audited by the regulated user and verified to determine that operations were performed correctly and whether any change (modification, deletion or overwriting) have been made to original information in electronic records, or whether any relevant unreported data was generated. All changes should be duly authorised.</p> <p data-bbox="308 792 1350 1162">規制対象となるユーザは、コンピュータ化システムで生成された GMP/GDP 関連の電子データをすべて特定し、そしてそのデータの重要性を認識するために、リスクアセスメントを実施すべきである。ひとたび特定されたならば、その重要なデータを規制を受けるユーザーが監査し、その運営が正しく行われているかを決定するための確認をする。そして、電子記録のオリジナルの情報に何らかの変化（変更（modification）、削除（deletion）あるいは上書き（overwriting））がされたか、あるいは、何らかの関連する未報告データが発生したかを確認する。全ての変化は、正式に承認されるべきである。</p> <p data-bbox="308 1191 1366 1368">An SOP should describe the process by which data is checked by a second operator. These SOPs should outline the critical raw data that is reviewed, a review of data summaries, review of any associated log-books and hard-copy records, and explain how the review is performed, recorded and authorised.</p> <p data-bbox="308 1397 1350 1574">SOP は、データが第二のオペレータによってチェックされるプロセスを記述すべきである。これらのSOPは、レビューされる重要な生データ、データサマリーのレビュー、関連するログブック及びハードコピー記録のレビューについて概説し、レビューがどのように実行され、記録され、承認されるかを説明すべきである。</p> <p data-bbox="308 1603 1329 1688">The review of audit trails should be part of the routine data review within the approval process.</p> <p data-bbox="308 1718 1350 1803">監査証跡のレビューは、承認プロセスの範囲内にある日常的なデータレビューの一部となっているべきである。</p> <p data-bbox="308 1832 1342 2054">The frequency, roles and responsibilities of audit trail review should be based on a risk assessment according to the GMP/GDP relevant value of the data recorded in the computerised system. For example, for changes of electronic data that can have a direct impact on the quality of the medicinal products, it would be expected to review audit trails prior to the point that the data is relied upon to make a critical decision, e.g. batch</p> |



release.

監査証跡のレビューの頻度、役割及び責任は、コンピュータシステムに記録されたデータのGMP/GDPに関連する価値（GMP/GDP relevant value）に従ってのリスク評価に基づいて行われるべきである。例えば、医薬品の品質に直接影響を与える電子データの変更については、そのデータがバッチ出荷などの重要な決定段階に至る前に、監査証跡をレビューすることが期待される。

The regulated user should establish an SOP that describes in detail how to review audit trails, what to look for and how to perform searches etc. The procedure should determine in detail the process that the person in charge of the audit trail review should follow. The audit trail review activity should be documented and recorded.

法規制の対象となるユーザは、監査証跡をどの様にレビューするするのか、何を探すか、そして、どのように検索を実行するかなどを詳細に記述したSOPを確立するべきである。その手順は、監査証跡レビューの担当者が従うべきプロセスを詳細に決定すべきである。監査証跡のレビュー活動は、文書化して記録すべきである。

Any significant variation from the expected outcome found during the audit trail review should be fully investigated and recorded. A procedure should describe the actions to be taken if a review of audit trails identifies serious issues that can impact the quality of the medicinal products or the integrity of data.

監査証跡のレビュー中に発見された「期待される結果からの著しい変動」は、完全に調査し、記録するべきである。もし監査証跡のレビューが、医薬品の品質やデータの完全性に影響を及ぼす可能性のある重大な問題を特定した場合に、取るべき処置（actions）を、その手順書に記載すること。

Potential risk of not meeting expectations/items to be checked

期待値を満たさない場合の潜在的リスク／チェックすべき項目

Check local procedures to ensure that electronic data is reviewed based on its criticality (impact to product quality and/or decision making). Evidence of each review should be recorded and available to the inspector.

電子データがその重要性（製品品質および/または意思決定へのインパクト）に基づいてレビューされていることを確認するための、ローカル手順を確認する。各レビューの証拠を記録し、査察官が利用可能なようにすること。

Where data summaries are used for internal or external reporting, evidence should be available to demonstrate that such summaries have been verified in accordance with raw data.

内部または外部への報告のためにデータサマリーを使用する場合は、そのようなサマリーが生データと同様に検証されていることを示す証拠を入手できること。



| | |
|----|---|
| | <p>Check that the regulated party has a detailed SOP outlining the steps on how to perform secondary reviews and audit trail reviews and what steps to take if issues are found during the course of the review.</p> <p>法規制の対象となるユーザは、二次レビュー（secondary reviews）や監査証跡レビューの実施方法や、レビューの過程でもし問題が発見された場合、その対応手順を概説した詳細なSOPを持っていることを確認する。</p> <p>Where global systems are used, it may be necessary for date and time records to include a record of the time zone to demonstrate contemporaneous recording.</p> <p>グローバルシステムが使用されている場合、日時の記録には、同時期の記録を証明するために、タイムゾーン（訳注：同じ標準時を使う地域の時刻）の記録を含めることが必要な場合がある。</p> <p>Check that known changes, modifications or deletions of data are actually recorded by the audit trail functionality.</p> <p>データの変更、修正、削除が、監査証跡機能によって実際に記録されているかどうかを確認する。</p> |
| 2. | <p>The company's quality unit should establish a program and schedule to conduct ongoing reviews of audit trails based upon their criticality and the system's complexity in order to verify the effective implementation of current controls and to detect potential non-compliance issues. These reviews should be incorporated into the company's self-inspection programme.</p> <p>企業の品質部門は、現行の管理が効果的に実施されていることを検証するために、そして潜在的なコンプライアンス違反の問題を検出するために、監査証跡の重要性とシステムの複雑さに基づいて、継続的なレビューを行うプログラムとスケジュールを確立すべきである。これらのレビューは、会社の自己点検プログラムに組み込むべきである。</p> <p>Procedures should be in place to address and investigate any audit trail discrepancies, including escalation processes for the notification of senior management and national authorities where necessary.</p> <p>監査証跡のあらゆる不一致に対処し、調査するための手順は、適切なものであること。これには、必要な場合には、上級管理職および国家機関に通知するためのエスカレーションプロセスを含むものであること。</p> <p>Potential risk of not meeting expectations/items to be checked 期待を満たさない場合の潜在的なリスク／確認すべき項目</p> <ul style="list-style-type: none"> • Verify that self-inspection programs incorporate checks of audit trails, with the intent to verify the effectiveness of existing controls and compliance with internal procedures regarding the review of data. <p>自己点検プログラムは、監査証跡のチェックが組み込まれていることを確認する。これは、既存の管理の有効性と、データのレビューに関する内部手順の遵守を検証</p> |

| | |
|--|--|
| | <p>することを目的としている。</p> <ul style="list-style-type: none"> • Audit trail reviews should be both random (selected based on chance) and targeted (selected based on criticality or risk). <p>監査証跡のレビューは、無作為（偶然に基づいて選択される）であって、かつ目標を絞った（targeted）（重大性またはリスクに基づいて選択される）の両方であること。</p> |
|--|--|

9.9 Storage, archival and disposal of electronic data

電子的データの保管、アーカイビング、および廃棄

| Item: | Storage, archival and disposal of electronic data 電子的データの保管、アーカイビング、および廃棄 |
|-------|--|
| 1. | <p>Expectation 期待されること</p> <p>Storage of data should include the entire original data and all relevant metadata, including audit trails, using a secure and validated process.</p> <p>データの保管には、安全でバリデートされたプロセスを用いて、監査証跡を含むオリジナルデータ全体、及び関連するすべてのメタデータを含めるべきである。</p> <p>If the data is backed up, or copies of it are made, then the backup and copies should also have the same appropriate levels of controls so as to prohibit unauthorised access to, changes to and deletion of data or their alteration. For example, a firm that backs up data onto portable hard drives should prohibit the ability to delete data from the hard drive. Some additional considerations for the storage and backup of data include:</p> <p>もし、データがバックアップされているか、あるいはそのコピーが作成されているのであれば、そのバックアップあるいはコピーもまた、データへの不正アクセス、データの変更、削除、またはそれらの改変を禁止するために、バックアップおよびコピーにも同じ適切なレベルの管理が必要である。例えば、データを携帯用ハードディスクにバックアップする企業は、ハードディスクからデータを削除することを禁止する必要がある。データの保存とバックアップに関するその他の考慮事項は以下ものが含まれる：</p> <p>True copies of dynamic electronic records can be made, with the expectation that the entire content (i.e. all data and all relevant metadata is included) and meaning of the original records are preserved.</p> <p>動的な電子記録の真正コピーは、元の記録の内容全体（すなわち、すべてのデータと関連するすべてのメタデータが含まれている）と意味が保存されていることを期待して作成することができる。</p> <p>Stored data should be accessible in a fully readable format. Companies may need to maintain suitable software and hardware to access electronically stored data backups or copies during the retention period. Routine backup copies should be stored in a remote location (physically separated) in the event of disasters.</p> <p>保存されたデータは、完全に読み取り可能な形式（fully readable format）でアクセスできること。企業は、保存期間中に電子的に保存されたデータのバックアップまたはコピ</p> |



| | |
|----|--|
| | <p>ーにアクセスするために、適切なソフトウェアおよびハードウェアを維持する必要があるかもしれない。日常的なバックアップコピーは、災害時に備えて、遠隔地（物理的に分離された場所）に保管する必要がある。</p> <p>Back-up data should be readable for all the period of the defined regulatory retention period, even if a new version of the software has been updated or substituted for one with better performance.</p> <p>バックアップデータは、ソフトウェアの新しいバージョンが更新されたり、より性能の良いものに置き換えられたりした場合でも、法規制上の定義された保管期間の全てにわたって読むことができること。</p> <p>Systems should allow backup and restoration of all data, including meta-data and audit trails.</p> <p>システムは、メタデータや監査証拠を含め、全てのデータのバックアップと復元が可能であること。</p> <p>Potential risk of not meeting expectations/items to be checked 期待を満たさない場合の潜在的なリスク／確認すべき項目</p> <p>Check that data storage, back-up and archival systems are designed to capture all data and relevant metadata. There should be documented evidence that these systems have been validated and verified.</p> <p>データストレージ、バックアップ、アーカイブのシステムが、すべてのデータと関連するメタデータを取り込むように設計されていることを確認する。これらのシステムがバリデーションされ、確認されたことを文書化した証拠が必要である。</p> <p>The extent of metadata captured should be based on risk management principles, and users should ensure that all metadata critical in the reconstruction of activities or processes are captured.</p> <p>キャプチャする（訳注：取り込まれる）メタデータの範囲は、リスク管理の原則に基づいて決定されるべきであり、ユーザは活動やプロセスの再構築に重要なメタデータがすべてキャプチャされていることを確認する必要がある。</p> <p>Check that data associated with superseded or upgraded systems is managed appropriately and is accessible.</p> <p>後継システムまたはアップグレードされたシステムに関連するデータが適切に管理され、アクセス可能であることを確認する</p> |
| 2. | <p>Expectation 期待される事項</p> <p>The record retention procedures should include provisions for retaining the metadata. This allows for future queries or investigations to reconstruct the activities that occurred related to a batch.</p> <p>記録保持手順には、メタデータを保持するための規定を含めるべきである。これにより、将来の問い合わせや調査で、バッチに関連して発生した活動を再構築することができる。</p> |

3. Expectation 期待されること

Data should be backed-up periodically and archived in accordance with written procedures. Archive copies should be physically (or virtually, where relevant) secured in a separate and remote location from where back up and original data are stored.

データは定期的にバックアップされ、手順書に従ってアーカイブされること。アーカイブのコピーは、バックアップやオリジナルデータが保存されている場所とは別の、離れた場所に物理的に（または必要に応じて仮想的に）保管すること。

The data should be accessible and readable and its integrity maintained for all the period of archiving.

データは、アクセス可能であり、かつ読み取れること。そしてその完全性は、アーカイブ期間中、維持されること。

There should be in place a procedure for restoring archived data in case an investigation is needed. The procedure in place for restoring archived data should be regularly tested.

調査が必要な場合、アーカイブされたデータを復元するための手順を定めておくべきである。アーカイブされたデータを復元するための手順は、定期的にテストするべきである。

If a facility is needed for the archiving process then specific environmental controls and only authorised personnel access should be implemented in order to ensure the protection of records from deliberate or inadvertent alteration or loss. When a system in the facility has to be retired because problems with long term access to data are envisaged, procedures should assure the continued readability of the data archived. For example, it could be established to transfer the data to another system.

アーカイビングのプロセスのために施設が必要な場合は、特定の環境制御を行い、権限のある職員のみがアクセスできるようにする必要がある。これは、データの意図的または不注意による変更（alteration）や喪失（loss）からの保護を確実にするためである。データへの長期的なアクセスに関する問題が想定されるため、施設内のシステムを廃棄しなければならない場合、アーカイブされたデータの継続的な可読性を保証する手順が必要である。例えば、データを別のシステムに移すことを想定することが出来る。

Potential risk of not meeting expectations/items to be checked

期待を満たさない場合の潜在的なリスク／確認すべき項目

- There is a risk with archived data that access and readability of the data may be lost due to software application updates or superseded equipment. Verify that the company has access to archived data, and that they maintain access to the necessary software to enable review of the archived data.

アーカイブされたデータには、ソフトウェア・アプリケーションの更新や機器の更新により、データへのアクセスや読み取りができなくなるリスクがある。企業は、「アーカイブされたデータへのアクセス権を持っている」こと、および「アーカイブされたデータのレビューを可能にするために必要なソフトウェアへのアクセスを維持していること」を確認する。



| | |
|----|---|
| | <ul style="list-style-type: none"> Where external or third party facilities are utilised for the archiving of data, these service providers should be subject to assessment, and all responsibilities recorded in a quality technical agreement. Check agreements and assessment records to verify that due consideration has been given to ensuring the integrity of archived records. <p>データのアーカイブのために外部または第三者の施設を利用する場合、これらのサービスプロバイダーは評価の対象となるものであり、すべての責任は品質技術合意書（quality technical agreement）に記録すべきである。アーカイブされた記録の完全性を確保するために十分な配慮がなされていることを検証するために、合意書および評価記録（assessment records）を確認する。</p> |
| 4. | <p>Expectation 期待されること</p> <p>It should be possible to print out a legible and meaningful record of all the data generated by a computerised system (including metadata).</p> <p>コンピュータ化されたシステムによって生成されたすべてのデータ（メタデータを含む）の、読みやすく、かつ意味が判る記録（legible and meaningful record）をプリントアウトすることが可能であること。</p> <p>If a change is performed to records, it should be possible to also print out the change of the record, indicating when and how the original data was changed.</p> <p>記録に変更が加えられた場合、元のデータがいつ、どのように変更されたかを示す記録の変更も印刷することが可能であること。</p> <p>Potential risk of not meeting expectations/items to be checked 期待を満たさない場合の潜在的なリスク／確認すべき項目</p> <p>Check validation documentation for systems to ensure that systems have been validated for the generation of legible and complete records.</p> <p>そのシステムが、読みやすく完全な記録を作成することについて、バリデートされていることを確認するために、当該システムのバリデーション文書を確認する。</p> <p>Samples of print-outs may be verified.</p> <p>プリントアウトのサンプルを確認することもよい。</p> |
| 5. | <p>Expectation 期待されること</p> <p>Procedures should be in place that describe the process for the disposal of electronically stored data. These procedures should provide guidance for the assessment of data and allocation of retention periods, and describe the disposal of data that is no longer required.</p> <p>電子的に保存されたデータの廃棄のプロセスを記述した手順を整備すること。これらの手順では、データの評価および保存期間の割り当てに関するガイダンスを提供し、不要になったデータの処分について記述する必要がある。</p> |

| | |
|--|--|
| | <p>Potential risk of not meeting expectations/items to be checked 期待を満たさない場合の潜在的なリスク／確認すべき項目</p> <p>Check that the procedures clearly stipulate the conditions for the disposal of data, and that care is taken to avoid the inadvertent disposal of required data during its lifecycle.</p> <p>データの廃棄条件を明確に規定し、ライフサイクルの期間中、必要なデータの不用意の廃棄が避けられるような配慮されているかどうかを確認する。</p> |
|--|--|

9.10 Management of Hybrid Systems ハイブリッドシステムのマネジメント

| Item: | Management of Hybrid Systems ハイブリッドシステムのマネジメント |
|-------|--|
| 1. | <p>Hybrid systems require specific and additional controls in reflection of their complexity and potential increased vulnerability to manipulation of data. For this reason, the use of hybrid systems is discouraged and such systems should be replaced whenever possible.</p> <p>ハイブリッドのシステムは、その複雑さとデータの取り扱いに対する潜在的な脆弱性を反映して、特定の追加管理を必要とする。このような理由から、ハイブリッドシステムの使用は推奨されず、そのようなシステムは可能な限り交換するべきである。</p> <p>Each element of the hybrid system should be qualified and controlled in accordance with the guidance relating to manual and computerised systems as specified above.</p> <p>ハイブリッドシステムの各要素は、上述の手動のシステム及びコンピュータ化されたシステムに関するガイダンスに従って適格性を評価し、管理をするべきである。</p> <p>Appropriate quality risk management principles should be followed when assessing, defining, and demonstrating the effectiveness of control measures applied to the system.</p> <p>システムに適用される管理策の有効性を評価、定義、実証する際には、適切な品質リスク管理の原則に従うべきである。</p> <p>A detailed system description of the entire system should be available that outlines all major components of the system, the function of each component, controls for data management and integrity, and the manner in which system components interact.</p> <p>主要な構成要素、各構成要素の機能、データのマネジメントと完全性のための管理、及びシステム構成要素の相互作用の方法を概説した、システム全体の詳細な記述が利用可能であること。</p> <p>Procedures and records should be available to manage and appropriately control the interface between manual and automated systems, particularly steps associated with: manual input of manually generated data into computerised systems; transcription (including manual) of data generated by automated systems onto paper records; and automated detection and transcription of printed data into computerised systems.</p> <p>手動システムと自動システムの間のインターフェース、特に以下に関連する手順を管</p> |



| | |
|--|---|
| | <p>理し、適切に制御するための手順と記録が利用可能であること：</p> <ul style="list-style-type: none"> ・ 手動で生成されたデータの、コンピュータ化されたシステムへの手動入力； ・ 自動システムで生成されたデータの紙記録への転記（手動を含む）；及び ・ 印刷されたデータの自動検出と、コンピュータ化システムへの転記。 |
| | <p>Potential risk of not meeting expectations/items to be checked 期待を満たさない場合の潜在的なリスク／確認すべき項目</p> <p>Check that hybrid systems are clearly defined and identified, and that each contributing element of the system is validated.</p> <p>ハイブリッドシステムが明確に定義され、識別されていること、そしてシステムの各構成要素がバリデートされていることを確認する。</p> <p>Attention should be paid to the interface between the manual and computerised system. Inspectors should verify that adequate controls and secondary checks are in place where manual transcription between systems takes place.</p> <p>手動システムとコンピュータ化されたシステムの間インターフェースに注意を払うべきである。査察官は、システム間で手作業による転記が行われる場合、適切な管理と二次的なチェックが行われていることを確認するべきである。</p> <p>Original data should be retained following transcription and processing. Hybrid systems commonly consist of a combination of computerised and manual systems. Particular attention should be paid to verifying:</p> <p>The extent of qualification and/or validation of the computerised system; and, The robustness of controls applied to the management of the manual element of the hybrid system due to the difficulties in consistent application of a manual process.</p> <p>オリジナルデータは、転写および処理後においても、保持されていること。ハイブリッドシステムは、通常、コンピュータ化されたシステムとマニュアル・システムの組み合わせで構成されている。確認には特に注意を払うこと：</p> <ul style="list-style-type: none"> ・ コンピュータ化されたシステムの適格性および／または妥当性の範囲；及び ・ 手動プロセスの一貫した適用が困難なために、ハイブリッドシステムの手動要素のマネジメントに適用される管理の堅牢性。 <p>Procedures should be in place to manage the review of data generated by hybrid systems which clearly outline the process for the evaluation and approval of electronic and paper-based data. Procedures should outline:</p> <p>ハイブリッドシステムで生成されたデータのレビューをマネージ（管理）するために、電子データと紙ベースのデータの評価と承認のプロセスを明確に概説する手順を導入する必要がある。その手順には、以下を含めること：</p> <ul style="list-style-type: none"> ・ Instructions for how electronic data and paper-based data is correlated to form a complete record； 電子データと紙ベースのデータが、完全な記録を形成することに、どのように関連させるかの指示； ・ Expectations for approval of data outputs for each system； |

| | |
|----|---|
| | <p>各システムで出力されるデータの承認に関する期待；</p> <ul style="list-style-type: none"> • Risks identified with hybrid systems, with a focus on verification of the effective application of controls. <p>ハイブリッドシステムで特定されるリスク。管理の効果的な適用の確認に焦点をあてるようにする。</p> |
| 2. | <p>Potential risk of not meeting expectations/items to be checked</p> <p>期待を満たさない場合の潜在的なリスク／確認すべき項目</p> <p>Verify that instructions for the review of hybrid system data is in place.</p> <p>ハイブリッドシステムのデータをレビューするための指示が行われていることを確認する。</p> |

10. DATA INTEGRITY CONSIDERATIONS FOR OUTSOURCED ACTIVITIES

外部委託活動におけるデータ完全性の考慮事項

10.1 General supply chain considerations サプライチェーンに関する一般的な考慮事項

10.1.1 Modern supply chains often consist of multiple partner companies working together to ensure safe and continued supply of medicinal products. Typical supply chains require the involvement of API producers, dosage form manufacturers, analytical laboratories, wholesale and distribution organisations, often from differing organisations and locations. These supply chains are often supported by additional organisations, providing outsourced services, IT services and infrastructure, expertise or consulting services.

現代のサプライチェーンは、医薬品の安全かつ継続的な供給を確保するために、複数のパートナー企業が協力していることが多い。典型的なサプライチェーンは、原薬メーカー、製剤メーカー、分析機関、卸売・流通業者が関与しており、その組織や場所も様々である。また、これらのサプライチェーンは、外部委託サービス、ITサービス、それにインフラ、専門知識やコンサルティングサービスを提供する組織によって支えられていることが多い。

10.1.2 Data integrity plays a key part in ensuring the security and integrity of supplychains. Data governance measures by a contract giver may be significantly weakened by unreliable or falsified data or materials provided by supply chainpartners. This principle applies to all outsourced activities, including suppliersof raw materials, contract manufacturers, analytical services, wholesalers, contracted service providers and consultants.

データの完全性は、サプライチェーンのセキュリティと完全性を確保する上で重要な役割を果たす。契約締結者によるデータガバナンス対策は、サプライチェーンのパートナーから提供される信頼性の低い、または偽造されたデータや資料によって著しく弱められる可能性がある。この原則は、原材料の供給者、製造委託先、分析サービス、卸売業者、委託サービスプロバイダー、コンサルタントなど、すべてのアウトソーシングされた活動に適用される。

10.1.3 Initial and periodic re-qualification of supply chain partners and outsourced activities should include consideration of data integrity risks and appropriate control measures.

サプライチェーンのパートナー及び外部委託活動の、最初の、および定期的な再適格性確認には、データ完全性のリスク及び適切な管理手段についての考察を含めるべきである。

10.1.4 It is important for an organisation to understand the data integrity limitations of information obtained from the supply chain (e.g. summary records and copies / printouts) and the challenges of remote supervision. These limitations are similar to those discussed in section 8.11 of this guidance. This will help to focus resources towards data integrity verification and supervision using a quality risk management approach.



組織にとって、サプライチェーンから得られる情報（例えば、記録の概要やコピー／プリントアウト）のデータ 整合性の限界と、遠隔監視の課題を理解することが重要である。これらの限界は、本ガイダンスの 8.11項で述べられているものと同様である。これは、品質リスクマネジメントの手法を用いて、データの完全性の検証と監視に資源を集中させることができる。

10.2 Routine document verification 日常的な文書確認

10.2.1 The supply chain relies upon the use of documentation and data passed from one organisation to another. It is often not practical for the contract giver to review all raw data relating to reported results. Emphasis should be placed upon a robust qualification process for outsourced supplier and contractor, using quality risk management principles.

サプライチェーンでは、ある組織から別の組織へ渡される文書やデータの使用に依存している。委託側（contract giver）にとって、報告された結果に係る全ての生データ（raw data）を受領することは、往々にして現実的なものではない。品質リスクマネジメントの原則を用いて、外部委託しているサプライヤ及び受託者（contractor）の強固な適格性評価プロセス（robust qualification process）に重点を置くべきである。

10.3 Strategies for assessing data integrity in the supply chain

サプライチェーンでのデータ完全性の評価戦略

10.3.1 Companies should conduct regular risk reviews of supply chains and outsourced activity that evaluate the extent of data integrity controls required. The frequency of such reviews should be based on the criticality of the services provided by the contract acceptor, using risk management principles. Information considered during risk reviews may include:

企業は、必要なデータ完全性の管理の程度を評価するために、サプライチェーンやアウトソーシング活動の定期的なリスクレビューを行うべきである。そのようなレビューの頻度は、リスクマネジメントの原則を用いて、受託者（contract acceptor）が提供するサービスの重要性に基づくべきである：

- The outcome of site audits, with focus on data governance measures
データガバナンス対策に焦点を当てた事業所の監査（site audits）の結果；
- Demonstrated compliance with international standards or guidelines related to data integrity and security
データの完全性及びセキュリティに関連する国際的な基準又はガイドラインに準拠していることの証明；
- Review of data submitted in routine reports, for example ;
ルーチンレポートで提出されたデータのレビュー。例えば；



| Area for review レビューする分野 | Rationale 論理的な説明 |
|--|--|
| Comparison of analytical data reported by the contractor or supplier vs in-house data from analysis of the same material 委託先またはサプライヤから報告された分析データと、同じ材料を分析した社内データの比較 | To look for discrepant data which may be an indicator of falsification 改ざんの指標となりうる矛盾したデータを探すために |

10.3.2 Quality agreements (or equivalent) should be in place between manufacturers and suppliers of materials, service providers, contract manufacturing organisations (CMOs) and (in the case of distribution) suppliers of medicinal products, with specific provisions for ensuring data integrity across the supply chain. This may be achieved by setting out expectations for data governance, and transparent error/deviation reporting by the contract acceptor to the contract giver. There should also be a requirement to notify the contract giver of any data integrity failures identified at the contract acceptor site.

サプライチェーン全体でデータの完全性を確保するための特別な規定を含む品質協定（又はそれに相当するもの）が、製造業者と材料の供給者、サービスプロバイダー、製造受託機関（CMO）及び（流通の場合）医薬品の供給者との間には、結ばれているべきである。これは、データガバナンスに関する期待事項や、委託元（contract giver）に対して、委託先（contract acceptor）が報告する透明性のあるエラー／逸脱の報告を設定することで達成できる可能性がある。また、委託先（contract acceptor）のサイトで確認されたデータ完全性の失敗を、委託元（contract giver）に通知する要件も必要である。

10.3.3 Audits of suppliers and manufacturers of APIs, critical intermediate suppliers, primary and printed packaging materials suppliers, contract manufacturers and service providers conducted by the manufacturer (or by a third party on their behalf) should include a verification of data integrity measures at the contract organisation. Contract acceptors are expected to provide reasonable access to data generated on behalf of the contract giver during audits, so that compliance with data integrity and management principles can be assessed and demonstrated.

原薬の供給者及び製造者、重要な中間体の供給者、一次及び印刷された包装材の供給者、製造委託先、及びサービス提供者に対して、製造者（又は製造者に代わって第三者）が行う監査には、業務委託先組織（contract organisation）でのデータ完全性の確認を含めるべきである。業務受託者（contract acceptors）は、データの完全性及びマネジメントの原則の遵守を評価及び実証できるように、監査中に契約の提供者に代わって、生成されたデータへの合理的なアクセスを提供することが期待される。

10.3.4 Audits and routine surveillance should include adequate verification of the source electronic data and metadata by the Quality Unit of the contract giver using a quality risk management approach. This may be achieved by measures such as:

監査 (audits) 及び日常的な監視 (routine surveillance) は、品質リスクマネジメントの手法を用いて、業務委託者 (contract giver) の品質部門によるソース電子データ (source electronic data) 及びメタデータの適切な検証を含めるべきである。これは以下のような手段で達成できる。

| | |
|---|--|
| Site audit 製造所監査 | <p>Review the contract acceptors organisational behaviour, and understanding of data governance, data lifecycle, risk and criticality.</p> <p>業務受託者の組織的行動、およびデータガバナンス、データライフサイクル、リスクおよび重要性に関する理解を確認する。</p> |
| Material testing vs CoA 物品の試験 vs CoA | <p>Compare the results of analytical testing vs suppliers reported CoA. Examine discrepancies in accuracy, precision or purity results. This may be performed on a routine basis, periodically, or unannounced, depending on material and supplier risks. Periodic proficiency testing of samples may be considered where relevant.</p> <p>分析試験の結果とサプライヤが報告したCoAを比較する。精度、精密度、純度の結果の不一致を調べる。この作業は、物品サプライヤのリスクに応じて、日常的に、定期的に、または抜き打ちで行うことでもよい。必要に応じて、サンプルの（訳注：取り扱いについての）定期的な技能試験を検討する。</p> |
| Remote data review 遠隔データレビュー | <p>The contract giver may consider offering the Contracted Facility/Supplier use of their own hardware and software system (deployed over a Wide Area Network) to use in batch manufacture and testing. The contract giver may monitor the quality and integrity of the data generated by the Contracted Facility personnel in real time.</p> <p>業務委託者は、バッチ製造及び試験に使用するために、（Wide Area Network上に展開した）自身のハードウェア及びソフトウェアの Contracted Facility/Supplierの使用を提供することを考慮してよい。業務委託者は、業務受託者の施設の要員が生成したデータの品質及び完全性を、リアルタイムで監視することができる。</p> <p>In this situation, there should be segregation of duties to ensure that contract giver monitoring of data does not give provision for amendment of data generated by the contract acceptor.</p> <p>このような状況では、「データの業務委託者 (contract giver) のモニタリングは、業務受託者 (contract acceptor) が生成したデータの修正に係る条項を入れないこと（訳注：すなわち修正をさせないこと）」が確実となるように、職務の分離がなされるべきである。</p> |
| Quality monitoring 品質モニタリング | <p>Quality and performance monitoring may indicate incentive for data falsification (e.g. raw materials which marginally comply with specification on a frequent basis).</p> |

| | |
|--|--|
| | 品質と性能のモニタリングは、データ改ざん（data falsification）の誘因となる可能性がある（例：仕様を僅かに外れ原材料を頻繁に使用するなど）。 |
|--|--|

10.3.5 Contract givers may work with the contract acceptor to ensure that all client-confidential information is encoded to de-identify clients. This would facilitate review of source electronic data and metadata at the contract giver's site, without breaking confidentiality obligations to other clients. By reviewing a larger data set, this enables a more robust assessment of the contract acceptors data governance measures. It also permits a search for indicators of data integrity failure, such as repeated data sets or data which does not demonstrate the expected variability.

業務委託者（contract givers）は、業務受託者（contract acceptor）契約の受諾者と協力して、すべてのクライアントの機密情報がエンコード（符号化）され、クライアントを識別できないようにすることができる。これにより、他の顧客に対する守秘義務を破ることなく、業務委託者（contract givers）のサイトでソースの電子データ及びメタデータのレビューが容易になる。より多くのデータセットをレビューすることで、業務受託者（contract acceptors）のデータガバナンス対策をより強固に評価することができる。また、データの完全性が損なわれた場合の指標を探すことができる。その様な指標は、例えば、繰り返されるデータセットや、期待される変動性を示さないデータなどがある。

10.3.6 Care should be taken to ensure the authenticity and accuracy of supplied documentation (refer section 8.11). The difference in data integrity and traceability risks between 'true copy' and 'summary report' data should be considered when making contractor and supply chain qualification decisions.

提供された文書の真正性及び正確性を確保するために注意を払うべきである（8.11項参照）。業務受託者（contractor）及びサプライチェーンの適格性を判断する際には、「True Copy（真正コピー）」と「Summary Report（要約報告書）」のデータの間のデータ完全性及びトレーサビリティのリスクの違いを、考慮する必要がある。

11. REGULATORY ACTIONS IN RESPONSE TO DATA INTEGRITY FINDINGS

データ完全性に関する調査結果に対応する規制措置

11.1 Deficiency references 欠陥状態の参照

11.1.1 The integrity of data is fundamental to good manufacturing practice and the requirements for good data management are embedded in the current PIC/S Guides to GMP/GDP for Medicinal products. The following table provides a reference point

highlighting some of these existing requirements.

データ完全性はGMPの基本であり、かつ適正なデータマネジメントへの要求事項は、現行の PIC/S Guides to GMP/GDP for Medicinal Products に組み込まれている。以下の表は、これらの既存の要求事項の一部をハイライトした参考資料である。

| ALCOA principle ALCOAの原則 | PIC/S Guide to Good Manufacturing Practice for Medicinal products, PE 009 (Part I): PIC/S GMP PE 009 (Part I) | PIC/S Guide to Good Manufacturing Practice for Medicinal products, PE 009 (Part II): PIC/S GMP PE 009 (Part I) | Annex 11 (Computerised Systems) Annex 11 (コンピュータ化システム) | PIC/S Guide to Good Distribution Practice for Medicinal products, PE 011: PIC/S Guide PE 011 |
|-----------------------------|--|---|---|---|
| Attributable 帰属性 | [4.20, c & f], [4.21, c & i], [4.29 point 5] | [5.43], [6.14], [6.18], [6.52] | [2], [12.1], [12.4], [15] | [4.2.4], [4.2.5] |
| Legible 判読性 | [4.1], [4.2], [4.7], [4.8], [4.9], [4.10] | [6.11], [6.14], [6.15], [6.50] | [4.8], [7.1], [7.2] [8.1], [9], [10], [17] | [4.2.3], [4.2.9] |
| Contemporaneous 同時性 | [4.8] | [6.14] | [12.4], [14] | [4.1], [4.2.9] |
| Original 原本性 | [4.9], [4.27], [Paragraph "Record"] | [6.14], [6.15], [6.16] | [8.2], [9] | [4.2.5] |
| Accurate 正確性 | [4.1], [6.17] | [5.40], [5.42], [5.45], [5.46], [5.47], [6.6] | [Paragraph "Principles"] [4.8], [5], [6], [7.2], [10], [11] | [4.2.3] |
| Complete 完全性 | [4.8] | [6.16], [6.50], [6.60], [6.61] | [4.8], [7.1], [7.2], [9] | [4.2.3], [4.2.5] |
| Consistent 一貫性 | [4.2] | [6.15], [6.50] | [4.8], [5] | [4.2.3] |
| Enduring 耐久性 | [4.1], [4.10] | [6.11], [6.12], [6.14] | [7.1], [17] | [4.2.6] |
| Available 要事利用可能性 | [Paragraph "Principle"], [4.1] | [6.12], [6.15], [6.16] | [3.4], [7.1], [16], [17] | [4.2.1] |

11.2 Classification of deficiencies 欠陥のクラス分類

Note: The following guidance is intended to aid consistency in reporting and classification of data integrity deficiencies, and is not intended to affect the inspecting authority's ability to act according to its internal policies or national regulatory frameworks.

注：以下のガイダンスは、データ完全性の欠陥の報告と分類の一貫性を支援することを目的としているものであり、検査当局がその内部の方針または、国の規制の枠組みに従って行動する能力に影響を与えることを意図するものではない。

11.2.1 Deficiencies relating to data integrity failure may have varying impact to product quality. Prevalence of the failure may also vary between the actions of a single employee to an endemic failure throughout the inspected organisation.

データの完全性に関する欠陥は、製品の品質に様々な影響を与える可能性がある。また、欠陥の広がりも、一人の従業員の行動から、査察を行った組織全体に特有の欠陥まで様々である。



る。

11.2.2 The PIC/S guidance¹² on classification of deficiencies states:

欠陥の分類に関するPIC/Sガイダンス¹²には次のように記載されている。

“A critical deficiency is a practice or process that has produced, or leads to a significant risk of producing either a product which is harmful to the human or veterinary patient or a product which could result in a harmful residue in a food producing animal. A critical deficiency also occurs when it is observed that the manufacturer has engaged in fraud, misrepresentation or falsification of products or data”.

「重大な欠陥とは、ヒトあるいは動物のペイシェント（罹患者または罹患動物）に対して有害な製品を、あるいは食肉用動物（food producing animal）中に有害な残存物を生じるかも知れない製品を生じる欠陥か、あるいはそれを導くような欠陥である。“Critical”な欠陥は、製造業者が製品またはデータの詐欺（fraud）、不当表示（misrepresentation）、あるいは改竄（falsification）に関わっていたことが観察された時もまた、発生する。」

12. PI 040 PIC/S Guidance on Classification of GMP Deficiencies

訳注：上記のガイダンスは、ファルマソリューションズ(株)の技術資料のサイト (<http://www.phs.com/technology/index.html>) に、2019年1月付で「【対訳】PIC/Sガイダンス GMPの欠陥のクラス別け」として掲載されている。ただし、上記の文章は、上記のガイダンスの用語解説の項の先頭にある。

11.2.3 Not with standing the “critical” classification of deficiencies relating to fraud, misrepresentation or falsification, it is understood that data integrity deficiencies can also relate to:

詐欺（fraud）、虚偽の陳述（misrepresentation）または改ざん（falsification）に関連する欠陥を「重要」と分類しているが、データ完全性の欠陥は以下にも関連すると理解される：

- Data integrity failure resulting from bad practice,
不正行為によるデータ完全性の欠陥；
- Opportunity for failure (without evidence of actual failure) due to absence of the required data control measures.
必要なデータ管理手段がないために（実際に失敗したという証拠はないが）失敗する機会がある。

11.2.4 In these cases, it may be appropriate to assign classification of deficiencies by taking into account the following (indicative list only):

このような場合には、以下の点を考慮して欠陥の分類を行うことが適切であろう（例示リストのみ）：



Impact to product with actual or potential risk to patient health: Critical deficiency:

患者の健康への実際的なあるいは潜在的リスクを持つ製品へのインパクト：**致命的な欠陥**：

- Product failing to meet Marketing Authorisation specification at release or within shelf life.
出荷時または有効期間内に製造販売承認の規格に適合しなかった製品。
- Reporting of a 'desired' result rather than an actual out of specification result when reporting of QC tests, critical product or process parameters.
QCテスト、重要な製品、またはプロセスパラメータを報告する際に、実際の規格外の結果ではなく「望ましい（'desired'）」結果を報告すること。
- Wide-ranging misrepresentation or falsification of data, with or without the knowledge and assistance of senior management, the extent of which critically undermines the reliability of the Pharmaceutical Quality System and erodes all confidence in the quality and safety of medicines manufactured or handled by the site.
上級管理者の知識や支援の有無にかかわらず、広範囲にわたるデータの虚偽表示または改ざんが行われ、その程度が医薬品品質システム（PQS）の信頼性を決定的に損ない、製造所で製造または取り扱う医薬品の品質と安全性に対するすべての信頼を損なっていること。

Impact to product with no risk to patient health: Major deficiency:

患者の健康へのリスクがない製品へのインパクト。**重大な欠陥。**

- Data being misreported, e.g. original results 'in specification', but altered to give a more favourable trend.
データが誤って報告されている。例えば、当初の結果は「規格内」であったが、より好ましい傾向を示すように変更されている。
- Reporting of a 'desired' result rather than an actual out of specification result when reporting of data which does not relate to QC tests, critical product or process parameters.
QCテスト、重要な製品またはプロセスパラメータに関連しないデータを報告する際に、実際の規格外の結果ではなく「望ましい（desired）」結果を報告すること。
- Failures arising from poorly designed data capture systems (e.g. using scraps of paper to record info for later transcription).
データ収集システムの設計が不十分なために起こる失敗（例：後で転写するために情報を記録するために紙の切れ端を使用している）。

No impact to product; evidence of moderate failure: Major deficiency:

製品へのインパクトが無い：中程度の欠陥の証拠：**重大な欠陥。**

- Bad practices and poorly designed systems which may result in opportunities for data integrity issues or loss of traceability across a limited number of functional areas (QA, production, QC etc.). Each in its own right has no direct impact to product quality.

限られた機能領域（QA、製造、QCなど）において、データ完全性の問題や、トレーサビリティの喪失を引き起こす可能性のある、悪しき慣習や設計不良のシステム。それぞれが独立していても、製品品質には直接影響しない。

No impact to product; limited evidence of failure: Other deficiency:

製品への影響はない：失敗の証拠は限られている：その他の欠陥。

- Bad practice or poorly designed system which result in opportunities for data integrity issues or loss of traceability in a discrete area.
不適切な運用やシステム設計の不備により、データの整合性に問題が生じたり、個別の領域でトレーサビリティが失われる可能性がある
- Limited failure in an otherwise acceptable system, e.g. manipulation of non-critical data by an individual.
例えば、個人による重要ではないデータの操作など、他の点では許容できるシステムにおける限定的な欠陥。

11.2.5 It is important to build an overall picture of the adequacy of the key elements(data governance process, design of systems to facilitate compliant data recording, use and verification of audit trails and IT user access etc.) to make a robust assessment as to whether there is a company-wide failure, or a deficiency of limited scope/ impact.

全社的な障害なのか、それとも範囲や影響が限定的な欠陥なのかをしっかりと評価するためには、重要な要素（データガバナンスのプロセス、コンプライアンスに則ったデータ記録を容易にするシステムの設計、監査証跡の使用と検証、ITユーザのアクセスなど）の適切性について全体像を把握することが重要である。

11.2.6 Individual circumstances (exacerbating / mitigating factors) may also affect final classification or regulatory action. Further guidance on the classification of deficiencies and intra-authority reporting of compliance issues will be available in the *PIC/S Guidance on the classification of deficiencies* PI 040.

個々の状況（悪化要因／緩和要因）も、最終的な分類や法的措置に影響を与える可能性がある。欠陥の分類及び法令順守問題の当局内報告に関する更なるガイダンスは、*PIC/S Guidance on the classification of deficiencies* PI 040（訳注参照）に記載されています。

訳注：このガイダンスは、ファルマソリューションズ(株)の技術資料のサイト (<http://www.pharma-solutions.com/technology/index.html>) に、2019年1月付で「【対訳】PIC/Sガイダンス GMPの欠陥のクラス別け」として掲載されている。



12 REMEDIATION OF DATA INTEGRITY FAILURES データ完全性の欠陥の改善

12.1 Responding to Significant Data Integrity issues 重要なデータ完全性問題への対応

12.1.1 Consideration should be primarily given to resolving the immediate issues identified and assessing the risks associated with the data integrity issues. The response by the company in question should outline the actions taken as part of a remediation plan. Responses from implicated manufacturers should include:

主に、特定された当面の問題を解決し、データの完全性の問題に関連するリスクを評価することを考慮する必要がある。当該企業の回答は、改善計画の一環として実施された措置の概要を記載する必要がある。関係するメーカーからの回答には以下が含まれるべきである。

12.1.1.1 A comprehensive investigation into the extent of the inaccuracies in data records and reporting, to include:

データの記録および報告における不正確さの範囲についての包括的な調査。以下を含むものであること。

- A detailed investigation protocol and methodology; a summary of all laboratories, manufacturing operations, products and systems to be covered by the assessment; and a justification for any part of the operation that the regulated user proposes to exclude¹³; 詳細な調査プロトコルおよび方法論； 評価の対象となるすべてのラボ、製造作業、製品およびシステムの概要； 及び、規制対象となるユーザが除外することを提案する業務の一部についての正当な理由¹³。

13 The scope of the investigation should include an assessment of the extent of data integrity at the corporate level, including all facilities, sites and departments that could potentially be affected.

調査の範囲には、影響を受ける可能性のあるすべての施設、事業所、部門を含む、企業レベルでのデータ完全性のレベルの評価を含める必要がある。

- Interviews of current and where possible and appropriate, former employees to identify the nature, scope, and root cause of data inaccuracies. These interviews may be conducted by a qualified third party; データの不正確さの性質、範囲、および根本原因を特定するための、現在および可能かつ適切な場合には、元従業員のインタビュー。これらのインタビューは資格のある第三者 (qualified third party) が行ってもよい。
- An assessment of the extent of data integrity deficiencies at the facility. Identify omissions, alterations, deletions, record destruction, non-contemporaneous record completion, and other deficiencies; 施設におけるデータ完全性の欠陥の程度の評価。省略 (omissions)、変更 (alterations)、削除 (deletions)、記録の破棄 (record destruction)、記録の非同時的完了 (non-contemporaneous



record completion) 、およびその他の欠陥を特定する。

- Determination of the scope (data, products, processes and specific batches) and timeframe for the incident, with justification for the time-boundaries applied;
インシデントの範囲（データ、製品、プロセス、特定のバッチ）と時間枠を決定し、適用した時間枠の正当性を示すこと；
- A description of all parts of the operations in which data integrity lapses occurred, additional consideration should be given to global corrective actions for multinational companies or those that operate across multiple sites;
データ完全性が損なわれた業務の全ての部分についての説明。多国籍企業や複数のサイトで業務を行っている企業の場合は、グローバルな是正措置をさらに検討する必要がある；
- A comprehensive retrospective evaluation of the nature of the data integrity deficiencies, and the identification of root cause(s) or most likely root cause that will form the basis of corrective and preventative actions, as defined in the investigation protocol. The services of a qualified third-party consultant with specific expertise in the areas where potential breaches were identified may be required;

データ完全性の欠陥の性質についての包括的な回顧的評価、および調査プロトコールに定義されているように、是正措置および予防措置の基礎となる根本原因または最も可能性の高い根本原因を特定すること。侵害の可能性が指摘された分野に特化した専門知識を有する有資格の第三者コンサルタントのサービスが必要となる場合がある。；

- A risk assessment of the potential effects of the observed failures on the quality of the substances, medicines, and products involved. The assessment should include analyses of the potential risks to patients caused by the release/distribution of products affected by a lapse of data integrity, risks posed by ongoing operations, and any impact on the integrity of data submitted to regulatory agencies, including data related to product registration dossiers.

観察された欠陥（failures）が関係する物質、医薬品、製品の品質に及ぼす潜在的な影響に関するリスク評価。この評価には、データの完全性の欠如の影響を受けた製品の出荷／流通によって引き起こされる患者への潜在的なリスク、進行中の業務によってもたらされるリスク、製品登録書類（product registration dossiers）に関連するデータを含めた、規制当局に提出されるデータの完全性への影響の分析を含むべきである。

12.1.1.2 Corrective and preventive actions taken to address the data integrity vulnerabilities and timeframe for implementation, and including:

データインテグリティの脆弱性に対処するためにとられた是正措置および予防措置、および実施のための時間枠、および、以下の事項を含む：

- Interim measures describing the actions to protect patients and to ensure the quality of the medicinal products, such as notifying customers, recalling product, conducting additional testing, adding lots to the stability program to assure stability, drug application actions, and enhanced complaint monitoring. Interim measures should be monitored for effectiveness and residual risks should be communicated to senior management, and kept under review.

患者への安全性を保護し、医薬品の品質を確保するための措置を述べた暫定措置。これには、顧客への通知、製品の回収、追加試験の実施、安定性を確保するための安定性プログラムへのロットの追加、医薬品申請時の措置、苦情モニタリングの強化などがある。暫定措置（interim measures）対策が有効であることを監視し、残存するリスクを上級管理者に伝え、検討を続けるべきである。

- Long-term measures describing any remediation efforts and enhancements to procedures, processes, methods, controls, systems, management oversight, and human resources (e.g. training, staffing improvements) designed to ensure the data integrity. Where long term measures are identified interim measures should be implemented to mitigate risks.

データの完全性を確保するために設計された、手順、プロセス、方法、管理、システム、管理監督、及び人的資源（例：研修、人員配置の改善）に対する改善努力及び強化を記載した長期的対策。長期的な対策が特定された場合、リスクを軽減するために暫定的な対策を、実施する必要がある。

12.1.1.3 CAPA effectiveness checks implemented to monitor if the actions taken has eliminated the issue.

CAPAの有効性チェックを実施し、実施したアクションによって問題が解消されたかどうかをモニターする。

12.1.2 Whenever possible, Inspectorates should meet with senior representatives from the implicated companies to convey the nature of the deficiencies identified and seek written confirmation that the company commits to a comprehensive investigation and a full disclosure of issues and their promptre solution. A management strategy should be submitted to the regulatory authority that includes the details of the global corrective action and preventive action plan. The strategy should include:

可能な限り、査察当局は関与した企業の上級代表者と会い、指摘された欠陥の内容を伝え、その企業が包括的な調査、問題の完全な開示とその迅速な解決を約束することの確認書を求めるべきである。グローバルな是正措置及び予防措置計画の詳細を含む管理戦略を規制当局に提出すべきである。この戦略には以下を含むべきである。

- A comprehensive description of the root causes of the data integrity lapses, including

evidence that the scope and depth of the current action plan is commensurate with the findings of the investigation and risk assessment. This should indicate if individuals responsible for data integrity lapses remain able to influence GMP/GDP-related or drug application data.

データ完全性の違反の根本原因 (root causes) の包括的な説明。これには、現在の対応計画の範囲と深さが、調査とリスク評価の結果に見合っているという証拠を含む。これには、データインテグリティの失効に関与した個人が、GMP/GDP関連の、または医薬品申請データに影響を与えることができる状態にあるかどうかを示す必要がある。

- A detailed corrective action plan that describes how the regulated user intends to ensure the 'ALOCA+' attributes (see section 7.4) of all of the data generated, including analytical data, manufacturing records, and all data submitted or presented to the Competent Authority.

規制を受けるユーザーが、生成された全てのデータの「ALOCA+」属性（7.4項参照）をどのように確保しようとしているかを記述した詳細な是正処置計画。これには、分析データ、製造記録、及び所轄当局に提出又は提示された全てのデータを含む。

12.1.3 Inspectorates should implement policies for the management of significant data integrity issues identified at inspection in order to manage and contain risks associated with the data integrity breach.

査察当局は、データ完全性違反に関連するリスクを管理し、抑制するために、査察で特定された重大なデータ完全性問題の管理のためのポリシー（方針）を実施すべきである。

12.2 Indicators of improvement 改善の指標

12.2.1 An on-site inspection is recommended to verify the effectiveness of actions taken to address serious data integrity issues. Alternative approaches to verify effective remediation may be considered in accordance with risk management principles. Some indicators of improvement are:

深刻 (serious) なデータ完全性の問題に対処するために取られた措置の有効性を検証するために、現場査察 (on-site inspection) が推奨される。効果的な改善策を検証するために、リスクマネジメントの原則に基づいた別のアプローチを検討してもよい。改善の指標としては、次のようなものがある：

12.2.1.1 Evidence of a thorough and open evaluation of the identified issue and timely implementation of effective corrective and preventive actions, including appropriate implementation of corrective and preventive actions at an organisational level;

特定された問題を十分にかつオープンに評価した所の証拠、及び是正措置および予防措置のタイムリーな実施。これには、組織レベルでの是正措置および予防措置の適切な実施を含む；

12.2.1.2 Evidence of open communication of issues with clients and other regulators.

Transparent communication should be maintained throughout the investigation and remediation stages. Regulators should be aware that further data integrity failures may be reported as a result of the detailed investigation. Any additional reaction to these notifications should be proportionate to public health risks, to encourage continued reporting;

顧客および他の規制当局との問題のオープンなコミュニケーションの証拠。調査と是正の段階を通して、透明性のあるコミュニケーションを維持すべきである。規制当局は、詳細な調査の結果として、さらなるデータ完全性の欠陥が報告される可能性があることを認識すべきである。これらの通知に対する追加的な対応は、継続的な報告を促すために、公衆衛生上のリスクに見合ったものとすべきである。

12.2.1.3 Evidence of communication of data integrity expectations across the organisation, incorporating and encouraging processes for open reporting of potential issues and opportunities for improvement;

「組織全体へのデータ完全性の期待に関するコミュニケーション」、「潜在的な問題や改善の機会をオープンに報告するプロセスの取り入れ」及び「改善の機会と捉えていること」の証拠。；

12.2.1.4 The regulated user should ensure that an appropriate evaluation of the vulnerability of electronic systems to data manipulation takes place to ensure that follow-up actions have fully resolved all the violations. For this evaluation the services of qualified third party consultant with the relevant expertise may be required;

規制対象となるユーザは、電子システムのデータ操作に対する脆弱性の適切な評価が行われ、フォローアップ措置によってすべての違反が完全に解決されていることを確認すべきである。この評価には、関連する専門知識を有する有資格の第三者コンサルタントのサービスが必要となる場合がある；

12.2.1.5 Implementation of data integrity policies in line with the principles of this guide;

本ガイドの原則に沿ったデータ完全性のポリシーの実施。

12.2.1.6 Implementation of routine data verification practices.

日常的なデータ検証作業の実施

13. Glossary 用語集

Archiving アーカイビング

Long term, permanent retention of completed data and relevant metadata in its final form for the purposes of reconstruction of the process or activity.

プロセスまたは活動の再構築 (reconstruction) を目的として、その最終的な形で、完成したデータおよび関連するメタデータを長期的かつ恒久的に保存すること。

Audit Trail 監査証跡

GMP/GDP audit trails are metadata that are a record of GMP/GDP critical information (for example the creation, modification, or deletion of GMP/GDP relevant data), which permit the reconstruction of GMP/GDP activities.

GMP/GDP監査証跡とはメタデータであって、GMP/GDPの重要な情報（例えば、GMP/GDP関連データの作成、変更、削除など）を記録したものである。これによって、GMP/GDP活動の再構築が可能となる。

Back-up バックアップ

A copy of current (editable) data, metadata and system configuration settings (e.g. variable settings which relate to an analytical run) maintained for the purpose of disaster recovery.

災害復旧の目的で維持される、現在(current)の（編集可能な）データ、メタデータ、システム構成設定（例：分析実行に関連する変数設定）のコピーのこと。

Computerised system コンピュータ化システム

A system including the input of data, electronic processing and the output of information to be used either for reporting or automatic control.

データの入力、電子的な処理、報告または自動制御のために使用される情報の出力を含むシステム。

Data データ

Facts, figures and statistics collected together for reference or analysis.

参照や分析のために集められた事実 (facts)、数値、統計。

Data Flow Map データフローマップ

A graphical representation of the "flow" of data through an information system
情報システムにおけるデータの「流れ」を図式化したもの。

Data Governance データガバナンス

The sum total of arrangements to ensure that data, irrespective of the format in which it is generated, recorded, processed, retained and used to ensure a complete, consistent and accurate record throughout the data lifecycle.



データが生成された形式に関わらず、データが、そのライフサイクルを通じて、完全で、一貫性があり、そして正確な記録を確保するために、データを記録、処理、保持、使用するための取り決めの総体。

Data Integrity データの完全性

The degree to which data are complete, consistent, accurate, trustworthy, reliable and that these characteristics of the data are maintained throughout the data life cycle.

データが完全(complete)であり、一貫性があり(consistent)、正確であり(accurate)、真正のものである信頼でき(trustworthy)、信頼性があり(reliable)、データのこれらの特性が、データのライフサイクルを通して維持されている度合い。

The data should be collected and maintained in a secure manner, so that they are attributable, legible, contemporaneously recorded, original (or a true copy) and accurate. Assuring data integrity requires appropriate quality and risk management systems, including adherence to sound scientific principles and good documentation practices. The data should comply with ALCOA+ principles.

データは安全な方法で収集、維持されているべきである。それは、帰属性、判読可能性、同時的記録性、原本性（または真正コピー）、かつ正確性をもつことが必要である。データの完全性を確保するには、堅実な科学的原則や適正文書化規範を含む、適切な品質とリスクマネジメントシステムが必要である。また、データはALCOA+の原則に準拠する必要がある。

Data Lifecycle データライフサイクル

All phases in the life of the data (including raw data) from initial generation and recording through processing (including transformation or migration), use, data retention, archive / retrieval and destruction.

データ（生データを含む）の最初の生成と記録から、処理（変換や転送を含む）、使用、データの保持、アーカイブ／検索、破棄までの、データの一生におけるすべての段階。

Data Quality データ品質

The assurance that data produced is exactly what was intended to be produced and fit for its intended purpose. This incorporates ALCOA + principles.¹⁴

生成されたデータが意図された通りのものであり、意図された目的に適合していることを保証すること。これにはALCOA +の原則が含まれる¹⁴。

14 : 'GXP' Data Integrity Guidance and Definitions, MHRA, March 2018

Data Ownership データの所有権

The allocation of responsibilities for control of data to a specific process owner.

Companies should implement systems to ensure that responsibilities for systems and their data are appropriately allocated and responsibilities undertaken.

データの管理責任を、特定のプロセス所有者に割り当てること。企業は、システムとそのデ



ータに対する責任が適切に割り当てられ、責任を負うことを保証するシステムを導入する必要がある。

Dynamic Record 動的記録

Records, such as electronic records, that allow an interactive relationship between the user and the record content.¹³

電子記録のように、ユーザと記録内容の間にインタラクティブな関係を可能にする記録¹³。

13 The scope of the investigation should include an assessment of the extent of data integrity at the corporate level, including all facilities, sites and departments that could potentially be affected.

調査の範囲には、影響を受ける可能性のあるすべての施設(facilities)、拠点(sites)、部門を含む、企業レベルでのデータ完全性の程度の評価を含める必要があります。

Exception Report 例外レポート

A validated search tool that identifies and documents predetermined 'abnormal' data or actions, which require further attention or investigation by the data reviewer.

事前に設定された「異常な」データやアクションを特定して文書化する、有効な検索ツール。これらに対しては、データ照査者がさらなる注意や調査を必要である。

Good Documentation Practices (GdocP) 適正文書化規範 (GdocP)

Those measures that collectively and individually ensure documentation, whether paper or electronic, meet data management and integrity principles, e.g. ALCOA+.

紙媒体、電子媒体を問わず、文書がデータマネジメント及び完全性の原則を満たしていることを、集合的かつ個別に確認するための手段

Hybrid Systems ハイブリッドシステム

A system for the management and control of data that typically consists of an electronic system generating electronic data, supplemented by a defined manual system that typically generate a paper-based record. The complete data set from a hybrid system therefore consists of both electronic and paper data together. Hybrid systems rely on the effective management of both sub-systems for correct operation.

一般的に電子データを生成する電子システムが、一般的に紙ベースの記録を生成させる規定された手動のシステム (defined manual system) によって補われる所のデータマネジメントと管理のシステムである。ハイブリッドシステムから得られる完全なデータセットは、電子データと紙ベースのデータの両方で構成される。ハイブリッドシステムが正しく機能するためには、両方のサブシステムの効果的なマネジメントが必要となる。

Master Document マスタードキュメント

An original approved document from which controlled copies for distribution or use can be made.

承認された文書の原本であって、これから配布や使用のために管理されたコピーを作成することができる。



Metadata メタデータ

In-file data that describes the attributes of other data, and provides context and meaning.
他のデータの属性を記述し、文脈（context）や意味を提供するファイル内データ。

Typically, these are data that describe the structure, data elements, inter-relationships and other characteristics of data e.g. audit trails. Metadata also permit data to be attributable to an individual (or if automatically generated, to the original data source). Metadata form an integral part of the original record. Without the context provided by metadata the data has no meaning.

一般的に、それらはデータの構造、データ要素、相互関係、その他の特性、例えば監査証跡などを述べているデータが存在している。また、メタデータは、データを個人に帰属させることができる（あるいは、自動生成された場合は、元のデータソースに帰属させることができる）。メタデータはオリジナルの記録と一体化している。メタデータによって提供される文脈（context）がなければ、データは意味を持たない。

Quality Unit 品質部門

The department within the regulated entity responsible for oversight of quality including in particular the design, effective implementation, monitoring and maintenance of the Pharmaceutical Quality System.

規制対象となる企業の中で、特に医薬品品質システム（PQS）の設計、効果的な実施、監視及び維持を含む品質の監督に責任を持つ部門。

Raw Data 生データ

Raw data is defined as the original record (data) which can be described as the first-capture of information, whether recorded on paper or electronically. Information that is originally captured in a dynamic state should remain available in that state.¹⁴

生データとは、紙に記録されているか電子的に記録されているかを問わず、情報の第一段階での捕捉（first-capture）したオリジナルな記録（original record ; データ）と定義される。最初に、動的な状態で取得された情報は、その状態で利用可能でなければならない¹⁴。

¹⁴ ‘GXP’ Data Integrity Guidance and Definitions, MHRA, March 2018

Static Record 静的記録

A record format, such as a paper or electronic record, that is fixed and allows little or no interaction between the user and the record content.¹⁴

紙または電子記録などの記録形式で、固定されており、ユーザと記録内容との相互作用がほとんどまたは全くないもの。

Supply Chain サプライチェーン

The sum total of arrangements between manufacturing sites, wholesale and distribution sites that ensure that the quality of medicines is ensured throughout production and



distribution to the point of sale or use.

製造拠点、卸売拠点、流通拠点間の取り決めの総体であって、医薬品の品質を、製造から販売・使用の時点までの流通過程で確保するためのものである。

System Administrator システム管理者

A person who manages the operation of a computerised system or particular electronic communication service.

コンピュータ化されたシステムまたは特定の電子通信サービスの運用をマネジメントする人。

14 REVISION HISTORY 改定履歴

| Date | Version Number | Reasons for revision |
|------|----------------|----------------------|
| | | |

(2021年9月18日 訳了)

