EudraLex
The Rules Governing Medicinal Products in the European Union

Volume 4
Good Manufacturing Practice
Medicinal Products for Human and Veterinary Use

Annex 11: Computerised Systems

株式会社文善

改 0.1　**2024 年 11 月 8 日**

管理番号: BZLib-122
改訂番号: 0.1
名称: **Annex 11 Computerised System**
ﾍﾟｰｼﾞ数: 全 13ページ

【注記】

本書は、European Union が発行した英語原文の和訳翻訳です。本翻訳文はアズビル株式会社にて和文翻訳したものに対して、株式会社文善がアズビル株式会社の許諾を得て一部加筆修正したものです。

翻訳文はできるだけ英語原文に忠実になるよう努めましたが、あくまでも英語原文を正とするものです。本書は規制の理解を補助する目的で作成したものであり、アズビル株式会社及び株式会社文善は、翻訳文に誤りがないことについて保証いたしません。

原文の内容をご自身で必ず確認してください。アズビル株式会社及び株式会社文善は、本書を利用したことに起因して、お客様に何らかの損害が生じたとしても、これについては一切の責任を負いません。

本書に含まれる内容は、予告なしに変更されることがあります。

本書を含め、株式会社文善のサイト(https://bunzen.co.jp)では、電磁的記録・電子署名等に関する規制やガイダンスの翻訳を掲載しています。

本書、株式会社文善のサービス等への質問、コメント等は info1@bunzen.co.jp にお寄せください。

【本書の表記について】

文脈に応じ説明を補足した場合、〔 〕内にそれを記述しています。
読みやすさのために、論旨を補足するような文は適宜 ( ) に入れています。また”and”で並べられた単語を中黒点「・」、”or”で並べられた単語をスラッシュ「／」で区切る場合があります。なお、原文の「/」はそのまま訳文でも「/」にしています。

【訳注】には、訳又は内容についての説明を記載しています。

目次

Legal basis for publishing the detailed guidelines: Article 47 of Directive 2001/83/EC on the Community code relating to medicinal products for human use and Article 51 of Directive 2001/82/EC on the Community code relating to veterinary medicinal products. This document provides guidance for the interpretation of the principles and guidelines of good manufacturing practice (GMP) for medicinal products as laid down in Directive 2003/94/EC for medicinal products for human use and Directive 91/412/EEC for veterinary use.	詳細ガイドラインを発行するための法的根拠：ヒト向け医薬品製品に関する EC 規則であるディレクティブ 2001/83/EC 第 47 項及び動物用医薬品に関する EC 規則であるディレクティブ 2001/82/EC 第 51 項。本文書は、ヒト向け医薬品製品のための GMP を記載したディレクティブ 2003/94/EC 及び動物用医薬品のための GMP を記載したディレクティブ 91/412/EEC の原則及び指針について解釈を提供するものである。
Status of the document: revision 1	文書のステータス：リビジョン 1
Reasons for changes: the Annex has been updated in response to the increased use of computerised systems and the increased complexity of these systems. Consequential amendments are also proposed for Chapter 4 of the GMP Guide.	改訂理由：コンピュータ化システムの使用が増加し、その複雑さが増してきていることを受け、Annex の改訂を行った。 現状に対応するための修正は、GMP Guide【訳注】の Chapter 4 についても提案されている。 【訳注】EU Guide to GMP は、https://ec.europa.eu/health/medicinal-products/eudralex/eudralex-volume-4_en を参照のこと。
Deadline for coming into operation: 30 June 2011	運用開始までの期限：2011 年 6 月 30 日

Principle (原則)

This annex applies to all forms of computerised systems used as part of a GMP regulated activities. A computerised system is a set of software and hardware components which together fulfill certain functionalities.	本 annex は、GMP で規制された活動に利用されるあらゆる形態のコンピュータ化システムに適用される。 コンピュータ化システムは、ソフトウェア及びハードウェア部品の集合であり、それらが合わさって、ある機能を実現するものである。
The application should be validated; IT infrastructure should be qualified. Where a computerised system replaces a manual operation, there should be no resultant decrease in product quality, process control or quality assurance. There should be no increase in the overall risk of the process.	アプリケーションはバリデートすべきであり、IT インフラストラクチャは適格性評価すべきである。手動で行っている作業をコンピュータ化システムで置き換えたために製品品質、プロセス制御、又は品質保証のレベルが低下するようなことがあってはならない。プロセスの全般的なリスクが増大することのないようにすべきである。

1. Risk Management (リスク管理)

Risk management should be applied throughout the lifecycle of the computerised system taking into account patient safety, data integrity and product quality. As part of a risk management system, decisions on the extent of validation and data integrity controls should be based on a justified and documented risk assessment of the computerised system.	コンピュータ化システムのライフサイクルを通して、患者の安全、データインテグリティ及び製品の品質を考慮に入れたリスク管理を適用すべきである。リスク管理システムの一環として、正当性のある、文書化されたリスクアセスメントに基づいて、バリデーション及びデータインテグリティコントロールの範囲を決定すべきである。

2. Personnel (要員)

There should be close cooperation between all relevant personnel such as Process Owner, System Owner, Qualified Persons and IT. All personnel should have appropriate qualifications, level of access and defined responsibilities to carry out their assigned duties.	プロセスオーナ、システムオーナ、Qualified Person、IT 等の関連する全ての社員は密接に協力すべきである。それぞれの職務を遂行できるように、全ての社員に、適切な資格、アクセスレベル、定められた責任範囲を持たせるようにすべきである。

3. Suppliers and Service Providers (供給者及びサービスプロバイダ)

3.1 When third parties (e.g. suppliers, service providers) are used e.g. to provide, install, configure, integrate, validate, maintain (e.g. via remote access), modify or retain a computerised system or related service or for data processing, formal agreements must exist between the manufacturer and any third parties, and these agreements should include clear statements of the responsibilities of the third party. IT-departments should be considered analogous.	3.1 コンピュータ化システムや関連するサービスの提供／インストール／構成設定／統合／バリデート／（リモートアクセス経由等による）保守／変更／保管等、又はデータ処理に第三者（供給者、サービスプロバイダ等）を利用する場合、製造業者と全ての第三者との間に正式な合意書を交わされなければならない。これらの合意書は第三者の役割についての明確な記述を含むべきである。IT 部門も同様と考えるべきである。
3.2 The competence and reliability of a supplier are key factors when selecting a product or service provider. The need for an audit should be based on a risk assessment.	3.2 製品又はサービスプロバイダを選定する場合、供給者の能力及び信頼性が重要な要因となる。監査が必要かどうかは、リスクアセスメント〔結果〕に基づく。
3.3 Documentation supplied with commercial off-the-shelf products should be reviewed by regulated users to check that user requirements are fulfilled.	3.3 規制対象のユーザは市販製品とともに提供される文書資料をレビューし、ユーザ要求が満たされていることを確認すべきである。
3.4 Quality system and audit information relating to suppliers or developer of software and implemented systems should be made available to inspectors on request.	3.4 ソフトウェア及び実装されたシステムの供給者／開発者に関する品質システム及び監査の情報は、査察官の要求があったときに提示できるようにしておくべきである。

Project Phase (プロジェクトフェーズ)

4. Validation (バリデーション)

4.1 The validation documentation and reports should cover the relevant steps of the life cycle. Manufacturers should be able to justify their standards, protocols, acceptance criteria, procedures and records based on their risk assessment.	4.1 バリデーション文書資料及び各種報告書では、ライフサイクルにおける全ての関連ステップをカバーすべきである。製造業者は自分達の標準、プロトコル、受入基準、手順及び記録について、リスクアセスメント〔結果〕に基づいて正当性を示せるようにすべきである。

4.2 Validation documentation should include change control records (if applicable) and reports on any deviations observed during the validation process.	4.2 バリデーション文書資料には、変更コントロール記録（該当時のみ）及びバリデーションの過程で観察された逸脱の報告を含めるべきである。
4.3 An up to date listing of all relevant systems and their GMP functionality (inventory) should be available. For critical systems an up to date system description detailing the physical and logical arrangements, data flows and interfaces with other systems or processes, any hardware and software pre-requisites, and security measures should be available.	4.3 全ての関連するシステム及びその GMP 機能に関する最新の一覧表（システム台帳）を用意すべきである。重要なシステムについては、最新のシステムデスクリプション（物理的及び論理的配置、データフロー、他システム／プロセスとのインターフェイス、ハードウェア及びソフトウェアに関する必要条件、セキュリティ方策を詳述するもの）を用意すべきである。
4.4 User Requirements Specifications should describe the required functions of the computerised system and be based on documented risk assessment and GMP impact. User requirements should be traceable throughout the life-cycle.	4.4 ユーザ要求仕様書にはコンピュータ化システムに要求される機能を記載すべきであり、文書化されたリスクアセスメント及び GMP への影響に応じたものとすべきである。ライフサイクルを通じてユーザ要求まで辿ることができるようにすべきである。
4.5 The regulated user should take all reasonable steps, to ensure that the system has been developed in accordance with an appropriate quality management system. The supplier should be assessed appropriately.	4.5 規制対象ユーザは、あらゆる合理的な手段を講じ、システムが適切な品質管理システムに沿って開発されたことを確実にすべきである。供給者は適切にアセスメントすべきである。
4.6 For the validation of bespoke or customised computerised systems there should be a process in place that ensures the formal assessment and reporting of quality and performance measures for all the life-cycle stages of the system.	4.6 特注／カスタムコンピュータ化システムのバリデーションでは、システムライフサイクルの全ステージにおいて品質及びパフォーマンスの〔ために講じた〕方策を、確実に、正式にアセスメントし、及び報告するプロセスを設けるべきである。
4.7 Evidence of appropriate test methods and test scenarios should be demonstrated. Particularly, system (process) parameter limits, data limits and error handling should be considered. Automated testing tools and test environments should have documented assessments for their adequacy.	4.7 テスト方式及びテストシナリオが適切であったことを示す証拠を用意すべきである。特に、システム（プロセス）パラメータ限界値、データ限界値及びエラー処理を考慮すべきである。 自動テストツール及びテスト環境については、その妥当性を示すアセスメント記録を用意すべきである。

4.8 If data are transferred to another data format or system, validation should include checks that data are not altered in value and/or meaning during this migration process.	4.8 データを他のデータフォーマット又は他のシステムに移行する場合、移行によってデータの値及び（又は）意味が変わっていないことをバリデーションにより確認すべきである。

Operation Phase (運用フェーズ)

5. Data (データ)

Computerised systems exchanging data electronically with other systems should include appropriate built-in checks for the correct and secure entry and processing of data, in order to minimize the risks.	コンピュータ化システムが他システムと電子的にデータを交換する場合、リスクを最小化するために、データ入力及び処理が正確かつ安全に行われていることを示すビルトインチェック機能をシステムに持たせるべきである。

6. Accuracy Checks (正確性のチェック)

For critical data entered manually, there should be an additional check on the accuracy of the data. This check may be done by a second operator or by validated electronic means. The criticality and the potential consequences of erroneous or incorrectly entered data to a system should be covered by risk management.	重要度の高いデータを手で入力する場合は、そのデータの正確性について追加チェックを行うべきである。この追加チェックは、二人目の操作者が行ってもよいし、バリデートされた電子的な方法を用いて行ってもよい。システムに誤ったデータ又は不正確なデータを入力した場合の重大さ、及び起こりうる結果は、リスク管理で対応すべきである。

7. Data Storage (データ格納)

7.1 Data should be secured by both physical and electronic means against damage. Stored data should be checked for accessibility, readability and accuracy. Access to data should be ensured throughout the retention period.	7.1 物理的及び電子的両方の手段によってデータを損傷から保護すべきである。格納されているデータが、アクセスでき、読むことができ、かつ正確であることをチェックすべきである。保存期間を通じて、データに確実にアクセスできなければならない。
7.2 Regular back-ups of all relevant data should be done. Integrity and accuracy of backup data and the ability to restore the data should be checked during validation and monitored periodically.	7.2 全ての関連データは、定期的にバックアップすべきである。バックアップデータのインテグリティ・正確性、及びデータを復元する能力を、バリデーション時にチェックするとともに、定期的に監視すべきである。

8. Printouts (プリントアウト)

8.1 It should be possible to obtain clear printed copies of electronically stored data.	8.1 電子的に格納されたデータについては鮮明な印刷コピーを取れるようにすべきである。
8.2 For records supporting batch release it should be possible to generate printouts indicating if any of the data has been changed since the original entry.	8.2 バッチリリースを判断するための記録として、最初に入力された時からデータの変更があったかどうかを示す情報を印刷できるようにすべきである。

9. Audit Trails (監査証跡)

Consideration should be given, based on a risk assessment, to building into the system the creation of a record of all GMP-relevant changes and deletions (a system generated "audit trail"). For change or deletion of GMP-relevant data the reason should be documented. Audit trails need to be available and convertible to a generally intelligible form and regularly reviewed.	GMP に関連する全ての変更・削除についての記録の生成〔機能〕（システムが生成した監査証跡）をシステムに作りこむかどうかをリスクアセスメントに基づいて検討すべきである。GMP に関連する変更／削除については、理由も記録されるべきである。監査証跡は、いつでも利用でき、普通に判読できる形式に変換可能で、かつ定期的にレビューする必要がある。

10. Change control and configuration management (変更コントロールと構成管理)

Any changes to a computerised system including system configurations should only be made in a controlled manner in accordance with a defined procedure.	コンピュータ化システムに対するいかなる変更（システム構成設定の変更を含む）も、コントロールされた方法により、定められた手順に従ってのみ行うべきである。

11. Periodic evaluation (定期評価)

Computerised systems should be periodically evaluated to confirm that they remain in a valid state and are compliant with GMP. Such evaluations should include, where appropriate, the current range of functionality, deviation records, incidents, problems, upgrade history, performance, reliability, security and validation status reports.	コンピュータ化システムを定期的に評価し、それが有効な状態であり GMP に準拠していることを確認すべきである。このような評価項目には、現在の機能範囲、逸脱記録、インシデント、問題、アップグレード来歴、パフォーマンス、信頼性、セキュリティ及びバリデーション状態の報告等のうち該当するものが含まれる。

12. Security (セキュリティ)

12.1 Physical and/or logical controls should be in place to restrict access to computerized system to authorised persons. Suitable methods of preventing unauthorised entry to the system may include the use of keys, pass cards, personal codes with passwords, biometrics, restricted access to computer equipment and data storage areas.	12.1 コンピュータ化システムへのアクセスを許可された者に制限するため、物理的及び（又は）論理的なコントロールを設けるべきである。許可されない者によるシステムへのデータ入力を防止するための適切な方法としては、キー、パスカード、パスワード付きのパーソナルコード、生体認証、コンピュータ端末・データ格納装置の設置場所へのアクセス制限等がある。
12.2 The extent of security controls depends on the criticality of the computerised system.	12.2 セキュリティコントロールの程度はコンピュータ化システムの重要度に従う。
12.3 Creation, change, and cancellation of access authorisations should be recorded.	12.3 アクセス権限の生成、変更、及び取り消しは記録に残すべきである。
12.4 Management systems for data and for documents should be designed to record the identity of operators entering, changing, confirming or deleting data including date and time.	12.4 データ及び文書を管理するシステムは、データの入力／変更／確認／削除を行う操作者を日付・時刻付きで記録するように設計すべきである。

13. Incident Management (インシデント管理)

All incidents, not only system failures and data errors, should be reported and assessed. The root cause of a critical incident should be identified and should form the basis of corrective and preventive actions.	インシデントは、システム障害やデータエラーに限らず、全て報告し、アセスメントすべきである。重大なインシデントについては、根本原因を突き止め、それを是正・予防措置に役立てるべきである。

14. Electronic Signatures (電子署名)

Electronic records may be signed electronically. Electronic signatures are expected to: a. have the same impact as hand-written signatures within the boundaries of the company,	電子記録への署名は電子的なものでもよい。電子署名については以下が期待される。 a. 会社の中で手書き署名と同等の効果をもっている
b. be permanently linked to their respective record,	b. 署名された記録に永続的に紐付けされている
c. include the time and date that they were applied.	c. 署名を行ったときの日時が含まれている

15. Batch Release (バッチリリース)

When a computerised system is used for recording certification and batch release, the system should allow only Qualified Persons to certify the release of the batches and it should clearly identify and record the person releasing or certifying the batches. This should be performed using an electronic signature.	認証の記録及びバッチリリースのためにコンピュータ化システムを用いる場合、システムは Qualified Person のみがバッチリリースを認証できるようにし、バッチをリリース／認証した者を明確に識別し、記録すべきである。これは電子署名により行うべきである。

16. Business Continuity (ビジネス継続)

For the availability of computerised systems supporting critical processes, provisions should be made to ensure continuity of support for those processes in the event of a system breakdown (e.g. a manual or alternative system). The time required to bring the alternative arrangements into use should be based on risk and appropriate for a particular system and the business process it supports. These arrangements should be adequately documented and tested.	重大なプロセスを支援するコンピュータ化システムの可用性について、システムが故障した場合もプロセスが確実に継続してサポートされるよう準備すべきである（例：手動又は代替システム）。〔故障してから〕これらの対策を実行に移すまでに要する時間は、リスクに基づいたものとし、当該システム及びシステムが支援する業務プロセスに対し適切なものとすべきである。これらの対策は適切に文書化し、テストすべきである。

17. Archiving (アーカイブ)

Data may be archived. This data should be checked for accessibility, readability and integrity. If relevant changes are to be made to the system (e.g. computer equipment or programs), then the ability to retrieve the data should be ensured and tested.	データを〔別メディアに〕アーカイブしてもよい。この〔アーカイブした〕データについて、アクセス可否、見読性及びインテグリティをチェックすべきである。システム（例：コンピュータ機器又はプログラム）を変更する場合、データを取り出すことができることを確実にし、〔そのことを〕テストしておくべきである。

Glossary (用語)

Application: Software installed on a defined platform/hardware providing specific functionality	アプリケーション：定められたプラットフォーム/ハードウェア上にインストールされたソフトウェアであり、特定の機能を提供する
Bespoke/Customized computerised system: A computerised system individually designed to suit a specific business process	特注/カスタムコンピュータ化システム：特定の業務プロセスに合わせて個別に設計されたコンピュータ化システム
Commercial of the shelf software: Software commercially available, whose fitness for use is demonstrated by a broad spectrum of users.	市販ソフトウェア：市販されているソフトウェアであり、多数のユーザが利用していることから、利用に適していると考えられる
IT Infrastructure: The hardware and software such as networking software and operation systems, which makes it possible for the application to function.	IT インフラストラクチャ：アプリケーションが機能するためのネットワークソフトウェア、OS 等のハードウェア及びソフトウェア
Life cycle: All phases in the life of the system from initial requirements until retirement including design, specification, programming, testing, installation, operation, and maintenance.	ライフサイクル：最初の要件定義から退役までのシステムのライフにおける全てのフェーズであり、設計、仕様、プログラミング、テスト、設置、運用、及び保守を含む
Process owner: The person responsible for the business process.	プロセスオーナ：業務プロセスについて責任を負う者
System owner: The person responsible for the availability, and maintenance of a computerised system and for the security of the data residing on that system.	システムオーナ：コンピュータ化システムの可用性〔の確保〕・保守、及びシステムに格納されているデータのセキュリティについて責任を負う者
Third Party: Parties not directly managed by the holder of the manufacturing and/or import authorization.	第三者：製造及び（又は）輸入の許可を受けている者から直接管理されていない者