 

**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

**Legal basis for publishing the detailed guidelines:** ガイドラインの詳細を公表する法的根拠

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.

ヒトに使用する医薬品に関する委員会基準2001/83/EC指針第47項および動物用医薬品に関する委員会基準2001/82/EC指針第51項。この文書は、ヒトに使用する医薬品指針2003/94/ECおよび動物用医薬品指針91/412/EECに定められた医薬品製造管理および品質管理基準（GMP）の原則ならびにガイドラインの解釈のガイダンスを提供する。

**Status of the document**: 版数

revision 1

改定 1

**Reasons for changes**: 変更理由

The Annex has been revised 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.

本Annexは、コンピュータ化システムの使用の増加およびそれらシステムの複雑性の増加に対応するため、改定された。その結果としてGMPガイドの第4章の修正も発表された。

**Deadline for coming into operation**: 対応期限

30 June 2011

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 規制作業の一部として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する。コンピュータ化システムは、ソフトウェアとハードウェアといった要素の組み合せであり、双方が相まって特定の機能を満たす。

The application should be validated; IT infrastructure should be qualified.

アプリケーションはバリデートされていなければならず、ITインフラストラクチャは適格性が確認されていなければならない。

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.

マニュアルベースの作業をコンピュータ化システムに置き換える場合、結果として製品の品質、プロセスコントロールつまり品質保証を劣化させてはならない。プロセスの全般的なリスクが増えてもいけない。

### General　概要

#### 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.

リスク管理は、患者の安全性、データの完全性および製品の品質を考慮したコンピュータ化システムのライフサイクルで一貫して、適用されなければならない。リスク管理システムの一部として、バリデーションとデータの完全性の管理の範囲の決定は、正当と説明のできる文書化された当該コンピュータ化システムのリスク評価に基づいていなければならない。

#### 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、適格性のある担当者、および IT 等、すべての関連する要員間では、密接な協力を必要とする。 すべての要員は適切な適格性、アクセスレベルおよび定義された責任を持って割り当てられた任務を果たさなければならない。

## 3. Suppliers and Service Providers　サプライヤおよ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. |

サードパーティ（例：サプライヤ、サービスプロバイダ等）を、コンピュータ化システムまたは関連サービスまたはデータ・プロセッシングなどの、供給、インストール、構成設定、バリデート、メンテナンス（例：リモートアクセス経由等）、変更または維持するために利用する場合は、公式な合意が製造業者とサードパーティ間で存在しなければならず、これらの合意はサードパーティの責任を明確にした文書を含まなければならない。IT 部門も同様とみなされなければならない。

| | |
|---|---|
| 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. |

サプライヤの能力と信頼性は、製品またはサービスプロバイダを選ぶ際の鍵となる要素である。監査の必要性はリスク評価に基づく。

| | |
|---|---|
| 3.3 | Documentation supplied with commercial off-the-shelf products should be reviewed by regulated users to check that user requirements are fulfilled. |

既成のソフトウェアで提供された文書は、規制関係ユーザによってレビュされ、ユーザ要件を満たしているかチェックされなければならない。

| | |
|---|---|
| 3.4 | Quality system and audit information relating to suppliers or developers of software and implemented systems should be made available to inspectors on request. |

品質システム、サプライヤまたはソフトウェア開発者に関する監査情報および実装されたシステムは、査察官の要求に対応可能でなければならない。

**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.

バリデーション文書および報告書は、ライフサイクルの関連するステップを対象としなければならない。製造業者は、リスク評価に基づき、それらの標準、計画書、受入基準、手順および記録を正当に説明できなければならない。

4.2　Validation documentation should include change control records (if applicable) and reports on any deviations observed during the validation process.

バリデーション文書には、変更管理の記録（該当する場合）およびバリデーションプロセス中に観察された逸脱の報告が含まれていなければならない。

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.

関連するすべてのシステムおよびGMP関連機能（一覧表）の最新リストが利用可能でなければならない。

重要なシステムについては、物理的および論理的要素、データ・フロー、他のシステムやプロセスとのインタフェース、ハードウェアおよびソフトウェアの必要条件、ならびにセキュリティ基準の詳細を記載した最新のシステム記述書が利用可能でなければならない。

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.

ユーザ要求仕様書は、コンピュータ化システムに要求された機能を記述し、リスク評価およびGMPへの影響に基づいていなければならない。ユーザ要求仕様書は、バリデーションのライフサイクルを通してトレーサブル（追跡可能）でなければならない。

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.

規制関連ユーザは、あらゆる適格な措置をとって、適切な品質管理システムに従ってシステムが開発された事を証明しなければならない。ソフトウェアのサプライヤは適切に評価されなければならない。

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.

特注のあるいはカスタマイズされたコンピュータ化システムのバリデーションに関して、システムのすべてのライフサイクルの段階にわたって、公式な評価および品質と性能の測定に関する報告を保証するプロセスが実施されなければならない。

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.

適切なテスト方法とテストシナリオの証拠が、明示されなければならない。特に、システム（プロセス）パラメータリミット、データリミットおよびエラーハンドリングは考慮されなければならない。自動テストツールおよびテスト環境について、その妥当性の評価は文書化されなければならない。

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.

別のデータフォーマットあるいは別システムからデータが移行された場合、バリデーションには、この移行プロセス中にデータの値や意味が変更されていないことをチェックする作業を含まなければならない。

 

**Operational 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. |

他のシステムと電子的にデータを交換するコンピュータ化システムは、正確性と入力の安全性およびデータの処理に対し、リスクを最小化するために、適切なチェック機能が組み込まれていなければならない。

**6.**　Accuracy Checks　**正確性チェック**

| |
|---|
| 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. |

手入力された重要なデータにおいては、それらのデータの正確性を追加チェックしなければならない。このチェックは、別オペレータまたはバリデートされた電子的な手段によって実施する。誤りもしくは不正確なシステムへの入力による重大性と影響の可能性は、リスク管理によりカバーされなければならない。

**7.　Data Storage　データ保管**

| | |
|---|---|
| 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. |

データは損失に対し、物理的および電子的な手段で安全を確保されなければならない。保管されたデータは、アクセスの容易性、見読性および正確性をチェックしなければならない。 データへのアクセスは、保存期間を通して確保されなければならない。

| | |
|---|---|
| 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. |

関連するすべてのデータは、規則的にバックアップが実施されなければならない。バックアップデータの完全性および正確性、データの復元性は､バリデーション中および定期的にモニタリングしてチェックされなければならない。

**8.　Printouts　印刷物**

| | |
|---|---|
| 8.1 | It should be possible to obtain clear printed copies of electronically stored data. |

電子的に保管されたデータについては、明確に印刷されたコピーを出力できなければならない。

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.

バッチリリースを裏付ける記録に対しては、データが原本の入力時から変更されているかどうかを示す印刷物を生成できなければならない。

**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 に関連するすべての変更と削除の記録を作成するシステム（システム生成の‘監査証跡’）の構築は、リスク評価に基づいて考慮されるべきである。GMP に関連するデータの変更および削除に関しては、その理由が文書化されなければならない。監査証跡は入手可能で一般的に理解できる形式に変換可能で、定期的にレビュされる必要がある。

**10. Change and Configuration Management 変更およびコンフィグレーション管理**

Any changes to a computerised system including system configurations should only be made in a controlled manner in accordance with a defined procedure.

システムコンフィグレーションを含むコンピュータ化システムの変更は、定義されたプロシージャに従い、管理された方法のみによって実施されなければならない。

**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は、当該システムがバリデートされている状態を保持し、GMP を遵守していることを確認するため定期的に評価されなければならない。そのような評価には、必要に応じて、現行の機能の範囲、逸脱の記録、障害、問題、アップグレードの履歴、性能、信頼性、セキュリティおよびバリデーション状況の報告が含まれなければならない。

**12. Security 安全性**

12.1 Physical and/or logical controls should be in place to restrict access to computerised 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.

コンピュータ化システムのアクセスを認可された者に制限するため、物理的、論理的に制御しなければならない。不正エントリーを防ぐ適切な方法として、鍵、パスカード、パスワードを伴う個人コード、バイオメトリックスなどの利用、コンピュータ機器やデータ保管場所へのアクセス制限が含まれる。

 

12.2 The extent of security controls depends on the criticality of the computerised system.

セキュリティ管理の範囲は、コンピュータ化システムの重大性に基づく

12.3 Creation, change, and cancellation of access authorisations should be recorded.

アクセス権限の付与、変更および取消は記録されなければならない。

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.

データおよび文書の管理システムは、データ入力、変更、確認あるいは削除を行ったオペレータを、日付と時刻とともに記録するよう設計されていなければならない。

**13. Incident Management 障害管理**

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.

システムの故障やデータエラーのみならず、すべての障害は、報告され、評価されなければならない。重大な障害の根本的原因は、特定され、是正および予防措置の基本としなければならない。

**14. Electronic Signature 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,
b. be permanently linked to their respective record,
c. include the time and date that they were applied.

電子記録には電子的に署名が付されているかも知れない。電子署名には以下のことが求められる
a. 企業内において、手書き署名と同等であること
b. 各記録に恒久的にリンクしていること
c. 署名された時刻と日付を含むこと

**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.

コンピュータ化システムが、承認およびバッチリリースの記録に使用される場合には、そのシステムは適格な者にのみバッチのリリースの承認を許可し、バッチをリリースした者すなわち承認した者を明確に記録しなければならない。当該作業には、電子署名を利用しなければならない。

 

### 16. Business Continuity　業務の継続性

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.

重要なプロセスをサポートするコンピュータ化システムの利用においては、システムが故障した際にプロセスの継続的サポートを供給する保証がなければならない（例えば手動および代替のシステム）。代替の方法が利用可能になるまでの要求される時間は、リスクに基づき、特定のシステムおよび支援するビジネスに対して適切でなければならない。当該処置は適切に文書化かつテストされなければならない。

### 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.

データはアーカイブされるかも知れない。当該データは、アクセスの容易性、見読性および完全性をチェックされなければならない。システム（コンピュータ装置またはプログラム等）に変更がなされた場合、データの抽出が可能であることが保証され、テストされなければならない。

**Glossary　用語**

**Application**: Software installed on a defined platform/hardware providing specific functionality

アプリケーション: 特定の機能を提供するために、定められたプラットフォーム／ハードウェアにインストールされたソフトウェア

**Bespoke/Customized computerised system: A** computerised system individually designed to suit a specific business process

**特注／カスタマイズされたコンピュータ化システム：**特定のビジネスプロセスに適合するよう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.

**既成ソフトウェア：**広範囲のユーザに、その実用性を認められており、商業ベースで販売されているソフトウェア

**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：**ハードウェアおよびネットワーク・ソフトウェアやオペレーションシステム等のソフトウェアで、アプリケーションに機能を持たせたもの

**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：**設計、仕様、プログラミング、テスト、導入、運用および維持を含む初期の要件定義から廃棄までのシステムのライフにおけるすべてのフェーズ

**Process owner**: The person responsible for the business process.

**プロセスオーナ：**ビジネスプロセスに責任をもつ者

**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利用と維持、および当該システムに存在するデータのセキュリティに対する責任をもつ者

**Third Party**: Parties not directly managed by the holder of the manufacturing and/or import authorisation.

**サードパーティ：**製造業者および／または輸入許可機関による直接的な管理をうけない関係者