別紙(10) PIC/S GMP ガイドライン アネックス11

原文	和訳
COMPUTERISED SYSTEMS	コンピュータ化システム
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 fulfil certain functionalities.	本文書はGMPの規制を受ける業務の一部として使用されるコンピュータ化システムの全形態に適用する。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の構成要素が一体となって特定の機能を満たすものである。
The application should be validated; IT infrastructure should be qualified.	アプリケーションをバリデートすること。さらに、ITインフラストラクチャは要件を満たしていること。
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.	コンピュータ化システムが手動操作に取って換わっている場合には、製品の品質、工程管理、品質保証の低下があってはならない。全体的な工程のリスクが増加しないこと。
GENERAL	一般事項
1. Risk Management	1. リスクマネジメント
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.	リスクマネジメントは、患者の安全性、データの完全性、製品の品質を考慮に入れ、コンピュータ化システムのライフサイクル全体に適用すること。リスクマネジメントの一部として、バリデーションの範囲とデータの完全性の判断は正当化し、文書化したコンピュータ化システムのリスク評価に基づいて行うこと。
2. Personnel	2. 職員
There should be close cooperation between all relevant personnel such as Process Owner, System Owner, Authorised Persons and IT. All personnel should have appropriate qualifications, level of access and defined responsibilities to carry out their assigned duties.	プロセスオーナー、システムオーナー、出荷責任者、IT部門などあらゆる関連のある職員に密接な協力関係があること。全職員は、割り当てられた職務を行なうための、適切な能力、アクセスレベル、明確な責任を持つこと。
3. Suppliers and Service Providers	3. 供給者と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.	サードパーティー(例えば供給者、サービスプロバイダ)をコンピュータ化システム或いは関連したサービス、データ処理のためのサービスを提供、インストール、環境設定、集約、バリデート、保守管理(例えば、リモートアクセスを経由して)、変更、維持するために使う場合、製造業者とサードパーティーの間に、正式な契約が存在せねばならず、これらの契約には、サードパーティーの責任の明確な記載を含むこと。IT部門は同様に責任があるとみなすこと。
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 製品或いはサービスプロバイダを選ぶときの供給者の能力と信頼性は主要な要素である。監査の必要性はリスク評価を基にすること。
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 市販の製品に関する文書は、ユーザーの要求事項を満たすことを確認するために規制を受けるユーザーが照査すること。

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.	3.4 供給者、ソフトウェア及び運用しているシステムの開発者に関する品質システム及び監査情報は査察官の要求があり次第、提示できるようにすること。
PROJECT PHASE	開発・検証段階
4. Validation	4. 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 バリデーションの文書及び報告書はライフサイクルの該当する段階を網羅すること。製造業者は、リスク評価を基にした、基準、プロトコル、許容基準、手順書、記録を正当化できるようにすること。
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に変更管理記録(該当する場合)及びバリデーションの工程で認められた逸脱に関する報告書を含めること。
4.3 An up to date listing of all relevant systems and their GMP functionality (inventory) should be available.	4.3 すべての該当するシステムとGMPで果たしている機能の最新のデータリスト(一覧表)が入手できること。
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.	重要なシステムについては、物理的及び論理的な配列、データの流れ、他のシステム或いは工程とのインターフェイスを詳しく述べている最新のシステム、ハードウェア、ソフトウェアの必須条件の記述及びセキュリティ対策が利用できること。
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 要求事項仕様書は、コンピュータ化システムに要求された機能を記述し、文書化されたリスク評価及びGMPへの影響に基づいてこと。ユーザー要求事項は、ライフサイクルを通じて追跡可能であること。
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 規制を受けるユーザーは、適切な品質管理システムに従って、システムが開発されていることを保証するための、あらゆる妥当な措置を講じること。供給者を適切に評価をすること。
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 特注或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ついては、システムの全ライフサイクルを通じて品質及び性質について採られた措置は正式に評価して報告を保証するための工程があること。
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 適切な試験方法及び試験計画の証拠を示すこと。特にシステム(工程)パラメータの限界値、データの限界値及びエラーの扱いを考慮すること。自動テストツール及び試験環境については、文書化した適性評価の結果を保有していること。
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 データを別のデータフォーマット或いはシステムに変換する場合は、バリデーションにおいては、データがこの移行処理の間に、量及び/又は意味が変わっていないかの確認を含むこと。
OPERATIONAL PHASE	運用段階
5. Data	5. 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.	他のシステムでコンピュータを用いてデータを変換するコンピュータ化システムは、リスクを最小にするために、正確で安全な入力及びデータ処理のための適切な組込検査を含むこと。
6.Accuracy Checks	6. 正確性の確認
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.	手動で入力された重要なデータは、データの正確性に関する追加確認をすること。この確認は、別の操作者或いはバリデートされたコンピュータを用いた方法で行って差し支えない。システムに誤って或いは不正確に入力されたデータの重篤度と起こりうる結果は、リスクマネジメントで防ぐこと。
7.Data Storage	7. データの保存
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 データは、物理学的方法及び電子的方法によって損傷害から守ること。記憶されたデータはアクセスのしやすさ、可読性、正確性を確認すること。
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 すべての該当データの定期的なバックアップを行うこと。バックアップデータの完全性と正確性及びデータを保存する能力は、バリデーションで確認し、定期的にモニターすること。
8. Printouts	8. 印刷物
8.1 It should be possible to obtain clear printed copies of electronically stored data.	8.1 電子的に記憶されたデータの鮮明に印刷した副本を入手可能にすること。
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 バッチの出荷を判定する記録のために、オリジナルの入力以降に、データのいかなる部分が変更されているかどうかを示せる印刷物を作成できるようにしておくこと。
9. Audit Trails	9. 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.	リスク評価を基にして、あらゆるGMP上の変更及び削除の記録の作成をシステムに組入れることを考慮すること。(システムに組込まれた「監査証跡」であること。)GMP上のデータの変更或いは削除のための理由を文書化すること。監査証跡は入手することができ、一般的にわかりやすい書式に変換可能で定期的に照査する必要がある。
10. Change and Configuration Management	10. 変更と環境設定の管理
Any changes to a computerised system including system configurations should only be made in a controlled manner in accordance with a defined procedure.	システムの環境設定を含めたコンピュータ化システムの変更は、定義された手順に従って管理された方法で行うこと。
11. Periodic Evaluation	11. 定期的な照査
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, deviation records, incidents, problems, upgrade history, performance, reliability, security and validation status reports.	コンピュータ化システムについては、システムが有効な状態を保ち、かつGMPに適合しているかを確認するための定期的な照査を行うこと。そのような照査は、必要であれば、逸脱の記録、偶発的な事故、問題、アップグレードの履歴、性能、信頼性、セキュリティ及びバリデーションの状況報告書の最新版を含めること。

12. Security	12. セキュリティ
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.	12.1 コンピュータ化システムへのアクセスを権限を与えられた作業者に制限するための物理的及び／又は論理的管理を設けること。システムへの不正な入力を予防する適切な方法は、キー、パスカード、パスワードによる個人コード、生体認証、コンピュータ装置及びデータ記憶領域へのアクセス制限を含める。
12.2 The extent of security controls depends on the criticality of the computerised system.	12.2 セキュリティ管理の程度は、コンピュータ化システムの重要度による。
12.3 Creation, change, and cancellation of access authorisations should be recorded.	12.3 アクセス権限の設定、変更、解除を記録すること。
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 データ及び書類の管理システムは、日付と時間を含む、システムへのアクセスをし、データを変更し、確認又は削除を行った操作者の識別を記録するように設計すること。
13. Incident Management	13. 事故の管理
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.	システムの機能停止及びデータの誤りだけでなく、あらゆる事故を管理し評価すること。重大な事故の根本的な原因を特定し、それを基に是正措置・予防措置を作り上げること。
14. Electronic Signature	14. 電子署名
Electronic records may be signed electronically. Electronic signatures are expected to:	電子書類はコンピュータを用いた署名ができる。電子署名は以下の通りである。
a. have the same impact as hand-written signatures within the boundaries of the company,	a. 会社内での手書きの署名と同じ効力がある
b. be permanently linked to their respective record,	b. 記録が存在する限り、個々の記録と関連付ける
c. include the time and date that they were applied.	c. 署名を行った日時を含む
15. Batch release	15. バッチの出荷判定
When a computerised system is used for recording certification and batch release, the system should allow only Authorised 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.	判定及びバッチ出荷の記録にコンピュータシステムを使用する場合は、出荷判定者のみにバッチ出荷の判定の権限を認め、バッチの出荷或いは判定を行った作業者を明確に識別し記録すること。これは電子署名を使用すること。
16. Business Continuity	16. 事業継続性
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.	重要工程をサポートするコンピュータ化システムの有効性のために、システムの故障が発生した場合の工程のサポートの持続性を保証する規則を作成すること(例えば、手動或いは代替のシステム)。代替手段を使い始めるのに必要な時間はリスクに基づき、特殊なシステム及びシステムがサポートする業務に適応していること。この処置を適切に文書化し演習すること。
17. Archiving	17. 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に保存することができる。このデータは、アクセスのしやすさ、可読性、完全性を確認すること。システム(コンピュータの装置或いはプログラム)に変更がある場合は、データ復元の能力を保証し演習すること。
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プラットフォーム／ハードウェア。
Bespoke/Customised computerised system : A computerised system individually designed to suit a specific business process.	特注の／カスタマイズされたコンピュータ化システム:特定の事業に適するように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.	市販のソフトウェア:商業的に入手できるソフトウェア。使用適合性は広範囲のユーザーに立証される。
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:ネットワークソフトウェア及びオペレーションシステムなどのハードウェア及びソフトウェア。アプリケーションを機能させることが可能になる。
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、規格、プログラム作成、試験、設置、操作、保守管理を含めた、初期の要求事項から廃棄までのシステムの耐用期間における全段階。
Process owner : The person responsible for the business process.	プロセスオーナー:業務に対して責任を負う人物。
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.	システムオーナー:コンピュータ化システム及びシステム上に存在するデータのセキュリティの有用性、及び保守管理に対して責任を負う人物。
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／輸入業者により直接管理されない団体。