別紙（10） PIC/S GMP ガイドライン アネックス11

原文	和訳
COMPUTERISED SYSTEMS	コンピューター化システム
PRINCIPLE	原則
The introduction of computerised systems into systems of manufacturing, including storage, distribution and quality control does not alter the need to observe the relevant principles given elsewhere in the Guide. Where a computerised system replaces a manual operation, there should be no resultant decrease in product quality or quality assurance. Consideration should be given to the risk of losing aspects of the previous system by reducing the involvement of operators.	保管、配送、及び品質管理を含む製造システムにコンピュータ化システムを導入しても、PIC/S GMPガイドの他の規定の遵守の必要性は変わらない。コンピュータ化システムが人の手による作業に置き換わった場合には、結果的に製品品質又は品質保証における低下が起きてはならない。オペレータの関与が減少するため起こり得る、従前のシステムから失われる側面のリスクについて考慮しなければならない。
PERSONNEL	人員
1. It is essential that there is the closest co-operation between key personnel and those involved with computer systems. Persons in responsible positions should have the appropriate training for the management and use of systems within their field of responsibility which utilises computers.This should include ensuring that appropriate expertise is available and used to provide advice on aspects of design, validation, installation and operation of computerised system.	1. 主要な人員及びコンピュータシステムに関与する人員との間に、緊密な連携があることが不可欠である。責任ある立場の者は、彼らの責任分野においてコンピュータを使用する業務についてシステムの管理と使用の訓練を受けていなければならない。 適切な専門家が配置され、コンピュータ化システムの設計、バリデーション、据付及び運転に関し助言を提供できるようにしなければならない。
VALIDATION	バリデーション
2. The extent of validation necessary will depend on a number of factors including the use to which the system is to be put, whether it is prospective or retrospective and whether or not novel elements are incorporated. Validation should be onsidered as part of the complete life cycle of a computer system.This cycle includes the stages of planning, specification, programming, testing, commissioning, documentation, operation, monitoring and changing.	2. バリデーションが必要な度合いは、システムの投入される用途、バリデーションが予測的又は回顧的であるのか、取り込まれる新規要素の有無を含め多くの要因に依存する。バリデーションはコンピュータシステムのライフサイクル全体の一部をなすと考えなければならない。このサイクルには計画、規格、プログラミング、検収、運用開始、文書記録、運転、モニタリング及び変更の段階がある。
SYSTEM	システム
3. Attention should be paid to the siting of equipment in suitable conditions where extraneous factors cannot interfere with the system.	3. 外的因子がシステムを妨害することのない、適切な条件の下に装置を設置しなければならない。
4. A written detailed description of the system should be produced (including diagrams as appropriate) and kept up to date. It should describe the principles, objectives, security measures and scope of the system and the main features of the way in which the computer is used and how it interacts with other systems and procedures	4. システムについて、詳細な記述を文書化し（適切な場合はダイアグラムを含め）、常に最新の状態にしておかなければならない。 原則、目的、セキュリティ確保の方法及びシステムの適用範囲、コンピュータの使われ方における主な特徴、及びそれらの他のシステム及び手順との相互作用について記述すること。

5. The software is a critical component of a computerised system. The user of such software should take all reasonable steps to ensure that it has been produced in accordance with a system of Quality Assurance.	5. ソフトウェアはコンピュータ化システムにとって、非常に重要な要素である。そのようなソフトウェアの使用者は、ソフトウェアが品質保証システムに従い製造されたことを確認するため、全ての妥当な確認手順を実施しなければならない。
6. The system should include, where appropriate, built-in checks of the correct entry and processing of data.	6. システムは適切な場合には、正確なデータ入力及びデータ処理について確認するための機能が組み込まれていなければならない。
7. Before a system using a computer is brought into use, it should be thoroughly tested and confirmed as being capable of achieving the desired results.If a manual system is being replaced, the two should be run in parallel for a time, as part of this testing and validation.	7. コンピュータを用いたシステムが使用に供される前に、徹底的に試験を実施し、期待通りの結果が達成されることを確認しなければならない。人的操作が置き換えられる場合は、試験及びバリデーションの一環として当面の期間は両者を並行して運用すること。
8. Data should only be entered or amended by persons authorised to do so. Suitable methods of deterring unauthorised entry of data include the use of keys, pass cards, personal codes and restricted access to computer terminals. Consideration should be given to systems allowing for recording of attempts to access by unauthorised persons.	8. データは、認証を受けた者のみが入力或いは修正できるようになっていなければならない。 権限のないデータ入力を阻止する適切な方法として、キー、パスカード、個人コードの使用、及びコンピュータ端末へのアクセス制限が挙げられる。権限のない者がアクセスしようとした事をシステムに記録可能とすることについて考慮すること。
9. When critical data are being entered manually (for example the weight and batch number of an ingredient during dispensing), there should be an additional check on the accuracy of the record which is made. This check may be done by a second operator or by validated electronic means.	9. 重要なデータが手入力（例えば、成分の払い出し時の重量及びバッチ番号）される場合、記録の正確性について追加の確認を行わなければならない。 この確認は第2のオペレータ又はバリデーションを実施済の電子的手段により実施できる。
10. The system should record the identity of operators entering or confirming critical data.. Authority to amend entered data should be restricted to nominated persons. Any alteration to an entry of critical data should be authorised and recorded with the reason for the change.Consideration should be given to the system creating a complete record of all entries and amendments (an ″audit trail″)	10. 重要なデータの入力又は確認を行ったオペレータの特定がコンピュータシステムとして記録されるようになっていなければならない。入力されたデータを修正する権限は指名された者に制限しなければならない。重要データ入力に対するいかなる変更も承認され、当該変更についての理由と共に記録されること。すべての入力及び修正の完全な記録を作成する機能をシステムに組み込むことについて考慮しなければならない。(“監査証跡”)
11. Alterations to a system or to a computer program should only be made in accordance with a defined procedure which should include provision for validating, checking, approving and implementing the change. Such an alteration should only be implemented with the agreement of the person responsible for the part of the system concerned, and the alteration should be recorded. Every significant modification should be validated.	11. システム又はコンピュータプログラムに対する変更は、バリデーション、確認、承認及び変更実施の条項等が定められた一定の手順に従うことによってのみ行うことができる。 変更は、問題となるシステムの該当部分に責任を有する者の同意を得て、初めて実施できる。又、当該変更は記録しなければならない。重大な変更についてはバリデーションを実施しなければならない。
12. For quality auditing purposes, it should be possible to obtain meaningful printed copies of electronically stored data.	12. 品質監査の目的のため、電子的に保管されたデータについて、意味のわかる(コンピュータ言語や記号のようなものでない)印刷コピーが得られるようにしておかなければならない。

13. Data should be secured by physical or electronic means against wilful or accidental damage, and this in accordance with item 4.9 of the Guide. Stored data should be checked for accessibility, durability and accuracy.If changes are proposed to the computer equipment or its programs, the above mentioned checks should be performed at a frequency appropriate to the storage medium being used.	13. 本ガイドの4.9項に従い、データは故意又は偶発的なダメージに対し、物理的又は電子的手段により保護されなければならない。保存されたデータについてアクセス可能性、堅牢性及び正確性について確認しなければならない。コンピュータ装置又はそのプログラムに対し変更を行う場合は、使用する保存媒体に関して適切な頻度で、上述の確認が実行されること。
14. Data should be protected by backing-up at regular intervals. Back-up data should be stored as long as necessary at a separate and secure location.	14. データは定期的にバックアップすることにより保護しなければならない。バックアップデータは必要な限り、離れた安全な場所に保管しなければならない。
15. There should be available adequate alternative arrangements for systems which need to be operated in the event of a breakdown. The time required to bring the alternative arrangements into use should be related to the possible urgency of the need to use them. For example, information required to effect a recall must be available at short notice.	15. システムが故障した場合に運用する適切な代替手段を準備しておかなければならない。 代替手段を使用に移すために要する時間は、それらの使用を必要とする緊急度に関連していなければならない。例えば、回収を実行するため必要な情報は、すぐに利用できるようにしておかなければならない。
16. The procedures to be followed if the system fails or breaks down should be defined and validated. Any failures and remedial action taken should be recorded.	16. システムが故障した場合に遵守する手順が規定され、バリデーションを実施しなければならない。 いかなる不具合、及び実施した改善措置も記録しなければならない。
17. A procedure should be established to record and analyse errors and to enable corrective action to be taken.	17. 不具合を記録し分析し、また是正措置の実行を可能とする手順を確立しなければならない。
18. When outside agencies are used to provide a computer service, there should be a formal agreement including a clear statement of the responsibilities of that outside agency (see Chapter 7).	18. コンピュータ サービスを提供する外部機関を使用する場合、その外部機関の責任について明確に記載した正式な契約を締結していなければならない。(第 7章参照)。
19. When the release of batches for sale or supply is carried out using a computerised system, the system should recognize that only an Authorised Person can release the batches and it should clearly identify and record the person releasing the batches.	19. コンピュータシステムを使用した、販売又は供給のためのバッチの出荷可否判定においては、システムはオーソライズドパーソンのみが出荷可否判定可能なことを認識し、バッチの出荷可否判定を実施した者を明確に特定し、記録する必要がある。