

PIC/S ガイダンス

PI 011-3

GxP 規制下のコンピュータ化システムに対する実践規範

(25 September 2007)

抜粋意訳

2013/1/3

PIC/S GUIDANCE

GOOD PRACTICES FOR COMPUTERISED SYSTEMS

IN REGULATED “GXP” ENVIRONMENTS

(PI 011-3 25 September 2007)



PHARMACEUTICAL INSPECTION CONVENTION
PHARMACEUTICAL INSPECTION CO-OPERATION SCHEME

PI 011-3
25 September 2007

PIC/S GUIDANCE

GOOD PRACTICES FOR COMPUTERISED SYSTEMS IN REGULATED “GXP” ENVIRONMENTS

© PIC/S September 2007
Reproduction prohibited for commercial purposes.
Reproduction for internal use is authorised,
provided that the source is acknowledged.

Editor: PIC/S Secretariat
e-mail: info@picscheme.org
web site: <http://www.picscheme.org>

PI 011-3

25 September 2007

目次

1.	はじめに	4
2.	原文の目次と意識の範囲	5
3.	ガイダンスの概要	6
3.1.	目的	6
3.2.	対象システム	6
3.3.	解説の範囲	6
3.4.	想定読者	6
3.5.	イタリック体部分	6
3.6.	読み方	6
4.	意識部分の概要	7
4.1.	バリデーション方針と優先順位（14章）	7
4.2.	データ変更-監査証跡と重要データ入力（20章）	7
4.3.	電子記録と電子署名（21章）	7
4.4.	査察において考慮すべきこと（23章）	7
5.	抜粋意識	9

1. はじめに

本書は下記 PIC/S ガイダンスを部分的に意識したものである。

PI 011-3

GOOD PRACTICES FOR COMPUTERISED SYSTEMS IN REGULATED “GXP” ENVIRONMENTS

25 September 2007

原文：<http://www.picscheme.org/publication.php?id=8>

意識した部分は「表 1 原文の目次と意識の範囲」に灰色背景で示した。

原文の表現は決して容易ではないので、読みやすさを重視し以下の方針で意識した。

- 原文の構成にはとられない。すなわち、必要に応じ：
 - ・ 長文は複数の短文にわけ
 - ・ 箇条書きにする
- 削除しても大意が変わらない文言は、必ずしも訳さない
- 原文にない文言で補足する

従って、意識というより「解釈訳」というのが適切かもしれない。

本意識に対するコメントは下記へご連絡いただければ幸甚である。

GxP コンピュータ広場 管理人：望月 清

mochizuki-kiyoshi@xpro-asso.com

2. 原文の目次と意識の範囲

表 1 原文の目次と意識の範囲

TABLE OF CONTENTS	目次
1. Document history	1. 文書履歴
PART ONE - PREAMBLE	パート 1 - 緒言
2. Purpose	2. 目的
3. Scope	3. 適用範囲
4. Introduction	4. 序文
PART TWO - IMPLEMENTATION OF SYSTEM	パート 2 - システムの実装
5. Implementation of computerised systems	5. コンピュータ化システムの実装
6. The structure and functions of the computer system(s)	6. コンピュータシステムの構造と機能
7. Planning and life-cycle management	7. 計画とライフサイクルマネジメント
8. Management and responsibilities	8. マネジメントと責任
9. User requirement specifications (URS)	9. ユーザー要求仕様(URS)
10. Functional specifications (FS)	10. 機能仕様(FS)
11. Suppliers, software developers and quality management	11. 供給者、ソフトウェア開発者及び品質管理
12. Important QMS and software standards attributes	12. 重要な QMS とソフトウェア規格の特質
13. Testing	13. テスト
14. Validation strategies and priorities	14. バリデーション方針と優先順位
15. GAMP validation approach based on different categories of software products	15. ソフトウェアカテゴリ別の GAMP バリデーションアプローチ
16. Retrospective validation	16. 回顧的バリデーション
PART THREE - SYSTEM OPERATION / INSPECTION / REFERENCES	パート 3 - システム運用／査察／参照
17. Change management	17. 変更管理
18. Change control and error report system	18. 変更管理とエラー報告システム
19. System security, including back-up	19. システムセキュリティとバックアップ
20. Data changes - audit trail/critical data entry	20. データ変更-監査証拠と重要データ入力
21. Electronic records and electronic signatures	21. 電子記録と電子署名
22. Personnel	22. 職員
23. Inspection considerations	23. 査察において考慮すべきこと
24. Checklists and aide memoires	24. チェックリストと備忘録
25. References for relevant standards and GMP guides / codes	25. 関連基準と GMP ガイド/規約の参照文献
26. Suggested further reading	26. 推奨図書
27. Glossary of terms	27. 用語集
28. Abbreviations used in the document	28. 本文書で用いた略語
29. Revision history	29. 改訂履歴

意識した章を灰色背景で示す。

3. ガイダンスの概要

以下にガイダンスの概要を紹介する。(§ aa.bb) は参照した原文のセクション番号を示す。

3.1. 目的

GMP 査察の基本は PIC/S の GMP ガイドである。コンピュータ化システムの査察においては PIC/S GMP Annex 11 “Computerised Systems”が参照される。PIC/S ガイダンス「PI 011-3」はコンピュータ化システムに関する**推奨事項及び背景情報を査察官に対し提供するものであり**、以下の場合に役立つ。(§ 2.2)

- ・ トレーニング
- ・ 査察の現場

3.2. 対象システム

このガイダンスは GMP 以外の査察官にとっても役立つ。従って、このガイダンスは以下のシステムの査察において有益である。(§ 2.2)

GxP 領域におけるコンピュータ化システム

3.3. 解説の範囲

このガイダンスの解説範囲は以下のとおりである。(§ 2.5)

- ・ システム構築
- ・ バリデーション
- ・ システム運用

3.4. 想定読者

このガイダンスの想定読者は以下のとおりである。(§ 2.4)

- ・ GxP 規制対象ユーザー
- ・ システムの供給者
- ・ 査察官

3.5. イタリック体部分

ガイダンス原文にイタリック体で記載された部分がある。監査者や査察官はその部分に対する適合性の証拠を検討したいと思うかもしれない。(§ 2.8)

3.6. 読み方

このガイダンスは長年にわたり、多国籍の多様な研究班による作業により進化してきた。そのため、このガイダンスにはある程度の重複記述がある。また以下の理由から、いくつかのセクションは独立したものとなっている。(§ 2.10)

- ・ 最初から最後まで通読されることを意図していない
- ・ 必要なときに参考書として「チョイ読み」されることを意図している

4. 意識部分の概要

意識した各セクションの概要もしくはキーワードを以下に 1 行程度で参考として記載する。「5. 抜粋意識」に目を通す場合のイメージ把握に活用されたい。

4.1. バリデーション方針と優先順位 (14 章)

- ・ システムのバリデーション状況を示す証拠を提示できること (§ 14.1)
- ・ ライフサイクル全般の品質と性能の度合いを評価・報告する仕組みがあること (§ 14.2)
- ・ システムを一覧表にリストアップし、GxP 適合性の管理を行うこと (§ 14.3)
- ・ GxP 適合の証拠を残すこと (§ 14.4)
- ・ 紙ベースからコンピュータ化システムに移行しても、GxP 適合必要性は減らない (§ 14.5)
- ・ GAMP の供給者ガイドは供給者にとって必須のガイドである (§ 14.6)

4.2. データ変更-監査証跡と重要データ入力 (20 章)

- ・ 監査証跡の要件 (20.1)
- ・ 二次チェックが必要な重要なデータ入力には、特別な手順が必要である (§ 20.2)
- ・ 監査証跡の対象記録は文書で規定しておくこと (§ 20.3)
- ・ GxP 電子記録・電子署名には権限ユーザーの登録などを適切に維持管理する必要がある (§ 20.4)
- ・ システム・装置間のデータ伝送を確認した記録が必要 (§ 20.5)

4.3. 電子記録と電子署名 (21 章)

- ・ EU-GMP における電子記録のバリデーション要件 (§ 21.1)
- ・ EU-GMP の文書要件から導かれる電子記録に対する実践規範 (§ 21.2)
- ・ 製造工程をとおして明確で正確な監査証跡があり、適切な期間、当局に提示できること (§ 21.3)
- ・ 記録とは、全ての重要な活動や出来事がトレース可能であり、また明確でかつ容易に参照可能でなければならない (§ 21.4)
- ・ 電子記録および電子署名を使用する場合、GxP 要件を満たすこと (§ 21.5)
- ・ 電子記録を採用した場合の監査証跡、およびハイブリッドにおける手順管理による監査証跡 (§ 21.6)
- ・ バッチリリースを電子的に署名してよい (§ 21.7)
- ・ コンピュータ化システムに対する管理・運用のポイント (§ 21.8)
- ・ 電子署名使用時の GxP 適合性評価ポイント (§ 21.9)
- ・ GxP データ保持に電子記録を使用している場合の検討ポイント (§ 21.10)
- ・ 変更管理および改訂処理の監査証跡に確実に文書化する手順があること (§ 21.11)
- ・ GxP システムがシステム外部にアクセスする場合 (オープンシステム) の検討事項 (§ 21.1)
- ・ 追加のセキュリティ対応が必要になる場合 (§ 21.13)

4.4. 査察において考慮すべきこと (23 章)

- ・ GxP 査察はサイトだけでなく本社の IT 部門に及ぶかもしれない (§ 23.1)

- ・ 査察官は自動化されたシステムの GxP 適合性を技術面だけではなく、GxP リスクの面からも調査すること (§ 23.2)
- ・ 自動化システムが適切に管理されていないと、危機的エラーが発生しうる (§ 23.3)
- ・ 査察官はこのガイダンスを選択的に使用し、リスクの高い部分を選択的に調査すべきである (§ 23.4)
- ・ 必要に応じ、事前査察質問票を使用し、査察前に状況把握を行うこと (§ 23.5)
- ・ 重要システムに対し、バリデーション記録と日常業務の管理を調査すること (§ 23.6)
- ・ GxP の重要システムは、製品品質および患者の安全性に直接影響する (§ 23.7)
- ・ 供給者の支援が得られずバリデートできないシステムは、ユーザーレベルで正当化を行い、フェールセーフ導入による補強や、更新の検討を行うこと (§ 23.8)
- ・ バリデーション取り組みはライフサイクル方法論に従うべき (§ 23.9)
- ・ 査察官はバリデーションサマリ報告書をレビューし、必要に応じシステム受入テスト仕様書とその下位文書を参照すること (§ 23.10)
- ・ 査察官はエラーや逸脱が解決できていることを確認すること (§ 23.11)
- ・ 査察官は、PIC/S GMP Annex 11 の原則、1、2、3、4、5、7を確認すべき (§ 23.12)
- ・ PIC/S GMP Annex 11 の 4 項および 5 項の不備は、バリデーション記録の不備とともに重要かつ主要な欠陥となりうる (§ 23.13)
- ・ バリデーションの証拠が十分である場合に査察官が調査すべきポイント (§ 23.14)
- ・ 考慮すべきその他の規格/標準/ガイドライン (§ 23.15)
- ・ 査察官による欠点評価は、アプリケーションのリスク評価とリスク重要度に基づく (§ 23.16)

5. 抜粋意訳

14. VALIDATION STRATEGIES AND PRIORITIES

- 14.1 Regulated users need to be able to provide evidence for their computerised systems to demonstrate their range, complexity, functionality, control and validation status.
- 14.2 For the validation of computerised systems there should be a system in place that assures the *formal assessment and reporting* of quality and performance measures for all the life-cycle stages of software and system development, its implementation, qualification and acceptance, operation, modification, requalification, maintenance and retirement²³. This should enable both the regulated user, and competent authority, to have a high level of confidence in the integrity of both the processes executed within the controlling computer system(s) and in those processes controlled by and/or linked to the computer system(s), within the prescribed operating

²³ Tools and controls within the QMS, such as audits, change controls, configuration management and continuous improvement programmes may feature here.

14. バリデーション方針と優先順位

- 14.1 規制対象ユーザーは、コンピュータ化システムの範囲、複雑度、機能、管理、バリデーション状況を示す証拠を提示できる必要がある。
- 14.2 コンピュータ化システムをバリデートする場合、以下に対するライフサイクルの全段階における品質と性能の度合いを確実に**正式に評価・報告**する仕組みが実施されていること²³。
- ・ ソフトウェアとシステムの開発
 - ・ その実装
 - ・ 適格性評価と受入
 - ・ 操作
 - ・ 変更

²³ QMS（品質管理システム）における方法と管理、すなわち監査、変更管理、構成管理、継続的な改良計画が主要なものだろう。

environment(s)²⁴. (See also Section ‘4.6’)

14.3 ***The regulated user’s range of computerised systems needs to be formally listed in an inventory and the scope/extent of validation for each detailed in a consolidated written Validation programme²⁵. Validation scope should include GxP compliance criteria, ranked for product/process quality and data integrity risk criticality, should the system fail or malfunction. This process represents one of the most important pre-requisites of Validation Master Planning (see PIC/S doc. PI 006), in that it is essential to assign priorities and attention to those systems (and features within systems) that***

- 再適格性評価
- 保守と退役

このことにより、上述の稼働環境において、以下の両方が完全であることを規制対象ユーザーと管轄当局の双方が確信できる²⁴。
(セクション 4.6 も参照のこと)。

- 制御コンピュータ化システムにおいて実行されている処理
- コンピュータ化システムにより制御され、そのコンピュータ化システムに接続されているプロセス

14.3 ***コンピュータ化システムにおける規制対象ユーザーの範囲は、正式に一覧表にしておく必要がある。個々のシステムに対するバリデーション範囲と程度は一元管理されたバリデーションプログラムに詳述しておく必要がある²⁵。バリデーション範囲には GxP 適合性判定基準を含むこと。この判定基準は、システムが故障あるいは動作不良となった場合の製品/プロセスの品質とデータの正確性リスクの危険度に基づいて等級付けされる。この一覧表作成はバリデーションマスタープランにおける最も重要***

²⁴ The italicised-bold part of this definition should be interpreted as requiring controlled documented methodology and records based on best compliance practices. This is to ensure that firms have generated documented evidence (electronic and/ or paper based), that gives a high level of assurance that both the computer system and the computerised system, will consistently perform as specified, designed, implemented and validated. Related validation dossiers for complex integrated projects should be clearly cross-linked for audit purposes.

²⁵ The scope or extent of validation for each system can be detailed in individual validation plans. A hierarchy of linked validation plans may be appropriate as outlined in GAMP 4 guidance Appendix M1: ‘Guideline for validation planning’.

²⁴ この規定におけるイタリック太文字は、文書管理された手順と最良の遵守行為に基づいた記録が要求されていると解釈すべきである。コンピュータシステム及びコンピュータ化システムの両者が仕様、設計、実装、バリデートされたとおりに一貫して機能することを高い水準で保証する文書化された証拠（電子及び/または紙）を企業が作成したことが保証されることになる。複雑に統合されたプロジェクトのバリデーションに関連する書類は、監査のために明確に相互リンクされるべきである。

²⁵ 各システムのバリデーションの範囲と程度を、それぞれのバリデーション計画に詳細に記載してよい。GAMP4 ガイダンスのアペンディクス M1:「バリデーション計画のガイドライン」に概説されているように、個々のバリデーション計画書を紐付けて階層化するのが適切であろう。

represent the highest potential for disaster, should they malfunction or become inoperative. The risk analyses and the results, together with reasoning for *critical* or *non-critical* classifications, should be documented. Risks potentially impacting on GxP compliance should be clearly identified. There are a number of techniques to help identify and analyse risks and to select risk reduction and control measures. For further information refer to the GAMP Guide appendix and the GAMP Forum special interest group paper on 'Functional Risk Assessment'.

14.4 GxP compliance evidence is essential for the following aspects and activities²⁶ related to computerised systems:

- data input (capture and integrity), data filing, data-processing, networks, process control and monitoring, electronic records, archiving, retrieval, printing, access, change management, audit trails and decisions associated with any automated GxP related activity;
- in this context, examples of GxP related activities might include: regulatory submissions, R&D, clinical trials, procurement, dispensing/weighing, manufacturing, assembly, testing, quality control, quality assurance, inventory control, storage and distribution, training, calibration, maintenance, contracts/technical agreements and associated

²⁶ These examples are intended to be illustrative, not exhaustive.

な事前実施事項である (PIC/S doc. PI 006 参照)。すなわち、動作不良あるいは操作不能になった場合に惨事の可能性が最も高いシステム（およびシステム機能）に優先度を与え注目するのが必須である。リスク分析とその結果は、**重要か否か**の判定根拠と共に文書化すること。GxP 適合性に影響する可能性のあるリスクは明記しておくこと。リスクの特定と分析の助けとなる技術、リスクの低減とリスクコントロール方法を選択する技術にはいくつかある。さらなる情報は GAMP ガイドのアペンディクスと GAMP Forum special interest group の「機能リスク評価」を参照すること。

14.4 GxP 適合の証拠は、以下のコンピュータ化システムに関連した局面と活動²⁶において必須である：

- データ入力（取り込みと完全性）、データファイリング、データ処理、ネットワーク、プロセス制御とモニタリング、電子記録、保管、復元、印刷、アクセス、変更管理、監査証跡、および自動化された GxP に関連する活動に伴う判断。
- この範囲においては GxP に関連した活動の例として、以下のものを含む：規制当局への提出、研究・開発、治験、調達、調合/秤量、製造、組立、検査、品質管理、品質保証、在庫管理、保管と配送、訓練、校正、保守、契約/技術の同意、および関連する記録と報告。

²⁶ これらの例は説明を意図したものであり、網羅的なものではない。

records and reports.

- 14.5 Historically, these systems have relied on manual systems, some electromechanical controls and paper based documentation. The introduction of computerised systems does not diminish the need for compliance with GxP requirements and guidelines.
- 14.6 The current Good Automated Manufacturing Practice (GAMP) Supplier Guide provides essential guidance to suppliers of software to the Industry. The guide also provides a concise explanation of the interrelationship between various stages of software development and the requirements for Installation, Operational & Performance Qualification. The **GAMP Guide** identifies five different categories of software.

20. DATA CHANGES - AUDIT TRAIL/CRITICAL DATA ENTRY

- 20.1 Where applicable, the audit trail for the data integrity may need to include functions such as authorised user, creations, links, embedded comments, deletions, modifications/corrections, authorities, privileges, time and date, interalia. *All linked components are to be immutably³² linked in an IT system security controlled audit trail. All original data records and masters and any subsequent alterations, additions, deletions or modifications are to be retained accurately and comprehensively within the retrievable audit trail. The nature and context of transactions logged in the audit trail to be deducible from and in agreement with, the firm's approved Standard*

³² Penguin English Dictionary: 'Immutable [imewtab'ɪ] adj unchangeable; without variation - immutably adv.

- 14.5 歴史的には、これらのシステムは手動、電気機械による制御、および紙ベースの文書に依存してきた。コンピュータ化システムの導入によって、GxP 要求と GxP 指針への適合必要性が減るわけではない。
- 14.6 現在の自動化製造実践規範 (GAMP) の供給者ガイドは、この業界におけるソフトウェア供給者に必須のガイダンスである。このガイドはソフトウェア開発の種々段階と要求事項の関係を簡潔に説明している。種々の段階とは、据付時適格性評価、運転時適格性評価および稼動性能適格性評価である。**GAMP ガイド** はソフトウェアを 5 つの異なったカテゴリーに分類している。

20. データ変更 - 監査証跡/重要データの入力

- 20.1 可能であれば、データ完全性のために次のような機能を監査証跡の対象にする必要があるだろう。それは、権限ユーザー、作成、紐付け、埋め込まれたコメント、削除、変更/訂正、権限、特権、日時等の機能である。リンクされるすべての要素は、IT システムセキュリティにより管理された監査証跡に不変的に³²リンクされるべきである。すべての原データ記録と原本およびその後の変更、追加、削除または変更は、読み出し可能な監査証跡中に正確かつ包括的に保持されるべきである。監査証跡に記録された処理の本質や事情は標準操作手順書により推論できる。こ

³² Penguin 英辞書 : Immutable [imewtab'ɪ] 形容詞 変わらない ; 変化を伴わない - immutably 副詞

*Operating Procedures for information security management for the particular computerised applications and user's authorities*³³. Firms will need clearly documented policies, standard operating procedures, validation reports and training records covering such system controls. Information Security Management standards such as ISO/IEC 17799:2000³⁴ may be of assistance with the design, implementation and control of such systems.

20.2 Where applicable, there should be *special procedures for critical data entry* requiring a second check, for example the data entry and check for a manufacturing formula or the keying in of laboratory data and results from paper records³⁵. A second authorised person with logged name and identification, with time and date, may verify data entry via the keyboard. For other automated systems featuring direct data capture linked to other databases and intelligent peripherals then the second check may be part of validated system functionality (e.g. in a dispensary). Special access, system

の標準操作手順書とは、特定のコンピュータ化アプリケーションやユーザー権限³³に対する情報セキュリティ管理について会社が承認したものである。会社はこのようなシステム管理を対象とする明確に文書化されたポリシー、標準操作手順、バリデーション報告及び訓練の記録を必要とするだろう。ISO/IEC 17799:2000³⁴のような情報セキュリティ管理の標準規格がそのようなシステムの計画、実行及び管理の助けになるかもしれない。

20.2 可能であれば、二次チェックが必要な重要なデータ入力のために、特別な手順があるべきである³⁵。二次チェックが必要な重要なデータ入力とは、製造処方書の入力とチェック、あるいは紙の記録から試験室データと結果をキー入力する場合などである。ログインした名前と ID、日時を付した上で、認定された第二の人が、キーボード入力されたデータを検証しても良い。他のデータベースあるいはインテリジェント型周辺機器とリンクされ、それらから直接データを取り込める自動化システムがあ

³³ The systematic contextual 'labelling' of transactions in the electronic audit trail log is recommended as it can have automated functional feedback control links with security validation features.

³⁴ Information Technology -- "Code of practice for information security management" BSI/DISC and national standards bodies. Other guidance will be found in the guidelines supporting FDA's 21 CFR Part 11.

³⁵ This is an established compliance requirement in the GMP discipline.

³³ 電子監査証跡のログにおいて、監査証跡処理の意味を示す「ラベル付け」を行うことを推奨する。このラベル付けにより、セキュリティバリデーション機能へのフィードバックリンクを自動機能として持つことができる。

³⁴ Information Technology -- "Code of practice for information security management" BSI/DISC and national standards bodies. FDA の 21 CFR Part 11 を補完するガイドライン中に他のガイダンスを見いだせるだろう。

³⁵ これは GMP 基準において規定されている遵守要件である。

control features and/or special devices such as identification code bars, and the inclusion and use of an audit trail to capture the diversity of changes possibly impacting the data may facilitate this check.

- 20.3 The *records pertaining to the audit trail* events should be documented, ideally as features of the operating system, database management system (DBMS), document management system (DMS) and other major applications. Timelinked audit trail records should be available, if required, in a human readable form as required by the inspector³⁶. *GxP Inspectors may see evidence for different forms of audit trail depending on the regulations prevailing in the intended regulated markets for the products or data.*
- 20.4 It is expected that appropriate controls will exist such as the maintenance of a *register of authorised users, identification codes, scope of authorised actions*, in support of GxP electronic records and electronic signatures.
- 20.5 There should be *records of checks* that the data/control/monitoring interface(s) between the system and equipment ensure correct input and

る。そのような自動化システムにおいては、バリデートされたシステム機能により二次チェックしてもよい（例えば、調剤室において）。このチェックには次のものが見えるかもしれない。特別のアクセス、システム管理機能、識別バーコードのような特別な機器、データに影響するかもしれない様々な変更を検知する監査証跡の採用。

- 20.3 *監査証跡事象の対象となっている記録*は文書で規定しておかねばならない。監査証跡は、オペレーティングシステム、データベース管理システム (DBMS)、文書管理システム (DMS) 及びその他の主たるアプリケーションの機能であるのが理想的である。時刻が紐付いた監査証跡記録は、査察官に要求された時、人間が読める形で提供出来ねばならない³⁶。監査証跡は色々な形式があるので、それらが規制に従っているかどうかの根拠を査察官が調べるかもしれない。その製品もしくはデータが目的とする規制市場における主な規制を対象にして調べる。
- 20.4 GxP 電子記録及び電子署名のサポートにおいては、*認定ユーザー、識別コード、権限範囲の登録記録*に対する保守のような適切な管理が期待される。
- 20.5 システムと装置間のデータ/管理/監視のインターフェースにより、正確な入出力の伝達が保証されていることの *チェック記録*

³⁶ It should be noted that for the USA market it may be a requirement in for audit trails to be available in electronic form, not just paper, but the implementation and enforcement of compliance with 21 CFR Part 11 is under review by FDA in 2003, (see Ref. 11).

³⁶ 米国市場においては監査証跡が紙ではなく電子化された形で利用できることが要求され得ることに注意すべきである。ただし、21 CFR Part 11 遵守の履行と執行は 2003 年に FDA により再検討されている (Ref. 11 参照)。

output transmission.

21. ELECTRONIC RECORDS AND ELECTRONIC SIGNATURES

EC Directive 91/356 sets out the legal requirements for EU GMP. The GMP obligations include a requirement to maintain a system of documentation, (Article 9)³⁷. The main requirements here being that the regulated user has validated the system by proving that the system is able to store the data for the required time, that the data is made readily available in legible form and that the data is protected against loss or damage.

21.2 The guidelines relating to documentation in the GMP Guide are in Chapter 4 and there is no requirement here that documents be in writing. Indeed in paragraph 4.9 the section amplifies Article 9.2 (see above). It references electronic data processing (EDP) systems and implies a number of good practice measures that should be in place to protect the data:

- access by authorised personnel only
- use of passwords

があるべきである。

21. 電子記録及び電子署名

21.1 EC Directive 91/356 では、EU GMP に対し法的な要求を定めている。GMP は文書システムの維持を要求している(Article 9)³⁷。主な要求事項としては、規制対象ユーザーが以下を立証することによりシステムをバリデートしていることである。

- ・ システムが要求期間データを保存することができる
- ・ データはいつでも判読可能な状態である
- ・ データは消失や損傷から保護されている

21.2 GMP ガイドにある文書化関連のガイドラインは第4章に記されており、そこでは文書が書面であることは求めている。確かにパラグラフ 4.9 では、9.2 項を詳細に記載している(上記参照)。そこでは電子データ処理(EDP)システムを参照しており、データを保護するための実践規範を多数暗示している：

- 許可された人のみによるアクセス
- パスワードの使用

³⁷ The main requirements in Article 9.1 are that documents are clear, legible and up to date, that the system of documentation makes it possible to trace the history of manufacture (and testing) of each batch and that the records are retained for the required time. Article 9.2 envisages that this documentation may be electronic, photographic or in the form of another data processing system, rather than written.

³⁷ 9.1 項の主な要求は、文書が明確であり、読み取ることができ、更新されていること、システムの文書化がそれぞれのバッチの製造(そしてテスト)の履歴をトレースすることを可能とし、そして、記録が要求される期間、保持されることである。9.2 項は、この文書化が書かれているものよりむしろ、電子的、写真あるいは別のデータ処理システムの形であることを想定している。

- creation of backup copies
- independent checking of critical data
- safe storage of data for the required time

Such systems also require evidence to demonstrate:

- (fundamental) the use of validated, secure computerised systems
- The systematic use of an accurate, secure, audit trail, (where appropriate)

21.3 The central consideration here as in Directive 91/356, is that records are

- バックアップの作成
- 重要データの独立チェック
- 必要期間をとおして安全に保管

このようなシステムでも実証の証拠を必要とする：

- (基本的には) バリデートされた、信頼性の高いコンピュータ化したシステムを用いる。
- (可能であれば) 正確で確実な監査証跡を体系的に使用

パラグラフ 4.9

データは、電子的データ処理システム、写真又は他の信頼できる手段により記録できるが、使用されるシステムに関する詳細な手順を設定し、又記録の正確さを確認しなければならない。文書記録が電子的データ処理方法により取り扱われる場合には、認定された者のみがコンピュータ内のデータの入力又は修正が可能であるようにしなければならない；変更及び削除の記録を残さなければならない；アクセスはパスワード又は他の手段により制限され、また重要データの入力結果は別途確認すること。電子的に保管するバッチレコードは、磁気テープ、マイクロフィルム、紙面又は他の手段へのバックアップ転送によって保護すること。データが保存期間の全期間にわたり速やかに利用できることが特に重要である。

21.3 Directive 91/356 にあるように、ここでの主たる考えとしては、

accurately made and protected against loss or damage or unauthorised alteration so that there is a clear and accurate audit trail throughout the manufacturing process available to the licensing authority for the appropriate time.

21.4 The situation for an authorised wholesale distributor is similar for records covering purchases/sales invoices, (on paper or on computer, or any other form)³⁸. The requirements for records are clear: “*Records should be made... in such a way that all significant activities or events are traceable... and are clear and readily available*”.

21.5 Regulated user companies generally have a choice as to whether to use electronic records or electronic signatures instead of paper based records. When regulated users elect to use electronic records for GxP applications then it will be necessary for the companies to identify the particular regulations being applied and whether they are to be considered legally binding and equivalent to their paper-based counterparts. *Regulations applicable to particular GxP disciplines may impose specific rules e.g. when electronic records and electronic signatures are used as a primary of data, records and/or evidence.*

It is for the regulated user to explain and justify the technologies and controls in place.

記録は正確に作られ、紛失、損傷あるいは権限外の変更から守られている。従って、製造工程をとおして明確で正確な監査証拠があり、適切な期間、医薬品許可機構に提示できる。

21.4 認定卸売業者の状況は購入/販売の送り状と似ている（紙、コンピュータもしくはその他の形式）³⁸。記録に対する要求事項は明瞭である。すなわち、「記録とは、全ての重要な活動や出来事がトレース可能であり、また明確でかつ容易に参照可能でなければならない」。

21.5 規制対象ユーザーの会社は一般的に、紙ベースに代わって電子記録あるいは電子署名を使用するかどうかの選択権をもっている。規制対象ユーザーの会社がGxPアプリケーションに電子記録を使用すると決定する場合、どの規制が適用され、電子記録に法的拘束力があり紙ベースと法的に同等なものとなされるかどうかをその会社は確認する必要がある。あるGxP規律に適用される規制は、特定のルールを強いるかもしれない。例えば、電子記録および電子署名が、データ、記録および証拠の一次資料となる場合である。

規制対象ユーザーはその技術及び管理が適正であることを説明

³⁸ The relevant EC directive being 92/25, Article 6(e), as amplified in the GDP guidelines (94/C 63/03). Article 8 of 92/25 requires that the documentation system makes it possible to trace the distribution path for every product.

³⁸ EC directive 92/95, Article 6(e)は、GDP ガイドライン(94/C 63/03)に拡大されている。Article 8 of 92/95 はすべての製品の流通経路をトレースすることが可能となる文書化システムを要求している。

An appropriate form of Electronic signature³⁹ or authentication / identification⁴⁰ should be applied where

- external access can be made to a computerised GxP system
- the system electronically generates GxP regulatory records, or
- key decisions and actions are able to be undertaken through an electronic interface.

21.6 Generally there is no requirement for records and documents created and maintained, as part of GxP, to be in ‘writing’⁴¹, and validated, secure electronic versions are permitted. In the absence of provisions to the contrary this will arguably extend to “electronic signatures”. Certainly, **where regulated users have elected to use electronic records in place of paper-based media**, then it can be argued, (from the forgoing requirements) that for accurate, authorised, secure electronic record systems

し、正当性を立証しなくてはならない。電子署名³⁹あるいは認証/識別⁴⁰の適切なフォームは次のような場合に適用すべきである。

- コンピュータ化された GxP システムに外部からアクセスできる場合
- システムが電子的に GxP 規制対象記録を作成する場合
- キーとなる判断及び行動が電子的インターフェースを通して可能な場合

21.6 GxP の一部として作成・保存される記録が「書かれたもの」⁴¹であることという一般的な要求はない。バリデートされ確実な電子版は許容される。それどころか規定がない限り、間違いなく「電子署名」へと進んで行くであろう。確かに、**規制下のユーザーが紙ベースの媒体に代えて電子記録を採用することを決定した場合**、正確で正式に認められる確実な電子記録システムとするために、（要求事項がない状態から）以下のものが理論的

³⁹ It has been proposed via industry comments that a signature should be unique to the owner of that signature but not necessarily unique to the system. It has also been argued that it may be desirable to issue and maintain only one signature across a multitude of systems. Regulated users may need to explain and justify such arrangements, controls and logic.

⁴⁰ The regulated user is expected to justify the choice of methods to be used to ensure compliance with regulations and GxP, (see glossary ‘Advanced Electronic Signature’, ‘Electronic Signature (3)’ etc.

⁴¹ In this context ‘writing’ meaning ‘written by hand and/or signed by hand’ on paper media.

³⁹ 産業側のコメントを経て、以下のことが提唱されている。すなわち、署名はその署名の所有者に対して特有のもので無ければならないが、システムに対して特有である必要は無い。また、多数のシステムにわたって、唯一の署名を発行し、保持することが望ましいかについても議論されている。規制対象ユーザーは、このような取り決め、管理及びロジックを説明し、正当化する必要があるかもしれない。

⁴⁰ 規制対象ユーザーは規制及び GxP を遵守していることを保証するために使用した方法の選択を正当化することを期待されている（用語集「高度な電子署名」「電子署名」参照）。

⁴¹ この文脈の中で「書かれたもの」とは紙媒体に「手で書かれた、あるいは手書き署名された」ことを意味する。

these systems would logically require *an attached immutable audit trail identifying person, time and date and linking to particular transactions. However, some systems may utilise a combination of human actions together with other automated functions and a variety of media for GxP data processing, records and information. Such systems may be described as ‘hybrid’ and in such cases documented procedural controls with recorded links, by reference and signatures may have to be used to complete the audit trail across, for example, a mixture of paper based records⁴² and electronic files.*

21.7 Whilst EC Directive 2001/83⁴³ requires a Qualified Person to “certify” in a ‘register’ that batches for release meet the required condition we are not aware of any provisions that would restrict this activity to paper based media and a handwritten certifying signature. Validated and secure

に必要になることが議論されることになる。

- ・ 変更されことなく付加される監査証跡
- ・ 個人を特定できる監査証跡
- ・ 日時を特定できる監査証跡
- ・ 特定のデータ処理への紐付けがなされる監査証跡

しかるに、システムによっては以下のことを利用していることがある。

- ・ 自動化機能と人による操作の組み合わせ
- ・ GxP データ処理、記録、情報のための様々な媒体

このようなシステムは「ハイブリッド」と称され、文書化された手順管理を使って監査証跡を完全なものにする必要がある。この手順管理には、資料と署名による紐付けの記録がつけられる。監査証跡は、例えば、紙ベースの記録⁴²と電子ファイルの組み合わせに対してつけられる。

21.7 EC Directive 2001/83⁴³は、バッチリリースが要求条件に適合していることをQP (Qualified Person) が「登録」において“認定”することを求めている。しかしながら、この行為を紙ベースの媒体や手書き署名に制限するような規定を我々は知らない。従っ

⁴² Including printouts from computerised systems.

⁴³ Superseding 75/319 Article 22 following codification.

⁴² コンピュータ化システムからの打ち出しを含む。

⁴³ 法令化され 75/319 Article 22 に取って代わった。

electronic data processing systems may therefore be used in this context.

21.8 *The key aspects of infrastructure, system and specific application to be controlled and managed are:*

- *the authorised user log-on for a specific application*
- *a unique combination of user ID and password called for by the computerised system and linked to the user's authorised account for the use of a specific application*
- *permitted task functionality for that user*
- *the system to have defined time zone(s) and date standard referencing with relative transaction linking, (complex systems may span several time zones)*
- *the audit trail⁴⁴*
- *other physical and logical system information security infrastructure control features.*

21.9 Issues to consider when assessing GxP compliance in the use of electronic signatures include that:

- *Documentary evidence of compliance exists for all aspects of*

て、バリデートされかつ安全な電子データ処理システムをこのような状況において使用してよいであろう。

21.8 管理・運営すべきインフラ、システム及び特定のアプリケーションにおける主要な特徴とは：

- 権限ユーザーによる特定アプリケーションへのログオン
- ユーザーID とパスワードのユニークな組み合わせ。ユーザーID とパスワードは、特定のアプリケーションを使用する際にコンピュータ化システムにより求められ、また認定ユーザーアカウントに紐付けられる。
- そのユーザーに許可された機能
- データ処理の紐付けに、タイムゾーンと日付基準を規定しているシステム（複雑なシステムはいくつかのタイムゾーンをまたがる可能性がある。）
- 監査証跡⁴⁴
- 物理的あるいは論理的なシステム情報セキュリティインフラの管理機能

21.9 電子署名使用時の GxP 適合を評価する際に検討する課題例：

- インフラ、システム及び特定のアプリケーションの全側面に対し、文書化された適合性の証拠が存在すること

⁴⁴ See previous Section ('20.1').

⁴⁴ セクション 20.1 を参照のこと

infrastructure, system and specific application.

- *Where risk assessment concludes that the use of a digital signature may be necessary (e.g. Certification to a third party or in GCP field data collection and transmission) that adequate security measures exist to protect the key to a digital signature. The level of security that is appropriate depends on the sensitivity of the transaction and the possible impact of the unauthorised use of the key. Public Key Infrastructure (PKI) may be appropriate where risk assessment indicates that a high level of security is required.*
- *A register of entities that are authorised is being maintained.*
- *There are procedures that ensure that entities authorised to use electronic signatures are aware of their responsibilities for actions initiated under their electronic signatures.*
- *Personnel administering the systems have appropriate security clearances, training, skills and knowledge.*
- *Procedures are in place to record the printed name, or 'identity', of the signer, the date and time when the signature was executed and the meaning associated with the signature.*
- *Procedures exist to try to detect the unauthorised use of an electronic signature or compromised ID password combinations.*

21.10 *Issues to consider where electronic records are used to retain GxP data:*

- *Documentary evidence of compliance exists*

- *リスク評価により、デジタル署名の使用が必要であろうと結論された場合（例えば第三者機関への認証送信、あるいはGCPにおけるデータ収集と送信）、デジタル署名の鍵を保護するための適切なセキュリティ手段が存在すること。適切なセキュリティレベルは、トランザクションの敏感さや鍵の不正使用により起こりうる影響に依存する。リスク評価において高度のセキュリティーが要求される場合は、公開鍵基盤(PKI)が適切であろう。*
- *認証された本人性登録の維持*
- *電子署名を使用する権限者に、電子署名することで生じる責任を確実に認識させる手順があること*
- *システムを管理する職員は適切な機密取扱者人物調査、訓練、技術と知識を持つこと*
- *署名者の記名または「本人識別」、署名がなされた日付、および署名の意味を記録する手順が実施されていること*
- *電子署名の不正使用、あるいは信用出来なくなったIDとパスワードの組み合わせを検出する手順があること*

21.10 *GxP データ保持に電子記録が使われている場合の検討課題：*

- *文書化された適合性の証拠が存在すること*

- *Archiving procedures* are provided and records of use exist
- *Procedures exist* to ensure accuracy, reliability and consistency in accordance with the validation exercise reported for the electronic record system
- *System controls and detection measures (supported by procedures) exist* to enable the identification, quarantining and reporting of invalid or altered records
- *Procedures exist* to enable the retrieval of records throughout the retention period
- *The ability exists* to generate accurate and complete copies of records in both human readable and electronic form
- Access to records is limited to authorised individuals
- *Secure, computer-generated, time-stamped audit trails to independently record GxP related actions following access to the system are used*⁴⁵.

21.11 *Procedures exist* to ensure that change-control and revision (additions, modifications, deletions) transactions are documented in the audit trail.

- *保管手順*があり、その手順を使用した記録が存在すること
- 正確性、信頼性、一貫性を確実にする *手順*があること。その手順は、電子記録システムに対し報告されたバリデーション内容に合致していること。
- 無効または改変された記録を識別し、隔離保管し、そして報告できる *システム管理と検出方法 (手順によりサポート)* があること
- 保存期間を通して、記録を取り出す *手順*があること
- 人が読める形式かつ電子フォームにより記録を正確かつ完全に複製できること
- 記録へのアクセスが権限のある個人に制限されていること
- システムにアクセスした後に、*GxP 関連の操作を個別に記録*するために、*確実な、コンピュータで生成され、タイムスタンプされた監査証跡*が使用されること⁴⁵

21.11 変更管理及び改訂処理（追加、修正、削除）を監査証跡に確実に文書化する *手順*があること。

⁴⁵ A database management system (DBMS) will have this included as an optional feature, but for other systems it may be necessary to ensure that it is an added function. Regulated users will then need to ensure that it is left 'switched' on.

⁴⁵ データベース管理システム（DBMS）は監査証跡をオプション機能として取り込むだろう。しかし、他のシステムでは、監査証跡が追加機能であることを保証する必要があるだろう。規制対象ユーザーは、監査証跡を確実にオンの状態にしておく必要があるだろう。

21.12 *Issues to consider when the GxP system has a provision for external access*⁴⁶:

- The system has a method of ensuring that external access and inputs come *only from authorised clients* and that they come *in the correct format*, for example as encrypted, digitally signed mail or data packets. *A mechanism must exist to quarantine external inputs where security conditions are not met.* The information security management arrangements need to cover the quarantine, notification and the final sentencing of such inputs.
- Mechanisms are in place to ensure that all external access can be tracked. *Each element of the processing stage should incorporate logging and monitoring facilities. However, inspectors may expect to see less onerous tracking for ‘read only’ access to a suitably secure and protected system.*
- *The capacity should exist to keep copies of data and to re-send them from one stage to another if they get “lost” or corrupted at a later stage of processing.*

21.13 *Additional security arrangements and controls will be needed for GxP computerised systems which electronically generate regulatory records,*

21.12 GxP システムに外部アクセス⁴⁶の用意がある場合に考慮すべき課題

- 外部からのアクセス及び入力に許可されたクライアントからのみ来ており、正しいフォーマットで来ていることを保証する方法をシステムが持っていること。デジタル署名をしたメールやデータパケットはその方法例である。セキュリティ状態が十分でない場合には、外部入力を検疫するようなメカニズムがなくてはならない。情報セキュリティマネージメントを調整して、このような外部入力に対する検疫、通知および最終判決を行えるようにする必要がある。
- 全ての外部アクセスを確実に探知できるようなメカニズムを整えておくこと。このメカニズムの処理段階における各要素は、記録機能とモニタリング機能を備えていること。しかしながら、査察官は、十分に安全で保護されたシステムへの「読み取り専用」アクセスという楽なシナリオを期待している。
- 処理の後段階でデータが「消失」あるいは破壊される場合、データのコピーを保持し、次の段階へデータを再送する能力が必要である。

21.13 以下のような GxP コンピュータ化システムに追加のセキュリティ対策や管理が必要になるだろう。

⁴⁶ Sometimes referred to as ‘open’ systems

⁴⁶ 「オープン」システムと呼ばれることがある。

allow external access, or enable key decisions and actions to be undertaken through electronic interfaces. These requirements are being determined largely by international initiatives to establish electronic commerce⁴⁷. However, where firms are interfacing such open system (external access) functionality, in whole or in part, with their GxP systems, *then the security, control and validation information will need to be documented and available to GxP inspectors.*

23. INSPECTION CONSIDERATIONS

23.1 The attention paid by inspectors to the assessment of the GxP implications of computerised systems on a site (and between sites), will be determined to some extent by the overall *site history and risk assessment* carried out by the inspector in preparing for the inspection. Information computer technology management arrangements for the procurement and validation of software and systems may be centralised at the regulated user's headquarter site rather than at the site of inspection. In such circumstances the controls, SOPs and records in place to ensure GxP compliance at

- 電子的に規制記録を生成
- 外部アクセスが許されている
- 電子的インターフェースを通し、主要な判断や操作が実行できる

このような要求事項は多くの場合、電子商取引を確立しようとする国際的な取り組みのもとに決定される⁴⁷。しかしながら、企業がこのようなオープンシステム（外部アクセス）機能の全部もしくは一部を GxP システムに接続する場合、セキュリティ、管理、およびバリデーション情報が文書化され、GxP 査察官に利用できるようになっている必要がある。

23. 査察において考慮すべきこと

23.1 査察準備の過程において査察官はそのサイトの歴史やリスクを全体的に評価する。サイトもしくはサイト間コンピュータ化システムの GxP 影響度を評価するにあたり査察官が払う注意は、ある程度その歴史やリスクの評価結果による。ソフトウェアやシステムの調達やバリデーションに対するコンピュータ技術管理は、査察されるサイトではなく規制対象ユーザーの本社で集約して取り決められるだろう。このような状況下では、査察サイトでの GxP 適合を確かなものとする管理・SOP・記録が

⁴⁷ Including 21 CFR Part 11. Title 21 Code of Federal Regulations Part 11 (21 CFR Part 11), which was issued by the US FDA in 1997 and provides criteria under which that agency considers electronic records and electronic signatures to be equivalent to paper records and hand-written signatures. In Europe EC Directive 1999/93/EC (December 1999) on a community framework for electronic signatures and EC Directive 2000/31/EC (May 2000) on electronic commerce in the internal market are important. These directives were implemented during 2001. It is not the purpose of GxP guides to reproduce such business and commerce requirements.

⁴⁷ 21 CFR Part 11 を含む。21 CFR Part 11 は 1997 年にアメリカ FDA により公布され、当局が電子記録・電子署名を紙の記録及び手書き署名と同等とみなすための基準を与えた。欧州では、電子署名に対する EC 枠組みに関する EC Directive 1999/93/EC (1999 年 12 月) 及び EC 内市場における電子商取引に関する EC Directive 2000/31/EC (2000 年 3 月) が重要である。これらの指令は 2001 年に履行された。このようなビジネスや商取引の要求を複製するのは GxP ガイドの目的ではない。

inspection sites will need to be made available on site. In some circumstances it may also be necessary to consider an inspection at the HQ site.

- 23.2 Clearly where a site has a lot of automation and integrated computerised systems - and manufactures a range of sterile products - (for example), then the **potential** risks from a GxP failure, (whether computer related or otherwise) for the patient are high. However, where such automated systems are well designed, implemented, managed and controlled, then potential risks to product quality (and to patients) may be considerably reduced, compared with labour intensive operations, as the latter carry inherent risks from human variability and errors. Inspectors have to come to a judgement on this by *studying the firm's evidence not just in relation to the technology aspects (through the application of GAMP etc.) but also the GxP risks identified (through PQ⁵⁰ reports and such-like)*
- 23.3 Humans design, build, test, implement **and change** these complex systems and there is opportunity for critical error with automated systems at any stage in the life-cycle unless properly managed. The GAMP Guide provides relevant guidance on these aspects.
- 23.4 It is not intended that this guidance should be used as a 'blunt instrument' for all on-site inspections but inspectors should use it selectively to build up a

そのサイトで利用できるようにしておく必要がある。場合によっては、本社サイトでの査察も考慮に入れる必要があるかもしれない。

- 23.2 自動化され統合されたコンピュータ化システムを多く持つサイト、そして（例えば）様々な無菌製品を製造するサイトでは、コンピュータに関連するか否かに関わらず患者にとって **GxP** 不適合となりうる潜在的なリスクが高いのは明らかである。しかしながら、自動化システムがうまく設計、実装、管理、制御されている場合、製品品質及び患者に対する潜在リスクは、人が操作する場合に比べて軽減される。それは、後者には人の変動やエラーに内在するリスクがあるからである。査察官はこれらの判断ができるようにならなければならない。そのためには、企業が提示する **GAMP** 等の適用を通じた技術面の証拠だけでなく、**PQ⁵⁰** 報告書や類似のものを通して認識される **GxP** 上のリスクについても調査を行うこと。
- 23.3 人はこれらの複雑なシステムを設計、構築、テスト、実装し、**変更を加える**。自動化システムが適切に管理されていない場合、そのライフサイクルのあらゆる場面において危機なエラーが発生する可能性がある。**GAMP** のガイドはこういった面に対して適切なガイダンスを提供している。
- 23.4 本ガイダンスを鈍器（＝効果のない手段）としてすべての現場査察で使用すべきと言うつもりはない。査察官は本ガイダンス

⁵⁰ PQ = Performance Qualification

⁵⁰ PQ = 稼動性能適格性評価

clear picture of a company's scale and complexity of on-site computerization (or automation) and investigate selectively the critical systems and risks. As stated in '2.7' of this PIC/S guidance, inspectors may wish to consider evidence for compliance with GxP as indicated by *italicised text* throughout the document. Table 1 (page 34) immediately following this section provides a suggested checklist for information to be considered prior to inspection⁵¹.

- 23.5 Where little is known about computerization on a site, then it may be necessary to use a *pre-inspection questionnaire* to amplify the Site Master File details.
- 23.6 Inspectors should *select the GxP critical computerised systems* from the information provided and consider firstly the *validation evidence* for the selected system(s) and then the *routine operational controls* for maintaining a valid system that is accurate and reliable. Inspectors may find that different departments in pharmaceutical companies will have responsibility for GxP aspects of commercial, or business (IT systems) and lower level process control systems. *Look for evidence of inconsistency, or muddled standards.*
- 23.7 GxP critical computerised systems are those that can affect product quality

を選択的に使用して企業の規模や現場のコンピュータ化（あるいは自動化）の複雑さを明確にイメージし、重要なシステムとリスクを選択的に調査すべきである。本 PIC/S ガイダンスの"2.7"に記載したが、査察官は本書にイタリック体で示したように GxP に適合していることの証拠を検討したいと思うであろう。このセクションの直後にある（34 ページの）表 1 は、査察に先立ち検討する情報の推奨チェックリストである⁵¹。

- 23.5 サイトのコンピュータ化についてわかっていることが少ない場合、*事前査察質問票*を使用してサイトマスターファイルの詳細を明らかにしておくべきである。
- 23.6 査察官は提供された情報から *GxP の重要なコンピュータ化システム*を選択し、まず選択されたシステムのバリデーションの証拠を、そして正確で信頼性のある妥当なシステムを維持するための*日常業務の管理*を検討すべきである。商取引、ビジネス (IT システム) および下位のプロセス制御システムの GxP 面に対する責任を製薬企業における様々な部門が負っていることを、査察官は発見するであろう。*矛盾した証拠や曖昧な基準を探すこと。*
- 23.7 GxP の重要なコンピュータ化システムは、製品の品質および患

⁵¹ An electronic keyword search of GxP documents will reveal specific compliance requirements to assist in preparing for particular topic inspections. Keywords such as: 'document', 'specification', 'formula', 'procedure', 'record', 'data', 'log book', 'instruction', 'written', 'sign', 'approve', 'writing', 'signature' are particularly helpful for records, data, documentation, authorisation and signature issues.

⁵¹ GxP 文書に電子的キーワード検索を行えば、遵守すべき特定の内容が明らかになり、特定課題の査察を準備する助けとなろう。キーワードとして、「文書」、「仕様」、「処方」、「手順」、「記録」、「データ」、「ログブック」、「指示」、「書かれた」、「サイン」、「承認」、「記載」、「署名」が、記録、データ、文書、権限付与や署名といった課題の役に立つ。

and patient safety, either directly (e.g. control systems) or the integrity of product related information (e.g. data/information systems relating to coding, randomisation, distribution, product recalls, clinical measures, patient records, donation sources, laboratory data, etc.). This is not intended as an exhaustive list.

23.8 *It is essential that firms have a computerised systems validation policy together with linked SOPs and plans, including a listing, or inventory, of all their computerised systems - classified as to their use, criticality and validation status.* For long standing systems, validation may have been carried out retrospectively and for systems purchased or implemented in the last few years, the validation should have been carried out (and recorded) prospectively. Firms should have plans to complete any outstanding retrospective validation of GxP related computer systems within a reasonable time period depending on the risks and complexity of the systems. The continued use of critical systems that are unsupported by suppliers and cannot be validated must be justified by regulated users, supported by alternative fail-safe arrangements and considered for urgent phased replacement.

23.9 The firm's validation approach should follow a life-cycle methodology, with management controls and documentation as outlined in this guidance, which contains consensus best practice guidelines.

者の安全に直接（例えば制御システム）影響する。あるいはコーディング、ランダム化、流通、製品リコール、臨床方法、患者記録、寄付源、試験室データに関するデータ/情報システムなどの製品関連情報の完全性にも影響する。上述は網羅的なリストではない。

23.8 企業がコンピュータ化システムのバリデーションポリシーを持っているのは必須である。また、ポリシーに紐付けられた SOP や計画も持っており、全てのコンピュータ化システムのリストか一覧表も含まれている。コンピュータ化システムは、用途、重要度およびバリデーション状況に関してクラス分けされている。長く稼動しているシステムでは回顧的にバリデーションが実施されたであろうし、ここ数年で購入または構築されたシステムでは稼動前にバリデーションが予測的に実施され（記録され）たはずである。GxP に関連するコンピュータシステムのうち回顧的バリデーションが完了していないものについて、システムのリスクや複雑さに応じて適切な期間の間に企業はバリデーションを完了させる計画を持つべきである。重要なシステムの内、供給者からサポートが受けられずバリデートできないシステムを継続利用するためには、規制対象ユーザーが正当化を行い、代替のフェールセーフ導入により補強し、早い段階での更新を検討しなければならない。

23.9 企業のバリデーション取り組みは、ライフサイクル方法論に従うべきであり、合意された最良の規範ガイドラインを含む本ガイダンスで概観したような管理や文書化を伴う。

23.10 Inspectors should review the firm's *Validation Summary Report*⁵², (VSR) for the selected system and refer as necessary to the *System Acceptance Test Specification* and lower level documents. They should *look for evidence that the qualification testing has been linked with the relevant specification's acceptance criteria, viz:*

- PQ versus URS .
- OQ versus FS⁵³
- IQ versus DS or DR⁵⁴
- Supplier audit reports
- Validation and *quality plans. e.g. Validation Master Plan, (VMP) or Policy.

(*For big projects there should be a project quality plan and a QMS for the documentation. For smaller projects established SOPs may suffice)

23.10 査察官は選定したシステムに対するバリデーションサマリー報告書⁵² (VSR) をレビューし、必要に応じ、システム受け入れテスト仕様書とその下位文書を参照すべきである。適格性テストが、関連する仕様書の受け入れ基準に紐付けられている証拠を査察官は探すべきである。すなわち：

- PQ と URS
- OQ と FS⁵³
- IQ と DS あるいは DR⁵⁴
- 供給者監査報告書
- バリデーション文書と品質計画文書*。例えば、バリデーションマスタープラン (VMP) あるいはバリデーションポリシー

(*大規模プロジェクトではプロジェクト品質計画書があり、文書の QMS がある。小規模プロジェクトでは既定の SOP があれば十分である。)

⁵² VSR=A best practice high level report, summarising the validation exercise, results and conclusions, linking via cross referencing to lower level project records, detailed reports and protocols. This is useful for briefing both senior managers, in regulated user organisations and for reference by auditors/ inspectors.

⁵³ OQ = Operational Qualification; FS = Functional Specification

⁵⁴ IQ = Installation Qualification; DS= Design Specification; DR = Design Review

⁵² VSR=最上位の実践報告書で、バリデーションの実施、結果、結論を要約し、より下位のプロジェクト記録、詳細な報告書やプロトコルと相互参照されるもの。これは、規制対象ユーザーの組織内の上級管理者間の打ち合わせ及び監査者や査察官が参照するの役に立つ。

⁵³ OQ=運転時適格性評価、 FS=機能仕様書

⁵⁴ IQ=据付時適格性評価、 DS=設計時適格性評価、 DR=設計レビュー

- 23.11 *Inspectors should look for the traceability of actions, tests and the resolution of errors and deviations in selected documents. If the firm has **not** got proper change and version controls over its system life-cycle and validation documents, then the validation status is suspect.*
- 23.12 *Inspectors should consider all parts of PIC/S GMP Annex 11 for relevance to particular **validation projects** and in particular, the 'Principle' and items 1, 2, 3, 4, 5 and 7.*
- 23.13 ***The lack of a written detailed description of each system, (kept up-to-date with controls over changes), its functions, security and interactions (A11.4); a lack of evidence for the quality assurance of the software development process (A11.5), coupled with a lack of adequate validation evidence to support the use of GMP related automated systems may very well be either a critical or a major deficiency. The ranking will depend on the inspector's risk assessment judgement for particular cases. (NB. Since 1983, the GMPs have called for validated electronic data-processing systems and since 1992 for the validation of all GMP related computer systems).***
- 23.14 *If satisfied with the validation evidence, inspectors should then study the system when it is being used and calling for printouts of reports from the system and archives as relevant. All points in Annex 11 (6, 8-19) may be relevant to this part of the assessment. Look for correlation with validation work, evidence of change control, configuration management, accuracy and*
- 23.11 査察官は、選択した文書にあるエラー及び逸脱について、対応、テスト、解決が追跡できることを確認すべきである。査察している企業がシステムのライフサイクル及びバリデーション文書に適切な変更並びに版管理をしていなければ、そのシステムがバリデートされている状態であるとはいえない。
- 23.12 査察官は特定のバリデーションプロジェクトの妥当性についてはPIC/S GMP Annex 11 のすべての項目を検討すべきである。特に'PRINCIPLE'と1,2,3,4,5 及び7項を検討すべきである。
- 23.13 各システム、(変更管理により最新状態に保たれている)、その機能、セキュリティと相互作用を詳細に記述した文書の欠如(PIC/S GMP Annex11 の第4 項) ; ソフトウェア開発プロセスの品質保証の証拠の欠如(PIC/S GMP Annex11 の第5 項); これらは、GMP 関連の自動化システムの使用を支援する適切なバリデーション証拠の欠如と共に、重要かつ主要な欠陥となりうる。順位付けは特定のケースに対する査察官のリスク評価判断に依存する。(注 1983 年以來 GMP は、バリデートされた電子データ処理システムを求めてきた。そして、1992 年以來、GMP 関連のコンピュータシステムはすべてバリデーションするようになっている。)
- 23.14 バリデーションの証拠が十分であれば、実使用中のシステムにおいて報告および関連するアーカイブをプリントアウトしようとしているときに査察官はシステムの調査を行うべきである。PIC/S GMP Annex 11 (6, 8-19)中のすべてのポイントはこの部分の評価に関連していそうである。バリデーション作業、変更管

reliability. Security, access controls and data integrity will be relevant to many of the systems particularly EDP (i.e.: **Electronic Data Processing**) systems.

23.15 Consider also PIC/S GMP 4.9 and EC Directive 91/356/EEC Article 9(2) for EDP systems. Guidance on the common industry interpretation of Annex 11 is given in the GAMP Guide, from the German APV.

23.16 Deficiency ratings applied by Inspectors will be based on the relative risk

理の証拠、構成管理、精度と信頼性の相関を探ること。セキュリティ、アクセスコントロール、およびデータの完全性は多くのシステム、特にEDP (**Electronic Data Processing**) システムに関連するであろう。

23.15 PIC/S GMP 4.9 と EC Directive 91/356/EEC Article 9(2) for EDP systems も検討すべきである。PIC/S GMP Annex 11 の業界共通解釈に対するガイダンスが、ドイツ APV から出された GAMP ガイドにある。

PIC/S GMP 4.9

データは、電子的データ処理システム、写真又は他の信頼できる手段により記録できるが、使用されるシステムに関する詳細な手順を設定し、又記録の正確さを確認しなければならない。文書記録が電子的データ処理方法により取り扱われる場合には、認定された者のみがコンピュータ内のデータの入力又は修正が可能であるようにしなければならない、変更及び削除の記録を残さなければならない；アクセスはパスワード又は他の手段により制限され、また重要データの入力結果は別途確認すること。電子的に保管するバッチレコードは、磁気テープ、マイクロフィルム、紙面又は他の手段へのバックアップ転送によって保護すること。データが保存期間の全期間にわたり速やかに利用できることが特に重要である。

23.16 査察官による欠陥評価は、アプリケーションの相対的なリスク

of the application and their judgement of risk criticality.

評価と、リスクの重要度の判断に基づいて行われる。

国内規制 (医薬品関 連)

- [電磁的記録・電子署名](#)
- [薬事法関連](#)
- [GLP](#)
- [治験薬](#)
- [GCP](#)
- [GPSP](#)
- [GVP](#)
- [GMP](#)
- [GQP](#)
- [CTD/eCTD](#)
- [国内法令検索](#)
- [総合機構 \(PMDA\) のお役立ちページ](#)

ICHガイドライン

FDA規制

EU規制

PIC/S GMP

■ PIC/S GMP Guideについて

PIC/S発出文書は[こちらからダウンロード](#)。

PIC/S GMP Guideとして以下のものが掲載されており、カテゴリは「Documents for industry」（業界向け文書）。

PE 009-10 (Intro)	PIC/S GMP GUIDE (INTRODUCTION)
PE 009-10 (Part I)	PIC/S GMP GUIDE (PART I: BASIC REQUIREMENTS FOR MEDICINAL PRODUCTS)
PE 009-10 (Part II)	PIC/S GMP GUIDE (PART II: BASIC REQUIREMENTS FOR ACTIVE PHARMACEUTICAL INGREDIENTS)
PE 009-10 (Annexes)	PIC/S GMP GUIDE (ANNEXES)
PI 020-3	SITE MASTER FILE FOR PLASMA WAREHOUSES

「Documents for inspectors」（査察官むけ文書）として以下のものが掲載。

PI 011-3	GOOD PRACTICES FOR COMPUTERISED SYSTEMS IN REGULATED GXP ENVIRONMENTS 査察官向けガイダンス GxP規制環境下のコンピュータ化システムに対する実践規範
--------------------------	---

● PIC/S GMP Guideの履歴

文書番号	発効日
PE 009-10	2013/1/1
PE 009-09	2009/9/1
PE 009-08	2009/1/15

● PIC/S GMP Guideの位置づけ

- David Stokes （英国のコンサルタント、GAMP COP）
@日本PDA ERESシンポジウム 2013/10/10
 - Annex 11は法律か？
Annex 11はガイダンスである
正当な理由がない限り、規制ガイダンスには従うべき
他の方法を採用するなどガイダンスに従わない場合、その論拠を文書化しておくのがよい
 - Annex 11はほとんどが一般常識であり、一般的な実践規範である
 - GAMPを適用しているほとんどの企業においては、Annex 11の要件を満たすための課題はない

- Karl-Heinz Menges (ドイツの査察官、Annex 11策定メンバー)
@日本PDA ERESシンポジウム 2013/10/10
 - **Annex 11を理解するには、EU-GMP (PIC/S GMP) Part Iの第4章「文書化」を熟知していること**

● **PI 011(査察官ガイド) の位置づけ**

- Karl-Heinz Menges (ドイツの査察官、Annex 11策定メンバー)
@日本PDA ERESシンポジウム 2013/10/10
 - 査察官はコンピュータを熟知しているとは限らない。PI 011はそのような査察官むけのガイダンスである
 - **PI 011は製薬企業に対する要件ではない**
 - **製薬企業に対する要件はPE-009 (PIC/S GMP Guide) である**

■ **PE 009-10 GMP Guide** 発効 : 2013/1/1

● **原文 (PIC/S)**

- [Introduction](#)
- [Part I \(Medicinal Products\)](#)
- [Part II \(APIs\)](#)
- [Annexes](#)

● **邦訳 (厚労省)**

事務連絡「PIC/SのGMPガイドラインを活用する際の考え方について」

(2012/2/1) および事務連絡「PIC/SのGMPガイドラインを活用する際の考え方についての一部改正について」(2013/3/28) に添付されている邦訳。

- [Part I \(医薬品\)](#)
[第4章「文書化」](#) (Documentation) ★改定
- [Annex 1 :](#) 無菌医薬品の製造
- [Annex 2 :](#) 生物学的製剤の製造
- [Annex 3 :](#) 放射性医薬品の製造
- [Annex 6 :](#) 医療用ガスの製造 ★改定
- [Annex 7 :](#) 植物性医薬品の製造 ★改定
- [Annex 8 :](#) 原料及び包材のサンプリング
- [Annex 9 :](#) 液剤、クリーム剤及び軟膏剤の製造
- [Annex 10 :](#) 定量噴霧式吸入剤の製造
- [Annex 11 :](#) コンピューター化システム ★改定
(Part 1の第4章「文書化」を理解したうえでAnnex 11を解釈すること)
- [Annex 12 :](#) 医薬品製造における電離放射線の使用
- [Annex 13 :](#) 治験薬の製造 ★改定
- [Annex 14 :](#) ヒト血液及びヒト血漿由来製品の製造
- [Annex 15 :](#) 適格性評価及びバリデーション
2014/2 [改訂ドラフト \(EU-GMP\)](#)
2014/10 改訂版発出予定 (EU-GMP)
- [Annex 17 :](#) パラメトリックリリース
- [Annex 19 :](#) 参考品及び保存サンプル

■ **PE 009-9 GMP Guide (廃止)** 発効 : 2009/9/1

- 原文 (PIC/S)

- [Introduction](#)
- [Part I \(Medicinal Products\)](#)
- [Part II \(APIs\)](#)
- [Annexes](#)

- 邦訳 (厚労省)

事務連絡「PIC/SのGMPガイドラインを活用する際の考え方について」
(2012/2/1) に添付されている邦訳。

- [Part I](#) (医薬品)
- [Annex 1](#) : 無菌医薬品の製造
- [Annex 2](#) : 生物学的製剤の製造
- [Annex 3](#) : 放射性医薬品の製造
- [Annex 6](#) : 医療用ガスの製造
- [Annex 7](#) : 植物性医薬品の製造
- [Annex 8](#) : 原料及び包材のサンプリング
- [Annex 9](#) : 液剤、クリーム剤及び軟膏剤の製造
- [Annex 10](#) : 定量噴霧式吸入剤の製造
- [Annex 11](#) : コンピューター化システム
- [Annex 12](#) : 医薬品製造における電離放射線の使用
- [Annex 13](#) : 治験薬の製造
- [Annex 14](#) : ヒト血液及びヒト血漿由来製品の製造
- [Annex 15](#) : 適格性評価及びバリデーション
- [Annex 17](#) : パラメトリックリリース
- [Annex 19](#) : 参考品及び保存サンプル

- [PI 011-3 査察官向けガイダンス](#) 発出：2007/9/25

[Good Practice for Computerised Systems in Regulated GxP Environments](#)

GxP規制環境下のコンピュータ化システムに対する実践規範

- **ガイダンスの目的**

- PIC/S査察官に対するトレーニング
- 査察において役立つ推奨事項と背景説明
- GMP以外の査察官にとっても有益であるので「GxP規制下」とした

- **改定状況**

- PI 011-3は旧版のAnnex11とGAMP 4を参照している
- 最新版のAnnex11とGAMP 5を取り込むべく改訂作業中
- 改訂版の発出次期は未定
- 改訂版発出までの間は、PI 011-3が有効

- **翻訳**

- 全文対訳：日本QA研究会 GLP部会2008年成果物「資料No.90a」
 - 全文和訳：株式会社シーエムプラスのサイトから[無償ダウンロード](#)
 - 抜粋意訳：本ページから [無償ダウンロード](#)
-