



ワークショップー 1

[講演要約]

# 21 CFR Part 11時代の実践的コンピュータ・バリデーション対応

GXP インターナショナル

テリ・ストークス博士

昨今の医薬品産業、特に製薬ビジネスを取り巻く状況においては、電子化への強い流れが見られる。このような流れを先取りする形で、米国医薬品安全局（FDA）は1997年8月に製薬企業が電子記録、またはその電子記録に対して電子署名を行う際の基準、21 CFR Part 11を施行した。当時、私は今日の講演者であるテリ・ストークス博士と、SQAP（Systems Quality Assurance Plan）の作成を一緒にやっており、その後、コンピュータ・バリデーションや Part 11に関する意見交換を現在まで引き続き行ってきた。

テリ・ストークス博士はボストン大学で生物学と科学を専攻し、ケンブリッジのレズリー大学院で MBA、そしてミネアポリスのウォルデン・ユニバーシティで経営学修士と博士号を取得。

彼女のビジネスキャリアの始まりは、医療技術者として病院や研究所のコンピュータ・システムの品質保証を11年間、担当。その後、当時のデジタルイクイップメント（DEC）社に勤務し、DEC 社に16年間在籍している間に、製薬企業、バイオカンパニー、科学企業等にコンピュータ・バリデーション・サービスを確立した。

1996年3月に DEC 社を退職し、コンサルティング事務所、GXP インターナショナルを開設し、コンピュータ・バリデーションに関するコンサルティング・サービスを開始。その後、北米、ヨーロッパ、そして日本で多くの実績を積んでいる。特に日・米・欧の3極で国際的にビジネス展開をしている製薬企業において、多くの実績がある。

(株式会社シーエーシー センター・オブ・エクセレンス統括本部  
製薬コンサルティング イニシアティブ 松井 一)

## 1. GXP の歴史と要点

21 CFR Part 11（以下、Part 11）は世界的に注目されている。どこの製薬会社であっても北米市場で事業をする

ためには、Part 11に準拠することが必要である。したがって、多くの国の製薬、医療器具、バイオ・ファーマシューティカルの企業が関心を持っている。

Part 11の歴史は長い（図1参照）。

コンピュータ・バリデーションと言われる一連の規制の

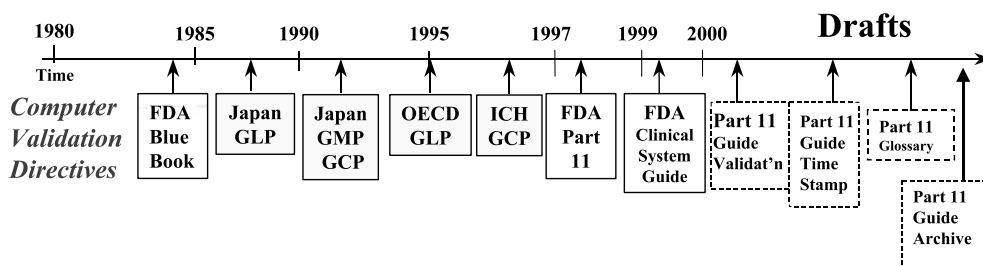


図1 コンピュータ・バリデーションに関する指針の歴史



起源は、1983年に遡る。FDA は当時、Blue Bookとして、これを発表した。このBlue Bookは、査察官に対する手引き書であり、GMP (Good Manufacturing Practice) という観点からコンピュータ・システムを査察するときに、手引きとなるものであった。

そして、80年代にはいろいろな論議が業界と当局の間で交わされた。

日本の厚生省も、1987年にGLP (Good Laboratory Practice) チェックリストを作成、そして1993年にはGMP、GCP (Good Clinical Practice) を発表した。

1997年1月に、日本、ヨーロッパ、北米が一緒になってICH (International Conference on Harmonization) の活動を行い、GCPをまとめた。

GLP、GMP、GCP、これら一連の規制を総称してGXPと呼んでいる。

さて、1997年8月、Part 11がファイナル・ルールとして登場した。つまり、米国の法規制の一部となり、製薬製品に関する規制が入った。このドキュメントは業界内に論議を呼んだ。古いシステムも規制の対象であるとしたからだ。レガシー・システムは業界に既にあったが、それもPart 11の対象とせざるをえないと読めるわけである。

Part 11に関しては、その後FDAが4つのガイダンス・ドキュメントを出した。これらはまだドラフト段階であり、ファイナルではない。だから、FDAに対して企業は、支持・不支持、反対意見等々を出すチャンスがある。

4種類のガイダンスのうち、1番最初に出たのがバリデーションに関するもの。次に、タイムスタンプに関するもの。3番目がグロスアリー、すなわち用語集。そして最新のものが、アーカイブ関係。これは、電子記録の維持管理に関するガイドである。アーカイブに関しては、今年9月5日に出たばかりである。

すべての規制には、4つのメインテーマがあると考えられる。

第1に、マネジメント・コントロール。すなわち経営陣

がコンピュータ・システムを管理する責任があるということである。エレクトロニック・データも、ワークプロセスもそれに含まれる。

第2に、システムの信頼性 (Reliability)。コンピュータは意図するように作動し、かつ反復してそれが実証されなければならない。

第3に、データの完全性 (Integrity) を保証すること。例えば、誤ったデータが入力されたら誤ったデータが出力されなければならない。コンピュータがそれを修正するようでは困る。

第4に、監査可能な品質 (Auditable Quality)。監査・査察ができるということは、コントロールの部分も、システムの信頼性の部分も、データの完全性の部分も、文書化され、文書が完備しているということである。文書がない限り、それは事実と見なされない。文書ありきということが、FDAの見方である。

上記の4つの観点から図2のようなマトリクスを想定すると、Part 11による規制の全てがこの中にマッピングできる。

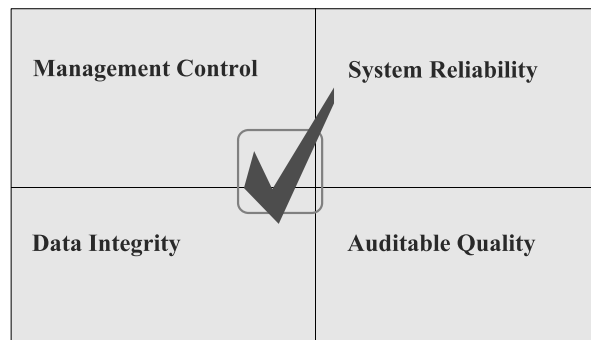


図2 要求事項のマトリクス

## 2. バリデーションに関するガイダンス

それぞれのガイダンスの内容を見てみよう。

まず、バリデーションに関するガイダンスでは、第1にシステム要件定義が重要である。エンドユーザーの要件が分かっているなければ、システム・テストもできない。また、システム仕様書はトレース可能であり、ユーザー要件と対応するものでなければならない。

バリデーションの作業のドキュメントとしては、まずマネジメントが承認したバリデーション・プランが必要とされる。そして、バリデーションを実際にシステムで実行することについて、マネジメントの承認が必要である。バリ

デーションの手順もドキュメント化されていなければならないし、実施後のバリデーション報告書も必要となる。

機器設備のインストールについては、システム・テストに先立って、ハードウェアとソフトウェアが適切にインストールされているという品質保証が必要である。システムをテストしても、それぞれのハード/ソフトが適切にインストールされていなければ何の意味もないからである。ユーザー・マニュアル、標準作業手順書（SOP: Standard Operating Procedure）、機器リスト、仕様書などが参照可能な状態にあるかということもチェックの対象となる。

ガイダンスでは、テストについて2種類を取り上げている。1つは、ダイナミック・テスト、つまりユーザーが物理的にシステムを利用している状態でのテスト。もう1つがスタティック・テクニク、これはシステム化のためのドキュメントおよびソースコードについて、ウォークスルーと技術的なレビューを行うものである。

ダイナミック・テストでは、テスト状態を明確に記録しておくことが重要である。テストプランを記載し、どのようにテストするかを明らかにし、そのテストプランのもとで実際に行ったテスト方法を記載しておく。境界値のデータレンジ、予想外のエントリーに対するチェック、エラー時の対応方法などが重要である。

ソフトウェア・テストには、構造的テスト、機能的テスト、プログラム・テストが含まれる。通常は開発者が行うものだが、テスト報告書には、合格・不合格だけでなく、定量化した記述が求められる。

バリデーションの範囲については、システム・リスクも含まれる。製品の安全性、有効性、品質にどのようなリスクがあるかを分析しておくということだ。また、データの完全性、信憑性、機密性に関してどのようなリスクがあるか、システムの複雑さによるリスクも対象範囲となる。

FDA が重視していることとして、レビューの独立性がある。システム開発者ではない別の人間がテストをすべきだということだ。複数の人の評価が入ることによって、適切な稼働を保証するのに役立つからである。

変更管理もたいへん重要であり、すべての変更について変更記録が残っていることが必要である。変更に関して何度テストをしたか、回帰テストはどれだけやっているかが問われる。それは、システムに変更が入っても以前と同じ品質が保証されなければならないからである。

市販ソフトについても、同様にテストと変更管理が行われなければならない。

インターネットのバリデーションに関しては、FDA もインターネットのそのものの検証自体はできないと認識し

ている。しかし、データの送信元、および送信先についてはシステムとしてバリデーション可能と認識している。電子署名の技術を使って、セキュリティと機密性を確保することも要求している。つまり、送信元から送信先までのやりとりが完全であったかということを確認し、かつ、送信元に照らしてみても送信先に送られたデータが正確であるか、完全であるかを見ることである。

### 3. FDA の基本的な関心事

FDA が基本的に関心を持っていることは何か？

これはガイダンスの中でもはっきりと述べられているが、コンピュータ・システムのデータを取り扱っている人たちが十分な信頼を持って、これは「紙のフォーマットと同様の信頼性があると確信できること」である。すなわち、紙の書類とコンピュータ・データが同様の信頼性がなくてはならない。このことは、コンピュータだから完全であればいいと言っているわけではない。紙も完全ではないかもしれない。ただし、完全性のレベルは同じでなくてはいけないのである。

では、データの品質という場合には、何を基準にしているのであるか。1999年4月から公式化しているガイダンス・ドキュメントの中でFDA は、次の5つの点を重視すると明記している。

1つは「Attributable」、責任の所在がわかること。すなわち記録した人をトレースできるということである。

2つ目は「Legible」、判読性ということ。

3つ目は「Contemporaneous」、同時性ということ。すなわち、データが読みとられた時点ですぐに記録されたということである。昨日見たものを観察値として今日記入することは駄目であり、即時に記入しなさいということである。

4つ目は「Original」、原本であるということ。責任を有する者が書いたオリジナルなデータでなければいけない。

5つ目は「Accurate」、正確さ。読み値、観察値に関しては正確にそれを反映していなければいけないということである。

この5つの特性の頭文字を取って「ALCOA」と覚えておくと、覚えやすい。

### 4. タイムスタンプに関するガイダンス

タイムスタンプに関するドラフトでは、主要な原則を次のように述べている。すなわち、タイムスタンプは正確で、信頼性のあるシステム時計を基準にしなければならない。

そのためには、ネットワーク・コンピュータを1つの標準的なマスター・クロック・サーバーと同期させ、マスター・クロック・サーバーを標準的なコンピュータ・クロックと同期させておかなければならない。標準的なコンピュータ・クロックとは、現地の標準時に基づいた時刻である。

システム・クロックのセキュリティを保つには、権限のない人が時間変更を行わないようなSOPが必要である。

タイムゾーンの概念もある。日本にはタイムゾーンはないが、米国には3つのタイムゾーン、ヨーロッパでも3つのタイムゾーンがある。したがって、欧米では6つのタイムゾーンがあると意識して記入をしなければいけない。つまり、ローカル・タイムとタイムゾーン・レファレンスが入ったタイムスタンプが必要となる。多くの場合は、グリニッジ標準時を指標として使っている。

年月日および時刻の表記方法も定義されている。

また、タイムスタンプは、監査証跡ともリンクしている必要がある。署名タイムスタンプ、監査証跡は日時分までトレースできなければならない。

タイムスタンプをほかの電子記録保存にも使用する際には、システムへのアクセスを制限して使うこととされている。

## 5. 電子アーカイブのガイダンス

電子アーカイブのガイダンスについて、主要な原則だけ説明しておきたい。

FDAは、電子アーカイブのガイダンスを設けると言っていた。しかし、「アーカイブ」という言葉を問題にしたようだ。アーカイブというと、銀行の貸金庫のように入れっぱなしとか、古文書といったイメージがあるかもしれない。実際はそうではなく、アーカイブと言いながらメンテナンスがなければいけない。図書館のようにアクティブなものである。

例えば、インデックスがあって検索ができる、チェックができる。媒体に関してもリフレッシュしていつでも使えるようにして、カタログ化しておくことが必要だと。そういう理由でガイダンスを「Record Maintenance Procedures」という名前に変更している。

まず、保管条件に関してチェックが必要である。修復やアクセスの制限も必要となる。提出後の記録については、変更できないようセキュリティがかかっているはずであり、閲覧も少数の人にしか許されないはずである。

IDと管理によって電子レコードの信頼性を担保する必

要がある。

電子レコードにも継続性と判読性が求められる。定期的修復、バックアップ・コピー、そしてメディアのリフレッシュが必要である。

適切な保存環境の維持も大切である。湿度、温度、ほこりなどの状態をモニターするということだ。

実際に電子レコードが検索・利用可能かというチェックも必要となる。

さらに、コピーした記録についても精度と完全性を検証しなければならない。すなわち、完全な、かつ正確なコピーを得ることが必要である。

電子レコードについて、FDAは2つのアプローチを考えている。

1つは「タイムカプセル・アプローチ」。これは、データ、ハードウェア、ソフトウェア等を全てアーカイブし、システム全体をタイムカプセルにするもの。しかし、これは大きなシステムにとっては簡単ではなく、実務的ではない。

もう1つが「マイグレーション・アプローチ」。例えば、SASの次のバージョンに、あるいはオラクルの次のバージョンにデータを移植するというアプローチである。それによって記録のアーカイブを行う。

## 6. Part 11がビジネスに与える影響

ここで、Part 11がビジネスに与える影響について考えてみたい。Part 11の影響について、経営トップが関心を向け始めており、まさに時機が到来していると思われる。

Y2K問題のあと、さまざまなコンピュータ・ウィルスの攻撃に多くの企業が直面した。そういったこともあって、マネジメントのセキュリティ意識は高まってきている。

機密性が高いデータを、不正行為から守るべきだ、そのためにも、信頼性のあるシステムが必要である。システムがクラッシュすると、ビジネス・プロセスもクラッシュし、機能しない。また、データの完全性が保たれていなければ、正しい意思決定も下せない。

さらにインターネットが浸透し、これがビジネス・チャンスでもあり、いわゆる脅威でもある。例えば、ウィルスや外部の人間がネットワークに侵入してくるからである。したがって、ファイアーウォール、ウィルスに対するプロテクトの必要性が理解されるようになった。

トップはPart 11の重要性は理解し始めているが、まだ十分に理解できていない問題点もある。すなわち、実際に電子的なオペレーションの中で、いかに自社のコントロールを発揮するか。また、電子データをどうコントロールす

るかということである。したがって、経営者の側にも今、Part 11のポリシーを策定し、コンピュータ・バリデーションを実践しようという気運がある。そのためには、まずマネジメントの役割を定義し、プランを策定し、優先順位を付けて実行していくことが必要である。

マネジメントの観点からは、システムのROI (Return on Investment: 投資対効果) が重要となる。その際に、先ほどの図2のマトリクスに示した「マネジメント・コントロール」「システムの信頼性」「データの完全性」「監査可能な品質」という4つの観点からROIを測定することが有効であろう (図3参照)。

<p>MANAGEMENT CONTROL</p> <p>Controlled and enhanced work process with e-systems</p>	<p>SYSTEM RELIABILITY</p> <p>Dependable performance of e-systems in a work process</p>
<p>DATA INTEGRITY</p> <p>Asset protection for e-data, e-systems, e-work processes</p>	<p>AUDITABLE QUALITY</p> <p>Documented quality of e-records for uneventful audits and inspections</p>

図3 ROIのマトリクス

FDAによるPart 11の適用は非常に厳格である。査察官は、システムが実際にすべてPart 11の要件に適合しているかどうかを判定する。

Part 11に不適な部分があれば、その程度も問題にする。製品の品質やデータの完全性に影響があるか、すなわち安全性、有効性、品質のファクターにどれだけ影響があるかを調査する。

また、会社が是正措置を計画しているかどうか。そのプランが適切で迅速なものかも判断基準となる。

コンプライアンスの履歴もチェックの対象になる。特に、データの完全性については過去の履歴を監査する。

FDAは監査の結果を483と呼ばれる記録用紙に記入して、問題点を経営陣に対して警告する。

非常に深刻な問題について過去に警告をしたのに改善されない場合、ウォーニング・レターが経営者に対して届く。これは、2週間以内にどのように改善したか回答せよというもので、きちんと回答しない限り、米国で新薬を発売することができなくなったり、製品の製造ができなくなったりする。

つまり、Part 11は経営者にとっても非常に重要な問題だということである。

Part 11をビジネス上で実践するステップは、次の5つに集約される。

- (1) Part 11関連システムの棚卸し
- (2) Part 11対応施策の定義と実行
- (3) 電子署名を使用する場合には、FDA へてにコーポレート・レター提出
- (4) 電子署名プロセスの管理
- (5) Part 11に則ったシステム・バリデーションの品質フレームワークに基づく責任あるドキュメント管理

## 7. Part 11対応実践の体制

Part 11とは、我が家のペットのようなものである。つまり、ライフタイムケアが必要となる。エサも水も毎日やり続けなければならない。家族の一員だから、しつけも必要。セキュリティのためにフェンスや鎖が必要となる。運動も、遊びも必要である。具合が悪い場合には獣医に診せなければならない。

Part 11も同じである。まず電源、無停電の電源が確保されなければならない。ユーザーが正しく作業できるようにトレーニングも必要。ファイアウォール、ウイルススキャン等でプロテクトしなければいけない。バックアップも必要である。テスト、変更管理、そして本当に病気になってしまうと災害復旧が必要となる。これが健康なシステムであり、健康なペットと同じである。ライフタイムケアとは、日々の業務に直結しているのである。

では、Part 11に対応する体制とシステムをいかにつくっていくか。

まず、ポリシーを明確にすること。これは法令遵守について経営陣がコミットメントするということだ。そして、企業文化の中にPart 11を埋め込むということでもある。したがって、経営陣のサポートが重要である。また、標準化を進めてCSV (Computer System Validation) を実現していかなければならない。CSVの業務とビジネスゴール、そして会社の方針・方向性が一致していることが重要である。

Part 11のポリシーは、実施され、モニターされねばならない。それを担保するためには、CSVのSOPが必要である。これは、CSVパッケージを開発するための標準となるものである。また、テストや変更管理の基準となるものでもある。

システム・バリデーションとビジネスの指示とを直結させるために、システム・クオリティ・アシュアランス・プラン (SQAP) が必要になる。

SQAP は、3種類必要である。

1つは、ERPを導入するなどといった全社的なソフトウェアに関するSQAP。

2つ目に、GCP関連、GLP関連要、GMP関連などの各グループに関するSQAP。

3つ目は、サーバーなどITプラットフォームに関するSQAP。

それぞれのSQAPの下でCSVパッケージが開発される。

各CSVパッケージの中にプランを用意しなければならない。プランに基づいて、アプリケーションおよびプラットフォームに関するコントロール、ヒューマン・インタフェース、そしてテストのワークフローを決定していく(図4参照)。

以上、Part 11に関するポリシー決定からCSVパッケージ開発までの体制について、1つの事例を紹介した。

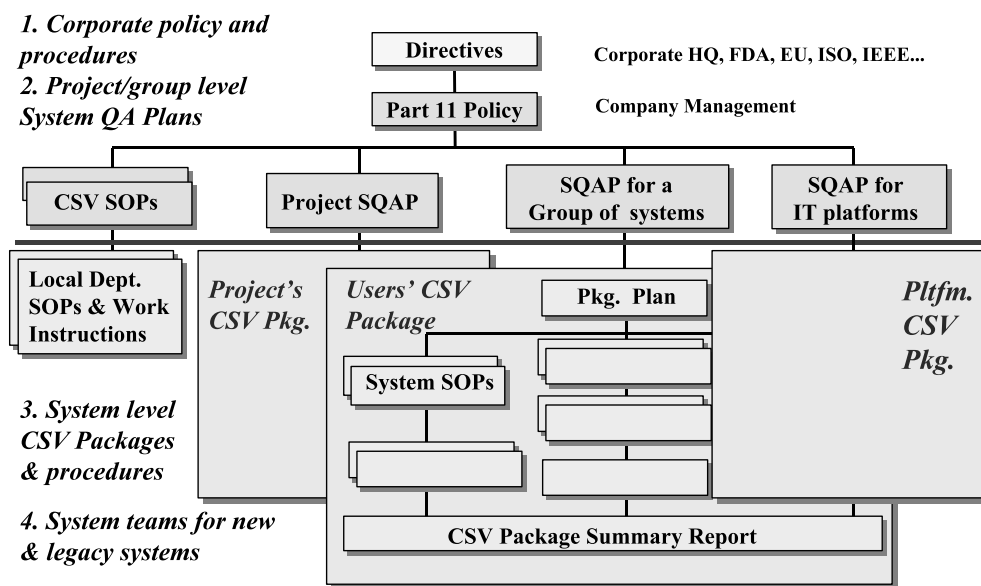


図4 CSVの体制