コンピュータ化システムバリデーションの最新動向

デジタルソリューションビジネスユニット
デジタルITプロダクト部
ヘルスケアITグループ
参事
松井　一

1. はじめに

コンピュータ化システムバリデーション（Computerized System Validation、以下CSV）の歴史を紐解いてみると、1983年にFDAが発出したA Guide to Inspection of Computerized Drug Processing Systemsに遡ることができる。このガイドは、青い色のカバーで出版されたため、通称、Blue Bookと呼ばれている。Blue Bookでは、コンピュータシステムバリデーションは、コンピュータシステムがデータの処理や保存、あるいは作業プロセスを管理するために意図された通りに動作することを示すドキュメント化されたエビデンスを準備することと規定している。なお、当時は、「コンピュータ化システム」ではなく、「コンピュータシステム」であった。

次にCSVに関するエポックメイキングな事象として、同じくFDAが1997年に発出した電子記録と電子署名の利用に関する規制21CFR Part11（以下、Part11）がある。これはFDAが、製薬企業や医療機器メーカーが、電子記録や電子記録に対する電子署名を従来使用していた紙の記録と署名と同等と見做すための基準を示した。Part11は電子記録や電子署名を使用する前提条件として、CSVを求めている。

上記については、主に欧米の製薬業界が中心の動きで、CSVに関して日本では、規制も含めては常に周回遅れで追従していた。したがって、欧米でビジネス展開をしている日本の製薬企業を除いて、CSVをしっかり実践していた企業は少なかった。日本で、CSVが製薬企業においてコンピュータ化システムを使用する際、必須事項として意識されるようになったのは、「医薬品等の承認又は許可等に係わる申請等における電磁的記録及び電子署名の利用について」（薬食発第0401022号）として、2005年4月1日付けで発出されてからである。本通知の別紙「医薬品等の承認又は許可等に係る申請等に関する電磁的記録・電子署名利用のための指針」において、Part11同様にCSVが電子記録・電子署名を利用する際の前提条件として示された。更に、2010年10月21日付けで発出され、2012年4月1日より施行された「医薬品・医薬部外品製造販売業者等におけるコンピュータ化システム適正管理ガイドライン」によって、CSVの実施が日本でも徹底された。

ただし、これらの規制は、CSVの実施を求めているが、何をどこまで行うのか、あるいはどのように行うのかといった方法論のようなものは、FDAが、2002年に

General Principles of Software Validation; Final Guidance for Industry and FDA Staff

として考え方を示していた以外、提示されていなかった。そのため

- DIA Computerized Systems in Clinical Research: Current Data Quality and Data Integrity Concepts（通称、Red Apple II Book）
- DIA Computerized Systems in Clinical Research: Current Quality and Data Integrity Concepts（通称、Peach Book）
- ISPE GAMP（Good Automated Manufacturing Practice、自動化製造実践規範）ガイダンス

といったガイドが出版された。このなかで日本では、GAMP4の時代から参照されるガイドとして使われており、GAMP5が、2008年にA Risk-Based Approach to Compliant GxP Computerized Systemsとして、改訂されてから、GMP領域以外のGxPシステムに対しても利用されるようになった。なお、医薬品・医薬部外品製造販売業者等におけるコンピュータ化システム適正管理ガイドラインは、日本の医薬品製造販売業者の多くを占める中小企業を対象としているため、何を行えばよいかについて、例示している。しかし、GAMP4をベースにしているため、Risk Basedアプローチは取り入れておらず、運用面では工夫が必要である。

さて、Risk Basedの考え方は、FDAが、2002年8月にPharmaceutical cGMPs for the 21st Century-A Risk-Based Approachを公表したときに遡ることができる。このイニシア

ティブでは、重要な分野に行政と産業のリソースを集中するためにRisk-Basedアプローチを採用することを推奨しており、GAMP5でも採用されたRisk Based Approachが、CSVに対する方法論で一般化している。さらに、ICH E6(R2)では、CSVに関して、次のような補遺が追加された。

・「システムバリデーション」とは、電子データ処理システムが要求される仕様について、システムの設計から廃棄まで又は新システムへの移行まで常に満たすことを検証し、文書化(記録化)する過程をいう。システムバリデーションの取組は、システムの用途や被験者保護及び治験結果の信頼性への影響を与える可能性を考慮したリスク評価に基づくこと。

・電子データ処理システムが、完全性、正確性、信頼性及び意図された性能についての治験依頼者の要件を満たしていることを保証し、文書化すること(すなわちバリデーションされること)。なお、その際には、システムの用途並びにシステムが被験者保護及び治験結果の信頼性に影響を与える可能性を考慮したリスク評価に基づいて行うこと。

また、ICH E6(R2)では、Quality Risk Management(以下、QRM)の考え方を導入している。ICH E6(R2)のQRMは、重要なプロセス及びデータの特定、リスクの特定、リスクの評価、リスクのコントロール、リスクコミュニケーション、リスクレビューのステップから構成されるが、このアプローチは、ICH Q9 Quality Risk Management(品質リスクマネジメントに関するガイドライン)を参考に概念として取り入れている。

最近、規制当局が、CSVに関して、新たな考え方としてData Integrityを打ち出した。これは、GMPの世界ではホットな話題になっている。従来のSystem Lifecycleをベースに考えるCSVから、Data Lifecycleを通したData Integrityを保証する考えが導入されている。

本稿では、CSVの最新の動向として、Quality Risk ManagementをベースにしたRisk Based ApproachとData Integrityについて解説する。

2. Quality Risk Managementとは

ICH Q9では、Quality、Risk、Managementを次のように定義している。

・Quality
製品、システム、又は工程に係わる本質的性質の組み合わせが要求事項を満たす程度

・Risk
危害の発生の確率とそれが発生したときの重大性の組み合わせ

・Management
製品ライフサイクルを通じて、医薬品の品質に係るリスクについてのアセスメント、コントロール、コミュニケーション、レビューからなる系統だったプロセス

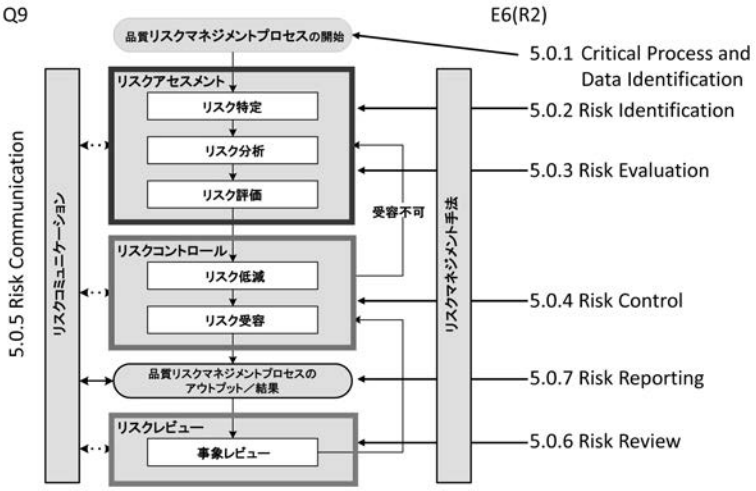
これらの定義のうち、製品に相当するところをコンピュータ化システムのQRMとなり得ることがわかるであろう。

リスクに関しては、ICH Q9よりビジネスプロセスに近いICH E6(R2)では、Quality Managementを以下のように行うように規定している。

5.0.1 Critical Process and Data Identification
5.0.2 Risk Identification
5.0.3 Risk Evaluation
5.0.4 Risk Control
5.0.5 Risk Communication
5.0.6 Risk Review
5.0.7 Risk Reporting

ICH Q9が規定しているQRMのプロセスとマッピングすると図1のようになる。

図1 Quality Risk Managementのプロセス



医薬品に対するQRMとプロセスに対するQRMの全体像がわかりやすくなると思う。では、QRMのなかで重要な位置を占めるリスクアセスメントについて、次に述べる。

3. リスクアセスメントの行い方

ICH Q9品質リスクマネジメントブリーフィング・パックには、リスクアセスメントの行い方が記載されている。リスクアセスメントは、リスクの特定→リスク分析→リスク評価のステップで行うが、このとき3つの基本的な質問を用いるとわかりやすくなると紹介されている。リスクの特定は、何がうまくいかないかもしれないのか。リスク分析は、うまくいかない可能性(確率)はどれくらいか。リスク評価は、うまくいかなかった場合、どんな結果(重大性)となるのか。これらの質問をコンピュータ化システムについて検討することが、コンピュータ化システムのリスクアセスメントになる。次に各プロセスについて、もう少し詳しく内容を述べる。

3.1 リスクの特定

リスクの特定をするには、ハザード(危害の要素)を特定するためにシステムの仕様や特徴といった体系的な情報を利用する必要がある。具体的には、システムの複雑性(複雑なほどリスクは高)、システムが採用しているテクノロジーの新規性(新規テクノロジーなほどリスクは高)、サプライヤ監査の結果、当該システムを利用した過去の経験、あるいはシステムを利用したユーザーの意見等を参考に特定する。また、当該システムで収集、あるいは管理するデータの重要度や再生成可能なデータなのか等、データの持つ意味も検討項目に追加しなければならない。

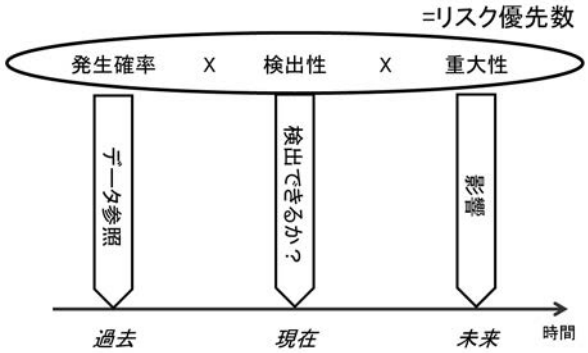
3.2 リスク分析

リスク分析は、特定されたハザードに関連するリスクの推定を行うことである。危害が生じる確率とその重大性を定性的または定量的に結びつけるプロセスである。定量的に分析するには、データが必要で有り、過去の経験、例えば、GLP試験や臨床試験で利用した結果等が、システムのメトリクスが必要になる。リスク評価のため、検出性も検討する。

3.3 リスク評価

リスク評価は、特定、分析されたリスクを予め定めたリスク基準に従って比較することである。ICH Q9品質リスクマネジメントブリーフィング・パックでは、FMEA(Failure Mode and Effect Analysis、欠陥モード影響解析)を参考にリスク優先数を図2のように算出することを勧めている。

図2　リスク優先数の算出



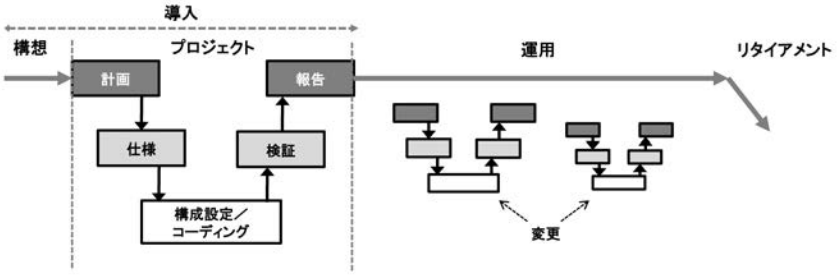
FEMAでは、リスク優先数としてリスクを数値化することにより、客観的な評価尺度として利用している。コンピュータ化システムの場合も大まかな尺度としては、利用できる。ただし、予め、スコアを三段階程度に分類して、それに応じたCSVを検討しないと、実務では尺度として利用できない恐れがあるので留意する必要がある。

4. Risk Based CSVとは

これまでQRMとリスクアセスメントについて述べてきたが、コンピュータ化システムのCSVにどのように活用すればよいかについて述べる。まず、GAMP5をベースにしたシステムライフサイクルを図3に示す。

現在、GxPシステムの多くは、特にGCPシステムやGVPシステムは、SaaSシステムに移行しつつある。GLPシステムやGMPシステムでもクラウドベースのシステムがサービスを開始しており、将来的には、GxPシステムの多くがOn-PremiseからSaaSへの移行が見込まれる。SaaSシステムの場合、システム導入フェーズは、サービスサプライヤが行うことになる。これまでユーザーが、On-Premiseのシステム開発で慣れ親し

図3　システムライフサイクル



んだIQ、OQ、PQといったCSV活動は、どうすればよいのであろうか?

GAMP5では、サプライヤが実施したテスト文書等のシステム文書を活用することを勧めている。要するにユーザー側で重複した作業は、なるべく行わないというスタンスである。これを実践するには、サプライヤアセスメントが重要になる。予めサプライヤアセスメントを行うことにより、ユーザー側で実施するCSV活動の内容を決めることができる。その際に重要になるのが、先に述べたリスクアセスメントの結果である。仮に、リスク優先度を大、中、小の3種類に分類したとしよう。リスク優先数が小の場合、サプライヤに対する訪問調査は行わず調査票のみで対応する。中の場合も調査票で調査を行うが、回答内容によっては訪問調査を行い、サプライヤのQMS(Quality Management System)を確認する。大の場合は、原則、訪問調査を前提にアセスメントを行う。また、利用しようとしているシステムが広く利用されているシステムの場合は、調査票だけの調査に省略しても良い。

5. Data Integrity

Data IntegrityがGMPの世界でホットな話題になったのは、イギリスの規制当局であるMHRAが2015年にMHRA GMP Data Integrity Definitions and Guidance for Industry March 2015というガイドラインを発出してからである。それ以降、これまでに発出された主なData Integrityに関するガイドラインやガイダンスを次に示す。

- MHRA GMP Data Integrity Definitions and Guidance for Industry(2015年1月)
- PDA Elements of a Code of Conduct for Data Integrity in the Pharmaceutical Industry(2016年2月)
- WHO Guidance on Good Data and Record Management Practices(2016年5月)
- FDA Guidance for Industry Data Integrity and Compliance with CGMP(ドラフト、2016年4月)
- MHRA GxP Data Integrity Definitions and Guidance for Industry(ドラフト、2016年7月)
- NMPA医薬品データ管理規範(意見募集稿、2016年9月、2018年1月)
- ISPE GAMP GUIDE RECORDS & DATA INTEGRITY(2017年4月)
- MHRA 'GXP' Data Integrity Guidance and Definitions(2018年3月)
- PIC/S GOOD PRACTICES FOR DATA MANAGEMENT AND INTEGRITY IN REGULATED GMP/GDP ENVIRONMENTS(査察官向けドラフト3判、2018年11月)
- FDA Data Integrity and Compliance With Drug CGMP Questions and Answers Guidance for Industry(2018年12月)

このようにMHRAに続いて、PDA、WHO、FDA、中国のNMPA(旧CFDA)と続き、MHRAはスコープをGxPに拡大したガイドラインのMHRA 'GXP' Data Integrity Guidance and Definitionsを2018年3月に発出している。日本ではData Integrityに関する指針は発出されていないが、改正が予定されているGMP基準では、Data Integrityを確保するため、手順書を作成する際に、「文書及び記録の完全性を確保」するよう作成することを明記される予定である。このようにData Integrityに関するガイダンスが多く発出された背景には、GMP査察時にData Integrityに関する指摘が、インドや中国の工場で増加したことがある。FDAのWarning LetterにみられたData Integrityに関する指摘事項を次に示す。

- The laboratory employees shared a common log-in and password to access the system
  研究室の従業員は、共有のシステム・ログインとパスワードを利用していた。
- Unacceptable practices in the management of electronic data were also noted.
  電子データの管理に許容できない行為も指摘された。
- The management of electronic data permitted unauthorized changes, as digital computer folders and files could be easily altered or deleted.
  デジタルコンピュータのフォルダやファイルが簡単に変更や削除できるような、未承認の変更が、電子データの管理として許可されていた。
- Your inability to detect and prevent poor data integrity practices raises serious concerns about the lack of quality system effectiveness.
  不十分なData Integrityの実施を検出し防止することができないことが、品質システムの有効性欠如に関する深刻な懸念を高めている。

これらの指摘は、システムライフサイクルを前提とした従前のCSVのアプローチだけでは、意図的なデータの変更(改竄)や組織としてData Integrityに対する不十分な体制の場合、Data Integrityの保証ができないからである。そのためデータライフサイクルを通したデータの完全性を保証する、すなわちData Integrityの考え方を導入した。

5.1 データライフサイクル

Data Integrityを理解する上で欠かせないデータライフサイクルを、GAMP GUIDE RECORD & DATA INTEGRITYでは次のように定めている。

- Creation(生成)
  データは意図した用途のために収集され、保持される

表1　ALCOA+CCEA

A	Attributable	帰属性（データを生成した人に帰属可能）
L	Legible	判読性（恒久的に判読可能）
C	Contemporaneous	同時性（同時に記録）
O	Original	原本（オリジナル記録か真のコピー）
A	Accurate	正確性（記録が正確）
C	Complete	完全性（記録が完結している）
C	Consistent	一貫性（記録に矛盾がない）
E	Enduring	恒久性（記録の保存期間を通した永続性）
A	Available when needed	要事利用可能性（記録を必要なときに取り出せる）

・Processing（処理）
　データは必要なフォーマットで情報を取得、提出するため処理される
・Use（利用）
　データは情報に基づく意思決定に使用される
・Retention and Retrieval（保持と取り出し）
　データは安全に保持され、定義された保存期間を通して直ちに利用できる
・Destruction（破棄）
　データは必要な期間経過後、破棄される

Data Integrityは、MHRA ‘GXP’ Data Integrity Guidance and Definitionsでは次のように定義されている。

The extent to which all data are complete, consistent and accurate throughout the data lifecycle.

すべてのデータがデータライフサイクル全体にわたって完全で、一貫性があり、正確である程度。

したがって、Data Integrityを保証するには、データライフサイクルを通じて、データの正確性、網羅性、内容と意味が保存されることである。

MHRAのData Integrityの定義は、何も新しいものではなく、以前から言われているALOCA+CCEAの考え方をデータライフサイクルに当てはめれば、達成できることに気づくであろう。ここでALOCA+CCEAを復習してみよう（表1参照）。

次のことが、データライフサイクルを通して、保証されることがALOCA+CCEAを達成していることになる。データが生成時に記録され（Contemporaneous）、オリジナルな正確で完全な記録で（Original、Accurate、Complete）、判読性が保たれ（Legible）、データの生成された時点から現在に至るまでデータに処理を行った人がわかり（Attributable）、データの保存期間を通して、一貫性と永続性が保証される（Consistent、Enduring）。CCEAのAであるAvailable when neededは、当局側からの要求的側面が強いので、Data Integrityに対しては考慮する必要はあまりない。

5. 2 Data Governance

MHRAガイダンスでは、Data Governanceにより、データライフサイクルを通して、完全性（Complete）、一貫性及び、恒久性を保証する必要があると述べている。では、あまり聞き慣れないData Governanceとは、どのようなことをMHRAは意図しているのだろうか？ MHRAガイダンスでは、Data Governanceは、次のように定義している（一部抜粋）。

・組織文化、業績評価指標、目標、および上級経営層の行動が、Data Governanceの各対策の成功に与える影響を過小評価すべきではない。Data Governanceポリシー（またはそれに相当するもの）は、組織の最高レベルで承認されるべきである。
・Data Governance措置が、データライフサイクルを通して、データのComplete（完全性）、Consistent（一貫性）、Enduring（恒久的）およびavailable（可用性）を確実にする必要がある。
・Data Governanceはデータライフサイクルを通したデータの所有権と責任を取り扱うと同時に、情報の意図したおよび意図しない変更の管理を含むデータ完全性の原則に準拠するため、プロセス/システムの設計、運用、および監視を検討しなければならない。
・Data Governanceシステムには、データ完全性の原則の重要性のスタッフトレーニング、およびエラー、手抜かり、ならびに好ましくない結果について、見える化と積極的に報告できる作業環境の構築が含まれる必要がある。

この中で留意すべきこととして、「積極的に報告できる作業環境」、すなわちオープンに報告する文化を奨励する作業環境の醸成がある。オープンに報告する環境構築は、日本ではあまり行われてこなかったように思われる。オープンな報告と懲戒は別な話であるので、報告ができる作業環境構築は非常に重要である。

5. 3 電子記録及び電子的な必須文書におけるData Integrity

最後に、電子記録及び電子的形式で管理されているGxP文書や申請関連文書（以下、電子文書）におけるData Integrityを保証するにはどのようにすればよいかについて述べる。GxP活動の電子記録を収集及び管理、および電子文書を管理するコンピュータ化システムの機能については、CSV活動により保証される。Data Integrityの背景で述べたように、システム機能を保証しただけでは、Data Integrityの保

証はできない。Data Integrityを保証するには、MHRAガイダンスを参考に検討すると次のようなことを行う必要がある。

- コンピュータ化システムを利用して生データを電子的に取得、処理、報告、保管、またはアーカイブする場合、システム設計は、常に前のデータおよび原データを保持しながら、データの変更または削除をすべて示すための監査証跡の保持ができるようにする必要がある。
- 監査証跡（リスクアセスメントによって必要とされた場合）を有効にする必要がある。ユーザーは、監査証跡を修正または無効にするべきではない。システム管理者が監査証跡を修正するか、または監査証跡をオフにする場合、その行為の記録を保持する必要がある。
- 日常的なデータレビューには、文書化された監査証跡レビューを含む必要があり、これはリスク評価によって決定される。
- データのレビューと承認のプロセスを記載した手順が必要である。また、データレビューには、関連する監査証跡記録を含む関連するメタデータのリスクに基づくレビューを含める必要がある。データのレビューは文書化され、記録には問題が発見されたかどうかの明確な陳述、レビューが行われた日、レビュー担当者の署名を含める必要がある。
- 全ての適切なスタッフ（上級経営層を含む）に対するデータ完全性の原則に関する十分なトレーニングの実施

これらのなかで、これまであまり行われていなかった作業として、監査証跡の定期的なレビューがある。監査証跡をレビューすることにより、先に述べたデータが生成されて、現在に至るまで正確で一貫性を含む全体的な完全性を確認することができる。したがって、データの重要度やリスクアセスメントの結果、リスクが高いデータの場合、監査証跡のレビュー頻度を多くする必要がある。

6. まとめ

Risk Based CSVとは、予めリスクアセスメントによりハザードを調査することによりリスクを評価し、その結果に応じてCSVの詳細さのレベルを変更することにより、要求する品質水準にあったCSV結果とCSV活動を効率的に実施する手法である。さらに、CSVでシステムの信頼性を確保した先にあるのが、個々のデータの信頼性を確保するのがData Integrityである。Data Integrityは、これまでのシステムライフサイクルに通したシステム毎の信頼性保証から、データライフサイクルを通した個々のデータの信頼性保証を意味している。しかし、Data Integrityの概念は、新しいものではなく以前から言われているALOCA+CCEAを保証することにより、実現できるものである。そのためには、Data Governanceの導入と監査証跡の定期的なレビューが重要になることを指摘して、本稿を終えることとする。