製造プロセスをサポートする自動化システムを使用するためのリスクアセスメント

Part 1 – 機能的リスク

By ISPE GAMP Forum
翻訳　ISPE GAMP JAPAN 第一分科会

FDA は最近、医薬品の製造と製品品質に対する米国の規制を強化する重要かつ新規のイニシアティブを発表した [1,2]。このイニシアティブは FDA の cGMP プログラムに基づき、ワクチン等の人用の生物製剤を含む、動物および人体薬に適用される。その目的は既に確立しているリスクマネージメントを使用した”quality systems”のアプローチをさらに強化することにある。他の規制当局は科学に基づくリスクマネージメントを主要な運用原理として既に取り入れている [3,4]。このことを念頭において、本稿では製造プロセスをサポートするために使用される種々のタイプの自動化システムがもたらす相対的なリスクについての共通の理解を策定することを試みる。背景となる前提は、自動化システムのバリデーションの厳密さは、リスクに見合ったものであるべきである、ということである。したがって、当該システムを製造プロセスのサポートに使用するに当たっては、規制に適合しないことがあればその意味合いを考慮する必要がある。関連するリスクについての本分析は次の二つのパートに分けられる。

- 最初のパートはソフトウェアソリューションのクラスの違いに伴う機能リスクに焦点を置いている。
- 二つ目のパートは本年の後半に出版予定であるが、電子記録に伴う相対リスクを論ずる。

本稿は GAMP4[5] で論じられているリスク分析のガイダンスを説明するものである。GAMP のリスク分析手法を一般的な 3 種類のクラスのソフトウェアに適用することによって、手法の紹介と、その使用法の説明の両方の役目を果たすものである。

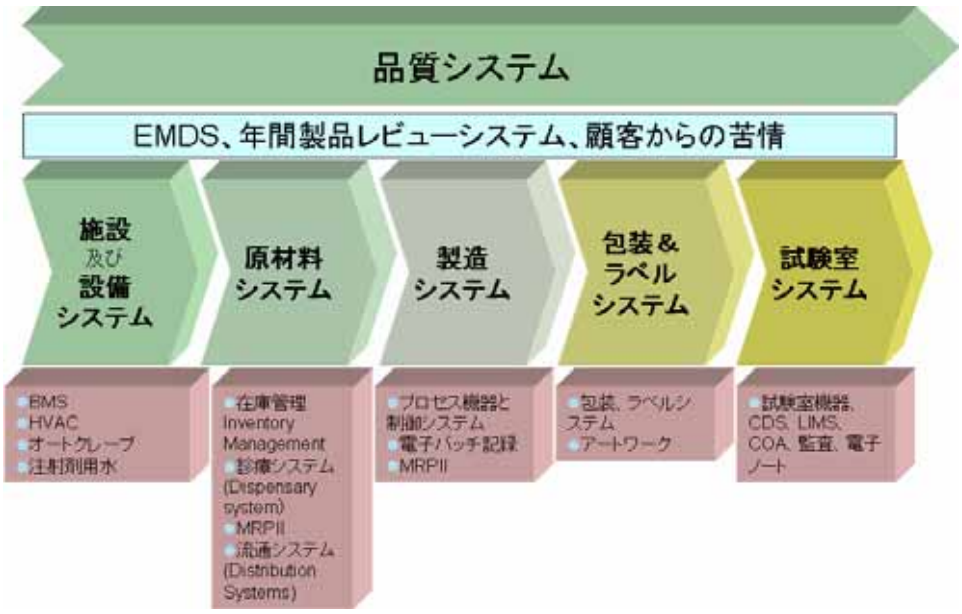

図 1 自動化システムの使用

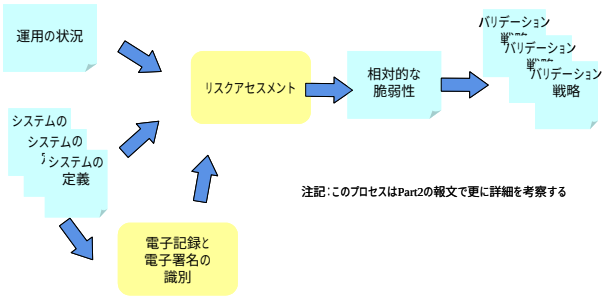

図 2 リスクアセスメントのプロセス

自動化システムの使用

自動化システムは、医薬品製造をサポートするために広く用いられている。製造プロセスのワークフロー分析（FDA の査察における Systems アプローチ [6] に基づく）によりコンピュータシステムの使用される 6 つの主要な業務上の観点が特定される。

- 品質システム — 職務と手順による管理を取り扱う
- 施設と設備のシステム – 医薬品の製造に使用される物理的環境を取り扱う
- 原材料システム — 医薬品の成分、在庫管理、および医薬品の保管を取り扱う
- 製造のシステム — 製造管理を取り扱う
- 包装およびラベルのシステム — 包装とラベルを取り扱う
- 試験室のシステム — 分析試験を取り扱う

図1に、種々の自動化システムがどこで使用され得るかを図示する。自動化システムによっては MRPII のように製造プロセスの複数の局面をサポートするものと、HPLC システムのようにプロセスの特定の局面に特化して使用されるものがあることを認識することが重要である。

リスクアセスメントプロセス

1. ここで使用するリスクアセスメントプロセスの最初のステップは、自動化システムの重要度を特定するために製造プロセスの 6 つの局面を使用することである。
2. 二つ目のステップは不完全な運用に対する自動化システムの脆弱性を分析することである。
3. 三番目のステップはバリデーション戦略の決定である。システムの脆弱性に応じて必要なバリデーション業務の厳密さのレベルが決められる。

同様に、バリデーションでは電子記録･署名の要件を取り上げなければならない(must)。この3段階のリスクアセスメントプロセスは図2に図示されている。

機能の重要度

製造プロセスのどの運用局面が最も重要であるかを決めるに当たっては、それらの局面が医薬品の安全性、品質、有効性に及ぼしうる影響を理解する必要がある。Canadian Health Products と Food Branch Inspectorate は既に、不適合の医薬品を生み、公共の健康に差し迫ったまたは潜在的なリスクをもたらし得る数多くのリスク項目を特定している。これらのハイリスク項目はここで自動化システムに適用され、ここまでに特定した6つの運用エリアに合うよう調整されている。

品質システム

- 文書管理
- SOP 管理
- 安全なアクセス管理（例：ユーザプロフィールとパスワード管理）
- 変更管理記録
- 顧客の苦情
- 有害事象報告
- レビュー／オーディット／是正措置管理
- 教育訓練記録

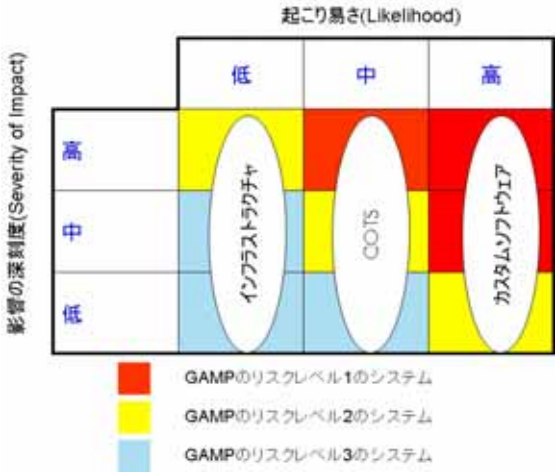

図 3 GAMP のリスク分類

施設と設備のシステム

- HVAC 制御とアラーム処置
- 重要設備と機器（校正と保守）
- 変更管理記録
- バリデーション記録

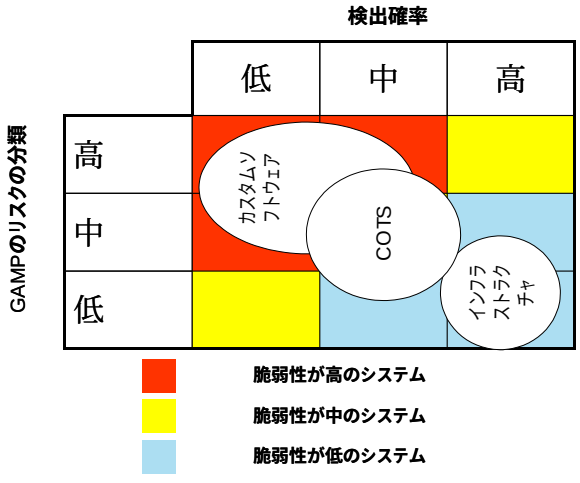

図 4 相対的なシステムの脆弱性

原材料のシステム

- 原材料取り扱いのトレーサビリティ
- 原料の検査／試験／状態管理
- 保管条件
- 容器の使用とクリーニング管理
- 流通記録と回収管理

製造のシステム

- レシピ／処方管理
- バッチの製造指図と記録
- 工程内試験
- 収率計算
- 精製水
- 無菌充填

包装およびラベルのシステム

- ラベル情報

試験室のシステム

- QC 生データ
- 安定性試験
- 無菌試験
- QC 分析結果
- 品質判定
- 規格外結果の調査

製造プロセスのこれらの重要な運用局面をサポートする自動化システムのバリデーションの厳密さは、そのカスタム(特注)ソフトウェア、市販既製（COTS）のソフトウェアおよびそれをサポートするコンピュータネットワークのインフラストラクチャを考慮すべきである。

システムの脆弱性

ここでは、次の3種の典型的なソフトウェアシステムの相対的な脆弱性を分析するために GAMP のリスクアセスメント手法を使用する。

- *カスタムソフトウェア*とは、医薬品製造にかかわる一連の要件のアプリケーションのために特に開発されたソフトウェアソリューションを指す（GAMP4 の用語集を参照のこと）。この語は GAMP のソフトウェアカテゴリー5 — 「カスタム(特注)ソフトウェア」あるいはGAMP のソフトウェアカテゴリー4 — 「構成可能なソフトウェアパッケージ」のアプリケーション特有の構成コードを示している。

- *市販の既製ソフトウェア（COTS）*とは、製薬業または他の産業において多くのアプリケーションにわたって使用されている既存の（つまり、あるアプリケーションのために開発されたものではない）標準的なソフトウェア製品を指す。この語は、GAMP のソフトウェアカテゴリー3 — 「標準ソフトウェアパッケージ」または GAMP のソフトウェアカテゴリー1 — 「オペレーティングシステム」またはGAMP のソフトウェアカテゴリー4 — 「構成可能なソフトウェアパッケージ」のシステムのうち標準的な製品構成要素を示している。

- *インフラストラクチャ*とは、物理的なネットワーク部品、スイッチ、ハブ、ルータ、サーバ、ファイアウォール、ネットワーク OS,およびその組み合わせからなる典型的なインフラストラクチャを指す。

最初に、システムの機能とシステムデータの両面から、システムのもたらす脅威がどの程度重大なものであるかということに基づき、これらの3つのクラスの自動化システムを分析する — 図3。3種のシステムのどれをとっても、システムによりもたらされ得る影響の厳しさはそのアプリケーションに依存する（すなわち、システムがサポートしている製造プロセスの重要運用局面の数、システムが影響を及ぼすビジネスの範囲、どの程度にシステムが不具合を起こすか）。したがって、それぞれの種類のシステムが低、中、高いずれの程度の厳しさの脅威をもたらしうるのである。しかしながら不具合の起こり易さはシステムの種類に応じて変わる。

カスタムソフトウェア

これらのシステムは、特定のアプリケーションのために開発されたものである。したがって、そのアプリケーションがソフトウェアの最初の使用例となり、そのため実運用により機能動作が証明されたものではない。したがってこのクラスのシステムは高程度の不具合の起こり易さを示すことが多い。GAMP のリスク等級のグリッドの起こり易さ「高」を適用するとカスタムソフトウェアは主としてレベル1またはレベル2のリスクに分類される。

COTS

これらのシステムは通常は実際の運用例が相当数ある。したがって、ソフトウェアは過去のバリデーション活動や実使用により部分的には機能動作が証明されているであろう。しかしながら、不具合の起こり易さがないというわけではない。というのは、これらは多くの場合極めて複雑なシステムで高度の構成が可能であるためコードの部分によっては証明されていないことがあるからである。このクラスのシステムは、したがって、中程度の不具合の*起こり易さ*を示すことが多い。*起こり易さ*「中」を適用すると、*COTS* はレベル1、レベル 2、レベル 3 のリスクに分類される。

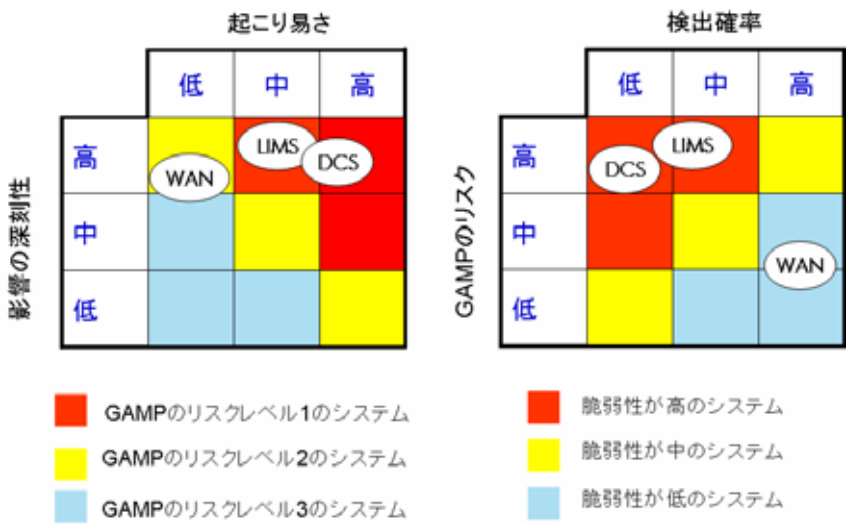

図 5 脆弱性のシステムでの実例

インフラストラクチャ

通常インフラストラクチャは業界標準のネットワーク構成要素を使用して作り上げられている。これらの要素は、多くの業界において極めて堅牢で、また自己修復能力を持っていることが証明されている(例：TCP/IP プロトコル)。構成要素の不具合はしばしばインフラストラクチャの機能やパフォーマンスに重大な影響を与えることなく認容され得る。したがって、このクラスのシステムは比較的低い*起こり易さ*を示す傾向にある。*起こり易さ*「低」を適用すると、*インフラストラクチャ*はレベル 2、または大部分レベル3のリスクに分類される。

次に、システムのリスク分類（レベル 1、2、3）とシステムに発生する不具合を検知する確率とを対比して相対的な脆弱性を推定する（図 4）。システムに発生する不具合を*検知する確率*は、以下にその例を示す多くの要素に依っている。

- ソフトウェアの機能そのものに組み込まれたエラー検知機能
- 特定の機能を二重化する（冗長性）、またはシステムのアウトプットをモニタして逸脱を報告するための、別個かつ独立したシステムの使用
- システムの正確な挙動をモニタするための手動の検査またはテストの利用

明らかに後ろの2項はソフトウェアのクラスではなくアプリケーションに依存しているであろう。しかしながら、これらのクラスの違いにより実際にエラー検知の能力も異なってくる傾向があるのである：

カスタムソフトウェア

エラー検知はかなり複雑で開発に費用のかかることが多い。したがって、*カスタムソフトウェア*のソリューションが良質のエラー検出機能を持っていることはあまりありそうにない。したがって、これらのシステムは低または中程度の*検出確率*を持つ傾向にあり、結果として大部分が高い脆弱性に分類される。

COTS

COTS は運用される底辺が広いので、開発予算も*カスタムソフトウェア*のソリューションより大きく、COTS 製品が何らかの形のエラー検知機構を持っている可能性は*カスタムソフトウェア*よりも高い。これらのシステムは主として中程度の*検出確率*を持つ傾向にあり、結果として脆弱性は高、中、低いずれの可能性もある。

インフラストラクチャ

大部分のネットワーク構成要素はいまや何らかの形のエラー検出機構を持っている（例：イーサネットレベルでのコリジョン検知、TCP/IP におけるデータグラムチェックサム）。インフラストラクチャが正しく機能しているかどうかは人の目にはほとんど検知することはできないものの、インフラストラクチャ自体が検知することなくエラーがインフラストラクチャによって広がっていくことは極めて起こりにくいことである。重大な不具合が生じた場合、通常はそのインフラストラクチャを使用しているアプリケーションが不具合をレポートするか、例えばクラッシュのように完全に停止してしまう。したがって不具合が検知されないままということはあり得ない。この結果システム脆弱性は低となる。

バリデーションの厳密さ

概して、*インフラストラクチャ*から*カスタムソフトウェア*までのソフトウェアシステムの3つのクラスは、医薬品の安全性、品質、および有効性に起因する公共の健康にこの順番で大きくなる脆弱性を示す。脆弱性の増加にしたがってシステムバリデーションに求められる厳密性も大きくなる。表 A にこれらのリスクのクラスを、そのシステムをバリデートに必要な規制適合のための業務の推奨される適切なレベルとともに示す。

	脆弱性/バリデーションの厳密性	ユーザーのバリデーション活動の重要性		
		計画/報告書	設計フェーズ	適格性評価フェーズ
カスタムソフトウェアアプリケーション	高	• バリデーション計画と報告書 • 開発の SOP • 重要な欠損を解決するサプライヤオーディット • プロジェクトオーディット • 定期レビュー • 変更管理	• URS(ビジネスと規制上の要求) • FS(システムの全機能性) • モジュールの仕様にまでレベルダウンして設計 • 設計レビューのプロセス • ソースコードレビュー(一般的なコーディングの内容と特にリスクの高いコードの詳細なウォークスルーによる確認) • トレーサビリティマトリックス(包括的)	• この文書で確認された製造プロセスの運用状況に対する詳細なリスクアセスメント • 包括的なポジティブ機能テスト(すべきことをする) • リスクに焦点を当てたネガティブ機能テスト(リスクアセスメントで脆弱だと確認された箇所で起きてはならないことが起きない
COTS アプリケーション	中	• バリデーション計画と報告書 • 開発の SOP • 重要な欠損を補うサプライヤオーディット • 定期レビュー • 変更管理	• URS (ビジネスと規制での要求) • FS(アプリケーションに特有な要件に対しては完全な機能性を、標準的な機能には標準的な製品の書類に対してポイントを) • 設計文書にはアプリケーションの構成状況のみ • 設計レビューのプロセス • トレーサビリティマトリックス(標準の製品文書に対するユーザー文書)	• この文書で確認された製造プロセスの運用状況に対する高水準のリスクアセスメント • 特定のアプリケーションに対する規定したユーザーの操作のポジティブ機能テスト(すべきことをする) • リスクに焦点を当てたネガティブ機能テスト(リスクアセスメントで脆弱だと確認された箇所で起きてはならないことが起きない
インフラストラクチャ	低	• SLA • 品質とコンプライアンス計画 • 機能の SOP • 定期的なレビュー • 変更管理	• ネットワーク接続ダイアグラム • ネットワーク定義(サポートされたアプリケーションのリスト、ネットワーク性能及びセキュリティの要件のみ)	• この文書で確認された製造プロセスの運用状況に対する高リスクのアセスメント • リスクに焦点を当てた機能テスト(たとえば、セキュリティコントロール、データの完全性、バックアップ及びリカバリ)

脆弱性の増大、バリデーションの厳密さの必要性の増大

表 A 脆弱性と必要なバリデーションの厳密性のサマリ

実例説明

説明のために、上述したソフトウェアシステムの各クラスの観点を含む3つの典型的なシステムに対するリスクの深刻さ（GAMP のリスク分析）を考慮する。

分散型制御システム（DCS）

ほとんど間違いなく証明済みの一つまたは複数の DCS 製品

に基づいているものの、医薬品原体のバッチ製造を制御するDCS 導入のエンジニアリングはアプリケーションに特有の構成とコーディングが中心となる。したがって、この DCS 内の「制御アプリケーション」はカスタムアプリケーションのカテゴリーに入る。

試験室情報システム（LIMS）

現在では、ほとんどの GMP 試験室の情報管理に必要な機能の全てを提供している、充分確立された LIMS 製品が市販されている。通常の導入に必要な機能の大部分が標準機能で満たされるので、LIMS は GAMP カテゴリー4のソリューション、すなわち COTS とアプリケーション特有の構成の組み合わせ、と考えられる。

全社ワイドエリアネットワーク（WAN）

複数の事業所を持つほとんど全ての組織は、何らかの形の WAN を持っている。WAN は明らかにインフラストラクチャシステムであり、ドメインサーバ、ルータ、ファイアウォールといった標準的なハードウェアおよびソフトウェアの構成要素を含むことがある。

	高リスクの問題		
	DCS の実例	LIMS の実例	WAN の実例
品質システム			• セキュリティアクセスコントロール
施設/装置システム			
原(材)料システム		• 原材料のテストと状態の管理	
生産システム	• 処方設計と管理 • バッチ製造	• 工程内試験	
包装及びラベルシステム			
試験室システム		• QC 生データ • QC 分析結果	

表 B 実例のシステムの高リスク機能の例

ステップ1 — リスクの深刻度

DCS、LIMS、WAN 導入事例の正確な役割とそれに関連するリスクは導入毎に異なるであろう。本説明の目的のために、表 B に各々のシステムが提供する可能性があり、高リスクであると特定されうる機能を提案する。

表 B では、我々の取り上げた 3 つの例いずれもが高リスクの機能を含んでおり、それゆえに高リスクシステムと考えられるべきであることを示している。しかしながら、この表を使うことにより、個々のシステムの相対的なリスクの深刻度を明確にすることができる。LIMS は、3 つの FDA 査察対象システムにわたる 5 つの高リスク点に影響があり、明らかに公共の健康に最も深刻なリスクを潜在的に持っている。

ステップ2 と3 — 全体的脆弱性

上述の、カスタムソフトウェア、COTS、およびインフラストラクチャに対する起こり易さと検知確率に関する議論がこれら3つの説明例にも適用できるとして、GAMP のリスク分析手法のステップ 2 と 3 を適用すると図 5 に示すような相対的脆弱性が導かれる。

GAMP の機能リスク分析手法ステップ 1、2、3 を併せると、DCS と LIMS の両方とも高脆弱性システムであり、それゆえに表 A に提起した最も厳密なバリデーションの対象となることが示唆される。一方、WAN は比較的低い脆弱性のシステムであり、その脆弱性に対応した厳密さのバリデーション対象となるだけでよい。

結論

本稿は、製造工程をサポートする自動化システムの使用に、機能リスクアセスメントの手法を適用したものである。機能リスクアセスメントが、コンピュータシステムにより引き起こされるリスクのアセスメントと順位付けを行うメカニズムを提供することが示された。バリデーションの厳密さをシステムの全体としての脆弱性と結びつけることにより、リスクに適切なバリデーション戦略を開発するプロセスが証明された。規制当局による既成の成果に基づいて、自動化システムの使用にかかわる製造工程における高リスクの運用観点が特定された。カスタムアプリケーション、COTS アプリケーション、およびインフラストラクチャのもたらす相対的なリスクも分析され、インフラストラクチャが間違った操作による医薬品の品質、有効性、安全性への影響という点で比較的脆弱性の低いことが示された。

個々の自動化システムに本稿で示した一般的なリスクアセスメントを適用する際には気をつけなければならない。個々のシステムが異なっていることを認識すること。それにもかかわらず、この一般的なアプローチは充分に確立されたもので、医薬品製造業者と規制当局が同様に、特定の自動化システムのバリデーションに適切な相対的厳密さを評価する助けとなるべきである。

電子記録の相対リスクを考える本稿の Part 2 は本年後半に出版される。

References

1. U.S. FDA (2002), Pharmaceutical cGMPs for the 21st Century: A Risk Based Approach, FDA News, 21 August, www.fda.gov.
2. European Union Guide to Directive 91/356/EEC (1991), European Commission Directive Laying Down the Principles of Good Manufacturing Practice for Medicinal Products for Human Use.
3. Trill, A. J., Computerised Systems and GMP - Current Issues, Presentation UK Medicines Control Agency Seminar 'Top 10 GMP Inspection Issues' 24 September 2002.
4. Canadian Health Products and Food Branch Inspectorate (2000), Good Manufacturing Practices - Risk Classification for GMP Observations.
5. ISPE (2001), GAMP Guide for Validation of Automated Systems (known as GAMP 4), International Society for Pharmaceutical Engineering (www.ispe.org).
6. FDA (2002), CPG 7356.002 Drug Manufacturing Inspections: Systems Based Approach.

謝辞

ISPE GAMP フォーラムは、本稿の作成に関し GAMP ヨーロッパと GAMP アメリカの運営委員会に感謝する。特に草稿作成に対し Guy Wingate と Sam Brooks に感謝する。