

タイトル：製造実行システムにおけるクラウドコンピューティングの意義

著者: Paul Irving, Gregory M. Ruklic, and Jonathan Hurlle

(Pharmaceutical Engineering, 2021, Vol. 41, No. 3, 29–35)

翻訳: 京都大学大学院医学研究科薬剤疫学分野 大学院生 梶田崇一郎 (Soichiro MASUDA)

クラウドコンピューティングとは、遠隔地にある組織が提供・維持するコンピュータシステム上のデータや情報の保存、処理機能、適用、その他のサービスなどの構成可能なコンピューティングリソースに、ネットワークを介してアクセスし、利用することをいう。ライフサイエンス企業がクラウドサービスを利用するメリットやコストを検討する際には、まず、クラウドベースモデルを理解し、製造実行システム (Manufacturing Execution Systems; MES) ドメインの設計や移行に適用する際の意義を理解するためにリソースを投入する必要がある。

MES ドメインとは、製造業務に関連する、または製造業務をサポートする何らかの機能を持つすべてのシステムと定義されている¹⁾。これには、企業資源計画 (Enterprise Resource Planning; ERP)、自動化、文書管理 (標準操作手順管理)、MES ソフトウェア (レシピおよびバッチ管理など)、臨床検査情報システム (Laboratory Information System; LIMS) どのシステムが含まれるが、これらに限定されるものではない。

クラウドベースモデルへ移行する契機は、様々なライフサイエンス製造企業がコアビジネスに集中しつつ、必要に応じてコンピュータリソースや関連業務を専門のプロバイダーに外部委託することにある。クラウドコンピューティングの規格情報については、米国国立標準技術研究所の“NISTによるクラウドコンピューティングの定義”²⁾、および“NISTによるクラウドコンピューティング標準ロードマップ”³⁾、クラウドコンピューティングの定義や詳細に関する推奨資料として参照されている。NISTが特定したクラウドコンピューティングの特徴²⁾、サービスモデル、導入モデルを視覚的に表したものが図1である。

テクノロジータイプの紹介

クラウドベースのサービスは、通常、外部のクラウドサービスプロバイダー (cloud service provider; CSP) によってエンドユーザー (顧客の組織) に提供される。クラウド構造は仮想化方式を提供し、エンドユーザーは、全体の CSP の所在地に関わらず、コンピュータシステムに関連するアクションやインターフェースが自分の視界の中で正常に動作していることを体験できる。また、エンドユーザー組織内の専用グループは、たとえ物理的には施設内に配置されていなくても、地域や全体の施設にクラウドベースのサービスを提供すること

ができる。

この記事では、NIST が定義した²⁾、3 つのクラウドコンピューティングサービス提供モデルに焦点を当て、それぞれがライフサイエンス企業にとって様々な利点とリスクを持つことを紹介する。

- **Software as a service; SaaS**。エンドユーザーは、CSP がホストおよび管理するアプリケーションにアクセスする。アプリケーションによって作成または利用されるデータは、CSP に属する下部構造上に存在する。アプリケーションは多くの場合、CSP によって提供されるが、エンドユーザーがアプリケーションを開発し、その後 CSP がホストとして管理する場合もある。エンドユーザーは、基盤となるクラウド下部構造を管理しない。エンドユーザーは遠隔アプリケーションの特定の構成パラメータを定義することができる。
- **Platform as a Service; PaaS**。CSP は、エンドユーザーがアクセス可能なコンピューティングプラットフォーム（ハードウェア、オペレーティングシステムなど）をホストし、エンドユーザーは、自分で購入したアプリケーションや CSP が提供するツールを使って作成したアプリケーションをインストールして管理する。プラットフォームには、ネットワークやその他の接続性や、サーバー、ストレージなどの機器・システムが含まれる。エンドユーザーは、基盤となるクラウド下部構造を管理しない。
- **Infrastructure as a Service; IaaS**。エンドユーザー組織は、通常、アプリケーションやオペレーションシステムの環境を提供し、管理する。CSP は、ネットワーク、サーバー、プロセッサ、ユーティリティやシステムサポートソフトウェアなど、コンピュータシステムの基盤となるすべての構造に責任を負う。エンドユーザーは、会社の要件に応じて、ファイヤウォールなどのセキュリティソフトウェアを管理することもでき、CSP にその管理を委ねることもできる。

これら 3 つのクラウドモデルを総称して XaaS と呼ぶ。図 2 は、XaaS のサービス提供形態が製造環境でどのように運用されるかを示したものである。

ビジネスドライバー

ISPE Pharma 4.0TMイニシアティブの一環として、企業はサプライチェーンのグローバル化、システムやデータの互換性の向上、コストの最適化などの機会を得る。XaaS 技術を利用することで、企業は最高品質の製品やサービスを低コストで、効率的に提供することができる。XaaS は以下のような利点を提供する。

- 高度な技術を設計、インストール、維持するために必要な社内の部署を削減することで、社内の人員を実際の製品やサービスの提供に集中させることができる。
- グローバル展開は、単一または削減した数のソースで管理することができる。
- 社内の技術環境を毎日管理する代わりに、品質管理部門が監査やその他の定期的な監

視によって CSP の品質管理システムを監視することができる。

望ましい投資収益率を達成するために、多様な製品群を持つ企業は、複数の XaaS 提供モデルを利用して、拠点やプロセスごとにコストを最小化し、利益を最大化することができる。

IaaS、PaaS、または SaaS のいずれを導入するかを選択は、戦略的な評価に基づいて行う必要がある。これは、企業の既存のテクノロジープロセスとパフォーマンス、および将来の望ましい状態を文書化したものである。このプロセスについては後述する。

MES とクラウド

前述したように、生産環境全体、つまり MES ドメインは、様々な技術によって提供される複数の機能で構成されている。MES 技術の例としては、材料マスターと在庫データのための材料管理、プロセスのための自動化/設備、レシピ管理と生産記録、品質材料のテストと状態制御などがある。エンドユーザーの視点から見ると、適切に吟味された単一ソースの XaaS に MES 機能を統合することは、従来のオンサイトで管理されていたシステムやインフラに比べて、導入や長期的なメンテナンスのコストを抑えることができる。企業は通常、戦略的評価の一環としてコスト/ベネフィット分析を行い、ソフトウェアやハードウェアの提供や管理に外部ソースを利用することの価値を判断する。

MES ドメインの設計においては、GAMP® *Good Practice Guide: 製造実行システム戦略的プログラムマネジメントアプローチ*に記されている¹⁾、ANSI/ISA-95 (IEC62264) ビジネスシステム及び製造システムの統合標準に盛り込まれたパデュー大企業参照アーキテクチャで定義されている層 (図 3 参照) は、特定のハードウェアやシステムに縛られるものではない^{4,5)}。その代わりに、アーキテクチャは、適切なコンピュータ化されたシステムによって提供されるべき機能を記述している。

ISA-95 のモデルでは、レベル 0、1、2 は、製造のために定義されたオペレーションの実行を制御する。レベル 3 のシステム機能は、レベル 4 でビジネスによって決定された生産計画を実行する。ライフサイエンス業界では、良くも悪くも、ERP や LIMS などのシステム全体をモデルのいずれかの層に割り当てているため、業界の専門家の中には、ISA-95 モデルはクラウドコンピューティングや Pharma 4.0™には適用できないと結論付ける人もいる。しかし、コンピュータシステムは複雑で幅広い機能を持っていることから、ISA-95 モデルでは、システムに存在する機能を適切な ISA-95 モデル層に割り当てるアプローチを採用している。

例えば、ERP システムの中には、ハードウェアの秤やその他の自動化装置に連動した計量・払出機能が含まれているものがある。ERP システムのビジネス機能は ISA モデルの最上位層にあり、レシピや調剤業務はモデルの下位層にある。クラウドパラダイムを検討する際には、製造環境をモデル化して設計する際の思考プロセスは、基本的に ISA-95 の階層的なアプローチを採用している。

ライフサイエンス業界では、ビッグデータや解析をレベル 4 の計画システムに適用したり、レシピ/バッチ制御、リソース管理、生産実績などの MES 機能がレベル 4 からの計画情報を受け取るレベル 3 に相互に適用したりすることが議論されている。これらのコンセプトは、Pharma 4.0™に関連しており、将来のビッグデータや解析が複数のレベルのシステムと相互作用することになる。このような業界の議論の詳細については本稿では触れないが、Pharma 4.0™の進化に合わせて MES 機能のクラウドへの移行を計画する際には、専門家のリソースを利用することを推奨する。高度な情報を提供する推奨リソースの一つは、NIST が発行した“スマートマニュファクチャリングシステムモデルによる ISA95 レベル 3 制御の定式化”がある⁶⁾。

この記事では、MES ドメインにおける典型的なシステムの機能と技術をクラウドに移行することに焦点を当てているが、分析と計画の方法は将来のパラダイムにも適用できる。本稿で取り上げる戦略的評価には、スマートマニュファクチャリング、モノのインターネット (Internet of Things; IoT)、Pharma 4.0™などの検討が含まれており、エンドユーザー組織がこれらのパラダイムへの移行の必要性と方法論を判断するのに役立つ。

MES の機能ドメインは、ビジネス機能だけの場合よりも、クラウド導入のための分析が複雑になることがある。継続的かつライブなプロセスでの GxP 生産では、データ、レシピ、品質単位の処分状況、その他のタイムリーな情報を、グローバルなオペレーションのどこからでも、いつでも電子生産記録から得ることが必要になることが多い。特定の施設や製造プロセスにどのクラウドサービスモデルを適用するのが最適かを判断するために、事業者はすべての製造オペレーションからの生産要件を分析し、現在の方法論と今後予定されている方法論の両方を評価する。この組織では、既存の MES ドメインをクラウドベースのモデルに移行する際にも同様の評価を行っているが、エンドユーザーは既存の機能を維持し、既存の MES ドメインと提案されているクラウドベースのバージョンとの間で機能の同等性を実証するための検証活動を行わなければならないという制約が追加される。エンドユーザーにとってリアルタイムオートメーションやセンサーモニタリング (IoT を含む) に関連する機能をクラウドに移行するかどうか決断する事は重要である。

初期の戦略上の障害

一般的に、クラウドコンピューティングを利用しようとする組織は、次のような課題に直面する。

- 組織には、一貫した戦略を策定するのに十分なクラウドの経験がないため、クラウドコンピューティングによって達成すべき目標が明確ではなく、検証もできない。
- 導入プロセスの重要な要素が、計画の不備やリソースの不足によって見落とされている。例えば、組織は、CSP 自身が下請け業者からサービス (データの管理やバックアップなど) を受けることが多いことを十分に理解していない可能性があるため、クラウドサービスの下請けが組織の業務にどのような影響を与えるかを検討していない場合が

ある。下請け業者を利用することで、個人情報や専有データが不正または意図しない方法で流出するリスク（法的な影響を受ける可能性）が高まり、監査人が CSP の下請け業者を監査できないためにセキュリティ認証が危険に晒される可能性がある。また、CSP による事業継続計画やコンテンジェンシー、クラウドサービスと顧客の下請け業者との統合計画全体が、特定の製造業の重要性に対して不適切な場合がある。

アクセスに関する考慮事項

MES ドメインのシステムでは、多くの場合、24 時間 365 日の連続稼働が求められる。ローカルビジネスオペレーション、特にグローバルに展開しているオペレーションでは、CSP のロケーションとは異なるタイムゾーンのサービスに継続的にアクセスする必要がある。CSP のアプリケーションとローカルサイトのシステムが、リアルタイムオートメーションシステムによる生産を実現するために厳密な調整を必要とする場合、アクセスに関する考慮事項はさらに複雑になる。主な考慮事項は以下の通りである。

- 生産記録、活動ログ、監査証跡のタイムスタンプは、事業運営、内部調査、規制当局による監査のために、ローカルサイトでの作成/実行時間に合わせて、人間が読める形式で表示されなければならない。
- リモートでのデータダウンロード/アップロードの要件を明確にし、実施する必要がある。
- アプリケーションインターフェースは、スムーズかつ効率的に動作し、オペレーターの指示をタイムリーに提示し、オペレーターの応答を記録するなど、製造システムへの即時アクセスを可能にする必要がある。
- システムを超えた活動の品質単位の評価をタイムリーに調整することが必要である。
- ゲーティングオペレーションは、電気機械システムのシーケンスやレシピの実行に関連したアクティビティについて、生産や品質部門の担当者がタイムリーに承認できるように、十分に設計されていなければならない。
- 連続プロセスのマスターデータは、リアルタイムに下流のシステムで参照できるように、常に検証可能な手段で入手できなければならない。
- マスターデータの更新は、エンドユーザーと CSP の間で慎重に調整し、業務の中断やレシピやその他のプロセスの意図しない変更を防ぐ必要がある。
- 施設、生産ライン、プロセス間のインベントリの使用、作成、処分の更新が調整されなければならない。
- 製造記録のアラート/アラーム管理と、製造および品質部門のレビュー/承認へのタイムリーなアクセスを実現する必要がある。
- 規制要件やビジネス分析に適合した形式で履歴データにタイムリーにアクセスできなければならない。

クラウドベースのシステムへのアクセスに関する IT リスクは以下の通りである。

- インターネット/国際的なネットワークの障害
- ローカル・ネットワークの障害（CSP またはエンドユーザーにとって）
- 不適切な一時停止や再同期の方法やアルゴリズム
- 不十分なデータ伝送の検証
- 共通のサーバー/システム上のクライアント間でのデータの混在
- 不適切な災害復旧要素、または企業とプロバイダーのネットワーク設備と人のコミュニケーションの間の調整不足
- リアルタイムでのエラーや障害に対するプロバイダーの応答時間が許容範囲を超えていること
- 事業者と連携したプロセス制御の乱れによる、遠隔地（プロバイダー）でのデータ修正の手順・方法の欠如

XAAS モデル特有の考慮事項

XaaS の各サービス提供モデルは、エンドユーザーにさまざまなリスクとメリットをもたらす^{3,7)}。

- SaaS。マスター、プロダクションマスター、オリジナルデータは通常、クラウドに保存されるため、エンドユーザーはホストされたオペレーション機能に強く依存する。SaaS はエンドユーザーに大幅なコスト削減をもたらすが、ローカルオートメーションシステムとのインターフェースには多大な時間を要することがある。
- PaaS。標準化されたアプリケーションでは、グローバルな拠点、言語、文化の違いによるエンドユーザーのニーズに対応できない場合がある。しかし、PaaS は検証の手間やソフトウェアのメンテナンスコストを削減することができる。
- IaaS。IaaS は、エンドユーザーや下請け業者によるインフラのセットアップやメンテナンスがすでに一般的に行われているため、XaaS の中では一般的に最もリスクが低く、社内のビジネスリソースの節約も比較的容易である。したがって、IaaS は標準的なやり方に近く、クラウドモデルを準備している多くの企業にとっては、より小さな進化である。

サイバーセキュリティと脆弱性

グローバル企業では、一般的にサイバーセキュリティ対策が施されているが、時折、大規模なデータ漏洩が発生している。業務をクラウドに移行することでセキュリティリスクが高まる可能性があるが、標準的なネットワークセキュリティシステムによってほとんどのリスクは軽減される。手続き的または技術的に追加の保護を提供するためには、以下の点を考慮する必要がある。

- IoT は、デジタルで接続されたすべての機器を相互に接続しようとするものであるた

め、利便性は向上するが、新たなセキュリティ上のリスクが生じる可能性がある。

- 業務遂行のためにオンサイトまたはオフサイトで使用されるスマートフォンやタブレットなどのモバイルデバイスは、セキュリティを確保する必要がある。
- データの暗号化は、データの破損を防ぐのに非常に効果的だが、システムのネットワークとデータの需要を増加させる。
- エンドユーザー組織の従業員のミスや怠慢は、CSP やその下請け業者に内在するリスクを高める可能性がある。つまり組織は、吟味された雇用、監督、トレーニングの基準と方法によって、このようなリスクを軽減することが重要である。

この分野の最新のガイダンスとして、著者らは、安全なクラウドコンピューティング環境を確保するためのベストプラクティスを策定し、認知度を高めることを目的とした非営利団体であるクラウドセキュリティアライアンスのガイダンスを推奨している⁷⁾。

規制に関する考慮事項

エンドユーザーは、クラウドベースのすべての要素を含む MES の実装を検証することが求められる（規制要件の詳細については参考文献 1 を参照）。クラウド要素の一部として認識され標準化されたコンポーネントを使用すると、CSP がバリデーションの一部の側面を担うため、エンドユーザーの検証の負担が軽減される可能性があるが、コンプライアンスの判断に決定されるように、エンドユーザーの負担が完全になくなるわけではない。

ライフサイエンス企業は、クラウドベースのデータの暗号化/復号化、安全なデータの入力と保存、および関連する問題に対処するガイダンスが適切であることを確認する必要がある。データ入力には、最終的にはエンドユーザーが直接管理できない外部でサポートされたツール、製品、インフラが関与することになり、そのプロセスは適切に記録、検証、妥当性確認をされなければならない。

対象とする環境、対象とする市場、提案する解決策に基づいて、関連する規制を特定することは、エンドユーザー組織の責任である。そして、提案された XaaS アプリケーションがこれらの規制にどの程度準拠しているか、またどこに逸脱があるかを判断しなければならない。

戦略的評価の概要

前述したように、クラウドベースモデルの導入や移行を効率的に計画、設計するためには、戦略的評価が不可欠である。戦略的評価については、*GAMP® Good Practice Guide: 製造実行システム戦略的プログラムマネジメントアプローチ*で詳しく定義されている¹⁾。図 4 にプロセスの概要を示し、このセクションでは主な考慮事項を説明する。

MES ドメインには部門横断的な機能が含まれているため、戦略的評価をリードするには、高レベルの経営陣がサポートするプロジェクトマネジメントオフィスを強く推奨する。戦

戦略的評価では、エンドユーザー組織の現状、つまりクラウドサービスの対象となるサイトや生産活動、それに伴うリソース、要件、制約、そしてクラウド移行の具体的な目標、メリット、リスク、導入の障壁、そして企業のニーズを満たすプロジェクト計画の基礎を確立する。このような評価は以下のように行われるべきである。

- ビジネス関連と製造関連のプロセス/機能を分離し、要件を明確に定義する。
- 全体設計に関する情報を提供する。この設計は、潜在的なアプリケーションとは無関係に、機能とその相互作用によって定義されるべきであり、事業者はこのような設計をハイレベルな要件として CSP に提示することができなければならない。
- 正確で適切なシステム設計と構成のために、エンドユーザーがプロセスを理解し、文書化していることを確認する。

エンドユーザー企業の現状と希望を把握することの重要性は、いくら強調しても過ぎることはない。CSP には数多くの選択肢があるが、戦略的アセスメントを実施することで、各 CSP を賢く評価し、最適なベンダーを選択することができる。確立された CSP は、グローバルセキュリティポリシーをはじめとするコアサービスに精通しており、エンドユーザー組織が独自に実施するよりも強力なコントロールを提供することができる。

戦略的評価では、以下の質問に対する幅広い議論と決定を記録することで、初期目標と長期目標を定義する。

- 組織は XaaS を 1 つのサイト、地域、またはグローバルに導入する必要があるか？
- 実装は垂直方向（サイト全体の MES ドメイン全体をカバー）か、部分的（1 つまたは複数のサイトで特定の MES 機能、プロセス、または製品を扱う）か？
- 組織のタイムラインとリソースの制約は何か？
- XaaS は生産スケジュールにどのような影響を与えるか？
- MES に XaaS を採用、または変更した場合のコストとメリットは何か？
- スマートマニュファクチャリング（Pharma 4.0™、IoT など）を実現するための要件と範囲は何か？
- XaaS を導入した場合、既存システムのアップグレードや代替は何が必要か？

戦略的評価は、これらの質問に答えるだけでなく、クラウド導入を成功させるためのプロジェクト計画を策定するための準備にもなる。

Pharma 4.0™モデルやテクノロジーの導入は、戦略的評価に複雑さをもたらす。例えば、IoT には、情報を統合された監視・制御システムに供給する膨大な機器のネットワークや、人工知能に基づく未来の意思決定アプリケーションが含まれる。このようなパラダイムや技術の設計では、継続的な運用とフェイルセーフを保証する必要がある。なぜなら、CSP の優れた実績にもかかわらず、どの技術もすべての状況で 100%の運用アップタイムを保証することはできないからである。

< P 34 左上枠内部分 >

適切に審査されたクラウドサービスプロバイダーは、技術的な専門知識、システムの信頼性、ビジネスサポートを高いレベルで一貫して提供する。

プロバイダーサービス選択

適切に審査された CSP は、技術的な専門知識、システムの信頼性、ビジネスサポートを高いレベルで一貫して提供する。以下のような CSP の属性や条件を考慮し、戦略的な評価で文書化する必要がある。

- ベンダーの関連する履歴。MES の経験や製薬業界の既存顧客を持つ CSP が望ましい。
- 規制に関する専門知識。CSP は、エンドユーザーに関連する分野の知識と経験を持っているか？
- スタッフのレベル、専門知識、トレーニング。
- CSP の財務的安定性を示すエビデンス。
- CSP の運用、ネットワーク、およびデータの物理的およびデジタル的なセキュリティ。
- CSP 施設の所在地。地域、国、地域の安定性、地域のネットワーク・インフラ、地域に適切な労働力があるかなどの要因を考慮する。
- エンドユーザーに提供される機器/ソフトウェア。GAMP® 5 ガイダンス、ASTM 国際標準、情報技術インフラライブラリー、ISA 標準などに記載されている、ソフトウェアおよびハードウェアの開発、実装、保守、検証のベストプラクティスへの準拠。
- CSP の内部監査能力が確立され、検証されていることの証明。

エンドユーザーの責任と能力

戦略的評価と CSP の選択プロセスにおいては、エンドユーザーが以下の点について最終的な責任を負うことを理解することが重要である。

- サービス品質保証、サポートモデル、品質保証、エスクローに関する事項
- ソフトウェアやハードウェアの開発および検証監査の実施
- 定期的なインフラおよび監査のレビューの実施
- 顧客とサービスプロバイダーのメンテナンスの範囲と厳密さを決定する（サービスの種類によって要件は異なる）。
- 要件収集とコミュニケーションのための明確なポリシーと手順
- 厳格なデータ整合性コントロールのためのテスト

CSP を利用することで、エンドユーザーの IT 導入や保守のリスクは軽減されるが、CSP や XaaS には評価すべき多くのリスクがある。例えば、エンドユーザーは、自社では制御できない広範囲の地域的なインターネット/ネットワーク障害の可能性を評価し、グローバルなシステムを破壊する可能性のあるサービス妨害攻撃などのシナリオに対する緊急時計画を評価する必要がある。

戦略的評価の際、エンドユーザーはレビューと文書化を行う必要がある。

- CSP ベンダーとエンドユーザー組織の間で、場合によってはタイムゾーンを越えて調整しなければならないリアルタイム制御システムのための一時停止と再同期のアルゴリズム
- エンドユーザー組織から CDS へ、および CDS から組織への外部データの更新および送信の検証に関するポリシーおよび手順
- エンドユーザー企業のネットワークと CSP のネットワークの間のループ、および人的コミュニケーションに適用される代表的な災害復旧要素
- リアルタイム運用中のエラーや障害に対する CSP の応答時間
- CSP とエンドユーザー組織の間でのデータ修正の調整方法を含む、プロセス・コントロールの乱れに起因するリモートのデータ修正に関する方針および手順 (CSP)

エンドユーザー組織は、クラウドベースのシステムの信頼性を確保し、MES のリスクを最小限に抑えるために、手続きや可能な限り電子的な管理を行う必要がある。MES の検証状態を維持するためには、エンドユーザーが XaaS に情報を転送・更新する際に、正確かつ徹底的に文書化する必要がある。検証の対象となるのは、以下のタイプのデータだが、これに限定されるものではない。

- 重要な品質属性
- 重要なプロセスパラメータ
- 重要な側面情報
- 作業指示書/レシピ
- メタデータ
- 監査証跡

CSP は、エンドユーザー組織の不適切な管理に起因するシステムの誤設定には責任を負わない。エンドユーザーと CSP の要員を明確に識別し、エンドユーザーの監視構造の中で調整される検証プロセスに専念させる必要がある。

結語

この記事では、ライフサイエンス企業における MES の戦略および導入フェーズにクラウドベースのモデルを適用する際のコンセプトと考慮事項を紹介している。読者には、参考文

献に引用されている出版物を参照し、さらに詳しい情報を得ることを推奨する。

本文以上

図の説明

図 1 クラウドコンピューティングの視覚化モデル

図 2 機能インターフェースの概要

図 3 ANSI/ISA-95 の機能階層。(GAMP® *Good Practice Guide: 製造実行システム戦略的プログラムマネジメントアプローチ*より転載)¹⁾

図 4 CSP サービスを検討する組織のための戦略的評価