データインテグリティ詳細レビュー

siemens.com/pharma

目次

表の索引

図表の目次

1 概要

医薬品の品質はデータに大きく依存しています。データは、品質に関する意思決定に必要な情報を提供し、製品の品質を記録するために使用されます。データインテグリティ要件への不適合は、製薬会社の市場参入に大きな影響を与え、最終的には患者の安全性に悪影響を及ぼす可能性があります。データインテグリティを患者の安全性や製品の品質と同列に扱う規制は、これらの懸念を強調するものです。

近年、査察報告書ではデータインテグリティに関する問題が頻繁に指摘されています。その原因は、文書の破棄や改ざんなどの意図的な行為によるものもあれば、共有ログインの使用などプロセスやシステムの使用上の問題によるものもあります。このような報告書や、電子記録におけるデータインテグリティの不適合を指摘する最近の警告書を受けて、公的機関や製薬会社の専門家グループがこのテーマについ熱心に議論しています。

お客様固有のインストールされたシステムでは、最初の作成から削除まで、データのライフサイクル全体をマッピングすることが重要です。アーカイブ戦略は、特にエラーが発生しやすい分野ですが、エラーを優れたシステム設計によって排除することができるため、特に注目するに値します。

本書では、医薬品原体製造におけるデータインテグリティのためのシーメンスのソリューションを紹介しています。

2 ソースの索引

[1] FDA 21 CFR Part 11

[2] FDA Draft Guidance for Industry: Data Integrity and Compliance with CGMP（FDA 業界向けドラフトガイダンス：データインテグリティとCGMP準拠）

[3] Eudralex GMP guidelines Chapter 4, Q&A Data Integrity and Appendix 11（Eudralex GMPガイドライン 第4章 データインテグリティに関するQ&A および付属書11）

[4] MHRA GMP Data Integrity Definitions and Guidance for Industry（MHRA GMPデータインテグリティの定義と業界向けガイダンス）

[5] MHRA GxP Data Integrity Definitions and Guidance for Industry（MHRA GxPデータインテグリティの定義と業界向けガイダンス）

[6] WHO Annex 5 Guidance on Good Data and Record Management Practices（WHO附属書5 データおよび記録の適正な管理の実施に関するガイダンス）

[7] PIC/S Draft 2 Guidance: Good Practices for Data Management and Integrity in Regulated GMP/GDP Environments（PIC/S ドラフト2ガイダンス：GMP/GDP規制下におけるデータマネジメントとインテグリティに関する実践規範）

[8] ISPE-GAMP Guideline Records and Data integrity（ISPE-GAMP 記録とデータのインテグリティガイドライン）

[9] Draft VDI/VDE 3516 Blatt 5 Validation in the GxP area - Types of raw data（ドラフト VDI/VDE 3516 Blatt 5 GxP領域におけるバリデーション - 生データの種類）

3 データインテグリティ：説明と定義

3.1 データのライフサイクル

データインテグリティを確保するためには、初めにデータのライフサイクルを理解することが必須です。まず、GxP（対象分野の実施基準）に関連すると認識されているデータと、そうでないデータを区別しなければなりません。GxP関連性は、リスクベースの手法を用いて個々のプロセスごとに決定する必要があります。

一般的に、データのライフサイクルは次のように説明できます。

- データが作成される。
- データが評価、活用される。
- データがすべてのメタデータとともに初めて保存される。
- データがデータ保存領域からアーカイブに転送されるか、即座に削除される。
- アーカイブされたデータが、保存期間後に復元または削除される。

データのライフサイクル全体をリスクベースのアプローチで評価し、その有効性を確認する必要があります。プロセスでは、データの保存とアーカイブだけでなく、データの削除も文書化する必要があります。さらに、データのライフサイクル全体において、意図しないデータの紛失や変更を防止しなければなりません。また、データの保存に使用されるメディアの技術的特徴や、適用可能なインターフェイスを介した計画的なデータ転送を考慮し、適切な管理戦略を提供する必要があります。

3.2 ALCOAとALCOA+

医薬品査察協定・医薬品査察共同スキーム（PIC/S）のガイダンス[7]およびWHOのガイダンス（WHO 2016）[6]に記載されている用語「ALCOA」および「ALCOA+」（表3-1）は、電子的な記録と紙ベースの記録の両方について、データインテグリティの基準に言及するためにしばしば使用されます。

ALCOAまたはALCOA+の原理	説明
Attributable（帰属性）	データの出典を特定することが可能であること。
Legible（判読性）	すべての記録は、すべての変更と削除を含め、人間が読み取れるものであること。
Contemporaneous（同時性）	アクション、イベント、決定の証拠は、それらが行われたときに記録されること。
Original（原本性）	原本記録は、情報を最初に記録したものといえること。
Accurate（正確性）	妥協のない正確なデータであること。
Complete（完璧性）（ALCOA+）	イベントを再現するために重要となるテストや繰り返しを含むすべての情報は重要であり、保持しておく必要がある。
Consistent（一貫性）（ALCOA+）	適正な文書化は、正しいタイムスタンプの使用を含め、例外なくすべてのプロセスに適用されるべきである。
Enduring（耐久性）（ALCOA+）	記録を確実に利用できるようにするには、その記録が必要となる可能性のある全期間にわたって記録が存在することを確認する必要がある。
Available（可用性）（ALCOA+）	記録は、必要とされる保存期間中、いつでもレビュー、監査、または検査に利用できなければならない。

表 3-1 「ALCOA」と「ALCOA+」の説明

3.3 コンピュータ化システムのライフサイクル

電子記録に使用されるコンピュータシステムは、データインテグリティに不可欠な要素です。データインテグリティを確保するためには、コンピュータシステムは、例えば、国際製薬技術協会の自動化製造実践規範（GAMP）5ガイドライン（ISPE 2017）に記載されているような、管理されたライフサイクルを持つ必要があります。コンピュータ化システムのライフサイクルでは、データ移行時のデータの完全性にも配慮する必要があります。

3.4 データインテグリティマネジメント

データインテグリティとそれに関連するプロセスは、製薬会社のすべての従業員の責任です。経営陣は、トレーニングと基本的な文書を提供し、特定の責任を割り当て、従業員のコンプライアンスとそれを支えるプロセスの両方をレビューすることによって、データインテグリティの重要性を強調し、強化しなければなりません（図3-1）。

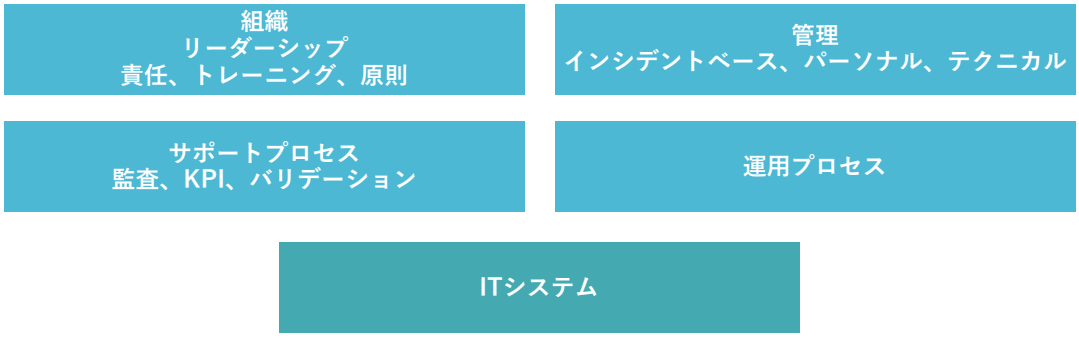

図 3-1 データインテグリティマネジメント

3.5 電子署名

電子署名は、以下の点を保証する適切な管理メカニズムが整っていれば、手書きの署名に置き換えることができます。

- 署名が文書にされており
- 文書に署名した個人を特定することが可能である（FDA業界向けガイダンス「Data Integrity and Compliance with cGMP」2016年4月を参照）。

電子署名は、一連の規則と一連のパラメータから算出される暗号手法を用いて、署名者の身元を確認し、署名データの完全性を確保するものです（21 CFR Part 11 [2]）。現在のトレンドは、電子署名の認証と追跡のために、バイオメトリクス手法に基づいた高度な文書署名プロセスを使用することです。バイオメトリクス手法は、各個人に固有で記録可能な特定の身体的属性または反復可能な動作に基づいて、人物の身元を検証するものです（21 CFR Part 11）[2]）。PIC/Sは、ドラフトガイダンス「Good Practices for Data Management and Integrity in Regulated GMP/GDP Environments」（PIC/S、2016年8月）において、そのような手法の導入を推奨し、電子署名が準拠すべき一連の基準を定めています。

- 電子署名は検証されなければならない。
- 電子署名は、管理されたプロセスで割り当てられなければならない。
- 電子署名は、いかなる時も一人の人物に帰属させることができなければならない。
- 署名されたデータに後から変更を加えた場合、データを確認して再署名するまで、署名は無効としなければならない。

これらの要件と、米国食品医薬品局（FDA）の規則21 CFR Part 11 - Electronic Records; Electronic Signatures（電子記録・電子署名、1997年）の要件を組み合わせることで、電子署名を作成・管理するための技術システムが満たすべき一連の具体的な基準が生まれます。

- 文書や署名の偽造を抑止するためには、電子署名を使用して実行されたアクションに対する人物の説明責任を定義する書面による指示がなければならない（21 CFR 11.10 (j); Annex 11, 14.a）。
- 署名された電子文書には以下が含まれなければならない。
  - ブロック体での署名者の名前
  - 署名をした日付と時間
  - 署名の目的（例：リリース、レビュー、責任）（21 CFR 11.50 (a); Annex 11, 14.c）
- この情報は、電子記録の表示版と印刷版の両方に記載されるべきである（21 CFR 11.50 (b)）。
- 電子署名は、通常の手段で電子記録を偽造する目的で署名を削除、コピー、または転送できないように、一致する電子記録と恒久的にリンク付けがされなければならない（21 CFR 11.70; Annex 11, 14.b）。
- すべての電子署名は、一人の人物に固有のものでなければならず、他の人物が再使用したり、他の人物に再割り当てたりすることはできない（21 CFR 11.100 (a), 11.200 (a)）。
- 電子バッチ記録システムを認証およびバッチのリリースに使用する場合は、権限を与えられた者のみがバッチのリリースを認証できるようにシステムを設定しなければならない（Annex 11, 15）。
- ある人物に電子署名の構成要素を割り当てる前に、その人物の身元を確認するプロセスを設けなければならない（21 CFR 11.100 (b)）。
- 連続したセッションではなく、繰り返し署名を行う場合は、すべての署名行為に電子署名のすべての構成要素が含まれていなければならない（21 CFR 11.200 (a)）。以降の署名は、電子署名のパーソナライズされた構成要素の少なくとも1つを使用して行うことができる（21 CFR 11.200 (a)）。
- 自分以外の人物が電子署名を使用する場合は、2人以上の者の共同作業により行わなければならない（21 CFR 11.200 (a)）。
- バイオメトリクスデータに基づく電子署名は、真の所有者のみが使用できるように考案しなければならない（21 CFR 11.200 (b)）。

技術的な問題とは別に、電子署名を開発、管理、維持、または使用するすべての人には、自分に割り当てられたアクションを実行するために必要な資格、トレーニング、および経験がなければなりません。

3.6　パスワード管理

バイオメトリクス手法によらない電子署名の場合、21 CFR Part 11では、ユーザーがシステム内で自分を識別するために2つの機能（例えば、ユーザーIDとパスワード）を使用しなければならないようにすることを推奨しています。そのため電子署名の真正性を確認するための2つのセキュリティ機能のうちの1つとして使用されるパスワードを管理することは、特に正しいパスワードの使用方法をユーザーに教育するという意味で、重要なプロセスです。

また、パスワードを管理するコンピュータシステムは、パスワードの安全性と完全性を確保するために、以下のような適切な管理メカニズムを提供する必要があります。

- 各ユーザーIDとパスワードが一意であることを保証する
- ユーザーIDとパスワードが定期的に見直し、リコール、または変更されることを保証する

パスワードの使用期間の長期化と操作に対する本質的な保護を提供するために、パスワードは一定の間隔で期限切れとなり、変更されなければなりません（21 CFR 11.300(b)）。

これらを考慮した結果、コンピュータ化システムでのパスワード管理には、いくつかの具体的な要件があります。

- パスワードの設定と有効期限設定：ユーザーは、ユーザープロファイルで定義された一定期間後に、パスワードを変更する必要がある。パスワードは、n個の新しいパスワードが生成された後でなければ再利用できないようにする。
- パスワードの設定と有効期限設定：ユーザーは、ユーザープロファイルで定義された一定期間後に、パスワードを変更する必要がある。パスワードは、n個の新しいパスワードが生成された後でなければ再利用できないようにする。
- 初回ログイン時に強制的に新しいパスワードを設定する機能
- ログインに失敗した回数に応じてユーザーアカウントを自動的にロックし、ロック解除にはユーザー管理権限を持つ管理者が必要
- マウスやキーボードの操作がない状態が一定時間続くと、またはアプリケーションがバックグラウンドで一定時間動作していると、自動的にロックされる
- ログイン、手動および自動ログアウト、ログインの失敗、間違ったパスワードを繰り返し入力した後のユーザーアカウントのロック、ユーザーによるパスワードの変更など、アクセス保護に関連するアクションのロギング
- データ入力のためのパラレルアクセスの遮断

さらに、システムへの不正アクセスや意図しないデータ操作を防ぐために、ユーザーにはOSレベルで特定の権限を割り当てる必要があります。

3.7　ユーザー管理

コンピュータ化システムへのアクセスについて、明確なガイドラインがあります。ユーザー管理システムでは、権限を与えられた人だけがデータにアクセスできるようにしなければなりません（FDA 2008, 21 CFR 211.68(b)）。また、FDAは、可能な限り、仕様、プロセスパラメータ、およびメソッドにアクセスできる人を制限することを推奨しています。

これらの推奨事項は、ユーザー管理に関する一連の要求事項につながります。まず、ファイルシステム、フォルダー構造、システムデータへの不正なアクセスや操作を防ぐために、ユーザーは自分の役割や職務に応じて必要な権限のみを持つ必要があります。このアプローチのモデルは次のようなものです。

- 管理者によるユーザーの一元管理（作成、停止、ブロック、ロック解除、ユーザーグループの割り当て）
- 特定のユーザーグループに対するアクセス権の定義
- 施設内の特定のユニットに応じたアクセスとアクセス権のレベル、および固有の識別方法（ユーザーID）とパスワードの使用

さらに、FDAは、システム管理者の役割は、レポートの内容を作成または変更するような他の役割を持たない人に割り当てることを推奨しています。会社やユーザーグループの規模によってこれができない場合は、設定や記録の内容を第二の担当者に確認させるなど、追加の管理方法を実施する必要があります。例外的に、この追加チェックは同じ人が行うこともできます。

具体的には、ユーザー管理システムは以下の要件を満たす必要があります。

- システムへのアクセスは、権限を与えられた人に限定する（21 CFR 11.10 (d); 21 CFR 11.10 (g); Annex 11, 12.1）。
- セキュリティ対策の程度は、コンピュータ化システムの重要性による（附属書11、12.2）。
- アクセス権の作成、変更、取り消しはすべて記録される（Annex 11、12.3）。
- システムが特定のデータやコマンドを特定のデバイス（端末など）を使って入力することを要求する場合、システムはすべてのデータやコマンドのソースの有効性をチェックする（21 CFR 11.10 (h)）。
- 各ユーザーIDとパスワードの組み合わせの一意性が維持され、指定された組み合わせが一度だけ割り当てられることを保証する管理メカニズムがある（21 CFR 11.300 (a)）。
- ユーザーIDの有効性を定期的にチェックするメカニズムがある（21 CFR 11.300 (b)）。
- パスワードは有効期限があり、一定期間ごとに変更する必要がある（21 CFR 11.300 (b)）。
- 組織を離れたり、新しいポジションに移ったりしたときに、ユーザーIDとパスワードを失効させるメカニズムがある（21 CFR 11.300 (b)）。
- このシステムにより、ユーザー ID やパスワードを含む、あるいは生成するトークン、カード、その他のデバイスを紛失した場合の損害管理措置、関連する権限を取り消す措置、一時的または恒久的な代替品を発行するための厳密かつ管理された手順が提供される（21 CFR 11.300 (c)）。
- 不正アクセスの試みを検知し、セキュリティ組織および会社の経営陣に通知するメカニズムがある（21 CFR 11.300 (d)）。
- トークンやカードなど、ユーザーIDやパスワードを含むまたは生成するデバイスは、発行時および定期的にテストされ、指定されたとおりに動作し、許可なく操作されていないことを確認する（21 CFR 11.300 (e)）。

3.8 アーカイブと削除

データインテグリティは、データのライフサイクル全体にわたって確保されなければなりません。特に、システムには、データをアーカイブするための安全で検証されたプロセスと、データの有効期限および/または保存期間後にデータを安全に削除するためのプロセスが含まれていなければなりません。具体的には、FDAは以下を要求しています。

- すべての関連データを定期的にバックアップすること（Annex 11, 7.2）、および
- 電子記録は、文書保管期間中、いつでも取り出すことができること（21 CFR 11.10 (c); Annex 11, 17）。

これらの目的のために、データの保存と復元、アーカイブと取り出し、および削除のための適切な管理手順を確立する必要がありま

す。データのアーカイブは継続的およびバッチ単位の両方でできなければならず、また、データの正確さに応じて、いくつかのアーカイブレベルを設定する必要があります。

- アラートと測定値は、まずローカルアーカイブに保存される。
- ローカルにアーカイブされたデータは、自動的に長期アーカイブに転送することができる。この場合、アーカイブされたデータが操作されていないかどうかをチェックするために、チェックサム生成などの適切な手段を講じる必要がある。
- アーカイブされたデータは、保存期間中に取り出すことができなければならない。
- 保存期間終了後は、データを安全かつ確実に削除しなければならない。
- データの削除は、記録して文書化する必要がある。

3.9 監査証跡のレビュー

監査証跡とは、電子バッチ記録の生成、変更、削除の際に行われたすべてのアクションを、関連するタイムスタンプに基づいて追跡するための、セキュリティで保護されたコンピュータ生成のレポートです。監査証跡では、誰がいつ、システムの何を変更したかを確認することができます。例えば、クロマトグラフィーの監査証跡には、ユーザー名、分析日時、使用したパラメータ、後に行われた手直しや変更の情報（理由を含む）が含まれています。

ここでいう電子監査証跡とは、データ（プロセスのパラメータや結果など）の記録、変更、削除に関するすべての情報を含み、また、システムレベルでの変更（システムへのアクセスやファイルの名前変更、削除の試みなど）も記録します。GMP（製造管理及び品質管理規則）に準拠した文書・データ管理の重要な要素である監査証跡は、データの損失を防ぐことができます（FDA 21 CFR 211.160(a), 211.194; FDA 2010, 21 CFR 212.110(b)）。監査証跡は、ユーザーが通常の操作中に規制対象の記録を作成、変更、削除できる場合に特に重要となります（FDA業界向けガイダンス「Part 11 - Scope and Application（Part 11－範囲と適用）」2003年）。ユーザーによる変更や削除ができない、自動的に生成される電子記録は、システムが適切なセキュリティ対策（アクセス保護など）を提供している場合、監査証跡を必要としません。

FDAおよび欧州委員会の勧告によると、データおよび文書のシステムでは以下のことを行う必要があります。

- GMPに関連するすべての変更と削除の記録（システムによる監査証跡）を生成する
- GMP関連データのすべての修正または削除の理由を記録する（21 CFR 11.10 (e); Annex 11, 9）
- データの入力、変更、確認、削除を行ったオペレーターのユーザーIDとその日時を記録する機能を有する（Annex 11, 12.4）
- 電子記録の変更により、以前に記録されたデータが判読できなくなることを防ぐ（21 CFR 11.10 (e)）
- 関連する電子文書の保存期間と同等またはそれ以上の期間、監査証跡を保存する（21 CFR 11.10 (e); Annex 11, 9）
- 監査証跡を当局がレビューやコピーできるようにする（21 CFR 11.10 (e)）

データとプロセスの品質を確保するために、FDAは、重要なデータの変更を記録する監査証跡を、バッチまたは製造記録と一緒に、記録をリリースする前にレビューすることを推奨しています。また、FDAは、企業が監査証跡のレビューのための適切な手順とルーチンを確立することを推奨しています。

このような背景から、2016年8月のPIC/Sドラフトガイダンス「*Good Practices for Data Management and Integrity in Regulated GMP/GDP Environments*」では、企業が監査証跡のレビューのための包括的な機能をサポートする適切なソフトウェアソリューションを使用することを推奨しています。

具体的には、以下のような機能が求められます。

- ユーザーによる変更を許さないプロセスデータの記録
- ユーザーの介入や電子署名を含む、バッチ記録におけるすべてのバッチ関連記録の文書化
- バッチ記録のアーカイブ
- ファイルの操作を防止・検出するメカニズム
- 操作中にオペレーターが行ったすべての変更や関連データの入力のロギング
- 必要なイベントや情報（古い値、新しい値、ユーザーID、日付とタイムスタンプ、操作内容、バッチ名など）のイベントログへのロギング
- 動作やイベントの順序が重要な場合の適切なシステム側でのチェック

3.10 バックアップと復元

データのアーカイブは、データバックアップのためのソリューションによって補完されなければなりません。FDAは、21 CFR 211.68(b)に基づき、バックアップを「オリジナルデータの全保存期間にわたって安全に保管されたオリジナルデータの真正コピー」と定義しています。バックアップには、すべてのデータとメタデータがオリジナルのフォーマットまたは互換性のあるフォーマットで含まれている必要があります。ここで重要なのは、GMPに準拠したデータバックアップと、システムクラッシュやネットワーク障害などでデータを復元するためのコンピュータ化システムで生成される従来型のデータバックアップとを区別することです。従来のバックアップは一般的に揮発性であり、21 CFR 211.68(b)で規定された要件を満たしていません。

国際製薬技術協会の「*ISPE GAMP Guide:Records and Data Integrity*」では、21 CFR 211.68(b)に従ってバックアップの追加要件を定義し、バックアップと復元の実行方法、バックアップの頻度、検証および適切なバックアップメディア、場所と条件、その他の技術的要件を規定しています。

適切なシステムを使えば、動的な電子記録のバックアップを取ることができます。そのためには、オリジナル文書の意味が曖昧でなく明確になるように、すべてのコンテンツとメタデータを記録しなければなりません。どのような場合でも、バックアップはオリジナルデータとまったく同じ管理メカニズムが適用され、不正なアクセスや操作を防ぎます。場合によっては、ポータブルメディアからの記録の削除を防止するなど、追加の措置が必要になることもあります。

さらに、コンテンツ、製品、またはバッチの検索を可能にするために、保存期間全体にわたってバックアップ、特にメタデータへのアクセスを可能にする適切なソフトウェアとハードウェアのソリューションを導入しなければなりません。バックアップデータは別の場所に保管することで、災害時や極限状態でのデータの安全性を高めることができます。

4 システムの説明

4.1 構造

国際自動制御学会（ISA）は、自動化プロセスのピラミッドモデル（図4-1）を作成しました。このモデルは、データの記録、管理、保存、送信に使用できる制御ソリューション内の技術とシステムを分類するのに役立ちます。

コンピュータシステムにおけるデータインテグリティの観点から、本書ではピラミッドの下位3階層、すなわち機械とセンサ、SIMATIC PCS 7 と SIMATIC Batch を搭載した分散型制御システム（DCS）、Opcenter Execution Pharma を搭載した製造実行システム（MES）を取り上げます。

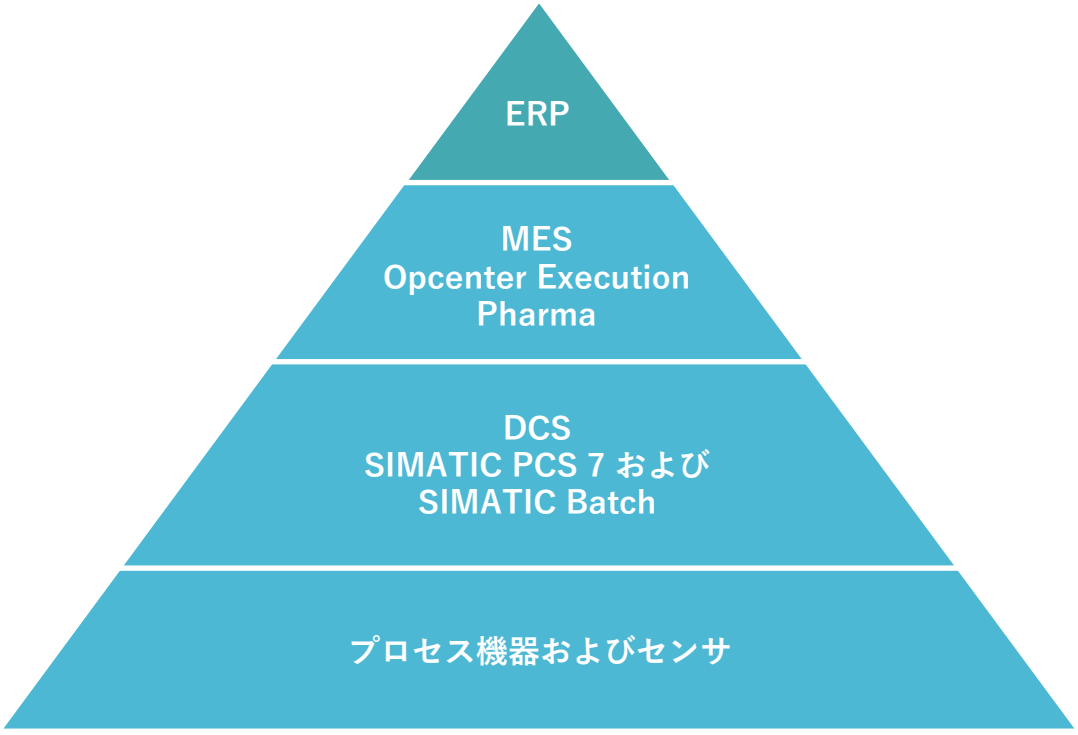

図 4-1 ANSI/ISA 95に基づく自動化のピラミッド

4.2 データフローとデータストレージ

オートメーションシステムには、データを記録、送信、または保存するさまざまなコンポーネントが含まれています。オートメーションレベルのセンサとコントローラ、DCSとMESレベルのさまざまなサーバ、各種バスシステムを備えた典型的なシステムアーキテクチャを図4-2に示します。

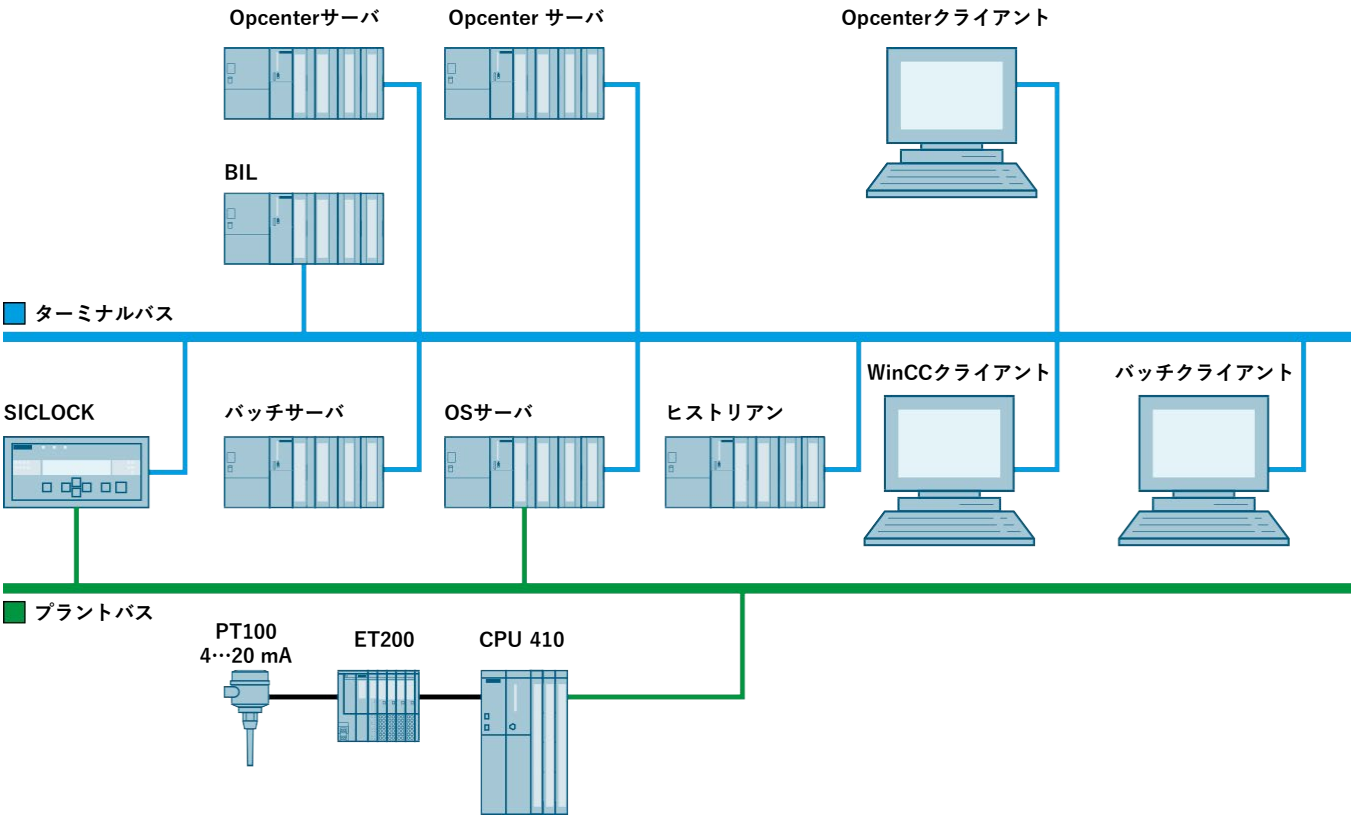

図 4-2 一般的なシステムアーキテクチャ

4.3 オートメーションレベル

センサはさまざまな技術で接続することができます。断線（<4mA）や過電流（>20mA）の検出に対応した4…20mAの接続など、故障の検出が可能な接続を選ぶことが重要です。

分散型システム（ET 200）は、Profibus/Profinet経由でCPUに接続することができます。チェックサムを生成・評価することで、データ伝送を検証します。Profinetは、予約帯域幅で動作し、リアルタイムの通信を保証します。予約帯域幅の中で、標準的なネットワーク通信を妨げることなく、タイムクリティカルなデータを送信することができます。

オートメーションレベルは、フィールドレベルのプラントバスを介してリンクされています。このバスは、システムからデータを受信し、独自のS7プロトコルでデータを送信（CPU→WinCC、WinCC→CPU）します。

4.4　データフロー

図4 3は、異なるレベルやシステム間のデータフローを示しています。具体的には、個々のデータフローは以下の通りです。

1. オートメーションレベルでのプロセスデータの受信
2. 監視、制御、アーカイブのためのOSサーバへのデータ転送
3. 監視、制御のためのOSサーバからバッチサーバへのデータ送信
4. アーカイブのためのOSサーバからプロセスヒストリアン（PH）へのデータ転送
5. アーカイブのためのバッチサーバからPHへのデータ転送
6. バッチサーバとOpcenter Execution Pharmaサーバ間のネイティブバッチ統合レイヤー（BIL）インターフェイスを介したデータ転送
7. バッチサーバとOpcenter Execution Pharmaサーバ間のBILインターフェイスによるデータ転送
8. クライアントとOpcenter Execution Pharmaサーバ間の通信
9. クライアントとOSサーバ間の通信
10. クライアントとバッチサーバ間の通信

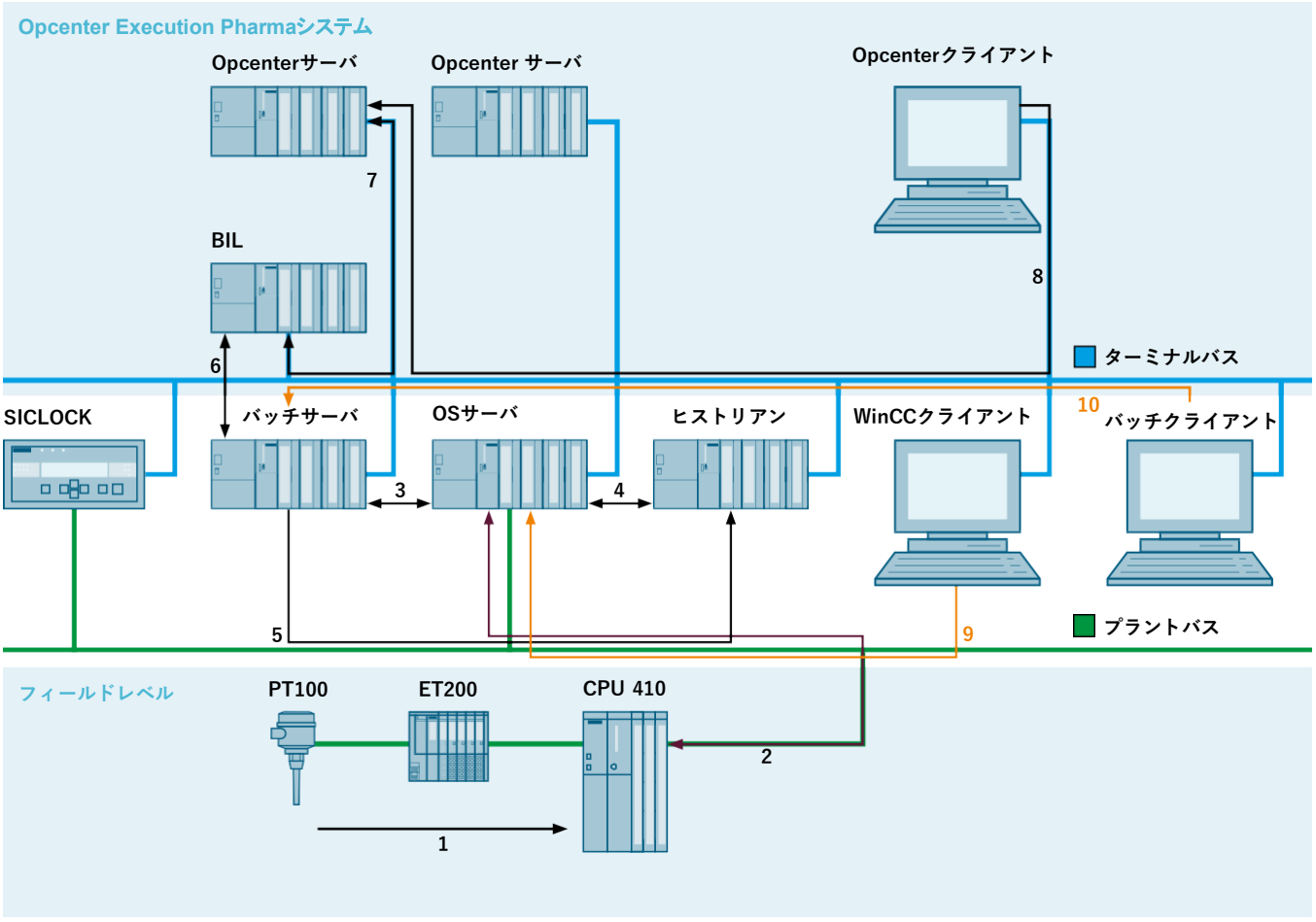

図 4-3 異なるレベルやシステムを横断するデータフロー

4.5 時刻の同期

データを正しく処理・評価するためには、すべてのシステムが同じタイムベースで動作していることが重要です。

図4-3には、時刻同期のための対応システムが含まれています。

4.6 データのライフサイクル

4.6.1 センサレベルのデータ

センサレベルのデータはCPUに送信され、永久保存はされません。分散型システムは、データが技術的な制限（例えば、4...20mA）の範囲内にあるかどうか、また、センサが正しく動作しているかどうかをチェックすることで、データの最初の評価を行います。

この評価の結果がステータスとなり、測定値とともにCPUに送信されます。

4.6.2 DCSレベルのデータ

取得したセンサデータは、対応するIOドライバを介してCPU410で評価されます。制御ロジック内では、測定値の送信ステータスを使用して、プロセス定義に従って行動することができます。所定のエラーイベントでは、システムはエラーを文書化したOSサーバ用のメッセージを生成します。測定値やメタデータを定性的に評価するためには、データのタイムスタンプがシステム間で同期している必要があります（測定値、ステータス、メッセージ）。

ここでは、通常の操作では操作できないデータについて説明します。すべてのデバイスを物理的な手段で保護し、権限を与えられた人だけがシステムにアクセスできるようにすることが重要です。

4.6.3 OSサーバとバッチサーバのデータライフサイクル

データは、SIMATIC PCS 7プロジェクトの構成に基づいて、DCSレベルからOSサーバおよびバッチサーバに送信され、変更することはできません。

ユーザーとパスワードの管理

SIMATIC PCS 7に含まれる強力なツールの1つであるSIMATIC Logonは、Microsoft Windowsのセキュリティ機能を採用したユーザー管理システムを構築することができます。

- 個々のユーザーと、関連するWindowsユーザーグループは、Microsoft Windowsのユーザー管理システムで定義されます。
- SIMATIC Logonは、Windowsのユーザーグループを、SIMATIC PCS 7 OSやSIMATIC BATCHなどのSIMATICコンポーネントのユーザーグループに結びつけます。
- ユーザーグループに基づいて、それぞれのSIMATICコンポーネント（例：PCS 7 OS）に異なる権限レベルの権限が定義されます。
- SIMATIC PCS 7マルチプロジェクトのプロジェクトは、SIMATIC Logonによる不正アクセスからの保護ができません。このようなプロジェクトでは、ユーザーIDとパスワードの組み合わせをカスタマイズしてアクセスするように設定できます。

監査証跡

OSサーバ上のプロセスデータ（プロセスパラメータ、プロセスやオペレーターのメッセージなど）は、ユーザーが変更できないように保存されています。操作中にユーザーが行ったOSサーバやバッチサーバへの変更やデータ入力は、すべて監査証跡に記録する必要があります。SIMATIC PCS 7のメッセージアーカイブは、必要なイベントや情報（古い値、新しい値、ユーザーID、日付とタイムスタンプ、操作内容、バッチ名など）を記録します。監査証跡を印刷することができます。

すべてのバッチ関連記録は、オペレーターの介入や電子署名を含むバッチ記録に記録されます。バッチ記録は、XMLやPDF形式で保存できます。

SIMATIC PCS 7およびSIMATIC BATCHでは、これらのデータを変更するためのユーザーアクションはありません。これらのファイル内のデータを直接操作することは、OSのセキュリティ設定で禁止する必要があります。それにもかかわらずファイルが変更された場合は、操作が検出され、バッチ記録を開く際にアラートが表示されます。

バックアップと復元

SIMATIC PCS 7は、構成可能で拡張性のあるアーカイブコンセプトを提供します。メッセージと測定値は、統合されたシステムアーカイブに継続的に保存されます。これらのローカルにアーカイブされたデータは、長期アーカイブに自動的に転送することができます。

チェックサムを生成することで、アーカイブされたデータの不正操作を検知します。

アーカイブされたデータは、保存期間全体にわたって取り出すことができます。システム障害が発生しても、アーカイブのデータを再リンクすることができます。

このバックアップと復元の機能は、最初に設定され、適切な手順によって記述されなければなりません。規制対象となる企業は、この機能を初期および定期的に確認する責任があります。

電子署名

DCSでの操作に電子署名が必要な場合は、SIMATIC PCS7電子署名アプリケーションを使用して構成し、どのユーザーが現在ログインしているかに関係なく、ユーザーによる明示的な認証を強制することができます。また、アプリケーションで署名シーケンスを定義し、複数のユーザー（異なる権限を持つ）がアクションに署名しなければならないようにすることも可能です。

成功した署名はすべて、オペレーターメッセージとしてWinCCアラームロギングシステムに保存され、変更保護されて表示されます。

4.6.4 プロセスヒストリアンのデータアーカイブ

PH長期アーカイブは、SIMATIC PCS 7とネイティブに統合されているので、バッチサーバやOSサーバからPHへのデータ転送は完全に自動で行われます。また、「ストア＆フォワード」メカニズムにより、バッチサーバやOSサーバとPHとの間のネットワーク接続に不具合が生じた場合でも、データの損失を防ぐことができます。システム障害を防ぐために、PHはRAID（Redundant Array of Inexpensive Disks）に合わせて設置された冗長システムとして実装することができます。システムが完全にクラッシュした場合には、バックアップからデータベースを完全に復元することができます（ディザスタリカバリ）。

アーカイブされたデータは、変更できないセグメントに保存され、読み取り専用のアクセスが可能です。

データは、保存期間中、PHに確実かつ安全に保存され、アクセスが可能です。期限切れのデータや不要になったデータの削除は、文書に記録しなければなりません。

4.6.5 バッチサーバとOpcenter Execution Pharmaシステム間のデータ交換

データはネイティブのBILインターフェイスを介して送信され、このプロセスで変更されることはありません。このインターフェイスは、ネットワークやシステムの障害時に、高可用性を確保し、データを損失しないように設計されています（BILのリカバリー管理）。

データは、バッチサーバとOpcenter Execution Pharmaの間でコピーとして交換されます。お客様の仕様に応じて、オリジナルデータを2つのシステムのどちらかにGMP要件に沿って保存し、もう一方のシステムにコピーとして保存することができます。

BILサーバは、冗長化されたシステムとして実装することができます。操作中にはBILインターフェイスはユーザーには見えず、ユーザーはBIL内のデータにアクセスできません。BILの設定の変更は権限を与えられたユーザーのみが行うことができ、ログファイルに記録されます。

4.6.6 Opcenter Execution Pharmaシステムにおけるデータのライフサイクル

MESで受信または生成されたデータは、内部のデータベースに保存されますが、このデータベースは管理者権限を必要とするため、操作されないように保護されています。MESのオペレーター権限を持つユーザーに、管理者権限を与えてはいけません。データ損失に対するシステムの強化のために、インストール文書に記載されているように、データベースにバックアップと復元の機能を設定する必要があります。

自動または手動の操作は、タイムスタンプ、ユーザー、操作の理由とともにシステムに記録されます。これらのデータは、GMP環境でのレポート作成に利用できます。

Opcenter Execution Pharmaでは、バッチレポートの電子署名など、DCSレベルに転送されないGMP関連のデータやメタデータがバッチリリース用に生成されます。その結果、Opcenter Execution Pharmaシステム内のデータはオリジナルデータとして定義する必要があります。

ユーザーとパスワードの管理

ユーザー管理は、Opcenter Execution Pharmaの基本機能であり、Microsoft Windowsのセキュリティメカニズムに基づいて、またはスタンドアロンのソリューションとして、ユーザー管理システムを構築するために使用することができます。

Opcenter Execution Pharmaのユーザー管理は、アクセス保護の要件を満たしています。さらに、Opcenter Execution Pharmaシステムプログラムのファイル構造への不正アクセスや意図しない操作を防ぐために、ユーザーにはOSレベルで特定の権限を割り当てる必要があります。ユーザー管理におけるすべての変更は、監査証跡に記録されます。

監査証跡

Opcenter Execution Pharmaは、GMPに関連する設定とオペレーターのアクション（「誰が」、「何を」、「いつ」、そしてオプションとして「なぜ」）を記録することで、これらのアクションの監査証跡の要件をサポートし、そのような電子記録に適したレベルのシステムセキュリティ（例えば、アクセス制御）を提供します。GMP関連データは、規制対象企業が、対応する法的要求事項に基づいて定義します。

すべての監査証跡は、紙に印刷することも、電子ファイルとしてエクスポートすることも可能です。

バックアップと復元

バックアップ戦略は、Oracleデータベースと利用可能なデータベースメカニズムを使用して定義することができます。データベース管理者がデータを復元することができます。

電子署名

Opcenter Execution Pharmaは、電子署名を構成するための機能を備えています。電子署名を必要とする操作やアクション、これらのアクションに対してどのグループが署名できるか、署名の順序などは、設定段階で指定されます。個別の検証プロセスに対応するために、次の4種類の電子署名があらかじめ定義されています。

- 単一の電子署名（アクションを実行したユーザーの署名）
- 二重（条件付き）電子署名（オリジナルのオペレーターが実行されたアクションを検証する権限を持っていない場合、責任あるユーザーの追加署名が必要）
- シングルチェック電子署名（アクションを実行したユーザーとは異なるユーザーの署名）
- ダブルチェック電子署名（アクションを実行したユーザーとアクションを実行していないユーザーの署名）

4.7 Opcenter Execution Pharmaシステムでのアーカイブ

Opcenter Execution Pharmaは、設定可能でスケーラブルなアーカイブ機能を提供します。メッセージと測定値は、ローカルのOpcenter Execution Pharmaアーカイブに継続的に保存されます。これらのローカルに保存されたデータは、長期アーカイブに自動的に転送することができます。アーカイブされたデータは、設定された保存期間内であれば取り出すことができます。

また、アーカイブデータベースからエクスポートデータベースにデータを移動し、サードパーティのアーカイブツールのインターフェイスとして使用することもできます。

すべてのアーカイブ手順は記録され、監査証跡でアクセス可能です。

バッチ記録の一部である外部データは、Opcenter Execution Pharmaの自動アーカイブ手順の一部ではないことに注意することが重要です。このようなデータに対しては、お客様のアーカイブ戦略に合わせて、お客様と連携した個別のソリューションを設計する必要があります。

5 シーメンスの過去の出版物

- SIMATIC PCS 7 V9.0 適合宣言書 ERES(www.siemens.com/gmp)
- SIMATIC IT eBR V6.1 SP3 適合宣言書 ERES(www.siemens.com/gmp)

※SIMATIC IT eBRはOpcenter Execution Pharmaの旧製品名です。

Published by
Siemens AG 2019

Siemens AG, Process Industries and Drives
Östliche Rheinbrückenstraße 50

76187 Karlsruhe, Germany

Article No.: VRPH-B10018-00-7600
Printed in Germany