

21 CFR Part 11 および Annex 11 コンプライアンスのサポート： OpenLab Server および OpenLab ECM XT

概要

米国 FDA が定める連邦規則 (CFR) 第 21 条第 11 章 (21 CFR Part 11) と、それに相当する欧州連合の Eudralex 第 4 章附属書 11 (Annex 11) では、規制対象の製薬会社で電子記録および電子署名を使用する際の要件を規定しています。21 CFR Part 11 は 1997 年に制定され、1999 年より施行されています。これらのガイドラインの目的は、該当するすべての電子記録について、ALCOA の原則 (責任の所在が明確であること、判読できること、同時であること、原本であることおよび正確であること) を確保し、その完全性を維持することにあります。

このホワイトペーパーは、これらの規制の遵守が求められる、OpenLab Server または OpenLab ECM XT のユーザーを対象としています。OpenLab Server は、アジレントのデータシステム (OpenLab CDS など) によって取得および処理されたデータのために、安全な中央のリポジトリを提供します。OpenLab ECM XT は安全なレポジトリを拡張し、他社製のデータシステム (Waters Empower など) によって生成されたデータや、その他のソフトウェアデータ (Microsoft Office ファイル、PDF など) を保存します。一方、ユーザーは、OpenLab Server および OpenLab ECM XT の機能を適切に使用し、コンプライアンス態勢を整えることによって、ラボのデータを安全に保存する責任を負います。ユーザーは、OpenLab Server および OpenLab ECM XT で提供される技術的管理に加え、関連のビジネス要件、IT 手順および管理に対応するための標準操作手順書 (SOP) を通じて、手順管理を確立する必要があります。例えば、内部監査プログラムなどのガバナンスを確立し、システムオペレータに確実に SOP に従うよう教育する必要があります。

付録 1 では、21 CFR Part 11 の各項、EU Annex 11 の関連条項の要件、およびその他の国の規制を満たすうえで役立つ OpenLab Server/ECM XT の機能について詳しく説明します。この説明では、機器のハードウェアおよびソフトウェアを含むシステムアクセスが、システムに保持されている電子記録に対する責任を担うスタッフによって管理されていることを前提としています。すなわち、システムが、21 CFR Part 11.3 (b)(4) で規定される「クローズドシステム」として設計されているものとします。

本文書では、OpenLab CDS、その他のデータシステム、および Microsoft Excel をはじめとするソフトウェアアプリケーションなど、データを生成するアプリケーションの機能が、どのように電子記録や電子署名の要件を満たすかについては説明していません。これらのアプリケーションはプライマリアプリケーションと呼ばれます。安全な中央のレポジトリとしての OpenLab Server/ECM XT と統合されたプライマリアプリケーションによって作成されたファイルは、すべてのバージョンが追跡されます。OpenLab Server/ECM XT はその他のファイルのための安全な中央レポジトリとして機能し、すべてのバージョンを追跡可能です。新しいバージョンのファイルは、OpenLab Server/ECM XT で安全に保存され、追跡されます。ただし、ファイル内の変更に関する具体的な内容は、プライマリアプリケーションの監査証跡およびログによって追跡されます。

「セキュリティ原則としての職務の分離の主な目的は、不正行為と過失を防ぐことにあります。この目的は職務と関連する権限を複数のユーザーに分散させることにより達成できます。」

21 CFR Part 11

21 CFR Part 11 では、規制対象のラボの運営における次の 3 つの要素について規定しています。

- 電子記録のセキュリティ
- 作業の責任の所在の明確化
- 電子署名（使用する場合）

セキュリティ

セキュリティとは、「正当な人が正当な情報への正当なアクセス権を持つ」ということを意味します。規制対象のラボは、システムユーザーの本人確認をし、かつ教育を受けた権限のある個人にシステムアクセスを限定できなければなりません (11.10 (d)、(i)、および (g)、11.100 (b))。ラボのスタッフは、職務に応じてさまざまな責任を担っていることから、データアクセスを分けることができ、特定のユーザーが特定のデータセットに対して適したアクセス権を持ち、また他のデータセットへ別のアクセス権を持つように定義できる必要があります。

作業の責任の所在の明確化

作業の責任の所在を明確にすることは、作業を「誰が、何を、いつ、どこで、どんな理由で」行ったのかを文書化することです。これは通常、自動化された監査証跡機能を使用して実施されます。自動化された監査証跡では、ユーザーの操作が個別に記録され、ラボの

スタッフと、そのスタッフが実行した作業が関連付けられます。監査証跡をもとに、スタッフおよび査察官は、電子記録の完全な履歴を再構成することができます。

- 誰が：記録を作成、変更、または削除するといった操作に責任を負っている者を明確に示します。
- 何を：実行された操作を示します。該当する場合は、記録に保持されている古い値と新しい値を含みます。
- いつ：操作が実行された日時を明確に示します。
- どこで：影響を受けた記録を明確に示します。
- 理由：規制対象の記録に対する変更の理由を説明します。一貫性を保つため、また監査証跡の検索および並べ替えを可能にするために、理由はあらかじめ定義されたリストから選択することができます。

電子署名

21 CFR Part 11 では、電子署名の使用を義務付けていませんが、使用する場合の規定を定めています。この場合、システムでは電子署名について次の条件を満たす必要があります。

- 取り消しできない方法で該当する記録に関連付けられていること
- 署名者の氏名および署名日時のほか、署名の意味（レビュー、承認、責任、作成者など）が示されていること
- 署名された記録を表示または印刷するたび表記されること

付録 1 : OpenLab Server または OpenLab ECM XT による、US FDA 21 CFR Part 11 および関連する各国規制で規定されている要件の遵守

付録 1 の表に関する注意事項

1 列目

表では、21 CFR Part 11 の要件を US FDA の参考文献 [2] に記載されている順に記載します。²

2 列目

完全性を保つために、2 列目には、21 CFR Part 11 およびその他の関連する各国規制のすべての要件を示します。表中の「システム」は、データの取り込みおよび解析などの処理に使用される分析システムを指します。

多くの要件は、技術的管理（ソフトウェア機能）または手順管理（SOP）のいずれかにより満たされます。技術的管理とは、ソフトウェアの管理機能です。また、手順管理は、ユーザーの責任において実施する必要がある管理措置です。太字で記載されている 21 CFR の要件は、技術的管理によって満たされる要件です。その他の各国要件は標準フォントで示しています。

また、手順管理によって対処する必要がある要件は、青色で示しています。

3 列目

3 列目には、各要件の責任の所在を示します。「S」は分析システムのメーカーを表し、「U」はユーザーを表します。「S」と「U」の使用は、技術的管理および手順管理の両方が組み合わされていることを意味します。

4 列目

4 列目には、可能な場合に適宜、関連する各国要件とコメントを記載します。

5 列目

5 列目には、OpenLab Server/ECM XT で提供される技術的管理（ソフトウェア機能）により要件を満たすことができるかどうかを「可」または「不可」で示します。手順管理によって要件に対処しなければならない場合は、N/A（該当せず）が使用されます。

6 列目

6 列目では、OpenLab Server/ECM XT の技術的管理（ソフトウェア機能）により、規制要件をいかに満たすことができるかを説明します。また、関連する場合は、ユーザーに対するその他の推奨事項も示します。

1. バリデーション

Part 11 その他	要件	S、U	その他の規制またはコメント	可/不可	「可」の場合は具体的に要件がいかに満たされるか、または「不可」の場合、推奨される事柄。
Part 11 11.10 (a)	1.1 正確性、信頼性、意図した性能の一貫性、および無効な記録や変更された記録を識別する機能を保証するために、システムのバリデーションが実施されていますか。	S、U	すべての規制で義務付けられています。 この要件は、システム供給元とユーザーがともに責任を負う代表例です。ユーザーがバリデーションの最終的な責任を負う一方、例えば開発段階や関連するドキュメントのバリデーションといった一部の作業は、ソフトウェア供給元のみが実施でき、提供する必要があります。 第五章系統 第十三条在计算机化系统使用之前,应当对系统全面进行测试,并确认系统可以获得预期的结果。当计算机化系统替代某一人工系统时,可采用两个系统(人工和计算机化)平行运行的方式作为测试和验证内容的一部分。 第五章系統 第十三条在计算机化系统使用之前,应当对系统全面进行测试,并确认系统可以获得预期的结果。当计算机化系统替代某一人工系统时,可采用两个系统(人工和计算机化)平行运行的方式作为测试和验证内容的一部分。	可	アジレント・テクノロジーでは、正確性、信頼性、および一貫した性能を評価する試験により、OpenLab Server/ECM XT の性能を検証しています。ただし、ユーザーは、それぞれが保有するサンプル前処理システムを規制要件に従って検証する必要があります。 システムはすべてのファイルタイプに対応しています。 システムは一意のファイルを追跡し、一意のファイルが次にアップロードされるたびに、新規バージョンを作成します。 ソフトウェアは、安全なレポジトリにアップロードされたファイルが、プライマリアプリケーション（CDS など）によって作成されたファイルと同じであることを確認します。 ファイルの妥当性チェックは、プライマリアプリケーションの責任です。

1. バリデーション (続き)

Part 11 その他	要件	S、U	その他の規制またはコメント	可/不可	「可」の場合は具体的に要件がいかに満たされるか、または「不可」の場合、推奨される事柄。
Annex 11	1.2 設備は適切ですか。	U	Annex 11.Principle B ブラジル GMP 577	N/A	サーバーやネットワークなどの適切な設備を確保するのは、ユーザーの責任です。

2. 記録の正確なコピーと安全な保管および検索

Part 11 その他	要件	S、U	その他の規制またはコメント	可/不可	「可」の場合は具体的に要件がいかに満たされるか、または「不可」の場合、推奨される事柄。
Part 11 11.10 (b)	2.1 システムは、FDA による調査、審査に適した人間が判読できる形式と電子形式の両方で記録の正確かつ完全なコピーを生成できますか。	S、U	第五章系統 第十九条以电子数据为主数据时, 应当满足以下要求: (一) 为满足质量审计的目的, 存储的电子数据应当能够打印成清晰易懂的文件。	可	記録は、紙に印刷された形、または PDF ファイルといった電子形式で利用できます。
Annex 11	2.2 電子的に保管された電子記録は、明確に印刷されたコピーが得られますか。	S、U	Annex 11.8.1 ブラジル GMP 583	可	記録は、紙に印刷された形、または PDF ファイルといった電子形式で利用できます。
ブラジル	2.3 データのバックアップ、検索、および印刷で保守プロセスが適切に行われるための管理措置が設けられていますか。	S、U	ブラジル 585.2 第五章系統 第十九条以电子数据为主数据时, 应当满足以下要求: (三) 应当建立数据备份与恢复的操作规程, 定期对数据备份, 以保护存储的数据供将来调用。备份数据应当存储在另一个单独的、安全的地点, 保存时间应当至少满足本规范中关于文件、记录保存时限的要求。	可	データをバックアップするのは、ユーザーの責任です。システムは、すべての関連ファイルをバックアップできるように設計されています。アジレントは、データバックアップと復元を実施するための文書化された手順とユーティリティを提供します。
Part 11 11.10 (c)	2.4 システムでは、記録の保管期間を通して正確かつ容易に検索できるように記録が保護されていますか。	S、U	中国 GMP 163	可	システムにアップロードされるすべてのデータは、保護された場所に保存されます。 物理的セキュリティと、保護されたストレージへのアクセス制御を管理するのは、ユーザーの責任です。
Annex 11	2.5 アーカイブ期間中にデータのアクセスが容易か、判読できるかおよび完全であるかがチェックされていますか。	U	Annex 11.17	N/A	アーカイブ中にデータのアクセスが容易か、判読できるか、および完全であるかをチェックするのは、ユーザーの責任です。 システムは、アーカイブデータがアクセス可能で、判読でき、変更できないように設計されています。
Annex 11	2.6 システム (コンピュータ機器やプログラムなど) に対して該当する変更が行われた場合、データを復旧できることが確認され、テストされていますか。	S、U	Annex 11.17	可	システムは、旧バージョンからデータを読み取ることができるように設計されています。バリデーションプロセス中にデータ判読性を確保するのは、ユーザーの責任です。

2. 記録の正確なコピーと安全な保管および検索(続き)

Part 11 その他	要件	S、U	その他の規制またはコメント	可/不可	「可」の場合は具体的に要件がいかに満たされるか、または「不可」の場合、推奨される事柄。
Annex 11	2.7 データは、物理的および電子的手段によって損傷から保護されていますか。	S、U	Annex 11.7.1 ブラジル GMP 584 第五章系統 第十条系统应当安装在适当的位置，以防止外来因素干扰。 第五章系統 第十九条以电子数据为主数据时，应当满足以下要求： (二) 必须采用物理或者电子方法保证数据的安全，以防止故意或意外的损害。日常运行维护和系统发生变更（如 计算机设备或其程序）时，应当检查所存储数据的可访问性及数据完整性。	可	システムにアップロードされるすべての記録は、保護された場所に保存されます。物理的セキュリティを確保するのは、ユーザーの責任です。
臨床ガイド	2.8 FDA による（臨床）研究およびラボのテスト結果の審査のために電子的なソース/生の文書を再構成できるようにするための管理措置が実施されていますか。	S	臨床コンピュータガイド F2 FDA Q&A	N/A	電子データを再構成するために必要なプライマリアプリケーションにアクセスし、維持するのは、ユーザーの責任です。
臨床ガイド	2.9 FDA に提出される情報には、ソース/生データがどのように取得および管理され、データを取り込むために電子記録がどのように使用されたかが完全に記述され、説明されていますか。	U	臨床コンピュータガイド F2 FDA Q&A	N/A	ソース/生データがどのように取得および管理され、データを取り込むために電子記録がどのように使用されたかを記述するのは、ユーザーの責任です。
Annex 11	2.10 システムでは、すべての関連データを定期的にバックアップすることが可能ですか。	S、U	Annex 11.7.1 中国 GMP 163 ブラジル GMP 585 Part 211, 68 b	可	データをバックアップするのは、ユーザーの責任です。システムは、すべての関連ファイルをバックアップできるように設計されており、データバックアップと復元を行うためのユーティリティが含まれています。
Annex 11	2.11 バックアップデータの完全性と正確性、およびデータを復元する機能が検証中にチェックされ、定期的にモニタリングされていますか。	U	Annex 11.7.2 中国 GMP 163 ブラジル GMP 585 Part 211, 68 b	N/A	バックアップデータの完全性と正確性を確保し、復元データを定期的にチェック、検証、およびモニタリングするのは、ユーザーの責任です。
臨床 コンピュータ ガイド	2.12 保護されたシステムソフトウェアを経由していない外部ソフトウェアによるデータの変更、閲覧、照会、またはレポート作成を阻止するための手順および管理措置が実施されていますか。	S、U	臨床コンピュータガイド E	可	システムは、権限のあるユーザー資格情報を用いて、ウェブインタフェースからアクセスできます。アプリケーションによるファイルへのアクセスは API によって制御されます。またデータ転送は、HTTPS /TLS によって暗号化できます。
臨床 コンピュータ ガイド	2.13 研究データおよびソフトウェアに対するコンピュータウイルス、ワーム、またはその他の潜在的に有害なソフトウェアコードを防止、検出、および低減するための管理措置が実装されていますか。	S、U	臨床コンピュータガイド F	N/A	アジレントは、OpenLab Server/ECM XT を業界標準のアンチウイルスアプリケーションと組み合わせてテストしています。ただし、アンチウイルスソフトウェアを実装するのは、ユーザーの責任です。

3. システム、機能、およびデータに対する権限にもとづくアクセス

Part 11 その他	要件	S、U	その他の規制またはコメント	可/不可	「可」の場合は具体的に要件がいかに満たされるか、または「不可」の場合、推奨される事柄。
Part 11 11.10 (d)	3.1 システムへのアクセスは、権限のある者に限定されていますか。	S、U	中国 GMP 183 163 ブラジル GMP 579、ICH Q7.5.43	可	OpenLab Server/ECM XT のユーザーベースのアクセスコントロールでは、一意のユーザー名とパスワードの組み合わせが必要です。これらのユーザーを構成し管理するのは、ユーザーの責任です。
	3.2 各ユーザーは、そのユーザー自身のユーザー ID とパスワードなどによって明確に識別されますか。	S、U	複数の警告書	可	各ユーザーは、一意の ID とパスワードの組み合わせによって識別されます。システムにアクセスするには、その両方の情報を入力する必要があります。
臨床	3.3 ある時点における権限のある個人の氏名、役職、およびアクセス権限の説明を示す累積記録を維持することができますか。	S、U	臨床コンピュータガイド 4	可	OpenLab Server/ECM XT は、Windows ドメインまたはアプリケーションで Windows ローカルにユーザー認証を設定します。アクセス権限はアプリケーションで設定され、すべての変更はアクティビティログに記録されます。ユーザー個人の権限およびユーザーが継承したグループ権限を示すレポートも利用できます。セキュリティのレビューを定期的に行う必要があるラボでは、これらのレポートを役立てることができます。

4. 電子監査証跡

Part 11 その他	要件	S、U	その他の規制またはコメント	可/不可	「可」の場合は具体的に要件がいかに満たされるか、または「不可」の場合、推奨される事柄。
Part 11 11.10 (e)	4.1 オペレータがログオンや、電子記録の作成、変更、または削除操作を実行した日時が個別に記録され、コンピュータにより生成されるタイムスタンプ付きの安全な監査証跡はありますか。	S	中国 GMP 163 第五章系統 第十六条 计算机化系统应当记录输入或 确认关键数据人员的身份。只有经授权人员，方可修改已输入的数据。每次修改一个已输入的关键数据均应当经过批准，并应当记录更改数据的理由。应当根据风险评估的结果，考虑在计算机化系统中建立一个数据审计跟踪系统，用于记录数据的输入和修改。	可	OpenLab Server/ECM XT に保存されたファイルに対し実施されるすべての操作は、システムで生成されるタイムスタンプ付きの安全なアクティビティログに記録され、変更の理由も含まれます。
FDA GLP	4.2 監査証跡には、誰がどのような変更をいつどのような理由で行ったかが記録されますか。	S	FDA 21 CFF 58.130 e 臨床コンピュータガイド 2 臨床ソースデータ 3	可	OpenLab Server/ECM XT アクティビティログには、修正、変更の日時、ユーザー ID、および変更の理由が記載されます。
Annex 11	4.3 システムは、オリジナルの値から電子記録が変更されたかどうかを示す印字物を生成できますか。	S、U	Annex 11, 8.2	可	電子記録の監査証跡内の変更の詳細を追跡するのは、プライマリアプリケーションの責任です。 電子記録が OpenLab Server/ ECM XT に保存された後、ファイルに対するその後の更新はアクティビティログに記録されます。エンドユーザーはアクティビティログをエクスポートしたり印刷したりできます。
FDA GMP	4.4 監査証跡には、試験で採用された、既成のメソッドのすべての変更が含まれますか。 4.5 このような記録には、変更理由が含まれますか。	S	Part 211.194 8b	可	OpenLab Server/ECM XT は試験機器を管理しません。
	4.6 監査証跡は、常に有効ですか。また、システムユーザーが無効にできないようになっていますか。	S、U	警告書	可	ユーザーは、アクティビティログの記載を消去したり、変更したり、削除したりすることはできません。
Annex 11	4.7 監査証跡は、定期的なレビューのために一般にわかりやすい形式で利用できますか。	S	Annex 11, 9	可	OpenLab Server/ECM XT のアクティビティログは、簡単にレビューできるように設計されており、エンドユーザーがエクスポートしたり、印刷したりすることができます。
	4.8 監査証跡の内容は、監査証跡情報の現実的かつ意味のあるレビューを行えるように、関連する操作のみが記録されるように設定できますか。	N/A	監査証跡のレビューに関連する Annex 11 および多くの警告書の暗黙的要件	可	OpenLab Server/ECM XT では、情報のレビューに関するユーザーの好みに対応するため、内容を表示する前にアクティビティログをフィルタリングできます。

4. 電子監査証跡 (続き)

Part 11 その他	要件	S、U	その他の規制またはコメント	可/不可	「可」の場合は具体的に要件がいかに満たされるか、または「不可」の場合、推奨される事柄。
Part 11 11.10 (e)	4.9 記録が変更された場合、以前記録された情報はそのまま残されますか。	S		可	プライマリアプリケーション (OpenLab CDS など) は、データ入力に対する追加、変更、削除をすべて記録します。OpenLab Server/ECM XT に保存されたファイルへの変更は、元の記録の新しいリビジョンとして保存され、元の記録はそのまま残されます。追加の処理のためにファイルを開く際は、使用するファイルのバージョンをユーザーが (自身の権限に基づいて) 選択します。
Part 11 11.10 (e)	4.10 監査証跡は、少なくとも電子記録に求められる期間において維持されますか。	S、U		可	プライマリアプリケーション記録の監査証跡情報は、電子記録内に保存されます。 OpenLab Server/ECM XT に保存されるファイルのアクティビティログ情報は電子記録にリンクされ、分離することはできません。
Part 11 11.10 (e)	4.11 監査証跡は、FDA が審査およびコピーできる状態にありますか。	S		可	アクティビティログは、表示したり、フィルタリングを行ったり、印刷したりすることができます。
Annex 11	4.12 電子的に保存されている電子記録 (監査証跡など) の明確に印刷されたコピーを得られますか。	S	Annex 11, 8.1	可	プライマリアプリケーションによって提供されます。例えば、OpenLab CDS の監査証跡は表示したり、印刷したりすることができます。

5. 動作デバイスの確認

Part 11 その他	要件	S、U	その他の規制またはコメント	可/不可	「可」の場合は具体的に要件がいかに満たされるか、または「不可」の場合、推奨される事柄。
Part 11 11.10 (f)	5.1 必要に応じて、認められた順序に従って手順およびイベントが実行されるようにするための運用システムチェックは設けられていますか。	S、U		N/A	手順コントロールを指定および実施するのは、ユーザーの責任です。
Part 11 11.10 (g)	5.2 権限のある個人のみがシステムの使用、記録への電子署名、運用システムまたはコンピュータシステムの入出力デバイスへのアクセス、記録の変更、または操作を行えるようにするための権限の確認は行われていますか。	S	Part 211, 68 b	可	システムは、内容へのアクセスと、特定の操作を実行する権限を管理する、構成可能なユーザーロールに対応しています。
	5.3 システムは、データ入力、変更、確認、または削除を行ったオペレータを日時とともに記録するように設計されていますか。	S	Annex 11, 12.4	可	操作を行うオペレータは、アクティビティログに記録されます。
Part 11 11.10 (h)	5.4 システムでは、必要に応じてデータの入力元または操作の指示元の有効性を判断するためのデバイスチェックを利用できますか。	S、U	この要件には、有効な解釈が 2 つあります。すなわち、システムは次のように設計されていなければなりません。 1. 機器の操作またはデータを「ソース」から送信する前に、コンピュータとデータ入力の「ソース」(すなわち機器) 間の通信が適切であることを確認すること 2. システムで作成される規制対象の記録に、データの「ソース」(すなわち、どの機器またはコンポーネントがデータを生成したか) が明確に示されていること	部分的に 可	1. システムは、プライマリアプリケーションとサーバー間に有効な接続を継続的に確保するように設計されています。 2. OpenLab Server/ECM XT は、プライマリアプリケーションによって取得および処理された情報/記録を保存します。データを生成する機器コンポーネント (LC モジュールなど) には直接接続されず、データソースは認識しません。

5. 動作デバイスの確認 (続き)

Part 11 その他	要件	S、U	その他の規制またはコメント	可/不可	「可」の場合は具体的に要件がいか 満たされるか、または「不可」の場合、 推奨される事柄。
Part 11 11.10 (i)	5.5 電子記録/電子署名システムを開発、メンテナ ンス、または使用する者が、その者に割り当てられ た職務を遂行するための教育およびトレーニングを 受け、経験を積んでいることを証明する文書があり ますか。	U	中国 GMP 18 ブラジル 571	N/A	電子記録および電子署名システムを開発、メンテナ ンス、または使用する者が、これらの職務を遂行す るために必要な教育およびトレーニングを受け、経 験を積んでいることを証明する文書を維持するの は、ユーザーの責任です。 OpenLab Server/ECM XT の開発に携わるアジレン トのソフトウェアプロフェッショナルは、関連する データの完全性のトレーニングを受けています。
Part 11 11.10 (j)	5.6 記録および署名の偽造を阻止するために、個 人が各自で行った電子署名のもとで実施した操作 に対して説明義務と責任を負うことを明文化した ものが策定されていますか。	U		N/A	個人が各自で行った電子署名のもとで実施した 操作に対して責任を負うことを明文化した手順書 (SOP) を策定するのは、ユーザーの責任です。
	5.7 従業員は、この手順に関するトレーニングを受 けていますか。	U	Part 11 11.10 (j) の暗黙的要件	N/A	スタッフのトレーニングを実施するのは、ユーザー の責任です。
Part 11 11.10 (k)	5.8 次の内容を含んだシステム関連の文書化に関 する管理が適切に設けられていますか。 1. システムの運用およびメンテナンスに関する文 書の配布、アクセス、および使用に対する適切 な管理 2. システム関連の文書の作成および改訂を時系 列で文書化した監査証跡を維持するための改訂 および変更の管理手順	U	中国 GMP 161 第五章系統 第十一条应当有详细阐述系统的文件 (_必要时, 要有图纸), 并须及时更新。此文件应当 详细描述系统的工作原理、目的、安全措施和适用 范围、计算机运行方式的主要特征, 以及如何与其 他系统和程序相接。	N/A	1. システム関連の文書化に関する管理措置を確 立するのは、ユーザーの責任です。 2. アジレントでは、OpenLab Server/ECM XT の 開発および試験に関する文書を維持していま す。要求することでこの文書を確認することが できます。
Part 11 11.10 (i)	5.9 システム関連の文書の作成および改訂を時系 列で文書化した監査証跡を維持するための改訂お よび変更の管理手順は確立されていますか。	S、U	第五章系統 第十七条 计算机化系统的变更应当根据预定的操 作规程进行, 操作规程应当包括评估、验证、审核、 批准和实施变更等规定。计算机化系统的变更, 应 经过该部分计算机化系统相关责任人员的同意, 变 更情况应有记录。主要变更 应当经过验证。	可	アジレントでは、OpenLab Server/ECM XT の開 発および試験に関する文書を維持しています。要求 することで文書を確認することができます。 ユーザーには、それぞれが保有するシステムおよび 関連する変更に関する文書をそのままの状態でも 維持することが期待されます。

6. データの完全性、日時の正確性

Part 11 その他	要件	S、U	その他の規制またはコメント	可/不可	「可」の場合は具体的に要件がいかに満たされるか、または「不可」の場合、推奨される事柄。
Annex 11	6.1 他のシステムとデータを電子的に交換するコンピュータ化システムには、正確で安全に入力され、データが処理されるように適切なチェックが組み込まれていますか。	N/A	Annex 11.5	N/A	この文脈においては、OpenLab Server/ECM X は他のシステムとデータを交換しません。他のシステムで生成および処理されたデータを保存するだけです。OpenLab Server/ECM XT は、安全で確実なファイル転送を確保します。
Annex 11	6.2 データの正確性を確認するために追加でチェックする機能はありますか。 (このチェックは、他のオペレータまたはバリデーション済みの電子的手段で行うことができます)	U	Annex 11-6 ブラジル GMP 580 ICHQ7-5.45 第五章系統 第十五条 当人工输入关键数据时（例如在称重过程中输入物料的重量和批号），应当复核输入记录以确保其准确性。这个复核可以由另外一个操作人员完成，或采用经验证的电子方式。必要时，系统应当设置复核功能，确保数据输入的准确性和数据处理过程的正确性。	N/A	追加チェックの手順を定義し、データの精度を確保するのは、ユーザーの責任です。
臨床 コンピュータ ガイド	6.3 システムの正しい日時を維持するための管理措置は確立されていますか。	S、U	臨床コンピュータガイド D.3	可	アジレントは、システムの日時の正確性を確保するために、タイムサーバーを参照するようシステムを設定することをおすすめします。この設定と制御はオペレーティングシステムで行います。
臨床 コンピュータ ガイド	6.4 日付または時刻の変更は、権限のあるスタッフのみが行えますか。また、システムの日付または時刻のずれが検出された場合に、そのスタッフに通知されますか。	U	臨床コンピュータガイド D.3	N/A	OpenLab Server/ECM XT は Windows のローカル時間と同期するように設計されています。 次の作業は、ユーザーの責任で実施してください。 <ul style="list-style-type: none"> - Windows の時間設定へのアクセスと管理を、承認を受けた担当者に限定する。 - Windows の時間を正確に設定および維持する手順コントロールを管理する。
臨床 コンピュータ ガイド I	6.5 複数のタイムゾーンにまたがるシステムに対して、参照されているタイムゾーンが明確にわかるタイムスタンプが実装されていますか。	S、U	臨床コンピュータガイド D.3	可	すべての時刻データは、協定世界時 (UTC) /グリニッジ標準時 (GMT) でタイムスタンプが付けられ、使用コンピュータのローカル時刻で表示されます。

7. オープンシステムの管理（オープンシステムにのみ適用）

Part 11 その他	要件	S、U	その他の規制またはコメント	可/不可	「可」の場合は具体的に要件がいかに満たされるか、または「不可」の場合、推奨される事柄。
Part 11 11.30	7.1 電子記録の真正性および完全性、さらに該当する場合は機密性をその作成から受領まで確保するよう考案された手順および管理措置が設けられていますか。	N/A		N/A	OpenLab Server/ECM XT は、21 CFR Part 11.3 (b)(9) で定義される「オープン」システムとして導入することを目的としていません。
Part 11 11.30	7.2 状況に応じて必要な場合に記録の真正性、完全性、および機密性を確保するために、文書の暗号化や適切なデジタル署名規格の使用などの追加措置が講じられていますか。	N/A		N/A	OpenLab Server/ECM XT は、21 CFR Part 11.3 (b)(9) で定義される「オープン」システムとして導入することを目的としていません。

8. 電子署名 – 署名の明示および署名/記録の関連付け

Part 11 その他	要件	S、U	その他の規制またはコメント	可/不可	「可」の場合は具体的に要件がいか 満たされるか、または「不可」の場合、 推奨される事柄。
Annex 11	8.1 電子署名を使用する場合、企業の範囲内 で電子署名に手書き署名と同じ効力がありま すか。 電子署名は、該当する記録に永久的に関連付 けられていますか。 電子署名に署名日時が含まれていますか。	N/A	Annex 11.14 ICH Q7.6.18 第五章系統 第二十三条电子数据可以采用电子签名的方 式, 电子签名应当遵循相应法律法规的要求。	可	ユーザーは、電子署名の法的影響力を確立する必要が あります。 署名は、該当する記録に永久的に関連付けられています。 署名された電子記録には、署名者の氏名、署名日時、お よび署名の意味が示されます。
Part 11 11.50 (a)	8.2 署名された電子記録には、署名に関連した 情報が次に示す項目を含みますか。 1. 署名者の印字氏名 2. 署名が実行された日時 3. 署名に関連付けられた意味 (レビュー、承 認、責任、作成者など)	N/A		可	署名された電子記録には、 4. 署名者の氏名、署名日時、 5. および署名の意味が 6. 示されます。
Part 11 11.50 (b)	8.3 この項の段落 (a)(1)、(a)(2)、および (a)(3) に示した項目には、電子記録と同一の管理が 実施されますか。また、人間が判読可能な形式 の電子記録 (電子的表示や印刷物など) の一部 として含まれていますか。	N/A		部分的に 可	すべての電子署名の構成要素が人が読める形式で表示 されます。 電子署名は印刷できません。
Part 11 11.70	8.4 電子記録を改ざんする目的で署名を通常の 方法で削除、コピー、または転送できないよ うに、電子署名および手書き署名は、該当する電 子記録に関連付けられていますか。	N/A		可	システムは手書き署名に対応しておらず、ユーザーが手 順において管理する必要があります。 電子署名は電子記録に埋め込まれているため、変更、上 書き、削除はできません。
Part 11 序文	8.5 一定期間にわたって入力や操作がまったく 行われなかった場合にユーザーを「ログアウト」 する自動ログアウト機能が設けられていますか。	U	Part 11 序文 セクション 124	可	セッションの自動ロックにより、ユーザーを自動的にログ アウトするまでの時間を設定できます。

9. 電子署名の一般要件と署名の構成要素および管理

Part 11 その他	要件	S、U	その他の規制またはコメント	可/不可	「可」の場合は具体的に要件がいか 満たされるか、または「不可」の場合、 推奨される事柄。
Part 11 11.100 (a)	9.1 電子署名はそれぞれ一個人に一意のも ので、他人が再使用したり、他人に再割り当てさ れることはありませんか。	N/A		可	システムでは、重複したユーザー ID を使用することはで きません。 各ユーザーは、他のユーザーが使用できない一意のログ イン、すなわち一意の署名を持ちます。
Part 11 11.100 (b)	9.2 組織は、個人の電子署名または電子署名の 構成要素を設定、割り当て、認証、あるいは認 可する場合、事前にその個人の本人確認を行っ ていますか。	N/A		N/A	個人の電子署名または電子署名の要素を設定、割り当 て、認証、あるいは認可する前に、その個人の本人確認 を行うのは、ユーザーの責任です。

9. 電子署名の一般要件と署名の構成要素および管理(続き)

Part 11 その他	要件	S、U	その他の規制またはコメント	可/不可	「可」の場合は具体的に要件がいかに満たされるか、または「不可」の場合、推奨される事柄。
Part 11 11.100 (c)	9.3 電子署名を使用する者は、その使用前または使用時に、1997年8月20日以降に使用されているシステム内の電子署名が従来の手書き署名と同等の法的拘束力を持つよう意図されたものであることをFDAに対して証明していますか。 9.4 電子署名を使用する者は、FDAの要請に応じて、特定の電子署名が署名者の手書き署名と同等の法的拘束力を持つことを示す証明書または宣誓書を追加で提出していますか。	N/A		N/A	電子署名を使用する個人がこれらの要件を満たしていることを確認するのは、ユーザーの責任です。
Part 11 11.200 (a) (1)	9.5 バイオメトリックスによらない電子署名では、識別コードとパスワードなど、少なくとも2つの識別構成要素が使用されていますか。	N/A		可	電子署名を行うには、識別コード（ユーザー ID）とパスワードの両方が必要です。
Part 11 11.200 (a) (1) (i)	9.6 制御されたシステムのアクセスの連続的な期間内にユーザーが一連の署名を行わない場合、それぞれの署名の実行にはすべての電子署名コンポーネントが必要ですか。	N/A		可	最初の電子署名を行うには、識別コード（ユーザー ID）とパスワードの両方が必要です。
Part 11 11.200 (a) (1) (i)	9.7 制御されたシステムのアクセスの連続的な期間中にユーザーが一連の署名を実行する場合、次に続けて行う署名には、そのユーザーにのみ実行され、そのユーザーが使用するよう設計された1つ以上の電子署名コンポーネントを使用して実行されますか。	N/A		可	ユーザーがパスワードを共有していないことを確保するのは、ユーザーの責任です。
Part 11 11.200 (a) (1) (ii)	9.8 制御されたシステムのアクセスの連続的な期間内にユーザーが一連の署名を行わない場合、それぞれの署名の実行にはすべての電子署名コンポーネントが必要ですか。	N/A		可	制御されたシステムのアクセスの連続的な期間中に署名が実行されない場合、電子署名を行うには、識別コード（ユーザー ID）とパスワードの両方が必要です。
Part 11 11.200 (a) (2)	9.9 バイオメトリックスによらない電子署名が所有者本人のみによって使用されるようにするための管理措置が実施されていますか。	N/A		N/A	指定した個人のみユーザー名とパスワードが知られており、ユーザー名とパスワードにより個々のユーザーにまで追跡可能であることを確保するのは、ユーザーの責任です。
Part 11 11.200 (a) (3)	9.10 2名以上の協力が無い限り、個人の電子署名の使用を所有者本人以外の者が試みることができないように、電子署名が管理され、運用されていますか。	N/A		可	所有者本人以外の者が電子署名を不正利用するためには、ユーザーとシステム管理者による意図的な協力が必要となります。
Part 11 11.200 (b)	9.11 バイオメトリックスにもとづく電子署名は、所有者本人以外の者が使用できないように設計されていますか。	N/A		N/A	OpenLab Server/ECM XT で、バイオメトリックス認証はサポートされていません。

10. 識別コードとパスワードの管理

Part 11 その他	要件	S、U	その他の規制またはコメント	可/不可	「可」の場合は具体的に要件がいか 満たされるか、または「不可」の場合、 推奨される事柄。
Part 11 11.300 (a)	10.1 2名の者が同一の識別コードとパスワードの組み合わせを持つことがないよう、識別コードとパスワードの各組み合わせの一意性を維持するための管理措置が実施されていますか。	S、U		可	OpenLab Server/ECM XT では、重複したユーザー ID を使用することはできません。
Part 11 11.300 (b)	10.2 (例えば、同一パスワードの長期使用などの事象に対する対策として) 識別コードおよびパスワードの発行が定期的にチェック、取り消し、または変更されるようにするための管理措置が実施されていますか。	S、U		可	パスワードの有効期限は、Windows ドメインまたはアプリケーションで Windows ローカルに設定することができます。 ユーザーは、文書化されたリスク評価にもとづいてパスワードの有効期限を設定しなければなりません。
Part 11 11.300 (c)	10.3 識別コードまたはパスワードを保持または生成するトークン、カード、およびその他のデバイスが遺失、盗難、または紛失したり、その情報が漏洩した可能性がある場合に、これらのデバイスを電子的に無効にし、適切かつ厳格な管理に従って一時的または永久的な代替品を発行するための手順が設けられていますか。	U	第五章系統 第十四条数据的输入或修改只能由经许可的人员进行。杜绝未经许可的人员输入数据的手段有：使用钥匙、密码卡、个人密码和限制对计算机终端的访问。应当就输入和修改数据制订一个授权、取消、授权变更，以及改变个人密码的规程。必要时，应当考虑系统能记录未经许可的人员试图访问系统的行为。对于系统自身缺陷，无法实现人员控制的，必须具有书面程序，相关记录本及相关物理隔离手段，保证只有经许可的人员方能进行操作。	N/A	これらの手順を確立するのは、ユーザーの責任です。
Part 11 11.300 (d)	10.4 パスワードまたは識別コード、あるいはその両方の不正使用を防止し、システムを不正に使用しようとする行為を検出してシステムセキュリティ部門と、必要であれば組織の経営陣に直ちに緊急報告するための保護措置は設けられていますか。	U	第五章系統 第十四条数据的输入或修改只能由经许可的人员进行。杜绝未经许可的人员输入数据的手段有：使用钥匙、密码卡、个人密码和限制对计算机终端的访问。应当就输入和修改数据制订一个授权、取消、授权变更，以及改变个人密码的规程。必要时，应当考虑系统能记录未经许可的人员试图访问系统的行为。对于系统自身缺陷，无法实现人员控制的，必须具有书面程序，相关记录本及相关物理隔离手段，保证只有经许可的人员方能进行操作。	N/A	これらの保護措置を確立するのは、ユーザーの責任です。
Part 11 11.300 (e)	10.5 識別コードまたはパスワード情報を保持または生成するトークンやカードなどのデバイスが正常に機能し、不正に改変されていないことを確認するために、これらのデバイスを導入時および以後定期的にテストするための管理措置は設けられていますか。	U		N/A	これらのデバイスが正常に機能し、不正に改変されていないことを確認するために、デバイスを導入時および導入以降定期的にテストするための管理措置を確立するのは、ユーザーの責任です。

11. システムの開発とサポート

Part 11 その他	要件	S、U	その他の規制またはコメント	可/不可	「可」の場合は具体的に要件がいか 満たされるか、または「不可」の場合、 推奨される事柄。
Annex 11	11.1 ソフトウェアまたはシステムは、適切な品質管理システムに従って開発されましたか。	S、U	Annex 11 4.5 ブラジル GMP 577 GAMP これは、システム供給元とユーザーがともに責任を負う要件です。ユーザーは、ソフトウェアが品質管理システム (QMS) の枠組みに従って開発されていることを証明する文書を提出するよう供給元に請求する必要があります。 第二章原則 企业应当能够提供与供应商质量体系 and 审计信息相关的文件。	可	OpenLab Server/ECM XT は、ISO 9001 品質管理基準に従って開発されています (「LSCA Quality Manual (LSCA 品質マニュアル)」のセクション 2.2 をご覧ください)。
ブラジル	11.2 ソフトウェア供給元がソフトウェアおよび保守サービスを下請けに出している場合に、正式な契約が存在しますか。その契約には、請負業者の責任が規定されていますか。	S、U	ブラジル GMP 589 第二章原則 第四条企业应当注重计算机化系统供应商的管理, 制定相应的操作规程。供应商提供产品或服务时 (如安装、配置、集成、验证、维护、数据处理等), 企业应当与供应商签订正式协议, 明确双方责任。	可	アジレントは、すべてのサプライヤとの間で正式な契約を締結するよう義務付けています (「LSCA Quality Manual (LSCA 品質マニュアル)」のセクション 7.4 をご覧ください)。
ICH Q10	11.3 外部委託された (開発およびサポート) 業務について、委託側と受託側との間に書面による契約が存在しますか。	S、U	ICHQ10、2.7 c	可	アジレントは、すべてのサプライヤとの間で正式な契約を締結するよう義務付けています (「LSCA Quality Manual (LSCA 品質マニュアル)」のセクション 7.4 をご覧ください)。
ICH Q10	11.4 関連する関係者 (請負業者) の品質に関連する業務の責任およびコミュニケーションプロセスが定義されていますか。	S、U	ICHQ10、2.7 c	可	アジレントは、すべてのサプライヤとの間で正式な契約を締結するよう義務付けています (「LSCA Quality Manual (LSCA 品質マニュアル)」のセクション 7.4 をご覧ください)。
Part 11 11.10 (i)	11.5 ソフトウェアを開発およびサポートするスタッフはトレーニングを受けていますか。	S、U	第三章人員 第五条计算机化系统的“生命周期”中所涉及的各种活动, 如验证、维护、管理等, 需要各相关的职能部门人员之间的紧密合作。在职责中涉及使用和管理计算机化系统的人员, 应当接受相应的使用和管理培训。确保有适当的专业人员, 对计算机化系统的设计、验证、安装和运行等方面进行培训和指导。	可	アジレントのすべてのスタッフは、トレーニングを受けることが義務付けられています (「LSCA Quality Manual (LSCA 品質マニュアル)」のセクション 6.0 をご覧ください)。

参考文献

1. R. A. Botha and J. H. P. Eloff. Separation of duties for access control enforcement in workflow environments. IBM Systems Journal—End-to-end security. 40 (3), 666-682. (2001).
2. U.S. Food and Drug Administration. CFR - Code of Federal Regulations Title 21. Title 21—Food and Drugs, Chapter I—Food and Drug Administration Department of Health and Human Services, Subchapter A—
3. European Commission Health and Consumers Directorate-General. Public Health and Risk Assessment. Pharmaceuticals. EudraLex. The Rules Governing Medicinal Products in the European Union.
4. Good Manufacturing Practice. Medicinal Products for Human and Veterinary Use. Annex 11. Computerized Systems. [Online] http://ec.europa.eu/health/files/eudralex/vol-4/annex11_01-2011_en.pdf (accessed November 2, 2020)
5. “Agilent OpenLab Server and OpenLab ECM XT Administration Guide”

ホームページ

www.agilent.com/chem/jp

カスタマコンタクトセンター

0120-477-111

email_japan@agilent.com

本製品は一般的な実験用途での使用を想定しており、
医薬品医療機器等法に基づく登録を行っていません。
本文書に記載の情報、説明、製品仕様等は予告なしに
変更されることがあります。

アジレント・テクノロジー株式会社
© Agilent Technologies, Inc. 2021
Printed in Japan, April 13, 2021
5994-3228JAJP
DE44298.6300115741