

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

OpenLab CDS バージョン 2.8 に対応

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、Agilent OpenLab CDS システムのユーザーを対象としています。OpenLab CDS では、LC、GC、シングル四重極 LC/MS および GC/MS、A/D データの取り込みおよび解析などの処理が行われます。一方、ユーザーは、OpenLab CDS の機能を適切に使用し、規制に準拠した操作によってラボのデータの取り込みおよび解析などの処理を行う責任を負います。ユーザーは、OpenLab CDS で提供される技術的管理に加え、関連する手順管理、すなわち標準操作手順書（SOP）を策定する必要があります。例えば、内部監査プログラムなどの管理を確立し、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 の各項および EU Annex 11 の関連条項の要件を満たすうえで役立つ OpenLab CDS 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。

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

セキュリティは、「適切な者が適切な情報に対して適切なアクセス権を持つこと」と言い換えることができます。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、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、また場合によっては他のデータセットへ別のアクセス権を持つように定義する必要があります。

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。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、そのスタッフが行っ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、または削除する特定の操作を行った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操作前後の値を含みます。
- 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、通常、理由はあらかじめ定義されたリストから選択します。

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、使用する場合は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、署名の意味または理由（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に表記されること

「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。」

– Botha, Eloff, IBM Systems Journal¹

付録 1：OpenLab CDS 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 また、Part 11 の各条項の後に、それに関連する EU Annex 11³ などの要件を示します。

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 Part 11 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

一部の要件には、技術的管理と手順管理の両方が関連しています。3 列目には、各要件の責任の所在を示します。「S」は分析システムの供給元を表し、「U」はユーザーを表します。ユーザーが単独で満たす必要がある要件は、青色で示します。青色は、ユーザーが実施する責任のある技術的管理を示している場合もあります。

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 CDS 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。クロマトデータシステムに該当しない要件は「N/A」とします。

6 列目

6 列目では、OpenLab CDS 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 およびその他	要件	S、U	関連するその他の規制およびコメント	可/不可	「可」の場合、具体的に OpenLab CDS により要件がいか に満たされるか。 「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、例えば開発段階のバリデーションや関連する文書化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により、OpenLab CDS の性能を幅広く検証しています。ただし、ユーザーは、それぞれが保有する分析システムを規制要件に従って検証する必要があります。 Agilent OpenLab CDS に関連する「規制対象の記録」は次のとおりです。 - 機器の調整/パラメータ - 取り込みメソッド - 取り込まれたデータ - 分析メソッド - 分析結果 - レポートテンプレート - シーケンスプレート - 実行されたシーケンス - 関連付けられた監査証跡/電子署名 OpenLab CDS では、これらの記録に対してチェックサムを実行することにより、「無効な記録や変更された記録」が検出されます。このような記録が検出された場合、エラーが表示され、ユーザーはファイルを開くことができません。
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 およびその他	要件	S、U	関連するその他の規制およびコメント	可/不可	「可」の場合、具体的に OpenLab CDS により要件がいか に満たされるか。 「不可」の場合、顧客に推奨される事柄
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	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	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 数据应当储存在另一个单独的、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。 すべての関連ファイルに対し、適切に計画されたバックア ップを作成するための詳細な指示書があります。 ^{5, 6}
UTCPart 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	OpenLab CDS によって保護されるデータ（機器の調整パラ メータ、取り込みメソッド、取り込んだデータ、分析メソッド、 分析結果、レポートテンプレート、シーケステンプレート、 実行したシーケンスなどの記録を含む）は、ECM XT などの アジレントのデータ管理システム内に保管され、監督され ます。取り込み直後、および各インタラクティブレビューまたは 自動処理後に、OpenLab CDS はすべての生データ、メタ データ、結果データを自動的にアーカイブします。 ファイルに関連するすべての操作（削除を含む）は、アジレ ントのデータ管理システムの監査証跡/ログによってモニタリ ングされます。これらの記録はアジレントのデータ管理シス テム内に安全に保管され、レビュー時にデータ管理システム から取得されます。 物理的なセキュリティを管理し、アジレントのデータ管理シ ステムへのアクセスを制限するのは、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。
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、旧バージョンの OpenLab CDS 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。バリエーシ 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 およびその他	要件	S、U	関連するその他の規制およびコメント	可/不可	「可」の場合、具体的に OpenLab CDS により要件がいか に満たされるか。 「不可」の場合、顧客に推奨される事柄
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	システムで生成されるすべての生データ、メタデータ、およ び結果データは、保護された場所に保存されます。物理的 セキュリティを確保するのは、ユーザーの責任です。
Annex 11	2.8 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	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 ワークステーションおよびオールインワンサーバー用のユー ティリティや、すべてのトポロジ（マルチサーバ設定を含む） 用の文書化された手順と手動による手順を提供します。 詳細については、Agilent OpenLab Server および OpenLab ECM XT 管理者ガイドをご覧ください。 ⁵
Annex 11	2.9 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定期的にチェック、 検証、および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。 単一サーバーおよび 2 台サーバーポートロジの場合、バック アップおよび復元ユーティリティは、復元されたデータの履 歴に関する詳細な文書を提供し、復元されたデータの整合 性チェックを文書化します。 詳細については、Agilent OpenLab Server および OpenLab ECM XT 管理者ガイドをご覧ください。 ⁵

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 およびその他	要件	S、U	関連するその他の規制およびコメント	可/不可	「可」の場合、具体的に OpenLab CDS により要件がいか に満たされるか。 「不可」の場合、顧客に推奨される事柄
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	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。
	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。

4. 電子監査証跡

Part 11 およびその他	要件	S、U	関連するその他の規制およびコメント	可/不可	「可」の場合、具体的に OpenLab CDS により要件がいか に満たされるか。 「不可」の場合、顧客に推奨される事柄
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	ユーザーによるすべての操作は、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に記録されます。監査証跡は、すべての結果データ、メソッド、およびシーケンスに対して作成されます。
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 CFR 58.130 e	可	監査証跡には、ユーザー ID、変更日時、および変更前後の値と、変更が行われた理由が含まれます。
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	Annex 11、8.2	可	監査証跡ウィンドウから、記録の監査証跡を印刷できます。
FDA GMP	4.4 監査証跡には、試験で採用された、既存のメソッドに対する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	メソッドについては、メソッドに対するすべての変更理由を含む完全な監査証跡が記録されます。
	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	プロジェクトに対して有効になった監査証跡は、いかなるユーザーも無効に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	監査証跡は、手元のクライアント PC から査察官がアクセスできるよう設定し、容易に利用できます。 監査証跡を見る人は、どの監査証跡エントリがレビューされたかを示すことができます。
	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。	S	監査証跡のレビューに関連する多くの警告書による Annex 11 の暗黙的要件	可	OpenLab CDS では、ユーザーが監査証跡のレビュー作業を行いやすいように、内容の表示前に監査証跡をフィルタリングできます。
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	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。解析またはレポート作成のために結果を選択するときは、使用する結果のバージョンをユーザーが（ユーザーの権限にもとづいて）選択できます。
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	監査証跡情報は電子記録内に保存され、電子記録から切り離すことはできません。
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	監査証跡は、審査および印刷が可能です。
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	監査証跡は、審査および印刷が可能です。

5.動作およびデバイスの確認

Part 11 およびその他	要件	S, U	関連するその他の規制およびコメント	可/不可	「可」の場合、具体的に OpenLab CDS により要件がいか に満たされるか。 「不可」の場合、顧客に推奨される事柄
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		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、記録の改変、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	システムでは、システムアクセスを細かく制御するための ユーザーの権限がサポートされています。アクセスは、特定 ユーザーが特定のデータセットに対して特定のアクセス権を 持ち、また他のデータセットに対して別のアクセス権を持つ ように分離し、定義することができます。
	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	システムで操作を行うオペレータは、監査証跡およびアク ティビティログの両方に記録されます。
Part 11 11.10 (h)	5.4 システムでは、適宜、データ入力または操 作の妥当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	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 であるかを確認すること 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、サポート対象のアジレント機器とワークス テーション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。すべてのサポート対象機器のリストに ついては、 OpenLab CDS で制御可能な分析機器 ペー ジをご覧ください。 2. システムは、データの収集に使用された機器を示します。
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 明する文書を管理するのは、ユーザーの責任です。 OpenLab CDS 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。 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。（Part 11 11.10 (j) の暗 黙的要件）	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）とトレーニング を策定するのは、ユーザーの責任です。

5.動作およびデバイスの確認（続き）

Part 11 およびその他	要件	S、U	関連するその他の規制およびコメント	可/不可	「可」の場合、具体的に OpenLab CDS により要件がいか に満たされるか。 「不可」の場合、顧客に推奨される事柄
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 第五章系统 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。 第五章系统 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 CDS の開発および試験に関 する文書を維持しています。ユーザーは、要求すること でこの文書を確認することができます。

6.データインテグリティ、日時の正確性

Part 11 およびその他	要件	S、U	関連するその他の規制およびコメント	可/不可	「可」の場合、具体的に OpenLab CDS により要件がいか に満たされるか。 「不可」の場合、顧客に推奨される事柄
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。	S	Annex 11.5	N/A	この文脈においては、OpenLab CDS は他のシステムとデー タを交換しません。
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、 他のオペレータが行う、または検証済みの電子 的手段で行うことができます。	S、U	Annex 11-6 ブラジル GMP 580 ICHQ7-5.45 第五章系统 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。	可	OpenLab CDS では、電子署名ワークフローを使用したマ ルチユーザーによるレビューと承認が可能です。

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 およびその他	要件	S、U	関連するその他の規制およびコメント	可/不可	「可」の場合、具体的に OpenLab CDS により要件がいか に満たされるか。 「不可」の場合、顧客に推奨される事柄
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。	S、U		N/A	OpenLab CDS 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。	S		N/A	OpenLab CDS 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 およびその他	要件	S、U	関連するその他の規制およびコメント	可/不可	「可」の場合、具体的に OpenLab CDS により要件がいか に満たされるか。 「不可」の場合、顧客に推奨される事柄
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では同じ影響力があり 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。	S、U	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、電子署名の法的効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が行われた日時が含まれてい ます。
Part 11 11.50 (a)	8.2 署名された電子記録には、次のすべての項 目を明確に示す署名の関連情報が含まれます 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）	S		可	署名された電子記録には、 1. 署名者の氏名、署名日時、 2. および署名の意味が 3. 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。	S		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、印刷することができます。
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。	S		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おり、変更したり、上 書きしたり、削除したりすることはできません。
Part 11 序文	8.5 一定期間の間に入力および操作がまったく 行われなかった場合、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。	S	Part 11 序文 第 124 項	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 およびその他	要件	S、U	関連するその他の規制およびコメント	可/不可	「可」の場合、具体的に OpenLab CDS により要件がいか に満たされるか。 「不可」の場合、顧客に推奨される事柄
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。	S、U		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。	U		N/A	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 およびその他	要件	S、U	関連するその他の規制およびコメント	可/不可	「可」の場合、具体的に OpenLab CDS により要件がいか に満たされるか。 「不可」の場合、顧客に推奨される事柄
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。	U		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。	S、U		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。	S		可	すべての電子署名には、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に設計された 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。	S		可	すべての電子署名には、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) (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。	S		可	すべての電子署名には、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。	S		N/A	指定した個人以外にユーザー名とパスワードが知られておらず、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。	S、U		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。	S		N/A	OpenLab CDS では、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 およびその他	要件	S、U	関連するその他の規制およびコメント	可/不可	「可」の場合、具体的に OpenLab CDS により要件がいか に満たされるか。 「不可」の場合、顧客に推奨される事柄
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 CDS 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 時および導入以降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 およびその他	要件	S、U	関連するその他の規制およびコメント	可/不可	「可」の場合、具体的に OpenLab CDS により要件がいか に満たされるか。 「不可」の場合、顧客に推奨される事柄
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管理体系和审计信息相关的文件。	可	OpenLab CDS 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、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 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。供給元は、下請業者との間でこのような契約を締結する必要があり、ユーザーは、契約が締結されていることを確認する必要があります。 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の責任を定義しています（「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	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。サプライヤは、スタッフにトレーニングを受けさせる必要があり、ユーザーは、例えばソフトウェア開発者がトレーニングを受け、このトレーニングが文書化されていることを監査することにより、それを確認する必要があります。 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— General. Part 11 Electronic Records; Electronics Signatures [オンライン] <https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=11>.
3. European Commission Health and Consumers Directorate-General.
Public Health and Risk Assessment. Pharmaceuticals. EudraLex. The Rules Governing Medicinal Products in the European Union. Volume 4. Good Manufacturing Practice. Medicinal Products for Human and Veterinary Use. Annex 11. Computerised Systems. [オンライン] https://ec.europa.eu/health/sites/default/files/files/eudralex/vol-4/annex11_01-2011_en.pdf.
4. OpenLab CDS ワークステーション Plus (コンテンツ管理機能搭載) インストールおよび構成ガイド
5. Agilent OpenLab サーバーおよび OpenLab ECM XT 管理ガイド
6. Agilent OpenLab CDS データ取り込みフェールオーバーユーザーガイド (OpenLab CDS インストールメディアに収録)。

ホームページ

www.agilent.com/chem/jp

カスタム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おりません。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。

DE53585146

アジレント・テクノロジー株式会社
© Agilent Technologies, Inc. 2024
Printed in Japan, May 6, 2024
5994-3659JAJP