

# 21 CFR Part 11 および Annex 11 コンプライアンスのサポート： Agilent Cary 3500 用 Cary UV ワークステーションソフトウェア

## 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、Agilent Cary UV ワークステーションと OpenLab ソフトウェア (コントロールパネルおよびコンテンツ管理アプリケーションを含む) を連携させて使用するユーザーを対象としています。Cary UV ワークステーションソフトウェアでは、Cary 3500 UV-Vis 分光光度計の機器コントロールおよびデータ解析機能が提供されます。一方、ユーザーは、このソフトウェアパッケージの機能を適切に使用して、ラボにおけるデータの取り込みおよび解析を規制に準拠した操作によって行う責任を負います。ソフトウェアで提供される技術的管理に加え、ユーザーには、関連する非技術的要件を満たすために、手順管理、すなわち標準操作手順書 (SOP) を策定することが求められます。例えば、システムオペレータに SOP に従わせ、また従っていることを確認するために、内部監査プログラムなどの管理措置を確立する必要があります。

本書の付録 1 では、21 CFR Part 11 の各条項および EU Annex 11 の関連条項の要件を満たすうえで役立つ Cary UV ワークステーションソフトウェア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。規制対象の組織は、システムユーザーの本人確認を行い、かつトレーニング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))。ラボのスタッフが担う責任は職務によってさまざまであることから、データアクセスを分割し、特定のユーザーが特定のデータセットに対して特定タイプのアクセス権を持ち、場合によっては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定義する必要があります。

「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。」

Botha, Eloff, IBM Systems Journal [1]

### 作業の責任の所在の明確化

作業の責任の所在の明確化とは、実行された作業について「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、また監査証跡エントリの検索や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されます。

### 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

### システムトポロジー

アジレントは、OpenLab でのデータの保存場所について、Cary UV ワークステーションの 2 つの構成を用意しています。

- データを、Cary 3500 に接続された PC のローカルに保存・管理します
- データを、OpenLab オプションの 1 つで一元的に保存・管理します

詳細については、Cary UV ワークステーションおよび OpenLab Server または ECM 3.6 ソフトウェア、システムトポロジー、アーキテクチャコンセプトを参照してください。

## 付録 1：Agilent Cary UV ワークステーションによる、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 の表に関する注記

#### 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。また、Part 11 の各条項の後に、それに関連する EU Annex 11 [3] 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、すなわちソフトウェア供給元により提供される管理機能です。また、手順管理とは、ユーザーの責任において実施する必要のある管理措置です。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のある要件は、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のある要件は、青色で示します。青字は、ユーザーに実施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、Cary UV ワークステーション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。このソフトウェアに該当しない要件は「N/A」とします。

### 6 列目

6 列目では、Cary UV ワークステーションソフトウェアの技術的管理（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 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」の場合は具体的に要件がいかに満たされるか、「不可」の場合はユーザーに推奨される事柄
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	<p>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。バリデーションの最終的な責任はユーザーにあります。例えばソフトウェアの開発および関連する文書化の過程で行われるバリデーションなど、一部の作業はソフトウェア供給元のみが実施でき、ソフトウェア供給元が提供する必要があります。</p> <p>第五章系統</p> <p>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。</p> <p>第五章系統</p> <p>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。</p>	可	<p>アジレント・テクノロジーは、幅広いバリデーションによって Cary UV ワークステーションの性能を確認しており、ソフトウェアにはソフトウェア品質宣言書が付属しています。この宣言書は、精度、信頼性、および性能一貫性の評価テストによって用途に対するコンピュータシステムのバリデーションを行う規制上の責任からユーザーを解放するものではありません。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。</p> <p>Cary UV ワークステーションに関連する「規制対象の記録」は次のとおりです。</p> <ul style="list-style-type: none"> <li>メソッド</li> <li>バッチ結果ファイル</li> <li>関連する監査証跡</li> <li>電子署名</li> <li>メソッドおよび結果レポート</li> </ul> <p>Cary UV ワークステーションは、無効なファイルや変更されたファイルを検出することができ、これらのファイルはユーザーが開けないようになります。</p>
Annex 11	1.2 インフラストラクチャは適格ですか。	U	Annex 11.Principle B ブラジル GMP 577	—	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 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」の場合は具体的に要件がいかに満たされるか、「不可」の場合はユーザーに推奨される事柄
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。電子記録、データ、メソッド、監査証跡、オペレータの身元、および電子署名を含む結果ファイルは、Cary UV ワークステーションソフトウェアを使用して、FDA によるレビューまたは査察用のオリジナルデータのコピーとしていつでも読み込むことができます。「印刷された」レポートは元の電子ファイルにトレース可能です。これらのレポートには、レポートの作成日時、レポートを作成したユーザーおよびソフトウェアバージョン、ページ番号が表記されます。
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	電子記録を表す出力は、紙に印刷できる他、PDF ファイルとして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、およびメンテナンスプロセスが適切に実施されるようにす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	データのバックアッププロセスおよびそのデータのメンテナンスは、ユーザーの責任です。Cary UV ワークステーションは、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。 詳細な手順とバックアップスクリプトを使用して、すべての関連ファイルの適切なスケジュール済みバックアップを作成できます。 詳細については、Cary UV ワークステーションインストール手順書を参照してください。
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	記録の保存期間は、ユーザーの手順と規制要件に基づいて決定されています。ただし、Cary UV ワークステーション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、安全なデータベースに保存されます。 電子レポートおよびエクスポートされたデータは、OpenLab コンテンツ管理に安全に保存されます。 物理的なセキュリティ (ワークステーションおよびサーバーへの物理的アクセス管理) を確保するのは、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	ー	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、そのデータを検索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	システムに関連する変更は、ISO 9001 品質管理基準に従って開発およびテストされています。ただし、実装およびバリデーションプロセス中にデータの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 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」の場合は具体的に要件がいかに満たされるか、「不可」の場合はユーザーに推奨される事柄
Annex 11	2.7 データは物理的および電子的手段の両方で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  第十条系統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。
臨床ガイド	2.8 研究データおよび研究およびラボのテスト結果のレビュー用に電子形式のソース/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	可	必要に応じてラボのテスト結果を再構成できるように、すべての生データ、結果、ログ、および関連する監査証跡は安全なストレージで維持されます。
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	—	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	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。
Annex 11	2.11 バックアップデータが完全かつ正確で、データを復元する機能のチェック、バリデーション、およびモニタリングが定期的に行われていますか。	U	Annex 11.7.2 中国 GMP 163 ブラジル GMP 585 Part 211、68 b	—	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せずに外部ソフトウェアアプリケーションから行われるデータの改変、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	アプリケーションで生成された電子記録は、他のソフトウェアアプリケーションからアクセスできない保護された形式で保存されます。他のアプリケーションからこのような記録を改変しようとした場合、記録を読み取ろうとした時点で、その行為がシステムにより検出されます。
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上の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および検出し、その影響を低減するための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 F	可	アジレントは、Cary UV ワークステーションおよび OpenLab ソフトウェア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インストールするのは、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 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」の場合は具体的に要件がいかに満たされるか、「不可」の場合はユーザーに推奨される事柄
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	システムにより、システム管理者が明示的に追加したユーザーのみが利用できるようにアクセスが制限されています。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	システムへの適切なアクセス権を付与するのは、ユーザーの責任です。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 コントロールパネルにより、氏名、説明/役職、アクセス権限などのユーザーの詳細が記録されます。アクセス権限は OpenLab コントロールパネルで設定し、すべての変更はアクティビティログに記録されます。プロジェクト、役割と権限、システム、ユーザーおよびグループの役割の割り当てに関するレポートを作成することもできます。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。ユーザーまたはユーザーグループの役割と権限は、Cary UV ワークステーションアプリケーション内のログオンユーザーに対して有効です。

### 4. 電子監査証跡

Part 11 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」の場合は具体的に要件がいかに満たされるか、「不可」の場合はユーザーに推奨される事柄
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る、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、すべてのメソッドおよび結果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 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	監査証跡には、オペレータ、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	Cary UV ワークステーションのデータが変更されると、元のファイルが変更されたこと、その日時、およびオペレータを文書化したエントリが監査証跡に作成されます。監査証跡は、表示、電子形式でレビュー、および印刷することができます。 監査証跡レポートは、PDF ファイルとして作成し、OpenLab コンテンツ管理に安全に保存できます。

## 4. 電子監査証跡(続き)

Part 11 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」の場合は具体的に要件がいかに満たされるか、「不可」の場合はユーザーに推奨される事柄
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	監査証跡はコンピュータで生成され、常に有効です。関連するアプリケーションデータファイルとともに自動的に保存されます。
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、人間が判読して理解できる形式で設計されています。 該当するユーザーは、アプリケーションビューアでいつでも監査証跡を表示できます。 システムは、権限のあるユーザーが監査証跡エントリを電子形式でレビューするように設計されており、レビューされたエントリは電子記録として恒久的に保存されます。
	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 Annex 11 および多くの警告書の暗黙的要件	可	監査証跡の内容は、ユーザーが設定したり編集したりすることはできません。監査証跡は、ユーザーまたはエントリカテゴリでフィルタリングできます。監査証跡でエントリの各レビューを検索することもできます。OpenLab コントロールパネルでは、ユーザーが情報のレビュー作業を行いやすいように、内容の表示前にシステムの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	以前に記録されたエントリは、上書きすることも変更することもできません。これらのエントリは、記録が変更された際でも恒久的に監査証跡に記録されます。 以前記録された情報は、その電子記録に関連付けられた一意のファイル名で保存されます。
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	監査証跡は、関連する電子記録とともに自動的に保存され、その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 電子形式で保存されている電子記録（電子監査証跡など）は、印刷された明確なコピーが得られますか。	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 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」の場合は具体的に要件がいかに満たされるか、「不可」の場合はユーザーに推奨される事柄
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		可	<p>一定の順序を必要とするイベントについては、システムチェックによってその順序が確保されます。</p> <p>ユーザーアクセスを、保存されている承認済みメソッドに制限するか、ファイルに電子署名して以降の変更を防ぐことにより、QA/QC で必ず承認済みメソッドが使用されるようにできます。</p> <p>Cary UV ワークステーションでは、電子記録に関連してイベントの順序が適用されます。例えば、ソフトウェアは、必要な設定および設備が整ってから、データの収集および分析を許可します。また、アプリケーションを終了する前にファイルが保存されるようにします。</p>
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	アプリケーションおよび記録へのアクセスは、割り当てられた権限に基づいて制御および制限されますが、これを設定できるのは権限のあるユーザーまたは管理者ユーザーです。
	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の身元は、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、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	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。 指示を「ソース」(すなわち機器) へ、または「ソース」からデータを送信する前に、コンピュータとデータ入力「ソース」間の通信が適切であることを確認すること 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	可	<p>1. システムは、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。</p> <p>2. システムは、機器モデルとシリアル番号を認識し、これらの情報をデータソースとして監査証跡に記録します。</p> <p>注：コンピュータワークステーションは、前述のサポートされているトポロジセクションで定義されます</p>
Part 11 11.10(j)	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	—	<p>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。</p> <p>Cary UV ワークステーションに携わるアジレントの従業員は、それに関連するデータインテグリティのトレーニングを受けています。</p>
	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	—	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。



## 5. 動作およびデバイスの確認(続き)

Part 11 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」の場合は具体的に要件がいかに満たされるか、「不可」の場合はユーザーに推奨される事柄
Part 11 11.10 (k)	5.8 次のものを含む、システム関連文書に関する適切な管理措置が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) システム関連文書の作成および改訂が時系列で文書化され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。	—	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。
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	アジレントは、Cary UV ワークステーションおよび OpenLab ソリューションの開発およびテスト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。  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に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 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」の場合は具体的に要件がいかに満たされるか、「不可」の場合はユーザーに推奨される事柄
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	—	このような機能はシステムに実装されていません。
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がありますか。  (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)	S、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。	—	このような機能はシステムに実装されていません。
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。

## 6. データの完全性、日時の正確性 (続き)

Part 11 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」の場合は具体的に要件がいかに満たされるか、「不可」の場合はユーザーに推奨される事柄
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。	S、U	臨床コンピュータガイド D.3	可	Cary UV ワークステーションではオペレーティングシステムを使用して、Windows のローカル時刻と同期します。  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"> <li>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。</li> <li>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。</li> </ul>
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	タイムスタンプは常に UTC 形式で表示されます。

## 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 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」の場合は具体的に要件がいかに満たされるか、「不可」の場合はユーザーに推奨される事柄
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		—	システムは、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		—	システムは、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 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」の場合は具体的に要件がいかに満たされるか、「不可」の場合はユーザーに推奨される事柄
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。	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、最終的なレポートに含めることができます。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) 署名が行われた日時 (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	アプリケーションで作成されるレポートには、次の情報が示されます。 1) 署名者の氏名と署名レベル 2) 署名が行われた日時 3) 署名の理由を示すために強制的に入力されたコメント
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表示され、印刷されます。
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	電子署名は結果およびメソッドファイルに埋め込まれ、レコード間またはファイル間で転送することはできません。
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。	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 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」の場合は具体的に要件がいかに満たされるか、 「不可」の場合はユーザーに推奨される事柄
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。システム内ではユーザー名を一意にする必要があり、別の個人に再割り当てすることはできません。  ユーザーが企業の Windows ログインを使用してユーザーを認証している場合、2 人のユーザーが同じユーザー ID とパスワードの組み合わせを使用することはできません。ただし、ユーザー名とパスワードポリシーを管理するのは、ユーザーの責任です。
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		—	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。
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		—	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	電子署名を行う場合は、常に識別コード（ユーザー ID）とパスワードの両方が必要になります。

## 9. 電子署名の一般要件と署名の構成要素および管理 (続き)

Part 11 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」の場合は具体的に要件がいかに満たされるか、「不可」の場合はユーザーに推奨される事柄
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	制御された 1 回のアクセス期間中、ある個人がアプリケーション内で一連の文書に署名する場合、そのユーザーは、最初の署名時に 3 つの署名の構成要素、すなわちユーザー ID、パスワード、および署名の意味を入力する必要があります。
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		可	OpenLab ソリューションと Windows では、管理者が新規アカウントのユーザー、またはパスワードを忘れてしまったユーザーに初期パスワードを割り当て、そのパスワードを初回ログイン時に変更するようユーザーに要求することができます。これにより、ユーザー ID //パスワードの組み合わせは、その担当者のみが知り得る情報になります。OpenLab ソリューションで、企業の Windows NT ログインを使用してユーザーまたは OpenLab 管理ユーザーを認証している場合、複数のユーザーが同じユーザー ID //パスワードの組み合わせを使用することはできません。ユーザー名とパスワードを他のラボメンバーと共有しないようにすることは、ユーザーの責任です。
Part 11 11.200(a) (3)	9.10 2 名以上の協力がない限り、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	OpenLab ソリューションでは、ユーザー ID とパスワードを使用して電子署名を開始します。アプリケーションユーザーのパスワードはデータベース内に暗号化されて格納されており、ソフトウェア内のすべての場所でアスタリスクで表示されます。  OpenLab ソリューションでは、管理者が新規アカウントのユーザー、またはパスワードを忘れてしまったユーザーに初期パスワードを割り当て、そのパスワードを初回ログイン時に変更するようユーザーに要求することができます。これにより、ユーザー ID //パスワードの組み合わせは、その担当者のみが知り得る情報になります。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		—	このシステムではバイオメトリック署名を使用できません。

## 10. 識別コードとパスワードの管理

Part 11 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」の場合は具体的に要件がいかに満たされるか、 「不可」の場合はユーザーに推奨される事柄
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	<p>Cary UV ワークステーション認証は、ドメインレベルのユーザーの使用など、Windows ユーザー管理に関連付けることができます。Windows のユーザーとグループ管理を使用している場合、管理者は Windows パスワードポリシーを適切に設定できます。</p> <p>OpenLab ソリューションで、企業の Windows ドメインログインを使用してユーザーまたは OpenLab ソリューション管理ユーザーを認証している場合、複数のユーザーが同じユーザー ID /パスワードの組み合わせを使用することはできません。</p>
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、または見直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	<p>Cary UV ワークステーション認証では Windows ドメイン認証を使用できるため、Windows パスワードポリシー設定の一部としてパスワード更新間隔を設定しています。管理者は、パスワードの定期的な自動更新間隔を定義できます。また、ユーザーが同じパスワードを繰り返し使用しないようにしています。</p> <p>OpenLab ソリューションで管理しているユーザーは、パスワードが定期的に自動更新されるように設定できます。</p>

## 10. 識別コードとパスワードの管理(続き)

Part 11 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」の場合は具体的に要件がいかに満たされるか、「不可」の場合はユーザーに推奨される事柄
Part 11 11.300(c)	10.3 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、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措置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。	—	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使用。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。	—	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		—	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 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」の場合は具体的に要件がいかに満たされるか、「不可」の場合はユーザーに推奨される事柄
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体系 and 审计信息相关的文件。	可	アジレントのソフトウェアは、ISO 9001 に適合したアジレントのライフサイクルに従って開発およびテストされています。ライフサイクルのチェックポイントでの成果物は、経営側によってレビューおよび承認されています。製品は、機能仕様、性能仕様、および出荷時のリリース基準に適合していました。

## 11. システムの開発とサポート (続き)

Part 11 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」の場合は具体的に要件がいかに満たされるか、 「不可」の場合はユーザーに推奨される事柄
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ます。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に対して正式な契約を義務付けており、ISO 9001 サプライヤ品質管理ポリシーに従っています。
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	—	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	—	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	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。供給元はそのスタッフにトレーニングを受けさせる必要があります。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によって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）。



## 参考文献

1. R. A. Botha, 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; Electronic Signatures [Online] <https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=11> (accessed November 4, 2015).
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. [Online] [http://ec.europa.eu/health/files/eudralex/vol-4/annex11\\_01-2011\\_en.pdf](http://ec.europa.eu/health/files/eudralex/vol-4/annex11_01-2011_en.pdf) (accessed November 4, 2015).

## 詳細情報

アジレントの製品とサービスの詳細については、アジレントのウェブサイト [www.agilent.com/chem/jp](http://www.agilent.com/chem/jp) をご覧ください。

ホームページ

**[www.agilent.com/chem/jp](http://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](mailto: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。

アジレント・テクノロジー株式会社  
© Agilent Technologies, Inc. 2021  
Printed in Japan, September 1, 2021  
5994-1318JAJP  
DE44426.2696412037