

## 21 CFR Part 11 および Annex 11 コンプライアンスのサポート： ICP-MS MassHunter Workstation Plus ソフトウェア



### 概要

OpenLab Server と ECM XT は、複数の ICP-MS を運用する拡大中の中～大規模ラボに最適なコンプライアンスソリューションです。また OpenLab ECM は、複数の装置やサイトからの電子記録を管理したい大規模ラボに適しています。ただし、このようなサーバーベースのコンプライアンスソリューションはコストがかかり複雑であるため、シンプルなコンプライアンスツールで 1 台の ICP-MS の記録を管理する必要がある小規模ラボには適さない場合があります。

Agilent ICP-MS MassHunter Workstation Plus は、このような小規模ラボが低コストで 21 CFR Part 11 および Annex 11 に準拠するのに適したソフトウェアです。Workstation Plus を ICP-MS の PC にインストールすれば、1 台の Agilent ICP-MS または ICP-QQQ 用のシンプルでコスト効率の高いコンプライアンスソリューションとなります。

ICP-MS MassHunter ユーザーアクセスコントロールオプションは OpenLab Server、ECM XT、ECM 統合と同様に、OpenLab Shared Services (OLSS) 機能を使用してワークステーションへのユーザーアクセスを管理し、アプリケーションとワークステーションの監査証跡を記録します。

## コンプライアンスの構成要素

規制を遵守することは、医薬品製造などの多くの業界における分析ラボ運営の重要側面であり、そこでは製造管理及び品質管理の基準（GMP）が適用されます。

分析機器に関連するコンプライアンスの 4 つの構成要素は、次のとおりです。

- 分析機器およびそのソフトウェアの設計時適格性評価（DQ）、製造品質管理、ライフサイクルの管理と文書化、据付時適格性評価と運転時適格性評価（IQ/OQ）
- 機器コントロールおよびデータ処理用ワークステーションへのユーザーアクセス管理（パスワード保護によるユーザーログインアクセスの制限）
- 電子記録のセキュリティ、完全性、トレーサビリティ（安全な保存、ファイルのバージョンング、監査証跡、電子署名、アーカイブ/検索）
- システム運用、性能評価（PQ）、ラボおよび関連機器への物理的アクセス、標準操作手順書、トレーニングおよび記録の管理

## Agilent ICP-MS システム用コンプライアンス

最初のコンプライアンス構成要素は、装置メーカーの製造品質記録と機器バリデーション認定によって証明する必要があります。

### 設計時適格性評価

規制対象ラボは、使用する機器が、適切な品質プロセスのもとで設計、製造、試験、設置、適格性評価されていることを確認する必要があります。

機器ソフトウェアの場合、装置メーカーは製品バリデーション宣言書を提供する必要があります。これは、使用しているソフトウェアが 21 CFR 58（優良試験所基準）、21 CFR 210（医薬品優良製造基準）、または 21 CFR 211（現行医薬品優良製造基準）に基づく認定のユーザー要件を満たしていることを確認するためのものです。欧州では、同等の GxP 要件が ISO 規格および ICH ガイドライン Q8、Q9、Q10 で定められています。図 1 に、アジレントの ICP-MS MassHunter ソフトウェアの製品バリデーション宣言書の例を示します。



図 1. ソフトウェア品質宣言書（左）と IQ/OQ 適格性評価レポートの送付状の例

## 据付時適格性評価と運転時適格性評価 (IQ/OQ)

製品がユーザーのラボに納品されたら、さらなる適格性評価チェックを実施する必要があります。その目的は、納品された製品が所定の項目に適合しており、システムのハードウェアとソフトウェアがメーカーの意図どおりに機能することを確認することです。

これらのサービスは通常、メーカーが実施するものであり、据付時適格性評価 (IQ) および運転時適格性評価 (OQ) と呼ばれます。IQ/OQ サービスは自動化されていることが多く、装置システムのハードウェアと、その操作に必要なすべてのソフトウェアコンポーネントで利用できる必要があります。適格性評価サービスには通常、規制遵守の証明に必要な関連文書の作成が含まれます。

図 1 に、Agilent ICP-MS ハードウェアおよび ICP-MS MassHunter ソフトウェアの IQ/OQ 文書の送付状の例を示します。

## 性能と文書化

完全なコンプライアンスソリューションの 4 番目の構成要素を満たすには、ユーザー組織の責任者がラボのアクセスの適切な管理方法を策定し、目的のメソッドの分析性能が検証されるようにして、ルーチン操作で従うべき手順を文書化する必要があります。

装置の設置と適格性評価が完了したら、通常はルーチン測定されるメソッドとサンプルを用いてシステム適合性試験 (SST) と呼ばれる分析チェックが実施されます。SST では、システム性能がラボ固有の分析要件を満たすことを確認します。アジレントは、包括的な標準操作手順書 (SOP) を策定しています。これは USP<232> や ICH Q3D に基づく医薬品試験を準備しているラボに提供されるソリューション全体の一部を構成するものです。また、関連するその他の製品やサービス (サンプル前処理装置や認定標準液など) を提供し、新たな分析施設を準備するためのエンドツーエンドのワークフローベースアプローチを提供することもできます。

## ユーザーアクセスと電子記録

残りの 2 つの構成要素 (システムのログインアクセスと電子記録の管理) は通常、ソフトウェアパッケージで管理します。このソフトウェアパッケージがワークステーションへのユーザーアクセスを管理およびモニタリングし、ラボの活動中に生成されるデータやその他の電子記録を処理するための安全な統合型システムを提供します。これらのチェックはデータインテグリティを確保できるように設計されており、GMP 管理下で作成されるあらゆる記録に適用される ALCOA+ 原則にまとめられています。ALCOA では、記録の帰属性 (Attributable)、判読性 (Legible)、同時性 (Contemporaneous)、原本性 (Original)、正確性 (Accurate) が求められます。プラス (ALCOA+) ではこれに加えて、記録の完全性 (Complete)、一貫性 (Consistent)、永続性 (Enduring)、利用可能性 (Available) も求められます。

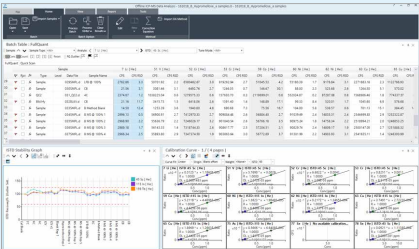
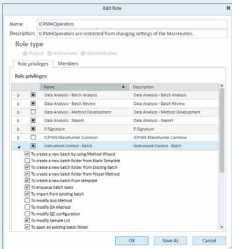
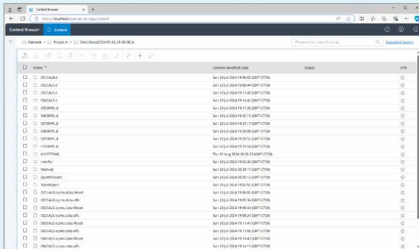
ICP-MS MassHunter のユーザーアクセスコントロール (UAC/OLSS) は、ユーザーアクセスとデータインテグリティの機能に加えて、アジレントのコンプライアンスソフトウェアオプションの 1 つ (Workstation Plus、OpenLab Basic Server、OpenLab Server、ECM XT、または OpenLab ECM) をサポートしています。

## ICP-MS MassHunter Workstation Plus

Workstation Plus とユーザーアクセスコントロールを組み合わせると、Agilent ICP-MS を規制に準拠しながら運用できます。すべてのソフトウェアは、標準の ICP-MS MassHunter ワークステーション PC にインストールされるため、設定が簡単かつ低コストです。

マルチレベルのユーザーアクセス権と監査証跡は、ラボ管理者が設定できます。または、デフォルトの監査証跡マップ (ATM) の設定を使用することもできます。ATM 設定では、特定の機能を実行できるユーザーレベル、パスワード入力の実否、それらの機能でアクセス権を確認すべき理由を定義します。データベースの設定と管理は、シンプルな設定ペインで実行されます。

次の表は、ICP-MS MassHunter バージョン 5.3 パッチ 1 以降の機能と UAC/OLSS の組み合わせにより、ラボがどのように 21 CFR Part 11、EU Annex 11、およびその他の関連規制の規制要件に対応できるかをまとめたものです。

		
<b>ICP-MS MassHunter</b> アプリケーションソフトウェアが、装置を制御してデータの取り込みと (再) 処理を実行します。	<b>OLSS によるユーザーアクセスコントロール</b> UAC/OLSS が、設計可能なマルチレベルのパスワードで保護されたユーザープロファイルによるセキュリティを実現します。ユーザーのログオン/ログオフとアクションを監査証跡に記録します。	<b>ICP-MS MassHunter Workstation Plus</b> Workstation Plus は内蔵の堅牢なコンテンツ管理システムであり、ラボのデータ処理を効率化および保護できるように設計されています。

## アジレントの ICP-MS MassHunter Workstation Plus ソフトウェアによる 21 CFR Part 11 の規制要件への対応

Part 11 またはその他	要件	可/不可	「可」の場合、要件がどのように満たされるか、「不可」の場合、ユーザーへの推奨事項を記載
1.バリデーション			
Part 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。	可	アジレントは、正確性、信頼性、性能の一貫性を評価するために特別に策定した試験により、ICP-MS MassHunter Workstation Plus を含む自社システムの性能の大規模バリデーションを実施してきました。アジレントでは、据付時適格性評価および運転時適格性評価 (IQ/OQ) サービスを利用したオンサイトシステムのバリデーションを推奨しています。安全なデータベースストレージにアップロードされるファイルのチェックサム保護、バージョン管理、および新旧の値を示す監査証跡を使用することは、電子記録の完全性、セキュリティ、トレーサビリティを確保するためのシステムと手順の導入に役立ちます。
Annex 11.Principle B、ブラジル GMP 577	1.2 設備は適切ですか。	N/A	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 11.10(b)	2.1 システムは、FDA による調査、審査、およびコピー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。	可	ICP-MS MassHunter Workstation Plus ソフトウェアにより生成される生データ、メタデータ、結果データは、ローカルの安全なデータベースで処理されます。人が読める電子記録形式である ICP-MS MassHunter Workstation Plus レポート (チューニングレポートや定量データレポートなど) は PDF ファイルとして保存でき、クライアントマシンにソースアプリケーションをインストールしなくても、印刷したり PDF ビューアで確認したりすることができます。これらのレポートに、すべてのデータや監査証跡を含めることができます。
Annex 11.8.1、ブラジル GMP 583	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を取得することはできますか。	可	人が読める電子記録形式である ICP-MS MassHunter Workstation Plus レポート (チューニングレポートや定量データレポートなど) は、PDF ファイルとして保存できます。これらのファイルは、クライアントマシンにソースアプリケーションをインストールしなくても、印刷したりビューアで確認したりすることができます。これらのレポートに、すべてのデータや監査証跡を含めることができます。
ブラジル 585.2	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行われるための管理措置が設けられていますか。	可	Windows ファイルシステムや Workstation Plus に保存されているすべてのファイルは、Workstation Plus の機能や Windows バックアップユーティリティを用いてバックアップを取ることができます。これらのバックアップのスケジュール設定と実行については、ユーザー組織が責任を持ちます。
Part 11.10(c)、中国 GMP 163	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。	可	電子記録は、Workstation Plus 内に配置されている安全なデータベースに自動的に保存されます。ユーザーは電子記録にアクセスします。すべてのデータファイルやその他の規制対象記録 (取り込みおよびデータ解析アクションの監査証跡を含む) も、Workstation Plus データベースに保存されます。
Annex 11.17	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。	N/A	保存データを定期的にチェックする機能はありますが、その使用についてはユーザーの責任です。
Annex 11.17	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。	可	修正されたソフトウェアは、リリース前に動作の一貫性と下位互換性のテストを受けます。新規または更新バージョンのインストール後に、アジレントがサービスとしてシステムの再バリデーションを提供する場合があります。
Annex 11.7.1、ブラジル GMP 584	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。	可	電子記録は保存され、安全なデータベースに自動的にアップロードされます。すべてのデータファイルやその他の規制対象記録 (取り込みおよびデータ解析アクションの監査証跡を含む) も、保存されます。ユーザー組織は、PC の物理的保護、データバックアップ、アーカイブのプロセスに責任を持ちます。
臨床コンピュータガイド F2、FDA Q&A	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。	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、すべての生データは安全なストレージにコピーされます。監査証跡エンタリには、例えばメソッドのパラメータ変更における新旧の値が記録されます。
臨床コンピュータガイド F2、FDA Q&A	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。	N/A	この情報はシステムから入手できますが、FDA への提供はユーザーの責任において実施します。
Annex 11.7.1、中国 GMP 163、ブラジル GMP 585、Part 211、68 b	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。	可	定期的なバックアップをサポートするツールが提供されていますが、(Workstation Plus の電子記録以外の) データバックアップシステムの導入は、ユーザー組織の責任です。また、管理 (バックアップスケジュールの設定など) もユーザー組織の責任です。
Annex 11.7.1、中国 GMP 163、ブラジル GMP 585、Part 211、68 b	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。	N/A	バックアップおよび復元されたデータをチェックする機能はありますが、その使用についてはユーザーの責任です。
臨床コンピュータガイド E	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アプリケーション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。	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 F	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。	可	アジレントは、ICP-MS MassHunter Workstation Plus 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。

Part 11 またはその他	要件	可/不可	「可」の場合、要件がどのように満たされるか、「不可」の場合、ユーザーへの推奨事項を記載
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 11.10(d)、 中国 GMP 183 163、 ブラジル GMP 579、 ICH Q7.5.43	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。	可	すべてのファイルおよびソフトウェア機能へのアクセスは、個々のユーザーまたはユーザーグループに割り当てられた特定の権限または役割によって管理されます。システム管理者は、許可されたユーザーまたはグループに適切なアクセスレベルを割り当てます。各ユーザーは、一意のユーザー ID とパスワードの組み合わせによって識別されます。ICP-MS MassHunter Workstation Plus にアクセスするには、ユーザー ID とパスワードで構成される一意の ID を入力する必要があります。
複数の警告書	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。	可	システムは、各ユーザーの電子署名に一意のユーザー ID とパスワードの組み合わせを使用します。ユーザー ID は一意であり、再利用したり、別の人に再割り当てしたりしてはなりません。これについては、システムを導入して使用する組織が責任を持ちます。
臨床コンピュータ ガイド 4	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。	可	QLSS ユーザー管理および Windows ユーザーアカウント管理機能には、この情報が含まれます。累積記録の維持は、ユーザー組織の責任です。
4. 電子監査証跡			
Part 11.10(e)、 中国 GMP 163	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。	可	電子記録の作成、変更、または削除に関連するすべての操作は、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、すべての変更内容、変更日時、ユーザー ID、および変更理由（該当する場合）のリストです。ユーザーが監査証跡エントリを消去、変更、削除することはできません。ICP-MS MassHunter Workstation Plus ソフトウェアは、取り込みおよび分析操作の完全で正確な履歴を維持するために、電子記録の一部としてタイムスタンプ付き監査証跡を自動的に生成します。また Workstation Plus は、ICP-MS バッチの更新に関する監査証跡エントリを保護します。
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	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。	可	監査証跡エントリには、ユーザー名、実施した変更の詳細、日時、署名に関する理由（監査証跡マップの設定で、監査証跡エントリをトリガーしたアクションの理由が必要と指定されている場合）が含まれます。
Annex 11、8.2	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。	可	この情報は、監査証跡エントリに記録されている新旧の値によるメソッド設定に使用できます。変更フラグは ICP-MS MassHunter レポートで直接サポートされていませんが、Workstation Plus で記録をバージョン管理できます。このため、バージョン番号を使用して、元のエントリから変更または更新された記録を特定できます。
FDA GMP Part 211.194 8b	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。	可	規制のメソッドであるかどうかにかかわらず、メソッドの変更は監査証跡に記録されます。
FDA GMP Part 211.194 8b	4.5 このような記録には、変更理由が含まれますか。	可	メソッド変更の理由は、監査証跡マップでそのアクションの「理由」が選択されている場合に記録されます。
FDA 警告書	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。	可	監査証跡機能は、常時オンに設定できます。この機能をいったん有効にすると、ICP-MS MassHunter の管理者権限を持つユーザーのみがオフにできます。つまり、通常のシステムオペレータはオフにできません。
Annex 11、9	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。	可	監査証跡の記録は簡単に理解できます。監査証跡に保存されるフィールドやエントリは、ICP-MS MassHunter Workstation Plus 機能に固有の言語ではなく、平易な言語で記述されています。
Annex 11 および警告 書の暗黙的要件（多くの 場合、顧客から求め られる）	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。	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 11.10(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。	可	新しい記録を ICP-MS MassHunter Workstation Plus に追加すると、既存の記録と以前に記録した監査証跡エントリの両方が保持されます。新しい記録が監査証跡ファイルに蓄積されます。そのとき、古い記録は変更されません。
Part 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。	可	ICP-MS MassHunter Workstation Plus バッチ監査証跡は、ユーザー組織が定めた保持期間中、データと共に保持されます。
Part 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。	可	監査証跡は ICP-MS MassHunter Workstation Plus ソフトウェアで閲覧できます。監査証跡や選択したエントリは、レポート機能を使用してコピーや印刷ができます。
Annex 11、8.1	4.12 電子的に保存されている電子記録（監査証跡など）は明確に印刷されたコピーを得られますか。	可	監査証跡エントリを含む電子的な記録は、直接印刷したり、印刷可能な形式にコピーしたりすることができます。

Part 11 またはその他	要件	可/不可	「可」の場合、要件がどのように満たされるか、「不可」の場合、ユーザーへの推奨事項を記載
<b>5.動作およびデバイスの確認</b>			
Part 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。	可	装置のシリアル番号は、ICP-MS から ICP-MS MassHunter Workstation Plus ソフトウェアに自動的に転送されます。シリアル番号はソフトウェアに表示でき、データファイルに記録されます。またソースコンピュータ名は、データベースに保存されるファイルに記録されます。データ転送の前に、デバイスの「ハンドシェイク」により、ICP-MS とアプリケーションホストコンピュータ間の正しいリンクが確認されます。
Part 11.10(i)、 中国 GMP 18、 ブラジル 571	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。	可	アジレントの企業ポリシーは、個人のトレーニング記録の開示を禁止しています。ただし、監査でトレーニングプログラムの存在を確認できます。また、資料によって「アジレントの従業員がトレーニングを受けている...」ことを明示できます。  アジレント・テクノロジーの従業員の教育および雇用履歴の記録は、個人記録により確認および保持されます。また ICP-MS MassHunter Workstation Plus のエンドユーザーは、顧客拠点での同システムの教育、トレーニング、経験の記録を保持する必要があります。  アジレントは、製品の設置時に、システムユーザーを対象に基本操作トレーニングを実施しています。アジレントが提供する追加のシステムトレーニングもあります。
Part 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。	N/A	ユーザーの責任です。
Part 11.10(j) の暗黙的要件	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。	N/A	ユーザーの責任です。
Part 11.10(k)、 中国 GMP 161	5.8 システム文書に関する適切な管理方法が用意されていますか。例：(1) システムの運用と保守に関する文書の配布、アクセス、使用に関する適切な管理方法	N/A	ユーザーの責任です。
Part 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。	可	アジレントの品質および製品ライフサイクルプロセスには、システム文書の正式な書面による改訂および変更管理手順が含まれています。管理対象の文書改訂はすべてタイムスタンプが付けられ、監査証跡の対象となります。
<b>6.データインテグリティ、日時の正確性</b>			
Annex 11.5	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	ICP-MS MassHunter Workstation Plus が他のシステムとデータをやり取りすることはありません。
Annex 11-6、 ブラジル GMP 580、 ICH Q7-5.45	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)	可	データの正確性とその他のチェック（検量線の妥当性チェックなど）は、ユーザー組織が定める適切な品質管理チェックにより確認できます。追加のチェック、例えばクオリファイア同位体の確認結果の報告などを使用できます。その他のチェック、例えば他のオペレータによる確認などは、ユーザー組織の責任において実施します。
臨床コンピュータ ガイド D.3	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。	部分的	ICP-MS MassHunter Workstation Plus は、オペレーティングシステム、ドメインコントローラ、またはタイムサーバーから日時を取得します（LAN/WAN に接続されている場合）。オペレーティングシステムの日時設定はユーザー組織の責任であり、SoP を用いて管理する必要があります。ユーザーが実行するローカル OS の日時変更は、システムの監査証跡に記録されます。
臨床コンピュータ ガイド D.3	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。	部分的	ICP-MS MassHunter Workstation Plus は、ワークステーション PC のオペレーティングシステム、ドメインコントローラ、またはタイムサーバーから日時を取得します（LAN/WAN に接続されている場合）。PC へのアクセス権限を持つ（ユーザーログオンが有効な）ユーザーのみが、ローカル PC の日時設定にアクセスして変更できます。これはシステムイベントログに記録され、確認できます。通知は自動的に送信されません。
臨床コンピュータ ガイド D.3	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。	可	ICP-MS MassHunter Workstation Plus はスタンドアロンの PC システムであるため、複数のタイムゾーンを網羅することはありません。ICP-MS MassHunter Workstation Plus の監査証跡は、現地時間 + UTC との時差で記録されます。例えば「Thursday, March 01, 2012, 6:52:21 PM (UTC+09:00)」のようになります。
<b>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）</b>			
Part 11.3	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	ICP-MS MassHunter Workstation Plus は、オープンシステムとして動作するように設計されていません。
Part 11.3	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	ICP-MS MassHunter Workstation Plus は、オープンシステムとして動作するように設計されていません。

Part 11 またはその他	要件	可/不可	「可」の場合、要件がどのように満たされるか、「不可」の場合、ユーザーへの推奨事項を記載
<b>8. 電子署名 - 署名の明示および署名/記録の関連付け</b>			
Annex 11.14、 ICH Q7.6.18	8.1 電子署名を使用する場合、企業の範囲内で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。	可	企業内での電子署名の使用と効力については、ユーザー組織の責任となります。電子署名は該当する記録に永久的に関連付けられ、適用された日時（および必要に応じて理由）が含まれます。
Part 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）	可	署名された電子記録に表示される内容： 1. 署名者の氏名と署名レベル 2. 署名が行われた日時 3. 署名の意味 4. 署名の理由を示すために入力されたコメント
Part 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。	可	ICP-MS MassHunter Workstation Plus ソフトウェアで適用される電子署名は、アプリケーション画面、および印刷レポートや電子レポートで確認できます。
Part 11.7	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。	可	ファイルは ICP-MS MassHunter ソフトウェア Workstation Plus で電子署名できます。電子署名はファイルと強固に関連付けられています。システムは、その独自の電子署名システム外で適用される署名（手書きの署名など）を認識しません。
Part 11 序文 第 124 項	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。	可	ICP-MS MassHunter Workstation Plus には、設定可能な時間ベースのロック機能があり、アプリケーションを再開するにはユーザーログイン（ユーザー名とパスワード）が必要です。
<b>9. 電子署名の一般要件と署名の構成要素および管理</b>			
Part 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。	可	システムは、各ユーザーの電子署名に一意のユーザー ID とパスワードの組み合わせを使用します。ユーザー ID は一意であり、再利用したり、別の人に再割り当てしたりしてはなりません。これについては、システムを導入して使用する組織が責任を持ちます。
Part 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	ユーザーの責任です。
Part 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。	N/A	ユーザーの責任です。
Part 11.100 (c)	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	ユーザーの責任です。
Part 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。	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 11.200(a) (1) (i)	9.6 制御されたシステム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う場合、最初の署名の実行には電子署名の構成要素がすべて必要ですか。	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。
Part 11.200(a) (1) (i)	9.7 制御されたシステムアクセスの連続的な期間内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 つ以上の電子署名構成要素を使用して実行されますか。	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。ユーザーがパスワードを共有しないようにすることは、ユーザー組織の責任です。

Part 11 またはその他	要件	可/不可	「可」の場合、要件がどのように満たされるか、「不可」の場合、ユーザーへの推奨事項を記載
9. 電子署名の一般要件と署名の構成要素および管理			
Part 11.200(a) (1) (ii)	9.8 制御されたシステムアクセスの連続的な期間内にユーザーが署名を行わない場合、それぞれの署名の実行には電子署名構成要素がすべて必要ですか。	可	ユーザーは各記録を個別に電子署名する必要があります。ユーザーは電子署名ごとに 2 つの異なる識別要素 (一意のユーザー ID とパスワード) を入力する必要があります。
Part 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。	可	システムでは、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 と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。またシステムでは、2 人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を禁じています。ユーザー ID とパスワードが真正な所有者によってのみ使用され、他のユーザーと共有されないようにすることは、ユーザー組織の責任です。
Part 11.200(a) (3)	9.10 2 名以上の協力がなく、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。	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 11.200(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	システムで提供されている電子署名は、バイオメトリックスベースではありません。
10. 識別コードとパスワードの管理			
Part 11.300(a)	10.1 2 名の方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。	可	各ユーザーが、一意のユーザー ID とパスワードの組み合わせを保持する必要があります。権限を持つユーザーが自身のアカウント情報やアクセス権を他のユーザーと共有しないようにすることは、ユーザー組織の責任です。ユーザー管理は OLSS で実施されます。OLSS では、2 人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を禁じています。
Part 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。	可	OLSS はユーザーアクセス管理に使用されます。パスワードの更新間隔は、OLSS のパスワードポリシー設定で設定できます。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。
Part 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。	N/A	Agilent ICP-MS MassHunter Workstation Plus の UAC/OLSS は、ID コードやパスワードの生成にトークン、カード、またはその他のデバイスを使用しません。
Part 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。	可	OLSS セキュリティポリシーは、不正アクセスの試行回数が、ユーザーが定義されている回数に達した場合に、ユーザーアカウントをロックするよう設定することができます。またこれを、システム管理者に伝えることができます。システム監査証跡は、一般的なイベント (コンピュータへのログオン試行、アプリケーションやユーザーの変更など) を、すべてのセキュリティ情報の中央監査リポジトリとしてシステムイベントログに記録します。これにはシステムとコンピュータ ID、およびオペレータ名とアプリケーション ID が含まれるため、潜在的なセキュリティ違反をすぐにチェックできます。セキュリティ情報の不正使用のモニタリングと報告は、ユーザー組織の責任です。
Part 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。	N/A	Agilent ICP-MS MassHunter Workstation Plus の UAC/OLSS は、ID コードやパスワードの生成にトークン、カード、またはその他のデバイスを使用しません。



Part 11 またはその他	要件	可/不可	「可」の場合、要件がどのように満たされるか、「不可」の場合、ユーザーへの推奨事項を記載
11. システムの開発とサポート			
Annex 11 4.5、 ブラジル GMP 577、 GAMP	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。	可	アジレントは、ICP-MS MassHunter Workstation Plus と UAC/OLSS ソフトウェアが最新の Agilent LSCA 製品ライフサイクルリビジョンおよび ISO QMS 認定で定められている品質管理システムのもとで開発されているという文書化された証拠と、製品試験および適格性評価サービス中に実施された試験の文書を維持し、提供できます。
ブラジル GMP 589	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。	N/A	Agilent ICP-MS MassHunter Workstation Plus ソフトウェアの開発やサポートに、下請業者は関与していません。
ICH Q10, 2.7 c	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。	N/A	Agilent ICP-MS MassHunter Workstation Plus ソフトウェアの開発やサポートに、下請業者は関与していません。

説明は 21 CFR Part 11 より抜粋：

<https://www.fda.gov/regulatory-information/search-fda-guidance-documents/part-11-electronic-records-electronic-signatures-scope-and-application>

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

**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。

DE-000617

アジレント・テクノロジー株式会社

© Agilent Technologies, Inc. 2024

Printed in Japan, October 2, 2024

5994-7766JAJP