白書

21 CFR Part 11 および Annex 11 コンプライアンスのサポート：Agilent ICP-MS MassHunter ソフトウェア用 SDA モジュール

概要

連邦規則第 21 条第 11 章（21 CFR part 11）は、米国の食品および医薬品を対象とするもので、電子記録の保存と保護および電子署名の適用に関する米連邦ガイドラインが収載されています。欧州連合では、これに相当するガイドラインを EU Annex 11 として規定しています。

これらの規制の目的は、メソッド情報、データや分析レポート、分析機器の動作に関するその他の記録（例えば、毎日の性能確認）などの電子記録について、セキュリティ、完全性、トレーサビリティを確保することにあります。

Agilent ICP-MS および ICP-QQQ 機器は、ICP-MS MassHunter ソフトウェアで制御されています。ICP-MS MassHunter は、Agilent Spectroscopy Database Administrator（SDA）、OpenLab ECM（Enterprise Content Manager）、OpenLab Server、または ECM XT ソフトウェアとの統合をサポートし、電子記録の取り扱いに関する FDA、欧州、その他の関連ガイドラインへのコンプライアンスを確保するためのツールを提供しています。

OpenLab Server および ECM XT は、複数の ICP-MS 機器を備えた現在拡大中の中規模ラボに対する最適なコンプライアンスソリューションであり、OpenLab ECM は、複数の機器およびサイトの電子記録を管理する必要がある大規模なラボに最適です。ただし、これらのサーバーベースのコンプライアンスソリューションのコストと複雑さは、1 台の ICP-MS 機器の記録を管理するためのシンプルなコンプライアンスツールセットを必要としている小規模のラボには適さない場合があります。

このような小規模のラボに対して、Agilent Spectroscopy Database Administrator（SDA）ソフトウェアは、21 CFR Part 11 および Annex 11 に適合するための低コストのソリューションを提供します。SDA（Agilent ICP-OES 機器にも対応）を ICP-MS 機器のワークステーション PC にインストールすることにより、1 台の Agilent ICP-MS または ICP-QQQ 機器に対する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を提供します。

OpenLab Server、ECM XT、および ECM との統合の場合と同様に、ICP-MS MassHunter ワークステーションへのユーザーアクセスおよびアプリケーションとワークステーションの監査証跡の記録の管理は、OpenLab Shared Services（OLSS）機能を使用した ICP-MS MassHunter ユーザーアクセスコントロールオプションにより実行します。

概要

規制へのコンプライアンスは、医薬品適正製造基準（GMP）の原則が適用される医薬品製造など、多くの業界の分析ラボの運用に関する重要な側面です。

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。

- 分析機器とそのソフトウェアに関する、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、据付時および稼働時適格性評価（IQ/OQ）。
- 機器コントロールおよびデータ処理のためのワークステーションへのユーザーアクセスの管理（パスワード保護によるユーザーログオンの制限）。
- 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ニング、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）、ラボと関連機器への物理的アクセス、標準操作手順書、トレーニングと記録の管理。

Agilent ICP-MS システムのコンプライアンス

コンプライアンスの最初の構成要素は、機器メーカーの製造品質記録および機器バリデーション証明書に基づいて実証する必要があります。

設計時適格性評価

規制対象ラボは、使用している機器が許容できる品質プロセス下で設計、製造、試験、据付、適格性確認されていることを確認する必要があります。

そのためには、機器ソフトウェアの場合、機器メーカーが製品バリエーション宣言書を提供し、当該ソフトウェアが 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）の認証に関してユーザーの要件を満たしていることを承認できなければなりません。欧州では、ISO 標準および ICH ガイドライン Q8、Q9、Q10 により同等の GxP 要件に対応しています。Agilent 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図 1 に示します。

据付時および稼働時適格性評価（IQ/OQ）

製品がユーザーのラボに納品されたら、詳細な適格性確認を実施し、納品された製品が指定した項目に適合していること、および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したとおりに機能することを確認する必要があります。

これらのサービスは通常メーカーが実施するもので、据付時適格性評価（IQ）および稼動時適格性評価（OQ）と呼ばれています。IQ/OQ サービスは多くの場合自動化されており、機器システムハードウェアおよびそれを操作するために必要なすべてのソフトウェアコンポーネントで使用できます。適格性評価サービスには通常、規制へのコンプライアンスを実証するために必要な関連文書化の完了が含まれています。

Agilent ICP-MS ハードウェアおよび ICP-MS MassHunter ソフトウェアの IQ/OQ 文書送付状の例を図 1 に示します。

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

性能と文書化

包括的なコンプライアンスソリューションの 4 番目の構成要素に適合するには、ユーザーの組織内の責任者がラボアクセスに関する適切なコントロールを設定して、目的のメソッドの分析性能を検証し、ルーチン分析で従うべき手順を文書化する必要があります。

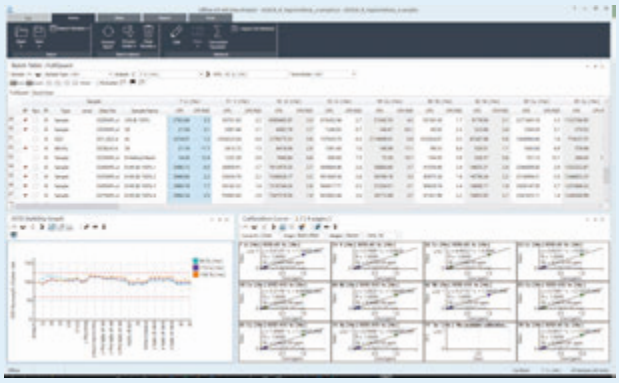
装置を据え付けて適格性確認をした後は通常、日常的に分析しているメソッドとサンプルを使用して、システム適合性試験（SST）と呼ばれる分析確認を実施します。SST では、システムの性能がラボ固有の分析要件に適合していることを確認します。 アジレントは包括的な標準操作手順書（SOP）を策定していま。この SOP が、USP<232> または ICH Q3D に従って医薬品試験を設定するラボに提供される包括的なソリューションの一部を形成します。サンプル前処理機器や認定標準溶液のようなその他の関連製品とサービスにより、新しい分析設備を設定するためのワークフローベースの包括的なアプローチも提供できます。

ユーザーアクセスと電子記録

残りの 2 つの構成要素（システムログオンアクセス、電子記録の管理）は通常、ソフトウェアパッケージで制御されます。このソフトウェアは、ワークステーションへのユーザーアクセスを制御して監視し、ラボの活動中に生成されたデータおよびその他の電子記録を取り扱うための安全で統合されたシステムを提供します。これらの確認は、データインテグリティを確保できように設計されており、GMP 制御下で作成されたすべての記録に適用される ALCOA+ 原則に要約されています。ALCOA は、記録には Attributable（帰属性）、Legible（判読性）、Contemporaneous（同時性）、Original（原本性）、Accurate（正確性）が必要であるという事実を示しており、プラス（ALCOA+）では Complete（完全性）、Consistent（一貫性）、Enduring（永続性）、Available（利用可能性）が加わります。

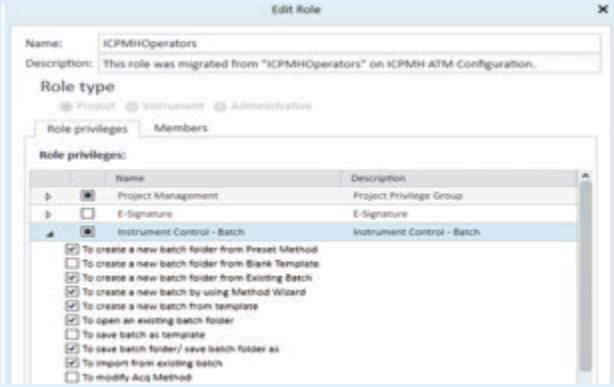
ユーザーアクセスおよびデータインテグリティ機能は、ICP-MS MassHunter 用のユーザーアクセスコントロール（UAC/OLSS）オプション、およびアジレントのコンプライアンスソフトウェアである SDA、OpenLab Server、ECM XT、または OpenLab ECM の 1 つによってサポートされています。

ICP-MS MassHunter



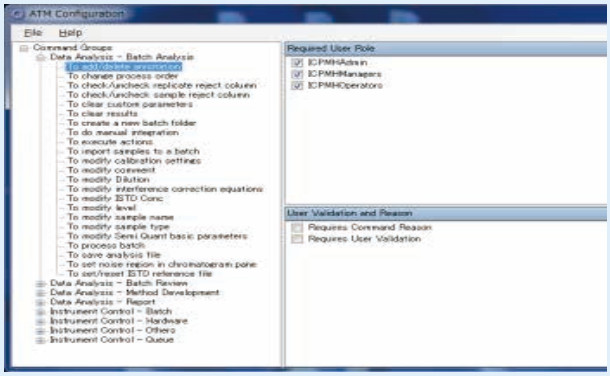
アプリケーションソフトウェアは、機器を制御してデータ取り込みと（再）処理を実行しています。

OLSS を使用したユーザーアクセスコントロール



UAC/OLSS は、設定可能なマルチレベルのパスワード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提供しています。ユーザーのログオン/ログオフおよび操作を監査証跡に記録します。

SDA ソフトウェア ICP-MS MassHunter バージョン



データベースは SDA によって作成され、アプリケーションソフトウェアがアクセスします。SDA は、Microsoft® SQL Server® Express 2014 を使用しています。

ICP-MS MassHunter と SDA

Agilent ICP-MS 機器の規制に準拠した操作を提供する ICP-MS MassHunter/UAC/SDA ソフトウェアシステムの構成要素を左に示します。すべてのソフトウェアは標準的な ICP-MS MassHunter ワークステーション PC にインストールされており、簡単かつ低コストで設定できます。

マルチレベルのユーザーアクセス権限と監査証跡はラボの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）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のはどのユーザーレベルであるか、またこれらの機能へのアクセス権限を検証するためにユーザーがパスワードと理由を入力する必要があるかどうかを定義します。データベースの設定と管理には、シンプルな SDA 設定ペインを使用します。

次の表は、ICP-MS MassHunter バージョン 5.x の機能と UAC/OLSS および SDA バージョン B.01.0x を組み合わせて、ラボがどのようにして 21 CFR Part 11、EU Annex 11、その他の関連規制の規制項目に適合できるかを示したものです。

Agilent ICP-MS SDA ソフトウェアを使用した 21 CFR Part 11 の規制項目への適合

Part 11 またはその他	要件	可/不可	「可」の場合、具体的に要件がいかに満たされるか、 または「不可」の場合、ユーザーに推奨される事柄
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、特に正確性、信頼性、一貫性の性能を評価するための試験を実施して、ICP-MS MassHunter および SDA を含むシステムの性能を広範にバリデーションしています。アジレントでは、据付時および稼働時適格性評価（IQ/OQ）サービスを使用してオンサイトシステムをバリデーションすることを推奨しています。安全な SDA データベースストレージにアップロードされたファイルのチェックサム保護、バージョン管理、監査証跡を使用して、システムと手順を実装する際にサポートユーザーに対して以前の値と新しい値を表示することにより、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しています。
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	生データ、ICP-MS MassHunter ソフトウェアが生成したメタデータと結果データを SDA にコピーして管理しています。これらすべての情報が含まれている結果セットはいつでも、確認用の元データのコピーとしてクライアント PC のハードディスクに転送できます。電子形式を読み取るには、ICP-MS MassHunter ソフトウェアが必要です。電子記録を人間が判読できる形式で表した ICP-MS MassHunter レポート（チューニングレポート、濃度データレポートなど）は PDF ファイルとして保存できるため、ソースアプリケーションがクライアントマシンにインストールされていなくても、PDF ビューアを使用して印刷または確認できます。これらのレポートには、すべてのデータと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が得られますか。	可	電子形式ファイルを読み取るには、ICP-MS MassHunter ソフトウェアが必要です。電子記録を人間が判読できる形式で表した ICP-MS MassHunter レポート（チューニングレポート、濃度データレポートなど）は PDF ファイルとして保存できるため、ソースアプリケーションがクライアントマシンにインストールされていなくても、ビューアを使用して印刷または確認できます。これらのレポートには、すべてのデータと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。	可	Windows ファイルシステムまたは SDA に保存されているファイルはすべて、SDA の機能または Windows のバックアップユーティリティを使用してバックアップできます。これらのバックアップをスケジューリングして実行することは、ユーザーが所属する組織の責任です。
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	SDA をローカルデータ保護モードで実行することにより、電子記録が保存され、安全な SDA データベースに自動的にアップロードされます。ユーザーは、SDA に置かれている電子記録にアクセスします。データの取り込みと分析操作用の監査証跡などのデータファイルとその他の規制記録はすべて SDA にコピーされます。
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	保存されているデータを定期的にチェックする機能は用意されていますが、その機能を使用すること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	改訂されたソフトウェアは、リリースの前に一貫性のある操作および下位互換性がテストされています。新規または更新されたリビジョンをインストールした後、アジレントが提供するサービスとしてシステムの再バリデーションを実施できます。
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	SDA をローカルデータ保護モードで実行することにより、電子記録が保存され、安全な SDA データベースに自動的にアップロードされます。データの取り込みと分析操作用の監査証跡などのデータファイルとその他の規制記録はすべて SDA にコピーされます。PC の物理的保護、データバックアップ、およびアーカイブプロセスは、ユーザーが所属する組織の責任です。
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場所にコピーされます。監査証跡のエントリには、例えば、メソッドで変更されたパラメータの以前の値と新しい値が記録されています。

Part 11 またはその他	要件	可/不可	「可」の場合、具体的に要件がいかに満たされるか、 または「不可」の場合、ユーザーに推奨される事柄
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で使用できますが、FDA に提供することはユーザーの責任です。
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	SDA からエクスポートされたデータなど、Windows ファイルシステムに保存されているファイルはすべて、Windows の通常のバックアップユーティリティを使用してバックアップできます。
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定期的にバリデーション時にチェックおよび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データをチェックする機能は用意されていますが、その機能を使用すること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。	部分的	取り込みデータ、レポート、および関連するメソッドファイルは、SDA データベースに転送することにより保護されます。これらの記録は、アプリケーションソフトウェア以外では表示したり変更したりできません。ワークステーション PC およびそのファイルへの不正ユーザーアクセスの阻止策を、ユーザーのアクセスコントロールおよび SOP を介して実装する必要があります。この記録を変更または削除しようとすると、システムのイベントログに表示されます。
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ィルス、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 および SDA 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、アンチウィルスソフトウェアを実装するのは、ユーザーが所属する組織の責任です。
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 11.10 (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	ファイルおよびソフトウェア機能へのすべてのアクセスは、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、権限を持つユーザーまたはグループに対して適切なレベルのアクセス権限を割り当てます。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 ワークステーション、ICP-MS MassHunter アプリケーションソフトウェア、および SDA 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、電子署名機能において各ユーザーに一意のユーザー ID とパスワードの組み合わせを使用します。ユーザー ID は一意に設定する必要があり、別のユーザーへの使い回しや再割り当てをしてはなりません。これは、システムを導入および使用する組織の責任です。
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	この要件には、UAC/OLSS および Active Directory サービスを通してユーザー管理と統合することにより適合します。
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、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。監査証跡のエントリは、いずれのユーザーも無効化、変更、および削除できません。ICP-MS MassHunter UAC/OLSS ソフトウェアは、電子記録の一部としてタイムスタンプ付きの監査証跡を自動的に生成することにより、取り込みおよび分析操作の完全かつ正確な履歴を保持します。SDA は、アップロードされた MassHunter 監査証跡を保護できます。さらに、SDA はアップロードされた ICP-MS バッチのすべての更新に対して監査証跡エントリを生成します。
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、行われた変更の詳細、日付と時刻、および署名に関連付けられた理由（監査証跡マップ設定において、監査証跡エントリを起動する操作に理由が必要であると指定されている場合）が含まれています。

Part 11 またはその他	要件	可/不可	「可」の場合、具体的に要件がいかに満たされるか、 または「不可」の場合、ユーザーに推奨される事柄
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。	部分的	変更情報は、監査証跡エントリに記録されている以前の値と新しい値を介してメソッド設定で使用できます。MassHunter レポートでは変更フラグは直接にはサポートされていませんが、記録を元のエントリから変更または更新できるかどうかはバージョン番号から判別できます。
FDA GMP Part 211.194 8b	4.4 監査証跡には、試験で採用された、既成のメソッドに対するすべての変更が含まれますか。	可	既成のメソッドかどうかにかかわらず、メソッドに対する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	監査証跡マップの該当する操作に対して「理由」が選択されている場合、メソッドを変更した理由が記録されます。
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、常に有効にするように設定できます。監査証跡機能を有効にした後は、ICP-MS MassHunter の管理者権限を持つユーザーのみが無効にできます。通常のシステムオペレータは無効にできません。SDA 管理者の監査証跡ログは、SDA 管理者が表示できます。
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	監査証跡の記録はフィールドとして非常にわかりやすく記載されており、監査証跡に保存されているエントリは ICP-MS MassHunter 機能に固有ではないプレインランゲージで記述されています。SDA 管理者の監査証跡ログも非常にわかりやすく記載されています。
Annex 11、警告書による暗黙的要件（および多くの場合、お客様が要求）	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。	部分的	すべてのユーザー操作が記録されるため、監査証跡の内容を直接には設定できません。ただし、フィルタ機能を使用するとエントリをさらに簡単に表示できます。SDA 管理者の監査証跡の場合、ログは SDA 管理者が表示できます。ログはフィルタ処理できます。
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	ICP-MS MassHunter に新しい記録が加わると、既存の記録と以前に記録された監査証跡エントリの両方が保持されます。新しい記録は監査証跡ファイルに蓄積されます。その際、古い記録は変更されません。SDA 管理者の監査証跡の場合、ログは SDA 管理者が表示できます。ログは累積します。
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 と SDA の監査証跡の記録は SDA に保存されます。ICP-MS MassHunter のバッチ監査証跡は、ユーザーが規定した保持期間にわたりデータとともに保持されます。SDA 管理者の監査証跡の場合、ログは SDA 管理者が表示できます。ログはローカルディスクにアーカイブして、保持期間またはユーザーが規定した期間にわたり表示できます。
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	ICP-MS MassHunter の監査証跡ファイルは表形式で表示され、確認およびコピーのためにレポート形式にエクスポートできます。SDA 管理者の監査証跡の場合、ログは SDA 管理者が表示できます。
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が得られますか。	可	電子監査証跡はレポートとして印刷できます。ハードウェア構成、取り込みメソッド、データ分析メソッド、定量結果などのその他の記録は明確に印刷できます。SDA 管理者の監査証跡の場合、ログは SDA 管理者が表示できます。ログは印刷して xml ファイルにエクスポートできます。
5.動作およびデバイスの確認			
Part 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。	可	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。例えば、バッチ（サンプル分析シーケンス）を実行する前に、バッチをバリデーションして保存する必要があります。そうしない場合、バッチは実行できません。
Part 11.10 (g)、 Part 211、68 b	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。	可	ユーザーは、有効なユーザー名とパスワードがない場合、取り込み、データ処理、または確認のためにシステムにアクセスできません。ログインしたら、ファイルおよびソフトウェア機能（ファイルへの署名、値の入力、記録の変更が含まれますが、これに限定されるものではありません）へのユーザーアクセスは、UAC/OLSS で割り当てられている権限によって決定されます。
Annex 11、12.4	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。	可	監査証跡には、データ入力、変更、確認、または削除を行ったオペレータが日時とともに記録されます。SDA の場合、ログは SDA 管理者が表示できます。ログはこの目的で機能します。

Part 11 またはその他	要件	可/不可	「可」の場合、具体的に要件がいかに満たされるか、 または「不可」の場合、ユーザーに推奨される事柄
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	機器のシリアル番号が、ICP-MS 機器から ICP-MS MassHunter 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。さらに、ソースコンピュータ名はファイルに記録され、このファイルは ICP-MS MassHunter ソフトウェアから SDA にアップロードされます。データ転送の前に、デバイス「ハンドシェイク」が ICP-MS とアプリケーションホストコンピュータ間のリンクが正しいことを確認します。
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	アジレントでは会社の方針により、個人のトレーニングの記録を開示することを禁止しています。監査では、トレーニングプログラムの存在を確認できます。資料には、「アジレントの担当者はトレーニングされています…」と記載できます。 アジレント・テクノロジーの従業員の教育および雇用に関する履歴の記録は検証され、個人の記録として保持されます。 ICP-MS MassHunter ソフトウェアと SDA のエンドユーザーは、お客様のサイトでの教育、トレーニング、システムに関する経験の記録も保有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。またアジレントでは、追加のシステムトレーニングも提供しています。
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 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 次の内容を含む、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	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、システム関連の文書用の正式に記述されたリビジョンおよび変更の管理手順が含まれています。管理されている文書に対するすべての改訂は、タイムスタンプが付けられ、監査証跡の対象となります。
6.データの完全性、日時の正確性			
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 と SDA は、他のシステムとデータを交換しません。
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	データの正確性および検量線の妥当性チェックのような追加のチェックは、ユーザーが規定した適切な品質管理チェックを使用して確認できます。クオリファイア同位体の確認結果の報告のような、追加のチェックを使用できます。別のオペレータによるチェックなどの詳細なチェックは、ユーザーが所属する組織の責任です。
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 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（LAN/WAN に接続されている場合）から日付/時刻を取得します。オペレーティングシステムの日付/時刻の設定はユーザーが所属する組織の責任であり、SoP を使用して管理する必要があります。 ユーザーが行ったローカル OS の日付/時刻への変更は、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 および SDA 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（LAN/WAN に接続されている場合）から日付/時刻を取得します。ローカル PC の日付/時刻設定にアクセスして変更できるのは、PC にアクセスする権限を持つユーザー（有効なユーザーログオン）のみです。これはシステムのイベントログに記録されるため、確認できます。通知は自動的には送信されません。
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 と SDA はシングル PC システムであるため、複数のタイムゾーンにはまたがりません。ICP-MS MassHunter の監査証跡は、現地時間 + UTC からの差、例えば、「2012 年 3 月 1 日、木曜日、午後 6 時 52 分 21 秒（UTC + 09:00）」を使用して記録されます。SDA は、タイムゾーンに関する情報を保存します。

Part 11 またはその他	要件	可/不可	「可」の場合、具体的に要件がいかに満たされるか、 または「不可」の場合、ユーザーに推奨される事柄
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 11.3	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 と SDA は、オープンシステムとして動作するようには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 と SDA は、オープンシステムとして動作するようには設計されていません。
8.電子署名 – 署名の明示および署名/記録の関連付け			
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。	可	企業内での電子署名の使用および効力は、ユーザーが所属する組織の責任です。 電子署名は該当する記録に永久的に関連付けられており、適用された日付/時刻（および必要に応じて、理由）が含まれています。
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	ICP-MS MassHunter と SDA によって作成された電子記録には、ユーザー名、日付と時刻、署名に関連付けられた理由（監査証跡マップで理由を選択した場合）が含まれています。
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、それらの項目は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 ソフトウェアで適用された電子署名は、アプリケーションの画面および印刷されたレポートで確認できます。SDA は、電子記録に適用された電子署名を表示できます。
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	ICP-MS MassHunter のファイルには、ICP-MS MassHunter ソフトウェアで電子的に署名できます。電子署名は、解読できないようにファイルに関連付けられています。システムの電子署名プラグイン以外で適用された署名は認識されません（手書き署名など）。
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 は、アプリケーションを再開するためにユーザーログオン（ユーザー名とパスワード）を必要とする、設定可能な時間ベースのロック機能を備えています。
9.電子署名の一般要件と署名の構成要素および管理			
Part 11.100 (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、電子署名機能において各ユーザーに一意のユーザー ID とパスワードの組み合わせを使用します。ユーザー ID は一意に設定する必要があり、別のユーザーへの使い回しや再割り当てをしてはなりませんこれは、システムを導入および使用する組織の責任です。
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 またはその他	要件	可/不可	「可」の場合、具体的に要件がいかに満たされるか、 または「不可」の場合、ユーザーに推奨される事柄
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	電子署名ツールでは、ファイルに署名を適用する前に一意のユーザー ID とパスワードという 2 つの識別構成要素が必要です。
Part 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。	可	通常、ユーザーは各記録に個別に電子的に署名しますが、これはユーザーの都合に合わせて設定可能です。制御されたアクセスの連続的な期間内に、1 つの署名を一連の操作に適用できるように、設定可能な「猶予時間」が用意されています。初回の電子署名の際に、ユーザーは一意のユーザー ID とパスワードという 2 つの識別構成要素を入力する必要があります。
Part 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。	可	通常、ユーザーは各記録に個別に電子的に署名する必要がありますが、これはユーザーの都合に合わせて設定可能です。制御されたアクセスの連続的な期間の猶予時間中、ユーザーは一意のユーザー ID とパスワードを入力する必要はありません。猶予時間が「0」に設定されている場合、ユーザーは以降の操作ごとにユーザー ID とパスワードを入力する必要があります。
Part 11.200 (a) (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。	可	ユーザーは、各記録に個別に電子的に署名する必要があります。毎回の電子署名の際に、ユーザーは一意のユーザー ID とパスワードという 2 つの識別構成要素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	システムの管理者が、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。システムでは、2 名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持つことを許可していません。ユーザー ID とパスワードを所有者本人のみが使用しており、共有されていないことを確認するのはユーザーが所属する組織の責任です。
Part 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。	可	ユーザー ID とパスワードはともに、ユーザーに対して一意に保持されています。ユーザーを設定する際にユーザー ID を知り得るのは、システム管理者のみです。各ユーザーは初回ログオン時に、自分のみが知り得る一意のパスワードを設定する必要があります。個人の電子署名の使用を所有者本人以外が試みる場合、パスワードを共有する目的で積極的に協力する必要があります。
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	システムが設定した電子署名は、バイオメトリックスには基づいていません。

Part 11 またはその他	要件	可/不可	「可」の場合、具体的に要件がいかに満たされるか、 または「不可」の場合、ユーザーに推奨される事柄
10.識別コードとパスワードの管理			
Part 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。	可	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を使用する必要があります。権限を持つユーザーがアカウント情報を共有していないこと、および他人によってアクセスされていないことを確認するのはユーザーが所属する組織の責任です。OLSS のユーザー管理では、2 名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許可していません。
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	ユーザーのアクセス管理には OLSS を使用しています。OLSS のパスワードポリシー設定では、パスワードの更新間隔を設定できます。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 UAC/OLSS は、ID コードまたはパスワードを生成するためにトークン、カード、その他のデバイスは使用していません。
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 のセキュリティポリシーは、不正アクセスの試行回数が、ユーザーによって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、このことをシステム管理者に通知できます。システムの監査証跡は、コンピュータやアプリケーションへのログオン試行またはユーザーの変更などの一般的なイベントを、すべてのセキュリティ情報の集中型監査リポジトリとしてシステムのイベントログに文書化します。この中には、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 が含まれており、セキュリティ違反の可能性を即座にチェックできます。セキュリティ情報の不正使用の監視と報告は、ユーザーが所属する組織の責任です。
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 UAC/OLSS は、ID コードまたはパスワードを生成するためにトークン、カード、その他のデバイスは使用していません。
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 UAC/OLSS および SDA ソフトウェアが現行の Agilent LSCA 製品ライフサイクルリビジョンおよび ISO QMS 証明書で規定されている品質管理システムの下で開発されており、製品試験および適格性評価サービス時に実施した試験を文書化していることを証明する文書を保持しており、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、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 ソフトウェアは、下請業者が開発もサポートもしていません。
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 ソフトウェアは、下請業者が開発もサポートもしていません。
ICH Q10、2.7 c	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。	N/A	Agilent ICP-MS MassHunter ソフトウェアは、下請業者が開発もサポートもしていません。

21 CFR Part 11 から取得した説明：
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

カストマコンタクトセンタ

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。

アジレント・テクノロジー株式会社

Printed in Japan, March 12, 2021
5991-2002JAJP
DE44243.0431712963

Agilent
Trusted Answers