Analyst MD ソフトウェア

ラボ管理者ガイド

IVD-IDV-05-0252-JA-E

2022 年 4 月

本書は SCIEX 機器をご購入され、実際に使用されるお客様にむけてのものです。本書の著作権は保護されています。本書および本書の一部分を複製することは、SCIEX が書面で合意した場合を除いて固く禁止されています。

本書に記載されているソフトウェアは、使用許諾契約書に基づいて提供されています。使用許諾契約書で特に許可されている場合を除き、いかなる媒体でもソフトウェアを複製、変更、または配布することは法律で禁止されています。さらに、使用許諾契約書では、ソフトウェアを逆アセンブル、リバースエンジニアリング、または逆コンパイルすることをいかなる目的でも禁止することがあります。正当とする根拠は文書中に規定されているとおりです。

本書の一部は、他の製造業者および/またはその製品を参照することがあります。これらには、その名称を商標として登録しているおよび/またはそれぞれの所有者の商標として機能している部分を含む場合があります。そのような使用は、機器への組み込みのため SCIEX により供給された製造業者の製品を指定することのみを目的としており、その権利および/またはライセンスの使用を含む、または第三者に対しこれらの製造業者名および/または製品名の商標利用を許可するものではありません。

SCIEX の保証は販売またはライセンス供与の時点で提供される明示的保証に限定されており、また SCIEX の唯一かつ独占的な表明、保証および義務とされています。SCIEX は、明示的・黙示的を問わず、制定法若しくは別の法律、または取引の過程または商慣習から生じるかどうかに関わらず、特定の目的のための市場性または適合性の保証を含むがこれらに限定されない、他のいかなる種類の保証も行いません。これらのすべては明示的に放棄されており、購買者による使用またはそれから生じる不測の事態に起因する間接的・派生的損害を含め、一切の責任または偶発債務を負わないものとします。

IVD

CE

UK CA

***In Vitro* 診断用です。**製品は一部の国では入手できません。詳細な情報については、最寄りの営業担当者にお問い合わせいただくか、または sciex.com/diagnostics を参照してください。

Rx only.

ここに記載されている商標および / または登録商標は、関連するロゴを含め、米国および / またはその他の特定の国における AB Sciex Pte. Ltd.、またはその該当する所有者の所有物です(sciex.com/trademarks をご覧ください)。

AB Sciex™ はライセンスの下で使用されています。

© 2022 年 DH Tech. Dev. Pte. Ltd.

EC REP

Leica Microsystems CMS GmbH
Ernst-Leitz-Strasse 17-37
35578 Wetzlar
Germany

AB Sciex Pte. Ltd.
Blk33, #04-06 Marsiling Industrial Estate Road 3
Woodlands Central Industrial Estate, Singapore 739256

目次

第 1 章 : はじめに 6

第 2 章 : セキュリティ構成の概要 7
セキュリティと監督法規の遵守 7
セキュリティ要件 7
Analyst MD ソフトウェアおよび Windows のセキュリティ: 互いに連動 7
Analyst MD ソフトウェアおよび Windows 内の監査証跡 7
MultiQuant MD ソフトウェアの監査証跡 8
21 CFR Part 11 8
システム構成 9
Windows セキュリティ構成 9
ユーザーとグループ 9
Active Directory への対応 9
Windows ファイルシステム 10
システム監査 10
ファイルおよびフォルダアクセス許可 10
イベントログ 10
Windows アラート 11

第 3 章 : 電子ライセンス 12

第 4 章 : Analyst MD ソフトウェアセキュリティの構成 13
ソフトウェアセキュリティのワークフロー 13
Analyst MD ソフトウェアのインストールのインストール 14
ソフトウェアコンポーネントを検証する 15

第 5 章 : Analyst MD ソフトウェアのセキュリティ構成 16
Analyst MD ソフトウェアを構成するためのステップ 16
セキュリティ情報の場所 16
Security Mode とアカウントについて 16
Security Mode を選択する 17
測定用アカウントを選択する 19
画面ロックと自動ログアウトを設定する 20
Analyst MD ソフトウェアのロックを解除するか、ログオフします 21
Analyst MD ソフトウェアへのアクセス 21
職員と役割について 22
Analyst MD ソフトウェアアクセス 24
MultiQuant MD ソフトウェアへのアクセス 35
Analyst MD ソフトウェアにユーザーまたはグループを追加します。 39
役割を変更する 39

Analyst MD ソフトウェアから職員を削除する 40
カスタム役割の作成 40
カスタム役割の削除 41
アクセスを設定する 41
測定用コンピュータとクライアントコンピュータにおける Windows ファイアウォール構成 45
リモートワークステーション 47
セキュリティ構成を印刷する 52

第 6 章：システム健全性の監視 53
補助トレース 53
補助トレースを有効にする 53
補助トレースを表示する 53
注入カウンタ 54
注入カウンタを有効にする 54

第 7 章：監査 56
監査証跡 56
監査マップ 57
監査マップの設定 58
インストール済みの監査マップ 59
監査マップの作業を行う 60
監査マップを作成する 60
監査マップを変更する 62
他のプロジェクトから監査マップをコピーする 62
監査マップを適用する 63
監査証跡の表示、印刷、検索 63
監査証跡の表示 63
Results Table に埋め込まれた監査構成を表示する 64
装置監査証跡の監査レコードの詳細を表示する 64
アーカイブ済み監査証跡の表示 65
監査証跡の印刷 65
監査レコードを検索する 65

付録 A：監査証跡 67
監査証跡レコード 67
監査証跡アーカイブ 67
装置監査証跡イベント 68
プロジェクト監査証跡イベント 69
定量化監査証跡イベント 70
AAC 監査証跡 71

付録 B：セキュリティを追加でカスタマイズする 72
データファイルの変更（Explore Processing） 72
Explore Processing History ファイルを作成する 72
Explore Processing History ファイルを表示する 73
装置メンテナンスログエントリを追加する 73
装置メンテナンスログエントリを表示する 73

メール通知を構成する 74
データファイルのチェックサム 75
データファイルのチェックサムを検証する 75
データファイルのチェックサム機能を有効または無効にする 75

付録 C：特別測定用アカウント 77

お問い合わせ先 78
お客様のトレーニング 78
オンライン学習センター 78
SCIEX サポート 78
サイバーセキュリティ 78
ドキュメント 78

はじめに 1

本書に記載されている情報は、主に以下の 2 種類の担当者を対象としています。

- ラボ管理者（機能面で Analyst MD ソフトウェアと付属装置の毎日の操作および使用に携わっている人物）
- システム管理者（システムセキュリティ、ならびにシステムとデータの整合性に関する作業に携わっている人物）

セキュリティ構成の概要 2

このセクションでは、Analyst MD ソフトウェアのアクセス制御および監査コンポーネントが、Windows アクセス制御および監査コンポーネントと併せてどのように機能するかについて説明します。また、Analyst MD ソフトウェアをインストールする前に Windows セキュリティを構成する方法についても説明します。

セキュリティと監督法規の遵守

セキュリティ要件

セキュリティ要件の内容は、リサーチラボや学術機関ラボなどの比較オープンな環境から、臨床ラボといった厳しい規制が課せられる環境に至るまでさまざまです。

Analyst MD ソフトウェアおよび Windows のセキュリティ: 互いに連動

Analyst MD ソフトウェアと Windows New Technology File System (NTFS)には、システムとデータへのアクセスを制御するように設計されたセキュリティ機能があります。

Windows セキュリティは、ログオン時に固有のユーザー ID とパスワードを入力するようユーザーに要求することで、第一線の保護として機能します。その結果、Windows ローカルまたはネットワークのセキュリティ設定で認識されたユーザーのみがアクセスできるようになりました。詳細な情報については、次のセクションを参照:Windows セキュリティ構成。

Analyst MD ソフトウェアには、セキュリティが向上した 3 種類のシステムアクセスモードが用意されています。

- シングルユーザーモード
- 混合モード
- 統合モード(デフォルト設定)

セキュリティモードとセキュリティ設定の詳細な情報については、次のセクションを参照:Security Mode とアカウントについて。

Analyst MD ソフトウェアの役割は Windows のユーザーグループから分離しているため、フル構成できます。役割を使用することにより、ラボのディレクターは、機能ごとにソフトウェアと質量分析装置へのアクセスを制御できます。詳細な情報については、次のセクションを参照:Analyst MD ソフトウェアへのアクセス。

Analyst MD ソフトウェアおよび Windows 内の監査証跡

Analyst MD 内の監査機能は、Windows 内蔵監査コンポーネントと併せて、電子記録の作成および管理に欠かせない要素となります。

Analyst MD ソフトウェアは、電子記録保持の要件を満たすための、監査証跡のシステムを提供します。監査証跡レコードは以下のように分けられます。

- 質量キャリブレーションテーブルまたは分解能テーブルの追加または置き換え、システム構成の変更、セキュリティイベント、装置メンテナンスログへのエントリ。
- プロジェクト、チューニング、バッチ、データ、測定メソッド、定量化メソッド、Results Tables、レポートテンプレートファイルの作成や修正イベント、およびモジュールの起動、終了、印刷イベント。監査証跡に記録される削除イベントは、リモートビューアの装置の削除、Analyst MD ソフトウェアでのユーザーの削除、ユーザータイプの削除、およびプロジェクトの役割の削除です。
- Results Table に埋め込まれた定量メソッドの作成と修正、Results Table のサンプル情報の修正、ピーク積分パラメータの修正。

監査イベントの完全なリストについては、次のセクションを参照：監査証跡レコード。

Analyst MD ソフトウェアは次を使用します。アプリケーションイベントログを用いて、ソフトウェアの動作に関する情報がキャプチャされます。このログには質量分析装置、デバイス、ソフトウェアのインタラクションに関する詳細が記録されるため、トラブルシューティング時のサポートとしても使用できます。

Windows で維持されるイベントログには、セキュリティの範囲、システム、アプリケーション関連のイベントがキャプチャされます。大半の Windows 監査は、ログオン障害といった例外的なイベントをキャプチャするよう設計されています。管理者は、幅広いイベント（特定のファイルへのアクセスや Windows 管理アクティビティなど）がキャプチャされるよう同システムを構成できます。詳細な情報については、次のセクションを参照：システム監査。

MultiQuant MD ソフトウェアの監査証跡

MultiQuant MD ソフトウェアには、MultiQuant MD ソフトウェア内の作成および変更イベントを監査する独自の監査証跡が含まれています。監査証跡機能は、MultiQuant MD ソフトウェアの 21 CFR Part 11 ライセンスでのみ使用できます。

21 CFR Part 11

Analyst MD ソフトウェアには、21 CFR Part 11 をサポートするための次の実装を備えた技術制御が含まれています:

- 「Mixed Mode」と「Integrated Mode」セキュリティを Windows セキュリティーとリンク。
- 役割をカスタマイズすることで機能へのアクセスを制限。
- プロジェクトへのアクセスを役割ごと、またはグループベースで制限。
- 装置の稼働、メンテナンス、データ収集、データのレビュー、レポートの生成に関する監査証跡を維持。
- ユーザー ID とパスワードの組み合わせを用いた電子署名。
- Windows オペレーティングシステムの適切な構成。
- 社内で適切な手順を設け、トレーニングを実施。

Analyst MD ソフトウェアは、21 CFR Part 11 準拠システムの一部として使用できるよう設計されているほか、21 CFR Part 11 準拠を満たすよう構成することも可能です。Analyst MD ソフトウェアの使用が 21 CFR Part 11 に準拠しているかどうかは、ラボでの Analyst MD ソフトウェアの実際の用途や構成に左右されます。

ご希望であれば、SCIEX Professional Services を介して検証サービスをご利用になれます。詳細な情報については、complianceservices@sciex.com までお問い合わせください。

システム構成

システムは通常、ネットワーク管理者、またはネットワーク権限と管理権限を持つ職員によって構成されます。

Windows セキュリティ構成

Analyst MD ソフトウェアを使用してセキュリティを管理できるようにするには、管理者はプロジェクトフォルダとそのすべてのサブフォルダのファイル権限を変更できる必要があります。ルートディレクトリがローカルコンピュータ上にない場合、ソフトウェア管理者をローカル管理者グループの一員とすることができます。セキュリティを管理する Analyst MD ソフトウェアユーザーのみがローカル管理者グループに所属している必要があります。

Analyst MD ソフトウェアが意図したとおりに動作するには、ユーザーは Microsoft Windows ローカルユーザーグループの一員でなくてはなりません。

注: ネットワークの取得は、Analyst MD ソフトウェアではサポートされていません。

ユーザーとグループ

Analyst MD ソフトウェアでは、プライマリードメインコントローラのセキュリティデータベースまたは Active Directory に記録されたユーザー名とパスワードが使用されます。パスワードは Windows に付属のツールを用いて管理されます。職員と役割の設定についての詳細な情報については、次のセクションを参照：Analyst MD ソフトウェアへのアクセス。

Active Directory への対応

Active Directory は混合環境またはネイティブ環境のいずれかで機能します。Analyst MD ソフトウェアセキュリティ構成ウィンドウと Analyst MD ソフトウェアセキュリティ データベースで、ユーザーアカウントを UPN (ユーザー プリンシパル名) 形式で指定します。

混合環境

Analyst MD ソフトウェアが混合環境で起動した場合、Log on ウィンドウに User Name、Password、Domain フィールドが表示されます。

これには以下のパラメータが含まれます。

- Windows 2008 R2 および 2012 サーバー。
- Windows 10、64 ビットクライアント.

ネイティブ環境

Analyst MD ソフトウェアがネイティブ環境で起動する場合、ドメインフィールドは表示されず、Analyst MD ソフトウェアは UPN 形式のユーザー名のみを受け入れます。Analyst MD ソフトウェアの Status ウィンドウにも、ユーザー名が UPN 形式で表示されます。

これには以下のパラメータが含まれます。

- Windows 2008 R2 および 2012 サーバー。
- Windows 10、64 ビットクライアント.

Windows ファイルシステム

Analyst MD ソフトウェアでは、ファイルとディレクトリは NTFS としてフォーマットされたハードディスクパーティションに保存する必要があります。これにより、Analyst MD ソフトウェアのファイルへのアクセスを制御および監査することができます。FAT ファイルシステム（FAT）では、フォルダまたはファイルへのアクセスを制御および監査することはできないため、安全性が重視される環境には適していません。

システム監査

Windows システムの監査機能を有効にすることで、セキュリティ違反またはシステムへの侵入を検出することができます。監査では、さまざまなタイプのシステム関連イベントを記録するよう設定できます。たとえば、監査機能を有効にして、システムへのログオンに失敗したか成功したかをイベントログに記録することができます。

ファイルおよびフォルダアクセス許可

ネットワークドライブのセキュリティを管理するには、Analyst MD ソフトウェア管理者が、フォルダとすべてのサブフォルダのアクセス許可を変更する権限を持っている必要があります。
`Analyst Data` このアクセスはネットワーク管理者が構成する必要があります。

監査対象となるイベントまたはアクションを選択する前に、ファイルとフォルダのアクセス許可を設定します。フォルダアクセス許可は、フォルダ内のサブフォルダとファイルに適用できます。ファイルおよびフォルダのアクセス許可を設定したら、セキュリティログに記録されるイベントについて定義します。

注: アクセスユーザーが必要とするドライブと各コンピュータのフォルダのレベルを考慮してください。共有の許可と他の関連許可も構成します。ファイル共有の詳細な情報については、Windows ドキュメントを参照してください。

Analyst MD ソフトウェアファイルとフォルダアクセス許可については、次のセクションを参照：
Analyst MD ソフトウェアのセキュリティ構成。

イベントログ

Analyst MD ソフトウェアまたは Windows 管理ツールから Windows イベントビューアを開きます。Windows Event Viewer では、監査済み Windows イベントがセキュリティログ、システムログ、アプリケーションログに記録されます。

ヒント! Analyst MD ソフトウェアからイベントビューアを開くには、**View** > **Event Log.**をクリックします。

イベントログは以下のようにカスタマイズします。

- 適切なイベントログサイズを設定します。
- 古いイベントの自動上書きを有効にします。

- Windows コンピュータのセキュリティを設定します。

レビューおよび保管のプロセスを導入することができます。セキュリティ設定と監査ポリシーの詳細な情報については、Windows ドキュメントを参照してください。

Windows アラート

システムまたはユーザー関連の問題が発生した場合に、同一または別のコンピュータ上で、自動メッセージを指定した人物（システム管理者など）に送信するためのネットワークを設定します。

- 送信側と受信側の両方のコンピュータで、Windows サービスのコントロールパネルで Messenger を起動します。
- 送信側コンピュータで、Windows サービスコントロールパネルのアラートサービスを開始します。

アラートオブジェクトの作成の詳細な情報については、Windows ドキュメントを参照してください。

電子ライセンス 3

電子ライセンスは、ノードロックのみ可能です。

今後のサービスやサポートコールで、アクティベーション ID が必要となることがあります。ノードロックライセンスまたはサーバーベースライセンスのアクティベーション ID にアクセスするには:

- Analyst MD ソフトウェアウィンドウで **Help** > **About Analyst** をクリックします。

注: ライセンスが期限切れになる前に更新してください。

Analyst MD ソフトウェアセキュリティの構成 4

このセクションでは、ソフトウェアを構成する方法について説明します。

注: ユーザーは、ソフトウェアがインストールされているコンピュータのローカル管理者権限を持っている必要があります。

ソフトウェアセキュリティのワークフロー

Analyst MD ソフトウェアは、Windows 管理ツールのセキュリティ、アプリケーション、システムイベント監査コンポーネントと併せて機能します。

セキュリティは以下のレベルで構成されます。

- Windows 認証:コンピュータへのアクセス。
- Windows 認証:ファイルとフォルダへのアクセス。
- Analyst MD ソフトウェアへのアクセス。
- Analyst MD ソフトウェア機能への選択的アクセス。
- 特定のプロジェクトへのアクセス。
- 装置用ワークステーションの状態へのアクセス。

セキュリティを設定するためのタスクのリストについては、次を参照:表 4-1。さまざまなセキュリティレベルを設定するためのオプションについては、次を参照:表 4-2。

表 4-1 : セキュリティの構成におけるワークフロー

タスク	処置
Analyst MD ソフトウェアをインストールします。	*Analyst MD Software Installation Guide* のドキュメントを参照してください。
Analyst MD ソフトウェアのセキュリティを構成します。	次のセクションを参照:Analyst MD ソフトウェアのセキュリティ構成。
監査証跡を構成します。	次のセクションを参照:監査。
Windows ファイルセキュリティと NTFS を構成します。	次のセクションを参照:アクセスを設定する。
装置、セキュリティ、データ、プロセスメンテナンス用のシステムメンテナンスログを維持。	次のセクションを参照:セキュリティを追加でカスタマイズする。

表 4-2 : セキュリティ構成のオプション

オプション	CFR21 Part 11
Windows セキュリティ	
ドライブを NTFS 形式でフォーマット。	Yes
ユーザーとグループを構成します。	Yes
Windows の監査、ならびにファイルとディレクトリの監査を有効化します。	Yes
ファイルアクセス権限を設定します。	Yes
Analyst MD ソフトウェアインストール	
Analyst MD ソフトウェアをインストールします。	Yes
MultiQuant MD ソフトウェアをインストールします。	Yes
監査オプションの選択。	Yes
Event Viewer（インストールの検査）	Yes
Analyst MD ソフトウェアセキュリティ	
Security Mode の選択。 **注:** CFR 準拠環境では、シングルユーザーモードの使用は推奨されません。	統合または混合
Analyst MD ソフトウェアの役割と担当者を設定します。	Yes
監査マップの作成、装置、プロジェクト、定量監査証跡の構成。	Yes
メール通知の構成。	Yes
チェックサムの有効化。 **注:** チェックサム機能は、Analyst MD ソフトウェアの新規インストールでデフォルトで有効になっています。	Yes
共通タスク	
新規プロジェクトおよびサブプロジェクトの追加。	Yes
新規プロジェクトおよびサブプロジェクト向けにプロジェクト監査証跡を構成。	Yes
既存のデータの転送。	Yes
装置のセキュリティ、データ、プロセスメンテナンス用のメンテナンスログを作成。	Yes

Analyst MD ソフトウェアのインストールのインストール

Analyst MD をインストールする前に、ソフトウェアインストール DVD または Web ダウンロードパッケージで入手できる次のドキュメントをお読みください : *ソフトウェアインストールガイド*および*リリースノート*。処理コンピュータと測定コンピュータの違いを理解したうえで、適切なインストールシーケンスを実行します。

注: Windows のコンポーネントに変更が加えられることを防ぐため、アプリケーション用コンピュータの Windows の更新機能およびインターネット接続を無効にしておくことをお勧めします。更新機能およびインターネット接続が無効になっていない場合は、Windows または.NET framework の更新後にシステムを検証する必要があります。測定用コンピュータには、セキュリティの変更など、重要な Windows Updates のみをインストールすることを強く推奨します。システムの機能がウイルスによって損なわれないよう、十分なウイルス保護対策が実施されていることを確認してください。

Windows の要件

- Windows 10 オペレーティングシステムの英語版にのみ対応しています。別のデフォルト言語を使用すると、ファイル情報や監査証跡が正しく表示されない場合があります。
- Region and Language の設定で、**English (United States)** が第一言語として設定されていることを確認します。

システム要件

最小インストール要件については、*『ソフトウェアインストールガイド』*のドキュメントを参照してください。

プリセット監査オプション

インストールされている監査マップの説明については、次のセクションを参照：インストール済みの監査マップ。インストール後、Analyst MD ソフトウェア管理者は、セキュリティ構成モジュールで選択を変更したり、Audit Trail Manager で監査マップを構成したりできます。

ソフトウェアコンポーネントを検証する

Analyst MD ソフトウェアがインストールされた後、Software Component Verification 手順によって、すべてのソフトウェアコンポーネントがインストールされていることが確認された後、インストールレポートが生成されます。このレポートは、Event Viewer アプリケーションログの Analyst MD インストーラからのイベントログアイテムです。完了したら、インストールが成功したことをただちに検証してください。

コアインストールファイルのチェックサム検査を対象としたイベントログもあります。チェックサムの詳細な情報については、次のセクションを参照：データファイルのチェックサム。

1. **Start** > **Control Panel.**をクリックします
2. **Administrative Tools** をダブルクリックして、**Event Viewer** をダブルクリックします。
3. **Tree** タブで、**Application Log** をクリックします。
4. **Source** カラムの **Analyst Installer** イベントをクリックします。
5. Event Detail メッセージの **Description** フィールドから、**Total files verified** に移動します。エラーはゼロと測定されなければなりません。

Analyst MD ソフトウェアのセキュリティ構成 5

このセクションでは、Analyst MD ソフトウェアのセキュリティを設定する方法について説明します。

注: Analyst MD ソフトウェアのセキュリティ構成への変更は、Analyst MD ソフトウェアの再起動後に有効になります。

Analyst MD ソフトウェアを構成するためのステップ

ヒント! Security Configuration ダイアログでさまざまなタスクを実行するときは、別のタブに移動する前に、必ず各タブの **Apply** をクリックして変更を保存してください。

Analyst MD ソフトウェアを設定するための一般的なタスクについては、次の表を参照: 表 5-1

表 5-1 : Analyst MD ソフトウェアの構成タスク

タスク	次を参照
セキュリティモードの構成。	Security Mode を選択する。
画面ロックと自動ログアウトの構成(混合モードのみ)。	画面ロックと自動ログアウトを設定する。
プロジェクトセキュリティの構成。	アクセスを設定する。
装置ワークステーションの構成	ワークステーションにアクセスを追加する または ワークステーションにアクセスを削除する。

セキュリティ情報の場所

Analyst MD ソフトウェアが単一のコンピュータまたはネットワーク構成で実行されている場合、すべてのセキュリティ情報は、コンピュータ上の次のフォルダーにある `SecurityDB.odb` ファイルに保存されます:

- `C:\Program Files (x86)\Analyst\Bin`

Security Mode とアカウントについて

このセクションでは、Security Configuration ダイアログの Security タブに示されるオプションについて説明します。

Single User Mode: 現在 Analyst MD ソフトウェア管理者として Windows にログオンしているユーザーは、Analyst MD ソフトウェアのすべての機能にフルアクセスできます。コンピュータの Windows に正常にログオンできるユーザーは、Analyst MD ソフトウェアの管理者権限を持っています。

統合モード：Windows に現在ログオンしているユーザーは、Windows ユーザーが有効な Analyst MD ソフトウェアユーザーでもある場合に限り、Analyst MD ソフトウェアにアクセスできます。

Mixed Mode：現在 Analyst MD ソフトウェアにログオンしているユーザーは、現在 Windows にログオンしているユーザーと同じであっても、異なっていてもかまいません。Analyst MD ソフトウェアにログオンしたユーザーは、統合モードと同じ方法で、指定されたロールに割り当てることができます。これにより、既知のパスワードを使用して Windows のグループログオンを使用できるようになりますが、Analyst MD ソフトウェアのユーザーは、一意のユーザー名、パスワード、および必要に応じてドメインを使用して Analyst MD ソフトウェアにログオンする必要があります。

Mixed Mode が選択されている場合、Screen Lock and Auto Logout 機能を使用できます。

測定用アカウント：通常の測定時にデータを読み取ってプロジェクトフォルダに書き込むために使用するネットワークアカウントです（チューニング時を除く）。ネットワーク管理者は、ネットワークアカウントに対して適切なアクセス権限を付与する必要があります。測定用アカウントでは、クライアントアカウントまたは特別取得用管理者アカウントのいずれかの権限を使用します。

クライアントアカウント：データ収集のために Analyst MD ソフトウェアにログオンするために使用したのと同じアカウントを使用します。統合モードでは、Windows にログオンしたユーザーは、Analyst MD ソフトウェアにもログオンします。Mixed mode では、Windows ユーザーと Analyst MD ソフトウェアユーザーは異なる場合があります。

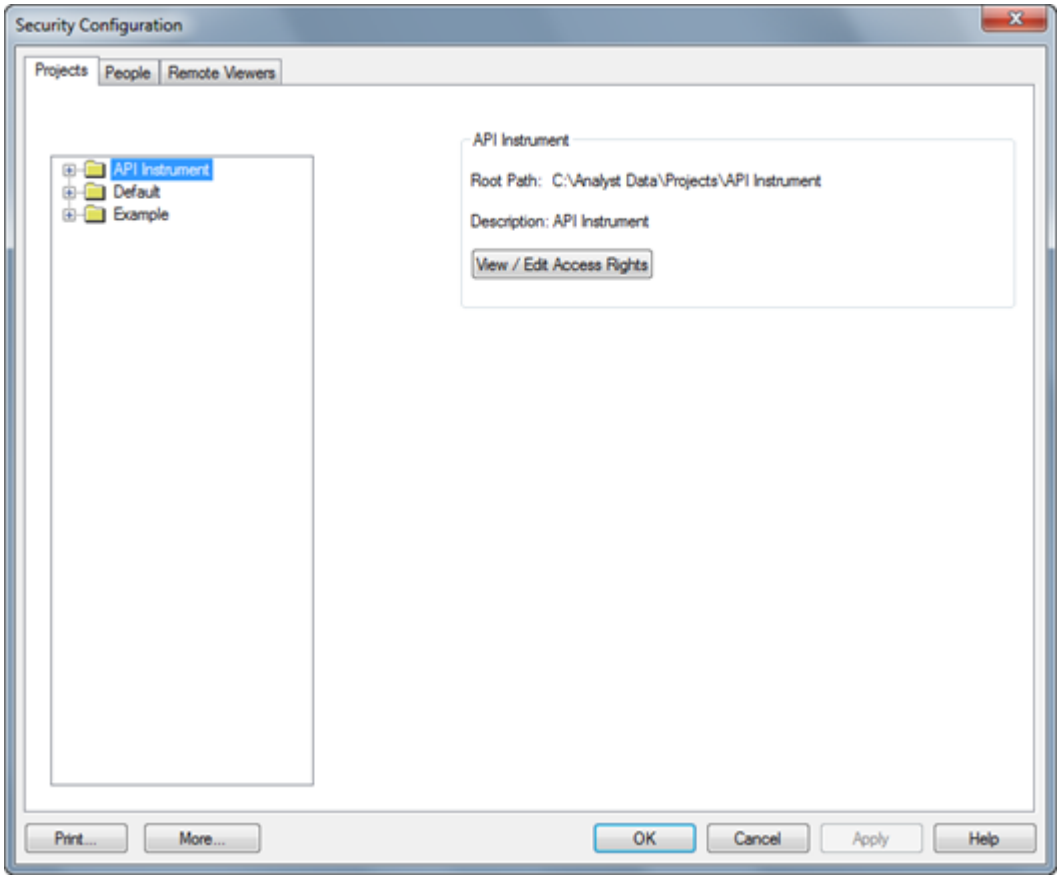
特別な取得管理者アカウント： Analyst MD ソフトウェアを使用する場合、ネットワーク取得はお勧めしません。この機能は、規制環境下で使用されることを意図しています。オペレータは、このパスワードのユーザー名、ドメイン、パスワードを入力する必要があります。ネットワーク管理者がこのアカウントを設定すると、Analyst MD ソフトウェアの現在のユーザーの ID に関係なく、このアカウントを使用してデータを取得できます。たとえ現在のユーザーに Data フォルダ内のデータを修正する権限がなくても、データ収集が実行されます。アカウント情報は暗号化されたうえでレジストリに保存されます。次のセクションを参照：特別測定用アカウント。

Screen Lock and Auto Logout：セキュリティ上の理由から、一定期間操作が行われていない場合にコンピュータの画面をロックするように設定できます。自動ログアウト時間を設定することもできます。この場合、一定期間操作がないと Analyst MD ソフトウェア クライアントが閉じます。Screen Lock and Auto Logout は、Mixed Mode でのみ使用できます。

Security Mode を選択する

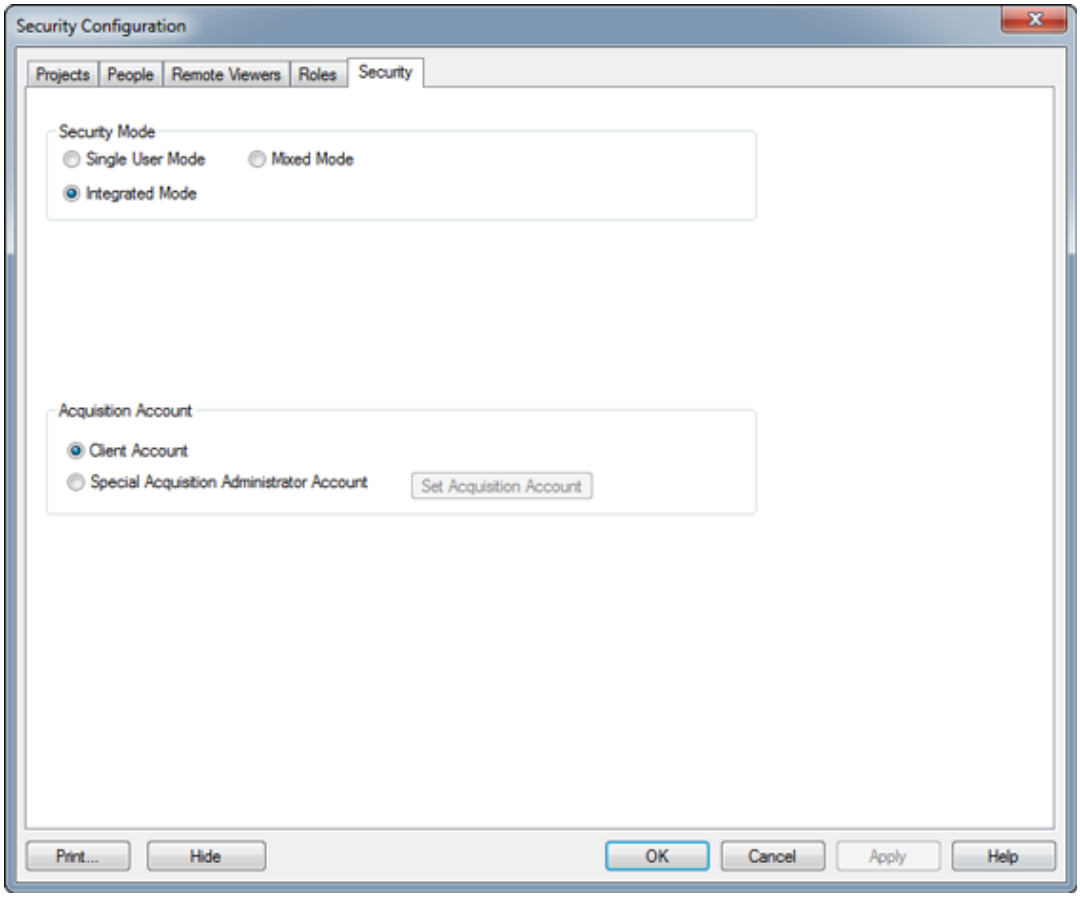
1. Navigation バーの **Configure** の下にある **Security Configuration** をダブルクリックします。

図 5-1 : Security Configuration ダイアログ : Projects タブ



2. **More** をクリックし、Security タブを開きます。

図 5-2 : Security Configuration ダイアログ:Security タブ



3. Security Mode グループでモードを選択し、**OK** をクリックします。
4. Analyst MD ソフトウェアを再起動します。

測定用アカウントを選択する

1. Navigation バーの **Configure** の下にある **Security Configuration** をダブルクリックします。
2. **More** をクリックし、Security タブを開きます。
3. Acquisition Account グループで、測定用アカウントを選択します。
4. **Special Acquisition Administrator Account** を選択した場合は、次を指定します。
   a. **Set Acquisition Account** をクリックします。
   b. **Password**、**User name**、さらに必要に応じて **Domain** と入力し、**OK** をクリックします。

   Active Directory がネイティブ環境で使用されている場合、ドメインフィールドは表示されず、ユーザー名は UPN 形式で入力できます。
5. **OK** をクリックします。

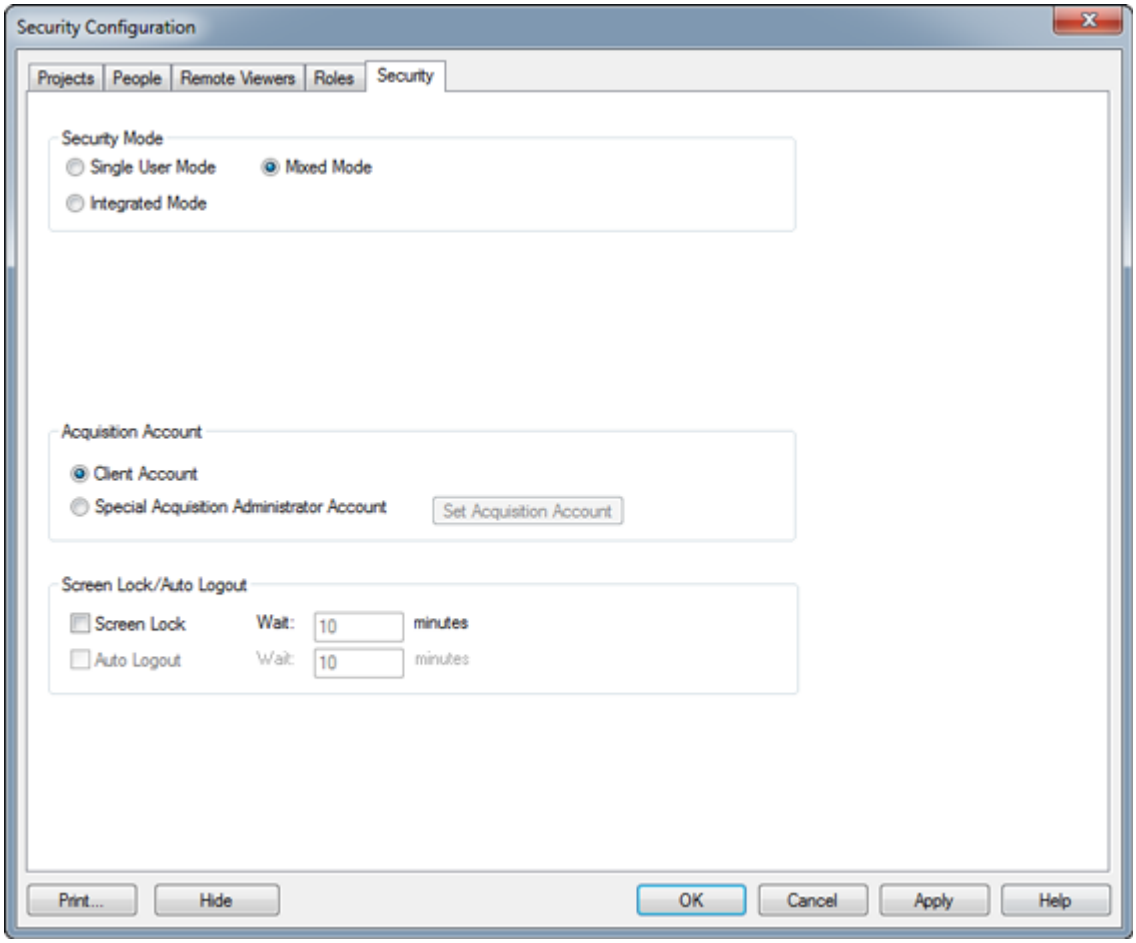
画面ロックと自動ログアウトを設定する

画面がロックされると、Unlock Analyst ダイアログが開き、システムがロックされていること、および現在ログオンしているユーザーの名前とドメインが表示されます。自動ログアウトオプションも設定されている場合は、Analyst MD ソフトウェアが閉じるまでの残り時間も表示されます。現在ログオンしているユーザー、または管理者またはスーパーバイザーの役割を持つユーザーのみが、Analyst MD ソフトウェアのロックを解除または閉じることができます。

注: Screen Lock と **Auto Logout** は、混合モードでのみ使用できます。

1. Navigation バーの **Configure** の下にある **Security Configuration** をダブルクリックします。
2. **More** をクリックし、Security タブを開きます。
3. **Mixed Mode** をクリックします。

図 5-3 : Security Configuration ダイアログ :Security タブ



4. **Screen Lock** チェックボックスを選択します。
5. **Wait** フィールドで、画面ロックが作動するまでの時間を分単位で入力します。

注: 自動ログアウトが有効で、画面のロックが解除されていない場合、定義された期間が経過すると、Analyst MD ソフトウェアクライアントが閉じます。測定中の場合は測定が続行されます。ただし、Results Table や Method Editor などが保存されずに開かれている場合、変更内容と未保存のデータは失われる可能性があります。

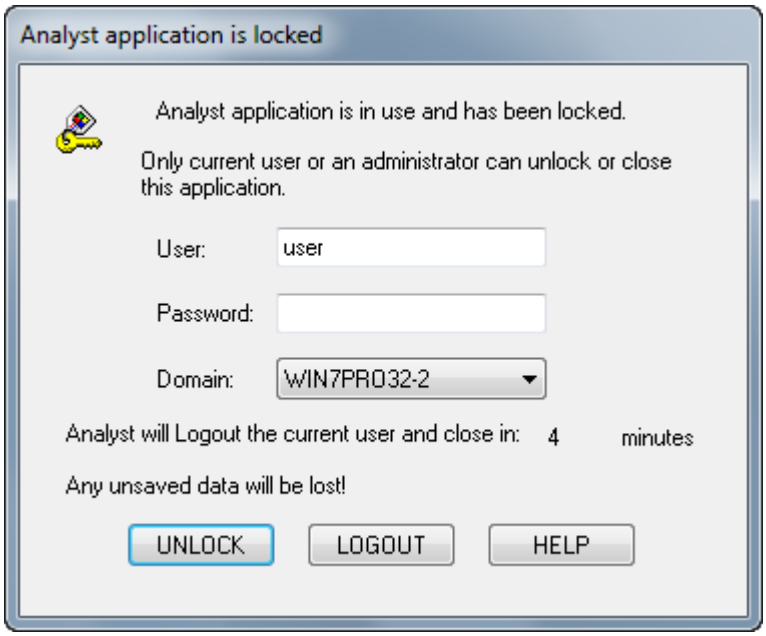
6. 必要に応じて、**Auto Logout** を選択し、**Wait** フィールドに Analyst MD ソフトウェアクライアントを終了するまでの経過時間(分)を入力します。

   10 秒間の猶予があるので、マウスを動かすか、キーを押して Unlock Analyst ダイアログを閉じます。現在ログオンしているユーザー、または管理者またはスーパーバイザーの役割を持つユーザーのみが、Analyst MD ソフトウェアのロックを解除または閉じることができます。
   Unlock Analyst ダイアログには、ユーザーがログアウトするまでの残り時間も表示されます。

Analyst MD ソフトウェアのロックを解除するか、ログオフします

画面ロックが有効になっている場合、画面ロック時間が経過すると、Unlock Analyst ダイアログが開きます。

図 5-4 : Unlock Analyst ダイアログ



次のいずれかの操作を行います。

- 画面のロックを解除するには、必要に応じてユーザー名とパスワードを入力し、**UNLOCK** をクリックします。
- ログアウトするには、必要に応じてユーザー名とパスワードを入力し、**LOGOUT** をクリックします。

Analyst MD ソフトウェアへのアクセス

セキュリティを構成する前に以下を実行します。

- 不要なユーザーとユーザーグループ（レプリケーター、パワーユーザー、バックアップオペレータなど）をローカルコンピュータおよびネットワークからすべて削除します。

  注: すべての SCIEX コンピュータには、ローカル管理者レベルのアカウント、**abservice** が設定済みです。このアカウントは、SCIEX サービスとテクニカルサポートがシステムのインストール、サービス、サポートのために使用します。このアカウントを削除したり、無効にしたりしないでください。アカウントを削除または無効にしなければならない場合は、SCIEX アクセス用の代替プランを用意し、ローカル FSE に伝えます。

- 管理者以外のタスクを持つグループを含むユーザーグループを追加します。
- システム権限を構成します。
- グループポリシー内のユーザーに対して、適切な手順とアカウントポリシーを作成します。

以下の詳細な情報については、Windows ドキュメントを参照してください。

- ユーザーおよびグループと Active Directory ユーザー。
- ユーザーアカウント用のパスワードとアカウントロックアウトポリシー。
- ユーザー権限ポリシー。

ユーザーが Active Directory 環境内で作業を行う際には、Active Directory グループポリシー設定の影響がコンピュータのセキュリティに及びます。包括的な Analyst MD のソフトウェア配備の一環として、Active Directory 管理者とグループポリシーについて確認します。

職員と役割について

Analyst MD ソフトウェアは、Mixed mode を使用する場合を除き、コンピュータと Analyst MD ソフトウェアへのログオンが許可された人だけが、Windows ユーザー名とパスワードを使用してアクセスできるように制限されています。Analyst MD ソフトウェアでは、複数のセッションを実行することはできません。

注: シングルユーザーモードでは、People と Role タブは使用できません。

Analyst MD ソフトウェアの管理者は、Windows ユーザーおよびグループを Analyst MD ソフトウェアセキュリティデータベースに追加することができます。職員またはグループには、6 種類ある既定の役割のいずれかを割り当てる必要があります。必要に応じて新しい役割を作成することも可能です。既定の役割は削除できませんが、その権限の内容は修正できます。Analyst MD ソフトウェアロールは、Analyst MD ソフトウェアコンポーネントにアクセスできます。

表 5-2 : Analyst MD ソフトウェア役割

役割	標準的なタスク	事前規定アクセス
管理者	• システムを管理する。 • セキュリティを構成する。	• すべての Analyst MD ソフトウェア機能

表 5-2 : Analyst MD ソフトウェア役割 (続き)

役割	標準的なタスク	事前規定アクセス
Analyst	• 質量分析装置の操作を監視する。 • エンドユーザーによるデータの使用を分析する。	• 測定メソッド • Analyst アプリケーション • 監査証跡マネージャー • 化合物データベース • Explore • ハードウェア構成 • 定量化 • Report Template Editor • サンプルキュー • チューニング • 状態の表示
演算子	日々のシステムの使用を監視（メンテナンス、サンプルの編成、データ収集、処理を含む）。	• 測定メソッド • Analyst アプリケーション • 監査証跡マネージャー • バッチ • 化合物データベース • Explore • ExpressView（レガシー設定 [1]） • ハードウェア構成 • Report Template Editor • サンプルキュー • チューニング • 状態の表示

[1] この機能は、Analyst MD ソフトウェアではサポートされていません。

表 5-2 : Analyst MD ソフトウェア役割 (続き)

役割	標準的なタスク	事前規定アクセス
エンドユーザー	• サンプルの提供。 • 処理された結果を受領。 • 結果を他のアプリケーションのインプットおよびアウトプットと統合。	• 測定メソッド • Analyst アプリケーション • 監査証跡マネージャー • 化合物データベース • Explore • ExpressView（レガシー設定 [1]） • Report Template Editor • 状態の表示
QA レビュアー	• データのレビュー。 • 監査証跡のレビュー。 • 定量結果のレビュー。	• Analyst アプリケーション • 監査証跡マネージャー • 定量化 • Report Template Editor • 状態の表示
スーパーバイザー	ソフトウェアのロック解除とユーザーのログアウト。	• アプリケーション

Analyst MD ソフトウェアアクセス

図 5-5 : Security Configuration ダイアログ

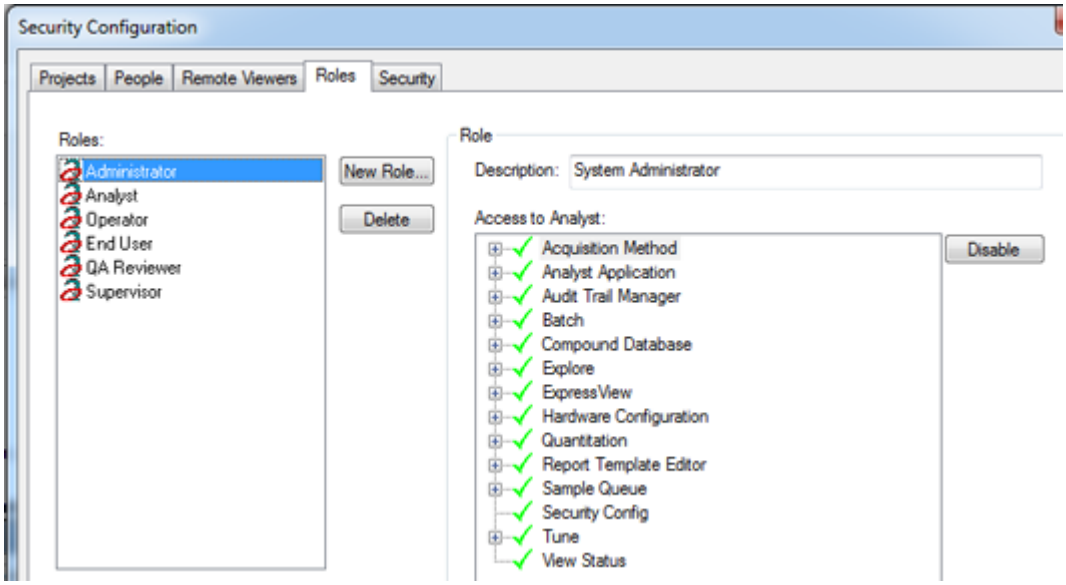


表 5-3 : Analyst MD ソフトウェアから測定メソッドへのアクセス

事前規定アクセス	説明
Create/save acquisition methods	ユーザーが取得メソッドを作成して保存できるようにします。
Open acquisition methods as read-only (acquire mode)	**Create/save acquisition methods** および **Overwrite acquisition methods** オプションが無効になっている場合、ユーザーが読み取り専用モードで取得メソッドを開くことができるようにします。
Overwrite acquisition methods	測定メソッドを上書きする許可をユーザーに与えます。

表 5-4 : Analyst MD ソフトウェアから Analyst アプリケーションへのアクセス

事前規定アクセス	説明
Use Workspace functions[2]	ワークスペース機能を使用する許可をユーザーに与えます。
Create Project	プロジェクトを作成する許可をユーザーに与えます。
Copy Project	プロジェクトをコピーする許可をユーザーに与えます。
Create Root Directory	ルートディレクトリを作成する許可をユーザーに与えます。
Set Root Directory	ルートディレクトリを設定する許可をユーザーに与えます。
Change Project	プロジェクトを変更する許可をユーザーに与えます。
Load/Save Processed Data Files	処理済みのデータファイルをロードし保存する許可をユーザーに与えます。
Lock/Logout Application	指定した時間が経過すると、アプリケーションを自動的にロックしたり、ユーザーを自動的にログアウトさせたりすることができます。この機能は、混合モードで、**Screen Lock** または **Auto Logout** オプションが選択されている場合にのみ使用できます。

表 5-5 : Analyst MD ソフトウェアから Audit Trail Manager へのアクセス

事前規定アクセス	説明
View Audit Trail Data	監査証跡データを表示する許可をユーザーに与えます。この許可に対するアクセスは、管理者を除き、全ユーザーに対して無効にします。
Change Audit Trail Settings	監査証跡設定を修正する許可をユーザーに与えます。

表 5-5 : Analyst MD ソフトウェアから Audit Trail Manager へのアクセス (続き)

事前規定アクセス	説明
Maintenance Log	メンテナンスログを表示する許可をユーザーに与えます。
Create or Modify Audit Maps	監査マップを作成または修正する許可をユーザーに与えます。

表 5-6 : Analyst MD ソフトウェアからバッチへのアクセス

事前規定アクセス	説明
Open existing batches	既存のバッチを開く許可をユーザーに与えます。
Create new batches	バッチを作成する許可をユーザーに与えます。
Import	既存のバッチ（mdb 、あるいは他の対応ファイル形式）からデータをインポートする許可をユーザーに与えます。
Save batches	バッチを保存する許可をユーザーに与えます。
Use template batches	テンプレートのバッチを保存または開く許可をユーザーに与えます。
Edit batches	バッチを編集する許可をユーザーに与えます。
Submit batches	バッチを送信する許可をユーザーに与えます。
Add or remove custom columns	Batch Editor にカスタム列を追加または削除する許可をユーザーに与えます。
Use template acquisition methods	測定メソッドをテンプレートとして使用する許可をユーザーに与えます。このオプションは Batch Editor で使用できます。メソッドが選択されると、**Use as template** オプションが有効になります。
Overwrite batches	既存のバッチを上書きする許可をユーザーに与えます。
Overwrite template batches	既存のテンプレートバッチを上書きする許可をユーザーに与えます。

表 5-7 : Analyst MD ソフトウェアから化合物データベースへのアクセス

事前規定アクセス	説明
Setup compound database location	化合物の場所と名前のオプションを読み取り専用にします（Browse ボタンは無効になります）。（Explore モードでは、**Tools** > **Settings** > **Optimization Options** をクリックします。） ユーザーが化合物データベースの場所と化合物データベースのユーザーオプションの双方にアクセスできる場合のみ、Optimization Options ダイアログの **Use Defaults Now** ボタンが有効になります。
Setup user options	最適化オプションダイアログでユーザー ID とパスワードのオプションを設定できるようにします。（Explore モードでは、**Tools** > **Settings** > **Optimization Options** をクリックします。） ユーザーが複合データベースの場所と複合データベースのユーザーオプションの両方にアクセスできる場合にのみ、Optimization Options ダイアログの **Use Defaults Now** ボタンを有効にします。（これらの機能にアクセスするには、化合物データベースを右クリックします。）
Add to compound database	化合物データベースに化合物を追加する許可をユーザーに与えます。（この機能にアクセスするには、化合物データベースを右クリックします。）
Modify database (overrides add/ delete if disabled)	化合物データベースに追加、削除、修正する許可をユーザーに与えます（化合物設定または最適化設定）。
Delete compound from database	化合物データベースから化合物を削除する許可をユーザーに与えます。（この機能にアクセスするには、化合物データベースを右クリックします。）
Delete optimization settings from database	化合物データベースから最適化設定を削除する許可をユーザーに与えます。（この機能にアクセスするには、化合物データベースを右クリックします。）

表 5-8 : Analyst MD ソフトウェアから Explore へのアクセス

事前規定アクセス	説明
Save data to text file	データをテキストファイルに保存する許可をユーザーに与えます。（スペクトルまたはクロマトグラムを右クリックし、**Save to Text File** をクリックします。）
Setup library location	ライブラリデータベースの場所を設定または選択する許可をユーザーに与えます。
Setup library user options	*ライブラリ用にセキュリティ情報（ユーザー名やパスワードなど）を設定する許可をユーザーに与えます。

表 5-8 : Analyst MD ソフトウェアから Explore へのアクセス (続き)

事前規定アクセス	説明
Add library record	ライブラリレコードを追加する許可をユーザーに与えます。(スペクトルを右クリックするか、Explore モードで、**Explore** > **Library Search** > **Add** をクリックします。)
Add spectrum to library record	無効にすると、ユーザーが Library Search ダイアログの Append MS ボタンをクリックできなくなります。(Explore モードでは、**Explore** > **Library Search** > **List** をクリックします。)
Modify library record (overrides add/ delete if disabled)	ライブラリレコードを修正する許可をユーザーに与えます。
Delete MS spectrum	選択した MS スペクトルを削除する許可をユーザーに与えます。
Delete UV spectrum	UV スペクトルを削除する許可をユーザーに与えます。
Delete structure	構造を削除する許可をユーザーに与えます。
View library	リストおよび制約機能付きリストを使用する許可をユーザーに与えます。(Explore モードでは、**Explore** > **Library Search** をクリックします。)
Search library	検索ライブラリを使用する許可、ならびに検索制約を設定する許可をユーザーに与えます。(スペクトルを右クリックするか、Explore モードで、**Explore** > **Library Search** をクリックします。)
Select processing algorithm to retrieve peak list	レガシー設定 [2]

表 5-9 : Analyst MD ソフトウェアから ExpressView*へのアクセス

事前規定アクセス	説明
Start Express View dialog	レガシー設定 [2]
Modify options	レガシー設定 [2]

[2] この機能は、Analyst MD ソフトウェアではサポートされていません。

表 5-10 : Analyst MD ソフトウェアからハードウェア構成へのアクセス

事前規定アクセス	説明
Create	ハードウェアプロファイルを作成する許可をユーザーに与えます。
Delete	ハードウェアプロファイルを削除する許可をユーザーに与えます。
Edit	ハードウェアプロファイルを編集する許可をユーザーに与えます。
Activate/ Deactivate	ハードウェアプロファイルを有効化または無効化する許可をユーザーに与えます。

表 5-11 : Analyst MD ソフトウェアから定量化へのアクセス

事前規定アクセス	説明
Create quantitation method	新しい定量化メソッドを作成する許可をユーザーに与えます。
Change default method options	デフォルトメソッドのオプションを変更する許可をユーザーに与えます。
Use full method editor	Quantitation Method Editor を使用する許可をユーザーに与えます。
Create “automatic” methods	Quantitation Wizard 内で定量化メソッドを作成する許可をユーザーに与えます。
Modify existing methods	既存の定量化メソッドを修正（上書き）する許可をユーザーに与えます。
Change peak names (in wizard)	Quantitation Wizard でピーク名を変更する許可をユーザーに与えます。
Change default number of smooths (in wizard)	Quantitation Wizard でデフォルトスムージング数を変更する許可をユーザーに与えます。
Change “advanced” parameters (in wizard)	Quantitation Wizard で高度なパラメータを変更する許可をユーザーに与えます。ユーザーに対してこのオプションを有効にしなかった場合、Advanced ボタンは非表示となります。
Change concentration units (in wizard)	Quantitation Wizard の高度なパラメータで、濃度の単位を変更する許可をユーザーに与えます。
Create new results tables	Quantitation Wizard を用いて、または **New** メニューで **File** を選択することで、新しい Results Table を作成する許可をユーザーに与えます。このオプションによって Save As ボタンが無効化されることはありません。

表 5-11 : Analyst MD ソフトウェアから定量化へのアクセス (続き)

事前規定アクセス	説明
Open existing results tables	既存の Results Table を開く許可をユーザーに与えます。
When saving, replace existing results tables	既存の Results Table を上書きする許可をユーザーに与えます。
Edit results tables' method	定量化メソッドファイルを修正する許可をユーザーに与えます。定量モードでは、**Tools** > **Results Table** > **Modify Method** をクリックします。これによって実際のファイルが修正されますが、Results Table 内の埋め込みメソッドは影響を受けません。
Create new "standard" queries (from wizard)	Quantitation Wizard を用いて新しい標準クエリーを作成する許可をユーザーに与えます。
Exclude standards from calibration	Calibration Curve ペイン、Results Table、Statistics ペインでキャリブレーションから標準を除外できるようにします。
Add and Remove samples from results table	サンプルを追加または削除する許可をユーザーに与えます。(**Quantitate** モードでは、**Tools** > **Results Table** > **Add/Remove samples** をクリックします。) この許可に対するアクセスは、管理者を除き、全ユーザーに対して無効にします。
Display metric plots	Results Table からメトリックプロットを表示する許可をユーザーに与えます。(Results Table を右クリックし、**Metric Plot** をクリックします。)
Create or modify formula columns	Results Table で Formula 列を作成または修正する許可をユーザーに与えます。
Modify sample name	サンプル名を修正する許可をユーザーに与えます。
Export results table as text file	Results Table をテキストファイルとしてエクスポートする許可をユーザーに与えます。(**Quantitate** モードで、Results Table を開いた状態で、**Tools** > **Results Table** > **Export as Text** をクリックします。)
Export settings from results table	表設定を新しい Results Table 設定にエクスポートする許可をユーザーに与えます。(Results Table を右クリックし、**Table Settings** > **Export To New Table Settings** をクリックします。)
Modify custom column title	カスタム列のタイトルを修正する許可をユーザーに与えます。Formula 列はカスタム列ではありません。

表 5-11 : Analyst MD ソフトウェアから定量化へのアクセス (続き)

事前規定アクセス	説明
Modify results table settings	Results Table の表設定（右クリックし、**Table Settings** > **Edit** をクリックします）またはグローバル表設定（**Quantitate** モードで、**Tools** > **Settings** > **New Quantitation Results Table Settings** をクリックします）を修正する許可をユーザーに与えます。このセキュリティは、既存の表設定の間で変更する必要はありません。
Modify global (default) settings	グローバル表設定を修正する許可をユーザーに与えます。**Quantitate**(モードでは、**Tools** > **Settings** > **New Quantitation Results Table Settings.)** をクリックします
Modify audit trail settings	監査証跡設定を編集する許可をユーザーに与えます。
Disable, enable and clear audit trail	レガシー設定 [2]
Change results table column visibility	Results Table に含める列を選択する許可をユーザーに与えます。（ダイアログにアクセスするには、Results Table を右クリックし、**Table Settings** > **Edit** をクリックします。）
Change results table column precision	Results Table で Significant Figures、Scientific Notation、Precision の各列を修正する許可をユーザーに与えます。（Table Settings ダイアログにアクセスするには、 Results Table を右クリックします。**Table Settings** > **Edit.**をクリック、**Columns** をクリックし、**Edit** をクリックします。）
Run temporary queries	クエリーを実行する許可をユーザーに与えます。
Modify or save queries	既存のクエリーを修正する許可、または新しいクエリーを保存する許可をユーザーに与えます。（クエリーを修正するには、Ctrl キーを押しながら Results Table を右クリックし、Query をクリックしてから既存のクエリーを選択します。）Results Table でクエリーを修正する許可をユーザーに与えます。（Results Table で、右クリックして **Table Settings** > **Edit** > **Queries.**をクリックします。既存のクエリを選択して、**Edit** をクリックします。）
Run temporary sorts	*クエリーを並び替える許可を与えます。
Modify or save sorts	*並び替えを編集または保存する許可を与えます。
Use metric plot settings dialog	Metric Plot Settings ダイアログを使用する許可を与えます。

表 5-11 : Analyst MD ソフトウェアから定量化へのアクセス (続き)

事前規定アクセス	説明
Modify or create metric plot settings	Results Table から新しいメトリックプロットを作成する許可をユーザーに与えます。(Results Table を右クリックし、**Metric Plot** > **New** をクリックします。) Results Table からメトリックプロットを修正する許可をユーザーに与えます(Results Table を右クリックし、**Table Settings** > **Edit** > **Metric Plot** をクリックします。)既存のメトリックプロットを選択し、**Edit** をクリックします。) このセキュリティ項目によって、ユーザーが既存のメトリックプロットを修正できなくなることはありません(メトリックプロットを実行し、プロットを右クリックして Edit Settings を選択すれば修正可能です)。
Create Analyte Groups	Results Table から分析試料グループを作成する許可をユーザーに与えます。(Results Table を右クリックし、**Analyte Group** > **New** をクリックします。)
Modify Analyte Groups	分析試料グループを修正する許可をユーザーに与えます。(Results Table を右クリックし、**Table Settings** > **Edit** > **Analyte Groups** をクリックします。)既存のグループを選択し、**Edit** をクリックします。)
Change default peak review options	デフォルトのピーク設定を変更する許可をユーザーに与えます。(**Quantitate** モードでは、**Tools** > **Settings** > **Quantitation Peak Review Settings** をクリックします。)
Change "simple" parameters in peak review	ピークレビューで「シンプル」パラメータを変更する許可をユーザーに与えます。Peak Review ペインが開いている間は、Show or Hide Parameters ボタンを 1 回クリックした際に表示されるパラメータがシンプルパラメータとなります。
Change "advanced" parameters in peak review	ピークレビューで高度なパラメータを変更する許可をユーザーに与えます。Peak Review ペインが開いている間は、Show or Hide Parameters ボタンを 2 回クリックした際に表示されるパラメータが高度なパラメータとなります。
Manually integrate	Peak Review ペインで手動積分モードを用いて、ピークを手動で積分する許可をユーザーに与えます。
"Update" method in peak review	Peak Review ペインで特定のピークの定量化メソッドを変更した後、メソッドを更新および元に戻す許可をユーザーに与えます。
Add or modify annotation	右クリックメニューで Sample Annotation オプションを使用することで、あるいは Results Table に Sample Annotation 列を追加することで、Peak Review ペインまたはウィンドウ内でサンプル注釈を追加または修正する許可をユーザーに与えます。
Change regression parameters	Calibration Curve ペインで回帰設定を変更する許可をユーザーに与えます。

表 5-11 : Analyst MD ソフトウェアから定量化へのアクセス (続き)

事前規定アクセス	説明
Modify Sample ID	Results Table でサンプル ID を追加または修正する許可をユーザーに与えます。
Modify Sample Type	Results Table でサンプルタイプを変更する許可をユーザーに与えます。
Modify Sample Comment	Results Table でサンプルコメントを追加または修正する許可をユーザーに与えます。
Modify Weight To Volume ratio	Results Table で比重量を修正する許可をユーザーに与えます。
Modify Dilution Factor	Results Table で希釈係数を修正する許可をユーザーに与えます。
Modify Analyte Concentration	Results Table で分析試料の濃度を修正する許可をユーザーに与えます。
Modify Analyte Units	レガシー設定 [2]
Modify IS Concentration	Results Table で IS の濃度を修正する許可をユーザーに与えます。
Modify IS Units	レガシー設定 [2]
Modify Processing Algorithm	定量アルゴリズムを変更する許可をユーザーに与えます。（**Quantitate** モードでは、**Tools** > **Settings** > **Quantitation Integration Algorithm** をクリックします。）
Enable or Disable percent rule in Manual Integration	手動積分（パーセントルール）を変更する許可をユーザーに与えます。（**Quantitate** モードでは、**Tools** > **Settings** > **Quantitation Peak Review Settings** をクリックします。）

表 5-12 : Analyst MD ソフトウェアから Report Template Editor へのアクセス

事前規定アクセス	説明
Create/modify report templates	新規レポートテンプレートを作成する許可、ならびに既存のテンプレートを修正する許可をユーザーに与えます。
Open report templates as read-only	rpt ファイルを読み取り専用として開く許可をユーザーに与えます。（**File** > **Open** をクリックします。）
Print	あらゆるモードで印刷する許可をユーザーに与えます。
Select report templates	Print ダイアログで既存のレポートテンプレートを選択する許可をユーザーに与えます。

表 5-13 : Analyst MD ソフトウェアからサンプルキューへのアクセス

事前規定アクセス	説明
Start Sample	キュー内のサンプルを開始する許可をユーザーに与えます。
Abort Sample	キュー内のサンプルを中断する許可をユーザーに与えます。
Stop Sample	キュー内のサンプルを停止する許可をユーザーに与えます。
Stop Queue	サンプルを停止する許可をユーザーに与えます。
Pause Sample Now[2]	サンプルを即座に一時停止する許可をユーザーに与えます。
Insert Pause Before Selected Sample(s)[2]	次のサンプルへと移動する前に、一時停止を入れる許可をユーザーに与えます。
Continue Sample[2]	現在のサンプルを継続（再始動）する許可をユーザーに与えます。
Next Period[2]	次の期間を即座に測定する許可をユーザーに与えます。
Extend Period[2]	測定中の期間を延長する許可をユーザーに与えます。
Next Sample[2]	次のサンプルを測定する許可をユーザーに与えます。
Advance Pump Gradient	レガシー設定 [2]
Equilibrate	システムを平衡化する許可をユーザーに与えます。
Stand By	質量分析装置をスタンバイモードに入れる許可をユーザーに与えます。
Ready	質量分析装置を準備完了モードに入れる許可をユーザーに与えます。
Reacquire	サンプルを再測定する許可をユーザーに与えます。
Insert Pause[2]	キューに一時停止を入れる許可をユーザーに与えます。
Delete Sample or Batch	キュー内のサンプルまたはバッチを削除する許可をユーザーに与えます。
Move Batch	キュー内のバッチ順序を変更する許可をユーザーに与えます。

表 5-14 : Analyst MD ソフトウェアから Tune へのアクセス

事前規定アクセス	説明
Edit parameter settings	パラメータ設定を編集する許可をユーザーに与えます。(Tune and Calibrate モードで、**Tools** > **Settings** > **Parameter Settings** をクリックします。)
Edit tuning options	キャリブレーション標準用の参照テーブルを作成、削除、更新する許可、ならびに低値およびオープンの分解能に対するユニット分解能をもとに、オフセットドロップを編集する許可をユーザーに与えます。
Edit instrument data	質量分析装置のキャリブレーションおよび分解能表を編集する許可をユーザーに与えます。

表 5-14 : Analyst MD ソフトウェアから Tune へのアクセス (続き)

事前規定アクセス	説明
Manual tune	チューニングおよびキャリブレーションモードで手動チューニング機能を使用する許可をユーザーに与えます。
Calibrate from current spectrum	現在のスペクトルを用いてキャリブレーションを実行する許可をユーザーに与えます。
Instrument optimization	チューニングおよびキャリブレーションモードで Instrument Optimization 機能を実行する許可をユーザーに与えます。
Compound optimization	Compound Optimization 機能を実行する許可をユーザーに与えます。
Tuning Instrument	質量分析装置のチューニングおよびキャリブレーションを実行する許可をユーザーに与えます。
Advanced Resolution Table Modification	Resolution タブの Advanced ボタンを用いて分解能を構成する許可をユーザーに与えます。
Auto TOF Mass Calibration	レガシー設定 [2]

表 5-15 : Analyst MD ソフトウェアのアクセス権限

事前規定アクセス	説明
Security Config	セキュリティ関連の設定を構成する許可をユーザーに与えます。
View Status	質量分析装置の状態を表示する許可をユーザーに与えます。

注: Formula 列の作成または使用時には、事前に式を検証することが推奨されます。

MultiQuant MD ソフトウェアへのアクセス

事前規定アクセス	説明
セッションファイルの作成	ユーザーは Results Table を作成できます。
Create quantitation method	ユーザーは定量化メソッドを作成できます。
定量化メソッドファイル	Analyst Data フォルダ内の Quantitation Methods フォルダにある定量化メソッドを修正できます。

事前規定アクセス	説明
ロック解除された Results Table のエクスポートとレポートの作成を許可	ロック解除された Results Tables のエクスポートとレポートの作成が可能です。
自動メソッドの作成	Results Tables を作成するときに自動メソッドオプションを選択できるようにします。
保存するときに既存の結果表を置き換える	ユーザーは既存の Results Tables を更新できますが、既存の Results Table 名を使って新しい Results Table を作成することはできません。たとえば、RT1 と呼ばれる Results Table を作成した場合、ユーザーはこれを更新することはできますが、RT1 の名前を使って新しい Results Table を作成することはできません。ユーザーは既存の Results Table の名前で無題の Results Table に名前を付けることはできません。
デフォルトの定量化メソッド統合アルゴリズムを変更	Integration Default ダイアログで、アルゴリズムを変更することができます。（**Edit** > **Project Integration Defaults** をクリックします。）
デフォルトの定量化メソッド統合パラメータを変更	Integration Default ダイアログで、アルゴリズムのデフォルトパラメータを変更することができます。（**Edit** > **Project Integration Defaults** をクリックします。）
プロジェクトの修正されたピーク警告の有効化を許可	Edit メニューで Project Modified Peak Warning オプションが可能になるフラグを有効または無効にできます。
Results Table にサンプルを追加	ユーザーはサンプルを追加することが可能です。（**Process** > **Add Samples** をクリックします。）
Results Table からサンプルを削除	表が選択したサンプルを削除できます。（**Process** > **Remove Selected Samples** をクリックします。）
外部キャリブレーションのエクスポート、インポート、または削除	次のオプションを 1 つ使って、外部キャリブレーションをエクスポート、インポートまたは削除できます。 • **Process** > **Export Calibration** をクリックします。 • **Process** > **Import External Calibration** をクリックします。 • **Process** > **Remove External Calibration** をクリックします。
アイソトープ補正を使用、編集、またはクリア	次のいずれかのオプションを使用して、アイソトープ補正を使用、編集、またはクリアできるようにします。 • **Process** > **Use Default Isotope Correction** をクリックします。 • **Process** > **Edit Current Isotope Correction** をクリックします。 • **Process** > **Clear Previous Isotope Correction** をクリックします。

事前規定アクセス	説明
監査マップ設定の変更	プロジェクトの監査マップおよび監査マップ定義を修正できます。（**Audit Trail** > **Audit Map Manager** をクリックします。）
サンプル名の変更	Results Table でサンプル名を修正する許可をユーザーに与えます。
サンプルタイプの修正	Results Table でサンプルタイプ（Standard、QC、Unknown）を変更できます。
サンプル ID の修正	Results Table でサンプル ID を修正する許可をユーザーに与えます。
実際の濃度の修正	Results Table の標準サンプルと QC サンプルの実際の濃度を修正する許可をユーザーに与えます。
希釈係数の修正	Results Table で希釈係数を変更できます。
コメントフィールドの修正	コメントフィールドを修正する許可をユーザーに与えます。 • コンポーネントコメント • IS コメント • IS ピークコメント • ピークコメント • サンプルコメント
手動積分を許可	Peak Review で手動積分モードにすることが可能です。
ピークが見つからないに設定	ピークレビューでピークを見つけられないように設定機能を使用できるようにします。このアクションを実行するには、Peak Review ペインを右クリックします。
Results Table にピークを含めるまたはそこから除外	Results Tables、Statistics Tables、およびキャリブレーションカーブのピークを含めるまたは除外できます。
Modify regression settings for fit and weight	Modify Results Table Method 機能、および New Quantitation Method wizard を使用した場合、キャリブレーションカーブペインで回帰設定を変更できます。
単一のクロマトグラムの results table 積分パラメータを変更	単一のクロマトグラムを変更できます。

事前規定アクセス	説明
Results Table コンポーネントの定量化メソッドを変更	単一のクロマトグラムの修正をコンポーネントに適用できます。 コンポーネントを更新してから単一の変更を適用する場合は、この権限と、単一のクロマトグラム権限の Results Table の変更の統合パラメータを有効にする必要があります。
Results Tables のメトリックプロットの作成、使用、またはエクスポート	Results Table（Metric Plot ボタンが有効）でメトリックプロットを作成または使用でき、メトリックプロットをエクスポートすることが可能です。（**File** > **Export** をクリックします。）
Set Peak Review Title Format（ピークレビュータイトルのフォーマットの設定）	Peak Review Title Format in Peak Review を変更することが可能です。このアクションを実行するには、Peak Review ペインを右クリックします。
カスタム列の追加、名前の変更、または変更	カスタム列の追加、名前の変更、または修正が可能です。この権限がない場合でも、自動的にカスタム列を作成するクエリを実行することができます。
カスタム列を削除	Results Table でカスタム列を削除できます。
結果表の列設定の修正	Results Table 内の Results Table 列の設定を変更できます。
列設定をプロジェクトのデフォルトとして保存	列の設定をプロジェクトに適用できます。
Results Table をロックして保存	Results Table をロックして保存できます。
Results Table を解除して保存	Results Table を解除して保存できます。
Results Table をレビューして保存	Results Table をレビューして保存できます。
Results Table にクエリを作成または編集	以下のオプションのいずれかを使用して、Results Table にクエリを作成または編集できるようにします。 • **Process** > **Create Simple Query** をクリックします。 • **Process** > **Edit Simple Query** をクリックします。
Use Results Table のクエリを使用	クエリーを実行する許可をユーザーに与えます。（**Process** > **Query** をクリックします。）

事前規定アクセス	説明
暗号化されていない MultiQuant クエリを使用	MQ 設定フォルダ内から.xls クエリーを実行できるようになります。

注: MultiQuant MD ソフトウェアをアンインストールした場合、Analyst MD ソフトウェアに含まれる MultiQuant MD ソフトウェアのセキュリティ項目は残ります。セキュリティ項目は、Security Configuration ダイアログの Roles タブにあります。

Analyst MD ソフトウェアにユーザーまたはグループを追加します。

注: Analyst MD ソフトウェアのセキュリティ構成への変更は、Analyst MD ソフトウェアの再起動後に有効になります。

1. Navigation バーの **Configure** の下にある **Security Configuration** をダブルクリックします。
   Security Configuration ダイアログが開きます。
2. People タブを開きます。
3. **New Person** をクリックします。
   Select Users or Groups ダイアログが開きます。
4. ユーザーまたはグループを追加.
5. Available Roles ペインで役割をクリックし、**Add** をクリックします。
6. **Apply** をクリックします。
7. **OK** をクリックします。
   Select Users or Groups ダイアログが閉じます。
8. **OK** をクリックします。
   Security Configuration ダイアログが閉じるます。

役割を変更する

1. Navigation バーの **Configure** の下にある **Security Configuration** をダブルクリックします。
   Security Configuration ダイアログが開きます。
2. People タブを開きます。
3. 左側のペインで人物をクリックし、以下のいずれかを実行します。
   - Available Roles ペインで必要な役割をクリックし、**Add** をクリックして役割を追加します。
   - Role(s) Selected ペインで役割をクリックし、**Remove** をクリックするとその役割が削除されます。
4. **Apply** をクリックします。
5. **OK** をクリックします。
   Security Configuration ダイアログが閉じるます。

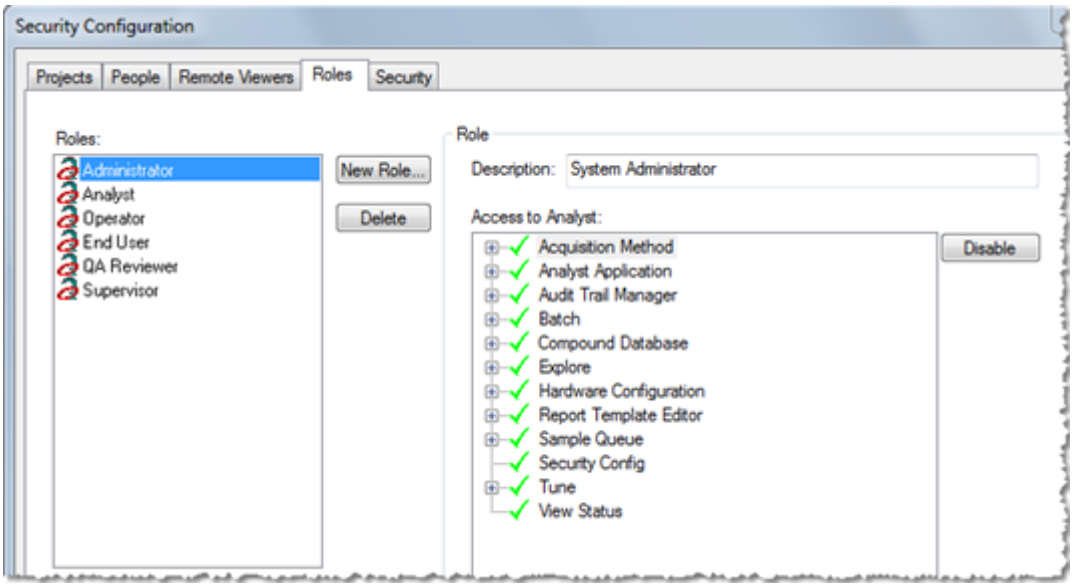
Analyst MD ソフトウェアから職員を削除する

1. Navigation バーの **Configure** の下にある **Security Configuration** をダブルクリックします。
   Security Configuration ダイアログが開きます。
2. People タブを開きます。
3. 左側のペインで、削除したい個人をクリックしてから **Delete** をクリックします。
4. **Apply** をクリックします。
5. **OK** をクリックします。
   Security Configuration ダイアログが閉じるます。

カスタム役割の作成

1. Navigation バーの **Configure** の下にある **Security Configuration** をダブルクリックします。
   Security Configuration ダイアログが開きます。
2. **More** をクリックし、Roles タブを開きます。

図 5-6 : Security Configuration ダイアログ:Roles タブ



3. **New Role** をクリックします。
   New Role ダイアログが開きます。
4. 適切なフィールドに **Role Name** と **Description** を入力します。
5. **OK** をクリックします。

注: 新しいユーザー定義の役割はすべて、Analyst MD ソフトウェアへのフルアクセス権を持っています。Access to Analyst ペインの緑色のチェックマークは、システムアクセスが有効になっていることを示しています。赤い X 印は、システムアクセスが拒否されていることを示しています。

---

6. **Access to Analyst** リストのコンポーネントをダブルクリックして、アクセスを有効または無効にします。
7. アクセスを機能レベルで構成するには、コンポーネントを展開し、機能をダブルクリックして有効または無効にします。
8. **Apply** をクリックします。
9. **OK** をクリックします。
   Security Configuration ダイアログが閉じるます。

カスタム役割の削除

注: 単独の職員に単一の役割が割り当てられている状態でその役割が削除された場合、役割と併せてその職員も削除するようメッセージが表示されます。

1. Navigation バーの **Configure** の下にある **Security Configuration** をダブルクリックします。
   Security Configuration ダイアログが開きます。
2. **More** をクリックし、Roles タブを開きます。
   Roles ペインが開きます。
3. 役割を選択し、**Delete** をクリックします。
4. **Apply** をクリックします。
5. **OK** をクリックします。
   Security Configuration ダイアログが閉じるます。

アクセスを設定する

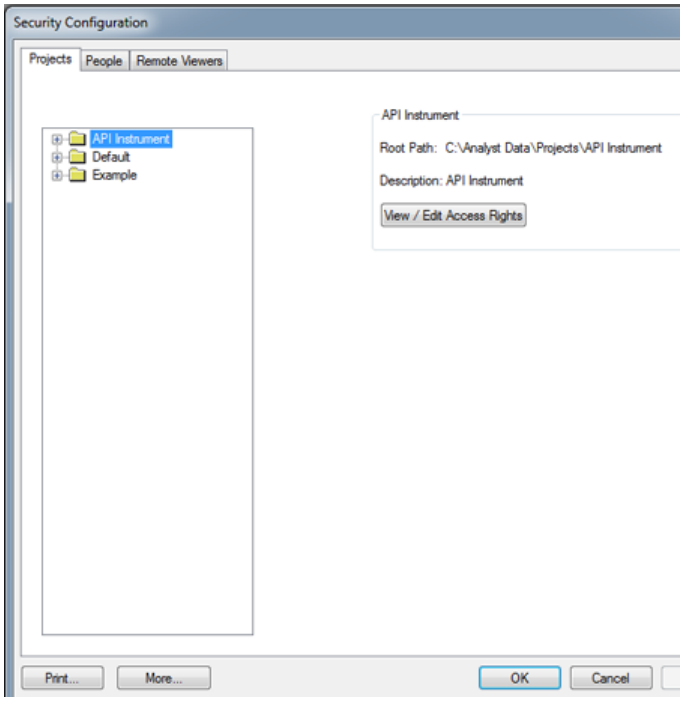
プロジェクトとプロジェクトファイルへのアクセスは人物またはグループ別に構成し、人物または Windows セキュリティグループ別に管理できます。

Analyst MD ソフトウェアセキュリティのこの機能を使用するには、作業ルートに NTFS を使用します。プロジェクトセキュリティを設定しない場合、オペレータがどのプロジェクトファイルにアクセスできるかは、NTFS における各 Windows ユーザーのデータ設定に左右されます。詳細な情報については、次のセクションを参照：Windows セキュリティ構成。

注: Analyst MD ソフトウェアを使用してプロジェクトを作成すると、すべてのユーザーがプロジェクトフォルダとサブフォルダにアクセスできます。

1. Navigation バーの **Configure** の下にある **Security Configuration** をダブルクリックします。

図 5-7 : Security Configuration ダイアログ : Projects タブ



2. 左側のペインで、フォルダまたはファイルをクリックします。
3. **View/Edit Access Rights** をクリックします。
   Properties ダイアログが開きます。
4. ユーザーまたはグループを追加または削除し、必要に応じて権限を設定して、**OK** をクリックします。
5. **Apply** をクリックします。
6. **OK** をクリックします。
   Select Users or Groups ダイアログが閉じます。
7. **OK** をクリックします。
   Security Configuration ダイアログが閉じるます。

プロジェクトフォルダ

各プロジェクトには、さまざまな種類のファイルを格納するフォルダがあります。各フォルダの内容については、次を参照 : 表 5-16。

表 5-16 : プロジェクトフォルダ

フォルダ	コンテンツ
\Acquisition Methods	使用した測定メソッドがすべて格納されています。測定メソッドには dam の拡張子が付いています。

表 5-16 : プロジェクトフォルダ (続き)

フォルダ	コンテンツ
\Acquisition Scripts	測定スクリプトは、Analyst MD ソフトウェアでは使用できません。このフォルダは空です。Analyst MD ソフトウェアのスクリプト記述を用いればカスタムスクリプト(Analyst のカスタム操作シーケンス)を作成できますが、これを *in vitro* 診断装置の一部として使用することは避けてください。Analyst MD ソフトウェアの使用時に実行される固有のソフトウェアチェックは、カスタムスクリプトでは実行されず、危険につながる可能性があります。
\Batch	保存されたすべての測定バッチファイルが格納されています。測定バッチには dab の拡張子が付いています。このフォルダには、取得バッチ テンプレートが含まれるサブフォルダ Templates も含まれています。バッチテンプレートには dat の拡張子が付いています。
\Data	測定データファイルが格納されています。これらのファイルには wiff の拡張子が付けられています。
\Log	定量と Compound Optimization の結果が保存されています。
\Processing Methods	使用した定性データ処理メソッドがすべて格納されています。
\Processing Scripts	2 つのデータ処理スクリプトが保存されています。 API Instrument プロジェクトに保存されている処理スクリプトは、**Scripts** メニューから利用できます。
\Project Information	プロジェクトの全情報とプロジェクトの設定が格納されています。このフォルダはサブプロジェクトに保存することはできません。
\Quantitation Methods	使用した定量化メソッドがすべて格納されています。定量化メソッドには qmf の拡張子が付いています。
\Results	定量 Results Table ファイル(rdb の拡張子)がすべて格納されています。
\Templates	レポートテンプレート(rpt の拡張子)が格納されています。

ソフトウェアのファイルタイプ

一般的な Analyst MD ソフトウェアのファイル タイプについては、次を参照:表 5-17。
API Instrument フォルダには、Processing Methods と Results を除く、すべてのサブディレクトリが含まれています。

表 5-17 : Analyst MD ソフトウェアファイル

拡張子	ファイルタイプ	フォルダ
ata	監査証跡アーカイブ	Project Information

表 5-17 : Analyst MD ソフトウェアファイル (続き)

拡張子	ファイルタイプ	フォルダ
atd	• 装置監査証跡データ • 装置監査証跡設定 • プロジェクト監査証跡データ • プロジェクト監査証跡設定	Project Information
cam	監査マップ	Project Information
dab	測定バッチ	Batch
dam	測定メソッド	Acquisition Methods
dat	測定バッチテンプレート	Batch\Templates
dll	動的リンクライブラリ	Processing Scripts
eph	Explore 処理履歴データ	Processing Methods
hwpf	ハードウェアプロファイル	Configuration[3]
ins	装置データキャリブレーション情報	Instrument Data[3]
ログ	自動収集のログレコード	Log
mdb	MS Access データベース	—
pdf	ポータブルドキュメントデータ	—
psf	パラメータ設定	Parameter Settings[3]
qmf	定量化メソッド	Quantitation Methods
rdb	Results Table.定量監査証跡データを保持	Results
rpt	Report template（レポートテンプレート）	• Templates\Batch • Templates\Method • Templates\ Report • Templates\Workspace
rtf	リッチテキスト形式	—
sdb	定量監査証跡設定	Project Information
tun	チューニング環境設定ファイル	Preferences[3]
txt	Text	—

[3] * API Instrument フォルダにのみ含まれています。他のサブフォルダは、いずれも各プロジェクトフォルダに含まれています。これらはプロジェクトレベルのフォルダ、または各サブプロジェクト内に保存されている場合があります。

表 5-17 : Analyst MD ソフトウェアファイル (続き)

拡張子	ファイルタイプ	フォルダ
wiff.scan	質量分析装置データファイル	• `Tuning` Cache[3] • `Data`
xls または xlsx	Excel スプレッドシート	`Batch`

`Example` プロジェクトでは、以下の形式がバッチ情報のインポートに対応しています。

- mdb
- txt
- xls または xlsx

測定用コンピュータとクライアントコンピュータにおける Windows ファイアウォール構成

クライアントコンピュータで Analyst MD ソフトウェアを使用して質量分析装置をリモートで管理するには、測定用コンピュータとクライアントコンピュータの両方で Windows ファイアウォールを構成します。測定用コンピュータの Windows ファイアウォールは、Analyst.exe と AnalystService.exe 両方の実行が許可されるよう構成する必要があります。クライアントコンピュータでは、Analyst.exe の実行が許可されるよう Windows ファイアウォールを構成する必要があります。

注: 測定用コンピュータ(リモートアクセス用)とクライアントコンピュータ(測定用コンピュータによるアクセス用)は、双方とも同一のネットワークドメインに存在しなくてはなりません。

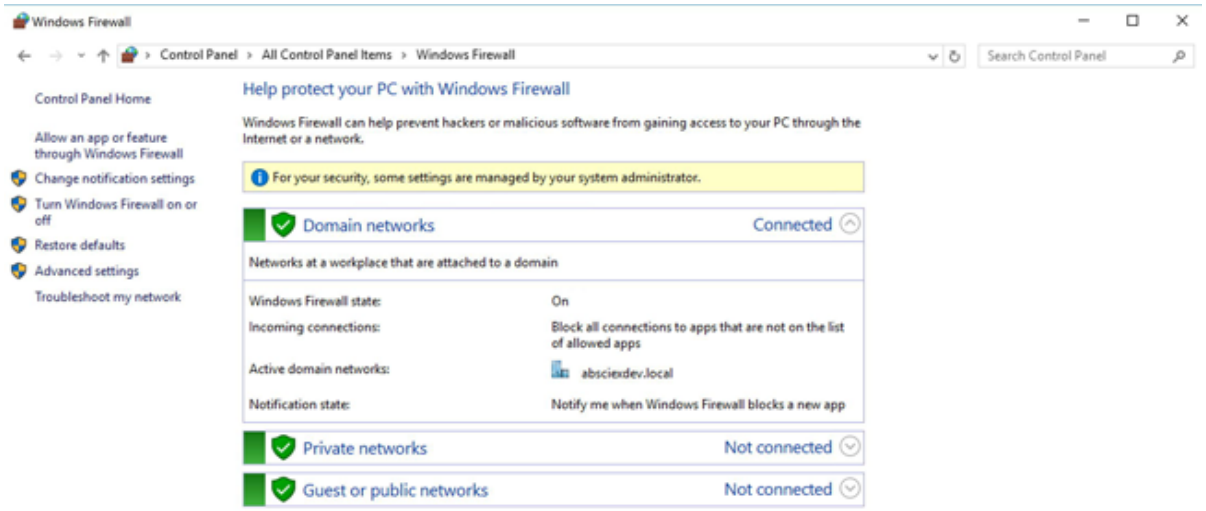
注: 測定用コンピュータでは、キューをクライアントコンピュータからリモートで表示できるよう、バッチの送信後にキューページが開かれた状態で維持されている必要があります。

Windows 測定用コンピュータでファイアウォールを構成する

測定用コンピュータは、Analyst.exe と AnalystService.exe が Windows ファイアウォールを通るよう構成する必要があります。

1. コントロールパネルを開き、Windows ファイアウォールを開きます。

図 5-8 : Control Panel



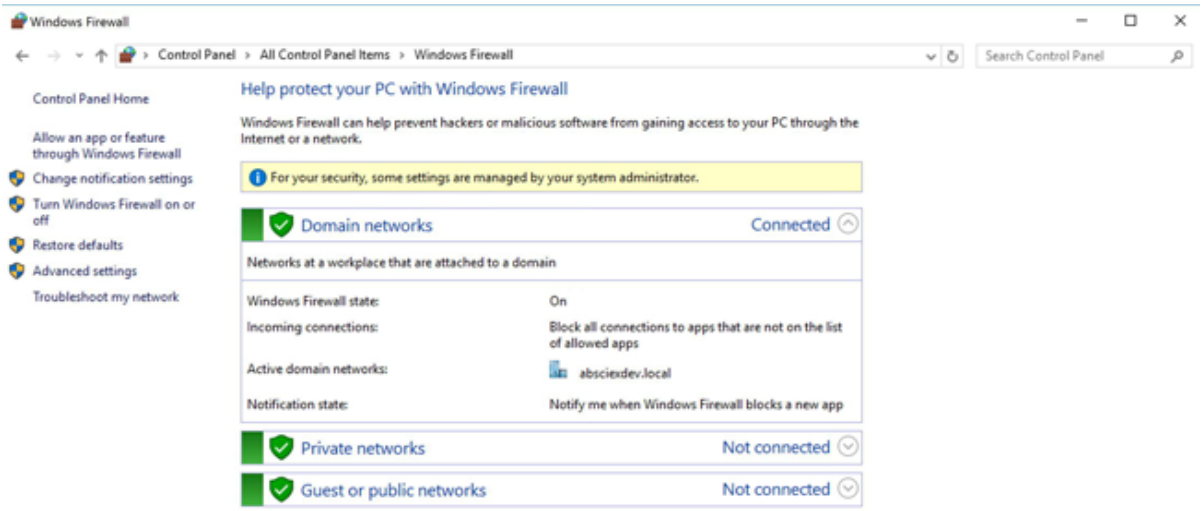
2. 左ペインの **Allow an app or feature through Windows Firewall** をクリックします。
3. **Change Settings.** をクリックします
4. **Allow another app** をクリックします。
   Add an app ダイアログが開きます。
5. **Browse** をクリックし、`C:\Program Files(x86)\Analyst\bin` フォルダーに移動します。
6. **AnalystService.exe** をクリックし、**Open** をクリックします。
7. **Add** をクリックします。
   AnalystService が **Allowed apps and features** リストに追加されます。
8. **AB SCIEX Analyst** がまだ **Allowed apps and features** リストにない場合は、**Analyst.exe** を追加します。追加するには、手順 3 から 7 までを繰り返します。ただし、AnalystService.exe の代わりに **Analyst.exe** を選択します（ステップ 6 で）。
9. **OK** をクリックします。

クライアントコンピュータで Windows ファイアウォールを構成する

クライアントコンピュータの Windows ファイアウォールで、"Allowed apps and features" のリストに Analyst.exe がない場合は、追加してください。

1. コントロールパネルを開き、Windows ファイアウォールを開きます。

図 5-9 : Control Panel



2. 左ペインの **Allow an app or feature through Windows Firewall** をクリックします。
3. **Change Settings.** をクリックします
4. **Allow another app** をクリックします。
   Add an app ダイアログが開きます。
5. **Browse** をクリックし、`C:\Program Files(x86)\Analyst\bin` フォルダーに移動します。
6. **Analyst.exe** をクリックし、**Open** をクリックします。
7. **Add** をクリックします。
   AB SCIEX Analyst が **Allowed apps and features** リストに追加されます。
8. **OK** をクリックします。

リモートワークステーション

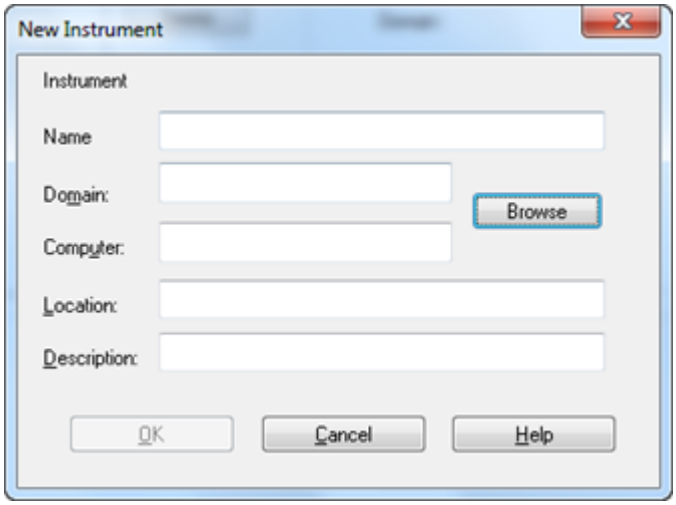
質量分析装置のリストをローカルコンピュータで設定し、これらの質量分析装置のサンプルキューをリモートでモニターできます。ユーザーはこれらのリモートワークステーションで、サンプルキューと質量分析装置の状態のみ表示できます。たとえローカルワークステーションで他のアクションを実行できても、これらをリモートワークステーションで実行することはできません。

注: 測定用コンピュータ(リモートアクセス用)とローカルワークステーション(測定用コンピュータによるアクセス用)は、双方とも同一のネットワークドメインに存在しなくてはなりません。

ワークステーションにアクセスを追加する

1. ドメインベース(user@domain)ユーザーとして Analyst MD ソフトウェアにログインします。
2. Navigation バーの **Configure** の下にある **Security Configuration** をダブルクリックします。
   Security Configuration ダイアログが開きます。
3. Remote Viewers タブを開き、**Add** をクリックします。

図 5-10 : New Instrument ダイアログ

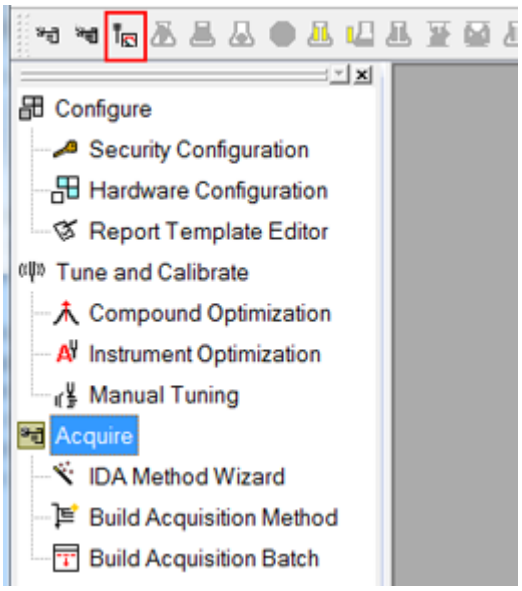


4. **Name** フィールドにワークステーション名を入力します。
   Active Directory がネイティブ環境で使用されている場合、ドメインフィールドは表示されず、ユーザー名は UPN 形式で入力できます。
5. 必要に応じて、**Location** フィールドに場所の情報を入力します。
6. **Browse** をクリックして、**Domain** と **Computer** を参照します。
   Select Computers ダイアログが開きます。
7. **Object Types** をクリックして質量分析装置を選択します。
   Windows Security ダイアログが開きます。
8. ドメイン認証情報を入力して **OK** をクリックします
   Select Computers ダイアログが表示されます。
9. **Locations** をクリックします。
   Locations ダイアログが開きます。
10. リモート測定用コンピュータが配置されているネットワークをクリックし、**OK** をクリックします。
    Select Computers ダイアログが表示されます。
11. **Enter the object names to select** ボックスに測定用コンピュータの名前を入力します。
12. **Check Names** をクリックします。
13. **OK** をクリックします。
14. 必要に応じて、**Description**New Instrument ダイアログのフィールドに説明を入力します。
15. **OK** をクリックします。
    測定用コンピュータ名とドメイン名が Remote Viewers タブに表示されます。
16. **Apply** をクリックします。
17. **OK** をクリックします。
    Security Configuration ダイアログが閉じるます。
18. Analyst MD ソフトウェアを再起動します。

リモート装置の状態とサンプル測定キューを表示する

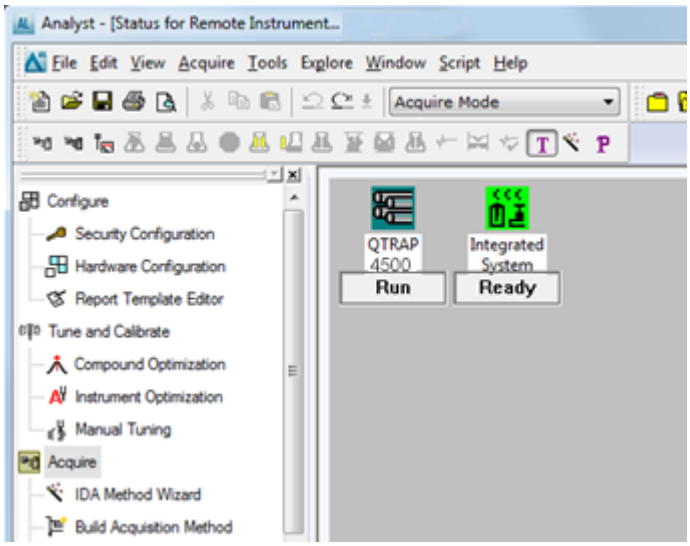
装置や接続中のデバイスの状態と、測定用コンピュータのサンプル測定キューをリモートで表示するには、クライアントコンピュータの Analyst MD ソフトウェアの **Status for Remote Instrument** アイコンを使用します。

図 5-11 : Analyst MD ソフトウェアのリモート装置アイコンのステータス



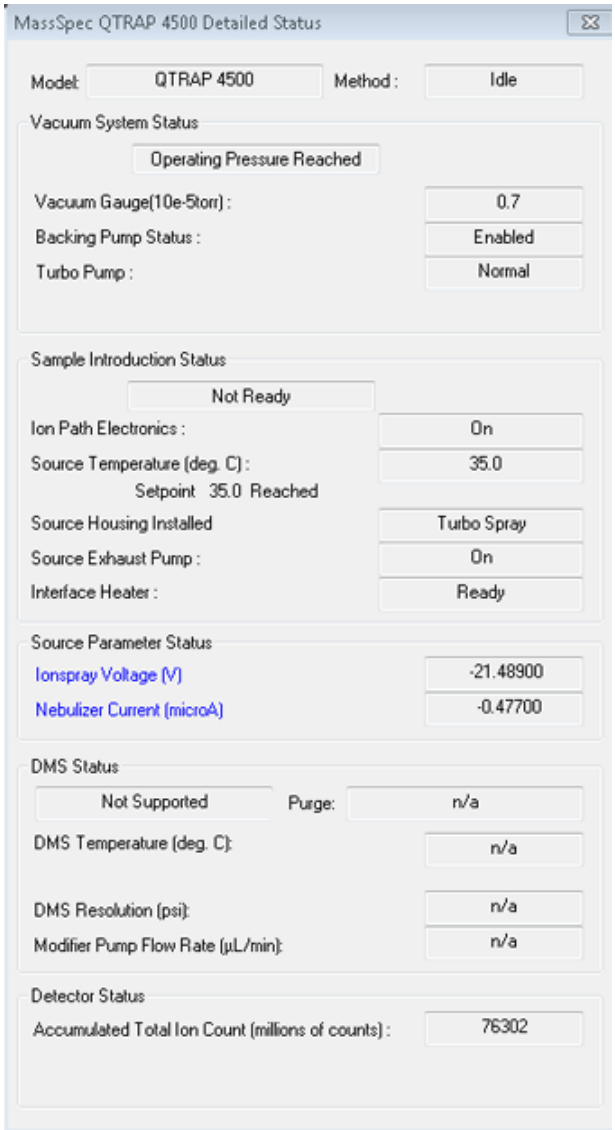
1. ワークステーションにアクセスを追加するの Security Configuration ダイアログでリモート装置を追加するために使用されたのと同じドメインベースのユーザーとして、Analyst MD ソフトウェアにログオンします。
2. クライアントコンピュータの Analyst MD ソフトウェアで、**Acquire** モードが選択されている状態で、**Status for Remote Instrument** アイコンをクリックします。
3. Remote Instrument Station ダイアログの **Select the Instrument Station** フィールドで装置を選択し、**Connect** をクリックします。

図 5-12 : Analyst MD ソフトウェアに表示されるリモートインストルメントステーションと統合デバイス



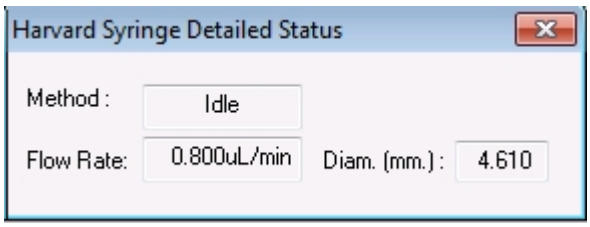
4. 「リモート装置」アイコンをダブルクリックして、詳しい状態を表示します。

図 5-13 : リモート装置の詳細ステータス



5. 「内蔵シリンジ」アイコンをダブルクリックして、詳細ステータスを表示します。

図 5-14 : 内蔵シリンジの詳細ステータス

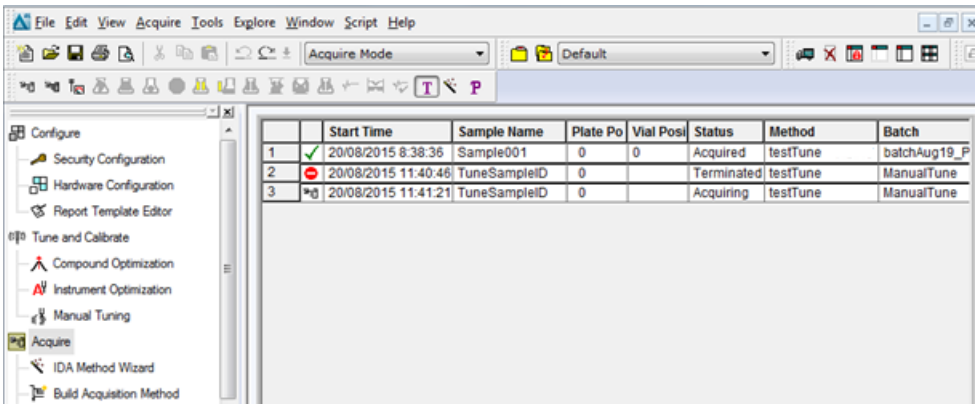


6. 測定コンピュータでサンプル測定キューを表示するには、**Acquire** モードで、Analyst MD ソフトウェアのツールバーにある **Instrument Queue** アイコンをクリックします。

注: クライアントコンピュータからキューをリモートで表示するには、測定用コンピュータでキューページが開かれている必要があります。

7. Remote Instrument Station ダイアログの **Select the Instrument Station** ボックスで装置を選択し、**Connect** をクリックします。
   測定用コンピュータのサンプル測定キューが Analyst MD ソフトウェアに表示されます。

図 5-15 : 測定用コンピュータのサンプル測定キュー



ワークステーションにアクセスを削除する

1. Navigation バーの **Configure** の下にある **Security Configuration** をダブルクリックします。
2. Security Configuration ダイアログで Remote Viewers タブを開きます。
3. 左側のペインでコンピュータを選択します。
4. **Delete** をクリックします。
5. **Yes** をクリックして確認します。
6. **OK** をクリックして Security Configuration ダイアログを閉じます。
7. Analyst MD ソフトウェアを再起動します。

セキュリティ構成を印刷する

セキュリティ構成のコピーをファイルに出力します。

1. Navigation バーの **Configure** の下にある **Security Configuration** をダブルクリックします。
   Security Configuration ダイアログが開きます。
2. **Print** をクリックします。
3. **Apply** をクリックします。
4. **OK** をクリックします。
   Security Configuration ダイアログが閉じるます。

システム健全性の監視 6

補助トレース

ポンプ圧力トレースやカラムオーブン温度トレースなど、LC システムの補助トレースは、各サンプルのデータファイルに保存できます。これらのトレースは、LC システムの状態を監視するために使用できます。トレース、特にポンプ圧力トレースは、LC 関連の問題のトラブルシューティングにも役立ちます。

補助トレース機能は、Analyst MD ソフトウェアバージョン 1.7.3 以降でサポートされています。

補助トレースを有効にする

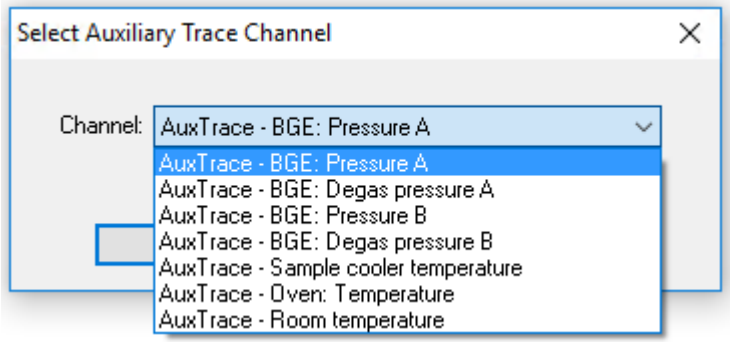
補助トレース機能を有効にするには、ハードウェアプロファイルで LC デバイスを構成するときに次の手順に従います。

1. Create New Hardware Profile または Edit Hardware Profile ダイアログで、LC システムを選択し、**Setup Device** をクリックします。
2. **Enable Aux Trace Monitoring** チェックボックスを選択します。
3. LC システムの構成が完了していることを確認してから、**OK** をクリックします。
4. ハードウェアプロファイルを有効にします。
5. データの取得。

補助トレースを表示する

1. プロジェクトフォルダが選択されていることを確認します。
2. Navigation バーの **Explore** の下にある **Open Data File** をダブルクリックします。
   Select Sample ダイアログが開きます。
3. **Data Files** フィールドで、補助トレース監視を有効にした後に取得したデータファイルをクリックします。
4. **Samples** リストでサンプルを選択してから、**OK** をクリックします。
5. **Explore** > **Show** > **Show Auxiliary Traces** をクリックします。

図 6-1 : Select Auxiliary Trace Channel ダイアログ



6. **Channel** リストからチャンネルを選択した後、**OK** をクリックします。
   選択した補助トレースは、アクティブなペインの下の新しいペインに表示されます。

注入カウンタ

注入カウンターを使用すると、ユーザーは単一の LC-MS/MS システムの特定の分析カラムでのサンプル注入回数を監視できます。この機能は、ユーザーが列を切り替えるタイミングを把握し、バッチの再実行を防ぐのに役立ちます。

注入カウンタを有効にする

1. システムがスタンバイ状態になっていることを確認してください。
2. **Configure** モードで、**Tools** > **Settings** > **Injection Counter Options** をクリックします
3. **Enable Injection Counter** チェックボックスを選択します。
4. 注入がカウントされる分析カラムごとに行を完成させます。
   各行には、次の表のフィールドが含まれています。

表 6-1 : Injection Counter ダイアログフィールド

フィールド	説明
Active	この分析カラムの注入カウントを有効にする場合に選択します。このオプションを選択すると、この分析カラムでの注入回数は、注入ごとに 1 つずつ増加します。列切り替えを使用すると、複数の分析カラムを同時に有効にすることができます。
Column Description	レポートと表示で列を識別するための情報を入力します。ブランド、タイプ、粒子サイズ、カラム径、カラムの長さなどの情報を含めます。
Column S/N	分析カラムのシリアル番号を入力します。
Number of injections	注入カウンタ設定を構成するときは、分析カラムですでに行われた注入の数を入力します。注入カウンタ機能が有効な場合、ソフトウェアは、オートサンプラーを持つ LC システムの操作中にこのフィールドを自動的に増やします。

表 6-1 : Injection Counter ダイアログフィールド (続き)

フィールド	説明
Threshold	警告をトリガーする注入の数を入力します。このしきい値を超えるようなバッチを送信した場合、警告が表示されます。その後、バッチを続行するかキャンセルして、別の分析カラムを使用するかを選択できます。アクティブな分析カラムが変わると、しきい値も変わりす。 **注:** 別のカラムを取り付けた後は、必ず注入カウンタの設定を更新してください。

5. 分析カラムを追加するには、**+**をクリックし、手順 4 を繰り返します。

注: リストから分析カラムを削除するには、カラムの右側にあるマイナス記号（**-**）をクリックします。

6. **OK** をクリックします。

監査 7

このセクションでは、監査機能の使用方法について説明します。Windows の監査機能については、次のセクションを参照：システム監査。

監査証跡

Analyst MD ソフトウェアでは、監査済みイベントが質量分析装置別、プロジェクト別、定量別に監査証跡へとグループ化されます。監査証跡とは、監査済みイベントの記録が保存されたファイルです。監査証跡は、wiff ファイルや Results Table などのファイルと併せて有効な電子記録となり、コンプライアンス目的で使用できるようになります。

表 7-1：Analyst MD ソフトウェア監査証跡監査証跡

監査証跡	記録されるイベントの例	利用可能な監査マップ	デフォルトの監査マップ

装置（ワークステーションごとにひとつ）	• 以下に変更が加えられた場合：
	  • 装置の分解能
	  • 質量キャリブレーション
	  • サンプルキュー
	  • セキュリティ
	  • ハードウェアプロファイル
	• 装置メンテナンスログエントリ
		• `API Instrument` プロジェクト
		• `Project Information` フォルダ
			• 新規インストールでは、デフォルトの監査マップ

表 7-1 : Analyst MD ソフトウェア監査証跡監査証跡 (続き)

監査証跡	記録されるイベントの例	利用可能な監査マップ	デフォルトの監査マップ

プロジェクト(プロジェクトごとにひとつ)	• 以下に変更が加えられた場合:
	  • プロジェクト
	  • メソッド
	  • 定量化
	  • バッチ
	  • データ
	  • Results Table
	  • チューニング
	  • レポートテンプレートファイル
	• モジュールの起動および終了
	• 印刷
		• 各プロジェクト
		• `Project Information` フォルダ
			• デフォルトプロジェクトからコピー

定量(Results Table ごとにひとつ)	以下に変更が加えられた場合: • 定量化メソッド • サンプル情報 • ピーク積分パラメータ	• Results Table ファイル(rdb ファイル)	• 親プロジェクトからコピー

機器監査証跡またはプロジェクト監査証跡に 1000 の監査レコードが含まれると、Analyst MD ソフトウェアは自動的にレコードをアーカイブし、新しい監査証跡を開始します。詳細な情報については、次のセクションを参照:監査証跡レコード。

監査マップ

監査マップは、以下を指定するためのファイルです。

- 監査対象となるイベント。
- オペレータが変更理由を記入する必要のある監査済みイベント。
- 電子署名が必要な監査済みイベント。

質量分析装置とプロジェクトに対して多くの監査マップを作成できますが、測定用コンピュータとプロジェクトごとに一度に使用できる監査マップは 1 つだけです。使用中の監査マップは、その質量分析装置またはプロジェクトのアクティブ監査マップと称されます。

それぞれの監査マップには、監査可能な全イベントのリストが含まれています。マップを使用する状況によっては、これらのイベントは装置監査証跡またはプロジェクトと定量監査証跡にも適用されます。イベントごとに、監査済みかどうか、電子署名が必要かを指定できるほか、イベントの理由について示した既定テキストを最大で 10 件まで設定できます。

ユーザーが新規プロジェクトを作成すると、プロジェクトの監査マップが `Default` プロジェクトからコピーされます。デフォルトプロジェクトのアクティブ監査マップが、新規プロジェクトのアクティブ監査マップとなります。

新たな Results Table を作成する際には、当該プロジェクトのアクティブ監査マップの定量イベントをもとに、定量監査証跡が構成されます。Results Table の保存時には、アクティブ監査マップに含まれている監査構成が、Results Table とともに永久的に保存されます。アクティブ監査マップ（プロジェクトに適用されている）を変更すると、元の監査構成は Results Table ファイルに埋め込まれたままとなります。埋め込み構成は、[設定]タブに表示される最終変更日時によって、変更された監査マップと区別できます。

監査マップの設定

監査が必要なプロジェクトに対して作業を行う前に、標準作業手順に適した監査マップを設定します。Analyst MD ソフトウェアをインストールすると、いくつかのデフォルトの監査マップが表示されますが、それらの 1 つ以上をカスタマイズできます。少なくとも、1 つの適切な監査マップが装置監査証跡で利用可能であり、1 つの適切な監査マップが各プロジェクトで利用可能であることを確認してください。

表 7-2：監査を構成するためのチェックリスト

タスク	次を参照
装置監査証跡用の監査マップを作成する。	• 監査マップを作成する. • 監査マップを変更する.
装置監査証跡用の監査マップを適用する。	• 監査マップを適用する.
新規プロジェクト用のデフォルトのアクティブ監査マップを作成する。	• 監査マップを作成する. • 監査マップを変更する.
新規プロジェクト用のデフォルトのアクティブ監査マップを指定する。	• 監査マップを適用する.
既存のプロジェクトで使用する監査マップを構成する。	• 監査マップを作成する. • 監査マップを変更する. • 他のプロジェクトから監査マップをコピーする.

表 7-2 : 監査を構成するためのチェックリスト (続き)

タスク	次を参照
既存のプロジェクトに監査マップを適用する。	• 監査マップを適用する.

インストール済みの監査マップ

ソフトウェアには、いくつかの監査マップが含まれています。インストール済みの監査マップを表示または修正する方法については、次のセクションを参照:監査マップを変更する。

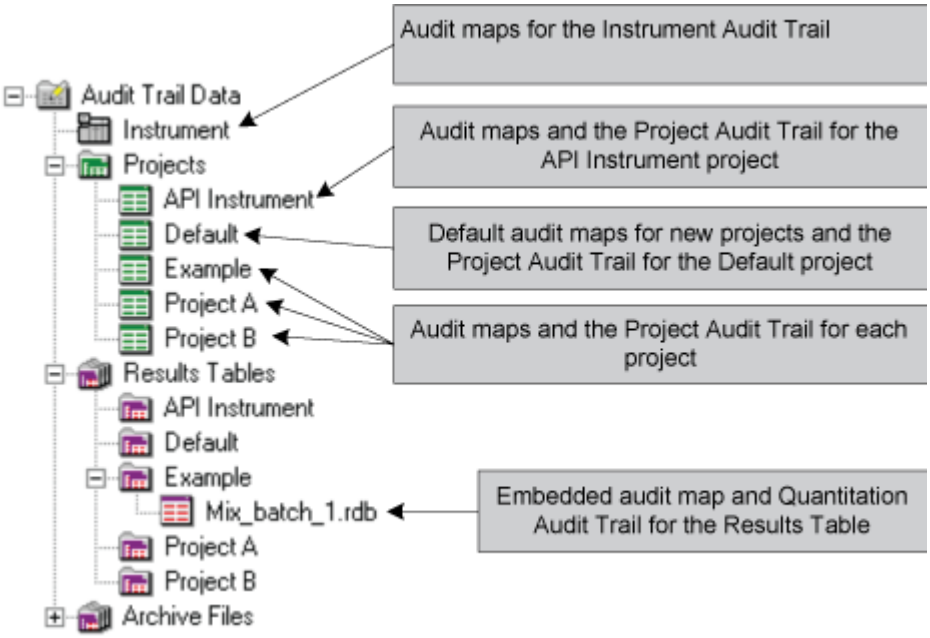
表 7-3 : インストール済みの監査マップ

監査マップ	説明
デフォルトの監査マップ	インストール時には、デフォルトの監査マップは新規プロジェクトのアクティブ監査マップになります。デフォルトでは、あらゆるイベントが Analyst MD では使用できません。以前のバージョンの Analyst MD ソフトウェアで作成されたプロジェクトの監査証跡設定が変換されている場合、デフォルトの監査マップにはその監査構成が含まれています。
Full Audit Map（フル監査マップ）	すべてのイベントが監査されます。すべてのイベントにおいて電子署名と理由の記入が必要です。
No Audit Map（監査マップなし）	イベントは監査されません。
Quant Only Audit Map	定量化イベントのみが監査されます。これらのイベントには電子署名と理由の記入が必要です。
Silent Audit Map（サイレント監査マップ）	すべてのイベントが監査されます。どのイベントでも電子署名と理由の記入は不要です。

監査証跡の種類と監査マップとの関係については、次を参照:表 7-1。監査証跡に記録されるイベントの詳細な情報については、次のセクションを参照:監査証跡レコード。

監査マップと監査証跡が Audit Trail Manager 内のどこに保存されているかについては、図 7-1 を参照してください。

図 7-1 : Audit Trail Manager: 監査マップと監査証跡の場所



監査プロセスについて詳しくは、次を参照: 表 7-2。

監査マップの作業を行う

Analyst MD ソフトウェアには、いくつかのインストール済み監査マップが含まれています。これらを表示して、ひとつまたは複数の既存のマップを修正するのと、新しいマップを作成するのとではどちらの方が簡単かを決定します。監査マップについては、次のセクションを参照: インストール済みの監査マップ。監査の設定における推奨ステップのチェックリストについては、次のセクションを参照: 監査マップの設定。

Analyst MD ソフトウェアまたは File Explorer でアクティブな監査マップが削除された場合、その監査マップを使用するプロジェクトはデフォルトの監査マップ (`Default Audit Map.cam`) を使用します。デフォルトの監査マップは削除できません。

監査マップを作成する

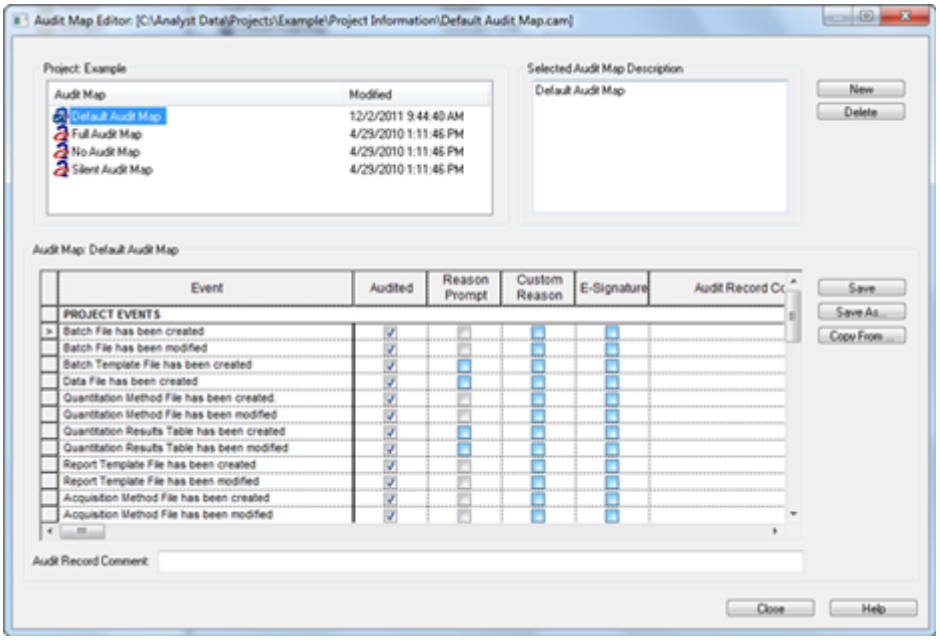
プロジェクトのアクティブ監査マップでは、作成された Results Table において、どのイベントがプロジェクト監査証跡および定量監査証跡に記録されるかが特定されます。

1. **View** > **Audit Trail Manager** をクリックします。
   Audit Trail Manager ウィンドウが開きます。
2. 左側のペインで、**Audit Trail Data** フォルダを展開します。
3. **Projects** フォルダを展開します。
4. Projects セクションで、監査マップを作成するプロジェクトをクリックします。装置監査証跡で使用する監査マップを作成するには、`API Instrument` フォルダをクリックします。

ヒント! 装置監査証跡で使用する監査マップを作成するには、`Projects` フォルダの上にある **Instrument** をクリックします。

5. **Settings** タブで **Edit** をクリックします。
   Audit Map Editor ダイアログが開き、アクティブな監査マップが表示されます。

図 7-2 : Audit Map Editor ダイアログ



6. **New** をクリックします。
   (まだイベントが監査されていない)新しい監査マップが表示されます。
7. 必要に応じて、**Selected Audit Map Description** フィールドに監査マップの説明を入力します。
8. **Audit Map** 表には、以下の各イベントが構成されています。
   - イベントを監査するには、**Audited** 列のチェックボックスを選択してください。

     ヒント! 列の後続のセルに同じテキストまたはチェックボックス値をコピーするには最初の行にテキストを入力し、(その行を先頭に)列内の行を複数選択します。選択した行を右クリックし、**Fill Down** をクリックします。

   - イベント発生時にユーザーが変更の理由を既定テキストから選択できるように要求するには、**Reason Prompt** 列のチェックボックスを選択し、**Predefined Reason** 列に理由を 10 件まで設定します。
   - ユーザーがカスタムの理由を入力できるように要求するには、**Reason Prompt** 列のチェックボックスを選択してから、**Custom Reason** 列のチェックボックスを選択します。
   - イベントの電子署名が必要な場合、**E-Signature** 列のチェックボックスを選択します。
   - このイベントの監査構成に関するメモを追加するには、**Audit Record Comment** 列にコメントを入力します。

9. 監査マップ構成を保存するには、**Save** をクリックします。

注: 監査マップ（cam の拡張子付き）を、使用したいプロジェクトフォルダの **Project Information** サブフォルダに保存します。

これで、監査マップをプロジェクトで使用したり、別のプロジェクトにコピーしたりできます。次のセクションを参照：監査マップを適用するまたは他のプロジェクトから監査マップをコピーする。

監査マップを変更する

変更は、選択したプロジェクトの監査マップにのみ適用されます。Results Table に埋め込まれた監査構成は修正できません。

注意: データ損失の可能性。別のユーザーによって変更中の監査マップを変更しないでください。監査マップを保存するために、前の人が行った変更のみが保持されます。

1. **View** > **Audit Trail Manager** をクリックします。
   Audit Trail Manager ウィンドウが開きます。
2. 左側のペインで、**Audit Trail Data** フォルダを展開します。
3. **Projects** フォルダを展開します。
4. **Projects** セクションで、変更する監査マップを含むプロジェクトをクリックします。
5. **Settings** タブで **Edit** をクリックします。
   Audit Map Editor ダイアログが開き、アクティブな監査マップが表示されます。
6. **Projects** セクションで、修正する監査マップをクリックします
7. 監査マップテーブルで、構成に変更を加えます。表の詳細な情報については、**Help** ヘルプをクリックしてください。
8. 監査マップを保存するには、**Save** をクリックします。

他のプロジェクトから監査マップをコピーする

監査マップはプロジェクト間でコピーできます。

注意: 結果が不正確になる可能性。Analyst MD ソフトウェア以外のプロジェクト間でカムファイル (監査マップ) をコピーしないでください。コピーすると、監査記録が不正確になる可能性があります。

1. **View** > **Audit Trail Manager** をクリックします。
   Audit Trail Manager ウィンドウが開きます。
2. 左側のペインで、**Audit Trail Data** フォルダを展開します。
3. **Projects** フォルダを展開します。
4. **Projects** セクションで、監査マップが貼り付けられるプロジェクトをクリックします。
5. **Settings** タブで **Edit** をクリックします。
   Audit Map Editor ダイアログが開き、アクティブな監査マップが表示されます。
6. **New** をクリックします。

Audit Map Editor ダイアログに（どのイベントも監査されていない）新しい監査マップが表示されます。

7. **Copy From** をクリックします。
   Open ダイアログボックスが表示されます。
8. コピーしたい監査マップを参照して選択し、**Open** をクリックします。監査マップファイルには cam の拡張子が付いています。これらは各プロジェクトの Project Information フォルダに保存されます。
   選択した監査マップの構成が開きます。
9. コピーした監査マップを現在のプロジェクトに保存するには、**Save** をクリックします。

監査マップを適用する

監査マップが装置監査証跡またはプロジェクト監査証跡に適用されると、これがアクティブ監査マップとなります。どのイベントが監査証跡に記録されるかは、アクティブ監査マップの監査構成によって決まります。

プロジェクトのアクティブ監査マップには、プロジェクト監査証跡用の監査構成に加え、（作成されたあらゆる Results Table の）定量監査証跡用の監査構成が格納されています。

1. **View** > **Audit Trail Manager** をクリックします。
   Audit Trail Manager ウィンドウが開きます。
2. 左側のペインで **Audit Trail Data** フォルダを展開し、以下のいずれかを実行します。
   - 監査マップを **Instrument Audit Trail** に適用するには、**Instrument** をクリックします。
   - プロジェクトに監査マップを適用するには、**Projects** フォルダを展開してから、監査マップを適用するプロジェクトをクリックします。
   - 新しいプロジェクト向けにデフォルトのアクティブ監査マップを指定する場合は、**Projects** フォルダを展開し、**Default** をクリックします。
3. 右側のペインで、**Settings** タブをクリックします。
4. **Available Audit Trail Maps** フィールドで、適用する監査マップをクリックします
5. **Apply** をクリックします。

監査証跡の表示、印刷、検索

本項では、監査証跡、アーカイブ済みの監査証跡、装置メンテナンスログのエントリーの表示について説明します。また、監査証跡内の監査レコードを印刷、検索、並べ替えるための手順も記されています。

監査証跡の表示

1. **View** > **Audit Trail Manager** をクリックします。
   Audit Trail Manager ウィンドウが開きます。
2. 左側のペインで **Audit Trail Data** フォルダを展開し、以下のいずれかを実行します。

- 装置監査証跡を表示するには、**Instrument** をクリックします。装置特有のイベント（質量校正テーブルの置き換えなど）を表示するには、質量分析装置に直接接続されているコンピュータ上に記録されている装置監査証跡を表示します。
- プロジェクト監査証跡を表示するには、**Projects** フォルダを展開し、監査証跡が含まれるプロジェクトをクリックします。
- 定量監査証跡を表示するには、**Results Tables** フォルダを展開し、プロジェクトフォルダを適宜に展開して、該当する監査証跡用の **Results Table** ファイルをクリックします。

ヒント!

- 監査されたイベントが wiff ファイルを参照している場合は、**Audit Trail** から wiff ファイルを開きます。**Change Description** 列で、ファイルへのリンクをクリックします。
- 監査レコードに保存されている定量メソッドとサンプルインデックスを使用してサンプルピークデータを表示するには、対応する **Results Table** を開き、監査証跡 **History** 列で **Review** をクリックします。定量化メソッドが監査証跡の作成時に使用された方法から変更された場合、元の結果とは異なる結果がピークに表示される可能性があります。元の結果を確認するには、適切なバージョンのソフトウェアを使用してください。

Results Table に埋め込まれた監査構成を表示する

Results Table に用いられる監査構成は、Results Table の作成時に Results Table ファイルに埋め込まれます。Results Table の監査構成は変更できません。監査マップ名の横に表示されるタイムスタンプは、構成の埋め込みに用いられた監査マップが最後に保存された時間を示しています。

1. **View** > **Audit Trail Manager.**をクリックします
   Audit Trail Manager ウィンドウが開きます。
2. 左側のペインで、**Audit Trail Data** フォルダを展開します。
3. **Results Tables** フォルダを展開します。
4. **Results Tables** セクションで、監査マップの表示元となる Results Table が含まれるプロジェクトを展開します。
5. 監査マップを表示する **Results Table** ファイルをクリックします。
   右側のペインで監査証跡が開きます。
6. Settings タブで **Details** をクリックします。

   Results Table Audit Trail Settings ダイアログが開き、Results Table の監査証跡構成が表示されます。

装置監査証跡の監査レコードの詳細を表示する

以下の監査済みイベントの詳細を表示できます：質量校正テーブルへの変更、分解能テーブルへの変更、装置メンテナンスログへのエントリー。

1. **View** > **Audit Trail Manager** をクリックします。
   Audit Trail Manager ウィンドウが開きます。
2. 左側のペインで、**Audit Trail Data** フォルダを展開します。

3. **Audit Trail Data** セクションの **Instrument** をクリックします。監査証跡が表示されない場合は、右側のペインで **History** タブをクリックします。
   監査証跡が開きます。
4. レコードに追加の詳細が含まれている場合は、**Review** 列で **History** をクリックします。

アーカイブ済み監査証跡の表示

装置監査証跡またはプロジェクト監査証跡に 1,000 の監査レコードが含まれると、Analyst MD ソフトウェアは自動的にレコードをアーカイブし、新しい監査証跡を開始します。アーカイブされた監査ファイルには、監査証跡のタイプと日付および時刻に基づいて名前が付けられます（例：PAT-Archive-201609300820.ata）。

1. **View** > **Audit Trail Manager** をクリックします。
   Audit Trail Manager ウィンドウが開きます。
2. 左側のペインで、**Audit Trail Data** フォルダを展開します。
3. **Archive Files** フォルダを展開します。
4. **Archive Files** セクションで、表示するアーカイブされた監査証跡を含むプロジェクトを展開します。
5. 表示したい監査証跡をクリックします。
   右側のペインでアーカイブ済み監査証跡が開きます。
6. 監査証跡が開かない場合、右側のペインの **History** タブをクリックします。
   監査証跡が開きます。

ヒント! 監査証跡は左側のペインを右クリックし、**Open Archives** をクリックして、アーカイブされた監査証跡を開きます。Open ダイアログボックスが表示されます。該当する Project フォルダを参照し、**Project Information** フォルダでアーカイブ済み監査証跡ファイルを選択します。これらのファイルには ata の拡張子が付けられています。

監査証跡の印刷

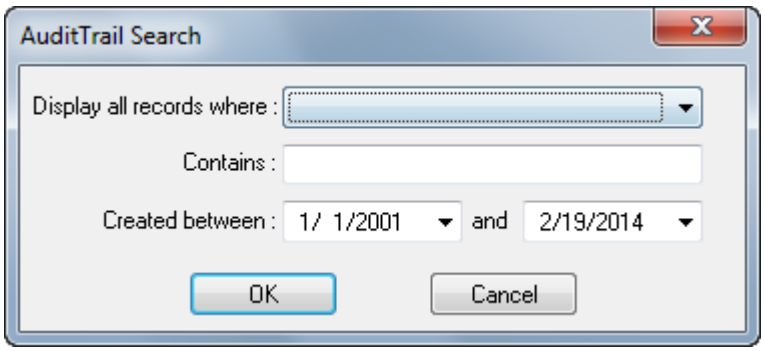
1. **View** > **Audit Trail Manager** をクリックします。
   Audit Trail Manager ウィンドウが開きます。
2. 監査証跡を選択します。
3. **History** タブを右クリックし、**Print** をクリックして以下のいずれかを実行します。
   - 現在のページを印刷するには、**Current Page** をクリックします。
   - 監査証跡の全ページを印刷するには、**All Pages** をクリックします。

監査レコードを検索する

1. **View** > **Audit Trail Manager** をクリックします。
   Audit Trail Manager ウィンドウが開きます。
2. 監査証跡を選択します。
3. 検索したい監査証跡を表示します。

4. **History** タブを右クリックし、**Search** をクリックします。

図 7-3 : Audit Trail Search ダイアログ



5. **Display all records where** リストと **Contains** フィールドを使用して、検索するレコードを選択します。
6. 必要に応じて、**Created between** リストで開始日と終了日を選択します。
7. **OK** をクリックします。
   指定した基準と一致するレコードのみがリストされます。

ヒント! すべてのレコードをリストするには、**All** をクリックします。レコードを数値順、アルファベット順、日付順に並び替えるには、該当する列の見出しをクリックします。

監査証跡 A

このセクションでは、装置、プロジェクト、および定量監査証跡に保存されているすべての監査済みイベントのリストを提供します。

ファイルに監査対象の変更が加えられるたびに、あるいは監査対象のイベントが発生するたびに、以下の情報が保存されます。

- レコード数
- 日付とタイムスタンプ
- ユーザー名
- ユーザーのフルネーム
- Analyst MD ソフトウェアモジュール。
- 変更の説明。
- 変更の理由（必要に応じて）
- 電子署名（必要に応じて）

監査証跡レコード

装置、プロジェクト、定量監査証跡は暗号化されたファイルです。いずれの監査証跡ファイルも、ルートディレクトリ下のプロジェクトディレクトリに保存されます。

ファイルに監査対象の変更が加えられるたびに、あるいは監査対象のイベントが発生するたびに、以下の情報が保存されます。

- レコード数
- 日付とタイムスタンプ
- ユーザー名
- ユーザーのフルネーム
- Analyst MD ソフトウェアモジュール。
- 変更の説明。
- 変更の理由（必要に応じて）
- 電子署名（必要に応じて）

監査証跡アーカイブ

プロジェクト監査証跡と装置監査証跡には監査記録が蓄積されるため、ファイルが次第に大きくなり、アクセスや管理が困難となる可能性があります。定量監査証跡に保存される記録の数は通常少なめで、管理しやすくなっています。

装置監査証跡またはプロジェクト監査証跡のレコード数が 1000 件に達した際には、ファイルがアーカイブされた旨についての通知と併せて、最終レコードが追加されます。続いて監査証跡が自動的に Project Information フォルダに保存され、監査証跡のタイプと日時に基づいて名前が付けられます（例:）、「PAT-Archive-201609300820.ata」。その後、新たな装置監査証跡またはプロジェクト監査証跡が作成され、アーカイブされた監査証跡の最初のレコードにはパスが示されます。

装置監査証跡イベント

コンピュータには、それぞれ 1 つの装置監査証跡があります。この監査証跡には、質量キャリブレーション分解能テーブルへの項目の追加または置き換え、システム構成の変更、セキュリティイベント、装置メンテナンスログへのエントリといった各種イベントが記録されます。質量分析装置に直接接続されていないコンピュータの装置監査証跡には、セキュリティイベントのみが記録されます。

装置監査証跡には以下のイベントが記録されます。

- 質量キャリブレーションテーブルの置き換え。
- 質量キャリブレーションテーブルの追加。
- 分解能テーブルの置き換え。
- 分解能テーブルの追加。
- ハードウェアプロファイルの有効化。[4]
- ハードウェアプロファイルの無効化。[4]
- 装置メンテナンスログエントリーへの入力。
- バッチファイルの送信。[4]
- 測定に向けたサンプルの送信。[4]
- バッチファイルにおけるポジション x からポジション y へのサンプルの移動。[4]
- バッチの移動。[4]
- サンプルの再測定。[4]
- 質量校正テーブルと分解能テーブルの変更。
- 分解能テーブルの置き換え - プロンプトなし。[4]
- 装置設定の変更。
- 装置キャリブレーションの承認。
- 質量キャリブレーションテーブルの置き換え。[4]
- ユーザーによるログイン。[4]
- ユーザーによるログアウト。[4]
- ユーザーがログインに失敗。[4]
- セキュリティ通知の送信。[4]
- セキュリティ構成の修正。[4]

[4] このイベントは特定の理由で監査することはできません。サイレントで監査するか、あるいはまったく監査しないかのいずれかです。

- デュオバルブスイッチカウンターのリセット。
- ユーザーの追加。[4]
- ユーザーの削除。[4]
- ユーザータイプの追加。[4]
- ユーザータイプの削除。[4]
- ユーザータイプの変更。[4]
- ユーザーモードの変更。[4]
- ユーザーによるユーザータイプの変更。[4]
- 測定用アカウントの変更。[4]
- 画面ロックの変更。[4]
- 自動ログアウトの変更。[4]
- 装置の追加。[4]
- 装置の削除。[4]
- プロジェクト役割の追加。[4]
- プロジェクト役割の変更。[4]
- プロジェクト役割の削除。[4]
- プロジェクトセキュリティの変更。[4]
- チューニングパラメータ設定の変更。[4]

プロジェクト監査証跡イベント

いずれのプロジェクトにもプロジェクト監査証跡が 1 つ存在します。プロジェクト監査証跡には、プロジェクト、データ、定量、メソッド、バッチ、チューニング、Results Table、レポートテンプレートファイルの作成、修正、削除といったイベント、ならびにモジュールの起動、終了、および印刷イベントが記録されます。

プロジェクト監査証跡には、以下のイベントが記録されます。

- 監査マップの作成。[5]
- 監査マップの修正。[5]
- 監査マップの削除。[5]
- バッチファイルの作成。[6]
- バッチファイルの修正。[6]
- バッチテンプレートファイルの作成。[6]
- データファイルの作成。[6]

[5] このイベントの監査はサイレントに実行されるため、Audit Map Editor ダイアログには表示されません。
[6] このイベントは特定の理由で監査することはできません。サイレントで監査するか、あるいはまったく監査しないかのいずれかです。

- 定量化メソッドファイルの作成時。[6]
- 定量化メソッドファイルの修正時。[6]
- 定量化 Results Table の作成時。[6]
- 定量化 Results Table の修正時。[6]
- レポートテンプレートファイルの作成。
- レポートテンプレートファイルの修正。
- 測定メソッドファイルの作成。
- 測定メソッドファイルの修正。
- モジュールへのアクセス。[6]
- モジュールを閉じる。[6]
- データファイルへのサンプルの追加。[6]
- プリンタでドキュメントを印刷。
- プリンタでドキュメントを印刷する操作を完了。[6]
- データファイルを開く。[6]
- Explore 履歴ファイルの保存。
- 処理済みデータファイルの保存。
- ファイルのチェックサムを実行。[6]
- プロジェクト設定の変更。[7]
- 処理アルゴリズムの変更。[6]

定量化監査証跡イベント

いずれの Results Table ファイルにも、定量監査証跡が 1 つ保存されます。Results Table が作成されると、プロジェクト内のアクティブ状態の Results Table が（定量の監査証跡に使用できるよう）Results Table ファイルに保存されます。この埋め込み監査マップは、Results Table の作成後は変更できません。Results Table への変更は、すべて埋め込み監査マップに基づいて監査されます。（プロジェクト内の）アクティブ監査マップへの変更は、既存の Results Table には反映されませんが、新しい Results Table ではいずれも変更済みのアクティブ監査マップが用いられます。

定量監査証跡イベントの説明として、データに対して実行された操作（キャリブレーションからのポイントの除去、自動および手動のベースライン適合、カーブ適合の変更など）が挙げられます。

定量監査証跡内のサンプルピーク積分に関する監査レコードには、追加の詳細が加えられます。これらのレコードとして、Results Table の各サンプルに関連した最新の定量処理パラメータが挙げられます。たとえば Results Table の監査証跡は、自動ピーク積分への手動修正で用いられたパラメータを表していることがあります。

定量監査証跡には、以下のイベントが記録されます。

- 定量化メソッドの更新。

[7] このイベントは常に監査されます。

- 定量ピークの元の状態への復元。
- 定量ピークの積分。
- Results Table の作成。
- 定量化メソッドの変更。
- Results Table へのファイルの追加。
- Results Table からのファイルの削除。
- QA レビュアーによる Results Table へのアクセス。
- Results Table の保存。
- Results Table の監査証跡エントリが削除されました。
- 「IT の使用」の変更。
- 「サンプル名」の変更。
- 「サンプル ID」の変更。
- 「サンプルタイプ」の変更。
- 「サンプルコメント」の変更。
- 「サンプルの注釈」の変更。
- 「比重量」の変更。
- 「希釈係数」の変更。
- 「濃度」の変更。
- 「分析試料の注釈」の変更。
- 「Formula 列」の変更。
- 「化学式名」の変更。
- 「化学式文字列」の変更。
- 「Formula 列」の削除。
- 「カスタムタイトル」の変更。
- サンプルの追加／削除。

AAC 監査証跡

各 Analyst Administrator Console (AAC)サーバには、対応する監査証跡があります。この機能は、Analyst MD ソフトウェアではサポートされていません。

セキュリティを追加でカスタマイズする　B

本項では、データを守るための Analyst MD は、データの安全性を確保するために提供されます。

データファイルの変更（Explore Processing）

Explore Processing History は、データファイル用の処理パラメータへの変更記録が含まれるファイルを指します。これらのレコードは、変更内容を追跡できるよう手動で作成する必要があります。現在の変更内容のみが保存されます。Explore Processing History ファイルが作成された後は、Analyst MD ソフトウェア内で変更または削除することはできません。

変更履歴をデータファイルに保存すれば、この履歴を用いることで、いかなる変更時点のデータファイルも表示することができます。履歴を修正すること、あるいは履歴内のデータファイルの前バージョンを保存することはできません。

Explore Processing History ファイルには以下の処理パラメータが記録されます。

- スムージング/前回のポイント加重
- スムージング/現在のポイント加重
- スムージング/次のポイント加重
- ガウシアンスムージング/フィルター幅
- ガウシアンスムージング/距離
- セントロイドオプション/統合距離
- セントロイドオプション/最小幅
- セントロイドオプション/X 値の最大ピークを使用
- ベースライン除去/ウィンドウ幅
- Threshold
- ノイズフィルター/最小ピーク幅
- ベースピーククロマトグラム/質量許容範囲
- 追加
- 除去

Explore Processing History ファイルを作成する

Explore Processing History ファイル（eph）は、Analyst MD ソフトウェアで変更または削除できません。

Explore モードで、データファイルのペインを右クリックし、**Save Explore History** をクリックします。Explore Processing History ファイルは、プロジェクトフォルダの Processing Methods サブフォルダに保存されます。

ヒント! Explore Processing History ファイルを追跡できるよう、履歴ファイルにデータファイルと似た名前を付けて保存します。

Explore Processing History ファイルを表示する

1. **File** > **Open** をクリックします。
   Open ダイアログボックスが表示されます。
2. **Files of type** リストの **Explore History Files (eph)** をクリックします。
3. **Files** フィールドでファイルをクリックし、**OK** をクリックします。
   wiff ファイルが、その下のペインで Explore Processing History ファイルとともに開きます。
4. 処理パラメータを用いて History タブで wiff ファイルを表示するには、History 列の下にある **Review** をクリックします。
5. Explore Processing ウィンドウを印刷するには、**History**History タブを右クリックして **Print** をクリックし、**Current Page** または **All Pages** のいずれかをクリックします。
6. **Explore** モードでアクティブなペインにデータファイルの現在のデータ処理履歴を表示するには、**Explore** > **Show** > **Show History.**をクリックします。表示される履歴は自動的に保存されず、処理のレビューに使用することもできません。

装置メンテナンスログエントリを追加する

質量分析装置の保守（システムメンテナンス、クリーンアップ、参照チェックなど）を実行する際には、装置メンテナンスログを使用して装置監査証跡にメンテナンス情報を記録します。

1. **View** > **Audit Trail Manager** をクリックします。
   Audit Trail Manager ウィンドウが開きます。
2. 左側のペインで、**Audit Trail Data** フォルダを展開します。
3. Audit Trail Data セクションで **Instrument** をクリックします。
4. 右側のペインで Maintenance Log タブを開きます。
5. 該当するフィールドにメンテナンス情報を入力します。
6. ログエントリーを保存するには、**Submit** をクリックします。

装置メンテナンスログエントリを表示する

1. **View** > **Audit Trail Manager** をクリックします。
   Audit Trail Manager ウィンドウが開きます。
2. 左側のペインで、**Audit Trail Data** フォルダを展開します。
3. Audit Trail Data セクションで **Instrument** をクリックします。
4. 監査証跡が表示されない場合は、右側のペインで History タブを開きます。
   監査証跡が開きます。
5. 装置メンテナンスログエントリのレコードを表示するには、**History** 列の **Review** をクリックします。
   Audit Trail History ダイアログが開き、ログエントリの詳細が表示されます。

ヒント! 装置監査証跡の全ログエントリを検索するには、**Search** をクリックします。Audit Trail Search ダイアログで、変更についての説明に装置メンテナンスが含まれる記録をすべて表示するオプションを使用します。

メール通知を構成する

Analyst MD ソフトウェア構成、設定は、1 日のうちにログオンに 3 回失敗した場合にメール通知が送信されるよう構成できます。このメール通知機能は、ソフトウェアが統合または混合モードに入っている場合にのみ使用できます。セキュリティモードの詳細な情報については、次のセクションを参照：Analyst MD ソフトウェアおよび Windows のセキュリティ: 互いに連動。

メールの受信者は、SMTP 準拠のメールサーバー上の有効なアカウントにアクセスできる必要があり、Analyst MD ソフトウェアを搭載したコンピュータは、SMTP サーバーにアクセスできる必要があります。

1. **View** > **Audit Trail Manager** をクリックします。
   Audit Trail Manager ウィンドウが開きます。
2. Audit Trail Manager ウィンドウの左側のペインを右クリックし、**Options** をクリックしてから **E-Mail Notification Settings** をクリックします。
   Audit Trail Options ダイアログが開き、**Security Mail Settings** タブが表示されます。
3. **Send e-mail message(s) after 3 logon failures within 24hr.** チェックボックスを選択します。
4. **SMTP Server** フィールドに、SMTP サーバーの名前を入力します。

   注: SMTP アカウントからメールサーバーにメールが送信されます。SMTP サーバーを特定するには、ご自身のメールアプリケーションを使用してください。

5. **Port Number** フィールドにポート番号を入力します。
   Default ボタンを押すと、デフォルトのポート番号である「25」が入力されます。
6. **To** フィールドに、メッセージの送信先のメールアドレスを入力します。例：
   username@domain.com.
7. **From** フィールドには、メッセージの **From** フィールドに表示する名前を入力します。たとえば、コンピュータの名前を入力して、ログオンに失敗したコンピュータの記録を保持します。**From** フィールドの値にはスペースを使用できません。
8. **Subject** フィールドに、メッセージの件名を入力します。
9. **Message** フィールドに、メッセージの本文を入力します。
10. 構成の内容を確認するには、**Send Test Mail** をクリックします。
11. 構成を保存するには、**OK** をクリックします。

    注: メール通知が **Inbox** に送信されない場合は、**Junk E-mail** フォルダを確認してください。

    ヒント! 電子メール通知を無効にするには、**Send email message(s) after 3 logon failures within 24hr.**チェックボックスをオフにします。

データファイルのチェックサム

データファイルのチェックサムをユーザーに実行させることが推奨されます。チェックサム機能は、データファイルの整合性を検証するための巡回冗長検査です。チェックサム機能は、Analyst MD ソフトウェアの新規インストールに対してデフォルトで有効になっています。ユーザーが Analyst MD ソフトウェアの現在のバージョンにアップグレードする場合、アップグレード前のチェックサム設定が維持されます。

このチェックサム機能の使用は、質量分析装置が in vitro 診断装置として用いられている場合には必須となります。

データファイルチェックサム機能が有効になっている場合、ユーザーがデータ（wiff）ファイルを作成するたびに、ソフトウェアは MD5 公開暗号化アルゴリズムに基づくアルゴリズムを使用してチェックサム値を生成し、その値をファイルに保存します。チェックサムが検証されると、ソフトウェアはチェックサムを計算し、計算されたチェックサムをファイルに保存されているチェックサムと比較します。

チェックサムの比較により、以下の 3 つの結果が生じることがあります。

- 値が一致する場合、チェックサムは有効となります。
- 値が一致しない場合、チェックサムは無効となります。無効なチェックサムは、ファイルがソフトウェアの外部で変更されたか、チェックサム計算が有効になっていてチェックサムが元のチェックサムと異なるときにファイルが保存されたことを示します。
- ファイルにチェックサム値が保存されていない場合、チェックサムは検出されません。データファイルのチェックサム機能が無効になっているときにファイルが保存されたため、ファイルにはチェックサム値が保存されていません。

データファイルのチェックサムを検証する

データファイルを開くたびに、ユーザーはチェックサムを確認できます。本項ではチェックサムを検証する方法、ならびにデータファイルのチェックサム機能を有効および無効にするステップについて説明します。

チェックサムの計算は、大きなデータファイルの場合、1 分以上かかることがあります。取得中は、作成中のファイルのチェックサムを確認できません。

1. **File** > **Open Data File** をクリックします。
   Select Sample ダイアログが開きます。
2. **Data Files** フィールドで、データ（wiff）ファイルを選択します。
3. **Verify Checksum** をクリックします。

   ExplorDir メッセージダイアログが開き、チェックサム比較の結果が Valid、Invalid、Not found として表示されます。

データファイルのチェックサム機能を有効または無効にする

Analyst MD ソフトウェアは、Audit Trail Manager のショートカットメニューのコマンドの横にあるチェックマークによって、データファイルチェックサム機能が有効になっているかどうかを示します。

1. **View** > **Audit Trail Manager** をクリックします。
   Audit Trail Manager ウィンドウが開きます。

2. Audit Trail Manager ウィンドウの左側のペインを右クリックし、**Options** をクリックします。
3. **Data File Checksum** をクリックします。
   データファイルのチェックサム機能が有効になっている場合は、コマンドの横にチェックマークが表示されます。データファイルのチェックサム機能が無効になっている場合、チェックマークは消えます。

特別測定用アカウント C

注: SCIEX は、Analyst MD ソフトウェアでのネットワーク取得機能の使用をサポートしていません

ネットワークフォルダにデータを取得する規制環境では、通常、ほとんどのユーザーは保存先フォルダの削除権限を持っていません。この場合、Analyst MD ソフトウェアがネットワークフォルダにデータを正常に取得するためには、削除アクセスが必要となるため、問題が発生します。

特別測定用アカウント(SAA)機能は、AnalystService にのみ削除権限を付与することにより、クローズドネットワーク環境でのネットワーク取得をサポートします。この機能を有効にするには、ラボの管理者は、該当するフォルダのフル コントロール権限を持つアカウントを作成し、そのアカウントを Analyst MD ソフトウェアの Security Configuration ダイアログの Special Acquisition Administrator Account グループに指定します。これにより、ほとんどのユーザーが削除権限を持っていないにもかかわらず、Analyst MD ソフトウェアは正常にデータを取得することができます。測定用アカウントの選択については、次のセクションを参照:測定用アカウントを選択する。

SAA には次が必要です:

- サーバーデータフォルダのフルコントロール(推奨)または変更(最小)権限。
- `WIFF_CACHE_BACKUP` フォルダのフルコントロール(推奨)または変更(最小)権限。

SAA は次を行う必要はありません。

- コンピュータの管理者グループに属します。
- Analyst Administrator Console (AAC)ユーザープール、コンソール管理者ワークグループ、またはその他のワークグループに属します。
- Analyst MD のソフトウェアセキュリティデータベースに登録します。

お問い合わせ先

お客様のトレーニング

- 北米：NA.CustomerTraining@sciex.com
- ヨーロッパ：Europe.CustomerTraining@sciex.com
- ヨーロッパおよび北米以外：sciex.com/education

オンライン学習センター

- SCIEX Now Learning Hub

SCIEX サポート

SCIEX およびその代理店は、十分に訓練を受けた保守/技術専門要員を世界中に配置しています。システムまたは起こり得る技術的問題に関するご質問にお答えします。詳細な情報については、SCIEX web サイト (sciex.com) を参照するか、以下の連絡先までお問い合わせください。

- sciex.com/contact-us
- sciex.com/request-support

サイバーセキュリティ

SCIEX 製品のサイバーセキュリティに関する最新のガイダンスについては、sciex.com/productsecurity を参照してください。

ドキュメント

このバージョンのドキュメントは、以前のすべてのバージョンのドキュメントに優先します。

このドキュメントを電子的に閲覧するには Adobe Acrobat Reader が必要です。最新バージョンをダウンロードするには、https://get.adobe.com/reader にアクセスします。

ソフトウェア製品のドキュメントについては、ソフトウェアに付属のリリースノートまたはソフトウェアインストールガイドを参照してください。

ハードウェア製品のドキュメントを検索するには、システムまたはコンポーネントに付属の *カスタマーリファレンス* DVD を参照してください。

注: このドキュメントの無料の印刷版を請求するには、sciex.com/contact-us までお問い合わせください。