ラボ管理者ガイド

SCIEX OS ソフトウェア

RUO-IDV-05-7370-JA-N

2024 年 11 月

目次

1 はじめに 6

2 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
SCIEX OS ソフトウェアおよび Windows セキュリティ：互いに連動 7
SCIEX OS ソフトウェアと Windows の監査証跡 8
カスタマーセキュリティガイダンス: バックアップ 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 10
Active Directory への対応 10
Windows ファイルシステム 10
ファイルおよびフォルダアクセス許可 10
システム監査 11
イベントログ 11
Windows アラート 11

3 電子ライセンス 12
サーバーベースの電子ライセンスの借用 12
サーバーベースの電子ライセンスの返却 13

4 アクセス制御 15
セキュリティ情報の場所 15
ソフトウェアセキュリティのワークフロー 15
SCIEX OS ソフトウェアをインストール 16
システム要件 16
プリセット監査オプション 17
セキュリティモードの設定 17
Security Mode を選択する 17
ワークステーションのセキュリティオプションの設定（Mixed mode） 18
メール通知の構成（Mixed Mode） 18
SCIEX OS ソフトウェアへのアクセスの構成 19
SCIEX OS 許可 20
ユーザーと役割について 27
ユーザーの管理 34
役割の管理 35
ユーザー管理設定のエクスポートとインポート 36
ユーザー管理設定のエクスポート 36
ユーザー管理設定のインポート 36

ユーザー管理設定の復元 37
プロジェクトとプロジェクトファイルへのアクセスの設定 37
プロジェクトフォルダ 37
ソフトウェアのファイルタイプ 38

5 中央管理者コンソール 40
ユーザー 40
ユーザープール 40
ユーザーの役割と権限 41
ワークグループ 48
ワークグループを作成する 49
ワークグループを削除する 49
ユーザーまたはグループをワークグループに追加する 49
ワークステーションをワークグループに追加する 50
プロジェクトをワークグループに追加する 51
プロジェクトの管理 52
プロジェクトとルートディレクトリについて 52
ルートディレクトリの追加 52
プロジェクトのルートディレクトリを削除 53
プロジェクトの追加 53
サブフォルダの追加 53
ワークステーション 54
ワークステーションの追加 54
ワークステーションを削除する 55
レポートおよびセキュリティ機能 55
データレポートの生成 55
CAC ソフトウェアのエクスポート 55
CAC ソフトウェア設定のインポート 56
CAC ソフトウェア設定の復元 56
CAC ユーザー管理設定のエクスポート 56
CAC ユーザー管理設定のインポート 57

6 ネットワーク取得 58
ネットワーク取得について 58
ネットワーク取得を使用することで得られる利点 58
安全ネットワークアカウント 58
データ転送プロセス 59
ネットワーク取得を構成 59
安全ネットワークアカウントの指定 59

7 監査 61
監査証跡 61
監査マップ 62
監査マップの設定 63
インストール済みの監査マップテンプレート 63
監査マップの作業を行う 64
プロジェクト監査マップ 64
ワークステーション監査マップ 66

CAC 監査マップ 68
監査証跡の表示、検索、エクスポート、印刷 70
監査証跡の記録の表示 70
監査レコードの検索またはフィルター 70
アーカイブ済み監査証跡の表示 71
監査証跡の印刷 71
監査証跡レコードのエクスポート 71
SCIEX OS 監査証跡レコード 71
CAC 監査証跡レコード 72
監査証跡アーカイブ 73

A ネットワーク中断中のデータへのアクセス 74
データをローカルに表示および処理する 74
ネットワーク転送フォルダからサンプルを削除 74

B Windows 権限 76

C 監査イベント 79

D SCIEX OS と Analyst ソフトウェア間の権限のマッピング 87

E データファイルのチェックサム 93
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 93

お問い合わせ先 94
住所 94
お客様のトレーニング 94
オンライン学習センター 94
SCIEX サポート 94
サイバーセキュリティ 94
説明書 94

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 SCIEX OS 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、SCIEX OS 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連携してどのように機能するかについて説明します。また、SCIEX OS 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

SCIEX OS ソフトウェア提供物:

- リサーチと監督法規の双方の要件を満たすため管理機能をカスタマイズする。
- セキュリティおよび監査ツールで電子記録の使用に対する 21 CFR Part 11 の遵守をサポートする。
- 重要な質量分析装置機能へのアクセスを柔軟かつ効果的に管理する。
- 重大なデータとレポートへのアクセスを管理および監査する。
- Windows セキュリティにリンクする容易なセキュリティ管理。

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、法医学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。

SCIEX OS ソフトウェアおよび Windows セキュリティ: 互いに連動

SCIEX OS 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。

SCIEX OS ソフトウェアには次の安全なシステム アクセス モードがあります。

- 混合モード
- 統合モード(デフォルト設定)

Security Mode 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: セキュリティモードの設定。

SCIEX OS は、Windows に関連するユーザーグループとは別個にフル構成できる役割も提供します。役割を使用することにより、ラボ管理者は、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: SCIEX OS ソフトウェアへのアクセスの構成。

SCIEX OS ソフトウェアと Windows の監査証跡

SCIEX OS 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。

SCIEX OS 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表または分解能テーブルの変更、システム構成の変更、およびセキュリティイベント。
- プロジェクト、チューニング、バッチ、データ、処理メソッド、レポートテンプレートファイルの作成や変更イベント、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には、役割の削除と SCIEX OS ソフトウェアのユーザーの削除が含まれます。
- サンプル情報、ピーク積分パラメータ、および定量テーブルに埋め込まれた処理メソッドの作成と変更。

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：監査イベント。

SCIEX OS 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。このログをトラブルシューティングの補助として使用してください。質量分析装置、デバイス、およびソフトウェアの相互作用に関する詳細情報が含まれています。

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。

カスタマーセキュリティガイダンス: バックアップ

顧客データのバックアップは、顧客の責任です。SCIEX のサービスおよびサポート担当者は、顧客データのバックアップに関するアドバイスや推奨事項を提供する場合がありますが、お客様のポリシー、ニーズ、規制要件に従ってデータを確実にバックアップするかどうかは、お客様次第です。顧客データのバックアップの頻度と範囲は、組織の要件および生成されるデータの重要度に応じて決定する必要があります。

バックアップはデータ管理全体の重要なコンポーネントであり、悪意のある攻撃、ハードウェア障害、またはソフトウェア障害が発生した場合の復元に不可欠であるため、お客様はバックアップが機能することを確認する必要があります。データ取得中は、コンピュータのバックアップを取得しないでください。また、取得中のファイルがバックアップソフトウェアによって無視されるようにしてください。セキュリティアップデートのインストールやコンピュータの修理を行う前に、コンピュータの完全なバックアップを作成することを強くお勧めします。これにより、セキュリティ パッチがアプリケーションの機能に影響を与えるというまれなケースでも、ロールバックが容易になります。

21 CFR Part 11

SCIEX OS ソフトウェアには、21 CFR Part 11 の実装をサポートするための技術的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。
- 装置の稼働、データ取得、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。

SCIEX OS 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。SCIEX OS 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、オプションの SCIEX OS CFR ライセンスの使用と SCIEX OS ソフトウェアの構成によって異なります。必要なポリシーと手順、および関連するトレーニング要件もラボに導入する必要があります。

検証サービスは、SCIEX プロフェッショナル サービスを通じて利用できます。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。

注: 検証済みのシステムに Instrument Settings Converter ソフトウェアを置いたままにしないでください。これは、装置の設定を Analyst から SCIEX OS ソフトウェア に初めて転送するためのものです。使用後は Instrument Settings Converter ソフトウェアをコンピュータから必ず削除してください。

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

このセクションでは、Windows の構成に関するガイドラインについて説明します。

- Windows アカウントとパスワードについては、次のガイドラインに従ってください。
  - Windows パスワードは 90 日ごとに変更する必要があります。
  - Windows パスワードは、次の反復で少なくとも 1 回は再利用できません。つまり、以前のパスワードと同じにすることはできません。
  - Windows のパスワードは 8 文字以上である必要があります。
  - 複雑さの要件を満たすには、Windows パスワードに次の 4 つの要件のうち少なくとも 2 つが含まれている必要があります。
    - 1 つの大文字英字
    - 1 つの小文字英字
    - 1 つの数値
    - 1 つの特殊文字(! @ # $ % ^ &)
  - Windows ユーザー名は、**管理者**、**管理者**、または**デモ**であってはなりません。

- SCIEX OS ソフトウェアの管理者が SCIEX OS Data フォルダのファイル権限を変更できることを確認してください。このフォルダがローカルコンピュータ上にある場合は、ソフトウェア管理者をローカル管理者グループに含めることをお勧めします。
- すべてのユーザーがネットワーク取得に必要なリソースへのアクセス権を持っていることを確認するには、ネットワーク管理者にネットワーク リソースにセキュア ネットワーク アカウント (SNA) を追加するように依頼します。このアカウントには、ルートディレクトリを含むネットワークフォルダへの書き込み権限が必要です。ルートディレクトリのプロパティで SNA として定義されています。

注: ライブラリ ファイルはローカル ドライブからインポートすることをお勧めします。

注: さまざまなユーザーの役割に必要な Windows 権限については、次のセクションを参照: Windows 権限。

ユーザーとグループ

SCIEX OS 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: SCIEX OS ソフトウェアへのアクセスの構成。

Active Directory への対応

SCIEX OS の構成ワークスペースにユーザーを追加する場合は、ユーザー プリンシパル名 (UPN) 形式でユーザー アカウントを指定します。Active Directory の以下のバージョンがサポートされています。

- Windows 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

SCIEX OS ソフトウェアでは、ファイルとディレクトリは NTFS 形式を使用するハードディスク パーティションに保存する必要があります。これにより、SCIEX OS 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。ファイル割り当てテーブル (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。

ファイルおよびフォルダアクセス許可

セキュリティを管理するには、SCIEX OS ソフトウェアの管理者が SCIEX OS Data 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。このアクセスはネットワーク管理者が設定しなければなりません。

注: 各コンピュータのドライブ、ルートディレクトリ、プロジェクトフォルダへのユーザーのアクセス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。

注: 権限に関する問題を回避するために、ライブラリ ファイルをローカル ドライブからインポートすることをお勧めします。

注: さまざまなユーザーの役割に必要な Windows 権限については、次のセクションを参照してください：Windows 権限。

SCIEX OS ソフトウェアのファイルとフォルダのアクセス許可については、次のセクションを参照してください：アクセス制御。

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。

イベントログ

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。

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 サービスします。
- 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

SCIEX OS ソフトウェアの場合、電子ライセンスはノードロックまたはサーバーベースにすることができます。

Central Administrator Console (CAC)ソフトウェアでは、ノードロック ライセンスのみが利用可能です。

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:

- 構成ワークスペースで、SCIEX OS ウィンドウの**ライセンス**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。CAC ソフトウェアのライセンスは年間ライセンスです。

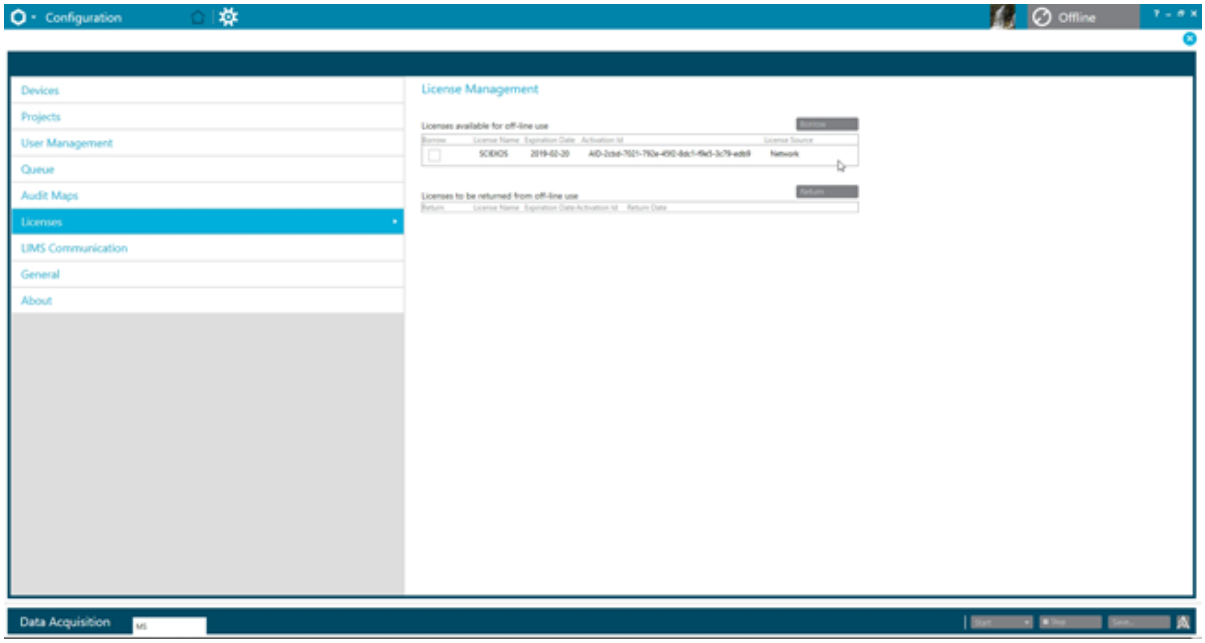
サーバーベースの電子ライセンスの借用

SCIEX OS を使用するにはライセンスが必要です。サーバーベースのライセンスが使用されている場合、オフラインで作業したいユーザーは最大 7 日間ライセンスを予約できます。この期間中は、借用された電子ライセンスはそのコンピュータ専用になります。

注: この手順は、Central Administrator Console (CAC)ソフトウェアには適用されません。

1. 構成ワークスペースを開きます。
2. **ライセンス**をクリックします。
   オフラインで使用できるライセンスの表には、借用できるすべてのライセンスが表示されます。

図 3-1 : License Management: ライセンスの借用



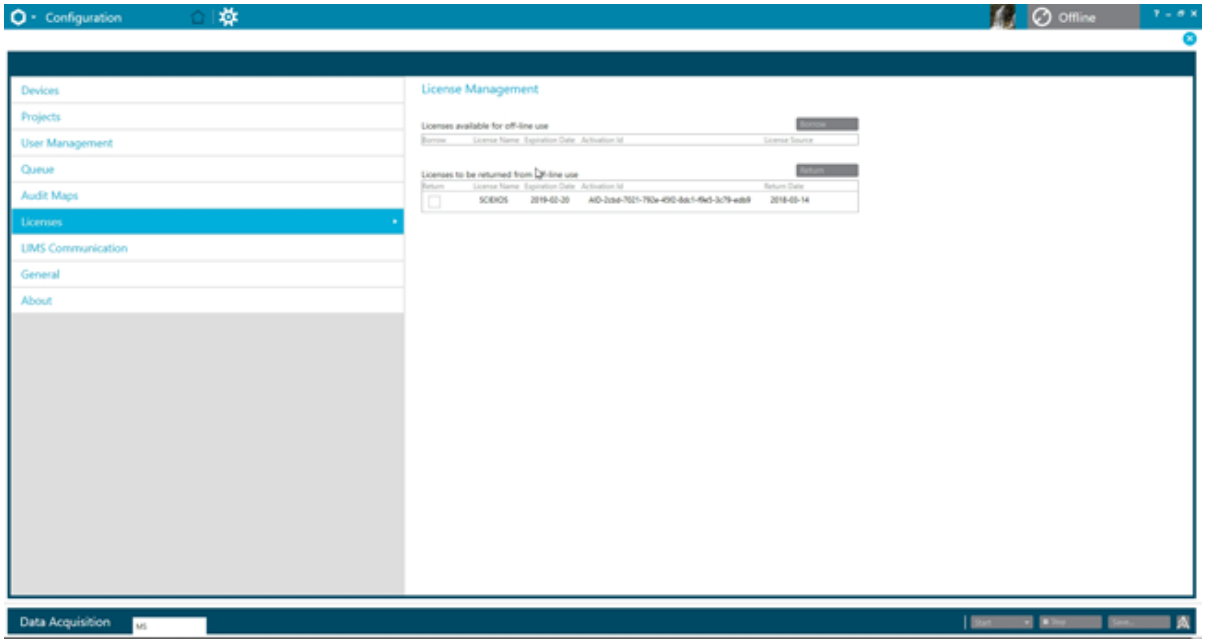
3. 借用するライセンスを選択し、**借用**をクリックします。

サーバーベースの電子ライセンスの返却

注: この手順は、Central Administrator Console (CAC)ソフトウェアには適用されません。

1. 構成ワークスペースを開きます。
2. **ライセンス**をクリックします。
   オフライン使用から返却されるライセンス表には、返却の対象となるすべてのライセンス、つまり、このコンピュータが借用しているすべてのライセンスが表示されます。

図 3-2 : ライセンス管理: ライセンスの返却



3. 返却するライセンスを選択し、**返却**をクリックします。

アクセス制御 4

このセクションでは、SCIEX OS ソフトウェアへのアクセスを制御する方法について説明します。ソフトウェアへのアクセスを制御するには、管理者は以下のタスクを実施します:

注: このセクションに記載のタスクを実施するユーザーには、ソフトウェアがインストールされているワークステーションへのローカル管理者権限が必要です。

- SCIEX OS ソフトウェアをインストールして構成します。
- ユーザーおよび役割を追加し、構成します。
- プロジェクトと、ルートディレクトリのプロジェクトファイルへのアクセスを構成します。

この手順では、SCIEX OS ソフトウェアのローカル管理について説明します。SCIEX OS ソフトウェアの集中管理については、次のセクションを参照:中央管理者コンソール

注: SCIEX OS の構成に加えた変更は、いずれも SCIEX OS の再起動後に有効になります。

セキュリティ情報の場所

すべてのセキュリティ情報は、ローカルコンピュータの `C:\ProgramData\SCIEX\Clearcore2.Acquisition` フォルダ内にある `Security.data` という名前のファイルに保存されます。

ソフトウェアセキュリティのワークフロー

SCIEX OS 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。
- SCIEX OS ソフトウェア認証:SCIEX OS を開く機能。
- SCIEX OS ソフトウェア認証:SCIEX OS の機能へのアクセス。

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、次の表を参照: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、次の表を参照: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
SCIEX OS ソフトウェアをインストールします。	*SCIEX OS ソフトウェアインストールガイド*を参照してください。

表 4-1：セキュリティの構成におけるワークフロー (続き)

タスク	処置
SCIEX OS ソフトウェアへのアクセスの構成。	SCIEX OS ソフトウェアへのアクセスの構成を参照してください。
Windows ファイルセキュリティと NTFS を構成します。	プロジェクトとプロジェクトファイルへのアクセスの設定を参照してください。

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	
ユーザーとグループを構成します（認証）。	はい
Windows の監査、およびファイルとディレクトリの監査を有効化します。	はい
ファイルアクセス権限を設定します（認証）。	はい
SCIEX OS ソフトウェアインストール	
SCIEX OS ソフトウェアをインストールします。	はい
イベントビューアを開いて、インストールを確認します。	はい
ソフトウェアのセキュリティ	
Security Mode を選択します。	はい
SCIEX OS ソフトウェアでユーザーとロールを構成します。	はい
メール通知の構成。	はい
監査マップテンプレートを作成し、プロジェクトおよびワークステーション監査証跡マップを構成します。	はい
`wiff` ファイルのチェックサム機能を有効にします。	はい
共通タスク	
新しいプロジェクトを追加します。	はい

SCIEX OS ソフトウェアをインストール

SCIEX OS ソフトウェア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 パッケージで入手可能な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。

システム要件

最小インストール要件については、次のドキュメントを参照: *ソフトウェアインストールガイド*。

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テンプレート。インストール後、SCIEX OS ソフトウェアの管理者はカスタム監査マップを作成し、構成ワークスペースで別の監査マップを割り当てることができます。

セキュリティモードの設定

このセクションでは、構成ワークスペースのユーザー管理ページにあるセキュリティモードオプションについて説明します。

Integrated Mode：現在 Windows にログオンしているユーザーがソフトウェアでユーザーとして定義されている場合、そのユーザーは SCIEX OS

Mixed Mode：ユーザーは Windows とソフトウェアに別々にログオンします。Windows へのログオンに使用される認証情報は、SCIEX OS へのログオンに使用される認証情報と同じである必要はありません。このモードを使用すると、ユーザー グループが同じ認証情報セットを使用して Windows にログオンできるようになりますが、各ユーザーは一意の認証情報でソフトウェアにログオンする必要があります。これらの一意の認証情報は、Integrated Mode 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。

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

Screen Lock and Auto Logoff：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。また、自動ログオフタイマーを設定し、一定時間ロックされた後にソフトウェアを終了させることも可能です。Screen Lock and Auto Logoff は、Mixed Mode でのみ使用できます。

注: 画面がロックされると、取得と処理が続行されます。処理中または定量テーブルが保存されていない場合、自動ログオフは行われません。ユーザーが強制ログオフを使用してログオフすると、すべての処理が停止し、保存されていないデータはすべて失われます。ユーザーがログオフした後、自動または手動で取得が続行されます。

セキュリティ通知：ソフトウェアは、設定可能な期間内に設定可能な数のログオンに失敗した後に自動的に電子メール通知を送信し、不正なユーザーによるシステムへのアクセスを警告するように設定できます。ログオン失敗数は 3～7 で、期間は 5 分～24 時間です。

注: Central Administrator Console (CAC)ソフトウェアで管理しているワークグループの場合、セキュリティモードは SCIEX OS ソフトウェアで管理できません。

Security Mode を選択する

1. 構成ワークスペースを開きます。
2. **ユーザー管理**をクリックします。
3. **セキュリティモード**タブをクリックします。
4. **統合モード**または**混合モード**を選択します。次のセクションを参照: セキュリティモードの設定。
5. **保存**をクリックします。
   確認ダイアログが表示されます。

6. **OK** をクリックします。

ワークステーションのセキュリティオプションの設定（Mixed mode）

実施前提手順
• Security Mode を Mixed Mode に設定します。次のセクションを参照: セキュリティモードの設定。

Mixed mode が選択されている場合、Screen Lock and Auto Logoff 機能を構成できます。

1. 構成ワークスペースを開きます。
2. **ユーザー管理**をクリックします。
3. セキュリティモードタブを開きます。
4. 画面ロック機能を構成するには、次の手順に従います。
   a. **画面ロック**を選択します。
   b. **待機**フィールドで、時間を分単位で指定します。
      ワークステーションがこの時間アクティブでない場合、自動的にロックされます。ログオンしたユーザーは、正しい認証情報を入力してワークステーションのロックを解除するか、管理者がユーザーをログオフできます。
5. 自動ログオフ機能を構成するには、次の手順に従います。
   a. **自動ログオフ**を選択します。
   b. **待機**フィールドで、時間を分単位で指定します。ワークステーションが自動または手動でこの時間ロックされている場合、現在ログオンしているユーザーはログオフされます。すべての処理が停止します。ただし、測定は継続されます。
6. **保存**をクリックします。
   確認ダイアログボックスが開きます。
7. **OK** をクリックします。

メール通知の構成（Mixed Mode）

実施前提手順
• Security Mode を Mixed Mode に設定します。次のセクションを参照: セキュリティモードの設定。

ソフトウェアは、構成可能な期間内に構成可能な数のログオンエラーが発生した後にメールメッセージを送信するように構成できます。ログオン失敗数は 3～7 で、期間は 5 分～24 時間です

ソフトウェアがインストールされているコンピュータは、ポートが開いている SMTP サーバーと通信できる必要があります。

1. 構成ワークスペースを開きます。

2. **ユーザー管理**をクリックします。
3. セキュリティモードタブを開きます。
4. **後にメールメッセージを送信**チェックボックスを選択してから、どの期間内に何回ログオンに失敗したかを分単位で指定し、メール通知を生成します。

   ヒント! 通知を無効にするには、**後にメールメッセージを送信**チェックボックスをオフにします。

5. **SMTP サーバー**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 サーバーは、社内メールアプリケーションで定義されています。

6. **ポート番号**をクリックして、開いているポート番号を入力します。
   デフォルトを適用をクリックして、デフォルトのポート番号 25 を挿入します。
7. **宛先**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.
8. **送信元**フィールドに、メッセージの**送信元**フィールドに表示される電子メールアドレスを入力します。
9. **件名**フィールドに、メッセージの件名を入力します。
10. **メッセージ**フィールドに、メッセージの本文に含めるテキストを入力します。
11. **保存**をクリックします。
    確認ダイアログが開きます。
12. **OK** をクリックします。
13. 構成の内容を確認するには、**テストメールの送信**をクリックします。

SCIEX OS ソフトウェアへのアクセスの構成

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 SCIEX OS 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。

SCIEX OS 許可

図 4-1 : User Management ページ

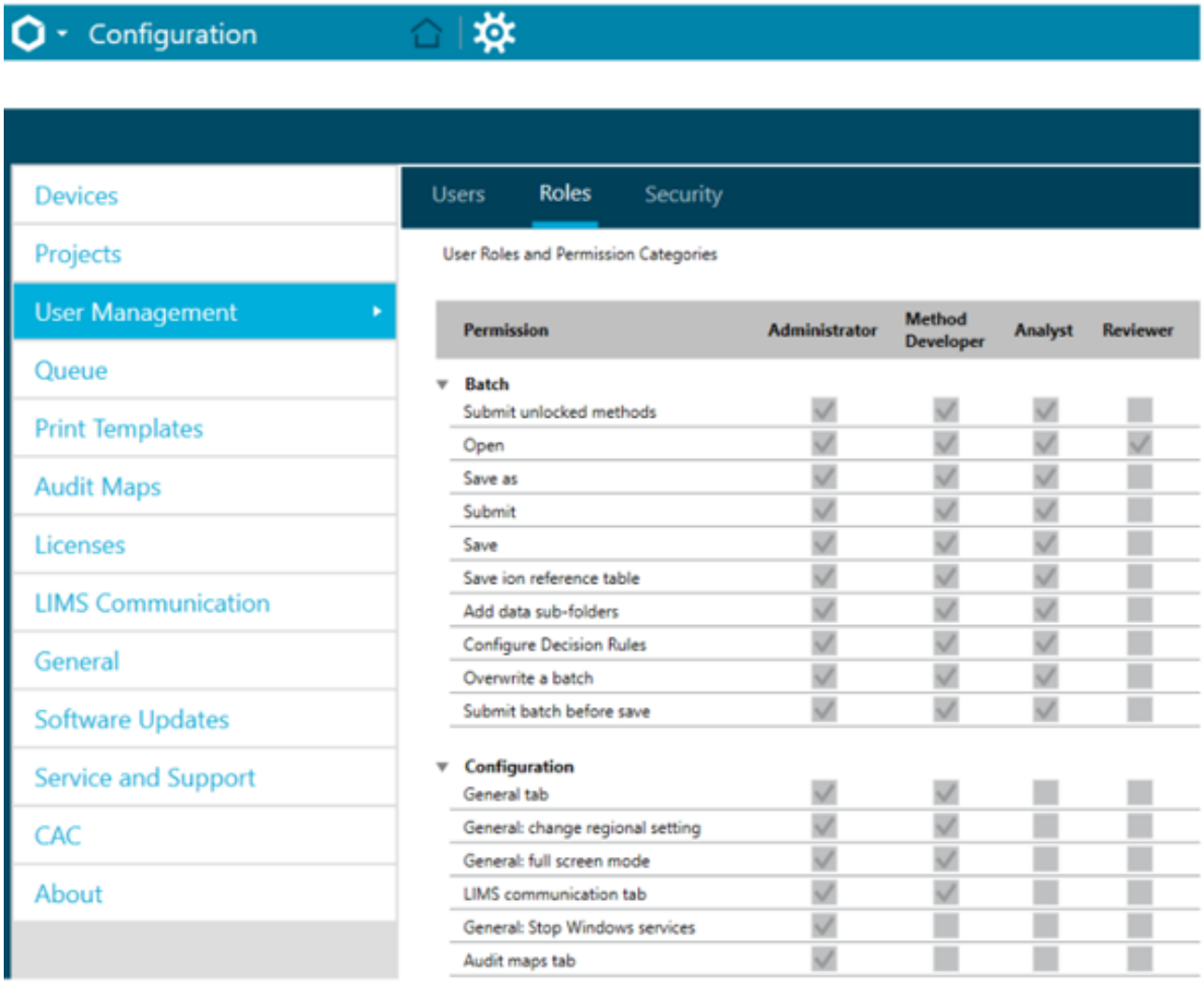


表 4-3 : 許可

権限	説明
バッチ	
ロック解除されたメソッドを送信	ロック解除されたメソッドを含むバッチを送信します。

表 4-3：許可 (続き)

権限	説明
開く	保存したバッチを開きます。
別名で保存	新しい名前でバッチを保存します。
送信	バッチを送信します。
保存	バッチを保存し、保存した内容を上書きします。
イオン参照表の保存	イオン参照表を編集します。
データのサブフォルダを追加	データ保存用のサブフォルダーを作成します。
決定ルールを設定	決定ルールを追加して変更します。
バッチを上書き	同じ名前でバッチを保存し、保存した内容を上書きします。
保存前にバッチを送信	保存されていないバッチを送信します。
構成	
全般タブ	構成 ワークスペースで 全般 ページを開きます。
全般：地域設定の変更	アクティブなシステムの地域設定を SCIEX OS ソフトウェアに適用します。
全般：全画面モード	全画面モードの有効と無効を切り替えます。
一般：Windows サービスの停止	**Windows の設定** オプションを有効または無効にします。
LIMS 通信タブ	構成 ワークスペースで LIMS 通信 ページを開きます。
監査マップタブ	構成 ワークスペースで 監査マップ ページを開きます。
キュータブ	構成 ワークスペースで キュー ページを開きます。
キュー：装置のアイドル時間	装置のアイドル時間を設定します。
キュー：取得サンプルの最大数	取得可能なサンプルの最大数を設定します。
キュー：他のキュー設定	他のキュー設定を構成します。
プロジェクトタブ	構成 ワークスペースで プロジェクト ページを開きます。
プロジェクト：プロジェクトの作成	プロジェクトを作成します。
プロジェクト：監査マップテンプレートを既存のプロジェクトに適用	監査マップをプロジェクトに適用します。
プロジェクト：ルートディレクトリの作成	プロジェクトストレージ用のルートディレクトリを作成します。
プロジェクト：現在のルートディレクトリの設定	プロジェクトのルートディレクトリを変更します。

表 4-3：許可 (続き)

権限	説明
プロジェクト：ネットワーク認証情報の指定	ログオンしているユーザーがネットワークリソースにアクセスできない場合に、ネットワークの取得時に使用するセキュアなネットワークアカウント（SNA）を指定します。
プロジェクト：wiff データ作成のチェックサム書き込みの有効化	`wiff` データ ファイルにチェックサムを書き込むようにソフトウェアを設定します。
プロジェクト：ルートディレクトリをクリアする	ルートディレクトリをリストから削除します。
デバイスタブ	構成 ワークスペースで デバイス ページを開きます。
ユーザー管理タブ	構成 ワークスペースで ユーザー管理 ページを開きます。
ユーザーの強制ログオフ	SCIEX OS ソフトウェアにログオンしているユーザーを強制的にログオフさせます。
CAC タブ [1]	構成 ワークスペースで CAC ページを開きます。
印刷テンプレートタブ	構成 ワークスペースで 印刷テンプレート タブを開きます。
印刷テンプレート：印刷テンプレートの作成と変更	新しい印刷テンプレートを作成するか、保存した印刷テンプレートを変更します。
印刷テンプレート：デフォルトの印刷テンプレートを設定	アクティブな印刷テンプレートをアクティブなプロジェクトのデフォルトにします。
印刷テンプレート：現在のテンプレートをルートディレクトリ内のすべてのプロジェクトに適用	選択したルート ディレクトリ内の選択したプロジェクトで使用可能な印刷テンプレートのリストに印刷テンプレートを追加します。
イベントログ	
イベントログワークスペースへのアクセス	イベントログワークスペースを開きます。
アーカイブログ	ログを イベントログ ワークスペースにアーカイブします。
監査証跡	
監査証跡ワークスペースにアクセス	監査証跡 ワークスペースを開きます。
アクティブな監査マップを表示	監査証跡ワークスペース内のワークステーションまたはプロジェクトのアクティブな監査マップを確認します。
監査証跡の印刷/エクスポート	監査証跡を印刷またはエクスポートします。
データ取得パネル	
開始	データ取得 ペインで取得を開始します。

[1] バージョン 3.1 では、**中央管理の有効化** 権限の名前が **CAC** に変更されました。構成 ワークスペースの CAC ページを使用して、SCIEX OS ソフトウェアの中央管理を構成できます。

表 4-3：許可 (続き)

権限	説明
停止	データ取得 ペインで取得を停止します。
保存	取得したデータを別のファイル名で データ取得 ペインに保存します。
MS と LC メソッド	
アクセスメソッドワークスペース	MS メソッド および LC メソッド ワークスペースを開きます。
新規	MS および LC メソッドを作成します。
開く	MS および LC メソッドを開きます。
保存	メソッドを保存し、保存した内容を上書きします。
別名で保存	新しい名前でメソッドを保存します。
メソッドのロック/ロック解除	編集を防ぐためにメソッドをロックし、ロック解除します。
測定メソッドの上書き	同じ名前で測定メソッドを保存し、保存した内容を上書きします。
キュー	
管理	キューワークスペースを開きます。
開始/停止	キューを開始または停止します。
印刷	キューを印刷します。
サンプルの編集	サンプルの名前またはデータファイルを変更します。
ライブラリ	
ライブラリワークスペースへのアクセス	ライブラリ ワークスペースを開きます。定量ワークフローには適用されません。
MS チューン	
MS チューンワークスペースへのアクセス	MS チューン ワークスペースを開きます。
高度な MS チューニング	X500 QTOF および ZenoTOF 7600/7600+ システム：**検出器の最適化**、**Positive TOF チューニング**、**Negative TOF チューニング**、**Positive Q1 Unit チューニング**、**Negative Q1 Unit チューニング**、**Positive Q1 High チューニング**、**Negative Q1 High チューニング** などの高度なチューニングオプションにアクセスできます。該当しません。
高度なトラブルシューティング	高度なトラブルシューティング ダイアログボックスを開きます。該当しません。
クイックステータスチェック	X500 QTOF および ZenoTOF 7600/7600+ システム：**正クイックステータスチェック** と **負クイックステータスチェック** を実行します。

表 4-3：許可 (続き)

権限	説明
装置データの復元	以前に保存したチューニング設定を復元します。
アナリティクス	
新しい結果	定量テーブルを作成します。
処理メソッドを作成	処理メソッドを作成します。
処理メソッドの変更	処理メソッドを変更します。
ロック解除された定量テーブルのエクスポートとレポートの作成を許可	定量テーブルがロックされていない場合は、定量テーブルまたは統計表からレポートをエクスポートまたは作成します。
自動化バッチの結果を保存	自動的に作成された定量テーブルを バッチ ワークスペースに保存します。この権限は、取得中の自動処理に必要です。
デフォルトの定量化メソッド積分アルゴリズムを変更	プロジェクトのデフォルト設定の積分アルゴリズムを変更します。
デフォルトの定量化メソッド積分パラメータを変更	プロジェクトのデフォルト設定の積分パラメータを変更します。
プロジェクトのピーク修正警告の有効化	プロジェクトの修正済みピーク警告プロパティを有効にします。
サンプルを追加	定量テーブルにサンプルを追加します。
選択したサンプルを削除	定量テーブルからサンプルを削除します。
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	外部キャリブレーションをエクスポート、インポート、または削除します。
サンプル名の変更	定量テーブルのサンプル名を変更します。
サンプルタイプの変更	定量テーブルのサンプルタイプを変更します。有効なサンプル タイプには、標準、品質管理 (QC)、および不明が含まれます。
サンプル ID の変更	定量テーブルでサンプル ID を修正します。
実際の濃度の修正	定量テーブルの標準および QC サンプルの実際の濃度を変更します。
希釈係数の修正	定量テーブルで希釈係数を変更します。

表 4-3：許可 (続き)

権限	説明
コメントフィールドの修正	以下のコメント欄を変更します。 • **成分コメント** • **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**
手動積分を有効化	手動積分を行います。
ピークを不検出に設定	**不検出** にピークを設定します。
定量テーブルにピークを含めるまたはそこから除外	定量テーブルにピークを含めたり、ピークを除外したりします。
回帰オプション	キャリブレーションカーブ ペインの回帰オプションを変更します。
単一のクロマトグラムの定量テーブル積分パラメータを変更	ピークレビューペインで単一クロマトグラムの積分パラメータを変更します。
定量テーブルの成分の定量化メソッドを変更	**成分処理メソッドの更新** オプションを使用して、ピークレビューペインで成分の別の処理方法を選択します。
メトリックプロットの新しい設定の作成	新しいメトリックプロットを作成し、設定を変更します。
カスタム列を追加	定量テーブルにカスタム列を追加します。
ピークレビュータイトルのフォーマットの設定	ピークレビュータイトルを変更します。
カスタム列を削除	定量テーブルからカスタム列を削除します。
定量テーブルの表示設定	定量テーブルに表示される列をカスタマイズします。
定量テーブルのロック	定量テーブルを編集できないようにロックします。
定量テーブルのロック解除	定量テーブルのロックを解除して、変更できるようにします。
結果ファイルをレビュー済みとしてマークして保存	定量テーブルをレビュー済みとしてマークし、保存します。
レポートテンプレートを変更	レポートテンプレートを変更します。
結果を LIMS に転送	結果を実験室情報管理システム（LIMS）にアップロードします。
バーコード列を変更	定量テーブルの **バーコード** 列を変更します。
比較サンプルの割り当てを変更	定量テーブルの **比較** 列で指定された比較サンプルを変更します。
MSMS スペクトルをライブラリに追加	選択した MS/MS スペクトルをライブラリに追加します。定量ワークフローには適用されません。

表 4-3：許可 (続き)

権限	説明
プロジェクトのデフォルト設定	プロジェクトのデフォルトの定量および定性処理設定を変更します。
すべての形式でレポートを作成	すべての形式でレポートを作成します。この権限のないユーザーは、PDF 形式でのみレポートを作成できます。
フラグ設定基準パラメータの編集	処理メソッドのフラグ設定パラメータを変更します。
自動外れ値除外パラメータの変更	自動外れ値除外のパラメータを変更します。
自動外れ値除外の有効化	自動外れ値除外機能をオンにするよう、処理メソッドを変更します。
FF/LS による処理メソッドの更新	Formula Finder とライブラリ検索を使用して処理メソッドを更新します。定量ワークフローには適用されません。
FF/LS による結果を更新	Formula Finder とライブラリ検索を使用して結果を更新します。定量ワークフローには適用されません。
付加物機能によるグループ化の有効化	付加物によるグループ化機能を使用するように処理方法を更新します。
ファイルを参照	ローカルデータフォルダー外部で参照します。
標準追加の有効化	標準の追加機能をオンにするよう、処理メソッドを更新します。
手動積分パーセントルールの設定	**手動積分 %** パラメータを変更します。
重量/容量の変更	**重量/容量** フィールドを変更します。
定量テーブルを上書き	同じ名前で定量テーブルを保存し、保存した内容を上書きします。
結果ファイルを承認済みとしてマークして保存	結果ファイルを承認済みとしてマークし、**Results** > **結果ファイルを承認済みとしてマークして保存** コマンドで保存します。
中央モニタリング	
キュータブへのアクセス	**中央モニタリング** ワークスペースを開きます。
キューの印刷	キューを印刷します。
開始/停止キュー	キューを開始または停止します。
エクスプローラ	
エクスプローラワークスペースへのアクセス	エクスプローラワークスペースを開きます。
エクスポート	エクスプローラ ワークスペースからデータをエクスポートします。
印刷	エクスプローラ ワークスペースでデータを印刷します。

表 4-3：許可 (続き)

権限	説明
オプション	エクスプローラ ワークスペースのオプションを変更します。
再キャリブレーション	エクスプローラ ワークスペースでサンプルとスペクトルを再度キャリブレートします。定量ワークフローには適用されません。
ファイルを参照	アクティブなプロジェクトの外側を参照します。

ユーザーと役割について

SCIEX OS ソフトウェアでは、管理者は Windows ユーザーとグループを User Management データベースに追加できます。ソフトウェアにアクセスするには、ユーザーはユーザー管理データベースに存在するか、データベース内のグループのメンバーである必要があります。

ユーザーは、次の表に示す 1 つ以上のプリセットロール、または必要に応じてカスタムロールに割り当てることができます。ユーザーがアクセスできる機能は役割によって指定されます。プリセットの役割は削除できず、その権限は変更できません。

注: Central Administrator Console (CAC) ソフトウェアで管理するワークグループの場合、ユーザー管理 ページは読み取り専用になります。

表 4-4：プリセットの役割

役割	標準的なタスク
管理者	• システムを管理する • セキュリティを構成する
メソッドディベロッパー	• メソッドを作成する • バッチを実行する • ユーザーが使用できるようにデータを分析する
Analyst	• バッチを実行する • ユーザーが使用できるようにデータを分析する
レビューア	• 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

表 4-5：プリセットされている許可

権限	管理者	メソッドディベロッパー	Analyst	レビューア
バッチ				

表 4-5 : プリセットされている許可 (続き)

権限	管理者	メソッドディベロッパー	Analyst	レビューア
ロック解除されたメソッドを送信	✓	✓	✓	×
開く	✓	✓	✓	✓
別名で保存	✓	✓	✓	×
送信	✓	✓	✓	×
保存	✓	✓	✓	×
イオン参照表の保存	✓	✓	✓	×
データのサブフォルダを追加	✓	✓	✓	×
決定ルールを設定	✓	✓	✓	×
バッチを上書き	✓	✓	✓	×
保存前にバッチを送信	✓	✓	✓	✓
構成				
全般タブ	✓	✓	×	×
全般:地域設定の変更	✓	✓	×	×
全般:全画面モード	✓	✓	×	×
一般:Windows サービスの停止	✓	×	×	×
LIMS 通信タブ	✓	✓	×	×
監査マップタブ	✓	×	×	×
キュータブ	✓	✓	✓	✓
キュー:装置のアイドル時間	✓	✓	×	×
キュー:取得サンプルの最大数	✓	✓	×	×
キュー:他のキュー設定	✓	✓	×	×
プロジェクトタブ	✓	✓	✓	✓
プロジェクト:プロジェクトの作成	✓	✓	✓	×

表 4-5 : プリセットされている許可 (続き)

権限	管理者	メソッドディベロッパー	Analyst	レビューア
プロジェクト:監査マップテンプレートを既存のプロジェクトに適用	✓	×	×	×
プロジェクト:ルートディレクトリの作成	✓	×	×	×
プロジェクト:現在のルートディレクトリの設定	✓	×	×	×
プロジェクト:ネットワーク認証情報の指定	✓	×	×	×
プロジェクト:wiff データ作成のチェックサム書き込みの有効化	✓	×	×	×
プロジェクト:ルートディレクトリをクリアする	✓	×	×	×
デバイスタブ	✓	✓	✓	×
ユーザー管理タブ	✓	×	×	×
ユーザーの強制ログオフ	✓	×	×	×
CAC タブ [1]	✓	×	×	×
印刷テンプレートタブ	✓	✓	×	×
印刷テンプレート:印刷テンプレートの作成と変更	✓	✓	×	×
印刷テンプレート:デフォルトの印刷テンプレートを設定	✓	✓	×	×
印刷テンプレート:現在のテンプレートをルートディレクトリ内のすべてのプロジェクトに適用	✓	×	×	×
イベントログ				
イベントログワークスペースへのアクセス	✓	✓	✓	✓

[1] バージョン 3.1 では、**中央管理の有効化** 権限の名前が **CAC** に変更されました。構成 ワークスペースの CAC ページを使用して、SCIEX OS ソフトウェアの中央管理を構成できます。

表 4-5 : プリセットされている許可 (続き)

権限	管理者	メソッドディベロッパー	Analyst	レビューア
アーカイブログ	✓	✓	✓	✓
監査証跡				
監査証跡ワークスペースにアクセス	✓	✓	✓	✓
アクティブな監査マップを表示	✓	✓	✓	✓
監査証跡の印刷/エクスポート	✓	✓	✓	✓
データ取得パネル				
開始	✓	✓	✓	×
停止	✓	✓	✓	×
保存	✓	✓	✓	×
MS と LC メソッド				
アクセスメソッドワークスペース	✓	✓	✓	✓
新規	✓	✓	×	×
開く	✓	✓	✓	✓
保存	✓	✓	×	×
別名で保存	✓	✓	×	×
メソッドのロック/ロック解除	✓	✓	×	×
測定メソッドの上書き	✓	✓	×	×
キュー				
管理	✓	✓	✓	×
開始/停止	✓	✓	✓	×
印刷	✓	✓	✓	✓
サンプルの編集	✓	✓	×	×
ライブラリ				
ライブラリワークスペースへのアクセス	✓	✓	✓	✓

表 4-5 : プリセットされている許可 (続き)

権限	管理者	メソッドディベロッパー	Analyst	レビューア
MS チューン				
MS チューンワークスペースへのアクセス	✓	✓	✓	×
高度な MS チューニング	✓	✓	×	×
高度なトラブルシューティング	✓	✓	×	×
クイックステータスチェック	✓	✓	✓	×
装置データの復元	✓	✓	×	×
アナリティクス				
新しい結果	✓	✓	✓	×
処理メソッドを作成	✓	✓	✓	×
処理メソッドの変更	✓	✓	×	×
ロック解除された定量テーブルのエクスポートとレポートの作成を許可	✓	×	×	×
自動化バッチの結果を保存	✓	✓	✓	×
デフォルトの定量化メソッド積分アルゴリズムを変更	✓	✓	×	×
デフォルトの定量化メソッド積分パラメータを変更	✓	✓	×	×
プロジェクトのピーク修正警告の有効化	✓	×	×	×
サンプルを追加	✓	✓	✓	×
選択したサンプルを削除	✓	✓	✓	×
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	✓	✓	✓	×
サンプル名の変更	✓	✓	✓	×
サンプルタイプの変更	✓	✓	✓	×

表 4-5 : プリセットされている許可 (続き)

権限	管理者	メソッドディベロッパー	Analyst	レビューア
サンプル ID の変更	✓	✓	✓	×
実際の濃度の修正	✓	✓	✓	×
希釈係数の修正	✓	✓	✓	×
コメントフィールドの修正	✓	✓	✓	×
手動積分を有効化	✓	✓	✓	×
ピークを不検出に設定	✓	✓	✓	×
定量テーブルにピークを含めるまたはそこから除外	✓	✓	✓	×
回帰オプション	✓	✓	✓	×
単一のクロマトグラムの定量テーブル積分パラメータを変更	✓	✓	✓	×
定量テーブルの成分の定量化メソッドを変更	✓	✓	✓	×
メトリックプロットの新しい設定の作成	✓	✓	✓	✓
カスタム列を追加	✓	✓	✓	×
ピークレビュータイトルのフォーマットの設定	✓	×	×	×
カスタム列を削除	✓	✓	×	×
定量テーブルの表示設定	✓	✓	✓	✓
定量テーブルのロック	✓	✓	✓	✓
定量テーブルのロック解除	✓	×	×	×
結果ファイルをレビュー済みとしてマークして保存	✓	×	×	✓
レポートテンプレートを変更	✓	✓	×	×
結果を LIMS に転送	✓	✓	✓	×
バーコード列を変更	✓	✓	×	×

表 4-5 : プリセットされている許可 (続き)

権限	管理者	メソッドディベロッパー	Analyst	レビューア
比較サンプルの割り当てを変更	✓	✓	×	×
MSMS スペクトルをライブラリに追加	✓	✓	×	×
プロジェクトのデフォルト設定	✓	✓	×	×
すべての形式でレポートを作成	✓	✓	✓	✓
フラグ設定基準パラメータの編集	✓	✓	✓	×
自動外れ値除外パラメータの変更	✓	✓	×	×
自動外れ値除外の有効化	✓	✓	✓	×
FF/LS による処理メソッドの更新	✓	✓	×	×
FF/LS による結果を更新	✓	✓	×	×
付加物機能によるグループ化の有効化	✓	✓	×	×
ファイルを参照	✓	✓	✓	✓
標準追加の有効化	✓	✓	✓	×
手動積分パーセントルールの設定	✓	×	×	×
重量/容量の変更	✓	✓	✓	×
定量テーブルを上書き	✓	✓	✓	×
結果ファイルを承認済みとしてマークして保存	✓	×	×	✓
エクスプローラ				
エクスプローラワークスペースへのアクセス	✓	✓	✓	✓
エクスポート	✓	✓	✓	×
印刷	✓	✓	✓	×

表 4-5 : プリセットされている許可 (続き)

権限	管理者	メソッドディベロッパー	Analyst	レビューア
オプション	✓	✓	✓	×
再キャリブレーション	✓	✓	×	×
ファイルを参照	✓	✓	✓	✓

ユーザーの管理

ユーザーまたはグループを追加

1. 構成ワークスペースを開きます。
2. ユーザー管理ページを開きます。
3. ユーザー タブを開きます。
4. **ユーザーの追加**( )をクリックします。
   ユーザーまたはグループの選択ダイアログが開きます。
5. ユーザーまたはグループの名前を入力し、**OK** をクリックします。

   ヒント! ユーザーまたはグループの選択ダイアログとその使用方法については、**F1** を押してください。
6. ユーザーをアクティブにするには、**有効なユーザーまたはグループ**チェックボックスをオンにします。
7. **役割**エリアで 1 つ以上のロールを選択し、**保存**をクリックします。

ユーザーまたはグループの無効化

1. 構成ワークスペースを開きます。
2. ユーザー管理ページを開きます。
3. ユーザー タブを開きます。
4. **ユーザー名またはグループ**リストの中から、無効化するユーザーまたはグループを選択します。
5. **有効なユーザーまたはグループ**チェックボックスをオフにします。
   ソフトウェアは確認を求めるプロンプトを表示します
6. **はい**をクリックします。

ユーザーまたはグループの削除

この手順を使用して、ユーザーまたはグループをソフトウェアから削除します。ユーザーまたはグループが Windows から削除された場合、ユーザーは SCIEX OS ソフトウェアからも削除される必要があります。

1. 構成ワークスペースを開きます。
2. ユーザー管理ページを開きます。
3. ユーザー タブを開きます。
4. **ユーザー名またはグループ**リストの中から、削除するユーザーまたはグループを選択します。
5. **削除**をクリックします。
   ソフトウェアは確認を求めるプロンプトを表示します
6. **OK** をクリックします。

役割の管理

ユーザーまたはグループに割り当てられた役割の変更

この手順を使用してユーザーまたはグループに新規ロールを割り当てたり、既存の役割の割り当てを削除したりします。

1. 構成ワークスペースを開きます。
2. ユーザー管理ページを開きます。
3. ユーザー タブを開きます。
4. **ユーザー名またはグループ**フィールドで、変更するユーザーまたはグループを選択します。
5. ユーザーまたはグループに割り当てる役割を選択し、削除する役割があればそれを消去します。
6. **保存**をクリックします。

カスタム役割の作成

1. 構成ワークスペースを開きます。
2. ユーザー管理ページを開きます。
3. 役割 タブを開きます。
4. **役割を追加**( )をクリックします。
   ユーザー役割の複製ダイアログが開きます。
5. **既存のユーザー役割**フィールドで、新しい役割のテンプレートとして使用する役割を選択します。
6. 役割の名前と説明を入力し、**OK** をクリックします。
7. 役割のアクセス権を選択します。
8. **すべての役割を保存**をクリックします。
9. **OK** をクリックします。

カスタム役割の削除

注: ユーザーに割り当てられている役割が、削除される役割だけである場合は、役割に加えてユーザーも削除するよう指示されます。

1. 構成ワークスペースを開きます。
2. ユーザー管理ページを開きます。
3. 役割 タブを開きます。
4. **役割を削除**をクリックします。
   ユーザー役割の削除ダイアログが開きます。
5. 削除する役割を選択し、**OK** をクリックします。

ユーザー管理設定のエクスポートとインポート

SCIEX OS ソフトウェアのユーザー管理データベースをエクスポートおよびインポートできます。たとえば、ある SCIEX コンピュータでユーザー管理データベースを設定した後、それをエクスポートし、他の SCIEX コンピュータでインポートすることで、ユーザー管理設定が一貫していることを確認します。

ドメインユーザーのみがエクスポートされます。ローカルユーザーはエクスポートされません。

ユーザー管理設定をインポートする前に、ソフトウェアは現在の設定を自動的にバックアップします。ユーザーは最後のバックアップを復元できます。

ユーザー管理設定のエクスポート

1. 構成ワークスペースを開きます。
2. ユーザー管理ページを開きます。
3. **詳細** > **ユーザー管理設定のエクスポート**をクリックします。
   ユーザー管理設定のエクスポートダイアログが開きます。
4. **参照**をクリックします。
5. 設定が保存されるフォルダを参照して選択し、**フォルダを選択**をクリックします。
6. **エクスポート**をクリックします。
   確認のメッセージが表示され、エクスポートした設定を含むファイルの名前が表示されます
7. **OK** をクリックします。

ユーザー管理設定のインポート

1. 構成ワークスペースを開きます。
2. ユーザー管理ページを開きます。
3. **詳細** > **ユーザー管理設定のインポート**をクリックします。
   ユーザー管理設定のインポートダイアログが開きます。
4. **参照**をクリックします。

5. インポートする設定を含むファイルを参照して選択し、**開く**をクリックします。
   ソフトウェアは、ファイルが有効であることを確認します。
6. **インポート**をクリックします。
   ソフトウェアは、現在のユーザー管理設定をバックアップし、新しい設定をインポートします。確認メッセージが表示されます。
7. **OK** をクリックします。

ユーザー管理設定の復元

ユーザー管理設定をインポートする前に、ソフトウェアは現在の設定をバックアップします。この手順を使用して、ユーザー管理設定の最後のバックアップを復元します。

1. 構成ワークスペースを開きます。
2. ユーザー管理ページを開きます。
3. **詳細** > **以前の設定を復元**をクリックします。
   ユーザー管理設定の復元ダイアログが開きます。
4. **はい**をクリックします。
5. SCIEX OS ソフトウェアを閉じて、もう一度開きます。

プロジェクトとプロジェクトファイルへのアクセスの設定

Windows のセキュリティ機能を使用して、`SCIEX OS Data` フォルダへのアクセスを制御します。デフォルトでは、プロジェクトファイルは `SCIEX OS Data` フォルダに保存されます。プロジェクトにアクセスするには、プロジェクトデータが格納されているルートディレクトリへのアクセス権が必要です。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。

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、次の表を参照: 表 4-6。

表 4-6 : プロジェクトフォルダ

フォルダ	コンテンツ
`\Acquisition Methods`	プロジェクトで作成された質量分析装置（MS）および LC メソッドが含まれます。MS メソッドには msm 拡張子があり、LC メソッドには lcm 拡張子があります。
`\Audit Data`	プロジェクト監査マップと、すべての監査記録が格納されています。
`\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 bch 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。測定データファイルには、wiff と wiff2 の拡張子があります。
`\Project Information`	プロジェクトのデフォルト設定ファイルが格納されています。

表 4-6 : プロジェクトフォルダ (続き)

フォルダ	コンテンツ
\Quantitation Methods	すべての処理メソッドのファイルが含まれています。処理メソッドには qmethod の拡張子が付いています。
\Quantitation Results	すべての定量 Results Table が含まれています。Results Table ファイルには qsession の拡張子が付いています。

ソフトウェアのファイルタイプ

SCIEX OS ソフトウェアの一般的なファイルタイプについては、次の表を参照 : 表 4-7。

表 4-7 : SCIEX OS ファイル

拡張子	ファイルタイプ	フォルダ
atds	• ワークステーション監査証跡データとアーカイブ • ワークステーション監査証跡の設定 • プロジェクト監査証跡データとアーカイブ • プロジェクト監査証跡設定	• プロジェクト : *<project name>*\Audit Data • ワークステーション : C:\ProgramData\SCIEX\Audit Data
atms	監査マップ	• プロジェクト : *<project name>*\Audit Data • ワークステーション : C:\ProgramData\SCIEX\Audit Data
bch	バッチ	Batch
cset	定量テーブルの設定	Project Information
dad	質量分析装置データファイル	• Optimization • Data
exml	プロジェクトのデフォルト設定	Project Information
journal	SCIEX OS ソフトウェアによって作成される一時ファイル	各種フォルダ
lcm	LC メソッド	Acquisition Methods
msm	MS メソッド	Acquisition Methods
pdf	ポータブルドキュメントデータ	—

表 4-7 : SCIEX OS ファイル (続き)

拡張子	ファイルタイプ	フォルダ
qlayout	ワークスペースのレイアウト	— **注:** プロジェクトのデフォルトのワークスペースレイアウトは、Project Information フォルダに保存されます。
qmethod	処理メソッド	Quantitation Methods
qsession	定量テーブルを保持。 **注:** SCIEX OS ソフトウェアは、SCIEX OS ソフトウェアで作成された qsession ファイルのみを開くことができます。	Quantitation Results
wiff	SCIEX OS ソフトウェアと互換性のある質量分析データ ファイル **注:** SCIEX OS ソフトウェアは、wiff と wiff2 ファイルの両方を作成します。	Data
wiff.scan	質量分析装置データファイル	• Optimization • Data
wiff2	SCIEX OS ソフトウェアによって生成された質量分析データファイル	• Optimization • Data
xls または xlsx	Excel スプレッドシート	Batch
xps	再校正	Data\Cal

中央管理者コンソール 5

Central Administrator Console (CAC)ソフトウェアは、SCIEX OS ソフトウェアによるローカル管理のオプションの代替手段です。CAC ソフトウェアには、中央の役割、ユーザー、ワークステーション、およびワークグループの管理とカスタマイズがすべて 1 つのアプリケーションに含まれています。

このセクションでは、CAC ソフトウェアについて説明し、職員、プロジェクト、ワークステーションを中央管理するために構成して使用する方法について説明します。

注: CAC ソフトウェアを使用してワークステーションをサーバーに登録するには、SCIEX OS ソフトウェアが各ワークステーションにインストールされていることを確認してください。

CAC ソフトウェアはライセンスに対応しており、SCIEX OS バージョン 3.0 および Windows Server 2019 をサポートするワークステーションにインストールできます。

CAC ソフトウェアは、SCIEX OS インストーラパッケージの一部です。ただし、CAC ソフトウェアと SCIEX OS を同じワークステーションにインストールすることはできません。

ユーザー

ユーザー管理ページを使用して、Windows ユーザーおよびグループを SCIEX OS ソフトウェアのユーザー管理データベースに追加します。管理者は、[ユーザーの役割と権限] セクションでユーザーの役割を追加、変更、および削除することもできます。ソフトウェアにアクセスするには、ユーザー管理データベースでユーザーが定義されているか、データベースで定義されたグループのメンバーである必要があります。

ユーザープール

SCIEX OS ソフトウェアが Central Administrator Console (CAC)ソフトウェアで管理されている場合、許可されたユーザーのみがワークステーションにログオンし、SCIEX OS ソフトウェアにアクセスできます。ユーザーをワークグループに追加する前に、ユーザー プールに追加する必要があります。

ユーザーまたはグループをユーザープールに追加する

1. 中央管理ワークスペースを開きます。
2. ユーザー管理ページを開きます。
3. ユーザープールタブを開きます。
4. **ユーザーをユーザープールに追加**( )をクリックします。
   ユーザーまたはグループの選択ダイアログが開きます。
5. ユーザーまたはグループの名前を入力し、**OK** をクリックします。

ヒント! 複数のユーザーまたはグループを選択するには、**Ctrl** キーを押したまま **OK** をクリックします。

ユーザーまたはグループを削除する

1. 中央管理ワークスペースを開きます。
2. ユーザー管理ページを開きます。
3. ユーザープールタブを開きます。
4. 右側のペインで、削除するユーザーまたはグループを選択し、**削除**をクリックします。
   ソフトウェアは確認を求めるプロンプトを表示します
5. **OK** をクリックします。

ユーザーの役割と権限

このセクションでは、ユーザーの役割と権限ページについて説明します。

ユーザーは、次の表で説明する 1 つ以上の既定の役割や、必要に応じてカスタム役割に対して割り当てることができます。ユーザーがアクセスできる機能は役割によって指定されます。既定の役割は削除できず、その権限は変更できません。

注: Central Administrator Console (CAC)ソフトウェアでは、権限がサポートされている SCIEX OS ソフトウェアの最も古いバージョンを確認することもできます。

表 5-1：既定の役割

役割	標準的なタスク
管理者	• システムを管理する • セキュリティを構成する
メソッドディベロッパー	• メソッドを作成する • バッチを実行する • ユーザーが使用できるようにデータを分析する
Analyst	• バッチを実行する • ユーザーが使用できるようにデータを分析する
レビューア	• 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。

表 5-2 : プリセットされている許可

権限	管理者	メソッドディベロッパー	Analyst	レビューア
バッチ				
ロック解除されたメソッドを送信	✓	✓	✓	×
開く	✓	✓	✓	✓
別名で保存	✓	✓	✓	×
送信	✓	✓	✓	×
保存	✓	✓	✓	×
イオン参照表の保存	✓	✓	✓	×
データのサブフォルダを追加	✓	✓	✓	×
決定ルールを設定	✓	✓	✓	×
構成				
全般タブ	✓	✓	×	×
全般 : 地域設定の変更	✓	✓	×	×
全般 : 全画面モード	✓	✓	×	×
LIMS 通信タブ	✓	✓	×	×
一般 : Windows サービスの停止	✓	×	×	×
監査マップタブ	✓	×	×	×
キュータブ	✓	✓	✓	✓
キュー : 装置のアイドル時間	✓	✓	×	×
キュー : 取得サンプルの最大数	✓	✓	×	×
キュー : 他のキュー設定	✓	✓	×	×
プロジェクトタブ	✓	✓	✓	✓
プロジェクト : プロジェクトの作成	✓	✓	✓	×
プロジェクト : 監査マップテンプレートを既存のプロジェクトに適用	✓	×	×	×

表 5-2 : プリセットされている許可 (続き)

権限	管理者	メソッドディベロッパー	Analyst	レビューア
プロジェクト:ルートディレクトリの作成	✓	×	×	×
プロジェクト:現在のルートディレクトリの設定	✓	×	×	×
プロジェクト:ネットワーク認証情報の指定	✓	×	×	×
プロジェクト:wiff データ作成のチェックサム書き込みの有効化	✓	×	×	×
プロジェクト:ルートディレクトリをクリアする	✓	×	×	×
デバイスタブ	✓	✓	✓	×
ユーザー管理タブ	✓	×	×	×
ユーザーの強制ログオフ	✓	×	×	×
CAC タブ [1]	✓	×	×	×
印刷テンプレートタブ	✓	✓	×	×
印刷テンプレート:印刷テンプレートの作成と変更	✓	✓	×	×
印刷テンプレート:デフォルトの印刷テンプレートを設定	✓	✓	×	×
印刷テンプレート:現在のテンプレートをルートディレクトリ内のすべてのプロジェクトに適用	✓	×	×	×
イベントログ				
イベントログワークスペースへのアクセス	✓	✓	✓	✓
アーカイブログ	✓	✓	✓	✓
監査証跡				
監査証跡ワークスペースにアクセス	✓	✓	✓	✓

[1] バージョン 3.1 では、**中央管理の有効化** 権限の名前が **CAC** に変更されました。構成 ワークスペースの CAC ページを使用して、SCIEX OS ソフトウェアの中央管理を構成できます。

表 5-2 : プリセットされている許可 (続き)

権限	管理者	メソッドディベロッパー	Analyst	レビューア
アクティブな監査マップを表示	✓	✓	✓	✓
監査証跡の印刷/エクスポート	✓	✓	✓	✓
データ取得パネル				
開始	✓	✓	✓	×
停止	✓	✓	✓	×
保存	✓	✓	✓	×
MS と LC メソッド				
アクセスメソッドワークスペース	✓	✓	✓	✓
新規	✓	✓	×	×
開く	✓	✓	✓	✓
保存	✓	✓	×	×
別名で保存	✓	✓	×	×
メソッドのロック/ロック解除	✓	✓	×	×
キュー				
管理	✓	✓	✓	×
開始/停止	✓	✓	✓	×
印刷	✓	✓	✓	✓
サンプルの編集	✓	✓	×	×
ライブラリ				
ライブラリワークスペースへのアクセス	✓	✓	✓	✓
MS チューン				
MS チューンワークスペースへのアクセス	✓	✓	✓	×
高度な MS チューニング	✓	✓	×	×
高度なトラブルシューティング	✓	✓	×	×

表 5-2 : プリセットされている許可 (続き)

権限	管理者	メソッドディベロッパー	Analyst	レビューア
クイックステータスチェック	✓	✓	✓	×
装置データの復元	✓	✓	×	×
アナリティクス				
新しい結果	✓	✓	✓	×
処理メソッドを作成	✓	✓	✓	×
処理メソッドの変更	✓	✓	×	×
ロック解除された定量テーブルのエクスポートとレポートの作成を許可	✓	×	×	×
自動化バッチの結果を保存	✓	✓	✓	×
デフォルトの定量化メソッド積分アルゴリズムを変更	✓	✓	×	×
デフォルトの定量化メソッド積分パラメータを変更	✓	✓	×	×
プロジェクトのピーク修正警告の有効化	✓	×	×	×
サンプルを追加	✓	✓	✓	×
選択したサンプルを削除	✓	✓	✓	×
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	✓	✓	✓	×
サンプル名の変更	✓	✓	✓	×
サンプルタイプの変更	✓	✓	✓	×
サンプル ID の変更	✓	✓	✓	×
実際の濃度の修正	✓	✓	✓	×
希釈係数の修正	✓	✓	✓	×
コメントフィールドの修正	✓	✓	✓	×
手動積分を有効化	✓	✓	✓	×
ピークを不検出に設定	✓	✓	✓	×

表 5-2 : プリセットされている許可 (続き)

権限	管理者	メソッドディベロッパー	Analyst	レビューア
定量テーブルにピークを含めるまたはそこから除外	✓	✓	✓	×
回帰オプション	✓	✓	✓	×
単一のクロマトグラムの定量テーブル積分パラメータを変更	✓	✓	✓	×
定量テーブルの成分の定量化メソッドを変更	✓	✓	✓	×
メトリックプロットの新しい設定の作成	✓	✓	✓	✓
カスタム列を追加	✓	✓	✓	×
ピークレビュータイトルのフォーマットの設定	✓	×	×	×
カスタム列を削除	✓	✓	×	×
定量テーブルの表示設定	✓	✓	✓	✓
定量テーブルのロック	✓	✓	✓	✓
定量テーブルのロック解除	✓	×	×	×
結果ファイルをレビュー済みとしてマークして保存	✓	×	×	✓
レポートテンプレートを変更	✓	✓	×	×
結果を LIMS に転送	✓	✓	✓	×
バーコード列を変更	✓	✓	×	×
比較サンプルの割り当てを変更	✓	✓	×	×
MSMS スペクトルをライブラリに追加	✓	✓	×	×
プロジェクトのデフォルト設定	✓	✓	×	×

表 5-2 : プリセットされている許可 (続き)

権限	管理者	メソッドディベロッパー	Analyst	レビューア
すべての形式でレポートを作成	✓	✓	✓	✓
フラグ設定基準パラメータの編集	✓	✓	✓	×
自動外れ値除外パラメータの変更	✓	✓	×	×
自動外れ値除外の有効化	✓	✓	✓	×
FF/LS による処理メソッドの更新	✓	✓	×	×
FF/LS による結果を更新	✓	✓	×	×
付加物機能によるグループ化の有効化	✓	✓	×	×
ファイルを参照	✓	✓	✓	✓
標準追加の有効化	✓	✓	✓	×
手動積分パーセントルールの設定	✓	×	×	×
重量/容量の変更	✓	✓	✓	×
エクスプローラ				
エクスプローラワークスペースへのアクセス	✓	✓	✓	✓
エクスポート	✓	✓	✓	×
印刷	✓	✓	✓	×
オプション	✓	✓	✓	×
再キャリブレーション	✓	✓	×	×

カスタム役割の追加

Central Administrator Console (CAC)ソフトウェアには 4 種類の既定の役割が用意されています。追加の役割が必要な場合は、既存の役割をコピーしてアクセス権を割り当てます。

1. 中央管理ワークスペースを開きます。
2. ユーザー管理ページを開きます。
3. ユーザーの役割と権限タブを開きます。

4. **役割を追加**( )をクリックします。
   ユーザー役割の複製ダイアログが開きます。
5. **既存のユーザー役割**フィールドで、新しい役割のテンプレートとして使用する役割を選択します。
6. 役割の名前と説明を入力し、**OK** をクリックします。
   新しいロールが ユーザーの役割と権限のカテゴリウィンドウに表示されます。
7. 該当するチェックボックスをオンにして、役割のアクセス権限を選択します。
8. **すべての役割を保存**をクリックします。

カスタム役割の削除

1. 中央管理ワークスペースを開きます。
2. ユーザー管理ページを開きます。
3. ユーザーの役割と権限タブを開きます。
4. **役割を削除**をクリックします。
   ユーザー役割の削除ダイアログが開きます。
5. 削除する役割を選択し、**OK** をクリックします。

ワークグループ

ワークグループ管理ページを使用して、ワークグループを管理します。ワークグループには、ユーザー、ワークステーション、およびプロジェクトがあります。

該当するプールからリソースを追加することで、ワークグループを作成します。ワークグループを作成する前に、すべての潜在的なユーザーをユーザープールに、ワークステーションをワークステーションプールに、プロジェクトルートディレクトリをプロジェクトプールに追加してください。

必要に応じて、役割を追加します。ワークグループごとに Security Mode を選択することも可能です。

ワークステーションが Central Administrator Console (CAC)ソフトウェアに登録されており、かつワークグループのメンバーである場合、ワークグループの Security Mode 設定はワークステーションのセキュリティモード設定よりも優先されます。

ローカルユーザーはワークグループに追加しないでください。CAC ソフトウェアはネットワークアプリケーションであるため、ワークグループにはネットワークユーザーしか追加できません。

注: 各ワークグループで、少なくとも 1 人のユーザーに次を割り当てる必要があります。管理者の役割。現在ログオンしているユーザーが利用できない場合は、管理者またはスーパーバイザだけが CAC ソフトウェア画面のロックを解除できます。

特定のワークステーションにサーバーベースのセキュリティが必要なくなった場合は、SCIEX OS ソフトウェアを使用してワークステーションのセキュリティをローカルに管理します。

ワークグループを作成する

1. 中央管理ワークスペースを開きます。
2. ワークグループ管理ページを開きます。
3. **ワークグループを追加**()をクリックします。
   ワークグループを追加ダイアログが開きます。
4. **ワークグループ名** フィールドに名前を入力します。
5. **説明**フィールドに説明を入力して、**追加**をクリックします。
   ワークグループが作成され、ワークグループと割り当てを管理ペインに追加されます。Central Administrator Console (CAC)ソフトウェアは、サーバー上に適切なワークグループ名を作成します。

   注: 統合モードはデフォルトのセキュリティ設定です。

ワークグループを削除する

ワークグループが不要となった場合は、これをワークグループリストから削除します。ワークグループを削除すると、そのワークグループだけが Central Administrator Console (CAC)ソフトウェアから削除されます。ワークステーションからデータが失われることはありません。

1. 中央管理ワークスペースを開きます。
2. ワークグループ管理ページを開きます。
3. **ワークグループ**リストを展開し、削除するワークグループを見つけます。**削除**をクリックします。
   ワークグループを削除ダイアログが開きます。
4. **はい**をクリックします。

ユーザーまたはグループをワークグループに追加する

注: ワークグループに追加されたユーザーには、ロールが自動的に割り当てられません。ユーザーに役割を割り当てるには、次のセクションを参照: 役割を追加または削除する。

1. 中央管理ワークスペースを開きます。
2. ワークグループ管理ページを開きます。
3. ワークグループと割り当てを管理ウィンドウで、変更するワークグループを展開し、**ユーザー**リストを展開します。
4. ユーザーまたはグループを選択してから、**追加**()をクリックします。

   ヒント! Shift を押してから必要なユーザーを選択することにより、複数のユーザーを追加または選択します。

   ユーザーまたはグループが現在のワークグループに追加されます。

5. 追加したユーザーまたはグループに 1 つ以上の役割を割り当てます。次のセクションを参照: 役割を追加または削除する。
6. **保存**をクリックします。

役割を追加または削除する

実施前提手順
• ユーザーまたはグループをワークグループに追加する。

Central Administrator Console (CAC)ソフトウェアで役割を作成する詳細な情報については、次のセクションを参照: カスタム役割の追加。役割が割り当てられたユーザーまたはグループには、役割に関連付けられたすべての権限があります。ユーザーまたはグループは、一度に複数のロールを持つことができます。

1. 中央管理ワークスペースを開きます。
2. ワークグループ管理ページを開きます。
3. ワークグループと割り当てを管理ウィンドウで、変更するワークグループを展開し、**ユーザー**リストを展開します。
4. 現在のワークグループのメンバーシップセクションで、**役割の割り当て**列のロールを割り当てるか削除します。
5. **保存**をクリックします。

ワークステーションをワークグループに追加する

注: ワークステーションは、Central Administrator Console (CAC)ソフトウェアに登録されている場合にのみワークステーションプールに表示されます。次のセクションを参照: ワークステーションの追加

1. 中央管理ワークスペースを開きます。
2. ワークグループ管理ページを開きます。
3. ワークグループと割り当てを管理ペインで、変更するワークグループを展開し、**ワークステーション**リストを展開します。
4. ワークステーションを選択してから、**追加**(>)をクリックします。
   ワークステーションが現在のワークグループに追加されます。
5. **保存**をクリックします。

ワークグループセキュリティ設定の割り当て

実施前提手順
• ワークステーションの追加 • ワークステーションをワークグループに追加する

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: セキュリティモードの設定。

1. 中央管理ワークスペースを開きます。
2. ワークグループ管理ページを開きます。
3. ワークグループと割り当てを管理ペインで、変更するワークグループを展開し、**ワークステーション**リストを展開します。
4. (オプション)現在のワークグループをそのワークステーションの既定のワークグループにするには、**デフォルトの設定**セクションで現在のワークグループのメンバーシップチェック ボックスをオンにします。
5. セキュリティ設定の割り当てセクションで、ワークグループの**セキュリティモード**を選択し、適切な**画面ロック** と**自動ログオフ**の時間を入力します。
6. **保存**をクリックします。

プロジェクトをワークグループに追加する

注: この手順は、プロジェクトアクセスが中央管理されている場合にのみ必要です。

注: 1 つのプロジェクトが複数のワークグループに追加された場合、プロジェクトへのユーザーアクセスが付け加えられ、上書きはされません。たとえば、ワークグループ 1 にユーザー A とユーザー B、そしてプロジェクト_01 が存在するとします。ワークグループ 2 にはユーザー B とユーザー C が存在するとします。Project_01 がワークグループ 2 に追加された場合、ユーザー A、ユーザー B、ユーザー C の全員がプロジェクト_01 にアクセスできます。

1. 中央管理ワークスペースを開きます。
2. ワークグループ管理ページを開きます。
3. ワークグループと割り当てを管理ペインで、変更するワークグループを展開し、**プロジェクト**リストを展開します。
4. **プロジェクトの中央管理設定を使用** チェックボックスを選択します。
   プロジェクト選択セクションが表示されます。
5. **プロジェクトのルートディレクトリ**を選択してプロジェクトのグループ全体を追加するか、プロジェクトルートを展開してワークグループに追加する特定のプロジェクトを選択します。
6. **追加**(>)をクリックして、プロジェクトをワークグループに追加します。
   プロジェクトルートが現在のワークグループのメンバーシップテーブルに追加されます。プロジェクトルートを展開して、ワークグループ内の現在のプロジェクトを表示します。
7. **保存**をクリックします。

プロジェクトの管理

Project Management ページを使用して、プロジェクトを作成、変更、および削除します。

プロジェクトにアクセスするには、プロジェクトデータが格納されているルートディレクトリへのアクセス権が必要です。詳細な情報については、次のセクションを参照: プロジェクトとルートディレクトリについて。

プロジェクトとルートディレクトリについて

ルートディレクトリは 1 つ以上のプロジェクトを含むフォルダです。これは、ソフトウェアがプロジェクトデータを検索するフォルダです。事前定義されたルートディレクトリは `D:\SCIEX OS Data` です。

プロジェクト情報が安全に保存されていることを確認するには、Central Administrator Console (CAC)ソフトウェアを使用してプロジェクトを作成します。プロジェクトをワークグループに追加する前に、プロジェクトのルートディレクトリに追加します。次のセクションを参照: プロジェクトの追加。

プロジェクトデータはサブフォルダに整理できます。CAC ソフトウェアでサブフォルダを作成します。次のセクションを参照: サブフォルダの追加。

注: プロジェクトが CAC ソフトウェアの外部で作成された場合は、プロジェクトの作成後にプロジェクトルートを更新する必要があります。ルートが更新されると、プロジェクトのルートディレクトリの内容はネットワーク上のプロジェクトルートの内容と同期されます。

ルートディレクトリの追加

ルートディレクトリは 1 つ以上のプロジェクトが保管されているフォルダです。

注: 最大 10 個のルートディレクトリを保存できます。

ヒント! ネットワークからはローカルドライブにアクセスできません。ルートディレクトリは、共有ドライブ上にのみ作成できます。

1. 中央管理ワークスペースを開きます。
2. Project Management ページを開きます。
3. **新規または既存のプロジェクトルートをプロジェクトプールに追加**( )をクリックします。
   ルートディレクトリ追加ダイアログが開きます。
4. ルートディレクトリ フォルダへのフル パスを入力し、**OK** をクリックします。
   フォルダが作成されます。

   ヒント! パスを入力する代わりに、**参照**クリックして、ルートディレクトリを作成するフォルダを選択します。

   ヒント! あるいは、File Explorer にフォルダを作成して、そのフォルダを参照し選択します。

注: 処理ライセンスを持つ SCIEX OS ソフトウェアをインストールする場合、ルートディレクトリは Analyst ソフトウェア(`Analyst Data\Projects`)フォルダ。

5. **OK** をクリックします。
   新しいルートディレクトリは、現在のプロジェクトのルートディレクトリになります。

プロジェクトのルートディレクトリを削除

ソフトウェアは、最後に使用された 10 個のルートディレクトリのリストを保持します。ユーザーは、このリストからルート ディレクトリを削除できます。

注: プロジェクトルートディレクトリを削除すると、プロジェクトルートプールからすべての関連プロジェクトも削除されます。

1. 中央管理ワークスペースを開きます。
2. Project Management ページを開きます。
3. 削除するプロジェクトルートディレクトリを見つけて、操作セクションで**プロジェクトルートを削除**をクリックします。
   ソフトウェアは確認を求めるプロンプトを表示します
4. **OK** をクリックします。

プロジェクトの追加

実施前提手順
• ルートディレクトリの追加

プロジェクトには、取得メソッド、データ、バッチ、処理メソッド、処理結果などが保存されます。各プロジェクトに対して別々のプロジェクトフォルダを使用することを推奨します。

Central Administrator Console (CAC)ソフトウェアの外部にプロジェクトを作成したり、ファイルをコピーまたは貼り付けしたりしないでください。

1. 中央管理ワークスペースを開きます。
2. Project Management ページを開きます。
3. ルート フォルダの操作セクションで**プロジェクトの追加**をクリックします。
   新規プロジェクトダイアログが開きます。
4. プロジェクト名を入力します。
5. **OK** をクリックします。
   新しいプロジェクトがプロジェクトルートの下に表示されます。

サブフォルダの追加

プロジェクト内のデータは、サブフォルダでさらに整理できます。

1. 中央管理ワークスペースを開きます。

2. Project Management ページを開きます。
3. ルート フォルダの操作セクションで**データのサブフォルダを追加**をクリックします。
   データのサブフォルダを追加ダイアログが開きます。
4. サブフォルダが属するプロジェクトを選択します。
5. **新しいデータサブフォルダを追加**( )をクリックします。
   データサブフォルダ名ダイアログが開きます。
6. サブフォルダの名前を入力します。
7. **保存**をクリックします。

   ヒント! サブフォルダは、他のサブフォルダ内にネストできます。ネストされたサブフォルダを作成するには、プロジェクトデータサブフォルダセクションで既存のサブフォルダを選択し、**新しいデータサブフォルダを追加**( )をクリックします。
8. データのサブフォルダを追加ダイアログを閉じます。

ワークステーション

ワークステーション管理ページを使用して、CAC ソフトウェアに接続されているすべてのワークステーションを管理します。CAC ソフトウェアの制御下にあるワークステーションには、カスタマイズされた設定が自動的に適用されます。

ワークステーションの追加

ワークステーション管理ページで、管理者はワークステーションの追加、ワークステーションの集中管理の有効化と無効化、およびワークステーションの削除を行うことができます。

1. 中央管理ワークスペースを開きます。
2. ワークステーション管理ページを開きます。
3. **ワークステーションをワークステーションプールに追加**( )をクリックします。
   コンピュータを選択ダイアログが開きます。
4. 追加するワークステーションの名前を入力し、**OK** をクリックします。
   ワークステーションの中央管理**ステータス**が**接続中**から**無効**に変わります。
5. (オプション) ワークステーションの集中管理を有効にするには:
   a. **ステータス**列で、**無効**をクリックします。
   b. **OK** をクリックします。

   ヒント! SCIEX OS ソフトウェアで中央管理を有効にすることもできます。次のドキュメントを参照:*SCIEX OS ソフトウェアヘルプシステム*。

ワークステーションを削除する

ワークステーションが使用されなくなった場合、またはワークグループの一部である必要がなくなった場合は、そのワークステーションをワークステーション プールから削除します。ワークステーションが削除されると、そのワークステーションは割り当てられていたワークグループのいずれからも削除されます。削除時にワークステーションのデータが失われることはありません。

1. 中央管理ワークスペースを開きます。
2. ワークステーション管理ページを開きます。
3. **ワークステーション管理**をクリックします。
4. ワークステーションプールペインで、削除したいワークステーションを検索してから**削除**をクリックします。
   ワークステーションを削除ダイアログが開きます。
5. **OK** をクリックします。

レポートおよびセキュリティ機能

データレポートの生成

この手順を使用して、構成されたユーザー、役割、ワークステーション、プロジェクト、およびワークグループなどの詳細を含むデータ レポートを生成します。

1. 中央管理ワークスペースを開きます。
2. **印刷**をクリックします。
   印刷オプション ダイアログが開きます。
3. 印刷するページを選択、**続行しますか**をクリックします。
4. 印刷オプションを設定し、**印刷**をクリックします。
5. （PDF への印刷のみ）レポートが保存される場所を参照し、**保存**をクリックします。

CAC ソフトウェアのエクスポート

この手順を使用して、セキュリティ設定をエクスポートし、別の Central Administrator Console (CAC)システムにインポートできるようにします。設定は、`ecac` ファイルとしてエクスポートされます。

1. 中央管理ワークスペースを開きます。
2. **詳細** > **CAC 設定のエクスポート**をクリックします。
   CAC 設定のエクスポートダイアログが開きます。
3. **参照**をクリックします。
4. 設定が保存されるフォルダを参照して選択し、**フォルダを選択**をクリックします。
5. **エクスポート**をクリックします。
   確認のメッセージが表示され、エクスポートした設定を含むファイルの名前が表示されます
6. **OK** をクリックします。

CAC ソフトウェア設定のインポート

前提となる手順
• CAC ソフトウェアのエクスポート

この手順を使用して、他の Central Administrator Console (CAC)システムからセキュリティ設定をインポートします。設定は、ecac ファイルからインポートされます。

1. 中央管理ワークスペースを開きます。
2. 構成ワークスペースを開きます。
3. ユーザー管理ページを開きます。
4. **詳細** > **CAC 設定をインポート**をクリックします。
   CAC 設定をインポートダイアログが開きます。
5. **参照**をクリックします。
6. インポートする設定を含むファイルを参照して選択し、**開く**をクリックします。
   ソフトウェアは、ファイルが有効であることを確認します。
7. **インポート**をクリックします。
   ソフトウェアは現在の設定をバックアップしてから、新しい設定をインポートします。確認メッセージが表示されます。

   注: インポートされた設定は、ソフトウェアの再起動後に適用されます。
8. **OK** をクリックします。

CAC ソフトウェア設定の復元

最後にエクスポートされた ecac 設定を自動的にインポートするには、この手順を使用します。

1. 中央管理ワークスペースを開きます。
2. **詳細** > **CAC 設定を復元**をクリックします。
   CAC 設定を復元ダイアログが開きます。

   注: 復元された設定は、Central Administrator Console (CAC)ソフトウェアが再起動された後に適用されます。
3. **はい**をクリックします。

CAC ユーザー管理設定のエクスポート

この手順を使用して、別の Central Administrator Console (CAC) システムに適用できるユーザー管理設定をエクスポートします。設定は、data ファイルとしてエクスポートされます。

注: エクスポートされた設定は、同じバージョンの CAC ソフトウェアを使用しているシステムにのみインポートできます。

1. 構成管理ワークスペースを開きます。
2. **詳細** > **ユーザー管理設定のエクスポート**をクリックします。
   CAC 設定のエクスポートダイアログが開きます。
3. **参照**をクリックします。
4. 設定が保存されるフォルダを参照して選択し、**フォルダを選択**をクリックします。
5. **エクスポート**をクリックします。
   確認のメッセージが表示され、エクスポートした設定を含むファイルの名前が表示されます
6. **OK** をクリックします。

CAC ユーザー管理設定のインポート

前提となる手順
• CAC ユーザー管理設定のエクスポート

この手順を使用して、他の Central Administrator Console (CAC)システムからセキュリティ設定をインポートします。設定は、`data` ファイルからインポートされます。

注: エクスポートされた設定は、同じバージョンの CAC ソフトウェアを使用しているシステムにのみインポートできます。

1. 構成管理ワークスペースを開きます。
2. **詳細** > **ユーザー管理設定のインポート**をクリックします。
   ユーザー管理設定のインポートダイアログが開きます。
3. **参照**をクリックします。
4. インポートする設定を含むファイルを参照して選択し、**開く**をクリックします。
   ソフトウェアは、ファイルが有効であることを確認します。
5. **インポート**をクリックします。
   ソフトウェアは現在の設定をバックアップしてから、新しい設定をインポートします。確認メッセージが表示されます。

   注: インポートされた設定は、CAC ソフトウェアの再起動後に適用されます。
6. **OK** をクリックします。

ネットワーク取得 6

このセクションでは、ネットワーク取得が SCIEX OS ソフトウェア内でどのように機能するか、ならびにネットワークベースプロジェクトの利点と限界について説明します。また、ネットワーク取得の設定手順も記載されています。

ネットワーク取得について

ネットワーク取得機能を使用すれば、1 つまたは複数の装置から、リモートワークステーションで処理することが可能なネットワークベースのプロジェクトフォルダにデータを取り込むことができます。このプロセスはネットワーク障害への耐性があるため、取得時にネットワーク接続障害が発生してもデータが失われることはありません。

ネットワークプロジェクトが使用されている場合は、ローカルプロジェクトが使用されている場合より、システムのパフォーマンスが遅くなる可能性があります。ネットワークフォルダには監査証跡が存在するため、プロジェクト監査レコードの生成を伴うアクティビティも低速化します。ネットワークパフォーマンスによっては、ファイルが開くまで時間がかかる場合があります。ネットワークパフォーマンスは、物理的なネットワークハードウェアのみならず、ネットワークトラフィックやそのデザインにも関連しています。

注: ネットワーク取得中に ClearCore2 が中断されると、中断時に取得中のサンプルの一部のサンプルデータは、データファイルに書き込まれません。

注: 規制環境のもとでネットワーク取得機能を使用する場合は、正確なタイムスタンプが得られるよう、ローカルコンピュータの時刻をサーバーの時刻と同期させてください。ファイルの作成時刻には、サーバーの時刻が用いられます。Audit Trail Manager では、ローカルコンピュータの時刻を用いてファイルの作成時刻が記録されます。

注意: データ損失の可能性。複数の取得コンピュータからのデータを同じネットワークのデータファイルに保存しないでください。

ネットワーク取得を使用することで得られる利点

ネットワークデータ取得は、すべてネットワークサーバーに存在しているプロジェクトフォルダで安全に作業を行うための手段となります。これにより、データをローカルでデータを収集した後、保存のためデータをネットワーク上の場所に移動する作業の複雑さが緩和されます。また、ネットワークドライブは通常自動的にバックアップされるため、ローカルドライブのバックアップ作業が軽減または撤廃されます。

安全ネットワークアカウント

ネットワークフォルダにデータを取得する規制された環境では、ユーザーが宛先フォルダの削除権限を持たないことを強くお勧めします。ただし、このフォルダへの削除アクセスがないと、SCIEX OS ソフトウェアは最適に動作できません。安全ネットワークアカウント（SNA）機能では、ネットワークル

ートディレクトリのフルコントロールファイル権限を持つネットワークアカウントを特定します。ClearCore2 サービスは、このアカウントを使用してデータをネットワークフォルダに転送します。

SNA は、次をフルコントロールする必要があります。

- ネットワークルートディレクトリフォルダ
- 取得コンピュータの `SCIEX OS Data\NetworkBackup` フォルダ
- 取得コンピュータの `SCIEX OS Data\TempData` フォルダ

SNA 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。
- SCIEX OS ソフトウェアの User Management データベースに存在します。

SNA は、構成 ワークスペースのプロジェクトページで指定されています。有効な Windows ネットワークまたはドメインアカウントのみを指定できます。

SNA が指定されていない場合、SCIEX OS ソフトウェアは現在ログオンしているユーザーの資格情報を使用して、データをネットワーク ルート ディレクトリに転送します。転送が成功するためには、どのユーザーが取得のためにバッチを送信したかにかかわらず、アカウントは、データの取得先のすべてのプロジェクトフォルダへの書き込み権限を有している必要があります。

データ転送プロセス

SCIEX OS ソフトウェアがネットワーク上の場所にデータを取得する場合、まず各サンプルをローカルドライブのフォルダに書き込み、次にそれをネットワークに転送します。データファイル全体の転送の成功が確認されると、データを含むローカルフォルダは削除されます。このプロセスでネットワークが使用できなくなった場合、SCIEX OS は、転送が成功するまで、15 分ごとに再試行します。

長期間のネットワーク接続切断中のデータアクセスについては、次のセクションを参照：ネットワーク転送フォルダからサンプルを削除。

ネットワーク取得を構成

ルートディレクトリは、SCIEX OS ソフトウェアがデータを保存するフォルダです。プロジェクト情報が安全に保存されるようにするには、SCIEX OS ソフトウェアでルートディレクトリを作成します。File Explorer にプロジェクトを作成しないでください。

オプションで、ネットワークリソースにルートディレクトリを作成する場合は、**安全ネットワークアカウントの認証情報**を定義してください。これがネットワークリソース上で定義されている安全ネットワークアカウントです。次のセクションを参照：安全ネットワークアカウント。

プロジェクトとサブプロジェクトの作成について詳しくは、次のドキュメントを参照：*SCIEX OS『ソフトウェアユーザーガイド』*。

安全ネットワークアカウントの指定

プロジェクトがネットワークリソースに保存されている場合、ワークステーションのすべてのユーザーがネットワークリソースに必要なアクセス権を持つようにするために、SNA を指定できます。

1. 構成ワークスペースを開きます。

2. **プロジェクト**をクリックします。
3. **詳細** セクションの **安全ネットワークアカウントの認証情報**をクリックします。
4. ネットワークリソースで定義されている安全ネットワークアカウントのユーザー名、パスワード、ドメインを入力します。
5. **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 の監査機能の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。

監査証跡

ソフトウェアは、監査証跡ワークスペースで監査イベントを整理します。ソフトウェアは、監査証跡にイベントを保管します。監査証跡は、監査済みイベントの記録を保管するファイルです。

ワークステーションイベントは、ワークステーション監査証跡に保存されます。ワークステーション監査証跡は、SCIEX OS 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監査済みイベントを保存するファイルです。

CACCAC システムは、ワークステーション監査証跡に保存されます。

プロジェクトイベントは、プロジェクト監査証跡に保存されます。監査証跡ワークスペースには、アクティブなルートディレクトリ内のプロジェクトの監査証跡が表示されます。処理監査証跡イベントはプロジェクト監査証跡に含まれ、定量テーブルとともに保存されます。

監査済み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: 監査イベント。

監査証跡は、`wiff2` ファイルや定量テーブル ファイルなどのファイルと組み合わせて、コンプライアンスの目的で使用できる有効な電子記録です。

表 7-1：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

ワークステーション（SCIEX OS）	• 以下のように変更:
	  • アクティブ監査マップの割り当て
	  • 装置のチューニング
	  • サンプルキュー
	  • セキュリティ
	  • チューニング
	  • 装置
		• `C:\ProgramData\SCIEX\Audit Data` フォルダ	• No Audit Map（監査マップなし）

表 7-1：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

CAC	• 以下のように変更：
	  • 監査マップ
	  • CAC
	  • セキュリティ
	  • ユーザーログ
		• `C:\ProgramData\SCIEX\Audit Data` フォルダ	• Silent Audit Map（サイレント監査マップ）

プロジェクト（プロジェクトごとに 1 つ）	• 以下のように変更：
	  • アクティブ監査マップの割り当て (SCIEX OS)
	  • プロジェクト
	  • データ
	• 印刷
		• `<project>\Audit Data` フォルダ	• 監査マップワークスペースの構成ページで指定

監査証跡に 20,000 件の監査レコードが含まれると、SCIEX OS および CAC 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：監査証跡アーカイブ。

監査マップ

監査マップは、監査可能なすべてのイベントのリストと、そのイベントに変更理由または電子署名が必要かどうかを含むファイルです。SCIEX OS ソフトウェアでは、ワークステーションとプロジェクトの 2 種類の監査マップを使用できます。CAC ソフトウェアでは次の 2 種類の監査マップを使用：CAC とプロジェクト。

ワークステーション監査マップは、ワークステーションで監査されるイベントを制御します。

プロジェクト監査マップは、プロジェクトについて監査されるイベントを制御し、プロジェクト フォルダに格納されます。

注: プロジェクトの監査マップは、SCIEX OS または Central Administrator Console (CAC)ソフトウェアで編集できます。

ユーザーは多数の監査マップを作成できますが、各ワークステーション、CAC システム、および各プロジェクトで使用できる監査マップは常に 1 つだけです。ワークステーション、CAC システム、またはプロジェクトで使用中の監査マップは、アクティブな監査マップと呼ばれます。

SCIEX OS をインストールすると、すべての新しいプロジェクトのデフォルトの監査マップは、監査マップなしです。CAC ソフトウェアをインストールすると、すべての新規プロジェクトのデフォルトの監査マップは[サイレント監査マップ]になります。別のアクティブ監査マップを特定し、すべての新規プ

ロジェクトのデフォルトとして使用することもできます。次のセクションを参照:プロジェクトのアクティブ監査マップの変更。

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。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テンプレートを使用できますが、カスタマイズしたマップを作成する必要がある場合があります。ワークステーションまたは CAC 監査証跡に 1 つの監査マップが使用可能であり、プロジェクトごとに 1 つの監査マップが使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

• SCIEX OS:ワークステーション監査証跡用の監査マップを作成する。
• CAC ソフトウェア:CAC 監査証跡の監査マップを作成する。
	• SCIEX OS:
	  • ワークステーション監査マップの作成
	  • ワークステーション監査マップの編集
	• CAC ソフトウェア:
	  • CAC 監査マップの作成
	  • CAC 監査マップの編集

• SCIEX OS ワークステーション監査証跡用の監査マップを適用する。 • CACCAC ソフトウェア:監査証跡用の監査マップを適用する。	• SCIEX OS:ワークステーションのアクティブ監査マップの変更 • CAC ソフトウェア:CAC システムのアクティブな監査マップを変更
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。	• プロジェクト監査マップの作成。
既存のプロジェクトで使用する監査マップを構成する。	• プロジェクト監査マップの作成。 • プロジェクト監査マップの編集。
既存のプロジェクトに監査マップを適用する。	• プロジェクトのアクティブ監査マップの変更。

インストール済みの監査マップテンプレート

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。これらのテンプレートの編集や削除はできません。

表 7-3：インストール済みの監査マップ

監査マップ	説明
監査マップ例示	選択されたイベントが監査されます。例示目的のみ。
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。

表 7-3：インストール済みの監査マップ (続き)

監査マップ	説明
監査マップなし	イベントは監査されません。 **注: アクティブ監査マップの割り当ての変更**イベントは、No Audit Map テンプレートが使用されている場合でも常に記録されます。
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、次の表を参照：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：SCIEX OS 監査証跡レコード。

監査プロセスの詳細な情報については、次の表を参照：表 7-2。

監査マップの作業を行う

ソフトウェアには、いくつかのインストール監査マップ テンプレートがインストールされています。監査マップテンプレートについては、次のセクションを参照: インストール済みの監査マップテンプレート。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。

アクティブな監査マップ テンプレートがソフトウェアまたはファイル エクスプローラーで削除された場合、その監査マップ テンプレートを使用するプロジェクトはサイレント監査マップを使用します。

プロジェクト監査マップ

プロジェクト監査マップは、プロジェクトイベントの監査をコントロールします。監査済みプロジェクトイベントのリストについては、次のセクションを参照: プロジェクト監査証跡。

プロジェクト監査マップの作成

1. 構成ワークスペースを開きます。
2. **監査マップ**をクリックします。
3. プロジェクトテンプレートタブを開きます。
4. **マップテンプレートの編集**フィールドで、新しいマップの基礎として使用するテンプレートを選択します。
5. **テンプレートを追加**（  ）をクリックします。
   プロジェクト監査マップテンプレートを追加ダイアログが開きます。
6. 新しいマップの名前を入力し、**OK** をクリックします。
7. 次の手順に従って、記録するイベントを選択して構成します。
   a. イベントの**監査済み**チェックボックスを選択します。
   b. （オプション）理由が必要な場合は、**必要な理由**を選択します。

c. （オプション）電子署名が必要な場合は、**電子署名が必要**を選択します。

d. （オプション）事前定義の理由が必要な場合は、**事前定義した理由のみを使用**を選択して理由を定義します。

8. 監査されないイベントについては、**監査済み**チェックボックスがオフになっていることを確認してください。

9. **テンプレートを保存**をクリックします。
システムは新しいマップをプロジェクトに適用するように求めます。

10. 次のいずれかの操作を行います。

- 新しいマップをプロジェクトに適用するには、**はい**をクリックして新規マップを使用するプロジェクトを選択し、**適用**をクリックします。
- 新規マップを既存のプロジェクトに適用しない場合は、**いいえ**をクリックします。

11. （任意）この監査マップをすべての新規プロジェクトのデフォルトとして使用する場合は、**新規プロジェクトのデフォルトとして使用**をクリックします。

プロジェクト監査マップの編集

注: インストールされている監査マップテンプレートは編集できません。

1. 構成ワークスペースを開きます。
2. **監査マップ**をクリックします。
3. プロジェクトテンプレートタブを開きます。
4. **マップテンプレートの編集**フィールドで、修正するマップを選択します。
5. 次の手順に従って、記録するイベントを選択して構成します。

a. イベントの**監査済み**チェックボックスを選択します。

b. （オプション）理由が必要な場合は、**必要な理由**を選択します。

c. （オプション）電子署名が必要な場合は、**電子署名が必要**を選択します。

d. （オプション）事前定義の理由が必要な場合は、**事前定義した理由のみを使用**を選択して理由を定義します。

6. 監査されないイベントについては、**監査済み**チェックボックスがオフになっていることを確認してください。

7. **テンプレートを保存**をクリックします。
システムは新しいマップをプロジェクトに適用するように求めます。

8. 次のいずれかの操作を行います。

- 新しいマップをプロジェクトに適用するには、**はい**をクリックして新規マップを使用するプロジェクトを選択し、**適用**をクリックします。
- 新規マップを既存のプロジェクトに適用しない場合は、**いいえ**をクリックします。

プロジェクトのアクティブ監査マップの変更

プロジェクトに監査マップを適用すると、それがアクティブ監査マップになります。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。

1. 構成ワークスペースを開きます。
2. **監査マップ**をクリックします。
3. プロジェクトテンプレートタブを開きます。
4. **マップテンプレートの編集**フィールドで、プロジェクトに適用する監査マップを選択します。
5. **既存のプロジェクトに適用**をクリックします。
   プロジェクト監査マップテンプレートの適用ダイアログが開きます。
6. この監査マップを適用するプロジェクトのチェックボックスを選択します。
7. **適用**をクリックします。

プロジェクト監査マップの削除

注: インストールされている監査マップテンプレートは削除できません。

1. 構成ワークスペースを開きます。
2. **監査マップ**をクリックします。
3. プロジェクトテンプレートタブを開きます。
4. **マップテンプレートの編集**フィールドで、削除するマップを選択します。
5. **テンプレートを削除**をクリックします。
   システムによって確認のメッセージが表示されます。
6. **はい**をクリックします。

ワークステーション監査マップ

ワークステーション監査マップは、ワークステーションイベントの監査をコントロールします。監査済みワークステーションイベントのリストについては、次のセクションを参照: ワークステーション監査証跡。

ワークステーション監査マップの作成

1. 構成ワークスペースを開きます。
2. **監査マップ**をクリックします。
3. ワークステーションテンプレート タブを開きます。
4. **マップテンプレートの編集**フィールドで、新しいマップの基礎として使用するテンプレートを選択します。
5. **テンプレートを追加**()をクリックします。
   ワークステーション監査マップテンプレートを追加ダイアログが開きます。

6. 新しいマップの名前を入力し、**OK** をクリックします。
7. 次の手順に従って、記録するイベントを選択して構成します。
    a. イベントの**監査済み**チェックボックスを選択します。
    b. （オプション）理由が必要な場合は、**必要な理由**を選択します。
    c. （オプション）電子署名が必要な場合は、**電子署名が必要**を選択します。
    d. （オプション）事前定義の理由が必要な場合は、**事前定義した理由のみを使用**を選択して理由を定義します。
8. 監査されないイベントについては、**監査済み**チェックボックスがオフになっていることを確認してください。
9. **テンプレートを保存**をクリックします。
10. （オプション）この監査マップをワークステーションのアクティブ監査マップとして使用するには、**ワークステーションに適用**をクリックします。

ワークステーション監査マップの編集

注: インストールされている監査マップテンプレートは編集できません。

1. 構成ワークスペースを開きます。
2. **監査マップ**をクリックします。
3. ワークステーションテンプレート タブを開きます。
4. **マップテンプレートの編集**フィールドで、変更するマップを選択します。
5. 次の手順に従って、記録するイベントを選択して構成します。
    a. イベントの**監査済み**チェックボックスを選択します。
    b. （オプション）理由が必要な場合は、**必要な理由**を選択します。
    c. （オプション）電子署名が必要な場合は、**電子署名が必要**を選択します。
    d. （オプション）事前定義の理由が必要な場合は、**事前定義した理由のみを使用**を選択して理由を定義します。
6. 監査されないイベントについては、**監査済み**チェックボックスがオフになっていることを確認してください。
7. **テンプレートを保存**をクリックします。
8. （オプション）この監査マップをワークステーションのアクティブ監査マップとして使用するには、**ワークステーションに適用**をクリックします。

ワークステーションのアクティブ監査マップの変更

ワークステーションに監査マップを適用すると、それがアクティブ監査マップになります。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。

1. 構成ワークスペースを開きます。
2. **監査マップ**をクリックします。

3. ワークステーションテンプレート タブを開きます。
4. **マップテンプレートの編集**フィールドで、ワークステーションに適用するマップを選択します。
5. **ワークステーションに適用**をクリックします。

ワークステーション監査マップの削除

注: インストールされている監査マップテンプレートは削除できません。

1. 構成ワークスペースを開きます。
2. **監査マップ**をクリックします。
3. ワークステーションテンプレート タブを開きます。
4. **マップテンプレートの編集**フィールドで、削除するマップを選択します。
5. **テンプレートを削除**をクリックします。
   システムによって確認のメッセージが表示されます。
6. **はい**をクリックします。

CAC 監査マップ

CAC 監査マップは、CAC ワークステーションイベントの監査をコントロールします。監査済みイベントのリストについては、次のセクションを参照: ワークステーション監査証跡。

CAC 監査マップの作成

1. 構成ワークスペースを開きます。
2. **監査マップ**をクリックします。
3. CAC テンプレートタブを開きます。
4. **マップテンプレートの編集**フィールドで、新しいマップの基礎として使用するテンプレートを選択します。
5. **テンプレートを追加**()をクリックします。
   CAC 監査マップテンプレートを追加ダイアログが開きます。
6. 新しいマップの名前を入力し、**OK** をクリックします。
7. 次の手順に従って、記録するイベントを選択して構成します。
   a. イベントの**監査済み**チェックボックスを選択します。
   b. (オプション)理由が必要な場合は、**必要な理由**を選択します。
   c. (オプション)電子署名が必要な場合は、**電子署名が必要**を選択します。
   d. (オプション)事前定義の理由が必要な場合は、**事前定義した理由のみを使用**を選択して理由を定義します。
8. 監査されないイベントについては、**監査済み**チェックボックスがオフになっていることを確認してください。

9. **テンプレートを保存**をクリックします。
10. （オプション）この監査マップを CAC ワークステーションのアクティブ監査マップとして使用するには、**CAC に適用**をクリックします。

CAC 監査マップの編集

注: インストールされている監査マップテンプレートは編集できません。

1. 構成ワークスペースを開きます。
2. **監査マップ**をクリックします。
3. CAC テンプレートタブを開きます。
4. **マップテンプレートの編集**フィールドで、変更するマップを選択します。
5. 次の手順に従って、記録するイベントを選択して構成します。
   a. イベントの**監査済み**チェックボックスを選択します。
   b. （オプション）理由が必要な場合は、**必要な理由**を選択します。
   c. （オプション）電子署名が必要な場合は、**電子署名が必要**を選択します。
   d. （オプション）事前定義の理由が必要な場合は、**事前定義した理由のみを使用**を選択して理由を定義します。
6. 監査されないイベントについては、**監査済み**チェックボックスがオフになっていることを確認してください。
7. **テンプレートを保存**をクリックします。
8. （オプション）この監査マップを CAC ワークステーションのアクティブ監査マップとして使用するには、**CAC に適用**をクリックします。

CAC システムのアクティブな監査マップを変更

CAC ワークステーションに監査マップを適用すると、それがアクティブ監査マップになります。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。

1. 構成ワークスペースを開きます。
2. **監査マップ**をクリックします。
3. CAC テンプレートタブを開きます。
4. **マップテンプレートの編集**フィールドで、CAC ワークステーションに適用するマップを選択します。
5. **CAC に適用**をクリックします。

CAC 監査マップの削除

注: インストールされている監査マップテンプレートは削除できません。

1. 構成ワークスペースを開きます。
2. **監査マップ**をクリックします。

3. CAC テンプレートタブを開きます。
4. **マップテンプレートの編集**フィールドで、削除するマップを選択します。
5. **テンプレートを削除**をクリックします。
   システムによって確認のメッセージが表示されます。
6. **はい**をクリックします。

監査証跡の表示、検索、エクスポート、印刷

本項では、監査証跡と、アーカイブ済みの監査証跡を表示する方法について説明します。また、監査証跡内の監査レコードをエクスポート、印刷、検索、並べ替えるための手順も記されています。

監査証跡の記録の表示

1. 監査証跡 ワークスペースを開きます。
2. 左ペインで、表示する監査証跡をクリックします。
3. 監査イベントの詳細情報を表示するには、イベントをクリックします。
   選択したイベントのタイプによって、表示される情報が制御されます。情報は、次の 1 つ以上のタブに表示されます。

表 7-4：イベント詳細タブ

タブ	情報
一般的な詳細	SCIEX OS ソフトウェアのタイムゾーンオフセット、ワークステーション名、バージョンなどの情報を表示します。
変更前	変更前の内容を表示します。
変更後	変更後の内容を表示します。
変更の詳細	元のコンテンツと新しいコンテンツを同じペインに表示します。差分ビューでは、元のコンテンツは赤色で表示され、新しいコンテンツは緑色で表示されます。並べて表示 では、元のコンテンツと新しいコンテンツが別のペインに表示されるため、変更を簡単に確認できます。
印刷詳細	印刷された情報を表示します。

監査レコードの検索またはフィルター

1. 監査証跡 ワークスペースを開きます。
2. 検索する監査証跡を選択します。
3. 特定の監査レコードを検索するには、**ページで検索**フィールドにテキストを入力します。
   検索対象のテキストがページ上でハイライト表示されます。
4. 監査証跡レコードをフィルターするには、以下の手順を実行します。
   a. フィルター（じょうご）のアイコンをクリックします。
      監査証跡をフィルターダイアログが開きます。

b. フィルター条件を入力します。

c. **OK** をクリックします。

アーカイブ済み監査証跡の表示

監査証跡に含まれる監査レコードが 20,000 件を超えると、SCIEX OS ソフトウェアはレコードを自動的にアーカイブして、新しい監査証跡を開始します。アーカイブされた監査証跡のファイルには、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。たとえば、ワークステーション監査証跡アーカイブのファイル名の形式は `WorkstationAuditTrailData-<workstation name>>-<YYYY><MMDDHHMMSS>.atds` です。

この手順は、定量テーブルの監査証跡を開くためにも使用されます。

1. 監査証跡 ワークスペースを開きます。
2. **参照**をクリックします。
3. 開きたいアーカイブ済み監査証跡を参照して選択し、**OK** をクリックします。

注: 定量テーブルの監査証跡を選択には、関連する `qsession` ファイルを選択します。

監査証跡の印刷

1. 監査証跡 ワークスペースを開きます。
2. 印刷する監査証跡を選択します。
3. **印刷**をクリックします。
   印刷ダイアログが開きます。
4. プリンタを選択し、**OK** をクリックします。

監査証跡レコードのエクスポート

1. 監査証跡 ワークスペースを開きます。
2. エクスポートする監査証跡を選択します。
3. **エクスポート**をクリックします。
4. エクスポートしたファイルを保管する場所を参照し、**ファイル名**を入力して**保存**をクリックします。
   監査証跡は、カンマ区切り（CSV）ファイルとして保存されます。

SCIEX OS 監査証跡レコード

このセクションでは、監査証跡レコードのフィールドについて説明します。

ワークステーション監査証跡およびプロジェクト監査証跡は暗号化されたファイルです。

注: ワークステーション監査証跡とアーカイブは、`Program Data\SCIEX\Audit Data` フォルダーに保管されます。プロジェクト監査証跡とアーカイブは、プロジェクトの `Audit Data` フォルダーに保管されます。

表 7-5 : 監査レコードフィールド

ラベル	説明
タイムスタンプ	レコードが作成された日時。
イベント名	イベントの名前。
説明	イベントの説明。
理由	イベントの理由。
電子署名	イベントの電子署名が入力されたかどうか。
ユーザーのフルネーム	ユーザーの名前。 **注:** 決定ルールによってトリガーされたイベントの場合は、これはバッチを送信したユーザーです。
ユーザー	レコードを生成したイベントを開始したユーザーのユーザー ID。
カテゴリ	イベントが属する機能またはカテゴリ。

監査証跡ワークスペースの下部ペインには、選択したイベントに関する詳細情報が表示されます。これには、該当する場合は変更の詳細も含まれます。

ワークステーションおよびプロジェクトの監査証跡に記録されるすべてのイベントのリストについては、次のセクションを参照 : ワークステーション監査証跡およびプロジェクト監査証跡。

CAC 監査証跡レコード

このセクションでは、監査証跡レコードのフィールドについて説明します。

CAC およびプロジェクトの監査証跡は、暗号化されたファイルです。

注: CAC 監査証跡とアーカイブは、`Program Data\SCIEX\Audit Data` フォルダに保存されます。プロジェクト監査証跡とアーカイブは、プロジェクトの `Audit Data` フォルダに保存されます。

表 7-6 : 監査レコードフィールド

ラベル	説明
タイムスタンプ	レコードが作成された日時。
イベント名	イベントの名前。
説明	イベントの説明。
理由	イベントの理由。

表 7-6：監査レコードフィールド (続き)

ラベル	説明
電子署名	イベントの電子署名が入力されたかどうか。
ユーザーのフルネーム	ユーザーの名前。 **注:** 決定ルールによってトリガーされたイベントの場合は、これはバッチを送信したユーザーです。
ユーザー	レコードを生成したイベントを開始したユーザーのユーザー ID。
カテゴリ	イベントが属する機能またはカテゴリ。

監査証跡ワークスペースの下部ペインには、選択したイベントに関する詳細情報が表示されます。これには、該当する場合は変更の詳細も含まれます。

CAC およびプロジェクト監査証跡に記録されるすべてのイベントのリストについては、次のセクションを参照：表 3 およびプロジェクト監査証跡。

監査証跡アーカイブ

プロジェクト監査証跡とワークステーション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。

監査証跡のレコード数が 20,000 件に達すると、アーカイブされます。最後のアーカイブレコードは監査証跡に追加され、監査証跡の種類と日時を示す名前が付けられ、監査証跡が保存されます。新しい監査証跡が作成されます。新しい監査証跡の最初のレコードには、監査証跡がアーカイブされていることと、アーカイブされた監査証跡へのパスが示されます。

ワークステーション監査証跡は、`C:\ProgramData\SCIEX\Audit Data` フォルダに保存されます。ファイル名の形式は、WorkstationAuditTrailData です。<*ワークステーション名*>-<*YYYY*><*MMDDHHMMSS*>.atds.たとえば、`WorkstationAuditTrailData-SWDSXPT158-20190101130401.atds` です。

プロジェクト監査証跡のアーカイブは、プロジェクトの `Audit Data` フォルダに保存されます。

ネットワーク中断中のデータへのアクセス A

データをローカルに表示および処理する

ネットワーク取得中に一時的なネットワークの中断が発生した場合、取得データは、取得コンピュータの NetworkBackup フォルダからアクセスすることができます。データの破損を避けるためには、NetworkBackup フォルダのデータファイルを表示または処理する前に新しい場所にコピーし、ファイルの元のコピーを NetworkBackup フォルダに残しておくことをお勧めします。

15 分ごとに SCIEX OS ソフトウェアは、ネットワークの場所が利用できるかどうかを判断します。利用できる場合、データの転送が再開されます。

NetworkBackup フォルダは、ローカルルートディレクトリ（通常は D:\SCIEX OS Data\NetworkBackup）に格納されています。各バッチのデータファイルは、フォルダ名として一意の識別子を持つフォルダに保存されています。フォルダの日時のスタンプは、バッチの開始日時を示し、どのフォルダに対象データが含まれているかを見分けるために使用することができます。

ネットワーク転送フォルダからサンプルを削除

ネットワーク接続が長期間切断された場合、またはネットワークルートディレクトリが変更された場合、ネットワーク転送フォルダからデータファイルを削除する必要があります。この措置は、高度なネットワーク技術を有するシステム管理者が行うことをお勧めします。

1. キューワークスペースを開きます。
2. キューを停止します。
3. 削除するサンプルを含むバッチにある残りのすべてのサンプルをキャンセルします。
4. SCIEX OS ソフトウェアを閉じます。
5. **Clearcore2.Service.exe** を停止します。

   ヒント! Windows のサービスマネージャーからこのタスクを実行します。

6. 利用できないルートディレクトリへの転送を待っているフォルダ OutBox および NetworkBackup 内のすべてのファイルとフォルダを一時的に別のフォルダに移動します。フォルダ OutBox も NetworkBackup も削除しないでください。

   注: OutBox フォルダは、ローカルルートディレクトリ（通常、D:\SCIEX OS Data\TempData\Outbox）の隠しフォルダです。Outbox 内のファイルやフォルダが不要になったら、削除してかまいません。

   注意: データ損失の可能性。スタックサンプルのデータを保存する必要がある場合は、ファイルを削除しないでください。

7. SCIEX OS ソフトウェアを起動します。
   15 分以内に、SCIEX OS ソフトウェアはネットワークリソースへの接続を試みます。接続が成功すると、転送が再開されます。転送が完了すると、`NetworkBackup` フォルダ内のフォルダは削除されます。

Windows 権限 B

ここでは、SCIEX OS ソフトウェアを正しく動作させるために、各ユーザーロールおよび SYSTEM ユーザーに必要な Windows 権限の一覧を示します。

注: インストールされたルート ディレクトリ フォルダの *デフォルトの* パスは `D:\SCIEX OS Data` です。

表 B-1：*インストールされたルート ディレクトリフォルダ*

権限	管理者、システム	Analyst、メソッド開発者、レビューア
フルコントロール	許可	—
フォルダのトラバース/ファイルの実行	許可	許可
フォルダのリスト/データの読み込み	許可	許可
属性の読み取り	許可	許可
拡張属性の読み取り	許可	許可
ファイルの作成/データの書き込み	許可	許可
フォルダの作成/データの追加	許可	許可
属性の書き込み	許可	許可
拡張属性の書き込み	許可	許可
サブフォルダとファイルの削除	許可	—
削除	許可	—
権限読み取り	許可	許可
権限の変更	許可	—
所有権を取得	許可	—

表 B-2：*Installed Root Directory*\NetworkBackup および *Installed Root Directory*\TempData フォルダ

権限	管理者、システム	Analyst、メソッド開発者、レビューア
フルコントロール	許可	—
フォルダのトラバース/ファイルの実行	許可	許可
フォルダのリスト/データの読み込み	許可	許可
属性の読み取り	許可	許可
拡張属性の読み取り	許可	許可
ファイルの作成/データの書き込み	許可	許可
フォルダの作成/データの追加	許可	許可
属性の書き込み	許可	許可
拡張属性の書き込み	許可	許可
サブフォルダとファイルの削除	許可	許可
削除	許可	許可
権限読み取り	許可	許可
権限の変更	許可	—
所有権を取得	許可	—

表 B-3：C:\ProgramData\SCIEX\Audit Data フォルダ

権限	管理者、システム	Analyst、メソッド開発者、レビューア
フルコントロール	許可	—
フォルダのトラバース/ファイルの実行	許可	許可
フォルダのリスト/データの読み込み	許可	許可
属性の読み取り	許可	許可

表 B-3：C:\ProgramData\SCIEX\Audit Data フォルダ (続き)

権限	管理者、システム	Analyst、メソッド開発者、レビューア
拡張属性の読み取り	許可	許可
ファイルの作成/データの書き込み	許可	許可
フォルダの作成/データの追加	許可	許可
属性の書き込み	許可	許可
拡張属性の書き込み	許可	許可
サブフォルダとファイルの削除	許可	—
削除	許可	—
権限読み取り	許可	許可
権限の変更	許可	—
所有権を取得	許可	—

監査イベント C

このセクションでは、SCIEX OS の監査イベントを一覧表示します。また、Analyst ソフトウェアから SCIEX OS に移行するユーザー向けに、Analyst ソフトウェアの対応する監査イベントも一覧表示します。

プロジェクト監査証跡

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は、プロジェクトの `Audit Data` フォルダに保管されます。監査証跡のファイル名は、`ProjectAuditEvents.atds` です。

注: Central Administrator Console (CAC)ソフトウェアで作成された新しいプロジェクトのデフォルトの監査マップは、サイレント監査マップです。

プロジェクトの監査証跡イベントは、CAC ソフトウェアと SCIEX OS の両方で表示されます。

表 C-1：プロジェクト監査証跡イベント

SCIEX OS または CAC	Analyst ソフトウェア
アナリティクス ワークスペース	
実際の濃度が変更されました	定量化イベント:**「濃度」が変更されました**
自動処理ファイルが保存されました	—
バーコード ID が変更されました	—
ノンターゲットワークフローでの比較サンプルが変更されました	—
カスタム列が修正されました	定量化イベント:**「カスタムタイトル」が変更されました**
データ探索が開始されました	プロジェクトイベント:**Data File has been opened**
データがエクスポートされました	—
LIMS にデータが転送されました	—
希釈係数が変更されました	定量化イベント:**「希釈係数」が変更されました**
外部キャリブレーションが変更されました	—
外部キャリブレーションがエクスポートされました	—

表 C-1：プロジェクト監査証跡イベント (続き)

SCIEX OS または CAC	Analyst ソフトウェア
ファイルの保存	プロジェクトイベント：**Quantitation Results Table has been created**、**Quantitation Results Table has been modified**、Quantitation Events：**Results Table has been saved**
数式列が変更されました	定量化イベント：**Formula name has been changed**、**Formula name has been added**、**Formula string has been changed**、**Formula column has been removed**
積分のクリア	—
積分パラメータが変更されました	定量化イベント：**Quantitation peak has been integrated**
ライブラリ検索結果が変更されました	—
手動積分	定量化イベント：**Quantitation Peak has been integrated**
手動積分が復元されました	定量化イベント：**Quantitation peak has been reverted back to original**
MS/MS 選択が変更されました	—
処理メソッドの印刷	—
処理メソッドの変更と適用	定量化イベント：**Quantitation method has been changed**
処理メソッドが保存されました	—
プロジェクトのデフォルト設定が変更されました	—
レポートの作成	プロジェクトイベント：**Printing document on printer**、**Finished printing document on printer**
定量テーブルの承認	定量化イベント：**QA reviewer has accessed a results table**
定量テーブルの作成	定量化イベント：**Results table has been created**
定量テーブルのロック	—
定量テーブルのロック解除	—
サンプル ID が変更されました	定量化イベント：**「Sample ID」has been changed**

表 C-1：プロジェクト監査証跡イベント (続き)

SCIEX OS または CAC	Analyst ソフトウェア
サンプル名が変更されました	定量化イベント：「Sample Name」has been changed
サンプルタイプが変更されました	定量化イベント：「Sample Type」has been changed
サンプルの追加または削除	定量化イベント：Files have been added to Results Table、Files have been removed from Results Table、Samples have been added/removed
標準添加の実際の濃度が変更されました	—
適用した列の選択が変更されました	定量化イベント：「Use IT」has been changed
重量/容量が変更されました	「Weight to Volume Ratio」has been changed
ウィンドウ/ペインの印刷	プロジェクトイベント：Printing document on printer、Finished printing document on printer
監査マップ ページ	
プロジェクト監査マップが変更されました	プロジェクトイベント：Project Settings have been changed
プロジェクト監査証跡のエクスポート	—
プロジェクト監査証跡の印刷	—
バッチ Workspace	
LIMS/text からインポートされたバッチ情報	—
バッチが保存されました	—
バッチが送信されました	装置イベント：Batch file submitted
印刷	プロジェクトイベント：Printing Document on printer、Finished printing document on printer
エクスプローラ ワークスペース [4]	
サンプルを開く	プロジェクトイベント：Data File has been opened
印刷	プロジェクトイベント：Printing Document on printer、Finished printing document on printer

[4] アクティブなプロジェクトのデータを使用すると、エクスプローラ イベントがプロジェクト監査証跡に記録されます。

表 C-1：プロジェクト監査証跡イベント (続き)

SCIEX OS または CAC	Analyst ソフトウェア
サンプルの再キャリブレーション	—
サンプルの再キャリブレーションの開始	—
LC メソッド Workspace	
LC メソッドが保存されました	—
印刷	プロジェクトイベント：**Printing Document on printer**、**Finished printing document on printer**
MS メソッド ワークスペース	
MS メソッドが保存されました	—
印刷	プロジェクトイベント：**Printing Document on printer**、**Finished printing document on printer**
キュー ワークスペース	
サンプル測定の完了	—
サンプルが編集されました	—
サンプルの測定開始	—
サンプル転送	—

ワークステーション監査証跡

ワークステーションには、それぞれ 1 つのワークステーション監査証跡があります。ワークステーション監査証跡は、`Program Data\SCIEX\Audit Data` フォルダに保管されます。監査証跡のファイル名の形式：`WorkstationAuditTrailData.atds`

注: Central Administrator Console (CAC)ソフトウェアで作成された新しいワークステーションのデフォルトの監査マップは、**サイレント監査マップ**です。

プロジェクトの監査証跡イベントは、CAC ソフトウェアと SCIEX OS の両方で表示されます。

表 C-2：ワークステーション監査証跡イベント

SCIEX OS	Analyst ソフトウェア
監査マップ	
ワークステーション監査マップが変更されました	装置イベント：**Instrument Settings have been changed**
ワークステーション監査証跡の印刷	—

表 C-2：ワークステーション監査証跡イベント (続き)

SCIEX OS	Analyst ソフトウェア
ワークステーション監査証跡のエクスポート	—
CAC	
中央管理の有効化/無効化	—
中央管理設定を取得しました/取得できませんでした	—
データファイルのチェックサム	
Wiff データファイルのチェックサムが変更されました	—
エクスプローラ ワークスペース [5]	
サンプルを開く	プロジェクトイベント：**Data File has been opened**
印刷	プロジェクトイベント：**Printing document on printer**、**Finished printing document on printer**
サンプルの再キャリブレーション	—
サンプルの再キャリブレーションの開始	—
ハードウェア構成	
デバイスのアクティブ化	装置イベント：**Hardware profile has been activated**
デバイスの非アクティブ化	装置イベント：**Hardware profile has been deactivated**
装置のチューニング	
自動 MS チューニングの更新	装置イベント：**Tune parameter settings changed**
ファームウェアが変更されました	—
MS チューニングの変更	装置イベント：**Tune parameter settings changed**
MS チューンの手順結果の印刷	プロジェクトイベント：**Printing Document on printer**、**Finished printing document on printer**
キュー ワークスペース	
自動注入が発生しました	—

[5] アクティブなプロジェクトにないデータを使用すると、エクスプローラ イベントがワークステーションの監査証跡に記録されます。

表 C-2：ワークステーション監査証跡イベント (続き)

SCIEX OS	Analyst ソフトウェア
自動再注入が発生しました	—
キューに移動したバッチ	装置イベント：**Move Batch**
キューの印刷	プロジェクトイベント：**Printing Document on printer**、**Finished printing document on printer**
サンプルの再取得	装置イベント：**Reacquiring sample(s)**
サンプル測定の完了	プロジェクトイベント：**Sample has been added to Data file**
キューに移動したサンプル	装置イベント：**Sample moved from position *x* to position *y* of Batch File**
サンプルの測定開始	—
セキュリティ	
システムによる自動ログオフ	装置イベント：**User Logged out**
別のユーザーによる強制ログオフ	装置イベント：**User Logged out**
強制ログオフに失敗しました	—
画面ロック解除に失敗しました	—
安全ネットワークアカウントの認証情報が変更	装置イベント：**Acquisition Account Changed**
安全ネットワークアカウントの認証情報が削除	装置イベント：**Acquisition Account Changed**
安全ネットワークアカウントの認証情報が指定	装置イベント：**Acquisition Account Changed**
セキュリティ構成が変更されました	装置イベント：**The Security Configuration has been modified**、**Screen Lock Changed**、**Auto Logout changed**
ユーザーの追加/削除	装置イベント：**User Added**、**User Deleted**
ユーザーがログインがしました	装置イベント：**User Logged In**
ユーザーがログアウトがしました	装置イベント：**User Logged out**
ユーザーが排他モードをオフにしました	—
ユーザーのログインが失敗	装置イベント：**User Login Failed**
ユーザー管理設定がエクスポートされました	—
ユーザー管理設定がインポートされました	—
ユーザー管理設定が復元されました	—

表 C-2：ワークステーション監査証跡イベント (続き)

SCIEX OS	Analyst ソフトウェア
ユーザー／ユーザーグループに割り当てられたユーザー役割	装置イベント：**User Changed User Type**
ユーザーの役割の削除	装置イベント：**User Type Deleted**
ユーザー役割の変更	装置イベント：**User Type Changed**
ユーザーログ	
イベントログの印刷	—

表 C-3：CAC 監査証跡イベント

CAC	Analyst ソフトウェア
監査マップ ページ	
ワークステーション監査マップが変更されました	装置イベント：**Instrument Settings have been changed**
ワークステーション監査証跡の印刷	—
ワークステーション監査証跡のエクスポート	—
CAC	
CAC の設定がエクスポートされました	—
CAC の設定がインポートされました	—
CAC の設定が復元されました	—
ワークグループで有効化/無効化にされたプロジェクト設定	—
ワークグループに割り当て済み/未割り当て	—
中央管理用にセキュリティ権限が追加	—
ユーザーの追加/削除	—
ユーザーの役割の追加	—
ユーザーの役割の削除	—
ユーザー役割の変更	—
ワークグループ内のユーザーに割り当て済み/未割り当てのユーザー役割	—
ワークグループに割り当て済み/未割り当てのユーザー/ユーザーグループ	—
ワークグループの追加/削除	—
名前が変更済みのワークグループ	—

表 C-3 : CAC 監査証跡イベント (続き)

CAC	Analyst ソフトウェア
ワークグループに割り当て済み/未割り当てのワークステーション	—
セキュリティ	
システムによる自動ログオフ	装置イベント: **User Logged out**
別のユーザーによる強制ログオフ	装置イベント: **User Logged out**
強制ログオフに失敗しました	—
画面ロック解除に失敗しました	—
安全ネットワークアカウントの認証情報が変更	装置イベント: **Acquisition Account Changed**
安全ネットワークアカウントの認証情報が削除	装置イベント: **Acquisition Account Changed**
安全ネットワークアカウントの認証情報が指定	装置イベント: **Acquisition Account Changed**
セキュリティ構成が変更されました	装置イベント: **The Security Configuration has been modified、Screen Lock Changed、Auto Logout changed**
ユーザーの追加/削除	装置イベント: **User Added、User Deleted**
ユーザーがログインがしました	装置イベント: **User Logged In**
ユーザーがログアウトがしました	装置イベント: **User Logged out**
ユーザーが排他モードをオフにしました	—
ユーザーのログインが失敗	装置イベント: **User Login Failed**
ユーザー管理設定がエクスポートされました	—
ユーザー管理設定がインポートされました	—
ユーザー管理設定が復元されました	—
ユーザー／ユーザーグループに割り当てられたユーザー役割	装置イベント: **User Changed User Type**
ユーザーの役割の削除	装置イベント: **User Type Deleted**
ユーザー役割の変更	装置イベント: **User Type Changed**
ユーザーログ	
イベントログの印刷	—

SCIEX OS と Analyst ソフトウェア間の権限のマッピング

D

このセクションは、Analyst ソフトウェアから SCIEX OS ソフトウェアに移行するユーザーが、ユーザーのセキュリティ設定を移行するために用意されています。SCIEX OS ソフトウェアの権限に対応する Analyst ソフトウェアの権限が表示されます。

表 D-1：権限のマッピング

SCIEX OS ソフトウェア	Analyst ソフトウェア
バッチ Workspace	
ロック解除されたメソッドを送信	—
開く	バッチ：**Open Existing Batches**
別名で保存	バッチ：**Create New Batches**、**Import**、**Edit Batches**、**Save Batches**、**Overwrite Batches**
送信	バッチ：**Submit Batches**
保存	バッチ：**Save Batches**、**Overwrite Batches**
イオン参照表の保存	—
データのサブフォルダを追加	—
決定ルールを設定	—
バッチを上書き	**バッチの上書き**
保存前にバッチを送信	—
構成 Workspace	
全般タブ	—
全般：地域設定の変更	—
全般：全画面モード	—
一般：Windows サービスの停止	—
LIMS 通信タブ	—
監査マップタブ	監査証跡マネージャー：**Change Audit Trail Settings**、**Create or Modify Audit Maps**
キュータブ	—
キュー：装置のアイドル時間	—
キュー：取得サンプルの最大数	—

表 D-1：権限のマッピング (続き)

SCIEX OS ソフトウェア	Analyst ソフトウェア
キュー：他のキュー設定	—
プロジェクトタブ	—
プロジェクト：プロジェクトの作成	Analyst アプリケーション：**Create Project**
プロジェクト：監査マップテンプレートを既存のプロジェクトに適用	Audit Trail Manager：**Change Audit Trail Settings**
プロジェクト：ルートディレクトリの作成	Analyst アプリケーション：**Create Root Directory**
プロジェクト：現在のルートディレクトリの設定	Analyst アプリケーション：**Set Root Directory**
プロジェクト：ネットワーク認証情報の指定	—
プロジェクト：wiff データ作成のチェックサム書き込みの有効化	—
プロジェクト：ルートディレクトリをクリアする	—
デバイスタブ	ハードウェア構成：**Create**、**Delete**、**Edit**、**Activate/Deactivate**
ユーザー管理タブ	セキュリティ構成
ユーザーの強制ログオフ	**Unlock/Logout Application**
CAC タブ [3]	—
印刷テンプレートタブ	—
印刷テンプレート：印刷テンプレートの作成と変更	—
印刷テンプレート：デフォルトの印刷テンプレートを設定	—
印刷テンプレート：現在のテンプレートをルートディレクトリ内のすべてのプロジェクトに適用	
イベントログ Workspace	
イベントログワークスペースへのアクセス	—
アーカイブログ	—
監査証跡 Workspace	
監査証跡ワークスペースにアクセス	Audit Trail Manager：**View Audit Trail Data**
アクティブな監査マップを表示	Audit Trail Manager：**View Audit Trail Data**

[3] バージョン 3.1 では、**中央管理の有効化** 権限の名前が **CAC** に変更されました。構成 ワークスペースの CAC ページを使用して、SCIEX OS ソフトウェアの中央管理を構成できます。

表 D-1：権限のマッピング (続き)

SCIEX OS ソフトウェア	Analyst ソフトウェア
監査証跡の印刷/エクスポート	Audit Trail Manager：**View Audit Trail Data**
データ取得パネル	
開始	—
停止	—
保存	—
MS メソッド および LC メソッド Workspaces	
アクセスメソッドワークスペース	—
新規	取得メソッド：**Create/Save acquisition method**
開く	取得メソッド：**取得メソッドを読み取り専用として開く（取得モード）**
保存	取得メソッド：**Overwrite acquisition methods**、**Create/Save acquisition method**
別名で保存	取得メソッド：**Overwrite acquisition methods**、**Create/Save acquisition method**
メソッドのロック/ロック解除	—
測定メソッドの上書き	測定メソッドの上書き
キュー Workspace	
管理	サンプルキュー：**Reacquire**、**Delete Sample or Batch**、**Move Batch**
開始/停止	サンプルキュー：**Start Sample**、**Stop Sample**、**Abort Sample**、**Stop Queue**
印刷	レポートテンプレートエディタ：**Print**
サンプルの編集	—
ライブラリ Workspace	
ライブラリワークスペースへのアクセス	Explore：**Setup library location**、**Setup library user options**、**Add library record**、**Add spectrum to library**、**Modify library record (overrides add/delete if disabled)**、**Delete MS spectrum**、**Delete UV spectrum**、**Delete structure**、**View library**、**Search library**
MS チューン Workspace	

表 D-1：権限のマッピング (続き)

SCIEX OS ソフトウェア	Analyst ソフトウェア
MS チューンワークスペースへのアクセス	—
高度な MS チューニング	チューニング：**Instrument Optimization**、**Manual Tune**、**Edit Tuning Options**
高度なトラブルシューティング	—
クイックステータスチェック	チューニング：**Instrument Opt**
装置データの復元	チューニング：**Edit Tuning Options**、**Edit instrument data**
アナリティクス Workspace	
新しい結果	定量化：**Create new results tables**
処理メソッドを作成	定量化：**Create quantitation methods**
処理メソッドの変更	定量化：**Modify existing methods**
ロック解除された定量テーブルのエクスポートとレポートの作成を許可	—
自動化バッチの結果を保存	—
デフォルトの定量化メソッド積分アルゴリズムを変更	定量化：**Change default method options**
デフォルトの定量化メソッド積分パラメータを変更	定量化：**Change default method options**
プロジェクトのピーク修正警告の有効化	—
サンプルを追加	定量化：**Add and Remove samples from results table**
選択したサンプルを削除	定量化：**Add and Remove samples from results table**
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	—
サンプル名の変更	定量化：**Modify sample name**
サンプルタイプの変更	定量化：**Modify Sample Type**
サンプル ID の変更	定量化：**Modify Sample ID**
実際の濃度の修正	定量化：**Modify Analyte Concentration**
希釈係数の修正	定量化：**Modify Dilution Factor**
コメントフィールドの修正	定量化：**Modify Sample Comment**
手動積分を有効化	定量化：**Manually integrate**

表 D-1：権限のマッピング (続き)

SCIEX OS ソフトウェア	Analyst ソフトウェア
ピークを不検出に設定	—
定量テーブルにピークを含めるまたはそこから除外	定量化：**Exclude standards from calibration**
回帰オプション	定量化：**Change regression parameters**
単一のクロマトグラムの定量テーブル積分パラメータを変更	定量化：**Change "simple" parameters in peak review**、**Change "advanced" parameters in peak review**
定量テーブルの成分の定量化メソッドを変更	定量化：**Edit results tables' method**
メトリックプロットの新しい設定の作成	定量化：**Modify or create metric plot settings**
カスタム列を追加	定量化：**Create or modify formula columns**
ピークレビュータイトルのフォーマットの設定	—
カスタム列を削除	定量化：**Create or modify formula columns**
定量テーブルの表示設定	定量化：**Change results table column precision**、**Change results table column visibility**、**Modify results table settings**
定量テーブルのロック	—
定量テーブルのロック解除	—
結果ファイルをレビュー済みとしてマークして保存	—
レポートテンプレートを変更	レポートテンプレートエディタ：**Create/Modify report templates**
結果を LIMS に転送	—
バーコード列を変更	—
比較サンプルの割り当てを変更	—
MSMS スペクトルをライブラリに追加	Explore：**Add spectrum to library record**
プロジェクトのデフォルト設定	定量化：**Modify global (default) settings**
すべての形式でレポートを作成	—
フラグ設定基準パラメータの編集	—
自動外れ値除外パラメータの変更	—
自動外れ値除外の有効化	—
FF/LS による処理メソッドの更新	—

表 D-1：権限のマッピング (続き)

SCIEX OS ソフトウェア	Analyst ソフトウェア
FF/LS による結果を更新	—
付加物機能によるグループ化の有効化	定量化：**Create Analyte Groups**、**Modify Analyte Groups**
ファイルを参照	—
標準追加の有効化	—
手動積分パーセントルールの設定	定量化：**Enable or Disable percent rule in Manual Integration**
重量/容量の変更	定量化：**Modify Weight To Volume ratio**
定量テーブルを上書き	保存時に既存の結果表を置き換え
結果ファイルを承認済みとしてマークして保存	—
中央モニタリング Workspace	
キュータブへのアクセス	—
キューの印刷	—
開始/停止キュー	—
エクスプローラ Workspace	
エクスプローラワークスペースへのアクセス	—
エクスポート	Explore：**Save data to text file**
印刷	レポートテンプレートエディタ：**Print**
オプション	—
再キャリブレーション	Tune：**Calibrate from current spectrum**
ファイルを参照	—

データファイルのチェックサム E

wiff ファイルにはデータファイルチェックサムを使用することをお勧めします。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。

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。

注: ユーザーは、Analyst ソフトウェアを使用してチェックサムを確認できます。Analyst ソフトウェアドキュメントを参照してください。

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

1. 構成ワークスペースを開きます。
2. **プロジェクト**をクリックします。
3. 必要に応じて、**データファイルのセキュリティ**を展開します。
4. データファイルのチェックサム機能を有効にするには、**wiff データ作成のチェックサム書き込みの有効化**チェックボックスを選択します。この機能を無効にするには、このチェックボックスをオフにします。

お問い合わせ先

住所

シンガポール製
AB Sciex Pte.Ltd.
Blk33, #04-06 Marsiling Industrial Estate Road 3
Woodlands Central Industrial Estate, Singapore 739256

SCIEX 本社

AB Sciex LLC
500 Old Connecticut Path
Framingham, Massachusetts 01701
USA

お客様のトレーニング

- グローバル: sciex.com/contact-us

オンライン学習センター

- SCIEX Now Learning Hub

SCIEX サポート

SCIEX およびその代理店には、十分な訓練を受けた保守 / 技術専門のグローバルスタッフがおり、システムに関する質問や技術的な問題にお答えします。詳細については、SCIEX の Web サイト sciex.com をご覧いただくか、以下のリンクから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。

説明書

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

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、次にアクセスしてください https://get.adobe.com/reader。

ソフトウェア製品の説明書については、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説明書については、システムまたはコンポーネントに付属の説明書を参照してください。

説明書の最新版は SCIEX の web サイト（sciex.com/customer-documents）で入手できます。

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。