SCIEX OS ソフトウェア

ラボ管理者ガイド

RUO-IDV-05-7370-JA-I

2022 年 6 月

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

目次

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 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、SCIEX OS インストール前に Windows の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 では、以下の機能を提供します。

- 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 セキュリティーにリンクする容易なセキュリティー管理。

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 および Windows のセキュリティ: 互いに連動

SCIEX OS と Windows の新テクノロジファイルシステム（NTFS）には、システムとデータ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 には、以下の安全なシステムアクセスモードが用意されています。

- 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：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：SCIEX OS へのアクセスの設定。

SCIEX OS および Windows 内の監査証跡

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テーブル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には、役割の削除と SCIEX OS 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 Results Table に埋め込まれた処理メソッドの作成と変更。

注: SCIEX OS は、MS メソッド、LC メソッド、バッチ、または処理メソッドの作成または変更を監査しません。これらのファイルはテンプレートとして機能します。パラメータ値は、取得または処理時にそれらから読み取られ、タスクに適用されます。MS メソッド、LC メソッド、およびバッチの場合、パラメータ値は wiff ファイルと wiff2 ファイルに記録されます。処理メソッドについては、qsession ファイルに記録されます。これらのファイルは、この情報の電子記録として機能します。

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 では 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 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。
- 装置の稼働、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。

SCIEX OS は、21 CFR Part 11 準拠システムの一部として使用されるよう設計されており、21 CFR Part 11 の遵守をサポートするよう構成することができます。SCIEX OS の使用が 21 CFR Part 11 に準拠しているかどうかは、ラボでの SCIEX OS 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。

注: 検証済みのシステムに Instrument Parameters 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 ソフトウェアから SCIEX OS に初めて転送するためのものです。使用後は Instrument Parameters 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

このシステムでは、ローカルの Windows ユーザーアカウントに対して次の制限を実施しています。

- 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、**admin**、**administrator**、または **demo** であってはなりません。

SCIEX OS 管理者には、SCIEX OS の Data フォルダのファイルに対する変更権限が必要です。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つようにするために、ネットワーク管理者は、ネットワークリソースに安全ネットワークアカウント（SNA）を定義することができます。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。

ユーザーとグループ

SCIEX OS 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 へのアクセスの設定。

Active Directory への対応

SCIEX OS 構成ワークスペースでユーザーを追加するには、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 7、64 ビットクライアント
- Windows 10、64 ビットクライアント

Windows ファイルシステム

SCIEX OS 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。この形式では、SCIEX OS ファイルへのアクセスを制御し、監査することが可能です。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。

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 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。

SCIEX OS 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：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 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)ソフトウェアの場合、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:

- 構成ワークスペースで、SCIEX OS ウィンドウの **Licenses** 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。

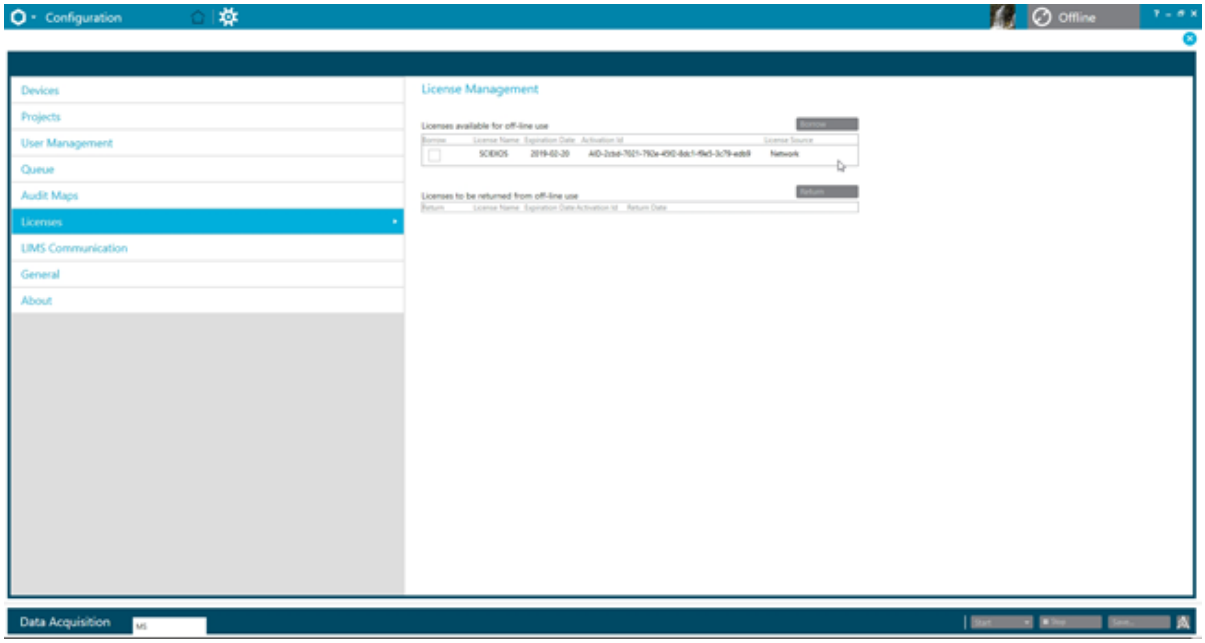
サーバーベースの電子ライセンスの借用

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. Configuration ワークスペースを開きます。
2. **Licenses** をクリックします。
   Licenses available for off-line use 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



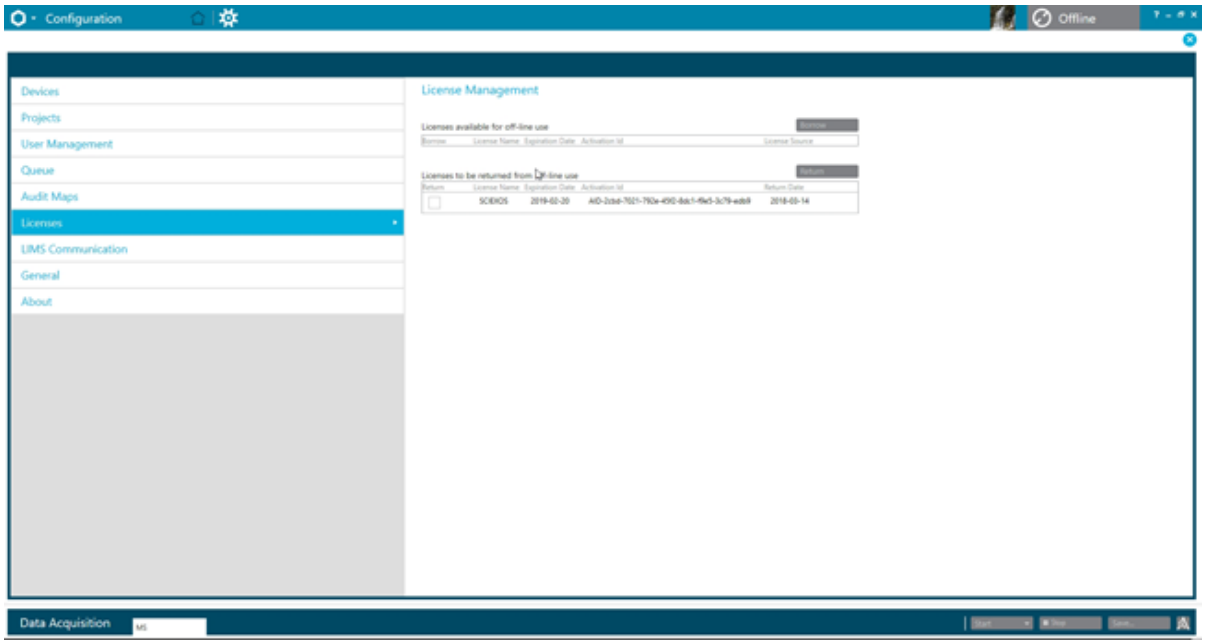
3. 借用するライセンスを選択し、**Borrow** をクリックします。

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. Configuration ワークスペースを開きます。
2. **Licenses** をクリックします。
   Licenses to be returned from off-line use 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、**Return** 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 へのアクセスを制御する方法について説明します。SCIEX OS 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 をインストールして構成します。
- ユーザーおよび権限を追加し、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 のローカル管理について説明します。SCIEX OS 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` フォルダー内にある `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 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:SCIEX OS を開く機能。
- SCIEX OS 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
SCIEX OS をインストールします。	*SCIEX OS Software Installation Guide* のドキュメント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 へのアクセスを構成します。	次のセクションを参照：SCIEX OS へのアクセスの設定。
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：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。

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）。	Yes
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。	Yes
ファイルアクセス権限を設定します（認証）。	Yes
SCIEX OS のインストール	
SCIEX OS をインストールします。	Yes
イベントビューアを開いて、インストールを確認します。	Yes
ソフトウェアのセキュリティ	
Security Mode を選択します。	Yes
SCIEX OS のユーザーと役割を構成します。	Yes
メール通知の構成。	Yes
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。	Yes
wiff ファイルのチェックサム機能を有効にします。	Yes
共通タスク	
新しいプロジェクトを追加します。	Yes

SCIEX OS のインストール

SCIEX OS 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。

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テンプレート。インストール後、SCIEX OS 管理者はカスタム監査マップを作成し、Configuration ワークスペースで異なる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、Configuration ワークスペースの User Management ページにある Security Mode 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 にアクセスできます。

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、そのユーザーはソフトウェアにアクセスできます。

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、 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 Results Table 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 で管理できません。

Security Mode を選択する

1. Configuration ワークスペースを開きます。
2. **User Management** をクリックします。
3. **Security Mode** タブをクリックします。

4. **Integrated Mode** または **Mixed Mode** 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. **Save** 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. Configuration ワークスペースを開きます。
2. **User Management** をクリックします。
3. Security Mode 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. **Screen Lock** を選択します。
   b. **Wait** 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. **Auto Logoff** を選択します。
   b. **Wait** 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. **Save** 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. Configuration ワークスペースを開きます。
2. **User Management** をクリックします。
3. Security Mode タブを開きます。
4. **Send e-mail messages after** 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、**Send e-mail messages after** チェックボックスをオフにします。

5. **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 サーバーは、社内メールアプリケーションで定義されています。

6. **Port Number** をクリックして、開いているポート番号を入力します。
   Apply Default 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. **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.
8. **From** フィールドに、メッセージの **From** 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. **Subject** フィールドに、メッセージの件名を入力します。
10. **Message** 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. **Save** 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、**Send Test Mail** をクリックします。

SCIEX OS へのアクセスの設定

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

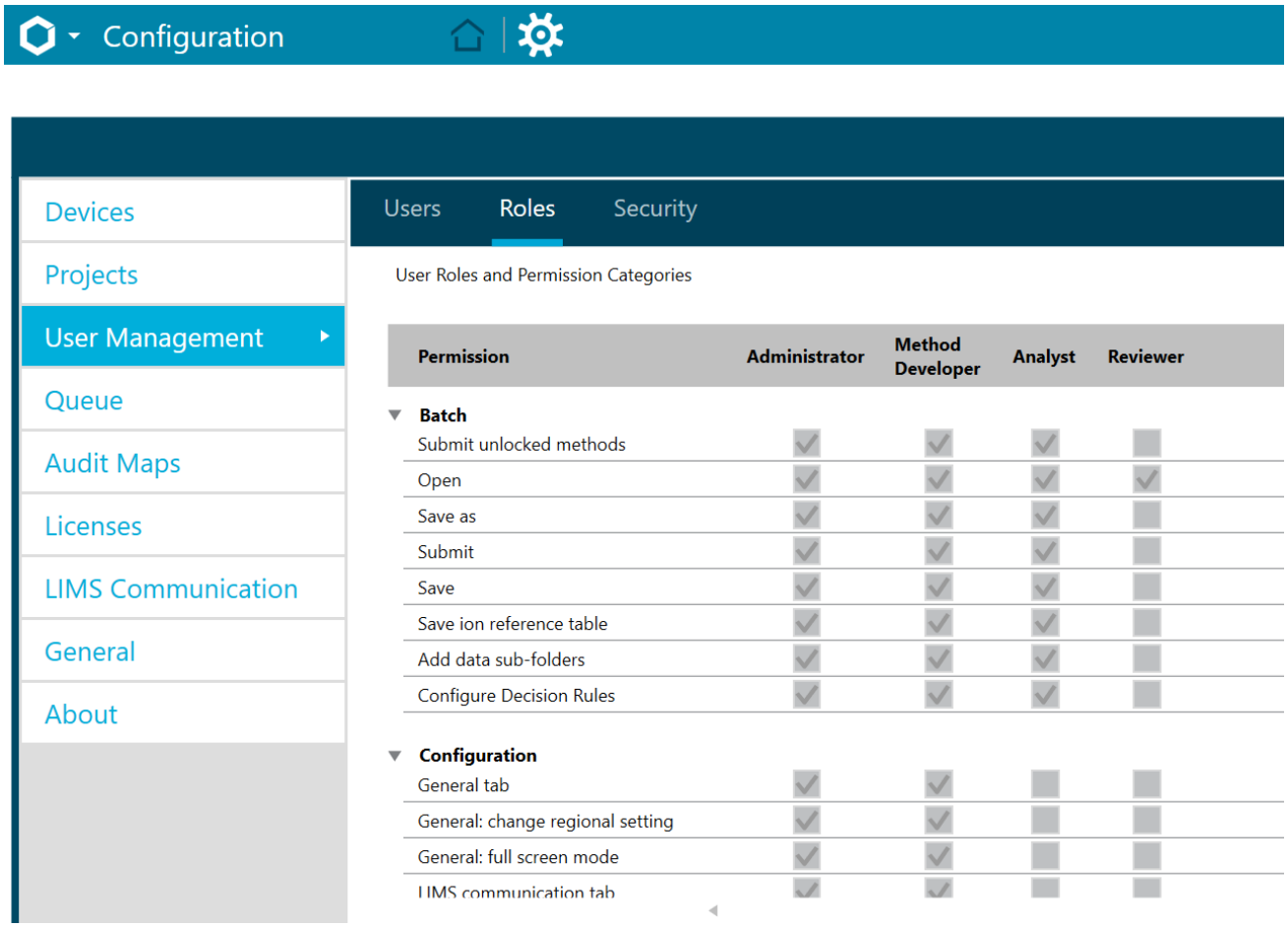


表 4-3：許可

権限	説明
Batch（バッチ）	

表 4-3：許可 (続き)

権限	説明
Submit unlocked methods	(ロック解除されたメソッドを送信)ロックされていないメソッドを含むバッチを送信する許可を与えます。
Open	(開く)既存のバッチを開く許可を与えます。
Save as	(名前を付けて保存)バッチを新しい名前で保存する許可を与えます。
Submit	(送信)バッチを送信する許可を与えます。
Save	(保存)バッチを保存し、既存のコンテンツを上書きする許可をユーザーに与えます。
Save ion reference table	(イオン参照表の保存)イオン参照表を編集できるようにします。
Add data sub-folders	(データサブフォルダの追加)データを格納するサブフォルダを作成できるようにします。
Configure Decision Rules	(決定ルールの構成)ユーザーが決定ルールを追加および変更できるようにします。
Configuration(構成)	
General tab	(全般タブ)Configuration ワークスペースの General ページを開くことができます。
General: change regional setting	(全般: 地域設定の変更)ユーザーが現在のシステム地域設定を SCIEX OS に適用できるようにします。
General: full screen mode	(全般: 全画面モード)全画面モードを有効または無効にできます。
General: Stop Windows services	(一般: Windows サービスの停止)**Windows Settings** オプションを有効または無効にできます。
LIMS communication tab	(LIMS 通信タブ)Configuration ワークスペースの LIMS Communication ページを開くことができます。
Audit maps tab	(監査マップタブ)Configuration ワークスペースの Audit Maps ページを開くことができます。
Queue tab	(キュータブ)Configuration ワークスペースの Queue ページを開くことができます。
Queue: instrument idle time	(キュー: 装置のアイドル時間)装置のアイドル時間を設定できるようにします。
Queue: max number of acquired samples	(キュー: 測定サンプルの最大数)ユーザーが許可される測定サンプルの最大数を設定できます。
Queue: other queue settings	(キュー: 他のキュー設定)他のキュー設定を構成できるようにします。

表 4-3：許可 (続き)

権限	説明
Projects tab	(プロジェクトタブ)Configuration ワークスペースの Projects ページを開くことができます。
Projects: create project	(プロジェクト: プロジェクトの作成)プロジェクトを作成できるようにします。
Projects: apply an audit map template to an existing 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)監査マップをプロジェクトに適用できるようにします。
Projects: create root directory	(プロジェクト: ルートディレクトリの作成)プロジェクトを格納するルートディレクトリを作成できます。
Projects: set current root directory	(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できるようにします。
Projects: specify network credentials	(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、ネットワーク取得中に使用する安全なネットワークアカウント(SNA)を指定できるようにします。
Projects: Enable checksum writing for wiff data creation	(プロジェクト: wiff データ作成のチェックサム書き込みを有効にする)ユーザーがチェックサムを wiff 日付ファイルに書き込むようにソフトウェアを構成できるようにします。
Projects: clear root directory	(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できます。
Devices tab	(デバイスタブ)Configuration ワークスペースの Devices ページを開くことができます。
User management tab	(ユーザー管理タブ)Configuration ワークスペースの User Management ページを開くことができます。
Force user logoff	(ユーザーの強制ログオフ)現在 SCIEX OS にログオンしているユーザーを強制的にログオフできるようにします。現在 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できるようにします。
Event Log(イベントログ)	
Access event log workspace	(イベントログワークスペースへのアクセス)Event Log ワークスペースを開くことができます。
Archive log	(ログのアーカイブ)ユーザーがイベントログをアーカイブできるようにします。
Audit Trail(監査証跡)	
Access audit trail workspace	(監査証跡ワークスペースにアクセス)ユーザーは Audit Trail ワークスペースを開くことができます。

表 4-3：許可 (続き)

権限	説明
View active audit map	(アクティブな監査マップを表示)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監査証跡ワークスペースに表示できます。
Print/Export audit trail	(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できるようにします。
CAC Server(CAC サーバー)(CAC のみ)	
Manage Workgroups	(ワークグループの管理)ユーザー管理ワークスペースでワークグループを作成および管理できます。
Manage Workgroups Projects	(ワークグループの管理)ユーザー管理ワークスペースでワークグループ プロジェクトを作成および管理できます。
Data Acquisition Panel(データ取得パネル)	
Start	(開始)ユーザーが Data Acquisition パネルで取得を開始できるようにします。
Stop	(停止)ユーザーが Data Acquisition パネルで取得を停止できるようにします。
Save	(保存)取得したデータを別のファイル名で Data Acquisition パネルに保存できます。
MS & LC Method(MS および LC メソッド)	
Access method workspace	(アクセスメソッドワークスペース)MS Method および LC Method ワークスペースを開くことができます。
New	(新規)MS および LC メソッドを作成できるようにします。
Open	(開く)ユーザーが MS および LC メソッドを開くことができます。
Save	(保存)メソッドを保存して、既存のコンテンツを上書きできるようにします。
Save as	(名前を付けて保存)メソッドを新しい名前で保存できます。
Lock/Unlock method	(メソッドのロック/ロック解除)メソッドをロックし、編集を防止し、メソッドをロック解除できるようにします。
Queue(キュー)	
Manage	(管理)Queue ワークスペースを開くことを許可します。
Start/Stop	(開始/停止)キューを開始または停止できるようにします。
Print	(印刷)キューを印刷できるようにします。
Library(ライブラリ)	
Access library workspace	(ライブラリワークスペースへのアクセス)Library ワークスペースを開くことができます。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
CAC settings（CAC クライアント）	
Enable Central Administration	（中央管理を有効にする）Central Administrator Console (CAC)ソフトウェアを使用して中央管理に SCIEX OS を構成できます。
MS Tune（MS チューン）	
Access MS Tune workspace	（MS チューンワークスペースにアクセス）MS Tune ワークスペースを開くことができます。
Advanced MS tuning	（高度な MS チューニング）（X500 QTOF システム）Detector Optimization、Positive and Negative Q1 Unit Tuning、Positive and Negative TOF MS Tuning、Positive and Negative Q1 High Tuning など、高度なチューニングオプションにアクセスできます。
Advanced troubleshooting	（詳細設定トラブルシューティング）Advanced Troubleshooting ダイアログを開くことができます。
Quick status check	（クイック状態チェック）（X500 QTOF システム）ポジティブおよびネガティブクイック状態チェックを実行できるようにします。
Restore instrument data	（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できます。
Explorer（エクスプローラ）	
Access Explorer workspace	（エクスプローラワークスペースへのアクセス）Explorer ワークスペースを開くことができます。
Export	（エクスポート）Explorer ワークスペースからデータをエクスポートできるようにします。
Print	（印刷）ユーザーが Explorer ワークスペースでデータを印刷できるようにします。
Options	（オプション）ユーザーが Explorer ワークスペースのオプションを変更できるようにします。
Recalibrate	（再キャリブレーション）ユーザーが Explorer ワークスペースでサンプルとスペクトルを再キャリブレーションできるようにします。定量ワークフローには適用されません。
Analytics（分析）	
New results	（新しい結果）ユーザーが Results Table を作成できるようにします。
Create processing method	（処理メソッドの作成）処理メソッドを作成または編集できます。
Modify processing method	（処理メソッドの修正）処理メソッドを変更できます。

表 4-3：許可 (続き)

権限	説明
Allow Export and Create Report of unlocked Results Table	(ロック解除された Results Table のレポートのエクスポートと作成を許可)Results Table がロックされていない場合、ユーザーは Results Table や統計表からレポートをエクスポートまたは生成できます。
Save results for Automation Batch	(自動化バッチの結果を保存)Batch ワークスペースで自動的に作成された Results Table を保存できます。この権限は、取得中の自動処理に必要です。
Change default quantitation method integration algorithm	(デフォルトの定量化メソッド統合アルゴリズムの変更)プロジェクトのデフォルト設定で統合アルゴリズムを変更できるようにします。
Change default quantitation method integration parameters	(デフォルトの定量化メソッド統合パラメータの変更)プロジェクトのデフォルト設定で統合アルゴリズムを変更できるようにします。
Enable project modified peak warning	(プロジェクトの修正されたピーク警告を有効)プロジェクトの修正されたピーク警告プロパティを有効にできます。
Add samples	(サンプルの追加)Results Table にサンプルを追加できるようにします。
Remove selected samples	(選択したサンプルの削除)Results Table からサンプルを削除できるようにします。
Export, import, or remove external calibration	(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、または削除できるようにします。
Modify sample name	(サンプル名の変更)Results Table のサンプル名を変更できます。
Modify sample type	(サンプルタイプの変更)Results Table のサンプルタイプ(標準、品質管理(QC)、不明など)を変更できます。
Modify sample ID	(サンプル ID の変更)Results Table でサンプル ID を変更できます。
Modify actual concentration	(実際の濃度の変更)Results Table の標準および QC サンプルの実際の濃度を変更できます。
Modify dilution factor	(希釈係数の変更)Results Table の希釈係数を変更できます

表 4-3：許可 (続き)

権限	説明
Modify comment fields	(コメントフィールドの変更)コメントフィールドを変更できるようにします。 • 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
Enable manual integration	(手動積分を有効)手動積分を実行できるようにします。
Set peak to Not Found	(ピークを「見つからない」に設定)ピークを **Not Found** に設定できるようにします。
Include or exclude a peak from the Results Table	(Results Table にピークを含めるまたはそこから除外)Results Table にピークを含めたり除外したりできます。
Regression options	(回帰オプション)Calibration Curve ペインの回帰オプションを変更できるようにします。
Modify Results Table integration parameters for a single chromatogram	(単一クロマトグラムの Results Table 積分パラメータの変更)ユーザーは、Peak Review ペインで単一クロマトグラムの積分パラメータを変更できます。
Modify quantitation method for the Results Table component	(Results Table コンポーネントの定量化メソッドの変更)ユーザーは、**Update Processing Method for Component** オプションを使用して、Peak Review ペインでコンポーネントの別の処理メソッドを選択できます。
Create metric plot new settings	(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、設定を変更できるようにします。
Add custom columns	(カスタム列の追加)Results Table にカスタム列を追加できるようにします。
Set peak review title format	(Peak Review タイトル形式の設定)Peak Review タイトルを変更できるようにします。
Remove custom column	(カスタム列の削除)Results Table にカスタム列を削除できるようにします。
Results Table display settings	(Results Table の表示設定)Results Table に表示される列をカスタマイズできるようにします。
Lock Results Table	(Results Table のロック)Results Table をロックして編集できないようにできます。
Unlock Results Table	(Results Table のロック解除)Results Table のロックを解除して編集できるようにします。

表 4-3：許可 (続き)

権限	説明
Mark Results file as reviewed and save	(結果ファイルをレビュー済みとしてマークして保存)Results Table をレビュー済みとしてマークして保存できます。
Modify report template	(レポートテンプレートの変更)レポートテンプレートを変更できるようにします。
Transfer results to LIMS	(結果を LIMS に転送): 結果をラボ情報管理システム(LIMS)にアップロードできるようにします。
Modify barcode column	(バーコード列の変更)Results Table の **Barcode** 列を変更できるようにします。
Change comparison sample assignment	(比較サンプル割り当ての変更)Results Table の **Comparison** 列で指定された比較サンプルを変更できます。
Add the MSMS spectra to library	(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できます。定量ワークフローには適用されません。
Project default settings	(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的および定性的処理設定を変更できるようにします。
Create report in all formats	(すべての形式でレポートを作成する)ユーザーがすべての形式でレポートを生成できるようにします。この権限のないユーザーは、PDF 形式でのみレポートを生成できます。
Edit flagging criteria parameters	(フラグ設定基準パラメータの編集)ユーザーが処理メソッドでフラグ設定パラメータを変更できるようにします。
Automatic outlier removal parameter change	(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できます。
Enable automatic outlier removal	(自動外れ値除外を有効)処理メソッドを変更して自動外れ値除外機能をオンにできます。
Update processing method via FF/LS	(FF/LS による処理メソッドの更新)Formula Finder および Library Search を使用して処理メソッドを更新できます。定量ワークフローには適用されません。
Update results via FF/LS	(FF/LS による結果の更新)Formula Finder および Library Search を使用して結果を更新できるようにします。定量ワークフローには適用されません。
Enable grouping by adducts functionality	(付加機能によるグループ化を有効)処理メソッドを更新して、グループ付加機能をオンにできるようにします。
Browse for files	(ファイルの参照)ローカルデータフォルダ外を参照できるようにします。
Enable standard addition	(標準追加を有効)処理メソッドを更新して標準追加機能をオンにできるようにします。

表 4-3：許可 (続き)

権限	説明
Set Manual Integration Percentage Rule	(手動積分パーセンテージルールの設定)ユーザーが **Manual Integration %**パラメータを変更できるようにします。

ユーザーと役割について

SCIEX OS では、管理者は Windows ユーザーとグループを SCIEX OS のユーザー管理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。役割は、ユーザーがアクセスできる機能を決定します。既定の役割は削除できず、その許可は変更できません。

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、User Management ページは読み取り専用になります。

表 4-4：既定の役割

役割	標準的なタスク
Administrator(管理者)	• システムを管理する。 • セキュリティを構成する。
Method Developer(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。 • エンドユーザーによるデータの使用を分析する。
Analyst(アナリスト)	• バッチを実行する。 • エンドユーザーによるデータの使用を分析する。
Reviewer(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
Batch(バッチ)				
Submit unlocked methods(ロック解除されたメソッドを送信)	✓	✓	✓	×

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
Open（開く）	✓	✓	✓	✓
Save as（名前を付けて保存）	✓	✓	✓	×
Submit（送信）	✓	✓	✓	×
Save（保存）	✓	✓	✓	×
Save ion reference table（イオン参照表の保存）	✓	✓	✓	×
Add data sub-folders（データのサブフォルダを追加）	✓	✓	✓	×
Configure Decision Rules（決定ルールを管理）	✓	✓	✓	×
Configuration（構成）				
General tab（全般タブ）	✓	✓	×	×
General: change regional setting（全般: 地域設定の変更）	✓	✓	×	×
General: full screen mode（全般: 全画面モード）	✓	✓	×	×
General: Stop Windows services（一般: Windows サービスの停止）	✓	×	×	×
LIMS communication tab（LIMS 通信タブ）	✓	✓	×	×
Audit maps tab（監査マップタブ）	✓	×	×	×
Queue tab（キュータブ）	✓	✓	✓	✓
Queue: instrument idle time（キュー: 装置のアイドル時間）	✓	✓	×	×

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
Queue: max number of acquired samples（キュー: 測定サンプルの最大数）	✓	✓	×	×
Queue: other queue settings（キュー: 他のキュー設定）	✓	✓	×	×
Projects tab（プロジェクトタブ）	✓	✓	✓	✓
Projects: create project（プロジェクト: プロジェクトの作成）	✓	✓	✓	×
Projects: apply an audit map template to an existing 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）	✓	×	×	×
Projects: create root directory（プロジェクト: ルートディレクトリの作成）	✓	×	×	×
Projects: set current root directory（プロジェクト: 現在のルートディレクトリの設定）	✓	×	×	×
Projects: specify network credentials（プロジェクト: ネットワーク認証情報の指定）	✓	×	×	×
Projects: Enable checksum writing for wiff1 data creation（プロジェクト: wiff1 データ作成のチェックサム書き込みを有効にする）	✓	×	×	×
Projects: clear root directory（プロジェクト: ルートディレクトリをクリアする）	✓	×	×	×

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
Devices tab（デバイスタブ）	✓	✓	✓	×
User management tab（ユーザー管理タブ）	✓	×	×	×
Force user logoff（ユーザーの強制ログオフ）	✓	×	×	×
Event Log（イベントログ）				
Access event log workspace（イベントログワークスペースへのアクセス）	✓	✓	✓	✓
Archive log（ログのアーカイブ）	✓	✓	✓	✓
Audit Trail（監査証跡）				
Access audit trail workspace（監査証跡ワークスペースへのアクセス）	✓	✓	✓	✓
View active audit map（アクティブな監査マップを表示）	✓	✓	✓	✓
Print/Export audit trail（監査証跡の印刷/エクスポート）	✓	✓	✓	✓
Data Acquisition Panel（データ取得パネル）				
Start（開始）	✓	✓	✓	×
Stop（停止）	✓	✓	✓	×
Save（保存）	✓	✓	✓	×
MS & LC Method（MS および LC メソッド）				
Access method workspace（アクセスメソッドワークスペース）	✓	✓	✓	✓
New（新規）	✓	✓	×	×
Open（開く）	✓	✓	✓	✓

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
Save（保存）	✓	✓	×	×
Save as（名前を付けて保存）	✓	✓	×	×
Lock/Unlock method（メソッドのロック/ロック解除）	✓	✓	×	×
Queue（キュー）				
Manage（管理）	✓	✓	✓	×
Start/Stop（開始/停止）	✓	✓	✓	×
Print（印刷）	✓	✓	✓	✓
Library（ライブラリ）				
Access library workspace（ライブラリワークスペースへのアクセス）	✓	✓	✓	✓
CAC settings（CAC クライアント）				
Enable Central Administration（サーバーの中央管理を有効にする）	✓	×	×	×
MS Tune（MS チューン）				
Access MS Tune workspace（アクセス MS チューンワークスペース）	✓	✓	✓	×
Advanced MS Tuning（高度な MS チューニング）	✓	✓	×	×
Advanced troubleshooting（高度なトラブルシューティング）	✓	✓	×	×
Quick status check（クイック状態チェック）	✓	✓	✓	×

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
Restore instrument data（装置データの復元）	✓	✓	×	×
Explorer（エクスプローラ）				
Access explorer workspace（エクスプローラワークスペースへのアクセス）	✓	✓	✓	✓
Export（エクスポート）	✓	✓	✓	×
Print（印刷）	✓	✓	✓	×
Options（オプション）	✓	✓	✓	×
Recalibrate（再キャリブレーション）	✓	✓	×	×
Analytics（分析）				
New results（新しい結果）	✓	✓	✓	×
Create processing method（処理メソッドの作成）	✓	✓	✓	×
Modify processing method（処理メソッドの変更）	✓	✓	×	×
Allow Export and Create Report of unlocked Results Table（ロック解除された Results Table のレポートのエクスポートと作成を許可）	✓	×	×	×
Save results for Automation Batch（自動化バッチの結果を保存）	✓	✓	✓	×

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
Change default quantitation method integration algorithm（デフォルトの定量化メソッド統合アルゴリズムの変更）	✓	✓	×	×
Change default quantitation method integration parameters（デフォルトの定量化メソッド統合パラメータの変更）	✓	✓	×	×
Enable project modified peak warning（プロジェクトの修正されたピーク警告を有効）	✓	×	×	×
Add samples（サンプルを追加）	✓	✓	✓	×
Remove selected samples（選択したサンプルを削除）	✓	✓	✓	×
Export, import, or remove external calibration（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）	✓	✓	✓	×
Modify sample name（サンプル名の変更）	✓	✓	✓	×
Modify sample type（サンプルタイプの変更）	✓	✓	✓	×
Modify sample ID（サンプル ID の変更）	✓	✓	✓	×
Modify actual concentration（実際の濃度の変更）	✓	✓	✓	×
Modify dilution factor（希釈係数の修正）	✓	✓	✓	×

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
Modify comment fields（コメントフィールドの修正）	✓	✓	✓	×
Enable manual integration（手動積分を有効）	✓	✓	✓	×
Set peak to not found（ピークを「見つからない」に設定）	✓	✓	✓	×
Include or exclude a peak from the results table（Results Table にピークを含めるまたはそこから除外）	✓	✓	✓	×
Regression options（回帰オプション）	✓	✓	✓	×
Modify results table integration parameters for a single chromatogram（単一のクロマトグラムの Results Table 統合パラメータの変更）	✓	✓	✓	×
Modify quantitation method for the results table component（Results Table コンポーネントの定量化メソッドを変更）	✓	✓	✓	×
Create metric plot new settings（メトリックプロットの新しい設定の作成）	✓	✓	✓	✓
Add custom columns（カスタム列の追加）	✓	✓	✓	×
Set peak review title format（peak review タイトルのフォーマットの設定）	✓	×	×	×

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
Remove custom column（カスタム列の削除）	✓	✓	×	×
Results table display settings（Results Table の表示設定）	✓	✓	✓	✓
Lock results table（Results Table のロック）	✓	✓	✓	✓
Unlock results table（Results Table のロック解除）	✓	×	×	×
Mark results file as reviewed and save（結果ファイルをレビュー済みとしてマークして保存）	✓	×	×	✓
Modify report template（レポートテンプレートの変更）	✓	✓	×	×
Transfer results to LIMS（結果を LIMS に転送）	✓	✓	✓	×
Modify barcode column（バーコード列の変更）	✓	✓	×	×
Change comparison sample assignment（比較サンプル割り当ての変更）	✓	✓	×	×
Add the MSMS spectra to library（MSMS スペクトルをライブラリに追加）	✓	✓	×	×
Project default settings（プロジェクトのデフォルト設定）	✓	✓	×	×
Create report in all formats（すべての形式でレポートを作成）	✓	✓	✓	✓

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
Edit flagging criteria parameters（フラグ設定基準パラメータの編集）	✓	✓	✓	×
Automatic outlier removal parameter change（自動外れ値除外パラメータの変更）	✓	✓	×	×
Enable automatic outlier removal（自動外れ値除外を有効）	✓	✓	✓	×
Update processing method via FF/LS（FF/LS による処理メソッドの更新）	✓	✓	×	×
Update results via FF/LS（FF/LS による結果の更新）	✓	✓	×	×
Enable grouping by adducts functionality（付加機能によるグループ化を有効）	✓	✓	×	×
Browse for files（ファイルの参照）	✓	✓	✓	✓
Enable standard addition（標準追加を有効）	✓	✓	✓	×
Set Manual Integration Percentage Rule（手動積分パーセンテージルールの設定）	✓	×	×	×

ユーザーの管理

ユーザーまたはグループを追加

1. Configuration ワークスペースを開きます。
2. User Management ページを開きます。
3. Users タブを開きます。

4. **Add User**()をクリックします。
   Select Users or Groups 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! Select User or Group 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、**Active user or group** チェックボックスをオンにします。
7. **Roles** エリアで 1 つ以上のロールを選択し、**Save** をクリックします。

ユーザーまたはグループの無効化

1. Configuration ワークスペースを開きます。
2. User Management ページを開きます。
3. Users タブを開きます。
4. **User name or group** 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. **Active user or group** 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. **Yes** 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を Windows から削除した場合、そのユーザーは SCIEX OS からも削除されなければなりません。

1. Configuration ワークスペースを開きます。
2. User Management ページを開きます。
3. Users タブを開きます。
4. **User name or group** 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. **Delete** 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. Configuration ワークスペースを開きます。
2. User Management ページを開きます。
3. Users タブを開きます。

4. **User name or group** 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. **Save** をクリックします。

カスタム役割の作成

1. Configuration ワークスペースを開きます。
2. User Management ページを開きます。
3. Roles タブを開きます。
4. **Add Role**（  ）をクリックします。
   Duplicate a User Role ダイアログが開きます。
5. **Existing user role** 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. **Save All Roles** 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. Configuration ワークスペースを開きます。
2. User Management ページを開きます。
3. Roles タブを開きます。
4. **Delete a Role** をクリックします。
   Delete a User Role 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 ユーザー管理データベースは、エクスポートや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、ユーザー管理の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. Configuration ワークスペースを開きます。
2. User Management ページを開きます。
3. **Advanced** > **Export User Management settings** をクリックします。
   Export User Management Settings ダイアログが開きます。
4. **Browse** 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、**Select Folder** をクリックします。
6. **Export** 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. Configuration ワークスペースを開きます。
2. User Management ページを開きます。
3. **Advanced** > **Import User Management settings** をクリックします。
   Import User Management Settings ダイアログが開きます。
4. **Browse** 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、**Open** 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. **Import** 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. Configuration ワークスペースを開きます。
2. User Management ページを開きます。
3. **Advanced** > **Restore previous settings** をクリックします。
   Restore User Management Settings ダイアログが開きます。
4. **Yes** をクリックします。
5. SCIEX OS 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 Method 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。
\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

一般的な SCIEX OS ファイル タイプについては、次を参照：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

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
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	Results Table 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 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	—
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	Results Table を保持。 **注:** SCIEX OS は、SCIEX OS で作成された qsession ファイルのみ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 は、wiff と wiff2 の両方のファイルを生成します。	Data

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
wiff.scan	質量分析装置データファイル	• Optimization • Data
wiff2	SCIEX OS によって生成された質量分析装置データファイル	• 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 インストーラー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

User Management ページを使用して、Windows ユーザーおよびグループを SCIEX OS 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 ロールと権限] セクションでユーザー ロールを追加、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 が Central Administrator Console (CAC)ソフトウェアで管理されている場合は、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て SCIEX OS 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. サーバーの Central Administration ワークスペースを開きます。
2. User Management ページを開きます。
3. User Pool タブを開きます。
4. **Add users to the User Pool**( )をクリックします。
   Select Users or Groups 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. サーバーの Central Administration ワークスペースを開きます。
2. User Management ページを開きます。
3. User Pool 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、**Delete** 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、User Roles and Permissions 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。役割は、ユーザーがアクセスできる機能を決定します。既定の役割は削除できず、その権限は変更できません。

表 5-1：既定の役割

役割	標準的なタスク
Administrator（管理者）	• システムを管理する。 • セキュリティを構成する。
Method Developer（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。 • エンドユーザーによるデータの使用を分析する。
Analyst（アナリスト）	• バッチを実行する。 • エンドユーザーによるデータの使用を分析する。
Reviewer（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
Batch（バッチ）				
Submit unlocked methods（ロック解除されたメソッドを送信）	✓	✓	✓	×
Open（開く）	✓	✓	✓	✓

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
Save as（名前を付けて保存）	✓	✓	✓	×
Submit（送信）	✓	✓	✓	×
Save（保存）	✓	✓	✓	×
Save ion reference table（イオン参照表の保存）	✓	✓	✓	×
Add data sub-folders（データのサブフォルダを追加）	✓	✓	✓	×
Configure Decision Rules（決定ルールを管理）	✓	✓	✓	×
Configuration（構成）				
General tab（全般タブ）	✓	✓	×	×
General: change regional setting（全般: 地域設定の変更）	✓	✓	×	×
General: full screen mode（全般: 全画面モード）	✓	✓	×	×
LIMS communication tab（LIMS 通信タブ）	✓	✓	×	×
General:Stop Windows services（一般: Windows サービスの停止）	✓	×	×	×
Audit maps tab（監査マップタブ）	✓	×	×	×
Queue tab（キュータブ）	✓	✓	✓	✓
Queue: instrument idle time（キュー: 装置のアイドル時間）	✓	✓	×	×

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
Queue: max number of acquired samples（キュー: 測定サンプルの最大数）	✓	✓	×	×
Queue: other queue settings（キュー: 他のキュー設定）	✓	✓	×	×
Projects tab（プロジェクトタブ）	✓	✓	✓	✓
Projects: create project（プロジェクト: プロジェクトの作成）	✓	✓	✓	×
Projects: apply an audit map template to an existing 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）	✓	×	×	×
Projects: create root directory（プロジェクト: ルートディレクトリの作成）	✓	×	×	×
Projects: set current root directory（プロジェクト: 現在のルートディレクトリの設定）	✓	×	×	×
Projects: specify network credentials（プロジェクト: ネットワーク認証情報の指定）	✓	×	×	×
Projects: Enable checksum writing for wiff1 data creation（プロジェクト: wiff1 データ作成のチェックサム書き込みを有効にする）	✓	×	×	×
Projects: clear root directory（プロジェクト: ルートディレクトリをクリアする）	✓	×	×	×

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
Devices tab（デバイスタブ）	✓	✓	✓	×
User management tab（ユーザー管理タブ）	✓	×	×	×
Force user logoff（ユーザーの強制ログオフ）	✓	×	×	×
Event Log（イベントログ）				
Access event log workspace（イベントログワークスペースへのアクセス）	✓	✓	✓	✓
Archive log（ログのアーカイブ）	✓	✓	✓	✓
Audit Trail（監査証跡）				
Access audit trail workspace（監査証跡ワークスペースへのアクセス）	✓	✓	✓	✓
View active audit map（アクティブな監査マップを表示）	✓	✓	✓	✓
Print/Export audit trail（監査証跡の印刷/エクスポート）	✓	✓	✓	✓
Data Acquisition Panel（データ取得パネル）				
Start（開始）	✓	✓	✓	×
Stop（停止）	✓	✓	✓	×
Save（保存）	✓	✓	✓	×
MS & LC Method（MS および LC メソッド）				
Access method workspace（アクセスメソッドワークスペース）	✓	✓	✓	✓
New（新規）	✓	✓	×	×
Open（開く）	✓	✓	✓	✓

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
Save（保存）	✓	✓	×	×
Save as（名前を付けて保存）	✓	✓	×	×
Lock/Unlock method（メソッドのロック/ロック解除）	✓	✓	×	×
Queue（キュー）				
Manage（管理）	✓	✓	✓	×
Start/Stop（開始/停止）	✓	✓	✓	×
Print（印刷）	✓	✓	✓	✓
Library（ライブラリ）				
Access library workspace（ライブラリワークスペースへのアクセス）	✓	✓	✓	✓
CAC settings（CAC クライアント）				
Enable Central Administration（サーバーの中央管理を有効にする）	✓	×	×	×
MS Tune（MS チューン）				
Access MS Tune workspace（アクセス MS チューンワークスペース）	✓	✓	✓	×
Advanced MS Tuning（高度な MS チューニング）	✓	✓	×	×
Advanced troubleshooting（高度なトラブルシューティング）	✓	✓	×	×
Quick status check（クイック状態チェック）	✓	✓	✓	×

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
Restore instrument data（装置データの復元）	✓	✓	×	×
Analytics（分析）				
New results（新しい結果）	✓	✓	✓	×
Create processing method（処理メソッドの作成）	✓	✓	✓	×
Modify processing method（処理メソッドの変更）	✓	✓	×	×
Allow Export and Create Report of unlocked Results Table（ロック解除された Results Table のレポートのエクスポートと作成を許可）	✓	×	×	×
Save results for Automation Batch（自動化バッチの結果を保存）	✓	✓	✓	×
Change default quantitation method integration algorithm（デフォルトの定量化メソッド統合アルゴリズムの変更）	✓	✓	×	×
Change default quantitation method integration parameters（デフォルトの定量化メソッド統合パラメータの変更）	✓	✓	×	×
Enable project modified peak warning（プロジェクトの修正されたピーク警告を有効）	✓	×	×	×

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
Add samples（サンプルを追加）	✓	✓	✓	×
Remove selected samples（選択したサンプルを削除）	✓	✓	✓	×
Export, import, or remove external calibration（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）	✓	✓	✓	×
Modify sample name（サンプル名の変更）	✓	✓	✓	×
Modify sample type（サンプルタイプの変更）	✓	✓	✓	×
Modify sample ID（サンプル ID の変更）	✓	✓	✓	×
Modify actual concentration（実際の濃度の変更）	✓	✓	✓	×
Modify dilution factor（希釈係数の修正）	✓	✓	✓	×
Modify comment fields（コメントフィールドの修正）	✓	✓	✓	×
Enable manual integration（手動積分を有効）	✓	✓	✓	×
Set peak to not found（ピークを「見つからない」に設定）	✓	✓	✓	×
Include or exclude a peak from the results table（Results Table にピークを含めるまたはそこから除外）	✓	✓	✓	×
Regression options（回帰オプション）	✓	✓	✓	×

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
Modify results table integration parameters for a single chromatogram（単一のクロマトグラムの Results Table 統合パラメータの変更）	✓	✓	✓	×
Modify quantitation method for the results table component（Results Table コンポーネントの定量化メソッドを変更）	✓	✓	✓	×
Create metric plot new settings（メトリックプロットの新しい設定の作成）	✓	✓	✓	✓
Add custom columns（カスタム列の追加）	✓	✓	✓	×
Set peak review title format（peak review タイトルのフォーマットの設定）	✓	×	×	×
Remove custom column（カスタム列の削除）	✓	✓	×	×
Results table display settings（Results Table の表示設定）	✓	✓	✓	✓
Lock results table（Results Table のロック）	✓	✓	✓	✓
Unlock results table（Results Table のロック解除）	✓	×	×	×
Mark results file as reviewed and save（結果ファイルをレビュー済みとしてマークして保存）	✓	×	×	✓

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
Modify report template（レポートテンプレートの変更）	✓	✓	×	×
Transfer results to LIMS（結果を LIMS に転送）	✓	✓	✓	×
Modify barcode column（バーコード列の変更）	✓	✓	×	×
Change comparison sample assignment（比較サンプル割り当ての変更）	✓	✓	×	×
Add the MSMS spectra to library（MSMS スペクトルをライブラリに追加）	✓	✓	×	×
Project default settings（プロジェクトのデフォルト設定）	✓	✓	×	×
Create report in all formats（すべての形式でレポートを作成）	✓	✓	✓	✓
Edit flagging criteria parameters（フラグ設定基準パラメータの編集）	✓	✓	✓	×
Automatic outlier removal parameter change（自動外れ値除外パラメータの変更）	✓	✓	×	×
Enable automatic outlier removal（自動外れ値除外を有効）	✓	✓	✓	×
Update processing method via FF/LS（FF/LS による処理メソッドの更新）	✓	✓	×	×

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
Update results via FF/LS（FF/LS による結果の更新）	✓	✓	×	×
Enable grouping by adducts functionality（付加機能によるグループ化を有効）	✓	✓	×	×
Browse for files（ファイルの参照）	✓	✓	✓	✓
Enable standard addition（標準追加を有効）	✓	✓	✓	×
Set Manual Integration Percentage Rule（手動積分パーセンテージルールの設定）	✓	×	×	×
Explorer（エクスプローラ）				
Access explorer workspace（エクスプローラワークスペースへのアクセス）	✓	✓	✓	✓
Export（エクスポート）	✓	✓	✓	×
Print（印刷）	✓	✓	✓	×
Options（オプション）	✓	✓	✓	×
Recalibrate（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. サーバーの Central Administration ワークスペースを開きます。
2. User Management ページを開きます。
3. User Roles and Permissions タブを開きます。

4. **Add Role**（  ）をクリックします。
   Duplicate a User Role ダイアログが開きます。
5. **Existing user role** 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 User Roles and Permission Categories 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. **Save All Roles** をクリックします。

カスタム役割の削除

1. サーバーの Central Administration ワークスペースを開きます。
2. User Management ページを開きます。
3. User Roles and Permissions タブを開きます。
4. **Delete a Role** をクリックします。
   Delete a User Role 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

Workgroup Management 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セキュリティモード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、ワークグループのセキュリティモード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でサーバーベースのセキュリティが不要になった場合は、SCIEX OS。

ワークグループを作成する

1. サーバーの Central Administration ワークスペースを開きます。
2. Workgroup Management ページを開きます。
3. **Add Workgroup**()をクリックします。
   Add a Workgroup ダイアログが開きます。
4. **Workgroup Name** フィールドに名前を入力します。
5. **Description** フィールドに説明を入力して、**Add** をクリックします。
   ワークグループが作成され、Manage Workgroups and Assignments 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. サーバーの Central Administration ワークスペースを開きます。
2. Workgroup Management ページを開きます。
3. **Workgroups** リストを展開し、削除するワークグループを見つけます。**Delete** をクリックします。
   Create Workgroup ダイアログが開きます。
4. **Yes** 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. サーバーの Central Administration ワークスペースを開きます。
2. Workgroup Management ページを開きます。
3. Manage Workgroups and Assignments ウィンドウで、変更するワークグループを展開し、**Users** 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、**Add**()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. **Save** 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. サーバーの Central Administration ワークスペースを開きます。
2. Workgroup Management ページを開きます。
3. Manage Workgroups and Assignments ウィンドウで、変更するワークグループを展開し、**Users** リストを展開します。
4. Current Workgroup Membership セクションで、**Assign Roles** 列のロールを割り当てるか削除します。
5. **Save** 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. サーバーの Central Administration ワークスペースを開きます。
2. Workgroup Management ページを開きます。
3. Manage Workgroups and Assignments ウィンドウで、変更するワークグループを展開し、**Workstations** 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、**Add**(>)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. **Save** 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. サーバーの Central Administration ワークスペースを開きます。
2. Workgroup Management ページを開きます。
3. Manage Workgroups and Assignments ウィンドウで、変更するワークグループを展開し、**Workstations** 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、Current Workgroup Membership セクションで **Set Default** チェック ボックスをオンにします。
5. Assign Security Settings セクションで、ワークグループの **Security mode** を選択し、適切な **Screen lock** と **Auto logoff** の時間を入力します。
6. **Save** 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. サーバーの Central Administration ワークスペースを開きます。
2. Workgroup Management ページを開きます。
3. Manage Workgroups and Assignments ウィンドウで、変更するワークグループを展開し、**Projects** リストを展開します。
4. **Use central settings for projects** 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. **Project root directory** 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. **Add**(>)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 Current Workgroup Membership 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. **Save** 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、Project Root Pool 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、Project Root Pool 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. サーバーの Central Administration ワークスペースを開きます。
2. Project Management ページを開きます。
3. **Add new or existing project root to project pool**( )をクリックします。
   Add Root Directory 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、**Browse** 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: 処理ライセンスのある SCIEX OS インストールの場合、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. サーバーの Central Administration 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、Actions セクションで **Delete Project Root** 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. サーバーの Central Administration 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 Actions セクションで **Add project** をクリックします。
   New Project 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. サーバーの Central Administration 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 Actions セクションで **Add data sub-folders** をクリックします。
   Add Data Subfolders 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. **Add a new data sub-folder**()をクリックします。
   Data Sub-Folder Name 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. **Save** 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、Project Data Sub-Folders セクションで既存のサブフォルダを選択し、**Add a new data sub-folder**()をクリックします。
8. Add Data Sub-Folders ダイアログを閉じます。

ワークステーション

Workstation Management ページを使用して、CAC サーバー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

Workstation Management ページで、管理者は Central Administrator Console (CAC)ソフトウェアの制御下にあるワークステーションを追加または削除できます。

1. サーバーの Central Administration ワークスペースを開きます。
2. Workstation Management ページを開きます。
3. **Add Workstation to the Workstations Pool**()をクリックします。
   Select Computers 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や、ワークグループで不要となった場合は、これ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を削除すると、そのワークステーションが割り当てられていたすべてのワークグループから削除されます。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. サーバーの Central Administration ワークスペースを開きます。
2. Workstation Management ページを開きます。
3. **Workstation Management** をクリックします。
4. Workstation Pool 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 **Delete** をクリックします。
   Delete Workstation 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

ワークグループ データ レポートの生成

ユーザーは、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、ワークグループなどの詳細を含むデータ レポートを生成できます。

1. サーバーの Central Administration ワークスペースを開きます。
2. **Print** をクリックします。
   Print ダイアログが開きます。
3. 印刷オプションを設定し、**Print** をクリックします。
4. （PDF への印刷のみ）レポートが保存される場所を参照し、**Save** をクリックします。

CAC ソフトウェアのエクスポート

ユーザーは、別の Central Administrator Console (CAC)サーバーに適用できるセキュリティ設定をエクスポートできます。設定は、ecac ファイルとしてエクスポートされます。

1. サーバーの Central Administration ワークスペースを開きます。
2. **Advanced** > **Export CAC settings** をクリックします。
   Export CAC Settings ダイアログが開きます。
3. **Browse** 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、**Select Folder** をクリックします。
5. **Export** 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 設定のインポート

実施前提手順
• CAC ソフトウェアのエクスポート

ユーザーは、SCIEX OS または他の Central Administrator Console (CAC)サーバーからセキュリティ設定をインポートできます。設定は、ecac ファイルからインポートされます。

1. サーバーの Central Administration ワークスペースを開きます。
2. **Advanced** > **Import CAC settings** をクリックします。
   Import CAC Settings ダイアログが開きます。
3. **Browse** 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、**Open** 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. **Import** 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。

CAC ソフトウェア設定の復元

ユーザーは、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できます。

1. サーバーの Central Administration ワークスペースを開きます。
2. **Advanced** > **Restore CAC settings** をクリックします。
   Restore CAC Settings 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. **Yes** 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、SCIEX OS でのネットワーク取得の仕組みと、ネットワークベースのプロジェクトの利点と制限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収集は、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。しかし、このフォルダへのアクセス権がないと、SCIEX OS は最適なパフォーマンスを発揮できません。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、次を完全に制御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 OSUser Management データベースに登録します。

SNA は、Configuration ワークスペースの Projects 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 は現在ログオンしているユーザーの認証情報を使用して、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 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ーは、SCIEX OS のデータ保存先のフォルダです。プロジェクト情報が安全に保存されるよう、SCIEX OS を使用して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、**Credentials for Secure Network Account** 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、*SCIEX OS『ソフトウェアユーザーガイド』*のドキュメントを参照してください。

安全なネットアカウントの指定

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. Configuration ワークスペースを開きます。
2. **Projects** をクリックします。
3. **Advanced** セクションの **Credentials for Secure Network Account** 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

監査済みイベントは監査証跡に格納されます。監査証跡には、ワークステーションとプロジェクトの 2 種類があります。

ワークステーションの監査証跡は、SCIEX OS または Central Administrator Console (CAC)ソフトウェアが実行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。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: ワークステーション監査証跡。

プロジェクト監査証跡は、プロジェクトの監査済みイベントを保存するファイルです。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: プロジェクト監査証跡。SCIEX OS および CAC ソフトウェアでは、Audit Trail ワークスペースに、現在のルート ディレクトリにあるプロジェクトの監査証跡が表示されます。監査証跡イベントの処理は、プロジェクト監査証跡マップに含まれており、Results Table とともに保管されます。

監査証跡は、wiff2 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：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

Workstation（CAC）	• 以下のように変更:
	  • 監査マップ
	  • CAC サーバー
	  • 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	• Configuration ワークスペースの Audit Maps ページで指定

ワークステーションの監査証跡またはプロジェクトの監査証跡に 20,000 の監査レコードが含まれると、SCIEX OS と 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。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。

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。

ワークステーション監査マップやプロジェクト監査マップを多数作成できますが、1 台のワークステーションや 1 つのプロジェクトで一度に使用できるのは 1 つの監査マップに限られています。ワークステーションやプロジェクトで使用される監査マップは、アクティブ監査マップと呼ばれます。

SCIEX OS をインストールすると、すべての新規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]になります。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監査証跡に 1 つの適切な監査マップが使用可能であり、プロジェクトごとに 1 つの適切な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
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。	• 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。
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。	• ワークステーションのアクティブ監査マップの変更。
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
Example Audit Map	選択されたイベントが監査されます。例示目的のみ。
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。 **注: Change Active Audit Map Assignment** 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。

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
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: 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. Configuration ワークスペースを開きます。
2. **Audit Maps** をクリックします。
3. Projects Templates タブを開きます。
4. **Edit map template** 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. **Add Template**（  ）をクリックします。
   Add a Project Audit Map Template 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 **Audited** 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、**Reason Required** を選択します。
   c. （オプション）電子署名が必要な場合は、**E-Sig Required** 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、**Use Predefined Reason Only** 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、**Audited** 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. **Save Template** 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、**Yes** 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、**Apply** 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、**No** 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、**Use as Default for New Projects** 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. Configuration ワークスペースを開きます。
2. **Audit Maps** をクリックします。
3. Projects Templates タブを開きます。
4. **Edit map template** 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 **Audited** 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、**Reason Required** を選択します。
    c. （オプション）電子署名が必要な場合は、**E-Sig Required** 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、**Use Predefined Reason Only** 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、**Audited** 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. **Save Template** 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、**Yes** 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、**Apply** 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、**No** 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. Configuration ワークスペースを開きます。
2. **Audit Maps** をクリックします。
3. Projects Templates タブを開きます。
4. **Edit map template** 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. **Apply to Existing Projects** をクリックします。
   Apply Project Audit Map Template 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. **Apply** 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. Configuration ワークスペースを開きます。
2. **Audit Maps** をクリックします。
3. Projects Templates タブを開きます。
4. **Edit map template** フィールドで、削除するマップを選択します。
5. **Delete Template** 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. **Yes** 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. Configuration ワークスペースを開きます。
2. **Audit Maps** をクリックします。
3. Workstation Templates タブを開きます。
4. **Edit map template** 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. **Add Template**( )をクリックします。
   Add a Workstation Audit Map Template 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 **Audited** 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、**Reason Required** を選択します。

c. （オプション）電子署名が必要な場合は、**E-Sig Required** 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、**Use Predefined Reason Only** 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、**Audited** 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. **Save Template** 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、**Apply to the Workstation** 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. Configuration ワークスペースを開きます。
2. **Audit Maps** をクリックします。
3. Workstation Templates タブを開きます。
4. **Edit map template** 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 **Audited** 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、**Reason Required** を選択します。

c. （オプション）電子署名が必要な場合は、**E-Sig Required** 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、**Use Predefined Reason Only** 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、**Audited** 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. **Save Template** 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マップとして使用するには、**Apply to the Workstation** 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. Configuration ワークスペースを開きます。
2. **Audit Maps** をクリックします。
3. Workstation Templates タブを開きます。
4. **Edit map template** 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. **Apply to the Workstation** 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. Configuration ワークスペースを開きます。
2. **Audit Maps** をクリックします。
3. Workstation Templates タブを開きます。
4. **Edit map template** フィールドで、削除するマップを選択します。
5. **Delete Template** 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. **Yes** 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。

監査証跡の表示

1. Audit Trail ワークスペースを開きます。
2. 表示する監査証跡を選択します。
   - ワークステーション監査証跡を表示するには、**Workstation** をクリックします。
   - プロジェクト監査証跡を表示するには、プロジェクトを選択します。
3. 監査レコードの詳細を表示するには、レコードを選択します。

監査レコードの検索またはフィルター

1. Audit Trail 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、**Find in Page** 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。
      Filter Audit Trail 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 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もと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、Results Table の監査証跡を開くためにも使用されます。

1. Audit Trail ワークスペースを開きます。
2. **Browse** 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: Results Table 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. Audit Trail 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. **Print** をクリックします。
   Print ダイアログが開きます。
4. プリンターを選択し、**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. Audit Trail 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. **Export** 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、**File name** を入力して **Save** 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。

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 7-4：イベントレコードフィールド

フィールド	説明
Timestamp	レコードの日時。
Event Name	イベントを生成したモジュール。
説明	イベントの説明。

表 7-4：イベントレコードフィールド (続き)

フィールド	説明
Reason	ユーザーが指定した変更の理由（必要に応じて）。
電子署名	電子署名が提供されているかどうか。
ユーザーのフルネーム	ユーザーの名前。
使用者	ユーザーのユーザープリンシパル名（UPN）。
Category	イベントの種類。

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、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を参照してください。

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。*<workstation name>*-*<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、測定用コンピュータの 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 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ー（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. Queue 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 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 を起動します。
   15 分以内に、SCIEX OS 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。

監査イベント B

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、**Silent Audit Map** 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 B-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
Analytics ワークスペース	
Actual Concentration changed	定量化イベント:「濃度」が変更されました
Auto-Processing File saved	—
Barcode ID changed	—
Comparison sample changed in non-targeted workflow	—
Custom columns modified	定量化イベント:「カスタムタイトル」が変更されました
Data exploration opened	プロジェクトイベント: データファイルが開かれました
Data exported	—
Data transferred to LIMS	—
Dilution Factor changed	定量化イベント:「希釈係数」が変更されました
External calibration changed	—
External calibration exported	—
File saved	プロジェクトイベント: 定量化 Results Table が作成、定量化 Results Table が変更されました、定量化イベント: Results Table が保存されました

表 B-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
Formula column changed	定量化イベント: 数式名が変更、数式名が追加、数式文字列が変更、数式列が削除されました
Integration cleared	—
Integration parameters changed	定量化イベント: 定量化ピークが統合されました
Library search result changed	—
Manual Integration	定量化イベント: 定量化ピークが統合されました
Manual Integration reverted	定量イベント: 定量ピークが元に戻されました
MS/MS selection changed	—
Processing method changed and applied	定量化イベント: 定量化メソッドが変更されました
Report created	プロジェクトイベント: プリンターでのドキュメントの印刷、プリンターでのドキュメントの印刷が終了
Results Table approved	定量化イベント: QA レビューアが Results Table にアクセスしました
Results Table created	定量化イベント: Results Table が作成されました
Results Table locked	—
Results Table unlocked	—
Sample ID changed	定量化イベント:「サンプル ID」が変更されました
Sample Name changed	定量化イベント:「サンプル名」が変更されました
Samples added or removed	定量化イベント: ファイルが Results Table に追加、ファイルが Results Table から削除、サンプルが追加/削除されました
Sample Type changed	定量化イベント:「サンプルタイプ」が変更されました
Std. Addition Actual concentration changed	—
Used column selection changed	定量化イベント:「その使用」が変更されました
Window/pane printed	プロジェクトイベント: プリンターでのドキュメントの印刷、プリンターでのドキュメントの印刷が終了
Audit Map ページ	

表 B-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
Project Audit Map changed	プロジェクトイベント: プロジェクト設定が変更されました
Project Audit Trail Printed	—
Project Audit Trail Exported	—
Batch ワークスペース	
Batch information imported from LIMS/ text	—
Print	プロジェクトイベント: プリンターでのドキュメントの印刷、プリンターでのドキュメントの印刷が終了
Explorer ワークスペース	
Open Sample(s)	プロジェクトイベント: データファイルが開かれました
Recalibrate sample(s)	—
Recalibrate sample(s) started	—
LC Method ワークスペース	
Print	プロジェクトイベント: プリンターでのドキュメントの印刷、プリンターでのドキュメントの印刷が終了
MS Method ワークスペース	
Print	プロジェクトイベント: プリンターでのドキュメントの印刷、プリンターでのドキュメントの印刷が終了
Queue ワークスペース	
Sample Transferred	—

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、**Silent Audit Map** です。

ワークステーション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 B-2 : ワークステーション監査証跡イベント

SCIEX OS または CAC	Analyst ソフトウェア
Instrument Tune（SCIEX OS）	
Firmware changed	—
Manual Tuning	装置イベント: チューニングパラメータ設定の変更
Automatic Tuning	装置イベント: チューニングパラメータ設定の変更
Print Procedure Result in MS Tune	プロジェクトイベント: プリンターでのドキュメントの印刷、プリンターでのドキュメントの印刷が終了
Hardware Configuration（SCIEX OS）	
Devices Activated	装置イベント: ハードウェアプロファイルの有効化。
Devices Deactivated	装置イベント: ハードウェアプロファイルの無効化
Data File Checksum（SCIEX OS）	
Wiff data file checksum has been changed	—
Explorer ワークスペース（SCIEX OS）	
Open Sample(s)	プロジェクトイベント: データファイルが開かれました
Recalibrate samples(s)	—
Recalibrate samples(s) started	—
Audit Map ページ [1]	
Workstation Audit Map changed	装置イベント: 装置設定が変更されました
Workstation Audit Trail printed	—
Workstation Audit Trail exported	—
CAC Server（CAC）	
Project settings enabled/disabled in a workgroup	—
Project assigned/unassigned to a workgroup	—

[1] これらのイベントは、SCIEX OS と CAC の両方に記録されます。

表 B-2 : ワークステーション監査証跡イベント (続き)

SCIEX OS または CAC	Analyst ソフトウェア
User Role(s) assigned/unassigned to user(s) in workgroup	—
User(s)/UserGroup(s) assigned/ unassigned to a workgroup	—
Workgroup added/deleted	—
Workgroup renamed	—
Workstation(s) assigned/unassigned to a workgroup	—
Queue ワークスペース（SCIEX OS）	
Sample moved in Queue	装置イベント: 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。
Batch moved in Queue	装置イベント: バッチの移動
Reaquiring sample	装置イベント: サンプルの再取得
Sample starts to acquire	—
Print Queue	プロジェクトイベント: プリンターでのドキュメントの印刷、プリンターでのドキュメントの印刷が終了
Sample acquistion has completed	プロジェクトイベント: データファイルへのサンプルの追加。
Automatic reinjections Occurred	—
Automatic injection Occurred	—
セキュリティ [1]	
Auto logoff by system	装置イベント: ユーザーログアウト
Forced logoff by another user	装置イベント: ユーザーログアウト
Forced Logoff failed	—
Screen unlock failed	—
Secure Network Account credentials have been changed	装置イベント: 取得アカウント変更
Secure Network Account credentials have been removed	装置イベント: 取得アカウント変更
Secure Network Account credentials have been specified	装置イベント: 取得アカウント変更
Security configuration changed	装置イベント: セキュリティ構成変更、画面ロック変更、自動ログアウト変更

表 B-2 : ワークステーション監査証跡イベント (続き)

SCIEX OS または CAC	Analyst ソフトウェア
User added/deleted	装置イベント: ユーザー追加、ユーザー削除
User has logged in	装置イベント: ユーザーログイン
User has logged out	装置イベント: ユーザーログアウト
User has turned off exclusive mode	—
User Login Failed	装置イベント: ユーザーログイン失敗
User management settings have been exported	—
User management settings have been imported	—
User management settings have been restored	—
User role assigned to user/user group	装置イベント: ユーザーが変更したユーザータイプ
User role deleted	装置イベント: ユーザータイプ削除
User role modified	装置イベント: ユーザータイプ変更
UserLog[1]	
Print Event Log	—

SCIEX OS と Analyst ソフトウェア間の権限のマッピング

C

このセクションは、Analyst ソフトウェアから SCIEX OS 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 権限に対応する Analyst ソフトウェア権限が表示されます。

表 C-1：権限のマッピング

SCIEX OS	Analyst ソフトウェア
Batch ワークスペース	
Submit unlocked methods	—
Open	バッチ: 既存のバッチを開く
Save as	バッチ: 新しいバッチの作成、インポート、バッチの編集、バッチの保存、バッチの上書き
Submit	バッチ: バッチを送信
Save	バッチ: バッチの保存、バッチの上書き
Save ion reference table	—
Add data sub-folders	—
Configure Decision Rules	—
Configuration ワークスペース	
General tab	—
General: change regional setting	—
General: full screen mode	—
General: Stop Windows services	—
LIMS Communication tab	—
Audit maps tab	Audit Trail Manager: 監査証跡設定の変更、監査マップの作成または変更
Queue tab	—
Queue: instrument idle time	—
Queue: max. number of acquired samples	—
Queue: other queue settings	—
Projects tab	—
Projects: create project	Analyst アプリケーション: プロジェクトの作成

表 C-1：権限のマッピング (続き)

SCIEX OS	Analyst ソフトウェア
Projects: apply an audit map template to an existing project	Audit Trail Manager: 監査証跡設定の変更
Projects: create root directory	Analyst アプリケーション: ルートディレクトリを作成
Project: set current root directory	Analyst アプリケーション: ルートディレクトリを設定
Projects: specify network credentials	—
Projects: Enable checksum writing for wiff data creation	—
Projects: clear root directory	—
Devices tab	ハードウェア構成: 作成、削除、編集、有効化/無効化
User management tab	セキュリティ構成
Force user logoff	アプリケーションのロック解除／ログアウト
Event Log ワークスペース	
Access event log workspace	—
Archive log	—
Audit Trail ワークスペース	
Access audit trail workspace	Audit Trail Manager: 監査証跡データの表示
View active audit map	Audit Trail Manager: 監査証跡データの表示
Print/Export audit trail	Audit Trail Manager: 監査証跡データの表示
データ取得パネル	
Start	—
Stop	—
Save	—
MS Method および LC メソッドワークスペース	
Access method workspace	—
New	取得メソッド: 取得メソッドの作成/保存
Open	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）
Save	取得メソッド: 取得メソッドの上書き、取得メソッドの作成/保存

表 C-1：権限のマッピング (続き)

SCIEX OS	Analyst ソフトウェア
Save as	取得メソッド: 取得メソッドの上書き、取得メソッドの作成/保存
Lock/Unlock method	—
Queue ワークスペース	
Manage	サンプルキュー: 再測定、サンプルまたはバッチの削除、バッチの移動
Start/Stop	サンプルキュー: サンプルの開始、サンプルの停止、サンプルの中止、キューの停止
Print	レポートテンプレートエディタ: 印刷
Library ワークスペース	
Access library workspace	Explore: ライブラリの場所の設定、ライブラリのユーザーオプションの設定、ライブラリレコードの追加、ライブラリへのスペクトルの追加、ライブラリレコードの変更（無効になっている場合は、追加/削除を上書き）、MS スペクトルの削除、UV スペクトルの削除、構造の削除、ライブラリの表示、ライブラリの検索
CAC 設定	
Enable Central Administration	—
MS Tune ワークスペース	
Access MS Tune workspace	—
Advanced MS tuning	チューニング: 装置の最適化、手動チューニング、チューニングオプションの編集
Advanced troubleshooting	—
Quick status check	チューニング: 装置の最適化
Restore instrument data	チューニング: チューニングオプションの編集、装置データの編集
Explorer ワークスペース	
Access explorer workspace	—
Export	Explorer: データをテキストファイルに保存
Print	レポートテンプレートエディタ: 印刷
Options	—
Recalibrate	チューニング: 現在のスペクトルからキャリブレーション

表 C-1：権限のマッピング (続き)

SCIEX OS	Analyst ソフトウェア
Analytics ワークスペース	
New results	定量化: 新しい Results Table の作成
Create processing method	定量化: 定量化メソッドの作成
Modify processing method	定量化: 既存のメソッドを変更
Allow Export and Create Report of unlocked Results Table	—
Save results for Automation Batch	—
Change default quantitation method integration algorithm	定量化: デフォルトメソッドのオプションを変更
Change default quantitation method integration parameters	定量化: デフォルトメソッドのオプションを変更
Enable project modified peak warning	—
Add samples	定量化: Results Table からサンプルを追加および削除
Remove selected samples	定量化: Results Table からサンプルを追加および削除
Export, import or remove external calibration	—
Modify sample name	定量化: サンプル名を変更
Modify sample type	定量化: サンプルタイプの変更
Modify sample ID	定量化: サンプル ID の変更
Modify actual concentration	定量化: 分析試料濃度の変更
Modify dilution factor	定量化: 希釈係数の変更
Modify comments fields	定量化: サンプルコメントの変更
Enable manual integration	定量化: 手動統合
Set peak to not found	—
Include or exclude a peak from the results table	定量化: キャリブレーションから標準を除外
Regression options	定量化: 回帰パラメータの変更
Modify the results table integration parameters for a single chromatogram	定量化: Peak Review で「シンプル」パラメータを変更、Peak Review で「アドバンスド」パラメータを変更

表 C-1：権限のマッピング (続き)

SCIEX OS	Analyst ソフトウェア
Modify quantitation method for results table component	定量化: Results Table のメソッドを編集
Create metric plot new settings	定量化: メトリックプロット設定を変更または作成
Add custom columns	定量化: 式列を作成または修正
Set peak review title format	—
Remove custom column	定量化: 式列を作成または修正
Results table display settings	定量化: Results Table の列の精度の変更、Results Table の列の可視性の変更、Results Table の設定の変更
Lock results table	—
Unlock results table	—
Mark results file as reviewed and save	—
Modify report template	レポートテンプレートエディタ: レポートテンプレートの作成/変更
Transfer results to LIMS	—
Modify barcode column	—
Change comparison sample assignment	—
Add the MSMS spectra to library	Explorer: ライブラリレコードにスペクトルを追加
Project default settings	定量化: グローバル（デフォルト）設定の変更
Create report in all formats	—
Edit flagging criteria parameters	—
Automatic outlier removal parameter change	—
Enable automatic outlier removal	—
Update processing method via FF/LS	—
Update results via FF/LS	—
Enable grouping by adducts functionality	定量化: 分析試料グループの作成、分析試料グループの変更
Browse for files	—
Enable standard addition	—

表 C-1：権限のマッピング (続き)

SCIEX OS	Analyst ソフトウェア
Set Manual Integration Percentage Rule	定量化: 手動統合でパーセントルールを有効または無効にする

データファイルのチェックサム D

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 ソフトウェアの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. Configuration ワークスペースを開きます。
2. **Projects** をクリックします。
3. 必要に応じて、**Data File Security** 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、**Enable checksum writing for wiff data creation** 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

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 にアクセスしてください。

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のドキュメント DVD を参照してください。

ドキュメントの最新版は 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。