監査ガイド

Version 2023.1
2024-01-02

InterSystems Corporation　1 Memorial Drive　Cambridge MA 02142　www.intersystems.com

監査ガイド
InterSystems IRIS Data Platform　Version 2023.1　2024-01-02

インターシステムズ社の製品に関するサポートやご質問は、以下にお問い合わせください：

InterSystems Worldwide Response Center (WRC)
Tel:　+1-617-621-0700
Tel:　+44 (0) 844 854 2917
Email:　support@InterSystems.com

目次

監査ガイド 1
1 監査の基本的な概念 1
2 監査の有効化または無効化 1
2.1 監査の有効化 2
2.2 監査の無効化 2
3 監査イベントの要素 2
4 システム監査イベントについて 4
4.1 %System/%Login/Logout および %System/%Login/Terminate 10
4.2 %System/%SQL/EmbeddedStatement 10
4.3 %System/%Security/DBEncChange 11
4.4 %System/%Security/X509CredentialsChange 12
4.5 %System/%System/DatabaseChange 12
4.6 %System/%System/RoutineChange 13
5 ユーザ定義監査イベントの管理 13
5.1 ユーザ定義監査イベントについて 13
5.2 ユーザ定義監査イベントの作成 13
5.3 監査ログへのエントリの追加 14
5.4 ユーザ定義監査イベントの削除 15
6 監査イベントの有効化または無効化 15
7 監査および監査データベースの管理 15
7.1 監査データベースの表示 15
7.2 監査データベースのコピー、エクスポート、および削除 16
7.3 監査データベースの暗号化 18
7.4 汎用管理関数 18
8 その他の監査の問題 19
8.1 監査データベースに書き込めない場合のシステムのフリーズ 19
8.2 監査イベントのカウンタ 20

テーブル一覧

テーブル 1: システム監査イベント 4

監査ガイド

安全な監査データベースのログに特定のキー・イベントを記録する機能は、インターシステムズのセキュリティが持つ大きな特長です。InterSystems IRIS® を使用すると、イベントを監視し、これらのイベントが発生したときに監査データベースにエントリを追加できます。このようなイベントには、InterSystems IRIS 内部で発生するものと、アプリケーションの一部で発生するものがあります。すべての動作が監視されていること、およびすべてのログを確認できることがわかっていると、悪意のある動作に対して、一般的に大きな抑止効果が期待できます。

注釈　このドキュメントでは、管理ポータルで監査イベントを管理する方法について説明します。プログラムで監査イベントを管理するには、Security.Events クラスを使用します。

構造化ログを有効にすることもできます。構造化ログでは、監査データベースと同じメッセージを機械で判読可能なファイルに書き込み、選択した監視ツールで取得できます。"構造化ログの設定" を参照してください。

1 監査の基本的な概念

InterSystems IRIS を使用すると、InterSystems IRIS のインスタンス全体に対する監査の有効化または無効化が可能になります。監査を有効にすると、要求したすべてのイベントが記録されます。監査できるイベントは、次の 2 つのカテゴリに分類できます。

- システム監査イベント ー 明示的に有効にした場合にのみ記録される InterSystems IRIS システム・イベントです。
- ユーザ定義監査イベント ー 明示的に有効にした場合にのみ記録されるアプリケーション・イベントです。

InterSystems IRIS システム・イベントは、InterSystems IRIS 内で発生する起動、シャットダウン、ログインなどの動作を監視する組み込みイベント、セキュリティ設定や監査設定の変更などのセキュリティ関連イベント、およびプロダクション構成やスキーマの変更などの相互運用関連イベントです。

テーブルに対するデータの挿入、更新、削除などのデータベースの動作は、InterSystems IRIS では自動的には監査されません。それは、このような動作では通常、あまりにも多数の監査エントリが生成されるので、これらが役立つことはなく、ときにはシステムの性能に影響を与えるために逆効果となるからです。例えば、医療記録アプリケーションで患者の医療情報へのアクセスをすべて記録するようにした場合、このようなアクセス・イベントが 1 回発生すると、データベースに対して数百から数千のアクセスが行われます。このような場合は、データベース・マネージャで数千の監査エントリを生成するより、アプリケーション側で監査エントリを 1 件生成する方がはるかに効率的です。

2 監査の有効化または無効化

[監査] メニュー (**[システム管理]**→**[セキュリティ]**→**[監査]**) には、監査を有効または無効にする選択項目があります。**[監査の有効化]** が選択できる状態であれば監査が無効になっています。また、**[監査の無効化]** が選択できる状態であれば監査が有効になっています。InterSystems IRIS の監査は、最小セキュリティ・インストールでは既定で無効、通常のインストールおよびロックダウン・インストールでは既定で有効です。

監査を有効にすると、InterSystems IRIS では次のイベントが監査されるようになります。

- 有効化されているすべてのシステム・イベント
- 有効化されているすべてのユーザ定義イベント

2.1 監査の有効化

監査を有効にするには、[**監査**] メニュー ([**システム管理**]→[**セキュリティ**]→[**監査**]) で [**監査を有効に**] を選択します。

2.2 監査の無効化

監査を無効にするには、[**監査**] メニュー ([**システム管理**]→[**セキュリティ**]→[**監査**]) で [**監査を無効に**] を選択します。

3 監査イベントの要素

監査情報は、**IRISAUDIT** データベースにあります。新しいエントリは、ログの末尾に追加されます。監査ログを表示すると、各エントリについて以下の情報が表示されます。

Time (UTCTimestamp とも呼ぶ)

イベントが記録された UTC 日時。

Event Source*

イベントの発生元である InterSystems IRIS インスタンスのコンポーネント。InterSystems IRIS イベントの場合は、“%System”または“%Ensemble”です。ユーザ定義のイベントの場合、この名前には、あらゆる英数字、およびコロンとコンマを除くあらゆる句読点記号を使用でき、先頭の文字には、これらの文字や記号のうち、パーセント記号を除くあらゆるものを記述できます。最大長は 64 バイトです。

Event Type*

イベントに対する情報の分類。この文字列には、あらゆる英数字、およびコロンとコンマを除くあらゆる句読点記号を使用できます。また、先頭の文字には、これらの文字や記号のうち、パーセント記号を除くあらゆるものを記述できます。最大長は 64 バイトです。

Event* (Event Name ともいいます)

記録されたイベントの識別子。この文字列には、あらゆる英数字、およびコロンとコンマを除くあらゆる句読点記号を使用できます。また、先頭の文字には、これらの文字や記号のうち、パーセント記号を除くあらゆるものを記述できます。最大長は 64 バイトです。

PID (Process ID ともいいます)

イベントを記録した InterSystems IRIS プロセスのオペレーティング・システム ID。InterSystems IRIS では、ネイティブ形式で OS PID を使用します。

Web Session (検索結果のみ)

イベントの原因となった Web セッションのセッション ID (存在する場合)。

User (Username ともいいます)

イベントを記録したプロセスの $USERNAME の値。

Description

アプリケーションが監査イベントを要約するために使用できる最大 128 文字のフィールド。このフィールドは、ユーザが判読できる説明または表示用です (これに対し、EventSource、EventType、および Event の組み合わせは監査イベントを一意に定義します)。

* 種類の異なるイベントは、そのイベントの EventSource、そのイベントの EventType、および Event 自体の組み合わせで一意に識別されます。

[詳細] をクリックすると、いくつかの同じ情報に加え、以下の追加情報が表示されます。

Timestamp

イベントが記録された日時 (ローカル時間)。

JobId

ジョブの ID。

IP Address

イベントを記録したプロセスに関連するクライアントの IP アドレス。

Executable

イベントが存在する場合に、そのイベントを記録したプロセスに関連するクライアント・アプリケーション。

System ID

イベントを記録したマシンと InterSystems IRIS インスタンス。例えば、マシンが MyMachine でインスタンスが MyInstance の場合、システム ID は `MyMachine:MyInstance` になります。

Index

監査ログを含むデータ構造内のインデックス・エントリ。

Roles

LoginFailure を除くすべてのイベントについて、イベントを記録したプロセスの $ROLES の値。LoginFailure の場合は、ユーザがログインしていないので “ ” の値が使用されます。

Namespace

イベントが記録されたときに使用されていたネームスペース。

Routine

イベントの記録時に実行されていたルーチンまたはサブルーチン。

User Info

プロセスについてのユーザ定義情報。**%SYS.ProcessQuery** インタフェースによりプログラムで追加されます。

O/S Username

オペレーティング・システムによりプロセスに付与されるユーザ名。表示されるときには、16 文字までに切り捨てられます。

これは、UNIX® システム専用の実際のオペレーティング・システム・ユーザ名です。

Windows では以下のようになります。

- コンソール・プロセスでは、オペレーティング・システム・ユーザ名となります。
- Telnet では、プロセスの $USERNAME となります。
- クライアント接続では、クライアントのオペレーティング・システム・ユーザ名となります。

Status

監査された任意の %Status オブジェクトの値。

Event Data

アプリケーションが監査イベントに関連するデータを最大で 3,632,952 バイト保存できるメモ・フィールド。例えば、イベント発生時のアプリケーションの値セットを入れたり、レコードやフィールドを古い状態のものから新しい状態のものまで集約したりできます。

4 システム監査イベントについて

システム監査イベントとは、既定で監査することが可能な事前定義イベントです。これらのイベントに関する一般的な情報は、[**システム監査イベント**] ページ ([**システム管理**] > [**セキュリティ**] > [**監査**] > [**システムイベントを構成**]) のテーブルに表示されます。このテーブルには以下の列があります。

- イベント名 ー イベント・ソース (%System または %Ensemble)、イベント・タイプ、およびイベントをスラッシュ (“/”) で連結した文字列です。%Ensemble イベント・ソースは、InterSystems IRIS の相互運用機能に関連するイベントに使用されます。
- 有効 ー イベントが監査の対象となっているかどうかを示します。
- 合計 ー InterSystems IRIS が前回起動した時点以降にこのタイプのイベントが発生した件数です。
- 書き込み ー InterSystems IRIS が前回起動した時点以降にこのタイプのイベントが監査ログに書き込まれた件数です。この数は、イベントの発生総件数とは異なることもあります。
- リセットーこのイベントの監査ログをクリアし、そのカウンタをゼロにリセットできます。カウンタの詳細は、″監査イベントのカウンタ″ を参照してください。
- 状態の変更 ー イベントを有効または無効にできます。これらのアクションの詳細は、″監査イベントの有効化または無効化″ を参照してください。

InterSystems IRIS プロダクションへの変更など、InterSystems IRIS システム内のイベントを監視します。システム・イベントは、イベント・ソースの値 %System または %Ensemble によって区別できます。

テーブル 1: システム監査イベント

イベント・ソース	イベント・タイプおよびイベント	発生するタイミング	イベント・データの内容	既定の状態
%Ensemble	%Message/ ViewContents	ユーザがメッセージ・ビューワでメッセージの内容を表示したとき。	メッセージに関するメタデータ。	オン
%Ensemble	%Production/ ModifyConfigura-tion	ユーザがプロダクションの構成を変更したとき。	変更内容の概要。	オン
%Ensemble	%Production/ StartStop	ユーザがプロダクションを開始または停止したとき。	アクション (開始または停止)、およびアクションの開始者のユーザ名。	オン
%Ensemble	%Schema/ Modify	ユーザがスキーマ構造を作成、変更、または削除したとき。	変更内容の概要。	オン

イベント・ソース	イベント・タイプおよびイベント	発生するタイミング	イベント・データの内容	既定の状態
%System	%DirectMode/ DirectMode	ダイレクト・モードでコマンドが実行されたとき。	コマンドのテキスト。	オフ
%System	%Login/ JobEnd	JOB コマンドがバックグラウンド・ジョブを終了したとき。	Job コマンドが実行されたルーチンと、そのルーチンが保存されているデータベース。これらのフィールドの値が NULL の場合、Job コマンドはシェルから実行されています。	オフ
%System	%Login/ JobStart	JOB コマンドがバックグラウンド・ジョブを開始したとき。	Job コマンドが実行されたルーチンと、そのルーチンが保存されているデータベース。これらのフィールドの値が NULL の場合、Job コマンドはシェルから実行されています。	オフ
%System	%Login/ Login	ユーザが正常にログインしたとき。	ログインに関連付けられているプロトコル、ポート番号、プロセス ID、およびアプリケーション。ユーザのログイン・ロール。	オフ
%System	%Login/ LoginFailure	ログインに失敗したとき。	ユーザ名	不定*
%System	%Login/ Logout	ユーザがログアウトしたとき。	ログアウトに関連付けられているアプリケーション（および関連する場合はクラス）。	オフ
%System	%Login/ TaskEnd	タスク・マネージャがプロセスを終了したとき。	なし。タスクの名前は、Description を参照してください。	オフ
%System	%Login/ TaskStart	タスク・マネージャがプロセスを開始したとき。	なし。タスクの名前は、Description を参照してください。	オフ
%System	%Login/ Terminate	プロセスが異常終了したとき。	Description フィールドの内容と同様に変化します。下記を参照してください。	オフ
%System	%SMPExplorer/ Change	ポータルを使用して（クラスまたはテーブルの作成、編集、削除、コンパイル、ドロップ、置換、パージなどによって）データが変更されたとき。	Description フィールドの内容と同様に、実行されるアクションに応じて変化します。関連するコンテンツ（コンパイル・フラグやドロップされるスキーマとテーブルなど）を含みます。	オフ

イベント・ソース	イベント・タイプおよびイベント	発生するタイミング	イベント・データの内容	既定の状態
%System	%SMPExplorer/ ExecuteQuery	ポータルの SQL ページを使用してクエリが実行されたとき。	実行されたクエリの構文。	オフ
%System	%SMPExplorer/ Export	ポータルを使用してデータがエクスポートされたとき。	データのエクスポート時に選択されたオプション。	オフ
%System	%SMPExplorer/ Import	ポータルを使用してデータがインポートされたとき。	データのインポート時に選択されたオプション。	オフ
%System	%SMPExplorer/ ViewContents	ポータルを使用してデータが表示されたとき。	表示されるデータを決定したフィルタ。Description フィールドによって、表示内容 (クラスのリスト、個々のグローバル、プロセス情報など) が指定されます。	オフ
%System	%SQL/ DynamicStatement	動的 SQL 呼び出しが実行されます。	文テキストとホスト変数引数の値が渡されます。文と文のパラメータの合計長が 3,632,952 文字を超える場合、イベント・データは切り詰められます。	オフ
%System	%SQL/ EmbeddedStatement	埋め込み SQL 呼び出しが実行されます。使用法の詳細は、下記を参照してください。	文テキストとホスト変数引数の値が渡されます。文と文のパラメータの合計長が 3,632,952 文字を超える場合、イベント・データは切り詰められます。	オフ
%System	%SQL/ PrivilegeFailure	SQLCODE=-99 エラーが発生したとき。このエラーは、ユーザが必要な特権なしで SQL 文を実行しようとしたときに発生します。	· SQL エラー・メッセージ · ユーザが持っていない、必要な特権 · 特権が欠落しているエンティティ・タイプ (テーブル、ビュー、ストアド・プロシージャなど) · ユーザが特権を持っていないテーブル、ビュー、またはその他のエンティティ · 列レベルの特権がある場合、関連フィールド	オフ

イベント・ソース	イベント・タイプおよびイベント	発生するタイミング	イベント・データの内容	既定の状態
%System	%SQL/XDBCStatement	ODBC または JDBC を使用して、リモート SQL 呼び出しが実行されます。	文テキストとホスト変数引数の値が渡されます。文と文のパラメータの合計長が 3,632,952 文字を超える場合、イベント・データは切り詰められます。	オフ
%System	%Security/ApplicationChange	アプリケーションの定義が作成、変更、または削除されたとき。	アクションの内容 (新規作成、変更、または削除)、新旧のアプリケーション・データ	オン
%System	%Security/AuditChange	監査が停止または開始したとき、エントリが消去または削除されたとき、あるいは監査対象イベントのリストが変更されたとき。	アクションの内容 (停止、開始、消去、削除、または指定)、新旧の監査設定	オン
%System	%Security/AuditReport	任意の標準監査レポートが実行されたとき。	監査レポートの識別情報	オン
%System	%Security/DBEncChange	データベースまたはデータ要素の暗号化に関連する変更があったとき。	Description フィールドの内容と同様に変化します。下記を参照してください。	オン
%System	%Security/DocDBChange	ドキュメント・データベースのアプリケーションの定義が作成、変更、または削除されたとき。	該当する場合、変更の概要と現在の値のリスト。	オン
%System	%Security/DomainChange	ドメイン定義が作成、変更、または削除されたとき。	アクションの内容 (新規、変更、または削除)、新旧のドメイン・データ	オン
%System	%Security/KMIPServer-Change	KMIP サーバの定義が作成、変更、または削除されたか、あるいは KMIP サーバがエクスポートまたはインポートされたとき。	該当する場合、アクションの概要と現在の値のリスト。他の詳細は、Description を参照してください。	オン
%System	%Security/LDAPCon-figChange	LDAP 構成が作成、変更、または削除されたとき。	該当する場合、変更の概要と現在の値のリスト。	オン
%System	%Security/OpenAMIdentity-ServicesChange	OpenAM ID サービスのレコードがエクスポートまたはインポートされたとき。	ファイル名、およびファイルに対してエクスポートまたはインポートされたレコードの数。	オン

イベント・ソース	イベント・タイプおよびイベント	発生するタイミング	イベント・データの内容	既定の状態
%System	%Security/ PhoneProvider–sChange	携帯電話サービス・プロバイダが作成、更新、または削除されたとき。	プロバイダの作成の場合は、その名前および SMS ゲートウェイの値。 プロバイダの更新の場合は、その名前および SMS ゲートウェイの古い値と新しい値 プロバイダの削除の場合は、イベント・データはありません。削除されたプロバイダの名前がイベントの説明に記載されます。	オン
%System	%Security/ Protect	プロセスによってセキュリティ保護エラーが生成されたとき。	エラー。	オフ
%System	%Security/ ResourceChange	リソース定義が作成、変更、または削除されたとき。	アクションの内容（新規、変更、または削除）、新旧のリソース・データ	オン
%System	%Security/ RoleChange	ロール定義が作成、変更、または削除されたとき。	アクションの内容（新規作成、変更、または削除）、新旧のロール・データ	オン
%System	%Security/ SSLConfigChange	TLS 構成の設定が変更されたとき。	新旧の値を持つ変更後のフィールド	オン
%System	%Security/ ServiceChange	サービスのセキュリティ設定が変更されたとき。	新旧のサービス・セキュリティ設定	オン
%System	%Security/ SystemChange	システムのセキュリティ設定が変更されたとき。	新旧のセキュリティ設定	オン
%System	%Security/ UserChange	ユーザ定義が作成、変更、または削除されたとき。	アクションの内容（新規作成、変更、または削除）、新旧のユーザ・データ	オン
%System	%Security/ X509Creden–tialsChange	ユーザが X.509 証明書のセットを作成、更新、または削除したとき。	イベントによって異なります。下記を参照してください	オン
%System	%Security/ X509UserChange	イベントは定義されていますが、将来のリリースまで監査には利用できません。	該当なし	オン

イベント・ソース	イベント・タイプおよびイベント	発生するタイミング	イベント・データの内容	既定の状態
%System	%System/ AuditRecordLost	監査システムに影響するリソース上の制限（ディスクやデータベースに空き領域がないなど）のために、監査エントリが監査データベースに追加されていないとき。	なし	オン
%System	%System/ Configura-tionChange	InterSystems IRIS が前回の起動時とは異なる構成で正常に起動したとき、InterSystems IRIS の実行中に新しい構成がアクティブになったとき、またはポータルあるいは ^LOCKTAB ユーティリティを通してロックが削除されたとき。	変更を実行したユーザの名前、変更された要素の新旧の値。ロックが削除された場合は、どのロックが削除されたかに関する情報。	オン
%System	%System/ DatabaseChange	データベース・プロパティへの変更があります。下記を参照してください。	特定の変更に関する詳細。下記を参照してください。	オン
%System	%System/ JournalChange	データベースまたはプロセスに対するジャーナリングが開始したとき、または停止したとき。	ジャーナリングが開始したときはデータベースの名前およびその最大サイズ、ジャーナリングが停止したときはなし。	オン
%System	%System/ OSCommand	$ZF(-100) 関数の呼び出しなどによって、システム内からオペレーティング・システム・コマンドが発行されたとき。	呼び出されたオペレーティング・システム・コマンド、コマンドが呼び出されたディレクトリ、およびコマンドに関連付けられているフラグ。	オン
%System	%System/ RoutineChange	ローカル・インスタンスでメソッドまたはルーチンがコンパイルまたは削除されたとき。詳細は、下記を参照してください。	なし。ただし、Description フィールドは変更そのものによって変化します。下記を参照してください。	オフ
%System	%System/ Start	システムが起動したとき。	リカバリが実行されたかどうかを示す情報	オン
%System	%System/ Stop	InterSystems IRIS をシャットダウンしたとき。	なし。	オン
%System	%System/ SuspendResume	プロセスが一時停止または再開したとき。	プロセスのプロセス ID。	オフ
%System	%System/ UserEventOver-flow	定義されていないイベントを、アプリケーションからログに記録しようとしたとき。	アプリケーションから記録しようとしたイベントの名前	オン

＊LoginFailure イベントの既定値は、最小セキュリティ・インストールでは [無効]、通常のインストールおよびロックダウン・インストールでは [有効] です。

重要　　監査を有効にすると、有効にしたすべてのイベントが監査されます。

4.1 %System/%Login/Logout および %System/%Login/Terminate

次のいずれかの原因でプロセスが終了すると、%System/%Login/Logout イベントが生成されます。

- HALT コマンドの実行
- QUIT コマンドの実行によるアプリケーション・モードの終了
- プロセスを終了するための SYS.Process クラスの Terminate メソッドの実行 (HALT の実行と同じ)

上記以外の原因でプロセスが終了すると、%System/%Login/Terminate イベントが生成されます。この原因の例として次のものがあります。

- ユーザがターミナル・ウィンドウを閉じた結果、ターミナルの接続が切断された場合。プロセスがアプリケーション・モードで動作している場合は、監査レコードの Description フィールドに “^routinename client disconnect” という文が記述されます (routinename はプロセスで実行した最初のルーチンです)。また、プロセスがプログラマ・モードで動作している場合は、Description フィールドに “Programmer mode disconnect” という文が記述されます。
- ^RESJOB や ^JOBEXAM などの別のプロセス、または管理ポータルで発生したアクションによってターミナル・セッションが終了した場合。プロセスがアプリケーション・モードで動作している場合は、監査レコードの Description フィールドに “^routinename client disconnect” という文が記述されます (routinename はプロセスで実行した最初のルーチンです)。また、プロセスがプログラマ・モードで動作している場合は、Description フィールドに “Programmer mode disconnect” という文が記述されます。イベント・データには、対象のプロセスを終了させたプロセスの PID が記述されています。
- コア・ダンプまたはプロセス例外が発生した場合。プロセスでコア・ダンプまたは例外が発生すると、その時点で既に監査ファイルへの書き込みはできなくなっています。したがって、クリーンアップ・デーモンの実行によってプロセスの状態がクリーンアップされると、“Pid <process nunber> Cleaned” という説明を添えた監査レコードがログに書き込まれます。
- TCP クライアントが切断された場合。クライアントが切断されたことがプロセスで検出されると、監査レコードの Description フィールドには、“<client application> client disconnect” のように、切断された実行可能プログラムの名前を示すメッセージが記述されます。

4.2 %System/%SQL/EmbeddedStatement

%System/%SQL/EmbeddedStatement イベントを使用するには、このイベントおよび `#sqlcompile audit` マクロ・プリプロセッサ指示文の両方を有効にする必要があります。

```
#sqlcompile audit = ON
```

参照情報は、″#sqlcompile audit″ を参照してください。

%System/%SQL/EmbeddedStatement を有効にすると、#sqlcompile audit = ON 指示文の後で埋め込み SQL を実行することで、EmbeddedStatement 監査イベントが生成されます。例を以下に示します。

```
  ...
#sqlcompile audit = ON
  ...
 &sql(delete from MyTable where %ID = :id)
 // This statement is audited at runtime if %System/%SQL/EmbeddedStatement is enabled.

  ...
#sqlcompile audit = OFF
  ...
 &sql(delete from MyOtherTable where %ID = :id)
 // This statement is not audited at runtime even if %System/%SQL/EmbeddedStatement is enabled.
  ...
```

アプリケーションでは数百あるいは数千もの SQL 文 (コンパイルされたクラス・コードの一部として生成されたものやシステム・コードに含まれるものなど) が使用されている可能性があるため、監査イベントとプリプロセッサ指示文を組み合わせることで、監査する埋め込み SQL 文を定義する際に選択しやすくなります。

その他の注意事項：

- #sqlcompile audit = ON 指示文を INSERT 文、UPDATE 文、または DELETE 文で実行した場合、トリガ内の埋め込み SQL コードは監査されません。入れ子になった SQL 文を監査するには、入れ子になったコードに #sqlcompile audit = ON 指示文を追加する必要があります。例えば、トリガ・コードに埋め込み SQL がある場合、そのトリガ・コードに #sqlcompile audit = ON 指示文を置く必要があります。
- 監査された文の結果は記録されません。

次に示すものを除いて、あらゆる埋め込み SQL を監査できます。

- %BEGTRANS
- %CHECKPRIV
- %INTRANS
- %INTRANSACTION
- COMMIT
- GET
- ROLLBACK
- SAVEPOINT
- SET OPTION
- STATISTICS

4.3 %System/%Security/DBEncChange

プロセスで次のいずれかが発生すると、%System/%Security/DBEncChange イベントが生成されます。

- 暗号化キーの有効化
- 暗号化キーの無効化
- 暗号化キーおよびキー・ファイルの作成
- 暗号化キー・ファイルの変更
- [開始時にインタラクティブにデータベース暗号化を有効化する] などの暗号化設定の変更。

EventData には、暗号化キー ID、キー・ファイル、キー・ファイルの管理者名などのイベント関連データが含まれます。

4.4 %System/%Security/X509CredentialsChange

作成および更新の操作の場合、イベント・データには、セキュリティに関する考慮事項に従って、変更されたプロパティがリストされます。Subject Key Identifier および Thumbprint の場合、イベント・データは、スペースで区切られた 1 バイト・ワードの 16 進数文字列です。Certificate、PrivateKey、PrivateKeyPassword、および PrivateKeyType の場合、イベント・データはありません。

削除操作の場合、イベント・データはありません。

4.5 %System/%System/DatabaseChange

プロセスは、以下に示すデータベースへの変更のいずれかによって、%System/%System/DatabaseChange を生成します。

- 作成
- 変更
- マウント
- ディスマウント
- 圧縮
- 削除
- グローバル圧縮
- デフラグ

作成と変更の場合、以下のプロパティへの変更により監査イベントが発生します (このイベントは、イベント・データに含まれます)。

- BlockSize (作成のみ)
- ClusterMountMode (クラスタ・システムのみ)
- ExpansionSize
- GlobalJournalState
- MaxSize
- NewGlobalCollation
- NewGlobalGrowthBlock
- NewGlobalIsKeep
- NewGlobalPointerBlock
- ReadOnly
- ResourceName
- Size

マウントとディスマウントの場合、イベント・データにはマウントまたはディスマウントされたデータベースが記録されます。圧縮、削除、グローバル圧縮、およびデフラグの場合、イベント・データにはユーザが選択したパラメータが含まれます。

4.6 %System/%System/RoutineChange

プロセスでルーチンがコンパイルまたは削除されると、%System/%System/RoutineChange イベントが生成されます。このイベントを有効にしておくと、ルーチンまたはクラスをコンパイルしたときに監査ログにレコードが書き込まれます。監査レコードの Description フィールドには、変更が発生したデータベース・ディレクトリ、および変更されたルーチンまたはクラスの名前が記述され、ルーチンが削除されている場合は“Deleted”という語が追記されます。

InterSystems IRIS はローカル・サーバのイベントを監査しますが、関連インスタンスのイベントは監査しません。例えば、InterSystems IRIS のあるインスタンスが、データベース・サーバである別のインスタンスに関連付けられたアプリケーション・サーバである場合、そのアプリケーション・サーバに新しいルーチンを作成してコンパイルするイベントは、RoutineChange 監査イベントがデータベース・サーバで有効になっていても、データベース・サーバでは監査されません。すべての関連インスタンスのすべての変更の包括的なリストを作成するには、すべてのインスタンスの関連イベントを有効にし、それらの監査ログを結合します。

5 ユーザ定義監査イベントの管理

このセクションでは、以下のトピックについて説明します。

- ユーザ定義監査イベントについて
- ユーザ定義監査イベントの作成
- 監査ログへのエントリの追加
- ユーザ定義監査イベントの削除

ユーザ定義監査イベントの有効化または無効化の詳細は、"監査イベントの有効化または無効化"を参照してください。

5.1 ユーザ定義監査イベントについて

InterSystems IRIS ではシステム・イベントを使用できるほか、アプリケーションから監査データベースに追加できるカスタム・イベントを作成できます。これらは、ユーザ定義監査イベントまたはユーザ監査イベントと呼ばれます。

現在定義されているイベントはすべて [**ユーザ定義の監査イベント**] ページ ([**システム管理**] > [**セキュリティ**] > [**監査**] > [**ユーザイベントを構成**]) に一覧表示されます。

5.2 ユーザ定義監査イベントの作成

InterSystems IRIS でユーザ定義イベントを監査するには、そのイベントをイベントのリストに追加した後、有効にする必要があります。以下はその方法です。

1. 管理ポータルで、[**ユーザ定義の監査イベント**] ページ ([**システム管理**] > [**セキュリティ**] > [**監査**] > [**ユーザイベントを構成**]) に移動します。
2. [**新規イベントの作成**] をクリックします。[**監査イベント編集**] ページが表示されます。
3. このページで、[**イベントソース**]、[**イベントタイプ**]、[**イベント名**]、および [**説明**] の各フィールドに値を入力します。これらのコンポーネントには、"監査イベントの要素" で説明しているような目的があります。
4. このページにある [**有効**] チェック・ボックスには、既定でチェックが付いています。イベントを無効にするには、このチェック・ボックスのチェックを外します。
5. このイベントを作成するには、このページの [**保存**] ボタンをクリックします。
6. 監査が有効になっていることを確認します。

7. イベントを定義し、監査を有効にすれば、以下のコマンドを実行することで、そのイベントを監査ログに追加できます。

   ```
   Do $SYSTEM.Security.Audit(EventSource,EventType,Event,EventData,Description)
   ```

   ポータルで定義した、EventSource、EventType、Event、および EventData の値を使用します。詳細は、"監査ログへのエントリの追加" を参照してください。

5.3 監査ログへのエントリの追加

以下の $SYSTEM.Security.Audit 関数を使用すると、アプリケーションから独自のエントリを監査ログに追加できます。

```
Do $SYSTEM.Security.Audit(EventSource,EventType,Event,EventData,Description)
```

EventSource、EventType、Event、EventData、および Description については、"監査イベントの要素" に説明があります。EventData と Description の両方の引数には、変数またはリテラル値を指定できます (文字列は二重引用符で囲みます)。ログ項目の他の要素は自動的に指定されます。

EventData の内容は複数の行にわたって記述できます。この内容は、ObjectScript Write コマンドの引数と同じように処理されるため、以下の形式が使用されます。

```
"Line 1"_$Char(13,10)_"Line 2"
```

この場合、監査詳細に示された内容が“Line 1”として表示され、`$Char(13,10)` はキャリッジ・リターンと改行で、その後“Line 2”が表示されます。

例えば、XYZ Software Company 製の医療記録アプリケーションで以下のような値が使用されているとします。

```
$SYSTEM.Security.Audit(
    "XYZ Software",
    "Medical Record",
    "Patient Record Access",
    765432,
    "Access to medical record for patient 765432"
    )
```

このアプリケーションでは、EventData 要素を使用して、アクセスされた記録を持つ患者の ID を記録しています。

さらに“XYZ Software/Record Update/Modify Assignment”イベントが定義されて有効になっている場合、以下のコードにより、リストからユーザが選択した要素の値が変更され、監査データベースにその変更が記録されます。

ObjectScript

```
For i=1:1:10 {
    Kill fVal(i)
    Set fVal(i) = i * i
}

Read "Which field to change? ",fNum,!
Read "What is the new value? ",newVal,!
Set oldVal = fVal(fNum)
Set fVal(fNum) = newVal
Set Data = "Changed field " _ fNum _ " from " _ oldVal _ " to "_ newVal _ "."
Set Description = "Record changed by user with an application manager role"
Do $SYSTEM.Security.Audit(
    "XYZ Software",
    "Record Update",
    "Modify Assignment",
    Data,
    Description
)
Write "Field changed; change noted in audit database."
```

Audit は、この追加処理が成功したか失敗したかを示す値 1 または 0 を返します。

監査ログにエントリを追加するために特権が必要になることはありません。

5.4 ユーザ定義監査イベントの削除

ユーザ・イベントを削除する方法は、以下のとおりです。

1. 管理ポータルのホーム・ページで、[**ユーザ定義の監査イベント**] ページ ([**システム管理**] > [**セキュリティ**] > [**監査**] > [**ユーザイベントを構成**]) に移動します。
2. このページで、有効または無効にするイベントを探し、テーブルの右側近くにある列で [**削除**] を選択します。
3. 指示に従って、イベントを削除することを確認します。

注釈　ユーザ定義監査イベントを削除すると、そのイベントは InterSystems IRIS インスタンスの構成要素として監査できなくなります。

6 監査イベントの有効化または無効化

監査イベントを有効または無効にするには、以下の手順に従います。

1. 管理ポータルのホーム・ページから、以下のいずれかに移動します。
   - [**システム監査イベント**] ページ ([**システム管理**] > [**セキュリティ**] > [**監査**] > [**システムイベントを構成**])
   - [**ユーザ定義の監査イベント**] ページ ([**システム管理**] > [**セキュリティ**] > [**監査**] > [**ユーザイベントを構成**])
2. [**システム監査イベント**] または [**ユーザ定義の監査イベント**] ページで、有効または無効にするイベントを探し、テーブルの最も右の列から [**状態変更**] を選択します。これにより、[**有効**] の状態が [**いいえ**] から [**はい**]、またはその逆に変わります。

7 監査および監査データベースの管理

イベントが記録されると、監査データベース **IRISAUDIT** にそのイベントが表示されます。この監査データベースには、一般的な情報も保存されています。この情報には、例えばサーバ名、InterSystems IRIS 構成の名前、ログ記録の開始日時、ログ記録の終了日時があります。

監査ログの管理では、以下のアクションが可能です。

- 監査データベースの表示
- 監査データベースのコピー、エクスポート、および削除
- 監査データベースの暗号化
- 汎用管理関数の実行

7.1 監査データベースの表示

監査データベースを表示するには、以下の手順に従います。

1. [**監査**] メニューから [**監査データベースの閲覧**] を選択して、[**監査データベースの閲覧**] ページ ([**システム管理**] > [**セキュリティ**] > [**監査**] > [**監査データベースの閲覧**]) を表示します。

2. 検索を絞り込むには、このページの左ペインにあるフィールドを使用して、ペインの下部にある **[検索]** ボタンを選択します(既定値に戻すには、ペインの下部にある **[値のリセット]** を選択します)。検索を絞り込むためのフィールドのリストは、以下を参照してください。
3. 特定の監査イベントの詳細を参照するには、その行の **[詳細]** リンクをクリックします。

検索を絞り込むためのフィールドは以下のとおりです。

- **イベントソース** ― イベントの発生元であるインスタンスのコンポーネント。
- **イベントタイプ** ― イベントの分類に関する任意の情報。
- **イベント名** ― 記録されているイベントの識別子 (単に「イベント」とも呼ばれます)。
- **システムID** ― 各監査ログ・エントリに表示されるインスタンスの識別子。machine_name:instance_name の形式です。例えば、MyMachine というマシンで実行されている MyInstance というインスタンスの場合、そのシステム ID は MyMachine:MyInstance になります。
- **PID** ― イベントを記録したプロセスのオペレーティング・システム ID。
- **ユーザ** ― イベントをトリガしたアクティビティを実行したユーザ。
- **認証** ― 監査イベントをトリガしたユーザがインスタンスに対して認証された方法。
- **開始日時** ― 最初に表示するイベントの日時 (既定では、現在の日の午前 0 時)。カレンダーから開始日を選択するには、フィールドの右側にあるカレンダー・アイコンをクリックします。
- **終了日時** ― 最後に表示するイベント (最新のイベント) の日時 (既定では、現在の日時)。カレンダーから終了日を選択するには、フィールドの右側にあるカレンダー・アイコンをクリックします。
- **最大行数** ― 監査ログの一覧に表示する最大行数 (最大 10,000 行)。

注釈　右側に矢印が付いているフィールドでは、矢印をクリックすると、使用中のすべての値のリストが表示されます。先頭にアスタリスク (“*”) が表示されているフィールドでは、アスタリスクを選択または入力すると、フィールドに設定できるすべての値が表示されます。

表示されているフィールドの背景情報は、"監査イベントの要素" を参照してください。

7.2 監査データベースのコピー、エクスポート、および削除

監査ログは %SYS ネームスペースの %SYS.Audit テーブルに格納されます。また、監査データはすべて IRISAUDIT データベースにマップされ、**%DB_IRISAUDIT** リソースによって保護されます。既定では、このリソースの　　許可は %Manager ロールが持っています。また、　　許可を持つロールはありません。

監査ログ・データベースは、他の InterSystems IRIS データベースと同じツールで管理されます。例えば、管理ポータルを使用して、データベースの初期サイズ、増分サイズ、場所を指定できます。監査イベントの喪失を防止するために、監査ログ・データベースに最大サイズを意図的に設定できないようにしています。ただし、ディスク容量などの他の要因による制約は引き続き機能しています。監査が無効なときに監査ログ・データベースの最大サイズの設定を試すと、設定されたように見えます。しかし、続いて監査を有効にすると、その最大サイズは 0 に戻され、最大サイズが設定されていないことが示されます。

管理ポータルでは、監査データベースに対して以下の特別な管理操作を実行できます。

- コピー ― 1 日分以上のエントリを指定のネームスペースにコピーできます。
- エクスポート ― 1 日分以上のエントリをログからファイルにエクスポートできます。
- 削除 ― 1 日分以上のエントリをログから削除できます。

注釈　これらすべての操作は、1 日分以上のエントリすべてに適用できます。特定のエントリのみを対象とした操作はありません。

7.2.1 監査データベースのコピー

InterSystems IRIS では、監査データベースの全体または一部を **IRISAUDIT** 以外のネームスペースにコピーできます。以下はその方法です。

1. 管理ポータルのホーム・ページで、**[監査ログのコピー]** ページ (**[システム管理]** > **[セキュリティ]** > **[監査]** > **[監査ログのコピー]**) に移動します。
2. **[監査ログのコピー]** ページで、まず以下のいずれかを選択します。
   - **監査ログからすべてのアイテムをコピー**
   - **この日数より古い項目を監査ログからコピー** : このフィールドに入力した日数より多くの日数が経過した古い項目が、新しいネームスペースにコピーされます。
3. 次にドロップダウン・メニューを使用して、監査エントリのコピー先とするネームスペースを選択します。
4. 監査項目をコピーした後、コピー元の項目を削除するには、該当するチェック・ボックスにチェックを付けます。
5. **[OK]** をクリックし、目的のエントリをコピーします。

選択した監査ログ・エントリが、指定のネームスペースにある ^IRIS.AuditD グローバルに置かれます。以下の手順で、このデータを表示できます。

1. 管理ポータルのホーム・ページで、**[グローバル]** ページ (**[システムエクスプローラ]→[グローバル]**) に移動します。
2. **[グローバル]** ページで、以下の項目を以下の順序で選択します。
   a. ページの左上の領域にある **[データベース]** ラジオ・ボタン。
   b. コピーした監査ログ・エントリが保持されているデータベースの名前。
   c. グローバルのリストの上に表示されている **[システム]** チェック・ボックス。

   これによって、データベースにある ^IRIS.AuditD などのグローバルのリストが表示されます。このリストでは、グローバルの名前の前に “^” 文字が表示されません。プログラムやターミナルでグローバルを操作する際は、名前の前にこの文字が必要です。

   注釈　このページで **[グローバル表示]** をクリックすると、ページの表示が更新されますが、**[システム]** チェック・ボックスのチェックが外されるので ^IRIS.AuditD が表示されなくなります。
3. IRIS.AuditD の行で **[データ]** をクリックすると、その監査ログ・エントリの詳細が表示されます。

別のネームスペースに監査データをコピーし終わったら、**%SYS.Audit** クラスのクエリを使用してそのデータを確認できます。

7.2.2 監査データベースのエクスポート

InterSystems IRIS では、監査データベースの全体または一部をエクスポートできます。以下はその方法です。

1. 管理ポータルのホーム・ページで、**[監査ログのエクスポート]** ページ (**[システム管理]** > **[セキュリティ]** > **[監査]** > **[監査ログのエクスポート]**) に移動します。
2. **[監査ログのエクスポート]** ページで、まず以下のいずれかを選択します。
   - **[監査ログからすべてのアイテムをエクスポート]**

- **[この日数より古い項目を監査ログからエクスポート]**：このフィールドに入力した日数より多くの日数が経過した古い項目が、新しいネームスペースにエクスポートされます。

3. 次に、監査エントリのエクスポート先とするファイルのパスを、**[ファイルにエクスポート]** フィールドに入力します。フル・パスで入力しない場合は、パスのルートには install-dir/**Mgr**/ が使用されます。
4. 監査項目をエクスポートした後、エクスポート元の項目を削除するには、該当するチェック・ボックスにチェックを付けます。
5. [OK] をクリックし、目的のエントリをエクスポートします。

7.2.3 監査データベースの削除

InterSystems IRIS では、データベースの全体または一部を削除できます。

重要　削除によるデータベース操作は元に戻せません。つまり、削除した項目は永久に削除されます。データベースから削除した項目は、元のデータベースにリストアできません。

以下はその方法です。

1. 管理ポータルのホーム・ページで、**[監査ログのパージ]** ページ (**[システム管理]** > **[セキュリティ]** > **[監査]** > **[監査ログのパージ]**) に移動します。
2. **[監査ログのパージ]** ページで、まず以下のいずれかを選択します。
   - **[監査ログからすべてのアイテムをパージ]**
   - **[この日数より古い項目を監査ログからパージ]**：このフィールドに入力した日数より多くの日数が経過した古い項目が削除されます。
3. [OK] をクリックし、目的のエントリを削除します。

7.3 監査データベースの暗号化

InterSystems IRIS では、監査ログを保持するデータベースを暗号化できます。詳細は、"暗号化の起動設定の構成" を参照してください。

7.4 汎用管理関数

監査ログはテーブルに格納されるため、InterSystems IRIS の標準的なシステム管理ツールおよび手法を使用して管理できます。

- ジャーナリングは監査ログに対して常に有効になっています。
- 監査ログは、標準的な ObjectScript コマンドを使用して読み取ることができます。また、その内容には標準 SQL を使用してアクセスでき、任意の標準 SQL ツールを使用して監査ログを処理できます。
- 監査ログは、InterSystems IRIS の標準的なデータベース・バックアップ機能を使用してバックアップできます。
- データベースがいっぱいになると <FILEFULL> エラーが発生し、他の InterSystems IRIS データベースに対する処理と同じ処理が行われます。このような状態を避けるには、"監査データベースのサイズの維持" を参照してください。

注釈　すべてのアクセスは、データベース・レベルおよびネームスペース・レベルにおいて、またはテーブル・ベースのアクティビティ用の SQL によって、標準的なセキュリティ制限の対象となります。

%SYS ネームスペースの %SYS.Audit テーブルは監査ログを保持します。監査データはすべて、IRISAUDIT データベースにマップされます (″監査データベースのコピー″ で説明されている機能を使用して、監査データを他のデータベースにコピーすることもできます。その後で、ネームスペースごとに使用可能な %SYS.Audit クラスを使用して、監査ログを照会できます)。

7.4.1 監査データベースのサイズの維持

InterSystems IRIS を実行すると監査ログへの書き込みが発生します。操作を行わないと、最終的に監査データベースが一杯になります。監査データベースがいっぱいになった場合、InterSystems IRIS は、監査エントリをキャプチャせずに実行を継続するか、監査データベースに書き込めるようになるまで停止します。この動作は、[監査データベースのエラー時にシステムを凍結する] の設定によって決まります。

監査情報を適切に保存し、問題を防ぐには、監査データベースの内容を定期的にエクスポートして保存し、その内容を削除する必要があります。以下はその方法です。

1. ″監査データベースのエクスポート″ の説明に従って、監査データベースの内容をエクスポートします。

   注釈　すべてのエントリをデータベースからエクスポートすることをお勧めします。

2. 監査データベースのエクスポートした内容が有効であることを確認します。

   重要　データの削除は元に戻せない操作であるため、このデータが有効であることを確認することをお勧めします。

3. ″監査データベースの削除″ の説明に従って、既存のデータベースから古いエントリを削除します。

   重要　最新日付のエントリを残して、それ以外のエントリを削除することをお勧めします。こうすることによって、エクスポート済みのエントリと重なるエントリが残り安全です。

注意　監査データベースがいっぱいになった場合に InterSystems IRIS が実行を継続すると、監査イベントを引き起こすアクションの監査エントリは記録されなくなります。さらに、法則の面から考えれば、AuditRecordLost 監査エントリのみが 1 件存在している場合は、レコードが 1 件以上失われたことを示しています。

8 その他の監査の問題

このセクションでは、以下のトピックについて説明します。

- 監査データベースに書き込めない場合のシステムのフリーズ
- 監査イベントのカウンタ

8.1 監査データベースに書き込めない場合のシステムのフリーズ

InterSystems IRIS の動作中に、監査データベースへの書き込みが不可能になることがあります。これは、ディスクがいっぱいになった場合やネットワーク接続に障害が起きた場合などに発生します。これが発生した場合、InterSystems IRIS は以下のいずれかを実行する可能性があります。

- エラーを生成して動作を継続する (既定)。
- システムをフリーズする。

この動作を変更するには、以下の手順に従います。

1. **[システムワイドセキュリティパラメータ]** ページ (**[システム管理]**→**[セキュリティ]**→**[システム・セキュリティ]**→**[システムワイドセキュリティパラメータ]**) に移動します。監査が有効な場合、このページで **[監査データベースにエラーが発生したときにシステムをフリーズしますか]** チェック・ボックスを使用できます。
2. **[監査データベースにエラーが発生したときにシステムをフリーズしますか]** チェック・ボックスにチェックを付けるか、チェックを外します。
3. ページの **[保存]** ボタンをクリックします。

例えば、監査データベースがいっぱいであるとします。監査ログに書き込もうとすると、<FILEFULL> エラー (ディスクの空き容量不足) が生成されます。この際、動作に次のような違いがあります。

- エラーを生成して動作を継続する場合 (既定) ー プロセスは監査レコードを監査ログに書き込まないため、監査レコードは失われます。問題を解決すると、失われた監査イベントの件数が記録された監査ログにエントリが書き込まれます。
- エラー発生時にインスタンスをフリーズする場合 ー プロセスが messages.log ファイルにエラー・メッセージを書き込んだ後、システムはフリーズします。

8.1.1 監査ログのエラーからの回復に関するヒント

ディスクの空き容量不足エラーから回復するには、システムを強制的に停止し、監査ディスクの空き容量を確保してから、システムを再起動します。

データベースの破損によるエラーから回復するには、監査データベースを削除または移動してから、新しい監査データベースを作成するか、新しい監査データベースを古い監査データベースの場所にコピーします(エラーをクリアするには、単にシステムを再起動するのではなく、新しいデータベースを使用する必要があります。再起動すると監査レコードが書き込まれ、それによりシステムが再びフリーズする可能性があるためです)。

8.2 監査イベントのカウンタ

セキュリティ監視を容易にするために、InterSystems IRIS では監査イベント・タイプごとにカウンタを保持し、InterSystems IRIS 監視インタフェースを介して、これらのカウンタを利用できるようにしています。これらのカウンタは、監査が有効ではない状態でも維持されています。例えば、LoginFailure イベント・カウンタを監視していれば、サイトに侵入しようとする行為の検出に役立ちます。

注釈　　監査のカウンタは、インスタンスの再起動時にリセットされます。

8.2.1 システム監査イベントのカウンタのリセット

システム・イベントのカウンタをリセットするには、以下の手順に従います。

1. 管理ポータルのホーム・ページで、**[システム監査イベント]** ページ (**[システム管理]** > **[セキュリティ]** > **[監査]** > **[システムイベントを構成]**) に移動します。
2. このページで、有効または無効にするイベントを探し、テーブルの右側近くにある列で **[リセット]** を選択します。
3. プロンプトが表示されたら、**[OK]** をクリックします。これによって、選択したイベントの **[合計]** カウンタと **[書き込み]** カウンタの両方がリセットされます。

8.2.2 ユーザ定義監査イベントのカウントのリセット

ユーザ・イベントのカウンタをリセットするには、以下の手順に従います。

1. 管理ポータルのホーム・ページで、**[ユーザ定義の監査イベント]** ページ (**[システム管理]** > **[セキュリティ]** > **[監査]** > **[ユーザイベントを構成]**) に移動します。

2. このページで、有効または無効にするイベントを探し、テーブルの右側近くにある列で **[リセット]** を選択します。これによって、選択したイベントの **[合計]** カウンタと **[記録数]** カウンタの両方がリセットされます。
3. プロンプトが表示されたら、[OK] をクリックします。これによって、選択したイベントの **[合計]** カウンタと **[書き込み]** カウンタの両方がリセットされます。