SOPHOS

Cybersecurity made simple.

Sophos Enterprise Console

監査ガイド

製品バージョン: 5.5

目次

1 このガイドについて

このガイドでは、Sophos Enterprise Console の設定変更や、ユーザーまたはシステムのアクティビティを監視する方法について説明します。

2 Sophos Auditing について

Sophos Auditing は、Enterprise Console の設定変更や、ユーザーやシステムのアクティビティを監視する機能です。これで得られる情報は、法令順守やトラブルシューティングのために利用したり、また悪質な行為が発覚した際にはフォレンシック分析に利用したりすることができます。

デフォルトで監査機能は無効になっています。Enterprise Console で監査を有効にすると、特定の環境設定に変更が加えられた場合や、特定のアクションが実行された場合に、「SophosSecurity」という SQL Server データベースに監査エントリが書き込まれます。

監査エントリには以下の情報が含まれます。

- 実行されたアクション
- アクションを実行したユーザー
- ユーザーのコンピュータ
- ユーザーのサブ管理サイト
- アクションの実行日時

成功したアクションと失敗したアクションの両方が監査されるため、監査エントリには、システムでアクションを実行したユーザー名や、正常に完了していないアクションを開始したユーザー名も表示されます。

監査データベースに保存されているデータは、Microsoft Excel、Microsoft Access、Microsoft SQL Server Reporting Services や Crystal Reports などのサードパーティ製プログラムを使用し、アクセスして解析することができます。

重要
Sophos Auditing は、サードパーティ製アプリケーションを使用したデータへのアクセスを可能にする機能です。この機能を使用する場合、お客様は、許可されたユーザーだけがデータにアクセスできるようにするなど、データのセキュリティに対して責任を負うこととなります。セキュリティに関する注意点は、製品に搭載されているデータベース保護機能 (p. 4)を参照してください。

監査されるアクションの詳細は、監査されるアクション (p. 20)を参照してください。

3 Sophos Auditing を使用する際の主なステップ

Sophos Auditing を使用する際の主なステップは次のとおりです。

- データベースの安全性の確保
- 監査の有効化
- 監査データへのアクセス権限の許可
- 監査レポートの作成

4 データベースの安全性の確保

4.1 製品に搭載されているデータベース保護機能

Enterprise Console および SophosSecurity データベースには、監査データを保護する次のような機能が搭載されています。

- アクセスコントロール
- タンパー プロテクション

アクセスコントロール

アクセスコントロールは、次の方法で適用されます。

- GUI

  Enterprise Console で「**監査**」権限があり、Sophos Console Administrators グループに所属するユーザーのみが監査を有効化/無効化できます。

- データベース

  デフォルトで、Sophos DB Admins グループのユーザーのみが、データベースのインターフェースにアクセスできます。さらに、データベースのインターフェースでストアドプロシージャを表示するには、有効なユーザーのセッショントークンが必要です。トークンは、ユーザーが GUI を開いたとき、またはサブ管理サイトを変更したときに、システムによって生成されます。

タンパー プロテクション

データベースは、監査イベントのデータが改ざんされることを防ぎます。一部の構成設定以外は、監査データベース内のデータをアップデートする必要はありません。また、テーブルのデータを更新または削除しようとするとロールバックするトリガーもあります。

データは、データベースをパージしない限り、削除されません。保存期間が 2年より長いデータは、Enterprise Console サーバーに埋め込まれた標準スケジュールタスクの一環として、24時間ごとに自動的にパージされます。また、PurgeDB ツールを使用してデータをパージすることもできます (http://www.sophos.com/ja-jp/support/knowledgebase/109884.aspx を参照してください)。

4.2 データベースのセキュリティの改善

データベースを監査する

データベースに組み込まれている保護機能の他に、SQL Server インスタンスに対して追加の保護レイヤーを設定し (未設定の場合)、ユーザーアクティビティや SQL Server への変更を監査することを推奨します。

たとえば、SQL Server 2008 Enterprise Edition を使用している場合は、SQL Server Audit 機能を使用できます。旧バージョンの SQL Server では、ビルトインのトレース機能を使用して、ログインの監査、トリガーを使用した監査、およびイベントの監査を実行できます。

SQL Server システムでのアクティビティおよび変更を監査するために使用できる機能の詳細は、該当するバージョンの SQL Server ドキュメントを参照してください。例:

- SQL Server Audit (データベース エンジン)
- 監査 (データベース エンジン)、SQL Server 2008 R2
- SQL Server 2008 の監査機能 (英語)
- 監査 (データベース エンジン)、SQL Server 2008

データベースへの接続を暗号化する

クライアントと データベースの接続を暗号化することを強く推奨します。詳細は、次の SQL Server のドキュメントを参照してください。

- データベース エンジンへの暗号化接続の有効化 (SQL Server 構成マネージャー)
- SQL Server 2008 R2 への暗号化接続
- Microsoft 管理コンソールで SQL Server インスタンス用に SSL 暗号化を有効にする方法

データベースのバックアップへのアクセスをコントロールする

データベースのバックアップやコピーにはアクセス制限を設定し、適切なアクセスが行われるようコントロールしてください。これによって、未認証のユーザーがファイルにアクセスしたり、改ざん、または誤って削除したりすることを防止できます。

注
このセクションに記載されているリンクの参照先は第三者によって管理されている情報であり、リンクはお客様の便宜を図る目的に限って提供しています。ソフォスでは、リンク切れなどについて定期的に確認していますが、第三者の Web サイトによって予告なしにリンクが変更される場合があります。

データベース接続のチェック

5.5.1 のインストーラの実行時に、データベースの接続がチェックされ (インストールやアップグレードの前に行われます)、TLS 1.2 でデータベースに接続できるかどうか判断されます。

TLS 1.2 を使用してデータベースに接続するようにするには、**CheckDBConnection.exe** ツールを使用します。接続チェックの結果が表示され、手動で変更を行うことができます。

詳細は、サポートデータベースの文章 127521 を参照してください。

5 Sophos Auditing の有効化

デフォルトで監査機能は無効になっています。監査を有効化する方法は次のとおりです。

1. Enterprise Console の「**ツール**」メニューで、「**監査の管理**」をクリックします。
2. 「**監査の管理**」ダイアログボックスで、「**監査を有効にする**」チェックボックスを選択します。

注
オプションがグレーアウト表示されている場合は、監査を管理する権限がないことを意味します。監査を有効化/無効化するには、Sophos Console Administrators グループのメンバーであること、また Enterprise Console で「**監査**」権限が割り当てられていることが必要です。ユーザー権限とロールベースの管理について、詳細は、Sophos Enterprise Console ヘルプを参照してください。

6 監査データへのアクセス権限の許可

監査データには、デフォルトでシステム管理者のみがアクセスできます。他のユーザーが監査レポートを作成するためにデータにアクセスするには、SophosSecurity データベースの「**Reports**」スキーマ内で明示的に「Select」権限が付与されている必要があります。この操作は、**sqlcmd** ユーティリティを使用するか、SQL Server Management Studio で実行できます。

6.1 sqlcmd ユーティリティを使用した監査データへのアクセス権付与

監査データへのアクセス権限を許可する方法は次のとおりです。

1. 次のスクリプトを「メモ帳」ファイルなどのテキストファイルにコピーします。

```
USE SophosSecurity;

DECLARE @stmt NVARCHAR(max);

DECLARE @Account VARCHAR(512)

/* <Domain>¥<User> は監査データへのアクセスを許可するユーザーのアカウントで置き換えてください。*/

SET @Account = N'<Domain>¥<User>'

IF NOT EXISTS( SELECT * FROM sys.server_principals WHERE name = @Account )
BEGIN
     SET @stmt = N'CREATE LOGIN [' + @Account + N'] FROM WINDOWS';
     EXEC sp_executesql @stmt;
END;

IF NOT EXISTS( SELECT * FROM sys.database_principals WHERE name = @Account )
BEGIN
     SET @stmt = N'CREATE USER [' + @Account + N'] FOR LOGIN [' + @Account +
 N']';
     EXEC sp_executesql @stmt;
END;

SET @stmt = N'GRANT SELECT ON SCHEMA :: [Reports] TO [' + @Account + N']';
EXEC sp_executesql @stmt;
GO
```

2. 「SET @Account = N'<Domain>¥<User>'」ステートメントにある <Domain> および <User> プレースホルダは、監査データへのアクセス権限を許可するユーザーのドメイン名とユーザー名で置き換えてください。

   ワークグループ環境のコンピュータの場合、<Domain> はデータベースがインストールされているコンピュータ名で置き換えてください。他のワークグループに属するコンピュータからアクセスする場合は、同じユーザー名とパスワードを持つユーザーアカウントが、両方のコンピュータ上に存在している必要があります。

3. コマンド プロンプトを開きます。
4. SQL Server インスタンスに接続します。次のように入力します。

```
sqlcmd -E -S <サーバー名>¥<SQL Server インスタンス>
```

   デフォルトの SQL Server インスタンスは SOPHOS です。
5. 先ほどファイルにコピーしたスクリプトをコマンドプロンプトに貼り付けます。
6. 「Enter」キーを押してスクリプトを実行します。
   スクリプト実行後、SophosSecurity データベースの「**Reports**」スキーマで、ユーザーに「Select」権限が許可され、監査データにアクセスできるようになります。
7. アクセスが必要な各ユーザーに対して、この操作を繰り返してください。

6.2 SQL Server Management Studio を使用した監査データへのアクセス権付与

SQL Server Management Studio を使用して、SophosSecurity データベースの「**Reports**」スキーマで、ユーザーに「Select」権限を許可する前に、ユーザーに SQL Server ログインがあり、SophosSecurity データベースのユーザーであることを確認してください。

- すでにユーザーに SQL Server ログインがある場合は、それを SophosSecurity データベースのユーザーとして追加してください。「オブジェクト エクスプローラ」で、サーバーを展開し、「**データベース**」-「**SophosSecurity**」-「**セキュリティ**」の順に展開します。「**ユーザー**」を右クリックして、「**新しいユーザー**」をクリックします。「**データベース ユーザー**」ダイアログボックスで、ユーザー名を入力し、ログイン名を選択します。「**OK**」をクリックします。

  データベース ユーザーの作成の詳細は、http://msdn.microsoft.com/ja-jp/library/aa337545.aspx#SSMSProcedureを参照してください。

- ユーザーに SQL Server ログインがない場合は、新しい SQL Server ログインを追加し、SophosSecurity データベースユーザーに指定してください。「オブジェクト エクスプローラ」で、サーバーを展開し、「**セキュリティ**」を展開します。「**ログイン**」を右クリックして、「**新しいログイン**」をクリックします。「**ログイン**」ダイアログボックスの「**全般**」ページで、アカウント名やグループ名を入力します。「**ユーザー マッピング**」ページで、「**SophosSecurity**」を選択します。「**OK**」をクリックします。

  SQL Server ログイン作成の詳細は、http://msdn.microsoft.com/ja-jp/library/aa337562.aspx#SSMSProcedure を参照してください。

SQL Server Management Studio を使用して、監査データへのアクセス権限をユーザーに許可する方法は次のとおりです。

1. 「オブジェクト エクスプローラ」で、サーバーを展開し、「**データベース**」-「**SophosSecurity**」-「**セキュリティ**」-「**スキーマ**」の順に展開します。
2. 「**Reports**」を右クリックして、「**プロパティ**」をクリックします。
3. 「**スキーマのプロパティ - Reports**」ダイアログボックスの「**権限**」ページで、「**検索**」をクリックします。「**ユーザーまたはロールの選択**」ダイアログボックスで、ユーザー (複数可) を追加します。
4. 各ユーザーに対して、「**<ユーザー>の権限**」セクションの「**明示的**」タブで、「**許可**」の下の「**選択**」を選択し、「**OK**」をクリックします。

7 Microsoft Excel での監査レポートの作成

ここでは、Microsoft Excel 2010 で、SQL Server データベースから監査データをインポートし、解析する方法について説明します。

また、次の手順に従ってMicrosoft Excel で監査レポートを作成する方法についても説明します。

- 監査データベースへの接続を設定する (新しいデータソースを作成する)。
- Microsoft Query で新しいクエリを作成する。
- Excel にデータを返す。
- Excel でレポートを作成する (テーブルまたはピボットテーブル レポート)。

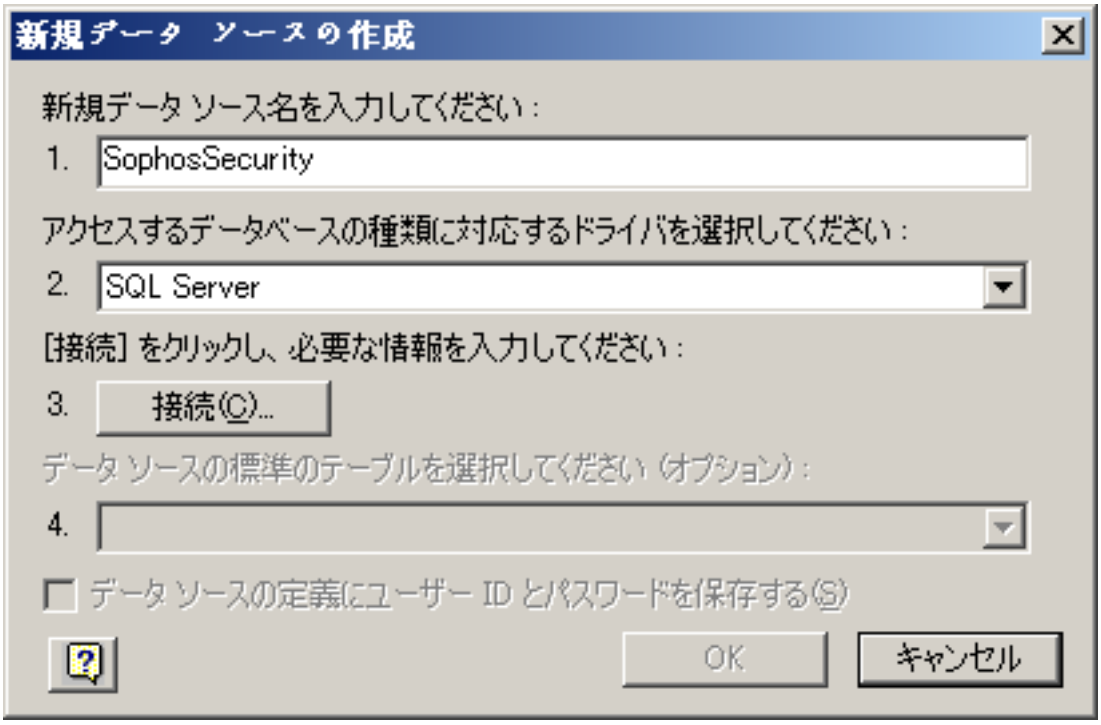
注
エクスポートした監査データに外部ロジックをバインドする場合は、文字列ではなく、数値 ID を使用することを推奨します。たとえば、「**TargetType**」フィールドの値ではなく、「**TargetTypeId**」フィールドの値を使用するようにしてください。これにより、今後の Enterprise Console のリリースで文字列が変更された場合でも、互換性の問題が起きる可能性を回避します。数値 ID の一覧表は、補足: データフィールド値の数値 ID (p. 28)を参照してください。

Excel に SQL Server のデータをインポートしてレポートを作成する方法について、詳細はマイクロソフト社のドキュメントを参照してください。

7.1 データベース接続の設定

まず、データベースに接続してください。

1. Excel を開きます。「**データ**」タブの「**外部データの取り込み**」グループで、「**その他のデータ ソース**」をクリックして、「**Microsoft Query**」をクリックします。
   「**データ ソースの選択**」ダイアログボックスが表示されます。
2. 「**データベース**」タブで、「**<新規データ ソース>**」を選択したままで、「OK」をクリックします。
3. 「**新規データソースの作成**」ダイアログボックスで、データソース名を入力します。この例では、「**SophosAuditing**」と入力します。
4. 「**アクセスするデータベースの種類に対応するドライバを選択してください**」ボックスで、「**SQL Server**」を選択します。

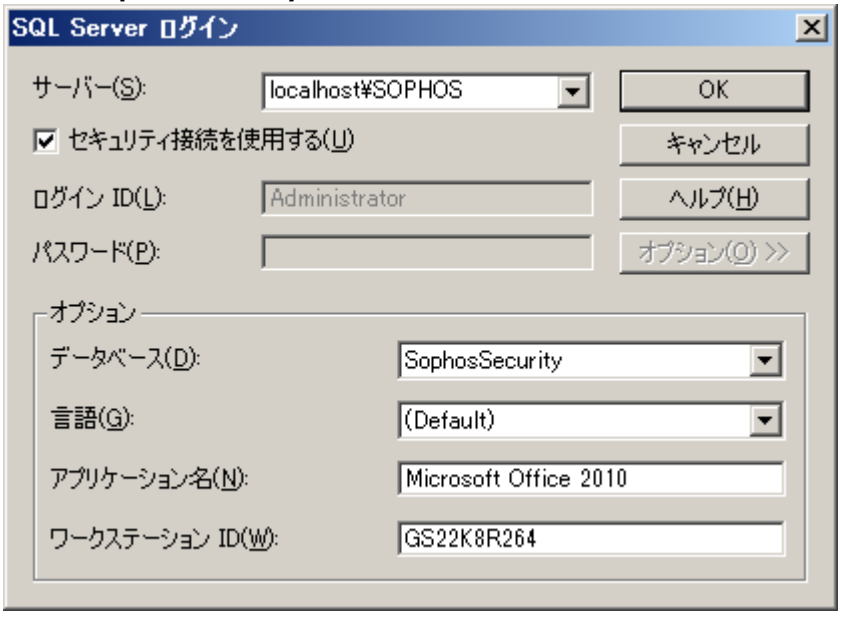


「**接続**」をクリックします。

5. 「**SQL Server ログイン**」ダイアログボックスの「**サーバー**」ボックスで、接続する SQL Server 名を入力します。

   この例では、同じコンピュータ (localhost) にあるデータベースのインスタンス、SOPHOS に接続します。

6. 「**オプション**」をクリックして、「**オプション**」パネルを展開します。「**データベース**」ボックスで「**SophosSecurity**」を選択します。



「**OK**」をクリックします。

7. 「**新規データソースの作成**」ダイアログボックスの「**データ ソースの標準のテーブルを選択してください (オプション)**」で、「**vAuditEventsAll**」を選択します。

   「**OK**」をクリックします。

7.2 クエリの作成

ここでは、過去 3か月のデータコントロール ポリシーの変更内容についての情報を取得するため、先ほど作成したデータソースのクエリを作成する方法について説明します。

1. 「**データ ソースの選択**」ダイアログボックスで、「**クエリ ウィザードを使ってクエリを作成/編集する**」チェックボックスを選択から外します。
2. 前のステップで作成したデータソース (この例では **SophosAuditing**) を選択し、「**OK**」をクリックします。
   「**Microsoft Query**」ダイアログボックスに、データソース作成時に選択した標準のテーブル「**vAuditEventsAll**」とともに「**SophosAuditing からのクエリ**」が表示されます。
3. 次のいずれかの手順を実行してください。
   - デザインビューでクエリを作成します。
     a) 「**Microsoft Query**」ダイアログボックスの「**条件**」メニューで、「**抽出条件の追加**」をクリックします。
     b) 「**抽出条件の追加**」ダイアログボックスの「**フィールド**」で、「**Timestamp**」を選択します。「**演算子**」フィールドが空であることを確認します。「**値**」フィールドで次のように入力します。

        >=DATEADD(mm,-3,GETUTCDATE())

        「コンロトールパネル」の「地域と言語」の設定で指定されている区切り記号を使用します。たとえば、区切り記号がセミコロンの場合、上記の入力例でカンマの代わりにセミコロンを使用します。無効な区切り記号を使うと「Extra ')'」というエラーメッセージが表示されることがあります。

        「**追加**」をクリックします。条件が「**SophosAuditing からのクエリ**」に追加されます。
     c) 「**抽出条件の追加**」ダイアログボックスの「**フィールド**」で、「**TargetType**」を選択します。「**演算子**」フィールドで、「**=**」(等号) を選択します。「**値**」フィールドで、「**Policy**」を選択または入力します。

        「**追加**」をクリックします。条件が「**SophosAuditing からのクエリ**」に追加されます。
     d) 「**抽出条件の追加**」ダイアログボックスの「**フィールド**」で、「**TargetSubType**」を選択します。「**演算子**」フィールドで、「**=**」(等号) を選択します。「**値**」フィールドで、「**Data control**」を選択または入力します。

        「**追加**」をクリックします。条件が「**SophosAuditing からのクエリ**」に追加されます。

        「**抽出条件の追加**」ダイアログボックスで、「**閉じる**」をクリックします。
     e) 「**Microsoft Query**」ダイアログボックスで、「**vAuditEventsAll**」の各フィールドをダブルクリックしてクエリに追加します。または、テーブルから表示エリアにドラッグして、フィールドをクエリに追加することもできます。
   - SQL ビューでクエリを作成します。

a) 「**Microsoft Query**」で「**SQL**」ボタンをクリックして、次のような SQL ステートメントを入力します。

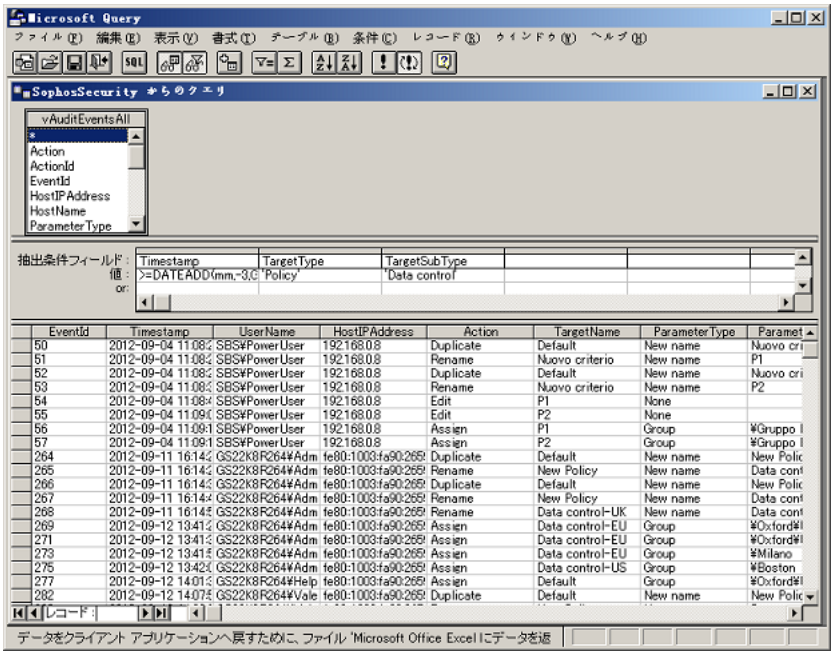
```
SELECT EventId, Timestamp, UserName, HostIPAddress, Action, TargetName,
 ParameterType, ParameterValue, Result

FROM SophosSecurity.Reports.vAuditEventsAll

WHERE (Timestamp>=DATEADD(mm,-3,GETUTCDATE()))
AND (TargetType='Policy')
AND (TargetSubType='Data control')

ORDER BY EventId ASC
```

「**OK**」をクリックします。



4. クエリを保存するには、「**ファイル**」メニューで「**上書き保存**」をクリックします。

7.3 Excel にデータを返す

Excel にデータを返すには、「**Microsoft Query**」ダイアログボックスで、「**データを返す**」ボタンをクリックします。

または、「**ファイル**」メニューで、「**Microsoft Excel にデータを返す**」をクリックします。

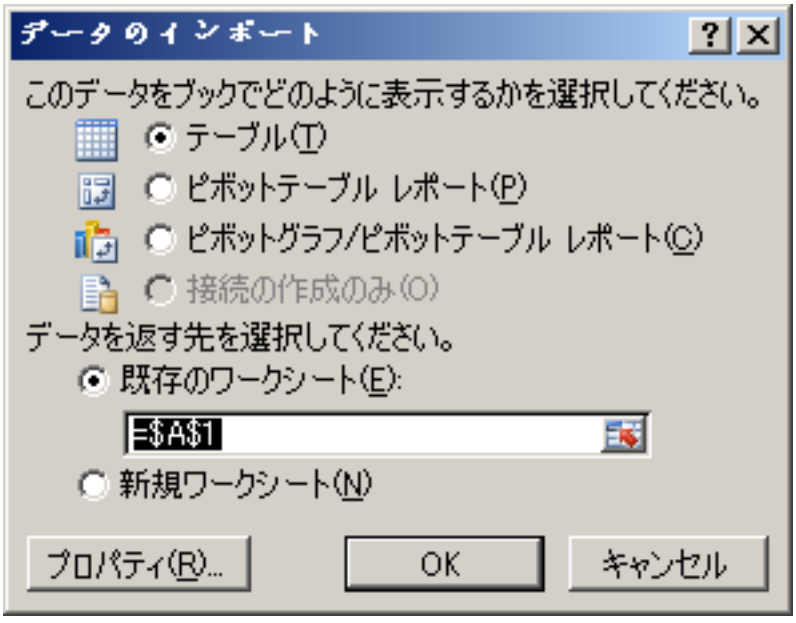
Excel に戻ると、「**データのインポート**」ダイアログボックスが表示され、作成するレポートの種類を選択できます。

以下の例では、次の操作について説明します。

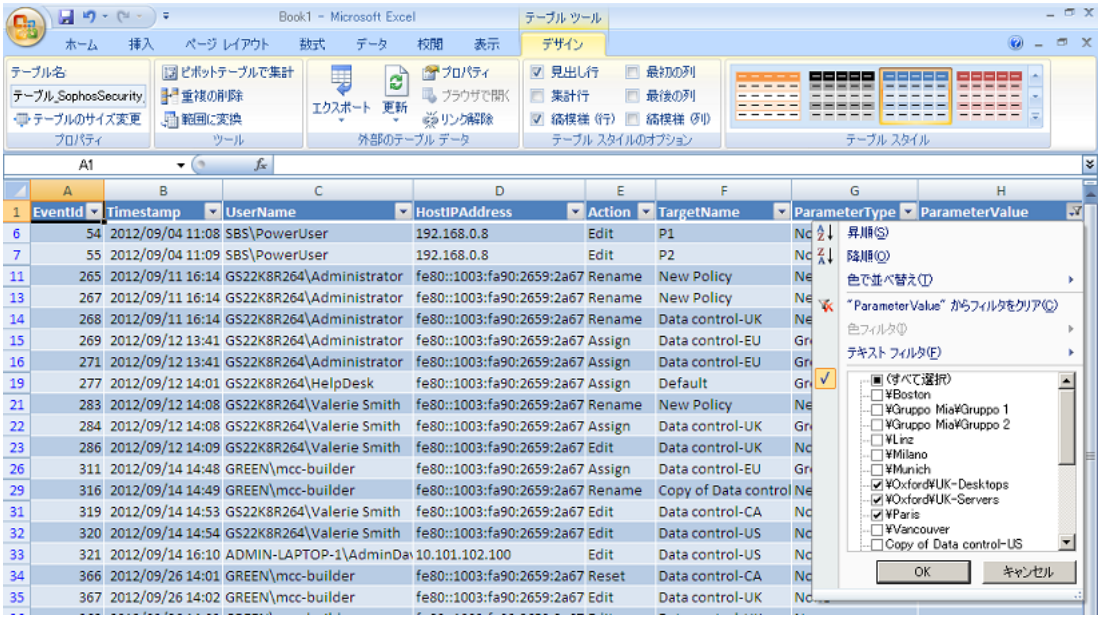
- テーブルの作成 (p. 13)
- ピボットテーブル レポートの作成 (p. 14)

7.4 テーブルの作成

1. Excel テーブルに監査データをインポートするには、「**データのインポート**」ダイアログボックスで、「**テーブル**」を選択したままにします。
   既存のワークシートのセル A1 からデータを配置するには、「**既存のワークシート**」を選択したままにします。



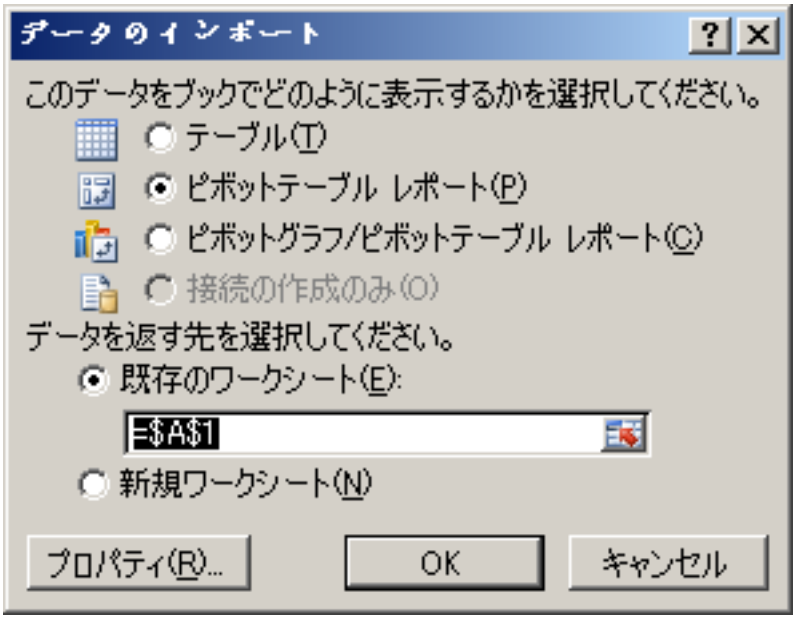
   「**OK**」をクリックします。
   監査データが Excel テーブルにインポートされます。
2. Excel ワークブックを保存します。
3. 「検索」フィルタを使用してデータを解析できます。



7.5 ピボットテーブル レポートの作成

1. Excel テーブルに監査データをインポートするには、「**データのインポート**」ダイアログボックスで、「**ピボットテーブル レポート**」を選択します。

   既存のワークシートのセル A1 からデータを配置するには、「**既存のワークシート**」を選択したままにします。



   「**OK**」をクリックします。

   空のピボットテーブルがワークシートに表示されます。

2. 右側に表示される「**ピボットテーブルのフィールド リスト**」で、表示するフィールドを選択します。

ヒント
フィールドを追加する前に、データをフィルタリング表示できます。「**ピボットテーブルのフィールド リスト**」の「**レポートに追加するフィールドを選択してください**」ボックスで、フィールド名にポインタを移動した後、フィルード名の横に表示されるフィルタ用ドロップダウン矢印をクリックします。「**フィルタ**」メニューで、フィルタのオプションを選択します。

3. ピボットテーブルの表示形式は、「**ピボットテーブルのフィールド リスト**」のボックス間でフィールドをドラッグして指定できます。たとえば、ポリシーを変更したユーザーの名前とポリシー名を行のヘッダとして表示し、ポリシーに対してユーザーが実行したアクションを列のヘッダとして表示します。
4. ピボットテーブルをフィルタリング表示するには、「**ピボットテーブル ツール**」-「**オプション**」で、「**スライサーの挿入**」をクリックします。
5. 「**スライサーの挿入**」ダイアログボックスで、使用するスライサーを選択し、「**OK**」をクリックします。

   スライサーは、ワークシートの任意の場所にドラッグ＆ドロップすることで並び替えることができます。また、異なる色を指定するなど、スライサーをカスタマイズすることもできます。これには、まずスライサーを選択します。「**スライサー ツール**」-「**オプション**」で、「**スライサー スタイル**」をいずれか 1つ選択します。
6. ワークブックを保存します。

8 監査レポートの作成例: その他

ここでは、Microsoft Excel の既存のデータソースから新しいクエリを作成する方法について説明し、監査レポートの作成に使用できるクエリの例をさらに挙げています。

また、XML 形式で表示した、詳細なポリシー変更内容を含むレポートを作成する方法についても説明します。

8.1 既存のデータソースからのクエリの作成

データベース接続の設定 (p. 9)で作成したデータソースから、さらに別の監査レポートを作成する方法は次のとおりです。

1. Excel の「**データ**」タブで、「**その他のデータソース**」をクリックした後、「**Microsoft Query**」をクリックします。
2. 「**データ ソースの選択**」ダイアログボックスで、「**クエリ ウィザードを使ってクエリを作成/編集する**」チェックボックスを選択から外します。先ほど作成したデータソース (例: SophosAuditing) を選択し、「**OK**」をクリックします。
3. 「**Microsoft Query**」で「**SQL**」ボタンをクリックして、作成するレポート用の SQL ステートメントを入力します。

ステートメントの例は、次のセクションを参照してください。

8.2 その他のクエリの例

例 1: 過去 60日間に特定のユーザーによって変更されたポリシー

```
SELECT EventId, Timestamp, TargetSubType, Action, TargetName, ParameterType,
 ParameterValue, Result

FROM SophosSecurity.Reports.vAuditEventsAll

WHERE (Timestamp>=DATEADD(dd,-60,GETUTCDATE()))
AND (TargetType='Policy')
AND (UserName='GS22K8R264¥Administrator')

ORDER BY Timestamp DESC
```

注
ステートメントでは、レポートに含める各フィールドを記載する代わりに、「SELECT *」と入力して、データベースビューにあるすべてのフィールドを指定することもできます。

例 2: 過去 6カ月間に特定のグループに対して適用されたポリシー

```
SELECT *

FROM SophosSecurity.Reports.vAuditEventsAll

WHERE (Timestamp>=DATEADD(mm,-6,GETUTCDATE()))
AND (TargetType='Policy')
AND (Action='Assign')
AND (ParameterType='Group')
AND (ParameterValue='¥Oxford¥UK-Servers')

ORDER BY EventId DESC
```

注
レポートの作成対象グループが、別のグループのサブグループである場合は、グループへのフルパスを入力するか、末尾を指定する記述をステートメントで使用する必要があります (グループ名が固有の場合)。たとえば、¥Oxford¥UK-Servers グループに関するレポートを作成する場合は、次のいずれかのように入力できます。

- ParameterValue='¥Oxford¥UK-Servers'
- ParameterValue Like '%UK-Servers'

例 3: 過去 3カ月間に特定のユーザーによって変更されたグループの変更内容

以下のステートメントを指定すると、過去 3ヵ月間に特定のユーザーによって、作成・削除・名前が変更されたグループ、およびグループに割り当てられたコンピュータ名に関するレポートが生成されます。

```
SELECT *

FROM SophosSecurity.Reports.vAuditEventsAll

WHERE (Timestamp>=DATEADD(mm,-3,GETUTCDATE()))
AND (UserName='GS22K8R264¥Administrator')
AND ((TargetType='Group') OR ((TargetType='Computer') AND (Action='Assign')))
```

例 4: 過去 3カ月間に特定のグループに加えられた変更

```
SELECT *

FROM SophosSecurity.Reports.vAuditEventsAll

WHERE (Timestamp>=DATEADD(mm,-3,GETUTCDATE()))
AND (ParameterValue='¥Oxford¥UK-Desktops')
```

8.3 Excel にデータを返す

監査レポート用のクエリを作成したら、Excel にデータを返し (「**ファイル**」 > 「**Microsoft Excel にデータを返す**」)、テーブルの作成 (p. 13)またはピボットテーブル レポートの作成 (p. 14)の説明に従ってレポートを作成してください。

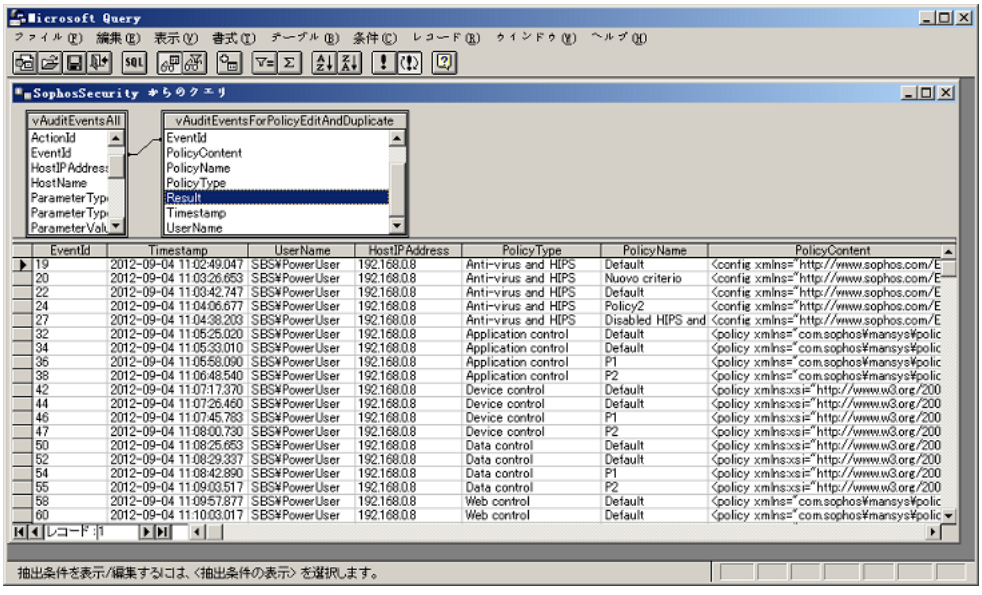
8.4 ポリシー変更に関する XML 形式のレポートの作成

ユーザーが編集したポリシーの設定内容は XML 形式で保存され、**Reports.vAuditEventsForPolicyEditAndDuplicate** データベースビューからアクセスできます。

この追加データを含むレポートは、2つのテーブル、**Reports.vAuditEventsAll** および **Reports.vAuditEventsForPolicyEditAndDuplicate** をリンクすることで作成できます。

1. 既存のデータソースからのクエリの作成 (p. 16)の説明に従って、既存のデータソースから新しいクエリを作成します。
2. 「**Microsoft Query**」で、「**テーブル**」-「**テーブルの追加**」をクリックします。「**テーブルの追加**」ダイアログボックスで、「**vAuditEventsForPolicyEditAndDuplicate**」を選択して、「**追加**」をクリックします。操作後、「**閉じる**」をクリックします。
3. 両方のテーブルに共通するフィールドをリンクすることで、2つのテーブルをリンクします。1つ目のテーブルにある共通のフィールド「**EventID**」をクリックしたまま、2つ目のテーブルの「**EventID**」フィールドにマウスを移動します。
4. 各フィールドをダブルクリックして、クエリに追加します。または、テーブルから表示エリアにドラッグして、フィールドをクエリに追加することもできます。

ヒント
Microsoft Query の「**結合**」ダイアログ (「**テーブル**」 > 「**結合**」) を使用しても、2つのテーブルを結合するクエリを作成できます。



5. クエリを保存するには、「**ファイル**」メニューで「**上書き保存**」をクリックします。
6. Excel に戻るには、「**データを返す**」ボタンをクリックします。

または、「**ファイル**」メニューで、「**Microsoft Excel にデータを返す**」をクリックします。

Excel に戻ると、「**データのインポート**」ダイアログボックスが表示されます。テーブルを作成します (テーブルの作成 (p. 13))。「**PolicyContent**」カラムに、XML 形式でポリシー設定の変更内容が表示されます。

ヒント
Microsoft SQL Server Management Studio を使用している場合は、直接、**Reports.vAuditEventsForPolicyEditAndDuplicate** ビューをクエリできます。そして、クエリ結果の「**PolicyContent**」カラム内のリンクをたどると、Excel のテーブルより読みやすい形式で、ポリシーの内容が XML エディタに表示されます。

9 監査されるアクション

監査対象のアクションのカテゴリは次のとおりです。

- コンピュータによるアクション
- コンピュータグループの管理
- ポリシーの管理
- ロールの管理
- Sophos Update Manager の管理
- システムイベント

9.1 コンピュータによるアクション

監視されるコンピュータによるアクションは次のとおりです。

- 警告およびエラーの消去/対処
- コンピュータの保護
- コンピュータのアップデート
- コンピュータの削除
- コンピュータでのシステムのフル検索の実行

9.2 コンピュータグループの管理

ログに記録されるグループの管理に関するアクションは次のとおりです。

- グループの作成
- グループの削除
- グループの移動
- グループ名の変更
- グループへのコンピュータの割り当て

9.3 ポリシーの管理

ログに記録されるポリシーの管理に関するアクションは次のとおりです。

- ポリシーの作成 (p. 21)
- ポリシー名の変更
- ポリシーの複製 (p. 21)
- ポリシーの編集
- コンピュータへのポリシーの適用

- ポリシーの製品出荷時へのリセット
- ポリシーの削除 (p. 21)

9.3.1 ポリシーの作成

ポリシーを新規作成すると、デフォルトポリシーが「新規ポリシー」という名称で複製されます。新規ポリシーの名前は、作成後、直ちに変更できます。たとえば、ウイルス対策および HIPS ポリシーを新規作成し、「サーバー」に名前を変更した場合、次のような監査エントリが作成されます。

表 1：新しいポリシーを作成して、名前を変更する

Action	Target Type	Target SubType	Target Name	Parameter Type	Parameter Value	Result
Duplicate	Policy	Anti-virus and HIPS	Default	New name	New Policy	Success
Rename	Policy	Anti-virus and HIPS	New Policy	New name	Servers	Success

9.3.2 ポリシーの複製

ポリシーを複製すると、「ポリシーの複製」イベントが作成されます。例:

表 2：ポリシーの複製

Action	Target Type	Target SubType	Target Name	Parameter Type	Parameter Value	Result
Duplicate	Policy	Web Control	TestPolicy1	New name	Copy of TestPolicy1	Success

9.3.3 ポリシーの削除

ポリシーを削除すると、削除されたポリシーを使用していたグループは、デフォルトポリシーを使用するようになります。この場合、デフォルトポリシーが再適用されたことを示す監査イベントは、新しく作成されません。

9.4 ロールの管理

ログに記録されるロールの管理に関するアクションは次のとおりです。

- ロールの作成
- ロールの削除
- ロール名の変更

- ロールの複製
- ロールへのユーザーの追加
- ロールからのユーザーの削除
- ロールへの権限の追加
- ロールからの権限の削除

9.5 Sophos Update Manager の管理

ログに記録される Sophos Update Manager の管理に関するアクションは次のとおりです。

- アップデートマネージャのアップデート
- アップデートマネージへの環境設定の適用
- 警告の消去
- アップデートマネージャの削除
- アップデートマネージャの設定

9.5.1 アップデートマネージャの環境設定変更の記録

Enterprise Console の「**アップデートマネージャの環境設定**」ダイアログボックスにあるタブや環境設定オプションを使用して、アップデートマネージャの環境設定をポリシーとして指定できます。アップデートマネージャの環境設定を編集すると、次のポリシーに対してアクションが記録されます。

- **Update Manager - subscription**: アップデートマネージャで最新の状態に保つソフトウェアのサブスクリプションを指定します。
- **Update Manager - upstream**: アップデートマネージャのアップデート元を指定します。
- **Update Manager - downstream**: アップデートマネージャによるソフトウェアのダウンロード先共有フォルダを指定します。
- **Update Manager - schedule**: アップデートマネージャが、脅威検出データおよびソフトウェアのアップデート版をチェックする頻度を指定します。
- **Update Manager - general**: アップデートマネージャのログオプションを指定します。
- **Software subscription**: 「推奨バージョン」など、ソフトウェアのサブスクリプションの内容を指定します。

1つのアップデートマネージャ ポリシーを変更することで、他のアップデートマネージャ ポリシーが変更されることもあります (パラメータ ID 値が変更された場合など)。このような場合、実行した 1つの変更に対して、複数のレコードが SophosSecurity データベースに記録されます。たとえば、「**アップデートマネージャの環境設定**」ダイアログボックスの「**スケジュール**」タブでスケジュールを設定して「OK」をクリックすると、次のような監査エントリが作成されます。

表 3：アップデートマネージャのアップデートスケジュールを作成する

EventId	Action	Target Type	Target SubType	Target Name	Parameter Type	Parameter Value	Result
22	Edit	Policy	Update Manager - schedule	New name	None		Success
21	Edit	Policy	Update Manager - upstream	New Policy	None		Success
20	Edit	Policy	Update Manager - subscription n		None		Success

この場合、「**Update Manager - schedule**」ポリシーに対してログ記録された最初のアクションのみが、実際の環境設定の変更を意味します。このイベントに対してログ記録された他のポリシー変更は、内部パラメータ ID の変更です。変更内容を確認するには、ポリシー変更に関する XML 形式のレポートの作成 (p. 18)で説明されている SophosSecurity データベースの「**Reports.vAuditEventsForPolicyEditAndDuplicate**」ビューを参照してください。

9.6 システムイベント

監視されるシステムイベントは次のとおりです。

- 監査の有効化
- 監査の無効化

10 Sophos Auditing のデータフィールド

Sophos Auditing で利用できるデータベースビューやデータソースは次のとおりです。

- Reports.vAuditEventsAll
- Reports.vAuditEventsForPolicyEditAndDuplicate

これらの各データソースで利用可能なデータフィールドは、以下を参照してください。日時データはすべて yyyy-mm-dd hh:mi:ss という形式の世界協定時 (24時間形式) で返されます。両方のビューに共通したフィールドは、太字で表記されています。

Reports.vAuditEventsAll

「**Reports.vAuditEventsAll**」データベースビューには、監査イベントの一覧と監査情報のほぼ全体が含まれます。

データフィールド	データ型	説明
EventId	integer	イベントの固有の数値 ID。
Timestamp	datetime	イベントにログ出力されたアクションの発生日時。
Action	nvarchar(128)	イベントにログ出力されたアクション。例: Create、Edit、Rename、Assign、Delete など。
TargetType	nvarchar(128)	アクションによって変更されたオブジェクトや設定のタイプ。例: Group、Computer、Policy、Role など。
TargetSubType	nvarchar(128)	アクションによって変更されたオブジェクトや設定のサブタイプ (該当する場合)。変更されたポリシーの種類。例: Anti-virus and HIPS、Data control など。
TargetName	nvarchar(4000)	アクションによって変更されたオブジェクトや設定の名前。例: ユーザー定義のポリシーやグループの名前。
ParameterType	nvarchar(128)	対象に適用された新しい設定やオブジェクトのタイプ。例: Action='Rename'と TargetType='Policy' に対して、ParameterType='New name'。Action='Assign' と TargetType='Computer' に対して、ParameterType='Group'。
ParameterValue	nvarchar(4000)	新しい設定やオブジェクトの名前。例: 新しいポリシーやコンピュータを割り当てた新しいグループのユーザー定義の名前など。

データフィールド	データ型	説明
Result	nvarchar(128)	アクションの結果 (Success、Failure)。
UserName	nvarchar(256)	アクションを実行したユーザーの名前。
HostName	nvarchar(256)	アクションの実行にユーザーが使用したコンピュータの名前。
HostIPAddress	nvarchar(48)	アクションの実行にユーザーが使用したコンピュータの IP アドレス。サーバーと Enterprise Console 間のネットワーク接続に IPv6 が使用される場合、IPv6 のアドレスが記録されます。それ以外の場合は、IPv4のアドレスが記録されます。
ActionId	integer	アクションの固有の数値 ID。
TargetTypeId	integer	対象タイプの固有の数値 ID。
TargetSubTypeId	integer	対象サブタイプの固有の数値 ID。
ParameterTypeId	integer	パラメータのタイプの固有の数値 ID。
SubEstateId	integer	ユーザーのサブ管理サイトの固有の数値 ID。
ResultId	integer	結果の固有の数値 ID。1 (成功)、0 (失敗)。
UserSid	nvarchar(128)	ユーザーのセキュリティ ID 。

Reports.vAuditEventsForPolicyEditAndDuplicate

Reports.vAuditEventsForPolicyEditAndDuplicate データベースビューには、ポリシーの変更に関する情報が含まれます。

データフィールド	データ型	説明
EventId	integer	イベントの固有の数値 ID。
Timestamp	datetime	イベントにログ出力されたアクションの発生日時。
Action	nvarchar(128)	イベントにログ出力されたアクション。
Result	nvarchar(128)	アクションの結果 (Success、Failure)。
PolicyType	nvarchar(128)	アクションによって変更されたポリシーの種類。例: Anti-virus and HIPS、 Web control など。

データフィールド	データ型	説明
PolicyName	nvarchar(4000)	ユーザー定義のポリシー名。
PolicyContent	XML	ポリシー設定の変更内容のスニペット (XML 形式)。
UserName	nvarchar(256)	アクションを実行したユーザーの名前。

11 トラブルシューティング

Sophos Auditing でエラーが発生すると、ソース名が「Sophos Auditing」というイベントが Windows のアプリケーションのイベントログに作成されます。通常、データベースの接続に問題がある場合に発生します。

12 補足: データフィールド値の数値 ID

Sophos Auditing のデータフィールドの値に対応する一意の ID 番号は、以下の表を参照してください。

エクスポートした監査データに外部ロジックをバインドする場合は、文字列ではなく、ID 番号を使用することを推奨します。これにより、今後の Enterprise Console のリリースで文字列が変更された場合でも、互換性の問題を回避できます。

データフィールド	データフィールド値	数値 ID
Action	Unknown	0
	Create	1
	Delete	2
	Duplicate	3
	Move	4
	Rename	5
	Add to	6
	Remove from	7
	Edit	8
	Log on	9
	Update	10
	Acknowledge	11
	Reset	12
	Assign	13
	Protect	14
	Scan	15
	Clean up	16
	Comply	17
TargetTyp e	Unknown	0
	Group	1
	Role	2
	Policy	3
	Computer	4
	Sub-estate	5
	AD synchronization point	6
	Report	7
	Update manager	8
	Configuration	9

データフィールド	データフィールド値	数値 ID
TargetSubType for TargetType=Policy	Legacy updating	1
	Anti-virus and HIPS	2
	Firewall	4
	Application control	7
	NAC	8
	Update Manager - upstream	9
	Update Manager - downstream	10
	Update Manager - general	11
	Update Manager - subscription	12
	Update Manager - schedule	13
	Data control	15
	Device control	16
	Software subscription	17
	Updating	18
	Tamper protection	19
	Web control	22
	Exploit prevention	30
TargetSubType for TargetType=Configuration	Unknown	0
	Dashboard	1
	Email alerts	2
	Purge	3
	Auditing	4
ParameterType	None	0
	New name	1
	New location	2
	Group	3
	User/Group	4
	Right	5
	Computer	6
	Alert	7
	Error	8
	Software update alert	9
	Configuration value	10

データフィールド	データフィールド値	数値 ID
Result	Pending	0
	Success	1
	Failure	2

13 テクニカルサポート

ソフォス製品のテクニカルサポートは、次のような形でご提供しております。

- ユーザー コミュニティ サイト「Sophos Community」(英語) (community.sophos.com/) のご利用。さまざまな問題に関する情報を検索できます。
- ソフォス サポートデータベースのご利用。www.sophos.com/ja-jp/support.aspx
- 製品ドキュメントのダウンロード。www.sophos.com/ja-jp/support/documentation.aspx
- オンラインでのお問い合わせ。 https://secure2.sophos.com/ja-jp/support/contact-support/support-query.aspx

14 利用条件