Microsoft

マイクロソフト サーバー製品のログ監査ガイド

[データベースサーバーにおける監査]

ホワイトペーパー

発行日 : 2008 年 3 月 31 日
最新の情報　http://www.microsoft.com/ja/jp/

注意事項：

マイクロソフト（米国 Microsoft Corporation、及び同社が直接または間接に所有する法人を含みます。以下同じ。）は、本書の内容及び本書を使用した結　果について明示的にも黙示的にも一切の保証を行いません。また、マイクロソフトは、本書を使用した結果に関し、(i)金融商品取引法、税法その他関係法令の遵守、(ii)その正確性、完全性及びその他の一切について、当該利用者及びその組織に対し、直接間接を問わず、いかなる責任も負担するものではありません。

本書で使用した環境は次のとおりです。

・Windows Server 2003 R2, Standard Edition

・SQL Server 2005 Standard Editon Service Pack 2

目次

はじめに

このガイドは、マイクロソフトのサーバー製品を利用している企業の IT 担当者が、様々な法令や規制などの遵守にあたり、マイクロソフトのサーバー製品の標準機能を利用したログの収集及び監査について、その手順を記述するものです。

このガイドを利用することで、コンプライアンスにおいて IT 環境を評価する作業を効率化することを目的としています。

現在、経営/事業における IT の位置づけは、ますます重要度を増しつつあります。

金融商品取引法による財務報告の信頼性を確保するための内部統制や、企業にとって重要な資産である個人情報を漏えいしないための統制など、企業において幅広いコンプライアンスと内部統制環境の構築が求められています。

国内だけではなく、現在のグローバルな経営環境においては、国内の法令や規制だけではなく、ビジネスを展開する様々な国や団体の法令や規制に遵守する必要があります。

現在の経営環境において、企業の内外における IT 環境は、ますます重要度を増しており、グローバルなビジネスを展開している企業では、ネットワークは世界中に張り巡らされています。こうした環境においては、一つ一つのコンプライアンスの為の IT 基盤を構築するのではなく、将来のコンプライアンスに備えた IT 統制のプロセスと基盤を構築していく必要があります。

適切な IT 統制を行うためには、システム状態を把握するための管理基盤の確立、システムを利用するユーザーのアクセスコントロールは勿論のこと、不正利用などの有事に備えたログの記録及び監査が必要です。

しかしながら、システムの稼働状態やユーザーの操作について、すべてのログを収集し、内容を確認することは、実際の業務を行う上で現実的とは言えません。監査にかかる経費や人手の問題だけでなく、膨大なログのなかに重要な情報が埋もれてしまう危険性も考えられるためです。

そのような事態を回避するためには、本当に必要なログは何であるのか、またどのような手順でどのような点を確認する必要があるのかについて、明確にしておく必要があります。

ドキュメント構成

マイクロソフト サーバー製品におけるログ監査ガイドは、マイクロソフト サーバー製品群のログ監査を支援するために、監査が必要となる項目、及び監査手順を提示します。

本ガイドを構成するドキュメントは、次の通りです。

- ファイルサーバー上のファイル操作における監査

  対象製品：Windows 2000 Server /Windows Server 2003

  プログラムファイル、設定ファイル等のローカル ファイル、及びファイルサーバー上のドキュメント等のネットワーク共有されたファイルについて、誰がどのファイルに対してどのような操作を行ったのか監査する手順を示します。

- 印刷ジョブについての監査

  対象製品：Windows 2000 Server /Windows Server 2003

  プリントサーバーが管理するプリンタにて、誰がどのようなファイルを印刷したのか監査する手順を示します。

- タスクについての監査

  対象製品：Windows 2000 Server /Windows Server 2003

  タスク スケジューラー、AT コマンドにより、誰がどのようなタスクを登録、または実行したのか監査する手順を示します。

- データベースサーバーにおける監査

  対象製品： SQL Server 2005

  SQL Server 2005 の標準のプロファイラおよび C2 監査の設定の手順を示します。

  ※ 本ガイドに記載されている監査の設定には、事前に十分なパフォーマンス検証を行う必要があります。

- Active Directory 上の各種操作における監査

  対象製品：Windows Server 2003

  Active Directory 上でどのようなユーザー、グループが作成または削除されたのか、Domain Admins 等の強力な権限を持つセキュリティ グループに対し、どのようなユーザーが追加されたのか、またグループ ポリシーに対してどのような変更が行われたのか監査する手順を示します。

- データベースサーバーにおける監査のガイド

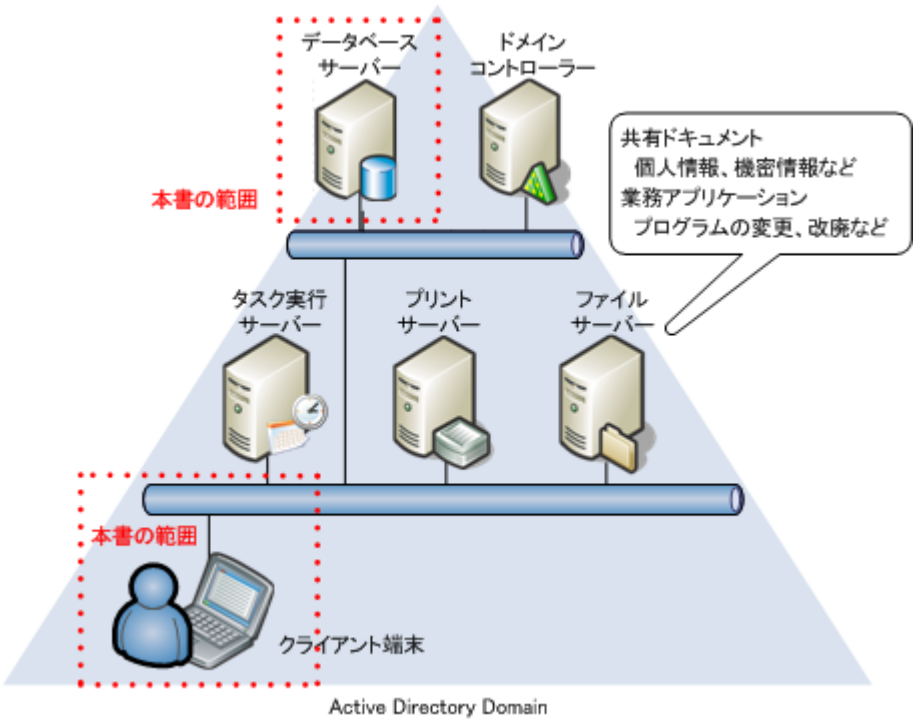
  対象製品：SQL Server 2005

  このドキュメントです。

  SQL Server プロファイラを利用し、データベースの操作ログを取得し、また取得した操作ログをテーブルに読み込み分析する方法について記述しています

環境と監査対象

本書では、監査対象環境の例示として、次の環境を想定します。



また、本ガイドにて監査対象とするデータベース操作を次に示します。

- データベースへのログインの成功と失敗
- オブジェクトへのアクセス（参照、挿入、更新、削除）
- オブジェクトの操作（作成、変更、削除）
- ユーザーの作成と権限付与

概要

データベースサーバーには、業務に携わる膨大な量の情報が格納されており、様々なシステムおよびユーザーにより、データの検索、登録、更新、削除などが実行されています。

重要なデータに対しては、適切なアクセス権を設定し、アクセスコントロールを実施することはもちろん、それに加えてログの取得及び監査を行うことで、不正利用を抑止し、また有事への対策強化をはかることができます。

本書では SQL Server2005 に付属している SQL Server プロファイラを利用し、データベースの操作ログを取得し、また取得した操作ログをテーブルに読み込み分析する方法について記述しています。

監査設定及び監査手順

監査証跡として記録する情報として、一般的に次のことが必要であると言われています。

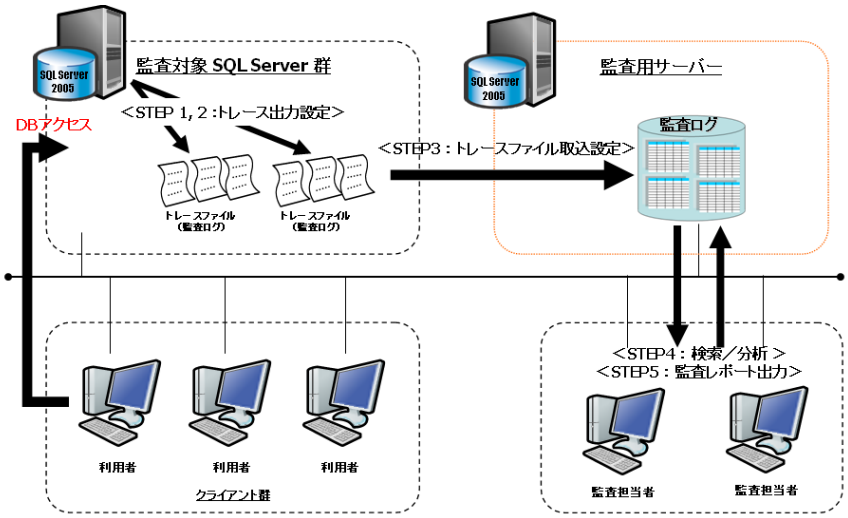
- いつ（When）
- 誰が（Who）
- どこから（Where）
- 何に対し（What）
- どのように操作したか（How）

SQL Server 2005 では、これらの操作について、SQL Server プロファイラにより監査を行うことができます。

本章では SQL Server プロファイラを使用することで、SQL Server に対し行われた各種操作に対して、これらの監査証跡情報を取得し分析するまでの手順を記述します。

監査設定の流れ

SQL Server プロファイラを使用し、SQL Server に対する監査を行うためには、監査対象 SQL Server 側に監査設定（トレース設定）を行い、監査対象 SQL Server が出力する監査ログ（トレースログ）を監査証跡とし、監査用 SQL Server に取り込み、管理及び検索、分析を行う事となります。



SQL Server に対する監査を行う場合は、以下の流れで設定を行います。

STEP1. 監査対象とする操作を選択し、設定する。

- SQL Server にてトレース設定を行う。
- トレース設定をスクリプト化する。

STEP2. 設定した監査を自動実行できるようにストアドプロシージャを作成する。

- STEP 1 で作成したスクリプトを自動実行できるようストアドプロシージャを作成する。
- 作成したストアドプロシージャをスタートアップに設定する。

STEP3. 監査対象 SQL Server より出力されるトレースログ（監査ログ）を監査用テーブルに取り込む設定をする。

- トレースログ（監査ログ）を監査テーブルに取り込むストアドプロシージャを作成する。
- 作成したストアドプロシージャを定期的に自動実行するためのジョブを登録する。

STEP4. 監査用テーブルに蓄積された監査ログを検索し、分析する。

STEP5. 監査レポートを出力する。

次ページより、上記の流れに従い設定および操作の手順をご説明します。

トレース定義スクリプトの生成

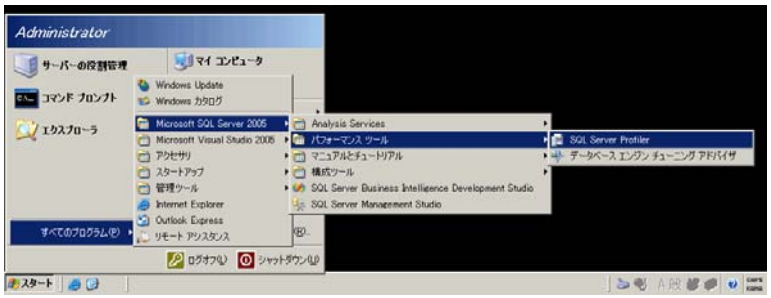
対象製品：SQL Server 2005

データベースの監査を行うためには、まず SQL Server Profiler にて、監査内容を定義したトレース定義スクリプトを生成します。

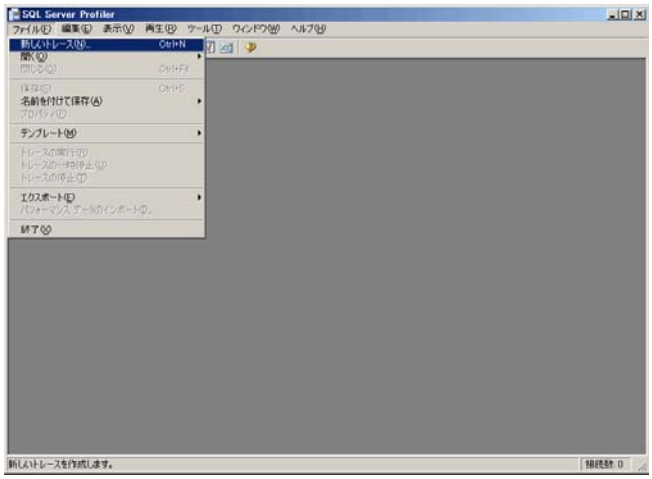
監査設定の追加手順を、次に示します。

1. 管理者アカウントにて、データベースサーバーにログオンします。

2. [スタート]メニューより、[すべてのプログラム]－[Microsoft SQL Server 2005]－[パフォーマンス ツール]と展開し、[SQL Server Profiler]をクリックします。

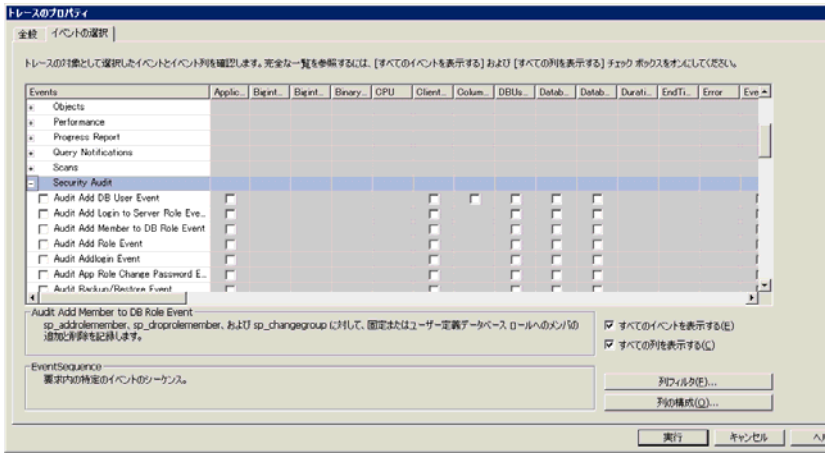


3. [SQL Server Profiler]が開いたら、[ファイル]メニューの[新しいトレース]をクリックします。

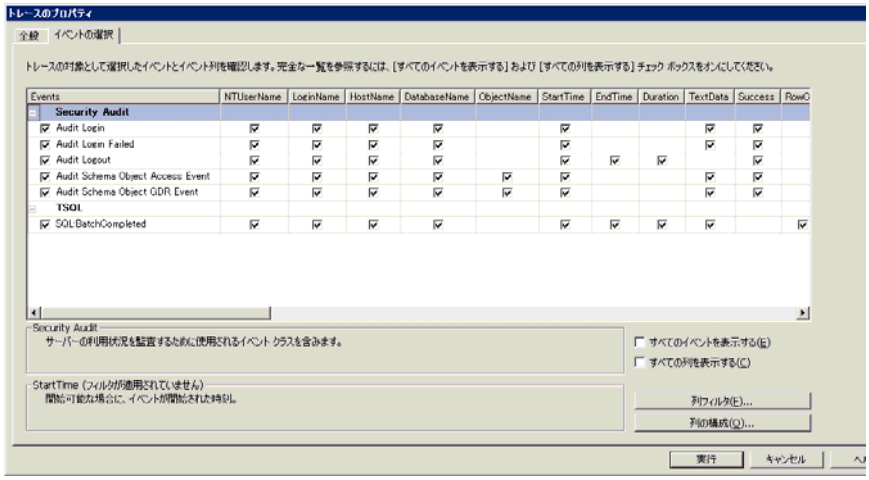


4. 認証ダイアログが表示されたら、管理者アカウントの認証情報を入力して、[接続]をクリックします。

5. [トレースのプロパティ]が開いたら、[イベントの選択]タブにて、“すべてのイベントを表示する”および“すべての列を表示する”にチェックをし、監査対象とするイベントと列を選択します。
本書での設定項目は“参考 1”をご覧下さい。



6. 監査対象とするイベントの選択および列の選択が終了したら[実行]をクリックします。



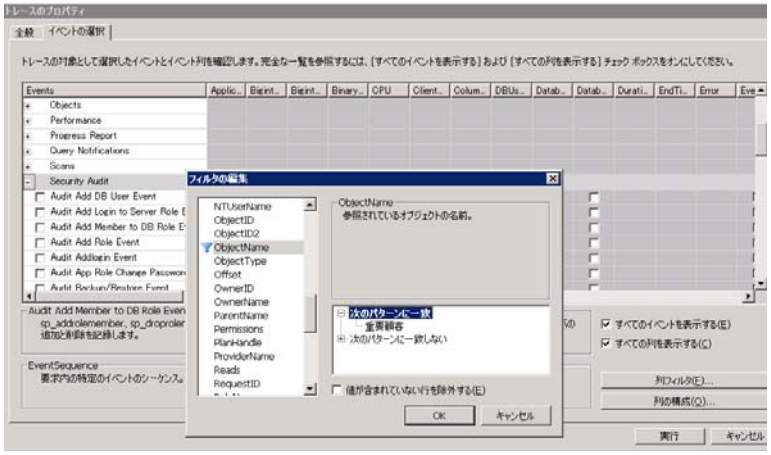
[補足 ： トレースログ出力量を絞るには]

トレースログの出力量は、監査対象とするイベントおよび列の数とシステムの利用頻度に大きく影響します。また、大量のトレースログの出力は監査対象サーバーのパフォーマンスに影響を与えるとともに、多くのリソースを必要とますので、実際の運用においては、監査に必要なトレースログのみを出力することが望ましいと言えます。

SQL Server Profiler では、必要なトレースログのみを取得するように、フィルタを設定することが可能です。例えば、特定のデータベース、テーブルまたは、アプリケーションのみをトレースログの出力対象とすることが可能です。

本書では、例として、監査対象を“重要顧客”テーブルへのアクセスとし、以下に設定の例をご紹介します。

SQL Server Profiler の[イベントの選択]、[列フィルタ]をクリックし[ObjectName]、[次のパターンに一致]に‘重要顧客’と入力し、[OK]をクリックします。

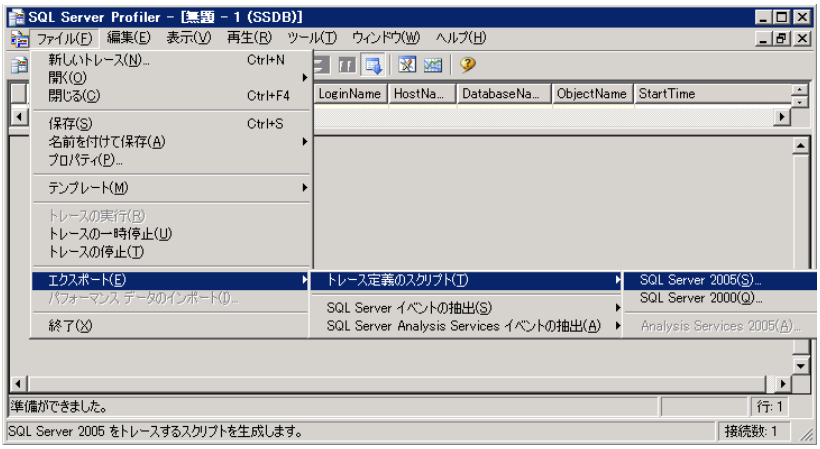


参考

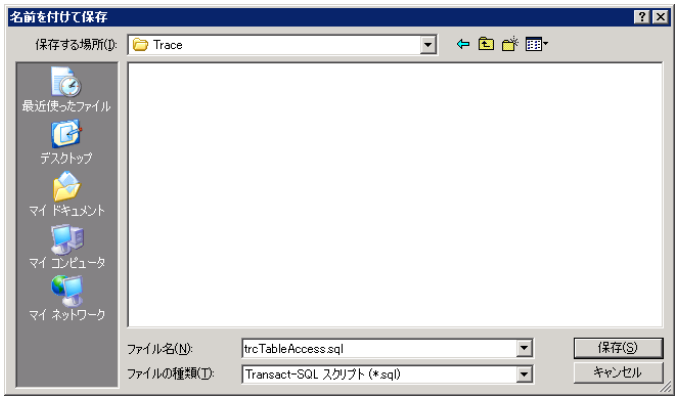
本ガイドでは次の項目に従い設定を行います。

監査項目	選択するイベント	選択する列
ログイン（成功／失敗）とログオフ	Security Audit ・Audit Login ・Audit Login Failed ・Audit Logout	・NTUserName(ユーザー) ・LoginName(ユーザー) ・HostName（端末情報） ・DatabaseName（DB名） ・StartTime（実施日時） ・Success（成否）
オブジェクトへのアクセス（参照/挿入/更新/削除）	Security Audit ・Audit Schema Object Access Event	・NTUserName(ユーザー) ・LoginName(ユーザー) ・HostName（端末情報） ・StartTime（実施日時） ・DatabaseName（DB名） ・ObjectName（テーブル） ・TextData（処理内容） ・Success（成否）
オブジェクトの操作（参照/挿入/更新/削除）	T-SQL ・SQL:BatchCompleted	・NTUserName(ユーザー) ・LoginName(ユーザー) ・HostName（端末情報） ・StartTime（実施日時） ・EndTime（終了日時） ・Duration（経過時間） ・DatabaseName（DB名） ・ObjectName（テーブル） ・TextData（処理内容） ・RowCounts（応答件数）
アクセス権限の操作	Security Audit ・Audit Schema Object GDR Event	・NTUserName(ユーザー) ・LoginName(ユーザー) ・HostName（端末情報） ・StartTime（実施日時） ・DatabaseName（DB名） ・ObjectName（テーブル） ・TextData（処理内容） ・Success（成否）

7. [SQL Server Profiler]に戻り、[ファイル]メニューより[エクスポート]ー[トレース定義のスクリプト]と展開し、[SQL Server 2005]をクリックします。

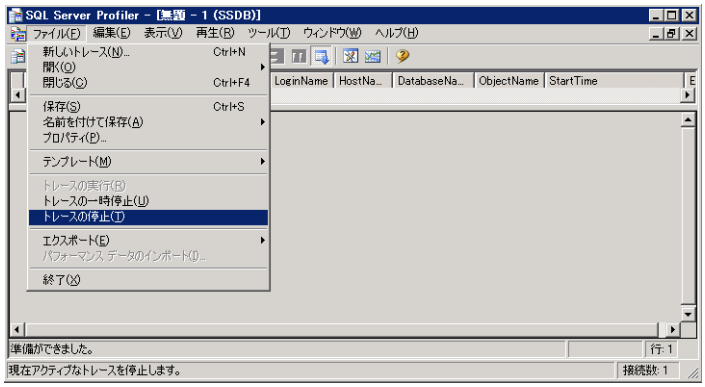


8. [名前をつけて保存]ダイアログが表示されたら、任意のディレクトリを選択し、[保存]をクリックします。



9. スクリプトファイルの保存が正常に完了した旨のメッセージボックスが表示されたら、[OK]をクリックします。

10. [SQL Server Profiler]に戻り、[ファイル]メニューより[トレースの停止]をクリックします。



以上で、トレース定義スクリプトの生成は終了となります。

トレース実行ストアドプロシージャの作成・設定

対象製品：SQL Server 2005

トレース定義スクリプトの生成が終了したら、定義した内容に従って自動的にトレースが行われるよう、トレース実行 ストアド プロシージャを作成し、スタートアップに設定します。

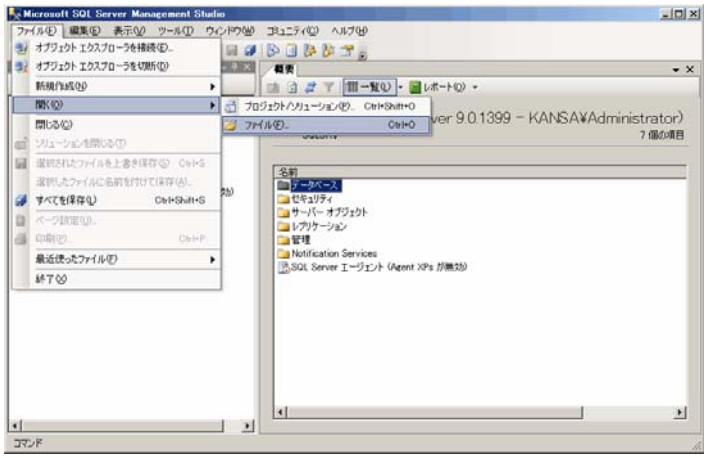
監査設定の追加手順を、次に示します。

1. 管理者アカウントにて、データベースサーバーにログオンします。

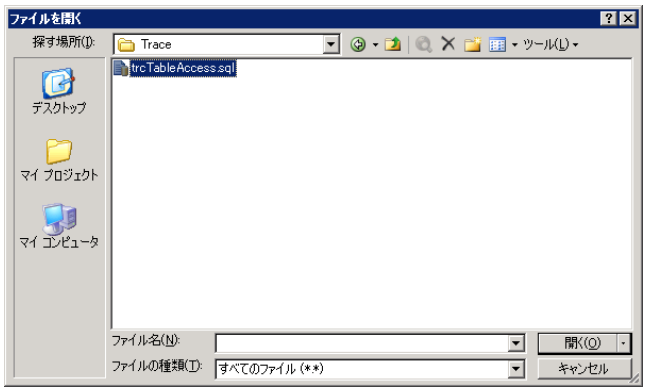
2. [スタート]メニューより、[すべてのプログラム]－[Microsoft SQL Server 2005]と展開し、[SQL Server Management Studio]をクリックします。

3. 認証ダイアログが表示されたら、管理者アカウントの認証情報を入力して、[接続]をクリックします。

4. [Microsoft SQL Server Management Studio]が開いたら、[ファイル]メニューより、[開く]ー[ファイル]をクリックします。

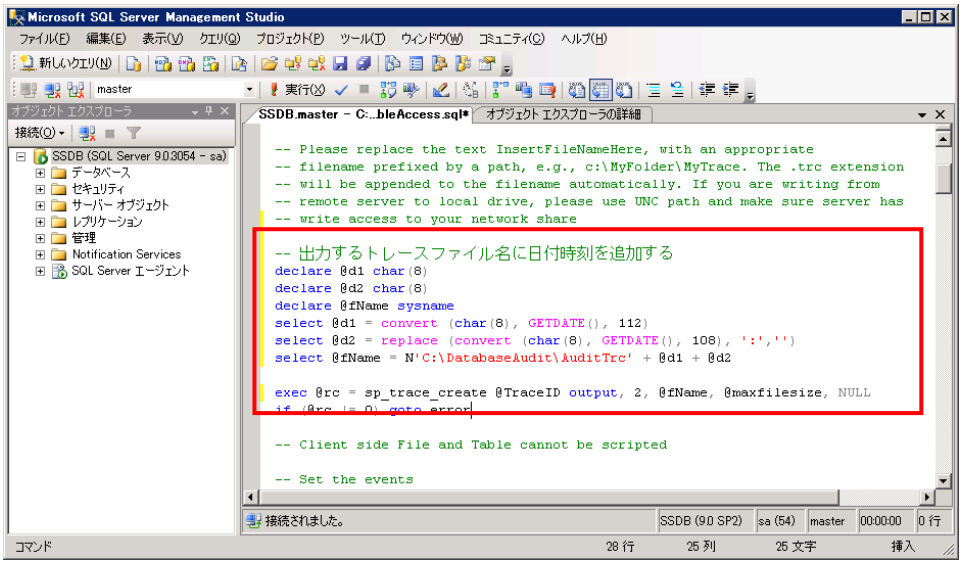


5. [ファイルを開く]ダイアログが表示されたら、」のNo.8 にて保存したファイルを選択し、[開く]をクリックします。



6. 認証ダイアログが表示されたら、管理者アカウントの認証情報を入力して、[接続]をクリックします。

7. トレース定義スクリプトが開いたら、出力するトレースファイルが上書きされないように、トレースファイル名に日付時刻を付与するロジックを追加します。また、[sp_trace_create]の第 2 引数の値を、0 から 2 に変更します。これにより、トレースファイルのサイズがの最大値（5MB）を超えた際に、自動的に次のファイルを作成し、トレース出力を継続させることができます。

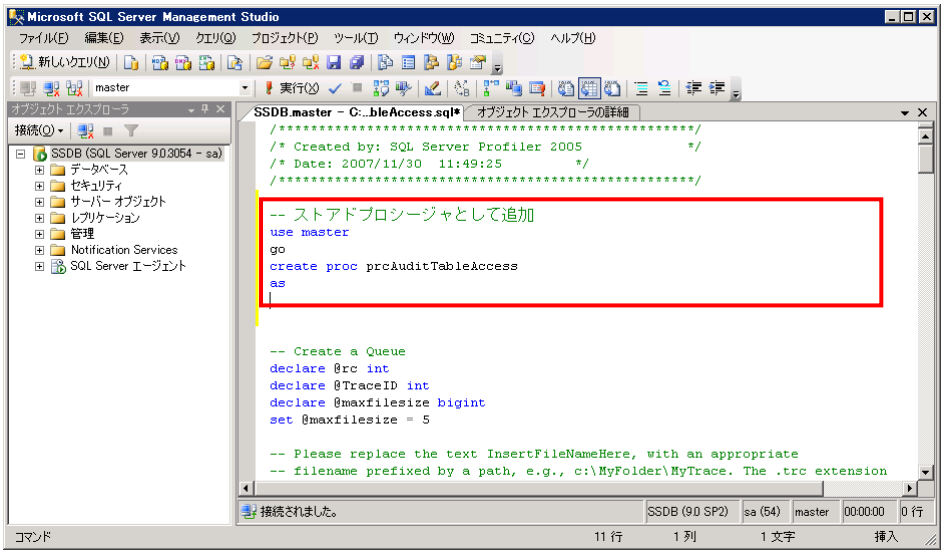



```
-- 以下のロジックを "set @maxfilesize = 5"の後に追記/改修
declare @d1 char(8)
declare @d2 char(8)
declare @fName sysname
select @d1 = convert (char(8), GETDATE(), 112)
select @d2 = replace (convert (char(8), GETDATE(), 108), ':', ``)
select @fName = FilePath + @d1 + @d2
exec @rc = sp_trace _create @TraceID output, 2, @fName, @maxfilesize,
NULL
```

[注意]

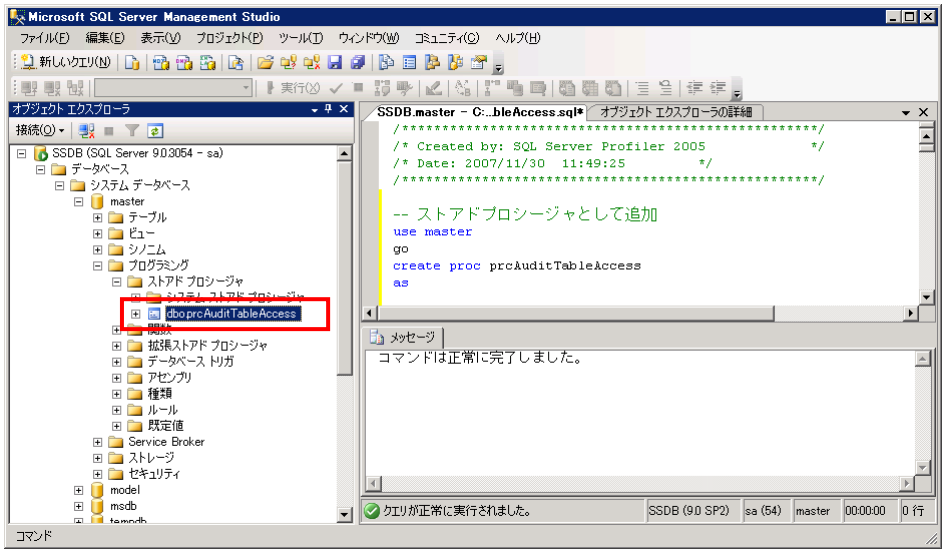
- ロジック中の「FilePath」は、トレースファイル出力先として指定する実際に存在するパスを指定して下さい。
- シングルコーテーションについては、コピー&ペーストを行うエラーとなる場合がありますので、直接入力して下さい。

8. ここまでの編集でトレース定義の変更が終了したら、[create proc]にて、トレース定義スクリプトを、ストアドプロシージャとして、[master]データベースに登録するロジックをスクリプト最上部に追加し、[実行]をクリックします。

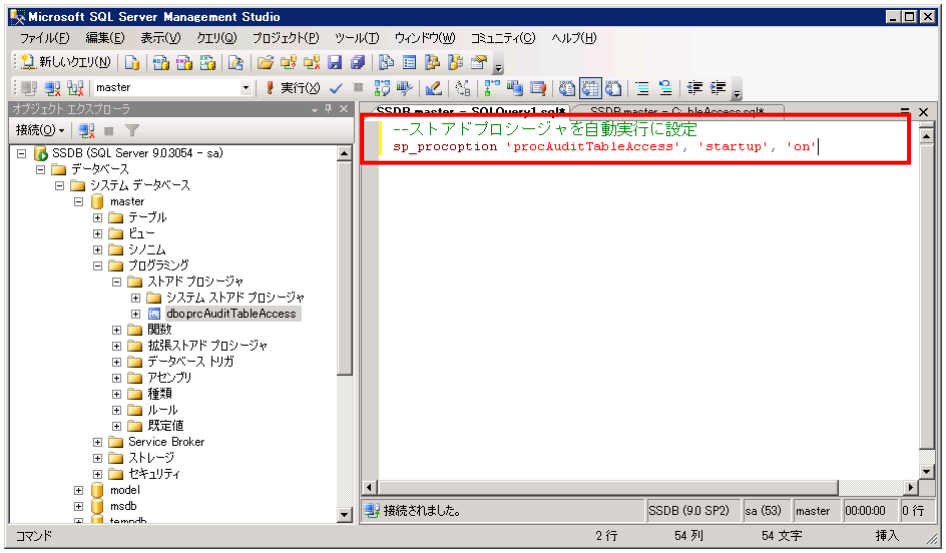



```
--以下のロジックを最上部に追記
use master
go
create proc procedureName
as
```

9. 左ペインのツリーより、[master]データベースの[システム ストアドプロシージャ]に、作成したストアド プロシージャが追加されていることを確認します。



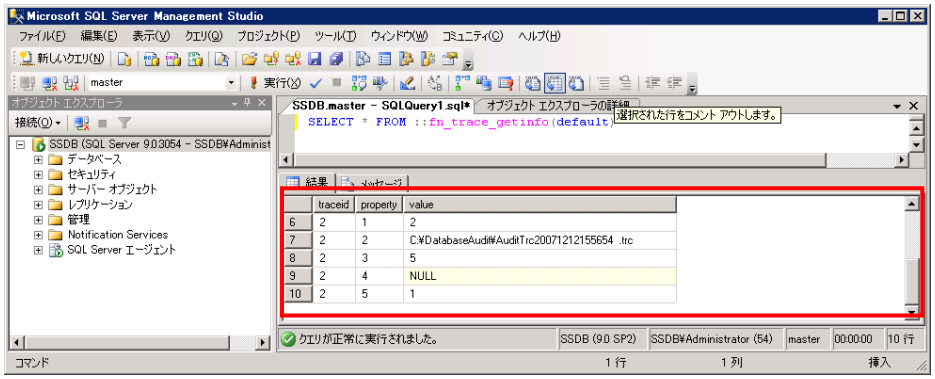
10. ストアドプロシージャの登録が完了したら、[sp_procoption]にて、ストアドプロシージャが自動実行されるよう、スタートアップに登録します。




```
--以下のクエリを master データベースに対して実行
sp_procoption ProceduerName, 'startup', 'on'
```

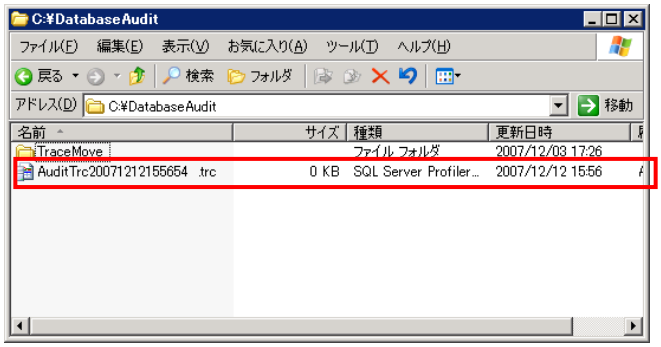
11. [サービス]管理画面にて、[SQL Server]サービスを再起動します。

12. SQL Server Management Studio より、コマンド入力しトレースが起動していることを確認します。[Property]の 2 は、指定したトレースファイル出力先が表示され、[Property]の 5 にて状態の確認（0＝停止、1＝動作中）が行えます。




```
--以下のクエリを master データベースに対して実行
SELECT * FROM ::fn_trace_getinfo(default)
```

13. №7 で指定したフォルダに、トレースファイルが出力されていることを確認します。



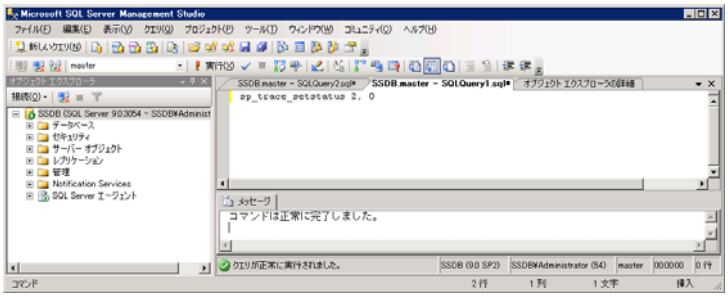
以上で、トレース実行ストアドプロシージャの作成・設定は完了となります。

【補足 ： トレースの起動と停止】

トレースは原則、常時動作していますが、なんらかの理由により、停止をしたり、起動する必要が発生します。下記に停止と起動の手順を記述します。

● 動作中のトレースを停止する。

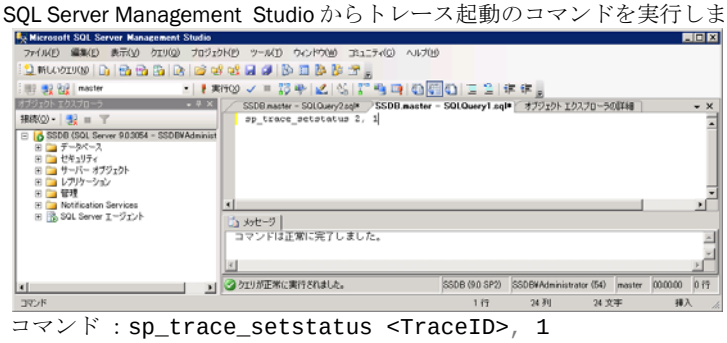
SQL Server Managemnt Studio からトレース停止のコマンドを実行します。



コマンド ： `sp_trace_setstatus <TraceID>, 0`

● 停止中のトレースを起動する。

SQL Server Management Studio からトレース起動のコマンドを実行します。



コマンド ：`sp_trace_setstatus <TraceID>, 1`

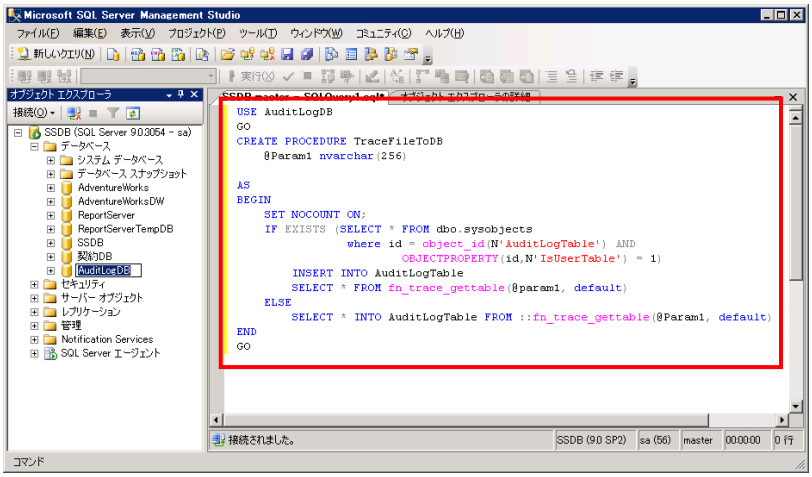
トレース ファイルをテーブルに挿入するストアドプロシージャを作成する

対象製品：SQL Server2005

監査設定の追加にて、トレースの自動実行設定が完了したら、トレース定義スクリプトに定義した内容に従って、トレースファイルが出力されるようになります。
日々出力されるトレースファイルを管理し、必要な時点で抽出を行うには、テーブルでトレースファイル中のトレースログを管理することが有効となります。

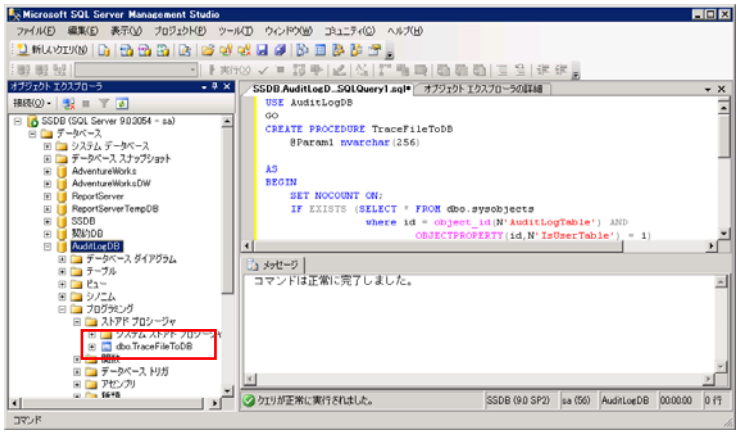
本節では、出力されたトレースログをテーブルに蓄積するストアドプロシージャの作成手順について記述します。

1. 管理者アカウントにてデータベースサーバーにログオンし、[Microsoft SQL Server Management Studio]を開きます。
2. [新しいクエリ]をクリックし、出力されたトレースファイルを SQL Server 上のテーブルに挿入するプロシージャを作成するクエリを実行します。




```
--以下のクエリを実行
USE master
GO
CREATE PROCEDURE TraceFileToDB
    @Param1 nvarchar(256)
AS
BEGIN
    SET NOCOUNT ON;
    IF EXISTS (SELECT * FROM dbo.sysobjects
                WHERE id =  object_id(N'TableName') AND
                      OBJECTPROPERTY(id,N'IsUserTable') = 1)
        INSERT INTO TableName
        SELECT * FROM fn_trace_gettable(@Param1, default)
    ELSE
        SELECT * INTO TableName FROM ::fn_trace_gettable(@Param1,
default)
END
GO
```

3. 左ペインのツリーより、[AuditLogDB]データベースの[システム ストアドプロシージャ]に、作成したストアド プロシージャが追加されていることを確認します。



トレース ログをテーブルに挿入するジョブを作成する

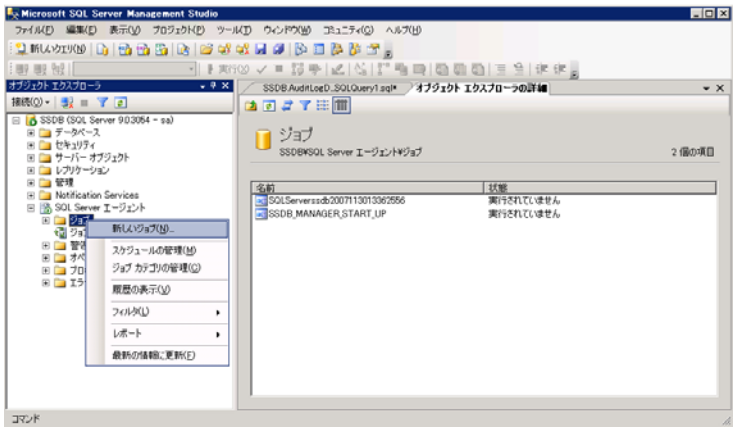
対象製品：SQL Server2005

トレースログをテーブルに挿入するストアドプロシージャの作成が完了したら、このプロシージャを定期的に呼び出し、自動的にトレースログの内容がテーブルに挿入されるようにジョブを作成します。

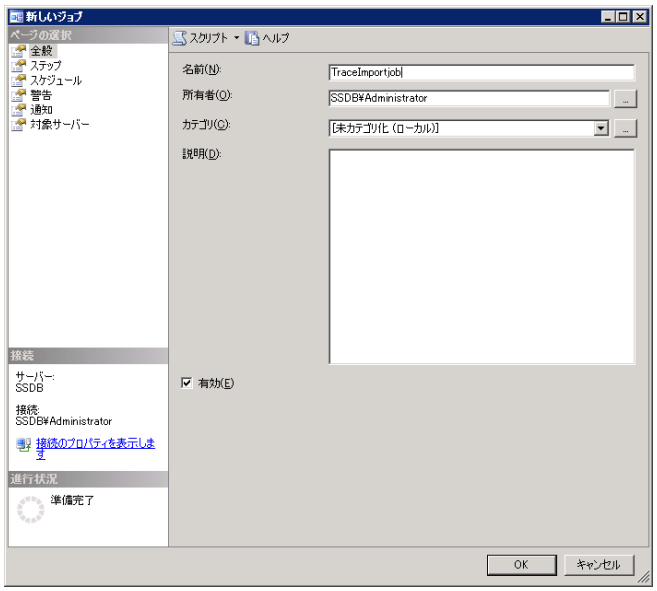
本節では、自動的にトレースログの内容がテーブルに挿入されるようにするジョブの作成手順およびテーブル挿入後のトレースファイルの移動処理に対する手順を記述します。

1. 管理者アカウントにてデータベースサーバーにログオンし、[Microsoft SQL Server Management Studio]を開きます。

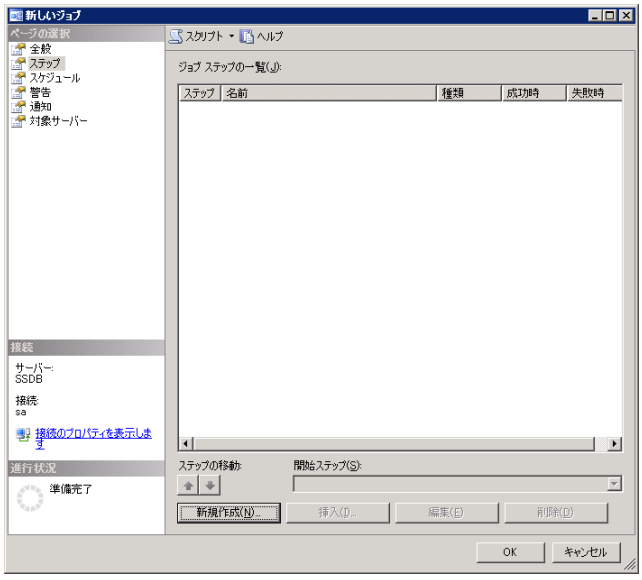
2. オブジェクトエクスプローラの「SQL Server エージェント」の下にある「ジョブ」を右クリックし、メニューより「新しいジョブ」をクリックします。



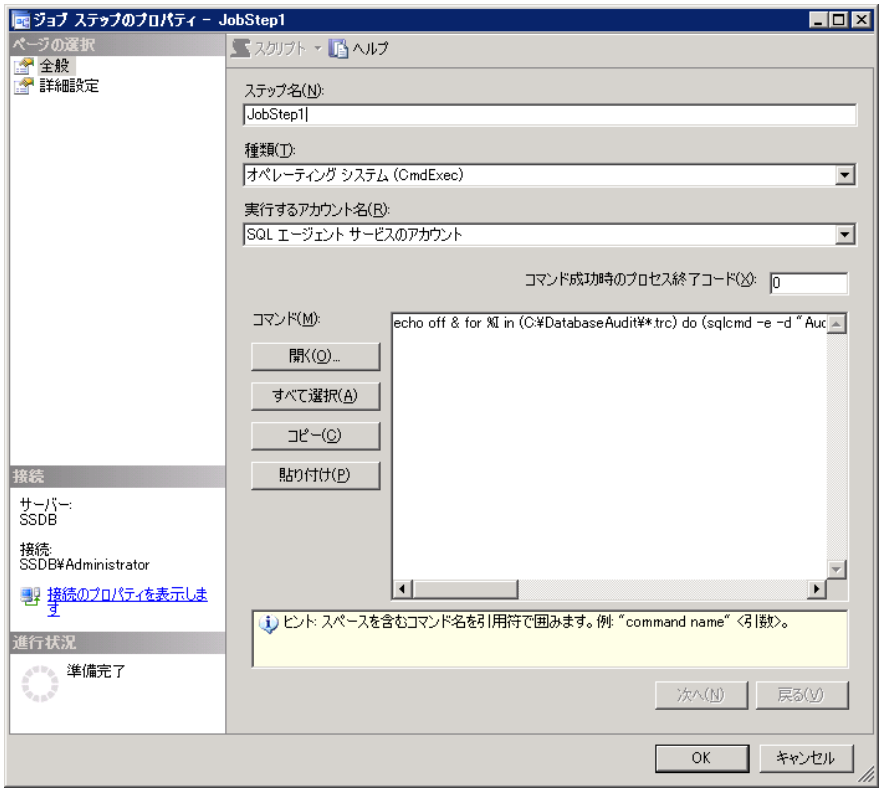
3. 「新しいジョブ」ダイアログが表示されたら、名前に任意の名前を入力します。



4. ページの選択で「ステップ」をクリックし、「新規作成」をクリックします。



5. テーブル挿入後のトレースファイルは、出力先として指定された場所から別の保管場所に移動する必要があります。次の手順にて移動の設定を行います。
「新しい ジョブステップ」ダイアログが表示されたら、ステップ名に任意の名前を入力、種類で「オペレーティングシステム（CmdExec）」を選択、コマンドに以下のコマンドを入力し、「OK」をクリックします。

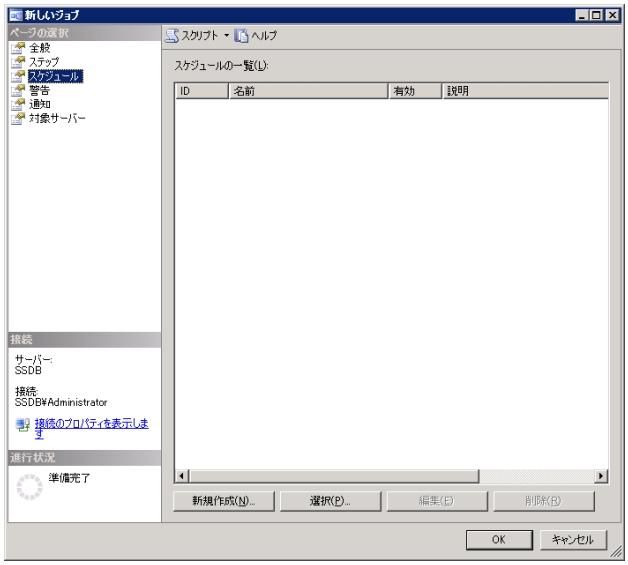



```
echo off & for %I in (TraceFilePath\*.trc) do (sqlcmd -e -d "master" -Q
"TraceFileToDB @Param1 = N'%I'" && move /Y "%I" "TraceMovePath\.">NUL &
if errorlevel 1 (echo %I ファイルは使用中です) else (echo %I を MOVE しました))
```

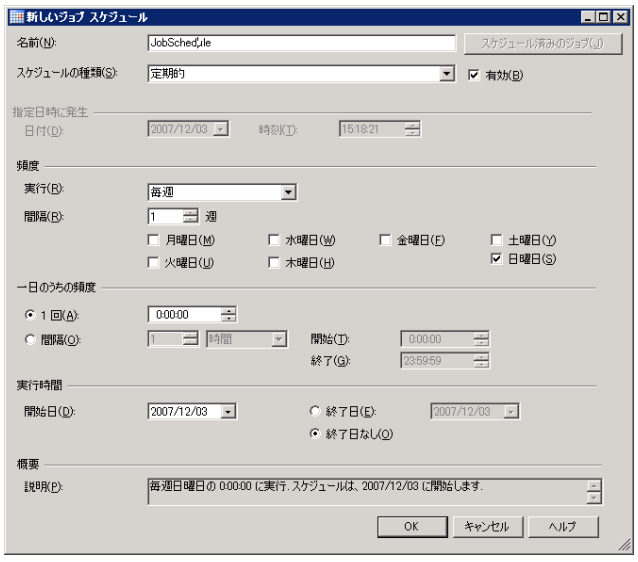
[注意]

- コマンドは 1 行で入力する必要があります。(改行等を入れるとエラーとなります。)
- コマンド中の「TraceFilePath」は前章でトレースファイル出力先として指定したパスを入力してください。また「TraceMovePath」には任意の存在するパスを入力してください。
- このコマンドは Windows 認証で DB に接続しています。SQLServer 認証を使用する場合にはコマンド中の「sqlcmd -e -d "master" -Q "TraceFileToDB @Param1 = N'%I'"」を「sqlcmd -U ＜ユーザ名＞ -P ＜パスワード＞ -d master -Q -Q "TraceFileToDB @Param1 = N'%I'"と置き換えてください。
- 移動先のフォルダには、トレースファイルが蓄積されます。定期的にディスク容量を確認の上で別媒体への退避または削除を実施してください。

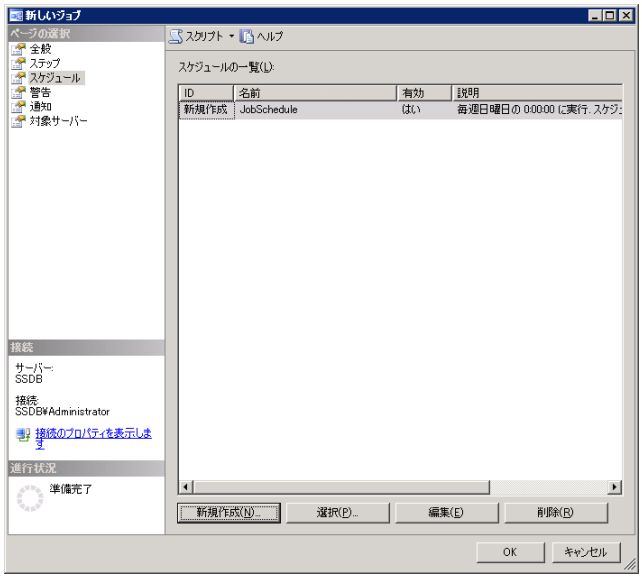
6. ページの選択で「スケジュール」をクリックし、「新規作成」をクリックします。



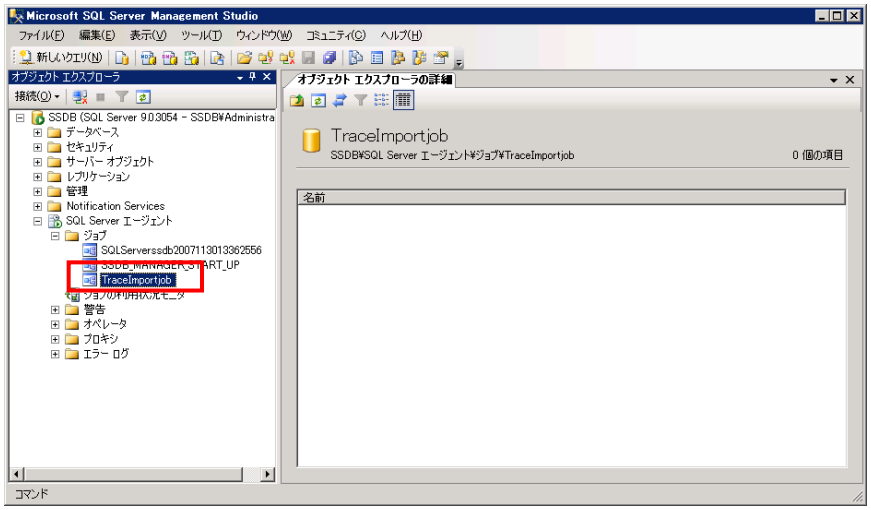
7. 「新しい ジョブスケジュール」ダイアログが表示されたら、名前に任意の名前を、スケジュールの種類、頻度などにトレースファイルをテーブルに読み込む頻度を入力し「OK」をクリックします。



8. 「新しいジョブ」ダイアログが表示されたら「OK」をクリックします。



9. 左ペインのツリーより、SQL Server エージェントの[ジョブ]に、作成したジョブが追加されていることを確認します。



トレース ログによる監査

対象製品：SQL Server 2005

テーブルに蓄積されたトレース ログを利用し、SQL Server2005 の監査を行うには、手順には、大量のトレースログの中から監査に必要な情報を効率的に抽出することが重要となります。

本節では、次の監査要件を例として、下記 2 つの方法で情報を抽出する手順について記述します。

- クエリの発行によるトレースログ監査
- SQL Server Profiler によるトレースログ監査

次の監査要件を例とします。

- 不正アクセスの疑いを検出（ログインの失敗を検出）
- 特定のテーブルに対する操作を抽出
- 改ざんの疑いを検出（特定のテーブルに対する更新の行為を検出）
- データ流出の疑いを検出（大量データの抽出を検出）

クエリの実行によるトレースログ監査

対象製品：SQL Server 2005

本節では、テーブルに蓄積されたトレース ログを Microsoft SQL Server Management Studio を利用しクエリを発行することで監査する手順について記述します。クエリを発行することで情報抽出が可能であり、分析をしたいイベントを選択し、更に条件を加えることで多くの情報から必要な情報を絞り込むことができます。

Microsoft SQL Server Management Studio からクエリを発行する場合には、SQL Server のイベント ID を知っている必要があります。本ガイドではよく利用されるイベントとイベント ID を記述します。

ID	イベント名	内容
12	SQL:BatchCompleted	T-SQL バッチが完了したときに発生
14	Audit Login	ユーザーが SQL Server に正常ログインしたときに発生
15	Audit Logout	ユーザーが SQL Server にログアウトしたときに発生
20	Audit Login Failed	ユーザーが SQL Server にログイン失敗したときに発生
102	Audit Statement GDR Event	SQL Server の任意ユーザーがステートメント権限の GRANT、DENY、REVOKE を実行したときに発生
103	Audit Object GDR Event	SQL Server の任意ユーザーがオブジェクト権限の GRANT、DENY、REVOKE を実行したときに発生
109	Audit Add DB User Event	データベースのユーザー（Windows 又は SQL Server）として、ログインが追加又は削除されたときに発生
113	Audit Statement Permission Event	CREATE TABLE などのステートメント権限が使用されたときに発生
114	Audit Schema Object Access Event	SELECT などのオブジェクト権限が使用されたときに発生
118	Audit Object Derived Permission Event	CREATE、ALTER および DROP のオブジェクトコマンドが実行されたときに発生

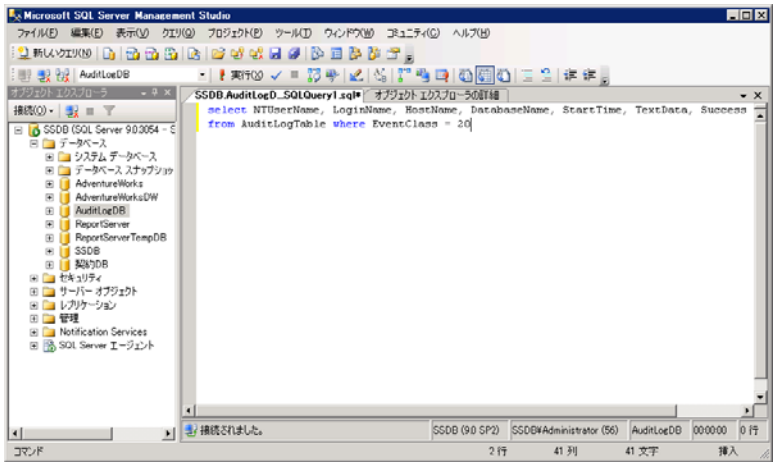
本節では、次の監査要件に対する抽出を行います。

- 不正アクセスの疑いを検出（ログインの失敗を検出）
- 特定のテーブルに対する操作を抽出
- 改ざんの疑いを検出（特定のテーブルに対する更新の行為を検出）
- データ流出の疑いを検出（大量データの抽出を検出）

ログインの失敗を検出

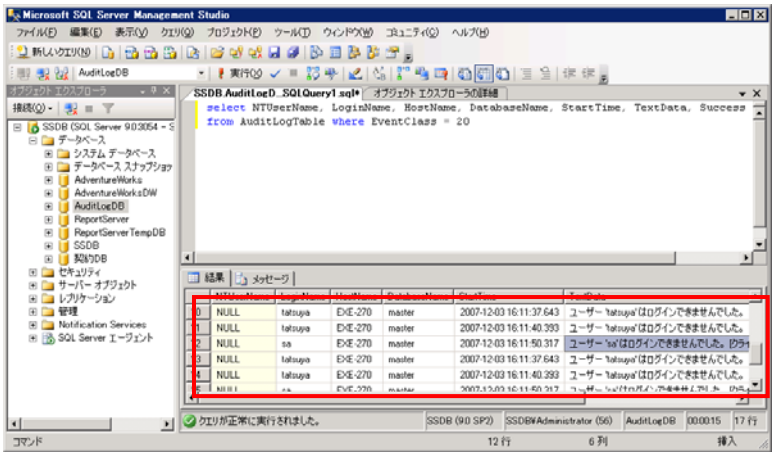
1. 管理者アカウントにてデータベースサーバーにログオンし、[Microsoft SQL Server Management Studio]を開きます。

2. 蓄積されたトレースログより必要な情報を取得するクエリを実行します。
ここでは、 ログイン失敗に関するイベントである“Audit Login Failed (EventClass=20)に 対し、[NTUserName]（実行ユーザー名）, [LohinName]（実行ユーザー名）, [HostName]（端末名）, [DatabaseName]（操作対象データベース名）,[StartTime]（操作開始日時）, [TextData]（操作内容）を取得するクエリを実行します。



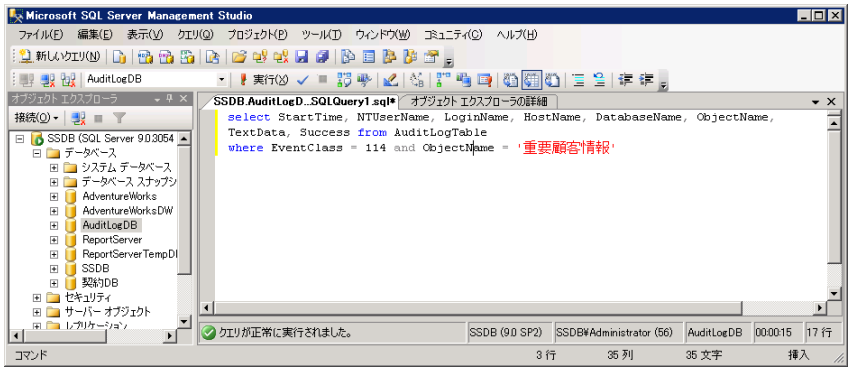

```
--以下のクエリを実行
Select
NTUserName, LoginName, HostName, DatabaseName, StartTime, TextData,
Success from TableName where EventClass=20
```

3. クエリの実行結果を確認します。



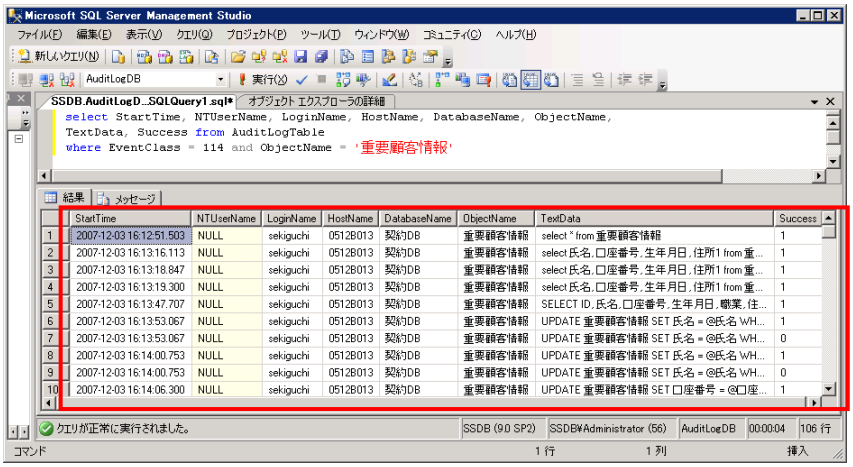
特定のテーブルに対する操作を抽出

1. 管理者アカウントにてデータベースサーバーにログオンし、[Microsoft SQL Server Management Studio]を開きます。
2. 蓄積されたトレースログより必要な情報を取得するクエリを実行します。ここでは、特定のテーブル（重要顧客情報）に対する操作全てを検出するためにオブジェクトへのアクセスに関するイベントである“Audit Schema Object Access Event (EventClass=114)” 対し、[NTUserName]（実行ユーザー名）, [LoginName]（実行ユーザー名）, [HostName]（端末名）, [DatabaseName]（操作対象データベース名）, [ObjectName]（テーブル名）,[StartTime]（操作開始日時）, [TextData]（操作内容）を取得するクエリを実行します。条件として、テーブル（ObjectName）に‘重要顧客情報’を指定します。



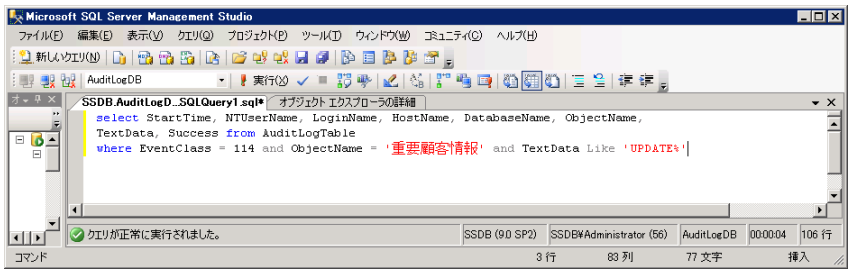

```
--以下のクエリを実行
Select
StartTime, NTUserName, LoginName, HostName, DatabaseName, ObjectName,
TextData, Success from TableName where EventClass= 114 and ObjectName
= '重要顧客情報'
```

3. クエリの実行結果を確認します。



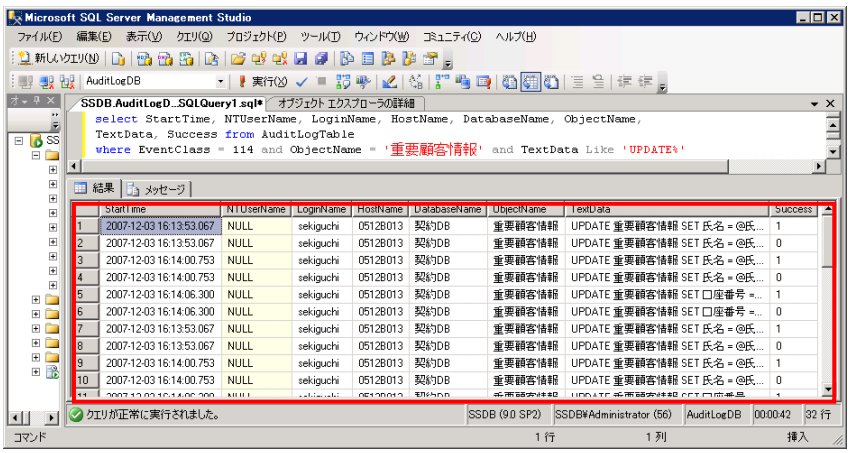
改ざんの疑いを検出

1. 管理者アカウントにてデータベースサーバーにログオンし、[Microsoft SQL Server Management Studio]を開きます。
2. 蓄積されたトレースログより必要な情報を取得するクエリを実行します。ここでは、特定のテーブル（重要顧客情報）に対する更新と削除の処理を検出するためにオブジェクトへのアクセスに関するイベントである“Audit Schema Object Access Event (EventClass=114)” 対し、[NTUserName]（実行ユーザー名）, [LoginName]（実行ユーザー名）, [HostName]（端末名）, [DatabaseName]（操作対象データベース名）, [ObjectName]（テーブル名）,[StartTime]（操作開始日時）, [TextData]（操作内容）を取得するクエリを実行します。条件として、テーブル（ObjectName）に‘重要顧客情報’を指定し、操作（TextData）にUPDATE（更新）を指定します。




```
--以下のクエリを実行
Select
StartTime, NTUserName, LoginName, HostName, DatabaseName, ObjectName,
TextData, Success from TableName where EventClass= 114 and ObjectName
= '重要顧客情報' and TextData like 'UPDATE%'
```

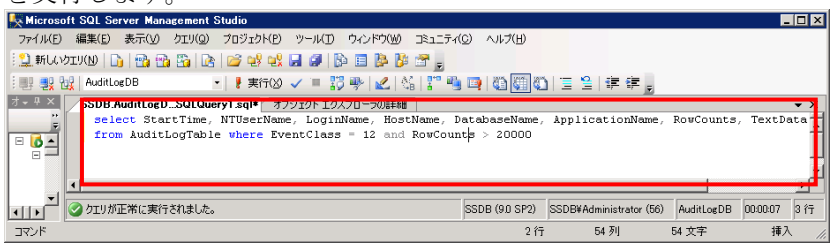
3. クエリの実行結果を確認します。



大量データの抽出を検出

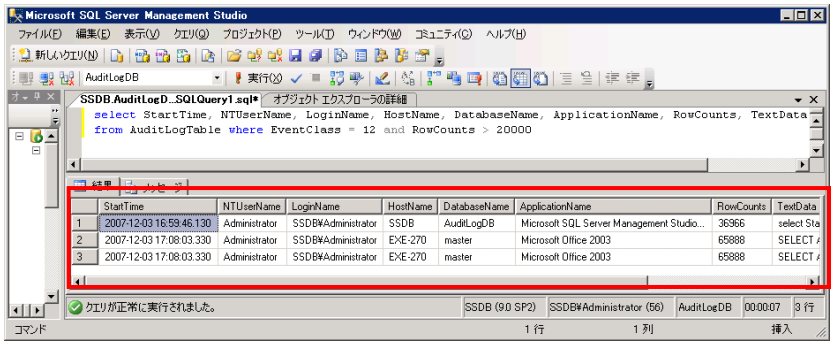
1. 管理者アカウントにてデータベースサーバーにログオンし、[Microsoft SQL Server Management Studio]を開きます。

2. 蓄積されたトレースログより必要な情報を取得するクエリを実行します。
ここでは、 大量のデータを抽出した行為を検出するため、
“SQL:BatchCompleted (EventClass=12)”の RowCounts(応答件数)が××以上のアクセスに 対し、[NTUserName]（実行ユーザー名）, [LoginName]（実行ユーザー名）, [HostName]（端末名）, [DatabaseName]（操作対象データベース名）,[StartTime]（操作開始日時） , [ApplicationName]（アプリケーション名）,[TextData]（操作内容）お呼び[RowCounts]（応答件数）を取得するクエリを実行します。




```
--以下のクエリを実行
Select StartTime, NTUserName, LoginName, HostName,DatabaseName,
ApplicationName, RowCounts, TextData from TableName
where EventClass= 12 and RowCounts > 0000
```

3. クエリの実行結果を確認します。



以上で、トレース ログによる監査手順は終了となります。

SQL Server Profiler によるトレース ログ監査

対象製品：SQL Server 2005

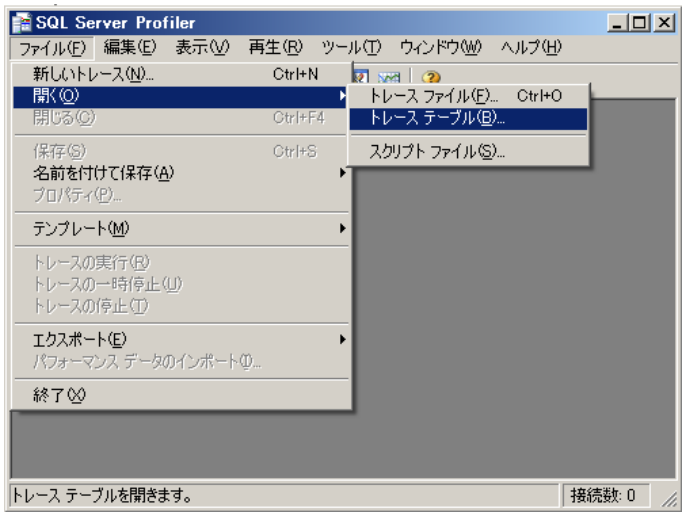
本節では、テーブルに蓄積されたトレース ログを SQL Server Profiler を利用し監査する手順について記述します。SQL Server Profiler では、フィルタによる情報抽出が可能であり、分析をしたいイベントを選択し、更に条件を加えることで多くの情報から必要な情報を絞り込むことができます。SQL Server Profiler では、GUI を通しての条件設定及びデータ抽出を行うことができます。

本節では、次の監査要件に対する抽出を行います。

- 不正アクセスの疑いを検出（ログインの失敗を検出）
- 特定のテーブルに対する操作を抽出
- 改ざんの疑いを検出（特定のテーブルに対する更新の行為を検出）

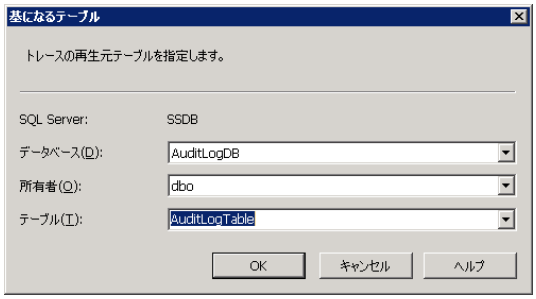
ログインの失敗を検出

1. [SQL Server Profiler]のファイルメニュー ー 開く ートレーステーブルを選択します。

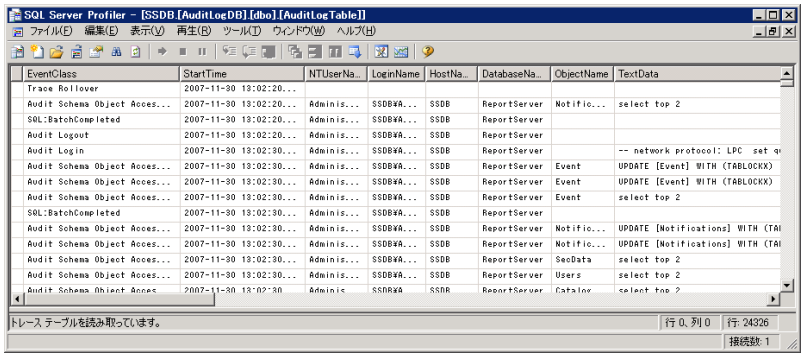


2. 管理者アカウントにてデータベースサーバーにログオンし、[SQL Server Profiler]を開きます。

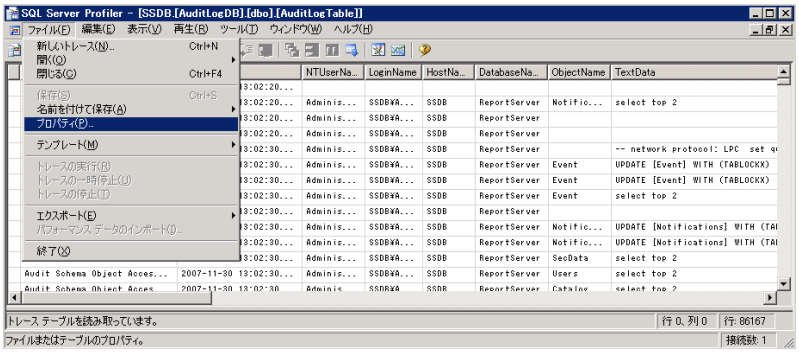
3. 対象となるテーブルを選択します。



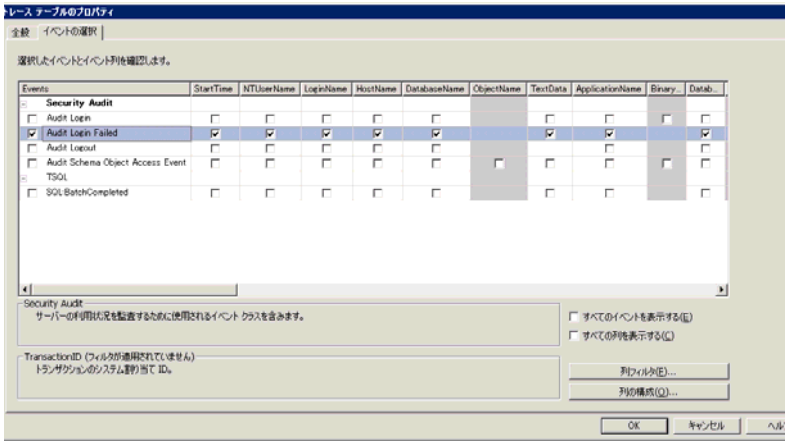
4. [SQL Server Profiler]が起動すると次のような画面が表示されます。



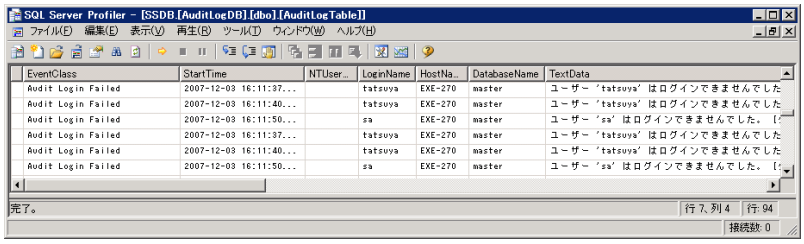
5. 蓄積されたトレースログより必要な情報を取得する処理を実行します。
ここでは、ログイン失敗に関するイベントである“Audit Login Failed”を取得する手順を示します。[SQL Server Profiler]のファイル ー プロパティを選択します。



6. [SQL Server Profiler] のトレーステーブルのプロパティにて“Audit Login Failed” のみを選択し、OK をクリックします。

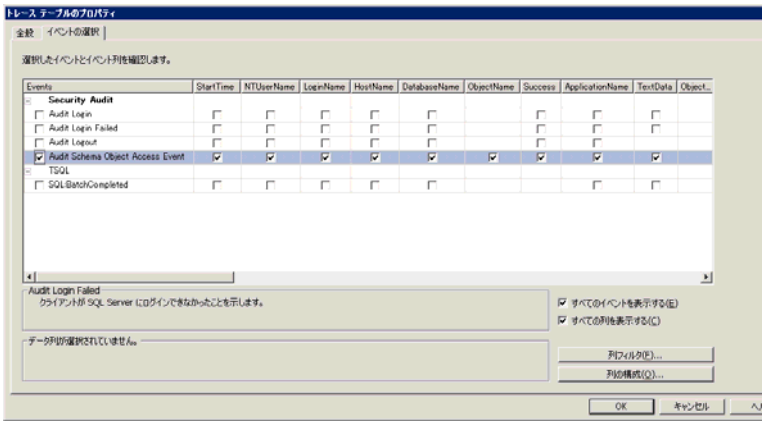


7. 実行結果を確認します。

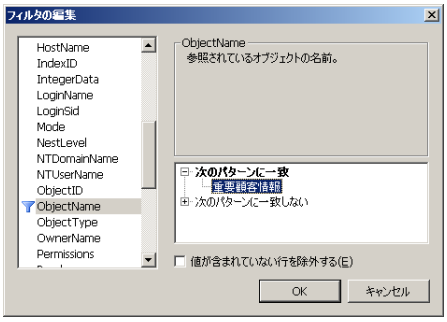


特定のテーブルに対する操作を抽出

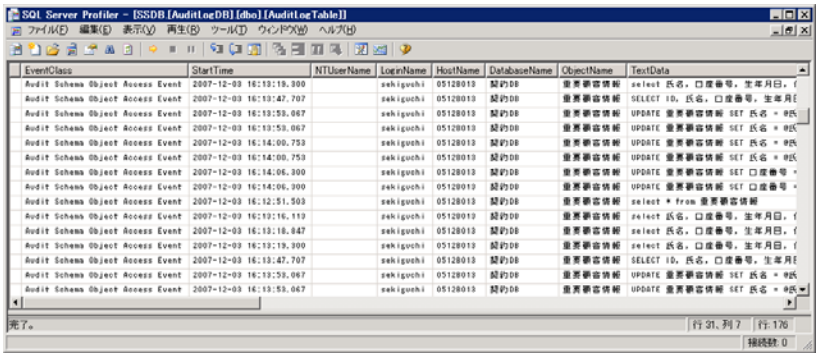
1. [SQL Server Profiler] のトレーステーブルのプロパティにて“Audit Schema Object Access Event”のみを選択します。



2. [列フィルタ]を選択し、[フィルタの編集]にて、次の設定を行います。
   [ObjectName]を選択し、[次のパターンに等しい]＝‘重要顧客情報’を入力
   設定が終了したら、[トレーステーブルのプロパティ] 画面にて[OK]を
   クリックします。

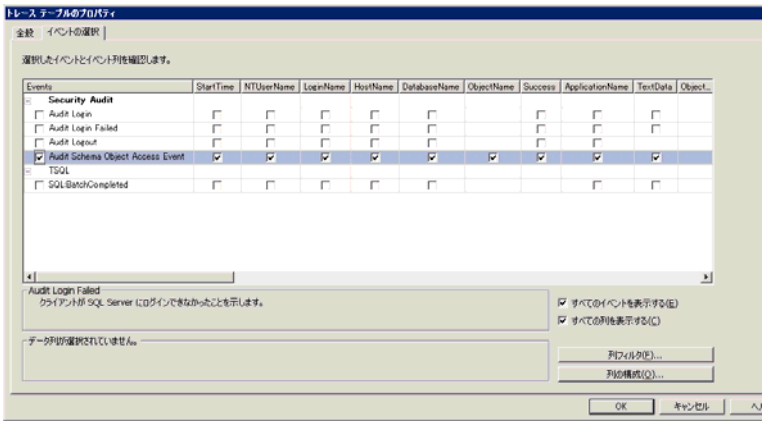


3. 実行結果を確認します。



改ざんの疑いを検出

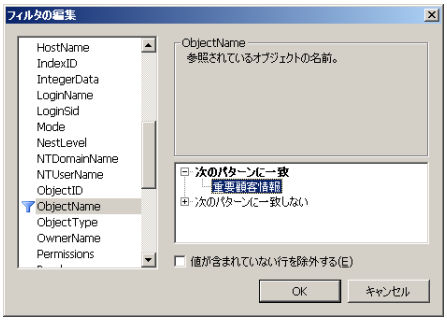
1. [SQL Server Profiler] のトレーステーブルのプロパティにて“Audit Schema Object Access Event”のみを選択します。

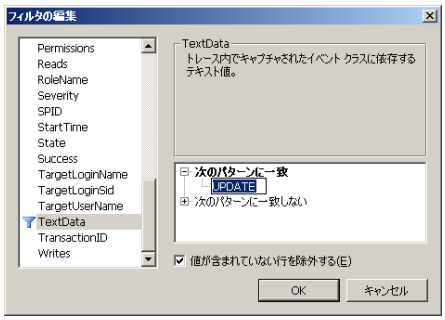


2. [列フィルタ]を選択し、[フィルタの編集]にて、次の設定を行います。

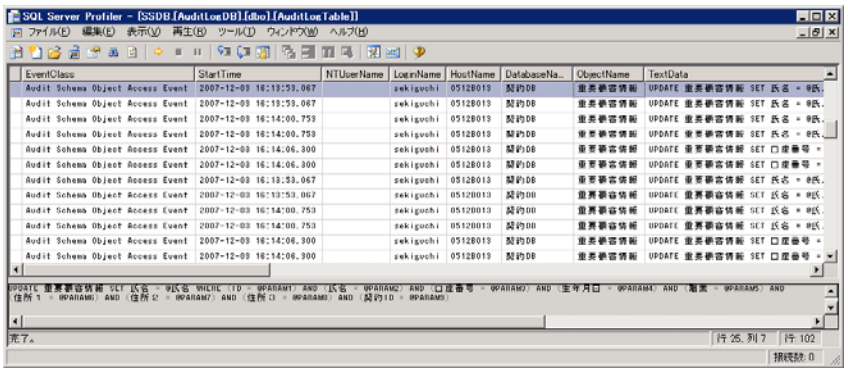
   - [ObjectName]を選択し、[次のパターンに等しい]＝‘重要顧客情報’を入力
   - [TexeData]を選択し、[次のパターンに等しい]＝‘UPDATE’を入力

   設定が終了したら、[トレーステーブルのプロパティ] 画面にて[OK]をクリックします。





3. 実行結果を確認します。



監査レポートの作成について

監査証跡として、トレースログを取得し、蓄積、分析を行った結果をレポートとして出力する必要があります。SQL Server 2005 では、これらの操作について、実現することがができます。

本章では SQL Server を使用することで、SQL Server に蓄積された情報を監査レポートとして出力する手順を記述します。

カスタムレポートによる監査レポート作成の流れ

対象製品：SQL Server 2005 SP2

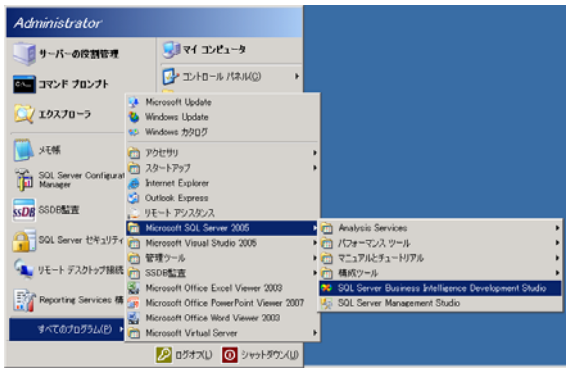
本節では、テーブルに蓄積されたトレース ログを SQL Server のレポート機能を利用し出力する手順について記述します。

監査レポートファイルを作成する

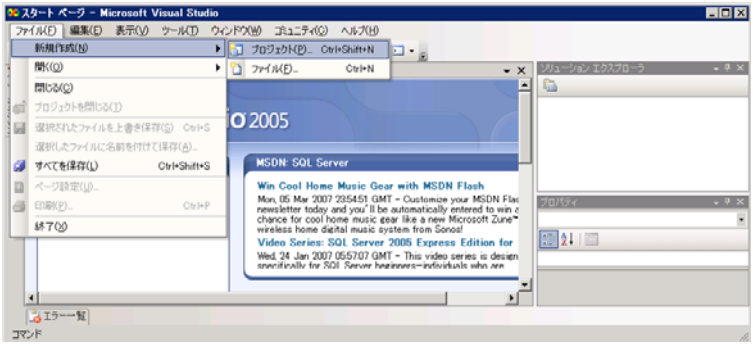
対象製品：SQL Server 2005 SP2

監査レポート作成を行うためには、まずレポートファイルを作成し、任意のフォルダに保存後に、そのファイルを SQL Server Management Studio にカスタムレポートとして追加します。

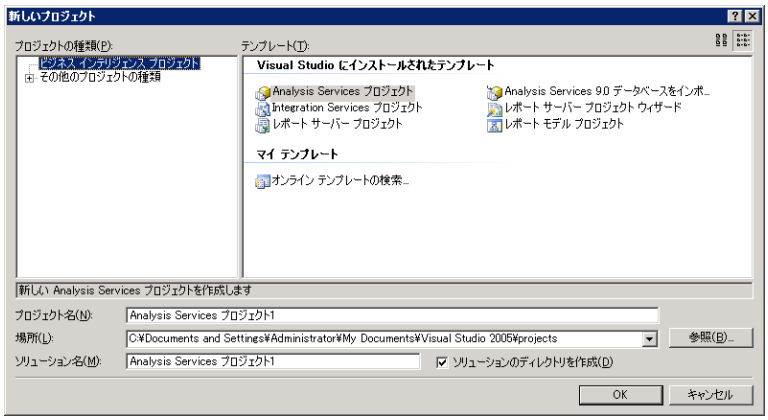
1. [スタート]ボタンをクリックし、[すべてのプログラム]、[Microsoft SQL Server]の順に操作し、[Business Intelligence Development Studio]を起動します。



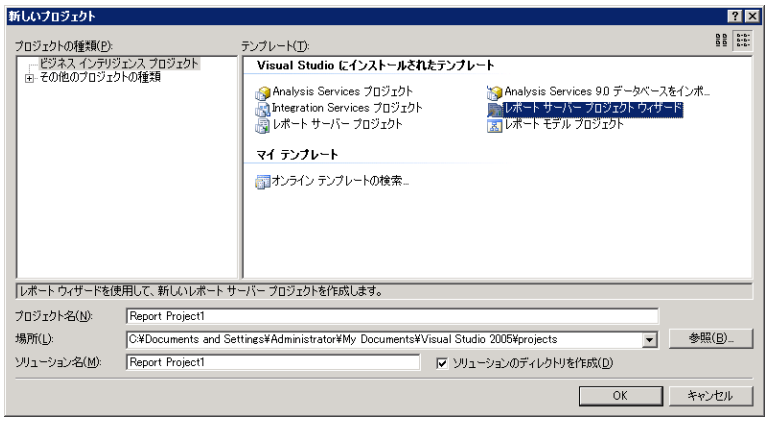
2. [ファイル]メニューの[新規作成]を選択し、[プロジェクト]をクリックします。



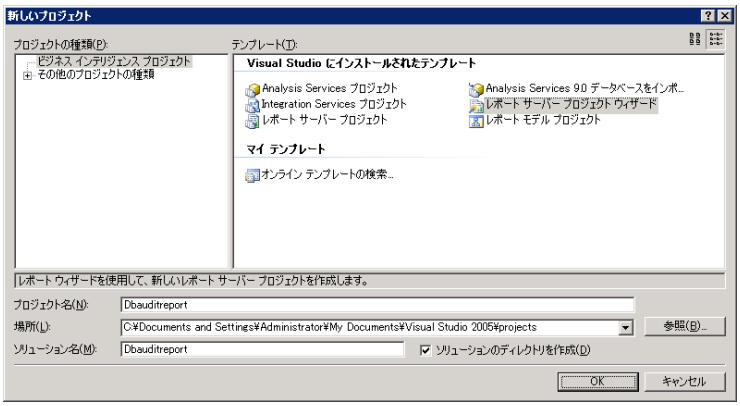
3. [プロジェクトの種類]ボックスの一覧で、[ビジネス インテリジェンス プロジェクト]をクリックします。



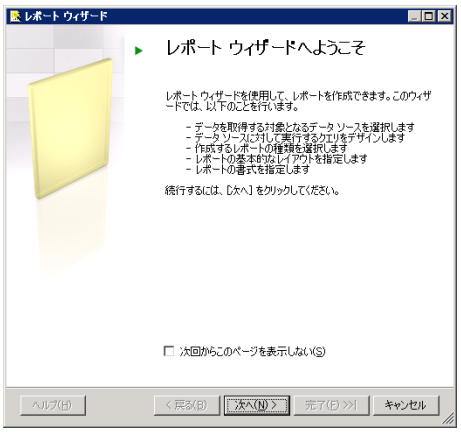
4. [テンプレート]ボックスの一覧で、[レポート サーバー プロジェクト ウィザード]をクリックします。



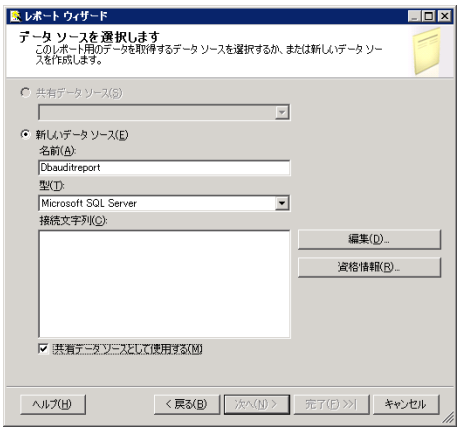
5. [名前]に「任意の名称（本節では“Dbauditreport”）」を入力して、[OK]をクリックします。



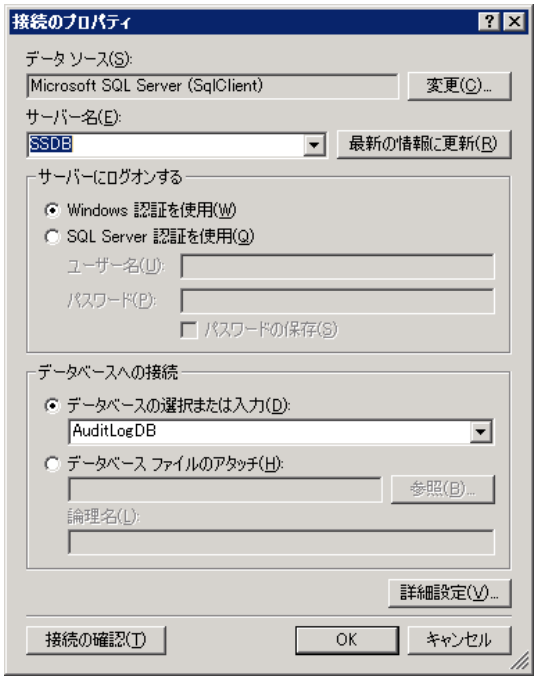
6. レポート ウィザードの最初のページで、[次へ]をクリックします。



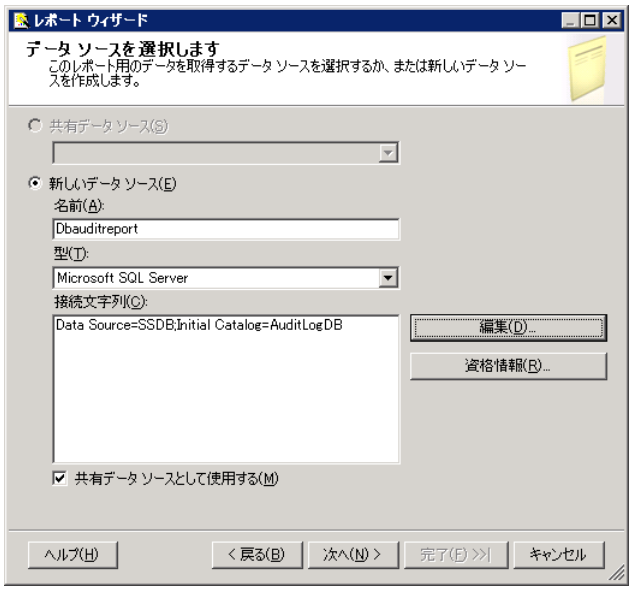
7. [データ ソースを選択します]ページの[名前]ボックスに、データベースエンジンへの接続で使用する名前を入力し、[編集]をクリックします。



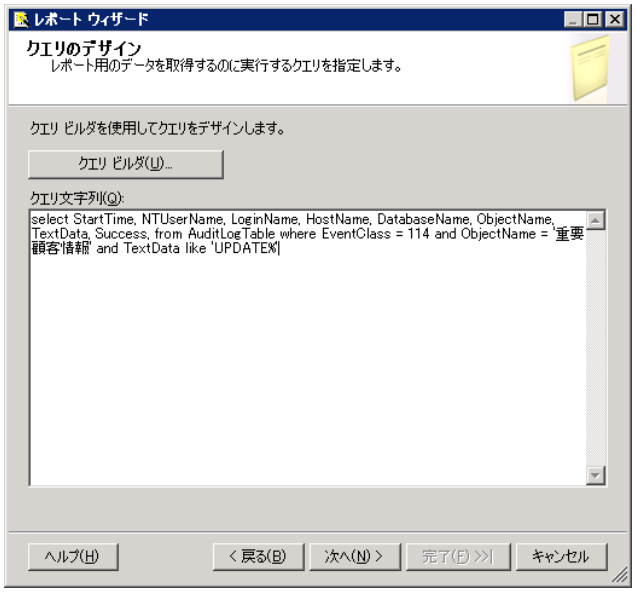
8. [接続プロパティ]ダイアログ ボックスの[サーバー名]ボックスに、サーバー名を入力します。その後、[データベースの選択または入力]ボックスに、任意の SQL Server データベースの名前（今回は、トレースログを管理するデータベース名）を入力し、[OK]をクリックします。



9. [データ ソースを選択します]ページで[次へ]をクリックします。



10. [クエリのデザイン]ページの[クエリ文字列]ボックスに、次の Transact-SQL ステートメント（前節 クエリの実行によるトレースログ監査で紹介した“改ざんの疑いを検出する”際のクエリ）を入力して、[次へ]をクリックします。



[注意]

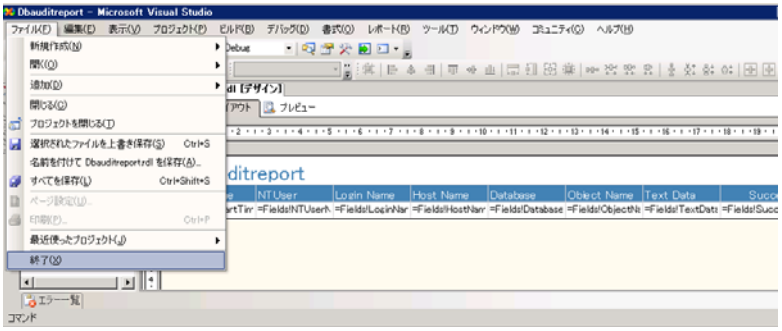
レポートウィザードの[クエリ文字列]ボックスにレポートパラメータは使用できません。

パラメータが必要となるような複雑なカスタムレポートは、手動で作成する必要があります。

11. [レポートの種類を選択します]ページで[テーブル]を選択し、[完了]をクリックします。

12. [ウィザードの完了]ページの[レポート名]ボックスに「任意のレポート名」を入力し、[完了]をクリックすると、レポートが作成され、保存されます。

13. BI Development Studio を終了します。

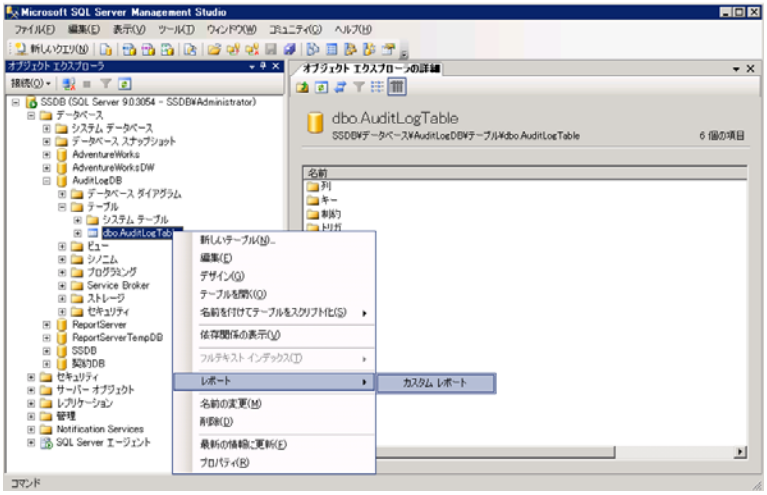


14. 監査用サーバー上の監査レポート用に作成した任意のフォルダに、<任意の監査レポート名> .rdl（本手順では ‘Dbauditreport .rdl’）をコピーします。

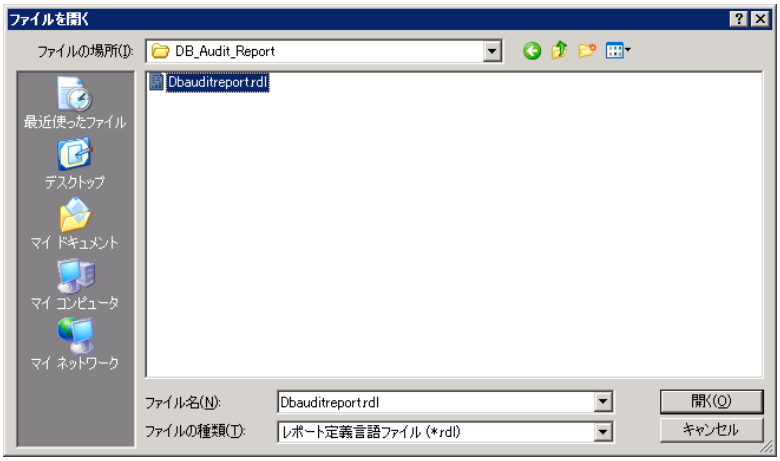
監査レポートを SQL Server Management Studio に追加する

対象製品：SQL Server 2005 SP2 以降

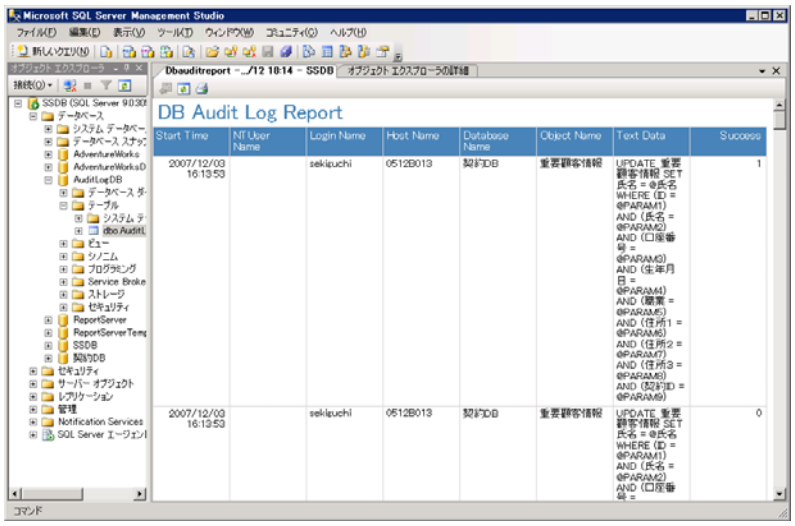
1. SQL Server Management Studio のオブジェクトエクスプローラでトレースファイルを管理するテーブルに対し右クリックし、[レポート]、[カスタム レポート]をクリックします。



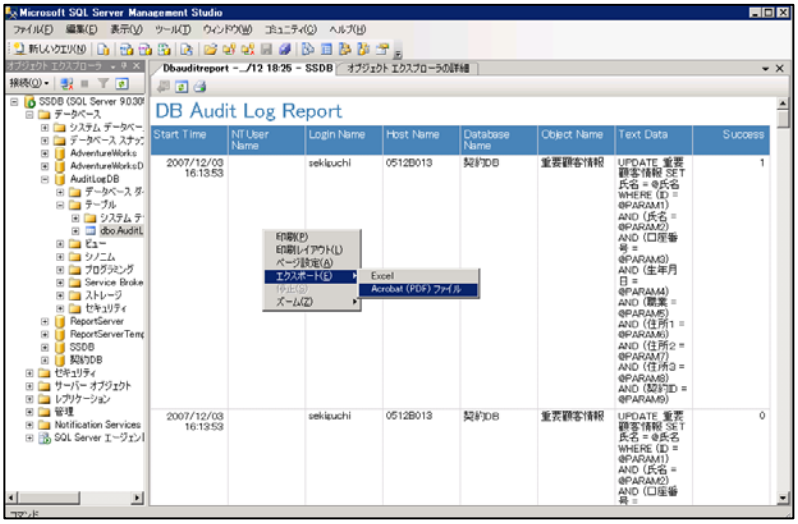
2. [ファイルを開く]ダイアログボックスで、カスタム レポート フォルダに移動し、<任意の監査レポート名> .rdl（本手順では、”Dbauditreport .rdl”）ファイルを選択し、[開く]をクリックします。



3. SQL Server Management Studio 上でレポート用データをテーブルから取得し、結果を表示されます。



4. 印刷を行う場合は、SQL Server Management Studio のレポート表示上で右クリックをし、[印刷]またはファイルへの[エクスポート]を指定します。



参考　：　監査レポートの出力について

データベース監査を開始し、期間が経つと監査ログは大量になります。また、監査レポートは、必要な事項に対し、必要な期間分を出力する必要があります。

監査レポート出力を行うためには、大きく下記　２つの方法が存在します。

- 監査レポート用のテーブルを用意する。

  本ガイドで紹介しました分析クエリの結果を、レポート用テーブルに取り込みカスタム　レポートでレポートを出力する。

- SQL Server Reporting Services を使い任意の条件で監査ログをレポート出力する仕組みを用意する。

  SQL Server Reporting Services を利用することで、レポート出力時に任意の条件でレポートを生成、出力することが可能となります。

  SQL Server Reporting Services の利用に際しては、下記の情報を参照下さい。

  SQL Server　2005自習書シリーズ

  http://www.microsoft.com/japan/technet/prodtechnol/sql/2005/exercises.mspx

パフォーマンスへの影響について

本書に記載されている SQL Server 2005 の監査設定については、トランザクション量や監査対象となるイベント、フィルタの設定などに応じて、トレースログ出力量が大きく変わるため、監査対象の設定によっては、アプリケーションシステム全体のパフォーマンスに重大な影響を与える恐れがあります。

また、データベース監査の必要性は、企業が保有するリスク、統制環境、そして業務プロセスにおける統制活動と組み合わせて検討されるべきもので、決してすべてのデータベースに対して本監査の設定が必要になるものではありません。

監査の設定をするにあたっては、テスト環境などを利用して、十分にパフォーマンス低下についての事前検証を行った上で、設定をされることを強くお勧めします。

実際に監査を実施するにあたり、パフォーマンスへの影響を考慮に入れ、必要なシステムの拡張や増強とともに検討されることを推奨いたします。

パフォーマンス負荷の参考値

■　環境

CPU	2.8GHz ×4
Memory	8Gbytes
OS	Windows Server 2003 Enterprise Edition　32bit
RDBMS	SQL Server 2000 Enterprise Edition SP4
SAN Storage	HDD16 本による RAID10 上の領域に SQL Sevrer 関連のデータを配置 Disk Cashe 8GB

(参考) テストに使用した DISK のデータ転送速度実測値(1GB のファイルのデータ転送速度)

・ローカル DISK　14.0MBytes/sec

・SAN Storage　69.7MBytes/sec

監査イベントを全取得したトレースファイルの出力先をローカル DISK と SAN Storage にした場合とで比較を行いました。

(監査イベント取得時/監査イベントを取得してないケース、両者とも CPU/IO ともに余裕がある状態で計測を実施しています)

■　参考値

ログ出力先	結果
LocalDISK	監査機能を使わない時と比較し 1SQL あたり 0.10ms～0.12 ms　処理時間が長くなる
SAN Storage	監査機能を使わない時と比較し 1SQL あたり 0.02ms ～0.06ms　処理時間が長くなる

おわりに

以上の各章にて、データベースサーバーにおける監査について、監査可能な要素、および手順を記載してきました。

IT 統制における監査は、必ずしも専用のソリューション製品の導入や専門機関への委託なしに実現不可能なものではありません。

また、無作為なログの収集は、結果的に監査に必要となるコスト、時間、人員を増大させるのみならず、監査結果の信頼性を低める事態にも繋がる可能性があります。

適切かつ有効な監査を実施するためには、まず監査すべき情報や手順を明確にすることが重要です。

監査対象とする要素の性質を把握し、それに見合った監査を検討されるにあたり、本書がその手助けとなりましたら幸いです。

協力：
株式会社 システムエグゼ
URL：http://www.system-exe.co.jp
データベースソリューション本部
DBユーティリティ開発室
井坂 雅／関口 達也
マイクロソフト認定パートナーとして、各特定業務（損保、生保、生産管理、人事給与、医療）および分野（データウエアハウス、データベース、コンテンツ管理、データベース監査、システム運用管理）におけるシステム提案、コンサルティング、システム要件分析、システム設計／開発、インフラ／ネットワーク構築、システム保守、システム運用管理などのサービス提供および自社ブランドとしデータベース監査製品を含むパッケージ製品の開発と販売。