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 : 2007 年 4 月 16 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 1

目次

はじめに 4
ドキュメント構成 5
概要 6
SQL Server 2005 パフォーマンスについて 7
監査設定及び監査手順 7
監査設定の追加 7
トレース定義スクリプトの生成 7
トレース実行ストアド プロシージャの作成・設定 11
トレース ログによる監査 17
C2 監査による監査 18
おわりに 21

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。

- 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

  対象製品：SQL Server 2005

  このドキュメントです。

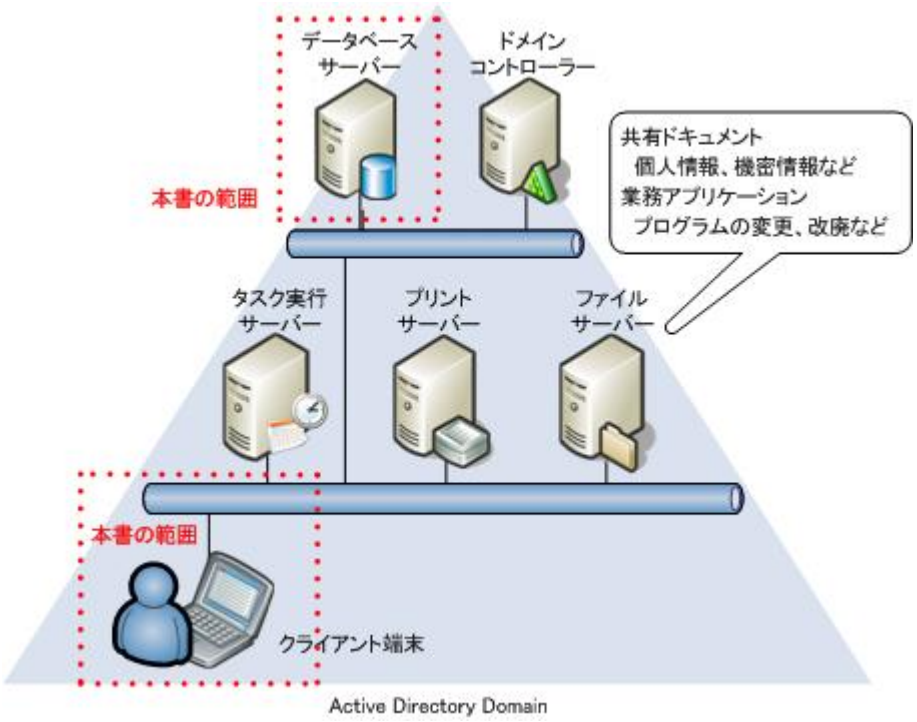
  SQL Server 2005 の標準のプロファイラおよび C2 監査の設定の手順を示します。

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、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が重要ですが、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。

また、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。



SQL Server 2005 パフォーマンスについて

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、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。

監査設定及び監査手順

SQL Server 2005 では、これらの操作について、標準のプロファイラ及び C2 監査により監査を行うことができます。

実際の手順について、次に記述します。

監査設定の追加

SQL Server 2005 のプロファイラを使用して監査を実施するためには、あらかじめ監査対象をスクリプト化して定義し、また自動で実行されるよう設定を行う必要があります。

本書では、例として、'Jinji'データベースの'employee'テーブルに対して実行された操作の内容を監査する場合の手順を記述します。

監査設定の追加手順を、次に示します。

トレース定義スクリプトの生成

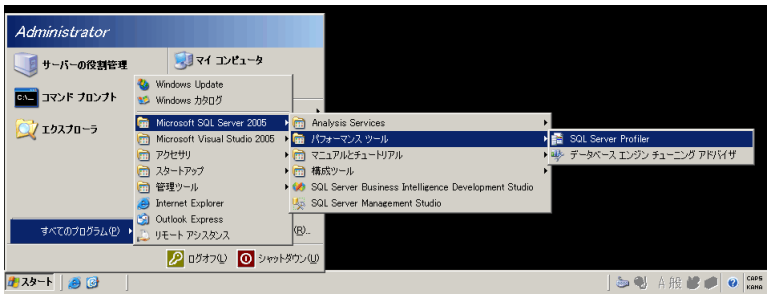
対象製品：SQL Server 2005

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。

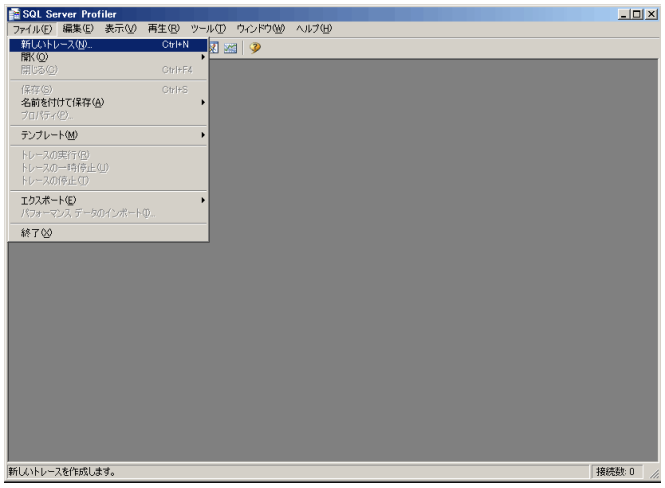
監査設定の追加手順を、次に示します。

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。

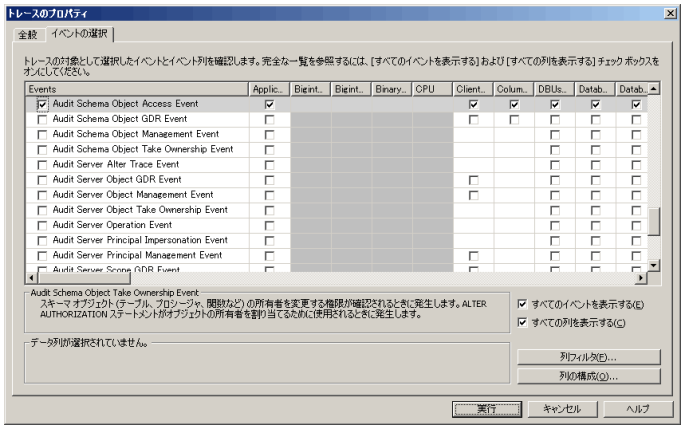


3. [SQL Server Profiler]が開いたら、[ファイル]メニューの[新しいトレース]をクリックします。



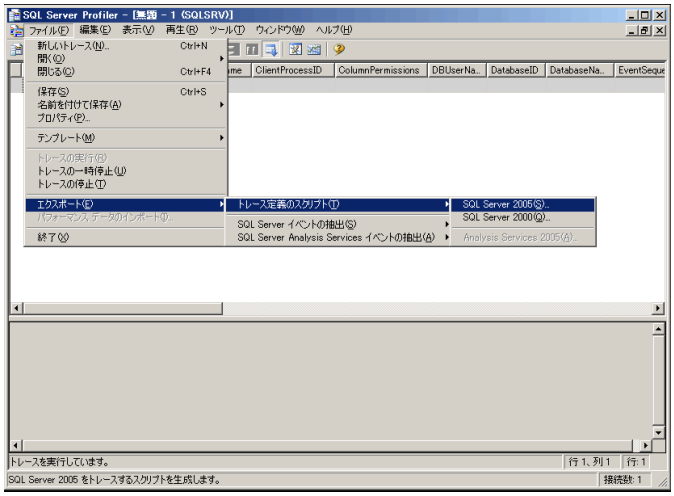
4. 認証ダイアログが表示されたら、管理者アカウントの認証情報を入力して、[接続]をクリックします。

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、監査対象とするイベントにチェックを入れて[実行]をクリックします。
本書では、例として、テーブルへのアクセスを監査する[Audit Schema Object Access Event]を選択します。

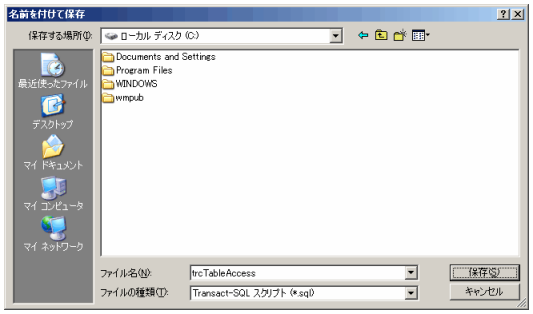


> 参考 **URL**
> その他、SQL Server Profiler よりトレース可能なイベントおよびデータ列については、以下をご参照下さい。
> Security Audit イベント クラス
> <http://msdn.microsoft.com/library/ja/default.asp?url=/library/ja/adminsql/ad_mon_perf_6zg3.asp>
> Security Audit データ列
> <http://msdn.microsoft.com/library/ja/default.asp?url=/library/ja/adminsql/ad_mon_perf_6zg3.asp>

6. [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。

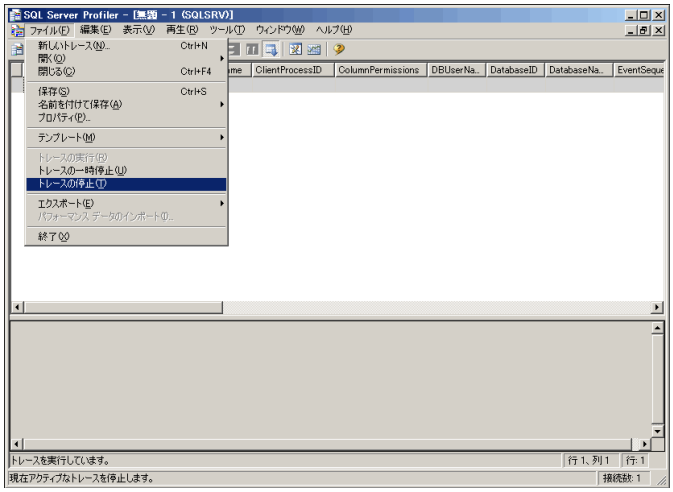


7. [名前をつけて保存]ダイアログが表示されたら、任意のディレクトリにトレース定義スクリプトを保存します。



8. 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。

9. [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。

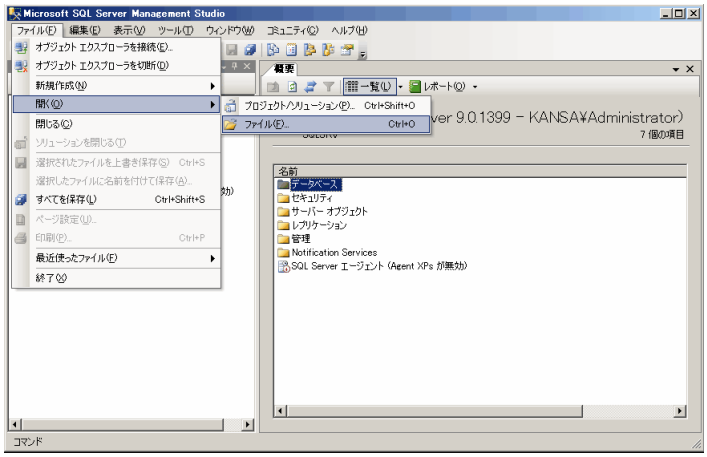
監査設定の追加手順を、次に示します。

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。

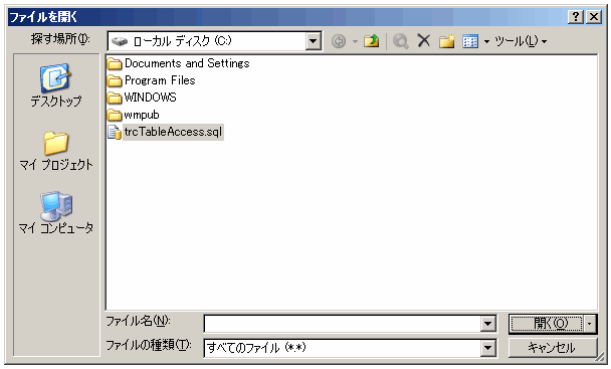
2. [スタート]メニューより、[すべてのプログラム]ー[Microsoft SQL Server 2005]と展開し、[SQL Server Management Studio]をクリックします。

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。

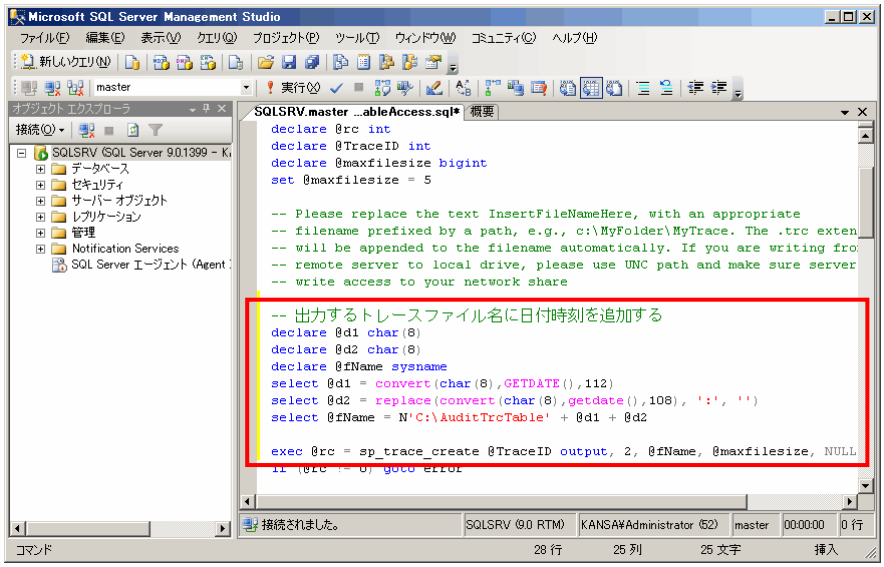


5. [ファイルを開く]ダイアログが表示されたら、「トレース定義スクリプトの生成」のNo.7 にて保存したファイルを選択し、[開く]をクリックします。



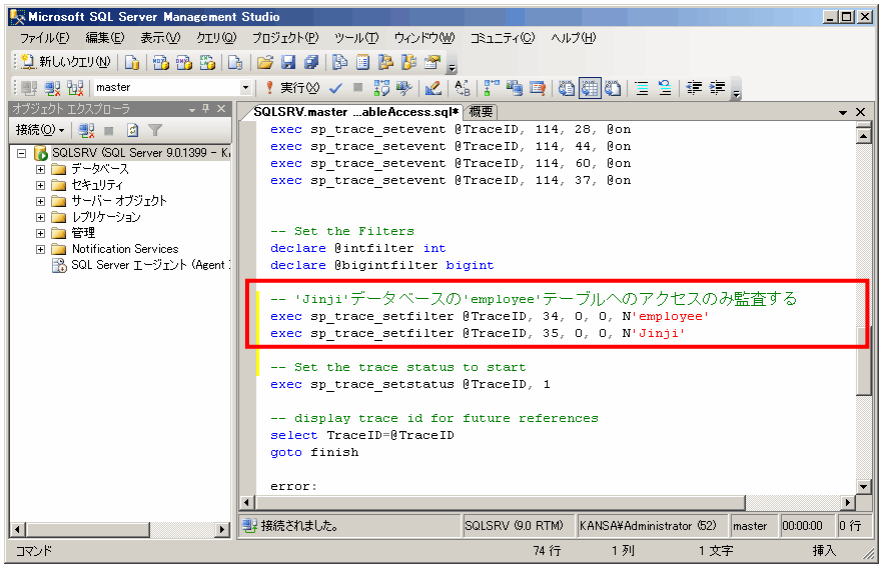
6. 認証ダイアログが表示されたら、管理者アカウントの認証情報を入力して、[接続]をクリックします。

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。



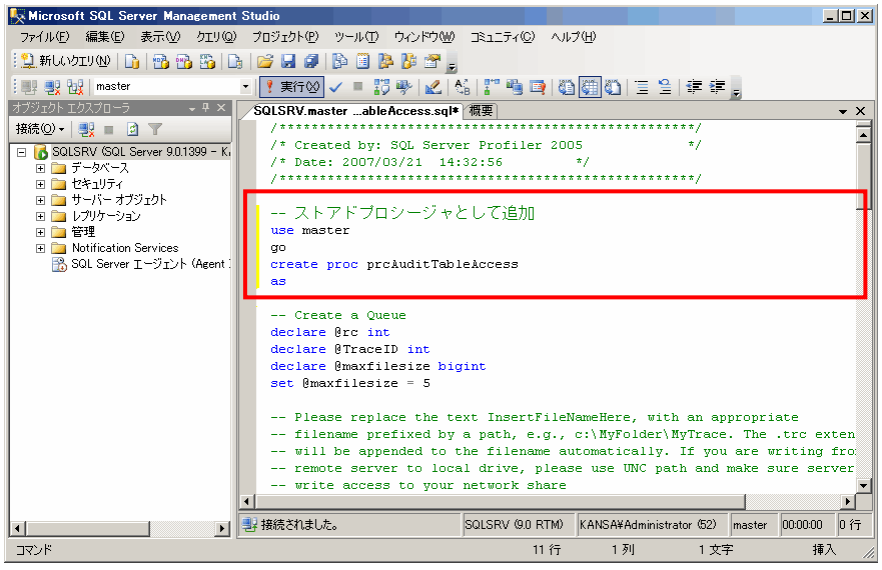

```
-- 以下のロジックを “set @maxfilesize = 5”の後に追記/改修
declare @d1 char(8)
declare @d2 char(8)
declare @fName sysname
select @d1 = convert (char(8), GETDATE(), 112)
select @d2 = replace (convert (char(8), GETDATE(), 108), ':', ``)
select @fName = FilePath + @d1 + @d2

exec @rc = sp_trace _create @TraceID output, 2, @fName, @maxfilesize,
NULL
```

8. また、必要なログのみを取得するよう、トレースにフィルタを設定します。本書では、例として’Jinji’データベースの’employee’テーブルへのアクセスのみをトレースするロジックを追加します。



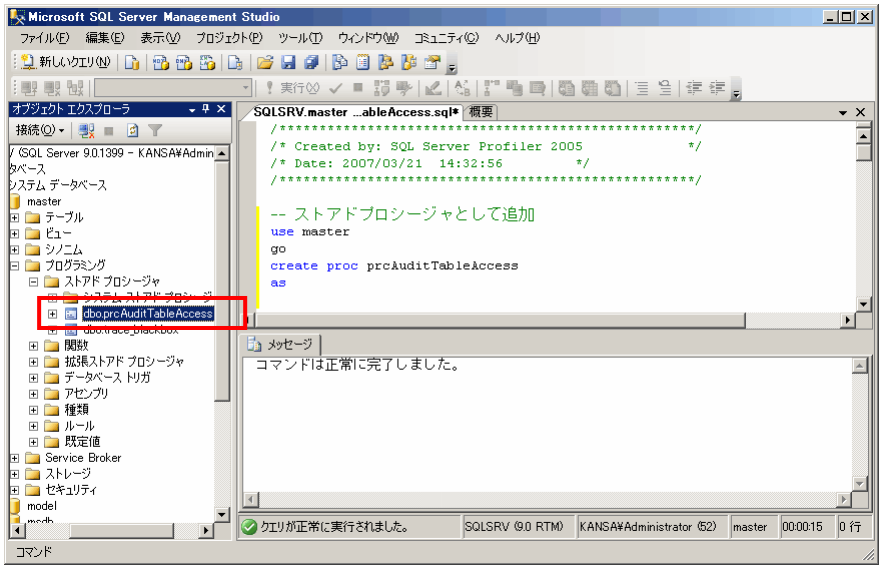

```
--以下のロジックを、”exec sp trace setstatus @TraceID, 1”の前に追記
exec sp trace setfilter @TraceID, 34, 0, 0, TableName
exec sp_trace_setfilter @TraceID, 35, 0, 0, DatabaseName
```

9. 以上の編集でトレース定義の改修が終了したら、[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。

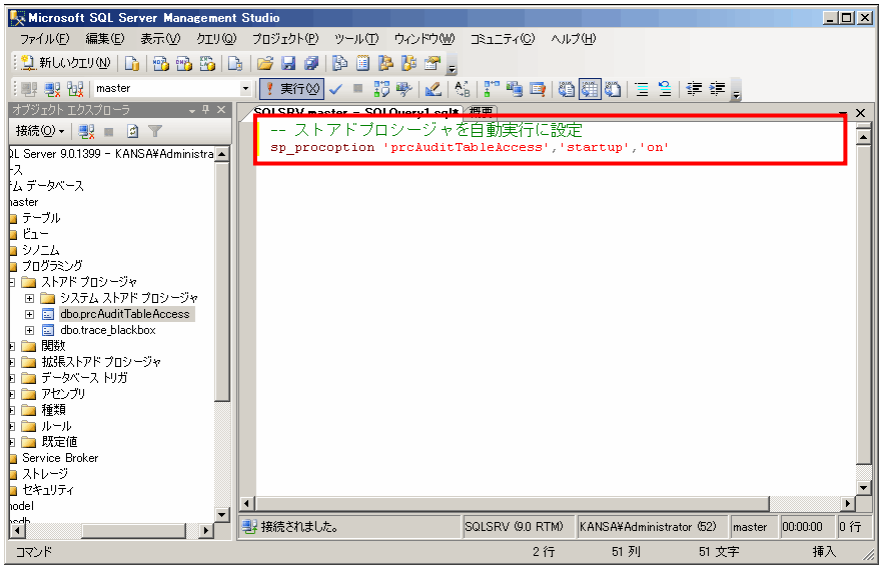



```
--以下のロジックを最上部に追記
use master
go
create proc procedureName
as
```

10. 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。



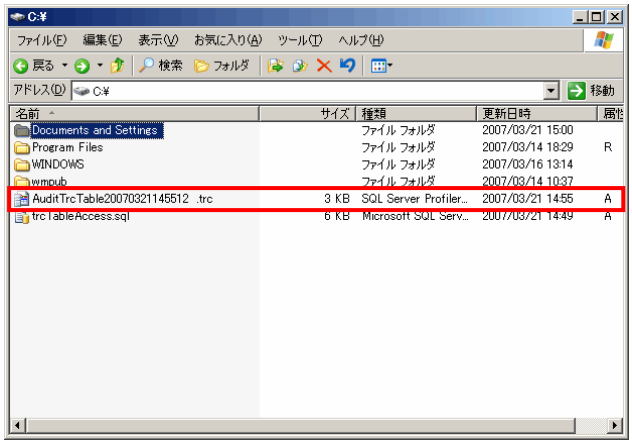
11. ストアド プロシージャの登録が完了したら、[sp_procoption]にて、ストアド プロシージャが自動実行されるよう、スタートアップに登録します。




```
--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'
```

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

13. No.7 で指定したディレクトリに、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。

トレース ログによる監査

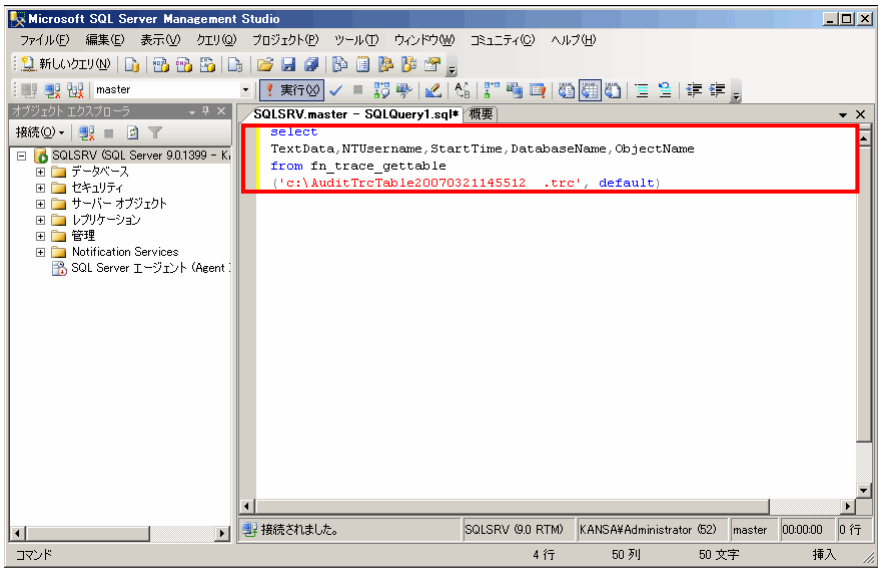
対象製品：SQL Server 2005

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 ログが出力されるようになります。

本節では、出力されたトレース ログを監査する手順について記述します。

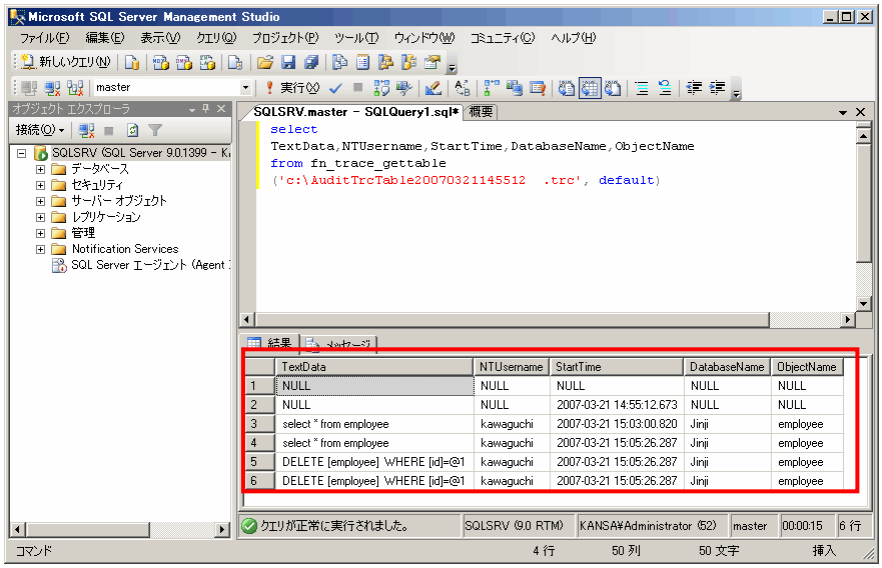
1. 管理者アカウントにてデータベースサーバーにログオンし、[Microsoft SQL Server Management Studio]を開きます。

2. [fn_trace_gettable]を使用して、出力されたトレースファイル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、例として[TextData]（操作内容）、[NTUsername]（実行ユーザー名）, [StartTime]（操作開始日時）, [DatabaseName]（操作対象データベース名）, [ObjectName]（操作対象テーブル名）を取得するクエリを実行します。




```
--以下のクエリを実行
select
TextData, NTUsername, StartTime, DatabaseName, ObjectName
from fn trace gettable
(TraceFileName, default)
```

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。

C2 監査による監査

対象製品：SQL Server 2005

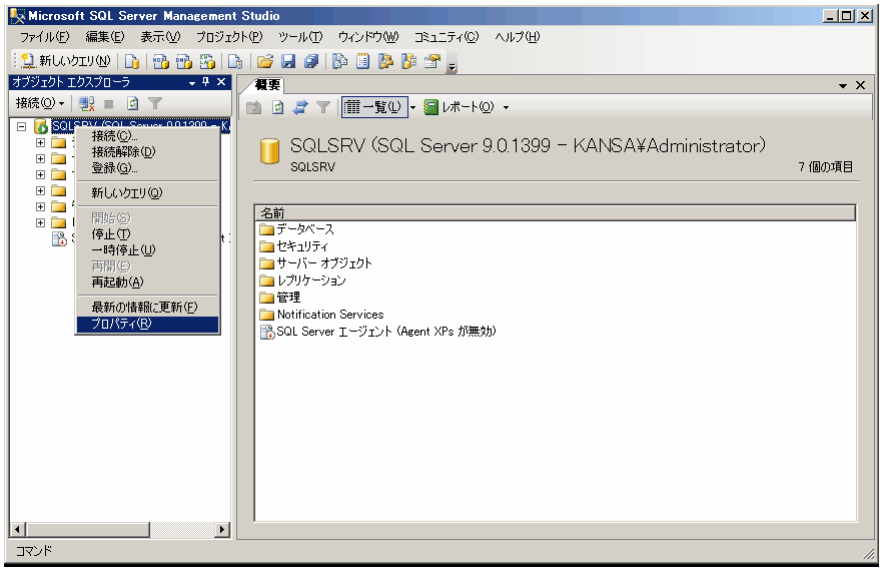
C2 監査とは、アメリカ国防総省により、Trusted Computer System Evaluation Criteria で定義されているもので、最下級の D から C1, C2, B1, B2, B3, A1 と設定されている 7 つのレベルのうちの 1 つです。

このうち、レベル C2 は、「ここのユーザーとオブジェクト間のアクセスを定義・制御する機構を持ち、複数のユーザー間で特定の個人、グループとを共有することを可能とする。この機構は、オブジェクトをアクセス権のないユーザーから保護し、アクセスの許可・排除は、個々のユーザー単位に可能である。オブジェクトのアクセス権の設定は、しかるべき権限を持ったユーザーによってのみ行われる」と定義されており、C2 監査では、この定義レベルのアクセス制御にかかわるアクセス状況を記録することができます。

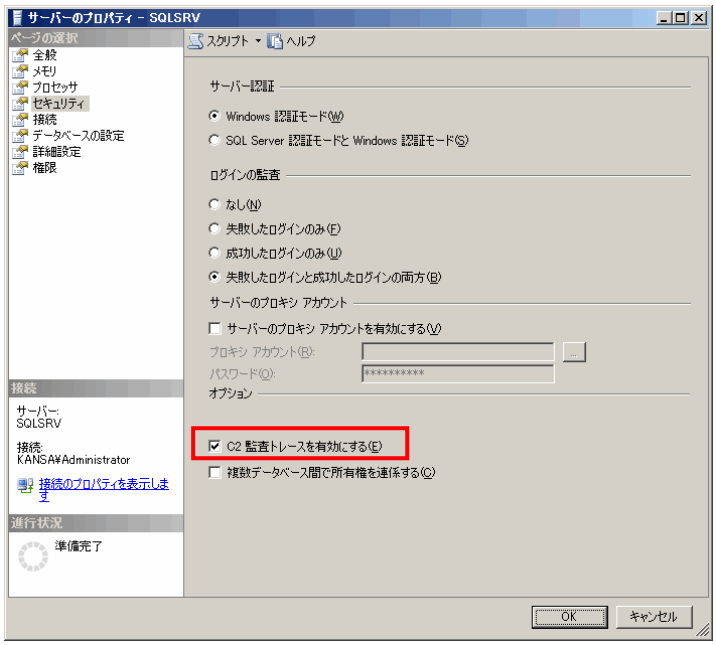
SQL Server 2005 による C2 監査の設定及び監査手順を、次に示します。

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、[Microsoft SQL Server Management Studio]を開きます。

2. [Microsoft SQL Server Management Studio]が開いたら、左ペインのツリーより、最上部のサーバーインスタンス名を右クリックして、[プロパティ]を選択します。

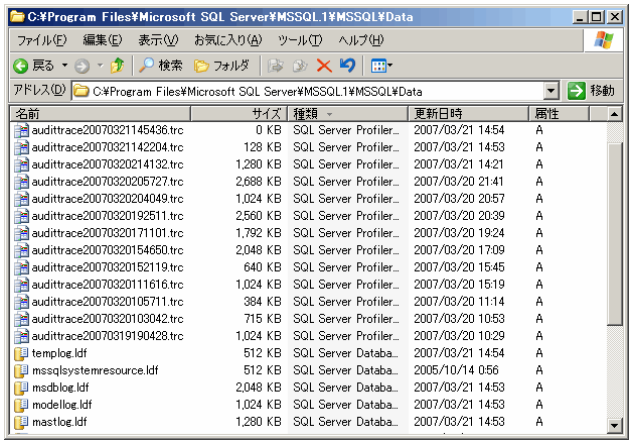


3. [サーバーのプロパティ]が開いたら、[セキュリティ]ページにて、[C2 監査トレースを有効にする]のチェックをオンにして、[OK]をクリックします。



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

5. エクスプローラより、[*SQL Server 2005 インストールディレクトリ*\MSSQL\Data]ディレクトリに、[AuditTrace_*yyyymmddhhmmss*.trc]というトレースファイルが出力されていることを確認します。



6. C2 監査で取得したログの監査を行う場合には、「トレース ログによる監査」と同様の手順にて、トレースファイルの内容を確認します。

以上で、C2 監査による監査手順は終了となります。

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化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。