Microsoft

マイクロソフト サーバー製品のログ監査ガイド

[タスクについての監査]

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 2000 Server Service Pack 4

・Windows Server 2003 R2, Standard Edition

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

  このドキュメントです。

  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

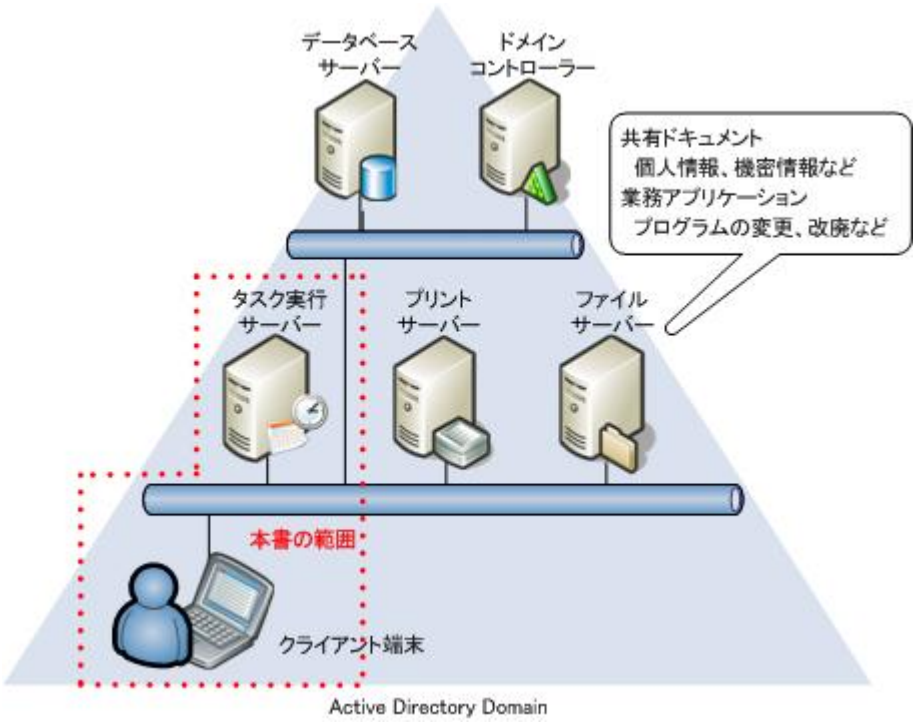
  SQL Server 2005 の標準のプロファイラおよび C2 監査の設定の手順を示します。

概要

通常のサーバー運用では、様々なタスクが登録され、利用者のオペレーションまたはスケジュールに従って、実行されています。

タスクは、その都度オペレーターがサーバーにログオンすることなく、サーバーに対する操作を実行できるため、サーバー上に不審なタスクが登録または実行されていないか監査する必要があります。

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。



監査設定及び監査手順

Windows 2000 Server 及び Windows Server 2003 では、タスクについて、標準のイベント ログ及びタスクの実行ログにより、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

対象製品：Windows 2000 Server /Windows Server 2003

タスクの監査を行うためには、まず、監査ログを出力するための設定を行う必要があります。

監査設定の追加手順を、次に示します。

プロセス追跡の監査の設定

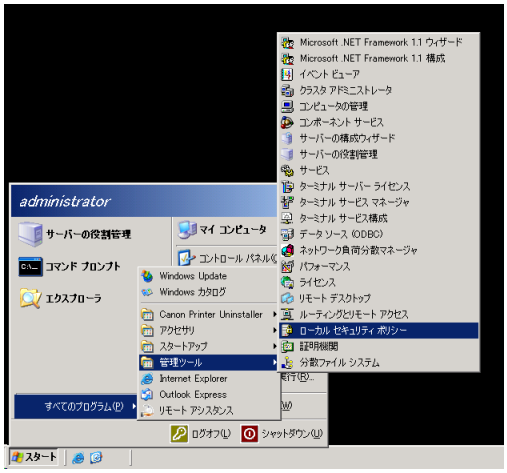
対象製品：Windows 2000 Server /Windows Server 2003

タスク登録および実行の監査ログを取得するために、ローカル セキュリティ ポリシーにて、オブジェクト アクセス及びログオンの成功/失敗をセキュリティ ログに出力するよう設定を行います。

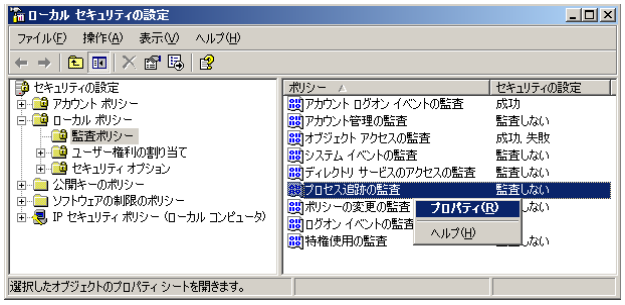
設定手順を、次に示します。

1. 管理者アカウントにて、タスク実行サーバーにログオンします。

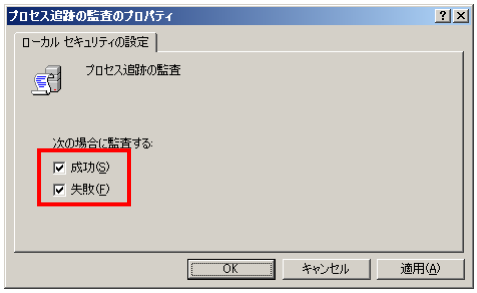
2. [スタート]メニューより、[すべてのプログラム]ー[管理ツール]と展開し、[ローカル セキュリティ ポリシー]をクリックします。



3. [ローカル セキュリティの設定]が開いたら、左ペインのツリーより、[セキュリティの設定]を展開し、[ローカル ポリシー]を選択します。
右ペインの[プロセス追跡の監査]を右クリックして[プロパティ]を選択します。



4. [プロセス追跡の監査のプロパティ]が開いたら、監査を行う項目にチェックを入れて、[OK]をクリックします。
ここでは、例として、アクセスの成功/失敗の両方を監査できるよう、[成功]、[失敗]の両方のチェックをオンにします。



以上で、プロセス追跡の監査の設定は終了となります。

タスクの登録の監査

対象製品：Windows 2000 Server /Windows Server 2003

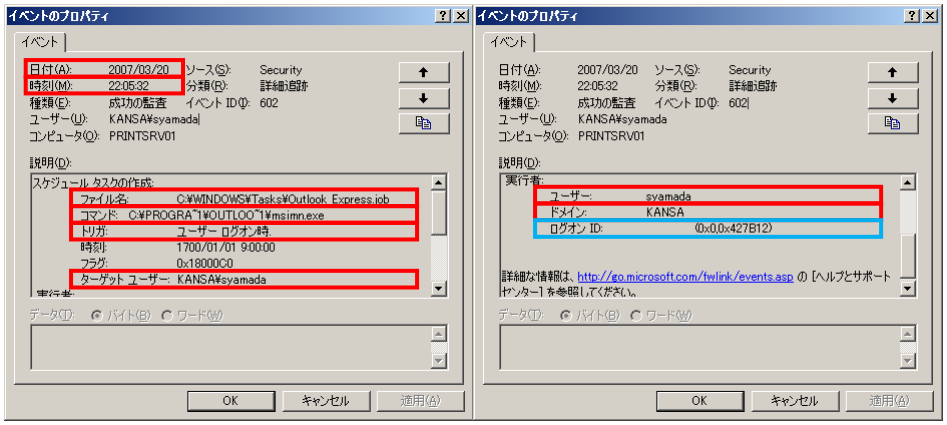
プロセス追跡の監査の設定が終了したら、タスクの登録に関するセキュリティログが、タスク実行サーバーのイベントログに出力されるようになります。

本項では、タスクの登録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、タスク実行サーバーにログオンし、[イベント ビューア]の[セキュリティ]イベント ログを開きます。

2. セキュリティイベント ログの一覧より、[ID602]イベントログを探して、プロパティを開きます。

[ID602]イベントログは、スケジュールタスクが作成された場合に出力されるイベント ログです。
[ID602]イベント ログにて確認する項目は、次の通りです。

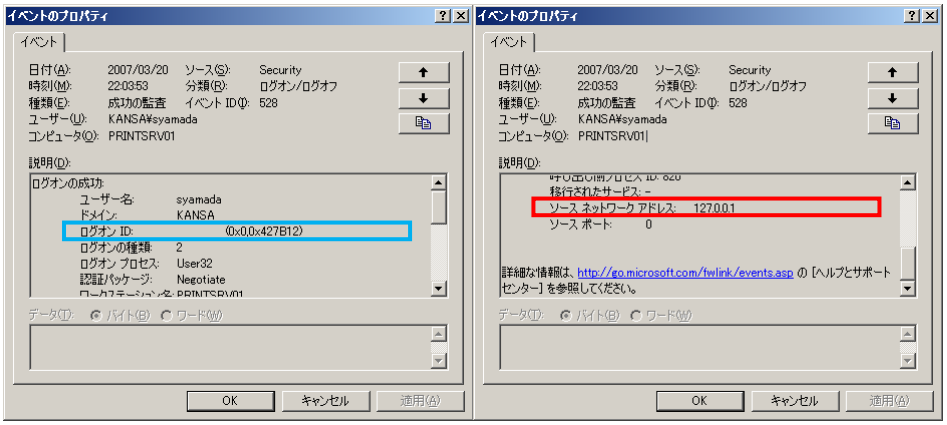


赤枠…監査対象とする項目

青枠…関連するイベント ログを特定するためのキーとなる情報

- 日付：操作が行われた日付
- 時刻：操作が行われた時刻
- 説明－ファイル名：タスクを実行するファイル
- 説明－コマンド：タスクで実行するコマンド
- 説明－トリガ：タスクを実行するトリガ
- 説明－ターゲットユーザー：タスクの実行ユーザー
- 説明－ユーザー：タスクを登録したユーザー
- 説明－ドメイン：タスクを登録したユーザーの所属ドメイン
- 説明－ログオン ID：[ID528]イベント ログの特定に使用

3. [イベント ビューア]の[セキュリティ]ログ一覧に戻り、[ログオン ID]の値が前項で確認した[ログオン ID]の値と一致する[ID528]イベント ログを特定し、プロパティを開きます。
[ID528]イベント ログは、サーバーに対するログオン/ログオフが行われた場合に出力されるイベント ログです。
[ID528]イベント ログにて確認する項目は、次の通りです。



[ID528]イベント ログのキーとなる項目は、次の通りです。

- 説明－ログオン ID：[ID602]イベント ログと一致していることを確認
- 説明－ソース ネットワーク アドレス：操作が行われたサーバーの IP アドレスを確認

以上で、イベント ログからの監査手順は、終了となります。

タスクの実行の監査

対象製品：Windows 2000 Server /Windows Server 2003

タスクの実行の履歴は、既定では SchedLgU.Txt テキスト ログに出力されます。

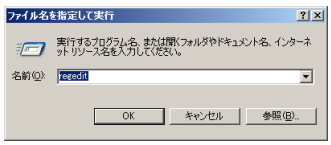
本節では、SchedLgU.Txt の確認方法について記述します。

SchedLgU.txt の出力先は、レジストリ エディタより確認することができます。

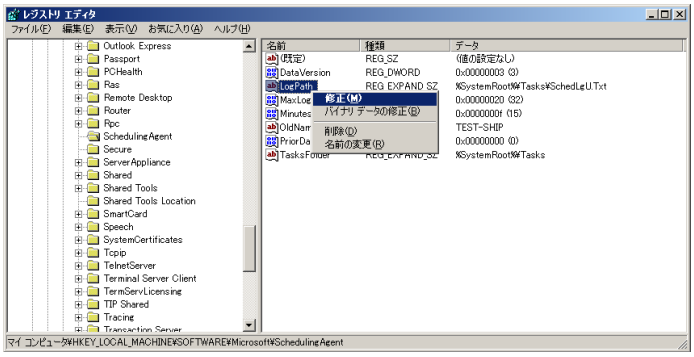
なお、レジストリ エディタの誤った使用は、システム全般に渡る重大な問題を引き起こす可能性があります。 こうした問題を解決するためには、Windows をインストールしなおさなければいけません。 Microsoft では、レジスト リエディタを使用することによって引き起こされた障害の解決については、一切保証しておりません。 レジストリ エディタを使用する場合には、お客様の責任において使用してください。

確認手順を、次に示します。

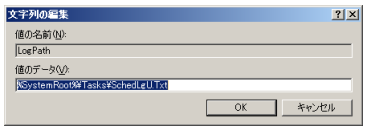
1. [スタート]メニューより、[ファイル名を指定して実行]をクリックして、“ regedit” と入力し、[OK]をクリックします。



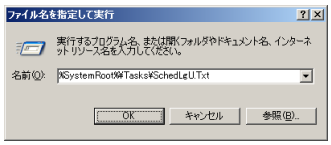
2. レジストリが開いたら、左ペインのツリーより、[HKEY_LOCAL_MACHINE]-[SOFTWARE]-[Microsoft]-[SchedulingAgent]と展開し、右ペインの[LogPath]を右クリックし、[修正]をクリックします。



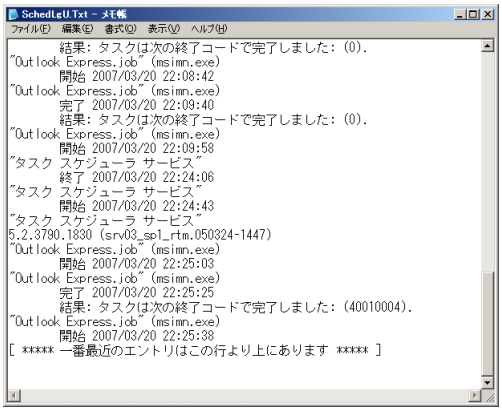
3. [文字列の編集]が開いたら、[値のデータ]欄の値をコピーして、[レジストリ エディタを終了します。



4. [スタート]メニューより、[ファイル名を指定して実行]をクリックして、 前項でコピーした値のデータを入力し、[OK]をクリックします。
このファイルは、エクスプローラ上からは確認できないため、注意が必要です。



5. ShedLgU.Txt より、タスクの実行履歴を確認します。



以上で、タスクの実行の監査手順は、終了となります。

注意事項

Windows 2000 Server 及び Windows Server 2003 にてログの収集及び監査を行う場合に、注意すべき項目については、別冊「マイクロソフト サーバー製品のログ監査ガイドーファイルサーバー上のファイル操作における監査」をご参照下さい。

おわりに

以上の各章にて、タスクの監査について、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。

付録 1: イベントログ 一覧

Windows 2000 Server

No.	Source	ID	Message	備考
1.	Security	602	スケジュール タスクの作成： ファイル名：%1 コマンド：%2 トリガ：%3 時刻：%4 フラグ：%5 ターゲット ユーザー：%6 実行者： ユーザー：%7 ドメイン：%8 ログオン ID：%9	

Windows Server 2003

No.	Source	ID	Message	備考
1.	Security	602	スケジュール タスクの作成： ファイル名：%1 コマンド：%2 トリガ：%3 時刻：%4 フラグ：%5 ターゲット ユーザー：%6 実行者： ユーザー：%7 ドメイン：%8 ログオン ID：%9	

付録 2: 関連情報

Windows 2000 Server 及び Windows Server 2003 におけるイベント ログ収集及び監査に関する次の情報については、別冊「マイクロソフト サーバー製品のログ監査ガイドーファイルサーバー上のファイル操作における監査」をご参照下さい。

- イベント ログのファイル出力

  [イベント ビューア]より、イベント ログをファイル出力する手順について記述しています。

- Excel を使用したイベント ログの確認

  CSV ファイルに出力したイベント ログ情報を、Excel のオートフィルタ機能を使用して確認する手順について記述しています。

- Log Parser 2.2

  マイクロソフトより無償で提供されている[Log Parser 2.2]のインストール手順、及び[Log Parser 2.2]を使用したイベント ログの収集手順について記述しています。

- Dump Event Log

  Windows 2000 Server リソース キットより提供されている[Dump Event Log]のインストール手順、及び[Dump Event Log]を使用したイベント ログの出力手順について記述しています。