

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。

お客様ご自身の責任において、適用されるすべての著作権関連法規に従ったご使用を願います。このドキュメントのいかなる部分も、米国 Microsoft Corporation の書面による許諾を受けることなく、その目的を 問わず、どのような形態であっても、複製または譲渡することは禁じら れています。ここでいう形態とは、複写や記録など、電子的な、または 物理的なすべての手段を含みます。

ただしこれは、著作権法上のお客様の権利を制限するものではありませ ん。マイクロソフトは、このドキュメントに記載されている内容に関し、 特許、特許申請、商標、著作権、またはその他の無体財産権を有する場 合があります。別途マイクロソフトのライセンス契約上に明示の規定の ない限り、このドキュメントはこれらの特許、商標、著作権、またはそ の他の知的財産に関する権利をお客様に許諾するものではありません。

© 2007 Microsoft Corporation. All rights reserved.

Microsoft、Windows、 Windows ロゴ、および Windows Server は米国 Microsoft Corporation の米国またはその他の国における登録商標または 商標です。

このドキュメントに記載されている会社名、製品名には、各社の商標を 含むものもあります。

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	. 4
ドキュメント構成	. 5
概要	. 6
監査設定及び監査手順	. 7
監査設定の追加	
プロセス追跡の監査の設定	
タスクの登録の監査8	
タスクの実行の監査10	
注意事項	13
おわりに	14
付録 1: イベントログ 一覧	15
Windows 2000 Server	
Windows Server 2003	
付録 2: 関連情報	16

3

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。
- [スタート]メニューより、[すべてのプログラム]-[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。

		酸 Microsoft .NET Framework 1.1 ウィザード
		n Microsoft .NET Framework 1.1 構成
		1 イベント ビューア
		வ クラスタ アドミニストレータ
		🔜 コンピュータの管理
		😰 コンボーネント サービス
		③ サーバーの構成ウィザード
		🧊 サーバーの役割管理
		🗞 サービス
		19 ターミナル サーバー ライセンス
administrator		都 ターミナル サービス マネージャ
		🖳 ターミナル サービス構成
バーの役割管理	3 41 T)CT-%	副 データソース (ODBC)
_	🔂 TYADHU KAUG	、🧔 ネットワーク負荷分散マネージャ
ロー コマンド プロンプト	3 Windows Undate	御 パフォーマンス
00	Windows that A	() ライセンス
🔍 エクスプローラ	· · · · · · · · · · · · · · · · · · ·	ひ リモート デスクトップ
	Canon Printer Uninstaller	夏 ルーティングとリモート アクセス
	💼 アクセサリ	Dーカル セキュリティ ボリシー
	💼 スタートアップ 🔹	· [2] 訂明機関
	💼 管理ツール 🔹	🍰 分散ファイル システム
	Internet Explorer	ETT(E)
オポアのゴロガニナ(の) ト	Outlook Express	240
97(0)09776	💫 リモート アシスタンス	
	DØ#7W 🚺 54	ットダウン(山)
🎝 スタート 🛛 🥭 🧭		

- 8 マイクロソフト サーバー製品のログ監査ガイド
- 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。

🎦 ローカル セキュリティの設定		_ 🗆 ×
ファイル(E) 操作(<u>A</u>) 表示(<u>V</u>) ヘルプ(<u>H</u>)		
	 割シーン 割アカウントログカンイベントの監査 20アカウントログカンイギョの監査 20アカウントマクスの監査 20アカイベントの監査 20アカレクトリケーとスのアクセスの監査 20アカレクトロクトロクトロクトロクトロクトロクトロクトロクトロクトロクトロクトロクトロク	セキュリティの設定 成功 成功、失敗 監査しない 監査しない 監査しない 監査しない 監査しない 監査しない を式 しない しない しない しない しない しない しない しない
選択したオブジェクトのプロパティ シートを開きます。	,	

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。

プロセス追跡の監査のプロパティ	? ×
ローカル セキュリティの設定	
「日本の話書	
:次の場合に話査する。 「 「 成功均② 「 「 失敗(E)	
適用	I(A)

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。

イベントのプロパティ <u>?!×</u>	<u>ብላントのプロパティ </u> ?	×
イベント 日白(4): 2007/03/20 ソース(5): Security 自身以(4): 220532 分類(2): 詳細)協飾 種類(2): 成功の監査 イベント ID(0): 602 ユーザー(2): KANS AF4syamada] 国面 コンピュータ(0): FRINTSRV01 国面	イベント 日付(Δ) 2007/03/20 ソース(S): Security 時初(M): 22:05:32 分類(E): 詳細)協飾 種類(E): 成功の動造者 イベント ID(D: 602) ユーザー(U): KANSAK4syamada 日) コンピュータ(D): PRINTSRV01 日)	
IX時間の):	IR明(D):	

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
- [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。

10 マイクロソフト サーバー製品のログ監査ガイド

イベントのプロパティ <u>? ×</u>	1 イベントのプロパティ ?×
1704	
日付(A) 2007/03/20 ソース(S): Security 時刻(M) 220533 分類(D) ログオン/ログオフ 種類(E): 成功の話査 イベント ID(D: 528 ユーザー(U): KANSAFeyamada コンピュータ(Q): PRINTSRV01	日付(A): 2007/03/20 ソース(S): Security 時初(他): 220363 分類(D): ログオン/ログオフ 種類(E): 成功の話苦 イベント ID(D: 528 ユーザー(L): KANSA¥syanada コンピュータ(Q): PRINTSRV01
	現明の: *FUGEUINT/I ECA IN 640 第月では、127001 ソースネットワークアドレス: 127001 リースホート: 0 詳細な情報は、http://go.microsoft.com/fwink/events.asp.の[ヘルプとサポート ビンターえを無してびだれ。 デークロン: アードの)
OK<	OK キャンセル 通用(金)

[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。

ファイル名	を指定して実行	? ×
	実行するプログラム名、または間くフォルダやドキュメント名、インットリソース名を入力してください。	ターネ
名前(<u>0</u>):	regedit	Ŧ
	OK キャンセル 参照(E)

 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。

文字列の編集	<u>?</u> ×
値の名前(N):	
jLogPath 値のデータ(V):	
NSystemRoo19#Tasks#SchedLgUTxt	
	OK キャンセル

 [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 エクスプローラトからけ確認できたいため 注意が必要です

このファイルは、エクスブローフ上からは確認できないため、汪意が必	、要です。
----------------------------------	-------

ファイル名	を指定して実行	<u>?</u> ×
	実行するプログラム名、または聞くフォルダやドキュメント名、イン ットリソース名を入力してください。	/ターネ
名前(Q):	NSystemRoot%#Tasks#SchedLgU.Txt	•
		<u>B</u>)

5. ShedLgU.Txtより、タスクの実行履歴を確認します。

■ SchedLgU.Txt - メモ帳	
ファイル(E) 編集(E) 書式(Q) 表示(V) ヘルブ(H)	
結果: タスクは次の終了コードで完了しました: (0). "Outlook Express.job" (msimn.exe) 開始 2007/03/20 22:08:42	3
^{"Out look Express.idb" (msimn.exe)} 完了 2007/03/20 22:09:40 (結果: タスクは次の終了コードで完了しました: (0).	
"Out look Express.job" (msim.exe) 開始 2007/03/20 22:09:58 "タスク スケジューラ サービス" 終了 2007/03/20 22:24:06	
ダスク スケンコーラ サービス 開始 2007/03/20 22:24:43 "タスク スケジューラ サービス" 5.2.3790.1890 (srv03.sp.1-tm.050324-1447) "Out look Express.job" (msimm_exe)	
「WHD 2007/03/0 22:22:08 「Outlook Express.job (msin,exe) 完了 2007/03/20 22:25:25 結果: タスクは次の終了コードで完了しました: (40010004). 「Outlook Express.job (msinn,exe) 開始 2007/03/20 22:25:38	
L ***** 一番最近のエントリはこの行より上にあります *****]	F

12 マイクロソフト サーバー製品のログ監査ガイド

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。