Microsoft

マイクロソフト サーバー製品のログ監査ガイド

[印刷ジョブについての監査]

ホワイトペーパー

発行日 : 2007 年 5 月 23 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

変更履歴

・2007/5/23　イベント ID 540/ID 528 に関する記述の修正

P.12、P.16

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

  このドキュメントです。

  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

  データベースのどのオブジェクトに対し、誰がどのような操作を行ったのか監査する手順を示します。

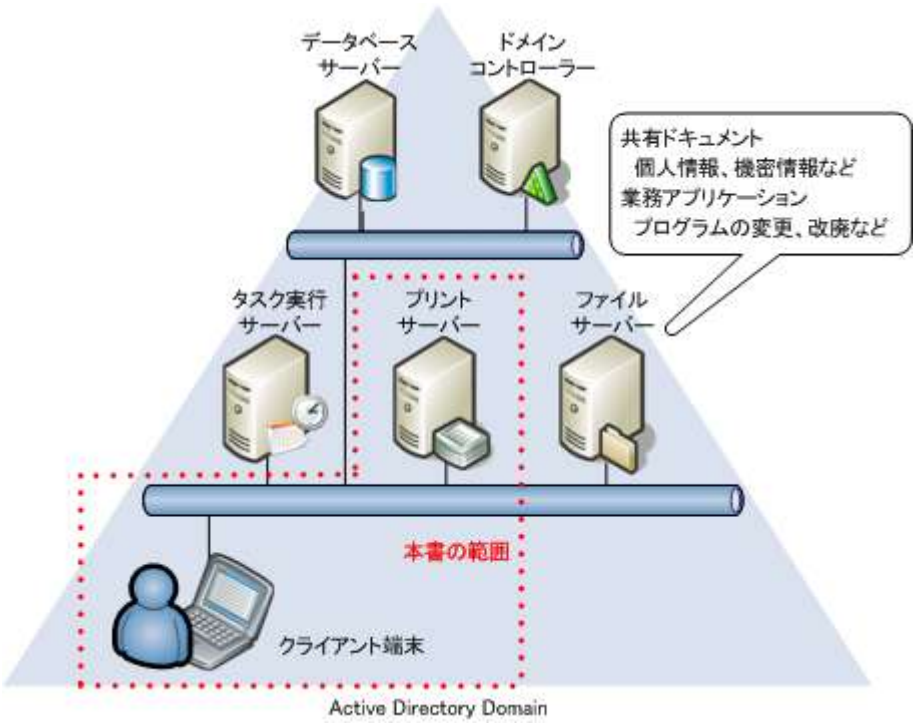
概要

実際の業務では、様々なユーザーがプリントサーバーに接続されたプリンタを使用して、様々なドキュメントの印刷を行っています。

情報漏洩の危険を抑止/防止するためには、ファイル自体のセキュリティだけではなく、印刷媒体の監査を抑止する必要があります。

よって、プリントサーバーの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。



監査設定及び監査手順

Windows 2000 Server 及び Windows Server 2003 では、印刷ジョブについて、標準のイベント ログ及びジョブの保存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

印刷ジョブの監査を行うためには、まず、監査ログの出力及びジョブの保存を行う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。

ローカル セキュリティ ポリシーの設定

対象製品：Windows 2000 Server /Windows Server 2003

印刷時のオブジェクト アクセスをセキュリティ イベントログに出力するために、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。

ローカル セキュリティ ポリシーの設定手順については、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。

プリントサーバーへのログ収集設定の追加

対象製品：Windows 2000 Server /Windows Server 2003

プリントサーバーに接続されたプリンタのログを出力するために、プリントサーバーへのログ収集設定の追加を行います。

設定手順を、次に示します。

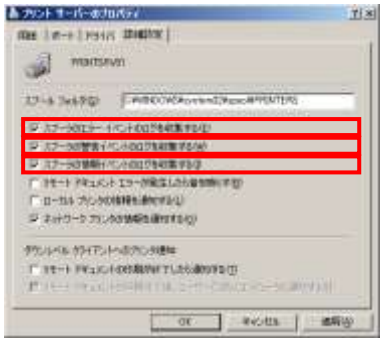
1. 管理者アカウントにて、プリントサーバーにログオンします。

2. [スタート]メニューより、[プリンタと FAX]をクリックします。

3. [プリンタと FAX]が開いたら、監査対象とするプリンタをツールバーより[ファイル]ー[サーバーのプロパティ]をクリックします。

4. サーバーのプロパティが開いたら、[詳細設定]タブをクリックします。

5. [詳細設定]が表示されたら、[スプーラのエラーイベントのログを収集する]、[スプーラの警告イベントのログを収集する]、[スプーラの情報イベントのログを収集する]にチェックを入れて、[OK]をクリックします。



以上で、プリントサーバーへのログ収集設定の追加は終了となります。

プリンタへのジョブ保存設定の追加

対象製品：Windows 2000 Server /Windows Server 2003

プリントサーバーに接続されたプリンタの印刷ジョブを保存するために、各プリンタへのジョブ保存設定の追加を行います。

この設定は、監査対象とするプリンタごとに行う必要があります。

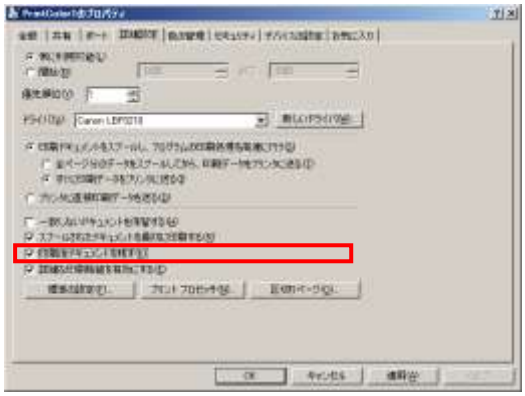
設定手順を、次に示します。

1. 管理者アカウントにて、プリントサーバーにログオンし、[スタート]メニューより[プリンタと FAX]をクリックします。

2. [プリンタと FAX]が開いたら、監査対象とするプリンタのアイコンを右クリックし、[プロパティ]をクリックします。

3. プリンタのプロパティが開いたら、[セキュリティ]タブにて、[詳細設定]をクリックします。

4. [詳細設定]タブが開いたら、[印刷後ドキュメントを残す]にチェックを入れて、[OK]をクリックします。



以上で、プリンタへのジョブ保存設定の追加は終了となります。

イベント ログからの監査

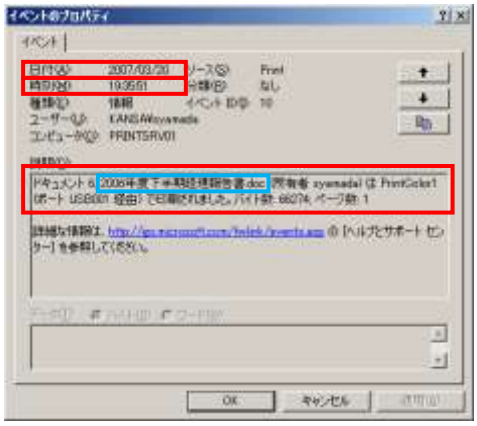
対象製品：Windows 2000 Server /Windows Server 2003

プリントサーバーへのログ収集設定の追加が完了したら、プリンタの動作に関するシステム　ログが、プリントサーバーのイベント ログに出力されるようになります。

本節では、システム ログを監査する手順について記述します。

1. プリントサーバーにログオンし、[イベント ビューア]の[システム]イベント ログを開きます。

2. システムイベント ログの一覧より、[ID10]イベントログを探して、プロパティを開きます。
   [ID10]イベントログは、印刷が行われた場合に出力されるイベント ログです。
   [ID10]イベント ログにて確認する項目は、次の通りです。

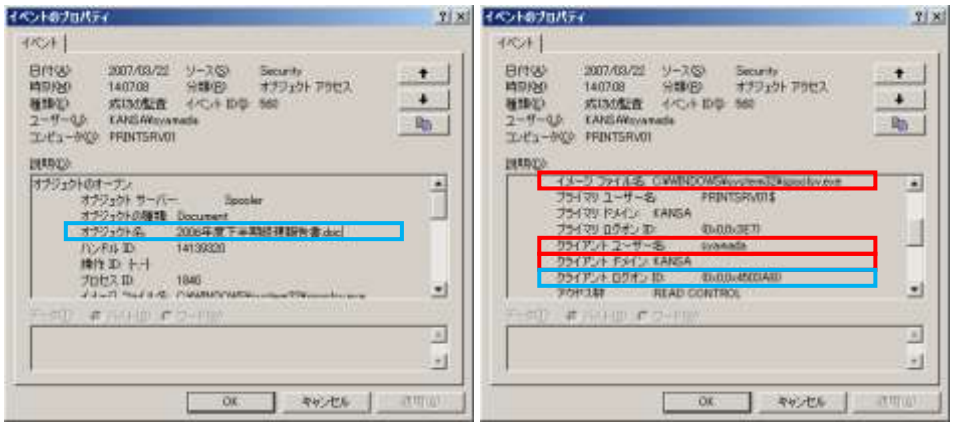


赤枠…監査対象とする項目

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

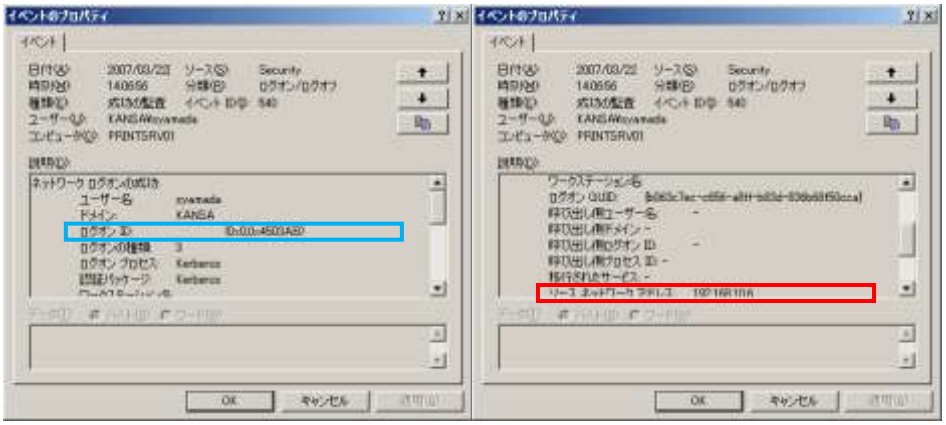
- 日付：操作が行われた日付
- 時刻：操作が行われた時刻
- 説明：印刷されたドキュメント名、プリンタ名、ドキュメントのバイト数、印刷したページ数
  [ID560]イベント ログの特定にも使用

3. [イベント ビューア]の[セキュリティ]ログ一覧に戻り、 [説明]欄の印刷されたドキュメント名が同じ [ID560]イベント ログを特定し、プロパティを開きます。
[ID560]イベント ログは、ファイルのオープンが行われた場合に出力されるイベント ログです。
[ID560]イベント ログにて確認する項目は、次の通りです。



- 説明－オブジェクト名：[ID10]と一致していることを確認
- 説明－イメージ ファイル名：操作を実行したアプリケーション
- 説明－クライアント ユーザー名：操作を行ったユーザー名
- 説明－クライアント ドメイン：操作を行ったユーザーの所属ドメイン
- 説明－クライアントログオン ID： [ID540]イベント ログの特定に使用

4. [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[クライアント ログオン ID]の値と一致する[ID540]イベント ログを特定し、プロパティを開きます。
[ID540]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。
[ID540]イベント ログにて確認する項目は、次の通りです。



- 説明－ログオン ID：[ID560]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：印刷を実行したクライアントの IP アドレス（Windows Server 2003 の場合のみ）
  ※ Windows 2000 Server の場合は、[ワークステーション名]よりアクセス元クライアントのワークステーション名を確認できます。

以上で、イベント ログからの監査手順は、終了となります。

印刷ジョブからの監査

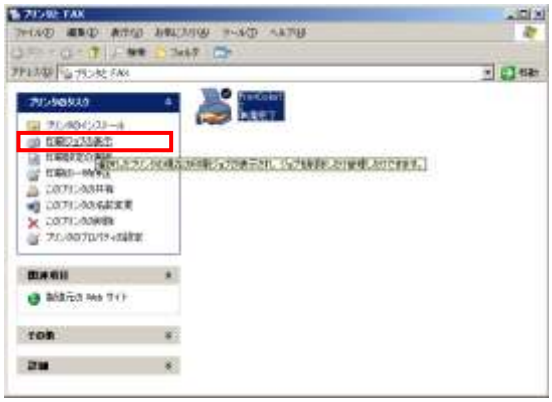
対象製品：Windows 2000 Server /Windows Server 2003

プリンタへのジョブ保存設定の追加が完了したら、プリンタより実行された印刷 ジョブが、印刷実行後も保存されるようになります。

本節では、印刷ジョブを監査する手順について記述します。

1. プリントサーバーにログオンし、[プリンタと FAX]を開きます。

2. [プリンタと FAX]が開いたら、右側の[プリンタのタスク]より、[印刷ジョブの表示]をクリックします。



3. [印刷ジョブの表示]が開いたら、プリンタに送信された印刷要求の一覧が確認できます。
   また、任意のドキュメントを右クリックして[印刷]を選択することで、同様の内容を印刷し、内容を確認することが可能です。

以上で、印刷ジョブからの監査手順は、終了となります。

注意事項

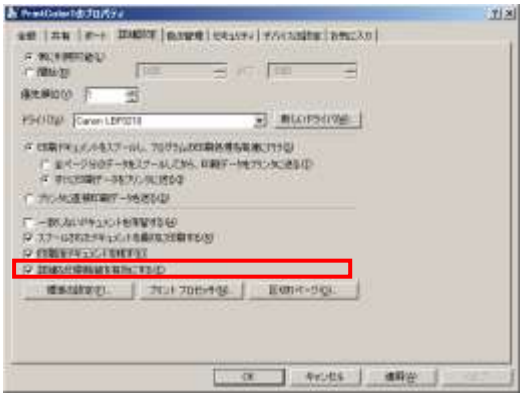
本章では、マイクロソフト サーバー製品にて、印刷ジョブに関するログの収集及び監査を行う場合に、注意すべき項目について記述します。

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、注意すべき一般的な項目については、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。

[ページ数]の表記について

[ID10]イベント ログの説明欄には、印刷されたオブジェクトの[ページ数]情報が含まれています。

監査対象プリンタのプロパティの[詳細設定]タブにて、[詳細な印刷設定を有効にする]チェックをオフにした場合に、この[ページ数]に不正な値が記録される場合があります。



[詳細な印刷設定を有効にする]のチェックがオンになっている場合には、印刷データはページごとに区切られた EMF 形式で送信されます。

[詳細な印刷設定を有効にする]のチェックをオフにすると、印刷データはページごとに区切られない RAW データとして送信されます。

後者の場合、ページ数はアプリケーション側でカウントされることとなりますが、ページ数のカウントを行わないアプリケーションから印刷が実行された場合には、[ページ数]の値が正しく記録されない可能性があります。

おわりに

以上の各章にて、印刷ジョブ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。

付録 1: イベントログ 一覧

Windows 2000 Server

No.	Source	ID	Message	備考
1.	Print	10	Document %1, %2 %3 は %4 で印刷されました。バイト数: %6; ページ数: %7※1	※1 印刷されたドキュメント名、プリンタ名、ドキュメントのバイト数、印刷したページ数
2.	Security	560	オブジェクトのオープン: オブジェクト サーバー:%1 オブジェクトの種類:%2 オブジェクト名:%3 新しいハンドル ID:%4 操作 ID:%5 プロセス ID:%6 プライマリ ユーザー名:%8 プライマリ ドメイン:%9 プライマリ ログオン ID:%10 クライアント ユーザー名:%11 ※2 クライアント ドメイン:%12※3 クライアント ログオン ID:%13 アクセス数:%14 特権:%15	※2 操作を実行したユーザー ※3 操作を実行したユーザーの所属ドメイン
3.	Security	540	ネットワーク ログオンの成功: ユーザー名:%1 ドメイン:%2 ログオン ID:%3 ログオンの種類:%4 ログオン プロセス:%5 認証パッケージ:%6 ワークステーション名:%7※4	※4 印刷を実行したクライアントのワーク ステーション名

Windows Server 2003

No.	Source	ID	Message	備考
4.	Print	10	Document %1, %2 %3 は %4 で印刷されました。バイト数: %6; ページ数: %7※1	※1 印刷されたドキュメント名、プリンタ名、ドキュメントのバイト数、印刷したページ数
5.	Security	560	オブジェクトのオープン: オブジェクト サーバー:%1 オブジェクトの種類:%2 オブジェクト名: %3 ハンドル ID:%4 操作 ID:%5 プロセス ID:%6 イメージ ファイル名:%7 ※2 プライマリ ユーザー名:%8 プライマリ ドメイン:%9 プライマリ ログオン ID:%10 クライアント ユーザー名:%11 ※3 クライアント ドメイン:%12※4 クライアント ログオン ID:%13 アクセス数:%14 特権:%15 制限された SID 数: %16 アクセス マスク:%17	※2 操作を実行したアプリケーション ※3 操作を実行したユーザー ※4 操作を実行したユーザーの所属ドメイン
6.	Security	540	ネットワーク ログオンの成功: ユーザー名:%1 ドメイン:%2 ログオン ID:%3 ログオンの種類:%4 ログオン プロセス:%5 認証パッケージ:%6 ワークステーション名:%7 ログオン GUID:%8 呼び出し側ユーザー名:%9 呼び出し側ドメイン:%10 呼び出し側ログオン ID:%11 呼び出し側プロセス ID: %12 移行されたサービス:%13 ソース ネットワーク アドレス:%14 ※5 ソース ポート:%15	※5 印刷を実行したクライアントの IP アドレス

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。