ファイル監査ツール

WhiteFox FileAccess Auditor

ユーザーズガイド

公開日： 2011 年 8 月 15 日

作成者： 株式会社エスディーケー

http://whitefox.jp/

この資料では、Windows サーバーにファイル監査ツール
WhiteFox FileAccess Auditor をインストール・設定し、
ファイルアクセス監査を行う手順について説明します。

はじめに

●概要

ファイル監査ツール WhiteFox FileAccess Auditor をダウンロード（あるいは購入）していただき誠にありがとうございます。WhiteFox FileAccess Auditor は、Windows サーバーのファイルアクセス ログをデータベース出力し、監査結果を検索・表示するツールです。Windows サーバーにインストール・設定するだけで簡単に ファイルアクセスが記録でき、検索・表示できます。

WhiteFox FileAccess Auditor に関する不具合、更新などのサポート情報は、すべて株式会社エスディーケー Web サイト（http://whitefox.jp/）で公開しています。また、ご不明な点、改善・機能追加して欲しい点などについても Web サイトで受け付けております。

●ドキュメントに関する注意事項

このドキュメントに記載されている情報（URL 等のインターネット Web サイトに関する情報を含む）は、将来予告無しに変更することがあります。別途記載していない場合、このソフトウェアおよび関連するドキュメントで使用している会社、組織、製品、ドメイン名、電子メールアドレス、ロゴ、人物、場所などの名称は架空のものです。実在する名称とは一切関係ありません。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お願いいたします。このドキュメントのいかなる部分も、株式会社エスディーケー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、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。

株式会社エスディーケーは、このドキュメントに記載されている内容に関し、知的財産権（特許、特許申請、商標、著作権など）を有する場合があります。別途、株式会社エスディーケーのライセンス契約上に明示のない限り、このドキュメントはこれらの知的財産権に関する権利をお客様に許諾するものではありません。

目次

このドキュメントは５つの章で構成されています。第１章では本製品の概要、第２章では導入計画について、第３章では本製品のインストール、第４章以降は本製品の使用方法について記載されています。本製品の導入をお考えのお客様は、第１章から順にお読みください。

第１章　製品紹介

ここでは、「ファイル監査ツール WhiteFox FileAccess Auditor」（以下、本製品）の製品概要、機能などについて説明します。

１．１　製品概要

●概要

個人情報保護(P マーク),情報セキュリティ管理(ISMS),内部統制,ITIL への対応で ファイルサーバーのアクセスログ収集・管理が必要となります。アクセスログは、クライアント PC（Windows XP/Vista など）からファイルサーバー（Windows Server 2003/2008 など）の共有フォルダにアクセスした場合の「いつ・誰が・どのファイルを・どのようにアクセスしたか」という記録ですが、Windows の標準設定では 記録されません。

本製品は、Windows サーバーのファイルアクセス ログをデータベース出力し、監査結果を検索・表示するツールです。Windows サーバーにインストール・設定するだけで簡単に ファイルアクセスが記録でき、検索・表示できます。

●特徴

本ツールの特徴は、以下の通りです。

- 簡単インストール～設定
- 監査対象フィルタリングによる 必要なログだけ保存
- 他社製品と比較して 低価格

●導入メリット

本ツールを導入するメリットは、以下の通りです。

メリット	内　容
導入コストの低さ	● 他社製品と比較して 「低価格」 ● 簡単インストール～設定で 導入の手間が少ない
管理コストの低さ	● 特定フォルダ、特定ファイル拡張子だけの「必要なログ」を保存するので ログのディスク容量が少ない ● 定期的なログ出力、必要時の検索・表示で 管理者の作業負担を軽減

１．２　機能一覧

本製品の機能一覧を下表に示します。

機能	機能概要
ファイルアクセスの定期的な記録	● ファイルアクセス監査を定期的におこない、必要なファイルアクセスの記録(ログ)をデータベースに出力
ファイルアクセスの検索・表示	● データベースに記録したファイルアクセスログを日時範囲、ファイル名、ユーザー名などで絞り込み 検索・表示 ● 検索結果は CSV 形式ファイル（Excel で表示できる カンマ区切りテキストファイル）に出力可能
E メール通知	● ファイルアクセスのログ出力時にエラーが発生した場合などにＥメールでシステム管理者に通知

１．３　本製品の構成

本製品の構成要素を下表に示します。

構成要素	概要
インストーラ (Setup.msi)	構成要素を対象コンピュータにインストールするファイル。 ファイルアクセス監査をおこなうファイルサーバーの Windows OS により、インストーラが異なる。 ● Windows Server 2008 版 ● Windows Server 2003 版
設定ツール (WFFAU-CFG.EXE)	ファイルアクセス監査に必要な セキュリティポリシー設定、監査対象フォルダ設定、監査対象ファイル拡張子設定などをおこなうツール。
監査サービス (WFFAU-SVC.EXE)	バックグラウンドで動作し、必要なファイルアクセスの記録(ログ)をデータベースに出力する Windows サービスプログラム。コンピュータが起動していれば ユーザーがログオンしていない時でも動作。
ビューア (WFFAU-VWR.EXE)	データベースに記録したファイルアクセスログを日時範囲、ファイル名、ユーザー名などで絞り込み 検索・表示するツール。

第２章　導入前の計画

ここでは、本製品を導入する前に計画すべき事項について説明します。

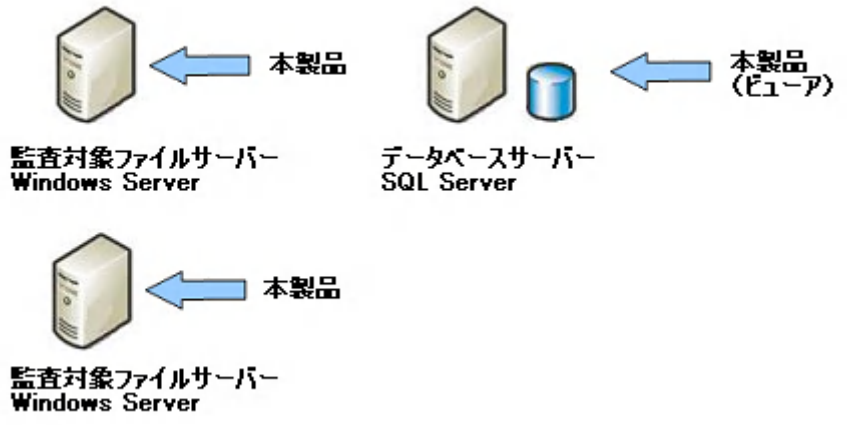
２．１　必要な機器、ソフトウェアの準備

●オールインワン構成

本製品の評価が目的である場合、１台のサーバーに 本製品とデータベースを導入する構成が考えられます。

●複数サーバー構成

複数台のファイルサーバーがあり、データベースサーバーを別サーバーとして構成できます。この構成では、監査対象ファイルサーバーに本製品を それぞれインストール・設定し、データベースサーバーに 本製品のビューアだけをインストールします。



本製品以外に必要なソフトウェアは、データベースソフトウェア Microsoft SQL Server です。SQL Server のバージョン 2000/2005/2008、すべてのエディションに対応していますので 評価が目的の場合には 無償の Express エディションでも OK です。

第３章　インストール

ここでは、本製品をインストールする前に、注意すべき事項（ライセンス、必要なシステム、インストールの準備）、インストールの手順について説明します。

３．１　ライセンス

本製品の無料体験版は、インストール後３０日間は無償で使用することができますが、それ以降はライセンスを購入しなければ、起動しなくなります。インストール後にお客様の環境で使用できるソフトウェアであるかを評価していただき、継続して使用する場合は、株式会社エスディーケーの Web サイトからライセンスを購入してください。

３．２　必要なシステム

インストールに必要なシステムを下表に示します。

ＯＳ	Windows Server 2008 版：Windows Server 2008　（または Vista、７） Windows Server 2003 版：Windows Server 2003　（または XP）
データベース	SQL Server 2000/ 2005/ 2008 ※全てのエディションで動作します。 ※無償の Express エディションは Microsoft の Web サイトからダウンロードできます。 ※SQL Server 認証モードでインストールしてください。
Framework	Microsoft .NET Framework 3.5 以降 ※Windows Server 2008/Vista 以降の OS には、標準でインストールされています。 ※Microsoft の Web サイトから無償ダウンロードできます。 ※インストーラの指示通りにインストールしてください。

３．３　インストール準備

●以前のバージョン、無料体験版がインストールされている場合

本製品の以前のバージョン（または、無料体験版）がインストールされている場合は、コントロールパネルの［プログラムの追加と削除］で、アンインストールしてから、新しいバージョンをインストールしてください。また、新しいバージョンがリリースされた際のリリースノートや、株式会社エスディーケーWeb サイトのアップデート情報などを参考に、アンインストール作業をおこなってください。

●ログインアカウント

インストールを行なうコンピュータにログインする際の「ログインアカウント」は、該当コンピュータのローカル管理者権限を持ったアカウントを使用してください。

３．４　インストール手順

オールインワン構成　Windows Server 2003/XP

１） Microsoft .NET Framework 3.5 のインストール

２） SQL Server 2000 または 2005 または 2008 のインストール

３） 本製品のインストール

オールインワン構成　Windows Server 2008/Vista

１） SQL Server 2000 または 2005 または 2008 のインストール

２） 本製品のインストール

複数サーバー構成　Windows Server 2003/XP

１） ファイルサーバーに Microsoft .NET Framework 3.5 のインストール

２） データベースサーバーに SQL Server 2000 または 2005 または 2008 のインストール

３） ファイルサーバーに 本製品のインストール

４） データベースサーバーに 本製品(ビューア)のインストール

複数サーバー構成　Windows Server 2008/Vista

１） データベースサーバーに SQL Server 2000 または 2005 または 2008 のインストール

２） ファイルサーバーに 本製品のインストール

３） データベースサーバーに 本製品(ビューア)のインストール

本製品のインストールは、インストーラ（SetupAll.msi または SetupViewer.msi）を起動し、以下の順序でおこないます。

画面名	説明
インストールしています	そのまま待ちます。
インストールが完了しました	[閉じる]をクリックします。 以上で、インストールは完了です。

第４章　設定

ここでは、本製品の設定ツールの画面表示・操作について説明します。設定ツールは、[スタート] メニュー → [すべてのプログラム] → [SDK-LTD] → [WhiteFox FileAccess Auditor 設定ツール] をクリックすると起動できます。設定ツールを終了するには、画面右下の [閉じる] ボタンをクリックしてください。

画面右下の [保存] ボタンをクリックすると 設定が保存されます。

４．１　データベース設定

まずはじめに、[監査の設定] タブの [データベース] タブで データベースを設定します。

1) 左上の「データベースサーバー ログイン設定」の「サーバー」で ネットワーク上のデータベースサーバー (SQL Server) を選択するか、サーバー名を入力します。
2) 「ログイン」に SQL Server のログイン（例：sa）を入力します。
3) 「パスワード」に パスワードを入力します。
4) [接続確認] をクリックします。

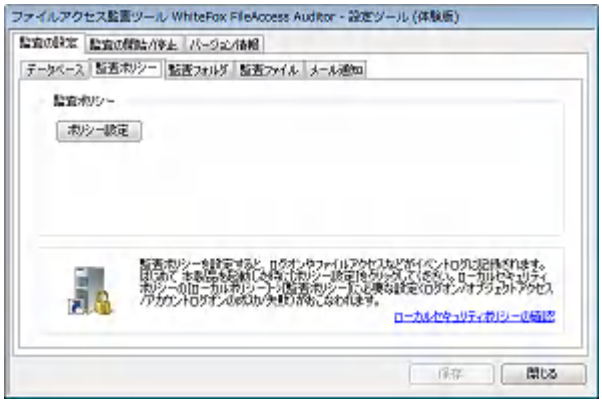
データベース接続が NG の場合、SQL Server サービスが稼働していない、ネットワーク経由で参照できないなどが考えられます。

5) データベース接続が OK の場合、右上の「データベース設定」の [新規作成] をクリックし、データベース名を入力し、[OK] をクリックします。

データベース作成エラーとなる場合、データベースサーバーのディスク容量が不足している、ログインに権限が不足しているなどが考えられます。

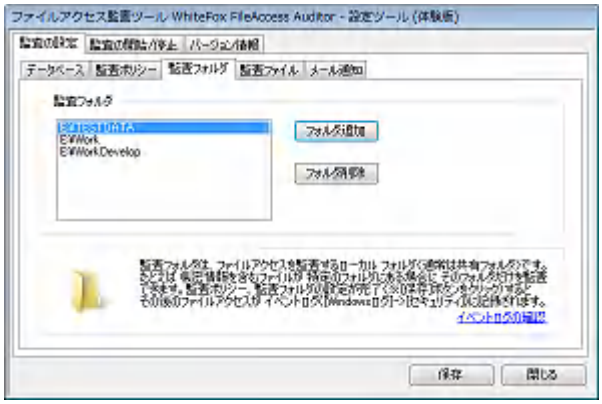
４．２　監査ポリシー設定

次に [監査の設定] タブの [監査ポリシー] タブで 監査ポリシーを設定します。左上の「監査ポリシー」の [ポリシー設定] をクリックすると ローカルセキュリティポリシーの監査ポリシーに ファイルアクセスログを記録するために必要な設定がおこなわれます。監査ポリシー設定は 設定ツールを はじめて起動したときに １度だけ行ってください。



４．３　監査フォルダ設定

次に [監査の設定] タブの [監査フォルダ] タブで ファイルアクセスを監査するフォルダを指定します。設定ツールをはじめて起動した際に、ローカルコンピュータの共有フォルダが自動的に一覧に追加されます。

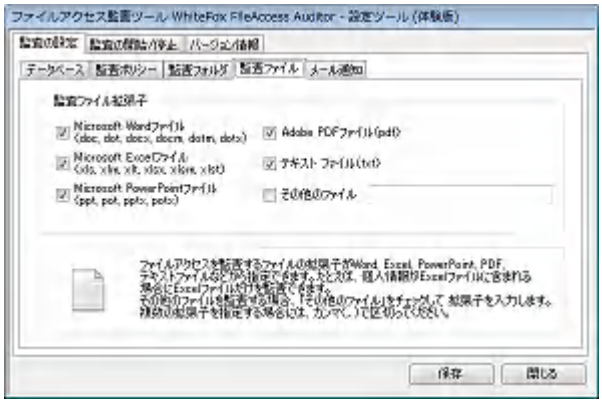


[フォルダ追加] をクリックすると フォルダを選択するダイアログが表示されますので、追加するフォルダを選択してください。監査フォルダの一覧で 不要なフォルダを選択し、[フォルダ削除] をクリックすると、監査対象から削除（除外）されます。

監査フォルダは 指定したフォルダ配下のサブフォルダ、ファイルです。例えば「D:¥Share」を監査フォルダに指定した場合、「D:¥Share¥SubFolder」は監査対象となります。

４．４　監査ファイル設定

次に[監査の設定]タブの[監査ファイル]タブで ファイルアクセスを監査するファイルの拡張子を指定します。Microsoft Word など 一般的なオフィスアプリケーションのファイル拡張子が選択できます。



Word,Excel,PPT,PDF,テキストファイル以外のファイル拡張子を監査対象とする場合は、[その他のファイル]をチェックし、ファイル拡張子を入力してください。複数のファイル拡張子を指定する場合は、「aaa,bbb」のように カンマ区切りで入力してください。

４．５　メール通知設定（オプション）

次に[監査の設定]タブの[メール通知]タブで エラーなどが発生した際のＥメール通知情報を設定します。差出人(FROM)、宛先(TO)、SMTP サーバーなどを入力し、[テストメール送信]をクリックすると テストメールが送信されます。エラー通知が不要であれば メール通知設定は不要です。

４．６　監査の開始/停止

データベース設定、監査ポリシー設定、監査フォルダ設定、監査ファイル設定が完了したら［監査の開始/停止］タブで監査を開始します。

ここまでの設定を保存する場合、画面右下の［保存］ボタンをクリックしてください。

監査の開始をクリックすると「１．３　本製品の構成」で説明した「監査サービス」が開始され、必要なファイルアクセスの記録（ログ）がデータベースに出力されます。監査サービスが開始している状態であれば［監査の停止］、停止している状態であれば［監査の開始］がクリックできます。

監査を開始したら、別コンピュータからファイルサーバーの共有フォルダにアクセスし、ファイルの作成／変更／削除／ファイル名変更／権限変更（読み取り専用などの設定/解除）をおこなうと、ファイルアクセスがデータベースに記録されます。

ファイルアクセスの記録は、ファイルアクセスが発生した日時よりも 数分程度（１～２分） 遅れてデータベースに記録されます。たとえば 18:30 に発生したファイルアクセスは、18:32 ごろにデータベースに記録されます。記録されるデータ（ファイルアクセスの日時）は、発生した日時どおりです。

データベースに記録されたファイルアクセス ログは 本製品のビューアで検索表示できます。ビューアについては「第５章 検索表示」を参照してください。

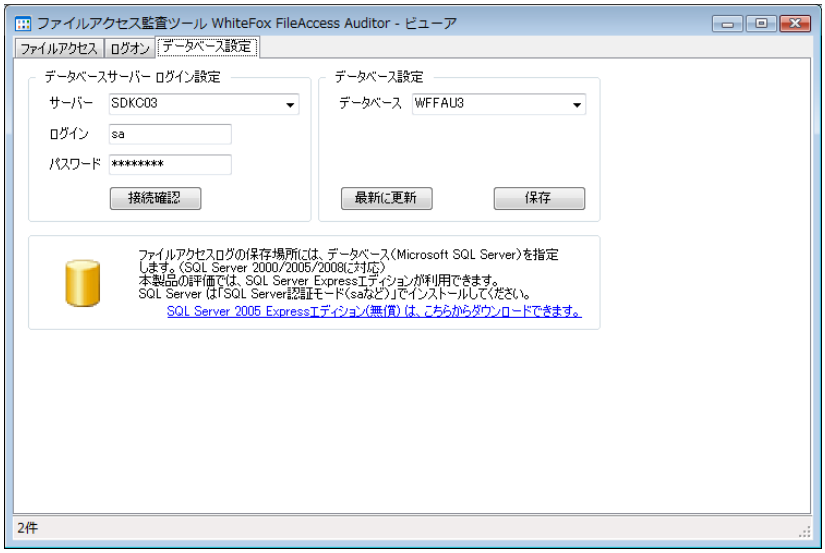
第５章　検索表示

ここでは、本製品のビューアの画面表示・操作について説明します。ビューアは、[スタート]メニュー → [すべてのプログラム] → [SDK-LTD]→ [WhiteFox FileAccess Auditor ビューア]をクリックすると起動できます。ビューアを終了するには、画面右上の[×]ボタンをクリックしてください。

５．１　データベースの設定

オールインワン構成（監査対象ファイルサーバーに本製品とデータベースをインストールする構成）の場合、本製品の「設定ツール」のデータベース設定が引き継がれます。

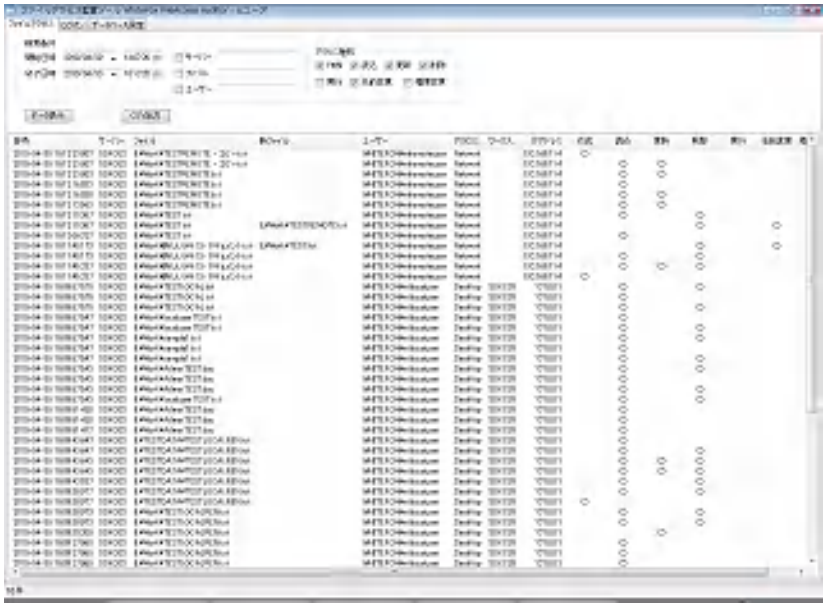
複数サーバー構成で データベースサーバーに 本製品のビューアのみをインストールした場合には、ビューアの[データベース設定]タブでデータベースを設定します。



1) 左上の「データベースサーバー ログイン設定」の「サーバー」で ネットワーク上のデータベースサーバー(SQL Server)を選択するか、サーバー名を入力します。
2) 「ログイン」に SQL Server のログイン（例：sa）を入力します。
3) 「パスワード」に パスワードを入力します。
4) [接続確認]をクリックします。
5) データベース接続が OK の場合、右上の「データベース設定」でデータベースを選択し、[保存]をクリックします。

５．２　ファイルアクセスの検索表示

ビューアの[ファイルアクセス]タブで ファイルアクセス ログの検索・表示ができます。画面上部の検索条件で 開始日時、終了日時を入力し、[データ表示]をクリックすると 画面下部に ファイルアクセス ログ（日時、サーバー名、ファイル名、新ファイル名、ユーザー名、アクセス場所、ワークステーション名、IP アドレス、アクセス種別）が表示されます。検索条件には サーバー名、ファイル名、ユーザー名、アクセス種別（作成／読込／更新／削除／実行／名前変更／属性変更）が指定できます。サーバー名、ファイル名、ユーザー名は 部分一致です。

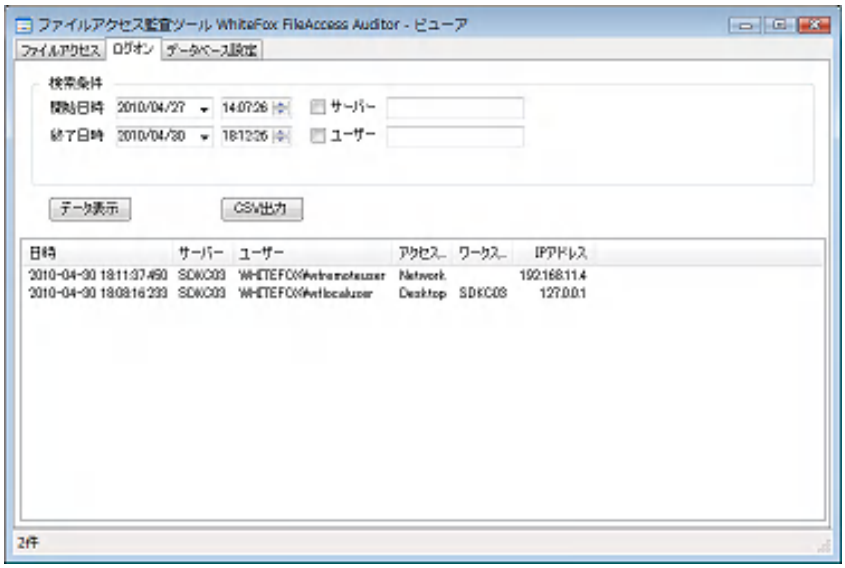


表示項目	説明
日時	アクセスした日時
サーバー名	アクセスしたサーバーのコンピュータ名
ファイル名	アクセスしたファイル名
新ファイル名	ファイル名を名前変更した場合の 新しいファイル名
ユーザー名	アクセスしたユーザー名（ドメイン名¥ユーザー名）
アクセス場所	アクセスした場所 Desktop：ローカルコンピュータへのログオン Network：ネットワーク経由のログオン
ワークステーション名	アクセスしたコンピュータ名 ※特定できない場合には 表示されません。
IP アドレス	アクセスしたコンピュータの IP アドレス ※アクセスに使われた通信により IPv4 または IPv6 の IP アドレスが表示されます。

表示項目		説明
アクセス種別		アクセスの種別
	作成	監査フォルダに 監査ファイル拡張子のファイルを新規作成した場合に発生 他のフォルダから移動した場合にも発生
	読込	監査フォルダの 監査ファイル拡張子のファイルを読み込んだ場合に発生
	更新	監査フォルダの 監査ファイル拡張子のファイルを変更した場合に発生
	削除	監査フォルダの 監査ファイル拡張子のファイルを削除した場合に発生 他のフォルダに移動した場合にも発生
	実行	監査フォルダの 監査ファイル拡張子のファイルを実行した場合に発生
	名前変更	監査フォルダの 監査ファイル拡張子のファイルを名前変更した場合に発生
	属性変更	監査フォルダの 監査ファイル拡張子のファイルの属性（読み取り専用、ファイル所有権など）を変更した場合に発生

５．３　ログオンの検索表示

ビューアの[ログオン]タブで ログオン ログの検索・表示ができます。画面上部の検索条件で 開始日時、終了日時を入力し、[データ表示]をクリックすると 画面下部に ログオン ログ（日時、サーバー名、ユーザー名、アクセス場所、ワークステーション名、IP アドレス）が表示されます。検索条件には サーバー名、ユーザー名が指定できます。サーバー名、ユーザー名は 部分一致です。



表示項目	説明
日時	ログオンした日時
サーバー名	ログオンしたサーバーのコンピュータ名
ユーザー名	ログオンしたユーザー名（ドメイン名¥ユーザー名）
アクセス場所	アクセスした場所 Desktop：ローカルコンピュータへのログオン Network：ネットワーク経由のログオン
ワークステーション名	アクセスしたコンピュータ名 ※特定できない場合には 表示されません。
IP アドレス	アクセスしたコンピュータの IP アドレス ※アクセスに使われた通信により IPv4 または IPv6 の IP アドレスが表示されます。