

LanScope Cat6

技術情報 Vol.24

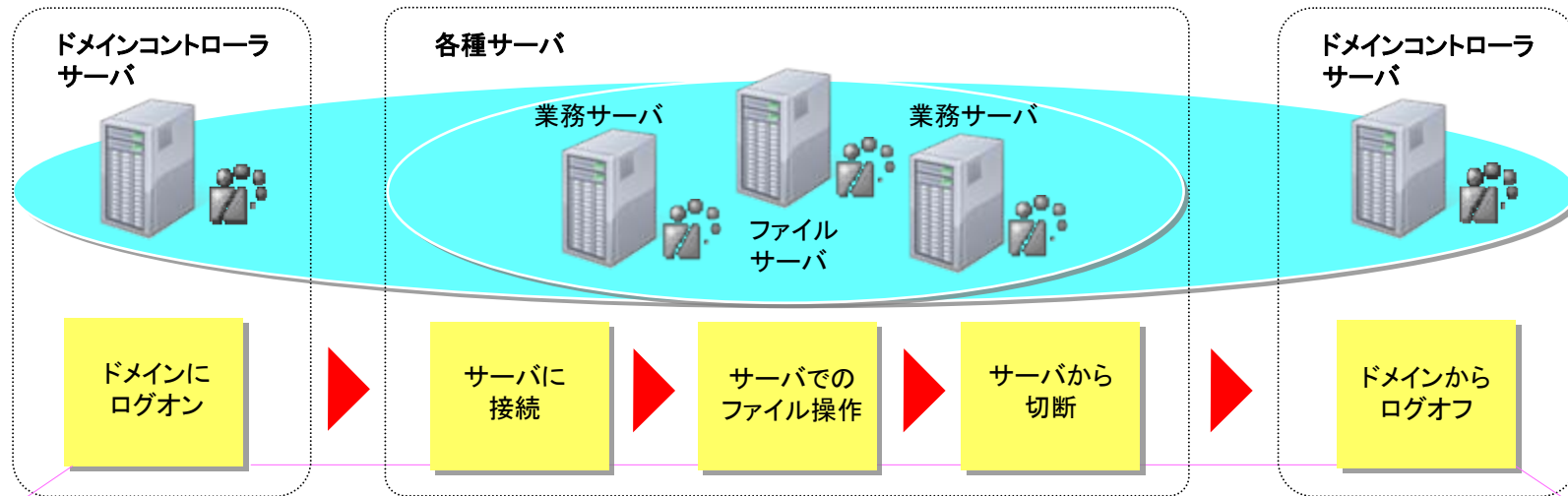
～サーバ監視機能のログ取得に関する技術情報～

2009年10月27日

第3版

エムオーテックス株式会社

●LanScope Cat サーバ監視機能の概要



出社から退社までの行為を3つのログでモニタリングできます。

ドメインへのログオン、ログオフ情報

ドメイン名	ログオンユーザ名	IPアドレス	ホスト名	イベント時刻	操作
SAPO26	luno	192.168.103.236	PC-0019	07:48:01	Logon
SAPO26	Administrator	192.168.102.126	SAPO-26	08:03:53	Logon
SAPO26	takahashi	192.168.101.115	PC-0005	08:04:08	Logon
SAPO26	sudou	192.168.100.105	PC-0029	08:06:36	Logon
SAPO26	hirose	192.168.101.108	PC-0034	08:15:43	Logon
SAPO26	inaba	192.168.103.238	PC-0018	08:16:07	Logon
SAPO26	endou	192.168.103.244	PC-0021	08:22:10	Logon
SAPO26	sudou	192.168.100.105	PC-0029	21:21:21	Logoff
SAPO26	Administrator	192.168.102.126	SAPO-26	21:45:02	Logoff

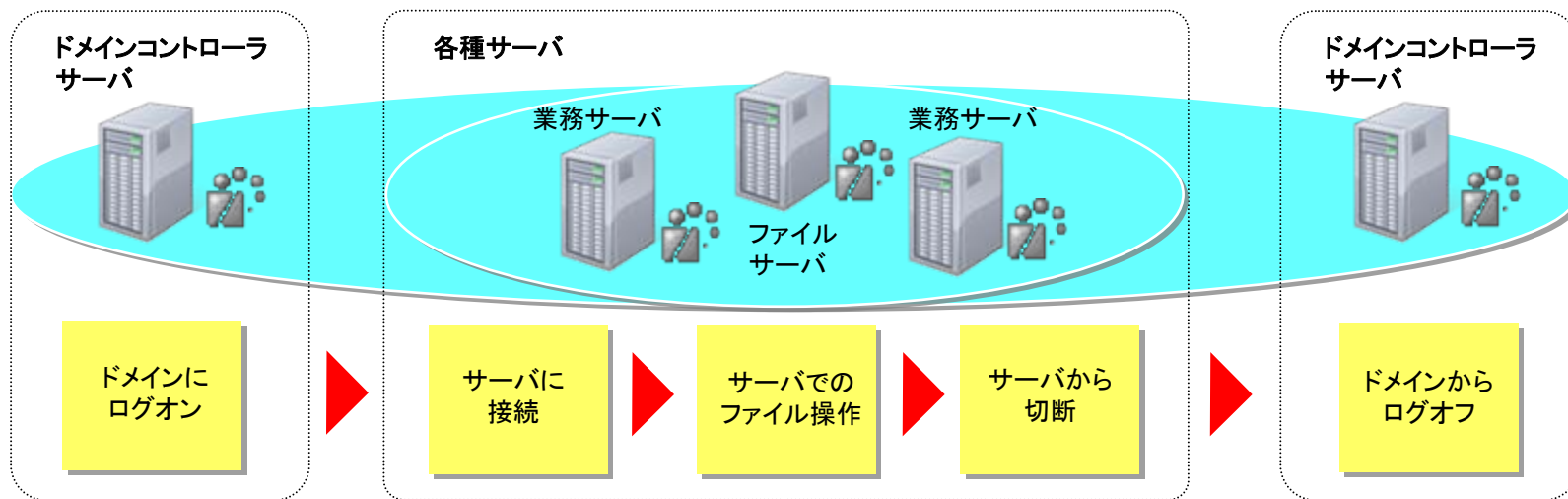
サーバへの接続、ファイル操作、サーバからの切断情報

ホスト名	イベント時刻	状態	ファイルパス	操作	アラーム種別
PC-0029	09:53:22	成功	-	接続	
PC-0029	09:53:41	成功	D:\共有\【社外秘】営業部\営業資料\最新営業資料.ppt	読出	
PC-0029	09:55:11	成功	D:\共有\【社外秘】営業部\営業資料\最新営業資料.ppt	読出	
PC-0029	09:55:11	成功	D:\共有\【社外秘】営業部\営業資料\最新営業資料.ppt	読出/書込	
PC-0029	09:55:15	成功	D:\共有\【社外秘】営業部\営業資料\最新営業資料.ppt	読出	
PC-0029	09:59:12	成功	-	切断	

サーバ監視機能で取得できる3つのログ

1. ドメインへのログオン、ログオフの履歴
2. サーバへの接続、切断の履歴
3. サーバ上のファイルへのアクセス履歴

●LanScope Cat サーバ監視機能の概要



3つのログを取得するには、それぞれのサーバで設定が必要です。

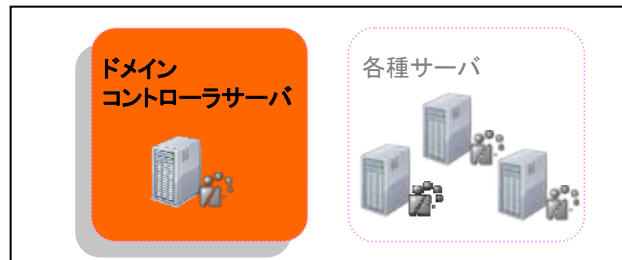
取得する情報	ドメインコントローラサーバでの設定	サーバでの設定	統合コンソールでの設定
ドメイン ログオン、ログオフの履歴	<ul style="list-style-type: none"> ・ログオンスクリプトの設定 ・ログオフスクリプトの設定 	—	<ul style="list-style-type: none"> ・サーバ監視設定画面での設定
サーバ 接続、切断の履歴	<ul style="list-style-type: none"> ・セキュリティポリシーの設定 ※1 	<ul style="list-style-type: none"> ・セキュリティポリシーの設定 	<ul style="list-style-type: none"> ・サーバ監視設定画面での設定 (アラームとログフィルタの設定)
サーバ ファイル操作の履歴	<ul style="list-style-type: none"> ・セキュリティポリシーの設定 ※1 ・フォルダのアクセス権の設定 ※1 ・監査の設定 ※1 	<ul style="list-style-type: none"> ・セキュリティポリシーの設定 ・フォルダのアクセス権の設定 ・監査の設定 	<ul style="list-style-type: none"> ・フォルダ監視設定画面での設定

※1・・・ドメインコントローラとファイルサーバや業務用サーバを兼用しているサーバで、サーバへの接続、切断、ファイルの操作履歴を取得する場合に設定します。

●ドメインへのログオン、ログオフの履歴を取得する仕組みと設定項目

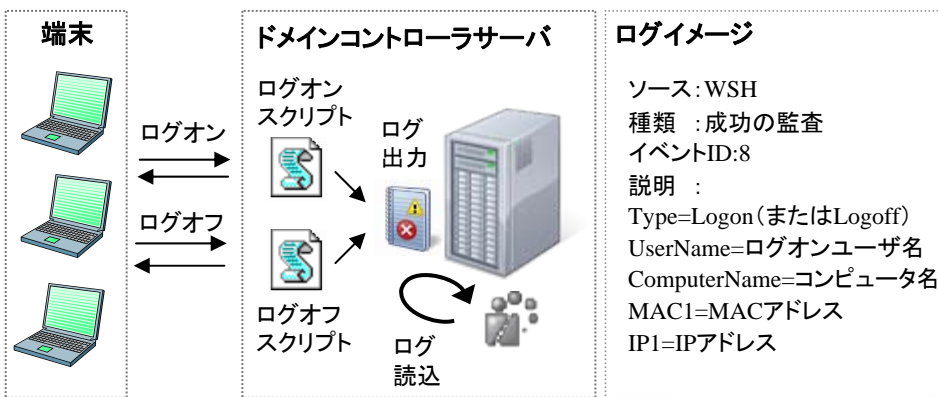
必要となる環境やライセンス

- ・ドメイン環境
- ・ドメインコントローラサーバ用のサーバエージェント(SA)ライセンス
 ※ドメインコントローラサーバとファイル操作を取得するサーバが同じサーバの場合は、サーバエージェントは同じライセンスで利用することができます。



動作仕様

ログオンスクリプト、ログオフスクリプトを利用し、ログオン時、ログオフ時にアプリケーションログを出力します。
 出力されたアプリケーションログをサーバエージェントが取得します。



※スクリプト用のvbsファイルは、SAのインストールフォルダに作成されます。

必要となる設定

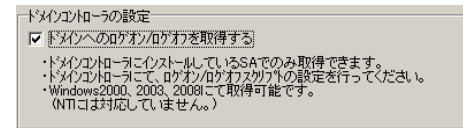
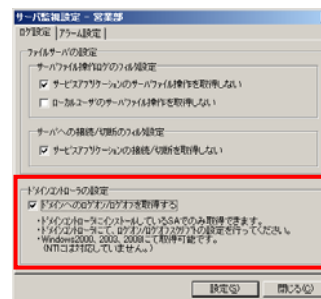
ドメインコントローラサーバと統合コンソールで設定が必要です。

○ドメインコントローラサーバでの設定

- ・ログオンスクリプトの設定
- ・ログオフスクリプトの設定

※設定後にドメインコントローラサーバの再起動が必要です。

○統合コンソールでの設定



「ドメインへのログオン/ログオフを取得する」にチェックを入れます。

制限事項

- ・ドメインコントローラがWindowsNT4.0、Windows Server 2008 R2の環境には対応していません。
- ・ログオンの失敗の情報は取得しません。

アラーム機能

ドメインへのログオン、ログオフの履歴を取得する機能については、アラーム機能はありません。

●サーバへの接続、切断の履歴を取得する仕組みと設定項目

必要となる環境やライセンス

・接続するサーバに対するサーバエージェント(SA)ライセンス

※複数のサーバの接続履歴を取得する場合、サーバごとにサーバエージェントのライセンスが必要です

ドメイン
コントローラサーバ

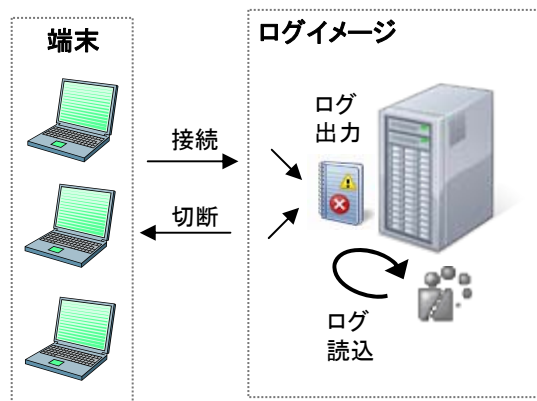


各種サーバ



動作仕様

接続先のサーバの**セキュリティログ**に出力されるファイル操作の情報をサーバエージェントが取得します。



セキュリティログのイベントID

OS	接続成功	接続失敗	切断
NT	528	529	538
2000	540	529	538
XP	540	529	538
2003	540	529	538
2008	4624	4625	4634

必要となる設定

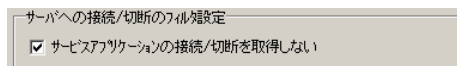
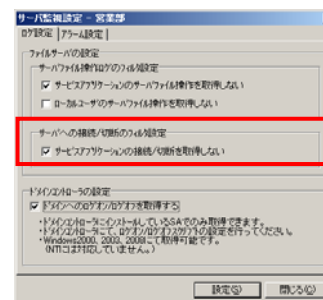
接続する各種サーバと統合コンソールで設定が必要です。

○各種サーバでの設定

- ・セキュリティポリシーの設定で「ログオンイベントの監査」を取得する設定
「成功」・・・必須設定 「失敗」・・・必要に応じて設定

※設定後に各種サーバを再起動する必要はありません。

○統合コンソールでの設定



「サーバへの接続/切断ログのフィルタ設定」を選択します。

サービスアプリケーションの接続/切断の情報を取得する必要がない場合は、チェックを入れて運用してください。

制限事項

- ・接続先のサーバが、NT、2000、XPの場合、接続時のログのIPアドレスが空白になります。
- ・切断時のログはIPアドレス、コンピュータ名が空白になります。
- ・アクセスしていないユーザからの接続/接続失敗のログが発生することがあります。

アラーム機能

- サーバへの接続が失敗した場合にアラームにすることができます。
- サーバ監視設定の「アラーム設定」タブ画面で設定します。
- ※アクセスしていない接続失敗ログが発生するため、接続失敗の監査が必要なサーバ以外ではアラームは設定しない形での運用をお奨めします。

●サーバ上のファイル操作履歴を取得する仕組みと設定項目

必要となる環境やライセンス

・接続するサーバに対するサーバエージェント(SA)ライセンス

※複数のサーバの接続履歴を取得する場合、サーバごとにサーバエージェントのライセンスが必要です

ドメイン
コントローラサーバ

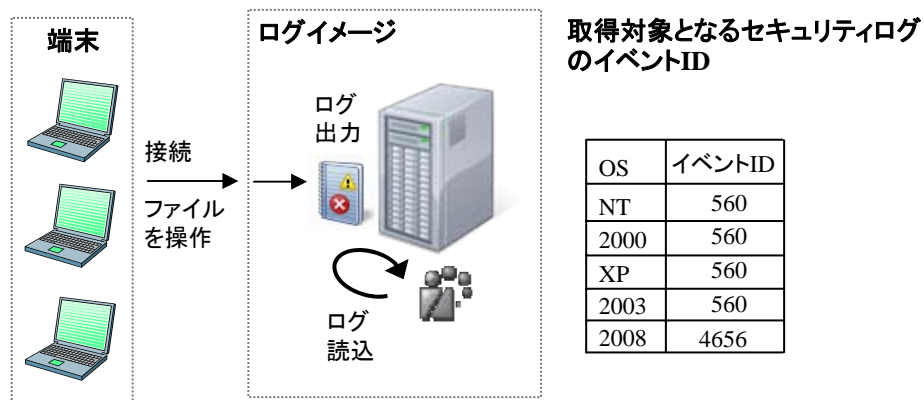


各種サーバ



動作仕様

サーバのファイルにアクセスした時に**セキュリティログ**に出力される情報をサーバエージェントが取得します。



必要となる設定

接続する各種サーバと統合コンソールで設定が必要です。

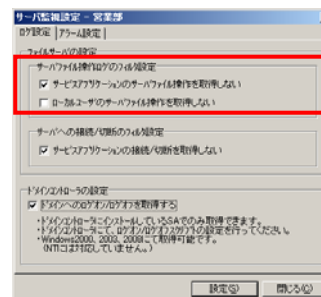
○各種サーバでの設定

- ・セキュリティポリシーの設定で「オブジェクトアクセスの監査」を取得する設定「成功」、「失敗」共に必須設定

○統合コンソールでの設定

ログを取得するための設定とフィルタするための設定の2つの設定があります。

- ・ログを取得するための設定・・・フォルダ監視設定
- ・ログをフィルタするための設定・・・サーバ監視設定



「サーバファイル操作ログのフィルタ設定」を選択します。

制限事項

- ・接続先のサーバがNT、2000、XPの場合、操作ログのIPアドレスが空白になります。
- ・OSのセキュリティログに準拠してログを取得しているため、実際の操作と異なる内容の操作ログが余分に発生する場合があります。
例：ファイル削除時にファイル削除+名前変更のログ等

アラーム機能

ファイルの削除、ファイル操作の失敗、業務時間外操作をアラームにすることができます。

●サーバ監視機能のフィルタの仕組み(統合コンソールでの設定)

管理上必要のないログを取得しないようにフィルタすることができます。

統合コンソールとサーバエージェント上のFilter.iniファイルからフィルタを設定できます。

・統合コンソール⇒サーバ表示⇒サーバ監視設定

- サーバファイル操作ログのフィルタ設定
- サーバへの接続/切断のフィルタ設定

ドメイン
コントローラサーバ

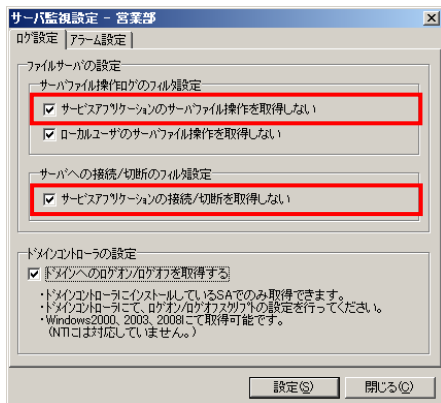


各種サーバ



サービスアプリケーションのフィルタ設定画面のイメージ

サービスで起動しているアプリケーションによるファイルアクセスの操作ログや接続/切断ログをフィルタすることができます。



設定情報の適用方法

設定ボタンをクリックするとSAのレジストリに設定情報をリアルタイムに書き込み適用します。

設定が有効になるタイミング

設定ボタンをクリックすると設定がすぐに有効になります。サーバエージェントの再起動は必要ありません。

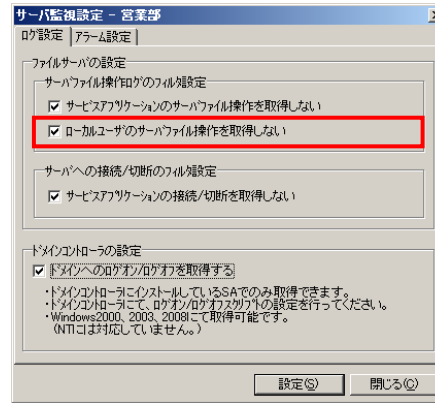
フィルタの対象となるサービスアプリケーションの定義

セキュリティログの「イベントID:560」の情報より判断します。
以下の組み合わせの場合に、サービスアプリケーションと判断します。

- ・プライマリユーザ名 : コンピュータ名 \$
- ・クライアントユーザ名: -

ローカルユーザのファイル操作のフィルタ設定画面のイメージ

サーバエージェントをインストールしているサーバにローカルでログインしてファイルにアクセスする際の操作ログをフィルタすることができます。



設定情報の適用方法

設定ボタンをクリックするとSAのレジストリに設定情報をリアルタイムに書き込み適用します。

設定が有効になるタイミング

設定ボタンをクリックすると設定がすぐに有効になります。サーバエージェントの再起動は必要ありません。

フィルタの対象となるローカルユーザのファイル操作の定義

セキュリティログの「イベントID:560」の情報より判断します。
以下の組み合わせの場合に、ローカルユーザのファイル操作と判断します。

- ・プライマリユーザ名 : ログオンユーザ名
- ・クライアントユーザ名: -

●サーバ監視機能のフィルタの仕組み(Filter.iniでの設定)

管理上必要のないログをフィルタすることができます。

統合コンソールとサーバエージェント上のFilter.iniファイルでフィルタを設定できます。

・サーバエージェントのインストールフォルダ⇒Filter.ini

ドメイン
コントローラサーバ



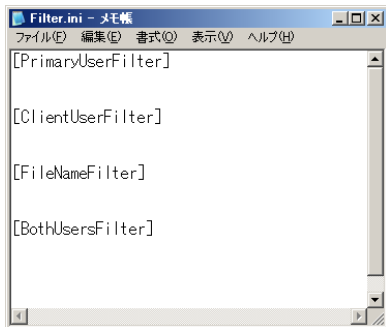
各種サーバ



Filter.iniによるフィルタ設定項目

Filter.iniの各項目にフィルタ条件を入力する方法で、条件に合致する
サーバファイル操作ログをフィルタすることができます。

セキュリティログの「イベントID:560(Win2008はID:4656)」の情報より判断します。



※「~\$xxx.doc」、「.tmp」、「.lnk」、「.ldb」の4つのファイルは、サーバエージェントによって自動的にフィルタされます。そのため、上記のファイル名については、Filter.iniに登録する必要はありません。

フィルタ方法は4パターンあります。

- [PrimaryUserFilter] ...セキュリティログのプライマリユーザ名でフィルタします。
- [ClientUserFilter] ...セキュリティログのクライアントユーザ名でフィルタします。
- [FileFilterName] ...セキュリティログのファイル名でフィルタします。
- [BothUsersFilter] ...プライマリユーザ名、クライアントユーザ名の両方の条件に合致するログをフィルタします。

設定方法の詳細は、サーバ監視操作ガイド、もしくは、「SAアカウントフィルタ設定手順書」に記載しています。

統合コンソールとFilter.iniのフィルタ設定の使い分けサンプル

ファイル名でのフィルタや、特定のユーザのファイル操作のフィルタは、Filter.iniで設定してください。

フィルタ例	統合コンソールの設定	Filter.iniでの設定
ファイル名でフィルタする	×	○
特定のユーザの操作をフィルタする	×	○
サービスアプリケーションを全てフィルタする	○	×
ローカルでのファイル操作をフィルタする	○	○
接続/切断ログのフィルタを設定する	○	×

○:設定できる ×:設定できない

Filter.iniの設定が有効になるタイミング

サーバエージェントの起動時にFilter.iniファイルの内容を読み込みます。そのため、Filter.iniの保存後、サーバエージェントの再起動が必要です。

●サーバ監視機能とリアルタイムイベントログの連携の仕組み

サーバのファイルを端末にコピー、または、移動した後のファイル操作を、Webコンソール画面で追跡できます。

サーバ監視機能のサーバファイル操作ログと、リアルタイムイベントログ(標準パッケージ)の2つのログを連携させて、サーバから端末までのファイルの操作を追跡できます。

- ・Webコンソールのサーバセキュリティ⇒「操作」アイコン⇒リアルタイムイベントログ



Webコンソールの画面イメージ

サーバアクセスの集計情報から個別の操作が分かり、更にファイルがローカルに移った後の操作まで分かります。

サーバセキュリティ(サーバ監視機能)

ログオンユーザ	合計	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
uchida	711(43)	0	0	5	43	30	35	30	21	0	15	20	30	2	10	31	9	0	50	13	41	33	71	0	0	20	60	66	33	4(15)	0	0
sano	651	0	0	15	21	8	32	10	0	20	40	14	40	4	0	94	22	14	21	9	0	148	51	78	12	52	0	0	0	0		
sudou	583	0	0	21	4	14	78	22	0	0	14	7	31	18	44	0	0	21	35	34	14	17	0	0	22	40	14	85	28	0	0	

集計から個別のファイル操作にたどりつきます。

2006/07/28	15:56:00	成功	D:\共有\【社外秘】営業部\営業1課用\顧客フォルダ\顧客リスト.xls	PC-0026	読出	操作
------------	----------	----	---------------------------------------	---------	----	-----------

リアルタイムイベントログ(標準パッケージ)

端末でファイルをどのように操作したのかが確認できます

ユーザ	時刻	操作	ファイル名	パス	結果
k-uchida	15:56:00	FileCopy	ファイルコピー元	\\192.168.102.241\【社外秘】営業部\営業1課用\顧客フォルダ\顧客リスト.xls	カスタム
k-uchida	15:56:00	FileCopy	ファイルコピー先	C:\Documents and Settings\uchida\Desktop\顧客リスト.xls	カスタム
k-uchida	15:57:00	00002	ACTIVE	OUTLOOK.EXE	送信済みアイテム - Microsoft Outlook
k-uchida	15:57:00	00006	ACTIVE	WINWORD.EXE	無題のメッセージ
k-uchida	15:57:00	00007	ACTIVE	WINWORD.EXE	ファイルの挿入
k-uchida	15:57:00	00203	ACTIVE	WINWORD.EXE	これです - メッセージ
k-uchida	15:57:00	FileRen	ファイル名変更前	C:\Documents and Settings\uchida\Desktop\顧客リスト.xls	カスタム
k-uchida	15:57:00	FileRen	ファイル名変更後	C:\Documents and Settings\uchida\Desktop\商品案内.xls	
k-uchida	15:58:00	00028	ACTIVE	OUTLOOK.EXE	送信済みアイテム - Microsoft Outlook

サーバファイル操作ログとリアルタイムイベントログの連携の仕組み

- ・サーバ監視機能の接続切断ログ
- ・標準パッケージの資産管理一覧

のホスト名の情報と、サーバ監視のサーバファイル操作ログの日時の情報から端末のファイル操作ログを紐付けしています。

サーバファイル操作一覧 - 営業部								
2006/07/28	サーバ接続/切断ログを表示							
クライアント名	クライアントユーザ名	IPアドレス	ホスト名	イベント時刻	状態	ファイルパス	操作	アラーム種別
-	uchida	192.168.102.208	PC-0026	08:37:49	成功	-	接続	

資産管理一覧 - 東京本社						
エージェントNO	エージェント名	IPアドレス	ホスト名	部署名1	部署名2	部署名3
2	内田 健太	192.168.102.208	PC-0026	全社	東京本社	営業部

ログの連携条件

- ・リアルタイムイベントポリシーのファイル操作ログを取得している場合に有効です。
- ・ライセンスを付与しているMRと紐付けできます。
※ライセンスを解除している場合は、紐付けされません。
- ・資産管理一覧画面に同じホスト名のエージェント情報が複数ある場合、前回起動日の日付が新しい方のエージェントと紐付けします。

サーバと端末でのファイルの操作を確認できる期間

環境設定で設定する、サーバファイル操作ログとリアルタイムイベントログの保存日数分のログを確認することができます。(2~90日分)