

待望の新機能！

「監査ログ分析レポート」発売開始！

(Audit Analysis Advisory report= 'AAA')

「監査ログ高速検索」と連動する ログ運用・分析の決定版！！

CWATログ運用ツールとしてご好評いただいている、Audit Finder Extreme/Diagnosisに新たな機能として「監査ログ分析レポート」(略称:AAA=Audit Analysis Advisory report)を発売致します。

この機能は、監査ログを「イベント別集計レポート」として集計し、そこから「時間帯別集計」、「日毎のイベント件数別ランキング集計」にドリルダウン、または特定のイベントについて「ユーザー別トップ10」、「PC別トップ10」を集計表示し、さらに「監査ログ検索」に抽出条件を自動設定した上で連動する画期的な機能です。

従来からの「監査ログ高速検索」「警告レポート」「アーカイブ」の各機能に加え、今まで内容を掴みにくかった監査ログの傾向を洗い出し、分析から検索までを連動して実行出来る、画期的な機能です。

【Audit Finder (全体) の機能】

【監査ログ分析/レポート機能】

監査ログをイベント別に集計し、時間帯別集計、日毎のランキング表示によりPC利用の傾向を「見える化」し、更に検索機能への連動により分析に威力を発揮します。

新機能

【監査ログ高速検索】

CWATで生成された監査ログをCSVファイルに抽出し、弊社独自の検索エンジンにより、設定された条件に基づいた高速検索を行います。

【警告ログレポート】

指定した期間の警告ログを集計し、「警告件数サマリーレポート」と「警告明細レポート」を自動、手動で出力します。

【アーカイブ】

保存期間を経過した警告ログ、監査ログデータを定期的にアーカイブします。アーカイブしたデータをリストアップ検索することも出来ます。

【監査ログ分析レポートの機能】

イベント別集計レポートを作成

Audit Finder イベント別集計 (週間)

レポート出力日時: 2009/02/20 19:20:36
集計対象期間: 2009/02/09 ~ 2009/02/15

イベント	2月9日 (月)		2月10日 (火)		2月11日 (水)		2月12日 (木)		2月13日 (金)		2月14日 (土)		2月15日 (日)		合計	
	件数	ラック	件数	ラック	件数	ラック	件数	ラック	件数	ラック	件数	ラック	件数	ラック	件数	ラック
ファイルの印刷	324	3	345	2	245	2	226	186	147	1	107			1,580		
スクリーンショット	242		276	3	143		645	542	123	2	561			2,532		
アプリケーションのインストール	160		207		41		1,064	898	99	3	1,015			3,484		
外部メディア書き出し	78		138		61		1,484	3	1,254	3	76			4,559	3	
新規外部機器の接続	1,213	1	69		163	3	1,903	2	1,610	2	52			6,932	2	
メールの送信	453	2	632	1	265	1	2,322	1	1,965	1	28			8,042	1	
早朝(0時~7時)	0		0													
午前(7時~12時)	118		110													
午後(12時~17時)			254													
夜間(17時~21時)	126		226													
深夜(21時~24時)	20		42													
Webメールの送信																
Web参照																
Web操作																
電源ON監視(休日のみ)																
ログオン監視	700		825		30		944	1,300	120							



時間帯別集計をドリルダウン表示

- ・早朝(0時~7時)
- ・午前(7時~12時)
- ・午後(12時~17時)
- ・夜間(17時~21時)
- ・深夜(21時~24時)

イベント別ランキング集計レポートを作成

- ・ユーザー別トップ10
- ・PC別トップ10

Audit Finder ランキング集計 (週間)

レポート出力日時: 2009/02/20 19:20:36
集計対象期間: 2009/02/09 ~ 2009/02/15
集計対象イベント: 外部メディア書き出し

ユーザー別ランキング		2月9日	2月10日	2月11日	2月12日	2月13日	2月14日	2月15日	合計
順位	ユーザー名	件数	件数	件数	件数	件数	件数	件数	件数
1	Administrator	30	17	6	3	1	1	1	63
2	I00099	17	17	1	1	1	1	1	38
3	I00123	6	1	1	1	1	1	1	11
4	I00001	1	1	1	1	1	1	1	5
5	I00576	1	1	1	1	1	1	1	5
6	Kanri	3	1	1	1	1	1	1	8
7	I00176	1	1	1	1	1	1	1	5
8	I00075	1	1	1	1	1	1	1	5
9	I00098	1	1	1	1	1	1	1	5
10	S00011	1	1	1	1	1	1	1	5
計		63	38	11	8	8	8	8	136

PC別ランキング		2月9日	2月10日	2月11日	2月12日	2月13日	2月14日	2月15日	合計
順位	PC名	件数	件数	件数	件数	件数	件数	件数	件数
1	PC02-04	30	17	6	3	1	1	1	63
2	PC07-04	17	17	1	1	1	1	1	38
3	PC04-11	6	1	1	1	1	1	1	11
4	PC04-09	1	1	1	1	1	1	1	5
5	PC02-43	1	1	1	1	1	1	1	5
6	PC02-11	1	1	1	1	1	1	1	5
7	PC02-16	1	1	1	1	1	1	1	5
8	PC04-08	1	1	1	1	1	1	1	5
9	PC04-19	1	1	1	1	1	1	1	5
10	PC07-04	1	1	1	1	1	1	1	5
計		63	38	11	8	8	8	8	136

検索条件を自動設定し検索実行

「集計・レポート」から「検索」へと連動する画期的機能

ユーザー別ランキング

順位	ユーザー名	件数	ユーザー名
1	Administrator	30	Administrator
2	I00099	17	Kanri
3	I00123	6	I00099
4	I00001	1	I00001
5	I00576	1	I00541
6	Kanri	3	I00002
7	I00176	1	
8	I00075	1	
9	I00098	1	
10	S00011	1	
計		63	

【Audit Finder検索画面】

検索条件が入力された状態で、検索画面を表示

【開発元】

株式会社アイ・ティー・ワン

ソリューション営業本部

〒160-0022

東京都新宿区新宿2-8-8 とみん新宿ビル

TEL(03)5363-5891 FAX(03)5363-5892

http://www.it-one.co.jp