

情報セキュリティ E X P O

WEEDS

TRUE TECHNOLOGY TO THE WORLD

SASのセキュリティ対策にはWEEDS SAS - Trace

2009年5月15日(金)

ウィーズ・システムズ株式会社
営業部 星 光史

環境変化対応型情報処理技術集団
ウィーズ・システムズ株式会社

SAS

ビジネス・インテリジェンス[BI]ツールの代表格「SAS」は、多くの企業で使われ様々なデータマイニングに使用され続けています。
データを色々な角度から分析し、ビジネスを加速させる「SAS」は、企業内の非常に重要なデータを取り扱う場合が多いです。

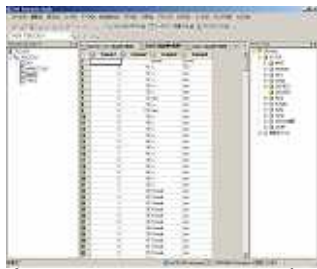
課題



サーバー側で演算処理した記録をログとして出力しますが、サーバーでの処理に限られ、クライアント側の操作は記録されません。

クライアント操作でデータを参照、コピー、貼り付け、インポート、エクスポートなど、監査が必要なアクセス状況を把握する事が困難でした。

WEEDS SAS - Trace開発の背景



SASクライアントでの操作

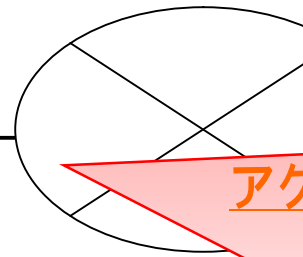
- ・データ参照
 - ・データEXPORT操作
 - ・データIMPORT操作
 - ・印刷操作
- などの操作履歴の取得が困難

- SASサーバーより出力されるログには、
- ・SAS9を利用したPCのIPアドレス
 - ・アクセスした時間
 - ・アクセス処理内容の詳細
 - ・DataSetに対する変更
- などの情報が出力



SASクライアント

分析処理



これらの記録は、
アクセスした処理時間(主にパフォーマンス)
に着目したもので、
情報漏洩やIT統制の観点における記録内容
ではありません。

WEEDS SAS-Traceとは？

WEEDS Traceシリーズ「WEEDS Windows-Trace」をSASクライアントソフト用にログ取得機能を強化し、SASクライアント側の操作を取得しログ生成します。どのデータセットを参照したか、サーバーからデータをインポートしたか、Excelでタスクを実行したか、など、誰が・いつ・どの端末で実行したか、取得し監査することができます。

SASクライアントでの操作と、SASサーバーへのアクセスを突合し、SAS全体の操作記録をレポートニングできることが実現できます。これで、SASの操作記録は完全に取得でき、監査証跡としても十分な記録を残すことができます。

SAS操作記録を監査レポートとして出力する事が出来るので、システム監査、内部統制など様々なシーンでご活用いただけます。

WEEDS SAS - Trace操作履歴取得内容 「SAS Enterprise Guide」

SAS Enterprise Guideは、標準的なものから高度なものまで多岐にわたった解析機能と、それらを簡易に実行する操作性を提供する機能です。主な機能として、

- ローカルPC上のSASデータ、および Microsoft Excel や Microsoft Access などの外部ファイル / データへのアクセス
- SAS Systemサーバ上のSASデータや、Oracle、DB2 など他のリレーショナルデータベースへのリモートアクセス
- SASデータをUNIXからPCへ・・・といった移動がドラッグ&ドロップで可能 など様々な操作が可能です。

EGクライアント操作履歴を全て取得するのがWEEDS SAS-Traceです。

<データエクスポート>

<データアクセス>

SAS EG操作

WEEDS SAS-Trace
Client

<データインポート>

<プリントアウト>

左記のような様々な操作内容を取得し、
監査レポートとして出力します。

EGでSASデータが正しく使用されている
という事を証明する事が出来ます。

IT統制対応・セキュリティ強化・システム監査
など様々な舞台にご活用頂けます。

WEEDS SAS - Trace操作履歴取得内容 「SAS Enterprise Miner」

SAS Enterprise Minerは、データマイニングに求められるすべてのプロセスを一元的に実行・管理できる、業界唯一のデータマイニング統合ツールです。主な機能として、

- ・サンプル抽出（膨大なデータから傾向を損なわないようにサンプルを作成したり、様々な形式にデータを分割。）
- ・データ探索（データの特徴を統計的・視覚的に捉え、データ加工の準備）
- ・データ加工（分析のためのデータ準備を行い、変数の追加や既存変数の変換、自己組織化マップの作成など豊富なデータ加工機能を実装）など様々なデータ加工が可能です。

EMクライアント操作履歴を全て取得するのがWEEDS SAS-Traceです。

<データアクセス>



SAS EM操作



WEEDS SAS-Trace
Client

<データ分析>



左記のような様々な操作内容を取得し、
監査レポートとして出力します。



データ分析におけるセキュリティ補強を
実現します。



IT統制対応・セキュリティ強化・システム監査
など様々な舞台にご活用頂けます。

<データ加工>



<データ変換>

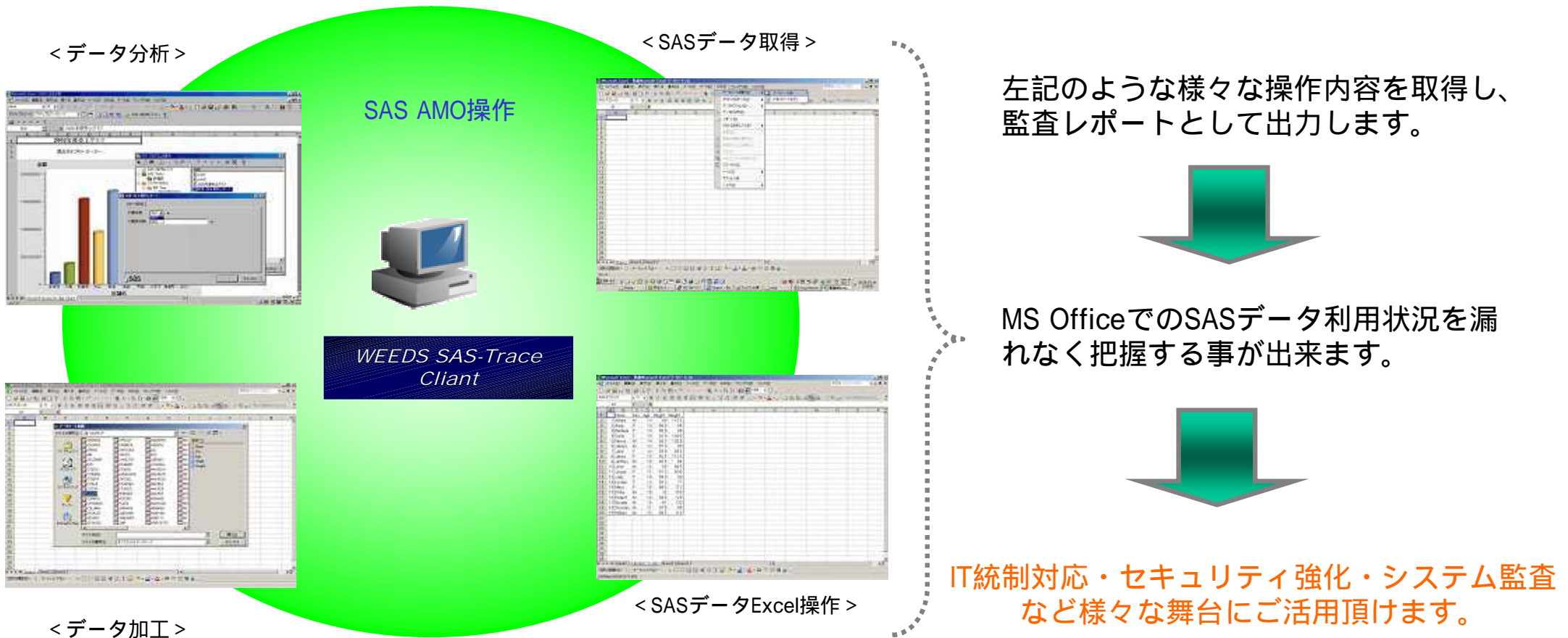


WEEDS SAS - Trace操作履歴取得内容 「SAS Add-In for Microsoft Office」

SAS Add-In for Microsoft Officeは、Microsoft Officeのメニューから直接SASを実行し、データの分析結果を取得し高度な分析機能を利用出来ます。主な機能として、

- ・Microsoft Officeユーザーが使用可能な高度な分析機能
- ・容易にSASデータにアクセスし、クエリやデータ分析を実行、レポートを作成
- ・使い慣れたWordやExcelインターフェイスにてデータ加工、分析が実現などが実現出来ます。

AMOクライアント操作履歴を全て取得するのがWEEDS SAS-Traceです。



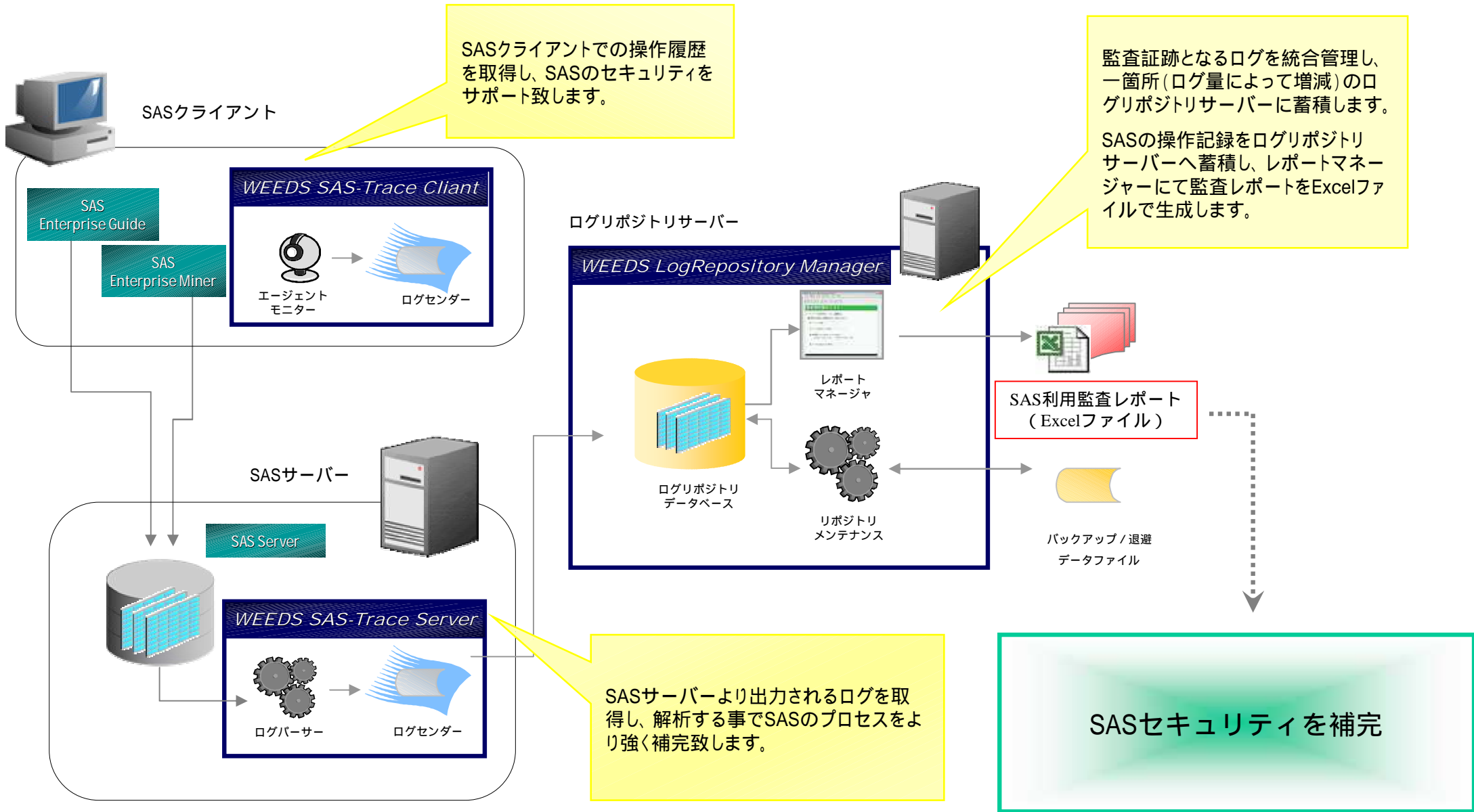
SASのセキュリティ対策への対応

WEEDS SAS-Traceでは、SAS単体では取得不可能なクライアント側でのアクセス履歴を全て取得する事により、SASセキュリティ対策への対応が可能となります。

SASの利用状況を正確に把握

セキュリティはもちろんの事、TCOの観点でSASの利用状況を正確に把握し、サーバーの拡張や、ユーザーの拡大を図る上での基礎情報を導き出す事が可能となります。

WEEDS SAS - Traceシステム概要



機能要件に対する対応策

セキュリティ機能要件

SAS - Trace
標準機能にて対応

SAS - Trace
カスタマイズにて対応

<p>特権IDによる操作をすべて記録するような設定にしている。</p>	<p>* 標準機能</p>	
<p>情報システムのログイン時に、以下の情報を提供する機能を設定している。 前回アクセスの日付、時刻、成功・失敗の区別等のログイン履歴情報。</p>	<p>* 標準機能</p>	
<p>利用者および運用者等の個人データへのアクセス記録が系統的に記録され、当該記録が分析・保管されている。</p>	<p>* 標準機能 SAS-TRACEのリポジトリに全てのアクセス履歴が格納されます。</p>	
<p>利用者および運用者等の個人データへのアクセス記録はディスク内へ保管され、アクセス記録のアクセスはシステム管理権限を持つ者に限定される。</p>	<p>* 標準機能 リポジトリ内の情報は、個別に設定されたIDにてアクセスします。</p>	
<p>アクセス実績記録を作成している。系統的に取得できない場合、手作業でアクセス実績記録を作成している。</p>	<p>* 標準機能 SAS上の操作は自動的に記録されます。</p>	

機能要件に対する対応策

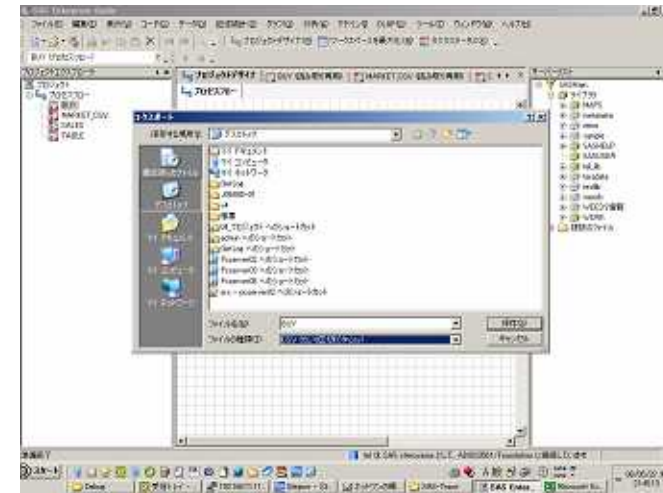
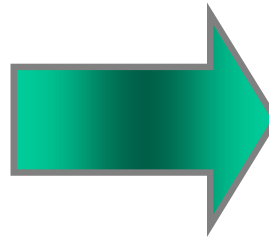
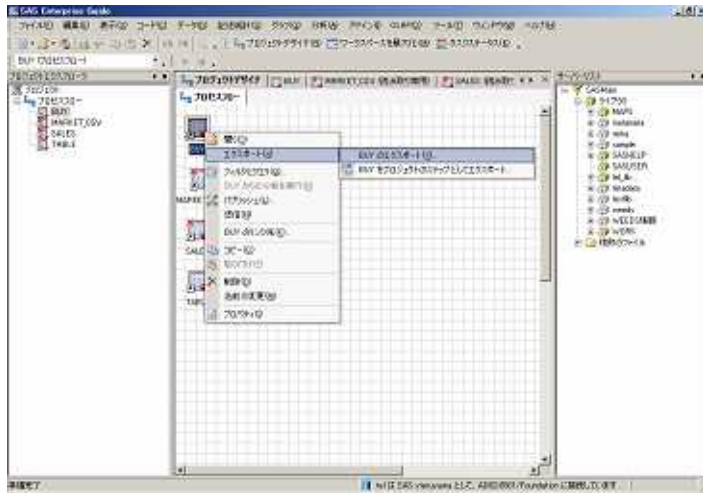
セキュリティ機能要件

SAS - Trace 標準機能にて対応

SAS - Trace カスタマイズにて対応

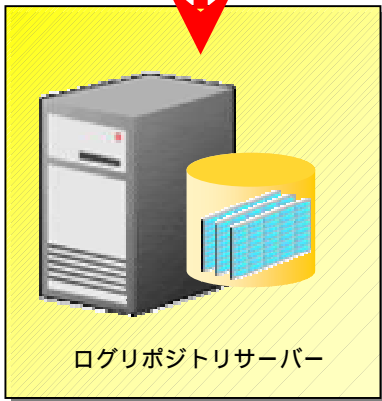
<p>アクセス実績記録の検証にて不正使用が発見された場合は、情報セキュリティ責任者まで報告をする。</p>		<p>* 個別カスタマイズ 監査上において、報告が必要なレポートがあった場合は、自動的に管理者へメールする</p>
<p>利用者および運用者等の個人データへのアクセス記録を、定期的に分析している。</p>	<p>* 標準機能</p>	
<p>不正アクセスに備え、監視機能を組み込み監視している。 ～ 例としては以下のとおり ・モニタリング ・アクセスログ ・アラーム、等</p>	<p>* 標準機能 指定IP又は通常利用PC以外のアクセスレポート</p>	
<p>アクセス実績記録の検証を操作担当者以外の管理部署で行わせている。</p>	<p>* 標準機能 SAS-TRACEのリポジトリ監査は、専用のIDにて監査レポートを生成する</p>	

WEEDS SAS - Traceサンプルレポート 「EG操作:SASデータエクスポート」



<データエクスポート>

<操作履歴取得>



ログリポジトリサーバー

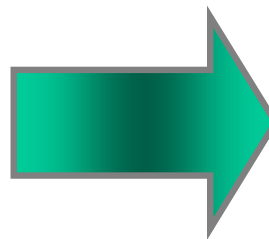
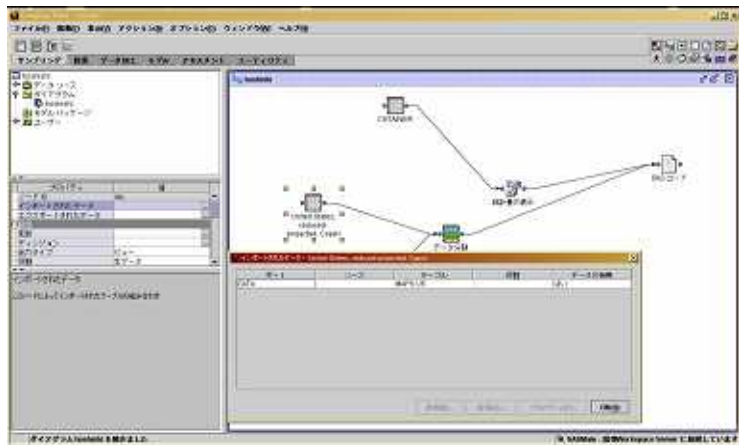


<レポート生成>

実行開始 日付	実行終了 時刻	実行終了 日付	実行終了 時刻	アプリケーション名	アクション名	ユーザー名	オブジェクト ユーザー名	データセット名	ファイル名
2007/11/14	13:12:00.547	2007/11/14	13:12:00.547	SAS EG	META ACCESS	passadm			
2007/11/14	13:12:08.390	2007/11/14	13:12:08.390	SAS EG	EG Workspace	passadm	passadm		
2007/11/14	13:12:09.230	2007/11/14	13:12:09.230	SAS EG	EG Workspace	passadm	passadm	_PRODSAVAIL	
2007/11/14	13:12:15.141	2007/11/14	13:12:15.406	SAS EG	OPEN DATA SET	passadm	passadm	PASSWORDINFO	
2007/11/14	13:13:55.750	2007/11/14	13:13:55.797	SAS EG	EXPORT TO LOCAL	passadm	passadm	検索(&E)...	3c:\windows\TEMP\SEG1920\0f6cbfd4c44e6f59f2b7e4
2007/11/14	13:14:01.250	2007/11/14	13:14:01.281	SAS EG	OPEN DATA SET	passadm	passadm	PASSWORDINFO.xls (PASSWORDINFO)	
2007/11/14	13:15:05.031	2007/11/14	13:15:05.062	SAS EG	EXPORT TO LOCAL	passadm	passadm	パスワード	3c:\windows\TEMP\SEG1920\057004195ad99494c6bf432c

「ユーザー名」
「どのデータセットから」
「エクスポートファイル名」
などEG操作履歴の詳細までレポートिंगが
出来ます。

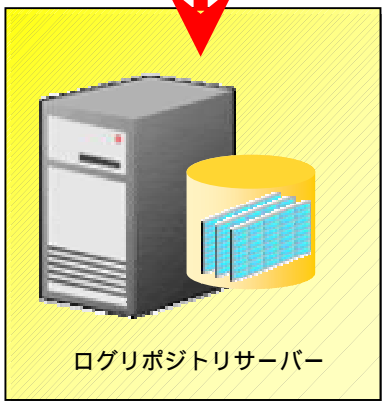
WEEDS SAS - Traceサンプルレポート 「EM操作: データ加工 / 分析」



< EMデータ加工操作 >



< 操作履歴取得 >



ログリポジトリサーバー



< レポート生成 >

「誰が」
「いつ」
「どのデータセットに対して操作を行ったのか」
など詳細な操作履歴まで監査する事が出来ます。

実行開始		実行終了		アプリケーション名	アクション名	ユーザー名	オブジェクト名	データセット名	ファイル名	作業番号
日付	時刻	日付	時刻							
2007/10/23	23:39:00.580	2007/10/23	23:39:49.970	SAS EM	EM START	tel	tel			
2007/10/23	23:39:00.920	2007/10/23	23:39:40.670	SAS EM	EM Workspace	tel	tel	MAPS.US		1
2007/10/23	23:39:00.920	2007/10/23	23:39:40.670	SAS EM	EM Workspace	tel	tel	MAPS.US		2
2007/10/23	23:39:00.920	2007/10/23	23:39:40.670	SAS EM	EM Workspace	tel	tel	MAPS.US		3

WEEDS SAS - Traceサンプルレポート「検索条件」

<レポート画面>

The screenshot shows the WEEDS SAS-Trace application interface. A red box highlights the search filter section on the right, which includes:

- 監視レポート選択** (Monitoring Report Selection): A list with options like 'ユーザー利用履歴' (User Usage History), 'アプリケーション利用履歴' (Application Usage History), and 'アプリケーション利用履歴詳細' (Application Usage History Details).
- ユーザー氏名** (User Name): A dropdown menu with 'SAS管理ユーザ' (SAS Management User) selected.
- OSユーザー名** (OS User Name): A dropdown menu with 'Administrator' selected.
- 部署** (Department): A dropdown menu with 'セールスコンサルティング部' (Sales Consulting Department) selected.
- アプリタイプ** (App Type): A dropdown menu with 'SAS EG' selected.
- データセット名** (Dataset Name): A list of dataset names including 'ACCENTRY', 'ADMIN.EMAIL_B.1', 'ADOMSG', 'ADSMMSG', 'B', 'BUY', 'CANDY', 'CLASS', 'COMMON.TBL_BRINF', 'DBSCHEMA', and 'DIRECTRY'.
- 監視報告書生成** (Generate Monitoring Report): A button at the bottom right of the filter section.

On the left, a smaller screenshot shows the main application window with a calendar and a data table. A red box highlights the search filter section in this window as well.

<検索条件レポート>

WEEDS SAS-Trace									
条件検索									
期間	2007/10/23~2007/10/23	氏名	匿名	マシン名	WEEDS12	OSユーザー名	Administrator	部署	セールスコンサルティング部
ユーザー名	shesh	ユーザーID	0011	アプリタイプ	SAS EG	データセット名	ACCENTRY	監視報告書生成	
実行開始	実行終了	アプリケーション名	アクション名	ユーザー名	オブジェクト	データセット名	ファイル名	作業番号	
2007/10/23 23:39:40.766	2007/10/23 23:39:40.766	SAS EG	META ACCESS	project	project				
2007/10/23 23:49:06.516	2007/10/23 23:49:06.516	SAS EG	OBJ ACCESS	project	project			1	options metaport=8561 meta
2007/10/23 23:39:40.766	2007/10/23 23:39:40.766	SAS EG	EG Workspace	project	project	ASIA		2	%let EM_USERID = %bquote

様々な角度から条件指定が可能です。
1つの操作に特化した監査が実現出来ます。

検索指定項目				SAS EG		-				
実行開始		実行終了		アプリケーション名	アクション名	ユーザー名	オブジェクト	データセット名	ファイル名	作業番号
日付	時刻	日付	時刻			ユーザー名				
2007/10/23	23:39:40.766	2007/10/23	23:39:40.766	SAS EG	META ACCESS	project	project			
2007/10/23	23:49:06.516	2007/10/23	23:49:06.516	SAS EG	OBJ ACCESS	project	project			1
2007/10/23	23:39:40.766	2007/10/23	23:39:40.766	SAS EG	EG Workspace	project	project	ASIA		2

WEEDS SAS-Traceサンプルレポート

Microsoft Excel - SAS_DATA_SETList.xls

ファイル(F) 編集(E) 表示(V) 挿入(I) 書式(O) ツール(T) データ(D) ウィンドウ(W) ヘルプ(H)

WEEDS SAS-Trace

質問を入力

2009年03月31日

WEEDS SAS-Trace

対象期間 2008/03/01 ~2008/03/31

監査対象SASサーバー weeds Server

監査指定項目

ログイン日時 データセット名 ユーザー名 オブジェクトユーザー名 アプリケーション名 OSユーザー名 マシン名 IPアドレス データセットアクセス数

ログイン日時	データセット名	ユーザー名	オブジェクトユーザー名	アプリケーション名	OSユーザー名	マシン名	IPアドレス	データセットアクセス数
2008/03/25	PRODS.AVAL		mhoshi001	SAS EG	Administrator	weeds1 2	192.168.11.110	2
			aadachi004	SAS EG	7899	weeds009	192.168.11.112	3
	weedsdata		mhoshi001	SAS EG	Administrator	weeds1 2	192.168.11.110	10
			aadachi004	SAS EG	7899	weeds009	192.168.11.112	31
	WEEDS_SAS TRACE_TEST		mhoshi001	SAS EG	Administrator	weeds1 2	192.168.11.110	2
			aadachi004	SAS EG	7899	weeds009	192.168.11.112	3
	WEEDS_20090325		mhoshi001	SAS EG	Administrator	weeds1 2	192.168.11.110	11
			aadachi004	SAS EG	7899	weeds009	192.168.11.112	9
	TANUKI1		mhoshi001	SAS EG	Administrator	weeds1 2	192.168.11.110	6
			aadachi004	SAS EG	7899	weeds009	192.168.11.112	3
WEEDS_DB-Trace_DATA		mhoshi001	SAS EG	Administrator	weeds1 2	192.168.11.110	12	
		aadachi004	SAS EG	7899	weeds009	192.168.11.112	21	
TEST		mhoshi001	SAS EG	Administrator	weeds1 2	192.168.11.110	16	
		aadachi004	SAS EG	7899	weeds009	192.168.11.112	12	
SASHELP.CLASS AS CLASS		mhoshi001	SAS EG	Administrator	weeds1 2	192.168.11.110	1	
		aadachi004	SAS EG	7899	weeds009	192.168.11.112	2	
2008/03/26	TEST_20090326		mhoshi001	SAS EG	Administrator	weeds1 2	192.168.11.110	4
			aadachi004	SAS EG	Administrator	weeds009	192.168.11.112	7
	TANUKI02		mhoshi001	SAS EG	Administrator	weeds1 2	192.168.11.110	3
	TANUKI03		mhoshi001	SAS EG	Administrator	weeds1 2	192.168.11.110	3
	WEEDS_Unix-Trace_20071223_test1		aadachi004	SAS EG	7899	weeds009	192.168.11.112	12

図形の調整(R) オートシェイプ(U) コマンド

データセット毎のアクセス状況をレポート致します。
 「いつ」「どのデータセットが」「どのアプリケーション」「どのユーザー」にてアクセスされたのかを確認

WEEDS SAS - Traceサンプルレポート

Microsoft Excel - SAS_LOGIN.xls

ファイル(F) 編集(E) 表示(V) 挿入(I) 書式(O) ツール(T) データ(D) ウィンドウ(W) ヘルプ(H)

質問を入力してください

78%

Arial Black 14

WEEDS SAS-Trace

出力日: 2009年04月13日

WEEDS SAS-Trace

ログイン一覧レポート

対象期間 2009/03/25 対象サーバ weeds Server

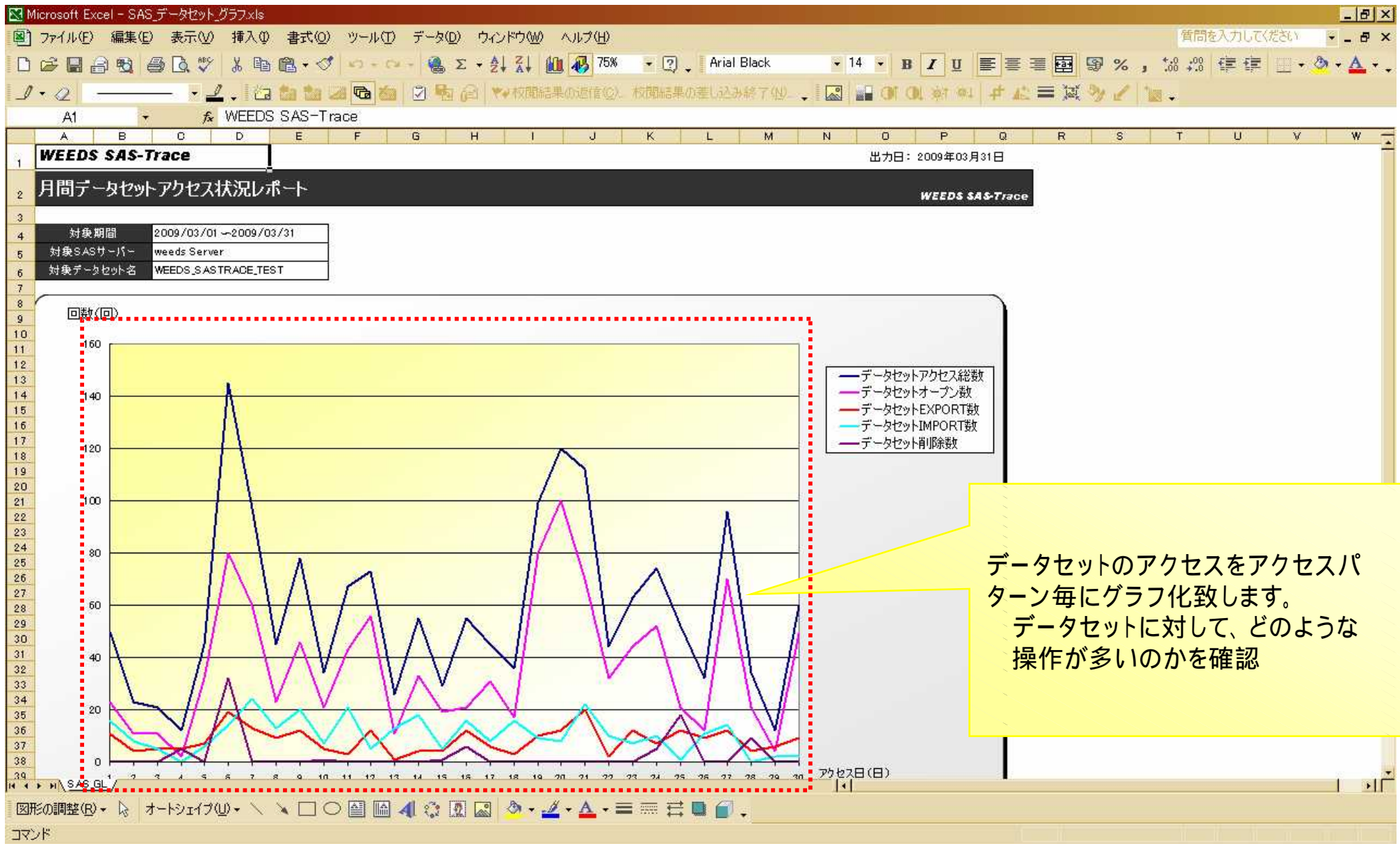
部署名 WEEDS開発

監査指定項目

OSログイン日時	OSログオフ日時	SAS開始日時	SAS終了日時	氏名	メタユーザー名	オブジェクトユーザー名	OSユーザー名	アプリケーション名
2009/03/25(水)16:01:13.000	2009/03/25(水)18:03:05.077	2009/03/25(水)16:01:15.156	2009/03/25(水)18:02:07.950	WEEDS星		mhoshi001	Administrator	SAS EG
2009/03/25(水)13:33:35.000	2009/03/25(水)13:56:34.413	2009/03/25(水)13:35:39.422	2009/03/25(水)13:35:54.516	WEEDS安達		aadachi004	07477	SAS EM
		2009/03/25(水)13:40:13.316	2009/03/25(水)13:46:18.682	WEEDS安達		aadachi004	07477	SAS EM
		2009/03/25(水)13:47:29.596	2009/03/25(水)13:47:35.818	WEEDS安達		aadachi004	07477	SAS EM
		2009/03/25(水)13:47:39.241	2009/03/25(水)13:47:43.650	WEEDS安達		aadachi004	07477	SAS EM
2009/03/25(水)10:31:47.000	2009/03/25(水)18:37:51.667	2009/03/25(水)10:38:46.235	2009/03/25(水)16:37:35.725	WEEDS星		mhoshi001	Administrator	SAS EG
		2009/03/25(水)10:55:01.804	2009/03/25(水)11:06:38.971	WEEDS星		mhoshi001	Administrator	SAS EG
		2009/03/25(水)11:06:58.330	2009/03/25(水)11:11:41.693	WEEDS星		mhoshi001	Administrator	SAS EG
		2009/03/25(水)11:13:59.248	2009/03/25(水)14:28:36.448	WEEDS星		mhoshi001	Administrator	SAS EG
		2009/03/25(水)14:50:01.718	2009/03/25(水)16:00:00.668	WEEDS星		mhoshi001	Administrator	SAS AMD
		2009/03/25(水)16:16:01.065	2009/03/25(水)16:16:59.876	WEEDS星		mhoshi001	Administrator	SAS AMD
		2009/03/25(水)16:34:43.017	2009/03/25(水)18:35:19.136	WEEDS星		mhoshi001	Administrator	SAS AMD

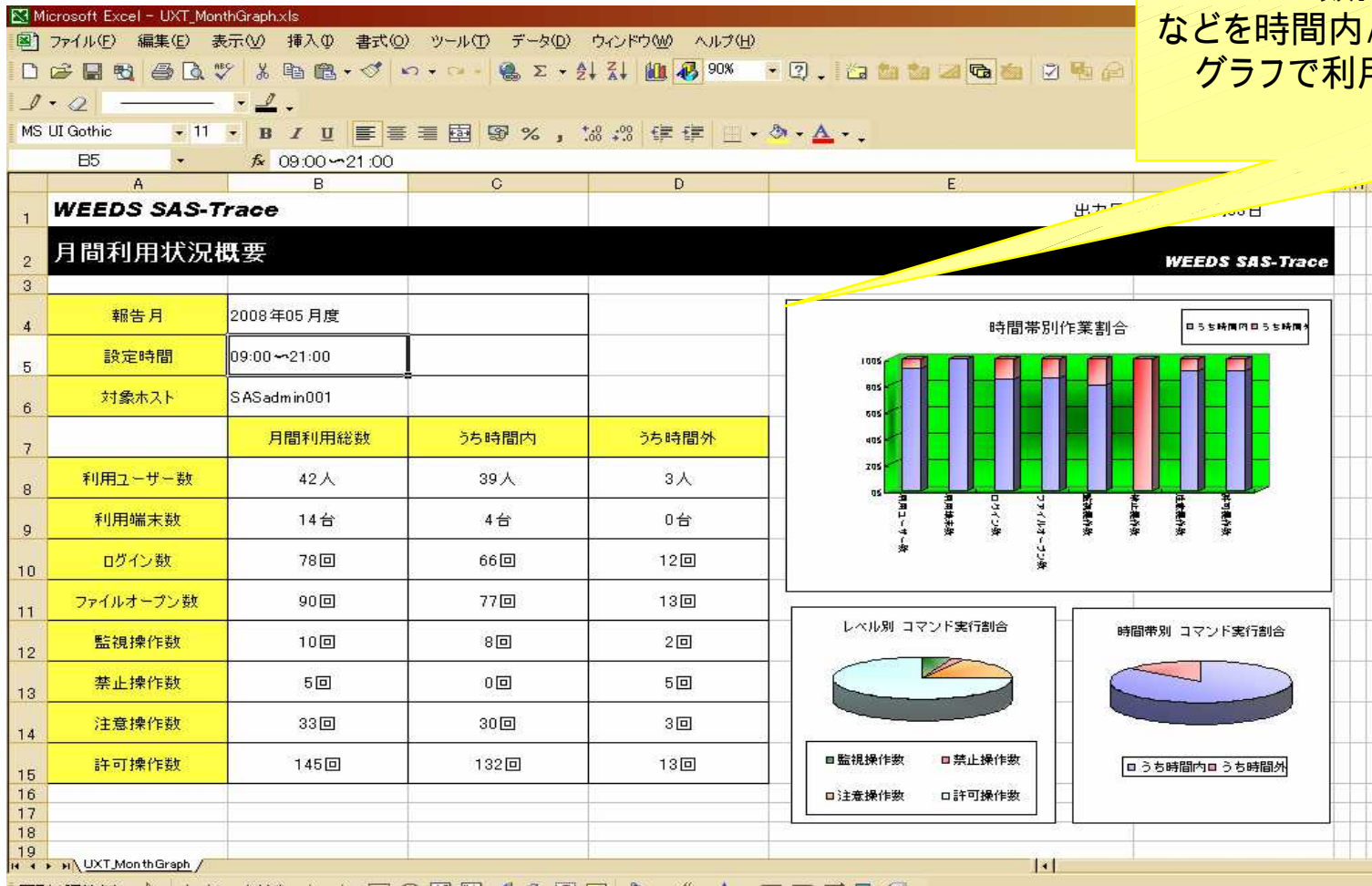
指定日時でのログイン状況をレポートिंग致します。
EGのみならず、EMを使用した際のログイン情報も出力する事が可能です。

WEEDS SAS - Traceサンプルレポート



WEEDS SAS - Traceサンプルレポート「月間利用状況概要」

< 月間利用状況概要 >



月間トータルでの「ユーザー数」「端末数」「ログイン数」「操作内容」などを時間内/時間外での利用状況を出力します。グラフで利用状況を把握する事が出来ます。

WEEDS SAS - Trace取得可能項目一覧

取得可能操作一覧	
OSユーザー名	EG操作 データセット削除
メタユーザー名	EG操作 タスク実行
オブジェクトユーザー名	EM操作 ログイン
アプリケーション名	EM操作 データセット参照
データセット名	EM操作 データセット探索
メタデータサーバへのアクセス(EGログイン)	EM操作 ノード実行
オブジェクトスポーナーへのアクセス	EXCEL操作 タスク実行(AMO利用)
EG操作 データセットオープン	管理コンソール操作 ライブラリ作成
EG操作 データセットエクスポート	管理コンソール操作 ユーザー作成
EG操作 データセットインポート	管理コンソール操作 ログイン作成
EG操作 プリントアウト	SAS発行SQL取得

WEEDS

TRUE TECHNOLOGY TO THE WORLD

ご清聴、誠にありがとうございました。

開発・販売

ウーズ・システムズ株式会社

東京都豊島区高田1-36-10 〒171-0033

アペックヒルズ目白 本社301号 / 開発センター302号

TEL / FAX 03-5950-6350

URL: <http://www.weeds-japan.co.jp>