ログの出力形式詳細情報

ダブルブラウザでは　　色の部分のみが出力されます。

No	項目名	出力内容	データ型	値のサンプル	備考
1	No	ログ番号	bigint	3789718	
2	時刻	操作を行った時刻	datetime	2015-08-29 19:10:49.397	YYYY-MM-DD hh:mm:ss.mmm
3	コンピュータ名	操作を行ったコンピュータ名	varchar(30)	SERVER01	
4	ログインユーザ	操作を行ったユーザ	varchar(64)	SERVER01\admin	コンピュータ名¥アカウント or ドメイン名¥アカウント
5	イベント	操作内容 (1) ログイン (2) ログオフ (3) 切断 (4) 画面ロック開始 (5) 画面ロック解除 (6) アプリケーション起動 (7) アプリケーション終了 (8) ファイル参照 (9) ファイル書込 (10) ライティングソフト書込 (11) ファイルコピー (12) ファイル移動 (13) ファイル削除 (14) ウィンドウタイトル (15) 印刷開始 (16) 印刷終了 (17) 送信 (18) 受信 (19) ウェブ (20) 通信 (21) コピー (22) ペースト (23) コマンド (24) イベントログ (25) デバイス接続 (26) デバイス取出 (27) アップロード (28) FTP コマンド (29) システム日時変更	varchar(128)	ログイン	ダブルブラウザでは 「ウェブ」のみ対象

No	項目名	出力内容	データ型	値のサンプル	備考
6	アプリケーションパス	操作に使用したアプリケーションパス	varchar(2000)	C:\Windows\Explorer.EXE	ダブルブラウザでは 「Firefox」のみ
7	ウィンドウタイトル	ウィンドウタイトル	varchar(1000)	スタート メニュー	
8	ファイルパス	操作対象ファイルパス	varchar(2048)	C:\Documents and Settings\admin\デスクトップ¥新しいフォルダ¥ドキュメント.txt	
9	ファイルパス（移動先）	操作後のファイルパス	varchar(2048)	C:\Documents and Settings\admin\デスクトップ¥新しいフォルダ(2)\ドキュメント.txt	ファイルコピー、ファイル移動時のみ使用
10	デバイスタイプ	操作対象ファイルのデバイスタイプ (1) HDD (2) CDROM (3) REMOVABLEDISK (4) NETWORK (5) RAM (6) UNKNOWN (7) NO ROOT DIR (8) PORTABLEDEVICE (9) NETWORK(REMOVABLEDISK)	varchar(100)	HDD	
11	デバイスタイプ（移動先）	操作後のファイルのデバイスタイプ (1) HDD (2) CDROM (3) REMOVABLEDISK (4) NETWORK (5) RAM (6) UNKNOWN (7) NO ROOT DIR (8) PORTABLEDEVICE (9) NETWORK(REMOVABLEDISK)	varchar(100)	REMOVABLEDISK	ファイルコピー、ファイル移動時のみ使用

No	項目名	出力内容	データ型	値のサンプル	備考
12	クリップボード内容	クリップボードの内容	varchar(4000)	C:\Documents and Settings\admin\デスクトップ¥新しいフォルダ¥ドキュメント.txt	
13	種別	クリップボード使用の種別 (1) TEXT (2) FILE (3) PICTURE	varchar(100)	FILE	
14	印刷ドキュメント	印刷したファイル	varchar(1000)	提案資料1.ppt	
15	プリンタ名	印刷先のプリンタ名	varchar(100)	Canon LBP-2810	
16	印刷頁数	印刷ページ数	varchar(100)	2	
17	プリンタタイプ	印刷したプリンタのタイプ (1) ローカルプリンタ (2) ネットワークプリンタ	varchar(100)	ネットワークプリンタ	
18	URL	WEB アクセスしたサイトの URL	varchar(2000)	http://www.google.co.jp	
19	送信元アドレス	メール送信時の From アドレス	varchar(512)	aaa<aaa@sec.jp>	
20	送信先アドレス	メール送信時の To、Cc、Bcc アドレス	varchar(1024)	ccc<ccc@sec.jp>;ddd<ddd@sec.jp>;d22<d22@sec.jp>	
21	From	メール送受信時の From アドレス	varchar(1024)	ccc<ccc@sec.jp>	
22	To	メール送受信時の To アドレス	varchar(2048)	ddd<ddd@sec.jp>;d22<d22@sec.jp>	
23	CC	メール送受信時の Cc アドレス	varchar(2048)	eee<eee@sec.jp>;e22<e22@sec.jp>	

No	項目名	出力内容	データ型	値のサンプル	備考
24	件名	メール送受信時の件名	varchar(2048)	来週の商談について	
25	コンピュータ名（操作端末）	接続元端末のコンピュータ名	varchar(64)	CLIENT01	RDP,ICA 等でのリモート接続時の接続元の端末情報
26	MAC アドレス（操作端末）	接続元端末の MAC アドレス	varchar(31)	00:1F:D0:CE:8B:D2	RDP,ICA 等でのリモート接続時の接続元の端末情報
27	IP アドレス（操作端末）	接続元端末の IP アドレス	varchar(16)	0.0.0.0	RDP,ICA 等でのリモート接続時の接続元の端末情報
28	セッション名	操作を行ったログインセッション名	varchar(128)	Console	
29	セッション ID	操作を行ったログインセッション ID	varchar(32)	1	
30	SID	操作を行ったコンピュータの SID	varchar(256)	S-1-5-21-1431655909-1449347727-864547803	
31	MAC アドレス	操作を行ったコンピュータの MAC アドレス	varchar(31)	00:1F:D0:CE:8B:D2	
32	IP アドレス	操作を行ったコンピュータの IP アドレス	varchar(16)	192.168.0.134	
33	接続先 IP アドレス	通信先の IP アドレス	varchar(2000)	192.168.0.1	
34	ポート番号	通信先のポート番号	varchar(100)	1434	
35	メール本文	メール送信時のメール本文	varchar(4000)	○×システム　△△様お世話になります。	

No	項目名	出力内容	データ型	値のサンプル	備考
36	添付ファイル名	メール送信時の添付ファイル名	varchar(2048)	提案資料1.ppt	
37	ソース	Windows イベントログの「ソース」項目	varchar(64)	Microsoft-Windows-Security-Auditing	
38	種類	Windows イベントログの「種類」項目	varchar(128)	成功の監査	
39	分類 ID	Windows イベントログの「分類 ID」項目	varchar(64)	12289	
40	分類	Windows イベントログの「分類」項目	varchar(64)	セキュリティ システムの拡張	
41	イベント ID	Windows イベントログの「イベント ID」項目	varchar(64)	4697	
42	説明	Windows イベントログの「説明」項目	varchar(4000)	サービスがシステムにインストールされました。サブジェクト: セキュリティ ID: …	
43	実行コマンド	実行コマンド	varchar(2000)	ipconfig	
44	ICL ファイル名	ICL ファイル名	varchar(512)	C:\SessionRecordings\2013\12\12****.icl	Citrix Smart Auditor と連携した、IVEX Recording 機能を導入している場合のみ出力
45	ベンダ ID	外部デバイスのベンダ ID	varchar(256)	IMATION	
46	プロダクト ID	外部デバイスのプロダクト ID	varchar(256)	IMATION_USB	
47	リビジョン番号	外部デバイスのリビジョン番号	varchar(256)	01	
48	シリアル番号	外部デバイスのシリアル番号	varchar(256)	1234567890	

No	項目名	出力内容	データ型	値のサンプル	備考
49	アラート	アラートログの場合「警告」出力	varchar(32)	警告	
50	部署名	操作を行ったユーザの部署名	varchar(2048)	セキュリティ商事¥営業部	
51	氏名	操作を行ったユーザの氏名	varchar(512)	機密太郎	
52	プロトコル	アップロード時の使用プロトコル	varchar(32)	HTTP	
53	接続先サーバ	アップロード時の接続先サーバ	varchar(256)	jp.f1004.mail.yahoo.co.jp	
54	アップロード先	アップロード時のアップロード先	varchar(2048)	http://jp.f1004.mail.yahoo.co.jp/ya/upload	
55	Bcc	メール送信時の Bcc アドレス	varchar(2048)	fff<fff@sec.jp>;f22<f22@sec.jp>	
56	成否	操作許可/拒否	varchar(256)	拒否	
57	変更前日時	システム日時変更時の変更前日時	varchar(100)	2015/09/30 10:30:58	
58	変更後日時	システム日時変更時の変更後日時	varchar(100)	2015/10/01 10:30:58	
59	経過時間	アプリケーション使用時間 ログイン時間	varchar(128)	00:32:50.600	
60	SCID	iDoperation SC サーバ接続情報	varchar(256)	n:192.168.0.84:18082:24553b6941345b99f92a5ed2fbbb4d5d08ab851c	録画オプション用データ