WIndowsのイベントログ取得方法

1. キーボードの [Windows] + [R] を押します。

2. ファイル名を指定して実行のウィンドウに、「eventvwr」と入力して、 [OK] ボタンをクリック します。

3. 画面左側を [Windows ログ] > [Application] と展開します。画面右側の [すべてのイベントを 名前をつけて保存] をクリックします。

🛃 イベント ビューアー			- 🗆 X
ファイル(F) 操作(A) 表示(V) ヘル	プ(H)		
🗢 🔿 🙋 📅 🚺 🖬			
【書 イベント ビューアー (ローカル)	Application イベント数:	45,482	操作
 > → カスタム ビュー ✓ Windows 日グ ▲ Application 〒 セキュリティ ■ Setup ※マニュレ 	レベル	日付と時刻 ^	Application 🔺 📤
	() 情報	2022/12/20 13:5	🧉 保存されたログを開く
	1 情報	2022/12/20 13:5	🍸 カスタムビューの作成
	() 情報	2022/12/20 13:5 🗸	カスタム ビューのインポート
Forwarded Events	<	>	ログの消去
> 🖺 アプリケーションとサービス ログ	1 イベント 16384, Security-SPP ★ 全般 詳細		▼ 現在のログをフィルター
> 📫 保存されたログ 🔂 サブスクリブション			70/71
	へ ソフトウェア保護サービスの 2122-11-26T04:52:01Z の		—————————————————————————————————————
			📕 すべてのイベントを名前をつけて保存
			このログにタスクを設定
	ログの名前(M):	Application	表示
	リース(S):	Security-SPP	

4. 任意の場所に適切なファイル名を指定し、ファイルの種類をイベントファイルを選択して保存します。

※表示情報 のウィンドウが表示された場合は、表示情報なしを選択しOKとしてください。

5. 画面左側を [Windows ログ] > [システム] と展開します。画面右側の [すべてのイベントを 名前をつけて保存] をクリックします。



6. 任意の場所に適切なファイル名を指定し、ファイルの種類をイベントファイルを選択して 保存します。

※表示情報 のウィンドウが表示された場合は、表示情報なしを選択しOKとしてください。

7. 手順4・手順6で保存したファイルをお送りください。

株式会社エムエステクノシステムズ